Содержание

Введение

Этот документ описывает некоторые существующие ограничения и доступные обходные пути для создания AnyConnect и OpenDNS, Бродящего по Работе с клиентами вместе.

Предварительные условия

Опыт работы AnyConnect и OpenDNS, Бродящего по клиенту.

Знакомство с ASA или конфигурацией головного узла IOS/IOS-XE (туннельная группа/групповая политика) для VPN AnyConnect.

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- ASA или головной узел IOS/IOS-XE
- Оконечная точка, выполняющая Клиента AnyConnect VPN Client и OpenDNS, Бродящий по клиенту

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Головной узел ASA рабочий выпуск 9.4
- Windows 7
- Клиент AnyConnect 4.2.00096
- OpenDNS, Бродящий по клиенту 2.0.154

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

OpenDNS разрабатывает плагин AnyConnect с командой AnyConnect Cisco, чтобы быть доступным в будущем. В то время как никакие даты не были назначены, эта интеграция позволит Бродящему Клиенту работать с клиентом AnyConnect без обращенных обходных путей. Это также позволит AnyConnect быть механизмом доставки для Бродящего Клиента.

Функциональность

Обработка DNS AnyConnect

Головная станция VPN может быть настроена парой других способов обработать трафик от клиента AnyConnect.

1. Полная конфигурация туннеля (туннель - все): Это вынуждает весь трафик от оконечной точки передаваться через VPN-туннель, зашифрованный, и поэтому трафик никогда не оставляет адаптер открытого интерфейса в открытом тексте
2. Конфигурация разделения туннеля:

o. Разделение - включает туннелирование: Трафик предназначил только к определенным подсетям, или хосты, определенные на головной станции VPN,

передается через туннель, весь другой трафик передается возле туннеля в открытом тексте

b. Разделение - исключает туннелирование: Трафик предназначил только к определенным подсетям, или хосты, определенные на головной станции VPN, исключен из шифрования и оставляет открытый интерфейс в открытом тексте, весь другой трафик зашифрован и только передан через туннель

Каждая из этих конфигураций определяет, как Разрешение DNS обрабатывается клиентом AnyConnect, в зависимости от операционной системы на оконечной точке. Было изменение в поведении в механизме обработки DNS на AnyConnect для Windows в выпуске 4.2 после исправления для CSCuf07885.

Windows 7 +

Tunnel - вся конфигурация (и раздельное туннелирование с туннелем - весь DNS включил),

Пред AnyConnect 4.2:

Только запросы DNS к серверам DNS, настроенным под групповой политикой (туннельные серверы DNS), позволены. Драйвер AnyConnect отвечает на все другие запросы с 'никаким таким названием' ответ. В результате Разрешение DNS может только быть выполнено с помощью туннельных серверов DNS.

AnyConnect 4.2 +

Запросы DNS к любым серверам DNS позволены, пока они инициируются из адаптера VPN и передаются через туннель. Все другие запросы не отвечают с 'никаким таким названием' ответ, и Разрешение DNS может только быть выполнено через VPN-туннель

До CSCuf07885 исправляют, AC ограничивает целевые серверы DNS, однако с исправлением для CSCuf07885, это ограничивает, какие адаптеры сети могут инициировать запросы DNS.

Разделение - включает конфигурацию (туннель - весь отключенный DNS и никакой split-DNS)

Драйвер AnyConnect не вмешивается в собственного Распознавателя DNS. Поэтому Разрешение DNS выполнено на основе заказа адаптеров сети, и AnyConnect является всегда предпочтительным адаптером, когда связана VPN. Таким образом, запрос DNS будет сначала передаваться через туннель и если это не станет решенным, то преобразователь попытается решить его через открытый интерфейс. Разделение - включает access-list, должен будет включать подсеть, покрывающую Туннельный сервер (серверы) DNS. Начиная с AnyConnect 4.2 маршруты хоста для Туннельного сервера (серверов) DNS автоматически добавлены, как разделено - включают сети (безопасные маршруты) клиентом AnyConnect, и поэтому разделение - включает access-list, больше не требует явного добавления туннельной подсети сервера DNS.

Разделение - исключает конфигурацию (туннель - весь отключенный DNS и никакой split-DNS)

Драйвер AnyConnect не вмешивается в собственного Распознавателя DNS. Поэтому Разрешение DNS выполнено на основе заказа адаптеров сети, и AnyConnect является всегда предпочтительным адаптером, когда связана VPN. Таким образом, запрос DNS будет сначала передаваться через туннель и если это не станет решенным, то преобразователь попытается решить его через открытый интерфейс. Разделение - исключает access-list, не должен включать подсеть, покрывающую Туннельный сервер (серверы) DNS. Начиная с AnyConnect 4.2 маршруты хоста для Туннельного сервера (серверов) DNS автоматически добавлены, как разделено - включают сети (безопасные маршруты) клиентом AnyConnect, и поэтому который предотвратит неверную конфигурацию в разделении - исключают access-list.

Split-DNS (туннель - весь отключенный DNS, разделение - включают настроенный),

Пред AnyConnect 4.2

Запросам DNS, совпадающим с доменами split-dns, позволяют туннелировать серверы DNS, но не позволяют другим серверам DNS. Чтобы препятствовать тому, чтобы такие запросы Internal DN просочились туннель, драйвер AnyConnect не отвечает 'таким названием', если запрос передается другим серверам DNS. Таким образом, домены split-dns могут только быть решены через туннельные серверы DNS.

Запросы DNS, не совпадающие с доменами split-dns, позволены другим серверам DNS, но не позволены туннелировать серверы DNS. Даже в этом случае, если запрос для доменов split-dns non предпринят через туннель, драйвер AnyConnect не отвечает 'таким названием'. Таким образом, домены split-dns non могут только быть решены через общие серверы DNS возле туннеля.

AnyConnect 4.2 +

Запросы DNS, совпадающие с доменами split-dns, позволены любым серверам DNS, пока они происходят из адаптера VPN. Если запрос инициируется открытым интерфейсом, драйвер AnyConnect не отвечает 'никаким таким названием', чтобы вынудить преобразователь всегда использовать туннель для разрешения имен. Таким образом, домены split-dns могут только быть решены через туннель.

Запросы DNS, не совпадающие с доменами split-dns, позволены любым серверам DNS, пока они происходят из физического адаптера. Если запрос инициируется адаптером VPN, AnyConnect не отвечает 'таким названием', чтобы вынудить преобразователь всегда делать попытку разрешения имен через открытый интерфейс. Таким образом, домены split-dns non могут только быть решены через открытый интерфейс.

Mac OS X

Tunnel - вся конфигурация (и раздельное туннелирование с туннелем - весь DNS включил),

Когда AnyConnect связан, только Туннельные серверы DNS поддержаны в системной Конфигурации DNS, и поэтому запросы DNS могут только быть переданы Туннельному серверу (серверам) DNS.

Разделение - включает конфигурацию (туннель - весь отключенный DNS и никакой split-DNS)

AnyConnect не вмешивается в собственного Распознавателя DNS. Туннельные серверы DNS настроены как предпочтенные преобразователи, имеющие приоритет по общим серверам DNS, таким образом гарантировав, что начальный запрос DNS для разрешения имен передается по туннелю. Так как параметры настройки DNS являются глобальным на MAC OS X, для запросов DNS не возможно использовать общие серверы DNS возле туннеля, как задокументировано в CSCtf20226. Начиная с AnyConnect 4.2 маршруты хоста для Туннельного сервера (серверов) DNS автоматически добавлены, как разделено - включают сети (безопасные маршруты) клиентом AnyConnect, и поэтому разделение - включает access-list, больше не требует явного добавления туннельной подсети сервера DNS.

Разделение - исключает конфигурацию (туннель - весь отключенный DNS и никакой split-DNS)

AnyConnect не вмешивается в собственного Распознавателя DNS. Туннельные серверы DNS настроены как предпочтенные преобразователи, имеющие приоритет по общим серверам DNS, таким образом гарантировав, что начальный запрос DNS для разрешения имен передается по туннелю. Так как параметры настройки DNS являются глобальным на MAC OS X, для запросов DNS не возможно использовать общие серверы DNS возле туннеля, как задокументировано в CSCtf20226. Начиная с AnyConnect 4.2 маршруты хоста для Туннельного сервера (серверов) DNS автоматически добавлены, как разделено - включают сети (безопасные маршруты) клиентом AnyConnect, и поэтому разделение - включает access-list, больше не требует явного добавления туннельной подсети сервера DNS.

Split-DNS (туннель - весь отключенный DNS, разделение - включают настроенный),

Если split-DNS включен для обоих Протоколов "IP" (IPv4 и IPv6), или это только включено для одного протокола и нет никакого пула адресов, настроенного для другого протокола:
Истинный split-DNS, подобный Windows, принужден. Истинный split-DNS означает, что запросы, совпадающие с доменами split-DNS, только решены через туннель, они не пропущены к серверам DNS возле туннеля.

Если split-DNS включен только для одного протокола, и адрес клиента назначен для другого протокола, только "нейтрализация DNS для раздельного туннелирования" принуждена. Это означает, что AC только позволяет запросы DNS, совпадающие с доменами split-DNS через туннель (другим запросам отвечает AC с "отказанным" ответом для принуждения аварийного переключения к общим серверам DNS), но не может принудить, который запрашивает, чтобы соответствующие домены split-DNS не были представлены ясное через общий адаптер.

Linux

Tunnel - вся конфигурация (и раздельное туннелирование с туннелем - весь DNS включил),

Когда AnyConnect связан, только Туннельные серверы DNS поддержаны в системной Конфигурации DNS, и поэтому запросы DNS могут только быть переданы Туннельному серверу (серверам) DNS.

Разделение - включает конфигурацию (туннель - весь отключенный DNS и никакой split-DNS)

AnyConnect не вмешивается в собственного Распознавателя DNS. Туннельные серверы DNS настроены как предпочтенные преобразователи, имеющие приоритет по общим серверам DNS, таким образом гарантировав, что начальный запрос DNS для разрешения имен передается по туннелю.

Разделение - исключает конфигурацию (туннель - весь отключенный DNS и никакой split-DNS)

AnyConnect не вмешивается в собственного Распознавателя DNS. Туннельные серверы DNS настроены как предпочтенные преобразователи, имеющие приоритет по общим серверам DNS, таким образом гарантировав, что начальный запрос DNS для разрешения имен передается по туннелю.

Split-DNS (туннель - весь отключенный DNS, разделение - включают настроенный),

Если split-DNS включен, только "нейтрализация DNS для раздельного туннелирования" принуждена. Это означает, что AC только позволяет запросы DNS, совпадающие с доменами split-DNS через туннель (другим запросам отвечает AC с "отказанным" ответом для принуждения аварийного переключения к общим серверам DNS), но не может принудить, который запрашивает, чтобы соответствующие домены split-DNS не были представлены ясное через общий адаптер.

OpenDNS, Бродящий по клиенту

Бродящий клиент является компонентом программного обеспечения, который управляет сервисами DNS на оконечной точке и использует общие серверы DNS OpenDNS, чтобы защитить и зашифровать трафик DNS.

Идеально, клиент должен быть в защищенном и зашифрованном состоянии. Однако, если клиент неспособен установить сеанс TLS с общим сервером преобразователя OpenDNS (208.67.222.222), он пытается передать трафик DNS, дешифрованный на порту 53 UDP к 208.67.222.222. Бродящий Клиент исключительно использует общий IP-адрес преобразователя OpenDNS 208.67.222.222 (существуют немногие другие такой как

208.67.220.220, 208.67.222.220, и 208.67.220.222). Бродящий клиент однажды установил, устанавливает 127.0.0.1 (локальный узел) как локальный DNS - сервер и отвергает текущие поинтерфейсные параметры настройки DNS. Текущие параметры настройки DNS сохранены в локальных resolv.conf файлах (даже на Windows) в Бродящей папке Конфигурации клиента. OpenDNS будет резервировать даже те серверы DNS, которые изучены через адаптер AnyConnect. Например, если 192.168.92.2 будет сервер DNS на общем адаптере, то OpenDNS создаст resolv.conf в следующем местоположении:

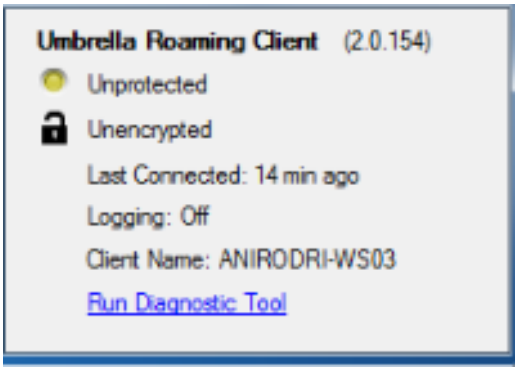
C : \ProgramData\OpenDNS\ERC\Resolver1-LocalAreaConnection-resolv.conf
сервер имен 192.168.92.2

Бродящий клиент зашифрует каждый пакетный набор к OpenDNS; однако, это не запускает или использует зашифрованный туннель для 208.67.222.222. У Бродящего Клиента действительно есть дополнительная функция Осуществления IP - уровня, которая откроет IP - безопасное соединение в целях не-DNS заблокировать IP-адреса. Это автоматически отключит в присутствии активного Соединения AnyConnect. Это также связывает с 127.0.0.1:53 для получения запросов, локально генерируемых на компьютере. Когда оконечная точка должна решить название, локальные запросы направлены к 127.0.0.1 должным к замене, и затем базовому процессу Бродящего Клиента dnscrypt-прокси вперед их к общим серверам OpenDNS по зашифрованному каналу.

Если DNS не разрешат течь к 127.0.0.1:53, то Бродящий Клиент не будет в состоянии функционировать, и придерживающееся произойдет. Если клиент будет неспособен достигнуть общих серверов DNS или 127.0.0.1:53 связанный адрес, то он перейдет к открытому состоянию сбоя и восстановит параметры настройки DNS на локальных адаптерах. В фоновом режиме, если безопасное соединение восстановлено, это продолжает передавать зонды к 208.67.222.222 и может перейти к активному режиму.

Ограничения

Посмотрев на функциональность высокого уровня обоих клиентов, очевидно, что у бродящего клиента должна быть способность изменить настройки локального DNS и связать с 127.0.0.1:53 для передачи запросов через безопасный канал. Когда VPN связана, единственные конфигурации, где AnyConnect не вмешивается в собственного Распознавателя DNS, являются разделением - включают и разделяются - исключают (с split-tunnel-all отключенным DNS). Когда бродящий клиент также используется, Поэтому в настоящее время рекомендуется использовать одну из тех конфигураций. Бродящий клиент останется в незащищенном/незашифрованном состоянии , если туннель - вся конфигурация будет использоваться, или split-tunnel-all DNS включен, как показано в образе.



Обходной путь

Если намерение состоит в том, чтобы защитить связь между бродящим клиентом и серверами OpenDNS с помощью VPN-туннеля, то фиктивное разделение - исключает access-list, может использоваться на головной станции VPN. Это будет самой близкой вещью к полной конфигурации туннеля. Если нет такого требования, то разделенный - включают, может использоваться, где access-list не включает общие серверы OpenDNS, или разделение - исключает, может использоваться где access-list includes общие серверы OpenDNS.

Кроме того, при использовании Бродящего Клиента, режимы split-DNS не могут использоваться, поскольку это приведет к потере разрешения локального DNS. DNS Split-tunnel-all должен также остаться отключенным; однако, это частично поддерживается и должно позволить Бродящему Клиенту становиться зашифрованным поставарийным переключением.

Конфигурации

Туннель трафик OpenDNS

Данный пример использует фиктивный IP-адрес в разделении - исключают access-list. С этой конфигурацией вся связь с 208.67.222.222 происходит через VPN-туннель, и бродящий клиент действует в зашифрованном и защищенном состоянии.

Исключите трафик OpenDNS из VPN-туннеля

Данный пример использует адрес преобразователя OpenDNS в разделении - исключают access-list. С этой конфигурацией вся связь с 208.67.222.222 происходит вне VPN-туннеля, и бродящий клиент действует в зашифрованном и защищенном состоянии.

Данный пример показывает, что разделение - включает конфигурацию для внутренней 192.168.1.0/24 подсети. С этой конфигурацией бродящий клиент будет все еще действовать в зашифрованном и защищенном состоянии, так как трафик к 208.67.222.222 не передается через туннель.

Проверка

Когда VPN связана, Бродящий клиент должен показать защищенный и зашифрованный как показано в этом образе: