Comprendre le comportement de basculement ASA/FTD avec les interfaces SR IOV

Table des matières

Introduction

Ce document décrit le fonctionnement de Cisco Secure Firewall en haute disponibilité lorsqu'il dispose d'interfaces SR IOV.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appliance de sécurité adaptative virtuelle (ASAv).
- Firepower Threat Defense Virtual (FTDv).
- Basculement/Haute disponibilité (HA).
- Interface SR-IOV (Single Root I/O Virtualization).

Informations générales.

Adresses IP actives/en veille et adresses MAC.

Pour Active/StandbyHigh Availability, le comportement de l'utilisation des adresses IP et MAC dans un événement de basculement est le suivant :

1. L'unité active utilise toujours l'adresse IP principale et l'adresse MAC.
2. Lorsque l'unité active bascule, l'unité en veille assume les adresses IP et MAC de l'unité défaillante et commence à transmettre le trafic.

Interfaces SR-IOV.

SR-IOV permet au trafic réseau de contourner la couche de commutation logicielle de la pile de virtualisation Hyper-V.

Étant donné que la fonction virtuelle (VF) est attribuée à une partition enfant, le trafic réseau circule directement entre la fonction virtuelle et la partition enfant.

Par conséquent, la surcharge d'E/S dans la couche d'émulation logicielle est réduite et permet d'obtenir des performances réseau presque identiques à celles des environnements non virtualisés.

Soyez conscient de la limitation SRIOV où la machine virtuelle invitée n'est pas autorisée à définir l'adresse MAC sur le VF.

De ce fait, l'adresse MAC n'est pas transférée pendant la haute disponibilité comme c'est le cas sur d'autres plates-formes ASA et avec d'autres types d'interface.

Le basculement haute disponibilité fonctionne en transférant l'adresse IP de l'état actif à l'état de veille.

Diagramme du réseau

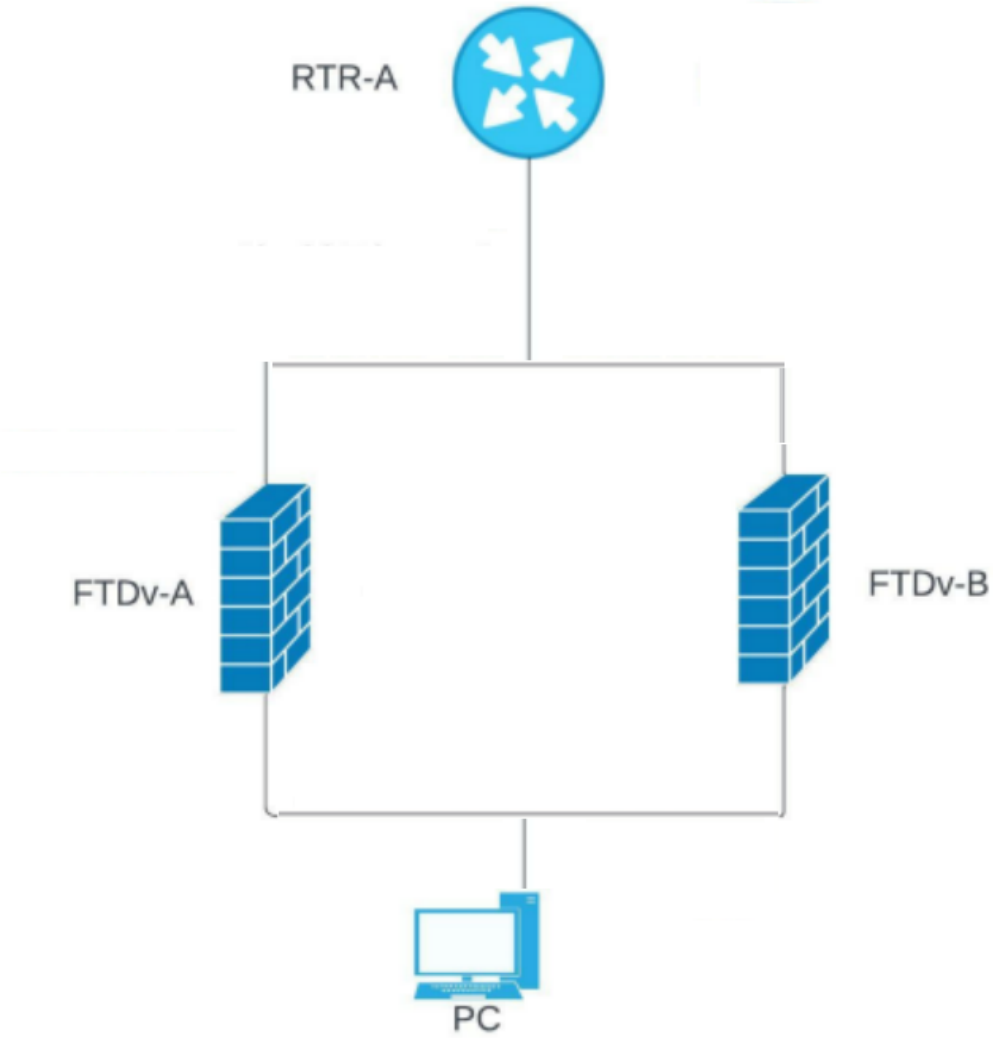

Image 1. Exemple de schéma.

Dépannage

Adresses IP actives/en veille et adresses MAC avec interfaces SR-IOV.

Dans une configuration de basculement, lorsqu'une paire FTDv/ASAv (unité principale) tombe en panne, l'unité FTDv/ASAv de secours prend le relais en tant qu'unité principale, et son adresse IP d'interface est mise à jour mais conserve l'adresse MAC de l'unité ASAv de secours.

Par la suite, l'ASAv envoie une mise à jour gratuite du protocole ARP (Address Resolution Protocol) pour annoncer la modification de l'adresse MAC de l'adresse IP de l'interface aux autres périphériques du même réseau.

Cependant, en raison d'une incompatibilité avec ces types d'interfaces, la mise à jour ARP gratuite n'est pas envoyée à l'adresse IP globale qui est définie dans les instructions NAT ou PAT pour traduire l'adresse IP de l'interface en adresses IP globales.

Quand il y a un FTDv dans HA et qu'il y a du trafic traduit dans l'adresse IP de l'une des interfaces de données FTDv (et simultanément), l'interface de données est une interface SRIOV tout fonctionne bien jusqu'à ce qu'il y ait un événement de basculement.

Le périphérique FTD n'envoie pas de requêtes ARP gratuites pour les connexions traduites lorsqu'il prend l'adresse IP principale, de sorte que les routeurs connectés ne mettent pas à jour l'adresse MAC pour ces connexions traduites et que le trafic échoue.

Démonstration

Ces résultats montrent comment fonctionne le basculement FTDv/ASAv.

Dans cet exemple, FTD-B est l'unité active et possède l'adresse IP 172.16.100.4 et l'adresse 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'autre part, FTD-A est l'unité en veille et elle a l'adresse IP 172.16.100.5 et l'adresse 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
```

Voici à quoi ressemble la table ARP côté routeur :

<#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
```

Après le basculement.

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

5757 bytes copied in 0.60 secs
[OK]

Switching to Active
```

L'adresse IP change, mais MAC est identique.

<#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
```

Ici, nous pouvons voir comment le routeur met à jour les entrées ARP, mais il ne met pas à jour la même chose pour les hôtes derrière la haute disponibilité FTD, ce qui entraîne une panne.

<#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
```

Pendant le basculement, pour l'interface connectée, ASA envoie GARP en utilisant l'adresse MAC/la nouvelle adresse IP, de sorte que le commutateur et/ou le routeur de passerelle le mette à jour. Mais pas de GARP pour l'adresse IP traduite, et donc le paquet de retour du routeur continue à transférer en utilisant l'adresse MAC du routeur maintenant en veille, mais l'adresse IP pointe vers l'ASA actif.

Nous avons donc besoin du protocole GARP pour l'adresse IP traduite par NAT.

Solution

Afin d'éviter une panne, vous devez garder l'IP traduite pas dans l'interface de sous-réseau et nous avons une route à partir de la passerelle les choses doivent fonctionner sans problème. Dans cet exemple, l'adresse IP traduite doit être hors de la plage de sous-réseaux 172.16.100.0/24.

Informations connexes

- Assistance et documentation techniques - Cisco Systems

- Approvisionnement des interfaces ASAv et SR-IOV
- Adresses MAC et adresses IP dans le basculement
- Guide de démarrage de l'appliance virtuel de sécurité adaptatif Cisco (ASAv), 9.8

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.