تكوين ميزة تجاوز حالة TCP على سلسلة ASA 5500

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين ميزة تجاوز حالة TCP، والتي تسمح لحركة المرور الصادرة والواردة بالتدفق من خلال أجهزة الأمان المعدلة (ASA) من السلسلة Cisco ASA 5500 Series.

المتطلبات الأساسية

المتطلبات

يجب أن يحتوي Cisco ASA على الترخيص الأساسي المثبت على الأقل قبل أن تتمكن من متابعة التكوين الموضح في هذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى سلسلة Cisco ASA 5500 التي تشغل الإصدار x.9 من البرنامج.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة

المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

يقدم هذا القسم نظرة عامة على ميزة تجاوز حالة TCP ومعلومات الدعم ذات الصلة.

نظرة عامة على ميزة تجاوز حالة TCP

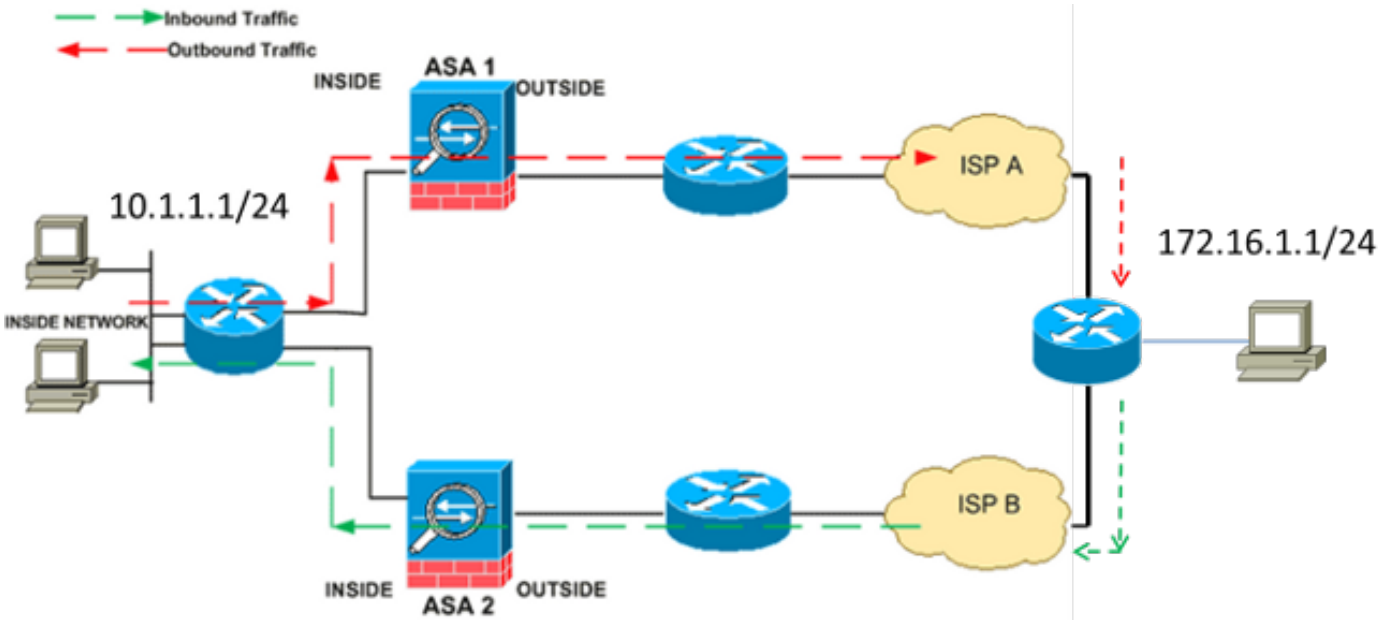
وبشكل افتراضي، يتم فحص جميع حركة المرور التي تمر عبر ASA عبر خوارزمية الأمان المعدلة ويتم السماح بها أو إسقاطها استنادا إلى سياسة الأمان. من أجل زيادة أداء جدار الحماية إلى الحد الأقصى، يتحقق ASA من حالة كل حزمة (على سبيل المثال، يتحقق مما إذا كان اتصالا جديدا أو اتصالا منشئا) ويعينه إما إلى مسار إدارة جلسة العمل (حزمة مزامنة اتصال جديدة (SYN)) أو المسار السريع (اتصال قائم) أو مسار مستوى التحكم (فحص متقدم).

يمكن لحزم TCP التي تطابق الاتصالات الحالية في المسار السريع المرور عبر ASA دون إعادة التحقق من 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، ويجب أن تمر كل من التدفقات الصادرة والواردة 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 على هذا الاتصال عبر *ASA 1*، فإن الحزم تطابق 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، فيمكنك تكوين ميزة تجاوز حالة TCP لحركة مرور معينة. تغير ميزة تجاوز حالة TCP طريقة 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 سلسلة Cisco ASA 5500. بالإضافة إلى ذلك، يمكن أن يتسبب تكوين تجاوز حالة TCP في عدد كبير من الاتصالات إذا لم يتم تنفيذه بشكل صحيح.

معلومات الدعم

يصف هذا القسم معلومات الدعم لميزة تجاوز حالة TCP.

- **وضع السياق**Aميزة تجاوز حالة TCP مدعومة في أوضاع السياق الأحادية والمتعددة.
- **وضع جدار الحماية**نقل **يتم دعم ميزة تجاوز حالة TCP في الأوضاع الموجهة والشفافة.**

• **تجاوز** الفشلنقل نقل تدعم ميزة تجاوز حالة TCP تجاوز الفشل.
لا يتم دعم هذه الميزات عند إستخدام ميزة تجاوز حالة TCP:

• **فحص التطبيق** يتطلب فحص التطبيق AA **فحص التطبيق أن تمر حركة المرور الواردة والصادرة على حد سواء عبر نفس ASA، وبالتالي فإن فحص التطبيق غير مدعوم مع ميزة تجاوز حالة TCP.**

• **المصادقة والتفويض والمحاسبة (AAA)** والجلسات **المصدق** عليهاA عندما يقوم المستخدم بالتصديق باستخدام ASA واحد، يتم رفض حركة المرور التي ترجع عبر ASA الآخر لأن المستخدم لم يصدق مع ASA هذا.

• **اعتراض TCP، الحد الأقصى لاتصال الوليد، الرقم التسلسلي ل** TCPAA لا يتتبع ASA حالة الاتصال، لذلك لا يتم تطبيق هذه الميزات.

- **تم** تعطيل **تطبيع** TCPAATCP Normalizer.

• **وظيفة وحدة خدمات الأمان النمطية (SSM) وبطاقة خدمات الأمان** (ÂA)SSC لا يمكنك إستخدام ميزة تجاوز حالة TCP مع أي تطبيقات تعمل على SSM أو SSC، مثل IPS أو أمان المحتوى (CSC).

ملاحظة: نظرا لأنه قد تم إنشاء جلسة عمل الترجمة بشكل منفصل لكل ASA، فتأكد من تكوين ترجمة عنوان الشبكة (NAT) الثابتة على كل من ASAs لحركة مرور تجاوز حالة TCP. إن يستعمل أنت حركي nat، العنوان أن يكون أخترت للجلسة على *ASA 1* يختلف من العنوان أن يكون أخترت للجلسة على *ASA 2*.

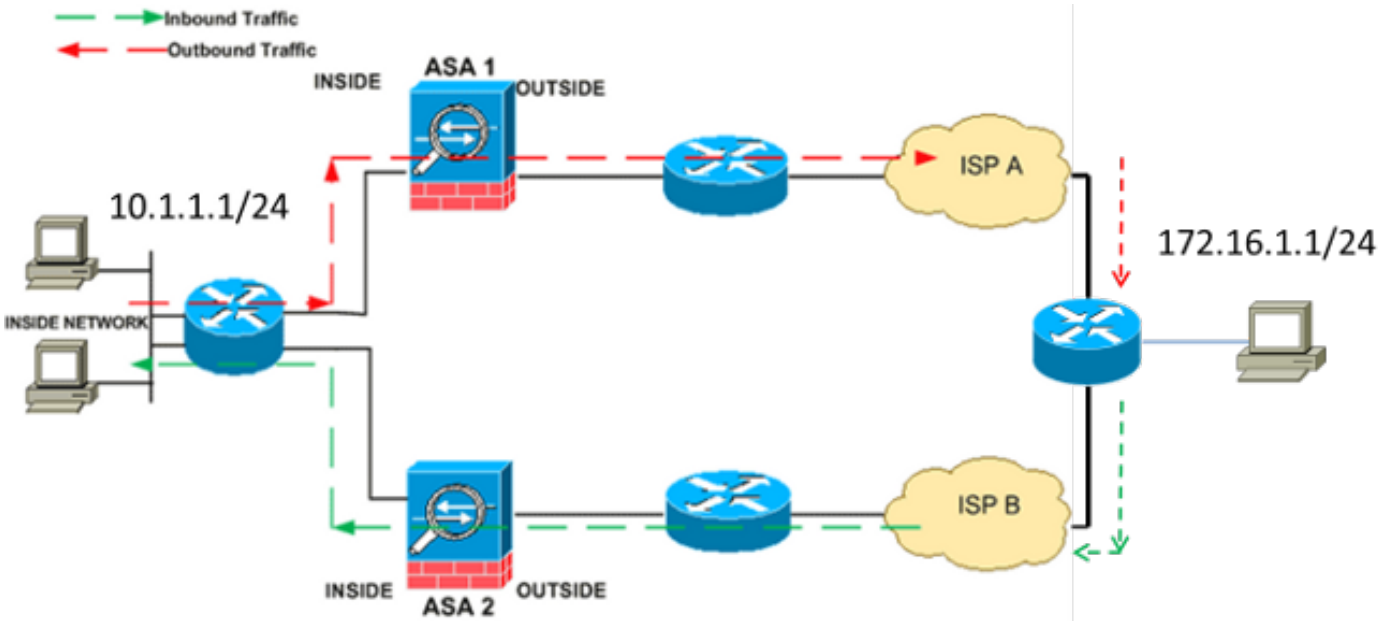
التكوين

يصف هذا القسم كيفية تكوين ميزة تجاوز حالة TCP على سلسلة ASA 5500 في سيناريوين مختلفين.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر التي يتم إستخدامها في هذا القسم.

السيناريو 1

هذه هي الطوبولوجيا المستخدمة للسيناريو الأول:



ملاحظة: يجب تطبيق التكوين الموضح في هذا القسم على كل من ASAs.

أتمت هذا steps in order to شكلت ال TCP دولة تجاوز سمة:

1. أدخل 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.**ملاحظة**: خريطة الفئة التي يتم إستخدامها في هذا المثال هي **tcp_bypass**.
```
ASA(config)#class-map tcp_bypass
```
2. أدخل الأمر match parameter لتحديد حركة مرور المصالح داخل خريطة الفئة. عند إستخدام "إطار عمل السياسة النمطية"، أستخدم الأمر **match access-list** في وضع *تكوين خريطة الفئة* لاستخدام قائمة وصول لتعريف 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
```

ملاحظة: **tcp_bypass** هو اسم قائمة الوصول التي يتم إستخدامها في هذا المثال. أحلت ال يعين حركة مرور (طبقة 4/3 صنف خريطة) قسم من *ال cisco ASA 5500 sery تشكيل مرشد يستعمل ال 8.2، CLI* ل كثير معلومة حول كيف أن يعين حركة مرور الاهتمام.

3. أدخل الأمر policy-map name لإضافة خريطة سياسة أو تحرير خريطة سياسة (موجودة بالفعل) تقوم بتعيين الإجراءات التي يجب إتخاذها فيما يتعلق بحركة مرور خريطة الفئة المحددة. عندما تستخدم إطار عمل السياسة

النمطية، أستخدم الأمر policy-map (بدون الكلمة الأساسية *النوع*) في وضع *التكوين العام* لتعيين الإجراءات لحركة المرور التي قمت بتعريفها باستخدام خريطة فئة الطبقة 4/3 (الأمر **class-map** أو إدارة نوع خريطة الفئة). في هذا المثال، خريطة السياسة هي **tcp_bypass_policy**:

```
ASA(config-cmap)#policy-map tcp_bypass_policy
```

4. أدخل الأمر class في وضع *تكوين خريطة السياسة* من أجل تعيين خريطة الفئة التي تم إنشاؤها (*tcp_bypass*) إلى خريطة السياسة (*tcp_bypass_policy*) حتى يمكنك تعيين الإجراءات إلى حركة 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. أدخل 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. أدخل service-policy policy map_name [عمومي | *قارن*> أمر في *وضع التكوين العام* من أجل تنشيط خريطة سياسة بشكل عام على جميع الواجهات أو على واجهة مستهدفة. لتعطيل سياسة الخدمة، أستخدم الصيغة **no** من هذا الأمر. أدخل الأمر **service-policy** لتمكين مجموعة من السياسات على واجهة. تقوم الكلمة الأساسية **global** بتطبيق خريطة السياسة على جميع الواجهات، كما تقوم الكلمة الأساسية **الواجهة** بتطبيق خريطة السياسة على واجهة واحدة فقط. يتم السماح بسياسة عمومية واحدة فقط. لتجاوز السياسة العامة على واجهة، يمكنك تطبيق سياسة خدمة على تلك الواجهة. يمكنك تطبيق خريطة سياسة واحدة فقط على كل واجهة. فيما يلي مثال:

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

وفيما يلي مثال على تكوين ميزة تجاوز حالة TCP على *ASA1*:

```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance

ASA1(config)#access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.0
255.255.255.0 172.16.1.0

!--- Configure the class map and specify the match parameter for the
!--- class map to match the interesting traffic

ASA1(config)#class-map tcp_bypass
"ASA1(config-cmap)#description "TCP traffic that bypasses stateful firewall
ASA1(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map
!--- inside this policy map for the class map

ASA1(config-cmap)#policy-map tcp_bypass_policy
ASA1(config-pmap)#class tcp_bypass

!--- Use the set connection advanced-options tcp-state-bypass
!--- command in order to enable TCP state bypass feature

ASA1(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 ---!

ASA1(config-pmap-c)#service-policy tcp_bypass_policy outside

NAT configuration ---!

ASA1(config)#object network obj-10.1.1.0
ASA1(config-network-object)#subnet 10.1.1.0 255.255.255.0
ASA1(config-network-object)#nat(inside,outside) static 192.168.1.0
```

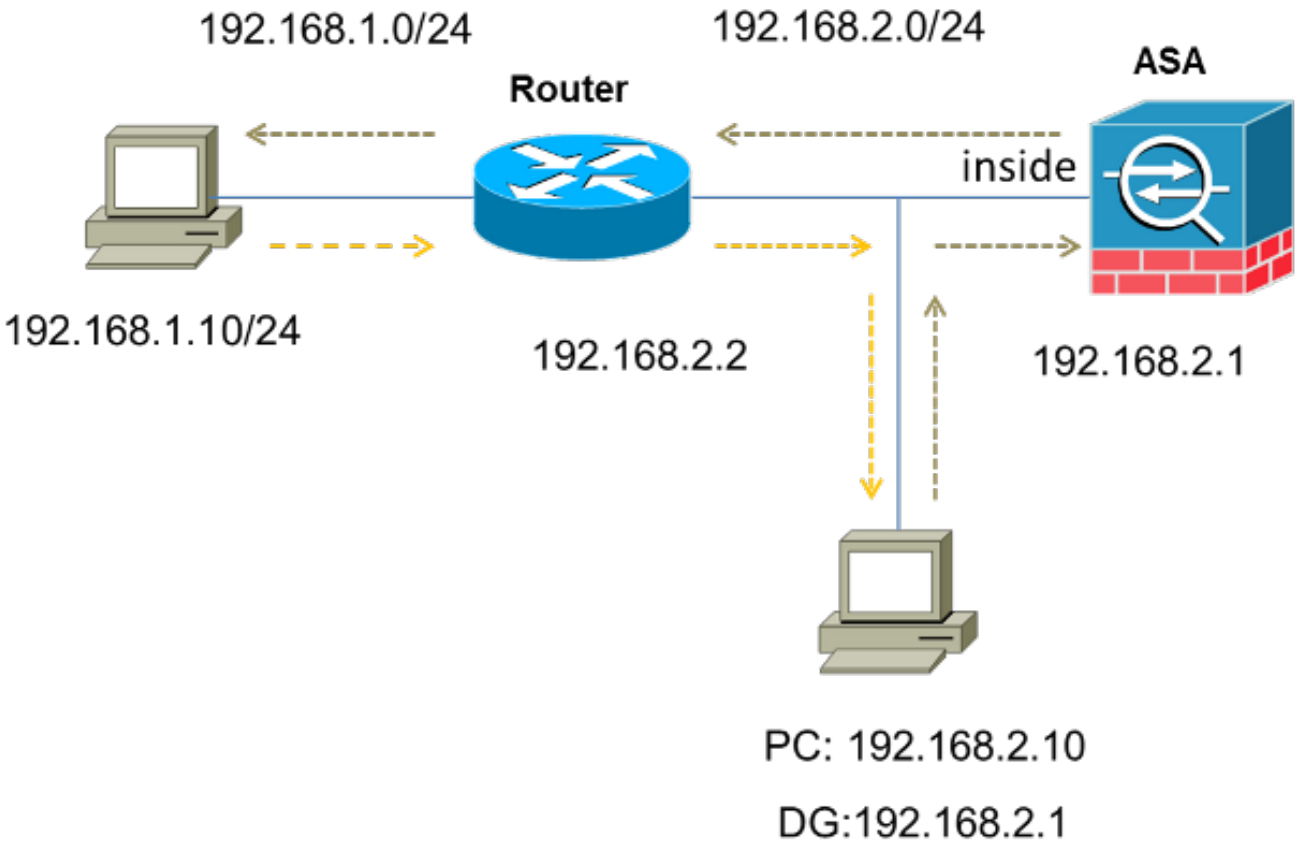
وفيما يلي مثال على تكوين ميزة تجاوز حالة TCP على *ASA2*:

```
Configure the access list to specify the TCP traffic ---!
.that needs to by-pass inspection to improve the performance ---!

ASA2(config)#access-list tcp_bypass extended permit tcp 172.16.1.0 255.255.255.0
255.255.255.0 10.1.1.0

Configure the class map and specify the match parameter for the ---!
.class map to match the interesting traffic ---!

ASA2(config)#class-map tcp_bypass
"ASA2(config-cmap)#description "TCP traffic that bypasses stateful firewall
ASA2(config-cmap)#match access-list tcp_bypass

Configure the policy map and specify the class map ---!
.inside this policy map for the class map ---!

ASA2(config-cmap)#policy-map tcp_bypass_policy
ASA2(config-pmap)#class tcp_bypass

Use the set connection advanced-options tcp-state-bypass ---!
.command in order to enable TCP state bypass feature ---!

ASA2(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 ---!

ASA2(config-pmap-c)#service-policy tcp_bypass_policy outside

NAT configuration ---!

ASA2(config)#object network obj-10.1.1.0
ASA2(config-network-object)#subnet 10.1.1.0 255.255.255.0
ASA1(config-network-object)#nat(inside,outside) static 192.168.1.0
```

السيناريو 2

يصف هذا القسم كيفية تكوين ميزة تجاوز حالة TCP على ASA لسيناريوهات تستخدم التوجيه غير المتماثل، حيث تدخل حركة المرور وتترك ASA من الواجهة نفسها (*u-turning*).

فيما يلي المخطط المستخدم في هذا السيناريو:



أتمت هذا steps in order to شكلت ال TCP دولة تجاوز سمة:

1. قم بإنشاء *قائمة وصول* لمطابقة حركة المرور التي يجب أن تتجاوز فحص TCP:

```
ASA(config)#access-list tcp_bypass extended permit tcp 192.168.2.0 255.255.255.0
255.255.255.0 192.168.1.0
```

2. أدخل 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.**ملاحظة**: خريطة الفئة التي يتم إستخدامها في هذا المثال هي **tcp_bypass**.

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

3. أدخل الأمر match parameter لتحديد حركة مرور المصلحة في خريطة الفئة. عند إستخدام "إطار عمل السياسة النمطية"، أستخدم الأمر **match access-list** في وضع *تكوين خريطة الفئة* لاستخدام قائمة وصول لتعريف 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
```

ملاحظة: **tcp_bypass** هو اسم قائمة الوصول التي يتم إستخدامها في هذا المثال. أحلت يعين حركة مرور (طبقة 4/3 صنف خريطة) قسم من *ال cisco ASA 5500 sery تشكيل مرشد يستعمل ال 8.2، CLI* ل كثير معلومة حول كيف أن يعين حركة مرور الاهتمام.

4. أدخل الأمر policy-map name لإضافة خريطة سياسة أو تحرير خريطة سياسة (موجودة بالفعل) تعمل على تعيين الإجراءات التي يجب إتخاذها فيما يتعلق بحركة مرور خريطة الفئة المحددة. عندما تستخدم إطار عمل السياسة النمطية، أستخدم الأمر policy-map (بدون الكلمة الأساسية *النوع*) في وضع *التكوين العام* لتعيين الإجراءات لحركة المرور التي قمت بتعريفها باستخدام خريطة فئة الطبقة 4/3 (الأمر **class-map** أو إدارة نوع خريطة الفئة). في هذا المثال، خريطة السياسة هي **tcp_bypass_policy**:

```
ASA(config-cmap)#policy-map tcp_bypass_policy
```

5. أدخل الأمر class في وضع *تكوين خريطة السياسة* لتعيين تعيين الفئة التي تم إنشاؤها (*tcp_bypass*) على خريطة السياسة (*tcp_bypass_policy*) حتى يمكنك تعيين الإجراءات 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
```

6. أدخل 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
```

7. أدخل service-policy policy map_name [عمومي | interface *intf*> أمر في *وضع التكوين العام* من أجل تنشيط خريطة سياسة بشكل عام على جميع الواجهات أو على واجهة مستهدفة. لتعطيل سياسة الخدمة، أستخدم الصيغة **no** من هذا الأمر. أدخل الأمر **service-policy** لتمكين مجموعة من السياسات على واجهة. تقوم الكلمة الأساسية **global** بتطبيق خريطة السياسة على جميع الواجهات، وتطبق الكلمة الأساسية **الواجهة** السياسة على واجهة واحدة فقط. يتم السماح بسياسة عمومية واحدة فقط. لتجاوز السياسة العامة على واجهة، يمكنك تطبيق سياسة خدمة على تلك الواجهة. يمكنك تطبيق خريطة سياسة واحدة فقط على كل واجهة. فيما يلي مثال:

```
ASA(config-pmap-c)#service-policy tcp_bypass_policy inside
```

8. السماح بنفس مستوى الأمان لحركة المرور في ASA:

```
ASA(config)#same-security-traffic permit intra-interface
```

هنا مثال تشكيل ل ال TCP دولة تجاوز سمة على ال ASA:

```
Configure the access list to specify the TCP traffic ---!
.that needs to bypass inspection to improve the performance ---!

ASA(config)#access-list tcp_bypass extended permit tcp 192.168.2.0 255.255.255.0
255.255.255.0 192.168.1.0

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 inside
```

```
Permit same security level traffic on the ASA to support U-turning ---!

ASA(config)#same-security-traffic permit intra-interface
```

التحقق من الصحة

أدخل **عرض المخروط** لعرض عدد إتصالات TCP و UDP النشطة ومعلومات حول الاتصالات من أنواع مختلفة. لعرض حالة الاتصال لنوع الاتصال المعين، أدخل **عرض المخروط** في وضع *EXEC* ذي *الامتيازات*.

ملاحظة: يدعم هذا الأمر عناوين IPv4 و IPv6. يتضمن الإخراج الذي يتم عرضه للاتصالات التي تستخدم ميزة تجاوز حالة TCP العلامة **b**.

فيما يلي مثال للمخرجات:

```
ASA(config)show conn
in use, 3 most used 1
TCP tcp 10.1.1.1:49525 tcp 172.16.1.1:21, idle 0:01:10, bytes 230, flags b
```

استكشاف الأخطاء وإصلاحها

لا توجد معلومات محددة حول أستكشاف الأخطاء وإصلاحها لهذه الميزة. ارجع إلى هذه المستندات للحصول على معلومات أستكشاف أخطاء الاتصال وإصلاحها العامة:

- التقاط حزمة ASA باستخدام CLI ومثال تكوين ASDM
- ASA 8.2: تدفق الحزمة من خلال جدار حماية Cisco ASA

ملاحظة: لا يتم نسخ إتصالات تجاوز حالة TCP نسخا متماثلا إلى الوحدة الاحتياطية في زوج تجاوز الفشل.

رسائل الخطأ

يعرض ASA رسالة الخطأ هذه حتى بعد تمكين ميزة تجاوز حالة TCP:

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

يتم إسقاط حزم بروتوكول رسائل التحكم في الإنترنت (ICMP) من قبل ASA بسبب فحوصات الأمان التي تتم إضافتها بواسطة ميزة ICMP المعبرة عن الحالة. وعادة ما تكون هذه ردود *صدى* ICMP دون *طلب صدى* صالح يتم تمريره عبر ASA، أو رسائل خطأ ICMP غير المرتبطة بأي TCP أو UDP أو جلسة ICMP التي يتم إنشاؤها حاليا في ASA.

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

أدخل هذا الأمر لمنع ظهور هذه الرسائل:

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

معلومات ذات صلة

- مدير أجهزة حلول الأمان المعدلة من Cisco
- 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).