УДК 621.391:004.056

КОНФІГУРАЦІЯ ПРИВАТНОГО VPN-СЕРВЕРУ

Тараненко І. О.
e-mail: ilia.taranenko@nure.ua
Науковий керівник – к.т.н., доц. Іваненко С. А.
Харківський національний університет радіоелектроніки, каф. IMI
м. Харків, Україна

Practical aspects of configuring a personal VPN server to prevent unauthorized access to user data by third parties are examined. Risks of information interception in untrusted networks are analyzed, justifying the transition to a personal infrastructure. The WireGuard protocol is utilized as a modern tool for building secure communication channels. Key stages of implementation and the advantages of private infrastructure over commercial solutions are outlined.

Проблема захисту конфіденційної інформації під час її передачі через публічні мережі залишається однією з найактуальніших у сучасній сфері кібербезпеки [1].

Оскільки наше життя все більше переходить в онлайн, нам доводиться постійно підключатися до ресурсів, правила безпеки яких часто залишаються для нас незрозумілими. Ризик перехоплення даних третіми особами, включаючи зловмисників, які реалізують атаки типу «man-in-the-middle», а також інтернет-провайдерів, що здійснюють глибокий аналіз пакетів, вимагає використання надійних методів інкапсуляції та шифрування трафіку [2]. Навіть при використанні захищених протоколів прикладного рівня, витік метаданих може дозволити стороннім спостерігачам формувати детальний профіль поведінки суб’єкта в мережі.

Хоча сучасний ринок пропонує велику кількість комерційних VPN-сервісів, вони не завжди є панацеєю. Основна проблема полягає в необхідності повної довіри до постачальника послуг, який теоретично має технічну можливість дешифрувати або логувати користувацьку активність. Численні інциденти з витоком баз даних провайдерів підтверджують, що концепція «zero-log» часто є лише маркетинговим твердженням.

У зв'язку з цим, власна інфраструктура стає найнадійнішим способом гарантувати справжню анонімність у мережі, не покладаючись на обіцянки комерційних сервісів. Такий підхід дозволяє користувачеві самостійно контролювати всі рівні доступу до інфраструктури та виключає участь посередників у ланцюгу передачі даних.

Для практичної реалізації захищеного з’єднання пропонується використання протоколу WireGuard. На відміну від традиційних рішень, таких як IPsec або OpenVPN, цей протокол базується на концепції «stateful» з’єднання та використовує передові криптографічні примітиви. Компактна кодова база протоколу забезпечує вищу енергоефективність для пристроїв, що є критичним фактором у сучасних умовах [3].

Процес конфігурації такої системи передбачає налаштування віртуального мережевого інтерфейсу, генерацію унікальних пар ключів для кожного клієнтського пристрою та реалізацію фільтрації трафіку.

Важливим аспектом впровадження VPN-інфраструктури є вибір методу розгортання, який залежить від вимог до масштабованості та компетенцій адміністратора мережі.

Ручне розгортання безпосередньо на базі операційної системи є актуальним для сценаріїв, що потребують максимального рівня кастомізації. Цей метод передбачає ручну інсталяцію пакетів та самостійне створення файлів конфігурації, вимагає від адміністратора глибших знань, проте дозволяє детально контролювати кожен етап.

У хмарних середовищах найбільш ефективним підходом є використання концепції IaC. Це дозволяє автоматизувати процес створення віртуальних інстансів та їх подальшого налаштування за допомогою скриптів ініціалізації. Такий метод забезпечує швидке відтворення ідентичних конфігурацій, проте водночас вимагає додаткових знань і навичок роботи із хмарною інфраструктурою.

Альтернативним методом є використання технології контейнеризації. Застосування Docker-контейнерів дозволяє відокремити VPN-сервер від хостової операційної системи, що значно спрощує процес оновлення компонентів та перенесення всієї інфраструктури між різними апаратними середовищами. Використання імейджів дозволяє розгорнути захищене з’єднання за лічені хвилини.

Вибір між автоматизованими хмарними методами, ручним налаштуванням на машині або використанням контейнерів дозволяє адаптувати систему до певних потреб користувача.

Отримана архітектура надійно захищає дані від перехоплення та аналізу, не знижуючи при цьому швидкість роботи мережі. Власний VPN-сервер фактично суттєво знижує ризики, пов’язані зі зламом проміжних вузлів, що робить його ідеальним вибором для користувачів, які прагнуть максимальної безпеки в інтернеті.

Список використаних джерел:

1. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. Global Edition. 8th ed. Harlow: Pearson Education Limited, 2021. 800 с

2. Stallings W. Cryptography and Network Security: Principles and Practice. 5-те вид. Pearson Education, 2010. 900 с.

3. Donenfeld J. WireGuard: Next Generation Kernel Network Tunnel. *Wireguard*. URL: https://www.wireguard.com/papers/wireguard.pdf (дата звернення: 03.03.2026).