ASA مجموعة مع مشتركة مشاكل الموقع داخل شفافة

المحتويات

المقدمة

يصف هذا وثيقة بعض من المشاكل المشتركة مع ال يجسر EtherChannel أسلوب شفاف بين موقع مجموعة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- جدار حماية أجهزة الأمان المعدلة (ASA)
- مجموعات ASA

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

بدءا من الإصدار ASA 9.2، يتم دعم ميزة التجميع بين المواقع حيث يمكن وضع وحدات ASA في مراكز بيانات مختلفة، كما يتم توصيل إرتباط التحكم في المجموعة (CCL) عبر اتصال بيني لمركز البيانات (DCI). سيناريوهات النشر المحتملة هي:

- مجموعة الواجهات الفردية بين المواقع
- EtherChannel Transparent Mode Inter-Site Cluster
- نظام المجموعة بين المواقع في الوضع الموجه ل EtherChannel الممتدة (مدعوم من الإصدار 9. 5 وما بعده)

إعلامات نقل MAC

عندما يغير عنوان MAC في Content Addressable ذاكرة (CAM) طاولة ميناء، MAC نقل إعلام ولدت. ومع ذلك، لا يتم إنشاء إعلام نقل MAC عند إضافة عنوان MAC أو إزالته من جدول CAM. افترضت إن علمت {upper}mac address X يكون عبر قارن GigabitEthernet0/1 في VLAN10 وبعد بعض الوقت ال نفسه ماك يرى من خلال GigabitEthernet0/2 في VLAN 10، بعد ذلك ماك نقل إعلام ولدت.

Syslog من المحول:

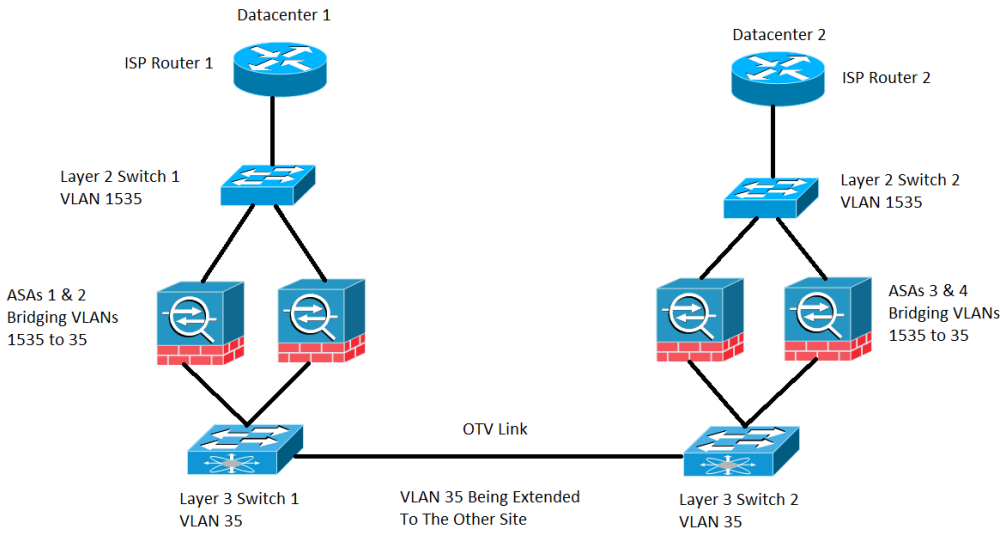
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1
to GigabitEthernet0/2
```

Syslog من ASA

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

الرسم التخطيطي للشبكة

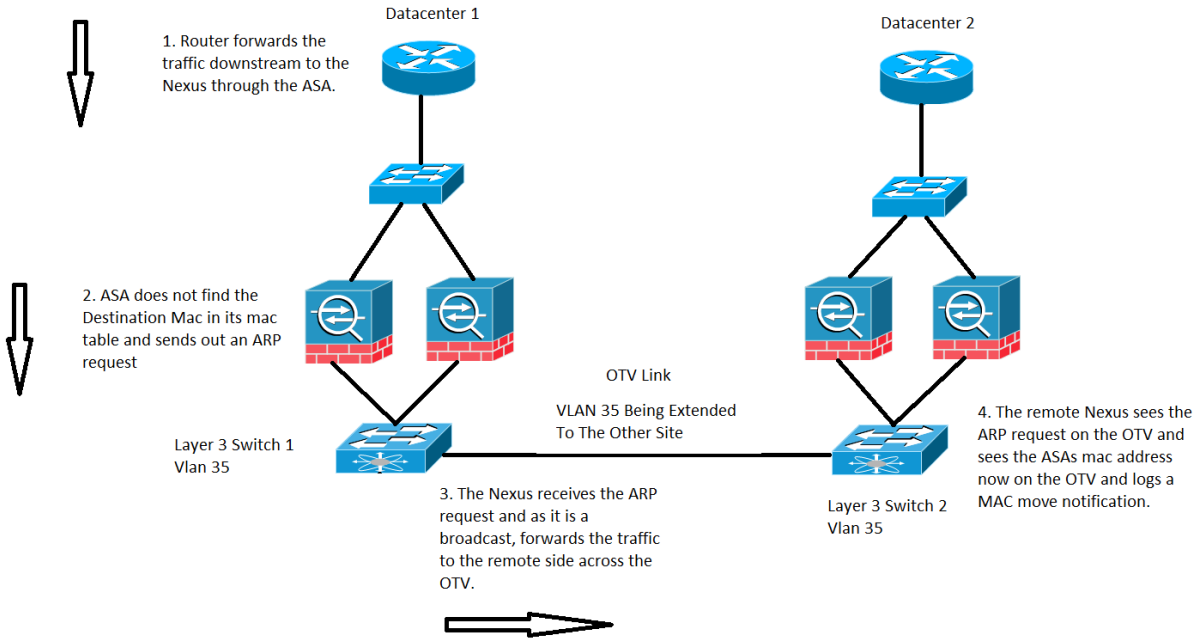
نشر نظام المجموعة بين المواقع حيث يتم تكوين وحدات ASA في الوضع الشفاف الذي يربط بين شبكة VLAN 1535 وشبكة VLAN 35. يتم تمديد شبكة VLAN الداخلية 35 عبر المحاكاة الظاهرية للنقل المتداخل (OTV) بينما لا يتم تمديد شبكة VLAN الخارجية 1535 عبر OTV، كما هو موضح في الصورة



إعلامات نقل MAC على المحول

السيناريو 1

حركة المرور الموجهة إلى عنوان MAC الذي لا يكون إدخاله موجودا على جدول MAC الخاص ب ASA، كما هو موضح في الصورة:



في ASA شفاف، إن الغاية {upper}mac address من الربط قادم على ال ASA ليس في ماك عنوان طاولة، هو يرسل عنوان بروتوكول العنوان (ARP) طلب لتلك الغاية (إن في ال نفسه subnet as BVI) أو إنترنت رسالة بروتوكول (ICMP) طلب مع وقت أن يعيش 1(1 TTL) مع مصدر MAC جسر قارن ظاهري (BVI {upper}mac) عنوان وغاية {upper}mac غاية وحدة تحكم الوصول إلى الوسائط (DMAC) مفقود.

في الحالة السابقة، يكون لديك تدفق حركة المرور هذا:

1. يقوم موجه ISP على مركز البيانات 1 بإعادة توجيه حركة مرور البيانات إلى وجهة محددة تقع خلف ASA.
2. إما من ال asa يستطيع إستلمت الحركة مرور وفي هذه الحالة، الغاية {upper}mac address من الحركة مرور لا يعرف ب ال asa.
3. الآن يكون عنوان IP للوجهة لحركة المرور في الشبكة الفرعية نفسها الخاصة بمعرف فئة المورد (BVI) وكما ذكر سابقا، يقوم ASA الآن بإنشاء طلب ARP للوجهة IP.
4. يستلم المفتاح 1 الحركة مرور وبما أن الطلب هو بث، هو يرسل الحركة مرور إلى DataCenter 2 as well as عبر ال OTV خطوة.
5. عندما يرى المحول 2 طلب ARP من ASA على إرتباط OTV، فإنه يسجل إعلام نقل MAC لأنه قد تم تعلم عنوان MAC الخاص ب ASA سابقا عبر الواجهة المتصلة مباشرة والآن يتم التعرف عليه عبر إرتباط OTV.

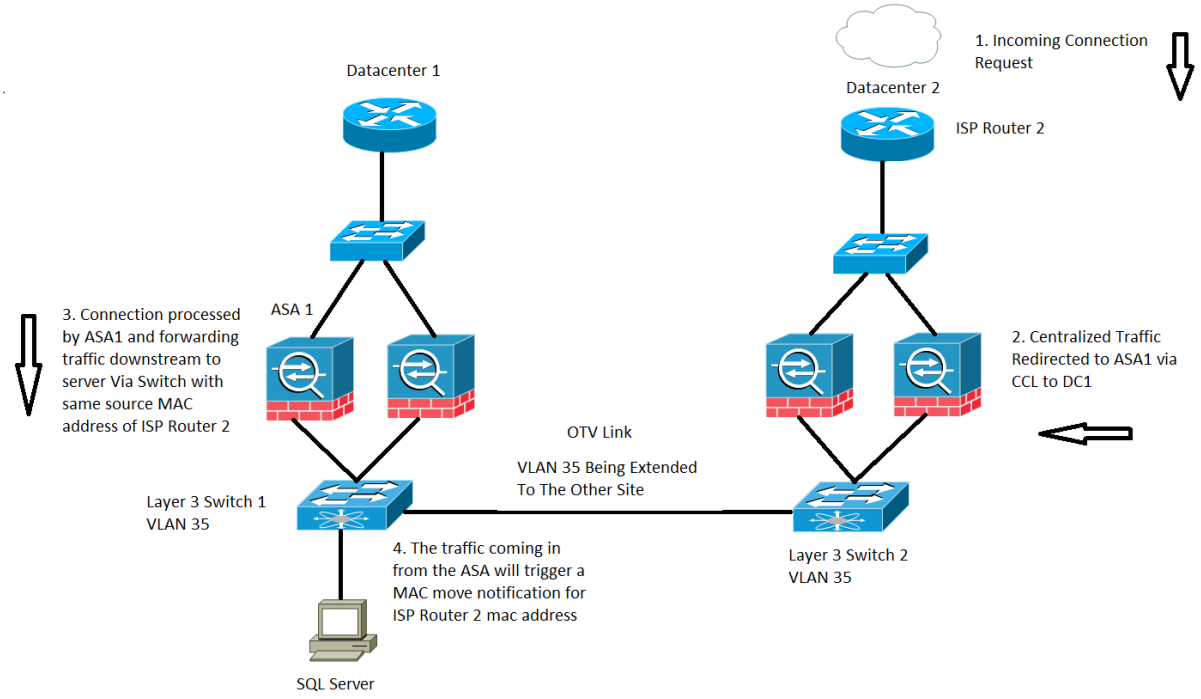
التوصيات

إنه سيناريو متدرج. تتم مزامنة جداول MAC في مجموعات، لذا فمن غير المحتمل أن يكون لعضو ما إدخال لمضيف

معين. ويعتبر نقل MAC من حين إلى آخر من أجل BVI MAC المملوك من قبل نظام المجموعة مقبولا.

السيناريو 2

معالجة التدفق المركزي بواسطة ASA، كما هو موضح في الصورة:



يتم تصنيف حركة المرور المستندة إلى الفحص عبر مجموعة ASA إلى ثلاثة أنواع:

- متمركز
- مُوزعة
- شبه موزع

في حالة التفتيش المركزي، تتم إعادة توجيه أي حركة مرور تحتاج إلى التفتيش إلى الوحدة الرئيسية لمجموعة ASA. إذا تلقت وحدة تابع لمجموعة ASA حركة المرور، فإنها تتم إعادة توجيهها إلى المدير عبر قائمة التحكم في الوصول (CCL).

في الصورة السابقة، يمكنك العمل مع حركة مرور SQL وهي بروتوكول فحص مركزي (CIP) والسلوك الموضح هنا قابل للتطبيق على أي CIP.

تتلقى حركة المرور على مركز البيانات 2 حيث لا يكون لديك سوى وحدات فرعية من نظام المجموعة ASA، حيث تكون الوحدة الرئيسية موجودة في مركز البيانات 1 وهو ASA 1.

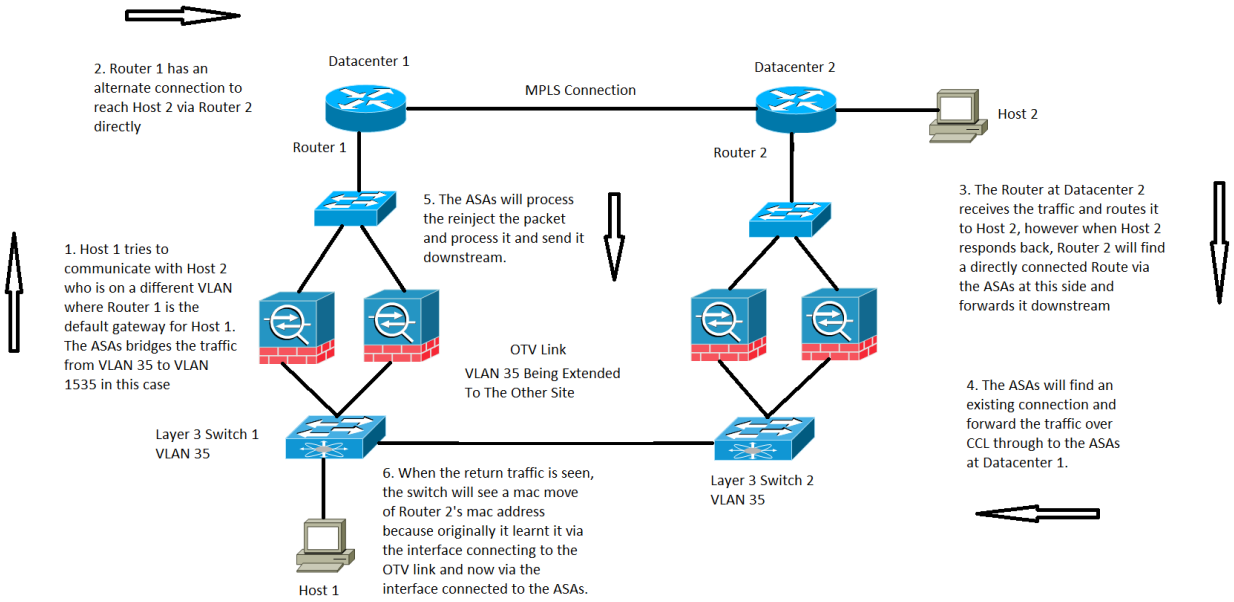
1. يستقبل موجه ISP 2 على مركز البيانات 2 حركة المرور ويعيد توجيهها إلى الخادم إلى وحدات ASA في موقعها.
2. يمكن لأي من ASAs تلقي حركة المرور هذه وبمجرد أن تحدد أن حركة المرور هذه تحتاج إلى فحص ونظرا لأن البروتوكول مركزي، فإنها تقوم بإعادة توجيه حركة المرور إلى الوحدة الرئيسية عبر CCL.
3. يستلم ASA 1 تدفق حركة المرور عبر CCL، وبمعالجة حركة المرور ويرسلها إلى الخادم إلى خادم SQL.
4. الآن عندما يقوم ASA 1 بإعادة توجيه حركة مرور البيانات إلى الخادم، فإنه يحتفظ بعنوان MAC المصدر الأصلي لموجه ISP 2 الموجود في DataCenter 2 ويرسلها إلى الخادم.

5. عندما يستلم المفتاح 1 هذا حركة مرور خاص، هو يسجل في ماك نقل إعلام لأن هو يرى أصلا isp مسحاج تخديد 2 ماك عنوان عن طريق ال OTV خطوة أن يكون ربطت إلى DataCenter 2 وهو الآن يرى الحركة مرور أي يأتي من القارن يربط إلى ال ASA 1.

التوصيات

يوصى بتوجيه الاتصالات المركزية إلى أي موقع يستضيف المدير (استنادا إلى الأولويات)، كما هو موضح في الصورة:

السيناريو 3



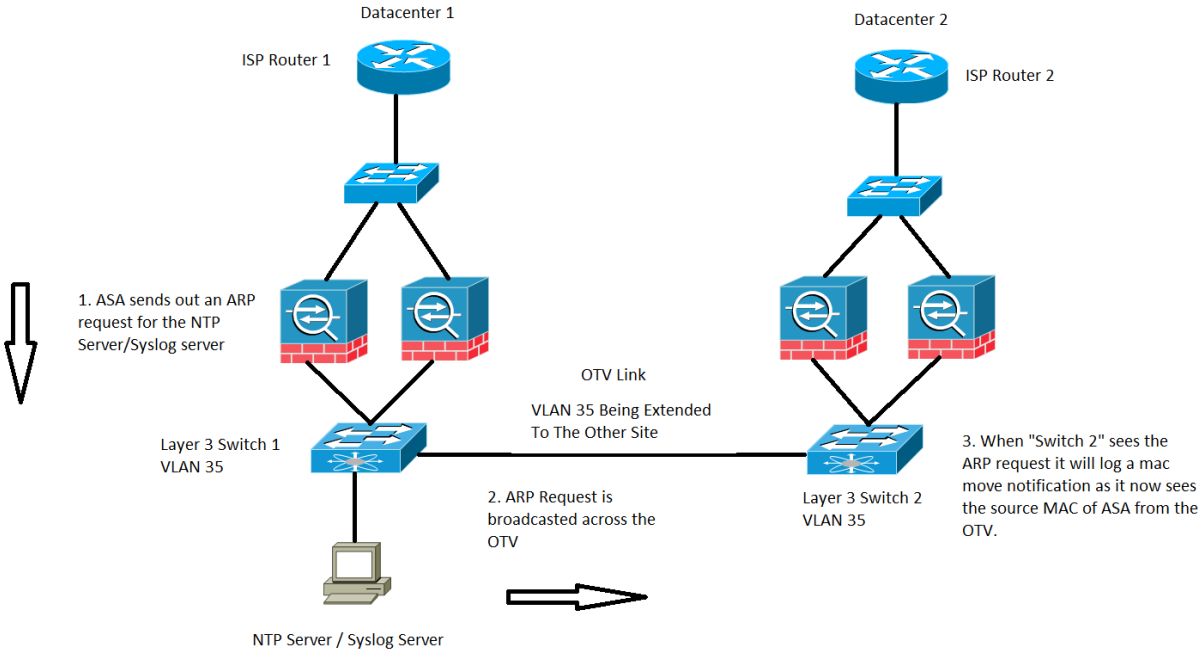
بالنسبة لاتصال وحدة التحكم بين المجالات (DC) في الوضع الشفاف، لا يتم تغطية تدفق حركة المرور المحدد هذا أو توثيقه ولكن تدفق حركة المرور هذا يعمل من وجهة نظر معالجة تدفق ASA. ومع ذلك، قد ينتج عنها إعلامات نقل MAC على المحول.

1. يحاول المضيف 1 على شبكة VLAN رقم 35 الاتصال بالمضيف 2 الموجود على مركز البيانات الآخر.
2. تحتوي المضيف 1 على بوابة افتراضية هي الموجه 1 والموجه 1 لديه مسار للوصول إلى المضيف 2 عن طريق القدرة على الاتصال بالموجه 2 مباشرة عبر إرتباط بديل وفي هذه الحالة نفترض تحويل التسمية متعدد البروتوكولات (MPLS) وليس من خلال مجموعة ASA.
3. يستلم الموجه 2 حركة المرور الواردة ويوجهها إلى المضيف 2.
4. الآن عندما يستجيب المضيف 2، يستلم الموجه 2 حركة مرور الإرجاع ويجد مسارا متصلا مباشرة من خلال وحدات التحكم في الوصول الخاصة (ASA) بدلا من حركة المرور التي ترسلها عبر نقاط الوصول الخاصة الظاهرية (MPLS).
5. في هذه المرحلة، يتلقى حركة المرور التي تترك الموجه 2 المصدر MAC الخاص بواجهة خروج الموجه 2.
6. يستلم ASAs في DataCenter 2 حركة مرور الإرجاع ويجد اتصالا موجود ويتم إجراؤه بواسطة ASAs في DataCenter 1.
7. يرسل ASAs في DataCenter 2 حركة مرور البيانات العائدة عبر CCL مرة أخرى إلى ASAs في DataCenter 1.
8. في هذه المرحلة يقوم ASAs في مركز البيانات 1 بمعالجة حركة مرور البيانات العائدة وإرسالها لأسفل نحو المحول 1. الربط بعد يتلقى ال نفسه مصدر MAC مثل أن من المسحاج تخديد 2 مخرج قارن.
9. الآن عندما يستلم المفتاح 1 الربط، هو يدون ماك نقل إعلام لأن في البداية هو علمت المسحاج تخديد 2 {mac address}upper عبر القارن أي يكون ربطت إلى ال OTV خطوة، مهما في هذه المرحلة هو يبدأ يعلم

ال mac عنوان من القارن يربط إلى ال ASAs.

السيناريو 4

حركة المرور التي تم إنشاؤها بواسطة ASA، كما هو موضح في الصورة:

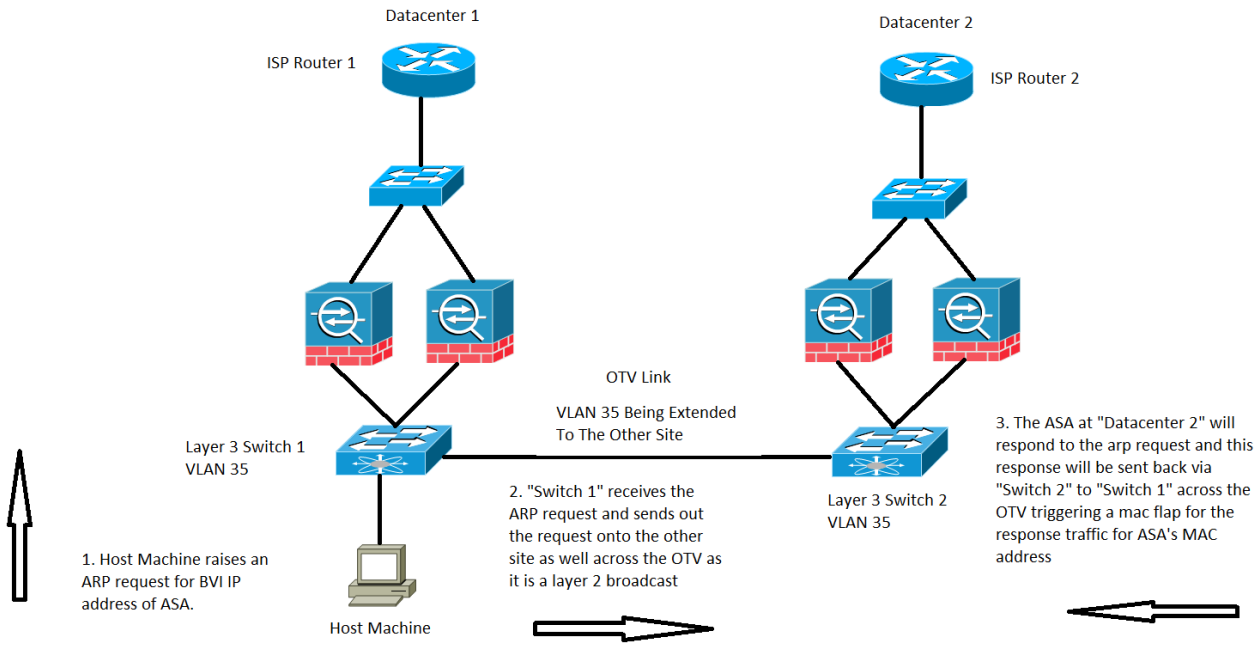


سيتم ملاحظة هذه الحالة المحددة لأي حركة مرور يتم إنشاؤها بواسطة ASA نفسها. هنا يتم مراعاة حالتين محتملتين، حيث يحاول ASA إما الوصول إلى بروتوكول وقت الشبكة (NTP) أو خادم syslog، الذي يكون على الشبكة الفرعية نفسها التي تكون عليها واجهة BVI الخاصة به.ومع ذلك، لا يقتصر هذا الوضع على هذين الشرطين فقط، ويمكن أن يحدث هذا الموقف كلما تم إنشاء حركة مرور بواسطة ASA لأي عنوان IP متصل مباشرة بعناوين BVI IP.

1. إذا لم يكن ASA لديه معلومات ARP الخاصة بخادم NTP/خادم syslog، فسيقوم ASA بإنشاء طلب ARP لذلك الخادم.
2. بما أن طلب ARP هو حزمة بث، المفتاح 1 سيستلم هذا ربط من ه يربط قارن من ال ASA ويفيض هو عبر all the قارن في VLAN خاص بما في ذلك الموقع بعيد عبر ال OTV.
3. سيتلقى محول الموقع البعيد 2 طلب ARP هذا من إرتباط OTV ونظرا لأن مصدر MAC من ASA، فإنه يلد إعلام MAC flap لأن نفس عنوان MAC يتم التعرف عليه عبر OTV من خلال واجهات OTV المحلية المتصلة مباشرة إلى ASA.

السيناريو 5

حركة المرور الموجهة إلى عنوان IP BVI الخاص ب ASA من مضيف متصل مباشرة، كما هو موضح في الصورة:



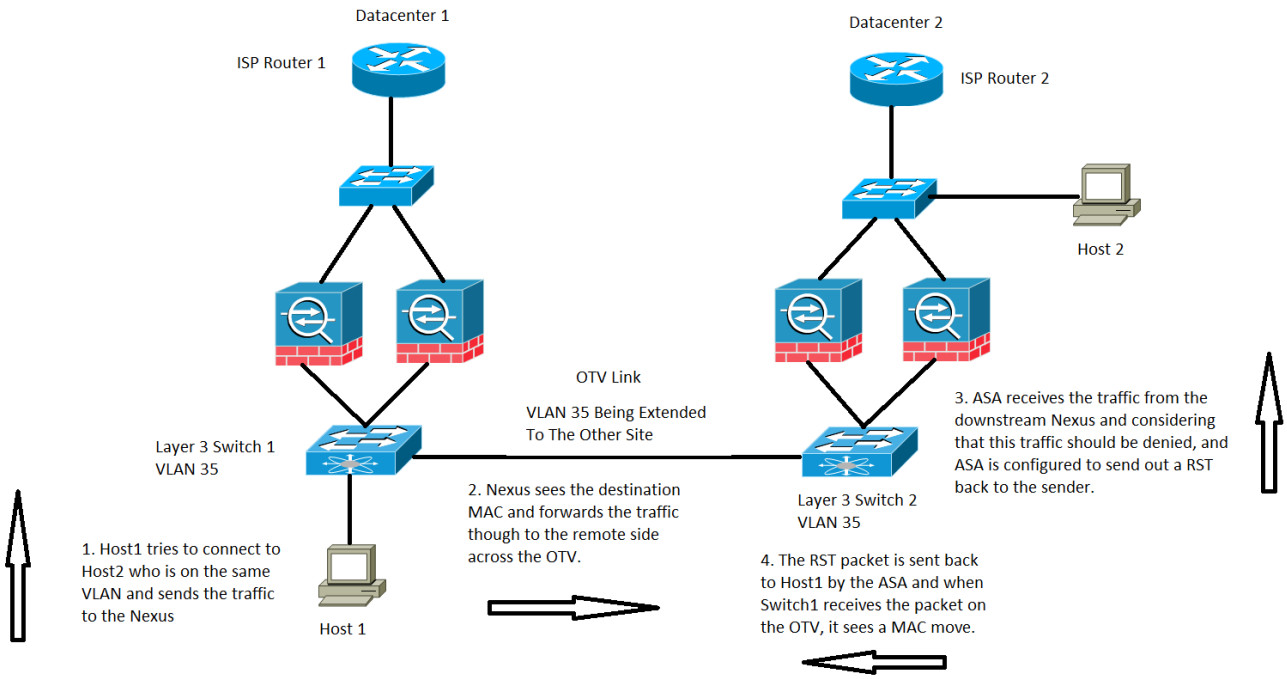
كما يمكن ملاحظة حركة MAC في بعض الأحيان عندما تكون حركة المرور موجهة إلى عنوان BVI IP الخاص ب ASA.

في السيناريو، لدينا جهاز مضيف على شبكة متصلة مباشرة من ASA ونحاول الاتصال ب ASA.

1. لا يحتوي المضيف على ARP الخاص ب ASA ويقوم بتشغيل طلب ARP.
2. يستلم ال nexus الحركة مرور ومرة أخرى بما أن هو إذاعة حركة مرور يرسل الحركة مرور عبر ال OTV إلى الآخر موقع أيضا.
3. يمكن أن يستجيب ASA الموجود على مركز البيانات البعيد 2 لطلب ARP ويرسل حركة مرور البيانات مرة أخرى من خلال نفس المسار وهو المحول 2 على الجانب البعيد، OTV، المحول 1 على الجانب المحلي ثم المضيف الطرفي.
4. عندما يرى ال ARP إستجابة على المحلي مفتاح 1، هو يطلق ماك نقل إعلام بما أن هو يرى ال MAC عنوان من ال ASA أي يأتي من ال OTV خطوة.

السيناريو 6

تم تعيين ASA لرفض حركة المرور التي يرسل معها RST إلى المضيف، كما هو موضح في الصورة:



في هذه الحالة، نحن مضيف 1 على VLAN 35، يحاول هو أن يتصل مع المضيف 2 في ال نفسه طبقة VLAN 3، مهما، مضيف 2 في الواقع على VLAN 1535 datacenter 2.

1. المضيف 2MAC عنوان كنت رأيت على مفتاح 2 عن طريق القارن يربط إلى ال ASAs.
2. سيكون المحول 1 قادرا على رؤية عنوان MAC للمضيف 2 من خلال إرتباط OTV.
3. المضيف 1 يرسل حركة مرور إلى المضيف 2 وهذا يتبع المسار من مفتاح 1، OTV، مفتاح 2، ASAs في مركز البيانات 2.
4. يتم رفض هذا الإجراء المحدد بواسطة ASA ونظرا لأنه يتم تكوين ASA لإرسال RST إلى المضيف 1، تعود حزمة RST باستخدام عنوان MAC المصدر الخاص ب ASA.
5. عندما تجعلها هذه الحزمة مرة أخرى إلى المفتاح 1 عبر ال OTV، المفتاح 1 يسجل ماك نقل إعلام ل ASA {upper}mac address لأن هو الآن يرى ال MAC عنوان عبر ال OTV، أي قبل أن يرى هو العنوان من هو مباشرة يربط قارن.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- دليل تكوين Cisco ASA Series CLI
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).