Understand ASA/FTD Failover Behavior with SR IOV Interfaces

Contents

Introduction

This document describes how Cisco Secure Firewall in High Availability works when they have SR IOV interfaces.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Adaptive Security Appliance Virtual (ASAv).
- Firepower Threat Defense Virtual (FTDv).
- Failover / High Availability (HA).
- Single Root I/O Virtualization (SR-IOV) Interface.

Background Information.

Active/Standby IP Addresses and MAC Addresses.

For Active/StandbyHigh Availability, the behavior of IP address and MAC address usage in a failover event is the following:

1. The active unit always uses the primary IP address and MAC address.

2. When the active unit fails over, the standby unit assumes the IP addresses and MAC addresses of the failed unit and begins passing traffic.

SR-IOV interfaces.

SR-IOV enables network traffic to bypass the software switch layer of the Hyper-V virtualization stack.

Because the Virtual Function (VF) is assigned to a child partition, the network traffic flows directly between the VF and the child partition.

As a result, the I/O overhead in the software emulation layer is diminished and achieves network performance that is nearly the same performance as in nonvirtualized environments.

Be aware of the SRIOV limitation where the guest VM is not allowed to set the MAC address on the VF.

Because of this, the MAC address is not transferred during HA like it is done on other ASA platforms and with other interface types.

HA failover works by transferring the IP address from active to standby.

Network Diagram

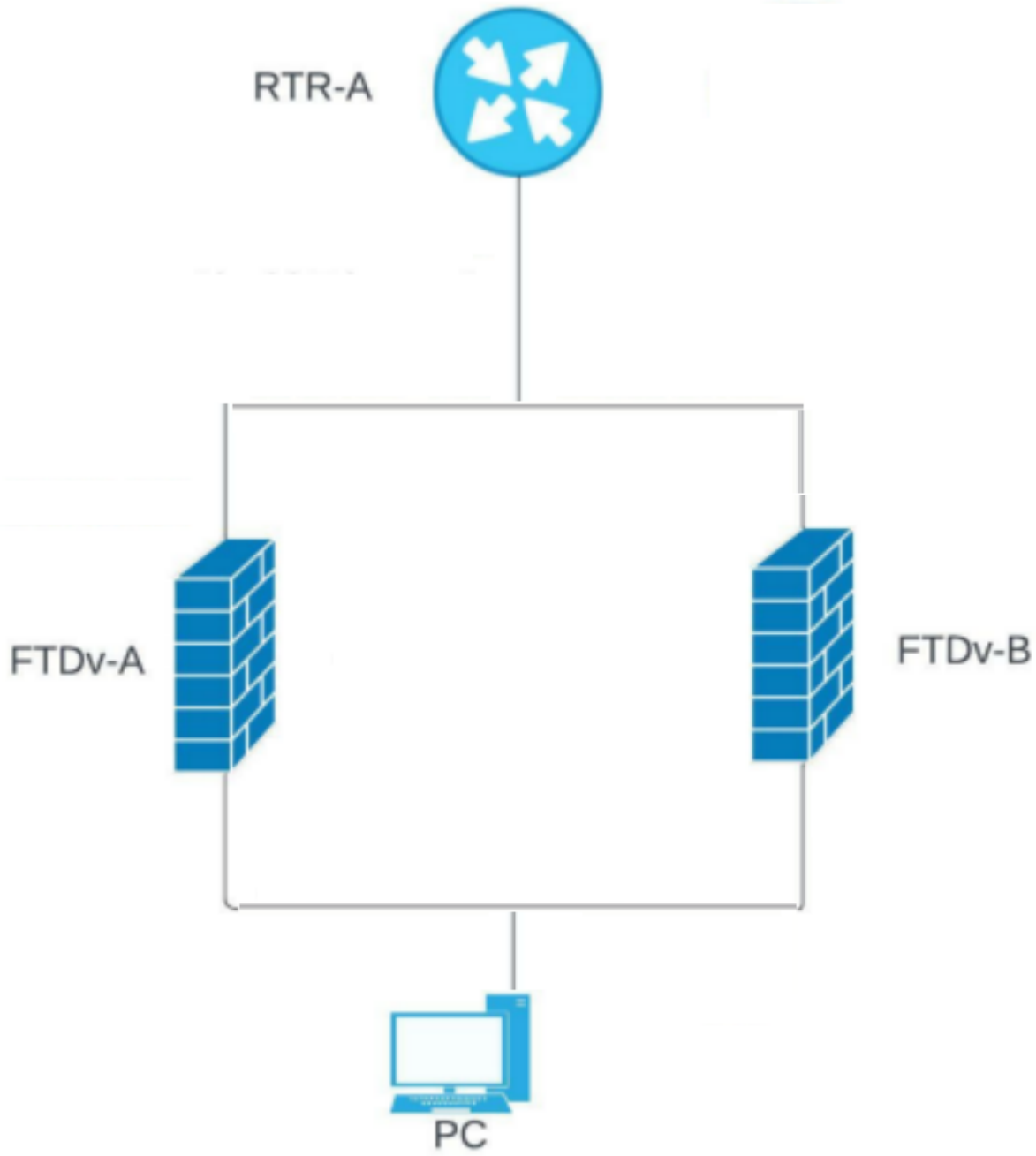

Image 1. Diagram example.

Troubleshoot

Active/Standby IP Addresses and MAC Addresses with SR-IOV interfaces.

In a failover setup, when a paired FTDv/ASAv (primary unit) fails, the standby FTDv/ASAv unit takes over as the primary unit role, and its interface IP address is updated but keeps the MAC address of the standby ASAv unit.

Thereafter, the ASAv sends a gratuitous Address Resolution Protocol (ARP) update to announce the change in the MAC address of the interface IP address to other devices on the same network.

However, due to incompatibility with these types of interfaces, the gratuitous ARP update is not sent to the

global IP address that is defined in the NAT or PAT statements for translating the interface IP address to global IP addresses.

When there is an FTDv in HA and there is traffic translated into the IP address of one of the FTDv data interfaces (and simultaneously), the data interface is an SRIOV interface everything works fine until there is a failover event.

The FTD device does not send gratuitous ARPs for the translated connections when it takes the primary IP address, so connected routers do not update the MAC address for those translated connections and traffic fails.

Demostration

These outputs show how FTDv/ASAv failover works.

In this example, FTD-B is the Active unit and it does have 172.16.100.4 IP address and 5254.0094.9af4 MAC address.

<#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
```

On the other hand, FTD-A is the Standby unit and it does have 172.16.100.5 IP address and 5254.0014.5a27 MAC address.

```
<#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
```

Here is what the ARP table looks like on the Router side:

<#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
```

After failover.

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

5757 bytes copied in 0.60 secs
[OK]

Switching to Active
```

IP changes but MAC is the same.

<#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
```

Here we can see how the Router update the ARP entries but it does not update the same for the Hosts behind the FTD HA which leads to an outage.

<#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
```

During switchover, for the connected interface, ASA sends GARP using the MAC/new IP, so that the switch and/or the gateway router updates it. But no GARP for the translated IP address, and hence the return packet from Router keeps forwarding using the now standbyâ€™s MAC address but the IP address points to the active ASA.

Hence we need GARP for the NAT-translated IP address.

Solution

In order to avoid an outage you need to keep the Translated IP not in the subnet interface and we have a route from the gateway things must work without issues. In this example, the translated IP address must be out of the 172.16.100.0/24 subnet range.

Related Information

- **Technical Support & Documentation - Cisco Systems**
- **ASAv and SR-IOV Interface Provisioning**
- MAC Addresses and IP Addresses in Failover
- **Cisco Adaptive Security Virtual Appliance (ASAv) Getting Started Guide, 9.8**