Gemeenschappelijke problemen met ASA intersite Transparent Cluster

Inhoud

Inleiding

Dit document beschrijft een aantal gemeenschappelijke problemen met de Spanning EtherChannel Transparent Mode Inter-Site-cluster.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Adaptieve security applicatie (ASA) firewall
- ASA-clustering

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Met ingang van ASA versie 9.2 wordt clustering tussen sites ondersteund, waarbij de ASA-eenheden zich in verschillende datacenters kunnen bevinden en de Cluster Control Link (CCL) is verbonden via een Data Center Interconnect (DCI). De mogelijke inzetscenario's zijn:

- Individuele interface voor intersite cluster
- Spanning EtherChannel Transparent Mode Inter-Site Cluster
- Spanning EtherChannel Routed Mode Inter-Site Cluster (ondersteund vanaf 9.5)

MAC-BEWEGINGEN

Wanneer een MAC-adres in de CAM-tabel (Content Adressable Memory) poort verandert, wordt er een MAC MOVE-melding gegenereerd. Er wordt echter geen MAC MOVE-melding gegenereerd wanneer het MAC-adres is toegevoegd of verwijderd in de CAM-tabel. Stel dat een MAC-adres X via interface Gigabit Ethernet0/1 in VLAN10 wordt geleerd en dat na enige tijd dezelfde MAC door Gigabit Ethernet0/2 in VLAN 10 wordt gezien, dan wordt er een MAC MOVE-bericht gegenereerd.

Van switch:

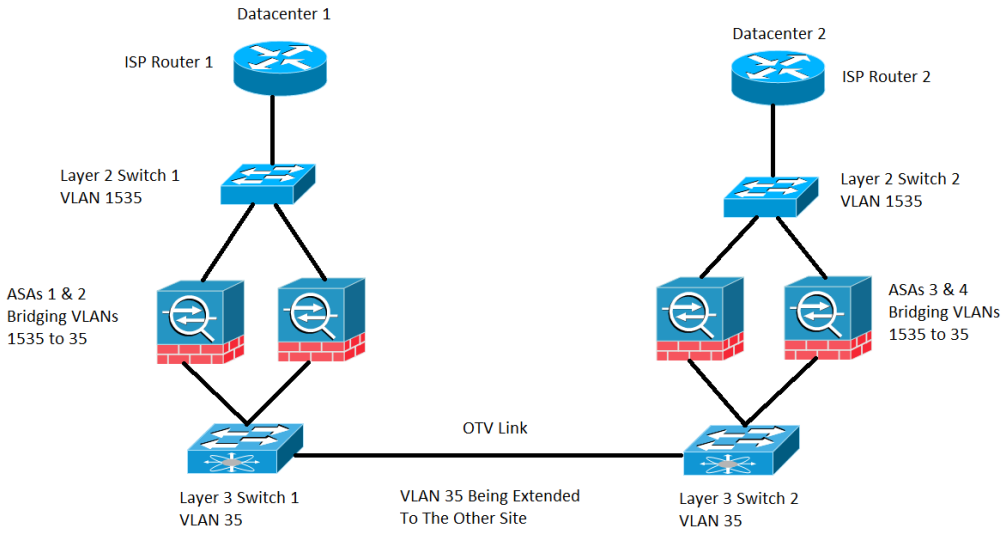
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1
to GigabitEthernet0/2
```

Syslog van ASA:

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

Netwerkdiagram

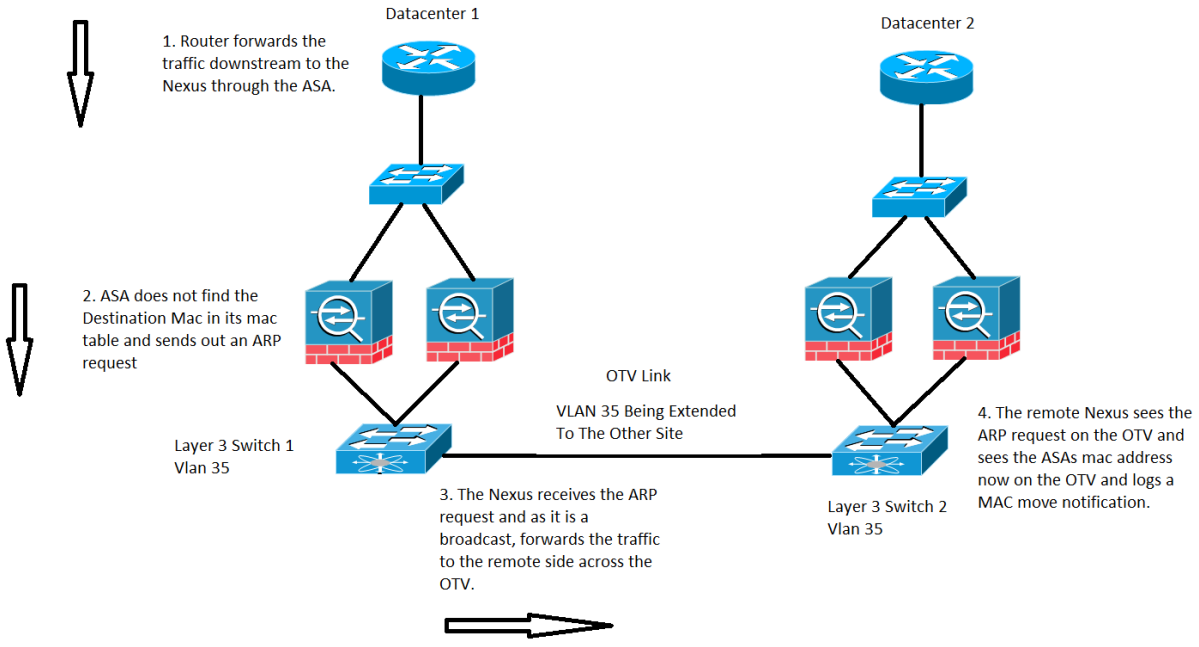
Inter-site clusterimplementatie waarbij de ASA's worden geconfigureerd in transparante modus door VLAN 1535 en VLAN 35 te overbruggen. De binnenkant VLAN 35 wordt uitgebreid over de Overlay Transport Virtualization (OTV) terwijl het externe VLAN 1535 niet uitgebreid wordt via OTV, zoals in de afbeelding wordt getoond



MAC-bewegingsmeldingen op switch

Scenario 1

Verkeer bestemd voor een MAC-adres waarvan de vermelding niet aanwezig is in de ASA MAC-tabel, zoals in de afbeelding wordt weergegeven:



In een transparante ASA, als het bestemmings-MAC-adres van het pakket dat op de ASA

aankomt niet in de mac-adrestabel is, stuurt het een protocol (ARP)-aanvraag voor adresresolutie voor die bestemming (indien in hetzelfde subnet als BVI) of een ICMP-verzoek Internet Control Message Protocol (Time To Live 1(TTL 1) met bron-MAC als Bridge Virtual Interface (BVI) adres en bestemming MAC-adres als Destination Media Access Controller (DMAC) wordt gemist.

In het voorgaande geval, heb je deze verkeersstroom:

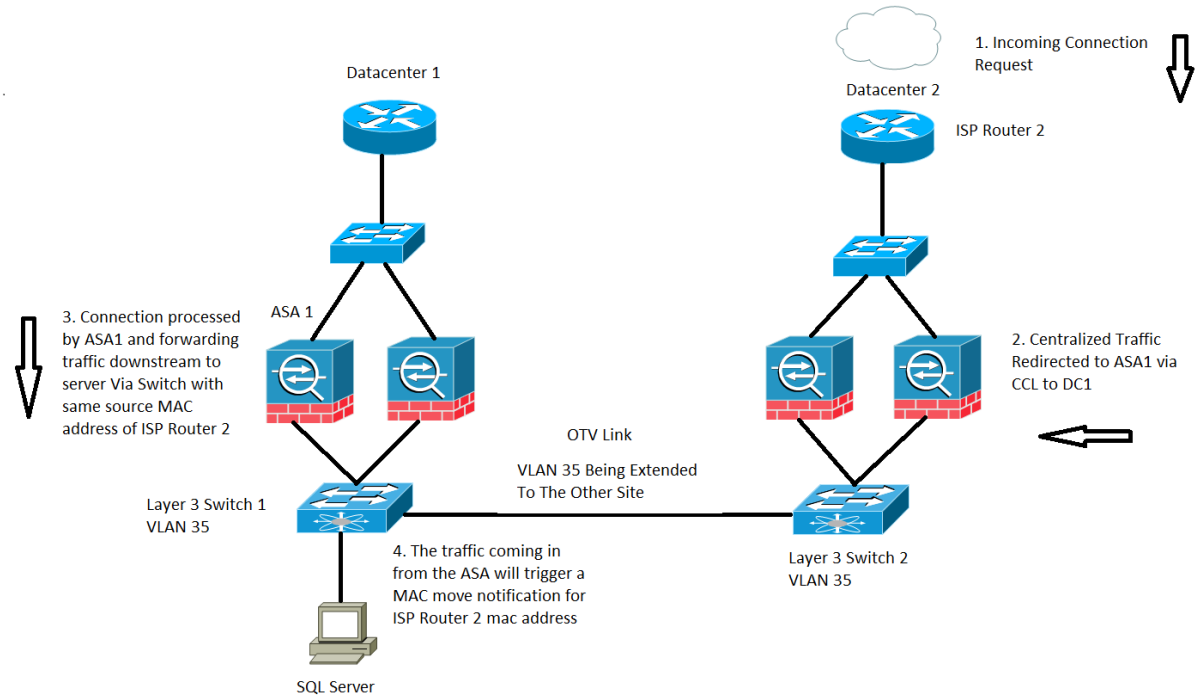
1. De ISP router op Datacenter 1 verstuurt verkeer naar een specifieke bestemming die achter de ASA ligt.
2. Een van de ASA's kan het verkeer ontvangen en in dit geval is het MAC-adres van de bestemming van het verkeer niet bekend door de ASA.
3. Nu is de bestemming IP van het verkeer in zelfde voorwerp als die van BVI en zoals eerder vermeld, produceert ASA nu een ARP verzoek voor de bestemming IP.
4. Schakelaar 1 ontvangt het verkeer en aangezien het verzoek een uitzending is, zendt het het verkeer naar Datacenter 2 evenals over de OTV verbinding door.
5. Wanneer switch 2 het ARP-verzoek van de ASA op de OTV-link ziet, noteert het een MAC MOVE-melding omdat het MAC-adres van de ASA voorheen via een direct aangesloten interface werd geleerd en nu wordt het geleerd via de OTV-link.

Aanbevelingen

Het is een hoekscenario. MAC-tabellen zijn gesynchroniseerd in clusters, dus is het minder waarschijnlijk dat een lid geen vermelding heeft voor een bepaalde host. Een incidentele MAC-zet voor een clusterBVI MAC wordt aanvaardbaar geacht.

Scenario 2

Gecentraliseerde stroomverwerking door ASA, zoals in de afbeelding getoond:



Op inspectie gebaseerd verkeer over een ASA-cluster is ingedeeld in drie typen:

- Gecentraliseerd
- Gedistribueerd
- semigedistribueerd

In het geval van gecentraliseerde inspectie wordt elk verkeer dat geïnspecteerd moet worden, omgeleid naar de master-unit van het ASA-cluster. Als een slaafse eenheid van het ASA-cluster het verkeer ontvangt, wordt het aan de kapitein doorgestuurd via de CCL.

In de vorige afbeelding werkt u met SQL-verkeer dat een Gecentraliseerde Inspection Protocol (CIP) is en het hier beschreven gedrag is van toepassing op elke CIP.

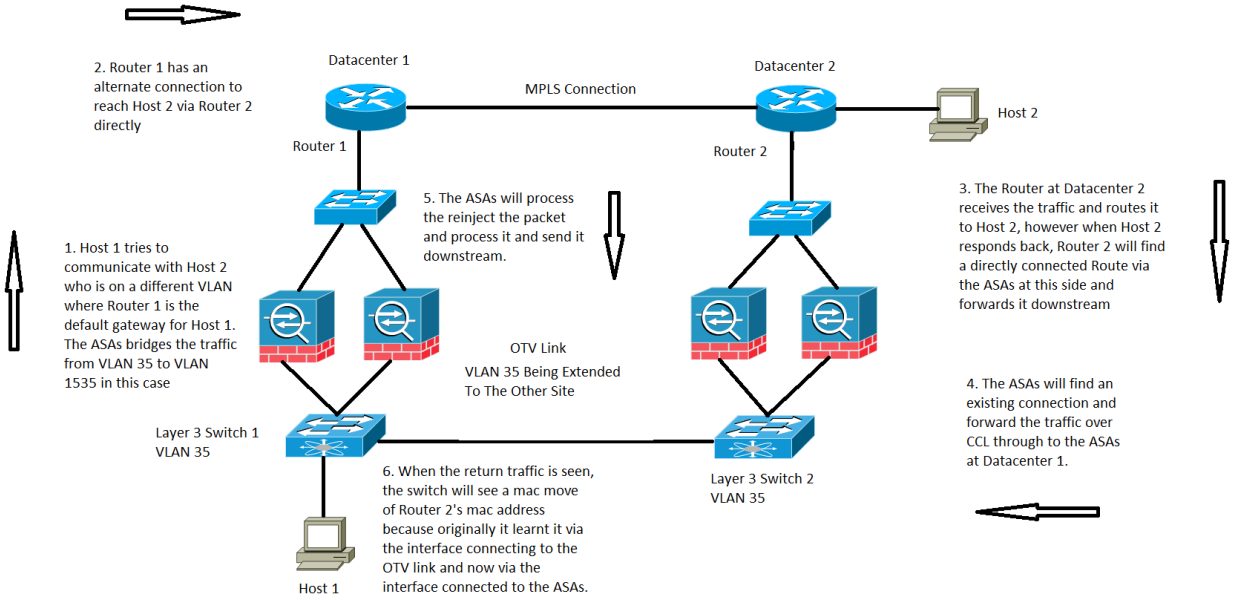
U ontvangt het verkeer op Datacenter 2 waar u alleen slave eenheden van de ASA cluster hebt, is de master unit op Datacenter 1, dat ASA 1 is.

1. ISP Router 2 op Datacenter 2 ontvangt het verkeer en zendt het stroomafwaarts naar de ASA's op zijn site.
2. Elk van de ASA's kan dit verkeer ontvangen en zodra het bepaalt dat dit verkeer geïnspecteerd moet worden en wanneer het protocol gecentraliseerd is, stuurt het het verkeer via de CCL door naar de master unit.
3. ASA 1 ontvangt de verkeersstroom via de CCL, verwerkt het verkeer en stuurt het stroomafwaarts naar de SQL Server.
4. Wanneer ASA 1 het verkeer stroomafwaarts vooruitstuurt, behoudt het het oorspronkelijke Bron Mac-adres van ISP Router 2, dat zich op Datacenter 2 bevindt en het stroomafwaarts stuurt.
5. Wanneer switch 1 dit specifieke verkeer ontvangt, logt het in een MAC MOVE-kennisgeving omdat het oorspronkelijk ISP Router 2 MAC-adres ziet via de OTV-link die is aangesloten op Datacenter 2 en nu het verkeer ziet dat binnenkomt uit de interfaces die zijn aangesloten op de ASA 1.

Aanbevelingen

Aanbevolen wordt om gecentraliseerde verbindingen te leiden naar welke locatiehosts de master (gebaseerd op prioriteiten), zoals in de afbeelding wordt getoond:

Scenario 3

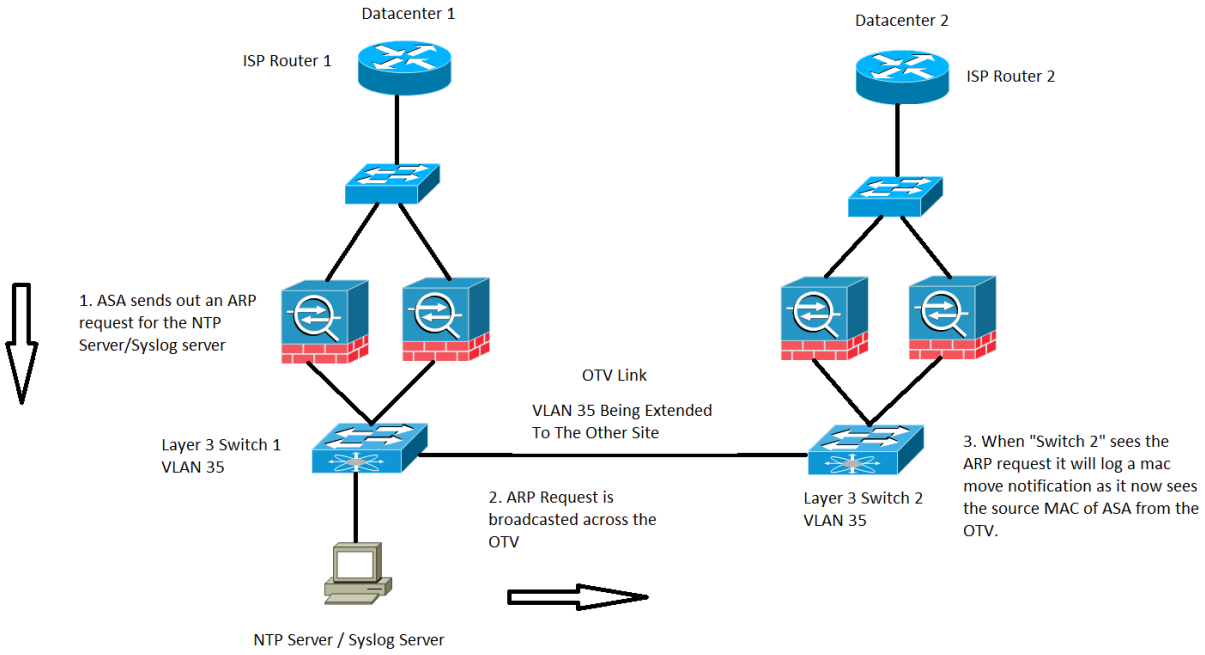


Voor een communicatie tussen Domain Controller (DC) in transparante modus wordt deze specifieke verkeersstroom niet gedekt of gedocumenteerd, maar deze specifieke verkeersstroom werkt vanuit een ASA-stroomverwerkingsstandpunt. Dit kan echter resulteren in MAC-bewegingsmeldingen op de switch.

1. Host 1 op VLAN 35 probeert met Host 2 te communiceren dat op het andere Datacenter aanwezig is.
2. Host 1 heeft een standaardgateway die router 1 is en Router 1 heeft een pad om Host 2 te bereiken door met router 2 direct over een alternatieve link te kunnen communiceren en in dit geval gaan we ervan uit dat Multiprotocol Label Switching (MPLS) en niet door de ASA-cluster.
3. Router 2 ontvangt het inkomende verkeer en routeert het naar Host 2.
4. Wanneer Host 2 terugreageert, ontvangt Router 2 het retourverkeer en vindt het een direct aangesloten route door de ASA's in plaats van het verkeer dat het via de MPLS verstuurt.
5. In dit stadium heeft het verkeer dat router 2 verlaat de bron MAC van de exit interface van router 2.
6. De ASA's bij Datacenter 2 ontvangen het retourverkeer en vinden een verbinding die bestaat en wordt gemaakt door de ASA's op Datacenter 1.
7. De ASA's bij Datacenter 2 sturen het retourverkeer via CCL terug naar de ASA's bij Datacenter 1.
8. In dit stadium verwerken de ASA's bij Datacenter 1 het retourverkeer en sturen het naar Switch 1. Het pakket heeft nog steeds dezelfde bron MAC als de exit interface van Router 2.
9. Wanneer Switch 1 het pakket ontvangt, logt het een MAC-bewegingskennisgeving omdat het aanvankelijk het MAC-adres van Router 2 van de interface leerde die is aangesloten op de OTV-link. In dit stadium begint het echter het MAC-adres te leren van de interface die is aangesloten op de ASA's.

Scenario 4

Door de ASA gegenereerd verkeer, zoals in de afbeelding wordt getoond:

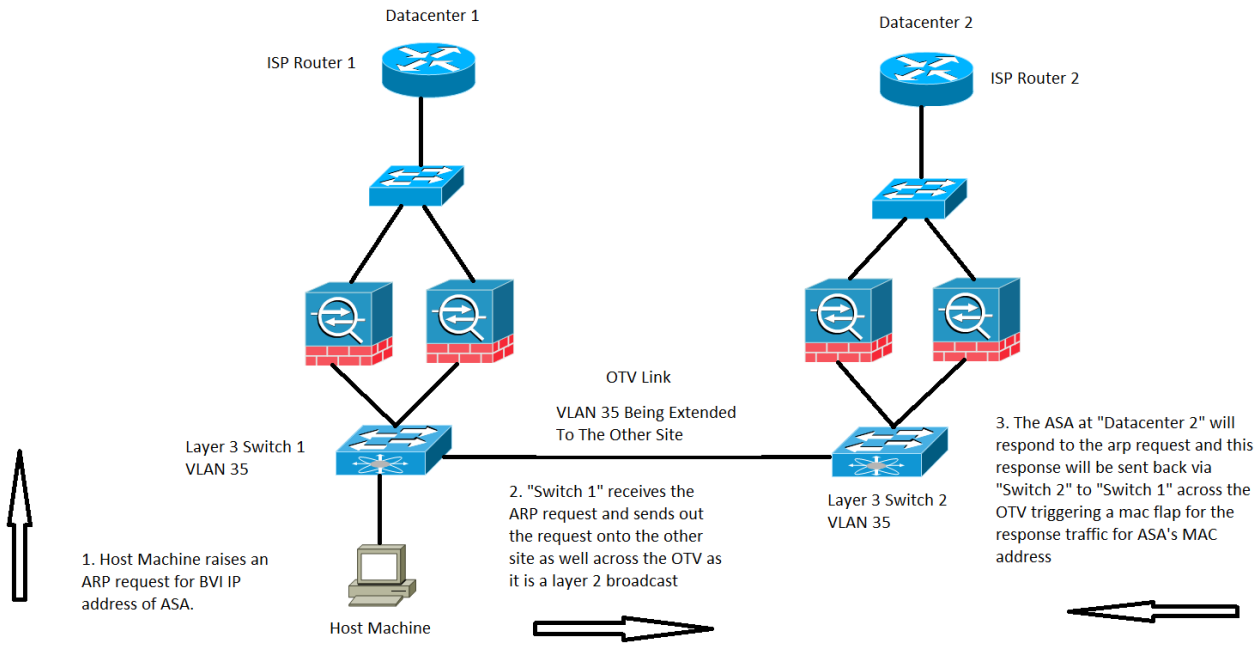


Dit specifieke geval zal worden waargenomen voor elk verkeer dat door de ASA zelf wordt gegenereerd. Hier worden twee mogelijke situaties overwogen, waarbij de ASA probeert een Network Time Protocol (NTP) of een Syslog server te bereiken, die op dezelfde subnet zijn als de BVI-interface. Hoewel de ASA zich niet alleen tot deze twee voorwaarden beperkt, kan deze situatie zich voordoen wanneer er door de ASA verkeer gegenereerd wordt voor een IP-adres dat direct verbonden is met de BVI IP-adressen.

1. Als ASA niet de ARP informatie van de NTP server/Syslog server heeft dan zal de ASA een ARP verzoek voor die server genereren.
2. Aangezien het ARP-verzoek een broadcast-pakket is, zal de switch 1 dit pakket ontvangen vanuit de aangesloten interface van de ASA en de OTV-indeling overspoelen naar alle interfaces in het specifieke VLAN, inclusief de externe site via de OTV.
3. De Remote Site Switch 2 zal dit ARP-verzoek van de OTV-link ontvangen en door de bron MAC van de ASA genereert het een MAC-flap-melding omdat hetzelfde MAC-adres via de lokale direct aangesloten interfaces op de ASA wordt geleerd.

Scenario 5

Verkeer bestemd voor BVI IP-adres van de ASA vanaf een direct aangesloten host, zoals in de afbeelding:



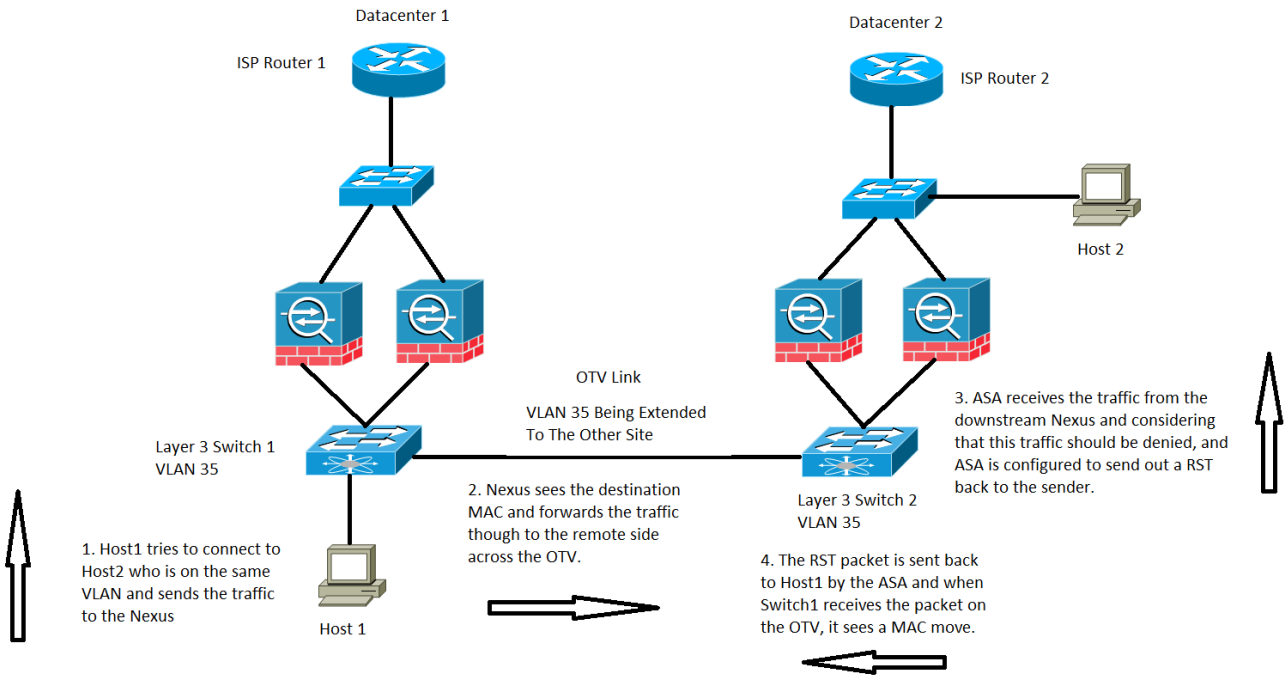
Een MAC MOVE kan ook worden waargenomen op tijden dat het verkeer is bestemd voor het ASA BVI IP-adres.

In het scenario hebben we een hostmachine op een direct aangesloten netwerk van de ASA en proberen we verbinding te maken met de ASA.

1. De host heeft niet het ARP van de ASA en voert een ARP-aanvraag in.
2. De Nexus ontvangt het verkeer en ook weer omdat het een uitzendverkeer is, wordt het verkeer via de OTV naar de andere site verzonden.
3. ASA op het externe Datacenter 2 kan reageren op het ARP-verzoek en het verkeer terugsturen door hetzelfde pad dat Switch 2 op de afstandszijde is, OTV, Switch 1 op de lokale zijde en dan de eindhost.
4. Wanneer de ARP-respons op de lokale side Switch 1 wordt gezien, wordt er een MAC-verplaatsing-kennisgeving gestart omdat het MAC-adres van de ASA wordt weergegeven dat via de OTV-link wordt ontvangen.

Scenario 6

ASA was ingesteld om verkeer te ontkennen waarmee het een RST naar de Host stuurt, zoals in de afbeelding wordt getoond:



In dit geval, hebben we een host Host 1 op VLAN 35, probeert het te communiceren met Host 2 in hetzelfde Layer 3 VLAN, echter Host 2 is feitelijk op Datacenter 2 VLAN 1535.

1. Host 2MAC-adres wordt gezien op Switch 2 via de interface die wordt aangesloten op de ASA's.
2. Switch 1 zou het MAC-adres van Host 2 zien via de OTV-link.
3. Host 1 verstuurt verkeer naar host 2 en volgt het pad van switch 1, OTV, switch 2, ASA's op Datacenter 2.
4. Dit specifieke wordt ontkend door de ASA en aangezien ASA is ingesteld om een RST naar Host 1 terug te sturen, komt het RST-pakket terug met het MAC-adres van ASA.
5. Wanneer dit pakket het terug maakt om 1 over de OTV over te schakelen, noteert de schakelaar 1 een bericht van het MAC-station voor het adres van ASA omdat het nu het MAC-adres in OTV ziet, waar alvorens het adres van zijn direct aangesloten interface wordt weergegeven.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Cisco ASA Series CLI-configuratiegids
- Technische ondersteuning en documentatie – Cisco Systems