Принципы работы частных виртуальных сетей

Содержание

Введение

Данный документ охватывает основы виртуальных частных сетей (VPN), а именно: основные компоненты, технологии VPN, туннелирование и безопасность VPN.

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.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

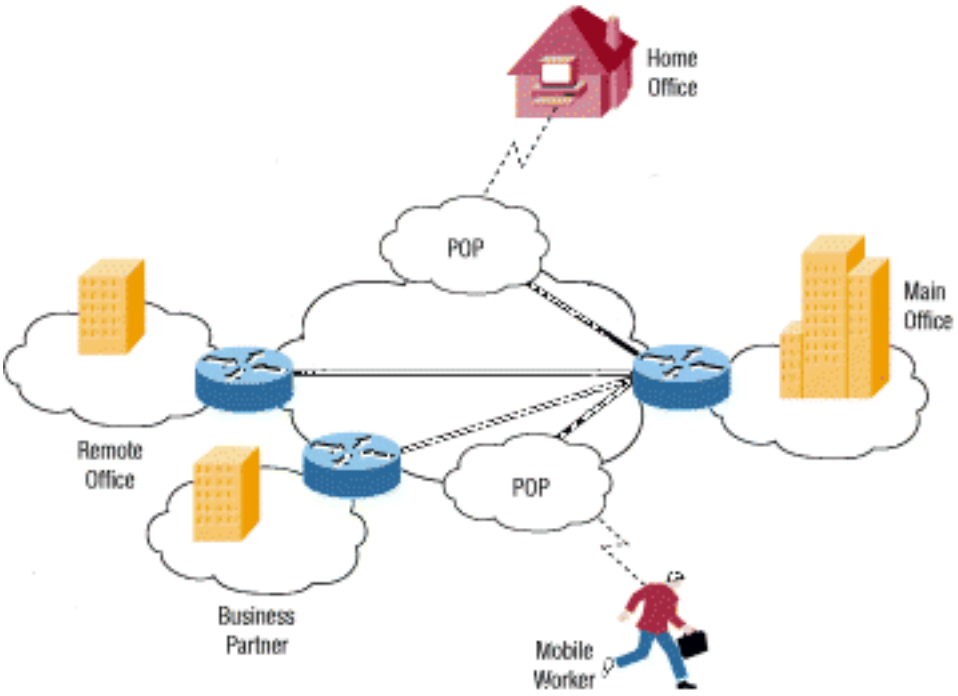
Общие сведения

За последние пару десятилетий в мире многое изменилось. Вместо простых деловых отношений с местными или региональными филиалами, многие компании сейчас вынуждены думать о глобальных рынках и логистике. Филиалы многих компаний

распределены по всей стране и даже по всему миру. Однако все компании нуждаются в одном: способе поддержания быстрого, безопасного и надежного обмена информацией, независимо от местонахождения своих офисов.

До недавнего времени надежная связь означала использование выделенных линий для поддержания глобальной сети (WAN). Выделенные линии от цифровой сети связи с комплексными услугами (ISDN, поддерживает передачу данных со скоростью 144 кбит/с) до оптоволоконной линии связи Optical Carrier-3 (OC3, поддерживает передачу данных со скоростью 155 мбит/с) предоставляют компаниям способ расширения своих частных сетей за пределы своего географического региона. WAN имеет очевидные преимущества по сравнению с сетью общего пользования, например Интернетом, в отношении надежности, быстродействия и безопасности; однако поддержание WAN, особенно при использовании выделенных линий, может оказаться очень дорогостоящим (как правило стоимость зависит от расстояния между филиалами). Кроме того, выделенные линии не являются эффективным решением для организаций, сотрудники которых большую часть времени проводят в разъездах (например маркетинговый персонал) и часто могут испытывать потребность в удаленном подключении к корпоративной сети для доступа к конфиденциальным данным.

По мере распространения Интернета организации обратились к этой общедоступной сети как средству расширения своих собственных сетей. Сначала появились интрасети, спроектированные на основе узлов, для использования только сотрудниками компании. Теперь многие компании создают свои собственные виртуальные частные сети (VPN) для удовлетворения потребностей удаленных сотрудников и региональных отделений.



Типичная VPN может состоять из главной локальной сети (LAN), находящейся в главном офисе компании, других LAN, находящихся в удаленных офисах или производственных филиалах, и отдельных пользователей, подключающихся к сети на своем месте.

VPN — это частная сеть, использующая сеть общего пользования (как правило Интернет) для обмена данными между удаленными узлами и пользователями. Вместо использования специального реального соединения, например выделенной линии, VPN использует "виртуальные" соединения, маршрутизируемые через Интернет из частной сети компании к

удаленному узлу или сотруднику.

Особенности VPN?

Существуют сети VPN двух общих типов.

- **Удаленный доступ—Также называется виртуальной частной сетью удаленного доступа (VPDN), это соединение между пользователем и LAN, используемое компанией, сотрудникам которой требуется подключение к частной сети из различных удаленных мест.** Как правило, корпорация при создании большой сети VPN удаленного доступа в некоторой форме предоставляет своим пользователям учетную запись удаленного подключения через Интернет с помощью поставщика услуг Интернета. После этого удаленные пользователи могут набрать номер 1-800 для выхода в Интернет и использовать свое клиентское ПО VPN для доступа к корпоративной сети. Наглядным примером компании, нуждающейся в сети VPN удаленного доступа, может служить большая фирма, в штате которой сотни торговых агентов, находящихся в разных местах. Сети VPN удаленного доступа обеспечивают безопасное соединение с шифрованием между частной сетью компании и удаленными пользователями через стороннего поставщика услуг.
- **Сеть-сеть—Используя специализированное оборудование и крупномасштабное шифрование, компания может объединить множество фиксированных узлов через сеть общего пользования, например Интернет.** Каждому узлу требуется только локальное подключение к той же общедоступной сети — это позволяет не тратить средства на протяженные частные выделенные линии. Сети VLAN типа "сеть-сеть" можно еще разделить на интрасети и экстрасети. Сеть VLAN типа "сеть-сеть", проложенную между офисами одной компании, называют интрасетью VPN, а проложенную для соединения компании со своим партнером или клиентом, называют экстрасетью VPN.

Эффективно спроектированная сеть VLAN может обеспечить компании значительные преимущества. Например:

- Расширение взаимодействия между различными географическими регионами
- Уменьшение эксплуатационных расходов по сравнению с традиционными WAN
- Сокращение транзитного времени и дорожных расходов для удаленных пользователей
- Повышение производительности
- Упрощение топологии сети
- Обеспечение возможности взаимодействия через глобальную сеть
- Обеспечение поддержки удаленных сотрудников
- Более быстрая отдача на инвестиции (ROI) по сравнению с традиционной WAN

Возможности, которые должна предоставлять эффективно спроектированная VPN? Сеть VPN должна обладать следующим:

- Безопасность
- Надежность
- Масштабируемость
- Управление сетью
- Управление политиками

Аналогия: Каждая ЛВС как остров

Представьте, что вы живете на острове посреди огромного океана. Вокруг вас разбросаны тысячи других островов, одни из них находятся ближе другие дальше. Обычный способ перемещения — это воспользоваться переправой между вашим островом и тем островом, куда нужно попасть. Перемещение переправой означает, что у вас практически отсутствует секретность. Все что вы делаете может увидеть кто-либо другой.

Проведем следующую аналогию: каждый остров представляет частную LAN, а океан — это Интернет. Перемещение переправой аналогично подключению к веб-серверу или другому устройству через Интернет. Вы не контролируете провода и маршрутизаторы, составляющие Интернет, это подобно отсутствию контроля над другими людьми, находящимися на средстве переправы. Это оставляет вас беззащитным перед проблемами с безопасностью при попытке установить соединение между двумя частными сетями, используя общий ресурс.

Ваш остров решает навести мост с другим островом, чтобы появился более легкий, безопасный и прямой путь для перемещения людей между островами. Наведение и содержание моста — дорогостоящая процедура, даже если эти острова находятся на очень близком расстоянии один от другого. Однако потребность в надежном и безопасном пути настолько велика, что вы решаетесь на этот шаг. Ваш остров хотел бы соединиться со вторым островом, который находится гораздо дальше первого, но вы решаете, что это слишком дорого.

Возникновение такой ситуации очень вероятно при использовании выделенной линии. Мосты (выделенные линии) отделены от океана (Интернет) и при этом они способны соединять острова (LAN). Многие компании выбрали этот путь из-за потребности в безопасной и надежной связи между своими удаленными офисами. Однако, если офисы находятся на очень большом расстоянии один от другого, стоимость может оказаться чрезмерно высокой — это подобно ситуации, когда нужно возводить очень длинный мост.

Какое место VPN занимает в этой аналогии? Каждому обитателю таких островов можно предоставить свою собственную небольшую подводную лодку, обладающую следующими свойствами.

- Быстрота.
- Легкое управление в нужном направлении.
- Полная невидимость для остальных средств переправы и подводных лодок.
- Надежность.
- После приобретения первой подводной лодки, стоимость приобретения дополнительных субмарин становится небольшой.

Хотя они плавают в океане вместе с остальными лодками, обитатели двух островов могут перемещаться туда и обратно в любое время, сохраняя секретность и безопасность. Именно в этом и заключается сущность функционирования VPN. Каждый удаленный пользователь вашей сети может взаимодействовать безопасным и надежным способом, используя Интернет в качестве среды для подключения к частной LAN. VPN гораздо легче расширяется добавлением новых пользователей и различных расположений чем выделенная линия. На самом деле, масштабируемость — это основное преимущество VPN в сравнении с типичными выделенными линиями. В отличие от выделенных линий, где стоимость возрастает прямо пропорционально протяженности соединения, географическое расположение каждого офиса имеет меньшее значение при создании VPN.

Технологии VPN

В эффективно спроектированной VPN используются несколько методов обеспечения безопасности соединения и данных.

- **Секретность данных — Вероятно, это наиболее важная особенность любой реализации VPN.** Поскольку ваши личные данные передаются через сеть общего пользования, секретность данных крайне необходима и может быть обеспечена шифрованием этих данных. Этот процесс подразумевает шифрование всех данных, отправляемых одним компьютером другому в такой форме, что только другой компьютер способен будет их расшифровать.Большинство сетей VPN используют один из следующих протоколов для шифрования.**IPsec — Набор протоколов (IPsec) для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, предоставляет средства повышения безопасности, такие как алгоритмы более устойчивого шифрования и более полную аутентификацию.** IPsec имеет два режима шифрования: транспортный и туннельный. В туннельном режиме шифруются заголовок и полезные данные каждого пакета, а в транспортном — только полезные данные. Преимуществами этого протокола могут воспользоваться только системы, совместимые с IPsec. Кроме того все устройства должны использовать один общий ключ или сертификат и иметь сходным образом настроенные политики безопасности.Пользователям сети VPN удаленного доступа некоторые пакеты ПО сторонних разработчиков обеспечивают подключение и шифрование на ПК пользователей. IPsec поддерживает шифрование с 56-битным ключом (DES) или с 168-битным ключом (тройной DES).**PPTP/MPPE — Протокол туннелирования между узлами (PPTP) был создан консорциумом PPTP Forum таких компаний как US Robotics, Microsoft, 3COM, Ascend и ECI Telematics.** PPTP поддерживает многопротокольные VPN с шифрованием 40-битным и 128-битным ключом, используя протокол шифрования данных от Microsoft (MPPE). Важно помнить, что протокол PPTP сам по себе не обеспечивает шифрование данных.**L2TP/IPsec — Как правило, его называют протоколом L2TP через IPsec. Он обеспечивает безопасность протокола IPsec при туннелировании по сетевому протоколу туннелирования канального уровня (L2TP).** L2TP — это продукт совместной работы членов PPTP forum, Cisco и инженерной группы по развитию Интернета (IETF). Используется, главным образом, для сетей VPN удаленного доступа с ОС Windows 2000, поскольку ОС Windows 2000 предоставляет собственного клиента IPsec и L2TP. Поставщик услуг Интернета также обеспечивает подключения L2TP для удаленных пользователей, а затем шифрует этот трафик с помощью IPsec между своей точкой доступа и сервером сети удаленного офиса.
- **Целостность данных — При том, что очень важно осуществлять шифрование данных при передаче через сеть общего пользования, не менее важно проверять их неизменность в процессе передачи.** Например, IPsec имеет механизм гарантирования того, что зашифрованная часть пакета или пакет целиком (заголовок и данные) не были изменены. В случае обнаружения изменения, пакет отбрасывается. Целостность данных также может включать аутентификацию удаленного узла.
- **Аутентификация источника данных — Очень важно проверять удостоверение источника отправленных данных.** Это обязательно для защиты от целого ряда атак, использующих подделку удостоверения отправителя.
- **Защита от повторений пакетов — Это способность обнаруживать и отбрасывать**

повторно передаваемые пакеты, которая помогает предотвратить спуфинг.

- **Туннелирование данных/конфиденциальность потока трафика — Туннелирование — это процесс инкапсуляции целого пакета внутрь другого пакета и отправка его по сети.** Туннелирование данных полезно в случаях, когда желательно скрывать удостоверение устройства, являющегося источником трафика. Например, одно устройство, использующее IPsec, инкапсулирует трафик, принадлежащий нескольким узлам, расположенным после него, и добавляет свой собственный заголовок в верхнюю часть имеющихся пакетов. Шифрованием исходного пакета и заголовка (и маршрутизацией пакета на основании дополнительного заголовка 3-го уровня, добавленного в верхнюю часть), устройство туннелирования эффективно скрывает фактический источник пакета. Только доверенный узел способен определить действительный источник после отделения дополнительного заголовка и расшифровки исходного заголовка. Как обращено внимание в RFC 2401, "... раскрытие внешних характеристик связи также может быть беспокойством при некоторых обстоятельствах. Конфиденциальность потока трафика — это сервис, который призван решать упомянутую выше проблему путем маскирования адресов источника и назначения, длины сообщения и активности информационного обмена. В контексте IPsec использование ESP в туннельном режиме, особенно на шлюзе безопасности, может обеспечить некоторый уровень конфиденциальности потока трафика."."Все перечисленные здесь протоколы шифрования также используют туннелирование как средство передачи шифрованных данных через сеть общего пользования. Важно понимать, что туннелирование само по себе не обеспечивает безопасность данных. Исходный пакет просто инкапсулируется внутри другого протокола и, по-прежнему, может быть виден с помощью устройства захвата пакетов, если не зашифрован. Однако это уже упомянуто здесь, поскольку является неотъемлемой частью функционирования VPN.Для туннелирования требуются три разных протокола.**Протокол Passenger — Передаваемые исходные данные (IPX, NetBeui, IP).Протокол инкапсуляции — Протокол (GRE, IPsec, L2F, PPTP, L2TP) инкапсулирующий исходные данные.Транспортный протокол — Протокол, используемый сетью, через которую передаются данные.**Исходный пакет (протокол Passenger) инкапсулируется внутри протокола инкапсуляции, который затем помещается внутрь заголовка транспортного протокола (обычно IP) для передачи через сеть общего пользования. Обратите внимание, что протокол инкапсуляции также во многих случаях осуществляет шифрование данных. Такие протоколы как IPX и NetBeui, которые обычно не передаются через Интернет, можно надежно и безопасно передавать.Для VLAN типа "сеть-сеть" протоколом инкапсуляции служит как правило IPsec или протокол туннелирования сетевых пакетов (GRE). GRE содержит сведения о типе инкапсулируемого пакета и данные о соединении между клиентом и сервером.Для сетей VPN удаленного доступа туннелирование, как правило, осуществляются с помощью протокола точка-точка (PPP). Часть стека TCP/IP, PPP является транспортом для других протоколов IP при обмене данными через сеть между узлом и удаленной системой. Туннелирование PPP будет использовать один из следующих протоколов: PPTP, L2TP или протокол эстафетной передачи на втором уровне Cisco (Layer 2 Forwarding, L2F).
- **AAA — Протокол AAA (аутентификации, авторизации и учета) используется для более безопасного доступа в среде VPN удаленного доступа.** Без аутентификации пользователя любое лицо, имеющее доступ к ноутбуку или ПК с предварительно настроенным ПО клиента VPN может установить безопасное подключение к удаленной сети. Однако при использовании аутентификации пользователя, чтобы установить

соединение требуется ввести действительные пароль и имя пользователя. Пароли и имена пользователя могут храниться в самом оконечном устройстве VPN или на внешнем сервере AAA, который может обеспечивать аутентификацию для целого ряда баз данных, например Windows NT, Novell, LDAP и др.Когда запрос установки туннеля исходит от удаленного клиента, устройство VPN запрашивает пароль и имя пользователя. Затем эти данные могут пройти аутентификацию локально или будут отправлены внешнему серверу AAA, который проверит:Удостоверение пользователя (Аутентификация)Права пользователя (Авторизация)Фактические действия пользователя (Учет)Данные учета особенно полезны для отслеживания действий клиента с целью аудита безопасности, биллинга или составления отчетности.
- **Неподдельность — Очень полезная функция при передаче определенных данных, например относящихся к финансовым операциям.** Она полезна для предотвращения ситуаций, когда одна сторона отказывается признавать участие в операции. Почти аналогично тому, как банк требует поставить подпись прежде чем заплатить по чеку, неподдельность функционирует путем присоединения цифровой подписи к отправляемому сообщению, исключая возможность отказа отправителя от участия в операции.

Существует целый ряд протоколов, которые можно использовать для создания решения VPN. Все эти протоколы предоставляют некоторый поднабор сервисов, перечисленных в данном документе. Выбор протокола определяется желаемым набором сервисов. Например, одна организация может быть удовлетворена передачей данных открытым текстом, но очень заинтересована в сохранении их целостности, тогда как для другой организации исключительно важным является сохранение конфиденциальности данных. В этом случае их выбор протоколов может отличаться. Дополнительную информацию о доступных протоколах и их сравнительных достоинствах см. в Выбор подходящего VPN-решения?

Продукты для VPN

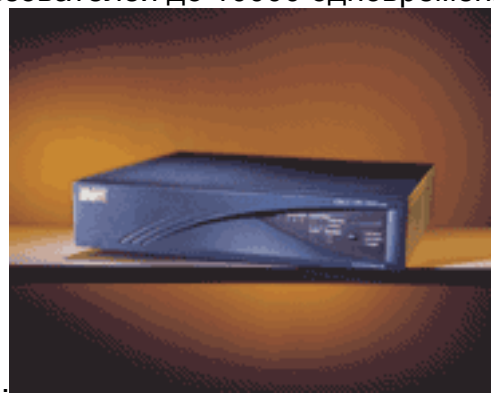
В зависимости от типа VPN (удаленный доступ или "сеть-сеть") потребуются определенные компоненты для создания VPN. К ним относятся:

- Клиентское ПО настольной системы для каждого удаленного пользователя
- Специализированное оборудование, например концентратор Cisco VPN Concentrator или межсетевой экран Cisco Secure PIX Firewall
- Специализированный VPN-сервер для служб удаленного доступа
- Сервер доступа к сети (NAS), используемый поставщиком услуг для доступа удаленных пользователей к виртуальной частной сети (VPN)
- Центр управления политиками и частной сетью

Поскольку нет общепринятого стандарта для реализации VPN, многие компании разрабатывают собственные решения "под ключ". Например, Cisco предлагает несколько решений VPN, включая:

- **Концентратор VPN Concentrator — Используя самые передовые существующие методы аутентификации и шифрования, концентраторы Cisco VPN сконструированы специально для создания VPN удаленного доступа и типа "сеть-сеть" и являются оптимальным решением для развертывания, когда требуется одно устройство для работы с очень большим числом VPN-туннелей.** VPN Concentrator специально разработан, чтобы

удовлетворить потребность в специализированном устройстве для VPN удаленного доступа. Эти концентраторы обеспечивают высокую доступность, производительность и масштабируемость и включают компоненты, называемые модулями Scalable Encryption Processing (SEP), которые позволяют пользователям легко повышать производительность и пропускную способность. Эти концентраторы предлагаются в моделях, подходящих как небольшим компаниям с числом удаленных пользователей не более 100, так и крупным коммерческим организациям с числом удаленных пользователей до 10000 одновременно работающих в



сети.

- **Маршрутизатор с поддержкой VPN и оптимизированный для VPN — Все маршрутизаторы Cisco, на которых выполняется ПО Cisco IOS®, поддерживают сети IPsec VPN.** Единственное требование состоит в том, что на маршрутизаторе должен выполняться образ ПО Cisco IOS с соответствующим набором функций. Решение VPN Cisco IOS полностью поддерживает удаленный доступ, требования сети VPN к интрасети и экстрасети. Это означает, что маршрутизаторы Cisco эффективно работают как при подключении к удаленному узлу, на котором выполняется ПО клиента VPN, так и при подключении к другому устройству VPN, например маршрутизатору, межсетевому экрану PIX Firewall или концентратору VPN Concentrator. Маршрутизаторы с поддержкой VPN подходят для сетей VPN с умеренными требованиями к шифрованию и туннелированию и предоставляют сервисы VPN полностью через функции ПО Cisco IOS. К маршрутизаторам с поддержкой VPN относятся модели Cisco серий 1000, 1600, 2500, 4000, 4500 и 4700.Маршрутизаторы Cisco оптимизированные для VPN обеспечивают масштабируемость, маршрутизацию, безопасность и качество обслуживания (QoS). Маршрутизаторы функционируют на основе ПО Cisco IOS, при этом имеется подходящее устройство для каждой ситуации: от решения доступа для SOHO через центральный сервер объединения VPN до решений для крупных коммерческих организаций. Маршрутизаторы, оптимизированные для VPN, сконструированы для удовлетворения высоких требований к шифрованию и туннелированию и часто используют дополнительные устройства, например криптоплаты, чтобы обеспечить высокую производительность. К маршрутизаторам оптимизированным для VPN относятся модели Cisco серий 800, 1700, 2600, 3600, 7200

и 7500.

- **Межсетевой экран Cisco Secure PIX Firewall — Межсетевой экран Private Internet eXchange (PIX) сочетает динамическую трансляцию сетевых адресов, прокси-сервер, фильтрацию пакетов, межсетевой экран и возможности VPN в одном устройстве.** Вместо использования ПО Cisco IOS, это устройство имеет высоко рациональную ОС, в которой вместо способности работать со множеством протоколов реализована высокая отказоустойчивость и производительность за счет сосредоточенности на протоколе IP. Как и маршрутизаторы Cisco, все модели межсетевого PIX поддерживают IPsec VPN. Все что требуется для включения функции VPN — это удовлетворение требований

лицензирования.

- **Клиенты Cisco VPN — Компания Cisco предлагает аппаратные и программные клиенты VPN.** Клиент Cisco VPN (ПО) поставляется вместе с концентратором Cisco VPN серии 3000 без дополнительной платы. Этот программный клиент можно установить на узле, используемом для безопасного подключения к концентратору центрального узла (или к любому другому устройству VPN, например маршрутизатору или межсетевому экрану). Аппаратный клиент VPN 3002 — это еще один способ развертывания программного клиента VPN на каждом ПК, обеспечивающий связность VPN для целого ряда устройств.

Выбор устройства для создания решения VPN в итоге определяется задачей проектирования и зависит от целого ряда факторов, включая требуемую пропускную способность и количество пользователей. Например, на удаленном узле с несколькими пользователями позади PIX 501 можно рассмотреть настройку имеющегося межсетевого экрана PIX в качестве конечной точки IPsec VPN при условии достаточности пропускной способности 3DES межсетевого экрана 501 (приблизительно 3 Мбит/с) и ограничения количества VPN узлов значением 5. С другой стороны на центральном узле, функционирующем в качестве конечной точки VPN для большого числа VPN-туннелей, целесообразным будет использование маршрутизатора, оптимизированного для VPN, или концентратора VPN. Выбор теперь зависит от типа ("сеть-сеть" или удаленный доступ) и количества настроенных VPN-туннелей. Широкий перечень устройств Cisco, поддерживающих VPN, обеспечивает проектировщикам сети большую гибкость и высокую отказоустойчивость решения для удовлетворения потребности в каждом решении.

Дополнительные сведения

- Общие сведения о VPDN (виртуальная частная коммутируемая сеть)
- Виртуальные частные сети (VPN)
- Страница поддержки концентраторов Cisco VPN серии 3000
- Страница поддержки Cisco VPN 3000 Client
- Страница поддержки IPsec Negotiation/IKE
- Страница поддержки межсетевых экранов PIX серии 500
- RFC 1661: Протокол PPP
- RFC 2661: уровень два протокола туннелирования "L2TP"
- Как работает система: Принципы работы частных виртуальных сетей
- Обзор VPN
- Страница VPN Тома Дунигэна
- Консорциум виртуальной частной сети
- Запросы комментариев (RFC)
- Техническая поддержка - Cisco Systems