Конспект лекции 12.
Технологии VPN

12.1. Вводные положения

Определение

VPN (Virtual Private Network) – совокупность технологий, обеспечивающих безопасную и по возможности качественную связь между территориально-распределенными подсетями и группами пользователей через общедоступную открытую сеть Интернет

2 смысла слова private

1) собственный

2) защищенный, конфиденциальный

В технологиях VPN имеется в виду 2-й смысл термина

Потребности в VPN

1) Интрасеть (связь между филиалами)

2) Экстрасеть (связь с внешними деловыми партнерами). Типичный пример – сеть межбанковских переводов SWIFT

3) Доступ к корпоративной сети мобильных и/или удаленных пользователей

4) Изоляция внутри корпоративной сети виртуальных сетей различных приложений и/или подразделений (средствами VLAN и/или MPLS VPN)/

12.2. Разновидности VPN

(с указанием их достоинств и недостатков)

1) Истинная частная сеть

2) Сеть, построенная на арендованных физических каналах или оптических частотах (лямбдах) (VPN L1)

3) Сеть, построенная на арендованной VLAN (VPN L2)

4) MPLS VPN (VPN L3)

5) VPN на базе общедоступной сети (предмет данной лекции)

Отметим, что рассмотренные способы построения VPN могут использоваться не только для изоляции распределённой корпоративной сети от внешних сетей (интернета), но и для взаимной изоляции различных распределённых подсетей корпоративной сети, наложенных на единую физическую инфраструктуру этой сети. К распеделенным подсетям корпоративной сети можно отнести сети распределённых (расположенных в нескольких зданиях) подразделений и сети распределённых приложений (АСУ, сеть видеонаблюдения и пр.). При этом такие сети могут надстраиваться над структурой, состоящей как из компонентов (MPLS VPN), обеспечиваемых MPLS магистралью корпоративной сети, так и из периферийных сегментов, оформленных в виде LAN. В работе (Букатов А.А., Шаройко О.В., Березовский А.Н. Принципы, задачи и методы построения интегрированной телекоммуникационной сети объединяемых учреждений // Информатизация образования и науки, № 1(17), 2013, с. 48-63.) предложен метод создания комбинированных L3/L2 VPN, предназначенных для создания двухуровневых (L3/L2) изолированных распределённых подсетей корпоративной сети.

Способы построения

1) VPN от оператора связи

2) VPN, создаваемая собственными средствами

12.3. Базовая архитектура VPN-сети

Взаимодействие через общедоступную сеть
Основное внимание – безопасность взаимодействия через защищенные каналы
Вопросы качества каналов остаются вне рамок рассмотрения

Основные компоненты базовой архитектуры VPN
- VPN-шлюз
- VPN-клиент
- RAS сервер

Функции указанных компонентов

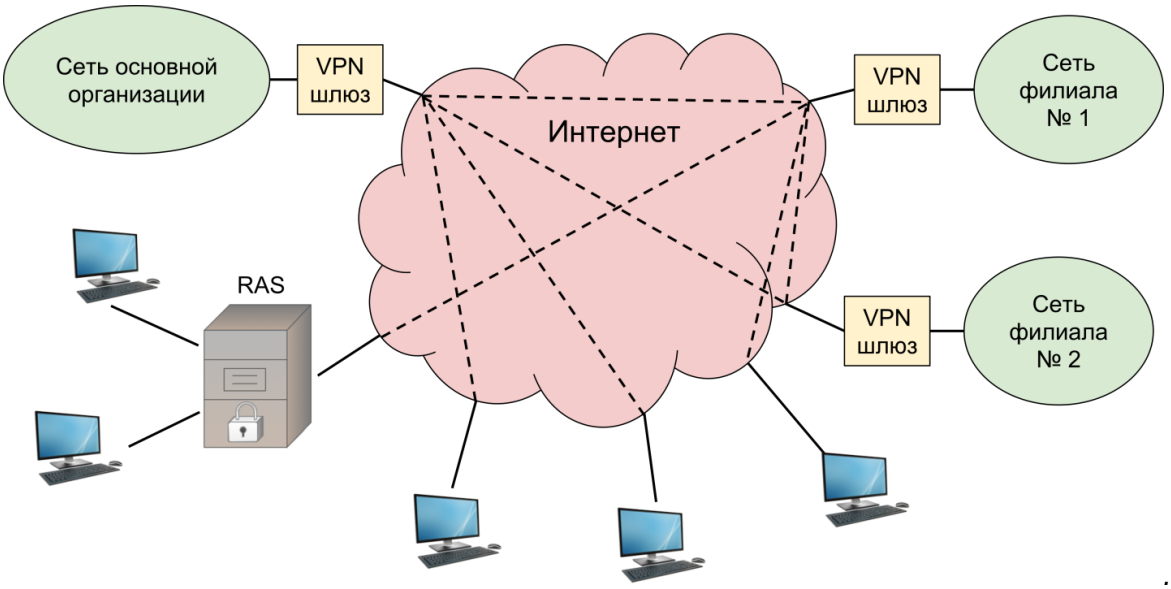

Рис. 11.1. Схема построения VPN-сети

12.4. Защита и туннелирование данных в каналах VPN

Определение защищенного канала
- конфиденциальность
- целостность
- доступность

Организация защищенного канала
- шифрование
- туннелирование
- аутентификация (не только пользователей, но и серверов), системы аутентификации Radius, Kerberous, Tacacs и др.
- авторизация доступа к ресурсам

Туннелирование, как метод организации защищенного канала

Туннелирование – инкапсуляция одних пакетов в другие (с возможной шифрацией инкапсулируемых пакетов). Тип инкапсулируемых пакетов может отличаться от типа инкапсулирующих.

Туннелирование может выполняться на разных уровнях стека протоколов, например, на уровне 2 может применяться протокол L2TP (Layer 2 Tunneling Protocol).

Чем ниже уровень, на котором выполняется туннелирование, тем выше уровень защищенности (заголовки пакетов более высоких уровней шифруются). (Но «дальнобойность» VPN-каналов разных уровней тоже различна).

Механизм туннелирования включает
- несущий протокол
- протокол «пассажир»
- собственно протокол туннелирования (процедура инкапсуляции/декапсуляции с возможной шифрацией/дешифрацией)

12.5. Типы VPN устройств по методам их технической реализации

- Маршрутзатор со специализированным ПО VPN-шлюза
- Специализированное аппаратное (компьютерное) устройство со специализированным ПО, имеющее не менее 2 сетевых интерфейсов (иногда – без IP-адресов) и аппаратную криптографическую поддержку (VPN Black Box). В случае отсутствия IP-адресов VPN Black Box абсолютно прозрачен для IP и протоколов более высокого уровня и не может быть атакован их средствами
- Программный продукт, работающий на обычном компьютере в среде его ОС (главным образом – для клиентских VPN устройств).
- Дополнительные программные средства, встроенные в ОС маршрутизатора

12.6. Обзор системы OpenVPN

Система OpenVPN является свободной (бесплатной и поставляемой в исходных кодах) программной реализаций VPN-устройств, позволяющих создавать VPN-сети типа сервер-клиенты (шлюз-клиенты) или точка-точка (клиент-клиент). Для сетей типа сервер-клиенты сервер не должен находиться за NAT (и должен иметь “белый” IP-адрес), клиенты же вполне могут находиться и за NAT и за межсетевым экраном. Для VPN-сетей типа точка-точка одна из этих точек (к которой обращаются при первом сетевом взаимодействии между этими точками) также не должна находиться за NAT. Отметим, что система OpenVPN предоставляет возможность создания VPN-каналов, используемых для защищённого доступа к серверу или клиентскому компьютеру компьютеров пользователей, подключенных к сети с использованием точек подключения Wi-Fi или ADSL-модемов. Эта возможность достаточно широко востребована среди сотрудников ЮФУ для обеспечения защищённого доступа со своих домашних компьютеров к их основному серверу, входящему в общую структуру корпоративной сети ЮФУ или в одну из её внутренних VPN.

Для организации работы с защищенным VPN-каналом в системе OpenVPN используется библиотека OpenSSL. Это даёт возможность при конфигурировании таких каналов применять любые из предоставляемых библиотекой OpenSSL алгоритмов шифрования, имеющихся в этой библиотеке. Для повышения уровня защищённости создаваемых VPN-каналов для них может быть сконфигурировано применение пакетной аутентификации HMAC (*Hash-based Message Authentication Code*, код аутентификации сообщений, использующий хеш-функции) - один из механизмов проверки целостности передаваемых пакетов, позволяющий гарантировать, что эти пакеты не были изменены сторонними лицами, перехватившими сетевое соединение. Возможно также применение средств аппаратного ускорения для повышения производительности шифрования и средств компрессии (уменьшения объёма) передаваемых данных с целью уменьшения требований к свободной ёмкости доступных каналов передачи данных.

Система OpenVPN, как это реализовано и в составляющей её основу библиотеке OpenSSL, может работать над транспортными протоколами и TCP и UDP. Однако использование UDP по ряду причин является более предпочтительными. Так в лекции 7

мы рассматривали, как использование UDP позволяет пакетам, адресованным работающим за NAT клиентским компьютерам, пройти сквозь NAT. Подобным же образом обеспечивается прохождение таких пакетов и через различные прокси-серверы и через межсетевые экраны.

Отметим, что система OpenVPN предоставляет возможность выбора одного из двух реализованных в ней (в драйвере TUN/TAP) вариантов сетевых интерфейсов. Возможно создание туннеля *TUN* сетевого уровня, и туннеля *TAP* канального уровня, обеспечивающего передачу Ethernet-трафика. Таким образом, туннель TAP может использоваться в роли разновидности сетевых мостов, соединяющих 2 удаленных Ethernet-сегмента. Такая возможность может быть использована распределёнными приложениями, использующими транспорт канального уровня.

Система OpenVPN доступна в исходных текстах для большинства разновидностей системы UNIX, большинства из применяющихся в настоящее время версий MS Windows (начиная с 7-й) и в ряде других ОС, включая Apple Mac OS X, QNX, Android, iOS (компании Apple а не Cisco). Поэтому эта система достаточно широко используется, также, как и потому, что может применяться даже в тех случаях, когда интернет-оператор блокирует прохождение трафика некоторых других VPN-протоколов.

И, в завершение рассмотрения системы OpenVPN она обеспечивает адекватное защищённое средство удалённого доступа к внутренним VPN корпоративной сети путём установки этой системы на один из серверов требуемой внутренней VPN и на компьютеры всех удалённых пользователей, имеющих права доступа к этой VPN.