

ОБ'ЄДНАННЯ ПРИСТРОЇВ МОНІТОРИНГУ НА БАЗІ RASPBERRY PI В VPN МЕРЕЖУ ДЛЯ ЗДІЙСНЕННЯ ВІДДАЛЕНОГО ДОСТУПУ

Гайдук Д.П., науковий керівник Кумейко В.О.

У цій статті розглядається можливість розгортання VPN-мережі з використанням одноплатних комп'ютерів Raspberry Pi, орієнтована на забезпечення безпечного віддаленого доступу до значної кількості обладнання з використанням однієї виділеної білої статичної IP-адреси.

У сучасних умовах віддаленого моніторингу та управління пристроями, такими як Raspberry Pi, виникає потреба у безпечному та надійному способі доступу до них через Інтернет. Традиційно для цього використовується біла (публічна) IP-адреса, яка дозволяє безпосередньо підключатися до пристрою з будь-якої точки світу.

Використання білої IP-адреси пов'язане з певними труднощами, серед яких насамперед варто відзначити високу вартість, оскільки отримання статичної публічної IP-адреси від провайдера часто потребує додаткових витрат. Також існують суттєві загрози безпеці, адже пристрій із білою IP-адресою стає легкою мішенню для сканування портів і різноманітних атак, таких як DDoS, brute force та інші. Додаткові складнощі створюють обмеження провайдерів, оскільки деякі інтернет-оператори блокують вхідні з'єднання на нестандартні порти. Також, використання білої IP-адреси вимагає здійснювати налаштування, що потребує змін у NAT/PAT, відкриття портів та інших технічних заходів.

Одним із ефективних рішень цієї проблеми є використання віртуальних приватних мереж (VPN). Побудова VPN між одноплатними комп'ютерами, зокрема Raspberry Pi, створює можливості для побудови компактних, енергоефективних та доступних рішень у сфері мережевих технологій.

Одним із ефективних рішень цієї проблеми є використання віртуальних приватних мереж (VPN). Зокрема, протокол OpenVPN дозволяє створити захищене з'єднання між пристроями, забезпечуючи безпечний доступ до Raspberry Pi без необхідності білої IP-адреси.

Віртуальна приватна мережа (VPN) дозволяє створити захищений тунельний зв'язок між приладами на базі Raspberry Pi через інтернет. Переваги такого підходу включають економію коштів, оскільки достатньо одного сервера з білою IP-адресою, наприклад VPS або корпоративний роутер. Також важливою перевагою є безпека, адже дані шифруються, а доступ обмежується авторизованими клієнтами. Крім того, цей підхід забезпечує гнучкість, надаючи можливість підключення з будь-якої точки світу.

Були проаналізовані різні VPN-протоколи, серед яких IPSec виявився складним у налаштуванні та вимагає підтримки на рівні мережевого обладнання. WireGuard характеризується високою швидкістю, але потребує додаткового програмного забезпечення для деяких застосувань. OpenVPN виявився найбільш зручним для Raspberry Pi.

OpenVPN — один із найпоширеніших протоколів організації VPN-з'єднань, що забезпечує високу гнучкість налаштувань та надійний рівень шифрування даних, що передаються. Завдяки відкритому вихідному коду та активній підтримці з боку спільноти, OpenVPN адаптується до потреб різноманітних сценаріїв використання — від корпоративних до індивідуальних рішень [1].

Для реалізації тестового розгортання VPN мережі був створений тестовий стенд. Як VPN сервер слугував роутер Mikrotik RouterBoard 750 (RB750). Як клієнт до даного сервера підключався одноплатний комп'ютер Raspberry Pi 4 версія B.

На маршрутизаторі Mikrotik були здійснені наступні налаштування:

1. Створенні сертифікати для сервера та клієнтів.

2. Увімкнена служба OpenVPN з використанням TCP порту 1194.
3. Були експортовані сертифікати для перенесення їх на плату Raspberry Pi.
4. Були здійснені налаштування правил маршрутизації для забезпечення правильної маршрутизації трафіку між клієнтами VPN та локальною мережею [3,4].

Для налаштування OpenVPN на Raspberry Pi були зроблені наступні кроки:

1. Встановлення OpenVPN: `sudo apt install openvpn -y`.
2. Створення конфігураційного файлу користувача VPN: `client.conf`.
3. Перенесення файлів сертифікатів і ключів.
4. Запуск підключення до OpenVPN сервера: `sudo openvpn --config /etc/openvpn/client.conf [2]`.

Після налаштування OpenVPN-з'єднання між Raspberry Pi та маршрутизатором MikroTik вдалося досягти значних переваг у декількох аспектах. Перш за все, було забезпечено безпечний віддалений доступ, який створює захищене з'єднання між пристроями без необхідності відкривати порти на та використовувати білу IP-адресу для Raspberry Pi. Крім того, спостерігається суттєве зниження витрат завдяки відсутності потреби в отриманні статичних білих IP-адрес для кожного віддаленого пристрою, що дозволить зменшувати загальні витрати на при експлуатації системи моніторингу. Також важливим досягненням стала гнучкість та масштабованість системи, яка надає можливість підключення кількох Raspberry Pi до одного VPN-сервера, що значно спрощує управління та моніторинг пристроїв.

Використання OpenVPN для віддаленого доступу до Raspberry Pi є ефективним рішенням, яке забезпечує безпечний доступ до пристроїв без необхідності білої IP-адреси для кожного віддаленого пристрою. Це дозволяє знизити витрати, підвищити безпеку та спростити процес налаштування та управління пристроями в мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

5. openvpn.net [Електронний ресурс] Official Raspberry Pi VPN Server with Access Server – Режим доступу: <https://openvpn.net/as-docs/raspberry-pi.html> (дата звернення 15.04.25)
6. www.vpnunlimited.com [Електронний ресурс] Інструкція з налаштування OpenVPN® для всіх основних платформ - Режим доступу: <https://www.vpnunlimited.com/ua/help/manuals/open-vpn/linux> (дата звернення 15.04.25)
7. <https://help.mikrotik.com> [Електронний ресурс] OpenVPN - Режим доступу: <https://help.mikrotik.com/docs/spaces/ROS/pages/2031655/OpenVPN> (дата звернення 15.04.25)
8. <https://forum.mikrotik.com> [Електронний ресурс] Форум обговорення Mikrotik – Режим доступу: <https://forum.mikrotik.com/viewtopic.php?t=212327> (дата звернення 15.04.25)

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**



ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ

**ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ
VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
СТУДЕНТІВ І АСПІРАНТІВ
*24 квітня 2025 року***

Київ 2025

УДК 004

Відповідальна за випуск: М.І. Лендел

Збірник наукових праць за матеріалами VII Всеукраїнської науково-практичної конференції студентів і аспірантів «ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ '2025», 24 квітня 2025 року, НУБіП України, Київ. – 452 с. (електронне видання)

Відповідальність за зміст публікацій несуть автори.

Передрук матеріалів, а також використання їх будь-якій формі допускається лише з дозволу авторів