Problemas comunes con el clúster transparente entre sitios de ASA

Contenido

Introducción

Este documento describe algunos de los problemas comunes con el clúster EtherChannel Transparent Mode Inter-Site extendido.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firewall Adaptive Security Appliance (ASA)
- clustering ASA

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Antecedentes

A partir de la versión 9.2 de ASA, se admite la agrupación en clúster entre sitios, en la que las unidades ASA se pueden ubicar en distintos Data Centers y el enlace de control de clúster (CCL) se conecta a través de un Data Center Interconnect (DCI). Los posibles escenarios de implementación son:

- Clúster entre sitios de interfaz individual
- Clúster entre sitios de modo transparente EtherChannel extendido
- Clúster entre sitios de modo enrutado EtherChannel extendido (compatible a partir de 9.5)

Notificaciones MAC MOVE

Cuando una dirección MAC en la tabla Content Addressable Memory (CAM) cambia de puerto, se genera una notificación MAC MOVE. Sin embargo, una notificación MOVE MAC no se genera cuando la dirección MAC se agrega o quita de la tabla CAM. Suponga que si se detecta una dirección MAC X a través de la interfaz GigabitEthernet0/1 en VLAN10 y después de cierto tiempo se ve el mismo MAC a través de GigabitEthernet0/2 en VLAN 10, se genera una notificación MAC MOVE.

Registro del sistema desde el switch:

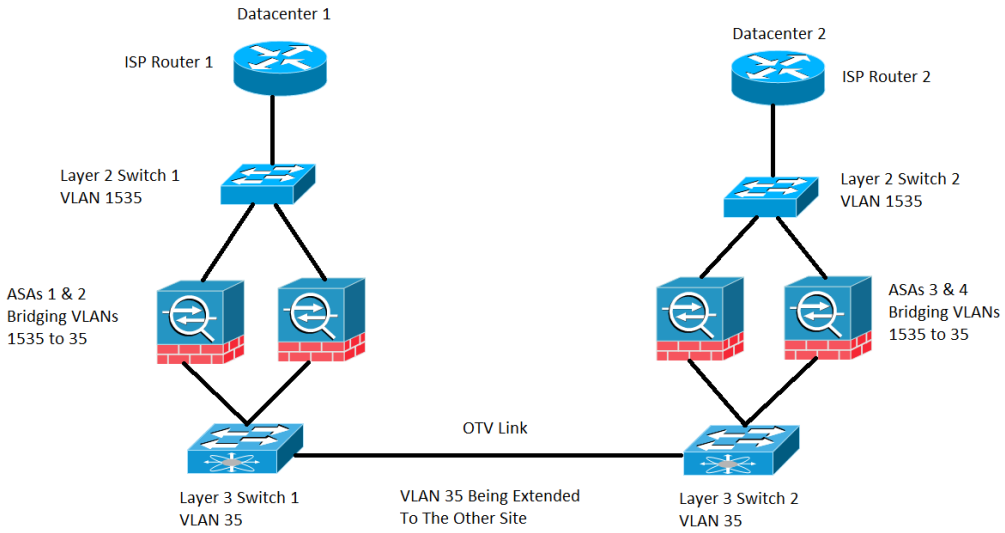
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1
to GigabitEthernet0/2
```

Syslog de ASA:

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

Diagrama de la red

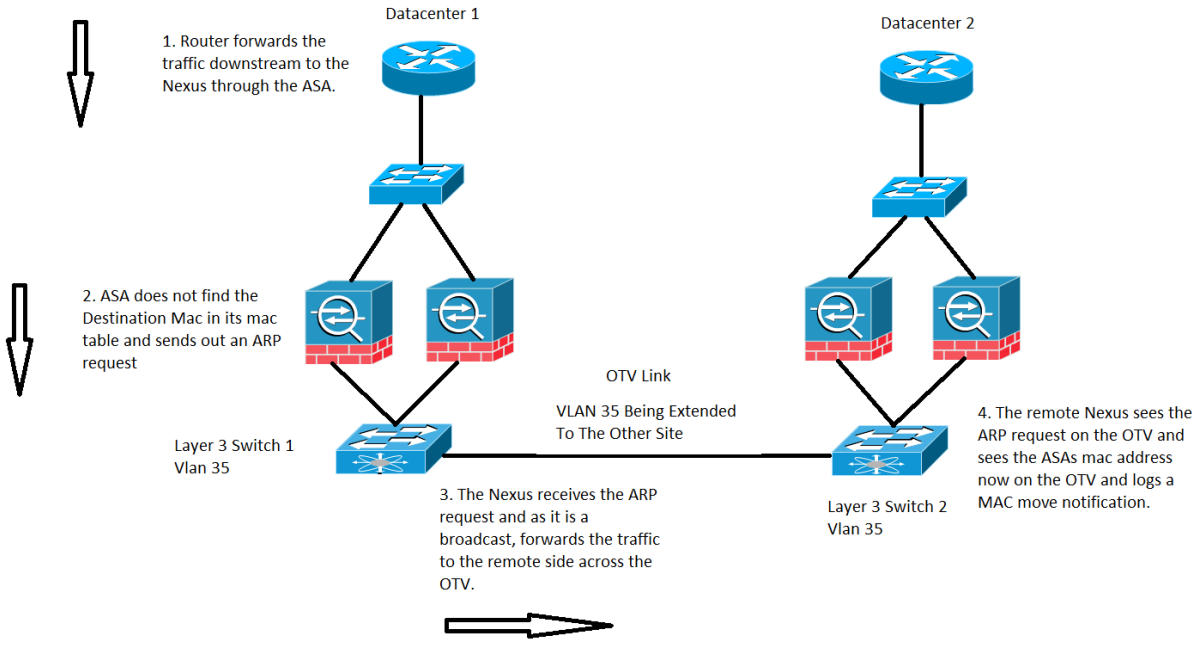
Implementación de clúster entre sitios donde los ASA se configuran en modo transparente bridging VLAN 1535 y VLAN 35. La VLAN 35 interna se amplía sobre la Overlay Transport Virtualization (OTV), mientras que la VLAN 1535 externa no se amplía sobre la OTV, como se muestra en la imagen



MAC Move Notifications on Switch

Escenario 1

Tráfico destinado a una dirección MAC cuya entrada no está presente en la tabla MAC del ASA, como se muestra en la imagen:



En un ASA transparente, si la dirección MAC de destino del paquete que llega al ASA no está en

la tabla de direcciones MAC, envía una solicitud de protocolo de resolución de direcciones (ARP) para ese destino (si se encuentra en la misma subred que BVI) o una solicitud de protocolo de mensajes de control de Internet (ICMP) con Tiempo de vida 1(TTL 1) con MAC de origen como dirección MAC de interfaz virtual de puente (BVI) Se ha perdido la dirección MAC como Controlador de acceso a medios de destino (DMAC).

En el caso anterior, tiene este flujo de tráfico:

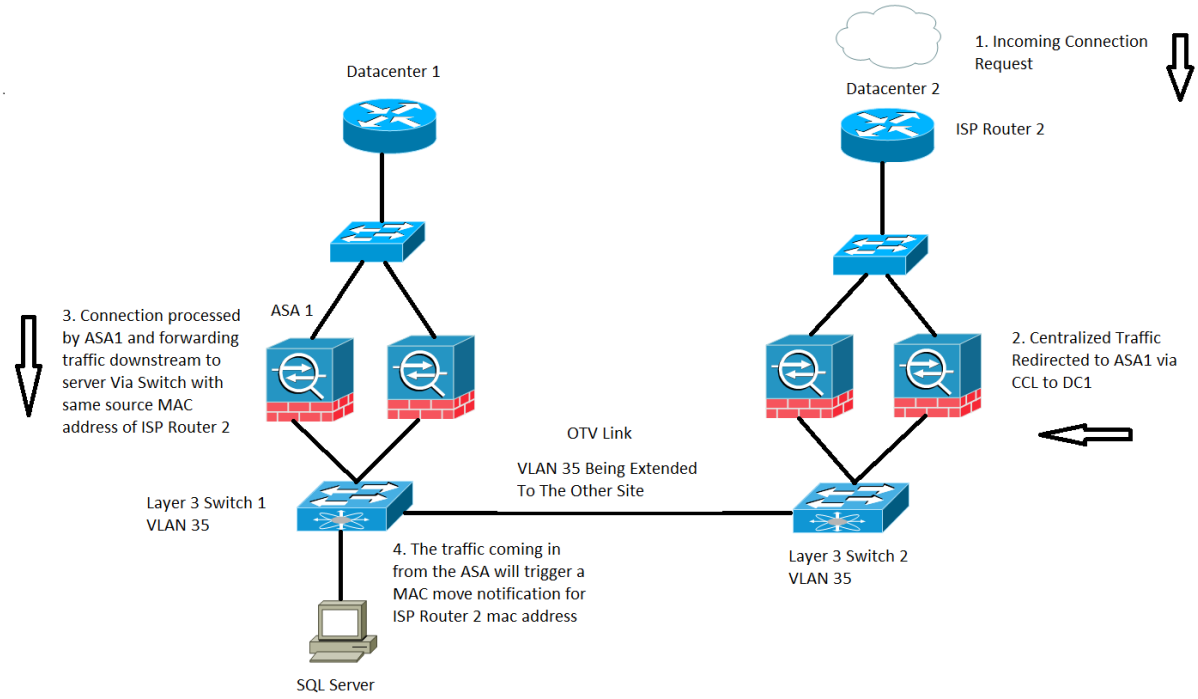
1. El router ISP en el Data Center 1 reenvía el tráfico a un destino específico que se encuentra detrás del ASA.
2. Cualquiera de los ASA puede recibir el tráfico y, en este caso, ASA no conoce la dirección MAC de destino del tráfico.
3. Ahora, la IP de destino del tráfico está en la misma subred que la de la BVI y, como se mencionó anteriormente, ASA ahora genera una solicitud ARP para la IP de destino.
4. El Switch 1 recibe el tráfico y, como la solicitud es una difusión, reenvía el tráfico al Data Center 2 así como a través del enlace OTV.
5. Cuando el Switch 2 ve la solicitud ARP del ASA en el link OTV, registra una notificación MAC MOVE porque anteriormente la dirección MAC de ASA se aprendió a través de la interfaz conectada directamente y ahora se está aprendiendo a través del link OTV.

Recomendaciones

Es un escenario de esquina. Las tablas MAC se sincronizan en clústeres, por lo que es menos probable que un miembro no tenga una entrada para un host determinado. Se considera aceptable un movimiento ocasional de MAC para MAC BVI propiedad del clúster.

Escenario 2

Procesamiento de flujo centralizado por ASA, como se muestra en la imagen:



El tráfico basado en inspección en un clúster ASA se clasifica en tres tipos:

- Centralizado
- Distribuido
- Semidistribuido

En el caso de la inspección centralizada, cualquier tráfico que deba inspeccionarse se redirige a la unidad maestra del clúster ASA. Si una unidad esclava del clúster ASA recibe el tráfico, se reenvía al maestro a través de la CCL.

En la imagen anterior, se trabaja con el tráfico SQL, que es un protocolo de inspección centralizado (CIP), y el comportamiento descrito aquí se aplica a cualquier CIP.

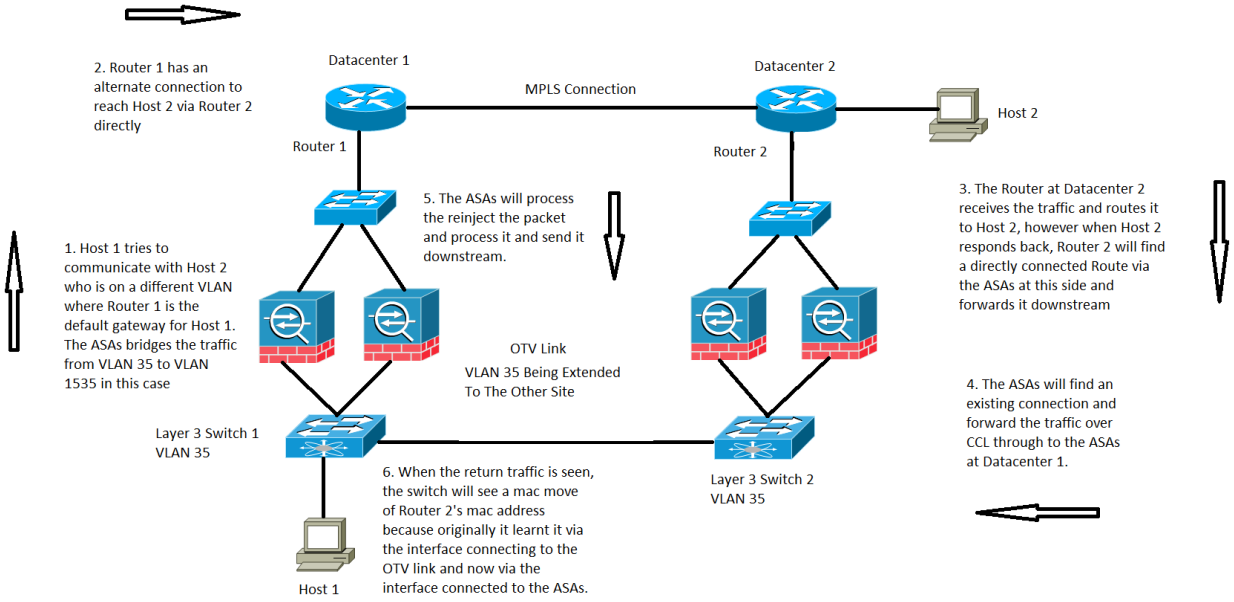
Recibe el tráfico en el Data Center 2, donde sólo tiene unidades esclavas del clúster ASA, la unidad maestra se encuentra en el Data Center 1, que es ASA 1.

1. El router ISP 2 en el Data Center 2 recibe el tráfico y lo reenvía a los ASA en su sitio.
2. Cualquiera de los ASA puede recibir este tráfico y una vez que determina que este tráfico debe ser inspeccionado y, como el protocolo está centralizado, reenvía el tráfico a la unidad maestra a través de la CCL.
3. ASA 1 recibe el flujo de tráfico a través de la CCL, procesa el tráfico y lo envía de flujo descendente a SQL Server.
4. Ahora, cuando ASA 1 reenvía el tráfico descendente, conserva la dirección MAC de origen original del router ISP 2, que se encuentra en el Data Center 2 y lo envía en sentido descendente.
5. Cuando el Switch 1 recibe este tráfico específico, inicia sesión en una notificación MAC MOVE porque originalmente ve la dirección MAC del Router ISP 2 a través del link OTV que está conectado al Data Center 2 y ahora ve el tráfico que viene de las interfaces conectadas al ASA 1.

Recomendaciones

Se recomienda rutear las conexiones centralizadas a cualquier sitio que aloje al maestro (en función de las prioridades), como se muestra en la imagen:

Escenario 3



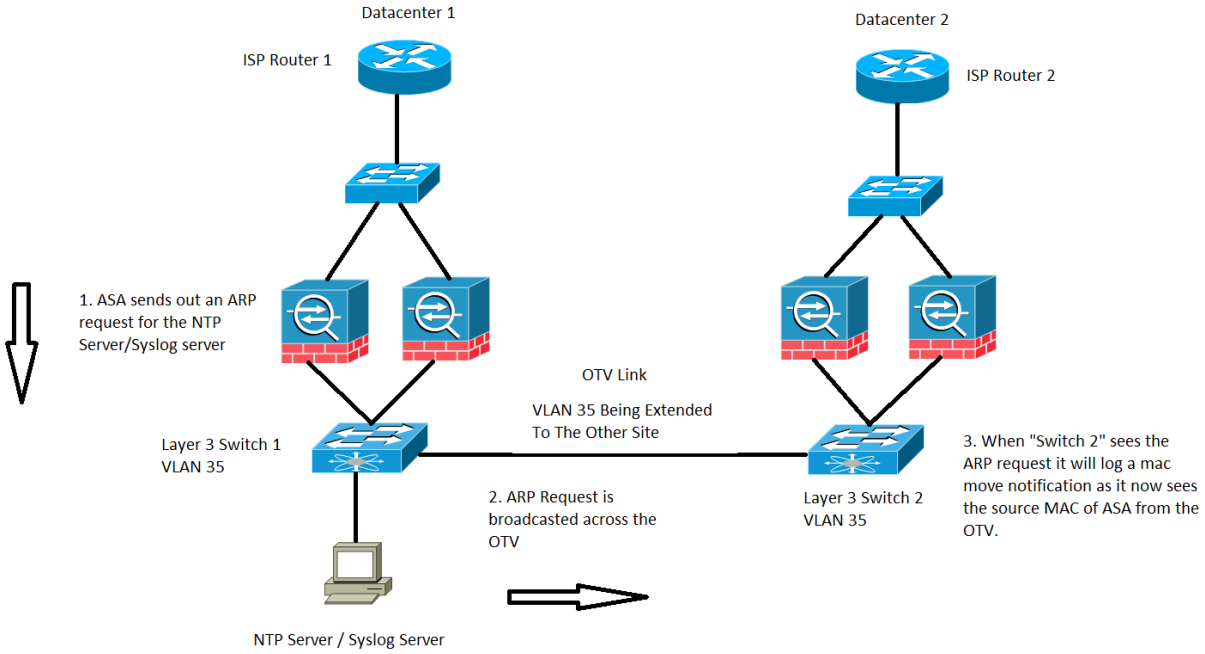
Para una comunicación entre controladores de dominio (DC) en modo transparente, este flujo de tráfico específico no está cubierto ni documentado, pero este flujo de tráfico específico funciona desde un punto de vista de procesamiento de flujo ASA. Sin embargo, puede dar lugar a notificaciones de movimiento de MAC en el switch.

1. El Host 1 en la VLAN 35 intenta comunicarse con el Host 2 que está presente en el otro Data Center.
2. El Host 1 tiene una gateway predeterminada que es el Router 1 y el Router 1 tiene una trayectoria para alcanzar el Host 2 al poder comunicarse con el Router 2 directamente a través de un link alternativo y en este caso asumimos Multiprotocol Label Switching (MPLS) y no a través del clúster ASA.
3. El Router 2 recibe el tráfico entrante y lo rutea al Host 2.
4. Ahora, cuando el Host 2 responde, el Router 2 recibe el tráfico de retorno y encuentra una ruta directamente conectada a través de los ASA en lugar del tráfico que envía a través de MPLS.
5. En esta etapa, el tráfico que sale del Router 2 tiene el MAC de origen de la interfaz de salida del Router 2.
6. Los ASA en el Data Center 2 reciben el tráfico de retorno y encuentran una conexión que existe y es realizada por los ASA en el Datacenter 1.
7. Los ASA en el Data Center 2 envían el tráfico de retorno a través de CCL a los ASA en el Data Center 1.
8. En esta etapa, los ASA en el Data Center 1 procesan el tráfico de retorno y lo envían hacia el Switch 1. El paquete aún tiene el mismo MAC de origen que la interfaz de salida del Router 2.
9. Ahora, cuando el Switch 1 recibe el paquete, registra una notificación de movimiento de MAC porque inicialmente aprendió la dirección MAC del Router 2 a través de la interfaz que

está conectada al link OTV; sin embargo, en esta etapa comienza a aprender la dirección MAC de la interfaz conectada a los ASA.

Situación 4

Tráfico generado por el ASA, como se muestra en la imagen:

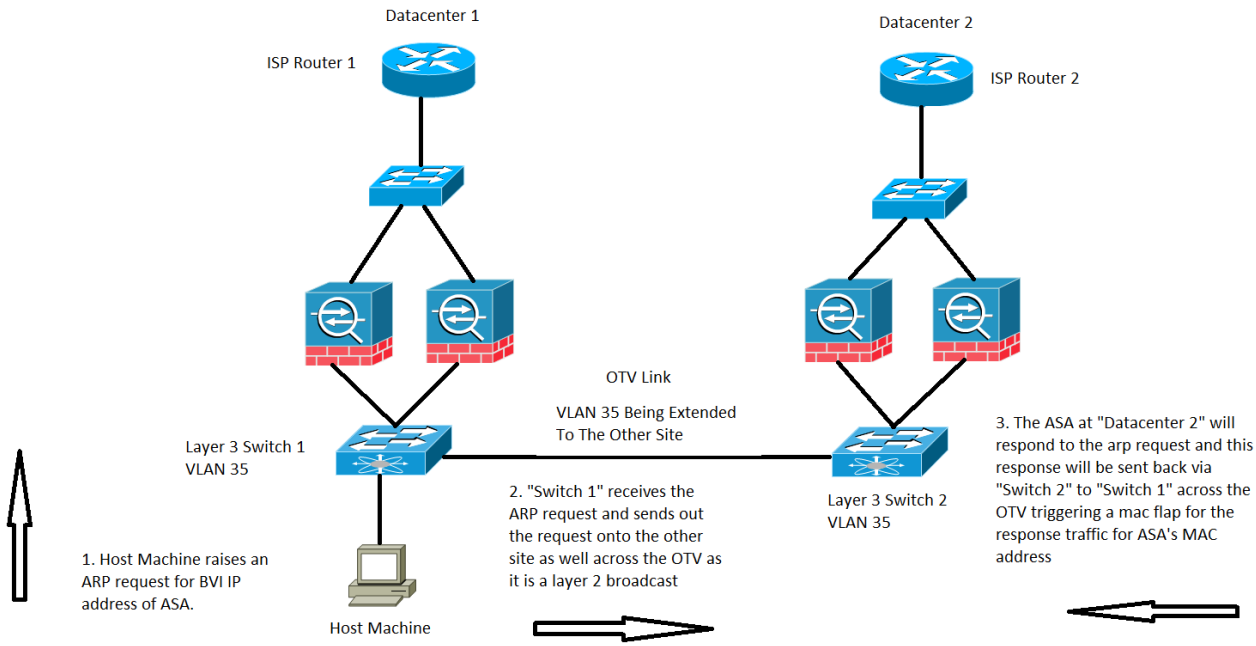


Este caso específico se observará para cualquier tráfico generado por el propio ASA. Aquí se consideran dos situaciones posibles, en las que el ASA intenta alcanzar un protocolo de tiempo de red (NTP) o un servidor Syslog, que se encuentran en la misma subred que la de su interfaz BVI. Sin embargo, no sólo se limita a estas dos condiciones, esta situación puede ocurrir siempre que el ASA genere tráfico para cualquier dirección IP que esté directamente conectada a las direcciones IP BVI.

1. Si ASA no tiene la información ARP del servidor NTP/servidor Syslog, el ASA generará una solicitud ARP para ese servidor.
2. Como la solicitud ARP es un paquete de difusión, el Switch 1 recibirá este paquete de su interfaz conectada del ASA e lo inundará a través de todas las interfaces en la VLAN específica, incluido el sitio remoto a través del OTV.
3. El switch 2 del sitio remoto recibirá esta solicitud ARP del link OTV y debido a la MAC de origen del ASA, genera una notificación de inestabilidad MAC ya que la misma dirección MAC se aprende a través del OTV a través de sus interfaces locales directamente conectadas al ASA.

Situación 5

Tráfico destinado a la dirección IP BVI del ASA desde un host conectado directamente, como se muestra en la imagen:



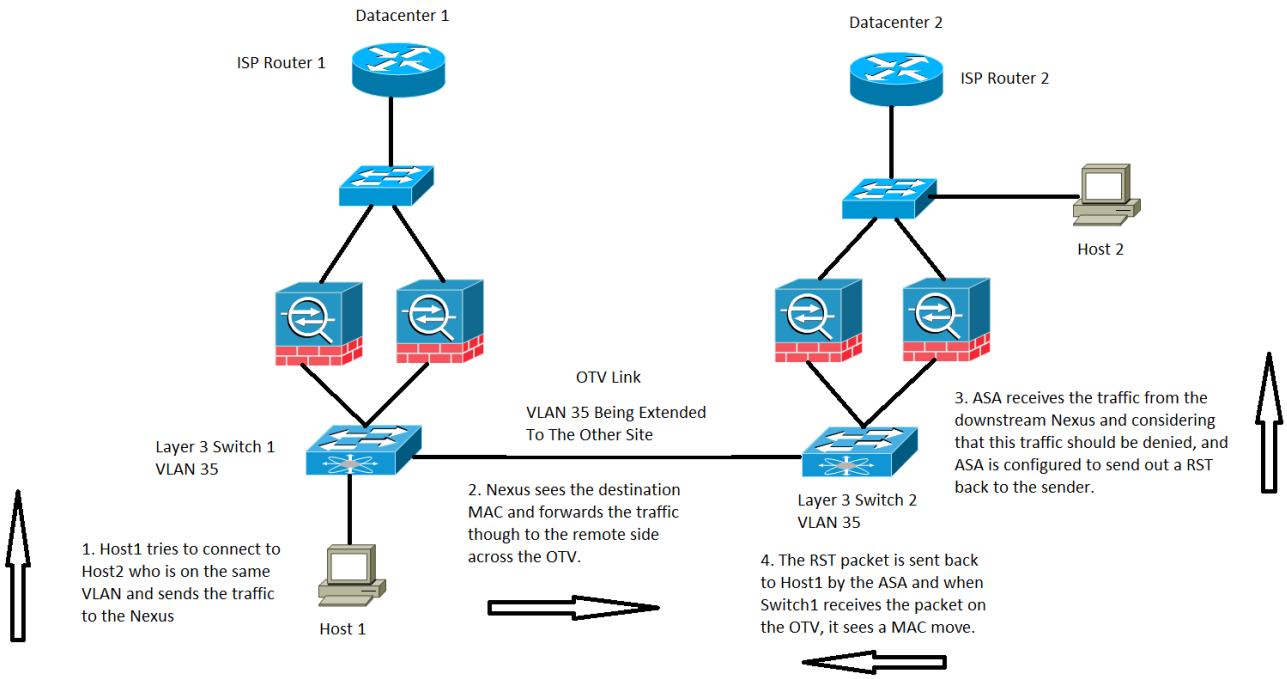
También se puede observar un MOVE MAC en momentos en que el tráfico se dirige a la dirección IP BVI del ASA.

En esta situación, disponemos de una máquina host en una red conectada directamente del ASA y estamos intentando conectarse al ASA.

1. El Host no tiene el ARP del ASA y activa una solicitud ARP.
2. El Nexus recibe el tráfico y, de nuevo, como tráfico de difusión, también envía el tráfico a través de OTV al otro sitio.
3. El ASA en el Data Center remoto 2 puede responder a la solicitud ARP y enviar el tráfico de vuelta a través de la misma trayectoria que el Switch 2 en el lado remoto, OTV, el Switch 1 en el lado local y luego el host final.
4. Cuando se ve la respuesta ARP en el switch 1 del lado local, se activa una notificación de movimiento de MAC ya que ve la dirección MAC del ASA que ingresa desde el link OTV.

Situación 6

ASA se configura para denegar el tráfico junto con el cual envía un RST al host, como se muestra en la imagen:



En este caso, tenemos un host Host 1 en VLAN 35, intenta comunicarse con el Host 2 en la misma VLAN de Capa 3, sin embargo, el Host 2 está realmente en la VLAN 1535 del Data Center 2.

1. La dirección MAC del host 2 se vería en el switch 2 a través de la interfaz conectada a los ASA.
2. El switch 1 vería la dirección MAC del host 2 a través del link OTV.
3. El Host 1 envía tráfico al Host 2 y esto sigue la trayectoria del Switch 1, OTV, el Switch 2, ASA en el Data Center 2.
4. El ASA niega esta información específica y, como ASA está configurado para devolver un RST al Host 1, el paquete RST regresa con la dirección MAC de origen del ASA.
5. Cuando este paquete vuelve al Switch 1 a través del OTV, el Switch 1 registra una notificación MAC MOVE para la dirección MAC del ASA porque ahora ve la dirección MAC a través del OTV, donde antes ve la dirección desde su interfaz conectada directamente.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Guía de Configuración de Cisco ASA Series CLI
- Soporte Técnico y Documentación - Cisco Systems