了解使用SR IOV接口的ASA/FTD故障切换行为

目录

简介

本文档介绍高可用性思科安全防火墙在具有SR IOV接口时如何工作。

先决条件

要求

Cisco 建议您了解以下主题：

- 自适应安全设备虚拟(ASAv)。
- Firepower威胁防御虚拟(FTDv)。
- 故障转移/高可用性(HA)。
- 单个根I/O虚拟化(SR-IOV)接口。

背景信息.

主用/备用IP地址和MAC地址。

对于主用/备用高可用性，故障切换事件中的IP地址和MAC地址使用行为如下：

1. 主用设备始终使用主IP地址和MAC地址。
2. 当主用设备发生故障转移时，备用设备会接管故障设备的IP地址和MAC地址，并开始传输流量。

SR-IOV接口。

SR-IOV允许网络流量绕过Hyper-V虚拟化堆栈的软件交换机层。

由于虚拟功能(VF)分配给子分区，因此网络流量直接在VF和子分区之间流动。

因此，软件仿真层中的I/O开销会降低，并且网络性能几乎与非虚拟化环境中的性能相同。

请注意SRIOV限制，其中不允许访客VM在VF上设置MAC地址。

因此，MAC地址在HA期间不会像在其他ASA平台上使用其他接口类型时那样进行传输。

HA故障切换的工作方式是，将IP地址从主用设备传输到备用设备。

网络图

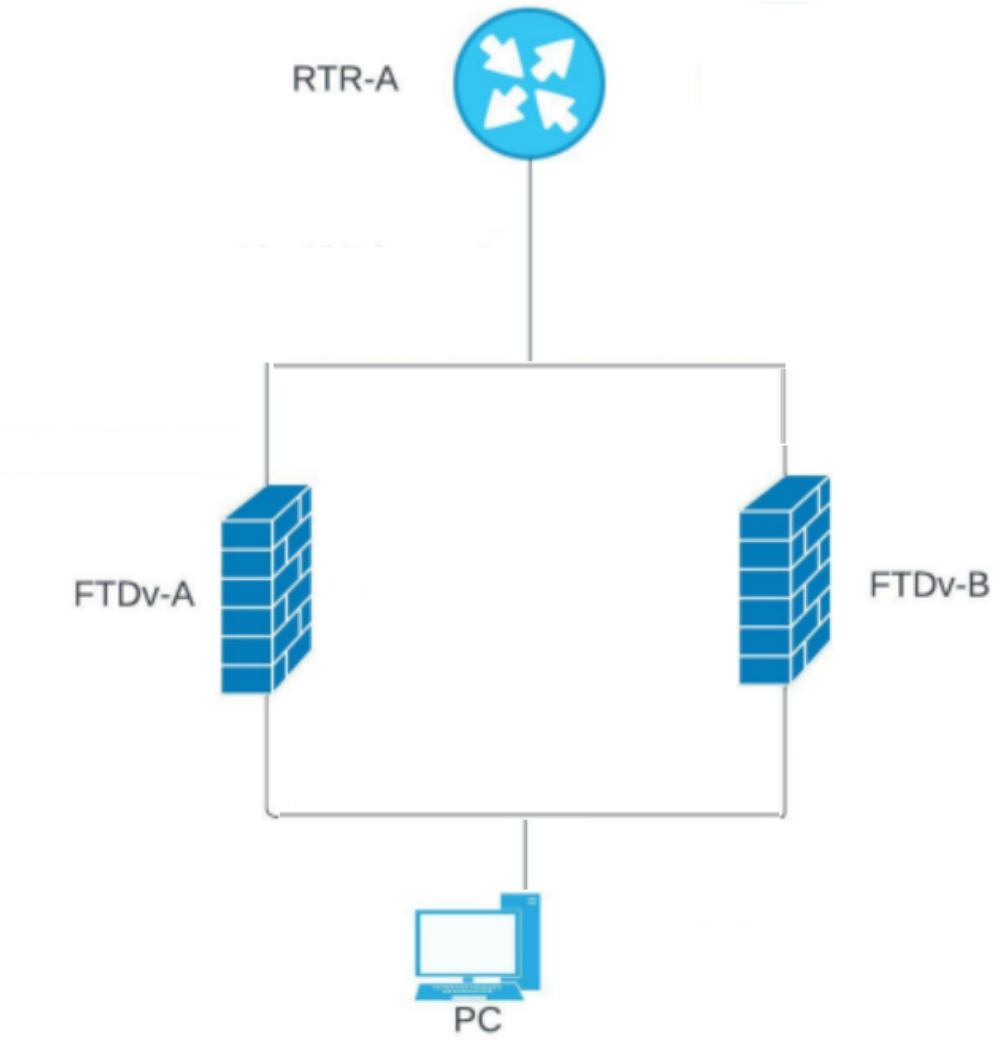

图1.图示例。

故障排除

主用/备用IP地址和SR-IOV接口的MAC地址。

在故障切换设置中，当配对FTDv/ASAv（主设备）发生故障时，备用FTDv/ASAv设备将接管主设备角色，并且其接口IP地址会更新，但会保留备用ASAv设备的MAC地址。

然后，ASAv发送无故地址解析协议(ARP)更新，将接口IP地址的MAC地址更改通告给同一网络上的其他设备。

但是，由于与这些类型的接口不兼容，无偿ARP更新不会发送到NAT或PAT语句中定义的全局IP地

址，以便将接口IP地址转换为全局IP地址。

当HA中存在FTDv并且有流量被转换为某个FTDv数据接口的IP地址（同时）时，数据接口为SRIOV接口，在出现故障转移事件之前，一切正常。

当FTD设备获取主IP地址时，它不会为转换的连接发送免费ARP，因此连接的路由器不会更新这些转换的连接的MAC地址，流量会失败。

演示

以下输出显示了FTDv/ASAv故障切换的工作原理。

在本示例中，FTD-B是主用设备，它有172.16.100.4 IP地址和5254.0094.9af4 MAC地址。

<#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
```

另一方面，FTD-A是备用设备，它有172.16.100.5 IP地址和5254.0014.5a27 MAC地址。

<#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
```

以下是ARP表在路由器端显示的内容：

<#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
```

故障切换后。

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

5757 bytes copied in 0.60 secs
[OK]

Switching to Active
```

IP发生变化，但MAC相同。

<#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
```

此处我们可以看到路由器如何更新ARP条目，但它对FTD HA后面的主机不进行相同更新，从而导致中断。

<#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
```

在切换期间，对于连接的接口，ASA使用MAC/新IP发送GARP，以便交换机和/或网关路由器对其进行更新。但是转换后的IP地址没有GARP，因此来自路由器的返回数据包继续使用现在备用的MAC地址转发，但IP地址指向活动ASA。

因此，我们需要GARP来获取NAT转换后的IP地址。

解决方案

为了避免网络中断，您需要保持已转换的IP不在子网接口中，并且我们有来自网关的路由，因此必须能够顺利工作。在本示例中，转换后的IP地址必须位于172.16.100.0/24子网范围之外。

相关信息

- 技术支持和文档 - Cisco Systems
- ASAv和SR-IOV接口调配
- 故障切换中的MAC地址和IP地址
- 思科自适应安全虚拟设备(ASAv)入门指南，9.8

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。