Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: " Використання OpenVPN для створення захищеного доступу до внутрішніх ресурсів "

Виконав: студент (ка) IV курсу, групи СБ-41
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Опуда Вадим Володимирович
підпис (прізвище та ініціали)

Керівник _____ Тимощук Д. І.
підпис (прізвище та ініціали)

Нормоконтроль _____ Дроздова Т. В.
підпис (прізвище та ініціали)

Завідувач кафедри _____ Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент _____
підпис (прізвище та ініціали)

м. Тернопіль – 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Опуді Вадиму Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Використання OpenVPN для створення захищеного доступу до внутрішніх ресурсів

Керівник роботи Тимощук Дмитро Іванович, старший викладач кафедри КБ.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 02 » 05 2025 року № 4/7-361

2. Термін подання студентом завершеної роботи 12.06.2025

3. Вихідні дані до роботи Документація OpenVPN та Mikrotik, документація XigmaNAS, Документація Windows та Ubuntu Linux, вимоги до безпеки VPN мережі.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1. Аналіз завдання та огляд предметної області
2. Розгортання лабораторного середовища
3. Налаштування та тестування OpenVPN
4. Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титульна сторінка. 2. Актуальність дослідження. 3. Мета, Об'єкт, Предмет дослідження. 4. Задачі. 5. Схема передачі даних з використанням VPN. 6. Типи VPN. 7. OpenVPN протокол. 8. Схема лабораторного середовища тестування. 9. Складові лабораторного середовища тестування. 10. Налаштування сервісу OpenVPN маршрутизатора MikroTik. 11. Налаштування спільного доступу до каталогу через службу Samba в XigmaNAS. 12. Налаштування OpenVPN connect на різних ОС. 13. Тестування OpenVPN: Ubuntu Linux. 14. Тестування OpenVPN: Windows 10. 15. Тестування OpenVPN: MikroTik. 16. Висновки. 17. Завершальний.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко С. Ю., к.т.н. доцент кафедри МТ		

7. Дата видачі завдання 29.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.01.2025	
2.	Опрацювання джерел в галузі дослідження	02.02 – 30.01	
3.	Оформлення розділу «Аналіз завдання та огляд предметної області»	21.02 – 10.03	
4.	Оформлення розділу «Розгортання лабораторного середовища»	11.03 – 25.03	
5.	Оформлення розділу «Налаштування та тестування OpenVPN»	10.04 – 05.05	
6.	Оформлення розділу «Безпека життєдіяльності, основи охорони праці»	10.05 – 21.05	
7.	Оформлення кваліфікаційної роботи	23.05 – 06.06	
8.	Нормоконтроль	06.06 – 10.06	
9.	Перевірка на плагіат	11.06 – 12.06	
10.	Попередній захист кваліфікаційної роботи	14.06 – 15.06	
11.	Захист кваліфікаційної роботи	26.06.2025	

Студент _____ Опуда В. В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Тимощук Д. І.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Використання OpenVPN для створення захищеного доступу до внутрішніх ресурсів // Кваліфікаційна робота ОР «Бакалавр» // Опуда Вадим Володимирович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2025 // С. 81, рис. – 43, табл. – 0, кресл. – 13, додат. – 1.

Ключові слова: OpenVPN, MikroTik CHR, NAS, SMB, XigmaNAS.

У кваліфікаційній роботі бакалавра розглянуто розгортання та налаштування системи захищеного доступу до корпоративних ресурсів із використанням OpenVPN. Для побудови тестового середовища застосовано гіпервізор Oracle VM VirtualBox, на якому розгорнуто програмний маршрутизатор MikroTik CHR та NAS-сервер XigmaNAS. У роботі проаналізовано принципи роботи VPN, особливості різних протоколів і типів VPN-з'єднань, а також висвітлено процес створення сертифікатів та налаштування брандмауера й NAT на MikroTik. Проведено налаштування клієнтських підключень OpenVPN з операційних систем Windows 10, Android та Ubuntu Linux, виконано тестування доступу до локальних ресурсів (зокрема NAS-сервера по протоколу SMB), а також перевірено стабільність та безпеку з'єднань. Результати роботи можуть бути впроваджені у компаніях різного масштабу, забезпечуючи віддаленим користувачам захищений доступ до внутрішніх мережевих ресурсів.

ABSTRACT

Use of OpenVPN to Create Secure Access to Internal Resources. // Thesis of educational level "Bachelor"// Vadym Opuda // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБ-41 // Ternopil, 2025 // P. 81, figs. 43, tables – 0, drawings 13, added. 1.

Keywords: OpenVPN, MikroTik CHR, NAS, SMB, XigmaNAS.

The bachelor's thesis describes the deployment and configuration of a secure access system for corporate resources using OpenVPN. To build the test environment, the Oracle VM VirtualBox hypervisor was used, on which the MikroTik CHR software router and the XigmaNAS NAS server were deployed. The paper analyses the principles of VPN operation, the features of various protocols and types of VPN connections, and covers the process of creating certificates and configuring firewall and NAT on MikroTik. OpenVPN client connections from Windows 10, Android, and Ubuntu Linux operating systems were configured, access to local resources (including a NAS server using the SMB protocol) was tested, and the stability and security of connections were verified. The results can be implemented in companies of various sizes, providing remote users with secure access to internal network resources.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

NAS	—	Network Attached Storage
SSL	—	Secure Sockets Layer
L2TP	—	Layer 2 Tunneling Protocol
IPSec	—	Internet Protocol Security
NAT	—	Network Address Translation
IKEv2	—	Internet Key Exchange version 2
CA	—	Certificate Authority
LAN	—	Local Area Network
PPP	—	Point-to-Point Protocol
AES	—	Advanced Encryption Standard
TCP	—	Transmission Control Protocol
TLS	—	Transport Layer Security
CLI	—	Command-Line Interface
HMAC	—	Hash-based Message Authentication Code
VPN	—	Virtual Private Network
CHR	—	Cloud Hosted Router
ICMP	—	Internet Control Message Protocol
SMB	—	Server Message Block
ВМ	—	Віртуальна машина
UDP	—	User Datagram Protocol

ВСТУП

Актуальність теми. З стрімким розвитком інформаційних технологій питання захисту даних і забезпечення безпечного доступу до корпоративних ресурсів стає дедалі важливішим. Зростання кількості віддалених працівників, розширення бізнесу та збільшення кількості загроз у кіберпросторі вимагають ефективних рішень для захисту мережевих комунікацій. Одним із найпоширеніших методів забезпечення конфіденційності даних та безпеки доступу є використання віртуальних приватних мереж (VPN). Серед багатьох VPN-рішень OpenVPN виділяється своєю надійністю, гнучкістю та відкритим кодом, що дозволяє адаптувати його під специфічні потреби організацій. Ця тема є актуальною для компаній, які прагнуть підвищити рівень безпеки своїх внутрішніх ресурсів, забезпечуючи віддаленим користувачам безпечний доступ, що є ключовим для ефективної роботи у сучасних умовах.

Мета і задачі дослідження. Метою дослідження є розробка та впровадження системи захищеного доступу до внутрішніх ресурсів компанії за допомогою OpenVPN.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- вивчити принципи роботи і типи технологій, що застосовуються для створення захищених VPN мереж;
- дослідити можливості OpenVPN;
- розробити архітектуру системи на основі Mikrotik CHR з налаштуванням OpenVPN сервера, брандмауера та NAT;
- здійснити налаштування клієнтських підключення до VPN з Windows 10, Android та Ubuntu Linux;
- налаштувати віддалений доступ по VPN мережі до NAS-сервера XigmaNAS по протоколу SMB;
- провести тестування системи та оцінити її ефективність.

Об’єкт дослідження. Процеси створення та забезпечення захищеного доступу до внутрішніх ресурсів компанії у мережах загального користування.

Предмет дослідження. Технології та інструменти створення VPN-мережі із використанням OpenVPN для захисту корпоративних ресурсів.

Практичне значення одержаних результатів. Результати дослідження можуть бути використані для впровадження систем захищеного доступу до внутрішніх ресурсів у компаніях різного масштабу. Розроблена система на основі OpenVPN може бути адаптована під конкретні потреби підприємств, забезпечуючи високий рівень безпеки та стабільності роботи. Отримані знання та реалізовані рішення також можуть бути використані для навчання IT-фахівців і розробки модернізованих технологічних підходів у сфері захисту даних.

РОЗДІЛ 1 АНАЛІЗ ЗАВДАННЯ ТА ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Принцип роботи VPN

Віртуальна приватна мережа - це технологія, яка дозволяє створити захищений, зашифрований канал зв'язку через незахищені мережі, такі як Інтернет. VPN забезпечує конфіденційність, цілісність і аутентифікацію даних, переданих між користувачем і кінцевою мережею.

На рисунку 1.1 зображено, як працює передача даних в Інтернеті без використання VPN.

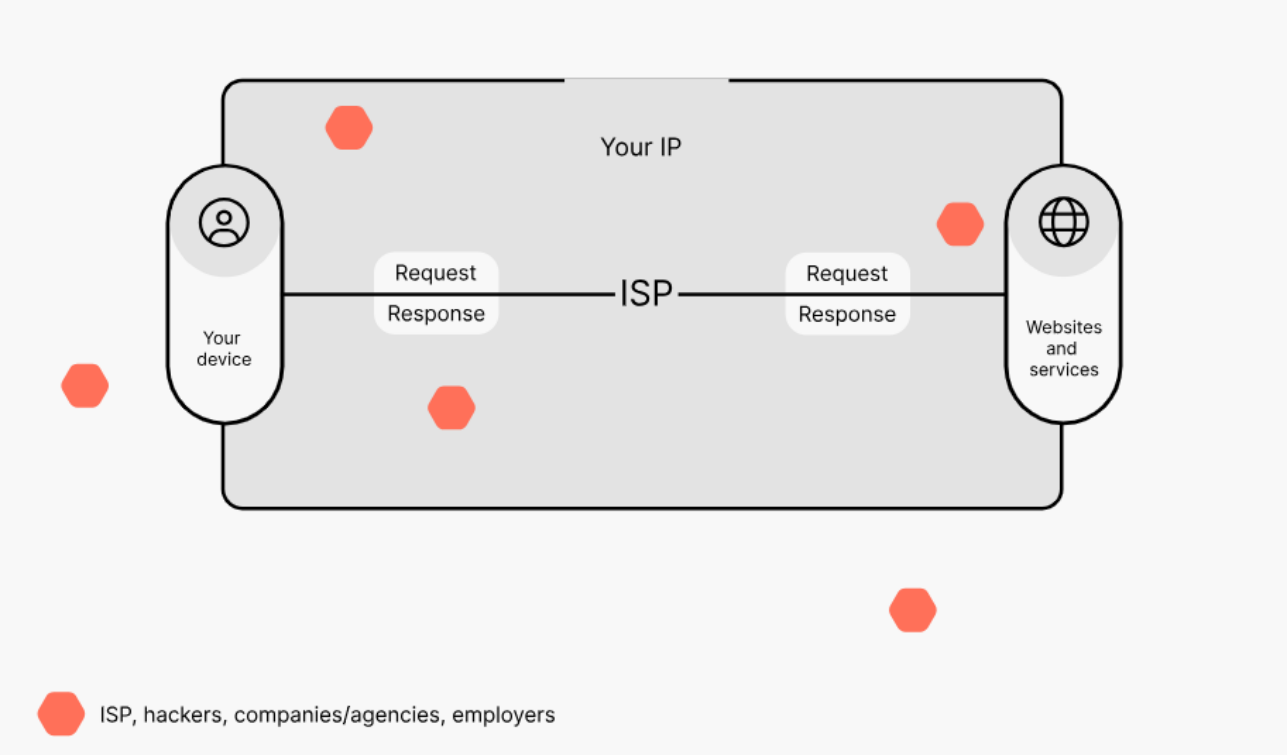

Рисунок 1.1 – Передача даних без використання VPN

Пристрій створює запити на доступ до вебсайтів або онлайн-сервісів. Ці запити передаються через інтернет-провайдера (ISP), який виступає посередником. Після цього провайдер перенаправляє запити до потрібних серверів вебсайтів чи сервісів. Сервери обробляють ці запити, генерують відповіді й передають їх назад через той самий шлях спочатку до провайдера, а потім пристрою. Під час цього процесу трафік не зашифрований [1]. Це означає,

що дані, які передаються між пристроєм і вебсайтами, можуть бути легко перехоплені, прочитані або модифіковані сторонніми особами. Інтернет-провайдер бачить усі запити та відповіді. Крім того, реальна IP-адреса передається разом із запитами. IP-адреса - це унікальний ідентифікатор, який дозволяє приблизно визначити місцезнаходження, а також створювати профіль активності в Інтернеті. Без додаткового захисту, як у випадку, показаному на рисунку, є вразливість до багатьох загроз. Наприклад, хакери можуть перехоплювати дані, особливо якщо є підключені до публічної Wi-Fi мережі, де відсутні базові заходи захисту. У таких мережах дані можна перехопити за допомогою спеціального програмного забезпечення. Крім того, компанії, агентства, роботодавці або рекламодавці можуть аналізувати трафік, створюючи профілі поведінки, інтересів або звичок. Відсутність шифрування означає, що особисті дані, такі як паролі, фінансова інформація або інші конфіденційні відомості, залишаються доступними для перехоплення. Це особливо ризиковано під час використання незахищених протоколів передачі даних або відвідування вебсайтів без HTTPS-захисту. Крім того, через видимість реальної IP-адреси можливі DDoS-атаки або спроби зловмисників отримати доступ до локальної мережі [15]. Ситуація, зображена на схемі, демонструє типову незахищеність користувачів під час роботи в Інтернеті без VPN або інших захисних технологій. Інкапсуляція та шифрування, які використовуються в VPN, відсутні, тому всі дані передаються у відкритому вигляді.

На рисунку 1.2 зображено, як працює передача даних через Інтернет із використанням VPN.

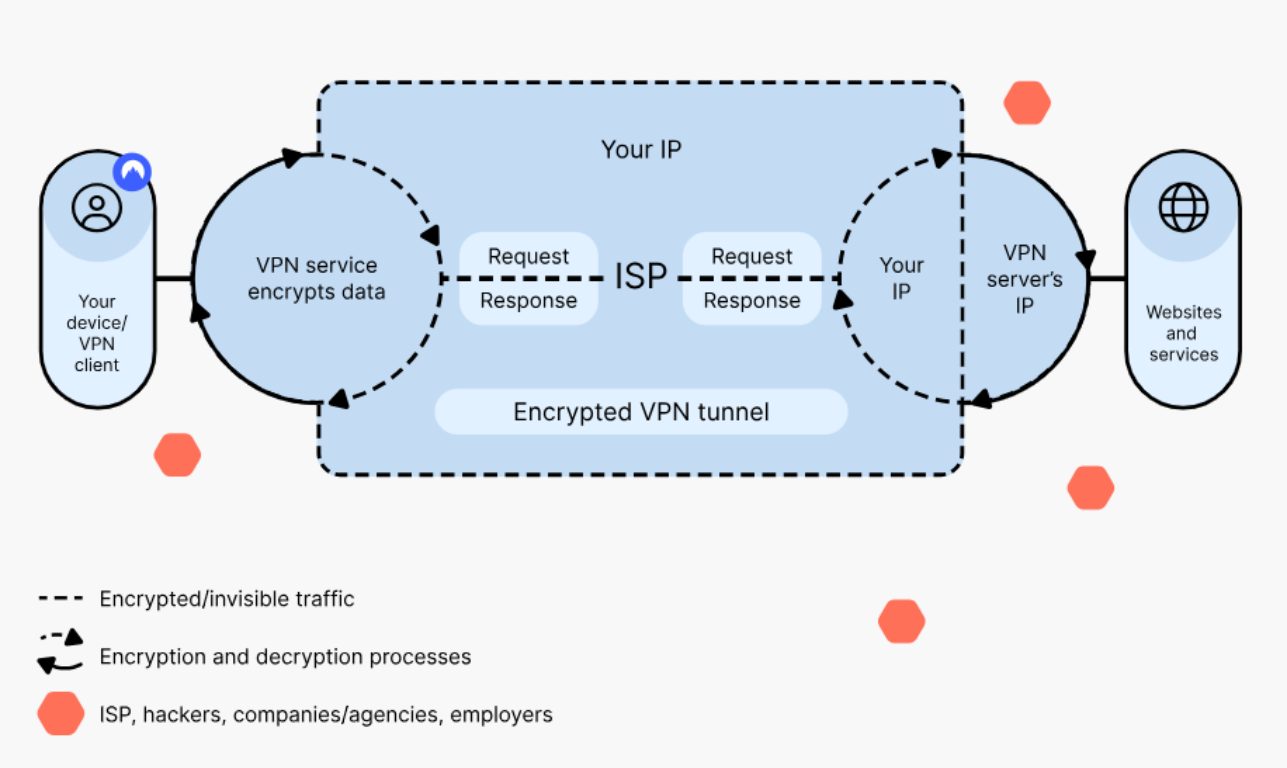

Рисунок 1.2 – Передача даних з використання VPN

Основна ідея полягає в тому, що VPN створює зашифрований тунель між клієнтським пристроєм і сервером VPN, забезпечуючи конфіденційність і захист даних під час передачі через незахищені мережі, такі як Інтернет. Перед початком передачі даних VPN-клієнт на пристрої шифрує всю інформацію, що передається через Інтернет. Цей процес шифрування гарантує, що дані стають невидимими для сторонніх осіб, таких як ISP, хакери. Зашифровані пакети даних потім надсилаються через інтернет-провайдера, але, на відміну від звичайного з'єднання, трафік захищений і видимий лише для сервера VPN.

Сервер VPN виступає посередником між пристроєм користувача і вебсайтами або онлайн-сервісами. Після отримання даних від пристрою сервер розшифровує їх і перенаправляє до кінцевого пункту призначення, такого як вебсайт або сервіс, із використанням своєї IP-адреси. Це приховує реальну IP-адресу, замінюючи її на IP-адресу VPN-сервера, що додає ще один рівень анонімності. Таким чином, вебсайти бачать запит як такий, що походить від VPN-сервера, а не клієнтського пристрою. Зворотні дані, які надсилають вебсайти у відповідь, спершу надходять на сервер VPN, де вони знову шифруються та відправляються через тунель до пристрою клієнта. На стороні

клієнта VPN-клієнт розшифровує ці дані та робить їх доступними для користувача. Навіть якщо зловмисники перехоплять трафік, вони не зможуть прочитати його вміст, оскільки дані зашифровані. З використанням VPN реальна IP-адреса приховується, а вебсайти бачать лише IP-адресу VPN-сервера. Це унеможливлює відстеження реальної геолокації та підвищує рівень анонімності в Інтернеті.

Тунелювання – це один із ключових механізмів роботи VPN, який забезпечує безпечну передачу даних через незахищені мережі, такі як Інтернет. Суть тунелювання полягає у створенні логічного "тунелю", що об'єднує пристрій користувача та сервер VPN. У межах цього тунелю дані передаються у вигляді інкапсульованих пакетів, які захищають інформацію від перехоплення або втручання. Процес тунелювання починається з інкапсуляції вихідних даних у новий мережевий пакет. Цей пакет містить не лише початкову інформацію, але й новий заголовок, що вказує на VPN-сервер як кінцевий пункт призначення. Таким чином, навіть якщо зловмисник перехопить пакет, він не зможе дізнатися про його реальний вміст або кінцеве призначення. Тунелювання працює завдяки використанню спеціалізованих протоколів, які відповідають за створення та підтримку логічного тунелю. Тунелювання передбачає процес маршрутизації даних через VPN-сервер. Всі запити клієнта спочатку надходять на сервер VPN, де відбувається їх розшифрування та перенаправлення до реального кінцевого пункту призначення, наприклад, веб-сайту чи внутрішнього ресурсу компанії. Зворотний трафік проходить через сервер, де він шифрується та надсилається через тунель до клієнта. Тунелювання також дозволяє обійти географічні обмеження та цензуру, адже зовнішній трафік виглядає так, ніби він надходить від VPN-сервера, а не від реального користувача. Це досягається завдяки тому, що зовнішній спостерігач бачить лише зашифровані пакети та IP-адресу VPN-сервера. Важливою перевагою тунелювання є можливість забезпечити цілісність даних. У рамках VPN кожен пакет супроводжується контрольними сумами або іншими механізмами перевірки, які дозволяють виявити та відкинути змінені або пошкоджені пакети, гарантуючи, що дані дійдуть до адресата в незмінному вигляді.

Шифрування є механізмом, який забезпечує конфіденційність даних, що передаються через VPN. Його основна мета полягає у перетворенні відкритих даних (plain text) у зашифрований формат (cipher text), який є незрозумілим для сторонніх осіб. Це забезпечує захист інформації від несанкціонованого доступу навіть у разі перехоплення переданих даних. Процес шифрування починається на стороні клієнта, де інформація, що передається через VPN, за допомогою алгоритмів шифрування кодується у захищену форму. Ключ шифрування, який використовується в цьому процесі, відомий лише клієнту та серверу VPN. Сервер, отримавши зашифровані дані, за допомогою того ж або відповідного ключа розшифровує інформацію, перетворюючи її назад у зрозумілий формат. Зворотний процес відбувається для даних, що передаються від сервера до клієнта. Для забезпечення високого рівня безпеки VPN використовують різні типи шифрування. Найпоширенішим є AES, який забезпечує надійний захист даних і має довжину ключів 128, 192 і 256 біт. AES-256 є найстійкішим і найчастіше використовується у VPN-рішеннях для захисту конфіденційних даних. Інший популярний алгоритм - ChaCha20, який відзначається високою швидкістю роботи та використовується в сучасних VPN-протоколах, таких як WireGuard. Шифрування в VPN також тісно пов’язане з використанням протоколів безпеки. Наприклад, OpenVPN використовує SSL/TLS для шифрування трафіку, забезпечуючи як захист даних, так і аутентифікацію між клієнтом і сервером. Протокол L2TP/IPSec реалізує двошаровий захист, де IPSec відповідає за шифрування, а L2TP забезпечує тунелювання. Крім забезпечення конфіденційності, шифрування також гарантує цілісність даних. Це досягається за допомогою контрольних сум і криптографічних хешів, які додаються до кожного пакета даних. Якщо під час передачі інформації пакет змінюється або пошкоджується, сервер або клієнт відкидають його як ненадійний. Шифрування VPN також сприяє анонімності користувача. Зашифрований трафік маскує його вміст, а також справжню IP-адресу клієнта, підміняючи її адресою VPN-сервера. Це унеможливлює визначення місця перебування користувача чи його активності в мережі сторонніми спостерігачами. Ще одним важливим моментов шифрування є обмін ключами. Для захисту процесу передачі ключів між

клієнтом і сервером використовуються асиметричні методи шифрування, такі як RSA, які гарантують, що сторонні не можуть перехопити ключі під час їхньої передачі. Після встановлення з'єднання VPN зазвичай переходить до використання симетричних алгоритмів шифрування, які є швидшими та ефективнішими.

Автентифікація в контексті роботи VPN є процесом перевірки достовірності користувача або пристрою перед наданням доступу до захищеної мережі. Її основна мета – гарантувати, що доступ отримують лише автентифіковані користувачі, виключаючи можливість підключення сторонніх або зловмисників. Процес автентифікації починається на етапі встановлення з'єднання між клієнтом і сервером VPN. Клієнт надсилає серверу свої облікові дані або інші засоби ідентифікації, після чого сервер перевіряє їх за допомогою бази даних користувачів або зовнішніх сервісів автентифікації, таких як RADIUS чи Active Directory. Якщо облікові дані є правильними, сервер дозволяє встановлення з'єднання. Для забезпечення безпеки в VPN використовуються різні методи автентифікації. Найпростішим і найпоширенішим є автентифікація за допомогою логіна та пароля. Це базовий спосіб, де користувач вводить своє ім'я та пароль, які перевіряються сервером. Однак такий підхід може бути вразливим до атак, якщо використовуються слабкі паролі або відсутні додаткові рівні захисту. Більш складним і надійним методом є використання цифрових сертифікатів. У цьому випадку і клієнт, і сервер використовують сертифікати, підписані центром сертифікації (CA). Сертифікати містять криптографічні ключі, які забезпечують високий рівень захисту під час автентифікації. Такий метод особливо популярний у корпоративному середовищі, де важлива безпека доступу до внутрішніх ресурсів. Двофакторна автентифікація (2FA) додає ще один рівень безпеки. Крім логіна і пароля, користувач повинен підтвердити свою особу за допомогою додаткового фактора, такого як одноразовий пароль (OTP), що генерується мобільним додатком (наприклад, Google Authenticator) або надсилається SMS. Це суттєво ускладнює завдання зловмисникам, навіть якщо вони отримали доступ до основних облікових даних. Інші сучасні методи автентифікації включають використання апаратних токенів або біометричних

даних, таких як відбитки пальців або розпізнавання обличчя. Апаратні токени генерують унікальні коди, які можуть бути використані лише протягом короткого часу, забезпечуючи додатковий рівень безпеки. Аутентифікація також може включати перевірку пристрою, з якого здійснюється підключення. Це робиться за допомогою унікальних сертифікатів або відбитків пристроїв, що гарантує, що навіть у разі компрометації облікових даних з'єднання не буде дозволене з невідомого пристрою.

1.2 Сфери застосування VPN

Віртуальні приватні мережі мають широке застосування завдяки своїй здатності забезпечувати безпеку [2]. Однією з основних сфер використання VPN є корпоративна діяльність. Компанії використовують VPN для надання своїм співробітникам захищеного доступу до внутрішніх мереж, особливо під час роботи з дому або в умовах віддаленої праці. Це дозволяє з'єднувати пристрої співробітників із корпоративною мережею через зашифрований тунель, забезпечуючи безпечний доступ до внутрішніх документів, серверів і додатків, що захищає дані компанії від несанкціонованого доступу.

Ще однією важливою сферою є особисте використання VPN приватними особами. Користувачі застосовують VPN для забезпечення конфіденційності та анонімності в Інтернеті. VPN приховує реальну IP-адресу користувача, замінюючи її IP-адресою сервера, що унеможливлює відстеження місцезнаходження чи онлайн-активності. Це особливо актуально для захисту особистих даних під час підключення до публічних Wi-Fi мереж, які можуть бути вразливими до атак хакерів.

VPN також активно використовуються для обходу географічних обмежень і цензури. У деяких країнах доступ до певних сайтів або сервісів може бути заблокований через політичні, юридичні чи інші обмеження. Завдяки VPN користувачі можуть підключатися до серверів у країнах, де ці ресурси доступні, отримуючи вільний доступ до інформації та послуг. Наприклад, VPN дозволяє

переглядати контент на стримінгових платформах, який недоступний у певних регіонах, чи отримувати доступ до соціальних мереж, заблокованих урядом.

Ще одна значна сфера застосування VPN - це забезпечення безпеки під час передачі конфіденційних даних. Це особливо важливо для банківських операцій, роботи з фінансовими системами або інших транзакцій, що містять особисту або комерційну інформацію. VPN забезпечує шифрування даних, переданих між користувачем і сервером, що унеможливлює їх перехоплення навіть у випадку атак.

У сфері IT VPN є інструментом для тесту створення безпечних середовищ для розробки та навчання, а також для організації захищеного обміну даними між віддаленими офісами. Організації також можуть використовувати VPN для забезпечення приватного з'єднання між хмарними сервісами та локальними мережами, що особливо актуально для бізнесу, який працює із хмарними обчисленнями.

1.3 Типи VPN

Типи VPN-з'єднань забезпечують різноманітні потреби, пропонуючи широкий вибір рішень як для професійного, так і для особистого використання на комп’ютерах та мобільних пристроях.

1.3.1 Технологічні рішення

Одним із найбільш поширених є VPN для віддаленого доступу (Client-to-Site VPN). Це рішення призначене для окремих користувачів, які потребують безпечного підключення до приватної мережі чи стороннього сервера зі своїх пристроїв [3]. Віддалений доступ до VPN особливо популярний серед працівників, які працюють поза офісом.

На рисунку 1.3 зображено принцип роботи VPN для віддаленого доступу.

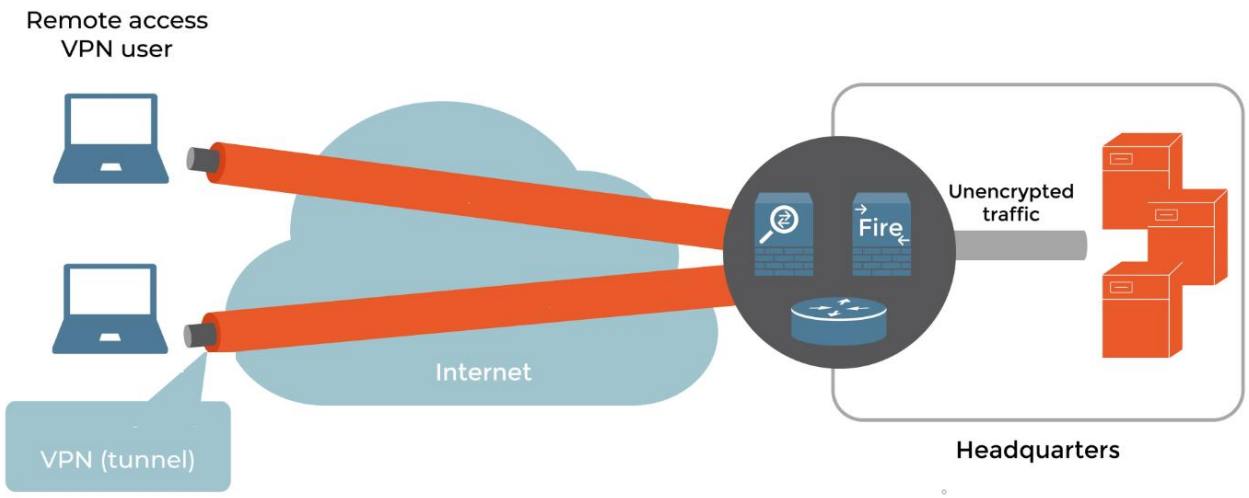

Рисунок 1.3 – Client-to-Site VPN

Такий VPN дозволяє їм безпечно підключатися до ресурсів компанії, таких як файли, сервери чи системи, незалежно від їхнього фізичного розташування. Користувач вводить свої облікові дані через сторінку входу або VPN-додаток, який забезпечує безпечне з'єднання та доступ до додаткових функцій. У приватному використанні VPN для віддаленого доступу є незамінним для захисту персональних даних під час перегляду Інтернету. Він надає анонімність, запобігає відстеженню провайдерами та допомагає обходити обмеження доступу до контенту чи мережеві фаєрволи.

VPN для з’єднання між офісами (Site-to-Site VPN) орієнтований на організації, які потребують безпечного підключення кількох локальних мереж (LAN) через різні місця [3].

На рисунку 1.4 зображено принцип роботи VPN для з’єднання між офісами.

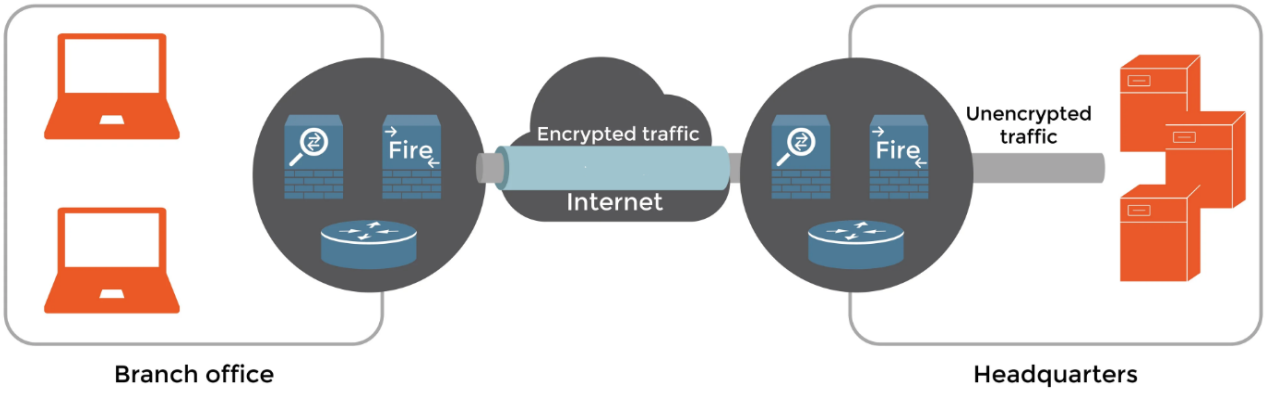

Рисунок 1.4 – Site-to-Site VPN

Це дозволяє компаніям створювати приватну мережу, яка об'єднує офіси чи відділи, забезпечуючи можливість обміну ресурсами та даними. У межах Site-to-Site VPN розрізняють два види: внутрішньомережевий VPN (Intranet VPN), який з'єднує кілька офісів однієї компанії, і зовнішньомережевий VPN (Extranet VPN), який об’єднує мережі різних організацій для співпраці з партнерами, постачальниками чи клієнтами. Такий тип VPN забезпечує високий рівень безпеки і дозволяє організаціям обмінюватися ресурсами, водночас зберігаючи контроль над тим, що саме доступно для зовнішніх користувачів. Site-to-Site VPN є оптимальним рішенням для великих підприємств із підрозділами в різних регіонах.

1.3.2 Протоколи

Протоколи VPN - це набір правил, які визначають, як дані передаються між пристроєм користувача та VPN-сервером через Інтернет. Вони впливають на швидкість, безпеку та стабільність VPN-з'єднання [4]. Існує кілька основних типів протоколів VPN, кожен із яких має свої переваги, недоліки та сфери застосування.

L2TP/IPSec – це поєднання двох протоколів, яке забезпечує створення безпечного та зашифрованого VPN-з’єднання. L2TP сам по собі є протоколом тунелювання, що дозволяє створити тунель між пристроєм користувача та VPN-

сервером [5]. Однак він не надає шифрування даних, тому для забезпечення конфіденційності й захисту використовується IPSec, який додає шифрування й автентифікацію до цього з’єднання (див. рисунок 1.5).

Рисунок 1.5 – L2TP/IPS VPN

Коли L2TP/IPSec використовується для підключення, дані спочатку інкапсулюються за допомогою протоколу L2TP, що створює тунель для їх передачі. Потім IPSec шифрує ці дані, що гарантує їх безпеку навіть у разі перехоплення. IPSec також забезпечує автентифікацію з'єднання, перевіряючи особу клієнта і сервера, що додає додатковий рівень захисту. Поєднання цих двох протоколів дозволяє забезпечити як надійний механізм передачі даних, так і їх захист. L2TP/IPSec працює на рівні мережевих протоколів, що дозволяє йому підтримувати широкі можливості маршрутизації й сумісність із різними пристроями та мережами. Завдяки використанню IPSec цей протокол забезпечує високий рівень шифрування, зазвичай використовуючи алгоритми AES із ключами 128, 192 або 256 біт. Це робить його підходящим для передачі конфіденційних даних. Основними перевагами L2TP/IPSec є високий рівень безпеки, надійність і сумісність із багатьма операційними системами та пристроями, такими як Windows, macOS, Linux, Android та iOS. Протокол також може використовуватися для створення як VPN для віддаленого доступу, так і Site-to-Site VPN, що робить його універсальним рішенням для корпоративного та приватного використання. Проте L2TP/IPSec має й недоліки. Через використання подвійного інкапсулювання (L2TP і IPSec) цей протокол може

бути менш ефективним із точки зору швидкості порівняно з іншими сучасними протоколами, такими як WireGuard чи OpenVPN.

IKEv2/IPSec – це сучасний і надійний протокол VPN, який забезпечує безпечне та швидке з'єднання між клієнтом і сервером [6]. IKEv2 - це протокол, який використовується для встановлення і управління захищеними з'єднаннями, тоді як IPSec відповідає за шифрування та автентифікацію даних, що передаються через це з'єднання. Разом вони створюють потужну комбінацію для забезпечення високого рівня безпеки, стабільності та продуктивності. IKEv2 був розроблений компаніями Microsoft і Cisco і є покращеною версією IKE, який є частиною IPSec. Він забезпечує швидкий процес встановлення з'єднання та автоматичне відновлення VPN-з'єднання у разі його тимчасового розриву, що робить його ідеальним для мобільних пристроїв і користувачів, які часто переключаються між Wi-Fi і мобільними мережами. Завдяки своїй здатності підтримувати безперервність з'єднання, IKEv2/IPSec вважається одним із найкращих протоколів для смартфонів, планшетів і інших портативних пристроїв. Безпека IKEv2/IPSec забезпечується шифруванням на основі IPSec. Протокол використовує сучасні алгоритми шифрування, такі як AES із довжиною ключа 128, 192 або 256 біт, що забезпечує високий рівень захисту даних [7]. Крім шифрування, IPSec також виконує автентифікацію, що гарантує, що з'єднання встановлюється лише між довіреними пристроями. Це досягається через використання сертифікатів, попередньо спільних ключів (pre-shared keys) або облікових даних користувача.

Процес встановлення з'єднання в IKEv2/IPSec складається з кількох етапів. Спочатку IKEv2 створює захищений канал для обміну ключами між клієнтом і сервером (див. рисунок 1.6).

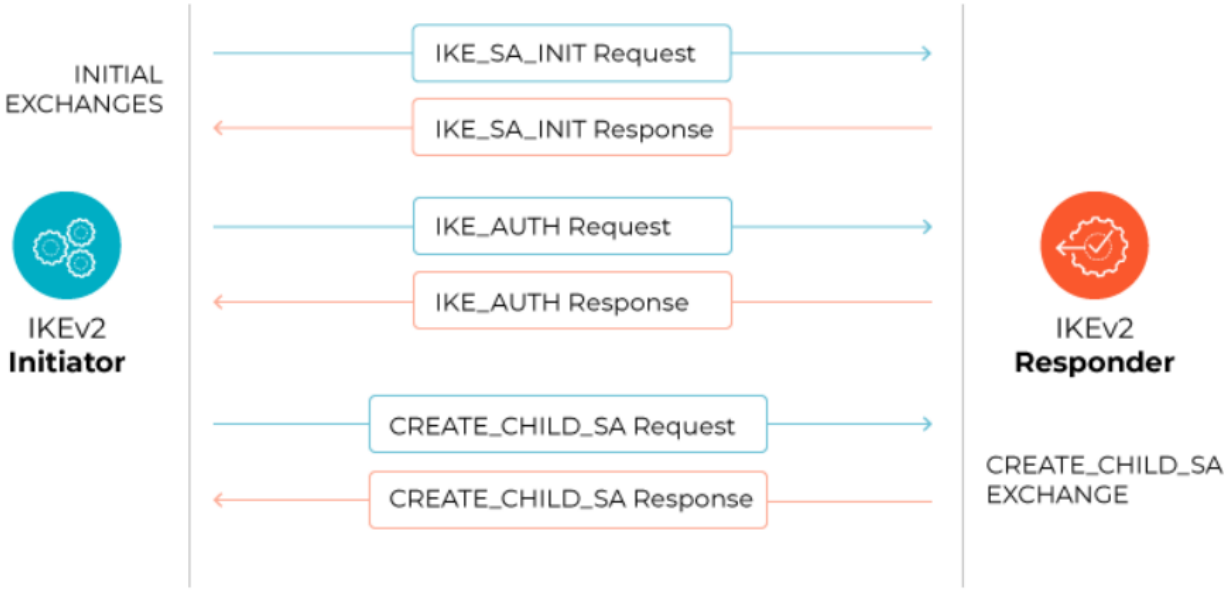

Рисунок 1.6 – Процес встановлення з'єднання в IKEv2

Потім цей канал використовується для створення IPSec-з'єднання, через яке передаються зашифровані дані. Завдяки своїй оптимізації цей процес відбувається швидко, що мінімізує затримки під час підключення до VPN. IKEv2/IPSec відзначається високою продуктивністю. Завдяки ефективній архітектурі він забезпечує швидшу передачу даних, ніж багато інших протоколів VPN, таких як L2TP/IPSec. Це робить його підходящим для роботи з високошвидкісним Інтернет-з'єднанням і для завдань, які вимагають великої пропускної здатності, таких як стримінг або передача великих файлів.

Протокол також стійкий до втрати з'єднання. Якщо VPN-з'єднання розривається через зміну мережі (наприклад, перехід із Wi-Fi на мобільний Інтернет), IKEv2 автоматично відновлює сесію без потреби повторної аутентифікації. Це забезпечує безперервний і комфортний користувацький досвід, особливо для мобільних користувачів. Ще однією перевагою IKEv2/IPSec є його підтримка сучасних операційних систем, таких як Windows, macOS, Linux, Android та iOS. Це робить його універсальним рішенням для різних пристроїв і платформ. Крім того, він підтримує технологію MOBIKE (Mobility and Multihoming), яка дозволяє зберігати з'єднання навіть у разі зміни IP-адреси, що підвищує зручність і надійність для користувачів, які перебувають у русі.

Попри свої численні переваги, IKEv2/IPSec може бути вразливим до блокування, оскільки використовує специфічні порти, які можуть бути закриті мережевими фаєрволами. У таких випадках інші протоколи, такі як OpenVPN, можуть бути більш підходящими.

WireGuard – це сучасний протокол VPN, який був створений для забезпечення високої швидкості, безпеки та простоти у використанні [8] (див. рисунок 1.7).

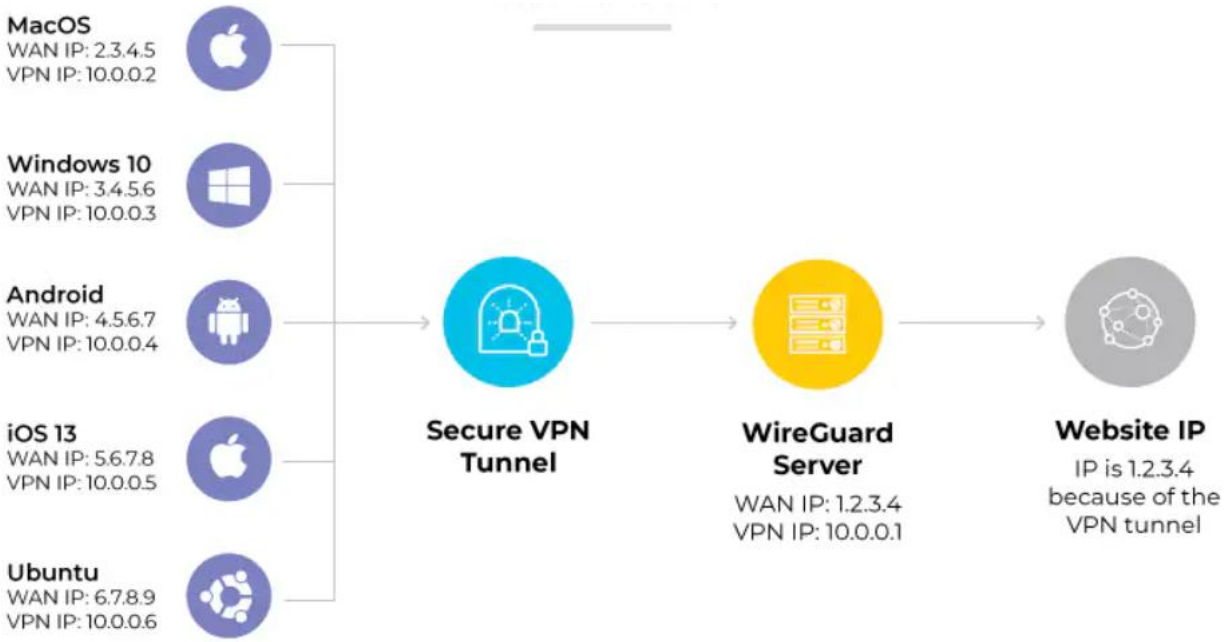

Рисунок 1.7 – WireGuard VPN

Він розроблений з мінімалістичним підходом, що передбачає невеликий обсяг коду порівняно з традиційними VPN-протоколами, такими як OpenVPN або IPSec. Цей компактний дизайн значно знижує ризик вразливостей і помилок у коді, підвищуючи рівень захисту. Основна перевага WireGuard - його висока продуктивність. Він використовує сучасні криптографічні алгоритми, такі як ChaCha20 для шифрування [9], Poly1305 для аутентифікації [10], BLAKE2 для хешування [11] та Curve25519 для обміну ключами [12]. Ці алгоритми забезпечують надійне шифрування та автентифікацію з мінімальними затримками. Завдяки цьому WireGuard забезпечує високу швидкість передачі даних і є ефективним навіть на пристроях із низькою потужністю, таких як

смартфони або маршрутизатори. WireGuard працює на рівні ядра операційної системи, що забезпечує оптимальну інтеграцію з системою і додаткове підвищення продуктивності. Це відрізняє його від традиційних VPN-протоколів, які зазвичай працюють на рівні користувацького простору і можуть мати більші накладні витрати. Завдяки цьому WireGuard ідеально підходить для завдань, які потребують низької затримки, таких як онлайн-ігри, стримінг чи віддалена робота. Простота налаштування є ще однією важливою перевагою WireGuard. Для встановлення з'єднання використовуються публічні та приватні ключі, що значно спрощує процес автентифікації та усуває необхідність використання складних сертифікаційних систем, характерних для інших протоколів. Завдяки цьому користувачі можуть легко налаштувати WireGuard на різних платформах, включаючи Windows, macOS, Linux, Android і iOS. WireGuard використовує фіксовані IP-адреси для кожного підключеного клієнта, що робить його більш передбачуваним і простим для адміністрування. Це також сприяє його інтеграції в мережеві середовища з великим числом клієнтів. Протокол працює через UDP, що дозволяє уникати затримок і зберігати стабільність навіть у випадках, коли TCP-з'єднання були б неефективними. WireGuard підтримує технологію roaming, що дозволяє користувачам зберігати активне VPN-з'єднання навіть при зміні мережі чи IP-адреси. Це робить його ідеальним для мобільних пристроїв і мандрівників, які часто перемикаються між Wi-Fi і мобільним інтернетом. Завдяки цій функції WireGuard забезпечує безперервність роботи без необхідності повторного підключення.

Незважаючи на всі переваги, WireGuard має деякі обмеження. Наприклад, оскільки він використовує статичні IP-адреси, це може створити певні виклики з точки зору конфіденційності, якщо не застосовуються додаткові заходи, такі як використання динамічних ключів. Проте ці питання можна вирішити шляхом правильного налаштування.

OpenVPN – це один із найпопулярніших і найбільш універсальних VPN-протоколів, який забезпечує високу безпеку, гнучкість і стабільність з'єднання [13]. Він заснований на технології з відкритим вихідним кодом, що дозволяє будь-кому перевірити його код на наявність вразливостей і забезпечує довіру з

боку користувачів та організацій. Завдяки своїй сумісності з різними платформами та пристроями OpenVPN є одним із найбільш широко використовуваних VPN-рішень як у корпоративному середовищі, так і для особистого використання.

OpenVPN використовує протоколи SSL/TLS для створення захищених тунелів між клієнтом і сервером [14]. Це забезпечує високу безпеку передачі даних завдяки шифруванню, яке підтримує сучасні алгоритми, такі як AES із довжиною ключа 128 або 256 біт. SSL/TLS також забезпечує автентифікацію клієнта і сервера, що захищає з'єднання від підробки та несанкціонованого доступу. OpenVPN підтримує два режими передачі даних: UDP та TCP (див. рисунок 1.8).

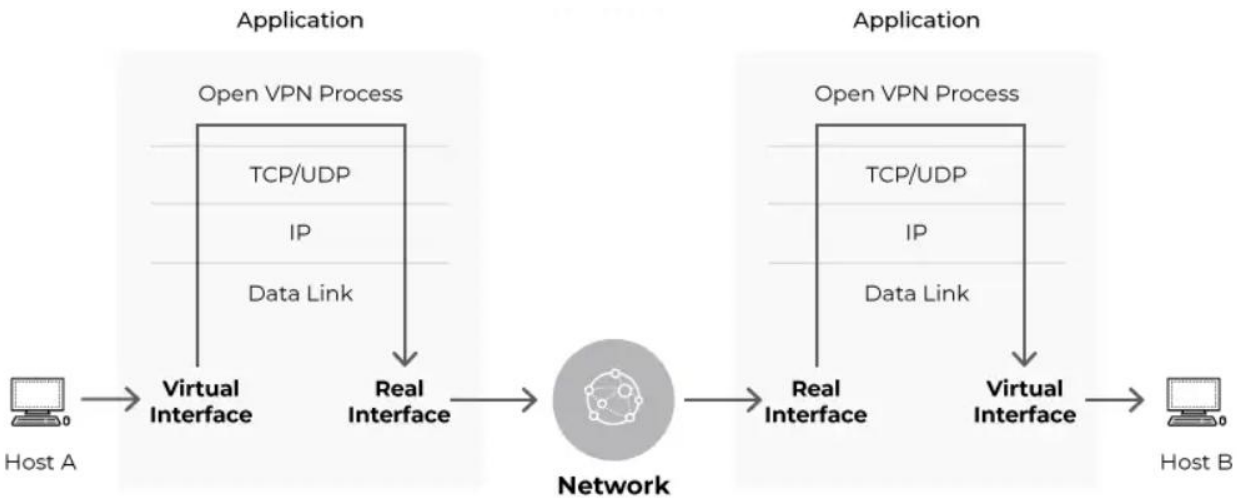

Рисунок 1.7 – OpenVPN протокол

UDP зазвичай використовується для швидких і легких з'єднань, оскільки він має низькі накладні витрати, що робить його ідеальним для стримінгу, онлайн-ігор і роботи з великими обсягами даних. TCP, навпаки, забезпечує високу надійність передачі даних, оскільки перевіряє кожен переданий пакет. Цей режим підходить для сценаріїв, де важлива стабільність з'єднання, наприклад, для передачі конфіденційної інформації або електронної пошти.

Гнучкість OpenVPN полягає в його здатності адаптуватися до різних мережевих середовищ. Він підтримує широкий спектр конфігурацій, включаючи Site-to-Site VPN, Remote Access VPN та гібридні мережі. OpenVPN також може

працювати через порт 443, що робить його дуже ефективним у мережах із суворими обмеженнями, оскільки цей порт зазвичай відкритий для HTTPS-трафіку. Завдяки цьому OpenVPN може обійти більшість мережевих фаєрволів та систем блокування трафіку. Безпека OpenVPN також підвищується за рахунок використання сертифікатів X.509 для автентифікації та попередньо спільних ключів (Pre-Shared Keys), які гарантують, що лише авторизовані пристрої можуть встановлювати з’єднання. Крім того, OpenVPN підтримує багатофакторну автентифікацію, що додає ще один рівень захисту.

OpenVPN сумісний із багатьма операційними системами, включаючи Windows, macOS, Linux, Android та iOS. Його підтримка є також на рівні маршрутизаторів і серверного обладнання, що робить його універсальним рішенням для будь-яких потреб. Він пропонує як графічний інтерфейс (GUI), так і текстову консоль для налаштування, що дозволяє як новачкам, так і досвідченим адміністраторам використовувати його з легкістю.

Продуктивність OpenVPN залежить від налаштувань і доступної пропускної здатності мережі. Хоча він може бути трохи повільнішим порівняно з сучасними протоколами, такими як WireGuard, його головними перевагами є безпека та надійність. OpenVPN також активно підтримується спільнотою та розробниками, що забезпечує постійне вдосконалення та оновлення.

Одним із недоліків OpenVPN є те, що його налаштування може бути складним для користувачів без технічного досвіду, особливо у випадках, коли потрібні специфічні конфігурації. Проте це компенсується численними інструкціями та підтримкою від спільноти.

1.4 Висновки до першого розділу

У першому розділі було проведено аналіз роботи VPN, розглянуто його основні принципи, сфери застосування, типи з'єднань та протоколів. Проаналізовано, як працює передача даних у відкритих мережах без VPN, та продемонстровано вразливість таких з'єднань до перехоплення, атак і втрати

конфіденційності. Було показано, що використання VPN забезпечує безпечну передачу даних завдяки шифруванню, тунелюванню та автентифікації.

Сфери застосування VPN були описані як у корпоративному середовищі, так і для особистого використання. Було зазначено, що VPN надає безпечний доступ до внутрішніх ресурсів організації, дозволяє обійти географічні обмеження, захищає користувачів у публічних мережах та забезпечує конфіденційність під час роботи в Інтернеті. Також розглянуто типи VPN-з'єднань, такі як Client-to-Site VPN для індивідуального використання і Site-to-Site VPN для організацій. Було продемонстровано, як ці з'єднання дозволяють безпечно об'єднувати мережі та забезпечувати захищений доступ до даних. Особливу увагу було приділено огляду VPN-протоколів, таких як L2TP/IPSec, IKEv2/IPSec, WireGuard та OpenVPN. Кожен із протоколів має свої переваги, недоліки та області застосування. Було зазначено, що OpenVPN забезпечує високу гнучкість і безпеку.

Таким чином, перший розділ закладає теоретичну основу для подальшого дослідження та практичного впровадження VPN. Розуміння принципів роботи VPN і особливостей кожного типу з'єднання та протоколу є критично важливим для вибору оптимального рішення, яке забезпечить захист даних, анонімність і надійність.

РОЗДІЛ 2 РОЗГОРТАННЯ ЛАБОРАТОРНОГО СЕРЕДОВИЩА

2.1 Використання гіпервізорів в середовищах тестування

Гіпервізори є важливим елементом у створенні та управлінні віртуальними середовищами для тестування, забезпечуючи гнучкість, масштабованість і ізоляцію ресурсів [16]. Вони дозволяють запускати кілька віртуальних машин (VM) на одному фізичному сервері, ефективно використовуючи апаратні ресурси та забезпечуючи відокремленість тестового середовища від основної інфраструктури. Використання гіпервізорів у тестових середовищах має низку переваг, які сприяють покращенню процесів розробки, тестування та експериментування з різними конфігураціями систем [17] [18].

Гіпервізори можуть бути двох основних типів: першого рівня (bare-metal) і другого рівня (hosted). Гіпервізори першого рівня, такі як VMware ESXi, Microsoft Hyper-V і XCP-ng, працюють безпосередньо на апаратному забезпеченні, забезпечуючи високу продуктивність і мінімальні затримки. Вони часто використовуються в корпоративних середовищах для створення високопродуктивних тестових інфраструктур. Гіпервізори другого рівня, такі як VirtualBox або VMware Workstation, встановлюються поверх операційної системи та забезпечують простоту налаштування та гнучкість, що робить їх популярними для персонального використання чи невеликих проєктів.

Однією з ключових переваг використання гіпервізорів у тестових середовищах є ізоляція. Віртуальні машини, створені на основі гіпервізора, працюють незалежно одна від одної, що дозволяє проводити тестування в ізольованих середовищах без ризику впливу на інші системи. Це особливо важливо при тестуванні шкідливого коду, експериментуванні з конфігураціями мережі або моделюванні реальних атак у сфері кібербезпеки. Гіпервізори також дозволяють швидко розгортати тестові середовища за допомогою шаблонів і клонування віртуальних машин. Це спрощує створення однотипних середовищ для багаторазового використання. Крім того, можливість створення знімків

(snapshots) віртуальних машин дозволяє повертатися до попередніх станів системи у разі збоїв або необхідності повторного тестування.

У середовищах тестування часто виникає потреба у моделюванні різних конфігурацій мережі, операційних систем і апаратного забезпечення. Гіпервізори дозволяють створювати віртуальні машини з різними операційними системами, такими як Windows, Linux або macOS, а також налаштовувати мережеві параметри для симуляції складних топологій. Це забезпечує реалістичні умови для тестування програмного забезпечення, мережевих протоколів і рішень галузі кібербезпеки. Використання гіпервізорів також сприяє ефективному використанню апаратних ресурсів. Завдяки можливості динамічного розподілу CPU, пам’яті та дискового простору між віртуальними машинами, гіпервізори дозволяють оптимізувати використання обчислювальних ресурсів і знижувати витрати на створення тестових середовищ. Це особливо корисно в умовах обмеженого бюджету або потреби в економії енергії.

У сфері кібербезпеки гіпервізори активно використовуються для створення тестових полігонів де можна безпечно аналізувати підозріле програмне забезпечення або моделювати атаки [18]. Такі середовища дозволяють імітувати різні сценарії загроз і оцінювати ефективність захисних механізмів, таких як антивірусні програми чи системи виявлення вторгнень [17].

Гіпервізори також використовуються для автоматизації тестування за допомогою інтеграції з інструментами DevOps, такими як Ansible або Terraform. Це дозволяє створювати складні тестові середовища, розгортати їх заздалегідь визначеними сценаріями та автоматично збирати результати тестування. Такий підхід підвищує ефективність роботи команд розробки та тестування, скорочуючи час на ручну конфігурацію та аналіз результатів.

Oracle VM VirtualBox - це hosted гіпервізор, який дозволяє створювати і керувати віртуальними машинами на різних операційних системах [19]. Його використання у тестовому середовищі забезпечує легкість налаштування та можливість створення ізольованих середовищ для тестування програмного забезпечення, мережевих конфігурацій або безпекових сценаріїв. VirtualBox забезпечує можливість створення кількох віртуальних машин на одному

фізичному пристрої, дозволяючи ефективно використовувати апаратні ресурси. Користувач може налаштовувати кількість виділених ресурсів для кожної ВМ, таких як процесорні ядра, оперативна пам’ять та обсяг дискового простору. Це дає змогу створювати середовища, які відповідають конкретним вимогам тестування, наприклад, моделювати сервери, робочі станції або мережеві пристрої. Однією з ключових переваг VirtualBox є його підтримка широкого спектра операційних систем як гостьових. Це дозволяє створювати тестове середовище з різними операційними системами, такими як Windows, Linux, MacOS або Unix, що є корисним для перевірки сумісності програмного забезпечення чи симуляції гетерогенної мережі.

У VirtualBox реалізована підтримка функцій, які роблять його зручним для тестування. Зокрема, можливість створення знімків стану (snapshots) дозволяє зберігати поточний стан віртуальної машини та повертатися до нього у разі збоїв або необхідності повторного тестування. Це особливо корисно для експериментів, де може знадобитися багаторазове відновлення середовища до початкового стану. Для побудови складніших середовищ VirtualBox підтримує налаштування віртуальних мереж. Це дозволяє моделювати різноманітні мережеві топології, створювати ізольовані мережі, встановлювати NAT-з’єднання або створювати мережі типу "міст" (bridge). Завдяки цьому тестове середовище може включати декілька віртуальних машин, які взаємодіють одна з одною через віртуальні мережі, моделюючи роботу в реальних умовах. VirtualBox також підтримує функцію спільних папок (shared folders), яка дозволяє обмінюватися файлами між гостьовою і хостовою операційними системами. Це спрощує процес тестування, оскільки користувач може легко переносити дані або результати тестування між системами.

Для автоматизації налаштувань і тестування VirtualBox надає засоби командного рядка (VBoxManage), що дозволяють створювати, налаштовувати та керувати віртуальними машинами за допомогою скриптів. Це особливо корисно для тестових сценаріїв, які вимагають повторюваних дій. Важливим моментом, що до VirtualBox є те що він безкоштовний, що робить його доступним для широкого кола користувачів, включаючи індивідуальних розробників, невеликі

команди та освітні установи. Попри це, VirtualBox забезпечує достатньо потужний функціонал, який підходить навіть для складних сценаріїв тестування.

Використання VirtualBox у тестовому середовищі є оптимальним вибором для задач, які вимагають гнучкого управління, багатоплатформності та можливості створення ізольованих середовищ. Він забезпечує баланс між функціональністю, простотою використання та доступністю, що робить його популярним інструментом для створення та управління віртуальними середовищами у сфері тестування.

2.2 Схема лабораторного середовища тестування

Лабораторне середовище тестування, побудоване на основі Oracle VM VirtualBox, забезпечує ізоляцію та масштабованість, необхідні для проведення експериментів і перевірок у безпечному та контрольованому середовищі. Хостова машина повинна мати достатньо апаратних ресурсів, таких як оперативна пам’ять, процесорні ядра та дисковий простір, щоб забезпечити одночасну роботу кількох віртуальних машин.

Схема лабораторного середовища тестування демонструє організацію мережевої інфраструктури для перевірки роботи OpenVPN на основі гіпервізора Oracle VM VirtualBox (див. рисунок 2.1).

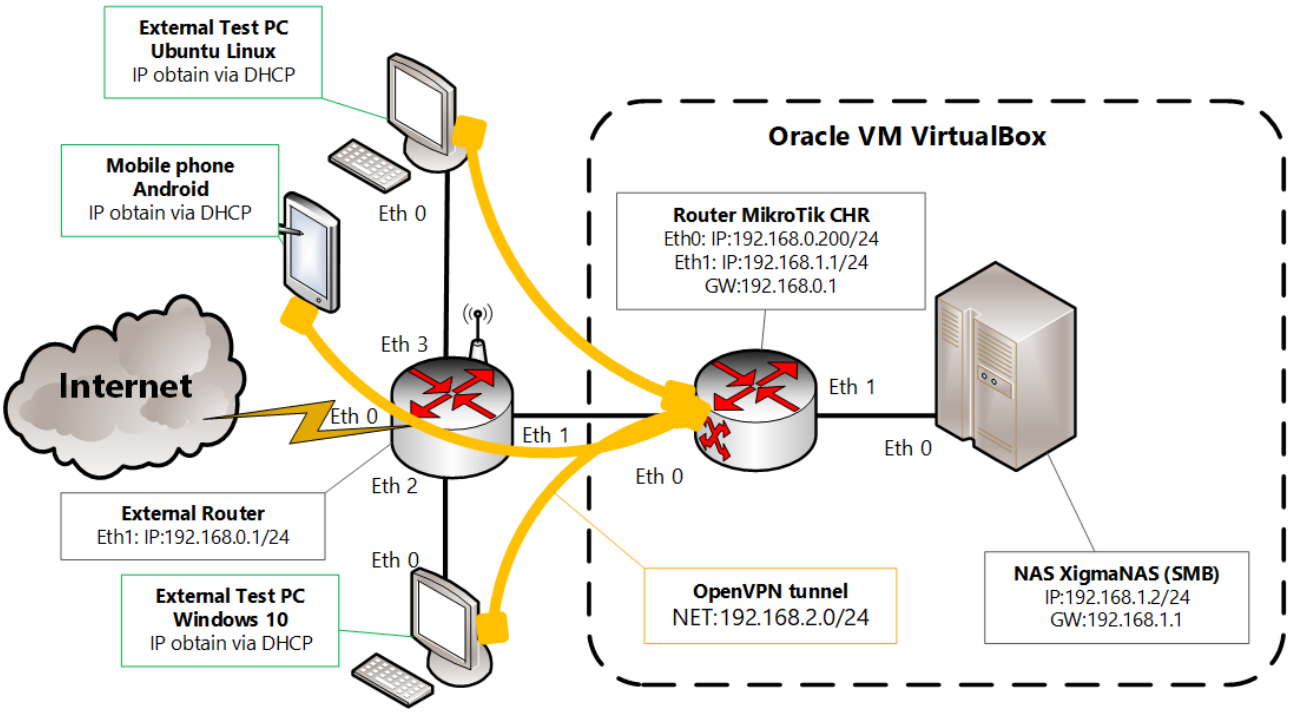

Рисунок 2.1 – Схема середовища тестування

У центрі середовища знаходиться маршрутизатор MikroTik CHR, який виконує роль основного мережевого вузла для управління трафіком, створення VPN-тунелю та взаємодії між різними пристроями й мережами. Цей маршрутизатор підключений до зовнішнього маршрутизатора (External Router), що забезпечує доступ до Інтернету.

На маршрутизаторі MikroTik CHR налаштовано кілька мережевих інтерфейсів. До зовнішнього маршрутизатора підключено інтерфейс Eth0 маршрутизатора MikroTik з IP-адресою 192.168.0.200/24. Цей інтерфейс відповідає за передачу трафіку до зовнішньої мережі. Другий інтерфейс Eth1 підключено до внутрішньої мережі (192.168.1.0/24), де розташований NAS-сервер XigmaNAS. NAS-сервер має IP-адресу 192.168.1.2 і функціонує як файлове сховище з доступом через SMB-протокол. VPN-тунелі використовують мережу 192.168.2.0/24, що дає можливість взаємодії віддаленим пристроям, таким як мобільний телефон Android або тестовий ПК на Windows 10 чи Ubuntu Linux з ресурсами локальної мережі.

Мобільний телефон Android і зовнішні тестовs ПК, які отримують IP-адреси через DHCP, використовуються для перевірки з’єднань з OpenVPN. Підключення цих пристроїв до VPN дозволяє протестувати різні сценарії, такі як

доступ до внутрішніх ресурсів мережі або забезпечення анонімності під час виходу в Інтернет через VPN-тунель.

У віртуальному середовищі Oracle VM VirtualBox маршрутизатор MikroTik і NAS-сервер розгорнуті як віртуальні машини, що забезпечує ізоляцію середовища і зручність налаштування.

Ця конфігурація забезпечує надійну перевірку функціональності VPN-тунелю, тестування доступу до внутрішніх ресурсів мережі, таких як NAS, а також аналіз продуктивності з'єднання через різні типи клієнтських пристроїв. Схема лабораторного середовища дозволяє реалізувати сценарії моделювання реальних умов використання VPN, забезпечуючи безпеку, ізоляцію та повторюваність тестів.

2.3 Програмний маршрутизатор Mikrotik

MikroTik CHR – це програмний маршрутизатор, розроблений компанією MikroTik [20], який працює у вигляді віртуальної машини на гіпервізорах, таких як Oracle VM VirtualBox, VMware, Hyper-V, KVM або інші платформи віртуалізації. MikroTik CHR призначений для виконання функцій маршрутизації, брандмауера, VPN-сервера, NAT і інших мережевих завдань, забезпечуючи той самий функціонал, що і фізичні маршрутизатори MikroTik, але з можливістю запуску в хмарному середовищі або на локальній віртуальній машині. MikroTik CHR базується на операційній системі RouterOS, яка забезпечує широкий набір мережевих інструментів.

RouterOS – це спеціалізована мережева операційна система, розроблена компанією MikroTik, яка забезпечує широкі можливості для налаштування, управління та контролю мережевої інфраструктури [21]. Вона є основою для програмного маршрутизатора MikroTik CHR і фізичних пристроїв MikroTik. RouterOS розроблена для забезпечення продуктивності, надійності та масштабованості в мережевих середовищах різного масштабу від домашніх мереж до великих корпоративних і ISP рішень. RouterOS включає функціонал, який дозволяє виконувати завдання маршрутизації, брандмауера, VPN,

балансування навантаження, управління пропускною здатністю, а також моніторингу та аналізу трафіку. Вона підтримує різноманітні протоколи маршрутизації, такі як OSPF, BGP, RIP та MPLS, що робить її потужним інструментом для побудови динамічних і складних мережевих топологій.

Брандмауер в RouterOS дозволяє створювати правила для фільтрації трафіку, управління доступом, а також забезпечення безпеки мережі. Адміністратори можуть налаштовувати фільтрацію за IP-адресами, портами, протоколами та іншими параметрами, що дозволяє захистити мережу від зовнішніх атак і внутрішніх загроз. Крім того, брандмауер RouterOS підтримує функцію NAT, яка використовується для маскування внутрішніх IP-адрес і надання спільного доступу до Інтернету.

RouterOS також має потужний функціонал для організації VPN-з'єднань. Вона підтримує різноманітні VPN-протоколи, включаючи OpenVPN, L2TP/IPSec, PPTP, SSTP і WireGuard, що дозволяє створювати захищені канали для віддаленого доступу або з'єднання між офісами. Цей функціонал забезпечує конфіденційність і безпеку переданих даних навіть у незахищених мережах.

Функція управління пропускною здатністю в RouterOS дозволяє налаштовувати черги (queues) для обмеження швидкості передачі даних для окремих користувачів або сервісів. Це корисно для оптимізації використання ресурсів мережі, забезпечення пріоритетів для важливих додатків і зменшення перевантаження мережі. Шейпінг трафіку, реалізований у RouterOS, дозволяє ефективно розподіляти доступну пропускну здатність між користувачами. RouterOS включає інструменти для моніторингу та аналізу мережевого трафіку. Вона підтримує журналювання подій, графіки використання ресурсів і реальний час моніторингу трафіку через інструменти, такі як Torch і Packet Sniffer. Це дозволяє мережевим адміністраторам відслідковувати активність у мережі, діагностувати проблеми та оптимізувати роботу системи. Система також забезпечує підтримку бездротових мереж. Вона може працювати як точка доступу, клієнт або ретранслятор у Wi-Fi-мережах, підтримуючи стандарти IEEE 802.11. RouterOS дозволяє налаштовувати мережі з декількома SSID, захистом

WPA/WPA2 та іншими функціями, необхідними для побудови надійних бездротових інфраструктур.

Адміністрування RouterOS здійснюється через кілька інтерфейсів, включаючи текстовий CLI, інструмент Winbox для роботи через графічний інтерфейс, веб-інтерфейс і API для автоматизації завдань.

На рисунку 2.2 показано веб-інтерфейс для входу в RouterOS, який використовується для управління маршрутизаторами MikroTik.

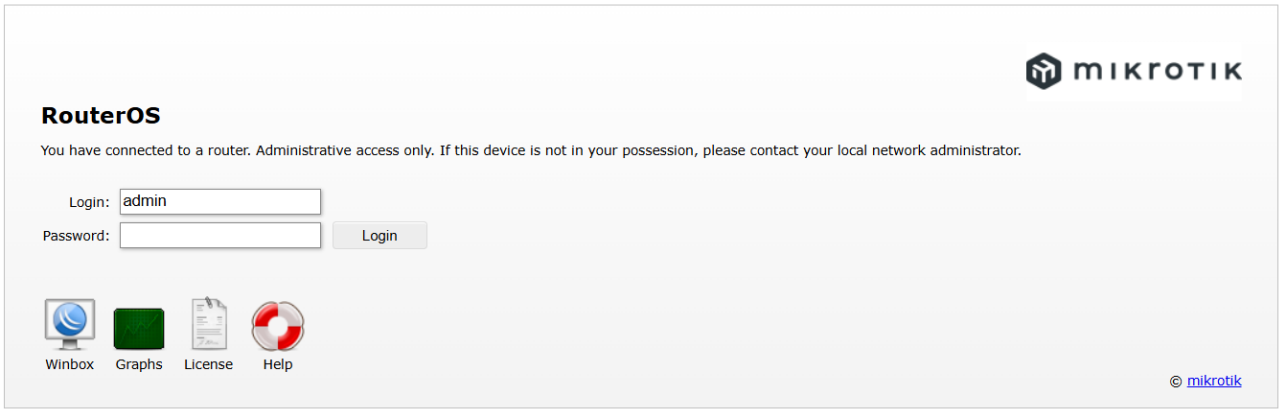

Рисунок 2.2 – Веб-інтерфейс для управління маршрутизаторами MikroTik

Веб-інтерфейс RouterOS забезпечує базовий доступ до налаштувань маршрутизатора, але для більш складних операцій зазвичай використовується CLI. Веб-інтерфейс є зручним для швидкого доступу до основних функцій або для користувачів, які віддають перевагу роботі через веб-браузер. Він дає змогу переглядати графіки використання ресурсів маршрутизатора, таких як пропускна здатність інтерфейсів, використання центрального процесора, оперативної пам’яті та дискового простору. Це дозволяє адміністраторам відслідковувати продуктивність маршрутизатора в реальному часі та діагностувати потенційні проблеми.

RouterOS також підтримує оновлення програмного забезпечення, що дозволяє отримувати нові функції, виправлення вразливостей і покращення продуктивності. Система має ліцензійну модель, яка включає кілька рівнів доступу до функцій, що дозволяє адаптувати її до потреб різних користувачів.

На рисунку 2.3 представлено веб-інтерфейс управління інтерфейсами маршрутизатором MikroTik.

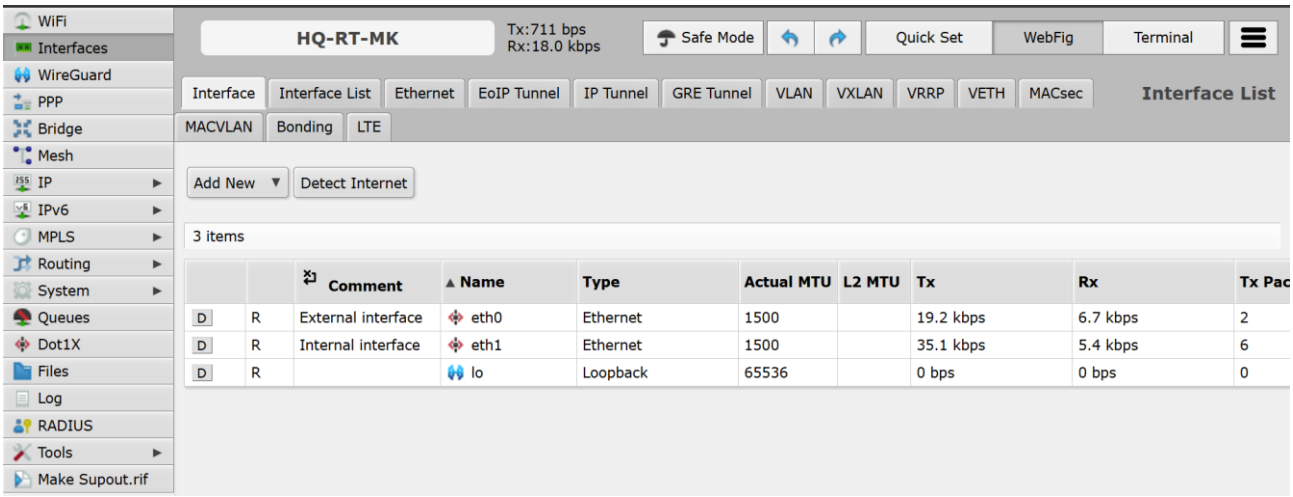

Рисунок 2.3 – Веб-інтерфейс управління інтерфейсами маршрутизатором MikroTik

Поточний екран показує список інтерфейсів, налаштованих на пристрої, з їхніми параметрами та статистикою трафіку. У списку інтерфейсів наведені три активні інтерфейси: зовнішній (eth0), внутрішній (eth1) та петлі (loopback).

На рисунку 2.4 представлено веб-інтерфейс управління IP-адресами маршрутизатором MikroTik.

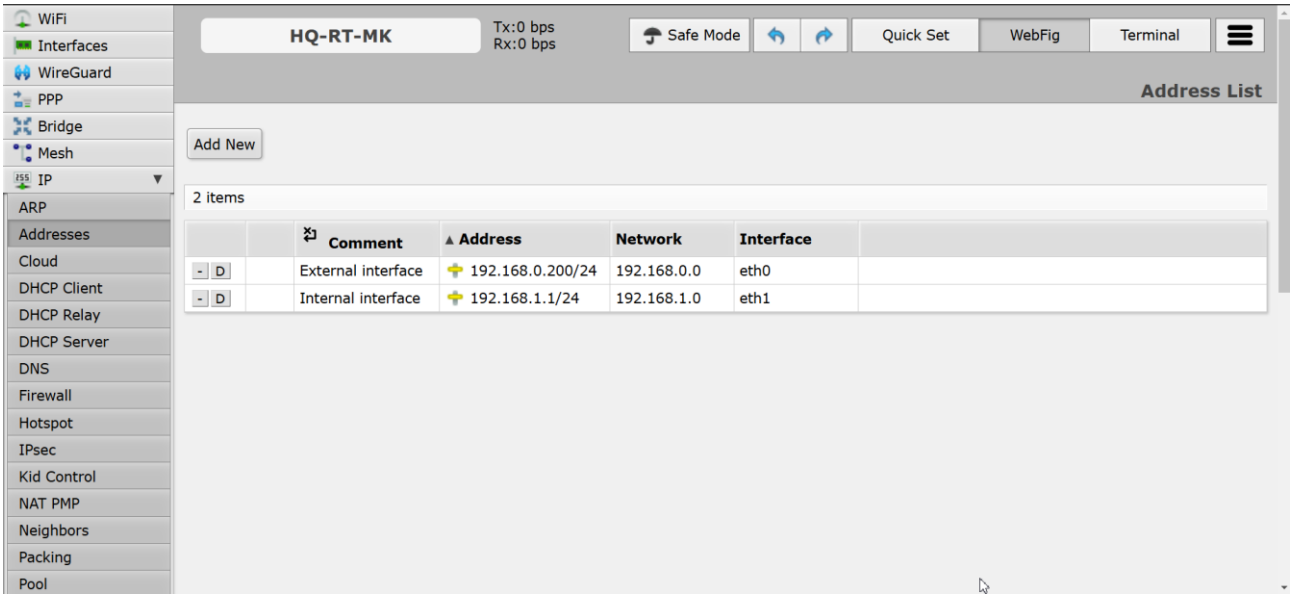

Рисунок 2.4 – Веб-інтерфейс управління IP-адресами маршрутизатором MikroTik

Є два активні записи: зовнішній інтерфейс (External interface) та внутрішній інтерфейс (Internal interface). Зовнішній інтерфейс має IP-адресу 192.168.0.200/24, що належить до мережі 192.168.0.0/24, і прив'язаний до інтерфейсу eth0. Цей інтерфейс використовується для підключення маршрутизатора до зовнішньої мережі або Інтернету. Внутрішній інтерфейс має IP-адресу 192.168.1.1/24, яка належить до локальної мережі 192.168.1.0/24, і прив'язаний до інтерфейсу eth1. Цей інтерфейс забезпечує зв’язок маршрутизатора з внутрішніми пристроями локальної мережі.

На рисунку 2.5 представлено розділ маршрутизації у веб-інтерфейсі MikroTik RouterOS.

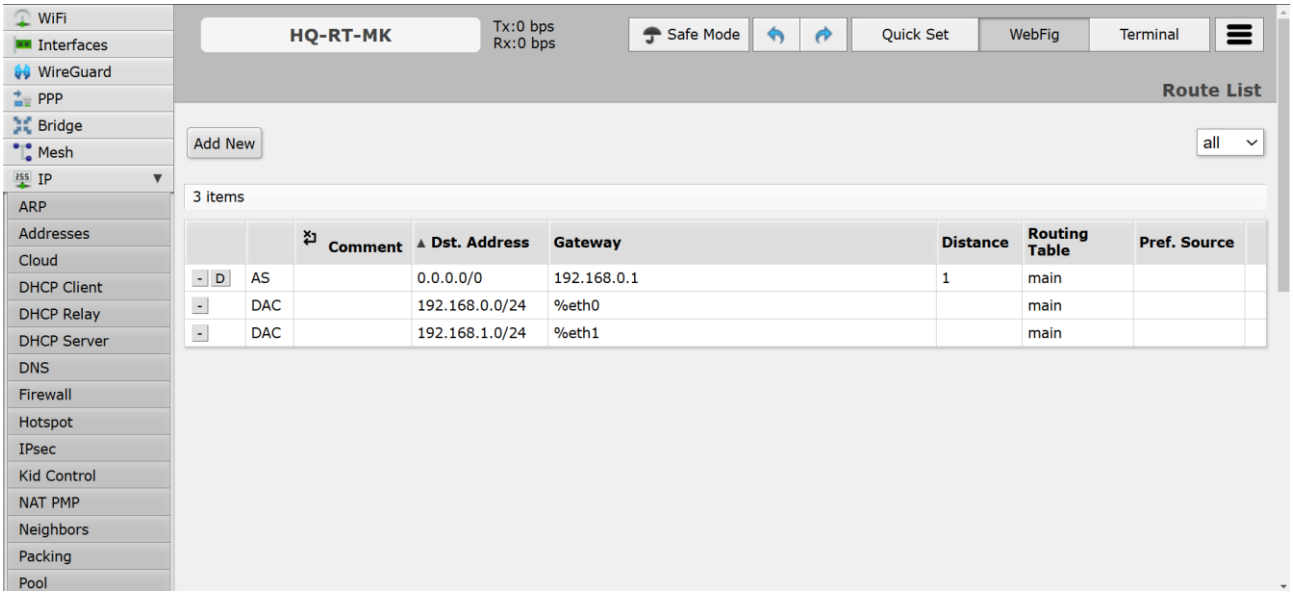

Рисунок 2.5 – Веб-інтерфейс управління розділом маршрутизації в MikroTik

Цей розділ відображає список маршрутів, які маршрутизатор використовує для передачі трафіку до відповідних мереж. Перший маршрут вказує на маршрут за замовчуванням (0.0.0.0/0), що використовується для передачі трафіку до будь-якої адреси, яка не належить до локальних мереж. Шлюз для цього маршруту визначений як 192.168.0.1, що відповідає шлюзу зовнішньої мережі. Цей маршрут має метрику зі значенням 1, що означає його високу пріоритетність. Другий і третій маршрути позначені як DAC (Directly Attached Connected). Ці маршрути автоматично створюються для кожної локальної мережі,

налаштованої на маршрутизаторі, і забезпечують прямий доступ до цих підмереж без потреби в додаткових шлюзах.

На рисунку 2.6 показано налаштування DNS на маршрутизаторі MikroTik через веб-інтерфейс.

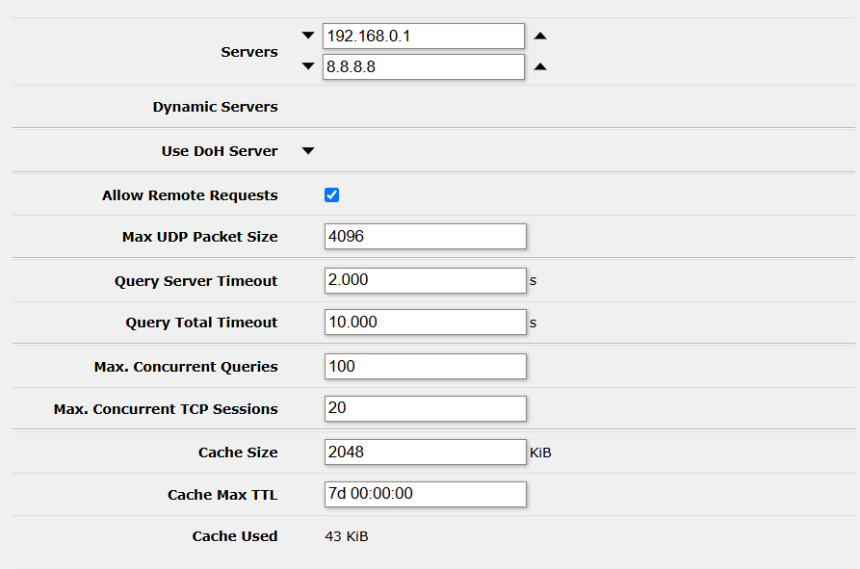

Рисунок 2.6 – Веб-інтерфейс налаштування DNS в MikroTik

У конфігурації задані два DNS-сервери: 192.168.0.1 (локальний сервер) та 8.8.8.8 (публічний DNS-сервер Google). Це дозволяє маршрутизатору використовувати ці сервери для перетворення доменних імен.

На рисунку 2.7 представлено розділ Firewall у веб-інтерфейсі MikroTik RouterOS, де налаштовані правила фільтрації трафіку (Filter Rules).

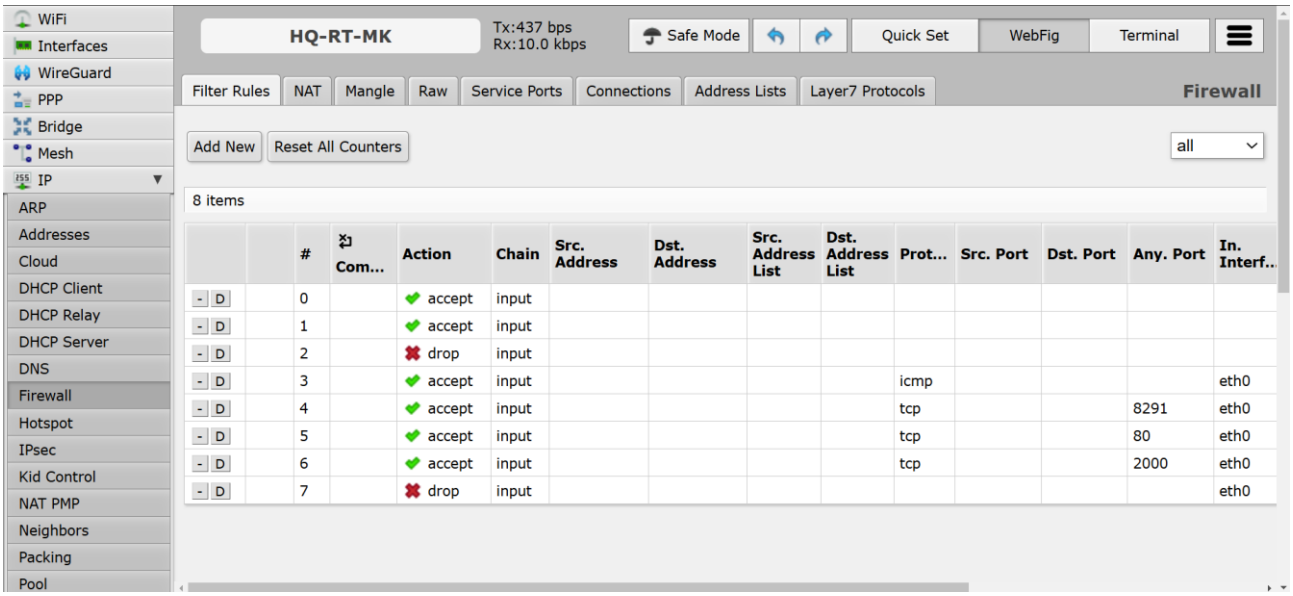

Рисунок 2.7 – Веб-інтерфейс налаштування Filter Rules в MikroTik

Цей розділ дозволяє адміністратору створювати, редагувати та управляти правилами брандмауера для контролю трафіку в мережі.

У таблиці відображаються вісім активних правил, кожне з яких має кілька ключових параметрів. Поле Action вказує, яку дію виконуватиме маршрутизатор, наприклад, accept для дозволу трафіку або drop для його блокування. Поле Chain визначає, на якому етапі обробляється трафік: у цьому випадку використовується input, що означає обробку вхідного трафіку, який прямує до самого маршрутизатора.

На рисунку 2.8 відображено розділ Firewall у веб-інтерфейсі MikroTik RouterOS, де налаштовані правила NAT.

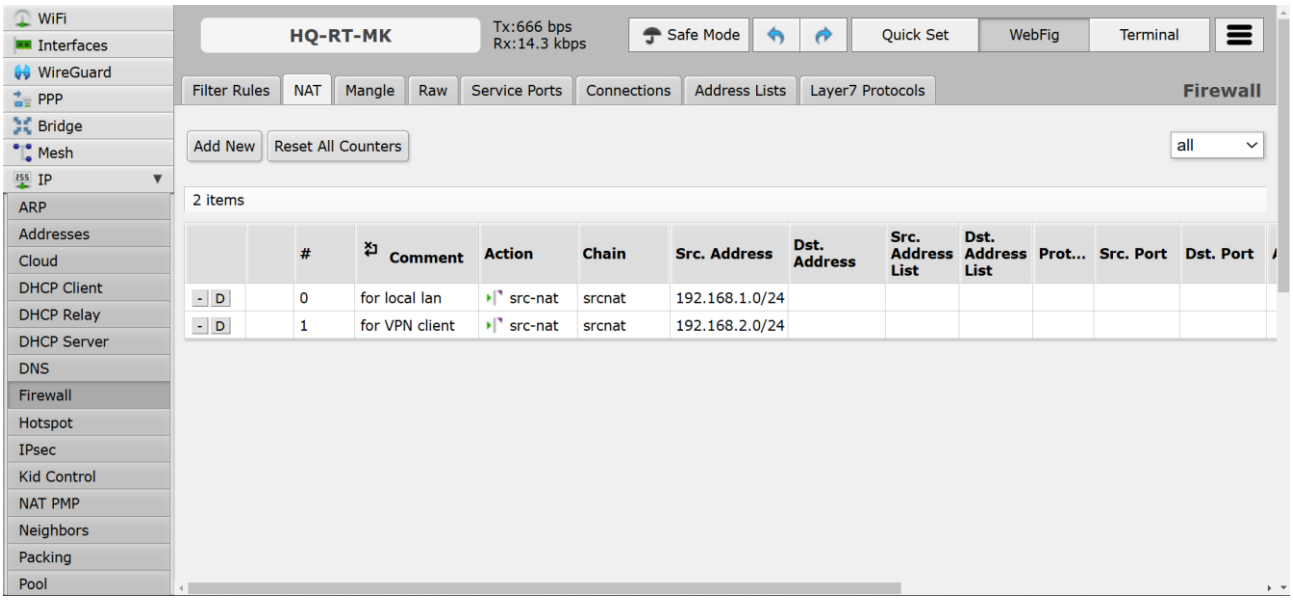

Рисунок 2.8 – Веб-інтерфейс налаштування NAT в MikroTik

Цей розділ дозволяє адміністратору управляти трансляцією мережевих адрес. Таблиця містить два активні правила, які використовують ланцюжок srcnat (source NAT) для трансляції вихідних адрес у зазначених підмережах. Поле Action для обох правил встановлене як "src-nat", що означає трансляцію вихідних IP-адрес з підмінною на IP-адресу маршрутизатора при виході в іншу мережу.

2.4 NAS-сервер XigmaNAS

XigmaNAS - це операційна система з відкритим вихідним кодом, розроблена для створення та управління мережевим сховищем даних [22]. Вона заснована на системі FreeBSD і є одним із популярних рішень для створення файлових серверів, медіасерверів і резервного копіювання в корпоративних середовищах. XigmaNAS підтримує широкий набір мережевих протоколів і технологій, що робить її гнучким і надійним інструментом для управління даними.

На рисунку 2.9 представлено консольне меню NAS-сервера XigmaNAS.

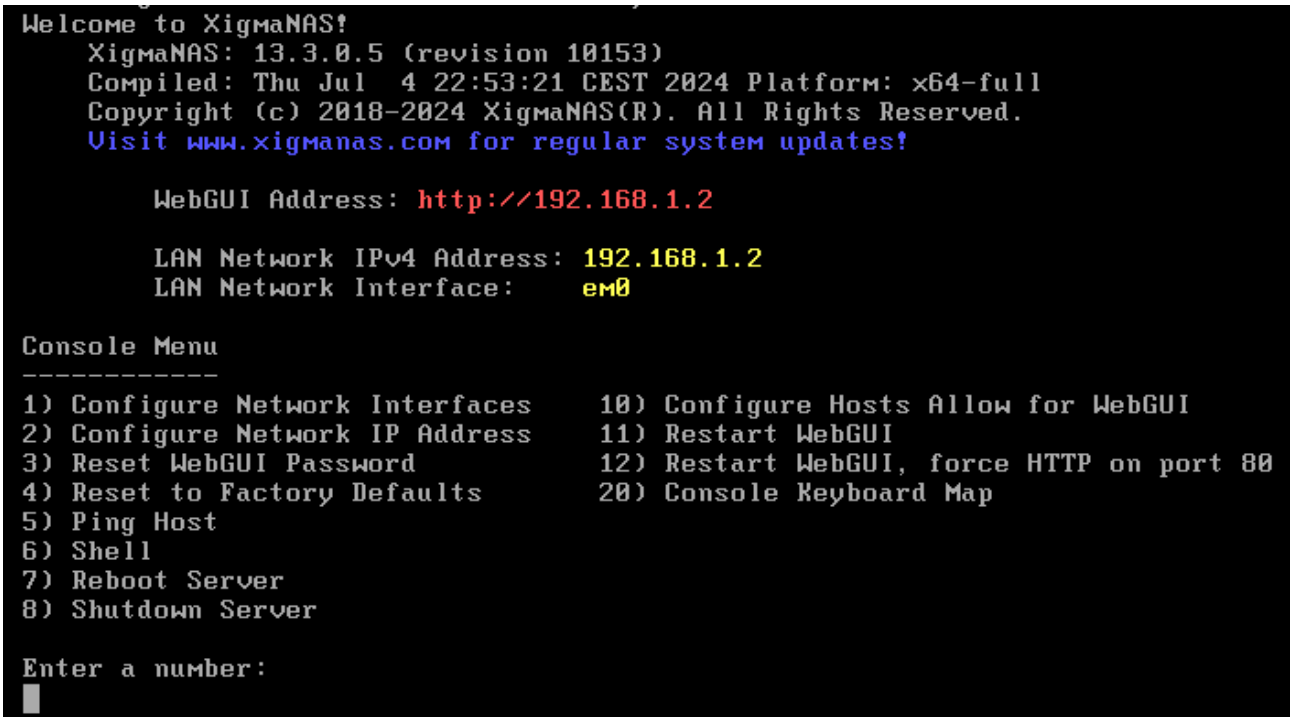

Рисунок 2.9 – Консольне меню NAS-сервера XigmaNAS

Головний екран містить інформацію про систему IP-адресу локального мережевого інтерфейсу 192.168.1.2. Меню дозволяє виконувати базові налаштування і дії для керування сервером.

Система XigmaNAS пропонує користувачам інтуїтивно зрозумілий веб-інтерфейс для адміністрування, що дозволяє легко виконувати налаштування, навіть без глибоких технічних знань (див. рисунок 2.10).

На рисунку 2.10 показано інформаційну панель веб-інтерфейсу XigmaNAS, що надає детальну інформацію про поточний стан системи.

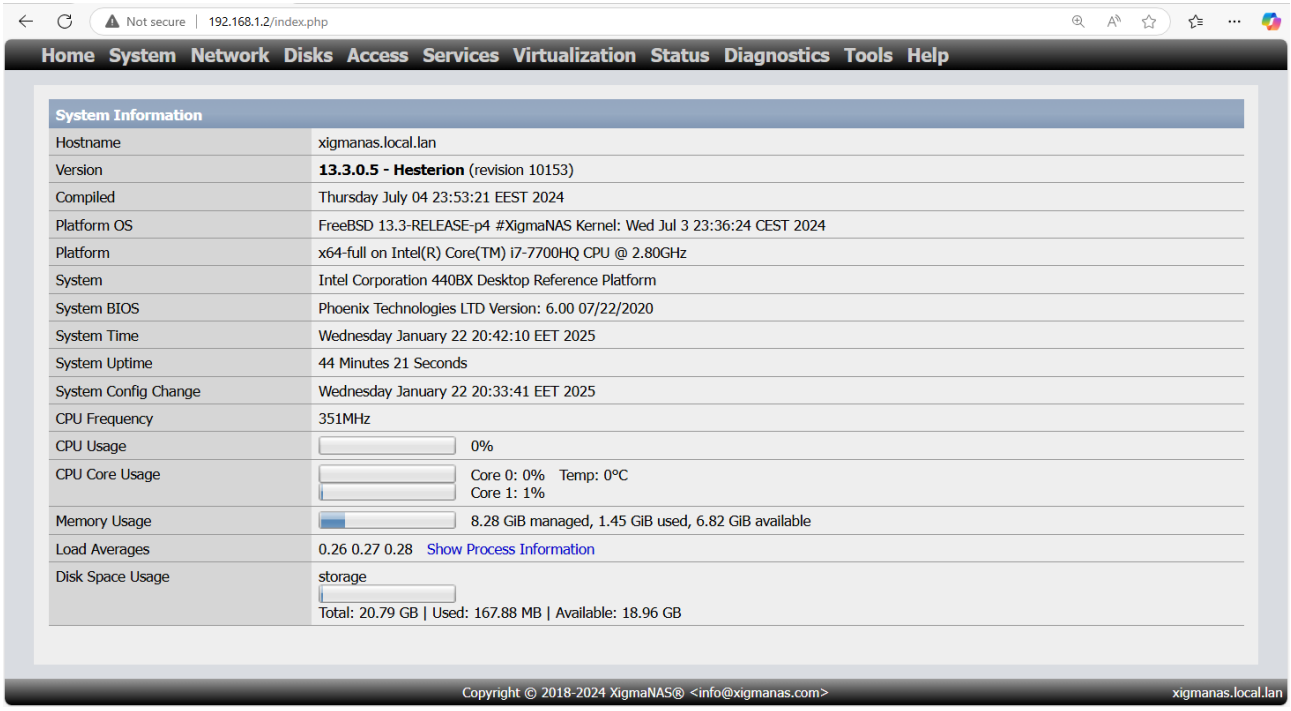

Рисунок 2.10 – Інформаційна панель веб-інтерфейсу XigmaNAS

Панель містить розділ System Information, який відображає основні параметри системи та її апаратної конфігурації. Цей інтерфейс надає інформацію про стан системи в реальному часі, що дозволяє адміністратору швидко оцінити продуктивність і виявити можливі проблеми.

Через веб-інтерфейс можна налаштувати мережеві підключення, створити файлові системи, налаштувати доступ через різні протоколи і моніторити стан сервера. Система також підтримує створення RAID-масивів для підвищення надійності та продуктивності зберігання даних. XigmaNAS підтримує апаратні й програмні конфігурації RAID, включаючи RAID 0, RAID 1, RAID 5 та RAID 10. Завдяки цьому забезпечується стійкість до відмови дисків і збільшується швидкість обробки даних. Однією з ключових особливостей XigmaNAS є підтримка файлової системи ZFS, яка забезпечує високий рівень захисту даних, підтримку моментальних копій (snapshots) і легке управління томами. ZFS дозволяє виявляти та виправляти пошкодження даних у реальному часі, а також створювати резервні копії без переривання роботи системи.

На рисунку 2.11 показано розділ для управління точками монтування у веб-інтерфейсі XigmaNAS.

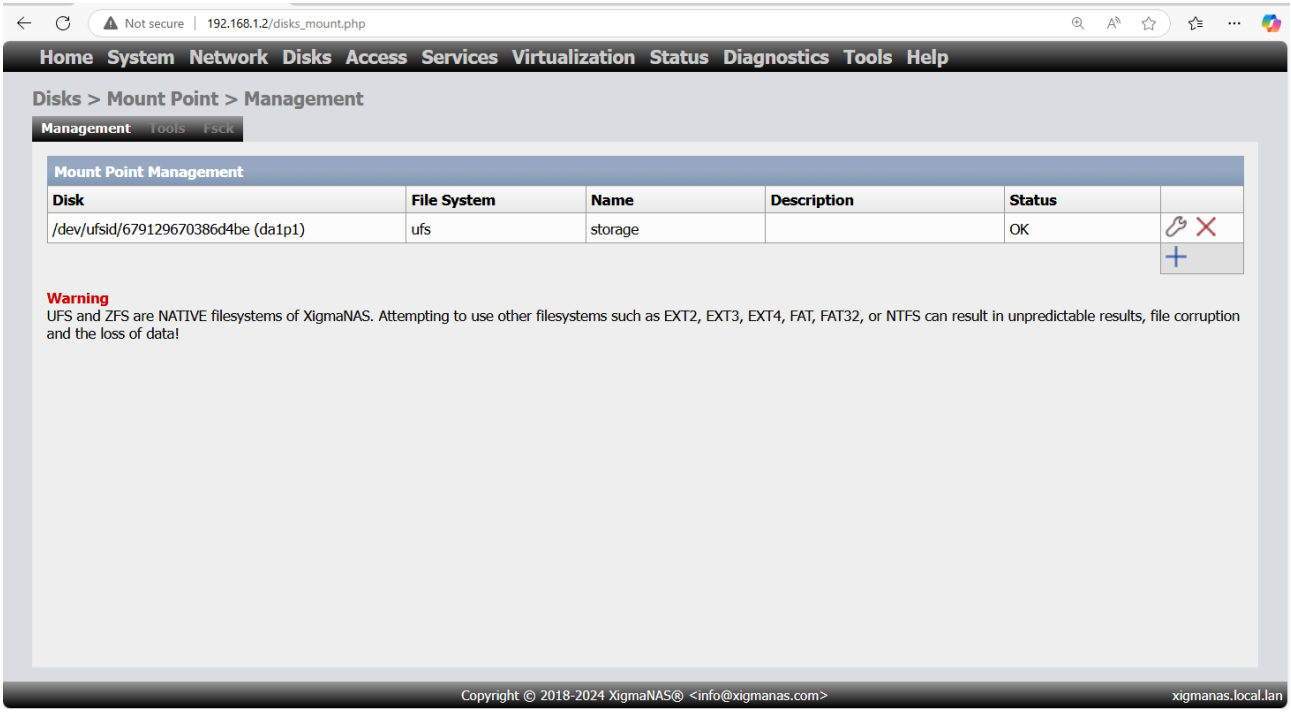

Рисунок 2.11 – Управління точками монтування в XigmaNAS

Поле File System вказує, що диск форматовано у файлову систему UFS (Unix File System), яка є рідною для XigmaNAS.

Цей інтерфейс надає адміністраторам можливість ефективно керувати точками монтування, перевіряти статус дисків і налаштовувати файлові системи для оптимального використання. Завдяки підтримці UFS і ZFS система гарантує високу продуктивність і захист даних, що робить її ідеальним рішенням для зберігання важливої інформації.

XigmaNAS підтримує популярні протоколи доступу до файлів, включаючи SMB/CIFS (Microsoft Windows), NFS (Unix/Linux) і AFP (Apple). Це дозволяє організувати спільний доступ до даних для пристроїв із різними операційними системами. Для забезпечення захисту даних система підтримує автентифікацію користувачів, доступ на основі ролей та шифрування файлів.

На рисунку 2.12 показано налаштування служби SMB (Samba) у XigmaNAS. Служба SMB використовується для забезпечення спільного доступу до файлів і папок у локальній мережі для клієнтів, що працюють на операційних системах Windows, macOS і Linux.

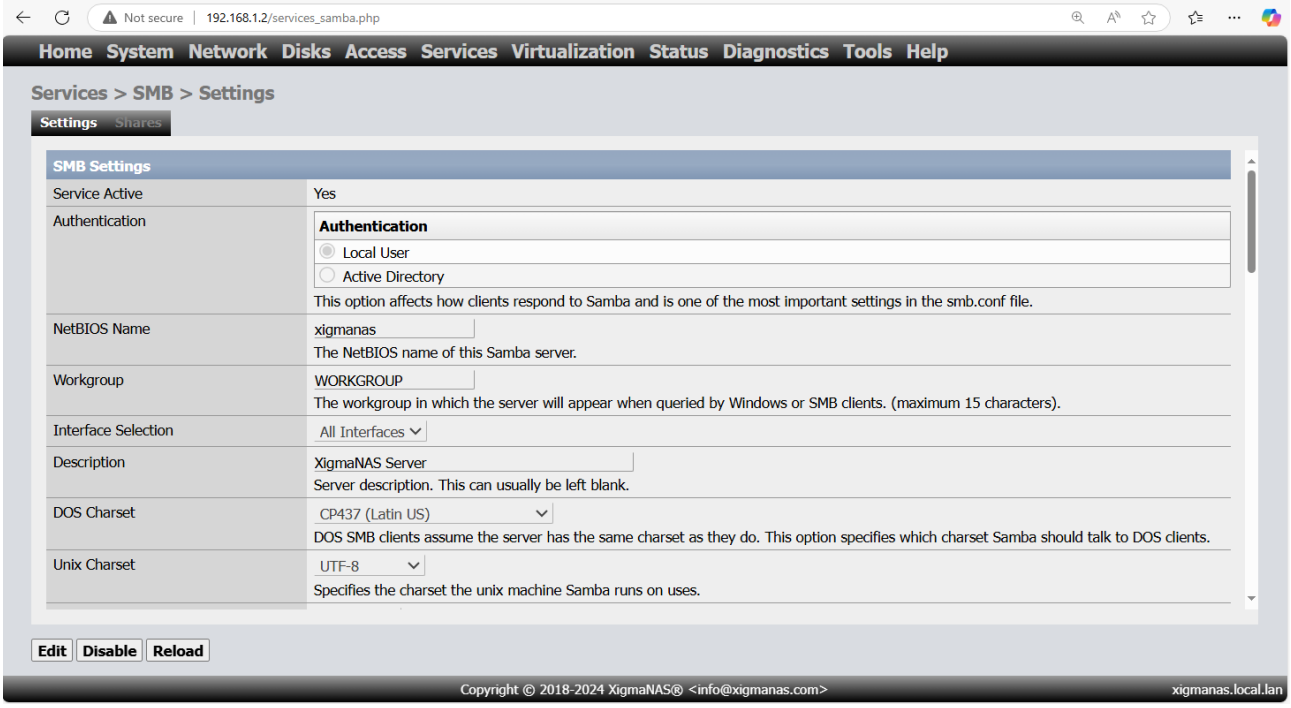

Рисунок 2.12 – Налаштування служби SMB в XigmaNAS

Це налаштування забезпечує гнучкість і сумісність сервера SMB із різними клієнтськими системами, дозволяючи налаштовувати автентифікацію, інтерфейси та робочу групу. Використання локальної бази користувачів є зручним для невеликих мереж, де немає необхідності в складній інтеграції з доменом.

На рисунку 2.13 показано налаштування спільного доступу до папки через службу Samba в XigmaNAS.

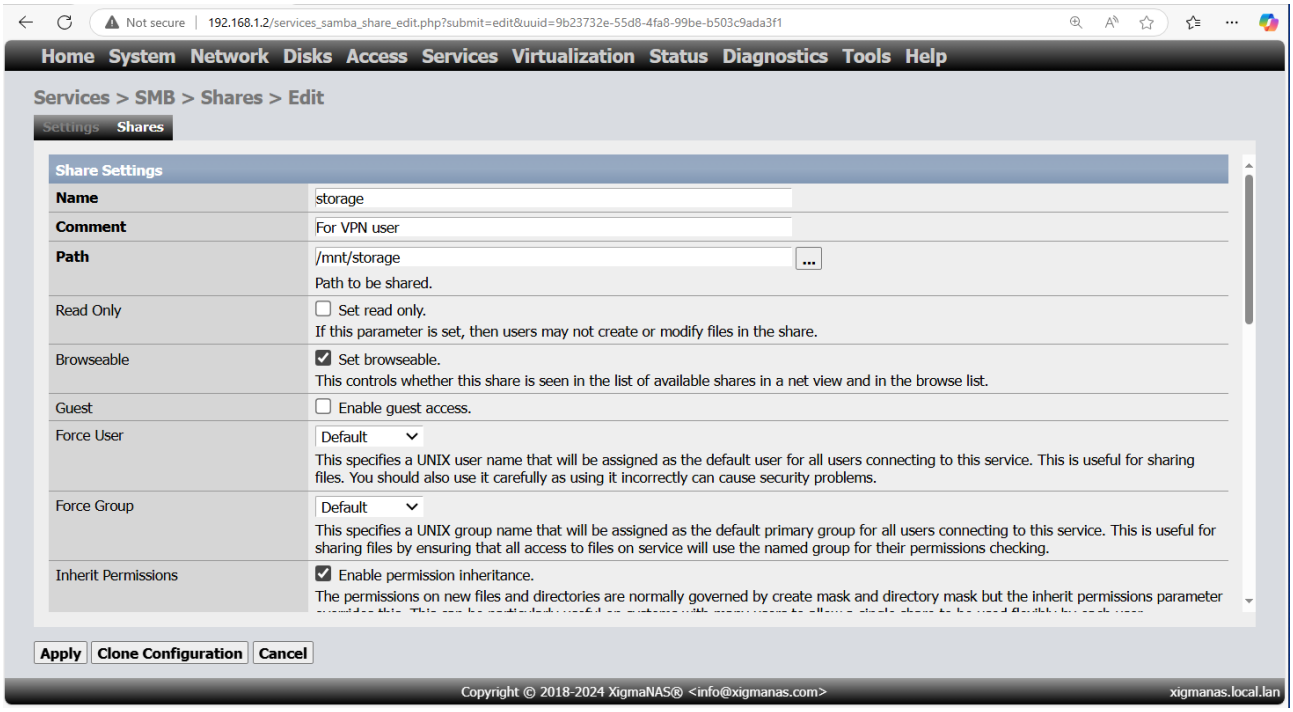

Рисунок 2.13 – Налаштування спільного доступу до папки через службу Samba в XigmaNAS

Розділ Share Settings дозволяє налаштовувати параметри для спільного ресурсу, який буде доступний у локальній мережі. У даному випадку ім'я ресурсу - storage. Шлях до папки, яка надається в спільний доступ задано як /mnt/storage.

Параметр Browseable увімкнено, що означає, що ресурс буде відображатися у списку доступних папок для користувачів SMB. Це полегшує виявлення ресурсу для підключення. Параметр Inherit Permissions увімкнено, що означає, що нові файли й папки, створені в ресурсі, успадковуватимуть права доступу від батьківської папки. Це спрощує управління правами доступу для нових елементів.

Ці налаштування дозволяють адміністратору точно визначити, як ресурс буде використовуватися і хто матиме до нього доступ. Завдяки можливостям налаштування доступу, прав і успадкування дозволів, цей інтерфейс надає ефективний інструмент для управління спільними ресурсами у мережі.

XigmaNAS підтримує розгортання на широкому спектрі обладнання, включаючи старі комп'ютери, сучасні сервери та віртуальні середовища. Це дозволяє легко інтегрувати систему у вже існуючу інфраструктуру без необхідності придбання додаткового обладнання. Завдяки своїй гнучкості,

підтримці багатьох протоколів і можливостям розширення XigmaNAS є надійним інструментом для організації мережевого сховища. Вона може використовуватися як у малих офісах так і у великих корпоративних середовищах, де необхідне централізоване зберігання й управління даними.

2.5 Висновки до другого розділу

В другому розділі було розглянуто процес розгортання лабораторного середовища тестування на основі гіпервізора Oracle VM VirtualBox та програмного маршрутизатора MikroTik CHR. Описано використання гіпервізорів для створення віртуальних середовищ, їхніх переваг та можливості для створення тестового середовища. Показано, що Oracle VM VirtualBox, забезпечує гнучкість, масштабованість і можливість створення ізольованих середовищ для безпечного тестування.

Було детально описано організацію лабораторного середовища, включаючи побудову мережевої інфраструктури для тестування OpenVPN, де центральним елементом є маршрутизатор MikroTik CHR. Його роль у маршрутизації трафіку, налаштуванні VPN-тунелів і управлінні мережевими інтерфейсами була розглянута через функціональні можливості RouterOS. Налаштування брандмауера, DNS, NAT і маршрутизації дозволили створити захищене й оптимізоване середовище для взаємодії локальних і віддалених пристроїв. Також було описано NAS-сервер XigmaNAS, який виконує роль файлового сховища в тестовому середовищі. Розглянуто його можливості, зокрема підтримку різних файлових систем і мережевих протоколів, таких як SMB, NFS і AFP. Завдяки інтуїтивно зрозумілому веб-інтерфейсу адміністрування XigmaNAS забезпечує простоту управління файлами та спільними ресурсами.

Результатом проведеної роботи було створення гнучкого й функціонального лабораторного середовища, яке дозволяє тестувати VPN-рішення, аналізувати мережеву взаємодію, перевіряти конфігурації та забезпечувати безпеку даних.

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ OPENVPN

3.1 Налаштування OpenVPN

3.1.1 Маршрутизатор MikroTik CHR

Для налаштування OpenVPN на маршрутизаторі MikroTik CHR використовується RouterOS, яка має вбудовану підтримку OpenVPN. Ця процедура передбачає налаштування серверної частини OpenVPN на маршрутизаторі MikroTik CHR, включаючи створення сертифікатів, налаштування сервісу OpenVPN Server і відповідні мережеві налаштування.

На рисунку 3.1 відображено налаштування bridge інтерфейсу OpenVPN-bridge у веб-інтерфейсі маршрутизатора MikroTik.

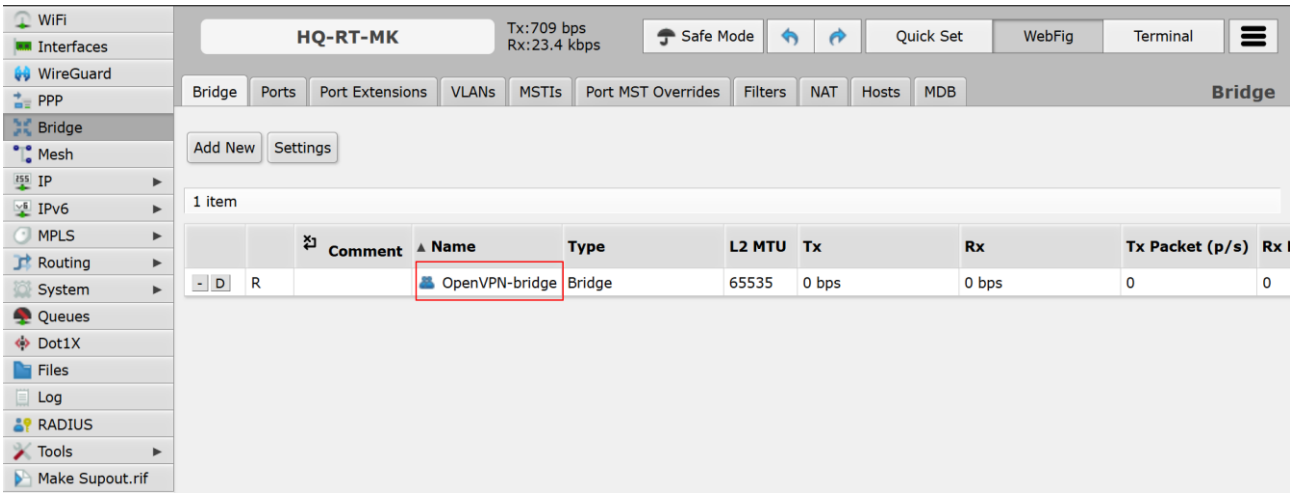

Рисунок 3.1 – Налаштування bridge інтерфейсу OpenVPN-bridge в MikroTik

У контексті OpenVPN міст буде використаний для спільної маршрутизації трафіку між клієнтами VPN і внутрішньою мережею. Завдяки цьому клієнти OpenVPN можуть отримувати доступ до локальних ресурсів мережі.

На рисунку 3.2 відображено розділ управління IP-адресами маршрутизатора MikroTik, де наведено три активні записи, кожен із яких відповідає певному інтерфейсу.

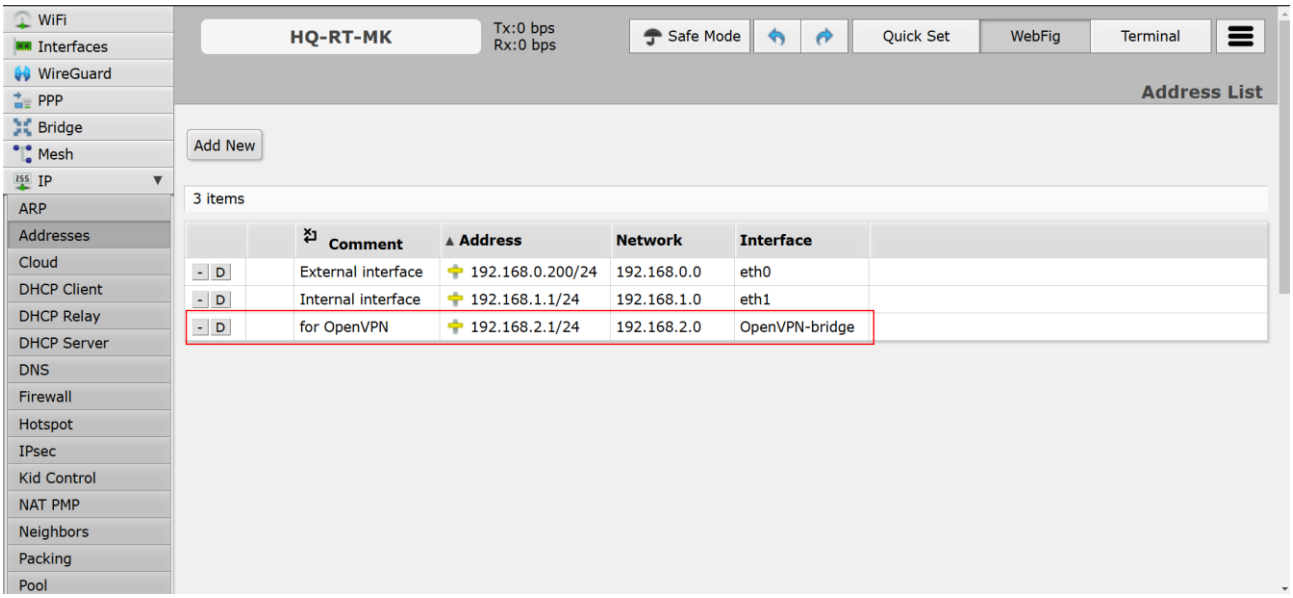

Рисунок 3.2 – Розділ управління IP-адресами маршрутизатора MikroTik

Третій запис позначено як for OpenVPN і має IP-адресу 192.168.2.1/24, що належить до мережі 192.168.2.0/24. Цей запис прив'язаний до віртуального інтерфейсу OpenVPN-bridge, який було попередньо створено. Інтерфейс OpenVPN-bridge використовується для об'єднання клієнтів OpenVPN у єдиний мережевий сегмент і забезпечення їхнього доступу до локальної мережі або інших ресурсів через VPN.

На рисунку 3.3 представлено конфігурацію IP Pool у веб-інтерфейсі маршрутизатора MikroTik.

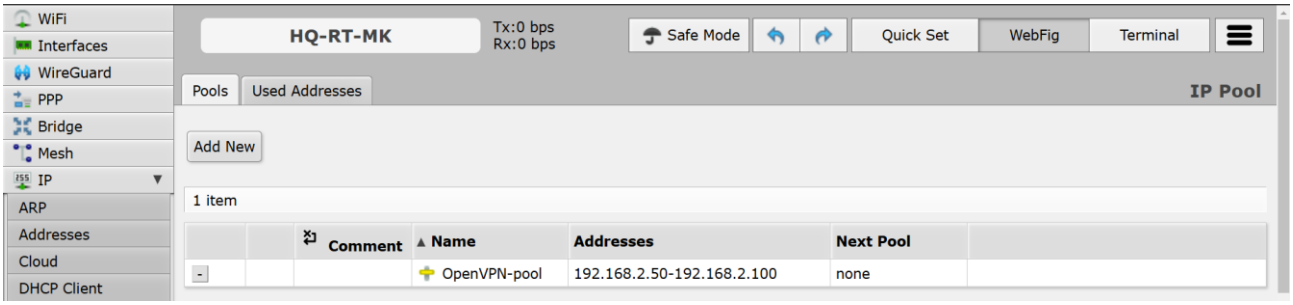

Рисунок 3.3 – Конфігурація IP Pool маршрутизатора MikroTik

Діапазон адрес у цьому пулі визначений як 192.168.2.50–192.168.2.100, що належить до підмережі 192.168.2.0/24. Цей пул адрес призначений для автоматичного розподілу IP-адрес клієнтам OpenVPN після їхнього успішного підключення до серверу. Ця конфігурація дозволяє сервісу OpenVPN

забезпечувати підключеним клієнтам унікальні IP-адреси з визначеного діапазону. Це необхідно для ідентифікації кожного клієнта в мережі та забезпечення їхньої взаємодії з іншими ресурсами, доступними через VPN.

На рисунку 3.4 відображений розділ Filter Rules у веб-інтерфейсі маршрутизатора MikroTik.

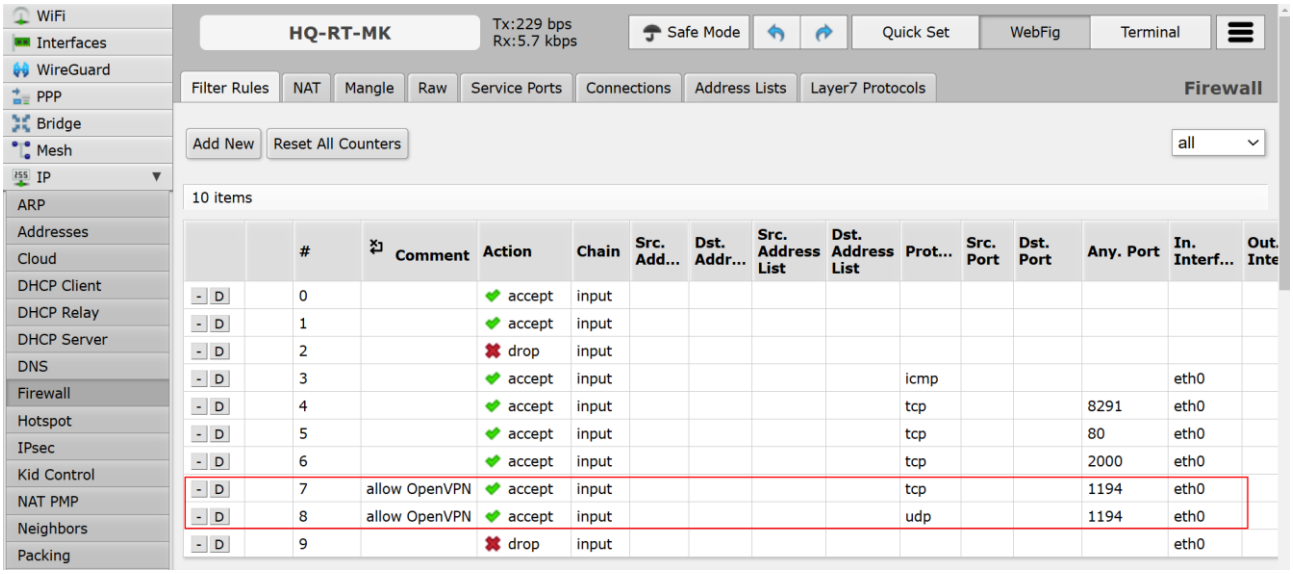

Рисунок 3.4 – Розділ Filter Rules маршрутизатора MikroTik

Виділені два правила налаштовані для дозволу вхідного трафіку на порт 1194 через протоколи TCP і UDP, який використовується для з'єднань OpenVPN. Це забезпечує доступ клієнтів OpenVPN до маршрутизатора MikroTik через зовнішній інтерфейс.

На рисунку 3.5 представлений розділ Certificates у веб-інтерфейсі MikroTik, який використовується для управління сертифікатами.

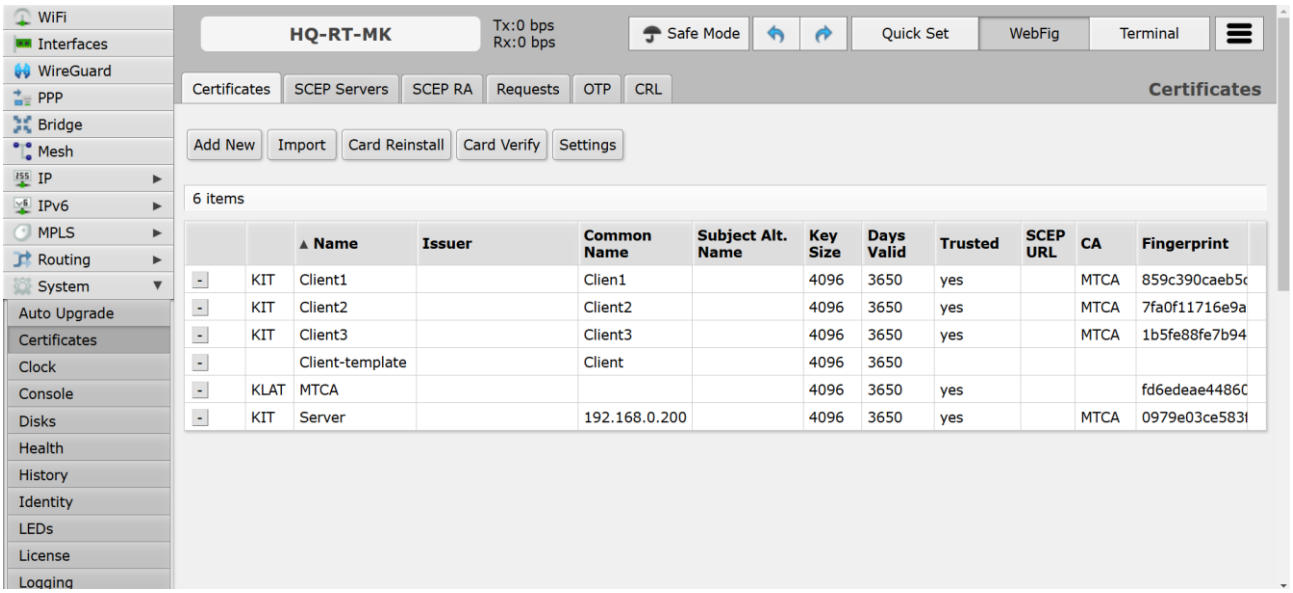

Рисунок 3.5 – Розділ Certificates маршрутизатора MikroTik

У таблиці відображені наявні сертифікати, що використовуються для забезпечення безпеки з'єднань OpenVPN [23]. Створені сертифікати для клієнтів (Client1, Client2, Client3, Client-template), сертифікат серверу (Server) та сертифікат центру сертифікації (MTCA). Усі сертифікати видані центром сертифікації MTCA (MikroTik Certification Authority).

Для всіх сертифікатів використовується тип ключа RSA з розміром 4096 біт, що забезпечує високий рівень безпеки. Усі сертифікати, окрім шаблону, активні та мають термін дії 10 років. Клієнтські сертифікати призначені для автентифікації в OpenVPN, а серверний сертифікат використовується для забезпечення безпечного з'єднання з клієнтами.

На рисунку 3.6 показано налаштування сервісу OpenVPN на маршрутизаторі MikroTik CHR.

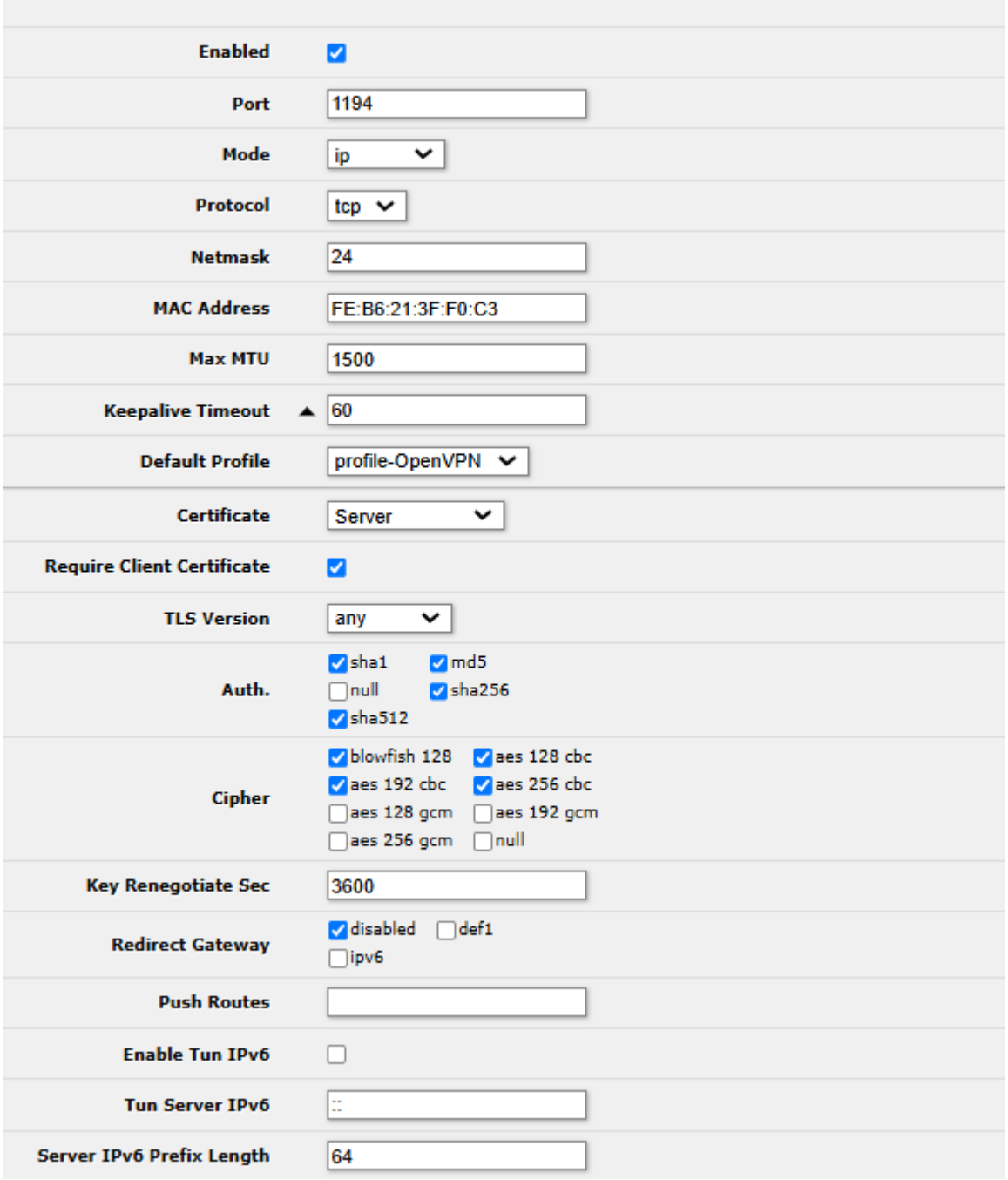

Рисунок 3.6 – Налаштування сервісу OpenVPN маршрутизатора MikroTik

Конфігурація визначає параметри роботи OpenVPN-сервера [23]. Встановлено порт 1194, який є стандартним портом для OpenVPN-з’єднань. Протокол вибрано як TCP, що забезпечує гарантовану доставку пакетів через VPN-канал. Параметр Keepalive Timeout встановлено на 60 секунд, що означає період перевірки активності з’єднання. У полі Default Profile вибрано профіль profile-OpenVPN, який визначає додаткові параметри для з’єднання. Для забезпечення безпечного з’єднання використовується сертифікат із назвою Server, який був попередньо налаштований і створений через центр сертифікації

(CA). Параметр Require Client Certificate увімкнено, що означає необхідність використання клієнтських сертифікатів для автентифікації. TLS-версія дозволена та встановлено можливість підтримку різних версій TLS, залежно від клієнтських налаштувань. Серед алгоритмів аутентифікації увімкнено sha1, md5, sha256, а також sha512, що забезпечує гнучкість. У полі Cipher увімкнено підтримку кількох шифрів: blowfish 128, aes 128 cbc, aes 192 cbc, і aes 256 cbc, які забезпечують захист переданих даних за допомогою сучасних алгоритмів шифрування. Параметр Key Renegotiate Sec встановлено на 3600 секунд, що означає автоматичне перевстановлення ключів кожну годину для підвищення безпеки. Опція Redirect Gateway вимкнена, що означає, що VPN-сервер не змінює маршрут за замовчуванням для клієнтів. Ці налаштування забезпечують безпечний і стабільний VPN-зв’язок, з підтримкою сучасних стандартів шифрування та аутентифікації.

На рисунку 3.7 представлено налаштування профілю profile-OpenVPN на маршрутизаторі MikroTik CHR.

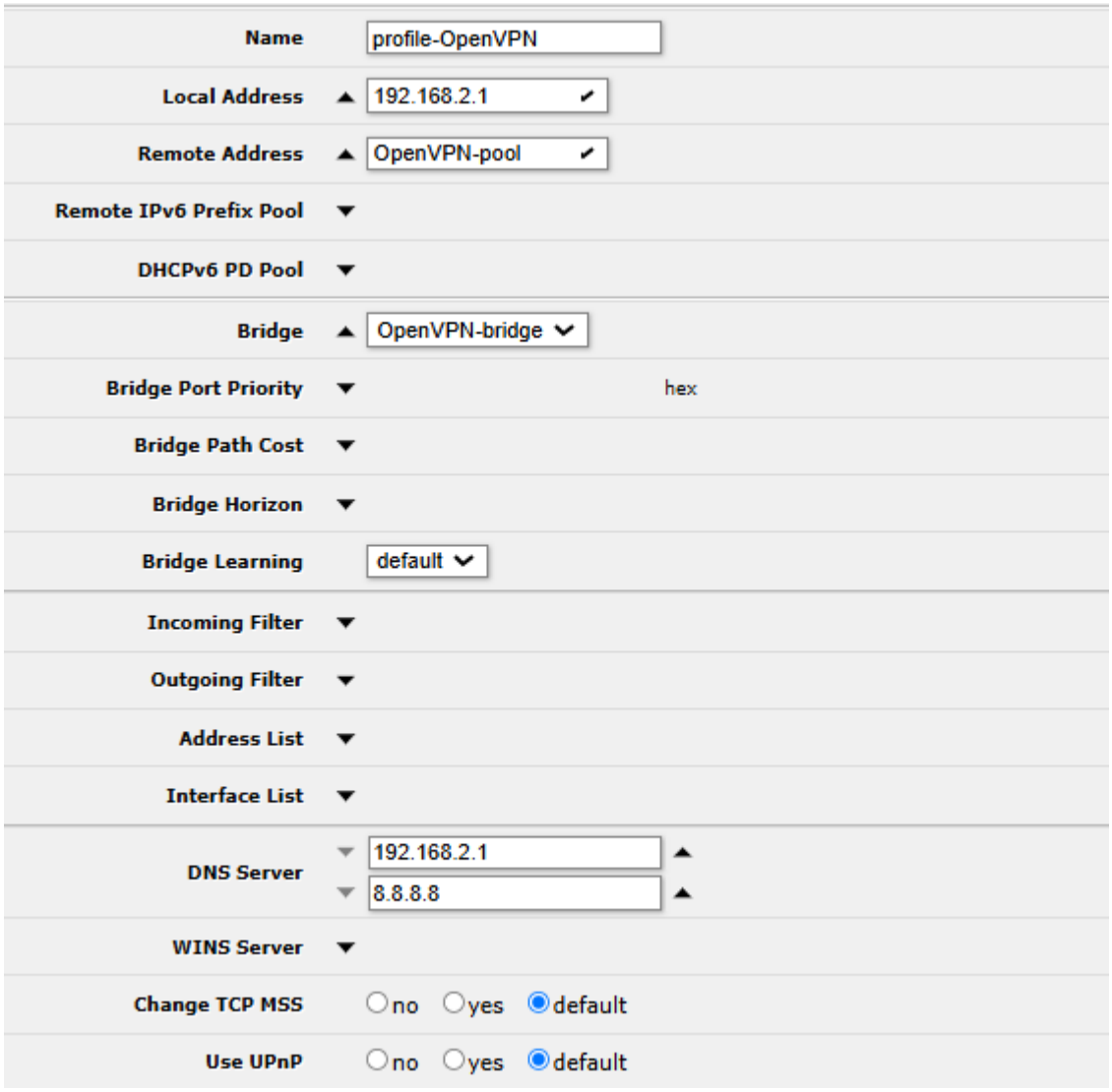

Рисунок 3.7 – Налаштування профілю profile-OpenVPN маршрутизатора MikroTik

Цей профіль використовується для визначення параметрів з'єднання клієнтів OpenVPN з сервером. Поле Local Address вказує локальну адресу OpenVPN-сервера - 192.168.2.1. Це IP-адреса, яка використовується сервером для взаємодії з клієнтами. Поле Remote Address пов’язане з пулом IP-адрес, визначеним як OpenVPN-pool, з якого клієнтам призначатимуться IP-адреси при підключенні до VPN. Поле Bridge вказує, що OpenVPN-з’єднання інтегровані з бриджем OpenVPN-bridge, що дозволяє забезпечити прозору маршрутизацію та взаємодію з іншими пристроями у внутрішній мережі. У полі DNS Server зазначено дві адреси серверів DNS: 192.168.2.1 (локальний сервер) і 8.8.8.8 (публічний DNS-сервер Google). Ці сервери забезпечують перетворення доменних імен у відповідні IP-адреси для клієнтів, які підключаються через VPN.

На рисунку 3.8 показано розділ налаштувань PPP на маршрутизаторі MikroTik CHR, де створено три записи для автентифікації користувачів OpenVPN.

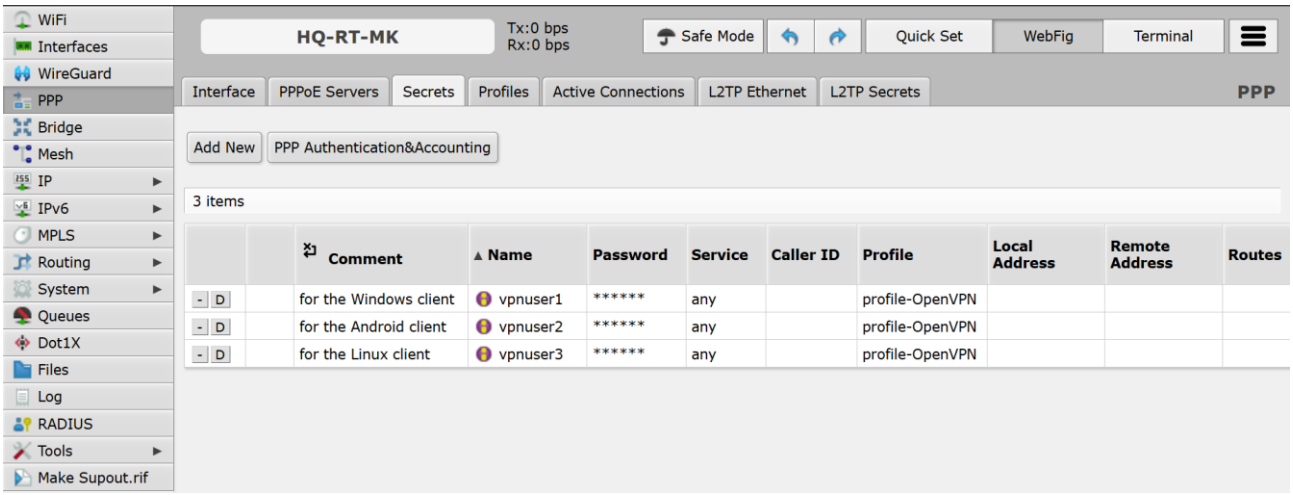

Рисунок 3.8 – Облікові дані клієнтів VPN

У полі Profile зазначено профіль profile-OpenVPN, який використовується для цих облікових записів. Цей профіль визначає параметри, такі як локальна IP-адреса, пул віддалених адрес та інші налаштування, специфічні для клієнтів OpenVPN. Поле Local Address залишено порожнім, оскільки локальна IP-адреса визначається у профілі OpenVPN. Поле Remote Address також залишено порожнім, оскільки IP-адреси для клієнтів виділяються з пулу, налаштованого в профілі profile-OpenVPN. Поле Routes залишено порожнім, що означає, що додаткових маршрутів для цих облікових записів не налаштовано. Всі маршрути визначаються в конфігураційному файлі клієнтів VPN.

Для створення конфігураційного файлу для OpenVPN клієнта потрібно забезпечити відповідність параметрів конфігурації клієнта налаштуванням сервера. Конфігураційний файл містить параметри підключення та використовувані сертифікати. В Додатку А наведено шаблон конфігураційного файлу для OpenVPN клієнта.

3.1.2 Клієнти VPN

Для налаштування клієнта OpenVPN на Windows 10 необхідно завантажити та встановити програмне забезпечення з офіційного сайту [24]. Скориставшись конфігураційним фалом MikroTik-OpenVPN-vpnuser1.ovpn було налаштовано клієнт VPN (див. рисунок 3.9).

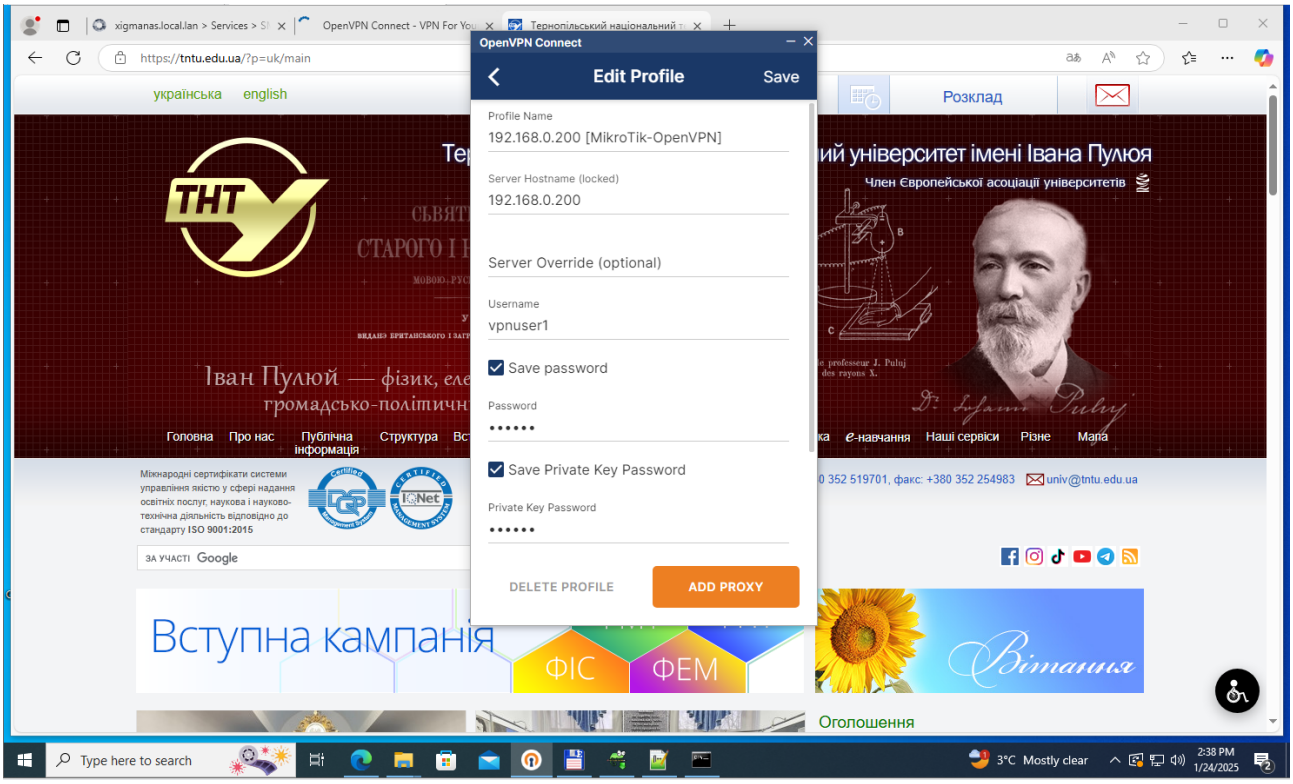

Рисунок 3.9 – Налаштування клієнта OpenVPN на Windows 10

В клієнтському додатку OpenVPN Connect у поле Server Hostname (locked) містить IP-адресу, до якої буде встановлено з’єднання. Це значення зафіксоване, що означає, що його не можна змінювати вручну в цьому інтерфейсі. В поле Username занесено логін vpnuser1, який буде використовуватися для автентифікації клієнта на сервері. Поле Save Private Key Password активоване, що дозволяє зберігати пароль до приватного ключа, використаного у конфігурації. Це забезпечує автоматичне введення пароля при встановленні з'єднання, спрощуючи процес підключення.

Для налаштування клієнта OpenVPN на Android використовується офіційний додаток OpenVPN Connect, який доступний у Google Play Store. Після

встановлення додатку необхідно імпортувати конфігураційний файл MikroTik-OpenVPN-vpnuser2.ovpn. Цей файл містить усі необхідні параметри для встановлення з'єднання з VPN-сервером, зокрема IP-адресу, порт, протокол, параметри шифрування, а також сертифікати й ключі для автентифікації.

На рисунку 3.10 показано налаштування профілю в мобільному додатку OpenVPN Connect на пристрої Android.

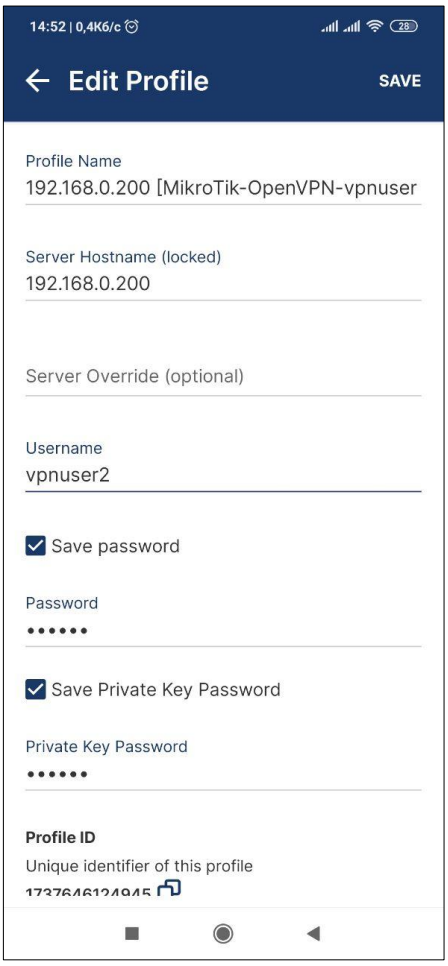

Рисунок 3.10 – Налаштування клієнта OpenVPN на Android

Усі налаштування OpenVPN-клієнта в Android ідентичні до налаштувань у Windows 10. Функціонально профіль OpenVPN-клієнта в Android нічим не відрізняється від Windows-версії, оскільки і на мобільному, і на десктопному клієнті реалізовано однаковий підхід до налаштування OpenVPN-з'єднання. Це дозволяє користувачу легко налаштувати клієнта OpenVPN на різних платформах із однаковим рівнем безпеки та функціональності.

Налаштування клієнта OpenVPN в Ubuntu Linux починається з встановлення необхідного програмного забезпечення та імпорту конфігураційного файлу сервера. Команда `sudo apt install openvpn` використалась для встановлення пакета OpenVPN [25]. Оскільки для управління мережею буде використовуватись Network Manager було встановлено плагін OpenVPN для Gnome за допомогою команди `sudo apt install network-manager-openvpn-gnome`. Після встановлення OpenVPN було завантажено конфігураційний файл MikroTik-OpenVPN-vpnuser2.ovpn.

На рисунку 3.11 показано вікно налаштувань мережі в операційній системі Ubuntu Linux. У ньому відображено поточний стан мережевих підключень.

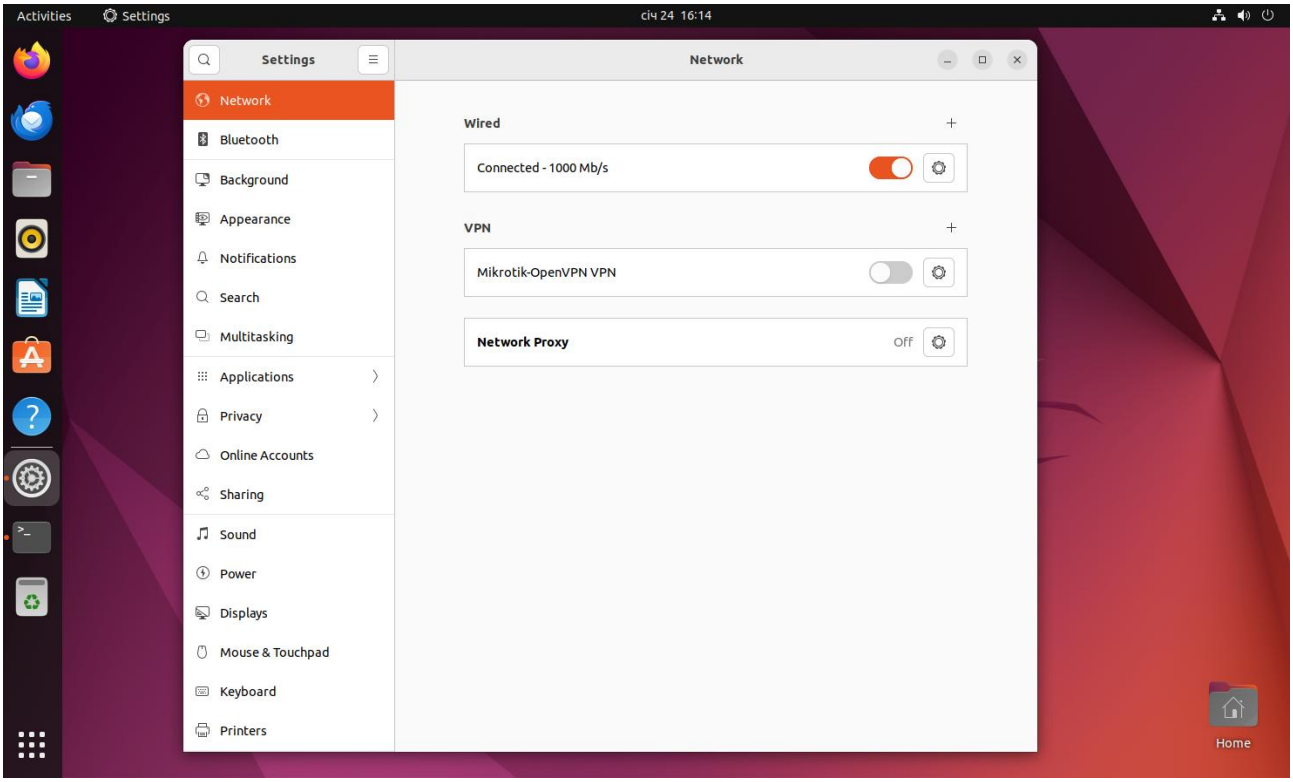

Рисунок 3.11 – Вікно налаштувань мережі в операційній системі Ubuntu Linux

В секції VPN відображається налаштоване VPN-з'єднання з назвою Mikrotik-OpenVPN VPN. Це свідчить про те, що в системі вже додано профіль VPN для підключення до сервера OpenVPN, розгорнутого на MikroTik. VPN-з'єднання на даний момент неактивне.

На рисунку 3.12 показано вікно налаштувань VPN-з'єднання в Ubuntu Linux.

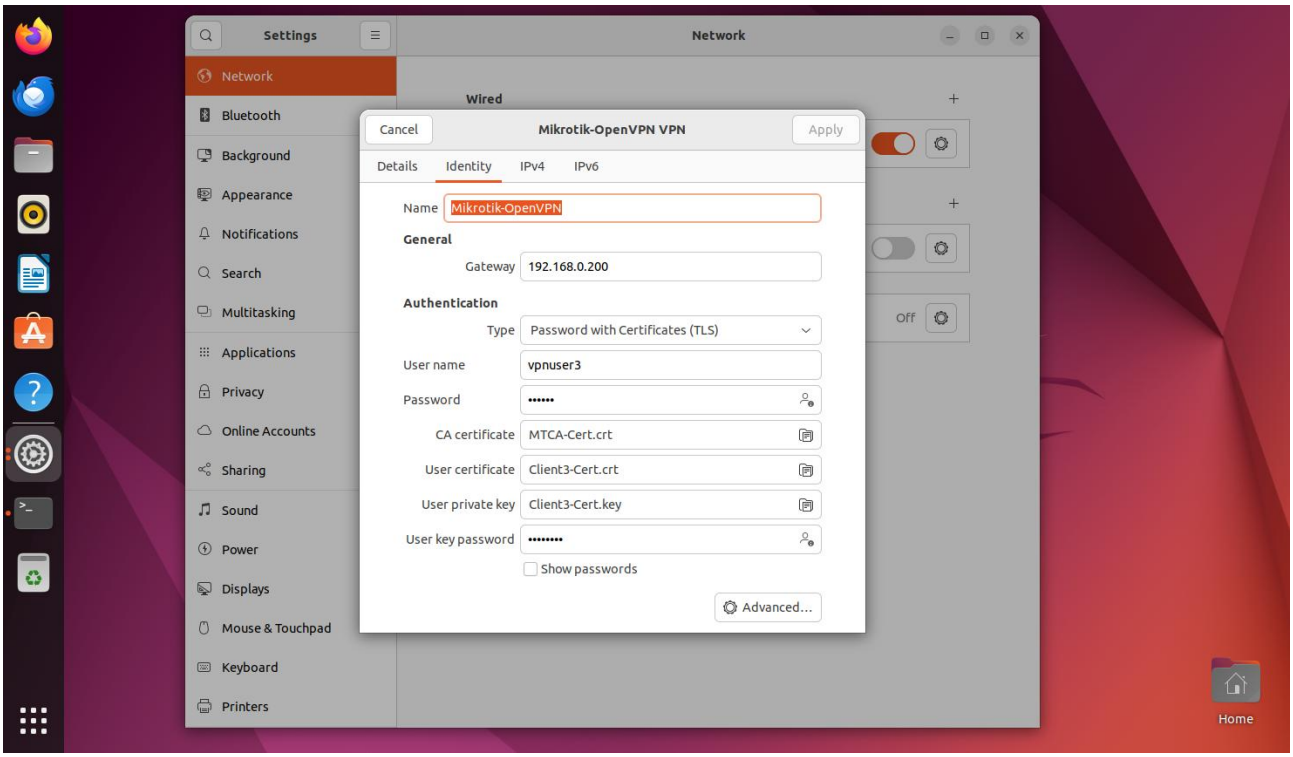

Рисунок 3.12 – Вікно налаштувань VPN-з'єднання в операційній системі Ubuntu Linux

У цьому вікні можна побачити детальну конфігурацію для підключення до сервера OpenVPN, розгорнутого на MikroTik. У полі Gateway зазначена IP-адреса шлюзу, до якого клієнт підключається, у нашому випадку це 192.168.0.200. Це адреса сервера OpenVPN, до якого встановлюється з'єднання. Для аутентифікації використовується метод Password with Certificates (TLS). У полі "User name" зазначено ім'я користувача, яке у даному випадку є vpnuser3. У секції сертифікатів вказано файл сертифіката центру сертифікації (CA), який використовується для перевірки сервера (MTCA-Cert.crt), клієнтський сертифікат, необхідний для автентифікації клієнта (Client3-Cert.crt) та вказаний файл із приватним ключем клієнта, який відповідає клієнтському сертифікату(Client3-Cert.key). Також у полі User key password введено пароль для захисту приватного ключа.

На рисунку 3.13 відображено вкладку General у вікні Advanced Properties для налаштування OpenVPN-клієнта в Ubuntu Linux. Ця вкладка надає можливість точного налаштування параметрів VPN-з'єднання.

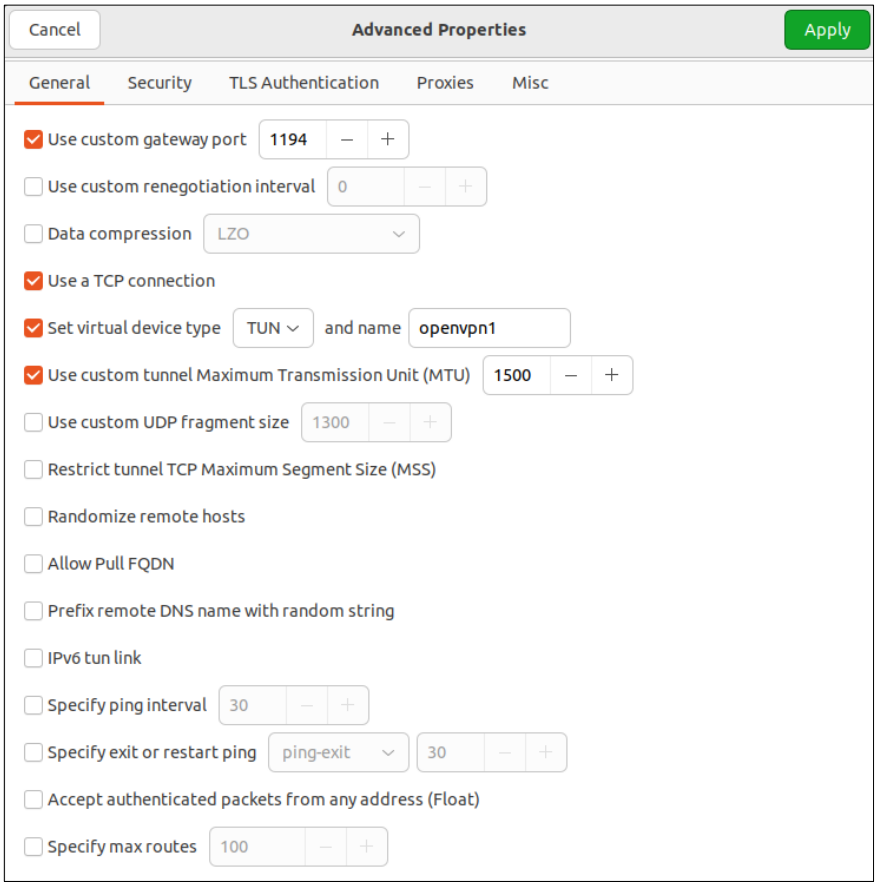

Рисунок 3.13 – Вкладка General у вікні Advanced Properties для налаштування OpenVPN-клієнта в Ubuntu Linux

Встановлений порт шлюзу 1194 відповідає стандартному порту, що використовується OpenVPN-серверами. Також увімкнено опцію Use a TCP connection, що дозволяє використовувати протокол TCP для з'єднання, забезпечуючи більшу стабільність, хоча й із меншою швидкістю порівняно з UDP. Опція Set virtual device type увімкнена, і обраний тип віртуального пристрою TUN, що є типовим для тунелювання в OpenVPN. Ім'я пристрою задано як openvpn1. Це ім'я ідентифікує створений віртуальний мережевий інтерфейс у системі. Увімкнено параметр Use custom tunnel Maximum Transmission Unit (MTU), значення якого встановлено на 1500. Цей параметр визначає максимальний розмір пакета, який може бути переданий через VPN-тунель, і є важливим для забезпечення коректної передачі даних без фрагментації.

На рисунку 3.14 відображено вкладку Security у вікні Advanced Properties налаштування OpenVPN-клієнта в Ubuntu Linux.

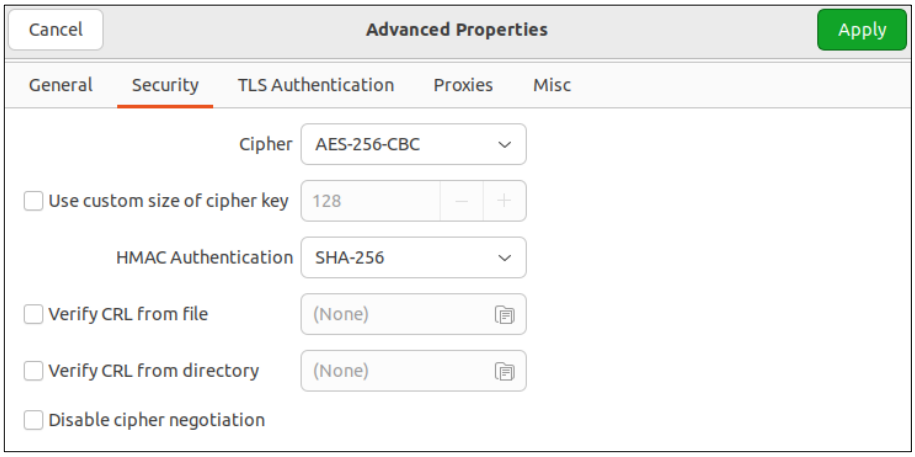

Рисунок 3.14 – Вкладка Security у вікні Advanced Properties для налаштування OpenVPN-клієнта в Ubuntu Linux

Ця вкладка містить параметри безпеки, які визначають алгоритми шифрування та автентифікації, що використовуються у VPN-з'єднанні. Обраний алгоритм шифрування (Cipher) - AES-256-CBC. Це один із найнадійніших алгоритмів шифрування, що забезпечує високий рівень безпеки завдяки 256-бітному ключу. Він часто використовується для VPN через його стійкість до криптоаналітичних атак. Для автентифікації HMAC вибраний алгоритм SHA-256. Цей алгоритм забезпечує надійну перевірку цілісності та автентичності переданих даних. Він широко застосовується для створення криптографічних підписів завдяки його високій надійності.

Клієнти OpenVPN на всіх трьох платформах (Windows, Android, Ubuntu Linux) налаштовані відповідно до вимог та готові до тестування VPN-з'єднання. Усі клієнти мають належно встановлені сертифікати, що забезпечує аутентифікацію та захист від несанкціонованого доступу. Всі клієнти готові до тестування VPN-з'єднання, включаючи перевірку роботи через OpenVPN-тунель та доступу до локальних ресурсів NAS-сервера XigmaNAS.

3.2 Тестування OpenVPN

Тестування OpenVPN включає кілька етапів для перевірки якості з'єднання та доступу до локальних ресурсів.

На рисунку 3.15 представлено вивід команди `ifconfig` в Ubuntu Linux.

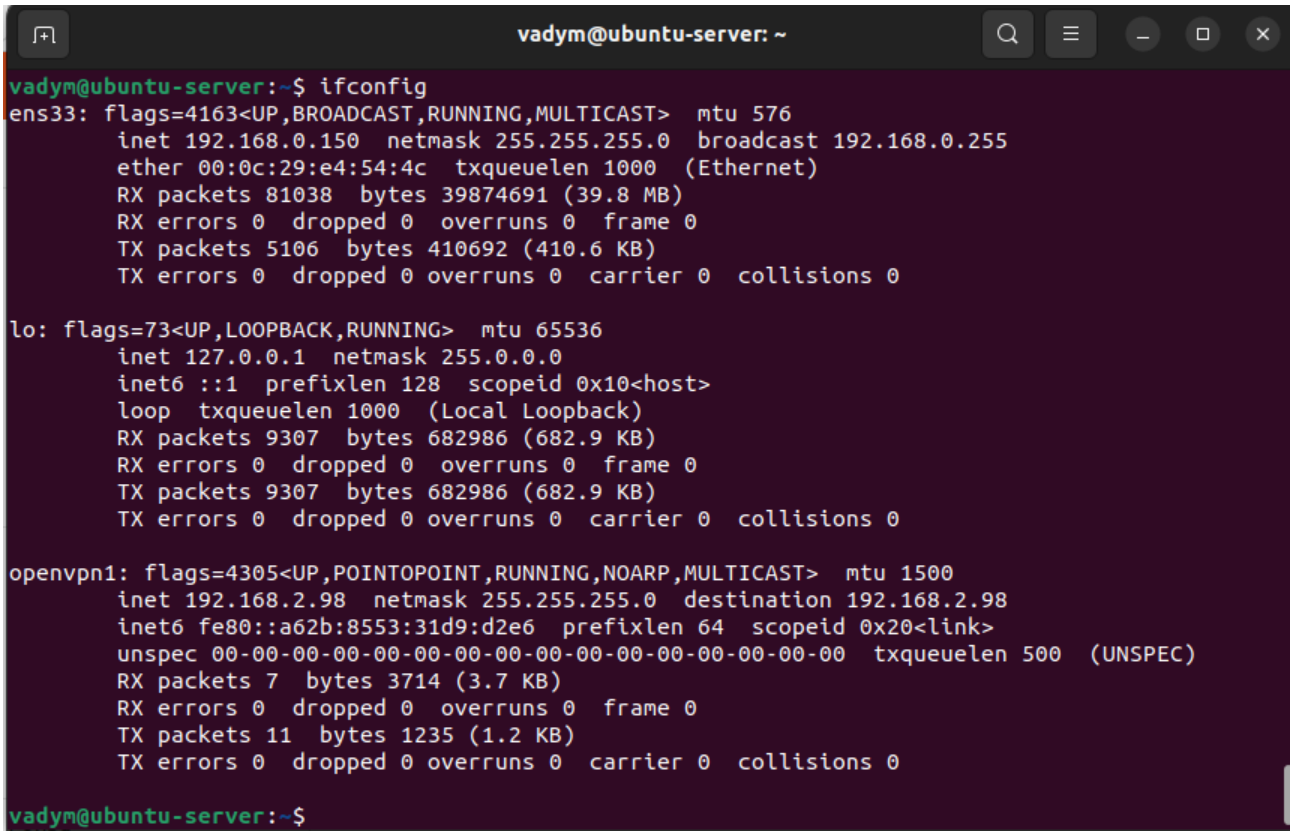

Рисунок 3.15 – Вивід команди `ifconfig` в Ubuntu Linux

Інтерфейс openvpn1 є віртуальним інтерфейсом, створеним OpenVPN-клієнтом. Він відповідає за роботу VPN-тунелю. Інтерфейс має IP-адресу 192.168.2.98 з маскою підмережі 255.255.255.0. Це вказує, що VPN-клієнт підключений до віртуальної мережі 192.168.2.0/24. Значення RX і TX свідчать про успішний обмін даними через тунель OpenVPN. Ця конфігурація вказує, що OpenVPN-клієнт успішно підключився до сервера. На рисунку 3.16 представлено результат виконання команди `mtr` в Ubuntu Linux.

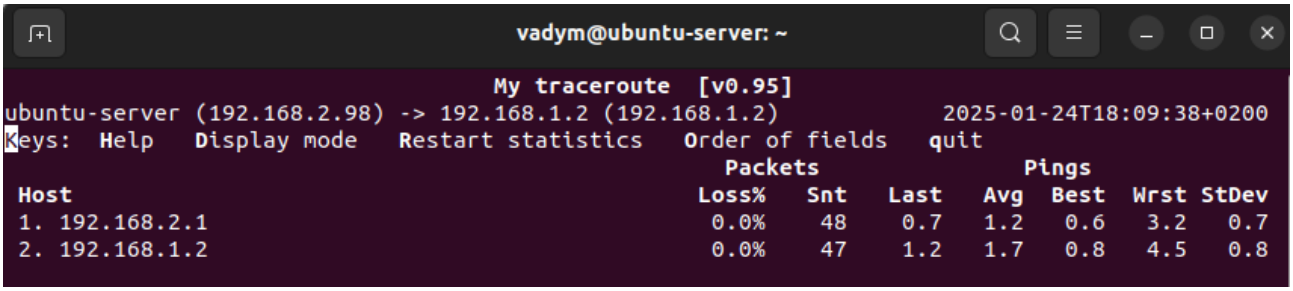

Рисунок 3.16 – Вивід команди `mtr` в Ubuntu Linux

Ця команда використовується для діагностики маршруту передачі пакетів до NAS-сервера XigmaNAS через VPN мережу. У даному випадку запит виконується з хоста з IP-адресою 192.168.2.98 до цільового хоста 192.168.1.2.

Перший вузол з IP-адресою 192.168.2.1 це шлюз, який обслуговує забезпечує зв'язок між VPN-тунелем і внутрішньою мережею. Значення Loss% дорівнює 0.0%, що означає відсутність втрат пакетів. Другий вузол з IP-адресою 192.168.1.2 це XigmaNAS. Втрати пакетів також відсутні (Loss% = 0.0%). Середній час затримки до цього вузла становить 1.7 мс, а найменша - 0.8 мс. Це свідчить про стабільний зв'язок.

Показники затримки та відсутність втрат пакетів вказують на ефективну роботу VPN-тунелю та правильне налаштування маршрутизації в тестовому середовищі. Тест підтверджує, що пакети успішно досягають цільового хоста через OpenVPN-тунель.

На рисунку 3.17 показано результат виконання команди `mount`, яка використовується для перевірки змонтованих файлових систем.

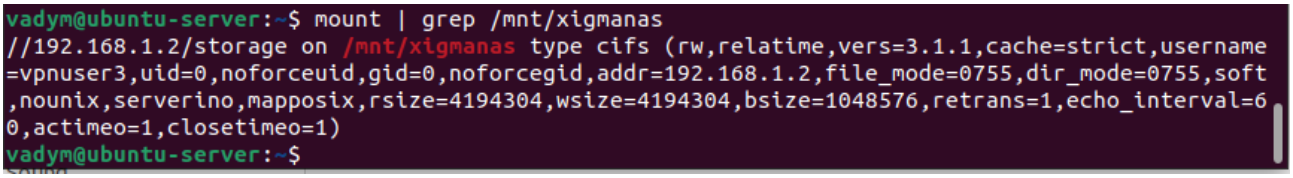

Рисунок 3.17 – Вивід команди `mount` в Ubuntu Linux

У нашому випадку відображено успішне підключення SMB ресурсу, розташованого на NAS-сервері з IP-адресою 192.168.1.2.

Мережевий ресурс `//192.168.1.2/storage` змонтований у директорію `/mnt/xigmanas`. Тип файлової системи – cifs, що є стандартом для мережевого доступу до спільних ресурсів для Windows і Linux клієнтів. Цей вивід свідчить про те, що мережевий ресурс змонтовано успішно, і клієнт Linux має доступ до файлової системи NAS-сервера XigmaNAS.

На рисунку 3.18 показано вміст каталогу `/mnt/xigmanas`, доступ до якого отримано через файловий менеджер операційної системи Ubuntu Linux.

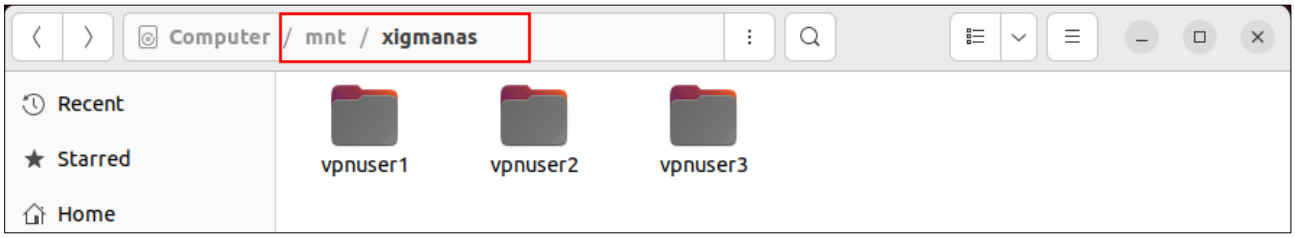

Рисунок 3.18 – Вміст каталогу `/mnt/xigmanas` в Ubuntu Linux

Каталог `/mnt/xigmanas` є точкою монтування мережевого ресурсу, розташованого на NAS-сервері XigmaNAS. У цьому каталозі видно три підкаталоги: vpnuser1, vpnuser2 і vpnuser3.

Ці підкаталоги відповідають окремим користувачам, які мають доступ до мережевого сховища. Це важливий етап у перевірці VPN-з'єднання та роботи мережевого сховища, оскільки підтверджує можливість клієнтів отримувати доступ до локальних ресурсів через OpenVPN-тунель.

На рисунку 3.19 представлено інтерфейс мобільного додатку OpenVPN Connect на пристрої Android.

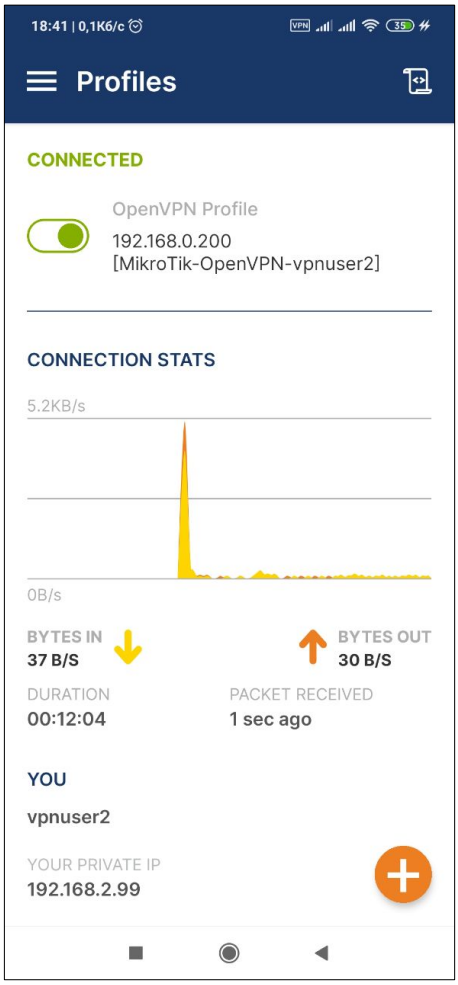

Рисунок 3.19 – Інтерфейс мобільного додатку OpenVPN Connect на пристрої Android

Профіль під назвою 192.168.0.200 [MikroTik-OpenVPN-vpnuser2] успішно підключено, що підтверджується статусом CONNECTED. Це свідчить про встановлений VPN-з'єднання з сервером OpenVPN, розташованим на маршрутизаторі MikroTik. Користувач vpnuser2 асоціюється з приватною IP-адресою 192.168.2.99, виділеною через OpenVPN-сервер. Це підтверджує, що клієнт отримав адресу з пулу, налаштованого для VPN-користувачів, і може безпечно взаємодіяти з ресурсами внутрішньої мережі. Успішне підключення підтверджує правильність налаштувань OpenVPN на клієнтському пристрої та сервері.

На рисунку 3.20 показано вивід команди `ipconfig` у Windows 10 для мережевого адаптера OpenVPN.

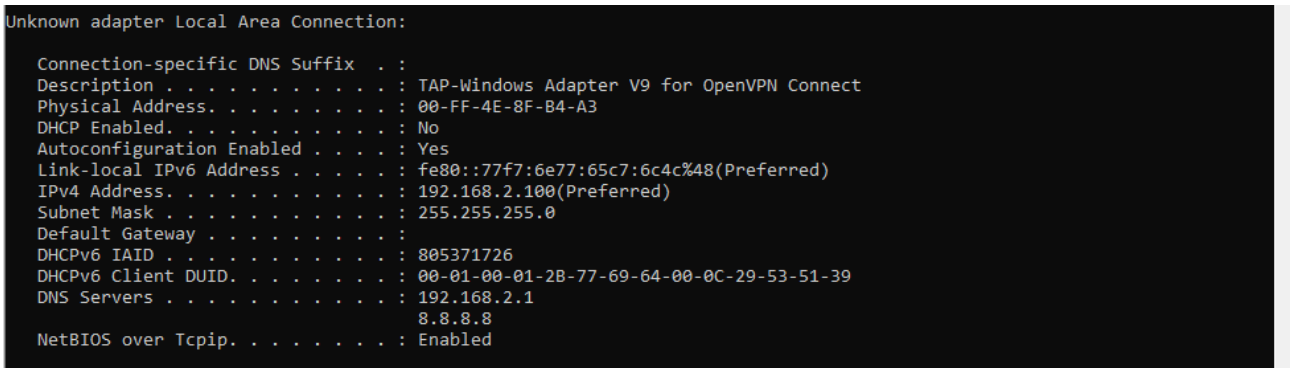

Рисунок 3.20 – Вивід команди `ipconfig` у Windows 10

Адаптер позначений як Unknown adapter Local Area Connection, що є TAP-адаптером, створеним для OpenVPN Connect. Поле Description вказує на те, що цей адаптер використовується спеціально для OpenVPN. Фізична адреса адаптера (Physical Address) - 00-FF-4E-8F-84-A3, що є стандартною для віртуальних мережевих інтерфейсів TAP. IP-адреса адаптера - 192.168.2.100 з маскою підмережі 255.255.255.0. Ця адреса була видана сервером OpenVPN, що підтверджує успішне підключення до VPN. Поле Default Gateway пусте, що означає, що трафік через цей адаптер маршрутизується специфічно для OpenVPN-з'єднання без використання шлюзу для всього мережевого трафіку. NetBIOS over Tcpip увімкнено, що забезпечує доступ до NetBIOS-ресурсів через TCP/IP-протокол. Цей параметр потрібний для доступу до мережевих ресурсів, таких як SMB на NAS-сервері XigmaNAS.

На рисунку 3.21 відображено частину таблиці маршрутизації IPv4 у Windows 10, що показує активний маршрут, налаштований через OpenVPN-з'єднання.

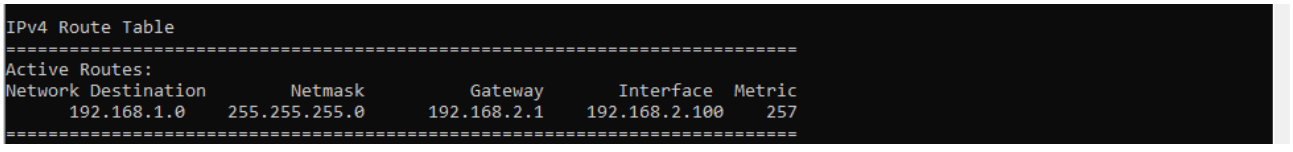

Рисунок 3.21 – Вивід частини таблиці маршрутизації у Windows 10

Ця інформація свідчить про те, що клієнт OpenVPN налаштований для маршрутизації трафіку до внутрішньої мережі 192.168.1.0/24 через VPN-тунель. Це дозволяє клієнту доступ до NAS-сервера. Налаштування підтверджує

правильну конфігурацію маршрутизації, яка є необхідною для повноцінного функціонування VPN-з'єднання.

На рисунку 3.21 показано результати виконання команди `tracert` в Windows 10, яка використовується для трасування маршруту до IP-адреси 192.168.1.2.

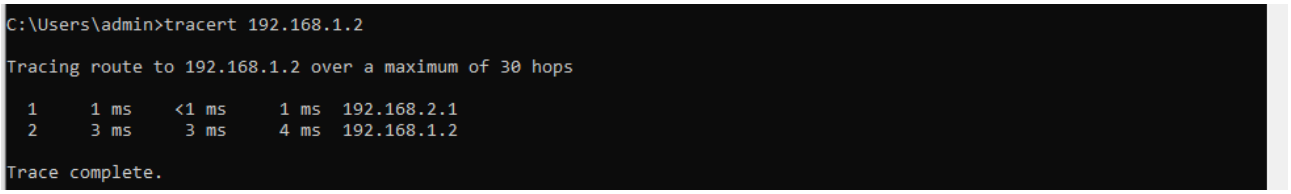

Рисунок 3.21 – Результати виконання команди `tracert` в Windows 10

Результати демонструють успішний зв'язок через VPN-тунель. Перший стрибок (hop) показує IP-адресу 192.168.2.1. Це є шлюзом, яким є OpenVPN-сервер, що виконує роль першого вузла для передачі трафіку. Час відповіді (RTT - round-trip time) на цей стрибок становить приблизно 1 мілісекунду, що свідчить про швидкий і стабільний зв'язок. Другий стрибок показує IP-адресу кінцевого пункту - 192.168.1.2, яка відповідає внутрішньому NAS-серверу. Час відповіді на цей стрибок становить 3-4 мілісекунди, що свідчить про низьку затримку при доступі до внутрішньої мережі через VPN. Команда завершилася успішно, підтверджуючи, що маршрут до цільового IP-адресата 192.168.1.2 налаштований правильно і доступ до нього через VPN-тунель забезпечується без проблем.

На рисунку 3.22 показано два елементи: вікно файлового менеджера Windows і інтерфейс OpenVPN Connect.

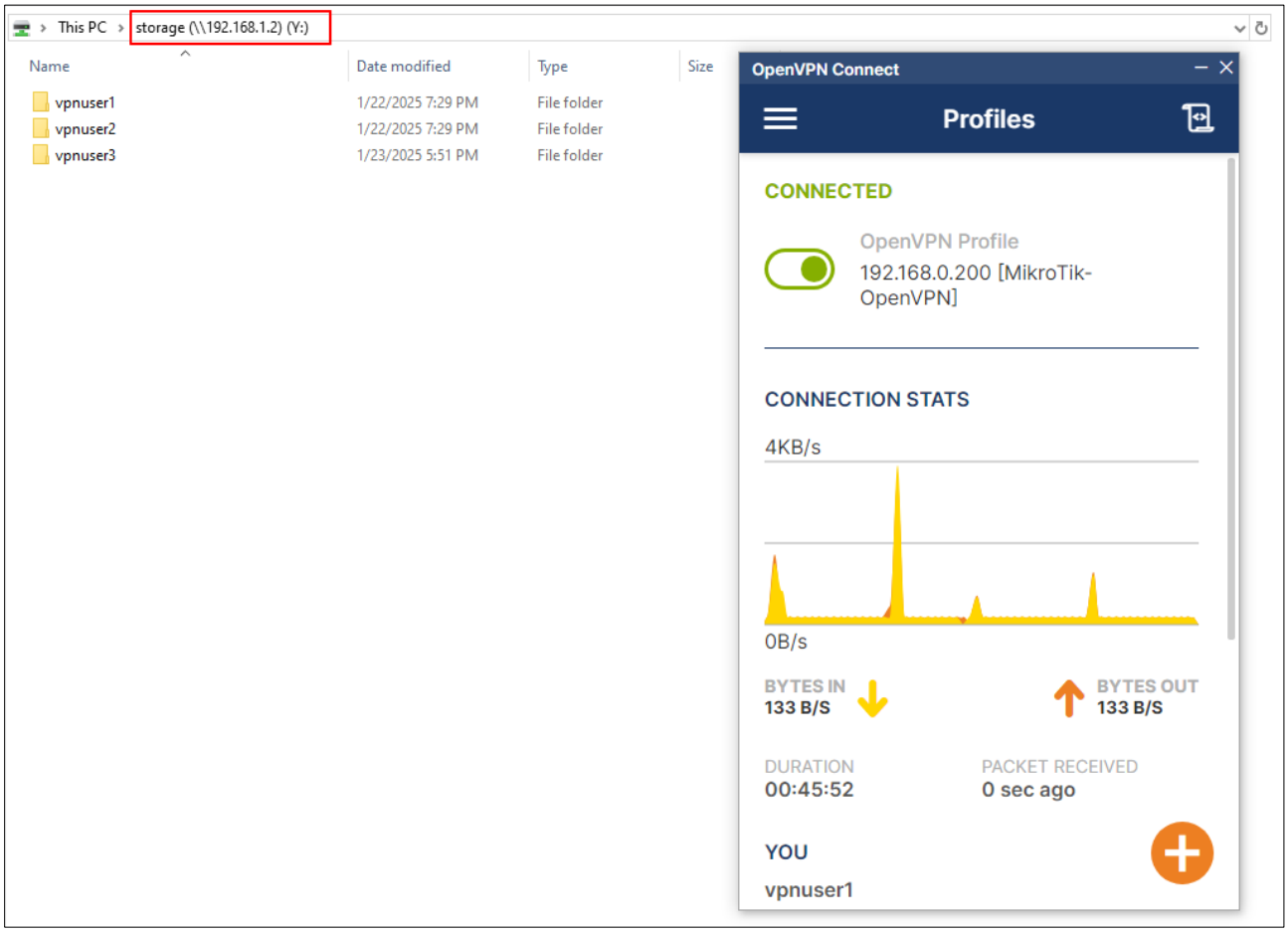

Рисунок 3.22 – Вікно файлового менеджера Windows і інтерфейс OpenVPN Connect

У вікні файлового менеджера Windows показано, що мережевий ресурс NAS-сервера, доступний за адресою `\\192.168.1.2\storage`, успішно підключено як мережевий диск (позначено літерою Y:). У кореневій папці диска відображені три підкаталоги: vpnuser1, vpnuser2, і vpnuser3. Це підтверджує, що клієнт має доступ до ресурсу NAS через VPN-з'єднання.

У вікні OpenVPN Connect демонструється статус з'єднання клієнта з OpenVPN-сервером. Профіль підключення має ім'я 192.168.0.200 [MikroTik-OpenVPN]. З'єднання активне. Статистика з'єднання показує вхідний і вихідний трафік у реальному часі, а також тривалість підключення 45 хвилин 52 секунди.

Це свідчить про успішне налаштування OpenVPN-сервера, правильну маршрутизацію трафіку через тунель і доступ клієнта до локальних мережевих ресурсів, зокрема до NAS-сервера XigmaNAS. Тестування підтвердило функціональність VPN-з'єднання.

На рисунку 3.23 відображено активні VPN-з'єднання через OpenVPN в MikroTik.

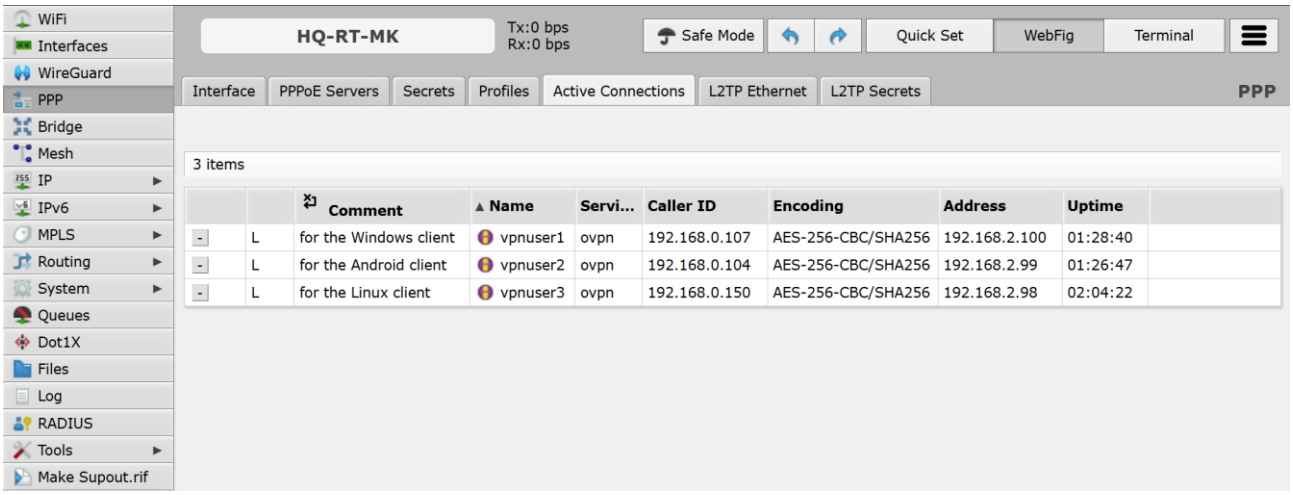

Рисунок 3.23 – Активні VPN-з'єднання через OpenVPN в MikroTik

У таблиці наведені три записи, кожен з яких відповідає окремому користувачу OpenVPN-клієнта. У колонці Caller ID вказані локальні IP-адреси пристроїв клієнтів: 192.168.0.107 для Windows, 192.168.0.104 для Android, та 192.168.0.150 для Linux. Ці адреси відповідають реальним мережевим інтерфейсам клієнтських пристроїв у локальній мережі перед встановленням VPN-з'єднання. У колонці Encoding зазначено шифрування, яке використовується для забезпечення безпеки VPN-з'єднання. Алгоритм шифрування - AES-256-CBC із алгоритмом HMAC SHA256 для автентифікації даних, що забезпечує високий рівень безпеки та стійкість до атак. У колонці Address вказані IP-адреси клієнтів, видані сервером OpenVPN після встановлення з'єднання: 192.168.2.100 для Windows, 192.168.2.99 для Android, і 192.168.2.98 для Linux. Ці адреси належать до пулу OpenVPN і використовуються для маршрутизації трафіку через VPN. Ця інформація підтверджує успішне налаштування OpenVPN-сервера та стабільну роботу клієнтів.

3.3 Висновки до третього розділу

В третьому розділі було розглянуто процес налаштування OpenVPN на маршрутизаторі MikroTik CHR та клієнтських пристроях із різними операційними системами (Windows 10, Android, Ubuntu Linux). Детально описано конфігурацію серверної частини OpenVPN на маршрутизаторі MikroTik, включаючи створення bridge-інтерфейсу, налаштування IP-адрес, створення IP Pool для клієнтів VPN, налаштування сертифікатів для шифрування та автентифікації, а також конфігурацію профілю для клієнтів VPN. Проведено налаштування клієнтів OpenVPN на трьох платформах з урахуванням сумісності та безпеки. Кожен клієнт було налаштовано за допомогою конфігураційного файлу, який містить параметри підключення до VPN-сервера, сертифікати та ключі. Усі клієнти успішно підключилися до OpenVPN-сервера, підтвердивши правильність їхнього налаштування.

Під час тестування OpenVPN-з'єднання виконано перевірку роботи через VPN-тунель. На Ubuntu Linux, Windows 10 і Android було перевірено налаштування мережевих інтерфейсів, трасування маршрутів до внутрішньої мережі, а також доступ до ресурсів NAS-сервера XigmaNAS. Усі клієнти отримали IP-адреси із налаштованого пулу, маршрутизація трафіку через VPN була успішною, а мережевий ресурс NAS-сервера був доступним. Результати тестування показали стабільність і безпеку з'єднання. Затримки у передачі даних були мінімальними, а втрати пакетів відсутні. Це підтверджує, що налаштування VPN-середовища відповідають поставленим вимогам та забезпечують захищений доступ до локальних ресурсів мережі.

Це свідчить про готовність розгорнутого середовища до реальної експлуатації, забезпечуючи стабільний, захищений і функціональний VPN-зв’язок для віддалених користувачів.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при тепловому ударі

Тепловий удар - це серйозний медичний стан, який виникає внаслідок перегрівання організму, зазвичай внаслідок тривалого перебування на сонці або у дуже спекотному середовищі. Це може призвести до серйозних ушкоджень органів і навіть може привести до смерті потерпілого.

Симптоми теплового удару можуть включати:

- висока температура тіла (понад 40°C);
- запаморочення, слабкість та втома;
- головний біль;
- червона, гаряча суха шкіра;
- швидке та поверхневе дихання;
- слабкість, запаморочення або втрата свідомості.

Долікарська допомога постраждалим при підозрі на тепловий удар є важливою процедурою, яку можуть виконувати особи без медичної освіти.

Наказ Міністерства охорони здоров'я України від 09.03.2022 р. № 441 " Про затвердження порядків надання домедичної допомоги особам при невідкладних станах" встановлює порядки надання домедичної допомоги постраждалим при підозрі на тепловий удар. У цьому порядку термін “тепловий удар” вживаються у такому значенні - невідкладний стан, викликаний дією високої температури навколишнього середовища, що спричиняє системні розлади у постраждалого [26].

Надання домедичної допомоги постраждалим при тепловому ударі передбачає такі кроки:

- переконатися, що немає небезпеки для себе, оточуючих та постраждалого, перед тим, як надавати допомогу;
- заспокоїти постраждалого та пояснити свої дії;
- викликати екстрену медичну допомогу та слухати інструкції диспетчера;

– перемістити постраждалого в прохолодне приміщення, щоб припинити дію тепла на нього;

– виміряти внутрішню температуру тіла постраждалого;

– використовувати методи охолодження, які доступні:

- повністю занурити постраждалого у холодну воду (18-26 °C), якщо його внутрішня температура тіла перевищує 40°C, та продовжувати занурення, поки температура не знизиться до 39°C;
- якщо повне занурення неможливе, можна використовувати пакети з льодом, обгорнуті у рушники, і накласти їх на тіло постраждалого. Можна також обдувати постраждалого вентиляторами або накласти вологі серветки на тіло.

– наглядати за постраждалим до прибуття медичної бригади;

– якщо постраждалий залишається свідомим, давати йому пити багато рідини;

– якщо стан постраждалого погіршується, повторно викликати екстрену медичну допомогу;

– зібрати інформацію про обставини виникнення теплового удару і передати її медичним працівникам при прибутті;

– якщо постраждалий втратив свідомість до прибуття медичної бригади, перейти до надання домедичної допомоги при раптовій зупинці кровообігу, відповідно до встановлених протоколів.

Це загальна послідовність дій, яку слід виконати, але завжди важливо дотримуватись інструкцій медичних фахівців та адаптувати допомогу до конкретної ситуації. Виконання цих кроків допоможе забезпечити постраждалому першу необхідну допомогу та зберегти його життя до прибуття медичних фахівців.

4.2 Техніка безпеки при роботі з ПК

До самостійної роботи на комп’ютерах допускаються особи, які пройшли медичний огляд, навчання по професії, вступний інструктаж з охорони праці та первинний інструктаж з охорони праці на робочому місці. В подальшому вони проходять повторні інструктажі з охорони праці на робочому місці один раз на півріччя, періодичні медичні огляди один раз на два роки [27].

Під час роботи на комп’ютерах можуть діяти такі небезпечні та шкідливі фактори, як:

– фізичні;

– психофізіологічні.

Основним обладнанням робочого місця користувача комп’ютера є монітор, системний блок та клавіатура, мишка.

Робочі місця мають бути розташовані на відстані не менше 1,5 м від стіни з вікнами, від інших стін на відстані 1м, між собою на відстані не менше 1,5 м. Відносно вікон робоче місце доцільно розташовувати таким чином, щоб природне світло падало на нього збоку, переважно зліва.

Робочі місця слід розташовувати так, щоб уникнути попадання в очі прямого світла. Джерела освітлення рекомендується розташовувати з обох боків екрану паралельно напрямку погляду. Для уникнення світлових відблисків екрану, клавіатури в напрямку очей користувача, від світильників загального освітлення або сонячних променів, необхідно використовувати анти полискові сітки, спеціальні фільтри для екранів, захисні козирки, на вікнах – жалюзі.

Монітор повинен бути розташований на робочому місці так, щоб поверхня екрана знаходилася в центрі поля зору на відстані 400-700 мм від очей користувача. Рекомендується розміщувати елементи робочого місця так, щоб витримувалася однакова відстань очей від екрана, клавіатури, тексту.

Зручна робоча поза при роботі з комп’ютером забезпечується регулюванням висоти робочого столу, крісла та підставки для ніг. Раціональною робочою позою може вважатися таке положення, при якому ступні працівника розташовані горизонтально на підлозі або підставці для ніг, стегна зорієнтовані

у горизонтальній площині, верхні частини рук – вертикальні. Кут ліктєвого суглоба коливається в межах 70-90°, зап'ястя зігнуті під кутом не більше ніж 20°, нахил голови 15-20°.

Для нейтралізації зарядів статичної електрики в приміщенні, де виконується робота на комп'ютерах, в тому числі на лазерних та світлодіодних принтерах, рекомендується збільшувати вологість повітря за допомогою кімнатних зволожувачів. Не рекомендується носити одяг з синтетичних матеріалів.

Згідно статті 18 Закону України "Про охорону праці" працівник зобов'язаний:

– знати і виконувати вимоги нормативних актів про охорону праці, правила поводження з устаткуванням та іншими засобами виробництва, користуватися засобами колективного та індивідуального захисту;

– дотримуватись зобов'язань щодо охорони праці, передбачених колективним договором та правилами внутрішнього трудового розпорядку підприємства;

– співробітничати з власником у справі організації безпечних і нешкідливих умов праці, особисто вживати посильних заходів щодо усунення будь-якої виробничої ситуації, яка створює загрозу його життю чи здоров'ю, або людей, які його оточують, повідомляти про небезпеку свого безпосереднього керівника або іншу посадову особу.

Вимоги безпеки перед початком роботи:

– увімкнути систему кондиціювання в приміщенні;

– перевірити надійність встановлення апаратури на робочому столі;

– повернути монітор так, щоб було зручно дивитися на екран – під прямим кутом (а не збоку) і трохи зверху вниз, при цьому екран має бути трохи нахиленим, нижній його край ближче до оператора;

– перевірити загальний стан апаратури, перевірити справність електропроводки, з'єднувальних шнурів, штепсельних вилок, розеток, заземлення захисного екрана;

– відрегулювати освітленість робочого місця;

– відрегулювати та зафіксувати висоту крісла, зручний для користувача нахил його спинки;

– приєднати до системного блоку необхідну апаратуру. Усі кабелі, що з'єднують системний блок з іншими пристроями, слід вставляти та виймати при вимкненому комп'ютері;

– ввімкнути апаратуру комп'ютера вимикачами на корпусах в послідовності: монітор, системний блок, принтер (якщо передбачається друкування);

– відрегулювати яскравість свічення монітора, мінімальний розмір світної точки, фокусування, контрастність. Не слід робити зображення надто яскравим, щоб не втомлювати очей.

Рекомендується:

– яскравість свічення екрана – не менше 100Kg/м2;

– відношення яскравості монітора до яскравості оточуючих його поверхонь в робочій зоні – не більше 3:1;

– мінімальний розмір точки свічення не більше 0,4 мм для монохромного монітора і не менше 0,6 мм для кольорового, контрастність зображення знаку – не менше 0,8.

При виявленні будь-яких несправностей роботу не розпочинати, повідомити про це керівника.

Вимоги безпеки під час виконання роботи:

– необхідно стійко розташовувати клавіатуру на робочому столі, не опускати її хитання.

– під час роботи на клавіатурі сидіти прямо, не напружуватися;

– для забезпечення несприятливого впливу на користувача пристроїв типу "миша" належить забезпечувати вільну велику поверхню столу для переміщення "миші" і зручного упору ліктьового суглоба;

– не дозволяються сторонні розмови, подразнюючі шуми;

– періодично при вимкненому комп'ютері прибирати ледь змоченою мильним розчином бавовняною ганчіркою порох з поверхонь апаратури;

– екран протирають ганчіркою, змоченою у спирті;

– не дозволяється використовувати рідинні або аерозольні засоби чищення поверхонь комп’ютера.

Психофізіологічне розвантаження є одним з варіантів зменшення стресу. Дана практика включає в себе застосування методу аутогенного тренування, що передбачає свідоме використання комплексу прийомів психічної саморегуляції та виконання простих фізичних вправ зі словесним самонавіюванням. Основна увага приділяється розслабленню м'язів (релаксації).

Під час сеансів психофізіологічного розвантаження рекомендується використовувати три періоди, що відповідають фазам відновлення.

Перший період - абстрагування від виробничого середовища, що відповідає фазі залишкового збудження. В цей час відтворюється повільна мелодійна музика та звуки пташиного співу. Працівники знаходять зручну позу та психологічно готуються до наступних періодів.

Другий період - заспокоєння, що відповідає фазі відновлювального гальмування. Показуються фотослайди з зображеннями природи, таких як квітучі луки, березові гаї, ставки і т.д. Звуковий супровід включає спокійну музику та заспокійливі формули аутогенного тренування.

Третій період - активізація, що відповідає фазі підвищеної збудженості. Спочатку світло повністю вимикається, а потім на екрані появляється червона пляма, розмір і яскравість якої поступово збільшуються. В кінці періоду звучить бадьора музика, а працівники виконують мобілізуючі формули аутогенного тренування, попередньо зробивши глибоке вдихання та видихання.

Сеанси психофізіологічного розвантаження можуть проводитись за єдиною програмою через індивідуальні навушники і складатись із двох періодів по 5 хвилин кожний: повне розслаблення та активізація працездатності. При необхідності, на фоні музики можуть використовуватись фрази, що сприяють відпочинку, покращенню самопочуття та бадьорості на заключному етапі. Після сеансів психофізіологічного розвантаження працівники відчувають зменшення втоми, з'являється бадьорість та гарний настрій, а загальний стан помітно поліпшується.

Додатково до сеансів психофізіологічного розвантаження, працівники також можуть скористатись іншими методами для зниження стресу та покращення психологічного благополуччя.

Одним з ефективних підходів є впровадження регулярних перерв під час робочого дня. Це можуть бути короткі паузи, під час яких працівники займаються розслаблюючими вправами, дихальними техніками або просто відпочивають. Це допомагає знизити напругу і покращити фокусування під час робочого процесу.

Також важливо створити комфортне робоче середовище для працівників. Це може включати забезпечення комфортних стільців і столів, добре освітлення та достатню вентиляцію. Природне освітлення та наявність рослин у приміщенні також можуть позитивно вплинути на настрій та самопочуття працівників.

Підтримка від керівництва та колег також має важливе значення. Створення сприятливого та підтримуючого робочого середовища, де працівники можуть відчути підтримку та співпрацю, сприяє зниженню стресу та покращує загальний настрій в колективі.

Крім того, особисте самоуправління і здібність до саморегуляції є важливими навичками для працівників. Це включає уміння регулювати власні емоції, реагувати на стресові ситуації та знаходити способи їх подолання, наприклад, за допомогою медитації, йоги або інших релаксаційних технік.

Усі ці підходи сприяють створенню здорової та продуктивної робочої атмосфери, де працівники можуть ефективно керувати стресом, забезпечуючи своє фізичне та емоційне благополуччя.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи бакалавра було розгорнуто та налаштовано середовище захищеного доступу до внутрішніх ресурсів компанії на базі OpenVPN і програмного маршрутизатора MikroTik CHR. У процесі роботи проведено аналіз VPN-технологій та особливостей їх застосування, розглянуто найбільш поширені протоколи й типи VPN-з'єднань. На основі цього аналізу було вибрано OpenVPN як оптимальне рішення для розгортання захищеної віртуальної мережі.

У ході дослідження створено лабораторне середовище для тестування із використанням гіпервізора Oracle VM VirtualBox. Для маршрутизації, управління трафіком та забезпечення VPN-підключень розгорнуто MikroTik CHR, а для зберігання та спільного доступу до файлів використано NAS-сервер на основі XigmaNAS. Виконано детальне налаштування MikroTik CHR: від створення пулу IP-адрес і профілів автентифікації до генерації сертифікатів та конфігурування брандмауера й NAT. Здійснено налаштування клієнтських підключень OpenVPN на різних операційних системах: Windows 10, Android та Ubuntu Linux. Проведені випробування підтвердили коректність налаштувань і стабільність VPN-з'єднань. Віддалені клієнти отримують IP-адреси із заданого пулу, успішно аутентифікуються на сервері, можуть взаємодіяти з ресурсами внутрішньої мережі та мати захищений доступ до NAS-сервера XigmaNAS по протоколу SMB. Аналіз трафіку, перевірка таблиць маршрутизації та команди трасування свідчать про правильну роботу тунелю, мінімальні затримки й відсутність втрат пакетів.

Поставлені завдання було повністю виконано, та мети дослідження досягнуто. Запропоноване рішення може бути адаптоване до потреб підприємств різного масштабу, забезпечуючи високу стабільність роботи, захист даних та можливість легкого масштабування. Отримані результати й напрацьовані матеріали можуть слугувати основою для подальших досліджень у сфері безпеки корпоративних мереж та навчання IT-фахівців.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is a VPN? Virtual private network meaning. (n.d.). NordVPN. https://nordvpn.com/what-is-a-vpn/

2. 14 most interesting uses of a VPN. (n.d.). NordVPN. https://nordvpn.com/blog/interesting-vpn-uses/

3. Global, P. (2022, November 24). Lock it down: Your introduction to securing data with VPN technology. Find the Resources You Need from PivIT Global. https://info.pivitglobal.com/resources/introduction-to-securing-data-with-vpn-technology

4. What are the different types of VPN protocols? (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/types-of-vpn-protocols

5. What is L2TP (layer 2 tunnel protocol)? (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-l2tp

6. What Is IKEv2 (Internet Key Exchange version 2)? (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-ikev2

7. Karnaukhov, A., Tymoshchuk, V., Orlovska, A., & Tymoshchuk, D. (2024). USE OF AUTHENTICATED AES-GCM ENCRYPTION IN VPN. Матеріали конференцій МЦНД, (14.06. 2024; Суми, Україна), 191-193.

8. What Is WireGuard? (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-wireguard

9. The ChaCha family of stream ciphers. (n.d.). cr.yp.to. https://cr.yp.to/chacha.html

10. Poly1305-AES: A state-of-the-art message-authentication code. (n.d.). cr.yp.to. https://cr.yp.to/mac.html

11. Blake2. (n.d.). BLAKE2. https://www.blake2.net/

12. Curve25519: High-speed elliptic-curve cryptography. (n.d.). cr.yp.to. https://cr.yp.to/ecdh.html

13. What Is OpenVPN? (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-openvpn

14. Tymoshchuk, V., Karnaukhov, A., & Tymoshchuk, D. (2024). USING VPN TECHNOLOGY TO CREATE SECURE CORPORATE NETWORKS. Collection of scientific papers «ΛΌГОΣ», (June 21, 2024; Seoul, South Korea), 166-170.

15. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N. & Tymoshchuk, V.(2024). Detection and classification of DDoS flooding attacks by machine learning method. CEUR Workshop Proceedings, 3842, 184–195.

16. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ. Матеріали конференцій МЦНД, (24.05. 2024; Запоріжжя, Україна), 145-146.

17. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.

18. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.

19. Oracle VirtualBox - Oracle VirtualBox Documentation. (2019, November 5). Oracle Help Center. https://docs.oracle.com/en/virtualization/virtualbox/

20. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп’ютерні мережі. Книга 1. [навчальний посібник] - Львів, "Магнолія 2006", 2013. – 256 с.

21. WinBox - RouterOS - MikroTik Documentation. (n.d.). MikroTik Routers and Wireless - Support. https://help.mikrotik.com/docs/spaces/ROS/pages/328129/WinBox

22. Documentation:Setup_and_user_guide [XigmaNAS WIKI]. (n.d.). XigmaNAS – XigmaNAS.

23. OpenVPN - RouterOS - MikroTik Documentation. (n.d.). MikroTik Routers and Wireless - Support. https://help.mikrotik.com/docs/spaces/ROS/pages/2031655/OpenVPN

24. OpenVPN connect user guide. (n.d.). Business VPN For Secure Networking | OpenVPN. https://openvpn.net/connect-docs/user-guide.html

25. Official ubuntu documentation. (n.d.). Official Ubuntu Documentation. https://help.ubuntu.com/

26. Микитишин, А. Г., Митник, М. М., Голотенко, О. С., & Карташов, В. В. (2023). Комплексна безпека інформаційних мережевих систем. Навчальний посібник для студентів спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка».

27. Mishko, O., Matiuk, D., & Derkach, M. (2024). Security of remote iot system management by integrating firewall configuration into tunneled traffic. Вісник Тернопільського національного технічного університету, 115(3), 122-129.

28. Nedzelskyi, D., Derkach, M., Tatarchenko, Y., Safonova, S., Shumova, L., & Kardashuk, V. (2019, August). Research of efficiency of multi-core computers with shared memory. In 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 111-114). IEEE.

29. Nedzelky, D., Derkach, M., Skarga-Bandurova, I., Shumova, L., Safonova, S., & Kardashuk, V. (2021, September). A Load Factor and its Impact on the Performance of a Multicore System with Shared Memory. In 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol. 1, pp. 499-503). IEEE.

30. Derkach, M., Lysak, V., Skarga-Bandurova, I., & Kotsiuba, I. (2019, September). Parking Guide Service for Large Urban Areas. In 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol. 1, pp. 567-571). IEEE.

31. Про затвердження порядків надання домедичної допомоги особам при невідкладних станах. (n.d.). Офіційний вебпортал парламенту України. https://zakon.rada.gov.ua/laws/show/z0356-22#n769

32. Стручок В.С. Техноекологія та цивільна безпека. Частина «Цивільна безпека». Навчальний посібник. Тернопіль: ТНТУ. 2022. 150 с.

Додаток А Шаблон конфігураційного файлу OpenVPN клієнта

```
client
dev tun
remote 192.168.0.200 1194 tcp
nobind
persist-key
persist-tun
remote-cert-tls server
data-ciphers AES-256-CBC
cipher AES-256-CBC
auth-user-pass
auth SHA256
tls-client
# redirect-gateway def1
route 192.168.1.0 255.255.255.0
verb 4
<ca>
-----BEGIN CERTIFICATE-----
<Вставити сертифікат CA>
-----END CERTIFICATE-----
</ca>

<cert>
-----BEGIN CERTIFICATE-----
<Вставити сертифікат клієнта>
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
<Вставити приватний ключ клієнта>
-----END PRIVATE KEY-----
</key>
```