Implement Hardening Measures for Secure Client AnyConnect VPN

Contents

Introduction

This document describes how to improve the security of your Remote Access VPN implementation.

Prerequisites

Requirements

Cisco recommends you to have knowledge of these topics:

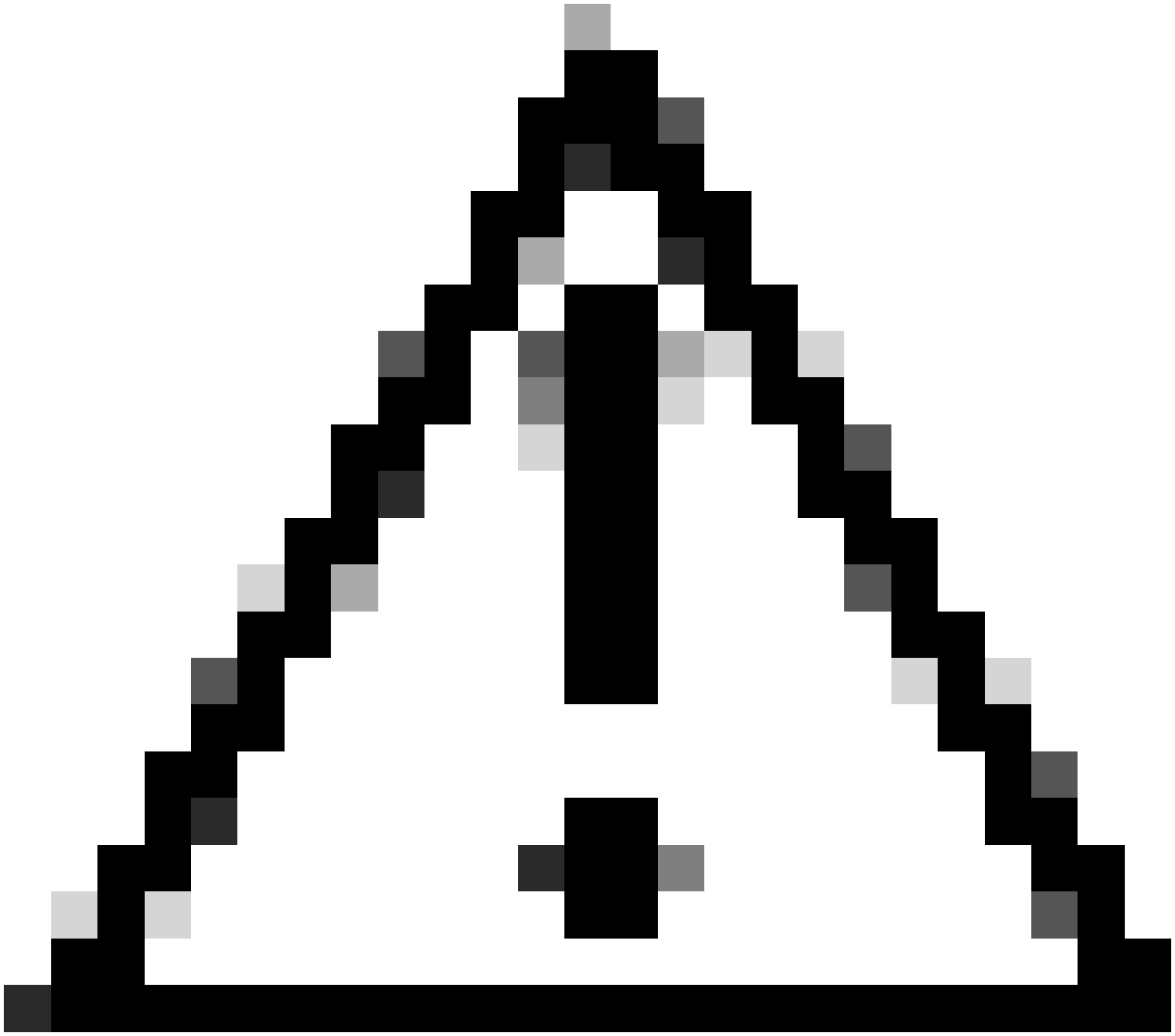
- Cisco Secure Client AnyConnect VPN.
- ASA/FTD remote access configuration.

Components Used

The best practices guide is based on these hardware and software versions:

- Cisco ASA 9.x
- Firepower Threat Defense 7.x / FMC 7.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.



Caution: This document does not contain steps for Firepower Device Manager (FDM). The FDM only supports changing the authentication method on the DefaultWEBVPNGroup. Please use control-plane ACLs, or a custom port in the Remote Access VPN 'Global Settings' section within the FDM UI. Please reach out to Cisco Technical Assistance Center (TAC) for further assistance if needed.

Background Information

The purpose of this document is to ensure the Cisco Secure Client AnyConnect VPN configuration is adhering to security best practices in a modern world where cybersecurity attacks are common.

Brute force attacks usually involve repeated attempts to gain access to a resource by using username and password combinations. Attackers try to use their internet browser, the Secure Client User Interface, or other tools to enter multiple usernames and passwords hoping they match a legitimate combination in a AAA database. When using AAA for authentication we expect the end user to enter their username and password since this is necessary to establish the connection. At the same time, we are not verifying who the user is until they enter their credentials. By nature, this allows attackers to take advantage of these scenarios:

1. Exposed fully qualified domain names for the Cisco Secure Firewall (especially when using a group-aliases in the connection profile):
    - If the attacker discovers the FQDN of your VPN firewall, they then have the option to select the tunnel-group using the group-alias in which they want to start the brute-force attack.

2. Default Connection Profile configured with AAA or Local Database:
    - If the attacker finds the FQDN of the VPN firewall, they can attempt to brute-force attack the AAA server or local database. This occurs because the connection to the FQDN lands on the Default Connection Profile, even if no group-aliases are specified.

3. Resource exhaustion on the firewall or on AAA servers:
    - Attackers can overwhelm AAA servers or firewall resources by sending large amounts of authentication requests and creating a Denial of Service (DoS) condition.

Concepts

Group-Aliases:

- An alternate name by which the firewall can refer to a connection profile. After initiating a connection to the firewall, these names appear in a drop-down menu in the Secure Client UI for users to select. The removal of group-aliases removes the drop-down functionality in the Secure Client UI.

Group-URLs:

- A URL that can be tied to a connection profile so that incoming connections are direcly mapped to a desired connection profile. There is no drop-down functionality, as users can enter the full URL in the Secure Client UI, or the URL can be integrated with a 'Display Name' in the XML profile to hide the URL from the user.

The difference here is when group-aliases are implemented, a user initiates a connection to vpn_gateway.example.com and is presented with aliases to select that drive them to a connection profile. With group-URLs, a user initiates a connection to vpn_gateway.example.com/example_group and that drives them directly to the connection profile without the need or option for a drop-down menu.

Secure Client Hardening Practices on Cisco Secure Firewall:

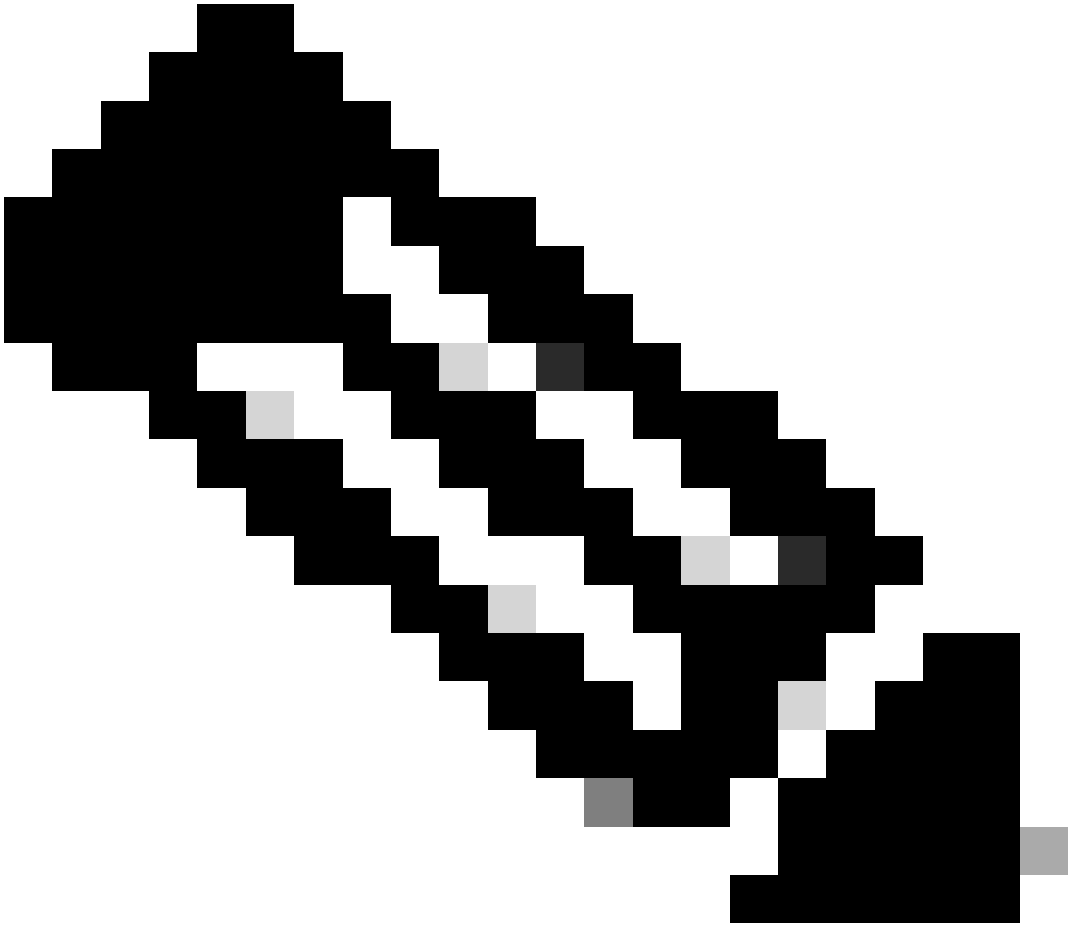
These methods rely on mapping legitimate users to proper tunnel-groups/connection profiles while potentially malicious users are sent to a trap tunnel-group that we configure to not allow username and password combinations. Though not all combinations must be implemented, disabling group-aliases and changing the authentication method of the DefaultWEBVPNGroup and DefaultRAGroup are required for the recommendations to work effectively.

- Remove group aliases and only use group-url in the Connection Profile configuration, this allows you to have a specific FQDN that is not going to be easy for an attacker to discover and select since only the clients with the proper FQDN are able to initiate the connection. For example vpn_gateway.example.com/example_group is harder for an attacker to discover than vpn_gateway.example.com.

- Disable AAA authentication in the DefaultWEBVPNGroup and DefaultRAGroup and configure certificate authentication, this avoids a possible brute-force against the local database or AAA server. The attacker in this scenario would be presented with immediate errors upon attempting to connect. There is no username or password field since the authentication is based on certificates, thus stopping brute force attempts. Another option is to create a AAA server with no supporting configuration to create a sinkhole for malicious requests.

- Utilize certificate-mapping for the connection profile. This allows incoming connections to be mapped to specific connection profiles based on attributes received from certificates on the client device. Users who have the proper certificates are mapped correctly, while attackers who fail the mapping criteria are sent to the DefaultWEBVPNGroup.

- The usage of IKEv2-IPSec instead of SSL causes tunnel-groups rely to on a specific user-group mapping in the XML profile. Without this XML on the end user machine, users are automatically sent to the default tunnel-group.



Note: For a more information regarding the group-alias functionality, see ASA VPN Configuration Guide and observe 'Table 1. Connection Profile Attributes for SSL VPN'.

Identify Attacks using Logging and Syslog IDs

Brute-force attacks represent the predominant method of compromising Remote Access VPNs, exploiting weak passwords to gain unauthorized entry. It is crucial to know how to recognize signs of an attack by leveraging the use of logging and evaluating syslogs. Common syslogs IDs that can indicate an attack if encountered with abnormal volume are:

%ASA-6-113015

<#root>

%ASA-6-113015

: AAA user authentication Rejected : reason = User was not found : local database : user = admin : user

%ASA-6-113005

<#root>

%ASA-6-113005

: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = ***** : user IP =

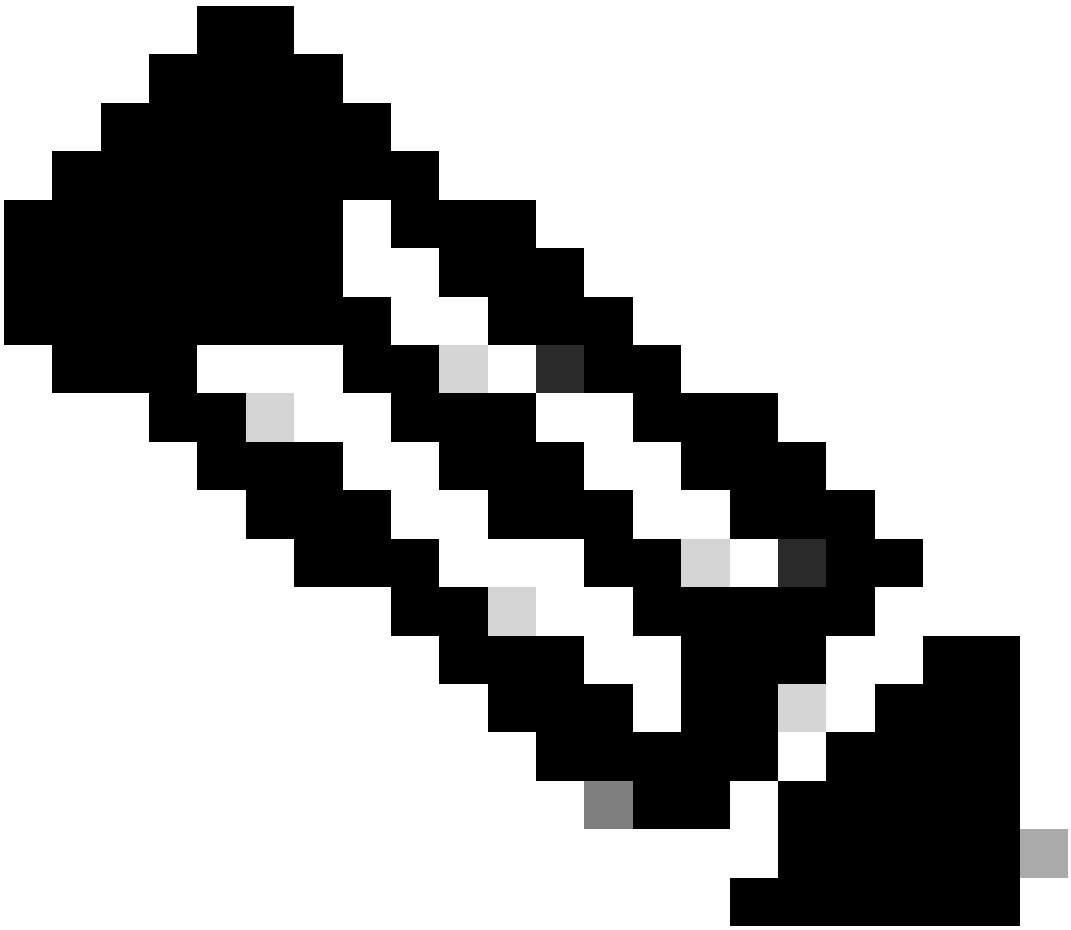
%ASA-6-716039

<#root>

%ASA-6-716039

: Group <DfltGrpPolicy> User <admin> IP <x.x.x.x> Authentication: rejected, Session Type: WebVPN

The username is always hidden until the **no logging hide username** command is configured on ASA.



Note: Note: This provides insight if valid users are generated or known by offending IPs however, please be cautious as usernames are visible in the logs.

Cisco ASA Logging:
Logging chapter of the Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide

Cisco FTD Logging:

Configure Logging on FTD via FMC

Configure Syslog section in the Platform Settings chapter of the Cisco Secure Firewall Management Center Device Configuration Guide
Configure and Verify Syslog in Firepower Device Manager
Configuring System Logging Settings section in the System Settings chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager

Attack Verification

To verify, log in to the ASA or FTD Command Line Interface (CLI), run the show aaa-server command and investigate for an unusual number of attempted and rejected authentication requests to any of the configured AAA servers:

<#root>

ciscoasa#

show aaa-server

```
Server Group: LOCAL - - - - - >>>> Sprays against the LOCAL database
Server Protocol: Local database
Server Address: None
Server port: None
Server status: ACTIVE, Last transaction at 16:46:01 UTC Fri Mar 22 2024
Number of pending requests 0
Average round trip time 0ms
Number of authentication requests 8473575 - - - - - >>>> Unusual increments
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 0
Number of rejects 8473574 - - - - - >>>> Unusual increments
```

<#root>

ciscoasa#

show aaa-server

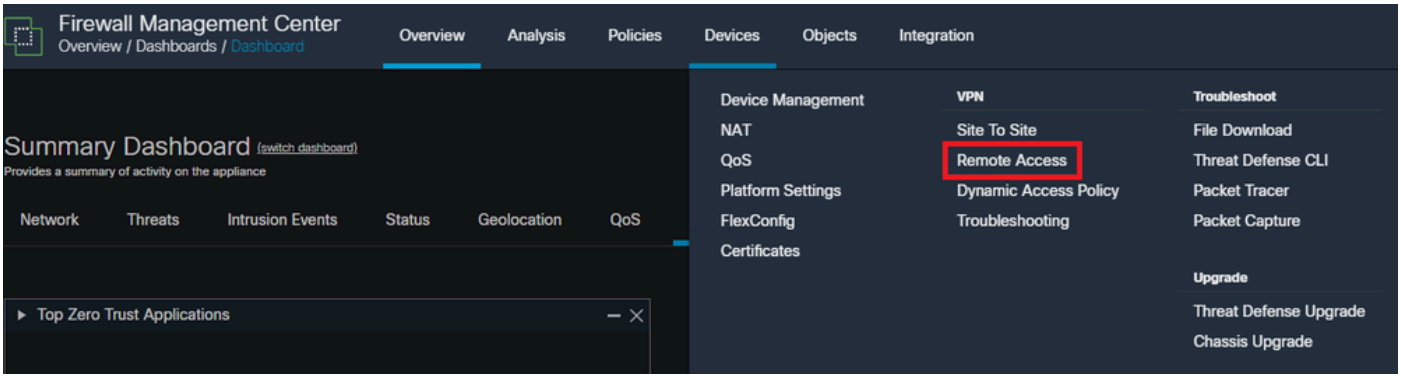
```
Server Group: LDAP-SERVER - - - - - >>>> Sprays against the LDAP server
```

```
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.10.10.10
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms
Number of authentication requests 2228536 - - - - - >>>> Unusual increments
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 1312
Number of rejects 2225363 - - - - - >>>> Unusual increments
Number of challenges 0
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 1
Number of unrecognized responses 0
```

FMC Configuration Examples

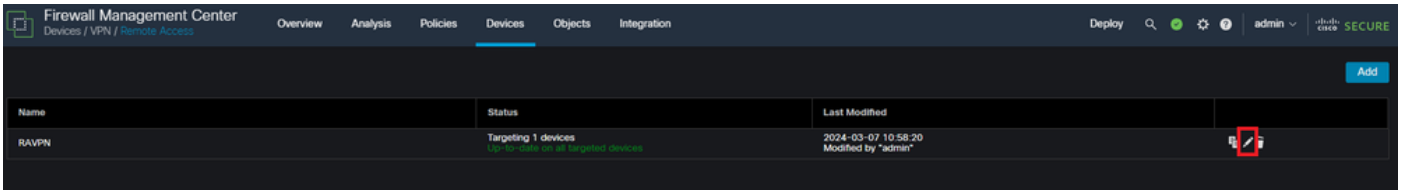
Disable AAA Authentication in the DefaultWEBVPNGroup and DefaultRAGroup Connection Profiles

Navigate to **Devices > Remote Access**.



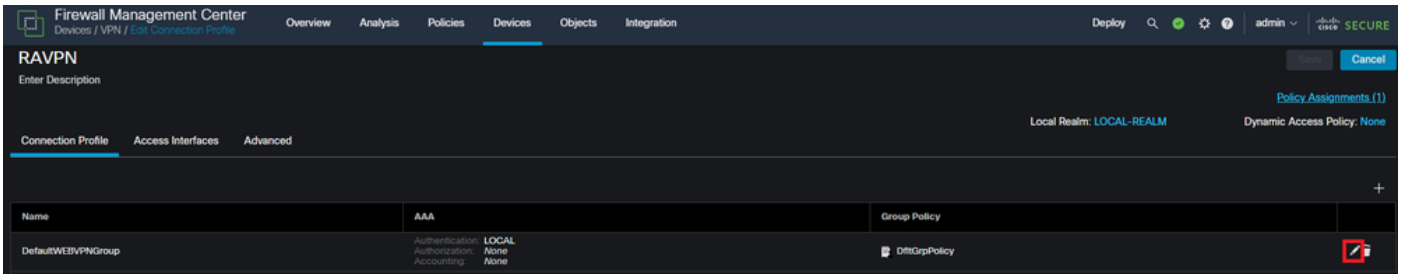
Displays navigating the FMC GUI to get to the Remote Access VPN Policy configuration.

Edit the existing Remote Access VPN Policy and create a connection profile named 'DefaultRAGroup'



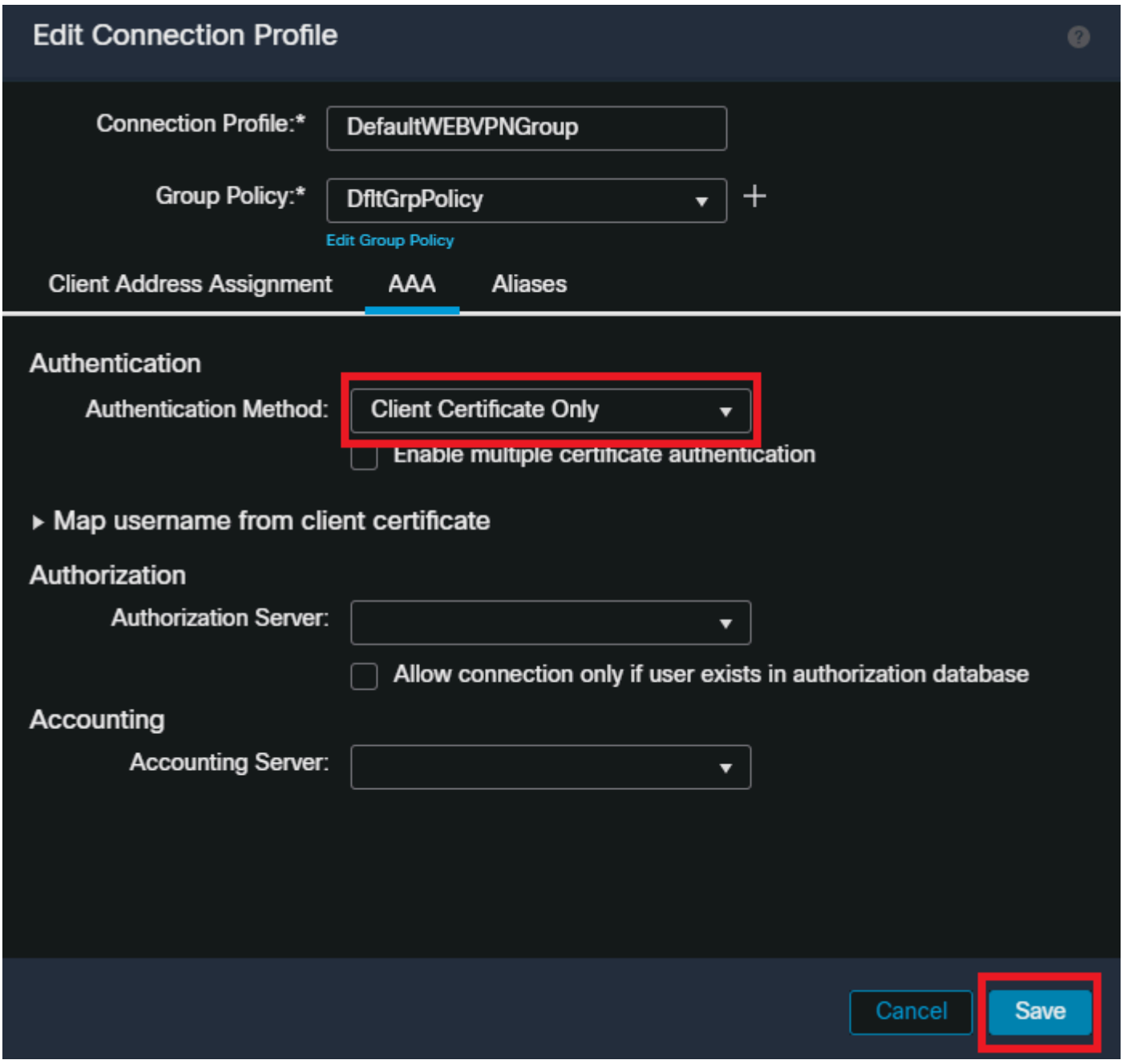
Displays how to edit the Remote Access VPN Policy within the FMC UI..

Edit the connection profiles named 'DefaultWEBVPNGroup' and 'DefaultRAGroup'



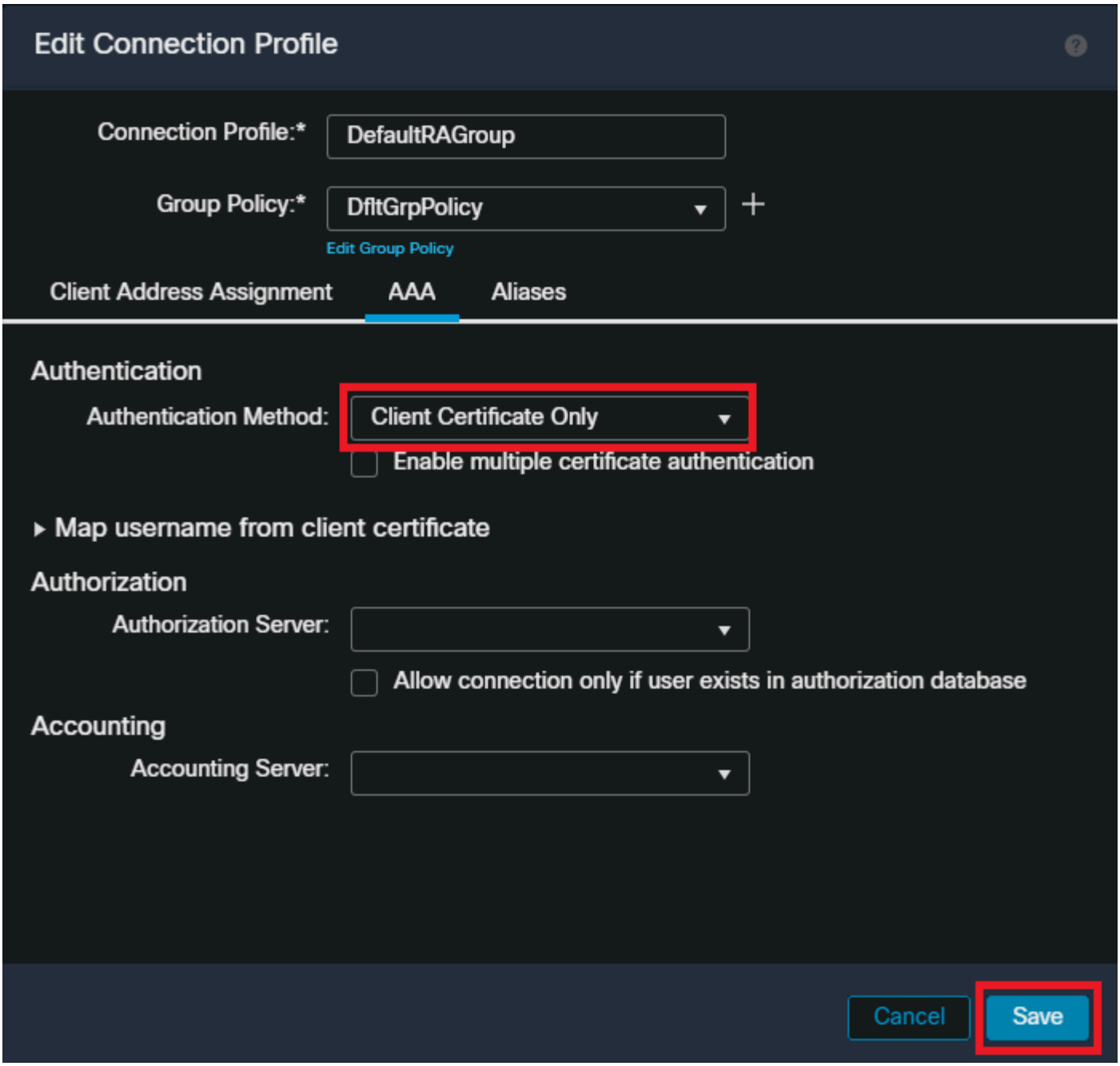
Displays how to edit the DefaultWEBVPNGroup within the FMC UI.

Navigate to the **AAA** tab and select the **Authentication Method** dropdown. Select '**Client Certificate Only**' and select **Save**.

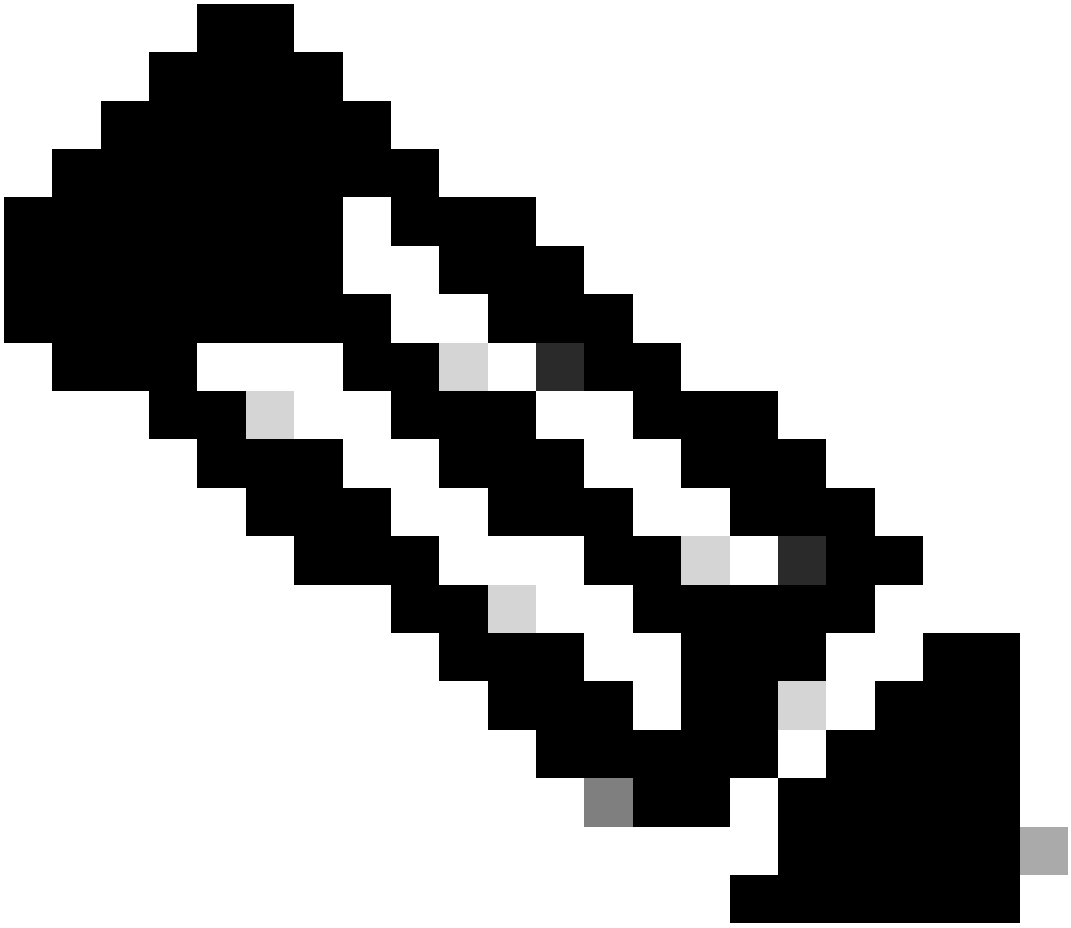


Changing the authentication method to client certificate only for the DefaultWEBVPNGroup within the FMC UI.

Edit the DefaultRAGroup and Navigate to the **AAA** tab and select the **Authentication Method** dropdown. Select **'Client Certificate Only'** and select **Save**.



Changing the authentication method to client certificate only for the DefaultRAGroup within the FMC UI.

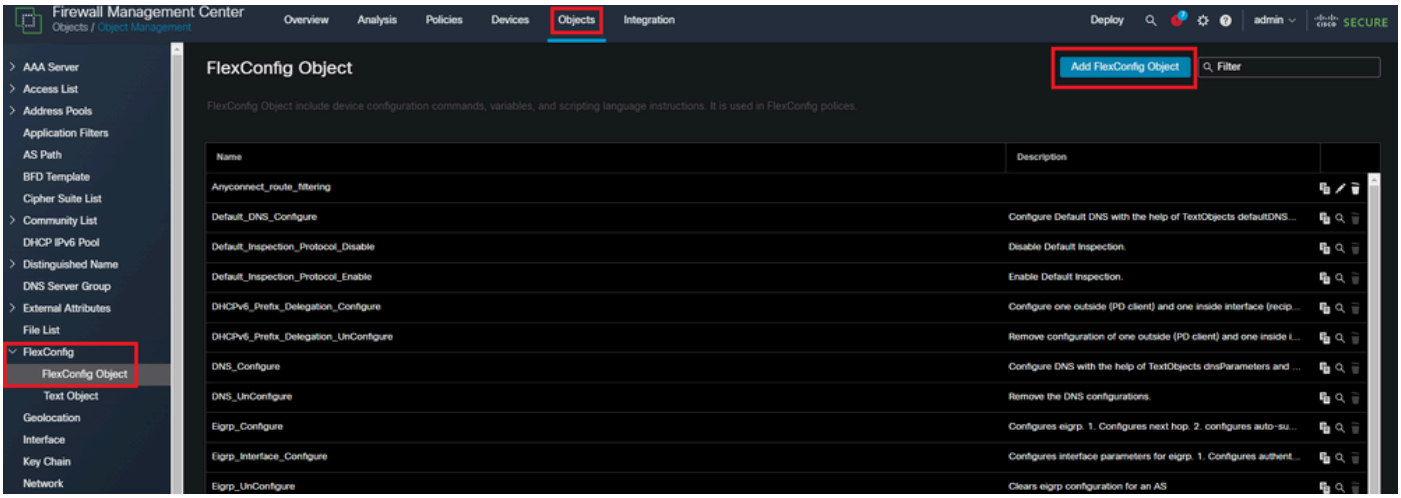


Note: The authentication method can also be a sinkhole AAA server. If this method is used, the AAA server configuration is fake, and does not actually process any requests. A VPN pool must also be defined in the 'Client Address Assignment' tab to save the changes.

Disable Hostscan / Secure Firewall Posture on the DefaultWEBVPNGroup and DefaultRAGroup (optional)

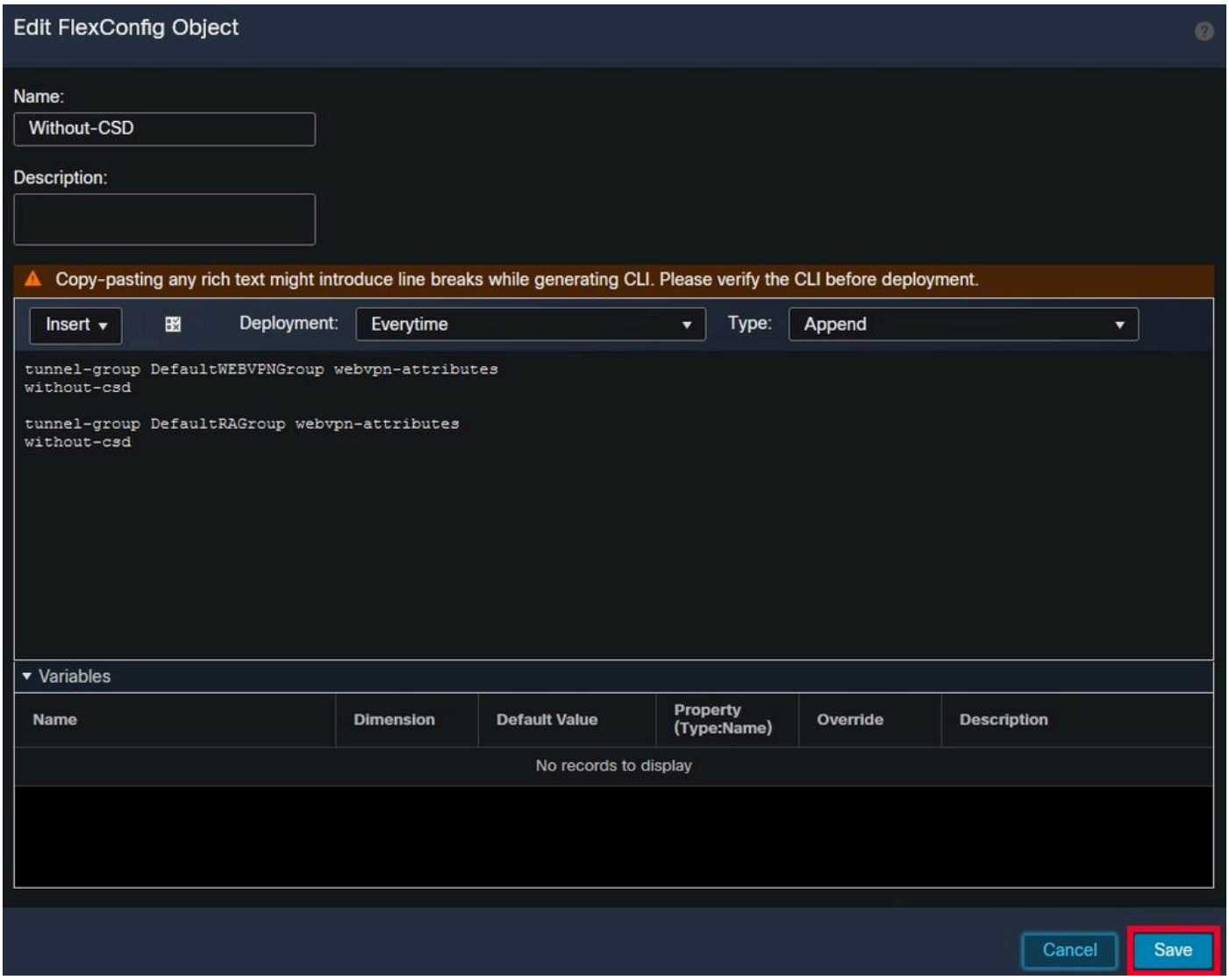
This is only necessary if you have Hostscan / Secure Firewall Posture in your environment. This step prevents attackers from increasing the resource utilization on the firewall caused by the endpoint scanning process. In the FMC, this is achieved by creating a FlexConfig object with the command **without-csd** to disable the endpoint scanning functionality.

Navigate to Objects > Object Management > FlexConfig Object > Add FlexConfig Object.



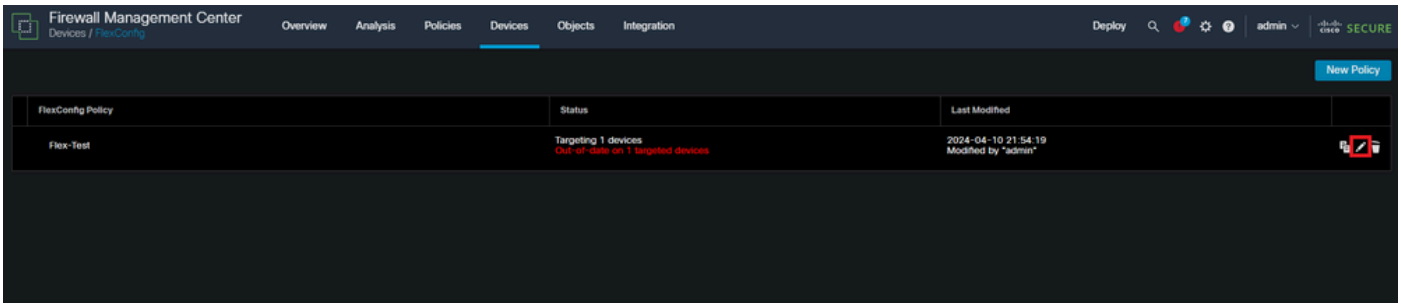
Navigating the FMC UI to create a FlexConfig object.

Name the FlexConfig object, set the deployment to **Everytime** with the type **Append**. Then, enter the syntax exactly as shown and save the object.



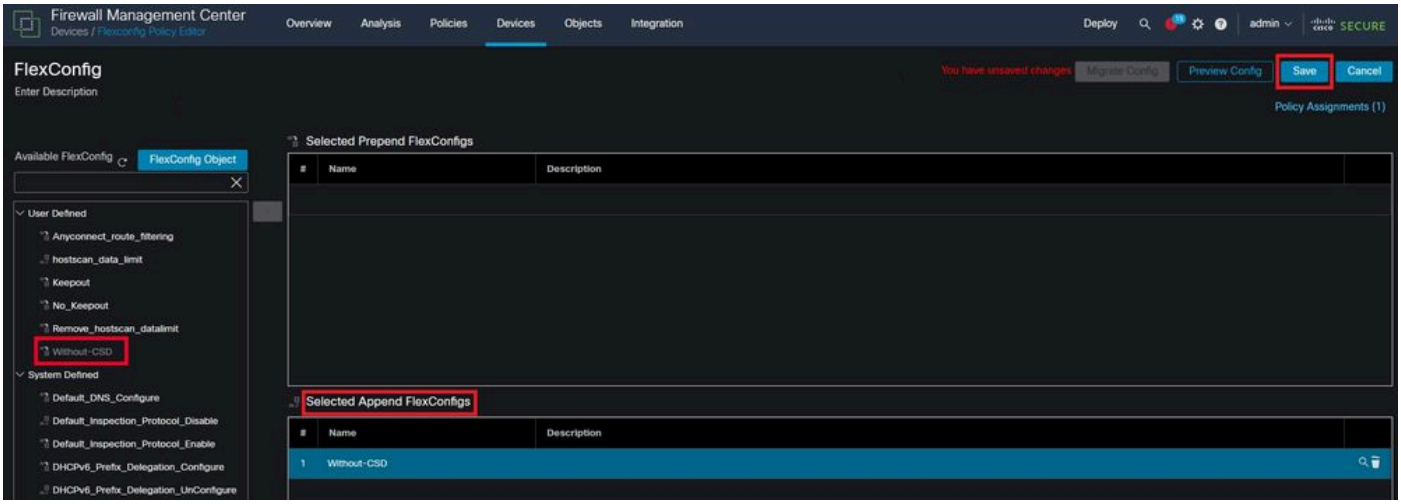
Creating a FlexConfig object with 'without-csd'

Navigate to **Devices** > **FlexConfig** and then click the **Pencil** to edit the FlexConfig Policy.



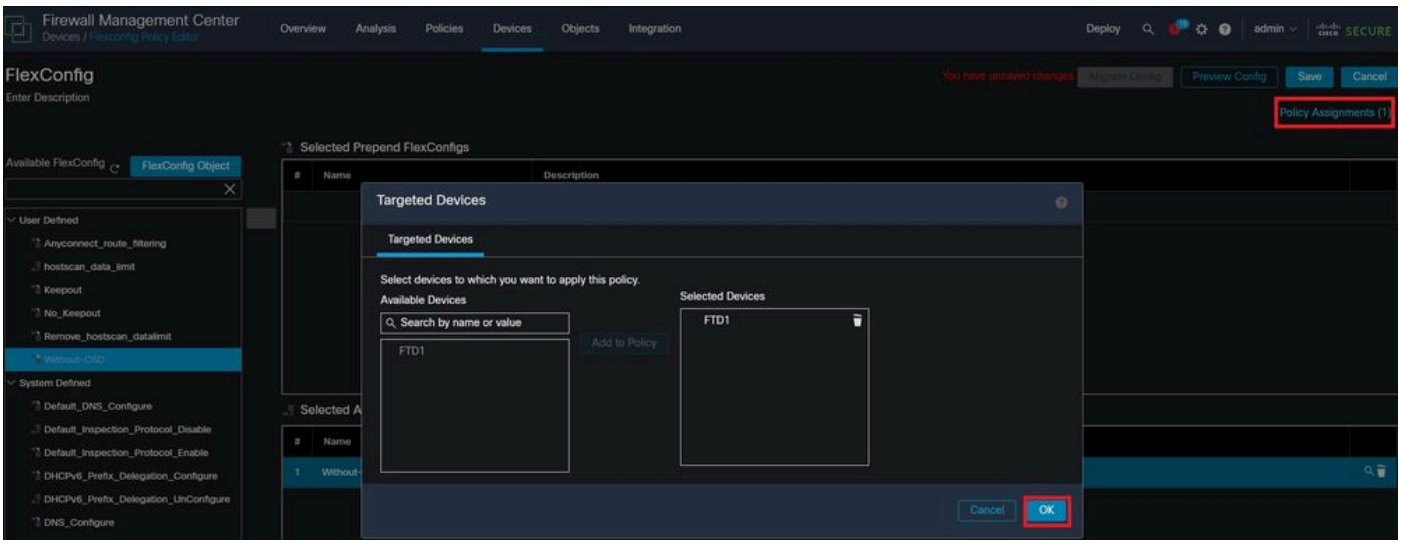
Editing the FlexConfig policy within the FMC.

Locate the object you created from the **User Defined** section. Then, select the arrow to add it to the **Selected Append FlexConfigs**. Lastly, select **Save** to save the FlexConfig policy.



Attach the FlexConfig object to the FlexConfig Policy.

Select **Policy Assignments** and choose the FTD you want to apply this FlexConfig policy to, then select **OK**. Select **Save** again if this is a new FlexConfig assignment and deploy the changes. Once deployed, verify



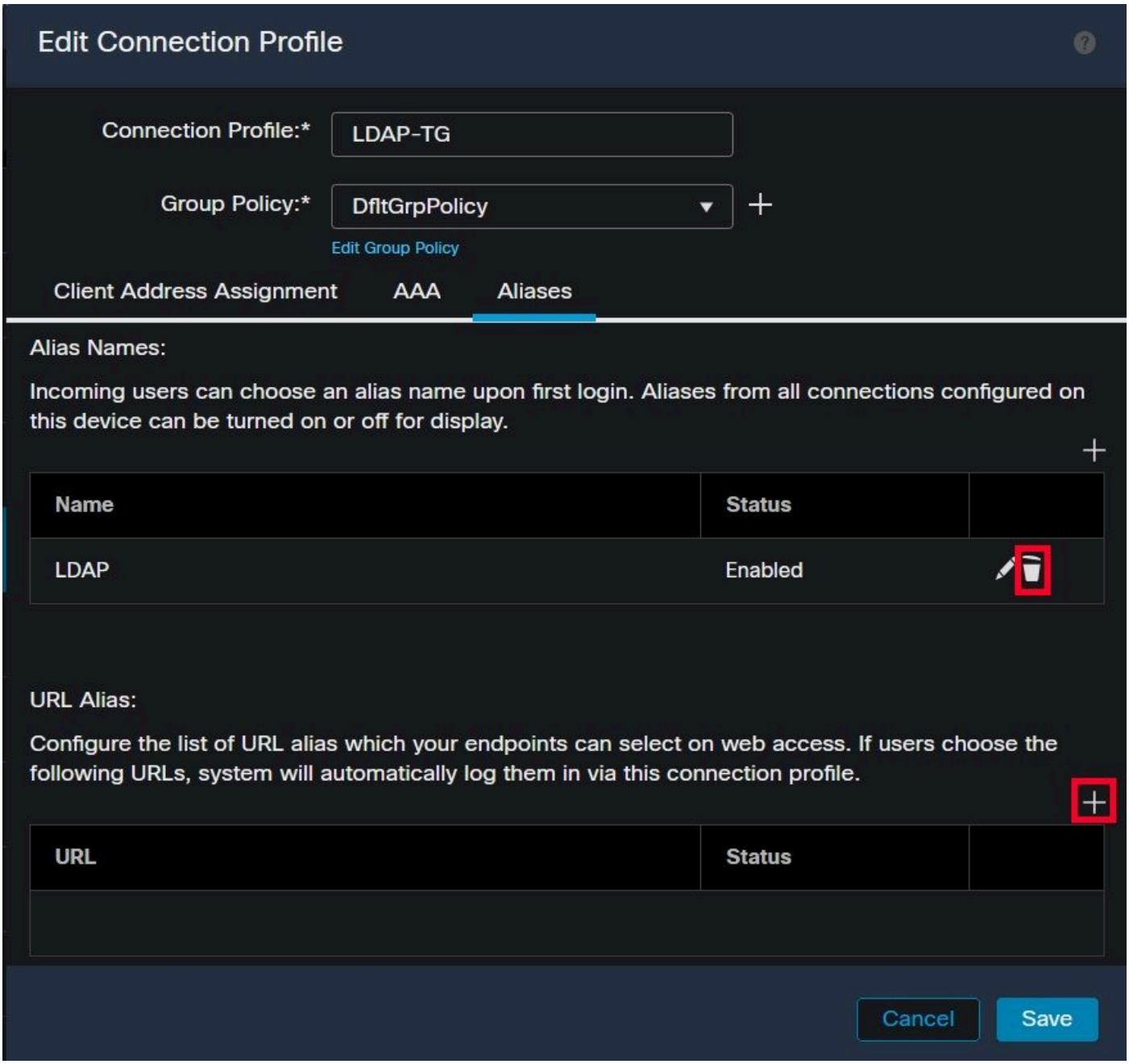
Assign the FlexConfig Policy to a FirePOWER device.

Enter the FTD CLI and issue the command **show run tunnel-group** for the DefaultWEBVPNGroup and DefaultRAGroup. Verify that **without-csd** is now present in the configuration.

```
<#root>

FTD72#

show run tunnel-group DefaultRAGroup


tunnel-group DefaultRAGroup general-attributes
address-pool TEST-POOL
tunnel-group DefaultRAGroup webvpn-attributes
authentication certificate

without-csd



FTD72#

show run tunnel-group DefaultWEBVPNGroup


tunnel-group DefaultWEBVPNGroup general-attributes
address-pool TEST-POOL
tunnel-group DefaultWEBVPNGroup webvpn-attributes
authentication certificate

without-csd
```

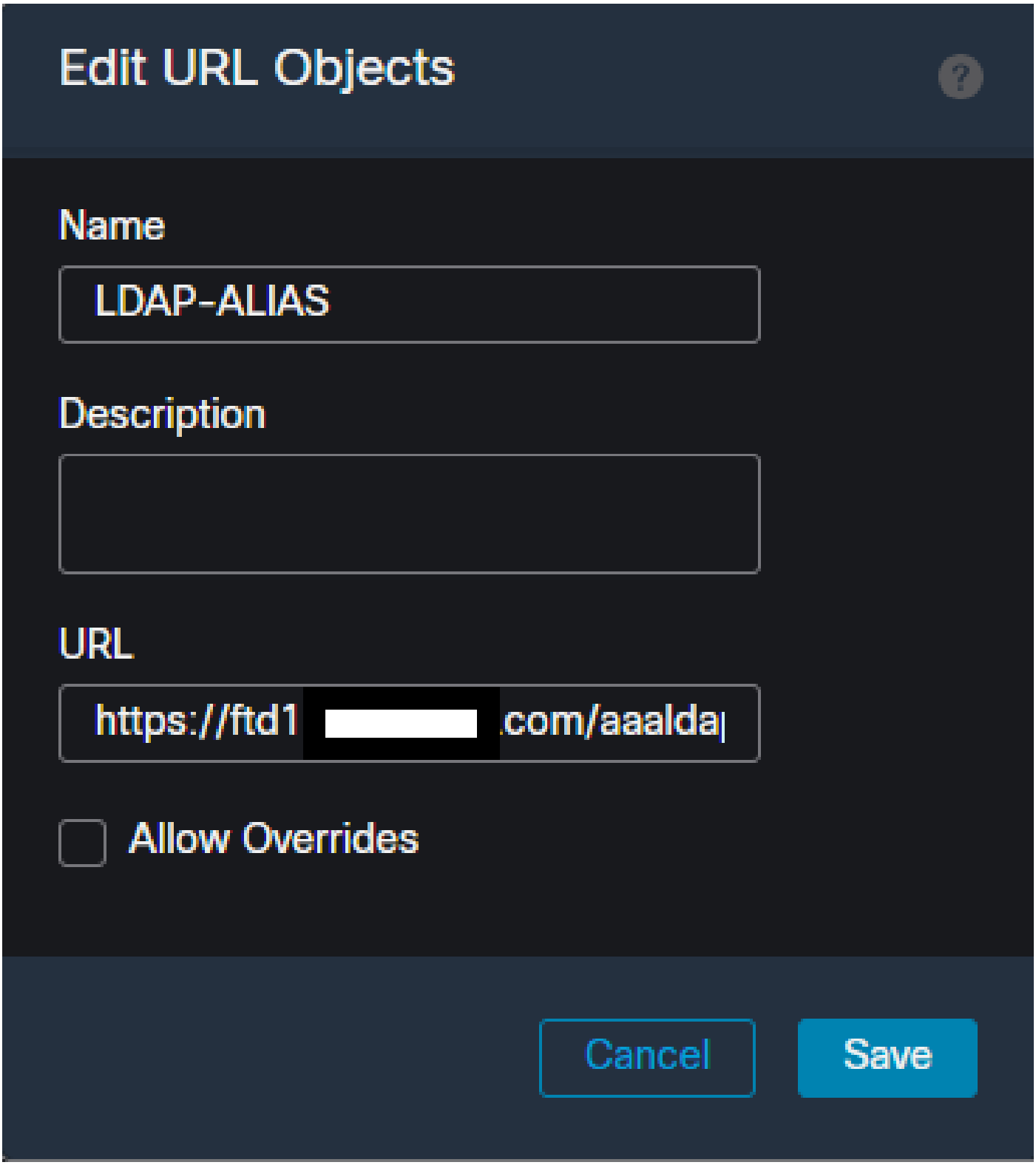
Remove Group-aliases and Enable Group-URLs

Navigate to a connection profile and select the '**Aliases**' tab. Delete the group-alias, and click the **plus** icon to add a URL alias.



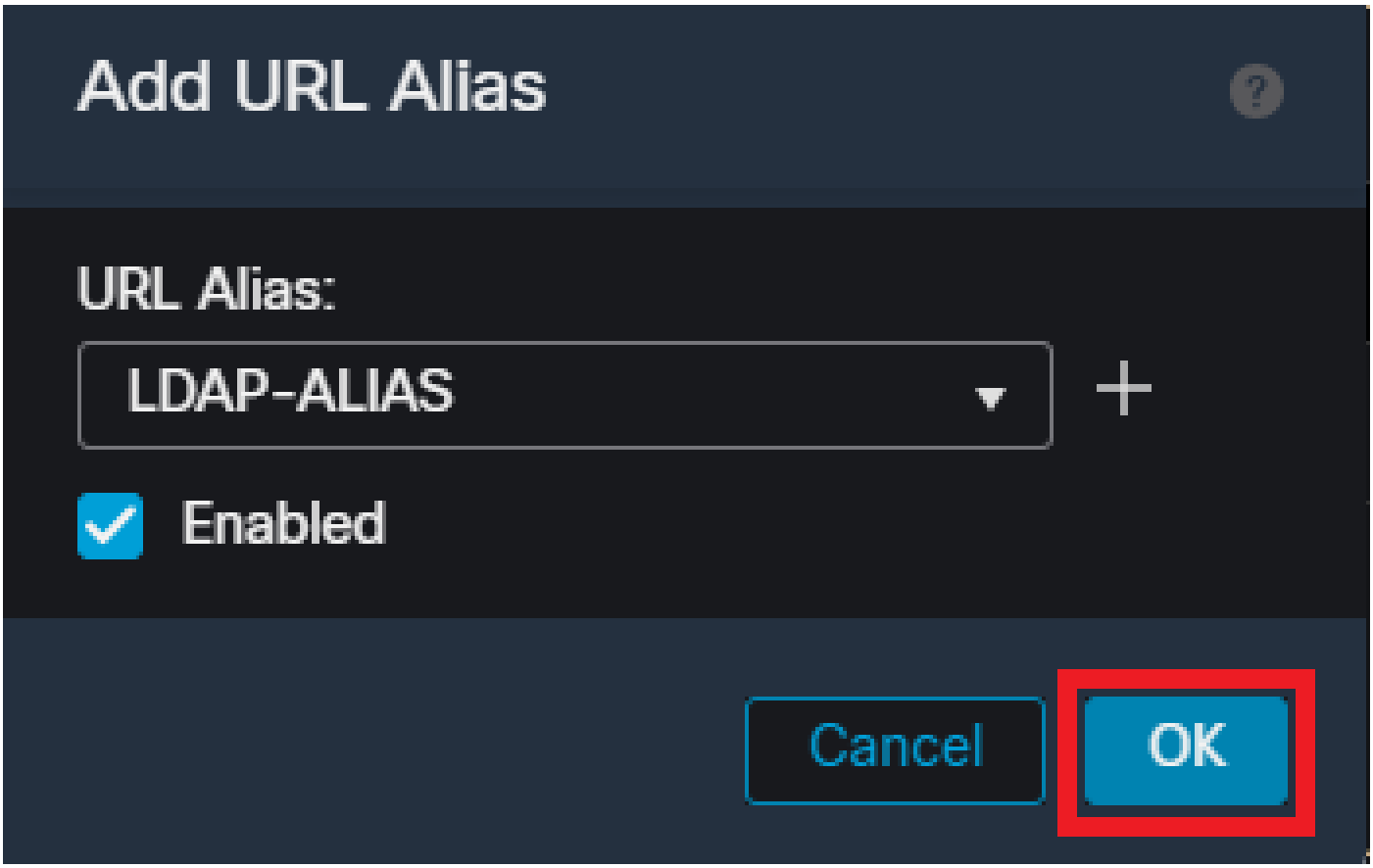
Deleting the group-alias option for a tunnel-group within the FMC UI.

Configure an object name for the URL alias, and fill out the FQDN and/or IP address of the firewall for the URL, followed by the name you want to associate the connection profile with. In this example, we chose 'aaaldap'. The more obscure, the more secure, as it is less likely for attackers to guess the full URL even if they have obtained your FQDN. Once finished, select **Save**.



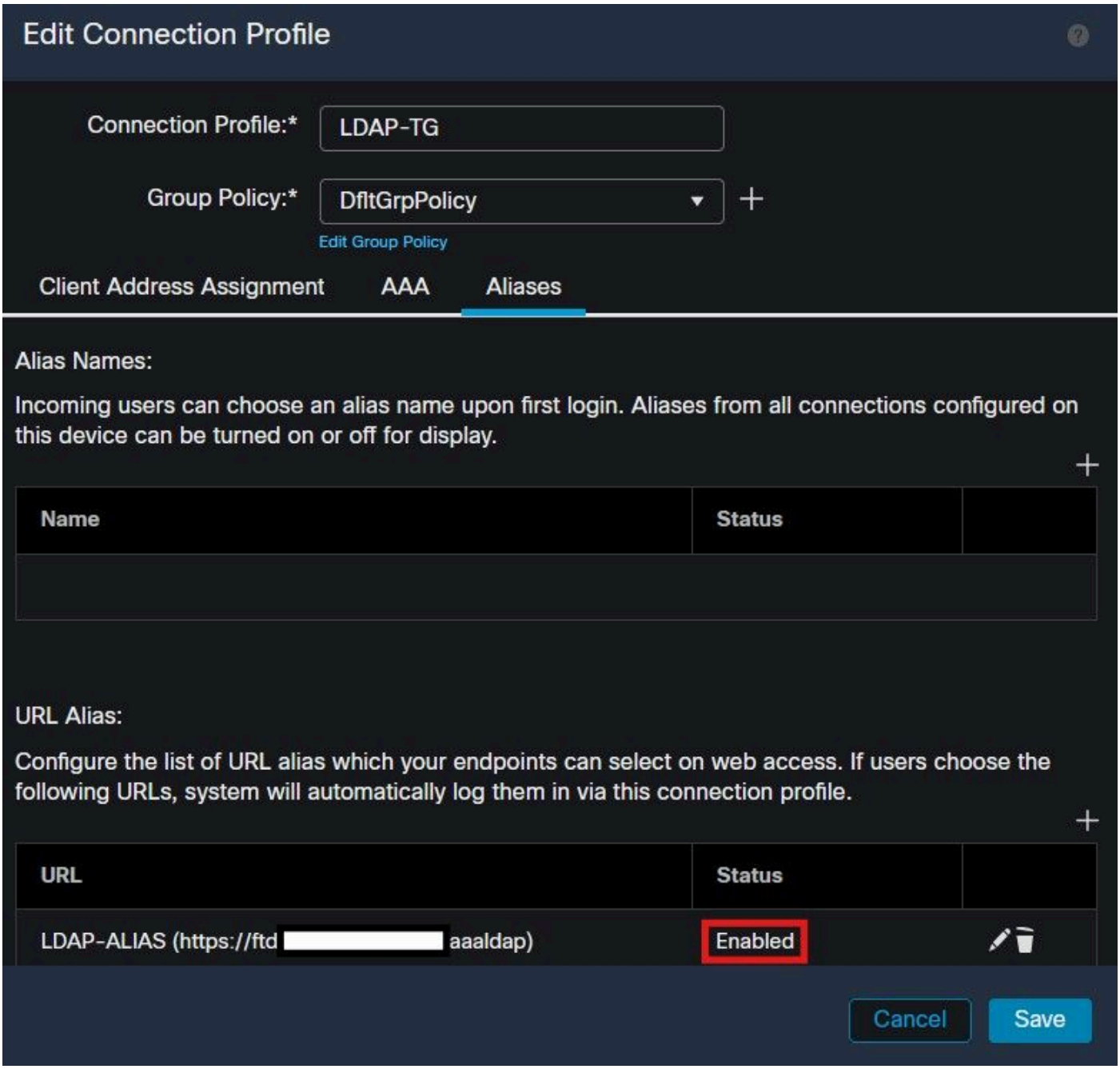
Creating a URL-Alias object within the FMC UI.

Select the URL Alias from the dropdown, check the **Enabled** box and select **OK.**



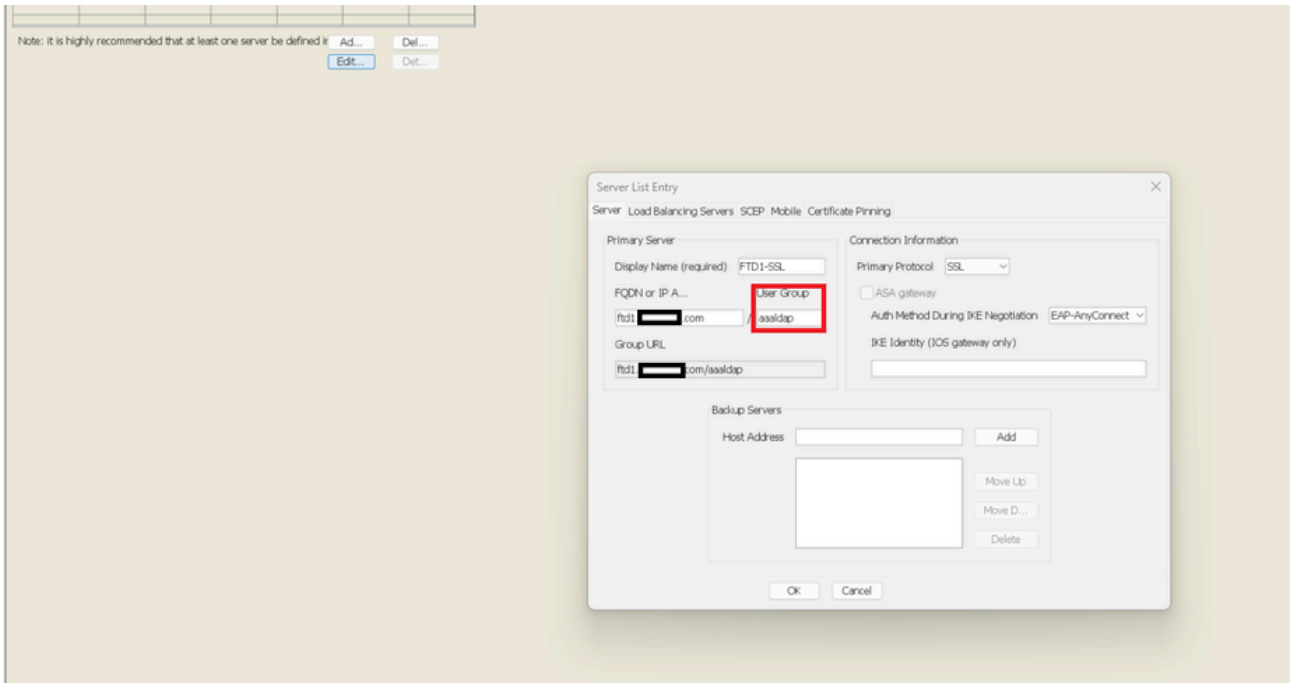
Ensure the URL-Alias is enabled within the FMC UI.

Ensure the group-alias is deleted and check that your URL Alias is now enabled then select **Save**.



Enabling the URL-Alias option for a tunnel-group within the FMC UI.

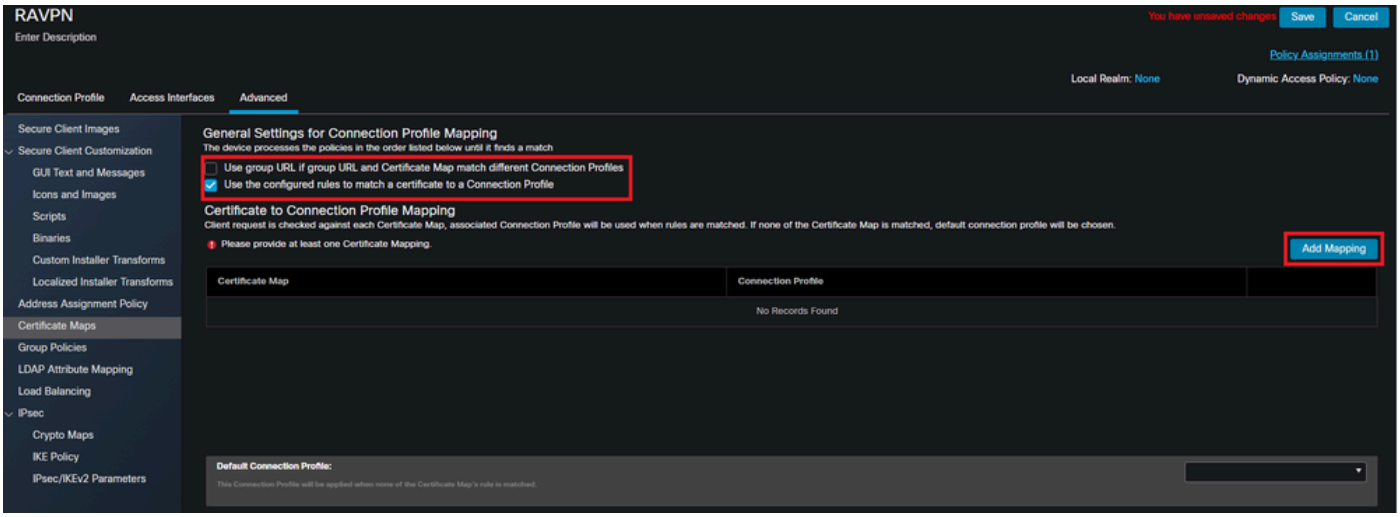
If desired, URL Aliases can also be pushed as part of the XML. This is achieved by editing the XML using the VPN Profile Editor or the ASA Profile Editor. To accomplish this, navigate to the Server List tab and ensure the User Group field matches the URL Alias of the connection profile when using SSL. For IKEv2, ensure the User Group field matches the exact name of the connection profile.



Editing the XML profile to have a URL-Alias for SSL connections.

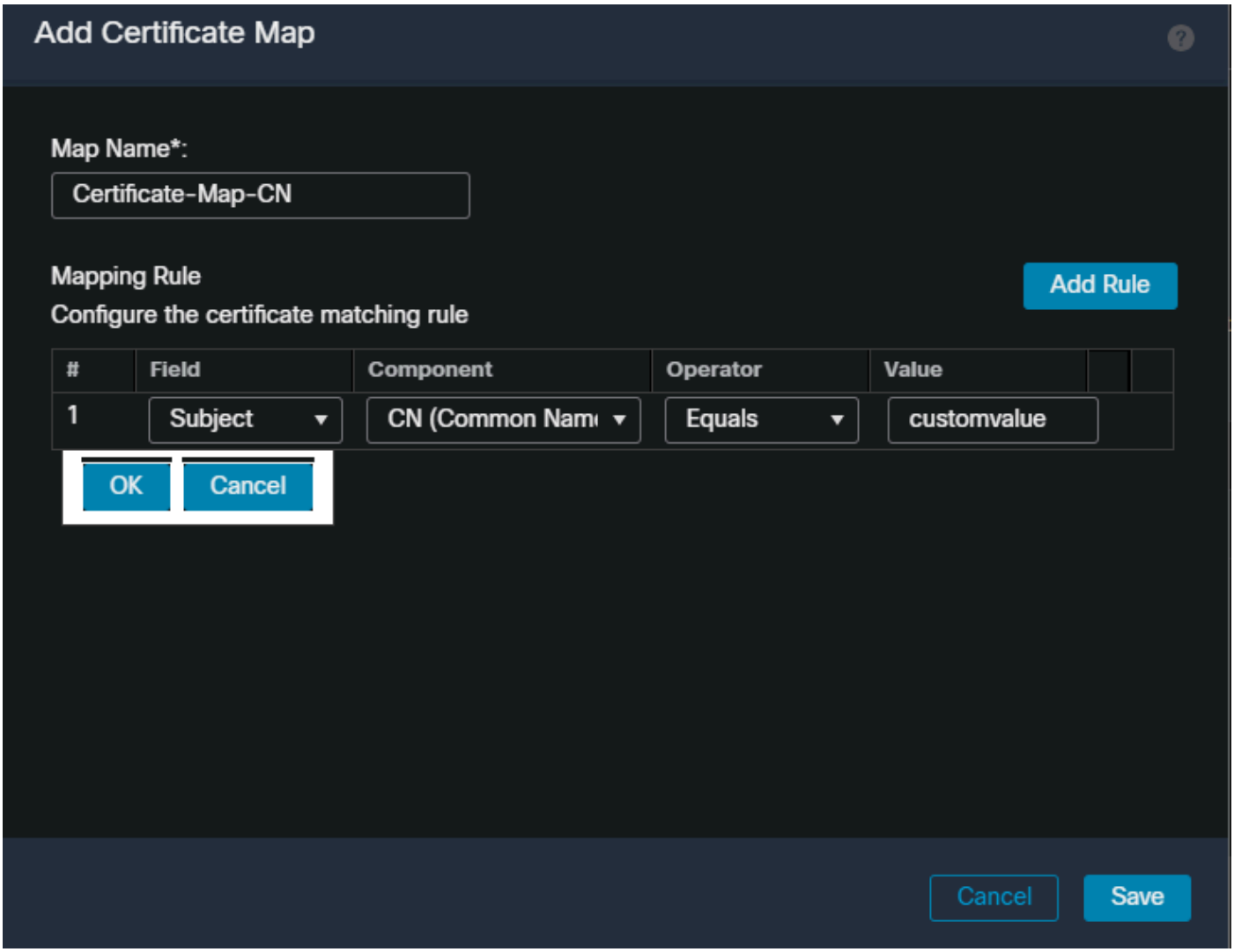
Certificate Mapping

Navigate to the **Advanced** tab within the Remote Access VPN Policy. Choose a general setting option based upon preference. Once selected, select **Add Mapping**.



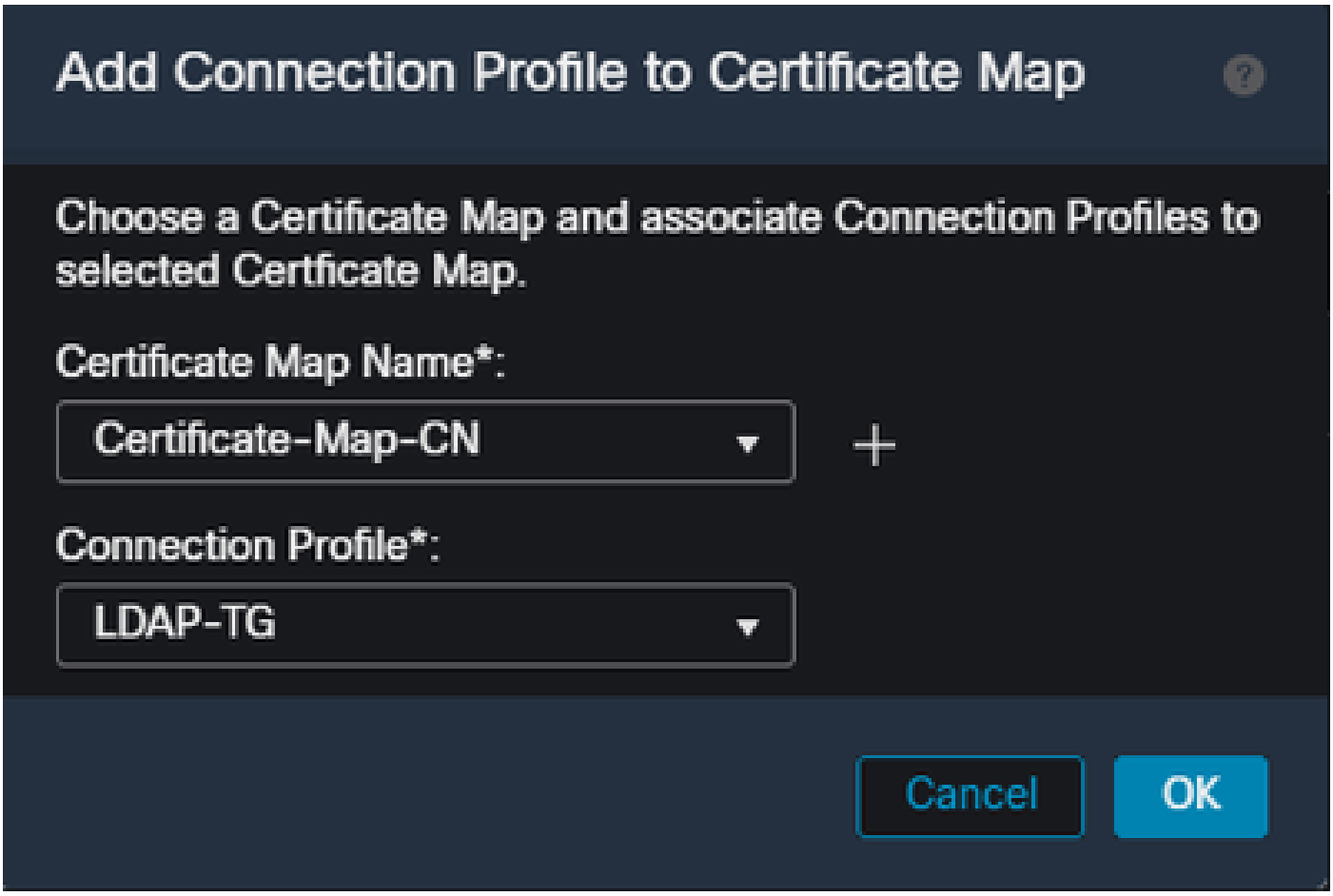
Navigating to the Advanced tab within the FMC UI to create a certificate map object within the FMC UI.

Name the certificate map object and select **Add Rule**. In this rule, define the properties of the certificate you would like to identify to map the user to a certain connection profile. Once finished, select **OK** and then select **Save**.



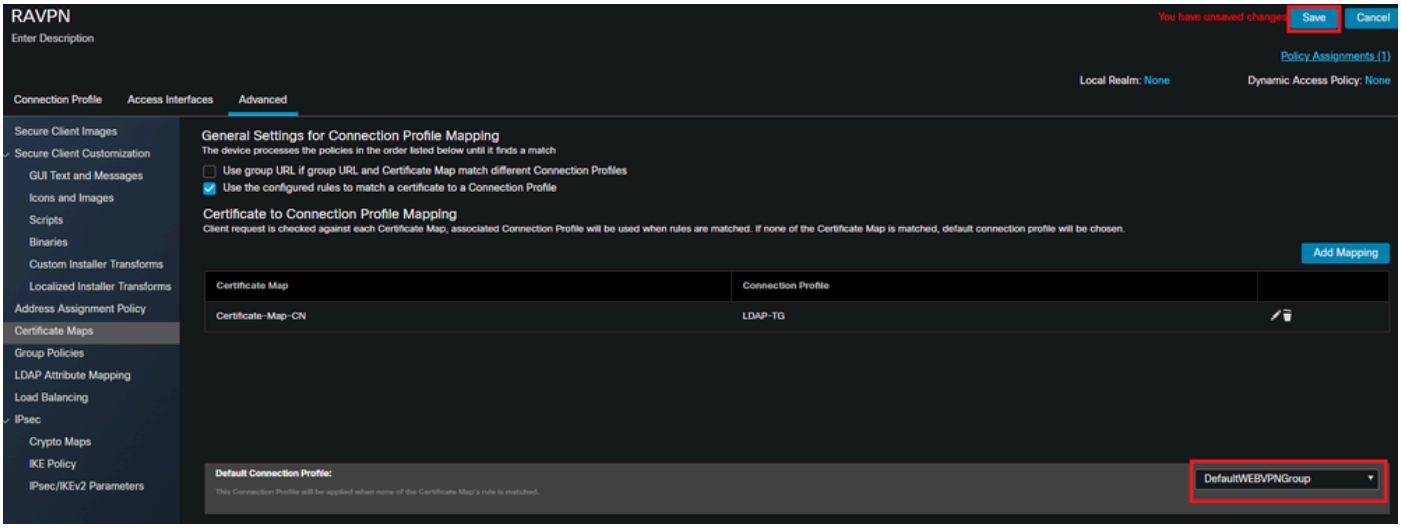
Create a certificate map and add criteria for the map within the FMC UI.

From the dropdown, select the certificate map object, and the connection profile you want the certificate map to be associated with. Then select **OK**.



Tie the certificate map object to the desired tunnel-group within the FMC UI.

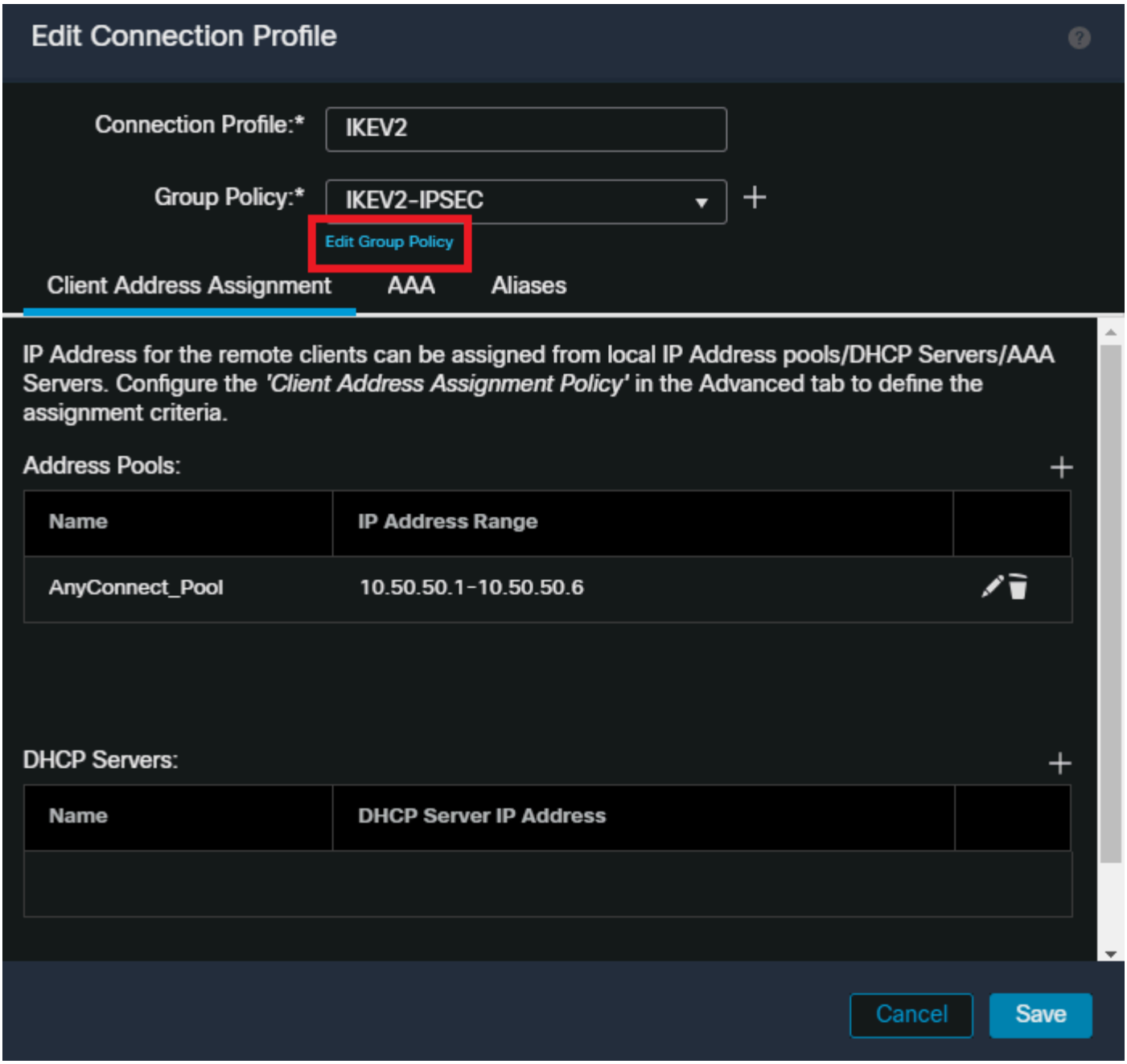
Ensure the Default Connection Profile is configured as DefaultWEBVPNGroup so if a user fails the mapping they are sent to the DefaultWEBVPNGroup. Once finished, select **Save** and deploy the changes.



Change the default connection profile for certificate mapping to the DefaultWEBVPNGroup within the FMC UI.

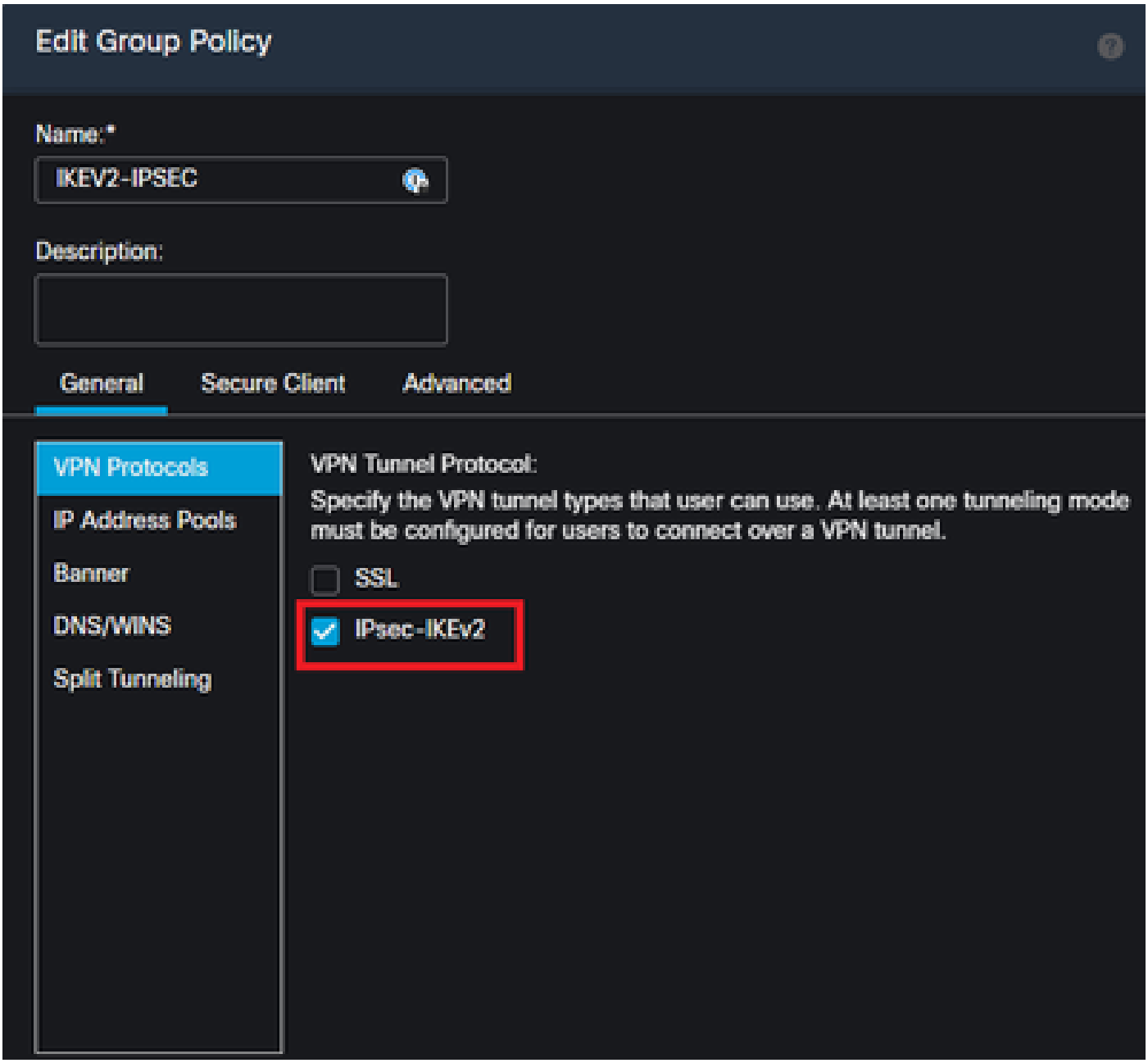
IPsec-IKEv2

Select the desired IPsec-IKEv2 connection profile, and navigate to **Edit Group Policy**.



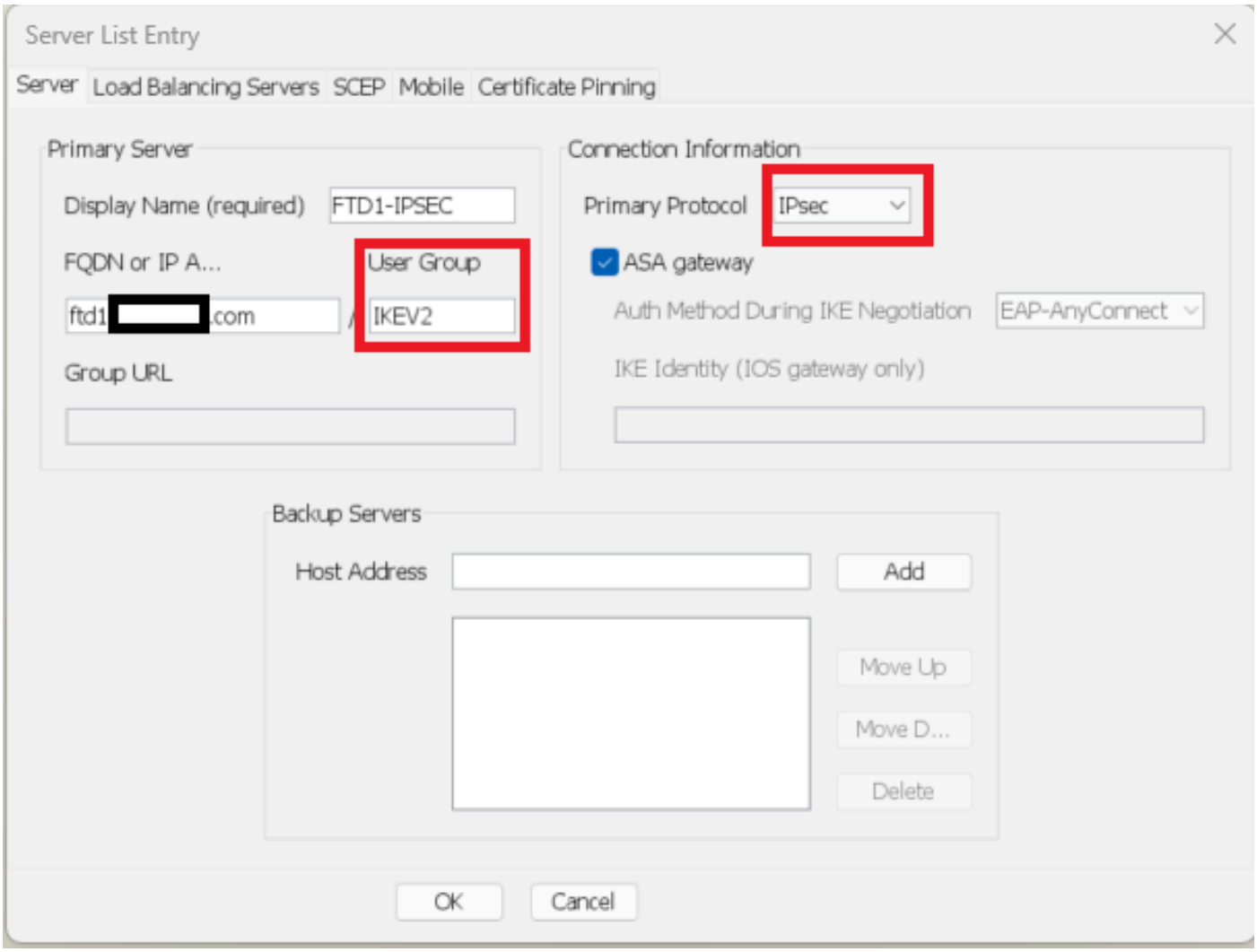
Edit a group-policy within the FMC UI.

In the **General** tab, navigate to the **VPN Protocols** section and ensure the **IPsec-IKEv2** box is checked.

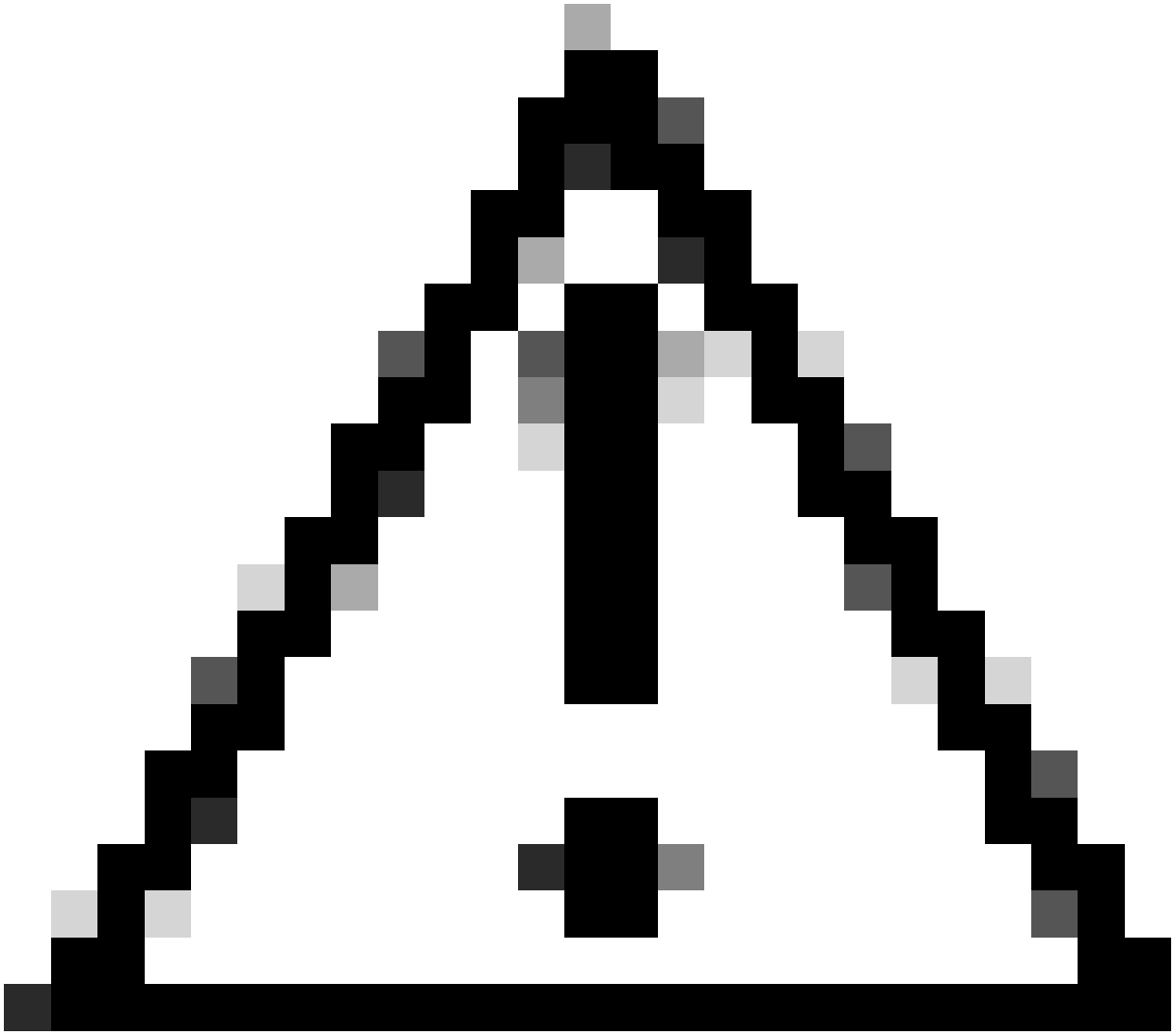


Enable IPsec-IKEv2 within a group-policy in the FMC UI.

In the VPN Profile Editor, or ASA Profile Editor, navigate to the Server List tab. The User Group name MUST be an exact match to the connection profile name on the firewall. In this example, IKEV2 was the connection profile / User Group name. The primary protocol is configured as IPsec. The 'Display Name' in is displayed to the user in the Secure Client UI when establish a connection to this connection profile.

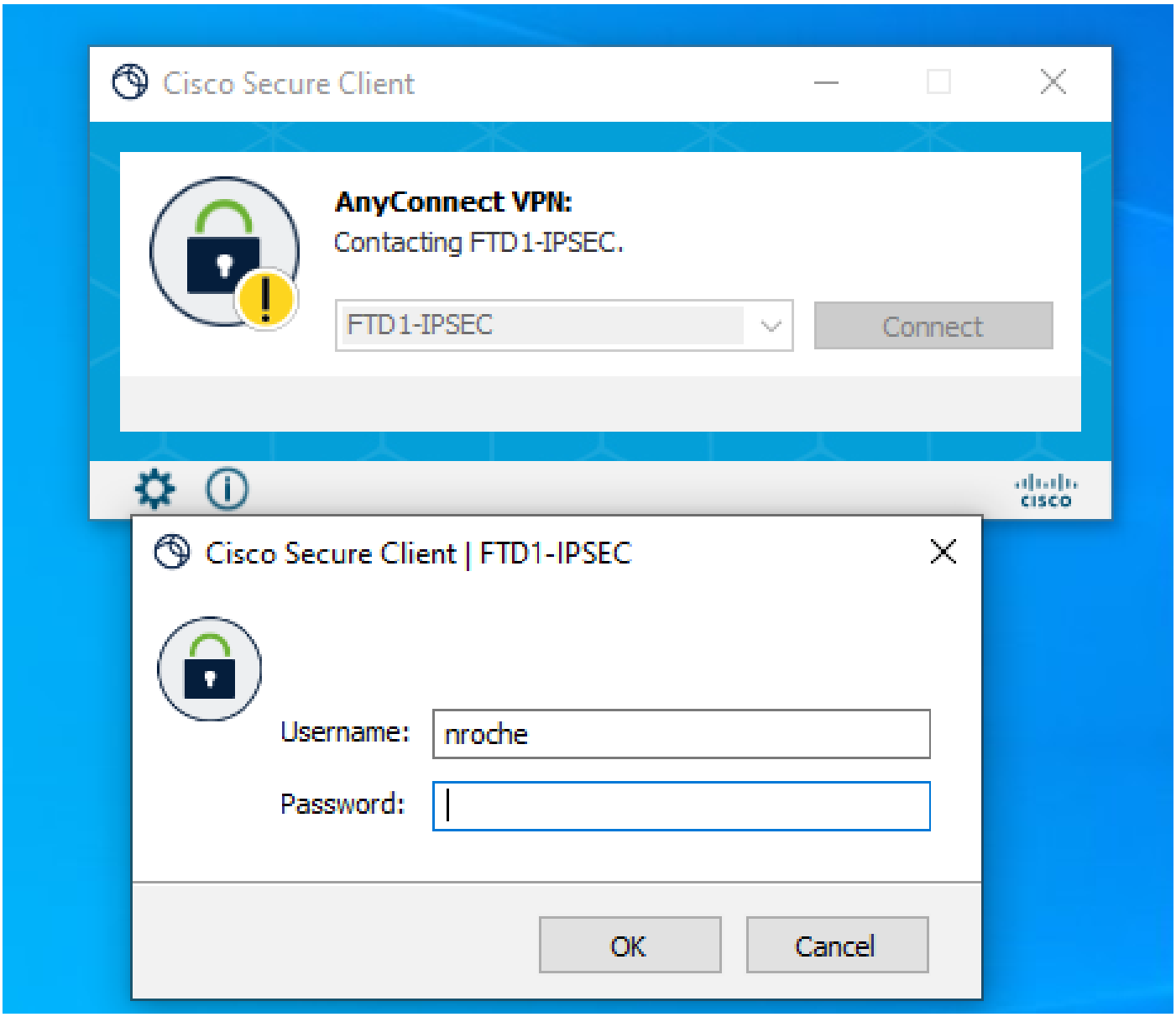


Edit the XML profile so that the primary protocol is IPsec, and the User Group matches the connection profile name.



Caution: An SSL connection is required to push XML profiles to the client from the firewall. When only using IKEV2-IPsec, the XML profiles must be pushed to the clients via an out-of-band method.

Once the XML profile is pushed to the client, Secure Client uses the **User Group** from the XML profile to connect to the IKEV2-IPsec connection profile.



Secure Client UI view of the IPsec-IKEv2 RAVPN connection attempt.

ASA Configuration Examples

Disable AAA Authentication in the DefaultWEBVPNGroup and DefaultRAGroup Connection Profiles

Enter the webvpn-attributes section for tunnel-group DefaultWEBVPNGroup and specify the authentication as certificate based. Repeat this process for the DefaultRAGroup. Users who land on these default connection profiles are forced to present a certificate for authentication and are not presented with the opportunity to enter username and password credentials.

```
ASA# configure terminal
ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
ASA(config-tunnel-webvpn)# authentication certificate

ASA# configure terminal
ASA(config)# tunnel-group DefaultRAGroup webvpn-attributes
ASA(config-tunnel-webvpn)# authentication certificate
```

Disable Hostscan / Secure Firewall Posture on the DefaultWEBVPNGroup and DefaultRAGroup (optional)

This is only necessary if you have Hostscan / Secure Firewall Posture in your environment. This step prevents attackers from increasing the resource utilization on the firewall caused by the endpoint scanning process. Enter the webvpn-attributes section for the DefaultWEBVPNGroup and DefaultRAGroup and connection profiles and implement **without-csd** to disable the endpoint scanning functionality.

```
ASA# configure terminal
ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
ASA(config-tunnel-webvpn)# without-csd

ASA# configure terminal
ASA(config)# tunnel-group DefaultRAGroup webvpn-attributes
ASA(config-tunnel-webvpn)# without-csd
```

Remove Group-aliases and Enable Group-URLs

Enter the tunnel-group(s) users are connecting to. If there is an existing group-alias, remove it. In this example it is removed. Once that is complete, create a group-url using the FQDN or IP address of the RAVPN terminating interface. The name on the end of the group-url needs to be obscure. Avoid common values such as VPN, AAA, RADIUS, LDAP as these make it easier for attackers to guess the full URL if they obtain the FQDN. Instead use internally significant names that help you identify the tunnel-group.

```
ASA# configure terminal
ASA(config)# tunnel-group NAME webvpn-attributes
ASA(config-tunnel-webvpn)# no group-alias NAME
ASA(config-tunnel-webvpn)# group-url https://FQDN/name enable
```

Certificate Mapping

From global configuration mode, create a certificate map and assign it a name and a sequence number. Then define a rule that users must match to utilize the mapping. In this example, users would have to match the criteria of a common name value that equals "customvalue". Next, enter the webvpn configuration and apply the certificate map to the desired tunnel-group. Once completed, enter the DefaultWEBVPNGroup and make this tunnel-group the default for users who fail the certificate mapping. If users fail the mapping, they are directed to the DefaultWEBVPNGroup. While the DefaultWEBVPNGroup is configured with certificate authentication, users do not have the option to pass username or password credentials.

```
ASA(config)# crypto ca certificate map NAME 1
ASA(config-ca-cert-map)# subject-name attr cn eq customvalue

ASA(config)# webvpn
ASA(config-webvpn)# certificate-group-map NAME 1 TG-NAME
```

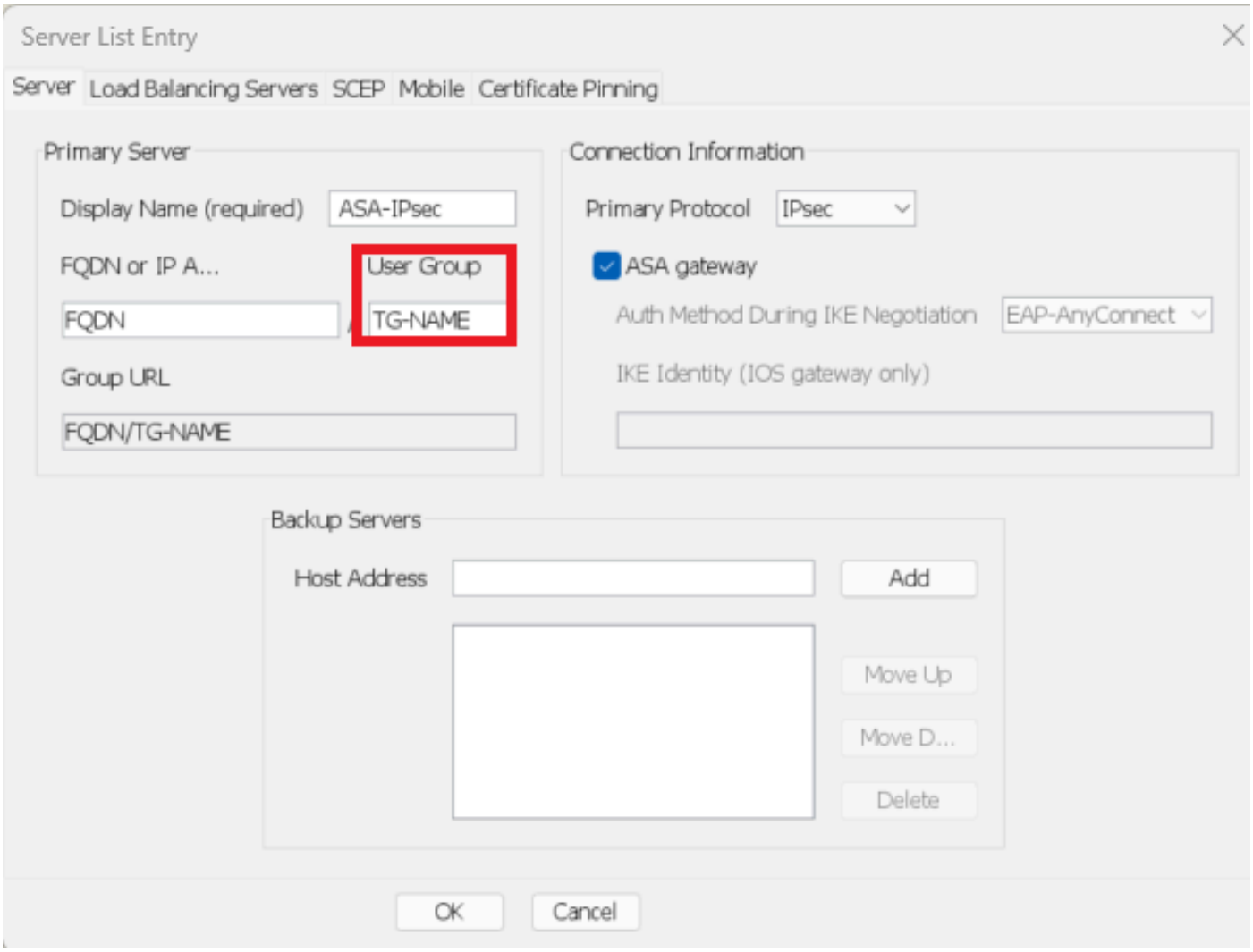
```
ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
ASA(config-tunnel-webvpn)# tunnel-group-map default-group
```

IPsec-IKEv2

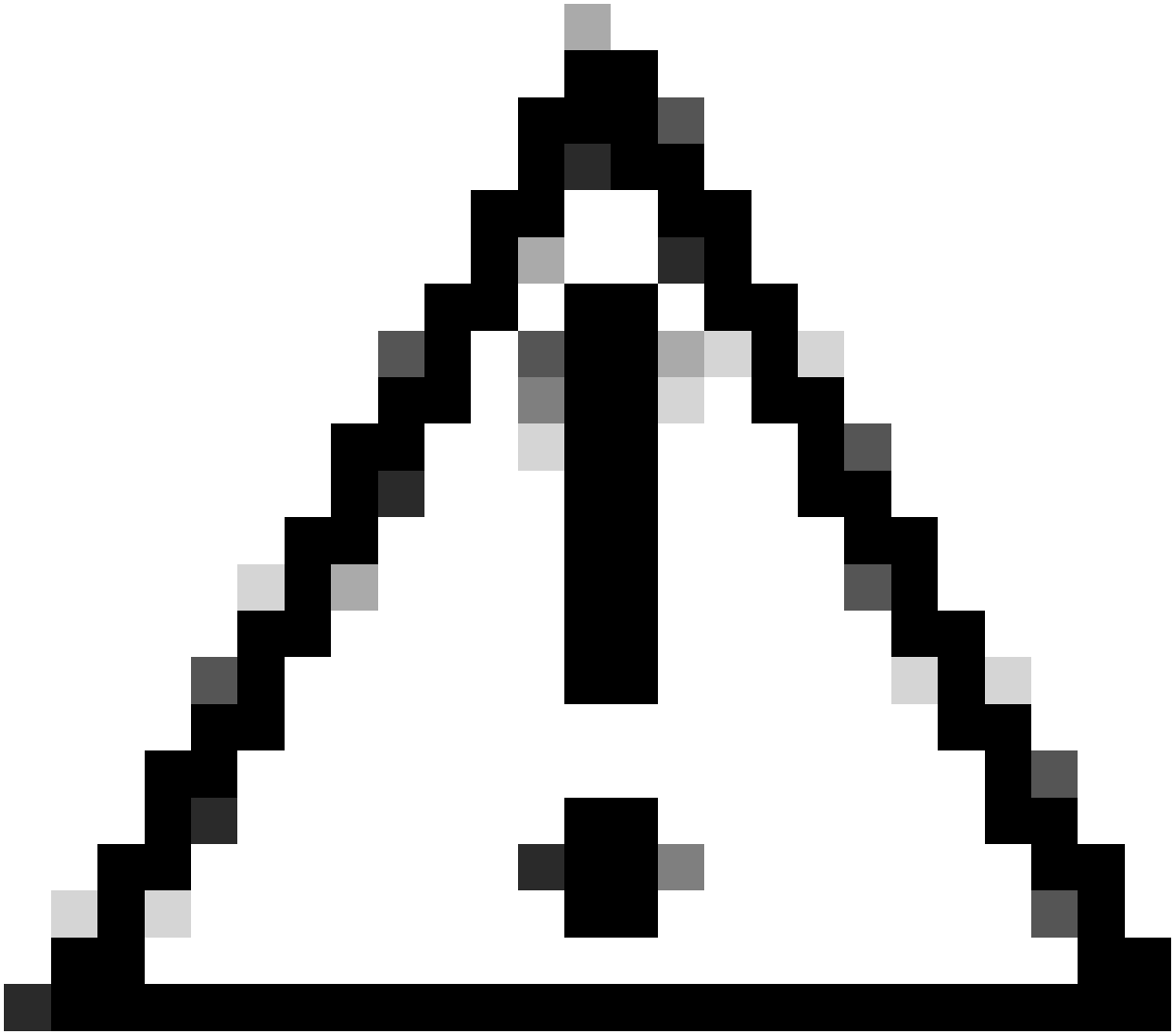
From global configuration mode, you can edit an existing group-policy or create a new one and enter the attributes for that group-policy. Once you are in the attributes section, enable IKEv2 as the only vpn tunnel protocol. Ensure that this group-policy is tied to a tunnel-group that is going to be utilized for IPsec-IKEV2 remote access VPN connections. Similar to the FMC steps, you must edit the XML profile via the VPN Profile Editor or the ASA Profile Editor and change the User Group field to match the name of the tunnel-group on the ASA, and change the protocol to IPsec.

```
ASA# configure terminal
ASA(config)# group-policy GP-NAME internal
ASA(config)# group-policy GP-NAME attributes
ASA(config-group-policy)# vpn-tunnel-protocol ikev2

ASA(config)# tunnel-group TG-NAME general-attributes
ASA(config-tunnel-general)# default-group-policy GP-NAME
```

In the VPN Profile Editor, or ASA Profile Editor, navigate to the Server List tab. The User Group name MUST be an exact match to the connection profile name on the firewall. The primary protocol is configured as IPsec. The display name is shown to the user in the Secure Client UI when establishing a connection to this connection profile.



Edit the XML profile so that the primary protocol name is IPsec and the User Group name matches the tunnel-group name of the ASA for IPsec-IKEv2 RAVPN connections.



Caution: An SSL connection is required to push XML profiles to the client from the firewall. When only using IKEV2-IPsec, the XML profiles must be pushed to the clients via an out-of-band method.

Conclusion

In summation, the purpose of the hardening practices in this document is to map legitimate users to custom connection profiles while attackers are forced to the DefaultWEBVPNGroup and the DefaultRAGroup. In an optimized configuration, the two default connection profiles do not have any legitmate custom AAA server configuration. Additionally, the removal of group-aliases prevents attackers from easily identifying custom connection profiles by removing the drop-down visibility upon navigating to the FQDN or public IP address of the firewall.

Related Information

Cisco Technical Support and Downloads

Password Spray Attacks

Unauthorized Access Vulnerability September 2023

ASA Configuration Guides

FMC / FDM Configuration Guides