# Entender o comportamento de failover do ASA/FTD com interfaces SR IOV

## Contents



## Introdução

Este documento descreve como o Cisco Secure Firewall em alta disponibilidade funciona quando eles têm interfaces SR IOV.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Adaptive Security Appliance Virtual (ASAv).
- Firepower Thread Defense Virtual (FTDv) (em inglês).
- Failover/alta disponibilidade (HA).
- Interface de virtualização de E/S de raiz única (SR-IOV).

## Informações de Apoio.

#### Endereços IP ativos/em standby e endereços MAC.

Para alta disponibilidade ativa/em espera, o comportamento do uso do endereço IP e do endereço MAC em um evento de failover é o seguinte:

1. A unidade ativa sempre usa o endereço IP principal e o endereço MAC.

2. Quando a unidade ativa falha, a unidade de standby assume os endereços IP e MAC da unidade que falhou e começa a passar tráfego.

#### Interfaces SR-IOV.

O SR-IOV permite que o tráfego de rede ignore a camada de switch de software da pilha de virtualização Hyper-V.

Como a Virtual Function (VF) é atribuída a uma partição filha, o tráfego de rede flui diretamente entre a VF e a partição filha.

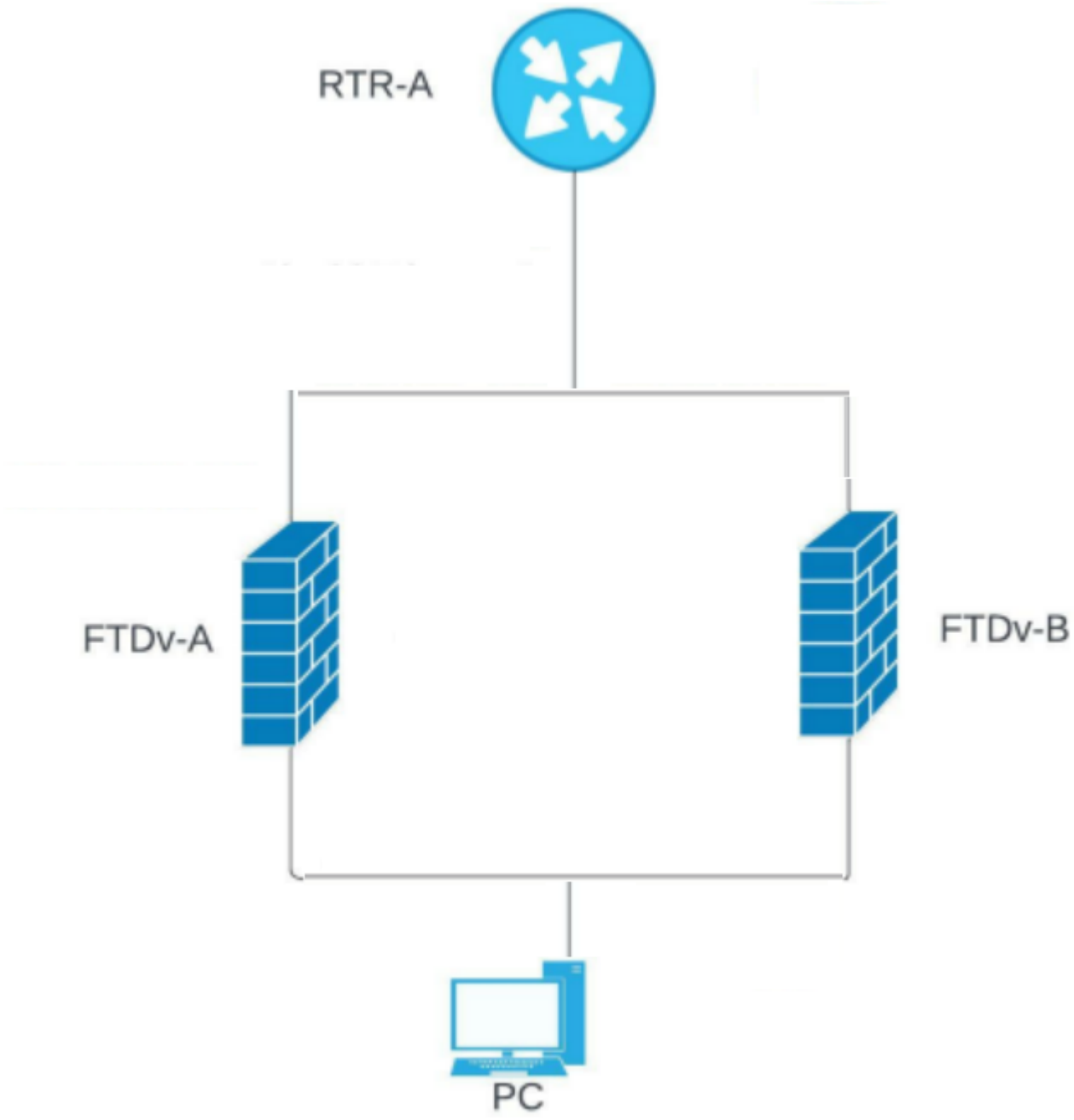
Como resultado, a sobrecarga de E/S na camada de emulação de software é reduzida e alcança um desempenho de rede que é quase o mesmo desempenho que em ambientes não virtualizados.

Esteja ciente da limitação do SRIOV em que a VM convidada não pode definir o endereço MAC no VF.

Por causa disso, o endereço MAC não é transferido durante o HA como é feito em outras plataformas ASA e com outros tipos de interface.

O failover de HA funciona transferindo o endereço IP de ativo para standby.

# Diagrama de Rede




# Troubleshooting

### Endereços IP ativos/em espera e endereços MAC com interfaces SR-IOV.

Em uma configuração de failover, quando um FTDv/ASAv em par (unidade primária) falha, a unidade FTDv/ASAv em standby assume como a função de unidade primária e seu endereço IP de interface é atualizado, mas mantém o endereço MAC da unidade ASAv em standby.

Portanto, o ASAv envia uma atualização de Protocolo de Resolução de Endereço (ARP) gratuita para anunciar a alteração no endereço MAC do endereço IP da interface para outros dispositivos na mesma rede.

No entanto, devido à incompatibilidade com esses tipos de interfaces, a atualização ARP gratuita não é enviada ao endereço IP global que é definido nas instruções NAT ou PAT para converter o endereço IP da interface em endereços IP globais.

Quando há um FTDv em HA e há tráfego convertido no endereço IP de uma das interfaces de dados de FTDv (e simultaneamente), a interface de dados é uma interface SRIOV, tudo funciona bem até que haja um evento de failover.

O dispositivo FTD não envia ARPs gratuitos para as conexões convertidas quando recebe o endereço IP primário, de modo que os roteadores conectados não atualizam o endereço MAC para essas conexões convertidas e o tráfego falha.

## Demonstração

Essas saídas mostram como o failover de FTDv/ASAv funciona.

Neste exemplo, o FTD-B é a unidade ativa e tem o endereço IP 172.16.100.4 e o endereço 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 outro lado, o FTD-A é a unidade em standby e tem o endereço IP 172.16.100.5 e o endereço 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
```

Esta é a aparência da tabela ARP no lado do Roteador:

<#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
```

Após o failover.

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

```
5757 bytes copied in 0.60 secs
[OK]

Switching to Active
```

O IP muda, mas o MAC é o mesmo.



```
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
```

Aqui podemos ver como o Roteador atualiza as entradas ARP, mas ele não atualiza o mesmo para os Hosts atrás do HA FTD que leva a uma interrupção.



```
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 o switchover, para a interface conectada, o ASA envia o GARP usando o MAC/novo IP, para que o switch e/ou o roteador do gateway o atualize. Mas nenhum GARP para o endereço IP convertido e, portanto, o pacote de retorno do Roteador continua encaminhando usando o endereço MAC do agora standby, mas o endereço IP aponta para o ASA ativo.

Portanto, precisamos do GARP para o endereço IP convertido em NAT.

### Solução

Para evitar uma interrupção, você precisa manter o IP traduzido fora da interface de sub-rede e temos uma rota do gateway que deve funcionar sem problemas. Neste exemplo, o endereço IP convertido deve estar fora do intervalo de sub-rede 172.16.100.0/24.

## Informações Relacionadas

- **Suporte Técnico e Documentação - Cisco Systems**
- **Provisionamento de interface ASAv e SR-IOV**
- Endereços MAC e endereços IP em failover
- **Guia de introdução do Cisco Adaptive Security Virtual Appliance (ASAv), 9.8**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.