DOMANDE FREQUENTI SULL'APPLIANCE ASA: Perché l'ASA invia i pacchetti al modulo IPS senza alcuna configurazione dei criteri IPS?

Sommario

Introduzione

In questo documento viene descritto perché Cisco Adaptive Security Appliance (ASA) potrebbe inviare traffico a un modulo di servizio incorporato per l'ispezione quando non sono presenti criteri per i moduli IPS (Intrusion Prevention System) nella configurazione.

D. Perché l'ASA invia i pacchetti al modulo IPS per l'ispezione quando non sono configurati criteri IPS?

R.

Èpossibile che una connessione sia stata creata per inviare il traffico al modulo IPS per l'ispezione quando l'ASA è stata configurata e che la connessione sia ancora attiva.

Ad esempio, un cliente con ASA5515-IPS non ha configurato alcun criterio in una mappa dei criteri per inviare il traffico al modulo IPS del software; tuttavia, il traffico arriva al modulo dall'ASA.

Quando si usa la funzione di visualizzazione dei pacchetti sull'IPS, è possibile visualizzare il traffico che arriva all'IPS dall'appliance 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
```

Le statistiche sull'interfaccia di rilevamento IPS sono state cancellate e i pacchetti sono stati ricevuti:

```
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 è che in passato è stata aggiunta una configurazione all'appliance ASA per inviare il traffico al modulo IPS e le connessioni non sono state eliminate dopo la rimozione della configurazione IPS sull'appliance ASA. Questa condizione è comune ai protocolli non TCP che passano costantemente il traffico.

Sull'appliance ASA, immettere il comando **show conn** per determinare se i pacchetti visualizzati sul modulo IPS dispongono di voci di connessione. Per visualizzare i tempi di attività, immettere il comando **show conn detail**. Per verificare che le connessioni non vengano reindirizzate all'IPS, potrebbe essere necessario immettere il comando **clear conn** ***<indirizzo>*** sull'appliance ASA per cancellare le connessioni specifiche:

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

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems