ASA常見問題：為什麼ASA向沒有IPS策略配置的IPS模組傳送資料包？

目錄

簡介

本文說明為什麼在配置中沒有入侵防禦系統(IPS)模組策略時，思科自適應安全裝置(ASA)可能會將流量傳送到嵌入式服務模組進行檢查。

問：如果未配置IPS策略，ASA為什麼會將資料包傳送到IPS模組進行檢測？

A.

當配置了ASA時，可能會建立連線以將流量傳送到IPS模組進行檢查，並且該連線仍然處於活動狀態。

例如，具有ASA5515-IPS的客戶在策略對映中沒有配置策略以將流量傳送到軟體IPS模組；但是，流量從ASA到達模組。

當您在IPS上使用資料包顯示功能時，可以看到從ASA進入IPS的流量：

```
14:34:38.341927 IP 192.168.1.2.1719 > 192.168.10.39.1888: UDP, length 128
14:34:38.341992 IP 192.168.1.2.1719 > 192.168.10.39.1888: UDP, length 128
14:34:38.345031 IP 192.168.1.2.1719 > 192.168.110.39.1888: UDP, length 34
14:34:38.345068 IP 192.168.1.2.1719 > 192.168.110.39.1888: UDP, length 34
```

已清除IPS感應介面上的介面統計資訊，並接收資料包：

```
sensor#  show interfaces portChannel
MAC statistics from interface PortChannel0/0
Interface function = Sensing interface
Description =
Media Type = backplane
Default Vlan = 0
InlineMode = Unpaired
Pair Status = N/A
Hardware Bypass Capable = No
Hardware Bypass Paired = N/A
```

```
Link Status = Up
Admin Enabled Status = Enabled
Link Speed = N/A
Link Duplex = N/A
Missed Packet Percentage = 0
Total Packets Received = 128
Total Bytes Received = 17904
Total Packets Transmitted = 128
Total Bytes Transmitted = 17904
```

問題的原因在於，在過去的某個時間，向ASA新增了一個配置以將流量傳送到IPS模組，而在ASA上刪除了IPS配置後，連線未清除。這種情況在持續傳遞流量的非TCP協定中很常見。

在ASA上，輸入**show conn**命令以確定您在IPS模組上看到的資料包是否具有連線條目。要檢視正常運行時間，請輸入**show conn detail**命令。為了確保連線不會重定向到IPS，您可能必須在ASA上輸入**clear conn *<address>***命令以清除這些特定連線：

```
ASA# clear conn address 192.168.1.2
3 connection(s) deleted.
ASA#
```

相關資訊

- 技術支援與文件 - Cisco Systems