Comprensión del comportamiento de conmutación por fallo de ASA/FTD con interfaces SR IOV

Contenido

Introducción

Este documento describe cómo funciona Cisco Secure Firewall en alta disponibilidad cuando tienen interfaces SR IOV.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo de seguridad virtual adaptable (ASAv).
- Firepower Thread Defense Virtual (FTDv).
- Conmutación por fallo/alta disponibilidad (HA).
- Interfaz de virtualización de E/S de raíz única (SR-IOV).

Antecedentes.

Direcciones IP y MAC activas/en espera.

Para Active/StandbyHigh Availability, el comportamiento de la dirección IP y el uso de la dirección MAC en un evento de failover es el siguiente:

1. La unidad activa siempre utiliza la dirección IP y la dirección MAC principales.

2. Cuando la unidad activa falla, la unidad standby asume las direcciones IP y las direcciones MAC de la unidad fallada y comienza a pasar el tráfico.

Interfaces SR-IOV.

SR-IOV permite que el tráfico de red omita la capa de switch de software de la pila de virtualización de Hyper-V.

Dado que la función virtual (VF) está asignada a una partición secundaria, el tráfico de red fluye directamente entre la VF y la partición secundaria.

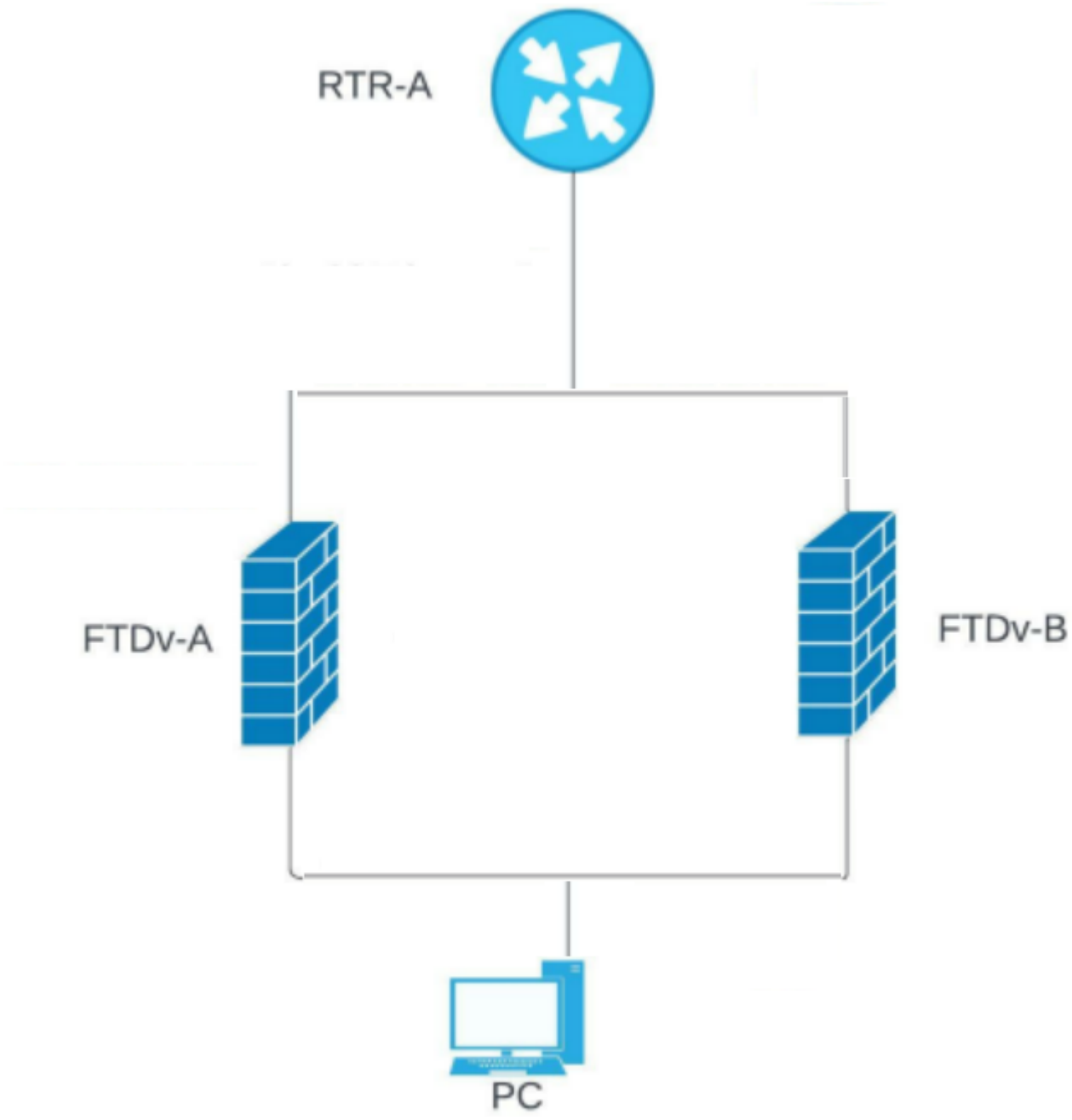
Como resultado, se reduce la sobrecarga de E/S en la capa de emulación de software y se logra un rendimiento de red que es prácticamente el mismo que en los entornos no virtualizados.

Tenga en cuenta la limitación SRIOV en la que la VM invitada no puede establecer la dirección MAC en la VF.

Debido a esto, la dirección MAC no se transfiere durante HA como se hace en otras plataformas ASA y con otros tipos de interfaz.

La conmutación por fallo de HA funciona mediante la transferencia de la dirección IP de activa a en espera.

Diagrama de la red



Troubleshoot

Direcciones IP activas/en espera y Direcciones MAC con interfaces SR-IOV.

En una configuración de failover, cuando un FTDv/ASAv (unidad primaria) emparejado falla, la unidad FTDv/ASAv standby asume como el rol de unidad primaria, y su dirección IP de la interfaz se actualiza pero mantiene la dirección MAC de la unidad ASAv standby.

Posteriormente, ASAv envía una actualización gratuita del Protocolo de resolución de direcciones (ARP) para anunciar el cambio en la dirección MAC de la dirección IP de la interfaz a otros dispositivos de la misma red.

Sin embargo, debido a la incompatibilidad con estos tipos de interfaces, la actualización ARP gratuita no se envía a la dirección IP global definida en las sentencias NAT o PAT para traducir la dirección IP de la interfaz a direcciones IP globales.

Cuando hay un FTDv en HA y hay tráfico traducido en la dirección IP de una de las interfaces de datos FTDv (y simultáneamente), la interfaz de datos es una interfaz SRIOV, todo funciona bien hasta que hay un evento de failover.

El dispositivo FTD no envía ARP gratuitos para las conexiones traducidas cuando toma la dirección IP principal, de modo que los routers conectados no actualizan la dirección MAC para esas conexiones traducidas y el tráfico falla.

Demostración

Estos resultados muestran cómo funciona el failover FTDv/ASAv.

En este ejemplo, FTD-B es la unidad activa y tiene la dirección IP 172.16.100.4 y la dirección MAC 5254.0094.9af4.

<#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
```

Por otro lado, FTD-A es la unidad en espera y tiene la dirección IP 172.16.100.5 y la dirección MAC 5254.0014.5a27.

<#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
```

Este es el aspecto de la tabla ARP en el lado del router:

<#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
```

Después del failover.

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

5757 bytes copied in 0.60 secs
[OK]

Switching to Active
```

IP cambia, pero MAC es el mismo.

<#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
```

Aquí podemos ver cómo el router actualiza las entradas ARP pero no actualiza lo mismo para los hosts detrás del FTD HA que conduce a una interrupción.

<#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
```

Durante el switchover, para la interfaz conectada, ASA envía GARP usando la MAC/nueva IP, de modo que el switch y/o el router del gateway lo actualicen. Sin embargo, no hay GARP para la dirección IP traducida y, por lo tanto, el paquete de retorno del router sigue reenviando utilizando la dirección MAC del dispositivo ahora en espera, pero la dirección IP apunta al ASA activo.

Por lo tanto, necesitamos GARP para la dirección IP traducida por NAT.

Solución

Para evitar una interrupción, debe mantener la IP traducida no en la interfaz de subred y tenemos una ruta desde el gateway. Las cosas deben funcionar sin problemas. En este ejemplo, la dirección IP traducida debe estar fuera del rango de subred 172.16.100.0/24.

Información Relacionada

- **Soporte Técnico y Documentación - Cisco Systems**
- **Aprovisionamiento de interfaz ASAv y SR-IOV**
- Direcciones MAC e IP en Failover
- **Guía de inicio de Cisco Adaptive Security Virtual Appliance (ASAv), 9.8**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).