Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Общие сведения](#)
[Уведомления ПЕРЕМЕЩЕНИЯ MAC](#)
[Схема сети](#)
[Уведомления перемещения MAC на коммутаторе](#)
[Сценарий 1](#)
[Рекомендации](#)
[Сценарий 2](#)
[Рекомендации](#)
[Ситуация 3](#)
[Сценарий 4](#)
[Сценарий 5](#)
[Сценарий 6](#)
[Проверка](#)
[Устранение неполадок](#)
[Дополнительные сведения](#)

Введение

Этот документ описывает некоторые общие проблемы с Охваченным кластером Межузла Прозрачного режима EtherChannel.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Межсетевой экран Устройства адаптивной защиты (ASA)
- Объединение в кластеры ASA

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Стартовая версия ASA 9.2, объединение в кластеры межузла поддерживается в чем,

модули ASA могли быть расположены в других центрах обработки данных, и Кластерный канал управления (CCL) связан по Межсоединению ЦОД (DCI). Возможные сценарии развертывания:

- Кластер межузла отдельного интерфейса
- Охваченный кластер межузла прозрачного режима EtherChannel
- Охваченный Кластер Межузла Режима маршрутизации EtherChannel (поддерживаемый от 9.5 и далее)

Уведомления ПЕРЕМЕЩЕНИЯ MAC

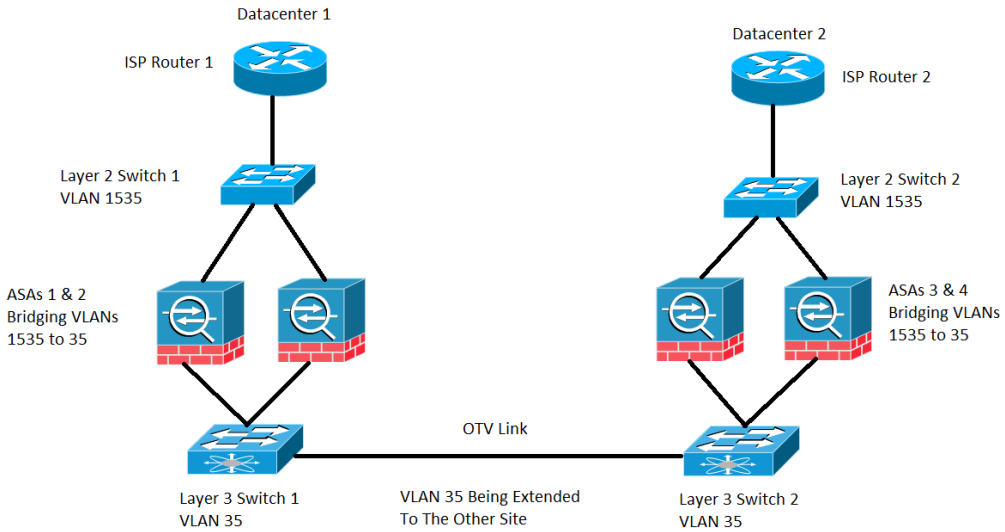
Когда MAC-адрес в Порт изменений Таблицы ассоциативно-запоминающего устройства (CAM), уведомление ПЕРЕМЕЩЕНИЯ MAC генерируется. Однако уведомление ПЕРЕМЕЩЕНИЯ MAC не генерируется. Предположим, изучен ли MAC-адрес X через интерфейсный GigabitEthernet0/1 в VLAN10, и через какое-то время тот же MAC замечен через GigabitEthernet0/2 в VLAN 10, то уведомление ПЕРЕМЕЩЕНИЯ MAC генерируется.

Системный журнал от коммутатора:

Системный журнал от ASA:

Схема сети

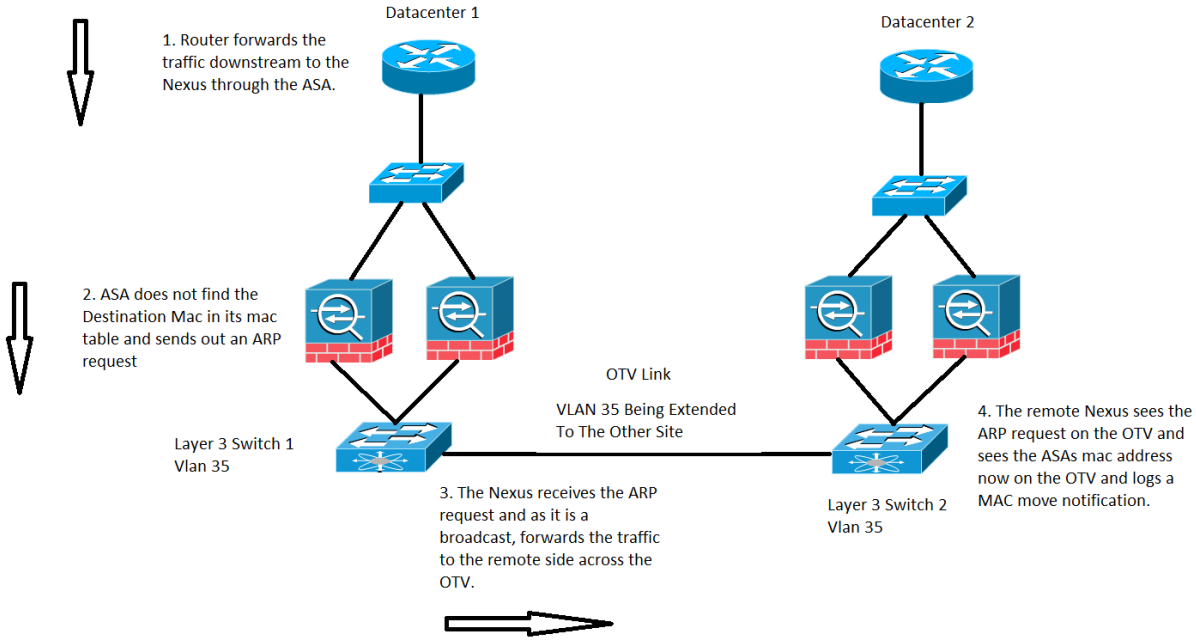
 Развертывания кластера межузла в чем ASA настроены в прозрачном режиме, соединяющем VLAN 1535 и VLAN 35. Внутренний VLAN 35 расширен по Виртуализации транспорта наложения (OTV), тогда как внешняя VLAN 1535 не расширена по OTV, как показано в образе



Уведомления перемещения MAC на коммутаторе

Сценарий 1

Трафик предназначил к MAC-адресу, запись которого не присутствует на таблице MAC ASA, как показано в образе:



В прозрачном ASA, Если MAC - адрес назначения пакета, поступающего в ASA, не находится в таблице MAC-адресов, это отсылает Запрос протокола переопределения адресов (ARP) для того назначения (если в той же подсети как BVI) или запрос протокола управляющих сообщений интернета (ICMP) со Временем жизни 1 (TTL 1) с адресом MAC источника как MAC-адрес Виртуального интерфейса моста (BVI) и MAC - адрес назначения, поскольку пропущен Контроллер доступа интерфейса назначения (DMAC).

В предыдущем случае у вас есть они трафик:

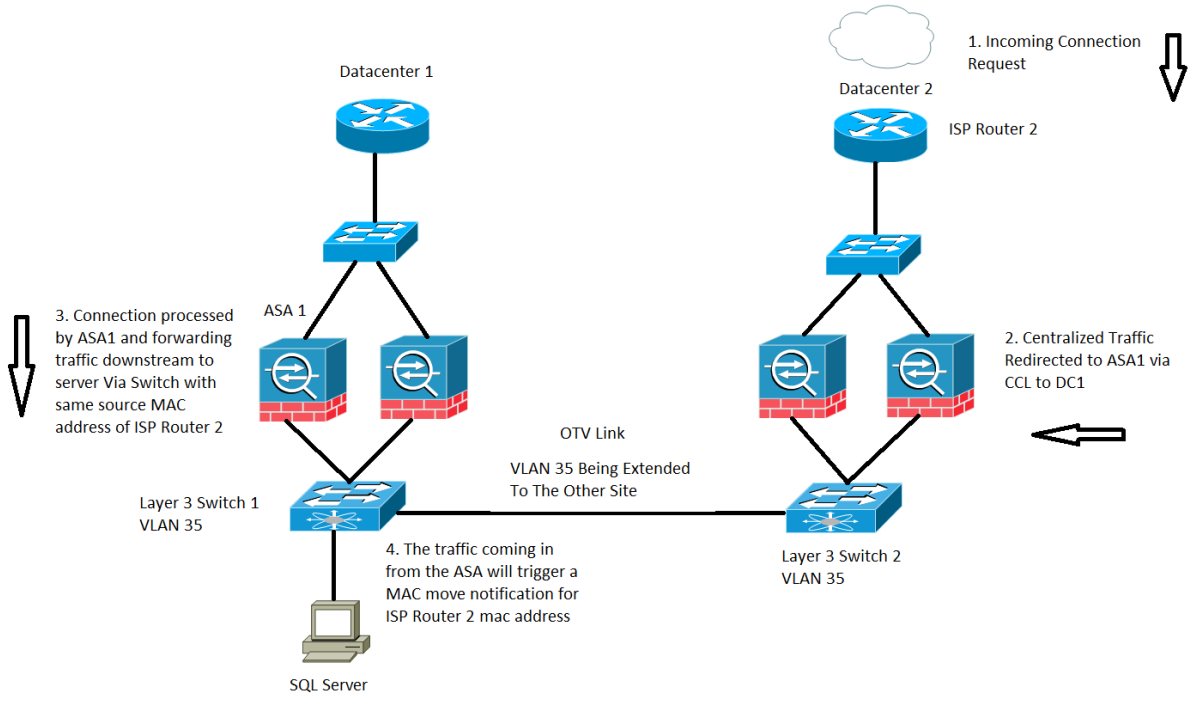
1. Маршрутизатор ISP на Центре обработки данных 1 передает трафик определенному назначению, которое находится позади ASA.
2. Любой из ASA может получить трафик и в этом случае, MAC - адрес назначения трафика не известен ASA.
3. Теперь IP - адрес назначения трафика находится в той же подсети как тот из BVI и, как упомянуто прежде, ASA теперь генерирует запрос ARP для IP - адреса назначения.
4. Коммутатор 1 получает трафик и поскольку запрос является широковещанием, это передает трафик к Центру обработки данных 2, а также через ссылку OTV.
5. Когда Коммутатор 2 видит запрос ARP от ASA на ссылке OTV, это регистрирует уведомление ПЕРЕМЕЩЕНИЯ MAC, потому что ранее MAC-адрес ASA был изучен через непосредственно связанный интерфейс, и теперь это изучается через ссылку OTV.

Рекомендации

Это - угловой сценарий.

Сценарий 2

Централизованная обработка потока ASA, как показано в образе:



Контроль базировался, трафик через кластер ASA классифицирован в три типа:

- Централизованный
- Распределенный
- Полураспределенный

В случае Централизованного контроля любой трафик, который должен быть осмотрен, перенаправлен к основному модулю кластера ASA. Если ведомый модуль кластера ASA получает трафик, это передано ведущему устройству через CCL.

В более раннем образе вы работаете с трафиком SQL, который является Централизованным инспекционным протоколом (CIP), и поведение, описанное здесь, применимо для любого CIP.

Вы получаете трафик на Центре обработки данных 2, где у вас только есть ведомые модули кластера ASA, основной модуль расположен в Центре обработки данных 1, который является ASA 1.

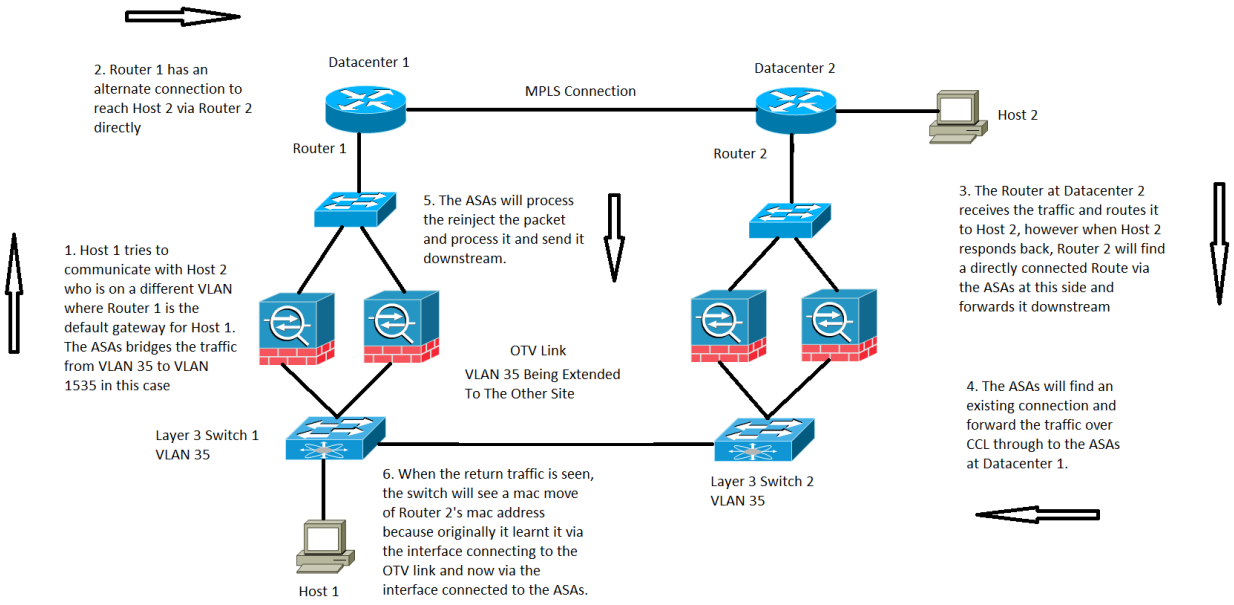
1. Маршрутизатор ISP 2 на Центре обработки данных 2 получает трафик и вперед это нисходящий к ASA на его узле.
2. Любой из ASA может получить этот трафик и как только это решает, что этот трафик

должен быть осмотрен и поскольку протокол централизован, это передает трафик к основному модулю через CCL.
3. ASA 1 получает трафик через CCL, обрабатывает трафик и передает его нисходящий к Серверу SQL.
4. Теперь, когда ASA 1 вперед трафик нисходящий, это сохраняет мак адрес исходного источника Маршрутизатора ISP 2, который расположен в Центре обработки данных 2 и передает его нисходящий.
5. Когда Коммутатор 1 получает этот определенный трафик, он входит в уведомление ПЕРЕМЕЩЕНИЯ MAC, потому что он первоначально видит Маршрутизатор ISP 2 MAC-адреса через ссылку OTV, которая связана с Центром обработки данных 2, и теперь он видит трафик, который входит от интерфейсов, связанных с ASA 1.

Рекомендации

Рекомендуется направить централизованные соединения с тем, какой бы ни узел размещает ведущее устройство (на основе приоритетов), как показано в образе:

Ситуация 3



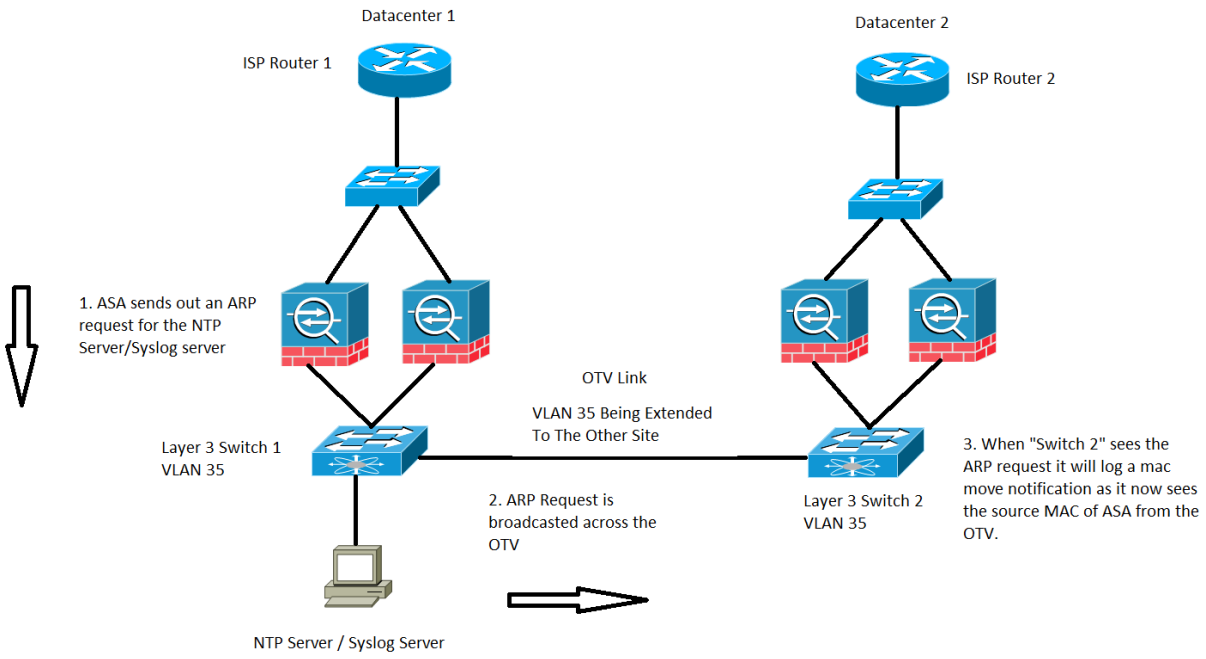
Для Предавать земле связи Контроллера домена (DC) в прозрачном режиме этот определенный трафик не покрыт или задокументирован, но этот определенный трафик действительно работает с точки зрения обработки потока ASA. Однако это может привести к уведомлениям перемещения MAC на коммутаторе.

1. Хост 1 на VLAN 35 пытается связаться с Хостом 2, который присутствует на другом Центре обработки данных.
2. Хост 1 имеет шлюз по умолчанию, который является маршрутизатором 1, и маршрутизатор 1 имеет путь для достижения Хоста 2 способностью связаться с маршрутизатором 2 непосредственно через альтернативную ссылку, и в этом случае мы принимаем Многопротокольную коммутацию по меткам (MPLS) а не через кластер ASA.

3. Маршрутизатор 2 получает входящий трафик и направляет его к Хосту 2.
4. Теперь, когда Хост 2 отвечает назад, маршрутизатор 2 получает ответный трафик, и это находит маршрут прямого соединения через ASA вместо трафика, который это передает по MPLS.
5. На данном этапе трафик, который оставляет маршрутизатор 2, имеет адрес MAC источника выходного интерфейса маршрутизатора 2.
6. ASA в Центре обработки данных 2 получают ответный трафик и находят соединение, которое существует и сделано ASA в Центре обработки данных 1.
7. ASA в Центре обработки данных 2 передают ответный трафик по CCL назад к ASA в Центре обработки данных 1.
8. На данном этапе ASA в Центре обработки данных 1 процесс ответный трафик и передают его вниз к Коммутатору 1. Пакет все еще имеет тот же адрес MAC источника как тот из выходного интерфейса маршрутизатора 2.
9. Теперь, когда Коммутатор 1 получает пакет, он регистрирует уведомление перемещения MAC, потому что первоначально он изучил MAC-адрес маршрутизатора 2 через интерфейс, который связан со ссылкой OTV, однако на данном этапе он начинает изучать MAC-адрес из интерфейса, связанного с ASA.

Сценарий 4

Трафик, генерируемый ASA, как показано в образе:

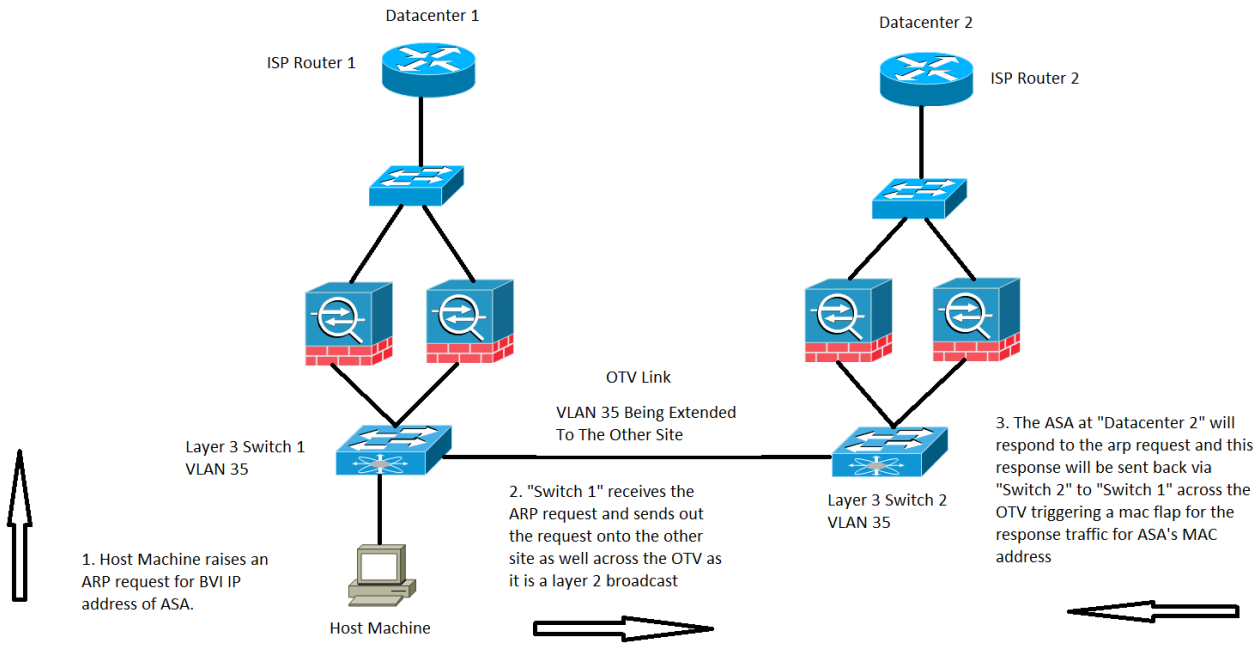


Этот конкретный случай будет наблюдаться для любого трафика, который генерируется самим ASA. Здесь две возможных ситуации рассматривают, в чем ASA или пытается достигнуть Протокола NTP или Сервера системного журнала, которые находятся в той же подсети как тот из ее интерфейса BVI. Однако, это не только ограничено этими двумя условиями, эта ситуация может произойти каждый раз, когда трафик генерируется ASA для любого IP-адреса, который напрямую подключается к IP-адресам BVI.

1. Если ASA не будет иметь информации о ARP сервера NTP / Сервером системного журнала, то ASA будет генерировать запрос ARP для того сервера.
2. Поскольку запрос ARP является транслируемым пакетом, Коммутатор 1 получит этот пакет от своего связанного интерфейса ASA и лавинно разошлет его через все интерфейсы в определенной VLAN включая удаленный узел через OTV.
3. Удаленный Коммутатор 2 узла получит этот запрос ARP от ссылки OTV и из-за адреса MAC источника ASA, это генерирует уведомление откидной створки MAC, так как тот же MAC-адрес изучен через OTV через его локальную переменную непосредственно связанные интерфейсы к ASA.

Сценарий 5

Трафик, предназначенный к IP-адресу BVI ASA от напрямую подключенного узла, как показано в образе:



Когда трафик предназначен к IP-адресу BVI ASA, ПЕРЕМЕЩЕНИЕ MAC может также время от времени наблюдаться.

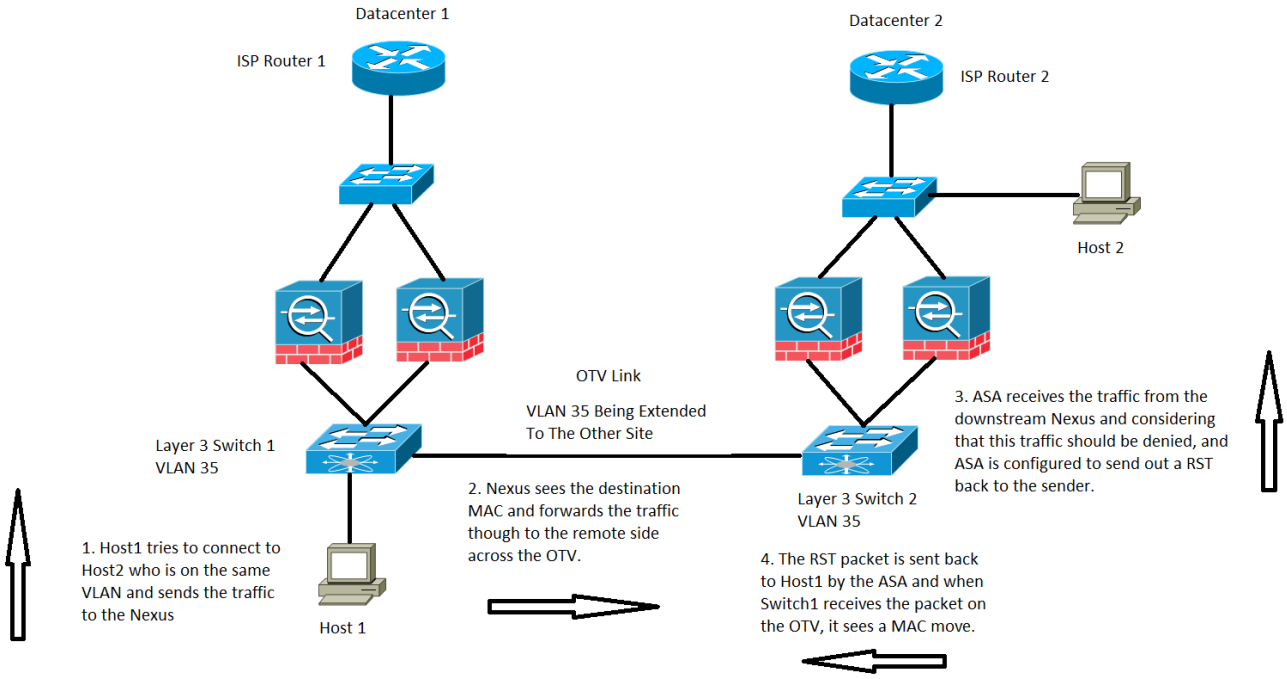
В сценарии у нас есть Главный компьютер на непосредственно связанная сеть ASA, и пытается соединиться с ASA.

1. Хост не имеет ARP ASA и инициирует запрос ARP.
2. Nexus получает трафик и снова поскольку это - широковещательный трафик, который это передает трафику через OTV к другому узлу также.
3. ASA на удаленном Центре обработки данных 2 может ответить на запрос ARP и передает трафик обратно через тот же путь, который является Коммутатором 2 на удаленной стороне, OTV, Коммутаторе 1 на локальной стороне и затем конечном хосте.
4. Когда ответ ARP замечен на Коммутаторе 1 локальной стороны, он инициирует уведомление перемещения MAC, поскольку он видит MAC-адрес ASA, который входит

от ссылки OTV.

Сценарий 6

Набор ASA для запрета трафика, наряду с которым это передает RST к Хосту, как показано в образе:



В этом случае у нас есть Хост 1 хоста на VLAN 35, это пытается связаться с Хостом 2 в той же VLAN Уровня 3, однако, Хост 2 находится фактически на Центре обработки данных 2 VLAN 1535.

1. Адрес хоста 2MAC был бы замечен на Коммутаторе 2 через интерфейс, связанный с ASA.
2. Коммутатор 1 видел бы MAC-адрес Хоста 2 через ссылку OTV.
3. Хост 1 передает трафик к Хосту 2, и это придерживается пути Коммутатора 1, OTV, Коммутатора 2, ASA в Центре обработки данных 2.
4. Это определенное запрещено ASA и поскольку ASA настроен для передачи RST обратно в Хост 1, пакет RST возвращается с источником с MAC-адресом ASA.
5. Когда этот пакет возвращается к Коммутатору 1 через OTV, Коммутатор 1 регистрирует уведомление ПЕРЕМЕЩЕНИЯ MAC для MAC-адреса ASA, потому что это теперь видит MAC-адрес через OTV, в чем прежде чем это будет видеть адрес от непосредственно связанный интерфейс.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Руководство по настройке интерфейса командной строки для Cisco ASA
- Cisco Systems – техническая поддержка и документация