Virtual Private Network

Виртуальная частная сеть: процедуры защиты данных

Виртуальная частная сеть (VPN) — весьма сложная система, включающая в себя множество компонентов. Это компьютеры нескольких типов, начиная с настольных и кончая мейнфреймами, системное и прикладное программное обеспечение, сетевые адаптеры, концентраторы, коммутаторы и маршрутизаторы, а также кабельная система.

Основная задача системных интеграторов и администраторов состоит в том, чтобы эта громоздкая и весьма дорогостоящая система как можно лучше справлялась с обработкой потоков информации, циркулирующих между сотрудниками предприятия, и позволяла им принимать рациональные решения, обеспечивающие выживание предприятия в жесткой конкурентной борьбе. А так как жизнь не стоит на месте, то и содержание корпоративной информации, интенсивность ее потоков и способы обработки постоянно меняются. Резкое изменение технологии автоматизированной обработки корпоративной информации связано с беспрецедентным ростом популярности Интернета.

Истоки проблемы

Гипертекстовая служба WWW изменила способ представления информации, собрав на своих страницах все популярные ее виды — текст, графику и звук. Транспорт Интернета — недорогой и доступный практически всем предприятиям (а через телефонные сети и одиночным пользователям) — существенно облегчил задачу построения территориальной корпоративной сети. Одновременно на первый план выдвинулась проблема защиты корпоративных данных при их передаче через абсолютно общедоступную Всемирную сеть. Стек TCP/IP сразу же вышел на первое место, потеснив прежних лидеров локальных сетей IPX и NetBIOS, а в территориальных сетях — X.25 и frame relay.

Так как Интернет постепенно становится общемировой сетью интерактивного взаимодействия людей, он начинает все больше использоваться не только для распространения информации, в том числе и рекламной, но и для осуществления деловых операций — покупки товаров и услуг, перемещения капитала и т. п. Меняется сама структура ведения бизнеса. Миллионы потенциальных покупателей снабжаются рекламными объявлениями, тысячам интересующихся продукцией клиентов нужно предоставлять дополнительную информацию и вступать с ними в активный диалог через Интернет, и, наконец, сотни покупателей совершают электронные сделки. Сюда нужно добавить и обмен информацией с предприятиями-соисполнителями или партнерами по бизнесу.

Изменения схемы ведения бизнеса меняют и требования, предъявляемые к корпоративной сети. Например, использование технологии Intranet сломало привычные пропорции внутреннего и внешнего трафика предприятия в целом и его подразделений — старое правило, гласящее, что 80% трафика является внутренним и только 20% идет вовне, сейчас не отражает истинного положения дел. Интенсивное обращение к web-сайтам внешних организаций и других подразделений предприятия резко повысило долю внешнего трафика и, соответственно, увеличило нагрузку на пограничные маршрутизаторы и брандмауэры корпоративной сети.

Другим примером влияния Интернета на бизнес-процессы может служить необходимость аутентификации и авторизации огромного числа клиентов, обращающихся за информацией на серверы предприятия извне, если предприятие использует Интернет для рекламы или продажи своих товаров и услуг. Старые способы, основанные на ведении учетной информации на каждого пользователя в базе данных сети и выдаче ему индивидуального пароля, здесь уже не годятся — ни администраторы, ни серверы аутентификации сети с таким объемом работ не справятся. Поэтому появляются новые методы проверки легальности пользователей, основанные на сертификатах.

Возможные ошибки

Влияние Интернета на корпоративную сеть — это только один, хотя и яркий, пример постоянных изменений, которые претерпевает технология автоматизированной обработки информации на современном предприятии, желающем не отстать от конкурентов. Постоянно появляются технические, технологические и организационные новинки, которые необходимо использовать в корпоративной сети для поддержания ее в состоянии, соответствующем требованиям времени. Без внесения изменений корпоративная сеть быстро морально устареет и не сможет работать так, чтобы предприятие смогло успешно конкурировать на мировом рынке.

Чтобы предприятию не нужно было бы полностью перестраивать свою корпоративную сеть каждые 3–5 лет, что связано с огромными расходами, нужно постоянно следить за основными тенденциями развития мира сетевых и информационных технологий и постоянно вносить в сеть (в программы, сервисы, аппаратуру) такие изменения, которые позволили бы сети плавно отраба- »

Термины

Глоссарий

TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/протокол Internet) известен также как стек протоколов Internet (Internet Protocol Suite). Этот стек протоколов используется в семействе сетей Internet и для объединения гетерогенных сетей.

IPX — протокол Novell, обеспечивающий дейтаграммную доставку сообщений, обмен информацией между конечными станциями, поддержку достаточно большого числа приложений, а также функции адресации сетевого уровня и маршрутизации между клиентами и серверами NetWare.

X.25 — стандарт для коммуникационных протоколов доступа к сетям с коммутацией пакетов.

Frame relay – высокоскоростная технология, основанная на коммутации пакетов для передачи данных между интеллектуальными оконечными устройствами типа маршрутизаторов, работающих со скоростью от 56 Кбит/с до 1,544 Мбит/с. Данные делятся на кадры переменной длины передающим устройством, а каждый кадр содержит заголовок с адресом получателя. Кадры передаются цифровым устройством и собираются на приемном конце. Эта технология обеспечивает меньшее количество ошибок и большую (примерно втрое) скорость доставки по сравнению с X.25, на основе которой она была разработана. Большим преимуществом сетей frame relay общего пользования является звездная топология на логическом уровне.

Ethernet/Fast Ethernet/Gigabit Ethernet — спецификации для передачи по неэкранированным медным или оптическим кабелям со скоростью до 100 Мбит/с.

Термины

Глоссарий

Token Ring — спецификации локальной сети. Кадр управления (supervisory frame), называемый также маркером (token), последовательно передается от одной станции к соседней. При этом станция, которая хочет получить доступ к среде передачи, должна ждать получения кадра и только после этого может начать передачу данных.

High Speed Token Ring от предыдущего, как очевидно по названию, отличается лишь более высокой скоростью.

PPP (Point-to-Point Protocol) является наследником протокола Serial Line IP, обеспечивает соединения типа маршрутизатор-маршрутизатор и хост-сеть как для синхронных, так и для асинхронных устройств. В частности применяется для аутентификации по протоколу PAP (Password Authentication Protocol).

DECnet — торговая марка для сетевой архитектуры компании DEC, позволяющей связывать компьютеры DEC по протоколу DDCMP или NetBEUI (транспортный протокол, используемый Microsoft LAN Manager, Windows for Workgroups, Windows NT и других сетевых ОС).

OSI (Open Systems Interconnection — взаимодействие открытых систем) — семиуровневая модель протоколов передачи данных для обеспечения взаимодействия открытых систем, на которых работают протоколы данного стандарта. Существуют следующие уровни модели OSI (снизу-вверх): физический (physical), канальный (data link), сетевой (network), транспортный (transport), сеансовый (session), представления данных (presentation) и прикладной (application).

DDCMP — Digital Data Communications Message Protocol, протокол цифровой передачи сообщений.

» тывать каждый резкий поворот. Важно правильно видеть стратегическое направление развития корпоративной сети и постоянно приводить его в соответствие с направлением развития всего сетевого мира. Тогда меньше шансов завести корпоративную сеть в такой тупик, откуда нет иного выхода, кроме полной ее перестройки. По крайней мере, нельзя вкладывать большие деньги и силы в решения, в будущем которых имеются большие сомнения. Например, весьма рискованно строить сегодня новую сеть исключительно на технологии Token Ring, так как перспективы Token Ring по сравнению с перспективами семейства технологий Ethernet/Fast Ethernet/Gigabit Ethernet всеми признаются очень сомнительными, несмотря на усилия компании IBM по развитию следующего члена семейства — High Speed Token Ring. Естественно, добавление нескольких сегментов Token Ring к уже существующим не изменит общей картины корпоративной сети, но выбор этой технологии нельзя назвать стратегически верным. Fast Ethernet и Gigabit Ethernet дают гораздо больше гарантий относительно своей жизнеспособности.

Другим сомнительным решением явилось бы построение крупной локальной сети центрального подразделения предприятия целиком на коммутаторах второго уровня. Плоская топология такой сети, пропускающая между сегментами любой трафик, в том числе и ошибочный, обязательно принесет много хлопот администраторам, а специализированные процессоры «истинных» коммутаторов второго уровня не позволят провести относительно безболезненной модернизации сети только за счет загрузки в коммутаторы нового программного обеспечения. В результате придется использовать гибкие коммутаторы третьего уровня, позволяющие разделять сеть на подсети и фильтровать трафик между ними. Это повышает как устойчивость сети к сбоям и отказам, так и защищенность подсетей от несанкционированного доступа.

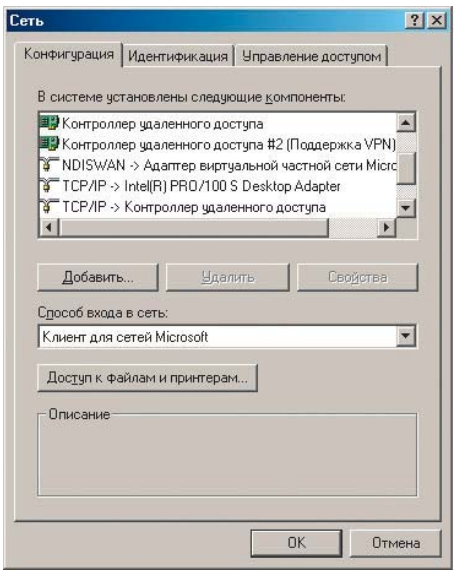
Очень важно и правильное использование стека TCP/IP в корпоративной сети. В большинстве случаев протоколы стека IPX/SPX вполне справляются со всеми задачами по переносу трафика внутри локальных сетей, а шлюзы и proxy-серверы позволяют эффективно связывать эти сети с внешним IP-миром. Однако большинство разработчиков сетевых устройств, операционных систем и сетевых приложений сосредоточили сегодня свои усилия на поддержке и использовании протокола IP в своих продуктах. Поэтому приверженцам стека IPX/SPX придется постоянно отказываться от новых возможностей и функций IP-ориентированных продуктов, ограничивая свой выбор все более сужающимся рынком IPX-продуктов. Существует большая вероятность, что в один прекрасный день такую корпоративную сеть вместо плавного внедрения в нее последних достижений сетевой индустрии придется перестраивать с нуля.

Стратегическое планирование сети состоит в нахождении компромисса между потребностями предприятия в автоматизированной обработке информации, его финансовыми возможностями и возможностями сетевых и информационных технологий сегодня и в ближайшем будущем. Но самой сутью построения виртуальной частной сети является надежная защита корпоративных данных.

Подключение локальной сети к любой публичной сети чревато некоторыми неприятными последствиями. Становятся доступными как внутренние ресурсы этой локальной сети, так и ее данные, передаваемые через публичную сеть.

Способы защиты

В идеале уровень безопасности виртуальной частной сети должен приближаться к истинной частной сети, в которой нет места этим проблемам. Что нужно для того, чтобы »



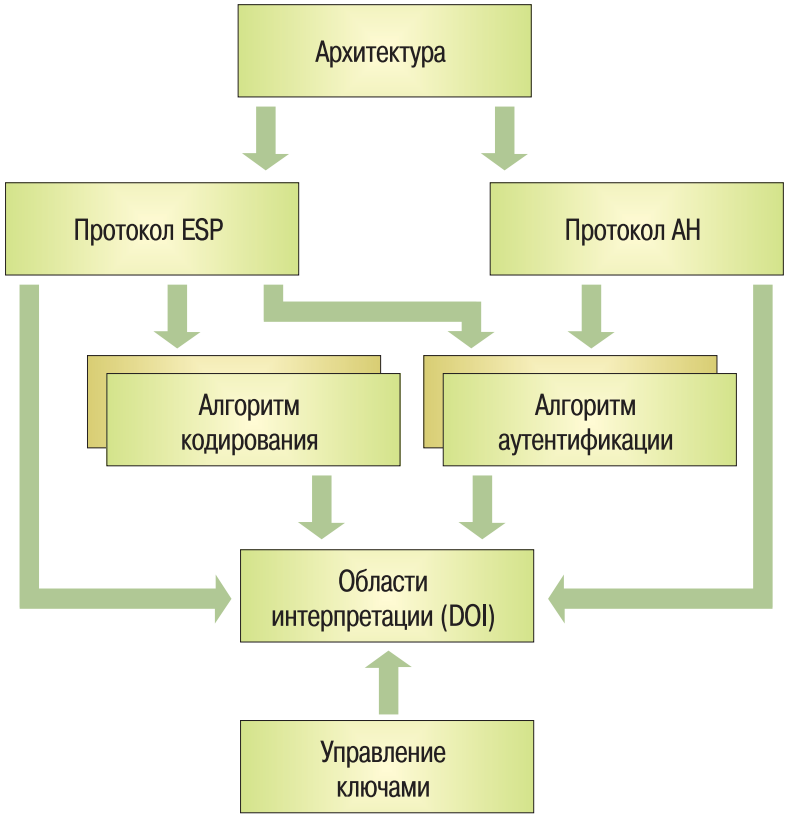
▲ За этим окном, знакомым многим, скрываются важные вопросы безопасности

» свести на нет угрозы несанкционированного доступа к внутренним ресурсам и передаваемым данным? Необходимы определенные средства для отражения этих угроз. Круг этих средств довольно широк. Устройств безопасности на сегодняшний день вполне хватает: многофункциональные брандмауэры, маршрутизаторы со встроенными возможностями фильтрации пакетов, proxy-серверы, аппаратные и программные шифраторы передаваемого трафика.

Но существует и другая, широко распространенная точка зрения, когда под средствами защиты данных локальной сети понимают только защиту передаваемого трафика. Оно и понятно, ведь Интернет долго использовался только для передачи открытого трафика, который не нуждался в защите. Информация ftp-архивов и web-серверов, понятное дело, была общедоступной. Если какая-либо фирма или корпорация нуждалась в защите своих данных, она передавала свой конфиденциальный трафик по выделенным каналам. Поэтому корпоративная сеть защищалась прежде всего от несанкционированного доступа. И только когда Интернет превратился в универсальное транспортное средство для всех видов корпоративного трафика, в том числе и секретного, возникла проблема защиты данных при передаче через публичную сеть.

Функции защиты трафика иногда встраиваются в продукты, традиционно предназначенные для защиты от несанкционированного доступа, такие, как брандмауэры или маршрутизаторы.

Чтобы создать защищенный канал, в виртуальных частных сетях принято применять определенные процедуры. Остановимся подробнее на некоторых из них.



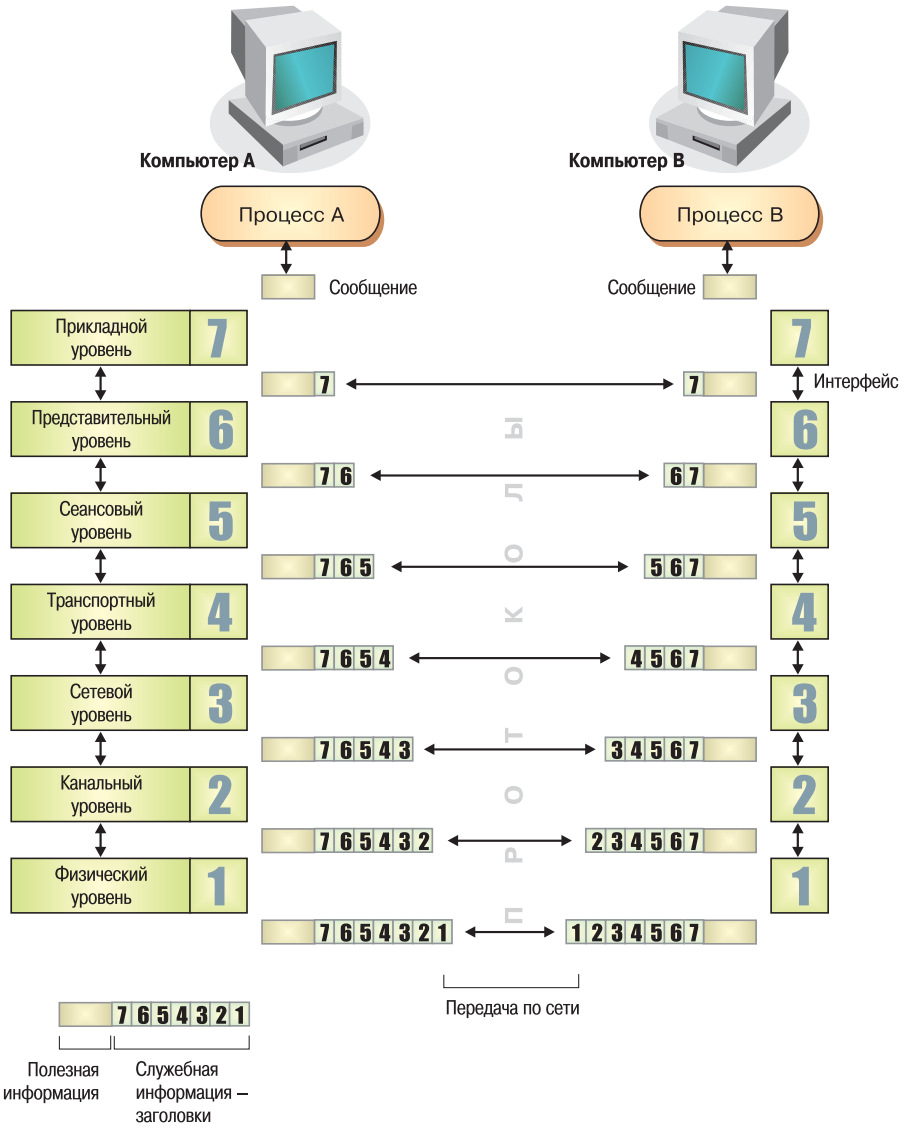
▲ Архитектура построения механизмов защиты информации

Авторизация

Наиболее традиционный способ — авторизация (предоставление легальным абонентам разных способов шифрования их трафика). Относится к таким средствам и аутентификация. Она разрешает устанавливать соединения частной виртуальной сети только между легальными пользователями и предотвращает доступ нежелательных лиц к средствам частной сети. В переводе с латыни «аутентификация» означает «установление подлинности». Аутентификацию следует отличать от идентификации. Идентификаторы пользователей применяются с теми же целями, что и идентификаторы любых других объектов, файлов, процессов, структур данных, но они не связаны непосредственно с обеспечением безопасности. Идентификация заключается в сообщении пользователем системе своего идентификатора. При процедуре аутентификации пользователь доказывает, что он именно тот, за кого себя выдает. В процессе участвуют две стороны: одна доказывает свою аутентичность, а другая (аутентификатор) проверяет эти доказательства и принимает решение. При достаточной простоте и ясности метод аутентификации на основе паролей имеет и свои уязвимые места, такие, как раскрытие и разгадывание паролей и определение пароля путем анализа сетевого трафика. Чтобы предупредить раскрытие паролей, администраторы сети, как правило, используют встроенные программные средства для формирования политики их назначения и использования.

Происходит это следующим образом. Паролю задаются максимальный и минимальный срок действия; сохраняется список уже использованных паролей, наблюдается поведение системы после нескольких неудачных попыток логического входа и т. п. Кроме того, перехват паролей по сети можно предупредить, если зашифровать их как следует перед передачей в сеть.

Некоторыми системными администраторами используются методы и алгоритмы симметричного и асимметричного шифрования. Вообще-то, именно на шифровании держится основа всех служб информационной безопасности, в том числе системы аутентификации и авторизации. Шифрование — это составная часть криптосистемы, состоящей из шифрования и дешифрации (приведения зашифрованных данных в читабельный вид). В современных алгоритмах шифрования предусматривается наличие параметра — секретного ключа. В криптографии принято правило Керкхоффа: стойкость шифра должна определяться только секретностью ключа. Несмотря на то, что детальное описание стандартных алгоритмов шифрования, таких, например, как DES и PGP, содержится в легкодоступных документах, на их эффективности это не отражается. Тот, кто хочет проникнуть в ваши конфиденциальные данные, может знать все об алгоритмах шифрования, кроме секретного ключа. А процедура подбора ключа обычно дело муторное, долгое и неблаго- »



▲ Так можно представить модель OSI (Open Systems Interconnection)

» дарное, иначе говоря, она достаточно сложна как по времени исполнения, так и по самой своей сути. Если крипты системы защиты данных достаточно стойкие, подобрать ключ практически невозможно, даже если взломщик не ограничен во времени.

К другим способам защиты данных относится определение абонентами друг друга с помощью цифровых сертификатов, смарт-карт, многоразовых и одноразовых паролей. Существуют и различные варианты технологии электронной подписи, основанные на симметричных и асимметричных методах шифрования и односторонних функциях.

Аутентификация

Легальность пользователя устанавливается по отношению к различным системам. Так, работая в сети, пользователь может проходить процедуру аутентификации и как локальный пользователь, претендующий на использование ресурсов только данного компьютера, и как пользователь сети, желающий получить доступ ко всем сетевым ресурсам. При локальной аутентификации пользователь вводит свой идентификатор и пароль, которые автономно обрабатываются операционной системой, установленной на данном компьютере. При логическом входе в сеть идентификатор и пароль передаются на сервер, где хранятся учетные записи обо всех пользователях сети. Многие приложения имеют свои средства определения, является ли пользователь законным. В этом случае приходится проходить дополнительные этапы проверки.

В качестве объектов, требующих аутентификации, могут выступать не только пользователи, но и различные устройства, приложения, текстовая и другая информация. Так, например, пользователь, обращающийся с запросом к корпоративному серверу и доказывающий ему свою легальность, должен также сам убедиться, что ведет диалог действительно с сервером своего предприятия. Другими словами, сервер и клиент проходят процедуру взаимной аутентификации. Здесь мы имеем дело с аутентификацией на уровне приложений. При установке сеанса связи между двумя устройствами также часто предусматриваются процедуры взаимной аутентификации на более низком, канальном уровне. Примером такой процедуры является аутентификация по протоколу PAP (Password Authentication Protocol — протокол аутентификации пароля), входящему в семейство протоколов PPP (протоколы связи между терминалом и маршрутизатором).

Аутентификация данных является доказательством целостности этих данных, а также того, что они поступили именно от человека, который объявил об этом. В этом случае используется механизм электронной подписи.

В вычислительных сетях процедуры аутентификации часто реализуются теми же программными средствами, что и процедуры авторизации. В отличие от аутентификации, распознающей легальных и нелегальных пользователей, система авторизации имеет дело только с легальными пользователями, которые уже успешно прошли процедуру аутентификации. Цель подсистем авторизации состоит в том, чтобы предоставить каждому легальному пользователю именно те виды доступа к ресурсам, которые были для него определены администратором системы.

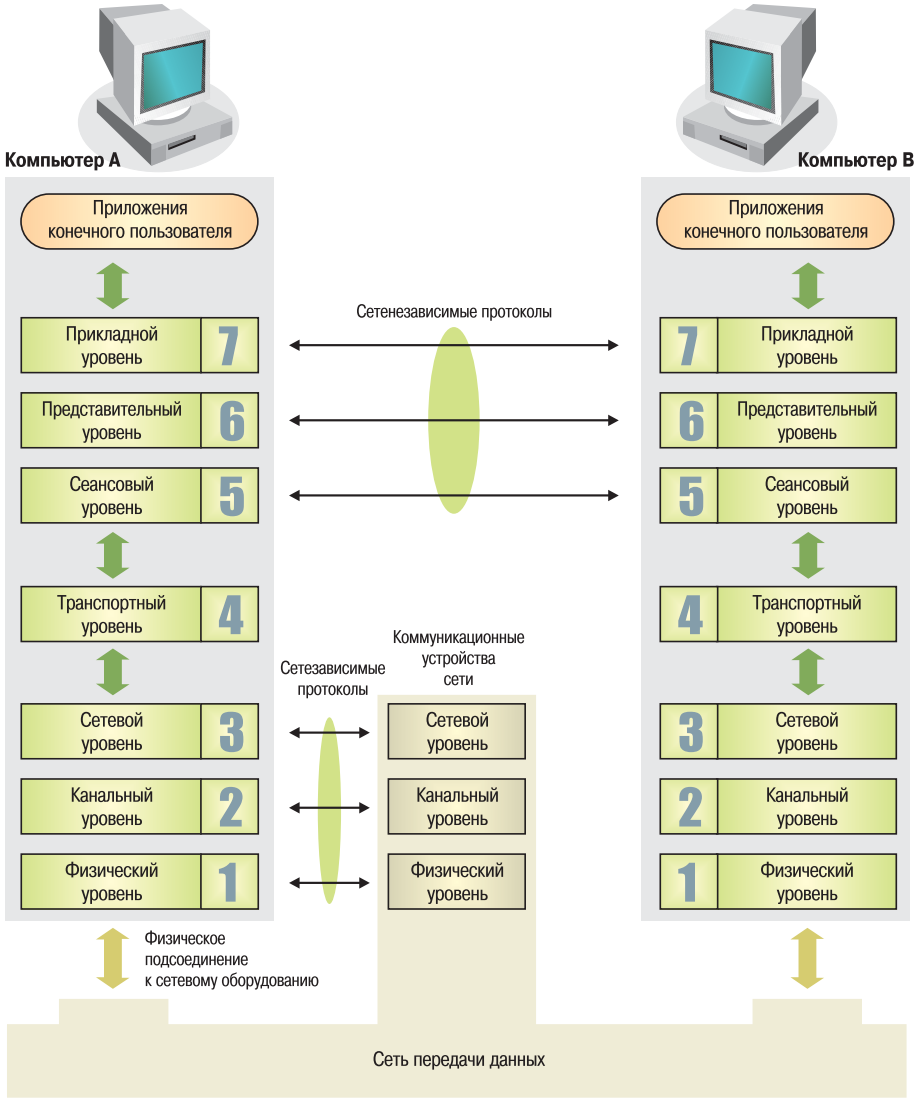
Средства авторизации контролируют доступ легальных пользователей к ресурсам системы, предоставляя каждому из них именно те права, которые были определены администратором. Кроме предоставления прав доступа пользователей к каталогам, файлам и принтерам, система авторизации может контролировать возможность выполнения пользователями различных системных функций, таких, как локальный доступ к серверу, установка системного времени, создание резервных копий данных, выключение сервера и т. п. Применительно к виртуальным частным сетям система авторизации может регулировать доступ пользователя к тем или иным средствам шифрования пакетов или даже в целом к определенным устройствам виртуальной частной сети. »

» Программные системы построены таким образом, что сервер управляет процессом предоставления ресурсов пользователю, реализуя принцип единого входа. Пользователь один раз логически входит в сеть и получает на все время работы некоторый набор разрешений по доступу к ресурсам сети. Kerberos, с ее сервером безопасности и архитектурой «клиент-сервер», является наиболее известной системой этого типа. Системы TACACS и RADIUS, часто применяемые совместно с системами удаленного доступа, также реализуют этот подход.

В другом случае рабочая станция сама является защищенной — средства защиты работают на каждой машине, и вмешательство сервера не требуется. Рассмотрим работу системы, в которой не предусмотрена процедура однократного логического входа. Теоретически доступ к каждому приложению должен контролироваться средствами безопасности самого приложения или же средствами, существующими в той операционной среде, в которой оно работает. В корпоративной сети администратору придется отслеживать работу механизмов безопасности, используемых всеми типами приложений — электронной почтой, службой каталогов локальной сети, базами данных хостов и т. п. Когда администратору приходится добавлять или удалять пользователей, часто требуется вручную конфигурировать доступ к каждой программе или системе.

В крупных сетях часто применяется комбинированный подход предоставления пользователю прав доступа к ресурсам сети. Сервер удаленного доступа ограничивает доступ пользователя к подсетям или серверам корпоративной сети, то есть к укрупненным элементам сети. А каждый отдельный сервер сети сам по себе ограничивает доступ пользователя к своим внутренним ресурсам — разделяемым каталогам, принтерам или приложениям. Сервер удаленного доступа предоставляет доступ на основании имеющегося у него списка прав доступа пользователя. Ресурсы каждого отдельного сервера сети становятся доступны на основании хранящегося у него списка прав доступа — например, ACL (Access Control List — список управления доступом) файловой системы.

Системы аутентификации и авторизации совместно выполняют одну задачу, поэтому к ним необходимо предъявлять одинаковый уровень требований. Ненадежность одного звена здесь не может быть компенсирована высокой надежностью другого. Если при аутентификации используются пароли, то требуются чрезвычайные меры по их защите. Однажды украденный пароль открывает двери ко всем приложениям и данным, к которым пользователь с этим паролем имел легальный доступ.



▲ Защита информации на различных уровнях OSI

Помимо защиты

Поскольку никакая система безопасности не гарантирует абсолютную защиту, то последним рубежом в борьбе с нарушениями оказывается система аудита. Аудит — фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам. Действительно, после того, как злоумышленнику удалось провести успешную атаку, пострадавшей стороне не остается ничего другого, как обратиться к службе аудита. Если при настройке службы аудита были правильно заданы события, которые требуется отслеживать, то подробный анализ записей в журнале может дать много полезной информации. Эта информация, возможно, позволит найти злоумышленника или, по крайней мере, предотвратить повторение подобных атак путем устранения уязвимых мест в системе защиты.

Протоколы защищенного канала часто используют в своей работе такой механизм, как туннелирование (инкапсуляция). При туннелировании пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня. Например, при туннелировании и кадр Ethernet, и пакет IPX могут быть размещены в пакете IP. Возможен и такой вариант: пакет IP размещается в пакете IPX. »

Аппаратная реализация

Физическая организация VPN

Каким же образом физически организовать безопасность виртуальной частной сети, какие устройства, типы платформы, протоколы шифрования и аутентификации при этом применяются? Ведь виртуальные частные сети представляют собой весьма разнообразную и пеструю картину. Существуют комбинированные пограничные устройства, которые включают в себя функции маршрутизатора, брандмауэра, средства управления пропускной способностью и функции виртуальной частной сети.

Шлюз виртуальной частной сети — это сетевое устройство, подключенное к нескольким сетям, которое выполняет функции шифрования и аутентификации для многочисленных хостов позади него. Размещение шлюза должно быть аналогично размещению брандмауэра, то есть таким, чтобы через него проходил весь трафик, предназначенный для внутренней корпоративной сети. Если в сети имеется и брандмауэр, и шлюз, то их относительное расположение представляет собой задачу, требующую особого рассмотрения. Сетевое соединение частной сети прозрачно для пользователей позади шлюза, оно представляется им выделенной линией, хотя в действительности прокладывается через сеть с коммутацией пакетов.

В зависимости от стратегии безопасности предприятия исходящие пакеты либо шифруются, либо посылаются в открытом виде, либо блокируются шлюзом. Для входящих туннелируемых пакетов внешний адрес является адресом шлюза, а внутренний адрес — адресом некоторого хоста позади шлюза.

Шлюз может быть реализован всеми перечисленными выше способами, то есть в виде отдельного аппаратного устройства, отдельного программного решения, а также в виде брандмауэра или маршрутизатора, дополненного функциями виртуальной частной сети.

Клиент виртуальной частной сети — это программный или программно-аппаратный комплекс, обычно на базе персонального компьютера. Его сетевое транспортное обеспечение модифицировано для выполнения шифрования и аутентификации трафика, которым устройство обменивается с шлюзами VPN и/или другими VPN-клиентами. Ввиду стоимостных ограничений реализация VPN-клиента чаще всего представляет собой программное решение, дополняющее стандартную операционную систему, например Windows 98/2000 или Unix.

Для создания виртуальной частной сети крупного предприятия нужны как шлюзы, так и клиенты. Шлюзы целесообразно использовать для защиты локальных сетей предприятия, а VPN-клиенты — для удаленных и мобильных пользователей, которым требуется устанавливать соединения с корпоративной сетью через Интернет. В том случае, когда организацию VPN берет на себя провайдер, вся виртуальная частная сеть может быть построена на его шлюзах, прозрачно для сетей и удаленных пользователей предприятия.

Важной характеристикой стандартов защищенного канала является уровень модели OSI. Защищенный канал можно построить на основе системных средств, реализованных на разных уровнях стека коммуникационных протоколов. Конечно, возможен и такой вариант, когда приложение самостоятельно, без обращения к системным средствам, обеспечивает конфиденциальность и целостность передаваемых им данных. Но поскольку в этом случае от прикладного программиста потребуются дополнительные усилия, такой вариант встречается довольно редко.

» Туннелирование

Туннелирование широко используется для безопасной передачи данных через публичные сети путем упаковки пакетов во внешнюю оболочку. Туннель создается двумя пограничными устройствами, которые размещаются в точках входа в публичную сеть.

Особенностью туннелирования является то, что эта технология позволяет зашифровать исходный пакет целиком, вместе с заголовком, а не только его поле данных. И это очень важно, так как многие поля заголовка содержат информацию, которая может быть использована злоумышленником. Из заголовка он может почерпнуть, например, сведения о внутренней структуре сети: данные о количестве подсетей и узлов и их IP-адресах. Такая информация используется для организации различных атак на корпоративную сеть или при анализе интенсивности исходящего и входящего трафика для получения данных о деловой активности предприятия, например о его бизнес-партнерах.

С другой стороны, если заголовок зашифровать, то он не может быть использован по своему прямому назначению — для обеспечения транспортировки пакета по сети. Именно в такой ситуации для защиты пакета прибегают к туннелированию. Исходный пакет зашифровывают полностью, вместе с заголовком, и этот зашифрованный пакет помещают в другой, внешний пакет с открытым заголовком. Для транспортировки данных по «опасной» сети используются открытые поля заголовка внешнего пакета, а при прибытии внешнего пакета в конечную точку защищенного канала из него извлекают внутренний пакет, расшифровывают и используют его заголовок для дальнейшей передачи уже в открытом виде по сети, не требующей защиты.

Туннелирование используется не только для обеспечения конфиденциальности содержимого пакета, но и для обеспечения его целостности и аутентичности. И в этом случае защита данных осуществляется более полно, чем без туннелирования, так как электронная подпись распространяется на все поля пакета, а без туннелирования — только на те, которые в процессе передачи сети не изменяются (примером поля, которое нельзя подписать без туннелирования, может служить поле TTL пакета IP, которое уменьшается »

» на 1 каждым промежуточным маршрутизатором).

Обычно туннель создается только на участке публичной сети, где существует угроза нарушения конфиденциальности и целостности данных, например, между точкой входа в публичный Интернет и точкой входа в корпоративную сеть. При этом для внешних пакетов используются адреса пограничных маршрутизаторов, установленных в этих двух точках, а внутренние адреса конечных узлов содержатся во внутренних пакетах в защищенном виде.

Туннелирование часто применяется также для согласования разных транспортных технологий. Например, если данные протокола IPX нужно передать через транзитную сеть IP, то маршрутизатор на границе IPX- и IP-сетей упаковывает исходный IPX-пакет в создаваемый заново пакет IP и адресует его маршрутизатору, соединяющему транзитную IP-сеть с сетью IPX. Этот маршрутизатор извлекает пакет IPX из прибывшего IP-пакета и отправляет его далее по IPX-сети.

Само по себе туннелирование не защищает данные от несанкционированного доступа или искажения, а только создает предпосылки для защиты всех полей исходного пакета, включая и поля заголовка. Для того, чтобы обеспечить секретность передаваемых данных, исходные пакеты-пассажиры шифруются и/или снабжаются электронной подписью, а затем передаются по транзитной сети с помощью пакетов несущего протокола.

Выбор протокола

Что же касается системных средств поддержки защищенных каналов, то они встраиваются в разные уровни, начиная с прикладного. На прикладном уровне встречается много версий известных протоколов, которые отличаются от своих стандартных реализаций наличием тех или иных средств защиты передаваемых данных (например, протоколы S/MIME — Multipurpose Internet Mail Extensions, многоцелевые расширения почты Интернет), или PGP, защищающие данные электронной почты). Недостатком такого подхода является узкая область действия — протокол защищает только вполне определенную сетевую службу: файловую, гипертекстовую или почтовую. Поэтому для каждой службы необходимо разрабатывать соответствующую защищенную версию протокола и выполнять эту работу при разработке новой службы. Другой недостаток — необходимость переписывания приложений для соответствующих сетевых служб: в приложения должны быть встроены явные вызовы функций защищенных версий протокола.

Наиболее известным протоколом защищенного канала, работающим на следующем, представительном уровне, является протокол Secure Socket Layer (SSL) и его новая реализация — Transport Layer Security (TLS). Снижение уровня протокола сделало его гораздо более универсальным средством защиты. Теперь единым протоколом защиты могут воспользоваться любые приложения и любые протоколы прикладного уровня. Правда, при этом по-прежнему необходимо их переписывать, чтобы встроить вызовы функций протокола SSL.

> Наиболее известным протоколом **защищенного канала** является **Secure Socket Layer**

Чем ниже по стеку расположены средства защищенного канала, тем проще их сделать прозрачными для приложений и прикладных протоколов. Наиболее известным стандартным средством защиты сетевого уровня является протокол IPSec. Однако в этом случае приложения ограничены использованием вполне определенного протокола сетевого уровня, например протокол IPSec применим только в IP-сетях.

Протокол защищенного канала может работать также и на канальном уровне модели OSI. К таким протоколам относится, например, протокол PPTP. Как и в случае защищенного канала сетевого уровня, здесь также обеспечивается прозрачность средств защиты для приложений и служб прикладного уровня. Достоинством такого подхода является независимость средств защиты от применяемого протокола транспортировки пакетов сетевого уровня. В частности, протокол PPTP может переносить пакеты как в IP-сетях, так и в сетях, работающих на основе протоколов IPX, DECnet или NetBEUI.

Протоколы PPTP, L2F и L2TP объединяет то, что они представляют собой протоколы туннелирования канального уровня, которые инкапсулируют кадры канального протокола в протокол сетевого уровня. С помощью последнего данные затем передаются по составной сети. Кроме того, эти протоколы близки также и тем, что их главная область применения — решение задачи защищенного многопротокольного удаленного доступа к ресурсам корпоративной сети через публичную сеть, в первую очередь через Интернет. Так как практически любое клиентское программное обеспечение использует сегодня для удаленного доступа стандартный протокол канального уровня PPP, то и протоколы PPTP, L2F и L2TP основаны на инкапсуляции кадров PPP в пакеты сетевого уровня. В таком качестве используется прежде всего IP, но возможно применение и других сетевых протоколов, таких как IPX или DECnet. Хотя все три протокола часто относят к протоколам образования защищенного канала, строго говоря, этому определению соответствует только PPTP, обеспечивающий как туннелирование, так и шифрование данных. Протоколы L2F и L2TP являются только протоколами туннелирования, а функции защиты данных (шифрование, аутентификация, целостность) в них не поддерживаются. Предполагается, что при их применении защита туннелируемых данных будет выполняться с помощью некоторого третьего протокола, например, IPsec.

Таким образом, существует масса сетевых продуктов, предназначенных для обеспечения безопасности виртуальной частной сети. При грамотном их использовании, при подборе соответствующих устройств администратору вполне под силу решить две главные задачи VPN. Одна из них — защита данных от несанкционированного доступа злоумышленников, вторая — обеспечение скорости и качества передаваемых данных. Знакомство с современными сетевыми протоколами и коммутирующими устройствами — первый шаг при построении VPN.

■ ■ ■ Ольга Афанасьева

Ссылки по теме

- http://www.signal-com.ru
- http://www.cisco.com
- http://www.uniinc.msk.ru/uni/solutions/cp
- http://www.firewall.ru
- http://www.croc.ru/solutions/solutions.htm