瞭解使用SR IOV介面的ASA/FTD故障切換行為

目錄

簡介

必要條件

需求

背景資訊.

活動/備用IP地址和MAC地址。

簡介

本檔案介紹高可用性思科安全防火牆在具有SR IOV介面時的運作方式。

必要條件

需求

思科建議您瞭解以下主題：

- 自適應安全裝置虛擬(ASAv)。
- Firepower威脅防禦虛擬(FTDv)。
- 故障轉移/高可用性(HA)。
- 單根I/O虛擬化(SR-IOV)介面。

背景資訊.

活動/備用IP地址和MAC地址。

對於主用/備用高可用性，故障切換事件中的IP地址和MAC地址使用行為如下：

1. 主用裝置始終使用主IP地址和MAC地址。
2. 當主用裝置發生故障轉移時，備用裝置會接管故障裝置的IP地址和MAC地址，並開始傳輸流量。

SR-IOV介面。

SR-IOV允許網路流量繞過Hyper-V虛擬化堆疊的軟體交換機層。

由於虛擬功能(VF)分配給子分割槽，因此網路流量直接在VF和子分割槽之間流動。

結果，軟體模擬層中的I/O開銷減少，並且實現了幾乎與非虛擬化環境相同的網路效能。

請注意SRIOV限制，其中不允許訪客VM設定VF上的MAC地址。

因此，MAC地址在HA期間不會像在其他ASA平台上使用其他介面型別傳輸時那樣傳輸。

HA故障切換通過將IP地址從主用傳輸到備用來運行。

網路圖表

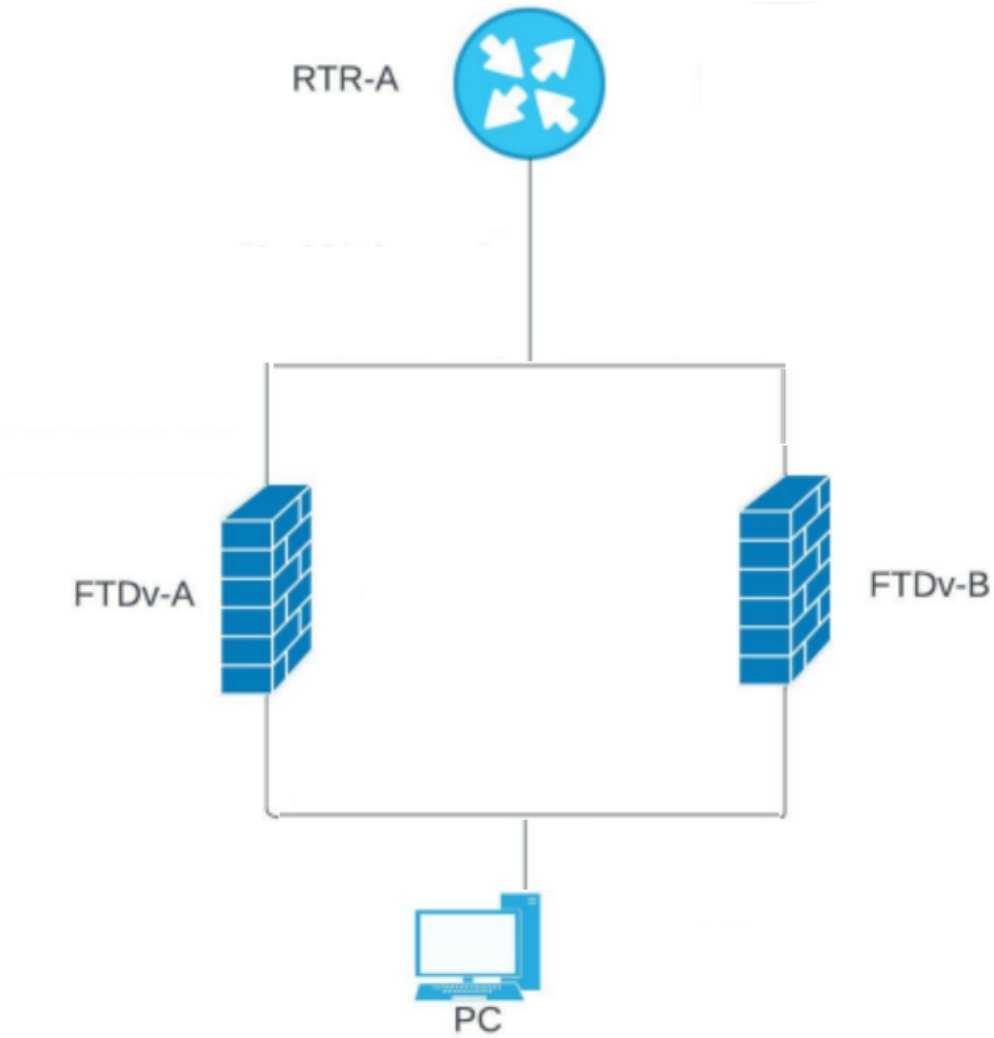

圖1.圖示示例。

疑難排解

使用SR-IOV介面的主用/備用IP地址和MAC地址。

在故障切換設定中，當配對FTDv/ASAv（主裝置）發生故障時，備用FTDv/ASAv裝置將接管主裝置角色，並且其介面IP地址會更新，但保留備用ASAv裝置的MAC地址。

此後，ASAv傳送一個免費地址解析協定(ARP)更新以向同一網路上的其他裝置通告介面IP地址的MAC地址更改。

但是，由於與這些型別的介面不相容，無償ARP更新不會傳送到在NAT或PAT語句中定義的將介面

IP地址轉換為全域性IP地址的全域性IP地址。

當HA中存在FTDv，且有流量轉譯到其中一個FTDv資料介面的IP位址時（同時），資料介面是SRIOV介面，除非發生容錯移轉事件，否則一切都會正常運作。

FTD裝置取得主IP位址時，不會為已轉換連線傳送免費ARP，因此連線的路由器不會更新這些已轉換連線的MAC位址，且流量會失敗。

示範

這些輸出顯示了FTDv/ASAv故障切換的工作原理。

在本例中，FTD-B是作用中單元，它有172.16.100.4 IP位址和5254.0094.9af4 MAC位址。

<#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是備用裝置，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表在路由器端顯示的內容：

<#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
```

故障切換之後。

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

5757 bytes copied in 0.60 secs
[OK]

Switching to Active
```

IP發生變化，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
```

此處我們可以看到路由器如何更新ARP專案，但路由器不會針對FTD HA背後的主機更新相同專案，從而導致中斷。

<#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
```

在切換期間，對於連線的介面，ASA使用MAC/新IP傳送GARP，以便交換機和/或網關路由器對其進行更新。但是轉換後的IP地址沒有GARP，因此來自路由器的返回資料包一直使用現在備用的MAC地址轉發，但IP地址指向活動ASA。

因此，我們需要GARP來獲取NAT轉換的IP地址。

解決方案

為了避免中斷，您需要保持已轉換的IP不在子網介面中，並且我們有從網關發出的路由，因此路由器必須能夠順利運行，而不會出現問題。在本例中，轉換後的IP地址必須位於172.16.100.0/24子網範圍之外。

相關資訊

- 技術支援與文件 - Cisco Systems
- ASAv和SR-IOV介面布建
- 故障切換中的MAC地址和IP地址
- 思科自適應安全虛擬裝置(ASAv)入門指南9.8

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。