# 在FTD上設定基於地理定位的流量封鎖，以進行傳入和傳出流量過濾

## 目錄

## 問題

- 描述在思科安全防火牆威脅防禦(FTD)上根據地理定位攔截流量（針對來自區域的流量和目的地為區域的流量）的最佳方法。
- 問題涉及入站和出站流量過濾是否需要單獨的訪問控制規則，以及在訪問控制規則「網路」(Networks)頁籤下的「地理位置」(Geolocations)頁籤中已經提供了地理位置條目時，是否需要建立其他地理位置對象。

## 環境

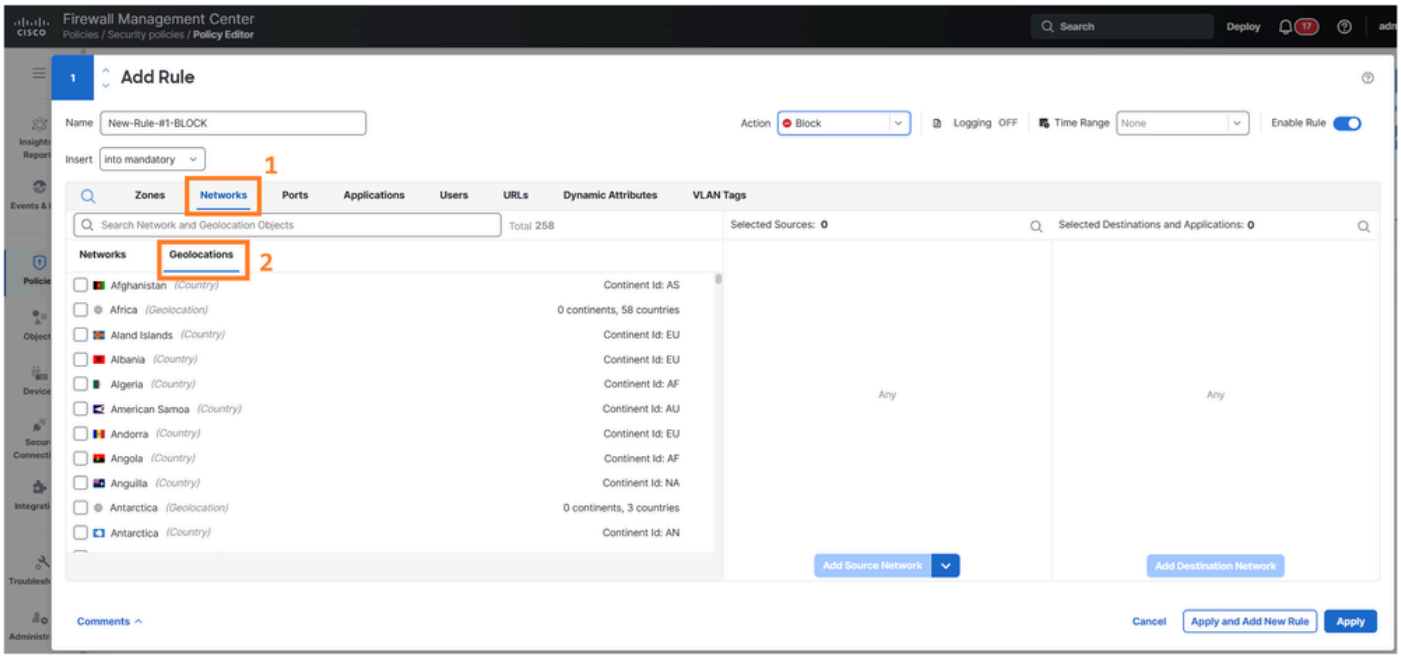
- FTD軟體版本7.1。其他軟體版本也受到影響。
- Cisco Secure Firewall Management Center(FMC)軟體版本7.1。其他軟體版本也會受到影響。

## 解析

使用FMC使用者介面(UI)的「Networks（網路）」頁籤的「Access Control Policy Rule（訪問控制策略規則）」部分中提供的現有地理定位功能，可以有效地管理思科FTD上基於地理定位的流量過濾。 配置方法取決於特定的流量方向和策略要求。

### 訪問地理位置配置

導航到Policies > Security policies > Policy Editor，編輯規則，然後在FMC UI中選擇Networks > Geolocations頁籤。本節中可用的現有地理定位條目可以直接用於建立訪問控制策略，無需單獨的地理定位對象。




## 規則建立策略

規則建立方法因流量方向性和策略目標而異。

用於阻止來自特定地理位置的入站流量

建立訪問控制規則，以識別源自特定地理區域的源流量並應用阻止操作。這些規則必須在規則中適當定位，以確保正確的策略實施。

用於控制到特定地理位置的出站流量

配置訪問控制規則，以識別定向到特定地理區域的目標流量。根據安全策略，可以將它們配置為允許或阻止流向這些目標的流量。

### 單獨的規則要求

實施雙向地理定位過濾時，需要獨立的訪問控制規則，因為：

- 入站篩選需要用於評估源地理定位屬性的規則。
- 出站篩選需要評估目標地理位置屬性的規則。
- 流量方向性決定訪問控制引擎評估哪個地理位置欄位（源或目標）。

具體規則配置取決於網路拓撲、安全要求以及每個地理區域的預期流量控制目標。

## 原因

需要澄清的原因在於基於地理定位的訪問控制實施的複雜性，因為基於流量方向需要不同的規則型別和配置。安全策略訪問控制規則的「網路」(Networks)頁籤中預先存在的地理位置條目的可用性，可能會使策略實施是否需要建立其他對象產生混亂。

## 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）。