Problèmes courants avec le cluster transparent intersite ASA

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Notifications MAC MOVE

Diagramme du réseau

Notifications de déplacement MAC sur le commutateur

- Scénario 1
  - Recommandations
- Scénario 2
  - Recommandations
- Scénario 3
- Scénario 4
- Scénario 5
- Scénario 6

Vérifier

Dépannage

Informations connexes

Introduction

Ce document décrit certains des problèmes courants avec le cluster intersite en mode transparent EtherChannel fractionné.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

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

- Cluster Inter-Site D'Interface Individuelle
- Cluster intersite en mode transparent EtherChannel fractionné
- Cluster inter-site en mode routé EtherChannel fractionné (pris en charge à partir de la version 9.5)

Notifications MAC MOVE

Lorsqu'une adresse MAC de la table CAM (Content Addressable Memory) 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 que si une adresse MAC X est apprise via l'interface GigabitEthernet0/1 dans VLAN10 et qu'après un certain temps, la même adresse MAC est vue via GigabitEthernet0/2 dans VLAN 10, alors une notification MAC MOVE est générée.

Syslog du commutateur :

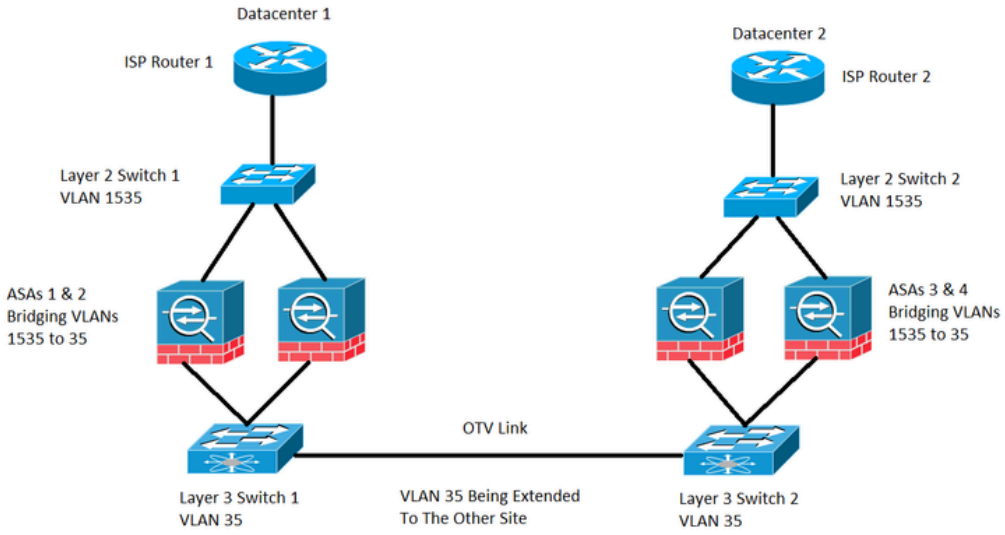
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1 to Gigab
```

Syslog depuis ASA :

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

Diagramme du réseau

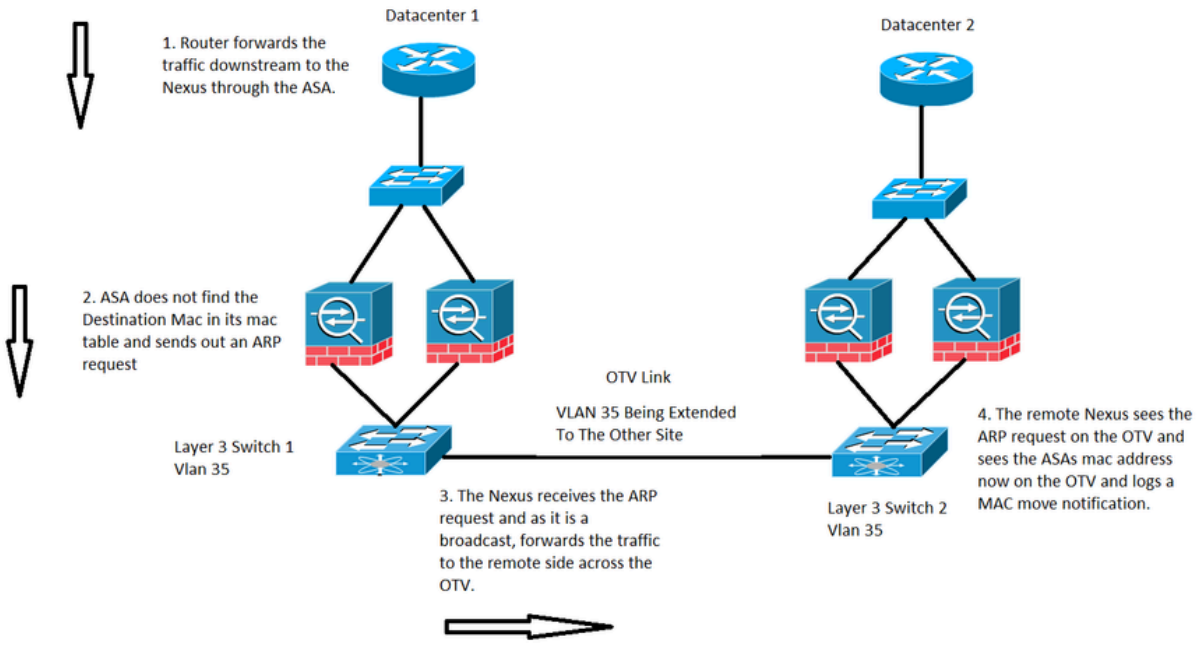
Déploiement de cluster inter-site dans lequel les ASA sont configurés en mode transparent pontant le VLAN 1535 et le VLAN 35. Le VLAN interne 35 est étendu sur l'OTV (Overlay Transport Virtualization), tandis que le VLAN externe 1535 n'est pas étendu sur l'OTV, comme illustré dans l'image



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 dans l'image :



Dans un ASA transparent, Si l'adresse MAC de destination du paquet arrivant sur l'ASA n'est pas dans la table d'adresses MAC, il envoie une requête ARP (Address Resolution Protocol) pour cette destination (si 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 adresse MAC de l'interface virtuelle de pont (BVI) et l'adresse MAC de destination comme DMAC (Destination Media Access Controller) est manquée.

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

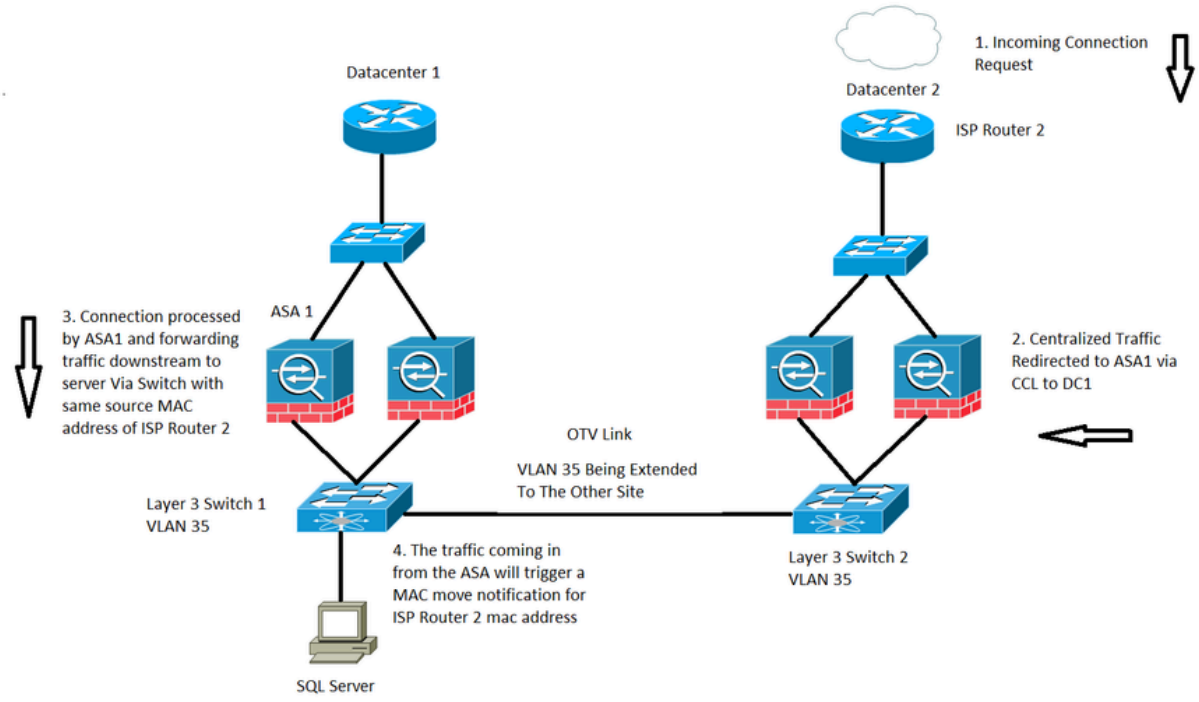
1. Le routeur ISP du data center 1 transfère le trafic vers une destination spécifique qui se trouve derrière l'ASA.
2. Chacun des ASA peut recevoir le trafic et dans ce cas, l'adresse MAC de destination du trafic n'est pas connue par l'ASA.
3. Maintenant, l'IP de destination du trafic se trouve dans le même sous-réseau que celui de l'interface BVI et comme mentionné précédemment, ASA génère maintenant une requête ARP pour l'IP de destination.
4. Le commutateur 1 reçoit le trafic et, comme la requête est une diffusion, il transfère le trafic vers le data center 2 ainsi que sur la liaison OTV.
5. Lorsque le commutateur 2 voit la requête ARP de l'ASA sur la liaison OTV, il consigne une notification MAC MOVE car auparavant l'adresse MAC de l'ASA était apprise via l'interface connectée directement et maintenant elle est apprise via la liaison OTV.

Recommandations

Il s'agit d'un scénario d'angle. Les tables MAC sont synchronisées en clusters, de sorte qu'il est moins probable qu'un membre ne possède pas d'entrée pour un hôte particulier. Un déplacement MAC occasionnel pour un 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 dans un cluster ASA est classé en trois types :

- Centralisé
- Distributed
- Semi-Distribué

Dans le cas de l'inspection centralisée, tout trafic devant être inspecté est redirigé vers l'unité principale du cluster ASA. Si une unité secondaire de la grappe ASA reçoit le trafic, il est transféré à la principale via la CCL.

Dans l'image précédente, vous travaillez avec le trafic SQL qui est un protocole CIP (Centralized Inspection Protocol) et le comportement décrit ici s'applique à n'importe quel CIP.

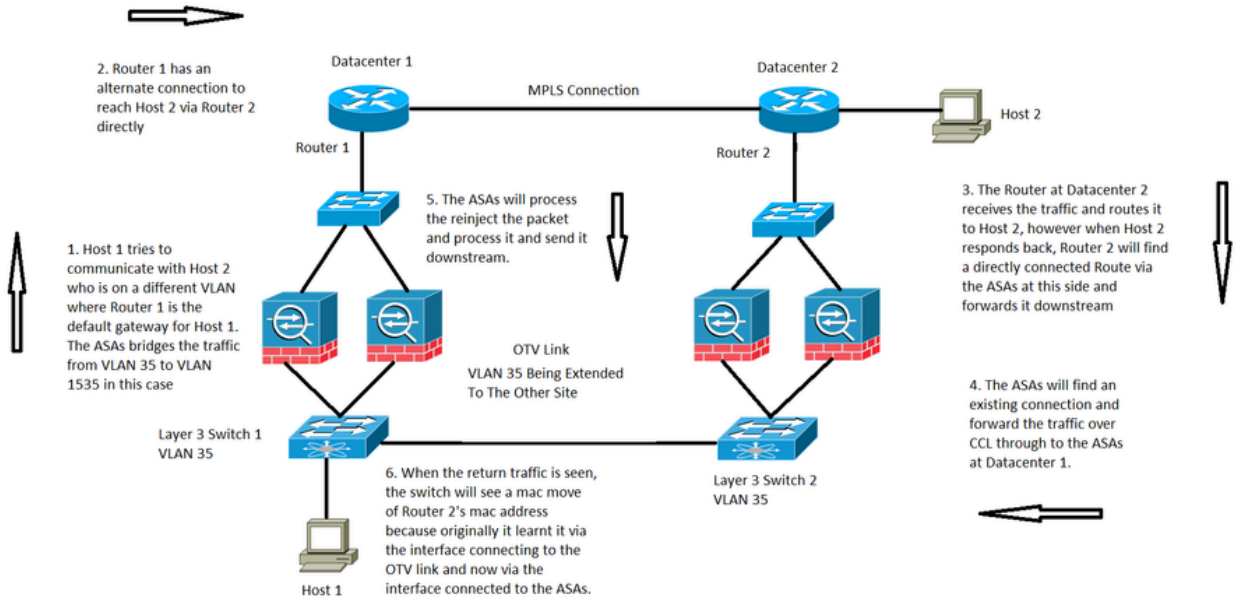
Vous recevez le trafic sur le Datacenter 2 où vous n'avez que des unités secondaires du cluster ASA, l'unité principale est située au Datacenter 1 qui est ASA 1.

1. Le routeur ISP 2 du data center 2 reçoit le trafic et le transfère en aval vers les ASA de son site.
2. Chacun 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 principale 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. À présent, lorsqu'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 à une notification MAC MOVE parce qu'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 qu'il voit maintenant le trafic qui provient des interfaces connectées à l'ASA 1.

Recommandations

Il est recommandé d'acheminer les connexions centralisées vers n'importe quel site hébergeant le site principal (en fonction des priorités), comme illustré dans l'image :

Scénario 3



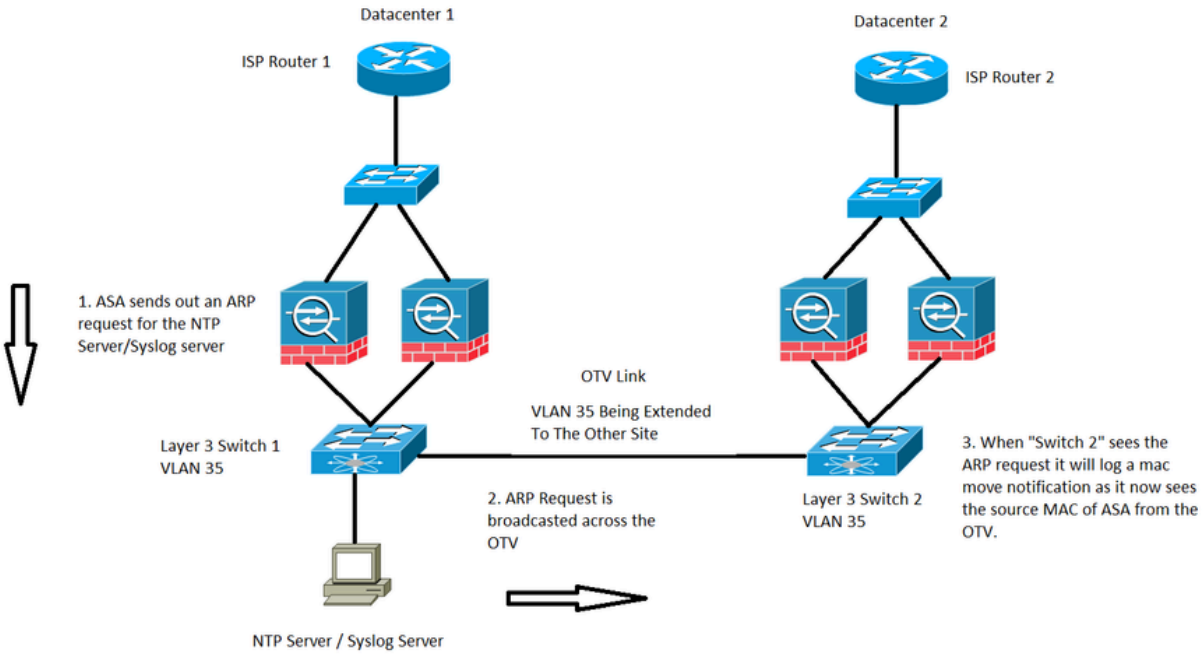
Pour une communication de contrôleur inter-domaines (DC) en mode transparent, ce flux de trafic spécifique n'est pas couvert ou documenté, mais ce flux de trafic spécifique fonctionne du point de vue du traitement de flux ASA. Cependant, cela peut entraîner des notifications de déplacement MAC sur le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

1. L'hôte 1 sur le VLAN 35 tente de communiquer avec l'hôte 2 qui est présent sur l'autre data center.
2. L'hôte 1 a une passerelle par défaut qui est le routeur 1 et le routeur 1 a un chemin pour atteindre l'hôte 2 en étant capable de communiquer avec le routeur 2 directement via une liaison alternative et dans ce cas, nous supposons la commutation multiprotocole par étiquette (MPLS) et non via le cluster ASA.
3. Le routeur 2 reçoit le trafic entrant et l’achemine vers l’hôte 2.
4. Maintenant, lorsque l'hôte 2 répond, le routeur 2 reçoit le trafic de retour et trouve une route connectée directement via les ASA au lieu du trafic qu'il envoie via le MPLS.
5. À ce 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 qui est établie par les ASA du data center 1.
7. Les ASA du data center 2 renvoient le trafic de retour via CCL aux ASA du data center 1.
8. À ce stade, les ASA du centre de données 1 traitent le trafic de retour et l’envoient vers le commutateur 1. Le paquet a toujours le même MAC source que celui de l’interface de sortie du routeur 2.

9. À présent, lorsque le commutateur 1 reçoit le paquet, il enregistre une notification de déplacement MAC, car il a initialement appris l'adresse MAC du routeur 2 sur l'interface qui est connectée à la liaison OTV. Cependant, à ce stade, il commence à apprendre l'adresse MAC à partir de l'interface connectée aux ASA.

Scénario 4

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

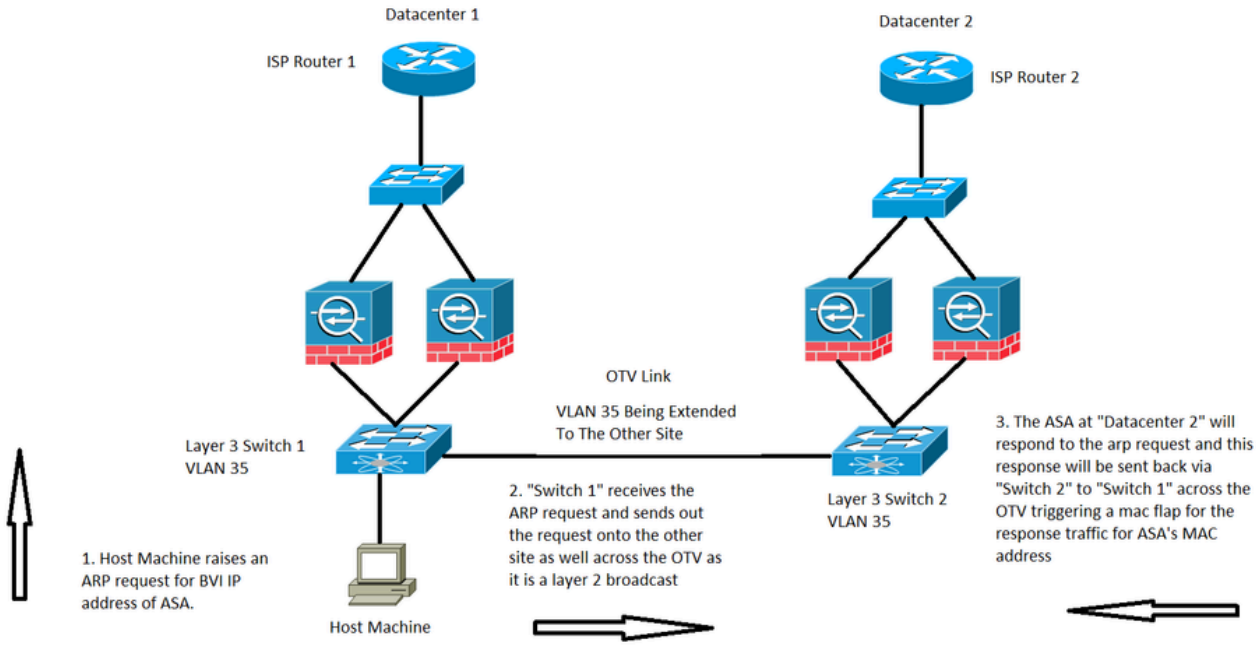


Ce cas spécifique sera observé pour tout trafic qui est généré par l'ASA lui-même. Ici, deux situations possibles sont considérées, dans lesquelles l'ASA tente d'atteindre un protocole NTP (Network Time Protocol) ou un serveur Syslog, qui sont sur le même sous-réseau que celui de son interface BVI.Cependant, il n'est pas seulement limité à ces deux conditions, cette situation peut se produire chaque fois que le trafic est généré par l'ASA pour n'importe quelle adresse IP qui est directement connectée aux adresses IP BVI.

1. Si ASA ne dispose pas des informations ARP du serveur NTP/serveur 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 l'inondera à travers toutes les interfaces dans le VLAN spécifique, y compris le site distant à travers l'OTV.
3. Le commutateur 2 du site distant 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 puisque 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 dans l'image :



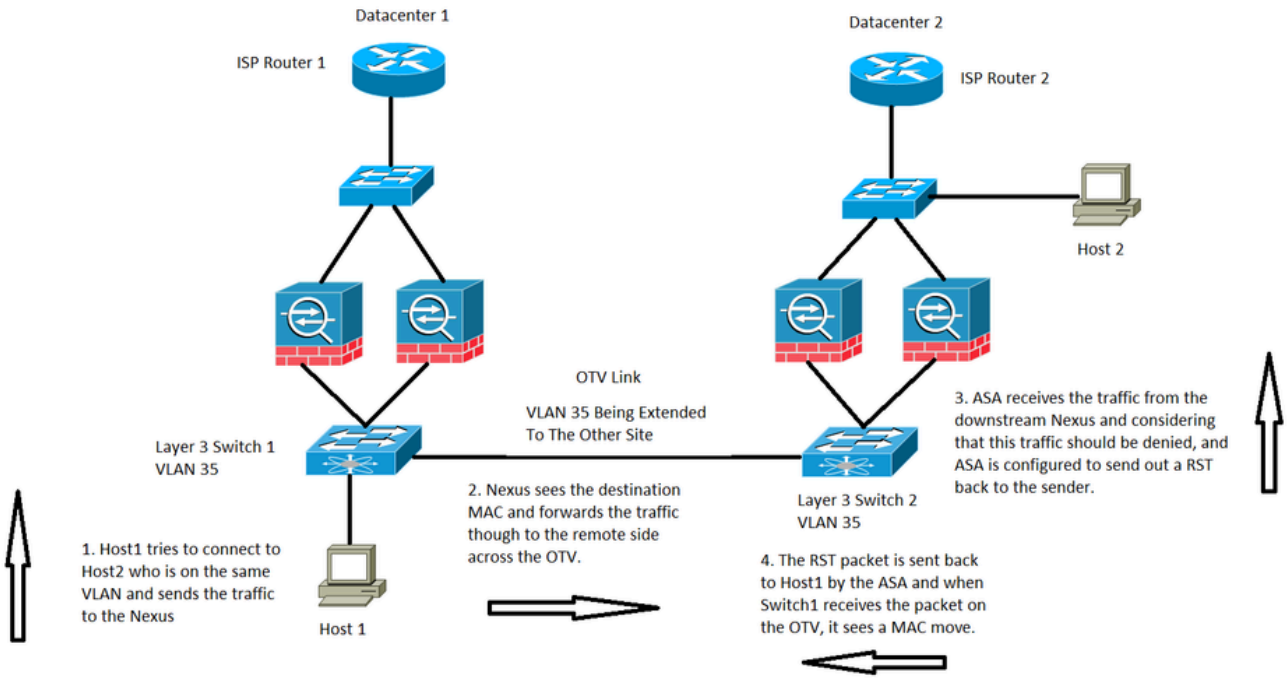
Un MAC MOVE peut également être observé lorsque le trafic est destiné à l'adresse IP BVI de l'ASA.

Dans le scénario, nous avons une machine hôte sur un réseau connecté directement de l'ASA et nous essayons de nous 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 de nouveau, comme il s'agit d'un trafic de diffusion, il envoie le trafic à travers l'OTV vers l'autre site également.
3. L'ASA du data center distant 2 peut répondre à la requête ARP et renvoie le trafic par le même chemin que le commutateur 2 du côté distant, OTV, le commutateur 1 du côté local, puis l'hôte final.
4. Lorsque la réponse ARP est vue sur le commutateur 1 côté local, elle déclenche une notification de déplacement MAC lorsqu'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 un RST à l'hôte, comme indiqué dans 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 data center 2.

1. L’adresse MAC de l’hôte 2 serait visible sur le commutateur 2 via l’interface connectée aux ASA.
2. Le commutateur 1 verrait l’adresse MAC de l’hôte 2 via la liaison OTV.
3. L'hôte 1 envoie le trafic à l'hôte 2, qui suit le chemin des commutateurs 1, OTV, 2 et ASA au centre de données 2.
4. Ce paquet spécifique est refusé par l'ASA et comme l'ASA est configuré pour renvoyer un RST à l'hôte 1, le paquet RST revient avec l'adresse MAC source de l'ASA.
5. Lorsque ce paquet est renvoyé 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, avant de voir l'adresse de son interface directement connectée.

Vérifier

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 CLI de la gamme Cisco ASA
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.