УДК 004.724.2, 004.056.55

Симбирцев Е.А.
Студент
РГУ нефти и газа (НИУ) имени И. М. Губкина
Россия, г. Москва

ТЕСТИРОВАНИЕ РАБОТЫ ПРОТОКОЛА IKEv2 ПОВЕРХ UDP НА БАЗЕ ОТЕЧЕСТВЕННОГО МАРШРУТИЗАТОРА ECOROUTER

Аннотация. *В статье рассматривается проблема совместимости протокола IPsec с устройствами трансляции сетевых адресов и практическая реализация механизма обхода NAT (NAT Traversal, NAT-T) на базе отечественной платформы EcoRouter под управлением операционной системы EcoOS. Проводится сравнительный анализ VPN-протоколов с точки зрения NAT-совместимости. Описывается архитектура тестового стенда на базе виртуальных образов EcoRouter и особенности настройки туннеля IKEv2/IPsec через промежуточный NAT-маршрутизатор. Приводится методика проведения нагрузочного тестирования и оценки накладных расходов*

Ключевые слова: *IKEv2, IPsec, NAT Traversal, EcoRouter, ESP, UDP, VPN, пропускная способность.*

Simbirtsev E.A.
Student
National University of Oil and Gas «Gubkin University»,
Russian Federation, Moscow

TESTING IKEv2 PROTOCOL OVER UDP BASED ON ROUTER ECOROUTER

Abstract. *This paper examines the compatibility issue of the IPsec protocol with network address translation devices and the practical implementation of the NAT Traversal mechanism on the domestic EcoRouter platform running the EcoOS operating system. A comparative analysis of VPN protocols in terms of NAT compatibility is conducted. The architecture of the test environment based on EcoRouter virtual instances is described, along with the configuration specifics of an IKEv2/IPsec tunnel through an intermediate NAT router. The methodology for load testing and encapsulation overhead evaluation is presented.*

Keywords: *IKEv2, IPsec, NAT Traversal, EcoRouter, ESP, UDP, VPN, throughput.*

Введение

Обеспечение защищенной передачи данных между территориально распределенными сегментами корпоративных сетей является одной из ключевых задач сетевой инженерии. Стек протоколов IPsec, включающий протокол обмена ключами IKEv2 (RFC 7296) [1] и протокол инкапсуляции полезной нагрузки ESP (RFC 4303) [2], занимает лидирующее положение среди стандартизированных решений для построения виртуальных частных сетей (VPN). Вместе с тем практическое развертывание IPsec в реальных инфраструктурах сопряжено с фундаментальной проблемой: классический протокол ESP несовместим с механизмом трансляции сетевых адресов (NAT), повсеместно применяемым в современных сетях.

ESP функционирует как самостоятельный IP-протокол с номером 50, не имея полей транспортных портов (PAT). Устройства NAT, осуществляющие трансляцию на уровне портов, не способны построить корректные таблицы трансляций для такого трафика, что делает невозможным подъем туннеля в сценариях с промежуточным NAT. Стандарт NAT Traversal (NAT-T), описанный в RFC 3947 [3] и RFC 3948

[4], решает данную проблему посредством инкапсуляции ESP-пакетов в UDP-дейтаграммы с портом 4500, предоставляя NAT-устройствам знакомые транспортные идентификаторы.

В контексте политики импортозамещения в Российской Федерации [5] все большую актуальность приобретает вопрос поддержки стандартных протоколов безопасности на отечественном сетевом оборудовании. Платформа EcoRouter, включенная в Реестр российского программного обеспечения и позиционируемая как замена зарубежным решениям класса enterprise, декларирует поддержку IKEv2/IPsec. Однако практические характеристики реализации NAT-T на данной платформе в открытой литературе не представлены [6].

Цель данной работы – экспериментально верифицировать корректность реализации механизма NAT-T на платформе EcoRouter и количественно оценить накладные расходы UDP-инкапсуляции на пропускную способность защищенного канала

Анализ VPN-протоколов в контексте NAT-совместимости

Для построения защищенных каналов применяется несколько семейств протоколов. Они различаются уровнем модели OSI, методом аутентификации, производительностью и поведением при прохождении через NAT.

IPsec/IKEv2 относится к протоколам сетевого уровня. ESP инкапсулируется непосредственно в IP, что дает высокую производительность, но создает несовместимость с PAT: NAT-устройство не может транслировать пакеты без портов. Проблема устранена механизмом NAT-T за счет добавления UDP-заголовка.

OpenVPN и SSL VPN работают поверх TCP или UDP на транспортном уровне. NAT-совместимость у них высокая, поскольку устройства трансляции видят обычный UDP или TCP. Ценой является

дополнительный overhead от двойной инкапсуляции и отсутствие единого стандарта IETF.

WireGuard использует UDP с фиксированным портом. Встроенный keepalive поддерживает NAT-сессию активной. Ключевым ограничением для корпоративного сегмента остается отсутствие завершенной стандартизации IETF и поддержки EAP-аутентификации для интеграции с корпоративными каталогами.

IPsec/IKEv2 является единственным протоколом из рассмотренных, несущим измеримые накладные расходы при обходе NAT. Сравнение протоколов приведено в таблице 1.

Таблица 1 – Сравнение VPN-протоколов по NAT-совместимости

Протокол	Проблема с NAT	Механизм обхода	Overhead	Стандарт
IPsec/IKEv2	ESP не имеет портов, PAT невозможен	NAT-T: UDP-инкапсуляция ESP на порту 4500	+8 байт/пакет	RFC 3947, 3948
L2TP/IPsec	Та же проблема ESP в финальном стеке	NAT-T (аналогично IKEv2)	+8 байт/пакет	RFC 3193
OpenVPN	Нет – изначально UDP/TCP	Нативный UDP/TCP-транспорт	Мин.	–
WireGuard	Нет – нативный UDP	Нативный UDP + keepalive	Мин.	–
SSL VPN	Нет – поверх TLS/TCP	Нативный TLS/TCP-транспорт	Средний	–

Протокол IKEv2 и механизм NAT Traversal

Протокол IKEv2, определенный в RFC 7296, обеспечивает согласование параметров и управление криптографическими ассоциациями (Security Association, SA) для стека IPsec. Установление защищенного соединения включает две обязательные фазы.

Фаза IKE_SA_INIT выполняется в открытом виде и решает три задачи: согласование криптографических алгоритмов (proposal), обмен открытыми ключами по алгоритму Диффи-Хеллмана и обнаружение присутствия NAT на пути. Для обнаружения NAT каждая сторона

добавляет в сообщение уведомления NAT_DETECTION_SOURCE_IP и NAT_DETECTION_DESTINATION_IP, содержащие SHA-1-хэши от IP-адресов и UDP-портов. Несовпадение хэшей у получателя сигнализирует о наличии промежуточного NAT-устройства.

При подтверждении наличия NAT стороны автоматически выполняют два переключения: управляющие IKE-сообщения переходят с UDP/500 на UDP/4500, а исходящие ESP-пакеты начинают инкапсулироваться в UDP с портом назначения 4500. Для разграничения IKE и ESP на одном порту IKE-сообщения предваряются 4-байтным нулевым маркером (Non-ESP Marker). Дополнительно активируется механизм NAT-keepalive – периодическая отправка пустых UDP-пакетов (типично каждые 20 с) для предотвращения удаления записей из PAT-таблицы провайдера.

Фаза IKE_AUTH, защищенная ключами из IKE_SA_INIT, выполняет взаимную аутентификацию сторон (в данном исследовании – PSK) и создает первый Child SA, непосредственно защищающий пользовательский трафик протоколом ESP с алгоритмами AES-256/SHA-256.

Структура пакета после применения NAT-T: *[IP] + [UDP src:4500, dst:4500] + [ESP SPI, Seq] + [зашифрованный IP-пакет]*. Дополнительный UDP-заголовок занимает 8 байт, что при стандартном MTU 1500 байт требует уменьшения MSS для предотвращения фрагментации, рассчитываемого по формуле (1):

$$MSS_{opt} = MTU – IP_{outer} – UDP – ESP – IP_{inner} \quad (1)$$

Описание тестового стенда и настройка туннеля

В состав стенда входят два маршрутизатора EcoRouter с EcoOS версии 3.2.6.2, два хоста ALT Linux и промежуточный узел с настроенным MASQUERADE, имитирующий NAT. Маршрутизатор ER1 подключен к подсети 172.16.0.0/24, ER2 – к подсети 172.16.1.0/24, между ними

расположен NAT-узел. Физическая реализация сети представлена в таблице 2.

Таблица 2 – Физическая реализация стенда

Характеристика	Маршрутизатор	Сервер-коллектор	Клиент
Операционная система	EcoRouter	ALT Linux	ALT Linux
Процессор	4 ядра	1 ядро	1 ядро
Оперативная память	4 ГБ	1 ГБ	1 ГБ
Дисковое пространство	6 ГБ	30 ГБ	30 ГБ
Сетевые адаптеры	2 интерфейса	3 интерфейса	1 интерфейс
Используемое ПО	–	tcpdump	iperf3, wireshark

Настройка выполнялась в четыре шага на каждом маршрутизаторе. Сначала создается криптопрофиль CIPROFILE0: для первой фазы задан AES-256 с хешированием SHA-256 и группой DH 14, для второй определен протокол ESP и селекторы трафика. Далее создается криптокарта, связывающая профиль с адресом удаленного узла. Затем настраивается filter-map с тремя правилами: правило 10 направляет трафик между подсетями в криптомодуль, правило 20 обрабатывает UDP-пакеты на порту 4500, правило 30 разрешает остальной трафик. На последнем шаге filter-map привязывается к физическим интерфейсам. После завершения настройки show crypto ikev2 sa отобразила статус SA как UP с портом 4500.

Проведение нагрузочного тестирования и анализ результатов

Для нагрузочного тестирования применялась утилита iPerf3 [7]. Каждый сценарий тестировался в пяти независимых прогонах продолжительностью 10 секунд с интервалом 5 секунд между ними.

Командная строка инициатора: iperf3 -c 172.16.1.1 -p 5201 -t 10 -P 1 -M 1300.

Командная строка ответчика: iperf3 -s -p 5201

Верификация NAT-T выполнялась посредством перехвата трафика утилитой tcpdump на транзитном хосте с последующим анализом в

Wireshark. Состояние SA контролировалось командами show crypto ikev2 sa и show crypto ipsec sa.

Формула для расчета overhead (2):

Overhead (%) = (1 – Bitrate_IPsec / Bitrate_open) × 100 %

(2)

На первом этапе измерялась пропускная способность открытого канала без шифрования. На втором после поднятия туннеля проводились аналогичные измерения внутри защищенного канала с флагом -M 1300.

Оптимальный MSS рассчитывается по формуле (1) вычитания заголовков из физического MTU:

MSS_opt = 1500 – IP_outer – UDP – ESP – IP_inner = 1500 – 20 – 8 – 8 – 20 = 1444 байт

Значение 1300 байт выбрано с запасом на выравнивание AES-блоков и ESP-трейлер. Каждый сценарий тестировался в пяти прогонах по 10 секунд. Результаты приведены в таблице 3.

Таблица 3 – Результаты нагрузочного тестирования

Прогон	Открытый канал, Мбит/с	Защищенный канал, Мбит/с
test 1	371	299
test 2	379	292
test 3	386	283
test 4	379	290
test 5	361	279
Среднее	375,5	288,6

Накладные расходы инкапсуляции рассчитаны по формуле (2):

Overhead = (1 – Bitrate_IPsec / Bitrate_open) × 100% = (1 – 288,6 / 375,5) × 100% = 23,1%

Для большей наглядности на рисунке 2 приведена столбчатая диаграмма, в которой синий столбец показывает полезную пропускную способность открытого канала (375,5 Мбит/с) и защищенного канала

(288,6 Мбит/с), а красный столбец наглядно отображает «съеденные» overhead’ом 86,9 Мбит/с, что составляет примерно 23,1%.

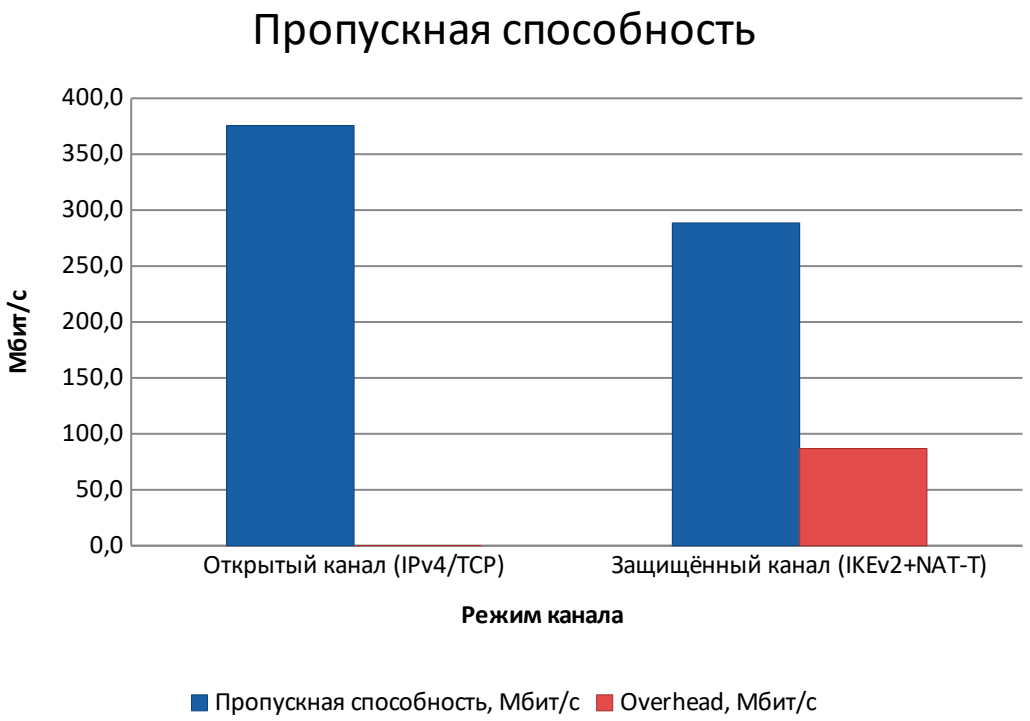

Рисунок 2. Столбчатая диаграмма пропускной способности

Снижение пропускной способности на 23,1% объясняется двумя факторами: криптографическими операциями AES-256 и SHA-256 для каждого пакета и добавлением заголовков ESP и UDP 4500, уменьшающих долю полезной нагрузки. Количество повторных передач во всех пяти прогонах равно нулю.

Дамп трафика в Wireshark подтвердил работу NAT-T. На внешнем интерфейсе вместо протокола ESP с номером 50 фиксируется UDP с портами 4500. Внутри UDP-дейтаграммы присутствует секция Encapsulating Security Payload. Адреса подсетей 172.16.x.x и порты iPerf3 в пакете не видны.

Заключение

В настоящей статье исследована проблема прохождения IPsec через NAT и проведена практическая проверка механизма NAT-T на платформе EcoRouter. Сравнительный анализ показал, что IPsec/IKEv2 –

единственный стандартизированный протокол с измеримыми накладными расходами при обходе NAT.

Нагрузочное тестирование зафиксировало снижение пропускной способности на 23,1% при переходе к защищенному IKEv2-туннелю с NAT-T. При MSS 1300 байт потери пакетов отсутствуют. Дамп трафика подтвердил переключение на UDP 4500 и скрытие внутренней топологии. EcoRouter корректно реализует механизм NAT Traversal в соответствии с RFC 3947 и RFC 3948. Полученные результаты применимы при проектировании IPsec-инфраструктуры на отечественном оборудовании.

Список источников

1. RFC 7296. Internet Key Exchange Protocol Version 2 (IKEv2) / C. Kaufman [и др.]. – IETF, 2014. – URL: https://datatracker.ietf.org/doc/html/rfc7296 (дата обращения: 09.05.2026).
2. RFC 4303. IP Encapsulating Security Payload (ESP) / S. Kent. – IETF, 2005. – URL: https://datatracker.ietf.org/doc/html/rfc4303 (дата обращения: 09.05.2026).
3. RFC 3947. Negotiation of NAT-Traversal in the IKE / T. Kivinen [и др.]. – IETF, 2005. – URL: https://datatracker.ietf.org/doc/html/rfc3947 (дата обращения: 09.05.2026).
4. RFC 3948. UDP Encapsulation of IPsec ESP Packets / A. Huttunen [и др.]. – IETF, 2005. – URL: https://datatracker.ietf.org/doc/html/rfc3948 (дата обращения: 09.05.2026).
5. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – URL: http://publication.pravo.gov.ru/Document/View/0001201707260008 (дата обращения: 09.05.2026).

6. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EcoRouter в рамках специальности 09.02.06 / А. Г. Уймин, И. М. Толмачев // Автоматизация и информатизация ТЭК. – 2025. – № 11(628). – С. 58–62. – EDN DMHQJU.
7. iPerf3: A TCP, UDP, and SCTP network bandwidth measurement tool [Электронный ресурс]. – URL: https://iperf.fr/ (дата обращения: 09.05.2026).
8. Калинин, М. Безопасность сетевого уровня в IP-сетях / М. Калинин, Н. В. Тутова // Архивариус. – 2020. – № 1(46). – URL: https://cyberleninka.ru/article/n/bezopasnost-setevogo-urovnya-v-ip-setyah (дата обращения: 09.05.2026).
9. RFC 4301. Security Architecture for the Internet Protocol / S. Kent, K. Seo. – IETF, 2005. – URL: https://datatracker.ietf.org/doc/html/rfc4301 (дата обращения: 09.05.2026).
10. EcoRouter OS. Руководство по установке и конфигурированию [Электронный ресурс]. – URL: https://docs.ecorouter.ru/EcoRouter-UserGuide.pdf (дата обращения: 09.05.2026).
11. Столлингс, В. Криптография и защита сетей: принципы и практика / В. Столлингс. – М.: Вильямс, 2019. – 1120 с. – ISBN 978-5-907144-01-1.
12. Уймин, А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 / А. Г. Уймин. – СПб.: Лань, 2020. – 480 с. – ISBN 978-5-8114-5519-5.