Preguntas frecuentes sobre ASA: ¿Por qué ASA envía paquetes al módulo IPS sin configuración de política IPS?

Contenido

Introducción

Este documento describe por qué el Cisco Adaptive Security Appliance (ASA) puede enviar tráfico a un módulo de servicio integrado para su inspección cuando no hay ninguna política de módulo del sistema de prevención de intrusiones (IPS) en la configuración.

P. ¿Por qué ASA envía paquetes al módulo IPS para su inspección cuando no hay ninguna política IPS configurada?

A.

Es posible que se haya creado una conexión para enviar tráfico al módulo IPS para su inspección cuando se configuró el ASA y que esa conexión siga activa.

Por ejemplo, un cliente con un ASA5515-IPS no tiene ninguna política configurada en un mapa de políticas para enviar el tráfico al módulo IPS de software; sin embargo, el tráfico llega al módulo desde el ASA.

Cuando utiliza la función de visualización de paquetes en el IPS, puede ver el tráfico que llega al IPS desde el ASA:

```
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
```

Se borraron las estadísticas de interfaz en la interfaz de detección IPS y se recibieron paquetes:

```
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
```

La causa del problema es que en el pasado se agregó una configuración al ASA para enviar tráfico al módulo IPS, y las conexiones no se eliminaron después de que se quitó la configuración IPS en el ASA. Esto es común con los protocolos no TCP que pasan tráfico constantemente.

En el ASA, ingrese el comando **show conn** para determinar si los paquetes que ve en el módulo IPS tienen entradas de conexión. Para ver los tiempos de actividad, ingrese el comando **show conn detail**. Para asegurarse de que las conexiones no se redirigen al IPS, es posible que tenga que ingresar el **comando clear conn *<address>*** en el ASA para borrar esas conexiones específicas:

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

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems