使用Firepower管理中心配置髮夾功能

目錄

簡介

必要條件

- 需求
- 採用元件

設定

- 圖表
- 步驟 1.配置外部內部Nat
- 步驟 2.配置內部內部Nat（髮夾型）
- 驗證

疑難排解

- 第1步：NAT規則配置檢查
- 步驟2：存取控制規則(ACL)驗證
- 步驟3：其他診斷

簡介

本檔案介紹使用Firepower管理中心(FMC)在Firepower威脅防禦(FTD)上成功配置髮夾的必要步驟。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower Management Center (FMC)
- Firepówer威脅防禦(FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Firepower管理中心虛擬7.2.4。
- Firepower威脅防禦虛擬7.2.4。

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。

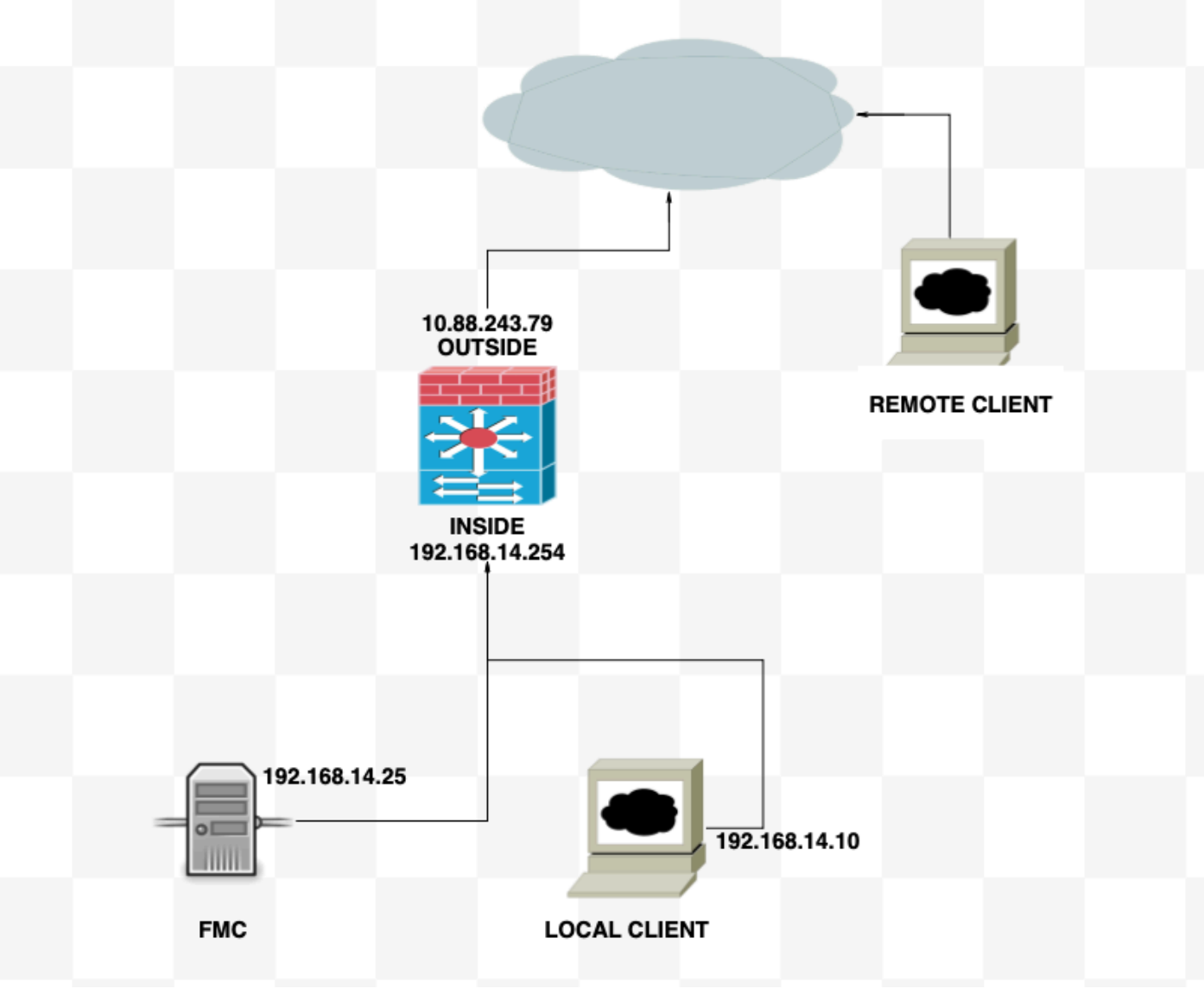
設定

之所以使用髮夾這一術語，是因為來自客戶端的流量會發往路由器（或實施NAT的防火牆），然後在轉換後像髮夾一樣返回到內部網路，以訪問伺服器的專用IP地址。

此功能對於網路服務（如本地網路中的Web託管）非常有用，因為本地網路上的使用者需要使用與外部使用者相同的URL或IP地址訪問內部伺服器。無論請求來自本地網路內部還是外部，它都可以確保資源的統一訪問。

在本範例中，必須透過FTD外部介面的IP存取FMC

圖表

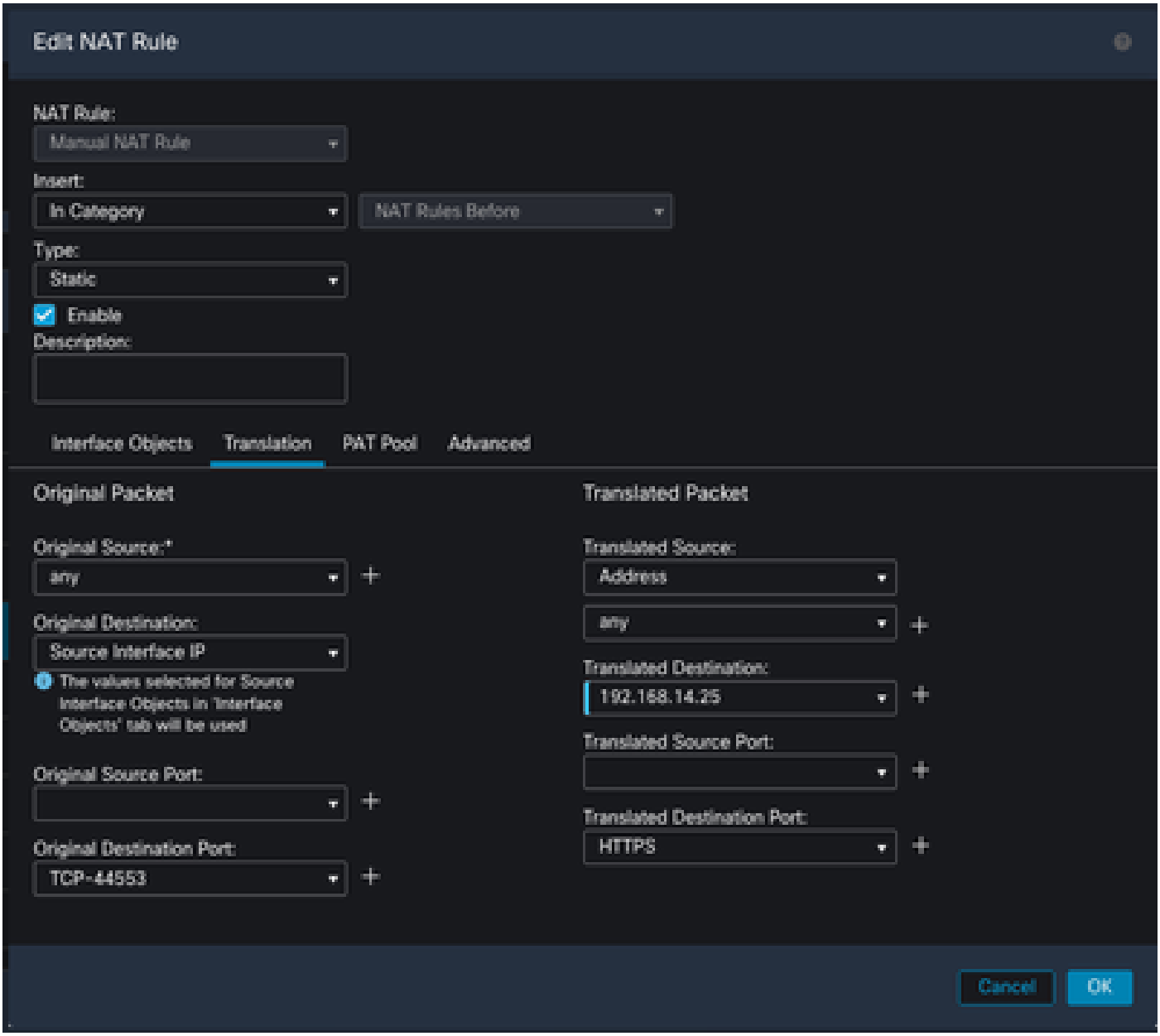


步驟 1.配置外部內部Nat

作為第一步，必須配置靜態NAT；在本示例中，使用外部介面的IP轉換目標IP和目標埠，44553換埠目標。

從FMC導航到裝置> NAT以建立或編輯現有策略，然後按一下增加規則框。

- NAT規則：手動Nat規則
- 原始來源：任意
- 原始目標：源介面IP
- 原始目的地連線埠： 44553
- 轉換後的目的地： 192.168.14.25
- 轉換後的目的埠：443



配置策略。導航到策略>訪問控制建立或編輯現有策略，然後按一下增加規則框。

來源區域：外部

目標區域：內部

源網路：任意

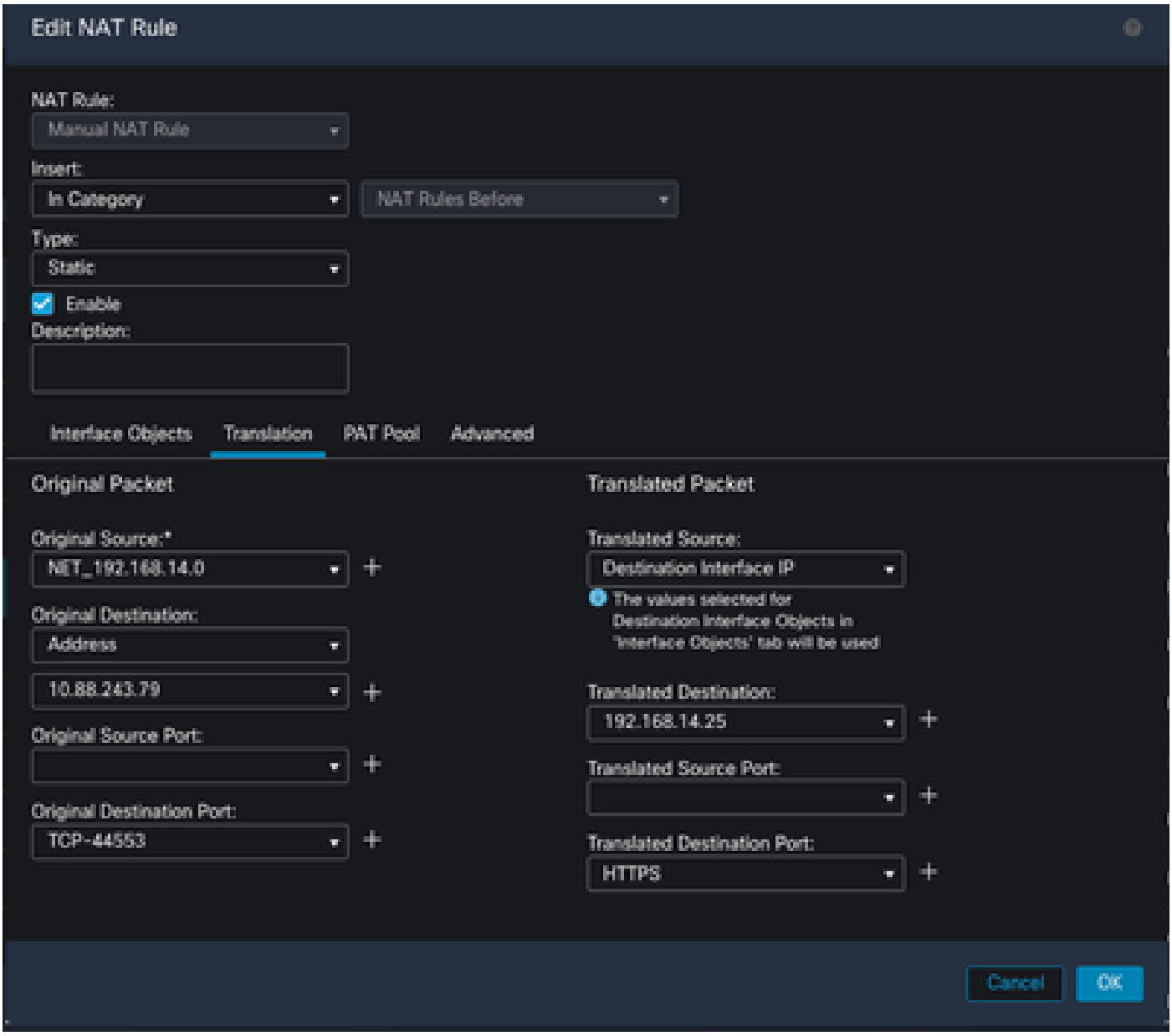
目的網路：10.88.243.79

步驟 2.配置內部內部Nat（髮夾型）

作為第二步，必須從內部配置靜態NAT；在本示例中，使用具有外部介面IP的對象轉換目標IP和目標埠，並且目標埠為44553。

從FMC導航到裝置> NAT以編輯現有策略，然後按一下增加規則框。

- NAT規則：手動Nat規則
- 原始來源： 192.168.14.0/24
- 原始目的地：地址10.88.243.79
- 原始目的地連線埠： 44553
- 轉換後的源：目標介面IP
- 轉換後的目的地： 192.168.14.25
- 轉換後的目的埠：443



配置策略。導航到策略>訪問控制以編輯現有策略，然後按一下增加規則框。

來源區域：任意

目標區域：任意

源網路：192.168.14.0/24

目的網路：10.88.243.79

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks
Mandatory - la primera (1-4)					
1	nat-fmc	OUTSIDE	INSIDE	any	Any
2	Hairpin	Any	Any	NET_192.168.14	10.88.243.79

驗證

從本地客戶端，對目標IP和目標埠執行telnet：

如果出現此錯誤消息「telnet unable to connect to remote host： Connection timed out」（Telnet無法連線到遠端主機：連線超時），則在配置期間的某個時間點出錯。

```
┌──(root💀kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
telnet: Unable to connect to remote host: Connection timed out
```

但如果它顯示Connected，則配置成功。

```
┌──(root💀kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
Connected to 10.88.243.79.
Escape character is '^]'.
```

疑難排解

如果您遇到網路地址轉換(NAT)問題，請使用本分步指南排除常見問題故障。

第1步：NAT規則配置檢查

- 檢視NAT規則：確保所有NAT規則都在FMC中正確配置。檢查源IP地址和目的IP地址以及埠是否正確。
- 介面分配：確認NAT規則中正確分配了源介面和目標介面。不正確的對映會導致無法正確轉換或路由流量。
- NAT規則優先順序：驗證NAT規則是否位於可匹配相同流量的任何其他規則的頂部。FMC中的規則按順序處理，因此放在較高位置的規則具有優先權。

步驟2：存取控制規則(ACL)驗證

- 檢視ACL：檢查訪問控制清單以確保它們適用於允許NAT流量。必須配置ACL才能辨識轉換後的IP地址。
- 規則順序：確保訪問控制清單的順序正確。與NAT規則一樣，ACL是從上到下進行處理，匹配流量的第一個規則是應用的規則。
- 流量許可權：驗證是否存在適當的訪問控制清單，以允許從內部網路到轉換目標的流量。如果缺少規則或規則配置不正確，可能會阻止所需的流量。

步驟3：其他診斷

- 使用診斷工具：利用FMC中提供的診斷工具監控和調試透過裝置的流量。這包括檢視即時日誌和連線事件。
- 重新啟動連線：在某些情況下，現有連線無法辨識對NAT規則或ACL所做的更改，直到它們重新啟動。考慮清除現有連線以強制應用新規則。

從LINA：

```
<#root>

firepower#

 clear xlate
```

- 驗證轉換：如果您使用的是FTD裝置，請在命令列中使用show xlate和show nat等命令來驗證是否正在按預期執行NAT轉換。

從LINA：

```
<#root>

firepower#

 show nat
```

```
<#root>

firepower#

 show xlate
```

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）。