Выбор подходящего VPN-решения?

Содержание

Введение

Виртуальные частные сети (VPNs) становятся все более популярными как менее затратный и более гибкий способ развертывания сети на обширную область. С прогрессом технологий растет многообразие вариантов внедрения решений для виртуальных частных сетей. В этих технических примечаниях объясняются некоторые из таких вариантов и описываются наиболее уместные их применения.

Перед началом работы

Условные обозначения

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

Предварительные условия

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям

программного обеспечения и оборудования.

Примечание: Cisco также обеспечивает поддержку шифрования на платформах, отличных от Cisco IOS, включая межсетевой экран Cisco Secure PIX, концентраторы Cisco VPN 3000 и Cisco VPN 5000.

NAT

Интернет испытал взрывной рост в скором времени, намного больше чем разработчики, возможно, предвидели. Ограниченное число адресов в протоколе IP версии 4.0 свидетельствует о его расширении и, как результат, о снижении уровня доступности адресного пространства. Одно из решений проблемы - трансляция сетевых адресов (NAT).

При помощи NAT маршрутизатор настраивается на внутренних/внешних границах так, что снаружи (обычно в Интернете) видно один или несколько зарегистрированных адресов, а внутри может использоваться любое количество хостов с применением частной схемы адресации. Для достижения сохранности схемы трансляции адресов NAT должна быть сконфигурирована на каждом граничном маршрутизаторе между внутренней (частной) сетью и внешней (открытой) сетью. Одним из преимуществ NAT с точки зрения безопасности является то, что системы в частной сети не могут получать данные по входящему IP-соединению из внешних сетей, если шлюз NAT не настроен особым образом для разрешения такого соединения. Кроме того, NAT абсолютно очевиден для источника и целевых устройств. Рекомендуемая операция NAT включает RFC 1918, который выделяет схемы адресации в частных сетях. Стандарт для NAT описан в RFC1631.

Следующие данные показывают определение границы маршрутизатора NAT с пулом сетевых адресов внутренней трансляции.

NAT обычно используется для сохранения маршрутизируемых в Интернете IP-адресов, которые являются дорогими и ограниченными в номере. NAT также предоставляет безопасность путем сокрытия внутренней сети от Интернета.

Для получения информации о работе NAT посмотрите, Как Работает NAT.

Туннелирование GRE-инкапсуляции

Туннели универсальной инкапсуляции маршрутизации (GRE) предоставляют определенный путь через совместно используемую глобальную сеть (WAN) и инкапсулируют трафик с новыми заголовками пакета, чтобы гарантировать доставку определенным назначениям. Сеть является частной, потому что трафик может ввести туннель только в оконечную точку и может уехать только в другой оконечной точке. Туннели не предоставляют истинную конфиденциальность (как шифрование, делает), но может нести зашифрованный поток данных. Туннели являются логическими оконечными точками, настроенными на физических интерфейсах, через которые несут трафик.

Как проиллюстрировано в схеме, Туннелирование GRE может также использоваться, чтобы инкапсулировать не-IP трафик в IP и передать его по Интернету или IP - сети. Межсетевой пакетный обмен (IPX) и Протоколы "AppleTalk" является примерами не-IP трафик. Для получения информации о настройке GRE см. "Настройку Туннельный интерфейс GRE" в GRE Настройки.

Если вы имеете многопротокольную сеть как IPX или AppleTalk и должны передать трафик по Интернету или IP - сети, GRE является правильным решением для VPN для вас. Кроме того, GRE-инкапсуляция обычно используется в сочетании с другими средствами обеспечения трафика, такого как IPSec.

Для большего количества технических подробностей на GRE обратитесь к RFC 1701 и RFC 2784.

Шифрование IPSec

Шифрование данных, передаваемое через общую сеть, является технологией VPN, чаще всего привязанной к VPN. Cisco поддерживает IP-безопасность (IPSec) методы шифрования данных. IPSec является платформой открытых стандартов, которая предоставляет конфиденциальность данных, целостность данных и проверку подлинности данных между взаимодействующими одноранговыми узлами на сетевом уровне.

IP - безопасное шифрование является стандартом инженерной группы по развитию Интернета (IETF), который поддерживает Стандарт шифрования данных (DES), 56-разрядный и Тройной DES (3DES) 168-разрядные алгоритмы шифрования с симметричным ключом в программном обеспечении Клиента IPSEC. Конфигурация GRE является дополнительной с IPSec. Протокол IPSec поддерживает также центры сертификации и согласование обмена ключами в Интернете (IKE). Шифрование IPSec может быть развернуто в автономной среде между клиентами, маршрутизаторами и межсетевыми экранами либо использоваться совместно с туннелированием L2TP при доступе к VPN. IPSec поддерживается в на различных платформах операционной системы.

Если вы хотите истинную конфиденциальность данных для своих сетей, IP - безопасное шифрование является правильным решением для VPN для вас. IPSec является также открытым стандартом, таким образом, совместимость между другими устройствами легко внедрить.

PPTP и MPPE

Протокол PPTP был разработан Microsoft; это описано в RFC2637. PPTP широко развернут в Windows 9x/ME, Windows NT, и Windows 2000 и клиентском программном обеспечении Windows XP для включения добровольных VPN.

Протокол шифрования MPPE – это информационный проект IETF компании Microsoft, который поддерживает 40-битное или 128-битное шифрование по протоколу RC4. MPPE является частью программного решения клиента PPTP Microsoft и полезен в Архитектурах VPN добровольного доступа в режиме. PPTP/MPPE поддерживается на большинстве Платформ cisco.

В Cisco IOS Software Release 12.0.5.XE5 добавлена поддержка PPTP для платформ Cisco 7100 и 7200. Поддержка других платформ была добавлена в Cisco IOS 12.1.5.T. Межсетевой экран Cisco Secure PIX Firewall и Cisco VPN 3000 Concentrator также имеют поддержку для клиентских подключений PPTP.

Так как PPTP поддерживает сети не-IP, полезно, где удаленные пользователи должны набрать в к корпоративной сети для доступа к неоднородным корпоративным сетям.

Для получения информации о настройке PPTP посмотрите PPTP Настройки.

VPDN и L2TP

VPDN

Virtual Private Dialup Network (VPDN) – стандарт Cisco, который позволяет сервису набора частной сети охватить серверы удаленного доступа. В контексте VPDN сервер доступа (например, AS5300), к которому произведено подключение, обычно называется сервером доступа сети (NAS). Назначение пользователя с наборным телефонным доступом упоминается как домашний шлюз (HGW).

Простой сценарий для протокола двухточечного соединения Point-to-Point Protocol (PPP) , с помощью которого клиент соединяется с локальным NAS. NAS решает, что сеанс PPP должен быть передан маршрутизатору домашнего шлюза для того клиента. Затем HGW выполняет проверку подлинности пользователя и начинает согласование PPP. После завершения настройки PPP все кадры посылаются через NAS к клиенту и домашним шлюзам. Этот метод объединяет в себе несколько протоколов и концепций.

Для получения информации о настройке VPDN посмотрите *Настройку Виртуальная частная коммутируемая сеть* в Характеристиках безопасности Настройки.

L2TP

Уровень 2 туннельного протокола (L2TP) является стандартом IETF, объединяющим лучшие свойства PPTP и L2F. Туннели L2TP используются в основном в режиме принудительного доступа (модемное соединение NAS с HGW) к VPN как для IP-трафика, так и для остального трафика. В Windows 2000 и Windows XP была добавлена встроенная поддержка этого протокола в качестве средства подключения клиента VPN.

L2TP используется для туннелирования PPP по открытой сети, такой как Интернет, с помощью IP. Так как туннель происходит на Уровне 2, протоколы верхнего уровня неосведомлены о туннеле. Как GRE, L2TP может также инкапсулировать любой протокол Уровня 3. Порт 1701 UDP используется для передачи трафика L2TP инициатором туннеля.

Примечание: В 1996 Cisco создала протокол переадресации уровня 2 (L2F), чтобы позволить соединениям VPDN происходить. Протокол L2F по-прежнему поддерживается другими функциями (но заменен на L2TP). Туннельный протокол "точка-точка" (PPTP) также был создан в 1996 г. рабочей группой IETF в качестве Интернет-проекта. PPTP предоставил функцию, аналогичную GRE-подобному туннельному протоколу для PPP-соединений.

Для получения дополнительной информации о L2TP посмотрите Протокол туннелирования Уровня 2.

PPPoE

PPP over Ethernet (PPPoE) является информационным RFC, который прежде всего развернут в средах цифровой абонентской линии (DSL). PPPoE эффективно использует существующую инфраструктуру Ethernet, позволяя пользователям инициировать несколько сеансов PPP в пределах одной и той же LAN. Эта технология позволяет осуществлять

селекцию на 3 уровне – это новое приложение, с помощью которого пользователь может одновременно подключаться по нескольким направлениям при помощи единого соединения удаленного доступа. PPPoE с Протоколом аутентификации пароля (PAP) или Протоколом аутентификации по квитированию вызова (CHAP) часто используется для информирования центрального узла, какие удаленные маршрутизаторы связаны с ним.

PPPoE главным образом используется в обслуживании развертывания DSL поставщика и топология Ethernet с сетевыми мостами.

Для получения дополнительной информации о настройке PPPoE посмотрите PPPoE Настройки по VLAN IEEE 802.1Q и Ethernet.

MPLS VPN

Многопротокольная коммутация по меткам (MPLS) представляет собой стандарт, основанный на маркерной коммутации, которая обеспечивает автоматическую инициализацию, срочную рассылку, масштабируемость, необходимые провайдерам для экономичного предоставления доступа, услуг интрасети и внешних виртуальных частных сетей. Cisco работает в тесном сотрудничестве с поставщиками услуг для обеспечения беспрепятственного обмена данными поддерживающим MPLS Сервисам VPN. MPLS работает на основе парадигмы меток, снабжая ими пакеты при входе в сеть поставщика, чтобы ускорить переадресацию через IP-ядро без установленного соединения. MPLS использует признаки маршрута, чтобы определить членство VPN и содержать трафик в сообществе VPN.

MPLS также добавляет преимущества подхода с установлением соединения к парадигме IP-маршрутизации посредством установления путей коммутации меток, которые созданы на основе информации о топологии скорее тогда трафик. MPLS VPN широко развернут в среде поставщика услуг.

Для получения информации о настройке MPLS VPN посмотрите Настройку Основной MPLS VPN.

Дополнительные сведения

- Страница поддержки IPSec
- Принципы работы частных виртуальных сетей
- Страница поддержки NAT
- Страница технической поддержки GRE
- Страница технической поддержки VPDN
- Страница поддержки PPTP
- Страница поддержки PPPoE
- Техническая поддержка - Cisco Systems