ASA 사이트 간 투명 클러스터의 일반적인 문제

목차

이 문서에서는 Spanned EtherChannel 투명 모드 사이트 간 클러스터의 몇 가지 일반적인 문제에 대해 설명합니다.

.

- ASA(Adaptive Security Appliance) 방화벽
- ASA 클러스터링

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

배경 정보

ASA 버전 9.2부터 사이트 간 클러스터링이 지원되는데, 이 경우 ASA 유닛이 서로 다른 데이터 센터에 위치할 수 있고 CACL(Cluster Control Link)이 DCI(Data Center Interconnect)를 통해 연결됩니다. 가능한 구축 시나리오는 다음과 같습니다.

- 개별 인터페이스 사이트 간 클러스터
- Spanned EtherChannel 투명 모드 사이트 간 클러스터
- Spanned EtherChannel 라우팅 모드 사이트 간 클러스터(9.5부터 지원됨)

MAC MOVE 알림

CAM(Content Addressable Memory) 테이블의 MAC 주소가 포트를 변경하면 MAC MOVE 알림이 생성됩니다.그러나 CAM 테이블에서 MAC 주소를 추가하거나 제거할 경우 MAC MOVE 알림이 생성되지 않습니다.VLAN10에서 인터페이스 GigabitEthernet0/1을 통해 MAC 주소 X를 학습하고 VLAN 10의 GigabitEthernet0/2를 통해 동일한 MAC을 확인한 후 MAC MOVE 알림이 생성된다고 가정합니다.

스위치의 Syslog:

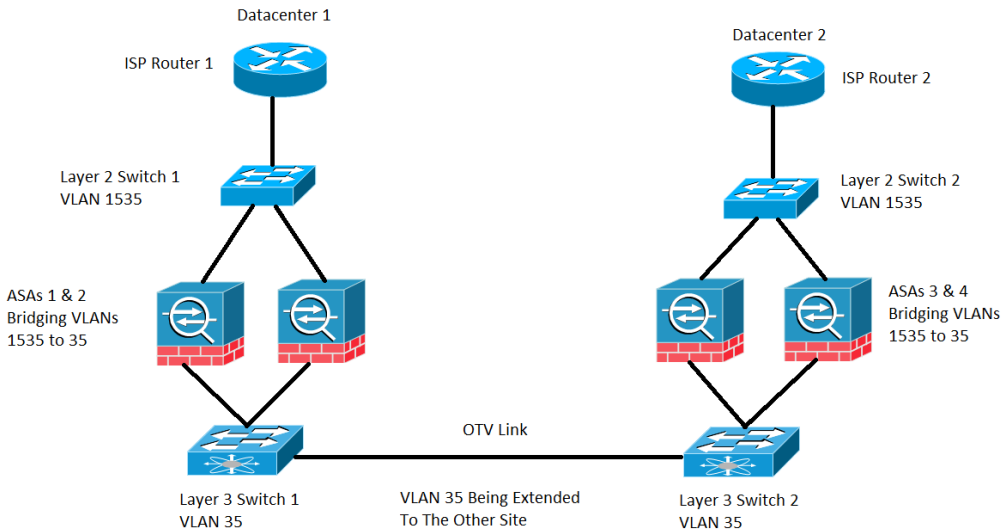
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1
to GigabitEthernet0/2
```

ASA의 Syslog:

```
ASA-4-412001: MAC 003a.7b58.24c5 moved from DMZ to INSIDE
```

네트워크 다이어그램

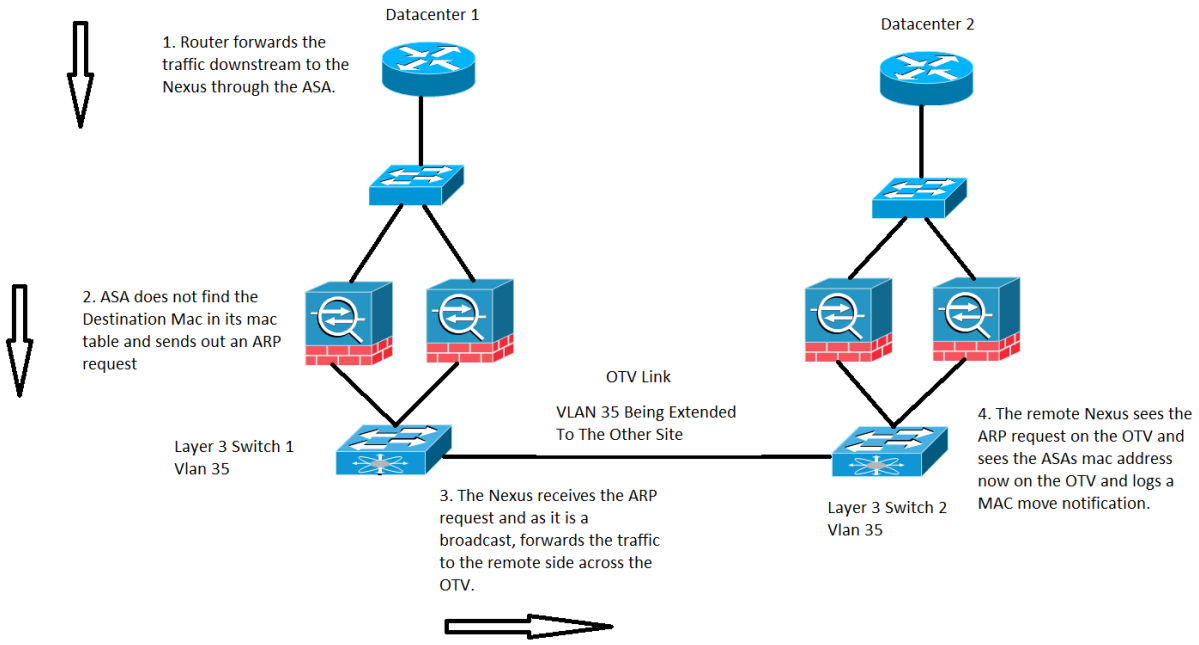
ASA가 투명 모드 브리징 VLAN 1535 및 VLAN 35로 구성된 사이트 간 클러스터 구축. 내부 VLAN 35는 OTV(Overlay Transport Virtualization)를 통해 확장되는 반면 외부 VLAN 1535는 OTV를 통해 확장되지 않습니다(이미지 참조).



스위치의 MAC 이동 알림

시나리오 1

이미지에 표시된 것처럼 ASA의 MAC 테이블에 항목이 없는 MAC 주소로 이동하는 트래픽:



투명 ASA에서 ASA에 도착하는 패킷의 대상 MAC 주소가 mac-address 테이블에 없는 경우 해당 대상(BVI와 동일한 서브넷에 있는 경우)에 대한 ARP(Address Resolution Protocol) 요청 또는 소스 TTL(Time To Live 1)을 Bridge BVI(Virtual Interface)로 소스 TTL(ICMP 1)로 전송합니다.) MAC 주소 및 목적지 MAC 주소(DMAC)가 누락되었습니다.

앞의 경우에는 다음과 같은 트래픽 플로우가 있습니다.

1. 데이터 센터 1의 ISP 라우터는 ASA 뒤에 있는 특정 대상에 트래픽을 전달합니다.
2. ASA에서 트래픽을 수신할 수 있으며 이 경우 트래픽의 대상 MAC 주소를 ASA에서 알지 못합니다.
3. 이제 트래픽의 대상 IP가 BVI와 동일한 서브넷에 있으며 앞에서 설명한 대로 ASA가 대상 IP에 대한 ARP 요청을 생성합니다.
4. 스위치 1은 트래픽을 수신하며, 요청은 브로드캐스트이므로 OTV 링크를 통해 트래픽을 데이터 센터 2로 전달합니다.
5. 스위치 2가 OTV 링크의 ASA에서 ARP 요청을 볼 때, 이전에 ASA의 MAC 주소가 직접 연결된 인터페이스를 통해 학습되어 이제 OTV 링크를 통해 학습되기 때문에 MAC MOVE 알림을 기록합니다.

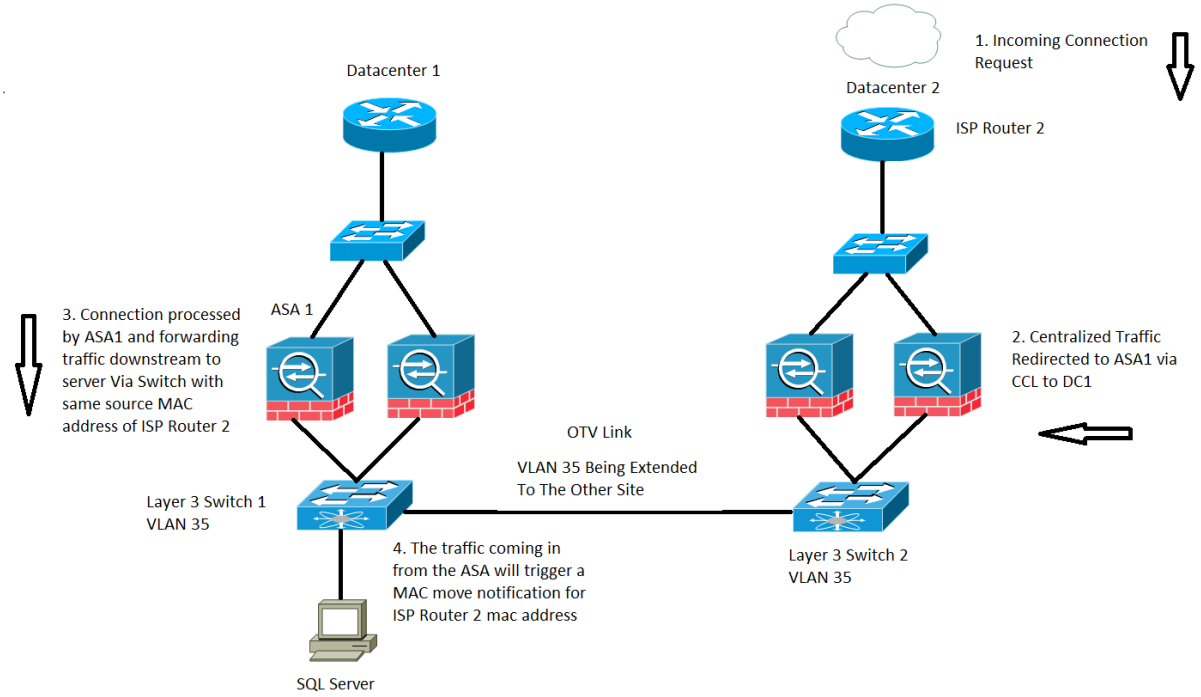
권장 사항

코너 시나리오입니다. MAC 테이블은 클러스터에서 동기화되므로 멤버가 특정 호스트에 대한 항목

을 갖지 않을 가능성이 낮습니다.클러스터 소유 BVI MAC에 대한 비정기적인 MAC 이동이 허용되는 것으로 간주됩니다.

시나리오 2

이미지에 표시된 대로 ASA를 통한 중앙 집중식 플로우 처리:



ASA 클러스터 전체의 검사 기반 트래픽은 다음 세 가지 유형으로 분류됩니다.

- 중앙 집중식
- 분산
- 반분산

중앙 집중식 검사의 경우 검사를 받아야 하는 모든 트래픽은 ASA 클러스터의 마스터 유닛으로 리디렉션됩니다.ASA 클러스터의 슬레이브 유닛에서 트래픽을 수신하면 CCL을 통해 마스터에 전달됩니다.

이전 이미지에서 CIP(Centralized Inspection Protocol)인 SQL 트래픽과 함께 작업하며 여기에 설명된 동작은 모든 CIP에 적용할 수 있습니다.

ASA 클러스터의 슬레이브 유닛만 있는 데이터 센터 2에서 트래픽을 수신하고 마스터 유닛은 ASA 1인 데이터 센터 1에 있습니다.

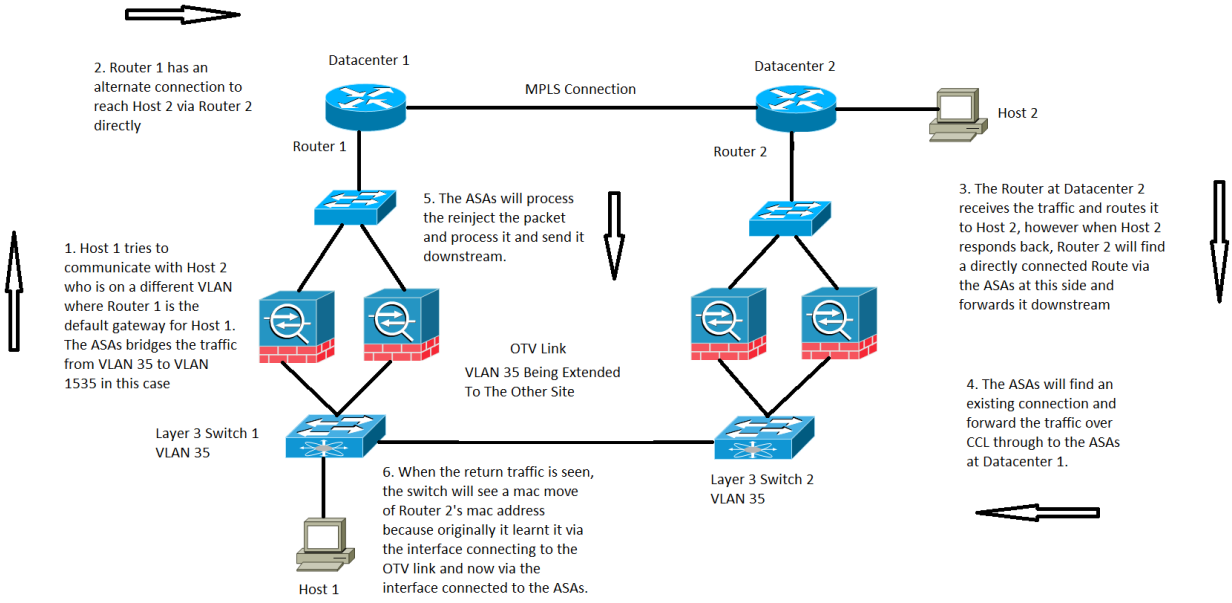
1. 데이터 센터 2의 ISP 라우터 2가 트래픽을 수신하여 다운스트림으로 사이트의 ASA에 전달합니다.
2. ASA 중 하나는 이 트래픽을 수신할 수 있으며, 일단 이 트래픽을 검사해야 한다고 판단하면 프로토콜이 중앙 집중화되면 CCL을 통해 트래픽을 마스터 유닛으로 전달합니다.
3. ASA 1은 CCL을 통해 트래픽 흐름을 수신하고 트래픽을 처리하고 SQL Server로 다운스트림으로 전송합니다.

4. 이제 ASA 1이 트래픽 다운스트림을 전달할 때 데이터 센터 2에 있는 ISP 라우터 2의 원본 소스 MAC 주소를 유지하고 다운스트림으로 전송합니다.
5. 스위치 1은 이 특정 트래픽을 수신하면 MAC MOVE 알림에 로그인합니다. 이는 원래 데이터 센터 2에 연결된 OTV 링크를 통해 ISP 라우터 2 MAC 주소를 확인하고 이제 ASA 1에 연결된 인터페이스에서 들어오는 트래픽을 볼 수 있기 때문입니다.

권장 사항

이미지에 표시된 것처럼, 중앙 집중식 연결을 마스터를 호스팅하는 사이트 호스트(우선 순위 기준)로 라우팅하는 것이 좋습니다.

시나리오 3



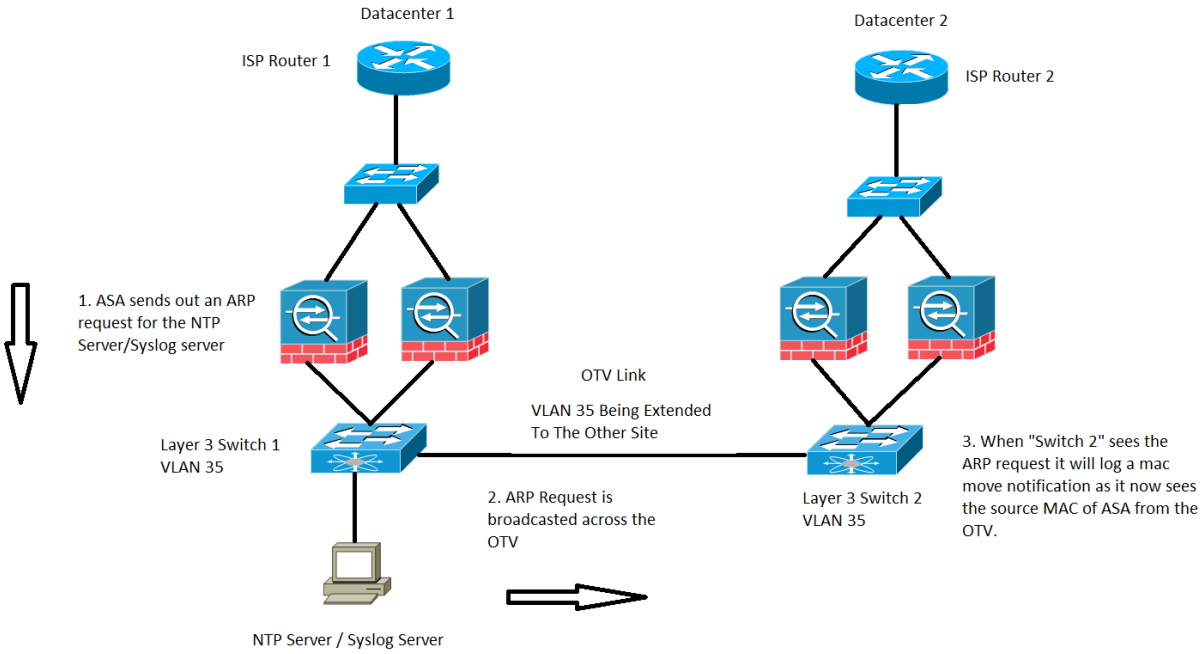
투명 모드의 DC(Inter Domain Controller) 통신의 경우 이 특정 트래픽 흐름은 적용 또는 문서화되지 않지만 이 특정 트래픽 흐름은 ASA 플로우 처리 관점에서 작동합니다.그러나 스위치에서 MAC 이동 알림을 생성할 수 있습니다.

1. VLAN 35의 호스트 1은 다른 데이터 센터에 있는 호스트 2와 통신을 시도합니다.
2. 호스트 1에는 라우터 1과 라우터 1이라는 기본 게이트웨이가 있으며, 대체 링크를 통해 라우터 2와 직접 통신할 수 있으므로 호스트 2에 도달하는 경로가 있습니다. 이 경우 ASA 클러스터를 통해서가 아니라 MPLS(Multiprotocol Label Switching)로 간주합니다.
3. 라우터 2는 수신 트래픽을 수신하고 이를 호스트 2로 라우팅합니다.
4. 이제 호스트 2가 다시 응답하면 라우터 2가 반환 트래픽을 수신하고 MPLS를 통해 전송하는 트래픽 대신 ASA를 통해 직접 연결된 경로를 찾습니다.
5. 이 단계에서는 라우터 2를 떠나는 트래픽에 라우터 2의 종료 인터페이스의 소스 MAC이 있습니다.
6. 데이터 센터 2의 ASA는 반환 트래픽을 수신하고 데이터 센터 1의 ASA에 의해 만들어지고 존재하는 연결을 찾습니다.
7. 데이터 센터 2의 ASA는 CCL을 통해 반환 트래픽을 데이터 센터 1의 ASA로 다시 전송합니다.
8. 이 단계에서 데이터 센터 1의 ASA는 반환 트래픽을 처리하고 스위치 1로 전달합니다. 패킷에는 라우터 2의 종료 인터페이스와 동일한 소스 MAC이 있습니다.

9. 이제 스위치 1이 패킷을 수신하면 MAC 이동 알림을 로깅합니다. 처음에는 OTV 링크에 연결된 인터페이스에서 라우터 2의 MAC 주소를 배웠기 때문입니다. 그러나 이 단계에서는 ASA에 연결된 인터페이스에서 MAC 주소를 학습하기 시작합니다.

시나리오 4

이미지에 표시된 대로 ASA에서 생성된 트래픽:

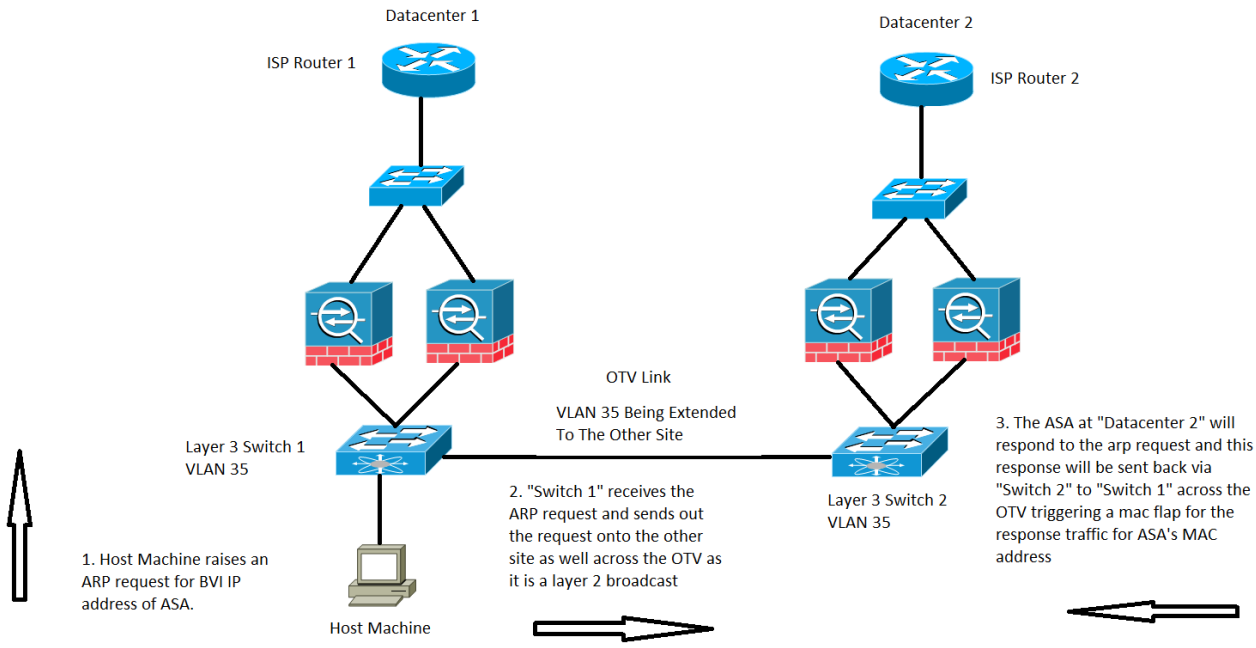


이 구체적인 사례는 ASA 자체에서 생성되는 모든 트래픽에 대해 관찰됩니다.여기서 두 가지 가능한 상황을 고려하는데, ASA가 BVI 인터페이스와 동일한 서브넷에 있는 NTP(Network Time Protocol) 또는 Syslog 서버에 연결하려고 시도합니다.그러나 이러한 두 가지 조건에 국한되지 않을 뿐만 아니라 BVI IP 주소에 직접 연결된 IP 주소에 대해 ASA에서 트래픽을 생성할 때마다 이러한 상황이 발생할 수 있습니다.

1. ASA에 NTP 서버/Syslog 서버의 ARP 정보가 없는 경우 ASA는 해당 서버에 대한 ARP 요청을 생성합니다.
2. ARP 요청이 브로드캐스트 패킷이므로 스위치 1은 ASA의 연결된 인터페이스에서 이 패킷을 수신하고 OTV를 통한 원격 사이트를 포함하여 특정 VLAN의 모든 인터페이스에 플러딩합니다.
3. 원격 사이트 스위치 2는 OTV 링크에서 이 ARP 요청을 수신하며 ASA의 소스 MAC로 인해 ASA에 직접 연결된 로컬 인터페이스를 통해 OTV에서 동일한 MAC 주소를 학습하기 때문에 MAC 플랩 알림을 생성합니다.

시나리오 5

이미지에 표시된 대로 직접 연결된 호스트에서 ASA의 BVI IP 주소로 이동하는 트래픽:



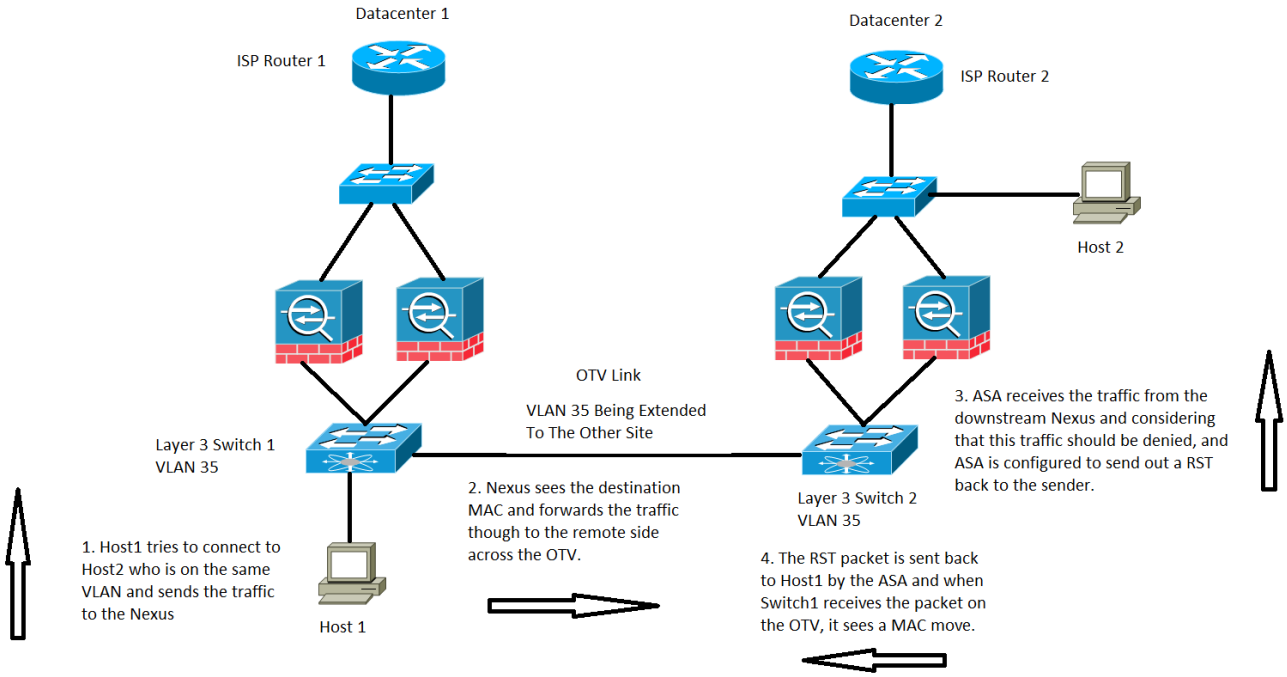
트래픽이 ASA의 BVI IP 주소로 이동하는 경우에도 MAC MOVE를 관찰할 수 있습니다.

이 시나리오에서는 ASA의 직접 연결된 네트워크에 Host Machine이 있으며 ASA에 연결하려고 시도합니다.

1. 호스트에 ASA의 ARP가 없으며 ARP 요청이 트리거됩니다.
2. Nexus는 트래픽을 수신하고 브로드캐스트 트래픽이므로 OTV를 통해 다른 사이트로 트래픽을 전송합니다.
3. 원격 데이터 센터 2의 ASA는 ARP 요청에 응답할 수 있으며, 원격 측의 스위치 2, 로컬 측의 스위치 1, 그리고 최종 호스트의 스위치 1과 같은 경로를 통해 트래픽을 다시 전송할 수 있습니다.
4. 로컬 측 스위치 1에서 ARP 응답이 확인되면 OTV 링크에서 수신되는 ASA의 MAC 주소를 볼 때 MAC 이동 알림이 트리거됩니다.

시나리오 6

ASA는 다음과 같이 호스트에 RST를 전송하는 트래픽과 함께 트래픽을 거부하도록 설정됩니다.



이 경우 VLAN 35에 호스트 호스트 1이 있고, 동일한 레이어 3 VLAN에서 호스트 2와 통신하려고 하지만, 실제로 호스트 2는 데이터 센터 2 VLAN 1535에 있습니다.

1. ASA에 연결된 인터페이스를 통해 스위치 2에서 호스트 2MAC 주소가 표시됩니다.
2. 스위치 1에는 OTV 링크를 통해 호스트 2의 MAC 주소가 표시됩니다.
3. 호스트 1은 호스트 2로 트래픽을 전송하며, 이는 데이터 센터 2의 스위치 1, OTV, 스위치 2, ASA의 경로를 따릅니다.
4. ASA에서 이 특정 항목을 거부하며, ASA가 RST를 호스트 1로 다시 전송하도록 구성되면 RST 패킷이 ASA의 소스 MAC 주소와 함께 다시 옵니다.
5. 이 패킷이 OTV를 통해 스위치 1로 다시 이동하면 스위치 1은 OTV에서 MAC 주소를 볼 수 있으므로 ASA의 MAC 주소에 대한 MAC MOVE 알림을 로깅합니다. OTV에서 MAC 주소를 볼 수 있으며, 여기서 MAC 주소는 직접 연결된 인터페이스에서 주소를 볼 수 있습니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

- Cisco ASA Series CLI 컨피그레이션 가이드
- 기술 지원 및 문서 – Cisco Systems