ASA FAQ：ASA はなぜ IPS ポリシーが設定されていない IPS モジュールにパケットを送信するのか。

内容

概要

このドキュメントでは、設定に侵入防御システム(IPS)モジュールポリシーがない場合、Cisco適応型セキュリティアプライアンス(ASA)がインスペクション用に組み込みサービスモジュールにトラフィックを送信する理由について説明します。

Q. IPSポリシーが設定されていない場合、ASAが検査のためにIPSモジュールにパケットを送信するのはなぜですか。

A.

ASAの設定時にトラフィックをIPSモジュールに送信して検査するために接続が確立され、その接続がアクティブである可能性があります。

たとえば、ASA5515-IPSを使用しているお客様のポリシーマップには、ソフトウェアIPSモジュールにトラフィックを送信するためのポリシーが設定されていません。ただし、トラフィックはASAからモジュールに到達します。

IPSでパケット表示機能を使用すると、ASAからIPSに到達するトラフィックを確認できます。

```
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
```

IPSセンシングインターフェイスのインターフェイス統計情報がクリアされ、パケットが受信されました。

```
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
```

この問題の原因は、過去にASAにトラフィックをIPSモジュールに送信するための設定が追加されたことがあり、IPS設定がASAで削除された後に接続がクリアされなかったことです。これは、トラフィックを常に通過させる非TCPプロトコルに共通です。

ASAで**show conn**コマンドを入力し、IPSモジュールに表示されるパケットに接続エントリがあるかどうかを確認します。アップタイムを表示するには、**show conn detail**コマンドを入力します。接続がIPSにリダイレクトされないようにするには、ASAで**clear conn** ***<address>*コマンドを入力して、特定の接続をクリアする必要がある場合があります。**

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

関連情報

- テクニカル サポートとドキュメント – Cisco Systems