إستخدام إجراءات التقاط الحزم على جهاز FirePOWER

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

خطوات التقاط الحزم

نسخ ملف PCAP

المقدمة

يصف هذا وثيقة كيف أن يستعمل ال tcpdump أمر in order to على قبض ربط أن يكون رأيت ب شبكة قارن من FirePOWER ك.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من ال cisco Firepower أداة وال virtual أداة نموذج.

المكونات المستخدمة

ال يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة. وهو يستخدم صياغة عامل تصفية حزم Berkeley (BPF).

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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

تحذير: إذا قمت بتشغيل أمر tcpdump على نظام إنتاج، فقد يؤثر ذلك على أداء الشبكة.

خطوات التقاط الحزم

سجل الدخول إلى CLI الخاص بجهاز FirePOWER.

في الإصدارات 6.1 والإصدارات الأحدث، أدخل capture-traffic. على سبيل المثال,

<#root>

```
> capture-traffic


Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set  (Interfaces s2p1, s2p2)
```

في الإصدارات 6.0.x.x والإصدارات الأقدم، أدخل حركة مرور بيانات دعم النظام. على سبيل المثال,

<#root>

```
> system support capture-traffic


Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set  (Interfaces s2p1, s2p2)
```

بعد أن تقوم بعمل تحديد، يتم مطالبتك بالخيارات:

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

in order to على قبض معطيات كاف من الربط، وهو ضروري أن يستعمل الـ -S خيار in order to تثبت الـ شباك بشكل صحيح. يمكن تعيين الشباك إلى قيمة تطابق قيمة وحدة الإرسال القصوى (MTU) التي تم تكوينها لتكوين مجموعة الواجهة، والتي يتم تعيينها افتراضيا على 1518.

تحذير: عند التقاط حركة مرور البيانات إلى الشاشة، يمكن أن يقلل ذلك من أداء النظام والشبكة. cisco يوصي أن تستعمل أنت الـ <filename> خيار مع tcpdump أمر. وهو درب إلى الربط على قبض. إذا قمت بتشغيل الأمر بدون خيار -W ، فاضغط على مجموعة مفاتيح Ctrl-C للإنهاء.

مثال على خيار <filename>w:

<#root>

```
-w capture.pcap -s 1518
```

⚠ تحذير: لا تستخدم أي عناصر مسار عندما تحدد اسم ملف التقاط الحزمة (PCAP). يجب عليك تحديد اسم ملف pcap فقط ليتم إنشاؤه في الجهاز.

إذا كان من المفضل التقاط عدد محدود من الحزم، فيمكنك إستخدام علامة <الحزم>-c لتحديد عدد الحزم التي سيتم التقاط بها. على سبيل المثال، من أجل التقاط 5000 حزمة باستخدام:

```
<#root>

-w capture.pcap -s 1518 -c 5000
```

بالإضافة إلى ذلك، يمكن إضافة مرشح BPF في نهاية الأمر لتحديد الحزم التي يتم التقاطها. مثل، in order to حددت الربط التقاط إلى 5000 ربط مع مصدر أو غاية عنوان من 192.0.2.1، أنت يستطيع استعملت هذه خيار:

```
<#root>

-w capture.pcap -s 1518 -c 5000 host 192.0.2.1
```

عندما على قبض أنت حركة مرور أن يكون ظاهري lan (VLAN) بطاقة، أنت ينبغي عينت ال VLAN عم ال BPF بناء جملة. وإلا، ال يحتوي ال pcap أي من ال VLAN بطاقة تمييز ربط. على سبيل المثال، يحي هذه المثال من الالتقاط على حركة مرور البيانات التي تكون VLAN مميزة من 192.0.2.1:

```
<#root>

-w capture.pcap -s 1518 -c 5000 vlan and host 192.0.2.1
```

إن يكون أنت غير متأكد إن حركة مرور يكون VLAN تحدد، هذه إعراب يستطيع كنت استعملت in order to على قبض حركة مرور من 192.0.2.1 أي يكون ولا VLAN يعين:

```
<#root>

-w capture.pcap -s 1518 -c 5000 'host 192.0.2.1 or (vlan and host 192.0.2.1)'
```

ملاحظة: في المثال السابق، يلزم وجود الأقواس حتى ال يتطابق 'أو' على 'VLAN' فقط. لمن ثم تكون هناك حاجة إلى الاقتباسات المفردة لمنع أي تفسير خاطئ محتمل بواسطة الصدفة للأقواس.

على قبض ومواصفة صفة VLAN على كل حركة مرور VLAN التي تطابق بقية ملف BPF

الخاص بك. مهما، إن يريد أنت أن على قبض VLAN بطاقة خاص، أنت يستطيع عينت أي VLAN بطاقة أنت تريد أن على قبض مثل ذلك:

<#root>

```
-w capture.pcap -s 1518 -c 5000 vlan 1 and host 192.0.2.1
```

بعد أن تقوم بتحديد الخيارات المرغوبة واضغط على Enter، تبدأ tcpdump في التقاط حركة المرور.

تلميح: إذا لم يتم إستخدام خيار -c، اضغط على مجموعة مفاتيح Ctrl-C لإيقاف الالتقاط.

بمجرد أن تقوم بإيقاف الالتقاط، تتلقى تأكيدا. على سبيل المثال:

<#root>

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

```
-w capture.pcap -s 1518 -c 5000 host 192.0.2.1
```

```
Cleaning up.
Done.
```

نسخ ملف PCAP

لنسخ ملف PCAP من جهاز أمان FirePOWER إلى نظام آخر يقبل إتصالات SSH الواردة، أستخدم هذا الأمر:

<#root>

```
> system file secure-copy hostname username destination_directory pcap_file
```

بعد الضغط على Enter، تتم مطالبتك بكلمة المرور إلى النظام البعيد. يمكن نسخ الملف عبر الشبكة.

ملاحظة: في هذا المثال، يشير اسم المضيف إلى اسم المضيف البعيد الهدف أو عنوان IP له، ويحدد اسم المستخدم اسم المستخدم على المضيف البعيد، بينما يحدد PCAP_file ملف pcap destination_directory مسار الوجهة على المضيف البعيد، ويحدد

المحلي لنقله.

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).