為安全防火牆威脅防禦的遠端訪問VPN配置基於地理位置的策略

目錄

簡介

本檔案介紹根據安全防火牆威脅防禦(FTD)上的特定地理位置允許或拒絕RAVPN連線的程式。

必要條件

要求和限制

思科建議您瞭解以下主題：

- 安全防火牆管理中心(FMC)
- 遠端存取VPN(RAVPN)
- 基本地理位置配置

基於地理定位的策略的當前要求和限制如下：

- 僅在FTD 7.7.0+版上受支援，由FMC 7.7.0+版管理。
- 在由安全防火牆裝置管理器(FDM)管理的FTD上不受支援。
- 群集模式中不支援
- 基於地理位置的未分類IP地址不按地理來源分類。對於這些情況，FMC會實施預設服務訪問

策略操作。

- 基於地理定位的服務訪問策略不適用於WebLaunch頁面，允許您無限制地下載安全客戶端。

採用元件

本檔案中的資訊是根據以下軟體版本：

- 安全防火牆版本7.7.0
- 安全防火牆管理中心版本7.7.0

有關此功能的完整詳細資訊，請參閱Cisco Secure Firewall Management Center 7.7 Device Configuration Guide中的Manage VPN Access of Remote Users Based on Geolocation部分。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

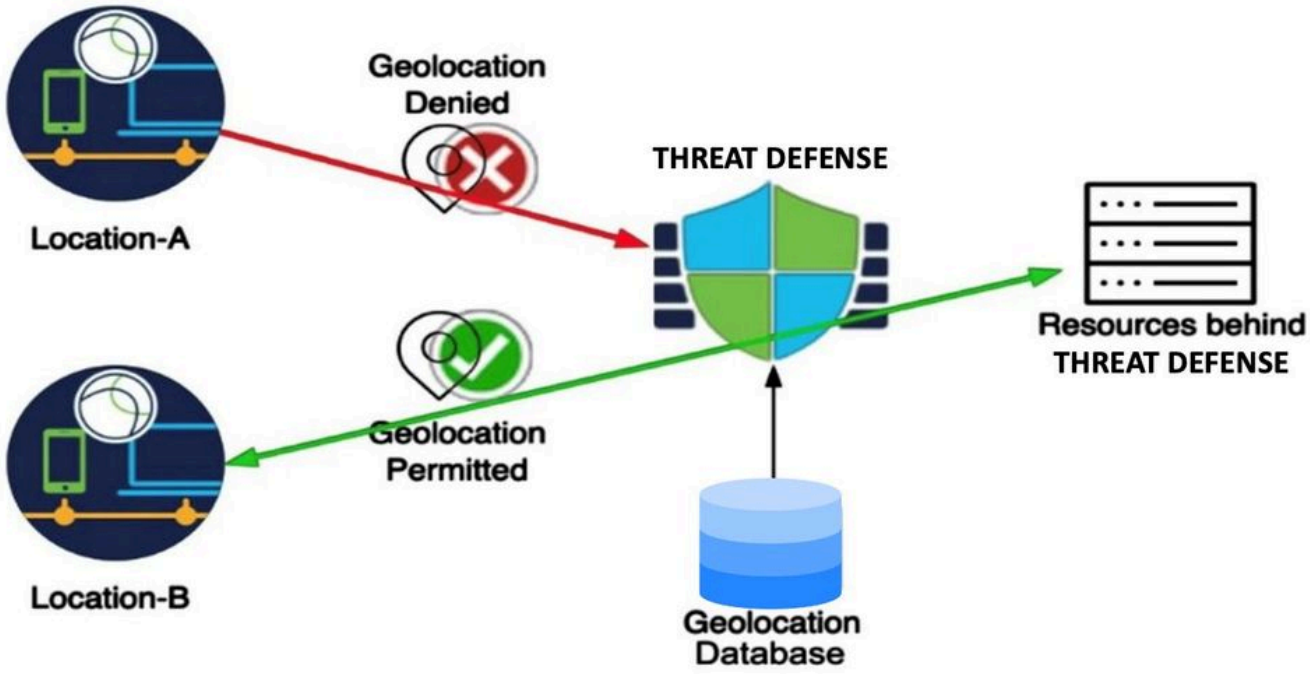
背景資訊

基於地理位置的訪問策略在當今的網路安全方面提供了巨大的價值，允許基於地理位置阻止流量。傳統上，組織可以為通過防火牆的一般網路流量定義流量訪問策略。現在，通過引入此功能，可以對遠端訪問VPN會話請求應用基於地理位置的訪問控制。

此功能提供以下優勢：

- 基於地理定位的規則：客戶可以建立規則，根據特定地理位置（如國家/地區或大陸）來允許或拒絕RAVPN請求。這樣可以精確控制哪些地理位置可以發起VPN會話。
- 預先驗證封鎖：由這些規則為deny操作標識的會話在身份驗證之前會被阻止，出於安全考慮，會正確記錄這些嘗試。此搶先操作有助於減少未經授權的訪問嘗試。
- 合規性和安全性：此功能有助於確保遵守本地組織和管理策略，同時減少VPN伺服器的攻擊面。

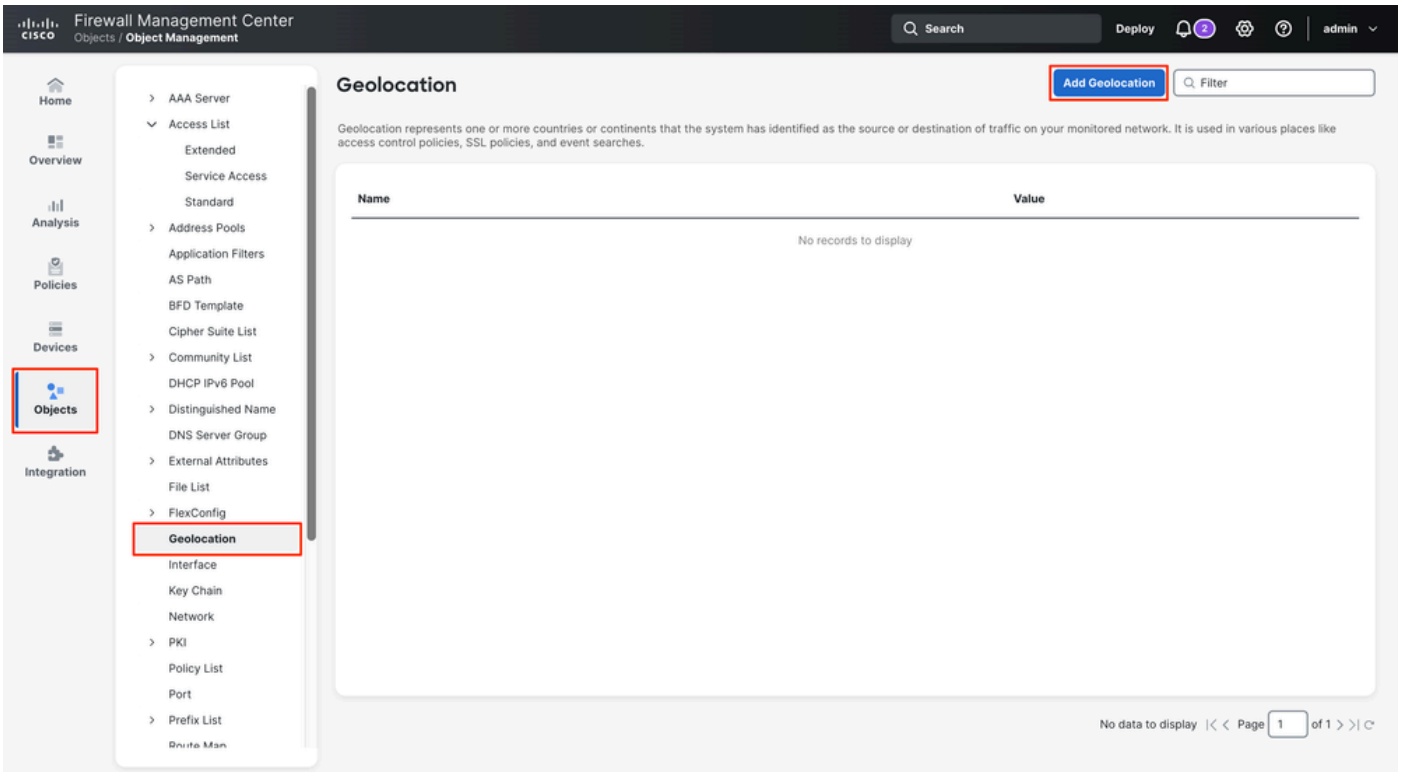
既然VPN伺服器具有可通過網際網路訪問的公有IP地址，引入基於地理定位的規則可以使組織有效限制來自特定地理定位的使用者請求，從而降低暴力攻擊的漏洞。



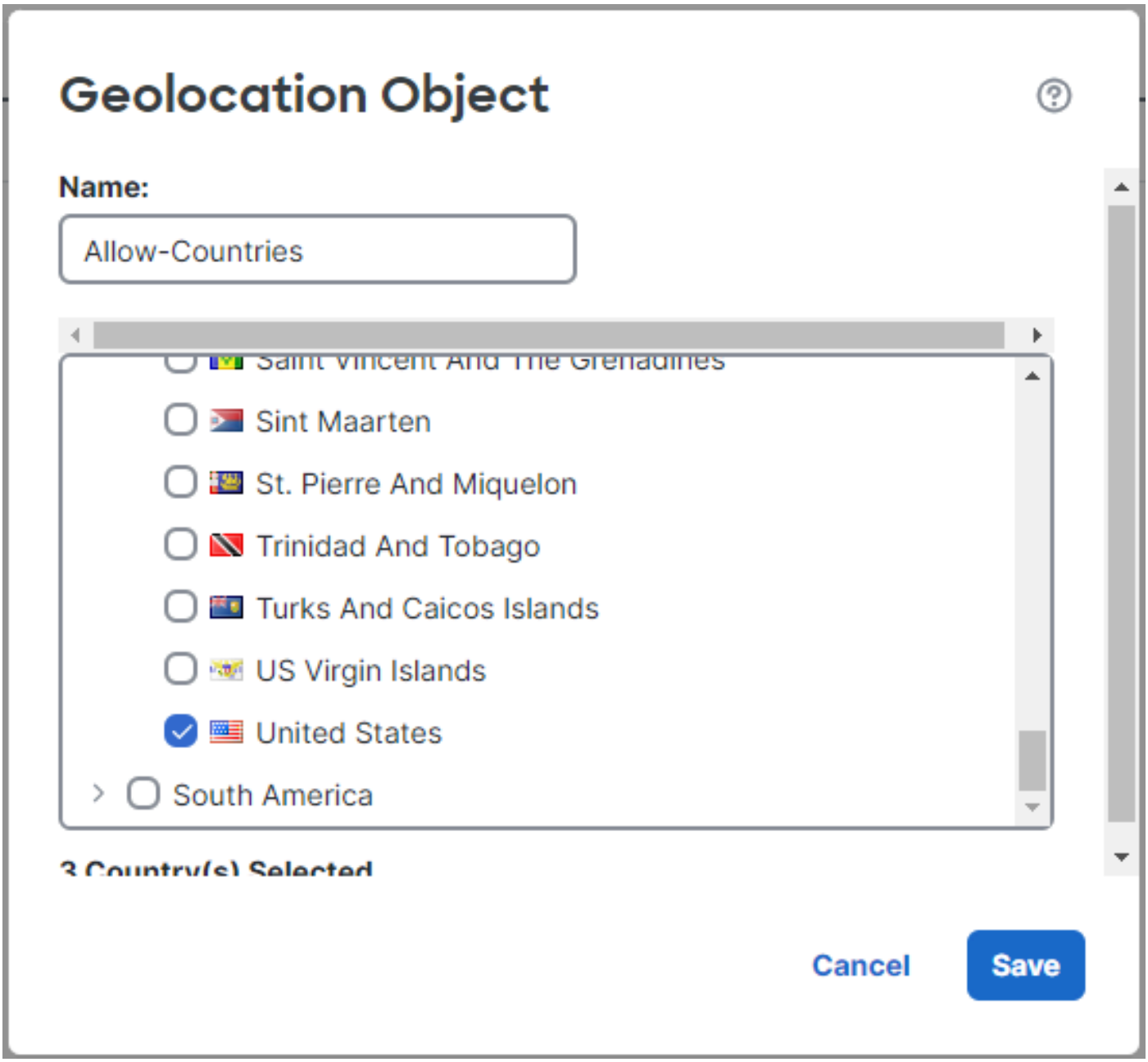
設定

步驟1.建立服務訪問對象

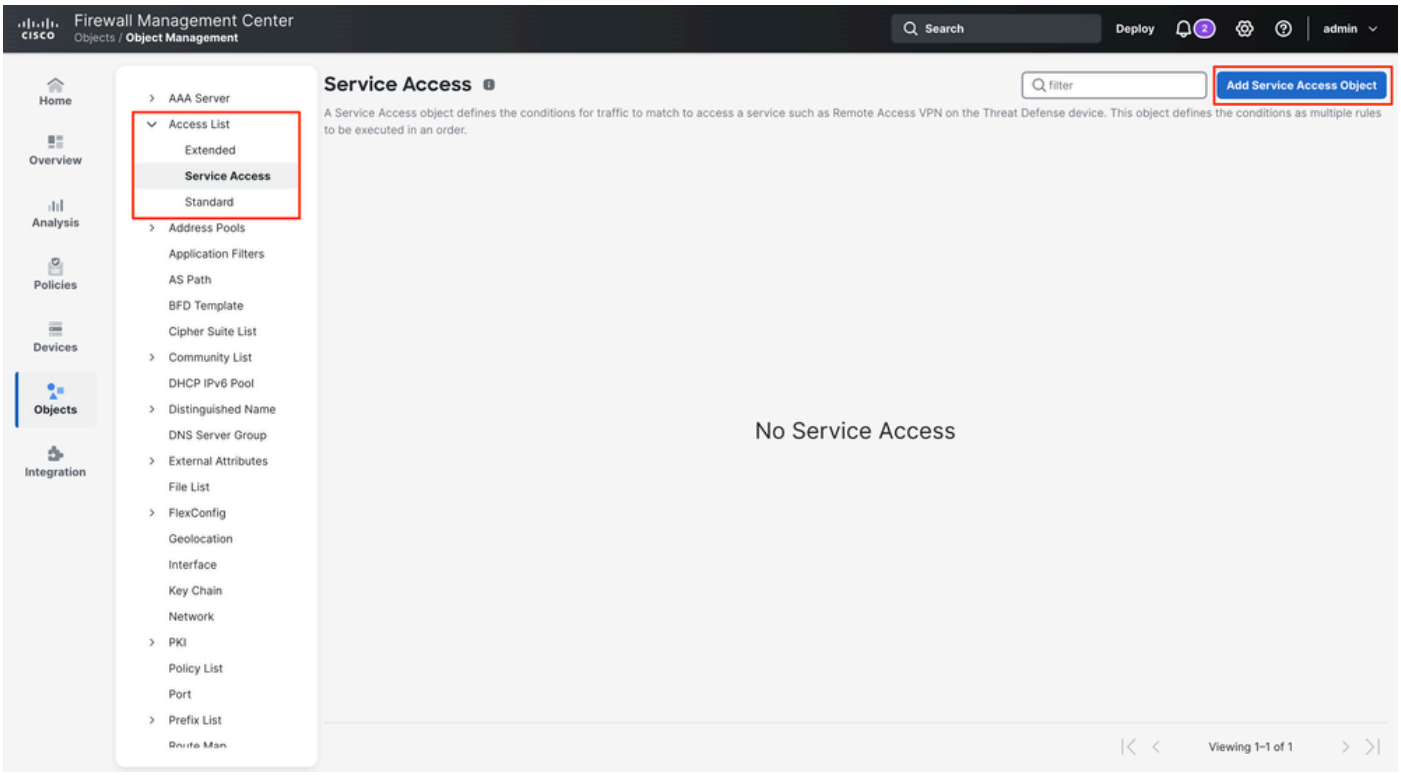
1.登入到安全防火牆管理中心。
2.定位至對象 > 對象管理 > 地理定位，然後按一下新增地理定位以建立地理定位對象。



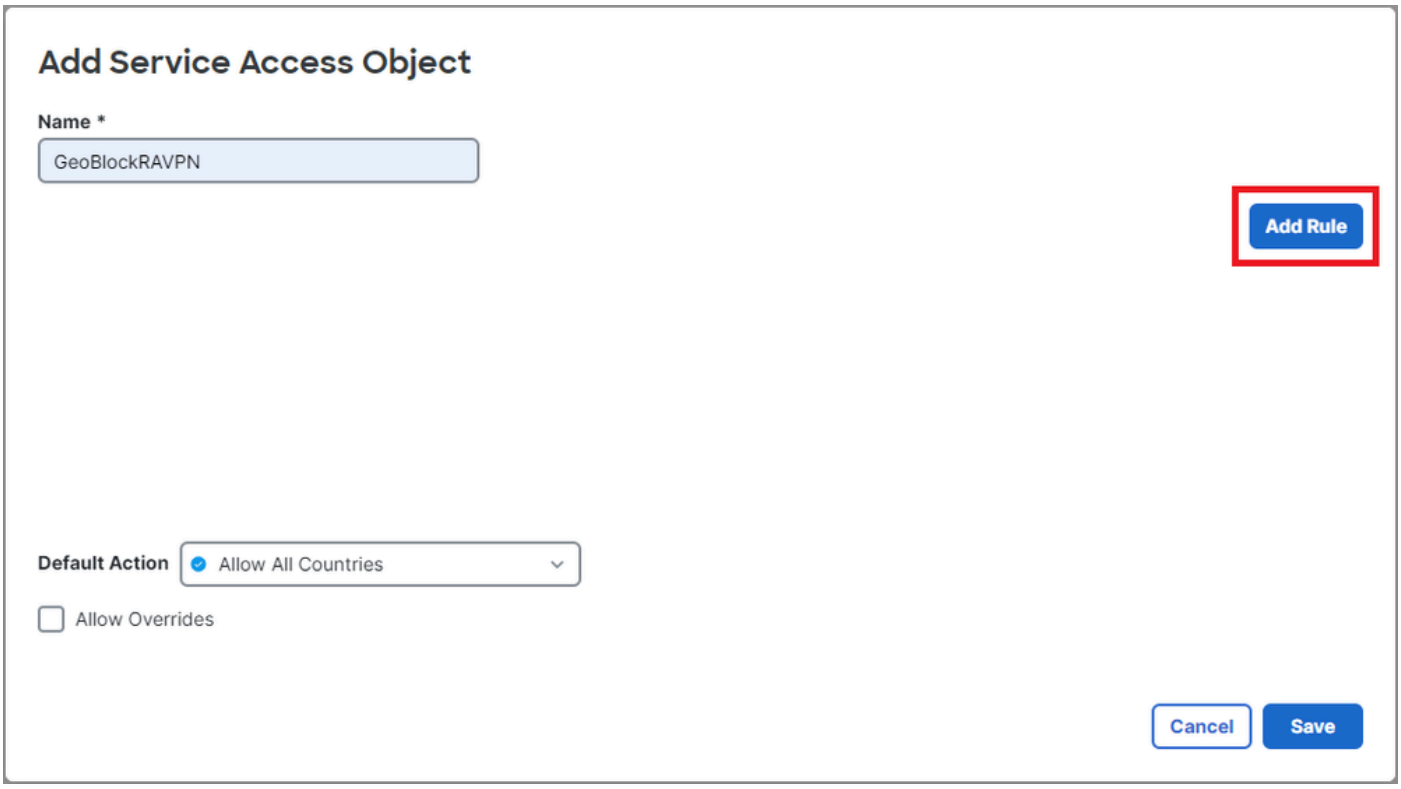
3.根據對象是被允許還是被拒絕，通過為每個組選擇適當的國家/地區標誌來建立對象。



4.建立Geolocation對象後，請轉至Objects > Object Management > Access List > Service Access，然後按一下AddService Access Object。



5.定義規則名稱，然後按一下Add Rule。

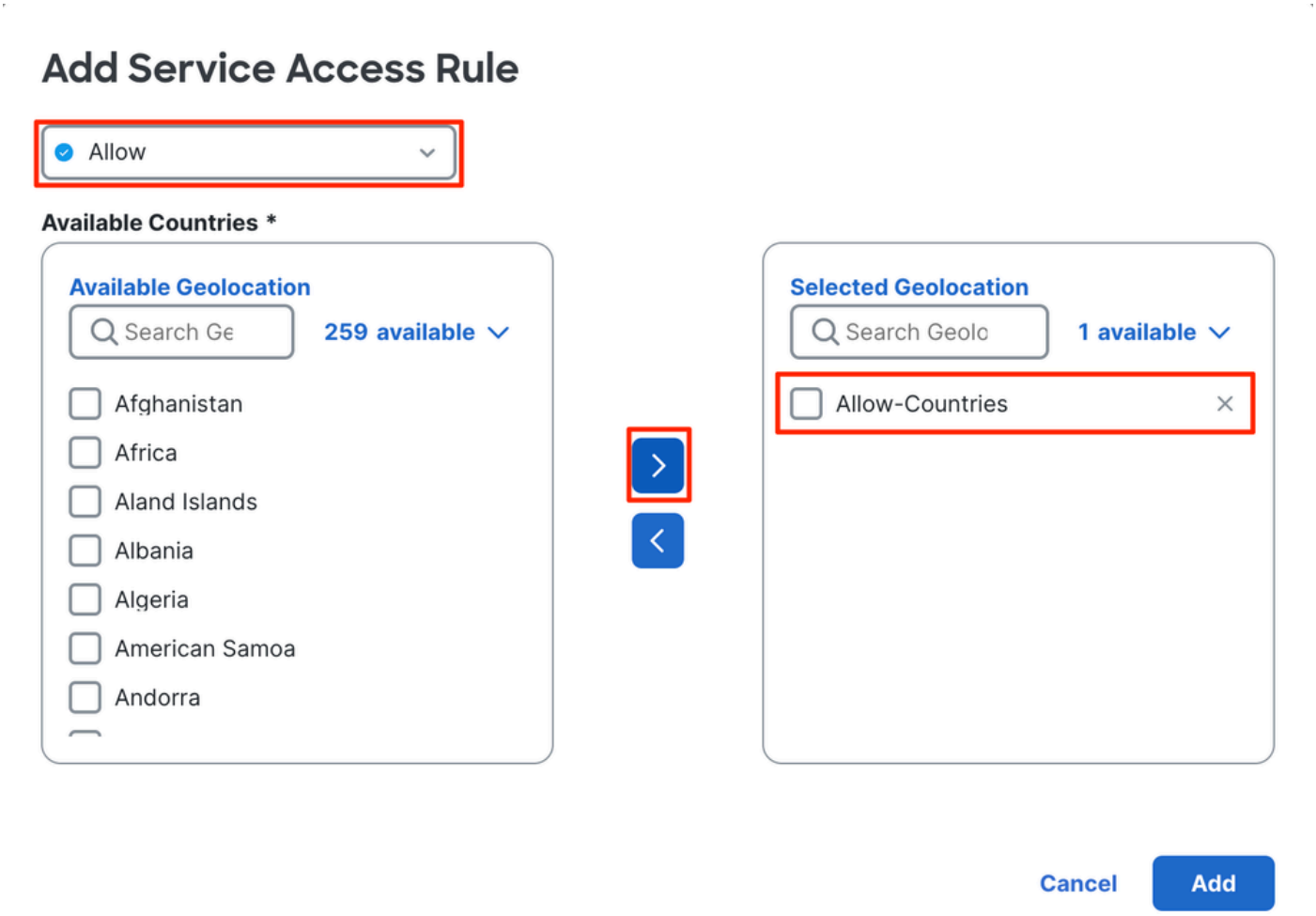


6.選擇規則的操作（允許或拒絕），找到先前建立的Geolocation對象，然後通過按一下右箭頭將其

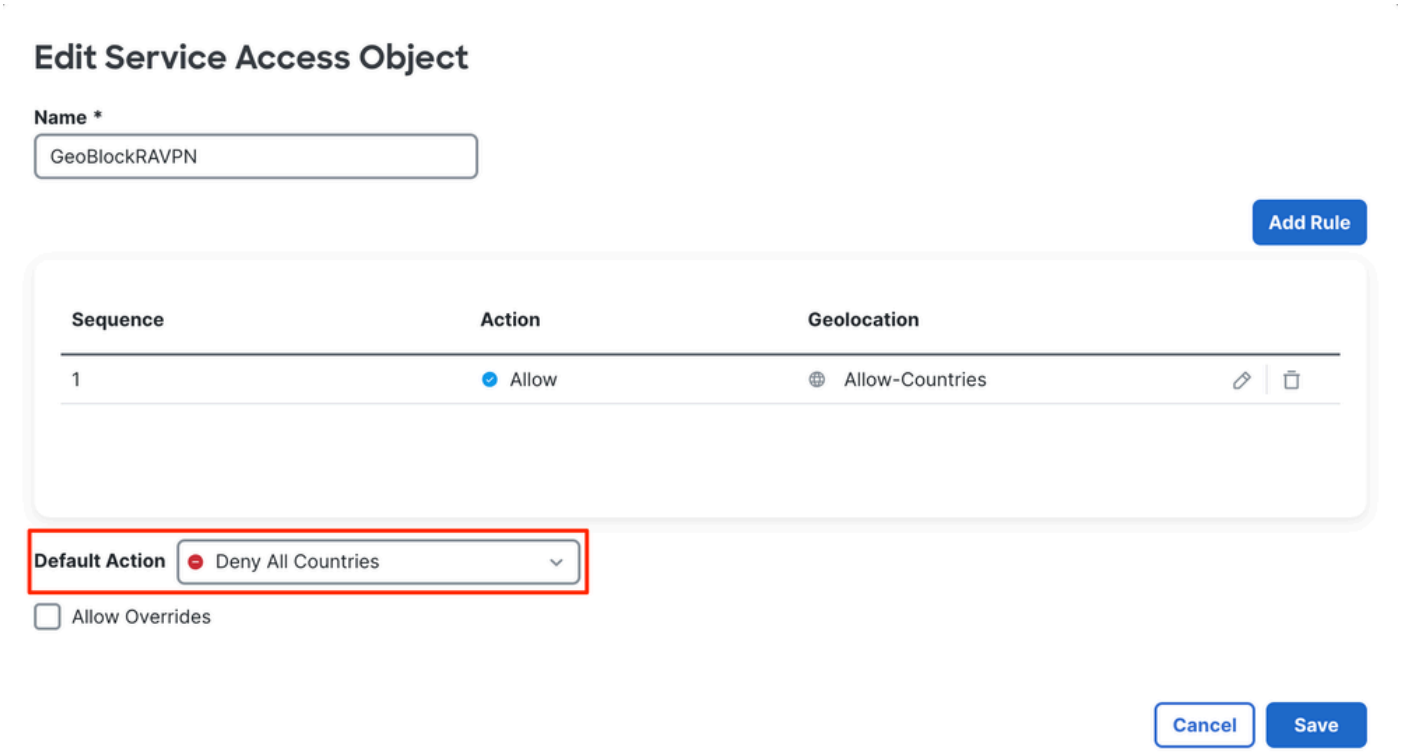
新增到規則中。然後，按一下Add建立規則。

附註：在服務訪問對象中，地理定位對象（國家/地區、大陸或自定義地理定位）只能用於一個規則。

注意：確保以正確的順序配置服務訪問規則，因為這些規則無法重新排序。



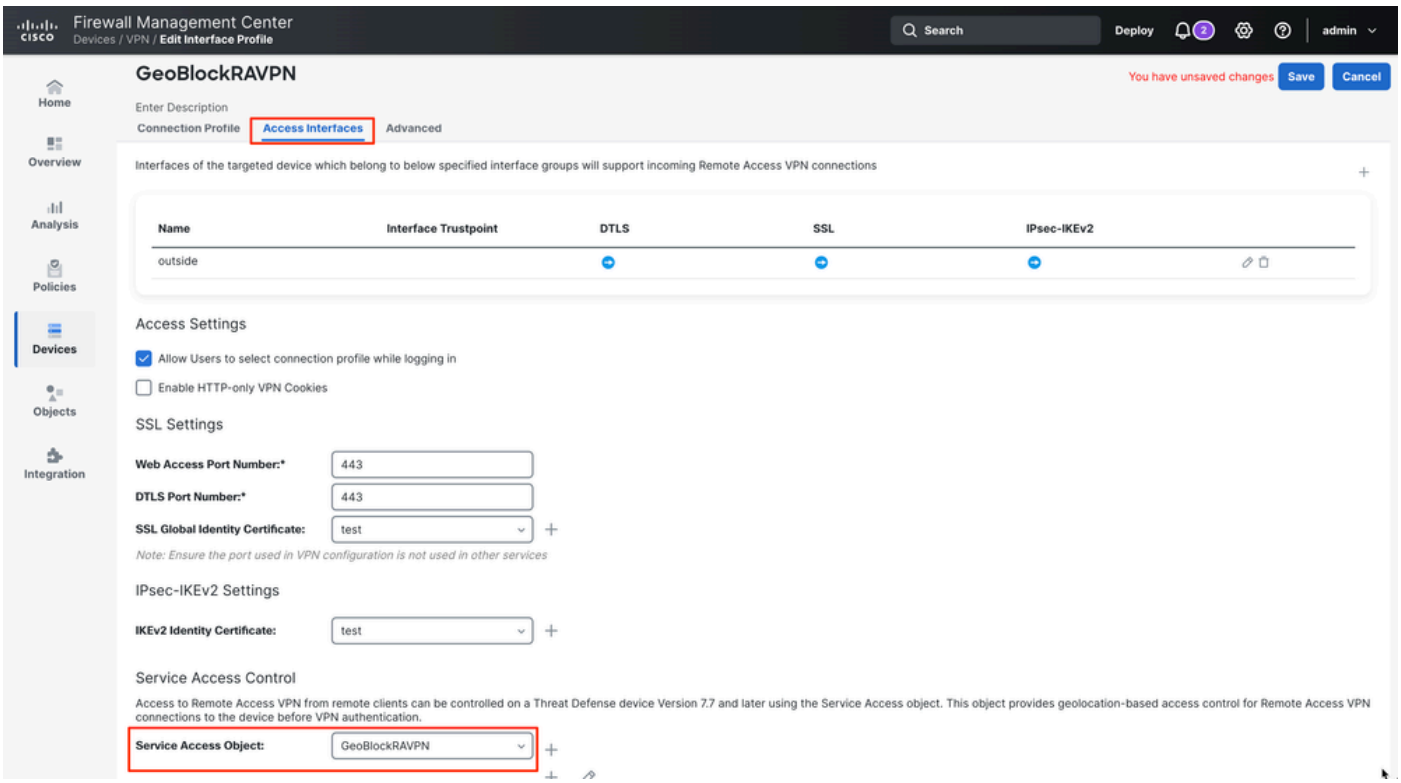
7.將預設操作更改為Deny All Countries，以拒絕來自其他國家的會議請求。



步驟2.應用RAVPN中的服務對象配置。

1.導航到裝置>遠端訪問> RAVPN配置對象>訪問介面中的RAVPN配置。

2.在服務訪問控制部分，選擇之前建立的服務訪問對象。

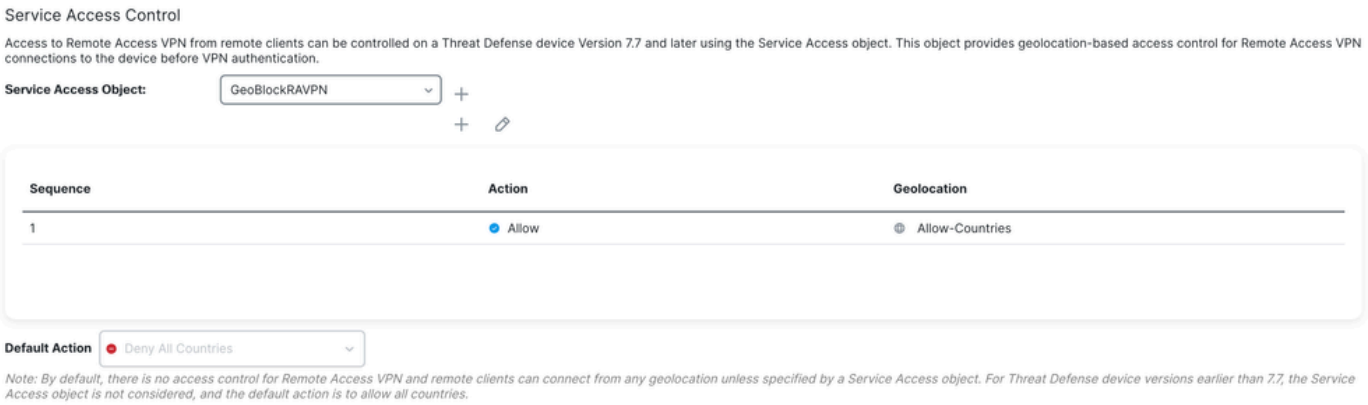


3.您選擇的「服務訪問」對象現在顯示規則摘要和預設操作。

4.最後，儲存變更並部署組態。

驗證

儲存配置後，規則將出現在服務訪問控制部分，允許您驗證哪些組和國家/地區被阻止或允許。



運行 show running-config service-access 命令，以確保服務訪問規則在FTD CLI中可用。

<#root>

```
firepower#
```

show running-config service-access

```
service-access permit ra-ssl-client ra-ikev2 geolocation FMC_GEOLOCATION_8589938211_418243765
service-access deny ra-ssl-client ra-ikev2 geolocation FMC_GEOLOCATION_8589938211_487190092
service-access permit ra-ssl-client ra-ikev2 geolocation any
```

系統日誌和監控

安全防火牆引入新的系統日誌ID來捕獲與基於地理定位的策略阻止的RAVPN連線相關的事件：

- 761031：指示基於地理定位的策略拒絕IKEv2連線的時間。此系統日誌是現有VPN 日誌記錄類的一部分。

%FTD-6-751031:根據基於地域的規則(geo=<country_name>, id=<country_code>)拒絕faddr <client_ip> laddr <device_ip>的IKEv2遠端訪問會話

- 751031：指示基於地理定位的策略拒絕SSL連線的時間。此系統日誌是現有WebVPN日誌記錄類的一部分。

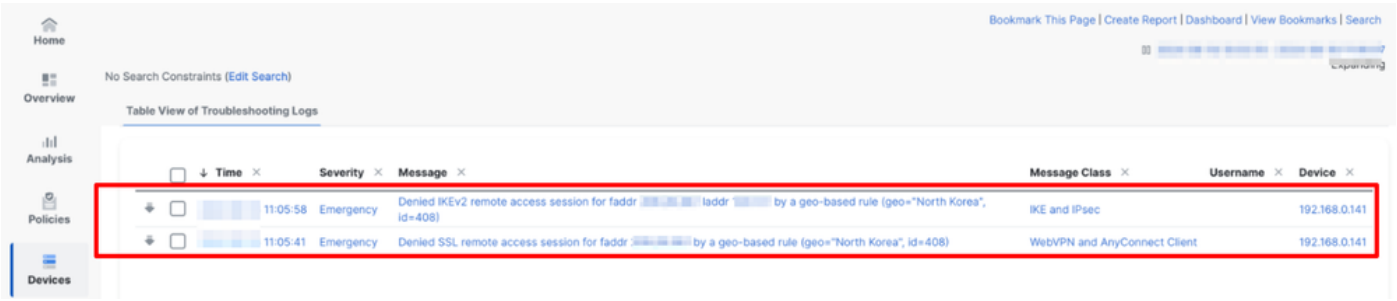
%FTD-6-716166:已拒絕基於地域的規則(geo=<country_name>, id=<country_code>)為faddr <client_ip>提供的SSL遠端訪問會話

附註：從相應的日誌記錄類啟用時，這些新系統日誌的預設嚴重性級別為資訊性。但是，您可以單獨啟用這些系統日誌ID並自定義其嚴重性。

監控被阻止的連線

要驗證阻止的連線，請導航至Devices > Troubleshooting > Troubleshooting日誌。此處顯示與被阻止連線相關的日誌，包括有關影響連線的規則和會話型別的資訊。

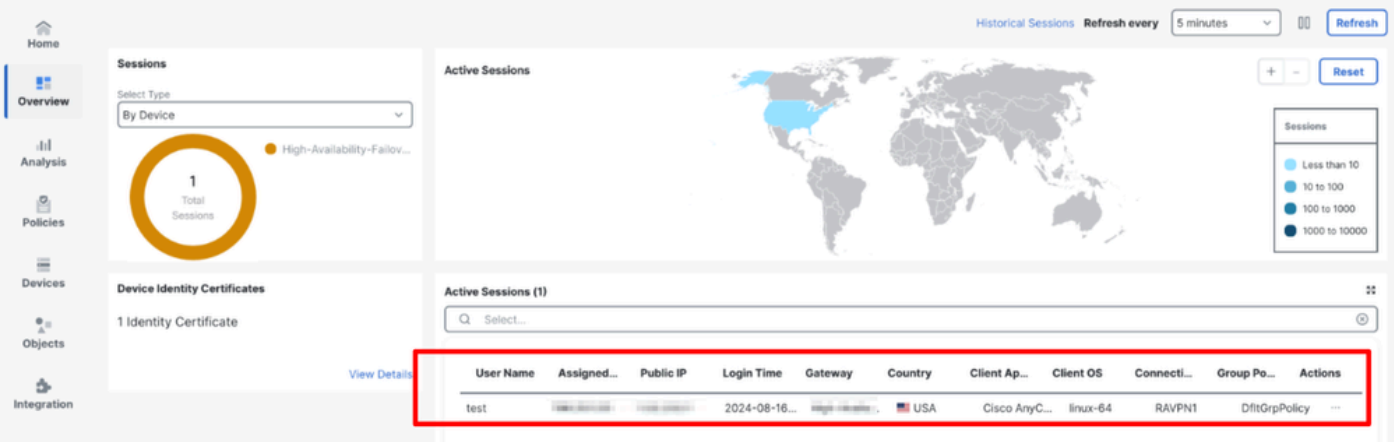
附註：必須將系統日誌配置為在故障排除日誌中收集此資訊。



監控允許的連線

在Overview > Remote Access VPN dashboard中監視允許的會話，其中顯示會話資訊，包括來源國家/地區。

附註：此儀表板中僅顯示來自允許連線的國家和使用者的連線。被拒絕的連線不會顯示在此儀表板中。



疑難排解

為了進行故障排除，請執行以下步驟：

1. 驗證服務訪問對象中是否正確配置了規則。
2. 當允許的地理位置請求會話時，檢查「故障排除日誌」(Troubleshooting Logs)部分中是否顯示拒絕系統日誌。
3. 確保FMC中顯示的組態與FTD CLI中的組態相符。
4. 使用以下命令收集更多詳細資訊，這些資訊對故障排除很有用：

- debug geolocation <1-255>
- show service-access
- show service-access detail
- show service-access interface
- show service-access location
- show service-access service
- show geodb context
- show geodb counters
- show geodb ipv4
- show geodb ipv6

相關資訊

- 如需其他協助，請聯絡TAC。需要有效的支援合約：思科全球支援聯絡人。
- 您還可以在此處訪問Cisco VPN社群。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。