Configureer het beleid voor toegangscontrole van besturingsplane voor beveiligde firewall-bedreigingsverdediging en ASA

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Achtergrondinformatie

Configureren

- Configuraties
  - Een ACL voor besturingsplane configureren voor FTD beheerd door FMC
  - Configureer een control-plane ACL voor FTD die wordt beheerd door FDM
  - Configureer een besturings-vlakke ACL voor ASA met CLI
  - Alternatieve configuratie om aanvallen voor beveiligde firewall te blokkeren met behulp van de 'shun' Command

Verifiëren

Verwante bugs

Inleiding

Dit document beschrijft het proces voor het configureren van toegangsregels voor het besturingsplane voor Secure Firewall Threat Defence en Adaptive Security Appliance (ASA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure Firewall Threat Defence (FTD)
- Secure Firewall Device Manager (FDM)
- Secure Firewall Management Center (FMC)
- Secure-firewall ASA
- Toegangscontrolelijst (ACL)
- FlexConfig

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Secure Firewall Threat Defense versie 7.2.5
- Secure Firewall Manager Center versie 7.2.5
- Secure Firewall Device Manager versie 7.2.5
- Secure Firewall ASA versie 9.18.3

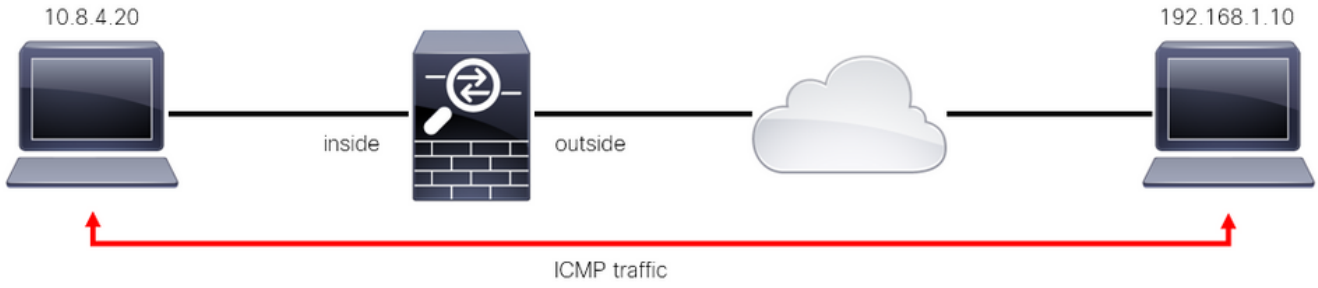
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het verkeer passeert gewoonlijk een firewall en wordt tussen gegevensinterfaces gerouteerd; in sommige omstandigheden, is het voordelig om verkeer te ontkennen dat "aan"de veilige firewall wordt bestemd. De beveiligde Cisco-firewall kan een toegangscontrolelijst (ACL) gebruiken om 'to-the-box'-verkeer te beperken. Een voorbeeld van wanneer een control-plane ACL nuttig kan zijn, is om te controleren welke peers een VPN-tunnel (Site-to-Site of Remote Access VPN) kunnen instellen naar de beveiligde firewall.

Secure Firewall-verkeer 'door de doos'

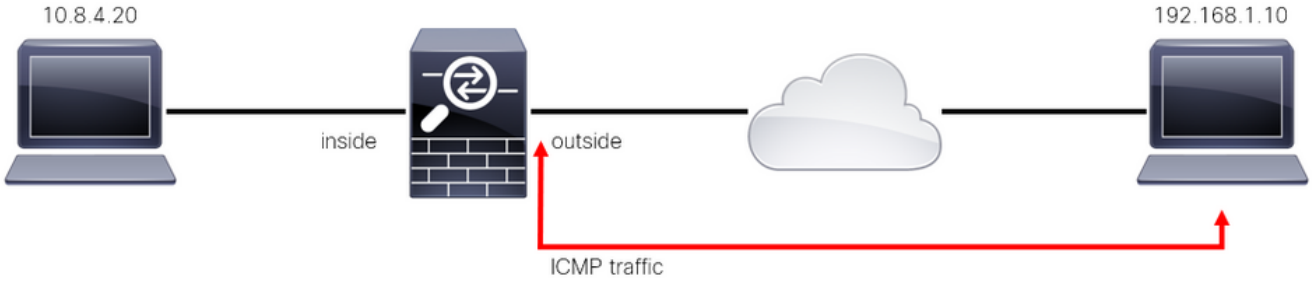
Het verkeer steekt normaal firewalls van één interface (binnenkomend) naar een andere interface (uitgaand) over, is dit gekend als "door-de-doos"verkeer en wordt beheerd door zowel, het Toegangsbeheer Beleid (ACS) en de Pre-filterregels.



Afbeelding 1. Voorbeeld van doorgaand verkeer

Secure Firewall-verkeer 'to-the-box'

Er zijn andere gevallen waarin verkeer rechtstreeks is bestemd voor een FTD-interface (Site-to-Site of Remote Access VPN). Dit wordt 'to-the-box'-verkeer genoemd en wordt beheerd door het besturingsplane van die specifieke interface.



Afbeelding 2. Voorbeeld van verkeer op de doos

Belangrijke overwegingen met betrekking tot ACL's van het besturingsplane

- Vanaf FMC/FTD versie 7.0 moet een ACL van een besturingsplane worden geconfigureerd met FlexConfig, met behulp van dezelfde opdrachtsyntaxis die op de ASA wordt gebruikt.
- Het sleutelwoord control-plane wordt toegevoegd aan de configuratie van de toegangsgroep, die verkeer 'naar' de beveiligde firewallinterface afdwingt. Zonder het control-plane woord toegevoegd aan de opdracht, zou de ACL verkeer 'door' de beveiligde firewall beperken.
- Met een besturingsplane ACL worden SSH, ICMP of TELNET niet beperkt tot een beveiligde firewall-interface. Deze worden verwerkt (toegestaan/geweigerd) volgens het Platform Settings Policy en hebben een hogere prioriteit.
- Een control-plane ACL beperkt verkeer 'tot' de beveiligde firewall zelf, terwijl het Access Control Policy voor de FTD of de normale ACL's voor de ASA verkeer 'door' de beveiligde firewall controleert.
- Anders dan een normale ACL is er geen impliciete 'ontkennen' aan het einde van de ACL.
- Op het moment dat dit document wordt gemaakt, kan de functie FTD Geolocation niet worden gebruikt om de toegang tot het FTD te beperken.

Configureren

In het volgende voorbeeld, een reeks IP adressen van een bepaald land probeert om brute kracht VPN in het netwerk door te proberen om in te loggen op de FTD RAVPN. De beste optie om de FTD te beschermen tegen deze aanvallen met brute VPN-kracht is om een besturingsplane ACL te configureren om deze verbindingen te blokkeren naar de buiten-FTD-interface.

Configuraties

Een ACL voor besturingsplane configureren voor FTD beheerd door FMC

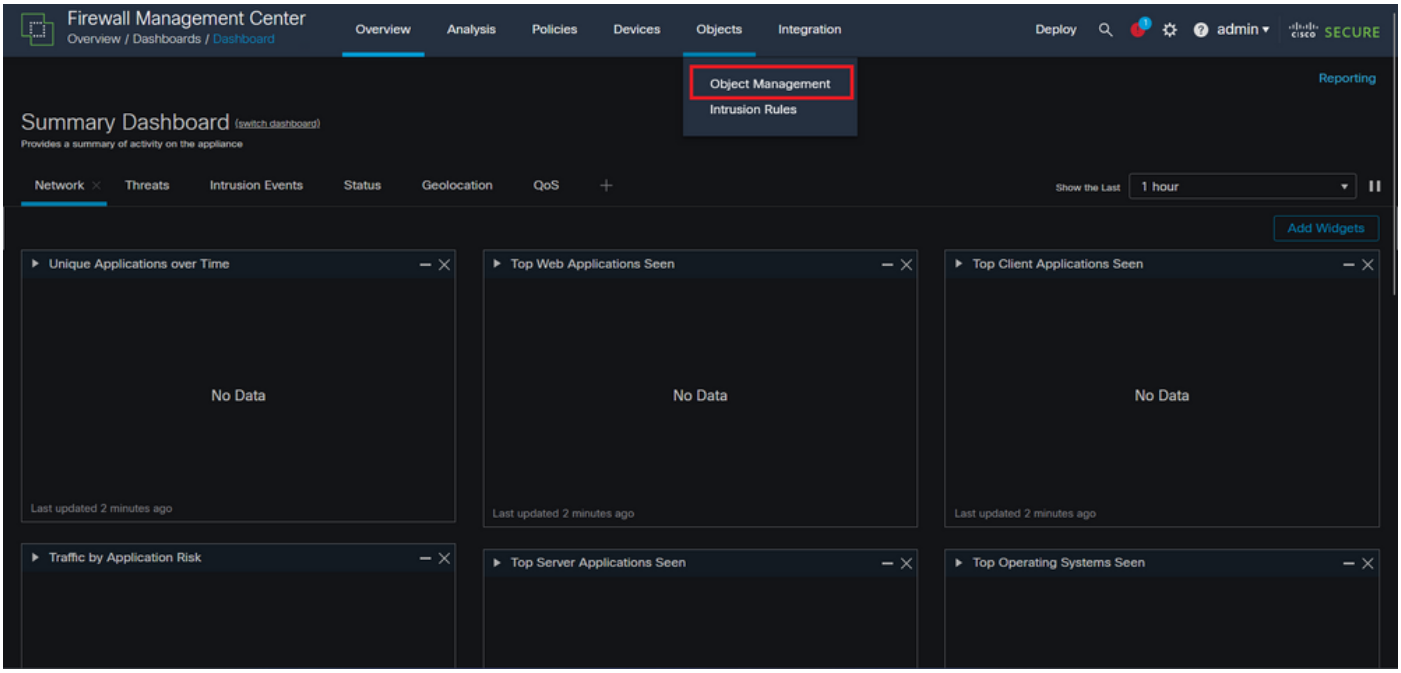
Dit is de procedure die u moet volgen in een FMC om een besturingsplane ACL te configureren om inkomende brute VPN-krachtaanvallen te blokkeren naar de buiten-FTD-interface:

Stap 1. Open de grafische gebruikersinterface van het VCC (GUI) via HTTPS en log in met uw

referenties.

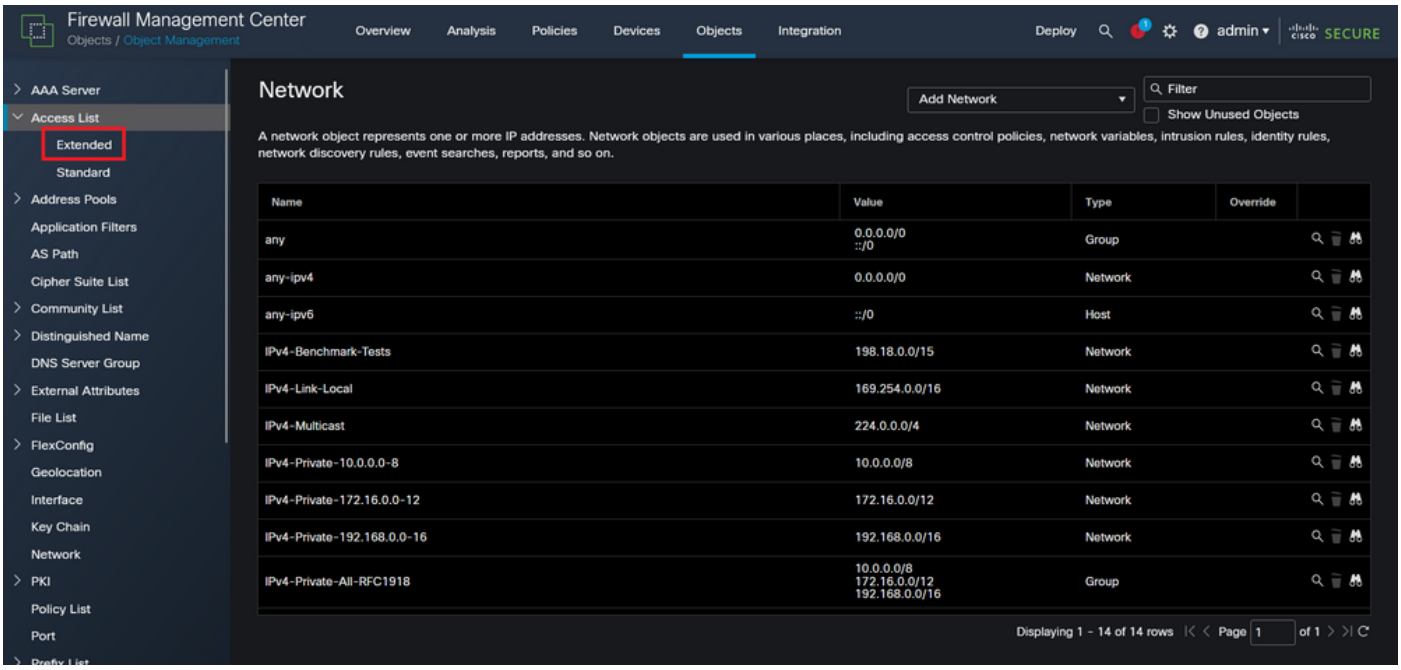
Afbeelding 3. Inlogpagina van FMC

Stap 2. U moet een uitgebreide ACL maken. Ga hiervoor naar Objecten > Objectbeheer.



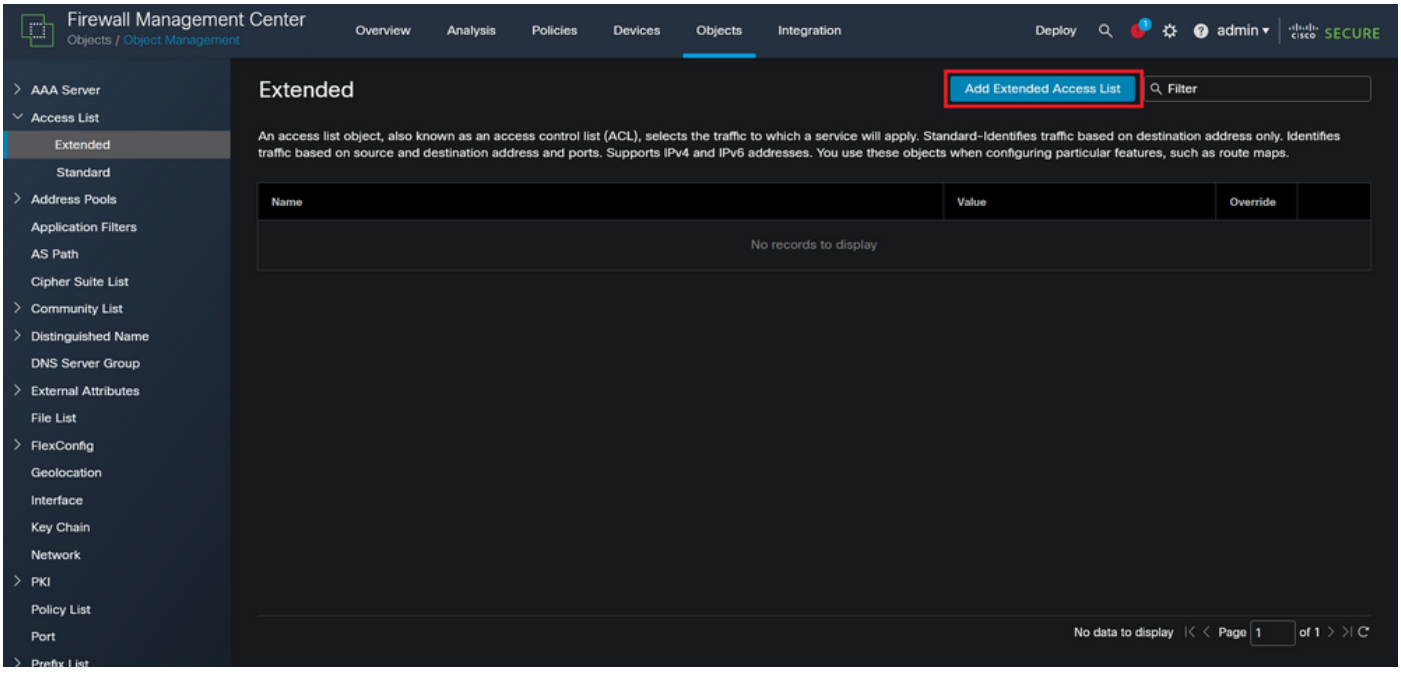
Afbeelding 4. Objectbeheer

Stap 2.1. Navigeer vanuit het linkerpaneel naar Toegangslijst > Uitgebreid om een uitgebreide ACL te maken.



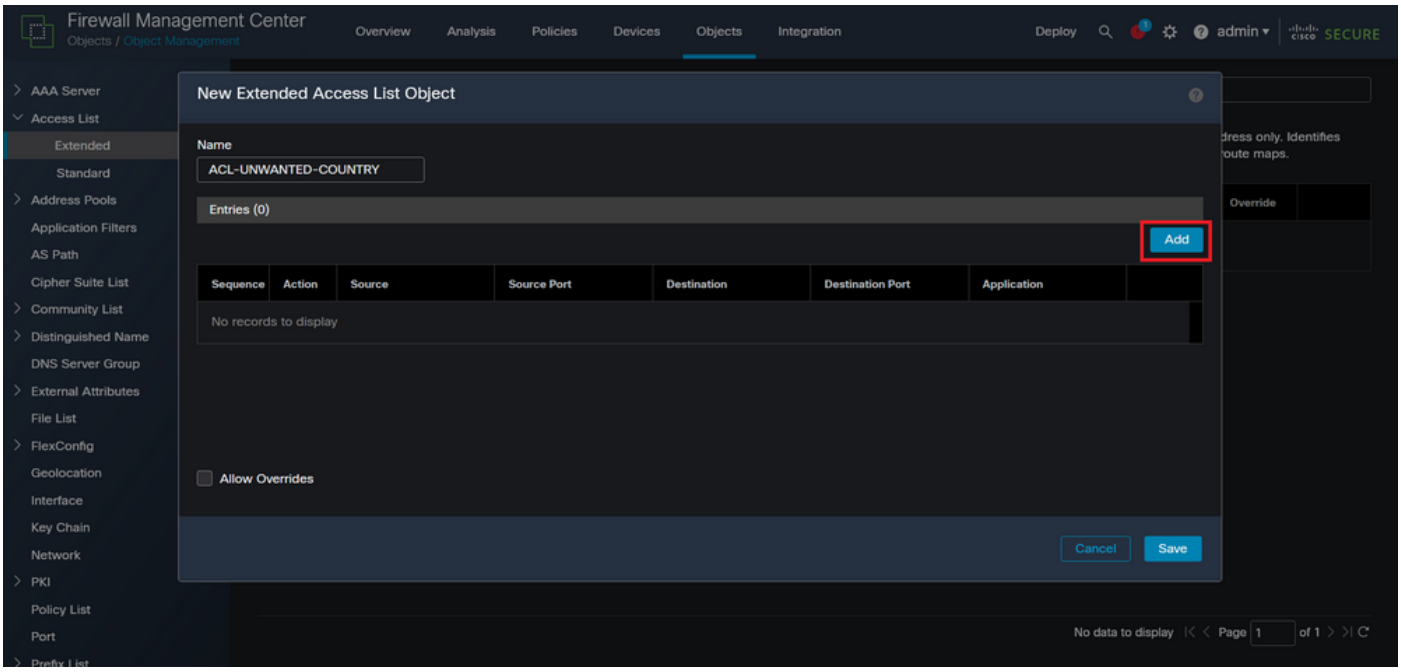
Afbeelding 5. Uitgebreid ACL-menu

Stap 2.2. Selecteer vervolgens Uitgebreide toegangslijst toevoegen.



Afbeelding 6. Uitgebreide ACL toevoegen

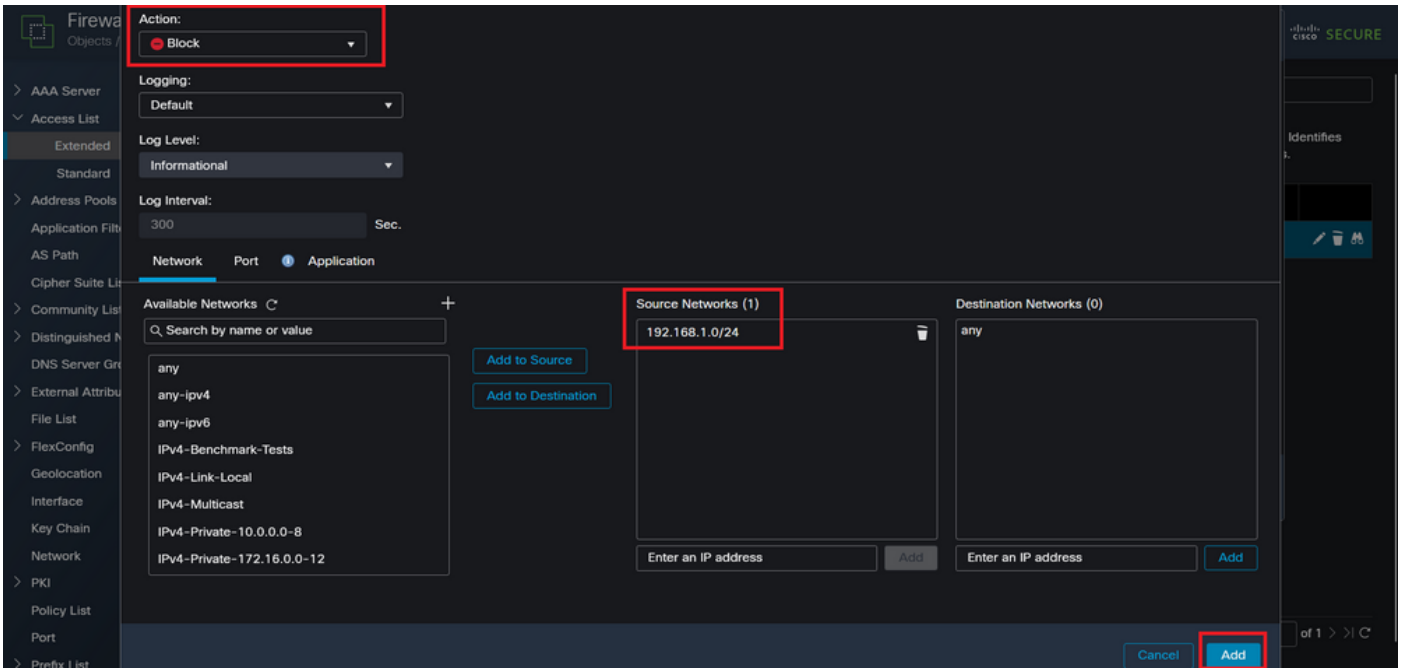
Stap 2.3. Typ een naam voor de uitgebreide ACL en klik vervolgens op de knop Toevoegen om een toegangscontrole-ingang (ACE) te maken:



Afbeelding 7. Uitgebreide ACL-vermeldingen

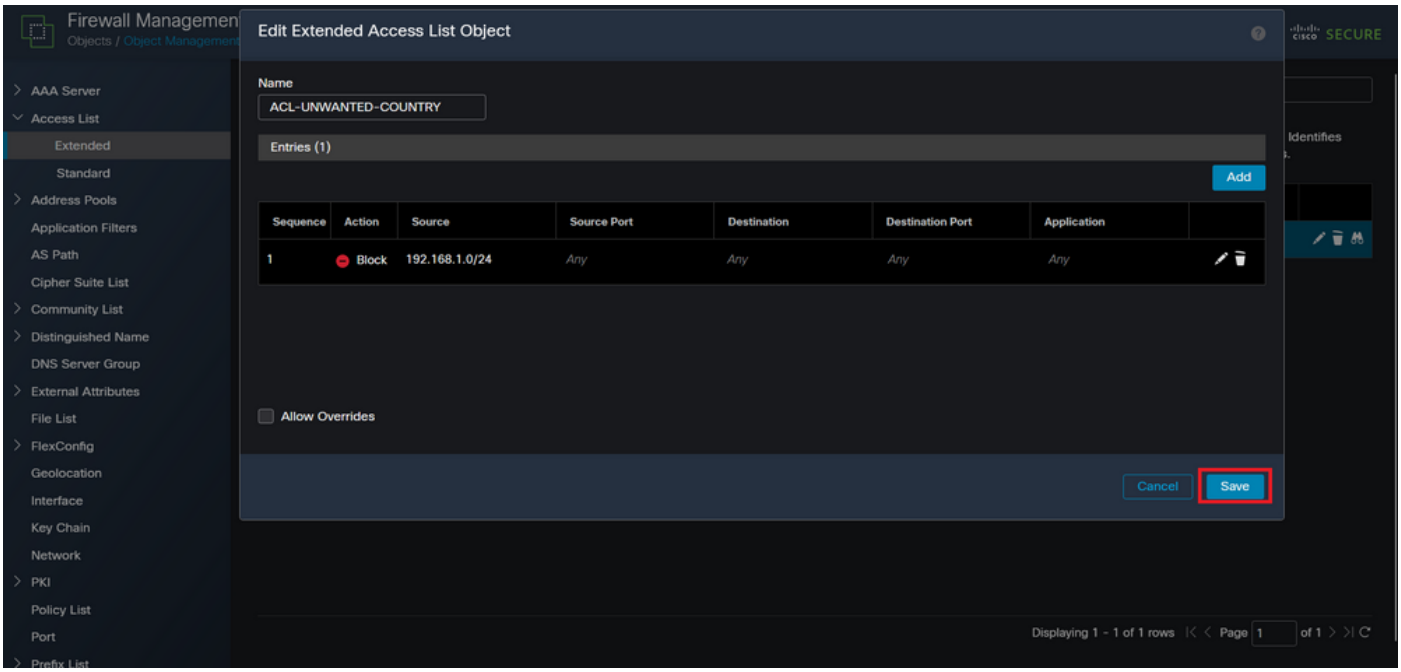
Stap 2.4. Verander de actie van ACE om te blokkeren, dan voeg het bronnetwerk toe om het verkeer aan te passen dat aan FTD moet worden ontkend, houd het bestemmingsnetwerk als om het even welk, en klik op de Add knop om de ingang van ACE te voltooien:

- In dit voorbeeld, zal de gevormde ingang van ACE VPN brute krachtaanvallen blokkeren die uit 192.168.1.0/24 subnetnet komen.



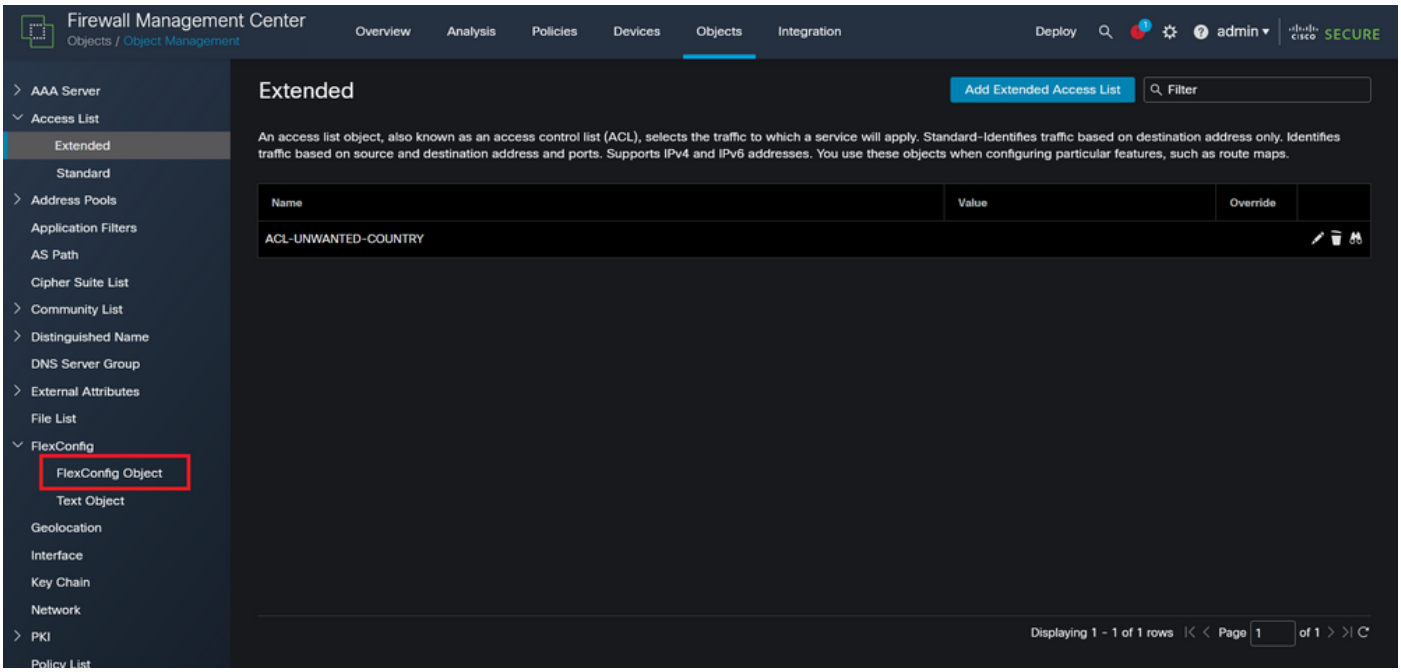
Afbeelding 8. Verboden netwerken

Stap 2.5. Als u meer ACE-vermeldingen moet toevoegen, klik dan nogmaals op de knop Toevoegen en herhaal stap 2.4. Klik vervolgens op de knop Opslaan om de ACL-configuratie te voltooien.



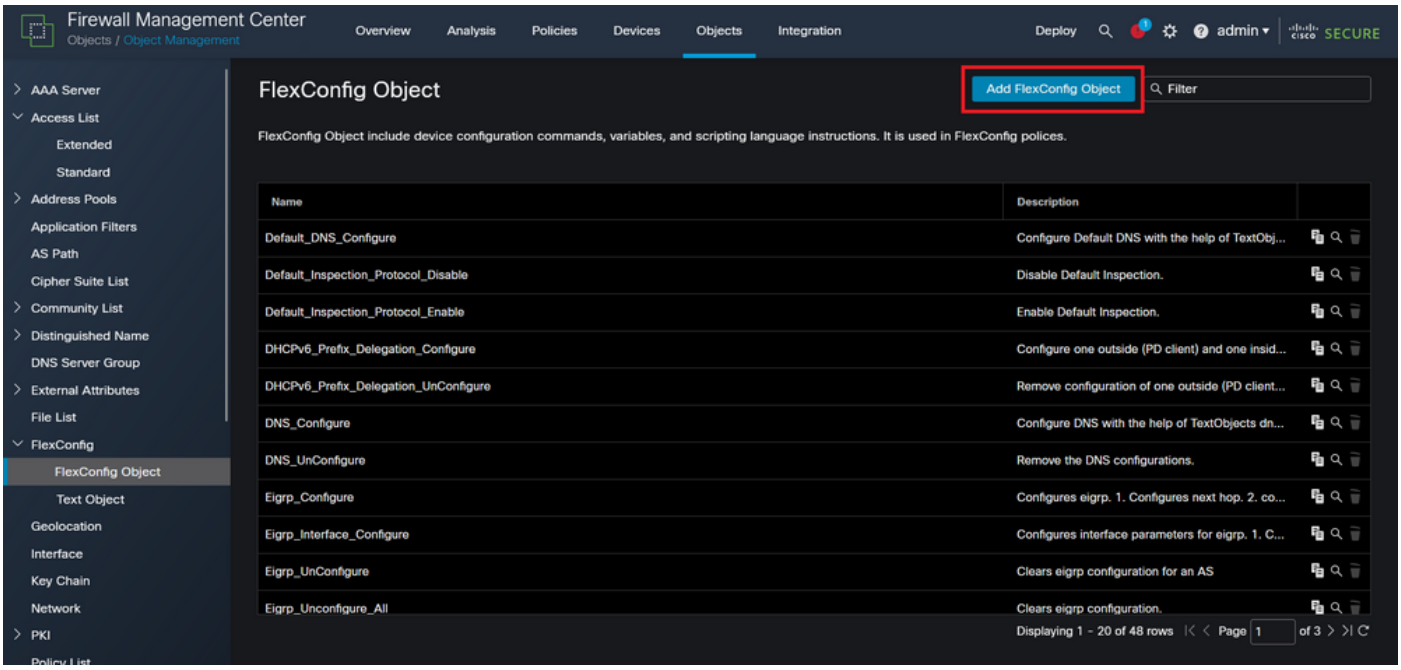
Afbeelding 9. Voltooide uitgebreide ACL-vermeldingen

Stap 3. Vervolgens moet u een Flex-Config-object configureren om de ACL van het besturingsplane toe te passen op de buiten-FTD-interface. Ga hiervoor naar het linkerpaneel en selecteer de optie FlexConfig > FlexConfig Object.



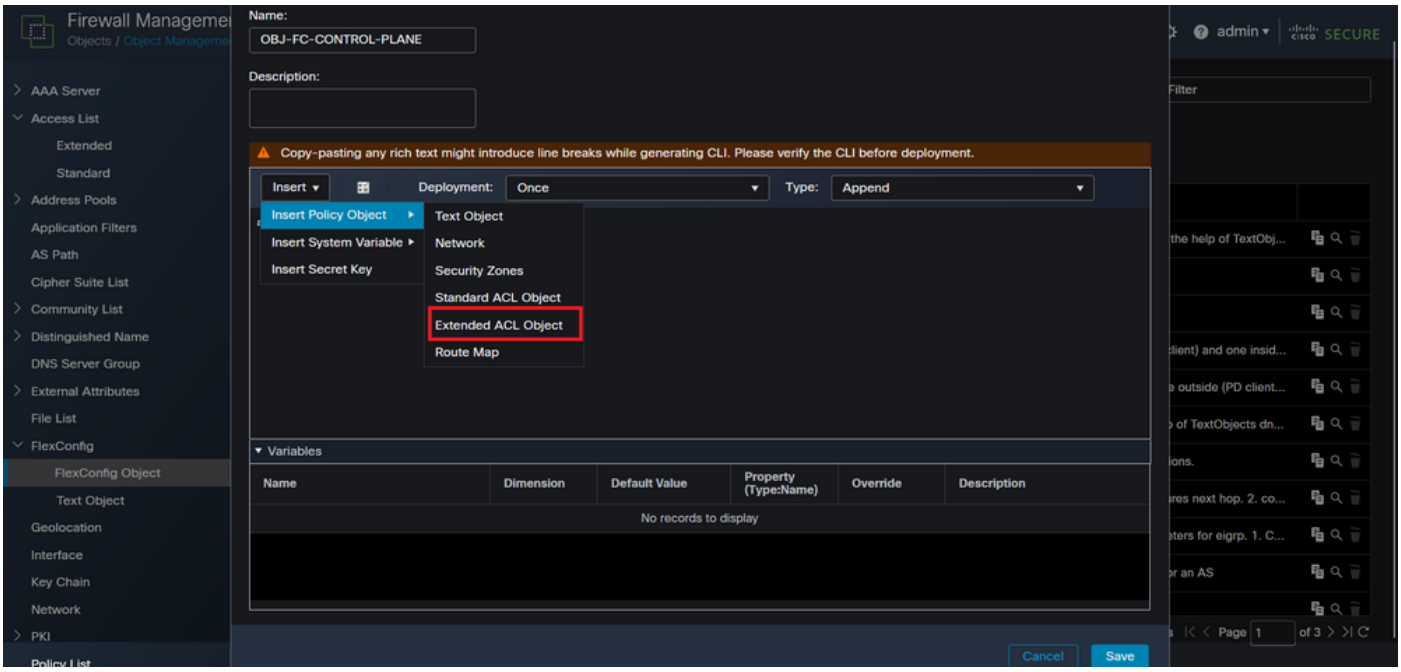
Afbeelding 10. Het menu FlexConfig-object

Stap 3.1. Klik op Add FlexConfig Object.



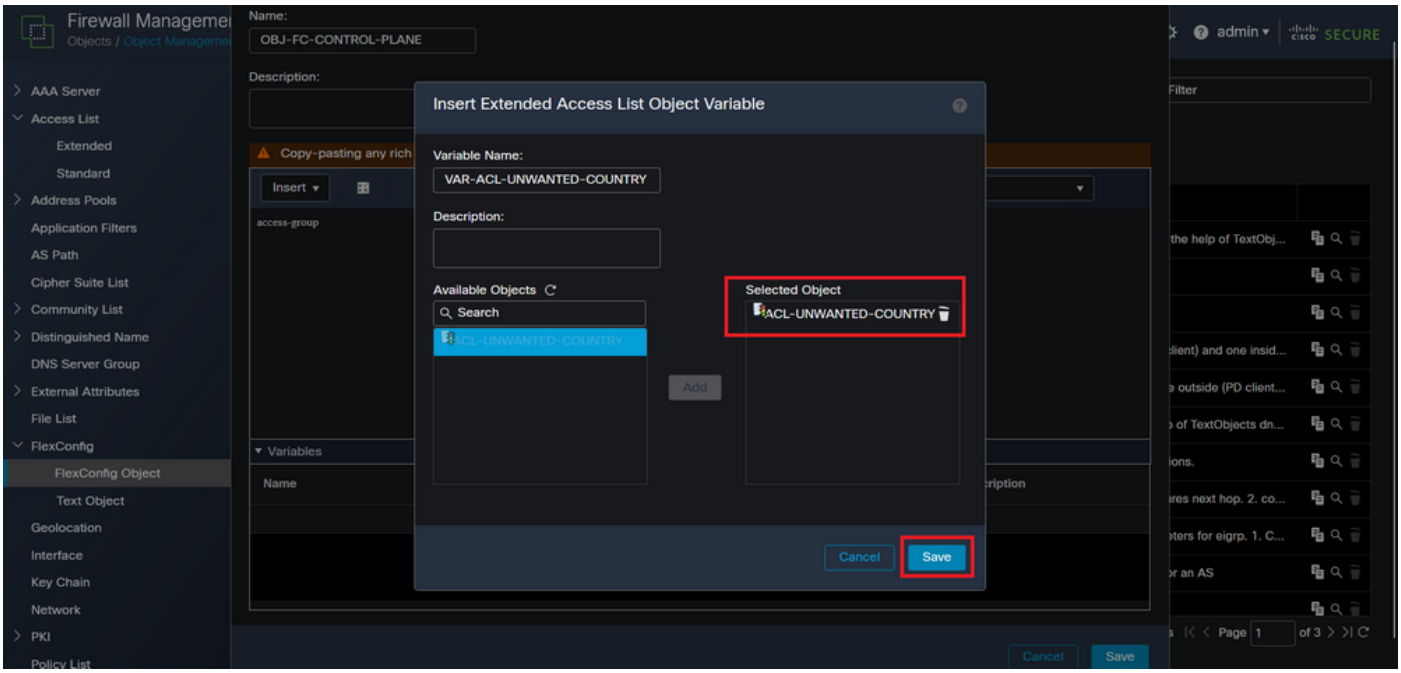
Afbeelding 11. Flexconfig-object toevoegen

Stap 3.2. Voeg een naam toe voor het object FlexConfig en voeg vervolgens een ACL-beleidsobject in. Selecteer hiervoor Invoegen > Beleidsobject invoegen > Uitgebreid ACL-object.



Afbeelding 12. FlexConfig-objectvariabele

Stap 3.3. Voeg een naam toe voor de ACL-objectvariabele en selecteer vervolgens de uitgebreide ACL die in stap 2.3 is gemaakt. Klik vervolgens op de knop Opslaan.



Afbeelding 13. Variabele ACL-toewijzing van FlexConfig-object

Stap 3.4. Dan, vorm controle-vlak ACL als binnenkomend voor de buiteninterface als volgt.

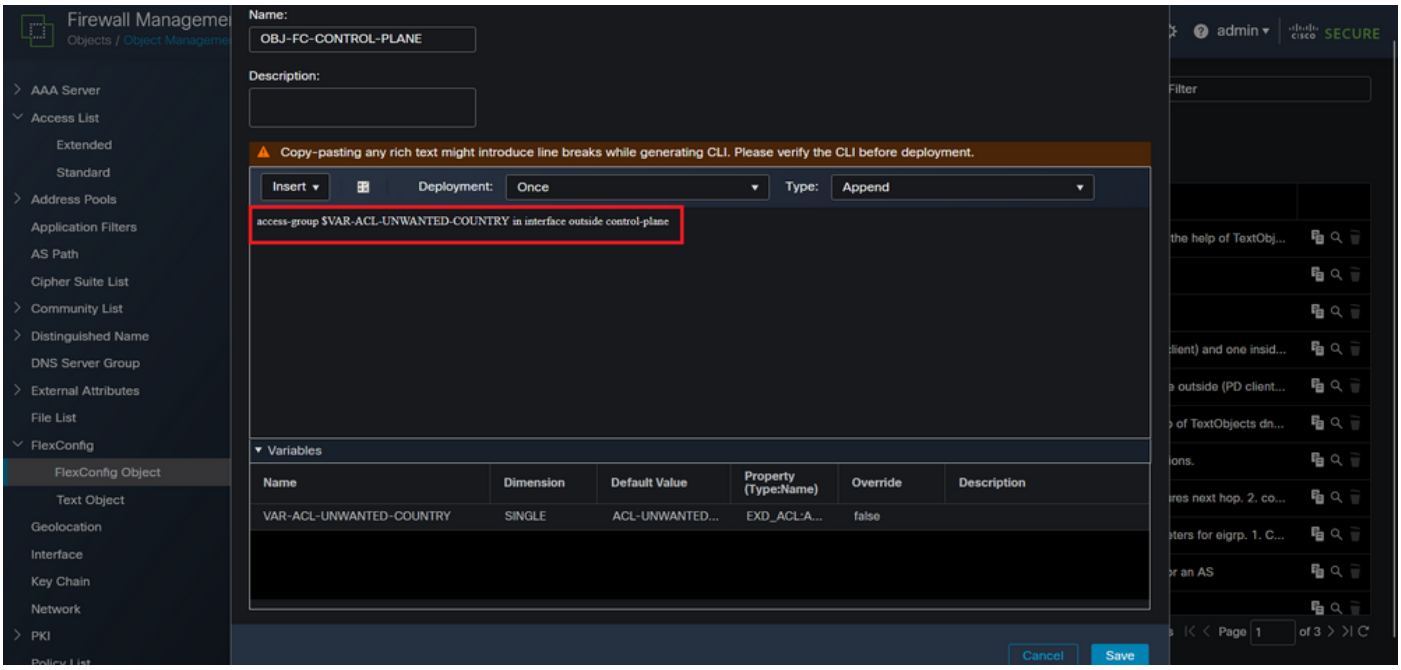
Syntaxis van opdrachtregel:

```
access-group "variable name starting with $ symbol" in interface "interface-name" control-plane
```

Dit vertaalt zich in het volgende opdrachtvoorbeeld, waarin de ACL-variabele die in de bovenstaande stap 2.3 'VAR-ACL-UNWANTED-COUNTRY' is gemaakt, als volgt wordt gebruikt:

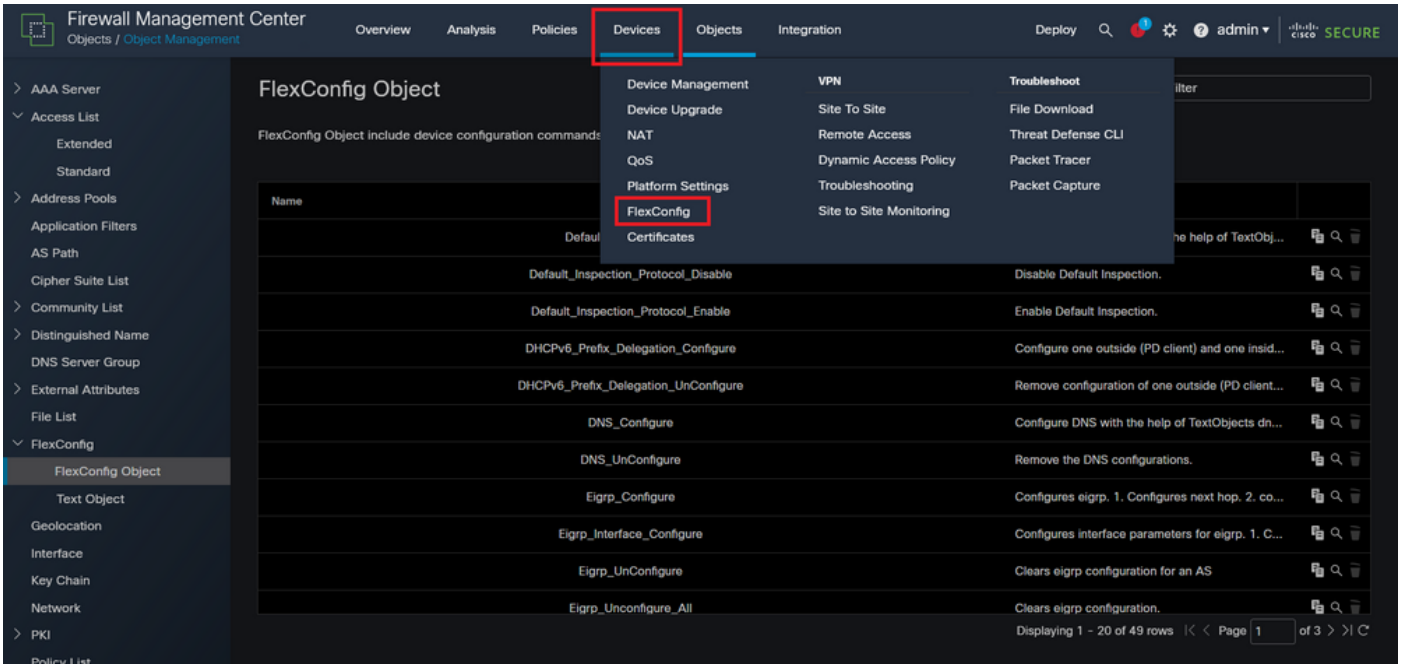
```
access-group $VAR-ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Zo moet het worden geconfigureerd in het objectvenster van FlexConfig, selecteert u vervolgens de knop Opslaan om het object FlexConfig te voltooien.



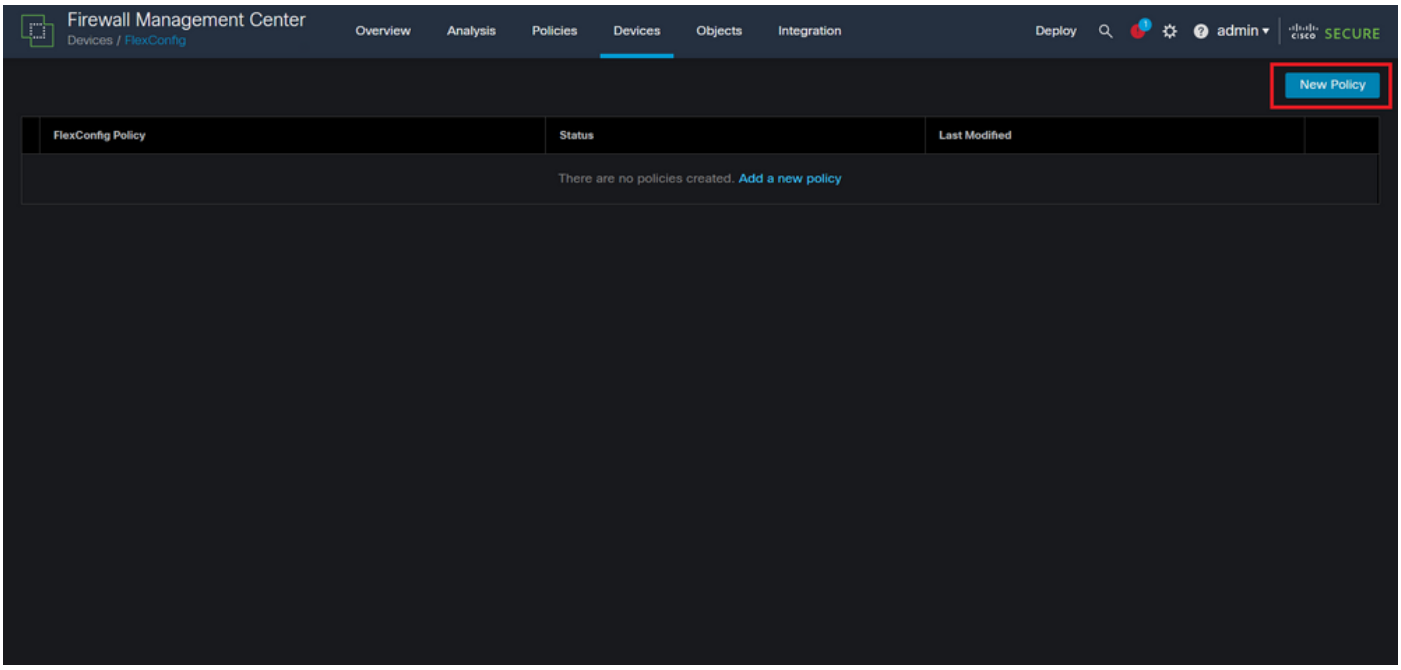
Afbeelding 14. Voltooide opdrachtregel voor Flexconfig Object

Stap 4. U moet de FlexConfig-objectconfiguratie op de FTD toepassen. Ga hiervoor naar Apparaten > FlexConfig.



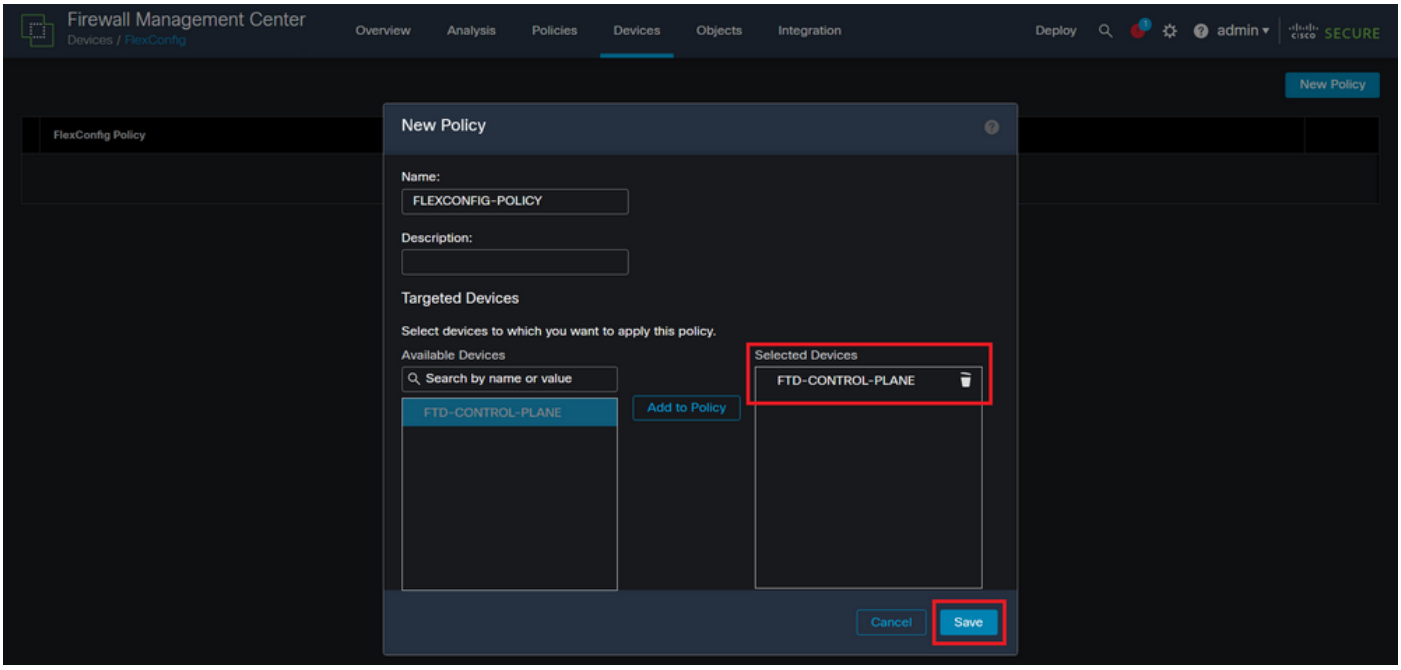
Afbeelding 15. Het menu FlexConfig-beleid

Stap 4.1. Klik vervolgens op Nieuw beleid als er nog geen FlexConfig voor uw FTD is gemaakt of bewerk het bestaande FlexConfig-beleid.



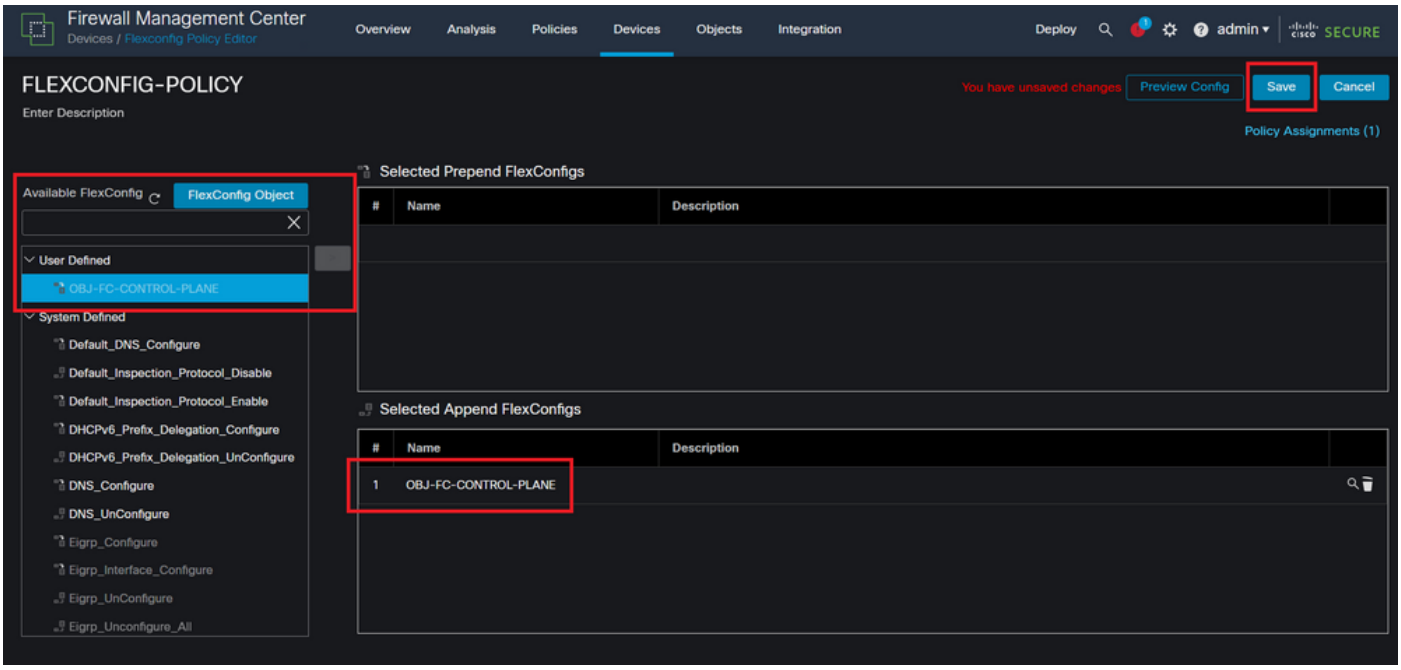
Afbeelding 16. FlexConfig-beleidsvorming

Stap 4.2. Voeg een naam toe voor het nieuwe FlexConfig-beleid en selecteer de FTD die u wilt toepassen op de gecreëerde Control-plane ACL.



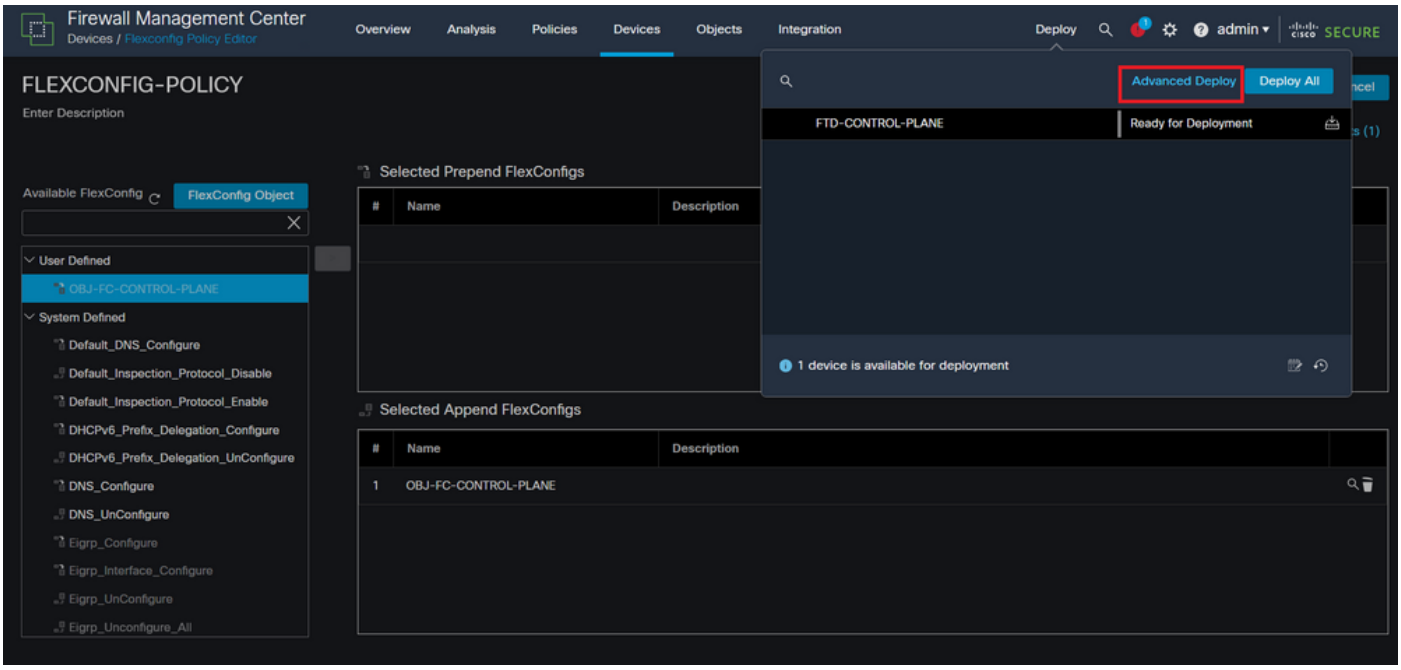
Afbeelding 17. FlexConfig-beleidsapparaattoewijzing

Stap 4.3. Zoek vanuit het linkerpaneel naar het object FlexConfig dat in de bovenstaande stap 3.2 is gemaakt en voeg het vervolgens toe aan het beleid van FlexConfig door op het pijltje rechts in het midden van het venster te klikken en vervolgens op de knop Opslaan te klikken.



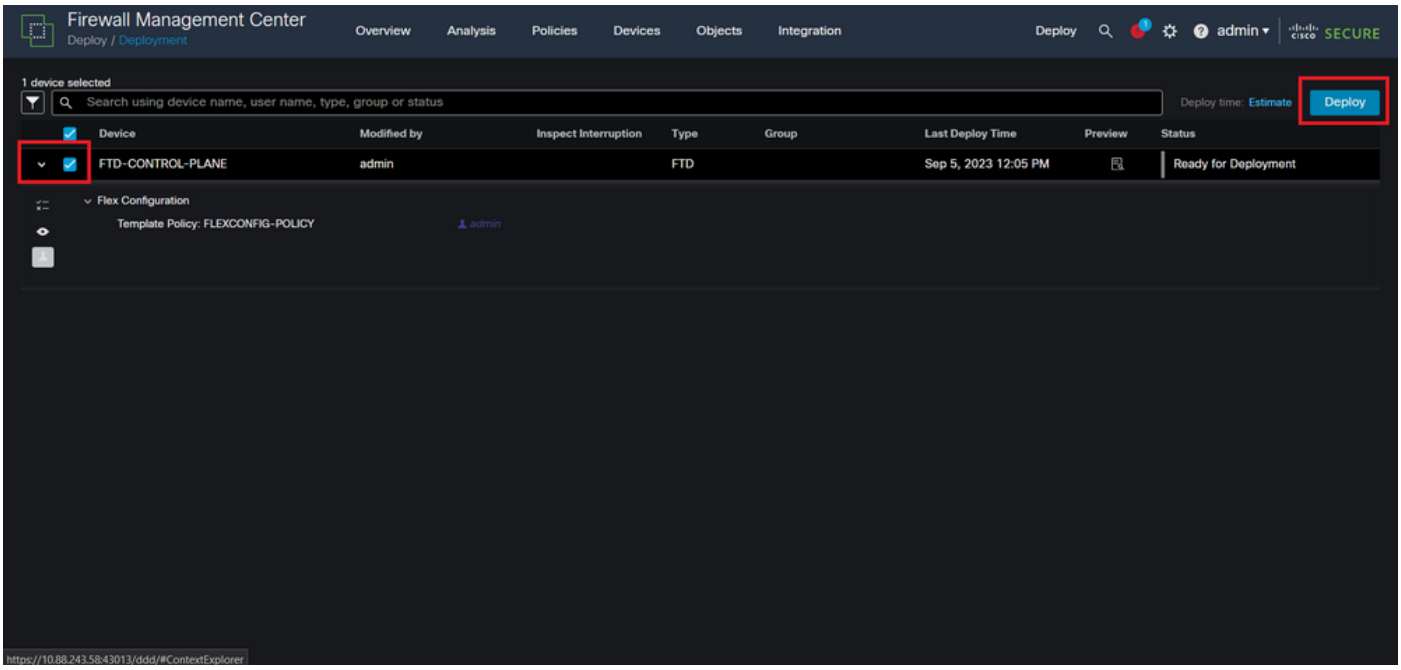
Afbeelding 18. Toewijzing van FlexConfig-beleidsobjecten

Stap 5. Ga verder met de implementatie van de configuratiewijziging in de FTD, hiervoor navigeer naar Implementeren > Geavanceerde implementatie.



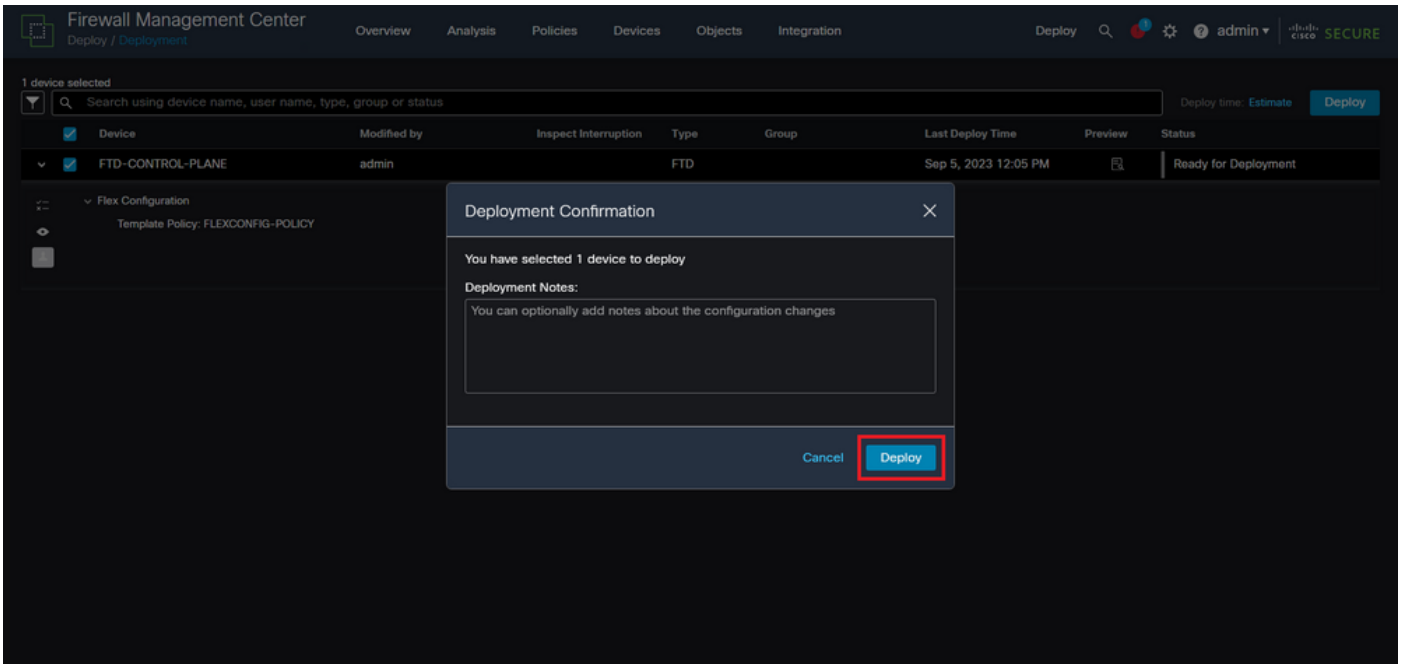
Afbeelding 19. FTD geavanceerde implementatie

Stap 5.1. Selecteer vervolgens de FTD waarop u het FlexConfig-beleid wilt toepassen. Als alles correct is, klik dan op Implementeren.



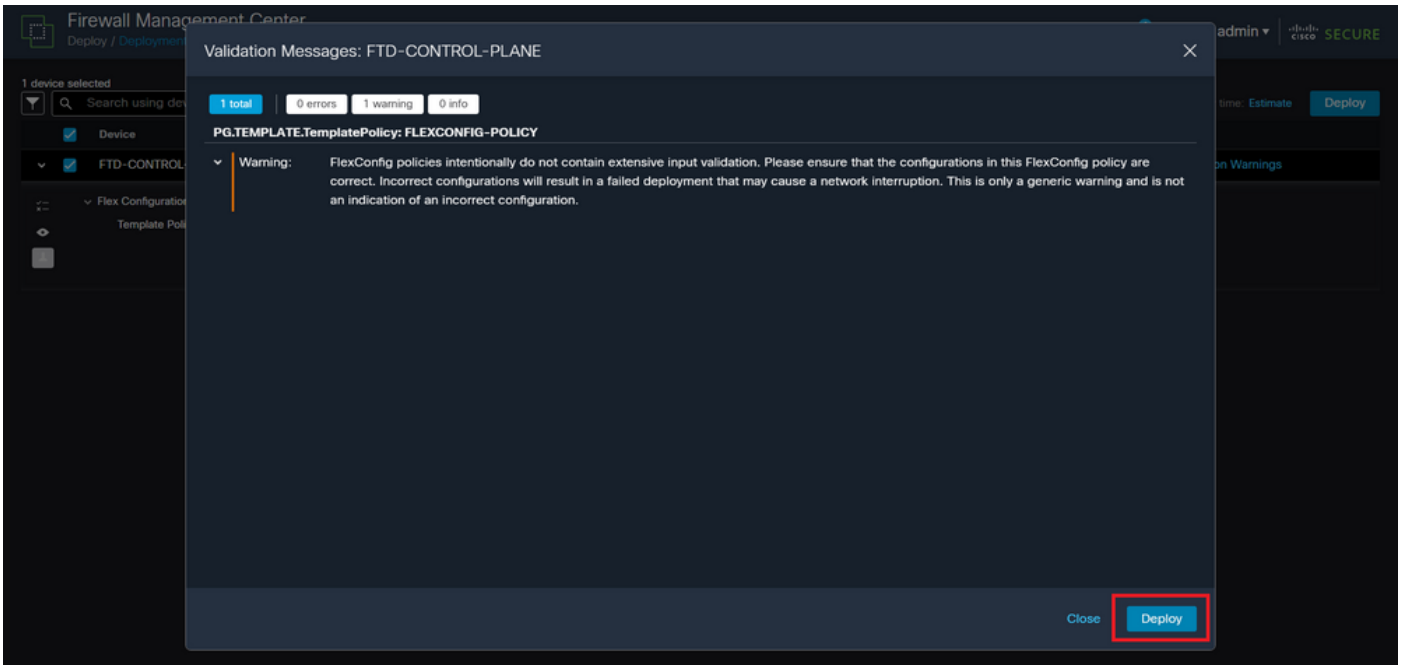
Afbeelding 20. FTD-implementatievalidering

Stap 5.2. Na dit, zal een venster van de Bevestiging van de Plaatsing verschijnen, zal een commentaar toevoegen om de plaatsing te volgen en te werk te gaan om op te stellen.



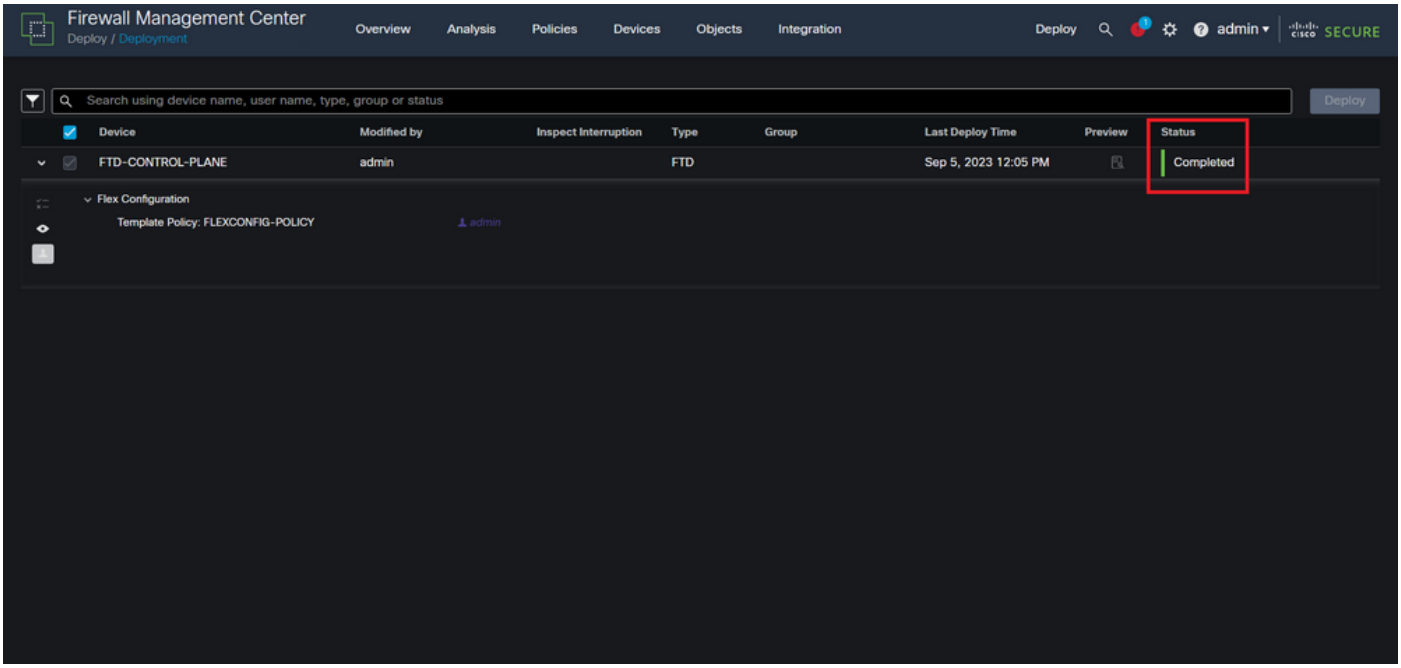
Afbeelding 21. Opmerkingen over FTD-implementatie

Stap 5.3. Er kan een waarschuwingsbericht verschijnen bij het implementeren van FlexConfig-wijzigingen. Klik op Implementeren alleen als u volledig zeker bent dat de beleidsconfiguratie correct is.



Afbeelding 2. Waarschuwing voor FTD-implementatie in Flexfig

Stap 5.4. Bevestig dat de beleidsontwikkeling voor het FTD succesvol is.



Afbeelding 23. FTD-implementatie geslaagd

Stap 6. Als u een nieuwe control-plane ACL voor uw FTD maakt of als u een bestaande ACL bewerkt die actief in gebruik is, dan is het belangrijk om te benadrukken dat de wijzigingen in de configuratie niet van toepassing zijn op reeds bestaande verbindingen met de FTD, daarom moet u de actieve verbindingspogingen met de FTD handmatig wissen. Hiervoor maakt u verbinding met de CLI van de FTD en verwijdert u de actieve verbindingen als volgt.

U kunt de actieve verbinding voor een specifiek IP-adres van de host als volgt wissen:

```
> clear conn address 192.168.1.10 all
```

U kunt de actieve verbindingen voor een heel subnetnetwerk als volgt wissen:

```
> clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

U kunt de actieve verbindingen voor een aantal IP-adressen als volgt wissen:

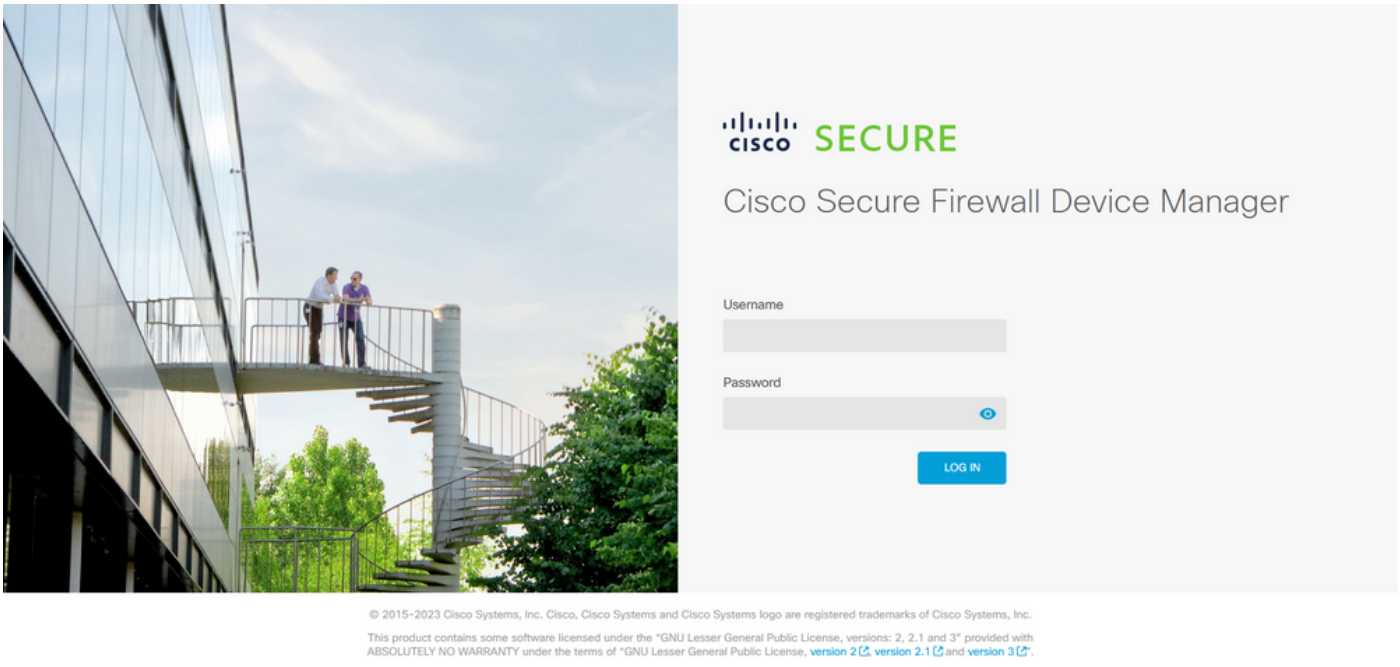
```
> clear conn address 192.168.1.1-192.168.1.10 all
```

Opmerking: het is sterk aanbevolen om het sleutelwoord 'all' aan het einde van de duidelijke conn adres commando te gebruiken om het verwijderen van de actieve VPN brute kracht verbinding pogingen te dwingen naar de veilige firewall, vooral wanneer de aard van de VPN brute kracht aanval start een explosie van constante verbinding pogingen.

Configureer een control-plane ACL voor FTD die wordt beheerd door FDM

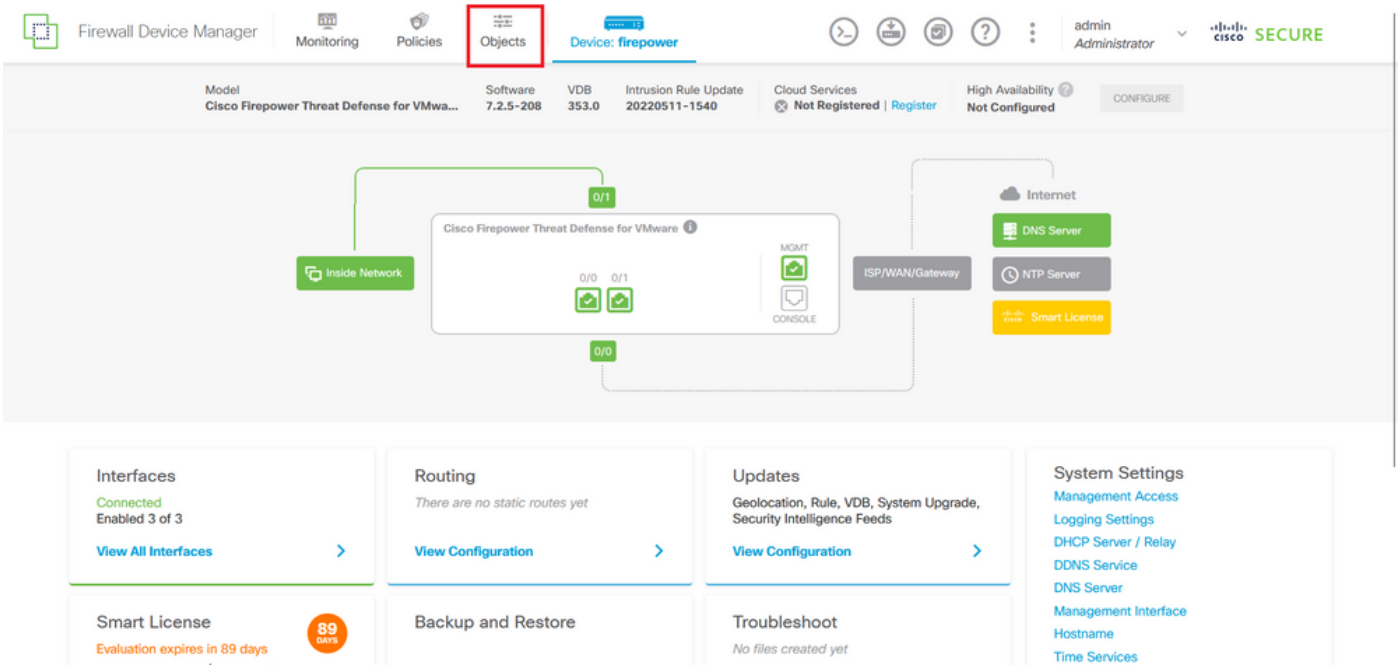
Dit is de procedure die u moet volgen in een FDM om een besturingsplane ACL te configureren om inkomende brute VPN-krachtaanvallen te blokkeren naar de buiten-FTD-interface:

Stap 1. Open de FDM GUI via HTTPS en log in met uw referenties.



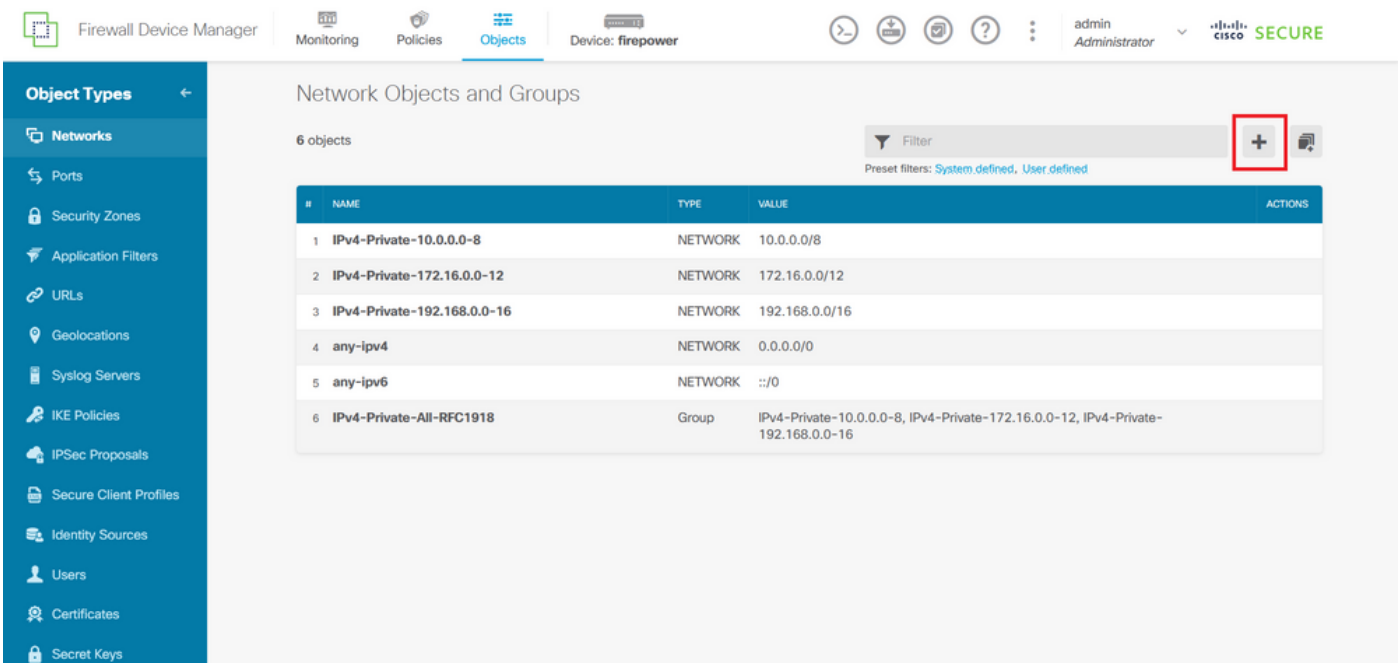
Afbeelding 24. FDM-inlogpagina

Stap 2. U moet een objectnetwerk maken. Ga hiervoor naar Objecten:



Afbeelding 25. FDM hoofddashboard

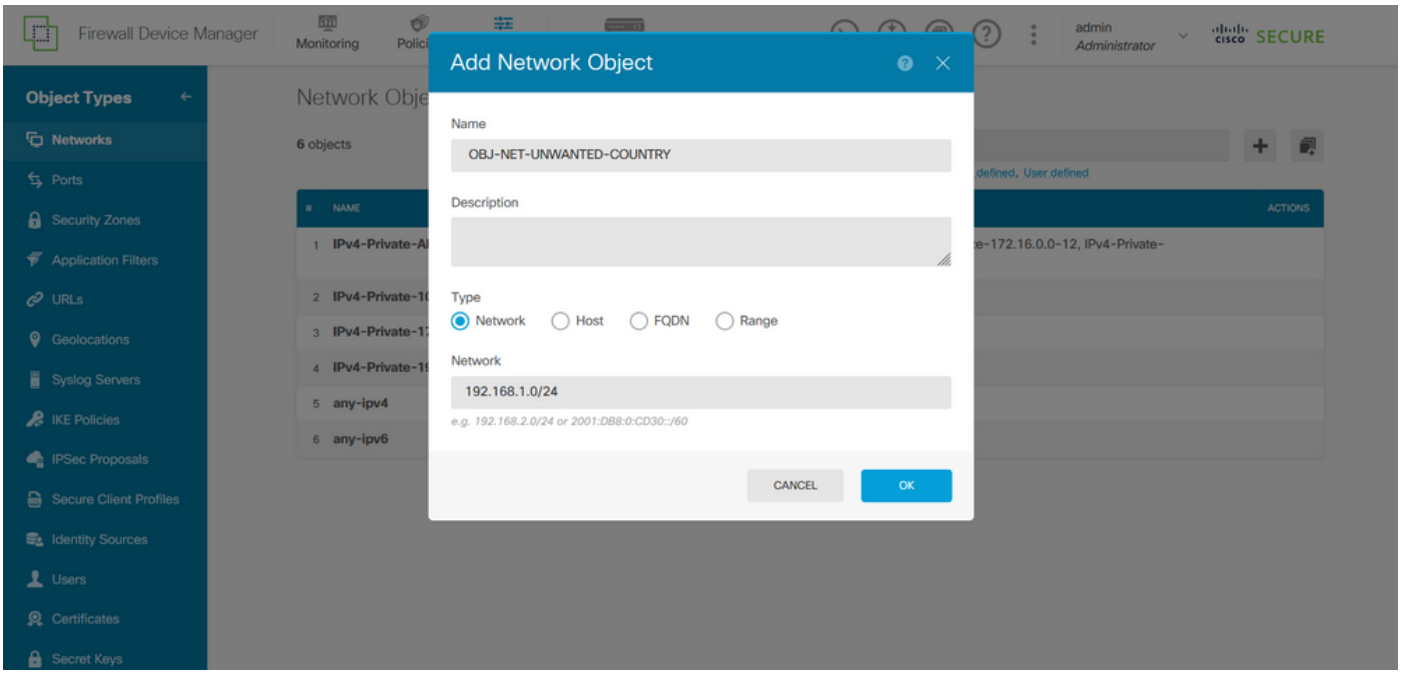
Stap 2.1. Selecteer Netwerken in het linkerdeelvenster en klik op '+' om een nieuw netwerkobject te maken.



Afbeelding 26. Object maken

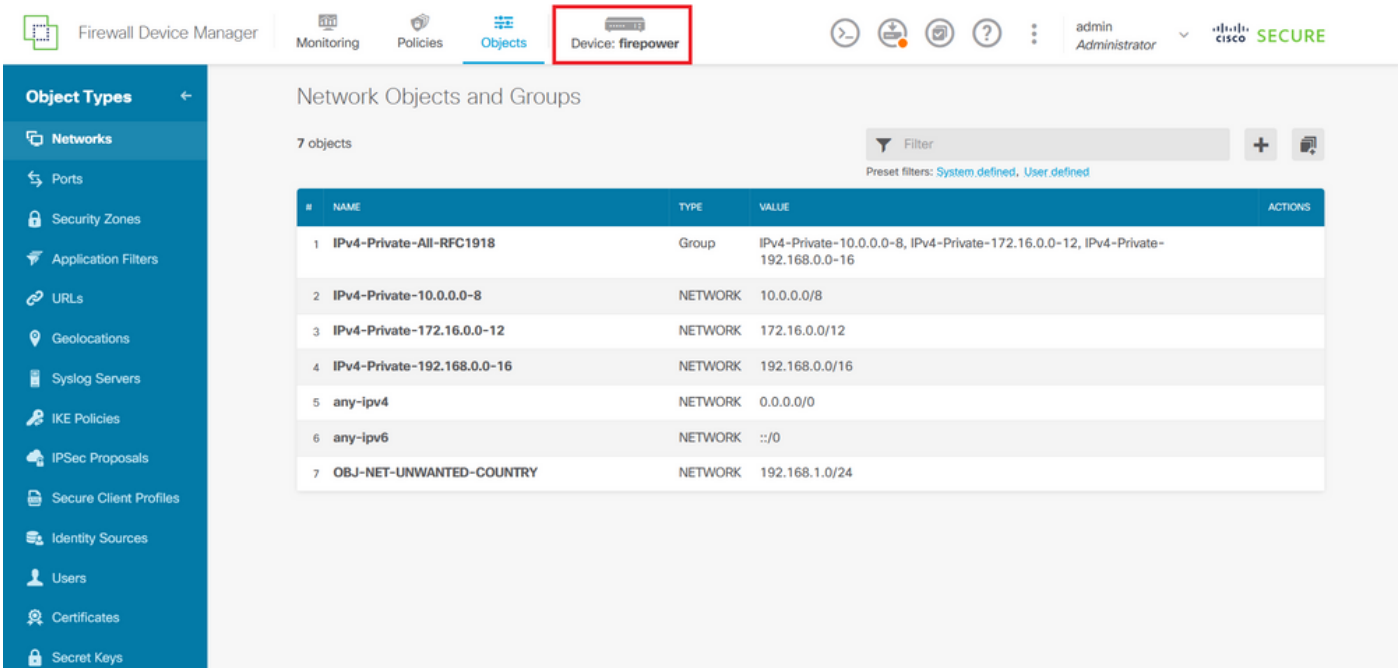
Stap 2.2. Voeg een naam toe voor het netwerkobject, selecteer het netwerktype voor het object, voeg het IP-adres, het netwerkadres of het IP-bereik toe voor het verkeer dat moet worden geweigerd voor de FTD. Klik vervolgens op de knop OK om het objectnetwerk te voltooien.

- In dit voorbeeld, het object netwerk geconfigureerd is bedoeld om VPN brute force aanvallen te blokkeren die komen van het 192.168.1.0/24 subnetnet.



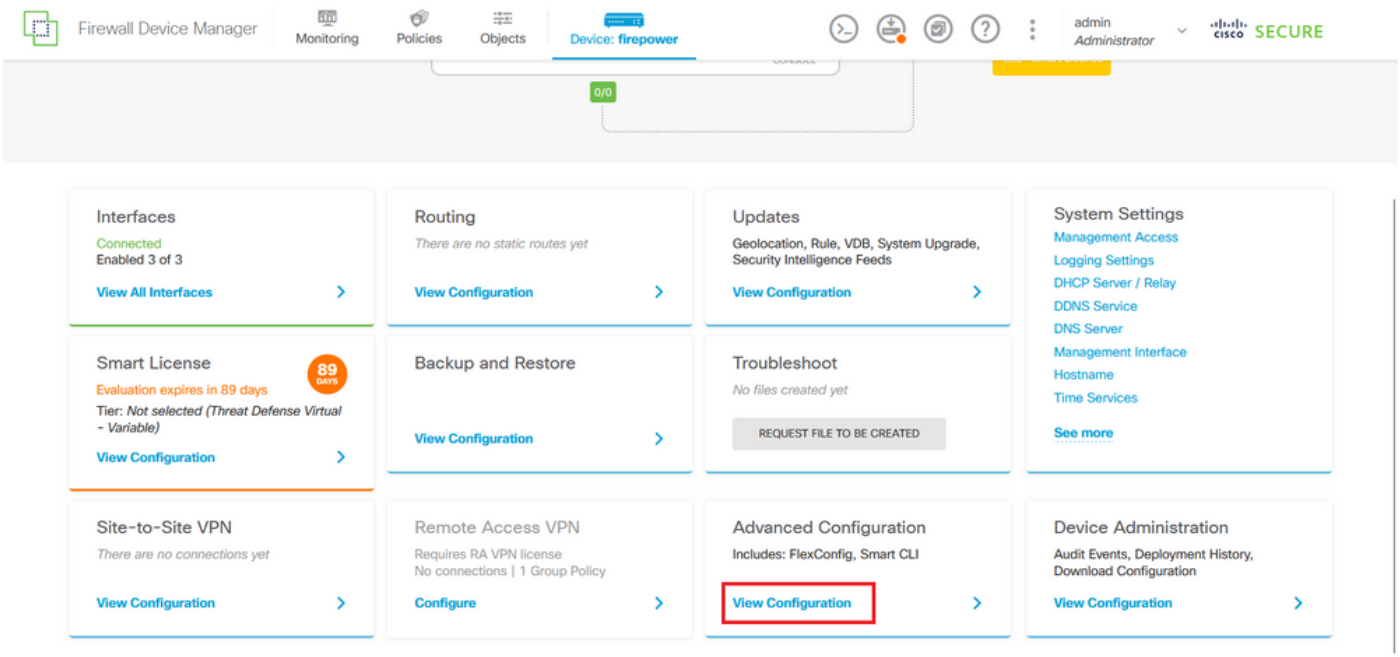
Afbeelding 27. Netwerkobject toevoegen

Stap 3. Vervolgens moet u een uitgebreide ACL maken. Hiervoor navigeer u naar het tabblad Apparaat in het bovenste menu.



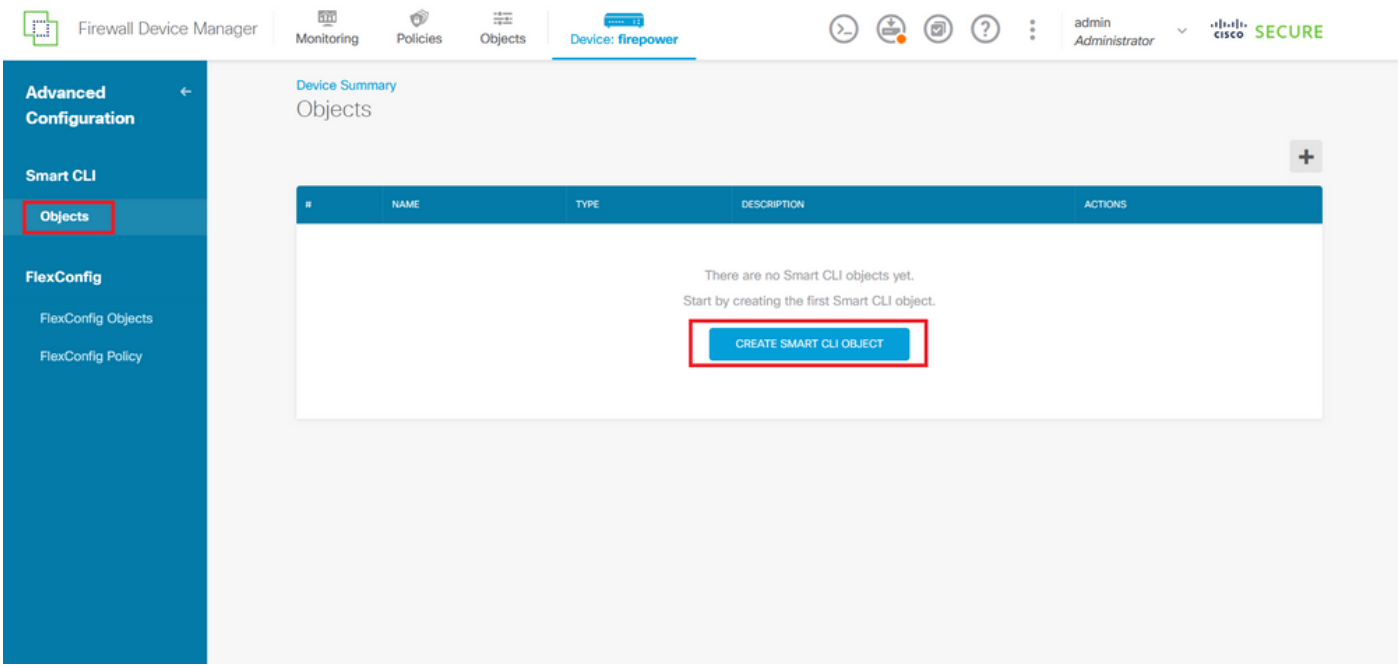
Afbeelding 28. Pagina met apparaatinstellingen

Stap 3.1. Blader naar beneden en selecteer Weergaveconfiguratie als volgt in het vierkant Geavanceerde configuratie.



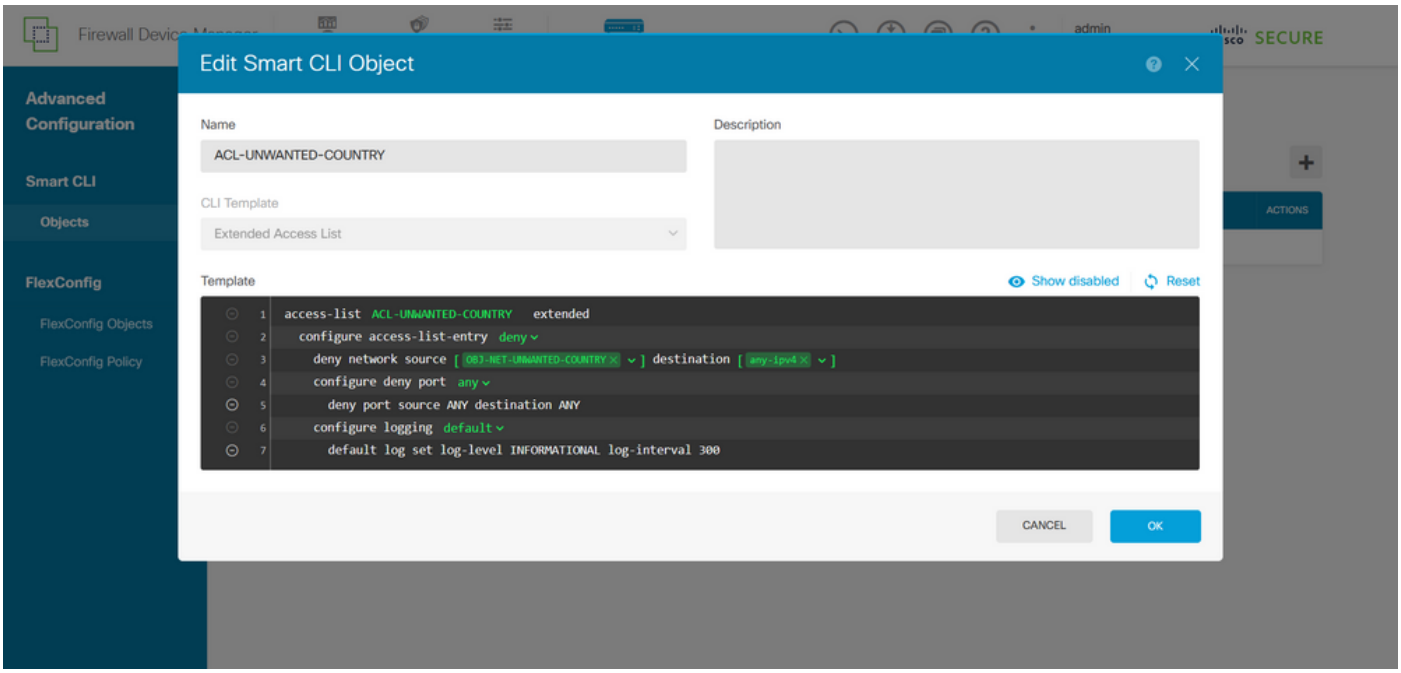
Afbeelding 29. FDM geavanceerde configuratie

Stap 3.2. Navigeer vervolgens vanuit het linkerpaneel naar Smart CLI > Objects en klik op CREATE SMART CLI OBJECT.



Afbeelding 30. Slimme CLI-objecten

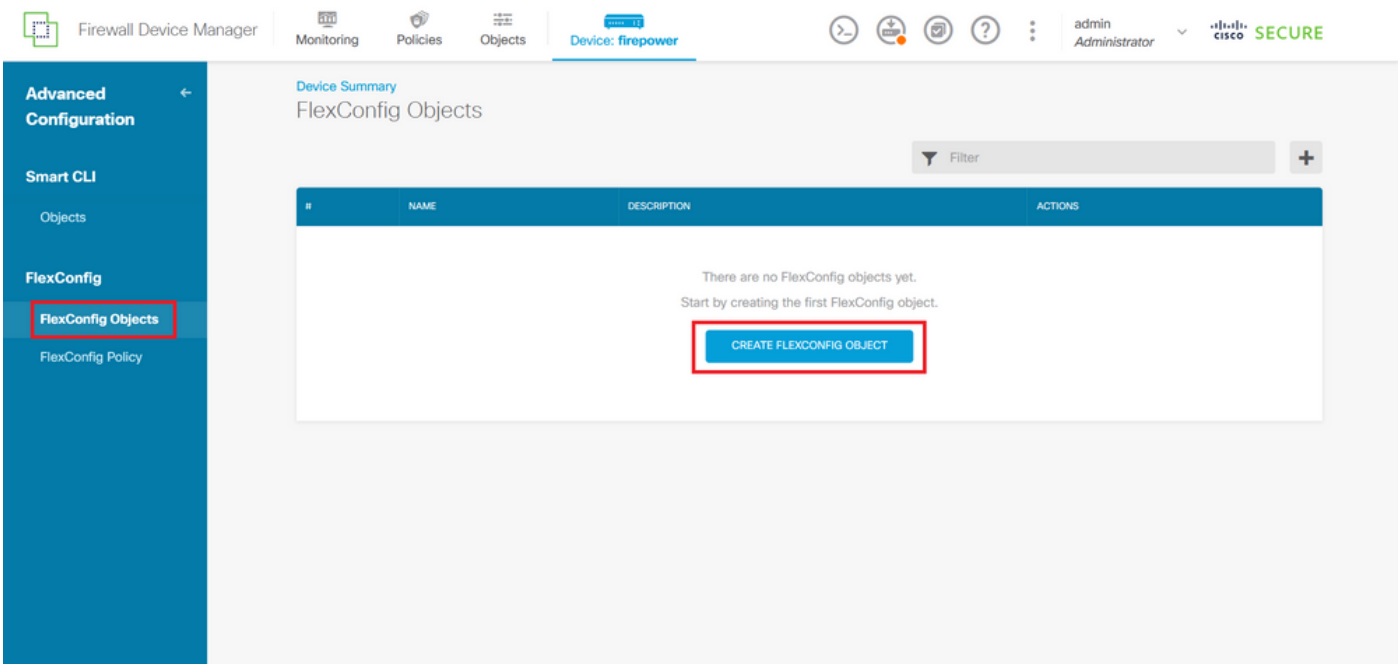
Stap 3.3. Voeg een naam toe voor de uitgebreide ACL om te maken, selecteer Uitgebreide toegangslijst in het vervolgkeuzemenu van de CLI-sjabloon en configureer de ACE's die nodig zijn met behulp van het netwerkobject dat in de bovenstaande stap 2.2 is gemaakt, en klik vervolgens op de knop OK om de ACL te voltooien.



Afbeelding 31. Uitgebreide ACL-aanmaak

Opmerking: als u meer ACE's voor de ACL moet toevoegen, kunt u dit doen door de muis links van de huidige ACE te laten zweven; dan verschijnen er drie aanklikbare punten. Klik op hen en selecteer Dupliceren om meer ACE's toe te voegen.

Stap 4. Vervolgens moet u een FlexConfig-object maken. Hiervoor navigeert u naar het linkerpaneel en selecteert u FlexConfig > FlexConfig-objecten. Klik vervolgens op FLEXCONFIG-OBJECT MAKEN.



Afbeelding 32. FlexConfig-objecten

Stap 4.1. Voeg als volgt een naam toe voor het object FlexConfig om de ACL voor besturingsplane als inkomend voor de buiteninterface te maken en te configureren.

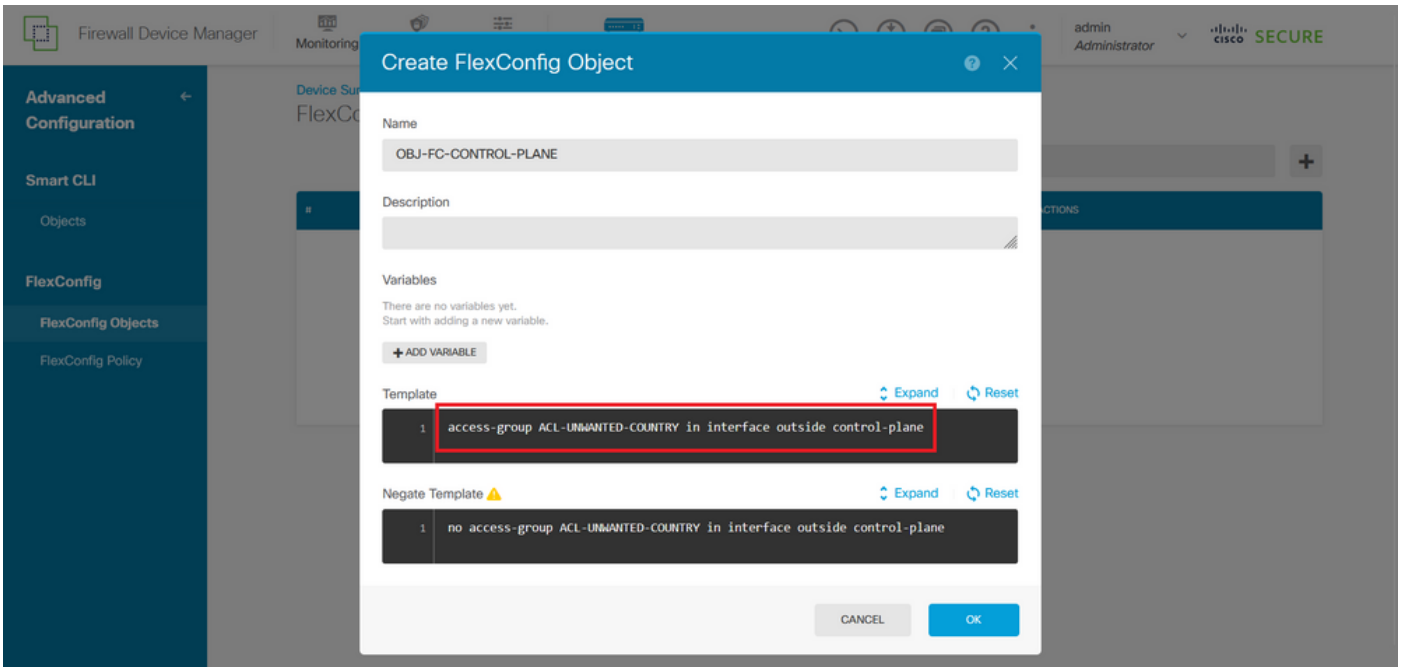
Syntaxis van opdrachtregel:

```
access-group "ACL-name" in interface "interface-name" control-plane
```

Dit vertaalt zich in het volgende opdrachtvoorbeeld, waarin de uitgebreide ACL die in de bovenstaande stap 3.3 'ACL-UNWANTED-COUNTRY' is gemaakt, als volgt wordt gebruikt:

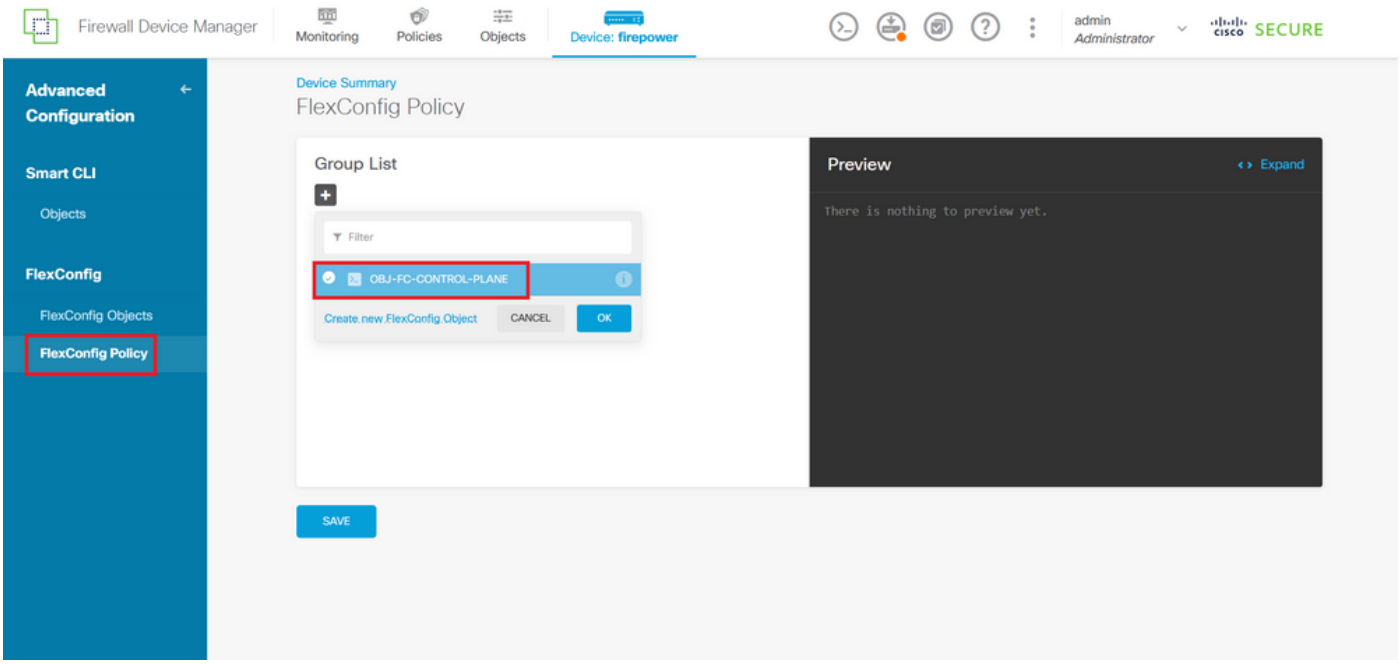
```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Zo moet het worden geconfigureerd in het objectvenster van FlexConfig, selecteert u vervolgens de knop OK om het object FlexConfig te voltooien.



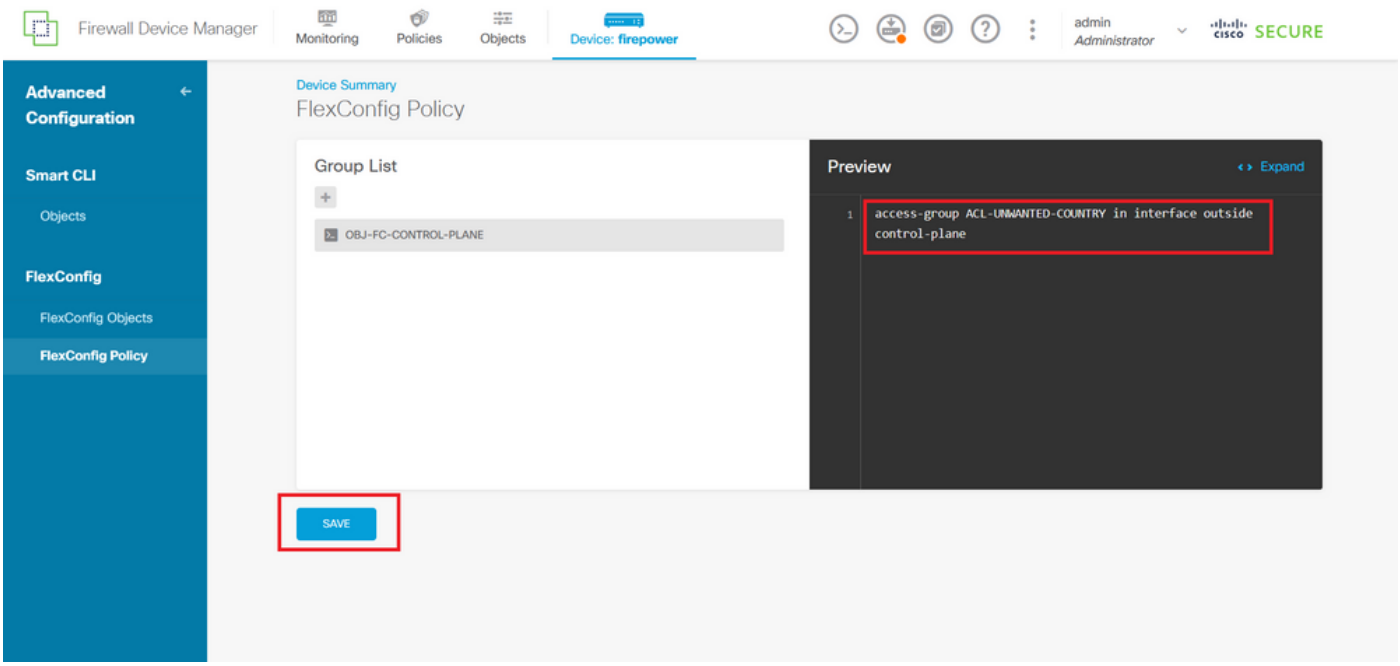
Afbeelding 33. Creatie van FlexConfig-objecten

Stap 5. Ga vervolgens verder met het maken van een FlexConfig-beleid. Ga hiervoor naar Flexfig > FlexConfig-beleid, klik op de knop '+' en selecteer het object FlexConfig dat in de bovengenoemde stap 4.1 is gemaakt.



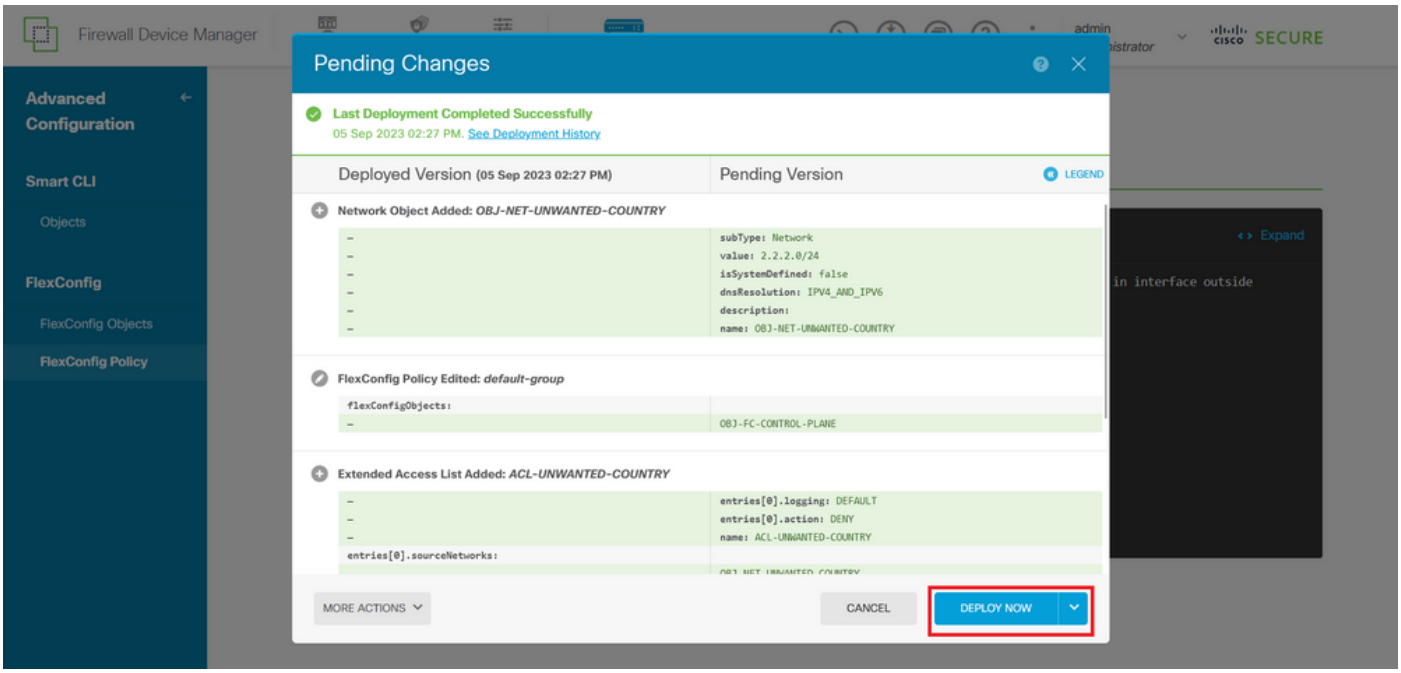
Afbeelding 34. FlexConfig-beleid

Stap 5.1. Bevestig dat de voorvertoning van FlexConfig de juiste configuratie toont voor de besturings-vlakke ACL die is gemaakt en klik op de knop Opslaan.



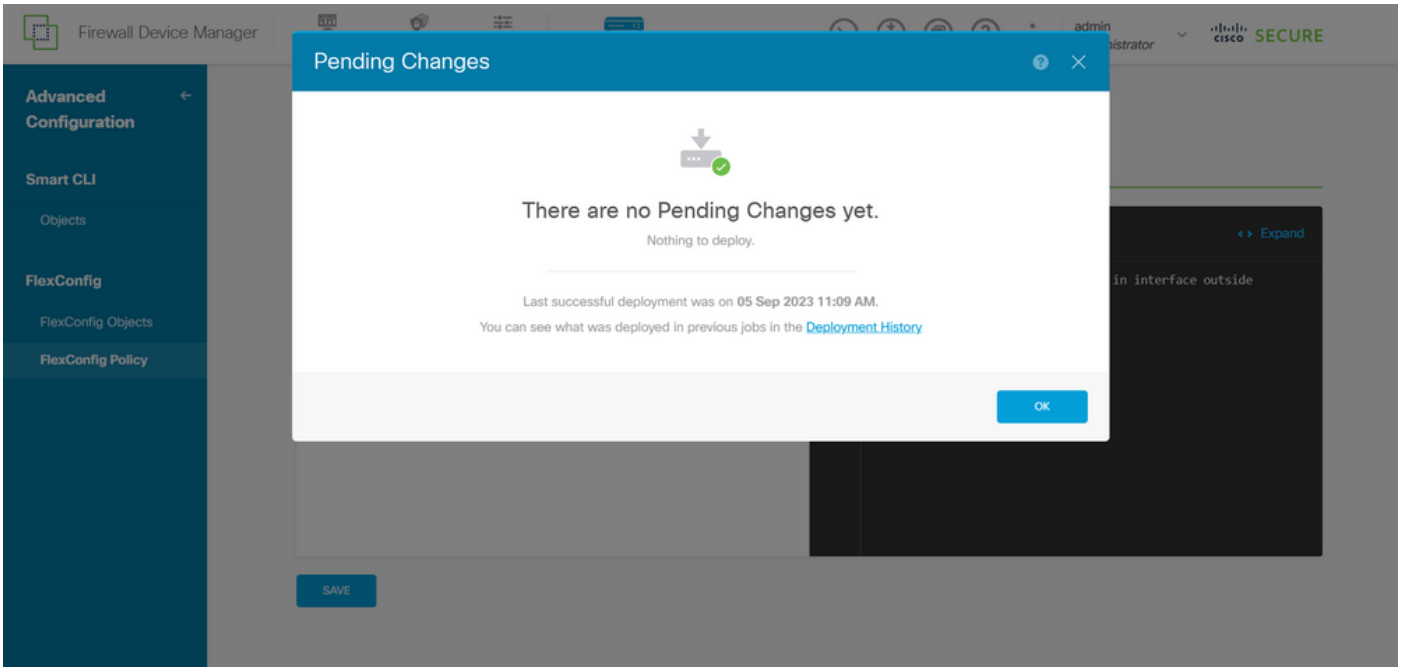
Afbeelding 35. FlexConfig-beleidsvoorbeeld

Stap 6. Stel de configuratieveranderingen in de FTD die u tegen de aanvallen van de de brute kracht van VPN wilt beschermen, voor dit, klik op de knop van de Plaatsing in het hoogste menu, bevestig dat de te opstellen configuratieveranderingen correct zijn, en klik dan op NU OPSTELLEN.



Afbeelding 36. Hangende implementatie

Stap 6.1. Bevestig dat de beleidsontwikkeling succesvol is.



Afbeelding 37. Implementatie geslaagd

Stap 7. Als u een nieuwe control-plane ACL voor uw FTD maakt of als u een bestaande ACL bewerkt die actief in gebruik is, dan is het belangrijk om te benadrukken dat de wijzigingen in de configuratie niet van toepassing zijn op reeds bestaande verbindingen met de FTD, daarom moet u de actieve verbindingspogingen met de FTD handmatig wissen. Hiervoor maakt u verbinding met de CLI van de FTD en verwijdert u de actieve verbindingen als volgt.

U kunt de actieve verbinding voor een specifiek IP-adres van de host als volgt wissen:

```
> clear conn address 192.168.1.10 all
```

U kunt de actieve verbindingen voor een heel subnetnetwerk als volgt wissen:

```
> clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

U kunt de actieve verbindingen voor een aantal IP-adressen als volgt wissen:

```
> clear conn address 192.168.1.1-192.168.1.10 all
```

Opmerking: het is sterk aanbevolen om het sleutelwoord 'all' aan het einde van de duidelijke conn adres commando te gebruiken om het verwijderen van de actieve VPN brute kracht verbinding pogingen te dwingen naar de veilige firewall, vooral wanneer de aard van de VPN brute kracht aanval start een explosie van constante verbinding pogingen.

Configureer een besturings-vlakke ACL voor ASA met CLI

Dit is de procedure die u moet volgen in een ASA CLI om een besturingsplane ACL te configureren om inkomende brute-krachtaanvallen van VPN te blokkeren naar de buiteninterface:

Stap 1. Log in op de beveiligde firewall ASA via CLI en krijg als volgt toegang tot de 'Configure terminal'.

```
asa# configure terminal
```

Stap 2. Gebruik de volgende opdracht om een uitgebreide ACL te configureren om een IP-adres of netwerkadres van de host te blokkeren voor het verkeer dat moet worden geblokkeerd naar de ASA.

- In dit voorbeeld, maakt u een nieuwe ACL genaamd 'ACL-UNWANTED-COUNTRY' en de ACE-ingang geconfigureerd zal VPN brute kracht aanvallen die komen van het 192.168.1.0/24 subnet blokkeren.

```
asa(config)# access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any
```

Stap 3. Gebruik de volgende opdracht voor toegangsgroepen om de ACL (ACL-UNWANTED-COUNTRY) te configureren als een besturings-vlak ACL voor de externe ASA-interface.

```
asa(config)# access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Stap 4. Als u een nieuwe control-plane ACL maakt of als u een bestaande ACL bewerkt die actief in gebruik is, dan is het belangrijk om te benadrukken dat de wijzigingen in de configuratie niet van toepassing zijn op reeds bestaande verbindingen met de ASA, daarom moet u de actieve verbinding pogingen tot de ASA handmatig wissen. Schakel hiervoor de actieve verbindingen als volgt uit.

U kunt de actieve verbinding voor een specifiek IP-adres van de host als volgt wissen:

```
asa# clear conn address 192.168.1.10 all
```

U kunt de actieve verbindingen voor een heel subnetnetwerk als volgt wissen:

```
asa# clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

U kunt de actieve verbindingen voor een aantal IP-adressen als volgt wissen:

```
asa# clear conn address 192.168.1.1-192.168.1.10 all
```

Opmerking: het is sterk aanbevolen om het sleutelwoord 'all' aan het einde van de duidelijke conn adres commando te gebruiken om het verwijderen van de actieve VPN brute kracht verbinding pogingen te dwingen naar de veilige firewall, vooral wanneer de aard van de VPN brute kracht aanval start een explosie van constante verbinding pogingen.

Alternatieve configuratie om aanvallen voor beveiligde firewall te blokkeren met behulp van de 'shun' Command

In het geval van een onmiddellijke optie om aanvallen voor de veilige firewall te blokkeren, dan kunt u de 'shun' opdracht gebruiken. Deze opdracht laat u verbindingen van een aanvallende gastheer blokkeren.

- Zodra u een IP-adres hebt uitgeschakeld, worden alle toekomstige verbindingen van het IP-bronadres verbroken en vastgelegd totdat de blokkeringsfunctie handmatig wordt verwijderd.

- De blokkerende functie van de hunopdracht wordt toegepast, ongeacht of er een verbinding met het opgegeven hostadres actief is.

- Als u het doeladres, de bron- en doelpoorten en het protocol opgeeft, laat u de bijbehorende verbinding vallen en zet u een waarschuwing op alle toekomstige verbindingen van de bron-IP

adres; alle toekomstige verbindingen worden gemeden, niet alleen die die deze specifieke verbindingsparameters aanpassen.

- U kunt alleen één opdracht per IP-bronadres hebben.

- Omdat deze opdracht wordt gebruikt om aanvallen dynamisch te blokkeren, wordt deze niet weergegeven in de configuratie van het bedreigingsverdedigingsapparaat.

- Wanneer een interfaceconfiguratie wordt verwijderd, worden alle shuns die aan die interface zijn verbonden ook verwijderd.

- Shun-opdrachtsyntaxis:

```
shun source_ip [ dest_ip source_port dest_port [ protocol]] [ vlan vlan_id]
```

- Gebruik de no form van deze opdracht om een schuine stand uit te schakelen:

```
no shun source_ip [ vlan vlan_id]
```

Om een host IP-adres af te sluiten, gaat u als volgt te werk voor de beveiligde firewall. In dit voorbeeld, wordt het "shun"bevel gebruikt om de brute krachtaanvallen van VPN te blokkeren die uit het bronIP adres 192.168.1.10 komen.

Configuratievoorbeeld voor FTD.

Stap 1. Log in op het FTD via CLI en pas de opdracht Shun als volgt toe.

```
<#root>

>

 shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf
```

```
Shun 192.168.1.10 successful
```

Stap 2. U kunt de volgende showopdrachten gebruiken om de gesloten IP-adressen in het FTD te bevestigen en om de shun-treffers per IP-adres te controleren:

```
<#root>

>

show shun

shun (outside) 192.168.1.10 0.0.0.0 0 0 0

>

show shun statistics

diagnostic=OFF, cnt=0
outside=ON, cnt=0

Shun 192.168.1.10 cnt=0, time=(0:00:28)
```

Configuratievoorbeeld voor ASA

Stap 1. Log in op de ASA via CLI en pas de shun-opdracht als volgt toe.

```
<#root>

asa#

 shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf


Shun 192.168.1.10 successful
```

Stap 2. U kunt de volgende showopdrachten gebruiken om de gesloten IP-adressen in de ASA te bevestigen en om de shun-hit tellingen per IP-adres te controleren:

```
<#root>

asa#

show shun

shun (outside) 192.168.1.10 0.0.0.0 0 0 0
```

```
asa#
```

```
show shun statistics
```

```
outside=ON, cnt=0
inside=OFF, cnt=0
dmz=OFF, cnt=0
outside1=OFF, cnt=0
mgmt=OFF, cnt=0

Shun 192.168.1.10 cnt=0, time=(0:01:39)
```

N.B.: Controleer de referentie van de opdracht Cisco Secure Firewall Threat Defence Command

---

Verifiëren

Ga als volgt te werk om te bevestigen dat de configuratie van de besturings-vlakke ACL op zijn plaats is voor de beveiligde firewall:

Stap 1. Log in op de beveiligde firewall via CLI en voer de volgende opdrachten uit om te bevestigen dat de configuratie van de besturings-vlak ACL wordt toegepast.

Outputvoorbeeld voor het door het VCC beheerde FTD:

<#root>

```
>
```

```
show running-config access-list ACL-UNWANTED-COUNTRY
```

```
access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any
```

```
>
```

```
show running-config access-group
```

```
***OUTPUT OMITTED FOR BREVITY***
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Outputvoorbeeld voor de FTD beheerd door FDM:

<#root>

```
> show running-config object id OBJ-NET-UNWANTED-COUNTRY
```

```
object network OBJ-NET-UNWANTED-COUNTRY
subnet 192.168.1.0 255.255.255.0
```

```
>
show running-config access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any4 log default

> show running-config access-group

***OUTPUT OMITTED FOR BREVITY***
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Outputvoorbeeld voor ASA:

```
<#root>
asa#
show running-config access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any

asa#
show running-config access-group

***OUTPUT OMITTED FOR BREVITY***
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Stap 2. Om te bevestigen dat de ACL-besturingsplane het vereiste verkeer blokkeert, gebruikt u de opdracht packet-tracer om een inkomende TCP 443-verbinding met de buiteninterface van de beveiligde firewall te simuleren en gebruikt u vervolgens de opdracht show access-list <acl-name>. De telling van de ACL-hit moet worden verhoogd telkens wanneer een VPN brute force-verbinding met de beveiligde firewall door de ACL-besturingsplane wordt geblokkeerd:

- In dit voorbeeld simuleert de pakkettracer-opdracht een inkomende TCP 443-verbinding die afkomstig is van host 192.168.1.10 en die bestemd is voor het externe IP-adres van onze beveiligde firewall. De 'packet-tracer'-uitvoer bevestigt dat het verkeer wordt gedropt en de uitvoer van de 'show access-list' geeft de toename van het aantal hit weer voor onze besturings-plane ACL:

Outputvoorbeeld voor FTD

```
<#root>
```

```
>

packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.251 443

Phase: 1
Type:

ACCESS-LIST

Subtype: log

Result: DROP

Elapsed time: 21700 ns
Config:
Additional Information:

Result:
input-interface: outside(vrfid:0)
input-status: up
input-line-status: up

Action: drop

Time Taken: 21700 ns

Drop-reason: (acl-drop) Flow is denied by configured rule

, Drop-location: frame 0x00005623c7f324e7 flow (NA)/NA


>

show access-list ACL-UNWANTED-COUNTRY


access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f
access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any (

hitcnt=1

) 0x142f69bf
```

Outputvoorbeeld voor ASA

```
<#root>

asa#

packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.5 443

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 19688 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
```

```
Type:

ACCESS-LIST

Subtype: log

Result: DROP

Elapsed time: 17833 ns
Config:
Additional Information:

Result:
input-interface: outside
input-status: up
input-line-status: up

Action: drop

Time Taken: 37521 ns

Drop-reason: (acl-drop) Flow is denied by configured rule

, Drop-location: frame 0x0000556e6808cac8 flow (NA)/NA

asa#

show access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f
access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any

(hitcnt=1)

 0x9b4d26ac
```

N.B.: Als een VPN-oplossing zoals Cisco Secure Client VPN in de beveiligde firewall is geïmplementeerd, kan een echte verbindingspoging met de beveiligde firewall worden uitgevoerd om te bevestigen dat de besturingsplane ACL werkt zoals verwacht om het vereiste verkeer te blokkeren.

Verwante bugs

- ENH | Geo-location gebaseerde AnyConnect-clientverbindingen: Cisco-bug-id CSCvs65322

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.