

# Invoeren van harde maatregelen voor beveiligde client-AnyConnect VPN

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Concepten](#)

[Beveiligde praktijken voor clientharding op Cisco Secure Firewall:](#)

[Identificeer aanvallen met vastlegging- en syslog-id's](#)

[Aanvalsverificatie](#)

[FMC-configuratievoorbeelden](#)

[AAA-verificatie uitschakelen in de standaard-WEBVPN-groep en DefaultRAGroup-verbindingsprofielen](#)

[Hostscan/Secure Firewall postuur uitschakelen in de DefaultWEBVPNGroup en DefaultRAGroup \(optioneel\)](#)

[Groepsaliassen uitschakelen en Groep-URL's inschakelen](#)

[Toewijzing van certificaten](#)

[IPsec-IKEv2](#)

[ASA-configuratievoorbeelden](#)

[AAA-verificatie uitschakelen in de standaard-WEBVPN-groep en DefaultRAGroup-verbindingsprofielen](#)

[Hostscan/Secure Firewall postuur uitschakelen in de DefaultWEBVPNGroup en DefaultRAGroup \(optioneel\)](#)

[Groepsaliassen uitschakelen en Groep-URL's inschakelen](#)

[Toewijzing van certificaten](#)

[IPsec-IKEv2](#)

[Conclusie](#)

[Gerelateerde informatie](#)

---

## Inleiding

Dit document beschrijft hoe u de beveiliging van uw implementatie van Remote Access VPN kunt verbeteren.

## Voorwaarden

### Vereisten

Cisco raadt u aan deze onderwerpen te kennen:

- Cisco Secure-client voor AnyConnect VPN.
- ASA/FTD-configuratie voor externe toegang.

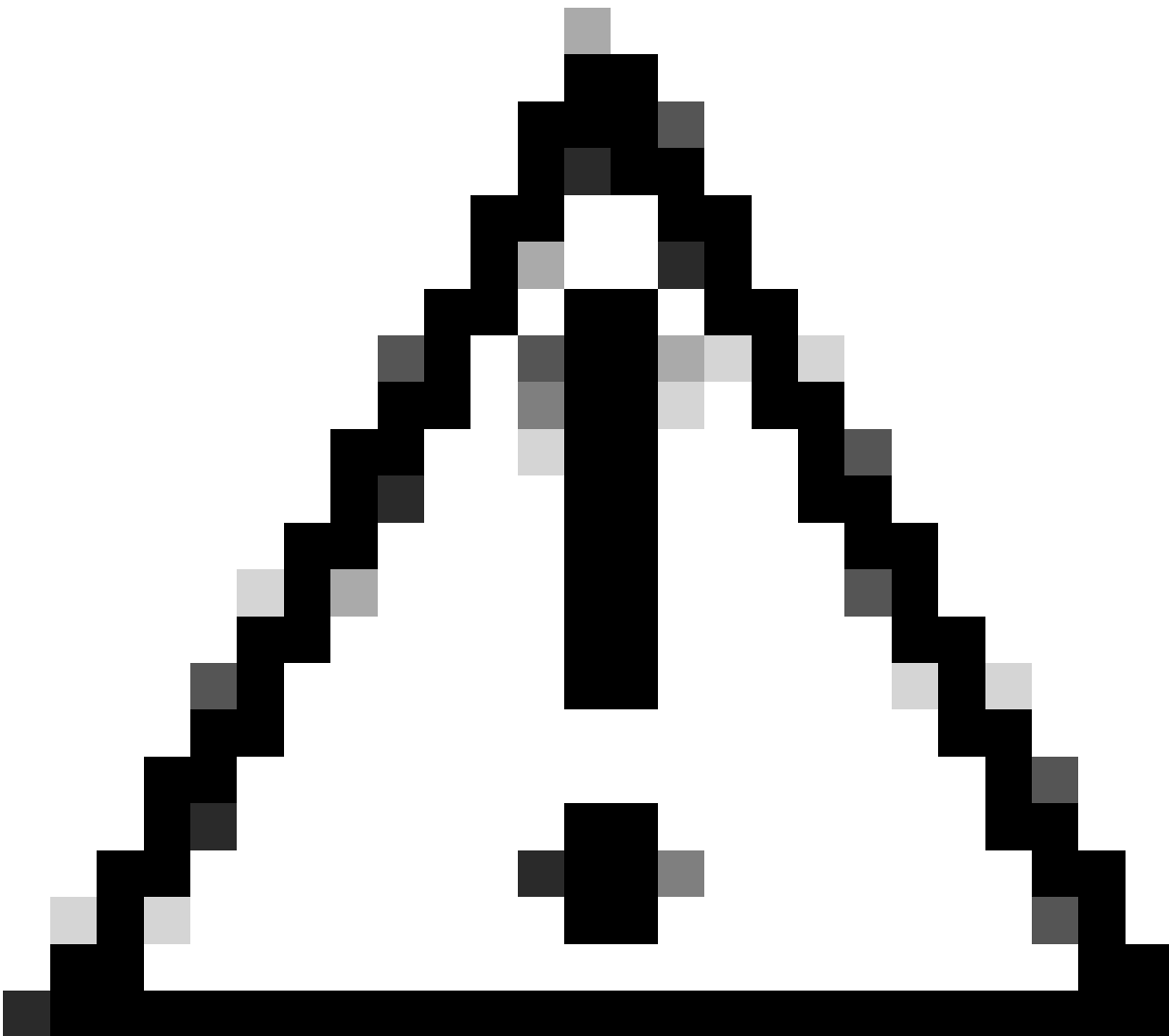
## Gebruikte componenten

De best practices guide is gebaseerd op deze hardware- en softwareversies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

---



Waarschuwing: dit document bevat geen stappen voor Firepower Device Manager (FDM). De FDM ondersteunt alleen het wijzigen van de verificatiemethode op de DefaultWEBVPNGroep. Gebruik ACL's (control-plane) of een aangepaste poort in de

---

---

sectie 'Global Settings' van Remote Access VPN in de FDM UI. Neem contact op met het Cisco Technical Assistance Center (TAC) voor verdere assistentie, indien nodig.

---

## Achtergrondinformatie

Het doel van dit document is om er zeker van te zijn dat de configuratie van Cisco Secure Client AnyConnect VPN voldoet aan de best practices op het gebied van beveiliging in een moderne wereld waarin cyberbeveiligingsaanvallen gebruikelijk zijn.

Brute force aanvallen impliceren gewoonlijk herhaalde pogingen om toegang tot een middel te krijgen door gebruikersbenaming en wachtwoordcombinaties te gebruiken. De aanvallers proberen hun internetbrowser, de Secure Client-gebruikersinterface of andere tools te gebruiken om meerdere gebruikersnamen en wachtwoorden in te voeren in de hoop dat ze een legitieme combinatie in een AAA-database evenaren. Bij het gebruik van AAA voor verificatie verwachten we dat de eindgebruiker zijn gebruikersnaam en wachtwoord invoert, omdat dit nodig is om de verbinding tot stand te brengen. Tegelijkertijd controleren we niet wie de gebruiker is totdat ze hun referenties invoeren. Dit stelt aanvallers van nature in staat om voordeel te halen uit deze scenario's:

1. Volledig gekwalificeerde domeinnamen voor de Cisco Secure Firewall (met name bij gebruik van een groepsalias in het verbindingsprofiel):
  - Als de aanvaller de FQDN van uw VPN-firewall ontdekt, hebben ze de optie om de tunnelgroep te selecteren met behulp van de groep-alias waarin ze de brute-force aanval willen starten.
2. Standaardverbindingsprofiel geconfigureerd met AAA of Local Database:
  - Als de aanvaller de FQDN van de VPN-firewall vindt, kan hij proberen brute-force aanvallen op de AAA-server of lokale database. Dit gebeurt omdat de verbinding met de FQDN op het Default Connection Profile landt, zelfs als er geen groep-aliassen zijn gespecificeerd.
3. Resourcetest op de firewall of op AAA-servers:
  - Aanvallen kunnen AAA-servers of firewallbronnen overweldigen door grote hoeveelheden verificatieverzoeken te verzenden en een Denial of Service (DoS)-voorwaarde te maken.

## Concepten

Groepsaliassen:

- Een alternatieve naam waarmee de firewall kan verwijzen naar een verbindingsprofiel. Na het initiëren van een verbinding met de firewall, verschijnen deze namen in een vervolgkeuzemenu in de Secure Client UI voor gebruikers om te selecteren. Door het verwijderen van groepsaliassen wordt de vervolgkeuzefunctie in de Secure Client UI

verwijderd.

Groep-URL's:

- Een URL die kan worden gekoppeld aan een verbindingsprofiel, zodat inkomende verbindingen direct worden toegewezen aan een gewenst verbindingsprofiel. Er is geen vervolgkeuzefunctie, aangezien gebruikers de volledige URL in de Secure Client UI kunnen invoeren, of de URL kan worden geïntegreerd met een 'Display Name' in het XML-profiel om de URL van de gebruiker te verbergen.

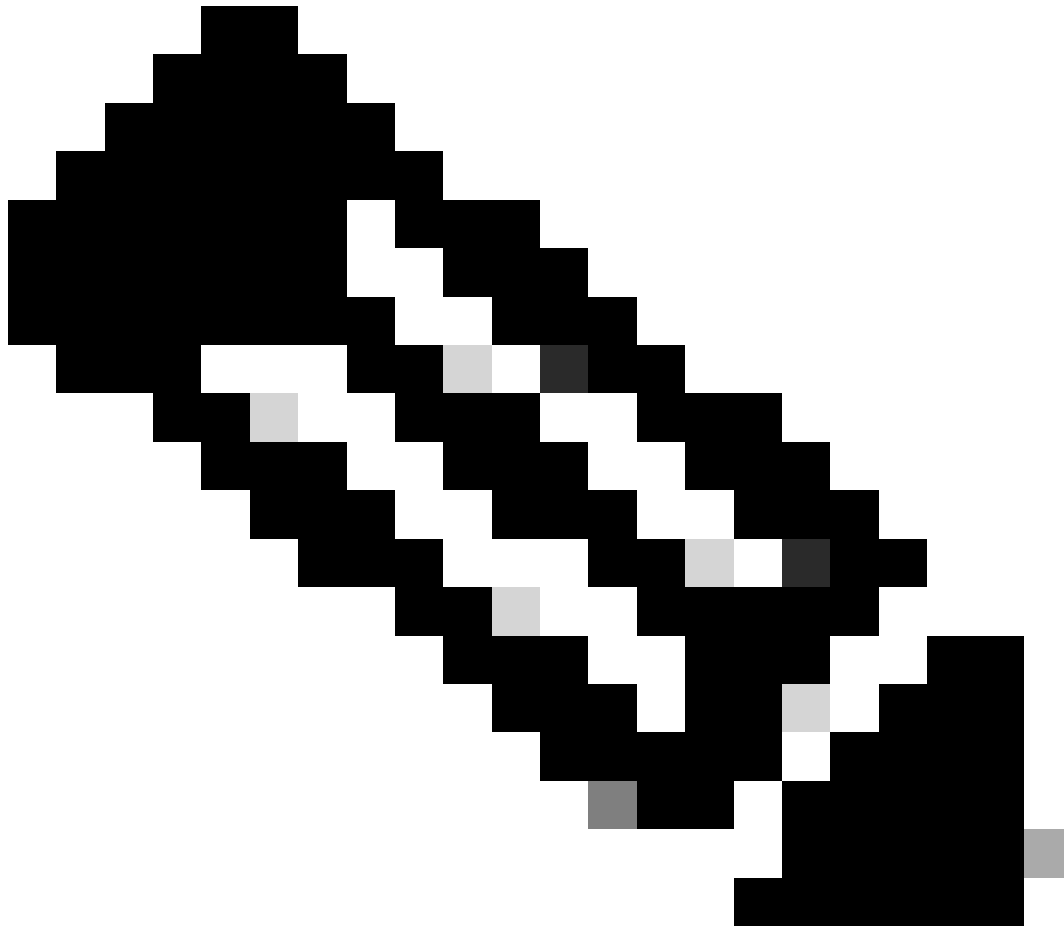
Het verschil is dat wanneer groepsaliassen worden geïmplementeerd, een gebruiker een verbinding to `vpn_gateway.example.com` start en met aliassen wordt voorgesteld om die aliassen naar een verbindingsprofiel te selecteren. Met groep-URL's start een gebruiker een verbinding naar `vpn_gateway.example.com/example_group` en die stuurt ze rechtstreeks naar het verbindingsprofiel zonder dat er een vervolgkeuzemenu nodig of optioneel is.

## Beveiligde praktijken voor clientharding op Cisco Secure Firewall:

Deze methodes zijn gebaseerd op het in kaart brengen van legitieme gebruikers aan juiste tunnelgroepen/verbindingsprofielen terwijl potentieel kwaadaardige gebruikers worden verzonden naar een val tunnelgroep die wij vormen om gebruikersbenaming en wachtwoordcombinaties niet toe te staan. Hoewel niet alle combinaties moeten worden geïmplementeerd, zijn het uitschakelen van groepsaliassen en het wijzigen van de verificatiemethode van de `DefaultWEBVPNGroup` en `DefaultRAGroup` vereist om de aanbevelingen effectief te laten werken.

- Schakel groepsaliassen uit en gebruik alleen groep-url in de configuratie van het verbindingsprofiel. Hierdoor kunt u een specifieke FQDN hebben die niet gemakkelijk te ontdekken en te selecteren is voor een aanvaller, aangezien alleen de clients met de juiste FQDN in staat zijn om de verbinding te starten. Bijvoorbeeld:  
`vpn_gateway.example.com/example_group` is moeilijker te ontdekken voor een aanvaller dan `vpn_gateway.example.com`.
- Schakel AAA-verificatie uit in de `DefaultWEBVPNGroup` en `DefaultRAGroup` en configureer certificaatverificatie, dit voorkomt een mogelijke brute-kracht tegen de lokale database of AAA-server. De aanvaller in dit scenario zou met onmiddellijke fouten bij het proberen worden voorgesteld te verbinden. Er is geen gebruikersnaam of wachtwoordveld omdat de authenticatie is gebaseerd op certificaten, dus het stoppen van brute force pogingen. Een andere optie is om een AAA-server zonder ondersteunende configuratie te maken om een 'sinkhole' te maken voor kwaadaardige aanvragen.
- Gebruik certificaattoewijzing voor het verbindingsprofiel. Hiermee kunnen binnenkomende verbindingen worden toegewezen aan specifieke verbindingsprofielen op basis van kenmerken die van certificaten op het clientapparaat zijn ontvangen. Gebruikers die over de juiste certificaten beschikken, worden correct in kaart gebracht, terwijl aanvallers die niet voldoen aan de criteria voor het in kaart brengen naar de `DefaultWEBVPNGroup` worden gestuurd.

- Het gebruik van IKEv2-IPSec in plaats van SSL veroorzaakt tunnelgroepen vertrouwen op een specifieke gebruiker-groep afbeelding in het XML-profiel. Zonder deze XML op de eindgebruikersmachine worden gebruikers automatisch naar de standaardtunnelgroep gestuurd.
- 



Opmerking: voor meer informatie over de functionaliteit van een groepsalias, zie [ASA VPN Configuration Guide](#) en neem 'Tabel 1' in acht. Verbindingsprofielkenmerken voor SSL VPN".

---

## Identificeer aanvallen met vastlegging- en syslog-id's

Brute-force aanvallen vertegenwoordigen de overheersende methode van het compromitteren van Verre Toegang VPNs, die zwakke wachtwoorden exploiteren om onbevoegde ingang te bereiken. Het is cruciaal om te weten hoe je signalen van een aanval herkent door gebruik te maken van het gebruik van houtkap en het evalueren van systemen. Gemeenschappelijke syslogs IDs die op een

aanval kunnen wijzen indien ontmoet met abnormaal volume zijn:

%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

De gebruikersnaam is altijd verborgen totdat de opdracht Gebruikersnaam voor niet-vastlegging verbergen is geconfigureerd op ASA.



Opmerking: Dit geeft inzicht als geldige gebruikers worden gegenereerd of bekend door beledigende IP's, maar wees voorzichtig, want gebruikersnamen zijn zichtbaar in de logbestanden.

---

Cisco ASA-vastlegging:

[Gebruikershandleiding voor Secure ASA Firewall](#)

[Vastlegging](#) hoofdstuk van de configuratiehandleiding voor Cisco Secure Firewall ASA Series General Operations CLI

Cisco FTD-vastlegging:

[Logboekregistratie configureren op FTD via FMC](#)

[Syslog](#)-sectie [configureren](#) in het hoofdstuk Platform-instellingen van de configuratiehandleiding voor apparaten van Cisco Secure Firewall Management Center

[Syslog configureren en controleren in Firepower Device Manager](#)

Sectie [Instellingen voor systeemvastlegging configureren](#) in het hoofdstuk Systeeminstellingen van de Cisco Firepower Threat Defense Configuration Guide voor Firepower Device Manager

## Aanvalsverificatie

Om te verifiëren, logt u in op de ASA of FTD Command Line Interface (CLI), voert u de opdracht `show aaa-server` uit en onderzoekt u of er een ongebruikelijk aantal pogingen en afgewezen verificatieaanvragen is voor een van de geconfigureerde 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
```

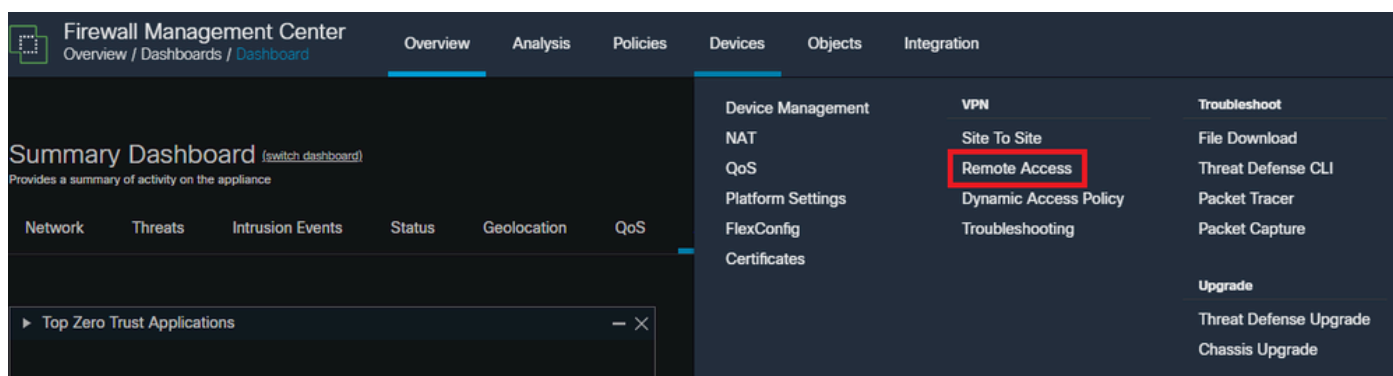


Number of bad authenticators 0  
Number of timeouts 1  
Number of unrecognized responses 0

## FMC-configuratievoorbeelden

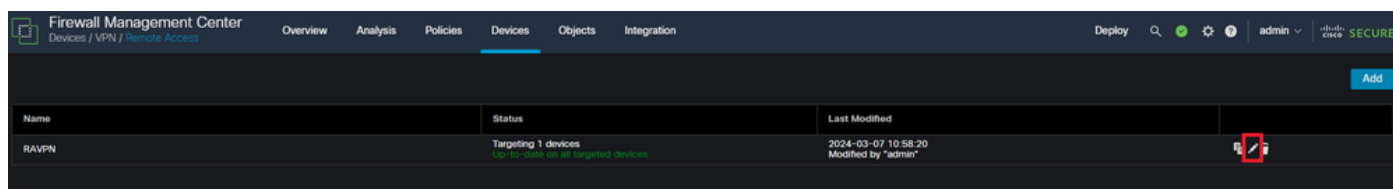
AAA-verificatie uitschakelen in de standaard-WEBVPN-groep en DefaultRAGroup-verbindingprofielen

Navigeer naar Apparaten > Externe toegang.



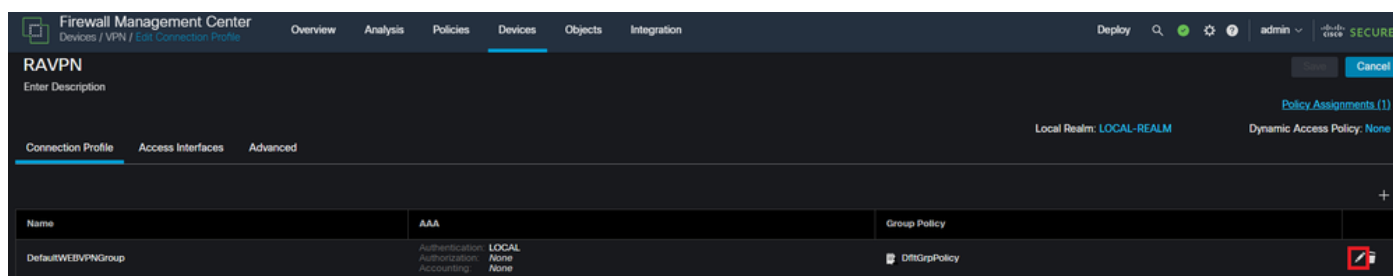
Toont het navigeren door de FMC GUI om naar de configuratie van het VPN-beleid voor externe toegang te gaan.

Bewerk het bestaande VPN-beleid voor externe toegang en maak een verbindingprofiel met de naam 'DefaultRAGroup'



Toont hoe u het beleid voor externe toegang VPN binnen de FMC UI kunt bewerken.

Bewerk de verbindingprofielen met de namen 'DefaultWEBVPNGroup' en 'DefaultRAGroup'



Hier wordt getoond hoe de DefaultWEBVPNGroup binnen de FMC UI moet worden bewerkt.

Navigeer naar het tabblad AAA en selecteer de vervolgkeuzelijst Verificatiemethode. Selecteer 'Alleen clientcertificaat' en selecteer Opslaan.

## Edit Connection Profile

Connection Profile:\*

Group Policy:\*  +

[Edit Group Policy](#)

Client Address Assignment

**AAA**

Aliases

### Authentication

Authentication Method:

Enable multiple certificate authentication

► Map username from client certificate

### Authorization

Authorization Server:

Allow connection only if user exists in authorization database

### Accounting

Accounting Server:

Cancel

Save

De verificatiemethode wijzigen in clientcertificaat alleen voor de DefaultWEBVPNGroep binnen de FMC UI.

Bewerk de DefaultRAG groep en navigeer naar het tabblad AAA en selecteer de vervolgkeuzelijst Verificatiemethode. Selecteer 'Alleen clientcertificaat' en selecteer Opslaan.

## Edit Connection Profile

Connection Profile:\*

Group Policy:\*  +

[Edit Group Policy](#)

Client Address Assignment

**AAA**

Aliases

### Authentication

Authentication Method:

Enable multiple certificate authentication

▶ Map username from client certificate

### Authorization

Authorization Server:

Allow connection only if user exists in authorization database

### Accounting

Accounting Server:

Cancel

Save

De verificatiemethode wijzigen in clientcertificaat alleen voor de DefaultRAGgroup binnen de FMC UI.



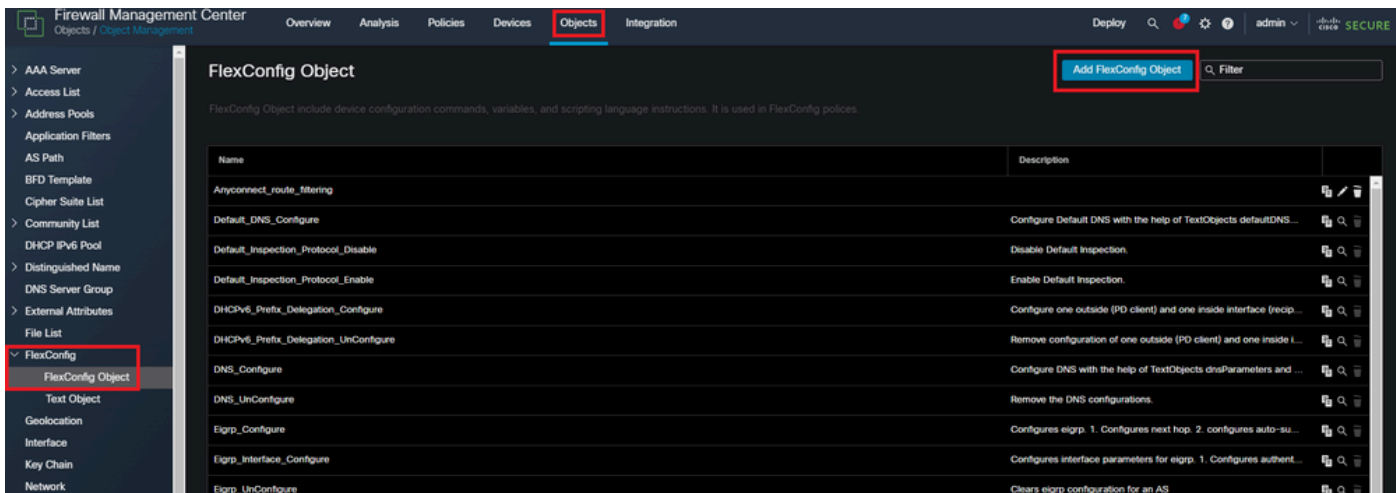
Opmerking: de verificatiemethode kan ook een AAA-server met een sinkhole zijn. Als deze methode wordt gebruikt, is de AAA-serverconfiguratie nep en worden geen aanvragen daadwerkelijk verwerkt. Een VPN-pool moet ook worden gedefinieerd in het tabblad 'Clientadrestoewijzing' om de wijzigingen op te slaan.

---

## Hostscan/Secure Firewall postuur uitschakelen in de DefaultWEBVPNGroup en DefaultRAGroup (optioneel)

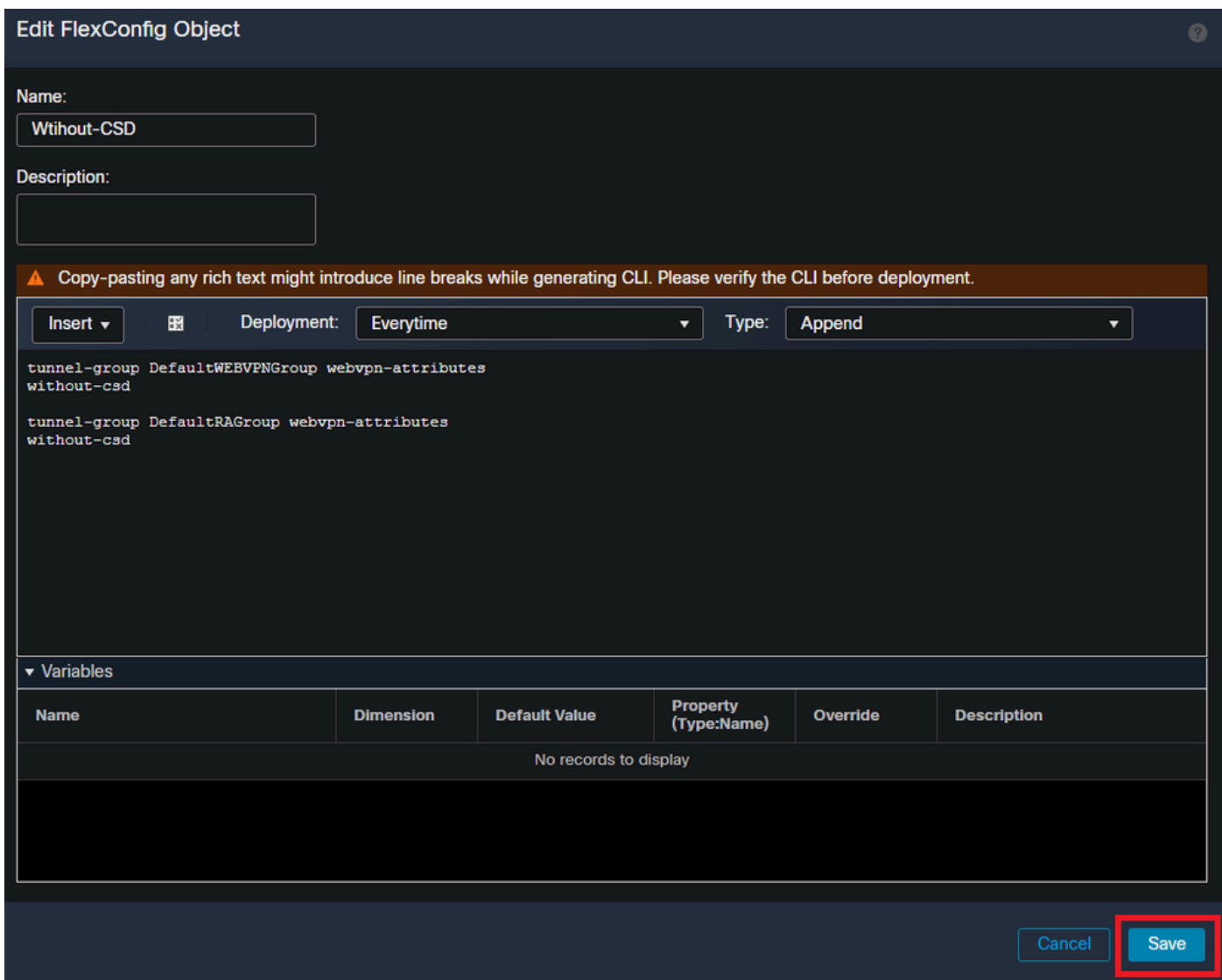
Dit is alleen nodig als u Hostscan / Secure Firewall postuur in uw omgeving heeft. Deze stap voorkomt dat aanvallers het resourcegebruik op de firewall vergroten, wat wordt veroorzaakt door het endpointscanproces. In het VCC wordt dit bereikt door een FlexConfig-object met de opdracht zonder CSD te maken om de functionaliteit voor endpointscannen uit te schakelen.

Navigeer naar objecten > Objectbeheer > FlexConfig-object > FlexConfig-object toevoegen.



Navigeren in de FMC UI om een FlexConfig-object te maken.

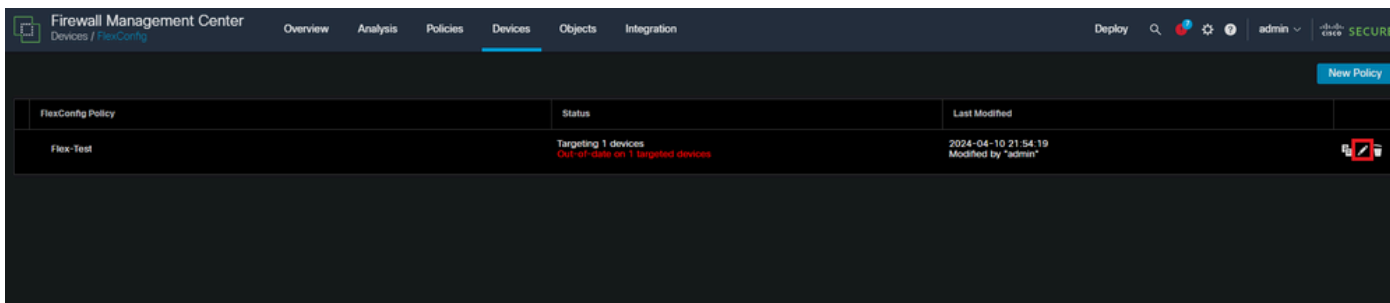
Geef het FlexConfig-object een naam en stel de implementatie in op Everytime met het type Add. Typ vervolgens de syntaxis precies zoals aangegeven op de afbeelding en sla het object op.



Een FlexConfig-object maken met 'zonder CSD'

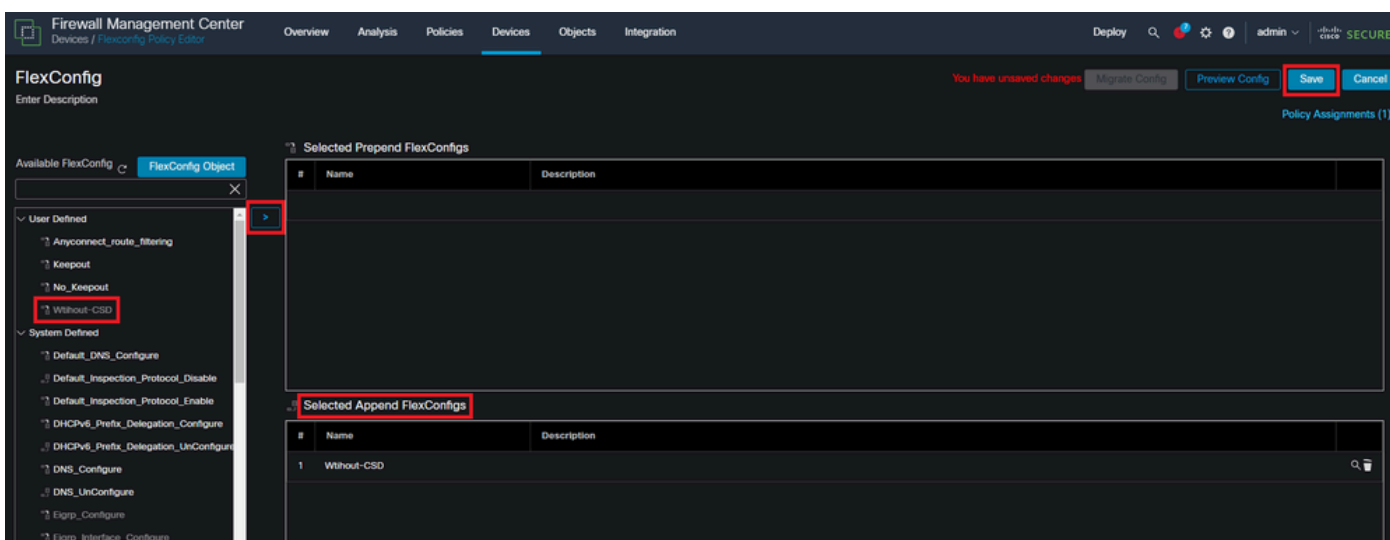
Navigeer naar Apparaten > FlexConfig en klik vervolgens op het potlood om het FlexConfig-beleid

te bewerken.



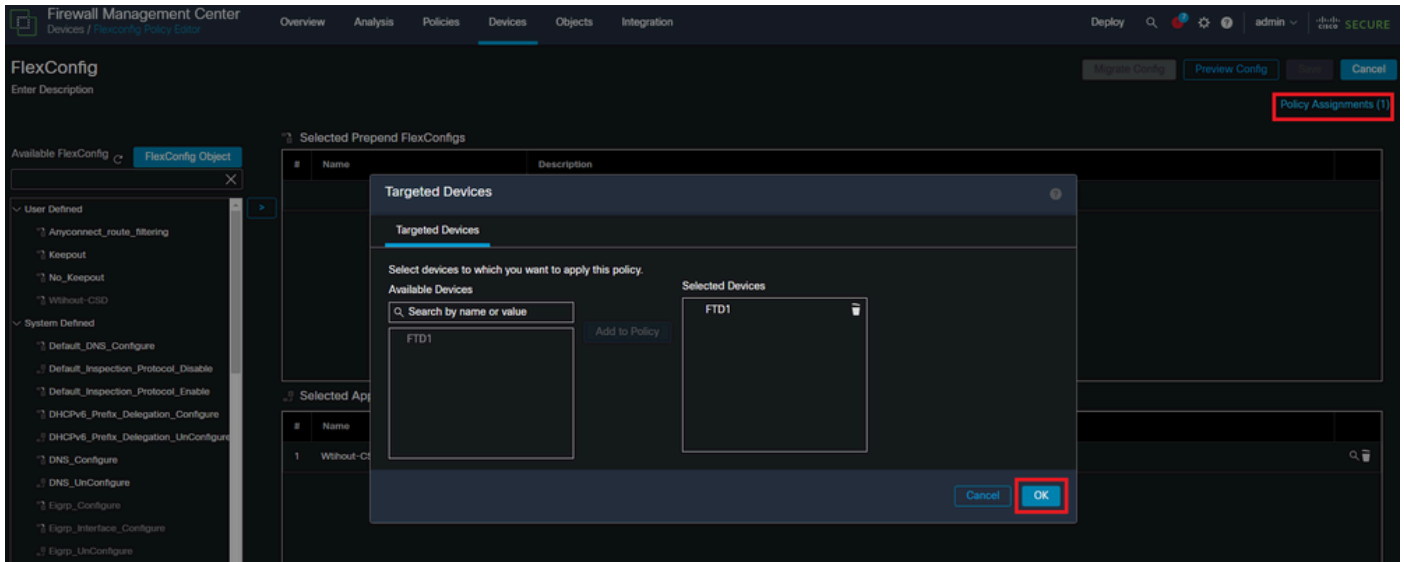
Het FlexConfig-beleid binnen het VCC bewerken.

Bepaal de plaats van het voorwerp u van de Gebruiker bepaalde sectie creerde. Selecteer vervolgens het pijltje om het toe te voegen aan de geselecteerde Toevoeging FlexConfiguraties. Selecteer ten slotte Opslaan om het FlexConfig-beleid op te slaan.



Hang het object FlexConfig aan het beleid voor FlexConfig.

Selecteer Beleidstoe wijzingen en kies de FTD waarop u dit FlexConfig-beleid wilt toepassen en selecteer vervolgens OK. Selecteer nogmaals Opslaan als dit een nieuwe FlexConfig-toewijzing is en implementeer de wijzigingen. Controleer na implementatie of



Wijst het FlexConfig-beleid toe aan een FirePOWER-apparaat.

Voer de FTD CLI in en geef de opdracht show run tunnel-group voor de DefaultWEBVPNGGroup en DefaultRAGroup. Controleer of zonder-csd nu in de configuratie aanwezig is.

```
<#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
```

## Groepsaliassen uitschakelen en Groep-URL's inschakelen

Navigeer naar een verbandsprofiel en selecteer het tabblad 'Aliassen'. Schakel de groep-alias

uit of verwijder de groep-alias en klik op het plus pictogram om een URL alias toe te voegen.

### Edit Connection Profile

Connection Profile:\* LDAP-TG

Group Policy:\* DfltGrpPolicy +  
[Edit Group Policy](#)

Client Address Assignment   AAA   **Aliases**

#### Alias Names:

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display. +

Name	Status	
LDAP	Disabled	

#### URL Alias:

Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile. +

URL	Status	
-----	--------	--

Schakel de optie voor groepsalias uit voor een tunnelgroep binnen de FMC UI.

Configureer een objectnaam voor de URL-alias en vul het FQDN- en/of IP-adres van de firewall voor de URL in, gevolgd door de naam waaraan u het verbindingsprofiel wilt koppelen. In dit voorbeeld kozen we voor 'aldap'. Hoe onduidelijker, hoe veiliger, omdat het minder waarschijnlijk is dat aanvallers de volledige URL raden, zelfs als ze uw FQDN hebben verkregen. Als u klaar bent, selecteert u Opslaan.



# Edit URL Objects



## Name

LDAP-ALIAS

## Description

## URL

https://ftd1 [redacted] .com/aaalda|

Allow Overrides

Cancel

Save

Een URL-aliassobject maken binnen de FMC UI.

Selecteer de URL-aliassen in de vervolgkeuzelijst, controleer het vakje Ingeschakeld en selecteer OK.

# Add URL Alias



URL Alias:

LDAP-ALIAS



Enabled

Cancel

OK

Zorg ervoor dat de URL-alias is ingeschakeld binnen de FMC UI.

Zorg ervoor dat de groep-alias is verwijderd of uitgeschakeld en controleer of uw URL-alias nu is ingeschakeld en selecteer Opslaan.

## Edit Connection Profile


Connection Profile:\* LDAP-TG

Group Policy:\* DfltGrpPolicy +

[Edit Group Policy](#)


Client Address Assignment   AAA   **Aliases**

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.

Name	Status	
LDAP	<b>Disabled</b>	

### URL Alias:

Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile.

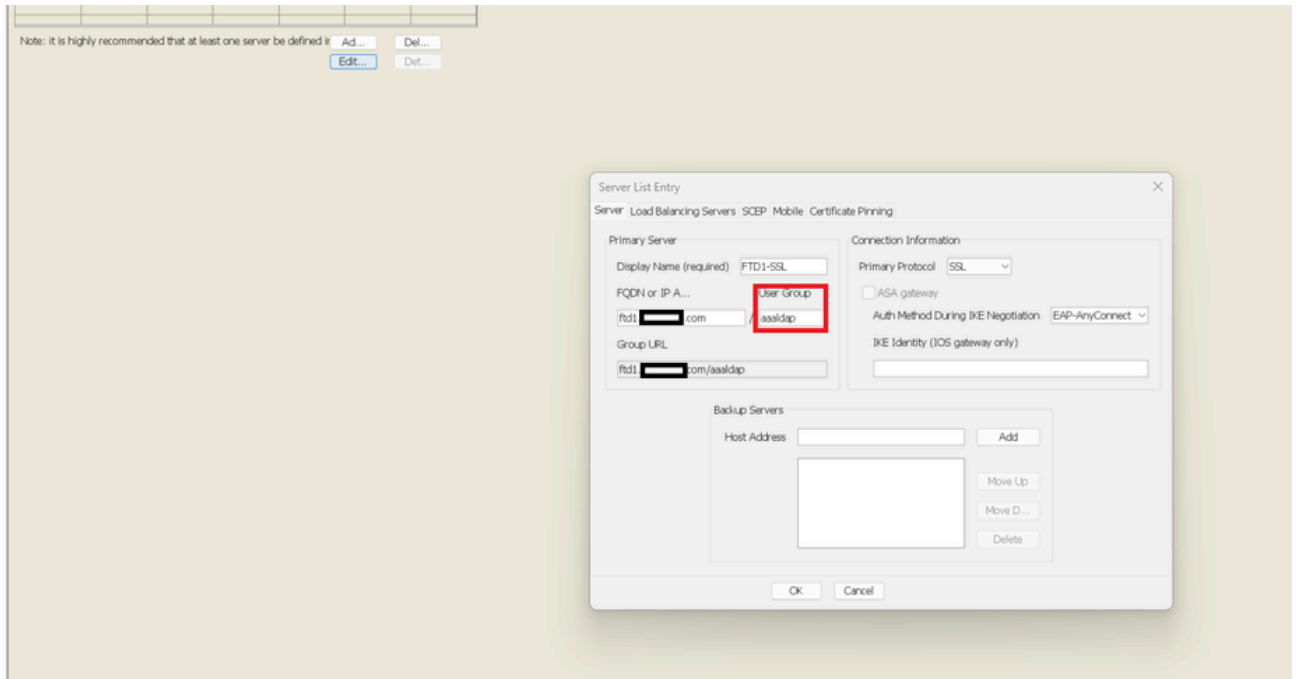
URL	Status	
LDAP-ALIAS (https://ftd1 [redacted] com/aaaldap)	<b>Enabled</b>	

Cancel

Save

De optie URL-alias inschakelen voor een tunnelgroep binnen de FMC UI.

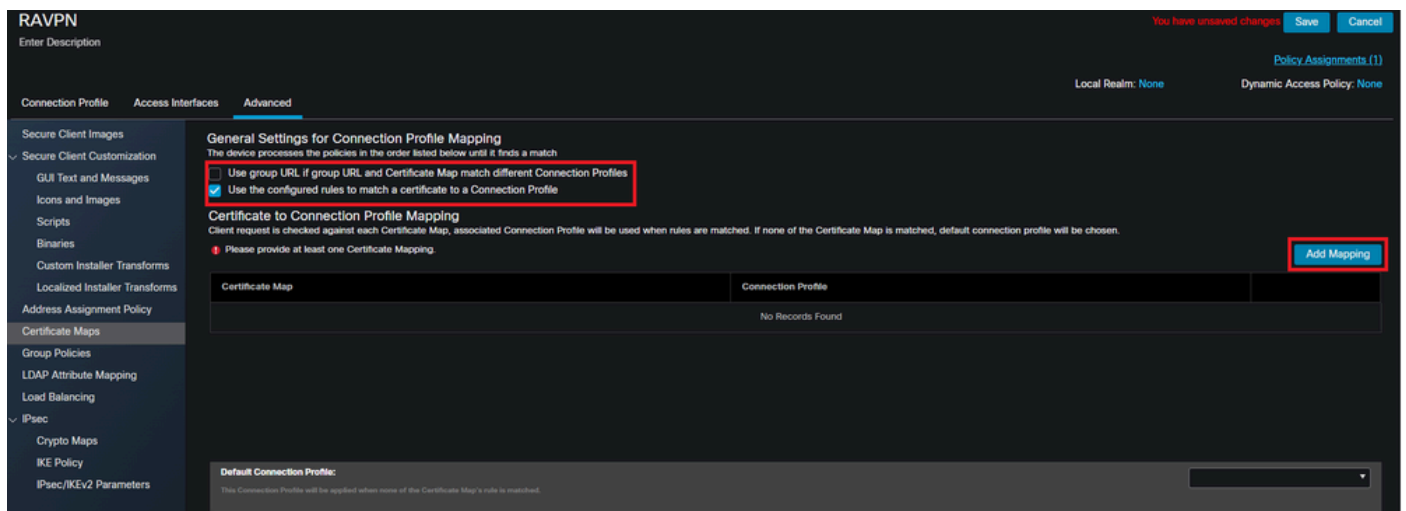
Indien gewenst, kunnen URL aliassen ook worden gedrukt als deel van de XML. Dit wordt bereikt door XML te bewerken met de VPN Profile Editor of de ASA Profile Editor. Om dit te realiseren, navigeer naar het tabblad Serverlijst en zorg ervoor dat het veld Gebruikersgroep overeenkomt met de URL-aliassen van het verbindingsprofiel bij gebruik van SSL. Zorg er voor dat voor IKEv2 het veld Gebruikersgroep overeenkomt met de exacte naam van het verbindingsprofiel.



Het bewerken van het XML-profiel om een URL-alias voor SSL-verbindingen te hebben.

## Toewijzing van certificaten

Navigeer naar het tabblad Geavanceerd binnen het VPN-beleid voor externe toegang. Kies een algemene instellingsoptie op basis van uw voorkeur. Selecteer Toewijzing toevoegen als u dit hebt geselecteerd.



Navigeren naar het tabblad Geavanceerd binnen de FMC UI om een certificaatkaartobject te maken binnen de FMC UI.

Geef het object van de certificaattoewijzing een naam en selecteer Regel toevoegen. Definieer in deze regel de eigenschappen van het certificaat dat u wilt identificeren om de gebruiker aan een bepaald verbindingprofiel toe te wijzen. Als u klaar bent, selecteert u OK en vervolgens selecteert u Opslaan.

## Add Certificate Map



Map Name\*:

Certificate-Map-CN

Mapping Rule

Add Rule

Configure the certificate matching rule

#	Field	Component	Operator	Value
1	Subject	CN (Common Name)	Equals	customvalue

OK

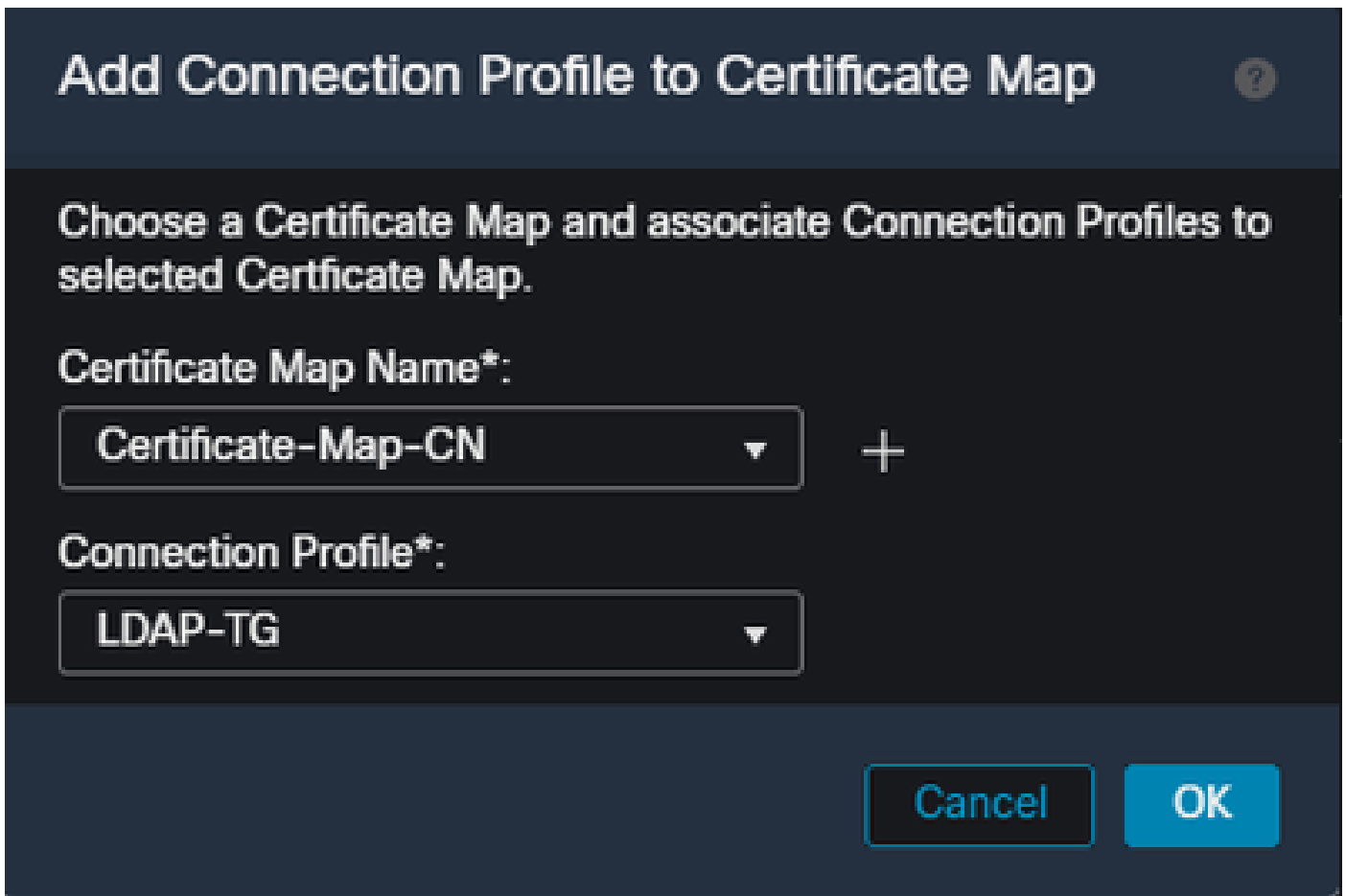
Cancel

Cancel

Save

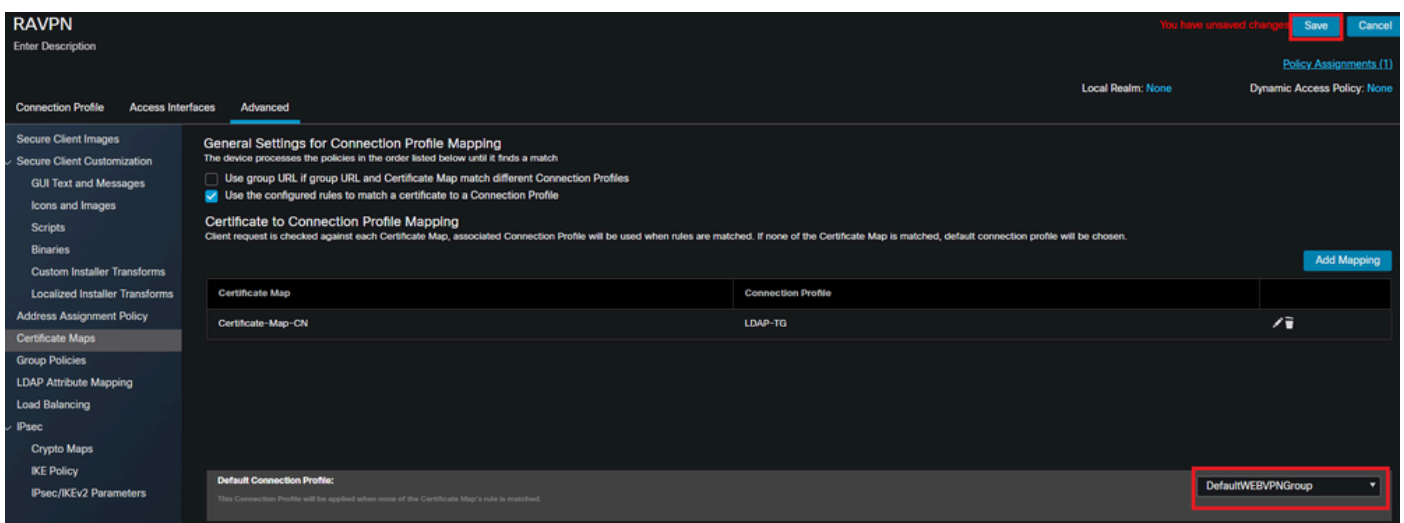
Maak een certificaatkaart en voeg criteria toe voor de kaart binnen de FMC UI.

Selecteer in de vervolgkeuzelijst het object van de certificaatkaart en het verbindingsprofiel waaraan u de certificaatkaart wilt koppelen. Selecteer vervolgens OK.



Koppel het object van de certificaatkaart aan de gewenste tunnelgroep binnen de FMC UI.

Zorg ervoor dat het Default Connection Profile is geconfigureerd als DefaultWEBVPNGgroup, zodat als een gebruiker de mapping mislukt, deze wordt verzonden naar de DefaultWEBVPNGgroup. Als u klaar bent, selecteert u Opslaan en implementeert u de wijzigingen.



Verander het standaardverbindingsprofiel voor certificaatomzetting in DefaultWEBVPNGgroup binnen de FMC UI.

## IPsec-IKEv2

Selecteer het gewenste IPsec-IKEv2 verbindingsprofiel en navigeer om het groepsbeleid te

bewerken.

### Edit Connection Profile

Connection Profile:\* IKEV2


Group Policy:\* IKEV2-IPSEC +

**Edit Group Policy**

Client Address Assignment   AAA   Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools: +

Name	IP Address Range	
AnyConnect_Pool	10.50.50.1-10.50.50.6	

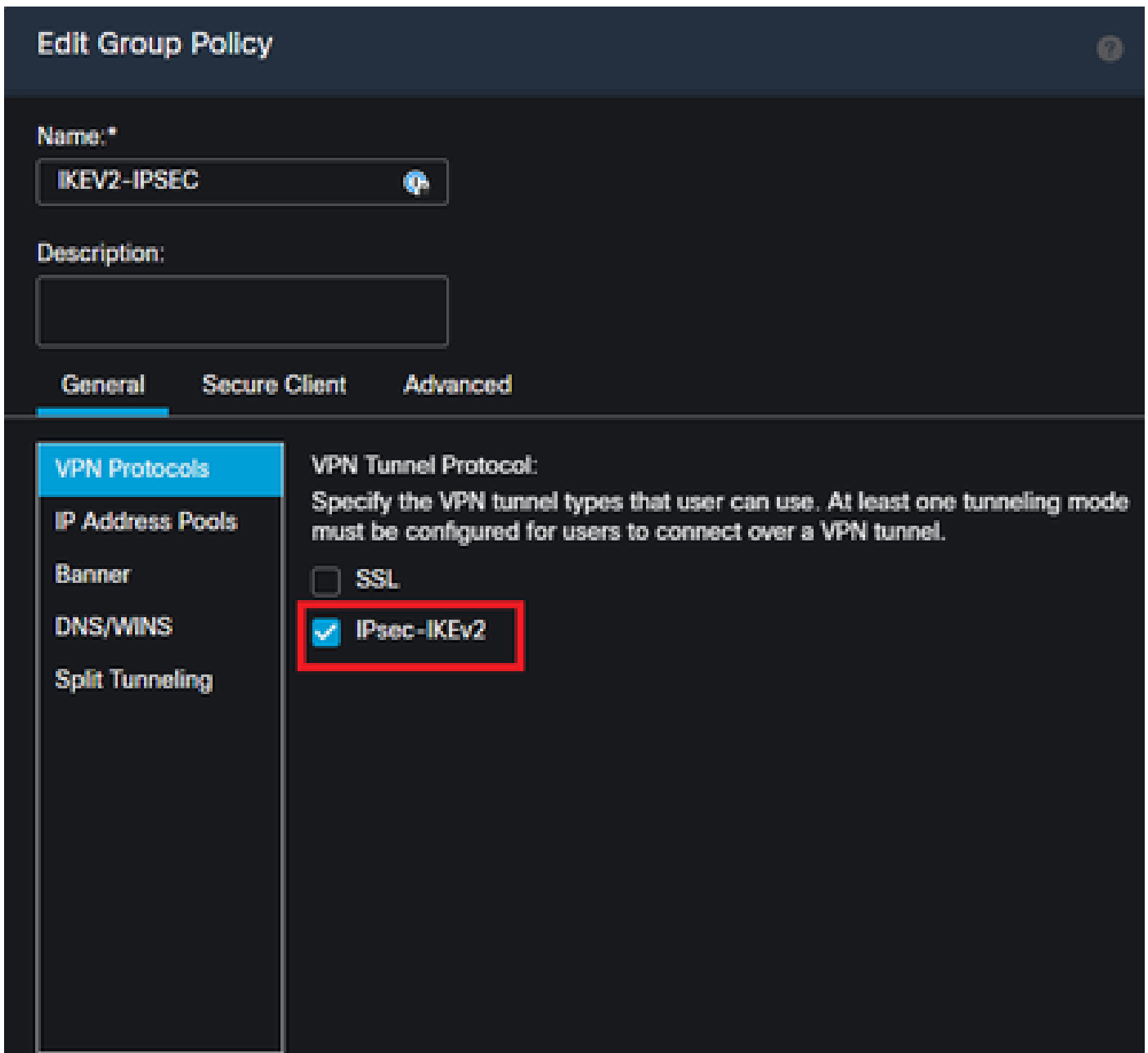
DHCP Servers: +

Name	DHCP Server IP Address	

Cancel Save

Bewerk een groepsbeleid binnen de FMC UI.

Ga op het tabblad Algemeen naar het gedeelte VPN-protocollen en controleer of het vakje IPsec-IKEv2 is ingeschakeld.



Schakel IPsec-IKEv2 in binnen een groepsbeleid in de FMC UI.

In de VPN Profile Editor of ASA Profile Editor navigeer je naar het tabblad Server List. De naam van de gebruikersgroep MOET exact overeenkomen met de naam van het verbindingsprofiel in de firewall. In dit voorbeeld, IKEV2 was de verbinding profiel / Gebruikersgroep naam. Het primaire protocol wordt geconfigureerd als IPsec. De 'Display Name' in wordt weergegeven aan de gebruiker in de Secure Client UI wanneer een verbinding met dit verbindingsprofiel wordt gemaakt.



Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) FTD1-IPSEC

FQDN or IP A... ftd1[redacted].com / User Group / IKEV2

Group URL

Connection Information

Primary Protocol IPsec

ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

IKE Identity (IOS gateway only)

Backup Servers

Host Address [text box] Add

[text box]

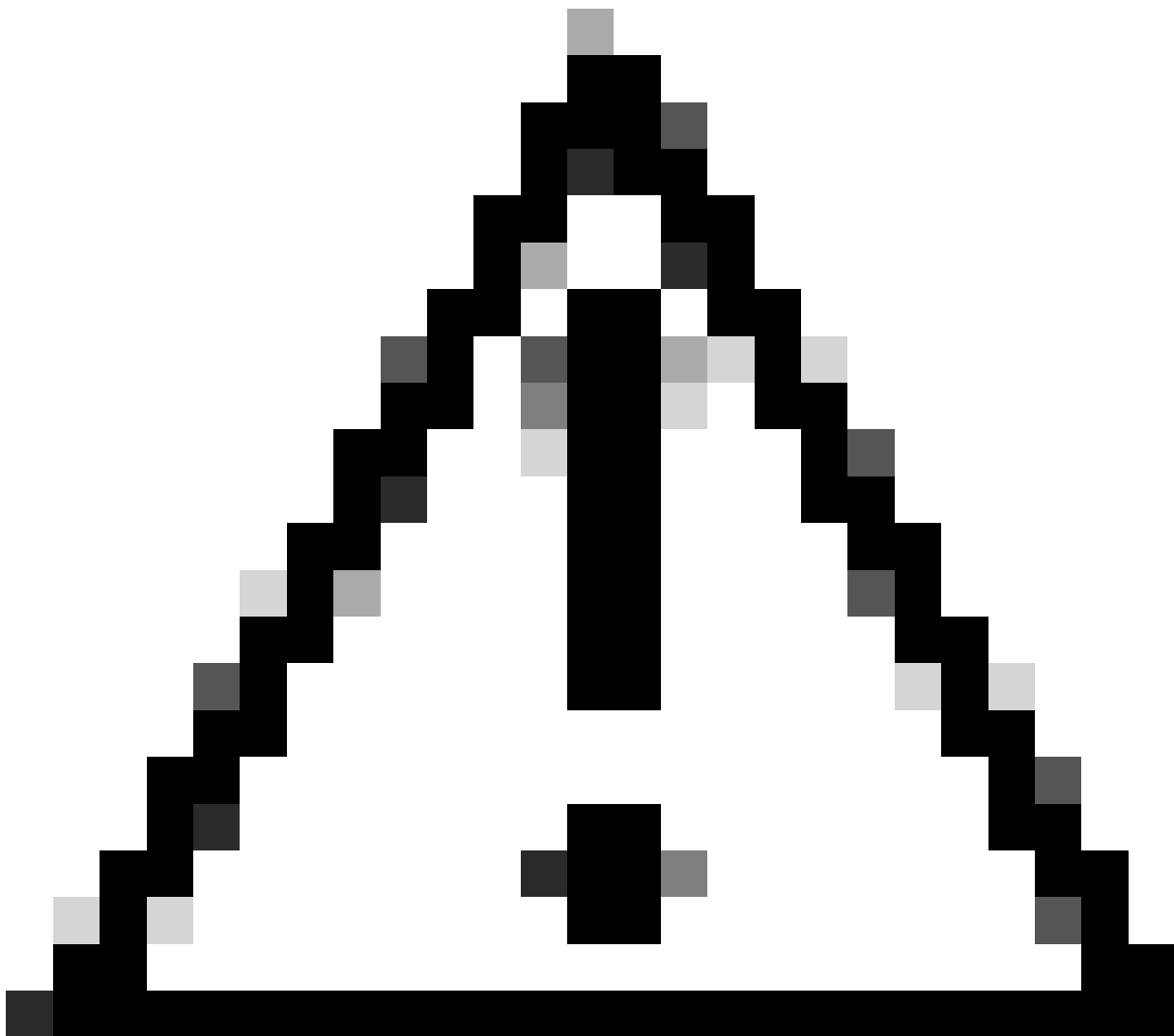
Move Up

Move D...

Delete

OK Cancel

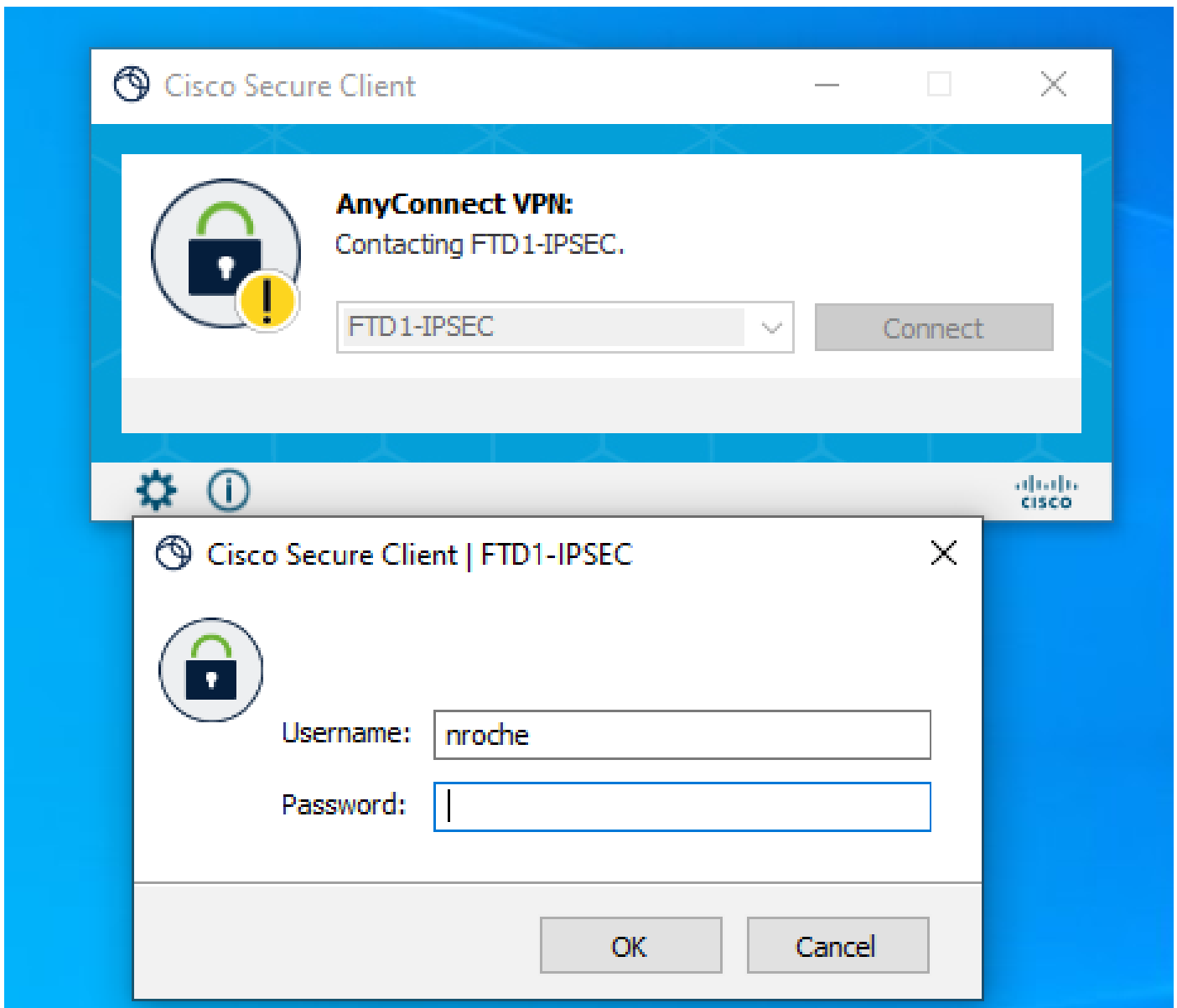
Bewerk het XML-profiel zodat het primaire protocol IPsec is, en de gebruikersgroep overeenkomt met de naam van het verbindingprofiel.



Waarschuwing: er is een SSL-verbinding nodig om XML-profielen vanuit de firewall naar de client te duwen. Wanneer alleen IKEV2-IPsec wordt gebruikt, moeten de XML-profielen via een out-of-band methode naar de clients worden gedrukt.

---

Nadat het XML-profiel naar de client is gedrukt, gebruikt Secure Client de gebruikersgroep van het XML-profiel om verbinding te maken met het IKEV2-IPsec-verbindingsprofiel.



Beveiligde client-UI-weergave van de poging tot verbinding met IPsec-IKEv2 RAVPN.

## ASA-configuratievoorbeelden

### AAA-verificatie uitschakelen in de standaard-WEBVPNG-groep en DefaultRAGroup-verbindingsprofielen

Voer de sectie webvpn-attributen voor de tunnelgroep DefaultWEBVPNGroup in en specificeer de verificatie als op certificaat gebaseerd. Herhaal dit proces voor de DefaultRAG groep. Gebruikers die landen op deze standaard verbindingsprofielen worden gedwongen om een certificaat voor authenticatie voor te stellen en krijgen niet de kans om gebruikersnaam en wachtwoord referenties in te voeren.

```
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
```

## Hostscan/Secure Firewall postuur uitschakelen in de DefaultWEBVPNGroup en DefaultRAGroup (optioneel)

Dit is alleen nodig als u Hostscan / Secure Firewall postuur in uw omgeving heeft. Deze stap voorkomt dat aanvallers het resourcegebruik op de firewall vergroten, wat wordt veroorzaakt door het endpointscanproces. Voer de sectie webvpn-attributen in voor de profielen DefaultWEBVPNGroup en DefaultRAGroup en connection en implementeer zonder-csd om de functionaliteit voor endpointscannen uit te schakelen.

```
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
```

## Groepsaliassen uitschakelen en Groep-URL's inschakelen

Voer de tunnelgroep(en) in waarmee gebruikers verbinding maken. Als er een bestaand groepsalias is, schakelt u het uit of verwijdert u het. In dit voorbeeld is het uitgeschakeld. Zodra dat is voltooid, maakt u een groep-url met behulp van het FQDN- of IP-adres van de RAVPN-afluitinterface. De naam aan het einde van de groep-url moet onduidelijk zijn. Vermijd gemeenschappelijke waarden zoals VPN, AAA, RADIUS, LDAP, aangezien deze het voor aanvallers gemakkelijker maken om de volledige URL te raden als zij FQDN verkrijgen. Gebruik in plaats daarvan intern significante namen die u helpen de tunnelgroep te identificeren.

```
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
```

## Toewijzing van certificaten

Van globale configuratiewijze, creëer een certificaatkaart en wijs het een naam en een opeenvolgingsaantal toe. Definieer vervolgens een regel die gebruikers moeten aanpassen om de afbeelding te gebruiken. In dit voorbeeld zouden gebruikers moeten voldoen aan de criteria van

een algemene naamwaarde die gelijk is aan "customvalue". Voer vervolgens de webvpn-configuratie in en pas de certificaatkaart toe op de gewenste tunnelgroep. Voer na voltooiing de DefaultWEBVPNG-groep in en maak van deze tunnelgroep de standaard voor gebruikers die de certificaattoewijzing niet doorstaan. Als gebruikers falen in de mapping, worden ze doorgestuurd naar de DefaultWEBVPNG groep. Terwijl de DefaultWEBVPNG groep is geconfigureerd met certificaatverificatie, hebben gebruikers niet de optie om gebruikersnaam of wachtwoordreferenties door te geven.

```
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

Van globale configuratiewijze, kunt u een bestaand groepsbeleid bewerken of nieuwe creëren en de attributen voor dat groepsbeleid invoeren. Zodra u in de attributensectie bent, laat IKEv2 als enig VPN tunnelprotocol toe. Zorg ervoor dat dit groepsbeleid is gekoppeld aan een tunnelgroep die wordt gebruikt voor IPsec-IKEV2 VPN-verbindingen voor externe toegang. Gelijkaardig aan de stappen van het FMC, moet u het profiel van XML via de Redacteur van het Profiel van VPN of de ASA Redacteur van het Profiel bewerken en het gebied van de Gebruikersgroep veranderen om de naam van de tunnelgroep op ASA aan te passen, en het protocol veranderen in 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 de VPN Profile Editor of ASA Profile Editor navigeer je naar het tabblad Server List. De naam van de gebruikersgroep MOET exact overeenkomen met de naam van het verbindingsprofiel in de firewall. Het primaire protocol wordt geconfigureerd als IPsec. De naam van de weergave wordt aan de gebruiker in de Beveiligde client-gebruikersinterface getoond wanneer een verbinding met dit verbindingsprofiel wordt gemaakt.

Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) ASA-IPsec

FQDN or IP A... User Group

FQDN TG-NAME

Group URL

FQDN/TG-NAME

Connection Information

Primary Protocol IPsec

ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

IKE Identity (IOS gateway only)

Backup Servers

Host Address

Add

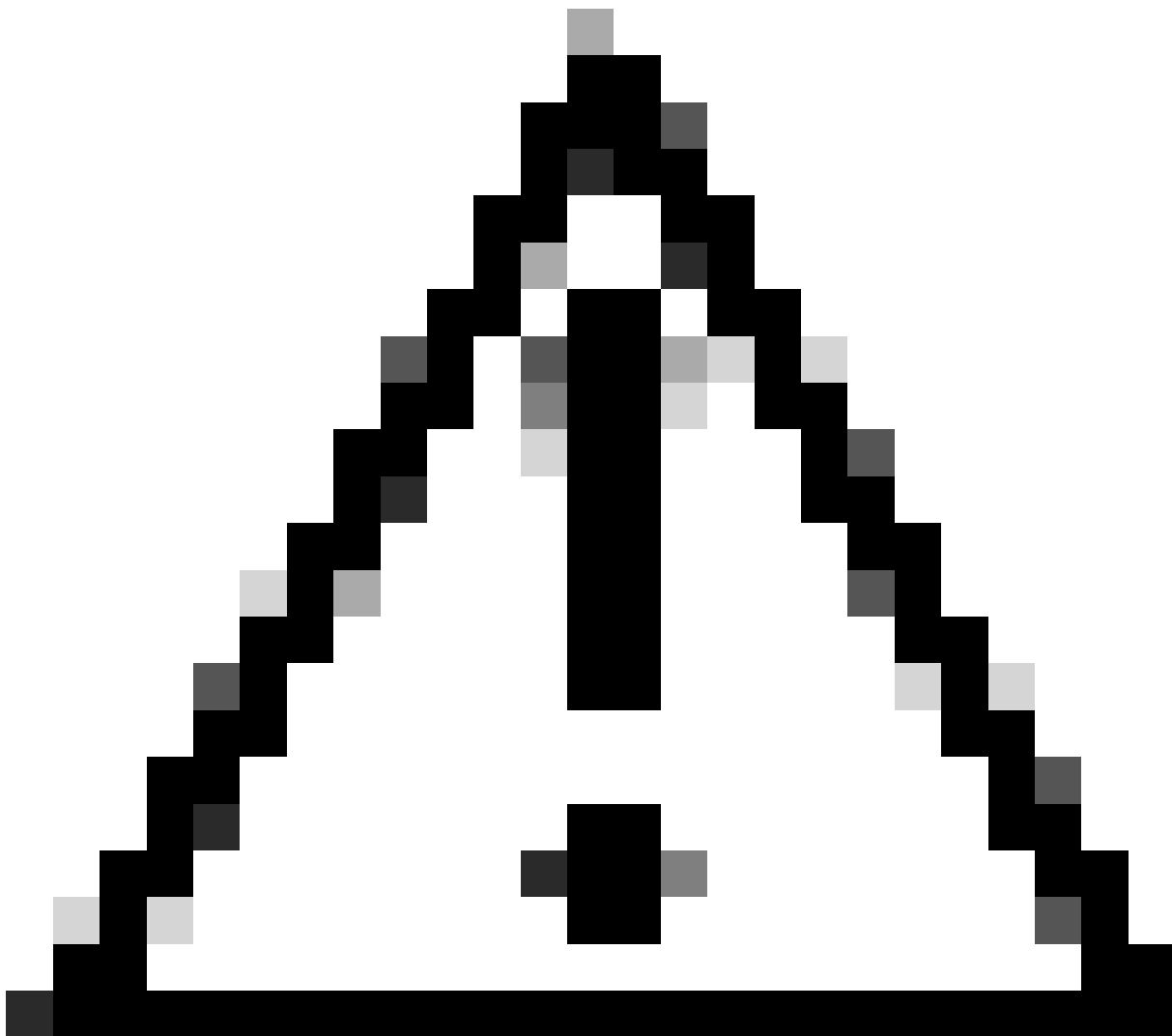
Move Up

Move D...

Delete

OK Cancel

Bewerk het XML-profiel zodat de primaire protocolnaam IPsec is en de gebruikersnaam voor de gebruikersgroep overeenkomt met de tunnelgroepnaam van de ASA voor IPsec-IKEv2 RAVPN-verbindingen.



Waarschuwing: er is een SSL-verbinding nodig om XML-profielen vanuit de firewall naar de client te duwen. Wanneer alleen IKEV2-IPsec wordt gebruikt, moeten de XML-profielen via een out-of-band methode naar de clients worden gedrukt.

---

## Conclusie

Samenvattend, het doel van de verhardende praktijken in dit document is legitieme gebruikers in kaart te brengen aan aangepaste verbindingsprofielen terwijl de aanvallers worden gedwongen aan de DefaultWEBVPNGroup en de DefaultRAGroup. In een geoptimaliseerde configuratie hebben de twee standaardverbindingsprofielen geen legitieme aangepaste AAA-serverconfiguratie. Bovendien voorkomt de verwijdering van groepsaliassen dat aanvallers eenvoudig aangepaste verbindingsprofielen kunnen identificeren door de drop-down zichtbaarheid te verwijderen bij het navigeren naar de FQDN of het openbare IP-adres van de firewall.

## Gerelateerde informatie

[Cisco technische ondersteuning en downloads](#)

[Aanvallen met wachtwoordspeling](#)

[Onbevoegde toegangskwetsbaarheid september 2023](#)

[ASA-configuratiehandleidingen](#)

[Configuratiehandleidingen voor FMC/FDM](#)



## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.