Geolocation Deploy Failure Behaviour mit aktivierter Bedrohungserkennung auf Secure Firewall FTD

Inhalt

Problem

Bei dem Versuch, eine standortbasierte Datenverkehrsfilterung auf einer Cisco Secure Firewall FTD 3105 zu konfigurieren, traten mehrere Probleme auf:

- Geobasierte Zugriffskontrollrichtlinien (ACP) und Vorfilterregeln blockierten keine HTTPS Remote Access VPN (RA-VPN)-Verbindungsversuche, um Regionen an die externe FTD-Schnittstelle zu blockieren.
- Nach dem Upgrade auf Version 7.7.11 konnte die Konfiguration des geobasierten RA-VPN-Servicezugriffs nicht bereitgestellt werden, wenn die Länder der Niederländischen oder Niederländischen Antillen in die Richtlinie aufgenommen wurden.
- Fehler bei der FMC-Bereitstellung bei 83 % mit folgender Fehlermeldung:

```
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"
```

Umwelt

- Cisco Secure Firewall FirePOWER Threat Defense (FTD) 3105, verwaltet durch FMC
- Aktualisierte Softwareversion: 7.7.11-1061

- RA-VPN-Konfiguration, die landesbasierte Zugriffsbeschränkungen erfordert

Auflösung

Die Lösung umfasste mehrere Schritte zur ordnungsgemäßen Validierung einer funktionierenden standortbasierten Zugriffskontrolle. Darüber hinaus wurde eine Beschränkung bei aktivierter Bedrohungserkennung erkannt, die zu neuen Hinweisen hinsichtlich des Verhaltens beim Abgleich von Datenverkehr führte.

1: Aktualisieren Sie sowohl FMC als auch FTD auf Version 7.7.11-1061, um die RA-VPN-Funktion für den geobasierten Servicezugriff zu aktivieren, da diese Funktion nur ab Version 7.7.0 unterstützt wird.

2: Konfigurieren Sie den geobasierten RA-VPN-Servicezugriff gemäß der Cisco Dokumentation, und ordnen Sie ihn der RA-VPN-Richtlinie zu.

3: Um den Bereitstellungsfehler aufgrund der Cisco Bug-ID CSCwq15499 beim Hinzufügen bestimmter Länder wie den Niederländischen oder Niederländischen Antillen zu beheben, wenden Sie diese Problemumgehung an:

1. Erstellen Sie ein leeres RA-VPN-Service-Zugriffsobjekt ohne konfigurierte Länder.
2. Wenden Sie das leere Servicezugriffsobjekt auf die RA-VPN-Richtlinie an, und stellen Sie es erfolgreich bereit.
3. Bearbeiten Sie dasselbe Service-Zugriffsobjekt, und fügen Sie die erforderlichen Länderregeln hinzu.
4. Stellen Sie die Konfiguration erneut bereit. Die Bereitstellung ist jetzt erfolgreich, und die Geolokalisierungsfilterung ist aktiviert.

4: Überprüfen Sie, ob die Bereitstellung erfolgreich abgeschlossen wurde und ob der RA-VPN-Zugriff und die RA-VPN-Protokolle den landesspezifischen Einschränkungen entsprechen. Überwachen Sie das System, um sicherzustellen, dass geografische Standortbeschränkungen wie erwartet funktionieren.

5: Prüfen Sie, ob auf dem FTD bereits eine Funktion zur Erkennung von Sicherheitsrisiken aktiviert ist, die den Datenverkehr vergleicht, bevor er die Zugriffsrichtlinie erreichen kann. Bei solchen Konfigurationen werden Geolokalisierungsregeln übersprungen, da die Erkennung von Sicherheitsrisiken vor der Anwendung der Richtlinie übernommen wird.

<#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: Korrelieren Sie alle Syslog-IDs, die sich auf Übereinstimmungen mit der Bedrohungserkennung beziehen, und Shuns, um zu bestätigen, dass der Datenverkehr die Bedrohungserkennung anstatt der Standortbestimmung erreicht.

- %FTD-4-401002: Shun fügte hinzu: IP_Adresse IP-Adresse Port-Port
- %FTD-4-401003: Shun gelöscht: IP-Adresse
- %FTD-4-401004: Shunned Packet: IP_Adresse ==> IP_Adresse auf Schnittstellenname
- %FTD-4-733102: Erkennung von Sicherheitsrisiken fügt Host zu Shun-Liste hinzu
- %FTD-4-733103: Die Erkennung von Sicherheitsrisiken entfernt den Host aus der Shun-Liste.
- %FTD-4-733201: Bedrohungserkennung: Service[remote-access-client-initiations] Peer[Peer-ip]: Fehlerschwellenwert überschritten: Hinzufügen von Shun zur Schnittstellenschnittstelle. SSL: Übermäßige RA-Anfragen zur Client-Initiierung
- %FTD-4-733201: Bedrohungserkennung: Service[remote-access-client-initiations] Peer[Peer-ip]: Fehlerschwelle des Schwellenwerts überschritten: Hinzufügen von Shun zur Schnittstellenschnittstelle. 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
```

Ursache

Die aufgetretenen Probleme haben zwei unterschiedliche Ursachen:

- Begrenzung der Übereinstimmung von Geolokalisierungs-Regeln: RA-VPN Geo-basierte Zugriffskontrolle wird nur ab Softwareversion 7.7.0 und höher unterstützt. Darüber hinaus kann die konfigurierte RAVPN-Bedrohungserkennung auf den Datenverkehr einwirken, sodass keine Übereinstimmung mit geobasierten Regeln möglich ist.
- Cisco Bug-ID CSCwq15499: In Version 7.7.11 treten Bereitstellungsfehler auf, wenn bestimmte Länder aufgrund eines bekannten Softwarefehlers im RA-VPN-Mechanismus für die Verarbeitung des Zugriffs auf den Geo-Service zu RA-VPN-Richtlinien hinzugefügt werden.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

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.