Problèmes courants avec la batterie transparente d'Inter-site ASA

Contenu

Introduction

Ce document décrit certains des problèmes courants avec la batterie répartie d'Inter-site de mode transparent d'EtherChannel.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Pare-feu de l'appliance de sécurité adaptable (ASA)
- Groupement ASA

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Commençant la version 9.2 ASA, le groupement d'inter-site est pris en charge où les unités ASA pourraient se trouvent dans différents datacenters et le lien de contrôle de batterie (CCL) est connecté au-dessus d'une interconnexion du centre de calculs (DCI). Les scénarios possibles de déploiement sont :

- Batterie d'Inter-site d'interface individuelle
- Batterie répartie d'Inter-site de mode transparent d'EtherChannel
- Batterie répartie d'Inter-site de mode conduite par EtherChannel (prise en charge à compter de 9.5)

Notifications de MOUVEMENT de MAC

Quand une adresse MAC dans les modifications associatives de table de mémoire (CAM) mettent en communication, une notification de MOUVEMENT de MAC est générée. Cependant, une notification de MOUVEMENT de MAC n'est pas générée quand l'adresse MAC est ajoutée ou retirée de la table de CAM. Supposez si une adresse MAC X est apprise par l'intermédiaire de l'interface GigabitEthernet0/1 dans VLAN10 et après une certaine heure le même MAC est vu par GigabitEthernet0/2 dans le VLAN 10, alors une notification de MOUVEMENT de MAC est générée.

Syslog de commutateur :

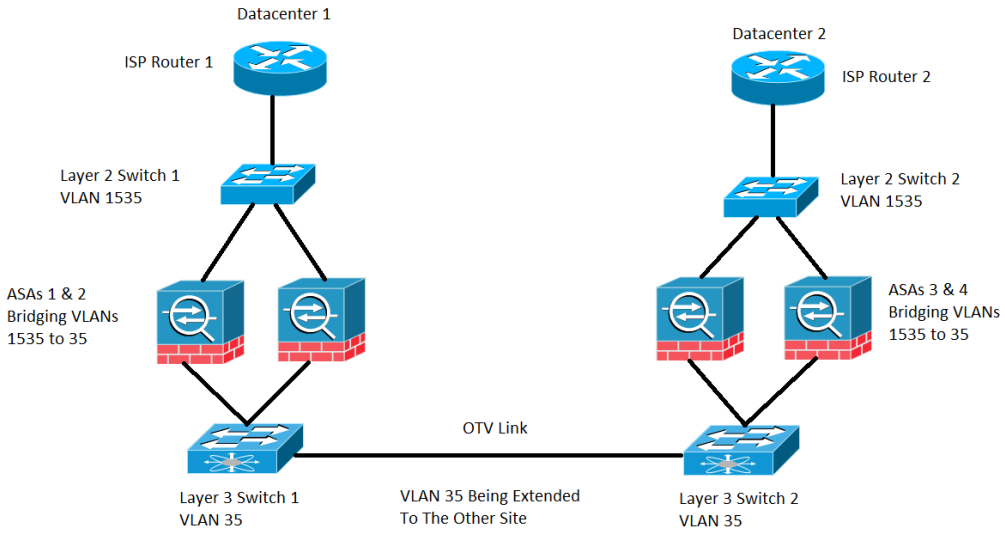
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1
to GigabitEthernet0/2
```

Syslog d'ASA :

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

Diagramme du réseau

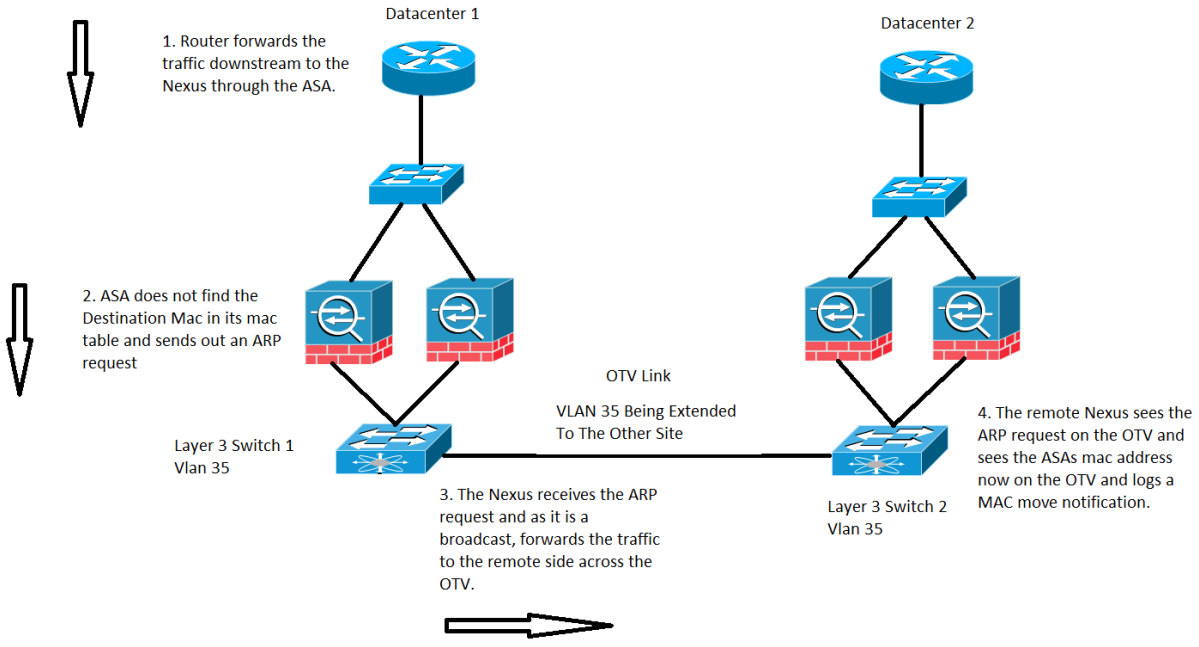
déploiement de batterie d'Inter-site où les ASA sont configurées en mode transparent jetant un pont sur VLAN 1535 et VLAN 35. Le VLAN intérieur 35 est étendu au-dessus de la virtualisation de transport de recouvrement (OTV) tandis que le VLAN extérieur 1535 n'est pas étendu au-dessus de l'OTV, suivant les indications de l'image



Notifications de mouvement de MAC sur le commutateur

Scénario 1

Trafiquez destiné à une adresse MAC dont l'entrée n'est pas présente sur la table du MAC de l'ASA, suivant les indications de l'image :



Dans une ASA transparente, si l'adresse MAC de destination du paquet arrivant sur l'ASA n'est

pas dans la table de mac-address, il envoie une demande de Protocole ARP (Address Resolution Protocol) de cette destination (si dans le même sous-réseau que BVI) ou une demande de Protocole ICMP (Internet Control Message Protocol) avec le Time to Live 1(TTL 1) avec le MAC de source comme adresse MAC de l'interface virtuelle de passerelle (BVI) et l'adresse MAC de destination en tant que contrôleur d'accès au support de destination (DMAC) est manquée.

Dans le cas précédent, vous avez ces la circulation :

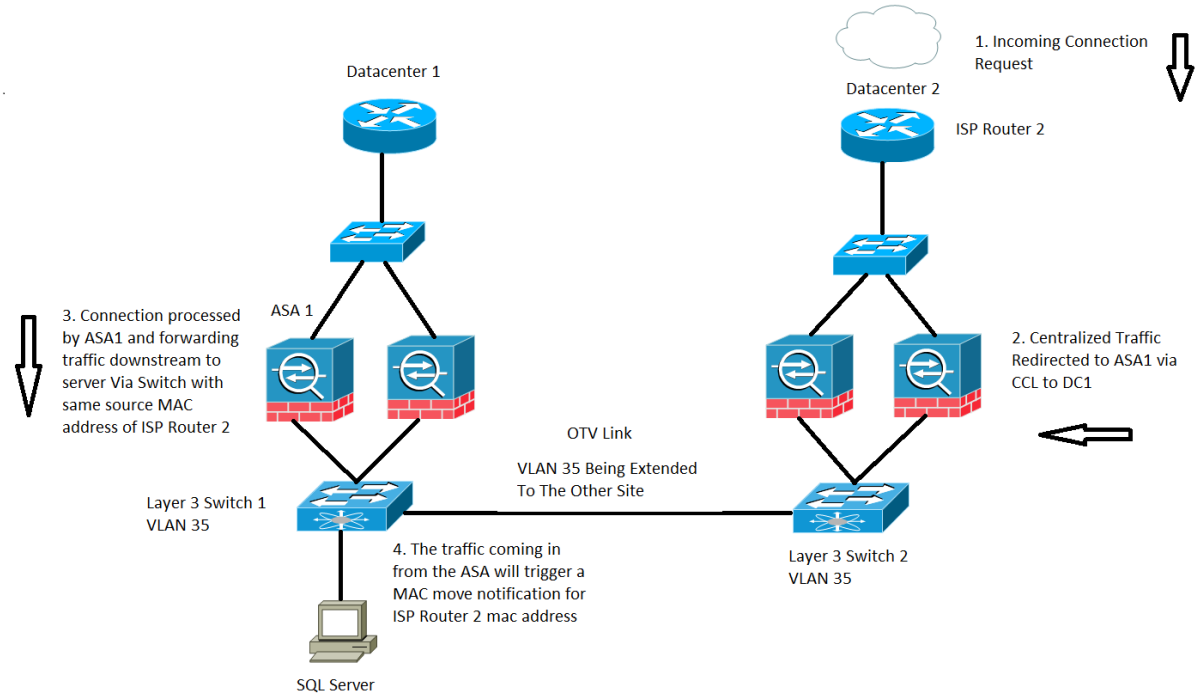
1. Le routeur de l'ISP sur le centre d'hébergement 1 trafiquent en avant à une destination spécifique qui est derrière l'ASA.
2. L'un ou l'autre de la boîte de l'ASA reçoit le trafic et dans ce cas, l'adresse MAC de destination du trafic n'est pas connue par l'ASA.
3. Maintenant l'IP de destination du trafic est dans le même sous-réseau que cela du BVI et comme indiqué précédemment, ASA génère maintenant une demande d'ARP d'IP de destination.
4. Le commutateur 1 reçoit le trafic et car la demande est une émission, elle en avant le trafic au centre d'hébergement 2 aussi bien qu'à travers le lien OTV.
5. Quand voit Comm2 la demande d'ARP de l'ASA sur le lien OTV, il se connecte une notification de MOUVEMENT de MAC parce que précédemment l'adresse MAC de l'ASA a été apprise par l'intermédiaire de l'interface directement connectée et maintenant on l'apprend par l'intermédiaire du lien OTV.

Recommandations

C'est un scénario faisant le coin. Des tables de MAC sont synchronisées dans les batteries, ainsi il est moins pour qu'un membre n'ait pas une entrée pour un hôte spécifique. Un MAC-mouvement occasionnel pour le MAC BVI batterie batterie est considéré acceptable.

Scénario 2

Écoulement centralisé traitant par ASA, suivant les indications de l'image :



Le trafic basé par inspection à travers une batterie ASA est classifié dans trois types :

- Centralisé
- Distribué
- Semi-distribué

Dans le cas de l'inspection centralisée, n'importe quel trafic que les besoins d'obtenir ont examiné est réorienté à l'unité principale de la batterie ASA. Si une unité slave de la batterie ASA reçoit le trafic, elle est expédiée au maître par l'intermédiaire du CCL.

Dans l'image plus tôt, vous travaillez avec le trafic SQL qui est protocol relatif aux inspections centralisé (CIP) et le comportement décrit ici s'applique pour n'importe quel CIP.

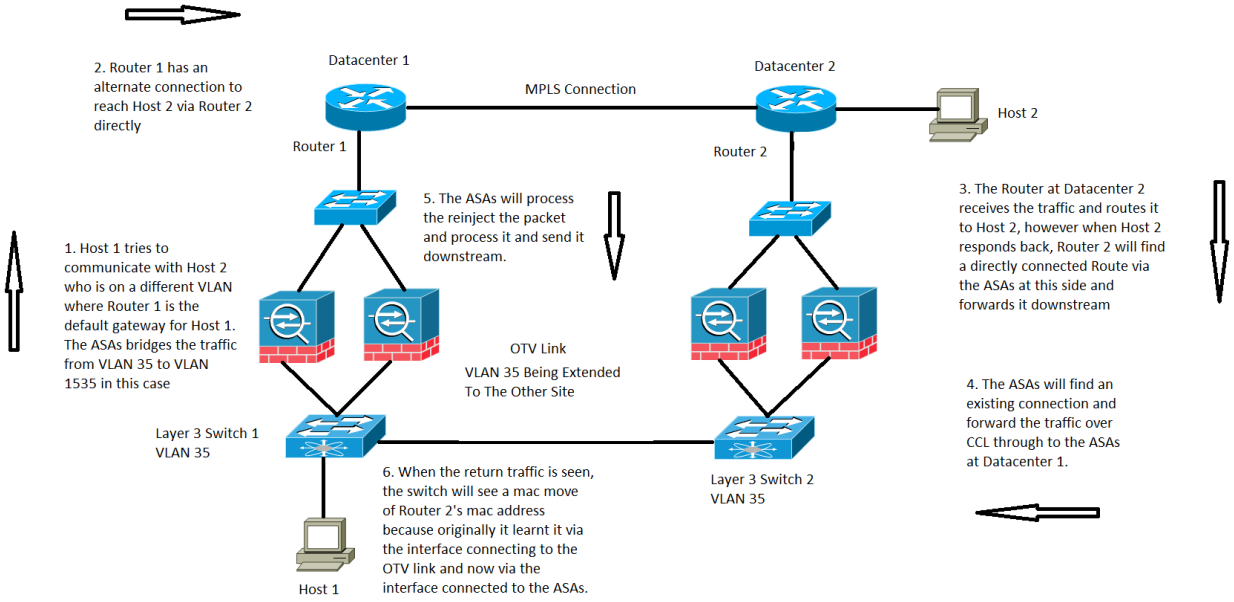
Vous recevez le trafic sur le centre d'hébergement 2 où vous avez seulement les unités slaves de la batterie ASA, l'unité principale se trouve au centre d'hébergement 1 qui est ASA 1.

1. Le routeur de l'ISP 2 sur le centre d'hébergement 2 reçoit le trafic et en avant lui en aval aux ASA à son site.
2. L'un ou l'autre des ASA peut recevoir ce trafic et une fois qu'il détermine que ce trafic doit être examiné et pendant que le protocole l'est centralisé en avant le trafic plus d'à l'unité principale par l'intermédiaire du CCL.
3. ASA 1 reçoit la circulation par l'intermédiaire du CCL, traite le trafic et lui envoie l'en aval au Serveur SQL.
4. Maintenant où ASA 1 en avant l'en aval du trafic, il retient le MAC address de source d'origine du routeur de l'ISP 2 qui se trouve au centre d'hébergement 2 et lui envoie l'en aval.
5. Quand le commutateur 1 reçoit ce trafic spécifique, il ouvre une session une notification de MOUVEMENT de MAC parce qu'il voit initialement qu'adresse MAC du routeur de l'ISP 2 par l'intermédiaire du lien OTV qui est connecté au centre d'hébergement 2 et maintenant il voit le trafic qui entre des interfaces connectées à l'ASA 1.

Recommandations

Il est recommandé pour conduire les connexions centralisées à n'importe quel site héberge le maître (basé sur des priorités), suivant les indications de l'image :

Scénario 3



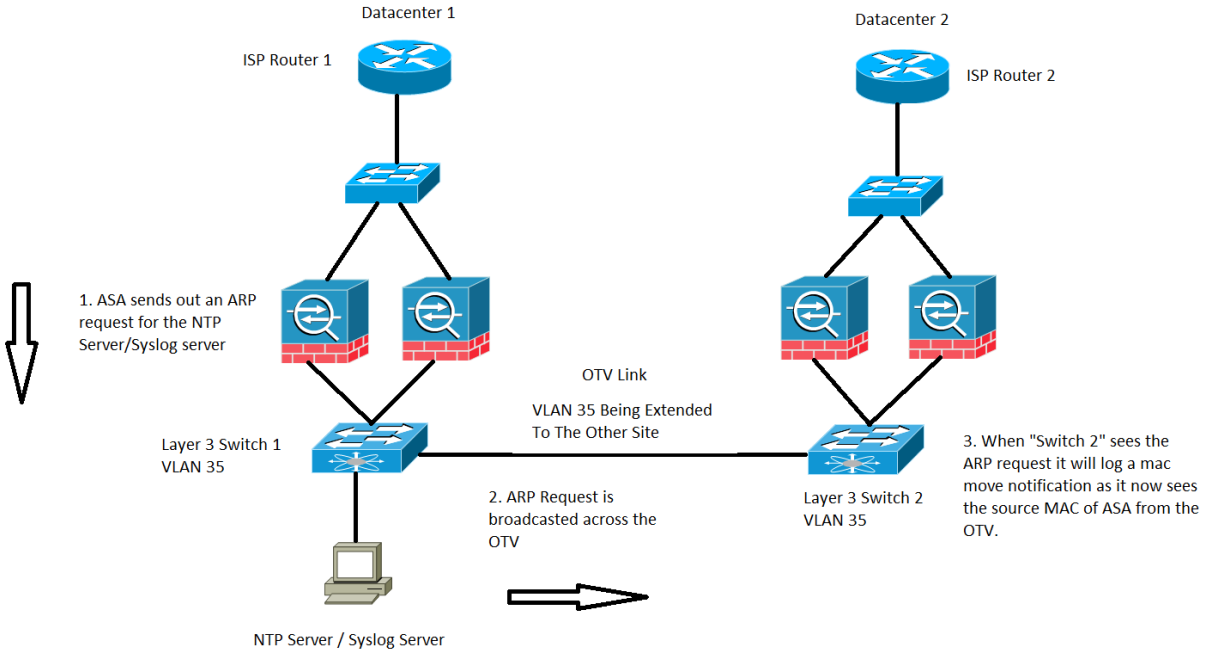
Pour une transmission inter du contrôleur de domaine (C.C) en mode transparent, cette circulation spécifique n'est pas couverte ou est documentée mais cette circulation spécifique fonctionne d'un écoulement ASA traitant le point de vue. Cependant, il peut avoir comme conséquence des notifications de mouvement de MAC sur le commutateur.

1. L'hôte 1 sur des essais VLAN 35 à communiquer avec l'hôte 2 qui est présent sur l'autre centre d'hébergement.
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 pouvant communiquer avec le Router2 directement à travers un lien alternatif et dans ce cas nous assumons le Commutation multiprotocole par étiquette (MPLS) et pas par la batterie ASA.
3. Le Router2 reçoit le trafic entrant et le conduit plus de pour héberger 2.
4. Maintenant où l'hôte 2 répond de retour, le Router2 reçoit le trafic de retour et il trouve directement une route connectée par les ASA au lieu du trafic qu'elle envoie au-dessus du MPLS.
5. Àce stade, le trafic qui part du Router2 a le MAC de source de l'interface de sortie du routeur 2's.
6. Les ASA au centre d'hébergement 2 reçoit le trafic de retour et trouve une connexion qui existe et est faite par les ASA au centre d'hébergement 1.
7. Les ASA au centre d'hébergement 2 envoie le trafic de retour au-dessus de CCL de nouveau aux ASA au centre d'hébergement 1.
8. Àce stade les ASA au centre d'hébergement 1 traite le trafic de retour et l'envoie vers le bas vers le commutateur 1. Le paquet a toujours le même MAC de source que celui de l'interface de sortie du routeur 2's.
9. Maintenant où le commutateur 1 reçoit le paquet, il se connecte une notification de mouvement de MAC parce qu'au commencement il a appris l'adresse MAC du routeur 2's à

travers l'interface qui est connectée au lien OTV, toutefois à ce stade elle commence apprendre l'adresse MAC à partir de l'interface connectée aux ASA.

Scénario 4

Le trafic généré par l'ASA, suivant les indications de l'image :

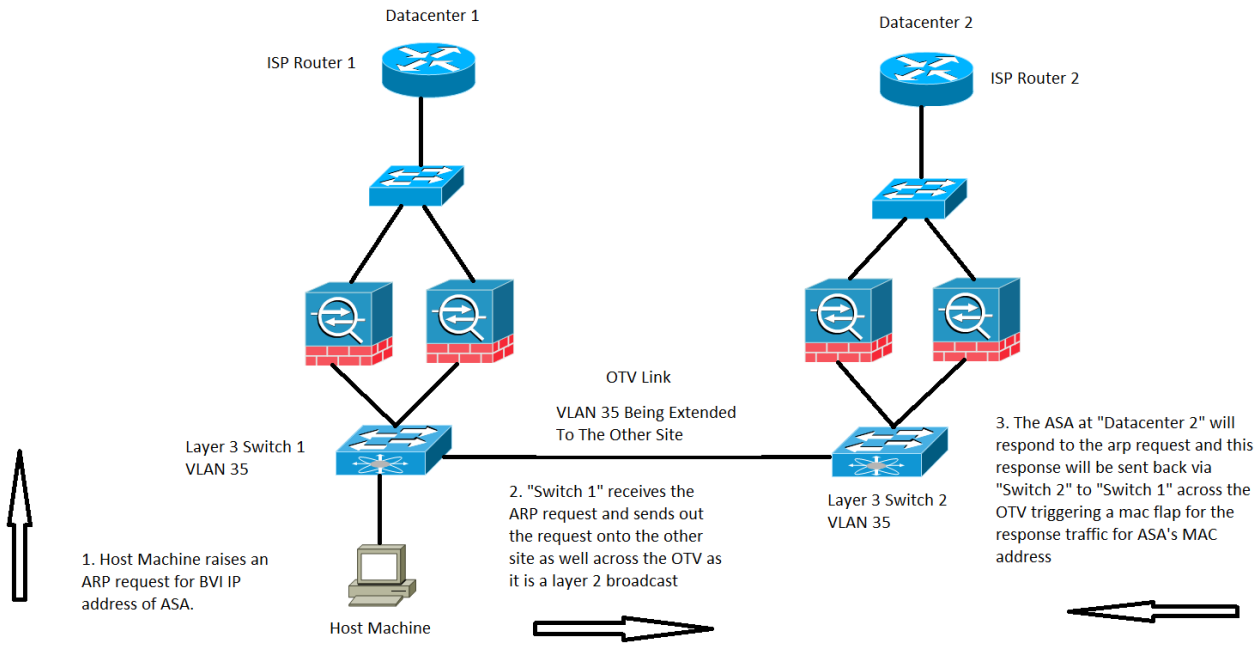


On observera ce cas spécifique pour n'importe quel trafic qui obtient généré par l'ASA elle-même. Ici deux situations possibles sont considérées comme, où les essais ASA pour atteindrees un Protocole NTP (Network Time Protocol) ou un serveur de Syslog, qui sont sur le même sous-réseau que celui de son interface BVI. Toutefois il est non seulement limité à ces deux conditions, cette situation peut se produire toutes les 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 l'ASA n'a pas les informations d'ARP du serveur de NTP/de serveur de Syslog, alors l'ASA génèrera une demande d'ARP de ce serveur.
2. Car la demande d'ARP est un paquet d'émission, le commutateur 1 recevra ce paquet de son interface connectée de l'ASA et l'inondera à travers toutes les interfaces dans la particularité VLAN comprenant le site distant à travers l'OTV.
3. Le site distant Comm2 recevra cette demande d'ARP du lien OTV et en raison du MAC de source de l'ASA, il génère une notification d'instabilité de MAC puisque la même adresse MAC est apprise à travers l'OTV par l'intermédiaire de ses interfaces directement connectées de gens du pays à l'ASA.

Scénario 5

Trafiquez destiné à l'adresse IP BVI de l'ASA directement d'un hôte connecté, suivant les indications de l'image :



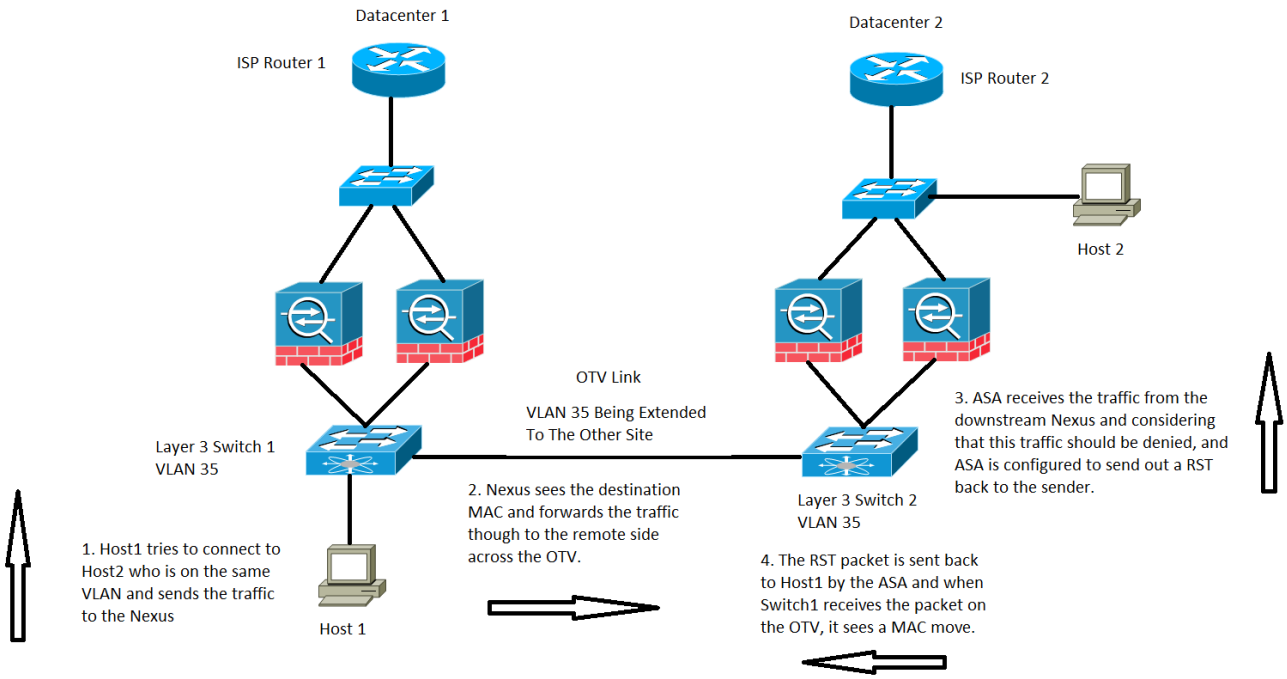
On peut également observer parfois UN MOUVEMENT de MAC quand le trafic est destiné à l'adresse IP BVI de l'ASA.

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

1. L'hôte n'a pas l'ARP de l'ASA et déclenche une demande d'ARP.
2. Le Nexus reçoit le trafic et de nouveau car c'est un trafic d'émission qu'il envoie le trafic à travers l'OTV à l'autre site aussi bien.
3. L'ASA sur le centre d'hébergement distant 2 peut répondre à la demande d'ARP et renvoie le trafic par le même chemin qui est Comm2 du côté distant, OTV, commute 1 sur le côté local et puis l'hôte d'extrémité.
4. Quand la réponse d'ARP est vue sur le commutateur 1 de côté local, il déclenche une notification de mouvement de MAC pendant qu'il voit l'adresse MAC de l'ASA qui entre du lien OTV.

Scénario 6

Positionnement ASA pour refuser le trafic avec lequel il envoie un RST à l'hôte, suivant les indications de l'image :



Dans ce cas, nous avons un hôte 1 d'hôte sur VLAN 35, il essaye de communiquer avec l'hôte 2 dans la même couche 3 VLAN, cependant, l'hôte 2 est réellement sur le centre d'hébergement 2 VLAN 1535.

1. L'adresse de l'hôte 2MAC serait vue en fonction Comm2 par l'intermédiaire de l'interface connectée aux ASA.
2. Le commutateur 1 verrait l'adresse MAC de l'hôte 2 par l'intermédiaire du lien OTV.
3. L'hôte 1 envoie le trafic pour héberger 2 et ceci suit le chemin du commutateur 1, OTV, Comm2, des ASA au centre d'hébergement 2.
4. Cette particularité obtient refusé par l'ASA et pendant que l'ASA est configurée pour renvoyer un RST pour héberger 1, le paquet RST revient avec l'adresse MAC source de l'ASA.
5. Quand ce paquet le fait de nouveau au commutateur 1 à travers l'OTV, le commutateur 1 se connecte une notification de MOUVEMENT de MAC pour l'adresse MAC de l'ASA parce qu'il voit maintenant l'adresse MAC à travers l'OTV, où avant qu'il voie l'adresse de son interface directement connectée.

Vérifiez

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

Dépannez

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

Informations connexes

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