УДК 004.738

Р. Э. Асратян, канд. техн. наук, вед. науч. сотр., e-mail: rea@ipu.ru,
В. Н. Лебедев, канд. техн. наук, зав. лаб., e-mail: lebvini@ipu.ru,
В. Л. Орлов, канд. техн. наук, вед. науч. сотр., e-mail: ovl@ipu.ru
Институт проблем управления им. В. А. Трапезникова РАН

Эффективность защищенных каналов взаимодействия на основе применения протокола HTTPS в прокси-серверах

Статья посвящена экспериментальному исследованию временных характеристик нового подхода к организации безопасного информационного взаимодействия в мультисетевой среде, основанного на применении протокола HTTPS и технологии прокси-серверов. Суть подхода заключается в организации защищенных HTTPS-соединений между прокси-серверами для безопасной передачи информационных запросов из одной частной локальной сети в другую через глобальную сеть. Приводятся результаты экспериментов, позволяющих определить область эффективного применения подхода.

Ключевые слова: *распределенные системы, Интернет-технологии, сетевые протоколы, прокси-серверы, информационное взаимодействие, информационная безопасность, web-сервисы*

Введение

Интерес разработчиков информационных систем к сетевому протоколу HTTPS [1] как к удобному и доступному средству организации защищенного информационного взаимодействия в глобальных сетях не ослабевает с течением времени. Отчасти это связано с появлением возможности защиты информационных запросов к электронным сервисам в рамках технологии .NET [2, 3] на его основе (протокол SOAP "поверх" HTTPS), отчасти же — с широким распространением распределенных информационных систем и постоянным возрастанием требований к безопасности данных [4, 5] в таких системах.

Аспект информационной безопасности особенно важен в разработках распределенных систем, ориентированных на работу в сложных мультисетевых средах, включающих в себя одну или несколько глобальных сетей и множество частных локальных сетей предприятий различного размера и различной административной подчиненности. Разработчики таких систем зачастую сталкиваются с серьезными проблемами при решении задач маршрутизации и защиты информационных запросов, направленных из одной частной сети в другую.

В работе [6] описан подход к организации безопасного взаимодействия между клиентскими и серверными компонентами, размещенными в разных частных сетях, основанный на применении прокси-серверов — серверов-посредников, размещаемых "на границах" частных сетей и обеспечивающих создание защищенных HTTPS-тоннелей через глобальную сеть (рис. 1). Преимущество данного подхода по сравнению с известными (например, с технологиями NAT или VPN [7, 8]) заключается в том, что на прокси-серверы можно возложить дополнительные функции, связанные с учетом (регистрацией), контролем, фильтрацией, маршрутизацией и защитой информационных запросов. При данном подходе удаленные клиентские и серверные программы пользуются протоколом HTTP и, как и при применении VPN, нисколько не заботятся об информационной защите, а на прокси-серверы возлагаются дополнительные функции шлюзов "HTTP → HTTPS" и "HTTPS → HTTP". Особен-

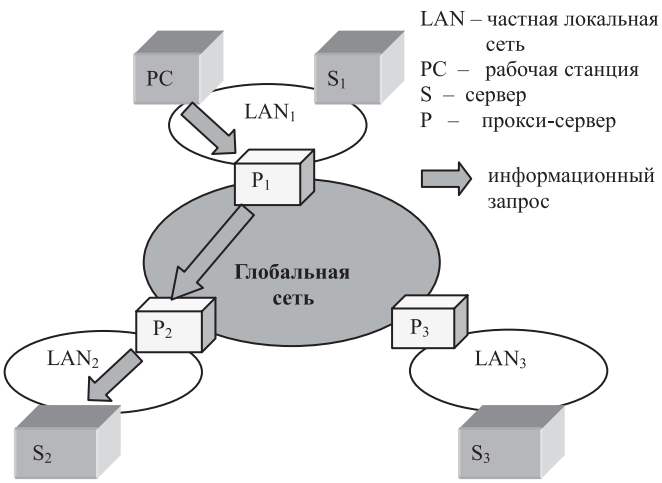

Рис. 1. Маршрутизация запросов в мультисетевой среде

ность подхода заключается в том, что в этом случае прокси-серверы "видят" проходящие через них информационные запросы клиентов и ответы серверов в открытой, дешифрованной форме и способны обеспечить необходимый контроль и высокоуровневую маршрутизацию потока запросов по символическим именам (URL) информационных ресурсов.

Однако данный подход имеет принципиальный недостаток — дополнительные временные задержки, вносимые прокси-серверами в обработку запросов между удаленными частными сетями. Так как эти задержки в значительной степени определяют область эффективного применения подхода, их оценка является необходимым условием его целенаправленного использования. В данной работе приводятся основные результаты экспериментов, направленных на оценку дополнительных накладных расходов времени, связанных с применением защищенных HTTPS-тоннелей на основе прокси-серверов.

Краткое описание принципов организации HTTPS-тоннеля

Суть рассматриваемого подхода заключается в соединении возможностей технологии HTTPS и технологии прокси-серверов для решения двух взаимосвязанных задач:

- обеспечения информационной безопасности данных в условиях угроз, исходящих от глобальной сети;
- маршрутизации запросов между клиентскими и серверными программами, функционирующими в разных частных сетях (см. рис. 1).

Главная особенность подхода заключается в обеспечении "высокоуровневых" средств защиты и маршрутизации, основанных на заголовках и данных HTTP-запросов, а не отдельных IP-пакетов (отметим, что решение этих задач на сетевом уровне, например на основе VPN, может оказаться невозможным или совершенно неэффективным, если число частных сетей исчисляется десятками).

Организация защищенного HTTPS-тоннеля с помощью двух прокси-серверов, выполняющих функции шлюзов "HTTP → HTTPS" и "HTTPS → HTTP", проиллюстрирована на рис. 2. Как видно из рисунка, каждый из прокси-серверов оснащается программной поддержкой SSL/TLS-технологии, обеспечивающей построение защищенного двустороннего канала взаимодействия "поверх" обычного TCP-соединения.

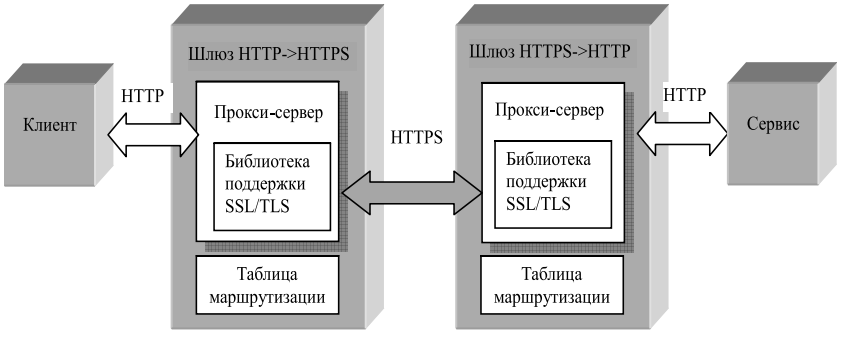

Рис. 2. Принципы организации HTTPS-тоннеля

Как видно из рис. 1, каждый запрос, направленный из одной частной сети в другую, проходит по крайней мере через два прокси-сервера и через два этапа маршрутизации. Из ближайшего прокси-сервера запрос сначала передается в удаленный прокси-сервер по глобальной сети, а уже потом — к адресуемому информационному ресурсу. На каждом этапе маршрутизация проводится на основе символического имени адресуемого ресурса, содержащегося в HTTP-заголовке запроса, с помощью двух таблиц маршрутизации: "глобальной", связывающей Интернет-имя ресурса с адресом удаленного прокси-сервера, и "локальной", связывающей Интернет-имя ресурса с его адресом в частной сети.

Скорость обработки и эффективность применения подхода

К принципиальным недостаткам описанного подхода следует отнести дополнительные временные задержки, вносимые защищенными HTTPS-каналами на основе технологии прокси-серверов. Для оценки этих задержек была проведена серия экспериментов с опытной реализацией шлюзов "HTTP → HTTPS" и "HTTPS → HTTP". Цель экспериментов заключалась в сравнении времен выполнения запросов к модельным электронным сервисам в условиях прямого обращения (без шлюзов) и при обращении через защищенный HTTPS-канал (т.е. через шлюзы). Важно подчеркнуть, что измерялось не только время выполнения одиночных запросов, но и скорость обработки (число обработанных запросов в секунду), достигаемая при одновременной обработке пакета информационных запросов. Другими словами, мы попытались провести сравнение с учетом распараллеливания обработки в множестве программных потоков (и в прокси-сервере, и в службе электронных сервисов для обработки каждого запроса создается отдельный программный поток). Скорость обработки вычислялась как частное от деления числа запросов в пакете на полное время его выполнения.

Эксперименты проводились в условиях скоростного (100 Мбит/с) Ethernet в локальной сети. Модельные web-сервисы [1, 2] с временами выполнения 500, 1000 и 2000 мс были установлены на четырехъядерном сервере приложений с тактовой частотой 3,4 ГГц и 4 Гбайт оперативной памяти (оценка скоростных характеристик выполнялась для каждого электронного сервиса в отдельности). Что же касается прокси-серверов, то для их установки использовались как доста-

точно скромные одноядерные компьютеры с тактовой частотой 2,8 ГГц, так и более современные четырехъядерные с тактовой частотой 3,4 ГГц (чтобы оценить, насколько важно использовать серверы с высокими характеристиками в реализации защищенного канала).

На рис. 3 показан характерный график, который дает представление о дополнительных задержках, вносимых защищенным HTTPS-каналом, при обращении к модельному web-сервису с фиксированным временем выполнения (задержкой), равным 0,5 с. В эксперименте измерялась скорость обработки (число обработанных запросов в секунду), достигаемая при обработке группы запросов, т.е. при одновременном обращении сразу нескольких клиентов. По горизонтальной оси графика отложено число запросов в группе, а по вертикальной — скорость обработки. Кривая, прорисованная тонкой сплошной линией, отражает скорость обработки при прямом обращении к сервису (без шлюзов), а кривые, прорисованные толстой и прерывистой линиями, отражают скорость обработки со шлюзами, функционирующими на одноядерном и четырехъядерном серверах соответственно.

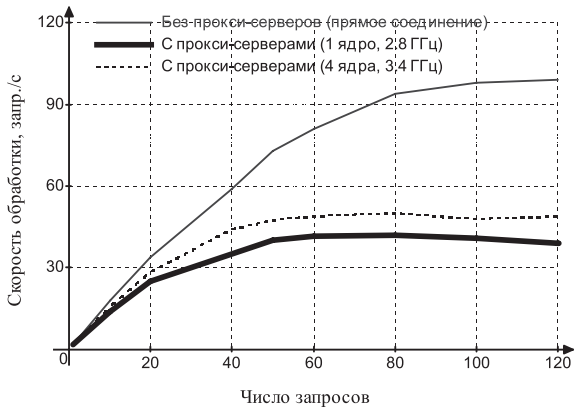

Рис. 3. График зависимости скорости обработки от числа одновременных запросов при задержке web-сервиса 500 мс

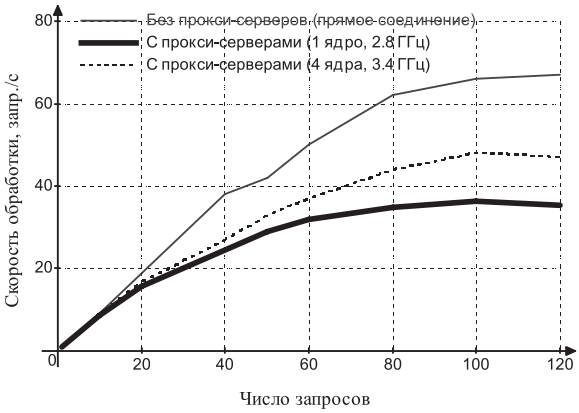

Рис. 4. График зависимости скорости обработки от числа одновременных запросов при задержке web-сервиса 1000 мс

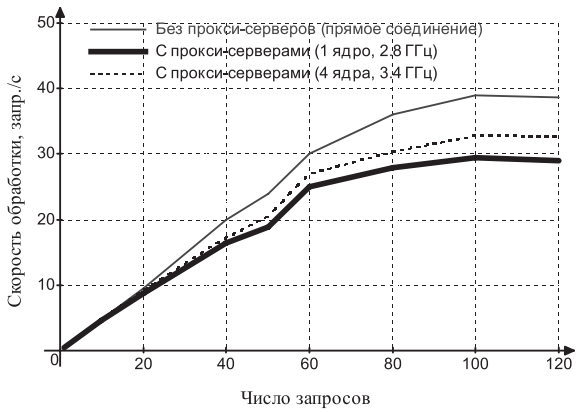

Рис. 5. График зависимости скорости обработки от числа одновременных запросов при задержке web-сервиса 2000 мс

При подаче одиночного запроса на вход сервиса со временем выполнения 0,5 с полное время обработки составило 515 мс без шлюзов, и 546 мс со шлюзами (1,94 и 1,88 запроса в секунду соответственно). Как видно из графика, при росте числа одновременных запросов растет и скорость обработки, что объясняется "многоканальной" природой и прокси-серверов, и электронного сервиса, т.е. положительным эффектом от распараллеливания обработки в нескольких программных потоках. Например, при одновременной подаче 10 запросов время их выполнения составило 544 мс без шлюзов, 627 мс со шлюзами, реализованными в четырехъядерных серверах и 697 мс со шлюзами, реализованными в одноядерных серверах (18,3, 15,9 и 14,3 запросов в секунду соответственно). Как видно из графика, при превышении числа запросов в группе значения 30...40, рост кривых сильно замедляется, а при превышении значения 60...80 — прекращается вовсе, достигая предельной производительности.

Как видно из рис. 3, при обращениях к быстрому web-сервису (0,5 с) применение прокси-серверов существенно замедляет обработку практически при любом числе запросов в группе. При увеличении числа запросов это замедление возрастает и становится более чем двукратным. Характерно, что переход от использования одноядерных серверов в шлюзах к использованию четырехъядерных не дает значительного эффекта (это тем более удивительно, что аналогичный переход в сервере приложений повышает скорость обработки в несколько раз). По-видимому, это связано с тем, что основные временные затраты в работе прокси-сервера связаны с выполнением сетевых функций (прежде всего функции connect) и мало зависят от числа ядер и тактовой частоты.

На рис. 4 и 5 показаны аналогичные кривые для ситуаций, в которых время выполнения модельного web-сервиса составляет 1 и 2 с соответственно. Можно констатировать, что общие закономерности в поведении кривых сохраняются и в этом случае, но эффект замедления обработки вследствие применения шлюзов "HTTP → HTTPS" и "HTTPS → HTTP" заметно сглаживается.

На рис. 6, 7 и 8 приведены графики зависимости среднего времени выполнения информационного

запроса от числа запросов в пакете при обращении к тем же трем модельным сервисам и в тех же обозначениях. В отличие от рис. 3, 4 и 5, здесь все кривые демонстрируют устойчивый рост. Легко видеть, что и по этому важному показателю влияние шлюзов HTTP → HTTPS" и "HTTPS → HTTP" является довольно ощутимым при обращении к более быстрому сервису (0,5 с) и менее ощутимым при обращении к более медленным сервисам (1 и 2 с). Например, при поступлении 20 одновременных запросов соотношение значений среднего времени обработки запроса со шлюзами и без шлюзов равно 1,29 в первом случае, 1,12 во втором и 1,08 в третьем (при использовании одноядерных серверов в шлюзах).

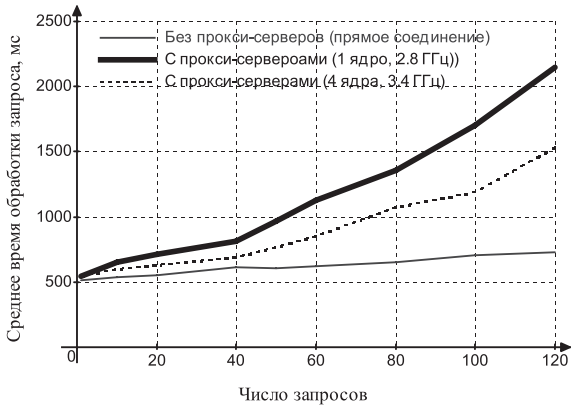

Рис. 6. График зависимости среднего времени обработки запроса от числа одновременных запросов при задержке web-сервиса 500 мс

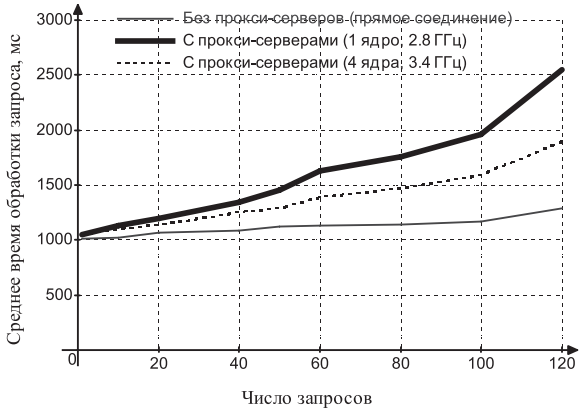

Рис. 7. График зависимости среднего времени обработки запроса от числа одновременных запросов при задержке web-сервиса 1000 мс

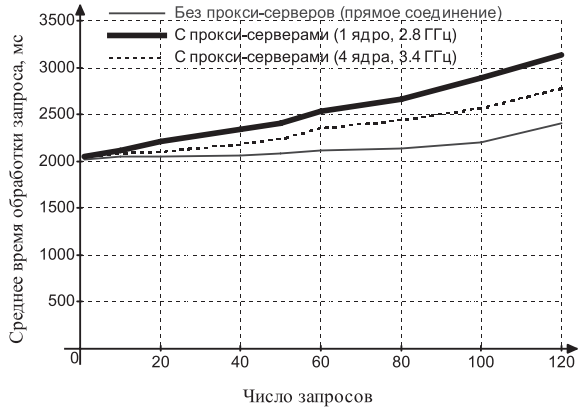

Рис. 8. График зависимости среднего времени обработки запроса от числа одновременных запросов при задержке web-сервиса 2000 мс

Заключение

В целом результаты проведенных экспериментов позволяют сформулировать следующие выводы.

- Применение шлюзов "HTTP → HTTPS" и "HTTPS → HTTP" в целом сохраняет положительный эффект от многопоточного распараллеливания обработки.
- Построенный по вышеописанным принципам защищенный HTTPS-канал вполне позволяет поддерживать скорость обработки до нескольких десятков запросов в секунду, что обычно бывает достаточным для большинства информационно-управляющих систем.
- Чем больше время выполнения электронного сервиса, тем менее заметна задержка, вносимая шлюзами. В частности, в проведенных экспериментах наблюдалось заметное снижение скорости обработки при одновременном обращении сразу нескольких клиентов к быстрым (со временем выполнения менее 1 с) электронным сервисам через защищенный HTTPS-канал и не столь существенное при обращении к более медленным (со временем выполнения более 1 с).

Существенный недостаток описанного подхода заключается в том, что в пределах частной локальной сети данные передаются в открытом виде. Поэтому его применение ограничено ситуациями, в которых частные сети можно рассматривать как "зоны доверия", а единственным источником угроз является глобальная сеть. В этих условиях он может обеспечить "централизованную" защиту информационных запросов при обращении к относительно "медленным" электронным сервисам (со временем выполнения более 1 с) без значительного снижения скорости обработки.

Список литературы

1. **Кришнамурти Б., Рэксфорд Д.** Web протоколы. М.: Бином, 2010. 592 с.
2. **Шапошников И. В.** Web-сервисы Microsoft.NET. СПб.: БХВ-Петербург, 2002. 336 с.
3. **Мак-Дональд М., Шпушта М.** Microsoft ASP.NET 3.5 с примерами на C# 2008 и Silverlight 2 для профессионалов. М.: Вильямс, 2009. 1408 с.
4. **Згоба А. И., Маркелов Д. В., Смирнов П. И.** Кибербезопасность: угрозы, вызовы, решения // Вопросы кибербезопасности. 2014. № 5. С. 30—38.
5. **Щеглов А. В.** Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и техника, 2004. 384 с.
6. **Асратян Р. Э., Лебедев В. Н., Орлов В. Л.** Организация защищенных каналов взаимодействия на основе применения протокола HTTPS в прокси-серверах // Информационные технологии. 2015. Т. 21, № 9. С. 670—674.
7. **Хант К.** TCP/IP. Сетевое администрирование. СПб.: Питер, 2007. 816 с.
8. **Андреев А. Г., Беззубов Е. Ю., Емельянов** и др. Windows 2000: Server и Professional. СПб.: БХВ-Санкт-Петербург, 2001. 1055 с.

R. E. Asratian, Leading Researcher, rea@ipu.ru, **V. N. Lebedev,** Head of Laboratory, lebvini@ipu.ru,
V. L. Orlov, Leading Researcher, ovl@ipu.ru, Institute of Control science RAS

Efficiency of a Secure Communication Channels Based on the Use of the HTTPS in Proxy Servers

The article is devoted to experimental study of characteristics of the new method of secure interactions organization in multi-network environment. The method is based on the use of HTTPS protocol and proxy server technology. The essence of approach consists in the organization of the protected HTTPS connections between proxy servers for safe transfer of information queries from one private local network in another through a global network while client and server components of distributed system are released from of information protection functions. In this approach client and server programs use HTTP protocol and proxy servers have additional functions of "HTTP -> HTTPS" and "HTTPS -> HTTP" gateways. The main advantage of approach over known (for example, VPN) consists in providing "high-level" means of HTTP queries routing and filtration the based on headers of HTTP queries, but not on separate IP packages. The application of approach is limited to situations in which private local networks can be considered as "a trust zone", and the only source of threats is the global network. The experimental study of efficiency of the offered approach in terms of influence of protection gateways on the speed of electronic services calls processing is conducted. This research showed that the area of effective application of the approach is made by electronic services with performance time over 1—2 s.

Keywords: *distributed systems, Internet technologies, network protocols, proxy servers, remote interactions, data security, web-services*

References

1. **Krishnamurti B., Reksford D.** *Web protokoly*. Moscow: Binom, 2010. 592 p.
2. **Shaposhnikov I. V.** *Web-servisy Microsoft.NET*. SPb: BHV-Peterburg, 2002. 336 p.
3. **Mak-Donal'd M., Shpushta M.** *Microsoft ASP.NET 3.5 s primerami na C# 2008 i Silverlight 2 dlja professionalov*. Moscow: Vil'jams, 2009. 1408 p.
4. **Zgoba A. I., Markelov D. V., Smirnov P. I.** Kiberbezopasnost': ugrozy, vyzovy, reshenija, *Voprosy kiberbezopasnosti*, 2014, no. 5, pp. 30—38.
5. **Shheglov A. V.** *Zashhita komp'juternoj informacii ot nesankcionirovannogo dostupa*. SPb.: Nauka i tehnika, 2004, 384 p.
6. **Asratjan R.Je., Lebedev V. N., Orlov V. L.** Organizacija zashhishhennyh kanalov vzaimodejstvija na osnove primenenija protokola HTTPS v proksi-serverah, *Informacionnye tehnologii*, 2015, vol. 21, no. 9, pp. 670—674.
7. **Hant K.** TCP/IP. *Setevoe administrirovanie*. SPb.: Piter, 2007. 816 p.
8. **Andreev A. G., Bezzubov E. Ju., Emel'janov** i dr. *Windows 2000: Server i Professional*. SPb.: BHV-Sankt-Peterburg, 2001. 1055 p.

УДК 004.45

В. В. Грибова, д-р техн. наук, зам. директора по научной работе, e-mail: gribova@iacp.dvo.ru,
А. В. Иванова, аспирант, e-mail: 2395146@gmail.com,
Институт автоматики и процессов управления Дальневосточного отделения Российской Академии наук

Концепция программного комплекса для управления безопасностью информационных систем

Рассмотрены существующие подходы к созданию систем защиты, их достоинства и недостатки. Описаны основные требования, принципы и концептуальная архитектура программного комплекса для управления безопасностью информационных систем, состоящая из двух подсистем: среды управления информационными ресурсами и клиентской среды управления безопасностью информационной системы. Описаны основные компоненты программного комплекса и их функции.

Ключевые слова: *информационная безопасность, управление, интеллектуальные системы, базы данных, онтологии, базы знаний, защита информации, информационные системы*

Введение

Обеспечение защиты информации в информационных системах является очень актуальной задачей. Исследование компании Dell, проведенное в 2014 г., показало [1], что из 1440 опрошенных компаний подавляющее большинство (90 % специалистов) отметили, что информационная безопасность становится одним из главных приоритетов в планируемом бюджете, и примерно 20 % всех затрат на информационные технологии (ИТ) будет