Поведенческие различия относительно запросов DNS и разрешения доменного имени в других ОС

Содержание

Введение

Этот документ описывает, как другие Операционные системы (ОС) обрабатывают запросы Системы доменных имен (DNS) и влияние на разрешении доменного имени с AnyConnect Cisco и разделяются или полное туннелирование.

Разделение по сравнению со стандартным DNS

Когда вы используете разделение - включают туннелирование, существует три параметра для dns:

1. **Разделение DNS** - запросы DNS, который совпадает с доменными именами, настроены на устройстве адаптивной защиты Cisco (ASA). Они перемещаются через туннель (к серверам DNS, которые определены на ASA, например), в то время как другие не делают.

2. **Tunnel-all-DNS** - Только трафик DNS к серверам DNS, которые определены ASA, позволен. Эта установка настроена в групповой политике.

3. **Стандартный DNS** - Все запросы DNS перемещаются через серверы DNS, которые определены ASA. В случае отрицательного ответа запросы DNS могли бы также перейти к серверам DNS, которые настроены на физическом адаптере.

Примечание: Split-tunnel-all-dns команда была сначала внедрена в Версии ASA 8.2 (5). Перед этой версией вы могли только сделать разделение DNS или стандартный DNS.

Во всех случаях запросы DNS, которые определены для перемещения через туннель, переходят к любым серверам DNS, которые определены ASA. Если нет никаких серверов DNS, определенных ASA, то параметры настройки DNS являются пробелом для туннеля. Если вам не определили разделение DNS, то все запросы DNS передаются серверам DNS, которые определены ASA. Однако способы поведения, которые описаны в этом документе, могут быть другими, в зависимости от Операционной системы (OS).

Примечание: Избегите использования NSLookup при тестировании разрешения имен на клиенте. Вместо этого полагайтесь на браузер или используйте **команду ping**. Это вызвано тем, что NSLookup не полагается на Распознавателя DNS ОС. AnyConnect не вызывает запрос DNS через некоторый интерфейс, но позволяет его или отклоняет его зависящий от конфигурации разделения DNS. Чтобы вынудить Распознавателя DNS попробовать приемлемый сервер DNS за запрос, важно, чтобы тестирование разделения DNS было только выполнено с приложениями, которые полагаются на собственного Распознавателя DNS для разрешения доменного имени (все приложения кроме NSLookup, Выройте, и подобные приложения, которые обрабатывают Разрешение DNS собой, например).

Истинный по сравнению с разделением DNS оптимального уровня

Выпуск 2.4 AnyConnect поддерживает Нейтрализацию разделения DNS (разделение DNS оптимального уровня), который не является истинным разделением DNS и найден в устаревшем Клиенте IPSEC. Если запрос совпадает с доменом разделения DNS, AnyConnect позволяет запросу быть туннелированным в ASA. Если сервер не может решить имя хоста, Распознаватель DNS продолжает и передает тот же запрос к серверу DNS, который сопоставлен с физическим интерфейсом.

С другой стороны, если запрос не совпадает ни с одним из доменов разделения DNS, AnyConnect не туннелирует он в ASA. Вместо этого это создает DNS - ответ так, чтобы

Распознаватель DNS переключился и передал запрос к серверу DNS, который сопоставлен с физическим интерфейсом. Именно поэтому эту функцию не называют разделением DNS, но нейтрализацией DNS для разделенного туннелирования. Мало того, что AnyConnect гарантирует, который только запрашивает, чтобы целевые домены разделения DNS были туннелированы в, это также полагается на поведение Распознавателя DNS клиентской операционной системы для разрешения имени хоста.

Это повышает проблемы безопасности из-за потенциальной утечки названия личного домена. Например, когда сервер имени DNS VPN не мог решить запрос DNS, собственный DNS - клиент может передать запрос за названием личного домена к общему серверу DNS в частности.

См. идентификатор ошибки Cisco CSCtn14578, в настоящее время решаемый на Microsoft Windows только, с Версии 3.0 (4235). Решение внедряет истинное разделение DNS, оно строго делает запрос настроенных доменных имен, который совпадает и позволен серверам DNS VPN. Все другие запросы только позволены другим серверам DNS, таким как настроенные на физическом адаптере (адаптерах).

Туннель все и туннель весь DNS

Когда разделенное туннелирование отключено (**туннель вся** конфигурация), трафик DNS позволен строго через туннель. **Туннель, который вся Конфигурация DNS** (настроенный в групповой политике) передает всем Поискам DNS через туннель, наряду с некоторым типом разделенного туннелирования и трафиком DNS, позволен строго через туннель.

Это совместимо через платформы с одним предупреждением на Microsoft Windows: когда любой **туннель, который все** или **туннель, весь DNS** настроен, AnyConnect, позволяют трафику DNS строго серверам DNS, которые настроены на защищенном шлюзе (применился к адаптеру VPN). Это - улучшение безопасности, внедренное наряду с ранее упомянутым истинным решением для разделения DNS.

Если это оказывается проблематичным в определенных сценариях (например, обновление/запросы регистрации DNS должно быть передано серверам DNS не-VPN), то выполните эти шаги:

1. Если текущая конфигурация является **туннелем все**, то включите **разделение - исключают туннелирование**. Любой один хост, разделение - сеть exclude приемлема для использования, такова как локальный для канала адрес.

2. Гарантируйте, что **туннелируют, весь DNS** не настроен в групповой политике.

Вопрос производительности DNS, решенный в версии 3.0 (4235) AnyConnect

Эта проблема Microsoft Windows главным образом распространена при этих условиях:

- С домашней настройкой маршрутизатора DNS и серверам DHCP назначают тот же IP-адрес (AnyConnect создает необходимый маршрут к серверу DHCP).

- Большое число Доменов DNS находится в групповой политике.
- **Туннель - вся** конфигурация используется.
- Разрешение имен выполнено неквалифицированным именем хоста, которое подразумевает, что преобразователь должен попробовать много суффиксов DNS на всех доступных серверах DNS до, одно соответствующее для делавшего запрос имени хоста предпринято.

Эта проблема происходит из-за собственного DNS - клиента, который пытается передать запросы DNS через физический адаптер, который AnyConnect блокирует (данный **туннель - вся** конфигурация). Это приводит к задержке разрешения имен, которая может быть значительной, особенно если большое число суффиксов DNS выдвинуто головным узлом. DNS - клиент должен идти через все запросы и доступные серверы DNS, пока это не получает положительный отклик.

Эта проблема решена в Версии 3.0 (4235) AnyConnect. Ссылочные идентификаторы ошибок Cisco CSCtq02141 и CSCtn14578, наряду с введением к ранее упомянутому истинному решению для разделения DNS, для получения дополнительной информации.

Если обновление не может быть внедрено, то это возможные обходной пути:

- Включите **разделение - исключают туннелирование** для IP-адреса, который позволяет запросам локального DNS течь через физический адаптер. Можно использовать адрес от linklocal подсети **169.254.0.0/16**, потому что маловероятно, что любое устройство передает трафик к одному из тех IP-адресов по VPN. После включения **разделения - исключают туннелирование**, включают доступ к локальной сети на клиентском профиле или на клиенте самом и отключают **туннель весь DNS**.

  На ASA сделайте эти изменения конфигурации:

  ```
  access-list acl_linklocal_169.254.1.1 standard permit host 169.254.1.1
  group-policy gp_access-14 attributes
  split-tunnel-policy excludespecified
  split-tunnel-network-list value acl_linklocal_169.254.1.1
  split-tunnel-all-dns disable
  exit
  ```

  На клиентском профиле необходимо добавить эту линию:

  ```
  <LocalLanAccess UserControllable="true">true</LocalLanAccess>
  ```

  Можно также включить это на на ну клиентской основе в GUI клиента AnyConnect. Перейдите к **Меню предпочтений AnyConnect** и проверьте **Разрешать** флажок **доступа к локальной сети**.
- Используйте полные доменные имена (FQDNs) вместо неполных имен хоста для разрешений имен.
- Используйте другой IP-адрес для сервера DNS на физическом интерфейсе.

DNS с разделенным туннелированием на других ОС

Другие ОС обрабатывают поиски DNS по-разному, когда используется через разделенное туннелирование (без разделения DNS) для AnyConnect. В этом разделе описываются те различия.

Microsoft Windows

В системах Microsoft Windows параметры настройки DNS поинтерфейсны. Если разделенное туннелирование используется, запросы DNS могут переключиться на физические серверы DNS адаптера после того, как они отказывают на адаптере VPN-туннеля. Если разделенное туннелирование без разделения DNS определено, то и внутреннее и внешнее Разрешение DNS работает, потому что это переключается на внешние серверы DNS.

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, где AnyConnect является всегда предпочтительным адаптером, когда связана VPN. Кроме того, запрос DNS сначала передается через туннель и если это не становится решенным, преобразователь пытается решить его через открытый интерфейс. Разделение - включает access-list includes подсеть, которая покрывает Туннельный сервер (серверы) DNS. Для начала 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, где AnyConnect является всегда предпочтительным адаптером, когда связана VPN. Кроме того, запрос DNS сначала передается через туннель и если это не становится решенным, преобразователь пытается решить его через открытый интерфейс. Разделение - исключает access-list, не должен включать подсеть, покрывающую Туннельный сервер (серверы) DNS. Для начала с AnyConnect 4.2 маршруты хоста для Туннельного сервера (серверов) DNS автоматически добавлены, как разделено - включают сети (безопасные маршруты) клиентом AnyConnect, и поэтому предотвращает неверную конфигурацию в разделении - исключают access-list.

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

Пред AnyConnect 4.2

Запросам DNS, который совпадает 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. Поэтому домены split-dns могут только быть решены через туннельные серверы DNS.

Запросы DNS, который не совпадает 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". Поэтому домены split-dns non могут только быть решены через общие серверы DNS возле туннеля.

AnyConnect 4.2 +

Запросы DNS, который совпадает 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. Поэтому домены split-dns могут только быть решены через туннель.

Запросы DNS, который не совпадает 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. Поэтому домены split-dns non могут только быть решены через открытый интерфейс.

Mac OS X

На Системах Macintosh параметры настройки DNS являются глобальным. Если разделенное туннелирование используется, но разделение DNS не используется, для запросов DNS не возможно достигнуть серверов DNS за пределами туннеля. Можно только решить внутренне, не внешне.

Это задокументировано в идентификаторы ошибок Cisco CSCtf20226 и CSCtz86314. В обоих случаях этот обходной путь должен решить вопрос:

- Задайте внешний IP-адрес сервера DNS под групповой политикой и используйте FQDN для запросов Internal DN.

- Если внешние названия разрешимы через туннель, то перешли к **Усовершенствованному> Разделенное туннелирование** и отключают разделение DNS через удаление имен DNS, которые настроены в групповой политике. Это требует использования FQDN для запросов Internal DN.

Случай разделения DNS решен в Версии 3.1 AnyConnect. Однако необходимо гарантировать, что соблюдают одно из этих условий:

- Разделение DNS должно быть включено для обоих Протоколов "IP", который требует Версии 9.0 Cisco ASA или позже.

- Разделение DNS должно быть включено для одного Протокола "IP". При выполнении Версии 9.0 Cisco ASA или позже то используйте клиентский обходной протокол для другого Протокола "IP". Например, гарантируйте, что нет никакого пула адресов и что **Клиентский Обходной Протокол** включен в групповой политике. Также, если вы выполняете версию ASA, которая является ранее, чем Версия 9.0, гарантируйте, что нет никакого пула адресов, настроенного для другого Протокола "IP". Это подразумевает, что другой Протокол "IP" является IPv6.

> **Примечание:** AnyConnect не изменяет **resolv.conf** файл на Macintosh OS X, а скорее изменяет специфичные для OS X настройки DNS. Macintosh OS X держит **resolv.conf** файл в курсе для обеспечений совместимости. Используйте **scutil - команда dns** для просмотра параметров настройки DNS на Macintosh 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, который имеет приоритет по общим серверам DNS, таким образом это гарантирует, 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. Для начала 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 это гарантирует, 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. Для начала 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 запрос, который совпадает с доменами split-DNS, только решен 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 запрос DNS, который совпадает 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 запрос, который совпадает с доменами split-DNS, которые не 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, который имеет приоритет по общим серверам DNS, таким образом это гарантирует, 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, который имеет приоритет по общим серверам DNS, таким образом это гарантирует, 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 запрос DNS, который совпадает 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 тот запрос, который совпадает с доменами split-DNS, которые не представлены ясное через общий адаптер.

iPhone

IPhone является завершенной противоположностью Системы Macintosh и не подобен Microsoft Windows, Если разделенное туннелирование определено, но разделение DNS не определено, то запросы DNS выходят через глобальный сервер DNS, который определен. Например, записи домена разделения DNS являются обязательными для внутреннего разрешения. Это поведение задокументировано в идентификатор ошибки Cisco CSCtq09624 и исправлено в Версии 2.5.4038 для клиента AnyConnect iOS Apple.

> **Примечание:** Знайте, что запросы DNS iPhone игнорируют **.local домены**. Это задокументировано в идентификатор ошибки Cisco CSCts89292. Инженеры Apple подтверждают, что проблема вызвана функциональностью ОС. Это - разработанное поведение, и Apple подтверждает, что нет никакого изменения к нему.

Дополнительные сведения

- CSCsv34395 - Добавьте поддержку в AnyConnect для проксирования FQDN к серверу DHCP
- CSCtn14578 - AnyConnect для поддержки истинного разделения DNS; не нейтрализация
- CSCtq02141 - Проблема DNS AnyConnect, когда DNS интернет-провайдера находится в

той же подсети как Общий IP

- CSCtn14578 - AnyConnect для поддержки истинного разделения DNS; не нейтрализация
- CSCtf20226 - Сделайте DNS AnyConnect w/поведением разделения туннеля для Mac то же как окна
- CSCtz86314 - Mac: запросы DNS, неправильно не передаваемые через туннель с разделением DNS
- CSCtq09624 - Сделайте DNS iPhone AnyConnect w/поведением разделенного туннелирования то же как Windows
- CSCts89292 - AC для запросов DNS iPhone игнорирует .local домены
- (межсетевой экран Cisco IOS)
- Cisco Systems – техническая поддержка и документация