Рубрика 1. Информатика и информационные процессы

УДК *004.056.53*

В. С. Скоромников [1], А. П. Андрюхина [1]

[1]ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина»,г. Москва, Российская Федерация

ИССЛЕДОВАНИЕ РЕАЛИЗАЦИИ IPsec IKEv2 НА БАЗЕ vESR

Аннотация: Статья посвящена экспериментальному исследованию реализации протокола IPsec IKEv2 на платформе виртуального расширенного коммутатора маршрутизации vESR в условиях развёртывания виртуализированных сетей NFV/SDN. Актуальность работы обусловлена необходимостью обеспечения защищённого туннелирования между распределёнными сетевыми узлами при ограниченных вычислительных ресурсах виртуальной инфраструктуры. В качестве основной проблемы рассматривается влияние выбора криптографических алгоритмов и количества одновременно устанавливаемых туннелей на производительность, загрузку CPU и устойчивость работы управляющей плоскости vESR. В ходе исследования был развернут тестовый стенд, включающий виртуальный маршрутизатор vESR, пир с реализацией IPsec IKEv2 и генератор сетевой нагрузки. Для оценки производительности применялось нагрузочное тестирование с использованием различных криптографических профилей, включая AES-128, AES-256, режимы GCM и CBC. Дополнительно анализировалось поведение системы при увеличении количества одновременных IPsec-туннелей. Полученные результаты показали наличие выраженного компромисса между уровнем криптографической защиты и производительностью: более стойкие алгоритмы повышают нагрузку на процессор и снижают запас масштабируемости. Установлено, что при росте числа туннелей нагрузка на управляющую плоскость увеличивается нелинейно, что ограничивает стабильную работу системы. На основе результатов сформулированы практические рекомендации по выбору оптимальной конфигурации IPsec IKEv2 на платформе vESR для достижения баланса между безопасностью, функциональностью и эффективным использованием ресурсов. Ограничения интерпретации результатов связаны с единичными измерениями и конкретной конфигурацией виртуального стенда.

Ключевые слова: *IPsec IKEv2; vESR; NFV/SDN; нагрузочное тестирование; криптографический алгоритм; пропускная способность; загрузка CPU.*

Введение

Актуальность работы обусловлена необходимостью обеспечения безопасности туннелей между распределёнными узлами при переходе на виртуальные сетевые функции (NFV/SDN). vESR как виртуальный маршрутизатор является ключевым элементом таких сетей. Протокол IKEv2 в связке с IPsec является стандартным решением для защищённого туннелирования [1]. Архитектурные ограничения IPsec и практические рекомендации по развёртыванию учитывались по RFC 4301 и NIST SP 800-77 Rev. 1 [5, 7].

Основные исследования IPsec и IKEv2 направлены на криптостойкость и производительность. Проблемы интеграции с виртуализацией изучены поверхностно.

Известны: архитектура IKEv2, методы оптимизации для аппаратного ускорения, базовые реализации в ПО (StrongSwan) [2]. Неизученным остаётся поведение и производительность стека IPsec IKEv2 на платформе vESR в условиях ограничения ресурсов ВМ.

Объектом исследования является обеспечение информационной безопасности в виртуализированных сетях передачи данных с использованием протоколов защищённого туннелирования.

Предмет исследования заключается в реализации и функционировании протокола обмена ключами IKEv2 в составе стека IPsec на программной платформе виртуального расширенного коммутатора маршрутизации (vESR).

Цель исследования – провести комплексное исследование реализации IPsec IKEv2 на платформе vESR, оценить её производительность и безопасность, а также разработать оптимизированные профили конфигурации для типовых сценариев развёртывания [4].

Методы исследования

Исследование является прикладным экспериментальным исследованием с элементами нагрузочного тестирования (бенчмаркинга). Цель – эмпирическая оценка производительности и поведения конкретной системы (IPsec IKEv2 на vESR) в контролируемых условиях.

К характеристикам сбора данных относятся vESR 8.2 (2 vCPU, 4 ГБ RAM, интерфейс eth1: 192.168.10.1/24). Пир (StrongSwan 5.9) с аналогичными ресурсами (eth1: 192.168.10.2/24). Генератор нагрузки (Ubuntu 22.04) с iperf3.

Для сравнения и формирования туннелей используются заранее подготовленные и настроенные образы виртуальных роутеров (например, на базе StrongSwan/Libreswan или другого vESR), выступающие в роли пиров (равноправных узлов).

Тестовая нагрузка. Сгенерированный сетевой трафик (TCP/UDP потоки) с использованием инструмента iperf3.

Мониторинг ресурсов для сбора данных. Сбор метрик потребления ресурсов vESR (загрузка CPU по ядрам, потребление оперативной памяти) средствами гипервизора (например, virt-top) и встроенными утилитами самой vESR.

Настройка первой фазы протокола IKEv2 (см. Приложение А).

Первая фаза отвечает за установление защищённого управляющего канала между маршрутизаторами. В рамках данной фазы были заданы следующие параметры:

- версия протокола: IKEv2;
- алгоритм шифрования: AES-256;
- алгоритм хэширования: SHA-256;
- метод аутентификации: Pre-Shared Key (PSK);
- время жизни ассоциации безопасности (SA).

Для аутентификации узлов в процессе установления IKE-соединения был использован метод предварительно распределенного ключа (Pre-Shared Key). Одинаковый ключ был задан на обоих виртуальных маршрутизаторах, что позволило успешно пройти процедуру взаимной аутентификации.

Настройка второй фазы протокола IKEv2 (см. Приложение В).

После успешной настройки первой фазы была выполнена настройка второй фазы IPsec, предназначенной для защиты пользовательского трафика.

В рамках Phase 2 были определены:

- протокол защиты: ESP (Encapsulating Security Payload); Выбор AES-GCM и AES-CBC сопоставлялся с актуальными требованиями к алгоритмам ESP [6].
- алгоритм шифрования данных: AES-256;
- алгоритм контроля целостности: SHA-256;
- параметры времени жизни IPsec-ассоциации.

На следующем этапе созданная IPsec-политика была привязана к соответствующему интерфейсу виртуального маршрутизатора. После применения политики инициировался процесс установления IPsec-туннеля между узлами. В результате была сформирована защищённая логическая связь между двумя удаленными локальными сетями.

Проверка состояния ассоциаций безопасности

На завершающем этапе была выполнена проверка состояния ассоциаций безопасности IKE и IPsec. Были получены таблицы IKE SA и IPsec SA, подтверждающие, что обе фазы протокола успешно установлены и находятся в активном состоянии.

Активное состояние IKE SA и IPsec SA подтверждено командами платформы; в таблице 1 приведён фрагмент захвата ESP и сопутствующего служебного трафика.

Таблица 1 – Фрагмент захвата ESP и сопутствующего служебного трафика в Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
18	39.219728	101.1.1.2	101.1.1.2	ESP	182	ESP (SPI=0x0d830193)
20	39.226789	101.1.1.2	101.1.1.2	ESP	182	ESP (SPI=0x0d830193)
21	39.231723	101.1.1.2	101.1.1.2	ESP	182	ESP (SPI=0x0d830193)

22	39.237195	101.1.1.2	101.1.1.2	ESP	182	ESP (SPI=0x0d830193)
24	39.247124	101.1.1.2	101.1.1.2	ESP	182	ESP (SPI=0x0d830193)
25	39.248372	101.1.1.2	101.1.1.2	ESP	182	ESP (SPI=0x0d830193)
26	39.254083	101.1.1.2	101.1.1.2	ESP	182	ESP (SPI=0x0d830193)
27	39.259122	101.1.1.2	101.1.1.2	ESP	182	ESP (SPI=0x0d830193)
28	39.266499	101.1.1.2	101.1.1.2	ESP	182	ESP (SPI=0x0d830193)
30	39.273128	101.1.1.2	101.1.1.2	ESP	182	ESP (SPI=0x0d830193)
31	39.280137	101.1.1.2	101.1.1.2	ESP	182	ESP (SPI=0x0d830193)
32	39.285124	101.1.1.2	101.1.1.2	ESP	182	ESP (SPI=0x0d830193)
33	39.286452	101.1.1.2	101.1.1.2	ESP	182	ESP (SPI=0x0d830193)
34	40.017135	aa:bb:cc:00:10:10	aa:bb:cc:00:10:10	LOOP	60	Reply
35	40.973158	aa:bb:cc:00:10:10	224.0.0.5	OSPF	90	Hello Packet
36	40.172154	aa:bb:cc:00:10:10	aa:bb:cc:00:10:10	CDP/VTP/DTP/ PAgP/UDLD	254	Device ID: ESPI - Port ID: Ethernet0/1
37	40.193640	aa:bb:cc:00:10:10	aa:bb:cc:00:10:10	LOOP	60	Reply
38	40.624894	aa:bb:cc:00:10:10	aa:bb:cc:00:10:10	LOOP	60	Reply

Методы обработки данных

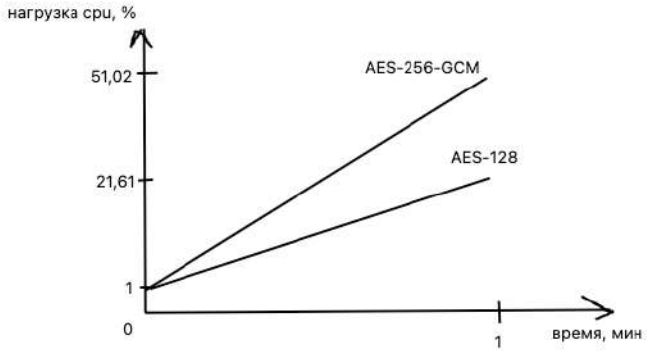

Рис. 1. Тест производительности AES-128 и AES-256-GCM

Результаты сравнения AES-128 и AES-256-GCM представлены в таблице 2.

Таблица 2 – Сравнительная таблица AES-128 vs AES-256-GCM

Параметр	AES-128	AES-256-GCM
Длина ключа	128 бит	256 бит
Тип режима	Обычный блочный (CBC/ECB)	AEAD (шифр + аутентификация)
Защита целостности	SHA2-256	Да (128-битный тег)

Устойчивость к анализу гистограммы	Средняя (зависит от режима, ECB уязвим)	Высокая — структура полностью скрыта
Производительность	• Загрузка CPU: 21,61 % • Средний RTT: 0,431 ms • Потери: 0%	• Загрузка CPU: 51,02 % • Средний RTT: 0,523 ms • Потери: 0%
Устойчивость к перебору	2^{128}	2^{256}
Применение	Устаревающие системы	Современные протоколы (TLS 1.3, IPsec)

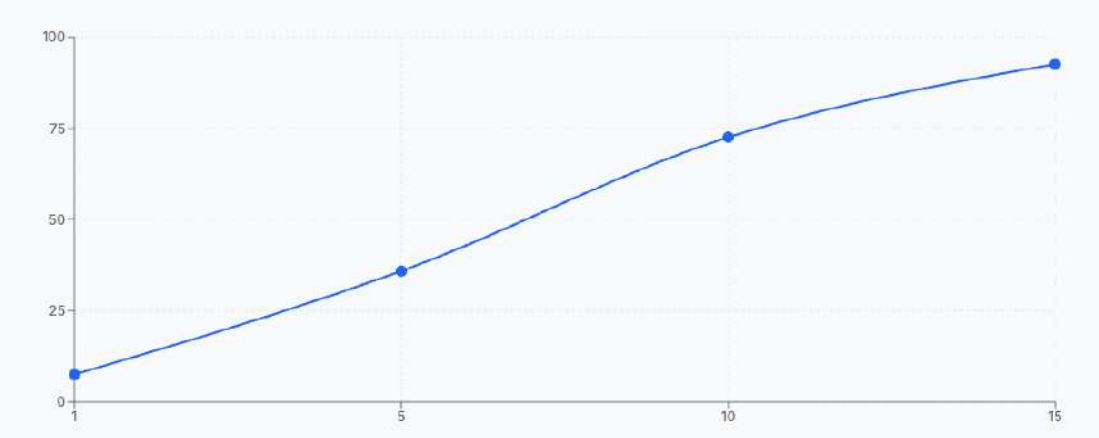

Рис. 2. Загрузка CPU (1, 5, 10, 15 туннелей)

Результаты тестирования производительности путем изменения количества туннелей представлены в таблице 3.

Таблица 3 – Влияние количества одновременных туннелей на производительность vESR

Кол-во туннелей	Загрузка CPU (управляющая плоскость, %)	Потребление памяти (MB)	Скорость установления (тунн./сек)
1	7,55	122	-
5	35,88	207	3,5
10	72,58	267	2,8
15	92,58	380	1,4

Обсуждение результатов

В рамках исследования была проведена комплексная экспериментальная оценка реализации стека IPsec IKEv2 на платформе виртуального расширенного коммутатора маршрутизации (vESR). Методология включала нагрузочное тестирование и сравнительный анализ различных криптографических алгоритмов (AES-128, AES-256, GCM, CBC). На специально развернутом стенде оценивались загрузка центрального процессора, RTT, потери и скорость установления туннелей; отдельная сводная метрика пропускной способности в представленные таблицы не включена.

1. Влияние алгоритмов шифрования. Единичные замеры CPU, RTT и потерь показывают различия между сравниваемыми профилями, однако не позволяют утверждать о статистически значимом снижении пропускной способности на 25 %, поскольку throughput, число повторов и разброс не приведены. В условиях данного стенда профиль AES-128 показал меньшую нагрузку CPU, чем AES-256-GCM; результат следует считать предварительным из-за одновременного изменения длины ключа и режима шифрования.

2. Масштабируемость и нагрузка на управляющую плоскость. Данные (Таблица 3) выявили нелинейную зависимость нагрузки от числа туннелей. Рост количества одновременных подключений с 1 до 15 приводит к увеличению загрузки CPU управляющей плоскости с 7,55% до 92,58%, а скорость установления новых туннелей падает с 3,5 до 1,4 тунн./сек.

3. Определение оптимальной конфигурации. На основе эмпирических данных была подтверждена гипотеза о существовании специфичной для vESR оптимальной конфигурации. Результаты показывают, что для достижения баланса между безопасностью, функциональностью и эффективным использованием ресурсов необходимо сместить выбор в сторону менее ресурсоёмких, но современных алгоритмов и жестко ограничивать масштабирование.

Заключение

Проведенное исследование позволило подтвердить ключевые гипотезы и сформулировать следующие выводы и рекомендации для практического применения IPsec IKEv2 на платформе vESR:

1. Существует выраженный компромисс между уровнем безопасности и производительностью. В условиях ограниченных виртуальных ресурсов (2 vCPU, 4 ГБ RAM) использование алгоритма AES-128-GCM является оптимальным для большинства стандартных сценариев.

2. Критическим параметром для стабильности системы является нагрузка на управляющую плоскость. Во избежание деградации сервиса и чрезмерных задержек рекомендуется ограничивать количество одновременных туннелей таким образом, чтобы устойчивая загрузка CPU не превышала 80-85%, что для тестового стенда соответствует приблизительно 10 туннелям.

3. Сформулированная оптимальная конфигурация (AES-128-GCM, группа Диффи-Хеллмана 19/14, контроль числа туннелей) обеспечивает разумный баланс, отличный от подходов, применяемых для аппаратных маршрутизаторов.

Направление дальнейших исследований:

1. Оценка влияния аппаратного ускорения шифрования (AES-NI) на производительность и поведение системы при миграции ВМ между хостами.

2. Анализ отказоустойчивости и времени переключения (failover) IPsec-туннелей в кластерных конфигурациях vESR.

3. Исследование безопасности реализации IKEv2 на vESR методами фаззинга для выявления потенциальных уязвимостей.

Библиографический список

1. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EcoRouter в рамках специальности 09.02.06 "Сетевое и системное администрирование". Вопросы импортозамещения и подготовки квалифицированных кадров в сетевом оборудовании / А. Г. Уймин, И. М. Толмачев // Автоматизация и информатизация ТЭК. – 2025. – № 11(628). – С. 58–62. – EDN DMHQJU.
2. Kaufman, C. Internet Key Exchange Protocol Version 2 (IKEv2) [Электронный ресурс] : RFC 7296 / C. Kaufman, P. Hoffman, Y. Nir [и др.]. – IETF, 2014. – URL: https://datatracker.ietf.org/doc/html/rfc7296 (дата обращения: 12.12.2025).
3. Nir, Y. IPsec Cluster Problem Statement [Электронный ресурс] : RFC 6027 / Y. Nir. – IETF, 2010. – URL: https://datatracker.ietf.org/doc/html/rfc6027 (дата обращения: 12.12.2025).
4. Sheffer, Y. Additional EAP Methods for IKEv2 [Электронный ресурс] : RFC 5106 / Y. Sheffer, S. Fluhrer. – IETF, 2008. – URL: https://datatracker.ietf.org/doc/html/rfc5106 (дата обращения: 12.12.2025).
5. Kent, S. Security Architecture for the Internet Protocol [Электронный ресурс] : RFC 4301 / S. Kent, K. Seo. – IETF, 2005. – URL: https://www.rfc-editor.org/rfc/rfc4301.html (дата обращения: 31.03.2025).
6. Wouters, P. Cryptographic Algorithm Implementation Requirements and Usage Guidance for ESP and AH [Электронный ресурс] : RFC 8221 / P. Wouters, D. Migault, J. Mattsson, Y. Nir, T. Kivinen. – IETF, 2017. – URL: https://www.rfc-editor.org/rfc/rfc8221.html (дата обращения: 31.03.2025).
7. Barker, E. Guide to IPsec VPNs [Электронный ресурс] : NIST SP 800-77 Rev. 1 / E. Barker, Q. Dang, S. Frankel, K. Scarfone, P. Wouters. – NIST, 2020. – DOI: 10.6028/NIST.SP.800-77r1 (дата обращения: 31.03.2025).

References

1. Uymin, A. G. The use of domestic Eltex and EcoRouter network equipment in the framework of specialty 09.02.06 "Network and system administration". Issues of import substitution and training of qualified personnel in network equipment / A. G. Uymin, I. M. Tolmachev // Automation and informatization of the fuel and energy complex. – 2025. – № 11(628). – Pp. 58-62. – EDN DMHQJU.
2. Kaufman, C. Internet Key Exchange Protocol Version 2 (IKEv2) [Electronic resource] : RFC 7296 / C. Kaufman, P. Hoffman, Y. Nir [et al.]. – IETF, 2014. – URL: https://datatracker.ietf.org/doc/html/rfc7296 (date of request: 12.12.2025).
3. Nir, Y. IPsec Cluster Problem Statement [Electronic resource] : RFC 6027 / Y. Nir. – IETF, 2010. – URL: https://datatracker.ietf.org/doc/html/rfc6027 (date of request: 12.12.2025).
4. Sheffer, Y. Additional EAP Methods for IKEv2 [Electronic resource] : RFC 5106 / Y. Sheffer, S. Fluhrer. – IETF, 2008. – URL: https://datatracker.ietf.org/doc/html/rfc5106 (date of request: 12.12.2025).
5. Kent, S., & Seo, K. (2005). Security architecture for the Internet Protocol (RFC 4301). IETF. https://www.rfc-editor.org/rfc/rfc4301.html
6. Wouters, P., Migault, D., Mattsson, J., Nir, Y., & Kivinen, T. (2017). Cryptographic algorithm implementation requirements and usage guidance for ESP and AH (RFC 8221). IETF. https://www.rfc-editor.org/rfc/rfc8221.html
7. Barker, E., Dang, Q., Frankel, S., Scarfone, K., & Wouters, P. (2020). Guide to IPsec VPNs (NIST SP 800-77 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-77r1

Информация об авторах

Скоромников Виталий Сергеевич — студент 2-го курса, группы КА-24-06 Факультета КБ ТЭК, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: skoromnikov.vita@yandex.ru

Андрюхина Анастасия Павловна — студентка 2-го курса, группы КА-24-06 Факультета КБ ТЭК, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: Anastashia33@yandex.ru

INVESTIGATION OF IPsec IKEv2 IMPLEMENTATION BASED ON vESR

V. S. Skoromnikov[1], A. P. Andryukhina[1]

[1]National University of Oil and Gas «Gubkin University»

Abstract. The article presents an experimental study of the IPsec IKEv2 protocol implementation on the virtual extended routing switch platform, vESR, in the context of NFV/SDN-based virtualized network deployment. The relevance of the study is determined by the need to provide secure tunneling between distributed network nodes under the limited computing resources of a virtual infrastructure. The main research problem is the influence of cryptographic algorithm selection and the number of simultaneously established tunnels on throughput, CPU utilization, and the stability of the vESR control plane. During the study, a test environment was deployed, including a vESR virtual router, a peer node with IPsec IKEv2 support, and a network traffic generator. Load testing was used to evaluate performance under different cryptographic profiles, including AES-128, AES-256, GCM, and CBC modes. The behavior of the system was also analyzed when the number of simultaneous IPsec tunnels was increased. The obtained results demonstrated a significant trade-off between cryptographic strength and performance: stronger algorithms increase CPU load and reduce scalability margins. It was found that the control plane load grows nonlinearly as the number of tunnels increases, which limits stable system operation. Based on the experimental data, practical recommendations are proposed for selecting an optimal IPsec IKEv2 configuration on the vESR platform in order to balance security requirements, functionality, and efficient resource utilization.

Keywords: IPsec IKEv2; vESR; NFV/SDN; load testing; cryptographic algorithm; bandwidth; CPU utilization.

Information about the authors

Skoromnikov Vitaly Sergeevich — 2nd year student of the KA-24-06 group of the Faculty of the Fuel and Energy Complex Design Bureau, Gubkin Russian State University of Oil and Gas (NRU), Moscow, e-mail: skoromnikov.vita@yandex.ru

Andryukhina Anastasia Pavlovna — student of the 2nd year, group KA-24-06 Faculty of the Fuel and Energy Complex Design Bureau, Gubkin Russian State University of Oil and Gas (NRU), Moscow, e-mail: Anastashia33@yandex.ru