Общие сведения о VPDN (виртуальная частная коммутируемая сеть)

Содержание

Введение

Виртуальная частная сеть удаленного доступа (VPDN) позволяет службе дозвона частной сети развертываться по серверам удаленного доступа (определяется как концентратор доступа L2TP [LAC]).

Когда клиент Протокола PPP набирает в LAC, LAC решает, что должен передать тот сеанс PPP на L2TP Network Server (LNS) для того клиента. Затем LNS аутентифицирует пользователя и начинает согласование PPP. После завершения установки PPP все кадры передаются через LAC клиенту и в LNS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Глоссарий

- **Клиент:** ПК или маршрутизатор подключили к сети удаленного доступа, которая является инициатором вызова.
- **L2TP**: Протокол туннелирования 2-го уровня. PPP определяет механизм инкапсуляции для переноса многопротокольных пакетов через уровень 2 (L2) каналы типа точка-точка. Как правило, пользователь получает соединение L2 с Сервером доступа к сети (NAS) с помощью способа, такого как коммутируемый PlainOld Telephone Service (POTS) (обычная телефонная сеть), ISDN или Ассиметричная цифровая абонентская линия (ADSL). Затем пользователь запускает PPP через это соединение. В такой конфигурации оконечная точка соединения L2 и оконечная точка сеанса PPP находятся на том же физическом устройстве (NAS).L2TP расширяет модель PPP, позволяя конечным точкам L2 и PPP размещаться на нескольких устройствах, взаимосвязанных по сети. С L2TP у пользователя есть соединение L2 с концентратором доступа, и концентратор тогда туннелирует отдельные кадры PPP к NAS. Это разрешает фактическую обработку пакетов PPP, отделенных от оконечного устройства схемы L2.
- **L2F:** Протокол пересылки 2-го уровня. L2F – это более старый туннельный протокол, чем L2TP.
- **LAC**: Концентратор доступа L2TP. Узел, который действует как одна сторона оконечной точки туннеля L2TP и является узлом к LNS. LAC находится между LNS и клиентом и передает пакеты к и от каждого. Пакеты, посланные с LAC на LNS, требуют туннелирования с протоколом L2TP. Соединение от LAC до клиента, как правило, через ISDN или аналог.
- **LNS:** L2TP Network Server. Узел, выступающий в роли одной стороны туннеля L2TP и являющийся одноранговым узлом для LAC. LNS – логическая оконечная точка сеанса PPP, туннелируемого от клиента с помощью LAC.
- **Домашний шлюз:** Такое же определение, как для LNS в терминологии L2F.
- **NAS:** Такое же определение, как для LAC в терминологии L2F.
- **Туннель**: В терминологии L2TP туннель существует между парой LAC-LNS. Туннель состоит из контрольного соединения, одного, нескольких или ни одного сеанса L2TP. Туннель передает инкапсулированные датаграммы PPP и сообщения управления между LAC и LNS. Процесс тот же самый для L2F.
- **Сеанс**: L2TP является ориентированным на соединение. LNS и LAC поддерживают состояние каждого вызова, инициированного или обработанного LAC. Запущен сеанс L2TP между LAC и LNS, если создано сквозное соединение PPP между клиентом и LNS. Дейтаграммы, связанные с PPP-соединением, посылаются по туннелю между LAC и LNS. Между установленными сеансами L2TP и их связанными вызовами существует взаимоотношение "один к одному". Процесс тот же самый для L2F.

Обзор процесса VPDN

В описании процесса VPDN используются термины L2TP (LAC и LNS).

1. Клиент вызывает LAC (как правило, использующий модем или плату ISDN).
2. Клиент и LAC начинают фазу PPP, согласуя параметры LCP (метод аутентификации с помощью протоколов PAP (протокола аутентификации с помощью пароля) или CHAP (протокола аутентификации с предварительным согласованием вызова), протокола PPP multilink, сжатия и т.д.).
3. Предположим, что согласование CHAP прошло успешно на этапе 2. Концентратор доступа по протоколу L2TP отправляет клиенту сообщение CHAP Challenge.
4. LAC получает ответ (например, имя_пользователя@имя_домена и пароль).
5. Основанный на доменном имени, полученном в отклике CHAP или DNIS, полученном в сообщении настройки ISDN, LAC проверяет, является ли клиент пользователем VPDN. Это делает это при помощи своей локальной конфигурации VPDN или контакта с аутентификацией, авторизацией и учетом (AAA).
6. Поскольку клиент является пользователем VPDN, LAC получает некоторую информацию (от ее локальной конфигурации VPDN или от AAA-сервера), что это использует для внедрения L2TP или туннеля L2F с LNS.
7. LAC переводит в рабочее состояние L2TP или туннель L2F с LNS.
8. Основанный на имени, полученном в запросе от LAC, LNS проверяет, разрешено ли LAC открыть туннель (LNS проверяет его локальную конфигурацию VPDN). Кроме того, LAC и LNS аутентифицируют друг друга (используя свою локальную базу данных или обращаясь к серверу AAA). Тогда между обоими устройствами открыт Туннель. В этом туннеле могут выполняться несколько сеансов VPDN.
9. Для клиента username@DomainName запускается сеанс VPDN от LAC к LNS. На одного пользователя один сеанс VPDN.
10. Концентратор LAC пересылает согласованные с клиентом параметры LCP серверу LNS вместе со следующими полученными от клиента данными: имя_пользователя@имя_домена и пароль.
11. LNS клонирует виртуальный доступ из виртуального шаблона, указанного в конфигурации VPDN. Сервер LNS принимает параметры протокола LCP, полученные от концентратора LAC и выполняет аутентификацию клиента локально или путем подключения к серверу AAA.
12. LNS передает ответ CHAP клиенту.
13. IP Control Protocol (IPCP), фаза выполнена и затем маршрут, установлен: сеанс PPP установлен между клиентом и LNS. Концентратор LAC просто перенаправляет PPP-кадры. кадры PPP туннелированы между LAC и LNS.

Протоколы туннелирования

Туннель VPDN может быть создан с помощью или Передачи уровня 2 (L2F) или Протокола туннелирования уровня 2 (L2TP).

- L2F был представлен Cisco в RFC 2341 и также использовался для пересылки сеансов PPP многоблочному мультиканальному протоколу PPP.
- L2TP, внесенный в RFC 2661, сочетает лучшие свойства протокола L2F от Cisco и протокола туннельного соединения типа точка-точка (PPTP) от Microsoft. Более того, L2F поддерживает только VPDN на входящих вызовах, вто время как L2TP поддерживает VPDN и на входящих, и на исходящих вызовах.

Оба протокола используют порт UDP 1701 для создания туннеля через IP-сеть для пересылки кадров канального уровня. Для L2TP настройка для туннелирования сеанса PPP

состоит из двух шагов:

1. Установление туннеля между LAC и LNS. Этот этап осуществляется только когда между двумя устройствами нет активного туннеля.
2. Установление сеанса связи между LAC и LNS.

Концентратор доступа по протоколу L2TP (LAC) решает, что необходимо создать туннель от него до LNS.

1. LAC отправляет запрос SCCRQ (Start-Control-Connection-Request). Запрос вызова CHAP и пары значение-атрибут включены в это сообщение.
2. LNS отвечает Start-Control-Connection-Reply (SCCRP). Данное сообщение содержит вызов CHAP, ответ на вызов LAC и AV Pairs.
3. LAC посылает сообщение Start-Control-Connection-Connected (SCCCN). В этом сообщении содержится ответ CHAP.
4. LNS отвечает подтверждением нулевой длины (ZLB ACK). Такое подтверждение может содержаться в другом сообщении. Туннель находится в рабочем состоянии.
5. LAC посылает на LNS запрос на входящий вызов (ICRQ).
6. LNS отвечает сообщением ответа входящего вызова (ICRP).
7. LAC отправляет ICCN (Incoming-Call-Connected).
8. LNS окликается ZLB ACK. Это подтверждение приема также может быть доставлено в другом сообщение.
9. Сеанс находится в рабочем состоянии.

Примечание: Сообщения выше используемого для открытия туннеля или сеанса несут Пары значений атрибутов (AVP), определенные в RFC 2661. Они описывают свойства и информацию (такие как Bearercap, имя хоста, имя поставщика и размер окна). Некоторые пары значений атрибутов обязательны, а некоторые опциональны.

Примечание: Туннельный ID используется, чтобы мультиплексировать и демультиплексировать туннели между LAC и LNS. Идентификатор сеанса используется для отождествления конкретного сеанса с данным туннелем.

Для L2F настройка для туннелирования сеанса PPP совпадает с для L2TP. Он предполагает следующие действия:

1. Установление туннеля между NAS и базовым шлюзом. Этот этап осуществляется только когда между двумя устройствами нет активного туннеля.
2. Установление сеанса между NAS и домашним шлюзом.

Сервер NAS определяет, что должно быть инициировано туннельное соединение от сервера NAS к домашнему шлюзу.

1. NAS посылает L2F_Conf домашнему шлюзу. Это сообщение содержит значение CHAP Challenge.
2. Домашний шлюз отвечает L2F_Conf. Это сообщение содержит значение CHAP Challenge.
3. NAS отправляет L2F_Open. В это сообщение включается ответ CHAP на запрос домашнего шлюза.
4. Домашний шлюз отвечает L2F_Open. Ответ CHAP проблемы NAS включен в это сообщение. Туннель находится в рабочем состоянии.
5. NAS передает L2F_Open к Домашнему шлюзу. Пакет включает имя пользователя

клиента (client_name), вызов CHAP, отправленный от NAS клиенту (challenge_NAS) и его ответ (response_client).

6. Домашний шлюз принимает клиента, отправляя обратно сообщение L2F_OPEN. Теперь трафик может свободно проходить в любом направлении между клиентом и домашним шлюзом.

Примечание: Туннель определен с CLID (Идентификатор клиента). Multiplex ID (MID) определяет определенное соединение в туннеле.

Настройка виртуальной частной коммутируемой сети (VPDN)

Для получения информации о настройке VPDN обратитесь к руководству Виртуальных частных сетей Настройки и перейдите к разделу по VPN Настройки.

Дополнительные сведения

- Набор номера и страницы поддержки технологий доступа
- Cisco Systems – техническая поддержка и документация