**Тема: Программное обеспечение виртуальных частных сетей (VPN): Структура VPN. Классификация VPN.**

**Введение**

   В последнее время в мире телекоммуникаций наблюдается повышенный интерес к 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. 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.

Кроме того, очень часто современному человеку, развивая свой бизнес, приходится много путешествовать. Это могут быть поездки в отдаленные уголки нашей страны или в страны зарубежья. Нередко людям нужен доступ к своей информации, хранящейся на их домашнем компьютере, или на компьютере фирмы. Эту проблему можно решить, организовав удалённый доступ к нему с помощью модема и телефонной линии. Использование телефонной линии имеет свои особенности. Недостатки этого решения в том, что звонок с другой страны стоит немалых денег. Есть и другое решение под названием VPN. Преимущества технологии VPN в том, что организация удалённого доступа делается не через телефонную линию, а через Internet, что намного дешевле и лучше.

**1. Понятие и классификация VPN сетей, их построение**

**1.1 Что такое VPN**

VPN (англ. Virtual Private Network - виртуальная частная сеть) - логическая сеть, создаваемая поверх другой сети, например, Internet. Несмотря на то, что коммуникации осуществляются по публичным сетям с использованием небезопасных протоколов, за счёт шифрования создаются закрытые от посторонних каналов обмена информацией. VPN позволяет объединить, например, несколько офисов организации в единую сеть с использованием для связи между ними неподконтрольных каналов.

   По своей сути VPN обладает многими свойствами выделенной линии, однако развертывается она в пределах общедоступной сети, например, Интернета. С помощью методики туннелирования пакеты данных транслируются через общедоступную сеть как по обычному двухточечному соединению. Между каждой парой «отправитель-получатель данных» устанавливается своеобразный туннель - безопасное логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого.

 Основными компонентами туннеля являются:

• инициатор

• маршрутизируемая сеть;

• туннельный коммутатор;

• один или несколько туннельных терминаторов.

    Сам по себе принцип работы VPN не противоречит основным сетевым технологиям и протоколам. Например, при установлении соединения удаленного доступа клиент посылает серверу поток пакетов стандартного протокола PPP. В случае организации виртуальных выделенных линий между локальными сетями их маршрутизаторы также обмениваются пакетами PPP. Тем не менее, принципиально новым моментом является пересылка пакетов через безопасный туннель, организованный в пределах общедоступной сети.

    Туннелирование позволяет организовать передачу пакетов одного протокола в логической среде, использующей другой протокол. В результате появляется возможность решить проблемы взаимодействия нескольких разнотипных сетей, начиная с необходимости обеспечения целостности и конфиденциальности передаваемых данных и заканчивая преодолением несоответствий внешних протоколов или схем адресации.

Существующая сетевая инфраструктура корпорации может быть подготовлена к использованию VPN как с помощью программного, так и с помощью аппаратного обеспечения. Организацию виртуальной частной сети можно сравнить с прокладкой кабеля через глобальную сеть. Как правило, непосредственное соединение между удаленным пользователем и оконечным устройством туннеля устанавливается по протоколу PPP.

Наиболее распространенный метод создания туннелей VPN - инкапсуляция сетевых протоколов (IP, IPX, AppleTalk и т.д.) в PPP и последующая инкапсуляция образованных пакетов в протокол туннелирования. Обычно в качестве последнего выступает IP или (гораздо реже) ATM и Frame Relay. Такой подход называется туннелированием второго уровня, поскольку «пассажиром» здесь является протокол именно второго уровня.

Альтернативный подход - инкапсуляция пакетов сетевого протокола непосредственно в протокол туннелирования (например, VTP) называется туннелированием третьего уровня.

Независимо от того, какие протоколы используются или какие цели преследуются при организации туннеля, основная методика остается практически неизменной.

Обычно один протокол используется для установления соединения с удаленным узлом, а другой - для инкапсуляции данных и служебной информации с целью передачи через туннель.

**1.2 Классификация VPN сетей**

Классифицировать VPN решения можно по нескольким основным параметрам:

**1. По типу используемой среды:**

• Защищённые VPN сети. Наиболее распространённый вариант приватных частных сетей. C его помощью возможно создать надежную и защищенную подсеть на основе ненадёжной сети, как правило, Интернета. Примером защищённых VPN являются: IPSec, OpenVPN и PPTP.

• Доверительные VPN сети. Используются в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети. Вопросы обеспечения безопасности становятся неактуальными. Примерами подобных VPN решении являются: MPLS и L2TP. Корректнее сказать, что эти протоколы перекладывают задачу обеспечения безопасности на другие, например, L2TP, как правило, используется в паре с IPSec.

**2. По способу реализации:**

• VPN сети в виде специального программно-аппаратного обеспечения. Реализация VPN сети осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости.

• VPN сети в виде программного решения. Используют персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN.

• VPN сети с интегрированным решением. Функциональность VPN обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.

**3. По назначению:**

• Intranet VPN. Используют для объединения в единую защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи.

• Remote Access VPN. Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера или, находясь в командировке, подключается к корпоративным ресурсам при помощи ноутбука.

• Extranet VPN. Используют для сетей, к которым подключаются «внешние» пользователи (например, заказчики или клиенты). Уровень доверия к ним намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных «рубежей» защиты, предотвращающих или ограничивающих доступ последних к особо ценной, конфиденциальной информации.

**4. По типу протокола:**

Существуют реализации виртуальных частных сетей под TCP/IP, IPX и AppleTalk. Но на сегодняшний день наблюдается тенденция к всеобщему переходу на протокол TCP/IP, и абсолютное большинство VPN решений поддерживает именно его.

**5. По уровню сетевого протокола:**

По уровню сетевого протокола на основе сопоставления с уровнями эталонной сетевой модели ISO/OSI.

**1.3. Построение 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 трафик, проходящий через брандмауэр шифруется. К программному обеспечению собственно брандмауэра добавляется модуль шифрования. Недостатком этого 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.

• 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.

Примером оборудования для построения VPN на маршрутизаторах является оборудование компании Cisco Systems. Начиная с версии программного обеспечения IOS 11.3, 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.

Для повышения производительности маршрутизатора может быть использован дополнительный модуль шифрования ESA. 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 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.

В качестве примера такого решения можно выступает программное обеспечение AltaVista Tunnel 97 компании Digital. При использовании данного программного обеспечения клиент подключается к серверу Tunnel 97, аутентифицируется на нем и обменивается ключами. Шифрация производится на базе 56 или 128 битных ключей, полученных в процессе установления соединения. Далее, зашифрованные пакеты инкапсулируются в другие IP-пакеты, которые в свою очередь отправляются на сервер. Кроме того, данное программное обеспечение 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 компании Microsoft. Для создания VPN Microsoft использует протокол PPTP, который интегрирован в систему Windows. 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 используется база пользователей NT, хранящаяся на Primary Domain Controller (главный контроллер домена) (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 c IPro-VPN компании Radguard. Данный продукт использует аппаратное шифрование передаваемой информации, способное пропускать поток в 100 Мбит/с. IPro-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.