Problèmes courants liés au cluster transparent entre sites ASA

Contenu

Introduction

Ce document décrit certains des problèmes courants avec le cluster inter-site Spanning EtherChannel Transparent Mode.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Pare-feu ASA (Adaptive Security Appliance)
- Mise en grappe ASA

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Àpartir de la version 9.2 d'ASA, la mise en grappe inter-sites est prise en charge, dans laquelle les unités ASA peuvent être situées dans différents data centers et la liaison de contrôle de cluster (CCL) est connectée via une interconnexion de data center (DCI). Les scénarios de déploiement possibles sont les suivants :

- Cluster inter-sites d'interface individuelle
- Cluster inter-sites en mode transparent EtherChannel fractionné
- Cluster inter-sites en mode routé EtherChannel fractionné (pris en charge à partir de 9,5)

Notifications MAC MOVE

Lorsqu'une adresse MAC de la table Content Addressable Memory (CAM) change de port, une notification MAC MOVE est générée. Cependant, une notification MAC MOVE n'est pas générée lorsque l'adresse MAC est ajoutée ou supprimée de la table CAM. Supposons qu'une adresse MAC X soit apprise via l'interface GigabitEthernet0/1 dans VLAN10 et qu'après un certain temps le même MAC soit vu via GigabitEthernet0/2 dans VLAN 10, une notification MAC MOVE est générée.

Syslog du commutateur :

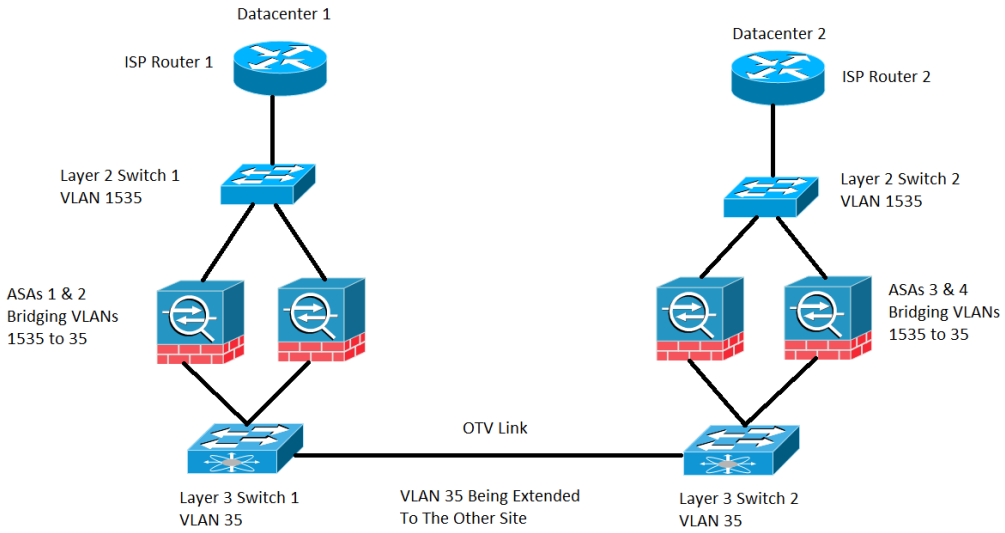
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1
to GigabitEthernet0/2
```

Syslog de ASA :

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

Diagramme du réseau

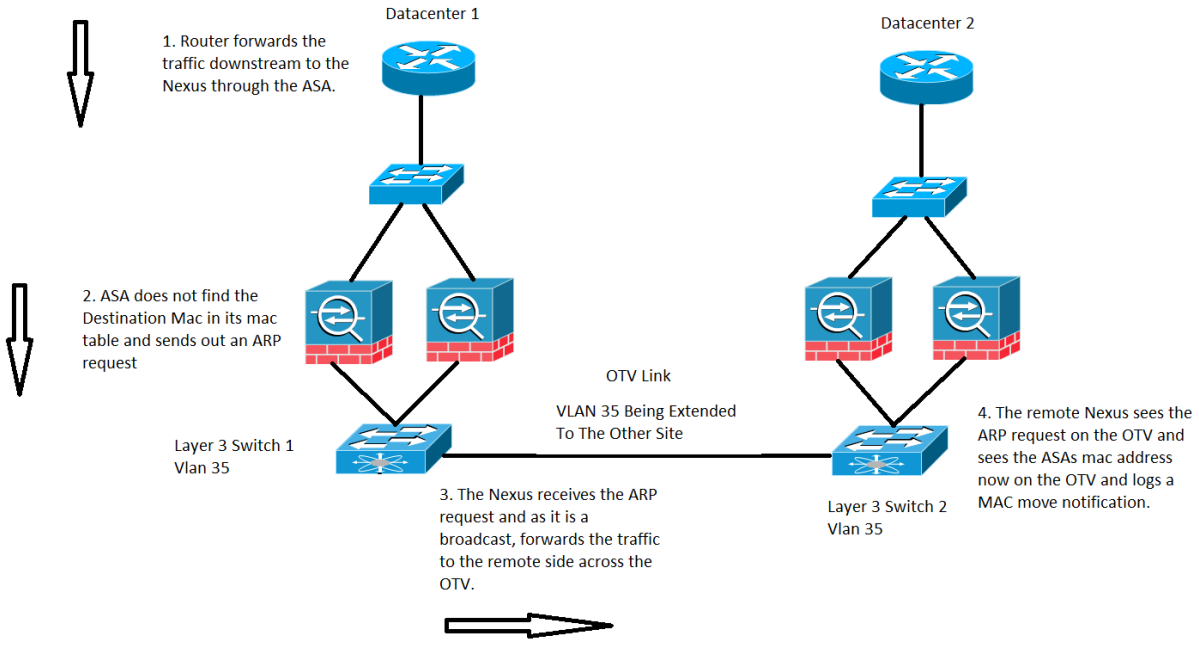
Déploiement de cluster inter-sites dans lequel les ASA sont configurés en mode transparent pour le pontage VLAN 1535 et VLAN 35. Le VLAN interne 35 est étendu sur OTV (Overlay Transport Virtualization) alors que le VLAN externe 1535 n'est pas étendu sur OTV, comme le montre l'image



Notifications de déplacement MAC sur le commutateur

Scénario 1

Trafic destiné à une adresse MAC dont l'entrée n'est pas présente dans la table MAC de l'ASA, comme illustré sur l'image :



Dans un ASA transparent, si l'adresse MAC de destination du paquet arrivant sur l'ASA ne figure

pas dans la table d'adresses MAC, il envoie une requête ARP (Address Resolution Protocol) pour cette destination (si elle se trouve dans le même sous-réseau que BVI) ou une requête ICMP (Internet Control Message Protocol) avec Time To Live 1(TTL 1) avec l'adresse MAC source comme interface virtuelle Bridge (BVI) L'adresse MAC et l'adresse MAC de destination en tant que contrôleur d'accès au support de destination (DMAC) sont manquées.

Dans le cas précédent, vous avez ce flux de trafic :

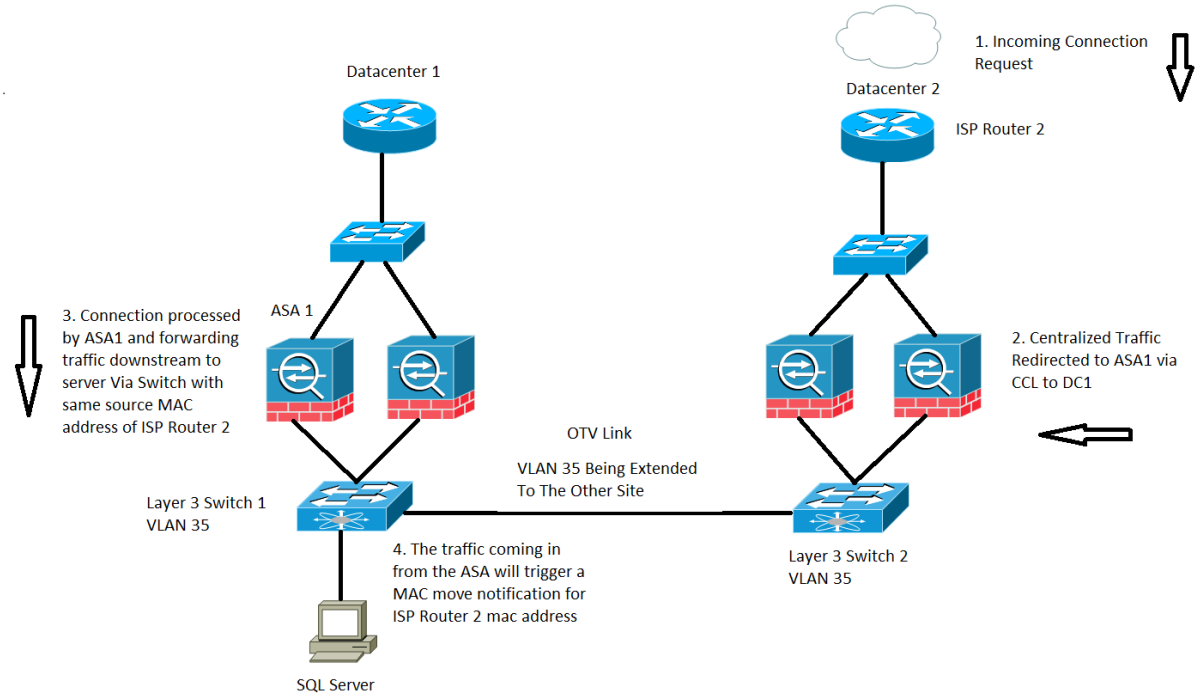
1. Le routeur ISP sur Datacenter 1 transfère le trafic vers une destination spécifique située derrière l'ASA.
2. L'un ou l'autre des ASA peut recevoir le trafic et, dans ce cas, l'adresse MAC de destination du trafic n'est pas connue par l'ASA.
3. Maintenant, l'adresse IP de destination du trafic se trouve dans le même sous-réseau que celui de l'interface BVI et, comme indiqué précédemment, ASA génère maintenant une requête ARP pour l'adresse IP de destination.
4. Le commutateur 1 reçoit le trafic et, comme la demande est une diffusion, il transfère le trafic vers le centre de données 2 ainsi que sur la liaison OTV.
5. Lorsque le commutateur 2 voit la requête ARP de l'ASA sur la liaison OTV, il enregistre une notification MAC MOVE car l'adresse MAC de l'ASA a été apprise par l'interface connectée directement et maintenant elle est apprise par la liaison OTV.

Recommandations

C'est un scénario d'angle. Les tables MAC sont synchronisées dans des clusters, de sorte qu'il est moins probable qu'un membre n'ait pas d'entrée pour un hôte particulier. Un déplacement MAC occasionnel pour les adresses MAC BVI appartenant à un cluster est jugé acceptable.

Scénario 2

Traitement de flux centralisé par ASA, comme illustré dans l'image :



Le trafic basé sur l'inspection sur un cluster ASA est classé en trois types :

- Centralisé
- Distribué
- Semi-distribué

Dans le cas d'une inspection centralisée, tout trafic qui doit être inspecté est redirigé vers l'unité principale du cluster ASA. Si une unité esclave du cluster ASA reçoit le trafic, il est transféré au maître via la CCL.

Dans l'image précédente, vous travaillez avec le trafic SQL qui est un protocole d'inspection centralisée (CIP) et le comportement décrit ici s'applique à tout CIP.

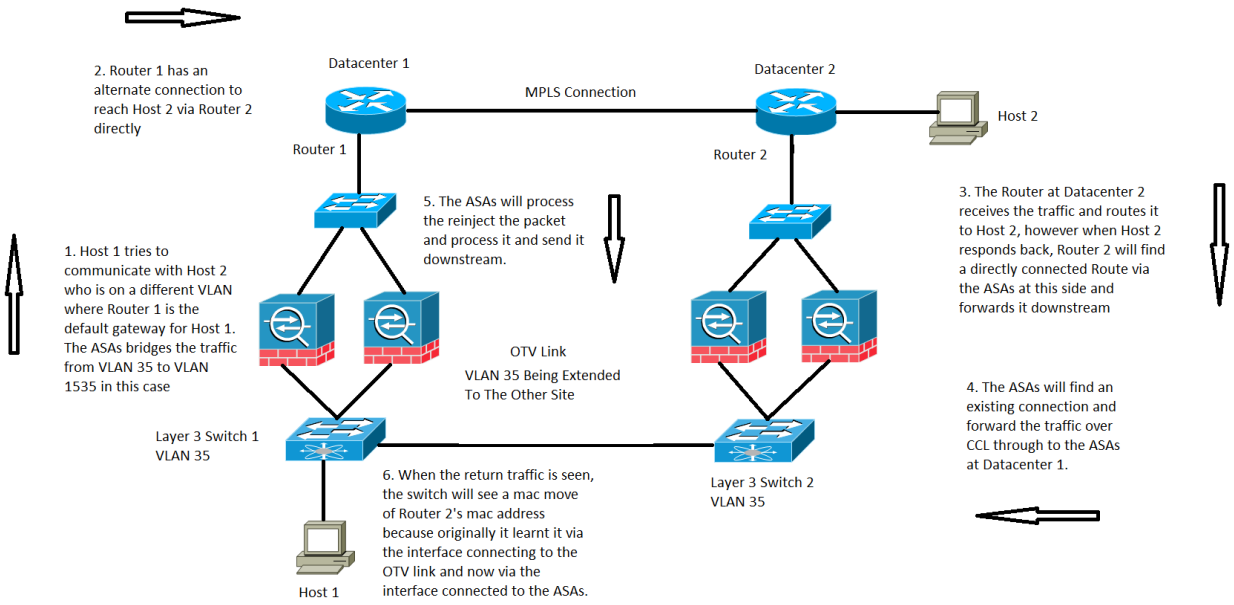
Vous recevez le trafic sur Datacenter 2 où vous n'avez que des unités esclaves du cluster ASA, l'unité principale se trouve au centre de données 1, qui est ASA 1.

1. Le routeur ISP 2 sur Datacenter 2 reçoit le trafic et le transfère en aval aux ASA sur son site.
2. L'un ou l'autre des ASA peut recevoir ce trafic et une fois qu'il a déterminé que ce trafic doit être inspecté et que le protocole est centralisé, il transfère le trafic à l'unité maître via la CCL.
3. ASA 1 reçoit le flux de trafic via la CCL, traite le trafic et l'envoie en aval vers SQL Server.
4. Maintenant, quand ASA 1 transfère le trafic en aval, il conserve l'adresse MAC source d'origine du routeur ISP 2 qui se trouve au centre de données 2 et l'envoie en aval.
5. Lorsque le commutateur 1 reçoit ce trafic spécifique, il se connecte dans une notification MAC MOVE car il voit à l'origine l'adresse MAC du routeur 2 du FAI via la liaison OTV qui est connectée au centre de données 2 et voit maintenant le trafic qui arrive des interfaces connectées à l'ASA 1.

Recommandations

Il est recommandé d'acheminer les connexions centralisées vers le site hôte principal (en fonction des priorités), comme le montre l'image :

Scénario 3

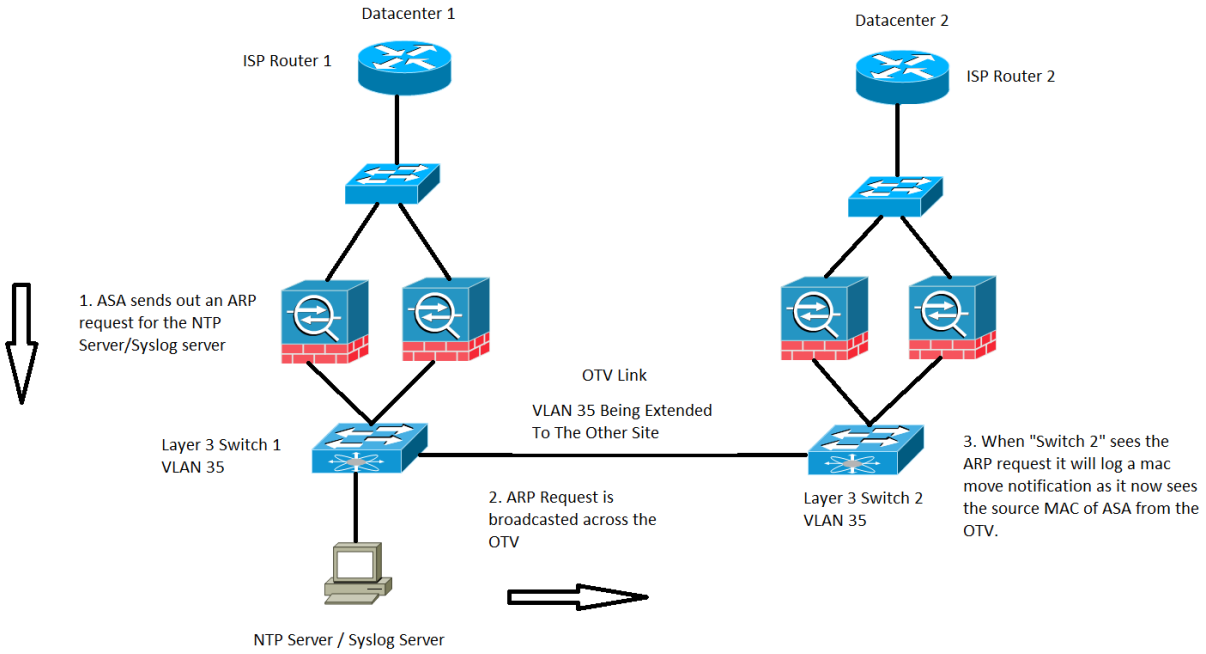


Pour une communication inter-contrôleur de domaine (DC) en mode transparent, ce flux de trafic spécifique n'est pas couvert ou documenté, mais ce flux de trafic spécifique fonctionne d'un point de vue de traitement de flux ASA. Cependant, il peut entraîner des notifications de déplacement MAC sur le commutateur.

1. L'hôte 1 sur le VLAN 35 tente de communiquer avec l'hôte 2 présent sur l'autre centre de données.
2. L'hôte 1 dispose d'une passerelle par défaut, à savoir le routeur 1 et le routeur 1 a un chemin pour atteindre l'hôte 2 en étant en mesure de communiquer directement avec le routeur 2 via une autre liaison. Dans ce cas, nous supposons que la commutation multiprotocole par étiquette (MPLS) et non via le cluster ASA.
3. Le routeur 2 reçoit le trafic entrant et le achemine vers l'hôte 2.
4. Maintenant, lorsque l'hôte 2 répond, le routeur 2 reçoit le trafic de retour et trouve une route directement connectée via les ASA au lieu du trafic qu'il envoie via le MPLS.
5. Àce stade, le trafic qui quitte le routeur 2 a l'adresse MAC source de l'interface de sortie du routeur 2.
6. Les ASA du data center 2 reçoivent le trafic de retour et trouvent une connexion qui existe et est établie par les ASA du data center 1.
7. Les ASA du centre de données 2 renvoient le trafic de retour via CCL aux ASA du centre de données 1.
8. Àce stade, les ASA du centre de données 1 traitent le trafic de retour et l'acheminent vers le commutateur 1. Le paquet a toujours la même adresse MAC source que celle de l'interface de sortie du routeur 2.
9. Maintenant, lorsque le commutateur 1 reçoit le paquet, il enregistre une notification de déplacement MAC car il a appris l'adresse MAC du routeur 2 sur l'interface connectée à la liaison OTV. Cependant, à ce stade, il commence à apprendre l'adresse MAC de l'interface connectée aux ASA.

Scénario 4

Trafic généré par l'ASA, comme illustré sur l'image :

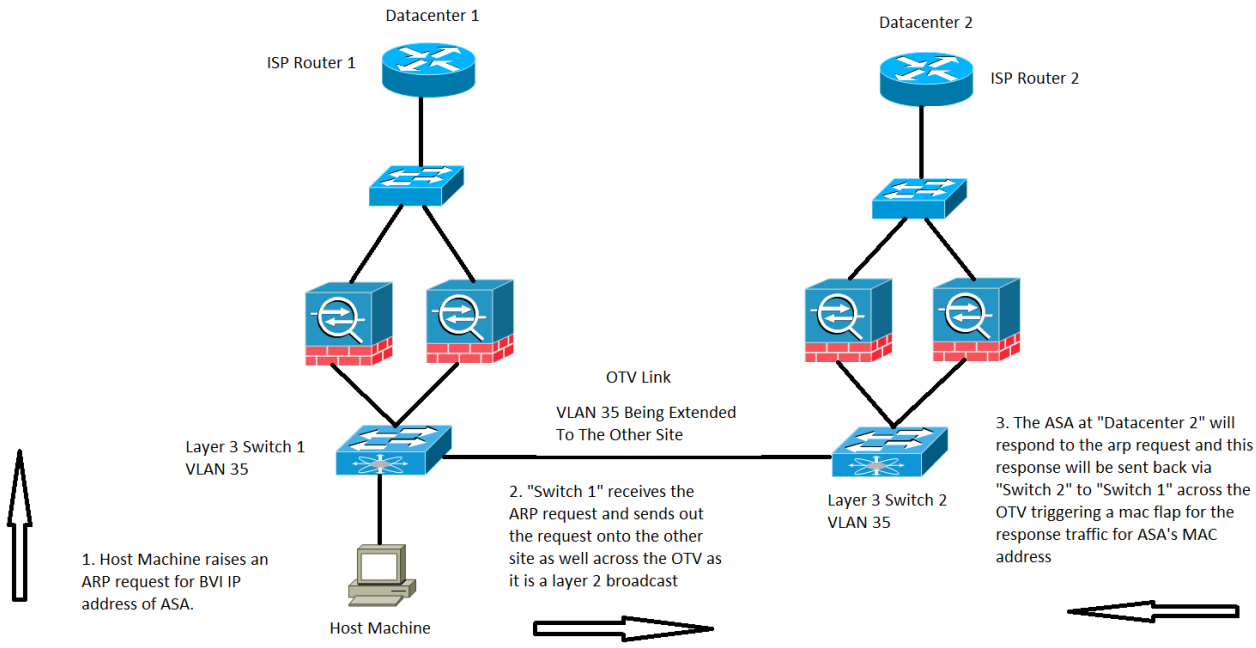


Ce cas spécifique sera observé pour tout trafic généré par l'ASA lui-même. Deux situations possibles sont prises en compte : l'ASA tente d'atteindre un protocole NTP (Network Time Protocol) ou un serveur Syslog, qui se trouvent sur le même sous-réseau que celui de son interface BVI.Cependant, cette situation ne se limite pas à ces deux conditions, elle peut se produire lorsque le trafic est généré par l'ASA pour toute adresse IP directement connectée aux adresses IP BVI.

1. Si ASA ne dispose pas des informations ARP du serveur NTP/Syslog, l'ASA génère une requête ARP pour ce serveur.
2. Comme la requête ARP est un paquet de diffusion, le commutateur 1 recevra ce paquet de son interface connectée de l'ASA et le diffusera sur toutes les interfaces du VLAN spécifique, y compris le site distant sur OTV.
3. Le commutateur de site distant 2 recevra cette requête ARP de la liaison OTV et, en raison de l'adresse MAC source de l'ASA, il génère une notification de battement MAC car la même adresse MAC est apprise sur l'OTV via ses interfaces locales directement connectées à l'ASA.

Scénario 5

Trafic destiné à l'adresse IP BVI de l'ASA à partir d'un hôte directement connecté, comme illustré sur l'image :



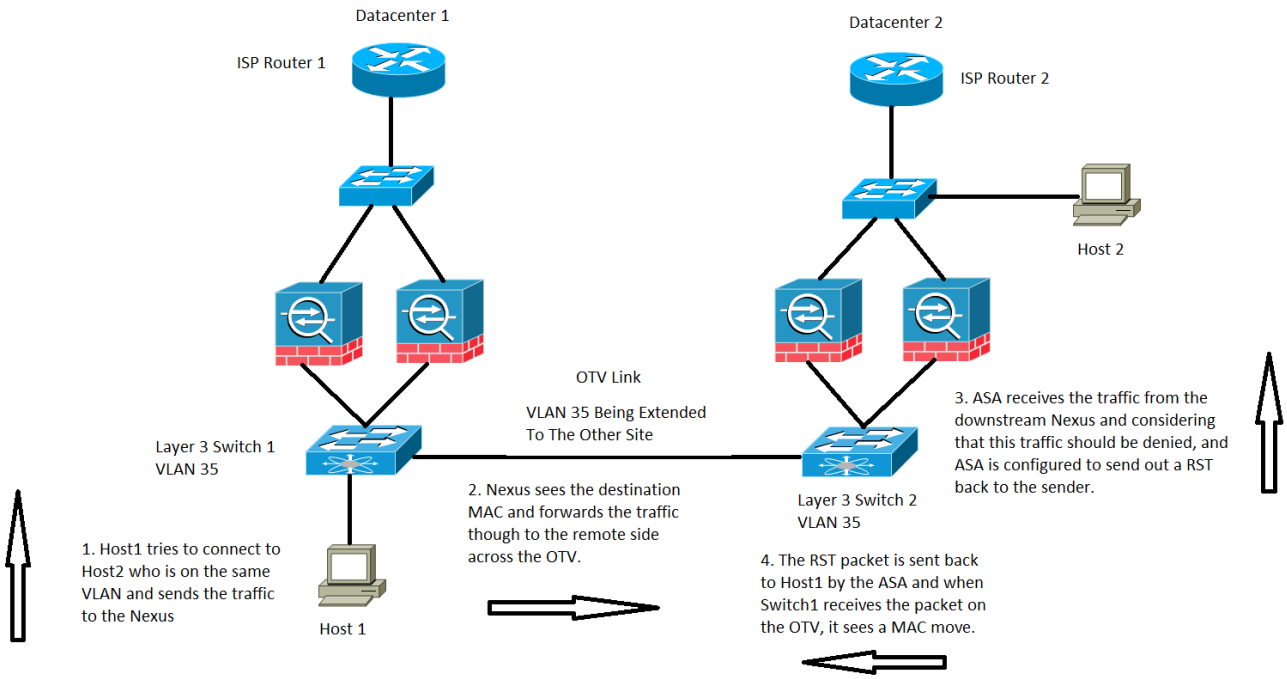
Un MAC MOVE peut également être observé lorsque le trafic est destiné à l'adresse IP BVI de l'ASA.

Dans le scénario, nous avons une machine hôte sur un réseau directement connecté de l'ASA et essayons de se connecter à l'ASA.

1. L'hôte ne dispose pas du protocole ARP de l'ASA et déclenche une requête ARP.
2. Le Nexus reçoit le trafic et, à nouveau, comme il s'agit d'un trafic de diffusion, il envoie le trafic via l'OTV à l'autre site également.
3. L'ASA sur le data center distant 2 peut répondre à la requête ARP et renvoyer le trafic par le même chemin que le commutateur 2 sur le côté distant, OTV, le commutateur 1 sur le côté local, puis l'hôte final.
4. Lorsque la réponse ARP est vue sur le commutateur local 1, elle déclenche une notification de déplacement MAC car elle voit l'adresse MAC de l'ASA qui provient de la liaison OTV.

Scénario 6

ASA est configuré pour refuser le trafic avec lequel il envoie une TVD à l'hôte, comme l'illustre l'image :



Dans ce cas, nous avons un hôte Host 1 sur le VLAN 35, il essaie de communiquer avec l'hôte 2 dans le même VLAN de couche 3, cependant, l'hôte 2 est en fait sur le VLAN 1535 du Datacenter 2.

1. L’adresse MAC de l’hôte 2est visible sur le commutateur2 via l’interface connectée aux ASA.
2. Le commutateur 1 voit l’adresse MAC de l’hôte 2 via la liaison OTV.
3. L’hôte 1 envoie le trafic à l’hôte 2 et suit le chemin du commutateur 1, OTV, du commutateur 2, des ASA au centre de données 2.
4. Ce paramètre spécifique est refusé par l'ASA et, lorsque l'ASA est configuré pour renvoyer un message RST à l'hôte 1, le paquet RST revient avec l'adresse MAC source de l'ASA.
5. Lorsque ce paquet revient au commutateur 1 via l'OTV, le commutateur 1 enregistre une notification MAC MOVE pour l'adresse MAC de l'ASA, car il voit maintenant l'adresse MAC sur l'OTV, où avant de voir l'adresse de son interface directement connectée.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Guide de configuration de la CLI de la gamme Cisco ASA
- Support et documentation techniques - Cisco Systems