دليل أستكشاف أخطاء تكوين IOS-XE ZBFW وإصلاحها

المحتويات

المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء ميزة جدار الحماية المستند إلى المنطقة (ZBFW) وإصلاحها على أفضل نحو على موجه خدمات التجميع (1000 (ASR، باستخدام الأوامر التي يتم إستخدامها لاستطلاع عدادات إسقاط الأجهزة على ASR. يعد ASR1000 بمثابة نظام إعادة توجيه قائم على الأجهزة. يقوم تكوين البرامج من Cisco IOS-XE® برمجة ASICs الخاصة بالأجهزة (QFP) من أجل تنفيذ وظائف إعادة توجيه الميزات. وهذا يسمح بإنتاجية أعلى وأداء أفضل. والعيب في ذلك هو أنه يمثل تحديا أكبر لاستكشاف الأخطاء وإصلاحها. لم تعد أوامر Cisco IOS التقليدية المستخدمة لاستطلاع الجلسات الحالية وعدادات الإسقاط عبر جدار الحماية المستند إلى المنطقة (ZBFW) صالحة حيث لم تعد عمليات الإسقاط في البرنامج.

الروابط والوثائق

مراجع الأوامر

- سلسلة موجهات خدمات التجميع طراز ASR 1000 من Cisco لمراجع الأوامر
- مراجع أوامر IOS XE 3S من Cisco

خطوات أستكشاف أخطاء DataPath وإصلاحها

لاستكشاف أخطاء قاعدة البيانات وإصلاحها، يجب تحديد ما إذا كان قد تم تمرير حركة المرور بشكل صحيح من خلال رمز ASR و Cisco IOS-XE. فيما يتعلق بميزات جدار الحماية، يتبع أستكشاف أخطاء البيانات وإصلاحها الخطوات التالية:

1. **دقةت تشكيل** - جمع التشكيل وفحص الإنتاج in order to دقةت التوصيل.

2. **التحقق من حالة الاتصال** - إذا مرت حركة المرور بشكل صحيح، يقوم Cisco IOS-XE بفتح اتصال على ميزة ZBFW. يقوم هذا الاتصال بتعقب حركة مرور البيانات ومعلومات الحالة بين العميل والخادم.

3. **التحقق من عدادات الإسقاط** - عندما لا تمر حركة المرور بشكل صحيح، يقوم Cisco IOS-XE بتسجيل عداد إسقاط لأي حزم يتم إسقاطها. فحصت هذا إنتاج in order to عزلت السبب من الحركة مرور إخفاق.

4. **التسجيل** - تجميع syslog لتوفير مزيد من المعلومات التفصيلية حول عمليات إنشاء الاتصال وحالات إسقاط الحزم.

5. **الحزم المسقطة لتتبع الحزم** - أستخدم تتبع الحزم من أجل التقاط الحزم المسقطة.

6. **تصحيح الأخطاء** - تجميع تصحيح الأخطاء هو الخيار الأكثر تفصيلا. يمكن الحصول على تصحيح الأخطاء بشروط لتأكيد مسار إعادة التوجيه الدقيق للحزم.

التحقق من التكوين

يتم تلخيص مخرجات **جدار حماية دعم التقنية** show هنا:

```
-------- show clock --------
------- show version --------
-------- show running-config --------
-------- show parameter-map type inspect --------
------- show policy-map type inspect --------
-------- show class-map type inspect --------
-------- show zone security --------
-------- show zone-pair security --------
-------- show policy-firewall stats global --------
-------- show policy-firewall stats zone --------
-------- <show platform hardware qfp active feature firewall datapath <submode --------
-------- <show platform software firewall RP <submode --------
```

التحقق من حالة الاتصال

يمكن الحصول على معلومات الاتصال بحيث يتم سرد جميع الاتصالات الموجودة على ZBFW. دخلت هذا أمر:

```
ASR#show policy-firewall sessions platform
-- show platform hardware qfp active feature firewall datapath scb any any any any any all any--
[s=session  i=imprecise channel  c=control channel  d=data channel]
```

```
[proto 6 (0:0)    [sc 23 14.36.1.206 41392 14.38.112.250
```

وهو يعرض اتصال برنامج Telnet ل TCP من 14.38.112.250 إلى 14.36.1.206.

ملاحظة: اعلم أنه إذا قمت بتشغيل هذا الأمر، فسيأخذ وقتا طويلا إذا كانت هناك إتصالات كثيرة على الجهاز. توصي Cisco بتشغيل هذا الأمر باستخدام عوامل تصفية معينة كما هو موضح هنا.

يمكن تصفية جدول الاتصال إلى عنوان مصدر أو وجهة محدد. أستخدم المرشحات بعد الوضع الفرعي **للنظام الأساسي**. خيارات التصفية هي:

```
? radar-ZBFW1#show policy-firewall sessions platform
      all                      detailed information
  destination-port          Destination Port Number
      detail                     detail on or off
     icmp                     Protocol Type ICMP
  imprecise                 imprecise information
    session                   session information
            source-port              Source Port
         source-vrf               Source Vrf ID
    standby                   standby information
      tcp                       Protocol Type TCP
      udp                       Protocol Type UDP
v4-destination-address  IPv4 Desination Address
    v4-source-address       IPv4 Source Address
v6-destination-address  IPv6 Desination Address
    v6-source-address       IPv6 Source Address
       Output modifiers                       |
                                             <cr>
```

تمت تصفية جدول الاتصال هذا حتى يتم عرض الاتصالات التي تم الحصول عليها من 14.38.112.250 فقط:

```
ASR#show policy-firewall sessions platform v4-source-address 14.38.112.250
show platform hardware qfp active feature firewall datapath scb 14.38.112.250--
                                                -- any any any any all any
                [s=session  i=imprecise channel  c=control channel  d=data channel]
                [proto 6 (0:0)    [sc 23 14.36.1.206 41392 14.38.112.250
```

وبمجرد تصفية جدول الاتصال، يمكن الحصول على معلومات الاتصال التفصيلية من أجل عملية تحليل بيانات أكثر شمولا. لعرض هذا الإخراج، أستخدم الكلمة الأساسية **detail**.

```
ASR#show policy-firewall sessions platform v4-source-address 14.38.112.250 detail
  show platform hardware qfp active feature firewall datapath scb 14.38.112.250--
                                          --any any any any all any detail
                [s=session  i=imprecise channel  c=control channel  d=data channel]
                      [proto 6 (0:0)       [sc 23 14.36.1.206 41426 14.38.112.250
                   ,pscb : 0x8c5d4f20,  bucket : 64672, fw_flags: 0x204 0x20419441
                                         scb state: active, scb debug: 0
          nxt_timeout: 360000, refcnt: 1,  ha nak cnt: 0,  rg: 0, sess id: 117753
                               hostdb: 0x0, L7: 0x0, stats: 0x8e118e40, child: 0x0
              l4blk0: 78fae7a7 l4blk1: e36df99c l4blk2: 78fae7ea l4blk3: 39080000
               l4blk4: e36df90e l4blk5: 78fae7ea l4blk6: e36df99c l4blk7: fde0000
                                                    l4blk8: 0 l4blk9: 1
                                                root scb: 0x0 act_blk: 0x8e1115e0
      (ingress/egress intf: GigabitEthernet0/0/2 (1021), GigabitEthernet0/0/0 (131065
  current time 34004163065573 create tstamp: 33985412599209 last access: 33998256774622
                  nat_out_local_addr:port: 0.0.0.0:0 nat_in_global_addr:port: 0.0.0.0:0
                                                    syncookie fixup: 0x0
                                                halfopen linkage: 0x0 0x0
                                                        cxsc_cft_fid: 0x0
```

```
tw timer: 0x0 0x0 0x372ba 0x1e89c181
Number of simultaneous packet per session allowed: 25
bucket 125084 flags 1 func 1 idx 8 wheel 0x8ceb1120
```

التحقق من عدادات إسقاط جدار الحماية

تم تغيير إخراج عداد الإسقاط أثناء XE 3.9. قبل XE 3.9، كانت أسباب إسقاط جدار الحماية عامة جدا. بعد XE 3.9، تم توسيع أسباب إسقاط جدار الحماية لتصبح أكثر دقة.

للتحقق من عدادات الإسقاط، قم بتنفيذ خطوتين:

1. تأكيد عدادات الإسقاط العمومية في Cisco IOS-XE. تظهر هذه العدادات الميزة التي أسقطت حركة المرور. وتتضمن أمثلة الميزات جودة الخدمة (QoS) وترجمة عنوان الشبكة (NAT) وجدار الحماية وما إلى ذلك.

2. بمجرد تحديد الميزة الفرعية، استفسر عن عدادات الإسقاط متعددة المستويات التي توفرها الميزة الفرعية. في هذا الدليل، الميزة الفرعية التي يتم تحليلها هي ميزة جدار الحماية.

عدادات الإسقاط العمومية على QFP

الأمر الأساسي الذي يمكنك الاعتماد عليه يوفر جميع حالات السقوط عبر منفذ QFP:

```
Router#show platform hardware qfp active statistics drop
```

يوضح هذا الأمر لك عمليات الإسقاط العامة بشكل عام عبر QFP. يمكن أن تكون هذه الإسقاطات في أي ميزة. بعض ميزات المثال هي:

```
    Ipv4Acl
Ipv4NoRoute
    Ipv6Acl
Ipv6NoRoute
  NatIn2out
     VfrErr
     etc...
```

لعرض جميع عمليات الإسقاط، قم بتضمين العدادات التي تحتوي على قيمة صفر، أستخدم الأمر:

```
show platform hardware qfp active statistics drop all
```

لمسح العدادات، أستخدم هذا الأمر. يقوم بمسح المخرجات بعد إظهارها على الشاشة. يكون هذا الأمر واضحا عند القراءة، بحيث يتم إعادة تعيين الإخراج إلى صفر **بعد** عرضه على الشاشة.

```
show platform hardware qfp active statistics drop clear
```

فيما يلي قائمة بعدادات الإسقاط لجدار الحماية العمومي QFP والشرح:

سبب الإسقاط العام لجدار الحماية	الشرح
الضغط الخلفي لجدار الحماية	إسقاط الحزمة بسبب الضغط الخلفي بواسطة آلية التسجيل
FirewallInvalidZone	لم يتم تكوين أي منطقة أمان للواجهة.
FirewallL4Insp	فشل التحقق من نهج L4. را الجدول أدناه لمزيد من أسبا الإسقاط متعدد المستويات

	(أسباب إسقاط ميزة جدار الحماية).
FirewallNoForwardingZone	لم يتم تهيئة جدار الحماية، ول يسمح لحركة المرور بالمرور.
FirewallNonsession	فشل إنشاء جلسة العمل. قد يرجع ذلك إلى وصول الحد الأقصى لجلسة العمل أو فش تخصيص الذاكرة.
FirewallPolicy	تم إسقاط نهج جدار الحماية الذي تم تكوينه.
جدار الحماية L4	فشل فحص L4. راجع الجدو أدناه لمزيد من أسباب الإسقا متعدد المستويات (أسباب إسقاط ميزة جدار الحماية).
جدار الحماية L7	إسقاط الحزمة بسبب فحص L7. انظر أدناه للاطلاع على قائمة بأسباب الإسقاط الأكثر دقة للمستوى 7 (أسباب إسقا ميزة جدار الحماية).
FirewallNotInitiator	ليس مهيئ جلسة عمل ل CP أو UDP أو ICMP. لم يتم إنشاء جلسة عمل. على سبيل المثال، بالنسبة ل ICMP، فإ الحزمة الأولى التي يتم استقبالها ليست ECHO أو الطابع الزمني. بالنسبة ل CP فإنه ليس SYN. قد يحدث ذلك في معالجة الحزمة العادية أو معالجة الق غير الدقيقة.
FirewallNoNewSession	جدار الحماية عالي التوفر لا يسمح بالجلسات الجديدة.
FirewallSyncookieMaxDST	لتوفير الحماية من فيضانات SYN المستندة إلى المضيف هناك معدل SYN لكل وجهة كحد لفيضان SYN. عندما يص عدد إدخالات الوجهة إلى الحد يتم إسقاط حزم SYN الجدي تم تشغيل منطق SyncCool
FirewallSyncookie	يشير هذا إلى أنه تم إرسال SYN/ACK مع ملف تعريف إرتباط SYN، ويتم إسقاط حزمة SYN الأصلية.
FirewallARStandby	لم يتم تمكين التوجيه غير المتماثل ومجموعة التكرار ليست في الحالة النشطة.

عدادات إسقاط ميزة جدار الحماية على QFP

التحديد الموجود على عداد الإسقاط العالمي QFP هو عدم وجود نقاوة في أسباب الإسقاط، ويتم تحميل بعض أسباب الإسقاط مثل **FirewallL4** بشكل زائد إلى النقطة التي لا يكون لها إستخدام كبير لاستكشاف الأخطاء وإصلاحها. وقد تم تحسين هذا منذ ذلك الحين في Cisco IOS-XE 3.9 (15.3(2)S)، حيث تمت إضافة عدادات

إسقاط ميزة جدار الحماية. ويعطي هذا مجموعة أكثر دقة من أسباب السقوط:

```
ASR#show platform hardware qfp active feature firewall drop all
-----------------------------------------------------------------------------
                                                                Drop Reason Packets
-----------------------------------------------------------------------------
                                                        Invalid L4 header 0
                                                         Invalid ACK flag 0
                                                       Invalid ACK number 0
                                                                       ....
```

فيما يلي قائمة بالأسباب والتوضيحات لإسقاط ميزة جدار الحماية:

سبب إسقاط ميزة جدار الحماية	الشرح
طول رأس غير صالح	مخطط البيا صغير جدا ل أنه لا يمكن يحتوي على الطبقة TCP UDP أو رأ ICMP. قد السبب إلى: 1. طول 20 < 2. طول /ICM P < 8
طول بيانات UDP غير صالح	لا يتطابق ط مخطط بيانا UDP مع ال المحدد في UDP.
رقم ACK غير صالح	قد يرجع ه الهبوط إلى هذه الأسبا 1. ACK يساو _seq الخاص بنظير 2. ACK من أ SEQ الذي إرسال بواس نظير في حالة مز TCP و VD من المتوقع يكون ACK مساويا ل 1 ولكنه ليس

قد يرجع هذ
الهبوط إلى
هذه الأسبا

1. من ال
وجود
ACK
لم يتم
تعيينه
حالة
مختلف

2. بالإض
إلى ع
ACK
أيضا
علامة
(مثل
RST

يحدث هذا ع

1. الحزم
الأولى
بادئ
ليست
(يتم ت
مقطع
غير ال
بدون
عمل
صالح

2. تحتوي
حزمة
الأولية
مجمو
علامات
ACK

تحتوي حزم
SYN على
هذا غير مدع
يمكن أن تك
علامات TCP
صالحة بسب

1. تحتوي
حزمة
الأولية
TCP
علامات
أخرى
SYN

2. في ح

علامة ACK غير صالحة

بادئ TCP غير صالح

SYN ببيانات

علامات TCP غير صالحة

إستما
TCP
يستقب
نظير
RST
ACK
3. يتم تا
حزمة
المست
الآخر
ACK
.
4. لم يتم
ACK
المتوق
المست
مقطع TCP
صالح في ح
SYNSENT
بسبب:
1. ACK
لديه
2. يحتوي
ACK
على
مجمو
علاما
أخرى
(SH،
URG،
(FIN
3. استلم
عابر
حمول
4. إستلا
حزمة
SYN
البادئ
يمكن أن يك
مقطع TCP
صالح في ح
SYNRCVD
بسبب:
1. إستلا
إعادة
بحمو
البادئ
2. إستلا

مقطع غير صالح في حالة SYNSENT

مقطع غير صالح في حالة SYNRCVD

مقطع
صالح
ACK
أو ST
FIN
المست
يحدث ذلك
حالة
yncRCVD
عندما تأتي
المقاطع من
البادئ. إنه ب
1. قيمة
أقل م
قيمة
2. إذا كا
حجم
CVD
المست
و:
يحتوي
المقط
على
أو
مقطع
الترتيب
(Seq
من
ACK
الخاص
بالمس
3. إذا كا
حجم
CVD
الخاص
بالمس
هو 0
رقم
يقع خ
النافذ
4. Seq#
يساوي
ولكن
حزمة
SYN
ينتج خيار م
نافذة TCP
صالح عن ص

SEQ غير صالح

خيار مقياس إطار غير صالح

بايت خيار م
النافذة غير
الصحيح.
الحزمة قديم
- نافذة واح
خلف ACK
الآخر. يمكن
يحدث هذا ف
حالة tWait
Lastack.
الحمولة التي
تلقيها بعد إر
FIN. يمكن
يحدث هذا ف
حالة
"كلوسيانتس
يحدث ذلك ع
تجاوز حجم
المقطع الوا
لنافذة المس
مهما، إن مك
vTCP يكو
شرط يسمح
جدار الحماي
يحتاج أن يخ
المقطع مؤق
ALG أن يس
فيما بعد.

تم بالفعل
الاعتراف بال
التي تمت إع
إرسالها بواس
المستلم.
يوشك تسلي
الحزمة التي
يتم طلبها إل
للفحص. إذا
يسمح L7 ب
OOO، سيت
إسقاط هذه
الحزمة.
تحت هجوم
فيضان TCP
SYN. بموج
شروط معين
عندما تتجاو
الاتصالات ال
بهذا المضيف
القيمة نصف
المفتوحة الت
تكوينها، سير
جدار الحماي

خرج TCP من النافذة

حمولة TCP الإضافية بعد إرسال FIN

تجاوز إطار TCP

إعادة مع علامات غير صحيحة

مقطع TCP خارج الترتيب

سين فلوود

خطأ داخلي - فشل خليط التحقق من Synflood

إسقاط بانقطاع التيار الكهربائي في Synflood

تجاوز حد جلسات العمل نصف المفتوحة

عدد كبير جدا من PKT لكل تدفق

حزم أخطاء ICMP كثيرة جدا لكل تدفق

إلغاء توقع حمولة TCP من RSP إلى Init

خطأ داخلي - إتجاه غير معرف

SYN داخل النافذة الحالية

RST داخل النافذة الحالية

مقطع شفاف

خطأ ICMP داخلي - معلومات ICMP NAT مفقودة

حزمة ICMP في حالة إغلاق SCB

رأس IP غير موجود في حزمة ICMP

خطأ ICMP لا IP أو ICMP

ICMP ERR PKT قصير جدا

تجاوز خطأ ICMP حد الاندفاع

خطأ ICMP الذي يتعذر الوصول إليه	الاندفاع البا تجاوز خطأ PKT الذي الوصول إليه يسمح فقط الحزمة [1] الت يتعذر الوصو إليها.
خطأ ICMP غير صالح Seq#	لا يتطابق q للحزمة المص مع seq# ال التي تنشأ خ ICMP.
ICMP ERR غير صحيح	ACK غير ص في الحزمة المضمنة لخ ICMP.
إسقاط إجراء ICMP	يتم إسقاط ICMP الذي تكوينه.
زوج مناطق بدون خريطة سياسة	السياسة غي موجودة عل المناطق. ق ذلك بسبب ع تكوين ALG (عبارة طبقة التطبيق) لفت الصنوبر لقنا بيانات التطبي أن ALG لم ثقب الصنوبر بشكل صحي بسبب عدم ثقب الصنوبر مشاكل في التوسعة.
فشل جلسة العمل وعدم وجود النهج	فشل البحث جلسة العمل يوجد نهج لل من هذه الح
خطأ ICMP والنهج غير موجودين	خطأ ICMP عدم تكوين نهج على زو المناطق.
فشل التصنيف	فشل التصني زوج منطقة عندما يحاول الحماية تحد إذا كان البرو قابلا للفحص
إسقاط إجراء التصنيف	تم إسقاط إ التصنيف.
تكوين نهج الأمان غير صحيح	فشل التصني

بسبب عدم
نهج الأمان ب
صحيح. قد ي
هذا أيضا إلى
وجود عنوان
بيانات L7.
إرسال RST
المستجيب ف
حالة مزامنة
لا يساوي #
IS+1.
إجراء السيا
هو الإسقاط
قم بإسقاط
الأجزاء المت
عند إسقاط
الأول.
يتم إسقاط
السياسة الخ
بحزمة CMP
المضمنة.
(L7 (ALG
إسقاط الحز
يمكن العثور
السبب من
إحصائيات G
المختلفة.
الحزمة المق
المستلمة عن
تلتزم ALG
تم إستلام ال
المجزأة (أو
عندما لا تلتز
ALG بذلك.
نوع بروتوكو
معروف.

إرسال RST إلى المستجيب

إسقاط سياسة جدار الحماية

قطرة الشظية

إسقاط سياسة جدار الحماية ل ICMP

ترجع عملية تفتيش L7 DROP

PKT مقطع L7 غير مسموح به

PKT لجزء L7 غير مسموح به

نوع بروتو L7 غير معروف

أستكشاف أخطاء عمليات إسقاط جدار الحماية وإصلاحها

بمجرد تحديد سبب الإسقاط من عدادات إسقاط ميزة جدار الحماية أو العامة أعلاه، قد تكون هناك حاجة إلى خطوات إضافية لاستكشاف الأخطاء وإصلاحها إذا كانت عمليات الإسقاط هذه غير متوقعة. بعيدا عن التحقق من صحة التكوين لضمان أن التكوين صحيح لوظائف جدار الحماية الممكنة، غالبا ما يكون مطلوبا التقاط الحزم لتدفق حركة المرور المعني لمعرفة ما إذا كانت الحزم قد تم تكوينها بشكل غير صحيح أو ما إذا كانت هناك أي مشاكل في تنفيذ البروتوكول أو التطبيق.

التسجيل

تقوم وظيفة تسجيل ASR بإنشاء syslog لتسجيل الحزم التي تم إسقاطها. توفر هذه syslog المزيد من التفاصيل حول سبب إسقاط الحزمة. هناك نوعان من sysloggings:

1. التخزين المؤقت المحلي للsysloing

2. التسجيل عن بعد عالي السرعة

التخزين المؤقت المحلي للsysloing

لعزل سبب عمليات الإسقاط، يمكنك إستخدام أستكشاف أخطاء ZBFW وإصلاحها، مثل تمكين عمليات إسقاط السجل. هناك طريقتان لتكوين تسجيل إسقاط الحزم.

الطريقة 1: إستخدام خريطة المعلمة العامة inspection-global لتسجيل جميع الحزم التي تم إسقاطها.

```
parameter-map type inspect-global     log dropped-packets
```

الطريقة 2: أستخدم خريطة معلمة الفحص المخصص لتسجيل الحزم التي تم إسقاطها لفئة محددة فقط.

```
parameter-map type inspect LOG_PARAM
                log dropped-packets
                                  !
policy-map type inspect ZBFW_PMAP
     class type inspect ZBFW_CMAP
                inspect LOG_PARAM
```

يتم إرسال هذه الرسائل إلى السجل أو وحدة التحكم بناء على كيفية تكوين ASR للتسجيل. هنا مثال على رسالة سجل إسقاط.

```
Apr  8 13:20:39.075: %IOSXE-6-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:103*
TS:00000605668054540031 %FW-6-DROP_PKT: Dropping tcp pkt from GigabitEthernet0/0/2
(target:class)-(INSIDE_OUTSIDE_ZP:class-default)14.36.1.206:23 <= 14.38.112.250:41433
,due to Policy drop:classify result with ip ident 11579 tcp flag 0x2, seq 2014580963
                                                                            ack 0
```

قيود التخزين المؤقت المحلي ل Sysloing

1. هذه السجلات محدودة المعدل طبقا لمعرف تصحيح الأخطاء من Cisco CSCud09943.

2. قد لا تتم طباعة هذه السجلات ما لم يتم تطبيق تكوين محدد. على سبيل المثال، لن يتم تسجيل الحزم التي يتم إسقاطها حسب الحزم الافتراضية للفئة ما لم يتم تحديد الكلمة الأساسية **log**:

```
policy-map type inspect ZBFW_PMAP
                class class-default
                          drop log
```

التسجيل عن بعد عالي السرعة

يقوم التسجيل عالي السرعة (HSL) بإنشاء syslog مباشرة من QFP وإرسالها إلى مجمع NetFlow HSL الذي تم تكوينه. هذا هو حل التسجيل الموصى به ل ZBFW على ASR.

ل HSL، أستخدم هذا تشكيل:

```
parameter-map type inspect inspect-global
          log template timeout-rate 1
```

```
log flow-export v9 udp destination 1.1.1.1 5555
```

لاستخدام هذا التكوين، يلزم مجمع NetFlow قادر على الإصدار 9 من NetFlow. وهذا مفصل في

[دليل التكوين: جدار حماية السياسات القائم على المناطق، التسجيل عالي السرعة لجدار الحماية Cisco IOS XE Release 3S (ASR 1000) Firewall]

تتبع الحزمة باستخدام المطابقة الشرطية

قم بتشغيل تصحيح الأخطاء الشرطي لتمكين تتبع الحزمة ثم قم بتمكين تتبع الحزمة لهذه الميزات:

```
ip access-list extended CONDITIONAL_ACL
permit ip host 10.1.1.1 host 192.168.1.1
permit ip host 192.168.1.1 host 10.1.1.1
!
debug platform condition feature fw dataplane submode all level info
debug platform condition ipv4 access-list CONDITIONAL_ACL both
```

ملاحظة: يمكن أن يستخدم شرط التطابق عنوان IP مباشرة، لأن قائمة التحكم في الوصول (ACL) ليست ضرورية. هذا سيطابق كمصدر أو غاية الذي يسمح للتتبع ثنائي الإتجاه. يمكن إستخدام هذه الطريقة إذا لم يتم السماح لك بتغيير التكوين. على سبيل المثال: debug platform condition ipV4 address 192.168.1.1/32.

تشغيل ميزة تتبع الحزم:

```
debug platform packet-trace copy packet both
debug platform packet-trace packet 16
debug platform packet-trace drop
debug platform packet-trace enable
```

هناك طريقتان لاستخدام هذه الميزة:

1. أدخل الأمر **debug platform packet-trace drop** لتتبع الحزم التي تم إسقاطها فقط.

2. سيؤدي إستبعاد الأمر **debug platform packet-trace drop** إلى تعقب أي حزمة تطابق الشرط، والتي تتضمن الحزم التي يتم فحصها/تمريرها بواسطة الجهاز.

تشغيل تصحيح الأخطاء الشرطي:

```
debug platform condition start
```

قم بتشغيل الاختبار، ثم قم بإيقاف تشغيل تصحيح الأخطاء:

```
debug platform condition stop
```

الآن يمكن عرض المعلومات على الشاشة. في هذا المثال، تم إسقاط حزم ICMP بسبب سياسة جدار الحماية:

```
Router#show platform packet-trace statistics
Packets Summary
    Matched  2
    Traced   2
Packets Received
    Ingress  2
    Inject   0
```

```
                                                  Packets Processed
                                                        Forward  0
                                                        Punt     0
                                                        Drop     2
                                              Count       Code  Cause
                                    FirewallPolicy   183           2
                                                        Consume  0



                                        Router#show platform packet-trace summary
                          Pkt   Input           Output          State  Reason
(Gi0/0/2          Gi0/0/0          DROP   183 (FirewallPolicy     0
(Gi0/0/2          Gi0/0/0          DROP   183 (FirewallPolicy     1



                                      Router#show platform packet-trace packet 0
                                               Packet: 0           CBUG ID: 2980
                                                                       Summary
                                               Input     : GigabitEthernet0/0/2
                                               Output    : GigabitEthernet0/0/0
                                          (State     : DROP 183 (FirewallPolicy
                                                                     Timestamp
  (Start   : 1207843476722162 ns (04/15/2014 12:37:01.103864 UTC
  (Stop    : 1207843477247782 ns (04/15/2014 12:37:01.104390 UTC
                                                                     Path Trace
                                                           Feature: IPV4
                                                  Source      : 10.1.1.1
                                               Destination : 192.168.1.1
                                                  (Protocol    : 1 (ICMP
                                                           Feature: ZBFW
                                                        Action  : Drop
                                     Reason  : ICMP policy drop:classify result
                                            Zone-pair name  : INSIDE_OUTSIDE_ZP
                                                Class-map name  : class-default
                                                           Packet Copy In
  c89c1d51 5702000c 29f9d528 08004500 00540000 40004001 ac640e26 70fa0e24
  172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415 01010800
                                                         Packet Copy Out
  c89c1d51 5702000c 29f9d528 08004500 00540000 40003f01 ad640e26 70fa0e24
  172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415 01010800
```

يفك **أمر num> packet-trace platform show>>**فك ترميز معلومات ومحتويات رأس الحزمة. تم إدخال هذه الميزة في XE3.11:

```
                                    Router#show platform packet-trace packet all decode
                                               Packet: 0           CBUG ID: 2980
                                                                       Summary
                                               Input     : GigabitEthernet0/0/2
                                               Output    : GigabitEthernet0/0/0
                                          (State     : DROP 183 (FirewallPolicy
                                                                     Timestamp
  (Start   : 1207843476722162 ns (04/15/2014 12:37:01.103864 UTC
  (Stop    : 1207843477247782 ns (04/15/2014 12:37:01.104390 UTC
                                                                     Path Trace
                                                           Feature: IPV4
                                                  Source      : 10.1.1.1
                                               Destination : 192.168.1.1
                                                  (Protocol    : 1 (ICMP
                                                           Feature: ZBFW
                                                        Action  : Drop
```

```
                                        Reason   : ICMP policy drop:classify result
                                               Zone-pair name  : INSIDE_OUTSIDE_ZP
                                                   Class-map name  : class-default
                                                                          Packet Copy In
c89c1d51 5702000c 29f9d528 08004500 00540000 40004001 ac640e26 70fa0e24
172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415 01010800
                                                                              ARPA
                                             Destination MAC     : c89c.1d51.5702
                                             Source MAC          : 000c.29f9.d528
                                               (Type               : 0x0800 (IPV4
                                                                          IPv4
                                                        Version            : 4
                                                        Header Length      : 5
                                                     ToS                : 0x00
                                                       Total Length       : 84
                                                   Identifier         : 0x0000
                                          (IP Flags           : 0x2 (Don't fragment
                                                        Frag Offset        : 0
                                                       TTL                : 64
                                                  (Protocol           : 1 (ICMP
                                                    Header Checksum    : 0xac64
                                                  Source Address     : 10.1.1.1
                                               Destination Address : 192.168.1.1
                                                                              ICMP
                                                  (Type               : 8 (Echo
                                               (Code               : 0 (No Code
                                                    Checksum           : 0x172a
                                                    Identifier         : 0x2741
                                                    Sequence           : 0x0001
                                                                       Packet Copy Out
c89c1d51 5702000c 29f9d528 08004500 00540000 40003f01 ad640e26 70fa0e24
172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415 01010800
                                                                              ARPA
                                           Destination MAC     : c89c.1d51.5702
                                           Source MAC          : 000c.29f9.d528
                                            (Type               : 0x0800 (IPV4
                                                                          IPv4
                                                        Version            : 4
                                                        Header Length      : 5
                                                     ToS                : 0x00
                                                       Total Length       : 84
                                                   Identifier         : 0x0000
                                          (IP Flags           : 0x2 (Don't fragment
                                                        Frag Offset        : 0
                                                       TTL                : 63
                                                  (Protocol           : 1 (ICMP
                                                    Header Checksum    : 0xad64
                                                  Source Address     : 10.1.1.1
                                               Destination Address : 192.168.1.1
                                                                              ICMP
                                                  (Type               : 8 (Echo
                                               (Code               : 0 (No Code
                                                    Checksum           : 0x172a
                                                    Identifier         : 0x2741
                                                    Sequence           : 0x0001
```

التقاط حزمة مضمنة

تمت إضافة دعم التقاط الحزمة المضمنة في Cisco IOS-XE 3.7 (15.2(4)S). لمزيد من التفاصيل، راجع

التقاط الحزم المضمن لمثال تكوين Cisco IOS و IOS-XE.

تصحيح الأخطاء

تصحيح الأخطاء الشرطي

في XE3.10، سيتم تقديم تصحيح الأخطاء المشروط. يمكن إستخدام العبارات الشرطية لضمان أن ميزة ZBFW تسجل رسائل تصحيح الأخطاء ذات الصلة بالشرط فقط. تستخدم الأخطاء الشرطية قوائم التحكم في الوصول لتقييد السجلات التي تطابق عناصر قائمة التحكم في الوصول. أيضا، قبل XE3.10، ال debug رسالة كان من الصعب أن يقرأ. تم تحسين إخراج تصحيح الأخطاء في XE3.10 لتسهيل فهمهم.

لتمكين تصحيح الأخطاء هذا، قم بإصدار هذا الأمر:

```
[debug platform condition feature fw dataplane submode [detail | policy | layer4 | drop
debug platform condition ipv4 access-list <ACL_name> both
debug platform condition start
```

لاحظ أنه يجب تعيين الأمر الشرط عبر قائمة التحكم في الوصول (ACL) والاتجاه. لن يتم تنفيذ تصحيح الأخطاء الشرطي حتى يتم بدء تشغيلها باستخدام الأمر **debug platform condition start**. لإيقاف تشغيل تصحيح الأخطاء الشرطي، أستخدم الأمر **debug platform condition stop**.

```
debug platform condition stop
```

لإيقاف تشغيل تصحيح الأخطاء الشرطي، **لا** تستخدم الأمر **undebug all**. لإيقاف تشغيل كل تصحيح الأخطاء الشرطي، أستخدم الأمر:

```
ASR#clear platform condition all
```

قبل XE3.14، لا تكون عمليات تصحيح أخطاء **ha** و**الحدث** مشروطة. ونتيجة لذلك، تتسبب ميزة **تصحيح أخطاء النظام الأساسي للوضع الفرعي لمستوى البيانات** في إنشاء جميع السجلات، بشكل مستقل عن الشرط المحدد أدناه. قد يؤدي ذلك إلى حدوث ضوضاء إضافية تجعل تصحيح الأخطاء أمرا صعبا.

بشكل افتراضي، يكون مستوى التسجيل المشروط هو **معلومات**. لزيادة/تقليل مستوى التسجيل، أستخدم الأمر:

```
[debug platform condition feature fw dataplane submode all [verbose | warning
```

تجميع وعرض التصحيح

لن تتم طباعة ملفات تصحيح الأخطاء إلى وحدة التحكم أو الشاشة. تتم كتابة جميع تصحيح الأخطاء إلى القرص الثابت ل ASR. تتم كتابة عمليات تصحيح الأخطاء إلى القرص الثابت تحت **عمليات** تتبع **المجلدات** باستخدام الاسم **<cpp_cp_f0-0.log.<date**. لعرض الملف الذي تتم كتابة تصحيح الأخطاء فيه، أستخدم الإخراج:

```
:ASR# cd harddisk
ASR# cd tracelogs
*ASR# dir cpp_cp_F0*Directory of harddisk:/tracelogs/cpp_cp_F0

/Directory of harddisk:/tracelogs

rwx 1048795 Jun 15 2010 06:31:51 +00:00- 3751962
cpp_cp_F0-0.log.5375.20100615063151
rwx 1048887 Jun 15 2010 02:18:07 +00:00- 3751967
cpp_cp_F0-0.log.5375.20100615021807
(bytes total (30680653824 bytes free 39313059840
```

سيتم تخزين كل ملف تصحيح أخطاء **كملف** <CPP_cp_F0-0.log.<date>. هذه ملفات نص عادية يمكن نسخها من ASR باستخدام TFTP. الحد الأقصى لملف السجل على ASR هو 1 ميجابايت. بعد 1 ميغابايت، تتم كتابة الأخطاء إلى ملف سجل جديد. هذا هو السبب في أن كل ملف سجل مختوم بختم زمني للإشارة إلى بداية الملف.

قد توجد ملفات السجل في هذه المواقع:

```
/harddisk:/tracelogs
/bootflash:/tracelogs
```

بما أن ملفات التدوين يتم عرضها فقط بعد تدويرها، فإن ملف التدوين يمكن تدويره يدويا باستخدام هذا الأمر:

```
ASR# test platform software trace slot f0 cpp-control-process rotate
```

يقوم هذا الإجراء بإنشاء ملف سجل "cpp_cp" على الفور ويبدأ تشغيل ملف جديد على QFP. على سبيل المثال:

```
ASR#test platform software trace slot f0 cpp-control-process rotate
,Rotated file from: /tmp/fp/trace/stage/cpp_cp_F0-0.log.7311.20140408134406
Bytes: 82407, Messages: 431

ASR#more tracelogs/cpp_cp_F0-0.log.7311.20140408134406
btrace continued for process ID 7311 with 159 modules : 10:22:54.462 04/02
cpp-dp-fw]: (info): QFP:0.0 Thread:110 TS:00000531990811543397] 16:52:41.164 04/07
FW_DEBUG_FLG_HA:[]: HA[1]: Changing HA state to 9:
cpp-dp-fw]: (info): QFP:0.0 Thread:120 TS:00000532153153672298] 16:55:23.503 04/07
FW_DEBUG_FLG_HA:[]: HA[1]: Changing HA state to 10:
(buginf]: (debug): [system] Svr HA bulk sync CPP(0) complex(0] 16:55:23.617 04/07
(epoch(0) trans_id(26214421) rg_num(1
```

يتيح هذا الأمر دمج ملفات تصحيح الأخطاء في ملف واحد لتسهيل المعالجة. فهو يدمج جميع الملفات في الدليل ويربطها حسب الوقت. يمكن أن يساعد ذلك عندما تكون السجلات سريعة جدا ويتم إنشاؤها عبر ملفات متعددة:

```
ASR#request platform software trace slot rp active merge target bootflash:MERGED_OUTPUT.log
[Creating the merged trace file: [bootflash:MERGED_OUTPUT.log
including all messages

[Done with creation of the merged trace file: [bootflash:MERGED_OUTPUT.log
```

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).