Problemas comuns com o cluster transparente entre locais ASA

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Notificações de MOVE MAC](#)
[Diagrama de Rede](#)
[Notificações de Movimentação de MAC no Switch](#)
[Cenário 1](#)
[Recomendações](#)
[Cenário 2](#)
[Recomendações](#)
[Cenário 3](#)
[Cenário 4](#)
[Cenário 5](#)
[Cenário 6](#)
[Verificar](#)
[Troubleshoot](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve alguns dos problemas comuns com o cluster entre sites do modo transparente EtherChannel estendido.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firewall ASA (Adaptive Security Appliance)
- Clustering ASA

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Informações de Apoio

A partir do ASA versão 9.2, há suporte para clustering entre locais, em que as unidades ASA podem estar localizadas em data centers diferentes e o Cluster Control Link (CCL) está conectado em uma interconexão de data center (DCI). Os possíveis cenários de implantação são:

- Cluster entre locais da interface individual
- Cluster entre locais do modo transparente EtherChannel estendido
- Cluster entre locais do modo roteado EtherChannel estendido (suportado a partir de 9,5)

Notificações de MOVE MAC

Quando um endereço MAC na tabela CAM (Content Addressable Memory) altera a porta, uma notificação de MAC MOVE é gerada. No entanto, uma notificação MAC MOVE não é gerada quando o endereço MAC é adicionado ou removido da tabela CAM. Suponha se um endereço MAC X é aprendido através da interface GigabitEthernet0/1 na VLAN10 e depois de algum tempo o mesmo MAC é visto através de GigabitEthernet0/2 na VLAN 10, então uma notificação de MOVE MAC é gerada.

Syslog do switch:

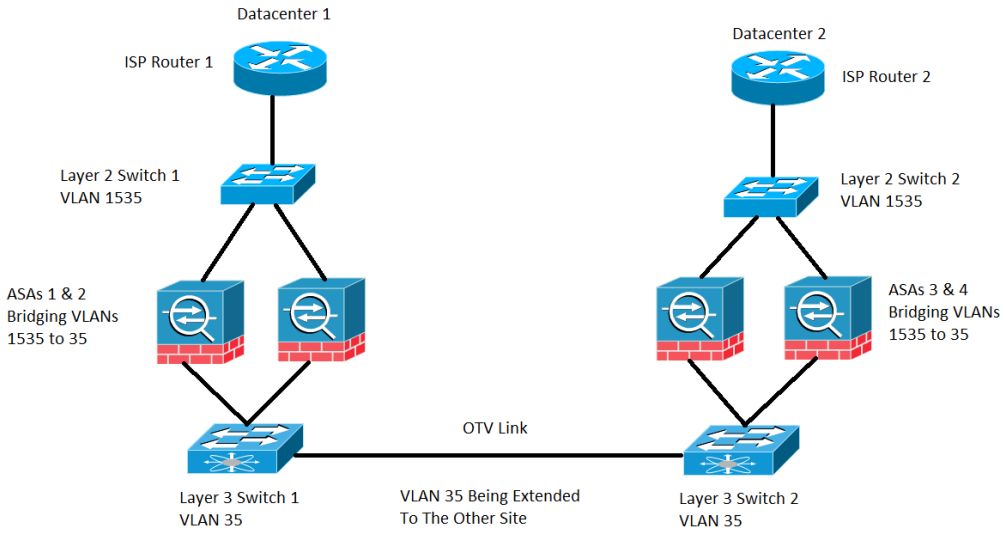
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1
to GigabitEthernet0/2
```

Syslog do ASA:

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

Diagrama de Rede

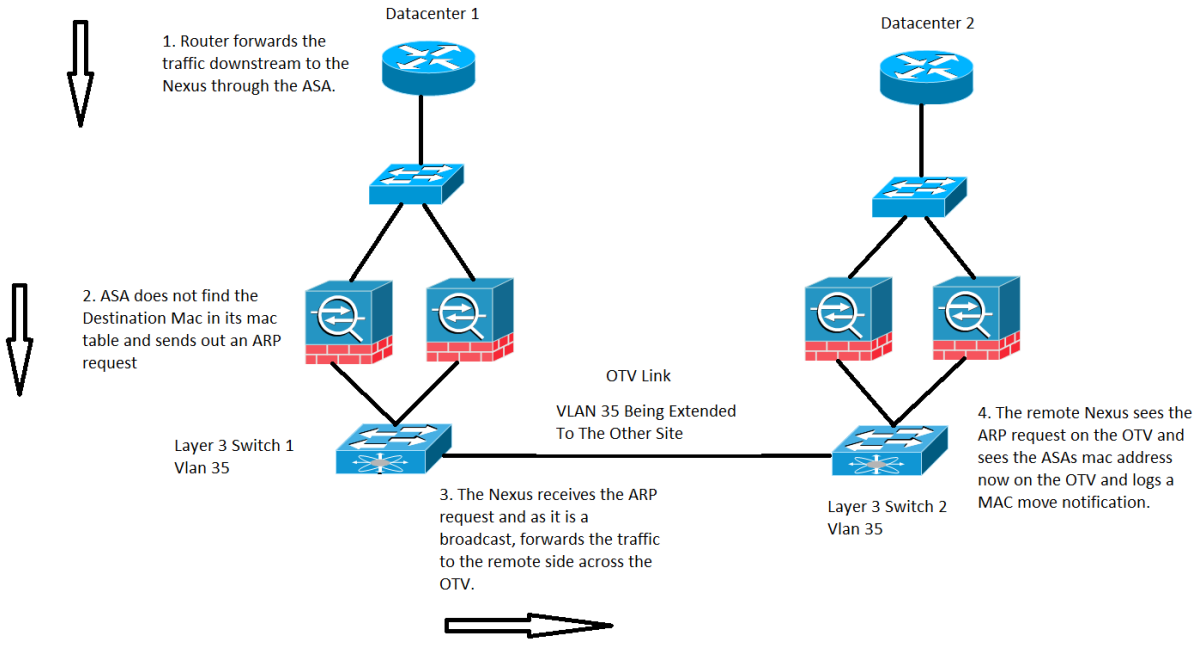
Implantação de cluster entre locais onde os ASAs são configurados no modo transparente Bridging VLAN 1535 e VLAN 35. A VLAN 35 interna é estendida sobre a Overlay Transport Virtualization (OTV) enquanto a VLAN 1535 externa não é estendida sobre a OTV, como mostrado na imagem



Notificações de Movimentação de MAC no Switch

Cenário 1

Tráfego destinado a um endereço MAC cuja entrada não está presente na tabela MAC do ASA, como mostrado na imagem:



Em um ASA transparente, se o endereço MAC de destino do pacote que chega ao ASA não

estiver na tabela de endereços mac, ele enviará uma solicitação do Address Resolution Protocol (ARP) para esse destino (se estiver na mesma sub-rede que o BVI) ou uma solicitação do Internet Control Message Protocol (ICMP) com Time To Live 1 (TTL 1) com o MAC de origem como a Interface Virtual Bridge (BVI) O endereço MAC e o endereço MAC de destino como Controlador de Acesso à Mídia de Destino (DMAC) são perdidos.

No caso anterior, você tem estes fluxos de tráfego:

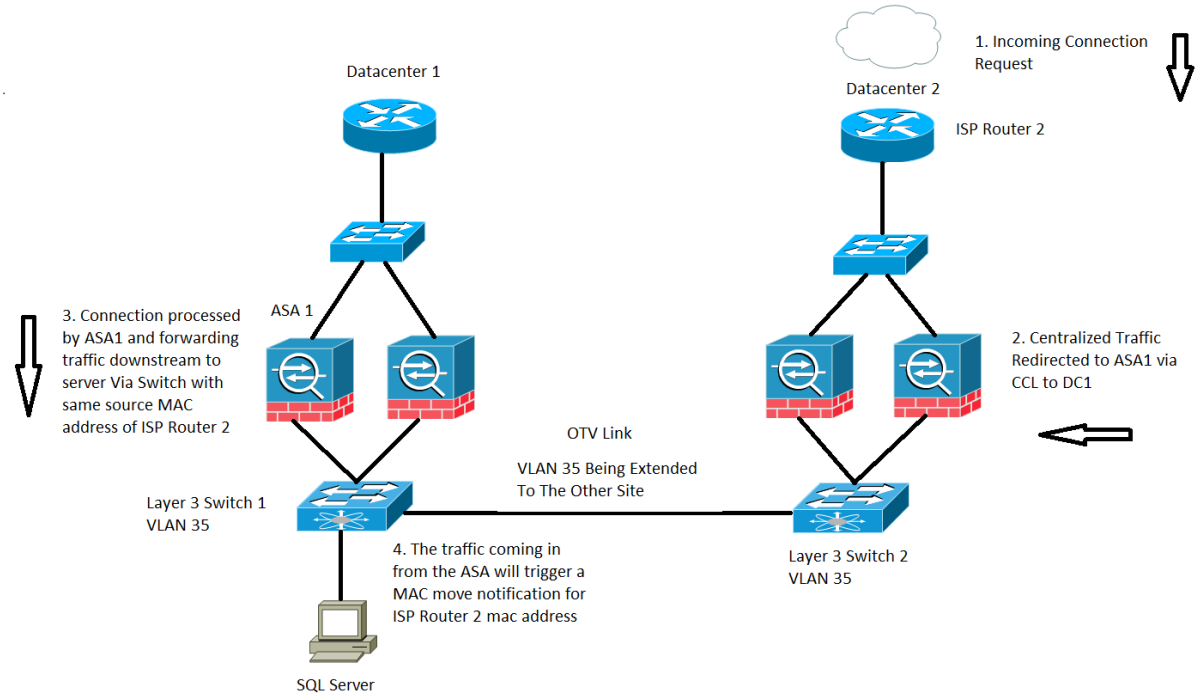
1. O roteador do ISP no datacenter 1 encaminha o tráfego para um destino específico que está por trás do ASA.
2. Qualquer um dos ASAs pode receber o tráfego e, nesse caso, o endereço MAC de destino do tráfego não é conhecido pelo ASA.
3. Agora, o IP de destino do tráfego está na mesma sub-rede do BVI e, como mencionado anteriormente, o ASA agora gera uma solicitação ARP para o IP de destino.
4. O Switch 1 recebe o tráfego e, como a solicitação é um broadcast, encaminha o tráfego para o Datacenter 2, bem como através do link OTV.
5. Quando o Switch 2 vê a solicitação ARP do ASA no link OTV, ele registra uma notificação de MOVE MAC porque o endereço MAC do ASA anterior foi aprendido via interface diretamente conectada e agora está sendo aprendido através do link OTV.

Recomendações

Éum cenário de canto. As tabelas MAC são sincronizadas em clusters, portanto, é menos provável que um membro não tenha uma entrada para um host específico. Uma mudança ocasional de MAC para o MAC de BVI pertencente ao cluster é considerada aceitável.

Cenário 2

Processamento de fluxo centralizado pelo ASA, como mostrado na imagem:



O tráfego baseado em inspeção em um cluster ASA é classificado em três tipos:

- Centralizado
- Distribuído
- Semidistribuído

No caso de inspeção centralizada, qualquer tráfego que precise ser inspecionado é redirecionado para a unidade mestre do cluster ASA. Se uma unidade escrava do cluster ASA receber o tráfego, ele será encaminhado ao mestre por meio do CCL.

Na imagem anterior, você trabalha com o tráfego SQL que é um Protocolo de Inspeção Centralizada (CIP - Centralized Inspection Protocol) e o comportamento descrito aqui é aplicável a qualquer CIP.

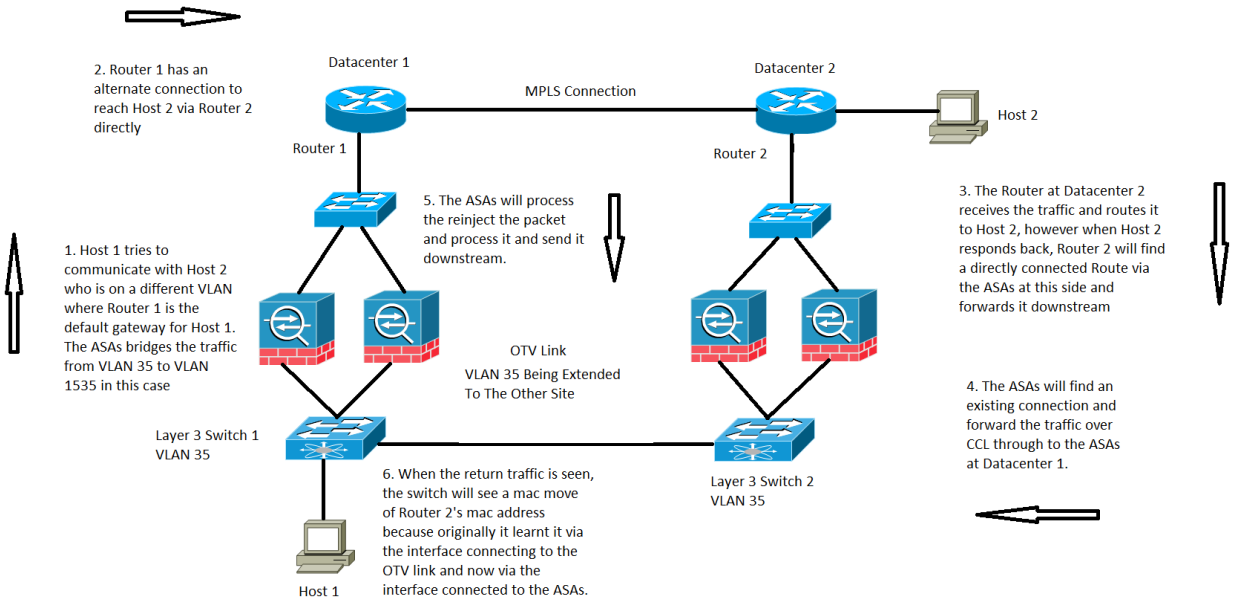
Você recebe o tráfego no Datacenter 2, onde você só tem unidades escravas do cluster ASA, a unidade mestre está localizada no Datacenter 1, que é ASA 1.

1. O roteador 2 do ISP no datacenter 2 recebe o tráfego e o encaminha para downstream para os ASAs em seu local.
2. Qualquer um dos ASAs pode receber esse tráfego e, uma vez que determina que esse tráfego precisa ser inspecionado e, como o protocolo é centralizado, ele encaminha o tráfego para a unidade mestre através do CCL.
3. O ASA 1 recebe o fluxo de tráfego através do CCL, processa o tráfego e o envia downstream para o SQL Server.
4. Agora, quando o ASA 1 encaminha o tráfego downstream, ele retém o endereço mac de origem do roteador 2 do ISP, localizado no datacenter 2 e o envia downstream.
5. Quando o Switch 1 recebe esse tráfego específico, faz login em uma notificação MAC MOVE porque vê originalmente o endereço MAC do Roteador 2 do ISP através do link OTV conectado ao Datacenter 2 e agora vê o tráfego que vem das interfaces conectadas ao ASA 1.

Recomendações

Recomenda-se rotear conexões centralizadas para os hosts do site mestre (com base nas prioridades), como mostrado na imagem:

Cenário 3



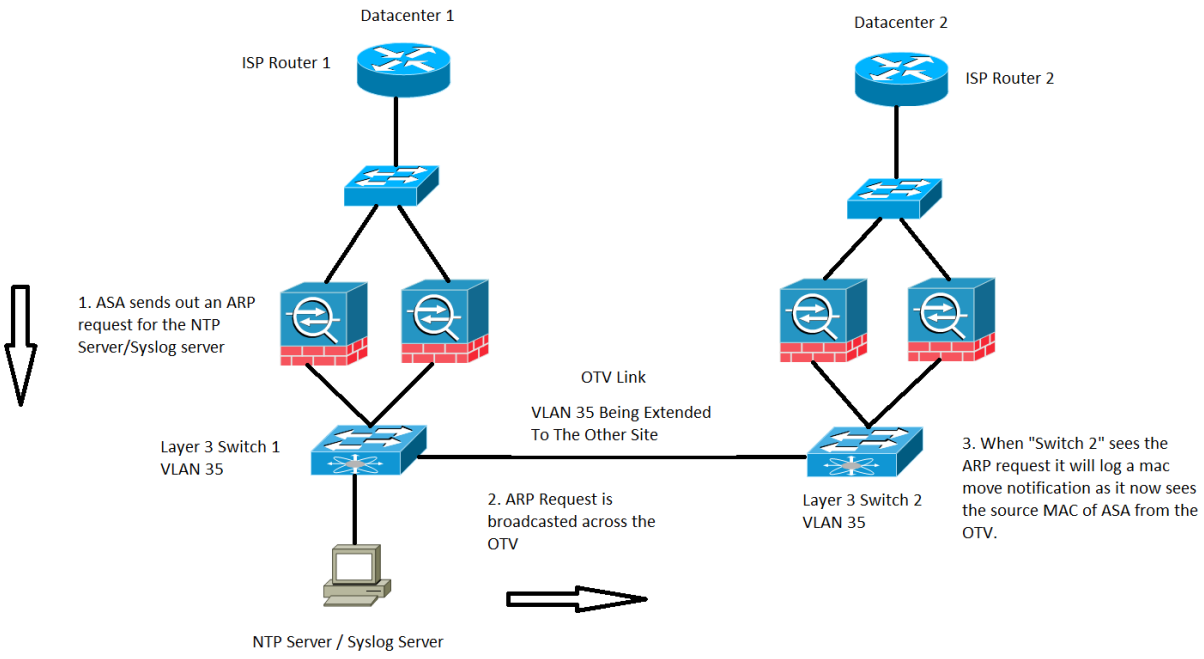
Para uma comunicação de controlador entre domínios (DC) em modo transparente, esse fluxo de tráfego específico não é coberto ou documentado, mas esse fluxo de tráfego específico funciona do ponto de vista de processamento de fluxo do ASA. No entanto, isso pode resultar em notificações de movimentação de MAC no switch.

1. O host 1 na VLAN 35 tenta se comunicar com o host 2 que está presente no outro datacenter.
2. O Host 1 tem um gateway padrão que é o Roteador 1 e o Roteador 1 tem um caminho para alcançar o Host 2, sendo capaz de se comunicar com o Roteador 2 diretamente através de um link alternativo e, nesse caso, presumimos Multiprotocol Label Switching (MPLS) e não através do cluster ASA.
3. O roteador 2 recebe o tráfego de entrada e o encaminha para o host 2.
4. Agora, quando o Host 2 responde, o Roteador 2 recebe o tráfego de retorno e encontra uma rota diretamente conectada através dos ASAs, em vez do tráfego que envia através do MPLS.
5. Neste estágio, o tráfego que sai do Roteador 2 tem o MAC origem da interface de saída do Roteador 2.
6. Os ASAs no Datacenter 2 recebem o tráfego de retorno e encontram uma conexão que existe e é feita pelos ASAs no Datacenter 1.
7. Os ASAs no datacenter 2 enviam o tráfego de retorno por CCL de volta aos ASAs no datacenter 1.
8. Neste estágio, os ASAs no datacenter 1 processam o tráfego de retorno e o enviam para o Switch 1. O pacote ainda tem o mesmo MAC origem que a interface de saída do Roteador 2.
9. Agora, quando o Switch 1 recebe o pacote, ele registra uma notificação de movimentação de

MAC porque inicialmente aprendeu o endereço MAC do Roteador 2 através da interface conectada ao link OTV, no entanto, nesse estágio, ele começa a aprender o endereço MAC da interface conectada aos ASAs.

Cenário 4

Tráfego gerado pelo ASA, como mostrado na imagem:

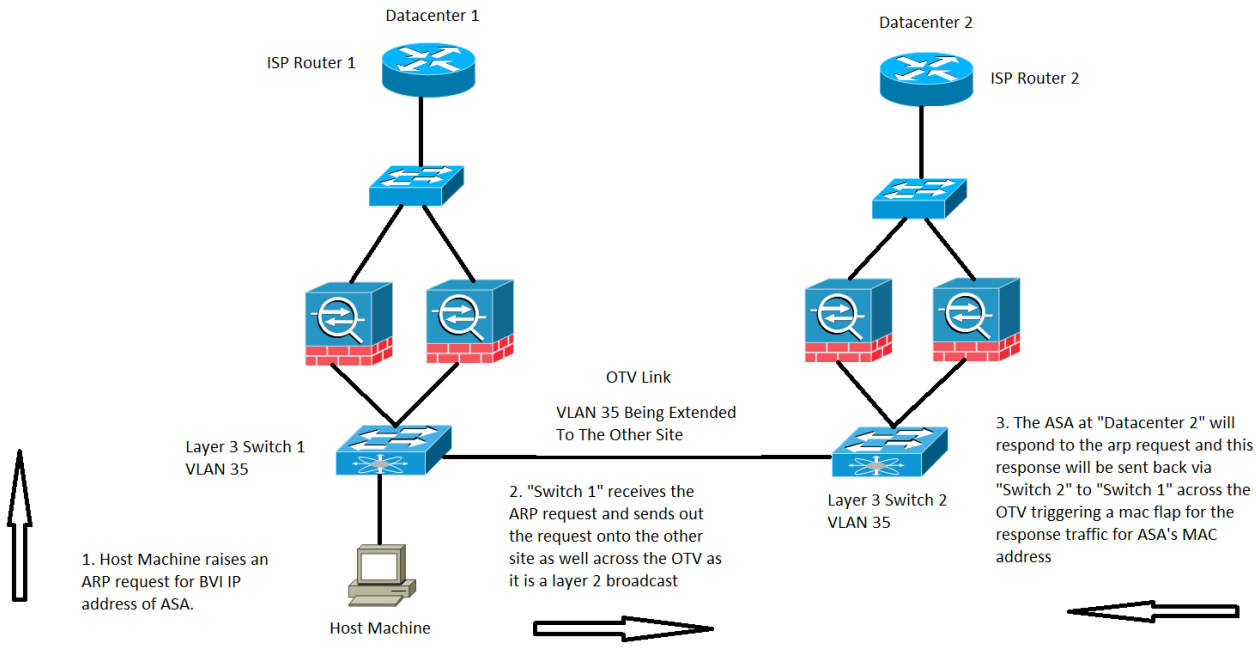


Esse caso específico será observado para qualquer tráfego gerado pelo próprio ASA. Aqui são consideradas duas situações possíveis, em que o ASA tenta alcançar um Network Time Protocol (NTP) ou um servidor Syslog, que estão na mesma sub-rede que sua interface BVI.No entanto, não está limitado a essas duas condições, essa situação pode acontecer sempre que o tráfego é gerado pelo ASA para qualquer endereço IP que esteja diretamente conectado aos endereços IP do BVI.

1. Se o ASA não tiver as informações ARP do servidor NTP/Syslog, o ASA gerará uma solicitação ARP para esse servidor.
2. Como a solicitação ARP é um pacote de broadcast, o Switch 1 receberá esse pacote de sua interface conectada do ASA e o inundará através de todas as interfaces na VLAN específica, incluindo o local remoto através do OTV.
3. O Switch 2 do local remoto receberá essa solicitação ARP do link OTV e, devido ao MAC de origem do ASA, ele gera uma notificação de oscilação de MAC, já que o mesmo endereço MAC é aprendido através do OTV através de suas interfaces locais diretamente conectadas ao ASA.

Cenário 5

Tráfego destinado ao endereço IP BVI do ASA de um host conectado diretamente, como mostrado na imagem:



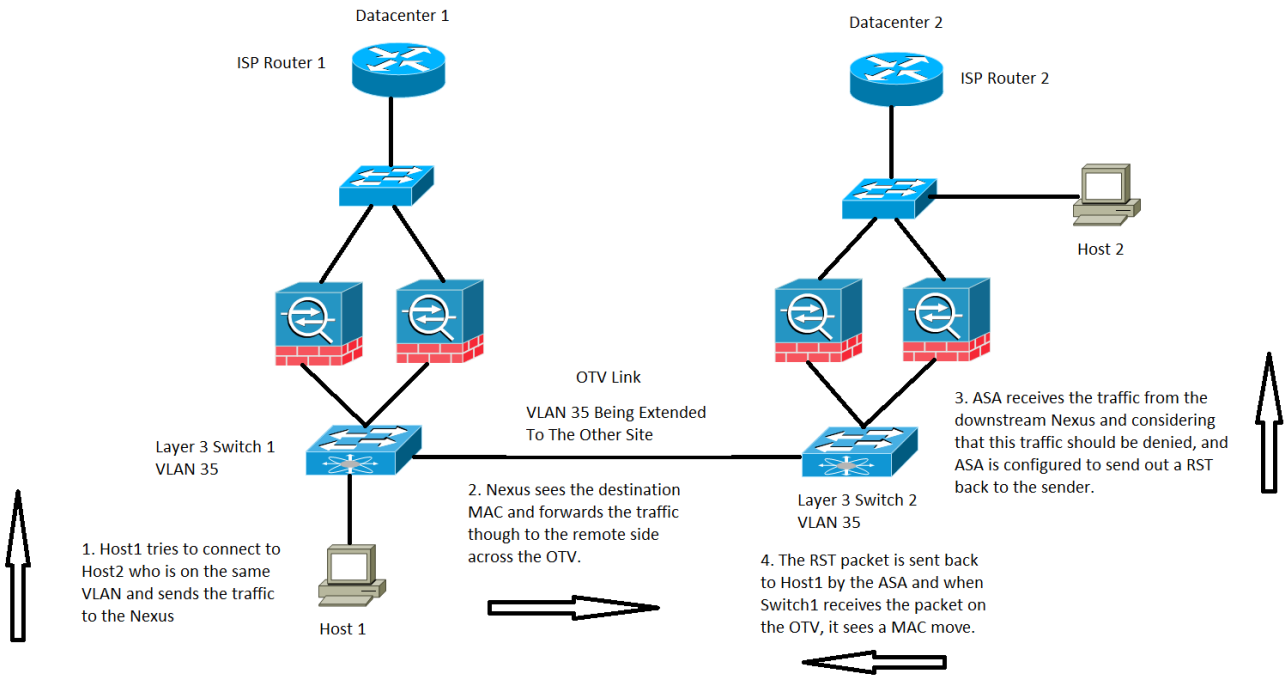
Um MOVE MAC também pode ser observado em momentos em que o tráfego é destinado ao endereço IP BVI do ASA.

No cenário, temos uma máquina host em uma rede diretamente conectada do ASA e estamos tentando se conectar ao ASA.

1. O host não tem o ARP do ASA e dispara uma solicitação ARP.
2. O Nexus recebe o tráfego e, novamente, como é um tráfego de broadcast, ele envia o tráfego através da OTV para o outro site também.
3. O ASA no datacenter remoto 2 pode responder à solicitação ARP e envia o tráfego de volta pelo mesmo caminho, que é o Switch 2 no lado remoto, OTV, Switch 1 no lado local e depois o host final.
4. Quando a resposta ARP é vista no Switch 1 do lado local, ela aciona uma notificação de movimentação do MAC enquanto vê o endereço MAC do ASA que vem do link OTV.

Cenário 6

ASA definido para negar o tráfego ao lado do qual envia um RST ao host, como mostrado na imagem:



Nesse caso, temos um host 1 na VLAN 35, ele tenta se comunicar com o host 2 na mesma VLAN da camada 3, no entanto, o host 2 está na verdade na VLAN 1535 do datacenter 2.

1. O endereço MAC do host 2 seria visto no Switch 2 através da interface conectada aos ASAs.
2. O switch 1 veria o endereço MAC do host 2 através do link OTV.
3. O host 1 envia tráfego para o host 2 e isso segue o caminho do switch 1, OTV, switch 2, ASAs no datacenter 2.
4. Esse específico é negado pelo ASA e como o ASA é configurado para enviar um RST de volta ao Host 1, o pacote RST volta com o endereço MAC origem do ASA.
5. Quando esse pacote volta ao Switch 1 através do OTV, o Switch 1 registra uma notificação de MOVE MAC para o endereço MAC do ASA porque agora vê o endereço MAC através do OTV, onde antes de ver o endereço de sua interface diretamente conectada.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Guia de configuração da CLI do Cisco ASA Series
- Suporte Técnico e Documentação - Cisco Systems