Op geolocatie gebaseerde beleidsregels voor externe toegang tot VPN configureren op basis van beveiligde firewall-bedreigingsverdediging

Inhoud

Inleiding

Dit document beschrijft het proces voor het toestaan of weigeren van RAVPN-verbindingen op basis van specifieke geolocaties op Secure Firewall Threat Defence (FTD).

Voorwaarden

Vereisten en beperkingen

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure Firewall Management Center (FMC)
- Externe toegang VPN (RAVPN)
- Basisconfiguratie van geolocatie

De huidige eisen en beperkingen voor op geolocatie gebaseerd beleid zijn:

- Alleen ondersteund op FTD versie 7.7.0+, beheerd door FMC versie 7.7.0+.
- Niet ondersteund op FTD die wordt beheerd door Secure Firewall Device Manager (FDM).

- Niet ondersteund in clustermodus
- Niet-geclassificeerde IP-adressen op basis van geolocatie worden niet gecategoriseerd op basis van geografische herkomst. Hiervoor dwingt het FMC de standaardmaatregelen voor het toegangsbeleid voor de dienst af.
- Het beleid voor toegang tot services op basis van geolocatie is niet van toepassing op WebLaunch-pagina's, zodat u de beveiligde client zonder beperkingen kunt downloaden.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Secure Firewall versie 7.7.0
- Secure Firewall Management Center versie 7.7.0

Volledige informatie over deze functie kunt u vinden in de sectie VPN-toegang beheren van externe gebruikers op basis van geolocatie binnen de configuratiehandleiding voor apparaten van Cisco Secure Firewall Management Center 7.7.

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

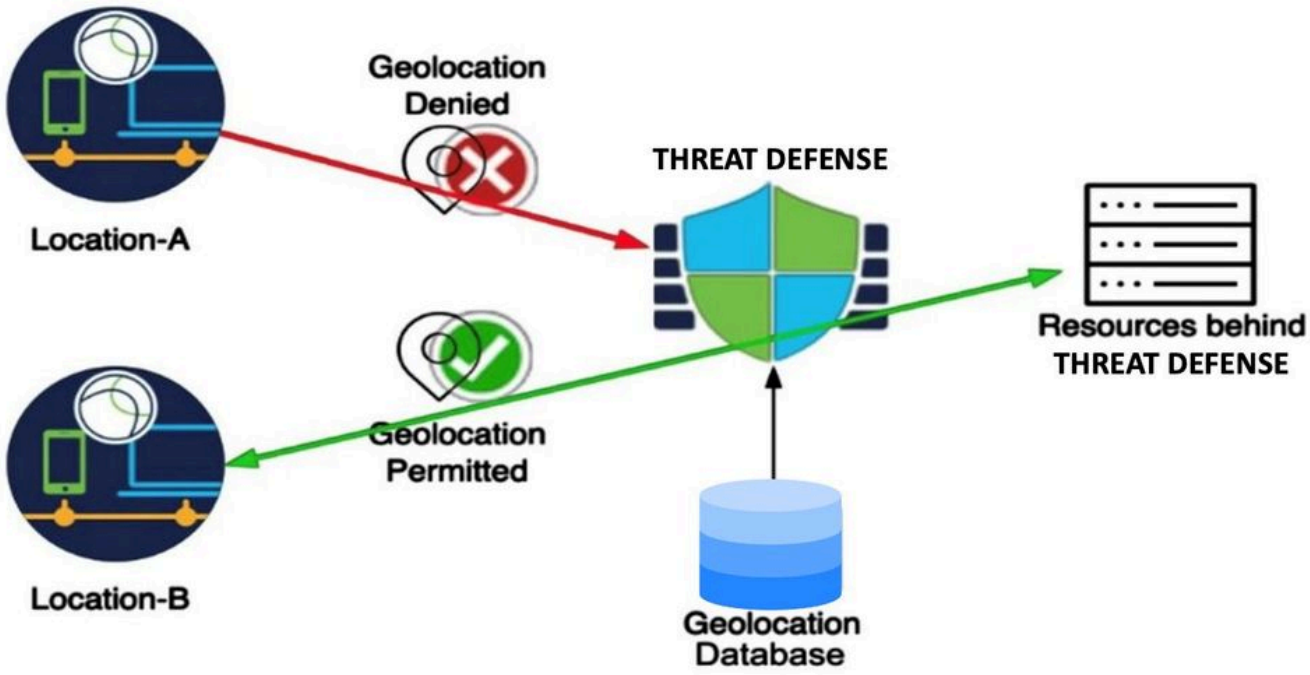
Het op geolocatie gebaseerde toegangsbeleid biedt vandaag de dag een aanzienlijke waarde in de netwerkbeveiliging, waardoor verkeer kan worden geblokkeerd op basis van de geografische oorsprong. Traditioneel kunnen organisaties beleid voor verkeerstoegang definiëren voor algemeen netwerkverkeer dat via de firewall verloopt. Nu, met de introductie van deze functie, is het mogelijk om op geolocatie-gebaseerde toegangscontrole toe te passen voor Remote Access VPN-sessieverzoeken.

Deze functie biedt de volgende voordelen:

- Op geolocatie gebaseerde regels: Klanten kunnen regels opstellen om RAVPN-aanvragen toe te staan of te weigeren op basis van specifieke geolocaties, zoals landen of continenten. Dit zorgt voor een nauwkeurige controle over welke geografische locaties VPN-sessies kunnen initiëren.
- Blokkering vóór verificatie: Sessies die door deze regels worden geïdentificeerd voor een actie 'ontkennen' worden geblokkeerd voor de verificatie, en deze pogingen worden correct vastgelegd voor beveiligingsdoeleinden. Deze preventieve actie helpt bij het beperken van ongeoorloofde toegangspogingen.
- Naleving en beveiliging: Deze eigenschap helpt in het verzekeren van naleving van lokaal organisatorisch en bestuursbeleid, terwijl ook het verminderen van de aanvalsoppervlakte

van de VPN server.

Gezien het feit dat VPN-servers openbare IP-adressen hebben die via het internet toegankelijk zijn, stelt de introductie van op geolocatie gebaseerde regels organisaties in staat om gebruikersverzoeken van specifieke geolocaties effectief te beperken, waardoor de kwetsbaarheid voor brute-geweldaanvallen wordt verminderd.

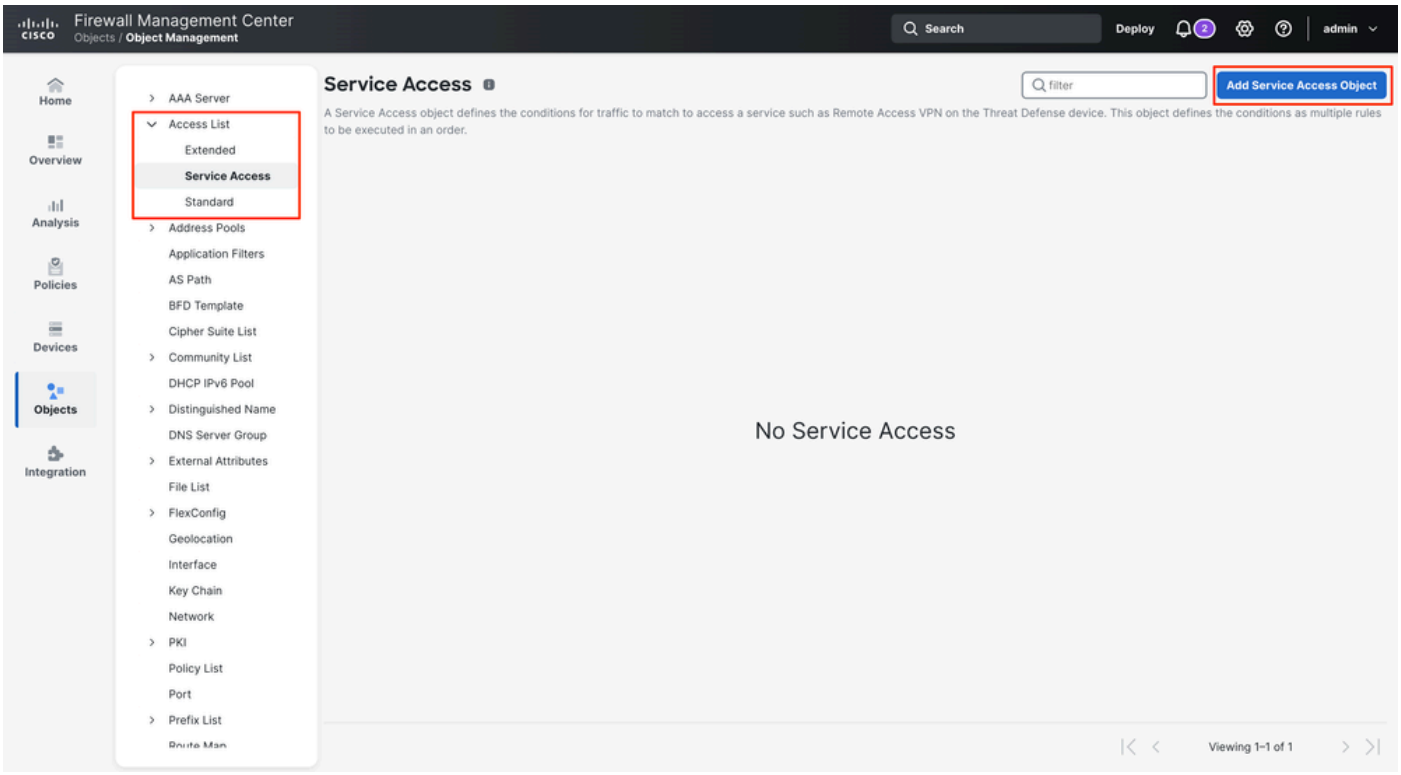


Configureren

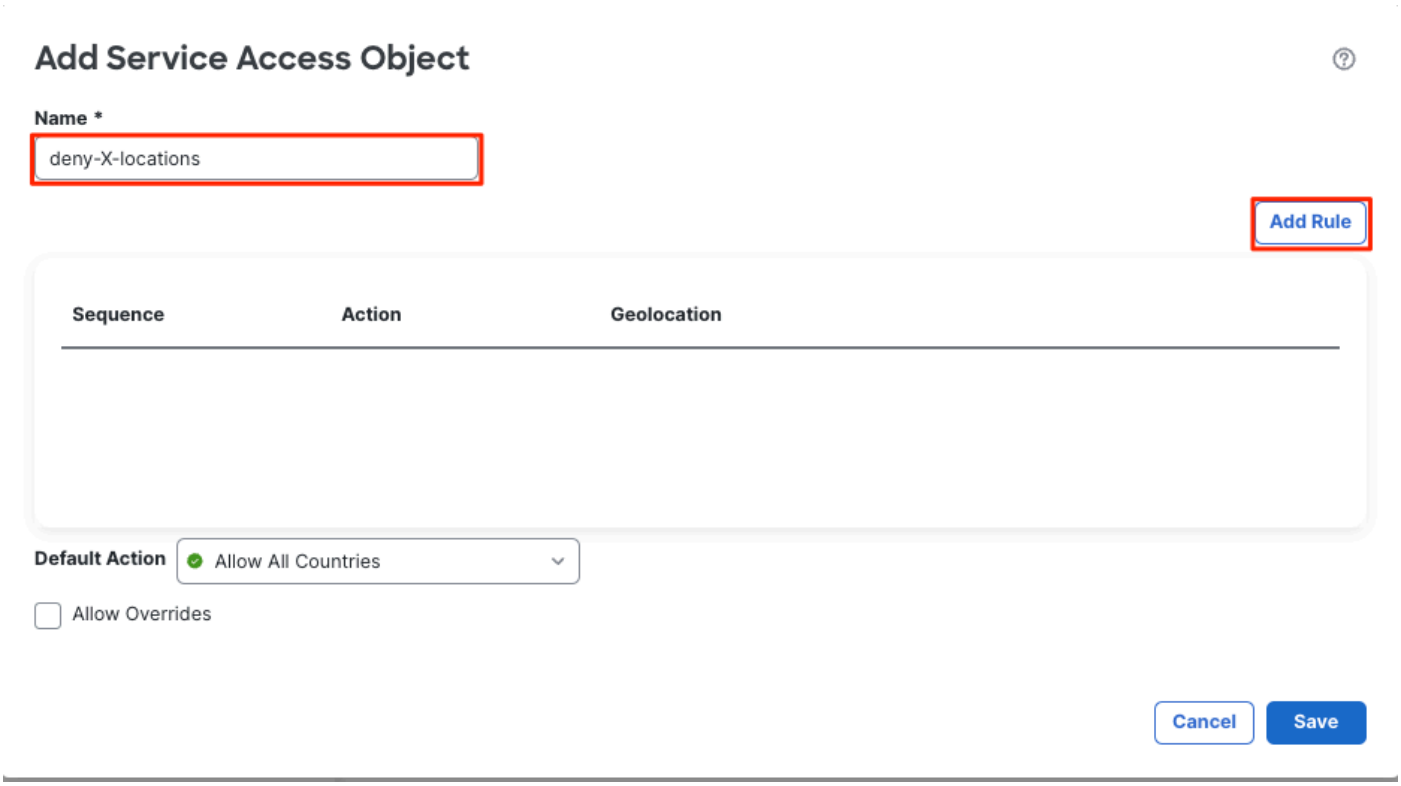
Stap 1. Maak een Service Access Object.

1. Log in op het Secure Firewall Management Center.

2. Navigeer naar Objecten > Objectbeheer > Toegangslijst > Servicetoegang en klik op Add Service Access Object.



3. Bepaal de regelnaam en klik vervolgens op Regel toevoegen.

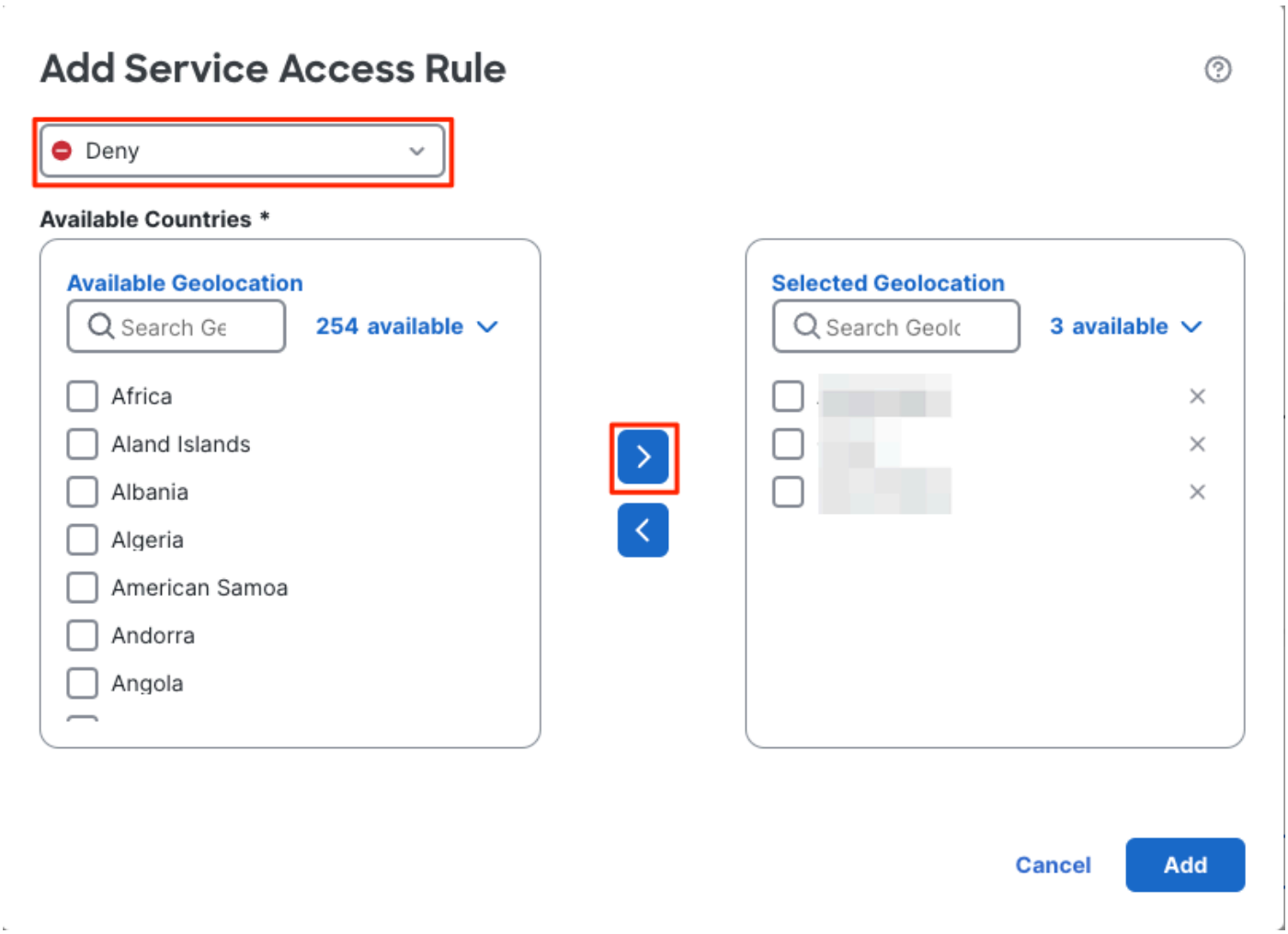


4. Configureer de Service Access Rule:

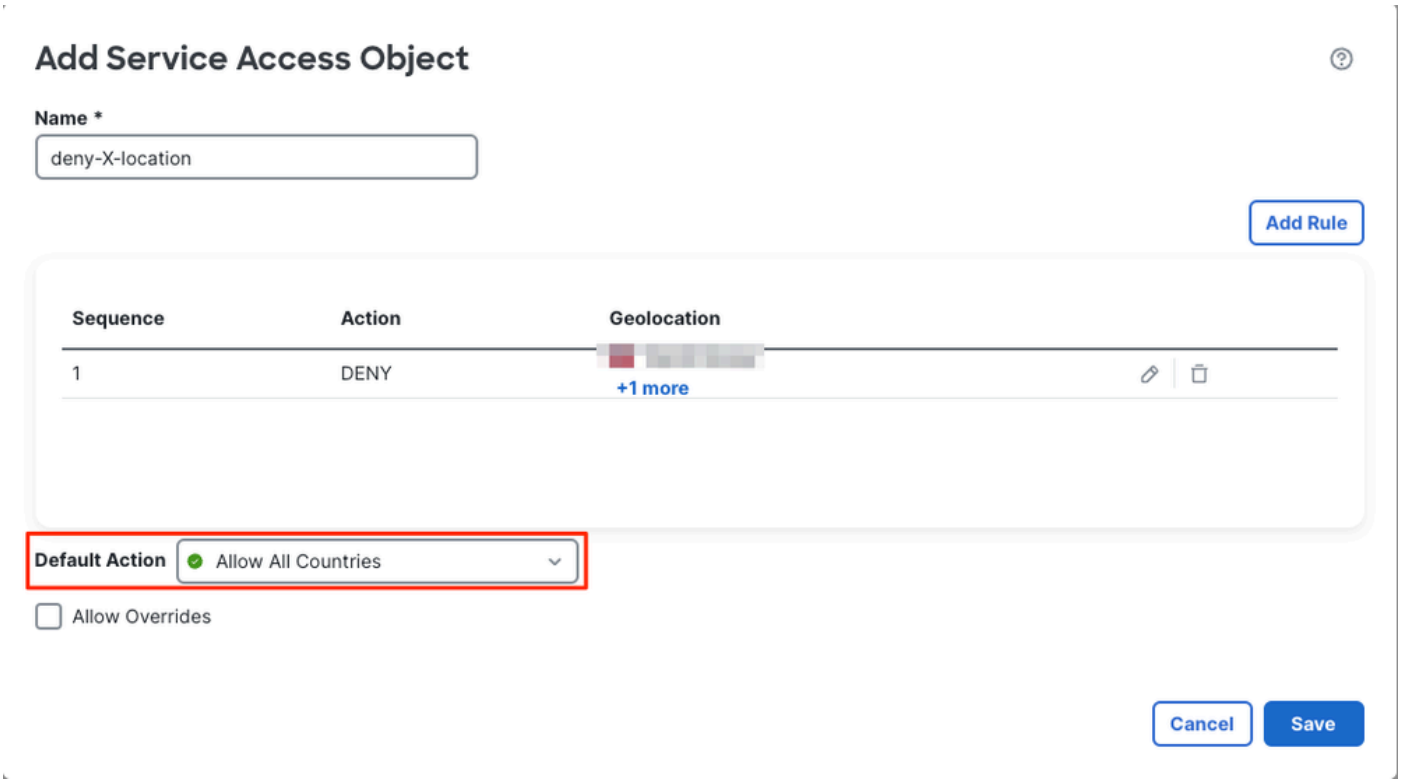
- Selecteer de actie van de regel: Toestaan of weigeren.
- Selecteer vanuit Beschikbare landen landen landen, continenten of door de gebruiker gedefinieerde geolocatie-objecten en verplaats deze naar de lijst Geselecteerde geolocatie.
- Klik op Add om de regel te maken.

Opmerking: In een dienstentoegangsobject kan een geolocatieobject (land, continent of aangepaste geolocatie) slechts in één regel worden gebruikt.

Opmerking: zorg ervoor dat u de toegangsregels voor services in de juiste volgorde configureert, aangezien deze regels niet opnieuw kunnen worden geordend.



5. Kies de standaardactie: Laat alle landen toe of ontken alle landen. Deze actie is van toepassing op verbindingen die niet voldoen aan een van de geconfigureerde Service Access Rules.

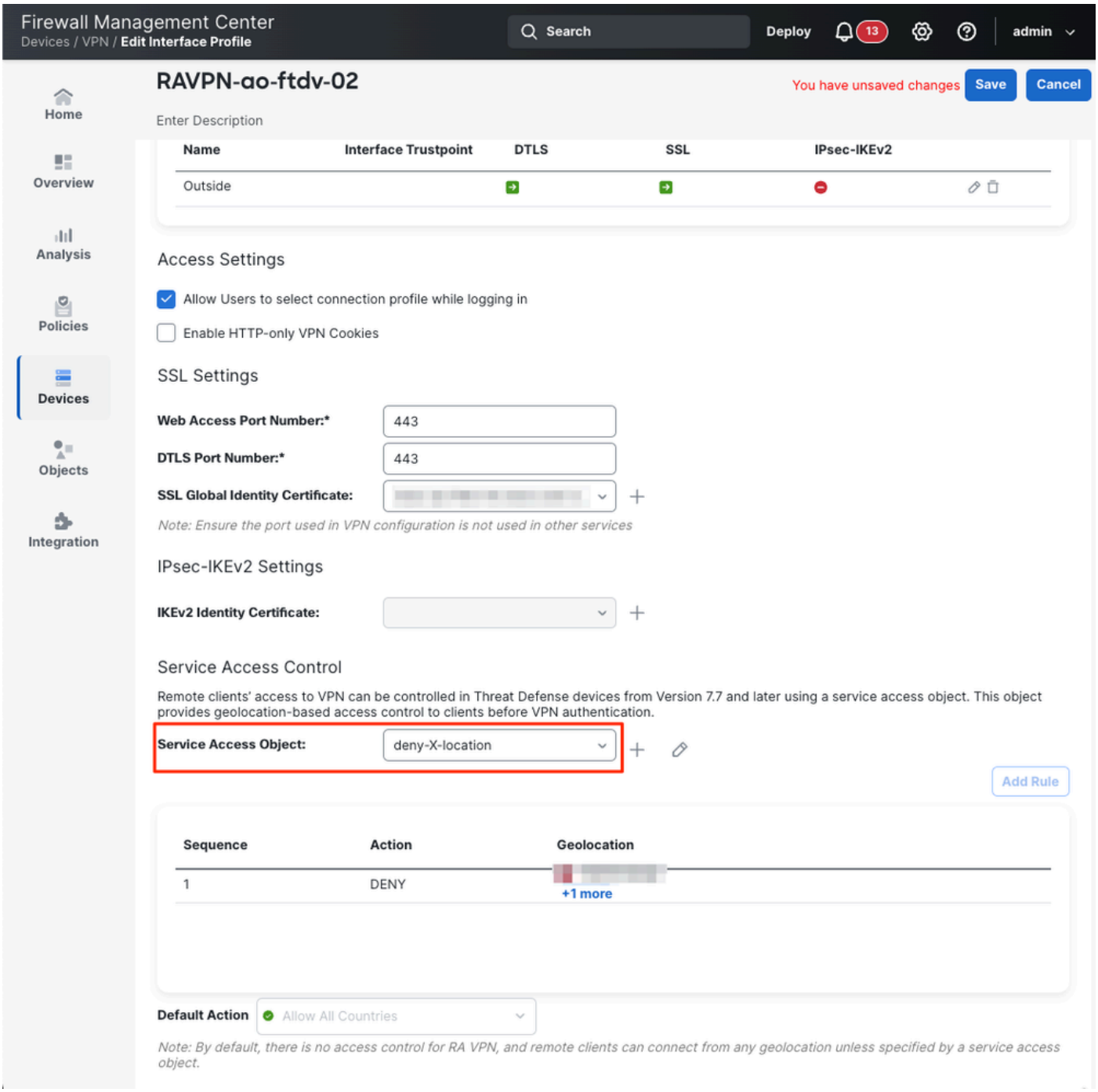


6. Klik op Opslaan.

Stap 2. Pas de configuratie van serviceobjecten toe in RAVPN.

1. Navigeer naar de RAVPN-configuratie in Apparaten > Externe toegang > RAVPN-configuratieobject > Access interface.

2. Selecteer in het gedeelte Service Access Control het Service Access Object dat u eerder hebt gemaakt.

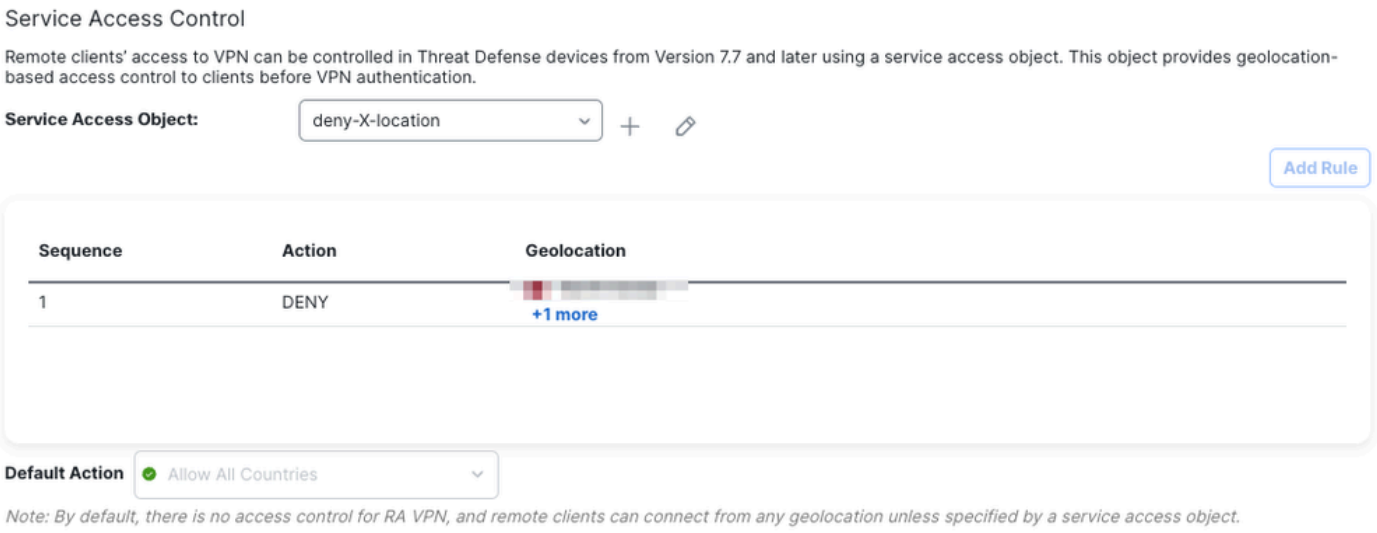


3. Het Service Access-object dat u hebt geselecteerd, geeft nu de samenvatting van de regels en de standaardactie weer. Controleer of dit klopt.

4. Sla de wijzigingen op en implementeer de configuratie.

Verifiëren

Zodra de configuratie is opgeslagen, worden de regels weergegeven in het gedeelte Service Access Control, zodat u kunt valideren welke groepen en landen zijn geblokkeerd of toegestaan.



Start de opdracht show in werking stelt-in-configuratie service-toegang om er zeker van te zijn dat de toegangsregels voor de service beschikbaar zijn op de FTD CLI.

<#root>

```
firepower#
```

show running-config service-access

```
service-access deny ra-ssl-client geolocation FMC_GEOLOCATION_146028889448_536980902
service-access permit ra-ssl-client geolocation any

firepower# show running-config object-group idFMC_GEOLOCATION_146028889448_536980902
object-group geolocation FMC_GEOLOCATION_146028889448_536980902
location "Country X"
location "Country Y"
```

Systeemlogs en bewaking

Secure Firewall introduceert nieuwe syslog-ID's om gebeurtenissen met betrekking tot RAVPN-verbindingen op te nemen die worden geblokkeerd door beleid op basis van geolocatie:

- 761031: Geeft aan wanneer een IKEv2-verbinding wordt geweigerd door een op geolocatie gebaseerd beleid. Deze syslog maakt deel uit van de bestaande VPN-logboekklasse.

%FTD-6-751031: Verboden IKEv2 externe toegangssessie voor faddr <client_ip><device_ip> door een op geo gebaseerde regel (geo=<country_name>, id=<country_code>)

- 751031: Geeft aan wanneer een SSL-verbinding wordt geweigerd door een op geolocatie gebaseerd beleid. Deze syslog maakt deel uit van de bestaande WebVPN logboekklasse.

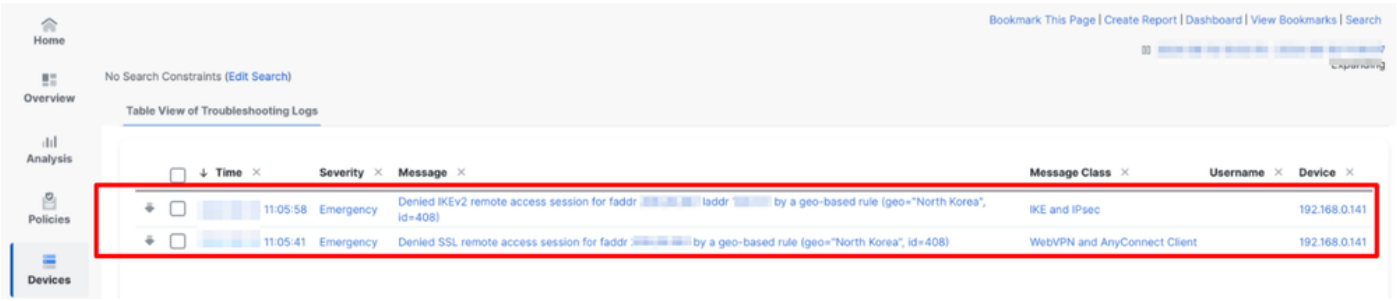
%FTD-6-716166: Verboden SSL externe toegangssessie voor faddr <client_ip> door een op geo gebaseerde regel (geo=<country_name>, id=<country_code>)

Opmerking: Het standaard prioriteitsniveau voor deze nieuwe syslogs is informatie wanneer deze is ingeschakeld vanuit de respectievelijke logboekklassen. U kunt deze syslog-ID's echter afzonderlijk inschakelen en de ernst ervan aanpassen.

Monitor geblokkeerde verbindingen

Als u geblokkeerde verbindingen wilt valideren, navigeert u naar Apparaten > Probleemoplossing > Logbestanden voor probleemoplossing. Hier worden logboeken weergegeven die betrekking hebben op geblokkeerde verbindingen, inclusief informatie over de regels die van invloed zijn op de verbinding en het type sessie.

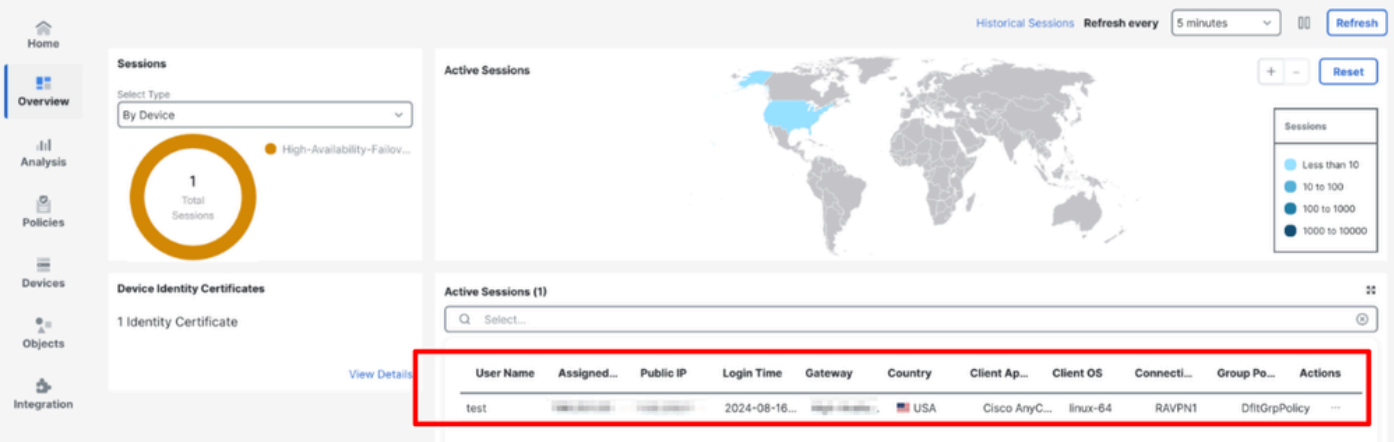
Opmerking: Syslog moet worden geconfigureerd om deze informatie in de logboeken voor probleemoplossing te verzamelen.



Monitorverbindingen toegestaan

De toegestane sessies worden bewaakt in Overzicht > Remote Access VPN-dashboard, waar sessieinformatie wordt weergegeven, inclusief het land van herkomst.

Opmerking: Alleen verbindingen van toegestane landen en gebruikers die verbinding mogen maken, worden op dit dashboard weergegeven. Aansluitingen die worden geweigerd, worden niet op dit dashboard weergegeven.



Problemen oplossen

Volg de volgende stappen voor het oplossen van problemen:

1. Controleer of de regels correct zijn geconfigureerd in het Service Access-object.
2. Controleer of een deny-syslog verschijnt in het gedeelte Problemen oplossen en logboeken wanneer een toegestane geolocatie een sessie vraagt.
3. Zorg ervoor dat de configuratie in het VCC overeenkomt met die in de FTD CLI.
4. Gebruik de volgende opdrachten om meer informatie te verzamelen die nuttig is voor probleemoplossing:

- geolocatie debuggen <1-25>
- show service-access
- toon dienst-toegang detail
- toon dienst-toegang interface
- toon de dienst-toegang plaats
- show service-access service
- geodb ipv4 locatie tonen <land> details
- geodb-tellers tonen
- geodb ipv4 [lookup <IP-adres>] tonen
- geodb ipv6 tonen

Gerelateerde informatie

- Voor extra hulp kunt u contact opnemen met TAC. Er is een geldig ondersteuningscontract vereist:Cisco's wereldwijde contactgegevens voor ondersteuning.
- U kunt hier ook de Cisco VPN-community bezoeken.

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.