ASA и собственный пример конфигурации клиента Android IPSEC L2TP

Содержание

Введение

Протокол туннелирования уровня 2 (L2TP) через IPSec предоставляет возможность развернуть и администрировать решение для VPN L2TP вместе с IPSEC VPN и сервисами межсетевого экрана в одной платформе. Основное преимущество конфигурации L2TP по IPSec в сценарии удаленного доступа - то, что удаленные пользователи могут обратиться к VPN по общедоступной IP - сети без шлюза или выделенной линии, которая включает удаленный доступ от фактически любого места с PlainOld Telephone Service (POTS) (обычная телефонная сеть). Дополнительное преимущество - то, что единственное клиентское требование для доступа VPN является использованием Windows с Microsoft Dial-Up Networking (DUN). Никакое дополнительное клиентское программное обеспечение, такое как Клиентское программное обеспечение Cisco VPN, не требуется.

В этом документе приведен пример конфигурации для клиента l2tp-IPSec, работающего в собственном (native) режиме на платформе Android. Это берет вас посредством всех необходимых команд, требуемых на устройстве адаптивной защиты Cisco (ASA), а также шаги, которые будут взяты на самом устройстве на базе Android.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- L2TP/IPSec Android требует версии программного обеспечения 8.2.5 Cisco ASA или позже, версия 8.3.2.12 или позже или версия 8.4.1 или позже.
- Когда протокол L2TP/IPSec используется, ASA поддерживает поддержку подписи сертификата Защищенного алгоритма хэширования 2 (SHA2) Microsoft Windows 7 и собственные Android клиенты VPN.
- Посмотрите, что руководство по настройке Cisco ASA 5500 использует CLI, 8.4 и 8.6: L2TP Настройки по IPSec: Требования при лицензировании для L2TP по IPSec.

Данные для документа были получены в специально созданных лабораторных условиях. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если используемая сеть является действующей, убедитесь в понимании возможного влияния любой из применяемых команд.

Настройка

В этом разделе описываются информацию, в которой можно было бы нуждаться для настройки функций, описанных в этом документе.

Настройте Соединение L2TP/IPSec на Android

Эта процедура описывает, как настроить соединение L2TP/IPSec на Android:

1. Откройте меню и выберите **Settings**.
2. Выберите **Wireless и Network** или **Wireless Controls**. Доступный параметр зависит от вашей версии Android.
3. Выберите **VPN Settings**.
4. Выберите **Add VPN**.
5. Выберите **Add L2TP/IPsec PSK VPN**.
6. Выберите **VPN Name** и введите описательное имя.
7. Выберите **Set VPN Server** и введите описательное имя.
8. Выберите **предварительный общий ключ Set IPSec**.
9. Анчек **Включают тайну L2TP**.
10. [Дополнительный] Набор идентификатор IPSec как имя группы туннелей ASA. Никакая установка не означает, что это попадет в DefaultRAGroup на ASA.
11. Откройте меню и выберите **Save**.

Настройте Соединение L2TP/IPSec на ASA

Это требуемая Версия 1 (IKEv1) Обмена ключами между сетями ASA (интернет-Сопоставление безопасности и Протокол управления ключами [ISAKMP]) параметры настройки политики, которые позволяют собственным клиентам VPN, интегрированным с операционной системой на оконечной точке, для создания VPN-подключения к ASA, когда используется L2TP по Протоколу IPSec:

- Фаза 1 IKEv1 - шифрование Стандарта тройного шифрования данных (3DES) с SHA1 хеширует метод
- Фаза IPSec 2 - 3DES или шифрование Расширенного стандарта шифрования (AES) с алгоритмом представления сообщения в краткой форме 5 (MD5) или SHA хеширует метод
- Проверка подлинности PPP - Протокол аутентификации пароля (PAP), Версия протокола 1 квитирования с аутентификацией Microsoft (MSCHAPv1) или MSCHAPv2 (предпочтены)
- Pre-shared-key *

Примечание: ASA поддерживает только PAP проверок подлинности PPP и MS-CHAP (версии 1 и 2) на локальной базе данных. Протокол EAP и CHAP выполнены по доверенности серверы проверки подлинности. Поэтому, если удаленный пользователь будет принадлежать туннельной группе, настроенной с **опознавательными** или **опознавательными** командами **парня прокси eap** и если ASA будет настроен для использования локальной базы данных, то тот пользователь будет неспособен соединиться.

Кроме того, Android не поддерживает PAP и, потому что Протокол LDAP не поддерживает MS-CHAP, LDAP не является механизмом допустимой аутентификации. Единственный обходной путь должен использовать RADIUS. Посмотрите идентификатор ошибки Cisco CSCtw58945, "L2TP по IP - безопасным соединениям отказывает с авторизацией ldap и mschapv2", для получения дальнейшей информации по проблемам с MS-CHAP и LDAP.

Эта процедура описывает, как настроить соединение L2TP/IPSec на ASA:

1. Определите пул локального адреса или используйте dhcp-server для устройства адаптивной безопасности для выделения IP-адресов клиентам для групповой политики.
2. Создайте внутреннюю групповую политику. Определите протокол туннелирования, чтобы быть l2tp-ipsec.Настройте сервер доменных имен (DNS), который будет использоваться клиентами.
3. Создайте новую туннельную группу или модифицируйте атрибуты существующего DefaultRAGroup. (Новая туннельная группа может использоваться, если идентификатор IPSec установлен как group-name по телефону; посмотрите шаг 10 для конфигурации телефона.)
4. Определите общие атрибуты туннельной группы, которые используются. Сопоставьте политику определенной группы с этой туннельной группой.Сопоставьте определенный пул адресов, который будет использоваться этой туннельной группой.Модифицируйте группу сервера аутентификации, если вы хотите использовать что-то другое, чем ЛОКАЛЬНЫЙ.
5. Определите предварительный общий ключ под атрибутами IPSec туннельной группы, которая будет использоваться.
6. Модифицируйте атрибуты PPP туннельной группы, которые используются так, чтобы только использовались парень, v1 парня мс и ms-chap-v2.
7. Создайте набор преобразований с определенным типом шифрования безопасного закрытия полезной нагрузки (ESP) и типом проверки подлинности.
8. Дайте IPSEC команду использовать транспортный режим, а не туннельный режим.

9. Определите политику ISAKMP/IKEv1 с помощью шифрования 3DES с методом хэша SHA1.
10. Создайте динамическую криптокарту и сопоставьте ее с криптокартой.
11. Примените криптокарту к интерфейсу.
12. Включите ISAKMP на том интерфейсе.

Команды файла конфигурации для совместимости ASA

> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Данный пример показывает команды файла конфигурации, которые гарантируют совместимость ASA собственным клиентом VPN на любой операционной системе.

ASA 8. 2.5 или более поздний пример конфигурации

```
Username <name> password <passwd> mschap
ip local pool l2tp-ipsec_address 192.168.1.1-192.168.1.10
group-policy l2tp-ipsec_policy internal
group-policy l2tp-ipsec_policy attributes
           dns-server value <dns_server>
           vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
           default-group-policy l2tp-ipsec_policy
           address-pool l2tp-ipsec_address
tunnel-group DefaultRAGroup ipsec-attributes
           pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
           no authentication pap
           authentication chap
           authentication ms-chap-v1
           authentication ms-chap-v2
crypto ipsec transform-set trans esp-3des esp-sha-hmac
crypto ipsec transform-set trans mode transport
crypto dynamic-map dyno 10 set transform-set set trans
crypto map vpn 65535 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto isakmp enable outside
crypto isakmp policy 10
           authentication pre-share
           encryption 3des
           hash sha
           group 2
           lifetime 86400
```

ASA 8. 3.2.12 или более поздний пример конфигурации

```
Username <name> password <passwd> mschap
ip local pool l2tp-ipsec_address 192.168.1.1-192.168.1.10
group-policy l2tp-ipsec_policy internal
group-policy l2tp-ipsec_policy attributes
           dns-server value <dns_server>
           vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
           default-group-policy l2tp-ipsec_policy
```

```
          address-pool l2tp-ipsec_addresses
tunnel-group DefaultRAGroup ipsec-attributes
          pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
          no authentication pap
          authentication chap
          authentication ms-chap-v1
          authentication ms-chap-v2
crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
crypto dynamic-map dyno 10 set ikev1 transform-set my-transform-set-ikev1
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
          authentication pre-share
          encryption 3des
          hash sha
          group 2
          lifetime 86400
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Эта процедура описывает, как установить соединение:

1. Откройте меню и выберите **Settings**.
2. Выберите **Wireless и Network** или **Wireless Controls**. (Доступный параметр зависит от вашей версии Android.)
3. Выберите конфигурацию VPN из списка.
4. Введите имя пользователя и пароль.
5. Выберите **имя пользователя Remember**.
6. Выберите **Connect**.

Эта процедура описывает, как разъединить:

1. Откройте меню и выберите **Settings**.
2. Выберите **Wireless и Network** или **Wireless Controls**. (Доступный параметр зависит от вашей версии Android.)
3. Выберите конфигурацию VPN из списка.
4. Выберите **Disconnect**.

Используйте эти команды, чтобы подтвердить, что ваше соединение работает должным образом.

- **покажите выполненного crypto isakmp** - Для версии ASA 8.2.5
- **покажите выполненный крипто-ikev1** - Для версии ASA 8.3.2.12 или позже
- **покажите vpn-sessiondb ra-ikev1-ipsec -** Для версии ASA 8.3.2.12 или позже
- **удаленный покажите vpn-sessiondb -** Для версии ASA 8.2.5

  Примечание: Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Известные предупреждения

- Идентификатор ошибки Cisco CSCtq21535, "обратная трассировка ASA при соединении с L2TP/КЛИЕНТОМ IPSEC Android"
- CSCtj57256 идентификатора ошибки Cisco, "соединение L2TP/IPSec от Android не устанавливает к ASA55xx"
- CSCtw58945 идентификатора ошибки Cisco, "L2TP по IP - безопасным соединениям отказывает с авторизацией ldap и mschapv2"

Дополнительные сведения

- Руководство по настройке Cisco ASA 5500 с помощью CLI, 8.4 и 8.6: L2TP Настройки по IPsec
- Комментарии к выпуску для серии 5500 Cisco ASA, версии 8.4 (x)
- Руководство по настройке Cisco ASA 5500 с помощью CLI, 8.3: информация о NAT
- ASA пред8.3 к 8.3 примерам конфигурации NAT
- Cisco Systems – техническая поддержка и документация