ASA/FTD-Failover-Verhalten mit SR IOV-Schnittstellen verstehen

Inhalt

Einleitung

In diesem Dokument wird die Funktionsweise der Cisco Secure Firewall in High Availability mit SR IOV-Schnittstellen beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Adaptive Security Appliance Virtual (ASAv)
- Firepower Thread Defense Virtual (FTDv)
- Failover/Hochverfügbarkeit (HA).
- SR-IOV-Schnittstelle (Single Root I/O Virtualization)

Hintergrundinformationen.

Aktive/Standby-IP-Adressen und MAC-Adressen.

Bei Aktiv/StandbyHochverfügbarkeit verhalten sich IP- und MAC-Adressen bei einem Failover-Ereignis wie folgt:

1. Das aktive Gerät verwendet immer die primäre IP- und MAC-Adresse.

2. Beim Failover übernimmt das Standby-Gerät die IP- und MAC-Adressen des ausgefallenen Geräts und leitet den Datenverkehr weiter.

SR-IOV-Schnittstellen.

Mit SR-IOV kann der Netzwerkverkehr die Software-Switch-Ebene des Hyper-V Virtualisierungs-Stacks umgehen.

Da die virtuelle Funktion (VF) einer untergeordneten Partition zugewiesen ist, fließt der Netzwerkverkehr direkt zwischen der VF und der untergeordneten Partition.

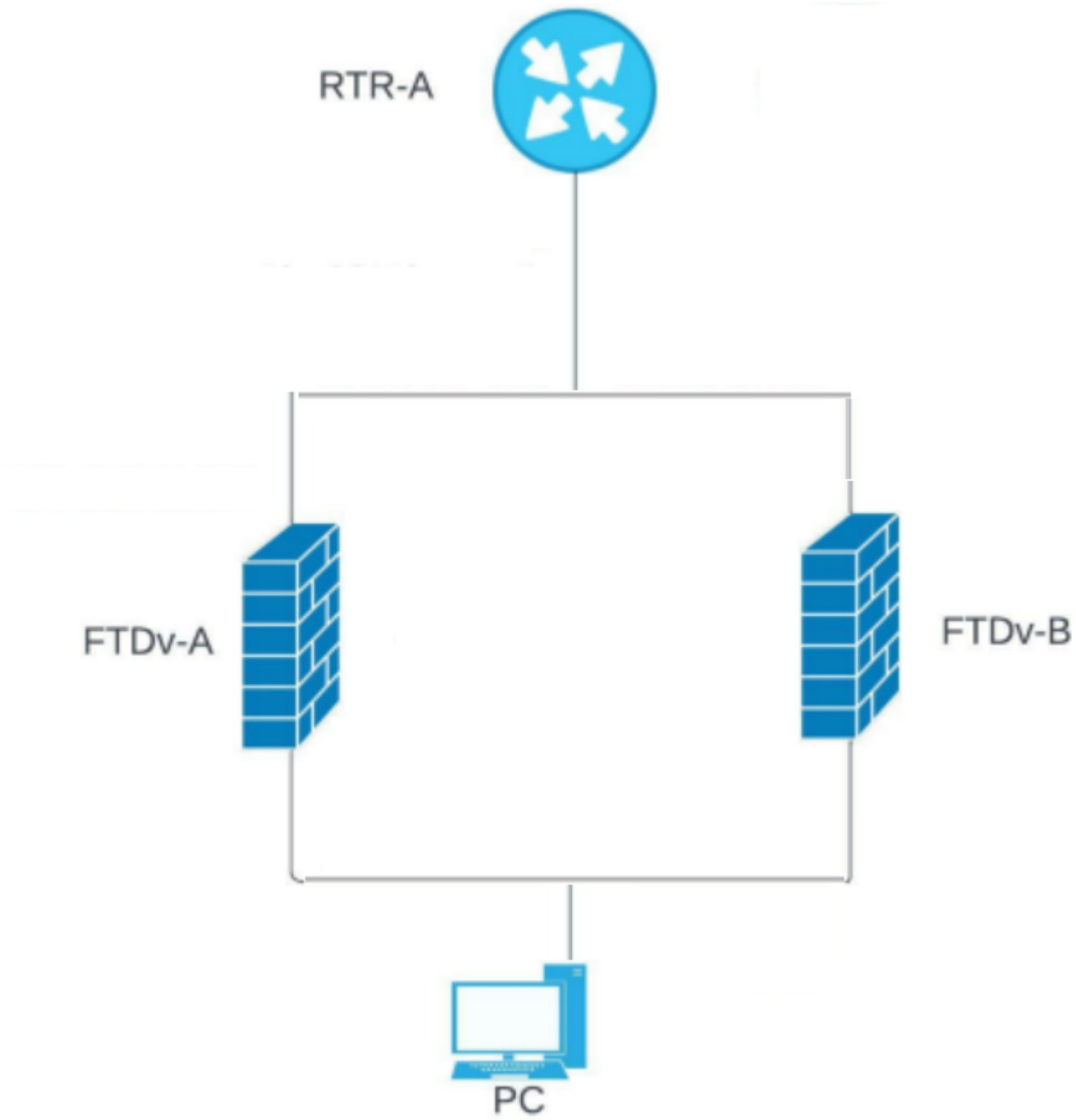
Dadurch wird der E/A-Overhead in der Softwareemulationsebene verringert und eine Netzwerkleistung erzielt, die nahezu der in nicht virtualisierten Umgebungen entspricht.

Beachten Sie die SRIOV-Einschränkung, wenn die Gast-VM die MAC-Adresse auf der VF nicht festlegen darf.

Aus diesem Grund wird die MAC-Adresse nicht wie bei anderen ASA-Plattformen und Schnittstellentypen während der Hochverfügbarkeit übertragen.

Ein HA-Failover funktioniert, indem die IP-Adresse vom aktiven in den Standby-Modus übertragen wird.

Netzwerkdiagramm



Fehlerbehebung

Aktive/Standby-IP-Adressen und MAC-Adressen mit SR-IOV-Schnittstellen.

Wenn bei einer Failover-Konfiguration ein paarweises FTDv/ASAv (primäre Einheit) ausfällt, übernimmt die FTDv/ASAv-Einheit im Standby-Modus die Rolle der primären Einheit, und ihre Schnittstellen-IP-Adresse wird aktualisiert, behält jedoch die MAC-Adresse der ASAv-Einheit im Standby-Modus bei.

Anschließend sendet die ASAv ein kostenloses ARP-Update (Address Resolution Protocol), um die Änderung der MAC-Adresse der Schnittstellen-IP-Adresse an andere Geräte im gleichen Netzwerk anzukündigen.

Aufgrund der Inkompatibilität mit diesen Schnittstellentypen wird das überflüssige ARP-Update jedoch nicht an die globale IP-Adresse gesendet, die in den NAT- oder PAT-Anweisungen für die Übersetzung der Schnittstellen-IP-Adresse in globale IP-Adressen definiert ist.

Wenn in HA ein FTDv vorhanden ist und Datenverkehr in die IP-Adresse einer der FTDv-Datenschnittstellen (und gleichzeitig) umgewandelt wird, ist die Datenschnittstelle eine SRIOV-Schnittstelle, und alles funktioniert gut, bis ein Failover-Ereignis eintritt.

Das FTD-Gerät sendet keine überflüssigen ARPs für die übersetzten Verbindungen, wenn es die primäre IP-Adresse verwendet, sodass angeschlossene Router die MAC-Adresse für diese übersetzten Verbindungen nicht aktualisieren und der Datenverkehr ausfällt.

Demonstration

Diese Ausgaben zeigen, wie FTDv/ASAv-Failover funktioniert.

In diesem Beispiel ist FTD-B die aktive Einheit und hat die IP-Adresse 172.16.100.4 und die MAC-Adresse 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
```

Andererseits ist FTD-A die Standby-Einheit und verfügt über die IP-Adresse 172.16.100.5 und die MAC-Adresse 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
```

So sieht die ARP-Tabelle auf der Router-Seite aus:

<#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
```

Nach Failover:

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

5757 bytes copied in 0.60 secs
[OK]

Switching to Active
```

Die IP-Adresse ändert sich, aber die MAC-Adresse ist identisch.

<#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 ist zu sehen, wie der Router die ARP-Einträge aktualisiert, dies gilt jedoch nicht für die Hosts hinter der FTD HA, was zu einem Ausfall führt.

<#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
```

Während des Switchovers sendet die ASA für die verbundene Schnittstelle GARP über die MAC/neue IP-Adresse, sodass der Switch und/oder der Gateway-Router dies aktualisiert. Es wird jedoch kein GARP für die übersetzte IP-Adresse erstellt, und das Rückpaket vom Router wird weiterhin über die MAC-Adresse des aktuellen Standby-Geräts weitergeleitet, die IP-Adresse verweist jedoch auf die aktive ASA.

Daher benötigen wir GARP für die NAT-umgewandelte IP-Adresse.

Lösung

Um einen Ausfall zu vermeiden, müssen Sie die übersetzte IP nicht in der Subnetz-Schnittstelle aufbewahren, und wir haben eine Route vom Gateway aus. Die Dinge müssen problemlos funktionieren. In diesem Beispiel muss die übersetzte IP-Adresse aus dem Subnetzbereich 172.16.100.0/24 stammen.

Zugehörige Informationen

- **Technischer Support und Dokumentation für Cisco Systeme**
- **ASAv- und SR-IOV-Schnittstellenbereitstellung**
- MAC- und IP-Adressen in Failover
- **Cisco Adaptive Security Virtual Appliance (ASAv) Erste Schritte, 9.8**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.