إمكانات أستكشاف أخطاء حزم البيانات وإصلاحها وتحليلها بسرعة اتصال ASA

المحتويات

المقدمة

يوضح اذه المستند كيفية أستكشاف أخطاء مدعل إخراج جهاز الأمان القابل للتكيف (ASA) وسرعة الاتصال وإصلاحها من Cisco.

المتطلبات الأساسية

المتطلبات

ال توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في اذه المستند إلى جهاز الأمان القابل للتكيف (ASA) من Cisco.

تم إنشاء المعلومات الواردة في اذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في اذه المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

قد يواجه بعض العملاء مشكلة عند نشر ASA لأول مرة أو عند إختبار اتصال جديد. المشكلة هي أن إخراج TCP للاتصالات التي تتدفق من خلال ASA أقل بكثير من عندما ال يكون ASA في مسار الاتصال (أو تكون الاتصالات أبطأ بكثير من قبل تنفيذ ASA في الشبكة).

على سبيل المثال، قد يستبدل العميل موجه D-Link منخفض الطرف (أو جهاز توجيه آخر) ب

ASA 5505 أو ASA 5510، وعم ذلك، بمجرد إستبدال الموجه، تنخفض سرعة الاتصال بشكل كبير. قد يثير العميل حالة عم Cisco TAC لأنهم يعتقدون أن ASA سبب الخفض في سرعة الاتصال.

منهجية أستكشاف الأخطاء وإصلاحها

يبطئ تدفق TCP عندما يكون هناك فقدان حزمة أو تأخر حزمة على الشبكة. لفهم سبب المشكلة بالضبط، يجب أن تظهر البيانات حزم TCP الفعلية على السلك لذلك الاتصال وكيف قد تؤثر الشبكة عليها. عادة ما يتم تنبيه مسؤول الشبكة إلى المشكلة عندما تنفيذ إجراء معين، مثل نقل ملف FTP أو إختبار سرعة عبر الإنترنت. وفي أغلب الأحيان يمكن تكرار المشكلة. وبالتالي، يمكن للمسؤول تجميع البيانات المطلوبة للعثور على السبب الجذري.

لتجميع البيانات المطلوبة، يجب تشغيل الأمر **show tech** من ASA قبل الاختبار وبعده. يبدي هذا أمر تشكيل وإحصائيات ربط (أساسا من **عرض خدمة-policy**) وأيضا يبدي إن القارن أخطأ زيادة.

عمليات التقاط حزم متزامنة وثنائية الإتجاه (مأخوذة من واجهات ASA التي تؤثر على إتجاز الاتصال) مطلوبة لتشخيص سبب المشكلة بشكل كامل.

ارجع إلى هذه المستندات للحصول على أمثلة حول كيفية تطبيق التقاط الحزم على ASA:

- أستكشاف أخطاء الاتصالات وإصلاحها من خلال PIX و ASA
- حلقة بث أمان TAC #1 - إستخدام الأداة المساعدة ASA Packet Capture Utility لاستكشاف الأخطاء وإصلاحها

تحليل البيانات

بمجرد تجميع البيانات المطلوبة، يمكن إستخدام التقاط الحزمة لتحديد أي من هذه المشاكل قد حدث:

- يتم إسقاط الحزم من المضيف الخارجي أو تأخيرها قبل الوصول إلى واجهة ASA الخارجية.
- يتم تأجيل الحزم أو إسقاطها من قبل ASA.
- يتم تأجيل الحزم أو إسقاطها في مكان ما على الشبكة الداخلية.

ملاحظة: يفترض هذا التحليل أنه تم إرسال البيانات من مضيف على الواجهة الخارجية إلى مضيف على الواجهة الداخلية.

يوضح هذا الفيديو مثال لكيفية إجراء التحليل على التقاط حزمة:

دمج تدفق TCP وهو إعتبار فني خاص بهذه المشكلة لأنه، عندما تقوم بإشراك ميزات معينة على ASA، يقوم جدار الحماية بدمج تدفق TCP الذي يمر خلاله بشكل كامل.

على سبيل المثال، إذا اكتشف ASA حزمة مفقودة على الشبكة (نظرا لأنه لم يتم استقبالها في ASA)، فإنه يرسل ACK بالنيابة عن نقطة نهاية TCP الأخرى للبيانات المفقودة. وهذا السيناريو شائع للغاية. إذا اكتشف ASA الحزم التي تصل خارج الأمر، فإن ASA يعيد طلب الحزم ويمررها إلى المستقبل بالترتيب المناسب. إذا لم يتم إسقاط الحزم المرسلة من قبل نقطة نهاية TCP عبر الشبكة و ASA، فلن تعرف أن هذه الميزة الشبكة أو إعادة ترتيب الحزم، فلا توجد آثار جانبية لتمكين هذه الميزة. إذا نجحت جميع ممكنة لأنها لا تتخذ إجراء على تدفقات الحزمة. لن يؤدي تمكين هذه الميزة إلى إبطاء حركة

رورم الشبكة بشكل إضافي إلا في حالة حدوث مشكلة في اتصال TCP على الشبكة. إن عملية جمد تدفق TCP هي عملية تستهلك موارد كثيرة جدا بالنسبة إلى ASA. بالنسبة لكل حزمة يتم إسقاطها على الشبكة، يجب ألا يقوم ASA بإرسال طلب حزمة TCP لإعادة إرسال تلك الحزمة فحسب، بل يجب أيضا تخزين الحزم المؤقتة التي استمر المرسل في إرسالها بعد فقدان الحزمة.

مشاكل مشتركة

سرعة سيئة التكوين وقيم إرسال ثنائي الاتجاه على الواجهة التي تصل ASA بالجهاز المجاور

يجب أن تكون السرعة وقيم الإرسال ثنائي الاتجاه على الواجهة ASA هي نفسها على الجهاز المجاور، وإلا فقد تحدث حالات إسقاط. إذا لم تكن قيم السرعة والإرسال ثنائي الاتجاه على الواجهة عند ASA هذه متطابقة عند أدائها وقتها، يجب أن تكون تلك القيم على الواجهة المجاورة كذلك.

تحقق من إخراج **show interface** ل ASA بحثا عن الأخطاء الواضحة التي هي أعراض هذه المشكلة:

```
Interface Ethernet0/0 "Outside", is up, line protocol is up
Hardware is i82546GB rev03, BW 100 Mbps
Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
MAC address 0019.2f58.c324, MTU 1500
IP address 192.168.222.122, subnet mask 255.255.255.252
124047996 packets input, 35340918453 bytes, 0 no buffer
Received 3 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
156918660 packets output, 40931551514 bytes, 0 underruns
1 output errors, 4286634 collisions, 0 interface resets
0 babbles, 123332 late collisions, 4752834 deferred
0 lost carrier, 0 no carrier
input queue (curr/max blocks): hardware (0/0) software (0/0)
output queue (curr/max blocks): hardware (0/245) software (0/0)
Traffic Statistics for "Outside":
124047995 packets input, 33107957301 bytes
157041993 packets output, 38195084709 bytes
103480 packets dropped
1 minute input rate 2140 pkts/sec, 477200 bytes/sec
1 minute output rate 2630 pkts/sec, 396763 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 2152 pkts/sec, 525496 bytes/sec
5 minute output rate 2701 pkts/sec, 421215 bytes/sec
5 minute drop rate, 0 pkts/sec
```

إرسال حركة مرور البيانات إلى الوحدة النمطية IPS

عند تكوين ASA لإرسال حركة مرور البيانات إلى وحدة IPS، يتم تشغيل ميزة جمد تدفق TCP على ASA. راجع قسم *تحليل البيانات* في هذا المستند للحصول على مزيد من المعلومات حول ميزة جمد تدفق TCP.

يتسبب تعديل ASA لخيار TCP MSS في انخفاض طفيف في الأداء

يعمل ASA بشكل افتراضي على تعيين خيار TCP MSS في حزم syn على 1380. لذلك، يجب ألا يتم إرسال حزم TCP الكبيرة في نطاق ما يتخطى TCP بإرسال مقطع TCP أكبر من 1380 بايت. هذه القيمة أقل من القيمة الافتراضية البالغة التي تبلغ 1460 بايت وتمثل انخفاضا في أداء بروتوكول TCP

بنسبة ستة في المائة (6٪) تقريبا. قد يتحسن الأداء إذا قمت بزيادة إعداد MSS الأقصى على ASA أو تعطيل ضبط MSS. قبل تعديل الأمر الافتراضي على ASA، تعرف على المخاطر المعنية فيما يتعلق بالتجزئة المحتملة إذا كانت الحزمة يتم تضمينها بشكل إضافي في المسار في مكان ما.

أحلت ل كثير معلومة، الـ sysopt توصيل قسم من *الـ cisco ASA 5500 sery أمر مرجع*.

معلومات ذات صلة

- cisco ASA 5500 sery أمر مرجع، 8.2
- 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).