VPN-технологии для Интернет-провайдеров ISP

Андрей Березин "Элвис+"
Сетевой журнал №10.2000

Корпоративным пользователям Интернета требуется качество передачи данных.

Сегодня глобальная компьютерная сеть Интернет становится доступной все большему числу российских компаний, для которых она является не только источником информации и удобным и, главное, дешевым средством ее передачи, но и необходимым условием для успешного ведения бизнеса любой современной компании. Однако увлечение Интернетом может самым негативным образом сказаться на бизнесе компании, поскольку утечка конфиденциальной информации о клиентах и поставщиках, финансовых потоках, деталях контрактов и тендерных предложений, товарных запасах, планах развития и т.д., может стать для нее причиной многих неожиданных неудач и нанести бизнесу данной компании вполне конкретный и значительный материальный ущерб.

Осознавая данную проблему, корпоративные пользователи Интернета в наиболее развитых странах мира уже начинают предъявлять все большие требования не только к скорости доступа, но и к качеству передачи данных, которое наряду с традиционными параметрами QoS включает в себя и обеспечение конфиденциальности, целостности и подлинности информации, передаваемой через Интернет. Особенно важным это требование становится в тех случаях, когда корпоративные пользователи по причине чрезвычайной дороговизны выделенных каналов и недостаточной их защищенности вынуждены строить собственные системы информационной безопасности (СИБ) как в рамках intranet, так и extranet сетей.

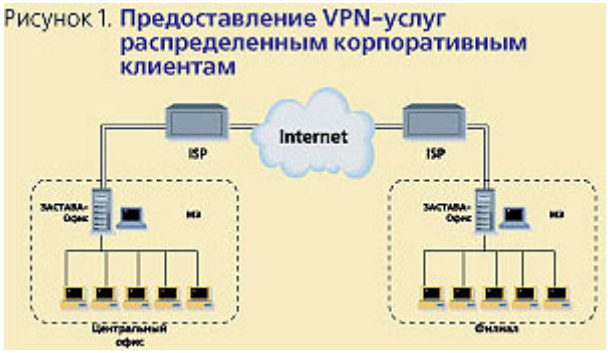

Рисунок 1. Предоставление VPN-услуг распределенным корпоративным клиентам

По мнению большинства экспертов сегодня одним из самых грамотных и экономически выгодных решений для создания СИБ становится построение так называемых Virtual Private Network (VPN) - защищенных виртуальных частных сетей, основанных на современных технологиях криптографической защиты передаваемых по открытым сетям данных. Стратегические преимущества применения VPN-технологий, видимо, уже осознали большинство распределенных компаний, поскольку отказ от выделенных линий связи и переход на VPN уже приобрел массовый характер не только на Западе, где рынок VPN-услуг в последнее время очень активно развивается, но и в России. Причем, что интересно, доминирующее положение на рынке VPN-услуг на Западе начинают занимать не специализированные фирмы - системные интеграторы, а Интернет-провайдеры, которые постепенно расширяют спектр предлагаемых своим клиентам услуг, в том числе и за счет VPN, превращаясь из традиционных Интернет-провайдеров (ISP) в сервис-провайдеров (xSP).

На наш взгляд, для такого развития событий есть целый ряд объективных причин: ISP "по определению" уже имеет доступ к каналам связи и другим сетевым сервисам своих клиентов, поэтому для последних становится организационно, экономически, и, если хотите, психологически выгодно передать решение всего комплекса проблем, связанных с использованием Интернет, "в одни руки"; часто ISP не только предоставляет (передает в аренду или лизинг) своим клиентам сложное телекоммуникационное оборудование доступа в Интернет, но и удаленно управляет этим оборудованием. Поэтому расширение списка оконечного оборудования клиента за счет еще одного устройства (VPN-шлюза) не является организационной проблемой ни для ISP, ни для клиента; ISP находится достаточно близко к клиенту, что позволяет ему оперативно манипулировать своей ценовой политикой, тем самым делая VPN-услуги выгодными для клиента, и т.д.

В такой ситуации российским ISP, очевидно, необходимо срочно предпринять какие-то действия, которые бы также позволили им занять значительную часть этого относительно нового для России рынка - рынка VPN-услуг. И нам кажется, что для этого в России уже имеются все предпосылки: рост интереса к СИБ, высокий профессиональный уровень специалистов ISP, наличие широкой номенклатуры VPN-продуктов от разных производителей и т.д. Вопрос заключается лишь в том, как начать предлагать VPN-услуги своим клиентам?

Давайте рассмотрим на практике реализацию ограниченного количества типовых VPN-услуг на базе, например, достаточно хорошо известных VPN-продуктов линии **ЗАСТАВА** московской компании "ЭЛВИС+" , функционирующих на базе ОС Windows 95/98/NT и Solaris Sparc/Intel:

- ЗАСТАВА-Клиент - программный продукт для защиты клиентских компьютеров корпоративной VPN.
- ЗАСТАВА-Сервер - программный продукт для защиты серверных, в том числе многопроцессорных, платформ, поддерживает защищенный режим обмена информацией пользователей ЗАСТАВА-Клиент с изменяющимися IP-адресами.
- ЗАСТАВА-Офис - программный продукт для защиты ЛВС компании, обладающий развитыми средствами управления политикой сетевой безопасности ЛВС и сокрытия топологии сети, а также выполняющий функций маршрутизатора.

  Выбор именно российских VPN-продуктов обоснован прежде всего тем, что, с одной стороны, "легальность" использования западных VPN-продуктов, вернее встроенных в сетевое оборудование ряда известных западных фирм (Cisco, Intel, 3Com и др.) VPN-модулей, на территории России вызывает большие сомнения (см. Указ Президента РФ №334 от 3.04.95). С другой стороны, известные экспортные ограничения, налагаемые правительством США на "сильные" криптографические алгоритмы, существенно снижают общую криптостойкость защиты трафика упомянутыми средствами. Российские же VPN-продукты лишены этих недостатков и, кроме того, благодаря высокой технологической проработанности, уже получили признание на международном рынке и полностью совместимы с продуктами мировых производителей Cisco, CheckPoint, Sun Microsystems и т.д.

  Очевидно, что предложение по предоставлению VPN-услуг может быть актуальным только для тех клиентов, которые имеют как минимум два удаленных друг от друга офиса. При этом услуги доступа в Интернет для этих офисов могут предоставляться как одним ISP, так и двумя или более. Последний вариант является более предпочтительным, поскольку снимает проблему построения взаимоотношений между двумя ISP на "горизонтальном" уровне. Однако это в любом случае не должно стать большой проблемой, поскольку оба ISP в результате получают значительный рост трафика своих клиентов и, как следствие, повышение своих доходов.

  Техническая реализация VPN-услуги на базе продуктов ЗАСТАВА очень проста и заключается в том, что в состав оконечного оборудования доступа к сети Интернет для обоих офисов компании (назовем их центральным офисом и филиалом), помимо стандартного телекоммуникационного оборудования, включается и VPN-шлюз на базе ЗАСТАВА-Офис (рис.1). Таким образом, клиент получает готовое управляемое решение по созданию VPN-сети между ЛВС удаленных офисов, а также возможность подключения к этой VPN сети своих удаленных/мобильных пользователей и партнеров по бизнесу в защищенном режиме при помощи VPN-продуктов ЗАСТАВА-Клиент.

  Данное техническое решение может быть также расширено предложением аутсорсинга услуг по обеспечению информационной безопасности ЛВС клиента путем включения в состав оконечного оборудования еще и МЭ. Такое предложение может оказаться очень привлекательным для небольших фирм или филиалов, в штате которых нет грамотных технических специалистов по СИБ. Наиболее грамотным решением в данном случае является использование в качестве аппаратной платформы персонального компьютера на базе процессора SunSparc/Intel с установленной ОС Solaris/WinNT. В таком случае на один компьютер можно будет установить как VPN-шлюз, так и МЭ, что является оптимальным решением с точки зрения построения СИБ. Кроме того, такое решение предоставляет ISP возможность осуществлять удаленное управления установленного ПО с рабочего места администратора в защищенном режиме, что также является удобным и выгодным решением для клиента.

Применение VPN-технологий для расширения бизнеса ISP не ограничивается только лишь предложением VPN-услуг распределенным компаниям. Эти технологии также могут быть успешно применены как для нужд самого ISP, так и для решения проблем обеспечения ИБ, например, популярных Интернет-магазинов.

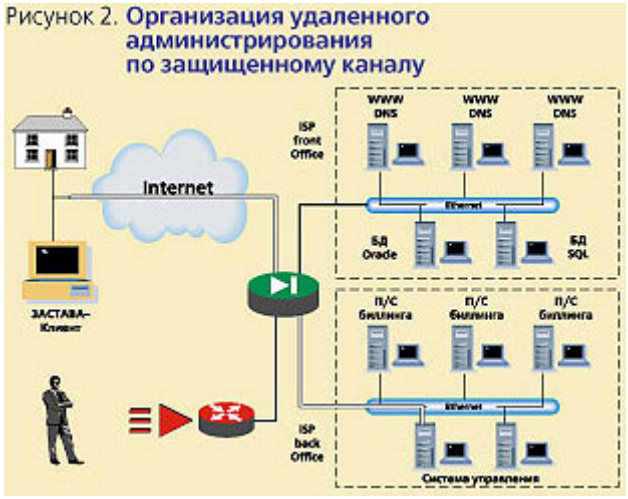

Рисунок 2. Организация удаленного администрирования по защищенному каналу

На рис. 2 показана типовая структурная схема информационной системы ISP. При этом базовым элементом обеспечения собственной внутренней безопасности ИС является логическое разделение ЛВС на два независимых сегмента: это ISP front-office, или так называемая демилитаризованная зона, в которой размещаются все выделенные сервера с клиентскими службами, сервисами и информационными ресурсами; и IPS back-office, в котором размещаются внутренние службы самого ISP: подсистемы управления, мониторинга, контроля, безопасности и т.д. Сегментирование ЛВС производится средствами межсетевого экрана (МЭ).

Применение VPN-технологий к данном случае позволяет ISP организовать безопасный способ удаленного администрирования своей ИС путем организации защищенного VPN-канала между удаленным рабочим местом администратора и сервером системы управления ISP (рис.1). Такое решение является очень популярным для многих ISP на Западе, где администратор ИС вынужден часто управлять своей ИС с мобильного рабочего места (ноутбук), находясь, например, дома или в офисе одного из клиентов.

В тех случаях, когда клиент ISP располагает ценными информационными ресурсами (Интернет-магазин, корпоративный информационный портал, центр управления и центральное хранилище данных корпоративной системы электронного документооборота и т.п.) и желает организовать к ним доступ только для авторизированных пользователей (при том, что стандартное решение на базе SSL-протокола клиента не устраивает по соображениям безопасности), VPN-технологии также помогут достаточно легко решить эту проблему. Техническое решение состоит в том, что ISP строит стандартную VPN-сеть типа "звезда", в центре которой на центральный информационный сервер устанавливается VPN-продукт ЗАСТАВА-Сервер, а на рабочих местах авторизированных пользователей ИС и банков-эмитентов кредитных карт - ЗАСТАВА-Клиент.

Такое техническое решение обеспечивает полную безопасность при авторизации кредитных карт пользователей и позволяет владельцам информационного ресурса удаленно и безопасно работать с ним, а также управлять доступом путем модификации конфигурационной базы данных VPN-продукта ЗАСТАВА-Сервер через удобный графический интерфейс.

Несмотря на кажущуюся логическую простоту применения VPN-технологий (криптографическая защита передаваемой информации "точка-точка"), они обеспечивают большое разнообразие возможных технических решений даже для одного типа IT-компаний - ISP, описать которые в рамках одной статьи не представляется возможным. Напомним, что еще ни слова не было сказано о таком важном качестве VPN-технологий, как масштабируемость: возможность расширения решения по ИБ как "вниз" - в сторону установки средств индивидуальной защиты ПК от

НСД, средств шифрации файлов, разграничения доступа, протоколирования событий и т.д., так и "вверх" - в сторону построения комплексной системы распределения открытых ключей (PKI) для больших корпоративных ИС. Видимо, совокупность всех упомянутых положительных свойств VPN-технологий и позволяет сегодня рассматривать их в качестве "скелета" для построения корпоративных информационных систем, на базе которого возможно создание комплектных систем обеспечения ИБ любой функциональности.