ASA FAQ: Por que o ASA envia pacotes ao módulo ips sem a configuração das normas IPS?

Índice

Introdução

Este documento descreve porque a ferramenta de segurança adaptável de Cisco (ASA) pôde enviar o tráfego a um módulo de serviço encaixado para a inspeção quando não há nenhuma política do módulo do Intrusion Prevention System (IPS) na configuração.

Q. Por que o ASA envia pacotes ao módulo ips para a inspeção quando não há nenhuma política IPS configurada?

R.

Épossível que uma conexão esteve construída para enviar o tráfego ao módulo ips para a inspeção quando o ASA foi configurado, e que a conexão é ainda ativa.

Por exemplo, um cliente com um ASA5515-IPS não tem nenhuma política configurada em um mapa de política para enviar o tráfego ao módulo ips do software; contudo, o tráfego chega no módulo do ASA.

Quando você usa a característica do indicador do pacote no IPS, você pode ver o tráfego que vem ao IPS do 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
```

As estatísticas da relação no IPS que detecta a relação foram canceladas, e os pacotes foram recebidos:

```
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
```

A causa da edição é aquela no após uma configuração foi adicionada algum dia ao ASA para enviar o tráfego ao módulo ips, e os connnections não foram cancelados para fora depois que a configuração IPS foi removida no ASA. Isto é comum com protocolos não-TCP que passam constantemente o tráfego.

No ASA, inscreva o **comando show conn** determinar se os pacotes que você vê no módulo ips têm entradas de conexão. A fim ver os uptimes, inscreva o **comando detail do show conn**. A fim assegurar as conexões não são reorientados ao IPS, você pôde ter que incorporar o comando **claro do *<address>* conexão no** ASA cancelar aquelas conexões específicas:

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

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems