ZYXEL NETWORKS

www.zyxel.com

# Handbook

## USG FLEX H Series

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

Firmware Version: uOS1.20

04/2024

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

**Table of Content**



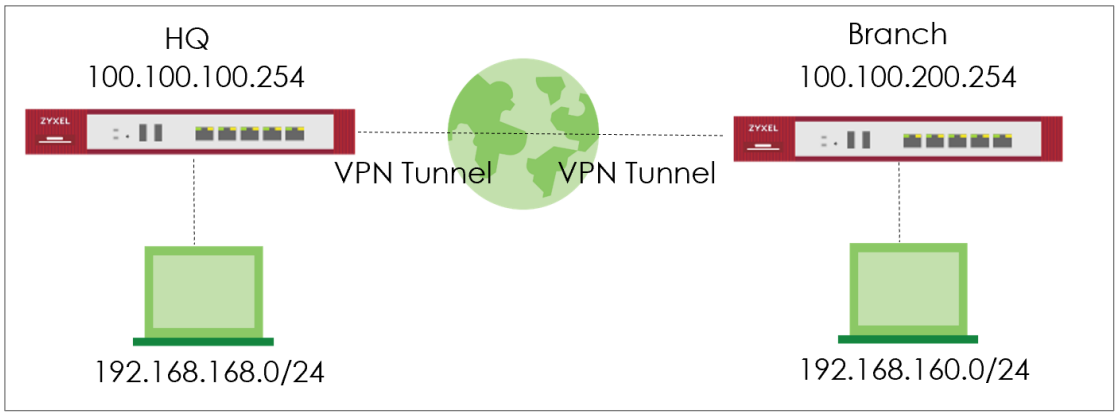
 

# Chapter 1- VPN

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

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

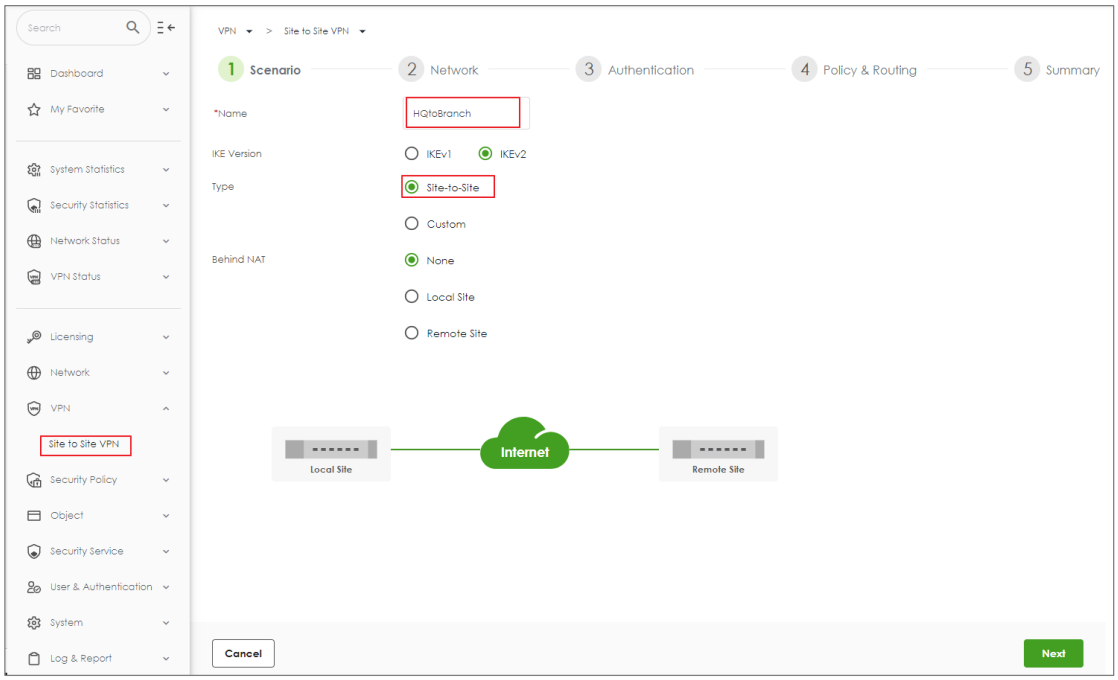


# Set up IPSec VPN Tunnel for HQ

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

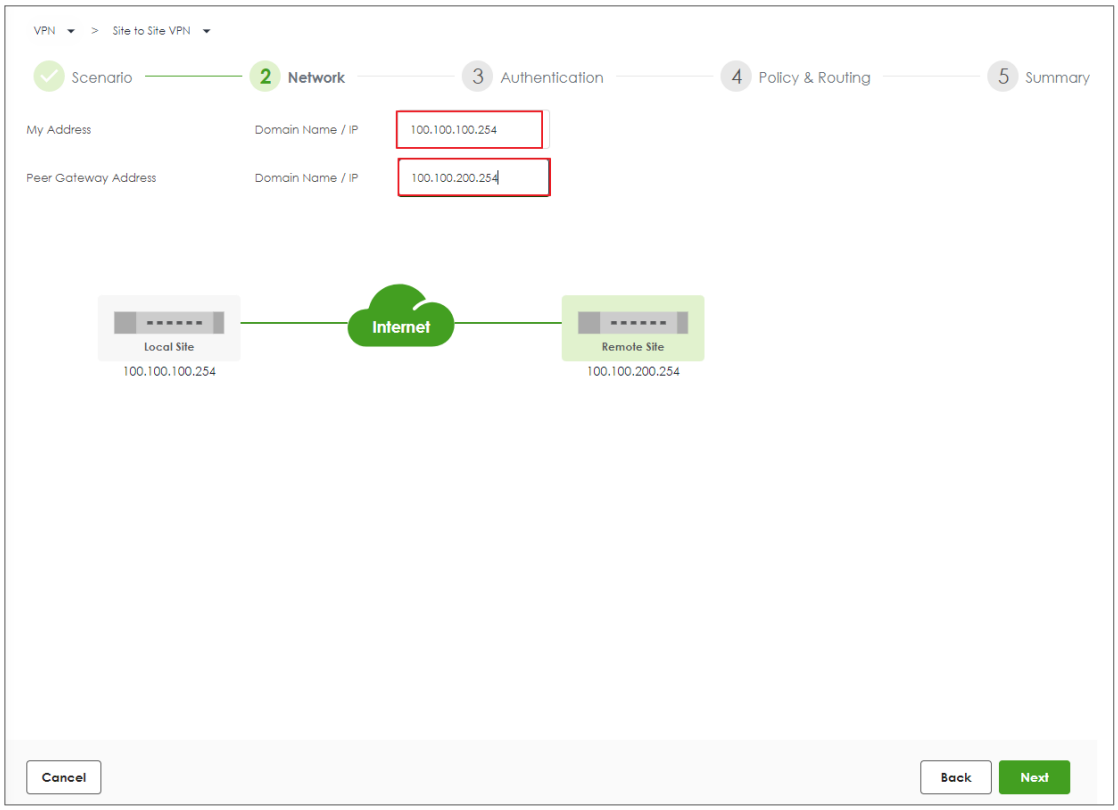
Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site. Click **Next**.



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

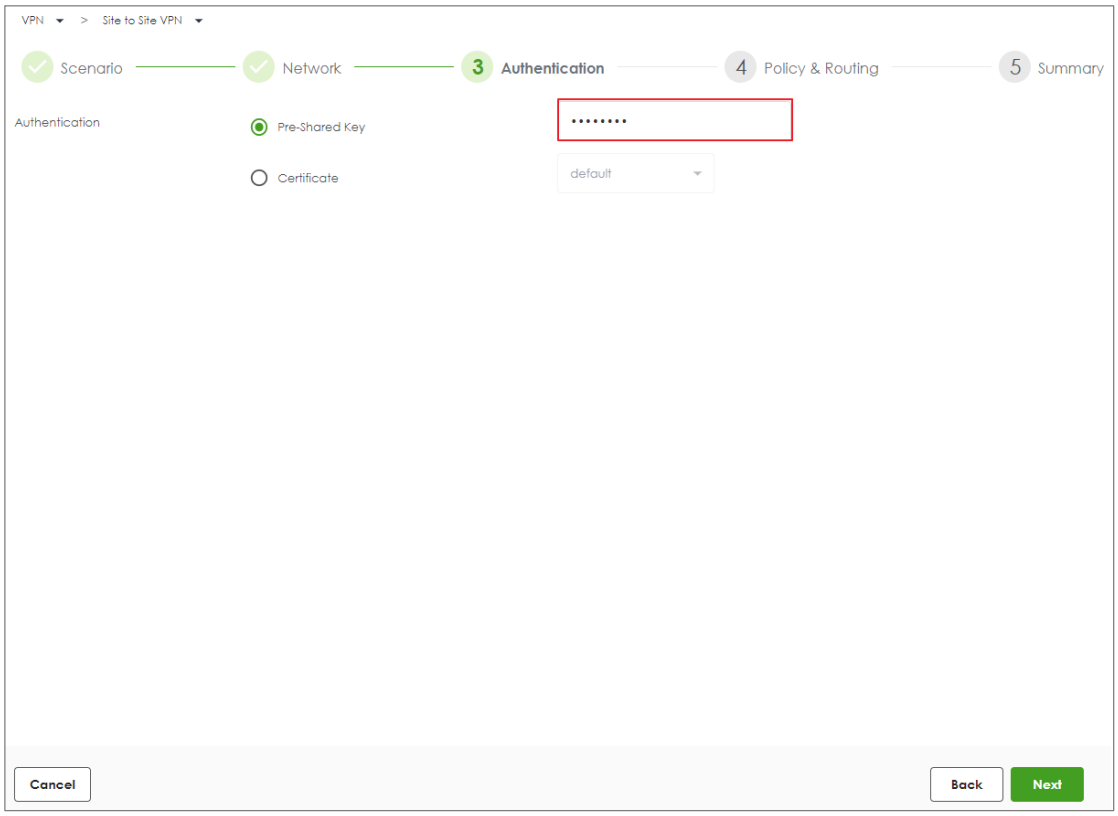
Configure My Address and Peer Gateway Address. Click **Next**.



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

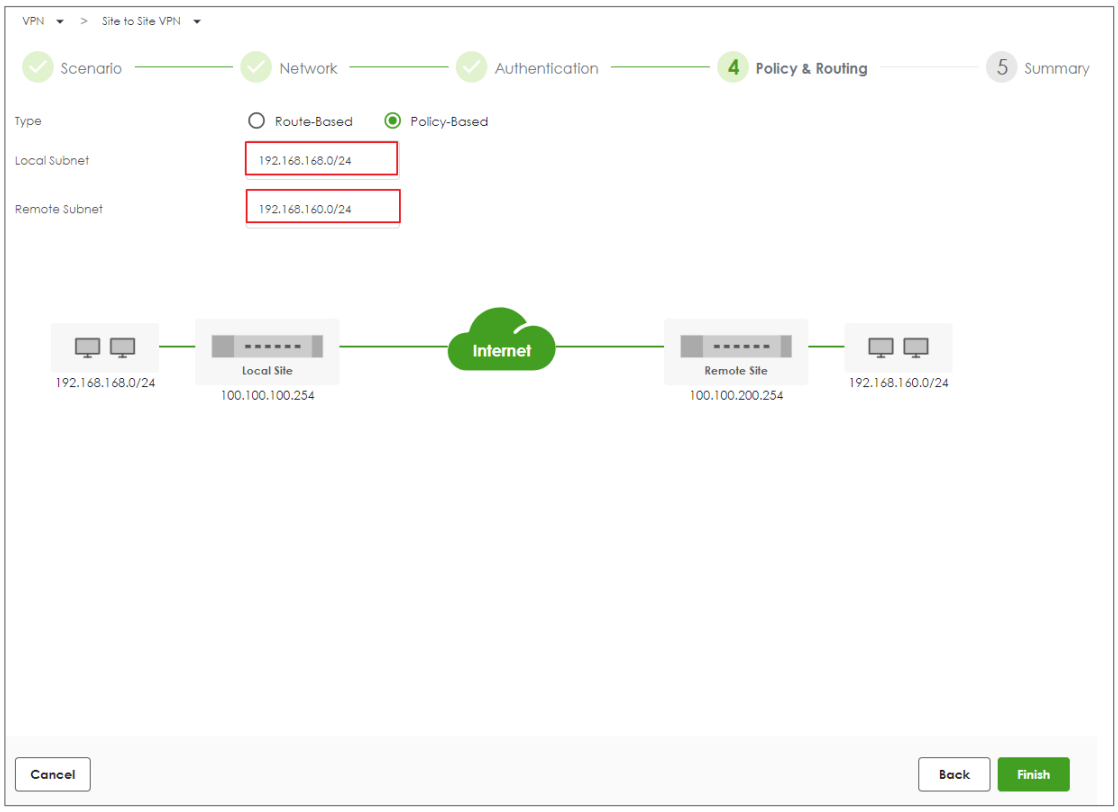
Type a secure Pre-Shared Key. Click **Next**



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

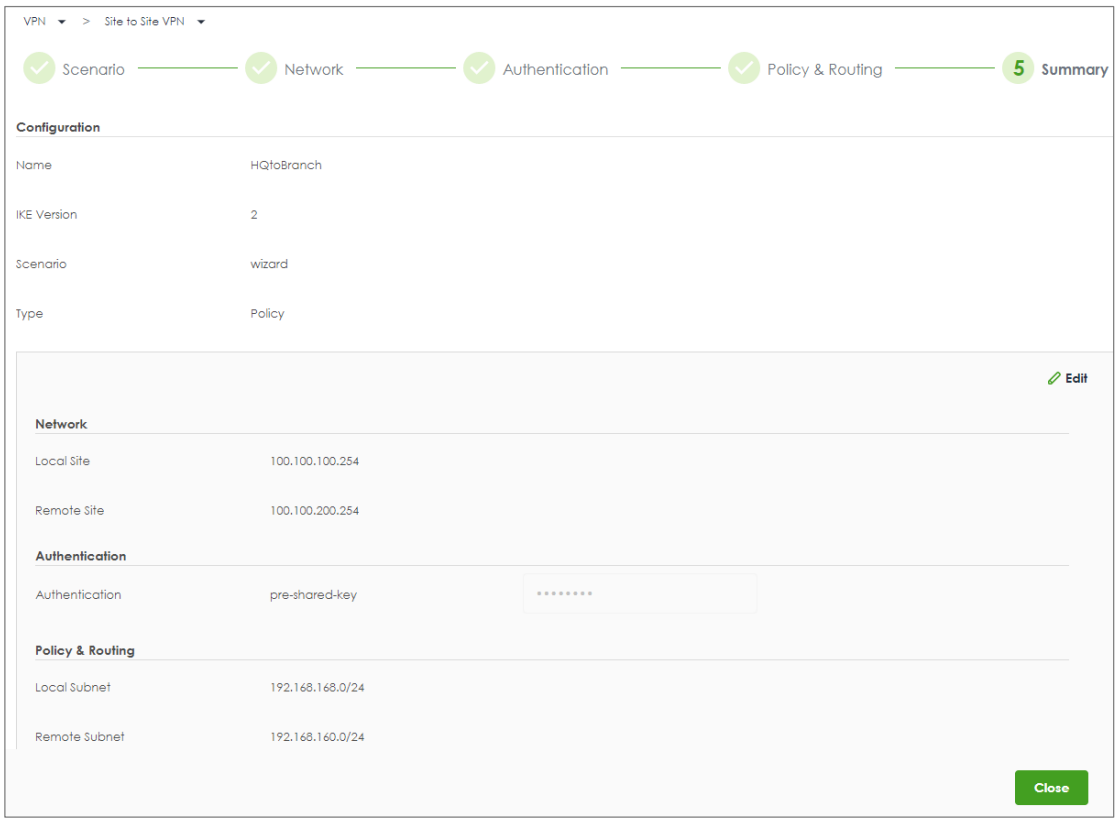
Set Local Subnet to be the IP address of the network connected to the gateway and Remote Subnet to be the IP address of the network connected to the peer gateway.



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

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

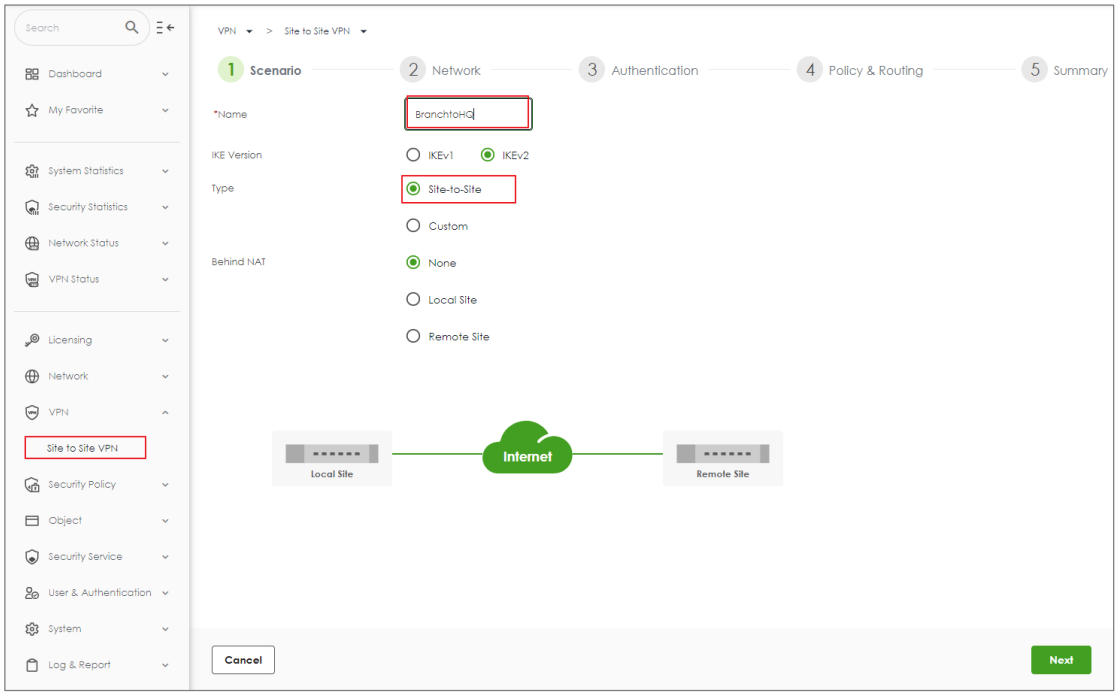


# Set up IPSec VPN Tunnel for Branch

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

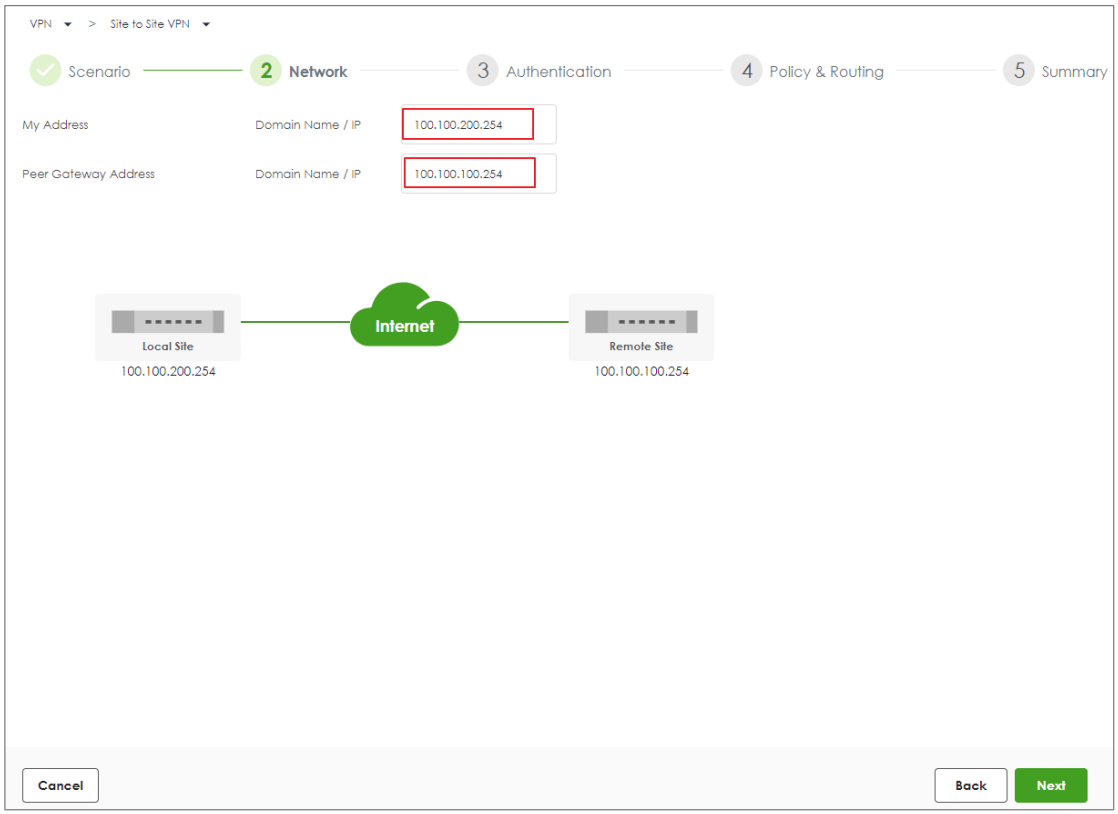
Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site. Click **Next**.



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

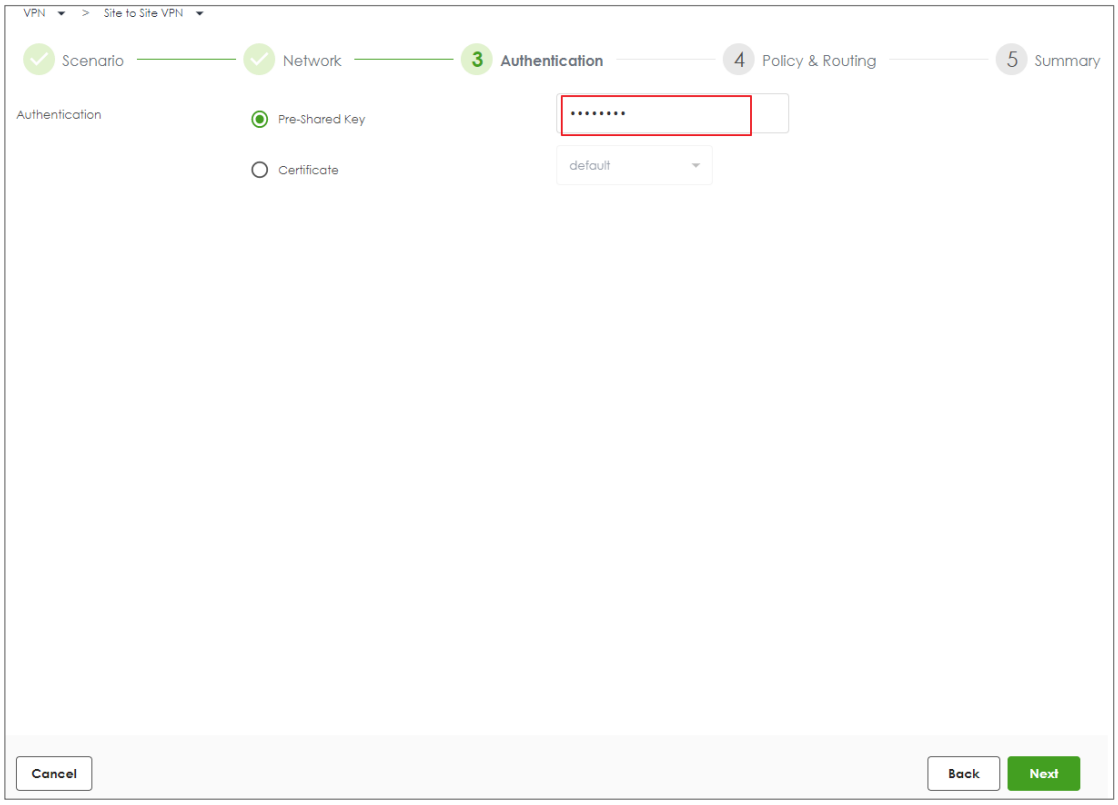
Configure My Address and Peer Gateway Address. Click **Next.**



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

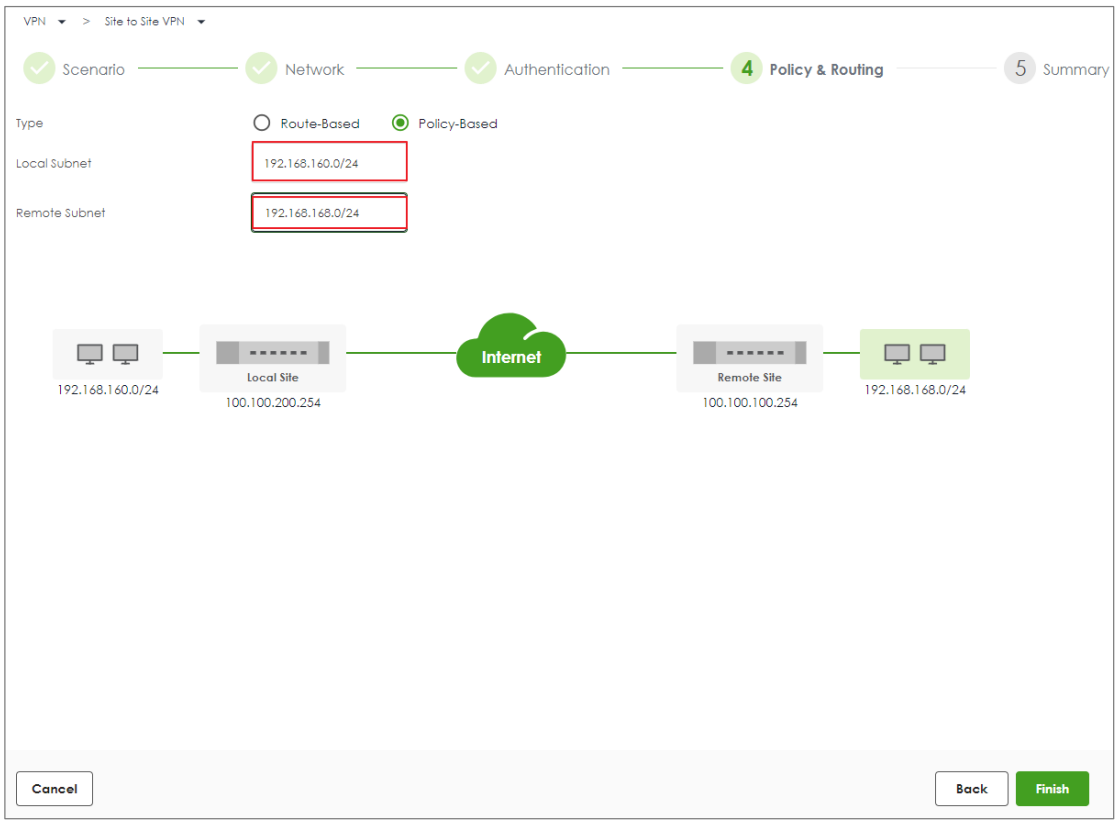
Type a secure Pre-Shared Key. Click **Next.**



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

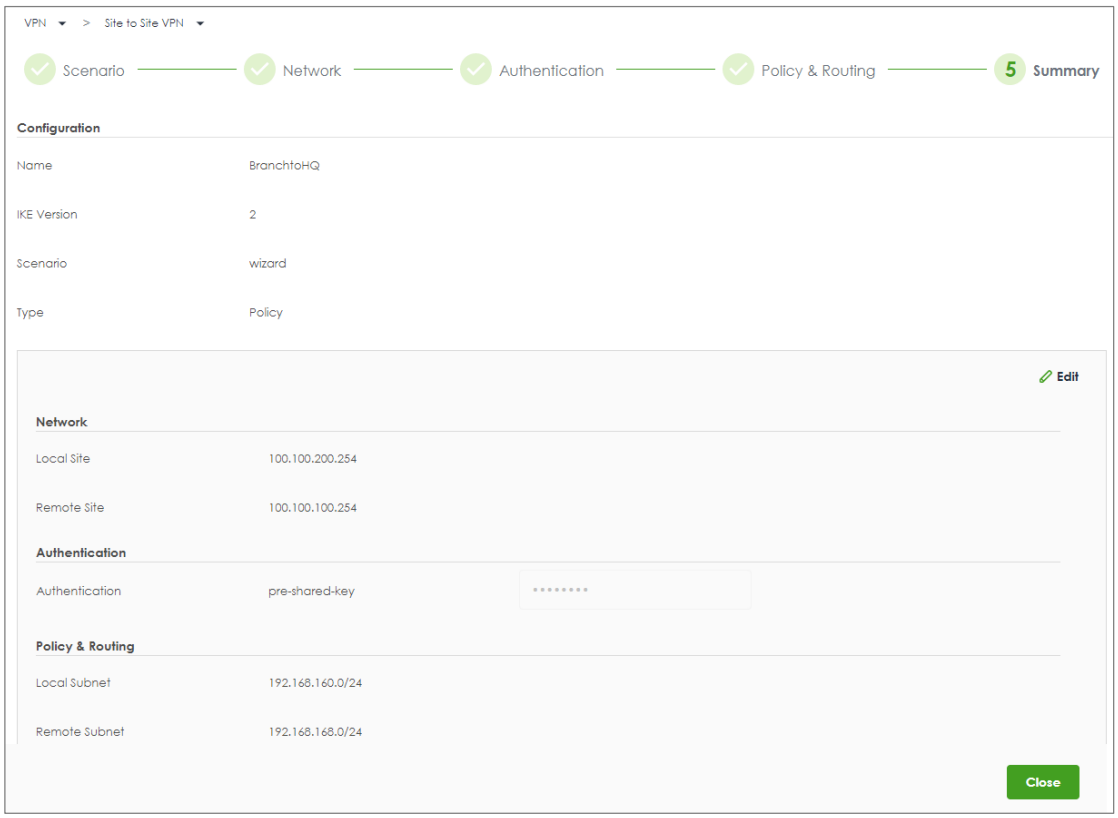
Set Local Subnet to be the IP address of the network connected to the gateway and Remote Subnet to be the IP address of the network connected to the peer gateway.



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

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

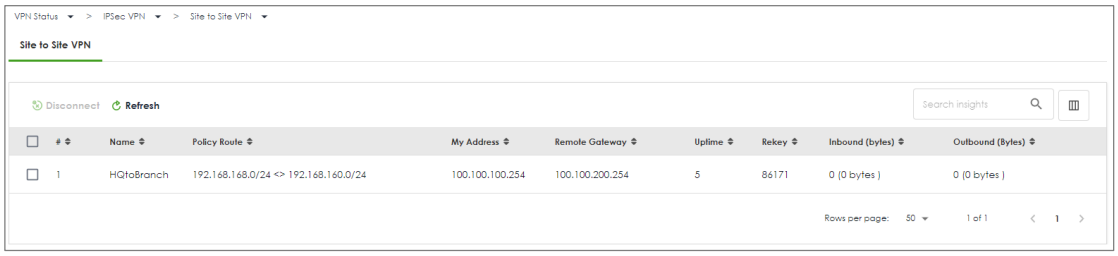


# Test IPSec VPN Tunnel

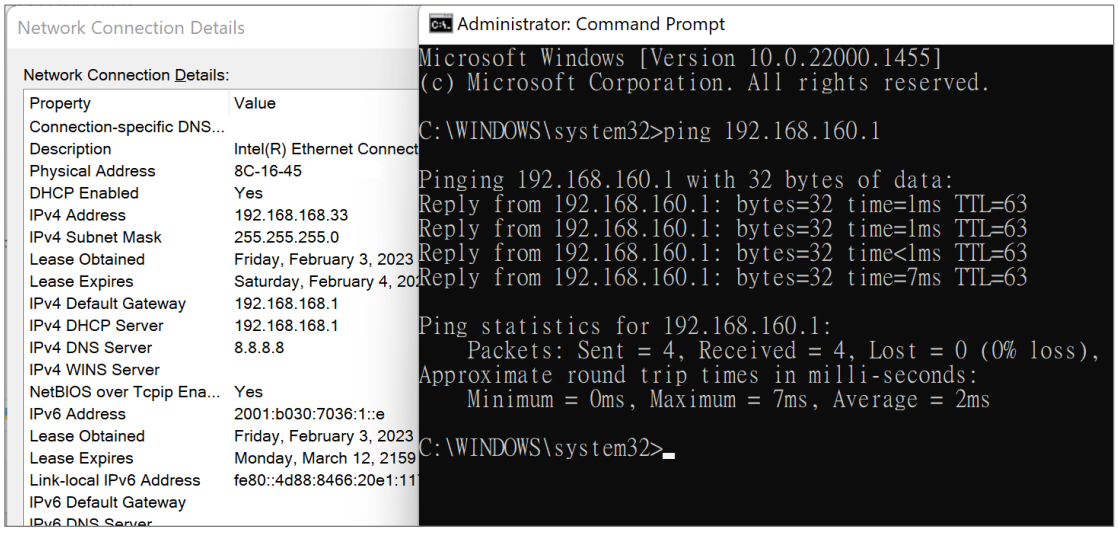
### VPN Status > IPSec VPN

Verify the IPSec VPN status.




### Ping the PC in Branch Office

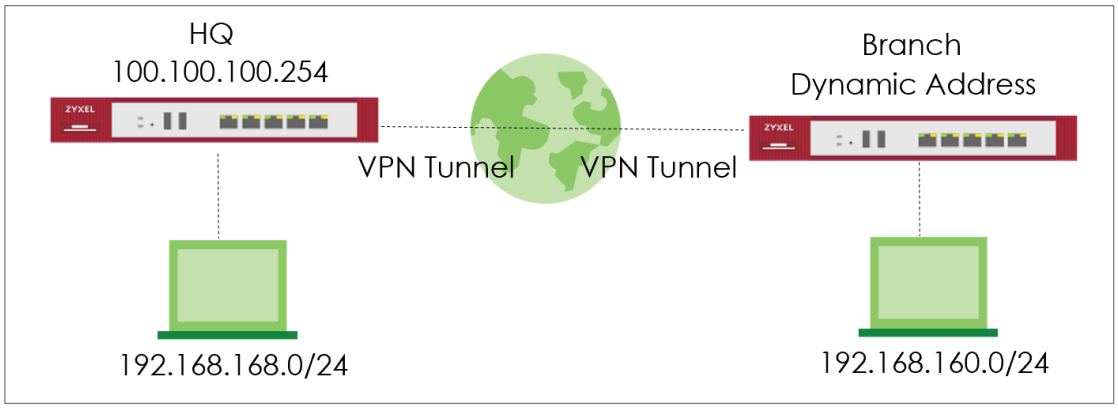
Win 11 > cmd > ping 192.168.160.1



# How to 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.

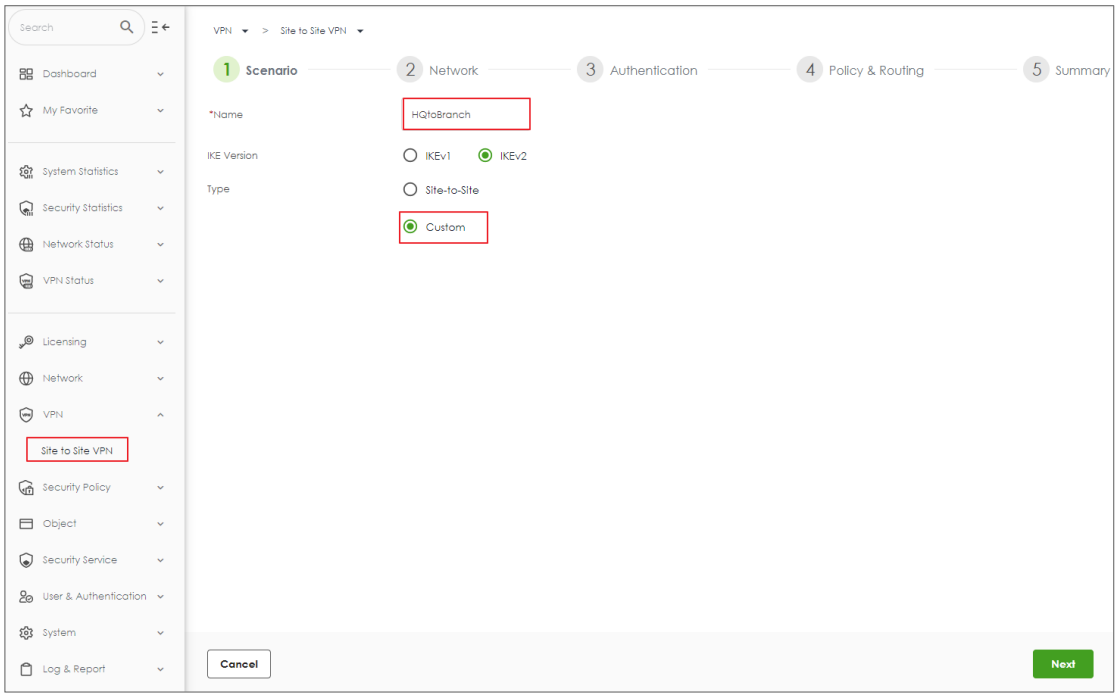


# Set up IPSec VPN Tunnel for HQ

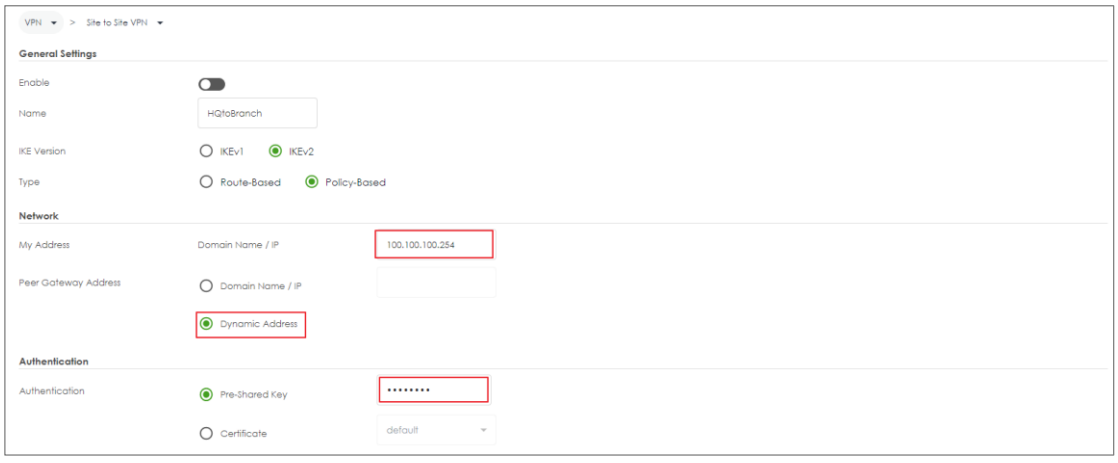
### VPN > Site to Site VPN > Scenario

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



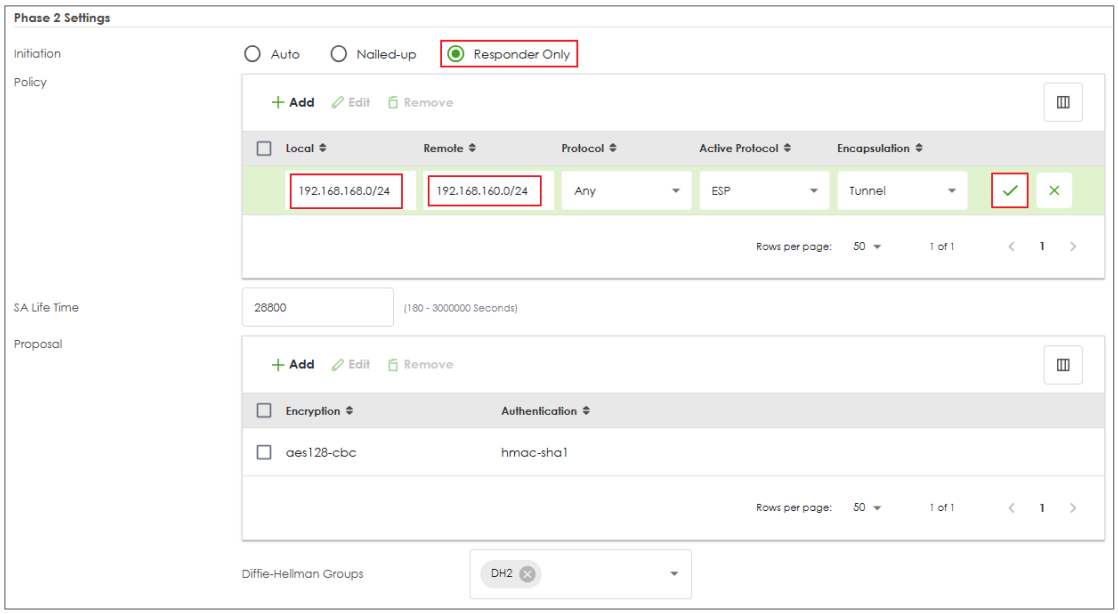

### VPN > Site to Site VPN

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.

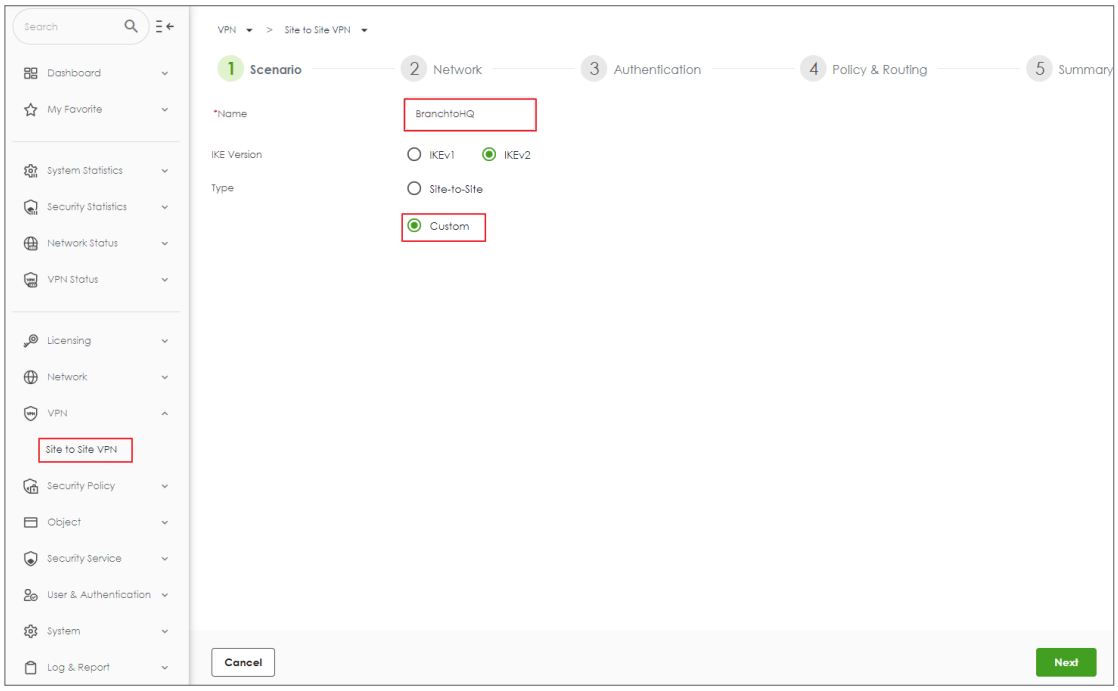


# Set up IPSec VPN Tunnel for Branch

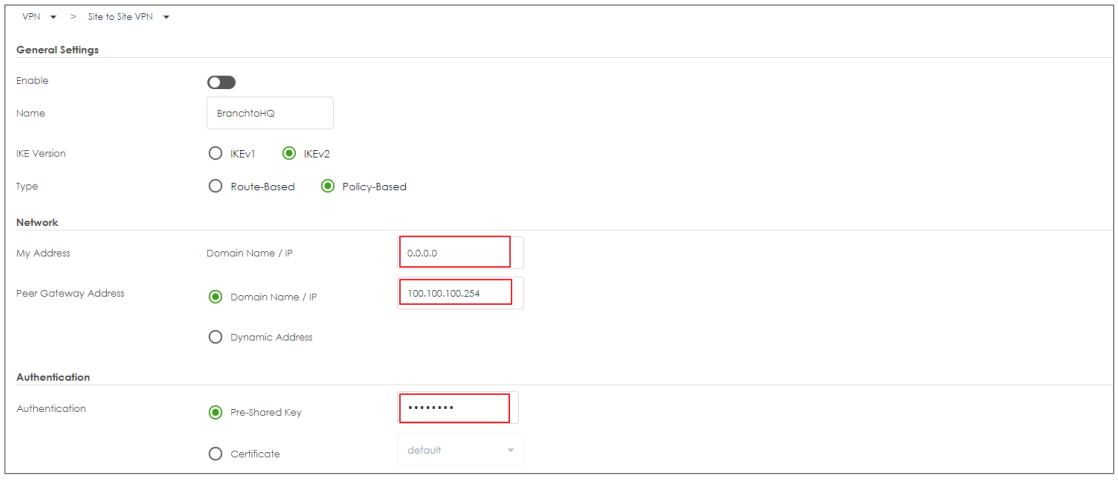
### VPN > Site to Site VPN > Scenario

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



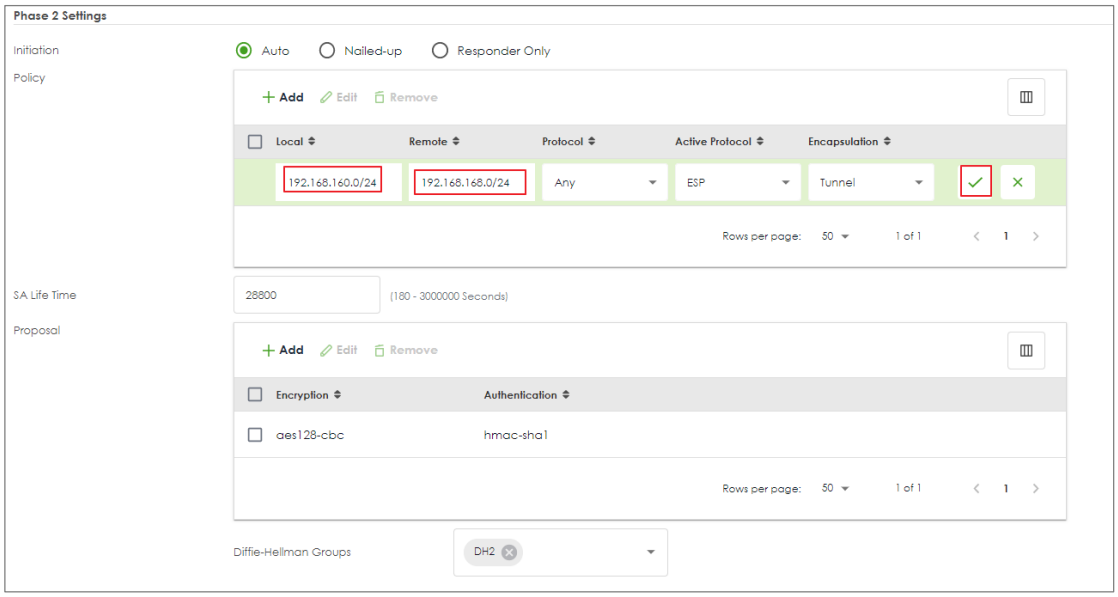

### VPN > Site to Site VPN

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



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

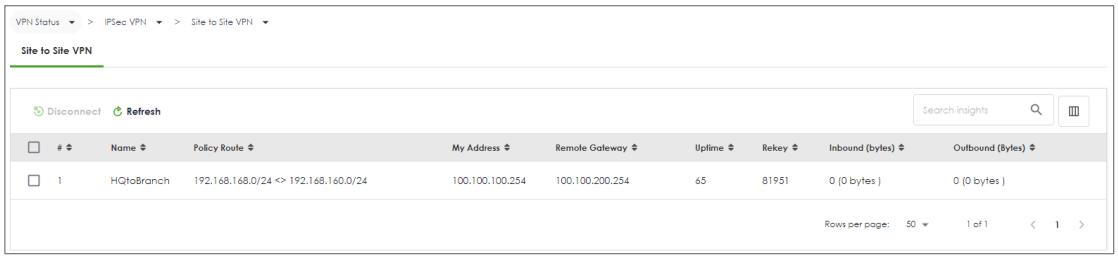


# Test IPSec VPN Tunnel

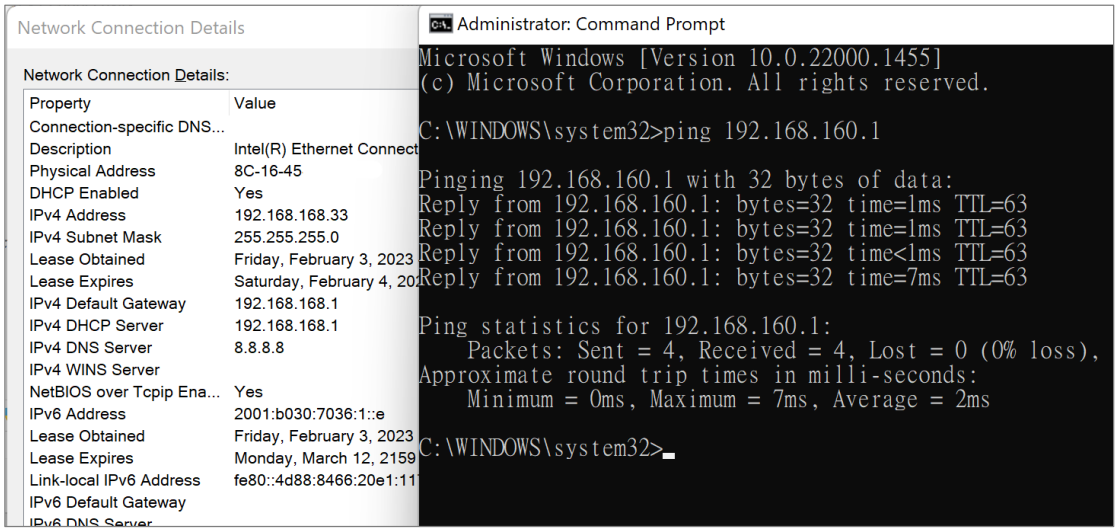
### VPN Status > IPSec VPN

Verify the IPSec VPN status.




### Ping the PC in Branch Office

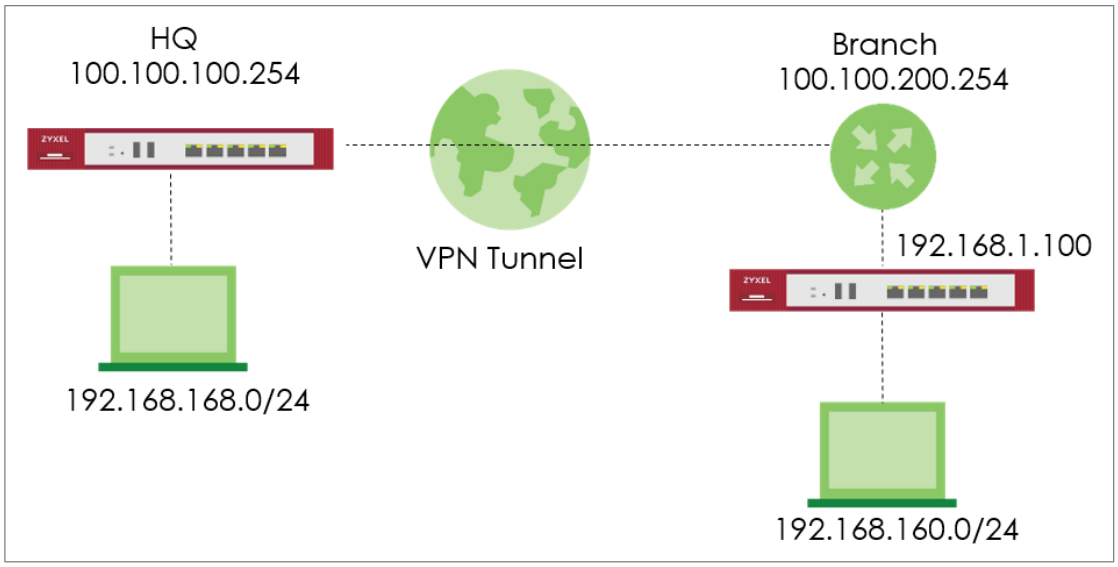
Win 11 > cmd > ping 192.168.160.1



# How to 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.



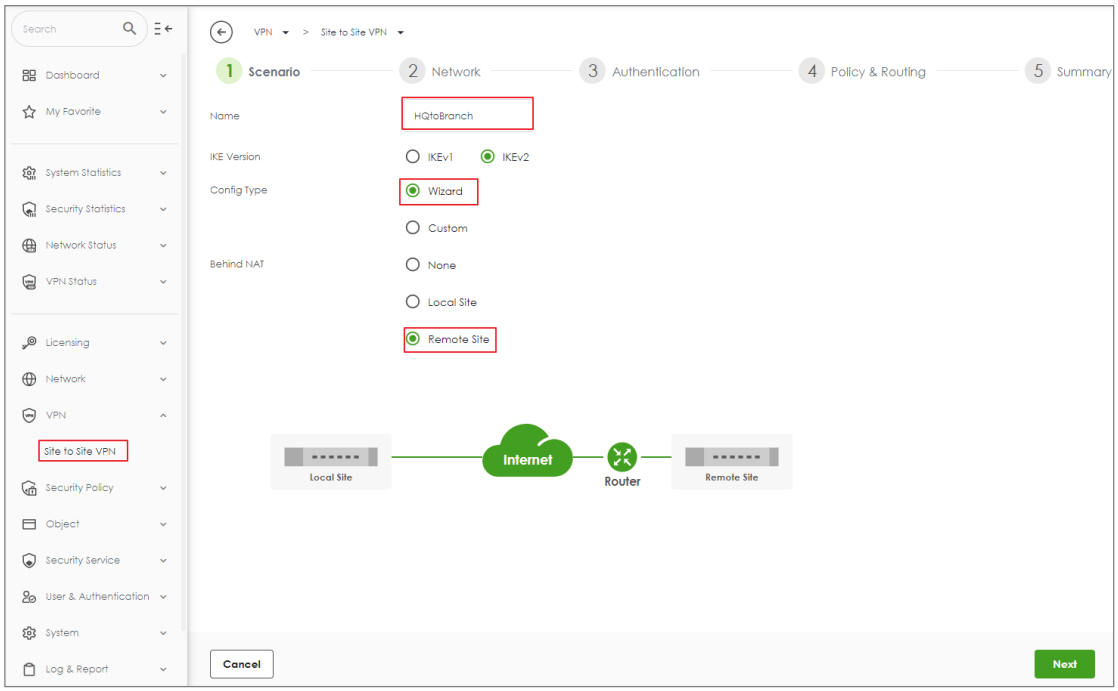

Note: Please ensure that you have NAT mapping UDP port 4500 to USG FLEX H device.

# Set up IPSec VPN Tunnel for HQ

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

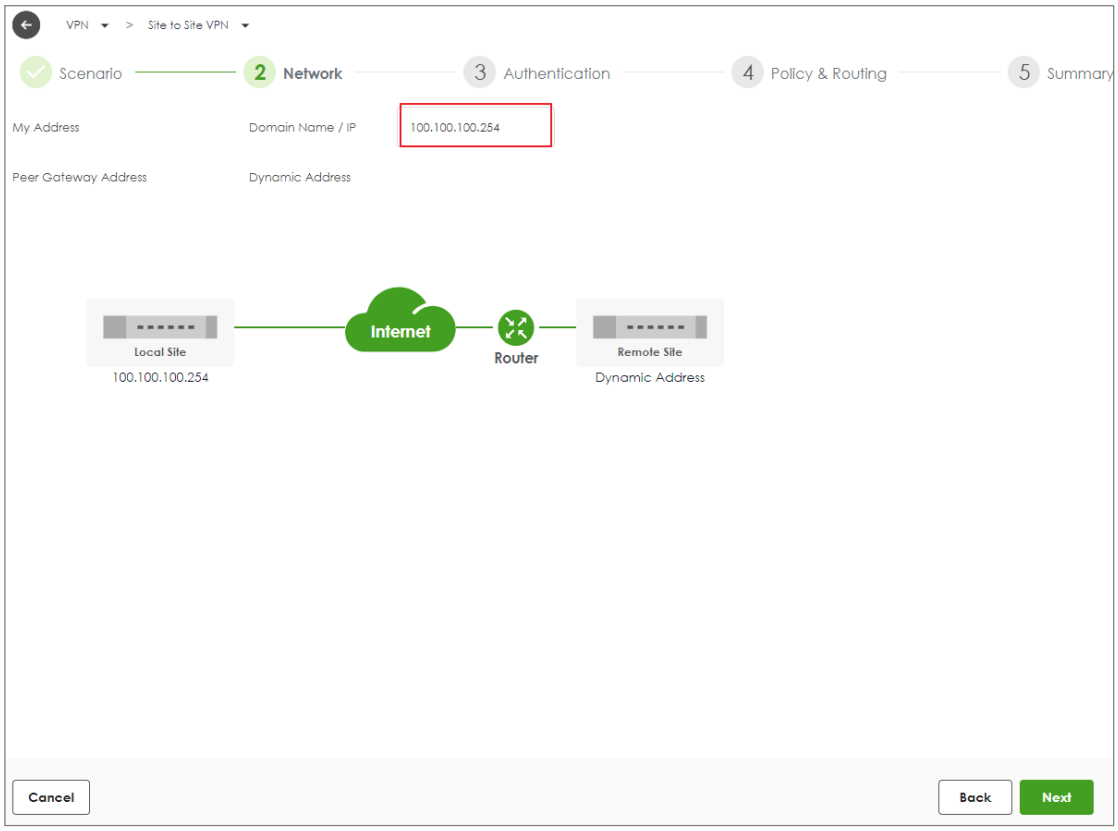
Type the VPN name used to identify this VPN connection. Select the Behind NAT to the Remote Site. Click **Next**.



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

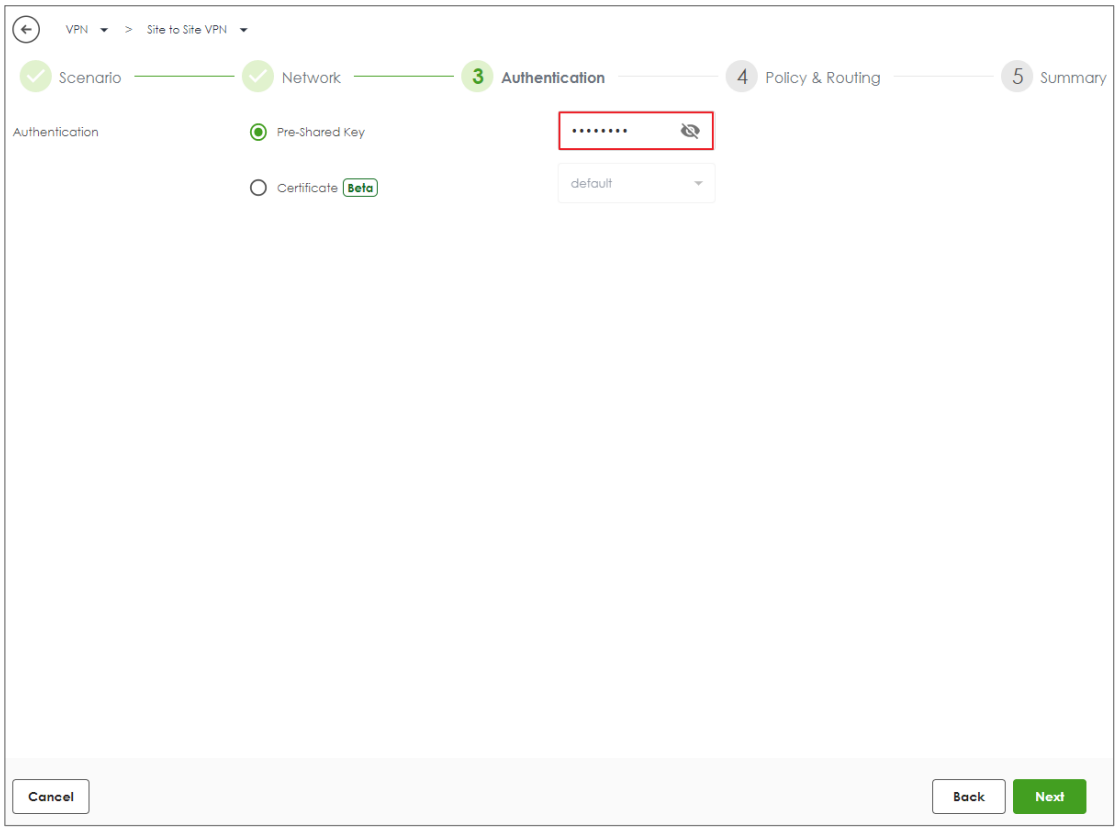
Configure My Address. Click **Next.**



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

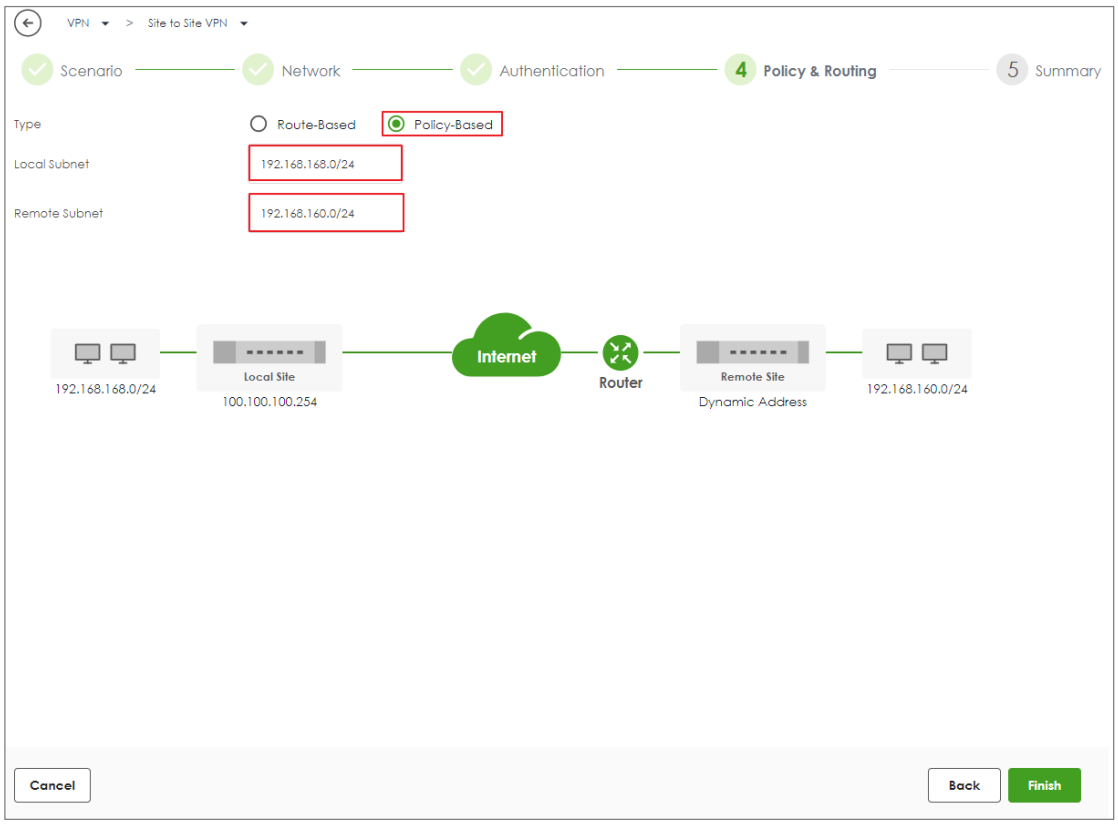
Type a secure Pre-Shared Key. Click **Next**



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

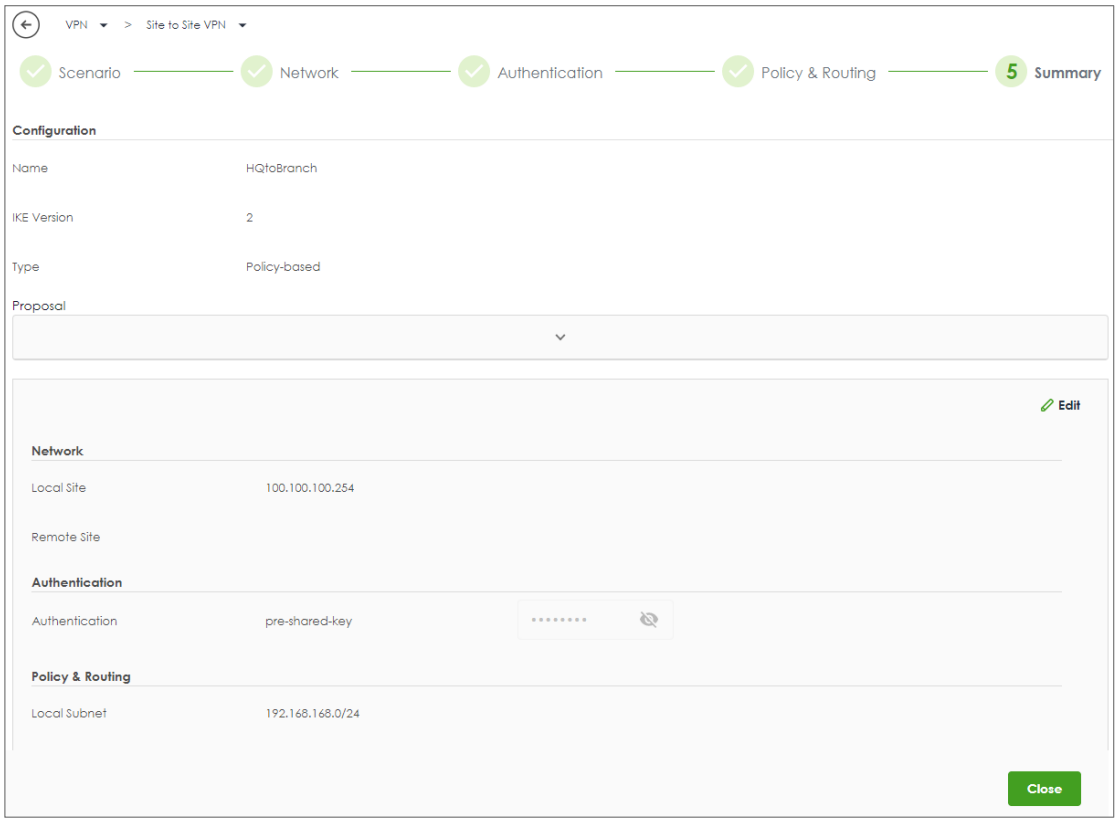
Set Local Subnet to be the IP address of the network connected to the gateway and Remote Subnet to be the IP address of the network connected to the peer gateway.



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

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

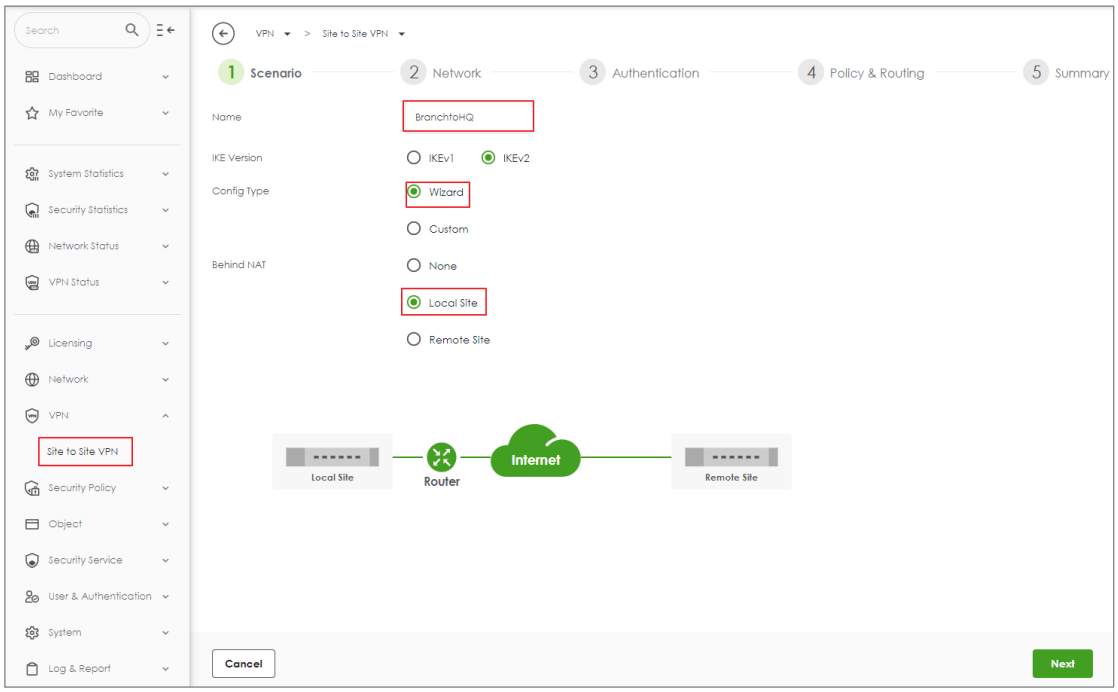


# Set up IPSec VPN Tunnel for Branch

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

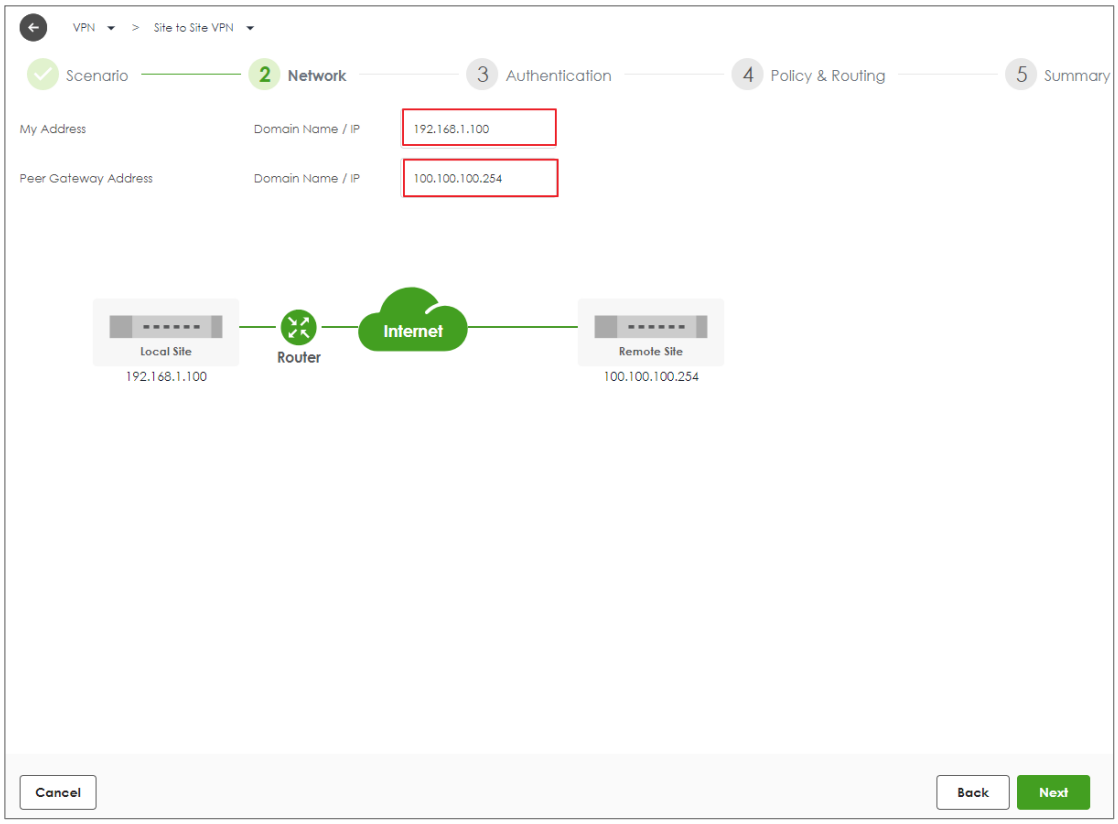
Type the VPN name used to identify this VPN connection. Select the Behind NAT to the Local Site. Click **Next.**



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

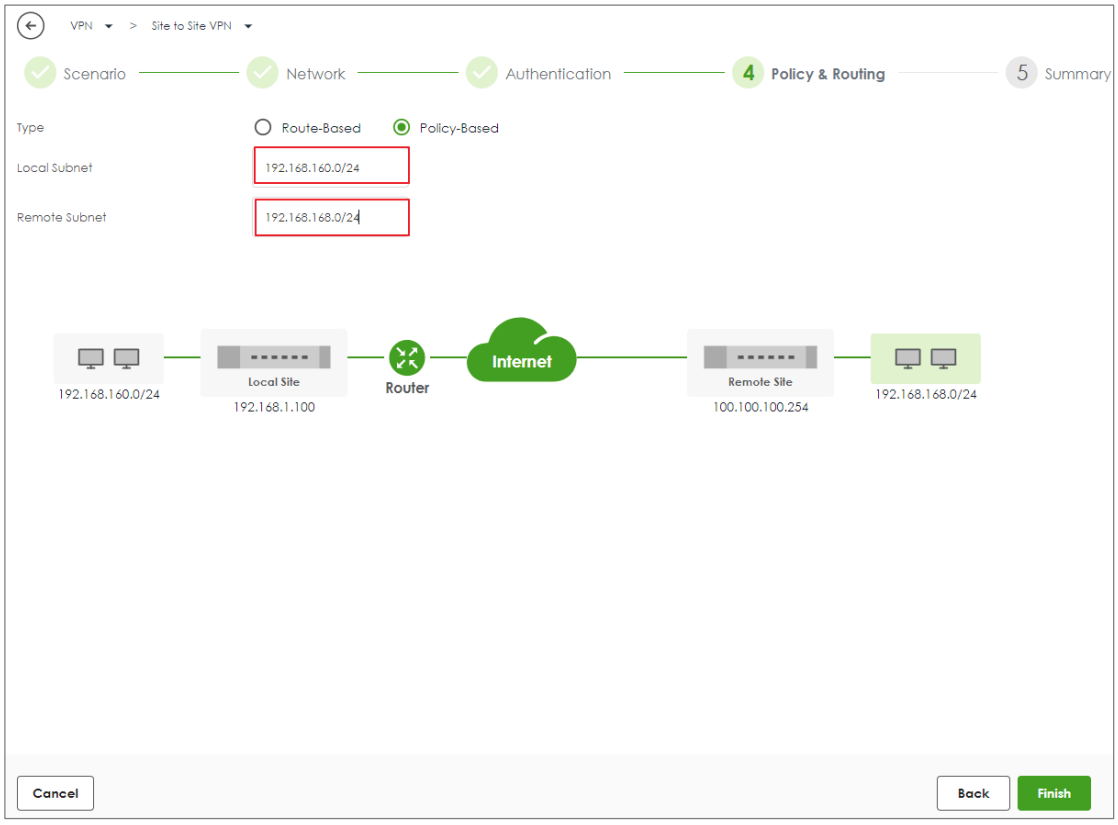
Configure My Address and Peer Gateway Address. Click **Next.**



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

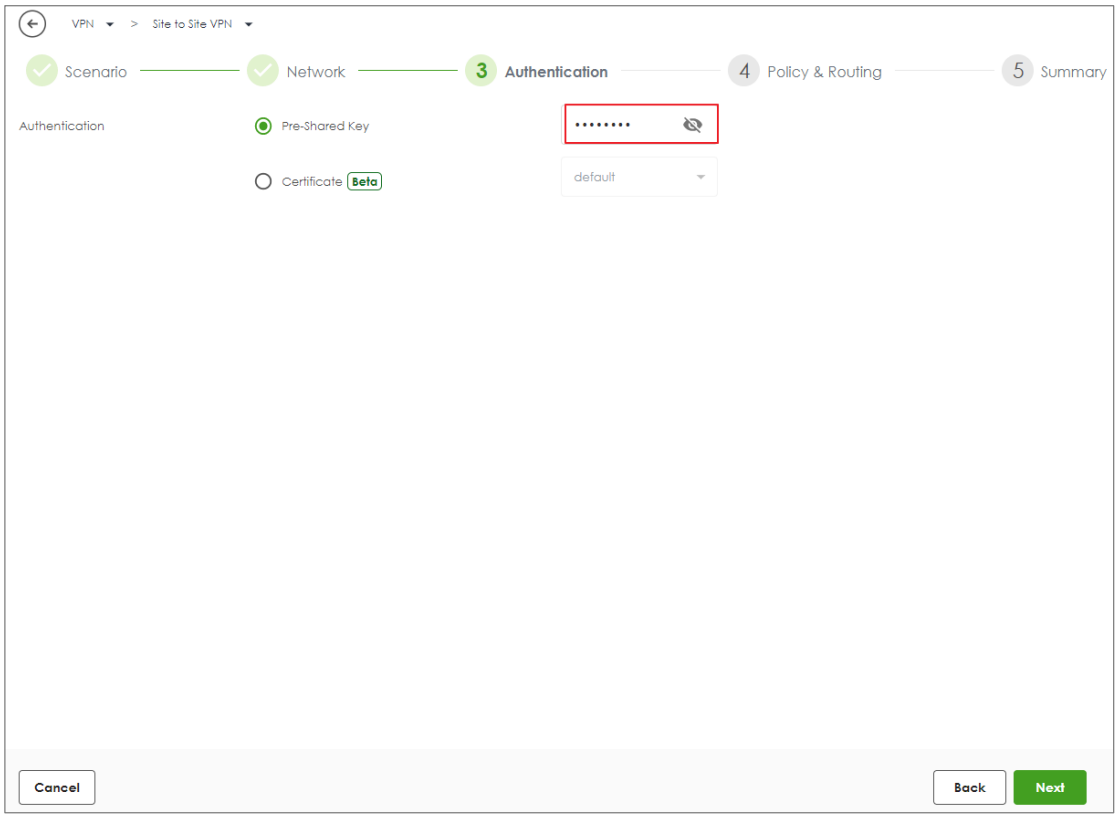
Set Local Subnet to be the IP address of the network connected to the gateway and Remote Subnet to be the IP address of the network connected to the peer gateway.



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

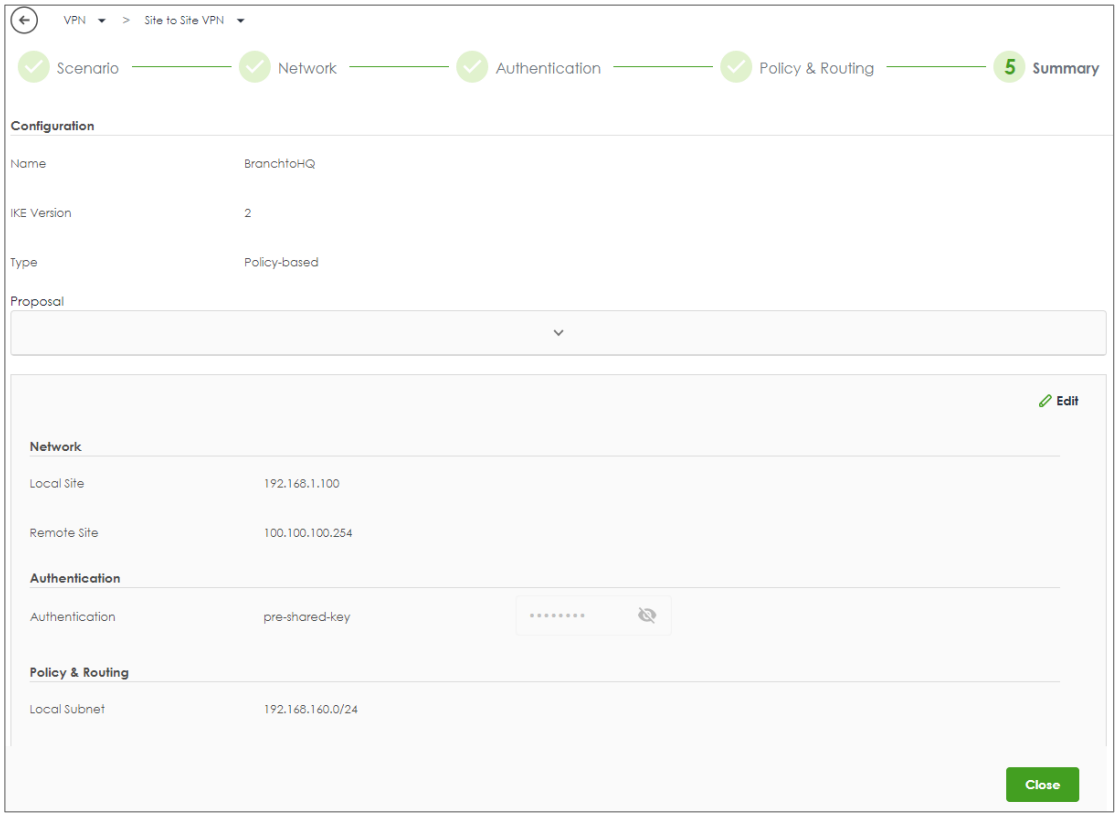
Type a secure Pre-Shared Key. Click **Next**



**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.

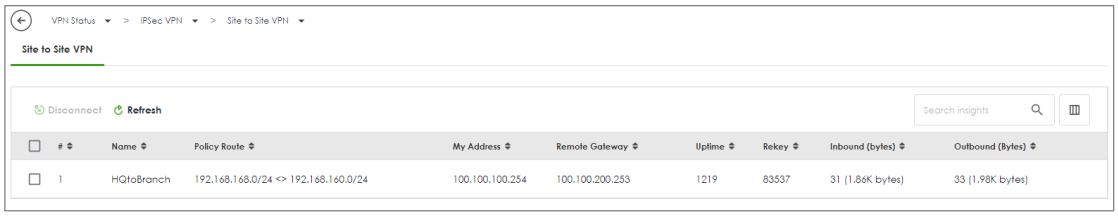


# Test IPSec VPN Tunnel

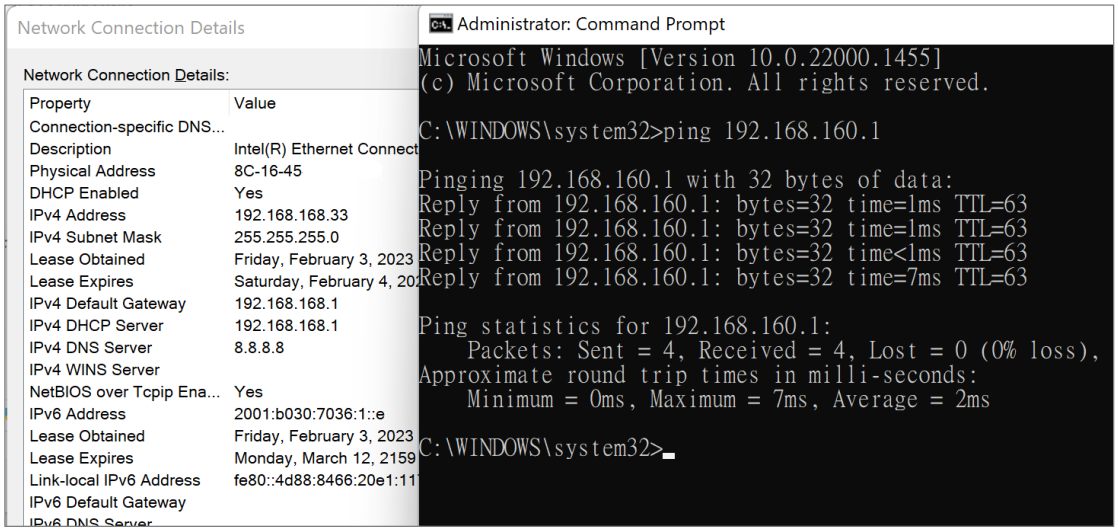
### VPN Status > IPSec VPN

Verify the IPSec VPN status.




### Ping the PC in Branch Office

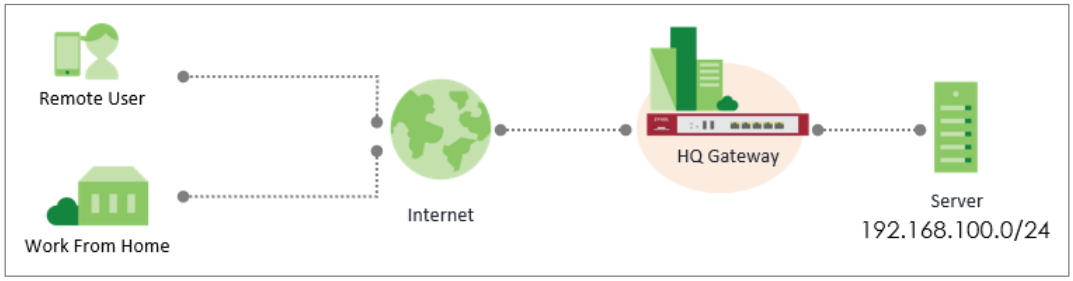
Win 11 > cmd > ping 192.168.160.1



# How to 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.

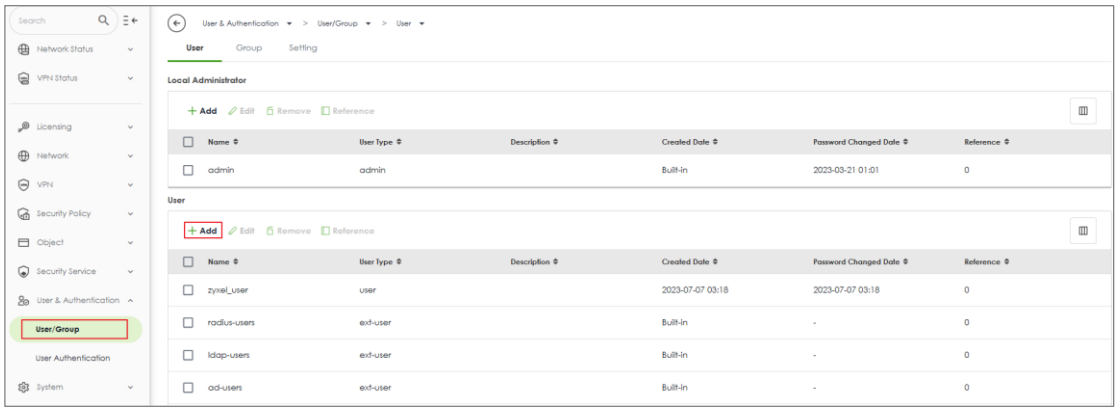


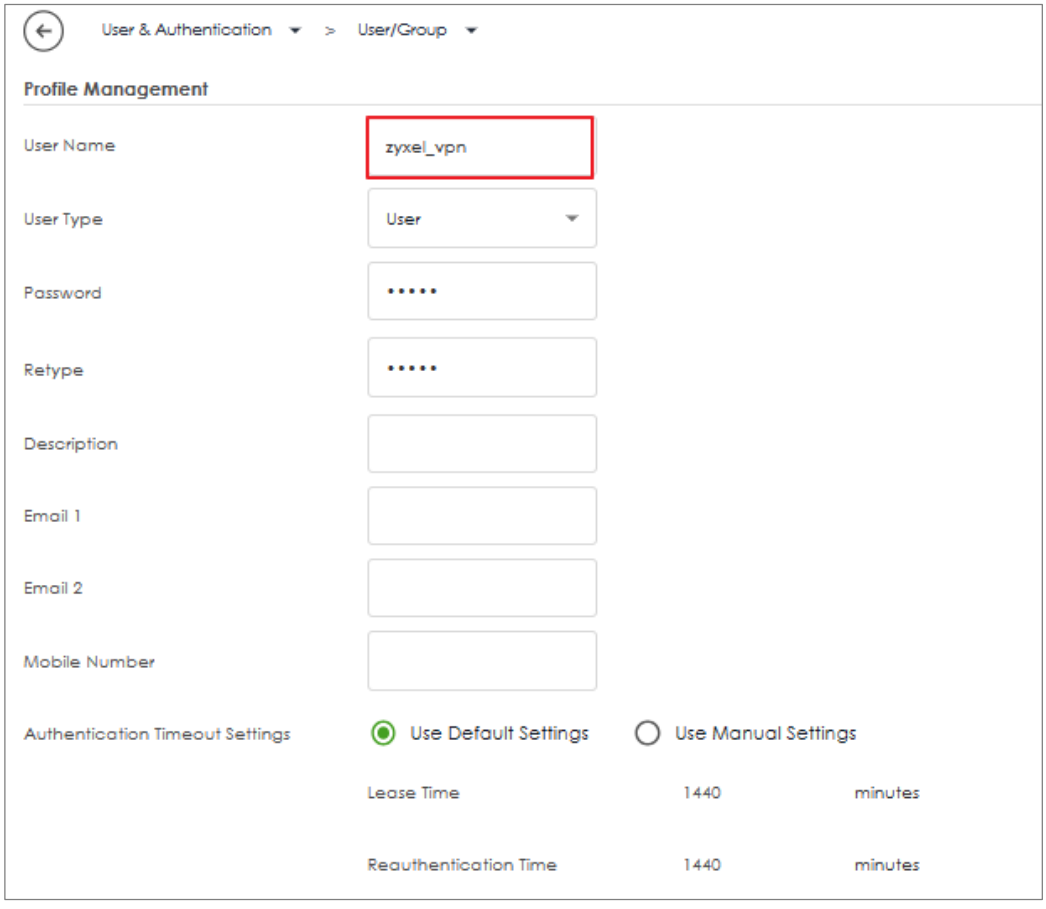

 

## Before Begin

**User & Authentication > User/Group > User**

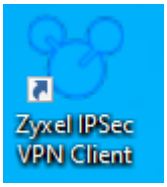
Create local user for remote access authentication.



**Download and install the new TGB Client**

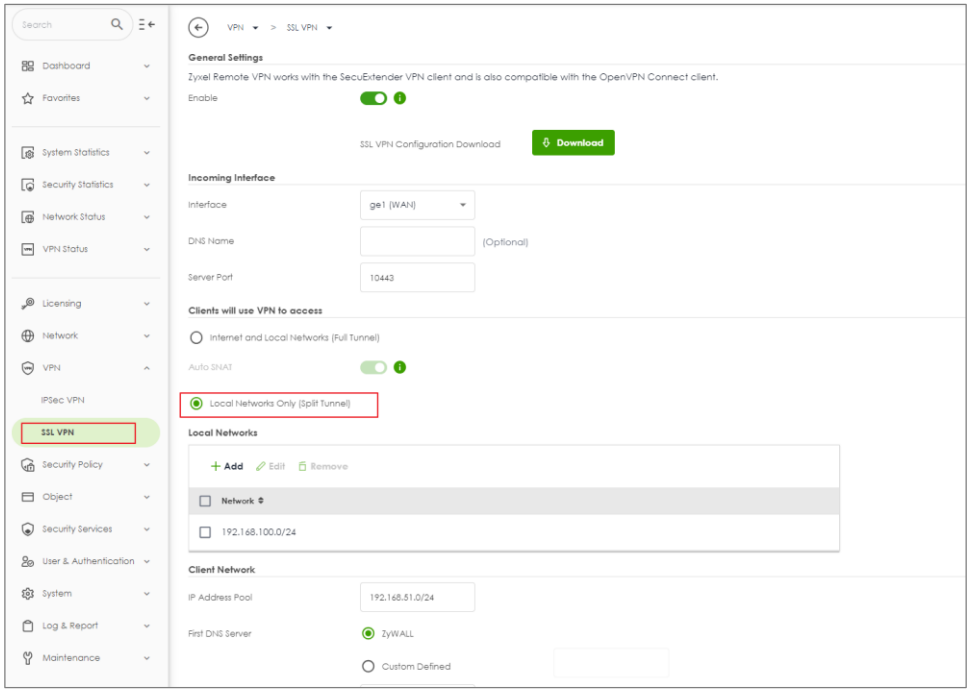



## Set up SSL VPN

**VPN > SSL VPN**

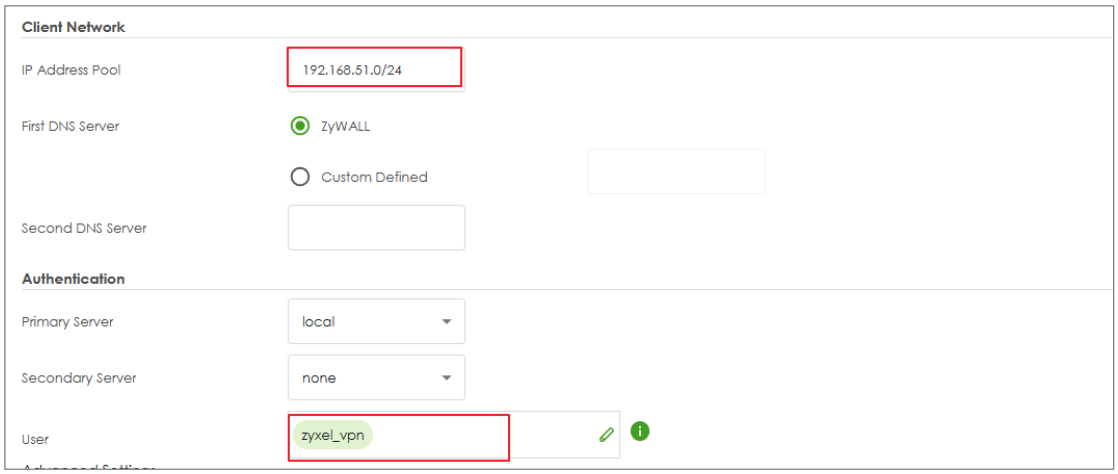
Select the incoming interface, the default port is 10443. And up to your requirement to select Full Tunnel or Split Tunnel. And we now support OpenVPN config file.

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.

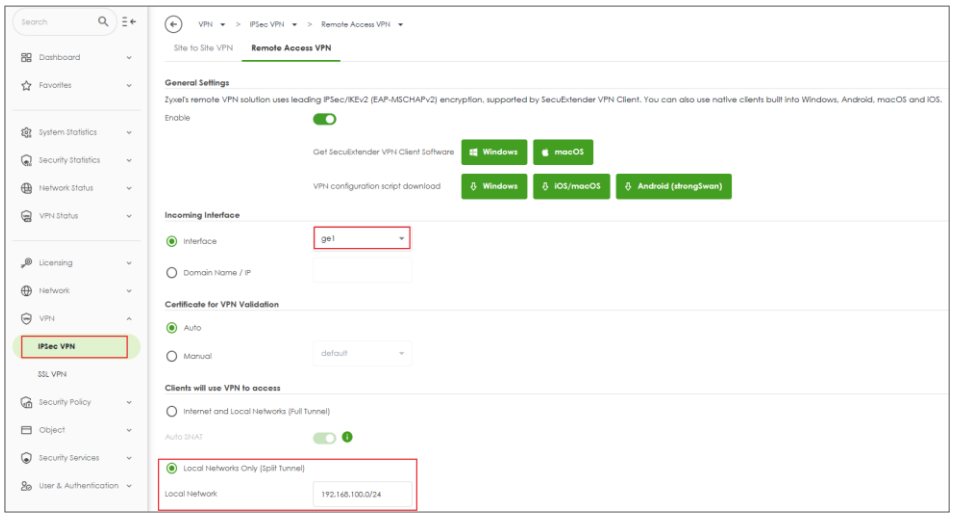



## Set up IKEv2 VPN

### VPN > IPSec VPN > Remote Access VPN

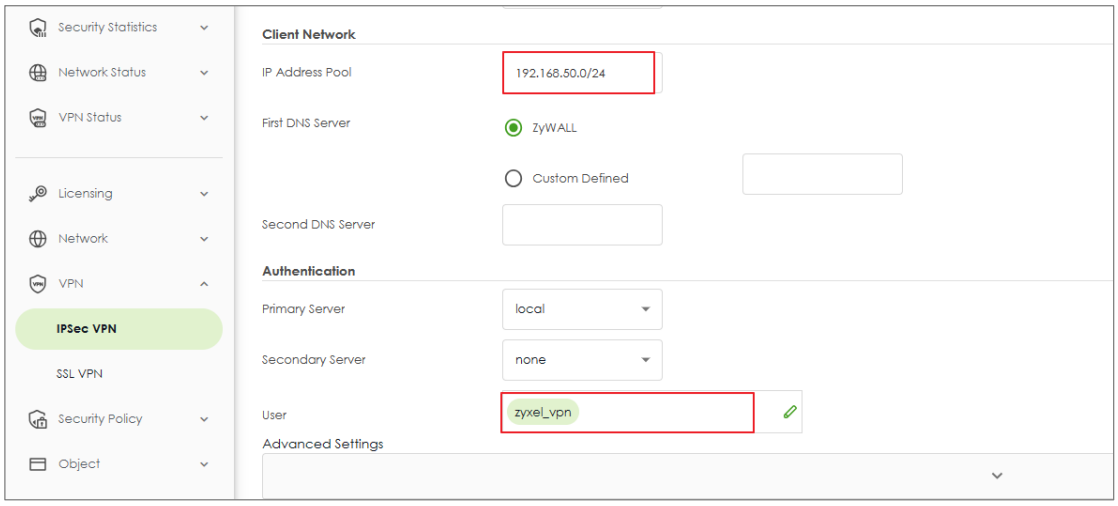
Select the incoming interface. And up to your requirement to select Full Tunnel or Split Tunnel.

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



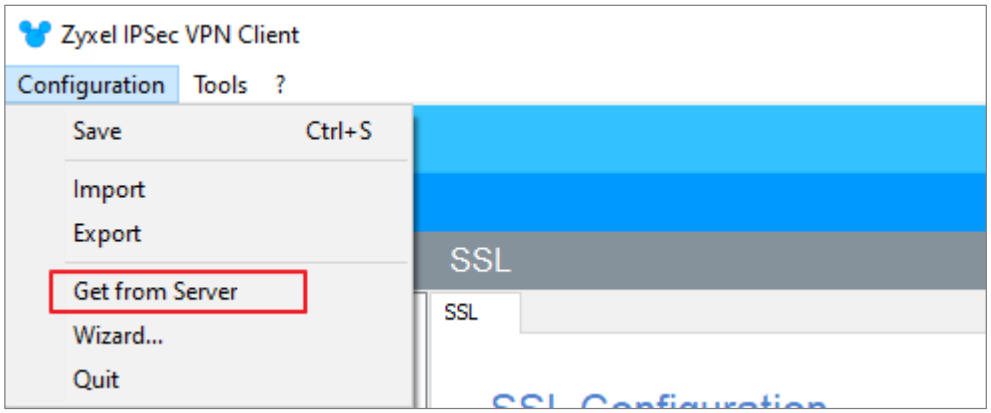

 

The default Address Pool is 192.168.50.0/24 and select the User who can access IKEv2 VPN.



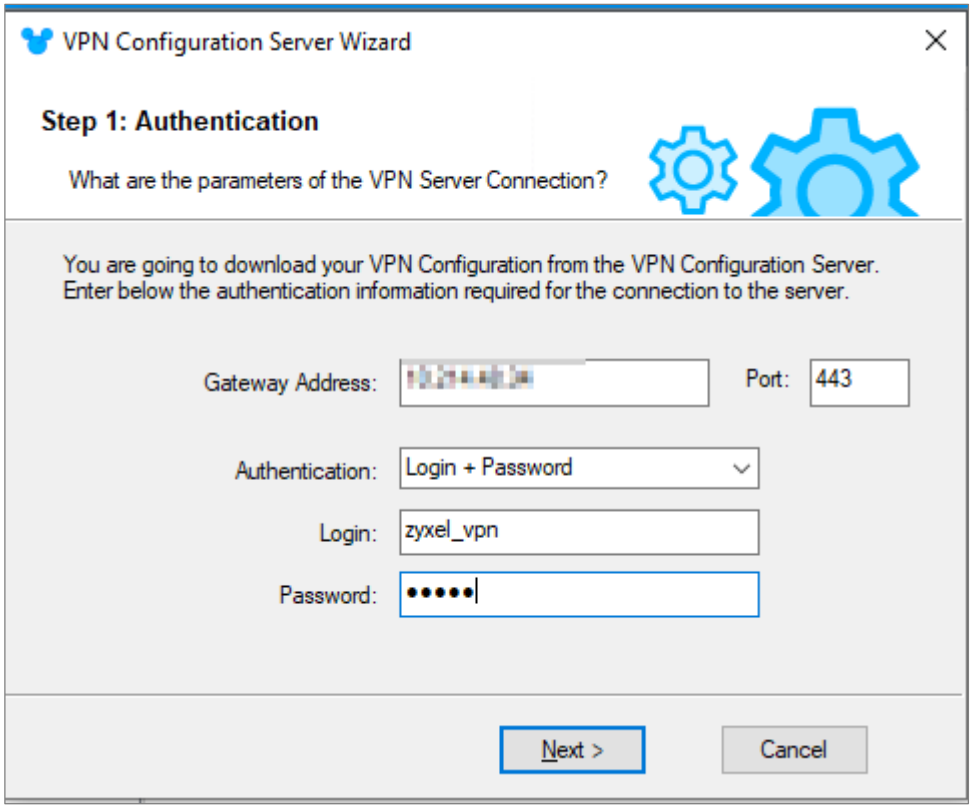

## Set up Remote Access on TGB Client

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



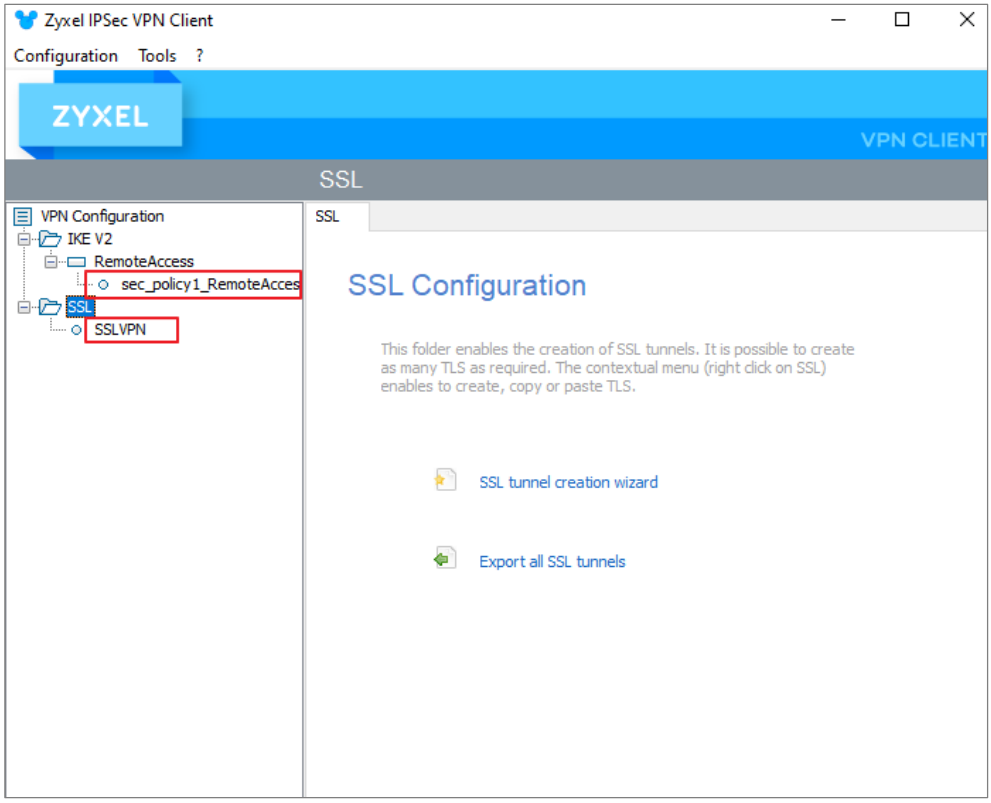

 

Input the Gateway Address, Username and password to fetch configuration file.



You will obtain IKEv2 as well as SSLVPN settings.

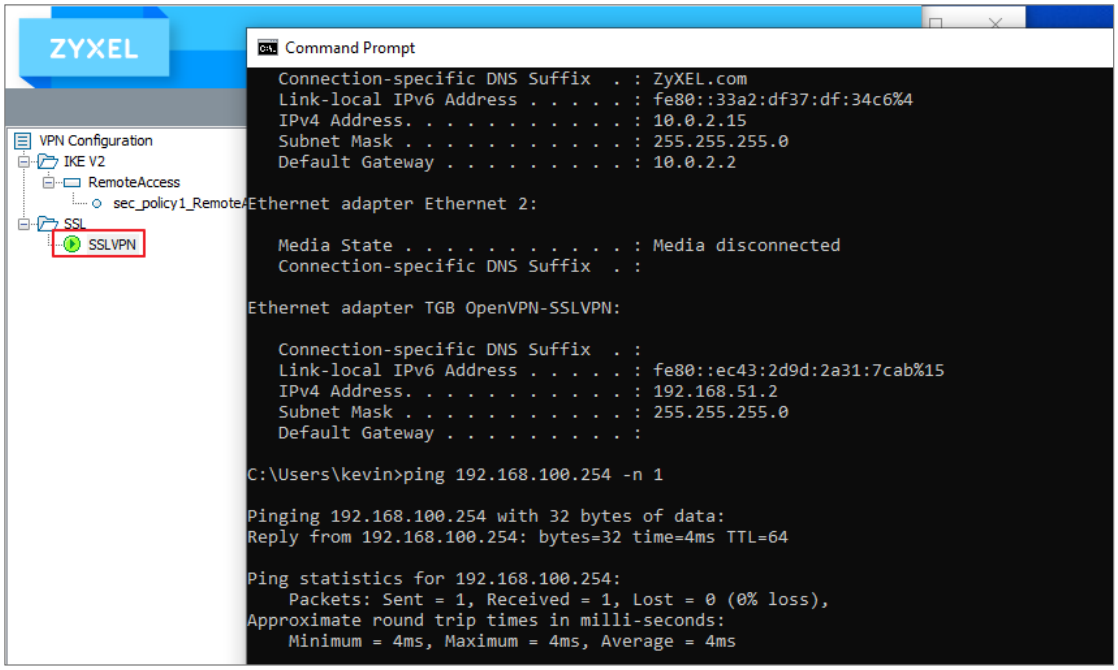


## Test SSLVPN Tunnel on TGB Client

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

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

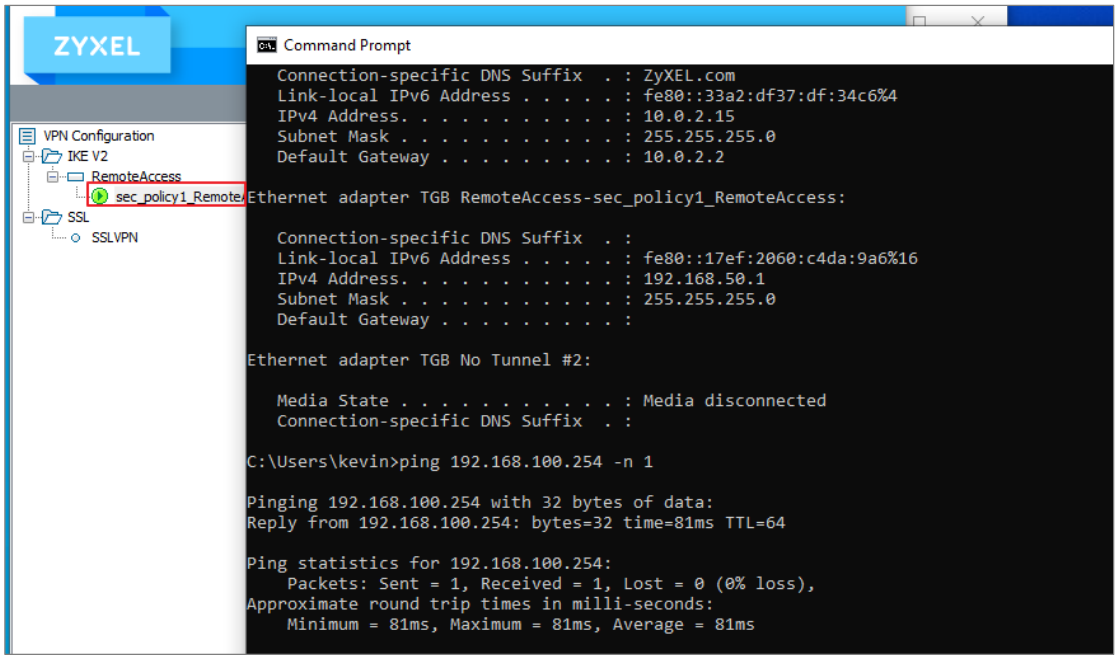


## Test IKEv2 Tunnel on TGB Client

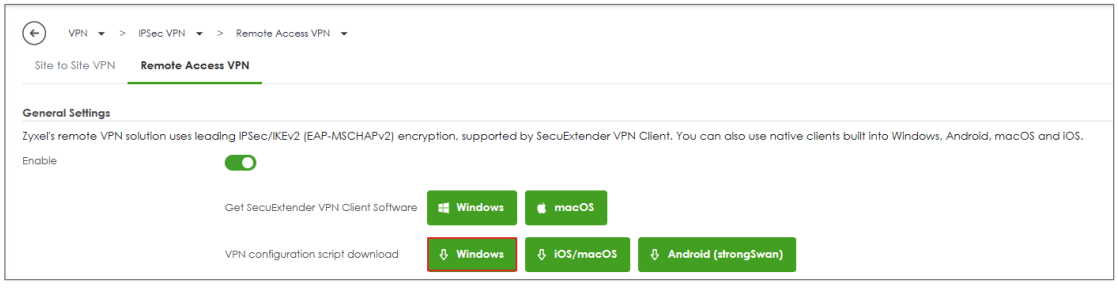
Right click the profile and "Open Tunnel" and log in.

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



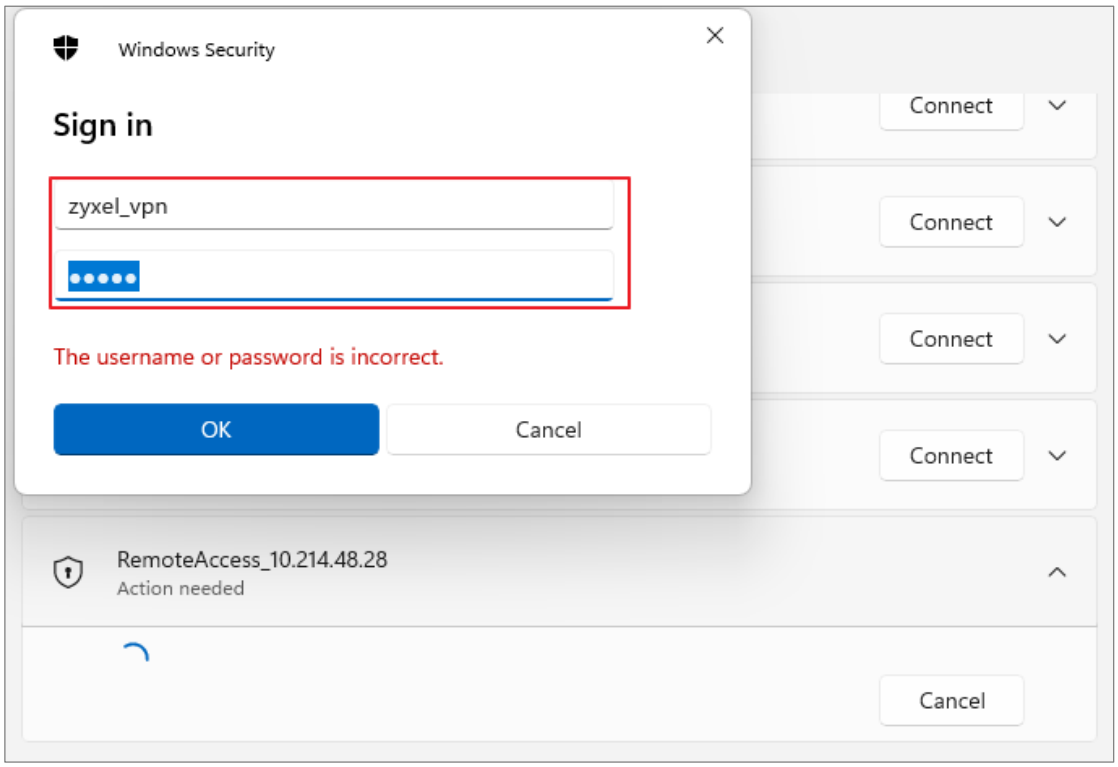

## Test IKEv2 Tunnel on Windows Client

Download Windows VPN configuration script



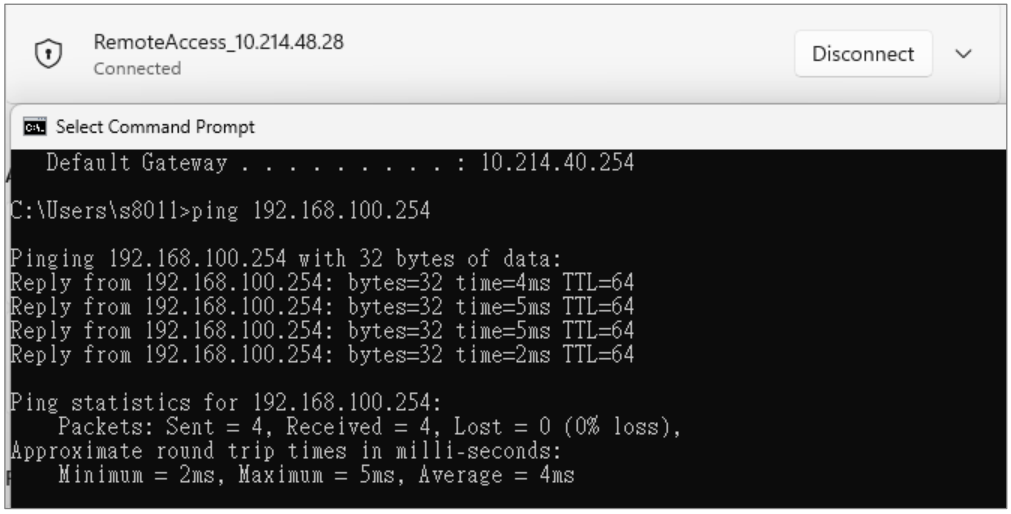

 

Perform the windows bat file and input credentials.



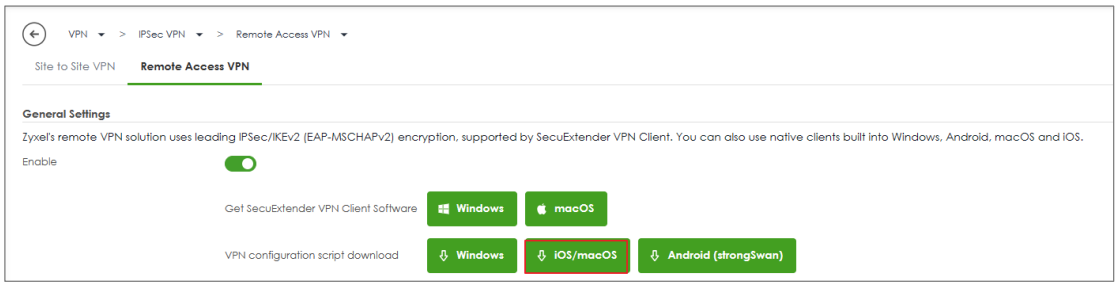

 

VPN is connected and can access internal resource.

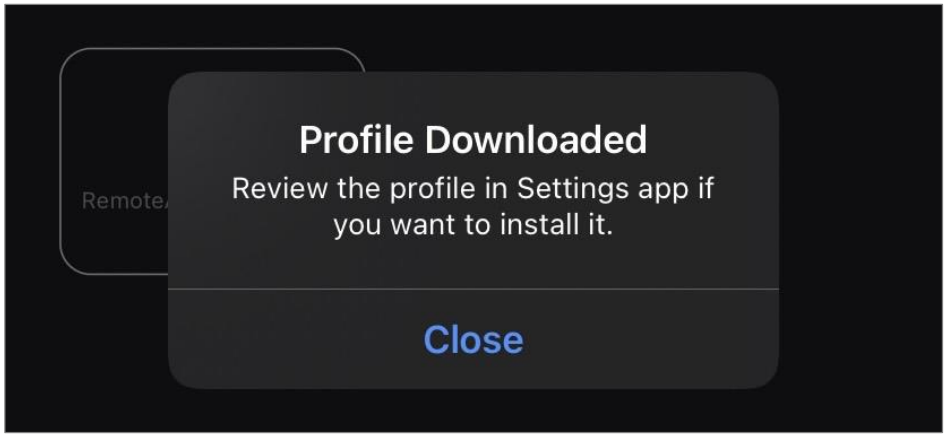



## Test IKEv2 Tunnel on iOS Client

Download iOS/macOS VPN configuration script.

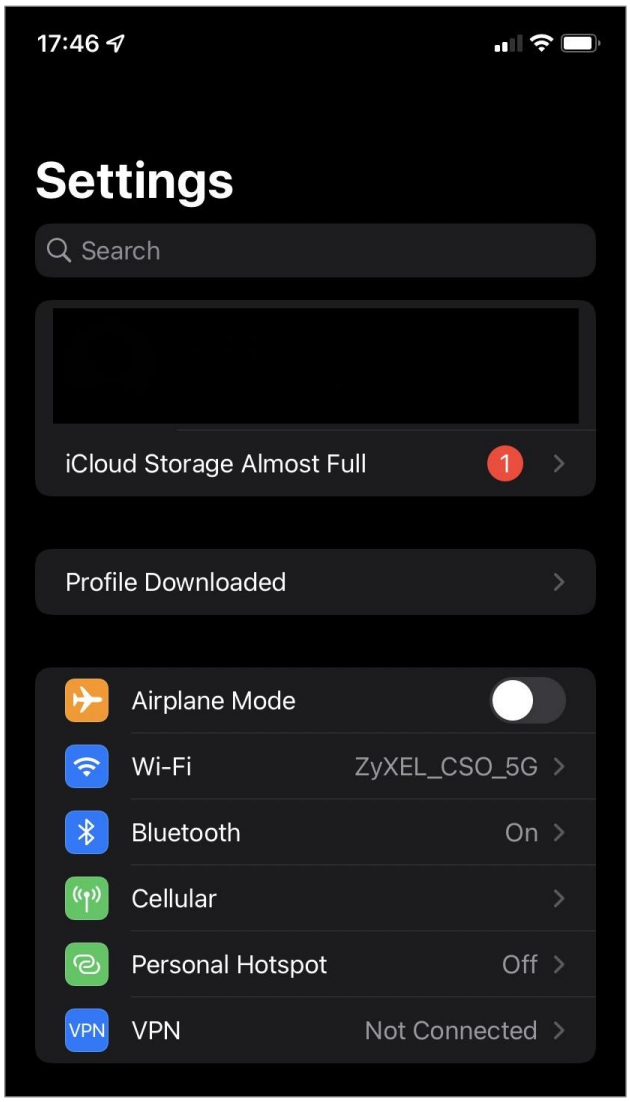



Send the script to Device.



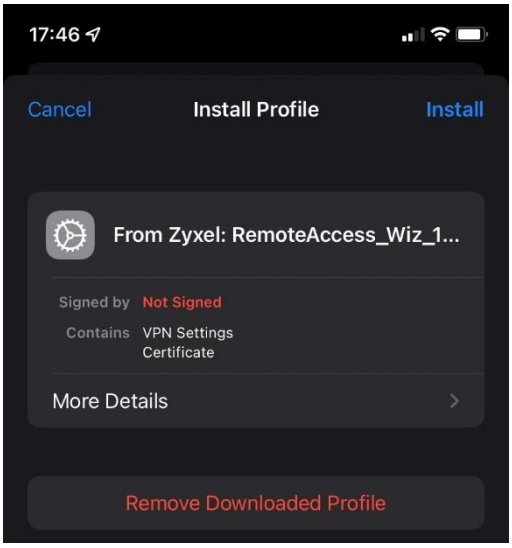

 

Settings > Profile Downloaded

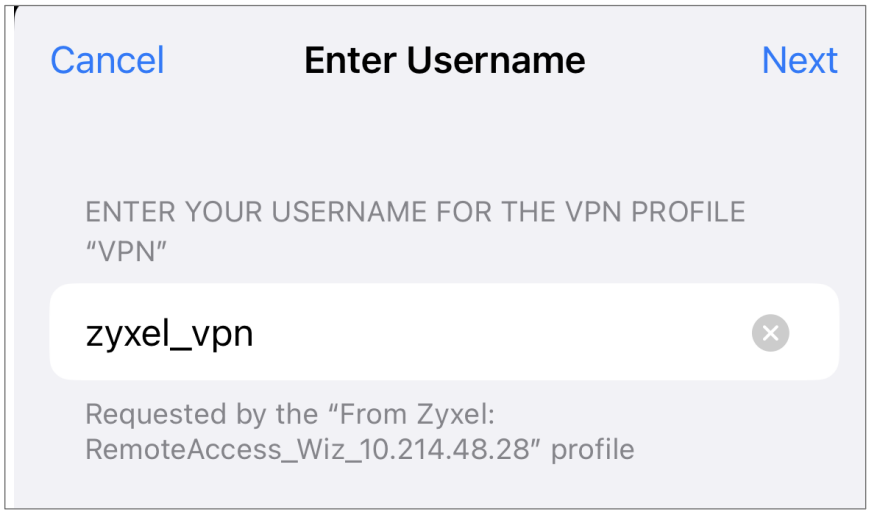


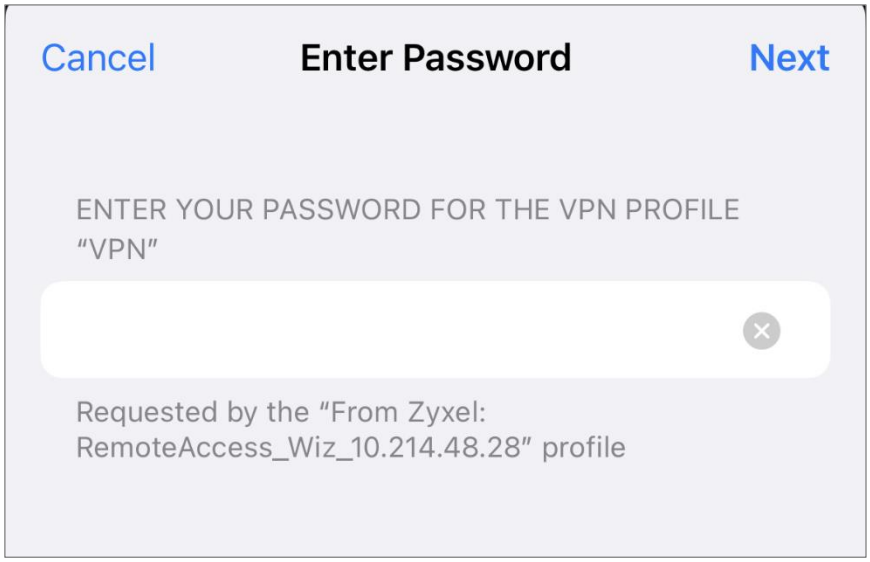
Press Install.



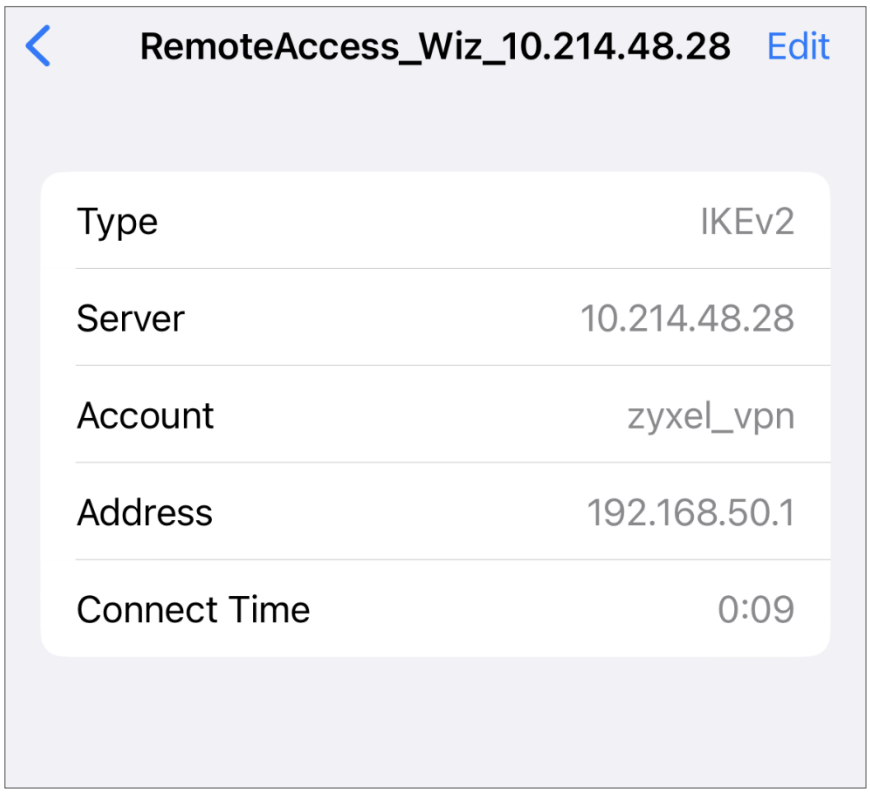

Enter Username and Password.





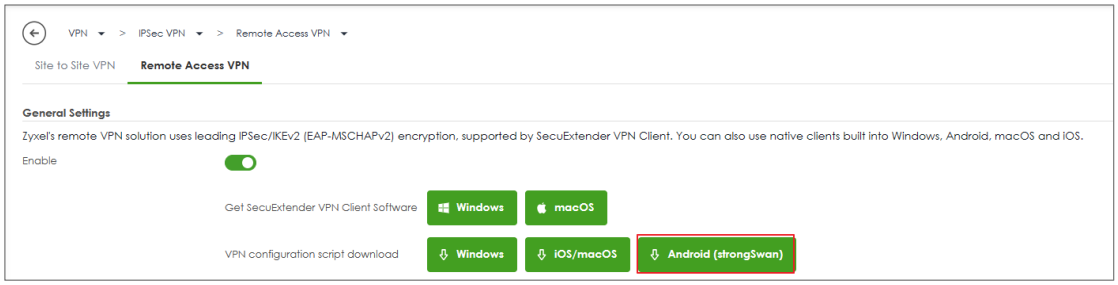

Now, it can connect.



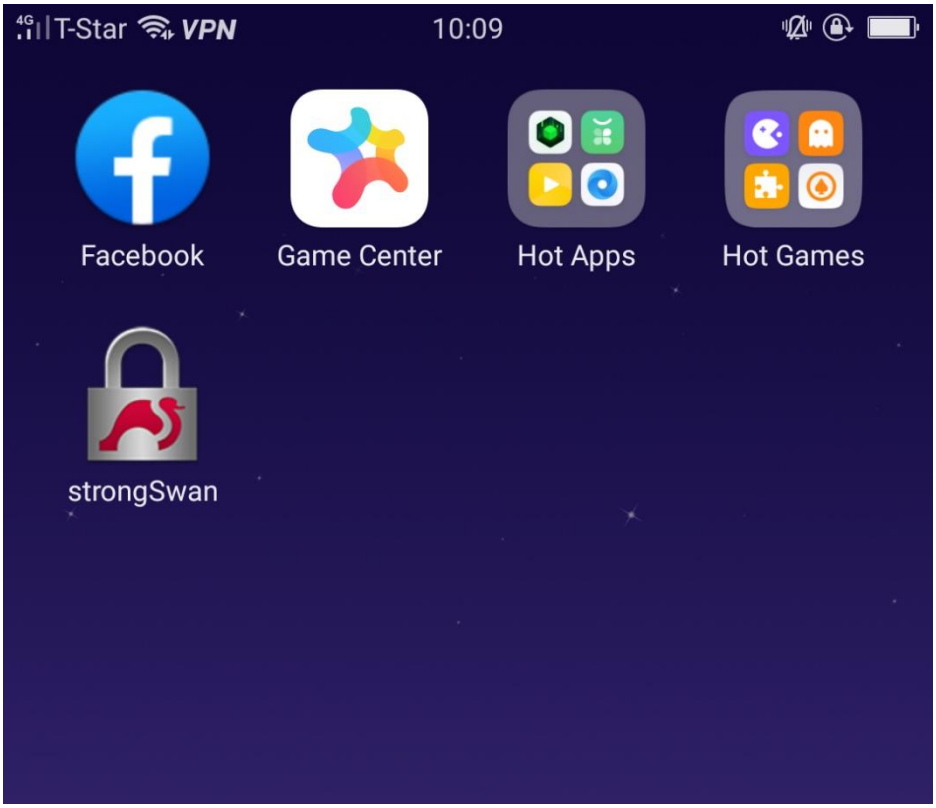

 

## Test IKEv2 Tunnel on Android Client

Download Android(strongSwan) VPN configuration script.

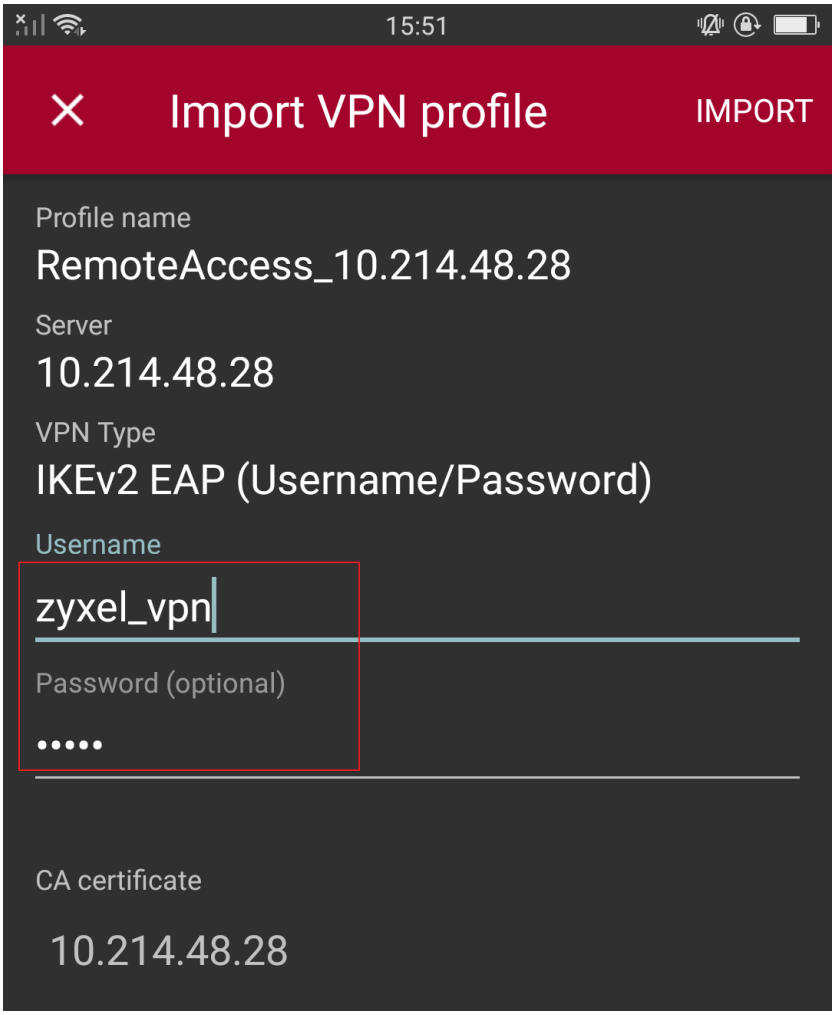



Download strongSwan from Google Play Store.



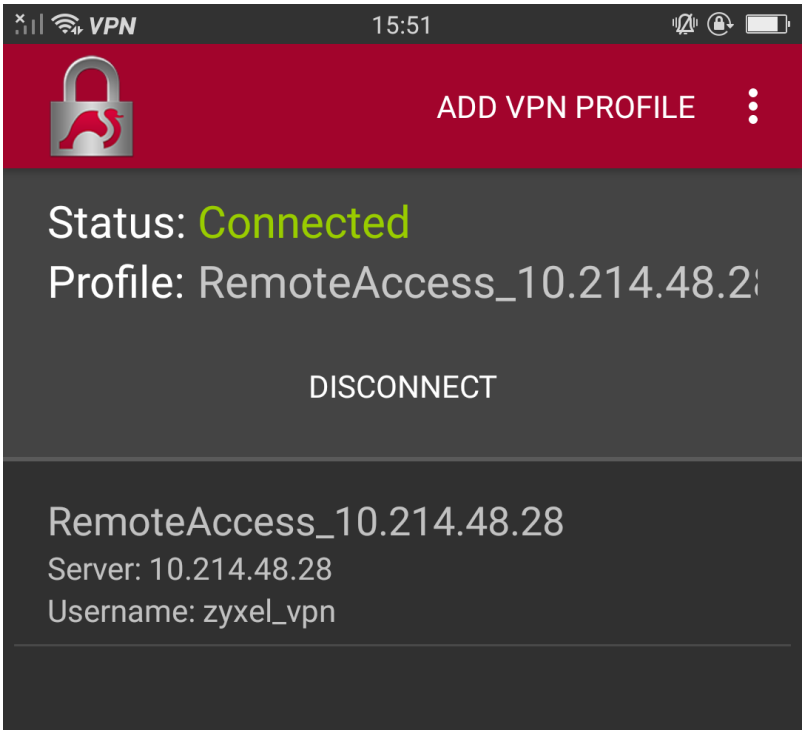

 

Send the script to device then Install and Import strongSwan profile.



VPN is connected.

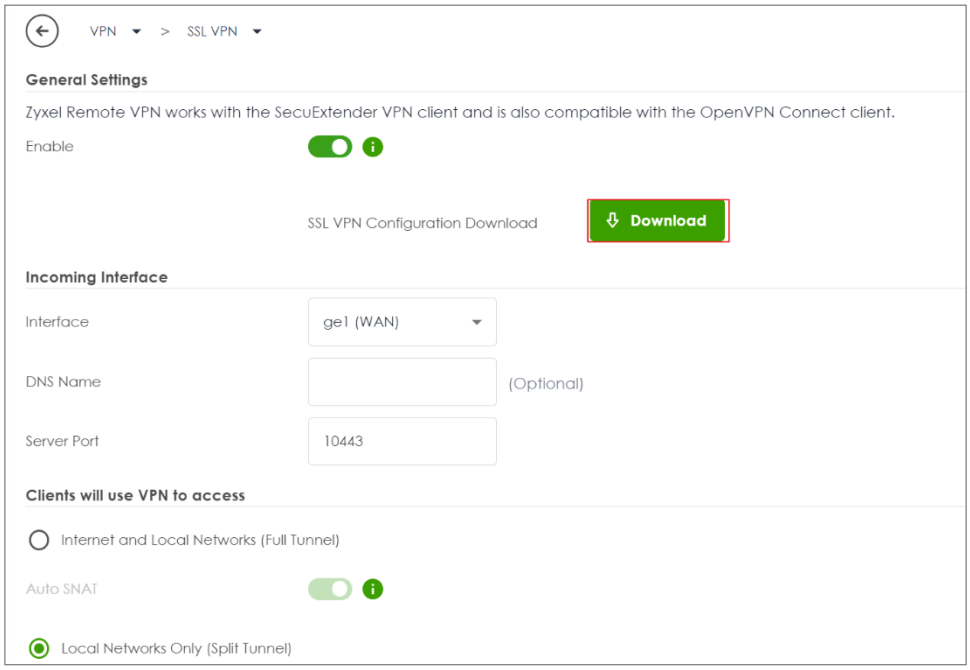


# Test OpenVPN

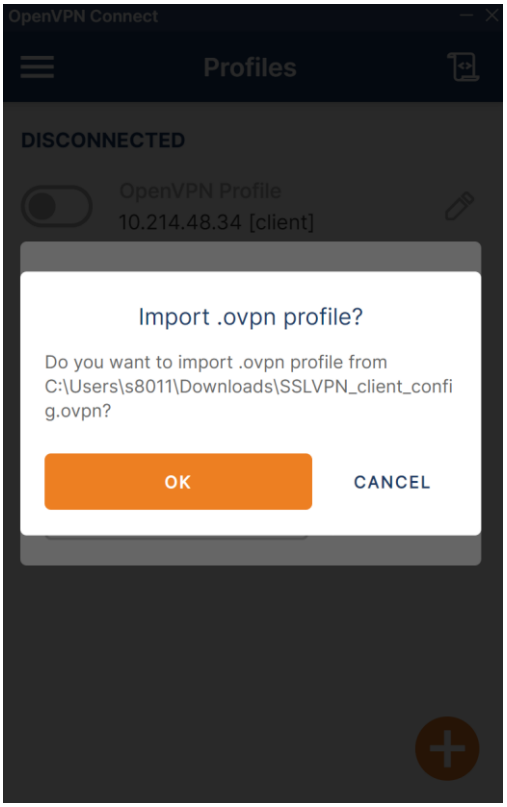
**VPN > SSL VPN**

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

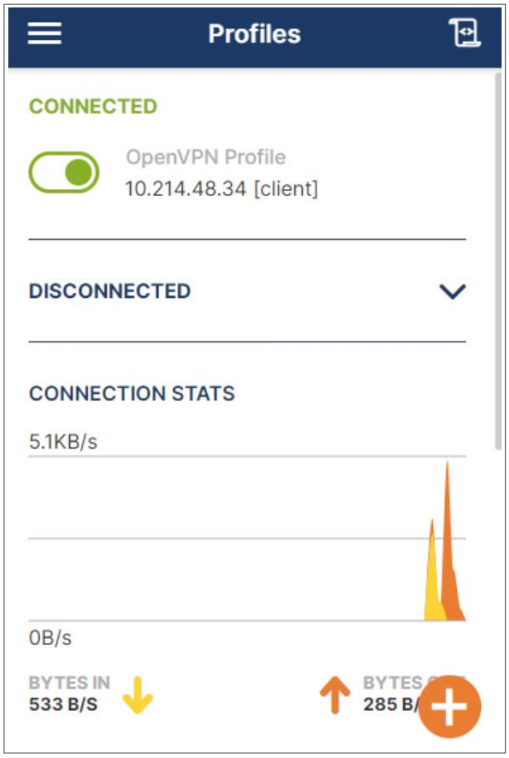


Import the config file.



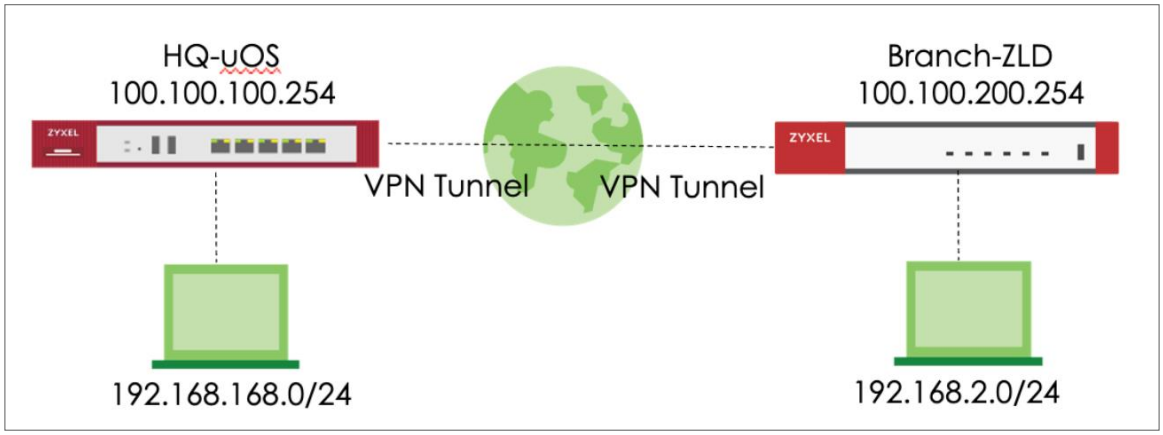

VPN is connected.



# 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.

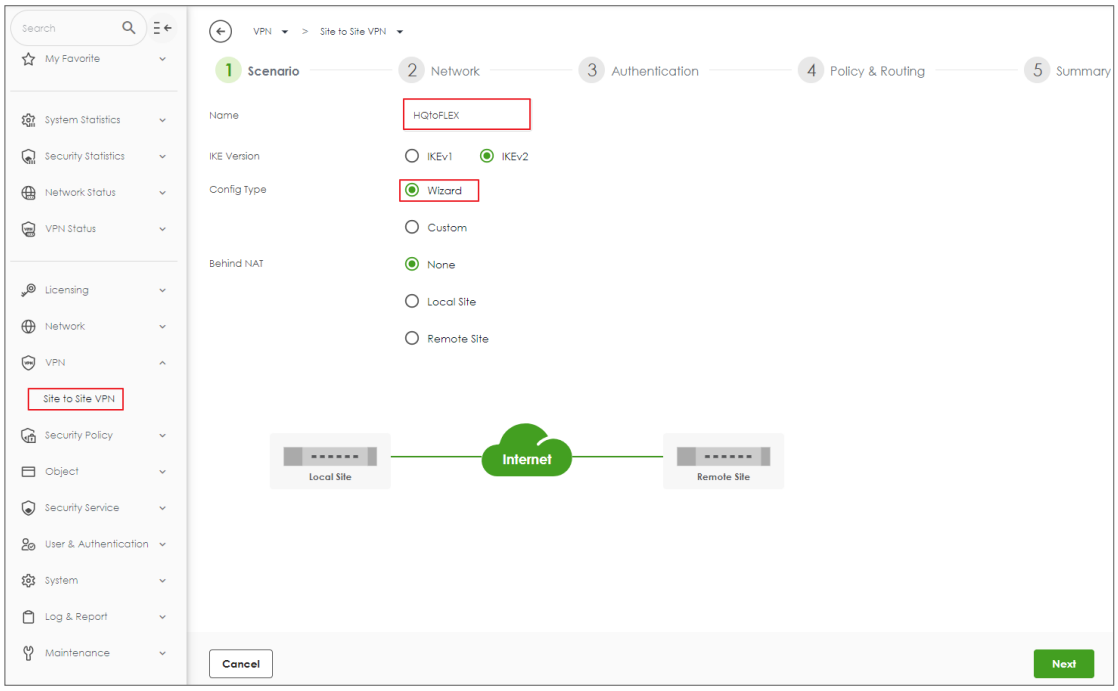


# Set up IPSec VPN Tunnel for uOS

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

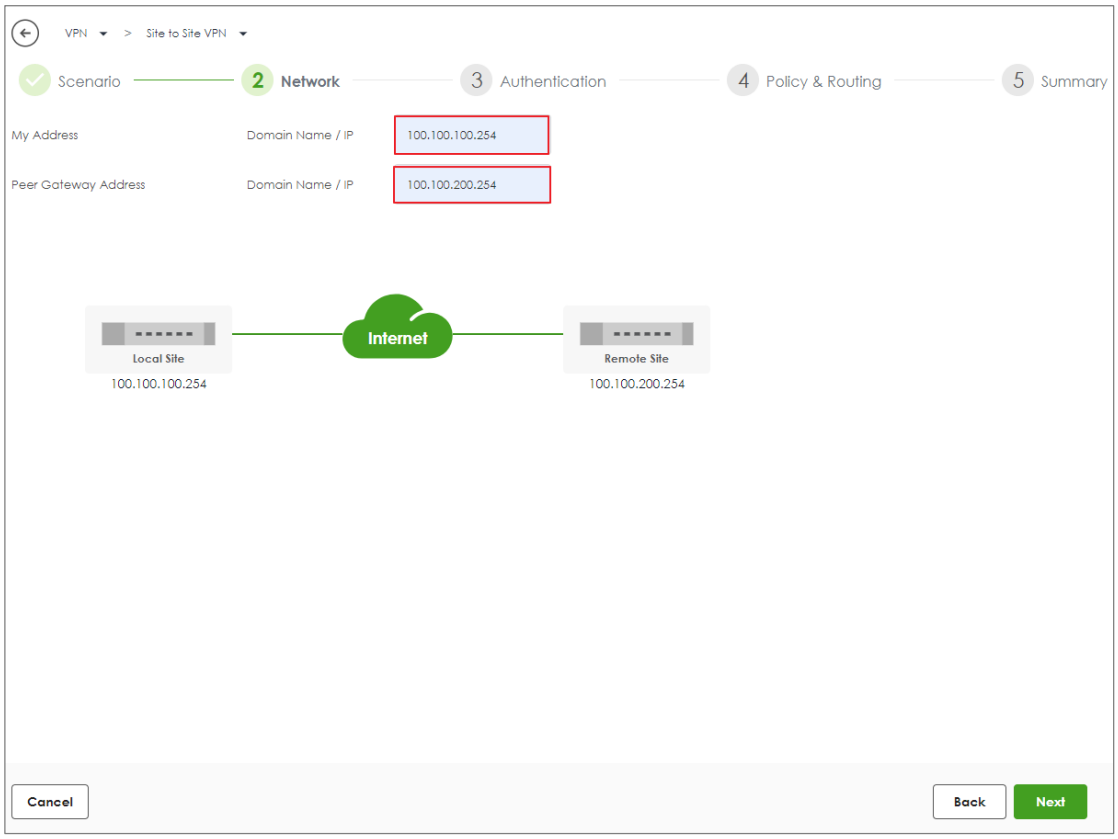
Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site. Click **Next**.



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

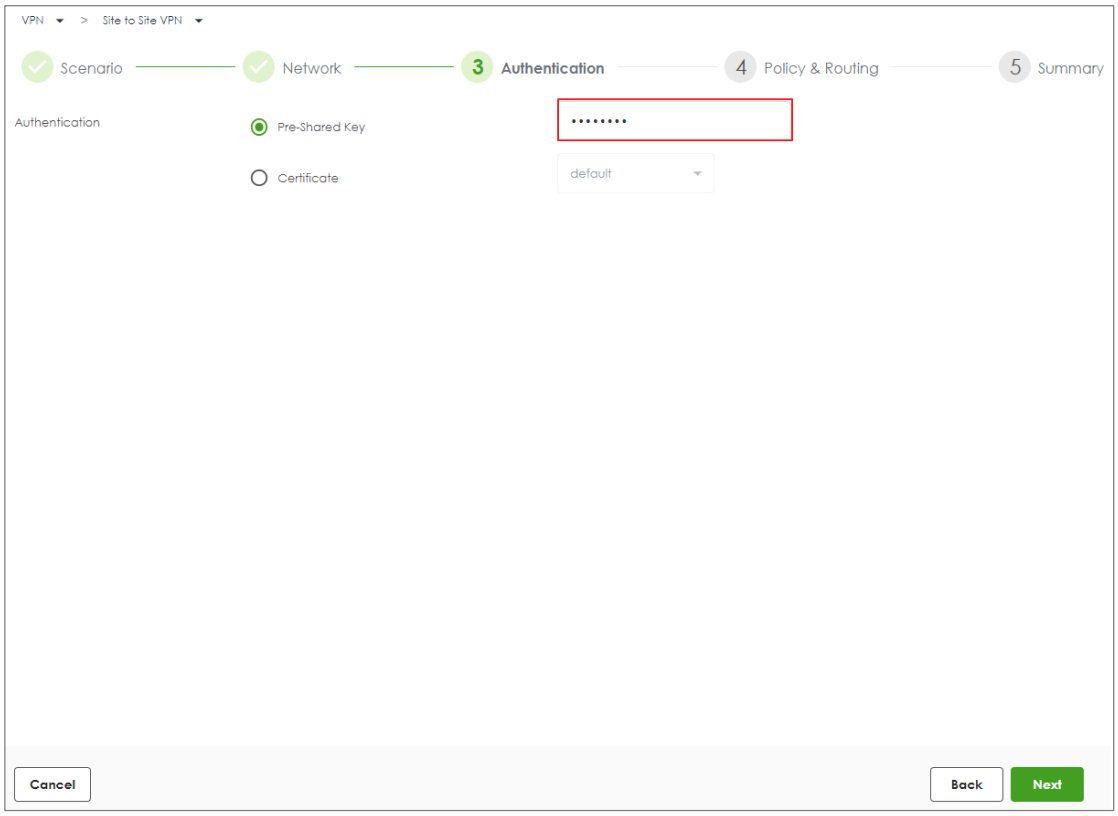
Configure My Address and Peer Gateway Address. Click **Next.**



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

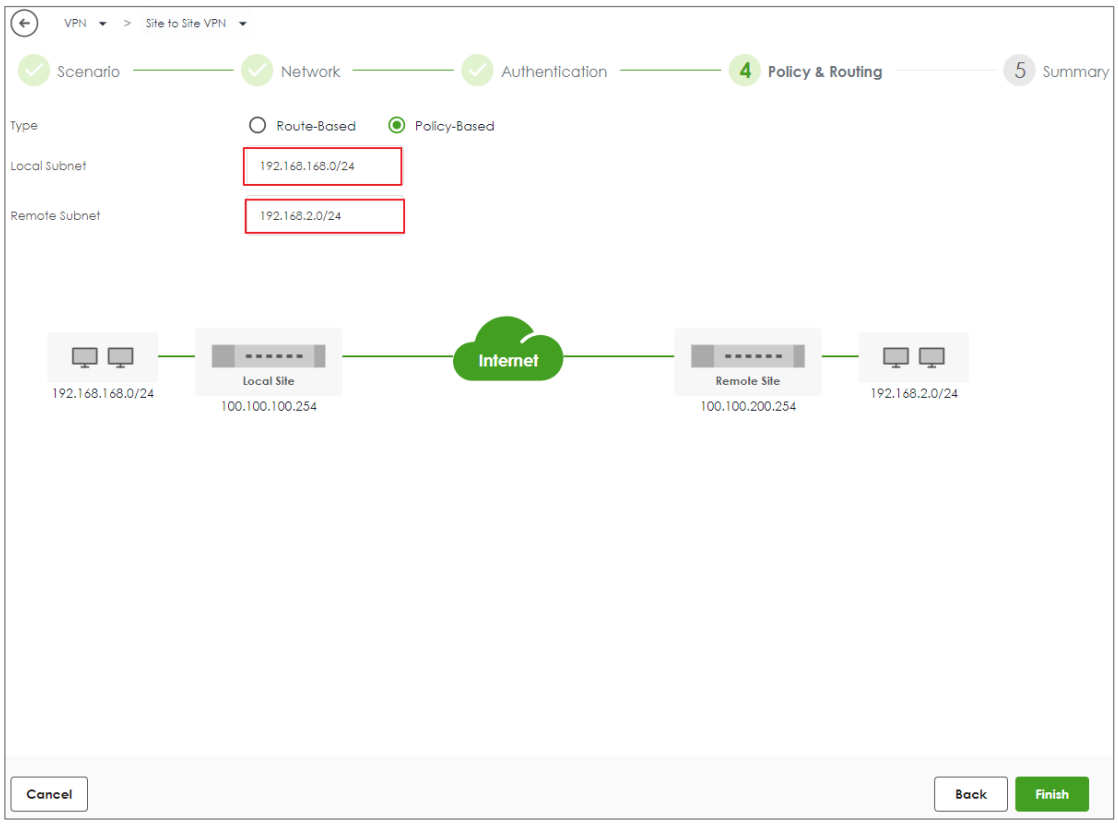
Type a secure Pre-Shared Key. Click **Next**



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

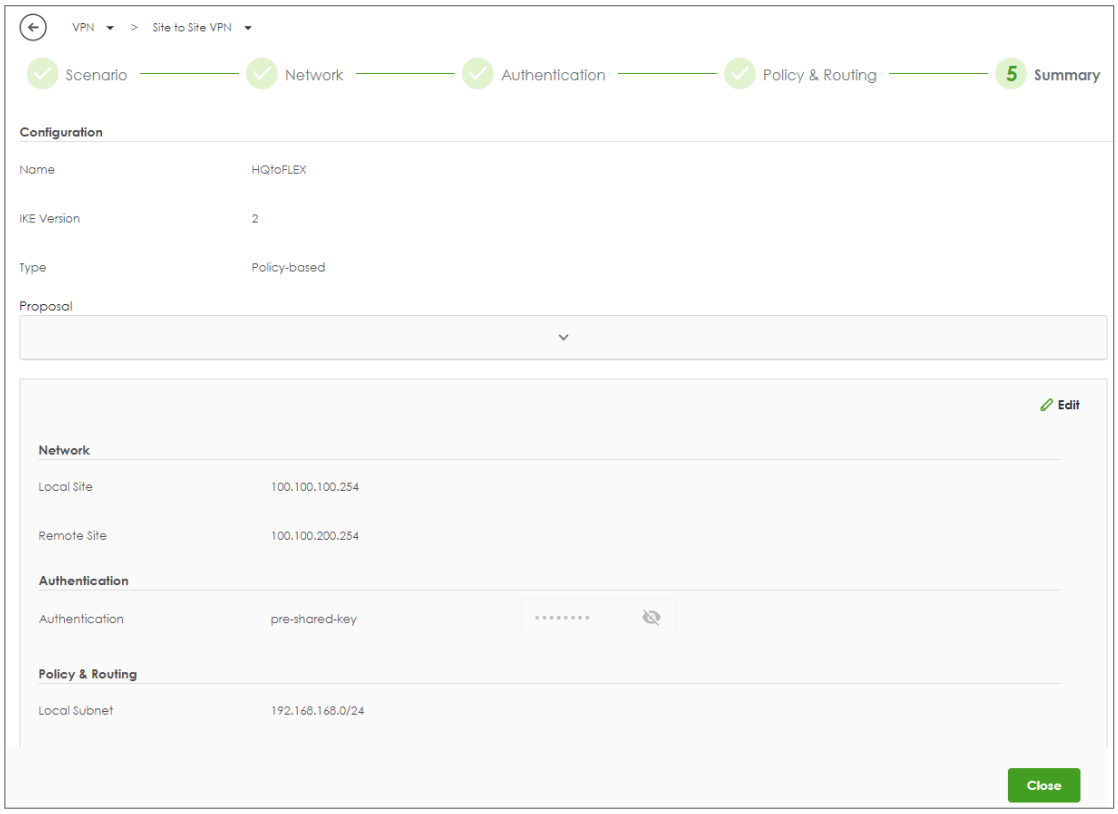
Set Local Subnet to be the IP address of the network connected to USG FLEX H and Remote Subnet to be the IP address of the network connected to the peer ZyWALL.



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

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

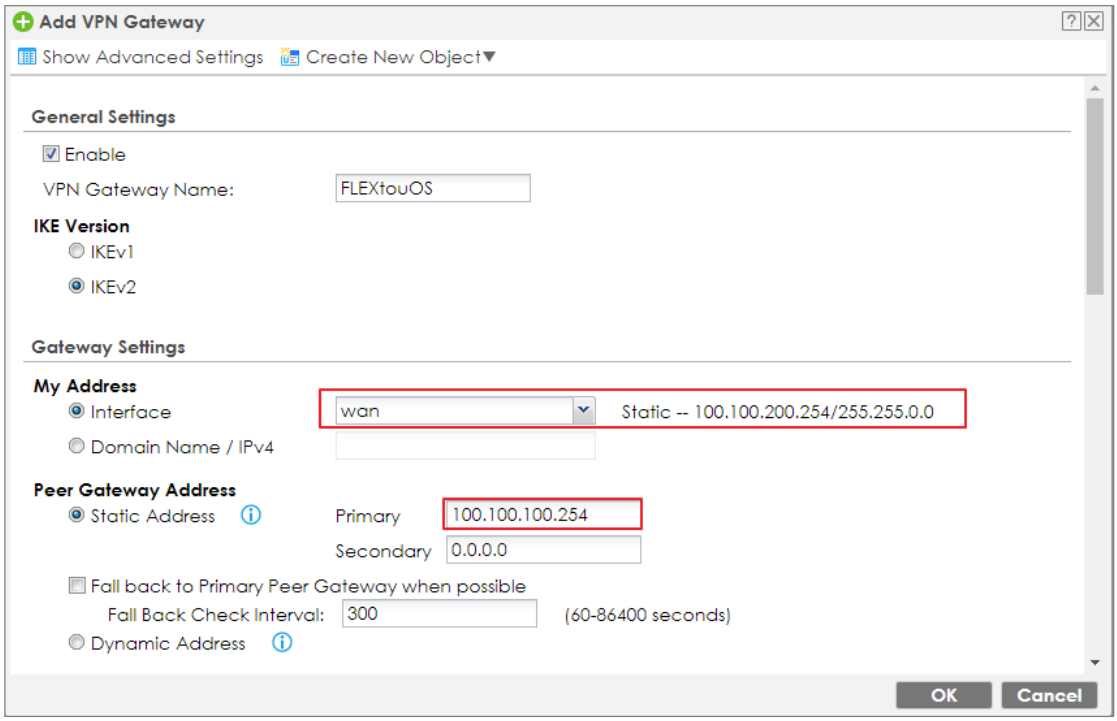


# Set up IPSec VPN Tunnel for ZLD

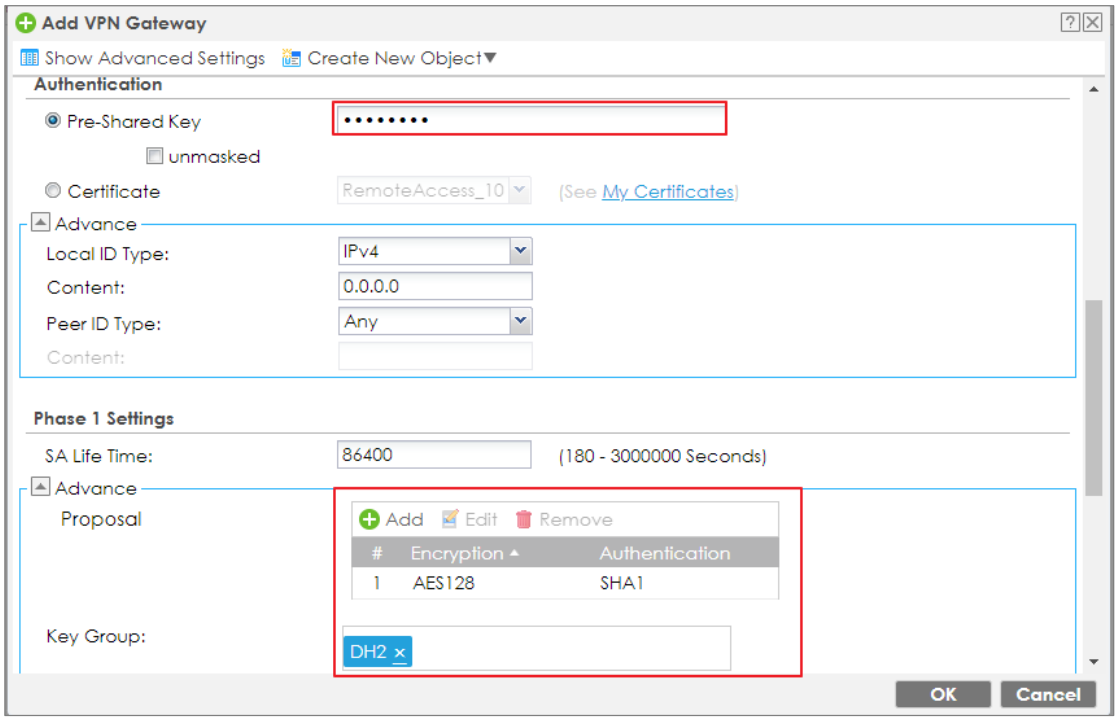
### VPN > IPSec VPN > VPN Gateway

Select the WAN interface and type the Peer Gateway Address.



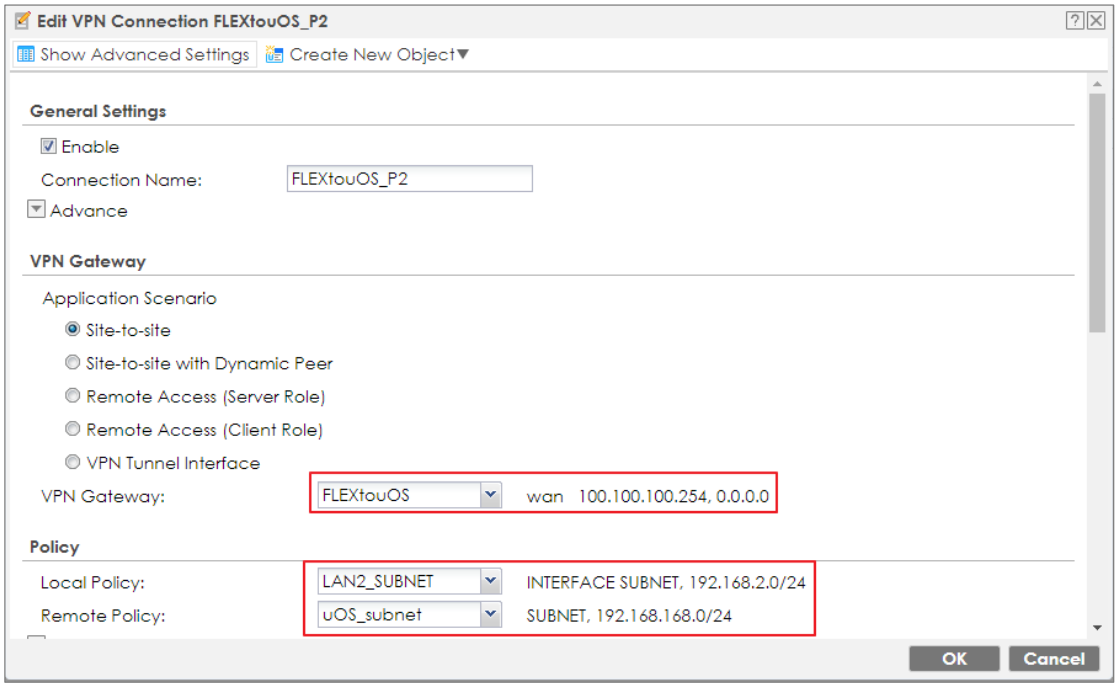
Type Pre-shared Key. The default proposal which created by wizard is "Encryption:AES128, Authentication:SHA1, Key Group:DH2". Those are the same as uOS.



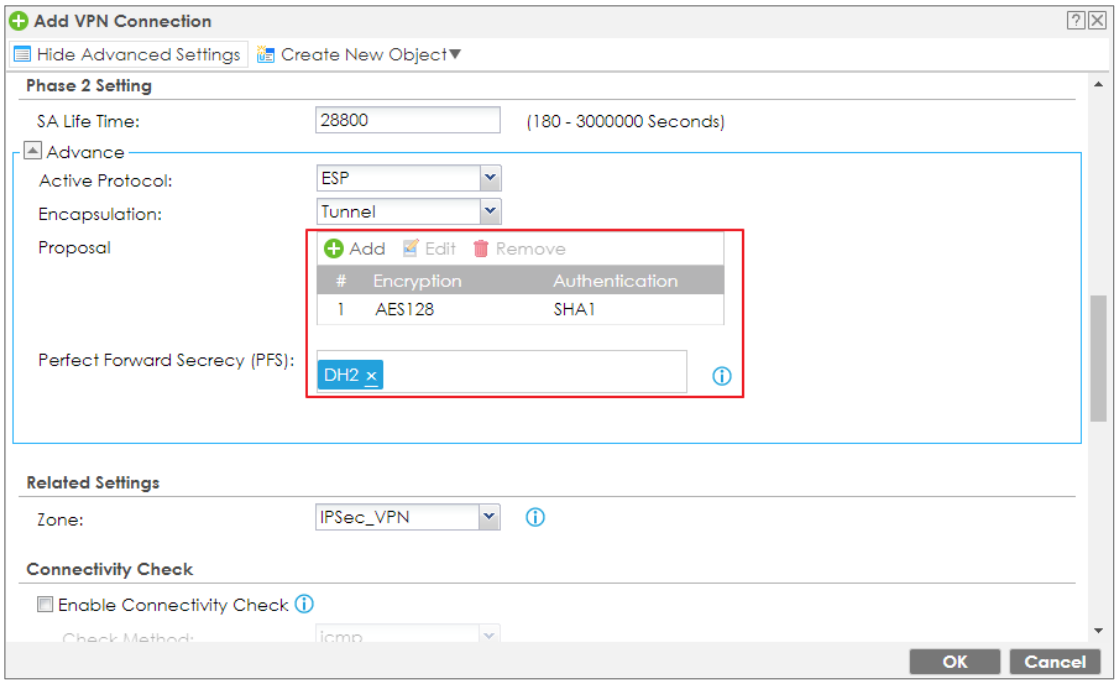
**VPN > IPSec VPN > VPN Connection**

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

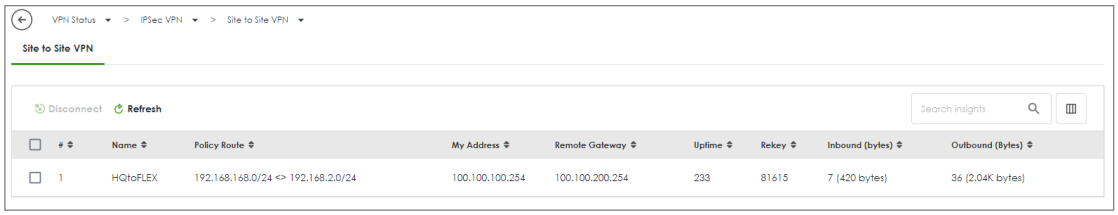


# Test IPSec VPN Tunnel

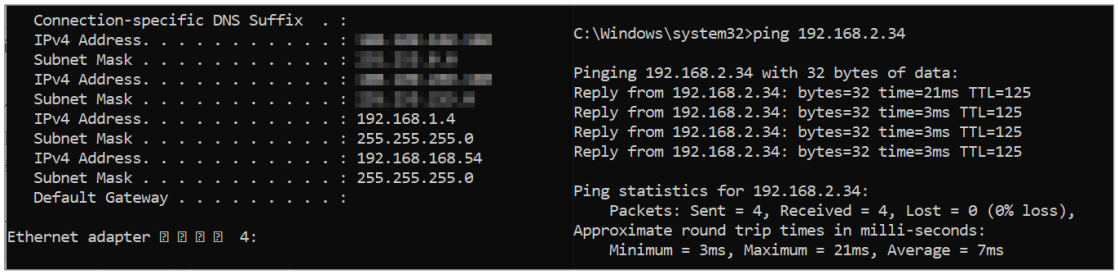
### VPN Status > IPSec VPN

Verify the IPSec VPN status on uOS device.




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

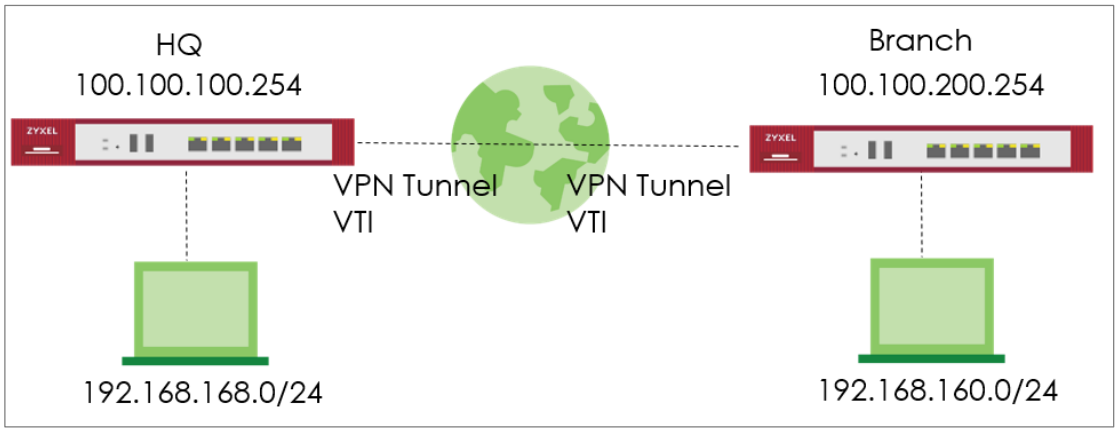
Win 11 > cmd > ping 192.168.2.34



## 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.

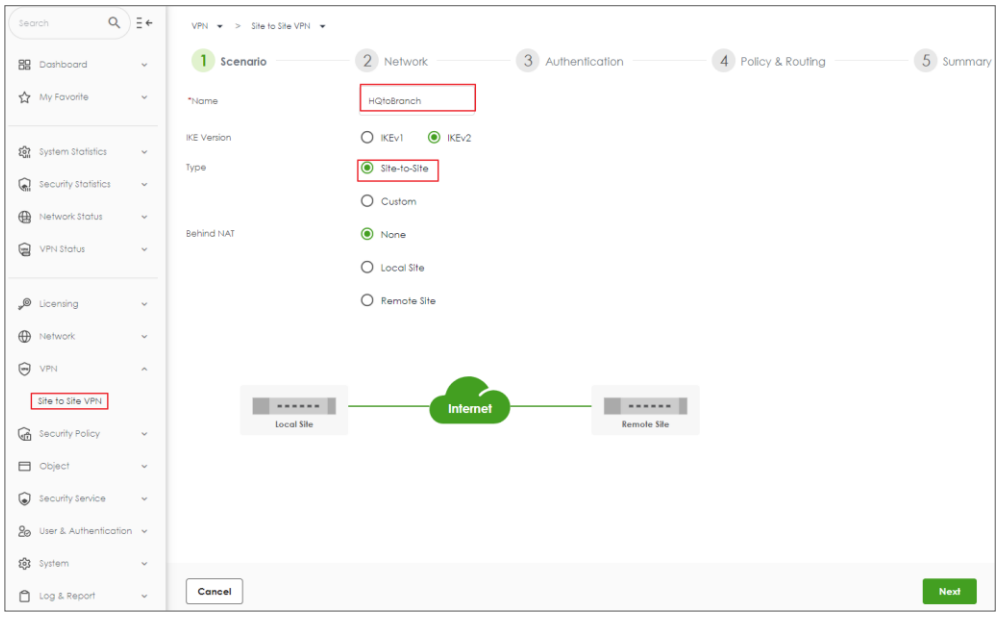


## Set up IPSec VPN Tunnel for HQ

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

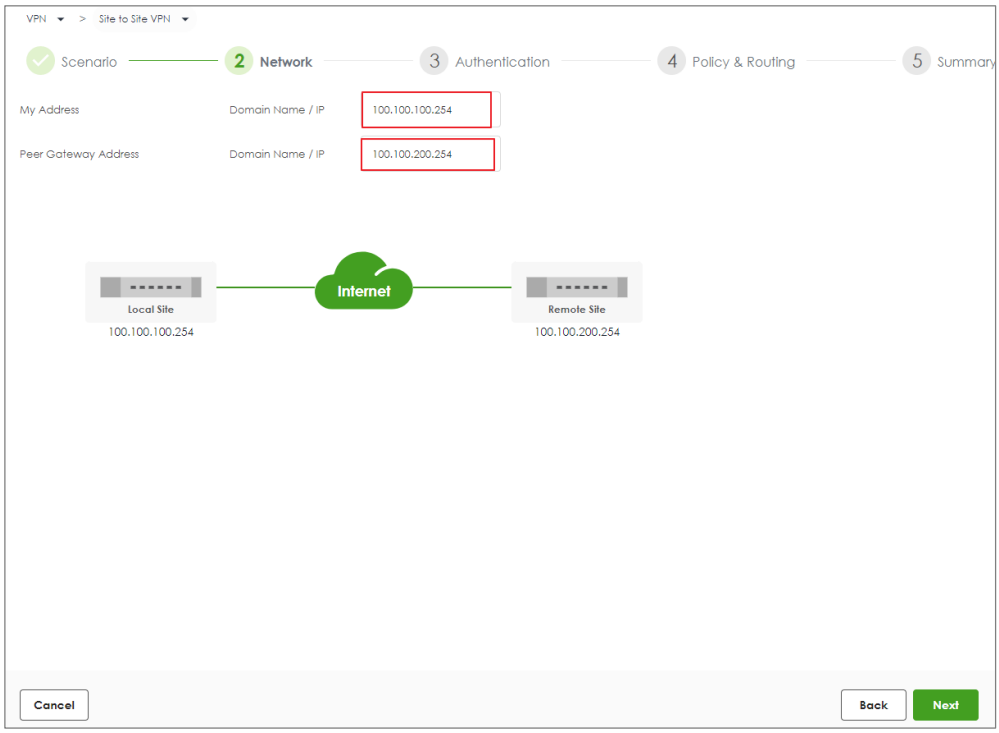
Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site. Click **Next**.



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

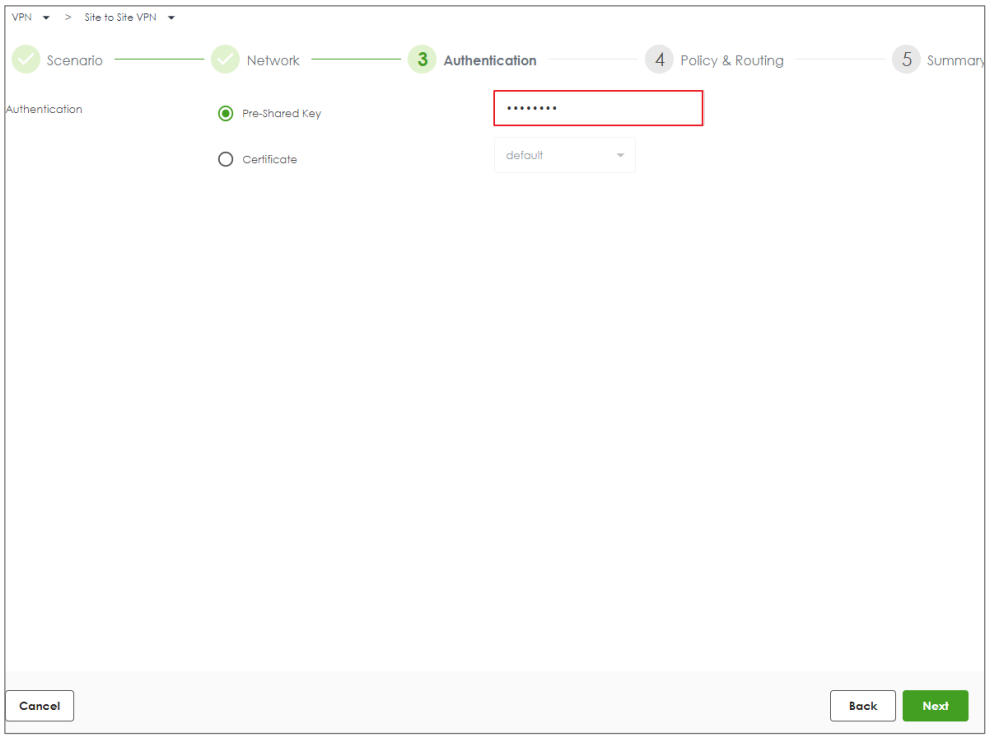
Configure My Address and Peer Gateway Address. Click **Next.**



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

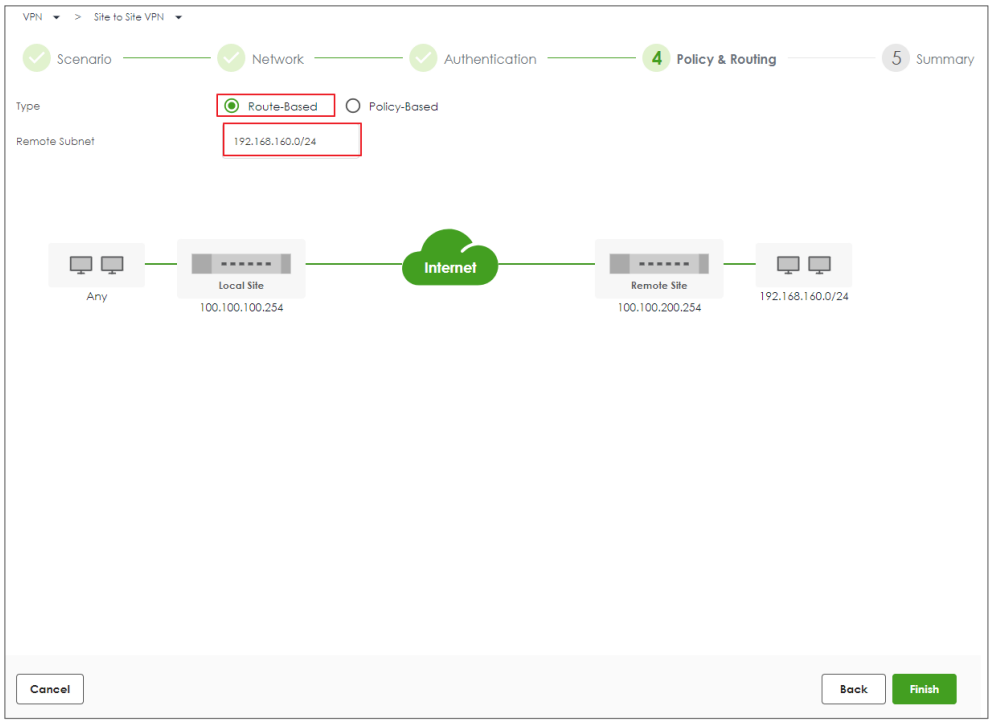
Type a secure Pre-Shared Key. Click **Next**



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

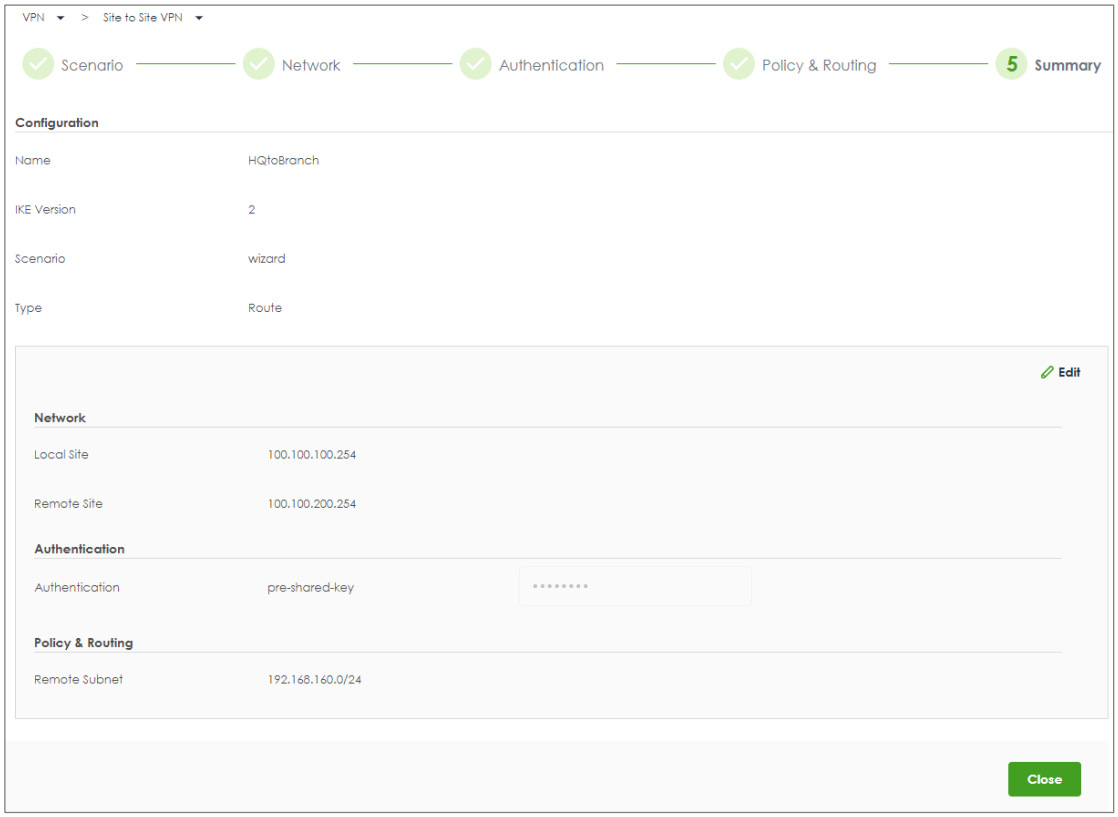
Set Type to Route-Based and configure the Remote Subnet.



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

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

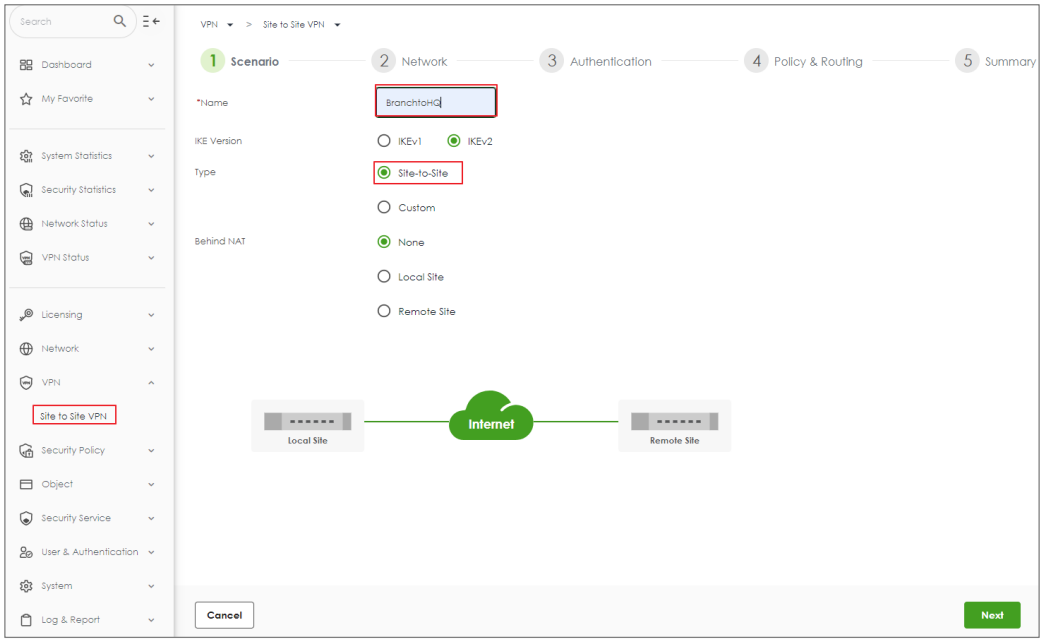


# Set up IPSec VPN Tunnel for Branch

## VPN > Site to Site VPN > Scenario

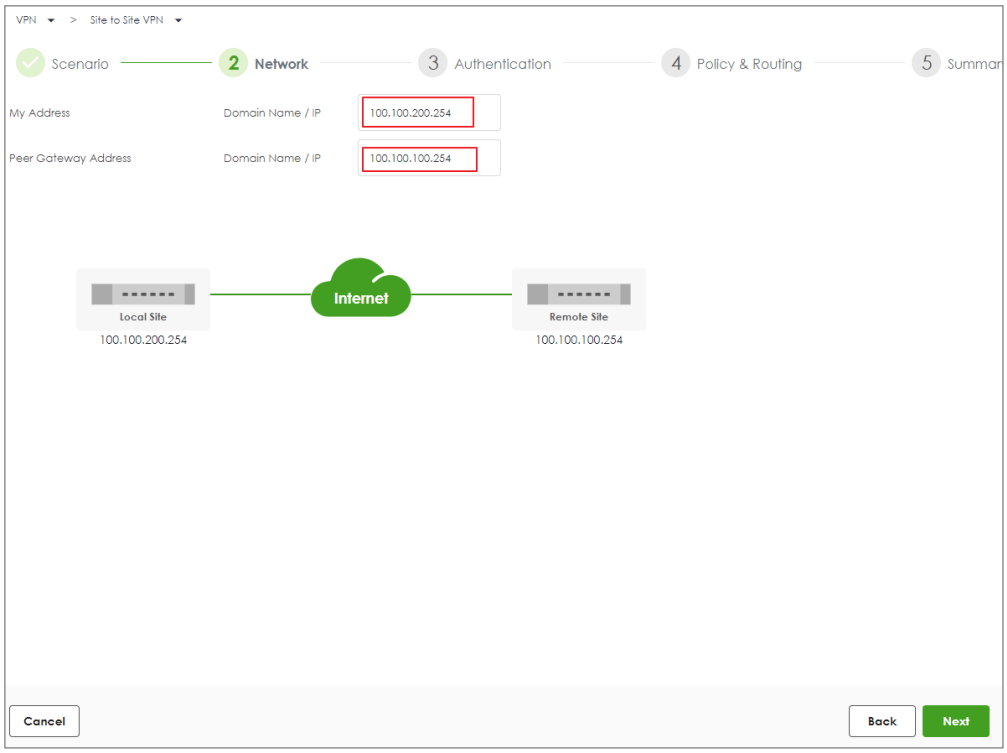
Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site. Click **Next**.



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

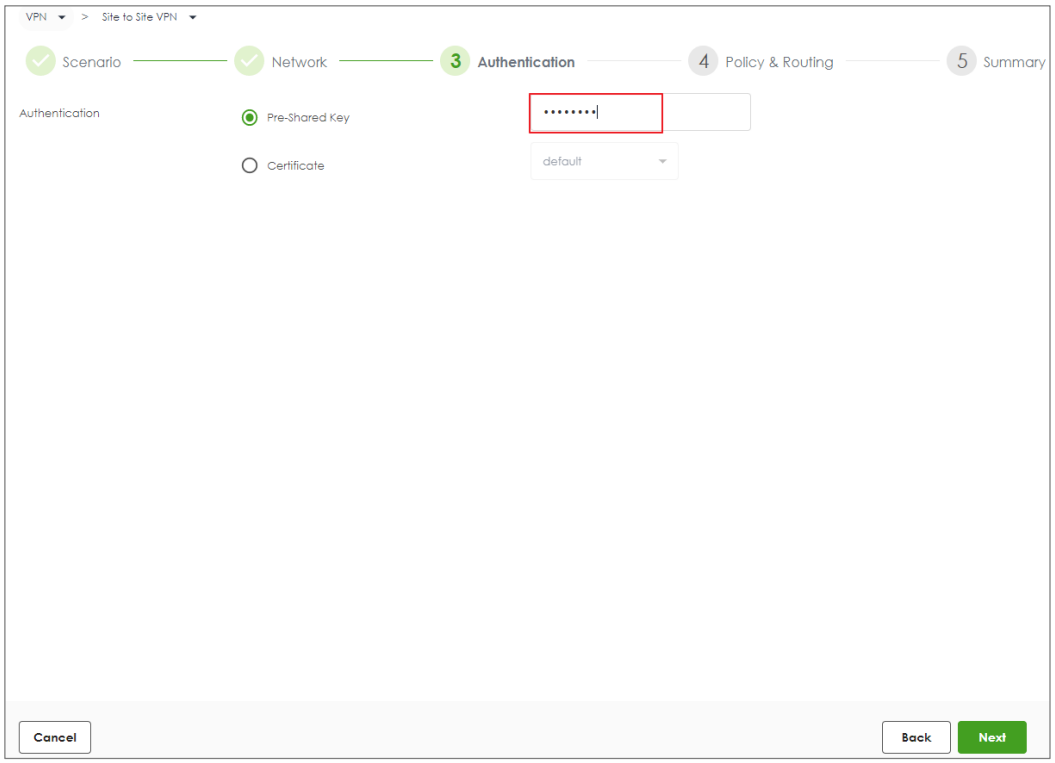
Configure My Address and Peer Gateway Address. Click **Next.**



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

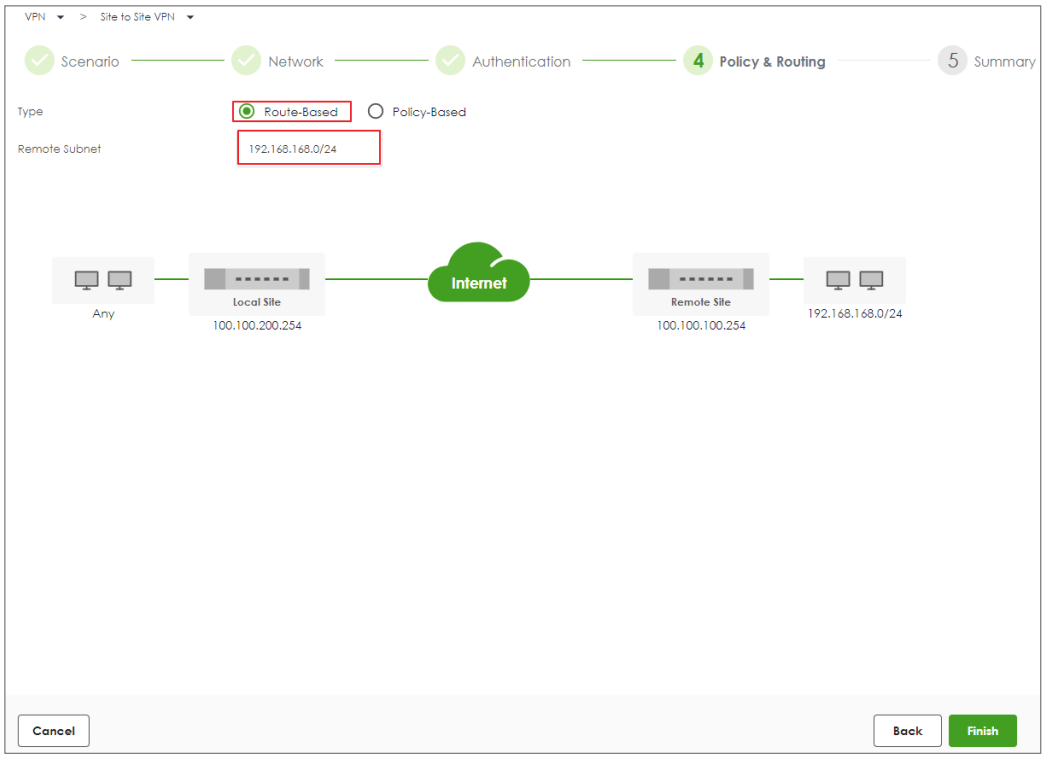
Type a secure Pre-Shared Key. Click **Next**



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

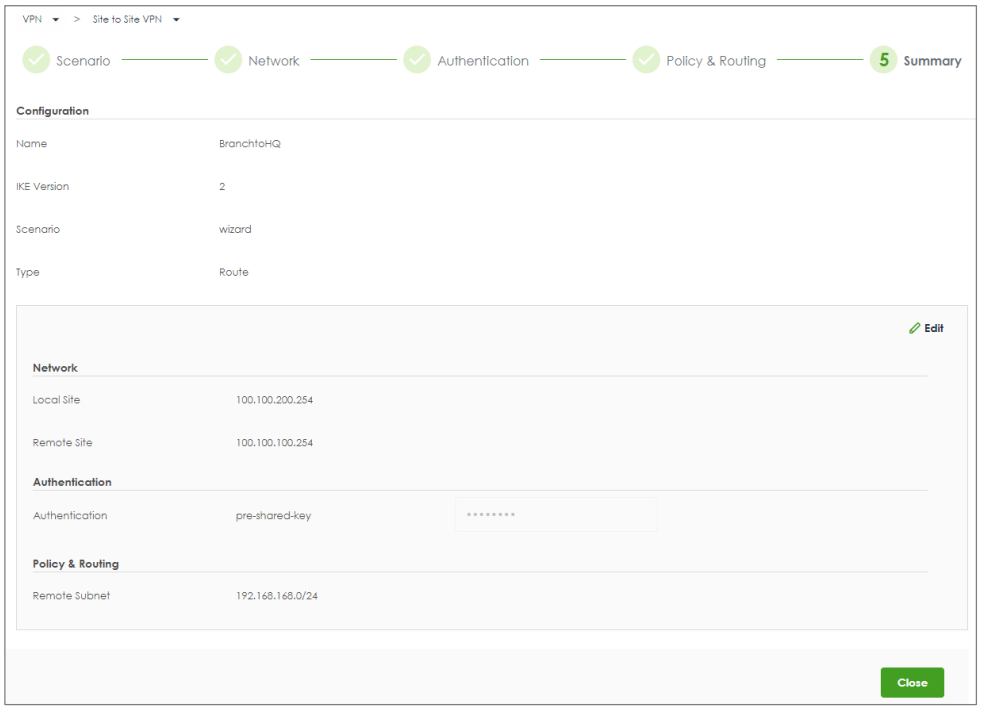
Set Type to Route-Based and Remote Subnet.



**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.

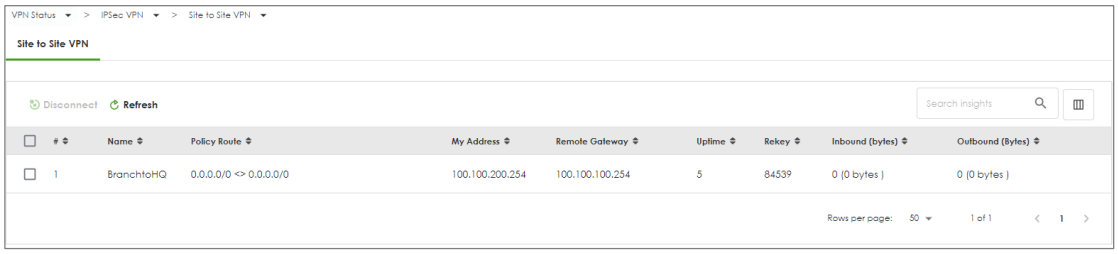


# Test IPSec VPN Tunnel

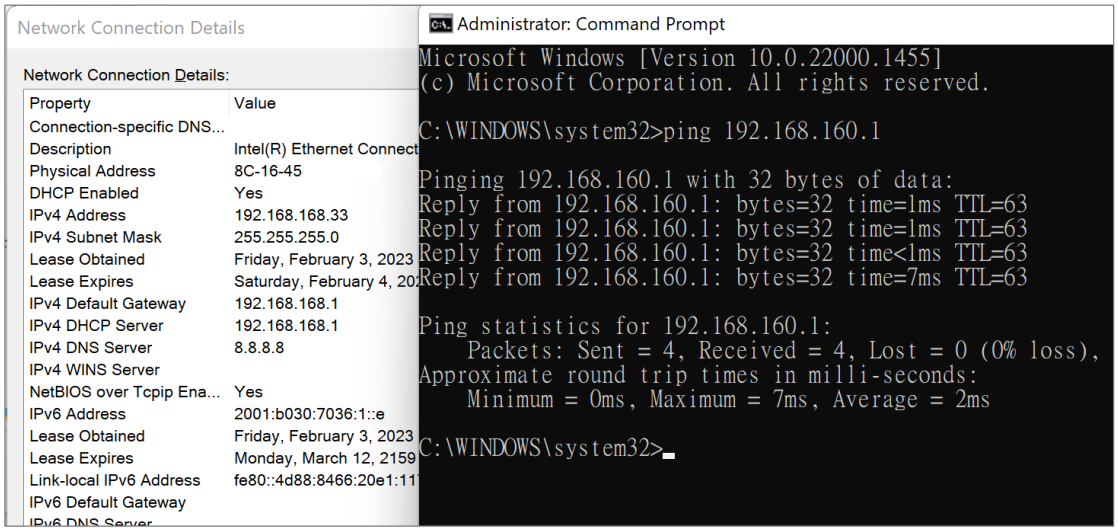
### VPN Status > IPSec VPN

Verify the IPSec VPN status.




### Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1

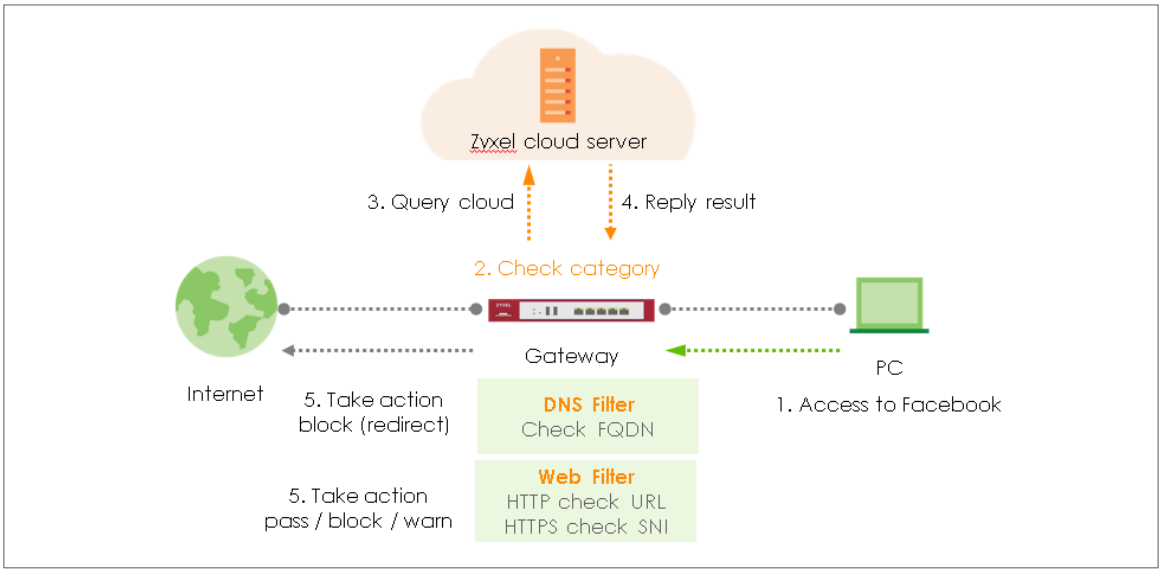


# Chapter 2- Security Service

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

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



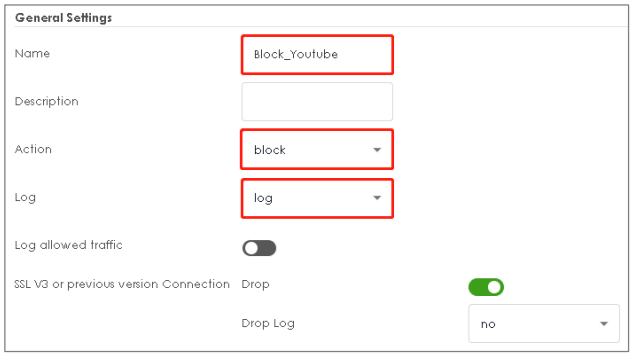

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

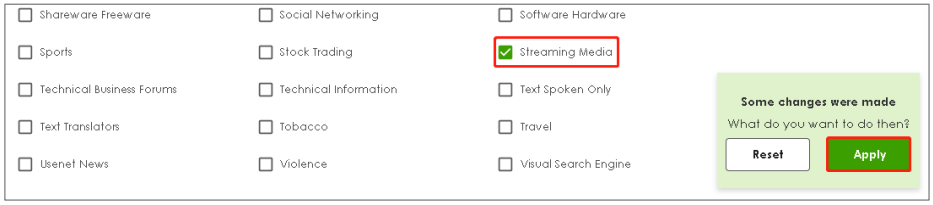
## Set Up Content Filter

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


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



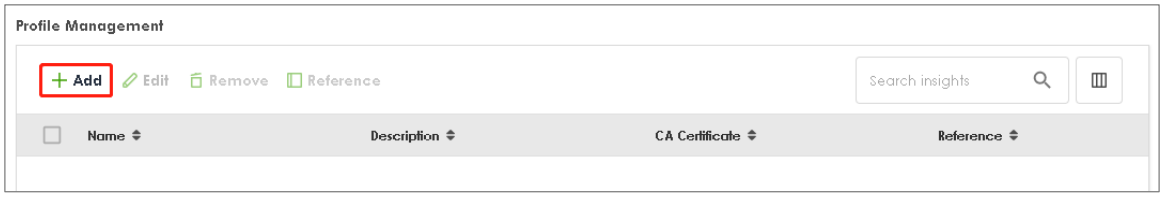

Tick Streaming Media category in Managed Categories, and click Apply.



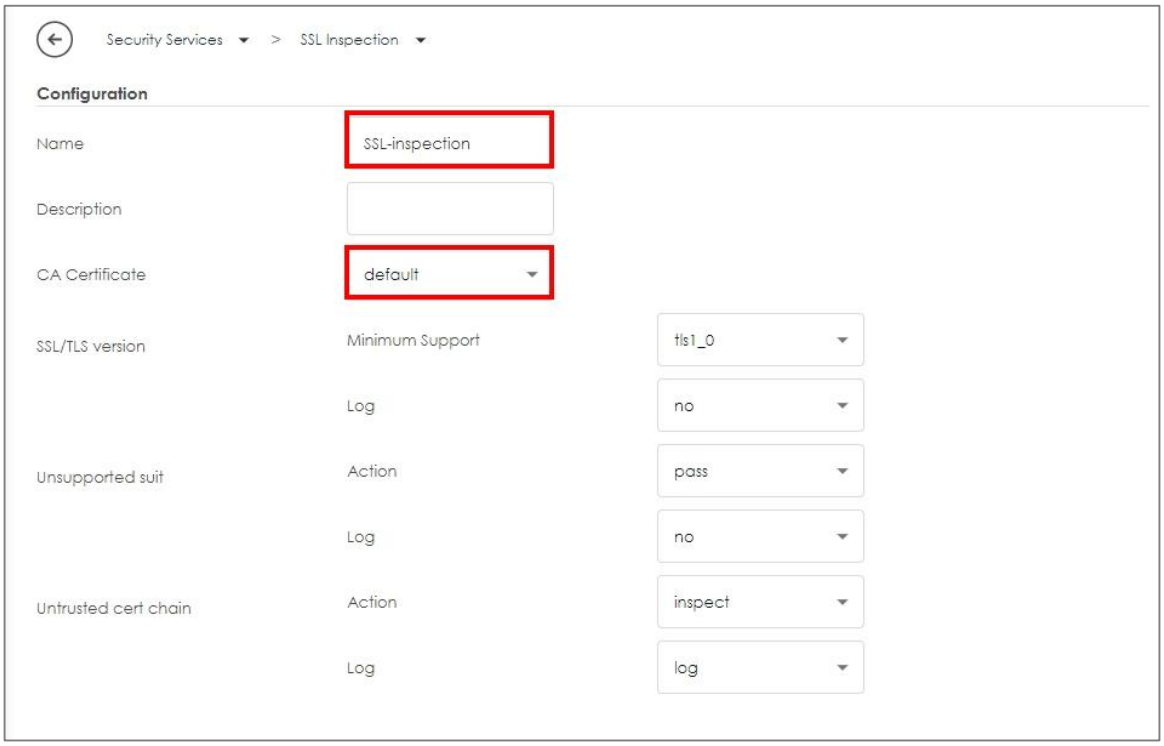

 

## Set Up SSL Inspection

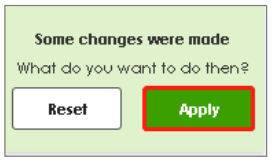
In the FLEX, go to Security Service > SSL inspection > profile > Profile Management, and click Add to create profile




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




Click Apply to add SSL Inspection profile.

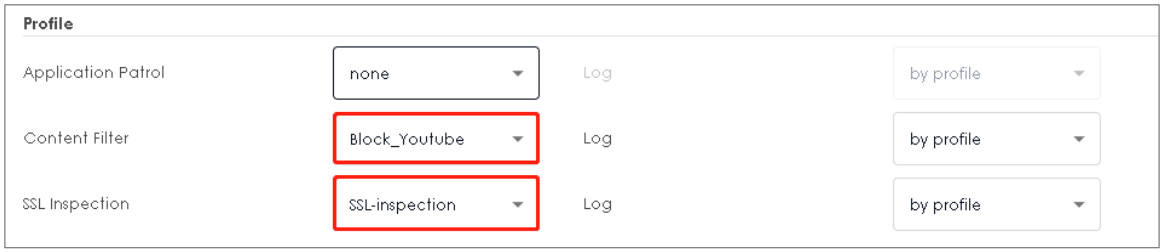


## Set Up the Security Policy

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

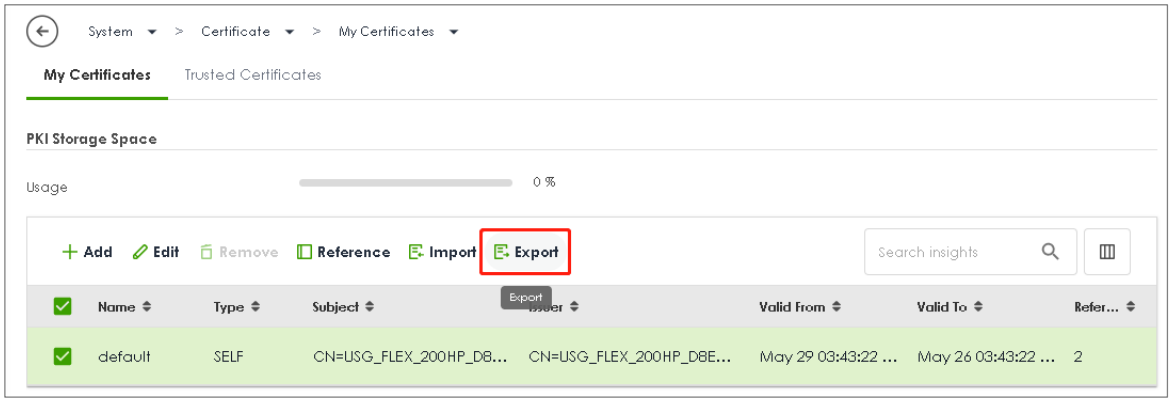
Select Content Filtering, and SSL Inspection. Click Apply to save.



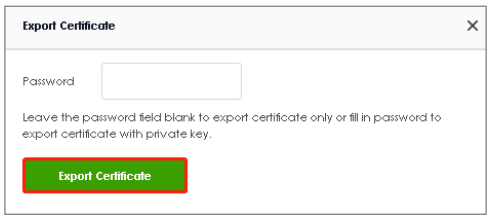

## Export Certificate from FLEX and Import it to Windows

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.

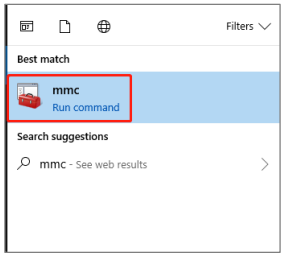



Click Export Certificate to export certificate file, and Save default certificate as default.crt file to Windows OS.

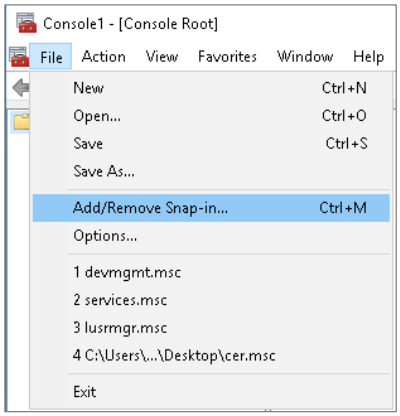


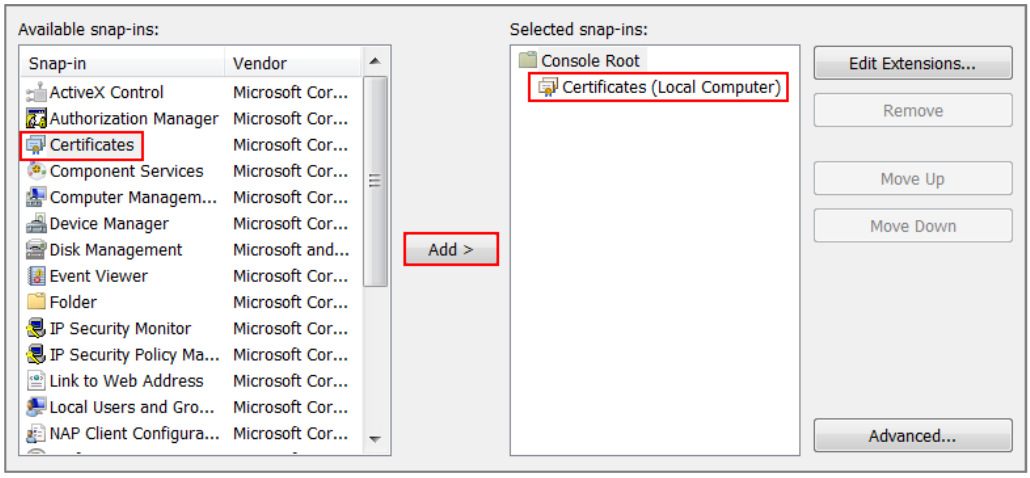
In Windows Start Menu > Search Box, type MMC and press Enter.




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



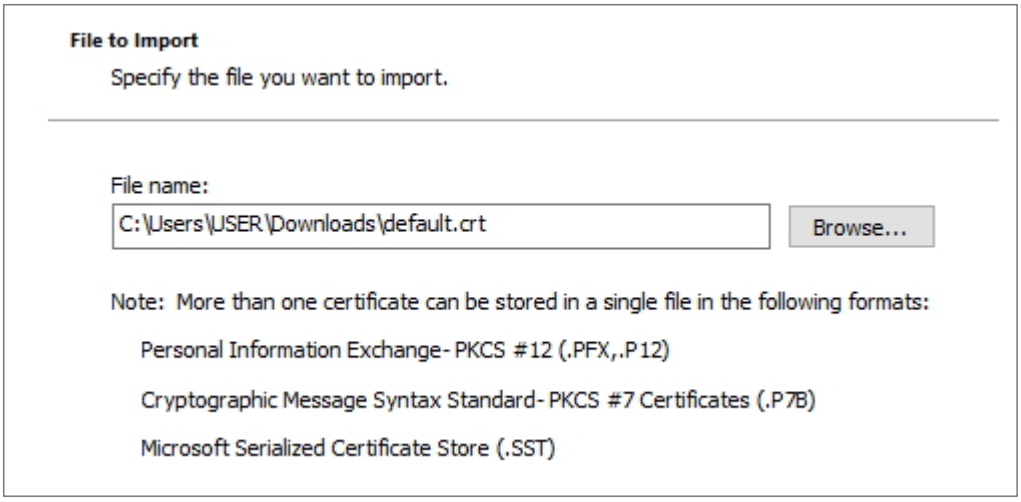

In the Available snap-ins, select the Certificates and click Add button. Select Computer account > Local Computer. Then, click Finished and OK to close the Snap-ins window.



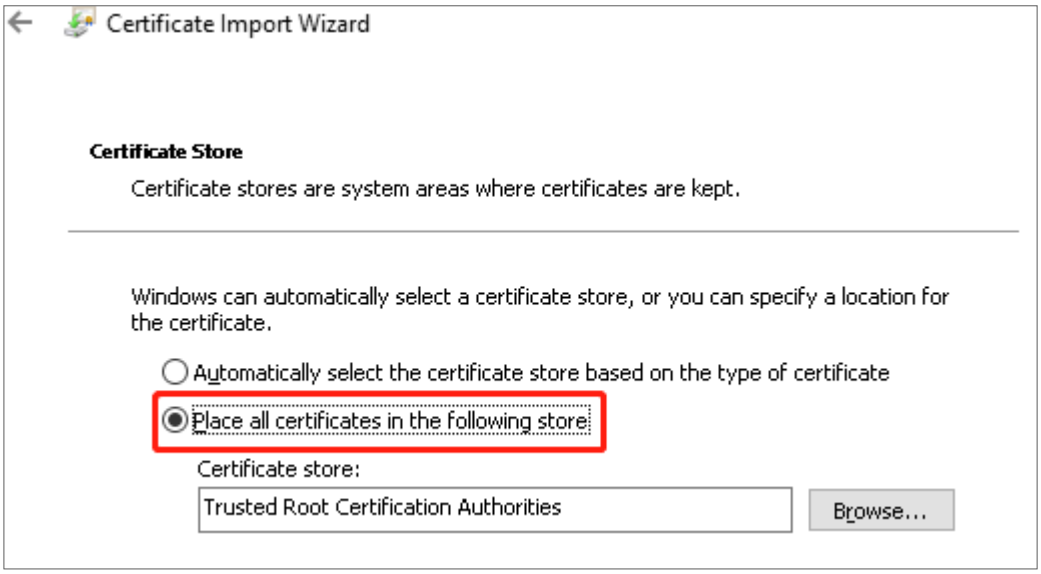
In the mmc console window, open the Certificates (Local Computer) > Trusted Root Certification Authorities, right click Certificate > All Tasks > Import…

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



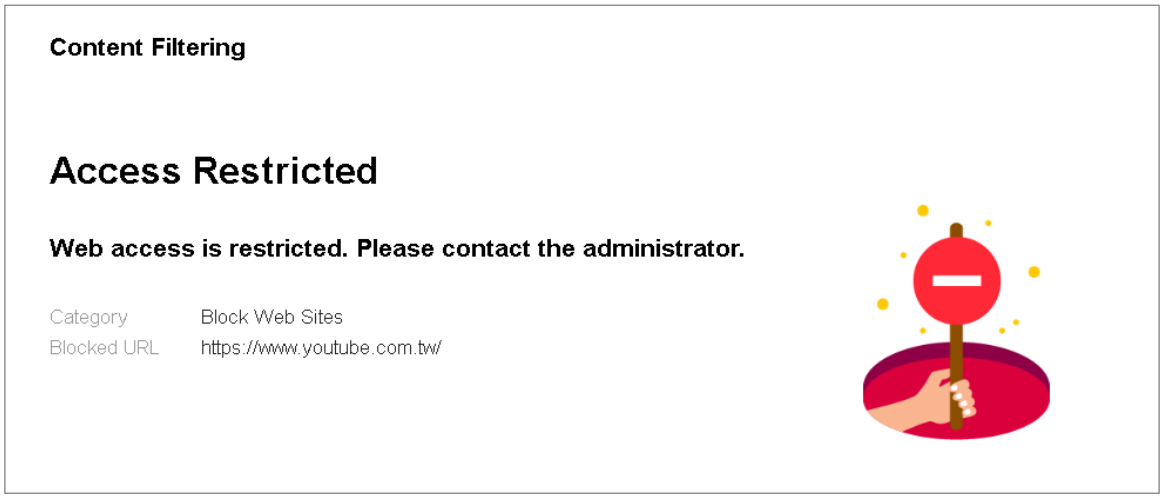
Select Place all certificates in the following store and then click Browse and find Trusted Root Certification Authorities. Click Next, then click Finish.



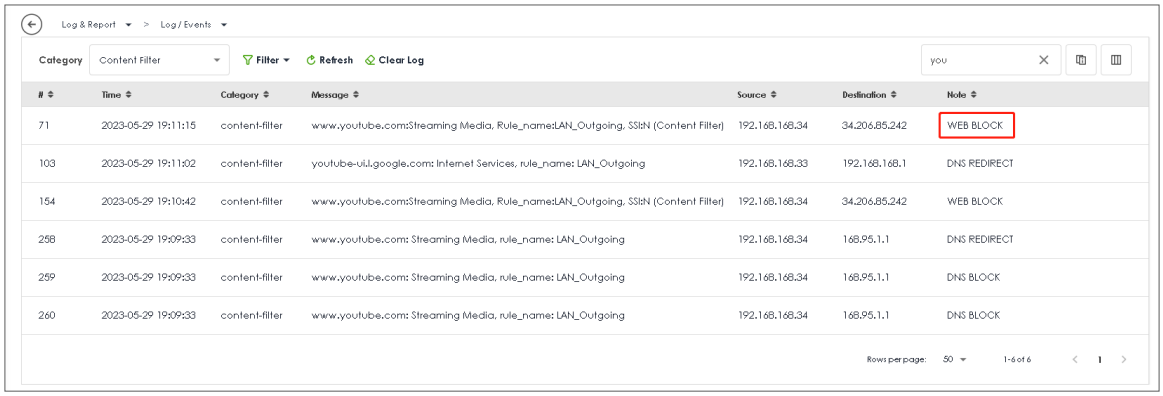

 

## Test the Result

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

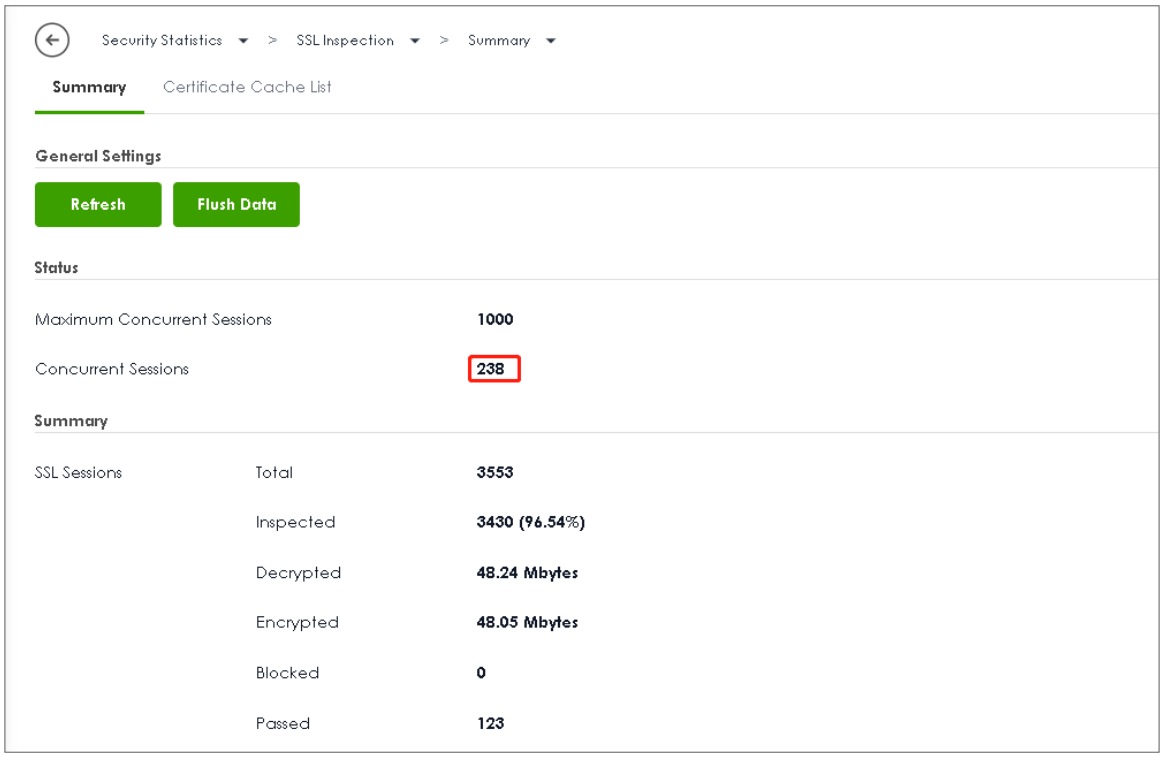



Go to Log & Report > Log/Events and select Content Filtering to check the logs.

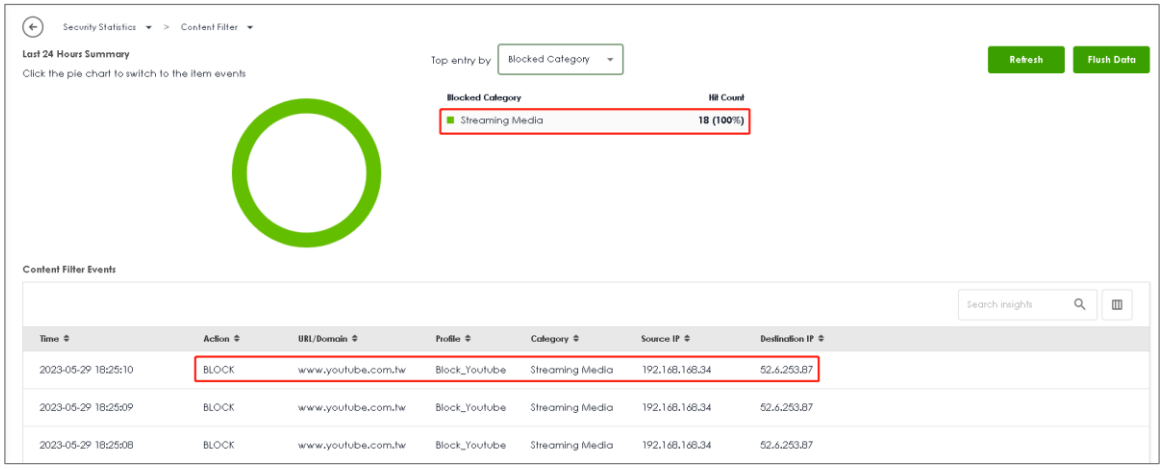


Go to Security Statistics > SSL Inspection > Summary. Traffic is inspected by SSL inspection.




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

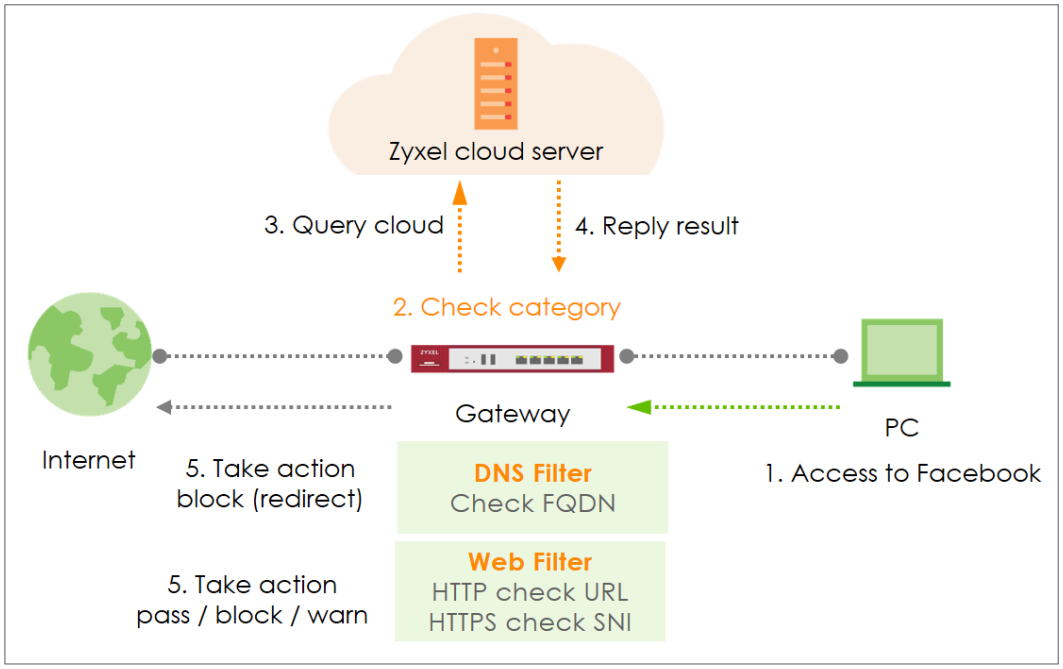


# How to Configure Content Filter with HTTPs Domain Filter

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.

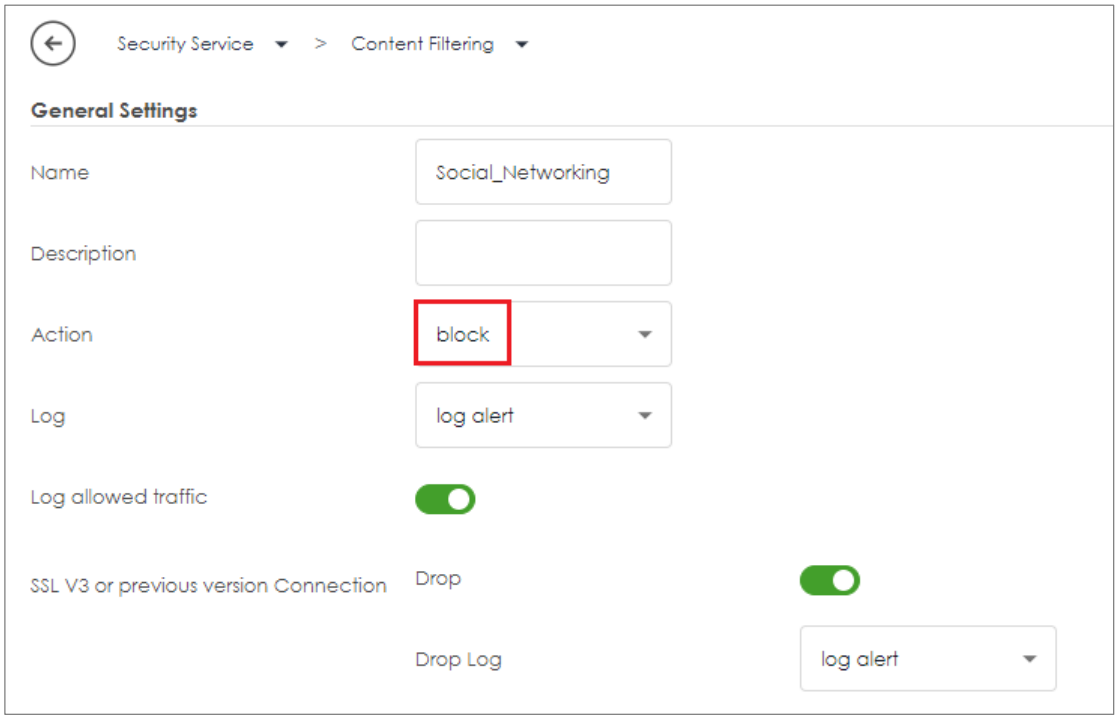



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

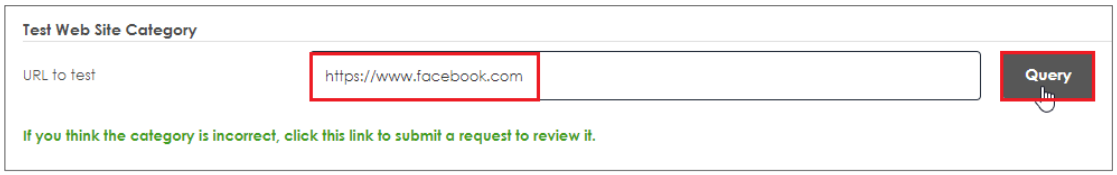
 

## Set Up the Content Filter

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.

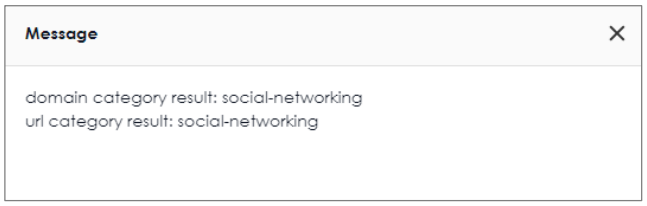



Navigate to **Test Web Site Category** and type URL to test the category and click **Query**.



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

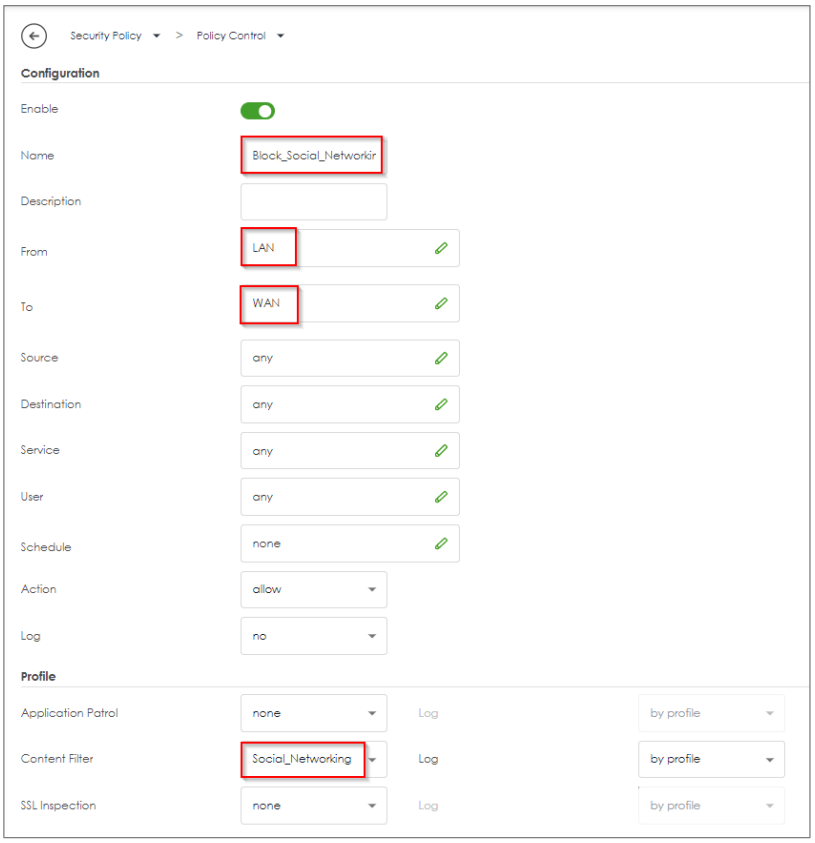



Scroll to the **Managed Categories** section, and select categories in this section to control access to specific types of Internet content.

## Set Up the Security Policy

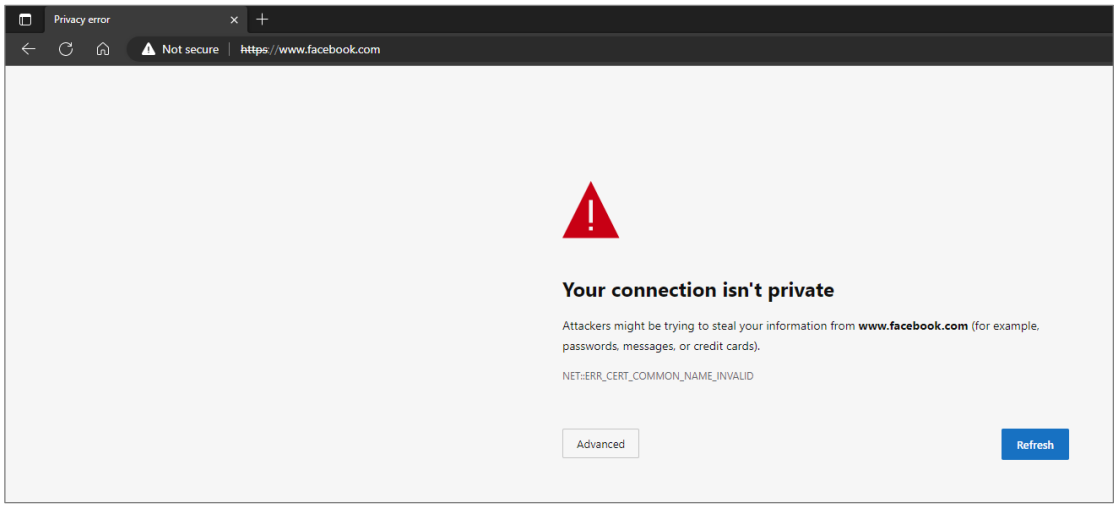
Go to **Security Policy > Policy Control** to configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies and apply the **Profile > Content Filter** "Social_Networking" on this security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



## Test Result

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

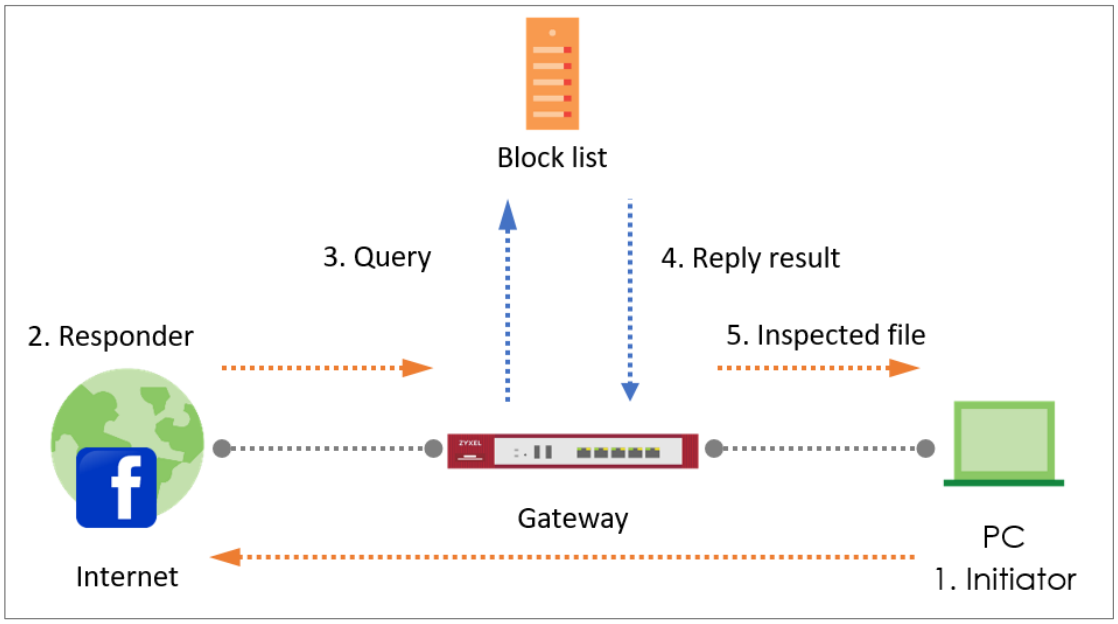



Navigate to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.

# 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.

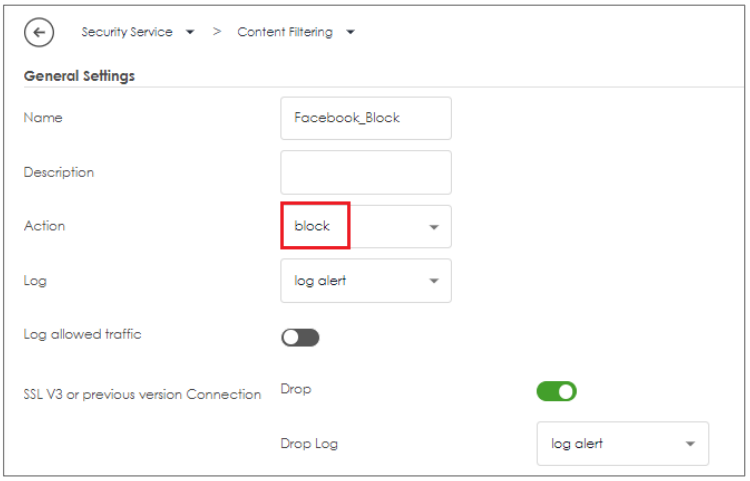



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

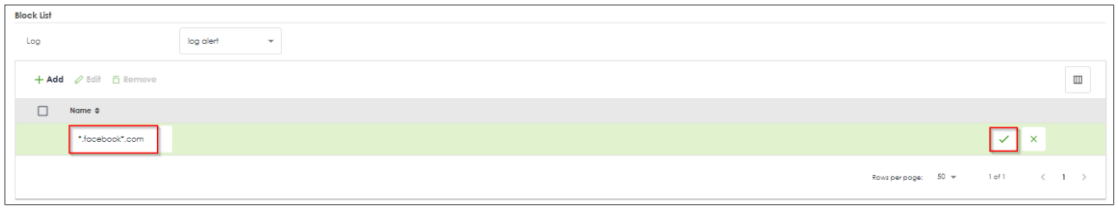
 

## Set Up the Content Filter

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.



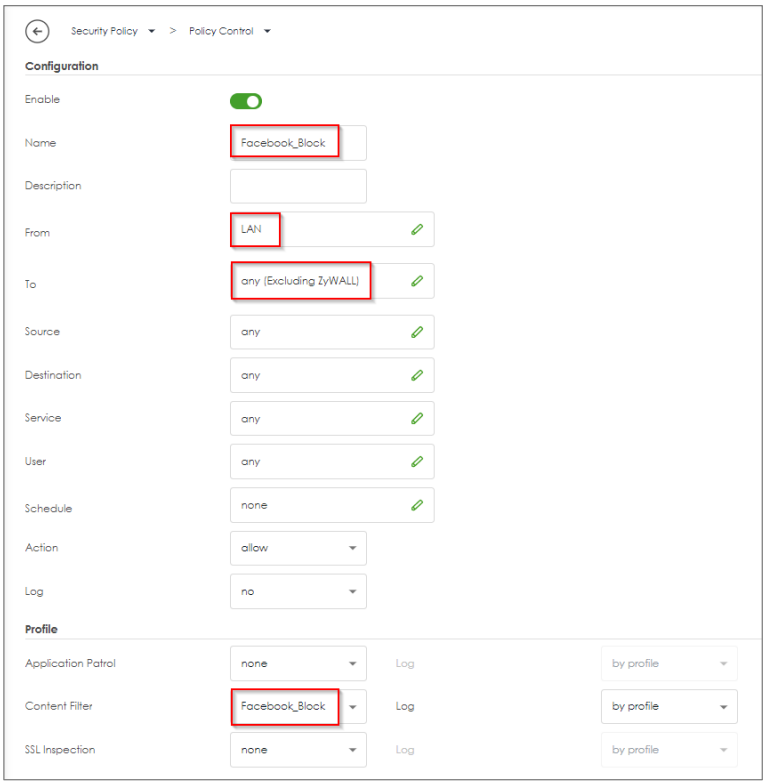

Go to **Block List** and type URL "*.facebook*.com" to add the URL that you want to block.



## Set Up the Security Policy

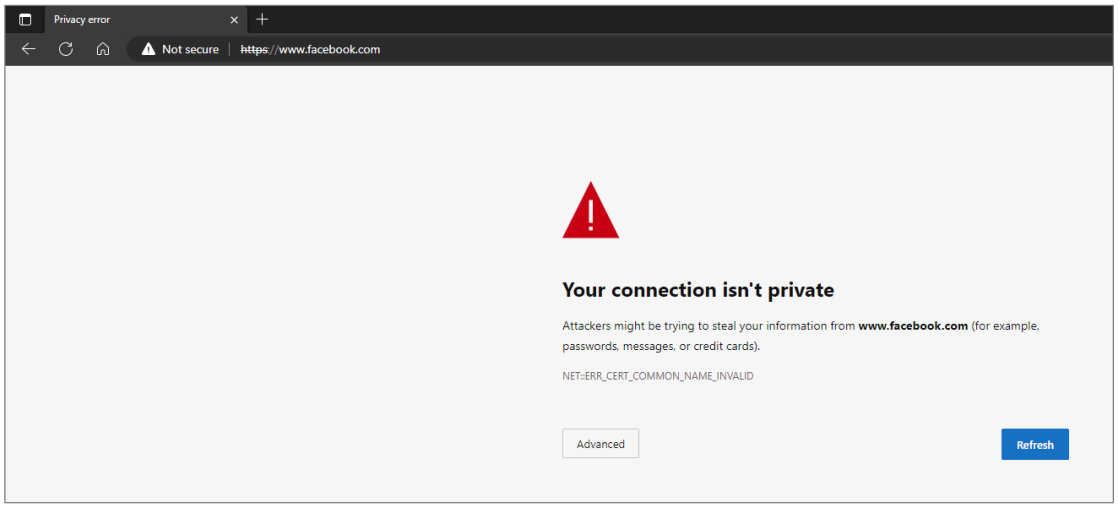
Go to **Security Policy > Policy Control** to configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies and apply the **Profile > Content Filter** "Facebook_Block" on this security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



## Test the Result

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

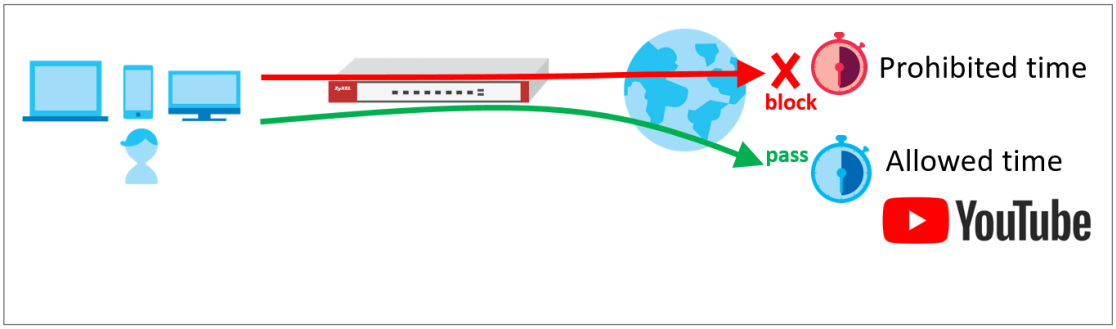



Go to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.

# 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.

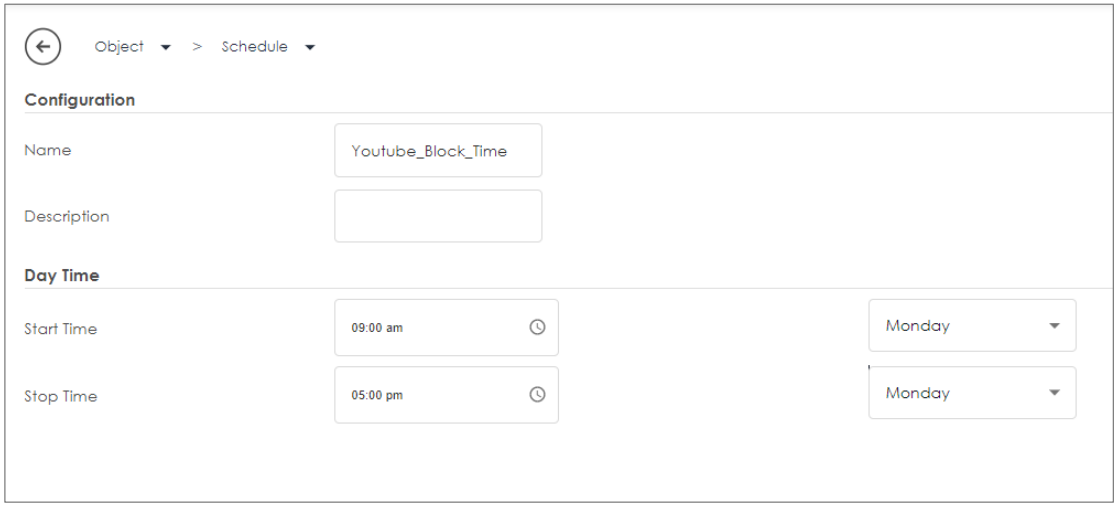



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

## Set Up the Schedule

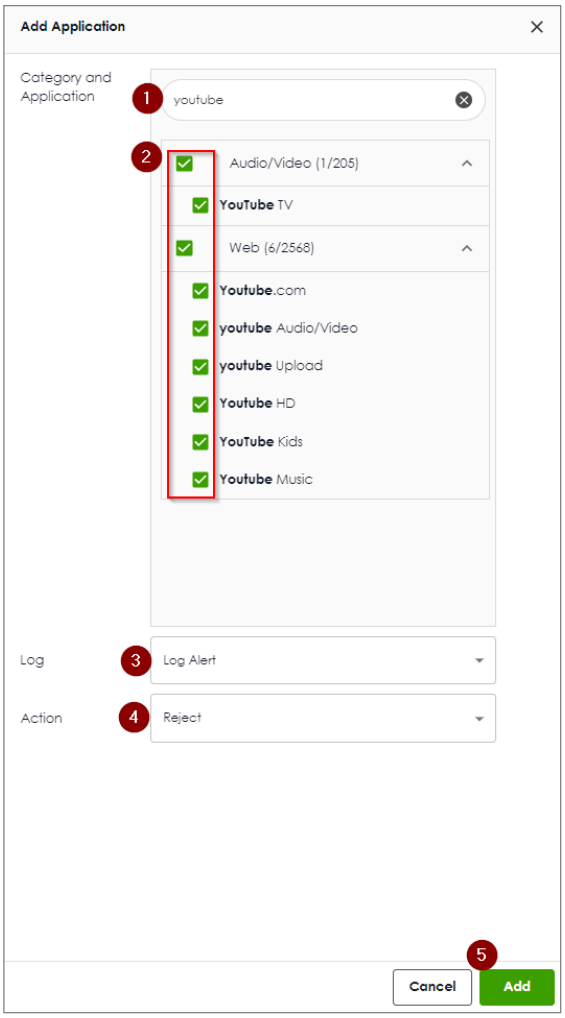
Go to **Object > Schedule > Recurring > Add Schedule Recurring Rule**. Configure a **Name** for you to identify the **Schedule Recurring Rule**. Specify the **Day Time** hour and minute when the schedule begins and ends each day.



## Create the Application Patrol profile

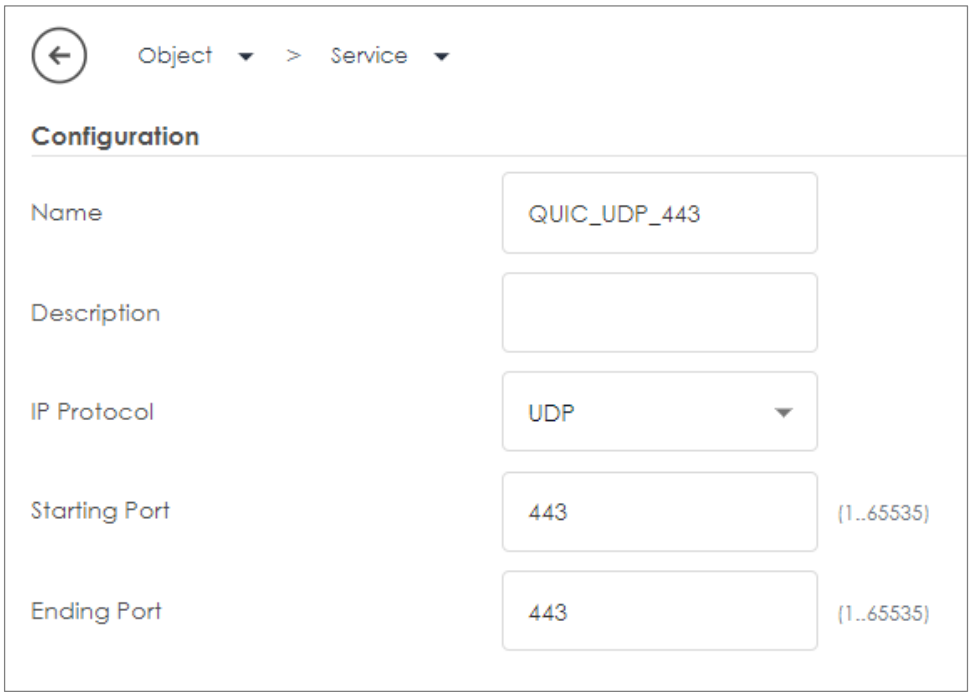
In the USG Flex H, go to **Security Service > App Patrol > General Settings > Application Management**. To add an App Patrol profile, configure the profile name and select "**Search Application**". Then enter the keyword "youtube" to search the key-related results and select all YouTube-related apps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



## Set Up the Security Policy

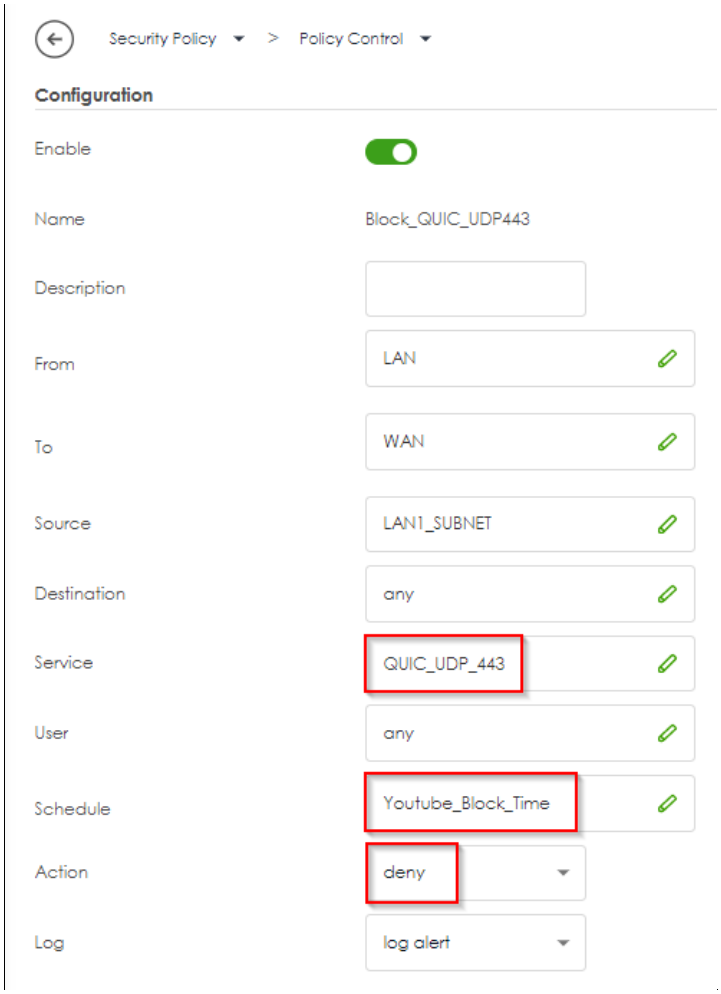
Go to **Object > Service** to add a UDP 443 service object.



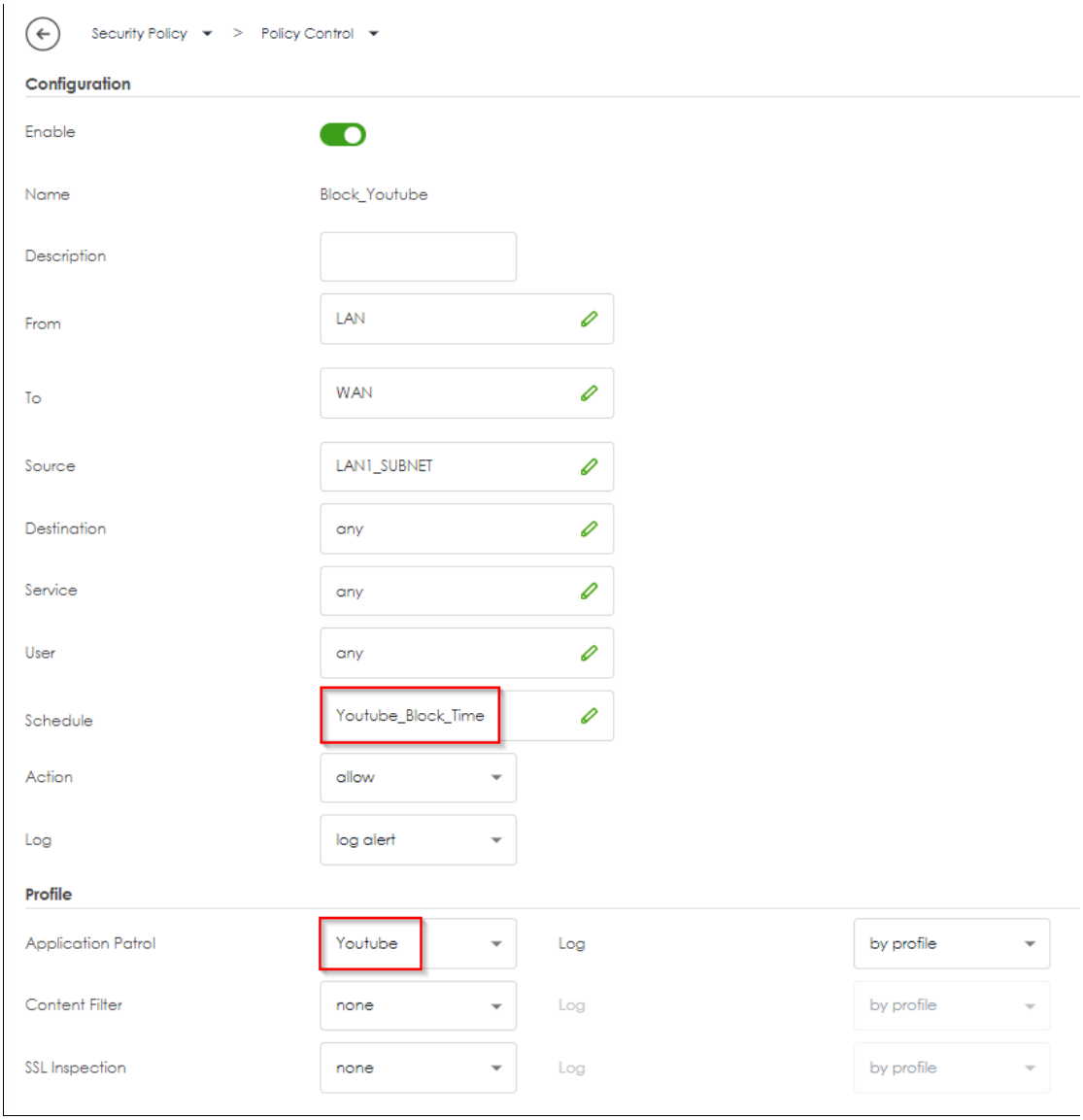
Go to **Security Policy > Policy Control** to configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select the **service** QUIC_UDP443 and select the **Schedule** that defines when the policy would be applied.

In this example, select "Youtube_Blocked_Time".



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.



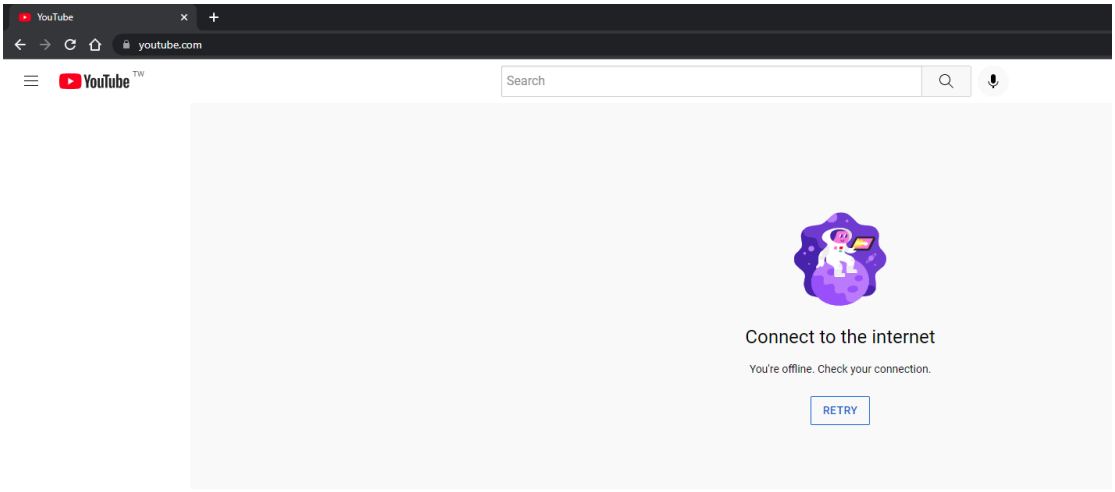
Then go back to the security policy page and move the security priority of block UDP 443 is higher than block YouTube by schedule.

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

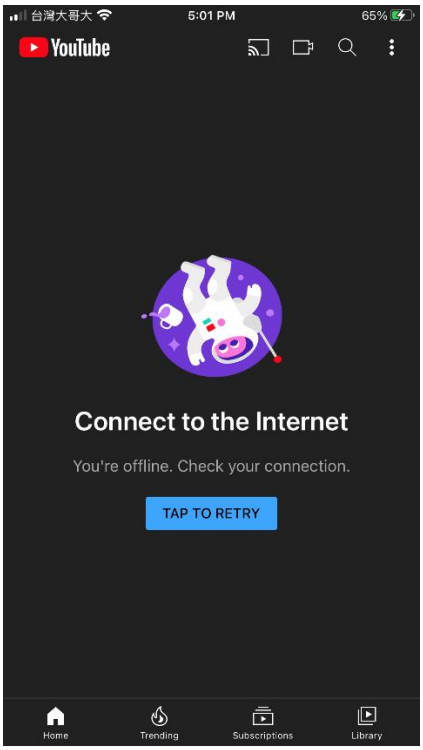
 

## Test the Result

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

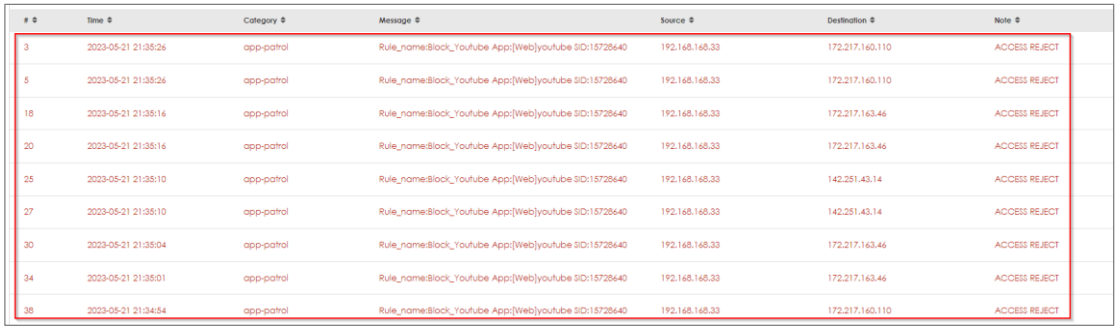



Open the YouTube APP on the phone and cannot access to YouTube.



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

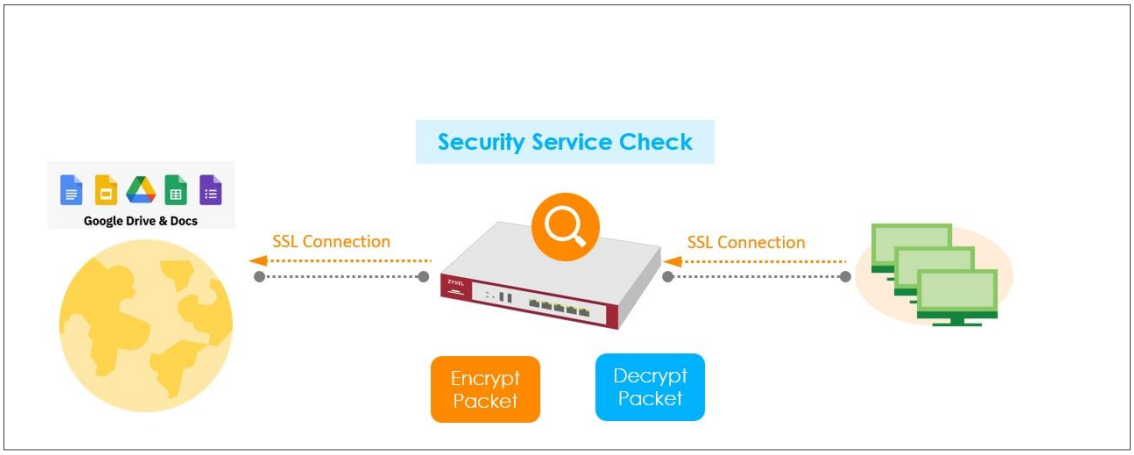


| # | Time | Category | Message | Source | Destination | Note |
|---|---|---|---|---|---|---|
| 3 | 2023-05-21 21:35:26 | app-patrol | Rule_name:Block_Youtube App:[Web]youtube SID:15728640 | 192.168.168.33 | 172.217.160.110 | ACCESS REJECT |
| 5 | 2023-05-21 21:35:26 | app-patrol | Rule_name:Block_Youtube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

# How to Control Access to Google Drive

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




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

## Create app patrol profile

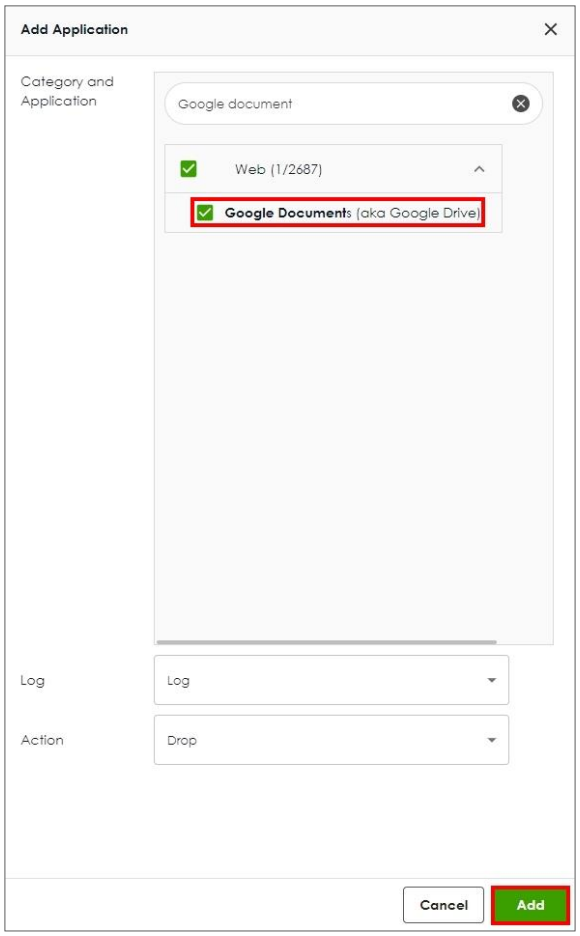
Go to Security Service > App patrol > Profile management, and click Add to create profile


Click add to add application in this profile.

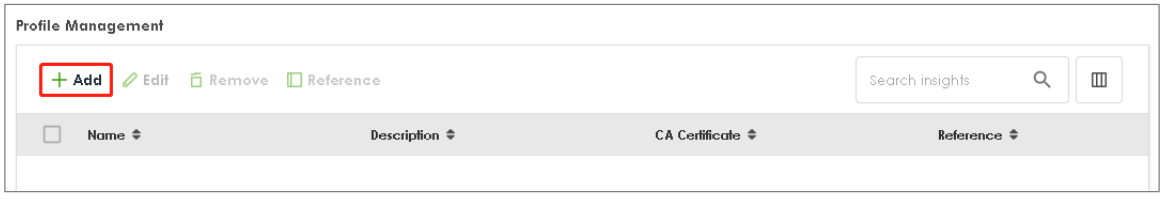
Search **Google Documents(aka Google Drive)**, and select this Application.

Action set to Drop, and click Add.



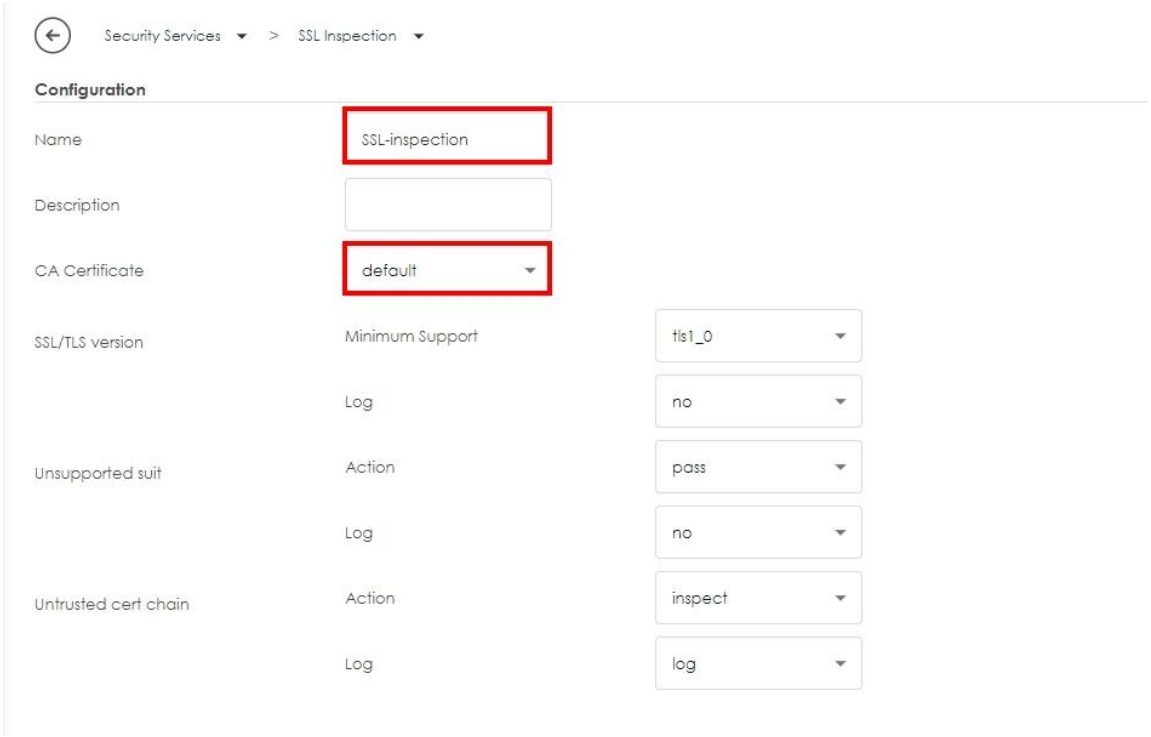

## Set Up SSL Inspection on the FLEX

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



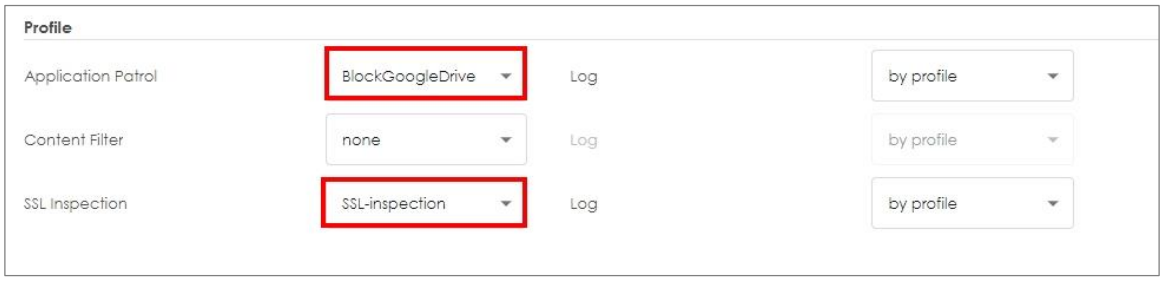
Type profile Name, and select the CA Certificate to be the certificate used in this profile. Leave other actions as default settings.




## 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.

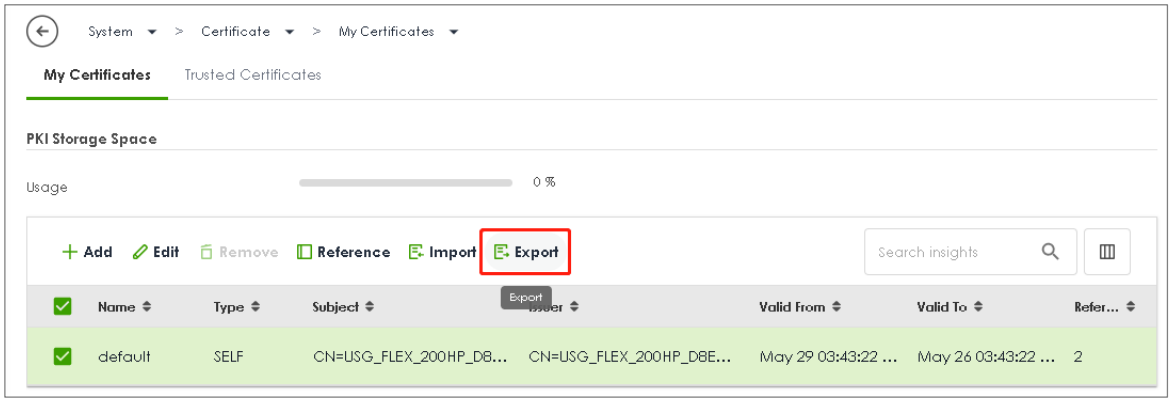


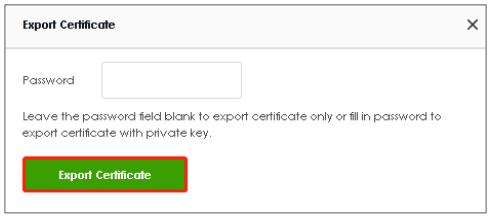
## Export Certificate from FLEX and import to Lan hosts

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

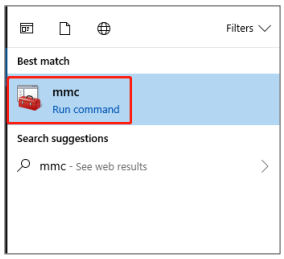
Go to System > Certificate > My Certificates to export default certificate from FLEX.




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

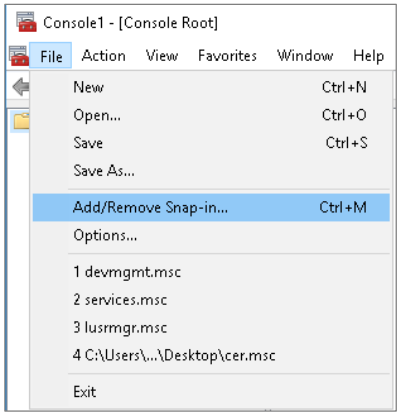



In Windows Start Menu > Search Box, type MMC and press Enter.

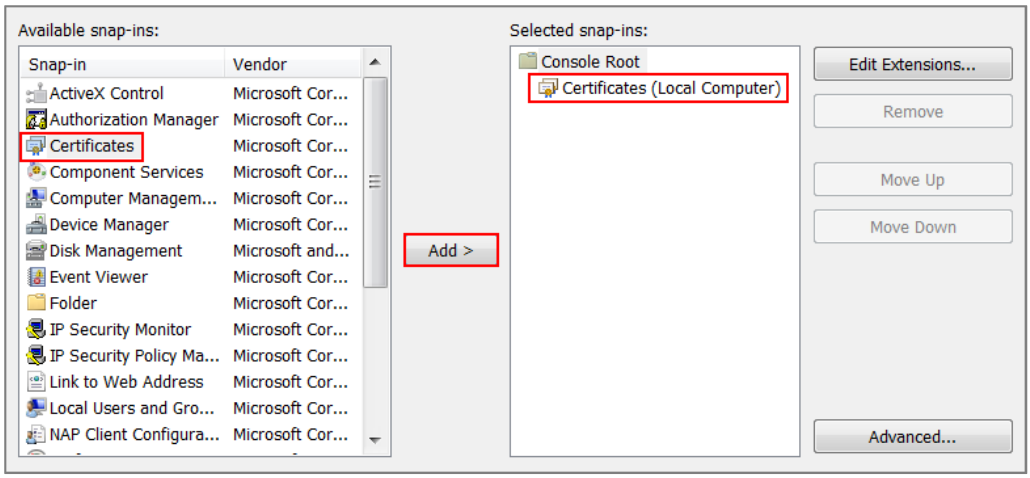


In the mmc console window, click File > Add/Remove Snap-in...

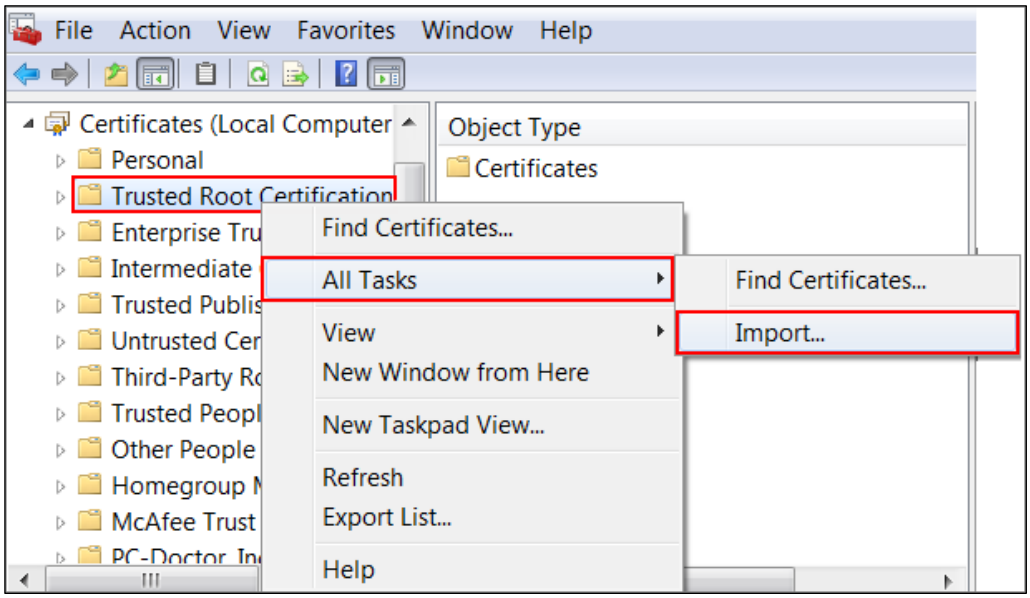



In the Available snap-ins, select the Certificates and click Add button. Select Computer account > Local Computer. Then, click Finished and OK to close the Snap-ins window.

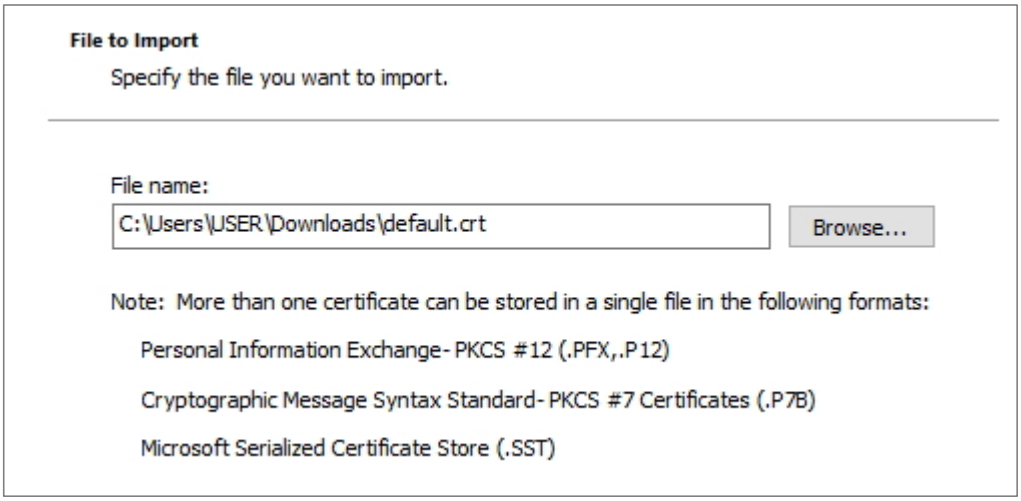


In the mmc console window, open the Certificates (Local Computer) > Trusted Root Certification Authorities, right click Certificate > All Tasks > Import…

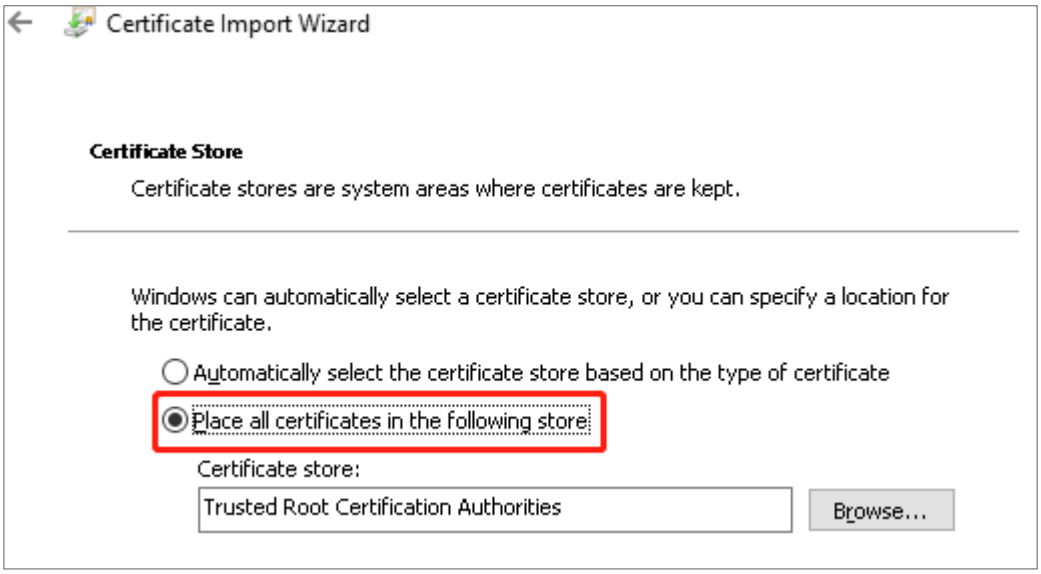



Click Next. Then, Browse..., and locate the default.crt file you downloaded earlier. Then, click Next.



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




## Test the Result

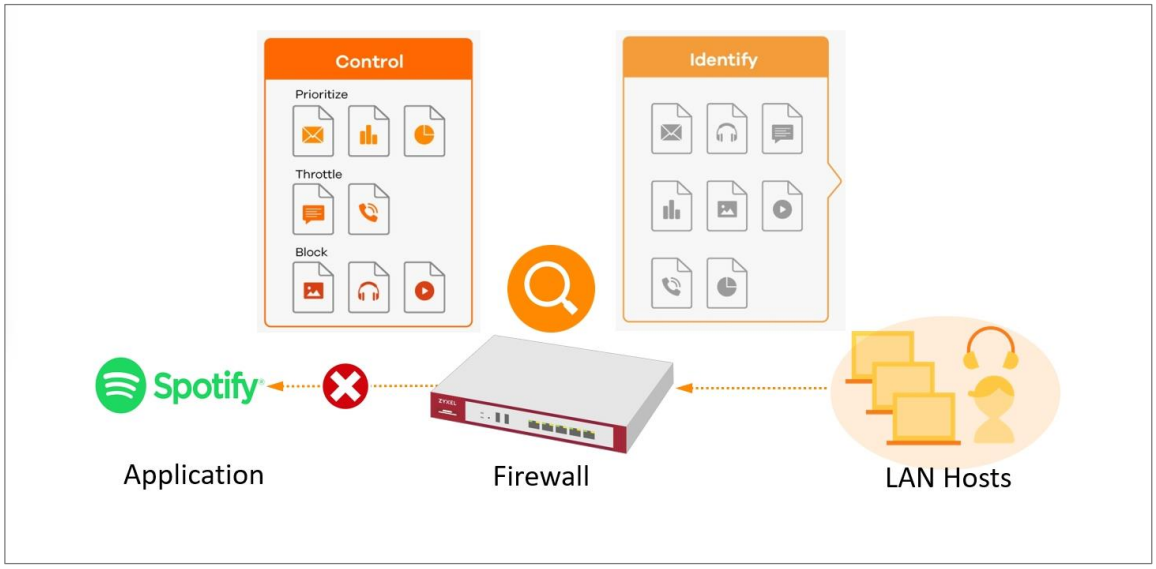
Access to Google drive from Lan host to verify if it is blocked by firewall Application patrol.

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

# 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).

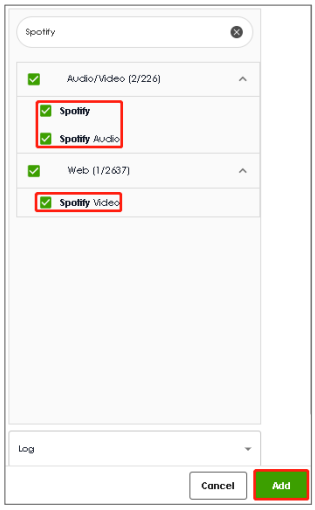
 

## Create a App Patrol profile

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.

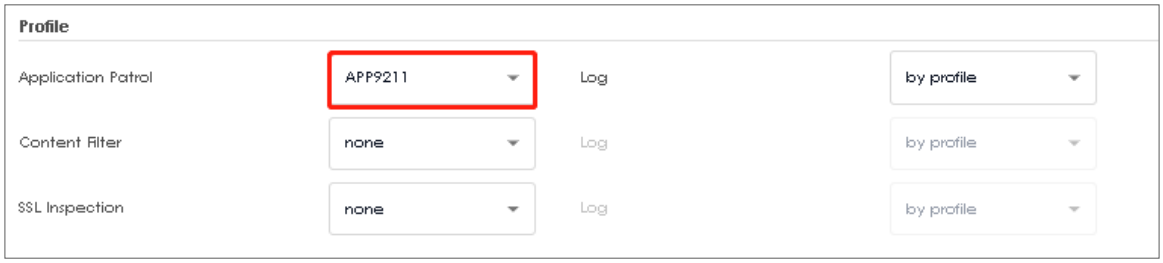


## Apply profile to security policy

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

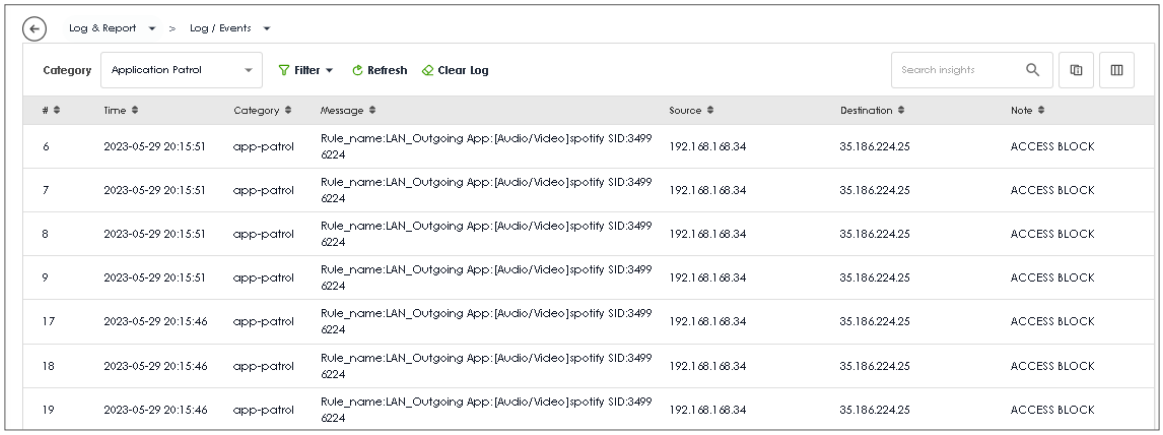
Apply Application Patrol profile to Security policy.




## Test the Result

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

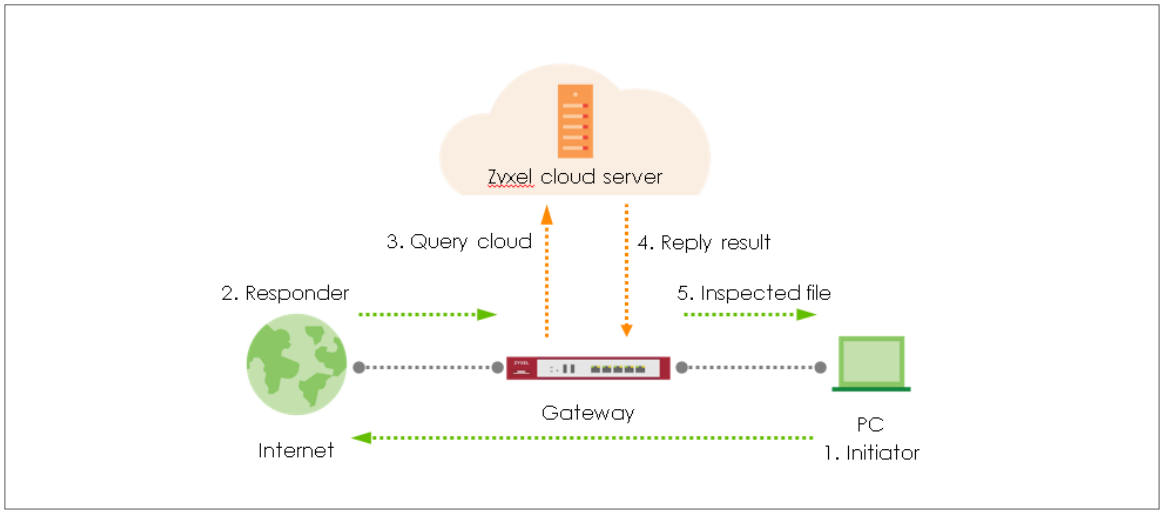
Go to Log & Report > Log/Events and select Application Patrol to check the logs.



## How does Anti-Malware Work

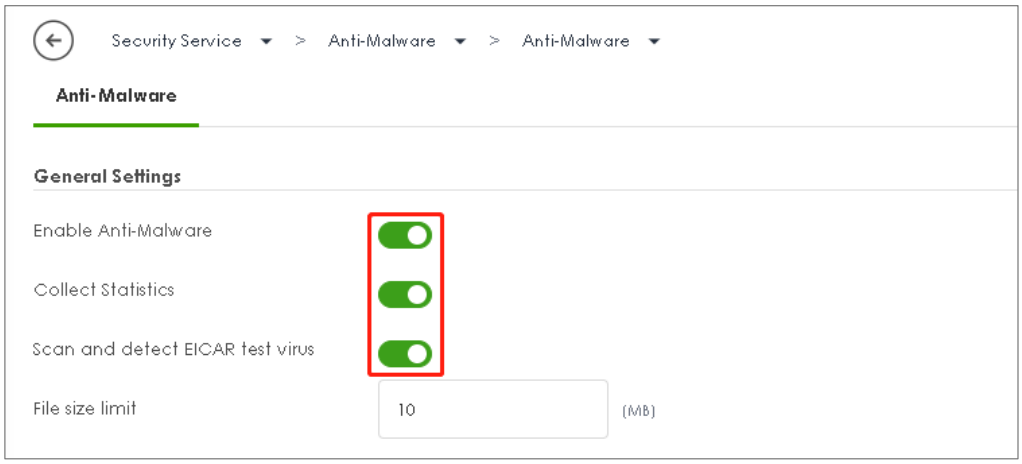
There are many viruses exist on the internet. And it may auto-downloaded on unexpected situation when you surfing between websites. The Anti-Malware is a good choose to protecting your computer to downloads unsafe application or files.



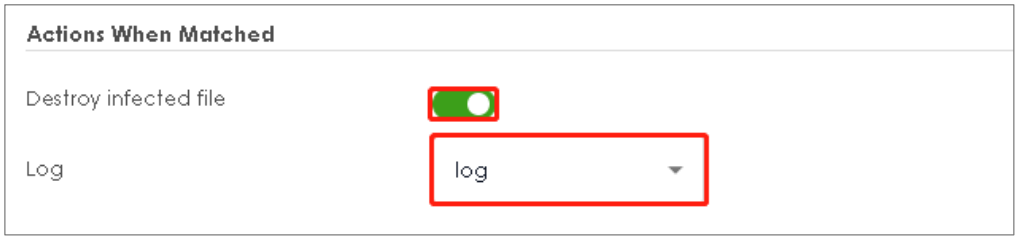

 

## Enable Anti-Malware function to protecting your traffic

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




Select Destroy infected file and log in Actions When Matched

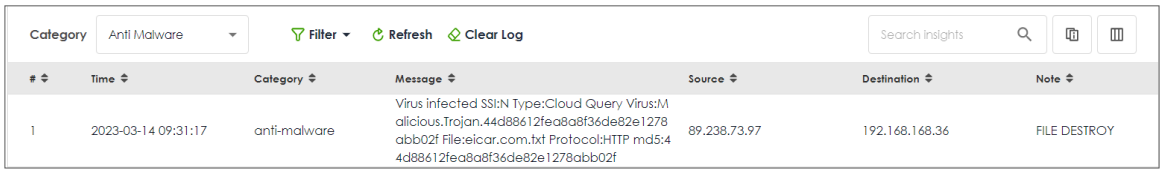


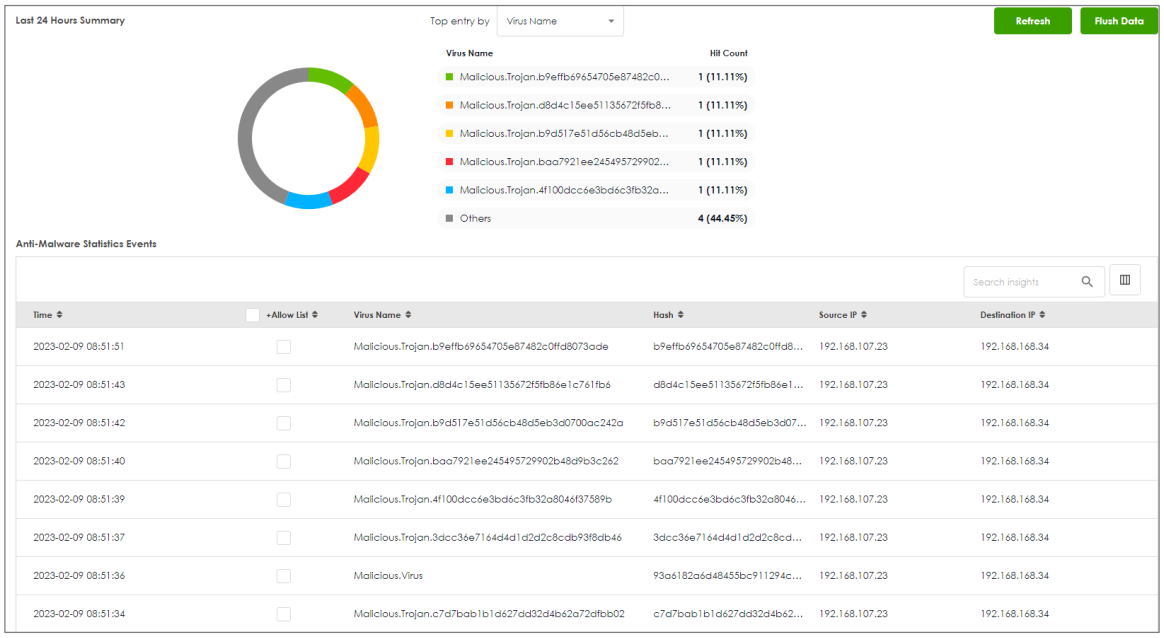
## Test the Result

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

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



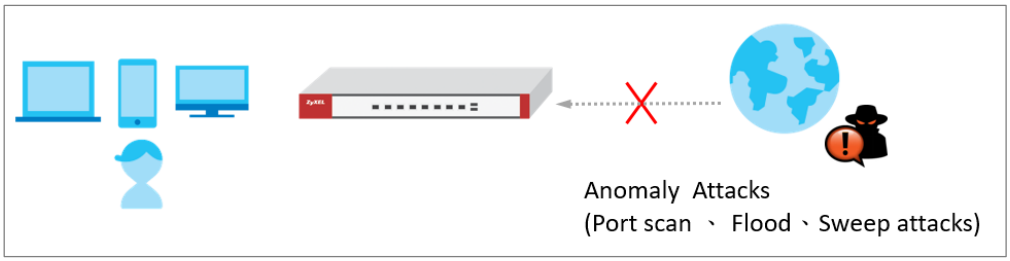

Go to Security Statistics > Anti-Malware to check summary of all events.



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

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

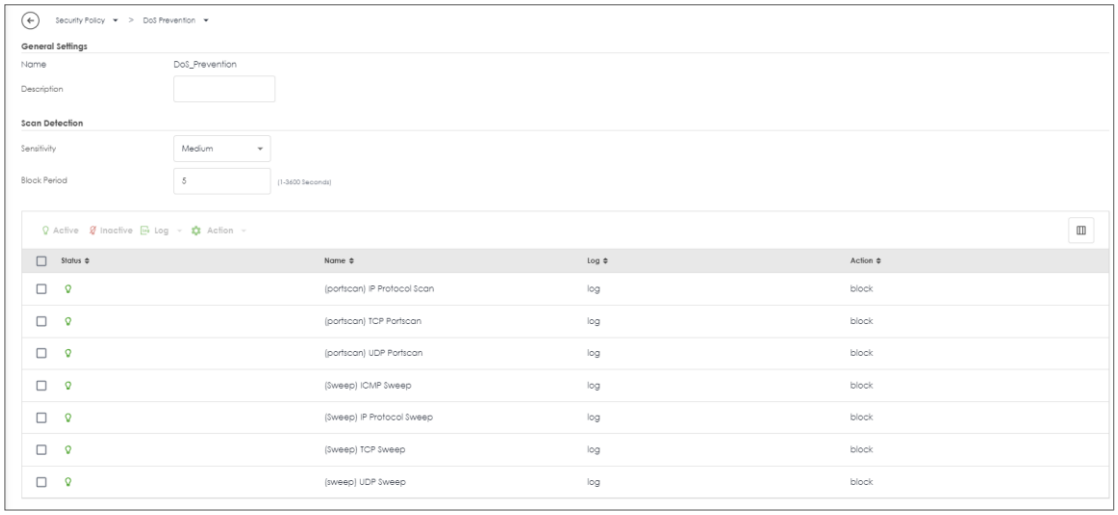


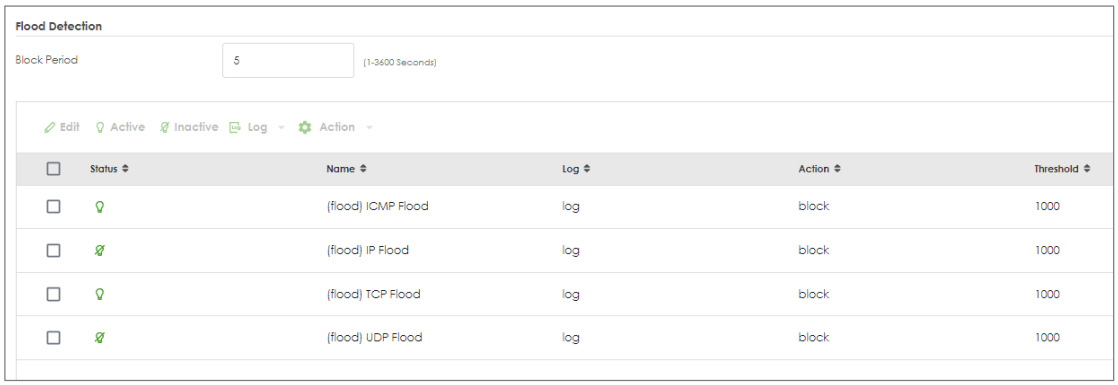

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

## Set Up the DoS Prevention

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



## 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.

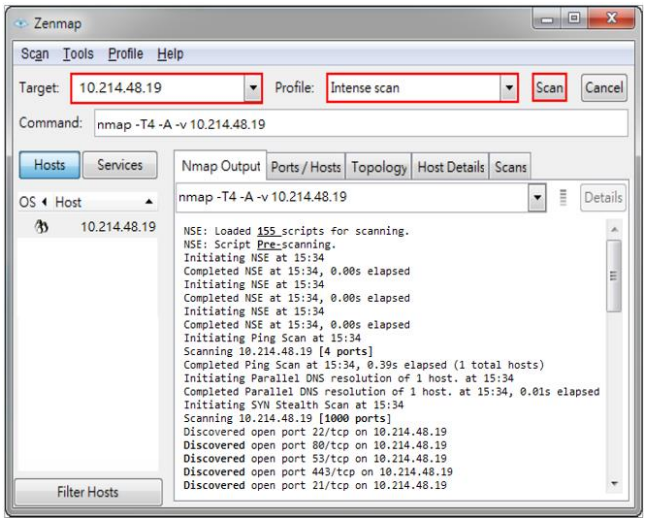

 

## Test the Result

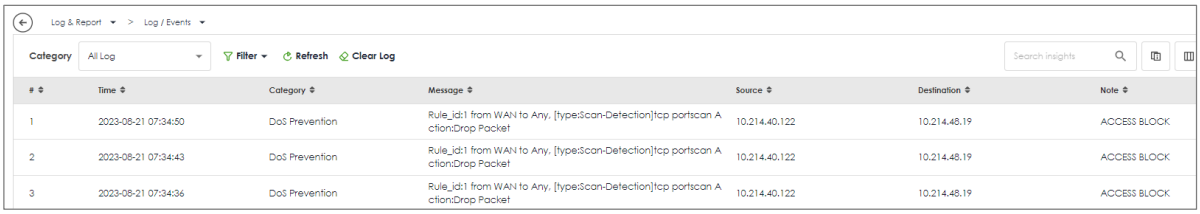
Using the port scan tool Nmap or hping3 to scan the wan interface.

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.

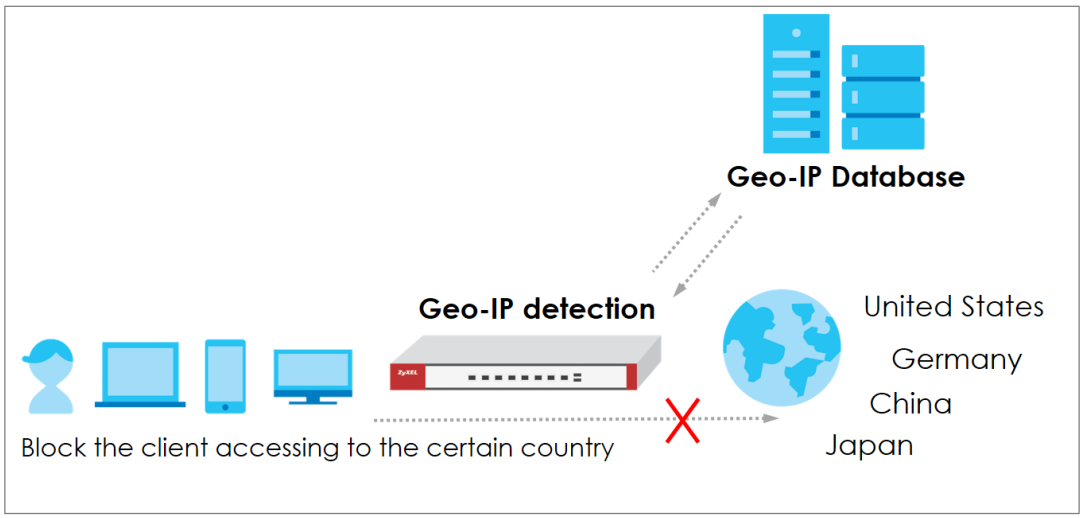


# How to block the client from accessing to certain country using Geo IP?

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

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

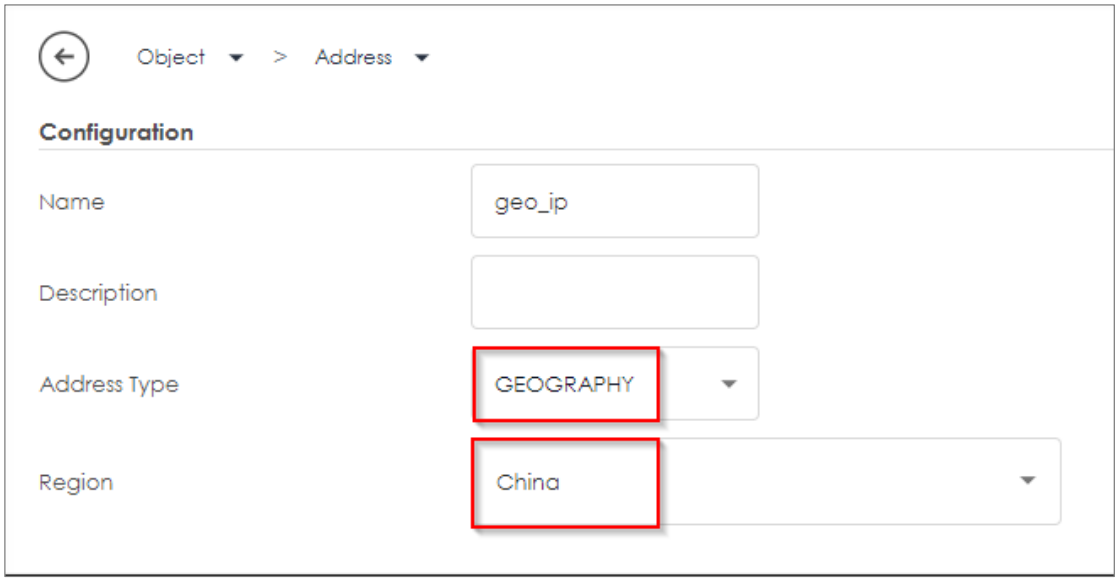


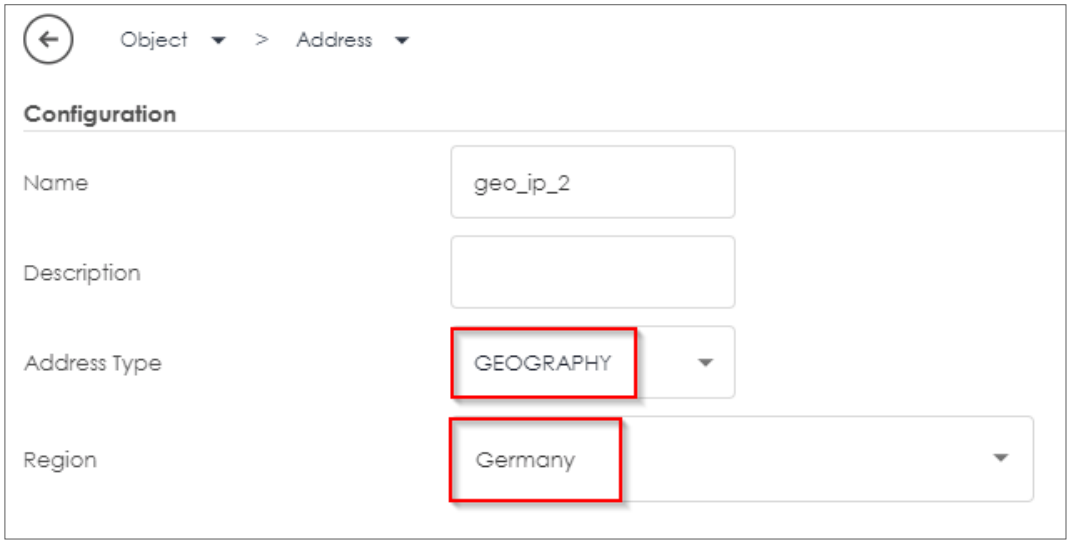

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG Flex 500H (Firmware Version: uOS 1.10)

## Set Up the Address Objet with Geo IP

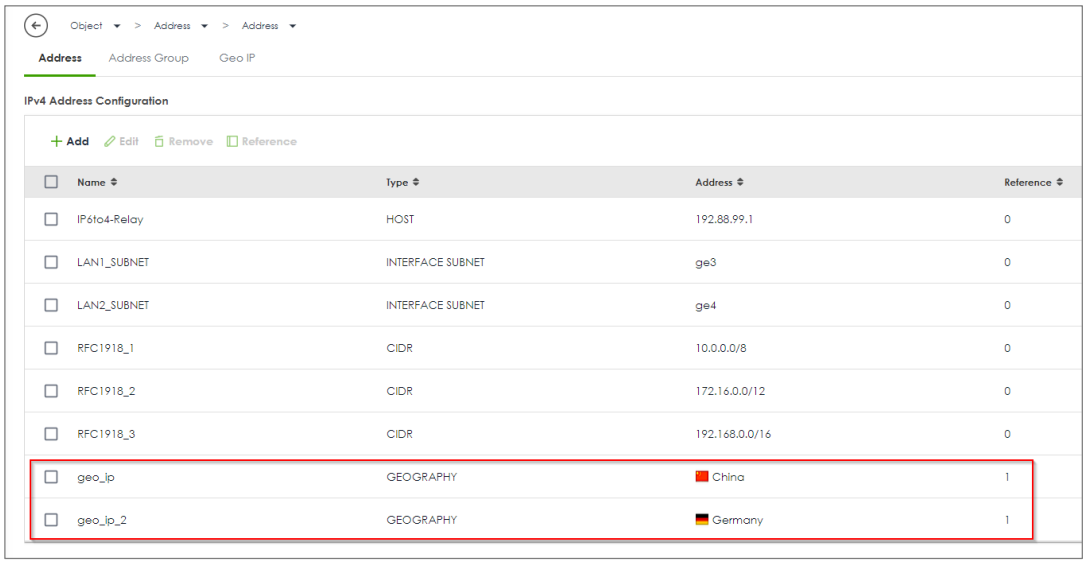
Navigate to **Object > Address > Geo IP > Add geo IP related objects.**



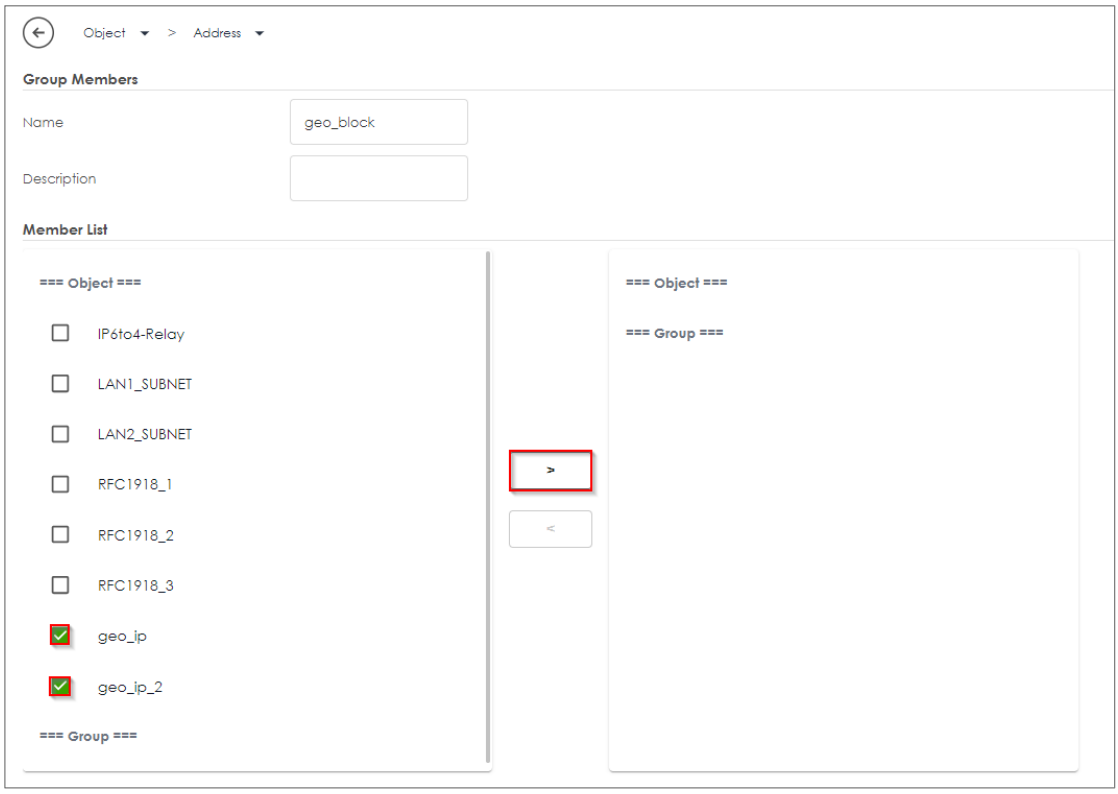



Navigate to **Object > Address > Address**, you can see the customized GEOGRAPHY address object.



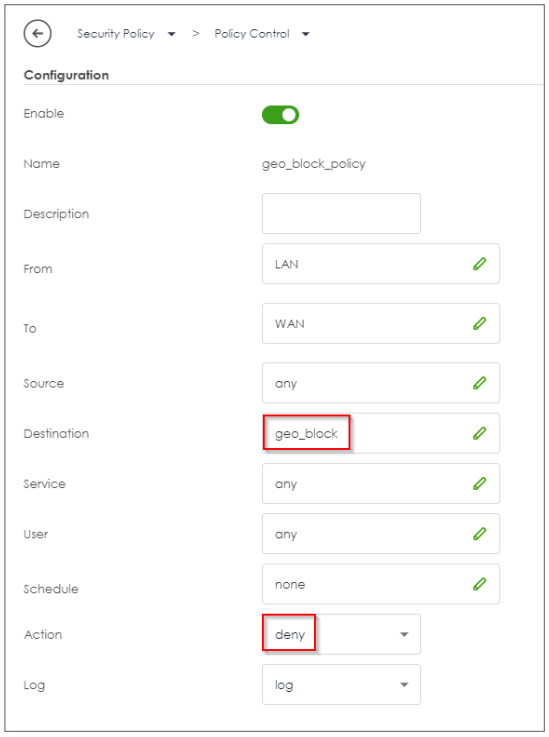

Go to **Object > Address > Address Group> Add Address Group Rule**, add all customized GEOGRAPHY addresses into the same **Member** object.



## Set Up the Security Policy

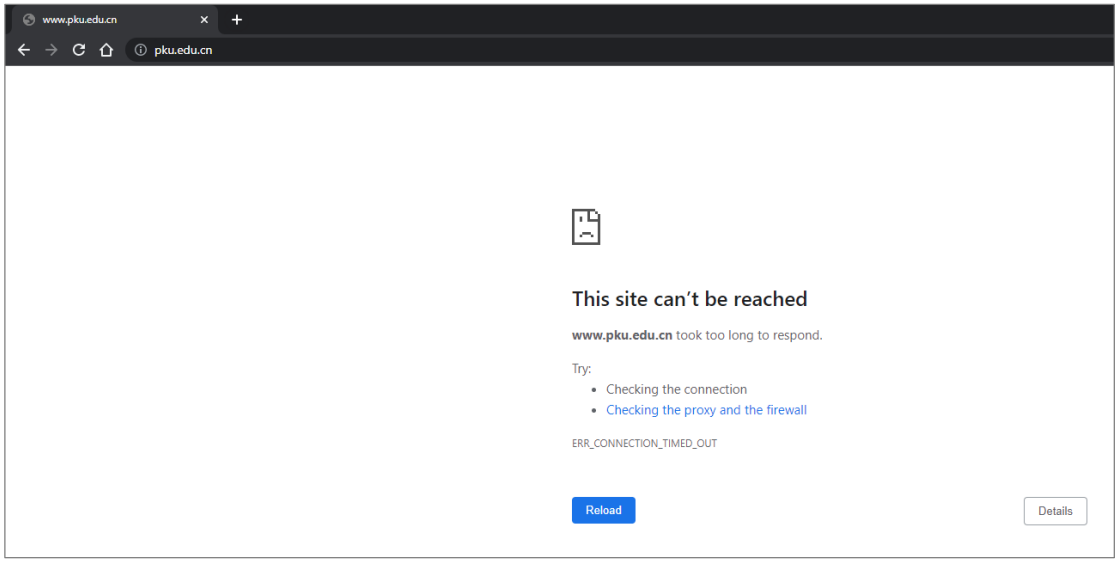
Go to **Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Set deny Geo IP traffic from LAN to WAN (geo_block_policy in this example).



## Test the Result

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



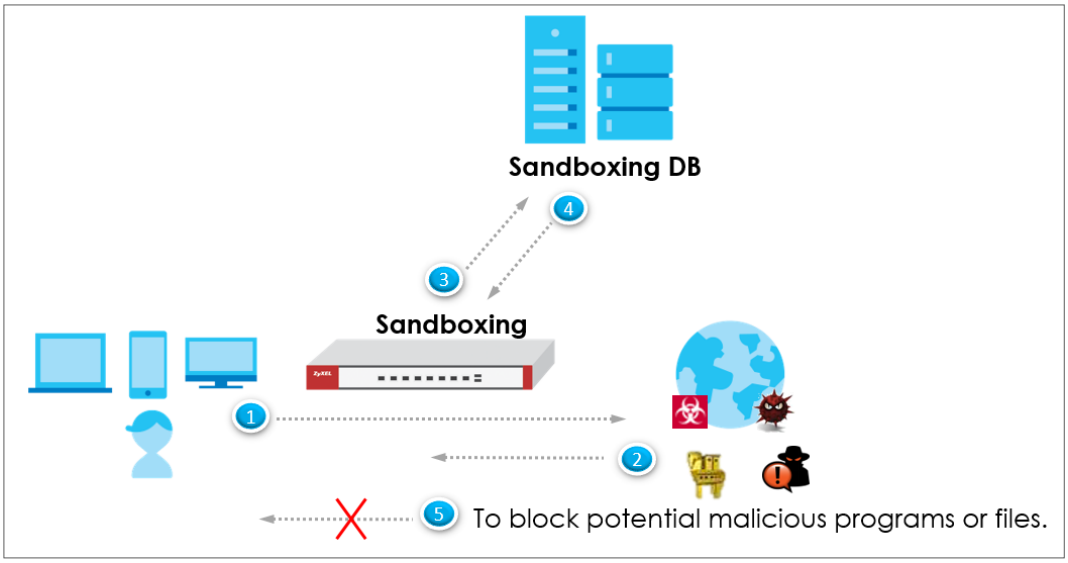

To view the log message, go to USG Flex H **Log & Report > Log / Events**. You will find log messages similar to the following. Any traffic that matches the Geo IP policy will be blocked, and the details will be displayed in the Message field.

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

# How to Use Sandbox to Detect Unknown Malware?

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

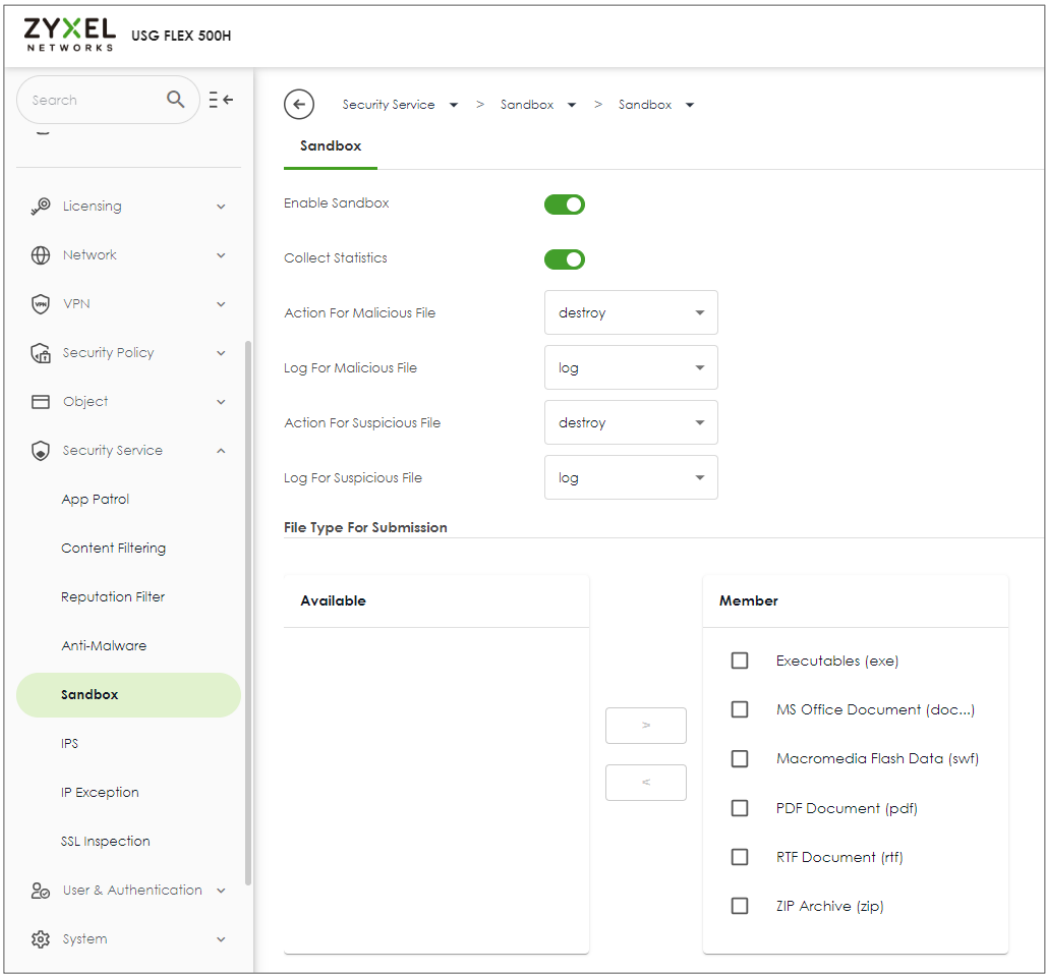



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

## Set Up the Sandbox

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



## Test the Result

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

# 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.

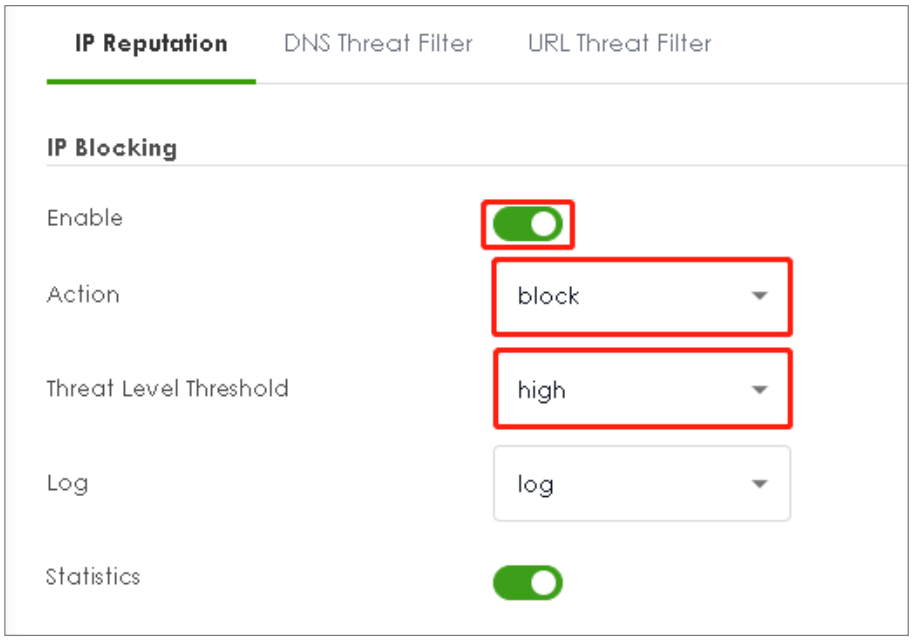
This example illustrates how to configure IP Reputation on FLEX gateway to detect cyber threats for both incoming and outgoing traffic.

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).

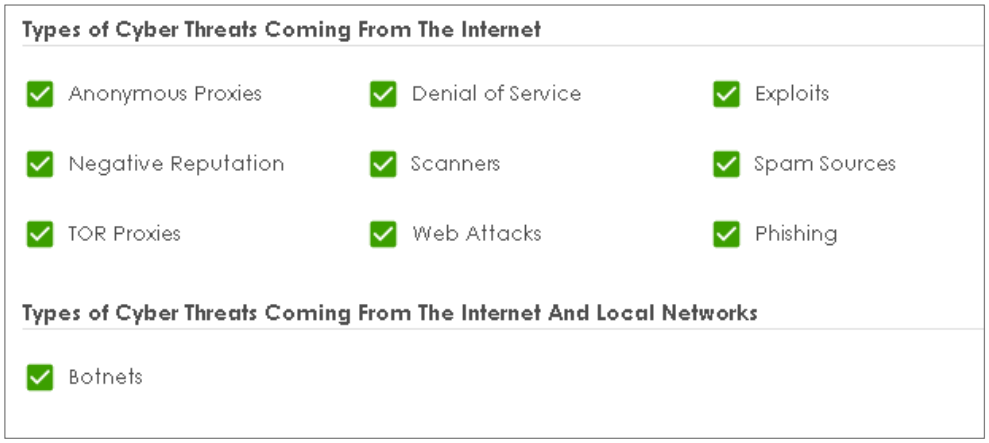
 

## Set Up the IP reputation filter

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.

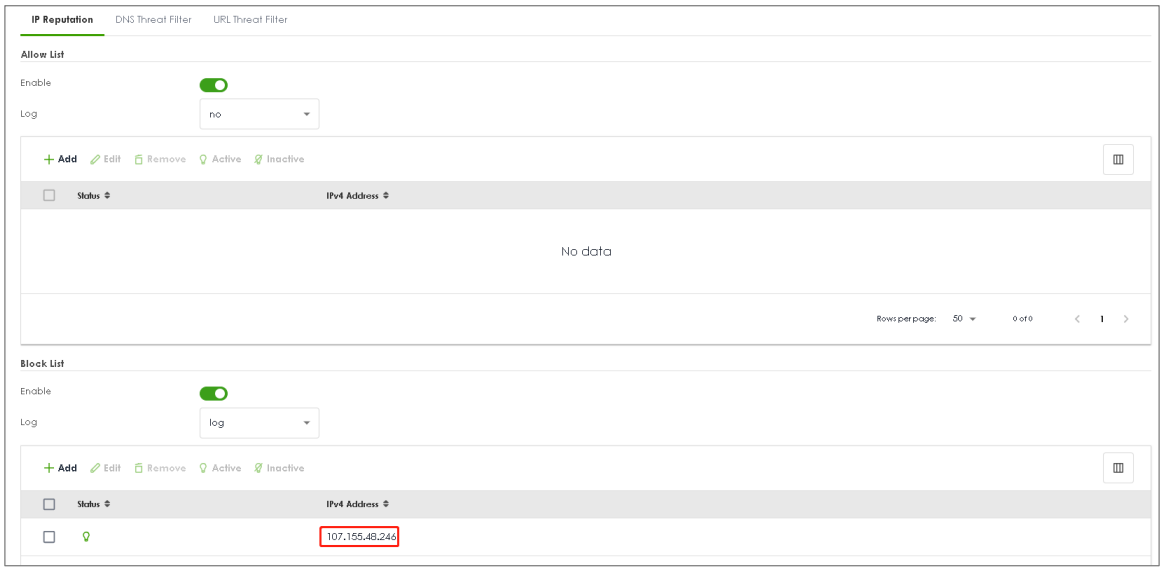



Select categories in Types of Cyber Threats Coming from the Internet, and Types of Cyber Threats Coming from The Internet and Local Networks.



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



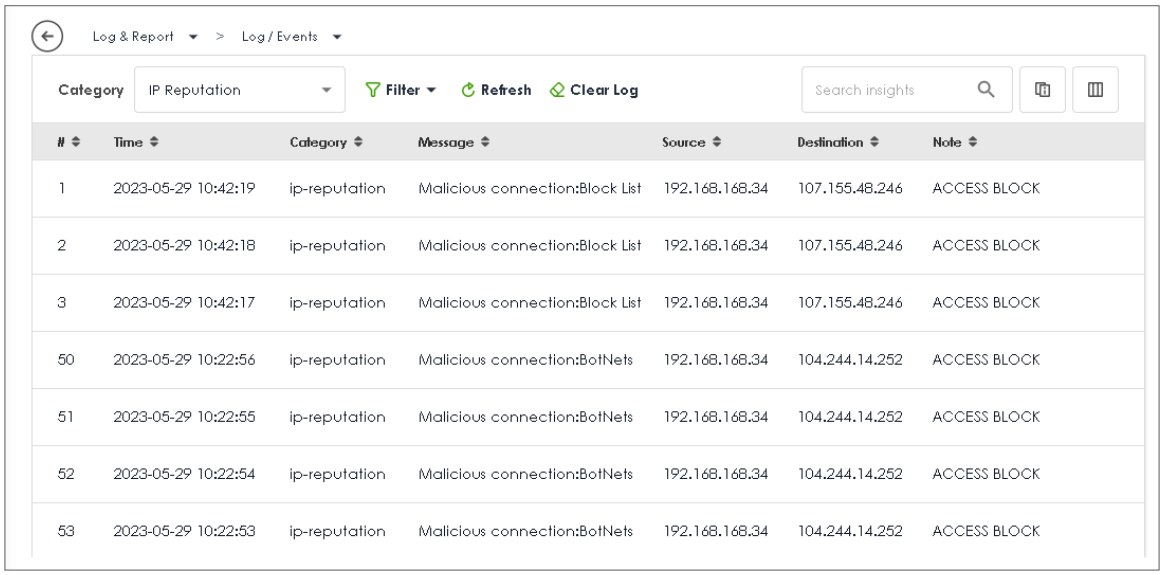
## Test the Result

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



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

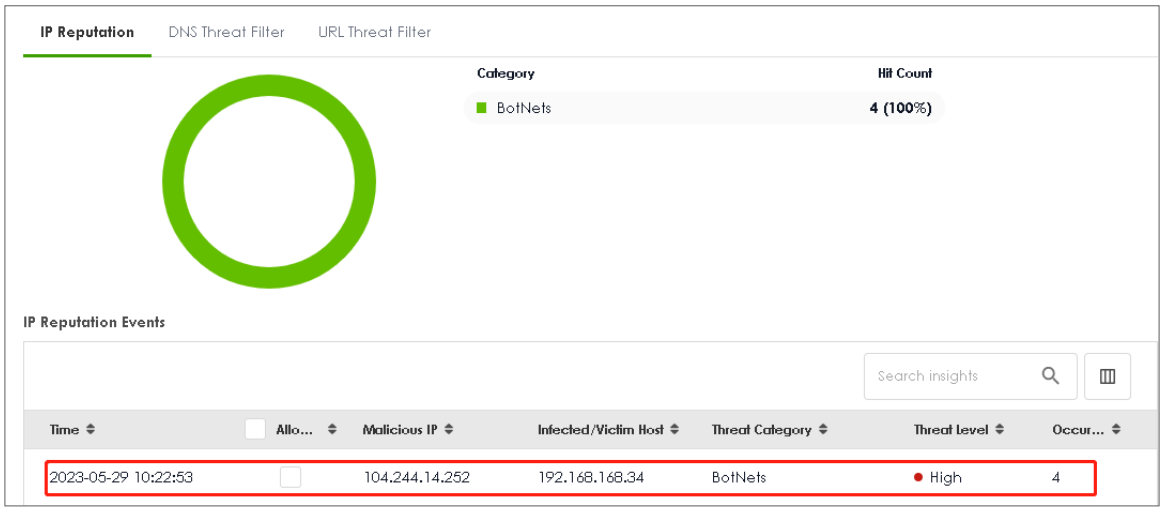
Go to Log & Report > Log/Events and select IP reputation Filter to check the logs.




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

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



# How to Configure Reputation Filter- URL Threat Filter

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

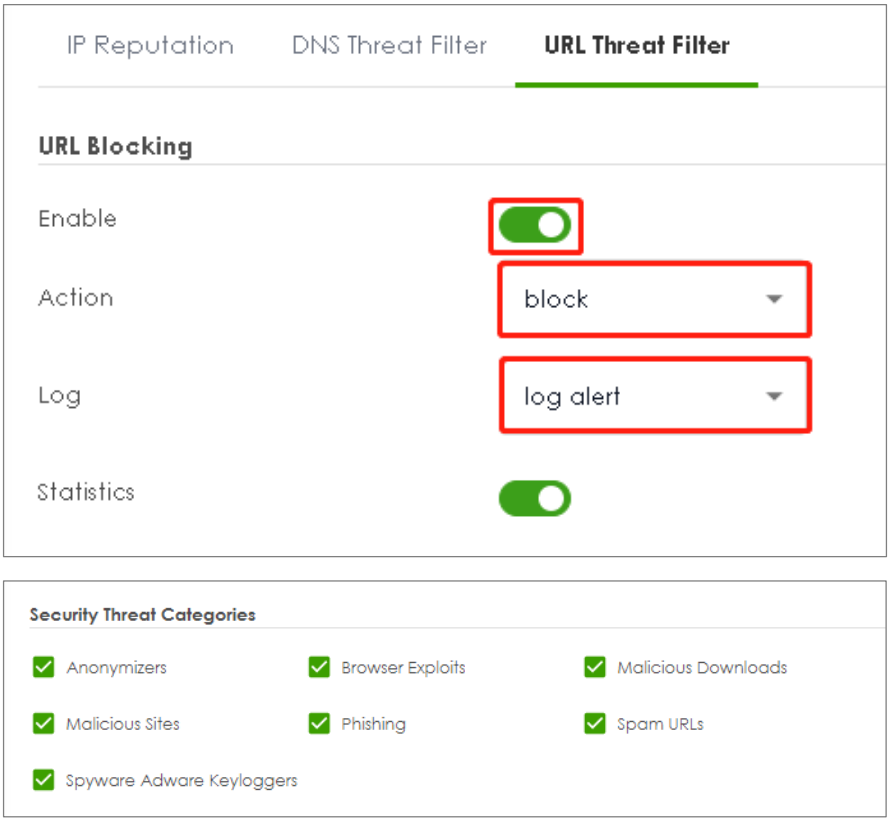
This example demonstrates how to configure the URL Threat Filter to redirect web access after the client hits the URL Threat Filter categories.

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

## Set Up the URL Threat Filter

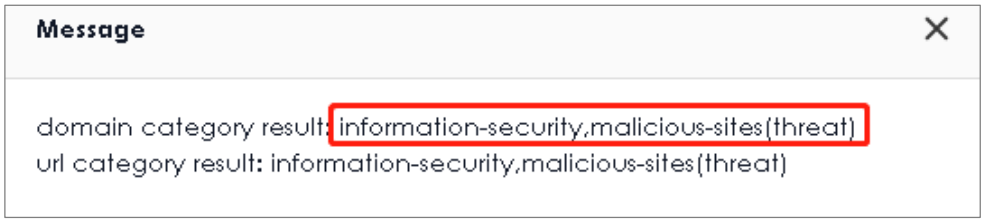
Go to Security Service > Reputation Filter > URL Threat Filter. Turn on this feature. Select Block on Action field. When a client hits URL Threat Filter, the page will be Blocked. Choose Log-alert on Log field.



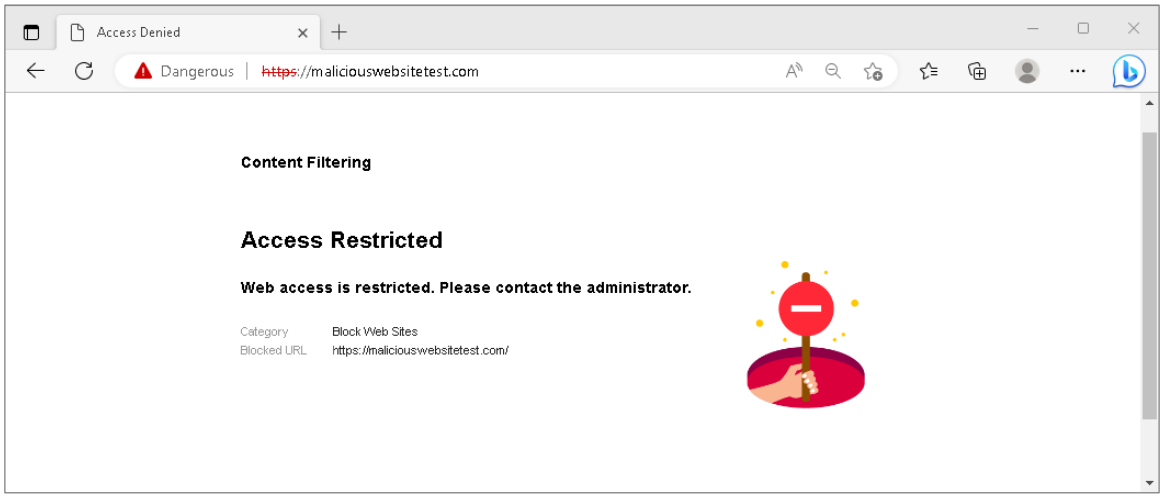

 

## Test the Result

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

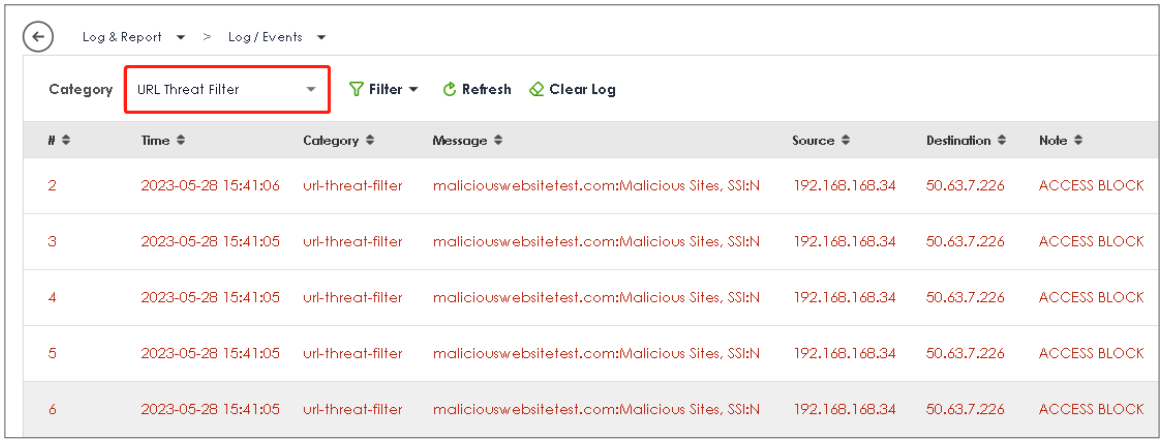




Using Web Browser to access the malicious site. The gateway will redirect you to a blocked page.

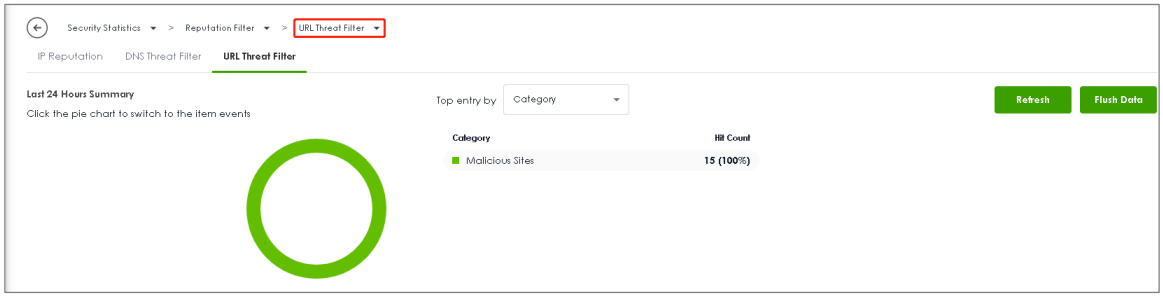


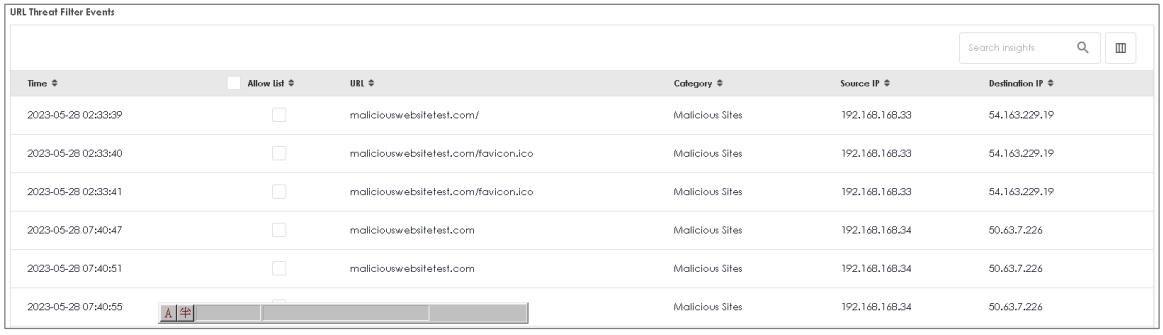

 

Go to Log & Report > Log/Events and select URL Threat Filter to check the logs.




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



# 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.

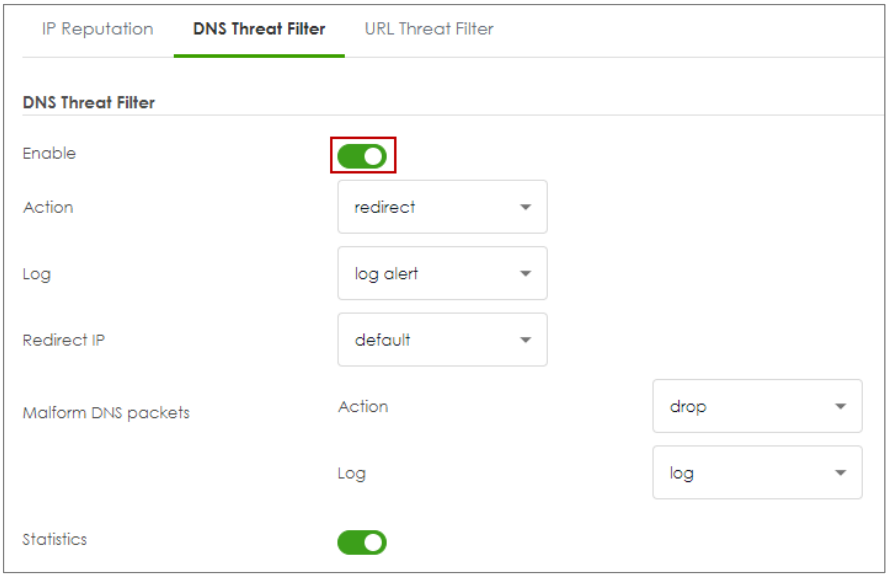
When a client wants to access a malicious domain, the query is sent to the DNS server for getting the domain name details. All of the traffic now here gateway intercepts this query which is outgoing. The cloud server identifies that this is bad site. What gateway can do here is send the redirect IP address 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.

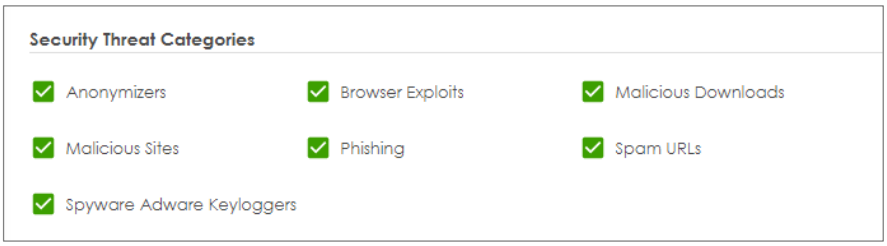
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

## 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.



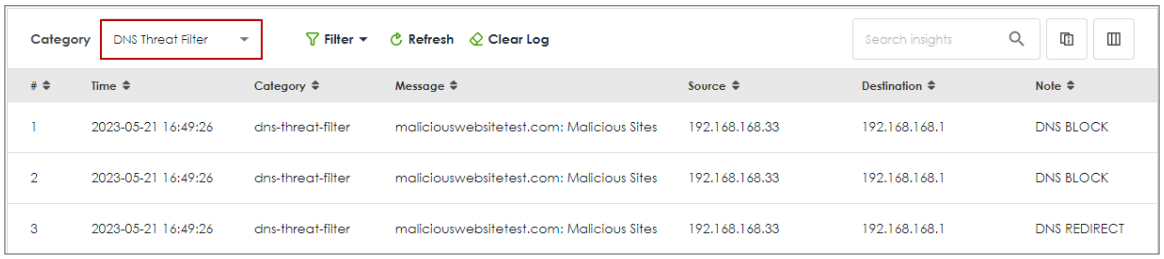
## Test the Result

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



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.



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

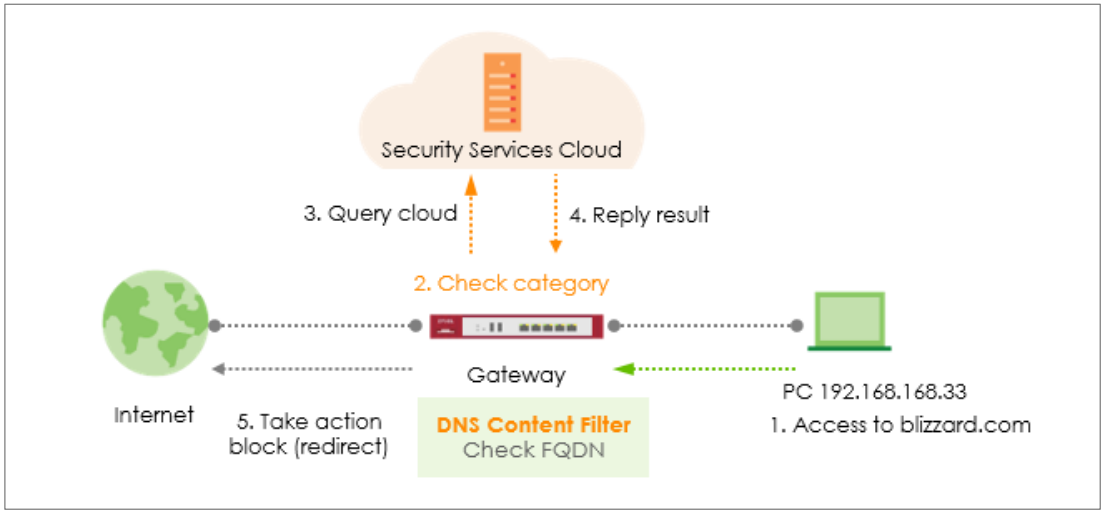


# How to Configure DNS Content Filter

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.

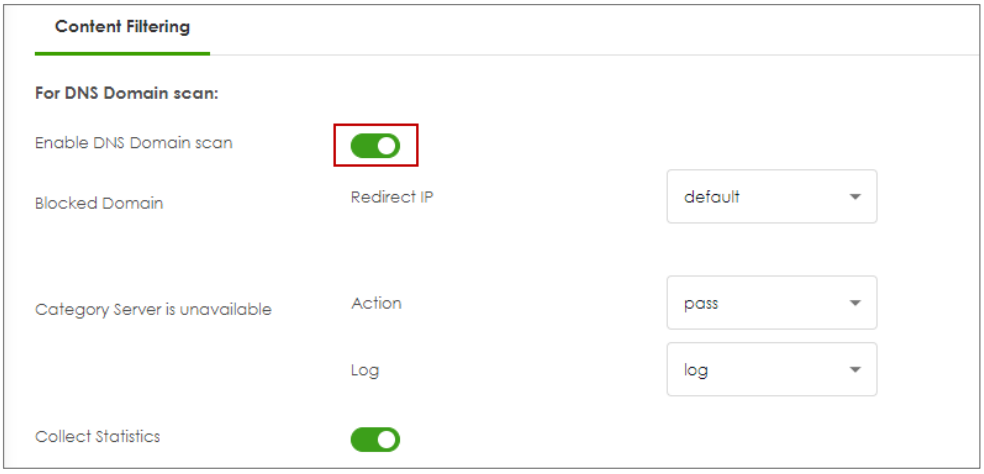



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

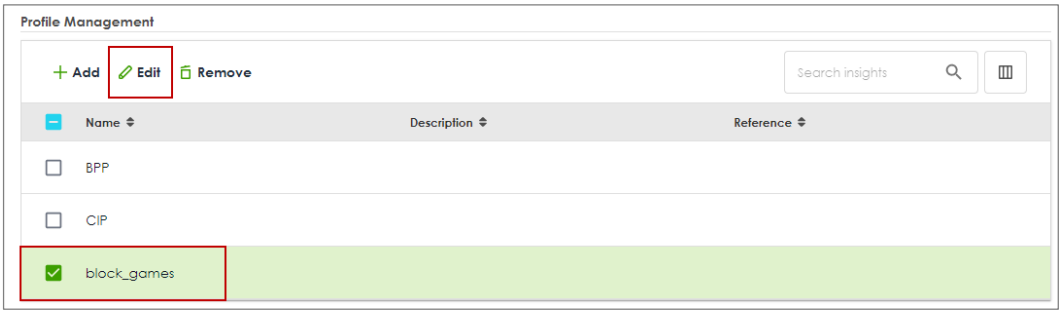
 

## Set Up the DNS Content Filter

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/.



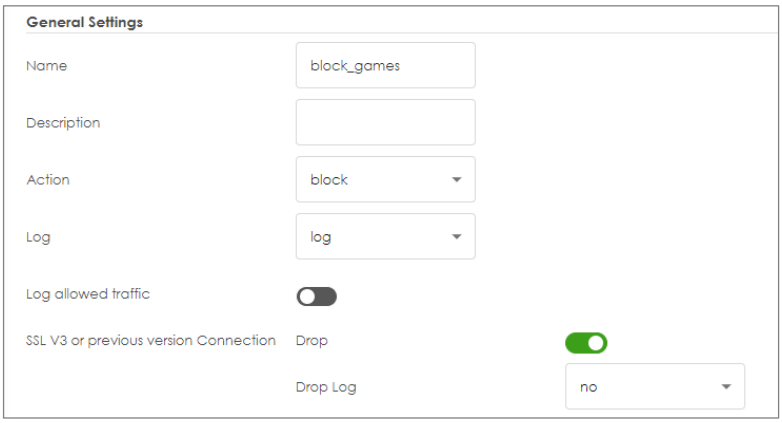

Add a new profile in Profile Management to block gaming websites.



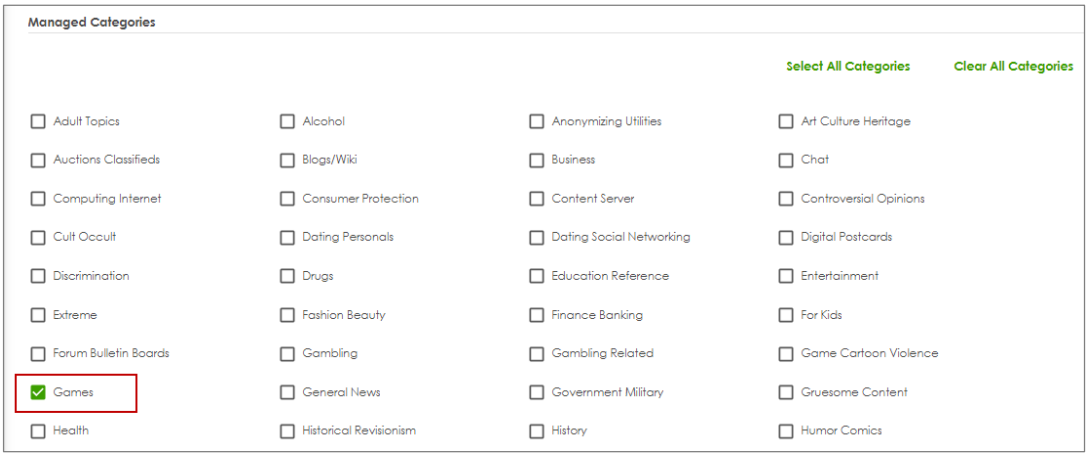

 

Action: block

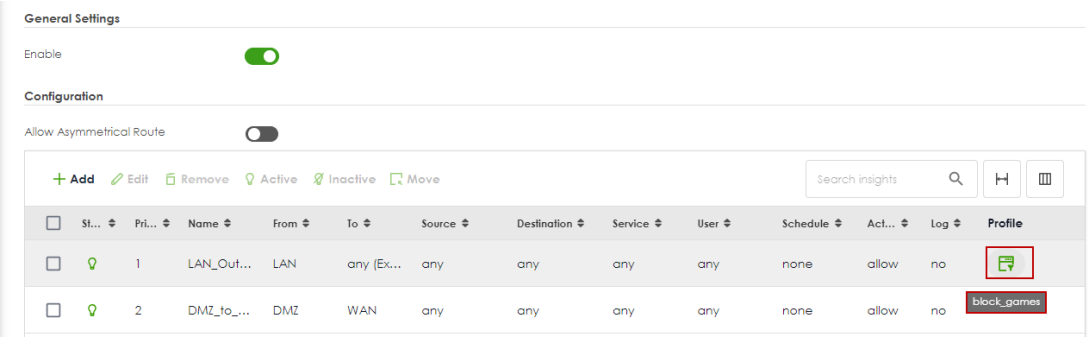
Log: log or log alert




Enable the checkbox of "Games" in managed categories.




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

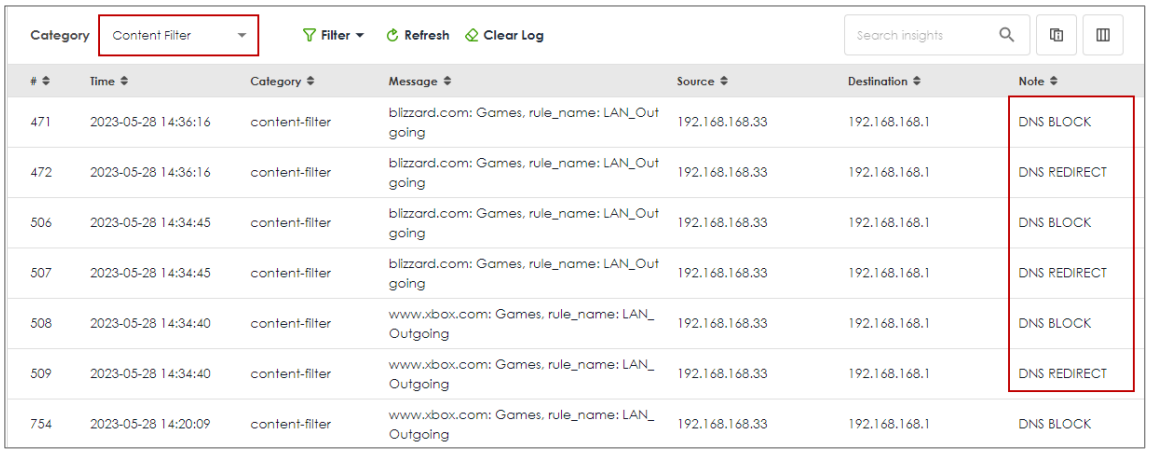


## Test the Result

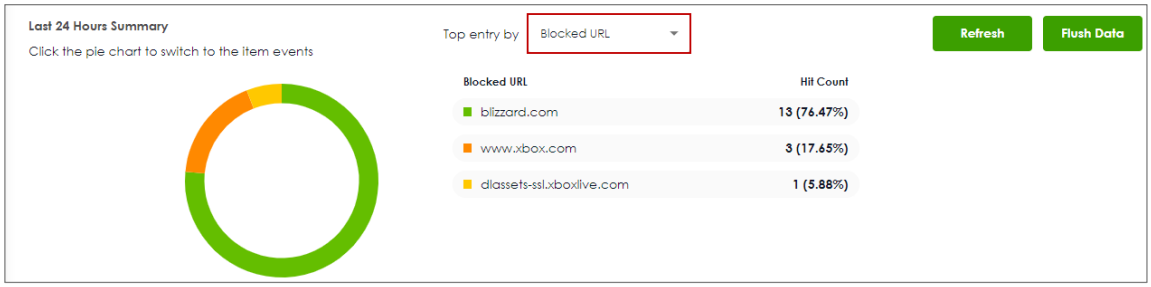
Access a gaming website blizzard.com. The gateway will redirect you to a blocked page.


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




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

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



Content Filter Events

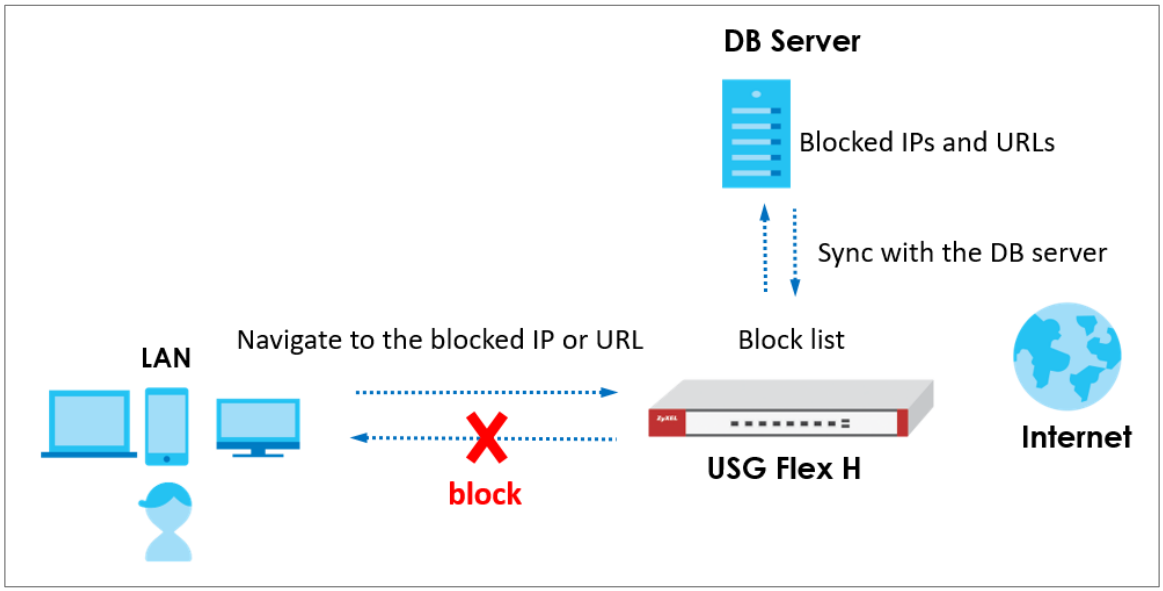
Search insights

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

## External Block List for Reputation Filter

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

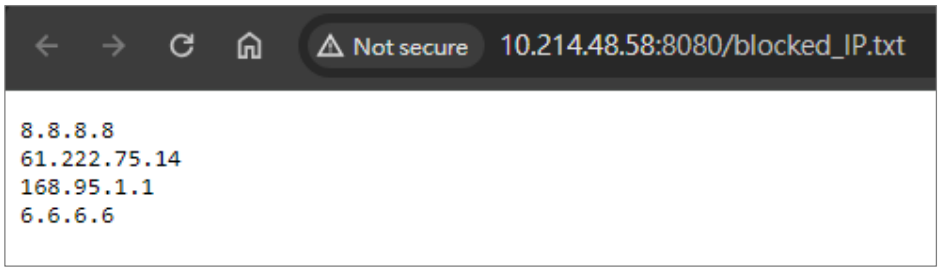



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.20).

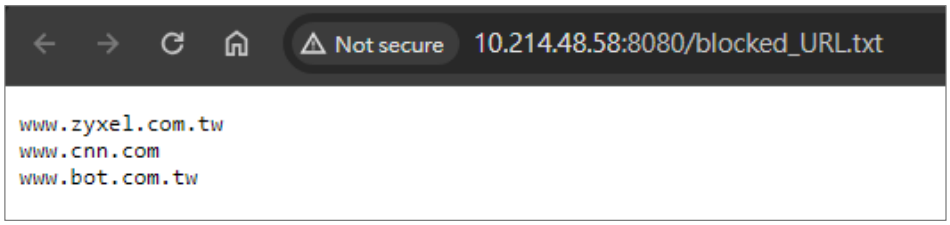
 

## Set Up the DB server

The administrator can set up websites to maintain external block lists. The USG Flex H firewall can update the external block list via a URL. For example,
http://10.214.48.58:8080/blocked_IP.txt



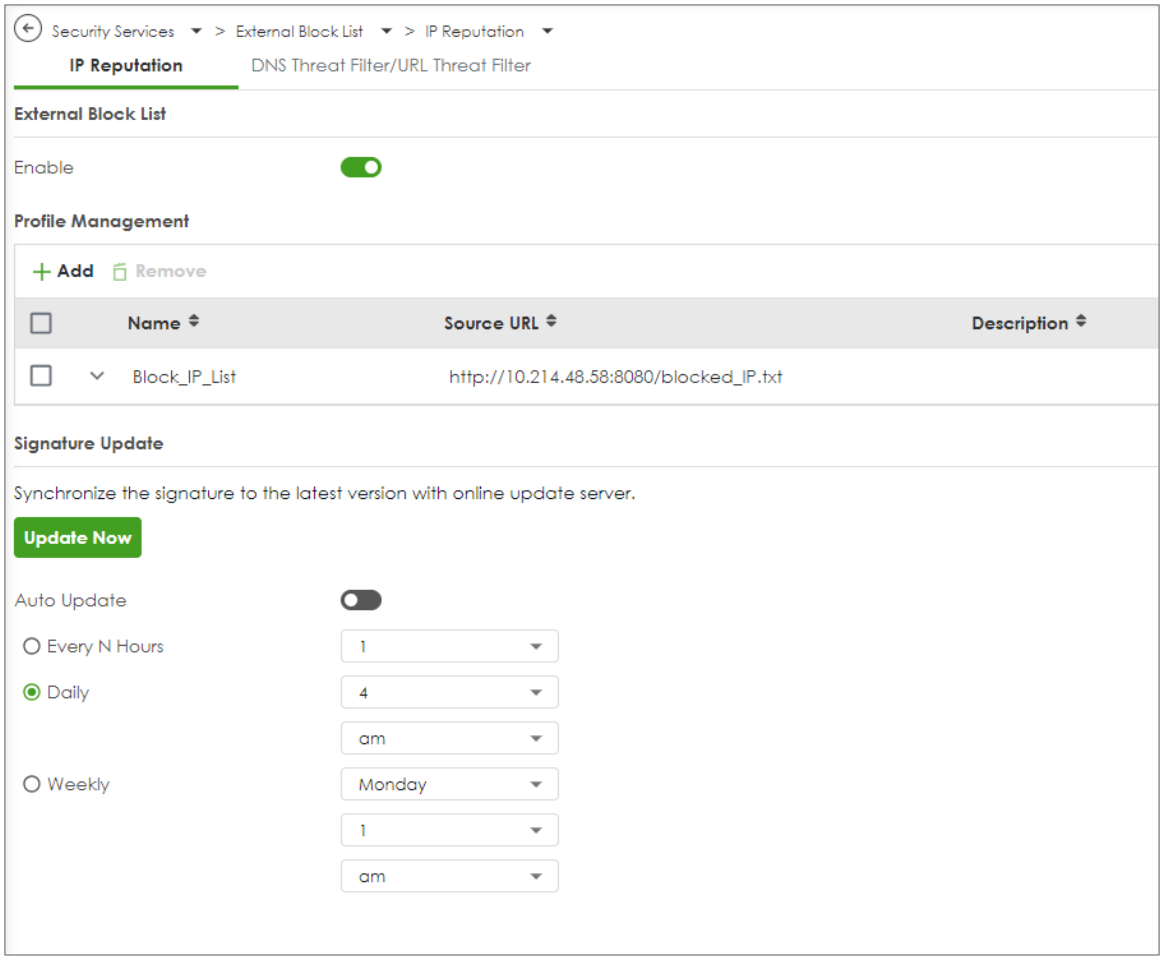

http://10.214.48.58:8080/blocked_URL.txt




## Set Up the External Block List of IP Reputation

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

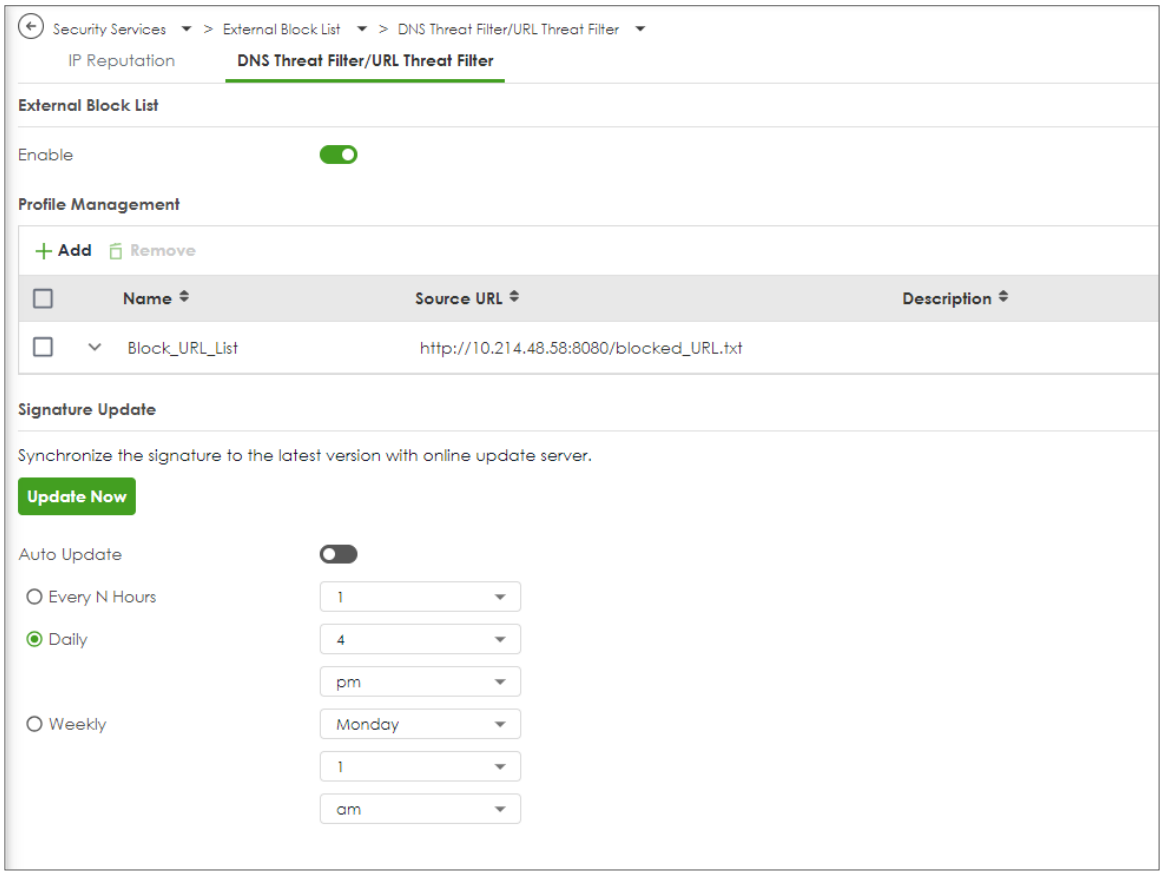



If the IP Reputation external block list is updated successfully and you can observe the corresponding log message.

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

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




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

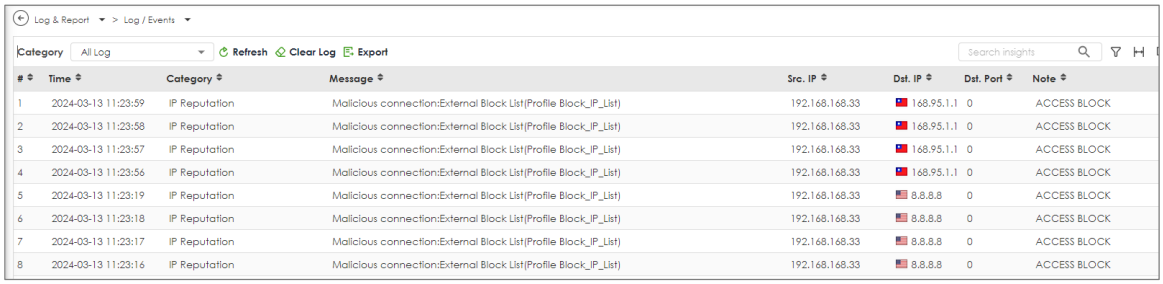

 

## Test the Result

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

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

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

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

C:\Users\[redacted]>ping 168.95.1.1

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

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

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

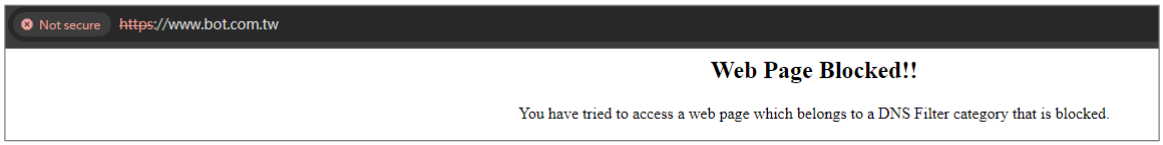


Log & Report > Log / Events

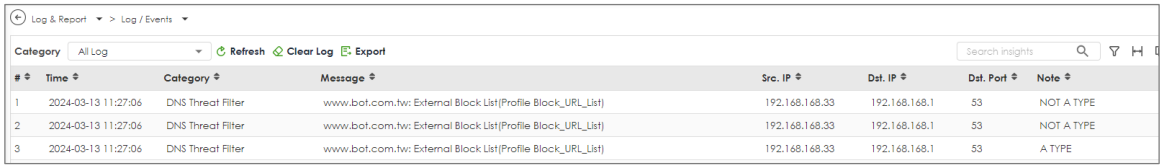
Category: All Log | Refresh | Clear Log | Export | Search insights

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

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




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



Log & Report > Log / Events

Category: All Log | Refresh | Clear Log | Export | Search insights

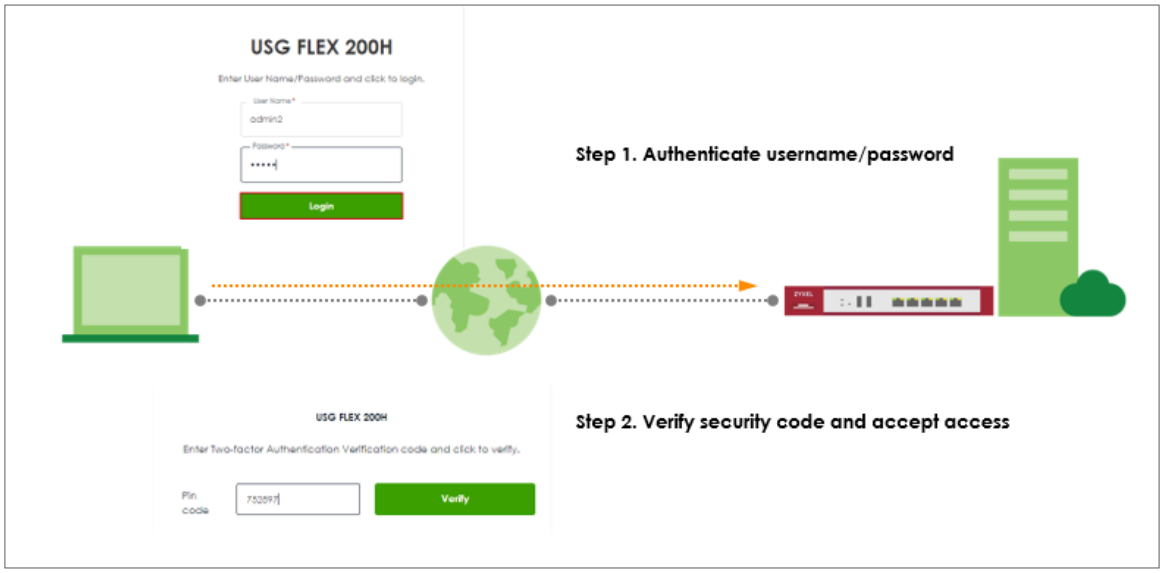
| # | Time | Category | Message | Src. IP | Dst. IP | Dst. Port | Note |
|---|---|---|---|---|---|---|---|
| 1 | 2024-03-13 11:27:06 | DNS Threat Filter | www.bot.com.tw: External Block List(Profile Block_URL_List) | 192.168.168.33 | 192.168.168.1 | 53 | NOT A TYPE |
| 2 | 2024-03-13 11:27:06 | DNS Threat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

# Chapter 3- Authentication

## How to Use Two Factor with Google Authenticator for Admin Access

Google authenticator is the most secure method to receive verification code for 2-factor authentication. Google authenticator gives a new code every 30 seconds, so each code expires in just 30 seconds which make it a secure option to generate codes for 2-step verification. Furthermore, Google authenticator is free to download, easy to use, and is able to work without Internet. This example illustrates how to set up two factor with Google Authenticator for admin access.




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

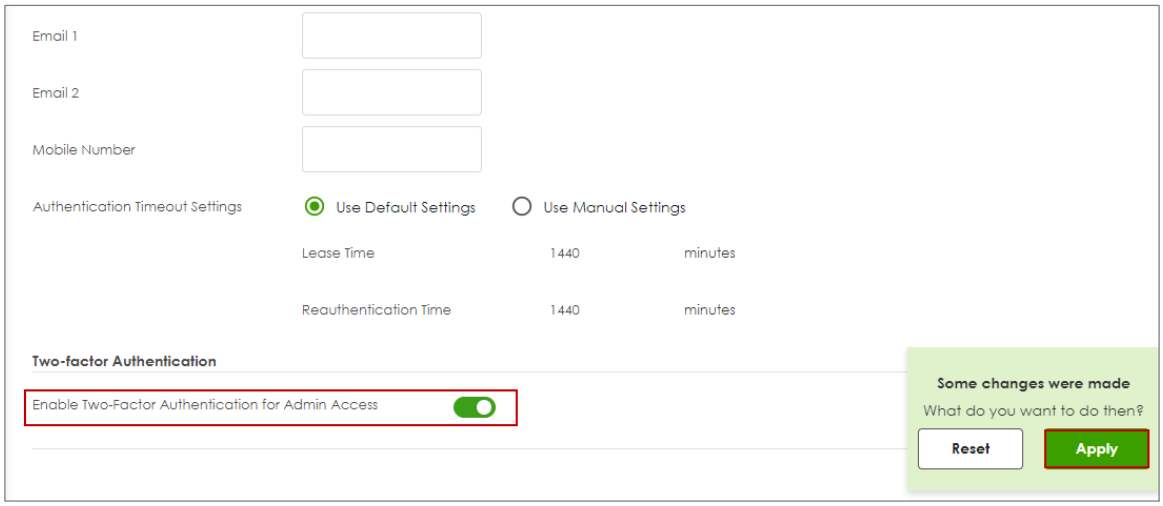
 

## Two Factor with Google Authenticator Flow

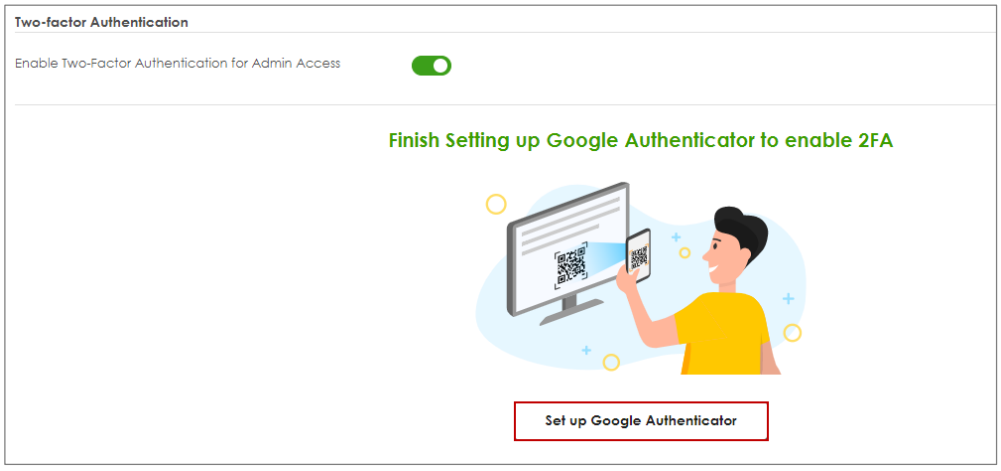
1. Enable Google Authentication on specific admin user.
2. Set up Google Authenticator.
3. Configure valid time and login service types.

## Enable Google Authentication on specific admin user

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

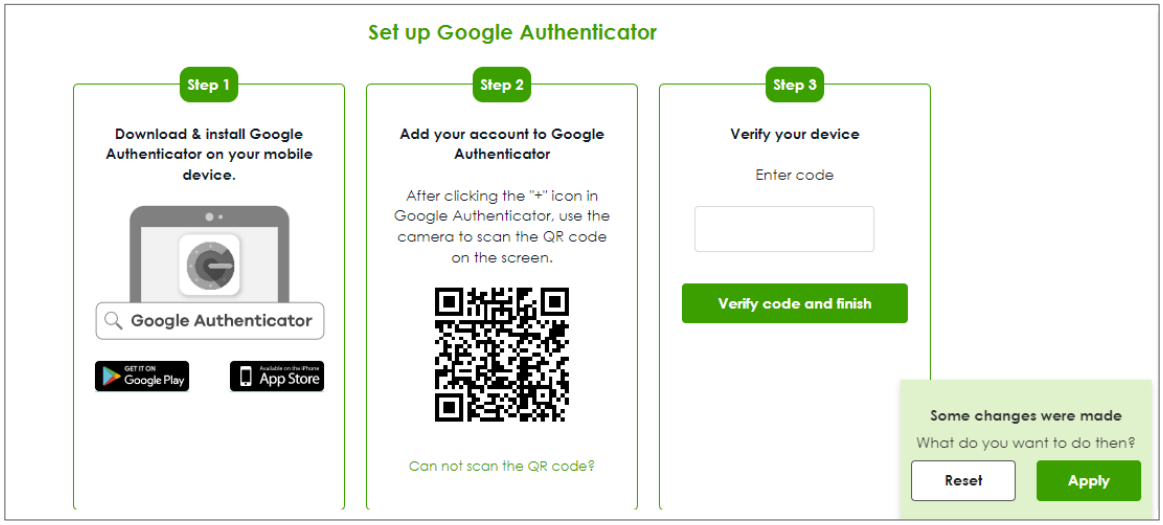



Click "Set up Google Authenticator" to start setting up Google Authenticator on your mobile phone.



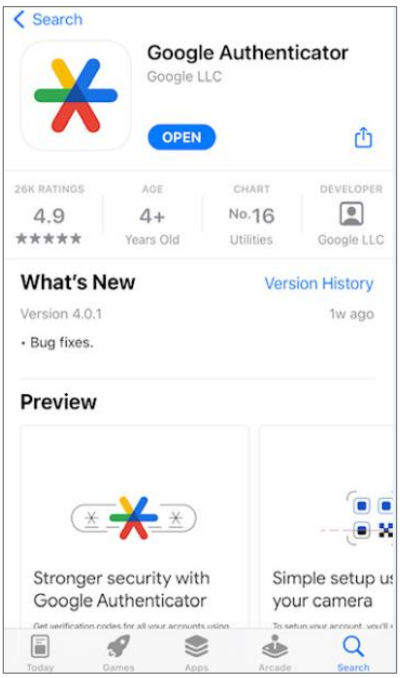

 

# Set up Google Authenticator

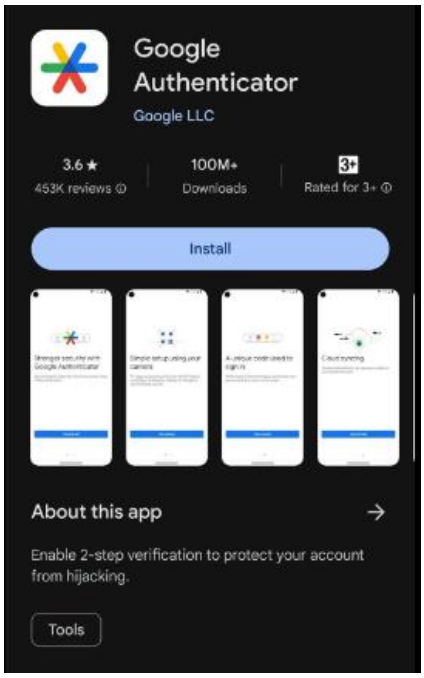



1. Download and install Google Authenticator on your mobile device.

**Apple Store**

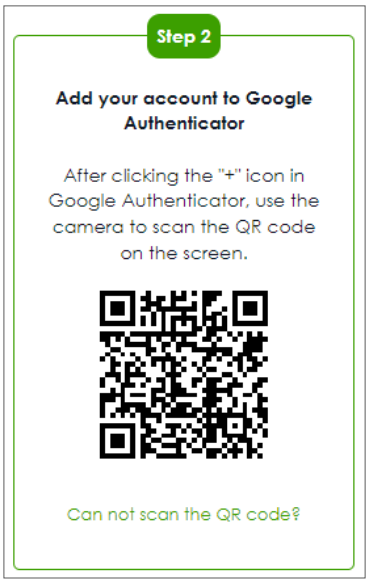


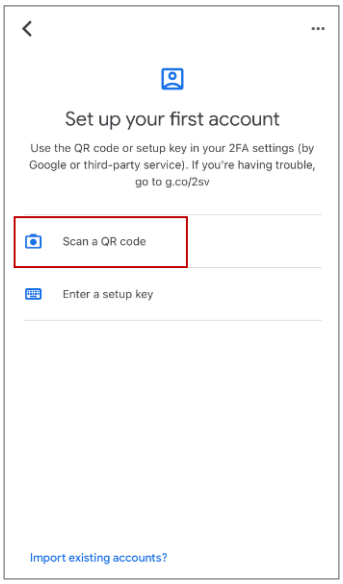

**Google Play**



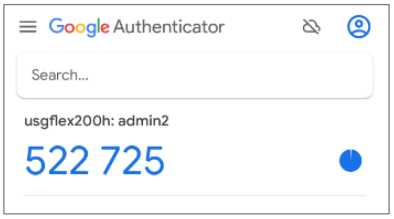

 

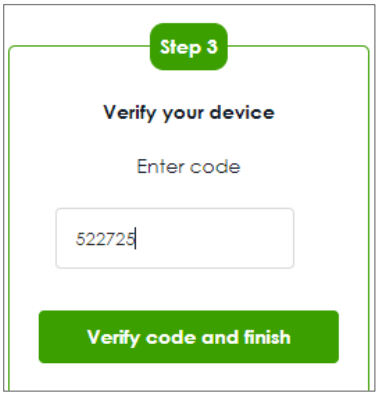
2. Register the admin account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.



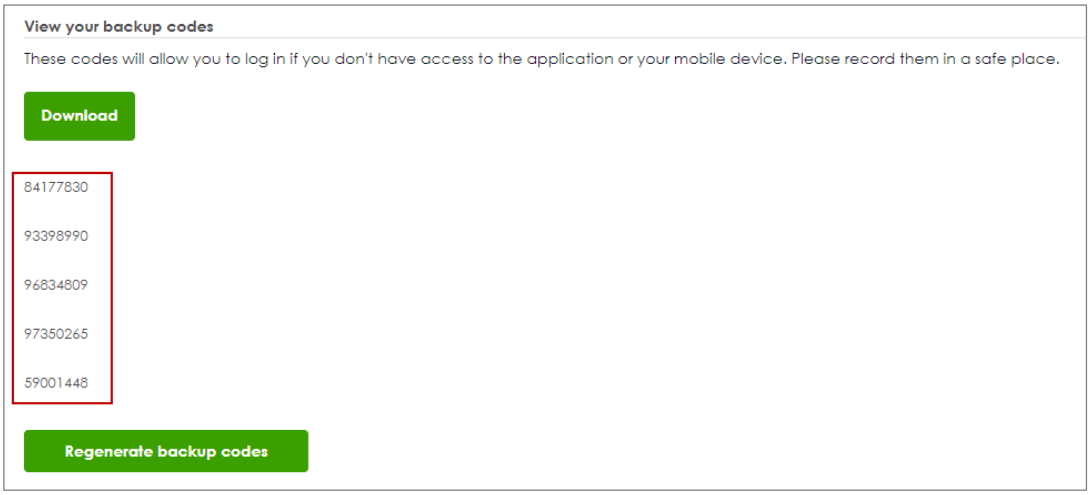

3. Enter the token code which displays on Google Authenticator to "Step 3" and click "Verify code and finish" to submit and verify the code.



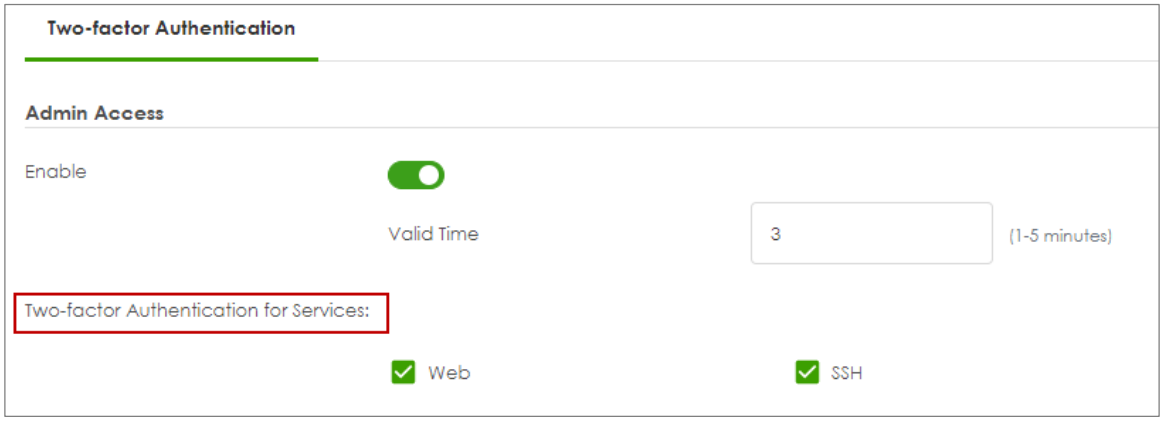

 

4. After 2FA registration is set up successfully, there are backup codes on web GUI. The backup codes are for device login in the case you don't have access to the application on your mobile device. Download the backup codes and record them in a safe place.




## Configure valid time and login service types

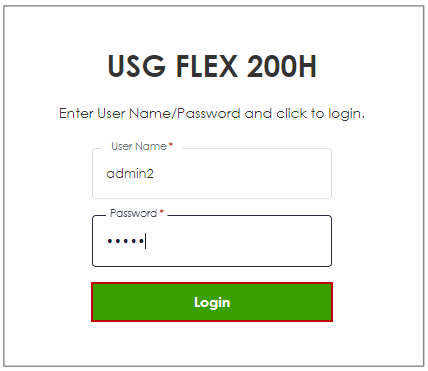
Go to User & Authentication > User Authentication. Two factor authentication for admin access is enabled by default. You need to select which services require two-factor authentication for admin user manually. The valid time is the deadline that admin needs to submit the two-factor authentication code 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.



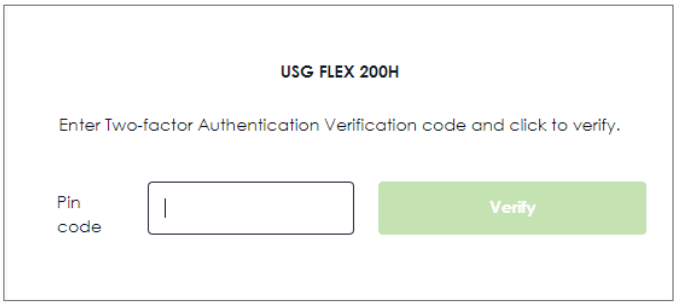

 

## Test the Result

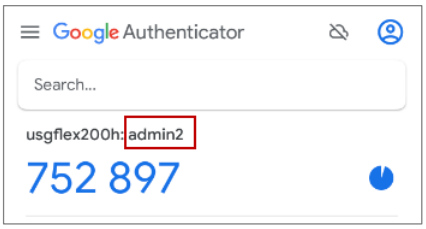
1. Login with the admin account "admin2".

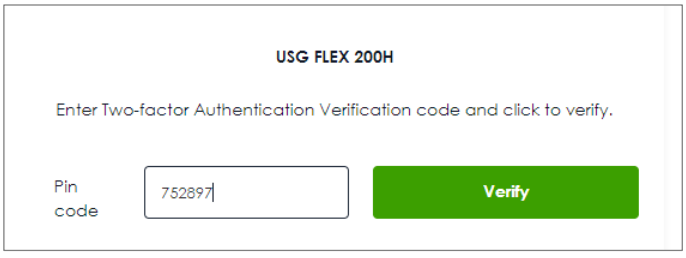



2. A pop-up window appears for administrator to enter the verification code.



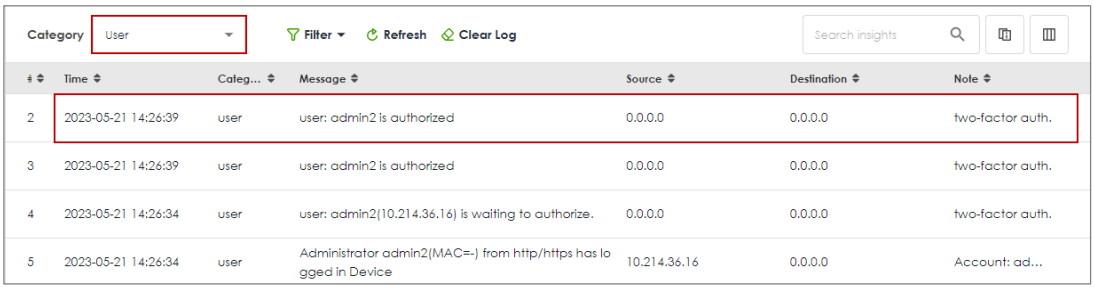

3. Enter the code shown on Google Authenticator and click "Verify". You can also enter the backup code if you don't have mobile device on hand.



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




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

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

Google authenticator is the most secure method to receive verification code for 2-factor authentication. Google authenticator gives a new code every 30 seconds, so each code expires in just 30 seconds which make it a secure option to generate codes for 2-step verification. Furthermore, Google authenticator is free to download, easy to use, and is able to work without Internet. This example illustrates how to set up two factor with Google Authenticator for Remote Access VPN and SSL VPN.


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

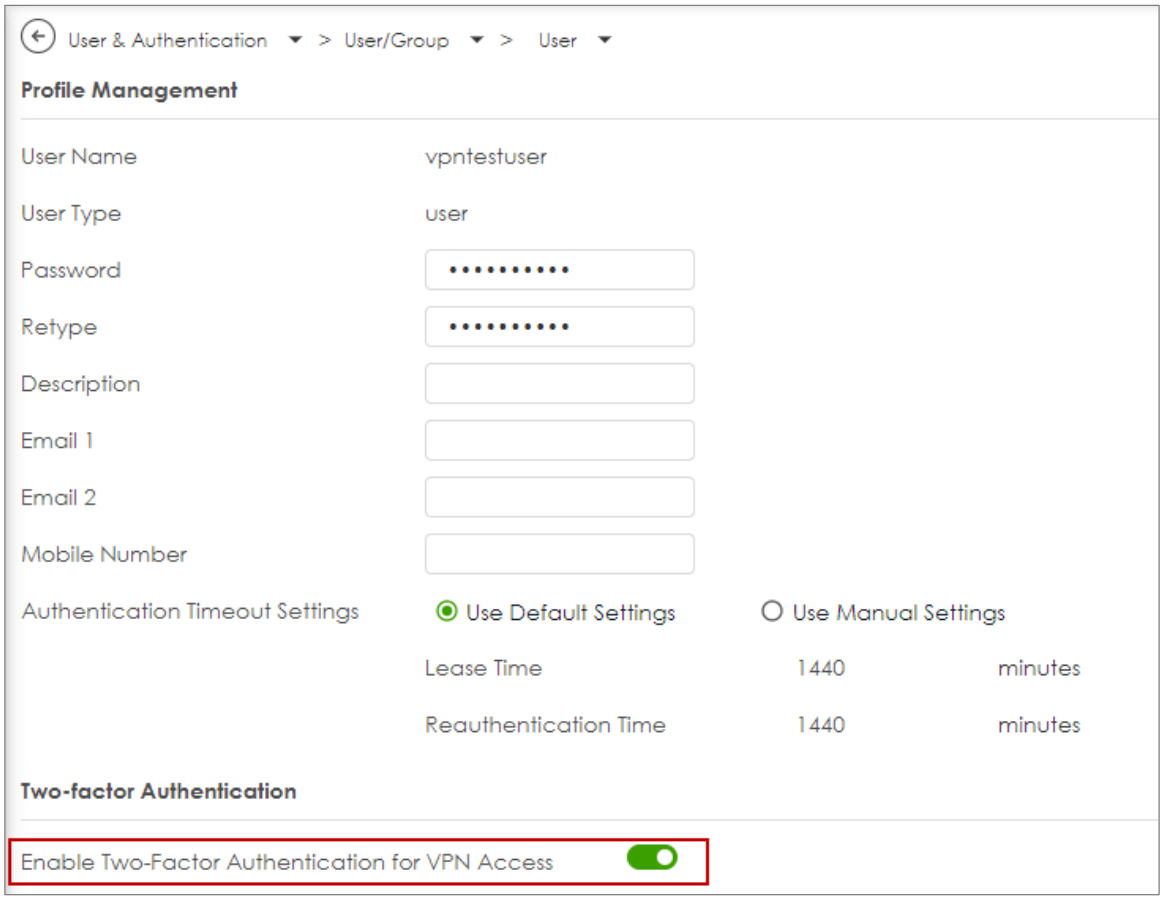
 

## Two Factor with Google Authenticator Flow

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

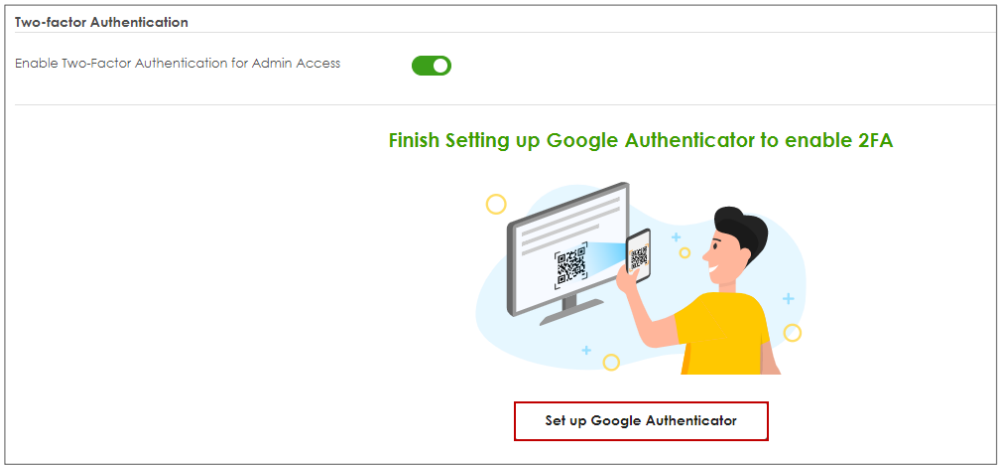
## Enable Google Authentication on a User

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

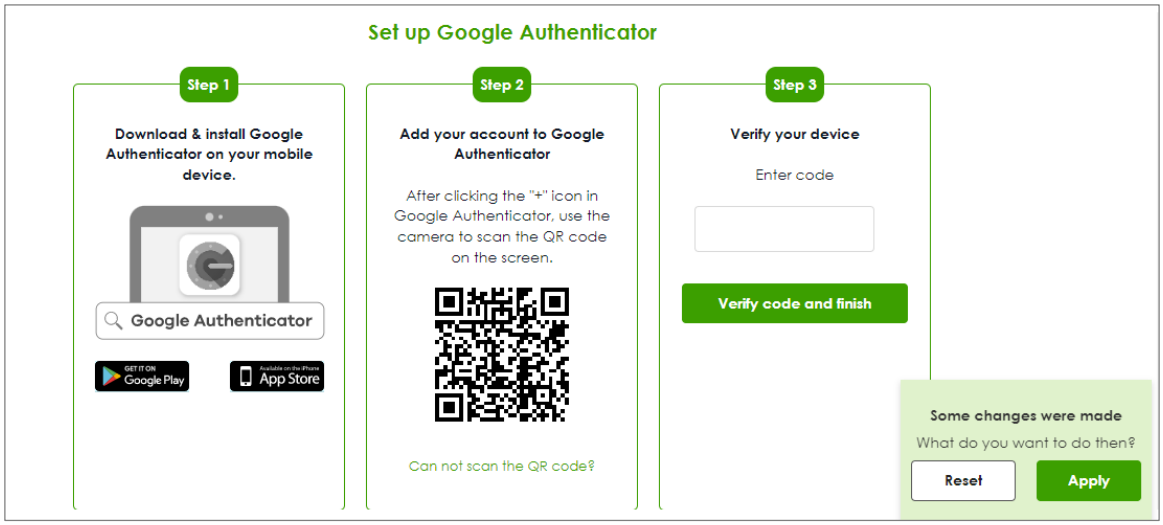


Click "Set up Google Authenticator" to start setting up Google Authenticator on your mobile phone.



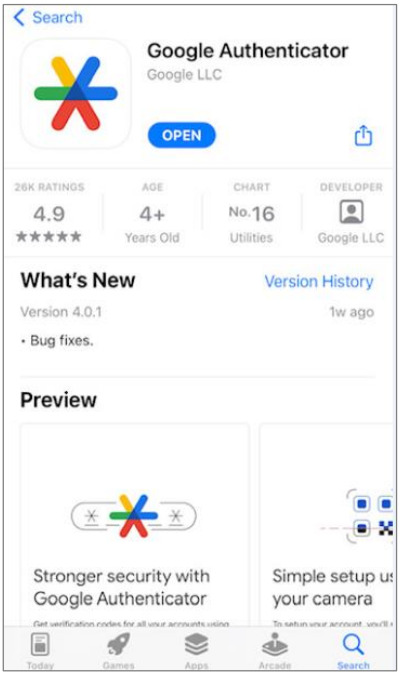

## Set up Google Authenticator



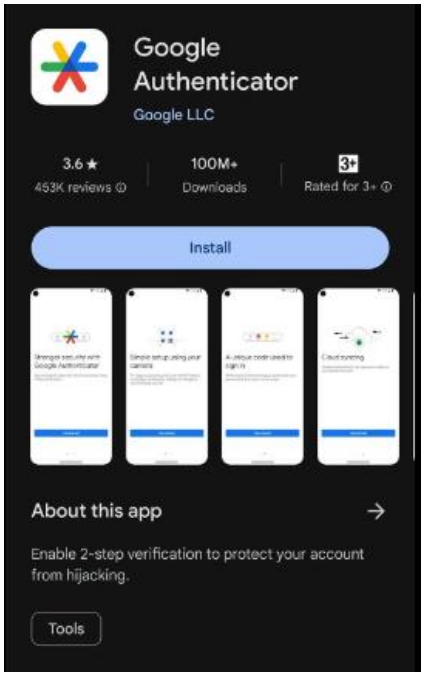

 

5. Download and install Google Authenticator on your mobile device.

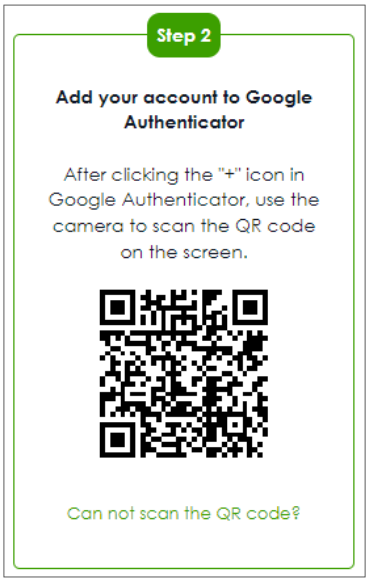
**Apple Store**

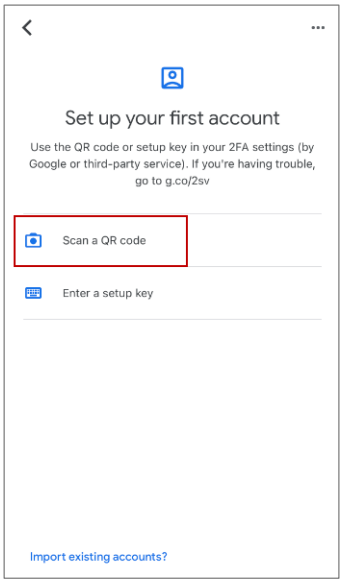



**Google Play**



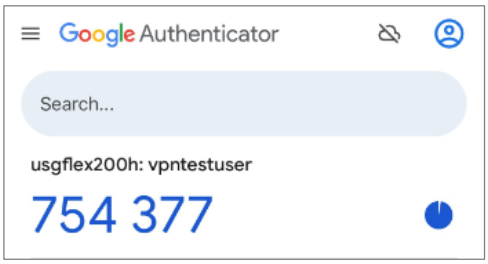

6. Register the user account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.

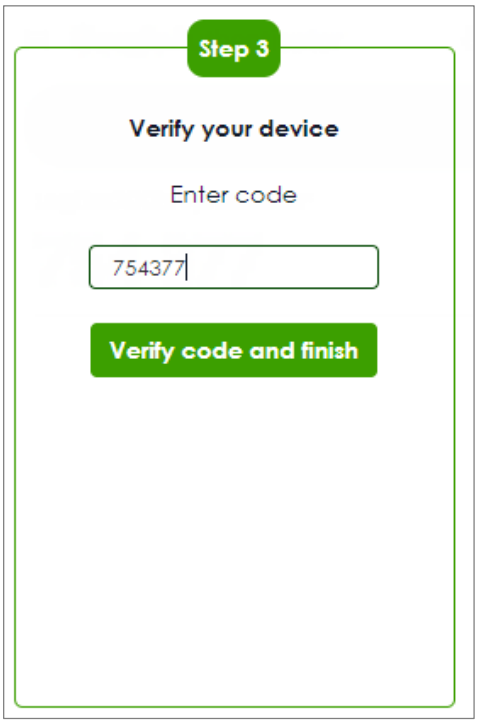


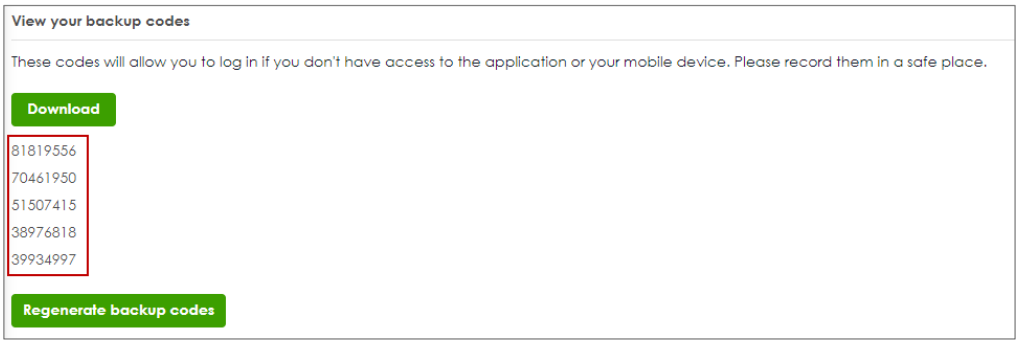

 

7. Enter the token code which displays on Google Authenticator to “Step 3” and click “Verify code and finish” to submit and verify the code.



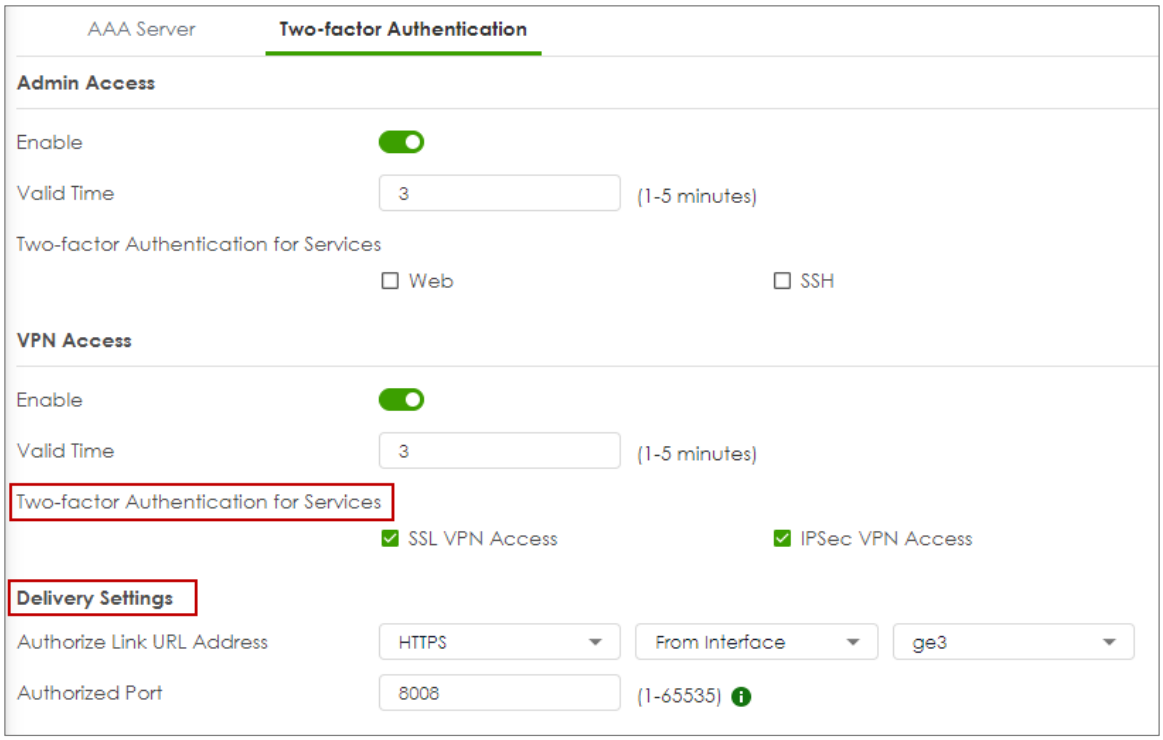

8. After 2FA registration is set up successfully, there are backup codes on web GUI. The backup codes are for device login in the case you don't have access to the application on your mobile device. Download the backup codes and record them in a safe place.



## 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.

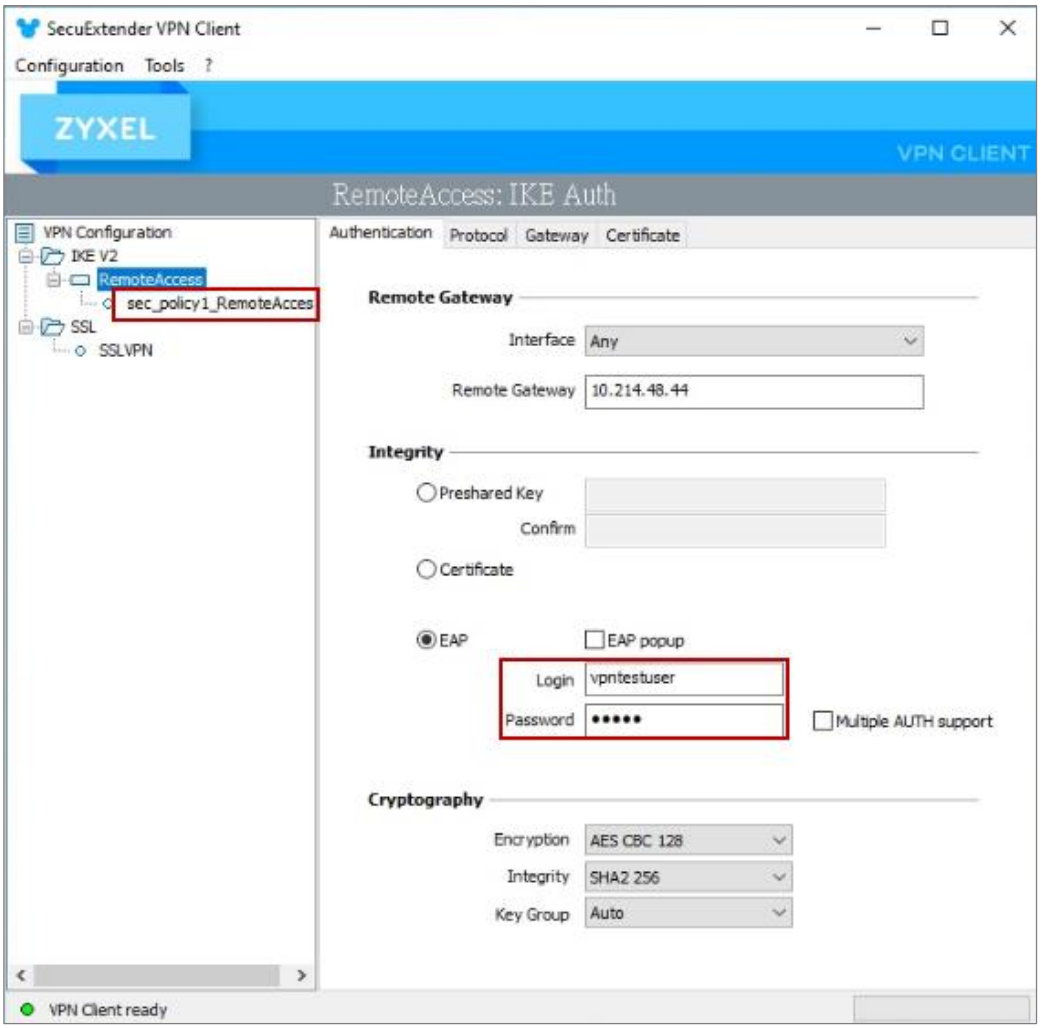


## Test the Result

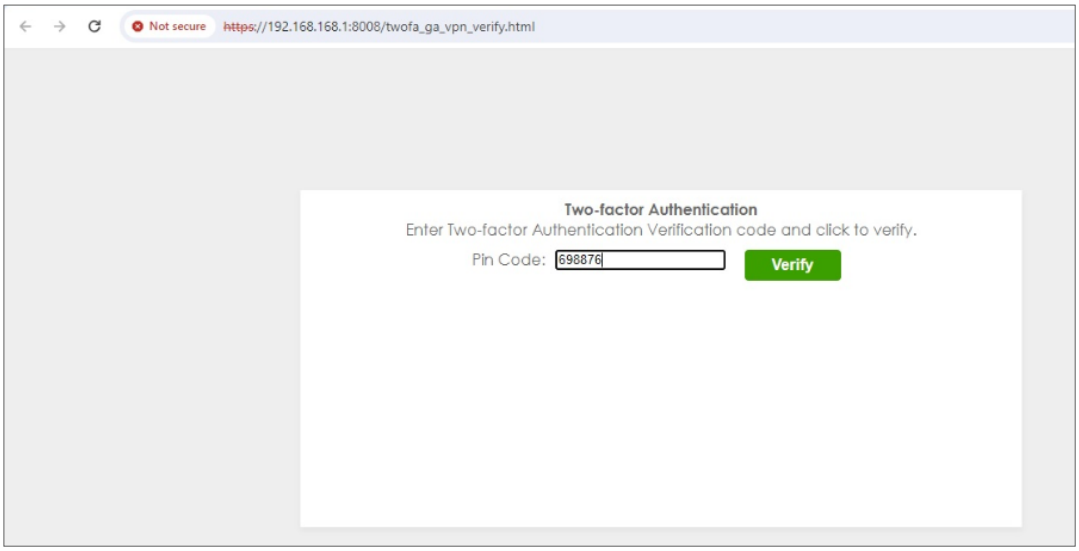
### Remote Access VPN (IKEv2)

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

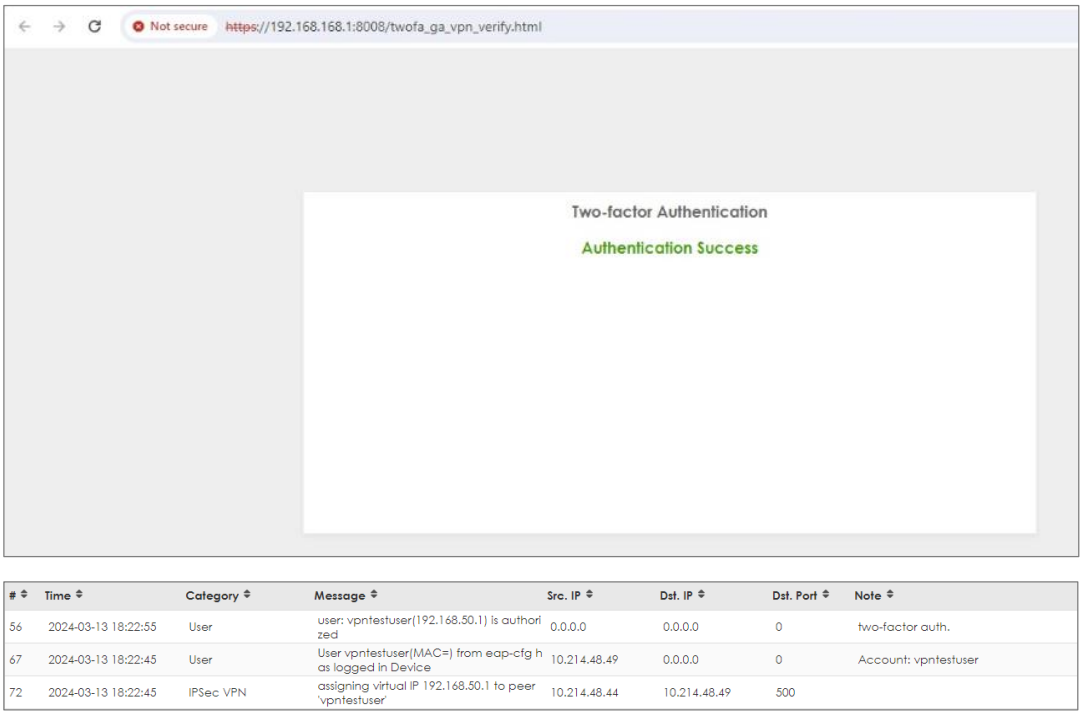


2. The browser will pop up authentication page to enter the verification code. Enter the code shown on Google Authenticator and click "Verify". You can also enter the backup code if you don't have mobile device on hand.



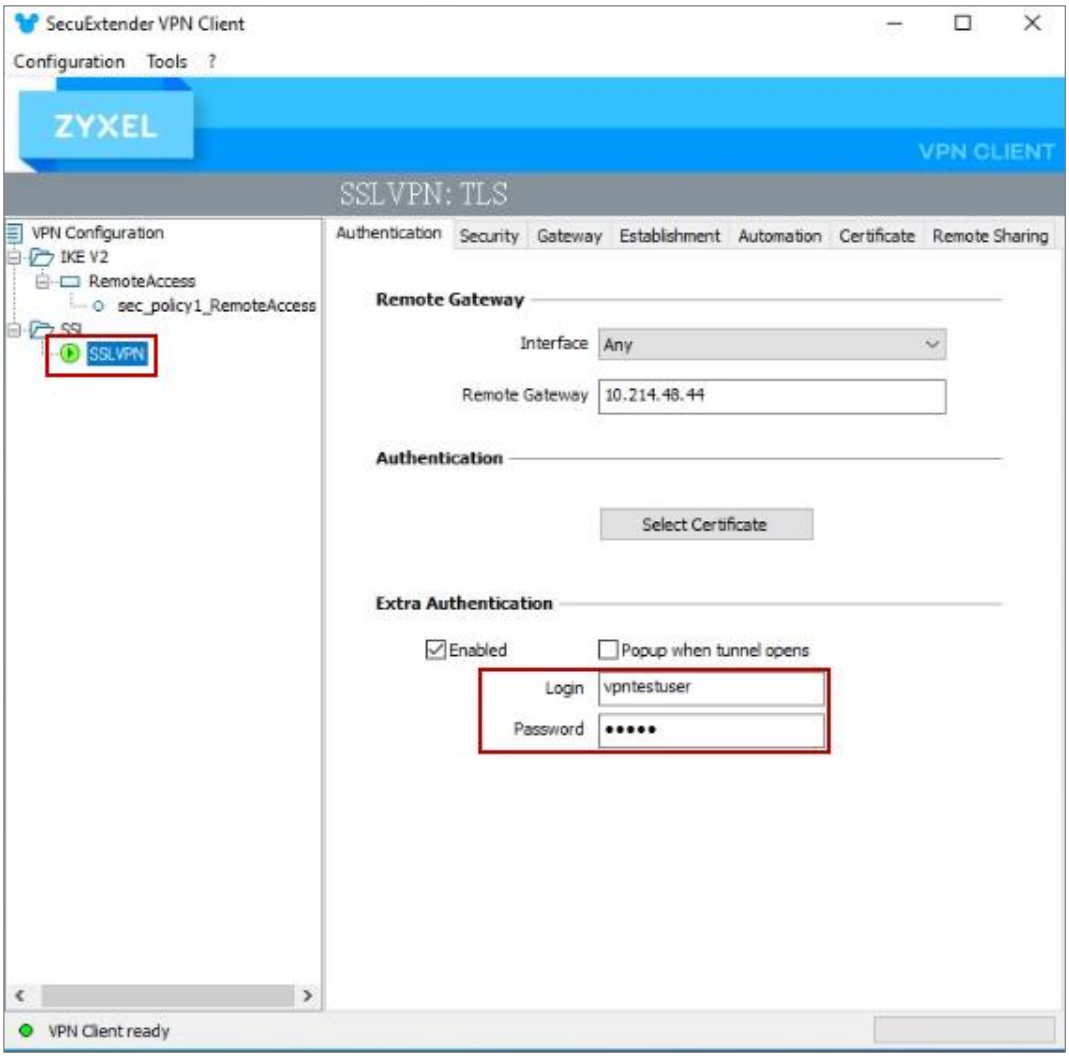

3. Authorize with username, password and the token code successfully.



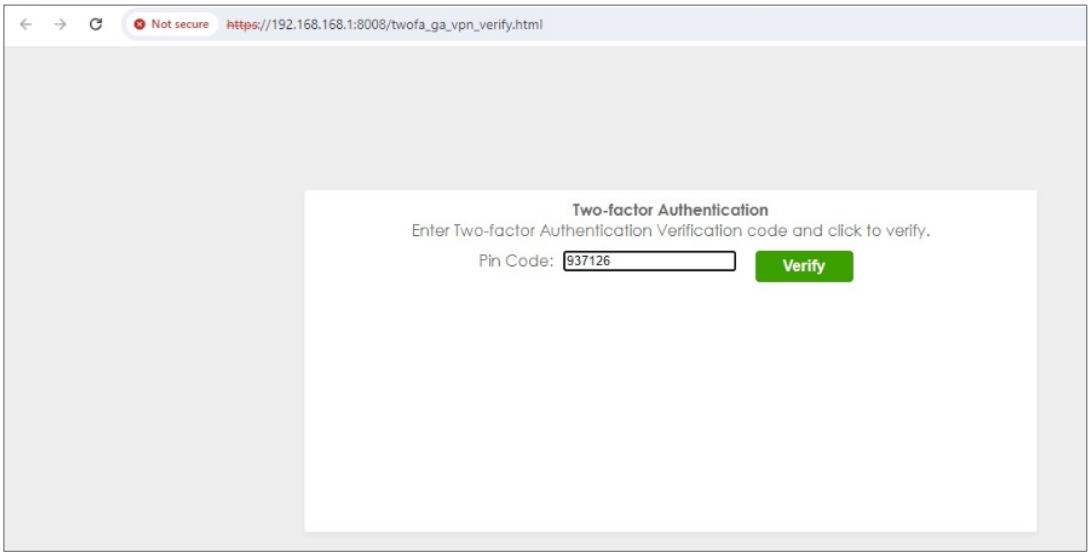
**SSL VPN**

1. Open SSL VPN tunnel on SecuExtender VPN Client.



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



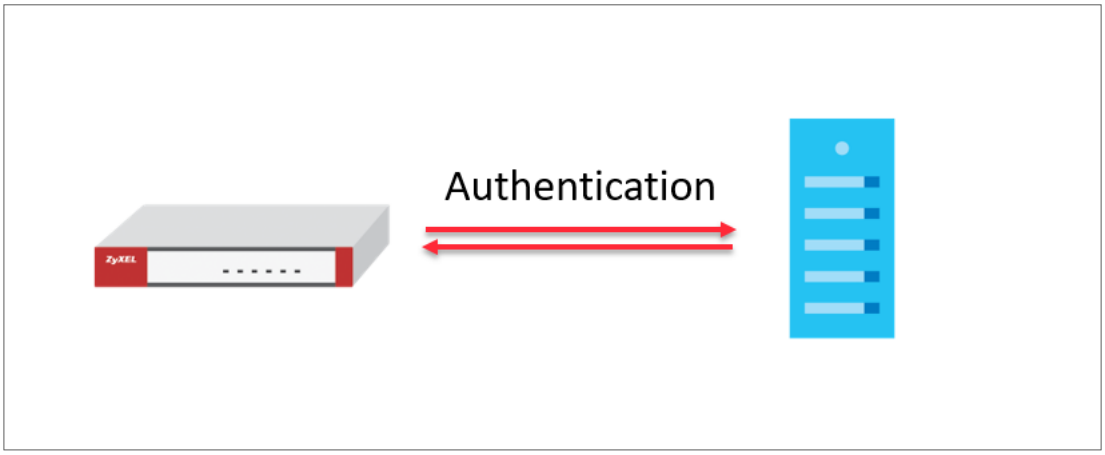

3. Authorize with username, password and the token code successfully.


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

# How to set up AD authentication with Microsoft AD

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

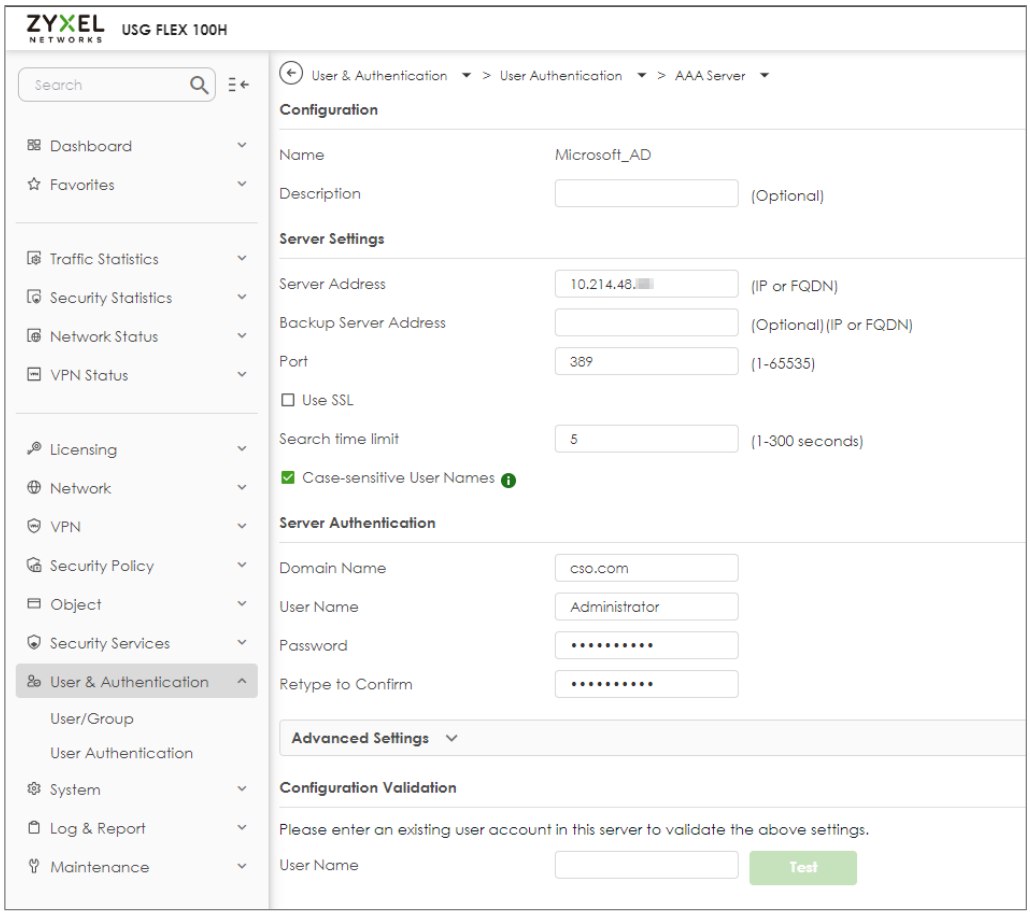


## Set Up a profile for AD server

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

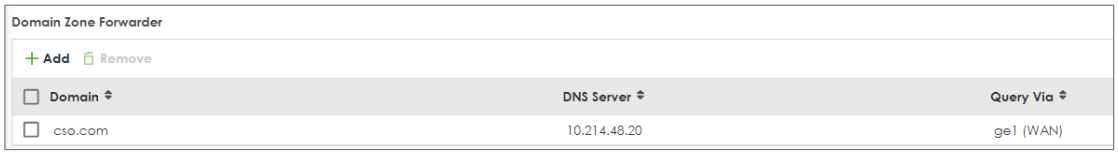

Enter the Server Address and port for Server settings. (10.214.48.XX:389 in this example). Enter the domain name and the credentials for logging into the AD server, and click Apply.



## Join Domain

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




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

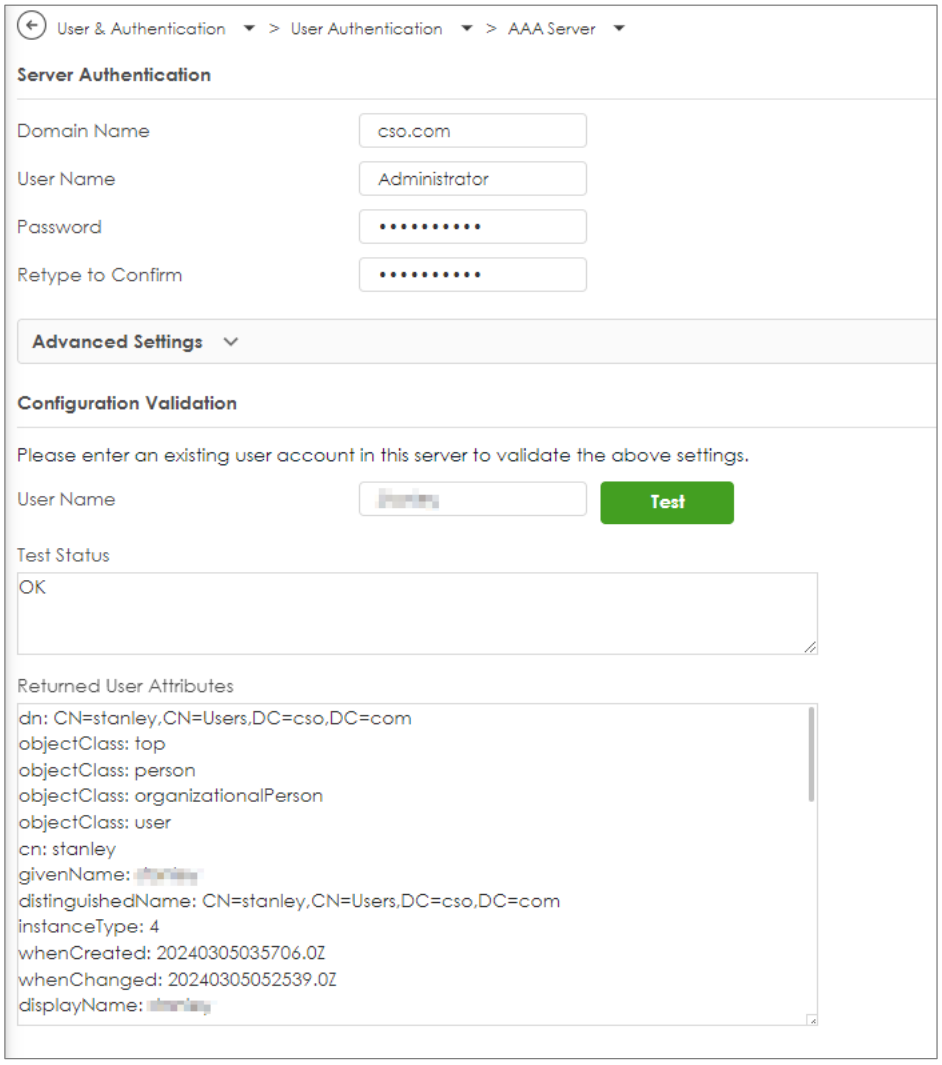

Enter NetBIOS Domain Name, Username and Password, click Apply.


After join domain successfully, you can see this icon.

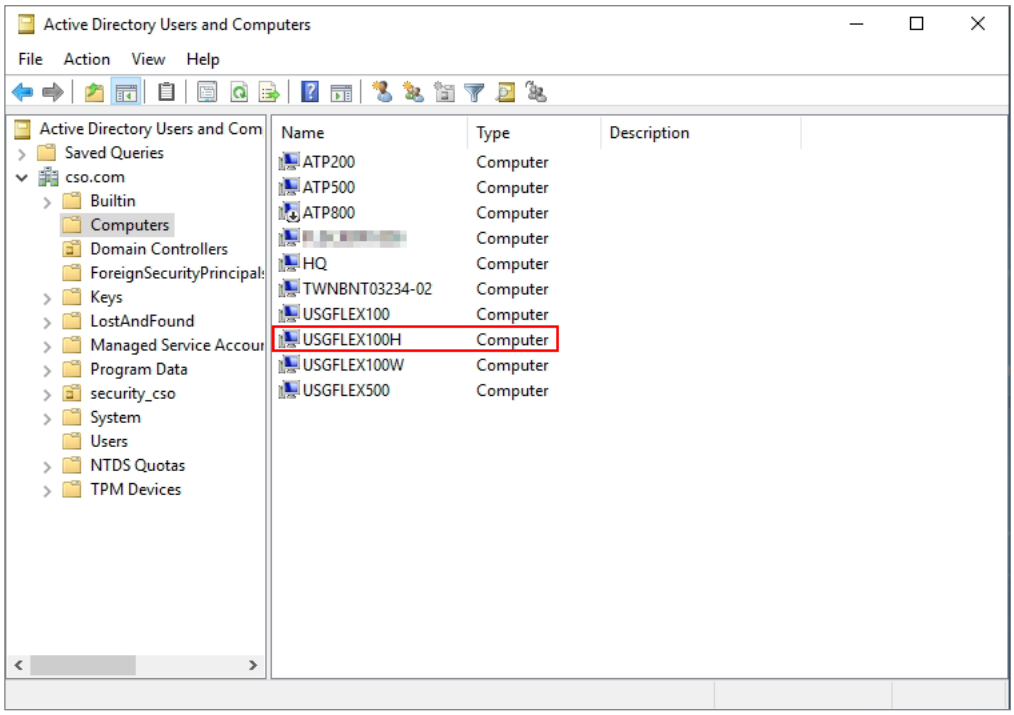
## Test the Result

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.



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

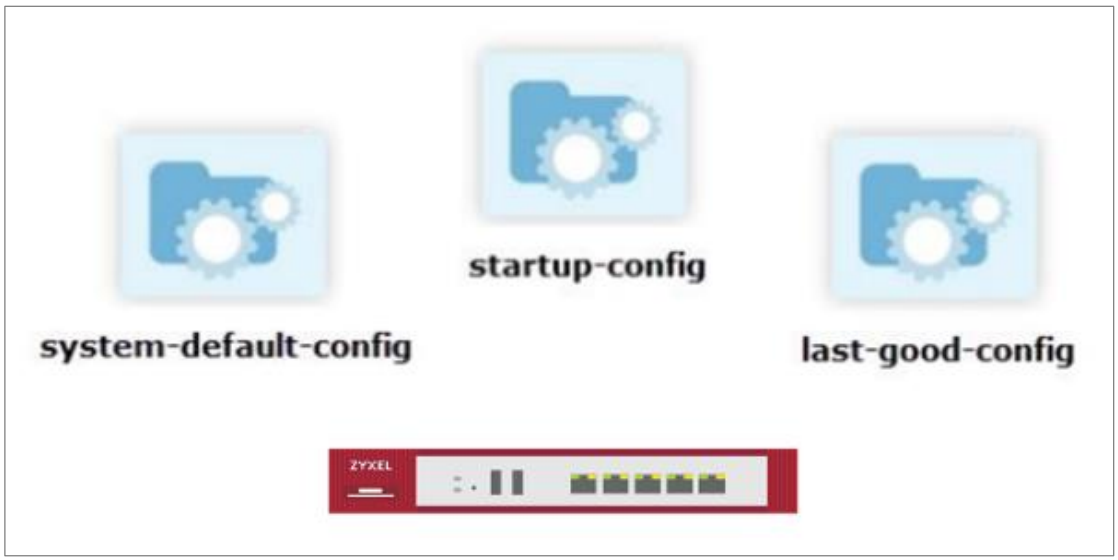


# Chapter 4- Maintenance

## How to Manage Configuration Files

This is an example of how to rename, download, copy, apply and upload configuration files. Once your USG FLEX H device is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.




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

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

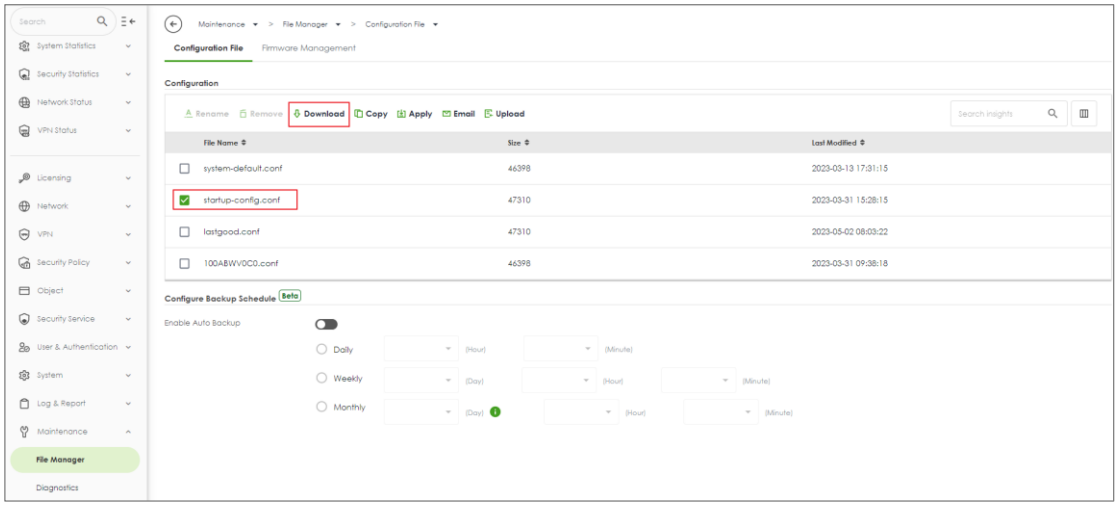
The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the device last restarted.

## Download the Configuration Files

**Maintenance > File Manager > Configuration File**

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




## Copy the Configuration Files

**Maintenance > File Manager > Configuration File**

Select the file and click “Copy”.

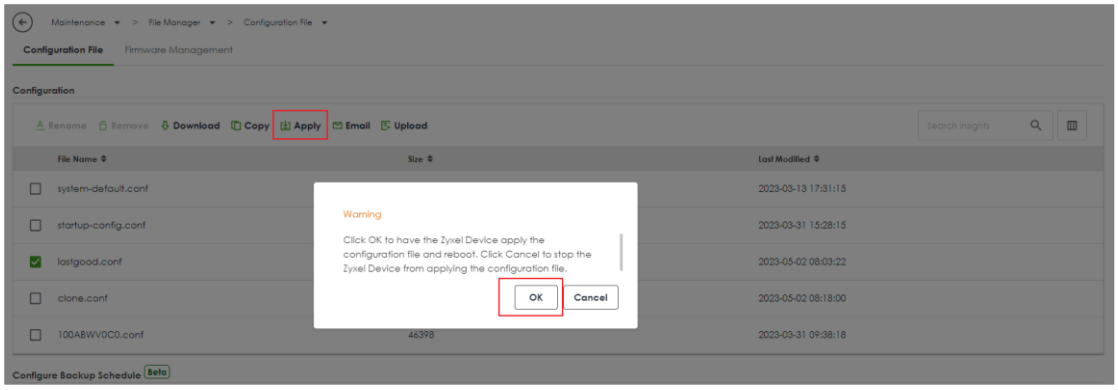
A pop-up screen will appear allowing you to edit the Target file name.

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


## 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.

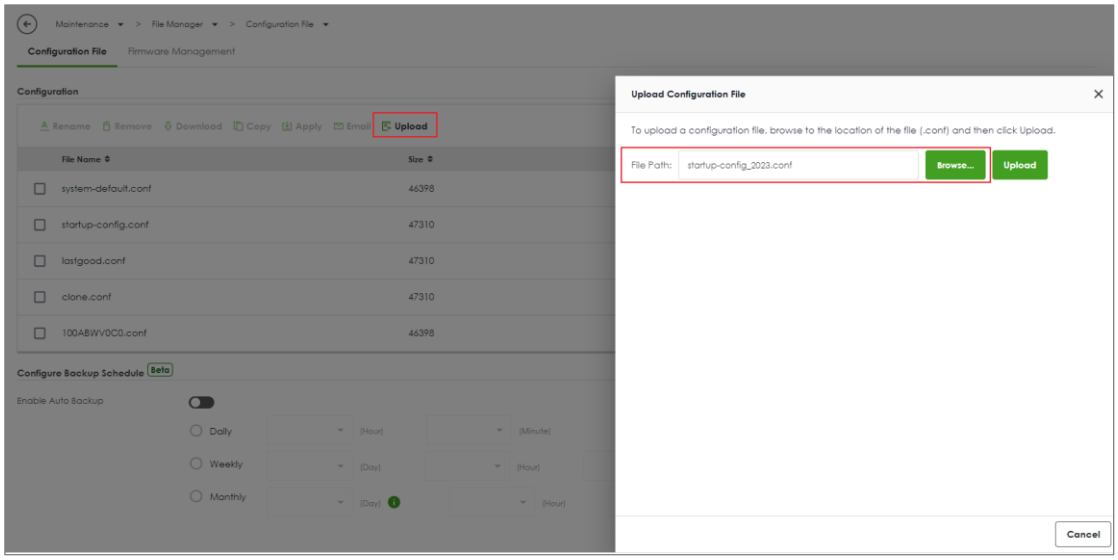


## Upload the Configuration Files

**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.



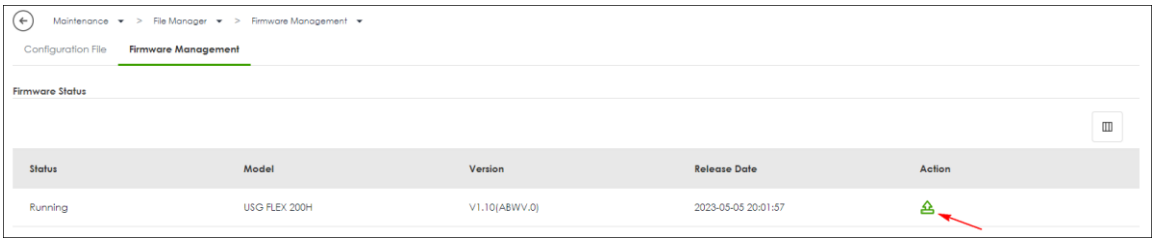
# How to Manage Firmware

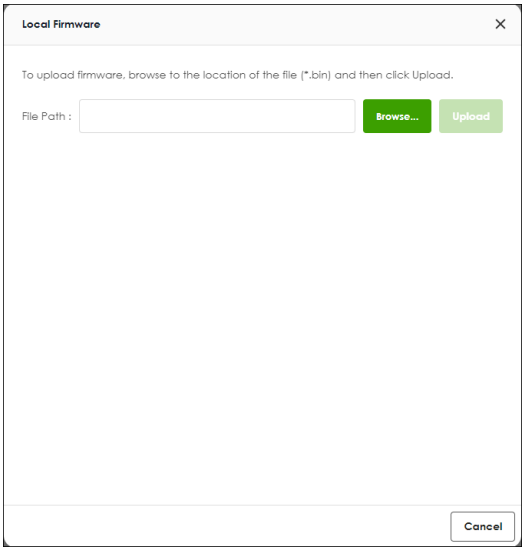
For management convenience, administrators have the capability to upgrade the firmware effortlessly either from a PC or using the cloud firmware upgrade function. Additionally, the firmware upgrade can be scheduled to occur automatically within a preconfigured timeframe.

## 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 portal. (https://portal.myzyxel.com/my/firmwares)



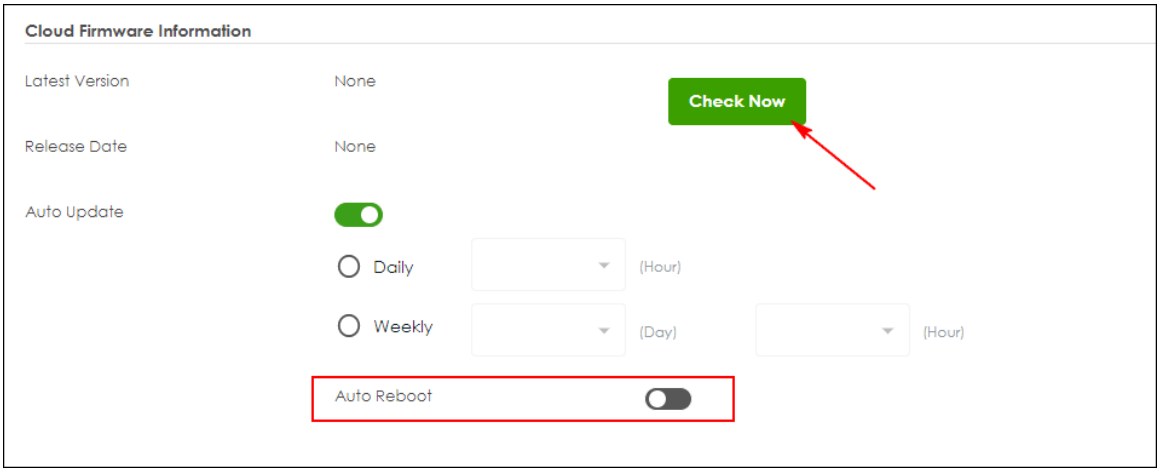



## Cloud Firmware Upgrade

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.



# Chapter 5- Others

## How to Setup and Configure Daily Report

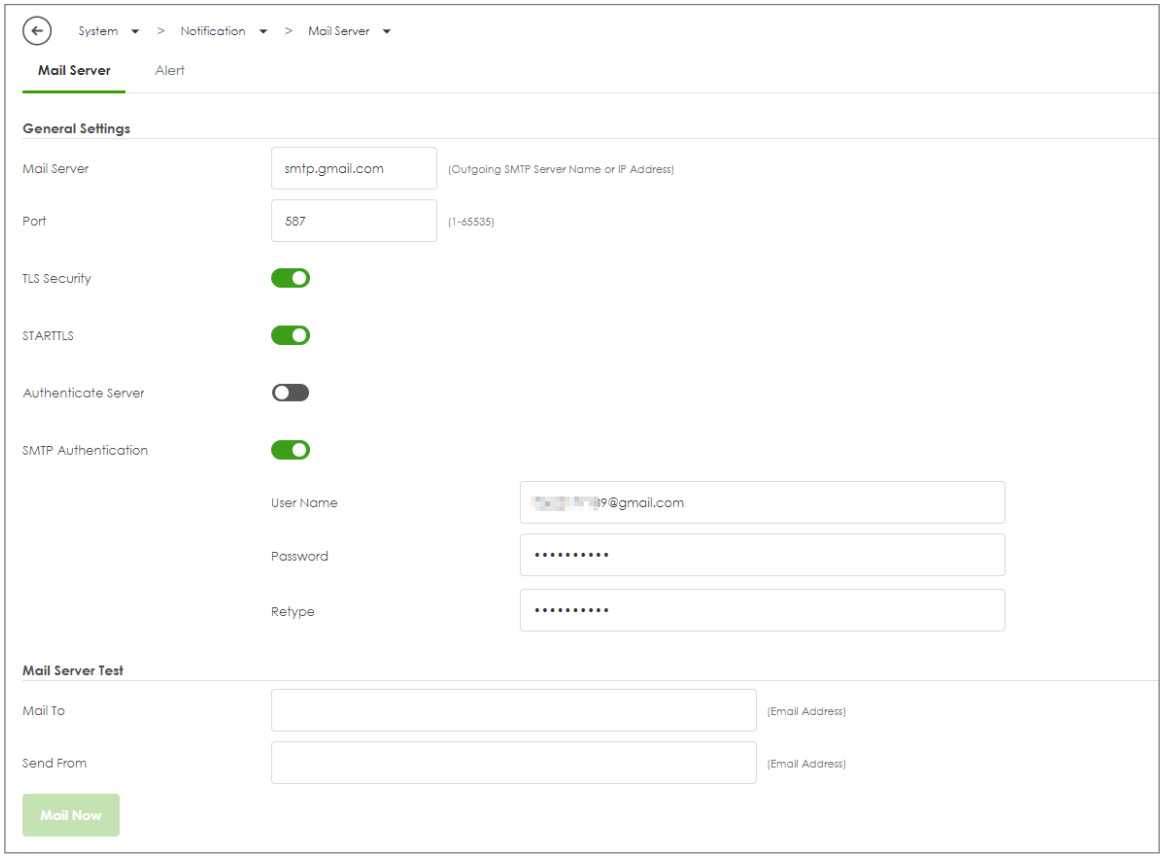
Administrators can efficiently oversee gateway events by reviewing the Daily Report for management purposes. This example demonstrates how to set up the Daily Report, including the option to select specific log messages for inclusion. Once configured, you can utilize "Send Report Now" to assess your 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).

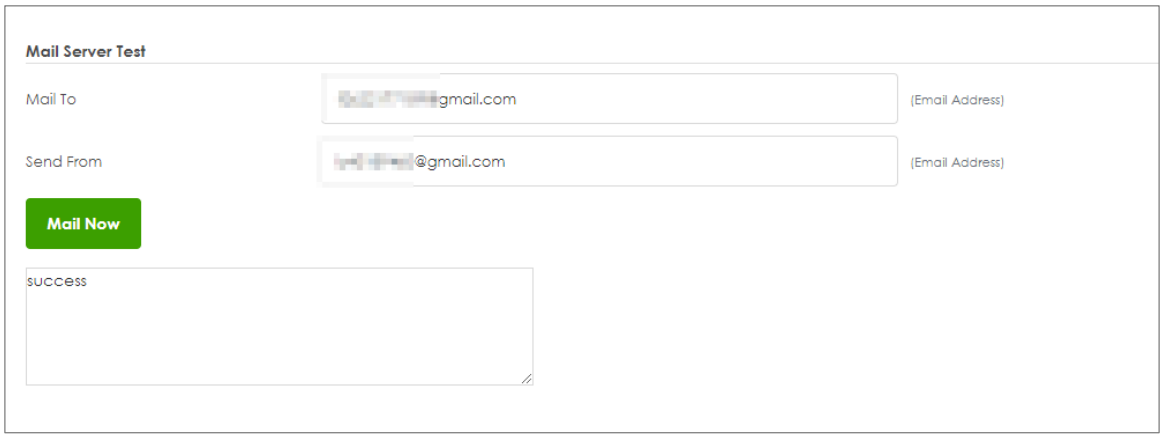
## Set Up the Mail Server

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.



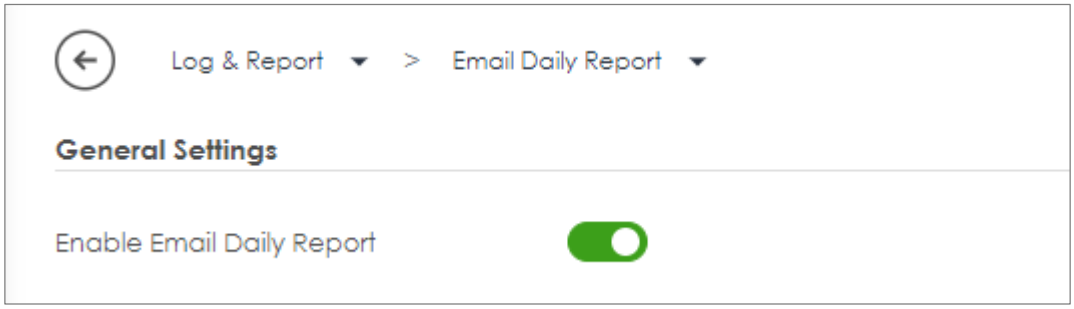
You can verify the correctness of the settings by using the Mail Server Test below. If it is successful, you will receive an email.





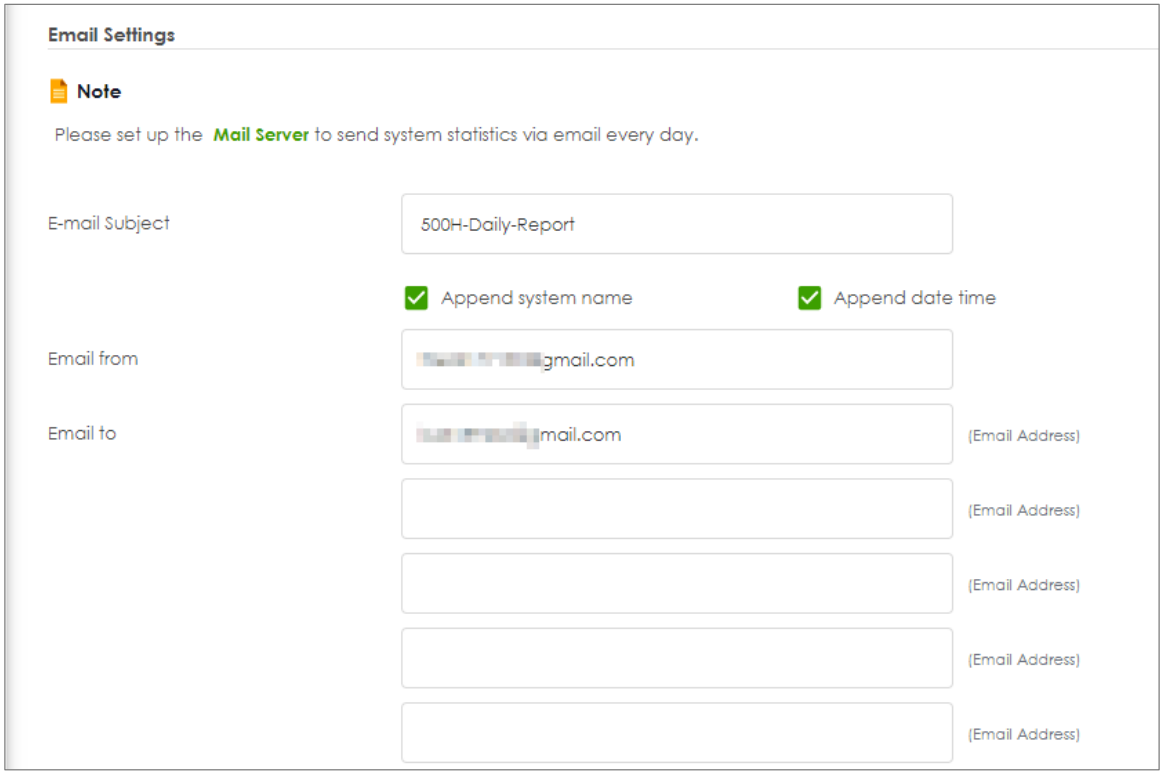
## Set Up Email Daily Report

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

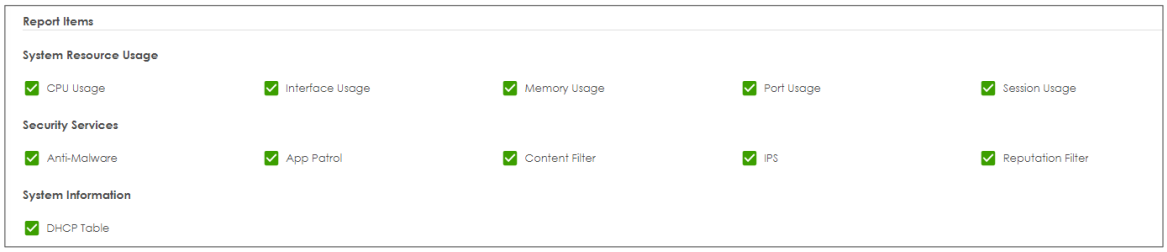


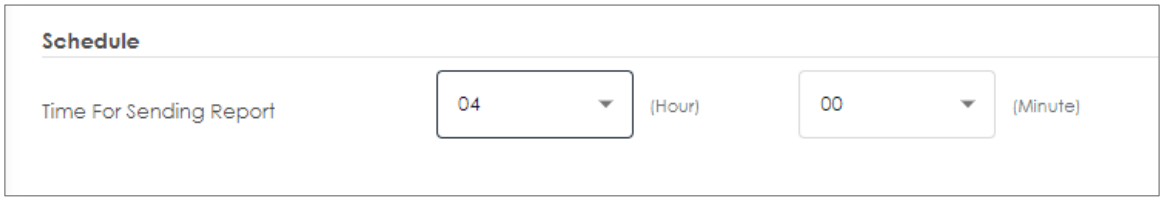
Type your Email Subject and your Sender and Receiver in the field.




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



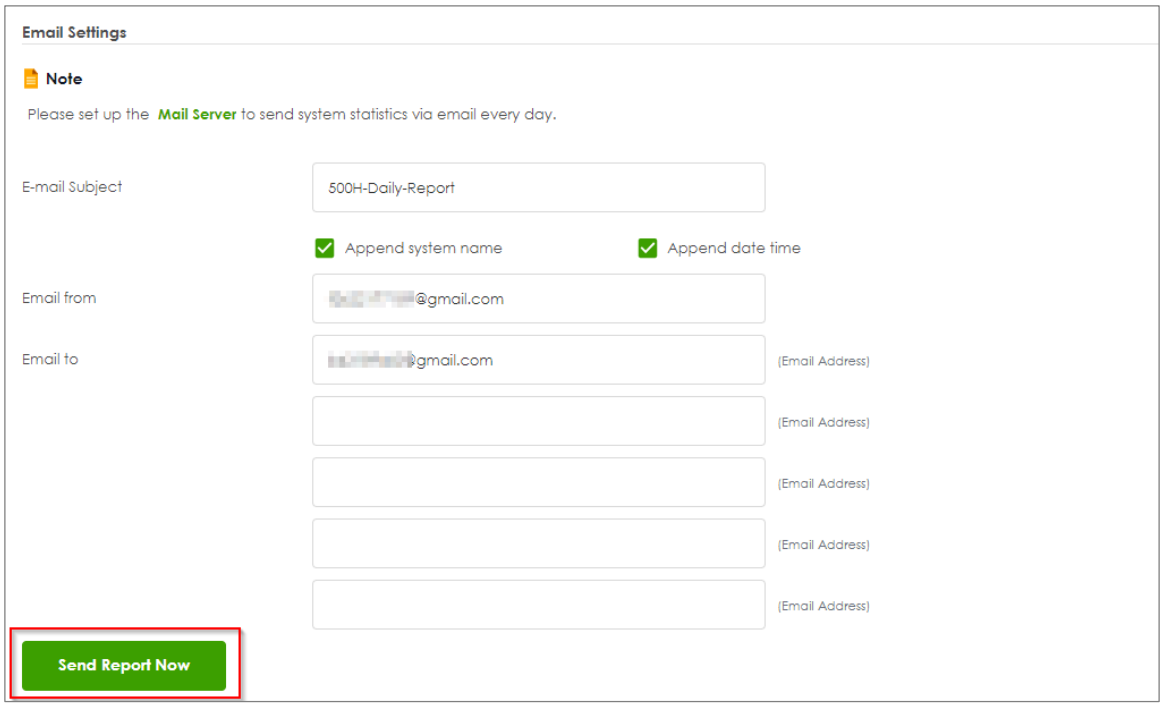

You can set up a Schedule at the bottom of the page

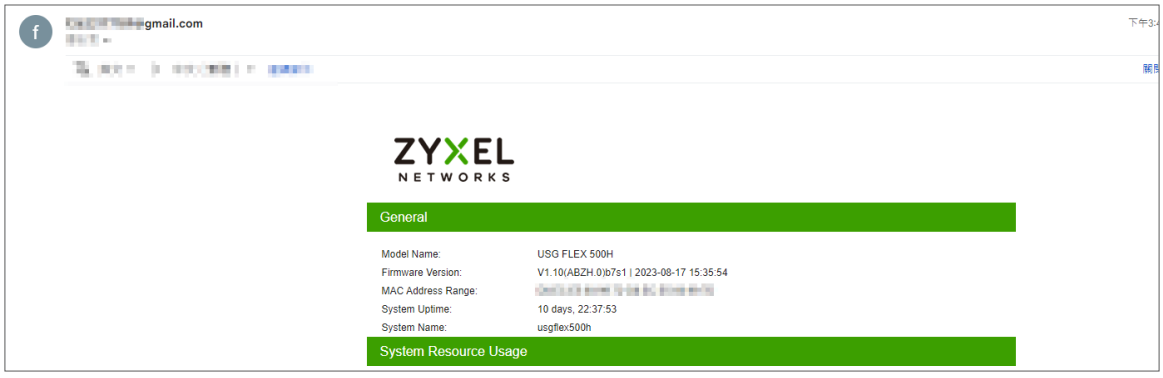


## Test the Email Daily Report

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

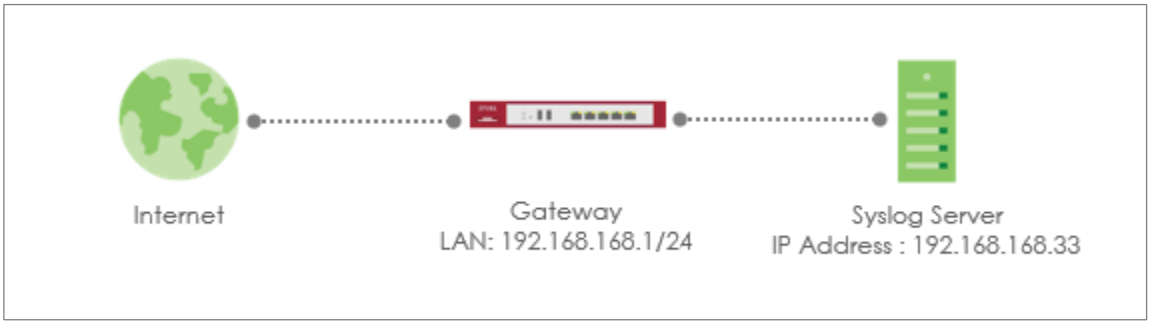


# How to Setup and Send Logs to a Syslog Server

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.

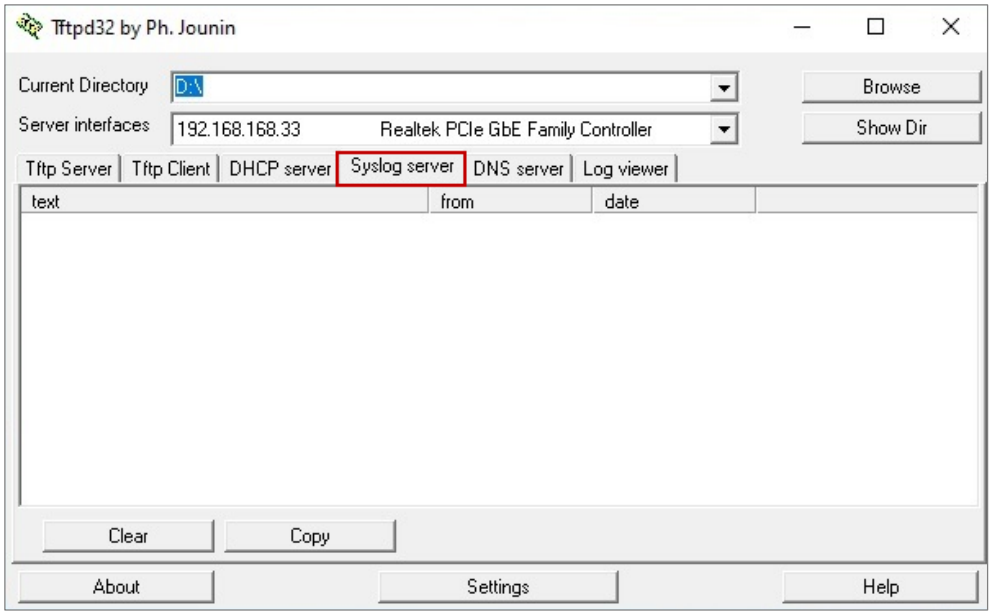



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

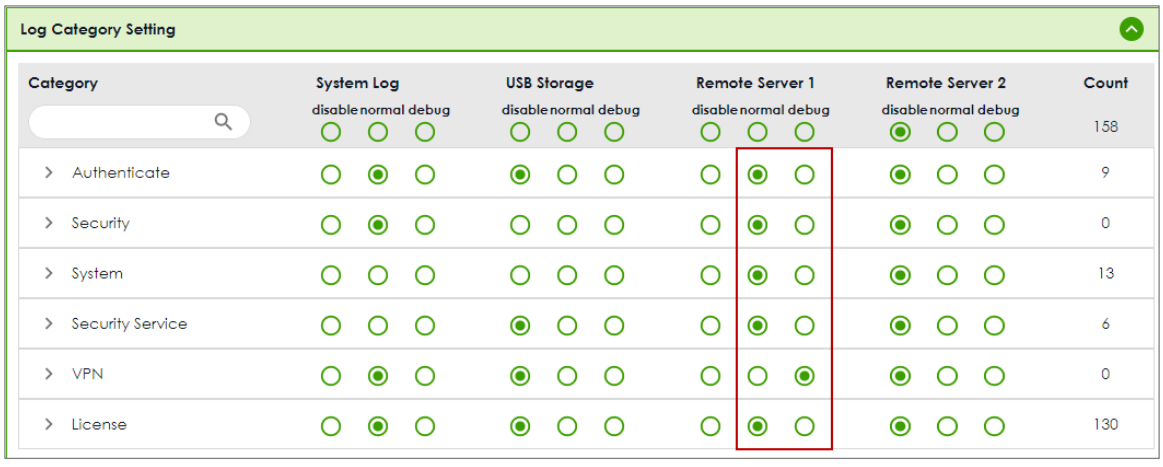
## Set Up the Syslog Server

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



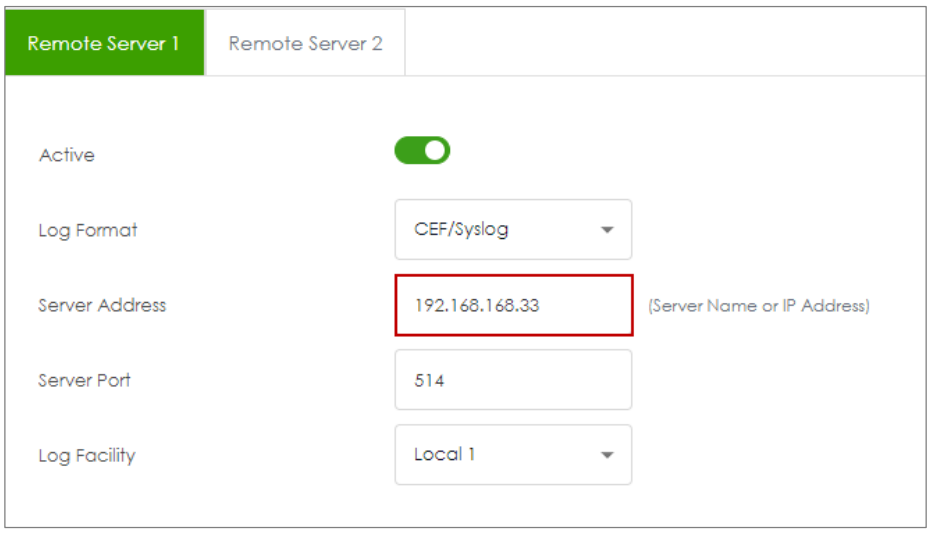

## Set Up Remote Server Setting on the Gateway

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.



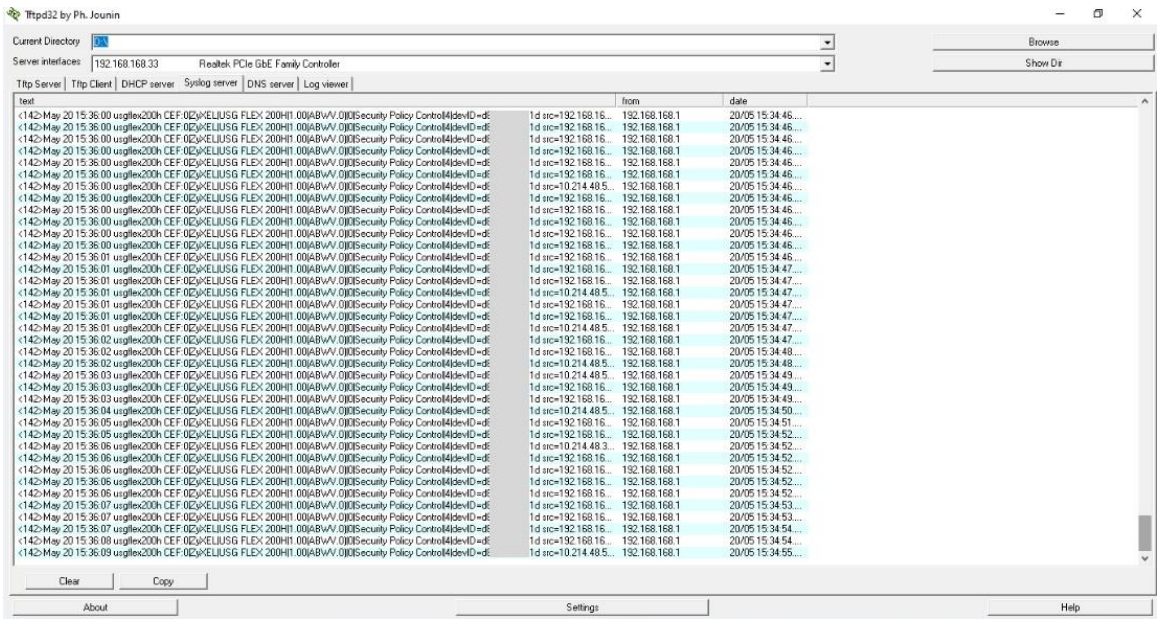

 

Go to Log & Report > Log Settings > Remote Syslog Server. Set Log Format to be CEF/Syslog and type the server name or the IP address of the syslog server. Turn on "Active" to send log information to the server.




## Test the Remote Syslog Server

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.

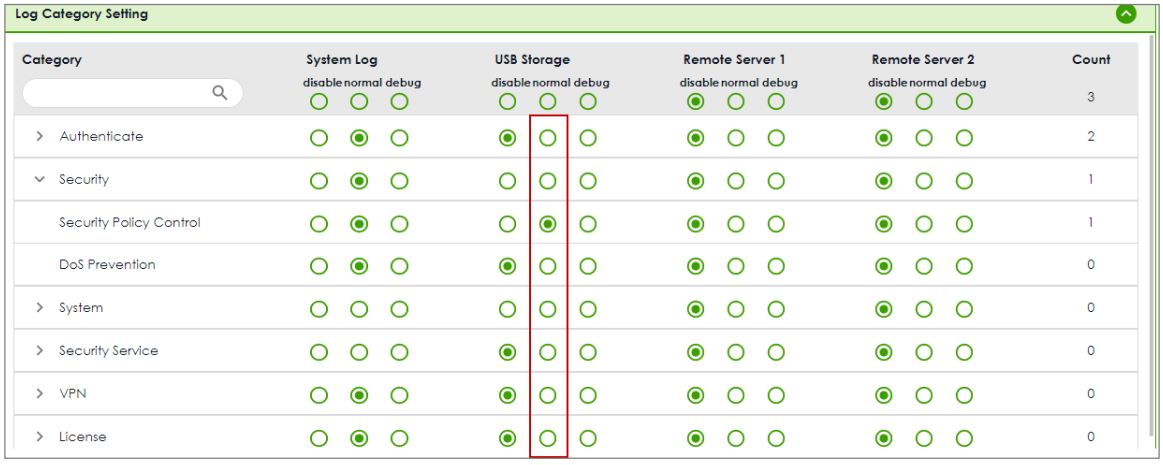
Note: The USB storage must allow writing (it cannot be read-only) and use the FAT16, FAT32, EXT2, or EXT3 file system. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10). The USB port can provide max. 900mA output power. You might need to connect external power for the USB storage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

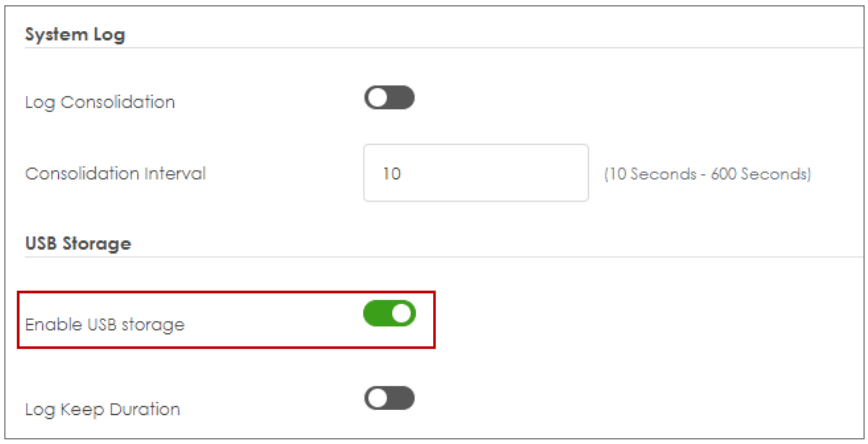
## Set Up the USB storage on the Gateway

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.



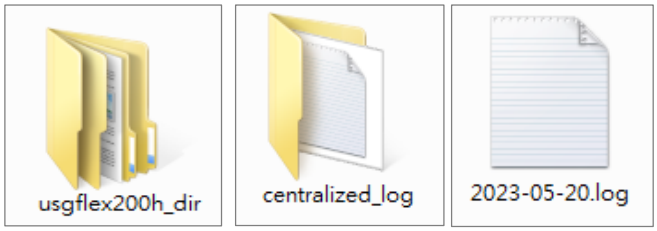
Go to Log & Report > Log Settings > USB Storage. Turn on “Enable USB storage” to store the system logs on a USB device.




## 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



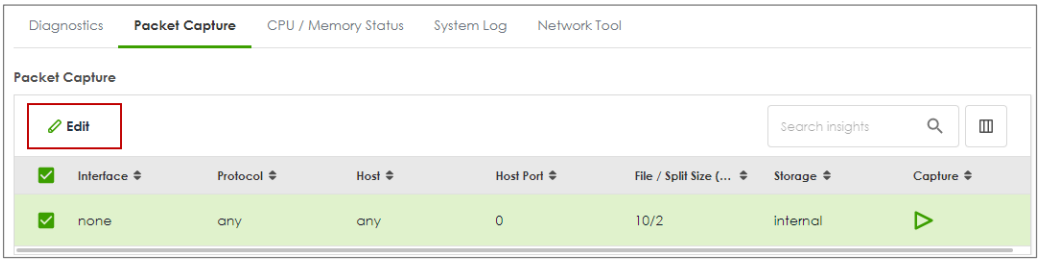
# How to Perform and Use the Packet Capture Feature

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.

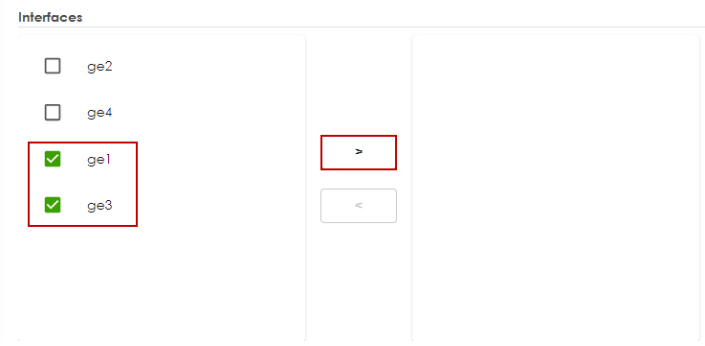
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

## Set Up the Packet Capture Feature

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



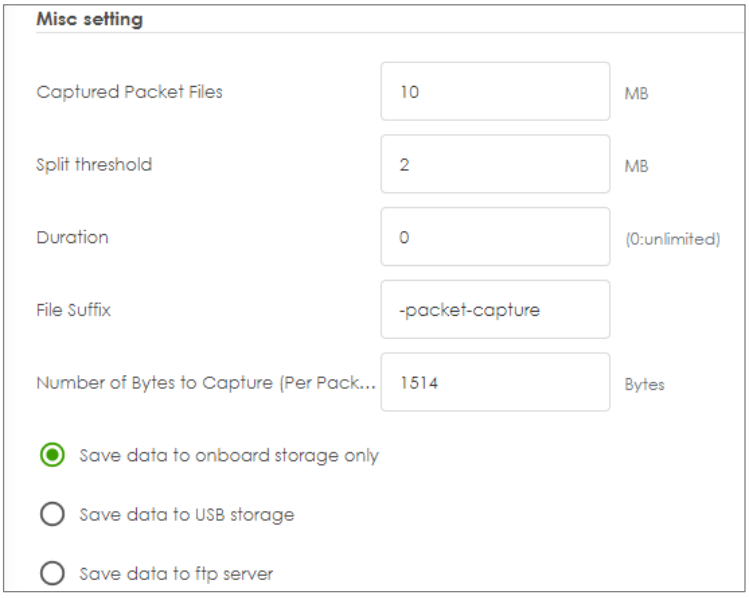

8. In Interfaces, select interfaces for which to capture packets and click the right arrow button to move them to the list.



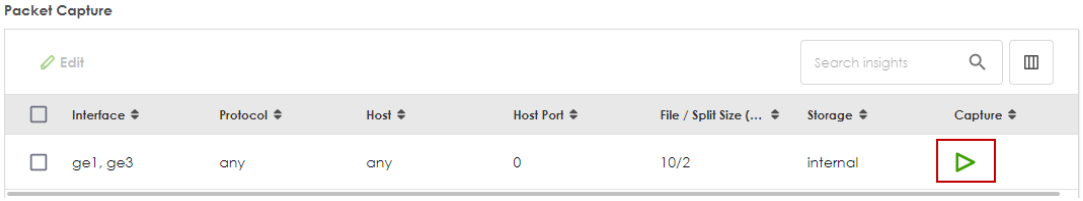
9. In Filter, select IP Version for which to capture packets. Select any to capture packets for all IP versions.
   Select the Protocol Type of traffic for which to capture packets. Select any to capture packets for all types of traffic.
   Select a Host IP address object for which to capture packets. Select any to capture packets for all hosts. Select User Defined to be able to enter an IP address.


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



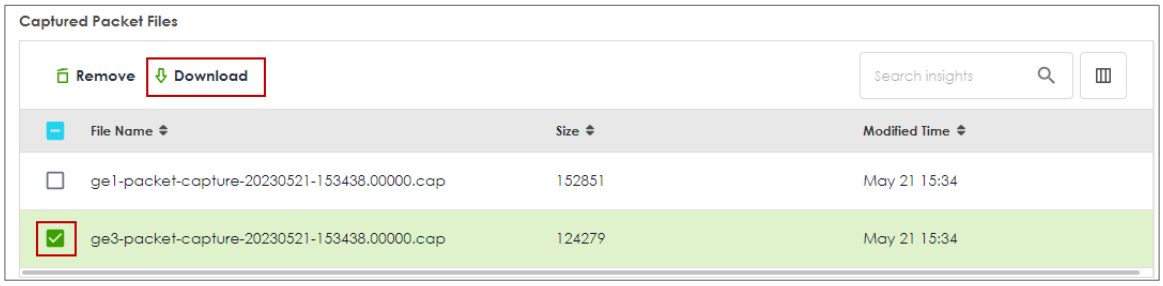
11. Click the icon to start capturing packets.




12. Click the icon to stop capturing packets.


## Download the Captured Packet Files

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




## Check Real-Time traffic using command

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

**Syntax**:

cmd traffic-capture <interface name>

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

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

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

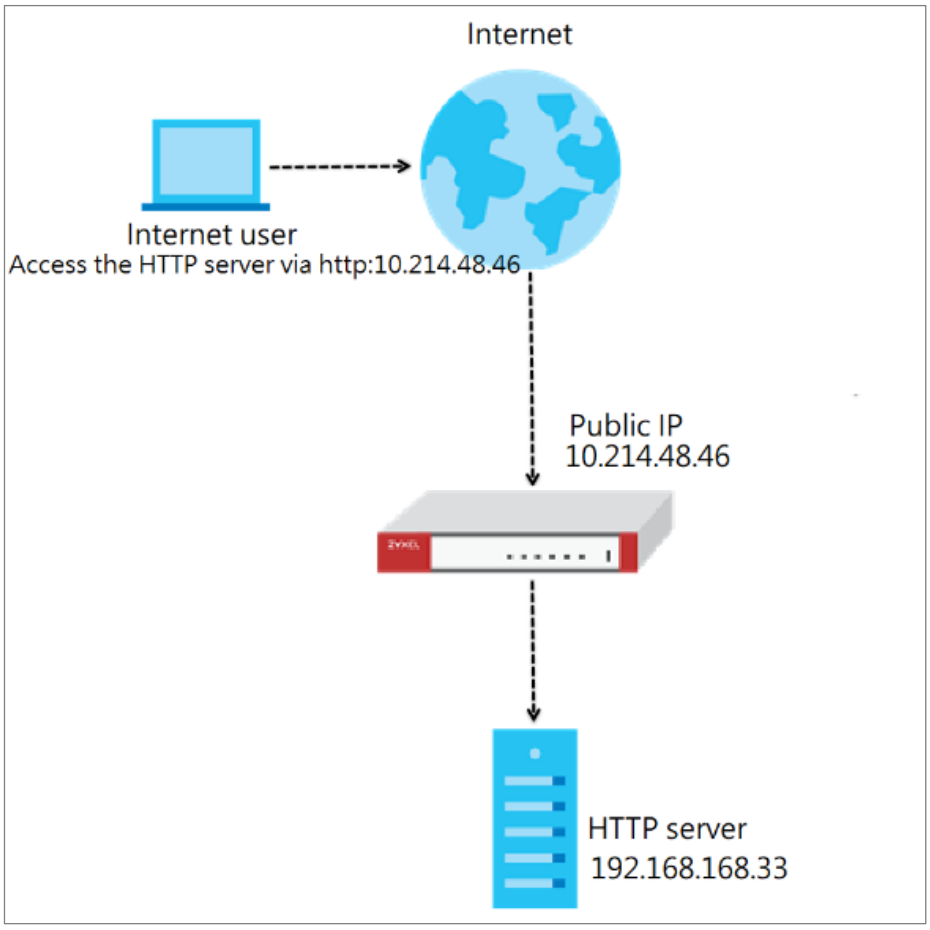
cmd traffic-capture <interface name> filter “host <ip address> and port <port number>”

```
usgflex200h> cmd traffic-capture ge3 filter "src 192.168.168.33"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge3, link-type EN10MB (Ethernet), capture size 262144 bytes
16:07:36.738176 [redacted] > [redacted], ethertype IPv4 (0x0800),
 length 77: 192.168.168.33.5353 > 224.0.0.251.5353: 0 A (QM)? zytwapexone.local
. (35)
16:07:36.738249 [redacted] > [redacted], ethertype IPv4 (0x0800),
 length 77: 192.168.168.33.5353 > 224.0.0.251.5353: 0 A (QM)? zytwapexone.local
. (35)
16:07:36.739617 [redacted] > [redacted], ethertype IPv4 (0x0800),
 length 77: 192.168.168.33.5353 > 224.0.0.251.5353: 0 AAAA (QM)? zytwapexone.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

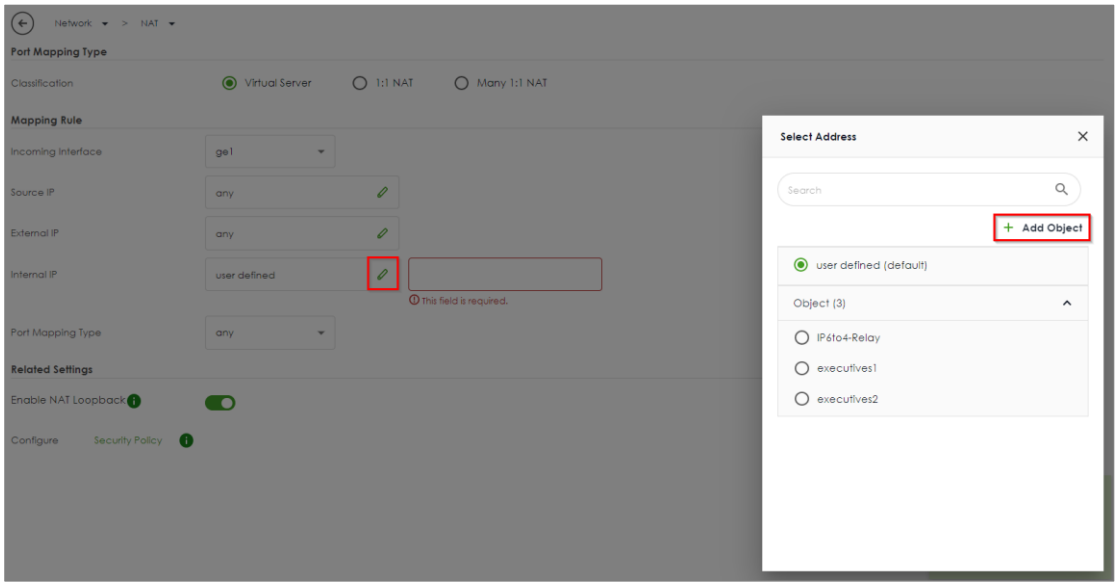
- select Virtual Server

- Incoming Interface: ge1

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

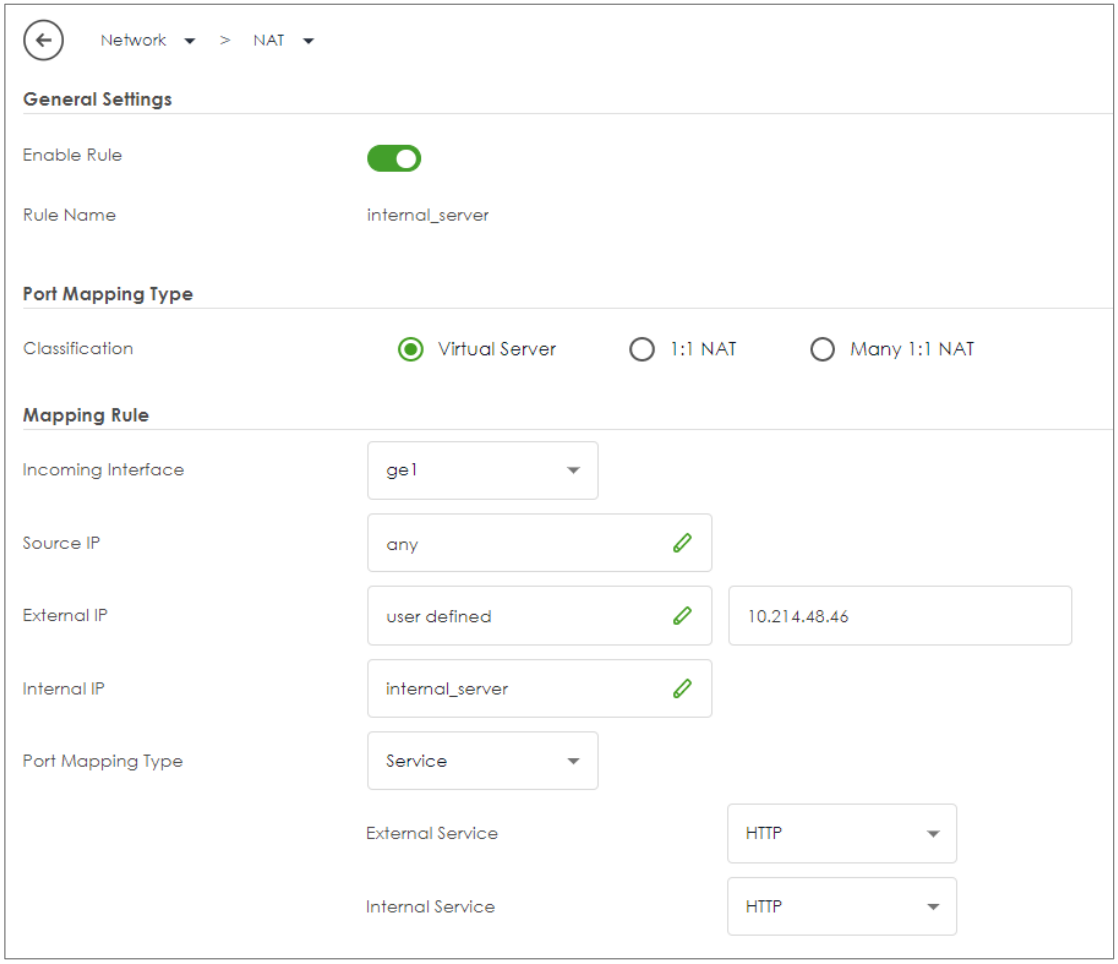
- Configure the External IP. Select Any to choose the ge1 interface IP as the external IP.

- 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.



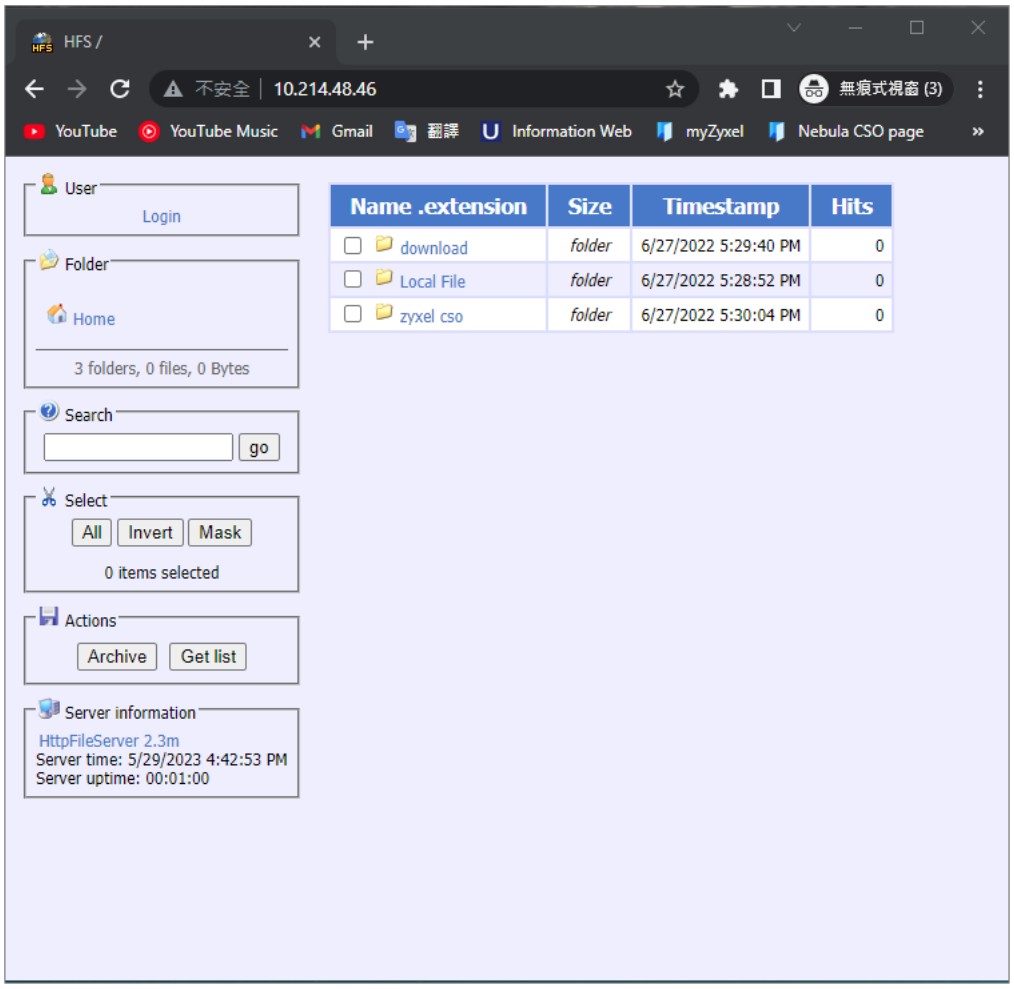
- Port Mapping Type: Select HTTP for both external and internal service.



## Test the Result

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



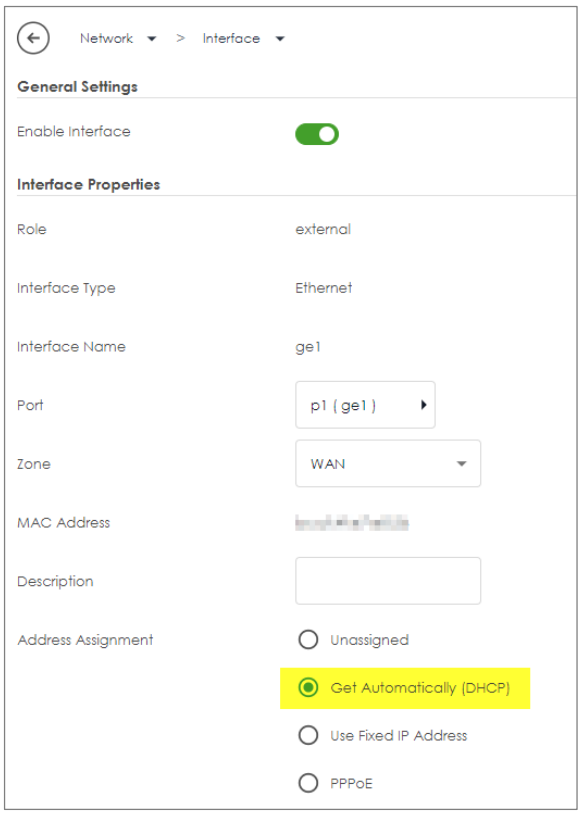

 

# How to Configure DHCP Option 60 – Vendor Class Identifier

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.

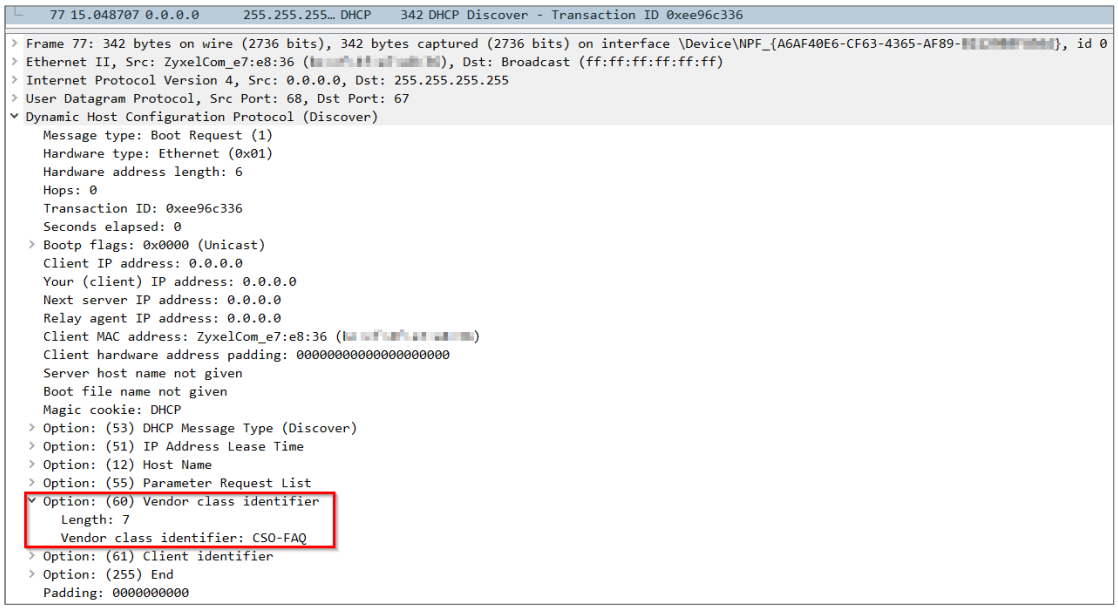


3. Scroll down and expand the Advanced Settings: DHCP Option 60
4. Enter the VCI string in the field of DHCP Option 60, and click **Apply**


## Test DHCP Option 60

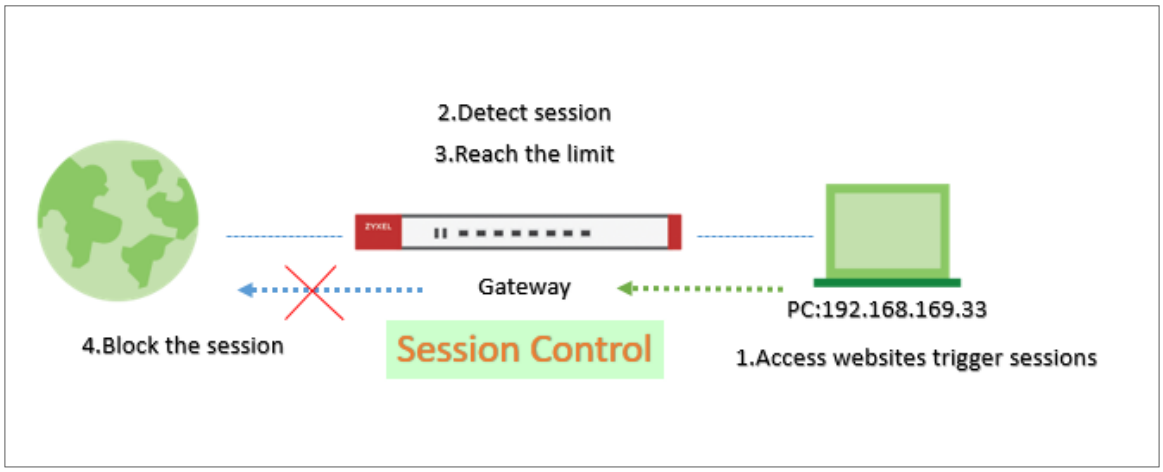
To check the functionality of DHCP Option 60, we can use packet capture software to check if option 60 string exists in the DHCP discover message that is sent from the USG FLEX H.



# How to Configure Session Control

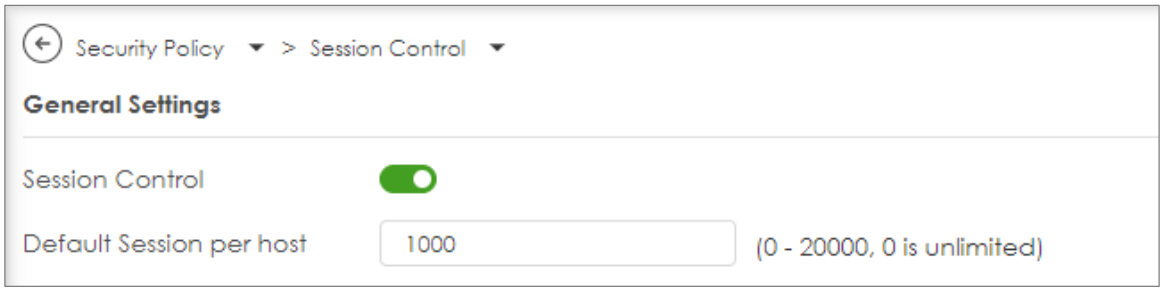
Session control can address abnormal user behavior. By monitoring session activities, the firewall can detect deviations from normal usage, such as sudden traffic spikes or unauthorized access attempts. This proactive approach enables prompt action to be taken to investigate and mitigate potential security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



## Set Up the Session Control

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

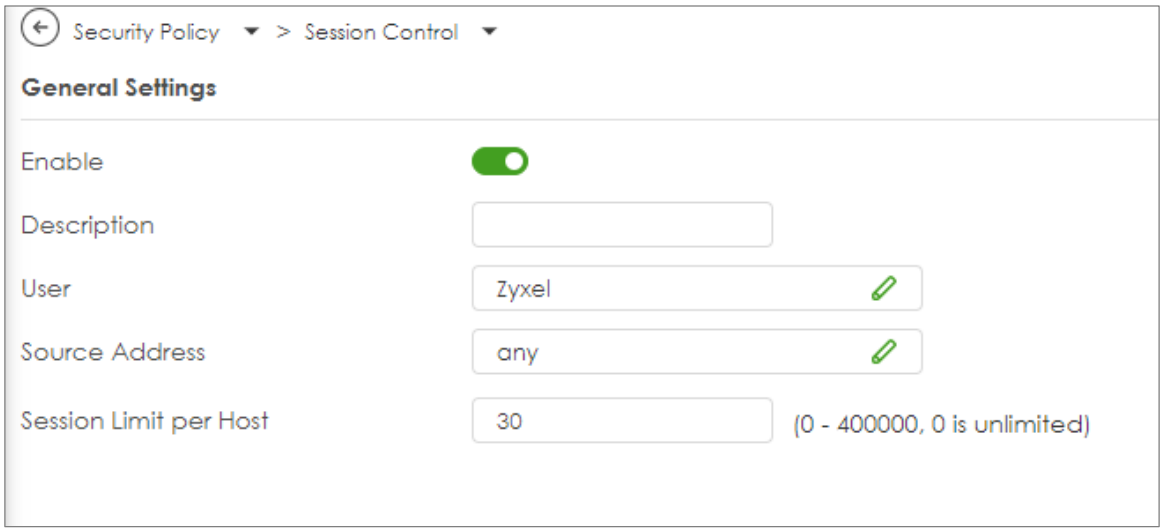



You can field in the value of the Session per hosts you would like to limit.

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


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.

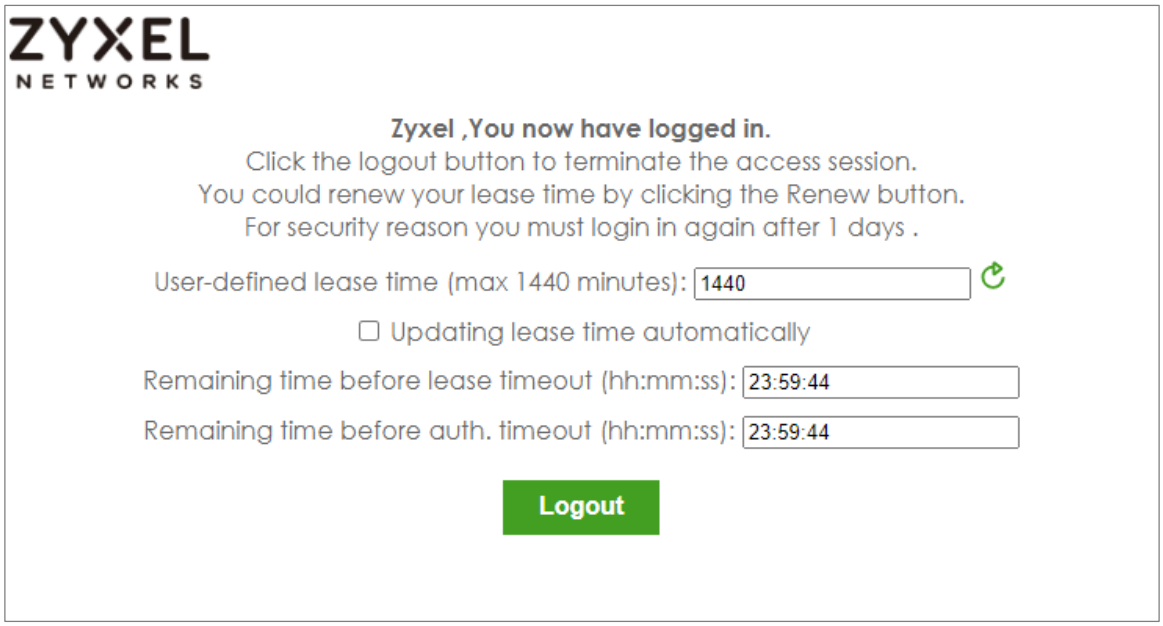




## Test the Result

Log in as User: Zyxel




Try to access web browser to hit the session limit

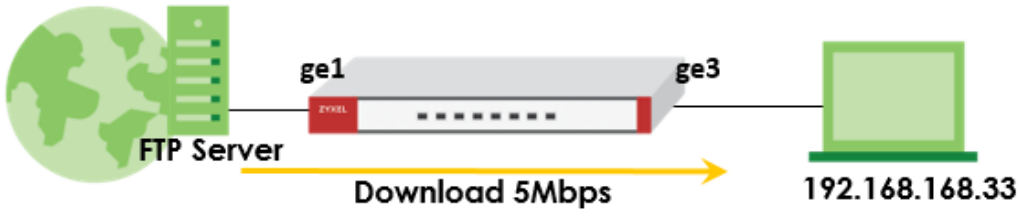
Go to Log & Report > Log/Events and select Session Control to check the logs.

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

# How to Configure Bandwidth Management for FTP Traffic

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

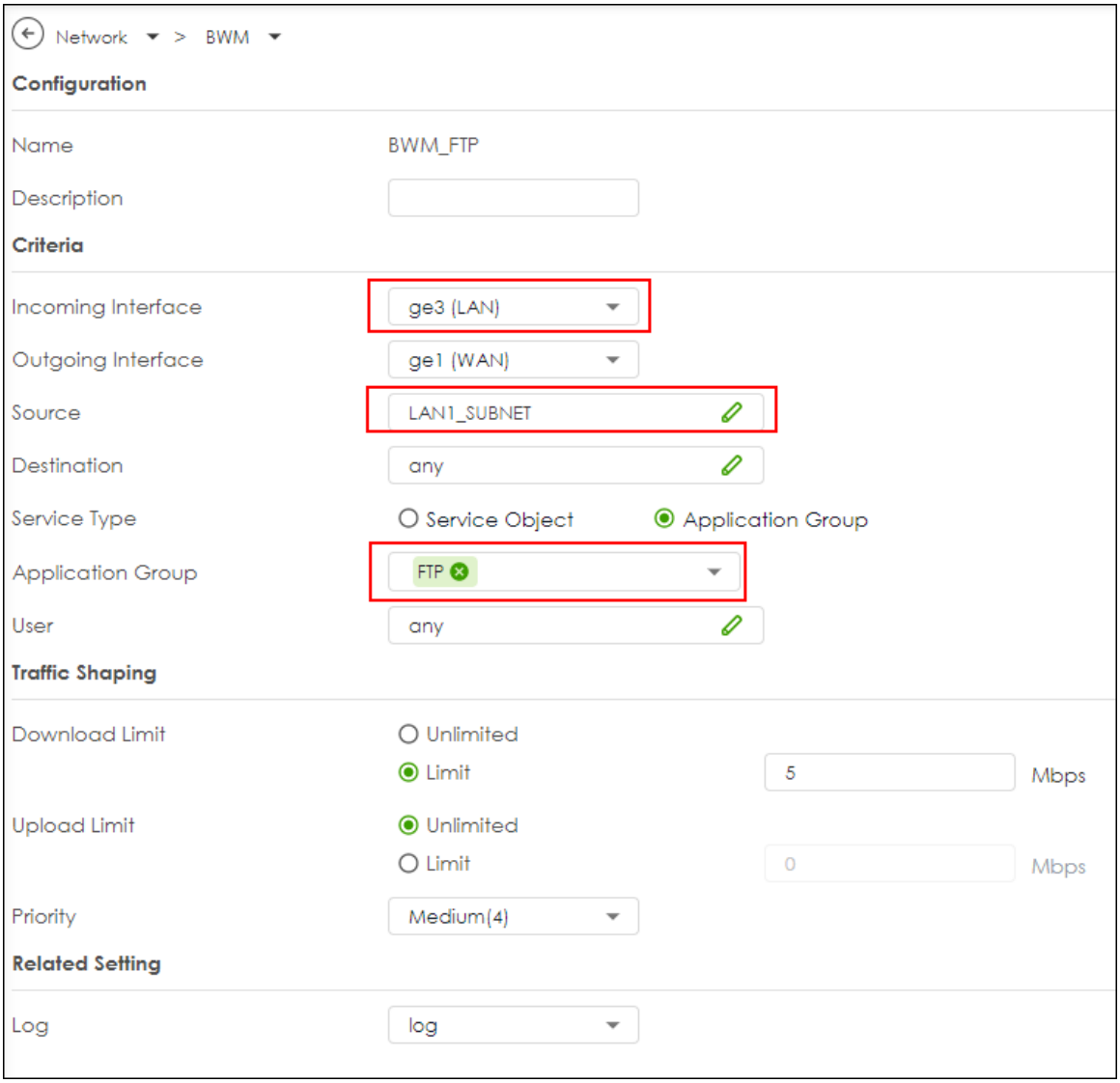



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. The total available bandwidth assumption is 5Mbps. This example was tested using USG FLEX 500H

## Set Up the BWM rule for FTP download.

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



Incoming Interface: ge3

Outgoing Interface: ge1

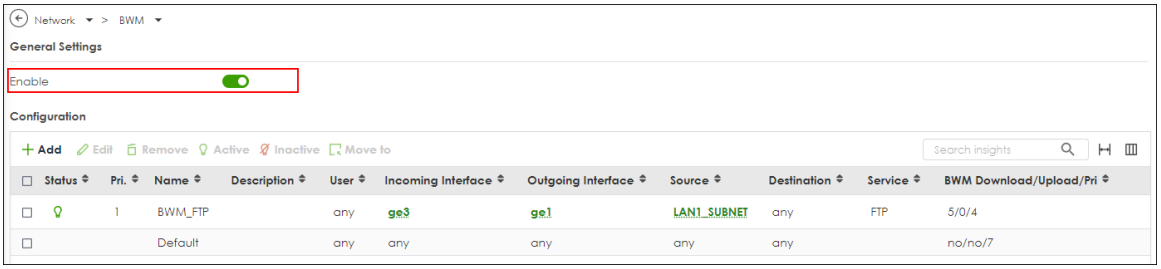
Source: LAN1 IP Subnet

Application Group: FTP

Traffic Shaping: Download Limit 5 Mbps.

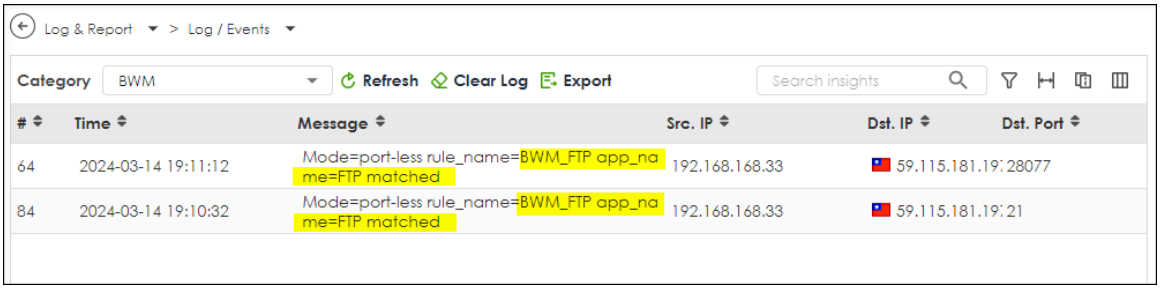
> Note: The terms "incoming interface" and "destination interface" indicate the direction of traffic that the client initiates during a session. The term "Source IP information" denotes the initial IP address. Furthermore, the Application Group function identifies client traffic types based not only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

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




## Test the Result

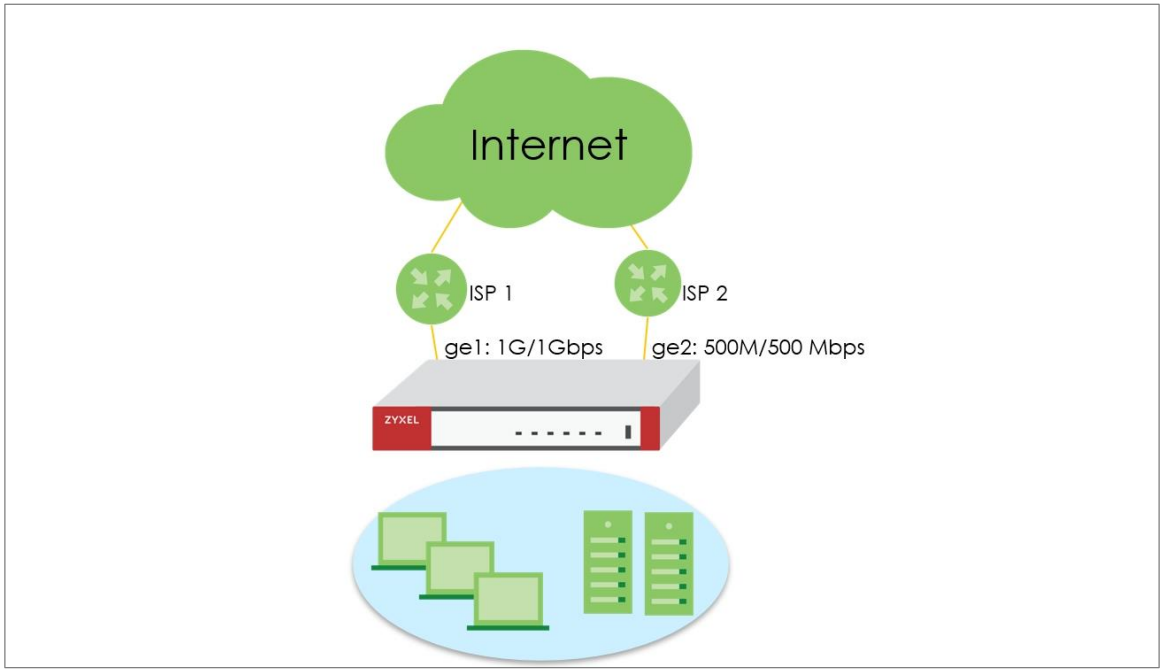
Go to Log & Report > Log/Events and select BWM to check the logs.



# 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**

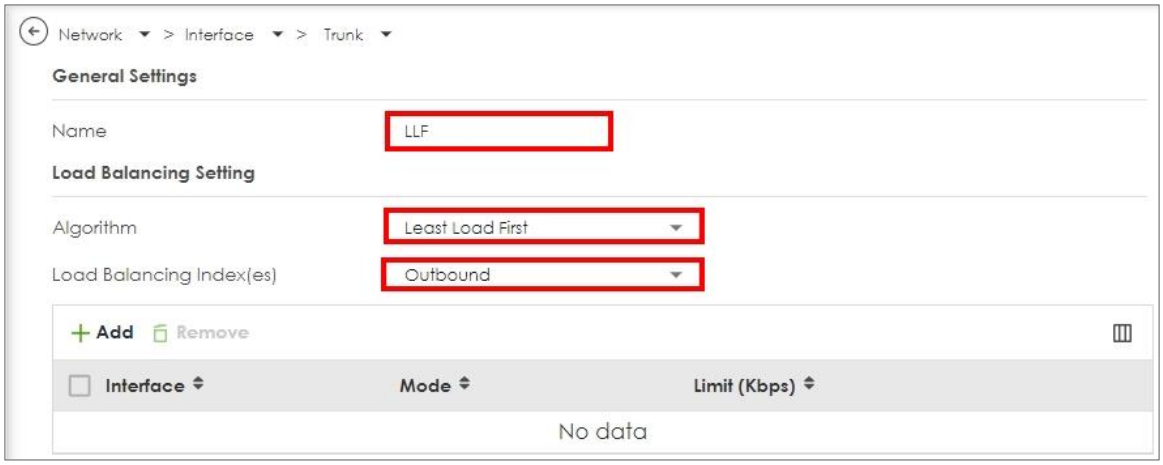
The "Spillover" load balancing algorithm prioritizes the first interface in the trunk member list until its maximum load capacity is reached. Any excess traffic from new sessions is then directed to subsequent interfaces in the list, continuing until all member interfaces are utilized or traffic demands 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.*




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

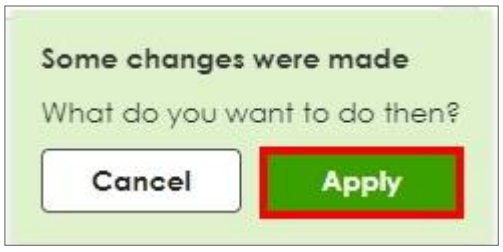
Limit(Kbps): 1024000

Member: ge2(Wan)

Mode: Active

Limit(Kbps): 512000


Click **Apply** to save changes.



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

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

Algorithm: Spillover

Load Balancing Index: Outbound


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

Member: ge1(Wan)

Mode: Active

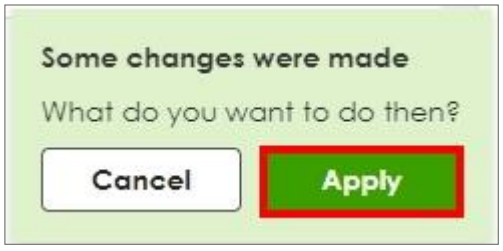
Limit(Kbps): 819200

Member: ge2(Wan)

Mode: Active

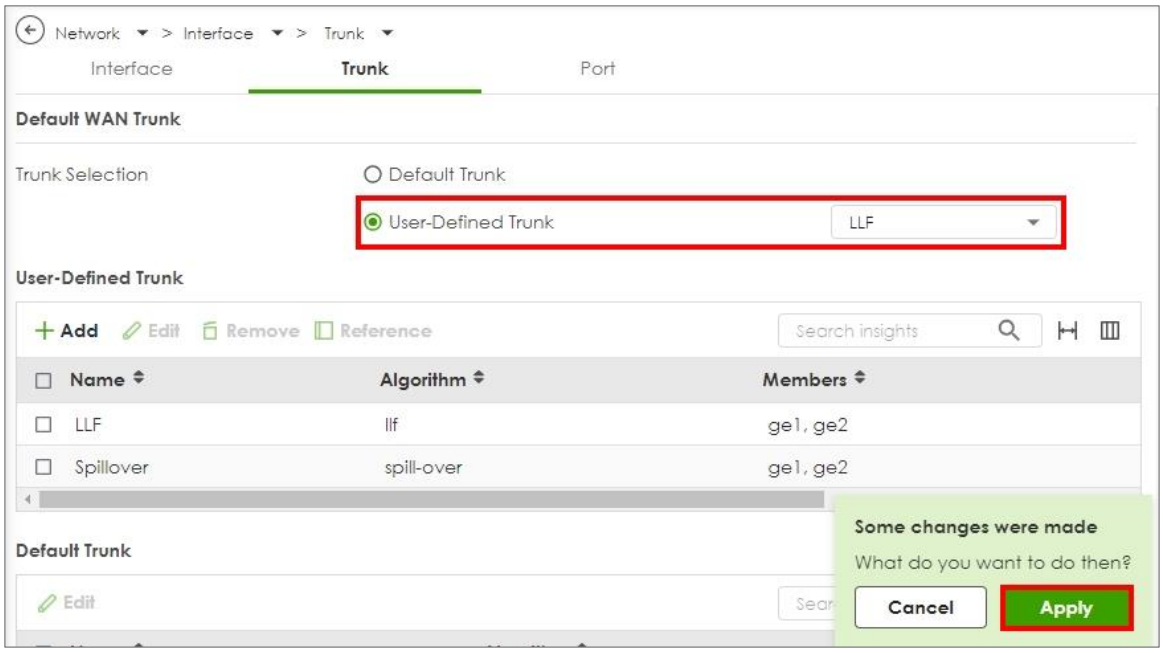
Limit(Kbps): 512000


Click **Apply** to save changes.



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.



## 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.