فشل حركة مرور UDP من خلال ASA بعد وقوع إعداد إرتباط ISP الأساسي إلى الإنترنت في جودزم ISP

المحتويات

المقدمة
قبل البدء
المتطلبات
المكونات المستخدمة
الاصطلاحات
المشكلة
الحل
معلومات ذات صلة

المقدمة

إذا كان جهاز الأمان القابل للتكيف (ASA) يحتوي على واجهات مخرج لكل شبكة فرعية للوجهة وتمت إزالة المسار المفضل إلى الوجهة من جدول التوجيه لبعض الوقت، فيمكن أن تفشل إتصالات بروتوكول مخطط بيانات المستخدم (UDP) عندما تتم إعادة إضافة المسار المفضل إلى جدول التوجيه. قد تتأثر إتصالات TCP أيضا بهذه المشكلة، ولكن نظرا لأن بروتوكول TCP يكتشف فقدان الحزم، يتم قطع هذه الاتصالات تلقائيا بواسطة نقاط النهاية، وإعادة الإنشاء باستخدام المسارات الأكثر مثالية بعد تغيير الموجهات.

كما يمكن ملاحظة هذه المشكلة إذا تم إستخدام بروتوكول توجيه وقام تغيير مخطط بتشغيل تغيير في جدول التوجيه على ASA.

قبل البدء

المتطلبات

لمواجهة هذه المشكلة، يجب تغيير جدول توجيه ASA. وهذا شائع مع إرتباطات ISP المزدوجة بطريقة متكررة أو عندما يكون ASA يتعلم المسارات عبر بروتوكول العبارة الداخلية (OSPF و EIGRP و RIP).

تحدث هذه المشكلة عندما يعود إرتباط ISP الأساسي إلى الإنترنت أو عندما يرى IGP المذكور عملية إعادة تقارب من خلالها يتم إستبدال المسار الأقل تفضيلا الذي كان يتم إستخدامه من قبل ASA بالمسار الأدنى من القياسات المفضل. يمكنك حينئذ مشاهدة الاتصالات طويلة العمر، مثل تسجيلات UDP SIP و GRE وما إلى ذلك، التي تفشل بمجرد إعادة تثبيت المسار الرئيسي أو المفضل في جدول توجيه ASA.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية والبرامج التالية:

- أي جهاز أمان قابل للتكيف فئة ASA 5500 من Cisco
- إصدارات 8.5(1)1، 8.4(1)1، 8.3(2)12، 8.2(5) ASA) والإصدارات اللاحقة

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

المشكلة

إذا تمت إزالة إدخال جدول توجيه من جدول توجيه ASA ولا يوجد مسارات خارج الواجهة للوصول إلى الوجهة، فسيتم حذف الاتصالات التي تم إنشاؤها من خلال جدار الحماية مع تلك الوجهة الخارجية بواسطة ASA. يحدث هذا حتى يمكن إنشاء الاتصالات مرة أخرى باستخدام واجهة مختلفة مع إدخالات التوجيه للوجهة الموجودة.

ومع ذلك، إذا تمت إضافة مسارات أكثر تحديدا إلى الجدول، فلن يتم تحديث الاتصالات لاستخدام المسارات الجديدة الأكثر تحديدا، وسنواصل إستخدام الواجهة الأقل مثالية.

على سبيل المثال، تذكر أن جدار الحماية يحتوي على واجهتين تتواجدان مع الإنترنت - "خارج" و"نسخ إحتياطي" - وأن هذين الموجهين موجودان في تكوين ASA:

```
route outside 0.0.0.0 0.0.0.0 10.1.1.1 1 track 1
route backup 0.0.0.0 0.0.0.0 172.16.1.1 254
```

إذا كانت كل من الواجهات الخارجية والنسخ الاحتياطي "up"، فسيتم إستخدام الواجهة الخارجية للاتصالات التي تم بناؤها للخارج من خلال جدار الحماية، نظرا لأنها تمتلك المقياس المفضل وهو 1. إذا تم إيقاف تشغيل الواجهة الخارجية (أو وظيفة مراقبة SLA التي تقوم بتعقب المسار تواجه فقدان الاتصال ب IP الذي تم تعقبه)، فسيتم قطع الاتصالات باستخدام الواجهة الخارجية وإعادة بنائها باستخدام واجهة النسخ الاحتياطي، حيث أن واجهة النسخ الاحتياطي هي الواجهة الوحيدة التي تحتوي على مسار إلى الوجهة.

تحدث المشكلة عند إرجاع الواجهة الخارجية أو عندما يصبح المسار المتتبع المسار المفضل مرة أخرى. يتم تحديث جدول التوجيه لتفضل المسار الأصلي، ولكن تستمر الاتصالات الموجودة في الوجود على ASA واجتياز واجهة النسخ الاحتياطي ولا يتم حذفها وإعادة إنشائها على الواجهة الخارجية باستخدام المقياس الأكثر تفضيلا. وهذا يرجع لأن المسار الافتراضي للنسخ الاحتياطي لا يزال موجودا في جدول التوجيه الخاص بواجهة ASA. يستمر الاتصال في إستخدام الواجهة مع المسار الأقل تفضيلا حتى يتم حذف الاتصال؛ في حالة UDP، قد يكون هذا غير محدد.

قد يتسبب هذا الموقف في حدوث مشاكل في الاتصالات طويلة العمر، مثل تسجيلات SIP الخارجية أو إتصالات UDP الأخرى.

الحل

ومن أجل معالجة هذه المشكلة المحددة، تمت إضافة ميزة جديدة إلى ASA ستؤدي إلى قطع الاتصالات وإعادة بنائها على واجهة جديدة إذا تمت إضافة مسار أكثر تفضيلا إلى الوجهة إلى جدول التوجيه. لتنشيط الميزة (يتم تعطيلها بشكل افتراضي)، قم بتعيين مهلة غير صفرية إلى الأمر **timeout floating-conn**. تحدد هذه المهلة (المحددة في HH:MM:SS) الوقت الذي ينتظره ASA قبل أن ينقطع الاتصال بمجرد إضافة مسار أكثر تفضيلا مرة أخرى إلى جدول التوجيه:

هذا مثال على واجهة سطر الأوامر (CLI) لتمكين الميزة. باستخدام واجهة سطر الأوامر هذه، إذا تم تلقي حزمة على اتصال حالي يوجد له الآن مسار مختلف وأكثر تفضيلا إلى الوجهة، فسيتم قطع الاتصال بعد دقيقة واحدة (وإعادة بنائه باستخدام المسار الجديد الأكثر تفضيلا):

```
ASA# config terminal
```

```
ASA(config)# timeout floating-conn 0:01:00
ASA(config)# end
ASA# show run timeout
timeout conn 1:00:00 half-closed 0:10:00 udp 0:50:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:01:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout xlate 0:01:00
timeout pat-xlate 0:00:30
timeout floating-conn 0:01:00
#ASA
```

تتم إضافة هذه الميزة إلى نظام ASA الأساسي في الإصدارات 8.2(5) و 8.3(2)12 و 8.4(1)1 و 8.5(1)، بما في ذلك الإصدارات الأحدث من برنامج ASA.

إذا قمت بتشغيل إصدار من رمز ASA لا يطبق هذه الميزة، فسيكون الحل البديل للمسألة هو مسح إتصالات UDP يدويا التي تستمر في أخذ المسار الأقل تفضيلا رغم توفير مسار أفضل عبر **مضيف محلي واضح *<IP>*** أو **clear-conn *<<IP>>*** .

يسرد مرجع الأمر هذه الميزة الجديدة ضمن قسم المهلة.

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).