Défaillance du déploiement de géolocalisation avec détection des menaces activée sur le pare-feu FTD sécurisé

Table des matières

Problème

Lors de la configuration du filtrage du trafic basé sur la géolocalisation sur un pare-feu sécurisé Cisco FTD 3105, plusieurs problèmes ont été rencontrés :

- Les règles de préfiltre et de politique de contrôle d'accès basée sur la zone géographique n'ont pas bloqué les tentatives de connexion VPN d'accès à distance HTTPS (RA-VPN) bloquant les régions vers l'interface externe FTD.
- Après la mise à niveau vers la version 7.7.11, la configuration de l'accès au service RA-VPN basé sur la géolocalisation n'a pas pu être déployée lorsque les pays des Pays-Bas ou des Antilles néerlandaises ont été inclus dans la stratégie.
- Échec du déploiement FMC à 83 % avec le message d'erreur suivant :

```
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"
```

Environnement

- Cisco Secure Firewall Firepower Threat Defense (FTD) 3105 géré par FMC
- Version logicielle mise à niveau : 7.7.11-1061

- Configuration RA-VPN nécessitant des restrictions d'accès basées sur le pays

Résolution

La résolution impliquait plusieurs étapes pour valider correctement un contrôle d'accès basé sur la géolocalisation. En outre, une limitation avec la détection des menaces activée a été découverte, ce qui a conduit à de nouvelles indications concernant le comportement de correspondance du trafic.

1: Mettez à niveau FMC et FTD vers la version 7.7.11-1061 pour activer la fonctionnalité d'accès au service RA-VPN basé sur la géo, car cette fonctionnalité n'est prise en charge qu'à partir de la version 7.7.0 et ultérieure.

2: Configurez l'accès au service RA-VPN basé sur la géolocalisation conformément à la documentation Cisco et associez-le à la politique RA-VPN.

3: Pour résoudre l'échec de déploiement dû au bogue Cisco ID CSCwq15499 lors de l'ajout de pays spécifiques tels que les Pays-Bas ou les Antilles néerlandaises, appliquez cette solution de contournement :

1. Créez un objet d'accès au service RA-VPN vide sans aucun pays configuré.
2. Appliquez l'objet d'accès au service vide à la stratégie RA-VPN et déployez-le avec succès.
3. Modifiez le même objet d'accès au service et ajoutez les règles de pays requises.
4. Redéployez la configuration : le déploiement réussit et le filtrage de géolocalisation est actif.

4: Vérifiez que le déploiement s'est terminé correctement et que l'accès et les journaux RA-VPN reflètent les restrictions de pays prévues. Surveillez le système pour vous assurer que les restrictions de géolocalisation fonctionnent comme prévu.

5: Déterminez si une fonctionnalité de détection des menaces est déjà activée sur le FTD qui correspondrait au trafic avant qu'il puisse atteindre la stratégie d'accès. De telles configurations entraînent l'abandon des règles de géolocalisation, car la détection des menaces prend le relais avant l'application de la stratégie.

<#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: Corrélez les ID Syslog associés aux correspondances et aux shuns de détection des menaces pour confirmer que le trafic atteint la détection des menaces au lieu de la géolocalisation.

- %FTD-4-401002 : Shun a ajouté : IP_address IP_address port port
- %FTD-4-401003 : Shun supprimé : Adresse_IP
- %FTD-4-401004 : Paquet ignoré : Adresse_IP ==> Adresse_IP sur l'interface nom_interface
- %FTD-4-733102 : La détection des menaces ajoute l'hôte à la liste de désactivation
- %FTD-4-733103 : La détection des menaces supprime l'hôte hôte de la liste de désactivation
- %FTD-4-733201 : Détection des menaces : Service[remote-access-client-initiations] Peer[peer-ip] : seuil de défaillance de la valeur dépassé : ajout de shun à l'interface. SSL : Demandes d'initiation client excessives RA.
- %FTD-4-733201 : Détection des menaces : Service[remote-access-client-initiations] Peer[peer-ip] : dépassement du seuil de défaillance de threshold-value : ajout de shun à l'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
```

Motif

Les problèmes rencontrés ont deux causes profondes distinctes :

- Limitation de correspondance des règles de géolocalisation : Le contrôle d'accès géo-basé RA-VPN est uniquement pris en charge à partir de la version 7.7.0 du logiciel et des versions ultérieures. En outre, la détection de menaces RAVPN configurée peut agir sur le trafic, ce qui l'empêche de correspondre aux règles basées sur la géographie.
- ID de bogue Cisco CSCwq15499 : Dans la version 7.7.11, des échecs de déploiement se produisent lors de l'ajout de certains pays aux politiques d'accès au service géo-basé RA-VPN en raison d'un bogue logiciel connu dans le mécanisme de gestion d'accès au service géo-basé RA-VPN.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.