إستخدام السيارة أثناء هجمات رفض الخدمة

المحتويات

المقدمة

في بعض الأحيان، تتلقى الشبكة تدفق من حزم هجوم رفض الخدمة (DoS) مع حركة مرور الشبكة العادية. في مثل هذه الحالات، يمكنك إستخدام آلية تسمى "تحديد المعدل" للسماح بانخفاض أداء الشبكة، بحيث تظل الشبكة قيد التشغيل. يمكنك إستخدام برنامج Cisco IOS®Software لتحديد المعدل من خلال هذه الأنظمة:

- معدل الوصول الملتزم به (CAR)
- تنظيم حركة البيانات
- التشكيل وتحديد النهج من خلال واجهة سطر أوامر الخدمة (QoS CLI) المعيارية لجودة الخدمة

يناقش هذا المستند السيارات لاستخدامها في هجمات رفض الخدمة (DoS). أما الخطط الأخرى فهي مجرد أشكال مختلفة للمفهوم الأساسي.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- برنامج IOS الإصدار 11.1CC و 12.0 Mainline من Cisco، والذي يدعم سيارة.
- برنامج IOS الإصدار 11.2 من Cisco والإصدارات الأحدث، الذي يدعم تنظيم حركة البيانات.
- برنامج IOS الإصدارات 12.0XE و 12.1E و 12.1T من Cisco، والتي تدعم واجهة سطر الأوامر لجودة خدمة الوحدة النمطية.

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

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

حد المعدل ICMP/Smurf

تكوين قوائم الوصول هذه:

```
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

```
<# interface <interface> <interface
rate-limit input access-group 102 256000 8000 8000 conform-action transmit
    exceed-action drop
```

لتمكين CAR، يجب عليك تمكين إعادة التوجيه السريع من Cisco (CEF) في المربع. وبالإضافة إلى ذلك، يجب تكوين واجهة تم تحويلها إلى CEF ل CAR.

يستخدم إخراج العينة قيم النطاق الترددي لعروض النطاق الترددي من نوع DS3. أخترت قيمة يؤسس على القارن عرض نطاق والسرعة ب أي أنت تريد أن يحد نوع خاص حركة مرور. لواجهات الدخول الأصغر، يمكنك تكوين معدلات أقل.

حزم نظام TCP للحد من المعدل

x)cc)11.1

إذا كنت تعرف المضيف الذي يتعرض للهجوم، فقم بتكوين قوائم الوصول هذه:

```
access-list 103 deny tcp any host 10.0.0.1 established
Let sessions in progress run. access-list 103 permit tcp any host 10.0.0.1 !--- Rate limit ---!
the initial TCP SYN packet, because the other packets !--- in the TCP session would have hit the
earlier entry in the ACL. interface <interface> <interface #> rate-limit input access-group 103
8000 8000 8000 conform-action transmit exceed-action drop
```

ملاحظة: في هذا المثال، المضيف الخاضع للهجوم هو 10.0.0.1.

إذا كنت لا تعرف المضيف الذي يقع ضمن هجوم رفض الخدمة (DoS)، وتريد حماية شبكة، فقم بتكوين قوائم الوصول هذه:

```
access-list 104 deny tcp any any established
Let sessions in progress run. access-list 104 permit tcp any any !--- Rate limit the ---!
initial TCP SYN packet, because the other packets !--- in the TCP session would have hit the
earlier entry in the ACL. interface <interface> <interface #> rate-limit input access-group 104
64000 8000 8000 conform-action transmit exceed-action drop
```

ملاحظة: حد المعدل إلى 64000 بت في الثانية لجميع حزم TCP syn.

[x)[S/T/M)12.0

إذا كنت تعرف المضيف الذي يتعرض للهجوم، فقم بتكوين قوائم الوصول هذه:

```
access-list 105 permit tcp any host 10.0.0.1 syn
Remember that your interest lies in syn packets only. interface <interface> <interface #> ---!
rate-limit input access-group 105 8000 8000 8000 conform-action transmit exceed-action drop
```

ملاحظة: في هذا المثال، 10.0.0.1 هي المضيف الذي يتعرض للهجوم.

إذا لم تكن متأكدا من المضيف الذي يتعرض للهجوم، وتريد حماية شبكة، فقم بتكوين قوائم الوصول هذه:

```
access-list 106 permit tcp any any syn
Remember that your interest lies in syn packets only. interface <interface> <interface #> ---!
rate-limit input access-group 106 64000 8000 8000 conform-action transmit exceed-action drop
```

ملاحظة: حد المعدل إلى 64000 بت في الثانية لجميع حزم TCP syn.

جمهورية أفريقيا الوسطى: الأسئلة المتكررة

كيف يمكنك تحديد القيم المراد إستخدامها لقواعد CAR لتصنيف حزم SYN ذات الحد الأقصى؟

فهم شبكتك. يحدد نوع حركة المرور عدد جلسات عمل TCP النشطة لمبلغ ثابت من البيانات.

- تحتوي حركة مرور WWW على مزيج أعلى بكثير من حزم TCP syn من حركة مرور مزرعة خادم FTP.
- تميل مكدسات عميل الكمبيوتر إلى التعرف على كل حزمة TCP أخرى على الأقل. يمكن أن تعترف المكدسات الأخرى بشكل أقل أو أكثر.
- تحقق مما إذا كنت بحاجة إلى تطبيق قواعد CAR هذه على حافة المستخدم الداخلية أو عند حافة شبكة العميل.

```
users ---- { ISP } --- web farm
```

على WWW، ها هو مزيج حركة المرور:

مقابل كل 5 آلاف ملف تقوم بتنزيله من مزرعة الويب، تتلقى مزرعة الويب 560 بايت، كما هو موضح هنا:

- 80 بايت [SYN، ACK]
- 400 بايت [بنية HTTP بحجم 320 بايت، وحدتا ACK]
- 80 بايت [FIN، ACK]

بافتراض أن النسبة بين حركة مرور الخروج من مزرعة الويب وحركة مرور الدخول من مزرعة الويب هي 10:1. مقدار حركة المرور التي تشكل حزم SYN هو 120:1.

إذا كان لديك إرتباط OC3، فستقوم بالحد من معدل حزم نظام TCP إلى 155 ميجابت في الثانية / 120 == 1.3 ميجابت في الثانية.

على واجهة الدخول في موجه مزرعة الويب، قم بتكوين:

```
rate-limit input access-group 105 1300000 256000 256000 conform-action transmit
exceed-action drop
```

يصبح معدل حزمة نظام TCP أصغر مع زيادة طول جلسات عمل TCP.

```
users ---- { ISP } --- MP3/FTP Farm
```

تميل ملفات MP3 إلى أن يكون حجمها من 4 إلى 5 ميجابت في الثانية في المتوسط. يؤدي تنزيل ملف بسرعة 4 ميجابت في الثانية إلى إنشاء حركة مرور بيانات للمدخل تصل إلى 3160 بايت:

- 80 بايت [SYN، ACK]
- 3000 بايت [ACKs + FTP get]
- 80 بايت [FIN، ACK]

معدل synS TCP أن مخرج حركة مرور 155 ميجابت في الثانية / 120000 == 1.3 كيلوبت في الثانية.

التكوين:

```
rate-limit input access-group 105 1300 1200 1200 conform-action transmit
exceed-action drop
```

كيف أعرف إذا قمت بتقييد العديد من حزم SYN؟

إذا كنت تعرف معدل الاتصال المعتاد على الخوادم، فيمكنك مقارنة الأشكال قبل تمكين CAR وبعده. تساعدك المقارنة على تحديد حدوث انخفاض في معدل الاتصال الخاص بك. وإذا وجدت انخفاضا في المعدل، فقم بزيادة معلمات CAR للسماح بمزيد من الجلسات.

تحقق مما إذا كان المستخدمون قادرين على إنشاء جلسات عمل TCP بسهولة أم لا. إذا كانت حدود السيارة الخاصة بك مقيدة للغاية، فسيحتاج المستخدمون إلى إجراء محاولات متعددة لإنشاء جلسة عمل TCP.

هل يمكنني تمكين السيارة على موجه محول جيجابت (GSR)؟

نعم. بطاقات خطوط المحرك 0 والمحرك 1 تدعم CAR. برنامج IOS الإصدار GS2(14)11.2 من Cisco وتقديم دعم لاحق ل CAR. يعتمد تأثير الأداء في جمهورية أفريقيا الوسطى على عدد قواعد جمهورية أفريقيا الوسطى التي تطبقها.

ويكون تأثير الأداء أيضا أكبر على بطاقات خطوط المحرك 1 منه على بطاقات الخط 0 Engine. إن يريد أنت أن يمكن CAR على محرك 0 خط بطاقة، أنت ينبغي كنت على علم من cisco بق CSCdp80432 id (يسجل زبون فقط). إن يريد أنت أن يمكن CAR أن rate-limit multicast حركة مرور، ضمنت أن cisco بق CSCdp32913 id (يسجل زبون فقط) لا يؤثر أنت. معرف تصحيح الأخطاء من CSCdm56071 Cisco (العملاء المسجلون فقط) هو خطأ آخر يجب أن تكون على دراية به قبل تمكين السيارة.

هل يمكنني تمكين السيارة الموزعة (dCAR) على Cisco 7500؟

نعم، يدعم النظام الأساسي RSP/VIP برنامج dCAR في الإصدار CC(20)11.1 من برنامج Cisco IOS وجميع إصدارات البرنامج 12.0.

تؤثر السيارة على الأداء إلى حد ما. استنادا إلى تهيئة السيارة، يمكنك تحقيق معدل الخط [لحركة مرور مزيج الإنترنت] مع VIP2-50 [من خلال dCAR] على نقطة وصول إلى الطراز OC3. تأكد من أن معرف تصحيح الأخطاء من Cisco CSCdm56071 (العملاء المسجلون فقط) لا يؤثر عليك. إن يريد أنت أن يستعمل إنتاج سيارة، cisco بق id

CSCdp52926 (يسجل زبون فقط) يستطيع أثرت موصولية أنت. إن يمكن أنت cisco ،dCAR بق CSCdp58615 id (يسجل زبون فقط) يستطيع سببت مهمة عطل.

هل يمكنني تمكين السيارة على Cisco 7200؟

نعم. يدعم NPE السيارة في برنامج Cisco IOS الإصدار 11.1(20)CC، وجميع إصدارات البرنامج 12.0.

تؤثر السيارة على الأداء إلى حد ما، بناء على تهيئة السيارة. احصل على الإصلاحات لهذه الأخطاء: معرف الأخطاء من Cisco CSCdm85458 (العملاء المسجلون فقط) ومعرف تصحيح الأخطاء من Cisco CSCdm56071 (العملاء المسجلون فقط).

ملاحظة: يؤدي عدد كبير من إدخالات CAR في واجهة/واجهة فرعية إلى انخفاض الأداء لأن الموجه يحتاج إلى إجراء بحث خطي على عبارات CAR للعثور على جملة "CAR" التي تتطابق.

ميزات وبدائل أخرى

قائمة التحكم في الوصول (ACL) الخاصة باستقبال IP

يحتوي الإصدار 12.0(22)S من برنامج Cisco IOS Software على ميزة قائمة التحكم في الوصول (ACL) لاستقبال IP على موجه الإنترنت Cisco 12000 Series.

توفر ميزة قائمة التحكم في الوصول (ACL) الخاصة باستقبال IP عوامل التصفية الأساسية لحركة المرور الموجهة للوصول إلى الموجه. يمكن أن يحمي الموجه حركة مرور بروتوكول التوجيه عالي الأولوية من هجوم ما لأن الميزة تعمل على تصفية قائمة التحكم في الوصول إلى الإدخال (ACL) بالكامل على واجهة الدخول. تقوم ميزة قائمة التحكم في الوصول (ACL) لاستقبال IP بتصفية حركة المرور على بطاقات الخط الموزعة قبل أن يستقبل معالج التوجيه الحزم. تسمح هذه الميزة للمستخدمين بتصفية فيضانات رفض الخدمة (DoS) مقابل الموجه. لذلك، تمنع هذه الميزة انخفاض أداء معالج التوجيه.

راجع قائمة التحكم في الوصول إلى IP Receive APL للحصول على مزيد من التفاصيل.

متعقب مصدر IP

يدعم برنامج IOS الإصدار 12.0(21)S من Cisco ميزة متعقب مصدر IP على موجه الإنترنت من السلسلة 12000 من Cisco. يدعم برنامج IOS الإصدار 12.0(22)S من Cisco هذه الميزة على موجه سلسلة 7500 من Cisco.

تسمح لك ميزة "متعقب مصدر IP" بجمع المعلومات حول حركة المرور التي تتدفق إلى مضيف تشك في أنه يتعرض للهجوم. كما تتيح لك هذه الميزة إمكانية تتبع أي هجوم بسهولة للعودة إلى نقطة الإدخال في الشبكة. عندما تحدد نقطة الدخول إلى الشبكة من خلال هذه الميزة، يمكنك إستخدام قوائم التحكم في الوصول أو CAR لحظر الهجوم بشكل فعال.

راجع متعقب مصدر IP للحصول على مزيد من المعلومات.

معلومات ذات صلة

- كيفية حماية شبكتك من فيروس NIMDA
- قائمة التحكم في الوصول ل IP Receive APL
- متعقب مصدر 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).