투명 모드에서 HSRP 라우터를 사용한 ASA 고가용성 MAC 테이블 동기화 이해

목차

소개

이 문서에서는 HSRP를 사용하는 라우터 클러스터에 연결된 ASA 쌍의 동작에 대해 설명합니다.

사전 요구 사항

- ASA(Adaptive Security Appliance)
- ASA HA(고가용성).
- HSRP(Hot Standby Router Protocol).
- 투명 모드의 방화벽.

사용되는 구성 요소

- HSRP가 포함된 CSR 라우터 2개
- HSRP 쌍을 가리키는 HA에 구성된 2 ASA.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

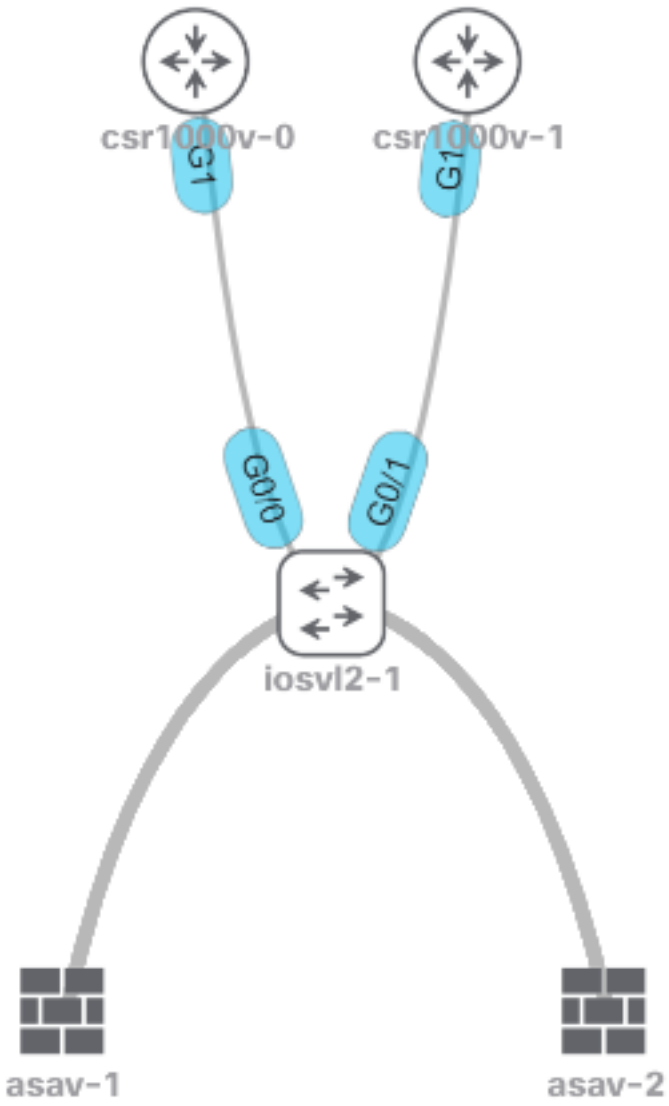
배경 정보

고가용성 투명 모드로 구성된 한 쌍의 ASA의 경우, 한 쌍의 방화벽이 라우터 클러스터에 업스트림으로 연결되고 인접한 라우터가 HSRP를 사용하는 경우, 방화벽의 트래픽은 특정 라우터의 MAC 주소를 가리키는 라우터 IP 주소로 연결됩니다. 그러나 반환 트래픽이 HSRP 쌍에 있는 다른 라우터 인터페이스의 MAC 주소에서 소싱되면 네트워크 중단이 발생할 수 있습니다.

문제는 mac-address-table 기간 시간 제한이 5분(300초)이며 ARP(Address Resolution Protocol) 시간 제한이 기본적으로 14400초라는 것입니다. 다음 홉 라우터는 HSRP를 사용하므로 HSRP MAC

주소에서 오는 트래픽은 없습니다. 이 경우 ASA의 mac-address-table 항목이 만료되고 트래픽이 실패합니다.

네트워크 다이어그램



문제 해결

HSRP를 사용하는 투명 모드의 ASA HA에 대한 MAC 테이블 동기화 이해

이러한 출력은 액티브 유닛이 새 항목을 학습하고 기존 엔트리를 삭제할 때 ASA 유닛이 MAC 테이블을 동기화하는 방법을 보여줍니다.

액티브 유닛 **asav-1은 HSRP** 라우터 중 하나(이 경우 csr1000**v-0)**에서 5254.0017.**8a8c** MAC 주소를 잃습니다.

```
ASAv-primary# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
```

```
----
outside 5254.0017.8a8c dynamic 1 1
inside 5254.001f.dfa8 dynamic 1 1
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

당신은 5분 후에 5254.0017.8a8c가 어떻게 사라지는지 알 수 있습니다.

```
ASAv-primary# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

스탠바이 유닛에서 5254.0017.8a8c MAC 항목이 손실되지 않습니다. 그러나 이 행동은 혼란을 야기할 수 있지만, 그것은 전적으로 기대됩니다.

스탠바이 유닛은 새 액티브 유닛이 되지 않는 한 MAC 주소 테이블을 업데이트하지 않습니다.

스탠바이 유닛은 몇 시간 후 5254.0017.8a8c를 유지하며 항상 1분의 나이를 유지합니다.

```
ASAv-secondary(config)# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
outside 5254.0017.8a8c dynamic 1 1
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

시간/일을 기다린 다음 동일한 명령을 실행하고 동일한 결과를 확인할 수 있습니다.

```
ASAv-secondary(config)# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
outside 5254.0017.8a8c dynamic 1 1
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

또한 show failover 이 명령을 사용하면 활성 유닛에서 HSRP 항목이 손실될 때 L2BRIDGE Tbl 카운터에 변경 사항이 없습니다.

```
Stateful Failover Logical Update Statistics
Link : failoverlink GigabitEthernet0/3 (up)
Stateful Obj xmit xerr rcv rerr
General 86751 0 77968 8
sys cmd 77854 0 77853 0
up time 0 0 0 0
RPC services 0 0 0 0
<--- More --->

TCP conn 0 0 0 0
UDP conn 8882 0 90 0
ARP tbl 4 0 1 0
```

```
L2BRIDGE Tbl 3 0 22 0
Xlate_Timeout 0 0 0 0
IPv6 ND tbl 0 0 0 0
SIP Session 0 0 0 0
SIP Tx 0 0 0 0
SIP Pinhole 0 0 0 0
Route Session 8 0 0 8
```

비대칭 라우팅으로 인해 MAC 주소 테이블 항목의 에이징 아웃

트래픽이 투명 방화벽을 통해 두 MAC 주소 간에 직접 흐르는 경우, ASA가 트래픽을 전송하는 두 MAC 주소에서 소싱된 프레임을 수신하므로 이러한 주소는 트래픽이 흐르는 동안 에이징되지 않습니다.

트래픽 흐름이 비대칭인 경우 ASA가 특정 MAC 주소에서 응답을 받지 못하면 항목이 시간 초과됩니다.

> **참고:** 비대칭 라우팅이란 ASA에서 특정 MAC 주소로 이동하는 트래픽을 확인하지만, 동일한 MAC 주소에서 오는 트래픽은 확인하지 않습니다

이 문제의 증상은 ASA가 MAC 주소 엔트리를 에이징한 후(해당 MAC 주소에서 오는 트래픽이 없는 5분 후) MAC 엔트리가 다시 채워질 때까지 해당 MAC 주소로 향하는 트래픽이 삭제됩니다.

일반적으로 한 두 번 시도한 후 서버에 대한 연결이 다시 설정되는 경우 문제가 발생합니다. 첫 번째 패킷이 삭제되어 ASA에서 MAC 주소의 위치를 확인하는 단계를 거칠 수 있기 때문입니다.

제안 솔루션

이 문제를 해결하려면 방화벽의 HSRP IP에 대한 고정 MAC 주소 항목 테이블을 추가하거나, 항목 시간이 초과되기 전에 해당 HSRP 라우터에서 ARP 응답이 오도록 사용 기간을 특정 값으로 늘립니다.

ASA가 HSRP 활성 라우터에서 ARP 응답을 수신하는지 확실하지 않으므로 더 나은 해결책은 고정 MAC 항목을 추가하는 것입니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems

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.