SR IOV 인터페이스의 ASA/FTD 페일오버 동작 이해

목차

소개

이 문서에서는 SR IOV 인터페이스가 있는 경우 고가용성의 Cisco Secure Firewall이 어떻게 작동하는지 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASAv(Adaptive Security Appliance Virtual).
- Firepower FTDv(Threat Defense Virtual)
- 장애 조치/고가용성(HA).
- 단일 루트 I/O 가상화(SR-IOV) 인터페이스.

배경 정보.

액티브/스탠바이 IP 주소 및 MAC 주소.

액티브/스탠바이 고가용성의 경우 장애 조치 이벤트에서 IP 주소 및 MAC 주소 사용의 동작은 다음과 같습니다.

1. 액티브 유닛에서는 항상 기본 IP 주소와 MAC 주소를 사용합니다.
2. 액티브 유닛이 장애 조치되면 스탠바이 유닛에서는 장애가 발생한 유닛의 IP 주소 및 MAC 주소를 가정하고 트래픽 전달을 시작합니다.

SR-IOV 인터페이스.

SR-IOV는 네트워크 트래픽이 Hyper-V 가상화 스택의 소프트웨어 스위치 레이어를 우회하도록 합니다.

VF(Virtual Function)는 하위 파티션에 할당되므로 네트워크 트래픽은 VF와 하위 파티션 간에 직접 흐릅니다.

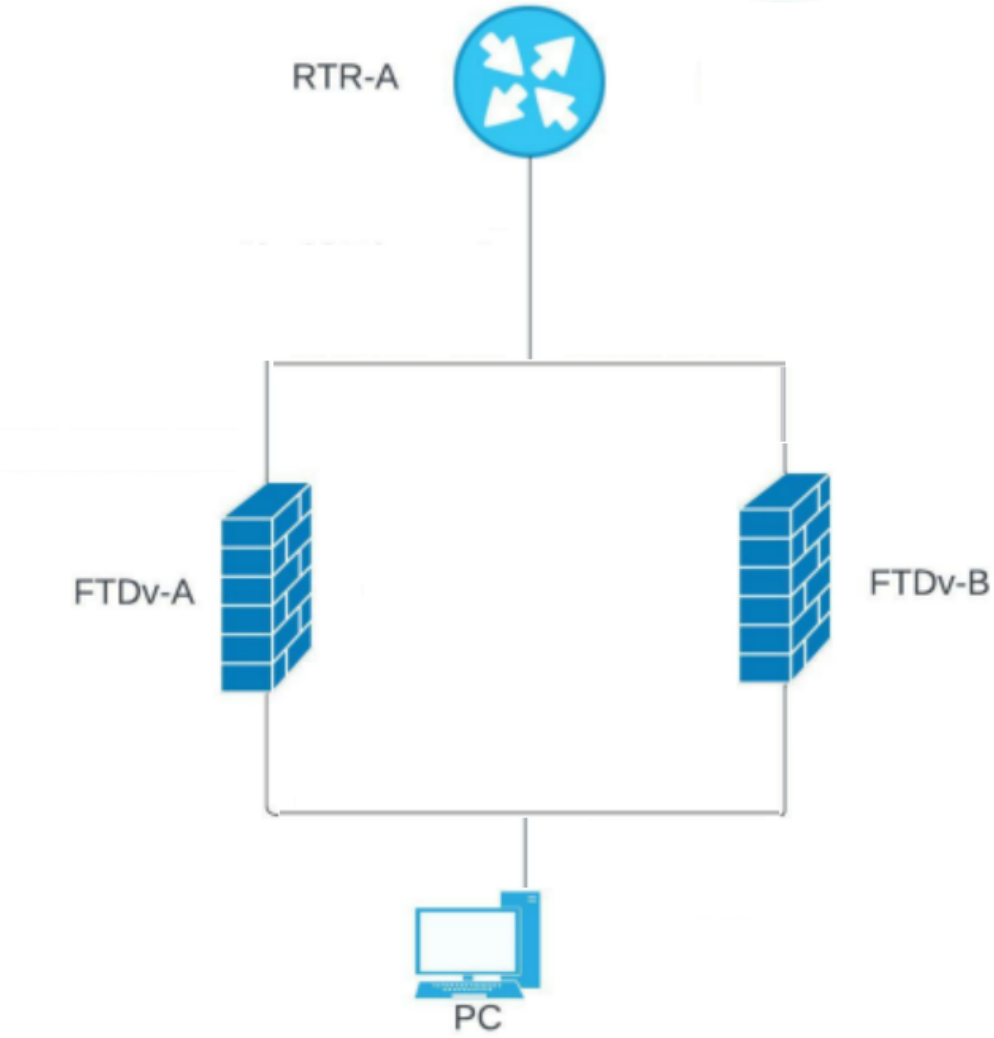
따라서 소프트웨어 에뮬레이션 레이어의 I/O 오버헤드가 줄어들고 가상화되지 않은 환경과 거의 동일한 수준의 네트워크 성능이 구현됩니다.

게스트 VM에서 VF의 MAC 주소를 설정할 수 없는 SRIOV 제한 사항에 유의하십시오.

따라서 MAC 주소는 다른 ASA 플랫폼 및 다른 인터페이스 유형에서 수행되는 것처럼 HA 중에는 전송되지 않습니다.

HA 장애 조치는 IP 주소를 액티브에서 스탠바이로 전송하는 방식으로 작동합니다.

네트워크 다이어그램



이미지 1. 다이어그램 예

문제 해결

SR-IOV 인터페이스를 사용하는 액티브/스탠바이 IP 주소 및 MAC 주소.

장애 조치 설정에서 페어링된 FTDv/ASAv(기본 유닛)에 장애가 발생하면 대기 FTDv/ASAv 유닛이 기본 유닛 역할을 인계받고 인터페이스 IP 주소가 업데이트되지만 대기 ASAv 유닛의 MAC 주소는 유지됩니다.

그 후 ASAv는 인터페이스 IP 주소의 MAC 주소 변경을 알리기 위해 ARP(Address Resolution Protocol) 업데이트를 같은 네트워크의 다른 디바이스에 전송합니다.

그러나 이러한 인터페이스 유형과의 비호환성 때문에 인터페이스 IP 주소를 전역 IP 주소로 변환하기 위해 NAT 또는 PAT 문에 정의된 전역 IP 주소로 불필요한 ARP 업데이트가 전송되지 않습니다.

HA에 FTDv가 있고 FTDv 데이터 인터페이스 중 하나의 IP 주소로 트래픽이 변환되는 경우(그리고 동시에), 데이터 인터페이스는 SRIOV 인터페이스이며 장애 조치 이벤트가 발생할 때까지 정상적으로 작동합니다.

FTD 디바이스는 기본 IP 주소를 사용할 때 변환된 연결에 대해 불필요한 ARP를 전송하지 않으므로, 연결된 라우터는 이러한 변환된 연결에 대한 MAC 주소를 업데이트하지 않으며 트래픽이 실패합니다.

데모

이러한 출력은 FTDv/ASAv 장애 조치가 작동하는 방식을 보여줍니다.

이 예에서 FTD-B는 액티브 유닛이며 172.16.100.4 IP 주소 및 5254.0094.9af4 MAC 주소를 가집니다.

<#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

반면, FTD-A는 스탠바이 유닛이며 172.16.100.5 IP 주소 및 5254.0014.5a27 MAC 주소를 가집니다
.

<#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
```

다음은 라우터 측의 ARP 테이블 모양입니다.

<#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
```

장애 조치 후

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

5757 bytes copied in 0.60 secs
[OK]

Switching to Active
```

IP는 변경되지만 MAC은 동일합니다.

<#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
```

여기서는 라우터가 ARP 항목을 업데이트하지만 FTD HA 뒤에 있는 호스트에 대해서는 동일한 업데이트를 수행하지 않아 가동 중단이 발생하는 방법을 확인할 수 있습니다.

<#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
```

전환 과정에서 연결된 인터페이스에 대해 ASA는 MAC/새 IP를 사용하여 GARP를 전송하므로 스위치 및/또는 게이트웨이 라우터가 이를 업데이트합니다. 그러나 변환된 IP 주소에 대한 GARP가 없으므로 라우터의 반환 패킷이 현재 대기의 MAC 주소를 사용하여 계속 전달되지만 IP 주소는 활성 ASA를 가리킵니다.

따라서 NAT 변환 IP 주소에 대한 GARP가 필요합니다.

솔루션

중단을 방지하려면 변환된 IP를 서브넷 인터페이스에 유지해야 하며 게이트웨이에서 오는 경로가 있어야 합니다. 이러한 작업은 문제 없이 동작해야 합니다. 이 예에서는 변환된 IP 주소가 172.16.100.0/24 서브넷 범위를 벗어나야 합니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems
- ASAv 및 SR-IOV 인터페이스 프로비저닝
- 장애 조치의 MAC 주소 및 IP 주소
- Cisco ASAv(Adaptive Security Virtual Appliance) 시작 가이드, 9.8

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.