着信および発信トラフィックフィルタリング用のFTDでの位置情報ベースのトラフィックブロッキングの設定

内容

お問い合わせ内容

- Cisco Secure Firewall Threat Defense(FTD)の位置情報に基づいてトラフィックをブロックする最適な方法を説明してください。これは、リージョンから発信されるトラフィックと、リージョンを宛先とするトラフィックの両方に対して行われます。
- 着信トラフィックフィルタリングと発信トラフィックフィルタリングに別個のアクセスコントロールルールが必要かどうか、およびアクセスコントロールルールのNetworksタブのGeolocationタブで位置情報エントリがすでに使用可能なときに追加の位置情報オブジェクトを作成する必要があるかどうかについて、疑問が生じます。

環境

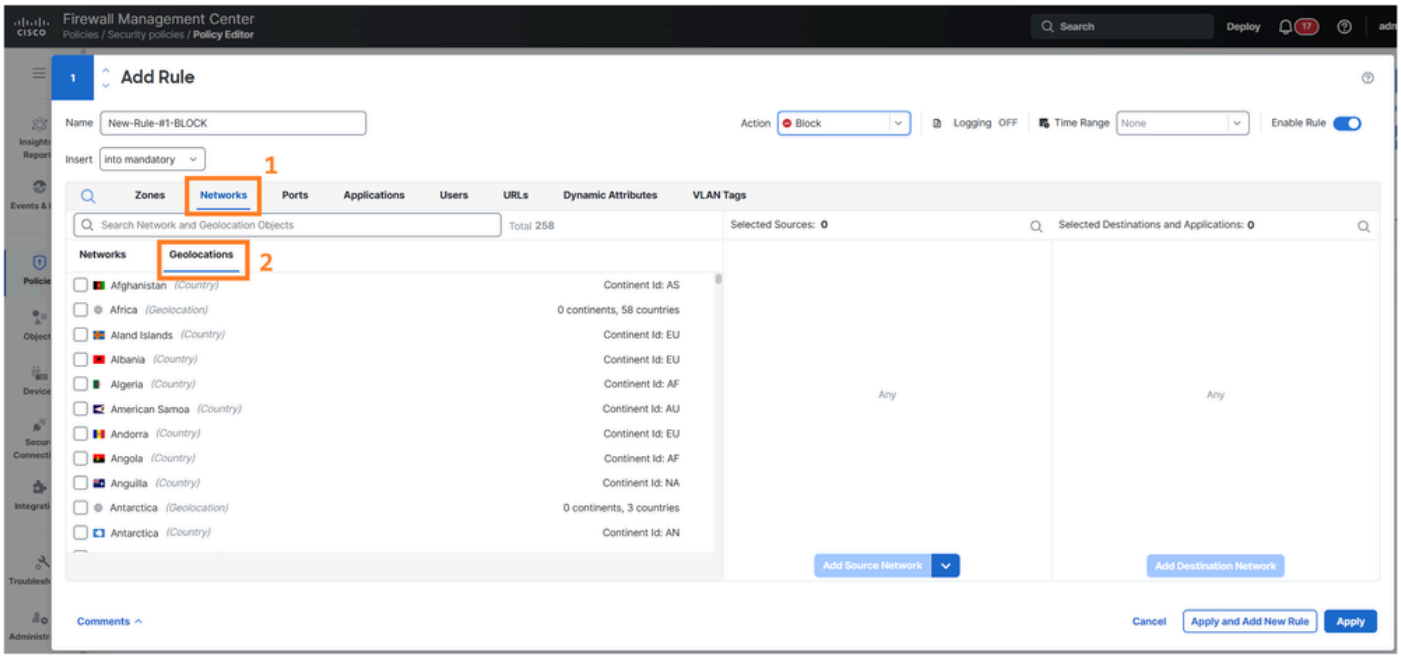
- FTDソフトウェアバージョン7.1他のソフトウェアバージョンも該当します。
- Cisco Secure Firewall Management Center(FMC)ソフトウェアバージョン7.1他のソフトウェアバージョンも該当します。

解決策

Cisco FTDでの位置情報ベースのトラフィックフィルタリングは、FMCユーザインターフェイス(UI)のAccess Control Policy Ruleセクションにあ るNetworksタブで使用可能な既存の位置情報の機能を使用して、効果的に管理できます。 設定方法は、トラフィックの方向とポリシー要件によって異なります。

位置情報の設定へのアクセス

FMCのUIで、Policies > Security policies > Policy Editorに移動し、ルールを編集して、Networks > Geolocations タブを選択します。このセクションで使用可能な既存の位置情報エントリは、個別の位置情報オブジェクトを必要とせずに、アクセスコントロールポリシーの作成に直接使用できます。



ルール作成戦略

ルール作成のアプローチは、トラフィックの方向性とポリシーの目的によって異なります。

特定の位置情報からの着信トラフィックをブロックするため

特定の地域から発信された送信元トラフィックを識別するアクセスコントロールルールを作成し、ブロックアクションを適用します。ポリシーを適切に適用するには、これらのルールをルールの順序に適切に配置する必要があります。

特定の位置情報への発信トラフィックを制御するため

特定の地理的領域に向けられた宛先トラフィックを識別するアクセスコントロールルールを設定します。セキュリティポリシーに応じて、これらの宛先へのトラフィックを許可またはブロックするように設定できます。

個別のルール要件

双方向の位置情報フィルタリングを実装する際には、次の理由から、個別のアクセスコントロールルールが必要です。

- 着信フィルタリングでは、発信元の位置情報の属性を評価するルールが必要です。
- アウトバウンドフィルタリングでは、宛先の位置情報の属性を評価するルールが必要です。
- トラフィックの方向性によって、アクセスコントロールエンジンで評価される位置情報フィールド（送信元または宛先）が決まります。

具体的なルール設定は、ネットワークトポロジ、セキュリティ要件、および地域ごとに必要なトラフィックフロー制御の目的によって異なります。

原因

明確にする必要があるのは、トラフィックの方向に基づいて異なるルールタイプと設定が必要になる、位置情報ベースのアクセスコントロールの実装が複雑であるためです。セキュリティポリシーのアクセスコントロールルールのNetworksタブで既存の位置情報エントリを使用できることで、ポリシーの実装に追加のオブジェクト作成が必要かどうかについて混乱が生じる可能性があります。

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。