在安全防火牆FTD上啟用威脅檢測的地理定位部署失敗行為

目錄

問題

嘗試在思科安全防火牆FTD 3105上設定基於地理位置的流量過濾時，遇到了幾個問題：

- 基於地域的訪問控制策略(ACP)和預過濾器規則未阻止HTTPS遠端訪問VPN(RA-VPN)連線嘗試阻止區域到FTD外部介面。
- 升級到版本7.7.11後，當策略中包含荷蘭或荷屬安地列斯群島國家/地區時，配置RA-VPN基於地理的服務訪問無法部署。
- FMC部署在83%時失敗，出現以下錯誤消息：

```
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

- 由FMC管理的思科安全防火牆Firepower威脅防禦(FTD)3105
- 升級的軟體版本：7.7.11-1061
- 需要基於國家/地區的訪問限制的RA-VPN配置

解析

解決方案涉及多個步驟，以正確驗證基於地理位置的工作訪問控制。此外，還發現啟用威脅檢測的限制，從而導致就流量匹配行為提供新的指導。

1:將FMC和FTD都升級到版本7.7.11-1061以啟用RA-VPN基於地理的服務訪問功能，因為只有版本7.7.0和更新版本支援此功能。

2:根據思科文檔配置RA-VPN基於地理的服務訪問，並將其與RA-VPN策略相關聯。

3:若要解決在新增特定國家/地區(如荷蘭或荷屬安地列斯)時由於Cisco錯誤ID CSCwq15499而導致的部署失敗，請應用以下解決方法：

1. 建立未配置國家/地區的空白RA-VPN服務訪問對象。
2. 將空白服務訪問對象應用於RA-VPN策略並成功部署。
3. 編輯相同的服務訪問對象並新增所需的國家/地區規則。
4. 重新部署配置 — 部署現在成功，地理位置過濾處於活動狀態。

4:驗證部署是否成功完成，以及RA-VPN訪問和日誌是否反映了預期的國家/地區限制。監控系統以確保地理位置限制按預期運行。

5:判斷是否已在FTD上啟用任何威脅偵測功能，該功能會在流量到達存取原則之前與其相符。此類配置會導致跳過地理定位規則，因為威脅檢測將在策略應用之前接管位置。

<#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:關聯與威脅檢測匹配項和分流項相關的任何系統日誌ID，以確認流量正在進入威脅檢測而不是地理定位。

- %FTD-4-401002:舜補充說：IP_address IP_address port port
- %FTD-4-401003:Shun已刪除：IP_address
- %FTD-4-401004:被避開的資料包：IP_address ==>介面interface_name上的IP_address
- %FTD-4-733102:威脅檢測將主機主機新增到規避清單
- %FTD-4-733103:威脅檢測從規避清單中刪除主機主機
- %FTD-4-733201:威脅檢測：Service[remote-access-client-initiations] Peer[peer-ip]:超出值的故障閾值：正在向介面介面新增shun。SSL:RA客戶端啟動請求過多。
- %FTD-4-733201:威脅檢測：Service[remote-access-client-initiations] Peer[peer-ip]:超出閾值的故障閾值：正在向介面介面新增shun。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

遇到的問題有兩個不同的根本原因：

- 地理定位規則匹配限制：僅從軟體版本7.7.0及更高版本開始支援RA-VPN基於地理的訪問控制。此外，配置的RAVPN威脅檢測可以對流量執行操作，從而阻止其在基於地理的規則上進行匹配。
- 思科錯誤ID CSCwq15499:在7.7.11版中，由於RA-VPN地理服務訪問處理機制中存在已知軟體錯誤，將某些國家/地區新增到RA-VPN基於地理服務的訪問策略時，會出現部署失敗。

相關內容

- 思科技術支援與下載

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）。