Implementierung von Härtungsmaßnahmen für Secure Client AnyConnect VPN

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Sicherheit Ihrer Remote Access VPN-Implementierung verbessern können.

Voraussetzungen

Anforderungen

Cisco empfiehlt Ihnen, sich mit folgenden Themen vertraut zu machen:

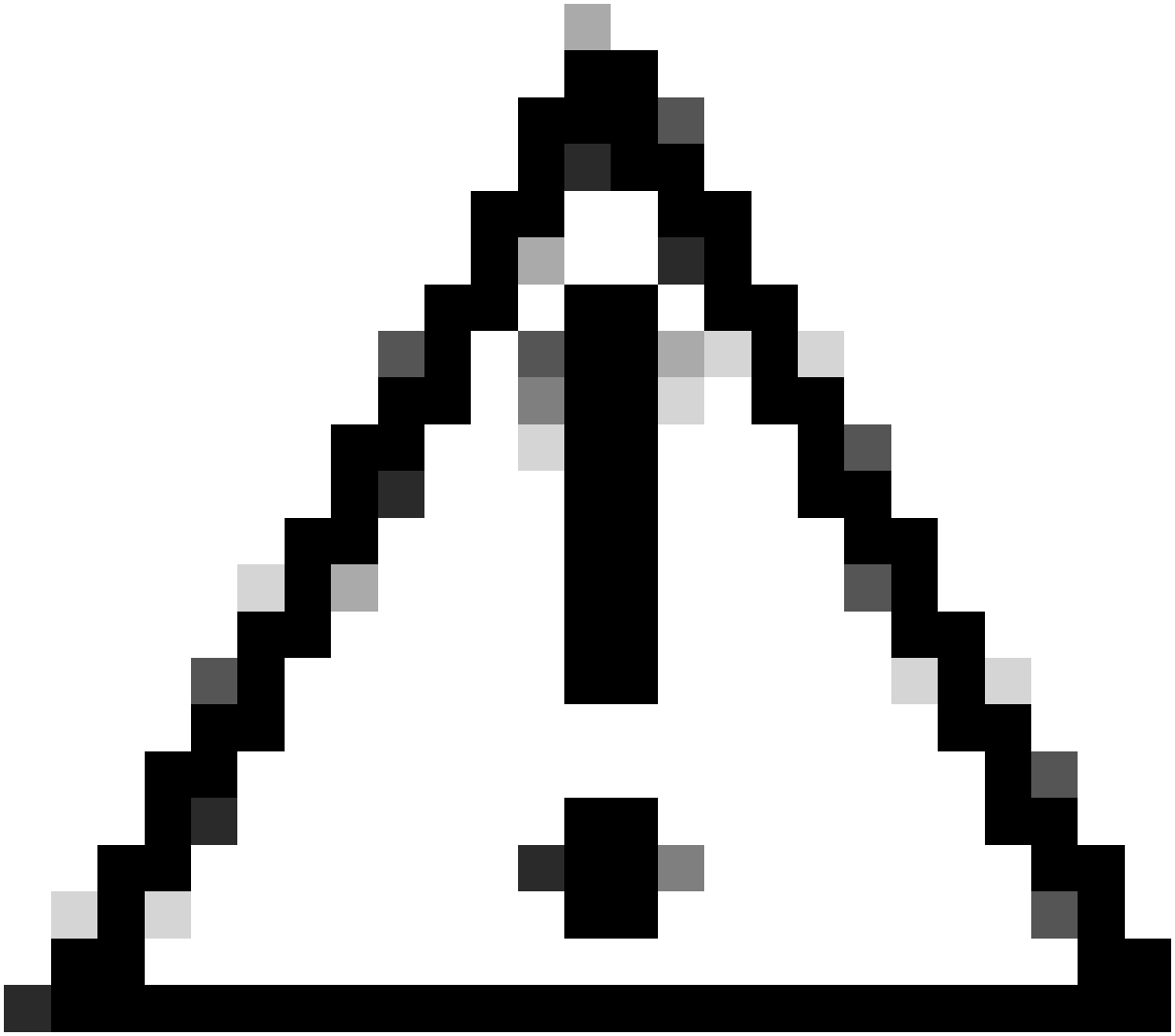
- Cisco Secure Client AnyConnect-VPN
- Konfiguration von ASA/FTD für Remote-Zugriff.

Verwendete Komponenten

Der Leitfaden mit Best Practices basiert auf den folgenden Hardware- und Softwareversionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.



Achtung: Dieses Dokument enthält keine Schritte für den FirePOWER Geräte-Manager (FDM). Der FDM unterstützt nur das Ändern der Authentifizierungsmethode in der DefaultWEBVPNGroup-Gruppe. Verwenden Sie Kontrollebenen-ACLs oder einen

---

benutzerdefinierten Port im Abschnitt "Globale Einstellungen" des Remote Access-VPN in der FDM-Benutzeroberfläche. Wenden Sie sich bei Bedarf an das Cisco Technical Assistance Center (TAC).

Hintergrundinformationen

Mit diesem Dokument soll sichergestellt werden, dass die Cisco Secure Client AnyConnect VPN-Konfiguration den Best Practices für die Sicherheit in einer modernen Welt entspricht, in der Cyberangriffe weit verbreitet sind.

Brute-Force-Angriffe beinhalten in der Regel wiederholte Versuche, über eine Kombination aus Benutzername und Passwort Zugriff auf eine Ressource zu erhalten. Angreifer versuchen, ihren Internet-Browser, die Secure Client-Benutzeroberfläche oder andere Tools zu verwenden, um mehrere Benutzernamen und Kennwörter einzugeben, in der Hoffnung, dass sie mit einer legitimen Kombination in einer AAA-Datenbank übereinstimmen. Bei Verwendung von AAA für die Authentifizierung erwarten wir, dass der Endbenutzer seinen Benutzernamen und sein Kennwort eingibt, da dies für die Herstellung der Verbindung erforderlich ist. Gleichzeitig überprüfen wir erst, wer der Benutzer ist, wenn er seine Anmeldeinformationen eingegeben hat. Dadurch können Angreifer die folgenden Szenarien ausnutzen:

1. Verfügbare vollqualifizierte Domänennamen für die Cisco Secure Firewall (insbesondere bei Verwendung von Gruppen-Aliasnamen im Verbindungsprofil):
    - Wenn der Angreifer den FQDN Ihrer VPN-Firewall erkennt, hat er die Möglichkeit, die Tunnel-Gruppe unter Verwendung des Gruppenalias auszuwählen, unter dem er den Brute-Force-Angriff starten möchte.

2. Mit AAA oder lokaler Datenbank konfiguriertes Standard-Verbindungsprofil:
    - Wenn der Angreifer den FQDN der VPN-Firewall findet, kann er versuchen, einen Brute-Force-Angriff auf den AAA-Server oder die lokale Datenbank durchzuführen. Dies liegt daran, dass die Verbindung zum FQDN im Standardverbindungsprofil landet, selbst wenn keine Gruppenaliase angegeben ist.

3. Auslastung der Ressourcen auf der Firewall oder auf AAA-Servern:
    - Angreifer können AAA-Server oder Firewall-Ressourcen überlasten, indem sie große Mengen an Authentifizierungsanforderungen senden und eine Denial of Service (DoS)-Bedingung auslösen.

Konzepte

Gruppenaliase:

- Ein alternativer Name, über den die Firewall auf ein Verbindungsprofil verweisen kann. Nach dem Herstellen einer Verbindung zur Firewall werden diese Namen in einem Dropdown-

Menü in der Secure Client UI angezeigt, das von Benutzern ausgewählt werden kann. Beim Entfernen von Gruppenaliasen wird die Dropdown-Funktion in der Secure Client-Benutzeroberfläche entfernt.

Gruppen-URLs:

- Eine URL, die mit einem Verbindungsprofil verknüpft werden kann, sodass eingehende Verbindungen direkt einem gewünschten Verbindungsprofil zugeordnet werden. Es gibt keine Dropdown-Funktion, da Benutzer die vollständige URL in der Secure Client-Benutzeroberfläche eingeben können, oder die URL kann mit einem Anzeigenamen im XML-Profil integriert werden, um die URL vor dem Benutzer auszublenden.

Der Unterschied besteht darin, dass bei der Implementierung von Gruppenaliasen ein Benutzer eine Verbindung to vpn_gateway.example.com herstellt und Aliase erhält, die ihn zu einem Verbindungsprofil führen. Mit Gruppen-URLs stellt ein Benutzer eine Verbindung zu vpn_gateway.example.com/example_group her und leitet diese direkt zum Verbindungsprofil weiter, ohne dass ein Dropdown-Menü erforderlich oder verfügbar wäre.

Sichere Client-Härtung bei Cisco Secure Firewall:

Diese Methoden basieren auf der Zuordnung legitimer Benutzer zu entsprechenden Tunnelgruppen/Verbindungsprofilen, während potenziell böswillige Benutzer an eine Trap-Tunnelgruppe gesendet werden, die wir so konfigurieren, dass sie keine Kombinationen von Benutzernamen und Kennwort zulassen. Obwohl nicht alle Kombinationen implementiert werden müssen, müssen Gruppenaliase deaktiviert und die Authentifizierungsmethode von DefaultWEBVPNGroup und DefaultRAGroup geändert werden, damit die Empfehlungen wirksam funktionieren.

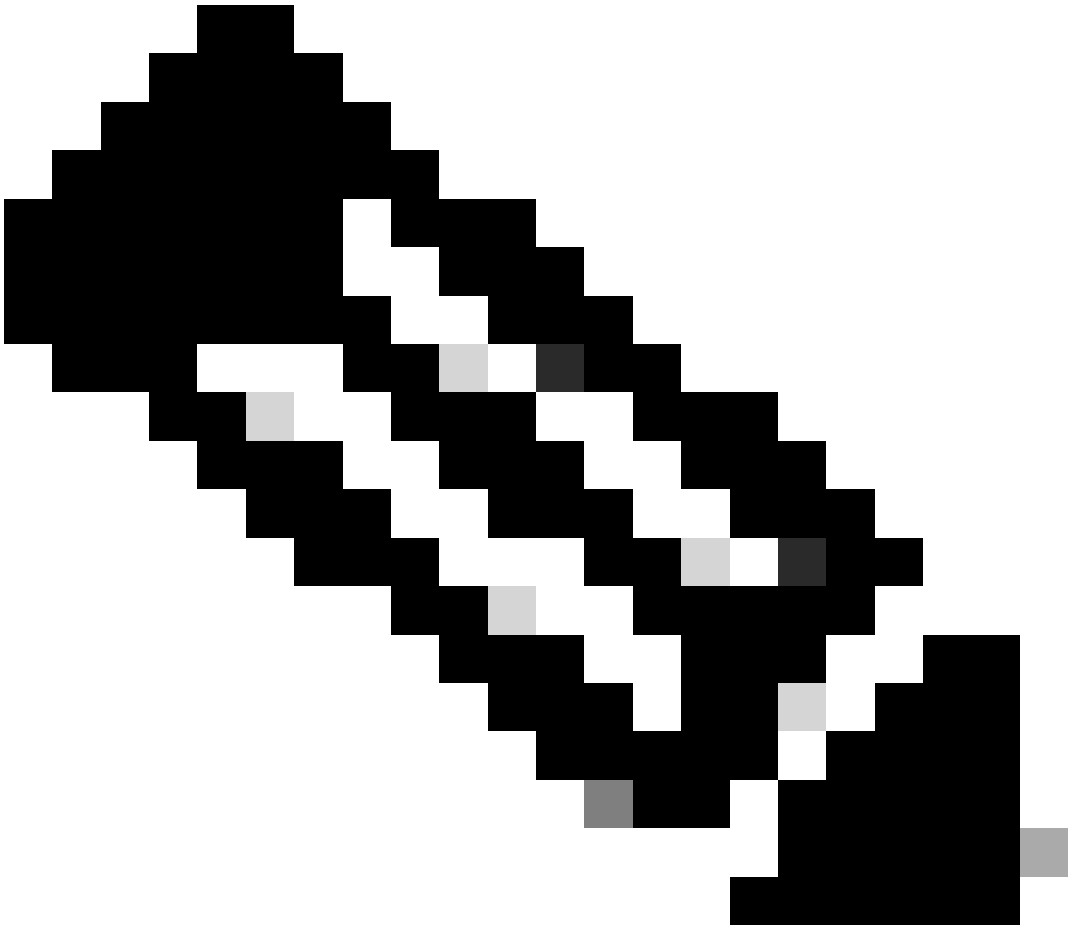
- Deaktivieren Sie Gruppen-Aliase, und verwenden Sie nur group-url in der Konfiguration des Verbindungsprofils. Dies ermöglicht Ihnen, einen bestimmten FQDN zu haben, der für einen Angreifer nicht einfach zu erkennen und auszuwählen ist, da nur die Clients mit dem richtigen FQDN die Verbindung initiieren können. Beispielsweise ist vpn_gateway.example.com/example_group für einen Angreifer schwieriger zu erkennen als vpn_gateway.example.com.

- Deaktivieren Sie die AAA-Authentifizierung in DefaultWEBVPNGroup und DefaultRAGroup, und konfigurieren Sie die Zertifikatsauthentifizierung. Dadurch wird Brute-Force-Angriffe auf die lokale Datenbank oder den AAA-Server vermieden. In diesem Szenario würde der Angreifer sofort Fehler erhalten, wenn er versucht, eine Verbindung herzustellen. Es gibt kein Feld für den Benutzernamen oder das Kennwort, da die Authentifizierung auf Zertifikaten basiert und somit Brute-Force-Versuche gestoppt werden. Eine weitere Option besteht darin, einen AAA-Server ohne unterstützende Konfiguration zu erstellen, um eine Sicherheitslücke für böswillige Anfragen zu schaffen.

- Verwenden Sie die Zertifikatszuordnung für das Verbindungsprofil. Auf diese Weise können eingehende Verbindungen bestimmten Verbindungsprofilen zugeordnet werden, basierend

auf Attributen, die von Zertifikaten auf dem Clientgerät empfangen wurden. Benutzer, die über die richtigen Zertifikate verfügen, werden korrekt zugeordnet, während Angreifer, die die Zuordnungskriterien nicht erfüllen, an die DefaultWEBVPNGroup gesendet werden.

- Die Verwendung von IKEv2-IPSec anstelle von SSL führt dazu, dass sich Tunnelgruppen auf eine bestimmte Benutzergruppenzuordnung im XML-Profil verlassen. Ohne diese XML auf dem Endbenutzercomputer werden die Benutzer automatisch an die standardmäßige Tunnelgruppe gesendet.



Hinweis: Weitere Informationen zur Gruppenalias-Funktion finden Sie im ASA VPN-Konfigurationshandbuch unter "Tabelle 1. Connection Profile Attributes for SSL VPN'.

Identifizierung von Angriffen mithilfe von Protokollierung und Syslog-IDs

Brute-Force-Angriffe stellen die vorherrschende Methode zur Kompromittierung von Remote

Access-VPNs dar. Dabei werden schwache Passwörter ausgenutzt, um sich unbefugten Zugriff zu verschaffen. Es ist wichtig zu wissen, wie man Anzeichen eines Angriffs erkennt, indem man die Verwendung von Protokollierung und Auswertung von Syslogs nutzt. Gängige Syslogs-IDs, die auf einen Angriff hinweisen können, wenn ein ungewöhnliches Volume auftritt, sind:

%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 =

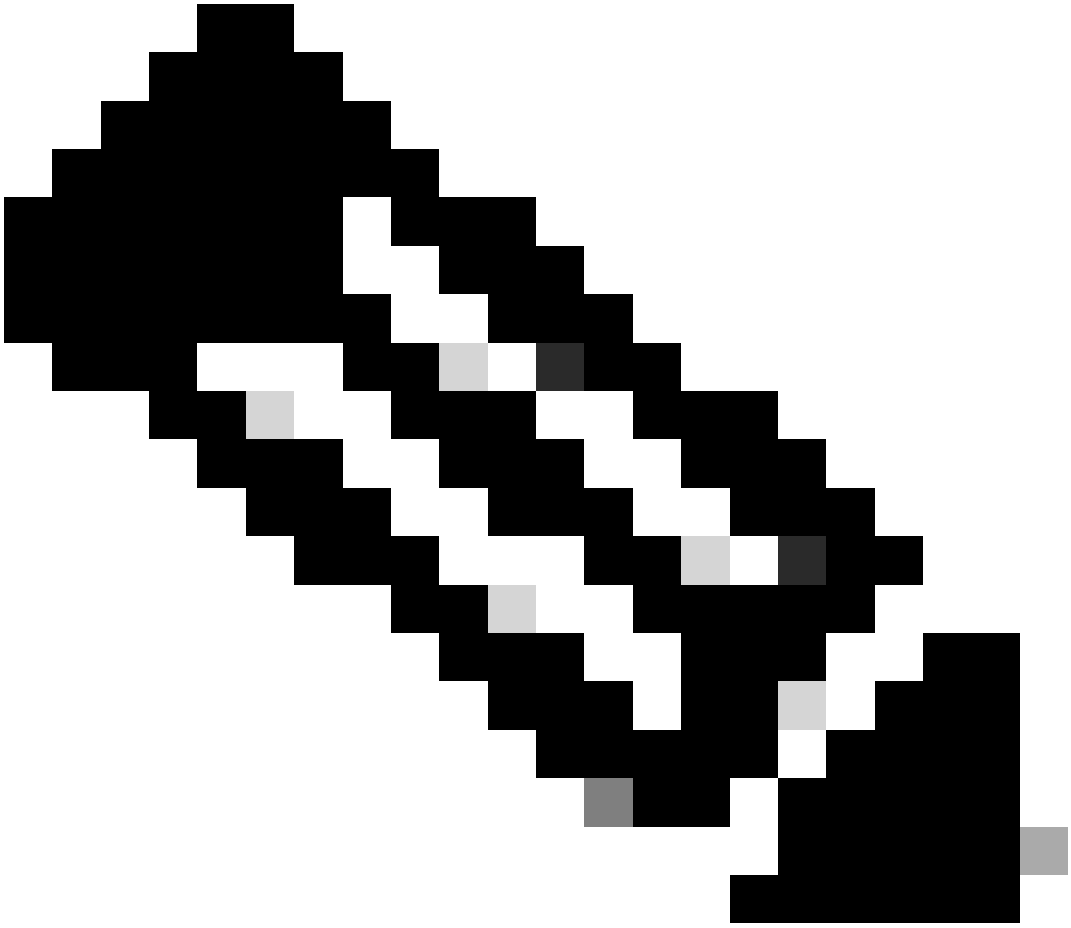
%ASA-6-716039

<#root>

%ASA-6-716039

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

Der Benutzername wird immer ausgeblendet, bis der Befehl no logging hide username auf der ASA konfiguriert wird.



Hinweis: Hinweis: Dies gibt Aufschluss darüber, ob gültige Benutzer von IP-Adressen mit Sicherheitsverletzungen erstellt wurden oder bekannt sind. Seien Sie jedoch vorsichtig, da die Benutzernamen in den Protokollen angezeigt werden.

Cisco ASA-Protokollierung:

Benutzerhandbuch zur sicheren ASA-Firewall
Protokollierung des Kapitels Cisco Secure Firewall ASA-Serie Allgemeiner CLI-Konfigurationsleitfaden für den Betrieb

Cisco FTD-Protokollierung:

Konfigurieren der Protokollierung auf FTD über FMC

Konfigurieren Sie den Abschnitt Syslog im Kapitel "Plattform-Einstellungen" des Cisco Secure Firewall Management Center Gerätekonfigurationsleitfadens.
Konfiguration und Überprüfung des Syslog im FirePOWER Geräte-Manager

Konfigurieren der Systemprotokollierungseinstellungen im Kapitel "Systemeinstellungen" des Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager

Überprüfung des Angriffs

Melden Sie sich zur Überprüfung bei der ASA- oder FTD-Befehlszeilenschnittstelle (CLI) an, führen Sie den Befehl show aaa-server aus, und untersuchen Sie die Anzahl der Authentifizierungsanforderungen, die an einen der konfigurierten AAA-Server gesendet wurden, auf ungewöhnlich viele, versucht oder abgelehnt wurden:

<#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

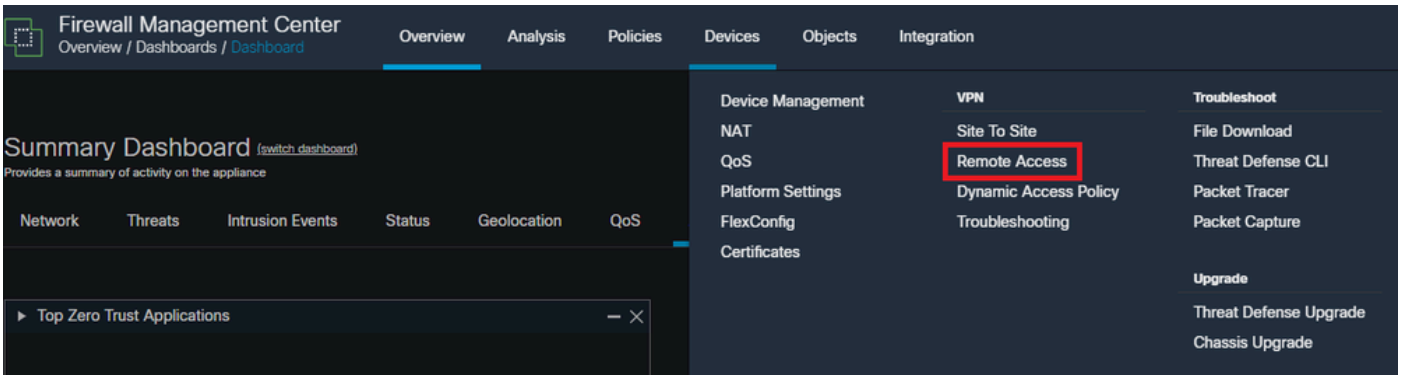
```
Server Group: LDAP-SERVER - - - - - >>>> Sprays against the LDAP server
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.10.10.10
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms
Number of 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
```

Beispiele für FMC-Konfiguration

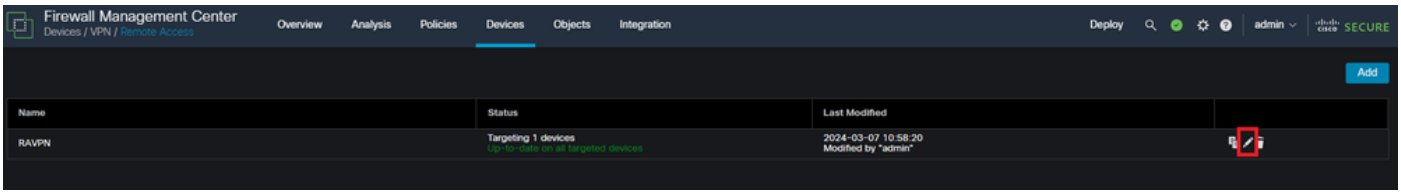
Deaktivieren Sie die AAA-Authentifizierung in den Verbindungsprofilen DefaultWEBVPNGroup und DefaultRAGroup.

Navigieren Sie zu Geräte > Remotezugriff.



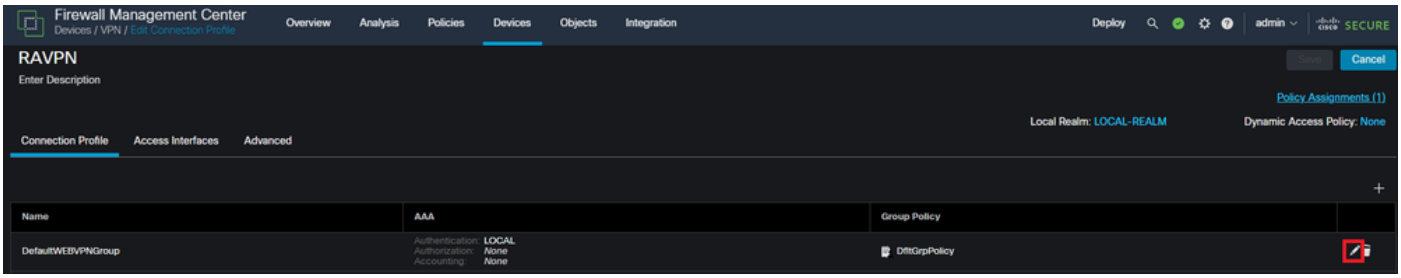
Zeigt an, wie Sie in der FMC-GUI zur Konfiguration der VPN-Richtlinie für den Remote-Zugriff navigieren.

Bearbeiten Sie die vorhandene VPN-Richtlinie für den Remote-Zugriff, und erstellen Sie ein Verbindungsprofil mit dem Namen "DefaultRAGroup".



Zeigt, wie die VPN-Richtlinie für den Remotezugriff in der FMC-Benutzeroberfläche bearbeitet wird.

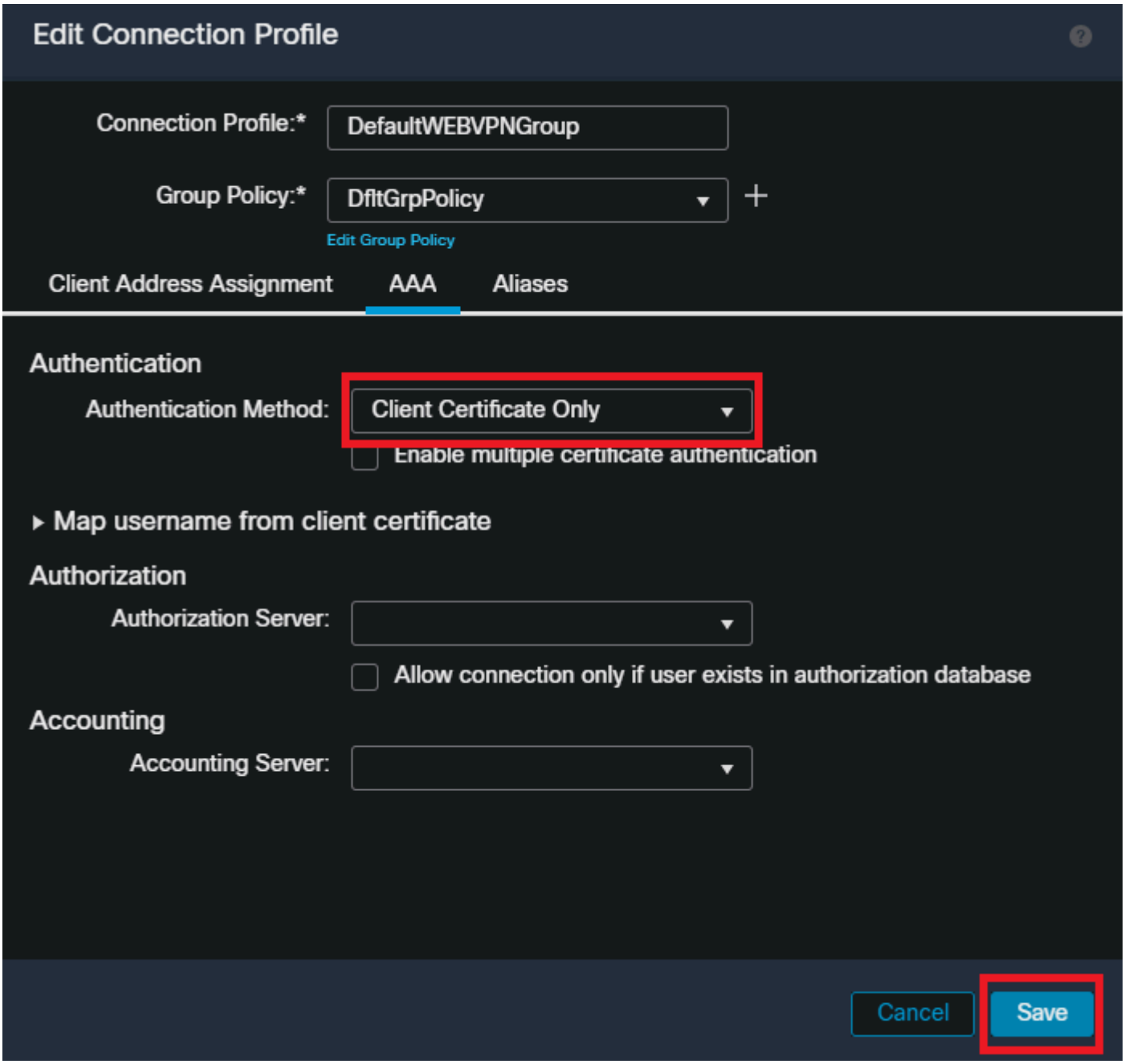
Bearbeiten Sie die Verbindungsprofile 'DefaultWEBVPNGroup' und 'DefaultRAGroup'.



Zeigt, wie die DefaultWEBVPNGroup in der FMC-Benutzeroberfläche bearbeitet wird.

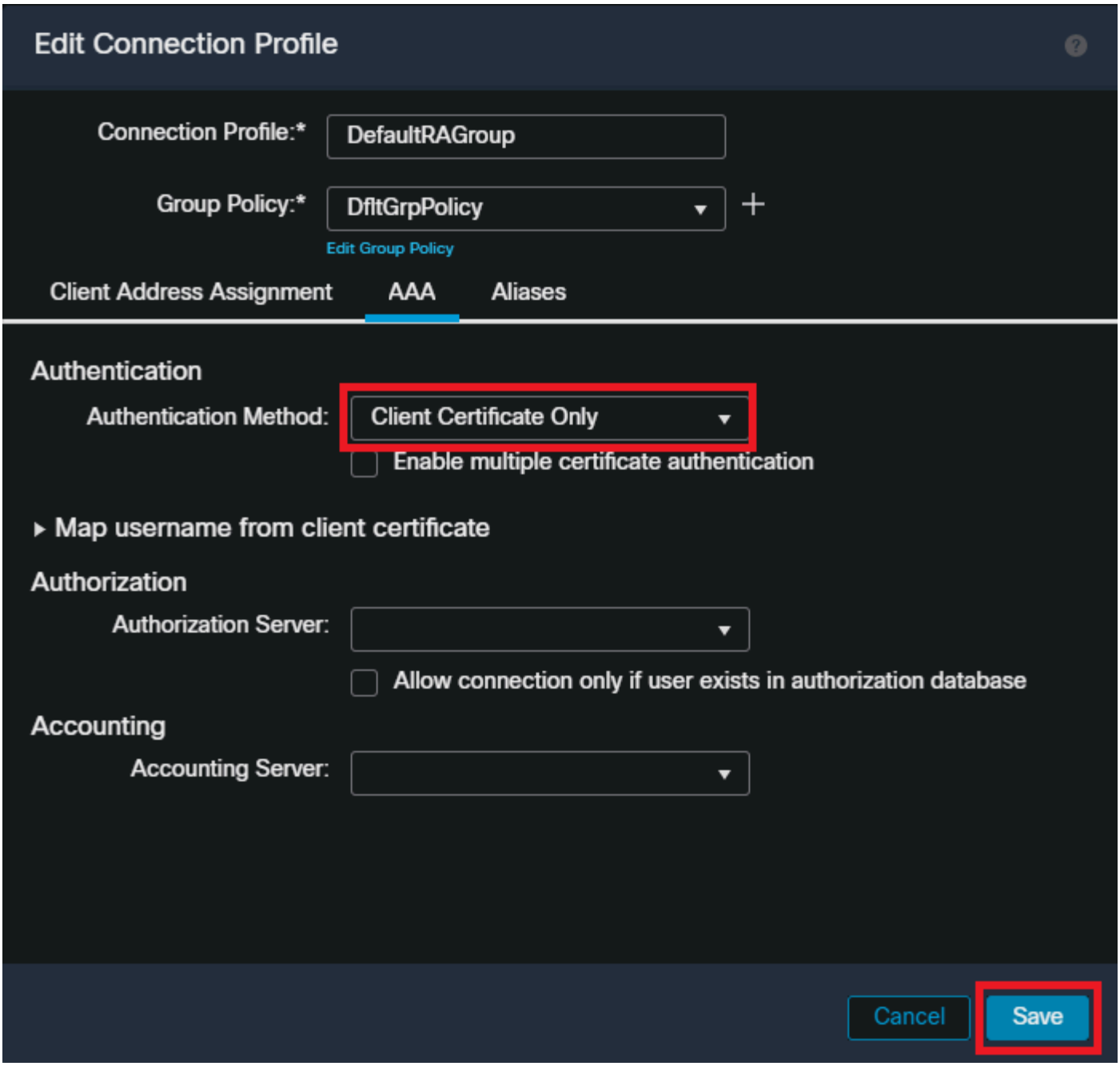
Navigieren Sie zur Registerkarte AAA, und wählen Sie das Dropdown-Menü Authentication

Method aus. Wählen Sie 'Nur Client-Zertifikat' und dann Speichern.

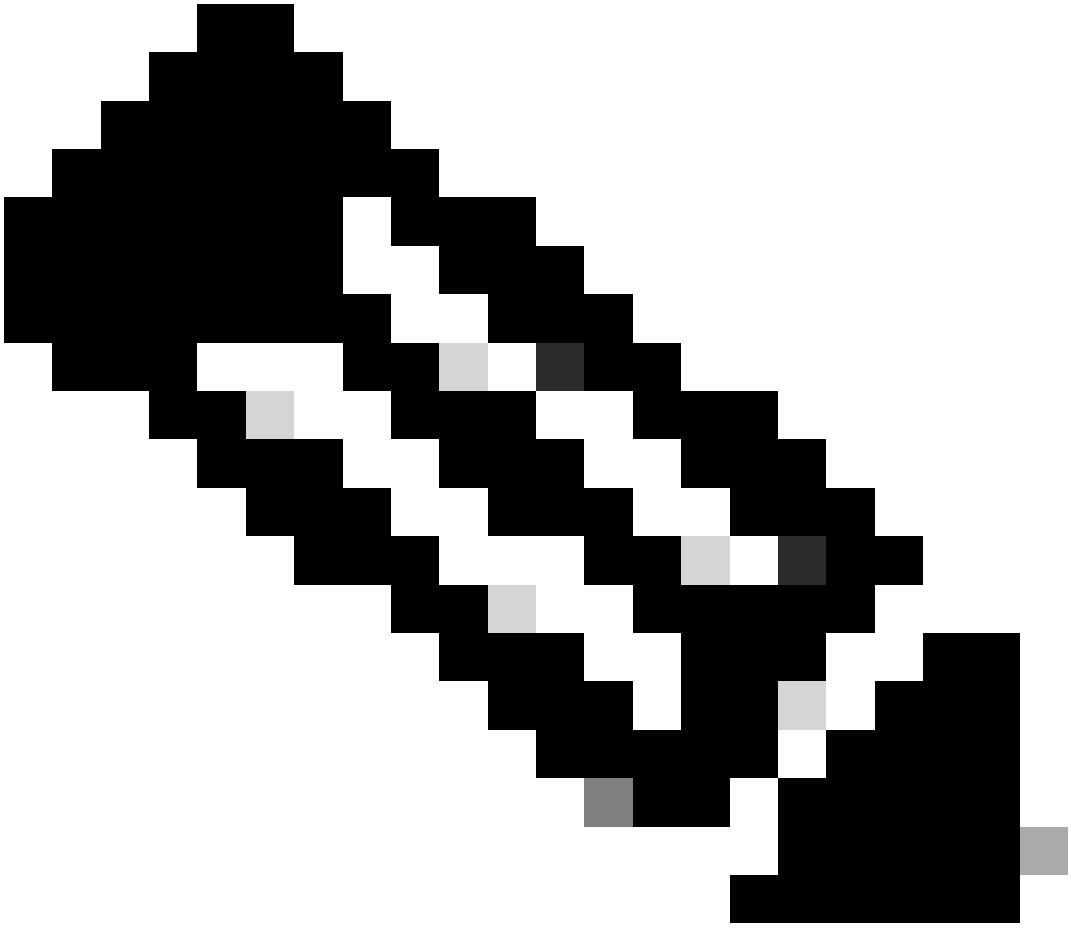


Ändern der Authentifizierungsmethode in ein Clientzertifikat nur für die DefaultWEBVPNGroup innerhalb der FMC-Benutzeroberfläche.

Bearbeiten Sie DefaultRAGroup, und navigieren Sie zur Registerkarte AAA, und wählen Sie das Dropdown-Menü Authentication Method (Authentifizierungsmethode) aus. Wählen Sie 'Nur Client-Zertifikat' und dann Speichern aus.



Ändern der Authentifizierungsmethode in ein Clientzertifikat nur für die DefaultRAGroup innerhalb der FMC-Benutzeroberfläche.

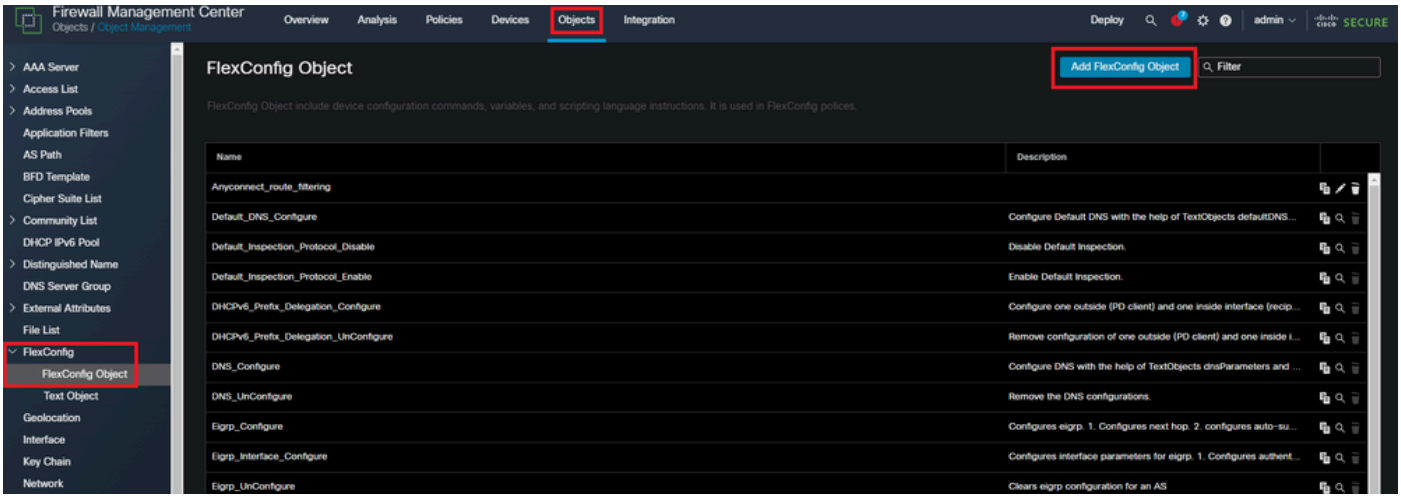


Hinweis: Bei der Authentifizierungsmethode kann es sich auch um einen Sinkhole-AAA-Server handeln. Wenn diese Methode verwendet wird, ist die AAA-Serverkonfiguration gefälscht und verarbeitet keine Anforderungen. Außerdem muss auf der Registerkarte "Client Address Assignment" (Client-Adressenzuweisung) ein VPN-Pool definiert werden, um die Änderungen zu speichern.

Deaktivieren Sie Hostscan/Secure Firewall Posture auf der DefaultWEBVPNGroup und DefaultRAGroup (optional).

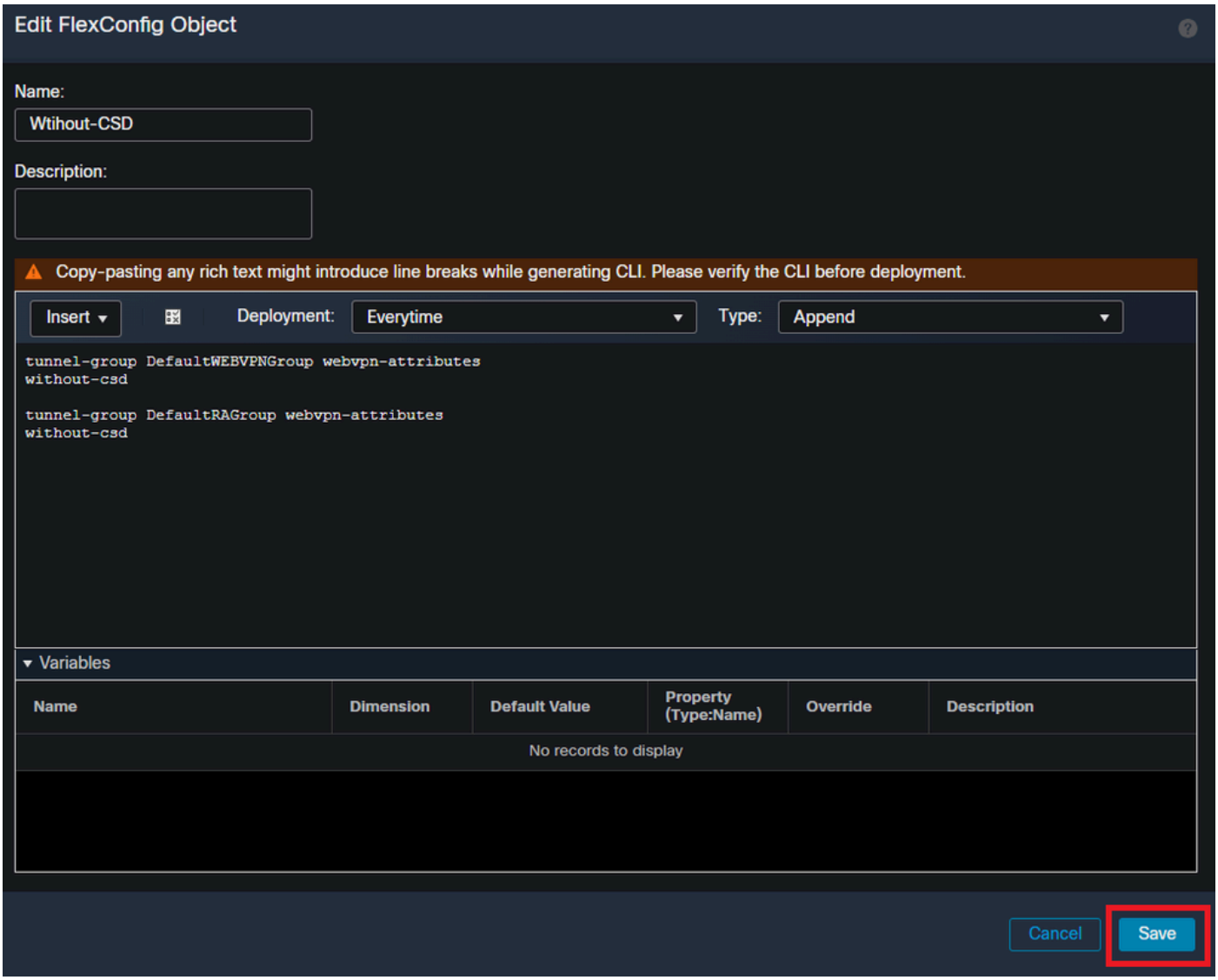
Dies ist nur erforderlich, wenn Sie Hostscan/Secure Firewall Posture in Ihrer Umgebung haben. Dieser Schritt verhindert, dass Angreifer die durch den Endpunkt-Scanvorgang verursachte Ressourcennutzung auf der Firewall erhöhen. Im FMC wird dies durch das Erstellen eines FlexConfig-Objekts mit dem Befehl without-csd erreicht, um die Endpunkt-Scanfunktion zu deaktivieren.

Navigieren Sie zu Objekte > Objektverwaltung > FlexConfig-Objekt > FlexConfig-Objekt hinzufügen.



Navigieren in der FMC-Benutzeroberfläche zum Erstellen eines FlexConfig-Objekts

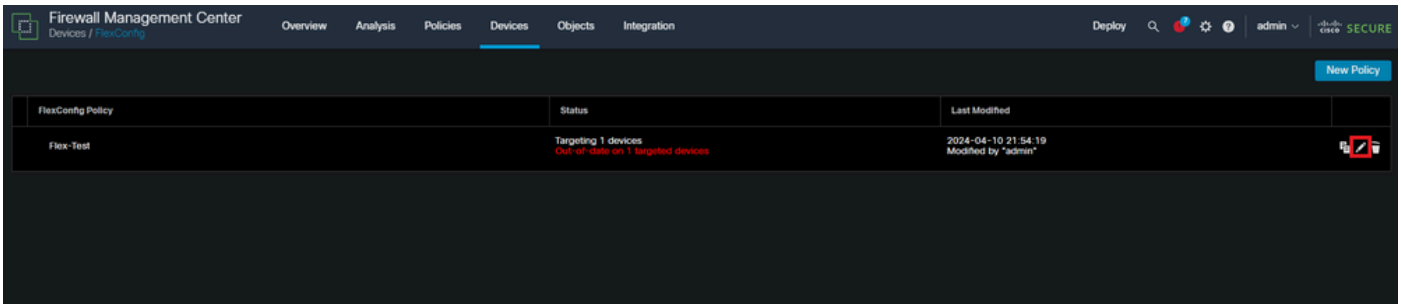
Nennen Sie das FlexConfig-Objekt, und legen Sie die Bereitstellung auf Everytime mit dem Typ Append fest. Geben Sie dann die Syntax genau wie dargestellt ein, und speichern Sie das Objekt.



Erstellen eines FlexConfig-Objekts mit "ohne CSD"

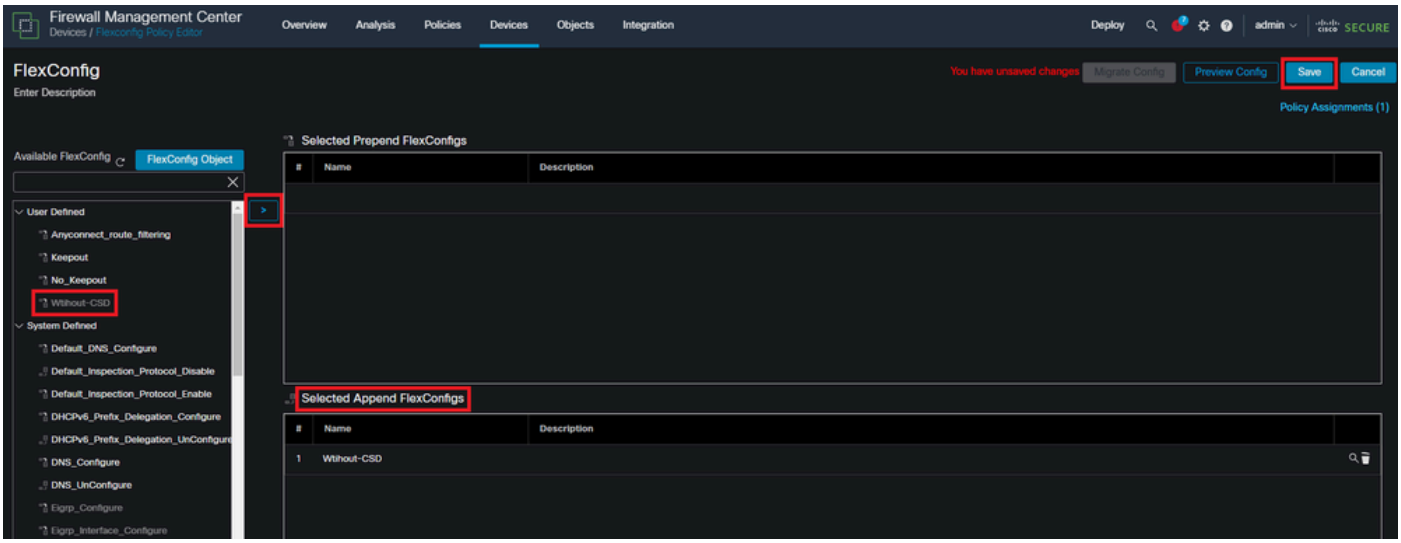
Navigieren Sie zu Devices > FlexConfig, und klicken Sie dann auf den Bleistift, um die FlexConfig-

Richtlinie zu bearbeiten.



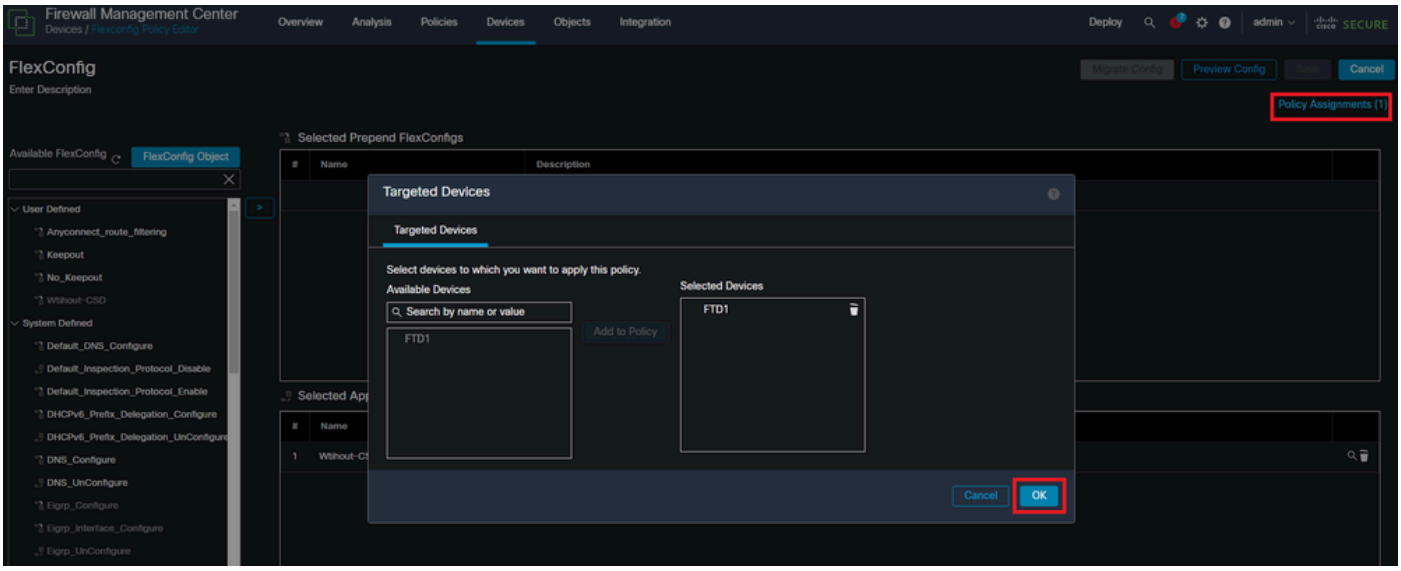
Bearbeiten der FlexConfig-Richtlinie innerhalb des FMC

Suchen Sie das Objekt, das Sie im Abschnitt Benutzerdefiniert erstellt haben. Klicken Sie anschließend auf den Pfeil, um es zu "Ausgewählte FlexConfigs anhängen" hinzuzufügen. Wählen Sie abschließend Speichern, um die FlexConfig-Richtlinie zu speichern.



Hängen Sie das FlexConfig-Objekt an die FlexConfig-Richtlinie an.

Wählen Sie Policy Assignments (Richtlinienzuweisungen) und das FTD aus, auf das Sie diese FlexConfig-Richtlinie anwenden möchten. Wählen Sie anschließend OK. Wählen Sie erneut Speichern, wenn es sich um eine neue FlexConfig-Zuweisung handelt, und stellen Sie die Änderungen bereit. Überprüfen Sie nach der Bereitstellung



Weisen Sie die FlexConfig-Richtlinie einem FirePOWER-Gerät zu.

Geben Sie die FTD-CLI ein, und geben Sie den Befehl show run tunnel-group für DefaultWEBVPNGroup und DefaultRAGroup aus. Vergewissern Sie sich, dass "without-csd" in der Konfiguration vorhanden ist.

<#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#

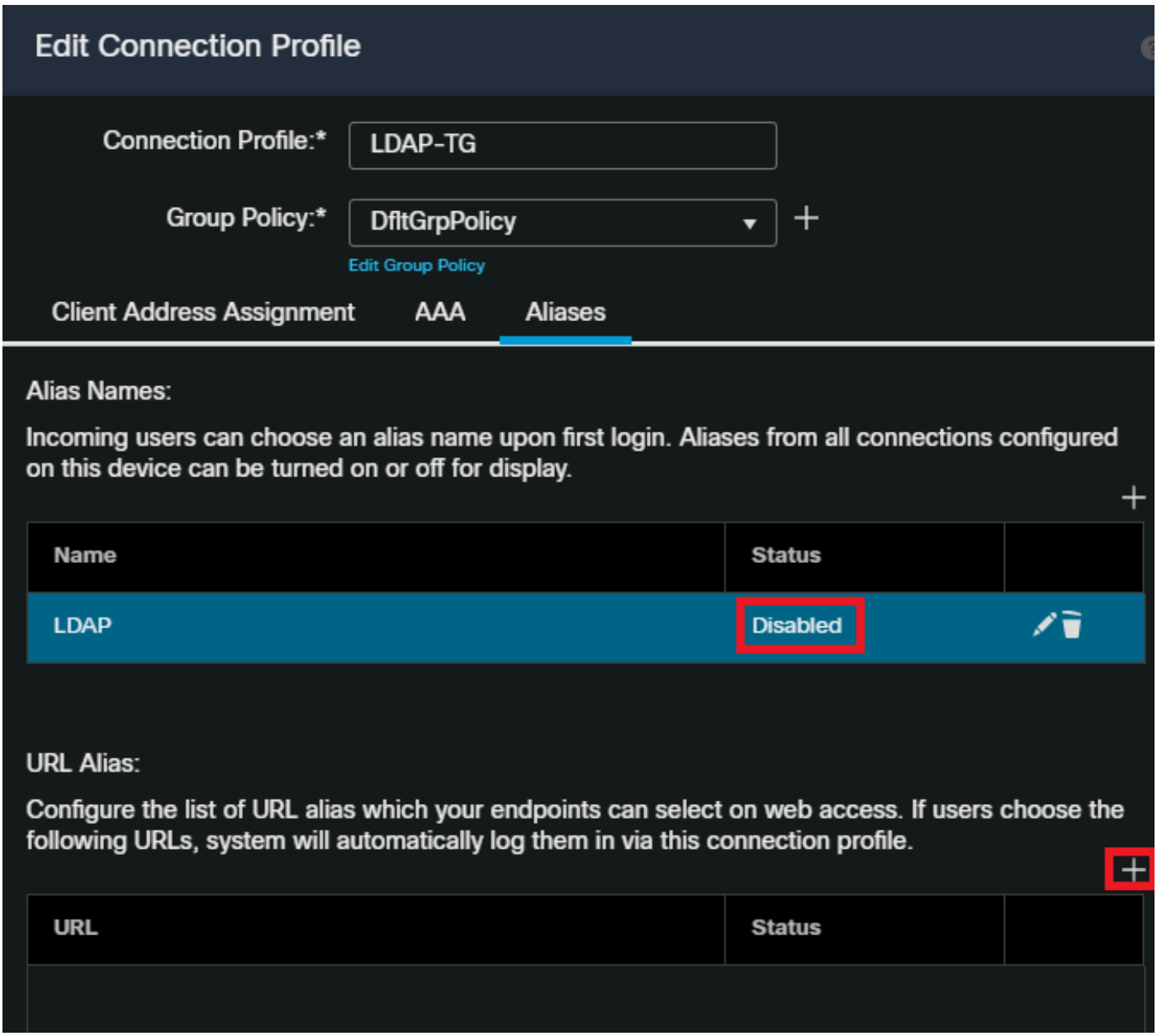
show run tunnel-group DefaultWEBVPNGroup

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

without-csd

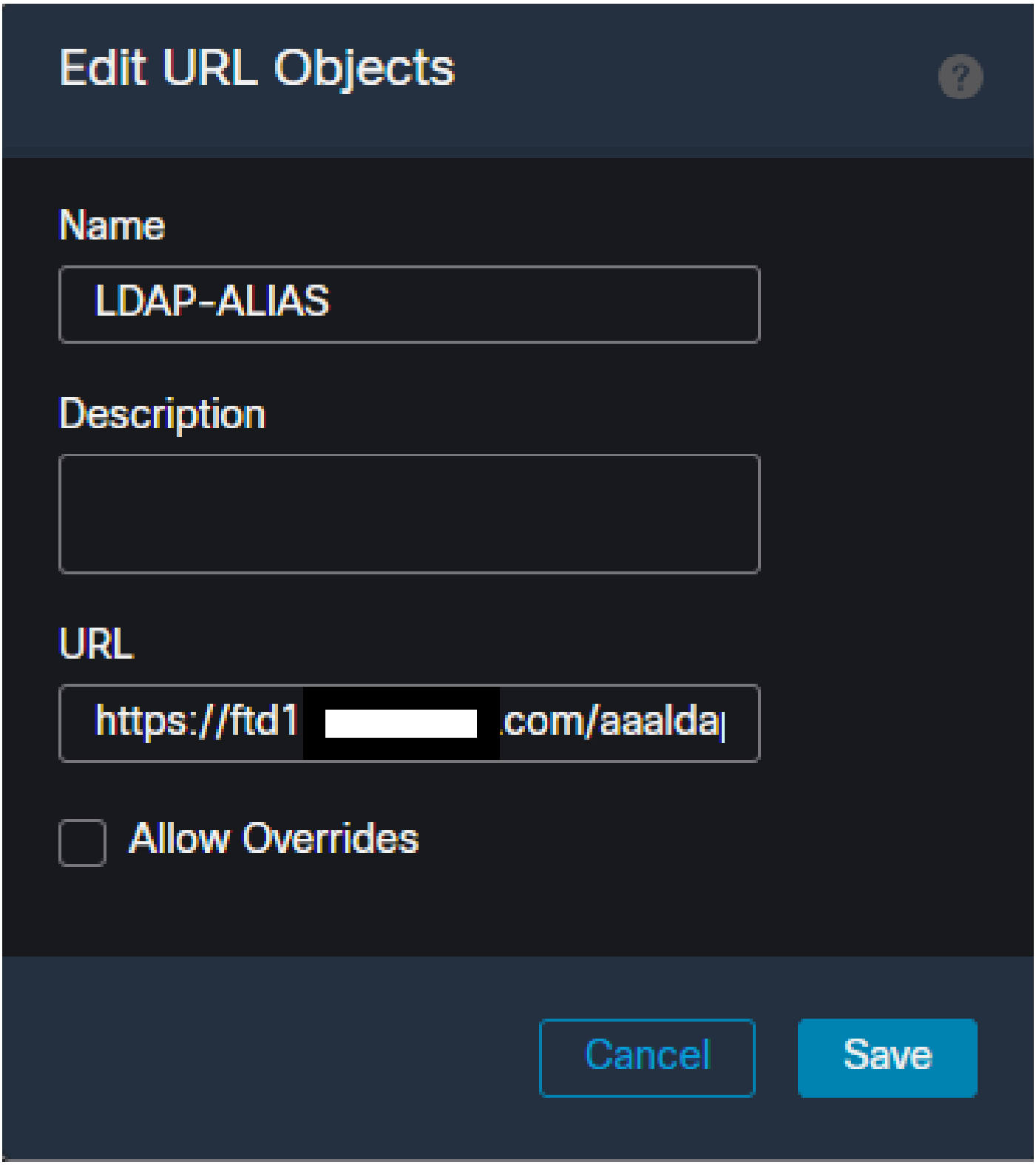
Gruppenaliase deaktivieren und Gruppen-URLs aktivieren

Navigieren Sie zu einem Verbindungsprofil und wählen Sie die Registerkarte 'Aliase'. Deaktivieren oder löschen Sie den Gruppenalias, und klicken Sie auf das Pluszeichen, um einen URL-Alias hinzuzufügen.



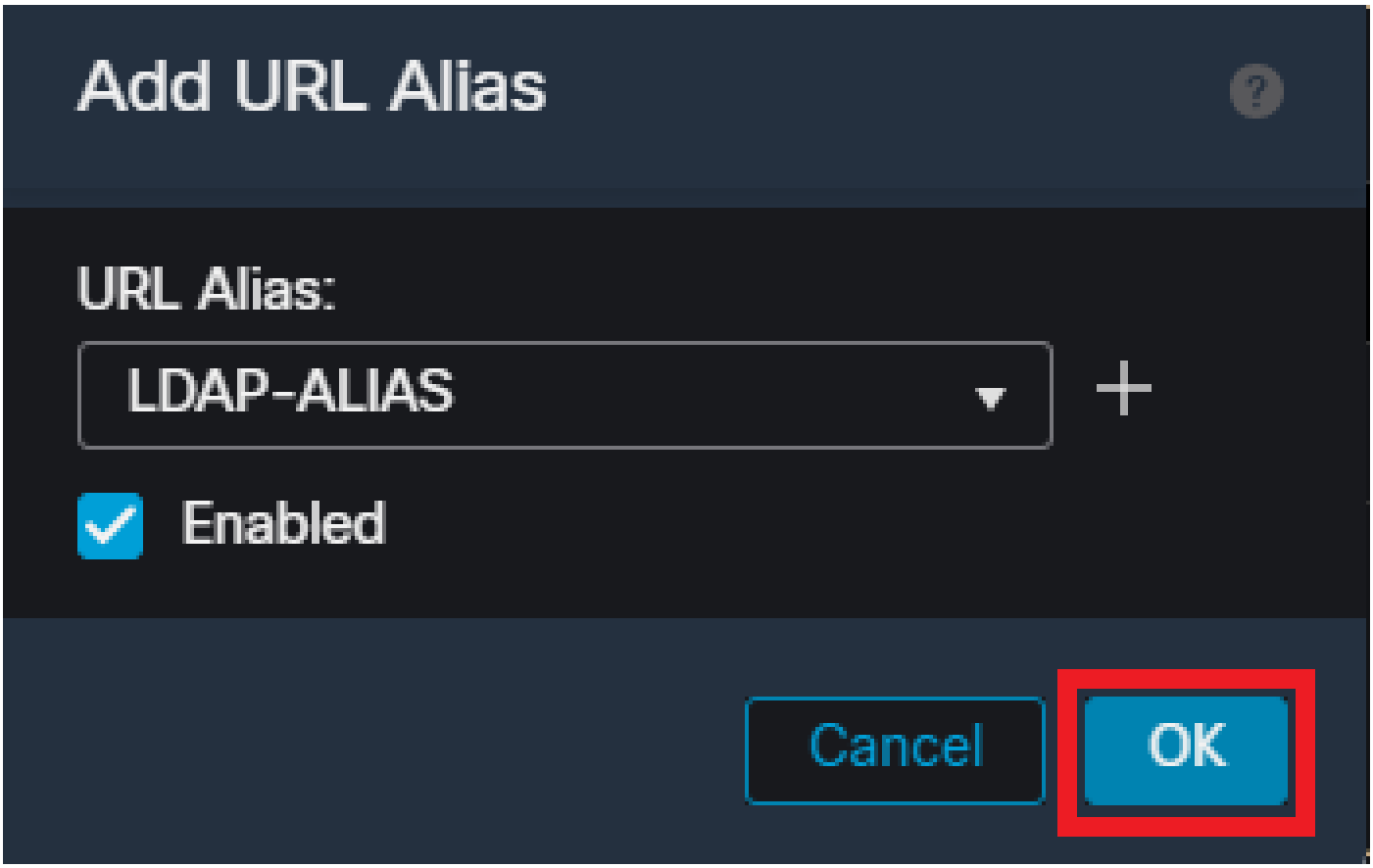
Deaktivieren der Gruppenalias-Option für eine Tunnelgruppe in der FMC-Benutzeroberfläche.

Konfigurieren Sie einen Objektnamen für den URL-Alias, und geben Sie den FQDN und/oder die IP-Adresse der Firewall für die URL ein, gefolgt vom Namen, mit dem Sie das Verbindungsprofil verknüpfen möchten. In diesem Beispiel haben wir 'aaaldap' gewählt. Je obskurer, desto sicherer, da es für Angreifer weniger wahrscheinlich ist, die vollständige URL zu erraten, selbst wenn sie Ihren FQDN erhalten haben. Wählen Sie anschließend Speichern aus.



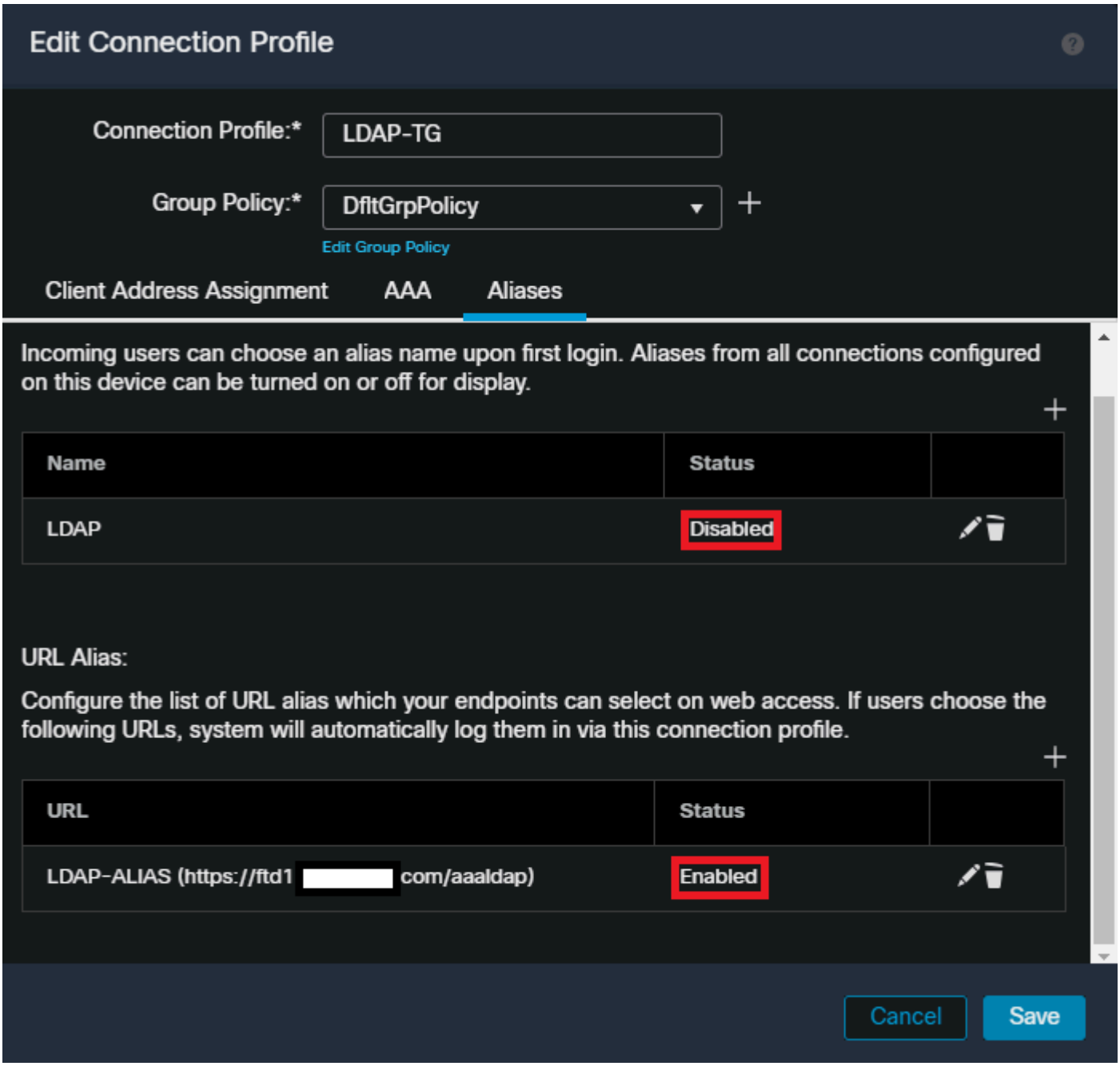
Erstellen eines URL-Alias-Objekts in der FMC-Benutzeroberfläche

Wählen Sie aus dem Dropdown-Menü den URL-Alias aus, aktivieren Sie das Kontrollkästchen Enabled (Aktiviert), und wählen Sie OK aus.



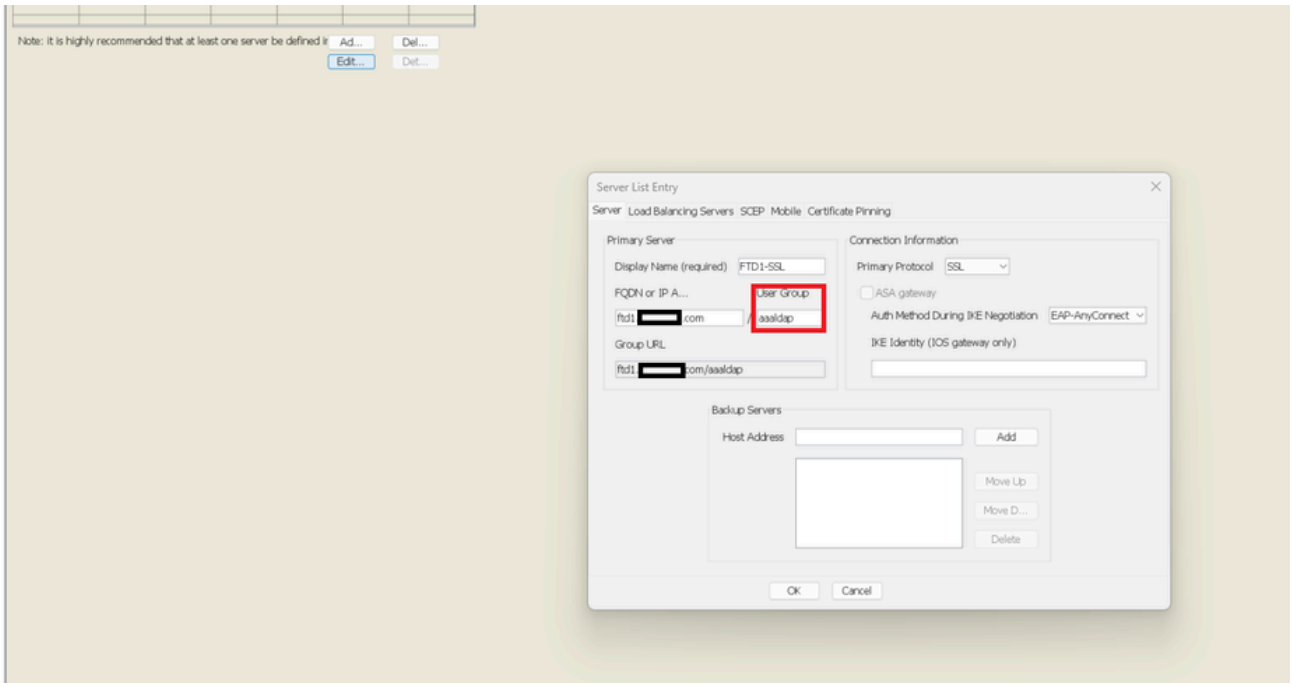
Stellen Sie sicher, dass der URL-Alias in der FMC-Benutzeroberfläche aktiviert ist.

Stellen Sie sicher, dass der Gruppenalias gelöscht oder deaktiviert ist, und stellen Sie sicher, dass der URL-Alias jetzt aktiviert ist. Wählen Sie anschließend Speichern aus.



Aktivieren der Option URL-Alias für eine Tunnelgruppe in der FMC-Benutzeroberfläche.

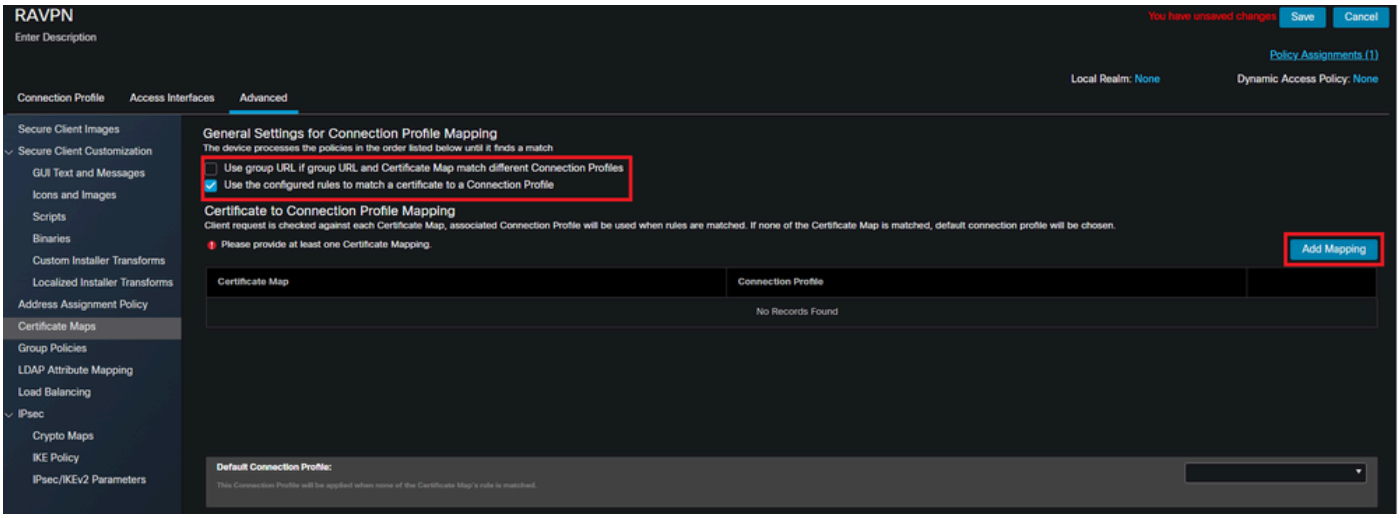
Bei Bedarf können URL-Aliase auch als Teil des XML-Codes weitergegeben werden. Dies wird durch die Bearbeitung des XML-Codes mit dem VPN Profile Editor oder dem ASA Profile Editor erreicht. Navigieren Sie zu diesem Zweck zur Registerkarte "Serverliste", und stellen Sie sicher, dass das Feld "Benutzergruppe" bei Verwendung von SSL mit dem URL-Alias des Verbindungsprofils übereinstimmt. Stellen Sie bei IKEv2 sicher, dass das Feld User Group (Benutzergruppe) mit dem genauen Namen des Verbindungsprofils übereinstimmt.



Bearbeiten des XML-Profils mit einem URL-Alias für SSL-Verbindungen.

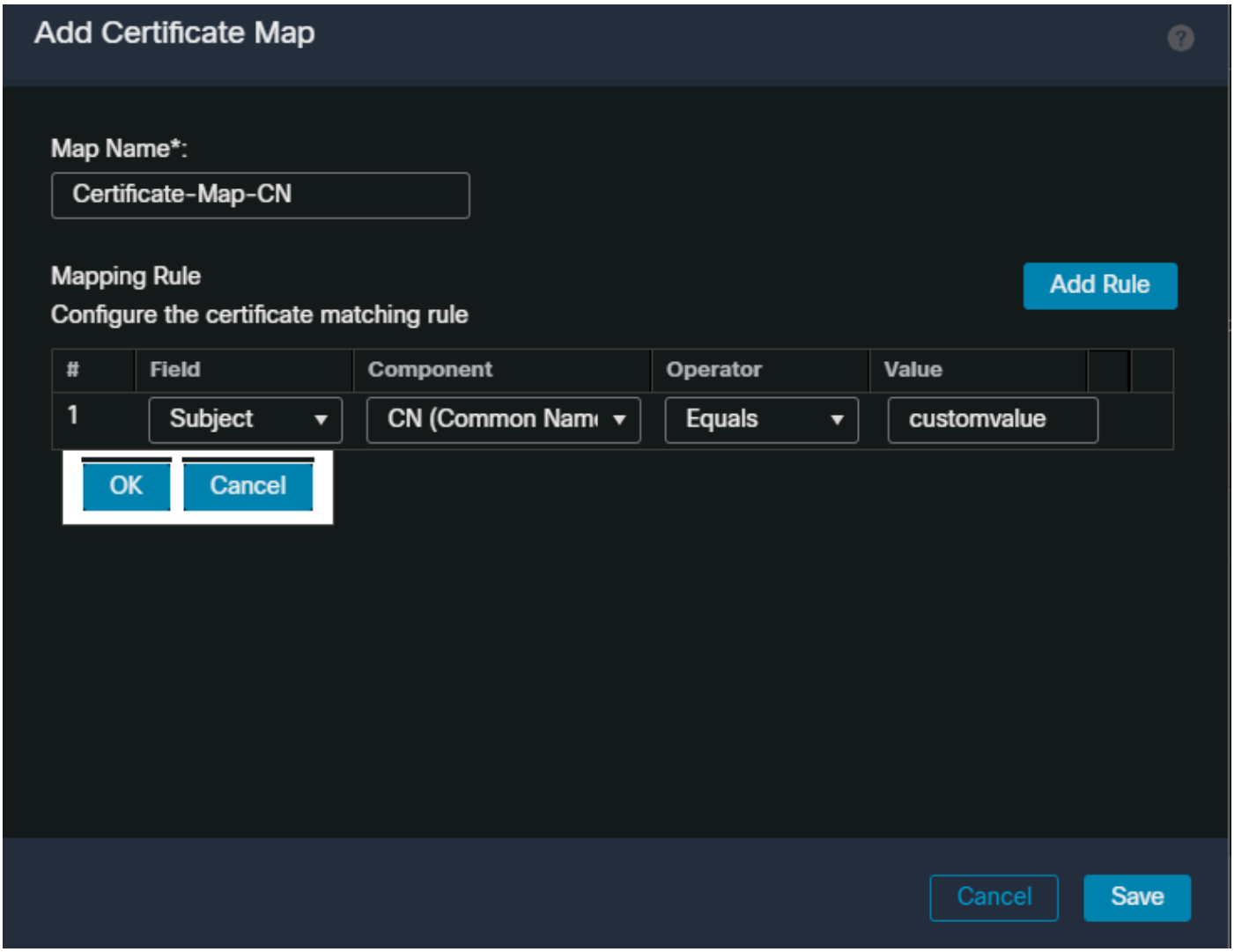
Zertifikatszuordnung

Navigieren Sie zur Registerkarte Advanced (Erweitert) in der VPN-Richtlinie für den Remote-Zugriff. Wählen Sie je nach Präferenz eine allgemeine Einstellungsoption aus. Wählen Sie anschließend Zuordnung hinzufügen aus.



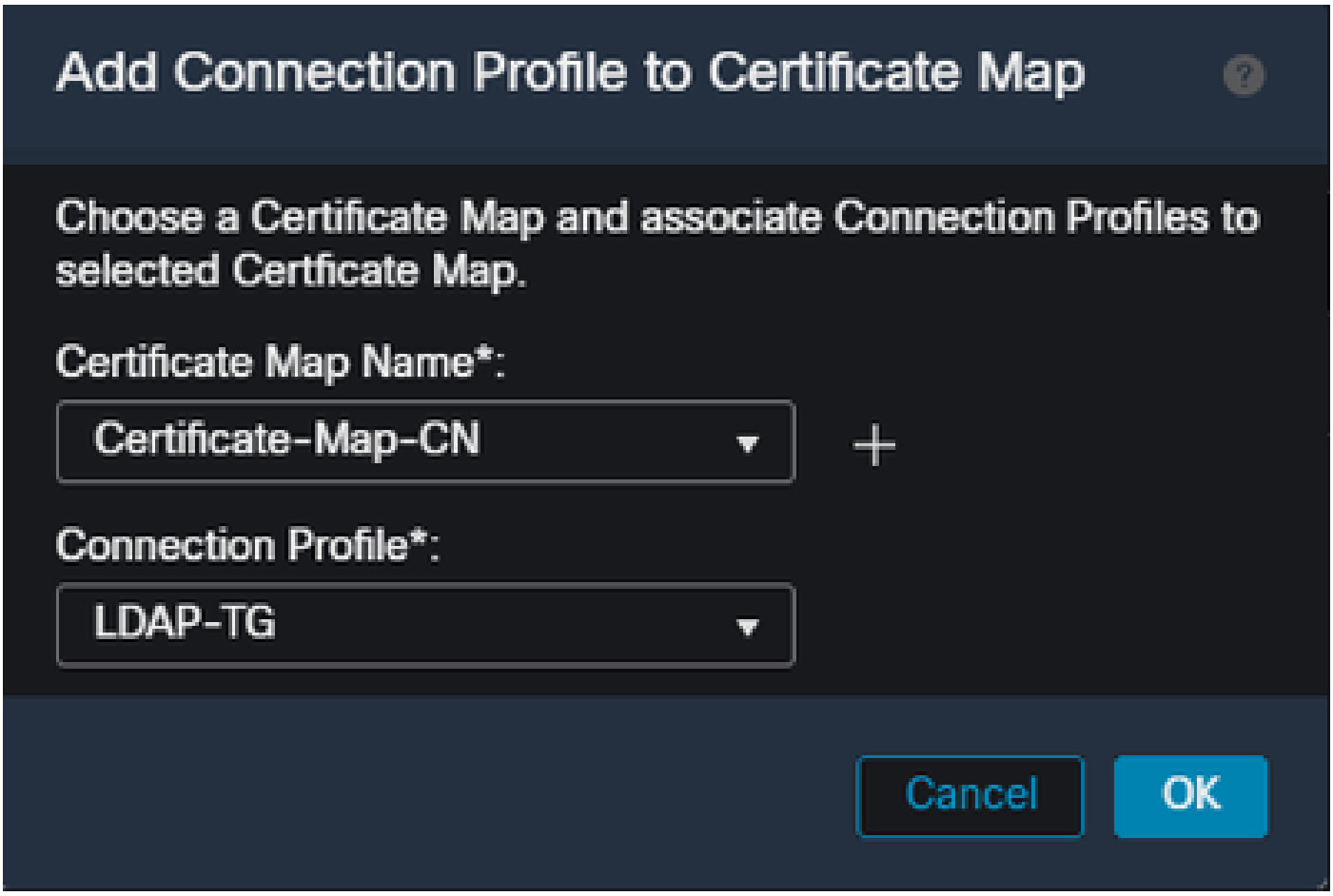
Navigieren Sie zur Registerkarte Erweitert in der FMC-Benutzeroberfläche, um ein Zertifikatzuordnungsobjekt in der FMC-Benutzeroberfläche zu erstellen.

Geben Sie dem Zertifikatzuordnungsobjekt einen Namen, und wählen Sie Regel hinzufügen aus. Definieren Sie in dieser Regel die Eigenschaften des Zertifikats, das Sie identifizieren möchten, um den Benutzer einem bestimmten Verbindungsprofil zuzuordnen. Wählen Sie anschließend OK und anschließend Speichern.



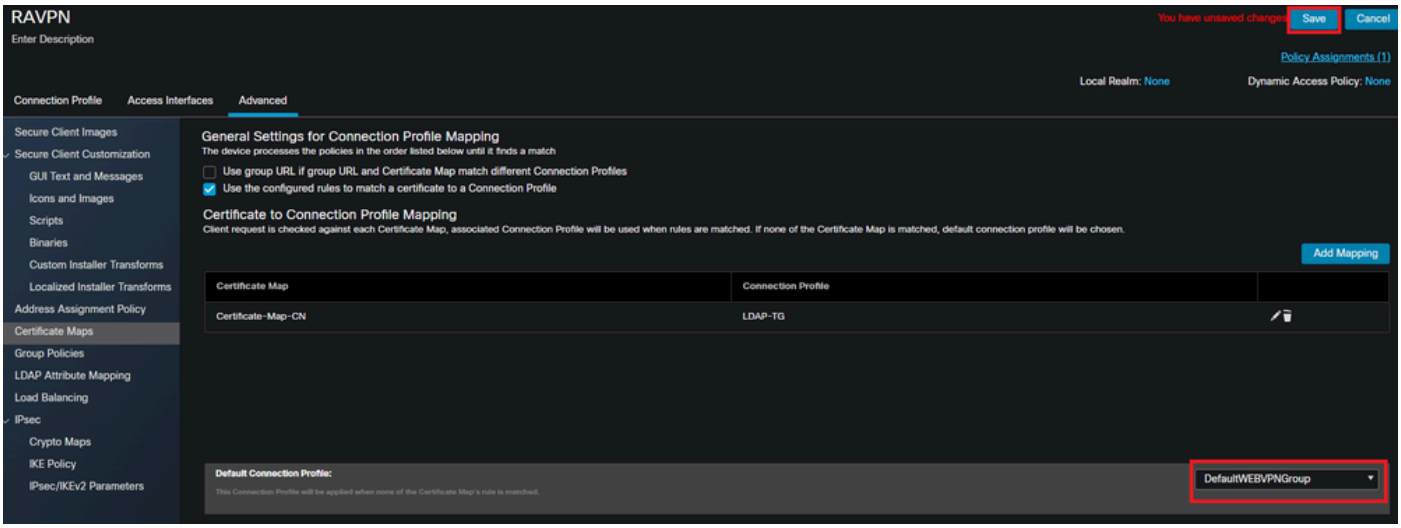
Erstellen Sie eine Zertifikatszuordnung, und fügen Sie Kriterien für die Zuordnung innerhalb der FMC-Benutzeroberfläche hinzu.

Wählen Sie aus dem Dropdown-Menü das Zertifikatzuordnungsobjekt und das Verbindungsprofil aus, dem die Zertifikatzuordnung zugeordnet werden soll. Wählen Sie dann OK aus.



Verknüpfen Sie das Zertifikatzuordnungsobjekt mit der gewünschten Tunnelgruppe in der FMC-Benutzeroberfläche.

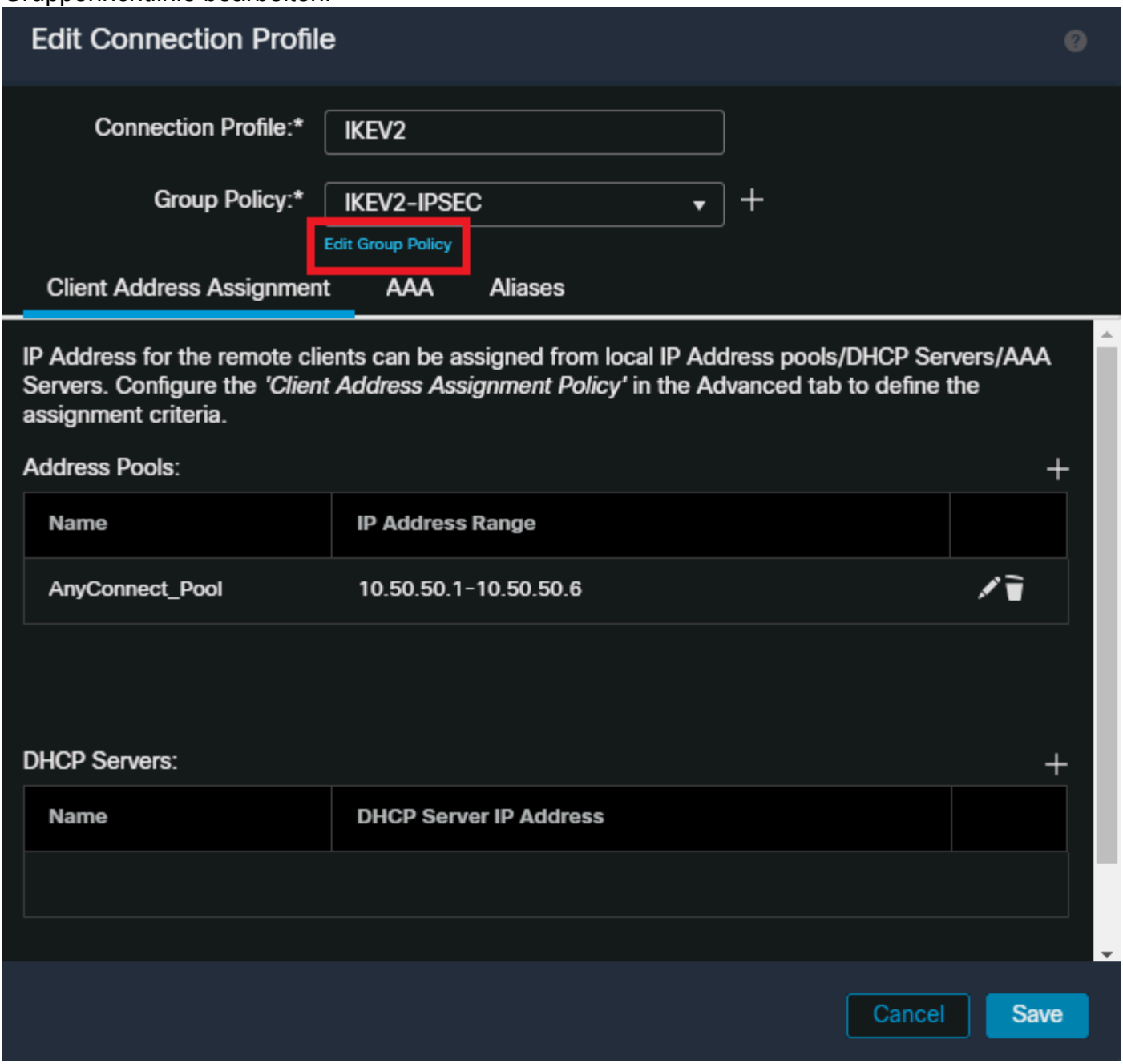
Vergewissern Sie sich, dass das Standardverbindungsprofil als DefaultWEBVPNGroup konfiguriert ist. Wenn ein Benutzer die Zuordnung nicht bekommt, wird er an DefaultWEBVPNGroup gesendet. Wählen Sie anschließend Speichern und verteilen Sie die Änderungen.



Ändern Sie das Standardverbindungsprofil für die Zertifikatszuordnung in die DefaultWEBVPNGroup innerhalb der FMC-Benutzeroberfläche.

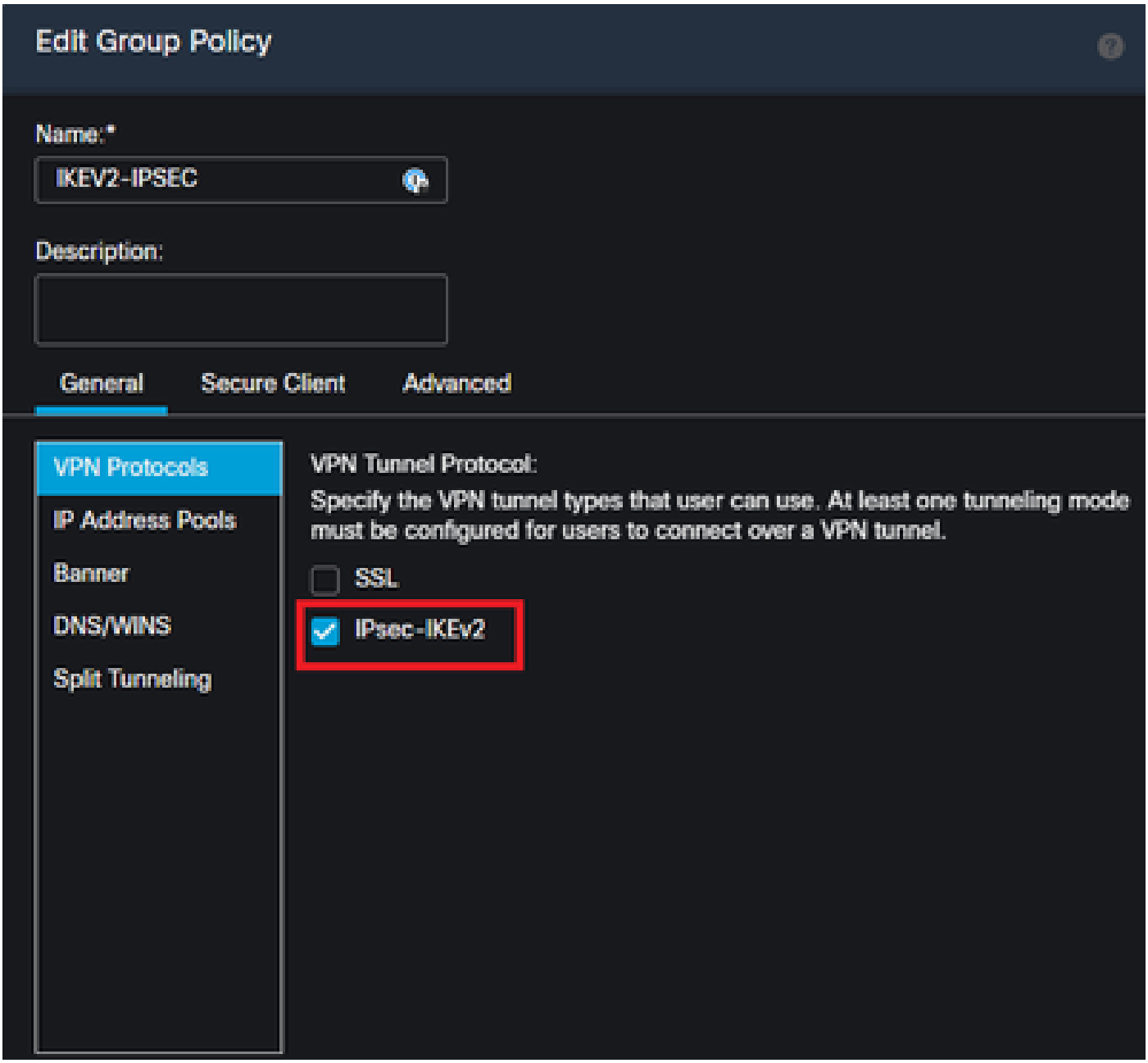
IPsec-IKEv2

Wählen Sie das gewünschte IPsec-IKEv2-Verbindungsprofil aus, und navigieren Sie zu Gruppenrichtlinie bearbeiten.



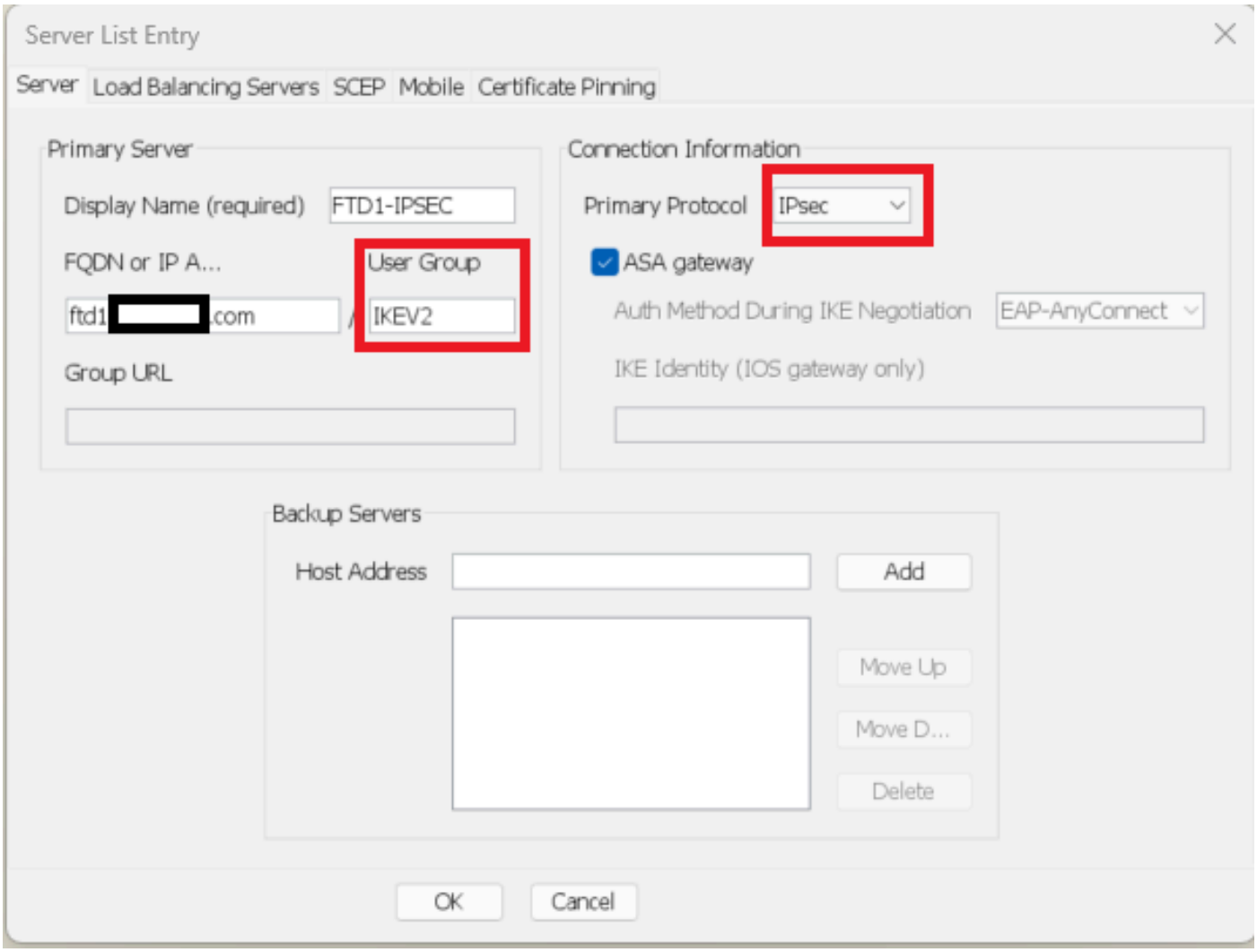
Bearbeiten einer Gruppenrichtlinie in der FMC-Benutzeroberfläche

Navigieren Sie auf der Registerkarte General (Allgemein) zum Abschnitt VPN Protocols (VPN-Protokolle), und stellen Sie sicher, dass das Kontrollkästchen IPsec-IKEv2 aktiviert ist.

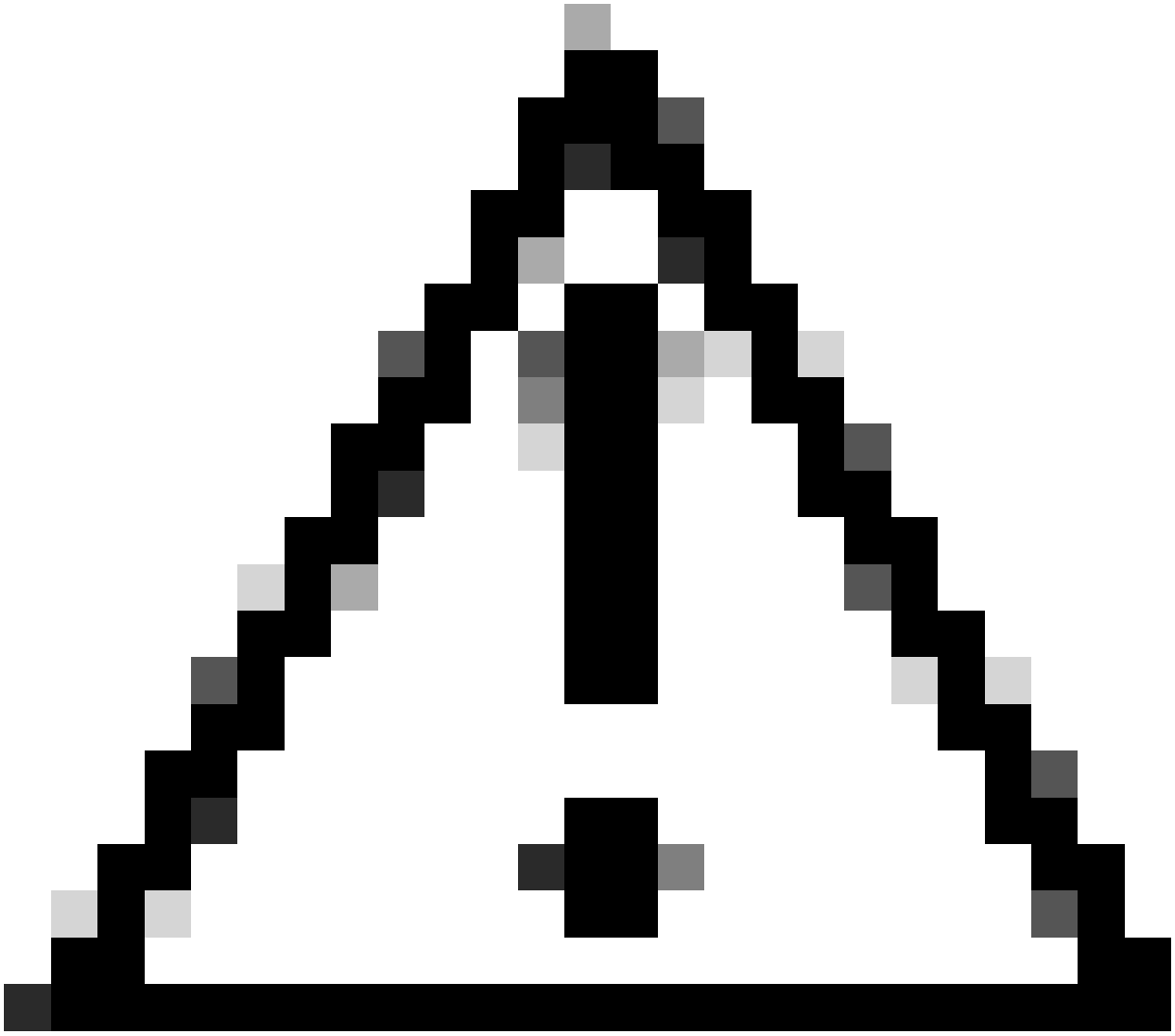


Aktivieren Sie IPsec-IKEv2 innerhalb einer Gruppenrichtlinie in der FMC-Benutzeroberfläche.

Navigieren Sie im VPN Profile Editor oder ASA Profile Editor zur Registerkarte Server List (Serverliste). Der Benutzername für die Benutzergruppe MUSS exakt mit dem Namen des Verbindungsprofils auf der Firewall übereinstimmen. In diesem Beispiel war IKEV2 der Name des Verbindungsprofils/der Benutzergruppe. Das primäre Protokoll wird als IPsec konfiguriert. Der Anzeigename in wird dem Benutzer in der Secure Client-Benutzeroberfläche angezeigt, wenn eine Verbindung mit diesem Verbindungsprofil hergestellt wird.

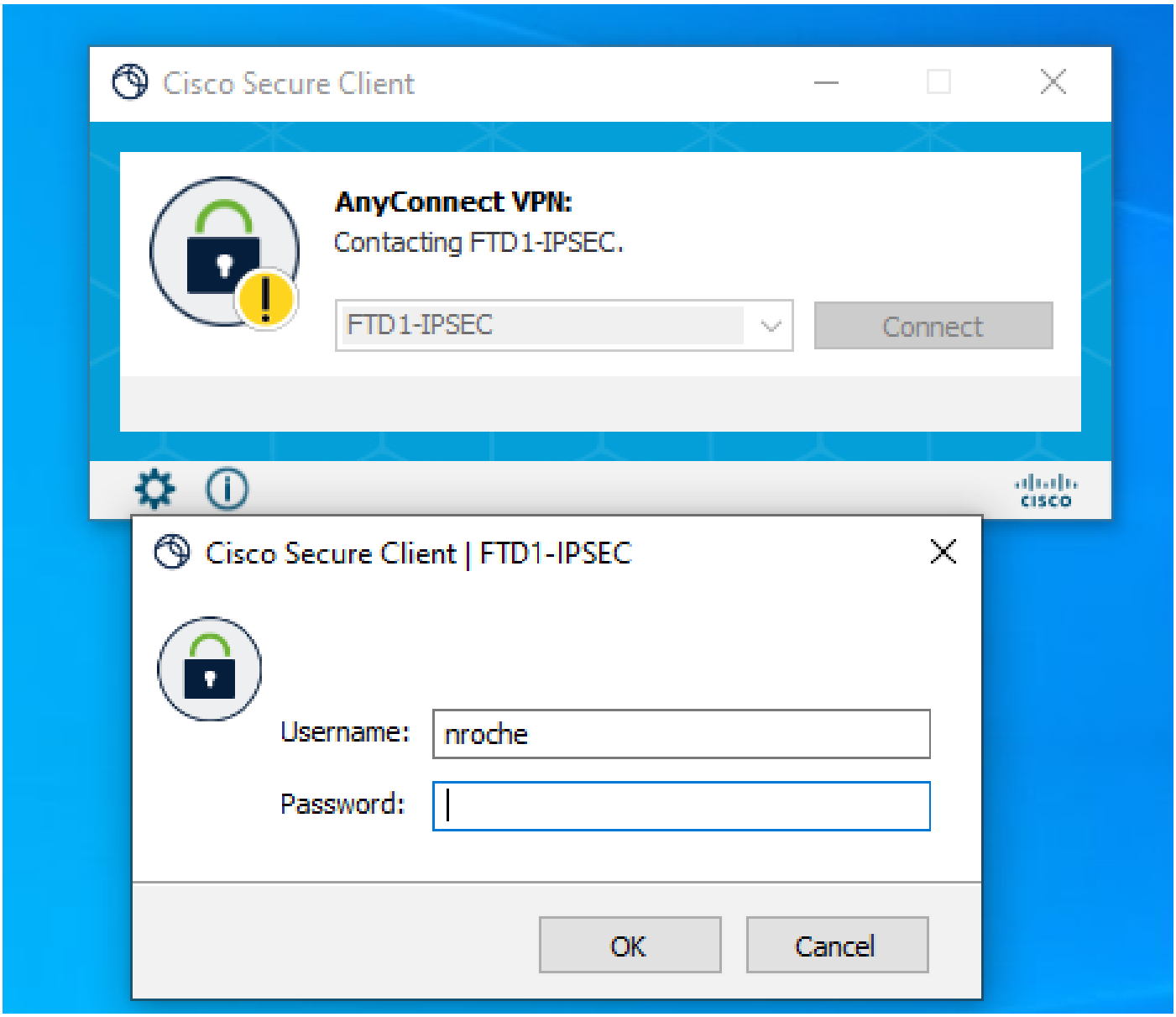


Bearbeiten Sie das XML-Profil so, dass das primäre Protokoll IPsec ist und die Benutzergruppe mit dem Namen des Verbindungsprofils übereinstimmt.



Vorsicht: Eine SSL-Verbindung ist erforderlich, um XML-Profile von der Firewall an den Client zu übertragen. Wenn nur IKEV2-IPsec verwendet wird, müssen die XML-Profile über eine Out-of-Band-Methode an die Clients übertragen werden.

Sobald das XML-Profil an den Client übertragen wurde, verwendet der sichere Client die Benutzergruppe aus dem XML-Profil, um eine Verbindung mit dem IKEV2-IPsec-Verbindungsprofil herzustellen.



Sichere Client-UI-Ansicht des IPsec-IKEv2 RAVPN-Verbindungsversuchs.

ASA-Konfigurationsbeispiele

Deaktivieren Sie die AAA-Authentifizierung in den Verbindungsprofilen DefaultWEBVPNGroup und DefaultRAGroup.

Geben Sie den Abschnitt "webvpn-attribute" für die Tunnelgruppe "DefaultWEBVPNGroup" ein, und geben Sie die Authentifizierung als zertifikatbasiert an. Wiederholen Sie diesen Vorgang für die DefaultRAGroup. Benutzer, die auf diesen Standard-Verbindungsprofilen landen, müssen ein Zertifikat für die Authentifizierung vorlegen. Sie erhalten keine Möglichkeit, Benutzernamen und Kennwörter einzugeben.

```
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
```

Deaktivieren Sie Hostscan/Secure Firewall Posture auf der DefaultWEBVPNGroup und DefaultRAGroup (optional).

Dies ist nur erforderlich, wenn Sie Hostscan/Secure Firewall Posture in Ihrer Umgebung haben. Dieser Schritt verhindert, dass Angreifer die durch den Endpunkt-Scanvorgang verursachte Ressourcennutzung auf der Firewall erhöhen. Öffnen Sie den Abschnitt "webvpn-attribute" für die DefaultWEBVPNGroup- und DefaultRAGroup- sowie die Verbindungsprofile, und implementieren Sie without-csd, um die Funktion zum Scannen von Endpunkten zu deaktivieren.

```
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
```

Gruppenaliase deaktivieren und Gruppen-URLs aktivieren

Geben Sie die Tunnelgruppe(n) ein, mit der Benutzer eine Verbindung herstellen. Wenn bereits ein Gruppenalias vorhanden ist, deaktivieren oder entfernen Sie ihn. In diesem Beispiel ist sie deaktiviert. Erstellen Sie anschließend eine Gruppen-URL, die den FQDN oder die IP-Adresse der RAVPN-Terminierungsschnittstelle verwendet. Der Name am Ende der Gruppen-URL muss unklar sein. Vermeiden Sie gängige Werte wie VPN, AAA, RADIUS oder LDAP, da diese es Angreifern erleichtern, die vollständige URL zu erraten, wenn sie den FQDN erhalten. Verwenden Sie stattdessen intern relevante Namen, mit denen Sie die Tunnelgruppe identifizieren können.

```
ASA# configure terminal
ASA(config)# tunnel-group NAME webvpn-attributes
ASA(config-tunnel-webvpn)# group-alias NAME disable
ASA(config-tunnel-webvpn)# group-url https://FQDN/name enable
```

Zertifikatszuordnung

Erstellen Sie im globalen Konfigurationsmodus eine Zertifikatszuordnung, und weisen Sie ihr einen Namen und eine Sequenznummer zu. Definieren Sie dann eine Regel, die die Benutzer zur Verwendung der Zuordnung abgleichen müssen. In diesem Beispiel müssen Benutzer die

Kriterien eines gemeinsamen Namenswerts erfüllen, der "customvalue" entspricht. Geben Sie dann die WebVPN-Konfiguration ein, und wenden Sie die Zertifikatszuordnung auf die gewünschte Tunnelgruppe an. Geben Sie nach Abschluss des Vorgangs die DefaultWEBVPNGroup (Standard-WEBVPN-Gruppe) ein, und legen Sie diese Tunnelgruppe als Standard für Benutzer fest, die die Zertifikatszuordnung nicht erfüllen. Wenn die Zuordnung für Benutzer fehlschlägt, werden sie an die DefaultWEBVPNGroup weitergeleitet. Während die DefaultWEBVPNGroup mit Zertifikatsauthentifizierung konfiguriert ist, haben Benutzer keine Möglichkeit, Benutzernamen oder Kennwörter weiterzugeben.

```
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
```

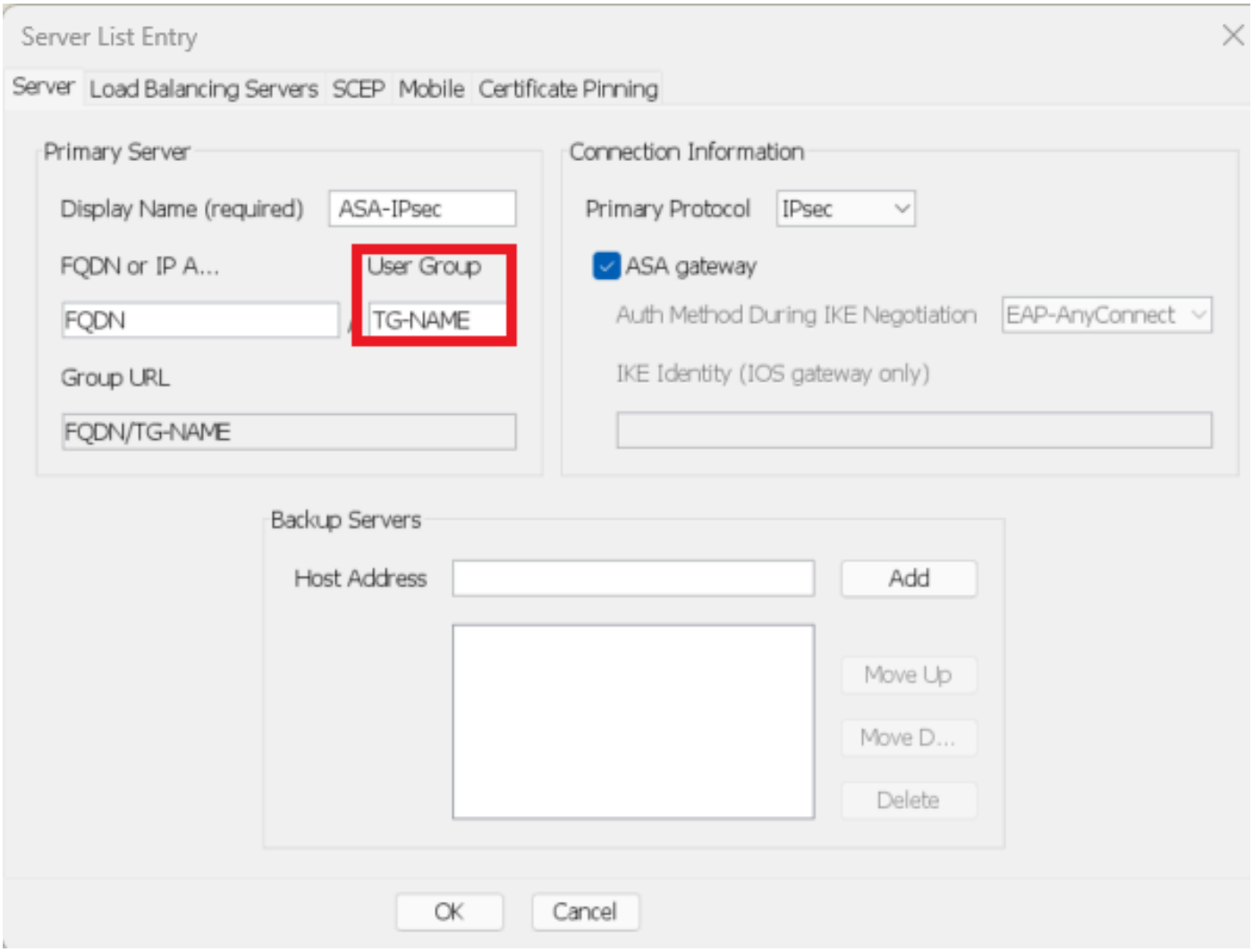
IPsec-IKEv2

Im globalen Konfigurationsmodus können Sie eine vorhandene Gruppenrichtlinie bearbeiten oder eine neue erstellen und die Attribute für diese Gruppenrichtlinie eingeben. Aktivieren Sie IKEv2 im Attributabschnitt als einziges VPN-Tunnelprotokoll. Stellen Sie sicher, dass diese Gruppenrichtlinie mit einer Tunnelgruppe verknüpft ist, die für IPsec-IKEV2-VPN-Verbindungen für den Remotezugriff verwendet wird. Ähnlich wie bei den FMC-Schritten müssen Sie das XML-Profil über den VPN Profile Editor oder den ASA Profile Editor bearbeiten und das Feld User Group so ändern, dass es mit dem Namen der Tunnelgruppe auf der ASA übereinstimmt, und das Protokoll in IPsec ändern.

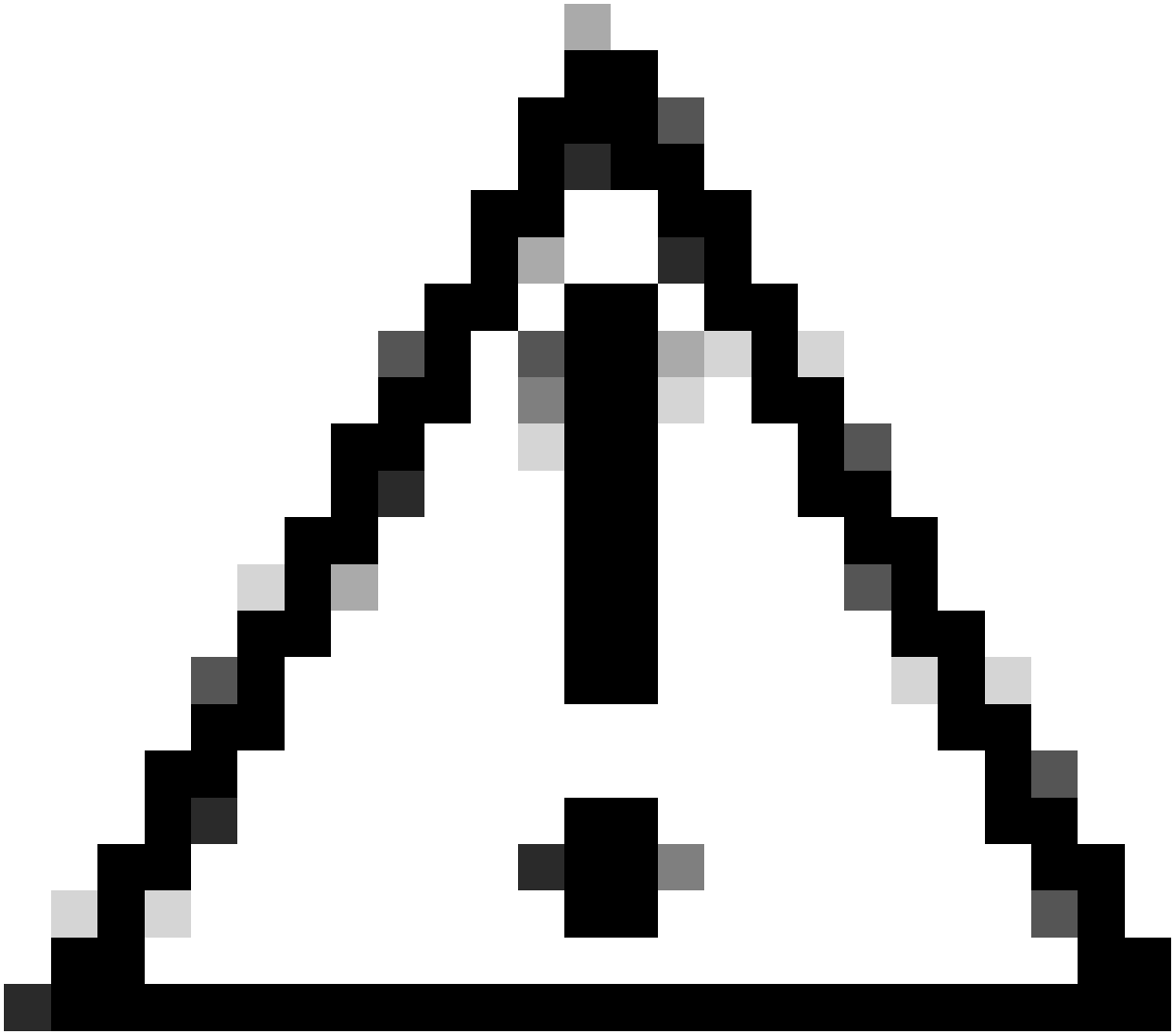
```
ASA# configure terminal
ASA(config)# group-policy GP-NAME internal
ASA(config)# group-policy GP-NAME attributes
ASA(config-group-policy)# vpn-tunnel-protocol ikev2

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

Navigieren Sie im VPN Profile Editor oder ASA Profile Editor zur Registerkarte Server List (Serverliste). Der Benutzername für die Benutzergruppe MUSS exakt mit dem Namen des Verbindungsprofils auf der Firewall übereinstimmen. Das primäre Protokoll wird als IPsec konfiguriert. Der Anzeigename wird dem Benutzer in der Secure Client-Benutzeroberfläche angezeigt, wenn eine Verbindung mit diesem Verbindungsprofil hergestellt wird.



Bearbeiten Sie das XML-Profil so, dass der primäre Protokollname IPsec lautet und der Benutzername mit dem Tunnelgruppennamen der ASA für IPsec-IKEv2-RAVPN-Verbindungen übereinstimmt.



Vorsicht: Eine SSL-Verbindung ist erforderlich, um XML-Profile von der Firewall an den Client zu übertragen. Wenn nur IKEV2-IPsec verwendet wird, müssen die XML-Profile über eine Out-of-Band-Methode an die Clients übertragen werden.

Schlussfolgerung

Zusammenfassend besteht der Zweck der Härtungspraktiken in diesem Dokument darin, legitime Benutzer benutzerdefinierten Verbindungsprofilen zuzuordnen, während Angreifer zur DefaultWEBVPNGroup und zur DefaultRAGroup gezwungen werden. In einer optimierten Konfiguration verfügen die beiden Standardverbindungsprofile über keine benutzerdefinierte AAA-Serverkonfiguration. Darüber hinaus wird durch das Entfernen von Gruppen-Aliasen verhindert, dass Angreifer auf einfache Weise benutzerdefinierte Verbindungsprofile identifizieren können, indem sie die Dropdown-Sichtbarkeit beim Navigieren zum FQDN oder zur öffentlichen IP-Adresse der Firewall entfernen.

Zugehörige Informationen

Technischer Support und Downloads von Cisco

Angriffe durch Passwortverbreitung

Sicherheitslücke bei nicht autorisiertem Zugriff September 2023

ASA-Konfigurationsanleitungen

FMC-/FDM-Konfigurationsanleitungen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.