

عم ASA HTTP URL ةي فرصت لماع فئاظو Regex

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[التكوين](#)

[خطوات التكوين](#)

[حدد قائمة قصيرة للمجالات التي يجب حظرها أو السماح بها](#)

[قم بإنشاء خريطة فئة regex تطابق كل المجالات المعنية](#)

[إنشاء خريطة سياسة فحص HTTP التي تسقط حركة مرور تطابق هذه المجالات أو تسمح بها](#)

[تطبيق خريطة سياسة فحص HTTP هذه على فحص HTTP في إطار عمل السياسة النمطية](#)

[المشكلات الشائعة](#)

المقدمة

يصف هذا المستند تكوين عوامل تصفية URL على جهاز الأمان القابل للتكيف (ASA) باستخدام محرك فحص HTTP. يتم إكمال هذا عند مطابقة أجزاء من طلب HTTP مع استخدام قائمة من أنماط regex. يمكنك إما حظر عناوين URL معينة أو حظر كافة عناوين URL باستثناء عدد محدد منها.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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.

التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم [أداة بحث الأوامر](#) (للعلماء [المسجلين](#) فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

خطوات التكوين

هذه هي خطوات التكوين العام:

1. حدد قائمة قصيرة للمجالات التي يجب حظرها أو السماح بها
 2. قم بإنشاء خريطة فئة regex تطابق كل المجالات المعنية
 3. إنشاء خريطة سياسة فحص HTTP التي تسقط حركة مرور تطابق هذه المجالات أو تسمح بها
 4. تطبيق خريطة سياسة فحص HTTP هذه على فحص HTTP في إطار عمل السياسة النمطية
- ويغض النظر عما إذا كنت تحاول حظر بعض المجالات والسماح بالمجالات الأخرى أو حظر جميع المجالات والسماح فقط ببعض المجالات، فإن الخطوات متطابقة باستثناء إنشاء خريطة سياسة فحص HTTP.

حدد قائمة قصيرة للمجالات التي يجب حظرها أو السماح بها

بالنسبة لمثال التكوين هذا، يتم حظر هذه المجالات أو السماح بها:

cisco1.com •
cisco2.com •
cisco3.com •

شكلت ال regex نمط ل هذا مجال:

```
"regex cisco1.com "cisco1.com"regex cisco2.com "cisco2.com"regex cisco3.com "cisco3.com"
```

قم بإنشاء خريطة فئة regex تطابق كل المجالات المعنية

تكوين فئة regex تطابق أنماط regex:

```
class-map type regex match-any domain-regex-classmatch regex cisco1.commatch regex  
cisco2.commatch regex cisco3.com
```

إنشاء خريطة سياسة فحص HTTP التي تسقط حركة مرور تطابق هذه المجالات أو تسمح بها

لفهم الشكل الذي سيبدو عليه هذا التكوين، اختر الوصف الذي يناسب الهدف من عامل تصفية URL هذا على أفضل وجه. سيتم إما أن تكون فئة regex التي تم إنشاؤها أعلاه قائمة بالمجالات التي يجب السماح بها أو قائمة بالمجالات التي يجب حظرها.

• السماح بجميع المجالات باستثناء المجالات المدرجة مفتاح هذا التكوين هو إنشاء خريطة فئة حيث يتم تصنيف معاملة HTTP التي تطابق المجالات المدرجة ك "blocked-domain-class". تمت إعادة تعيين حركة HTTP التي تطابق هذه الفئة وإغلاقها. بشكل أساسي، يتم إعادة تعيين حركة HTTP التي تطابق هذه المجالات فقط.

```
class-map type inspect http match-all blocked-domain-class match request header host regex  
class domain-regex-class!policy-map type inspect http regex-filtering-policy parameters  
class blocked-domain-class reset log
```

- حظر كافة المجالات باستثناء المجالات المدرجة المفتاح إلى هذا تشكيل أن خلقت صنف خريطة يستعمل الكلمة المفتاح "مطابقة لا". هذا يوضح لجدار الحماية أن أي مجالات لا تطابق قائمة المجالات يجب أن تطابق الفئة المسماة "allowed-domain-class". سيتم إعادة تعيين حركات HTTP التي تطابق هذه الفئة وإغلاقها. بشكل أساسي، سيتم إعادة تعيين جميع حركات HTTP ما لم تطابق المجالات المدرجة.

```
class-map type inspect http match-all allowed-domain-class match not request header host
  regex class domain-regex-class!policy-map type inspect http regex-filtering-policy
  parameters class allowed-domain-class reset log
```

تطبيق خريطة سياسة فحص HTTP هذه على فحص HTTP في إطار عمل السياسة النمطية

الآن بعد تكوين خريطة سياسة فحص HTTP ك "regex-filtering-policy"، قم بتطبيق خريطة السياسة هذه على فحص HTTP الموجود أو فحص جديد في إطار عمل سياسة الوحدات. على سبيل المثال، يؤدي ذلك إلى إضافة الفحص إلى الفئة "inspection_default" التي تم تكوينها في "global_policy".

```
policy-map global_policy class inspection_default inspect http regex-filtering-policy
```

المشكلات الشائعة

عند تكوين خريطة سياسة فحص HTTP وخريطة فئة HTTP، تأكد من عدم تكوين المطابقة أو المطابقة كما يجب أن تكون للهدف المرغوب. هذه كلمة أساسية بسيطة للتخطي ينتج عنها سلوك غير مقصود. كما أن هذا الشكل من معالجة regex، شأنه شأن أي معالجة متقدمة للحزم، قد يتسبب في زيادة استخدام وحدة المعالجة المركزية (CPU) ل ASA وكذلك إسقاط الخرج. أستخدم الحذر عند إضافة المزيد والمزيد من أنماط regex.

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا