Защита информации в сетях территориально распределенных организаций

Елена Турская, ОАО"Элвис+"
"CRN-Enterprise Partner", №14, 2000

Большие компании имеют множество потенциальных преимуществ, связанных с их размером. Но для реализации этих преимуществ необходимо, как минимум, одно условие- способность эффективно обрабатывать и передавать информацию, зачастую конфиденциальную, на большие расстояния. Причем, расстояния - не единственная проблема распределенного предприятия. Другая проблема - это время, такой же ресурс, как финансы, персонал, информация.

На рынке появляются онлайновые информационные системы, которые обеспечивают современному бизнесу необходимую оперативность информации. Стоимость циркулирующей в этих системах информации высока, и ее (информацию) необходимо защищать, причем не только от подглядывания, но и от изменения (всего один ноль превратит десять тысяч долларов в сто тысяч), а также от отказа от авторства..

Самая острая проблема распределенных организаций- защита передаваемого на большие расстояния трафика. Начиная ее решать, корпорации постепенно переходят к системному подходу к защите информации, соединяя различные средства и системы защиты информации (СЗИ) в единое целое.

С ЧЕГО НАЧИНАЕТСЯ РЕШЕНИЕ ПРОБЛЕМ

Исторически для защиты передаваемой на большие расстояния информации компании прокладывали свои собственные линии связи. Этот способ имеет ряд существенных недостатков - он требует очень больших затрат средств и времени, не обеспечивает надежную защиту коммуникаций и его применимость существенно ограничена. Как, к примеру, протянуть линию к сотруднику, который разъезжает по всей стране?

Существует большое количество открытых коммуникационных каналов, которые можно арендовать у провайдеров связи. Но они не обеспечивают защиту информации, ее конфиденциальность, аутентичность, целостность, что неприемлемо для реального бизнеса.

Благодаря развитию криптографических технологий появился способ преодолеть эти недостатки и ограничения. Одна из них - технология защищенных виртуальных частных сетей (Virtual Private Network - VPN), надежно шифрующих информацию, передаваемую по открытым (более дешевым) сетям, включая Интернет.

Потребительская сущность VPN - это "виртуальный защищенный туннель". С помощью технологии VPN можно организовать удаленный защищенный доступ через открытые Интернет-каналы к серверам баз данных, Web-, FTP- и почтовым серверам. VPN может защитить трафик любых информационных интранет- и экстранет-систем, аудиовидеоконференций, систем электронной коммерции.

Необходимо сразу развеять одно серьезное заблуждение, навязываемое некоторыми поставщиками VPN-систем. Оно состоит в том, что VPN - единственное средство, которое позволит вам организовать работу мультимедийных систем, электронную коммерцию, доступ к интрасетям и т.д. Все эти системы могут существовать и без VPN. Просто их опасно использовать без должной степени защиты. Все, что делает VPN, - это обеспечивает надежную защиту трафика *любой* из этих систем. Важно, что VPN делает это совершенно прозрачно для всех приложений, не вмешиваясь в их работу.

VPN можно воспринимать как:

- защиту трафика, основанную на криптографии;

- средство коммуникации; так как возможность получить защищенный доступ к вашим внутренним ресурсам из любой точки мира инициирует применение информационных систем для такого удаленного доступа - возможность, о которой вы раньше, возможно, и не задумывались;
- средство влияния на стратегию развития коммуникационных систем вашей фирмы: вместо расходования огромных средств на строительство собственных выделенных линий вы сможете практически сегодня получить надежно защищенные каналы связи от коммуникационных провайдеров.

Руководителю, принимающему решение об установке тех или иных средств или систем, может быть интересен финансовый аспект применения VPN. При *правильном выборе* VPN:

- компания получает защищенные собственные каналы и защищенный трафик отдельных приложений по цене доступа в Интернет, что на несколько порядков дешевле владения собственными линиями;
- при установке VPN не требуется изменять топологию сетей, переписывать приложения, обучать пользователей, т.е. тратить дополнительные ресурсы;
- обеспечивается масштабируемость: VPN не создаст проблем роста, что сохранит инвестиции в инфраструктуру безопасности.

Существуют три типовых подхода, позволяющих последовательно решать основные задачи компаний по защите передаваемой информации:

- защита всего трафика между многочисленными офисами компании, когда шифрование выполняется только на выходе из офисов во внешние сети; такая топология образует "защищенный периметр" вокруг локальных сетей компании ;
- защищенный доступ удаленных пользователей к информационным ресурсам, как правило, через Интернет;
- защита трафика отдельных приложений во внутрикорпоративных сетях (это также важно, поскольку от 50 до 70% атак осуществляется из внутренних сетей). При этом образуются отдельные непересекающиеся VPN для отдельных групп пользователей или приложений .

Функциональные свойства "правильной" VPN и ее интеграция с системой информационной безопасности

VPN как любая распределенная система в "физической сущности" представляет собой сложный комплекс, который требует целого ряда дополнительных комплементарных систем защиты. Способность VPN шифровать данные - необходимое, но далеко не достаточное условие для построения действительно надежной защиты.Что должна делать "правильная" VPN, каким она должна отвечать требованиям и как интегрироваться с другими СЗИ?
Основная задача VPN - защищать трафик. Эта задача исключительно сложна на криптографическом уровне, и для ее решения VPN должна удовлетворять большому числу требований: в первую очередь обладать надежной криптографией, защищающей от прослушивания, изменения, отказа от авторства , и иметь надежную систему управления ключами., Эти требования определены протоколами IPsec/IKE.Применение этихстандартных протоколов в VPN-системах сегодня практически обязательно, иначе:

- ни один заказчик не сможет быть уверенным, что поставщик VPN создал криптографически целостную и надежную систему;
- она будет несовместима в будущем с VPN, применяемыми контрагентами фирмы, что в конце концов приведет вас к необходимости смены оборудования и ни о каком сохранении инвестиций не может быть и речи.

Следующее требование - обеспечение масштабируемости конкретной VPN. Наиболее удачный подход к реализации этого требования- это использование программных VPN-агентов, которые могут обеспечить защиту трафика на всех типах компьютеров: рабочих станциях, серверах и шлюзах (на выходе из локальных сетей в открытые) - и работают под управлением всех популярных ОС.
Еще одна, не менее важная, составляющая масштабируемости - *централизованное целостное оперативное*управление VPN. Необходимо определиться со значениями этих понятий в данном контексте. "Централизованное" обозначает, что конфигурирование VPN происходит в одном месте на одной рабочей станции. "Целостное"подразумевает, что вся VPN должна создаваться 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 рассылаться на все узлы VPN; для больших систем недопустимо, когда оператор последовательно, пусть и удаленно, конфигурирует все 300 узлов VPN или передает им конфигурации на дискетах.
Такая система управления действительно обеспечит масштабируемость, поскольку при росте числа участников VPN система будет расширяться без коллизий.
Чтобы обеспечить удаленный доступ мобильным пользователям, центр управления должен допускать подключение компьютеров, IP-адрес которых ему заранее неизвестен. Участники информационного обмена опознаются по их криптографическим сертификатам. Криптографический сертификат пользователя представляет собой электронный паспорт, который, как и любой паспорт, должен соответствовать определенным стандартам - в криптографии это X.509.
Требование поддержки 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 задачи которой входит:

- создание и подпись сертификатов, что требует наличия иерархической системы нотариусов (пользователь VPN должен получать свой сертификатна рабочем месте);
- 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 PKI в целом ряде точек (передача сертификата на подпись, получение сертификата и "черного" списка при установлении взаимодействия и т.п.). Это взаимодействие с чуждой по отношению к VPN системой может осуществляться только при условии полной поддержки международных стандартов, которым удовлетворяют большинство современных PKI систем.
Еще один важный элемент интеграции систем - наличие криптоинтерфейса. Любая система, использующая криптооперации (VPN, защищенная почта, программы шифрования дисков и файлов, PKI), должна получать криптосервис из сертифицированных соответствующими органами криптоплагинов. Криптоплагины

создают специализирующиеся на этом компании. Исключительно опасно доверяться поставщику VPN, создавшему свой*собственный*, никому не известный, но, как он утверждает, надежный алгоритм.
Обеспечение безопасности представляет собой задачу построения множества линий обороны и наблюдения за ними. Независимо от того, как вы осуществляете это наблюдение сначала нужно получить информацию для анализа. Соответственно, для этого VPN должна создавать на всех своих агентах LOG-файлы с регистрационной информацией и SNMP-сообщения о текущих атаках, сбоях и проблемах. Вся эта информация должна собираться и обрабатываться в том же центре управления, о котором мы говорили раньше, или одной из специализированных систем наблюдения.
Обычно VPN различает только отдельные компьютеры, но не их пользователей. Корпоративным заказчикам важно, чтобы VPN *различала*отдельных пользователей и отдельные приложения. Пользователь должен получить свою конфигурацию VPN независимо от того, за каким компьютером он работает. Все необходимые для этого данные (ключи, сертификаты, конфигурация) находятся на его смарт-карте, электронном ключе или дискете. Если компания использует так называемые серверы доступа, то VPN должна работать совместно с такой системой; при этом VPN не включается 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. Критичные точки контакта с открытой сетью должны контролироваться межсетевыми экранами (firewall, FW). Более правильна ситуация, когда VPN обеспечивает функции FW в каждой точке, где есть ее агент. Такой распределенный FW контролируется из того же центра безопасности. FW и VPN представляют собой комплементарные системы, решающие две взаимосвязанные задачи: использование открытых сетей как канала недорогой связи (VPN) и обеспечение защиты от атак из открытых сетей при работе с открытой информацией, содержащейся в этих сетях (FW).
Обеспечивая защиту передаваемой информации, VPN не обеспечивает защиту во время ее хранения на конечных компьютерах - для этого существует целый ряд специальных СЗИ. Это системы криптозащиты файлов и дисков (а также почты); системы защиты от несанкционированного доступа к компьютерам; антивирусные системы и т.п.

Заключение

Подводя итоги, хочется подчеркнуть, что "правильные" СЗИ обладают следующим набором характеристик:

- построены на открытых международных стандартах;
- имеют открытые интерфейсы к другим СЗИ;
- могут взаимодействовать с одними и теми же "интегрирующими" элементами системы;
- обладают способностью к масштабированию.

И если априори понятно, как будет строиться и в дальнейшем развиваться система, можно создать комплексную систему защиты информации, начиная "снизу", с установки отдельных СЗИ. Это можно делать разными способами, главное - это выбирать "ПРАВИЛЬНЫЕ" СЗИ.