FAQ ASA : Pourquoi l'ASA envoie-t-il des paquets au module IPS sans configuration de stratégie IPS ?

Contenu

Introduction

Ce document explique pourquoi l'appliance de sécurité adaptative (ASA) de Cisco peut envoyer du trafic à un module de service intégré pour inspection lorsqu'il n'existe aucune stratégie de module IPS (Intrusion Prevention System) dans la configuration.

Q. Pourquoi l'ASA envoie-t-il des paquets au module IPS pour inspection alors qu'aucune stratégie IPS n'est configurée ?

A.

Il est possible qu'une connexion ait été créée pour envoyer le trafic au module IPS pour inspection lorsque l'ASA a été configuré, et que cette connexion soit toujours active.

Par exemple, un client doté d'un ASA5515-IPS n'a pas de stratégie configurée dans une carte de stratégie pour envoyer le trafic au module IPS logiciel ; cependant, le trafic arrive au module à partir de l'ASA.

Lorsque vous utilisez la fonction d'affichage des paquets sur l'IPS, vous pouvez voir le trafic qui arrive à l'IPS depuis l'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
```

Les statistiques d'interface sur l'interface de détection IPS ont été effacées et des paquets ont été reçus :

```
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 cause du problème est que parfois dans le passé une configuration a été ajoutée à l'ASA pour envoyer le trafic au module IPS, et les connexions n'ont pas été supprimées après la suppression de la configuration IPS sur l'ASA. C’est courant avec les protocoles non TCP qui transmettent constamment le trafic.

Sur l'ASA, entrez la commande **show conn** pour déterminer si les paquets que vous voyez sur le module IPS ont des entrées de connexion. Pour afficher les temps de fonctionnement, entrez la commande **show conn detail**. Afin de vous assurer que les connexions ne sont pas redirigées vers le système IPS, vous devrez peut-être entrer la commande **clear conn *<address>*** sur l'ASA pour effacer ces connexions spécifiques :

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

Informations connexes

- Support et documentation techniques - Cisco Systems