مثال تكوين ميزة تجاوز حالة ASA 8.2.X TCP

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين ميزة تجاوز حالة TCP. تتيح هذه الميزة التدفقات الصادرة والواردة من خلال أجهزة الأمان المعدلة Cisco ASA 5500 Series المنفصلة.

المتطلبات الأساسية

متطلبات الترخيص

يجب أن يكون لدى أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security الترخيص الأساسي على الأقل.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جهاز الأمان القابل للتكيف (ASA) من Cisco بالإصدار 8.2(1) والإصدارات الأحدث.

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.

الاصطلاحات

أحلت ال cisco فني طرف إتفاق لمعلومة على وثيقة إتفاق.

تجاوز حالة TCP

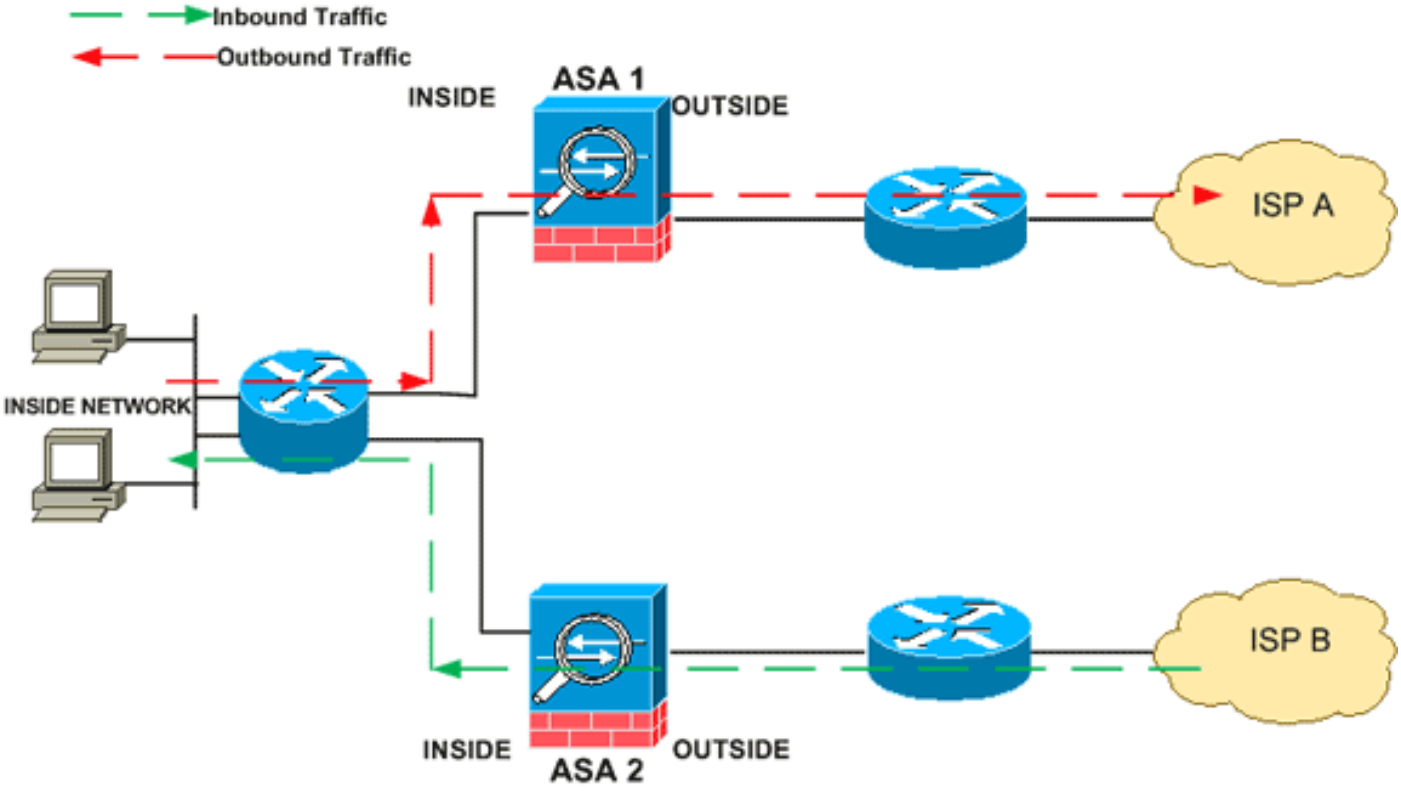
بشكل افتراضي، يتم فحص جميع حركات مرور البيانات التي تمر عبر جهاز الأمان القابل للتكيف (ASA) من Cisco باستخدام خوارزمية الأمان المعدلة ويتم السماح بها أو إسقاطها استنادا إلى سياسة الأمان. لزيادة أداء جدار الحماية إلى الحد الأقصى، يتحقق ASA من حالة كل حزمة (على سبيل المثال، هل هذا اتصال جديد أو اتصال تم إنشاؤه؟) ويعينه إما إلى مسار إدارة جلسة العمل (حزمة نظام اتصال جديدة) أو المسار السريع (اتصال تم إنشاؤه) أو مسار مستوى التحكم (فحص متقدم).

يمكن لحزم TCP التي تطابق الاتصالات الموجودة في المسار السريع المرور من خلال جهاز الأمان القابل للتكيف دون مراجعة كل جانب من نهج الأمان. تعمل هذه الميزة على زيادة الأداء إلى الحد الأقصى. ومع ذلك، فإن الطريقة المستخدمة لإنشاء الجلسة في المسار السريع (الذي يستخدم حزمة SYN) والتحقيقات التي تحدث في المسار السريع (مثل رقم تسلسل TCP) يمكن أن تقف في طريق حلول التوجيه غير المتماثل: يجب أن يمر كل من التدفق الصادر والوارد للاتصال عبر نفس ASA.

على سبيل المثال، ينتقل اتصال جديد إلى *ASA 1*. تمر حزمة SYN من خلال مسار إدارة جلسة العمل، ويتم إضافة إدخال للاتصال إلى جدول المسار السريع. إذا مرت الحزم التالية من هذا الاتصال عبر *ASA 1*، فستطابق الحزم الإدخال في المسار السريع ويتم تمريرها. إذا ذهبت الحزم التالية إلى *ASA 2*، حيث لا يوجد حزمة SYN تمر عبر مسار إدارة الجلسة، حينئذ لا يوجد إدخال في المسار السريع للاتصال، ويتم إسقاط الحزم.

إذا كان لديك توجيه غير متماثل تم تكوينه على موجهات الخادم، ومنافذ حركة مرور البيانات بين وحدتي ASA، عندئذ يمكنك تكوين تجاوز حالة TCP لحركة مرور معينة. يقوم تجاوز حالة TCP بتغيير الطريقة التي يتم بها إنشاء الجلسات في المسار السريع وتعطيل عمليات التحقق من المسار السريع. تعالج هذه الميزة حركة مرور TCP بقدر ما تتعامل مع اتصال UDP: عندما تدخل حزمة غير SYN تطابق الشبكات المحددة في ASA، ولا يوجد إدخال مسار سريع، ثم تنتقل الحزمة عبر مسار إدارة جلسة العمل لإنشاء الاتصال في المسار السريع. بمجرد أن تكون في المسار السريع، فإن حركة المرور تتجاوز التحققات السريعة للمسار.

توفر هذه الصورة مثالا للتوجيه غير المتماثل، حيث تمر حركة المرور الصادرة عبر ASA مختلف عن حركة المرور الواردة:



ملاحظة: يتم تعطيل ميزة تجاوز حالة TCP بشكل افتراضي على أجهزة الأمان القابلة للتكيف ASA 5500 Series.

معلومات الدعم

يوفر هذا القسم معلومات الدعم لميزة تجاوز حالة TCP.

- وضع السياق—مدعوم في وضع السياق المفرد والمتعدد.
- وضع جدار الحماية—مدعوم في الوضع الموجه والشفاف.
- تجاوز الفشل — دعم تجاوز الفشل.

لا يتم دعم هذه الميزات عند إستخدام تجاوز حالة TCP:

- فحص التطبيق—يتطلب فحص التطبيق مرور البيانات الواردة والصادرة على حد سواء من خلال ASA نفسه، لذلك لا يتم دعم فحص التطبيق من خلال تجاوز حالة TCP.
- جلسات عمل AAA المصدق عليها—عندما يصدق مستخدم مع ASA واحد، سيتم رفض حركة المرور التي ترجع عبر ASA الآخر لأن المستخدم لم يصدق على ASA ذلك.
- اعتراض TCP، الحد الأقصى للاتصال الوليد، الرقم التسلسلي لبروتوكول TCP العشوائية— لا يحتفظ ASA بتتبع حالة الاتصال، لذلك لا يتم تطبيق هذه الميزات.
- التطبيع TCP—تم تعطيل تطبيع TCP.
- SSM ووظائف SSC- لا يمكنك إستخدام تجاوز حالة TCP وأي تطبيق يعمل على SSM أو SSC، مثل IPS أو CSCs.

NAT Guidelines: لأن جلسة الترجمة خلقت بشكل مستقل لكل ASA، تأكدت أن يشكل NAT ساكن إستاتيكي على كلا ASAs ل TCP دولة تجاوز حركة مرور؛ إن يستعمل أنت حركي nat، العنوان يختار للجلسة على *ASA 1* يختلف من العنوان يختار للجلسة على *ASA 2*.

التكوين

يصف هذا القسم كيفية تكوين ميزة تجاوز حالة TCP على جهاز الأمان القابل للتكيف (ASA) من السلسلة Cisco ASA 5500 Series.

تكوين ميزة تجاوز حالة TCP

أكمل هذه الخطوات لتكوين ميزة تجاوز حالة TCP على جهاز الأمان القابل للتكيف ASA 5500 Series:

1. أستخدم الأمر class-map class_map_name لإنشاء *خريطة فئة*. يتم إستخدام خريطة الفئة لتحديد حركة المرور التي تريد تعطيل فحص جدار الحماية الذي يحدد الحالة لها. خريطة الفئة المستخدمة في هذا المثال هي *tcp_bypass*.

```
ASA(config)#class-map tcp_bypass
```

2. أستخدم الأمر match parameter لتحديد حركة مرور مثيرة للاهتمام في خريطة الفئة. عند إستخدام "إطار عمل السياسة النمطية"، أستخدم الأمر **match access-list** في وضع تكوين خريطة الفئة لاستخدام قائمة الوصول لتحديد حركة المرور التي تريد تطبيق الإجراءات عليها. هنا مثال من هذا تشكيل:

```
ASA(config)#class-map tcp_bypass
ASA(config-cmap)#match access-list tcp_bypass
```

tcp_bypass هو اسم قائمة الوصول المستخدمة في هذا المثال. راجع تعريف حركة المرور (خريطة الطبقة 4/3) للحصول على مزيد من المعلومات حول تحديد حركة المرور المفيدة.

3. أستخدم الأمر policy-map name لإضافة خريطة سياسة أو تحرير خريطة سياسة (موجودة بالفعل) لتعيين الإجراءات التي يجب إتخاذها مع حركة مرور خريطة الفئة المحددة بالفعل. عند إستخدام "إطار عمل السياسة النمطية"، أستخدم الأمر **policy-map** (بدون كلمة النوع الرئيسية) في وضع التكوين العام لتعيين إجراءات لحركة المرور التي قمت بتعريفها بخريطة فئة الطبقة 4/3 (أمر إدارة نوع خريطة الفئة أو نوع خريطة الفئة). في هذا

المثال، خريطة السياسة هي *tcp_bypass_policy*:
```
ASA(config-cmap)#policy-map tcp_bypass_policy
```

4. أستخدم الأمر class في وضع تكوين خريطة السياسة لتخصيص خريطة الفئة (*tcp_bypass*) التي تم إنشاؤها بالفعل إلى خريطة السياسة (*tcp_bypass_policy*) حيث يمكنك تعيين إجراءات لحركة مرور خريطة الفئة . في هذا المثال، خريطة الفئة هي *tcp_bypass*:
```
ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
```

5. أستخدم الأمر set connection advanced-options tcp-state-bypass في وضع تكوين الفئة لتمكين ميزة تجاوز حالة TCP. تم إدخال هذا الأمر في الإصدار 8.2(1). يمكن الوصول إلى وضع تكوين الفئة من وضع تكوين خريطة السياسة كما هو موضح في هذا المثال:
```
ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass
```

6. أستخدم service-policy policy map_name [interface *intf* | عمومي] أمر في وضع التكوين العام لتنشيط خريطة سياسة بشكل عام على جميع الواجهات أو على واجهة مستهدفة. لتعطيل سياسة الخدمة، أستخدم الصيغة **no** من هذا الأمر. أستخدم الأمر **service-policy** لتمكين مجموعة من السياسات على واجهة.**global** يطبق خريطة السياسة على جميع الواجهات، **وتطبق الواجهة** السياسة على واجهة واحدة. يتم السماح بسياسة عمومية واحدة فقط. يمكنك تجاوز السياسة العامة على واجهة بتطبيق سياسة خدمة على تلك الواجهة. يمكنك تطبيق خريطة سياسة واحدة فقط على كل واجهة.
```
ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
```

هنا عينة تشكيل ل TCP حالة تجاوز:

```
Configure the access list to specify the TCP traffic !--- that needs to by-pass inspection ---!
to improve the performance. ASA(config)#access-list tcp_bypass extended permit tcp 10.1.1.0
255.255.255.224 any

Configure the class map and specify the match parameter for the !--- class map to match the ---!
interesting traffic. ASA(config)#class-map tcp_bypass
"ASA(config-cmap)#description "TCP traffic that bypasses stateful firewall
ASA(config-cmap)#match access-list tcp_bypass

Configure the policy map and specify the class map !--- inside this policy map for the ---!
class map. ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
Use the set connection advanced-options tcp-state-bypass !--- command in order to enable ---!
.TCP state bypass feature

ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass
Use the service-policy policymap_name [ global | interface intf ] !--- command in global ---!
configuration mode in order to activate a policy map !--- globally on all interfaces or on a
.targeted interface

ASA(config-pmap-c)#service-policy tcp_bypass_policy outside

ASA(config-pmap-c)#static (inside,outside) 192.168.1.224 10.1.1.0 netmask
255.255.255.224
```

التحقق من الصحة

يعرض الأمر show conn عدد إتصالات TCP و UDP النشطة ويوفر معلومات حول الاتصالات من أنواع مختلفة. لعرض حالة الاتصال لنوع الاتصال المعين، أستخدم الأمر show conn في وضع EXEC ذي الامتيازات. يدعم هذا الأمر عناوين IPv4 و IPv6. يتضمن عرض الإخراج للاتصالات التي تستخدم **تجاوز حالة TCP** العلامة **b**.

استكشاف الأخطاء وإصلاحها

رسالة خطأ

يعرض ASA رسالة الخطأ هذه حتى بعد تمكين ميزة تجاوز TCP-State.

```
PIX|ASA-4-313004:Denied ICMP type=icmp_type, from source_address oninterface%
interface_name to dest_address:no matching session
```

تم إسقاط حزم ICMP بواسطة جهاز الأمان بسبب عمليات التحقق من الأمان التي تمت إضافتها بواسطة ميزة ICMP التي تحدد الحالة والتي تكون عادة إما ردود صدى ICMP دون طلب صدى صالح يتم تمريره بالفعل عبر جهاز الأمان أو رسائل خطأ ICMP غير المرتبطة بأي من TCP أو UDP أو جلسة ICMP التي تم إنشاؤها بالفعل في جهاز الأمان.

يعرض ASA هذا السجل حتى إذا تم تمكين تجاوز حالة TCP لأن تعطيل هذه الوظيفة (أي التحقق من إدخالات إرجاع ICMP للنوع 3 في جدول الاتصال) غير ممكن. ولكن ميزة تجاوز حالة TCP تعمل بشكل صحيح.

أستخدم هذا الأمر لمنع ظهور هذه الرسائل:

```
hostname(config)#no logging message 313004
```

معلومات ذات صلة

- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- طلبات التعليقات (RFCs)
- 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).