為具有HairPin流量的FTD上的VPN使用者配置內部資源訪問

目錄

問題

目標是在Cisco安全防火牆FTD上使用RADIUS（針對Windows加入域的伺服器）成功進行VPN身份驗證後，使VPN使用者能夠完全訪問內部網路資源。

VPN設定已可操作；使用者可以下載並安裝VPN客戶端並成功進行身份驗證。問題的重點是配置必要的訪問控制和NAT規則以允許通過VPN進行所需的內部資源訪問。

環境

- 產品：思科安全防火牆Firepower(FTD)7.6.0版（如CSF1220CX裝置）
- 管理：Firepower管理中心(FMC)、雲交付的FMC(cdFMC)或Firepower裝置管理器(FDM)
- VPN：配置針對Windows加入域的伺服器(NPS)的RADIUS身份驗證
- VPN地址池：192.168.250.1 - 192.168.250.200
- 目標內部子網示例：192.168.95.0/24
- 軟體版本：9.22.1（在工作流中引用）
- 相關介面：VPN入口的「outside」介面
- 需要通過VPN連線進行RDP和Active Directory訪問

解析

這些步驟詳細說明了允許VPN使用者訪問Cisco FTD上的內部資源（如RDP和Active Directory）所需的配置。這包括建立訪問策略規則、為VPN流量配置NAT豁免和髮夾型NAT，以及使用故障排除命令驗證配置。

第1步：新增訪問清單條目以允許VPN地址池訪問內部資源。

```
access-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: Default Access Control Policy - Mandat
access-list CSM_FW_ACL_ remark rule-id 268438528: L7 RULE: Permit_VPN_Pool
```

第2步：新增訪問清單規則以允許內部資源將返回流量傳送到VPN池：

```
access-list CSM_FW_ACL_ advanced permit ip any object VPN_Pool
```

以後可以對這些規則進行收緊，以根據需要限制特定源和目標。

第3步：為VPN流量配置NAT免除或髮夾型NAT

有兩種常見方法：

- ◦ 選項A:VPN池到內部子網的NAT免除

```
nat (outside,inside) source static VPN_Pool VPN_Pool destination static Net_192.168.95.1-24 Net_192.168
```

- ◦ 選項B：同一介面上VPN池的髮夾NAT(no-proxy-arp)

```
nat (any,any) source static VPN_Pool VPN_Pool no-proxy-arp
```

- ◦ 選項C：外部介面上VPN池的動態髮夾NAT

```
nat (outside,outside) dynamic VPN_Pool interface
```

正確的方法取決於內部資源是位於同一物理介面（要求髮夾型NAT）還是不同介面（NAT免除）。

第4步：使用packet-tracer命令模擬從VPN池到內部資源的流量，並驗證流量是否被預定規則、NAT和路由允許。

```
packet-tracer input outside icmp 192.168.250.1 8 0 192.168.95.1
packet-tracer input outside tcp 192.168.250.1 12345 192.168.95.1 80
packet-tracer input inside icmp 192.168.95.1 8 0 192.168.250.1
packet-tracer input inside tcp 192.168.250.1 54321 192.168.95.1 443
--
Phase 5
ID: 5
Type: ACCESS-LIST
Result: ALLOW
Config: access-group CSM_FW_ACL_ globalaccess-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any r
Additional Information:  This packet will be sent to snort for additional processing where a verdict wi
Elapsed Time: 0 ns
--
Phase 7
ID: 7
Type: NAT
Result: ALLOW
Config: nat (outside,outside) dynamic VPN_Pool interface
Additional Information: Static translate 192.168.250.1/12345 to 192.168.250.1/12345 Forward Flow based
Elapsed Time: 0 ns
```

注意：WebVPN階段的Packet Tracer輸出可能對外部介面上的VPN流量顯示「DROP」。這是外部介面上的純文字檔案流量的預期行為，仍可用於驗證NAT。

其他注意事項:

- 威脅防禦UI中的資料包捕獲可能只顯示傳入請求。如果未觀察到丟包，但流量未到達內部資源，請檢查NAT和訪問清單規則。
- 當SSH不可用時，可通過cdFMC中的威脅防禦UI功能執行所有故障排除，但命令使用受到限制。
- 可能需要對相鄰裝置進行某些修改才能實現端到端連線。

原因

根本原因是VPN到內部和內部到VPN池流量的訪問策略和NAT配置不足。預設配置不允許從VPN池到內部資源進行完全雙向通訊並返回，也不處理在同一介面上流量傳入和傳出的髮夾型NAT要求。

相關內容

- 在FTD上設定NAT豁免
- 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）。