內容安全裝置常見問題：如何在思科內容安全裝置上執行資料包捕獲？

目錄

簡介

本檔案介紹如何在思科內容安全裝置上執行封包擷取。

必要條件

需求

思科建議您瞭解以下主題：

- 思科電子郵件安全裝置(ESA)
- 思科網路安全裝置(WSA)
- 思科安全管理裝置(SMA)
- AsyncOS

採用元件

本文檔中的資訊基於AsyncOS的所有版本。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

如何在思科內容安全裝置上執行資料包捕獲？

完成以下步驟，以便使用GUI執行封包擷取(**tcpdump**命令):

1. 在GUI上導覽至**Help and Support > Packet Capture**。
2. 根據需要編輯資料包捕獲設定，例如運行資料包捕獲的網路介面。可以使用預定義過濾器之一，也可以使用Unix tcpdump命令支援的任何語法建立自定義**過濾**器。
3. 按一下「**Start Capture**」以開始捕獲。
4. 按一下「**Stop Capture**」以結束擷取。
5. 下載資料包捕獲。

完成以下步驟，以便使用CLI執行封包擷取(**tcpdump** 命令):

1. 在CLI中輸入以下命令：

```
wsa.run> packetcapture

Status: No capture running


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     (tcp port 80 or tcp port 3128)
```

2. 選擇要執行的操作：

```
- START - Start packet capture.

- SETUP - Change packet capture settings.

[]> setup
```

3. 輸入捕獲檔案允許的最大大小(MB):

```
[200]> 200

Do you want to stop the capture when the file size is reached? (If not, a new
 file will be started and the older capture data will be discarded.)

[N]> n

The following interfaces are configured:

1. Management

2. T1

3. T2
```

4. 輸入要從中捕獲資料包的一個或多個介面的名稱或編號，用逗號分隔：

```
[1]> 1
```

5. 輸入要用於捕獲的過濾器。輸入單詞CLEAR以清除過濾器並擷取選定介面上的所有封包。

```
[(tcp port 80 or tcp port 3128)]> host 10.10.10.10 && port 80

Status: No capture running

Current Settings:
 Max file size:      200 MB
 Capture Limit:      None (Run Indefinitely)
 Capture Interfaces: Management
 Capture Filter:     host 10.10.10.10 && port 80
```

6. 選擇start操作以開始捕獲：

```
- START - Start packet capture.
- SETUP - Change packet capture settings.
[]> start

Status: Capture in progress (Duration: 0s)
File Name: S650-00137262569A-8RVFDB1-20080919-174302.cap (Size: 0K)

Current Settings:
 Max file size:      200 MB
 Capture Limit:      None (Run Indefinitely)
 Capture Interfaces: Management
 Capture Filter:     host 10.10.10.10 && port 80
```

7. 選擇stop操作以結束捕獲：

```
- STOP - Stop packet capture.
- STATUS - Display current capture status.
- SETUP - Change packet capture settings.
[]> stop

Status: No capture running (Capture stopped by user)
```

```
Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     host 10.10.10.10 && port 80
```