الأسئلة المتداولة حول ASA: لماذا يرسل ASA الحزم إلى الوحدة النمطية IPS بدون تكوين نهج IPS؟

المحتويات

المقدمة

يوضح هذا المستند لماذا قد تقوم أجهزة الأمان المعدلة (ASA) من Cisco بإرسال حركة مرور البيانات إلى وحدة خدمة مضمنة للتفتيش عند عدم وجود سياسة الوحدة النمطية لنظام منع التسلل (IPS) في التكوين.

Q. لماذا يقوم ASA بإرسال الحزم إلى وحدة IPS للفحص في حالة عدم تكوين سياسة IPS؟

ج.

من المحتمل أن يكون قد تم إنشاء اتصال لإرسال حركة مرور البيانات إلى وحدة IPS للفحص عند تكوين ASA، وهذا الاتصال ما يزال نشطا.

على سبيل المثال، لا يوجد لدى عميل مزود ب ASA5515-IPS سياسة تم تكوينها في خريطة سياسة لإرسال حركة مرور البيانات إلى الوحدة النمطية Software IPS؛ ومع ذلك، تصل حركة مرور البيانات إلى الوحدة النمطية من ASA.

عندما يستعمل أنت الربط عرض سمة على ال ips، أنت يستطيع رأيت الحركة مرور أن يأتي إلى ال IPS من ال ASA:

```
IP 192.168.1.2.1719 > 192.168.10.39.1888: UDP, length 128 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 > 192.168.110.39.1888: UDP, length 34 14:34:38.345031
IP 192.168.1.2.1719 > 192.168.110.39.1888: UDP, length 34 14:34:38.345068
```

تم مسح إحصائيات الواجهة الخاصة بواجهة إستشعار IPS، وتم إستلام الحزم:

```
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
```

سبب المشكلة هو أنه في وقت ما في الماضي تمت إضافة تكوين إلى ASA لإرسال حركة مرور البيانات إلى وحدة IPS، ولم يتم مسح الاتصالات بعد إزالة تكوين IPS على ASA. وهذا شائع مع البروتوكولات بخلاف TCP التي تمر بحركة المرور باستمرار.

على ASA، أدخل الأمر **show conn** لتحديد ما إذا كانت الحزم التي ترى على وحدة IPS تحتوي على إدخالات اتصال. لعرض أوقات التشغيل، أدخل الأمر **show conn detail**. لضمان عدم إعادة توجيه الاتصالات إلى IPS، قد تحتاج إلى إدخال الأمر **clear conn <*address*>** على ASA لمسح تلك الاتصالات المحددة:

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

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).