|  |
| --- |
| ГОУ ВПО МГТУ «Станкин» |
| Реферат по методам и средствам защиты компьютерной информации |
| Создание и использование виртуальных частных сетей (VPN) |
|  |
|  |
|  |

Выполнил: Мишаков Д.Г. группа И-7-2

|  |
| --- |
| 2008г. |

В последнее время в мире телекоммуникаций наблюдается повышенный интерес к так называемым Виртуальным Частным Сетям (Virtual Private Network - VPN). Это обусловлено необходимостью снижения расходов на содержание корпоративных сетей за счет более дешевого подключения удаленных офисов и удаленных пользователей через сеть Internet (см. рис. 1). Действительно, при сравнении стоимости услуг по соединению нескольких сетей через Internet, например, с сетями Frame Relay можно заметить существенную разницу в стоимости. Однако, необходимо отметить, что при объединении сетей через Internet, сразу же возникает вопрос о безопасности передачи данных, поэтому возникла необходимость создания механизмов позволяющих обеспечить конфиденциальность и целостность передаваемой информации. Сети, построенные на базе таких механизмов, и получили название VPN.

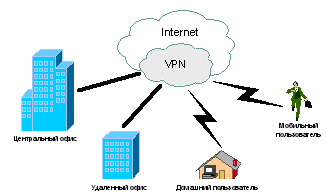


Рисунок 1. Виртуальная Частная сеть.

В свое реферате я попробую объяснить, что такое VPN, какими плюсами и минусами обладает данная технология и какие варианты реализации VPN существуют.

# Что такое VPN

Что же такое VPN? Существует множество определений, однако главной отличительной чертой данной технологии является использование сети Internet в качестве магистрали для передачи корпоративного IP-трафика. Сети VPN предназначены для решения задач подключения конечного пользователя к удаленной сети и соединения нескольких локальных сетей. Структура VPN включает в себя каналы глобальной сети, защищенные протоколы и маршрутизаторы.

Как же работает Виртуальная Частная Сеть? Для объединения удаленных локальных сетей в виртуальную сеть корпорации используются так называемые виртуальные выделенные каналы. Для создания подобных соединений используется механизм туннелирования. Инициатор туннеля инкапсулирует пакеты локальной сети (в том числе, пакеты немаршрутизируемых протоколов) в новые IP-пакеты, содержащие в своем заголовке адрес этого инициатора туннеля и адрес терминатора туннеля. На противоположном конце терминатором туннеля производится обратный процесс извлечения исходного пакета.

Как уже отмечалось выше, при осуществлении подобной передачи требуется учитывать вопросы конфиденциальности и целостности данных, которые невозможно обеспечить простым туннелированием. Для достижения конфиденциальности передаваемой корпоративной информации необходимо использовать некоторый алгоритм шифрования, причем одинаковый на обоих концах туннеля.

Для того чтобы была возможность создания VPN на базе оборудования и программного обеспечения от различных производителей необходим некоторый стандартный механизм. Таким механизмом построения VPN является протокол Internet Protocol Security (IPSec). IPSec описывает все стандартные методы VPN. Этот протокол определяет методы идентификации при инициализации туннеля, методы шифрования, используемые конечными точками туннеля и механизмы обмена и управления ключами шифрования между этими точками. Из недостатков этого протокола можно отметить то, что он ориентирован на IP.

Другими протоколами построения VPN являются протоколы PPTP (Point-to-Point Tunneling Protocol), разработанный компаниями Ascend Communications и 3Com, L2F (Layer-2 Forwarding) - компании Cisco Systems и L2TP (Layer-2 Tunneling Protocol), объединивший оба вышеназванных протокола. Однако эти протоколы, в отличие от IPSec, не являются полнофункциональными (например, PPTP не определяет метод шифрования), поэтому мы, в основном, будем ориентироваться на IPSec.

Говоря об IPSec, нельзя забывать о протоколе IKE (Internet Key Exchange), позволяющем обеспечить передачу информации по туннелю, исключая вмешательство извне. Этот протокол решает задачи безопасного управления и обмена криптографическими ключами между удаленными устройствами, в то время, как IPSec кодирует и подписывает пакеты. IKE автоматизирует процесс передачи ключей, используя механизм шифрования открытым ключом, для установления безопасного соединения. Помимо этого, IKE позволяет производить изменение ключа для уже установленного соединения, что значительно повышает конфиденциальность передаваемой информации.

# Как построить VPN

Существуют различные варианты построения VPN. При выборе решения требуется учитывать факторы производительности средств построения VPN. Например, если маршрутизатор и так работает на пределе мощности своего процессора, то добавление туннелей VPN и применение шифрования/дешифрования информации могут остановить работу всей сети из-за того, что этот маршрутизатор не будет справляться с простым трафиком, не говоря уже о VPN.

Опыт показывает, что для построения VPN лучше всего использовать специализированное оборудование, однако если имеется ограничение в средствах, то можно обратить внимание на чисто программное решение.

# Рассмотрим некоторые варианты построения VPN:

## VPN на базе брандмауэров

Брандмауэры большинства производителей поддерживают туннелирование и шифрование данных. Все подобные продукты основаны на том, что если уж трафик проходит через брандмауэр, то почему бы его заодно не зашифровать. К программному обеспечению собственно брандмауэра добавляется модуль шифрования. Недостатком данного метода можно назвать зависимость производительности от аппаратного обеспечения, на котором работает брандмауэр. При использовании брандмауэров на базе ПК надо помнить, что подобное решение можно применять только для небольших сетей с небольшим объемом передаваемой информации.

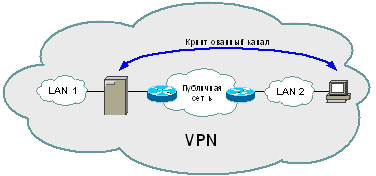


Рисунок 2. VPN на базе брандмауэра

В качестве примера решения на базе брандмауэров можно назвать FireWall-1 компании Check Point Software Technologies. FairWall-1 использует для построения VPN стандартный подход на базе IPSec. Трафик, приходящий в брандмауэр, дешифруется, после чего к нему применяются стандартные правила управления доступом. FireWall-1 работает под управлением операционных систем Solaris и Windows NT 4.0.

## VPN на базе маршрутизаторов

Другим способом построения VPN является применение для создания защищенных каналов маршрутизаторов. Так как вся информация, исходящая из локальной сети, проходит через маршрутизатор, то целесообразно возложить на этот маршрутизатор и задачи шифрования.

Ярким примером оборудования для построения VPN на маршрутизаторах является оборудование компании Cisco Systems. Начиная с версии программного обеспечения IOS 11.3(3)T маршрутизаторы Cisco поддерживают протоколы L2TP и IPSec. Помимо простого шифрования проходящей информации Cisco поддерживает и другие функции VPN, такие как идентификация при установлении туннельного соединения и обмен ключами.

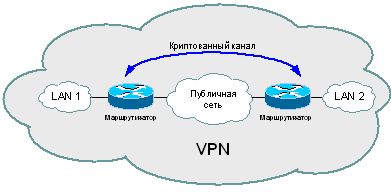


Рисунок 3. VPN на базе маршрутизаторов

Для построения VPN Cisco использует туннелирование с шифрованием любого IP-потока. При этом туннель может быть установлен, основываясь на адресах источника и приемника, номера порта TCP(UDP) и указанного качества сервиса (QoS).

Для повышения производительности маршрутизатора может быть использован дополнительный модуль шифрования ESA (Encryption Service Adapter).

Кроме того, компания Cisco System выпустила специализированное устройство для VPN, которое так и называется Cisco 1720 VPN Access Router (Маршрутизатор Доступа к VPN), предназначенное для установки в компаниях малого и среднего размера, а также в в отделениях крупных организаций.

## VPN на базе программного обеспечения

Следующим подходом к построению VPN являются чисто программные решения. При реализации такого решения используется специализированное программное обеспечение, которое работает на выделенном компьютере и в большинстве случаев выполняет роль proxy-сервера. Компьютер с таким программным обеспечением может быть расположен за брандмауэром.

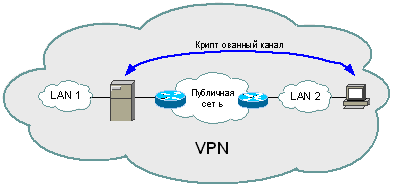


Рисунок 4. VPN на базе программного обеспечения

В качестве примера такого решения можно выступает программное обеспечение AltaVista Tunnel 97 компании Digital. При использовании данного ПО клиент подключается к серверу Tunnel 97, аутентифицируется на нем и обменивается ключами. Шифрация производится на базе 56 или 128 битных ключей Rivest-Cipher 4, полученных в процессе установления соединения. Далее, зашифрованные пакеты инкапсулируются в другие IP-пакеты, которые в свою очередь отправляются на сервер. В ходе работы Tunnel 97 осуществляет проверку целостности данных по алгоритму MD5. Кроме того, данное ПО каждые 30 минут генерирует новые ключи, что значительно повышает защищенность соединения.

Положительными качествами AltaVista Tunnel 97 являются простота установки и удобство управления. Минусами данной системы можно считать нестандартную архитектуру (собственный алгоритм обмена ключами) и низкую производительность.

## VPN на базе сетевой ОС

Решения на базе сетевой ОС мы рассмотрим на примере системы Windows NT компании Microsoft. Для создания VPN Microsoft использует протокол PPTP, который интегрирован в систему Windows NT. Данное решение очень привлекательно для организаций использующих Windows в качестве корпоративной операционной системы. Необходимо отметить, что стоимость такого решения значительно ниже стоимости прочих решений. В работе VPN на базе Windows NT используется база пользователей NT, хранящаяся на Primary Domain Controller (PDC). При подключении к PPTP-серверу пользователь аутентифицируется по протоколам PAP, CHAP или MS-CHAP. Передаваемые пакеты инкапсулируются в пакеты GRE/PPTP. Для шифрования пакетов используется нестандартный протокол от Microsoft Point-to-Point Encryption c 40 или 128 битным ключом, получаемым в момент установки соединения. Недостатками данной системы являются отсутствие проверки целостности данных и невозможность смены ключей во время соединения. Положительными моментами являются легкость интеграции с Windows и низкая стоимость.

## VPN на базе аппаратных средств

Вариант построения VPN на специальных устройствах может быть использован в сетях, требующих высокой производительности. Примером такого решения служит продукт cIPro-VPN компании Radguard

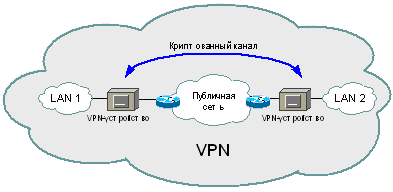


Рисунок 5. VPN на базе аппаратных средств

Данный продукт использует аппаратное шифрование передаваемой информации, способное пропускать поток в 100 Мбит/с. cIPro-VPN поддерживает протокол IPSec и механизм управления ключами ISAKMP/Oakley. Помимо прочего, данное устройство поддерживает средства трансляции сетевых адресов и может быть дополнено специальной платой, добавляющей функции брандмауэра

# Проблемы в VPN

Основной проблемой сетей VPN является отсутствие устоявшихся стандартов аутентификации и обмена шифрованной информацией. Эти стандарты все еще находятся в процессе разработки и потому продукты различных производителей не могут устанавливать VPN-соединения и автоматически обмениваться ключами. Данная проблема влечет за собой замедление распространения VPN, так как трудно заставить различные компании пользоваться продукцией одного производителя, а потому затруднен процесс объединения сетей компаний-партнеров в, так называемые, extranet-сети.

Как можно заметить из вышесказанного, продукты построения VPN могут оказаться узким местом в сети. Это происходит из-за того, что для поддержки множества соединений и шифрования информации, передаваемой по этим соединениям, требуется высокая производительность используемого оборудования (и/или программного обеспечения). Это является еще одним проблемным моментом в построении VPN.

Еще одним уязвимым местом VPN можно считать отсутствие единых, надежных способов управления такими сетями, что может стать кошмаром для сетевых администраторов.

И, наконец, отсутствие (или слабое развитие) механизмов обеспечения качества сервиса в сети Internet является проблемой построения сетей VPN, требующих для некоторых приложений гарантированной доставки информации за ограниченное время.

# Что ждать в будущем

Чего же можно ожидать в плане развития технологий VPN в будущем? Без всякого сомнения, будет выработан и утвержден единый стандарт построения подобных сетей. Скорее всего, основой этого стандарта будет, уже зарекомендовавший себя протокол IPSec. Далее, производители сконцентрируются на повышении производительности своих продуктов и на создании удобных средств управления VPN.

Скорее всего, развитие средств построения VPN будет идти в направлении VPN на базе маршрутизаторов, так как данное решение сочетает в себе достаточно высокую производительность, интеграцию VPN и маршрутизации в одном устройстве. Однако, будут развиваться и недорогие решения на базе сетевых ОС для небольших организаций.

В заключение, надо сказать, что, несмотря на то, что технология VPN еще очень молода, ее ожидает большое будущее. Так как уже в настоящее время она пользуется большим успехом среди разнообразных технических решений, для соединения различных частей фирмы/предприятия в единую сеть с хорошей степенью защищенности канала.