Комплексный подход к защите информации в сетях территориально распределенных корпораций

***Елена Турская**, ОАО «Элвис+»*
READ.ME #4 2000
Представленная статья может быть интересна руководителям, тем, кто определяет стратегию развития коммуникаций или информационных систем компаний, а также техническим специалистам, интересующимся вопросами защиты информации в распределенных системах.
Материал основан на обобщенном опыте работы специалистов компании ЭЛВИС+ с предприятиями, имеющими распределенную структуру, в первую очередь - нефтегазового комплекса, а также банковскими и государственными структурами.
Статья построена на подходе «от частного к общему», который отражает реальное развитие систем безопасности распределенных корпораций. Начав с самой «горящей» проблемы - защиты передаваемого на большие расстояния трафика, корпорации постепенно переходят к системному подходу к защите информации, соединяя различные средства и системы защиты информации в одно целое.

Актуальность проблемы защиты информации для распределенных корпораций
Большие компании обладают множеством потенциальных преимуществ, связанных с их размером. Но одним из условий реализации этих преимуществ является способность компании эффективно обрабатывать и передавать информацию, во многом конфиденциальную, на большие расстояния. Расстояния - не единственная проблема распределенного предприятия. Другой проблемой является время - такой же ресурс предприятия, как финансы, персонал, информация. На рынке появляются «on-line»-овые информационные системы, которые обеспечивают необходимую оперативность информации современному бизнесу.
Стоимость циркулирующей в этих системах информации высока, и ее надо защищать, причем не только от подглядывания (чтобы никто не узнал сумму платежа), но и от изменения ($100000 вместо $10000), а также от отказа авторства («мы этот платежный документ вообще не отправляли!»).
VPN - средство «первой неотложной помощи»
Исторически сложилось так, что 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 есть значительные ограничения в его применении. Как, к примеру, протянуть линию за сотрудником, который разъезжает по всей стране?
При этом существует большое количество открытых коммуникационных каналов, которые можно арендовать у провайдеров связи. Internet сама по себе - тоже канал связи. Но они также не обеспечивают защиту информации, ее конфиденциальность, аутентичность, целостность, что неприемлемо для реального бизнеса.
Благодаря развитию криптографических технологий появился способ преодолеть эти недостатки и ограничения - использовать технологию защищенных виртуальных частных сетей (Virtual Private Network - VPN), надежно шифрующих информацию, передаваемую по дешевым открытым сетям, включая Internet.
Маркетинговая трактовка товара подразумевает, как минимум, две его сущности: потребительскую и физическую. Потребительская сущность VPN проста и понятна - «виртуальный защищенный туннель». Физическая будет рассмотрена в следующем разделе.
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, аудио-, видеоконференций, систем электронной коммерции.
Необходимо сразу развеять одно серьезное заблуждение, навязываемое некоторыми поставщиками VPN-систем: то, что VPN - единственное средство, которое позволит вам организовать работу мультимедийных систем, электронную коммерцию, доступ к интранет и т. д. Все эти системы существуют и без VPN, если, конечно, они у вас существуют. Просто их опасно использовать без должной степени защиты. Все, что делает VPN, - обеспечивает надежную защиту трафика любой из этих систем. Важно то, что VPN делает это совершенно прозрачно для всех приложений, не вмешиваясь в их работу.
Существуют 3 аспекта восприятия VPN:

- VPN - это защита трафика, основанная на криптографии;
- VPN - это средство коммуникации, т.к. возможность получить защищенный доступ к вашим внутренним ресурсам из любой точки мира инициирует то, что вы начинаете применять информационные системы для этого удаленного доступа, - возможность, о которой вы, возможно, даже и не задумывались раньше;
- VPN - это средство влияния на стратегию развития коммуникационных систем вашей корпорации: вместо выделения огромных средств на строительство собственных выделенных линий вы сможете практически сегодня получить надежно защищенные каналы связи от коммуникационных провайдеров.

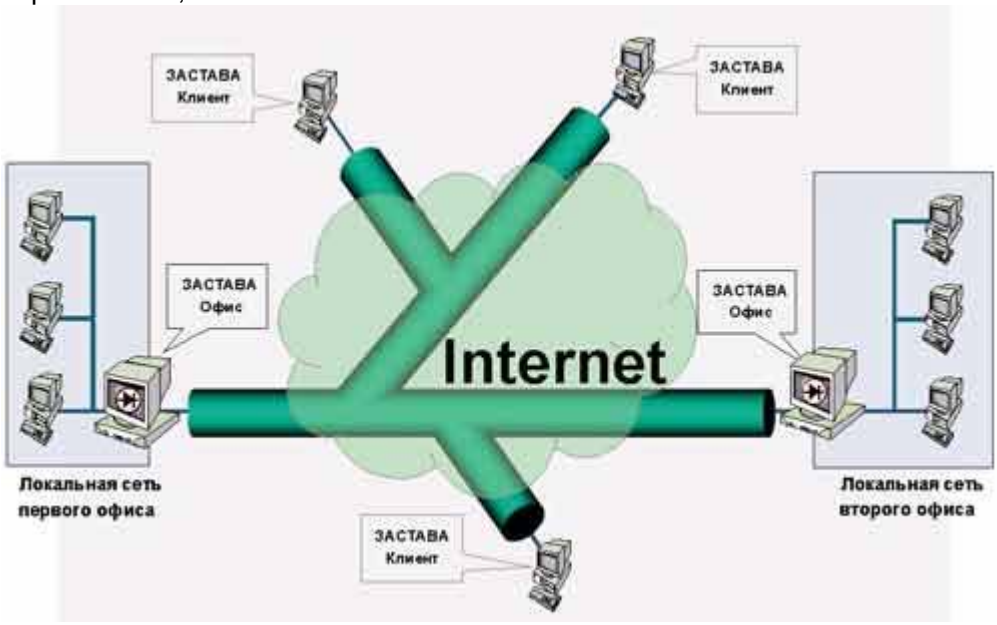
Для руководителя, принимающего решение об установке тех или иных средств или систем, может быть интересен финансовый аспект применения VPN. При правильном выборе VPN:

- вы получаете защищенные собственные каналы и защищенный трафик отдельных приложений по цене доступа в Internet, что на несколько порядков дешевле обладания 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.

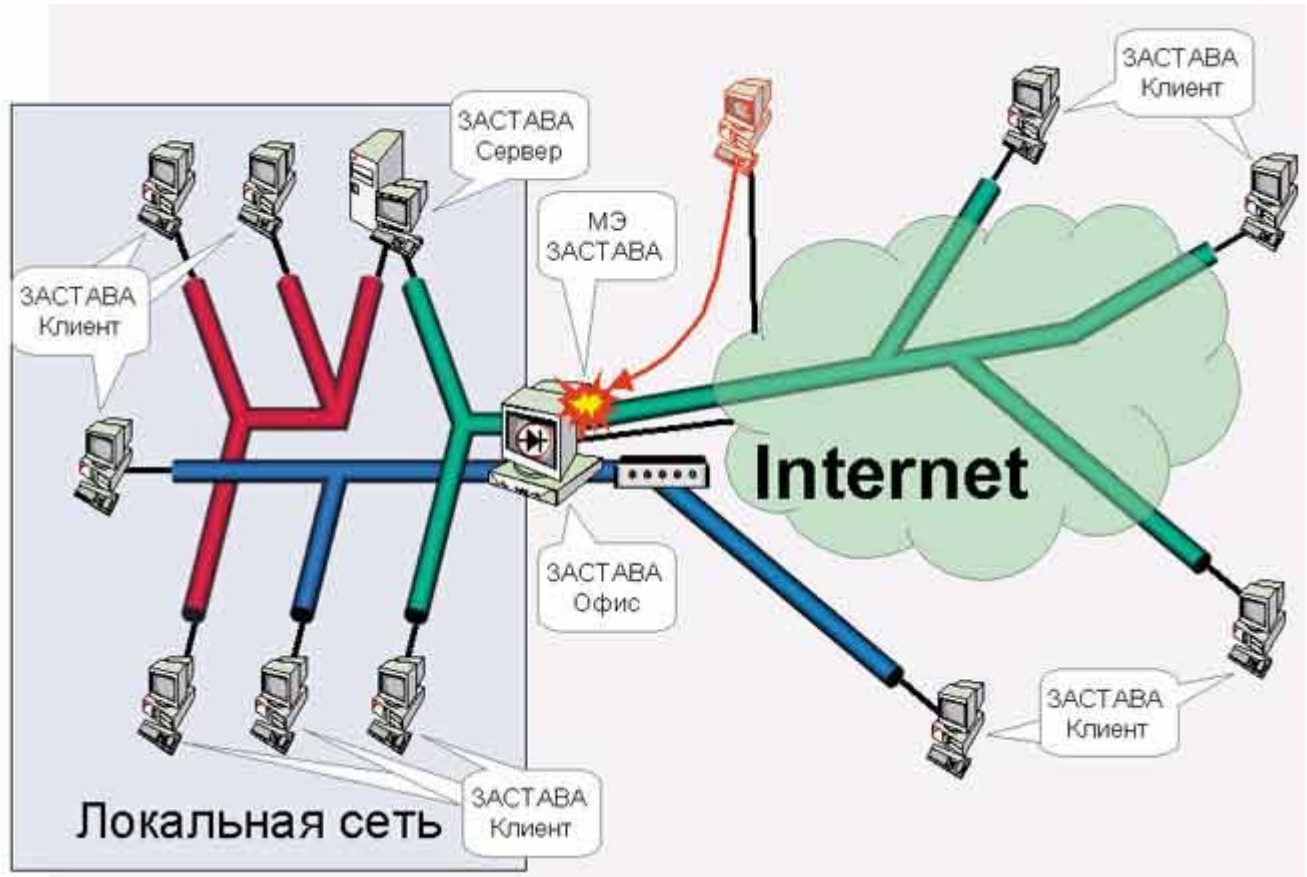
Существуют 3 типовых решения, которые последовательно решают основные задачи корпораций по защите передаваемой информации (для определенности в иллюстрациях используются конкретные продукты VPN ЗАСТАВА, произведенные компанией «Элвис+»):

- защита всего трафика между многочисленными офисами корпорации, когда шифрация выполняется только на выходе из офисов во внешние сети; такая топология образует «защищенный периметр» вокруг локальных сетей корпорации;

- защищенный доступ удаленных пользователей к информационным ресурсам, как правило, через Internet;



- защита трафика отдельных приложений на внутрикорпоративных сетях (это также важно, поскольку большинство атак осуществляется из внутренних сетей), при этом образуются отдельные непересекающиеся VPN для отдельных групп пользователей или приложений.



Эти 3 схемы соответствуют логике развития выполненных нами проектов в крупных корпорациях. Поскольку безопасность вообще и информационная в частности - тема деликатная, мы не имеем возможности описывать конкретные проекты, а ограничимся лишь описанием технологий и решений, основанных на опыте специалистов нашей компании в реализации проектов по защите информации.

Функциональные свойства «правильной» VPN и ее интеграция с системой информационной безопасности VPN, как любая распределенная система, в ее «физической сущности» является сложным комплексом, который требует целого ряда дополнительных комплиментарных систем защиты.
Ее способность шифровать данные является необходимым, но далеко не достаточным условием для построения действительно надежной защиты. В этом разделе мы рассмотрим, что должна делать «правильная» VPN, каким отвечать требованиям, и как она должна интегрироваться с другими средствами защиты информации (СЗИ).
Основная задача VPN - защищать трафик. Эта задача исключительно сложна уже на криптографическом уровне, поскольку VPN должна удовлетворять большому числу требований и, в первую очередь, обладать надежной криптографией, защищающей от прослушивания, изменения, отказа от авторства (это определяется протоколом IPsec), и иметь надежную систему управления ключами, защищать от replay атак, проверять, что абонент «живой» в данный момент (это обеспечивается принятым в 1998 г. протоколом IKE).
Применение стандартных протоколов IPsec/IKE в VPN-системах сегодня является практически обязательным, 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 корпорации, что в конце концов приведет вас к проблеме «вавилонской башни».

Следующим требованием является обеспечение масштабируемости конкретной VPN. Многолетний опыт нашей компании показывает, что наиболее удачно это обеспечивается наличием программных VPN-агентов разных типов, которые:

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

Вторая 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 - 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 быть разослана 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.
Для обеспечения удаленного доступа мобильных пользователей Центр Управления должен допускать подключение компьютеров, IP-адрес которых ему заранее неизвестен. Участники информационного обмена опознаются по их криптографическим сертификатам.
Криптографический сертификат пользователя является электронным паспортом, который, как 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 Москву;

- 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.). Очевидно, что это взаимодействие с чуждой по отношению к VPN системой может осуществляться только при условии полной поддержки международных стандартов, которым отвечают большинство современных PKI систем.
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 не осуществляли это наблюдение - ручной разборкой регистрационной информации или с помощью изощренных систем intrusion detection (обнаружения вторжения), - вы должны сначала получить эту информацию для «разборки полетов». Соответственно, VPN с целью ее получения 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 мы говорили раньше, или одной из специализированных систем наблюдения (типа HP OV).
Обычно VPN различает только отдельные компьютеры, не отличая 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 не его смарт-карте, электронном ключе или дискете. Если корпорация использует т.н. серверы доступа (технология single-sign-on), то VPN должна работать совместно с такой системой, не включая 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 Internet. Контроль в критичной точке контакта с открытой сетью должен осуществляться межсетевыми экранами (FW). Более правильная ситуация - VPN обеспечивает функции FW в каждой точке, где есть ее агент. Такой распределенный FW контролируется из того же центра безопасности. FW и VPN являются комплиментарными системами, решая 2 связанные задачи:

- использование открытых сетей как канал недорогой связи (VPN);
- обеспечение защиты от атак из открытых сетей при работе с открытой информацией, содержащейся в этих сетях (FW). Обеспечивая защиту передаваемой информации, VPN не обеспечивает ее защиту во время хранения на конечных компьютерах. Эта задача решается целым рядом специальных СЗИ:
- системы криптозащиты файлов и дисков (а также почты);
- системы защиты от несанкционированного доступа к компьютерам;
- антивирусные системы;
- и т. п.

Выводы

Начав с отдельного СЗИ, обеспечивающего «оперативное решение», - VPN, мы рассмотрели процесс «наращивания» системы, добавив сначала «необходимые» компоненты, без которых VPN

не может функционировать вообще (PKI, криптоплагины, FW), а затем дополнили схему более полным спектром продуктов. Необходимо обратить внимание на сложную взаимосвязь продуктов защиты информации. Например, система защиты компьютера от НСД должна работать с теми же смарт-картами, что и VPN, что требует реализации в обеих системах единого интефейса доступа к смарт-карте (например, PKCS#11 фирмы RSA).
Исходя из описанного выше, можно сделать практические выводы, что комплексную систему безопасности можно построить, начиная «снизу», с установки отдельных СЗИ, если сразу понимать, как она будет строиться, и как эта система будет развиваться в дальнейшем.
Можно делать это разными способами: привлекать системных интеграторов, не привлекать таковых (основываясь на русской привычке все делать своими руками), главное - выбирать «правильные» СЗИ.
«Правильные» СЗИ обладают следующим набором характеристик:

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