تكوين الحزمة المضمّنة والتقاطها في البرنامج

المحتويات

المقدمة

يصف هذا المستند ميزة التقاط الحزمة المضمنة (EPC) في برنامج Cisco IOS®

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 12.4(20)T من Cisco أو إصدار أحدث
- Cisco IOS XE الإصدار 15.2(4)S - 3.7.0 أو إصدار أحدث

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.

معلومات أساسية

عند تمكينها، يلتقط الموجه الحزم المرسلة والمستلمة. يتم تخزين الحزم داخل مخزن مؤقت في DRAM والتي تستمر من خلال إعادة التحميل. بمجرد التقاط البيانات، يمكن فحصها في عرض ملخص أو مفصل على الموجه.

بالإضافة إلى ذلك، يمكن تصدير البيانات كملف التقاط حزمة (PCAP) للسماح بالمزيد من الفحص. يتم تكوين الأداة في وضع EXEC وتعتبر أداة مساعدة مؤقتة. ونتيجة لذلك، الا يتم تخزين تكوين الأداة داخل تكوين الموجه والي يبقى في مكانه بعد إعادة تحميل النظام.

توفر أداة Packet Capture Config Engine (المولد والمحلل) لعملاء Cisco للمساعدة في تكوين التقاط الحزم والتقاط هذه الحزم واستخراجها.

مثال تكوين IOS من Cisco

تكوين EPC الأساسي

1. قم بتحديد 'capture buffer'، وهو مخزن مؤقت حيث يتم تخزين الحزم التي تم الاستيلاء عليها.
2. هناك خيارات متعددة يمكن تحديدها عند تعريف المخزن المؤقت، مثل الحجم وحجم الحزمة القياسي والدورة/الخطية:

```
monitor capture buffer BUF size 2048 max-size 1518 linear
```

3. يمكن تطبيق عامل التصفية لتحديد الالتقاط على حركة المرور المطلوبة. قم بتحديد قائمة التحكم في الوصول (ACL) داخل وضع التكوين وطبق عامل التصفية على المخزن المؤقت:

```
ip access-list extended BUF-FILTER
    permit ip host 192.168.1.1 host 172.16.1.1
    permit ip host 172.16.1.1 host 192.168.1.1
```

```
monitor capture buffer BUF filter access-list BUF-FILTER
```

4. قم بتعريف نقطة الالتقاط التي تعرف مكان حدوث الالتقاط.
5. كما تحدد نقطة الالتقاط ما إذا كان الالتقاط يحدث لـ IPv4 أو IPv6 وفي أي مسار تحويل (العملية مقابل CEF):

```
monitor capture point ip cef POINT fastEthernet 0 both
```

6. إرفاق المخزن المؤقت بنقطة الالتقاط:

```
monitor capture point associate POINT BUF
```

7. بدء الالتقاط:

```
monitor capture point start POINT
```

8. الالتقاط الآن نشط. السماح بجمع البيانات الضرورية.

9. إيقاف الالتقاط:

```
monitor capture point stop POINT
```

10. فحص المخزن المؤقت على الوحدة:

```
show monitor capture buffer BUF dump
```

ملاحظة: يظهر هذا الإخراج تفريغ الحزم السداسية العشرية فقط. من أجل رؤيتهم مقروئين من البشر هناك طريقتان.

تصدير المخزن المؤقت من الموجه لمزيد من التحليل:

```
monitor capture buffer BUF export tftp://10.1.1.1/BUF.pcap
```

الطريقة السابقة غير عملية دائما لأنها تتطلب وصول T/FTP إلى الموجه. في مثل هذه الحالات، قم بأخذ نسخة من تفريغ hex واستخدم أي محول hex-pcap على الإنترنت لعرض الملفات.

11. بمجرد تجميع البيانات الضرورية، احذف "نقطة الالتقاط" و"مخزن الالتقاط المؤقت":

```
no monitor capture point ip cef POINT fastEthernet 0 both
no monitor capture buffer BUF
```

معلومات تكوين IOS الإضافية من Cisco

- في الإصدارات الأقدم من الإصدار 15.0(1)M من Cisco IOS، كان حجم المخزن المؤقت محدودا إلى 512K.
- في الإصدارات الأقدم من الإصدار 15.0(1)M من Cisco IOS، كان حجم الحزمة التي تم التقاطها محدودا إلى 1024 بايت.
- خزنت الربط مصدر في DRAM والي يستمر من خلال reload.
- ال يتم تخزين تكوين التقاط في ذاكرة NVRAM والي يستمر من خلال عمليات إعادة التحميل.
- يمكن تعريف نقطة التقاط للتقاط في CEF أو معالجة مسارات التحويل.
- يمكن تعريف نقطة التقاط للتقاط فقط على واجهة أو بشكل عام.
- عندما يتم تصدير مخزن التقاط المؤقت بتنسيق PCAP، ال يتم الحفاظ على معلومات L2 (مثل تضمين الإيثرنت).
- راجع أفضل الممارسات لأوامر البحث للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

تكوين تصدير-حركة مرور IP الأساسية

تصدير حركة مرور IP هي طريقة مختلفة لتصدير حزم IP التي يتم استقبالها على واجهات متعددة ومتزامنة لشبكة WAN أو شبكة LAN.

1. في وضع التكوين، قم بتعريف ملف تعريف تصدير حركة مرور IP.

```
Device(config)# ip traffic-export profile mypcap mode capture
```

2. قم بتكوين حركة مرور ثنائية الإتجاه في ملف التعريف.

```
Device(config-rite)# bidirectional
```

3. الخروج

4. حدد الواجهة لحركة المرور المصدرة.

```
Device(config-if)# interface GigabitEthernet 0/1
```

5. تمكين تصدير حركة مرور IP على الواجهة.

```
Device(config-if)# ip traffic-export apply mypcap size 10000000
```

6. الخروج

7. ابدأ عملية الالتقاط. الالتقاط الآن نشط. السماح بجمع البيانات الضرورية.

```
Device# traffic-export interface GigabitEthernet 0/1 start
```

8. أوقف الأسر.

```
Device# traffic-export interface GigabitEthernet 0/1 stop
```

9. تصدير الالتقاط إلى خادم TFTP خارجي.

```
Device# traffic-export interface GigabitEthernet 0/1 copy tftp://<TFTP_Address>/mypcap.pcap
```

10. بمجرد تجميع البيانات اللازمة، احذف ملف التعريف.

```
Device(config)# no ip traffic-export profile mypcap
```

عيوب تصدير حركة مرور IP

يحتوي تصدير حركة مرور IP على هذه المميزات مقارنة بطريقة EPC:

- يجب أن تكون الواجهة التي يتم تصدير حركة المرور الملتقطة فيها واجهة إيثرنت.
- لا يوجد دعم لـ IPv6.
- لا توجد معلومات الطبقة 2، فقط الطبقة 3 وما فوقها.

مثال تكوين Cisco IOS-XE

تم إدخال ميزة "التقاط الحزمة المضمنة" في الإصدار 3.7 من Cisco IOS XE - 15.2(4)S. يختلف تكوين الالتقاط عن Cisco IOS لأنه يضيف المزيد من المميزات.

تكوين EPC الأساسي

1. قم بتحديد موقع حدوث الالتقاط:

```
monitor capture CAP interface GigabitEthernet0/0/1 both
```

2. إقران عامل تصفية. عامل التصفية إما محدد في السطر، أو يمكن الإشارة إلى قائمة تحكم في الوصول (ACL) أو خريطة الفئة:

```
monitor capture CAP match ipv4 protocol tcp any any limit pps 1000000
```

3. بدء الالتقاط:

```
monitor capture CAP start
```

4. الالتقاط الآن نشط. اسمح له بجمع البيانات الضرورية.

5. إيقاف الالتقاط:

```
monitor capture CAP stop
```

6. افحص الالتقاط في عرض ملخص:

```
show monitor capture CAP buffer brief
```

7. افحص الالتقاط بطريقة عرض تفصيلية:

```
show monitor capture CAP buffer detailed
```

8. إضافة إلى ذلك، قم بتصدير الالتقاط بتنسيق PCAP لمزيد من التحليل:

```
monitor capture CAP export tftp://10.0.0.1/CAP.pcap
```

9. بمجرد تجميع البيانات الضرورية، قم بإزالة عملية الالتقاط:

```
no monitor capture CAP
```

معلومات إضافية

- يتم إجراء الالتقاط على الواجهات المادية والواجهات الفرعية وواجهات النفق.
- المرشحات المستندة إلى التعرف على التطبيق (NBAR) المستندة إلى الشبكة (التي تستخدم **match protocol** الأمر ضمن class-map) غير مدعوم حاليا.
- راجع أفضل الممارسات لأوامر البحث للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لضمان إعداد EPC بشكل صحيح، يتم إستخدام أمر تصحيح الأخطاء هذا على Cisco IOS-XE® الذي يعمل على EPC:

```
debug epc provision
debug epc capture-point
```

معلومات ذات صلة

- التقاط الحزمة المضمنة - Cisco IOS-XE
- التقاط حزمة مضمنة - Cisco IOS
- الدعم التقني والتنزيلات من Cisco

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).