排除CSF CLI上的流量問題

目錄

簡介

本文說明如何使用Cisco Secure Firewall CLI驗證路由、資料包流和Snort行為，從而排除流量問題。

必要條件

本文件沒有特定需求。

需求

思科建議您瞭解以下主題：

- Firepower管理中心(FMC)策略和對象配置
- 思科安全防火牆(CSF)路由和介面邏輯
- 資料包檢測和防火牆故障排除概念

採用元件

本檔案所述內容不限於CSF的特定軟體和硬體版本。文檔中使用的裝置運行代碼7.6.5。

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。

相關產品

本文件也適用於以下硬體和軟體版本：

- 安全防火牆管理中心(FMC)
- 思科安全防火牆(CSF)
- Firepower威脅防禦CLI工具

重要資訊

當裝置遇到較高的CPU、記憶體或I/O利用率時，執行故障排除命令可能會加劇效能降級。建議首先調查並解決資源耗盡情況，然後進行流量問題診斷。診斷命令會消耗額外的系統資源，從而進一步降低可用性並延長恢復時間。

背景資訊

CSF上的流量故障排除通常從確認資料包必須通過防火牆的邏輯路徑開始。一旦瞭解路由和介面對映，下一步是將預期路徑與實際資料包流進行比較。這可以通過路由查詢、Packet Tracer模擬、資料包捕獲和Snort引擎跟蹤來執行。

每個工具都提供不同層次的可視性：

- show route可確認資料包的路由路徑和介面標識。
- packet Tracer模擬流量並識別ACL、NAT和介面決策。
- 封包擷取會檢查穿越防火牆的即時流量。
- 系統支援跟蹤公開了對策略相關塊或檢查事件的Snort決策。

提示：在捕獲流量之前，先進行路由和Packet Tracer驗證，這樣您就可以在分析即時流量之前，確認預期的路徑和訪問控制決策是否正確。

問題

流量未按預期工作，管理員需要確定資料包是否採用正確的路徑、防火牆是否允許或拒絕連線，以及Snort或策略檢查是否阻止流量。

步驟 1:查詢路由

確定路由路徑並確定與源IP地址和目標IP地址關聯的邏輯介面名稱。大多數故障排除命令都需要邏輯介面名稱，因此這必須是故障排除工作流程的第一步。

對源和目標IP地址運行命令：

```
show route <IP>
```

依賴預設路由的網際網路目標流量需要標識邏輯輸出介面。可通過執行以下步驟來確定邏輯介面名稱：

```
show route 0.0.0.0
```

輸出示例：

```
FTD1# show route 192.168.0.11

Routing entry for 192.168.0.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:

    directly connected, via Inside
    Route metric is 0, traffic share count is 1
```

```
FTD1# show route 0.0.0.0

Routing entry for 0.0.0.0 0.0.0.0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:

    128.107.0.1, via Outside
```

```
    Route metric is 0, traffic share count is 1
```

在本例中，邏輯輸入介面為Inside，輸出介面為Outside。

⚠ 注意：網路地址轉換(NAT)可以通過不同的介面重定向流量，路由表顯示NAT策略何時與流量匹配。排除連線故障時，請驗證NAT配置是否與預期流量路徑一致。

🔍 提示：邏輯介面名稱用於CLI故障排除命令。請注意邏輯名稱以供將來參考。

步驟 2:運行Packet Tracer

使用Packet Tracer模擬防火牆如何評估特定流量。此工具可幫助確認使用哪些介面、是否應用了NAT策略，以及ACL是否允許或拒絕流量。

使用以下命令語法：

```
packet-tracer input <source interface> <protocol> <source IP> <source port> <destination IP> <destinati
```

命令範例：

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443
```

檢視輸出以確認資料包是否遵循預期路徑並在模擬過程中被允許。當您在參與即時資料包分析之前需要確定問題是否與路由、NAT或策略匹配有關時，這很有用。

Packet Tracer中的transmit關鍵字導致模擬資料包被注入入口介面，使其能穿越所有防火牆處理階段，而不是作為模擬保留。

命令範例：

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443 transmit
```

步驟 3:運行捕獲

使用資料包捕獲檢查通過防火牆的即時流量。封包擷取與Packet Tracer不同，因為它們擷取實際流量，因此必須匹配擷取處於作用中時穿越防火牆的真實流量。資料包捕獲是雙向的，記錄連線的兩端。

對於大多數流量疑難排解案例，請設定以下擷取：

- 輸入擷取 — 擷取到達來源端介面的流量
- 輸出擷取 — 擷取目的地端介面上傳出的流量
- ASP Drop Capture — 捕獲防火牆丟棄的資料包並匹配配置的標準

常規捕獲語法：

```
capture <name> interface <interface name> trace match ip host <source IP> host <destination IP>
```

輸入擷取範例：

```
FTD1# capture in interface trace Inside match ip host 192.168.0.11 host 72.163.4.161
```

輸出捕獲示例：

```
FTD1# capture out interface trace Outside match ip host 128.107.0.22 host 72.163.4.161
```

ASP放置捕獲示例：

```
FTD1# cap asp type asp-drop match ip host 192.168.0.11 host 72.163.4.161
```

資料包捕獲是雙向的，這意味著可以根據定義的匹配條件捕獲轉發和返回流量。追蹤功能可顯示防火牆對實際流量所做的決策。

注意：如果正在執行NAT，則出口捕獲必須使用轉換後的源IP，而不是原始源IP，才能正確捕獲NAT後的流量。

步驟 4:運行系統支援跟蹤

使用系統支援跟蹤檢視特定流量的即時Snort檢測流程。當流量與ACL允許規則匹配，但仍被策略檢測阻止時，此功能尤其有用。標準封包擷取顯示封包遭封鎖，但系統支援追蹤軌跡可清楚瞭解為什麼以這種方式處理封包。系統支援跟蹤是雙向的，這意味著它接收來自兩端的流量。這表示將IP新增到工具中的順序並不重要。

運行此命令並響應提示：

```
> system support trace


Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 72.163.4.161
Please specify a server port: 443
```

當環境使用應用程式或URL規則、基於身份的規則、檔案策略或入侵策略時，此工具尤其有用。在ACL匹配之後會評估這些功能，因此訪問控制策略可以允許資料包通過，但Snort檢測仍會阻止該資料包。

附註：如果確切的源埠未知，則客戶端埠可以留空。

驗證

同時使用路由查詢、Packet Tracer模擬、資料包捕獲和系統支援跟蹤的輸出來確認流量行為。目標是確定資料包是否選擇正確的路徑、防火牆是允許還是拒絕，以及Snort是否基於更深入的檢查阻止資料包。

完整的故障排除流程通常會確認：

- 路由查詢顯示邏輯入口和出口介面。
- Packet Tracer確認預期的轉發路徑和策略評估。
- 封包擷取會確認流量是否如預期到達和離開。
- 系統支援跟蹤可確認Snort或策略檢查是否導致阻止。

疑難排解

當流量問題持續存在時，請檢視以下方面：

- 檢查路由查詢是否與預期的源介面和目標介面匹配。
- 驗證Packet Tracer輸出是否顯示ACL或NAT階段被拒絕的流量。
- 檢視輸入和輸出封包擷取，確認流量是否到達防火牆並在正確的介面上離開。
- 使用ASP丟棄捕獲確認防火牆是否在內部丟棄流量。
- 在ACL允許決定之後，使用系統支援跟蹤確定Snort是否正在阻止流量。

相關資訊

- 分析Firepower防火牆捕獲以排除網路故障
- 使用Firepower威脅防禦捕獲和Packet Tracer

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）。