Häufige Probleme mit dem transparenten ASA-Inter-Site-Cluster

Inhalt

Einführung

In diesem Dokument werden einige häufige Probleme mit dem STP (Spanned EtherChannel Transparent Mode Inter-Site Cluster) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Adaptive Security Appliance (ASA)-Firewall
- ASA-Clustering

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Ab ASA Version 9.2 wird standortübergreifendes Clustering unterstützt, bei dem sich die ASA-Einheiten in verschiedenen Rechenzentren befinden können und der Cluster Control Link (CCL) über eine Data Center Interconnect (DCI) verbunden ist. Mögliche Bereitstellungsszenarien sind:

- Individuelle Schnittstelle Inter-Site-Cluster
- Spanned EtherChannel Transparent Mode Inter-Site-Cluster
- Spanned EtherChannel Routed Mode Inter-Site-Cluster (unterstützt ab 9.5)

MAC MOVE-Benachrichtigungen

Wenn eine MAC-Adresse in der Tabelle Content Addressable Memory (CAM) den Port wechselt, wird eine MAC MOVE-Benachrichtigung generiert. Eine MAC-MOVE-Benachrichtigung wird jedoch nicht generiert, wenn eine MAC-Adresse zur CAM-Tabelle hinzugefügt oder daraus entfernt wird. Wenn eine MAC-Adresse X über die Schnittstelle GigabitEthernet0/1 in VLAN10 erfasst wird und nach einiger Zeit dieselbe MAC-Adresse über GigabitEthernet0/2 in VLAN 10 angezeigt wird, wird eine MAC MOVE-Benachrichtigung generiert.

Syslog vom Switch:

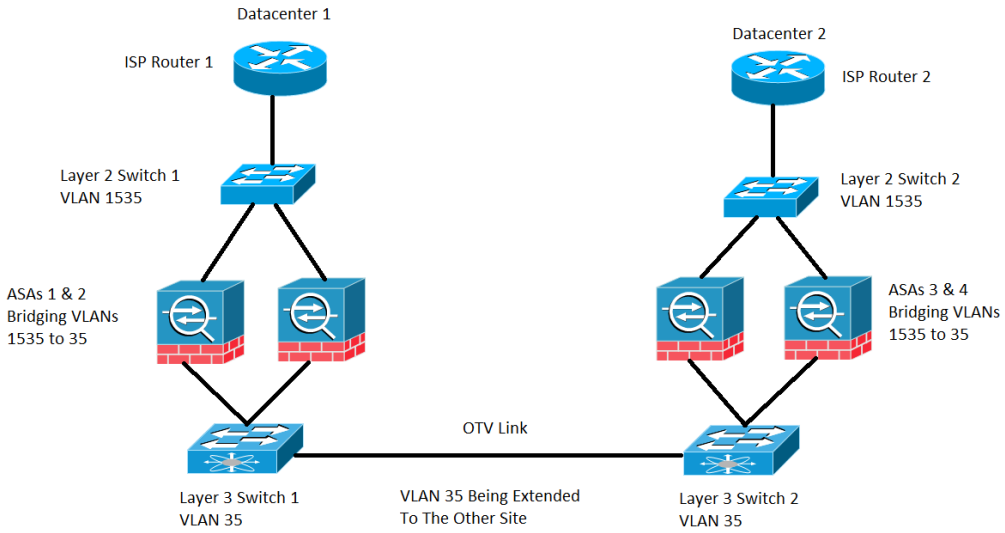
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1
to GigabitEthernet0/2
```

Syslog von ASA:

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

Netzwerkdiagramm

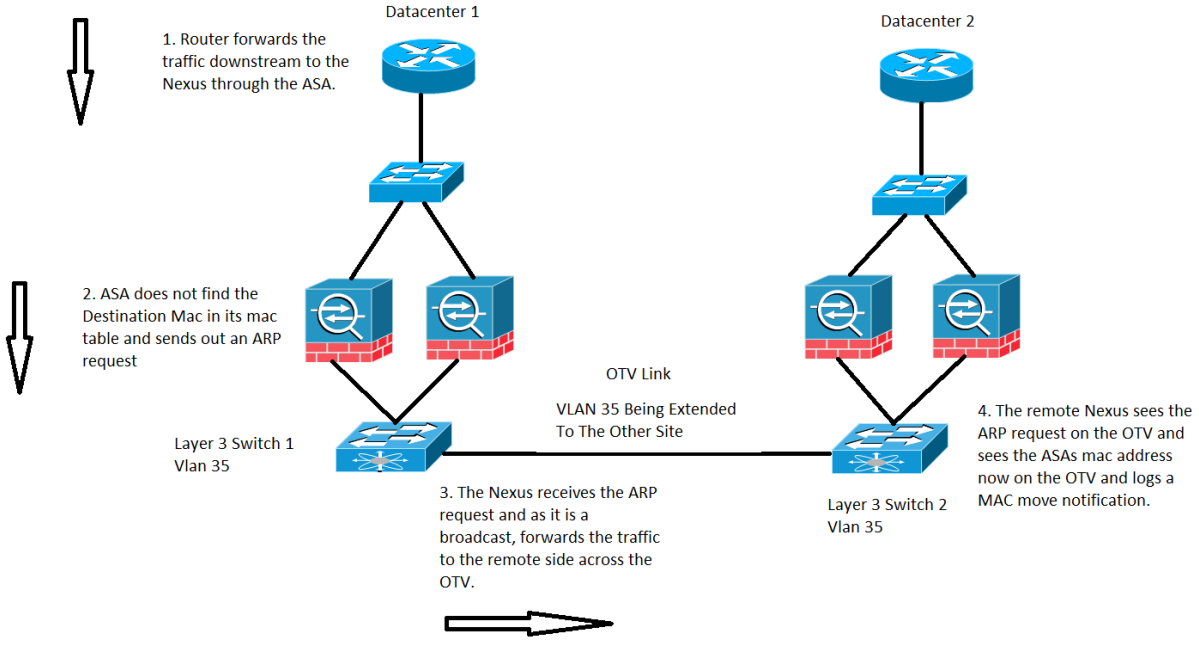
Standortübergreifende Cluster-Bereitstellung, bei der die ASAs im transparenten Modus als Bridging für VLAN 1535 und VLAN 35 konfiguriert werden. Das interne VLAN 35 wird über die Overlay Transport Virtualization (OTV) erweitert, während das externe VLAN 1535 nicht über das OTV erweitert wird, wie im Bild gezeigt.



MAC-Verschiebungsbenachrichtigungen auf dem Switch

Szenario 1

Datenverkehr, der an eine MAC-Adresse gerichtet ist, deren Eintrag nicht in der ASA-MAC-Tabelle vorhanden ist, wie im Bild gezeigt:



Wenn sich die MAC-Zieladresse des auf der ASA ankommenden Pakets in einer transparenten

ASA nicht in der MAC-Adresstabelle befindet, sendet sie eine ARP-Anfrage (Address Resolution Protocol) für dieses Ziel (wenn es sich im gleichen Subnetz wie BVI befindet) oder eine ICMP-Anfrage mit Time To Live 1(TTL 1) mit Quell-MAC als Bridge Virtual Interface. (BVI) MAC-Adresse und Ziel-MAC-Adresse als Ziel Media Access Controller (DMAC) wird übersehen.

Im vorherigen Fall gibt es folgende Datenverkehrsströme:

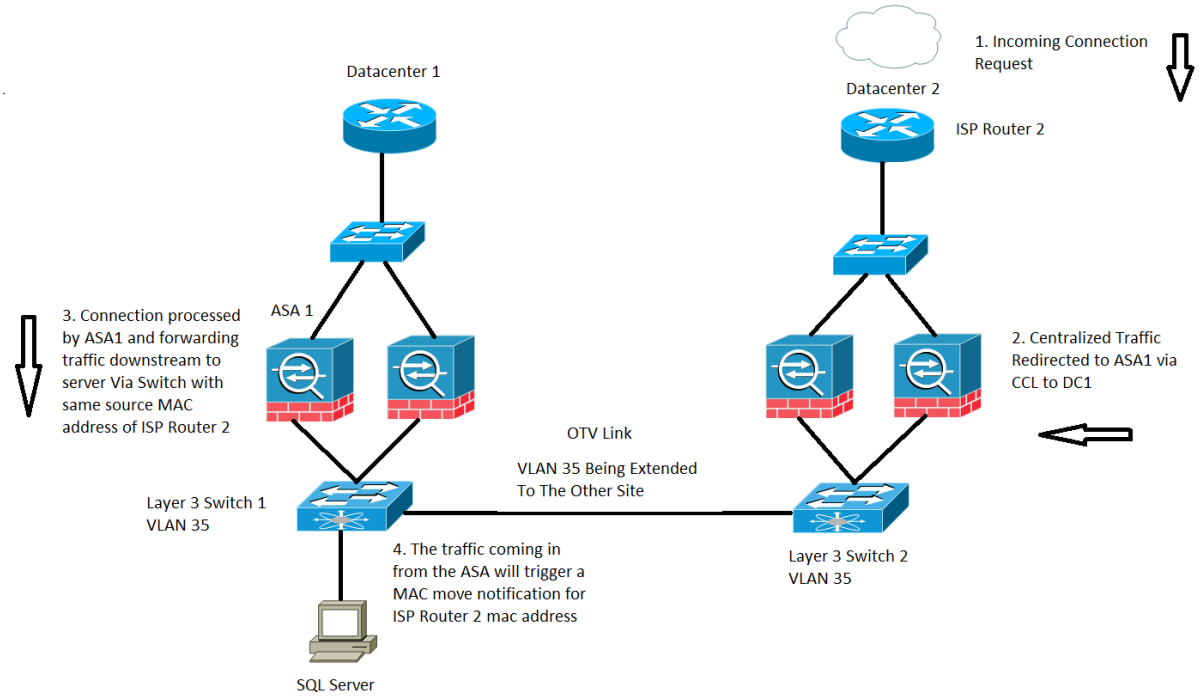
1. Der ISP-Router im Rechenzentrum 1 leitet Datenverkehr an ein bestimmtes Ziel weiter, das sich hinter der ASA befindet.
2. Jede der ASAs kann den Datenverkehr empfangen, und in diesem Fall ist die MAC-Zieladresse des Datenverkehrs von der ASA nicht bekannt.
3. Nun befindet sich die Ziel-IP des Datenverkehrs im gleichen Subnetz wie die BVI. Wie bereits erwähnt, generiert ASA jetzt eine ARP-Anfrage für die Ziel-IP.
4. Der Switch 1 empfängt den Datenverkehr, und da es sich bei der Anfrage um eine Broadcast-Anfrage handelt, leitet er den Datenverkehr an Rechenzentrum 2 sowie über die OTV-Verbindung weiter.
5. Wenn Switch 2 die ARP-Anfrage von der ASA auf der OTV-Verbindung sieht, protokolliert er eine MAC MOVE-Benachrichtigung, da zuvor die MAC-Adresse der ASA über eine direkt verbundene Schnittstelle abgerufen wurde und nun über die OTV-Verbindung abgerufen wird.

Empfehlungen

Es ist ein Eckszenario. MAC-Tabellen werden in Clustern synchronisiert, sodass es für ein Mitglied weniger wahrscheinlich ist, dass es keinen Eintrag für einen bestimmten Host gibt. Ein gelegentlicher MAC-Move für eine clustereigene BVI MAC-Adresse gilt als akzeptabel.

Szenario 2

Zentralisierte Flow-Verarbeitung durch ASA, wie im Bild gezeigt:



Der für die Inspektion erforderliche Datenverkehr innerhalb eines ASA-Clusters wird in drei Arten klassifiziert:

- Zentralisiert
- Verteilt
- Teilweise verteilt

Bei einer zentralen Überprüfung wird der Datenverkehr, der überprüft werden muss, an die Master-Einheit des ASA-Clusters umgeleitet. Wenn eine Slave-Einheit des ASA-Clusters den Datenverkehr empfängt, wird er über CCL an den Master weitergeleitet.

Im vorherigen Bild arbeiten Sie mit SQL-Datenverkehr, der ein zentrales Prüfprotokoll (CIP) ist, und das hier beschriebene Verhalten gilt für jeden CIP.

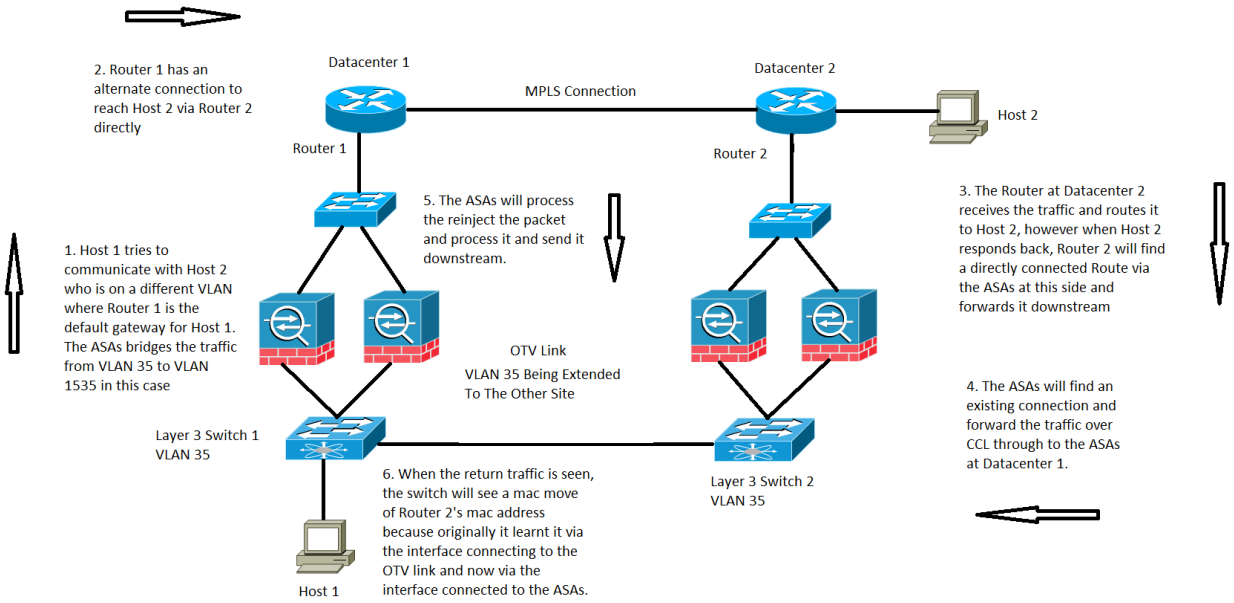
Sie erhalten den Datenverkehr im Rechenzentrum 2, wenn Sie nur Slave-Einheiten des ASA-Clusters haben. Die Master-Einheit befindet sich im Rechenzentrum 1, das ASA 1 ist.

1. ISP Router 2 im Rechenzentrum 2 empfängt den Datenverkehr und leitet ihn Downstream an die ASAs am Standort weiter.
2. Jeder der ASA-Geräte kann diesen Datenverkehr empfangen, sobald er feststellt, dass dieser Datenverkehr überprüft werden muss. Sobald das Protokoll zentralisiert ist, leitet es den Datenverkehr über die CCL an die Master-Einheit weiter.
3. ASA 1 empfängt den Datenverkehrsfluss über CCL, verarbeitet den Datenverkehr und sendet ihn Downstream an SQL Server.
4. Wenn ASA 1 den Datenverkehr Downstream weiterleitet, behält sie die ursprüngliche Quell-MAC-Adresse des ISP-Routers 2 bei, der sich in Rechenzentrum 2 befindet, und sendet sie Downstream.
5. Wenn Switch 1 diesen spezifischen Datenverkehr empfängt, meldet er eine MAC MOVE-Benachrichtigung an, da er die MAC-Adresse des ISP-Routers 2 ursprünglich über die OTV-Verbindung sieht, die mit Rechenzentrum 2 verbunden ist. Nun erkennt er den Datenverkehr, der von den mit der ASA 1 verbundenen Schnittstellen eingeht.

Empfehlungen

Es wird empfohlen, zentralisierte Verbindungen zu dem Standort zu routen, der den Master hostet (basierend auf Prioritäten), wie im Bild gezeigt:

Szenario 3



Für eine Kommunikation zwischen Domänen-Controllern (DC) im transparenten Modus ist dieser spezifische Datenverkehrsfluss nicht abgedeckt oder dokumentiert, aber dieser spezifische Datenverkehrsfluss funktioniert vom Standpunkt der ASA-Datenflussverarbeitung aus. Dies kann jedoch dazu führen, dass MAC-Verschiebungsbenachrichtigungen auf dem Switch gesendet werden.

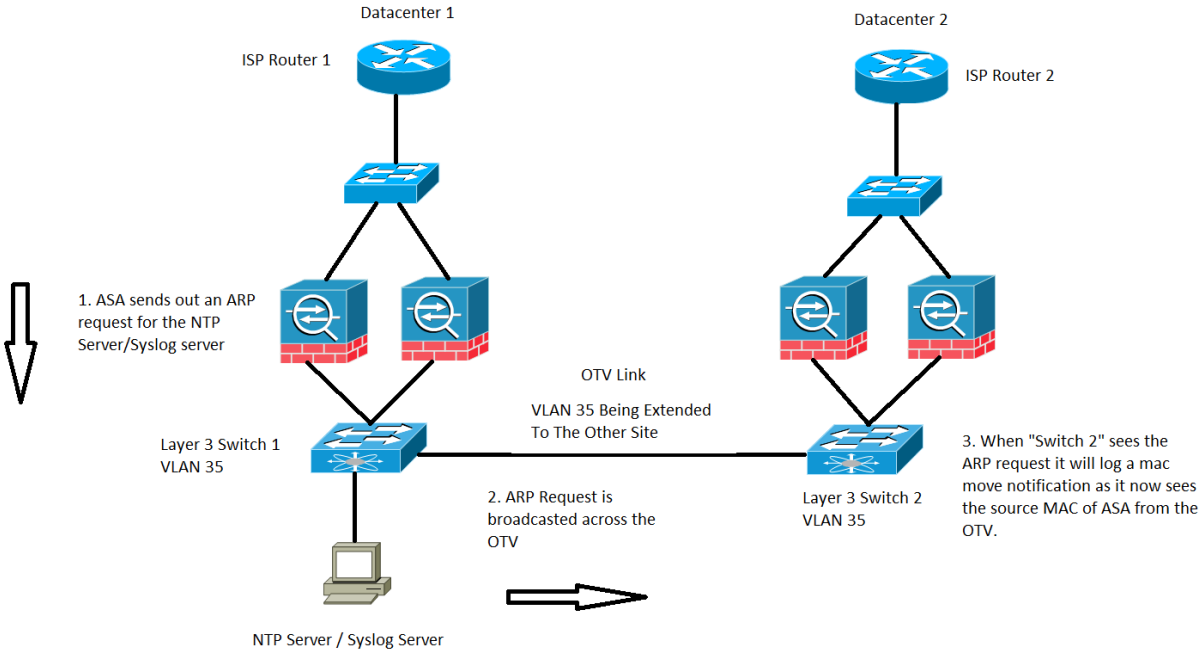
1. Der Host 1 auf VLAN 35 versucht, mit Host 2 zu kommunizieren, der sich im anderen Rechenzentrum befindet.
2. Host 1 verfügt über ein Standard-Gateway, d. h. Router 1 und Router 1 haben einen Pfad, um Host 2 zu erreichen, indem sie direkt über eine alternative Verbindung mit Router 2 kommunizieren können. In diesem Fall gehen wir von Multiprotocol Label Switching (MPLS) aus und nicht über das ASA-Cluster.
3. Router 2 empfängt den eingehenden Datenverkehr und leitet ihn an Host 2 weiter.
4. Wenn Host 2 jetzt zurückantwortet, empfängt Router 2 den Rückverkehr und findet eine direkt verbundene Route über die ASAs statt des Datenverkehrs, den er über das MPLS sendet.
5. In dieser Phase hat der Datenverkehr, der Router 2 verlässt, die Quell-MAC der Ausgangsschnittstelle von Router 2.
6. Die ASAs im Rechenzentrum 2 empfangen den Rückverkehr und finden eine Verbindung, die von den ASAs im Rechenzentrum 1 besteht und hergestellt wird.
7. Die ASAs in Rechenzentrum 2 senden den Rückverkehr über CCL zurück an die ASAs in Rechenzentrum 1.
8. In dieser Phase verarbeiten die ASAs in Rechenzentrum 1 den Rückverkehr und senden ihn an Switch 1. Das Paket verfügt weiterhin über die gleiche Quell-MAC wie die Exit-

Schnittstelle von Router 2.

9. Wenn Switch 1 das Paket empfängt, protokolliert er jetzt eine MAC-Bewegungs-Benachrichtigung, da zunächst die MAC-Adresse von Router 2 über die Schnittstelle abgerufen wurde, die mit der OTV-Verbindung verbunden ist. Zu diesem Zeitpunkt beginnt er jedoch, die MAC-Adresse von der Schnittstelle zu erfassen, die mit den ASAs verbunden ist.

Szenario 4

Von der ASA generierter Datenverkehr, wie im Bild gezeigt:

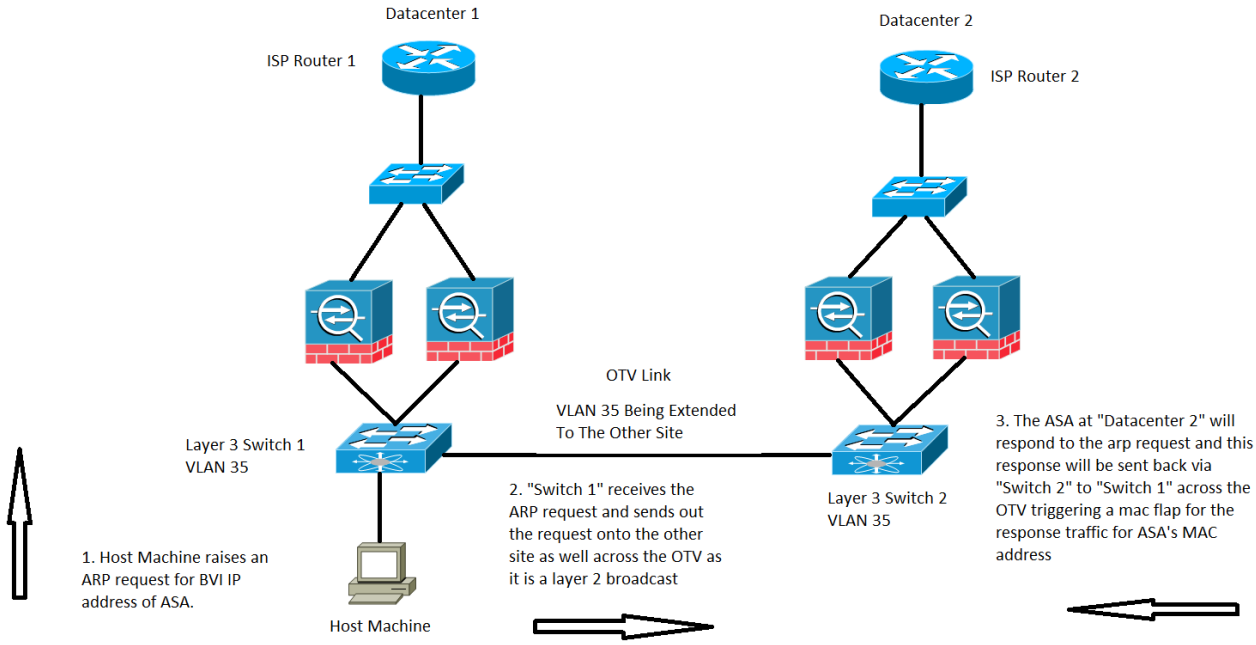


Dieser spezielle Fall wird bei jedem Datenverkehr beobachtet, der von der ASA selbst generiert wird. Hier werden zwei mögliche Situationen berücksichtigt, in denen die ASA entweder versucht, ein Network Time Protocol (NTP) oder einen Syslog-Server zu erreichen, die sich im gleichen Subnetz wie die BVI-Schnittstelle befinden. Diese Situation ist jedoch nicht nur auf diese beiden Bedingungen beschränkt, sondern kann immer dann auftreten, wenn der Datenverkehr von der ASA für eine IP-Adresse generiert wird, die direkt mit den BVI-IP-Adressen verbunden ist.

1. Wenn ASA nicht über die ARP-Informationen des NTP-Servers/Syslog-Servers verfügt, generiert die ASA eine ARP-Anfrage für diesen Server.
2. Da es sich bei der ARP-Anfrage um ein Broadcast-Paket handelt, empfängt der Switch 1 dieses Paket von der angeschlossenen ASA-Schnittstelle und überflutet es über alle Schnittstellen im spezifischen VLAN, einschließlich des Remote-Standorts über das OTV.
3. Der Remote-Standort-Switch 2 erhält diese ARP-Anfrage von der OTV-Verbindung. Aufgrund der Quell-MAC-Adresse der ASA wird eine MAC-Flapping-Benachrichtigung generiert, da dieselbe MAC-Adresse über die lokalen, direkt mit der ASA verbundenen Schnittstellen im OTV erfasst wird.

Szenario 5

Datenverkehr, der an die BVI-IP-Adresse der ASA von einem direkt verbundenen Host gerichtet ist, wie im Bild gezeigt:



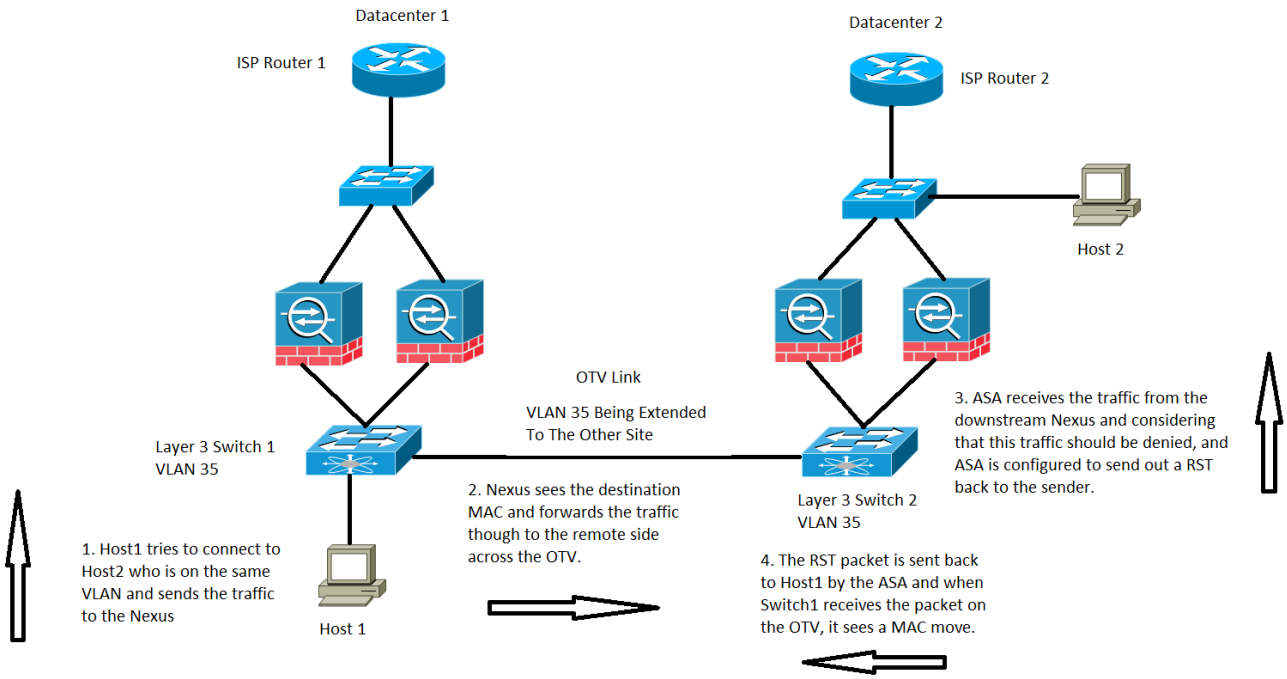
Eine MAC MOVE kann auch zu Zeiten beobachtet werden, in denen der Datenverkehr an die BVI-IP-Adresse der ASA gerichtet ist.

In diesem Szenario befindet sich ein Host-Rechner in einem direkt verbundenen Netzwerk der ASA und versucht, eine Verbindung mit der ASA herzustellen.

1. Der Host verfügt nicht über den ARP der ASA und löst eine ARP-Anforderung aus.
2. Der Nexus empfängt den Datenverkehr. Da es sich wiederum um einen Broadcast-Datenverkehr handelt, sendet er den Datenverkehr über das OTV an den anderen Standort.
3. Die ASA im Remote-Rechenzentrum 2 kann auf die ARP-Anfrage reagieren und den Datenverkehr über denselben Pfad zurücksenden, der Switch 2 auf der Remote-Seite, OTV, Switch 1 auf der lokalen Seite und dann der End-Host ist.
4. Wenn die ARP-Antwort auf dem lokalen Switch 1 angezeigt wird, löst sie eine MAC-Bewegungs-Benachrichtigung aus, da sie die MAC-Adresse der ASA erkennt, die von der OTV-Verbindung empfangen wird.

Szenario 6

ASA wird so eingestellt, dass Datenverkehr, mit dem ein RST an den Host gesendet wird, verweigert wird, wie im Bild gezeigt:



In diesem Fall haben wir einen Host-Host 1 im VLAN 35, der versucht, mit Host 2 im gleichen Layer-3-VLAN zu kommunizieren, Host 2 befindet sich jedoch tatsächlich im Rechenzentrum-2-VLAN 1535.

1. Host-2MAC-Adresse wird auf Switch 2 über die mit den ASAs verbundene Schnittstelle angezeigt.
2. Switch 1 würde die MAC-Adresse von Host 2 über den OTV-Link sehen.
3. Host 1 sendet Datenverkehr an Host 2 und folgt dem Pfad von Switch 1, OTV, Switch 2, ASAs im Rechenzentrum 2.
4. Diese spezielle wird von der ASA abgelehnt, und da ASA so konfiguriert ist, einen RST an Host 1 zurückzusenden, wird das RST-Paket mit der Quell-MAC-Adresse von ASA zurückgesendet.
5. Wenn dieses Paket wieder zu Switch 1 über OTV zurückgeleitet wird, protokolliert Switch 1 eine MAC MOVE-Benachrichtigung für die MAC-Adresse der ASA, da die MAC-Adresse nun über das OTV-Gerät erfasst wird, bevor die Adresse von der direkt verbundenen Schnittstelle erkannt wird.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Konfigurationsleitfaden für die CLI der Cisco ASA-Serie

- Technischer Support und Dokumentation - Cisco Systems