تكوين ASA باستخدام قواعد التحكم في الوصول إلى خدمات FirePOWER لتصفية حركة مرور عميل AnyConnect VPN إلى الإنترنت

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين قواعد سياسة التحكم في الوصول (ACP) لفحص حركة المرور التي تأتي من أنفاق الشبكة الخاصة الظاهرية (VPN) أو مستخدمي الوصول عن بعد (RA) واستخدام جهاز الأمان القابل للتكيف (ASA) من Cisco مع خدمات FirePOWER كبوابة إنترنت.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الشبكة الخاصة الظاهرية (VPN) للوصول عن بعد و/أو الشبكة الخاصة الظاهرية (VPN) لشبكة IPSec التي تعمل بنظام النظير إلى النظير.
- تكوين قائمة التحكم في الوصول (Firepower ACP).
- إطار عمل السياسة النمطية (MPF ASA).

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ASA5506W الإصدار 9.6(2.7) لمثال ASDM
- الإصدار 6.1.0-330 من وحدة FirePOWER النمطية لمثال ASDM.
- ASA5506W الإصدار 9.7(1) للمثال FMC.
- إصدار FirePOWER 6. 2. 0 من أجل مثال FMC.

• مركز إدارة Firepower (FMC)، الإصدار 6.2.0

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.

المشكلة

يتعذر على ASA5500-X مع خدمات FirePOWER تصفية حركة مرور مستخدمي AnyConnect و/أو فحصها مثل حركة المرور التي يتم الحصول عليها من مواقع أخرى متصلة بأنفاق IPSec التي تستخدم نقطة واحدة من أمان المحتوى الأساسي.

من الأعراض الأخرى التي يغطيها هذا الحل عدم القدرة على تحديد قواعد معينة ل ACP للمصادر المذكورة دون ظهور مصادر أخرى.

هذا السيناريو شائع جدا لمعرفة متى يتم إستخدام تصميم TunnelAll لحلول VPN التي يتم إنهاؤها على ASA.

الحل

ويمكن تحقيق ذلك بطرق متعددة. بيد أن هذا السيناريو يشمل التفتيش حسب المناطق.

تكوين ASA

الخطوة 1. حدد الواجهات التي يتصل فيها مستخدمو AnyConnect أو أنفاق VPN ب ASA.

أنفاق نظير إلى نظير

هذه خردة لمخرج **خريطة تشفير تشغيل العرض**.

```
crypto map outside_map interface outside
```

مستخدمو AnyConnect

يظهر الأمر **show run webVPN** مكان تمكين الوصول إلى AnyConnect.

```
webvpn
 enable outside
 hostscan image disk0:/hostscan_4.3.05019-k9.pkg
 hostscan enable
 anyconnect image disk0:/anyconnect-win-4.4.01054-webdeploy-k9.pkg 1
 anyconnect image disk0:/anyconnect-macos-4.4.01054-webdeploy-k9.pkg 2
 anyconnect enable
```

في هذا السيناريو، تستقبل الواجهة **الخارجية**، كلا، مستخدمي RA وأنفاق نظير إلى نظير.

الخطوة 2. قم بإعادة توجيه حركة المرور من ASA إلى وحدة FirePOWER باستخدام سياسة عامة.

يمكن القيام بذلك باستخدام **تطابق أي** شرط أو قائمة تحكم في الوصول (ACL) معرفة لإعادة توجيه حركة المرور.

مثال مع **مطابقة أي** تطابق.

```
class-map SFR
  match any

policy-map global_policy
  class SFR
    sfr fail-open

service-policy global_policy global
```

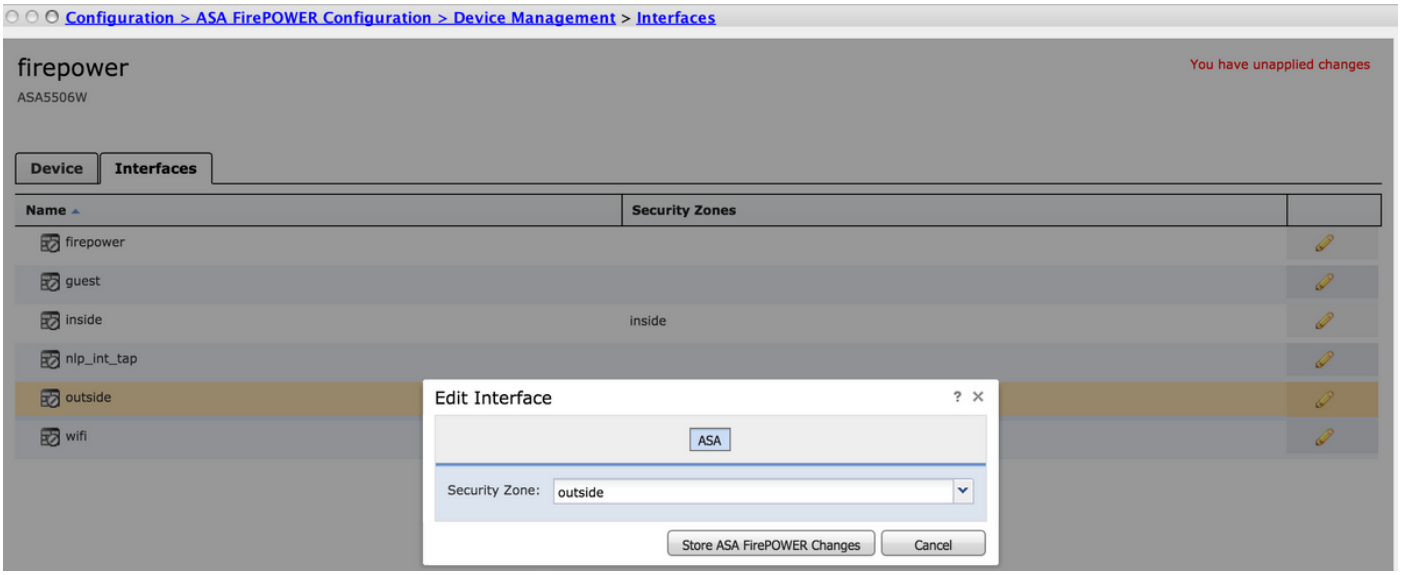
مثال على مطابقة قائمة التحكم في الوصول (ACL).

```
access-list sfr-acl extended permit ip any any

class-map SFR
  match access-list sfr-acl

policy-map global_policy
  class SFR
    sfr fail-open

service-policy global_policy global
```

في سيناريو أقل شيوعا، يمكن إستخدام سياسة خدمة للواجهة الخارجية. لا يتم تغطية هذا المثال في هذا المستند.

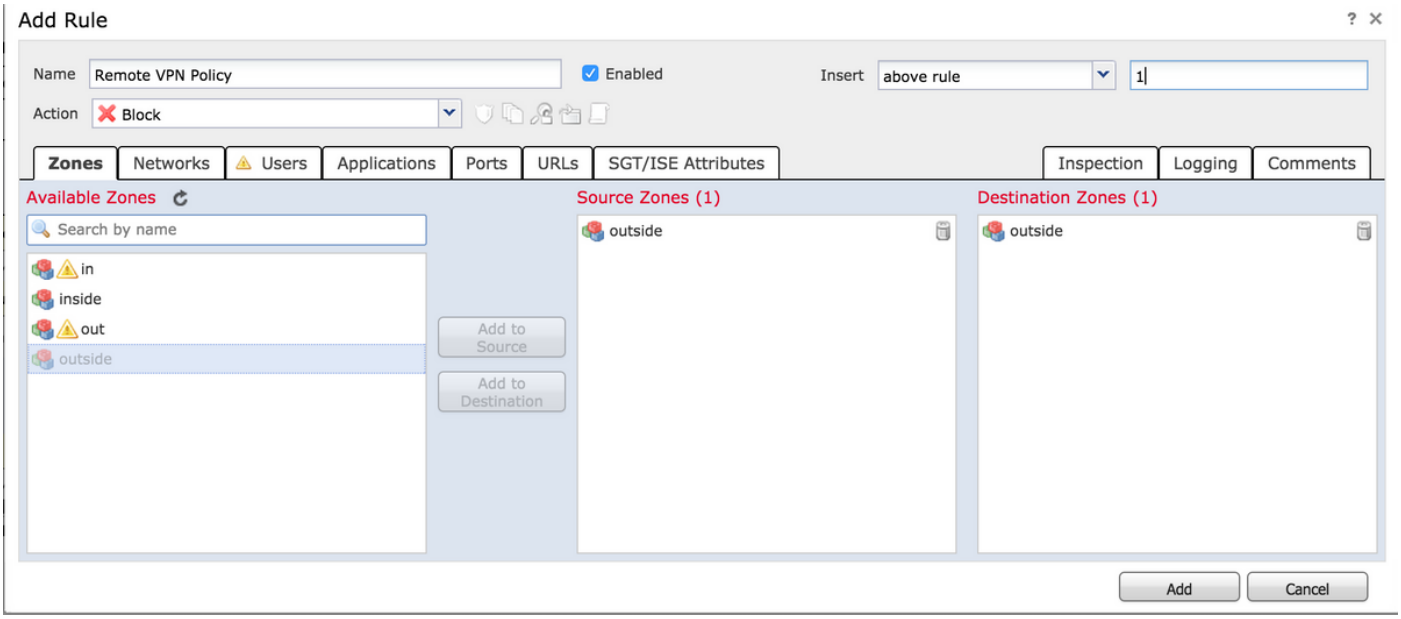
الوحدة النمطية ASA FirePOWER المدارة بواسطة تكوين ASDM

الخطوة 1. عينت القارن الخارجي منطقة واحدة في **التشكيل** > ASA FirePOWER **تشكيل** > **إدارة الجهاز**. في هذه الحالة، تلك المنطقة تسمى **خارج**.



الخطوة 2. حدد **إضافة قاعدة** في **التكوين** > تكوين ASA FirePOWER > **السياسات** > **سياسة التحكم في الوصول**.

الخطوة 3. من علامة التبويب **مناطق**، حدد **خارج** المنطقة كمصدر ووجهة للقاعدة الخاصة بك.



الخطوة 4. حدد الإجراء والعنوان وأي شروط أخرى مرغوبة لتعريف هذه القاعدة.

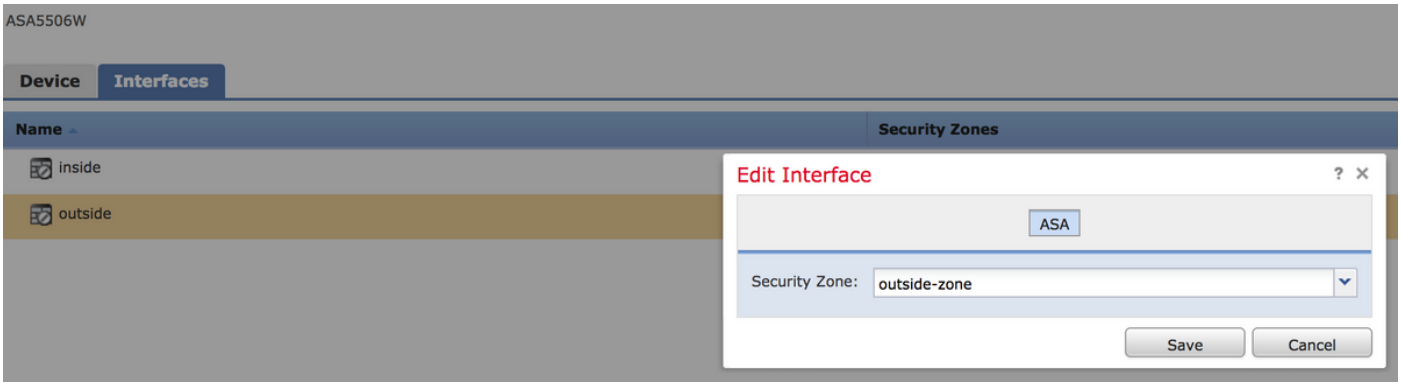
يمكن إنشاء قواعد متعددة لتدفق حركة المرور هذا. من المهم فقط أن نضع في الاعتبار أن مناطق المصدر والوجهة يجب أن تكون المنطقة المخصصة لمصادر الشبكة الخاصة الظاهرية (VPN) والإنترنت.

تأكد من عدم وجود سياسات عامة أخرى يمكن أن تتطابق قبل هذه القواعد. من المفضل أن تكون هذه القواعد أعلى من تلك المحددة إلى **أي** منطقة.

الخطوة 5. انقر فوق **تغييرات ASA FirePOWER للتخزين** ثم **نشر تغييرات FirePOWER** لتدخل هذه التغييرات حيز التنفيذ.

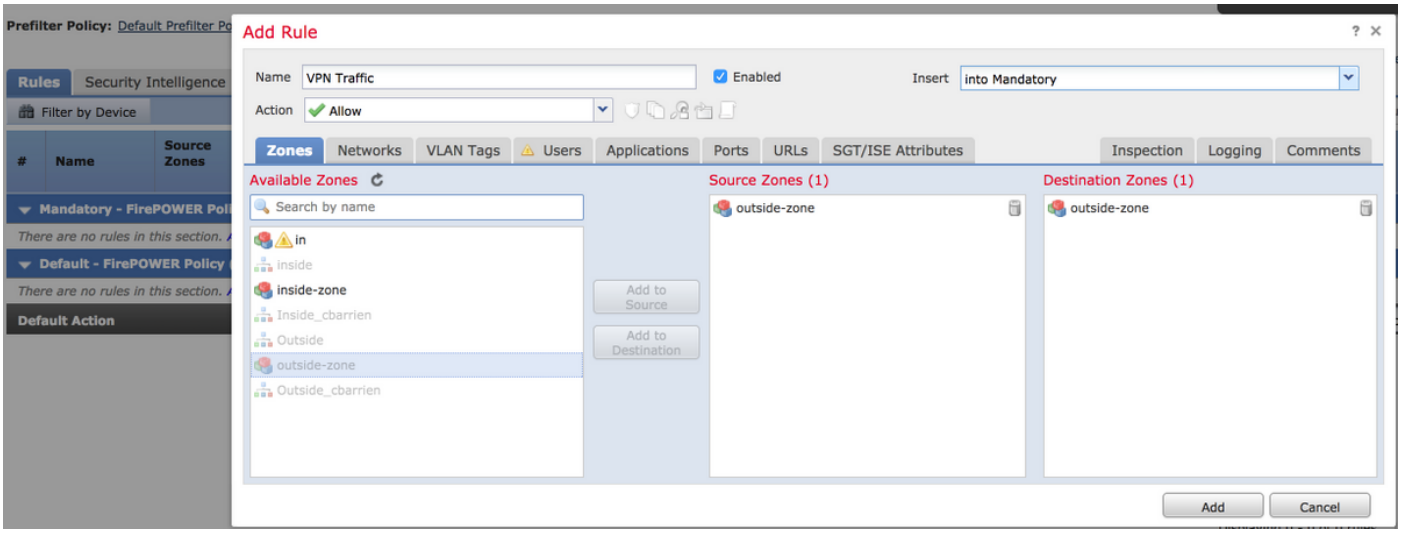
وحدة ASA FirePOWER النمطية المدارة بواسطة تكوين FMC

الخطوة 1. تخصيص منطقة واحدة للواجهة الخارجية في **الأجهزة > الإدارة > الواجهات**. في هذه الحالة، تلك المنطقة تسمى **المنطقة الخارجية**.



الخطوة 2. حدد **إضافة قاعدة** في **السياسات > التحكم في الوصول > تحرير**.

الخطوة 3. من علامة التبويب **مناطق**، حدد **المنطقة الخارجية** كمصدر ووجهة للقاعدة الخاصة بك.



الخطوة 4. حدد الإجراء والعنوان وأي شروط أخرى مرغوبة لتعريف هذه القاعدة.

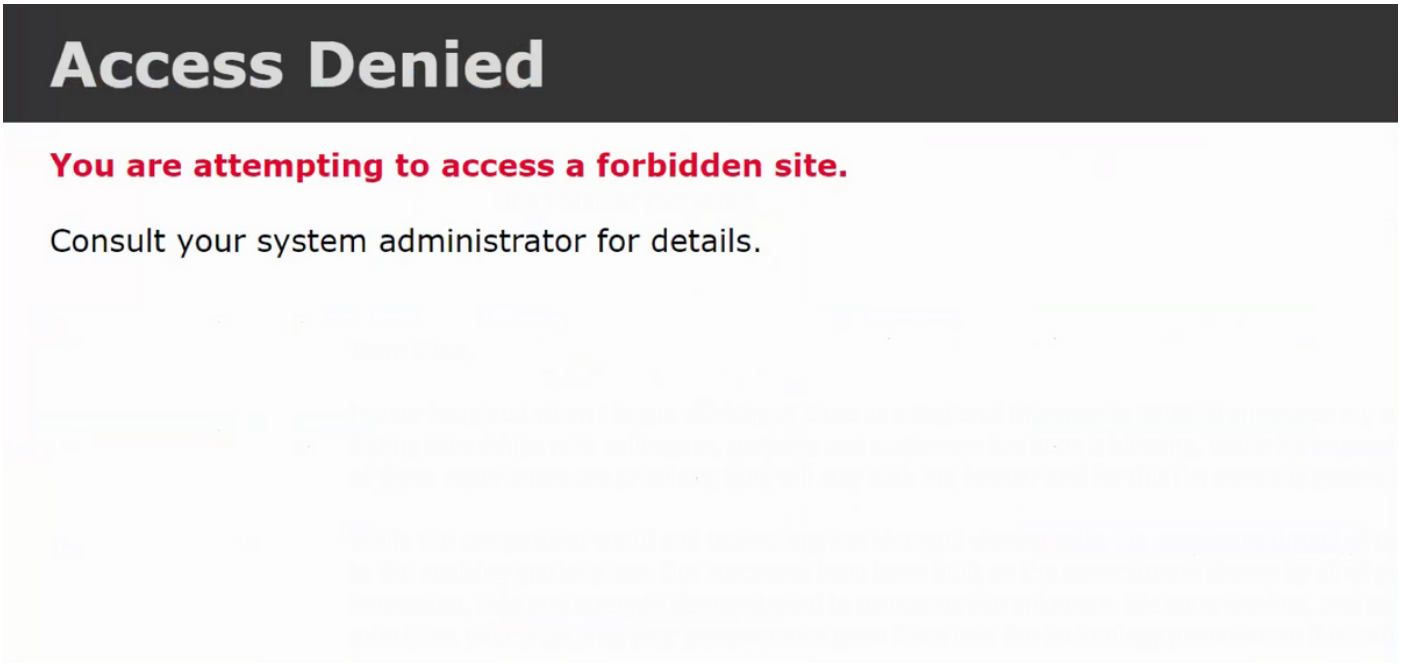
يمكن إنشاء قواعد متعددة لتدفق حركة المرور هذا. من المهم فقط أن نضع في الاعتبار أن مناطق المصدر والوجهة يجب أن تكون المنطقة المخصصة لمصادر الشبكة الخاصة الظاهرية (VPN) والإنترنت.

تأكد من عدم وجود سياسات عامة أخرى يمكن أن تتطابق قبل هذه القواعد. من المفضل أن تكون هذه القواعد أعلى من تلك المحددة إلى **أي** منطقة.

الخطوة 5. انقر فوق **حفظ** ثم **نشر** لتفعيل هذه التغييرات.

نتيجة

بعد انتهاء النشر، تتم الآن تصفية/فحص حركة مرور AnyConnect بواسطة قواعد ACP المطبقة. في هذا المثال، تم حظر عنوان URL بنجاح.



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).