

# VPN: плюсы и минусы

Александр Шахлевич, специалист отдела маркетинга компании "Информзащита"



## О ТЕХНОЛОГИИ

виртуальных частных сетей VPN не писал еще только ленивый, да и в мире ИБ VPN уже стала де-факто стандартом построения защищенных каналов связи.

## Плата за сохранность

Технология VPN отвечает основополагающим критериям сохранности информации: целостность, конфиденциальность, авторизованный доступ. При правильном выборе VPN обеспечивается масштабирование, то есть использование VPN не создаст проблем роста и поможет сохранить сделанные инвестиции в случае расширения бизнеса. Да и в сравнении с выделенными линиями и сетями на основе Frame Relay виртуальные частные сети не менее надежны в плане защиты информации, однако в 5–10, а иногда и в 20 раз дешевле.

Но у всего есть обратная сторона, и технология VPN не исключение. Одним из недостатков VPN является падение производительности сети, связанное с криптографической обработкой трафика, проходящего через VPN-устройство. Возникающие задержки можно разделить на три основных типа:

- задержки при установлении защищенного соединения между VPN-устройствами;
- задержки, связанные с шифрованием и расшифрованием защищаемых данных, а также с преобразованиями, необходимыми для контроля их целостности;
- задержки, связанные с добавлением нового заголовка к передаваемому пакетам.

Давайте подробнее остановимся на каждом из обозначенных типов.

1. С учетом криптографической стойкости применяемых алгоритмов смена ключа возможна через достаточно длительный интервал времени. Поэтому при использовании средств построения VPN такие задержки практически не влияют на скорость обмена данными.

2. Задержки этого типа начинают сказываться на производительности каналов связи только при передаче данных по высокоскоростным линиям (от 100 Мбит/с). В остальных случаях быстроедействие программной или аппаратной реализации выбранных алгоритмов шифрования и контроля целостности обычно достаточно велико, и в цепочке операций над пакетом "зашифрование – передача в сеть" и "прием из сети – расшифрование" время зашифрования (расшифрования) значительно меньше времени, необходимого для передачи данного пакета в сеть.

3. Здесь-то мы и сталкиваемся с основной проблемой, какой является добавление дополнительного заголовка к каждому пакету, пропускаемому через VPN-устройство. Для примера можно рассмотреть систему управления, которая в реальном времени осуществляет обмен данными между удаленными станциями и центральным пунктом. Размер передаваемых данных не велик – не более 25 байт, что сопоставимо с размером данных в банковской сфере (платежные поручения) и IP-телефонии. Интенсивность передаваемых данных – 50–100 переменных в секунду. Взаимодействие между узлами осуществляется по каналам с пропускной способностью в 64 кбит/с. Пакет со значением одной переменной имеет длину 25 байт (имя переменной – 16 байт, значение переменной – 8 байт, служебный заголовок – 1 байт). IP-протокол добавляет к длине пакета еще 24 байта (заголовок IP-пакета).

В случае использования каналов Frame Relay добавляется еще 10 байт FR-заголовка. Всего 59 байтов (472 бита). Таким образом, для нормальной работы необходима полоса пропускания, что хорошо вписывается в имеющиеся ограничения пропускной способности в 64 кбит/с.

Что мы получаем при использовании средств VPN? Для протокола IPSec и указанных параметров требуемая пропускная способность будет превышена на 6% (67,8 кбит/с). Для протокола, используемого в программно-

аппаратном комплексе "Континент", дополнительный заголовок, добавляемый к каждому пакету, составляет всего 36 байт (или 26 – в зависимости от режима работы), что в данных условиях не вызовет задержек в работе (57 и 51 кбит/с соответственно). Для протокола SSL и тех же условий дополнительный заголовок составит 21 или 25 байт, в зависимости от алгоритма шифрования, это также не вызовет падения производительности.

Пример взят для наглядности, но чем больше объем передаваемых данных, тем больше вносимые задержки. Такое падение производительности сети не критично для большинства приложений и сервисов, но, например, губительно для передачи потокового аудио и видео. Вдобавок с развитием информационных технологий потребность в скоростной передаче трафика большого объема все возрастает, соответственно растут и требования как к самим каналам связи, так и к средствам их защиты.

По мнению западных аналитиков, пока лишь 5% пользователей, работающих, например, в финансовом секторе, нуждаются в таких высоких стандартах. Остальные 95% не столь серьезно относятся к проблемам со связью, а затраты большего количества времени на получение информации не приводят к колоссальным убыткам.

## Модные тренды

Потребности бизнеса и подходы к построению ИБ сформировали к настоящему моменту два ключевых направления развития технологии VPN: это IPsec VPN и SSL VPN. Посмотрим, в чем основные плюсы и минусы каждой из них.

1. IPsec (IP Security) – это набор протоколов, решающих проблемы по шифрованию данных, их целостности и аутентификации. IPsec работает на сетевом уровне. Таким образом, защита данных будет прозрачна для сетевых приложений. В то время как SSL (Secure Socket Layer) – протокол уровня приложений, в основном используется для защищенного обмена информаци-

Определение компании Check Point Software Technologies: "VPN – это технология, которая объединяет доверенные сети, узлы и пользователей через открытые сети, которым нет доверия". На мой взгляд, это наиболее яркая характеристика технологии, получившей в наше время повсеместное распространение в среде не только технических специалистов, но и рядовых пользователей, нуждающихся в защите информации.

ей между удаленными приложениями (по большей части это обращение к Web-серверам), IPsec одинаково обращается с пакетами протоколов более высокого уровня, то есть аутентифицируются и шифруются, не обращая внимания на их содержание. А вот для работы SSL необходим надежный транспортный протокол (например, TCP). Надежность IPsec еще гарантируется тем, что информация о порте, с которым установлено соединение, также недоступна для злоумышленника.

2. IPsec поддерживает три вида установления соединения:

- Gateway-to-Gateway;
- Gateway-to-Host;
- Host-to-Host.

SSL поддерживает только соединение между двумя хостами или клиентом и сервером.

3. IPsec поддерживает цифровую подпись и использование Secret Key Algorithm, в то время как SSL – только цифровую подпись. И IPsec и SSL могут использовать PKI. Преимущество IPsec: для малых систем можно вместо PKI применять preshared keys, что заметно упрощает задачу. Методы, которые использу-

ются в SSL, идеально подходят для установления защищенного соединения между сервером и клиентом. Основное различие между способами аутентификации опять же заключается в том, что IPsec функционирует на сетевом уровне, что позволяет проследить адрес получателя и источника с тем же успехом, что и аутентификацию более высоких уровней. SSL же имеет доступ только к информации транспортного уровня и выше.

4. Среди недостатков IPsec – большой объем дополнительной информации, добавляемой к исходному пакету. В случае SSL этот размер значительно меньше.

5. Для сжатия IPsec применяется протокол IPComp. SSL в меньшей мере использует сжатие, и только OpenSSL поддерживает его полностью. В случае IPsec использование алгоритмов сжатия может приводить к разным результатам при применении их в разных условиях: производительность способна как увеличиваться, так и уменьшаться. Результат зависит от соотношения скоростей шифрования, сжатия и скорости передачи данных.

Большинство алгоритмов шифрования работают быстрее алгоритмов сжатия. Следовательно, это будет приводить к замедлению работы. Но в случае низкой скорости передачи использование сжатия заметно увеличит производительность.

### В качестве заключения

SSL очень быстро развивается в сегменте "клиент-сервер VPN" (по сравнению с IPsec), так как при небольших издержках предоставляет необходимый уровень защищенности информации. И хотя пока SSL пытается на равных конкурировать с IPsec, но с появлением и окончательной стандартизацией IPv6 ситуация должна измениться.

Что выбрать – решать только заказчику. Лидеры по производству средств защиты информации отлично справляются с развитием обоих направлений и способны предложить оптимальное решение, соответствующее индивидуальным потребностям конкретного клиента. ●

Большим преимуществом IPsec остается то, что он работает на любом производителе, поддерживающем IPsec RFC. Например, теоретически возможно установить VPN-соединение между Cisco- и Nortel-маршрутизаторами, но только теоретически, так как время показало: даже если различные производители поддерживают IPsec-стандарты, то все равно иногда встречаются проблемы совместимости. Поэтому в site-to-site сегменте преимущество остается за IPsec. Это связано и с отсутствием стандарта (RFC) на создание site-to-site SSL VPN-сетей, и с тем, что IPsec работает на более низком уровне модели OSI, а это позволяет ему решать более сложные задачи.

Ваше мнение и вопросы  
присылайте по адресу  
[infosec@groteck.ru](mailto:infosec@groteck.ru)