ЛЕКЦИЯ
«ТЕХНОЛОГИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ (VPN)»

ВОПРОСЫ ЛЕКЦИИ

1. VPN – Виртуальные частные сети
2. Основы туннелирования и протоколирования
3. Достоинства и недостатки VPN
4. Перспективы VPN
5. Как построить VPN

ЛИТЕРАТУРА:

1. Александр Барсков, Говорим WAN, подразумеваем VPN / «Журнал сетевых решений/LAN», № 06, 2010.

2. Запечников, С. В. Основы построения виртуальных частных сетей: Учебное пособие для вузов / С.В. Запечников, Н.Г. Милославская, А.И. Толстой. - Москва : Гор. линия-Телеком, 2011. - 249 с. (Специальность). ISBN 5-93517-139-2, 3000 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/563048

В современном мире информационных технологий и, в частности, сети Internet, приходит необходимость защиты информации, передаваемой в рамках распределенной корпоративной сети, использующей сети открытого доступа. При использовании своих собственных физических каналов доступа эта проблема так остро не стоит, так как в эту сеть не имеет доступа никто из посторонних. Однако стоимость таких каналов высока, поэтому не каждая компания позволит себе использовать их. В связи с этим Internet является наиболее доступным. Internet является незащищенной сетью, поэтому

приходиться изобретать способы защиты конфиденциальных данных, передаваемых по незащищенной сети.

VPN — это технология, которая объединяет доверенные сети, узлы и пользователей через открытые сети, к которым нет доверия. На первый взгляд, это наиболее яркий образ технологии, которая получает все большее распространение не только среди технических специалистов, но и среди рядовых пользователей, которым также требуется защищать свою информацию (например, пользователи Internet-банков или Internet-порталов).

Специалисты в области технологии VPN используют сугубо технические понятия, такие как "используемый алгоритм криптографического преобразования", "туннелирование", "сервер сертификатов" и т.д. Но для конечных пользователей эта терминология ничего не скажет. Скорее их интересует несколько иная интерпретация вопросов - сколько лет можно не беспокоиться за сохранность своей информации и насколько медленнее будет работать сеть, защищенная с помощью VPN-устройства.

1. VPN – Виртуальные частные сети

Любая организация, будь она производственной, торговой, финансовой компании или государственным учреждением, обязательно сталкивается с вопросом передачи информации между своими филиалами, а также с вопросом защиты этой информации. Не каждая фирма может себе позволить иметь собственные физические каналы доступа, и здесь помогает технология VPN, на основе которой и соединяются все подразделения и филиалы, что обеспечивает достаточную гибкость и одновременно высокую безопасность сети, а также существенную экономию затрат.

Виртуальная частная сеть (VPN - VirtualPrivateNetwork) создается на базе общедоступной сети Интернет. И если связь через Интернет имеет свои

недостатки, главным из которых является то, что она подвержена потенциальным нарушениям защиты и конфиденциальности, то VPN могут гарантировать, что направляемый через Интернет трафик так же защищен, как и передача внутри локальной сети. В тоже время виртуальные сети обеспечивают существенную экономию затрат по сравнению с содержанием собственной сети глобального масштаба.

История появления VPN тесно связана с услугой Centrex в телефонных сетях. Понятие Centrex появилось на рубеже шестидесятых годов в США как общее название способа предоставления услуг деловой связи абонентам нескольких компаний на основе совместно используемого оборудования одной учрежденческой станции PBX (PrivateBranchExchange). С началом внедрения в США и Канаде станций с программным управлением термин приобрел иной смысл и стал означать способ предоставления деловым абонентам дополнительных услуг телефонной связи, эквивалентных услугам PBX, на базе модифицированных станций сети общего пользования. Основное преимущество Centrex заключалось в том, что фирмы и компании при создании выделенных корпоративных сетей экономили значительные средства, необходимые на покупку, монтаж и эксплуатацию собственных станций. Хотя для связи между собой абоненты Centrex используют ресурсы и оборудование сети общего пользования, сами они образуют так называемые замкнутые группы пользователей CUG (ClosedUsersGroup) с ограниченным доступом извне, для которых в станциях сети реализуются виртуальные PBX.

В стремлении преодолеть свойственные Centrex ограничения была выдвинута идея виртуальной частной сети VPN - как объединение CUG, составляющих одну корпоративную сеть и находящихся на удалении друг от друга

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.

VPN-устройство располагается между внутренней сетью и Интернет на каждом конце соединения. Когда данные передаются через VPN, они исчезают «с поверхности» в точке отправки и вновь появляются только в точке назначения. Этот процесс принято называть «туннелированием». Это означает создание логического туннеля в сети Интернет, который соединяет две крайние точки. Благодаря туннелированию частная информация становится невидимой для других пользователей Интернета. Прежде чем попасть в интернет-туннель, данные шифруются, что обеспечивает их дополнительную защиту. Протоколы шифрования бывают разные. Все зависит от того, какой протокол туннелирования поддерживается тем или иным VPN-решением. Еще одной важной характеристикой VPN-решений является диапазон поддерживаемых протоколов аутентификации. Большинство популярных продуктов работают со стандартами, основанными на использовании открытого ключа, такими как X.509. Это означает, что, усилив свою виртуальную частную сеть соответствующим протоколом аутентификации, вы сможете гарантировать, что доступ к вашим защищенным туннелям получат только известные вам люди (рисунок 1).

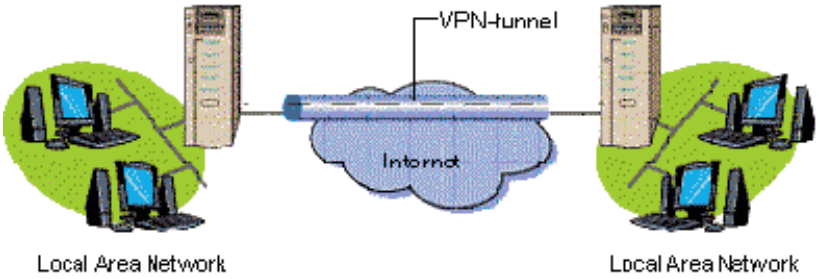

Рисунок 1 – Принцип работы технологии VPN

Сегодня технология VPN (VirtualPrivateNetwork - виртуальная частная сеть) завоевала всеобщее признание и любой администратор считает своим долгом организовать VPN-каналы для сотрудников, работающих вне офиса (рисунок 2).

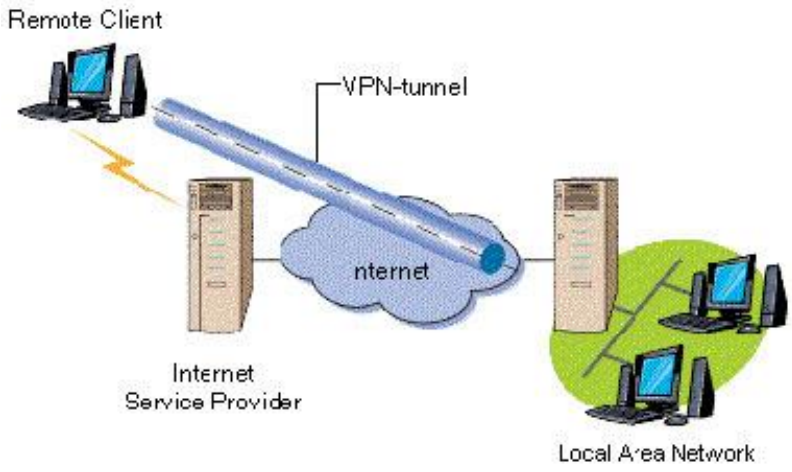

Рисунок 2 – VPN для удаленных пользователей

VPN (рисунок 3) представляет собой объединение отдельных машин или локальных сетей в виртуальной сети, которая обеспечивает целостность и безопасность передаваемых данных. Она обладает свойствами выделенной частной сети и позволяет передавать данные между двумя компьютерами через промежуточную сеть (internetwork), например Internet.

VPN отличается рядом экономических преимуществ по сравнению с другими методами удаленного доступа. Во-первых, пользователи могут обращаться к корпоративной сети, не устанавливая с ней коммутируемое соединение, таким образом, отпадает надобность в использовании модемов. Во-вторых, можно обойтись без выделенных линий (рисунок 3).

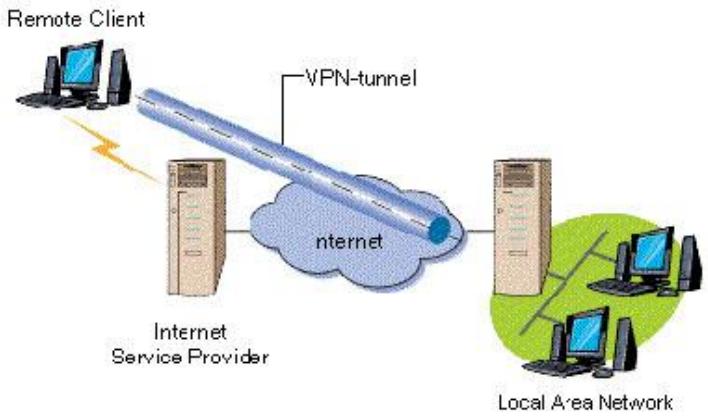

Рисунок 3 – VPN для двух офисных сетей

Имея доступ в Интернет, любой пользователь может без проблем подключиться к сети офиса своей фирмы. Следует заметить, что общедоступность данных совсем не означает их незащищенность. Система безопасности VPN — это броня, которая защищает всю корпоративную информацию от несанкционированного доступа. Прежде всего, информация передается в зашифрованном виде. Прочитать полученные данные может лишь обладатель ключа к шифру. Наиболее часто используемым алгоритмом кодирования является Triple DES, который обеспечивает тройное шифрование (168 разрядов) с использованием трех разных ключей.

Triple DES (3DES) — симметричный блочный шифр, созданный УитфилдомДиффи, Мартином Хеллманом и Уолтом Тачманном в 1978 году на основе алгоритма DES с целью устранения главного недостатка последнего — малой длины ключа (56 бит), который может быть взломан методом полного перебора ключа. Скорость работы 3DES в 3 раза ниже, чем у DES, но криптостойкость намного выше — время, требуемое для криптоанализа 3DES, может быть в миллиард раз больше, чем время, нужное для вскрытия DES. 3DES используется чаще, чем DES, который легко взламывается при помощи сегодняшних технологий (в 1998 году организация ElectronicFrontierFoundation, используя специальный компьютер DES Cracker, вскрыла DES за 3 дня). 3DES является простым способом устранения недостатков DES. Алгоритм 3DES построен на основе DES,

поэтому для его реализации возможно использовать программы, созданные для DES. Официальное название алгоритма, используемое в стандартах - TDEA или Triple DEA (англ. TripleDataEncryptionAlgorithm). Однако, термин "3DES" используется более широко поставщиками, пользователями и разработчиками криптосистем.

Подтверждение подлинности включает в себя проверку целостности данных и идентификацию пользователей, задействованных в VPN. Первая гарантирует, что данные дошли до адресата именно в том виде, в каком были посланы. Самые популярные алгоритмы проверки целостности данных - MD5 и SHA1.

MD5 — 128-битный алгоритм хеширования, разработанный профессором Рональдом Л. Ривестом из Массачусетского технологического института в 1991 году. Предназначен для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности.

Далее система проверяет, не были ли изменены данные во время движения по сетям, по ошибке или злонамеренно. Таким образом, построение VPN предполагает создание защищенных от постороннего доступа туннелей между несколькими локальными сетями или удаленными пользователями.

Для построения VPN необходимо иметь на обоих концах линии связи программы шифрования исходящего и дешифрования входящего трафиков. Они могут работать как на специализированных аппаратных устройствах, так и на ПК с такими операционными системами как Windows, Linux или NetWare.

Управление доступом, аутентификация и шифрование - важнейшие элементы защищенного соединения.

2. Основы туннелирования и протоколирования

Туннелирование (tunneling), или инкапсуляция (encapsulation), — это способ передачи полезной информации через промежуточную сеть. Такой информацией могут быть кадры (или пакеты) другого протокола. При инкапсуляции кадр не передается в сгенерированном узлом-отправителем виде, а снабжается дополнительным заголовком, содержащим информацию о маршруте, позволяющую инкапсулированным пакетам проходить через промежуточную сеть (Internet). На конце туннеля кадры деинкапсулируются и передаются получателю.

Этот процесс (включающий инкапсуляцию и передачу пакетов) и есть туннелирование. Логический путь передвижения инкапсулированных пакетов в транзитной сети называется туннелем.

Протокол VPN определяет, каким образом система VPN взаимодействует с другими системами в интернете, а также уровень защищенности трафика. Если рассматриваемая организация использует VPN только для внутреннего информационного обмена, вопрос о взаимодействии можно оставить без внимания. Однако если организация использует VPN для соединения с другими организациями, собственные протоколы использовать, скорее всего, не удастся. В разговоре об алгоритме шифрования было упомянуто, что внешние окружающие факторы могут оказывать большее влияние на безопасность системы, чем алгоритм шифрования. Протокол VPN оказывает влияние на общий уровень безопасности системы. Причиной этому является тот факт, что протокол VPN используется для обмена ключами шифрования между двумя конечными узлами. Если этот обмен не защищен, злоумышленник может перехватить ключи и затем расшифровать трафик, сведя на нет все преимущества VPN.

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 InternetProtocolSecurity (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-PointTunnelingProtocol), разработанный компаниями AscendCommunications и 3Com, L2F (Layer-2 Forwarding) - компании CiscoSystems и L2TP (Layer-2 TunnelingProtocol), объединивший оба вышеназванных протокола. Однако эти протоколы, в отличие от IPSec, не являются полнофункциональными (например, PPTP не определяет метод шифрования)

Говоря об IPSec, нельзя забывать о протоколе IKE (InternetKeyExchange), 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, какIPSec 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.

Инкапсуляция - обеспечивает мультиплексирование нескольких транспортных протоколов по одному каналу;

Протокол LCP - PPP задает гибкий LCP для установки, настройки и проверки канала связи. LCP обеспечивает согласование формата инкапсуляции, размера пакета, параметры установки и разрыва соединения, а

также параметры аутентификации. В качестве протоколов аутентификации могут использоваться PAP, CHAP и др.;

Протоколы управления сетью - предоставляют специфические конфигурационные параметры для соответствующих транспортных протоколов. Например, IPCP протокол управления IP.

Для формирования туннелей VPN используются протоколы PPTP, L2TP, IPsec, IP-IP.

Протокол PPTP - позволяет инкапсулировать IP-, IPX- и NetBEUI-трафик в заголовки IP для передачи по IP-сети, например Internet.

Протокол L2TP - позволяет шифровать и передавать IP-трафик с использованием любых протоколов, поддерживающих режим “точка-точка” доставки дейтаграмм. Например, к ним относятся протокол IP, ретрансляция кадров и асинхронный режим передачи (ATM).

Протокол IPsec - позволяет шифровать и инкапсулировать полезную информацию протокола IP в заголовки IP для передачи по IP-сетям.

Протокол IP-IP - IP-дейтаграмма инкапсулируется с помощью дополнительного заголовка IP. Главное назначение IP-IP - туннелирование многоадресного трафика в частях сети, не поддерживающих многоадресную маршрутизацию.

Для технической реализации VPN, кроме стандартного сетевого оборудования, понадобится шлюз VPN, выполняющий все функции по формированию туннелей, защите информации, контролю трафика, а нередко и функции централизованного управления.

На сегодняшний день VPN — это экономичное, надежное и общедоступное решение организации удаленного доступа. Каким бы ни было расстояние, VPN обеспечит соединение с любой точкой мира и сохранность передачи самых важных данных.

3. Достоинства и недостатки VPN

Виртуальные частные сети имеют несколько преимуществ над традиционными частными сетями. Главные из них - экономичность, гибкость и удобство использования.

Экономичность. С помощью VPN-сетей предприятиям удается хотя бы частично ограничить рост числа модемов, серверов доступа, коммутируемых линий и других технических средств, которые организации вынуждены внедрять, чтобы обеспечить удаленным пользователям доступ к своим корпоративным сетям. Кроме того, виртуальные частные сети дают возможность удаленным пользователям обращаться к сетевым ресурсам компании не по дорогим арендованным линиям, а через местную телефонную связь.

Особенно выгодны виртуальные частные сети в тех случаях, когда пользователи удалены на большие расстояния и поэтому арендованные линии обходятся очень дорого, а также когда таких пользователей много, в связи с чем и им требуется большое количество арендованных линий. Однако эти преимущества могут сойти на нет, если объем трафика в VPN-сети настолько велик, что система не успевает зашифровывать и расшифровывать пакеты данных. Чтобы избежать возникновения таких узких мест, предприятие вынуждено покупать дополнительное оборудование.

Кроме того, из-за относительной новизны технологии VPN и сложности используемых средств безопасности системный администратор для виртуальной сети обходится дороже, чем для традиционной.

Исследовательская компания ForresterResearch опубликовала следующие данные, характеризующие преимущество применения VPN поверх Internet (из расчета 1000 пользователей) по сравнению с созданием центра удаленного доступа (RemoteAccessService).

Таблица 1

Преимущество применения VPN поверх Internet

Статья затрат	Удаленный доступ (в млн. долл.)	VPN(в млн. долл.)
Оплата услуг провайдера связи	1,08	0,54
Расходы на эксплуатацию	0,3	0,3
Капиталовложения	0,1	0,02
Прочие расходы	0,02	0,03
Всего	1,5	0,89

Из таблицы можно видеть, что использование VPN позволяет снизить многие статьи затрат, включая закупку коммуникационного оборудования, оплату услуг Internet-провайдера и т.д. Эти, а также другие исследования, позволили Международной Ассоциации Компьютерной Безопасности (InternationalComputerSecurityAssociation, ICSA) причислить технологию VPN к десятке самых известных технологий, которые будут в первую очередь применяться многими компаниями. Это подтверждает и компания GartnerGroup, которая в одном из своих отчетов предсказала, что средства построения VPN будут применяться в 2002 г. в 90% компаний. Именно с этим связан прогноз рынка средств VPN, который исчисляется 11,94 миллиардами долларов в 2002 году и 18,77 миллиардами в 2004 году (по данным Frost&Sullivan).

Гибкость и удобство. Эти достоинства виртуальных частных сетей объясняются тем, что в отличие от традиционных такие сети могут обеспечить удаленный доступ к ресурсам компании любому уполномоченному пользователю, имеющему связь с Internet. Благодаря этому VPN-сети позволяют партнерам легко получить доступ к сетевым ресурсам предприятия через Internet, что способствует укреплению альянсов и повышению конкурентоспособности. Этого трудно достичь с помощью традиционных частных сетей, так как предприятия, желающие совместно

использовать сетевые ресурсы, часто имеют несовместимые системы. Особенно остро эта проблема возникает, когда большое число организаций, таких как крупное предприятие розничной торговли и его поставщики, хотят работать вместе через сеть.

Проблемы защиты данных, недостаток надежности и производительности, а также отсутствие открытых стандартов затрудняют широкое распространение виртуальных частных сетей.

Защита. Для большинства технологий Internet вопросы обеспечения безопасности при передаче данных являются ключевыми. И виртуальные частные сети не исключение. Для них главные проблемы заключаются в аутентификации пользователей с помощью паролей и защите зашифрованного VPN-канала (тоннеля). Кроме того, сетевые администраторы должны тщательно выбирать методы, которые помогают пользователям получать доступ к виртуальным частным сетям.

Эти проблемы заставили некоторых потенциальных пользователей усомниться в том, что степень защиты данных будет удовлетворительной, если виртуальной частной сетью управляет провайдер услуг Internet. Чтобы успокоить недоверчивых пользователей, провайдеры поддерживают широкий набор различных схем шифрования и аутентификации. Например, фирма Aventail, выпускающая ПО для виртуальных частных сетей, предлагает пакет программ для аутентификации клиентов и шифрования на уровне сеанса. Компания VPNetTechnologies поставляет оборудование, устанавливаемое между маршрутизатором и глобальной сетью, которое выполняет шифрование, аутентификацию и сжатие данных.

Большинство поставщиков используют методы шифрования с 56-разрядным ключом, соответствующие стандарту DES. По их мнению, такая длина ключа обеспечивает достаточно высокий уровень безопасности. Однако многие эксперты и аналитики полагают, что 56-разрядный ключ недостаточно надежен. Некоторые поставщики продуктов для виртуальных

частных сетей предлагают шифрование со 112-разрядным ключом. Тем не менее следует помнить, что увеличение длины ключа снижает производительность, так как чем сложнее алгоритм шифрования, тем более интенсивной вычислительной обработки он требует.

4. Перспективы VPN

По мере своего развития VPN превратятся в системы взаимосвязанных сетей, которые будут соединять мобильных пользователей, торговых партнеров и поставщиков с критически важными корпоративными приложениями, работающими в протоколе IP. VPN станут фундаментом для новых коммерческих операций и услуг, которые будут стимулировать рынок и помогать модернизировать производство.

Вероятно, первым из основных компонентов завтрашних VPN станет сервер каталогов, содержащий профили конечных пользователей и данные о конфигурации сети. Это отдельная компьети, управляемая провайдером VPN. При наличии сетевых каталогов и обеспечении безопасности информации и качества обслуживания конечные пользователи смогут практически мгновенно устанавливать соединения по VPN.

Вполне возможно, что будет использоваться протокол IpV6, работы над которым активно продолжаются. Данный протокол обладает всеми возможностями взаимодействия с VPN, какие только могут пожелать сетевые разработчики, в частности, управление полосой пропускания, определение принадлежности IpV6-пакетов к конкретному потоку (например, высший приоритет будут получать пакеты мультимедийных данных для передачи в реальном времени).

Главные игроки сетевого рынка уже активно готовятся к грядущему буму VPN. Нынешние вендоры программного обеспечения и оборудования предлагают наборы устройств для создания и эксплуатации VPN.

Выгоду от развертывания VPN следующего поколения получат не только сетевые разработчики. Не менее заинтересованы в них и операторы. Фирмы AT&T Level 3 Communications, MCI Worldcom и Sprint создают высокоскоростные IP-каналы в ATM-сетях для передачи видео, голоса и данных. VPN в настоящее время оказывают едва ли не решающее влияние на разработку стратегии глобальных операторов, в частности, Unisource (AT&T, Telia, PTT Suisse и PTT Netherlands), Concert (BT/MCI) и GlobalOne (DeutscheTelekom, FranceTelekom). Чем больше компаний будут предлагать VPN-услуги, тем заметнее будет расти их качество и падать цены, что, в свою очередь, повлияет на число клиентов.

Каждая революция в бизнесе начиналась с изобретения, которое способствовало активизации частной инициативы. Например, разделение перевозчиков и компаний, эксплуатирующих государственную железную дорогу, привело к резкому росту коммерческих перевозок. То же самое происходит при создании VPN поверх национальных и международных телекоммуникационных инфраструктур. Ближайшее время покажет, к каким изменениям это приведет.

5. 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 4).

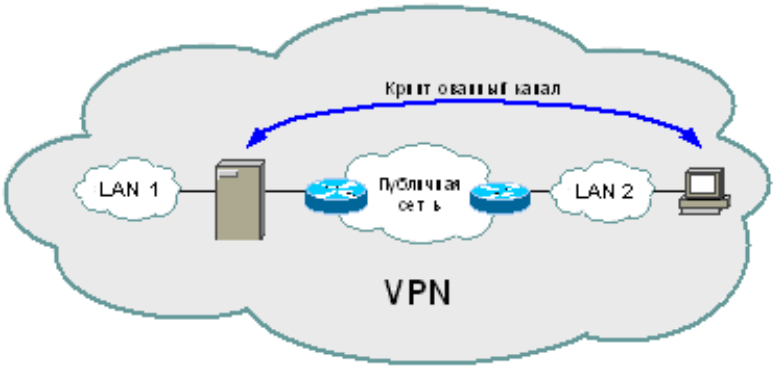

Рисунок 4 – VPN на базе брандмауэра

В качестве примера решения на базе брандмауэров можно назвать FireWall-1 компании CheckPointSoftwareTechnologies. 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 CiscoSystems. 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 5).

Рисунок 5 – 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 (EncryptionServiceAdapter).

Кроме того, компания CiscoSystem выпустила специализированное устройство для VPN, которое так и называется Cisco 1720 VPN AccessRouter (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 6).

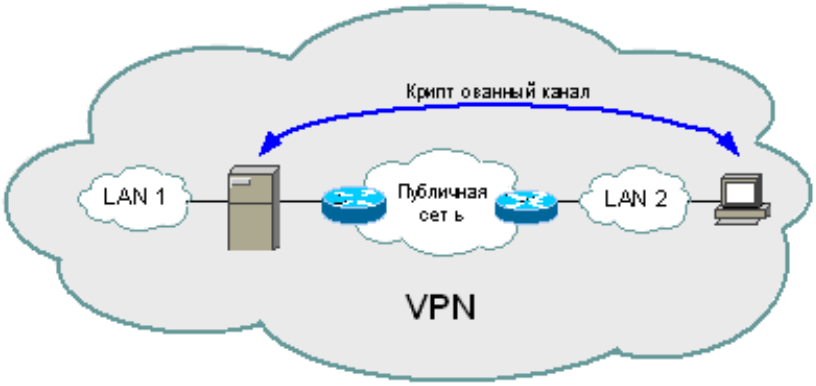

Рисунок 6 – VPN на базе программного обеспечения

В качестве примера такого решения можно выступает программное обеспечение AltaVistaTunnel 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 AltaVistaTunnel 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 PrimaryDomainController (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 MicrosoftPoint-to-PointEncryption с 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 7).

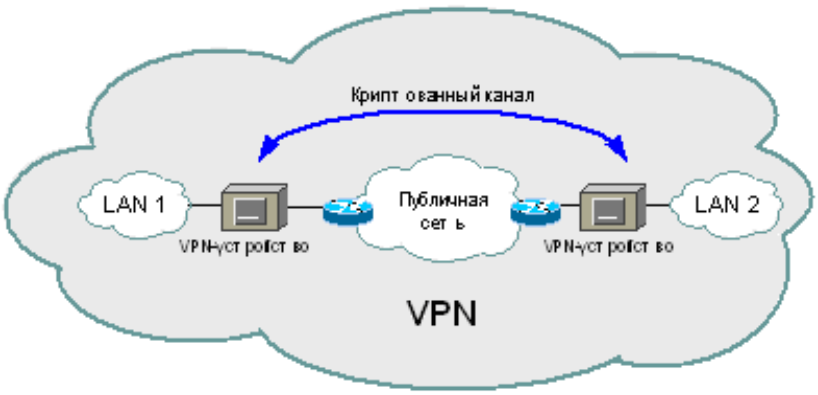

Рисунок 7 – VPN на базе аппаратных средств

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.