# 11 Лекция: Виртуальные частные сети

Рассмотрены вопросы, связанные с VPN. Дано их определение. Рассмотрены два типа VPN, их преимущества и недостатки. Дано понятие стандартных технологий функционирования VPN.

Частные сети используются организациями для соединения с удаленными сайтами и с другими организациями. Частные сети состоят из каналов связи, арендуемых у различных телефонных компаний и поставщиков услуг интернета. Эти каналы связи характеризуются тем, что они соединяют только два объекта, будучи отделенными от другого трафика, так как арендуемые каналы обеспечивают двустороннюю связь между двумя сайтами. Частные сети обладают множеством преимуществ.

- Информация сохраняется в секрете.
- Удаленные сайты могут осуществлять обмен информацией незамедлительно.
- Удаленные пользователи не ощущают себя изолированными от системы, к которой они осуществляют доступ.

К сожалению, этот тип сетей обладает одним большим недостатком - высокой стоимостью. Использование частных сетей - очень дорогое удовольствие. Используя менее скоростные каналы связи, можно сэкономить деньги, но тогда удаленные пользователи начнут замечать недостаток в скорости, и некоторые из указанных выше преимуществ станут менее очевидными.

С увеличением числа пользователей интернета многие организации перешли на использование виртуальных частных сетей (VPN). Виртуальные частные сети обеспечивают многие преимущества частных сетей за меньшую цену. Тем не менее, с внедрением VPN появляется целый ряд вопросов и опасностей для организации. Правильно построенная виртуальная частная сеть может принести организации большую пользу. Если же VPN реализована некорректно, вся информация, передаваемая через VPN, может быть доступна из интернета.

## Определение виртуальных частных сетей

Итак, мы намереваемся передавать через интернет секретные данные организации без использования арендуемых каналов связи, по-прежнему принимая все меры для обеспечения конфиденциальности трафика. Каким же образом нам удастся отделить свой трафик от трафика остальных пользователей глобальной сети? Ответом на этот вопрос является шифрование.

В интернете можно встретить трафик любого типа. Значительная часть этого трафика передается в открытом виде, и любой пользователь, наблюдающий за этим трафиком, сможет его распознать. Это относится к большей части почтового и веб-трафика, а также сеансам связи через протоколы telnet и FTP. Трафик Secure Shell (SSH) и Hypertext Transfer Protocol Secure (HTTPS) является шифруемым трафиком, и его не сможет просмотреть пользователь, отслеживающий пакеты. Тем не менее, трафик типа SSH и HTTPS не образует виртуальную частную сеть VPN.

Виртуальные частные сети обладают несколькими характеристиками.

- Трафик шифруется для обеспечения защиты от прослушивания.
- Осуществляется аутентификация удаленного сайта.
- Виртуальные частные сети обеспечивают поддержку множества протоколов.
- Соединение обеспечивает связь только между двумя конкретными абонентами.

Так как SSH и HTTPS не способны поддерживать несколько протоколов, то же самое относится и к реальным виртуальным частным сетям. VPN-пакеты смешиваются с потоком обычного трафика в интернете и существуют отдельно по той причине, что данный трафик может считываться только конечными точками соединения.

Примечание

Возможно реализовать передачу трафика через сеанс SSH с использованием туннелей. Тем не менее, в рамках данной лекции мы не будем рассматривать SSH как VPN.

Рассмотрим более детально каждую из характеристик VPN. Выше уже говорилось о том, что трафик VPN шифруется для защиты от прослушивания. Шифрование должно быть достаточно мощным, чтобы можно было гарантировать конфиденциальность передаваемой информации на тот период, пока она будет актуальна. Пароли имеют срок действия, равный 30 дням (подразумевается политика изменения пароля через каждые 30 дней); однако секретная информация может не утрачивать своей ценности на протяжении долгих лет. Следовательно, алгоритм шифрования и применение VPN должны предотвратить нелегальное дешифрование трафика на несколько лет.

Вторая характеристика заключается в том, что осуществляется аутентификация удаленного сайта. Эта характеристика может требовать аутентификацию некоторых пользователей на центральном сервере либо взаимную аутентификацию обоих узлов, которые соединяет VPN. Используемый механизм аутентификации контролируется политикой.

Политика может предусмотреть аутентификацию пользователей по двум параметрам или с использованием динамических паролей. При взаимной аутентификации может потребоваться, чтобы оба сайта демонстрировали знание определенного общего секрета (под секретом подразумевается некоторая информация, заранее известная обоим сайтам), либо могут потребоваться цифровые сертификаты.

Виртуальные частные сети обеспечивают поддержку различных протоколов, в особенности на прикладном уровне. Например, удаленный пользователь может использовать протокол SMTP для связи с почтовым сервером, одновременно используя NetBIOS для соединения с файловым сервером. Оба указанных протокола могут работать через один и тот же цикл связи или канал VPN (см. рис. 11.1).

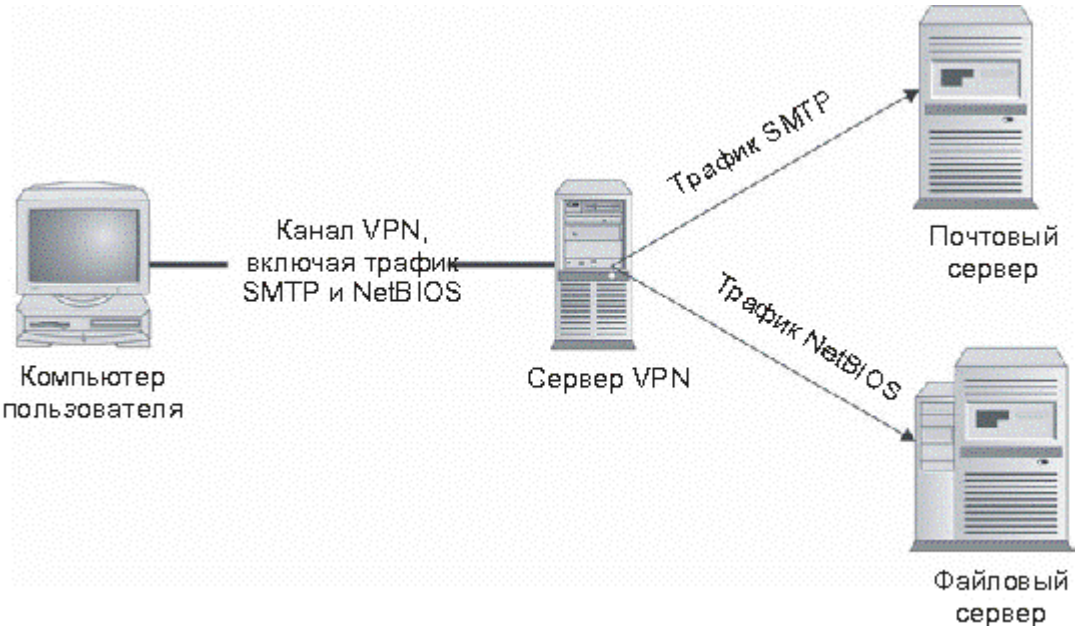


Рис. 11.1. Виртуальные частные сети поддерживают множество протоколов

VPN соединяет два конкретных объекта, образуя таким образом уникальный канал связи между двумя абонентами. Каждая из конечных точек VPN может единовременно поддерживать несколько соединений VPN с другими конечными точками, однако каждая из точек является отдельной от других, и трафик разделяется посредством шифрования.

Виртуальные частные сети, как правило, подразделяются на два типа: пользовательские VPN и узловые VPN. Различие между ними заключается в методе использования, а не в способе отделения трафика каждым из двух типов сетей. В оставшейся части данной лекции будет детально рассказываться о каждом из типов VPN.

**Развертывание пользовательских виртуальных частных сетей**

Пользовательские VPN представляют собой виртуальные частные сети, построенные между отдельной пользовательской системой и узлом или сетью организации. Часто пользовательские VPN используются сотрудниками, находящимися в командировке или работающими из дома. Сервер VPN может являться межсетевым экраном организации либо быть отдельным VPN-сервером. Пользователь подключается к интернету через телефонное подключение к локальному поставщику услуг, через канал DSL или кабельный модем и инициирует VPN-соединение с узлом организации через интернет.

Узел организации запрашивает у пользователя аутентификационные данные и, в случае успешной аутентификации, позволяет пользователю осуществить доступ ко внутренней сети организации, как если бы пользователь находился внутри узла и физически располагался внутри сети. Очевиден тот факт, что скорость сетевого соединения будет ограничиваться скоростью подключения пользователя к интернету.

Пользовательские VPN позволяют организациям ограничивать доступ удаленных пользователей к системам или файлам. Это ограничение должно базироваться на политике организации и зависит от возможностей продукта VPN.

В то время как пользователь имеет VPN-соединение с внутренней сетью организации, он также может соединяться и работать с интернетом или выполнять другие действия как обычный пользователь интернета. Сеть VPN поддерживается отдельным приложением на компьютере пользователя (см. рис. 11.2).


Рис. 11.2. Конфигурация пользовательской VPN

Внимание!

В некоторых случаях компьютер пользователя может выступать в роли маршрутизатора между интернетом и сетью VPN (и, следовательно, внутренней сетью организации). Этот тип сетевого атакующего воздействия необходимо тщательно изучить перед применением пользовательской виртуальной частной сети. Некоторые клиенты VPN содержат политику, снижающую риск проявления данной угрозы.

**Преимущества пользовательских VPN**

Пользовательские VPN обладают двумя основными преимуществами:

- Сотрудники, находящиеся в командировке, могут осуществлять доступ к электронной почте, файлам и внутренним системам в любое время без необходимости в осуществлении дорогостоящих междугородних и международных телефонных вызовов для соединения с серверами.
- Сотрудники, работающие из дома, могут осуществлять доступ к службам сети, как и сотрудники, работающие в организации, без аренды дорогостоящих выделенных каналов.

Оба эти преимущества можно приписать к экономии денежных средств. Экономия может заключаться в отказе от использования дорогостоящих междугородних и международных соединений, арендуемых каналов связи или в выполнении сотрудниками задач по администрированию серверов, принимающих входящие телефонные соединения. Домашние пользователи с DSL или кабельными модемами могут добиться увеличения скорости при использовании линий телефонной связи со скоростями 56 Кбит/с. Все больше гостиничных номеров оборудуются соединениями для доступа в сеть, поэтому для пользователей, находящихся в поездке, создаются все условия для высокоскоростного доступа в сеть.

Примечание

Увеличение скорости через канал 56 Кбит/с не гарантируется. Средняя скорость соединения зависит от множества факторов, включая скоростные возможности интернет-соединения пользователя, интернет-соединения организации, уровень нагрузки интернета, а также число единовременных соединений с VPN-сервером.

**Проблемы, связанные с пользовательскими VPN**

Правильное использование пользовательских VPN может снизить затраты организации, но пользовательские VPN не являются решением всех возможных проблем. При их использовании имеют место значительные

риски, связанные с безопасностью, и проблемы реализации, с которыми приходится считаться.

Возможно, самой большой проблемой безопасности при использовании VPN сотрудником является одновременное соединение с другими сайтами интернета. Как правило, программное обеспечение VPN на компьютере пользователя определяет, должен ли трафик передаваться через VPN, либо его необходимо отправить на какой-либо другой сайт в открытом виде. Если на компьютер пользователя была произведена атака с использованием "троянского коня", возможно, что некий внешний нелегальный пользователь использует компьютер сотрудника для подключения к внутренней сети организации (см. рис. 11.3). Атаки данного типа осуществляются довольно сложно, но они совершенно реальны.

Пользовательские VPN требуют такого же внимания к вопросам, связанным с управлением пользователями, как и внутренние системы. В некоторых случаях пользователи VPN могут быть привязаны к идентификаторам пользователей в домене Windows NT или Windows 2000 или к другой системе централизованного управления пользователями. Эта возможность упрощает управление пользователями, однако администраторам по-прежнему следует сохранять бдительность и следить за тем, каким пользователям требуется удаленный VPN-доступ, а каким - нет.

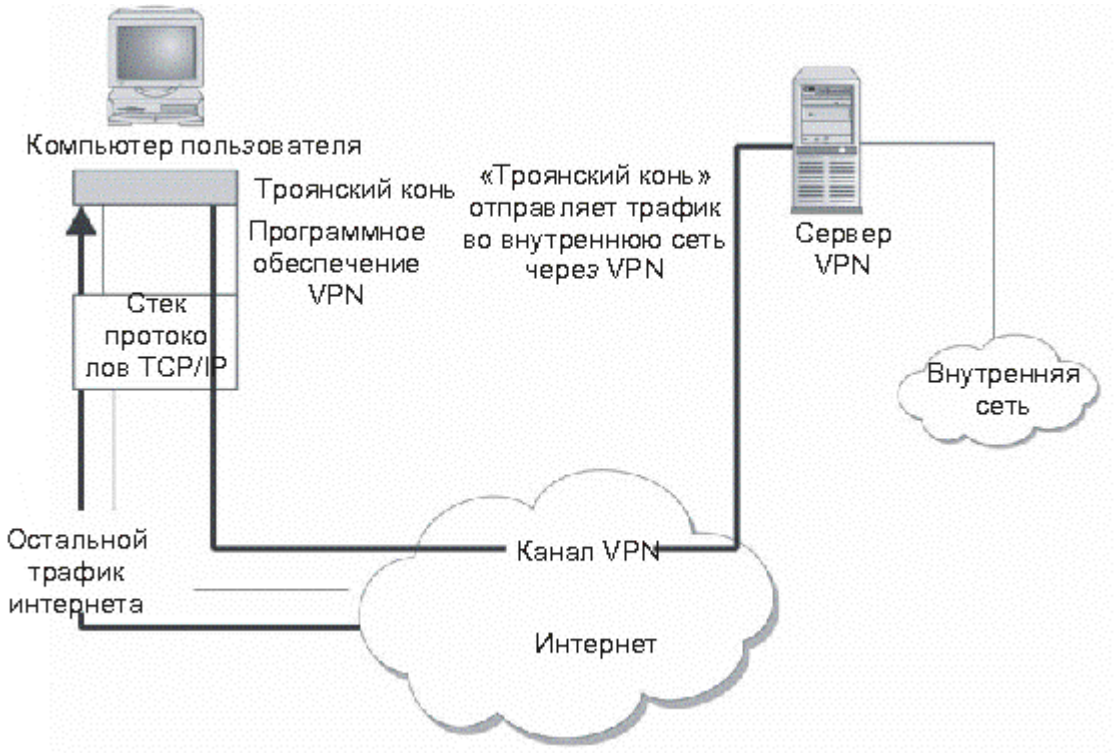


Рис. 11.3. Использование "троянского коня" для проникновения во внутреннюю сеть организации

Внимание!

Если управление VPN-пользователями не связано с центральной системой управления пользователями, этот факт должен учитываться в процедурах управления пользователями, покидающими организацию.

Пользователи должны проходить аутентификацию перед использованием сетей VPN. Так как VPN позволяет осуществлять удаленный доступ ко внутренней сети организации, эта аутентификация должна быть двухфакторной, то есть запрашивать два аутентификационных параметра. Одним из параметров может являться сам компьютер пользователя. В этом случае вторым параметром должно быть нечто известное пользователю или непосредственно с ним связанное. В любом случае, второй параметр не должен находиться на компьютере и не должен быть с ним связан.

В организациях должна приниматься в расчет нагрузка трафиком. Главной точкой нагрузки является VPN-сервер в узле организации. Ключевым параметром нагрузки является ожидаемое число одновременных соединений. При установке каждого соединения VPN-сервер должен иметь возможность расшифровывать дополнительный трафик. Хотя процессор может обеспечивать поддержку больших объемов трафика, он может не обеспечивать шифрование и расшифровку большого числа пакетов без значительных задержек. Следовательно, сервер VPN должен создаваться с учетом ожидаемого числа единовременных соединений.

Еще один момент может повлиять на использование организацией пользовательской VPN. Он связан с использованием трансляции сетевых адресов (NAT) на противоположном конце соединения. Если ожидается, что сотрудники организации будут пытаться использовать VPN с узлов, защищенных межсетевыми экранами, могут возникнуть проблемы. Например, если организация А является консалтинговой компанией с сотрудниками, работающими в организации Б, в А может возникнуть потребность предоставить своим сотрудникам обратную связь для работы с электронной почтой и получения доступа к файлам. Однако, если эти сотрудники работают с компьютеров, входящих в состав внутренней сети организации Б, в которой используется динамическая NAT для скрытия адресов внутренних систем, это окажется невозможным. Если в вашей организации предпочтение отдается использованию VPN именно таким образом, следует проверить возможности программного обеспечения VPN.

**Управление пользовательскими VPN**

Управление пользовательскими VPN, главным образом, заключается в управлении пользователями и их компьютерами. При разделении сотрудников необходимо выполнять соответствующие процедуры по управлению пользователями.

Разумеется, на компьютерах пользователей должны устанавливаться правильные версии программного обеспечения VPN и реализовываться соответствующие конфигурации. Если компьютеры принадлежат организации, это программное обеспечение является стандартным компонентом для каждого компьютера. Если организация разрешает сотрудникам использовать VPN со своих домашних компьютеров, ей понадобится увеличить общий уровень поддержки этих пользователей, так как различные компьютеры и поставщики услуг интернета могут требовать наличие различных конфигураций.

Совет

В организациях также может рассматриваться вопрос о предоставлении сотрудникам межсетевого экрана офисного или домашнего уровня. Многие из таких систем могут управляться удаленно, что позволяет организации отслеживать и настраивать системы.

Одним из ключевых аспектов пользовательской VPN, о котором не следует забывать, является установка хорошей антивирусной программы на компьютере пользователя. Этот программный пакет должен обеспечивать регулярное обновление своих баз (по крайней мере, ежемесячно) для противостояния вирусам и "троянским коням", проникающим на компьютер пользователя.

**Развертывание узловых сетей VPN**

Узловые виртуальные частные сети используются организациями для подключения к удаленным узлам без применения дорогостоящих выделенных каналов или для соединения двух различных организаций, между которыми необходима связь для осуществления информационного обмена, связанного с деятельностью этих организаций. Как правило, VPN соединяет один межсетевой экран или пограничный маршрутизатор с другим аналогичным устройством (см. рис. 11.4).

Чтобы инициировать соединение, один из узлов осуществляет попытку передать трафик другому узлу. Вследствие этого на обоих противоположных узлах соединения VPN инициируется VPN. Оба конечных узла определяют параметры соединения в зависимости от политик, имеющихся на узлах. Оба сайта будут аутентифицировать друг друга посредством некоторого общего предопределенного секрета либо с помощью сертификата с открытым ключом. Некоторые организации используют узловые VPN в качестве резервных каналов связи для арендуемых каналов.

Внимание!

При работе с данной конфигурацией необходимо обеспечивать правильную настройку маршрутизации. Кроме того, физический канал связи, используемый для VPN, обязательно должен отличаться от канала, используемого арендуемым соединением. Может оказаться так, что оба соединения осуществляются через один и тот же физический канал связи, вследствие чего не будет обеспечиваться должный уровень избыточности.

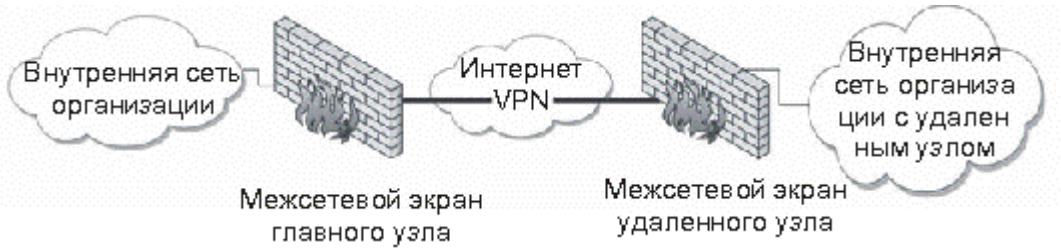


Рис. 11.4. Межузловое соединение VPN, проходящее через интернет

**Преимущества узловых VPN**

Как и в случае с пользовательскими VPN, основным преимуществом узловой VPN является экономичность. Организация с небольшими, удаленными друг от друга офисами может создать виртуальную частную сеть, соединяющую все удаленные офисы с центральным узлом (или даже друг с другом) со значительно меньшими затратами. Сетевая инфраструктура также может быть применена значительно быстрее, так как в удаленных офисах могут использоваться локальные ISP для каналов ISDN или DSL.

На базе политики организации могут быть разработаны правила, определяющие, каким образом удаленные сайты будут подключаться к центральному сайту или друг к другу. Если узловая VPN предназначена для соединения двух организаций, то на доступ ко внутренним сетям и компьютерным системам могут налагаться строгие ограничения.

**Проблемы, связанные с узловыми VPN**

Узловые VPN расширяют периметр безопасности организации, добавляя новые удаленные узлы или даже удаленные организации. Если уровень безопасности удаленного узла невелик, VPN может позволить злоумышленнику получить доступ к центральному узлу и другим частям внутренней сети организации. Следовательно, необходимо применять строгие политики и реализовывать функции аудита для обеспечения безопасности организации в целом. В случаях, когда две организации используют узловую VPN для соединения своих сетей, очень важную роль играют политики безопасности, установленные по обе стороны соединения. В данной ситуации обе организации должны определить, какие данные могут

передаваться через VPN, а какие - нет, и соответствующим образом настроить политики на своих межсетевых экранах.

Аутентификация узловых VPN также является важным условием для обеспечения безопасности. При установке соединения могут использоваться произвольные секреты, но один и тот же общий секрет не должен использоваться для более чем одного соединения VPN. Если предполагается использовать сертификаты с открытыми ключами, необходимо создать процедуры для поддержки изменения и отслеживания срока действия сертификатов.

Как и в случае с пользовательскими VPN, сервер VPN должен поддерживать дешифрование и шифрование VPN-трафика. Если уровень трафика высок, сервер VPN может оказаться перегруженным. В особенности это относится к ситуации, когда межсетевой экран является VPN-сервером, и имеет место интернет-трафик большого объема.

Наконец, необходимо обдумать вопросы, связанные с адресацией. Если узловая VPN используется внутри одной организации, в ней необходимо наличие одинаковой схемы адресации для всех узлов. В данном случае адресация не представляет какой-либо сложности. Если же VPN используется для соединения двух различных организаций, необходимо предпринять меры для предупреждения любых конфликтов, связанных с адресацией. На рисунке 11.5 отражена возникшая конфликтная ситуация. Здесь обе организации используют части одного и того же частного адресного пространства (сеть 10.1.1.x).

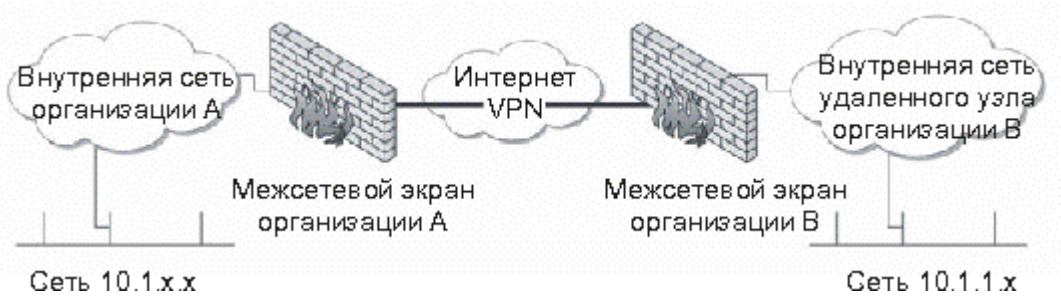


Рис. 11.5. Узловая VPN может вызывать конфликты, связанные с адресацией

Очевидно, что схемы адресации будут конфликтовать друг с другом, и маршрутизация трафика не будет функционировать. В данном случае каждая сторона соединения VPN должна выполнять трансляцию сетевых адресов и переадресовывать системы другой организации на их собственную схему адресации (см. рис. 11.6).

Управление узловыми VPN

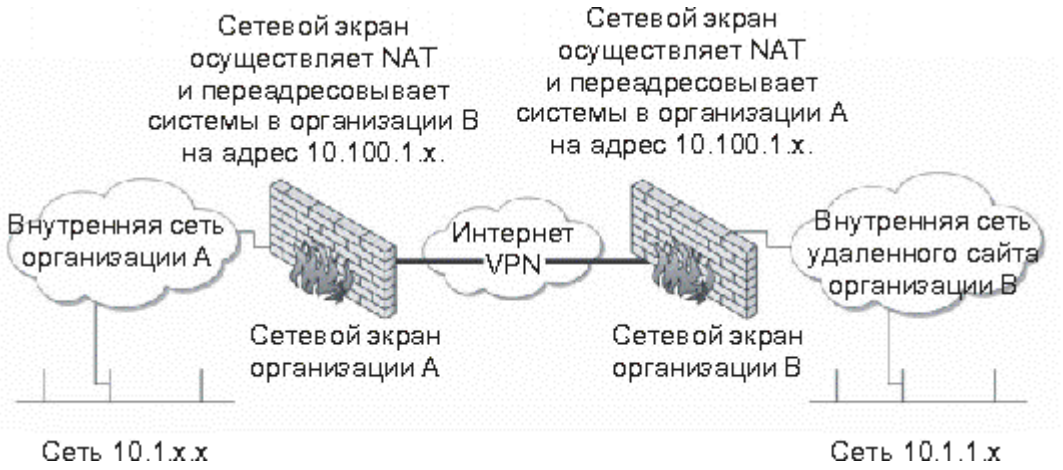


Рис. 11.6. Узловая VPN использует NAT для предотвращения конфликтов адресации

При осуществлении контроля над маршрутизацией могут понадобиться дополнительные функции по управлению. На маршрутизаторах внутренних сетей потребуется создать маршруты к удаленным сайтам. Эти маршруты, наряду с управлением схемой адресации, должны четко документироваться во избежание непреднамеренного удаления маршрутов в процессе управления маршрутизатором.

Вопросы для самопроверки

1. Что является основной причиной применения в организациях сетей VPN?
2. Информация, передаваемая через VPN, защищается с помощью _____.

**Понятие стандартных технологий функционирования VPN**

Сеть VPN состоит из четырех ключевых компонентов:

- Сервер VPN.
- Алгоритмы шифрования.
- Система аутентификации.
- Протокол VPN.

Эти компоненты реализуют соответствие требованиям по безопасности, производительности и способности к взаимодействию. То, насколько правильно реализована архитектура VPN, зависит от правильности определения требований. Определение требований должно включать в себя следующие аспекты.

- Количество времени, в течение которого необходимо обеспечивать защиту информации.
- Число одновременных соединений пользователей.
- Ожидаемые типы соединений пользователей (сотрудники, работающие из дома или находящиеся в поездке).
- Число соединений с удаленным сервером.
- Типы сетей VPN, которым понадобится соединение.
- Ожидаемый объем входящего и исходящего трафика на удаленных узлах.
- Политика безопасности, определяющая настройки безопасности.

При разработке системы также может оказаться полезным указать дополнительные требования, связанные с местоположением сотрудников, находящихся в поездке (имеются в виду узлы в других организациях или в номерах отелей), а также типы служб, которые будут работать через VPN.

**Сервер VPN**

Сервер VPN представляет собой компьютер, выступающий в роли конечного узла соединения VPN. Данный сервер должен обладать характеристиками, достаточными для поддержки ожидаемой нагрузки. Большая часть производителей программного обеспечения VPN должна предоставлять рекомендации по поводу производительности процессора и конфигурации памяти, в зависимости от числа единовременных VPN-соединений. Следует обеспечить наличие системы с соответствующими параметрами, а также позаботиться о ее дальнейшей модернизации.

Примечание

Может потребоваться создание нескольких серверов VPN, чтобы обеспечить поддержку ожидаемой нагрузки. В данном случае ожидаемые VPN-соединения должны как можно скорее распределяться между системами.

Некоторые производители включают в свои системы методы обхода ошибок и разрешают наличие избыточных серверов VPN. Обход ошибок может не подразумевать распределение нагрузки, поэтому соединения могут по-прежнему требовать распределения между серверами. Это обстоятельство необходимо принимать во внимание при построении систем.

VPN-сервер должен быть расположен в сети. Сервер может быть межсетевым экраном или пограничным маршрутизатором (см. рис. 11.7), что упрощает размещение VPN-сервера. В качестве альтернативы сервер может являться и отдельной системой. В этом случае сервер должен быть расположен в выделенной демилитаризованной зоне (DMZ) (см. рис. 11.8). В идеальном случае демилитаризованная зона VPN должна содержать только VPN-сервер и быть отдельной от DMZ интернета, содержащей веб-серверы и

почтовые серверы организации. Причиной является то, что VPN-сервер разрешает доступ ко внутренним системам авторизованным пользователям и, следовательно, должен рассматриваться как объект с большей степенью доверия, нежели почтовые и веб-серверы, доступ к которым может быть осуществлен лицами, не пользующимися доверием. Демилитаризованная зона VPN защищается набором правил межсетевого экрана и разрешает передачу только того трафика, который требует VPN.

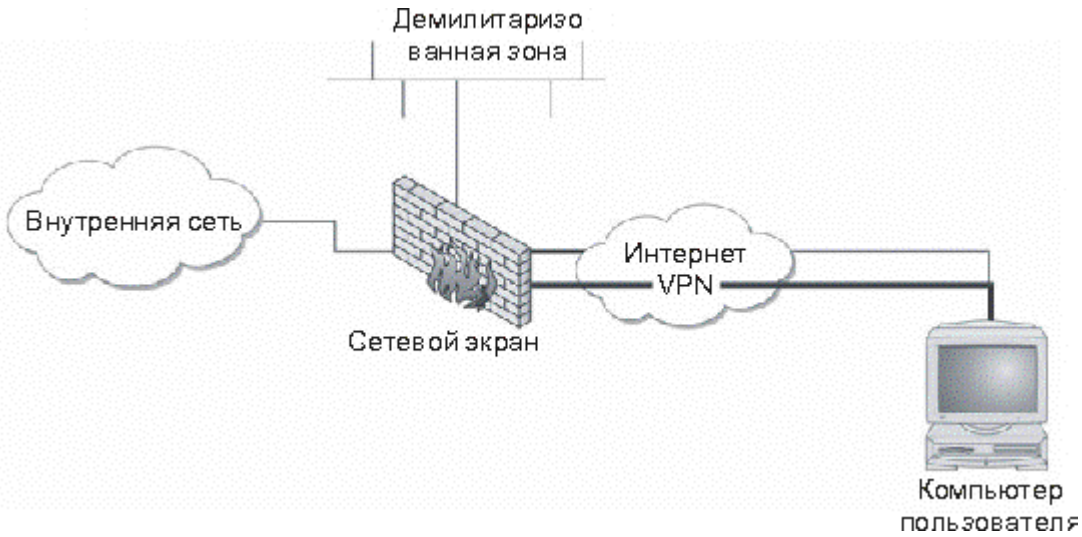


Рис. 11.7. Архитектура сети VPN, в которой межсетевой экран является VPN-сервером

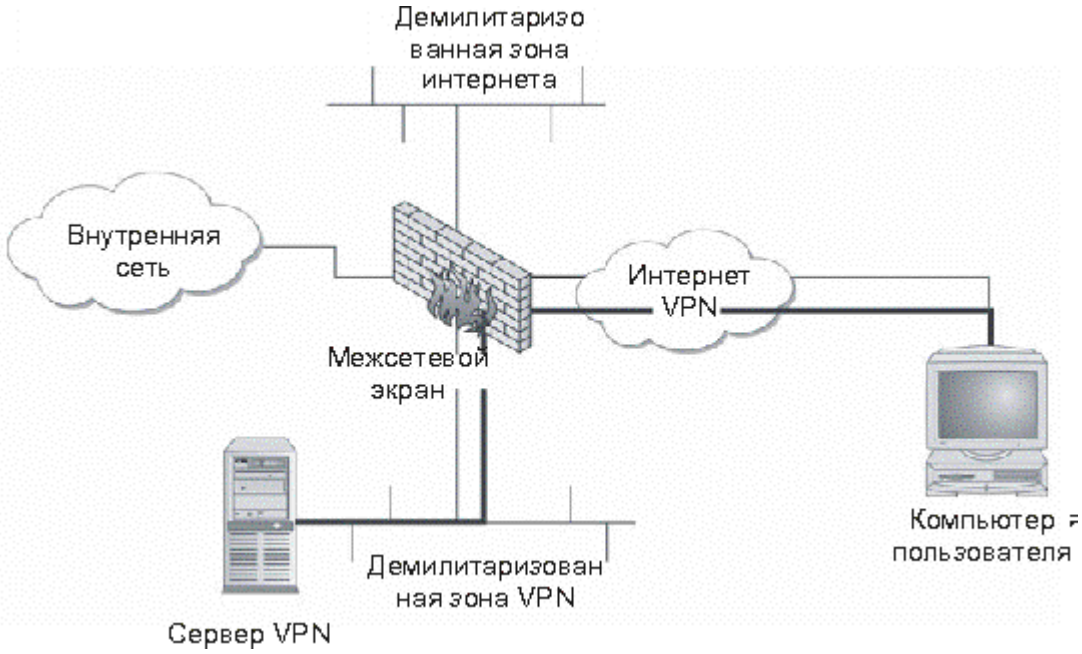


Рис. 11.8. Архитектура сети VPN для отдельного сервера VPN

Примечание

Если VPN-сервер расположен в демилитаризованной зоне VPN, межсетевой экран может потребовать усовершенствования для поддержки нагрузки трафика. Даже несмотря на то, что межсетевой экран не будет выполнять функцию шифрования, исходный межсетевой экран может обладать недостаточными характеристиками для обеспечения вычислительной мощности, необходимой для трафика VPN. Если трафик VPN является важным для организации, на межсетевом экране должна присутствовать некоторая система обхода ошибок. В качестве альтернативы можно использовать отдельную платформу VPN. Такое устройство обеспечит разгрузку межсетевого экрана, взяв на себя функции обработки VPN.

Правила политики межсетевого экрана для демилитаризованной зоны VPN определены в табл. 11.1. Здесь содержатся правила, необходимые для демилитаризованной зоны интернета и демилитаризованной зоны VPN.

Правила 1, 2 и 3 относятся к демилитаризованной зоне VPN. Правило 1 позволяет клиентам VPN осуществлять доступ к серверу VPN с использованием любой службы, требуемой программным обеспечением VPN. Правило 2 разрешает VPN-серверу осуществлять маршрутизацию этих соединений во внутреннюю сеть. Правило 3 исключает соединение демилитаризованной зоны интернета с демилитаризованной зоной VPN, изолируя демилитаризованную зону VPN от систем в DMZ интернета, пользующихся меньшим доверием.

**Таблица 11.1. Правила политики межсетевого экрана, включающие демилитаризованную зону VPN**

| Номер правила | Исходный IP | Конечный IP | Служба | Действие |
|---|---|---|---|---|
| 1 | Любой | VPN-сервер | Служба VPN | Принятие. |
| 2 | VPN-сервер | Внутренняя сеть | Любой | Принятие |
| 3 | Любой | VPN-сервер | Любой | Отклонение |
| 4 | Любой | Веб-сервер | HTTP | Принятие |
| 5 | Любой | Почтовый сервер | SMTP | Принятие |
| 6 | Почтовый сервер | Любой | SMTP | Принятие |
| 7 | Внутренняя сеть | Любой | HTTP, HTTPS, FTP, telnet, SSH | Принятие |
| 8 | Внутренняя DNS | Любой | DNS | Принятие |
| 9 | Любой | Любой | Любой | Сброс |

## Алгоритмы шифрования

Алгоритм шифрования, используемый в VPN, должен быть стандартным мощным алгоритмом шифрования. Возникает вопрос: какая же система шифрования самая лучшая? Вообще, все стандартные и мощные алгоритмы могут эффективно использоваться при построении VPN. Различные производители отдают предпочтение различным алгоритмам, в зависимости от ограничений реализации продукта, аспектов, связанных с лицензированием, и предпочтений по программированию. Приобретая программный пакет VPN, следует выслушать комментарии специалистов и убедиться в том, что производитель использует мощный алгоритм шифрования.

Читатель может обратить внимание на то, что в предыдущем абзаце уделено особое внимание выбору алгоритма шифрования. Следует заметить, что выбор алгоритма не имеет принципиального значения, если он будет стандартным и в достаточной степени мощным. Гораздо больше влияет на общий уровень безопасности реализация системы. Неправильно реализованная система может сделать бесполезным самый мощный алгоритм шифрования. Приняв во внимание сказанное выше, давайте изучим риски, связанные с использованием VPN. Для того чтобы получить доступ к информации, передаваемой через VPN, злоумышленник должен:

- захватить весь сеанс соединения, т. е. разместить устройство прослушивания между противоположными концами соединения в том месте, через которое должен передаваться весь трафик VPN;
- использовать большие вычислительные мощности и большое количество времени для перехвата ключа с помощью грубой силы и для дешифрования трафика.

Злоумышленнику гораздо проще использовать имеющуюся уязвимость на компьютере пользователя либо украсть портативный компьютер, например, в аэропорту. Если информация не представляет собой особой важности, в VPN можно использовать любой широко распространенный, мощный алгоритм шифрования.

## Система аутентификации

Третьим компонентом архитектуры VPN является система аутентификации. Как уже говорилось ранее, система аутентификации VPN должна быть двухфакторной. Пользователи могут проходить аутентификацию с использованием того, что они знают, того, что у них есть или с помощью данных о том, кем они являются. При использовании пользовательских VPN отдается предпочтение первым двум вариантам.

Хорошей комбинацией средств аутентификации являются смарт-карты в паре с персональным идентификационным номером или паролем. Производители программного обеспечения, как правило, предоставляют организациям на выбор несколько систем аутентификации. В данном перечне присутствуют ведущие производители смарт-карт.

Примечание

Использование смарт-карт повлечет за собой увеличение стоимости использования VPN для каждого пользователя. Несмотря на то, что это обстоятельство повысит стоимость использования соединения, обеспечение более высокого уровня защиты этого стоит.

Если в организации предпочитают при использовании VPN полагаться только на пароли, они должны быть мощными (как минимум, сочетание из восьми букв, цифр и специальных символов) и регулярно изменяться (каждые 30 дней).

**Протокол VPN**

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.

При соединении рекомендуется использовать стандартные протоколы. В настоящее время стандартным протоколом для VPN является IPSec. Этот протокол представляет собой дополнение к IP, осуществляющее инкапсуляцию и шифрование заголовка TCP и полезной информации, содержащейся в пакете. IPSec также поддерживает обмен ключами, удаленную аутентификацию сайтов и согласование алгоритмов (как алгоритма шифрования, так и хэш-функции). IPSec использует UDP-порт 500 для начального согласования, после чего используется IP-протокол 50 для всего трафика. Для правильного функционирования VPN эти протоколы должны быть разрешены.

Вопрос к эксперту

Вопрос. Работает ли IPSec через межсетевые экраны?

Ответ. С работой IPSec через межсетевые экраны связаны некоторые особенности. Во-первых, на межсетевом экране должен быть разрешен трафик UDP через порт 500 и последующий IP-трафик с протоколом 50. Возможность установки этих разрешений зависит от межсетевого экрана. Кроме этого, возникает вопрос, связанный с использованием трансляции межсетевых адресов (NAT). Если межсетевой экран осуществляет трансляцию адресов для пакетов при их поступлении из интернета во внутреннюю сеть, то ему нужно соответствующим образом транслировать конечный адрес, чтобы трафик достиг внутреннего клиента. Немногие межсетевые экраны способны выполнять эту функцию при работе с трафиком, не использующим порты UDP или TCP.

Внимание!

Некоторые поставщики сетевых услуг (в частности, поставщики каналов DSL и кабельных каналов) ограничивают использование этих протоколов в своих сетях. Для того чтобы иметь возможность их использования, клиенту придется приобрести бизнес-пакет услуг вместо обычного стандартного пакета.

Главной альтернативой протокола IPSec является протокол Secure Socket Layer (SSL), используемый для защиты HTTP (для HTTPS используется порт 443). Однако, принимая во внимание, что технология SSL предназначена для работы на прикладном уровне, она может оказаться не столь эффективной в сравнении с IPSec.

**Типы систем VPN**

Теперь, после обсуждения функционирования сетей VPN, давайте рассмотрим непосредственное применение VPN внутри организации. Помимо вопросов, связанных с политикой и управлением, организации нужно выбрать тип приобретаемой системы VPN. На момент написания данной книги можно выделить три типа VPN-построителей:

- аппаратные системы;
- программные системы;
- веб-системы.

**Аппаратные системы**

Аппаратные системы VPN, как правило, базируются на аппаратной платформе, используемой в качестве VPN-сервера. На этой платформе

выполняется программное обеспечение производителя, а также, возможно, некоторое специальное программное обеспечение, предназначенное для улучшения возможностей шифрования. В большинстве случаев для построения VPN на системе удаленного пользователя необходимо наличие соответствующего программного обеспечения. Аппаратные платформы также могут использоваться для построения межузловых VPN, хотя это зависит от производителя оборудования.

Аппаратная система VPN имеет два преимущества.

- Скорость. Оборудование, как правило, оптимизировано для поддержки VPN, посредством чего обеспечивается преимущество в скорости по сравнению с компьютерными системами общего назначения. За счет этого достигается возможность поддержки большего числа одновременных VPN-соединений.
- Безопасность. Если аппаратная платформа специально разработана для приложения VPN, из ее системы удалены все лишние программы и процессы. За счет этого снижается степень подверженности атакам по сравнению с компьютерной системой общего назначения, в которой работают другие процессы. Это не значит, что компьютер общего назначения не может быть должным образом защищен. Как правило, использование компьютера общего назначения требует дополнительных усилий по настройке безопасности.

Внимание!

Тот факт, что VPN используется на базе аппаратной платформы, не означает, что система никогда не подвергнется атаке. Владелец системы должен регулярно проверять наличие обновлений, выпускаемых производителем системы.

**Программные системы**

Программные VPN работают на компьютерных системах общего назначения. Они могут быть установлены на выделенной для VPN системе либо совместно с другим программным обеспечением, таким как межсетевой экран. При загрузке программного обеспечения необходимо обеспечить достаточную мощность аппаратной платформы для поддержки VPN. Так как VPN-продукт устанавливается на компьютеры, имеющиеся в организации, руководство организации должно позаботиться о соответствии компьютеров предъявляемым требованиям.

Программные VPN-системы могут использоваться таким же образом, как и аппаратные системы. Существует программное обеспечение для поддержки пользовательских и узловых VPN.

Примечание

При установке программного обеспечения VPN необходимо обеспечить соответствующую конфигурацию системы, а также устранить все уязвимости, установив нужные обновления.

**Веб-системы**

Главным недостатком большинства пользовательских систем VPN является потребность в установке программного обеспечения на систему-клиент. Бесспорно, что программное обеспечение, которое устанавливалось на клиентские системы, увеличивало объем работ по управлению пользовательскими VPN. Более того, клиентское программное обеспечение во многих случаях не работало должным образом с некоторыми приложениями, загруженными на компьютер-клиент. Это обстоятельство повышало стоимость поддержки и приводило к тому, что многие организации стали устанавливать на специально выделенные компьютеры только программное обеспечение VPN.

Указанные проблемы привели к тому, что некоторые производители VPN стали рассматривать веб-браузеры в качестве VPN-клиентов и реализовывать этот подход на практике. Он заключается в том, что пользователь с помощью браузера подключается к VPN через SSL. SSL обеспечивает шифрование трафика, а подтверждение подлинности пользователя выполняется с помощью средств аутентификации, встроенных в систему. Для предоставления пользователю необходимых услуг используется несколько различных механизмов. Среди них можно выделить надстройки браузера и виртуальные машины Java.

В то время как стоимость поддержки и обслуживания несомненно ниже, на момент написания этой книги ни одна из бесклиентных систем VPN не обеспечивает полную функциональность. Этим сетям VPN присущи ограничения, заключающиеся в наборе используемых приложений и методе подключения пользователей к внутренним системам. Организациям следует рассматривать вариант использования таких систем, так как это снижает затраты на обслуживание, однако необходимо учитывать непосредственные требования пользователей и согласовать их с ограничениями, имеющимися в системах.

**Определение различий между типами VPN**

На предприятии принято решение использовать VPN, в результате чего установлен VPN-построитель. Необходимо составить оценочный отчет о методах шифрования, протоколах туннелирования и аспектах безопасности, связанных с приложениями, которые могут использовать VPN, такими как средства передачи голоса и видеоданных через службы IP

(видеоконференции, усовершенствованные и измененные функции PBX) и средства удаленного хранения/резервирования и восстановления. Обязательно ли шифрование данных в каждом из случаев?

Для каждого из приложений следует выяснить следующее.

1. Какой тип VPN лучше использовать для приложения - межузловую или пользовательскую VPN?
2. Где расположены конечные узлы VPN? Каким опасностям могут подвергаться эти конечные узлы?
3. Налагают ли конечные узлы или пользователи приложения какие-либо дополнительные требования к механизму аутентификации, связанному с VPN?
4. Определите соответствующие приложению механизмы аутентификации.
5. Отследите информацию во время передачи. Является ли она открытой для перехвата или прослушивания? Если да, определите, обеспечивает ли используемый механизм шифрования должный уровень защиты информации.

**Выводы**

То, что хорошо работает с одним приложением, может вовсе не работать с другой программой. Межузловые и пользовательские VPN имеют различные требования к аутентификации и безопасности конечных узлов. Это необходимо принимать в расчет при построении VPN для использования приложением. Выбор механизма шифрования и мощность используемого алгоритма шифрования напрямую влияет на то, какие атаки будут пресекаться. В процессе разработки необходимо принимать во внимание все имеющиеся угрозы безопасности.

**Контрольные вопросы**

1. Можно ли рассматривать использование SSH как реализацию VPN?
2. Почему пользовательские VPN требуют строгой аутентификации?
3. Может ли шифрование полностью защитить данные, передаваемые через VPN.
4. С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?
5. Пригодны ли межузловые VPN для использования между организациями?
6. Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?
7. Какие два критерия должны использоваться для определения того, какое устройство следует использовать - межсетевой экран или VPN-сервер на отдельной системе?

8. Если используется отдельный VPN-сервер, должен ли он размещаться в демилитаризованной зоне интернета?
9. Почему процесс реализации VPN представляет собой гораздо большее, чем выбор алгоритма шифрования?
10. Какие механизмы аутентификации лучше всего использовать для пользовательской VPN?