セキュアファイアウォールFTDで脅威検出を有効にした場合の位置情報の展開の失敗動作

内容

お問い合わせ内容

Cisco Secure Firewall FTD 3105で位置情報ベースのトラフィックフィルタリングを設定しようとすると、次のような問題が発生します。

- Geo-based Access Control Policy(ACP)とプレフィルタルールがHTTPSリモートアクセスVPN(RA-VPN)接続の試行をブロックせず、FTD外部インターフェイスへの領域をブロックしました。
- バージョン7.7.11へのアップグレード後、オランダまたはオランダ領アンティル諸島の国がポリシーに含まれていると、RA-VPN地域ベースサービスアクセスの設定を導入できませんでした。
- FMCの導入が83 %で失敗し、次のエラーメッセージが表示されました。

```
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"
```

環境

- FMCによって管理されるCisco Secure Firewall Firepower Threat Defense(FTD)3105
- アップグレードされたソフトウェアバージョン：7.7.11-1061
- 国ベースのアクセス制限を必要とするRA-VPN設定

解決策

この問題を解決するには、地理的な場所に基づく有効なアクセスコントロールを適切に検証するための複数の手順が必要でした。さらに、脅威検出を有効にするための制限が見つかったため、トラフィック照合動作に関する新しいガイダンスが提供されました。

1:RA-VPNのGeo-Based Service Access機能を有効にするには、FMCとFTDの両方をバージョン7.7.11-1061にアップグレードします。この機能はバージョン7.7.0以降でのみサポートされています。

2：シスコのドキュメントに従ってRA-VPN地理的ベースサービスアクセスを設定し、RA-VPNポリシーに関連付けます。

3:NetherlandsやNetherlands Antillesなどの特定の国を追加する際に、Cisco Bug ID CSCwq15499が原因で発生する導入エラーを解決するには、次の回避策を適用します。

1. 国が設定されていない空のRA-VPNサービスアクセスオブジェクトを作成します。
2. ブランクのサービスアクセスオブジェクトをRA-VPNポリシーに適用し、正常に展開します。
3. 同じサービスアクセスオブジェクトを編集し、必要な国ルールを追加します。
4. 構成を再度展開します。展開が成功し、位置情報フィルタリングがアクティブになります。

4：展開が正常に完了し、RA-VPNアクセスおよびログに目的の国の制限が反映されていることを確認します。システムを監視し、地理的位置の制限が期待どおりに機能していることを確認します。

5：アクセスポリシーに到達する前にトラフィックに一致する脅威検出機能がFTDですでに有効になっているかどうかを確認します。このような設定では、ポリシー適用前に脅威検出が引き継がれるため、位置情報ルールがスキップされます。

<#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：脅威検出の一致と回避に関連するsyslog IDを関連付け、トラフィックが地理位置情報ではなく脅威検出に到達していることを確認します。

- %FTD-4-401002:Shun added: IP_address IP_address port port
- %FTD-4-401003:Shun deleted: IP_address
- %FTD-4-401004：回避パケット：IP_address ==> IP_address on interface interface_name
- %FTD-4-733102：脅威検出が排除リストにホストホストを追加
- %FTD-4-733103：脅威検出は排除リストからホストホストを削除
- %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] Peer[peer-ip]: failure threshold of value exceeded: adding shun to interface.SSL:RAのクライアント開始要求が過剰です。
- %FTD-4-733201：脅威検出： Service[remote-access-client-initiations] Peer[peer-ip]：しきい値の障害しきい値を超えました：インターフェイスにshunを追加しています。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
```

原因

発生する問題には、2つの根本的な原因があります。

- 位置情報ルールマッチングの制限： RA-VPNの位置情報ベースアクセスコントロールは、ソフトウェアバージョン7.7.0以降でのみサポートされています。また、設定済みのRAVPN脅威検出はトラフィックに対して機能するため、地理ベースのルールとの照合が行えなくなります。
- Cisco Bug ID CSCwq15499:バージョン7.7.11では、RA-VPN地域サービスアクセス処理メカニズムの既知のソフトウェアバグが原因で、特定の国をRA-VPN地域ベースサービスアクセスポリシーに追加するときに展開エラーが発生します。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。