VPN

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 каналы 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.

Реализация виртуальной частной сети на практике выглядит следующим образом. В локальной вычислительной сети офиса фирмы устанавливается сервер *VPN*. Удаленный пользователь (или маршрутизатор, если осуществляется соединение двух офисов) с использованием клиентского программного обеспечения *VPN* инициирует процедуру соединения с сервером. Происходит аутентификация пользователя - первая фаза установления *VPN*-соединения. В случае подтверждения полномочий наступает вторая фаза - между клиентом и сервером выполняется согласование деталей обеспечения безопасности соединения. После этого организуется *VPN*-соединение, обеспечивающее обмен информацией между клиентом и сервером в форме, когда каждый пакет с данными проходит через процедуры шифрования/дешифрования и проверки целостности - аутентификации данных.

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. С 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*.
- *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 играет роль proxy-сервера. Компьютер с таким программным обеспечением может быть расположен за брандмауэром.
- *VPN* на базе сетевой ОС.
- *VPN* на базе аппаратных средств. Вариант построения *VPN* на специальных устройствах может быть использован в сетях, требующих высокой производительности.

2. Основные составляющие и протоколы *VPN* сетей

Виртуальная частная сеть базируется на реализации трех составляющих:

· Туннелирование;
· Шифрование;
· Аутентификация.

Туннелирование обеспечивает передачу данных между двумя точками - окончаниями туннеля - таким образом, что для источника и приемника данных оказывается скрытой вся сетевая инфраструктура, лежащая между ними.

Транспортная среда туннеля, как паром, подхватывает пакеты используемого сетевого протокола у входа в туннель и без изменений доставляет их к выходу. Построения туннеля достаточно для того, чтобы соединить два сетевых узла так, что с точки зрения работающего на них программного обеспечения они выглядят подключенными к одной (локальной) сети. Однако нельзя забывать, что на самом деле «паром» с данными проходит через множество промежуточных узлов (маршрутизаторов) открытой публичной сети.

Такое положение дел таит в себе две проблемы. Первая заключается в том, что передаваемая через туннель информация может быть перехвачена злоумышленниками. Если она конфиденциальна (номера банковских карточек, финансовые отчеты, сведения личного характера), то вполне реальна угроза ее компрометации, что уже само по себе неприятно. Хуже того, злоумышленники имеют возможность модифицировать передаваемые через туннель данные так, что получатель не сможет проверить их достоверность. Последствия могут быть самыми плачевными. Учитывая сказанное, мы приходим к выводу, что туннель в чистом виде пригоден разве что для некоторых типов сетевых компьютерных игр и не может претендовать на более серьезное применение. Обе проблемы решаются современными средствами криптографической защиты информации, в частности применяются различные методы аутентификации и шифрования.

Чтобы воспрепятствовать внесению несанкционированных изменений в пакет с данными на пути его следования по туннелю, используется метод электронной цифровой подписи. Суть метода состоит в том, что каждый передаваемый пакет снабжается дополнительным блоком информации, который вырабатывается в соответствии с асимметричным криптографическим алгоритмом и уникален для содержимого пакета и секретного ключа ЭЦП отправителя. Этот блок информации является ЭЦП пакета и позволяет выполнить аутентификацию данных получателем, которому известен открытый ключ ЭЦП отправителя. Защита передаваемых через туннель данных от несанкционированного просмотра достигается путем использования сильных алгоритмов шифрования.

С помощью 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.

Сети *VPN* строятся с использованием протоколов туннелирования данных через сеть связи общего пользования Интернет, причем протоколы туннелирования обеспечивают шифрование данных и осуществляют их сквозную передачу между пользователями. Как правило, на сегодняшний день для построения сетей *VPN* используются протоколы следующих уровней:

- Канальный уровень
- Сетевой уровень
- Транспортный уровень.

2.1 Канальный уровень

На канальном уровне могут использоваться протоколы туннелирования данных *L2TP* и *PPTP*, которые используют авторизацию и аутентификацию.

PPTP.

В настоящее время наиболее распространенным протоколом VPN является протокол двухточечной туннельной связи или Point-to-Point Tunnelling Protocol - PPTP. Разработан он компаниями 3Com и Microsoft с целью предоставления безопасного удаленного доступа к корпоративным сетям через Интернет. PPTP использует существующие открытые стандарты TCP/IP и во многом полагается на устаревший протокол двухточечной связи PPP. На практике PPP так и остается коммуникационным протоколом сеанса соединения PPTP. PPTP создает туннель через сеть к NT-серверу получателя и передает по нему PPP-пакеты удаленного пользователя. Сервер и рабочая станция используют виртуальную частную сеть и не обращают внимания на то, насколько безопасной или доступной является глобальная сеть между ними. Завершение сеанса соединения по инициативе сервера, в отличие от специализированных серверов удаленного доступа, позволяет администраторам локальной сети не пропускать удаленных пользователей за пределы системы безопасности Windows Server.

Хотя компетенция протокола PPTP распространяется только на устройства, работающие под управлением Windows, он предоставляет компаниям возможность взаимодействовать с существующими сетевыми инфраструктурами и не наносить вред собственной системе безопасности. Таким образом, удаленный пользователь может подключиться к Интернету с помощью местного провайдера по аналоговой телефонной линии или каналу ISDN и установить соединение с сервером NT. При этом компании не приходится тратить большие суммы на организацию и обслуживание пула модемов, предоставляющего услуги удаленного доступа.

Далее рассматривается работа PPTP. PPTP инкапсулирует пакеты IP для передачи по IP-сети. Клиенты PPTP используют порт назначения для создания управляющего туннелем соединения. Этот процесс происходит на транспортном уровне модели OSI. После создания туннеля компьютер-клиент и сервер начинают обмен служебными пакетами. В дополнение к управляющему соединению PPTP, обеспечивающему работоспособность канала, создается соединение для пересылки по туннелю данных. Инкапсуляция данных перед пересылкой через туннель происходит несколько иначе, чем при обычной передаче. Инкапсуляция данных перед отправкой в туннель включает два этапа:

1. Сначала создается информационная часть PPP. Данные проходят сверху вниз, от прикладного уровня OSI до канального.
2. Затем полученные данные отправляются вверх по модели OSI и инкапсулируются протоколами верхних уровней.

Таким образом, во время второго прохода данные достигают транспортного уровня. Однако информация не может быть отправлена по назначению, так как за это отвечает канальный уровень OSI. Поэтому PPTP шифрует поле полезной нагрузки пакета и берет на себя функции второго уровня, обычно принадлежащие PPP, т.е. добавляет к PPTP-пакету PPP-заголовок и окончание. На этом создание кадра канального уровня заканчивается.

Далее, PPTP инкапсулирует PPP-кадр в пакет Generic Routing Encapsulation (GRE), который принадлежит сетевому уровню. GRE инкапсулирует протоколы сетевого уровня, например IPX, AppleTalk, DECnet, чтобы обеспечить возможность их передачи по IP-сетям. Однако GRE не имеет возможности устанавливать сессии и обеспечивать защиту данных от злоумышленников. Для этого используется способность PPTP создавать соединение для управления туннелем. Применение GRE в качестве метода инкапсуляции ограничивает поле действия PPTP только сетями IP.

После того как кадр PPP был инкапсулирован в кадр с заголовком GRE, выполняется инкапсуляция в кадр с IP-заголовком. IP-заголовок содержит адреса отправителя и получателя пакета. В заключение PPTP добавляет PPP заголовок и окончание.

Система-отправитель посылает данные через туннель. Система-получатель удаляет все служебные заголовки, оставляя только данные PPP.

L2TP

L2TP появился в результате объединения протоколов PPTP и L2F (Layer 2 Forwarding). PPTP позволяет передавать через туннель пакеты PPP, а L2F-пакеты SLIP и PPP. Во избежание путаницы и проблем взаимодействия систем на рынке телекоммуникаций, комитет Internet Engineering Task Force (IETF) рекомендовал компании Cisco Systems объединить PPTP и L2F. По общему мнению, протокол L2TP вобрал в себя лучшие черты PPTP и L2F. Главное достоинство L2TP в том, что этот протокол позволяет создавать туннель не только в сетях IP, но и в таких, как ATM, X.25 и Frame Relay.

L2TP применяет в качестве транспорта протокол UDP и использует одинаковый формат сообщений как для управления туннелем, так и для пересылки данных. L2TP в реализации Microsoft использует в качестве контрольных сообщений пакеты UDP, содержащие шифрованные пакеты PPP. Надежность доставки гарантирует контроль последовательности пакетов.

Функциональные возможности PPTP и L2TP различны. L2TP может использоваться не только в IP-сетях, служебные сообщения для создания туннеля и пересылки по нему данных используют одинаковый формат и протоколы. PPTP может применяться только в IP-сетях, и ему необходимо отдельное соединение TCP для создания и использования туннеля. L2TP поверх IPSec предлагает больше уровней безопасности, чем PPTP, и может гарантировать почти 100-процентную безопасность важных для организации данных. Особенности L2TP делают его очень перспективным протоколом для построения виртуальных сетей.

Протоколы L2TP и PPTP отличаются от протоколов туннелирования третьего уровня рядом особенностей:

1. Предоставление корпорациям возможности самостоятельно выбирать способ аутентификации пользователей и проверки их полномочий - на собственной «территории» или у провайдера Интернет-услуг. Обрабатывая туннелированные пакеты PPP, серверы корпоративной сети получают всю информацию, необходимую для идентификации пользователей.
2. Поддержка коммутации туннелей - завершения одного туннеля и инициирования другого к одному из множества потенциальных терминаторов. Коммутация туннелей позволяет, как бы продлить PPP - соединение до необходимой конечной точки.
3. Предоставление системным администраторам корпоративной сети возможности реализации стратегий назначения пользователям прав доступа непосредственно на брандмауэре и внутренних серверах. Поскольку терминаторы туннеля получают пакеты PPP со сведениями о пользователях, они в состоянии применять сформулированные администраторами стратегии безопасности к трафику отдельных пользователей. (Туннелирование третьего уровня не позволяет различать поступающие от провайдера пакеты, поэтому фильтры стратегии безопасности приходится применять на конечных рабочих станциях и сетевых устройствах.) Кроме того, в случае использования туннельного коммутатора появляется возможность организовать «продолжение» туннеля второго уровня для непосредственной трансляции трафика отдельных пользователей к соответствующим внутренним серверам. На такие серверы может быть возложена задача дополнительной фильтрации пакетов.

· **MPLS**

Также на канальном уровне для организации туннелей может использоваться технология MPLS (От английского Multiprotocol Label Switching - мультипротокольная коммутация по меткам - механизм передачи данных, который эмулирует различные свойства сетей с коммутацией каналов поверх сетей с коммутацией пакетов). MPLS работает на уровне, который можно было бы расположить между канальным и третьим сетевым уровнями модели OSI, и поэтому его обычно называют протоколом канально-сетевого уровня. Он был разработан с целью обеспечения универсальной службы передачи данных как для клиентов сетей с коммутацией каналов, так и сетей с коммутацией пакетов. С помощью MPLS можно передавать трафик самой разной природы, такой как IP-пакеты, ATM, SONET и кадры Ethernet.

Решения по организации VPN на канальном уровне имеют достаточно ограниченную область действия, как правило, в рамках домена провайдера.

2.2 Сетевой уровень

Сетевой уровень (уровень IP). Используется протокол IPSec реализующий шифрование и конфедициальность данных, а также аутентификацию абонентов. Применение протокола IPSec позволяет реализовать полнофункциональный доступ эквивалентный физическому подключению к корпоративной сети. Для установления VPN каждый из участников должен сконфигурировать определенные параметры IPSec, т.е. каждый клиент должен иметь программное обеспечение реализующее IPSec.

IPSec

Естественно, никакая компания не хотела бы открыто передавать в Интернет финансовую или другую конфиденциальную информацию. Каналы VPN защищены мощными алгоритмами шифрования, заложенными в стандарты протокола безопасности IPsec. IPSec или Internet Protocol Security - стандарт, выбранный международным сообществом, группой IETF - Internet Engineering Task Force, создает основы безопасности для Интернет-протокола (IP/ Протокол IPSec обеспечивает защиту на сетевом уровне и требует поддержки стандарта IPSec только от общающихся между собой устройств по обе стороны соединения. Все остальные устройства, расположенные между ними, просто обеспечивают трафик IP-пакетов.

Способ взаимодействия лиц, использующих технологию IPSec, принято определять термином «защищенная ассоциация» - Security Association (SA). Защищенная ассоциация функционирует на основе соглашения, заключенного сторонами, которые пользуются средствами IPSec для защиты передаваемой друг другу информации. Это соглашение регулирует несколько параметров: IP-адреса отправителя и получателя, криптографический алгоритм, порядок обмена ключами, размеры ключей, срок службы ключей, алгоритм аутентификации.

IPSec - это согласованный набор открытых стандартов, имеющий ядро, которое может быть достаточно просто дополнено новыми функциями и протоколами. Ядро IPSec составляют три протокола:

· **AH** или Authentication Header - заголовок аутентификации - гарантирует целостность и аутентичность данных. Основное назначение протокола AH - он позволяет приемной стороне убедиться, что:

- пакет был отправлен стороной, с которой установлена безопасная ассоциация;
- содержимое пакета не было искажено в процессе его передачи по сети;
- пакет не является дубликатом уже полученного пакета.

Две первые функции обязательны для протокола AH, а последняя выбирается при установлении ассоциации по желанию. Для выполнения этих функций протокол AH использует специальный заголовок. Его структура рассматривается по следующей схеме:

1. В поле следующего заголовка (next header) указывается код протокола более высокого уровня, то есть протокола, сообщение которого размещено в поле данных IP-пакета.
2. В поле длины полезной нагрузки (payload length) содержится длина заголовка AH.
3. Индекс параметров безопасности (Security Parameters Index, SPI) используется для связи пакета с предусмотренной для него безопасной ассоциацией.
4. Поле порядкового номера (Sequence Number, SN) указывает на порядковый номер пакета и применяется для защиты от его ложного воспроизведения (когда третья сторона пытается повторно использовать перехваченные защищенные пакеты, отправленные реально аутентифицированным отправителем).

5. Поле данных аутентификации (authentication data), которое содержит так называемое значение проверки целостности (Integrity Check Value, ICV), используется для аутентификации и проверки целостности пакета. Это значение, называемое также дайджестом, вычисляется с помощью одной из двух обязательно поддерживаемых протоколом AH вычислительно необратимых функций MD5 или SAH-1, но может использоваться и любая другая функция.

· **ESP или Encapsulating Security Payload** - инкапсуляция зашифрованных данных - шифрует передаваемые данные, обеспечивая конфиденциальность, может также поддерживать аутентификацию и целостность данных;

Протокол ESP решает две группы задач.

1. К первой относятся задачи, аналогичные задачам протокола AH, - это обеспечение аутентификации и целостности данных на основе дайджеста,
2. Ко второй - защита передаваемых данных путем их шифрования от несанкционированного просмотра.

Заголовок делится на две части, разделяемые полем данных.

1. Первая часть, называемая собственно заголовком ESP, образуется двумя полями (SPI и SN), назначение которых аналогично одноименным полям протокола AH, и размещается перед полем данных.
2. Остальные служебные поля протокола ESP, называемые концевиком ESP, расположены в конце пакета.

Два поля концевика - следующего заголовка и данных аутентификации - аналогичны полям заголовка AH. Поле данных аутентификации отсутствует, если при установлении безопасной ассоциации принято решение не использовать возможностей протокола ESP по обеспечению целостности. Помимо этих полей концевик содержит два дополнительных поля - заполнителя и длины заполнителя.

Протоколы AH и ESP могут защищать данные в двух режимах:

1. в транспортном - передача ведется с оригинальными IP-заголовками;
2. в туннельном - исходный пакет помещается в новый IP-пакет и передача ведется с новыми заголовками.

Применение того или иного режима зависит от требований, предъявляемых к защите данных, а также от роли, которую играет в сети узел, завершающий защищенный канал. Так, узел может быть хостом (конечным узлом) или шлюзом (промежуточным узлом).

Соответственно, имеются три схемы применения протокола IPSec:

1. хост-хост;
2. шлюз-шлюз;
3. хост-шлюз.

Возможности протоколов AH и ESP частично перекрываются: протокол AH отвечает только за обеспечение целостности и аутентификации данных, протокол ESP может шифровать данные и, кроме того, выполнять функции протокола AH (в урезанном виде). ESP может поддерживать функции шифрования и аутентификации / целостности в любых комбинациях, то есть либо всю группу функций, либо только аутентификацию / целостность, либо только шифрование.

· IKE или Internet Key Exchange - обмен ключами Интернета - решает вспомогательную задачу автоматического предоставления конечным точкам защищенного канала секретных ключей, необходимых для работы протоколов аутентификации и шифрования данных.

2.3 Транспортный уровень

На транспортном уровне используется протокол SSL/TLS или Secure Socket Layer/Transport Layer Security, реализующий шифрование и аутентификацию между транспортными уровнями приемника и передатчика. SSL/TLS может применяться для защиты трафика TCP, не может применяться для защиты трафика UDP. Для функционирования VPN на основе SSL/TLS нет необходимости в реализации специального программного обеспечения так как каждый браузер и почтовый клиент оснащены этими протоколами. В силу того, что SSL/TLS реализуется на транспортном уровне, защищенное соединение устанавливается «из-конца-в-конец».

TLS-протокол основан на Netscape SSL-протоколе версии 3.0 и состоит из двух частей - TLS Record Protocol и TLS Handshake Protocol. Различие между SSL 3.0 и TLS 1.0 незначительные.

SSL/TLS включает в себя три основных фазы:

1. Диалог между сторонами, целью которого является выбор алгоритма шифрования;
2. Обмен ключами на основе криптосистем с открытым ключом или аутентификация на основе сертификатов;
3. Передача данных, шифруемых при помощи симметричных алгоритмов шифрования.

Еще раз об аутентификации и шифровании

Обеспечение безопасности является основной функцией VPN. Все данные от компьютеров-клиентов проходят через *Internet* к VPN-серверу. Такой сервер может находиться на большом расстоянии от клиентского компьютера, и данные на пути к сети организации проходят через оборудование множества провайдеров. Как убедиться, что данные не были прочитаны или изменены? Для этого применяются различные методы аутентификации и шифрования.

Для аутентификации пользователей PPTP может задействовать любой из протоколов, применяемых для PPP

- EAP или Extensible Authentication Protocol;
- MSCHAP или Microsoft Challenge Handshake Authentication Protocol (версии 1 и 2);
- CHAP или Challenge Handshake Authentication Protocol;
- SPAP или Shiva Password Authentication Protocol;
- PAP или Password Authentication Protocol.

Лучшими считаются протоколы MSCHAP версии 2 и Transport Layer Security (EAP-TLS), поскольку они обеспечивают взаимную аутентификацию, т.е. VPN-сервер и клиент идентифицируют друг друга. Во всех остальных протоколах только сервер проводит аутентификацию клиентов.

Шифрование с помощью PPTP гарантирует, что никто не сможет получить доступ к данным при пересылке через Internet. В настоящее время поддерживаются два метода шифрования:

- Протокол шифрования MPPE или Microsoft Point-to-Point Encryption совместим только с MSCHAP (версии 1 и 2);
- EAP-TLS и умеет автоматически выбирать длину ключа шифрования при согласовании параметров между клиентом и сервером.

MPPE поддерживает работу с ключами длиной 40, 56 или 128 бит. Старые операционные системы Windows поддерживают шифрование с длиной ключа только 40 бит, поэтому в смешанной среде Windows следует выбирать минимальную длину ключа.

PPTP изменяет значение ключа шифрации после каждого принятого пакета. Протокол MMPE разрабатывался для каналов связи точка-точка, в которых пакеты передаются последовательно, и потеря данных очень мала. В этой ситуации значение ключа для очередного пакета зависит от результатов дешифрации предыдущего пакета. При построении виртуальных сетей через сети общего доступа эти условия соблюдать невозможно, так как пакеты данных часто приходят к получателю не в той последовательности, в какой были отправлены. Поэтому PPTP использует для изменения ключа шифрования порядковые номера пакетов. Это позволяет выполнять дешифрацию независимо от предыдущих принятых пакетов.

Хотя PPTP обеспечивает достаточную степень безопасности, но все же L2TP поверх IPSec надежнее. L2TP поверх IPSec обеспечивает аутентификацию на уровнях «пользователь» и 'компьютер', а также выполняет аутентификацию и шифрование данных.

Аутентификация осуществляется либо отрытым тестом (clear text password), либо по схеме запрос / отклик (challenge/response). С прямым текстом все ясно. Клиент посылает серверу пароль. Сервер сравнивает это с эталоном и либо запрещает доступ, либо говорит «добро пожаловать». Открытая аутентификация практически не встречается.

Схема запрос / отклик намного более продвинута. В общем виде она выглядит так:

- клиент посылает серверу запрос (request) на аутентификацию;
- сервер возвращает случайный отклик (challenge);
- клиент снимает со своего пароля хеш (хешем называется результат хеш-функции, которая преобразовывает входной массив данных произвольной длины в выходную битовую строку фиксированной длины), шифрует им отклик и передает его серверу;

- то же самое проделывает и сервер, сравнивая полученный результат с ответом клиента;
- если зашифрованный отклик совпадает, аутентификация считается успешной;

На первом этапе аутентификации клиентов и серверов VPN, L2TP поверх IPSec использует локальные сертификаты, полученные от службы сертификации. Клиент и сервер обмениваются сертификатами и создают защищенное соединение ESP SA (security association). После того как L2TP (поверх IPSec) завершает процесс аутентификации компьютера, выполняется аутентификация на уровне пользователя. Для аутентификации можно задействовать любой протокол, даже PAP, передающий имя пользователя и пароль в открытом виде. Это вполне безопасно, так как L2TP поверх IPSec шифрует всю сессию. Однако проведение аутентификации пользователя при помощи MSCHAP, применяющего различные ключи шифрования для аутентификации компьютера и пользователя, может усилить защиту.

Таким образом, связка «туннелирование + аутентификация + шифрование» позволяет передавать данные между двумя точками через сеть общего пользования, моделируя работу частной (локальной) сети. Иными словами, рассмотренные средства позволяют построить виртуальную частную сеть.