Secure Firewall Threat Defenseでのリモートアクセス VPNの位置情報ベースポリシーの設定

内容

はじめに

このドキュメントでは、Secure Firewall Threat Defense(FTD)の特定の位置情報に基づいてRAVPN接続を許可または拒否するプロセスについて説明します。

前提条件

要件および制約事項

次の項目に関する知識があることが推奨されます。

- セキュアファイアウォール管理センター(FMC)
- リモートアクセスVPN(RAVPN)
- 基本的な位置情報の設定

位置情報ベースポリシーの現在の要件と制限事項は次のとおりです。

- FTDバージョン7.7.0以降でのみサポートされ、FMCバージョン7.7.0以降で管理されます。
- Secure Firewall Device Manager(FDM)で管理されるFTDではサポートされません。
- クラスタモードではサポートされない

- 位置情報ベースの未分類のIPアドレスは、地理的な発信元によって分類されません。これらについては、FMCがデフォルトのサービスアクセスポリシーアクションを適用します。
- 位置情報ベースのサービスアクセスポリシーはWebLaunchページには適用されないため、制限なくセキュアクライアントをダウンロードできます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Secure Firewallバージョン7.7.0
- Secure Firewall Management Center(FMC)バージョン7.7.0

この機能の詳細については、『Cisco Secure Firewall Management Center 7.7デバイスコンフィギュレーションガイド』の「位置情報に基づいたリモートユーザのVPNアクセスの管理」セクションを参照してください。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

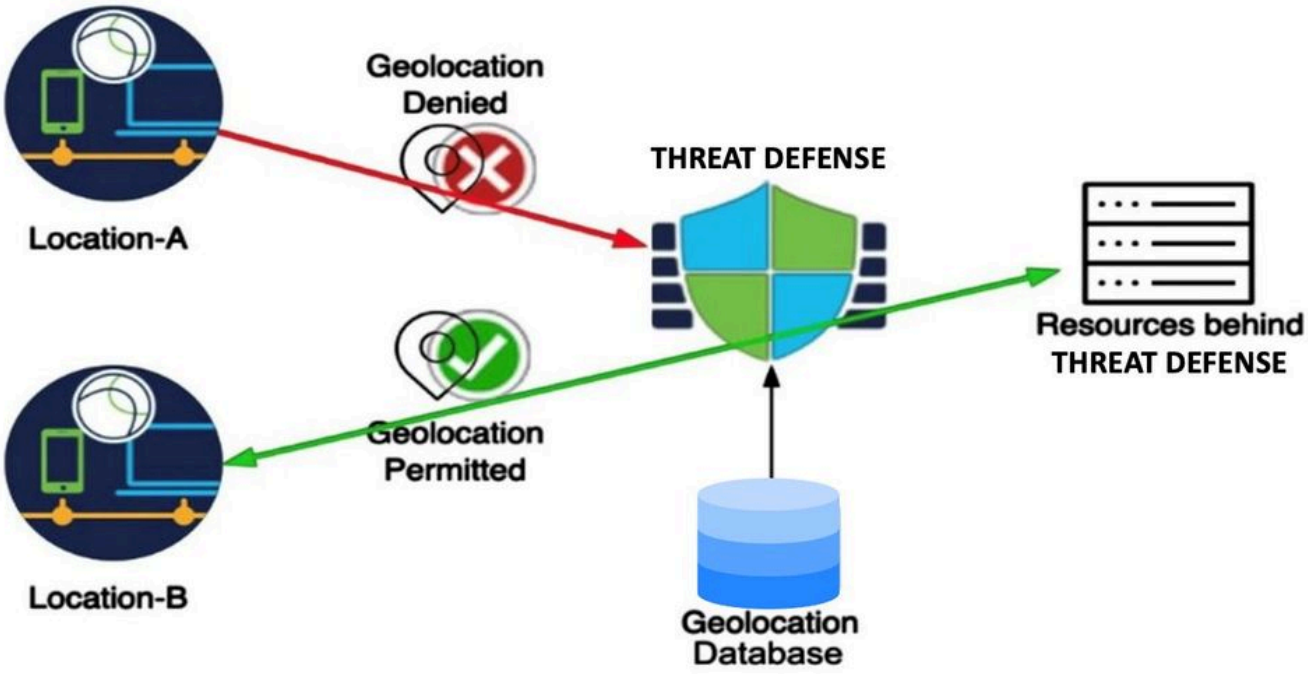
背景説明

位置情報ベースのアクセスポリシーは、今日のネットワークセキュリティに大きな価値をもたらし、トラフィックを地理的な発信元に基づいてブロックできます。従来、組織は、ファイアウォールを通過する一般的なネットワークトラフィックに対してトラフィックアクセスポリシーを定義できました。この機能の導入により、リモートアクセスVPNセッション要求に位置情報ベースのアクセス制御を適用できるようになりました。

この機能には、次のような利点があります。

- 位置情報ベースのルール：お客様は、国や大陸などの特定の位置情報に基づいてRAVPN要求を許可または拒否するルールを作成できます。これにより、地理的な場所によるVPNセッションの開始を正確に制御できます。
- 事前認証ブロック：これらのルールで拒否アクションとして識別されるセッションは、認証前にブロックされ、セキュリティの目的でこれらの試行が適切にログに記録されます。このプリエンプティブアクションは、不正アクセスの試みを軽減するのに役立ちます。
- コンプライアンスとセキュリティ：この機能は、ローカルの組織およびガバナンスポリシーの遵守を保証すると同時に、VPNサーバの攻撃対象領域を削減します。

VPNサーバがインターネット経由でアクセス可能なパブリックIPアドレスを持つことを前提として、位置情報ベースのルールを導入することで、組織は特定の位置情報からのユーザ要求を効果的に制限し、総当たり攻撃に対する脆弱性を軽減できます。

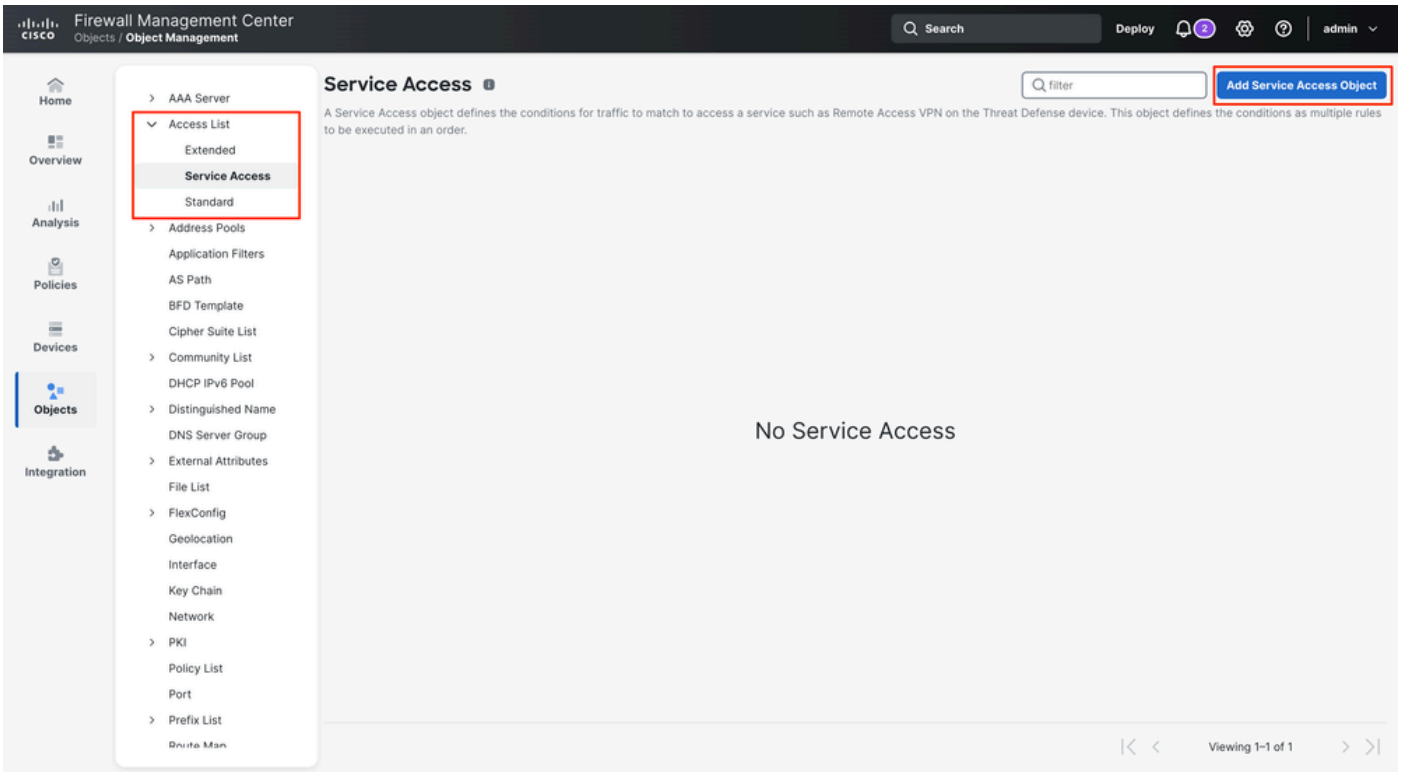


設定

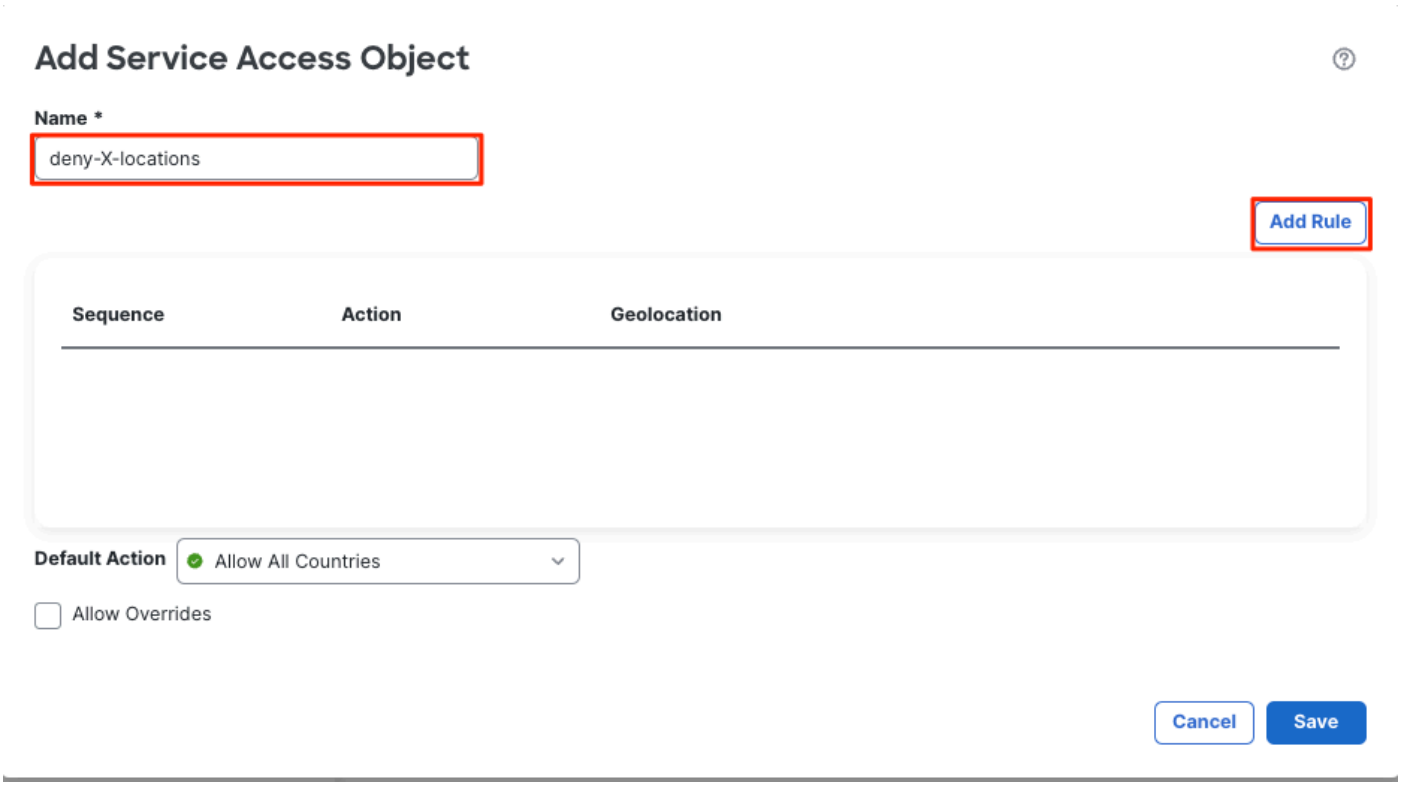
ステップ 1：サービスアクセスオブジェクトの作成

1. セキュアファイアウォール管理センターにログインします。

2. Objects > Object Management > Access List > Service Accessの順に移動し、Add Service Access Objectをクリックします。



3. ルール名を定義し、Add Ruleをクリックします。

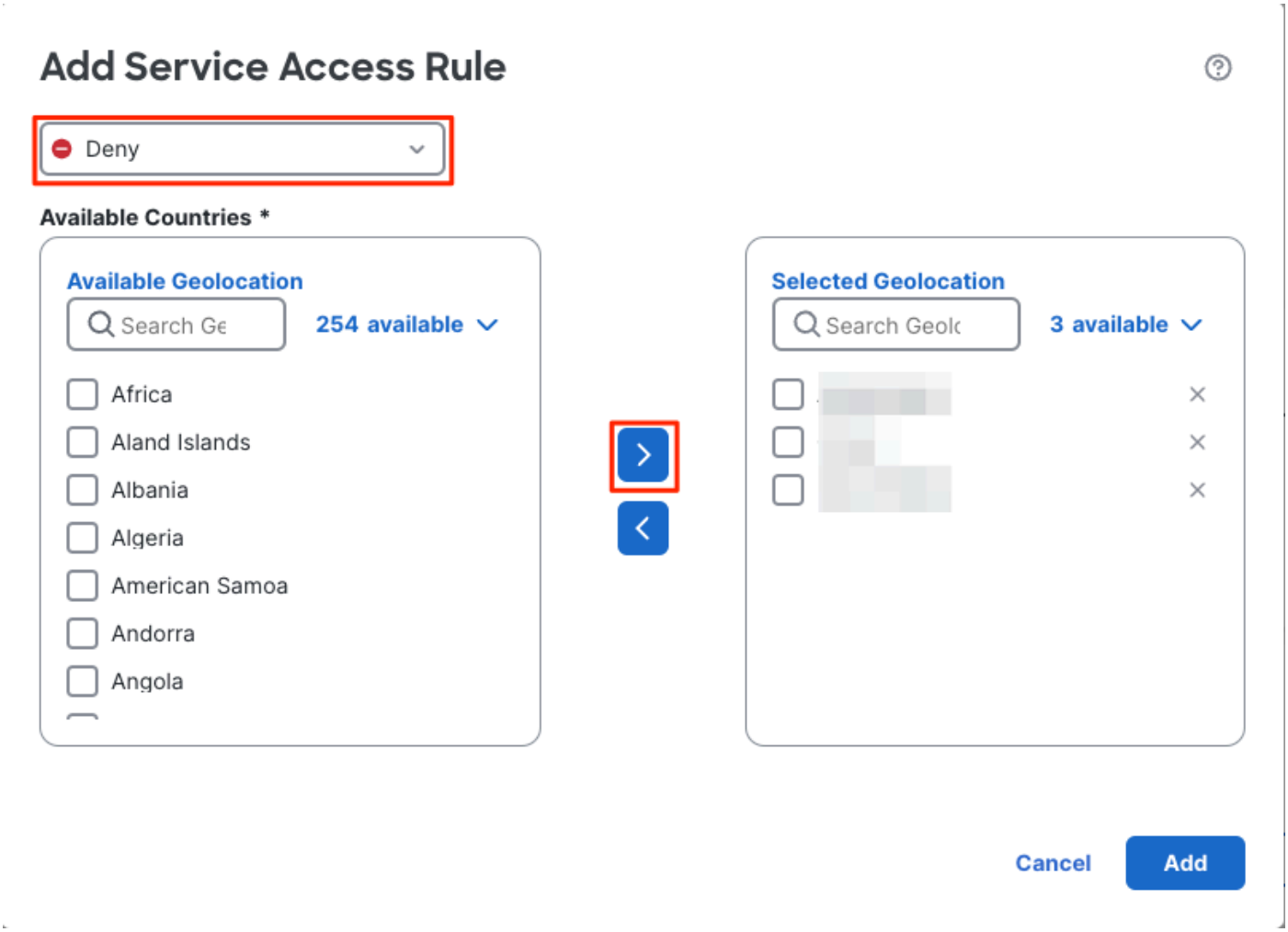


4. サービスアクセスルールを設定します。

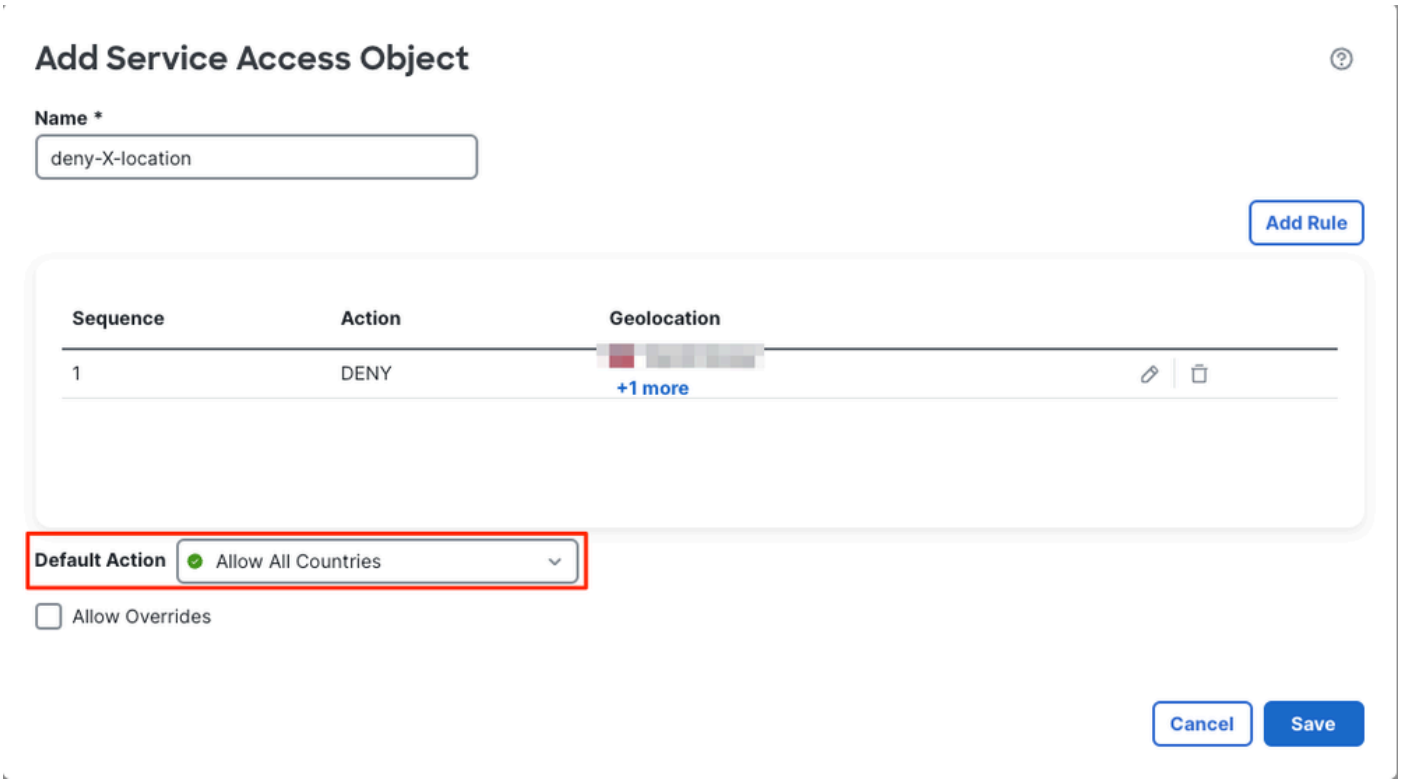
- ルールのアクションとして、AllowまたはDenyを選択します。
- 「使用可能な国」から、国、大陸またはユーザー定義の位置情報オブジェクトを選択し、「選択した位置情報」リストに移動します。
- Addをクリックして、ルールを作成します。

注：サービスアクセスオブジェクトでは、位置情報オブジェクト（国、大陸、またはカスタム位置情報）は1つのルールでのみ使用できます。

注：サービスアクセスルールは順序を変更できないので、これらのルールは正しい順序で設定してください。



5. デフォルト処理(「すべての国を許可」または「すべての国を拒否」)を選択します。このアクションは、設定されているどのサービスアクセスルールにも一致しない接続に適用されます。

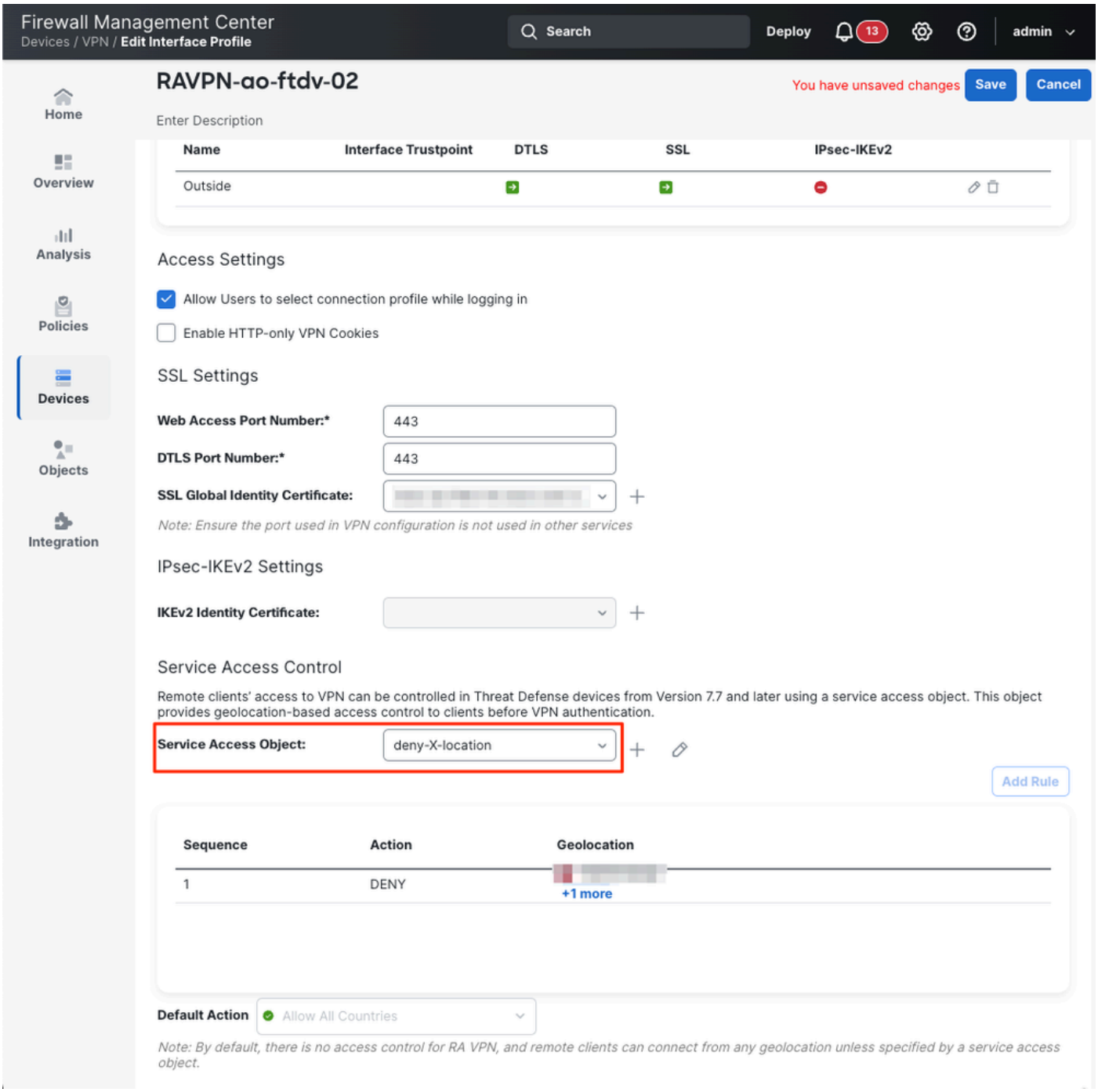


6. Saveをクリックします。

ステップ 2：RAVPNのサービスオブジェクト設定を適用します。

1. Devices > Remote Access > RAVPN configuration object > Access interfaceの順に選択し、RAVPN設定に移動します。

2. 「サービス・アクセス制御」セクションで、前に作成したサービス・アクセス・オブジェクトを選択します。

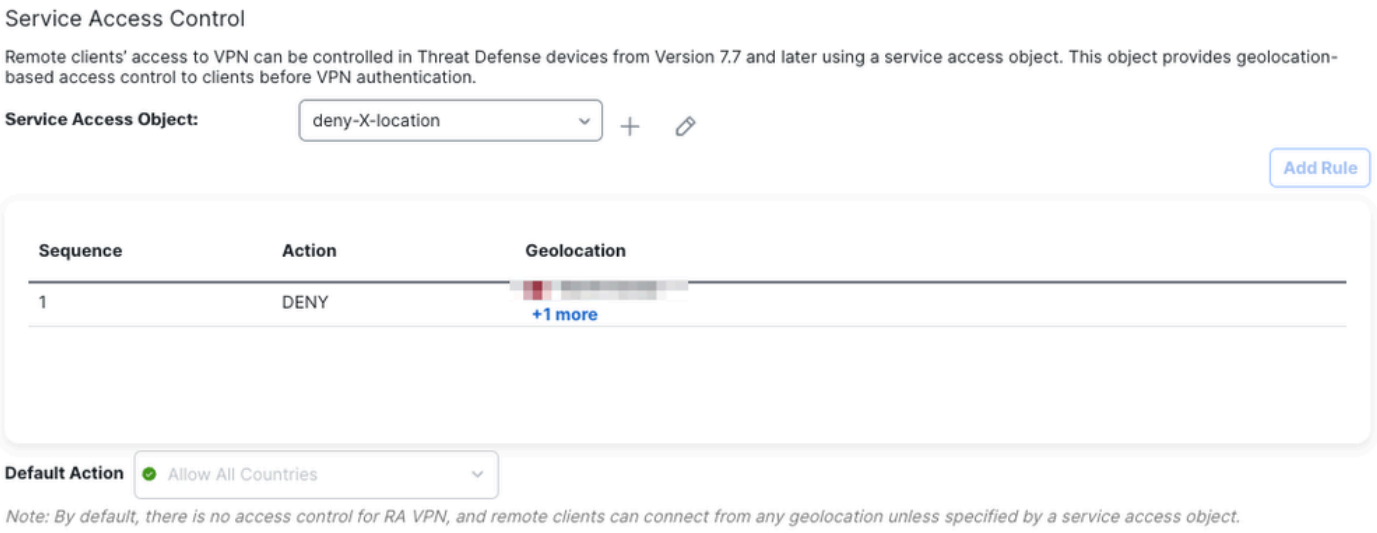


3. 選択したサービス・アクセス・オブジェクトに、ルールの要約とデフォルトのアクションが表示されます。これが正しいことを確認します。

4. 最後に、変更を保存し、設定を展開します。

確認

設定を保存すると、Service Access Controlセクションにルールが表示され、ブロックまたは許可されているグループと国を確認できます。



show running-config service-accessコマンドを実行して、FTD CLIからサービスアクセスルールを使用できることを確認します。

<#root>

```
firepower#

show running-config service-access


service-access deny ra-ssl-client geolocation FMC_GEOLOCATION_146028889448_536980902
service-access permit ra-ssl-client geolocation any

firepower# show running-config object-group idFMC_GEOLOCATION_146028889448_536980902
object-group geolocation FMC_GEOLOCATION_146028889448_536980902
location "Country X"
location "Country Y"
```

Syslogとモニタリング

セキュアファイアウォールは、位置情報ベースのポリシーによってブロックされたRAVPN接続に関連するイベントをキャプチャするために、新しいsyslog IDを導入します。

- 761031:位置情報ベースのポリシーによってIKEv2接続が拒否されるタイミングを示します。このsyslogは、既存のVPNロギングクラスの一部です。

%FTD-6-751031:geoベースのルール(geo=<country_name>, id=<country_code>)により、faddr <client_ip> laddr <device_ip>に対するIKEv2リモートアクセスセッションが拒否されました

- 751031:位置情報ベースのポリシーによってSSL接続が拒否された時点を示します。このsyslogは、既存のWebVPNロギングクラスの一部です。

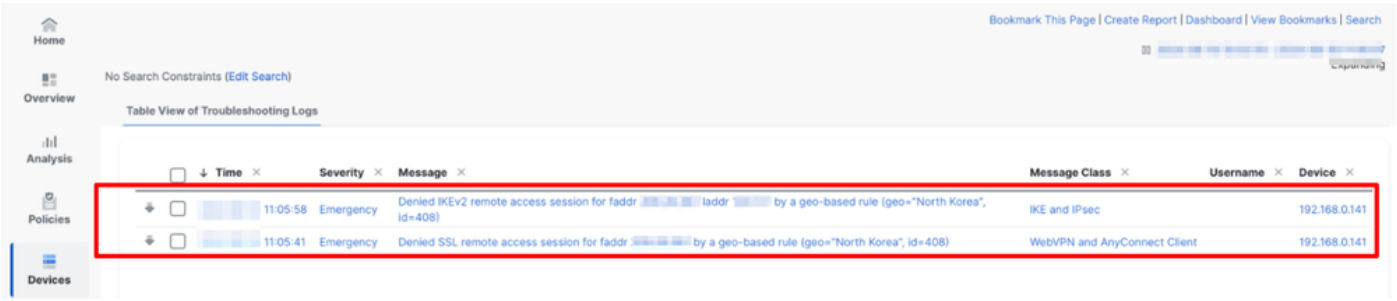
%FTD-6-716166：地域ベースのルール(geo=<country_name>, id=<country_code>)によりfaddr <client_ip>のSSLリモートアクセスセッションが拒否されました

注：これらの新しいsyslogのデフォルトの重大度レベルは、それぞれのロギングクラスで有効になっている場合はinformationalです。ただし、これらのsyslog IDを個別に有効にして、重大度をカスタマイズできます。

ブロックされた接続の監視

ブロックされた接続を検証するには、Devices > Troubleshoot > Troubleshooting Logsの順に選択します。ここでは、接続に影響するルールやセッションのタイプなどの情報を含む、ブロックされた接続に関連するログが表示されます。

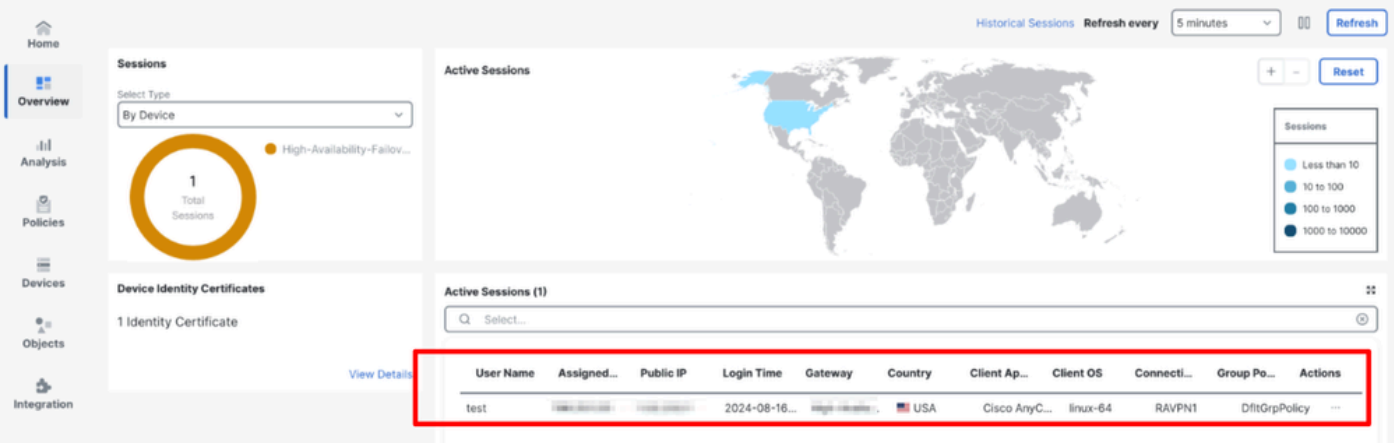
注：トラブルシューティングログでこの情報を収集するには、Syslogを設定する必要があります。



許可された接続の監視

許可されたセッションは、Overview > Remote Access VPN dashboardで監視されます。ここでは、発生国を含むセッション情報が表示されます。

注：このダッシュボードには、許可されている国からの接続と、接続が許可されているユーザのみが表示されます。拒否された接続は、このダッシュボードには表示されません。



トラブルシュート

トラブルシューティングの目的で、次の手順を実行します。

1. サービスアクセスオブジェクトでルールが正しく設定されていることを確認します。
2. 許可された位置情報がセッションを要求したときに、Troubleshooting Logsセクションにdeny syslogが表示されるかどうかを確認します。
3. FMCに表示される設定が、FTD CLIに表示されている設定と一致していることを確認します。
4. トラブルシューティングに役立つ詳細情報を収集するには、次のコマンドを使用します。

- debug geolocation <1-255>
- show service-access（隠しコマンド）
- サービスアクセスの詳細の表示
- show service-access interface（隠しコマンド）
- サービスアクセスの場所の表示
- show service-access service（登録ユーザ専用）
- show geodb ipv4 location <Country> detail
- geodbカウンタの表示
- show geodb ipv4 [lookup <IPアドレス>]
- show geodb ipv6（ベータ版）

関連情報

- 詳細については、TACにお問い合わせください。有効なサポート契約が必要です。シスコワールドワイドサポートの連絡先を参照してください。
- Cisco VPN Communityhereにもアクセスできます。

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。