УДК 004.056

В.В. Шейда

Использование протоколов TCP и UDP для защищенной передачи информации по SSL-VPN-туннелям

Исследованы возможности использования протоколов UDP и TCP для передачи информации по защищенным SSL-VPN-туннелям. Проведены измерения зависимости скорости передачи данных и качества, вещаемого видеоизображения, от вероятности потери пакетов в сети для обоих протоколов (TCP и UDP). Предложено решение проблемы «таяния трафика» и передачи UDP трафика по SSL-VPN-туннелям.
Ключевые слова: виртуальная частная сеть, клиент, сервер, туннель, протокол, эффект таяния трафика.

Эффективность ведения бизнеса современного предприятия зависит от возможности его сотрудников получать доступ к информационным ресурсам компании и от способности сотрудников передавать данные в компанию в любой момент времени, находясь в любой точке планеты.

Однако, открытие ресурсов вовне приведет к тому, что они станут доступны не только сотрудникам компании, но и конкурентам. Поддержка модемного пула – достаточно дорогостоящее решение, так как помимо затрат на оборудование оно предполагает непосредственно оплату телефонных звонков, вместе с этим также возникают вопросы, касающиеся безопасности.

Альтернативное решение – это использование VPN (*Virtual Private Network* – виртуальная частная сеть)-технологии, так как при обеспечении высокого уровня безопасности эта технология является наименее дорогостоящей и не вызывает сложностей в применении у конечных пользователей.

VPN-технология, помимо защищенного удаленного доступа для сотрудников, позволяет предприятиям объединять сети территориально разнесенных филиалов и организовывать защищенные видео- и аудиоконференции через Интернет.

На данный момент существует множество VPN решений, однако, в связи с тем, что часто для обеспечения дополнительной безопасности системные администраторы корпоративных сетей закрывают все порты, кроме 80 и 443, использовать многие из них не представляется возможным. Вместо этого используют SSL-VPN (*Secure Socket Layer* – уровень защищенных сокетов), для работы которого, необходим только порт 443 [4].

Очень важно обеспечить быструю и надежную работу *VPN*-сетей, так как от этого зависит оперативность информационного обмена между филиалами предприятия и его сотрудниками.

SSL-VPN обладает рядом недостатков, обусловленных используемыми протоколами, которые ограничивают применение SSL-VPN для осуществления потокового вещания.

Целью статьи является исследование передачи трафика в сети с потерями пакетов.

Для достижения поставленной цели были определены следующие задачи:

– теоретический анализ реализации SSL-VPN-туннеля;

– проведение эксперимента для определения зависимости скорости передачи данных от вероятности отброса пакетов;

– предложение оптимального способа решения выявленных проблем.

1. Механизм передачи информации по SSL-VPN туннелю

Опишем ситуацию передачи данных сотрудником в корпоративную сеть. Допустим, работнику компании необходимо обратиться к защищенному, невидимому извне Web-ресурсу организации. Для этого программное обеспечение (прикладной уровень) должно сформировать HTTP-запрос (*Hyper Text Transfer Protocol* – протокол передачи гипертекстовой информации), который затем инкапсулируется в TCP (*Transport Control Protocol* – протокол управления транспортом) пакет и направляется на порт 80 станции, на которой располагается нужный нам Web-ресурс. Однако по одному порту невозможно идентифицировать требуемую станцию, так как порт – это всего лишь точка доступа к какой-либо программе (в данном случае к Web-серверу). Для того чтобы добраться до нужной станции, необходимо указать её IP-адрес (сетевой уровень), но так как сеть назначения корпоративная, то IP-адрес Web-ресурса – локальный адрес из этой сети, не имеющий абсо-

лютно никакого значения в рамках глобального Интернета. Следовательно, для того чтобы доставить пакет до корпоративной сети, необходим какой-то транспорт по Интернету. Перед транспортировкой весь внутренний стэк протоколов шифруется (протокол SSL), а затем, с помощью внешнего IP, осуществляется передача по сети Интернет до VPN-шлюза. Далее, уже на VPN-шлюзе, пакеты передаются вышестоящему протоколу (TCP), который направляет их на порт, на котором работает программа, расшифровывающая информацию (протокол SSL). После этого, используя IP адрес локального Web-ресурса, внутренний TCP с изначальным HTTP-запросом передаются по корпоративной сети [4]. Полный стэк протоколов, используемый в SSL-VPN, изображен на рис. 1.

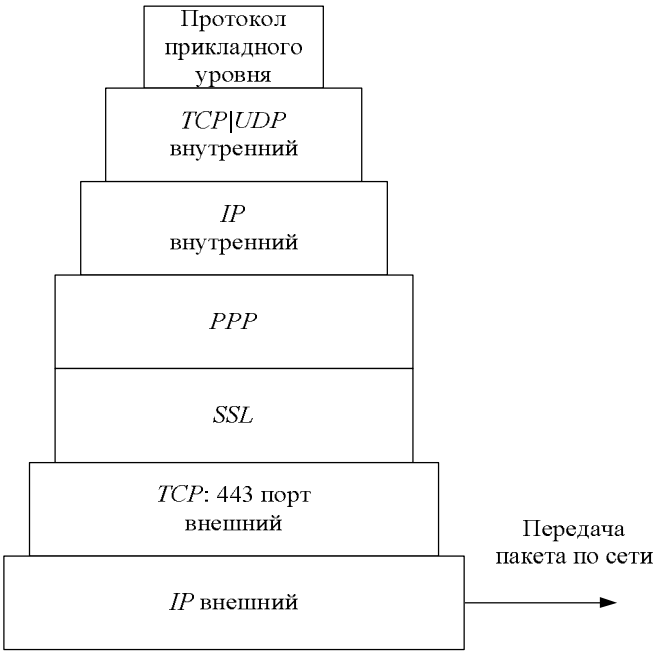

Рис. 1. Стандартный стек протоколов, применяемый в SSL-VPN

2. Проблемы реализации SSL-VPN

Существуют две основные проблемы такой реализации: «эффект таяния трафика» и транспортировка UDP (*User Datagram Protocol* – протокол пользовательских датаграм) поверх TCP.

Протокол TCP – протокол с гарантированной доставкой сообщений. Это значит, что если пакет, содержащий некоторое сообщение, не был доставлен, то он будет поставлен в очередь для повторной отправки и отослан по истечении определенного интервала времени (*retransmission timeout* – таймаут повторной передачи). Если по какой-то причине пакет снова не был доставлен, то TCP использует механизм увеличения таймаута повторной передачи, т.е. времени перед следующей повторной отправкой пакета. Это было сделано для того, чтобы учесть возникшие в сети задержки или просто дать пакету, который по какой-то причине пошел по неоптимальному маршруту, больше времени, чтобы дойти до получателя [1].

Однако при использовании протокола TCP поверх TCP увеличение таймаута повторной передачи внешнего TCP приводит к тому, что внутренний TCP не получит вовремя подтверждения о доставке пакета TCP, посланного по корпоративной сети, и начинет увеличивать свои таймауты. Это приводит к лавинообразному увеличению суммарных задержек, т.е. снижению скорости передачи – «эффект таяния трафика».

Еще одна проблема, связанная с наличием у TCP механизма повторной передачи, возникает при транспортировке UDP-трафика, например видео- или аудиоинформации.

В случае туннелирования UDP поверх TCP, внешний TCP, если пакет не был доставлен, возобновит передачу этого пакета. Следовательно, пакеты, следующие за ним, вынуждены ждать, пока потерянный пакет будет доставлен, что приводит к большим задержкам потокового вещания. Если еще принять во внимание механизм увеличения таймаута повторной передачи, то задержки при передаче потоковой информации становятся абсолютно неприемлемыми [3].

3. Результаты тестирования протоколов TCP и UDP

Для проведения эксперимента были реализованы две схемы: передача трафика по VPN-туннелю поверх TCP и туннелирование трафика поверх протокола UDP. В обоих случаях шифрование не применялось для того, чтобы можно было произвести более детальный анализ трафика.

При проведении эксперимента трафик между VPN-клиентом и сервером проходил через трафик Шейпер (*traffic shaper* – рабочая станция, управляющая трафиком, на которой установлена операционная система UNIX), где с помощью программы *ipfw* был реализован отброс пакетов с определенной вероятностью (рис. 2). Это было сделано для того, чтобы максимально приблизить ситуацию к реальной ситуации в сети.

Экспериментальный полигон (рис. 2) был реализован с применением виртуальных машин с установленными операционными системами *UNIX FreeBSD* 5.4 и *Linux Fedora Core* 5. В качестве среды передачи данных использовался реальный сегмент сети Ethernet.

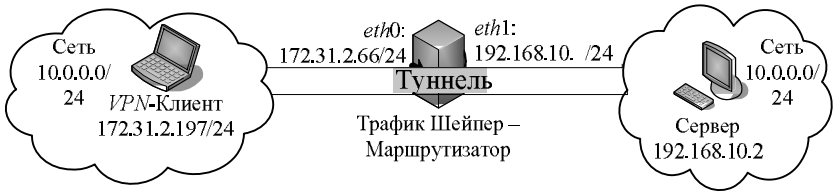

Рис. 2. Экспериментальный полигон системы защиты из двух локальных сетей

Эксперимент проходил в четыре этапа:

1) тестирование туннелирования TCP поверх стандартного TCP;
2) тестирование туннелирования TCP поверх UDP;
3) тестирование туннелирования UDP поверх стандартного TCP;
4) тестирование туннелирования UDP поверх UDP.

Для проведения первых двух этапов использовалась передача файла по FTP-протоколу через VPN-туннель, при этом производились замеры скорости передачи (*V*) в зависимости от различных вероятностей отброса пакетов (*P*). Результаты эксперимента отражены на рис. 3.

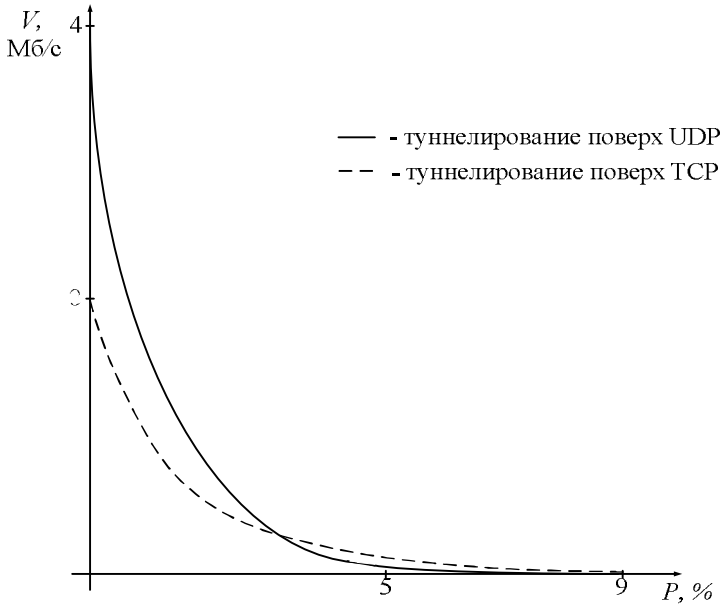

Рис. 3. График зависимости скорости передачи данных от вероятности отброса пакетов

Из рис. 3 видно, что при низких потерях туннелирование по протоколу UDP более эффективно: скорость передачи примерно в два раза выше, чем при туннелировании по TCP. Однако при больших потерях скорость передачи данных по протоколу TCP несколько выше, чем у протокола UDP, что объясняется наличием у внешнего протокола механизмов адаптации к текущей нагрузке сети [2].

Для проведения последних двух этапов на клиенте и сервере были соответственно установлены клиентская и серверная части программы *RealPlayer*, которая предназначена для вещания потокового видео по UDP-протоколу. Это позволило протестировать эффективность передачи UDP-трафика в зависимости от различных вероятностей отброса пакетов.

В результате проведения эксперимента было установлено, что при туннелировании видеопотока поверх *TCP* с вероятностью отброса пакетов менее 4 процентов качество изображения и скорость воспроизведения достаточны для проведения видеоконференций: звуковая информация передавалась без искажений, потери кадров оставались минимальными. Однако повышение вероятности отброса пакетов на один процент привело к значительному ухудшению качества вещания (таблица): видео-поток практически полностью остановился, чему свидетельствует скорость воспроизведения видео – 5, 6 кадров в секунду, чего явно недостаточно для восприятия видеоинформации человеком.

При туннелировании UDP-трафика поверх UDP ситуация заметно лучше: при потере пакетов с вероятностью, меньшей 9%, качество потока оставалось на уровне, достаточном для проведения видеоконференций, что подтверждается высокой скоростью воспроизведения кадров (таблица).

Результаты эксперимента туннелирования UDP

№ п/п	Вероятность отброса пакетов, %	Данные, полученные при туннелировании по TCP			Данные, полученные при туннелировании по UDP		
		FPS, кадр/с	Скорость потока, Кб/с	Количество потерянных кадров	FPS, кадр/с	Скорость потока, Кб/с	Количество потерянных кадров
1	0	24	235	0	24	235	0
2	1	24	235	0	24	235	0
3	2	20	235	22	24	235	0
4	3	24	235	0	24	235	0
5	4	5,6	75,6	440	24	234	3
6	5	<1	54,3	1087	24	234	10
7	6	–	–	–	24	230	10
8	7	–	–	–	23	226	20
9	8	–	–	–	<1	37	952

Как видно из результатов проведенных опытов, использование протокола UDP в качестве внешнего (поверх которого осуществляется туннелирование) можно считать более эффективным для передачи видеоинформации (UDP-трафика) по SSL-VPN-туннелям. Однако при передаче TCP-трафика по сетям с большой вероятностью потери пакетов, из-за отсутствия механизмов адаптации к текущей нагрузке сети, а именно механизма регулирования размера окна, протокол UDP показывает более низкие результаты, чем TCP.

Заключение

Очевидно, что использование лишь одного из протоколов (либо UDP, либо TCP) во всех рассмотренных случаях неприемлемо. Для решения вышеописанных проблем (эффекта таяния трафика и передачи UDP-данных по SSL-VPN-туннелю) необходимо использовать оба протокола – UDP и TCP. Выбор конкретного протокола должен осуществляться динамически в зависимости от типа туннелируемого трафика. В случае передачи TCP-данных, в качестве внешнего транспортного протокола необходимо использовать TCP-протокол, а при передаче UDP-трафика – UDP. Информация об используемом внутреннем транспортном протоколе может быть получена из специального поля IP-заголовка внутреннего IP-пакета [1]. Для гарантированного обмена ключами и установки SSL сессии необходимо использовать TCP-протокол. Для корректной расшифровки данных на стороне получателя в режиме *Cipher Block Chaining* (CBS) при туннелировании по UDP необходимо формировать IP-пакеты таким образом, чтобы зашифрованная информация, передаваемая в одном IP-пакете, не зависела от последующих посылок, тогда при потере одного или более IP-пакетов данные смогут быть расшифрованы.

Литература

1. Семенов Ю.А. Протоколы и ресурсы Internet. – М.: Радиосвязь, 1996. – 320 с.

2. Стивенс У. UNIX: разработка сетевых приложений. – СПб.: Питер, 2004. – 1086 с.

3. Сэтчел Стефен Т. Linux IP Stacks в комментариях / Т. Сэтчел Стефен, Х.Б. Дж. Клиффорд: пер. с англ. – Киев: ДиаСофт, 2001. – 288 с.

4. Хетч Б. Linux: Создание виртуальных частных сетей (VPN) / Б. Хетч, О. Колесников: пер. с англ. – М.: КУДИЦ-ОБРАЗ, 2004. – 464 с.

Шейда Владимир Владимирович
Аспирант каф. радиоэлектроники и защиты информации ТУСУРа
Эл. почта: v.sheyda@gmail.com

Sheyda V.V.
TCP and UDP protocols for secure information transfer through SSL-VPN tunnels

The following article is a summary of a thorough research on a possibility of UDP and TCP protocols usage for secure data transfer through SSL VPN tunnels. As a result of the research the measurements of data transfer speed and video streaming quality correspondence to probability of packet loss were taken for both TCP and UDP protocols. A solution for «traffic meltdown» and problems related to UDP traffic tunneling was also proposed as a result of this research.
Keywords: virtual private network, client, server, tunnel, protocol, traffic meltdown effect.