ASA/FTD-failovergedrag begrijpen met SR IOV-interfaces

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Achtergrondinformatie.](#)
[Active/Standby IP-adressen en MAC-adressen.](#)

Inleiding

Dit document beschrijft hoe Cisco Secure Firewall in hoge beschikbaarheid werkt wanneer ze SR IOV-interfaces hebben.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Adaptieve security applicatie virtueel (ASA).
- Firepower Thread Defence Virtual (FTDv).
- failover/hoge beschikbaarheid (HA).
- Single Root I/O-virtualisatie (SR-IOV) interface.

Achtergrondinformatie.

Active/Standby IP-adressen en MAC-adressen.

Voor Active/StandbyHigh Availability, is het gedrag van IP-adres en MAC-adresgebruik in een failover-gebeurtenis als volgt:

1. De actieve eenheid gebruikt altijd het primaire IP-adres en het MAC-adres.

2. Wanneer de actieve eenheid over faalt, neemt de standby-eenheid de IP-adressen en MAC-adressen van de mislukte eenheid over en begint het verkeer door te geven.

SR-IOV interfaces.

Met SR-IOV kan netwerkverkeer de software-switch van de Hyper-V virtualisatiestack omzeilen.

Omdat de virtuele functie (VF) aan een kindverdeling wordt toegewezen, stroomt het netwerkverkeer direct tussen VF en de kindverdeling.

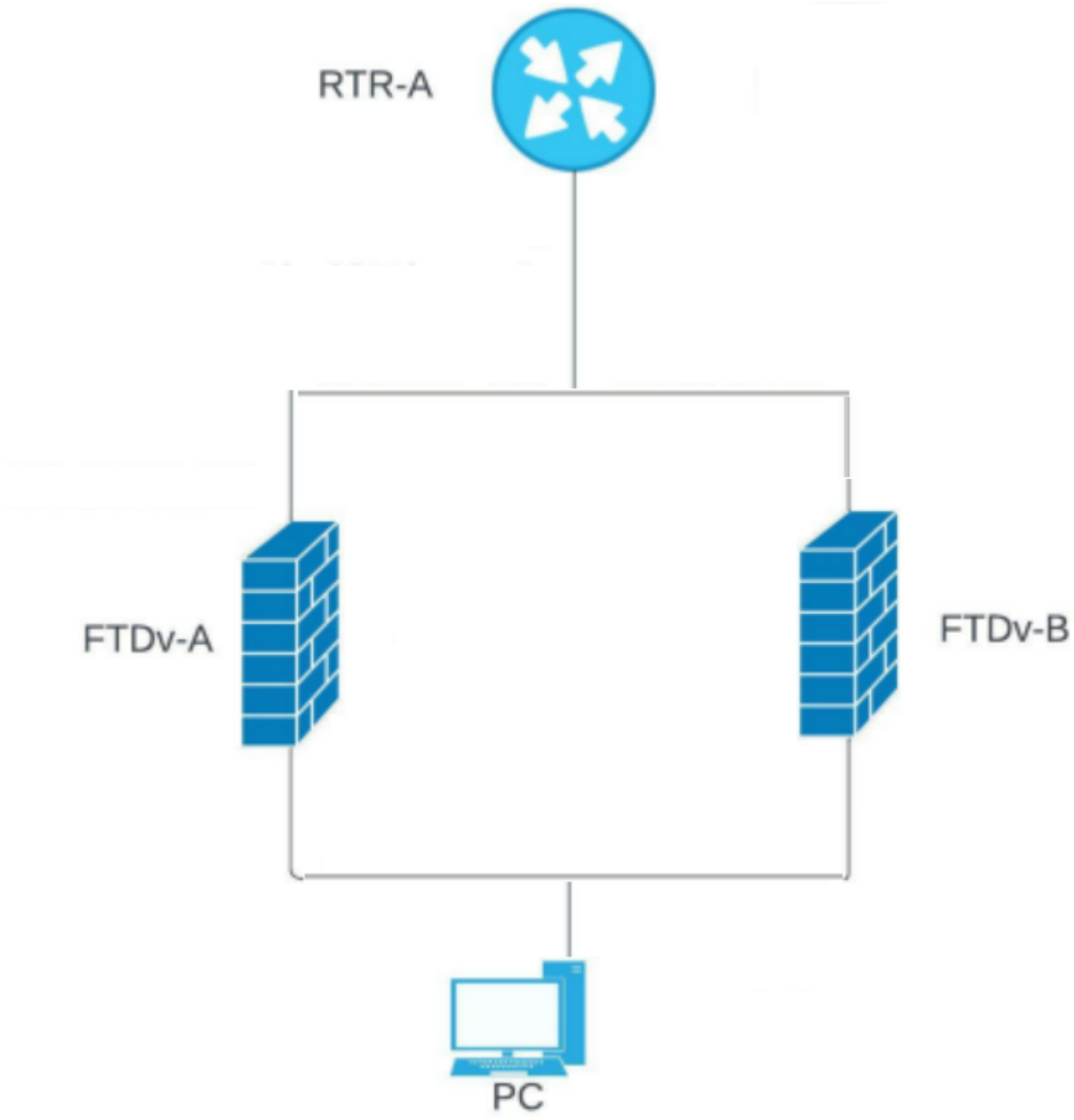
Hierdoor worden de I/O-overheadkosten in de software-emulatielaag verminderd en worden netwerkprestaties bereikt die vrijwel dezelfde prestaties zijn als in niet-gevirtualiseerde omgevingen.

Let op de SRIOV-beperking wanneer het gast-VM niet is toegestaan het MAC-adres op de VF in te stellen.

Hierdoor wordt het MAC-adres niet overgedragen tijdens HA zoals het wordt gedaan op andere ASA-platforms en met andere interfacetypen.

HA failover werkt door het IP-adres van active naar stand-by over te brengen.

Netwerkdiagram



Problemen oplossen

Active/Standby IP-adressen en MAC-adressen met SR-IOV interfaces.

In een failover-installatie, wanneer een gepaarde FTDv/ASAv (primaire eenheid) uitvalt, neemt de standby FTDv/ASAv-eenheid de primaire eenheidsrol over en wordt zijn IP-interfaceadres bijgewerkt, maar behoudt het MAC-adres van de standby ASAv-eenheid.

Daarna verstuurt de ASAv een gratis update van Address Resolution Protocol (ARP) om de wijziging in het MAC-adres van het interface-IP-adres aan te kondigen naar andere apparaten op hetzelfde netwerk.

Wegens onverenigbaarheid met deze types van interfaces, wordt de onnodige ARP update echter niet verzonden naar het globale IP adres dat in de NAT of PAT verklaringen voor het vertalen van het interfaceIP adres naar globale IP adressen wordt bepaald.

Wanneer er een FTDv in HA is en er verkeer vertaald in het IP-adres van een van de FTDv data interfaces (en tegelijkertijd), is de data interface een SRIOV interface alles werkt prima tot er een failover-gebeurtenis is.

Het FTD-apparaat verzendt geen onnodige ARP's voor de vertaalde verbindingen wanneer het het primaire IP-adres inneemt, dus verbonden routers werken het MAC-adres niet bij voor die vertaalde verbindingen en het verkeer mislukt.

Bewijs

Deze uitgangen tonen hoe FTDv/ASAv failover werkt.

In dit voorbeeld, is FTD-B de Actieve eenheid en het heeft 172.16.100.4 IP adres en 5254.0094.9af4 MAC adres.

<#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
```

FTD-A is daarentegen de Standby-unit en heeft 172.16.100.5 IP-adres en 5254.0014.5a27 MAC-adres.

<#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

Hier is wat de ARP-tabel eruit ziet aan de routerkant:

<#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

Na failover.

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

5757 bytes copied in 0.60 secs

```
[OK]

Switching to Active
```

IP verandert, maar MAC is hetzelfde.

<#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
```

Hier kunnen we zien hoe de router de ARP-vermeldingen bijwerken, maar het werkt niet hetzelfde voor de hosts achter de FTD HA wat leidt tot een storing.

<#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
```

Tijdens switchover verstuurt ASA voor de aangesloten interface GARP met behulp van de MAC/new IP, zodat de switch en/of de gateway-router deze bijwerkt. Maar geen GARP voor het vertaalde IP-adres en dus het retourpakket van de router blijft doorsturen met behulp van het nu stand-by MAC-adres, maar het IP-adres verwijst naar de actieve ASA.

Daarom hebben we GARP nodig voor het NAT-vertaalde IP-adres.

Oplossing

Om een stroomonderbreking te voorkomen moet u de Vertaalde IP niet in de subnetinterface houden en we hebben een route van de gateway dingen moeten zonder problemen werken. In dit voorbeeld, moet het vertaalde IP adres uit de 172.16.100.0/24 subnetbereik zijn.

Gerelateerde informatie

- **Technische ondersteuning en documentatie â€“ Cisco Systems**
- **ASA 550v en SR-IOV interfaceprovisioning**
- MAC-adressen en IP-adressen in failover
- **Cisco adaptieve security virtuele applicatie (ASAv) om aan de slag te gaan, 9.8**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.