جدار الحماية التقليدي/بروتوكول IPS من Cisco IOS: تكوين التحكم في الوصول المستند إلى السياق (CBAC) للحماية من رفض الخدمة

المحتويات

المقدمة

يصف هذا المستند إجراء التوليف لمعلمات رفض الخدمة (DoS) في جدار الحماية التقليدي من Cisco IOS® مع CBAC.

توفر CBAC وظيفة تصفية حركة المرور المتقدمة ويمكن إستخدامها كجزء متكامل من جدار حماية الشبكة.

تشير رفض الخدمة (DoS) بشكل عام إلى نشاط الشبكة الذي يؤدي عن قصد أو غير قصد إلى إرباك موارد الشبكة مثل النطاق الترددي لارتباط شبكة الاتصال واسعة النطاق (WAN) أو جداول اتصال جدار الحماية أو ذاكرة المضيف النهائي أو وحدة المعالجة المركزية (CPU) أو إمكانات الخدمة. في أسوأ السيناريوهات، يطغى نشاط رفض الخدمة (DoS) على المورد الضعيف (أو المستهدف) إلى درجة يصبح فيها المورد غير متوفر، ويحظر اتصال شبكة الاتصال واسعة النطاق (WAN) أو الوصول إلى الخدمة للمستخدمين الشرعيين.

يمكن أن يساهم جدار حماية Cisco IOS في التخفيف من نشاط رفض الخدمة (DoS) إذا كان يحتفظ بعدادات عدد إتصالات TCP "نصف المفتوحة"، بالإضافة إلى معدل الاتصال الإجمالي من خلال جدار الحماية وبرنامج منع التسلل في كل من جدار الحماية الكلاسيكي (**فحص ip**) وجدار الحماية المستند إلى منطقة.

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.

الاصطلاحات

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

معلومات أساسية

الاتصالات نصف المفتوحة هي إتصالات TCP التي لم تكمل مصافحة SYN-SYN/ACK الثلاثية الإتجاه التي يتم إستخدامها دائما من قبل نظراء TCP للتفاوض على معلمات إتصالهم المتبادل. يمكن أن تشير أعداد كبيرة من الاتصالات نصف المفتوحة إلى نشاط ضار، مثل هجمات رفض الخدمة (DoS) أو هجمات رفض الخدمة الموزعة. يتم تنفيذ أحد أنواع هجمات رفض الخدمة (DoS) بواسطة برامج ضارة تم تطويرها عن قصد، مثل الفيروسات المتنقلة أو الفيروسات التي تصيب أجهزة مضيفة متعددة على الإنترنت وتحاول إرباك خوادم معينة على الإنترنت بهجمات SYN، حيث يتم إرسال أعداد كبيرة من إتصالات SYN إلى الخادم بواسطة أجهزة مضيفة متعددة على الإنترنت أو داخل الشبكة الخاصة لإحدى المؤسسات. تمثل هجمات SYN خطرا على خوادم الإنترنت نظرا لأنه يمكن تحميل جداول اتصال الخوادم بمحاولات اتصال SYN "زائفة" التي تصل بشكل أسرع من قدرة الخادم على التعامل مع الاتصالات الجديدة. هذا نوع من هجمات رفض الخدمة (DoS) لأن العدد الكبير من الاتصالات في قائمة اتصال TCP الخاصة بخادم الضحية يمنع وصول المستخدم المشروع إلى خوادم الإنترنت للضحية.

كما يتعرف جدار حماية Cisco IOS على جلسات عمل بروتوكول مخطط بيانات المستخدم (UDP) مع حركة المرور في إتجاه واحد فقط على أنها "نصف مفتوحة" لأن العديد من التطبيقات التي تستخدم UDP للنقل تعترف باستقبال البيانات. من المحتمل أن تكون جلسات UDP دون حركة مرور الإرجاع مؤشرا على نشاط DoS أو محاولات الاتصال بين جهازين مضيفين، حيث أصبح أحد الأجهزة المضيفة غير مستجيب. العديد من أنواع حركة مرور UDP، مثل رسائل السجل، وحركة مرور إدارة شبكة SNMP، وبث وسائط الصوت والفيديو، وحركة مرور الإشارات، أستخدم حركة مرور البيانات في إتجاه واحد فقط لحمل حركة المرور الخاصة بها. يطبق العديد من هذه الأنواع من حركة المرور ذكاء خاص بالتطبيق لمنع أنماط حركة المرور أحادي الإتجاه من التأثير سلبا على سلوك جدار الحماية و IPS DoS.

قبل الإصدار 12.4(11)T من برنامج Cisco IOS Software و 12.4(10)، وفر فحص حزم Cisco IOS المعبرة الحماية من هجمات رفض الخدمة (DoS) كإعداد افتراضي عند تطبيق قاعدة فحص. قام الإصدار 12.4(11)T من برنامج Cisco IOS Software و 12.4(10) بتعديل إعدادات رفض الخدمة (DoS) الافتراضية بحيث لا يتم تطبيق حماية رفض الخدمة (DoS) تلقائيا، ولكن عدادات نشاط الاتصال لا تزال نشطة. عندما تكون حماية DoS نشطة، أي عند إستخدام القيم الافتراضية على إصدارات البرامج القديمة، أو عند تعديل القيم إلى النطاق الذي يؤثر على حركة المرور، يتم تمكين حماية DoS على الواجهة التي يتم تطبيق الفحص فيها، في الإتجاه الذي يتم فيه تطبيق جدار الحماية، لبروتوكولات تكوين سياسة جدار الحماية التي سيتم فحصها. لا يتم تمكين حماية رفض الخدمة (DoS) إلا على حركة مرور الشبكة إذا دخلت حركة المرور على واجهة أو تركتها مع تطبيق الفحص في نفس إتجاه حركة المرور الأولية (حزمة SYN أو حزمة UDP الأولى) لاتصال TCP أو جلسة UDP.

يوفر فحص جدار حماية Cisco IOS العديد من القيم القابلة للتعديل للحماية من هجمات رفض الخدمة (DoS). تتضمن إصدارات برنامج Cisco IOS software التي تسبق الإصدار 12.4(11)T و 12.4(10) قيم رفض الخدمة (DoS) الافتراضية التي يمكن أن تتداخل مع عملية الشبكة المناسبة إذا لم يتم تكوينها للمستوى المناسب من نشاط الشبكة في الشبكات حيث تتجاوز معدلات الاتصال القيم الافتراضية. تسمح لك هذه المعلمات بتكوين النقاط التي يبدأ عندها سريان حماية DoS لموجه جدار الحماية الخاص بك. عندما تتجاوز عدادات رفض الخدمة (DoS) الخاصة بالموجه لديك القيم الافتراضية أو التي تم تكوينها، يقوم الموجه بإعادة تعيين اتصال نصف مفتوح قديم لكل اتصال

جديد يتجاوز القيم القصوى غير المكتملة المكونة أو قيم عالية لمدة دقيقة واحدة حتى ينخفض عدد جلسات العمل نصف المفتوحة إلى أقل من القيم المنخفضة القصوى غير المكتملة. يرسل الموجه رسالة syslog إذا تم تمكين التسجيل، وإذا تم تكوين نظام منع التسلل (IPS) على الموجه، يرسل موجه جدار الحماية رسالة توقيع DoS من خلال تبادل أحداث جهاز الأمان (SDEE). إذا لم يتم تعديل معلمات رفض الخدمة (DoS) إلى السلوك العادي لشبكتك، فيمكن أن يؤدي نشاط الشبكة العادي إلى تشغيل آلية حماية رفض الخدمة (DoS)، وهو ما يتسبب في حالات فشل التطبيقات وضعف أداء الشبكة والاستخدام العالي لوحدة المعالجة المركزية (CPU) على موجه جدار حماية Cisco IOS.

التكوين

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

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

ضبط منع الخدمة لبرنامج Cisco IOS Software Classic (IP Inspection) وجدار الحماية ونظام منع التسلل

يحتفظ جدار حماية Cisco IOS التقليدي بمجموعة عالمية من عدادات رفض الخدمة (DoS) للموجه، ويتم تطبيق جميع جلسات عمل جدار الحماية لجميع سياسات جدار الحماية على جميع الواجهات على المجموعة العالمية من عدادات جدار الحماية.

يوفر الفحص التقليدي لجدار الحماية Cisco IOS الحماية من هجوم رفض الخدمة (DoS) بشكل افتراضي عند تطبيق جدار حماية تقليدي. يتم تمكين حماية رفض الخدمة (DoS) على جميع الواجهات التي يتم تطبيق الفحص عليها، في الإتجاه الذي يتم فيه تطبيق جدار الحماية، لكل خدمة أو بروتوكول تم تكوين سياسة جدار الحماية لفحصه. يوفر جدار الحماية التقليدي العديد من القيم القابلة للتعديل للحماية ضد هجمات رفض الخدمة (DoS). الإعدادات الافتراضية القديمة (من صور البرامج قبل الإصدار T(11)12.4) الموضحة في الجدول 1 يمكن أن تتداخل مع عملية الشبكة المناسبة إذا لم يتم تكوينها للمستوى المناسب من نشاط الشبكة في الشبكات حيث تتجاوز معدلات الاتصال القيم الافتراضية. يمكن عرض إعدادات DoS باستخدام أمر **show ip inspection config** EXEC، ويتم تضمين الإعدادات مع إخراج **فحص ip sh all**.

يستخدم CBAC مهلات وعتبات لتحديد مدة إدارة معلومات الحالة للجلسة، وكذلك لتحديد متى يتم إسقاط الجلسات التي لا تصبح مستقرة بالكامل. وتنطبق حالات انتهاء المهلة هذه والحدود بشكل عام على جميع جلسات العمل.

الجدول 1 حدود الحماية الافتراضية ل DoS لجدار الحماية الكلاسيكي		
قيمة حماية DoS	**قبل الإصدار T/12.4(10(11)12.4)**	**T/12.4(10(11)12.4) والإصدارات اللاحقة**
قيمة عالية غير مكتملة إلى أقصى حد	500	لامتناهي
قيمة منخفضة غير مكتملة إلى أقصى حد	400	لامتناهي
قيمة عالية لمدة دقيقة واحدة	500	لامتناهي
قيمة منخفضة لمدة دقيقة واحدة	400	لامتناهي
قيمة مضيف TCP القصوى غير المكتملة	50	لامتناهي

تحتفظ الموجهات التي تم تكوينها لتطبيق جدار الحماية Cisco IOS VRF-Aware بمجموعة واحدة من العدادات لكل VRF.

يحتفظ عداد "فحص ip عالي لمدة دقيقة واحدة" و"فحص ip منخفض لمدة دقيقة واحدة" بمجموع جميع محاولات اتصال TCP و UDP و ICMP (Internet Control Message Protocol) خلال الدقيقة السابقة من تشغيل الموجه، سواء كانت الاتصالات ناجحة أم لا. قد يشير إرتفاع معدل الاتصال إلى إصابة الدودة بشبكة خاصة أو إلى محاولة هجوم رفض الخدمة (DoS) على خادم.

بينما لا يمكنك "تعطيل" حماية "رفض الخدمة (DoS)" لجدار الحماية الخاص بك، يمكنك ضبط حماية "رفض الخدمة (DoS)" بحيث لا تصبح سارية المفعول ما لم يكن هناك عدد كبير جدا من الاتصالات نصف المفتوحة في جدول جلسات العمل الخاص بموجه جدار الحماية الخاص بك.

حماية جدار حماية DoS

اتبع هذا الإجراء لضبط حماية رفض الخدمة (DoS) لجدار الحماية الخاص بك على نشاط شبكتك:

1. تأكد من أن شبكتك ليست مصابة بفيروسات أو ديدان يمكن أن تؤدي إلى قيم اتصال نصف مفتوحة كبيرة بشكل خاطئ أو معدلات اتصال تم محاولة تحقيقها. إذا لم تكن شبكتك "نظيفة"، فلا توجد طريقة لضبط حماية رفض الخدمة (DoS) لجدار الحماية لديك بشكل صحيح. يجب عليك مراقبة نشاط شبكتك خلال فترة من النشاط النموذجي. إذا قمت بضبط إعدادات حماية رفض الخدمة (DoS) الخاصة بشبكتك خلال فترة من نشاط الشبكة الخامل أو المنخفض، فمن المحتمل أن تتجاوز مستويات النشاط العادية إعدادات حماية رفض الخدمة (DoS).
2. تعيين القيم العليا غير المكتملة إلى قيم عالية جدا:

```
ip inspect max-incomplete high 20000000
ip inspect one-minute high 100000000
ip inspect tcp max-incomplete host 100000 block-time 0
```

وهذا يمنع الموجه من توفير حماية رفض الخدمة (DoS) أثناء قيامك بمراقبة أنماط الاتصال لشبكتك. إذا كنت ترغب في ترك حماية رفض الخدمة (DoS) معطلة، فقم بإيقاف هذا الإجراء الآن.**ملاحظة:** إذا كان الموجه لديك يعمل ببرنامج Cisco IOS Software الإصدار 12.4(11)T أو إصدار أحدث، أو الإصدار 12.4(10) أو إصدار أحدث، فأنت لا تحتاج إلى رفع قيم حماية رفض الخدمة (DoS) الافتراضية؛ فهي معينة بالفعل إلى الحدود القصوى الخاصة بها بشكل افتراضي.**ملاحظة:** إذا كنت ترغب في تمكين منع منع منع الخدمة الخاص بمضيف TCP الأكثر صرامة والذي يتضمن حظر بدء الاتصال بالمضيف، فيجب عليك تعيين وقت الحظر المحدد في الأمر **ip inspection tcp max-incomplete host**

3. مسح إحصائيات جدار حماية Cisco IOS باستخدام هذا الأمر:

```
show ip inspect statistics reset
```

4. أترك الموجه الذي تم تكوينه في هذه الحالة لبعض الوقت، ربما لمدة تتراوح من 24 إلى 48 ساعة، لذلك يمكنك ملاحظة نمط الشبكة على مدى يوم كامل واحد على الأقل من دورة نشاط الشبكة النموذجية.**ملاحظة:** بينما يتم تعديل القيم إلى مستويات عالية جدا، لا تستفيد شبكتك من حماية جدار حماية Cisco IOS أو حماية رفض الخدمة (IPS).
5. بعد فترة المراقبة، تحقق من عدادات رفض الخدمة (DoS) باستخدام هذا الأمر:

```
show ip inspect statistics
```

المعلمات التي يجب عليك مراعاتها والتي يتم من خلالها ضبط حماية رفض الخدمة (DoS) وإبرازها **بأحرف داكنة**:

```
Packet inspection statistics
[process switch:fast switch]
[tcp packets: [218314:7878692
[udp packets: [501498:65322
```

```
                                                [packets: [376676:80455
                                                [packets: [5738:4042411
                                                [smtp packets: [11:11077
                                                   [ftp packets: [2291:0
                                      Interfaces configured for inspection 2
                                           Session creations since subsystem
                                             startup or last reset 688030
                                                      Current session counts
                                          [estab/half-open/terminating) [0:0:0)
                                                      Maxever session counts
                                      [estab/half-open/terminating) [207:56:35)
                                                  Last session created 00:00:05
                                                     Last statistic reset never
                                                   Last session creation rate 1
                                                Maxever session creation rate 330
                                                  Last half-open session total 0
                                                       TCP reassembly statistics
                                      received 46591 packets out-of-order; dropped 16454
                                           peak memory usage 48 KB; current usage: 0 KB
                                                       peak queue length 16
```

6. قم بتكوين **فحص ip** غير **مكتمل** إلى قيمة أعلى بنسبة 25٪ من عدد جلسات العمل maxEver المشار إليها وقيمة نصف مفتوحة للموجه الخاص بك. يوفر المضاعف 1. 25 مساحة خالية تزيد عن السلوك المرئي، على سبيل المثال:

```
                                                      Maxever session counts
                                          [estab/half-open/terminating) [207:56:35)
                                                          70 = 1.25 * 56
```

التكوين:

```
(router(config
ip inspect max-incomplete high 70#
```

ملاحظة: يصف هذا المستند إستخدام مضاعف 1.25 ضعف النشاط النموذجي لشبكتك لتعيين حدود للمشاركة في حماية رفض الخدمة (DoS). إذا لاحظت أن شبكتك في حالة الذروة النموذجية لنشاط الشبكة، فيجب أن يوفر ذلك مساحة كافية لتجنب تنشيط حماية رفض الخدمة (DoS) للموجه في جميع الظروف باستثناء الظروف غير المعتادة. إذا رأت شبكتك دوريا دفعات كبيرة من نشاط الشبكة المشروع التي تتجاوز هذه القيمة، يقوم الموجه باتصال إمكانيات حماية DoS، والتي يمكن أن تتسبب في تأثير سلبي على بعض حركة مرور الشبكة. يجب عليك مراقبة سجلات الموجه الخاصة بك لاكتشاف نشاط DoS وضبط **فحص ip للحد الأقصى غير المكتمل** و/أو **فحص ip** لحدود **عالية** لمدة دقيقة واحدة لتجنب تشغيل DoS، بعد تحديد أنه تم مواجهة الحدود نتيجة لنشاط الشبكة المشروع. يمكنك التعرف على تطبيق حماية DoS من خلال وجود رسائل السجل مثل:

7. قم بتكوين **فحص ip max-incomplete low** إلى القيمة التي يتم عرضها للموجه الخاص بك لعدد جلسات العمل maxEver الخاصة به، على سبيل المثال:

```
                                                      Maxever session counts
                                          [estab/half-open/terminating) [207:56:35)
```

التكوين:

```
(router(config
ip inspect max-incomplete low 56#
```

8. يحتفظ عداد **فحص ip** لمدة دقيقة واحدة ومنخفض **دقيقة واحدة** بمجموعة من جميع محاولات اتصال TCP و UDP و ICMP (Internet Control Message Protocol) خلال الدقيقة السابقة من عملية الموجه، سواء كانت الاتصالات ناجحة أم لا. قد يشير إرتفاع معدل الاتصال إلى إصابة أحد الفيروسات المتنقلة في شبكة خاصة أو إلى محاولة هجوم رفض الخدمة (DoS) على أحد الخوادم. تمت إضافة إحصائيات فحص إضافية إلى ناتج **إحصائيات** show ip الفحص في 12.4(11)T و 12.4(10) للكشف عن العلامة المائية العالية لمعدل إنشاء جلسة العمل. إذا قمت بتشغيل إصدار من برنامج Cisco IOS Software أقدم من 12.4(11)T أو 12.4(10)، فإن إحصائيات الفحص لا تحتوي على هذا السطر:

```
[Maxever session creation rate [value
```

لا تحتفظ إصدارات برنامج Cisco IOS software السابقة ل 12.4(11)T و 12.4(10) بقيمة الحد الأقصى

لمعدل اتصال الفحص لمدة دقيقة واحدة، لذلك يجب عليك حساب القيمة التي تطبقها استنادا إلى قيم "الحد الأقصى لعدد جلسات العمل" التي تم ملاحظتها. أظهرت ملاحظات العديد من الشبكات التي تستخدم الفحص عقائدي لجدار حماية Cisco IOS الإصدار 12.4(11)T في الإنتاج أن معدلات إنشاء جلسات عمل Maxever تميل إلى تجاوز مجموع القيم الثلاث (المحددة والمنخفضة والمفتوحة والمنتهية) في "عد جلسات Maxever" بنسبة 10٪ تقريبا. من أجل حساب قيمة فحص ip المنخفضة لمدة دقيقة واحدة، اضرب القيمة "المحددة" المشار إليها بمقدار 1.1، على سبيل المثال:

```
Maxever session counts
[estab/half-open/terminating) [207:56:35)
328 = 1.1 * (35 + 56 + 207)
```

التكوين:

```
ip inspect one-minute low 328
```

إذا قام الموجه بتشغيل الإصدار 12.4(11)T من البرنامج Cisco IOS Software أو إصدار أحدث، أو 12.4(10) أو إصدار أحدث، فيمكنك ببساطة تطبيق القيمة الموضحة في إحصائيات الفحص "معدل إنشاء جلسة عمل Maxever":

```
Maxever session creation rate 330
```

التكوين:

```
ip inspect one-minute low 330
```

9. حساب **فحص ip** وتكوينه **عالي لمدة دقيقة واحدة**. يجب أن تكون قيمة فحص ip عالية لمدة دقيقة واحدة أكبر بنسبة 25٪ من القيمة المنخفضة المحسوبة لمدة دقيقة واحدة، على سبيل المثال:

```
ip inspect one-minute low (330) * 1.25 = 413
```

التكوين:

```
ip inspect one-minute high 413
```

ملاحظة: يصف هذا المستند إستخدام مضاعف 1.25 ضعف النشاط النموذجي لشبكتك لتعيين حدود للمشاركة في حماية رفض الخدمة (DoS). إذا لاحظت أن شبكتك في حالة الذروة النموذجية لنشاط الشبكة، فيجب أن يوفر ذلك مساحة كافية لتجنب تنشيط حماية رفض الخدمة (DoS) للموجه في جميع الظروف باستثناء الظروف غير المعتادة. إذا رأت شبكتك دوريا دفعات كبيرة من نشاط الشبكة المشروع التي تتجاوز هذه القيمة، يقوم الموجه باتصال إمكانيات حماية DoS، والتي يمكن أن تتسبب في تأثير سلبي على بعض حركة مرور الشبكة. يجب عليك مراقبة سجلات الموجه الخاصة بك لاكتشاف نشاط DoS وضبط **فحص ip للحد الأقصى غير المكتمل** و/أو **فحص ip** لحدود **عالية** لمدة دقيقة واحدة لتجنب تشغيل DoS، بعد تحديد أنه تم مواجهة الحدود نتيجة لنشاط الشبكة المشروع. يمكنك التعرف على تطبيق حماية DoS من خلال وجود رسائل السجل مثل:

10. تحتاج إلى تحديد قيمة **لمضيف TCP** غير **المكتمل** الأقصى **لفحص** ip وفقا لمعرفتك لإمكانية الخوادم الخاصة بك. لا يمكن لهذا المستند توفير إرشادات لتكوين حماية رفض الخدمة (DoS) لكل مضيف نظرا لأن هذه القيمة تختلف بشكل كبير استنادا إلى أداء الأجهزة والبرامج لدى المضيف النهائي. إذا لم تكن متأكدا من الحدود المناسبة للتكوين لحماية رفض الخدمة (DoS)، فلديك بشكل فعال خياران يمكنك من خلالهما تحديد حدود رفض الخدمة (DoS):ويفضل خيار تكوين حماية رفض الخدمة (DoS) المستندة إلى الموجه لكل مضيف على قيمة عالية (أقل من أو تساوي القيمة القصوى التي تبلغ 4،294،967،295)، وتطبيق حماية خاصة بالمضيف يوفرها نظام التشغيل لكل مضيف أو نظام خارجي لحماية الاقتحام قائم على المضيف مثل وكيل أمان Cisco CSA)).اختبر سجلات الأنشطة والأداء للأجهزة المضيفة على شبكتك وحدد أقصى معدل اتصال مستدام لها. بما أن جدار الحماية التقليدي يوفر عداد عمومي واحد فقط، يجب عليك تطبيق الحد الأقصى للقيمة التي تحددها بعد التحقق من جميع مضيفي الشبكة للحصول على الحد الأقصى لمعدلات الاتصال. لا يزال من المستحسن إستخدام حدود النشاط الخاصة بنظام التشغيل ومعالجات IPS المستندة إلى المضيف مثل CSA.**ملاحظة:** يوفر جدار حماية Cisco IOS حماية محدودة ضد الهجمات الموجهة على نقاط الضعف الخاصة بنظام التشغيل والتطبيقات. لا توفر حماية رفض الخدمة (DoS) التي يوفرها جدار حماية Cisco IOS أي ضمان للحماية من التضحية بخدمات المضيف النهائي التي تتعرض للبيئات التي يحتمل أن تكون معادية.
11. مراقبة نشاط حماية DoS على شبكتك. وبشكل مثالي، يجب عليك إستخدام خادم syslog، أو بشكل مثالي، محطات المراقبة والإبلاغ (MARS) من Cisco لتسجيل تكرارات اكتشاف هجوم رفض الخدمة (DoS). إذا حدث الكشف بشكل متكرر، فإنك تحتاج إلى مراقبة معلمات حماية رفض الخدمة (DoS) وتعديلها.لمزيد من المعلومات حول هجمات TCP SYN DoS، ارجع إلى تحديد الاستراتيجيات للحماية من هجمات TCP SYN لرفض الخدمة.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر show .

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- 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).