9. ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ (VPN)

Под VPN понимается технология, которая обеспечивает безопасную и качественную связь между контролируемыми группами пользователей по открытой кабельной сети.

Организация VPN. Основными задачами технологий VPN являются обеспечение в публичной сети гарантированного качества обслуживания для потоков пользовательских данных, а также защита их от возможного несанкционированного доступа. К тому же, в Internet начинают постепенно внедряться такие технологии управления качеством обслуживания. В одном случае все функции по поддержанию VPN выполняет сеть провайдера, а корпоративные клиенты только пользуются услугами VPN. Провайдер гарантирует конфиденциальность и качество обслуживания клиентского трафика от точки входа в публичную сеть до точки выхода.

В другом случае предприятие организует виртуальную частную сеть собственными силами, за счет применения специальных VPN-продуктов в своей сети. В качестве таких продуктов могут использоваться самые различные средства: маршрутизаторы и брандмауэры с дополнительным программным обеспечением, выполняющим шифрование передаваемых данных, а также специальные программные и аппаратные средства ддя создания защищенных каналов. Однако все имеющиеся на рынке VPN продукты обеспечивают только защиту передаваемых данных, не предоставляя никаких способов поддержания заданного качества транспортого обслуживания.

Гарантии качества обслуживания. Администраторы корпоративных сетей хотят иметь определенные гарантии качества обслуживания и это отражается в соглашении об уровне услуг - Service Level Agreement, SLA. Такое соглашение заключается между предприятием и провайдером публичной сети, услуги которой используются для построения виртуальной частной сети. Предметом соглашения являются характеристики качества транспортного обслуживания: средняя пропускная способность соединения двух точек виртуальной частной сети, максимально допустимый уровень пульсации

трафика в этом соединении, средняя и максимальная величина задержек пользовательских пакетов, максимально допустимый процент потерянных кадров, коэффициент готовности транспортных услуг, отражающий долю времени в течение которого транспортные услуги были доступны клиенту, и т. д. Наиболее важными считаются следующие:

- l00%-ю доступность сетевой магистрали провайдера;
- высокую доступность сервера RAS для удаленных пользователей;
- гарантированную пропускную способность соединений;
- обеспечение всех характеристик между двумя точками подключения корпоративной сети.

Основным приемом, с помощью которого провайдеры решают эти задачи является постоянный мониторинг собственных сетей для статистического анализа работы сети. Замеры на реальной сети служат отправной точкой для - количественных значений гарантируемых характеристик. Пользователи услуг VPN также должны иметь инструменты для контроля действительных параметров качества услуг.

9.1.Методы управления качеством обслуживания

Сегодня существует немало технологий, способных предоставлять дифференцированное качество обслуживания (например, Diff'Serv, FR и ATM). Гарантируемыми технологией параметрами являются средняя согласованная пропускная способность и максимальная пульсация трафика, кроме этого технология ATM предоставляет трафику реального времени гарантии по задержкам передаваемых ячеек.

Приоритетное обслуживание. В повсеместно используемой сегодня версии протокола IPv4 предусматривается единственный механизм для организации дифференцированного обслуживания, который основан на поле типа сервиса (Type Of Service, TOS) в заголовке IP-пакета. Три бита этого поля позволяют задать 8 уровней приоритета пакета, а значит, и разбить весь трафик на 8 классов. Современные маршрутизаторы позволяют

администратору использовать приоритеты поля TOS для организации различных классов обслуживания. Хотя правила обслуживания этих классов могут быть различными, чаще всего на практике используется алгоритм так называемого *"взвешенного справедливого обслуживания" (Weighted Fair Queuing, WFQ*), когда из очереди каждого приоритета маршрутизатор периодически выбирает определенное число пакетов, соответствующее весу данного приоритета в общем трафике. Основной проблемой при использовании приоритетов пакетов является выработка согласованной политики настройки всех маршрутизаторов сети, которая в результате должна давать определенное качество обслуживания каждому классу трафика между конечными точками сети. Проще всего реализовать такую политику одному провайдеру в пределах контролируемой части сети, что и происходит сегодня в частных IP-сетях. Механизм приоритетов поля TOS получил дальнейшее развитие в комплексе спецификаций IETF дифференцированного обслуживания (Differentiated Services, DS). Эти спецификации расширяют поле приоритета в пакетах IPv4 и класса трафика в пакетах IPv6 до одного байта DS, в котором приоритет (класс трафика) задается уже шестью битами.

Резервирование полосы пропускания. Следует подчеркнуть, что в спецификациях DS термин "дифференцированное обслуживание" используется в узком смысле и противопоставляется "интегрированному обслуживанию". При этом под дифференцированным обслуживанием понимается приоритетная обработка пакетов без резервирования полосы пропускания в маршрутизаторах сети, а под интегрированным обслуживанием - с резервированием. Примером технологии интегрированного обслуживания является протокол резервирования ресурсов RSVP *(Resource reSerVation Protocol).*

В соответствии с протоколом RSVP узел-источник при передаче данных, требующих определенного нестандартного качества обслуживания (например, постоянной полосы пропускания для передачи видеоинформации), посылает по сети узлу назначения специальное RSVP-сообшение, называемое сообщением о пути - path. Это сообщение

содержит метку потока - признак, размещаемый в заголовке пакета и указывающий принадлежность данного пакета потоку, для которого требуется обеспечить заданные параметры обслуживания, отличные от принятых по умолчанию. Кроме того, сообщение path содержит требования к пропускной способности для данного потока. При прохождении сообщения path через сеть в нем фиксируется последовательность маршрутизаторов, лежащих на пути от узла-отправителя до узла назначения. На основании полученной информации узел назначения, используя маршрутизацию от источника, отправляет ответное сообшение resv, которым он запрашивает у всех промежуточных маршрутизаторое определенную пропускную способность для данного потока. Маршрутизатор, получивший сообщение resv, проверяет свои ресурсы, чтобы выяснить, может ли он выделить требуемую пропускную способность. Если нет, то маршрутизатор запрос отвергает. Если же да, то маршрутизатор настраивает алгоритм обработки пакетов таким образом, чтобы указанному потоку всегда предоставлялась требуемая пропускная способность.

При использовании протокола RSVP с целью резервирования пропускной способности для потоков VPN возникает одна проблема. Конечному узлу разрешается выполнять весьма опасное с точки зрения провайдера действие: он получает возможность управлять пропускной способностью сети провайдера. Эта проблема может быть решена с помощью другого варианта применения протокола RSVP, когда маршрутизаторы при получении запроса от конечного узла проверяют сначала его допустимость. Для этого они обращаются к специальному серверу правил, находящемуся в сети провайдера. Если правила разрешают, например, данному пользователю в данный день недели и в данное время запрашивать определенный объем пропускной способности для данного приложения, то маршрутизатор принимает запрос, а если нет - то отвергает.

Для организации интегрированного обелуживания используется и сравнительно новый протокол MPLS *(MultiProtocol Label Switching),*

который решает задачу резервирования пропускной способности в связке с протоколом RSVP. Этот протокол, помимо поддержки качества обслуживания, преследует и другую цель - повышение производительности продвиженяя IP-пакетов через маршрутизаторы за счет использования техники коммутации на основе локальных меток (подобный метод применяется в X.25, frame relay и ATM). С помощью MPLS в IP-сети подерживается виртуальный канал, а резервирование необходимой для него полосы пропускания выполняется с помощью протокола RSVP.

Управление потоками. Еще одним способом поддержания заданного качества обслуживания является управление потоками данных, поступающих от приложений, на основании механизма окна, встроенного в протокол TCP. Изменяя величину окна, можно повлиять на загрузку сети. В стандартном варианте этим механизмом пользуются либо конечный узел, либо маршрутизатор в случае их перегрузки.

Делегирование полномочий. И, наконец, IP-сеть может использовать механизмы обеспечения качества обслуживания, имеющиеся в транспортных технологиях нижнего уровня, над которыми работает протокол IP. У многих провайдеров IP-сети действуют сегодня поверх сетей ATM и FR, поэтому можно воспользоваться присущими этим сетям возможностями по резервированию полосы пропускания и обеспечению других параметров качества обслуживания. Для этого достаточно иметь механизм отображения параметров качества обслуживания канала пользователя уровня IP на параметры качества обслуживания виртуального канала ATM или FR.

9.2. Защита и туннелирование цанных

Функции VPN по защите данных. При подключении корпоративной локальной сети к любой публичной сети возникает два типа угроз:

1. Несанкционированный доступ к внутренним ресурсам корпоративной локальной сети, полученный злоумышленником в результате логического входа в эту сеть.

2. Несанкционированный доступ к корпоративным данным в процессе их передачи по публичной сети.

Для того чтобы виртуальная частная сеть по уровню безопасности приблизилась к истинной частной сети, в которой эти угрозы практически отсутствуют, VPN должна включать средства для отражения угроз как первого, так и второго типов. Отсюда следует, что к средствам VPN может быть отнесен самый широкий круг устройств безопасности: многофункциональные брандмауэры, маршрутизаторы со встроенными возможностями фильтрации пакетов, proxy-серверы, аппаратные и программные шифраторы передаваемого трафика.

Определение защищенного канала. Для обозначения важнейшей части технологии VPN, направленной на обеспечение безопасности передачи данных по открытой транспортной сети, используется специальный термин - защищенный канал (secure channel). В соответствии с общепринятым определением, безопасность данных означает их конфиденциальность, целостность и доступность.

- *Конфиденциальность* - гарантия того, что в процессе передачи данных по защищенным каналам VPN эти данные не могут быть просмотрены никем, кроме легальных отправителя и получателя.
- *Целостность* - гарантия сохранности передаваемыми данными правильных значений во время прохождения по защищенному каналу VPN. Никому не разрешено каким-либо образом изменять, модифицировать, разрушать или создавать новые данные.
- *Доступность* - гарантия того, что средства, выполняющие функции VPN, постоянно доступны легапьным пользователям. Доступность средств VPN - это комплексный показатель, зависящий от нескольких факторов: надежности реализации, качества обслуживания, а также степени защищенности самого средства от внешних атак.

Для создания защищенного канала средства VPN используют процедуры шифрования, аутентификации и авторизации. Так, например, конфиденциальность обеспечивается с помощью различных алгоритмов и методов сим-

метричного и асимметричного шифрования, а также путем взаимной аутентификации абонентов на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт и т. п. *Аутентификация* разрешает устанавливать VPN-соединения только между легальными пользователями и предотвращает доступ к средствам VPN нежелательных лиц. *Авторизация* подразумевает предоставление абонентам, уже доказавшим свою легальность (аутентичность), разных видов обслуживания, например, разных способов шифрования их трафика. Процедуры аутентификации и авторизации часто реализуются одними и теми же средствами и протоколами.

Целостность передаваемых данных обычно достигается с помошью различных вариантов технологии электронной подписи, основанных на симметричных и асимметричных методах шифрования и односторонних функциях.

Таким образом, для обеспечения безопасности передаваемых данных технология защищенного канала должна поддерживать три основные функции:

- взаимную аутентификацию абонентов при установлении соединения;
- защиту передаваемых по каналу сообшений от несанкционированного доступа;
- подтверждение целостности поступающих по каналу сообщений.

Шифрование. В современных алгоритмах шифрования предусматривается наличие параметра - секретного ключа. В криптографии принято правило Кирхгофа: *стойкость шифра должна определяться только секретностью ключа*. Так, все стандартные алгоритмы шифрования (например, DES, PGP) широко известны, их детальное описание содержится в легко доступных документах, но от этого их эффективность не снижается.

Аутентификация. *Аутентификация* - предотвращает доступ к сети нежелательных лиц и разрешает вход для легальных пользователей. Идентификация заключается в сообщении пользователем системе своего идентификатора, а аутентификация - это процедура доказательства пользователем того, что он именно тот, за кого себя выдает, в

частности, доказательство того, что именно ему принаддежит введенный им идентификатор.

В процедуре аутентификации участвует дне стороны: одна сторона доказывает свою аутентичность, предъявляя некоторые доказательства, а другая сторона - аутентификатор - проверяет эти доказательства и принимает решение. В качестве доказательства аутентичности используются разные приемы:

- аутентифицируемый может продемонстрировать знание некоего общего для обеих сторон секрета: слова (пароля) или факта (дату и место события, прозвище человека и т. п.);
- аутентифицируемый может продемонстрировать, что он владеет неким уникальным предметом (физическим ключом), в качестве которого может выступать, например, электронная магнитная карта;
- аутентифицируемый может доказать свою идентичность собственными биохарактеристиками, которые были занесены в базу данных аутентификатора.

Сетевые службы аутентификации строятся на основе всех этих приемов, но чаще всего применяются пароли. Для снижения уровня угрозы раскрытия паролей администраторы сети, как правило, используют встроенные программные средства ддя формирования политики назначения и использования паролей: задание максимального и минимального срока действия пароля, хранение списка использованных паролей, управление поведением системы после нескольких неудачных попыток логического входа и т.п. Перехват паролей по сети можно предупредить путем их шифрования перед передачей в сеть. Аутентификация данных означает доказательство целостности этих данных, а также того, что они поступили от конкретного человека, который объявил об этом. В данном случае используется механизм электронной подписи.

Авторизация. Средства авторизации контролируют доступ легальных пользо-вателей к ресурсам системы, предоставляя каждому из них именно те права, которые

были определены администратором. Кроме предоставления прав доступа пользователей к каталогам, файлам и принтерам, система авторизации может контролировать возможность выполнения пользователями различных системных функций, таких как локальный доступ к серверу, установка системного времени, создание резервных копий данных, выключение сервера и т. п. Применительно к VPN система авторизации может регулировать доступ пользователя к тем или иным средствам шифрования пакетов или даже в целом к определенным VPN-устройствам.

Процедуры авторизации реализуются программными средствами, которые могут быть встроены в операционную систему или в приложение, а также поставляться в виде отдельных программных продуктов. При этом программные системы авторизации строятся на базе двух схем:

- централизованная схема авторизации, базирующаяся на сервере;
- децентрализованная схема, базирующаяся на рабочих станциях.

В первой схеме сервер управляет процессом предоставления ресурсов пользователю. Главная цель таких систем - реализовать "принцип единого входа". В соответствии с централизованной схемой пользователь один раз логически входит в сеть и получает на все время работы некоторый набор разрешений по доступу к ресурсам сети. Kerberos, с ее сервером безопасности и архитектурой "клиент-сервер", является наиболее известной сисгемой этого типа.

При втором подходе рабочая станция сама является защищенной - средства защиты работают на каждой машине, и сервер не требуется. В корпоративной сети администратору придется отслеживать работу механизмов безопасности, используемых всеми типами приложений - элекгронной почтой, службой каталогов локальной сети, базами данных хостов и т. п. Когда администратору приходится добавлять или удалять пользователей, часто требуется вручную конфигурировать доступ к каждой программе или системе.

В крупных сетях часто применяется комбинированный подход предоставления пользователю прав доступа к ресурсам сети. Сервер удаленного доступа ограничивает доступ пользователя к подсетям или серверам корпоративной

сети, то есть к укрупненным элементам сети. А каждый отдельный сервер сети сам по себе ограничивает доступ пользователя к своим внутренним ресурсам - разделяемым каталогам, принтерам или приложениям. Сервер удаленного доступа предоставляет доступ на основании имеющегося у него списка прав доступа пользователя (ACL - *Access Control List).* Ресурсы каждого отдельного сервера сети становятся доступны на основании хранящегося у него списка прав доступа - например, ACL файловой системы. Подчеркнем, что системы аутентификации и авторизации совместно выполняют одну задачу, поэтому к ним необходимо предъявлять одинаковый уровень требований. Ненадежность одного звена здесь не может быть компенсирована высоким качеством другого. Если при аутентифугкации используются пароли, то требуются чрезвычайные меры по их защите.

Поскольку никакая система безопасности не гарантирует 100%-ю защиту, то последним рубежом в борьбе с нарушениями оказывается система аудита. *Аудит* - фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам. Эта информация, возможно, позволит найти злоумышленника или, по крайней мере, предотвратить повторение подобных атак путем устранения уязвимых мест в системе защиты.

Туннелирование. Протоколы защищенного канала часто используют в своей работе такой механизм, как туннелирование (инкапсуляция). При туннелировании пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня. Например, при туннелировании кадр Ethernet может быть размещен в пакете IP, а пакет IPX - в пакете IP, или: пакет IP размещается в пакете IP. Туннелирование широко используется для безопасной передачи данных через публичные сети путем упаковки пакетов во внешнюю оболочку. Туннель создается двумя пограничными устройствами, которые размещаются в точках входа в публичную сеть. Особенностью туннелирования является то, что эта технология позволяет зашифровать исходный пакет целиком, вместе с заголовком, а не только его поле данных. И это очень важно, так как многие поля заголовка содержат информацию, которая может быть использована злоумышленником. Из заголовка он может почерпнуть, например, сведения о внутренней структуре сети: данные о

количестве подсетей и узлов и их IP-адресах, что может использоваться для организации атак на корпоративную сеть или для получения данных о деловой активности предприятия, например, о его бизнес-партнерах.

С другой стороны, если заголовок зашифровать, то он не может быть использован по своему прямому назначению - для обеспечения транспортировки пакета по сети. Именно в такой ситуации для защиты пакета прибегают к туннелированию. Исходный пакет зашифровывают полностью, вместе с заголовком, и этот зашифрованный пакет помещают в другой, внешний пакет с открытым заголовком. Для транспортировки данных по "опасной" сети используются открытые поля заголовка внешнего пакета, а при прибытии внешнего пакета в конечную точку защищенного канала из него извлекают внутренний пакет, расшифровывают и используют его заголовок для дальнейшей передачи уже в открытом виде по сети, не требующей защиты.

Туннелирование часто применяется также для согласования разных транспортных технологий. Например, если данные протокола IPX нужно передать через транзитную сеть IP, то маршрутизатор на границе IPX и IP сетей упаковывает исходный IPX пакет в создаваемый заново пакет IP и адресует его маршрутизатору, соединяющему транзитную IP-сеть с сетью IPX. Этот маршрутизатор извлекает пакет IPX из прибывшего IP пакета и отправляет его далее по IPX-сети.

Само по себе туннеллирование не защищает данные от несанкционированного доступа или искажения, а только создает предпосылки для защиты всех полей исходного пакета, включая и поля заголовка. Для того чтобы обеспечить секретность передаваемых данных, исходные пакеты шифруются и/или снабжаются электронной подписью, а затем передаются по транзитной сети с помощью пакетов несущего протокола.

Типы VPN-устройств отличают друг от друга многие характеристики: набор функциональных возможностей, точки размещения VPN-устройств, тип платформы, на которой эти средства работают, применяемые протоколы шифрования и аутентификации.

Сегодня существует несколько основных типов VPN-устройств:

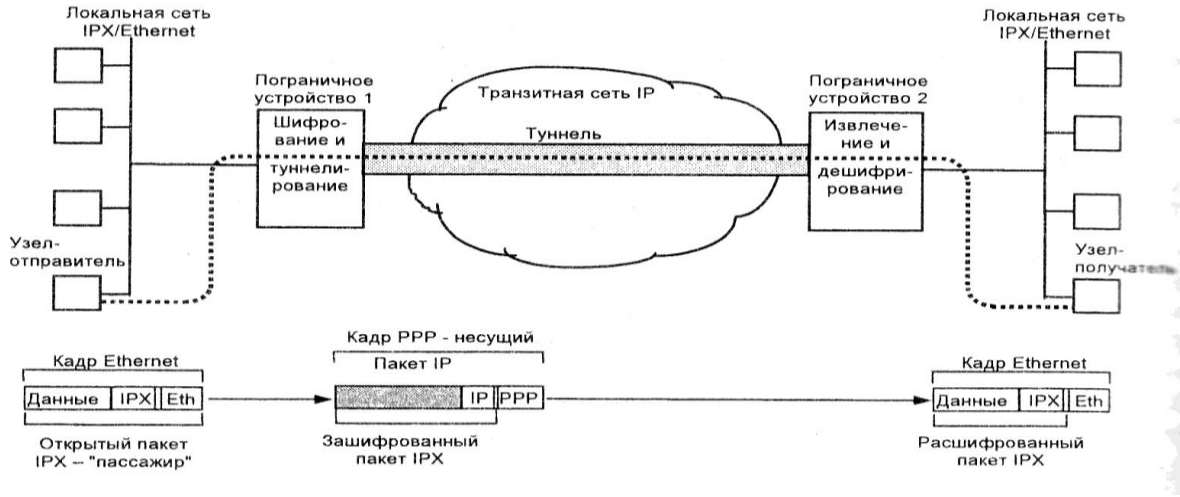

Рис. 9.1. *Схема использования туннелирования для зашифрованной передачи трафика IPX через сеть IP*

- *отдельное аппаратное устройство* VPN на основе специализированной ОС реального времени, имеющее 2 или более сетевых интерфейса и аппаратную криптографическую поддержку - так называемый "черный ящик VPN";
- *отдельное программное решение,* которое дополняет стандартную операционную систему функциями VPN;
- *расширение брандмауэра* за счет дополнительных функций защищенного канала;
- *средства VPN, встроенные в маршрутизатор* или коммутатор.

Существуют также комбинированные пограничные устройства, которые включают в себя функции маршрутизатора, брандмауэра, средства управления пропускной способностью и функции VPN. Устройства VPN могут играть в виртуальных частных сетях роль шлюза или клиента (рис. 9.2).

Шлюз VPN - это сетевое устройство, подключенное к нескольким сетям, которое выполняет функции шифрования и аутентификации для многочисленных хостов позади него. Размещение шлюза VPN должно быть аналогично размещению брандмауэра, то есть таким, чтобы через него проходил весь трафик, предназначенный для внутренней корпоративной сети. В зависимости от стратегии безопасности предприятия, исходящие пакеты либо шифруются, либо посылаются в открытом виде, либо блокируются шлюзом. Для входящих

туннелируемых пакетов внешний адрес является адресом VPN-шлюза, а внутренний адрес - адресом некоторого хоста позади шлюза. Шлюз VPN может быть реализован всеми перечисленными выше способами, то есть в виде отдельного аппаратного устройства, отдельного программного решения, а также в виде брандмауэра или маршрутизатора, дополненных функциями VPN.

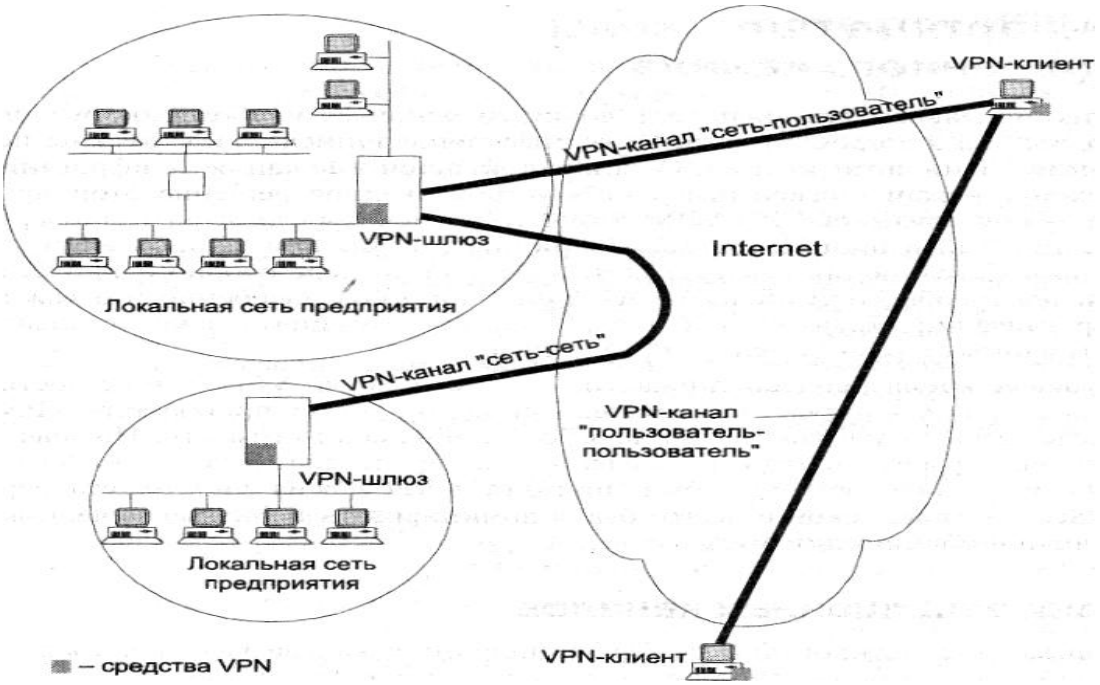

Рис. 9.2. *Шлюзы и клиенты VPN*

Клиент VPN - это программный или программно-аппаратный комплекс. обычно на базе персонального компьютера. Его сетевое транспортное обеспечение модифицировано для выполнения шифрования и аутентификации трафика, которым устройство обменивается с шлюзами VPN или VPN-клиентами. Для создания виртуальной частной сети крупного предприятия нужны как VPN-шлюзы, так и VPN-клиенты. Шлюзы целесообразно использовать для защиты локальных сетей предприятия, а VPN-клиенты - для удаленных и мобильных пользователей, которым требуется устанавливать соединения с корпоративной сетью через Internet.