SR IOVインターフェイスでのASA/FTDフェールオーバーの動作について

内容

はじめに

このドキュメントでは、SR IOVインターフェイスを備えたハイアベイラビリティのCisco Secure Firewallの動作について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 適応型セキュリティアプライアンス仮想(ASAv)。
- Firepower脅威対策の仮想(FTDv)。
- フェールオーバー/ハイアベイラビリティ(HA)
- シングルルートI/O仮想化(SR-IOV)インターフェイス

バックグラウンド情報.

アクティブ/スタンバイIPアドレスとMACアドレス。

アクティブ/スタンバイハイアベイラビリティの場合、フェールオーバーイベントにおけるIPアドレスとMACアドレスの使用状況の動作は次のようになります。

1. アクティブユニットは常にプライマリIPアドレスとMACアドレスを使用します。
2. アクティブユニットがフェールオーバーすると、スタンバイユニットが故障したユニットのIPアドレスとMACアドレスを引き継ぎ、トラフィックの受け渡しを開始します。

SR-IOVインターフェイス

SR-IOVでは、ネットワークトラフィックがHyper-V仮想化スタックのソフトウェアスイッチレイヤをバイパスできます。

仮想機能(VF)は子パーティションに割り当てられるため、ネットワークトラフィックはVFと子パーティションの間を直接流れます。

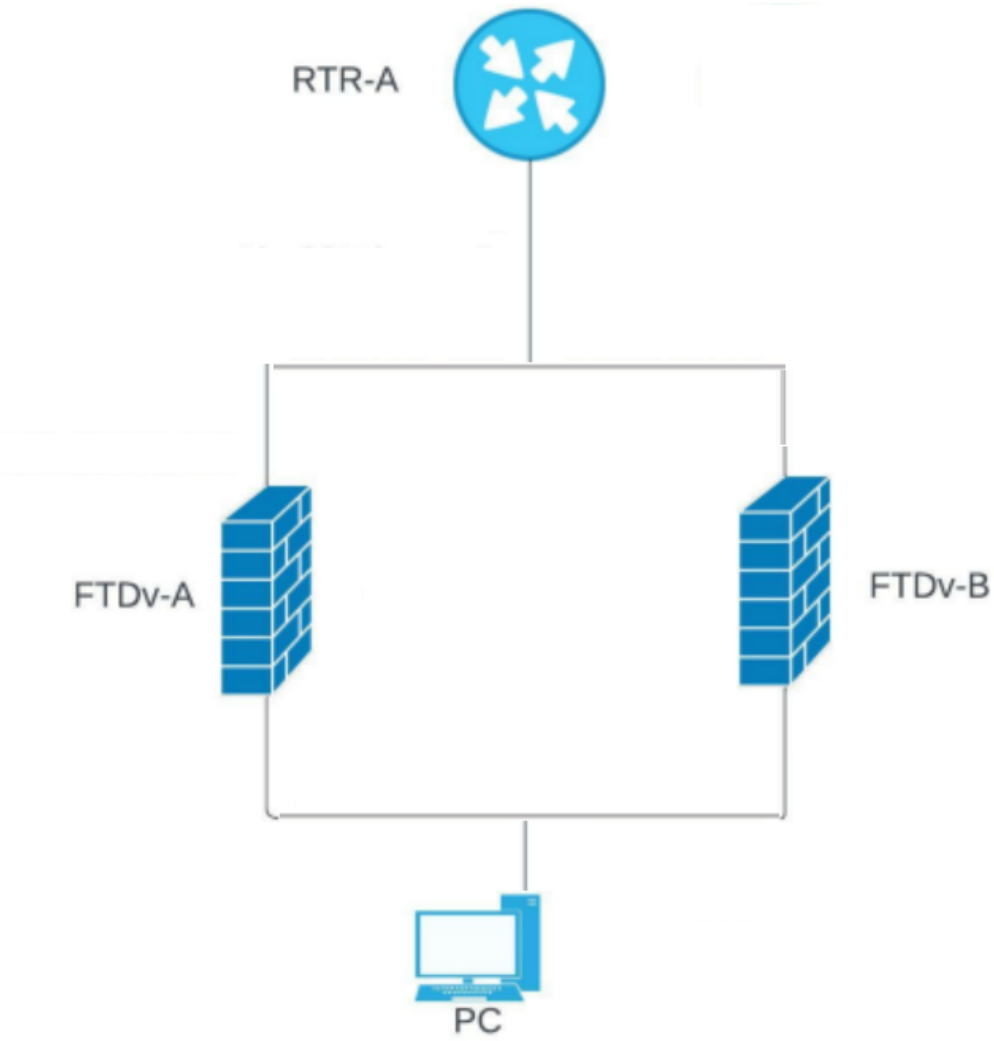
その結果、ソフトウェアエミュレーションレイヤのI/Oオーバーヘッドが削減され、非仮想化環境とほぼ同じパフォーマンスのネットワークパフォーマンスが実現します。

ゲストVMがVFのMACアドレスを設定できない場合は、SRIOVの制限に注意してください。

このため、MACアドレスは、他のASAプラットフォームや他のインターフェイスタイプで行われるようなHA中には転送されません。

HAフェールオーバーは、アクティブからスタンバイにIPアドレスを転送することによって機能します。

ネットワーク図



画像 1.図の例。

トラブルシュート

アクティブ/スタンバイIPアドレスとSR-IOVインターフェイスのMACアドレス。

フェールオーバー設定では、ペアになったFTDv/ASAv（プライマリユニット）に障害が発生すると、スタンバイFTDv/ASAvユニットがプライマリユニットの役割を引き継ぎ、そのインターフェイスIPアドレスは更新されますが、スタンバイASAvユニットのMACアドレスは保持されます。

その後、ASAvはgratuitous Address Resolution Protocol(ARP)アップデートを送信して、インターフェイスIPアドレスのMACアドレスの変更を同じネットワーク上の他のデバイスに通知します。

ただし、これらのタイプのインターフェイスとの非互換性により、gratuitous ARPアップデートは、インターフェイスIPアドレスをグローバルIPアドレスに変換するためのNATまたはPATステートメントで定義されたグローバルIPアドレスには送信されません。

HAにFTDvが存在し、トラフィックがいずれかのFTDvデータインターフェイスのIPアドレスに（同時に）変換されている場合、データインターフェイスはSRIOVインターフェイスであり、フェールオーバーイベントが発生するまでは問題なく動作します。

FTDデバイスはプライマリIPアドレスを取得する際に、変換された接続に対するgratuitous ARPを送信しないため、接続されたルータはこれらの変換された接続に対するMACアドレスを更新せず、トラフィックは失敗します。

降格

次の出力は、FTDv/ASAvフェールオーバーの仕組みを示しています。

この例では、FTD-Bがアクティブユニットで、IPアドレス172.16.100.4とMACアドレス5254.0094.9af4があります。

<#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

一方、FTD-Aはスタンバイユニットで、IPアドレス172.16.100.5とMACアドレス5254.0014.5a27があります。

<#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
```

ルータ側のARPテーブルは次のようになります。

<#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
```

フェールオーバー後。

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

5757 bytes copied in 0.60 secs
[OK]

Switching to Active
```

IPは変更されますが、MACは同じです。

<#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
```

ここでは、ルータがARPエントリをどのように更新するかを確認できますが、FTD HAの背後にあるホストについては同じものを更新しないため、停止します。

<#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
```

スイッチオーバー時に、接続されたインターフェイスに対して、ASAはMAC/新しいIPを使用してGARPを送信し、スイッチまたはゲートウェイルータがそれを更新します。ただし、変換されたIPアドレスのGARPがないため、ルータからの戻りパケットはスタンバイになったMACアドレスを使用して転送を続けますが、IPアドレスはアクティブなASAを指しています。

したがって、NAT変換されたIPアドレスにはGARPが必要です。

解決方法

停止を回避するには、変換されたIPをサブネットインターフェイスに含めないようにし、ゲートウェイからのルートを用意する必要があります。これは問題なく動作します。この例では、変換されたIPアドレスは172.16.100.0/24サブネットの範囲外である必要があります。

関連情報

- テクニカル サポートとドキュメント - Cisco Systems
- ASAvおよびSR-IOVインターフェイスプロビジョニング
- フェールオーバーのMACアドレスとIPアドレス
- Cisco適応型セキュリティ仮想アプライアンス(ASAv)スタートアップガイド、9.8

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。