Problemas comuns com o conjunto transparente do Inter-local ASA

Índice

Introdução

Este documento descreve alguns dos problemas comuns com o conjunto medido do Inter-local do modo transparente do EtherChannel.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firewall adaptável da ferramenta de segurança (ASA)
- Aglomeração ASA

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Começando a versão ASA 9.2, a aglomeração do inter-local é apoiada onde as unidades ASA poderiam ser ficadas em datacenters diferentes e o link de controle do conjunto (CCL) é conectado sobre uma interconexão do centro de dados (DCI). Os cenários de distribuição possíveis são:

- Conjunto do Inter-local da interface individual
- Conjunto medido do Inter-local do modo transparente do EtherChannel
- Conjunto roteado medido do Inter-local do modo do EtherChannel (apoiado de 9.5 avante)

O MAC MOVE notificações

Quando um MAC address na tabela do Content Addressable Memory (CAM) muda a porta, uma notificação do MOVIMENTO MAC está gerada. Contudo, uma notificação do MOVIMENTO MAC não é gerada quando o MAC address é adicionado ou removido da tabela CAM. Supõe se um MAC address X é instruído através da relação GigabitEthernet0/1 no VLAN10 e após alguma hora o mesmo MAC está visto com GigabitEthernet0/2 no VLAN10, a seguir uma notificação do MOVIMENTO MAC está gerada.

Syslog do interruptor:

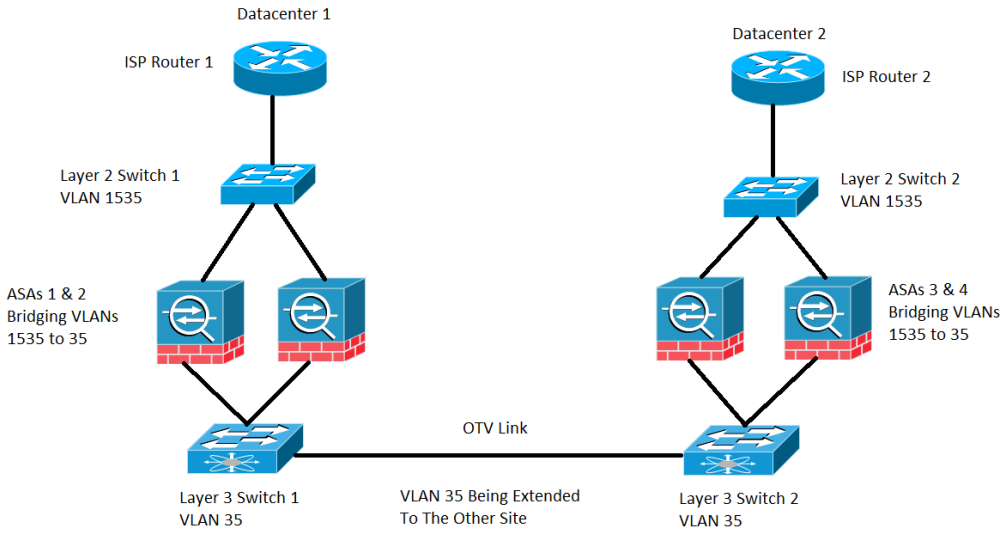
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1
to GigabitEthernet0/2
```

Syslog do ASA:

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

Diagrama de Rede

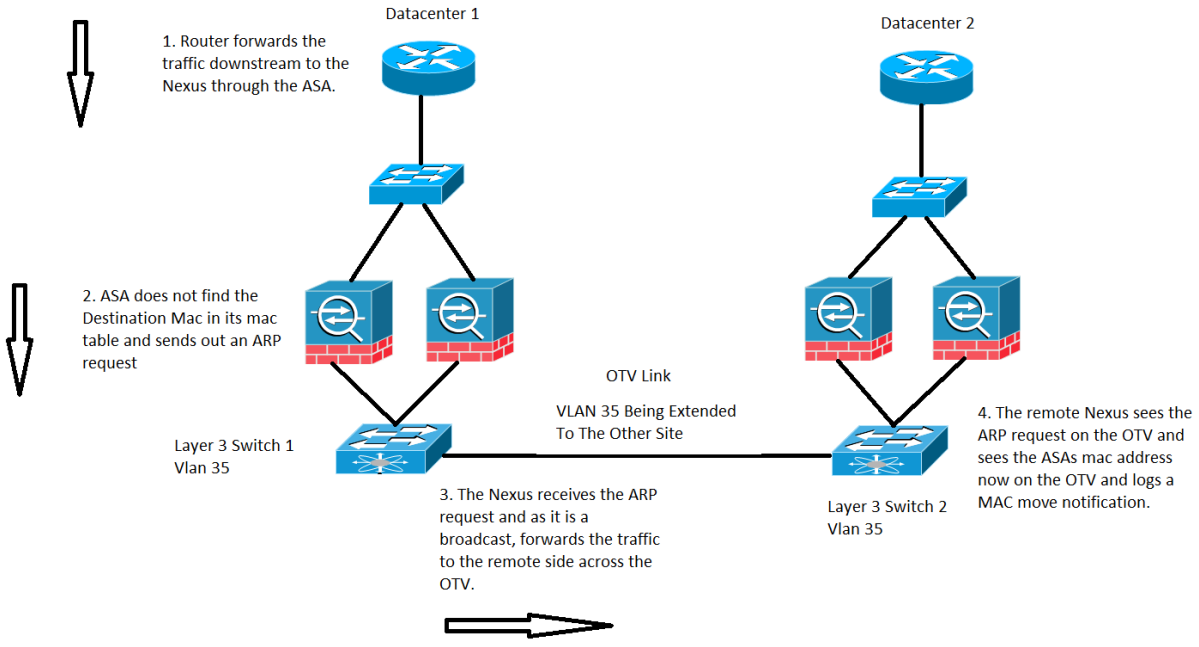
desenvolvimento do conjunto do Inter-local onde os ASA são configurados no modo transparente que constrói uma ponte sobre VLAN 1535 e VLAN 35. O VLAN interno 35 é prolongado sobre a virtualização do transporte da folha de prova (OTV) visto que o VLAN exterior 1535 não é prolongado sobre o OTV, segundo as indicações da imagem



O MAC move notificações no interruptor

Cenário 1

Trafique destinado a um MAC address cuja a entrada não esteja atual na tabela de MAC do ASA, segundo as indicações da imagem:



Em um ASA transparente, se o endereço MAC de destino do pacote que chega no ASA não está

na tabela de endereços MAC, manda uma requisição de protocolo de resolução de endereço (ARP) para esse destino (se na mesma sub-rede como o BVI) ou um pedido do Internet Control Message Protocol (ICMP) com Time to Live 1(TTL 1) com o MAC de origem como o MAC address do Bridge Virtual Interface (BVI) e o endereço MAC de destino como o controlador do acesso da mídia de destino (DMAC) é faltado.

No caso precedente, você tem este o fluxo de tráfego:

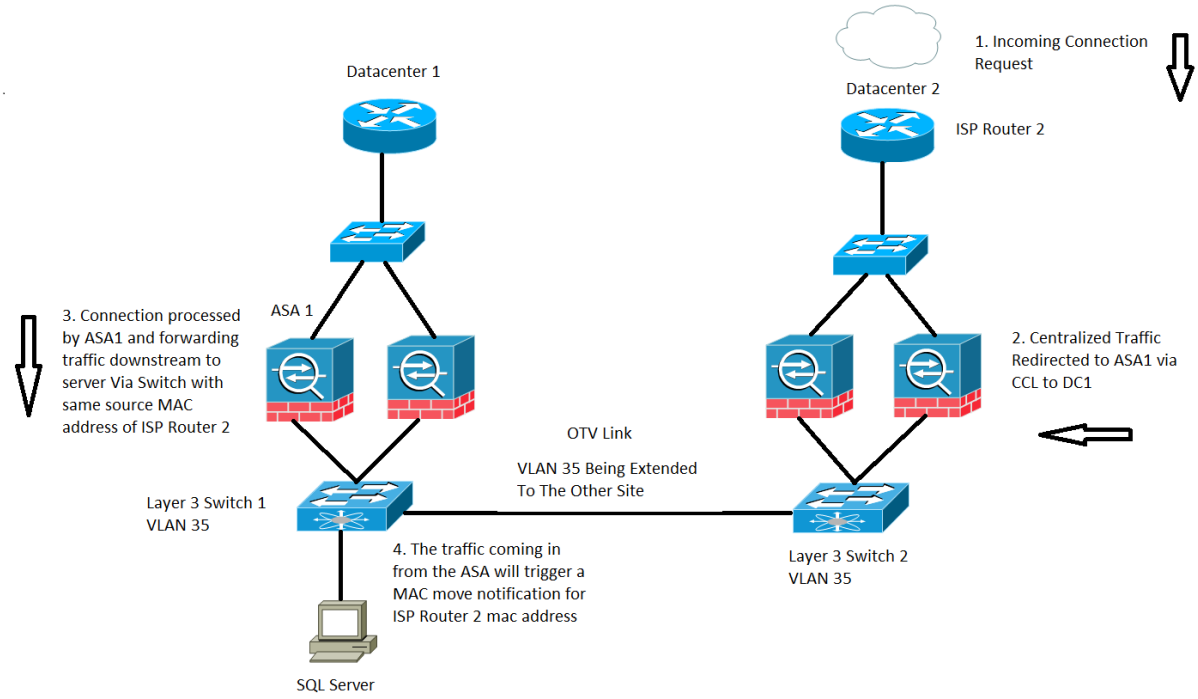
1. O roteador ISP em Datacenter 1 trafica para a frente a um destino específico que seja atrás do ASA.
2. Qualquer uma da lata do ASA recebe o tráfego e neste caso, o endereço MAC de destino do tráfego não é sabido pelo ASA.
3. Agora o IP de destino do tráfego está na mesma sub-rede como aquele do BVI e como mencionado antes, ASA gerencie agora uma requisição ARP para o IP de destino.
4. Switch1 recebe-ao tráfego e como o pedido é uma transmissão, para a frente o tráfego a Datacenter 2 assim como através do link OTV.
5. Quando Switch2 vê a requisição ARP do ASA no link OTV, registra uma notificação do MOVIMENTO MAC porque previamente o MAC address do ASA era instruído através diretamente da interface conectada e agora está sendo instruído através do link OTV.

Recomendações

Éuma encenação de canto. As tabelas de MAC são sincronizadas nos conjuntos, assim que é menos provável para um membro não ter uma entrada para um host particular. Um MAC-movimento ocasional para BVI conjunto-possuído MAC é julgado aceitável.

Cenário 2

Fluxo centralizado que processa pelo ASA, segundo as indicações da imagem:



O tráfego baseado inspeção através de um conjunto ASA é classificado em três tipos:

- Centralizado
- Distribuído
- Semi-distribuído

No caso da inspeção centralizada, todo o tráfego que as necessidades de obter inspecionem é reorientado à unidade mestra do conjunto ASA. Se uma unidade do escravo do conjunto ASA recebe o tráfego, está enviada ao mestre através do CCL.

Na imagem mais adiantada, você trabalha com tráfego SQL que é um protocolo de inspeção centralizado (CIP) e o comportamento descrito aqui é aplicável para todo o CIP.

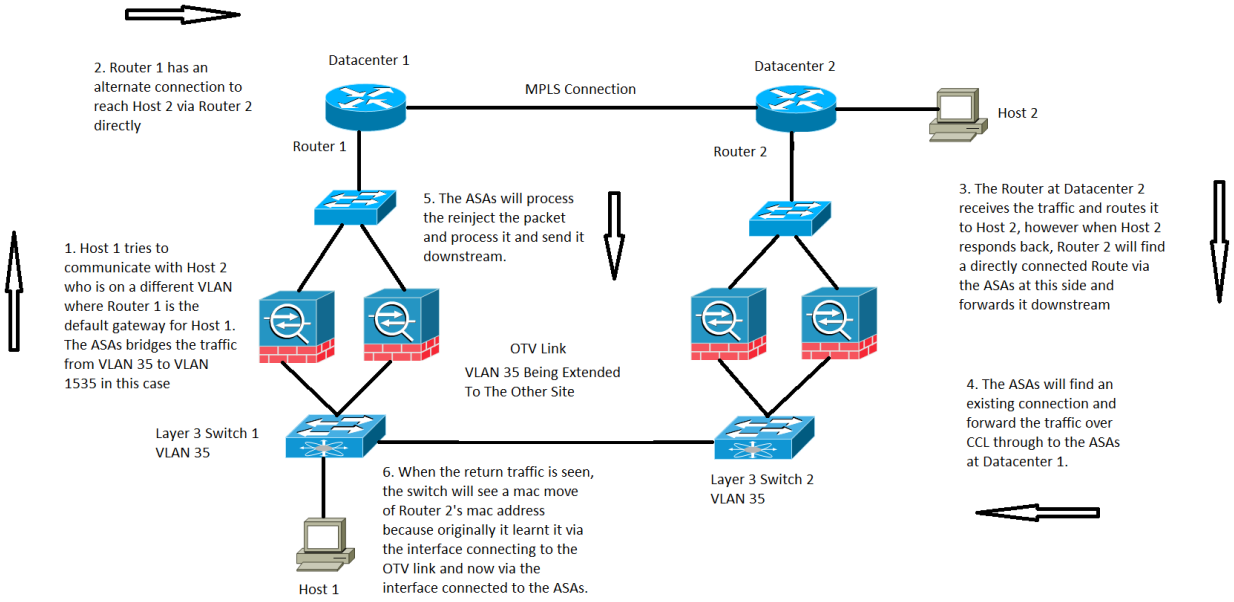
Você recebe o tráfego em Datacenter 2 onde você tem somente unidades do escravo do conjunto ASA, a unidade mestra é ficado situado em Datacenter 1 que é ASA 1.

1. O roteador ISP 2 em Datacenter 2 recebe-o o tráfego e para a frente rio abaixo aos ASA em seu local.
2. Qualquer um dos ASA pode receber este tráfego e uma vez que determina que este tráfego precisa de ser inspecionado e enquanto o protocolo o é centralizado para a frente o tráfego sobre à unidade mestra através do CCL.
3. O ASA 1 recebe o fluxo de tráfego através do CCL, processa o tráfego e envia-o rio abaixo ao servidor SQL.
4. Agora em que o ASA 1 para a frente o tráfego rio abaixo, ele retém o MAC address da fonte original do roteador ISP 2 que está ficado situado em Datacenter 2 e o envia rio abaixo.
5. Quando Switch1 recebe este tráfego específico, entra uma notificação do MOVIMENTO MAC porque considera originalmente que MAC address do roteador ISP 2 através do link OTV que é conectado a Datacenter 2 e agora ele vê o tráfego que vem dentro das relações conectadas ao ASA 1.

Recomendações

Recomenda-se distribuir as conexões centralizadas a qualquer local hospeda o mestre (baseado em prioridades), segundo as indicações da imagem:

Cenário 3



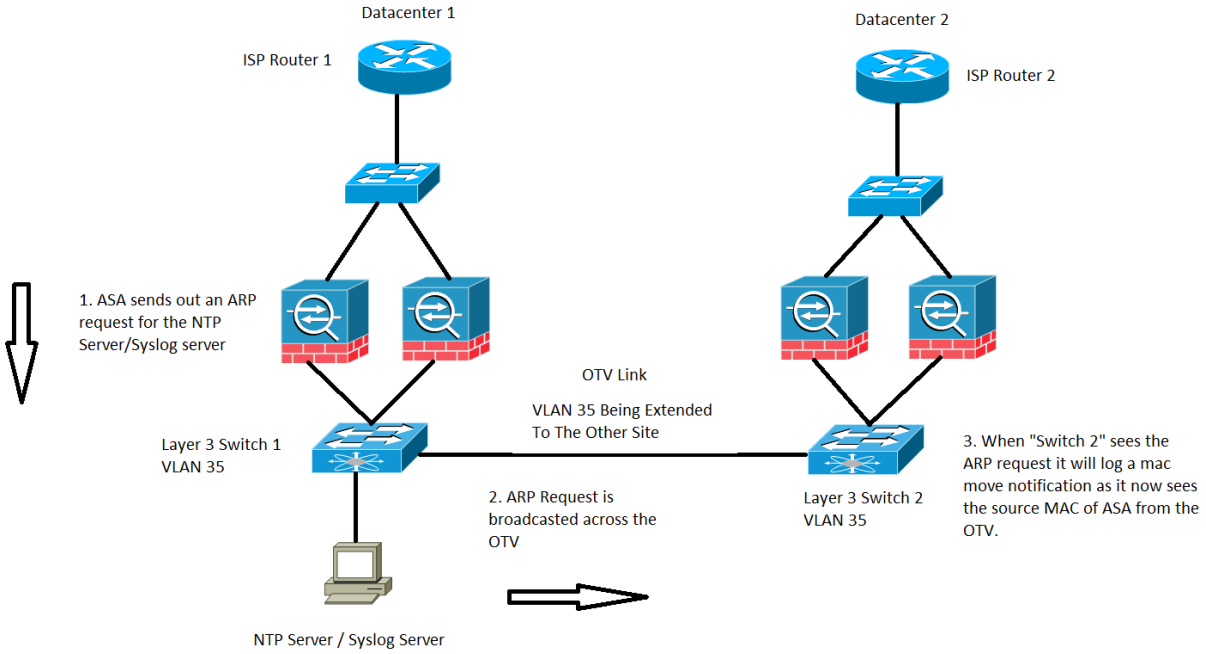
Para uma comunicação inter do controlador de domínio (DC) no modo transparente, este fluxo de tráfego específico não é coberto ou é documentado mas este fluxo de tráfego específico trabalha de um fluxo ASA que processa o ponto de vista. Contudo, pode conduzir às notificações do movimento MAC no interruptor.

1. O host 1 em VLAN 35 tenta comunicar-se com o host 2 que esta presente no outro Datacenter.
2. O host 1 tem um gateway padrão que seja roteador1 e o roteador1 tenha um trajeto para alcançar o host 2 podendo se comunicar com o roteador2 diretamente através de um link alternativo e neste caso nós supomos o Multiprotocol Label Switching (MPLS) e não através do conjunto ASA.
3. O roteador2 recebe o tráfego de entrada e distribui-o sobre para hospedar 2.
4. Agora em que o host 2 responde para trás, o roteador2 recebe o tráfego de retorno e encontra diretamente uma rota conectada com os ASA em vez do tráfego que envie sobre o MPLS.
5. Nesta fase, o tráfego que deixa o roteador2 tem o MAC de origem da relação da saída do roteador 2's.
6. Os ASA em Datacenter 2 recebem o tráfego de retorno e encontram uma conexão que exista e seja feita pelos ASA em Datacenter 1.
7. Os ASA em Datacenter 2 enviam o tráfego de retorno sobre o CCL de volta aos ASA em Datacenter 1.
8. Nesta fase os ASA em Datacenter 1 processam o tráfego de retorno e enviam-no para baixo para Switch1. O pacote ainda tem o mesmo MAC de origem que aquele da relação da saída do roteador 2's.
9. Agora em que Switch1 recebe o pacote, registra uma notificação do movimento MAC porque inicialmente aprendeu o MAC address do roteador 2's através da relação que é conectada

ao link OTV, porém nesta fase começa aprender o MAC address da relação conectada aos ASA.

Encenação 4

Tráfego gerado pelo ASA, segundo as indicações da imagem:

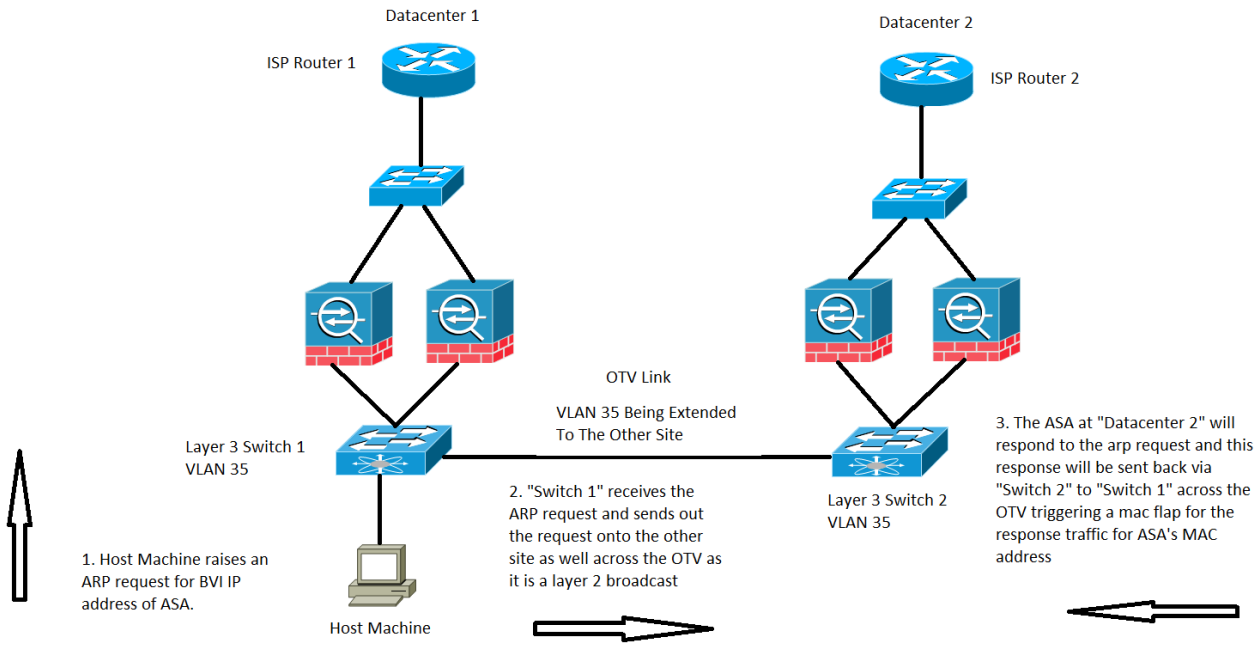


Este caso específico será observado para todo o tráfego que obtiver gerado pelo ASA próprio. Duas situações possíveis são consideradas aqui, onde o ASA tenta alcançar um Network Time Protocol (NTP) ou um servidor de SYSLOG, que estejam na mesma sub-rede como aquele de sua interface de BVI. Porém é limitada não somente a estas duas circunstâncias, esta situação pode acontecer sempre que o tráfego é gerado pelo ASA para todo o endereço IP de Um ou Mais Servidores Cisco ICM NT que for conectado diretamente aos endereços IP de Um ou Mais Servidores Cisco ICM NT BVI.

1. Se o ASA não tem a informação ARP do servidor de NTP/servidor de SYSLOG, a seguir o ASA gerará uma requisição ARP para esse server.
2. Porque a requisição ARP é um pacote de transmissão, Switch1 receberá este pacote de sua interface conectada do ASA e inundá-lo-á para fora através de todas as relações no VLAN específico que inclui o local remoto através do OTV.
3. O local remoto Switch2 receberá esta requisição ARP do link OTV e devido ao MAC de origem do ASA, gerencie uma notificação do flap MAC desde que o mesmo MAC address é instruído através do OTV através de suas interfaces conectadas do local diretamente ao ASA.

Encenação 5

Trafique destinado ao endereço IP de Um ou Mais Servidores Cisco ICM NT BVI do ASA diretamente de um host conectado, segundo as indicações da imagem:



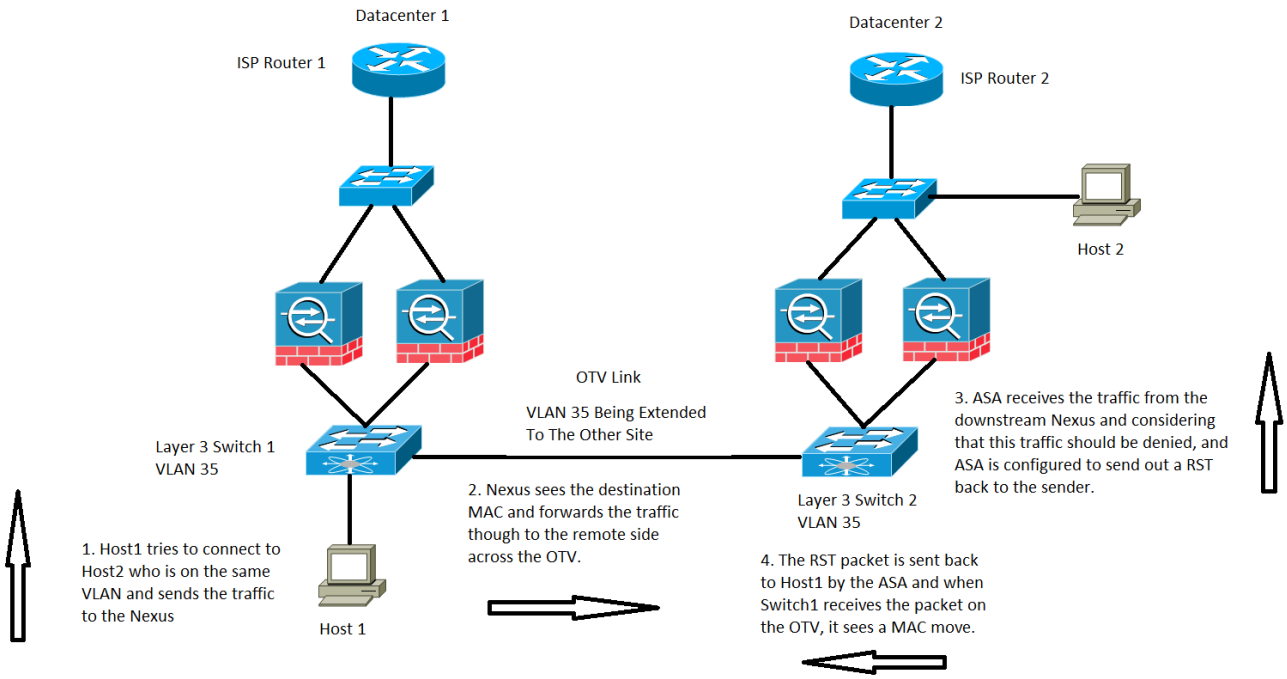
UM MOVIMENTO MAC pode igualmente ser observado às vezes quando o tráfego é destinado ao endereço IP de Um ou Mais Servidores Cisco ICM NT BVI do ASA.

Na encenação, nós temos uma máquina host diretamente em uma rede conectada do ASA e estamos tentando-a conectar ao ASA.

1. O host não tem o ARP do ASA e provoca uma requisição ARP.
2. O nexo recebe o tráfego e outra vez porque é um tráfego de broadcast que envia o tráfego através do OTV ao outro local também.
3. O ASA no Datacenter remoto 2 pode responder à requisição ARP e envia o tráfego para trás através do mesmo trajeto que é Switch2 no lado remoto, OTV, Switch1 no lado local e então no host final.
4. Quando a reação ARP é considerada no lado local Switch1, provoca uma notificação do movimento MAC enquanto considera o MAC address do ASA que vem dentro do link OTV.

Encenação 6

Grupo ASA para negar o tráfego junto com que envia um RST ao host, segundo as indicações da imagem:



Neste caso, nós temos um host 1 do host em VLAN 35, ele tentamos comunicar-se com o host 2 na mesma camada 3 VLAN, contudo, o host 2 está realmente em Datacenter 2 VLAN 1535.

1. O endereço do host 2MAC seria considerado em Switch2 através da relação conectada aos ASA.
2. Switch1 estaria vendo o MAC address do host 2 através do link OTV.
3. O host 1 envia o tráfego para hospedar 2 e este segue o trajeto de Switch1, OTV, Switch2, ASA em Datacenter 2.
4. Este específico obtém negado pelo ASA e como o ASA é configurado para enviar para trás um RST para hospedar 1, o pacote de RST volta com endereço MAC de origem do ASA.
5. Quando este pacote o faz de volta a Switch1 através do OTV, Switch1 registra uma notificação do MOVIMENTO MAC para o MAC address do ASA porque considera agora o MAC address através do OTV, onde antes que ver o endereço de sua diretamente interface conectada.

Verificar

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

Troubleshooting

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

Informações Relacionadas

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