在軟體上配置和捕獲嵌入式資料包

目錄

簡介

本檔案介紹Cisco IOS®軟體中的嵌入式封包擷取(EPC)功能。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS版本12.4(20)T或更高版本
- Cisco IOS XE®版本15.2(4)S - 3.7.0或更高版本

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

啟用時，路由器會捕獲已傳送和已接收的資料包。這些資料包儲存在DRAM中的緩衝區中，不會持續進行重新載入。一旦捕獲了資料，就可以在路由器的摘要或詳細檢視中檢視它。

此外，資料可以匯出為資料包捕獲(PCAP)檔案以供進一步檢查。該工具在exec模式下配置，被視為臨時輔助工具。因此，該工具配置不儲存在路由器配置中，並且在系統重新載入後不會保持不變。

思科客戶可使用Packet Capture Config Generator and Analyzer工具來協助配置、捕獲和提取資料包捕獲。

Cisco IOS配置示例

基本EPC配置

1. 定義「capture buffer」（捕獲緩衝區），它是儲存捕獲資料包的臨時緩衝區。
2. 定義緩衝區時，可選擇各種選項；例如大小、最大資料包大小和循環/線性：

```
monitor capture buffer BUF size 2048 max-size 1518 linear
```

3. 過濾器適用於將捕獲限製為所需流量。在設定模式下定義存取控制清單(ACL)，並將過濾器套用到緩衝區：

```
ip access-list extended BUF-FILTER
permit ip host 192.168.1.1 host 172.16.1.1
permit ip host 172.16.1.1 host 192.168.1.1

monitor capture buffer BUF filter access-list BUF-FILTER
```

4. 定義用於定義捕獲發生位置的捕獲點。
5. 捕獲點還定義捕獲是用於IPv4還是IPv6，以及交換路徑（進程與cef）位於哪個位置：

```
monitor capture point ip cef POINT fastEthernet 0 both
```

6. 將緩衝區附加到捕獲點：

```
monitor capture point associate POINT BUF
```

7. 開始捕獲：

```
monitor capture point start POINT
```

8. 捕獲現在處於活動狀態。允許收集必要資料。

9. 停止捕獲：

```
monitor capture point stop POINT
```

10. 檢查裝置上的緩衝區：

```
show monitor capture buffer BUF dump
```

附註：此輸出僅顯示資料包捕獲的十六進位制轉儲。為了便於閱讀，有兩種方式。從路由器匯出緩衝區以進行進一步分析：

```
monitor capture buffer BUF export tftp://10.1.1.1/BUF.pcap
```

因為需要通過T/FTP訪問路由器，所以上述方法並不總是切實可行。在這種情況下，請製作十六進位制轉儲的副本，並使用任何線上十六進位制轉換器來檢視檔案。

11. 收集完必要的資料後，刪除「捕獲點」和「捕獲緩衝區」：

```
no monitor capture point ip cef POINT fastEthernet 0 both
no monitor capture buffer BUF
```

其他Cisco IOS配置資訊

- 在低於Cisco IOS®版本15.0(1)M的版本中，緩衝區大小限製為512K。
- 在低於Cisco IOS®版本15.0(1)M的版本中，捕獲的資料包大小限製為1024位元組。
- 封包緩衝區儲存在DRAM中，不會透過重新載入而存留。
- 擷取組態不會儲存在NVRAM中，也不會在重新載入過程中存留。
- 可以定義捕獲點以在cef或進程交換路徑中捕獲。
- 捕獲點可以定義為僅在介面上或全域性捕獲。
- 當以PCAP格式匯出捕獲緩衝區時，不會保留第2層資訊（如乙太網封裝）。
- 有關本節中使用的命令的詳細資訊，請參閱搜尋命令的最佳實踐。

基本IP流量匯出配置

IP流量匯出是一種不同的方法，用於匯出在多個同時的WAN或LAN介面上接收的IP資料包。

1.在配置模式下，定義IP流量匯出配置檔案。

```
Device(config)# ip traffic-export profile mypcap mode capture
```

2.在配置檔案中配置雙向流量。

```
Device(config-rite)# bidirectional
```

3.退出

4.為匯出的流量指定介面。

```
Device(config-if)# interface GigabitEthernet 0/1
```

5.啟用介面上的IP流量匯出。

```
Device(config-if)# ip traffic-export apply mypcap size 10000000
```

6.退出

7.開始捕獲。捕獲現在處於活動狀態。允許收集必要資料。

```
Device# traffic-export interface GigabitEthernet 0/1 start
```

8.停止捕獲。

```
Device# traffic-export interface GigabitEthernet 0/1 stop
```

9.將捕獲匯出到外部TFTP伺服器。

```
Device# traffic-export interface GigabitEthernet 0/1 copy tftp://<TFTP_Address>/mypcap.pcap
```

10.收集完必要的資料後，刪除配置檔案。

```
Device(config)# no ip traffic-export profile mypcap
```

IP流量匯出缺點

與EPC方法相比，IP流量匯出具有以下缺點：

- 匯出捕獲流量的介面必須是乙太網介面。
- 不支援IPv6。
- 沒有第2層資訊，只有第3層及更高層。

Cisco IOS-XE配置示例

嵌入式封包擷取功能是在Cisco IOS-XE® 3.7 - 15.2(4)S版中匯入。擷取的組態與Cisco IOS®不同，因為它新增了更多功能。

基本EPC配置

1. 定義捕獲發生的位置：

```
monitor capture CAP interface GigabitEthernet0/0/1 both
```

2. 關聯篩選器。過濾器指定為內聯，或者可以引用ACL或類對映：

```
monitor capture CAP match ipv4 protocol tcp any any limit pps 1000000
```

3. 開始捕獲：

```
monitor capture CAP start
```

4. 捕獲現在處於活動狀態。允許它收集必要資料。

5. 停止捕獲：

```
monitor capture CAP stop
```

6. 在摘要檢視中檢查捕獲：

```
show monitor capture CAP buffer brief
```

7. 在詳細檢視中檢查捕獲：

```
show monitor capture CAP buffer detailed
```

8. 此外，以PCAP格式匯出捕獲以供進一步分析：

```
monitor capture CAP export tftp://10.0.0.1/CAP.pcap
```

9. 收集完必要的資料後，請刪除捕獲：

```
no monitor capture CAP
```

其他資訊

- 捕獲在物理介面、子介面和隧道介面上執行。
- 基於網路應用識別(NBAR)的過濾器(使用 **match protocol** 目前不支援class-map)下的命令。
- 有關本節中使用的命令的詳細資訊，請參閱搜尋命令的最佳實踐。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

對於在Cisco IOS-XE®上運行的EPC，此debug命令用於確保EPC設定正確：

```
debug epc provision
debug epc capture-point
```

相關資訊

- 內嵌式封包擷取 — Cisco IOS-XE
- 內嵌式封包擷取 — Cisco IOS
- 技術支援與文件 - Cisco Systems

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）。