ASA/PIX 7.x والإصدارات الأحدث: تخفيف هجمات الشبكة

المحتويات

المقدمة

يوضح هذا المستند كيفية تخفيف هجمات الشبكة المختلفة، مثل رفض الخدمات (DoS)، باستخدام جهاز أمان Cisco (ASA/PIX).

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جهاز الأمان القابل للتكيف (ASA) من السلسلة Cisco 5500 Series الذي يشغل الإصدار 7.0 من البرنامج 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.

المنتجات ذات الصلة

هذا وثيقة يستطيع أيضا كنت استعملت مع cisco 500 sery PIX أن يركض برمجية صيغة 7.0 ومتأخر.

الاصطلاحات

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

الحماية من هجمات ال SYN

كيف يمكنك تخفيف هجمات بروتوكول التحكم في الإرسال (TCP) المتزامنة/البدء (SYN) على ASA/PIX؟

هجوم TCP SYN

هجوم TCP SYN هو نوع من هجوم DoS يرسل فيه المرسل وحدة تخزين من الاتصالات التي لا يمكن إكمالها. وهذا يتسبب في تعبئة قوائم انتظار الاتصال، وبالتالي رفض الخدمة لمستخدمي TCP الشرعيين.

عندما يبدأ اتصال TCP عادي، يستلم مضيف الوجهة حزمة SYN من مضيف مصدر ويرسل مرة أخرى إقرار متزامن (SYN ACK). يجب على مضيف الوجهة بعد ذلك سماع ACK الخاص ب SYN ACK قبل إنشاء الاتصال. ويشار إلى هذا باسم مصافحة TCP الثلاثية.

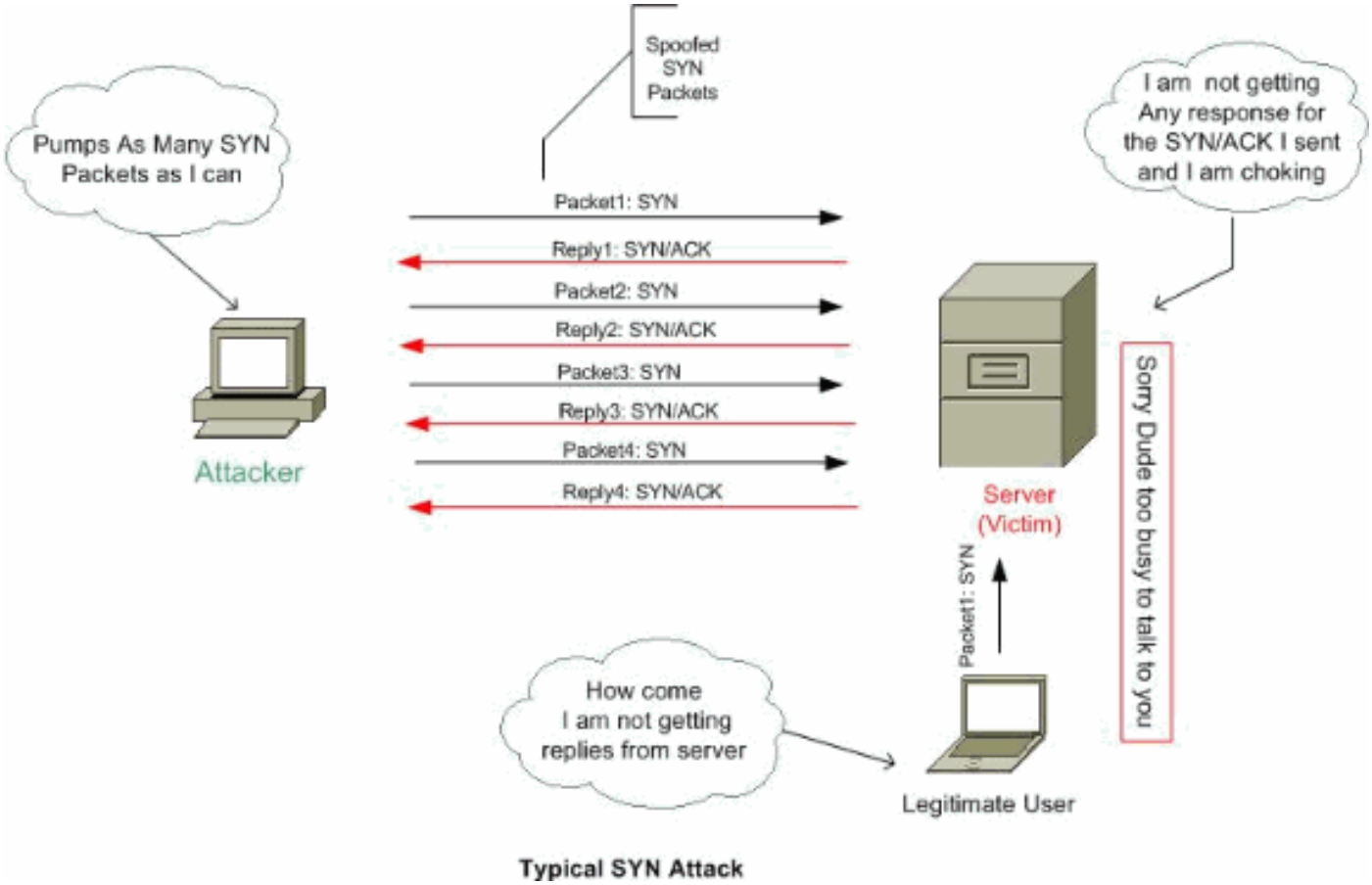
أثناء انتظار ACK إلى SYN ACK، تستمر قائمة انتظار إتصالات ذات حجم محدود على المضيف الوجهة في تعقب الاتصالات التي تنتظر إكمالها. يتم إفراغ قائمة الانتظار هذه بشكل سريع لأنه من المتوقع وصول ACK بعد SYN ACK ببضع مللي ثانية.

يستغل هجوم نظام TCP هذا التصميم من خلال وجود مضيف مصدر مهاجم يقوم بإنشاء حزم TCP SYN باستخدام عناوين مصدر عشوائية تجاه مضيف الضحايا. يرسل مضيف وجهة الضحية SYN ACK مرة أخرى إلى عنوان المصدر العشوائي ويضيف إدخالا إلى قائمة انتظار الاتصال. نظرا لأن SYN ACK مخصص لمضيف غير صحيح أو غير موجود، فإن الجزء الأخير من "تأكيد الاتصال الثلاثي" لا يتم إتمامه أبدا ويظل الإدخال في قائمة انتظار الاتصال حتى تنتهي صلاحية المؤقت، عادة لمدة دقيقة واحدة تقريبا. من خلال إنشاء حزم TCP SYN وهمية من عناوين IP العشوائية بمعدل سريع، من الممكن ملء قائمة انتظار الاتصال ورفض خدمات TCP (مثل البريد الإلكتروني أو نقل الملفات أو WWW) للمستخدمين الشرعيين.

لا توجد طريقة سهلة لتعقب منشئ الهجوم لأن عنوان IP الخاص بالمصدر مزور.

تتضمن المظاهر الخارجية للمشكلة عدم القدرة على الحصول على البريد الإلكتروني أو عدم القدرة على قبول الاتصالات بخدمات WWW أو FTP أو عدد كبير من إتصالات TCP على المضيف في الحالة SYN_RCVD.

ارجع إلى الدفاعات ضد هجمات غمر TCP SYN للحصول على مزيد من المعلومات حول هجمات TCP SYN.



Typical SYN Attack

تخفيف

يوضح هذا القسم كيفية تخفيف هجمات SYN من خلال تعيين الحد الأقصى لاتصالات TCP وبروتوكول مخطط بيانات المستخدم (UDP) والحد الأقصى للاتصالات الجنينية وحالات انتهاء المهلة الزمنية للاتصال وكيفية تعطيل تسلسل TCP.

إذا تم الوصول إلى حد الاتصال الجنيني، فإن جهاز الأمان يستجيب لكل حزمة SYN يتم إرسالها إلى الخادم باستخدام SYN+ACK، ولا يقوم بتمرير حزمة SYN إلى الخادم الداخلي. إذا كان الجهاز الخارجي يستجيب باستخدام حزمة ACK، فإن جهاز الأمان يعلم أنه طلب صالح (وليس جزءا من هجوم SYN محتمل). ثم يقوم جهاز الأمان بإنشاء اتصال بالخادم ويربط الاتصالات معا. إذا لم تحصل الأجهزة الأمنية على ACK مرة أخرى من الخادم، فإنها تقوم بمضاعفة هذا الاتصال الجنيني.

يحتوي كل اتصال TCP على رقمين تسلسليين أوليين (ISs): أحدهما تم إنشاؤه بواسطة العميل والآخر تم إنشاؤه بواسطة الخادم. يقوم جهاز الأمان بتنفيذ عشوائية على IS الخاص ب TCP SYN الذي يمر في كلا الاتجاهين الوارد والصادر.

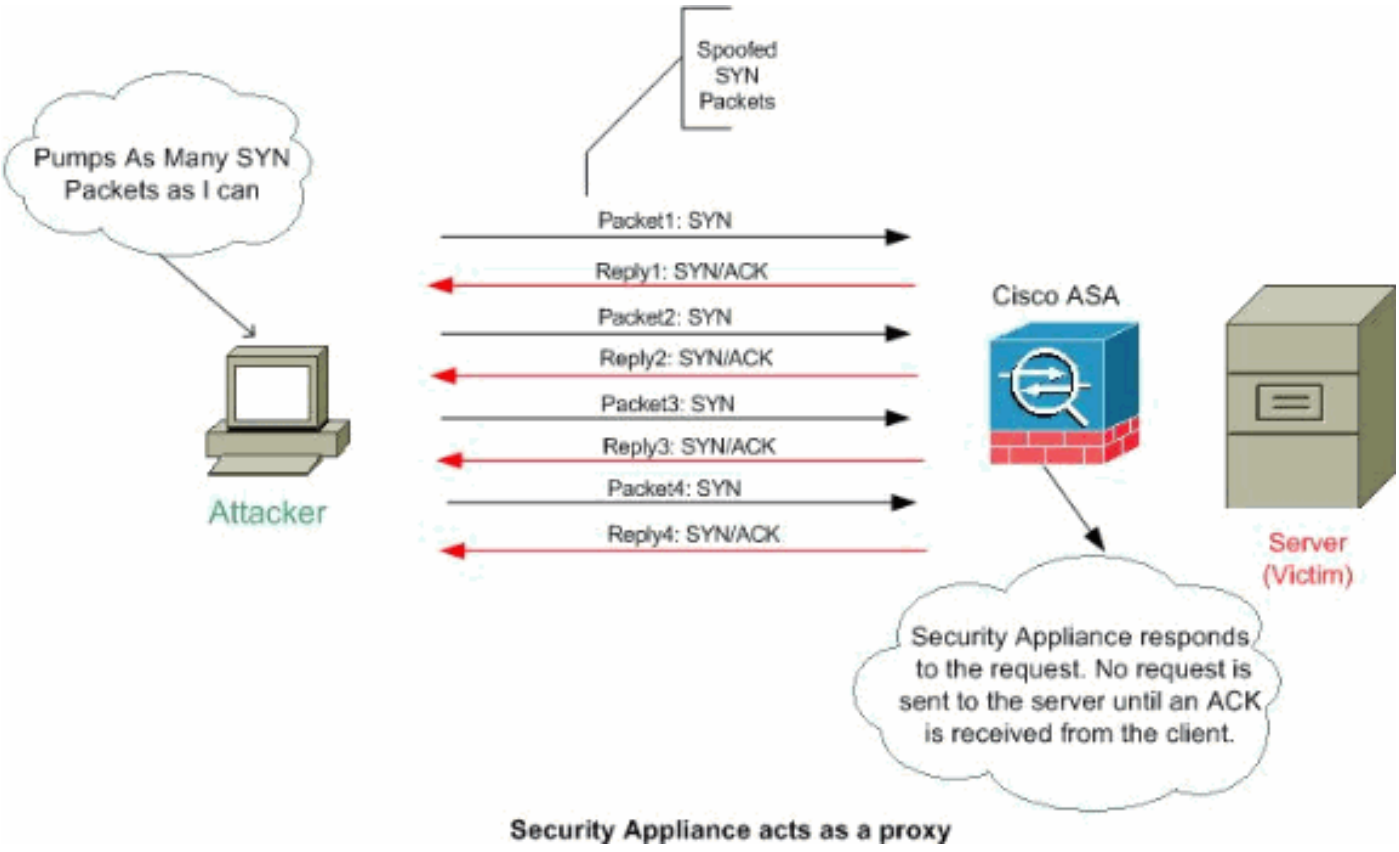
إن عشوائية تنظيم "IS" للمضيف المحمي تمنع المهاجم من التنبؤ ب ISN التالي من أجل اتصال جديد ومن المحتمل أن يستولي على الجلسة الجديدة.

يمكن تعطيل تعيين الرقم التسلسلي الأولي ل TCP عشوائيا إذا لزم الأمر. على سبيل المثال:

- إذا كان هناك جدار حماية داخلي آخر يقوم أيضا بعشوائية أرقام التسلسل الأولية، فلا حاجة لجدران الحماية كلاهما للقيام بهذا الإجراء، حتى وإن كان هذا الإجراء لا يؤثر على حركة المرور.
- إذا كنت تستخدم الخطوة المتعددة BGP الخارجي (eBGP) من خلال جهاز الأمان، وكانت نظائر eBGP تستخدم MD5، فإن العشوائية تفك المجموع الاختباري MD5.
- يمكنك إستخدام جهاز خدمات التطبيقات الواسعة (WAAS) الذي يتطلب من جهاز الأمان عدم أخذ الأرقام التسلسلية للاتصالات بشكل عشوائي.

ملاحظة: يمكنك أيضا تكوين الحد الأقصى للاتصالات، الحد الأقصى للاتصالات الجنينية، وترتيب TCP عشوائيا في

تكوين NAT. إن يشكل أنت هذا عملية إعداد ل ال نفسه حركة مرور يستعمل كلا الطريقتين، بعد ذلك يستعمل جهاز التأمين الحد الأدنى. بالنسبة لتعطيل تسلسل TCP عشوائيا، إذا تم تعطيله باستخدام أي من الطريقتين، فعندئذ يقوم جهاز الأمان بتعطيل تعيين تسلسل TCP عشوائيا.



أكمل الخطوات التالية لتعيين حدود الاتصال:

1. لتحديد حركة المرور، أضف خريطة فئة باستخدام الأمر **class-map** وفقا لاستخدام إطار عمل السياسة النمطية.
2. لإضافة **خريطة سياسة** أو تحريرها لتعيين الإجراءات التي يجب إتخاذها مع حركة مرور خريطة الفئة، أدخل هذا الأمر:
```
hostname(config)#policy-map name
```
3. لتحديد خريطة الفئة (من الخطوة 1) التي تريد تعيين عملية لها، أدخل هذا الأمر:
```
hostname(config-pmap)#class class_map_name
```
4. لتعيين الحد الأقصى من الاتصالات (كلا من TCP و UDP)، أدخل هذا الأمر على الحد الأقصى من الاتصالات الجنينية، لكل عميل-جنيني-max، لكل عميل-عميل-max، أو ما إذا كان سيتم تعطيل تسلسل TCP عشوائيا:
```
[hostname(config-pmap-c)#set connection {[conn-max number
[embryonic-conn-max number] [per-client-embryonic-max number]
| per-client-max number][random-sequence-number {enable]
{{disable
```
حيث العدد هو عدد صحيح بين 0 و 65535. الإعداد الافتراضي هو 0، مما يعني عدم وجود حد للاتصالات.يمكنك إدخال هذا الأمر الكل على سطر واحد (بأي ترتيب)، أو يمكنك إدخال كل سمة كأمر منفصل. يتم دمج الأمر على سطر واحد في التكوين الجاري تشغيله.
5. دخلت in order to ثبتت المهلة للاتصالات، جنيني توصيل (half-open) و half-closed توصيل، هذا أمر:
```
[[[hostname(config-pmap-c)#set connection {[embryonic hh[:mm[:ss
{[[[half-closed hh[:mm[:ss]]] [tcp hh[:mm[:ss]
```
حيث **يكون** h[:mm[:ss] هو وقت بين 0:0:5 و 1192:59:59. الافتراضي هو 0:0:30. يمكنك أيضا تعيين هذه القيمة على 0، وهو ما يعني أن الاتصال لا يتأخر كثيرا.إن قيمتي HH[:mm[:ss] و tcp hh[:mm[:ss] عبارة عن وقت بين 0:5:0 و 1192:59:59. التقصير ل **half-closed** هو 0:10:0 والافتراضي ل **TCP** هو 1:0:0. يمكنك أيضا تعيين هذه القيم إلى 0، مما يعني أن الاتصال لا يتأخر كثيرا.يمكنك إدخال هذا الأمر الكل على سطر واحد

(بأي ترتيب)، أو يمكنك إدخال كل سمة كأمر منفصل. يتم دمج الأمر على سطر واحد في التكوين الجاري تشغيله.**اتصال جنيني (نصف مفتوح)**- اتصال جنيني هو طلب اتصال TCP لم يتم إنهاء المصافحة الضرورية بين المصدر والوجهة.**اتصال نصف مغلق** — عندما يتم إغلاق الاتصال في إتجاه واحد فقط من خلال إرسال FIN. ومع ذلك، لا يزال النظير يحتفظ بجلسة عمل TCP.**الحد الأقصى لعدد الاتصالات الجنينية المتزامنة المسموح بها لكل عميل، بين 0 و 65535.** الافتراضي هو 0، والذي يسمح بالاتصالات غير المحدودة.**لكل عميل-**الحد الأقصى لعدد الاتصالات المتزامنة المسموح بها لكل عميل، بين 0 و 65535. الافتراضي هو 0، والذي يسمح بالاتصالات غير المحدودة.

6. لتنشيط خريطة السياسة على واجهة واحدة أو أكثر، أدخل هذا الأمر:

```
{hostname(config)#service-policy policymap_name {global | interface interface_name
```

حيث **عمومي** 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.

مثال:

```
ciscoasa(config)#class-map tcp_syn
ciscoasa(config-cmap)#match port tcp eq 80
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map tcpmap
ciscoasa(config-pmap)#class tcp_syn
ciscoasa(config-pmap-c)#set connection conn-max 100
ciscoasa(config-pmap-c)#set connection embryonic-conn-max 200
ciscoasa(config-pmap-c)#set connection per-client-embryonic-max 10
ciscoasa(config-pmap-c)#set connection per-client-max 5
ciscoasa(config-pmap-c)#set connection random-sequence-number enable
ciscoasa(config-pmap-c)#set connection timeout embryonic 0:0:45
ciscoasa(config-pmap-c)#set connection timeout half-closed 0:25:0
ciscoasa(config-pmap-c)#set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
ciscoasa(config)#service-policy tcpmap global
```

ملاحظة: للتحقق من العدد الإجمالي لجلسات العمل نصف المفتوحة لأي مضيف معين، أستخدم هذا الأمر:

```
ASA-5510-8x# show local-host all

        Interface dmz: 0 active, 0 maximum active, 0 denied
Interface management: 0 active, 0 maximum active, 0 denied
         Interface xx: 0 active, 0 maximum active, 0 denied
    Interface inside: 7 active, 18 maximum active, 0 denied

                                ,<local host: <10.78.167.69

                          TCP flow count/limit = 2/unlimited

                             TCP embryonic count to host = 0

                       TCP intercept watermark = unlimited

                          UDP flow count/limit = 0/unlimited
```

ملاحظة: يعرض السطر، TCP ، عدد جلسات العمل نصف المفتوحة.

الحماية ضد هجمات انتحال عناوين IP

هل يمكن أن يقوم PIX/ASA بحظر هجمات IP؟

انتحال عناوين IP

للحصول على الوصول، يقوم الدخلاء بإنشاء حزم باستخدام عناوين IP للمصدر المنتحلة. يؤدي هذا إلى أستكشاف التطبيقات التي تستخدم المصادقة استنادا إلى عناوين IP ويؤدي إلى وصول المستخدم غير المصرح به وربما الوصول الجذري إلى النظام المستهدف. الأمثلة هي خدمات rsh و rlogin.

من الممكن توجيه الحزم من خلال جدران الحماية الخاصة بموجه التصفية إذا لم يتم تكوينها لتصفية الحزم الواردة التي يكون عنوان المصدر الخاص بها في المجال المحلي. من المهم ملاحظة أن الهجوم الموضح ممكن حتى إذا لم تتمكن حزم الرد من الوصول إلى المهاجم.

وتتضمن أمثلة التكوينات التي يحتمل أن تكون عرضة للتأثر ما يلي:

- جدران الحماية للوكيل حيث تستخدم تطبيقات الوكيل عنوان IP المصدر للمصادقة
- الموجهات إلى الشبكات الخارجية التي تدعم الواجهات الداخلية المتعددة
- موجهات بواجهات تدعم تقسيم الشبكة إلى شبكات فرعية على الشبكة الداخلية

تخفيف

تحمي إعادة توجيه المسار العكسي للبث الأحادي (uRPF) من انتحال IP (تستخدم الحزمة عنوان IP مصدر غير صحيح لإخفاء مصدرها الحقيقي) عن طريق التأكد من أن جميع الحزم تحتوي على عنوان IP للمصدر الذي يطابق واجهة المصدر الصحيحة وفقا لجدول التوجيه.

عادة، ينظر جهاز الأمان فقط في عنوان الوجهة عند تحديد مكان إعادة توجيه الحزمة. ترشد إعادة توجيه المسار العكسي (RPF) للبث الأحادي جهاز الأمان للنظر أيضا في عنوان المصدر. هذا هو السبب في أنه يسمى **إعادة توجيه المسار العكسي**. بالنسبة لأي حركة مرور تريد السماح بها من خلال جهاز الأمان، يجب أن يتضمن جدول توجيه جهاز الأمان مسارا للعودة إلى عنوان المصدر. راجع RFC 2267 للحصول على مزيد من المعلومات.

ملاحظة: يمكن رؤية **التحقق من** المسار العكسي للبروتوكول `:PIX-1-106021 -` `dest_addr` `src_addr` رسالة سجل `int_name` عند تمكين التحقق من المسار العكسي. قم بتعطيل التحقق من المسار العكسي باستخدام الأمر **no ip verify reverse-path interface (اسم الواجهة)** لحل هذه المشكلة:

`(no ip verify reverse-path interface (interface name`

لحركة المرور الخارجية، على سبيل المثال، يمكن أن يستخدم جهاز الأمان المسار الافتراضي لتلبية حماية إعادة توجيه المسار العكسي (RPF) للبث الأحادي. إذا دخلت حركة المرور من واجهة خارجية، ولم يكن عنوان المصدر معروفا لجدول التوجيه، يستخدم جهاز الأمان المسار الافتراضي لتعريف الواجهة الخارجية بشكل صحيح كواجهة المصدر.

إذا دخلت حركة المرور إلى الواجهة الخارجية من عنوان معروف بجدول التوجيه، ولكنه يقترن بالواجهة الداخلية، عندئذ يقوم جهاز الأمان بإسقاط الحزمة. بالمثل، إن يدخل حركة مرور داخلي قارن من مصدر غير معروف، الجهاز أمن يسقط الربط لأن ال يماثل طريق (التقصير ممر) يشير إلى القارن خارجي.

يتم تنفيذ إعادة توجيه المسار العكسي (RPF) للبث الأحادي كما هو موضح:

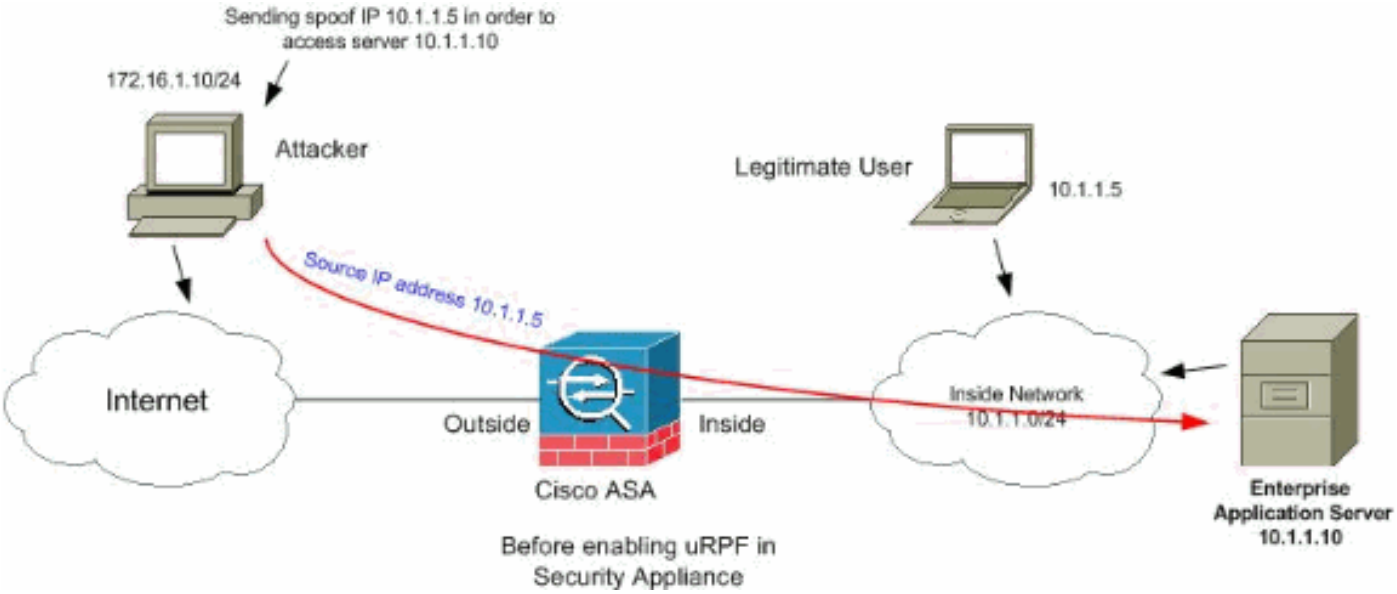
- لا تحتوي حزم ICMP على جلسة، لذلك يتم التحقق من كل حزمة.
- يحتوي UDP و TCP على جلسات عمل، لذلك تتطلب الحزمة الأولية بحث مسار عكسي. يتم التحقق من الحزم التالية التي تصل أثناء الجلسة باستخدام حالة موجودة يتم الاحتفاظ بها كجزء من الجلسة. يتم التحقق من الحزم غير الأولية لضمان وصولها إلى نفس الواجهة التي تستخدمها الحزمة الأولية.

دخلت in order to مكنت Unicast RPF، هذا أمر:

```
hostname(config)#ip verify reverse-path interface interface_name
```

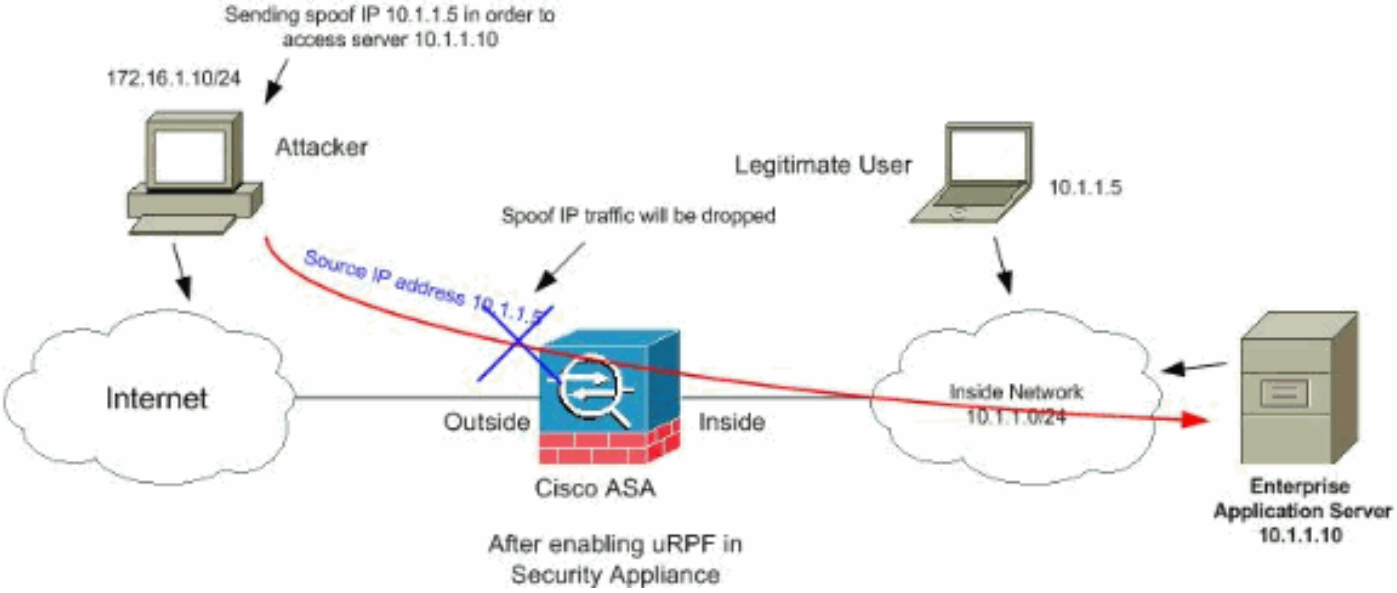
مثال:

كما هو موضح في هذا الشكل، يقوم كمبيوتر المهاجم بإنشاء طلب إلى خادم التطبيق 10.1.1.10 عن طريق إرسال حزمة ذات عنوان IP مصدر مزور 24/10.1.1.5، ويرسل الخادم حزمة إلى عنوان IP الحقيقي 24/10.1.1.5 إستجابة للطلب. هذا النوع من الحزم غير القانونية سيهاجم كل من خادم التطبيق والمستخدم الشرعي في الشبكة الداخلية.



يمكن أن تمنع إعادة توجيه المسار العكسي (RPF) للبث الأحادي الهجمات استنادا إلى انتحال عنوان المصدر. أنت تحتاج إلى تكوين uRPF في الواجهة الخارجية ل ASA كما هو موضح هنا:

```
ciscoasa(config)#ip verify reverse-path interface outside
```



تعريف الانتحال باستخدام رسائل syslog

يستمر جهاز الأمان في تلقي رسائل خطأ syslog كما هو موضح. وهذا يشير إلى الهجمات المحتملة باستخدام الحزم المنتحلة أو التي قد يتم تشغيلها بسبب التوجيه غير المتماثل.

.1

```
PIX|ASA-2-106001: Inbound TCP connection denied from IP_address/port%
to IP_address/port flags tcp_flags on interface interface_name
```

الشرحهذه رسالة متعلقة بالاتصال. تحدث هذه الرسالة عندما يتم رفض محاولة الاتصال بعنوان داخلي من قبل نهج الأمان الذي تم تعريفه لنوع حركة المرور المحدد. تتوافق قيم *tcp_flags* المحتملة مع العلامات الموجودة في رأس TCP والتي كانت موجودة عند رفض الاتصال. على سبيل المثال، وصلت حزمة TCP لا توجد حالة اتصال لها في جهاز الأمان، وتم إسقاطها. *tcp_flags* في هذه الحزمة هي FIN و ACK.ال *tcp_flags* كما يلي:ACK—تم إستلام رقم الإقرار.FIN — تم إرسال البيانات.PSH—قام المستقبل بتمرير البيانات إلى التطبيق.RST — تمت إعادة تعيين الاتصال.تمت مزامنة أرقام SYN—Sequence لبدء اتصال.URG—تم الإعلان عن صحة المؤشر العاجل.هناك العديد من الأسباب لفشل الترجمة الثابتة على PIX/ASA. ولكن، من الأسباب الشائعة أنه يتم تكوين واجهة المنطقة المنزوعة السلاح (DMZ) بنفس مستوى الأمان (0) الذي يتم تكوينه للواجهة الخارجية.لحل هذه المشكلة، قم بتخصيص مستوى أمان مختلف لجميع الواجهاتراجع تكوين معلمات الواجهة للحصول على مزيد من المعلومات.تظهر رسالة الخطأ هذه أيضا إذا كان جهاز خارجي يرسل حزمة IDENT إلى العميل الداخلي، والذي يتم إسقاطه بواسطة جدار حماية PIX. راجع مشاكل أداء PIX الناجمة عن بروتوكول المعلومات للحصول على مزيد من المعلومات

.2

```
PIX|ASA-2-106007: Deny inbound UDP from outside_address/outside_port%
{to inside_address/inside_port due to DNS {Response|Query
```

الشرحهذه رسالة متعلقة بالاتصال. يتم عرض هذه الرسالة إذا فشل الاتصال المحدد بسبب أمر **رفض الصادر**. يمكن أن يكون متغير البروتوكول ICMP أو TCP أو UDP.**الإجراء الموصى به:** أستخدم الأمر **show outbound** للتحقق من القوائم الصادرة.

.3

```
PIX|ASA-3-106014: Deny inbound icmp src interface_name: IP_address dst%
(interface_name: IP_address (type dec, code dec
```

الشرحرفض جهاز الأمان أي وصول إلى حزمة ICMP الواردة. بشكل افتراضي، يتم رفض الوصول إلى جميع حزم ICMP ما لم يتم السماح بها بشكل محدد.

.4

```
PIX|ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on%
.interface interface_name
```

الشرحيتم إنشاء هذه الرسالة عند وصول حزمة إلى واجهة جهاز الأمان التي تحتوي على عنوان IP للوجهة 0.0.0.0 وعنوان MAC للوجهة لواجهة جهاز الأمان. بالإضافة إلى ذلك، يتم إنشاء هذه الرسالة عندما يقوم جهاز الأمان بتجاهل حزمة بعنوان مصدر غير صالح، والذي يمكن أن يتضمن أحد العناوين التالية أو عنوان آخر غير صالح:شبكة الاسترجاع (127.0.0.0)البث (محدود، موجه عبر الشبكة، موجه عبر الشبكة الفرعية، وموجه عبر الشبكات الفرعية بأكملها)مضيف الوجهة (land.c)لتحسين اكتشاف حزمة الملعقة بشكل إضافي، أستخدم الأمر **icmp** لتكوين جهاز الأمان لتجاهل الحزم باستخدام عناوين المصدر التي تنتمي إلى الشبكة الداخلية. وذلك لأن أمر **access-list** تم إهماله ولم يعد مكفولا للعمل بشكل صحيح.**الإجراء الموصى به:** تحديد ما إذا كان مستخدم خارجي يحاول التضحية بالشبكة المحمية. تحقق من العملاء الذين تم تكوينهم بشكل غير صحيح.

.5

```
PIX|ASA-2-106017: Deny IP due to Land Attack from IP_address to%
IP_address
```

الشرحاستلم جهاز الأمان حزمة مع عنوان مصدر IP يساوي وجهة IP، والغاية ميناء يساوي المصدر ميناء. تشير هذه الرسالة إلى حزمة منتحلة تم تصميمها لمهاجمة الأنظمة. ويشار إلى هذا الهجوم بأنه هجوم بري.**الإجراء الموصى به:** إذا إستمرت هذه الرسالة، فقد يكون الهجوم قيد التقدم. لا توفر الحزمة معلومات كافية لتحديد مكان إنشاء الهجوم.

.6

```
PIX|ASA-1-106021: Deny protocol reverse path check from%
source_address to dest_address on interface interface_name
```

الشرحهناك هجوم قيد التنفيذ. يحاول شخص ما انتحال عنوان IP على اتصال وارد. كشفت إعادة توجيه المسار

العكسي (RPF) للبث الأحادي، المعروفة أيضا باسم بحث المسار العكسي، حزمة لا تحتوي على عنوان مصدر ممثلا بمسار ويفترض أنها جزء من هجوم على جهاز الأمان الخاص بك.تظهر هذه الرسالة عند تمكين إعادة توجيه المسار العكسي (RPF) للبث الأحادي باستخدام الأمر **ip verify reverse-path**. تعمل هذه الميزة على إدخال الحزم إلى واجهة. إذا تم تكوينه من الخارج، فعندئذ يتحقق جهاز الأمان من الحزم الواردة من الخارج.يقوم جهاز الأمان بالبحث عن مسار استنادا إلى عنوان المصدر. في حالة عدم العثور على إدخال وعدم تعريف مسار، تظهر رسالة سجل النظام هذه ويتم إسقاط الاتصال.إذا كان هناك مسار، يتحقق جهاز الأمان من أي واجهة يماثل. إذا وصلت الحزمة إلى واجهة أخرى، فإنها إما انتحال أو أن هناك بيئة توجيه غير متماثلة تحتوي على أكثر من مسار إلى وجهة. لا يدعم جهاز الأمان التوجيه غير المتماثل.إذا تم تكوين جهاز الأمان على واجهة داخلية، فإنه يتحقق من عبارات أوامر **المسار** الثابت أو بروتوكول معلومات التوجيه (RIP). إذا لم يتم العثور على عنوان المصدر، فعندئذ يقوم مستخدم داخلي بانتحال عنوانه.**الإجراء الموصى به:** حتى في حالة وجود هجوم قيد التقدم، في حالة تمكين هذه الميزة، لا يلزم إتخاذ أي إجراء من قبل المستخدم. جهاز الأمن يصد الهجوم.**ملاحظة:** يظهر الأمر **show asp drop** الحزم أو الاتصالات التي تم إسقاطها من مسار الأمان السريع (ASP)، والتي قد تساعدك على أستكشاف مشكلة وإصلاحها. كما يشير إلى وقت مسح آخر مرة تم فيها مسح عدادات إسقاط ASP. أستخدم الأمر **show asp drop rpf-violated** الذي يتم فيه زيادة العداد عند تكوين **ip verify reverse-path** على واجهة ويستلم جهاز الأمان حزمة لم ينتج عنها البحث عن المسار للمصدر IP نفس الواجهة كالتي تم إستلام الحزمة عليها.

```
ciscoasa#show asp drop frame rpf-violated
Reverse-path verify failed                       2
```

ملاحظة: التوصية: تتبع مصدر حركة المرور استنادا إلى IP المصدر المطبوع في رسالة النظام التالية، وتحقق من سبب إرسالها لحركة المرور المنتحلة.**ملاحظة: رسائل سجل النظام:** 106021

.7

```
PIX|ASA-1-106022: Deny protocol connection spoof from source_address%
to dest_address on interface interface_name
```

الشرحتصل حزمة تطابق اتصالا على واجهة مختلفة من الواجهة التي بدأ الاتصال بها.على سبيل المثال، إذا بدأ مستخدم في تشغيل اتصال على الواجهة الداخلية، ولكن جهاز الأمان يكتشف نفس الاتصال الذي يصل على واجهة المحيط، فإن جهاز الأمان لديه أكثر من مسار إلى وجهة. وهذا يعرف باسم التوجيه غير المتماثل وغير مدعوم على جهاز الأمان.كما قد يحاول المهاجم إلحاق الحزم من اتصال إلى آخر كطريقة لقطع اتصال جهاز الأمان. في كلتا الحالتين، يعرض جهاز الأمان هذه الرسالة ويقطع الاتصال.**إجراء التوصيات:** تظهر هذه الرسالة عند عدم تكوين الأمر **ip verify reverse-path**. تحقق من أن التوجيه غير متماثل.

.8

```
PIX|ASA-4-106023: Deny protocol src%
interface_name:source_address/source_port] dst]
interface_name:dest_address/dest_port [type {string}, code {code}] by
access_group acl_ID
```

الشرحتم رفض حزمة IP بواسطة قائمة التحكم في الوصول (ACL). تعرض هذه الرسالة حتى إذا لم يتم تمكين خيار **السجل** لقائمة تحكم في الوصول (ACL).**إجراء التوصية:** إذا إستمرت الرسائل من عنوان المصدر نفسه، فقد تشير الرسائل إلى محاولة للطباعة بالأقدام أو مسح المنفذ ضوئيا. اتصل بمديري المضيف البعيد.

.9

```
PIX|ASA-3-210011: Connection limit exceeded cnt/limit for dir packet%
.from sip/sport to dip/dport on interface if_name
```

.10

```
ASA-4-419002: Received duplicate TCP SYN from%
in_interface:src_address/src_port to out_interface:dest_address/dest_port with
.different initial sequence number
```

الشرحتشير رسالة سجل النظام هذه إلى أن إنشاء اتصال جديد من خلال جهاز جدار الحماية سيؤدي إلى تجاوز حد واحد على الأقل من الحد الأقصى الذي تم تكوينه للاتصال. يتم تطبيق رسالة سجل النظام على كل من حدود الاتصال التي تم تكوينها باستخدام أمر ثابت، أو تلك التي تم تكوينها باستخدام إطار عمل سياسة Cisco النمطية. لن يتم السماح بالاتصال الجديد من خلال جهاز جدار الحماية حتى يتم قطع أحد الاتصالات الحالية، وبالتالي تقليل عدد الاتصالات الحالية إلى أقل من الحد الأقصى الذي تم تكوينه.*CNT*—عدد الاتصالات الحالي*الحد*—حد الاتصال المكون*dir*— إتجاه حركة المرور، الواردة أو الصادرة*SIP*—عنوان IP المصدر*ميناء مصدر رياضة**dip*— غاية عنوان*dPort*—غاية ميناء*if_name*— اسم الواجهة التي يتم تلقي وحدة حركة المرور

عليها، إما أساسي أو ثانوي.**إجراء التوصية:** نظرا لتكوين حدود الاتصال لسبب وجيه، فقد تشير رسالة سجل النظام هذه إلى هجوم محتمل على رفض الخدمة (DoS)، وفي هذه الحالة، قد يكون مصدر حركة المرور عنوان IP منتحلا. إذا لم يكن عنوان IP للمصدر عشوائيا بالكامل، فقد يساعد تحديد المصدر وحظره باستخدام قائمة الوصول. في حالات أخرى، الحصول على آثار sniffer وتحليل مصدر الحركة مرور سيساعد في عزل حركة المرور غير المرغوب من حركة المرور الشرعية.

ميزة الكشف عن التهديدات الأساسية في ASA 8.x

يدعم جهاز الأمان Cisco ASA/PIX ميزة تسمى اكتشاف التهديدات من الإصدار 8.0 من البرنامج والإصدارات الأحدث. باستخدام الكشف عن التهديدات الأساسية، يراقب جهاز الأمان معدل الحزم التي تم إسقاطها وأحداث الأمان نظرا لهذه الأسباب:

- الرفض بواسطة قوائم الوصول
- تنسيق حزمة غير صحيح (مثل رأس ip غير صالح أو طول tcp-hdr غير صالح)
- تم تجاوز حدود الاتصال (حدود الموارد على مستوى النظام، والحدود المعينة في التكوين)
- تم الكشف عن هجوم رفض الخدمة (مثل SPI غير صالح، فشل التحقق من جدار الحماية المعبر عن الحالة)
- فشلت عمليات التحقق الأساسية من جدار الحماية (هذا الخيار هو معدل مجمع يتضمن جميع عمليات إسقاط الحزم المتعلقة بجدار الحماية في هذه القائمة ذات التعداد. ولا يتضمن عمليات إسقاط غير متعلقة بجدار الحماية مثل التحميل الزائد للواجهة، وفشل الحزم عند فحص التطبيق، واكتشاف هجوم للمسح الضوئي.)
- تم الكشف عن حزم ICMP المشبوهة
- فشلت الحزم في فحص التطبيق
- الحمل الزائد للواجهة
- تم الكشف عن هجوم المسح الضوئي (يراقب هذا الخيار هجمات المسح الضوئي؛ على سبيل المثال، حزمة TCP الأولى ليست حزمة SYN، أو فشل اتصال TCP في مصافحة TCP الثلاثية. يعمل الكشف الكامل عن تهديدات المسح الضوئي (ارجع إلى تكوين الكشف عن تهديدات المسح الضوئي للحصول على مزيد من المعلومات) على أخذ معلومات معدل هجوم المسح الضوئي هذا ويعمل عليه من خلال تصنيف البيئات المضيفة كمهاجمين وتجنبها تلقائيا، على سبيل المثال.)
- اكتشاف جلسة عمل غير مكتملة مثل هجوم TCP SYN الذي تم الكشف عنه أو لم يتم الكشف عن هجوم جلسة عمل UDP للبيانات.

عندما يكتشف جهاز الأمان وجود تهديد، فإنه يرسل رسالة سجل نظام (730100) على الفور.

يؤثر الكشف عن التهديد الأساسي على الأداء فقط عندما تكون هناك حالات إنخفاض أو تهديدات محتملة. حتى في هذا السيناريو، يكون تأثير الأداء ضئيلا.

يتم إستخدام الأمر **show threat-rate** لتحديد الهجمات المحتملة عند تسجيل دخولك إلى جهاز الأمان.

```
ciscoasa#show threat-detection rate
  Average(eps)    Current(eps) Trigger      Total events
  10-min ACL  drop:                  0               0       0               16
  1-hour ACL  drop:                  0               0       0              112
  1-hour SYN attck:                  5               0       2            21438
  10-min  Scanning:                  0               0      29              193
  1-hour  Scanning:                106               0      10           384776
  1-hour Bad  pkts:                 76               0       2           274690
  10-min  Firewall:                  0               0       3               22
  1-hour  Firewall:                 76               0       2           274844
  10-min DoS attck:                  0               0       0                6
  1-hour DoS attck:                  0               0       0               42
  10-min Interface:                  0               0       0              204
  1-hour Interface:                 88               0       0           318225
```

أحلت بشكل أساسي تهديد كشف قسم من ASA 8.0 تشكيل مرشد ل كثير معلومة على التشكيل جزء.

Syslog Message 733100

رسالة الخطأ:

```
ASA-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max%
configured rate is rate_val; Current average rate is rate_val per second, max configured rate is
rate_val; Cumulative total count is total_cnt
```

تجاوز الكائن المحدد في رسالة سجل النظام معدل حد الاندفاع المحدد أو متوسط معدل الحد الأدنى. يمكن أن يكون الكائن نشاط إسقاط لمضيف أو منفذ TCP/UDP أو بروتوكول IP أو عمليات إسقاط مختلفة بسبب هجمات محتملة. يشير ذلك إلى أن النظام يتعرض لهجوم محتمل.

ملاحظة: لا تنطبق رسائل الخطأ هذه التي لها حل إلا على ASA 8.0 والإصدارات الأحدث.

1. الكائن - المصدر العام أو الخاص لتعداد معدل الإفلات، والذي قد يتضمن ما يلي:جدار الحمايةPKTS غير صحيححد المعدلدوس تاكإسقاط ACLحد المخروطهجوم ICMPمسحسين أتكفحصالواجهة
2. rate_id—المعدل الذي تم تكوينه والذي يتم تجاوزه. يمكن تكوين معظم الكائنات بمعدل يصل إلى ثلاثة معدلات مختلفة لفترات زمنية مختلفة.
3. rate_val—قيمة معدل معينة.
4. total_cnt—إجمالي العدد منذ إنشاء الكائن أو مسحه.

هذه الأمثلة الثلاثة تبين كيفية حدوث هذه المتغيرات:

- بالنسبة لإسقاط الواجهة بسبب وحدة المعالجة المركزية (CPU) أو تحديد الناقل:

```
ASA-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per%
                                                                    ,second
,max configured rate is 8000; Current average rate is 2030 per second
        max configured rate is 2000; Cumulative total count is 3930654
```

- للحصول على انخفاض في المسح الضوئي بسبب الهجمات المحتملة:

```
ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per
                                                                    _second
_max configured rate is 10; Current average rate is 245 per second
(max configured rate is 5; Cumulative total count is 147409 (35 instances received
```

- بالنسبة للحزم السيئة بسبب الهجمات المحتملة:

```
ASA-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per%
                                                                    ,second
,max configured rate is 400; Current average rate is 760 per second
        max configured rate is 100; Cumulative total count is 1938933
```

الإجراء الموصى به:

قم بإجراء هذه الخطوات وفقا لنوع الكائن المحدد الذي يظهر في الرسالة:

1. إذا كان الكائن في رسالة syslog واحدا من التالي:جدار الحمايةPKTS غير صحيححد المعدلهجوم DoSإسقاط ACLحد المخروطهجوم ICMPمسحسين أتكفحصالواجهةتحقق مما إذا كان معدل الإسقاط مقبولا للبيئة قيد التشغيل.
2. قم بضبط معدل العتبة للإفلات المعين على قيمة مناسبة من خلال تشغيل الأمر ***xxx لمعدل اكتشاف التهديدات***، حيث *xxx* هو واحد من التالي:dos-drop-dropconn-limit-dropBad-Packet-drop-ACLإسقاط--fwICMP drop فحص الإسقاطinterface-dropتهديد الماسح الضوئيهجوم شعاعي
3. إذا كان الكائن في رسالة syslog هو منفذ TCP أو UDP، أو بروتوكول IP، أو إسقاط مضيف، فتحقق مما إذا كان معدل الإسقاط مقبولا للبيئة قيد التشغيل.
4. قم بضبط معدل الحد للإفلات المحددة على قيمة مناسبة من خلال تشغيل الأمر **bad-packet-drop لمعدل اكتشاف التهديدات**. أحلت ال بشكل أساسي تهديد كشف قسم من ال ASA 8.0 تشكيل مرشد ل كثير معلومة.

ملاحظة: إذا كنت لا تريد أن يظهر معدل الانخفاض الذي يتجاوز التحذير، فيمكنك تعطيله بتشغيل الأمر **no threat-**

. detection basic-threat

معلومات ذات صلة

- صفحة دعم أجهزة الأمان القابلة للتكيف طراز Series 5500 من Cisco
- صفحة دعم PIX لسلسلة Cisco 500
- الدفاعات ضد هجمات غمر نظام TCP
- نشرة التخفيف التطبيقية من Cisco: تحديد الاستغلال والتخفيف من آثاره على مواطن الضعف المتعلقة برفض الخدمة في وحدة تحويل المحتوى
- نشرة التخفيف التطبيقية من Cisco: تحديد إستغلال نقاط الضعف المتعددة في الوحدة النمطية لأجهزة Cisco PIX و ASA وخدمات جدار الحماية والتخفيف من آثاره
- انتحال عناوين IP
- 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).