ГРАМОТНАЯ ЗАЩИТА ИНФОРМАЦИОННЫХ ПОТОКОВ

Антон Александров,
менеджер продуктов и решений ОАО «ЭЛВИС-ПЛЮС»

BYTE, 10 апреля 2004 г.

В современном мире коммерческий успех любого предприятия все в большей степени зависит от оперативности и мобильности бизнеса. А это невозможно без надежного и качественного информационного взаимодействия между различными участниками бизнес-процессов. Сегодня предприятия в качестве среды для информационного обмена все чаще используют общедоступные (открытые) каналы связи сетей общего доступа (например, Интернета). Конечно, можно воспользоваться выделенными каналами, но это обходится дороже. Выбор в пользу открытых каналов Интернета делается именно по причине их дешевизны по сравнению с выделенными каналами. Однако сетям общего пользования присущ и существенный недостаток - открытость и доступность информационной среды. Другими словами, компания не может контролировать передачу своих данных по каналам Интернета, а следовательно, гарантировать их целостность и конфиденциальность. Злоумышленникам не составляет особого труда перехватить деловую информацию с целью ознакомления с нею, ее искажения, кражи и т. п.

Однако не стоит полагать, что вопросы безопасности информационного взаимодействия должны рассматриваться только применительно к сетям общего пользования. Современная инфраструктура крупных корпоративных информационных систем (КИС) не исключает возможности перехвата информации, передаваемой по ее внутренним каналам. Например, рядовой сотрудник с помощью специализированного и общедоступного ПО (которое можно свободно скачать из Интернета) может перехватить поток данных, идущий с компьютера генерального директора (что наверняка не понравится последнему). Поэтому в КИС необходимо предусмотреть защиту данных, передаваемых не только по каналам Интернета (защита от внешних злоумышленников), но и по внутренним каналам системы (защита от внутренних злоумышленников).

Постановка задачи

Каким же образом можно обеспечить защиту в КИС и что она собой представляет? Сегодня наиболее распространенный способ защиты передаваемого потока данных - это технология виртуальных частных сетей (Virtual Private Network, VPN). Технологию VPN поддерживают встроенные средства сетевых операционных систем, СУБД, прикладного ПО и т. д., реализующие VPN-протоколы PPP, L2TP, IPSec, SSL/TLS и т. д., на базе которых возможно построение VPN-соединений. Но это еще не выход из положения: применение этих средств, обеспечивающих защиту трафика на различных уровнях модели OSI, не позволяет создать единую, целостную и управляемую подсистему защиты информационных потоков (ПЗИП). Кроме того, в настоящее время практически не существует реализаций упомянутых технологий, поддерживающих российские алгоритмы шифрования и ЭЦП, что затрудняет их использование в госструктурах.

Для создания ПЗИП наиболее привлекательно семейство протоколов IPSec/IKE, поскольку IPSec - это общепризнанный международный стандарт безопасности сетевого уровня, тщательно проработанный и хорошо зарекомендовавший себя. Сетевой уровень - это тот уровень модели OSI, на котором сеть становится полносвязной системой, поэтому построение ПЗИП именно на сетевом уровне можно считать наиболее осознанным и перспективным решением. На более низких уровнях защита трафика реализуется только как набор двухточечных защищенных звеньев. А на сетевом уровне появляется возможность установить защищенное соединение между двумя компьютерами, расположенными в произвольных точках (глобальной) сети. Кроме того, на этом уровне появляется понятие топологии, различаются внешние и внутренние каналы; реализуются такие возможности, как фильтрация трафика, маскировка топологии внутренней сети и т. д. С другой стороны, сетевой уровень не оказывает существенного влияния на работающие в КИС приложения.

При установлении защищенного соединения (VPN-соединения) следует уделить особое внимание вопросам удостоверения подлинности (аутентификации) стороны информационного обмена. Аутентификация осуществляется с целью предотвратить угрозу, когда право на взаимодействие получает не имеющий на то полномочий пользователь или, еще хуже, злоумышленник. После успешного прохождения процедуры аутентификации доступ пользователя по защищенному соединению к ресурсам КИС должен осуществляться в соответствии с правилами, составляющими корпоративную политику безопасности. Наличие политики особенно важно, когда КИС имеет распределенную структуру и включает в себя критичные информационные узлы (рабочие станции, серверы), обрабатывающие важную информацию.

Характеристики подсистемы

В целом ПЗИП предназначена для того, чтобы обеспечить защиту от несанкционированного доступа к информации, передаваемой по открытым каналам Интернета или по внутренним каналам КИС, а также к информационным ресурсам, хранимым на информационных узлах (рабочих станциях, серверах) КИС.

Смысл технологии VPN заключается в сокрытии (криптографическом преобразовании) потока передаваемых данных. Даже если злоумышленник или неуполномоченный пользователь перехватит поток информации, он получит только беспорядочный набор символов, не поддающихся прочтению. Но, кроме сокрытия данных, необходимо обеспечить качественное выполнение еще нескольких задач.

Взаимная аутентификация сторон при установлении соединения. Аутентификация осуществляется на основе многоразовых и одноразовых паролей, цифровых сертификатов, протоколов строгой аутентификации и обеспечивает установление VPN-соединения только между уполномоченными на информационное взаимодействие сторонами.

Авторизация и управление доступом. Авторизация подразумевает предоставление сторонам, уже прошедшим аутентификацию, определенных видов обслуживания, в частности, фильтрации и шифрования их трафика разными способами.

Проверка подлинности (конфиденциальности) и целостности доставленной информации. Конфиденциальность обеспечивается различными алгоритмами симметричного и асимметричного шифрования. Целостность передаваемых данных достигается с помощью технологии электронной цифровой подписи (ЭЦП).

Реализация политики безопасности организации. Это достигается за счет централизованного управления средствами защиты информации (VPN-средствами).

Несмотря на то что КИС различных организаций неодинаковы по своей инфраструктуре и набору выполняемых производственных задач, для ПЗИП в общем случае можно определить следующий состав:

- VPN-агенты: на рабочих станциях пользователей (VPN-клиент), на серверах (VPN-сервер), на шлюзе безопасности (VPN-шлюз);
- средства централизованного управления VPN-агентами;
- аппаратный носитель ключевой информации.

Довольно удобно, если у VPN-агента, кроме основных механизмов безопасности, дополнительно будет функция фильтрации межсетевого потока данных. VPN-агенты, с помощью которых строят защищенные каналы, устанавливаются в точках туннелирования[1] VPN-канала. Обычно средства создания VPN-канала устанавливаются в точке сопряжения КИС с внешними сетями (VPN-шлюз). Но в целях защиты внутренних каналов целесообразно устанавливать такого рода средства на информационных узлах, участвующих в защищенном информационном обмене (рабочие станции пользователей, серверы рабочих групп, серверы общего доступа и т. п.). Кроме того, VPN-агенты должны быть предусмотрены на рабочих местах удаленных мобильных пользователей.

Электронный носитель ключевой информации служит своего рода хранилищем личных данных пользователя: открытый и закрытый ключи, сертификат, пароли, локальная политика безопасности и т. д. Личные данные пользователя используются для проведения процедур аутентификации, фильтрации и сокрытия потока данных.

Теперь определим основные требования, которым должны удовлетворять VPN-средства, используемые при построении ПЗИП. Итак, VPN-агенты должны обеспечивать:

- криптографическое преобразование потока данных в соответствии с промышленным стандартом IPsec;

[1] Точка туннелирования - место в сети, где непосредственно происходит сокрытие передаваемого потока данных.

- возможность добавления (подключения) криптомодулей, реализующих различные алгоритмы сокрытия данных;
- поддержку процедур аутентификации;
- поддержку различных форматов сертификатов открытых ключей;
- отсутствие влияния на работоспособность стандартного прикладного ПО;
- независимость от протоколов канального уровня;
- ведение локального регистрационного журнала;
- запрет на установление защищенного соединения в случае неудачной аутентификации и т. д.

Центр управления VPN-агентами предназначен для целостного и централизованного управления безопасностью информации. В его функции входит управление потоками информации (исключение возможности несанкционированного их перенаправления и изменения правил доступа к ним). Центр должен обеспечивать выполнение единого набора правил безопасности, определять индивидуальные полномочия каждого пользователя при организации доступа к защищаемым ресурсам (управление и создание политики безопасности); на него также возложено оперативное изменение правил обеспечения безопасности и контроль выполнения правил защиты. Кроме того, центр управления отвечает за безопасную транспортировку индивидуальных полномочий к средствам защиты элементов КИС и удаленную настройку средств защиты (загрузка локальных политик безопасности на VPN-агенты).

Структура решения

Рассмотрим, какие виды (конфигурации) информационных потоков существуют в современных КИС и, соответственно, какие сценарии их защиты следует применить. Очевидно, что число таких сценариев не ограничивается единицами. Из всего этого множества можно выделить несколько наиболее часто встречающихся вариантов построения защищенных VPN-соединений (рис. 1), на основе которых возможно построение ПЗИП. К ним, в частности, относятся:

- защищенная связь равноправных сторон информационного обмена;
- защищенное соединение с удаленным мобильным пользователем;
- сквозные (end-to-end) соединения внутри КИС;
- вложенные VPN-соединения.

Связь равноправных сторон информационного обмена представляет собой защищенное соединение между ИС рассматриваемой компании и информационной системой ее партнеров, заказчиков или собственного удаленного подразделения (филиала). Такой вариант предусматривает для каждой из взаимодействующих сторон наличие шлюза безопасности на стыке КИС с сетями общего пользования (Интернетом). Шлюз безопасности (VPN/FW-шлюз) представляет собой VPN-агент, функционирующий на высокопроизводительной аппаратной платформе, и может быть либо программно-аппаратным решением, либо полностью аппаратным. VPN-шлюз должен иметь возможность резервирования защищенного канала с функцией автоматического переключения трафика на резервный канал в случае "падения" основного. Шлюз VPN/FW сочетает в себе функции фильтрации (межсетевое экранирование) и туннелирования сетевого потока данных (установление VPN-соединения). При таком построении ПЗИП тесно интегрируется с подсистемой защиты периметра КИС.

Подключение к КИС (по каналам Интернета) удаленных мобильных пользователей - весьма актуальная сегодня задача, если требуется организовать их доступ к информационным ресурсам организации. На рабочую станцию удаленного мобильного пользователя, находящуюся вне КИС и не имеющую постоянного IP-адреса, устанавливается VPN-агент, который обеспечивает защищенное взаимодействие со шлюзом безопасности КИС.

Остальные варианты предусматривают установку VPN-агентов не только в точке сопряжения с каналами сетей общего пользования, но, при необходимости, и на информационных узлах внутри КИС, участвующих в защищенном информационном обмене (критичные серверы КИС, рабочие станции пользователей). Установка VPN-агентов внутри КИС обусловлена необходимостью защищать взаимодействие между рабочими станциями внутренних пользователей и другими информационными узлами по определенным правилам, зависящим от принадлежности пользователя к тому или иному подразделению, его функциональных обязанностей или функционального назначения сервера. В этом случае внутри КИС

образуются "виртуальные защищенные периметры" между участниками защищенного информационного обмена, доступ в которые невозможен для других пользователей КИС.

Вариант "сквозные соединения" использует механизм "вложенных VPN" и применяется в КИС, где VPN-агенты установлены как на шлюзе, так и на информационном узле. В этом случае поток данных, уже преобразованный на информационном узле, проходит повторное VPN-преобразование на шлюзе.

Рис. 1. Различные виды VPN-соединений.

Выбор продуктов

Теперь поговорим о выборе продуктов для практической реализации подсистемы защиты информационных потоков. Мировой рынок VPN-средств сегодня весьма насыщен, на нем предлагается множество продуктов. На российском рынке довольно хорошо представлены VPN-продукты как отечественных, так и зарубежных производителей. При выборе продуктов, кроме основных требований, предъявляемых к средствам построения VPN-соединений, должны учитываться дополнительные требования. Во-первых, это сертификация продукта: наличие сертификата соответствия требованиям Гостехкомиссии России[2] (для применения на государственных предприятиях) и сертификата ФАПСИ на криптомодуль (в случае обработки в КИС информации ограниченного доступа), а также возможность подключения российских криптомодулей. Следующее требование - "покрытие" продуктами одного производителя всех составляющих ПЗИП (информационные узлы, шлюз безопасности, управление). И наконец, весьма желателен успешный опыт применения продукта на территории РФ.

[2] Применение средств защиты информации (СЗИ) и средств криптографической защиты информации (СКЗИ) ограничено российским законодательством, а именно нормативно-методическими документами Гостехкомиссии России и ФАПСИ.

Очевидно, что на применение зарубежных средств защиты накладываются существенные ограничения, поскольку у них отсутствуют сертификаты Гостехкомиссии России и ФАПСИ. Из отечественных продуктов мы подробнее поговорим о семействе продуктов "Застава 3.3" (**http://www.zastava.ru**). Среди важных характеристик этого семейства - открытый криптоинтерфейс с внешними криптографическими модулями (OpenCryptoAPI), который поддерживает неограниченное количество криптомодулей различных производителей, реализующих разные алгоритмы. Продукты семейства "Застава 3.3" функционально совместимы по IPsec/IKE-протоколам с VPN-модулями ведущих мировых производителей сетевого оборудования, аппаратного и программного обеспечения. Возможно централизованное управление всеми продуктами семейства, а также средствами безопасности Cisco и Check Point с единой графической консоли.

Решение

Посмотрим, как можно использовать средства "Застава 3.3" применительно к структуре подсистемы защиты. По сути это будет одна из практических реализаций ПЗИП.

На стыке КИС с глобальными публичными сетями устанавливается шлюз безопасности, обеспечивающий функции VPN и межсетевую фильтрацию трафика. Для внешних пользователей, взаимодействующих с серверами открытого доступа, расположенными в демилитаризованной зоне (ДМЗ), должен быть обеспечен информационный обмен по открытым (незашифрованным) соединениям. Поэтому шлюз безопасности состоит из двух частей (рис. 2): межсетевой экран (например, Cisco PIX или Check Point FW-1) обрабатывает поступающий из Интернета открытый и защищенный поток данных и направляет его в ДМЗ и на VPN-шлюз соответственно, а VPN-шлюз обрабатывает (аутентифицирует и раскрывает) закрытый IPSec-трафик и передает его далее в локальную сеть.

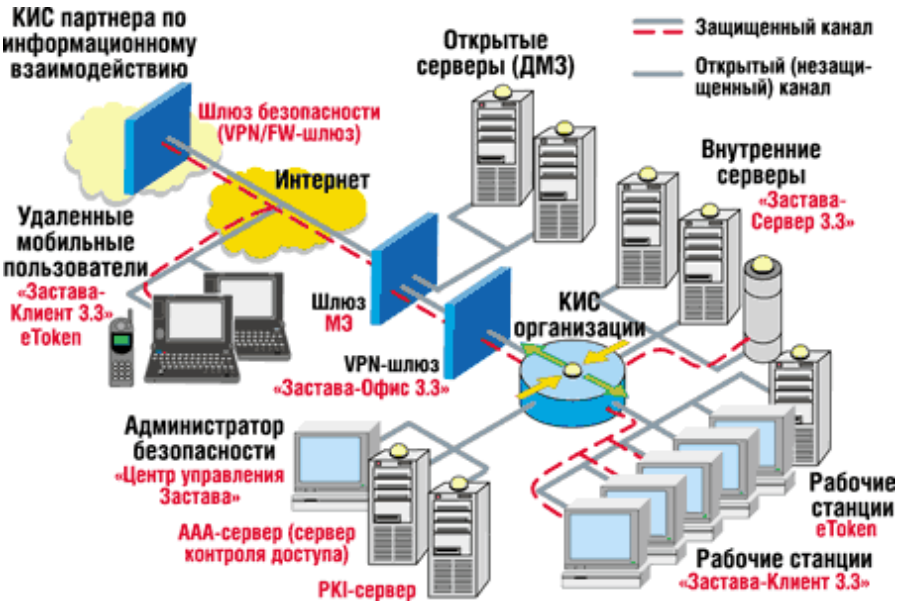

Рис. **2.** Подсистема защиты информационных потоков в КИС.

В качестве VPN-шлюза используется высокопроизводительная аппаратная платформа, на которую устанавливается ПО "Застава-Офис 3.3". Это ПО обеспечивает организацию защищенных соединений с отдельными рабочими станциями, шлюзами и серверами (как внутри КИС, так и по каналам Интернета), защищенных VPN-агентами семейства "Застава". Кроме того, "Застава-Офис" поддерживает функции расширенной пакетной фильтрации (межсетевого экранирования) и обеспечивает коллективную защиту информационных ресурсов КИС от несанкционированного доступа из внешних сетей.

На все рабочие станции пользователей, информационное взаимодействие которых проходит по закрытым каналам внутри КИС, а также на рабочие станции удаленных мобильных пользователей устанавливается ПО "Застава-Клиент 3.3". На серверы, содержащие информацию ограниченного доступа, устанавливается продукт "Застава-Сервер 3.3".

Задачи создания, хранения и распределения ключевой информации пользователей возлагаются на внешнюю службу PKI. В качестве аппаратного носителя ключевой информации пользователя предлагается использовать электронный ключ eToken.

На отдельную рабочую станцию администратора безопасности устанавливается ПО "Центр управления Застава 3.3", которое обеспечивает централизованное, оперативное и целостное управление всеми VPN-агентами, входящими в подсистему, и имеет следующие ключевые функциональные возможности. Глобальная политика безопасности, основанная на абстрактных понятиях, позволяет администратору безопасности создавать общую для всей КИС политику безопасности, базирующуюся на функциональных ролях объектов взаимодействия. Реализация этой политики безопасности и администрирование ПЗИП значительно упрощаются благодаря использованию группировки и иерархии объектов и удобной графической консоли управления. Все настройки и политики безопасности централизованно хранятся в БД Центра управления. Масштабируемость решения теоретически не ограничена; на практике она достигала 1000 управляемых VPN-агентов.

VPN "Застава 3.3" имеет сертификат Гостехкомиссии России № 653 от 30 июля 2002 г., удостоверяющий, что продукт может использоваться как средство организации защищенных виртуальных частных сетей (VPN) на различных каналах связи, в локальных и глобальных сетях общего пользования, включая Интернет.

Важное стратегическое преимущество предлагаемого решения - возможность технической интеграции ПЗИП на базе линейки VPN-продуктов "Застава" в сетевую инфраструктуру КИС, в большинстве случаев построенную на оборудовании компании Cisco Systems (http://www.cisco.ru). Такое решение предусматривает построение различных типовых сценариев взаимодействия VPN-агентов "Застава" и сетевого оборудования Cisco.

В качестве примера рассмотрим один из наиболее распространенных сценариев, при котором мобильный пользователь должен установить защищенное end-to-end соединение с сервером приложений в КИС, где в качестве шлюза безопасности используется Cisco IOS/PIX (либо маршрутизатор с ОС Cisco IOS, либо межсетевой экран Cisco PIX Firewall). Процесс аутентификации пользователя происходит следующим образом (рис. 3). Центр управления "Застава" транслирует заданную глобальную политику безопасности в локальную и доставляет ее на Cisco IOS/PIX и "Застава-Клиент" мобильного пользователя. В течение первой фазы аутентификации (по протоколу IKE) Cisco IOS/PIX распознает "своего" пользователя и предлагает ему пройти процедуру аутентификации. "Застава-Клиент" передает аутентификационные данные пользователя, хранимые на электронном носителе, по протоколу XAUTH на Cisco IOS/PIX, который пересылает эти данные пользователя на внешний AAA-сервер (например, Radius или ACE/Server). На AAA-сервере происходит аутентификация пользователя, после чего сервер посылает результат аутентификации (ACL-список и IP-адрес, назначенный пользователю) на Cisco IOS/PIX, который, в свою очередь, принимает решение о

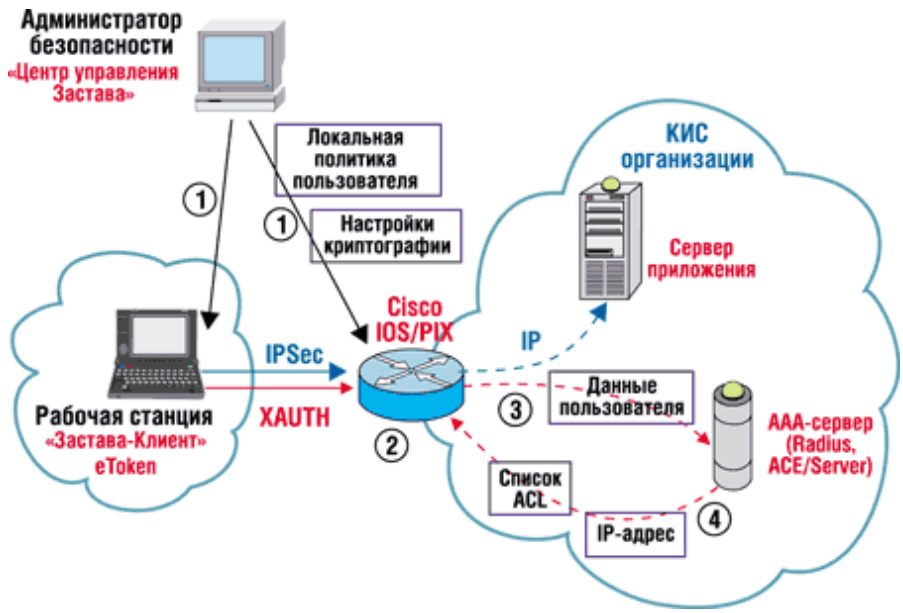

Рис. **3.** Процесс аутентификации мобильного пользователя.

передаче IPSec-потока от данного пользователя в КИС.

***

В последнее время простая установка VPN-средств, назначение которых - обеспечить безопасность взаимодействия между сторонами информационного обмена, становится все менее осмысленной. В современных условиях необходимо качественно повысить эффективность и надежность защиты

информационных потоков. В то же время остро встает вопрос о взаимодействии VPN-средств с другими средствами, решающими иные задачи безопасности. Для этого в КИС должна быть предусмотрена целая подсистема защиты, объединяющая все VPN-средства, распределенные на всех уровнях КИС, и предоставляющая возможность централизованного управления ими и интеграции с другими средствами защиты.

С другими статьями, посвященным вопросам информационной безопасности, Вы можете ознакомиться на сайте «ЭЛВИС-ПЛЮС»: http://www.elvis.ru/informatorium.shtml