ASA常见问题：为什么ASA向没有IPS策略配置的IPS模块发送数据包？

目录

简介

本文档介绍当配置中没有入侵防御系统(IPS)模块策略时，思科自适应安全设备(ASA)为何可能将流量发送到嵌入式服务模块进行检查。

问：当未配置IPS策略时，ASA为什么会将数据包发送到IPS模块进行检查？

A.

当配置ASA时，可能会建立连接，以将流量发送到IPS模块进行检查，并且该连接仍处于活动状态。

例如，具有ASA5515-IPS的客户在策略映射中没有配置策略来将流量发送到软件IPS模块；但是，流量从ASA到达模块。

在IPS上使用数据包显示功能时，您可以看到来自ASA的IPS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
```

IPS感应接口上的接口统计信息已清除，且已收到数据包：

```
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
```

问题的原因是，在过去某个时候，将配置添加到ASA以将流量发送到IPS模块，并且在ASA上删除IPS配置后，未清除连接。这在不断传递流量的非TCP协议中很常见。

在ASA上，输入**show conn**命令以确定您在IPS模块上看到的数据包是否具有连接条目。要查看更新时间，请输入**show conn detail**命令。为确保连接不会重定向到IPS，您可能必须在ASA上输入**clear conn *<address>***命令以清除这些特定连接：

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

相关信息

- 技术支持和文档 - Cisco Systems