VPN как средство "неотложной помощи"

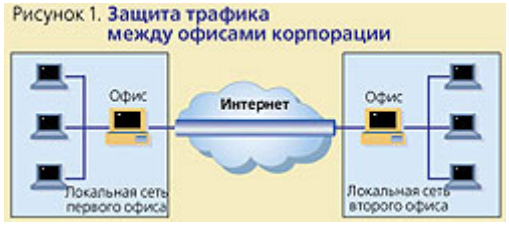
Елена Турская, ОАО"Элвис+"
Сетевой журнал №11.2000
VPN гарантирует надежную защиту информации, передаваемой по Интернет.
Исторически сложилось так, что для защиты передаваемой на большие расстояния информации компании прокладывали собственные линии связи. Этот способ имеет ряд существенных недостатков - не гарантирует надежной защиты коммуникаций, значительно ограничен в применении и требует больших затрат средств и времени. К примеру, как протянуть линию за сотрудником, если он периодически меняет место дислокации или постоянно разъезжает по всей стране?
Конечно, существует большое количество открытых коммуникационных каналов, которые можно арендовать у провайдеров связи или Интернета. Но они также не обеспечивают защиту информации, ее конфиденциальность, аутентичность, целостность, что неприемлемо для реального бизнеса.
Благодаря развитию криптографических технологий появился способ преодолеть эти ограничения - использовать технологию защищенных виртуальных частных сетей (Virtual Private Network - VPN), надежно шифрующих информацию, передаваемую по дешевым открытым сетям, включая Интернет.
Маркетинговая трактовка товара подразумевает, как минимум, две его сущности: потребительскую и физическую.
Потребительская сущность VPN - "виртуальный защищенный туннель, или путь", с помощью которого можно организовать удаленный защищенный доступ через открытые каналы Интернета к серверам баз данных, Web, FTP и почтовым серверам. Физическая сущность технологии VPN определяется тем, что она может защитить трафик любых информационных интранет- и экстранет-систем, аудио--видеоконференций, систем электронной коммерции и т. п.
Существует три аспекта восприятия VPN: VPN - это защита трафика, основанная на криптографии; VPN - это средство коммуникации, так как гарантия защиты доступа к внутренним ресурсам из любой точки страны или мира инициирует применение информационных систем для удаленного доступа - возможность, о которой вы даже и не задумывались раньше; VPN - это средство влияния на стратегию развития коммуникационных систем корпорации: вместо того, чтобы вкладывать огромные средства в строительство собственных выделенных линий, вы практически сегодня же можете получить надежно защищенные каналы связи от коммуникационных провайдеров.
Для руководителя, принимающего решение об установке тех или иных средств или систем, важна и финансовая сущность применения VPN. При правильном выборе VPN:

- вы получаете защищенные каналы связи и защищенный трафик отдельных приложений по цене доступа в Интернет, что в несколько раз дешевле собственных линий;
- при установке VPN не требуется изменять топологию сетей, переписывать приложения, обучать пользователей, т. е. тратить дополнительные средства;
- обеспечивается масштабирование: VPN не создаст проблем роста, что сохранит уже сделанные раньше инвестиции в инфраструктуру безопасности.

  Существует три типовых решения, которые последовательно решают основные задачи корпораций по защите передаваемой информации и созданию системы информационной безопасности:

- защита всего трафика между многочисленными офисами корпорации, когда шифрование выполняется только на выходе из офисов во внешние сети; такая

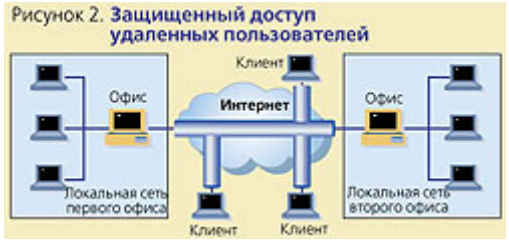
топология образует "защищенный периметр" вокруг локальных сетей корпорации (рис. 1);



- защищенный доступ удаленных пользователей к информационным ресурсам, как правило, через Интернет (рис. 2);
- защита трафика ряда приложений внутри корпоративных сетей (это также важно, поскольку большинство атак осуществляется из внутренних сетей), при этом образуются отдельные, непересекающиеся VPN для выделенных групп пользователей или приложений (рис. 3).

Виртуальная частная сеть VPN, как любая распределенная система, в ее "физической сущности" является сложным комплексом, который требует целого ряда дополнительных комплементарных средств и систем защиты. Ее способность шифровать данные является необходимым, но далеко не достаточным условием для построения действительно надежной защиты. Здесь мы рассмотрим, что должна делать "правильная" VPN, каким отвечать требованиям и как интегрироваться с другими средствами защиты информации.

Основная задача VPN - защита трафика. Эта задача исключительно сложна уже на криптографическом уровне, поскольку VPN должна удовлетворять большому числу требований. И в первую очередь обладать надежной криптографией, гарантирующей от прослушивания, изменения, отказа от авторства (это определяется протоколом IPsec), иметь надежную систему управления ключами, защищать от «подыгрывающих» (replay) атак и проверять, "жив" ли абонент в данный момент (это обеспечивается принятым в 1998 году протоколом IKE). Применение стандартных протоколов IPsec/IKE в VPN-системах сегодня практически обязательно. В противном случае ни один заказчик не сможет быть уверенным, что поставщик VPN создал криптографически целостную и надежную систему. Кроме того, в будущем она окажется несовместима с VPN, применяемыми контрагентами корпорации, что в конце концов приведет к проблеме "вавилонской башни".



Следующим требованием является обеспечение масштабируемости конкретной VPN. Многолетний опыт показывает, что наиболее успешно для этого применяются программные VPN-агенты, которые:

- могут обеспечить защиту трафика на всех типах компьютеров -- рабочих станциях, серверах и шлюзах (на выходе из локальных сетей в открытые сети);
- работают на всех популярных ОС.

Вторая составляющая масштабируемости - централизованное, целостное и оперативное управление VPN. Необходимо определиться со значениями этих понятий в данном контексте:

- централизованное - конфигурирование VPN происходит в одном месте на одной рабочей станции;
- целостное - вся VPN создается как единое целое, поскольку совершенно недопустима ситуация, когда разные узлы имеют несовместимую политику безопасности или включаются в VPN не одновременно;
- оперативное - созданная в центре «конфигурация VPN» должна автоматически за считанные секунды быть разослана на все узлы VPN. Для больших систем неприемлемо, чтобы оператор последовательно, пусть и удаленно, конфигурировал все 300 VPN-узлов или передавал им конфигурации на дискетах.

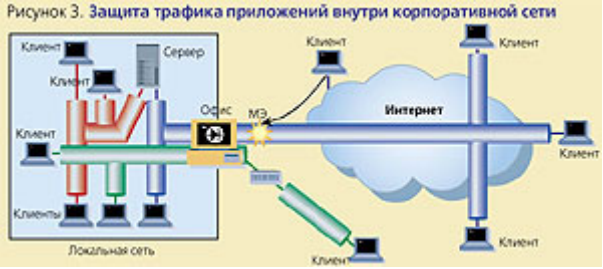


Рисунок 3. Защита трафика приложений внутри корпоративной сети

Наличие приведенных составляющих в системе управления VPN действительно обеспечит ее масштабируемость, поскольку при росте числа участников система будет расширяться без коллизий.

Для предоставления удаленного доступа мобильным пользователям центр управления должен допускать подключение компьютеров, IP-адрес которых ему заранее неизвестен. Участники информационного обмена опознаются по их криптографическим сертификатам. Так как криптографический сертификат пользователя является электронным паспортом, он, как и любой паспорт, должен соответствовать определенным стандартам. В криптографии это X.509.

Требование к поддержке стандарта X.509 далеко не случайно. Не секрет, что ни одна криптозащита, построенная на открытой криптографии, не может существовать без инфраструктуры открытых ключей - PKI (Public Key Infrastructure), в задачу которой входит:

- создание и подпись сертификатов, что требует наличия иерархической системы нотариусов, так как пользователь VPN должен получать свой сертификат по месту работы, а не ездить за ним, например, в центральный офис или в какую-то иную организацию;
- передача сертификатов на электронный носитель пользователя (смарт-карта, e-token, дискета) и публикация их на сервере сертификатов с тем, чтобы любой участник VPN мог легко получить сертификат своего партнера;
- регистрация фактов компрометации и публикация "черных" списков отозванных сертификатов.

VPN должна взаимодействовать с системой PKI в целом ряде точек (передача сертификата на подпись, получение сертификата и "черного" списка при установлении взаимодействия и т. п.). Очевидно, что это взаимодействие с чуждой по отношению к VPN системой может осуществляться только при условии полной

поддержки международных стандартов, которым удовлетворяет большинство современных PKI-систем (например, Baltimore, Entrust, Verisign).

Следующим важным элементом интеграции систем является наличие криптоинтерфейса. Любая система, использующая криптооперации (VPN, защищенная почта, программы шифрования дисков и файлов, PKI), должна получать криптосервис из сертифицированных соответствующими органами криптоплагинов, созданных специализирующимися в этом компаниями. Исключительно опасно доверяться поставщику VPN, создавшему свой собственный, никому не известный, но, как он утверждает, надежный алгоритм.

Обеспечение безопасности - задача построения множества линий обороны и наблюдения за ними. Как бы вы ни осуществляли это наблюдение - ручной разборкой регистрационной информации или с помощью изощренных систем intrusion detection (обнаружения вторжения), вы должны сначала получить эту информацию для "разбора полетов". Чтобы это было возможно, VPN должна создавать на всех своих агентах:

- LOG-файлы с регистрационной информацией;
- SNMP-сообщения о текущих атаках, сбоях и проблемах.

Вся эта информация должна собираться и обрабатываться в том же центре управления, о котором говорилось выше, или в одной из специализированных систем наблюдения (типа HP-OV).

Обычно VPN различает только отдельные компьютеры, но не их пользователей. Корпоративный заказчик требует, чтобы VPN отличала отдельных пользователей и отдельные приложения. Пользователь должен получить одну и ту же конфигурацию VPN независимо от того, за каким компьютером он сидит.

Все необходимые для этого данные (ключи, сертификаты, конфигурация) находятся на его смарт-карте, электронном ключе или дискете. Если корпорация использует так называемые серверы доступа (технология single-sign-on), то VPN должна работать совместно с такой системой, не подключая VPN тем пользователям, которые не прошли авторизацию в системе аутентификации.

VPN образует "непроницаемые" каналы связи поверх открытых сетей. В реальной жизни организации всегда требуется, чтобы сотрудники имели доступ из VPN в открытые сети и Интернет. Контроль в критичной точке контакта с открытой сетью должен осуществляться межсетевыми экранами. Более правильная ситуация - VPN обеспечивает функции межсетевого экрана в каждой точке, где есть ее агент. Такой "распределенный" межсетевой экран контролируется из того же центра безопасности. Межсетевой экран и VPN являются комплементарными системами, решая две связанные задачи:

- использование открытых сетей в качестве канала недорогой связи (VPN);
- обеспечение защиты от атак из открытых сетей при работе с открытой информацией, содержащейся в этих сетях (межсетевой экран).

Гарантируя защиту передаваемой информации, VPN не обеспечивает ее защиту во время хранения на конечных компьютерах. Эта задача решается целым рядом специальных средств:

- систем криптозащиты файлов и дисков (а также почты);
- систем защиты от несанкционированного доступа к компьютерам;
- антивирусных систем и т. п.

Необходимо обратить внимание на сложную взаимосвязь продуктов защиты информации. Например, система защиты компьютера от несанкционированного доступа должна работать с теми же смарт-картами, что и VPN, а это требует реализации в обеих системах единого интерфейса доступа к смарт-карте (например, PKCS#11 фирмы RSA).

"Правильные" средства защиты информации должны обладать следующим набором характеристик:

- соответствие открытым международным стандартам;
- открытые интерфейсы к другим средствам защиты информации;
- способность взаимодействовать с одними и теми же "интегрирующими" элементами системы;
- способность к масштабированию.

Продукты, создаваемые для защиты информации, должны быть совместимы с системами PKI, известными на российском рынке. И прежде всего с сервером сертификатов - программным средством управления VPN. Сервер сертификатов предназначен для хранения в виде базы данных открытых сертификатов всех пользователей VPN. Он осуществляет автоматическую раздачу сертификатов VPN-устройствам и взаимодействие с внешними системами PKI.

Итак, начав с отдельного средства, обеспечивающего оперативное решение проблемы защиты информации, - VPN, мы рассмотрели процесс наращивания системы, добавив сначала необходимые компоненты, без которых VPN не может функционировать вообще (PKI, криптоплагины, межсетевые экраны), и дополнили затем общую картину более полным спектром продуктов.