VPN на основе IPSec

Более масштабным средством защиты трафика по сравнению с защищенными каналами являются виртуальные частные сети (VPN). В зависимости от используемых технологий безопасности данных сети виртуальные частные сети делятся на два класса:

- *сети VPN на основе разграничения трафика*;
- *сети VPN на основе шифрования* работают на основе рассмотренной техники защищенных каналов.

Виртуальная частная сеть на основе шифрования может быть определена как совокупность защищенных каналов, созданных предприятием в открытой публичной сети для объединения своих филиалов.

Основной публичной сетью является сегодня Интернет и большинство типов защищенных каналов, стандартизованных сегодня, работают в Интернете «из конца в конец», используя стандартный протокол IP. Защищенный канал может быть образован силами клиента Интернета и от провайдеров обоих окончаний канала требуется только предоставление стандартного доступа в Интернет. В этом состоит основное преимущество VPN на основе шифрования от VPN на основе разграничения трафика — первые работают в пределах всего Интернета, в то время как вторые — в пределах сети одного провайдера, поддерживающего MPLS.

Сети VPN на основе шифрования могут быть организованы как силами клиентов, так и силами провайдеров, но последний вариант распространен мало.

Сеть VPN на основе шифрования представляет собой своего рода «сеть в сети», то есть сервис, создающий у пользователей иллюзию существования их частной сети внутри публичной сети. Одним из важнейших свойств такой «частной сети» является защищенность трафика от атак пользователей публичной сети. Сетям VPN доступна не только способность имитации частной сети; они дают пользователю возможность иметь собственное адресное пространство (например, частные IP-адреса, такие как адреса сети 10.0.0.0) и обеспечивать качество обслуживания, близкое к качеству выделенного канала.

Технологии VPN на основе шифрования включают шифрование, аутентификацию и туннелирование.

- Шифрование гарантирует конфиденциальность корпоративных данных при передаче через открытую сеть.
- Аутентификация отвечает за то, чтобы взаимодействующие системы (пользователи) на обоих концах VPN были уверены в идентичности друг друга.
- Туннелирование предоставляет возможность передавать зашифрованные пакеты по открытой публичной сети.

Для повышения уровня защищенности виртуальных частных сетей технологии VPN на основе шифрования можно применять совместно с технологиями VPN на основе разграничения трафика. Технологии VPN на основе разделения трафика иногда критикуют за недостаточный уровень безопасности, считая, что без шифрования трафика персонал поставщика услуг может получить несанкционированный доступ к данным. Действительно, такая вероятность существует, поэтому клиент услуг VPN на основе разграничения трафика, например, MPLS VPN, может самостоятельно повысить защищенность своего трафика, прибегнув, скажем, к шифрованию передаваемых данных.

Сейчас наиболее широко используются сети VPN на основе протоколов IPSec и SSL.

Стандарты IPSec обеспечивают высокую степень гибкости, позволяя выбрать нужный режим защиты (с шифрованием или только с обеспечением аутентичности и целостности данных), а также использовать различные алгоритмы аутентификации и шифрования. Режим инкапсуляции IPSec позволяет изолировать адресные пространства получателя (клиента) и поставщика услуг за счет применения двух IP-адресов — внешнего и внутреннего.

Сети VPN на основе IPsec, как правило, строятся по типу CPVPN, то есть как виртуальные частные сети, в которых клиент самостоятельно создает туннели IPSec через IP-сеть поставщика услуг. Конфигурирование сетей VPN на основе IPSec довольно трудоемко, поскольку туннели IPSec двухточечные, то есть при полносвязной топологии их количество пропорционально $N \times (N - 1)$, где N — число соединений. Необходимо учесть еще и непростую задачу поддержания инфраструктуры ключей. Кроме того, протокол IPSec может применяться для создания виртуальных частных сетей, поддерживаемых провайдером (PPVPN) — туннели в них также строятся на базе устройств клиента (CE-

based), но эти устройства удаленно конфигурируются и администрируются поставщиком услуг.

На рис. 1 показан пример организации виртуальной частной сети на основе шифрования, которая обслуживает сотрудников предприятия, работающих удаленно. В корпоративной сети установлен VPN-шлюз, который объединен с корпоративным файерволом (такое объединение функций не является обязательным, хотя часто встречается). На компьютерах удаленных пользователей установлена программа —PN-клиент. PN-клиент обращается к шлюзу и устанавливает с ним защищенный канал. Шлюз VPN должен обладать высокой производительностью для того, чтобы поддерживать одновременно достаточное количество сеансов с удаленными пользователями. Программное обеспечение шлюза должно также позволять администратору VPN управлять учетными записями удаленных пользователей, а также ключами, применяемыми для аутентификации и шифрования. Учитывая высокий риск ошибки аутентификации удаленного пользователя, эта процедура должна быть максимально надежной, например, двухфакторной аутентификацией с использованием пароля и аппаратного токена доступа.

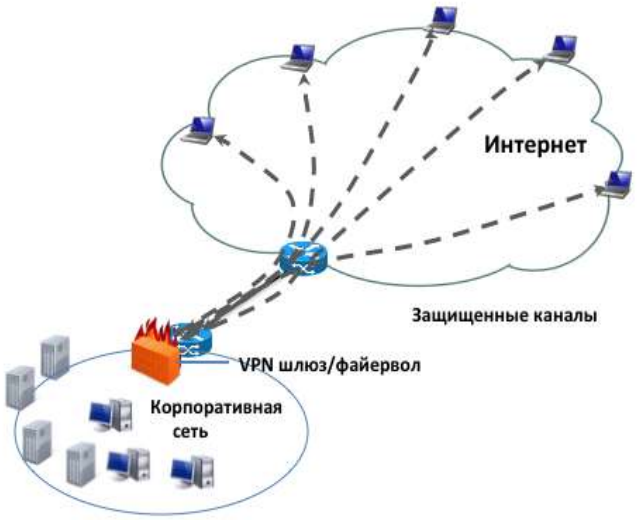

Рис. 1. VPN доступа на основе шифрования

В VPN на основе шифрования возможно также использование защищенного канала на основе протокола SSL. Напомним, что этот протокол работает на уровне представления, непосредственно под прикладным уровнем, так что приложения, чтобы создать защищенный канал для своего трафика, должны вызывать его *явным* образом. Наиболее популярным приложением, использующим защищенные каналы SSL, является веб-браузер. Защищенные каналы SSL образуются здесь на основе протокола HTTP, который в этом режиме работы называют протоколом HTTPS. Пользователи Интернета хорошо знают этот режим, так как браузер прибегает к нему во всех случаях, когда необходимо обеспечить конфиденциальность передаваемой информации: при покупках в интернет-магазинах, при интернет-банкинге, и т. п.

Служба VPN на основе SSL функционирует на базе веб-портала, развернутого в локальной сети организации. Пользователи такой защищенной службы VPN получают удаленный доступ к ресурсам этой локальной сети, обращаясь к веб-порталу посредством обычного браузера через порт 443 (TCP-порт протокола HTTPS). Отсутствие специального клиентского программного обеспечения, требующего настройки, является значительным преимуществом VPN на основе SSL.