Geolocatie-implementatiefout met detectie van bedreigingen ingeschakeld op FTD voor veilige firewall

Inhoud

uitgeven

Bij het configureren van een op geolocatie gebaseerde verkeersfiltering op een Cisco Secure Firewall FTD 3105 zijn verschillende problemen opgetreden:

- Geo-based Access Control Policy (ACP) en prefilterregels blokkeerden de pogingen van HTTPS Remote Access VPN (RA-VPN) om regio's te blokkeren voor de FTD-externe interface niet.
- Na het upgraden naar versie 7.7.11 kon de RA-VPN geo-based service-toegang niet worden geïmplementeerd toen Nederland of de Nederlandse Antillen landen in het beleid werden opgenomen.
- FMC-implementatie is mislukt bij 83% met deze foutmelding:

```
FMC >> object-group geolocation FMC_GEOLOCATION_184683596782_116848397
FMC >> location "Netherlands"
device >> [error] :
location "Netherlands"
^
ERROR: % Invalid input detected at '^' marker.
Config Error -- location "Netherlands"
```

milieu

- Cisco Secure Firewall Firepower Threat Defense (FTD) 3105 beheerd door FMC
- Bijgewerkte softwareversie: 7.7.11-1061

- RA-VPN-configuratie waarvoor toegangsbeperkingen per land zijn vereist

resolutie

De oplossing omvatte meerdere stappen om een werkend toegangsbeheer op basis van geolocatie correct te valideren. Daarnaast werd een beperking met Threat Detection ingeschakeld ontdekt, wat leidt tot nieuwe richtlijnen met betrekking tot verkeer matching gedrag.

1: Upgrade zowel FMC als FTD naar versie 7.7.11-1061 om RA-VPN geo-gebaseerde servicetoegangsfunctionaliteit in te schakelen, omdat deze functie alleen wordt ondersteund vanaf versie 7.7.0 en hoger.

2: Configureer RA-VPN geo-based service access volgens Cisco documentatie en koppel het aan het RA-VPN beleid.

3: Als u de implementatiefout wilt oplossen die het gevolg is van Cisco-bug-ID CSCwq15499 bij het toevoegen van specifieke landen zoals Nederland of de Nederlandse Antillen, past u deze oplossing toe:

1. Maak een leeg RA-VPN-servicetoegangsobject zonder landen geconfigureerd.
2. Pas het lege servicetoegangsobject toe op het RA-VPN-beleid en implementeer het succesvol.
3. Bewerk hetzelfde servicetoegangsobject en voeg de vereiste landregels toe.
4. Implementeer de configuratie opnieuw - de implementatie is nu geslaagd en de geolocatiefiltering is actief.

4: Controleer of de implementatie met succes is voltooid en of de RA-VPN-toegang en -logs de beoogde landbeperkingen weerspiegelen. Controleer het systeem om ervoor te zorgen dat geolocatiebeperkingen functioneren zoals verwacht.

5: Bepaal of een bedreigingsdetectiefunctie al is ingeschakeld op de FTD die overeenkomt met het verkeer voordat deze het toegangsbeleid kan bereiken. Dergelijke configuraties zorgen ervoor dat geolocatieregels worden overgeslagen, omdat Threat Detection het overneemt voordat het beleid wordt toegepast.

<#root>

```
device# show run threat-detection
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

threat-detection service invalid-vpn-access
threat-detection service remote-access-authentication hold-down 1440 threshold 5
threat-detection service remote-access-client-initiations hold-down 1440 threshold 5
```

6: Correleer alle syslog-ID's met betrekking tot Threat Detection-overeenkomsten en -schuwingen om te bevestigen dat het verkeer de Threat Detection raakt in plaats van de geolocatie.

- %FTD-4-401002: Shun toegevoegd: IP_address IP_address poort
- %FTD-4-401003: Shun verwijderd: IP_adres
- %FTD-4-401004: Afgewend pakket: IP_adres ==> IP_adres op interface_naam
- %FTD-4-733102: Threat-detection voegt host toe aan lijst met vermijdingen
- %FTD-4-733103: Dreigingsdetectie verwijdert host uit lijst met schuwingen
- %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] Peer[peer-ip]: foutdrempel van waarde overschreden: shun toevoegen aan interface. SSL: RA overmatige verzoeken voor clientinitiatie.
- %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] Peer[peer-ip]: drempelwaarde voor mislukking overschreden: shun toevoegen aan interface. IKEv2: RA_excessive_client_initiation_requests

```
<164>Feb 26 2026 23:05:45: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:07:36: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:12:25: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:00:00: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
<164>Feb 26 2026 23:00:01: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
<164>Feb 26 2026 23:00:01: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
---
device# show shun
```

Oorzaak

De ondervonden problemen hebben twee verschillende oorzaken:

- Geolocation Rule-Matching Limitation: RA-VPN geo-gebaseerde toegangscontrole wordt alleen ondersteund vanaf softwareversie 7.7.0 en hoger. Bovendien kan de geconfigureerde RAVPN Threat Detection op verkeer reageren, waardoor het niet kan matchen met op geo gebaseerde regels.
- Cisco bug ID CSCwq15499: Op versie 7.7.11 treden implementatiefouten op bij het toevoegen van bepaalde landen aan het RA-VPN geo-based servicetoegangsbeleid vanwege een bekende softwarebug in het RA-VPN geo-servicetoegangsmechanisme.

Verwante inhoud

- Cisco Technical Support en downloads

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.