فهم سلوك تجاوز فشل ASA/FTD مع واجهات SR IOV

المحتويات

المقدمة

يوضح هذا المستند كيفية عمل جدار الحماية الآمن من Cisco في حالة التوفر العالي عندما يكون لديهم واجهات SR IOV.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- أجهزة الأمان الظاهرية المعدلة (ASAv).
- برنامج الدفاع الظاهري ضد تهديد Firepower (FTDv).
- تجاوز الأعطال / التوفر الفائق (HA).
- واجهة محاكاة افتراضية أحادية الجذر للإدخال/الإخراج (SR-IOV).

معلومات أساسية.

عناوين IP وعناوين MAC النشطة/الاحتياطية.

بالنسبة للتوفر النشط/الاحتياطي، يكون سلوك إستخدام عناوين IP وعناوين MAC في حدث تجاوز الفشل كما يلي:

1. تستخدم الوحدة النشطة دائما عنوان IP الأساسي وعنوان MAC.

2. عند فشل الوحدة النشطة، تفترض الوحدة الاحتياطية عناوين IP وعناوين MAC للوحدة الفاشلة وتبدأ في تمرير حركة مرور البيانات.

واجهات SR-IOV.

تتيح تقنية SR-IOV لحركة مرور الشبكة تجاوز طبقة محول البرامج في مكدس المحاكاة الظاهرية Hyper-V.

نظرا لأنه قد تم تعيين الوظيفة الظاهرية (VF) إلى قسم تابع، فإن حركة مرور الشبكة تتدفق مباشرة بين VF والتقسيم التابع.

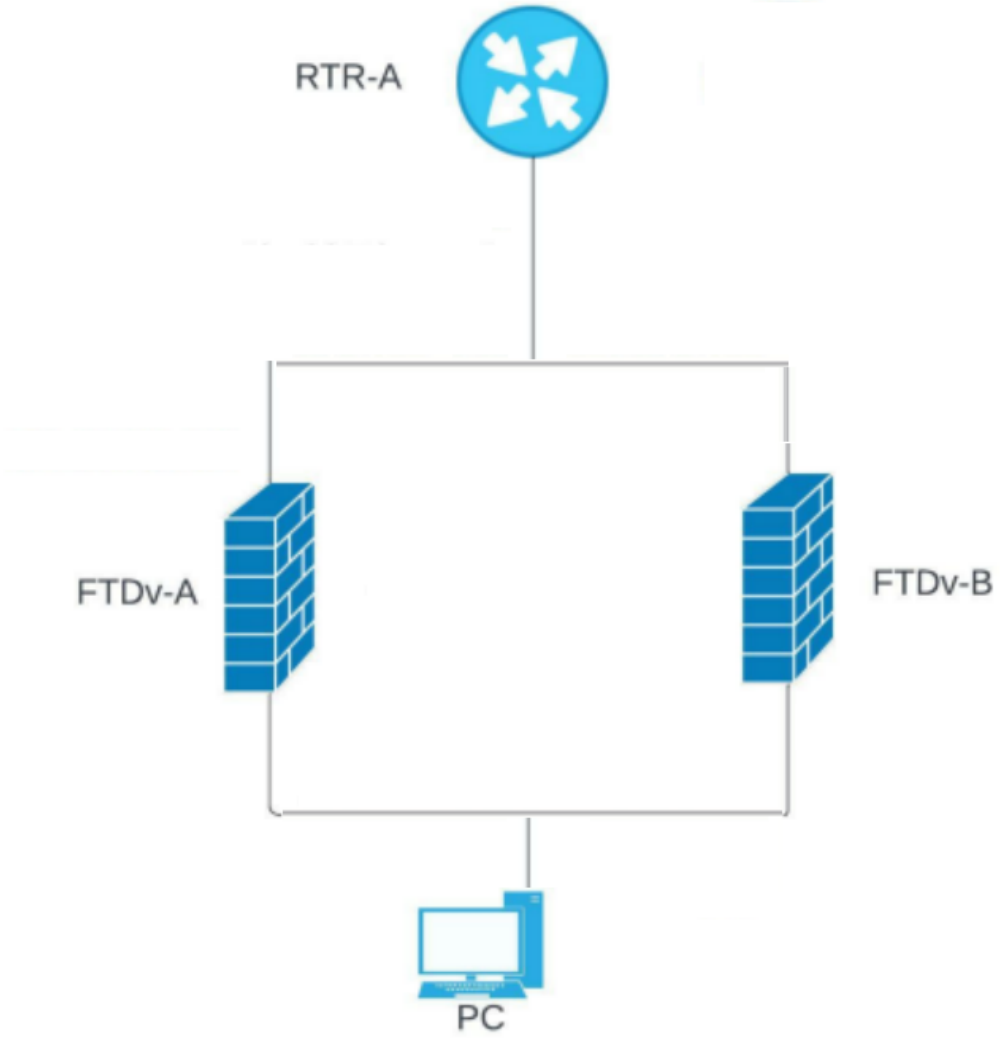
وتتيجة لذلك، تم تقليل مصروفات عمليات الإدخال/الإخراج في طبقة محاكاة البرامج مما يحقق أداء الشبكة الذي يكاد يكون مماثلا للأداء في البيئات غير الافتراضية.

كن على علم بقيود SRIOV حيث لا يسمح للضيف VM بتعيين عنوان MAC على VF.

ولهذا السبب، لا يتم نقل عنوان MAC أثناء HA كما هو الحال على منصات ASA الأخرى ومع أنواع الواجهة الأخرى.

يعمل تجاوز الفشل HA عن طريق نقل عنوان IP من نشط إلى وضع الاستعداد.

الرسم التخطيطي للشبكة



الصورة 1. مثال على الرسم التخطيطي.

استكشاف الأخطاء وإصلاحها

عناوين IP وعناوين MAC النشطة/الاحتياطية باستخدام واجهات SR-IOV.

في إعداد زواج الفشل، عند فشل FTDv/ASAv (الوحدة الأساسية) المقترنة، تتولى وحدة FTDv/ASAv الاحتياطية دور الوحدة الأساسية، ويتم تحديث عنوان IP الخاص بواجهة الوحدة ولكن يتم الاحتفاظ بعنوان MAC الخاص بوحدة ASAv الاحتياطية.

بعد ذلك، يرسل ASAv تحديث بروتوكول تحليل العنوان (ARP) مجاني للإعلان عن التغيير في عنوان MAC الخاص بعنوان IP للواجهة إلى أجهزة أخرى على الشبكة نفسها.

ومع ذلك، بسبب عدم التوافق مع هذه الأنواع من الواجهات، لا يتم إرسال تحديث ARP المجاني إلى عنوان IP العالمي الذي يتم تعريفه في عبارات NAT أو PAT لترجمة عنوان IP للواجهة إلى عناوين IP العالمية.

عندما يكون هناك FTDv في HA وهناك حركة مرور تتم ترجمتها إلى عنوان IP من أحد واجهات بيانات FTDv (وفي الوقت نفسه)، فإن واجهة البيانات هي واجهة SRIOV يعمل كل شيء بشكل جيد حتى يكون هناك حدث زواج الفشل.

لا يرسل جهاز FTD ARPs مجاني للاتصالات المترجمة عندما يأخذ هو العنوان الرئيسي، لذلك لا يتم تحديث بتحديث عنوان MAC لتلك الاتصالات المترجمة ويفشل حركة المرور.

خفض المرتبة

توضح هذه المخرجات كيفية عمل زواج فشل FTDv/ASAv.

في هذا المثال، يمثل FTD-B الوحدة النشطة ولديه 172.16.100.4 عنوان IP و 5254.0094.9af4 عنوان MAC.

<#root>

```
FTD-B# show failover state



State          Last Failure          Reason Date/Time

This host - Secondary


Active None


Other host - Primary
Standby Ready None
```

<#root>

```
FTD-B# show interface outside
Interface TenGigabitEthernet0/0 "Outside", is up, line protocol is up
Hardware is net_ixgbe_vf, BW 1000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
```

```
Input flow control is unsupported, output flow control is unsupported
MAC address
```

5254.0094.9af4

```
, MTU 1500
IP address
```

172.16.100.4

```
, subnet mask 255.255.255.0
1650789 packets input, 218488071 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
1669933 packets output, 160282355 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (0/0)
output queue (blocks free curr/low): hardware (0/0)
Traffic Statistics for "Outside":
1650772 packets input, 195376243 bytes
1669933 packets output, 136903293 bytes
411 packets dropped
1 minute input rate 2 pkts/sec, 184 bytes/sec
1 minute output rate 2 pkts/sec, 184 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 2 pkts/sec, 184 bytes/sec
5 minute output rate 2 pkts/sec, 184 bytes/sec
5 minute drop rate, 0 pkts/sec
```

وعلى الجانب الآخر، فإن FTD-A هو الوحدة الاحتياطية وهو يحتوي على 172.16.100.5 عنوان IP و 5254.0014.5a27 عنوان MAC.

<#root>

FTD-A#

show failover state

```
State Last Failure Reason Date/Time
```

This host - Primary

Standby Ready None

```
Other host - Secondary
Active None
```

<#root>

```
FTD-A# show interface Outside
Interface TenGigabitEthernet0/0 "Outside", is up, line protocol is up
Hardware is net_ixgbe_vf, BW 1000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address
```

5254.0014.5a27

```
, MTU 1500
IP address
```

172.16.100.5

```
, subnet mask 255.255.255.0
318275 packets input, 58152922 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
279428 packets output, 24490471 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (0/0)
output queue (blocks free curr/low): hardware (0/0)
Traffic Statistics for "Outside":
318265 packets input, 53696574 bytes
279428 packets output, 20578479 bytes
31221 packets dropped
1 minute input rate 0 pkts/sec, 13 bytes/sec
1 minute output rate 0 pkts/sec, 13 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 13 bytes/sec
5 minute output rate 0 pkts/sec, 13 bytes/sec
5 minute drop rate, 0 pkts/sec
```

فيما يلي ما يبدو عليه جدول ARP على جانب الموجه:

<#root>

```
RTR-A#show ip arp GigabitEthernet 2
Protocol Address Age (min) Hardware Addr Type Interface
Internet
```

172.16.100.4 112 5254.0094.9af4

```
 ARPA GigabitEthernet2
Internet
```

172.16.100.5 112 5254.0014.5a27

```
 ARPA GigabitEthernet2
Internet 172.16.100.10 251 5254.0094.9af4 ARPA GigabitEthernet2
Internet 172.16.100.11 193 5254.0094.9af4 ARPA GigabitEthernet2
Internet 172.16.100.1 - 0000.0c07.ac01 ARPA GigabitEthernet2
```

بعد تجاوز الفشل.

```
FTD-A# Building configuration...
Cryptochecksum: 6bde1149 8d2fc26f 2c7c6bb4 636401b3

5757 bytes copied in 0.60 secs
[OK]

Switching to Active
```

يتغير IP ولكن MAC وه نفسه.

<#root>

FTD-A# show interface Outside

```
Interface TenGigabitEthernet0/0 "Outside", is up, line protocol is up
Hardware is net_ixgbe_vf, BW 1000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address
```

5254.0014.5a27,

```
 MTU 1500
IP address
```

172.16.100.4

```
, subnet mask 255.255.255.0
318523 packets input, 58175566 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
279675 packets output, 24513001 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (0/0)
output queue (blocks free curr/low): hardware (0/0)
Traffic Statistics for "Outside":
318510 packets input, 53715608 bytes
279675 packets output, 20597551 bytes
31221 packets dropped
1 minute input rate 0 pkts/sec, 52 bytes/sec
1 minute output rate 0 pkts/sec, 54 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 13 bytes/sec
5 minute output rate 0 pkts/sec, 13 bytes/sec
5 minute drop rate, 0 pkts/sec
```

هنا يمكننا أن نرى كيف أن الموجه يحدث إدخالات ARP ولكنه لا يحدث نفسه للمضيفين الذين وراء FTD HA الذي يؤدي إلى انقطاع.

<#root>

```
RTR-A#show ip arp GigabitEthernet 2
Protocol Address Age (min) Hardware Addr Type Interface
Internet

172.16.100.4 0 5254.0014.5a27

 ARPA GigabitEthernet2
Internet

172.16.100.5 0 5254.0094.9af4

 ARPA GigabitEthernet2
Internet

172.16.100.10 252 5254.0094.9af4

 ARPA GigabitEthernet2
Internet

172.16.100.11 195 5254.0094.9af4

 ARPA GigabitEthernet2
Internet 172.16.100.1 - 0000.0c07.ac01 ARPA GigabitEthernet2
```

أثناء التحويل، يرسل ASA لا الواجهة المتصلة، GARP باستخدام MAC/IP الجديد، حتى يقوم المحول و/أو موجه العبارة بتحديثه. غير أنه لا يوجد GARP لعنوان IP الذي تمت ترجمته، وبالتالي تستمر الحزمة العائدة من الموجه في إعادة التوجيه باستخدام عنوان MAC الذي هو في وضع الاستعداد الآن ولكن عنوان IP يشير إلى ASA نشط.

لذلك نحن بحاجة إلى GARP لعنوان IP المترجم إلى NAT.

الحل

لتجنب انقطاع التيار الكهربائي، يلزمك الاحتفاظ بـ IP الذي تمت ترجمته ليس في واجهة الشبكة الفرعية ولديها مسار من البوابة ويجب أن تعمل الأشياء دون مشاكل. في هذا المثال، يجب أن يكون عنوان IP المترجم من نطاق الشبكة الفرعية 172.16.100.0/24.

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems
- إمداد واجهة ASAv و SR-IOV
- عناوين MAC وعناوين IP في تجاوز الفشل
- دليل بدء تشغيل أجهزة الأمان الظاهرية المعدلة (ASAv) من Cisco، الإصدار 9.8

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).