Problemi comuni con il cluster trasparente tra siti ASA

Sommario

Introduzione

Questo documento descrive alcuni dei problemi comuni del cluster tra siti in modalità trasparente EtherChannel con spanning.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firewall Adaptive Security Appliance (ASA)
- Clustering ASA

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

A partire dalla versione 9.2 di ASA, è supportato il clustering tra siti, in cui le unità ASA potrebbero trovarsi in data center diversi e il Cluster Control Link (CCL) sia connesso tramite un'interconnessione tra data center (DCI). Gli scenari di distribuzione possibili sono:

- Cluster intersito interfaccia singola
- Cluster tra siti in modalità trasparente EtherChannel con spanning
- Cluster tra siti in modalità di routing tra canali Spanning EtherChannel (supportato dalla versione 9.5 in avanti)

Notifiche di spostamento MAC

Quando un indirizzo MAC nella tabella CAM (Content Addressable Memory) cambia porta, viene generata una notifica di SPOSTAMENTO MAC. Tuttavia, non viene generata una notifica MAC MOVE quando l'indirizzo MAC viene aggiunto o rimosso dalla tabella CAM. Si supponga che un indirizzo MAC X venga appreso tramite l'interfaccia Gigabit Ethernet0/1 nella VLAN 10 e che dopo un certo periodo di tempo lo stesso MAC venga rilevato tramite Gigabit Ethernet0/2 nella VLAN 10, venga generata una notifica MAC MOVE.

Syslog da switch:

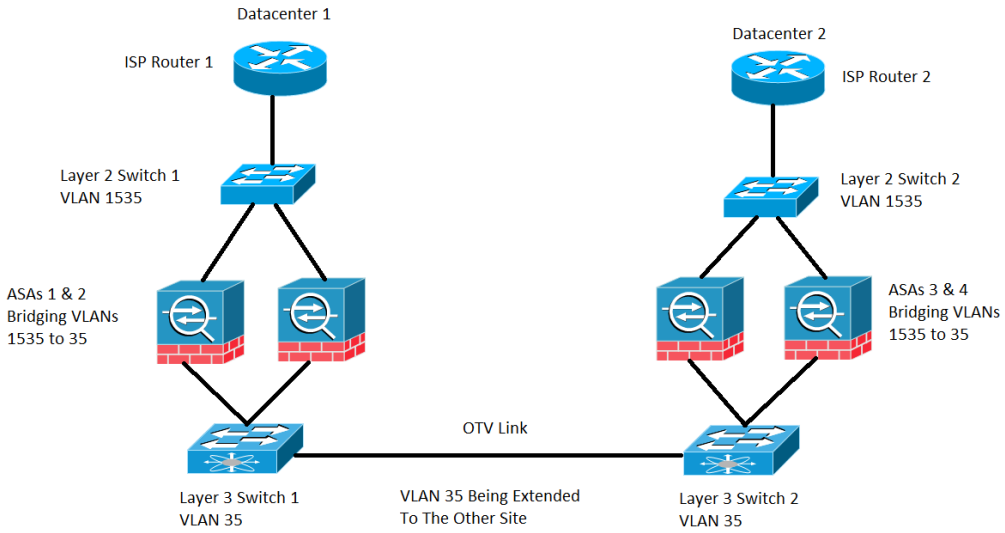
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1
to GigabitEthernet0/2
```

Syslog da ASA:

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

Esempio di rete

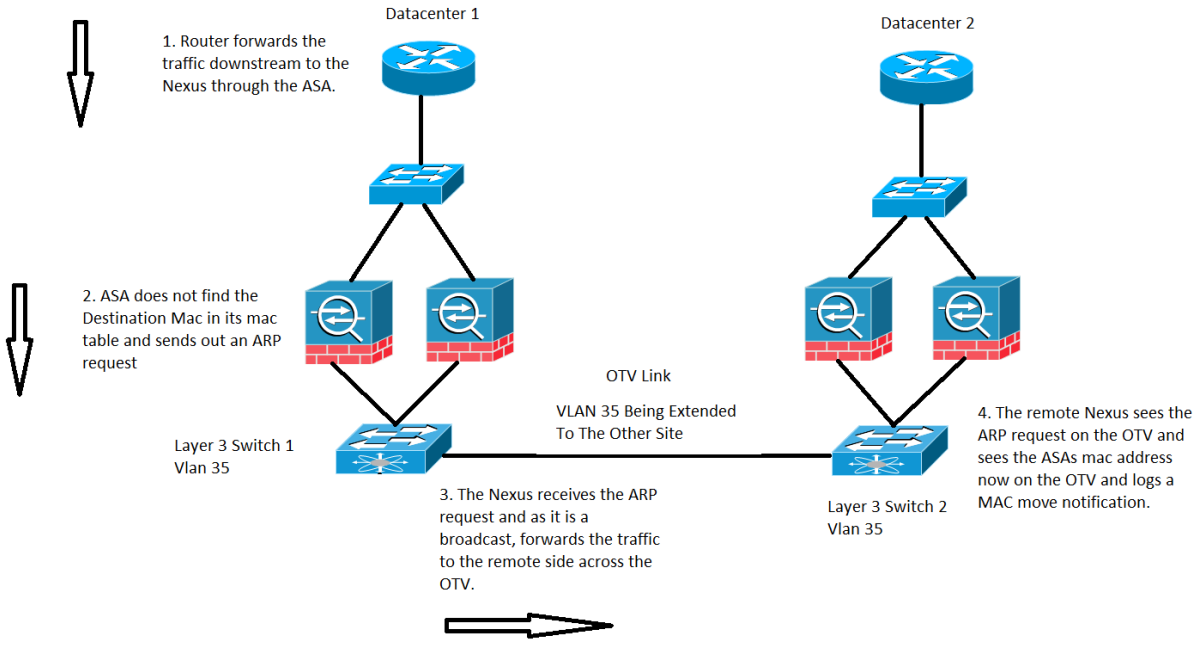
Distribuzione di cluster tra siti in cui le ASA sono configurate in modalità trasparente con bridging delle VLAN 1535 e 35. La VLAN interna 35 viene estesa su Overlay Transport Virtualization (OTV), mentre la VLAN esterna 1535 non viene estesa su OTV, come mostrato nell'immagine



Notifiche di spostamento MAC sullo switch

Scenario 1

Il traffico è destinato a un indirizzo MAC la cui voce non è presente sulla tabella MAC dell'ASA, come mostrato nell'immagine:



In un'ASA trasparente, se l'indirizzo MAC di destinazione del pacchetto in arrivo sull'ASA non è

presente nella tabella degli indirizzi MAC, invia una richiesta ARP (Address Resolution Protocol) per la destinazione (se si trova nella stessa subnet di BVI) o una richiesta ICMP (Internet Control Message Protocol) con Time To Live 1(TTL 1) e un indirizzo MAC di origine come indirizzo MAC BVI (Bridge Virtual Interface) e un indirizzo MAC di destinazione come DMAC (Destination Media Access Controller) non sono presenti.

Nel caso precedente, il flusso del traffico è il seguente:

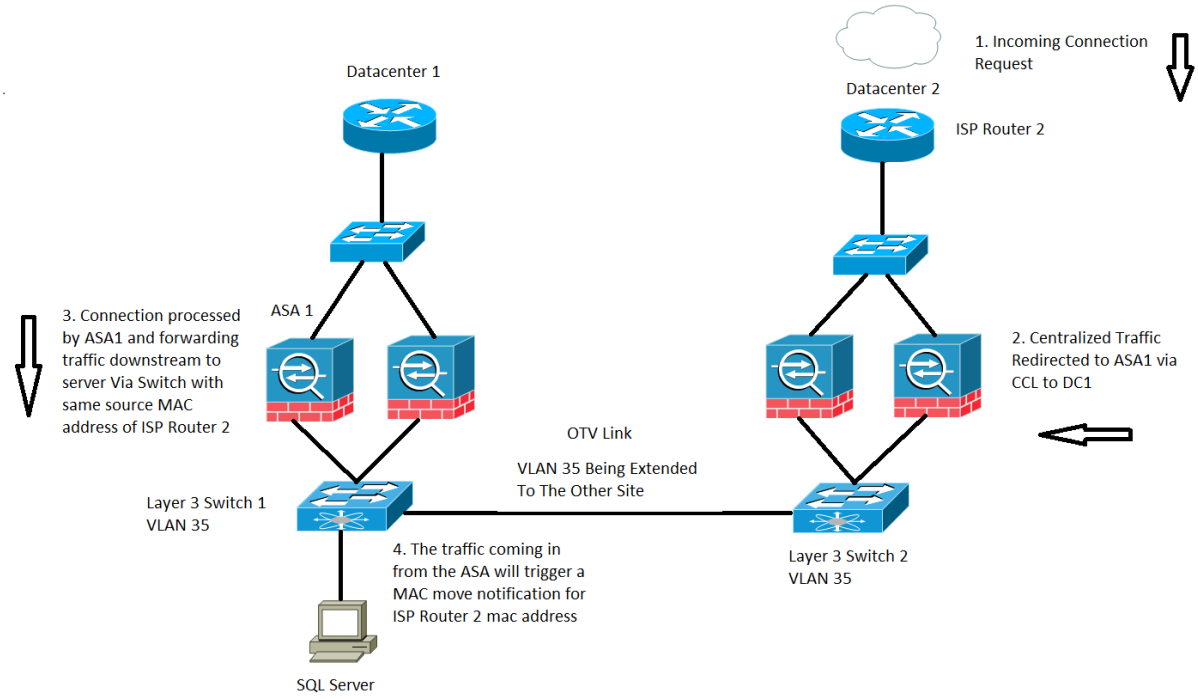
1. Il router ISP sul datacenter 1 inoltra il traffico a una destinazione specifica dietro l'ASA.
2. Il traffico può essere ricevuto da una delle appliance ASA e, in questo caso, l'indirizzo MAC di destinazione del traffico non è noto all'appliance ASA.
3. Ora l'IP di destinazione del traffico si trova nella stessa subnet della BVI e, come accennato in precedenza, l'ASA genera una richiesta ARP per l'IP di destinazione.
4. Lo switch 1 riceve il traffico e, poiché la richiesta è una trasmissione, inoltra il traffico al centro dati 2 e attraverso il collegamento OTV.
5. Quando lo switch 2 vede la richiesta ARP proveniente dall'ASA sul collegamento OTV, registra una notifica MAC MOVE perché in precedenza l'indirizzo MAC dell'ASA era stato appreso tramite l'interfaccia direttamente connessa e ora è stato appreso tramite il collegamento OTV.

Raccomandazioni

Si tratta di uno scenario ad angolo. Le tabelle MAC sono sincronizzate in cluster, pertanto è meno probabile che un membro non disponga di una voce per un host specifico. È ritenuto accettabile uno spostamento occasionale dell'indirizzo MAC BVI di proprietà del cluster.

Scenario 2

Elaborazione di flusso centralizzata da parte dell'ASA, come mostrato nell'immagine:



Il traffico basato sulle ispezioni su un cluster ASA è classificato in tre tipi:

- Centralizzato
- Distribuito
- Semidistribuito

In caso di ispezione centralizzata, il traffico che deve essere ispezionato viene reindirizzato all'unità master del cluster ASA. Se il traffico viene ricevuto da un'unità slave del cluster ASA, viene inoltrato al dispositivo master tramite la CCL.

Nell'immagine precedente viene utilizzato il traffico SQL CIP (Centralized Inspection Protocol) e il comportamento qui descritto è applicabile a qualsiasi CIP.

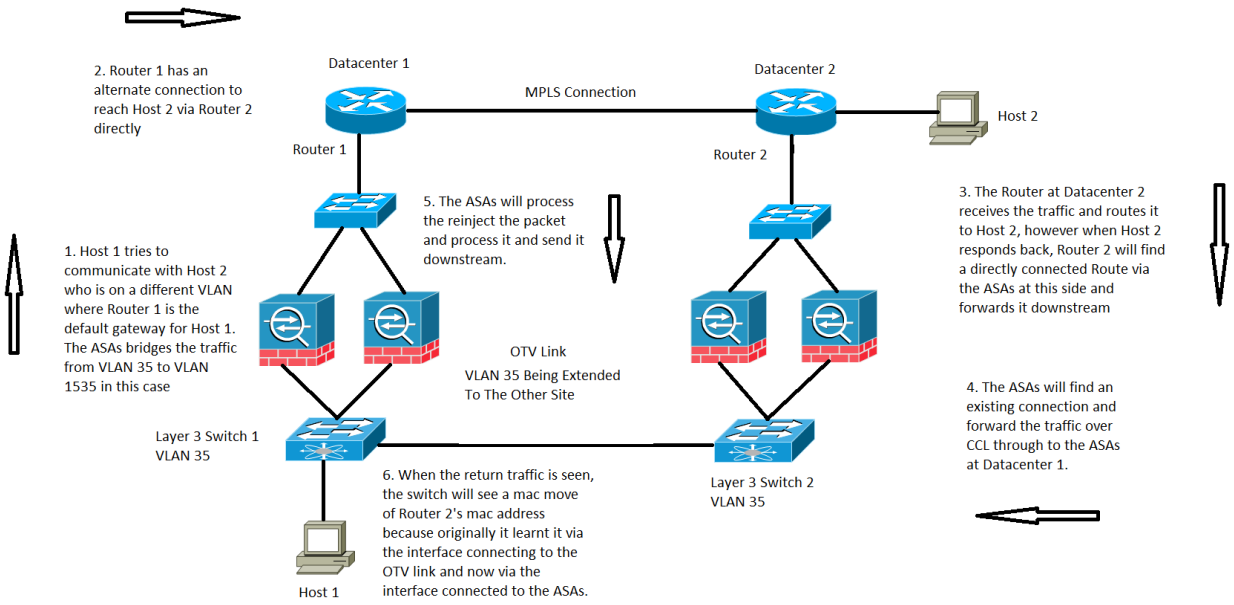
Si riceve il traffico sul datacenter 2 in cui si hanno solo unità slave del cluster ASA, l'unità master si trova nel datacenter 1, che è ASA 1.

1. Il router 2 ISP sul data center 2 riceve il traffico e lo inoltra a valle alle appliance ASA sul sito.
2. Ciascuna appliance ASA può ricevere questo traffico e, quando determina che deve essere ispezionato, il protocollo viene centralizzato e inoltra il traffico all'unità master tramite la CCL.
3. ASA 1 riceve il flusso del traffico tramite la CCL, lo elabora e lo invia a valle a SQL Server.
4. Ora, quando ASA 1 inoltra il traffico a valle, conserva l'indirizzo mac di origine originale del router 2 dell'ISP, che si trova al centro dati 2, e lo invia a valle.
5. Quando lo switch 1 riceve questo traffico specifico, esegue il log in una notifica MAC MOVE in quanto, in origine, vede l'indirizzo MAC del router 2 ISP tramite il collegamento OTV collegato al datacenter 2 e, ora, vede il traffico in entrata dalle interfacce connesse all'ASA 1.

Raccomandazioni

Si consiglia di instradare le connessioni centralizzate al sito che ospita il sito principale (in base alle priorità), come mostrato nell'immagine:

Scenario 3

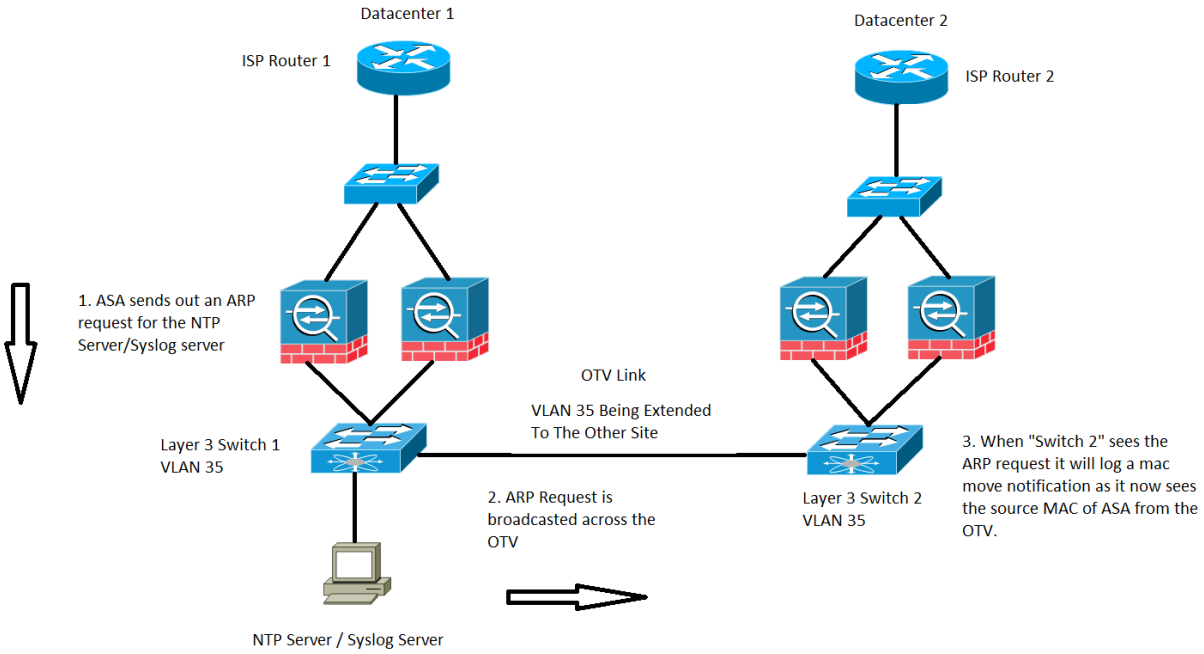


Nelle comunicazioni tra controller di dominio in modalità trasparente, il flusso di traffico specifico non è coperto o documentato, ma funziona dal punto di vista dell'elaborazione del flusso ASA. Tuttavia, può generare notifiche di spostamento MAC sullo switch.

1. L'host 1 sulla VLAN 35 cerca di comunicare con l'host 2 presente sull'altro data center.
2. L'host 1 ha un gateway predefinito, il router 1, e il router 1 ha un percorso che permette di raggiungere l'host 2 potendo comunicare con il router 2 direttamente attraverso un collegamento alternativo. In questo caso si presume che il protocollo Multiprotocol Label Switching (MPLS) sia connesso non tramite il cluster ASA.
3. Il router 2 riceve il traffico in entrata e lo instrada sull'host 2.
4. Ora, quando l'host 2 risponde, il router 2 riceve il traffico di ritorno e trova una route connessa direttamente tramite le appliance ASA anziché il traffico che invia tramite il protocollo MPLS.
5. In questa fase, il traffico che esce dal router 2 ha l'indirizzo MAC di origine dell'interfaccia di uscita del router 2.
6. Le appliance ASA del data center 2 ricevono il traffico di ritorno e trovano una connessione che esiste e che viene stabilita dalle appliance ASA del data center 1.
7. Le appliance ASA nel data center 2 inviano il traffico di ritorno sulla CCL alle appliance ASA nel data center 1.
8. In questa fase, le ASA del data center 1 elaborano il traffico di ritorno e lo inviano verso lo switch 1. Il pacchetto ha ancora lo stesso MAC di origine dell'interfaccia di uscita del router 2.
9. Ora, quando lo switch 1 riceve il pacchetto, registra una notifica di spostamento dell'indirizzo MAC perché inizialmente ha appreso l'indirizzo MAC del router 2 sull'interfaccia connessa al collegamento OTV, ma in questa fase inizia ad apprendere l'indirizzo MAC dall'interfaccia connessa alle appliance ASA.

Scenario 4

Il traffico generato dall'ASA, come mostrato nell'immagine:

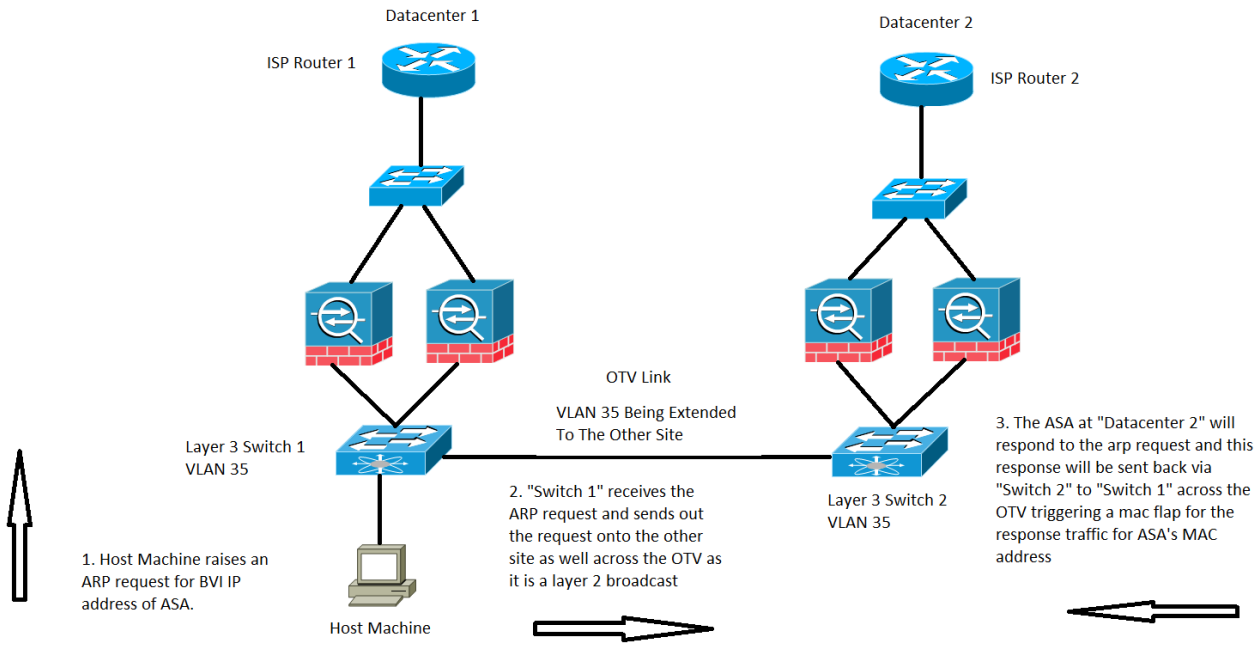


Questo caso specifico verrà osservato per tutto il traffico generato dall'ASA stessa. Qui vengono prese in considerazione due situazioni possibili, in cui l'ASA cerca di raggiungere un Network Time Protocol (NTP) o un server Syslog, che si trovano sulla stessa subnet dell'interfaccia BVI.Tuttavia, non si limita a queste due condizioni, questa situazione può verificarsi ogni volta che l'ASA genera traffico per un indirizzo IP connesso direttamente agli indirizzi IP BVI.

1. Se l'ASA non ha le informazioni ARP del server NTP o del server Syslog, genererà una richiesta ARP per quel server.
2. Poiché la richiesta ARP è un pacchetto broadcast, lo switch 1 riceve il pacchetto dall'interfaccia connessa dell'ASA e lo invia a tutte le interfacce della VLAN specifica, compreso il sito remoto sull'OTV.
3. Lo switch di sito remoto 2 riceve questa richiesta ARP dal collegamento OTV e, a causa dell'indirizzo MAC di origine dell'ASA, genera una notifica di link flap MAC, in quanto lo stesso indirizzo MAC viene appreso nell'OTV tramite le interfacce locali direttamente connesse all'ASA.

Scenario 5

Il traffico destinato all'indirizzo IP BVI dell'appliance ASA da un host collegato direttamente, come mostrato nell'immagine:



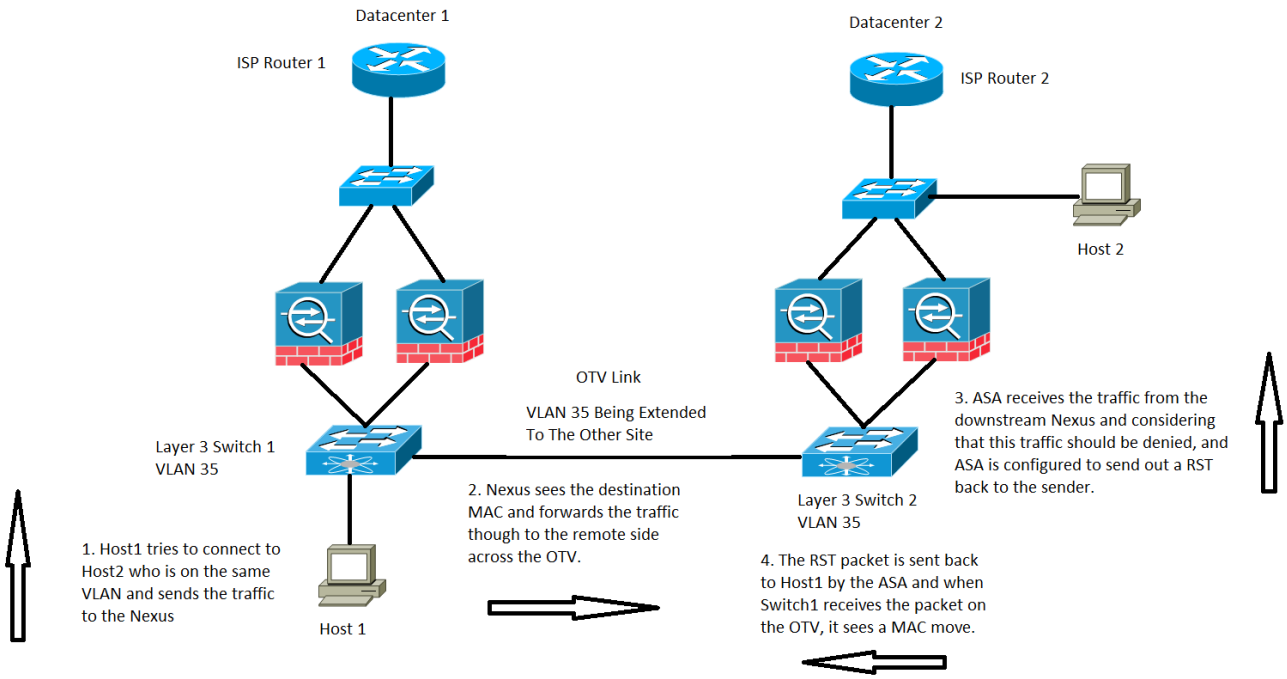
Lo spostamento del MAC può essere osservato anche nei momenti in cui il traffico è destinato all'indirizzo IP BVI dell'ASA.

Nello scenario, un computer host si trova su una rete dell'appliance ASA connessa direttamente e sta tentando di connettersi all'appliance.

1. L'host non dispone dell'ARP dell'ASA e attiva una richiesta ARP.
2. Il Nexus riceve il traffico e, di nuovo, poiché si tratta di traffico broadcast, invia il traffico attraverso l'OTV anche all'altro sito.
3. L'ASA sul datacenter remoto 2 può rispondere alla richiesta ARP e inviare il traffico indietro attraverso lo stesso percorso, ossia lo switch 2 sul lato remoto, OTV, lo switch 1 sul lato locale e quindi l'host finale.
4. Quando la risposta ARP viene rilevata sullo switch 1 lato locale, attiva una notifica di spostamento MAC quando rileva l'indirizzo MAC dell'appliance ASA che arriva dal collegamento OTV.

Scenario 6

L'appliance ASA è impostata in modo da bloccare il traffico e inviare un messaggio RST all'host, come mostrato nell'immagine:



In questo caso, si dispone di un host 1 sulla VLAN 35 e cerca di comunicare con l'host 2 sulla stessa VLAN di layer 3, ma l'host 2 si trova in realtà sulla VLAN 1535 del datacenter 2.

1. L'indirizzo MAC dell'host 2 viene visualizzato sullo switch 2 tramite l'interfaccia collegata alle appliance ASA.
2. Lo switch 1 vedrebbe l'indirizzo MAC dell'host 2 tramite il collegamento OTV.
3. L'host 1 invia il traffico all'host 2 e questo segue il percorso dello switch 1, OTV, switch 2 e ASA al datacenter 2.
4. Questa condizione specifica viene negata dall'ASA e, poiché l'ASA è configurata per inviare un RST all'host 1, il pacchetto RST restituisce l'indirizzo MAC di origine dell'ASA.
5. Quando il pacchetto torna allo switch 1 su OTV, lo switch 1 registra una notifica MAC MOVE per l'indirizzo MAC dell'ASA perché ora vede l'indirizzo MAC su OTV, quindi prima di vedere l'indirizzo dall'interfaccia direttamente connessa.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Guida alla configurazione della CLI per Cisco ASA Series
- Documentazione e supporto tecnico – Cisco Systems