Konfigurieren von standortbezogenen Richtlinien für Remote-Access-VPN auf der sicheren Firewall-Bedrohungsabwehr

Inhalt

Einleitung

Voraussetzungen

- Anforderungen und Einschränkungen
- Verwendete Komponenten

Hintergrundinformationen

Konfigurieren

- Schritt 1: Erstellen eines Dienstzugriffsobjekts
- Schritt 2: Anwenden der Service Object-Konfiguration in RAVPN

Überprüfung

Syslogs und Überwachung

- Blockierte Verbindungen überwachen
- Zugelassene Verbindungen überwachen

Fehlerbehebung

Zugehörige Informationen

Einleitung

In diesem Dokument wird der Prozess zum Zulassen oder Verweigern von RAVPN-Verbindungen basierend auf bestimmten geografischen Standorten in Secure Firewall Threat Defense (FTD) beschrieben.

Voraussetzungen

Anforderungen und Einschränkungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Secure Firewall Management Center (FMC)
- Remote Access-VPN (RAVPN)
- Grundlegende Standortkonfiguration

Derzeit gelten für standortbasierte Richtlinien folgende Anforderungen und Einschränkungen:

- Unterstützt nur auf FTD Version 7.7.0+, verwaltet von FMC Version 7.7.0+.
- Nicht unterstützt auf FTD, die vom Secure Firewall Device Manager (FDM) verwaltet wird.

- Im Clustermodus nicht unterstützt
- Standortbasierte, nicht klassifizierte IP-Adressen werden nicht nach geografischer Herkunft kategorisiert. Für diese setzt das FMC die standardmäßige Zugriffsrichtlinienaktion für den Service durch.
- Standortbasierte Zugriffsrichtlinien gelten nicht für WebLaunch-Seiten, sodass Sie den Secure Client ohne Einschränkungen herunterladen können.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Secure Firewall Version 7.7.0
- Secure Firewall Management Center Version 7.7.0

Ausführliche Informationen zu dieser Funktion finden Sie im Abschnitt Manage VPN Access of Remote Users Based on Geolocation (VPN-Zugriff für Remote-Benutzer basierend auf Standort verwalten) im Cisco Secure Firewall Management Center 7.7 Device Configuration Guide.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

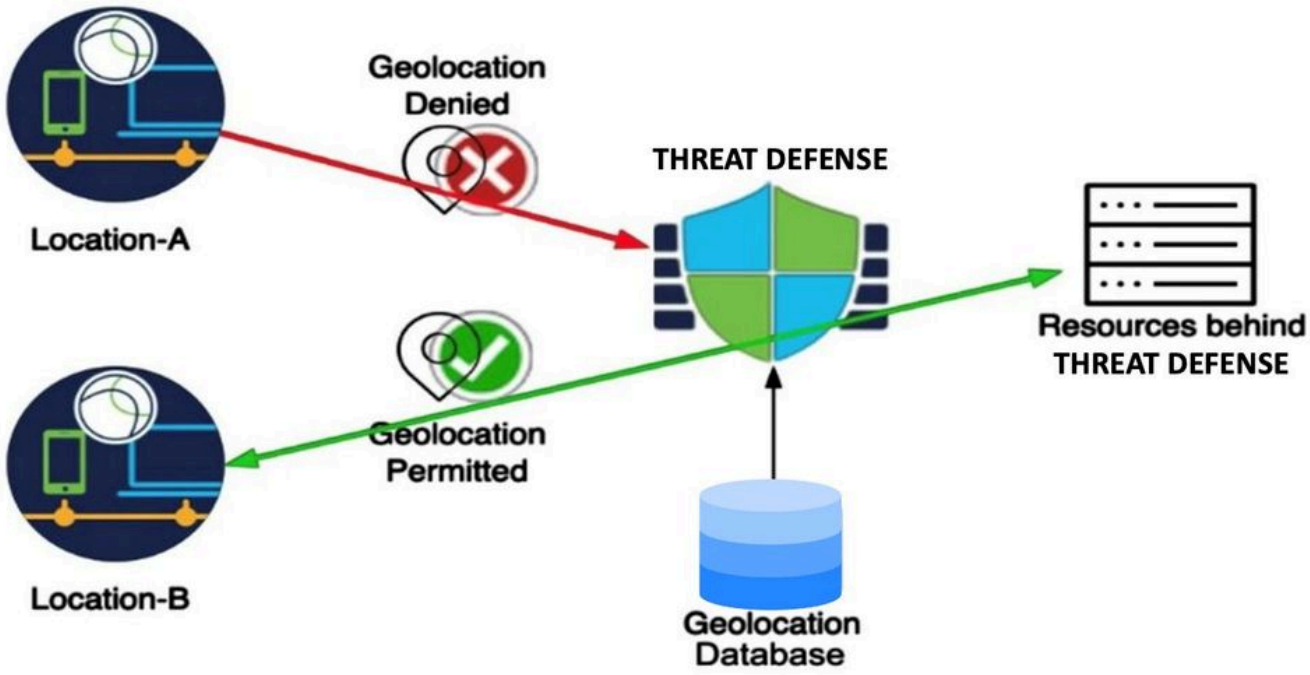
Standortbasierte Zugriffsrichtlinien bieten heute einen erheblichen Nutzen für die Netzwerksicherheit und ermöglichen die Blockierung von Datenverkehr basierend auf seiner geografischen Herkunft. Bisher konnten Unternehmen Richtlinien für den Datenverkehrszugriff für allgemeinen Netzwerkverkehr definieren, der die Firewall passiert. Mit der Einführung dieser Funktion ist es jetzt möglich, eine standortbasierte Zugriffskontrolle für Remotezugriff-VPN-Sitzungsanforderungen anzuwenden.

Diese Funktion bietet die nächsten Vorteile:

- Standortbasierte Regeln: Kunden können Regeln erstellen, um RAVPN-Anfragen basierend auf bestimmten Standorten, z. B. Ländern oder Kontinenten, zuzulassen oder abzulehnen. Dies ermöglicht eine präzise Kontrolle darüber, welche geografischen Standorte VPN-Sitzungen initiieren können.
- Blockierung vor der Authentifizierung: Von diesen Regeln für eine Ablehnungsaktion identifizierte Sitzungen werden vor der Authentifizierung blockiert, und diese Versuche werden aus Sicherheitsgründen ordnungsgemäß protokolliert. Diese Präventivmaßnahme trägt zur Verhinderung nicht autorisierter Zugriffsversuche bei.
- Compliance und Sicherheit: Diese Funktion hilft dabei, die Einhaltung lokaler Organisations- und Governance-Richtlinien sicherzustellen und reduziert gleichzeitig die Angriffsfläche des

VPN-Servers.

Da VPN-Server über öffentliche IP-Adressen verfügen, auf die über das Internet zugegriffen werden kann, ermöglicht die Einführung von Geolocation-basierten Regeln Organisationen, Nutzeranfragen aus bestimmten Geolocations wirksam einzuschränken und so die Anfälligkeit für Brute-Force-Angriffe zu verringern.

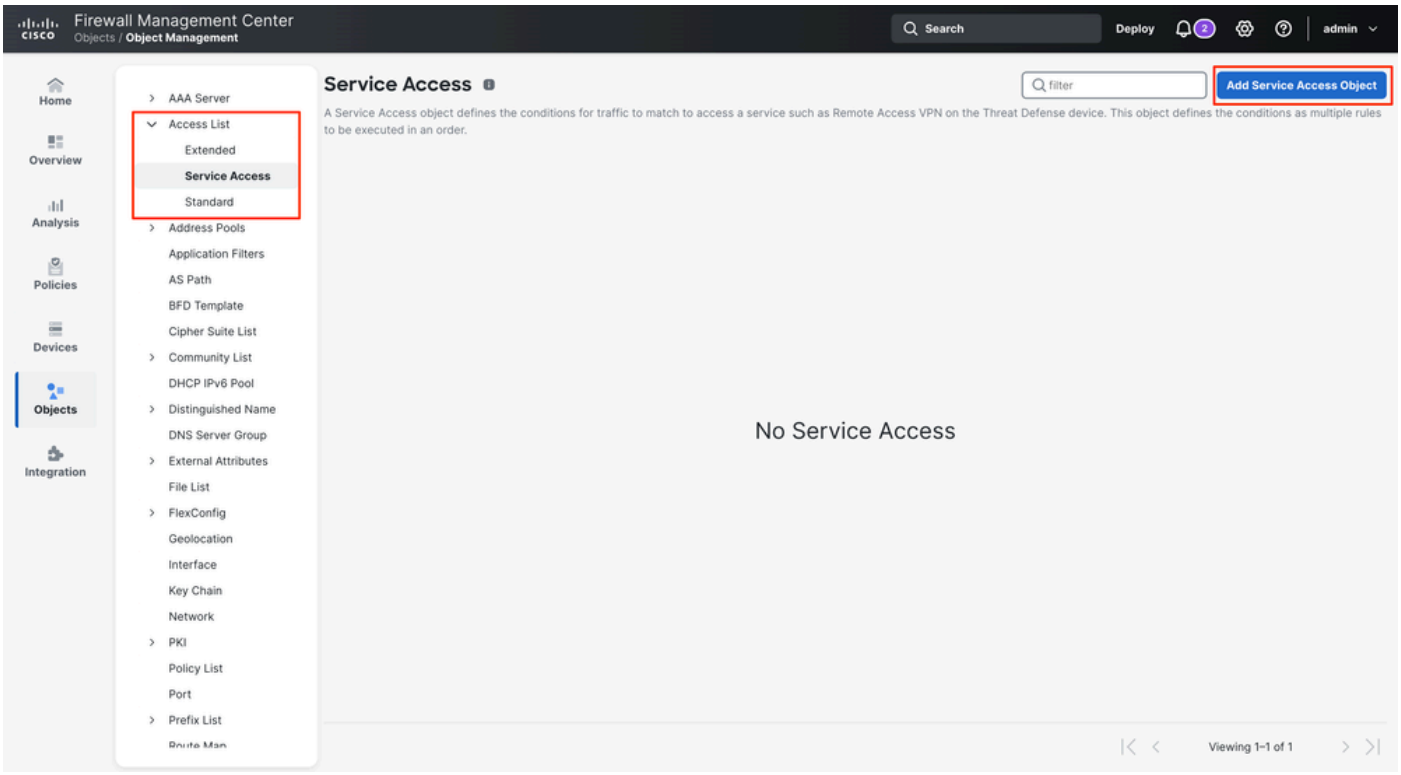


Konfigurieren

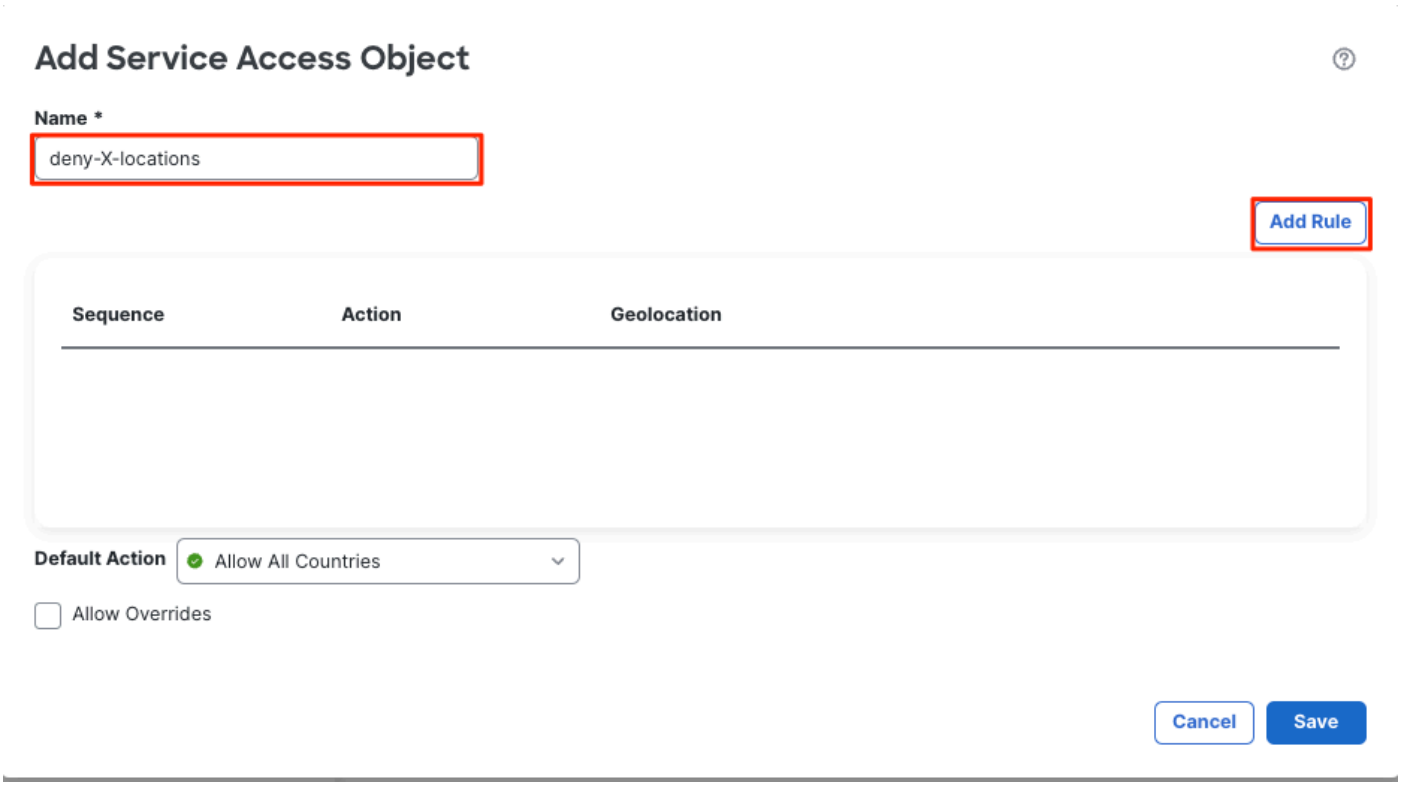
Schritt 1: Erstellen eines Dienstzugriffsobjekts

1. Melden Sie sich beim Secure Firewall Management Center an.

2. Navigieren Sie zu Objekte > Objektverwaltung > Zugriffsliste > Dienstzugriff, und klicken Sie auf Dienstzugriffsobjekt hinzufügen.Add (Dienstzugriffsobjekt hinzufügen).



3. Definieren Sie den Regelnamen, und klicken Sie dann auf Regel hinzufügen.

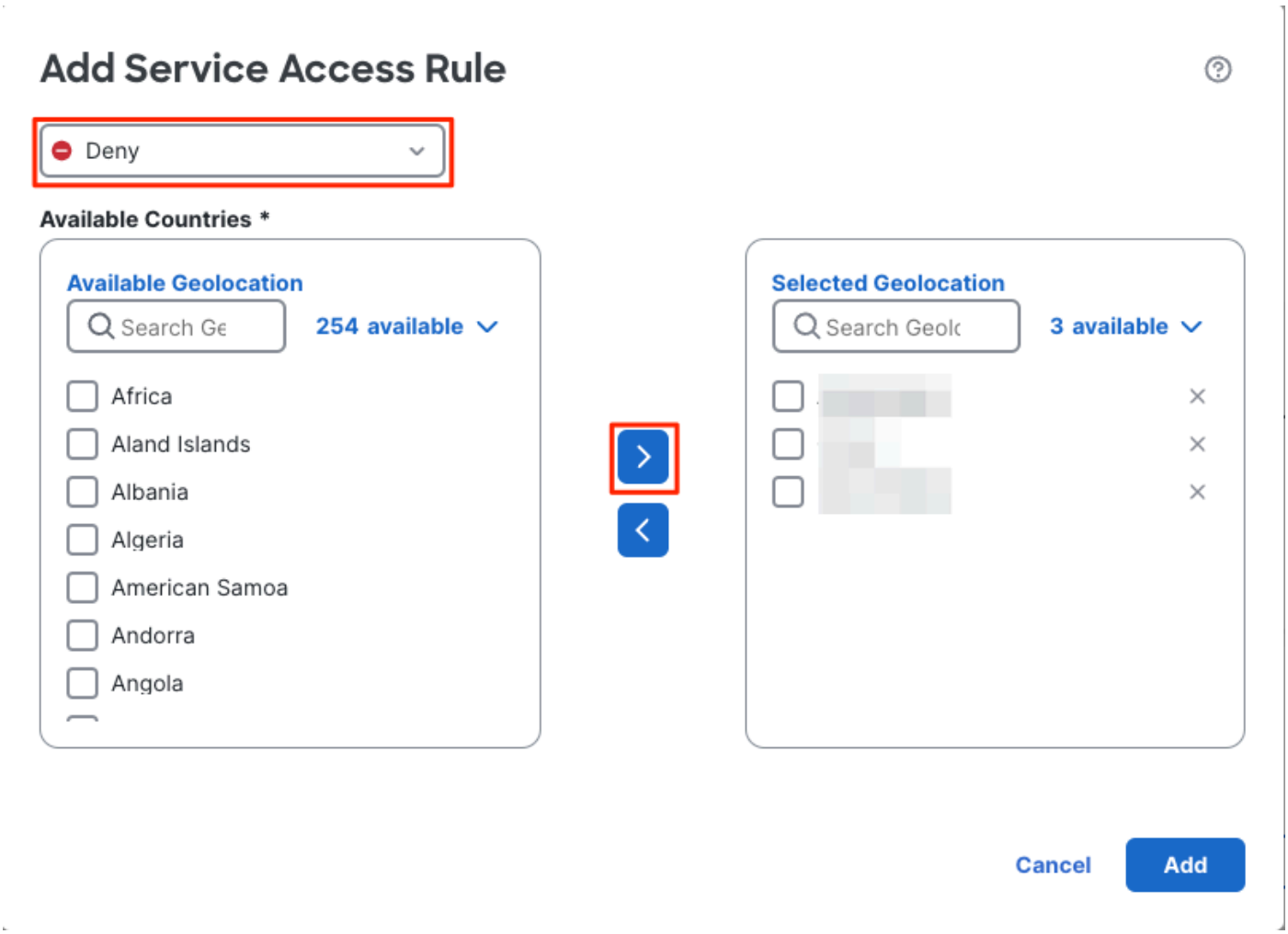


4. Konfigurieren Sie die Dienstzugriffsregel:

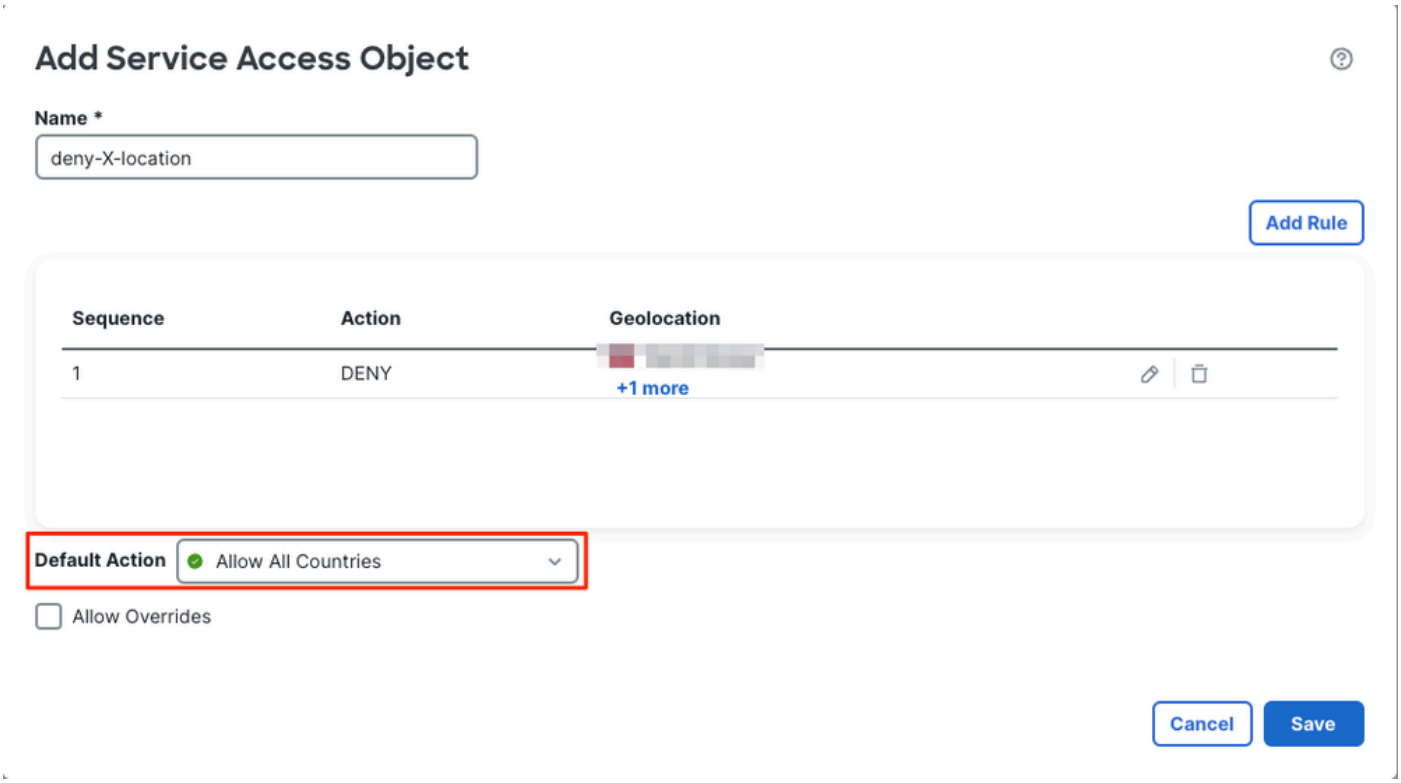
- Wählen Sie die Aktion der Regel aus: Zulassen oder Verweigern.
- Wählen Sie unter Verfügbare Länder Länder, Kontinente oder benutzerdefinierte Geolokationsobjekte aus, und verschieben Sie sie in die Liste Ausgewählte Geolokation.
- Klicken Sie auf Hinzufügen, um die Regel zu erstellen.

Anmerkung: In einem Dienstzugriffsobjekt kann ein Geolokationsobjekt (Land, Kontinent oder benutzerdefinierte Geolokation) nur in einer Regel verwendet werden.

Hinweis: Konfigurieren Sie die Zugriffsregeln für den Service in der richtigen Reihenfolge, da diese Regeln nicht neu sortiert werden können.



5. Wählen Sie die Standardaktion: entweder Alle Länder zulassen oder Alle Länder verweigern. Diese Aktion gilt für Verbindungen, die keiner der konfigurierten Dienstzugriffsregeln entsprechen.

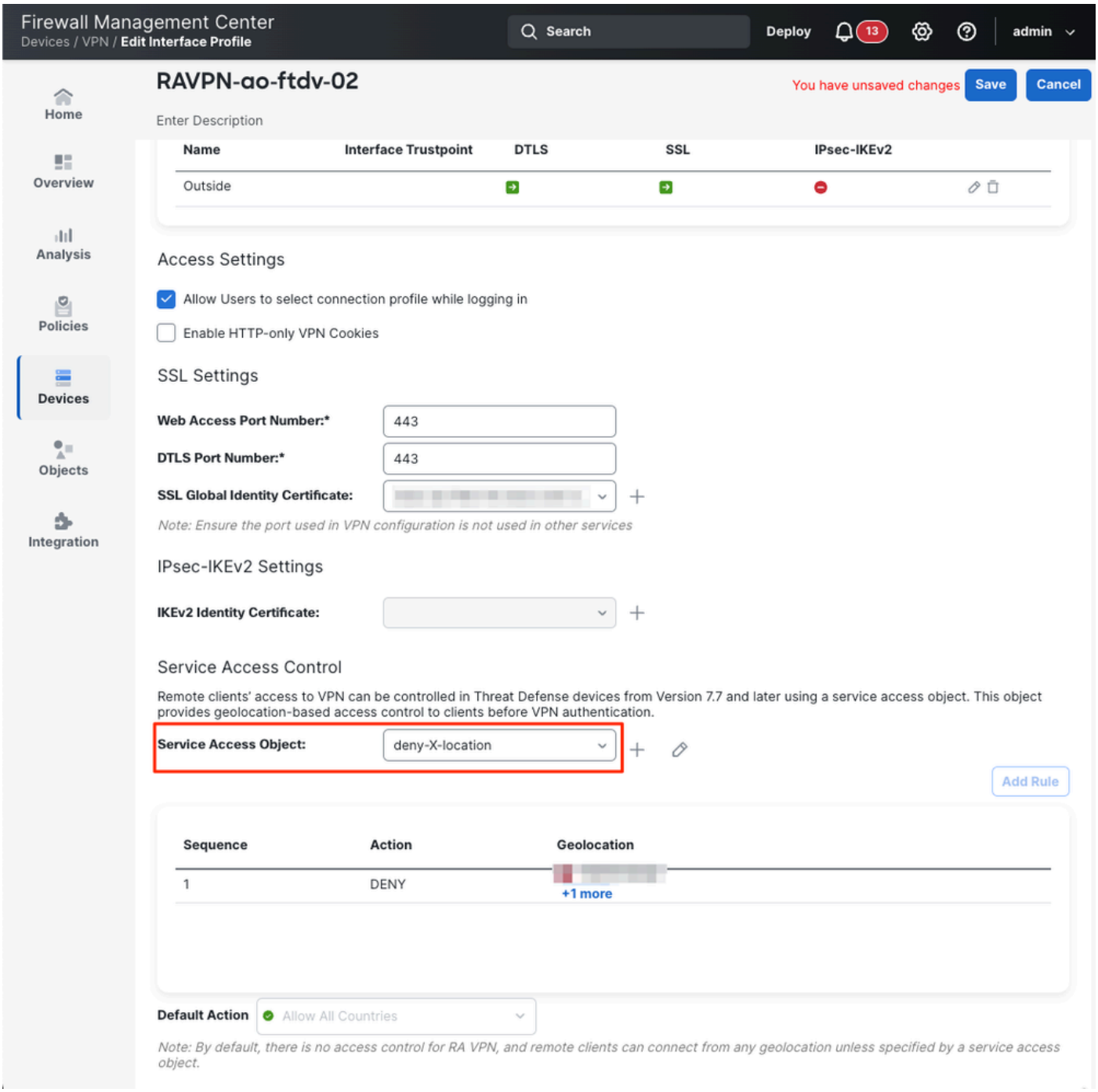


6. Klicken Sie auf Speichern.

Schritt 2: Anwenden der Service Object-Konfiguration in RAVPN

1. Navigieren Sie zur RAVPN-Konfiguration unter Devices (Geräte) > Remote Access (Remote-Zugriff) > RAVPN configuration object (RAVPN-Konfigurationsobjekt) > Access interface (Zugriffsschnittstelle).

2. Wählen Sie im Abschnitt Dienstzugriffskontrolle das zuvor erstellte Dienstzugriffsobjekt aus.



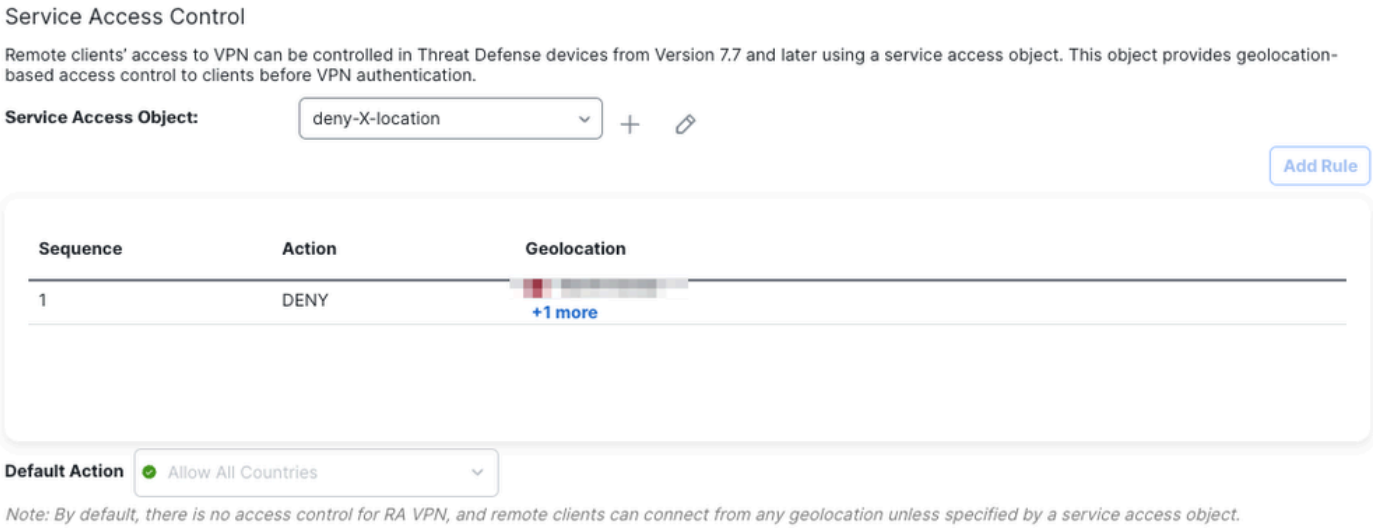
3. Das ausgewählte Service Access-Objekt zeigt jetzt die Regelübersicht und die Standardaktion an. Stellen Sie sicher, dass dies richtig ist.

4. Speichern Sie abschließend die Änderungen, und stellen Sie die Konfiguration bereit.

Überprüfung

Nach dem Speichern der Konfiguration werden die Regeln im Abschnitt Service Access Control (Dienstzugriffskontrolle) angezeigt, mit denen Sie überprüfen können, welche Gruppen und

Länder gesperrt oder zugelassen sind.



Führen Sie den Befehl show running-config service-access aus, um sicherzustellen, dass die Regeln für den Dienstzugriff über die FTD-CLI verfügbar sind.

<#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"
```

Syslogs und Überwachung

Secure Firewall führt neue Syslog-IDs ein, um Ereignisse zu erfassen, die mit RAVPN-Verbindungen zusammenhängen und durch standortbezogene Richtlinien blockiert werden:

- 761031: Gibt an, wenn eine IKEv2-Verbindung durch eine standortbasierte Richtlinie abgelehnt wird. Dieses Syslog ist Teil der vorhandenen VPN-Protokollierungsklasse.

%FTD-6-751031: IKEv2-Remotezugriffssitzung für faddr <client_ip> laddr <device_ip> wurde

durch eine geobasierte Regel (geo=<Ländername>, id=<Ländercode>) verweigert

- 751031: Gibt an, wenn eine SSL-Verbindung von einer Geolocation-basierten Richtlinie abgelehnt wird. Dieses Syslog ist Teil der vorhandenen WebVPN-Protokollierungsklasse.

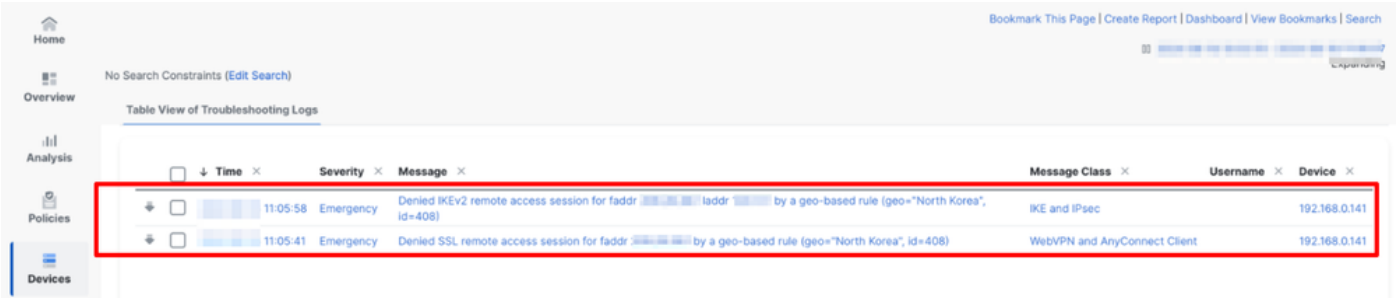
%FTD-6-716166: Remotezugriffssitzung mit verweigertem SSL für faddr <client_ip> durch eine geobasierte Regel (geo=<country_name>, id=<country_code>)

Anmerkung: Der Standardschweregrad für diese neuen Syslogs ist informativ, wenn er von den entsprechenden Protokollierungsklassen aktiviert ist. Sie können diese Syslog-IDs jedoch einzeln aktivieren und ihren Schweregrad anpassen.

Blockierte Verbindungen überwachen

Um blockierte Verbindungen zu überprüfen, navigieren Sie zu Geräte > Fehlerbehebung > Protokolle zur Fehlerbehebung. Hier werden Protokolle zu gesperrten Verbindungen angezeigt, einschließlich Informationen zu den Regeln, die sich auf die Verbindung auswirken, und zum Sitzungstyp.

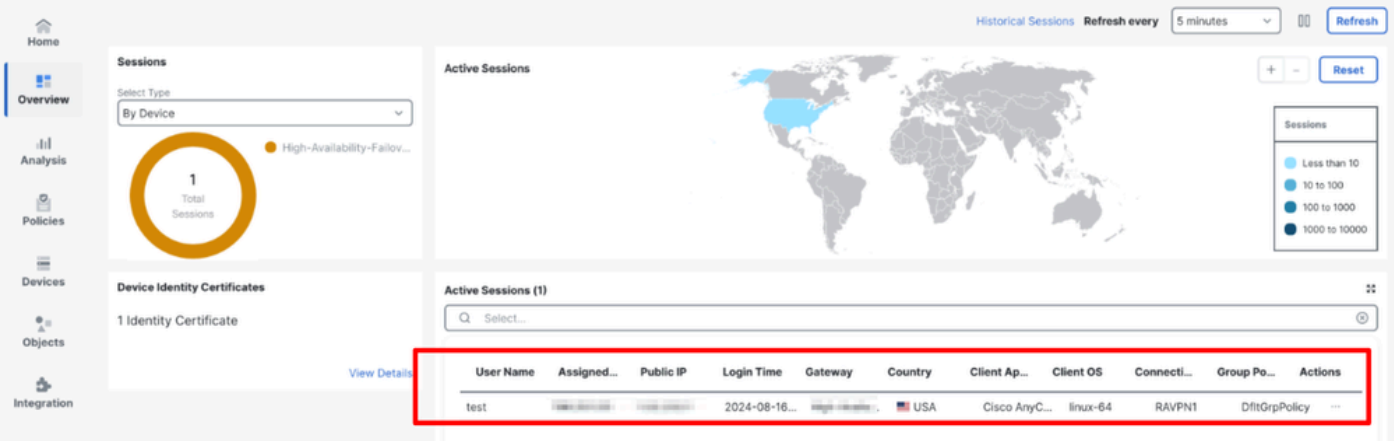
Anmerkung: Syslog muss so konfiguriert werden, dass diese Informationen in den Fehlerbehebungsprotokollen erfasst werden.



Zugelassene Verbindungen überwachen

Die zulässigen Sitzungen werden unter Übersicht > VPN-Dashboard mit Remote-Zugriff überwacht, wo Sitzungsinformationen angezeigt werden, einschließlich des Ursprungslandes.

Anmerkung: In diesem Dashboard werden nur Verbindungen aus zulässigen Ländern und Benutzer angezeigt, die eine Verbindung herstellen dürfen. Abgelehnte Verbindungen werden in diesem Dashboard nicht angezeigt.



Fehlerbehebung

Führen Sie zur Fehlerbehebung die folgenden Schritte aus:

1. Überprüfen Sie, ob die Regeln im Service Access-Objekt richtig konfiguriert sind.
2. Überprüfen Sie, ob im Abschnitt "Troubleshooting Logs" (Fehlerbehebungsprotokolle) ein Deny-Syslog angezeigt wird, wenn eine zulässige Standortbestimmung eine Sitzung anfordert.
3. Stellen Sie sicher, dass die im FMC angezeigte Konfiguration mit der Konfiguration in der FTD-CLI übereinstimmt.
4. Verwenden Sie die folgenden Befehle, um weitere Details zu sammeln, die für die Fehlerbehebung nützlich sind:

- debug geolocation <1-255>
- Dienstzugriff anzeigen
- Details zum Dienstzugriff anzeigen
- Show Service-Access-Schnittstelle
- Ort des Dienstzugriffs anzeigen
- Service-Zugriffsdienst anzeigen
- show geodb ipv4 location <Land> detail
- Geodb-Zähler anzeigen
- show geodb ipv4 [lookup <IP-Adresse>]
- geodb ipv6 anzeigen

Zugehörige Informationen

- Weitere Unterstützung erhalten Sie beim TAC. Ein gültiger Support-Vertrag ist erforderlich:Cisco Worldwide Support Contacts
- Besuchen Sie auch die Cisco VPN Community hier.

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.