Comprensione del comportamento di failover ASA/FTD con le interfacce SR IOV

Sommario

Introduzione

In questo documento viene descritto il funzionamento di Cisco Secure Firewall in alta disponibilità con interfacce SR IOV.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Adaptive Security Appliance Virtual (ASAv).
- Firepower Threat Defense Virtual (FTDv).
- Failover/Alta disponibilità (HA).
- Interfaccia SR-IOV (Single Root I/O Virtualization).

Premesse.

Indirizzi IP attivi/standby e indirizzi MAC.

Per Active/StandbyHigh Availability, il comportamento dell'utilizzo dell'indirizzo IP e dell'indirizzo MAC in un evento di failover è il seguente:

1. L'unità attiva utilizza sempre l'indirizzo IP primario e l'indirizzo MAC.

2. Quando l'unità attiva esegue il failover, l'unità in standby assume gli indirizzi IP e gli indirizzi MAC dell'unità guasta e inizia a trasmettere il traffico.

Interfacce SR-IOV.

SR-IOV consente al traffico di rete di ignorare il livello di switch software dello stack di virtualizzazione Hyper-V.

Poiché la funzione virtuale (VF) è assegnata a una partizione figlio, il traffico di rete passa direttamente tra la VF e la partizione figlio.

Di conseguenza, il sovraccarico di I/O nel livello di emulazione software viene ridotto e si ottengono prestazioni di rete pressoché identiche a quelle degli ambienti non virtualizzati.

Tenere presente la limitazione SRIOV in cui alla VM guest non è consentito impostare l'indirizzo MAC nella VF.

Per questo motivo, l'indirizzo MAC non viene trasferito durante il processo di HA, come avviene su altre piattaforme ASA e con altri tipi di interfaccia.

Il failover HA funziona trasferendo l'indirizzo IP da attivo a standby.

Esempio di rete

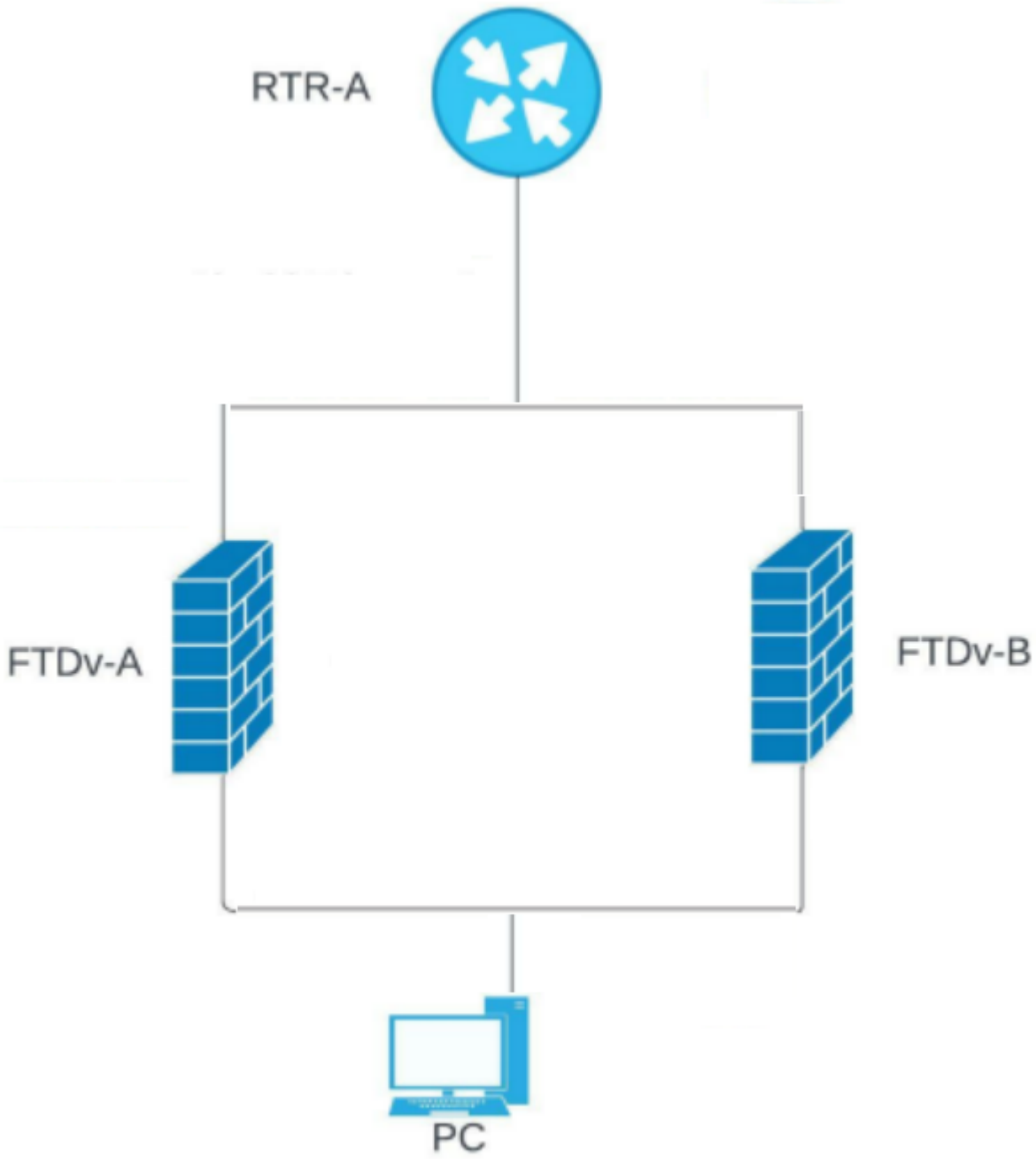

Immagine 1. Esempio di diagramma.

Risoluzione dei problemi

Indirizzi IP attivo/standby e indirizzi MAC con interfacce SR-IOV.

In una configurazione di failover, quando un FTDv/ASAv (unità primaria) accoppiato ha esito negativo, l'unità FTDv/ASAv di standby assume il ruolo di unità primaria e il relativo indirizzo IP di interfaccia viene aggiornato ma conserva l'indirizzo MAC dell'unità ASAv di standby.

Successivamente, ASAv invia un aggiornamento gratuito del protocollo ARP (Address Resolution Protocol) per annunciare la modifica dell'indirizzo MAC dell'interfaccia IP ad altri dispositivi della stessa rete.

Tuttavia, a causa dell'incompatibilità con questi tipi di interfacce, l'aggiornamento ARP gratuito non viene

inviato all'indirizzo IP globale definito nelle istruzioni NAT o PAT per convertire l'indirizzo IP dell'interfaccia in indirizzi IP globali.

Quando è presente un FTDv in HA e c'è traffico convertito nell'indirizzo IP di una delle interfacce dati FTDv (e contemporaneamente), l'interfaccia dati è un'interfaccia SRIOV tutto funziona bene fino a quando non c'è un evento di failover.

Il dispositivo FTD non invia ARP gratuiti per le connessioni tradotte quando accetta l'indirizzo IP primario, quindi i router connessi non aggiornano l'indirizzo MAC per le connessioni tradotte e il traffico non riesce.

Dimostrazione

Questi output mostrano il funzionamento del failover FTDv/ASAv.

Nell'esempio, FTD-B è l'unità attiva e ha un indirizzo IP 172.16.100.4 e un indirizzo 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
```

D'altra parte, l'FTD-A è l'unità di Standby e ha un indirizzo IP 172.16.100.5 e un indirizzo 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
```

Di seguito è riportato l'aspetto della tabella ARP sul lato 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
```

Dopo il failover.

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

5757 bytes copied in 0.60 secs
[OK]

Switching to Active
```

L'indirizzo IP cambia ma l'indirizzo MAC è lo stesso.

<#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
```

Qui possiamo vedere come il router aggiorna le voci ARP ma non lo stesso per gli host dietro l'FTD HA che porta a un'interruzione.

<#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 lo switchover, per l'interfaccia connessa, ASA invia un messaggio GARP con l'indirizzo MAC/new IP, in modo che lo switch e/o il router gateway lo aggiorni. Tuttavia, non essendo il GARP dell'indirizzo IP tradotto, il pacchetto di ritorno dal router continua a inoltrare usando l'indirizzo MAC del router in standby, ma l'indirizzo IP punta all'appliance ASA attiva.

Pertanto, è necessario GARP per l'indirizzo IP tradotto NAT.

Soluzione

Per evitare interruzioni è necessario mantenere l'indirizzo IP tradotto non nell'interfaccia della subnet e abbiamo un percorso dal gateway che funziona senza problemi. Nell'esempio, l'indirizzo IP tradotto deve essere esterno all'intervallo di subnet 172.16.100.0/24.

Informazioni correlate

- **Documentazione e supporto tecnico â€“ Cisco Systems**
- **Provisioning dell'interfaccia ASAv e SR-IOV**
- Indirizzi MAC e indirizzi IP nel failover
- **Guida introduttiva a Cisco Adaptive Security Virtual Appliance (ASAv), 9.8**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).