# Anyconnect OpenDNS, бродящий по руководству по развертыванию модуля безопасности

## Содержание



## Введение

Этот документ описывает установку, шаги конфигурации и устранения проблем для OpenDNS (Зонтик) модуль Роуминга. Начало с AnyConnect 4.3. X, OpenDNS, Бродящий по клиенту, теперь доступен как интегрированный модуль. Это также известно как модуль Безопасности облака, и это может предварительно развернутый на оконечной точке с помощью установщика AnyConnect или может быть загружено от ASA через сеть - развертываются.

## Предварительные условия

### Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Защищенный мобильный клиент Cisco AnyConnect Secure Mobility
- OpenDNS/Umbrella Бродящий модуль
- Устройство адаптивной защиты Cisco

### Используемые компоненты

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

- Устройство адаптивной защиты Cisco (ASA) версия 9.3 (3) 7
- Защищенный мобильный клиент Cisco AnyConnect Secure Mobility 4.3.01095
- OpenDNS, Бродящий по модулю 4.3.01095
- Cisco Adaptive Security Device Manager 7.6.2 или позже
- Windows 8.1
- **Примечание:** Минимальное требование для развертывания модуля Защиты OpenDNS:
  - Версия 4.3.01095 Клиента AnyConnect VPN Client или позже
  - Cisco Adaptive Security Device Manager 7.6.2 или позже
  OpenDNS, Бродящий по модулю, в настоящее время не поддерживается на платформе Linux.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, удостоверьтесь, что вы понимаете потенциальное воздействие любых команд или конфигурации.

## Общие сведения

### Орджинфо.джсон

Для надлежащего функционирования OpenDNS, Бродящего по модулю, файл **Орджинфо.джсона** должен быть загружен от информационной панели OpenDNS или выдвинут от ASA до использования модуля. Когда файл сначала загружен, он сохранен в определенном пути в зависимости от операционной системы.

Для MAC OS X **Орджинфо.джсон** загружен к **/opt/cisco/anyconnect/Umbrella**
Для Windows **Орджинфо.джсон** загружен к ' **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella**

```
{
"organizationId" : "XXXXXXX",
"fingerprint" : "XXXXXXXXXXXXXXXXXXXXXXXXXXXX",
"userId" : "XXXXXXX"
}
```

Как показано файл использует кодирование UTF 8 и содержит organizationId, отпечаток пальца и идентификатор пользователя. Идентификатор организации представляет информацию об организации для пользователя, который в настоящее время зарегистрирован в информационную панель OpenDNS. Идентификатор организации статичен, уникален и автоматически создан OpenDNS для каждой организации. Отпечаток пальца используется для проверки файла **Орджинфо.джсона** во время регистрации

устройства, и Идентификатор пользователя представляет уникальный идентификатор для зарегистрированного пользователя.

Когда Бродящий модуль запускается на Windows, файл Орджинфо.джсона копируется к каталогу данных в каталоге Umbrella и используется в качестве рабочей копии. На MAC OS X информация от этого файла сохранена к updater.plist в каталоге данных в каталоге Umbrella. Как только модуль успешно считал информации из файла Орджинфо.джсона, это пытается зарегистрироваться в OpenDNS с помощью облачного API. Эта регистрация приводит к OpenDNS, назначающему ID уникального устройства на машину, которая делала попытку регистрации. Если идентификатор устройства от предшествующей регистрации уже доступен, устройство пропускает регистрацию.

После того, как регистрация завершена, Бродящий модуль выполняет операцию синхронизации для получения информации о политике для оконечной точки. Идентификатор устройства необходим для операции синхронизации для работы. Синхронизирующие данные включают syncInterval, добавленные в белый список домены и IP-адреса среди прочего. Синхронизирующий интервал является количеством минут, после которых модуль должен попытаться повторно синхронизировать.

## Поведение зондирования DNS

После успешной регистрации и синхронизования, Бродящий модуль передает зонды DNS к своим локальным преобразователям. Эти запросы DNS включают запросы ТЕКСТА для debug.opendns.com. На основе ответа клиент в состоянии определить, существует ли собственное Виртуальное устройство (VA) OpenDNS в сети.

Если ВА присутствует, клиентские переходы к режиму 'позади ВА', и осуществление DNS не выполнено на оконечной точке. Клиент полагается на ВА для осуществления DNS в уровне сети.

Если ВА не присутствует, клиент передает запрос DNS к общим преобразователям OpenDNS (208.67.222.222) UDP/443 использования.

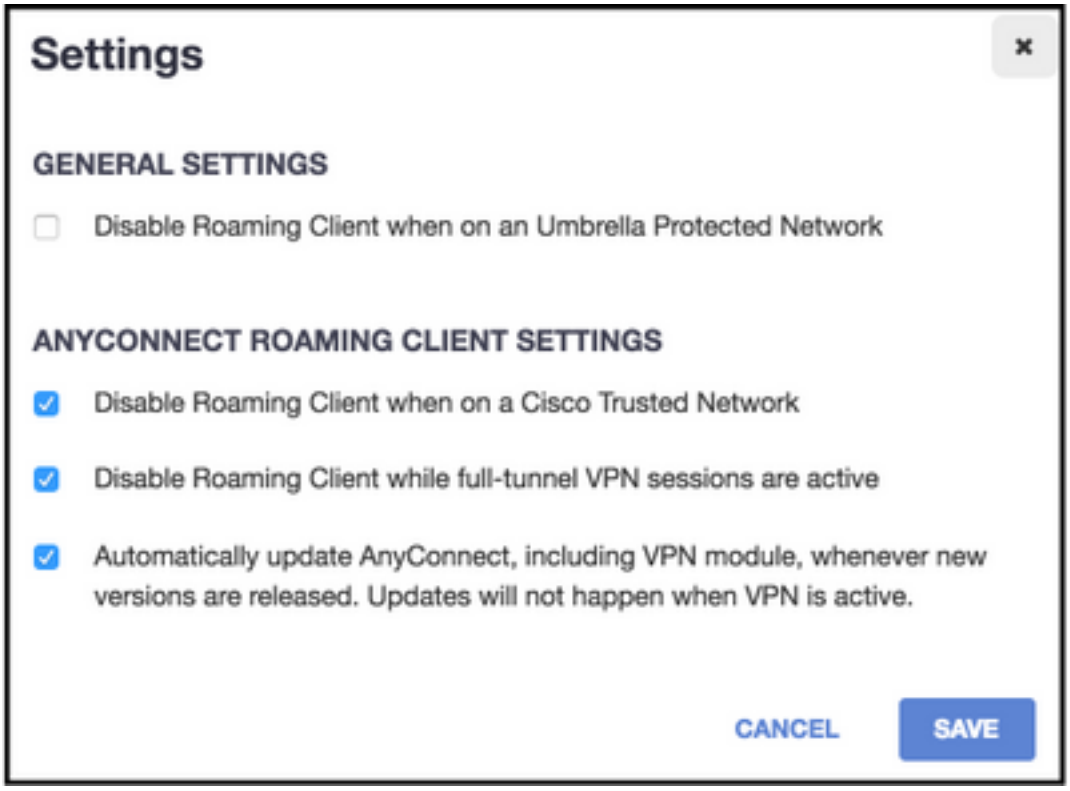
Положительный отклик указывает, что шифрование DNS возможно. Если отрицательный ответ получен, клиент передает запрос DNS к общим преобразователям OpenDNS с помощью UDP/53.

Положительный отклик к этому запросу указывает, что защита DNS возможна. Если отрицательный ответ получен, клиент повторяет запрос за несколько секунд.

После получения количества набора отрицательных ответов, клиентских переходов к открытому состоянию сбоя. Открытое состояние сбоя означает, что шифрование DNS и/или защита не возможны. Как только Бродящий модуль успешно перешел к защищенному и/или зашифрованному состоянию, все запросы DNS для областей поиска за пределами доменов локального поиска и доменов белого списка передаются преобразователям OpenDNS для разрешения имен. С зашифрованным включенным состоянием все транзакции DNS зашифрованы процессом dnscrypt.

## Поведение DNS с AnyConnect, туннелирующим режимы

### 1. Туннель - Все (или tunnel-all-DNS включил),




**Примечание:** Как показано, в то время как VPN-туннель с туннелем - вся конфигурация активен, поведение по умолчанию для Роуминга по модулю для отключения защиты DNS. Для модуля, чтобы быть активным во время туннеля AnyConnect - вся конфигурация, **Запрещать клиент роуминга, в то время как сеансы VPN полного туннеля являются активным параметром** , должен быть неконтролируем на портале OpenDNS. Способность активировать эту опцию требует усовершенствованного уровня подписки с OpenDNS. Информация ниже предполагает, что включена защита DNS через Бродящий модуль.

**Делавшая запрос доменная часть белого списка:**

Запросы DNS, которые происходят из туннельного адаптера, позволены и переданы туннельным серверам DNS через VPN-туннель. Запрос останется нерешенным, если он не может быть решен туннельными серверами DNS.

**Делавший запрос домен не часть белого списка:**

Запросы DNS, которые происходят из туннельного адаптера, позволены, и будут проксированы к общим преобразователям OpenDNS через Бродящий модуль и переданы через VPN-туннель. DNS - клиенту появится, как будто разрешение имен произошло через сервер DNS VPN. Если разрешение имен через преобразователи OpenDNS не успешно, Бродя по переключениям при отказе модуля к локально настроенным серверам DNS, начиная с адаптера VPN (который является предпочтительным адаптером, в то время как туннель подключен).

## 2. Split-DNS (tunnel-all-DNS отключенный)

**Примечание:** Все домены split-DNS автоматически добавлены к Бродящему белому

списку модуля после установки туннеля. Это сделано для обеспечения последовательного механизма обработки DNS между AnyConnect и Роумингом по модулю. Гарантируйте, что в конфигурации split-DNS (с разделением - включают туннелирование) общие преобразователи OpenDNS не включены в разделение - включают сети.

**Примечание:** На MAC OS X, 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.
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 AnyConnect 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.

**Делавшая запрос доменная часть белого списка и также часть доменов split-DNS:**

Запросы DNS, которые происходят из туннельного адаптера, позволены и переданы туннельным серверам DNS через VPN-туннель. Все другие запросы о соответствующих доменах от других адаптеров ответит драйвер AnyConnect с 'никаким таким названием' для достижения истинного split-DNS (предотвратите нейтрализацию DNS). Поэтому только нетуннельный трафик DNS защищен Бродящим модулем.

**Делавшая запрос доменная часть белого списка, но не часть доменов split-DNS:**

Запросы DNS, которые происходят из физического адаптера, позволены и переданы общим серверам DNS вне VPN-туннеля. Все другие запросы о соответствующих доменах от туннельного адаптера ответит драйвер AnyConnect с 'никаким таким названием', чтобы препятствовать тому, чтобы запрос был передан через VPN-туннель.

**Делавший запрос домен не часть белого списка или доменов split-DNS:**

Запросы DNS, которые происходят из физического адаптера, позволены и проксированы к общим преобразователям OpenDNS и переданы вне VPN-туннеля. DNS - клиенту появится, как будто разрешение имен произошло через общий сервер DNS. Если разрешение имен через преобразователи OpenDNS неуспешно, Бродя по переключениям при отказе модуля к локально настроенным серверам DNS, исключая тех настроенных на адаптере VPN. Все другие запросы о соответствующих доменах от туннельного адаптера ответит драйвер AnyConnect без такого названия, чтобы препятствовать тому, чтобы запрос был передан через VPN-туннель.

### 3. Разделение - включает, или Разделение - исключают туннелирование (никакой split-DNS и отключенный tunnel-all-DNS)

**Делавшая запрос доменная часть белого списка:**

Собственный преобразователь ОС выполняет Разрешение DNS на основе заказа адаптеров сети, и AnyConnect является предпочтительным адаптером, когда VPN активна. Запросы DNS сначала произойдут из туннельного адаптера и будут переданы туннельным серверам DNS через VPN-туннель. Если запрос не может быть решен туннельными серверами DNS, преобразователь ОС попытается решить его через общие серверы DNS.

**Делавший запрос домен не часть белого списка:**

Собственный преобразователь ОС выполняет Разрешение DNS на основе заказа адаптеров сети, и AnyConnect является предпочтительным адаптером, когда VPN активна. Запросы DNS сначала произойдут из туннельного адаптера и будут переданы туннельным серверам DNS через VPN-туннель. Если запрос не может быть решен туннельными серверами DNS, преобразователь ОС попытается решить его через общие серверы DNS.

Если общие преобразователи OpenDNS являются частью разделения - включают список или нет, часть разделения - исключает список, проксированный запрос отправлен через VPN-туннель
Если общие преобразователи OpenDNS не являются частью разделения - включают список, или часть разделения - исключают список, проксированный запрос отправлен вне VPN-туннеля

Если разрешение имен через преобразователи OpenDNS не успешно, Бродя по переключениям при отказе модуля к локально настроенным серверам DNS, начиная с адаптера VPN (который является предпочтительным адаптером, в то время как туннель подключен). Если конечный ответ, возвращенный путем Роуминга по модулю (и проксированный назад собственному DNS - клиенту), не будет успешен, то собственный клиент будет делать попытку других серверов DNS при наличии.

# Установите и настройте модуль роуминга зонтика

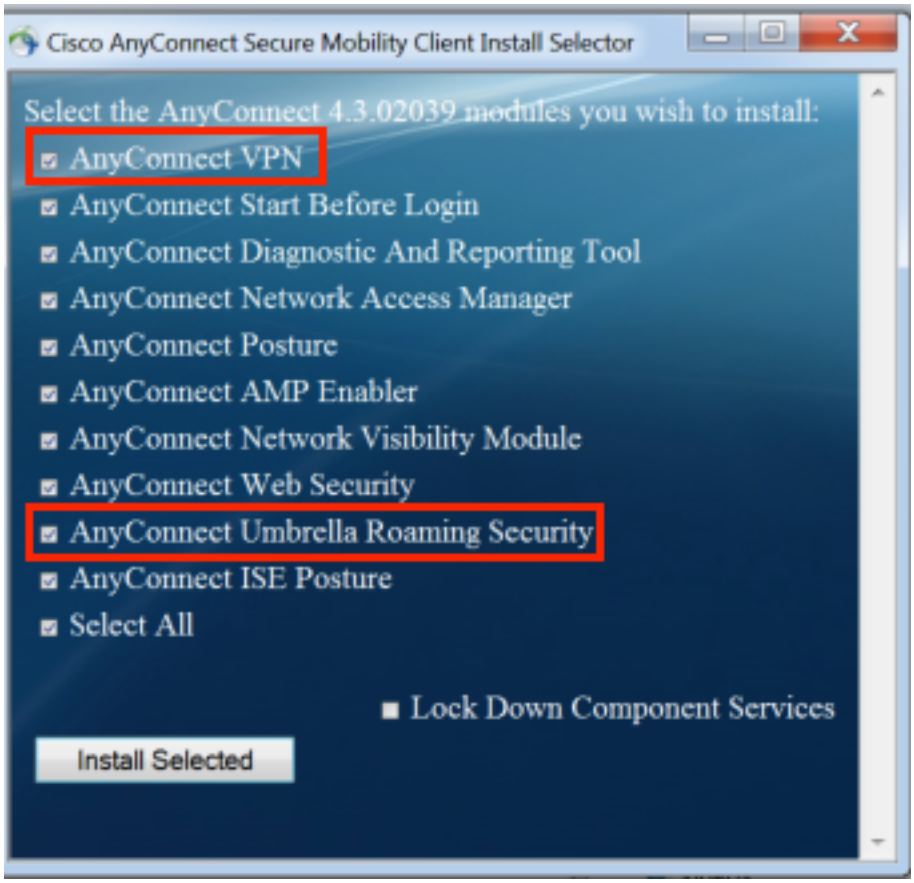
Для интеграции OpenDNS, Бродящего по модулю с Клиентом AnyConnect VPN Client, модуль должен быть установлен или через pre-deploment или через веб-метод развертываний:

## Предварительные развертывания (руководство) метод

Предварительные развертывания требуют ручной установки OpenDNS, Бродящего по модулю и копирующего файла Орджинфо.джсона на пользовательской машине. Широкомасштабные развертывания, как правило, достигаются с помощью систем управления корпоративного программного обеспечения (CM).

**Разверните OpenDNS, бродящий по модулю**

Во время AnyConnect установка пакета выбирают Anyconnect VPN и Anyconnect Umbrella Roaming Security modules:




### Развертывание Орджинфо.джсона

Загрузите файл Орджинфо.джсона путем вхождения в информационную панель OpenDNS и навигации к **Конфигурации> Личности> Бродящие Компьютеры** и Щелкните **+** знак. Прокрутите вниз и выберите **Module Profile** под **Зонтиком Anyconnect, Бродящим** по разделу **Модуля безопасности** как показано в этом образе:


Как только файл загружен, это должно быть сохраненный в этих путях в зависимости от операционной системы.

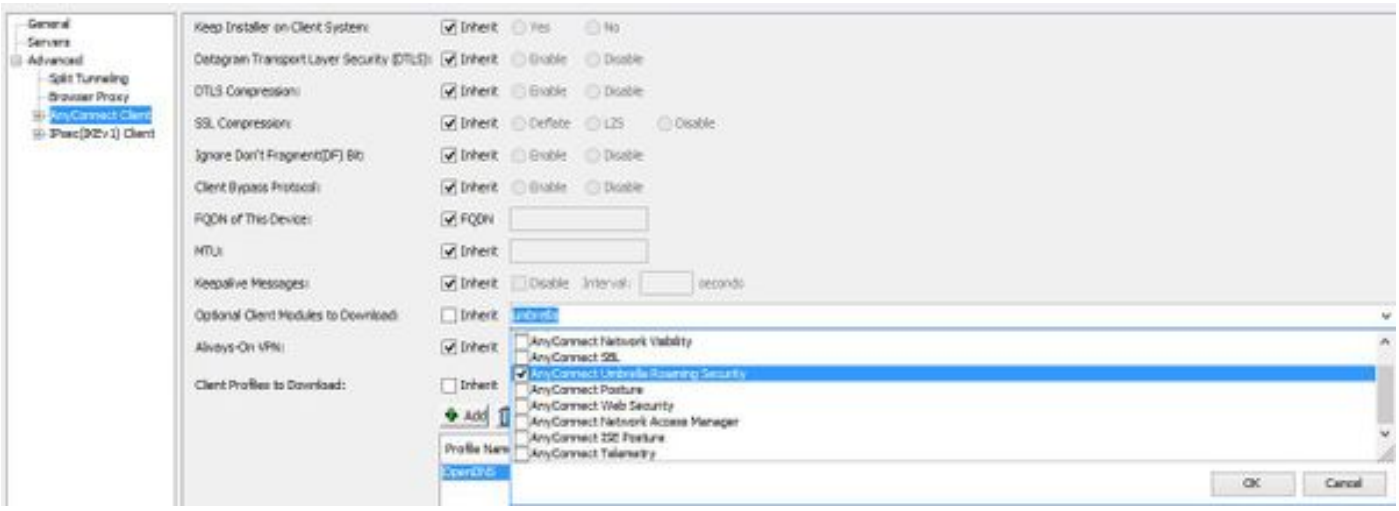
Для MAC OS X:/opt/cisco/anyconnect/Umbrella
Для Windows: C : \ProgramData\Cisco\Cisco AnyConnect безопасная мобильность Client\Umbrella

## Метод веб-развертываний

### Разверните OpenDNS, бродящий по модулю

Загрузите Клиента Мобильности Безопасности Anyconnect (например, anyconnect-win-4.3.02039-k9.pkg) пакет от Web - сайта Cisco и загрузите его к флэш-памяти ASA. После того, как загруженный, на ASDM переходят **к Групповой политике> Усовершенствованный> Клиент AnyConnect> Дополнительные Клиентские модули, чтобы Загрузить** и выбрать

Umbrella Roaming Security.

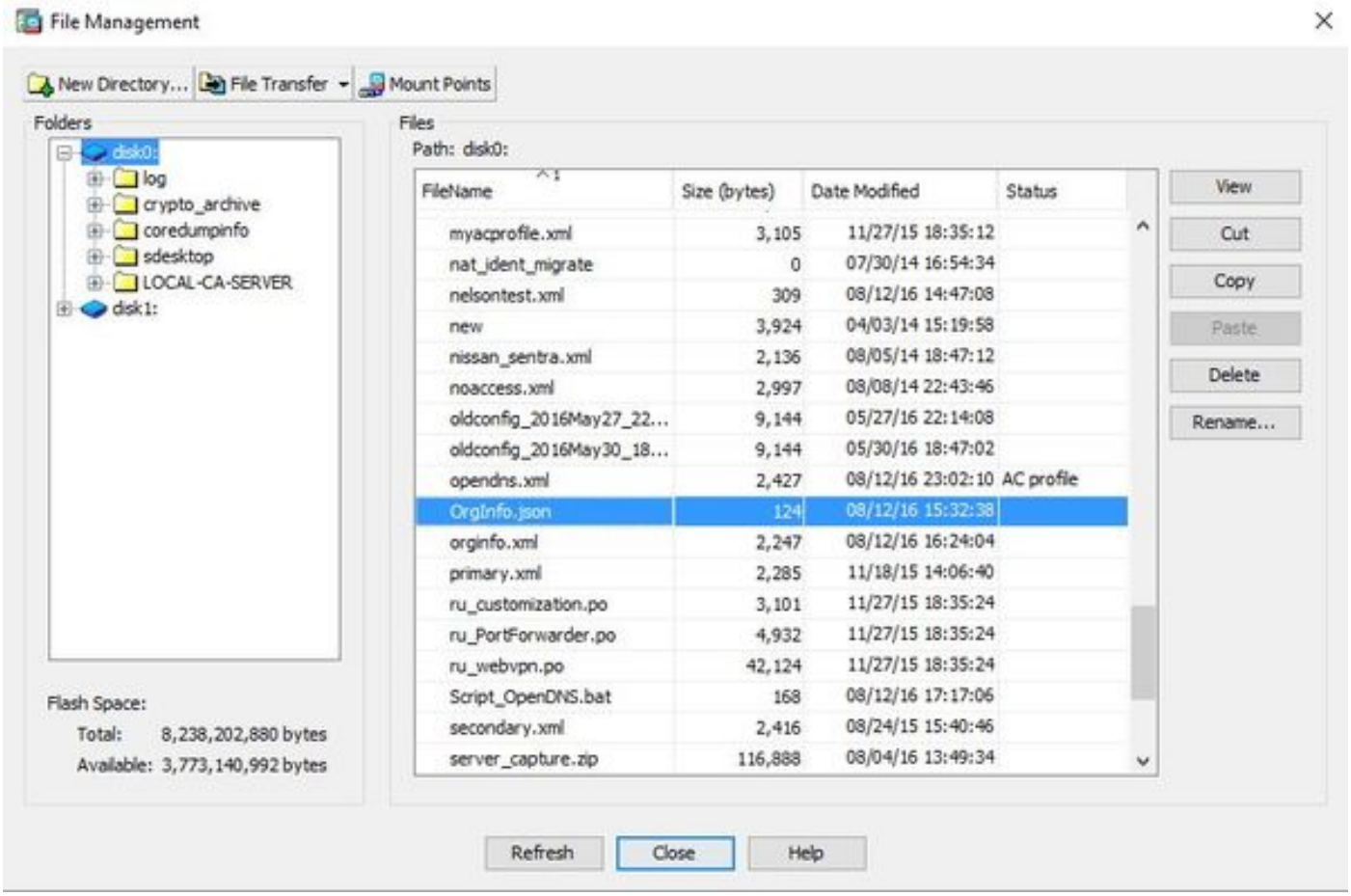



Эквивалентный CLI:

```
group-policy <Group_Policy_Name> attributes
webvpn
anyconnect modules value umbrella
```

Разверните Орджинфо.джсона

1. Загрузите файл Орджинфо.джсона от информационной панели OpenDNS и загрузите его к флэш-памяти ASA.




2. Настройте ASA для продвижения файла **Орджинфо.джсона** к удаленным оконечным точкам.

```
webvpn
```

```
anyconnect profiles OpenDNS disk0:/orginfo.json
!
!
group-policy <Group_Policy_Name> attribute
webvpn
anyconnect profiles value OpenDNS type umbrella
```

> **Примечание:** Эта конфигурация может только быть выполнена через CLI. Для использования ASDM для этой задачи, версии 7.6.2 ASDM или более поздних потребностей, которые будут установлены на ASA.

Как только клиент Роуминга Зонтика установлен с помощью одного из обсужденных методов, это должно появиться как интегрированный модуль в GUI AnyConnect как показано в этом образе


Пока **Орджинфо.джсон** не развернут на оконечной точке в корректном местоположении, модуль Роуминга Зонтика не будет инициализироваться.

# Настройка

Раздел показывает типовые фрагменты конфигурации интерфейса командой строки, необходимые для работы OpenDNS, Бродящим по модулю с различным AnyConnect, туннелирующим режимы.

```
!--- ip local pool for vpn
ip local pool vpn_pool 198.51.100.1-198.51.100.9 mask 255.255.255.224

!--- Optional NAT Hairpin configuration to reach OpenDNS servers through VPN tunnel
object network OpenDNS
subnet 198.51.100.0 255.255.255.0
nat (outside,outside) source dynamic OpenDNS interface
```

```
!
same-security-traffic permit intra-interface

!--- Global Webvpn Configuration
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.3.01095-k9.pkg 1
anyconnect profiles Anyconnect disk0:/anyconnect.xml
 anyconnect profiles OpenDNS disk0:/orginfo.json
anyconnect enable
tunnel-group-list enable

!--- split-include Configuration
access-list Split_Include standard permit <host/subnet>

group-policy OpenDNS_Split_Include internal
group-policy OpenDNS_Split_Include attributes
wins-server none
dns-server value 198.51.100.11
vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Split_Include
split-dns value <internal domains> (Optional Split-DNS Configuration)
webvpn
anyconnect profiles value AnyConnect type user
 anyconnect profiles value OpenDNS type umbrella
!
tunnel-group OpenDNS_Split_Include type remote-access
tunnel-group OpenDNS_Split_Include general-attributes
address-pool vpn_pool
default-group-policy OpenDNS_Split_Include
tunnel-group OpenDNS_Split_Include webvpn-attributes
group-alias OpenDNS_Split_Include enable


!--- Split-exclude Configuration
access-list Split_Exclude standard permit <host/subnet>

group-policy OpenDNS_Split_Exclude internal
group-policy OpenDNS_Split_Exclude attributes
wins-server none
dns-server value 198.51.100.11
vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy excludespecified
 split-tunnel-network-list value Split_Exclude
webvpn
anyconnect profiles value AnyConnect type user
 anyconnect profiles value OpenDNS type umbrella
!
tunnel-group OpenDNS_Split_Exclude type remote-access
tunnel-group OpenDNS_Split_Exclude general-attributes
address-pool vpn_pool
default-group-policy OpenDNS_Split_Exclude
tunnel-group OpenDNS_Split_Exclude webvpn-attributes
group-alias OpenDNS_Split_Exclude enable


!--- Tunnelall Configuration
group-policy OpenDNS_Tunnel_All internal
group-policy OpenDNS_Tunnel_All attributes
wins-server none
dns-server value 198.51.100.11
vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy tunnelall
```

```
webvpn
anyconnect profiles value AnyConnect type user
 anyconnect profiles value OpenDNS type umbrella
!
tunnel-group OpenDNS_Tunnel_All type remote-access
tunnel-group OpenDNS_Tunnel_All general-attributes
address-pool vpn_pool
default-group-policy OpenDNS_Tunnel_All
tunnel-group OpenDNS_Tunnel_All webvpn-attributes
group-alias OpenDNS_Tunnel_All enable
```

# Устранение неполадок

Шаги для устранения проблем связанных проблем AnyConnect OpenDNS:

1. Гарантируйте, что Модуль безопасности Роуминга Зонтика установлен наряду с Клиентом Secure Mobility Client Anyconnect
2. Гарантируйте, что Орджинфо.джсон присутствует на оконечной точке в корректном пути на основе операционной системы и находится в формате, заданном в этом документе
3. Если запросы DNS преобразователям OpenDNS предназначены, чтобы пробежаться через VPN-туннель AnyConnect, гарантировать, что шпилька настроена на ASA для разрешения достижимости преобразователям OpenDNS
4. Соберите захваты пакета (без любых фильтров) на виртуальном адаптере AnyConnect и физическом адаптере одновременно и запишите домены, которые не в состоянии решать
5. Если Бродящий модуль работает в зашифрованном состоянии, соберите захваты пакета после блокирующегося UDP 443 локально для целей устранения проблем только. Тем путем там является видимость в транзакции DNS
6. Выполните DART Anyconnect, диагностику Зонтика и запишите время Ошибки DNS:

Сбор DART: https://supportforums. cisco . com/document/12747756/how-collect-dart-bundle-anyconnect

7. Соберите журналы диагностики Зонтика и передайте получающийся URL своему администратору OpenDNS. Только у вас и администратора OpenDNS есть доступ к этой информации.

Для Windows: C : файлы \Program (x86) \Cisco\Cisco AnyConnect безопасная мобильность Client\UmbrellaDiagnostic.exe

Для MAC OSX:/opt/cisco/anyconnect/bin/UmbrellaDiagnostic

# Связанные дефекты

CSCvb34863: Задержка в решении DNS, когда AnyConnect, настроенный для разделения - включают туннелирование