檢測Firepower裝置上的大象流

目錄

簡介

本檔案介紹如何在Cisco Firepower威脅防禦(FTD)環境中執行大象流量偵測。

必要條件

需求

思科建議您瞭解以下產品：

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- Netflow

採用元件

本文檔中的資訊基於運行軟體版本7.1或更高版本的FMC。 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。

背景資訊

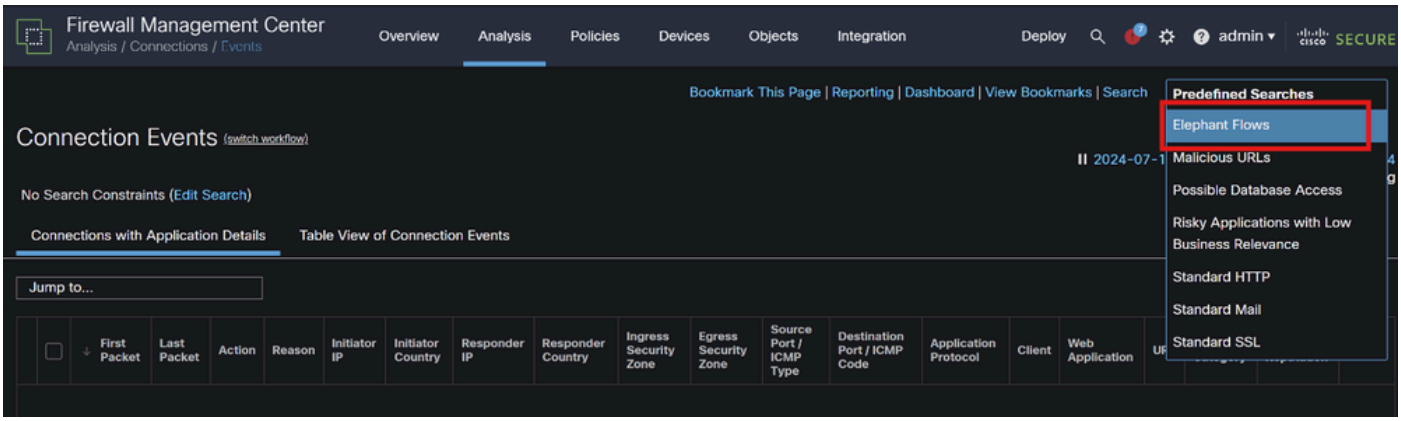
Cisco Firepower中的大象流檢測對於確定和管理可能佔用大量網路資源並影響效能的大型長期流至關重要。大象流可能發生在資料量大的應用程式中，如影片流、大型檔案傳輸和資料庫複製。可使用以下方法辨識此問題：

方法

1. 使用FMC

大象流量檢測在版本7.1中引入。7.2版允許更輕鬆的定製，並提供繞過甚至限制大象流量的選項。從7.2.0版開始，對於Snort 3裝置，智慧應用旁路(IAB)已作廢。

您可以在分析>連線>事件>預定義搜尋>大象流下檢測大象流。



連線事件

本文檔提供在訪問控制策略上配置大象流的分步過程

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72/elephant-flow.html#task_sxp_h2d_jsb

2. 使用CLI

a. Snort例項CPU尖峰也表示網路正在處理Elephant流，可使用以下命令辨識該流：

show asp inspect-dp snort

以下是指令輸出的範例。

> show asp inspect-dp snort

SNORT檢查例項狀態資訊Id Pid

Cpu-Usage Conns Segs/Pkts Status tot (使用者 | sys)

— ----- ---------- ---------- ---------- ----------

0 16450 8% (7%| 0%) 2,200就緒

1 16453 9% (8%| 0%) 2,200就緒

2 16451 6% (5%| 1%) 23000就緒

3 16454 5% (5%| 0%) 2.2 K 1就緒

4 16456 6% (6%| 0%) 23000就緒

5 16457 6% (6%| 0%) 23000就緒

6 16458 6% (5%| 0%) 2.2 K 1就緒

7 16459 4% (4%| 0%) 23000就緒

8 16452 9% (8%| 1%) 2200就緒

9 16455 100% (100%| 0%) 2.2 K 5 READY <<<< HIGH CPU utilization 10 16460 7% (6%| 0%) 2,200就緒

— ----- ---------- ---------- ---------- ----------

摘要15% (14%| 0%) 24.6 K 7

b.此外，根模式的「top」命令輸出也有助於檢查任何Snort例項是否升高。

c.使用此命令導出連線詳細資訊，以檢查透過防火牆的最大流量。

show asp inspect-dp snort

show conn detail | redirect disk0：/con-detail.txt

可以在Linux模式下的「/mnt/disk0」下找到該檔案。將相同內容複製到**/ngfw/var/common**以從FMC下載該文檔。

專家cp

/mnt/disk0/<檔名> /ngfw/var/common/

下面是連線詳細資訊輸出的示例。

UDP內部：10.x.x.x/137 inside：10.x.x.43/137，標誌- N1，空閒0，正常運行時間6D2h，超時2m0，位元組123131166926<<< 123 GB，正常運行時間似乎為6天2小時

連線查詢關鍵字ID： 2255619827

UDP內部：10.x.x.255/137 inside：10.x.x.42/137，標誌- N1，空閒0s，正常運行時間7D5h，超時2m0s，位元組116338988274

連線查詢關鍵字ID： 1522768243

UDP內部：10.x.x.255/137 inside：10.x.x.39/137，標誌- N1，空閒0，正常運行時間8D1h，超時2m0，位元組60930791876

連線查詢關鍵字ID： 1208773687

UDP內部：10.x.x.255/137 inside：10.x.x0.34/137，標誌- N1，空閒0，正常運行時間9D5h，超時2m0，位元組59310023420

連線查詢關鍵字ID： 597774515

3. 使用Netflow

大象流是會影響網路效能的大流量流量。檢測這些流量涉及監控網路流量，以辨識指示大型、持續流量的模式。Cisco Firepower提供檢測和分析網路流量（包括大象流量）的工具和功能。NetFlow工具可幫助收集IP流量資訊以進行監控。

本文檔提供在FMC上配置NetFlow策略的分步過程

https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-management-center-virtual/221612-htz-01-2024-configure-netflow-in-fmc.html

使用NetFlow收集器和分析器（例如：Cisco Stealthwatch、SolarWinds或任何其他NetFlow分析工具）來分析收集的資料。一旦大象流動得到確認，您可以採取措施減輕其影響：

- 流量整形和QoS：實施服務品質(QoS)策略，確定流量的優先順序並限制大象流量的頻寬。
- 訪問控制策略：建立訪問控制策略以管理和限制大象流。
- 分段：使用網路分段隔離大流量流量並將它們對網路其餘部分的影響降至最低。
- 負載均衡：實施負載均衡，以便在網路資源之間更平均地分配流量。

4. 持續監測和調整

定期監控網路流量以檢測新的大象流量，並根據需要調整策略和配置。

透過此過程，您可以有效檢測和管理Cisco Firepower部署中的大象流，從而確保更好的網路效能和資源利用率。

相關資訊

Cisco安全防火牆管理中心裝置配置指南7.2

在FMC中配置NetFlow

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）。