

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОДУКТИВНОСТІ ТУНЕЛЬНИХ ПРОТОКОЛІВ OPENVPN ТА WIREGUARD У ВІРТУАЛІЗОВАНИХ СЕРЕДОВИЩАХ

Анотація. У роботі представлено результати експериментального дослідження ефективності VPN-протоколів у хмарній інфраструктурі KVM. Показано, що WireGuard забезпечує приріст продуктивності у 5.1 рази порівняно з OpenVPN. Така істотна різниця зумовлена відсутністю накладних витрат на перемикання контексту та ефективною багатопотоковістю у просторі ядра, тоді як OpenVPN обмежений одним ядром.

Abstract. The paper presents the results of an experimental study on the efficiency of VPN protocols in KVM cloud infrastructure. It was demonstrated that WireGuard provides a 5.1x performance increase compared to OpenVPN. This significant difference is due to the elimination of context-switching overhead and efficient kernel-space multithreading, whereas OpenVPN is limited to a single core.

Вступ. Масовий перехід до хмарних обчислень та віртуалізації мережесих функцій (NFV) висуває нові вимоги до захищених каналів зв'язку. Традиційні рішення, такі як OpenVPN, стикаються з проблемою продуктивності на високошвидкісних каналах (1 Гбіт/с і вище). Актуальність дослідження зумовлена тим, що протоколи, які працюють у просторі користувача (User Space), створюють значне навантаження на процесор через накладні витрати на перемикання контексту. Це стає «вузьким місцем» у віртуалізованих середовищах. Метою роботи є експериментальне порівняння ефективності OpenVPN та WireGuard на платформі Linux KVM.

Методика дослідження. Для експерименту розгорнуто тестовий стенд із двох віртуальних машин (Клієнт та Сервер) під управлінням Ubuntu Server 24.04. Використано гіпервізор KVM/QEMU з драйверами VirtIO. Конфігурація вузлів: 2 vCPU, 2 ГБ RAM. Вимірювання пропускної здатності проводилося утилітою iperf3 (TCP, 30 с), моніторинг CPU — через htop. Дослідження включало три етапи: вимірювання еталонної швидкості (Baseline), тестування OpenVPN (UDP, AES-256-GCM) та тестування WireGuard (Kernel module, ChaCha20-Poly1305).

Результати. Еталонна пропускна здатність віртуального каналу склала 16.5 Гбіт/с при завантаженні одного ядра CPU на 96%. При використанні OpenVPN швидкість впала до 538 Мбіт/с (3.3% від еталону). Процес OpenVPN повністю завантажив одне ядро (96.2%), залишивши інше

незадіяним. Це підтверджує неефективність однопотокової архітектури в User Space для гігабітних каналів. Протокол WireGuard продемонстрував швидкість 2.76 Гбіт/с, що у 5.1 рази перевищує показники OpenVPN. Навантаження на процесор розподілилося рівномірно між обома ядрами. Висока ефективність досягнута завдяки інтеграції в ядро Linux (Zero-Copy) та ефективній роботі з механізмами розвантаження сегментації (GSO) драйверів VirtIO.

Висновки. Дослідження підтвердило перевагу WireGuard над OpenVPN. Архітектура WireGuard дозволяє уникнути накладних витрат на перемикання контексту, забезпечуючи 5-кратний приріст швидкості. OpenVPN у класичній конфігурації є неефективним для каналів >500 Мбіт/с. Рекомендується перехід на WireGuard для оптимізації хмарної інфраструктури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Anyam Z. [et al.] Empirical performance analysis of WireGuard vs. OpenVPN in cloud and virtualised environments. MDPI Computers. 2025. Vol. 14, no. 8, P. 326.
2. Donenfeld J. A. Next Generation Kernel Network Tunnel. URL: <https://www.wireguard.com/papers/wireguard.pdf> (дата звернення: 16.12.2025).
3. OpenVPN vs WireGuard: Top Two VPN Protocols Side By Side. GoodAccess. URL: <https://www.goodaccess.com/blog/openvpn-vs-wireguard> (дата звернення: 16.12.2025).