ASA لديه إستخدام عال لوحدة المعالجة المركزية (CPU) بسبب تكرار حركة مرور عند قطع اتصال عملاء VPN

المحتويات

المقدمة

يصف هذا المستند مشكلة مشتركة تحدث عندما ينفصل عملاء VPN عن جهاز الأمان القابل للتكيف (ASA) من Cisco الذي يعمل كنقطة الاستقبال VPN للوصول عن بعد. يصف هذا وثيقة أيضا الحالة حيث حركة مرور يقع أنشوطة عندما VPN مستعمل ينفصل من ASA جدار حماية. لا يغطي هذا المستند كيفية تكوين الوصول عن بعد إلى شبكة VPN أو إعداده، بل الحالة المحددة التي تنشأ من تكوينات توجيه شائعة معينة فقط.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين VPN للوصول عن بعد على ASA
- مفاهيم التوجيه الأساسية من الطبقة 3

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى طراز ASA 5520 الذي يشغل رمز ASA الإصدار 9.1(1).

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

المنتجات ذات الصلة

هذا وثيقة يستطيع كنت استعملت مع هذا جهاز وبرمجية صيغة:

- أي طراز ASA
- أي إصدار كود ASA

معلومات أساسية

عندما يتصل مستخدم بالموجه ASA كمركز وصول عن بعد VPN، يقوم ASA بتثبيت مسار قائم على المضيف في جدول توجيه ASA الذي يقوم بتوجيه حركة مرور البيانات إلى عميل VPN هذا خارج الواجهة الخارجية (نحو الإنترنت). عندما ينفصل ذلك المستخدم، تتم إزالة المسار من الجدول، وقد يتم تكرار الحزم الموجودة على الشبكة الداخلية (الموجهة إلى ذلك المستخدم الذي قام بقطع اتصال VPN) بين ASA وجهاز توجيه داخلي.

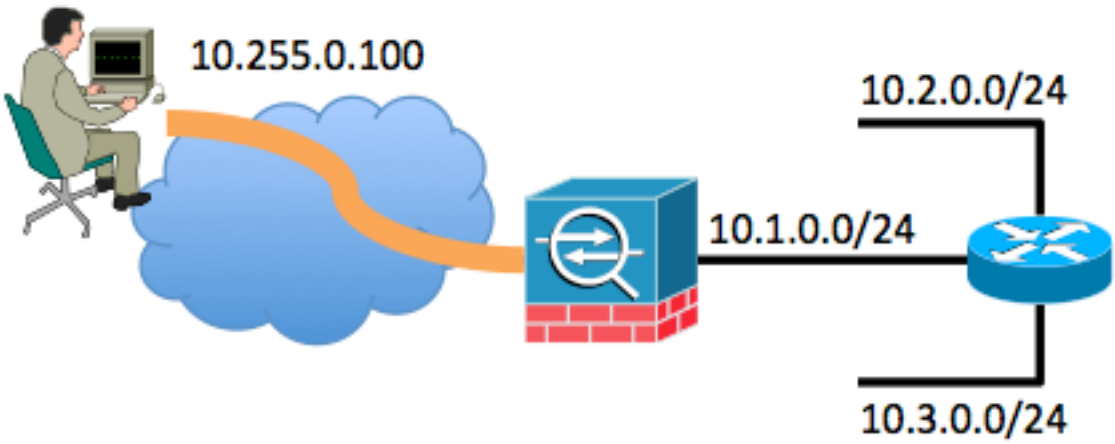
مشكلة أخرى هي أن حزم البث (الشبكة) الموجهة (التي تم إنشاؤها بواسطة إزالة عملاء VPN) قد يتم إعادة توجيهها بواسطة ASA كإطار أحادي البث باتجاه الشبكة الداخلية. قد يقوم هذا بإعادة توجيهه إلى ASA، والذي يتسبب في تكرار الحزمة حتى انتهاء صلاحية مدة البقاء (TTL).

يشرح هذا وثيقة هذا إصدار ويبدي ما تشكيل تقنية يستطيع كنت استعملت in order to منعت المشكلة.

مشكلة: الحزم الموجهة لحلقة عميل VPN غير متصلة داخل الشبكة الداخلية

عندما ينفصل مستخدم شبكة VPN للوصول عن بعد من جدار حماية ASA، فإن الحزم التي لا تزال موجودة على الشبكة الداخلية (الموجهة لهؤلاء المستخدمين الذين تم قطع الاتصال بهم) وعنوان IP VPN المعين قد تصبح مكررة داخل الشبكة الداخلية. قد تتسبب حلقات الحزمة هذه في زيادة إستخدام وحدة المعالجة المركزية على ASA إلى أن تتوقف الحلقة إما بسبب قيمة IP TTL في إصدار قرار برأس حزمة IP إلى 0، أو أن المستخدم يعيد الاتصال وأن يتم إعادة تعيين عنوان IP إلى عميل VPN.

ولفهم هذا السيناريو بشكل أفضل، تأمل في هذا المخطط:



في هذا المثال، تم تعيين عنوان IP لعميل الوصول عن بعد بقيمة 10.255.0.100. ال ASA في هذا مثال ربطت إلى ال نفسه داخل شبكة قطعة مع مسحاج تخديد. يحتوي الموجه على مقاطع شبكة إضافية من الطبقة 3 متصلة به. يتم عرض تكوينات الواجهة ذات الصلة (التوجيه) والشبكة الخاصة الظاهرية (VPN) ل ASA والموجه في الأمثلة.

يتم توضيح ميزات تكوين ASA في هذا المثال:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
```

```
ip address 198.51.100.100 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.0.1 255.255.255.0
!
same-security-traffic permit intra-interface
!
ip local pool VPNpool 10.255.0.1-10.255.0.255
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
route inside 10.0.0.0 255.0.0.0 10.1.0.2
```

يتم توضيح مميزات تكوين الموجه في هذا المثال:

```
interface FastEthernet0
description connected to the inside interface of the ASA G0/1
ip address 10.1.0.2 255.255.255.0
!
interface FastEthernet1
description connected to network segment
ip address 10.2.0.1 255.255.255.0
!
interface FastEthernet2
description connected to other network segment
ip address 10.3.0.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.0.1
```

يتضمن جدول التوجيه الخاص بالموجه المتصل بداخل ASA ببساطة مسار افتراضي يشير إلى واجهة ASA الداخلية ل 10.1.0.1.

بينما يتم توصيل المستخدم عبر VPN إلى ASA، يظهر جدول توجيه ASA كما يلي:

```
ASA# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
candidate default, U - per-user static route, o - ODR - *
P - periodic downloaded static route
Gateway of last resort is 198.51.100.1 to network 0.0.0.0
S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

تحدث المشكلة عندما ينفصل مستخدم شبكة VPN للوصول عن بعد من الشبكة الخاصة الظاهرية (VPN). عند هذه النقطة، تتم إزالة المسار المستند إلى المضيف من جدول توجيه ASA. إذا حاول مضيف داخل الشبكة إرسال حركة مرور البيانات إلى عميل VPN، فسيتم توجيه حركة مرور البيانات هذه إلى واجهة ASA الداخلية بواسطة الموجه. تحدث هذه السلسلة من الخطوات:

1. تصل الحزمة الموجهة إلى 10.255.0.100 إلى الواجهة الداخلية ل ASA.
2. يتم إجراء عمليات التحقق القياسية من قائمة التحكم في الوصول (ACL).
3. يتم التحقق من جدول توجيه ASA لتحديد واجهة مخرج حركة المرور هذه.

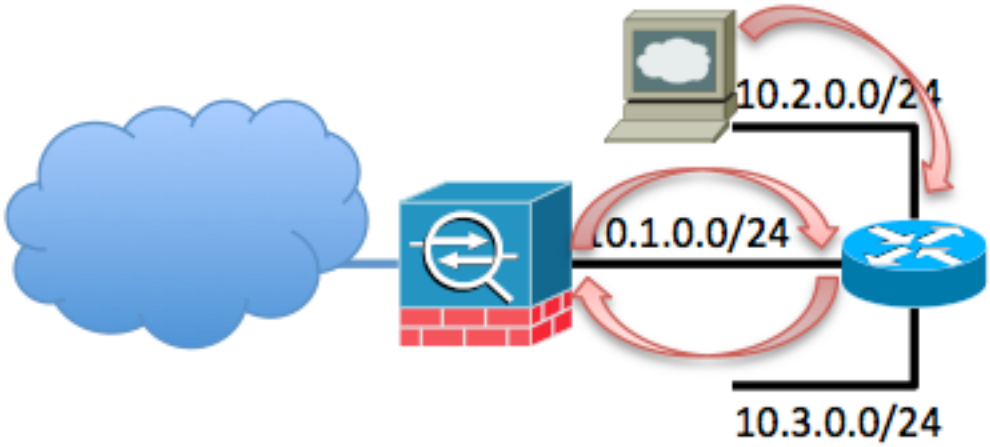
4. تطابق وجهة الحزمة المسار 8/10.0.0.0 العريض الذي يشير إلى الخلف من الواجهة الداخلية نحو الموجه.

5. يتحقق ASA مما إذا كان يسمح بحركة مرور تثبيت الشعر - فيبحث عن **تصريح الأمان نفسه داخل الواجهة** ويجد أنه مسموح بها.

6. يتم إنشاء اتصال من الواجهة الداخلية وإليها ويتم إرسال الحزمة مرة أخرى إلى الموجه كخطوة تالية.

7. يستقبل الموجه حزمة موجهة إلى 10.255.0.100 على الواجهة التي تواجه ASA. يتحقق الموجه من جدول التوجيه الخاص به للوصول إلى الخطوة التالية المناسبة. يكتشف الموجه أن الخطوة التالية ستكون هي واجهة ASA الداخلية، ويتم إرسال الحزمة إلى ASA.
8. العودة إلى الخطوة 1.

ويتم توضيح مثال هنا:



يقع هذا أنشوطة إلى أن ال TTL من هذا ربط ربط إلى 0. لاحظ أن جدار حماية ASA **لا** يقلل من قيمة TTL بشكل افتراضي عند معالجة حزمة. يقوم الموجه بخفض مدة البقاء (TTL) لأنه يقوم بتوجيه الحزمة. هذا يمنع التكرار من هذا التكرار إلى أجل غير مسمى، ولكن هذه الحلقة تزيد من حمل حركة مرور البيانات على ASA وتسبب في إرتفاع إستخدام وحدة المعالجة المركزية.

مشكلة: حزم البث الموجهة (الشبكة) التي تم إنشاؤها بواسطة عملاء VPN موجودة على شبكة داخلية

هي المشكلة متل المشكلة الأولى .. إذا قام عميل شبكة VPN بإنشاء حزمة بث موجه إلى شبكة IP الفرعية المخصصة له (10.255.0.255 في المثال السابق)، فقد تتم إعادة توجيه هذه الحزمة كإطار بث أحادي بواسطة ASA إلى الموجه الداخلي. وقد يقوم الموجه الداخلي بعد ذلك بإعادة توجيهه مرة أخرى إلى ASA، مما يتسبب في تكرار الحزمة حتى تنتهي صلاحية TTL.

تحدث هذه السلسلة من الأحداث:

1. يقوم جهاز عميل شبكة VPN بإنشاء حزمة موجهة إلى عنوان بث الشبكة 10.255.0.255، وتصل الحزمة إلى ASA.
2. يعالج ال ASA هذا ربط كإطار unicast (واجب إلى التوجيه طاولة) ويعيد توجيهها إلى المسحاج تخديد داخلي.

3. يقوم الموجه الداخلي، والذي يتعامل أيضا مع الحزمة كإطار أحادي البث، بخفض مدة البقاء (TTL) للحزمة وإعادة توجيهها إلى ASA.

4. تستمر العملية حتى يتم خفض مدة البقاء (TTL) للحزمة إلى 0.

حلول للمشكلة

وهناك العديد من الحلول المحتملة لهذه القضية. واعتمادا على مخطط الشبكة والحالة المحددة، قد يكون تنفيذ أحد الحلول أسهل من تنفيذ حل آخر.

الحل 1- المسار الثابت للواجهة Null0 (الإصدار 9.2.1 من ASA والإصدارات الأحدث)

عند إرسال حركة مرور البيانات إلى واجهة **Null0**، فإنها تتسبب في إسقاط الحزم الموجهة إلى الشبكة المحددة. تكون هذه الميزة مفيدة عندما تقوم بتكوين الثقب الأسود الذي يتم إطلاقه عن بعد (RTBH) لبروتوكول العبارة الحدودية (BGP). في هذه الحالة، إذا قمت بتكوين مسار إلى Null0 للشبكة الفرعية لعميل الوصول عن بعد، فإنها تفرض على ASA إسقاط حركة المرور الموجهة إلى الأجهزة المضيفة في هذه الشبكة الفرعية إذا لم يكن هناك مسار أكثر تحديدا (متوفر بواسطة إدخال المسار العكسي).

```
route Null0 10.255.0.0 255.255.255.0
```

الحل 2 - إستخدام تجمع IP مختلف لعملاء VPN

هذا الحل أن يعين ال VPN بعيد مستعمل عنوان أن لا يتداخل مع أي شبكة فرعية داخلية. وهذا قد يمنع ASA من إعادة توجيه الحزم الموجهة إلى الشبكة الفرعية VPN تلك مرة أخرى إلى الموجه الداخلي إذا لم يكن مستخدم شبكة VPN متصلا.

الحل 3 - جعل جدول توجيه ASA أكثر تحديدا للمسارات الداخلية

الغرض من هذا الحل هو ضمان عدم إحتواء جدول التوجيه الخاص ب ASA على أي مسارات واسعة جدا تتداخل مع تجمع IP لشبكة VPN. للحصول على مثال الشبكة المحدد هذا، قم بإزالة المسار 8/10.0.0.0 من المحول ASA وشكلت المزيد من المسارات الثابتة المحددة للشبكات الفرعية الموجودة خارج الواجهة الداخلية. واعتمادا على عدد الشبكات الفرعية وهيكل الشبكة، قد يكون هذا العدد كبيرا من المسارات الثابتة وقد لا يكون ممكنا.

الحل 4 - إضافة مسار أكثر تحديدا للشبكة الفرعية للشبكات الخاصة الظاهرية (VPN) مرة أخرى إلى الواجهة الخارجية

هذا الحل أكثر تعقيدا من الحلول الأخرى الموصوفة في هذه الوثيقة. توصي Cisco بمحاولة إستخدام الحلول الأخرى أولا بسبب الحالة الموضحة في الملاحظة لاحقا في هذا القسم. الغرض من هذا الحل هو منع ASA من إعادة توجيه حزم IP التي يتم الحصول عليها من الشبكة الفرعية IP الخاصة بشبكة VPN مرة أخرى إلى الموجه الداخلي؛ يمكنك القيام بذلك إذا قمت بإضافة مسار أكثر تحديدا للشبكة الفرعية لشبكة VPN من الواجهة الخارجية. نظرا لأن شبكة IP الفرعية هذه محجوزة لمستخدمي VPN الخارجيين، يجب ألا تصل الحزم ذات عنوان IP للمصدر من الشبكة الفرعية VPN IP هذه أبدا إلى الوارد على واجهة ASA الداخلية. أسهل طريقة لتحقيق هذا هو إضافة مسار لتجمع IP الخاص بالوصول عن بعد إلى VPN من الواجهة الخارجية مع عنوان IP للجنجل التالي من موجه ISP للتحميل.

في مثال مخطط الشبكة هذا، سيبدو هذا المسار كما يلي:

```
route outside 10.255.0.0 255.255.255.0 198.51.100.1
```

بالإضافة إلى هذا المسار، أضف الأمر **ip verify reverse-path inside** للسماح ل ASA بإسقاط أي حزم مستلمة واردة على الواجهة الداخلية المستمدة من الشبكة الفرعية VPN IP بسبب المسار الأكثر تفضيلا الموجود على الواجهة الخارجية:

```
ip verify reverse-path inside
```

بعد تنفيذ هذه الأوامر، يبدو جدول توجيه ASA مماثلا لهذا عند اتصال المستخدم:

```
ASA# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       candidate default, U - per-user static route, o - ODR - *
                                P - periodic downloaded static route

       Gateway of last resort is 198.51.100.1 to network 0.0.0.0

S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
          S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
S 10.255.0.0 255.255.255.0 [1/0] via 198.51.100.1, outside
C 198.51.100.0 255.255.255.0 is directly connected, outside
    C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

عندما يكون عميل VPN متصلا، يكون المسار المستند إلى المضيف إلى عنوان IP لشبكة VPN تلك موجودا في الجدول ويفضل. عندما ينفصل عميل VPN، يتم التحقق من حركة مرور البيانات التي يتم الحصول عليها من عنوان IP ذلك العميل الذي يصل إلى الواجهة الداخلية مقابل جدول التوجيه وإسقاطها بسبب الأمر **ip verify reverse-path inside**.

إذا قام عميل شبكة VPN بإنشاء بث شبكة موجه إلى الشبكة الفرعية IP لشبكة VPN، فسيتم إعادة توجيه الحزمة إلى الموجه الداخلي وإعادة توجيهها بواسطة الموجه مرة أخرى إلى ASA، حيث يتم إسقاطها بسبب الأمر **ip verify reverse-path inside**.

ملاحظة: بعد تنفيذ هذا الحل، إذا كان الأمر **نفسه**-allowed-interface **security** موجودا في التكوين وسمحت به سياسات الوصول، فقد يتم توجيه حركة المرور المستمدة من مستخدم شبكة خاصة ظاهرية (VPN) الموجهة إلى عنوان IP في تجمع VPN IP للمستخدم غير المتصل إلى خارج الواجهة الخارجية في نص واضح. هذه حالة نادرة ويمكن الحد منها باستخدام عوامل تصفية VPN داخل سياسة الشبكة الخاصة الظاهرية (VPN). لا يحدث هذا الموقف إلا إذا كان الأمر **نفسه-security permit intra-interface** موجودا في تكوين ASA.

وبالمثل، إذا قامت الأجهزة المضيفة الداخلية بإنشاء حركة مرور موجهة إلى عنوان IP في تجمع VPN ولم يتم تعيين عنوان IP هذا إلى مستخدم شبكة VPN بعيد، فقد تخرج حركة مرور البيانات من الخارج إلى ASA في نص واضح.

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).