تحديد حركة المرور التي لم يتم التعرف عليها من قبل NBAR

المحتويات

المقدمة

يوضح هذا المستند كيفية إستخدام ميزة "الوحدة النمطية للغة وصف الحزمة المخصصة (PDLM)" للتعرف على التطبيق المستند إلى الشبكة (NBAR) للمطابقة على حركة المرور غير المصنفة أو حركة المرور غير المدعومة بشكل محدد كبيان لبروتوكول المطابقة.

المتطلبات الأساسية

المتطلبات

يجب أن يكون لدى قراء هذا المستند معرفة بالمواضيع التالية:

- منهجيات جودة الخدمة الأساسية
- فهم أساسي ل NBAR

المكونات المستخدمة

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

- برنامج IOS® الإصدار 12.2(2)T من Cisco
- موجّه Cisco 7206

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة 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.

فهم PDLM المخصص

يدعم NBAR مجموعة متنوعة من البروتوكولات الثابتة والمحددة الحالة. تسمح PDLMs بدعم البروتوكول الجديد ل NBAR دون الحاجة إلى ترقية إصدار IOS وإعادة تحميل الموجه. تتضمن إصدارات IOS التالية دعم هذه البروتوكولات الجديدة.

ال PDLM مخصص يسمح أنت أن يعين بروتوكول إلى ساكن إستاتيكي مستعمل مخطط بيانات بروتوكول (UDP) و TCP ميناء لبروتوكول أن لا يساند حاليا في NBAR مع مطابقة بروتوكول كشف. بمعنى آخر، يقوم بتوسيع أو تحسين قائمة البروتوكولات المعترف بها بواسطة NBAR.

فيما يلي الخطوات اللازمة لإضافة PDLM المخصص إلى الموجه الخاص بك.

1. حدد مكان PDLM الخاص بشريط NBAR وتنزيله من صفحة تنزيل البرامج (العملاء المسجلون فقط) بتنزيل ملف **custom.pdlm**.
قم بتحميل PDLM على جهاز ذاكرة فلاش، مثل بطاقة PCMCIA في الفتحتين 0 أو 1، باستخدام الأمر أدناه2.
```
7206-15(config)# ip nbar pdlm slot0:custom.pdlm
```

3. التحقق من دعم البروتوكولات المخصصة باستخدام **show ip nbar port-map | تضمين** الأمر **المخصص** (كما هو موضح أدناه) أو الأمر **show ip nbar pdlm**.
```
7206-16#show ip nbar port-map | include custom
                port-map custom-01            udp 0
                port-map custom-01            tcp 0
                port-map custom-02            udp 0
                port-map custom-02            tcp 0
                port-map custom-03            udp 0
                port-map custom-03            tcp 0
                port-map custom-04            udp 0
                port-map custom-04            tcp 0
                port-map custom-05            udp 0
                port-map custom-05            tcp 0
                port-map custom-06            udp 0
                port-map custom-06            tcp 0
                port-map custom-07            udp 0
                port-map custom-07            tcp 0
                port-map custom-08            udp 0
                port-map custom-08            tcp 0
                port-map custom-09            udp 0
                port-map custom-09            tcp 0
                port-map custom-10            udp 0
                port-map custom-10            tcp 0
```
4. قم بتعيين منافذ للبروتوكولات المخصصة باستخدام الأمر **ip nbar port-map custom-XY {tcp|udp} {port1 port2..}**. على سبيل المثال، للمطابقة على حركة المرور في منفذ TCP 8877، أستخدم الأمر **ip nbar port-map custom-01 tcp 8877**.

تصنيف المنافذ "غير المصنفة"

على حسب حركة مرور الشبكة، قد تحتاج إلى إستخدام آليات تصنيف خاصة في NBAR. ما إن يصنف أنت هذا حركة مرور، أنت بعد ذلك يستطيع استعملت ال PDLM مخصص ومطابقة ال UDP و TCP ميناء رقم إلى مخصص ميناء-map.

بشكل افتراضي، لا يتم تمكين الآليات غير المصنفة ل NBAR. يرجع الأمر **show ip nbar unclassified-port-stats** رسالة الخطأ التالية:

```
d11-5-7206-16# show ip nbar unclassified-port-stats
.Port Statistics for unclassified packets is not turned on
```

تحت ظروف يتم التحكم فيها بعناية، أستخدم الأمر **debug ip nbar unclassified-port-stats** لتكوين الموجه لبدء التعقب على المنافذ التي تصل الحزم عليها. ثم أستخدم الأمر **show ip nbar unclassified-port-stats** للتحقق من المعلومات المجمعة. يعرض الإخراج الآن رسما بيانيا للمنافذ الأكثر إستخداما.

ملاحظة: قبل إصدار أوامر **تصحيح الأخطاء**، راجع المعلومات المهمة في أوامر تصحيح الأخطاء. يجب تمكين أوامر **debug ip nbar** فقط في ظل ظروف يتم التحكم فيها بعناية.

إذا كانت هذه المعلومات غير كافية، فيمكنك تمكين إمكانية الالتقاط، والتي توفر طريقة سهلة التقاط آثار الحزم للبروتوكولات الجديدة. أستخدم أوامر **تصحيح الأخطاء** التالية، كما هو موضح أدناه.

```
debug ip nbar filter destination_port tcp XXXX
debug ip nbar capture 200 10 10 10
```

يحدد الأمر الأول الحزم التي تريد الالتقاط فيها. الأمر الثاني يضع NBAR في وضع الالتقاط. الوسيطات من أمر **الالتقاط** هي كما يلي:

- عدد وحدات البايت التي سيتم التقاطها لكل حزمة.
- عدد الحزم الأولى التي سيتم التقاط، بمعنى آخر، عدد الحزم التي سيتم التقاطها بعد حزمة نظام TCP/IP.
- عدد الحزم النهائية التي سيتم التقاط، بمعنى آخر، عدد الحزم في نهاية التدفق التي يجب حجز مساحة لها.
- عدد الحزم الإجمالية التي سيتم الالتقاط بها.

ملاحظة: يؤدي تحديد معلمات الحزمة الأولية والنهائية إلى التقاط الحزم ذات الصلة فقط في تدفق طويل.

أستخدم الأمر **show ip nbar capture** لعرض المعلومات المجمعة. بشكل افتراضي، ينتظر وضع الالتقاط وصول حزمة SYN ثم يبدأ في التقاط الحزم على ذلك التدفق ثنائي الإتجاه.

حظر Gnutella باستخدام PDLM المخصص

لننظر إلى مثال حول كيفية إستخدام PDLM المخصص. نستخدم Gnutella كحركة مرور نريد تصنيفها ثم تطبيق سياسة جودة الخدمة التي تمنع حركة المرور هذه.

تستخدم Gnutella ستة منافذ TCP معروفة جيدا - 6346 و 6347 و 6348 و 6349 و 6355 و 5634. قد يتم اكتشاف منافذ أخرى عند إستلام ملفات ربط. إذا حدد المستخدمون منافذ أخرى للاستخدام في مشاركة ملفات Gnutella، يمكنك إضافة هذه المنافذ إلى بيان بروتوكول المطابقة المخصص الخاص بك.

فيما يلي الخطوات الخاصة بإنشاء سياسة خدمة QoS التي تتطابق مع حركة مرور Gnutella وتقطعها.

1. وكما تمت الإشارة إليه أعلاه، أستخدم الأمر **show ip nbar unclassified-port-stats** لعرض حركة مرور NBAR "غير المصنفة". إذا كانت شبكتك تنقل حركة مرور Gnutella، فسترى مخرجات مماثلة لما يلي.

```
Port     Proto    # of Packets
-------  -------- -------
 tcp      347679    6346
 udp       55043   27005
```

2. أستخدم الأمر **ip nbar port-map المخصص** لتحديد خريطة منفذ مخصصة تطابق على منافذ GnuTella.

```
ip nbar port-map custom-02 tcp 5634 6346 6347 6348 6349 6355
```

ملاحظة: حاليا، يجب عليك إستخدام اسم مثل custom-xx. سيتم دعم الأسماء المعرفة من قبل المستخدم ل PDLMs المخصص في إصدار قادم من برنامج Cisco IOS Software.

3. أستخدم الأمر **show ip nbar protocol stats** لتأكيد التطابقات إلى البيان المخصص.

```
2620#show ip nbar protocol stats byte-count
FastEthernet0/0
               Input                    Output
Protocol           Byte Count              Byte Count
------------------------------------------------
custom-02          43880517                52101266
```

4. قم بإنشاء سياسة خدمة جودة الخدمة باستخدام أوامر واجهة سطر الأوامر لجودة خدمة الوحدة النمطية (MQC).

```
d11-5-7206-16(config)# class-map gnutella
d11-5-7206-16(config-cmap)# match protocol custom-02
d11-5-7206-16(config-cmap)# exit
d11-5-7206-16(config)# policy-map sample
d11-5-7206-16(config-pmap)# class gnutella
d11-5-7206-16(config-pmap-c)# police 1000000 31250 31250 conform-action
drop exceed-action drop violate-action drop
```

ارجع إلى إستخدام قوائم التحكم في الوصول والتطبيق المستندة إلى الشبكة لحظر دودة "الرمز الأحمر" لأوامر التكوين الأخرى لحظر GnuTella وحركة المرور الأخرى غير المرغوب فيها.

معلومات ذات صلة

- موارد دعم جودة الخدمة
- الدعم الفني - 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).