УДК 004.056.5

DOI: 10.15827/0236-235X.132.605-612

Дата подачи статьи: 12.05.20

2020. Т. 33. № 4. С. 605–612

Оптимизация скорости VPN для удаленной работы с использованием маршрутизаторов с ARM-процессорами

С.В. Андреев¹, научный сотрудник, esa@gin.keldysh.ru

А.А. Хлупина¹, младший научный сотрудник, nastya_75@mail.ru

¹ Институт прикладной математики им. М.В. Келдыша РАН,
г. Москва, 125047, Россия

Данная статья посвящена задачам оптимизации скорости VPN-соединения при использовании маршрутизаторов с процессорами ARM. В современных условиях на многих предприятиях и в учреждениях по всему миру встает актуальный вопрос обеспечения доступа сотрудников, а также удаленного филиала или подразделения к ресурсам локальной сети головного офиса. В статье рассматривается возможность подключения сотрудников по зашифрованному VPN-каналу с использованием современных бытовых маршрутизаторов с ARM-процессорами. При таком подходе обеспечивается автоматическое подключение всех устройств удаленного пользователя к ресурсам локальных сетей головного офиса, предприятия и нет необходимости для IT-специалистов предприятия настраивать каждое устройство пользователя в отдельности.

В работе рассматривается решение ключевой проблемы такого подхода, а именно обеспечение максимальной скорости зашифрованного VPN-подключения и, следовательно, ускорение программных компонентов маршрутизаторов, включенных в его ПО для скоростного зашифрованного VPN-соединения. Рассматривается оптимизация скорости алгоритмов шифрования и дешифровки с использованием особенностей целевого процессора устройства, таких как распараллеливание выполнения инструкций процессора с помощью SIMD, общее улучшение производительности маршрутизатора при использовании оптимальных опций компилятора, нетрадиционное использование PCI-устройств аппаратного шифрования, использование альтернативных вариантов современных VPN-сетей для маршрутизаторов с относительно маломощным по тактовой частоте центральным ARM-процессором, но содержащим более двух ядер, обеспечивая при этом многопоточность VPN-канала.

Ключевые слова: удаленный доступ, маршрутизаторы, архитектура ARM, компьютерные вычисления SIMD, расширение инструкций для ARM-процессора NEON, OpenVPN, протокол OpenSSL, алгоритм шифрования AES, WireGuard.

Проблема обеспечения доступа сотрудников предприятий и учреждений, а также удаленных филиалов и подразделений к ресурсам локальной сети головного офиса не теряет актуальности во всем мире.

Удаленные пользователи, часто находящиеся даже в другом городе или стране, вынуждены использовать открытые сети Интернета, поэтому встает вопрос обеспечения безопасности данных и исключения утечки информации. Для решения проблемы сохранения безопасности данных и информации при необходимости удаленного доступа к локальным сетевым ресурсам и БД предприятия/учреждения применяется подход с использованием виртуальных частных сетей, или VPN (Virtual Private Network).

Это работает следующим образом: создается виртуальный цифровой канал поверх открытых сетей, и перехват трафика третьими лицами не позволит им получить доступ к секретной информации, так как при этом исполь-

зуются надежные алгоритмы шифрования потока данных.

VPN-решение подходит и частным лицам, нередко вынужденным использовать открытые незашифрованные сети в кафе или гостиницах, для обеспечения приватности доступа к своим домашним архивам.

Использование маршрутизаторов для VPN-соединений

На данный момент подавляющее большинство VPN-решений обеспечивают кросс-платформенную совместимость, демонстрируя отличную работу на различных типах устройств (Windows, Mac, Linux, iOS, Android) как при использовании специальных клиентов, так и при ручной настройке. Однако в большинстве случаев для системных администраторов головных предприятий и учреждений такой подход с использованием отдельных конфигурационных файлов VPN-клиентов для каждого

работника предприятия, часто имеющего несколько устройств (компьютер, телефон, планшет), неприемлем из-за трудоемкости настройки и поддержки всех этих устройств. Как решение в таких случаях применимо централизованное использование маршрутизаторов (роутеров), поддерживающих постоянное соединение с головным VPN-сервером предприятия/учреждения 24 часа в сутки и обеспечивающих одновременный доступ к данным локальных сетевых ресурсов предприятия для всех своих пользователей, подключенных проводным или беспроводным соединением. При таком подходе IT-специалистам, а также домашним пользователям достаточно настроить и поддерживать в рабочем состоянии только сам маршрутизатор, автоматически обеспечивая тем самым VPN-соединение для различных устройств одновременно.

Кроме того, сравнительно недорогой бытовой маршрутизатор может выступать и в качестве дешевого домашнего микросервера VPN для нужд частного лица, обеспечивая приватность его соединения при использовании открытых сетей Wi-Fi. Такие бытовые маршрутизаторы относятся к классу SOHO (Small Office, Home Office), они доступны по цене и могут использоваться для подключения относительно небольшого филиала или домашней квартиры работника к центральному серверу VPN.

Проблема при использовании маршрутизаторов для VPN-соединений

В настоящее время наибольшее распространение получила OpenVPN [1, 2] с открытым исходным кодом, применяемая для создания зашифрованных каналов и свободно распространяемая под лицензией GNU GPL [3]. Сеть позволяет устанавливать соединение между компьютерами и устройствами, находящимися за NAT и сетевым экраном, без изменения их настроек. Данные, передаваемые и принимаемые VPN-сервером, идут по зашифрованному каналу, защита которого обеспечивает безопасность и приватность. Шифрование и дешифрование данных происходят как на сервере, так и на клиентской машине. При этом чаще для шифрования канала используется OpenSSL – полноценная криптографическая библиотека с открытым исходным кодом [4], широко известная из-за расширения SSL/TLS, применяемого, например, в веб-протоколе HTTPS. Она поддерживает симметричный алгоритм блочного шифрования AES [5], который в настоящее

время является одним из самых распространенных алгоритмов криптографии. Так, аппаратная поддержка инструкций AES введена компаниями Intel/AMD в семейство процессоров x86/x64, которые в основном используются в современных мощных компьютерах – серверах VPN предприятий и учреждений.

Однако подавляющее большинство современных маршрутизаторов построено на базе намного более слабого типа процессоров ARMv7-A [6], управляемых специализированной версией Linux и чаще всего с аппаратным ускорением NAT и беспроводным соединением (прошивкой), но не обладающих поддержкой AES-шифрования на уровне инструкций *центрального процессора управления* (ЦПУ). Таким образом, при использовании маршрутизаторов критичной является скорость работы библиотеки OpenSSL. Необходимо, чтобы шифрование и дешифрование не замедляли скорость канала OpenVPN, тем самым обеспечивая быстрый доступ пользователей к ресурсам удаленной локальной сети.

Методы ускорения работы OpenSSL с учетом специфических возможностей ARM-процессора

Рассмотрим типичную ошибку, допускаемую разработчиками ПО маршрутизаторов. Часто они не являются постоянными сотрудниками компании-производителя маршрутизаторов, а временно наняты в формате аутсорсинга.

OpenSSL – кросс-платформенное решение, и ее стандартная сборка компилятором, как и само использование, возможны для различных типов процессоров (x86/x64, ARM, MIPS, PowerPC и т.д.). Однако такой формальный обобщенный подход к компиляции OpenSSL полностью не раскрывает всех возможностей целевого процессора, что приводит к деградации скорости шифрования и дешифрования, тем самым замедляя канал VPN-соединения. Первый процессор архитектуры ARM был создан еще в 1985 году, и с того времени его архитектура постоянно совершенствовалась и дополнялась. Так, например, ARMv7-A на базе ядра Cortex-A9, довольно широко используемый в маршрутизаторах, опционально поддерживает усовершенствованный SIMD (Single Instruction, Multiple Data) [7, 8], названный технологией NEON, что позволяет обеспечить параллелизм вычислений, а, следовательно, значительно ускорить процессы шифрования и дешифрования (рис. 1).

Кроме того, Cortex-A9 также опционально может содержать блок FPU VFPv3. Более продвинутый вариант процессора с ядром Cortex-A15 или близкий к нему вариант ARM-процессора Snapdragon Krait [9] компании Qualcomm уже в обязательном порядке содержит и NEON, и более продвинутый блок FPU VFPv4. Использование этих специальных возможностей позволяет значительно ускорить работу криптоалгоритмов на современных ARMv7-A, а значит, ускорить и VPN-канал.

Рассмотрим пример ошибки, допущенной разработчиками компании, создающей официальную прошивку для маршрутизатора R9000 компании NETGEAR. При этом R9000 позиционируется NETGEAR как самый быстрый маршрутизатор в мире. Он оснащен достаточно мощным четырехъядерным ARM-процессором с частотой 1,7 ГГц с ядром Cortex-A15. Представим результаты тестов OpenSSL, выполненных на официальной прошивке маршрутизатора:

The 'numbers' are in 1000s of bytes per second processed.

type	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
sha1	19729.61k	54213.54k	111554.18k	150575.10k	168700.40k
des cbc	33284.58k	34141.59k	34585.00k	34665.81k	34553.86k
des ede3	12548.81k	12727.87k	12788.65k	12801.71k	12782.25k
aes-128 cbc	57205.07k	60562.69k	62545.32k	63109.12k	63310.51k
aes-192 cbc	50571.55k	52632.14k	53764.35k	54159.02k	54274.73k
aes-256 cbc	44746.83k	45857.66k	47048.96k	47419.08k	47363.41k
sha256	13311.57k	29732.76k	50673.44k	61281.28k	65227.43k
sha512	3768.93k	14927.25k	21400.58k	29089.11k	32216.41k
sign verify sign/s verify/s					
rsa 2048 bits	0.036533s	0.001101s	27.4	908.0	
sign verify sign/s verify/s					
dsa 2048 bits	0.012148s	0.013405s	82.3	74.6	

Результаты того же теста при специализированном использовании инструкций NEON и

некоторых других возможностей Cortex-A15 для OpenSSL в созданной авторами данной статьи версии прошивки на том же маршрутизаторе выглядят следующим образом:

The 'numbers' are in 1000s of bytes per second processed.

type	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
sha1	21691.86k	67717.40k	163728.90k	251297.48k	296394.75k
des cbc	33224.61k	34769.92k	35351.13k	35573.21k	35370.33k
des ede3	13231.06k	13375.81k	13498.79k	13595.49k	13485.29k
aes-128 cbc	76702.52k	80093.80k	83207.17k	84156.70k	83875.16k
aes-192 cbc	61568.46k	66469.16k	70230.95k	71435.13k	71363.24k
aes-256 cbc	55345.12k	57141.60k	58567.85k	58935.30k	59026.09k
sha256	24173.65k	56915.65k	102226.09k	128476.16k	139047.56k
sha512	11151.64k	44457.20k	66356.57k	93356.71k	105865.22k
sign verify sign/s verify/s					
rsa 2048 bits	0.008718s	0.000212s	114.7	4709.8	
sign verify sign/s verify/s					
dsa 2048 bits	0.002358s	0.002485s	424.1	402.4	

Как можно заметить, скорость алгоритма AES увеличилась до 33 %, алгоритма хеширования SHA-512 [10] – более, чем в 3 раза, а алгоритма RSA [11] подписи и проверки – в 4–5 раз. Это значит, что скорость OpenVPN-соединения для данного маршрутизатора может быть увеличена примерно на 35–50 % при использовании альтернативной оптимизированной прошивки и, следовательно, «самый быстрый маршрутизатор в мире» может быть значительно ускорен.

Еще более интересные результаты тестов можно получить, применяя те же способы оптимизации для маршрутизаторов с двухъядерным процессором IPQ8064 компании Qualcomm с частотой 1,4 ГГц и ядром Snapdragon Krait. Данный процессор используется в маршрутизаторах NETGEAR R7500, R7500v2, ZyXEL NBG6816, ASUS RT-AC87U и во многих моделях других производителей. Так, для алгоритма AES-256-CBC в официальной прошивке от компании NETGEAR наблюдается скорость 24443,80 k для блока размером 1 Кб, а в прошивке, оптимизированной авторами, достигнут результат 42048,00 k, то есть скорость OpenVPN-соединения может и, следовательно, должна быть увеличена как минимум на 70 %.

Методы ускорения работы OpenSSL при нестандартном использовании дополнительных аппаратных средств маршрутизаторов

Многие современные маршрутизаторы, хотя и не обладают поддержкой AES-инструкций в ЦПУ в соответствии со спецификацией ARMv7-A, оснащены специальными аппаратными криптографическими ускорителями, которые чаще всего используются в закрытых кодах драйверов производителей чипсетов для

этих маршрутизаторов. Однако использование таких аппаратных ускорителей вполне применимо для ускорения OpenSSL, а следовательно, и для увеличения скорости OpenVPN-канала, что, к сожалению, очень часто игнорируется разработчиками официальных прошивок. Так, все тот же маршрутизатор R9000 компании NETGEAR оснащен специальным PCI-устройством аппаратного криптографического ускорителя, но в официальной прошивке данные возможности для ускорения OpenSSL не используются, как и возможности самого ЦПУ, что описано выше.

Для доступа к возможностям таких аппаратных криптографических ускорителей обычно используется метод доступа через драйвер ядра, так как сами ускорители поддерживают инструкции, отличающиеся от инструкций ЦПУ.

Драйвер ядра, разработанный авторами для R9000, создает после загрузки прошивки специальное устройство /dev/crypto, которое позволяет OpenSSL использовать аппаратные возможности ускорителя (рис. 2).

Тесты OpenSSL показали следующие результаты.

При использовании аппаратного ускорителя для алгоритма AES-256-CBC:

The 'numbers' are in 1000s of bytes per second processed.

type	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
aes-256-cbc	1313.02k	5265.17k	20732.59k	70701.06k	305261.23k

При полном использовании всех возможностей ЦПУ (NEON и т.п.):

The 'numbers' are in 1000s of bytes per second processed.

type	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
aes-256 cbc	55345.12k	57141.60k	58567.85k	58935.30k	59026.09k

При игнорировании специфики процессора в официальной прошивке:

The 'numbers' are in 1000s of bytes per second processed.

type	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
aes-256 cbc	44746.83k	45857.66k	47048.96k	47419.08k	47363.41k

Наблюдается существенная деградация производительности для малых блоков памяти размером менее 1 Кб (от 16 байт до 256 байт). Это происходит из-за специфики взаимодействия шины PCI с памятью RAM-устройства. Однако принцип работы OpenVPN основан на использовании достаточно больших блоков памяти, и, следовательно, этой деградацией для малых блоков можно пренебречь. Для достаточно больших блоков в 8 Кб получаем ускорение почти в 6,5 раза.

Для демонстрации возможностей маршрутизатора, достижимых при использовании аппаратных возможностей криптографических устройств, можно привести результаты аналогичного теста для процессора Intel Xeon L5420 с тактовой частотой 2,50 ГГц, использующегося в сервере HP Proliant, до сих пор применяемого во многих учреждениях и предприятиях:

The 'numbers' are in 1000s of bytes per second processed.

type	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
aes-256-cbc	114937.78k	144171.48k	154188.71k	156741.29k	157261.82k

То есть для блоков от 8 Кб скорость OpenSSL в относительно недорогом маршрутизаторе стоимостью в несколько сотен долларов США, с процессором на базе ARMv7-A, с тактовой частотой 1,7 ГГц почти в два раза превосходит скорость high-end сервера стоимостью в несколько десятков тысяч долларов США.

Методы общей оптимизации, использующие возможности компилятора и учитывающие специфику целевого ARM-процессора

Еще одна типичная ошибка, допускаемая разработчиками официального ПО маршрутизаторов, – некорректный набор опций компилятора GNU C/C++, используемый при сборке всей прошивки, а следовательно, и OpenVPN. Обычно такой набор опций устанавливается в конфигурационном файле один раз и затем автоматически используется для сборки всех программных пакетов прошивки и ядра Linux. Особенно это касается нестандартных целевых ARM-совместимых ЦПУ, например, таких как семейство процессоров Snapdragon с ядром Krait компании Qualcomm, созданных по лицензии от ARM. Например, рассмотрим двухъядерные процессоры Qualcomm IPQ8065 с тактовой частотой 1,7 ГГц, использующиеся в таких маршрутизаторах, как NETGEAR R7800, Synology RT2600ac, ASUS BRT-AC828, и в маршрутизаторах некоторых других производителей.

Разработчики официальных прошивок ошибочно предполагают, что данный процессор с ядром Krait является клоном ядра Cortex-A9 от ARM, не учитывая, что по набору инструкций и поддерживаемым расширениям Krait, скорее, является клоном более продвинутого ядра Cortex-A15, обладающего значительно большей производительностью и большими возможностями из-за этих расширений. Причем такую ошибку допускали в свое время разработчики усовершенствованной версии компилятора GNU C/C++ Linaro (Linaro – некоммерческая организация, занимающаяся консолидацией и оптимизацией ПО с открытыми исходными кодами для платформ ARM) и даже разработчики широко известной альтернативной прошивки OpenWRT/LEDE [12].

Так, в официальной версии прошивки для маршрутизатора NETGEAR R7800 до сих пор используются опции компилятора [13], например `-march=armv7-a` и `-mfpu=vfpv3-d16`, в то время как

ЦПУ с ядром Krait поддерживает более продвинутый блок FPU – VFPv4, а использование `-march=armv7-a` не позволяет, например, применять такие инструкции, как SDIV/UDIV для целочисленного деления чисел, которые выполняются намного быстрее аналогичных стандартных инструкций ARM. То есть набор инструкций для Cortex-A15, а следовательно, и для Krait, является надмножеством инструкций ARMv7-A. Таким образом, простая замена этих опций компилятора на `-mcpu=cortex-a15` и `-mfpu=neon-vfpv4` позволяет получить увеличение производительности OpenVPN на 10–15 %, как и общей производительности маршрутизатора, так как разработчики официальной прошивки ограничивали использование всех возможностей целевого ЦПУ выбором некорректных опций GNU C/C++ компилятора.

Например, результаты теста вычисления скорости работы с RAM и вычисления чисел Пи и Е с использованием опций, выбранных разработчиками официальной прошивки (`-march=armv7-a` и `-mfpu=vfpv3-d16`) на маршрутизаторе с процессором IPQ8065, будут следующими:

```
Time to run memory bench: 0.49[secs]
Time to run computation of pi (2400 digits, 10 times): 2.88[secs]
Time to run computation of e (9009 digits): 2.41[secs]
```

А этот же тест с опциями `-mcpu=cortex-a15` и `-mfpu=neon-vfpv4`:

```
Time to run memory bench: 0.43[secs]
Time to run computation of pi (2400 digits, 10 times): 1.50[secs]
Time to run computation of e (9009 digits): 1.43[secs]
```

Так, можно наблюдать значительное увеличение скорости вычислений, что ведет и к увеличению скорости канала OpenVPN (как, впрочем, и к увеличению общей производительности маршрутизатора).

Виртуальная частная сеть WireGuard

Многие бытовые маршрутизаторы класса SOHO не обладают достаточно мощным процессором для обеспечения скоростного соединения средствами OpenVPN. Тем не менее, значительная часть таких маршрутизаторов оснащена четырехъядерным процессором ARM. При использовании OpenVPN такая многоядерность ЦПУ не имеет значения, так как OpenVPN работает в пространстве пользователя (user space) и использует только один поток (single thread) для соединений, то есть одно ядро ЦПУ.

Однако в настоящее время все большую популярность приобретает новый тип виртуаль-

ной частной сети – WireGuard [14]. Это бесплатная VPN с полностью открытым исходным кодом. Создатели позиционируют ее как «экстремально простую в использовании, максимально быструю в настоящее время VPN, использующую ультрасовременные алгоритмы криптографии».

Одним из главных преимуществ WireGuard является то, что эта VPN включена в ядро Linux (kernel space) и поддерживает многопоточность (multi-threading) в отличие от OpenVPN. Таким образом, ключевой особенностью маршрутизатора для работы с этой VPN становится не тактовая частота ЦПУ, а количество ядер процессора.

Так, сравнительно низкопроизводительный маршрутизатор системы NETGEAR Orbi RBK50 (трехдиапазонная mesh-система для бесшовного покрытия сетью Wi-Fi протяженного пространства дома или офиса) с ARM-процессором IPQ4019 (ARM-процессор Cortex-A7, тактовая частота 710MHz) не может обеспечить приемлемую скорость канала OpenVPN, значительно проигрывая, например, маршрутизаторам с ARM-процессором IPQ8065 (Krait, 1,7 GHz, 2 ядра). Однако процессор IPQ4019 четырехъядерный, и при использовании WireGuard скорость VPN-канала по результатам тестов значительно превосходит скорость OpenVPN-канала с использованием процессора IPQ8065.

Хотя в VPN WireGuard и не используется библиотека OpenSSL, авторам удалось использовать многие методы ускорения работы WireGuard, описанные выше. Так, ARM-процессор Cortex-A7 также обладает блоком SIMD NEON, то есть работа по шифрованию и дешифрованию канала VPN может быть распараллелена не только по ядрам процессора, что обеспечивается самой VPN WireGuard (multi-threading), но и в каждом ядре (SIMD NEON).

Кроме того, разработчики ПО официальной прошивки этой системы повторили все те же ошибки, что и ранее с другими маршрутизаторами, не учитывая, что Cortex-A7 по набору инструкций абсолютно совпадает с Cortex-A15 и с Krait, используя достаточно общие опции компилятора GNU для архитектуры ARM, такие как `-march=armv7-a` и `-mfpu=vfpv3-d16`.

Помимо этого, разработчики официальной прошивки допустили еще одну очень серьезную ошибку, используя опцию `-mfloat-abi=soft`. На практике данная опция совершенно исключает из работы блок FPU, то есть блок FPU полностью выключен для арифметических операций с числами с плавающей точкой, что ведет к деградации общей производительности маршрутизатора.

Заменяя опции, выбранные разработчиками официальной прошивки, на оптимальные для данного целевого типа ARM-процессора, то есть `-mcpu=cortex-a7`, `-mfpu=neon-vfpv4`, `-mfloat-abi=soft`, удалось увеличить общую производительность системы в среднем на 10–15 %. Например, специализированный тест вычислений чисел Пи и Е, собранный с опциями разработчиков официальной прошивки, дает следующие результаты:

```
Time to run memory bench: 1.94[secs]
Time to run computation of pi (2400 digits, 10 times): 3.61[secs]
Time to run computation of e (9009 digits): 4.04[secs]
```

А собранный с опциями, выбранными авторами:

```
Time to run memory bench: 1.63[secs]
Time to run computation of pi (2400 digits, 10 times): 3.12[secs]
Time to run computation of e (9009 digits): 3.38[secs]
```

Данная оптимизация проявила себя в реальных тестах, показав достаточно удивительные результаты. Так, при фактической скорости прямого интернет-соединения в среднем 190/190 Mbps скорость при использовании VPN WireGuard для системы Orbi оказалась выше, превышая скорость фактического соединения (198/196 Mbps).

Заключение

Методы оптимизации скорости VPN, рассмотренные выше, включены авторами в прошивку Voxel для маршрутизаторов NETGEAR R7500/R7800/R9000, Orbi RBK50, которая используется тысячами владельцев этих маршрутизаторов по всему миру, успешно конкурируя как с официальной прошивкой от NETGEAR, так и с другими альтернативными прошивками, и позволяет получить высокую скорость VPN-канала.

Литература

1. Crist E.F., Keijser J.J. Mastering OpenVPN. USA, Packt Publ., 2015, 364 p.
2. OpenVPN. URL: <https://openvpn.net/> (дата обращения: 18.04.2020).
3. GNU General Public License. URL: https://ru.wikipedia.org/wiki/GNU_General_Public_License (дата обращения: 19.04.2020).

4. Ristic I. *OpenSSL Cookbook*. UK, Feisty Duck Ltd Publ., 2013, 49 p.
5. Аграновский А.В., Хади Р.А. *Практическая криптография: алгоритмы и их программирование*. М.: СОЛОН-Р, 2009. 258 с.
6. Список архитектур ARM. URL: https://ru.wikipedia.org/wiki/Список_архитектур_ARM (дата обращения: 19.04.2020).
7. SIMD. URL: <https://ru.wikipedia.org/wiki/SIMD> (дата обращения: 19.04.2020).
8. ARM (архитектура). URL: [https://ru.wikipedia.org/wiki/ARM_\(архитектура\)](https://ru.wikipedia.org/wiki/ARM_(архитектура)) (дата обращения: 21.04.2020).
9. Krait (CPU). URL: [https://ru.wikipedia.org/wiki/Krait_\(CPU\)](https://ru.wikipedia.org/wiki/Krait_(CPU)) (дата обращения: 22.04.2020).
10. Столлингс В. *Криптография и защита сетей. Принципы и практика*. М.: Вильямс, 2001. 671 с.
11. RSA. URL: <https://ru.wikipedia.org/wiki/RSA> (дата обращения: 22.04.2020).
12. О проекте OpenWrt/LEDE. URL: <https://openwrt.org/ru/about> (дата обращения: 23.04.2020).
13. ARM Options. URL: <https://gcc.gnu.org/onlinedocs/gcc/ARM-Options.html> (дата обращения: 23.04.2020).
14. WireGuard. URL: <https://www.wireguard.com> (дата обращения: 24.04.2020).

Software & Systems
DOI: 10.15827/0236-235X.132.605-612

Received 12.05.20
2020, vol. 33, no. 4, pp. 605–612

Optimizing speed for VPN providing the possibility of telework using routers powered by ARM CPU

S.V. Andreev¹, *Researcher, esa@gin.keldysh.ru*
A.A. Khlopina¹, *Junior Researcher, nastya_75@mail.ru*

¹ Keldysh Institute of Applied Mathematics of RAS, Moscow, 125047, Russian Federation

Abstract. This paper devotes to the problems of optimizing VPN speed connections when using routers with ARM processors. In the current context, many enterprises and institutions around the world raise the urgent issue of ensuring access for employees, as well as a remote branch or unit, to the resources of the head office local area network. The paper discusses the possibility of connecting employees through an encrypted VPN channel using modern home routers using ARM processors. With this approach, all remote user devices are automatically connected to the local network resources of the head office, enterprise, and there are no needs for enterprise IT specialists to configure each of the user's device individually.

The paper considers a solution to a key problem of this approach, namely, ensuring the maximum speed of an encrypted VPN connection, and, therefore, accelerating the software components of routers included in its internal software (firmware) to provide a high-speed encrypted VPN connection. We consider the optimization of the speed of encryption and decryption algorithms using the features of the target processor of the device, such as parallelizing the execution of processor instructions using SIMD (Single Instruction, Multiple Data), general improvement of router performance when using optimal compiler options, non-traditional use of PCI hardware encryption devices, use of alternative options for modern private virtual networks (VPNs) for routers with a relatively low clock cycle frequency of the ARM central processor (CPU), but containing more than two cores, while providing VPN channel multithreading.

Keywords: remote assistance, routers, ARM architecture, computer calculations SIMD, extension of ARM instructions NEON, Virtual Private Network OpenVPN, OpenSSL protocol, AES algorithm of encryption, Virtual Private Network WireGuard.

References

1. Crist E.F., Keijser J.J. *Mastering OpenVPN*. USA, Packt Publ., 2015, 364 p.
2. *OpenVPN*. Available at: <https://openvpn.net/> (accessed April 18, 2020).
3. *GNU General Public License*. Available at: https://ru.wikipedia.org/wiki/GNU_General_Public_License (accessed April 19, 2020).
4. Ristic I. *OpenSSL Cookbook*. UK, Feisty Duck Ltd Publ., 2013, 49 p.
5. Agranovsky A.V., Hadi R.A. *Practical Cryptography: Algorithms and their Programming*. Moscow, 2009, 258 p. (in Russ.).

6. *List of ARM Architectures*. Available at: https://ru.wikipedia.org/wiki/Список_архитектур_ARM (accessed April 19, 2020).
7. *SIMD*. Available at: <https://ru.wikipedia.org/wiki/SIMD> (accessed April 19, 2020).
8. *ARM (Architecture)*. Available at: [https://ru.wikipedia.org/wiki/ARM_\(architecture\)](https://ru.wikipedia.org/wiki/ARM_(architecture)) (accessed April 21, 2020).
9. *Krait (CPU)*. Available at: [https://ru.wikipedia.org/wiki/Krait_\(CPU\)](https://ru.wikipedia.org/wiki/Krait_(CPU)) (accessed April 22, 2020).
10. Stallings V. *Cryptography and Network Protection. Principles and Practice*. Moscow, 2001, 671 p. (in Russ.).
11. *RSA*. Available at: <https://ru.wikipedia.org/wiki/RSA> (accessed April 22, 2020).
12. *About the OpenWrt/LEDE Project*. Available at: <https://openwrt.org/ru/about> (accessed April 23, 2020).
13. *ARM Options*. Available at: <https://gcc.gnu.org/onlinedocs/gcc/ARM-Options.html> (accessed April 23, 2020).
14. *WireGuard*. Available at: <https://www.wireguard.com> (accessed April 24, 2020).

Для цитирования

Андреев С.В., Хлупина А.А. Оптимизация скорости VPN для удаленной работы с использованием маршрутизаторов с ARM-процессорами // Программные продукты и системы. 2020. Т. 33. № 4. С. 605–612. DOI: 10.15827/0236-235X.132.605-612.

For citation

Andreev S.V., Khlopina A.A. Optimizing speed for VPN providing the possibility of telework using routers powered by ARM CPU. *Software & Systems*, 2020, vol. 33, no. 4, pp. 605–612 (in Russ.). DOI: 10.15827/0236-235X.132.605-612.