الحل البديل لتمكين حركة مرور AVC من المرور عبر واجهة نفق IPSec

المحتويات

المقدمة

يصف هذا المستند التكوين المطلوب لنقل حركة مرور AVC عبر نفق IPSec إلى مجمع البيانات. بشكل افتراضي، لا يمكن تصدير معلومات AVC عبر نفق IPSec إلى مجمع البيانات

المتطلبات الأساسية

توصي cisco أن يتلقى أنت المعرفة الأساسية من هذا موضوع:

- إمكانية رؤية التطبيقات والتحكم فيها (AVC)
- شاشة سهلة الأداء (EzPM)

معلومات أساسية

يتم إستخدام ميزة التوافق الكهرومغناطيسي (AVC) من Cisco للتعرف على تطبيقات متعددة وتحليلها والتحكم فيها. وبفضل ميزة التوعية بالتطبيقات التي تم تضمينها في البنية الأساسية للشبكة، إلى جانب إمكانية الرؤية في أداء التطبيقات التي تعمل

على الشبكة، تعمل أداة التحكم المتقدمة (AVC) على تمكين نهج كل تطبيق للتحكم الدقيق في إستخدام النطاق الترددي العريض للتطبيقات، مما يؤدي إلى تحسين تجربة المستخدم النهائي. هنا يمكنك العثور على المزيد من التفاصيل حول هذه التقنية.

تعد EzPM طريقة أسرع وأسهل لتكوين التكوين التقليدي لمراقبة الأداء. لا توفر ميزة EzPM حاليا المرونة الكاملة لنموذج تكوين مراقبة الأداء التقليدي. هنا يمكنك العثور على مزيد من التفاصيل حول EzPM.

تحديد

لا يدعم AVC حاليا عدد بروتوكولات نفق المرور، يمكن العثور على التفاصيل هنا.

أمان بروتوكول الإنترنت (IPSec) هو أحد بروتوكولات نفق المرور غير المدعومة ل AVC ويعالج هذا المستند الحل البديل المحتمل لهذا الحد.

التكوين

يصف هذا القسم التكوين الكامل المستخدم لمحاكاة التحديد المحدد.

الرسم التخطيطي للشبكة

في هذا الرسم التخطيطي للشبكة، تتوفر لجميع الموجهات إمكانية الوصول إلى بعضها البعض باستخدام المسارات الثابتة. يتم تكوين R1 باستخدام تكوين EzPM ويحتوي على نفق IPSec واحد تم إنشاؤه باستخدام الموجه R2. يعمل R3 كمصدر هنا، والذي يمكن أن يكون Cisco Prime أو أي نوع آخر من المصدرين القادرين على تجميع بيانات الأداء.

يتم إنشاء حركة مرور AVC بواسطة R1 ويتم إرسالها إلى المصدر عبر R2. يرسل R1 حركة مرور AVC إلى R2 عبر واجهة نفق IPSec.

التهيئة الأولية

يصف هذا القسم التكوين الأولي ل R1 حتى R3.

R1

```
!
interface loopback0
عنوان IP 1.1.1.1 255.255.255.255
!

interface GigabitEthernet0/1

 عنوان IP 172.16.1.1 255.255.255.0

 الإرسال ثنائي الإتجاه التلقائي

 السرعة التلقائية

!
```

ip route 0.0.0.0.0.0.0.0 172.16.1.2

!

R2

!

واجهة GigabitEthernet0/0/0

عنوان IP 172.16.2.2 255.255.255.0

آلية التفاوض

!

واجهة GigabitEthernet0/0/1

عنوان IP 172.16.1.2 255.255.255.0

آلية التفاوض

!

R3

!

interface GigabitEthernet0/0

عنوان IP 172.16.2.1 255.255.255.0

الإرسال ثنائي الإتجاه التلقائي

السرعة التلقائية

!

ip route 0.0.0.0.0.0.0.0 172.16.2.2

!

تكوين IPSec

يصف هذا القسم تكوين IPSec للموجه R1 و R2.

R1

!

ip access-list extended IPSec_Match

السماح ب IP أي مضيف 172.16.2.1

!

سياسة التشفير ISAKMP 1

إنإيه إس 256

تجزئة MD5

مشاركة مسبقة للمصادقة

المجموعة الثانية

crypto isakmp مفتاح Cisco123 عنوان 172.16.1.2

!

!

crypto ipSec transform-set2 esp-aes 256 esp-sha-hmac

نفق النمط

!

!

خريطة التشفير VPN 10 IPsec-ISAKMP

set نظير 172.16.1.2

مجموعة تحويل المجموعة 2

مطابقة العنوان IPSec_Match

!

interface GigabitEthernet0/1

عنوان IP 172.16.1.1 255.255.255.0

الإرسال ثنائي الإتجاه التلقائي

السرعة التلقائية

شبكة VPN لخريطة التشفير

!

R2

```
!
ip access-list extended IPSec_Match
 السماح بمضيف IP 172.16.2.1 أي
!
سياسة التشفير ISAKMP 1
 إنإ هيإ سإ 256
 تجزئة MD5
 مشاركة مسبقة للمصادقة
 المجموعة الثانية
crypto isakmp مفتاح Cisco123 عنوان 172.16.1.1
!
!
crypto ipSec transform-set2 esp-aes 256 esp-sha-hmac
 طمنلا قفن
!
!
خريطة التشفير VPN 10 IPsec-ISAKMP
 set نظير 172.16.1.1
 مجموعة تحويل المجموعة 2
 مطابقة العنوان IPSec_Match
 سكاعم قيرط
!
واجهة GigabitEthernet0/0/1
 عنوان IP 172.16.1.2 255.255.255.0
 آلية التوافض
 تمكين CDP
 شبكة VPN لخريطة التشفير
```

!

للتحقق من ما إذا كان تكوين IPSec يعمل كما هو متوقع أم لا، تحقق من الإخراج show crypto isakmp sa

```
R1#show crypto isakmp sa

IPv4 crypto ISAKMP SA

حالة conn-id الحالة dst src state

IPv6 crypto ISAKMP SA
```

ومن أجل رفع مستوى الارتباطات الأمنية، أزيز المصدر (R3، 172.16.2.1) من R1.

```
R1#ping 172.16.2.1

اكتب تسلسل الهروب للإجهاض.

إرسال أصداء ICMP تأذ 5 و 100 إلى تياب 172.16.2.1، المهلة هي ثانيتان:

!!!!

دحلا وه اباإو اباهذ رفسلاو ، (5/5) ةئامل يف 100 وه حاجنلا لدعم
ألادنى/المتوسط/الحد ألاقصى = 1/1/4 مللي ثانية

R1#
```

الآن، سيكون للموجه اقتران أمان نشط، يؤكد أن حركة المرور التي يتم إنشاؤها من R1 وموجهة إلى المصدر هي ESP مضمنة.

```
R1#show crypto isakmp sa

IPv4 crypto ISAKMP SA

حالة conn-id الحالة dst src state

172.16.1.2 172.16.1.1 QM_Idle 1002 نشط

IPv6 crypto ISAKMP SA
```

تكوين EzPM

يصف هذا القسم تكوين EZpm للموجه R1.

R1

```
!

class-map match-all perf-mon-acl

الكيان الذي تم إنشاؤه ل PrimeAM للوصف - ال تقم بتعديل هذا الكيان أو إستخدامه
```

IP لبروتوكول المطابقة

!

تجربة تطبيق ملف تعريف مراقب أداء سياق مراقبة الأداء

غاية المصدر 172.16.2.1 مصدر GigabitEthernet0/1 نقل udp ميناء 991

تطبيق مراقبة حركة المرور - حالات حركة المرور

محادثة مراقبة حركة المرور-حالة حركة مرور IPv4

المرور حركة مراقبة تطبيق للاستجابة لمزن (IP) الإنترنت لبروتوكول من عبارل الإصدار

مدخل IPv4 ولسائط مراقبة حركة مرور

مخرج وسائط IPv4 لمراقبة حركة المرور

عنوان URL ipV4 لفئة Perf-mon-acl الخاص بمراقبة حركة المرور

!

تطبيق ملف تعريف EzPM على الواجهة التي يلزم مراقبتها؛ انه موقن بمراقبة واجهة الاسترجاع 0.

R1

!

interface loopback0

عنوان IP 1.1.1.1 255.255.255.255

مراقب أداء سياق مراقبة الأداء

!

الحل

مع وجود التكوين المذكور أعلاه، فعليك بمخرجات **show performance monitor** *contextcontext-* **nameSource**.

تحقق من حالة خيار **ميزات الإخراج**، بشكل افتراضي، يجب أن يكون في حالة **غير مستخدم**، وهو سلوك متوقع ولهذا السبب لا يتم تضمين حركة مرور AVC أو تشفيرها هنا.

للسماح لحركة مرور AVC بالمرور من خلال واجهة نفق IPsec، يجب أن يكون خيار **ميزات الإخراج** في الحالة المستخدمة. ولذلك، يجب تمكينها بشكل صريح في ملف تعريف مصدري التدفق. فيما يلي الإجراء بالتفصيل خطوة بخطوة لتمكين هذا الخيار.

الخطوة-1

قم بأخذ الإخراج الكامل لأمر **تكوين show performance monitor context** *name* واحفظه في

المفكرة. أدناه هو ال snip لهذا مخرجات،

```
R1#show مراقبة الأداء سياق مراقبة الأداء تشكيل شاشة الأداء

!=======================================================================
=========

!             سياق ! أداء مراقب مكافئ تكوين

!=======================================================================
=========

!المصدرون

!========

!

نظام مراقبة الأداء-1 المصدر التدفق

 وصف مصدر مراقب أداء السياق Performance-Monitor

 الوجهة 172.16.2.1

 GigabitEthernet0/1 المصدر

 Transport UDP 9991

 بروتوكول التصدير

 مهلة بيانات القالب 300

 خيار قارن-طاولة مهلة 300

 خيار vrf-table مهلة 300

 خيار c3pl-class-table مهلة 300

 option c3pl-policy-table timeout 300

 مهلة 300 جدول عينات الخيار

 خيار مهلة جدول التطبيق 300

 خيار مهلة سمات التطبيق 300

 مهلة جدول تطبيق الخيار الفرعي 300
—snip—
```

الخطوة-2

قم بإضافة خيار **ميزات الإخراج** بشكل صريح تحت كل تعريف مصدر التدفق. بعد إضافة

خيار مميزات المخرجات، يدو ملف تعريف مصدر التدفق بهذا الشكل،

نظام مراقبة الأداء-1 لمصدر التدفق

وصف مصدر مراقب أداء السياق Performance-Monitor

الوجهة 172.16.2.1

المصدر GigabitEthernet0/1

Transport UDP 9991

بروتوكول التصدير

مهلة بيانات القالب 300

مميزات المخرجات

خيار قارن-تواطؤ مهلة 300

خيار vrf-table مهلة 300

خيار c3pl-class-table مهلة 300

option c3pl-policy-table timeout 300

مهلة 300 لجدول عينات الخيار

خيار مهلة جدول التطبيق 300

خيار مهلة سمات التطبيق 300

مهلة جدول تطبيق الخيار الفرعي 300

أترك بقية المخرجات كما هي، لا تغير أي شيء آخر في المخرجات.

الخطوة-3

الآن، قم بإزالة ملف تعريف EzPM من الواجهة ومن الموجه أيضا.

!

إسترجاع الواجهة 0

لا مراقبة أداء سياق مراقبة الأداء

خرج

!

!

لا توجد تجربة تطبيق ملف تعريف مراقب أداء سياق مراقبة الأداء

!

الخطوة-4

قم بتطبيق التكوين المعدل على الموجه R1. تأكد من عدم فقد أي أمر، حيث أنه قد يؤدي إلى أي سلوك غير متوقع.

التحقق من الصحة

يصف هذا القسم طريقة التحقق المستخدمة في هذا المستند للتحقق وكيف ساعد هذا الحل البديل في التغلب على حدود حزم AVC المذكورة هنا.

قبل تطبيق الحل البديل، سيتم إسقاط الحزم التي يتم استقبالها بواسطة موجه نظير IPSec (R2). سيتم إنشاء الرسالة أدناه أيضا:

```
%IPSec-3-RECVD_PKT_NOT_IPsec: حزمة rec d ليست حزمة IPsec، dest_addr=
172.16.2.1، src_addr= 172.16.1.1، prot= 17
```

هنا يتوقع R2 حزم ESP المضمنة الموجهة ل 172.16.2.1، ولكن الحزم المستلمة هي حزم UDP العادية (prot=17) ومن السلوك المتوقع إسقاط هذه الحزم. يوضح التقاط الحزمة أدناه أن الحزمة المستلمة في R2 هي حزمة UDP عادية بدل من تضمين ESP، وهو سلوك افتراضي ل AVC.

```
Internet Protocol Version 4, Src: 172.16.1.1 (172.16.1.1), Dst: 172.16.2.1 (172.16.2.1)
  Version: 4
  Header Length: 20 bytes
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 1348
  Identification: 0x961a (38426)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: UDP (17)
⊞ Header checksum: 0xc56b [validation disabled]
  Source: 172.16.1.1 (172.16.1.1)
  Destination: 172.16.2.1 (172.16.2.1)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 50208 (50208), Dst Port: 9991 (9991)
  Source Port: 50208 (50208)
  Destination Port: 9991 (9991)
  Length: 1328
⊞ Checksum: 0xb7ec [validation disabled]
  [Stream index: 0]
Data (1320 bytes)
```

بعد تطبيق الحل، يتضح من التقاط الحزمة أدناه أن حزم AVC المستلمة في R2 هي ESP مضمنة ولا توجد رسائل خطأ أخرى مرئية على R2.

```
Internet Protocol Version 4, Src: 172.16.1.1 (172.16.1.1), Dst: 172.16.1.2 (172.16.1.2)
  Version: 4
  Header Length: 20 bytes
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 1448
  Identification: 0x0114 (276)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: Encap Security Payload (50)
⊞ Header checksum: 0x5aec [validation disabled]
  Source: 172.16.1.1 (172.16.1.1)
  Destination: 172.16.1.2 (172.16.1.2)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
Encapsulating Security Payload
  ESP SPI: 0x804c46a3 (2152482467)
  ESP Sequence: 203
```

استكشاف الأخطاء وإصلاحها

ال توجد حاليا معلومات خاصة حول أستكشاف الأخطاء وإصلاحها متوفرة لهذا التكوين.

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).