

在Firepower裝置上使用資料包捕獲過程

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[捕獲資料包的步驟](#)

[複製Pcap檔案](#)

簡介

本文說明如何使用tcpdump命令擷取Firepower裝置的網路介面所看到的封包。

必要條件

需求

思科建議您瞭解Cisco Firepower裝置和虛擬裝置型號。

採用元件

本文件所述內容不限於特定軟體和硬體版本。此指令使用Berkeley封包過濾器(BPF)語法。

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。

 **警告：**如果在生產系統上運行tcpdump命令，可能會影響網路效能。

捕獲資料包的步驟

登入到Firepower裝置的CLI。

在6.1及更新版本中，輸入capture-traffic。例如，

```
<#root>
```

```
> capture-traffic
```

```
Please choose domain to capture traffic from:  
0 - eth0  
1 - Default Inline Set (Interfaces s2p1, s2p2)
```

在6.0.x.x及更低版本中，輸入system support capture-traffic。例如，

```
<#root>
```

```
> system support capture-traffic
```

Please choose domain to capture traffic from:

0 - eth0

1 - Default Inline Set (Interfaces s2p1, s2p2)


進行選擇後，系統會提示您輸入選項：

Please specify tcpdump options desired.

(or enter '?' for a list of supported options)

Options:


為了從資料包中捕獲足夠的資料，必須使用-s選項來正確設定長度。可將長度設定為與介面集配置的已配置最大傳輸單元(MTU)值（預設為1518）匹配的值。

 **警告：**捕獲到螢幕的流量時，可能會降低系統和網路的效能。思科建議您將 `-w <filename>` 選項與tcpdump命令配合使用。將封包擷取到檔案。如果運行不帶-w 選項的命令，請按Ctrl-C組合鍵退出。

-w <filename>選項示例：

```
<#root>
```

```
-w capture.pcap -s 1518
```

 **注意：**指定資料包捕獲(pcap)檔名時，不要使用任何路徑元素。您只能指定要在裝置中建立的pcap檔名。

如果希望捕獲有限數量的資料包，可以使用 `-c <packets>` 標誌來指定要捕獲的資料包數量。例如，若要準確擷取5000個封包：

```
<#root>
```

```
-w capture.pcap -s 1518 -c 5000
```

此外，可以在命令末尾新增BPF過濾器，以限制捕獲的資料包。例如，若要將封包擷取限制為來源或目的地IP位址為192.0.2.1的5000個封包，可以使用以下選項：

```
<#root>
```

```
-w capture.pcap -s 1518 -c 5000 host 192.0.2.1
```

擷取已標籤的虛擬LAN(VLAN)流量時，必須使用BPF語法指定VLAN。否則，pcap不包含任何VLAN標籤的封包。例如，此範例將擷取限制為從192.0.2.1標籤VLAN的流量：


```
<#root>
```

```
-w capture.pcap -s 1518 -c 5000 vlan and host 192.0.2.1
```

如果您不確定流量是否具有VLAN標籤，則可以使用以下語法來擷取來自192.0.2.1的流量，此流量是且不是VLAN標籤：

```
<#root>
```

```
-w capture.pcap -s 1518 -c 5000 'host 192.0.2.1 or (vlan and host 192.0.2.1)'
```


 註：在上一個示例中，需要使用括弧，以便「or」不僅適用於「vlan」。然後需要單引號以防止外殼程式對圓括弧的任何可能的誤解。

指定VLAN標籤會捕獲與您的BPF其餘部分匹配的所有VLAN流量。但是，如果要捕獲特定VLAN標籤，可以指定要捕獲的VLAN標籤，如下所示：

```
<#root>
```

```
-w capture.pcap -s 1518 -c 5000 vlan 1 and host 192.0.2.1
```

指定所需的選項並按Enter後，tcpdump開始捕獲流量。

 提示：如果未使用 — c選項，請按Ctrl-C組合鍵停止捕獲。

一旦停止捕獲，您將收到確認。舉例來說：

```
<#root>
```

```
Please specify tcpdump options desired.
```

(or enter '?' for a list of supported options)

Options:

```
-w capture.pcap -s 1518 -c 5000 host 192.0.2.1
```

Cleaning up.

Done.


複製Pcap檔案

若要將pcap檔案從FirePOWER裝置複製到接受入站SSH連線的另一個系統，請使用以下命令：

```
<#root>
```

```
> system file secure-copy hostname username destination_directory pcap_file
```

按下Enter後，系統會提示您輸入遠端系統的密碼。可在整個網路中複製檔案。

 註：在本示例中，主機名是指目標遠端主機的名稱或IP地址，使用者名稱指定遠端主機上的使用者名稱，destination_directory指定遠端主機上的目標路徑，pcap_file指定用於傳輸的本地pcap檔案。

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）。