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

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Аналіз, розгортання і тестування технології Site-to-Site та Remote Access VPN

Виконав: студент IV курсу, групи СН-42
спеціальності 122 Комп’ютерні науки
(шифр і назва спеціальності)

_____ Кудрик Д.В.
(підпис) (прізвище та ініціали)

Керівник _____ Гром'як Р.С.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Марценко С.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ Лечаченко Т. А.
(підпис) (прізвище та ініціали)

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 комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«___» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

Студенту Кудрику Дмитру Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз, розгортання і тестування технології Site-to-Site та Remote Access VPN

Керівник роботи Гром'як Роман Сильвестрович, к.т.н., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*29*» *квітня* *2024* року № *4/7-470*

2. Термін подання студентом завершеної роботи 24 червня 2025р.

3. Вихідні дані до роботи Літературні та інтернет джерела інформації про технології Site-to-Site та Remote Access VPN. Документація по MikroTik, Windows Server 2022, Ubuntu Linux.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1) Аналіз завдання та огляд предметної області
2) Реалізація VPN на основі MikroTik
3) Практичне тестування VPN мережі
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. Завдання дослідження. 5. Схема під'єднання елементів системи. 6. Характеристика мікрокомп'ютера та мікроконтролера. 7. Характеристика давачів системи. 8. Характеристика давачів системи (продовження). 9. Вибір мови програмування та налаштування Arduino. 10. Налаштування MQTT та створення Telegram-bot на Raspberry Pi Zero 2 W. 11. Розробка корпусу для монтажу та вставлення системи. 12. Перевірка роботи системи. 13. Висновки. 14. Завершальний.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Сенчишин В. С., к.т.н. доцент кафедри МТ	12.06.2024	14.06.2024

7. Дата видачі завдання 29 січня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	30.01.2024	*Виконано*
2.	Підбір джерел по темі кваліфікаційної роботи	31.01.2024-03.02.2024	*Виконано*
3.	Опрацювання джерел по темі кваліфікаційної роботи	04.02.2024-06.02.2024	*Виконано*
4.	Виконання дослідження щодо розгортання	07.02.2024-11.02.2024	*Виконано*
	і тестування технології Site-to-Site та Remote Access		
	VPN		
5.	Оформлення розділу «Аналіз завдання та огляд	03.06.2024-05.06.2024	*Виконано*
	предметної області»		
6.	Оформлення розділу «Реалізація VPN на основі	06.06.2024-08.06.2024	*Виконано*
	MikroTik»		
6.	Оформлення розділу «Практичне тестування VPN	09.06.2024-11.06.2024	*Виконано*
	мережі»		
7.	Виконання завдання до розділу «Безпека життєдіяльності»	12.06.2024-13.06.2024	*Виконано*
8.	Виконання завдання до підрозділу «Основи охорони	14.06.2024-15.06.2024	*Виконано*
	праці»		
9.	Оформлення кваліфікаційної роботи	16.06.2024-17.06.2024	*Виконано*
10.	Нормоконтроль	18.06.2024-19.06.2024	*Виконано*
11.	Перевірка на плагіат	20.06.2024	*Виконано*
12.	Попередній захист кваліфікаційної роботи	21.06.2024	*Виконано*
13.	Захист кваліфікаційної роботи	30.06.2024	

Студент _____ Кудрик Д.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Гром'як Р.С.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аналіз, розгортання і тестування технології Site-to-Site та Remote Access VPN // Кваліфікаційна робота освітнього рівня «Бакалавр» // Кудрик Дмитро Володимирови // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СН-42 // Тернопіль, 2025 // С.73, рис. – 32, табл. – 0, кресл. – 14, додат. – 2, бібліогр. – 35.

Ключові слова: MikroTik, VPN, L2TP/IPSec, WireGuard, RDS, Remote Access, Site-to-Site, Windows Server.

У кваліфікаційній роботі бакалавра розглянуто питання побудови захищених віртуальних приватних мереж (VPN) у корпоративному середовищі з використанням мережевого обладнання MikroTik. Метою дослідження було проєктування, налаштування та практичне тестування VPN-рішень для забезпечення безпечного обміну даними між віддаленими користувачами та офісними сегментами мережі та між географічно розподіленими офісами. У роботі проаналізовано теоретичні основи протоколів тунелювання, зокрема L2TP/IPSec та WireGuard, а також розглянуто їх особливості впровадження в сучасних мережевих інфраструктурах. Результатом практичної частини стало розгортання двох типів VPN-з'єднань: Remote Access VPN для мобільних користувачів та Site-to-Site VPN для об'єднання головного офісу з філією. Проведене тестування в лабораторному середовищі засвідчило стабільність, безпечність і ефективність налаштованих тунелів. Отримані результати підтверджують доцільність і готовність запропонованого рішення до впровадження в умовах реального підприємства.

ANNOTATION

Analyse, deploy and test Site-to-Site and Remote Access VPN technology // Qualification work of the educational level "Bachelor" // Dmytro Kudryk // Ternopil Ivan Pulyu National Technical University, Computer and Information Systems and Software Engineering Faculty, Computer Sciences Department, group SN-42 // Ternopil, 2025 // P. 73, fig. - 32, tabl. - 0, drawings - 14, annexes. – 2, references - 35.

Keywords: MikroTik, VPN, L2TP/IPSec, WireGuard, RDS, Remote Access, Site-to-Site, Windows Server.

The bachelor's thesis examines the construction of secure virtual private networks (VPNs) in a corporate environment using MikroTik network equipment. The purpose of the study was to design, configure, and test VPN solutions to ensure secure data exchange between remote users and office segments of the network and between geographically distributed offices. The paper analyses the theoretical foundations of tunnelling protocols, in particular L2TP/IPSec and WireGuard, and discusses their implementation features in modern network infrastructures. The practical part resulted in the deployment of two types of VPN connections: Remote Access VPN for remote users and Site-to-Site VPN to connect the main office with a branch office. Testing in the lab environment proved the stability, security and efficiency of the configured tunnels. The results confirm the feasibility and readiness of the proposed solution for implementation in a real enterprise.

ПЕРЕЛІК СКОРОЧЕНЬ

VPN (англ. Virtual Private Network) - Віртуальна приватна мережа.

PPTP (англ. Point-to-Point Tunneling Protocol) - Протокол тунелювання точка-точка.

L2TP/IPSec (англ. Layer 2 Tunneling Protocol з IPSec) - Тунельний протокол 2-го рівня з IPSec.

CHR (англ. Cloud Hosted Router) - Хмарний маршрутизатор.

DMZ (англ. Demilitarized Zone) - Ізольований сегмент мережі,.

AES (англ. Advanced Encryption Standard) - Розширений стандарт шифрування.

CBC (англ. Cipher Block Chaining) - Ланцюжок блоків шифрування.

RDS (англ. Remote Desktop Services) - Служби віддаленого робочого столу.

RDP (англ. Remote Desktop Protocol) - Протокол віддаленого робочого столу.

ЗМІСТ

ВСТУП

Актуальність теми. В умовах стрімкого зростання обсягів передавання даних, гібридного формату роботи та зростання кіберзагроз, забезпечення захищеного мережевого доступу до корпоративних ресурсів стало одним із пріоритетних завдань для IT-інфраструктури підприємств. Особливої актуальності набувають технології VPN, які дозволяють створювати безпечні канали зв'язку через публічні мережі, зокрема Інтернет. Remote Access VPN забезпечує захищене підключення працівників до внутрішніх ресурсів організації з будь-якої локації, що є критично важливим у контексті віддаленої роботи. Site-to-Site VPN, у свою чергу, дозволяє об'єднувати окремі офіси підприємства в єдину корпоративну мережу. З огляду на широке застосування цих технологій, а також потребу в практичному впровадженні надійних і гнучких рішень - тема аналізу, розгортання та тестування VPN є надзвичайно актуальною.

Мета і задачі дослідження. Метою даної роботи є дослідження принципів побудови захищених VPN-з'єднань на основі технологій Remote Access VPN та Site-to-Site VPN, а також практична реалізація та тестування зазначених технологій у віртуальному середовищі з використанням MikroTik CHR.

Для досягнення поставленої мети було сформульовано такі основні задачі:

– провести огляд типів VPN, протоколів тунелювання та шифрування;

– дослідити архітектуру побудови Remote Access VPN для організації безпечного доступу працівників до внутрішньої мережі;

– проаналізувати принципи побудови Site-to-Site VPN між територіально віддаленими сегментами корпоративної мережі;

– реалізувати середовище тестування з VPN;

– налаштувати L2TP/IPSec Remote Access VPN та WireGuard Site-to-Site VPN, а також відповідні правила брандмауеру;

– здійснити тестування VPN-підключень з Windows 10 та Ubuntu Linux;

– перевірити доступність Windows Server 2022 RDS через захищені канали зв’язку.

Об’єкт дослідження. Об’єктом дослідження є засоби та методи побудови захищених віртуальних приватних мереж у корпоративному середовищі.

Предмет дослідження. Предметом дослідження є технології VPN типів Remote Access та Site-to-Site, їхнє налаштування, захист, інтеграція у корпоративну інфраструктуру та тестування.

Практичне значення одержаних результатів. Практичне значення дослідження полягає у розробці та впровадженні повноцінної моделі VPN-інфраструктури з використанням MikroTik CHR, що може бути адаптована для невеликих і середніх підприємств, навчальних закладів або організацій з територіально розподіленими офісами. Реалізована система дозволяє забезпечити безпечний віддалений доступ до внутрішніх ресурсів, а також об'єднання мереж філій у єдину захищену структуру, що підвищує загальний рівень інформаційної безпеки. Отримані результати можуть бути використані як основа для подальших розробок, оптимізації VPN-сценаріїв та навчальних цілей у сфері мережевої безпеки.

РОЗДІЛ 1. АНАЛІЗ ЗАВДАННЯ ТА ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Поняття та призначення VPN

Віртуальна приватна мережа - це технологія, яка дозволяє створювати захищене логічне з’єднання (тунель) між окремими вузлами або мережами через незахищену публічну інфраструктуру, зокрема через Інтернет. Основною функцією VPN є забезпечення конфіденційності, цілісності та автентичності переданої інформації, а також імітація прямого підключення користувача або віддаленої мережі до локальної корпоративної мережі [1].

З технічної точки зору, VPN працює шляхом інкапсуляції мережевого трафіку всередині спеціального протоколу тунелювання, який, у свою чергу, може бути зашифрований криптографічними алгоритмами для унеможливлення перехоплення або модифікації даних третіми сторонами. Це дозволяє забезпечити безпечну передачу інформації навіть через потенційно небезпечні мережі [2].

На рисунку 1.1 показано схему підключення до Інтернету без використання VPN, яка ілюструє, як відбувається обмін даними між пристроєм користувача та вебресурсами у відкритому середовищі, без шифрування або захисного тунелю.

У цьому випадку усі запити та відповіді передаються відкрито через інфраструктуру інтернет-провайдера (ISP), без застосування додаткового шифрування або тунелювання. Коли користувач із пристрою, наприклад ноутбука чи смартфона, надсилає запит до певного вебсайту чи онлайн-сервісу, цей запит проходить через провайдера, який забезпечує з’єднання з Інтернетом. Відповідь від сервера вебресурсу також повертається до користувача через того ж провайдера.

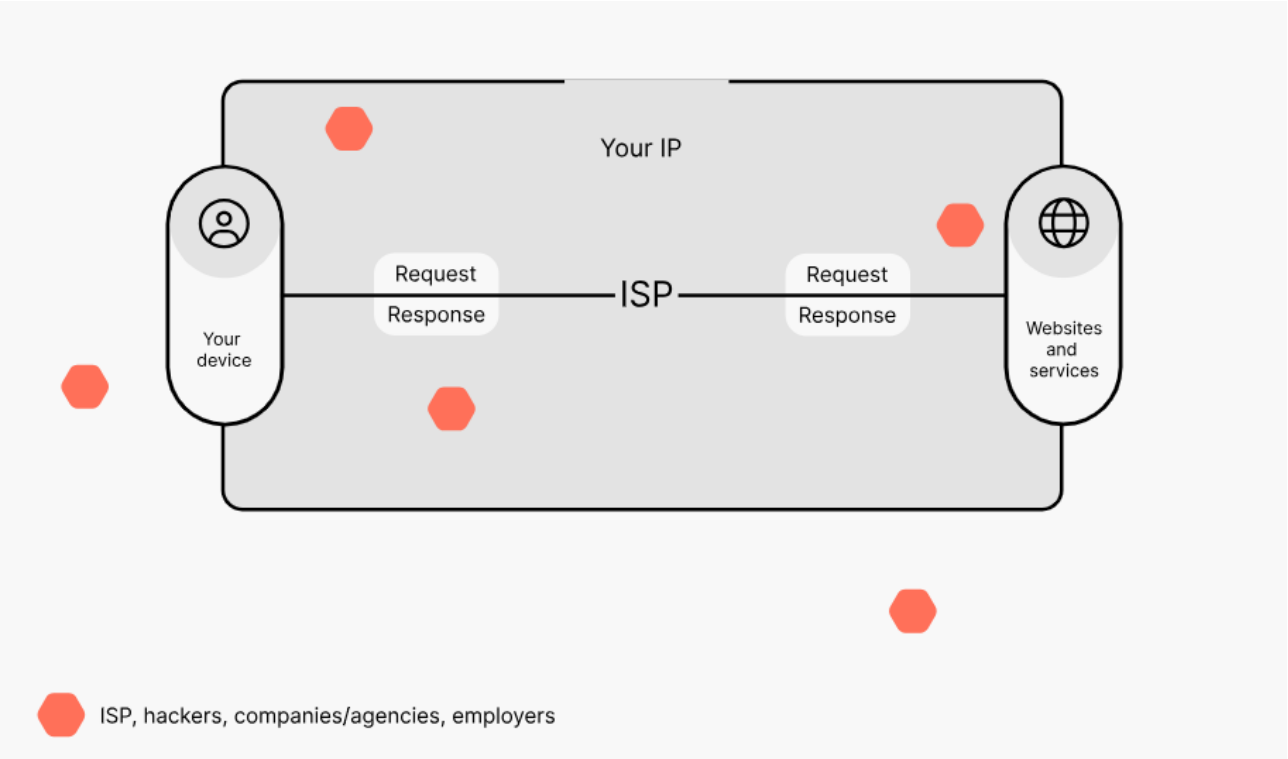

Рисунок 1.1 – Схема підключення до Інтернету без використання VPN

У цій конфігурації весь мережевий трафік є прозорим для будь-яких сторін, що мають доступ до транспортного каналу, включаючи самого провайдера, роботодавців, державні або приватні агентства, а також зловмисників. Вони можуть не лише бачити, куди саме прямує трафік і що він містить (якщо не використовується HTTPS), а також відстежувати IP-адресу користувача, його місце розташування та онлайн-активність. Саме IP-адреса користувача залишається видимою для зовнішніх ресурсів, що дозволяє їм формувати профіль активності, застосовувати геолокаційне фільтрування або персоналізовану рекламу.

Така модель з’єднання є типовою для ситуацій, коли не використовується VPN або будь-яка інша технологія шифрування на рівні мережевого з’єднання. Вона є технічно простою, проте водночас суттєво вразливою до кіберзагроз, витоку даних, атак типу «людина посередині» та несанкціонованого спостереження. Схема наочно демонструє, що без VPN користувач не має належного контролю над тим, хто бачить його трафік і яку інформацію можна з нього зчитати. Це створює потребу у впровадженні додаткових засобів захисту,

зокрема тунелювання та шифрування трафіку, які усувають видимість маршруту передачі даних та захищають інформацію від зовнішнього втручання.

На рисунку 1.2 представлено схему підключення до Інтернету з використанням VPN, яка демонструє, як працює зашифрований VPN-тунель між пристроєм користувача і віддаленим VPN-сервером [3].

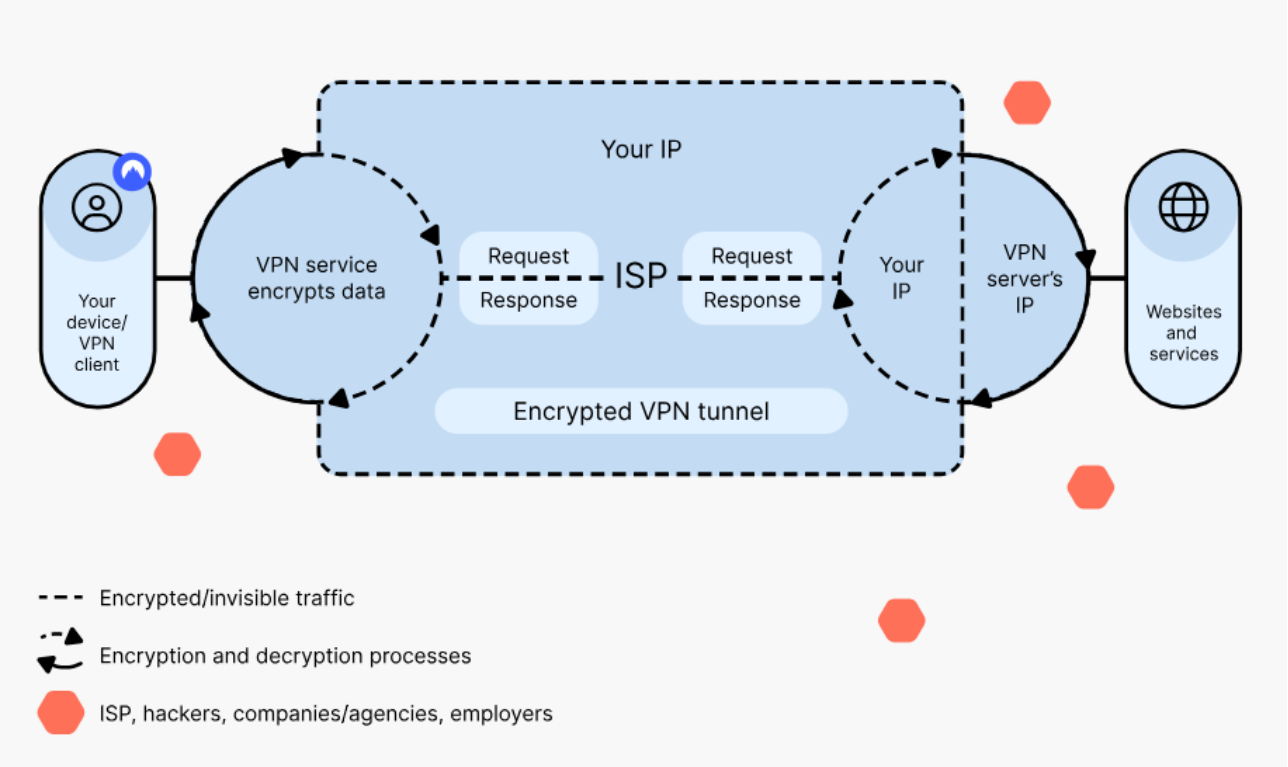

Рисунок 1.2 – Схема підключення до Інтернету з використання VPN

Така модель з'єднання дозволяє приховати справжню IP-адресу користувача, забезпечити конфіденційність передавання даних та захистити трафік від спостереження чи перехоплення з боку третіх осіб.

Початковою точкою є пристрій користувача (комп'ютер, смартфон тощо), на якому встановлено VPN-клієнт. Саме він ініціює з'єднання з VPN-сервером. Усі дані, які надсилаються з пристрою, спершу шифруються цим клієнтом [4]. Далі вони потрапляють до інтернет-провайдера, однак у зашифрованому вигляді, тобто провайдер технічно бачить лише факт передачі даних, але не може дізнатися ні їхнього вмісту, ні цільового вебресурсу. Після цього шифрований трафік проходить через тунель до VPN-сервера. Саме тут

відбувається розшифрування і передача даних далі - до вебсайтів або онлайн-сервісів. Тобто зовнішній ресурс бачить вже не вашу реальну IP-адресу, а адресу VPN-сервера. Це дозволяє приховати ваше місцезнаходження, а також обійти географічні обмеження або цензуру. Два процеси шифрування та дешифрування (на вході в тунель і на виході) символізують обробку даних VPN-сервісом. При цьому зовнішні загрози, такі як інтернет-провайдери, хакери, агентства чи роботодавці, все ще присутні в навколишньому середовищі, але не мають доступу до самого трафіку - він для них є зашифрованим і непрозорим.

Таким чином, ця схема показує, що при використанні VPN:

– усі передані дані є зашифрованими від пристрою до VPN-сервера;

– провайдер не має доступу до вмісту трафіку і не бачить кінцевих ресурсів;

– реальна IP-адреса користувача приховується;

– підключення до Інтернету стає значно безпечнішим, особливо у відкритих Wi-Fi мережах або при використанні публічної інфраструктури.

Це є основною перевагою VPN - створення захищеного та приватного каналу комунікації навіть у загальнодоступному середовищі.

1.2 Класифікація VPN за типами доступу

Віртуальні приватні мережі класифікуються за способом організації з’єднання та характером взаємодії між вузлами. Одним із ключових критеріїв класифікації є тип доступу, який VPN забезпечує для користувача або мережі. Залежно від цього є два основних типів VPN-доступу: Remote Access VPN, Site-to-Site VPN, а також допоміжні підходи, такі як Cloud VPN та SSL VPN, які використовуються в спеціалізованих сценаріях.

Remote Access VPN - це один із найпоширеніших типів віртуальних приватних мереж, призначений для забезпечення безпечного з'єднання окремого пристрою користувача з внутрішньою мережею організації через

загальнодоступний Інтернет [5]. Його ключова мета полягає у наданні співробітникам, підрядникам або партнерам можливості отримати повноцінний доступ до корпоративних ресурсів із будь-якої точки світу без ризику перехоплення чи модифікації даних.

Архітектура Remote Access VPN передбачає, що на стороні користувача встановлюється спеціалізоване програмне забезпечення - VPN-клієнт, який ініціює захищене з'єднання з VPN-сервером, розміщеним у внутрішній мережі компанії або у хмарній інфраструктурі (див. рисунок 1.3).

Рисунок 1.3 – Remote Access VPN

Перед передачею даних клієнт шифрує їх за допомогою криптографічних алгоритмів, після чого інформація проходить через VPN-тунель до сервера, де вона розшифровується і передається далі до внутрішніх систем, таких як файлові сховища, вебпортали, бази даних або термінальні сервери. У зворотному напрямку трафік проходить той самий шлях - але знову ж таки у зашифрованому вигляді. Remote Access VPN забезпечує кілька рівнів захисту. По-перше, трафік між клієнтом і корпоративною мережею не доступний для інспекції з боку провайдерів, хакерів або шпигунських програм, оскільки весь канал є зашифрованим. По-друге, такі системи зазвичай використовують механізми автентифікації - від простих логінів і паролів до двофакторної автентифікації або автентифікації на основі сертифікатів. Це значно ускладнює

доступ несанкціонованим користувачам. Нарешті, VPN-сервер може бути налаштований з обмеженнями доступу до певних сегментів мережі, що забезпечує принцип найменших привілеїв.

Особливу актуальність Remote Access VPN набув у період масового переходу на дистанційну роботу. У багатьох компаніях, зокрема в умовах пандемій або воєнного стану, працівники змушені працювати з дому або з тимчасових офісів. Завдяки VPN технології вони можуть підключатися до внутрішніх сервісів так, ніби знаходяться фізично у корпоративній мережі. Це дозволяє зберігати цілісність робочих процесів і гарантує відповідність політикам безпеки підприємства. Серед протоколів, які застосовуються для реалізації Remote Access VPN, найбільш популярними є L2TP/IPSec, IKEv2, OpenVPN, SSTP та сучасний WireGuard. Кожен з них має свої переваги залежно від операційної системи, середовища впровадження та вимог до продуктивності або рівня шифрування.

Загалом, Remote Access VPN є надійним інструментом створення захищеного доступу для індивідуальних користувачів і активно використовується у корпоративному секторі, освітніх установах та державних органах. Він дозволяє розширити периметр безпеки організації за межі фізичної мережі, не знижуючи при цьому рівень захисту даних.

Site-to-Site VPN - це тип віртуальної приватної мережі, який використовується для створення постійного, захищеного з'єднання між двома або більше віддаленими мережами, наприклад, між головним офісом компанії та її філіями [6]. Основна мета цієї технології полягає в об’єднанні розподілених мережевих сегментів в єдину логічну структуру, яка дозволяє пристроям з різних географічних локацій спілкуватися між собою так, ніби вони розташовані в одному локальному середовищі.

У Site-to-Site VPN відсутня потреба в індивідуальному VPN-клієнті на кожному пристрої. Натомість шифрування та тунелювання трафіку здійснюється на рівні мережевих шлюзів - зазвичай це маршрутизатори або міжмережеві екрани, які підтримують VPN-функції. У кожному офісі

конфігурується VPN-шлюз, який встановлює зашифроване з'єднання з відповідним вузлом в іншому офісі. Після встановлення тунелю весь трафік між локальними мережами автоматично шифрується та передається через Інтернет або іншу незахищену мережу, що забезпечує цілісність і конфіденційність даних (див. рисунок 1.4).

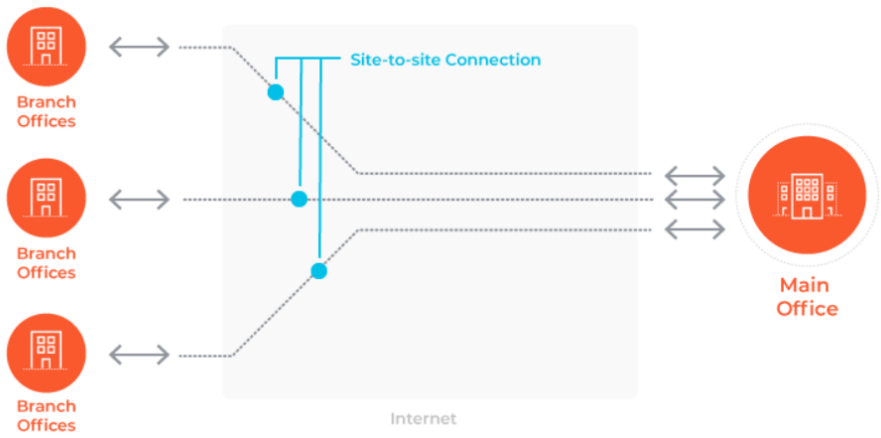

Рисунок 1.4 – Site-to-Site VPN

Типовий приклад використання Site-to-Site VPN - підключення офісу філії до головного офісу підприємства. Працівники філії можуть отримати доступ до файлових серверів, корпоративних застосунків, баз даних або телефонії, що розміщені в основному офісі, без потреби в налаштуванні окремих підключень на кожному пристрої. Аналогічно, сервери основного офісу можуть передавати дані у філію, наприклад, для резервного копіювання або синхронізації.

З технічного боку Site-to-Site VPN реалізується за допомогою різних протоколів, серед яких найбільш поширені - IPSec, OpenVPN, L2TP/IPSec, а також сучасний WireGuard. Протоколи IPSec та L2TP/IPSec забезпечують високий рівень сумісності між різними пристроями (Cisco, MikroTik, FortiGate, pfSense, тощо) та широко підтримуються апаратно. WireGuard, який є відносно новим рішенням, демонструє високу продуктивність і простоту налаштування при збереженні сильної криптографії. Окремою перевагою Site-to-Site VPN є централізація безпеки. Оскільки VPN-шлюз виконує роль єдиного каналу обміну між офісами, адміністратор має змогу централізовано контролювати

доступ, застосовувати політики безпеки, вести аудит трафіку та застосовувати міжмережевий екран. Це знижує ризики, пов’язані з налаштуванням кінцевих пристроїв, та забезпечує більш надійне управління інформаційними потоками.

Site-to-Site VPN особливо ефективний у великих підприємствах, де є потреба в постійному і надійному обміні даними між офісами, складами, дата-центрами або хмарною інфраструктурою. Таким чином, Site-to-Site VPN дозволяє підприємствам значно підвищити рівень захищеності міжмережевого трафіку, знизити залежність від фізичних каналів зв’язку, а також оптимізувати архітектуру розподіленої IT-інфраструктури без втрати продуктивності чи гнучкості.

1.3 Протоколи тунелювання та шифрування

Функціонування VPN базується на створенні зашифрованого тунелю між клієнтом і сервером, через який передаються дані. Для реалізації цього тунелю використовуються спеціальні протоколи, які забезпечують інкапсуляцію, шифрування та автентифікацію трафіку. Різні VPN-протоколи мають свої особливості в частині продуктивності, безпеки, складності налаштування та сумісності з операційними системами [7].

PPTP - один із перших масово застосовуваних VPN-протоколів. Він забезпечує інкапсуляцію трафіку PPP у GRE і підтримує базові механізми автентифікації, зокрема MS-CHAPv2. Хоча PPTP відзначається високою швидкістю з'єднання і простотою конфігурації, він має серйозні вразливості у сфері криптографії і більше не вважається безпечним для використання в умовах сучасних загроз. Його підтримка поступово зникає з нових версій операційних систем.

L2TP/IPSec - комбінація двох протоколів, де L2TP забезпечує тунелювання, а IPSec - шифрування та автентифікацію. Такий підхід дозволяє досягти високого рівня безпеки, зокрема завдяки використанню алгоритмів шифрування AES і автентифікації на базі попередньо узгоджених ключів або

сертифікатів. Протокол підтримується більшістю сучасних ОС і часто використовується для створення Remote Access VPN у корпоративному середовищі. Однак він вимагає відкриття додаткових портів і складнішої конфігурації.

OpenVPN - один із найпопулярніших і надійних VPN-протоколів з відкритим вихідним кодом. Він працює поверх протоколів TCP або UDP і використовує бібліотеку OpenSSL для реалізації криптографії, включаючи підтримку сертифікатів X.509, TLS-шифрування і HMAC для цілісності даних. OpenVPN вирізняється високим рівнем безпеки, гнучкістю налаштування та здатністю обходити міжмережеві екрани, маскуючись під звичайний HTTPS-трафік. Його мінусом є відносно високе навантаження на процесор і потреба в окремому програмному забезпеченні.

WireGuard - новітній VPN-протокол з відкритим кодом, який швидко здобув популярність завдяки своїй простоті, мінімалізму коду і використанню сучасної криптографії. WireGuard застосовує протоколи Curve25519, ChaCha20, Poly1305 та інші безпечні алгоритми, які забезпечують одночасно високий рівень шифрування та надзвичайну продуктивність. Протокол працює поверх UDP, забезпечує швидке встановлення тунелю і надійність передачі. Він став рідним модулем ядра Linux і активно інтегрується у сучасні VPN-рішення, зокрема MikroTik, OPNsense, pfSense тощо.

SSTP (Secure Socket Tunneling Protocol) - протокол, розроблений Microsoft, який використовує HTTPS (TCP порт 443) для передавання зашифрованого трафіку. Завдяки цьому він легко проходить через більшість міжмережевих екранів. SSTP забезпечує високий рівень захисту за рахунок використання TLS і шифрування за допомогою сертифікатів. Він підтримується переважно у середовищі Windows і є зручним для інтеграції у корпоративну інфраструктуру Microsoft. Утім, закритий вихідний код обмежує можливості незалежного аудиту.

IKEv2/IPSec (Internet Key Exchange версії 2 з IPSec) - сучасний і ефективний протокол тунелювання, який забезпечує стійке шифрування,

динамічну зміну ключів і підтримку мобільності, зокрема автоматичне відновлення з'єднання після зміни IP-адреси (наприклад, при переході між Wi-Fi та мобільною мережею). Він є дуже надійним у мобільних сценаріях використання (iOS і Android) та підтримується більшістю операційних систем. IKEv2, як і L2TP, вимагає налаштування IPSec.

Вибір протоколу залежить від конкретних завдань, апаратного середовища, очікуваного рівня безпеки, продуктивності й сумісності. У більшості сучасних рішень перевага віддається OpenVPN, WireGuard, L2TP/IPSec і IKEv2/IPSec як найоптимальнішим протоколам з точки зору балансу між безпекою, стабільністю та гнучкістю впровадження.

1.4 Висновок до першого розділу

У першому розділі було здійснено оглід предметної області, пов’язаної з побудовою віртуальних приватних мереж, їх призначенням, типами доступу та основними протоколами, що використовуються для забезпечення захищеної передачі даних у публічному середовищі. Розглянуто загальні принципи функціонування VPN як технології, що створює логічні захищені канали зв’язку через незахищені мережі, зокрема Інтернет. Показано, що VPN-технології відіграють ключову роль у забезпеченні конфіденційності, цілісності та автентичності даних, особливо в умовах зростаючої потреби в мобільності, віддаленому доступі та кіберзахисті. Розкрито поняття VPN та охарактеризовано його базові властивості, зокрема інкапсуляцію і шифрування трафіку. На основі аналізу було порівняно два підходи до з’єднання з мережею - без використання VPN та із застосуванням захищеного VPN-тунелю, що дало змогу наочно продемонструвати вразливість відкритого трафіку та переваги використання VPN для захисту особистих і корпоративних даних.

Проведено класифікацію VPN за типами доступу. Розглянуто два основні типи: Remote Access VPN та Site-to-Site VPN. Встановлено, що Remote Access VPN забезпечує захищений віддалений доступ окремих користувачів до

внутрішньої мережі підприємства, тоді як Site-to-Site VPN дозволяє об'єднувати географічно розподілені мережі в єдину захищену інфраструктуру без потреби в індивідуальному налаштуванні на кожному клієнтському пристрої. Визначено особливості архітектури кожного з типів, сценарії їх використання, а також їхнє значення для організації безпечного доступу до критично важливих ресурсів. Окремо проаналізовано найбільш поширені протоколи тунелювання та шифрування у VPN: PPTP, L2TP/IPSec, OpenVPN, WireGuard, SSTP та IKEv2/IPSec. Встановлено, що сучасні рішення надають перевагу OpenVPN, WireGuard, L2TP/IPSec та IKEv2/IPSec завдяки їхній надійності, гнучкості, високій швидкості роботи та підтримці сучасних криптографічних алгоритмів.

Отримані результати створюють міцне теоретичне підґрунтя для подальшого проєктування, розгортання та тестування VPN-рішень у практичній частині дослідження, де буде реалізовано моделі Remote Access VPN та Site-to-Site VPN з використанням MikroTik CHR.

РОЗДІЛ 2. РЕАЛІЗАЦІЯ VPN НА ОСНОВІ MIKROTIK

2.1 Схема тестового середовища

Лабораторне середовище дає змогу комплексно протестувати механізми VPN-доступу, перевірити ефективність тунелювання, маршрутизації та політик безпеки, а також змоделювати типову корпоративну інфраструктуру з підтримкою безпечної віддаленої роботи та міжофісного обміну даними [8] [9].

На рисунку 2.1 представлено схему лабораторного середовища, яке створено для моделювання, розгортання та тестування двох типів VPN-з'єднань — L2TP/IPSec Remote Access VPN та WireGuard Site-to-Site VPN.

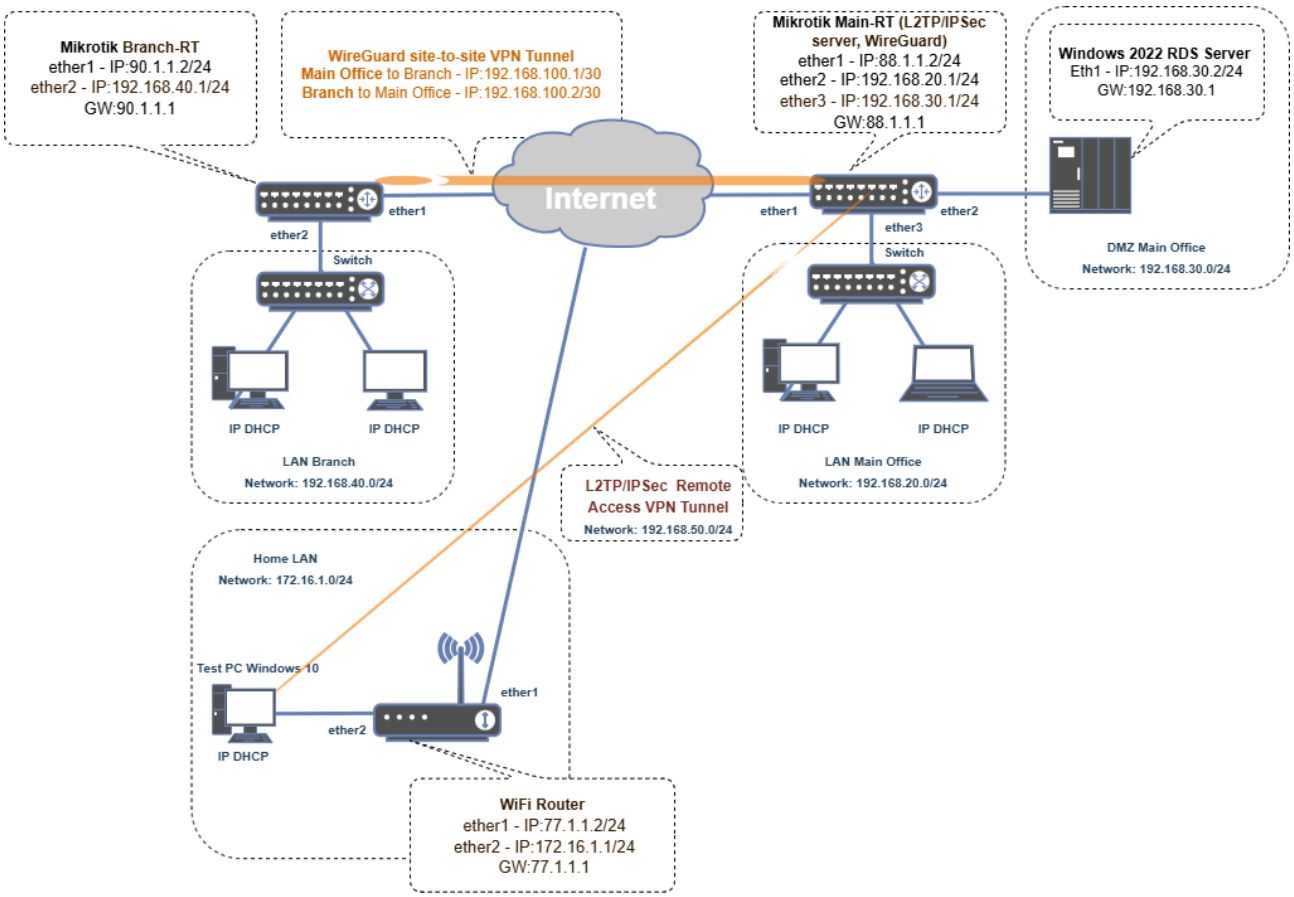

Рисунок 2.1 – Схема лабораторного середовища

Середовище тестування умовно поділене на три основні частини:

- Main Office (основний офіс);
- Branch (віддалений офіс);
- Home LAN (домашній сегмент для тестування Remote Access VPN).

Мережі з'єднані між собою через емульований доступ до мережі Інтернет (умовна хмара), за якою відбувається передавання VPN-трафіку.

Центральним елементом є віртуальний маршрутизатор MikroTik Main-RT, який виконує роль VPN-сервера та шлюзу. Він має три мережеві інтерфейси:

- ether1 (WAN) з IP–адресою 88.1.1.2/24, шлюз – 88.1.1.1;
- ether2 підключений до внутрішньої локальної мережі (LAN Main Office) з підмережею 192.168.20.0/24;
- ether3 підключений до DMZ-сегменту, де розташований Windows Server 2022 з RDS у мережі 192.168.30.0/24

На маршрутизаторі Main-RT налаштовані L2TP/IPSec сервер для забезпечення доступу віддалених користувачів та WireGuard VPN для Site-to-Site з’єднання з філією. Клієнтські пристрої отримують адреси по DHCP і мають доступ до внутрішніх ресурсів. Windows Server 2022 RDS розміщений у DMZ, має IP 192.168.30.2 та шлюз – 192.168.30.1. Надає віддалений доступ до сервісу RDS і використовується для перевірки функціональності доступу через обидва типи VPN.

Віддалений офіс також представлений віртуальним маршрутизатором MikroTik Branch-RT, що має такі інтерфейси:

- ether1 (WAN) з IP–адресою 90.1.1.2/24 та шлюзом – 90.1.1.1;
- ether2 підключення до локальної мережі філії з підмережею 192.168.40.0/24;

Між Branch-RT і Main-RT налаштовано WireGuard Site-to-Site VPN:

- тунель Main Office → Branch з IP–адресою 192.168.100.1/30;
- тунель Branch → Main Office з IP–адресою 192.168.100.2/30.

Клієнтські ПК у філії отримують IP через DHCP, мають доступ до ресурсів Main Office через захищене VPN-з’єднання.

Домашнє середовище Home LAN (тестовий сегмент для Remote Access VPN) включає WiFi-роутер, що має інтерфейси:

- ether1 з IP –адресою 77.1.1.2/24 та шлюзом – 77.1.1.1 (WAN-з'єднання з Інтернетом);
- ether2 з IP –адресою 172.16.1.1/24 (внутрішній сегмент).

Тестовий ПК з Windows 10 отримує IP через DHCP з підмережі 172.16.1.0/24. Саме на цьому ПК проводиться підключення до L2TP/IPSec сервера, розгорнутого на MikroTik Main-RT.

L2TP/IPSec Remote Access VPN забезпечує доступ із домашнього ПК до ресурсів головного офісу. Після підключення через тунель користувач стає частиною внутрішньої мережі 192.168.50.0/24. WireGuard Site-to-Site VPN реалізує постійне захищене з’єднання між Main Office і Branch, дозволяючи пристроям з 192.168.40.0/24 отримувати доступ до ресурсів в 192.168.20.0/24 та 192.168.30.0/24 підмережах.

Усі компоненти середовища розгорнуті як віртуальні машини в VMware Workstation Pro. Це дозволяє легко моделювати ізольовані сегменти, налаштовувати маршрутизацію, VPN-тунелі, фільтрацію трафіку, а також виконувати тестування без залучення фізичної інфраструктури.

2.2 Маршрутизатор MikroTik

MikroTik - це латвійська компанія, яка спеціалізується на розробці мережевого обладнання та програмного забезпечення, зокрема маршрутизаторів, точок доступу та бездротових систем [10]. Основним продуктом компанії є операційна система RouterOS [11], яка встановлюється як на власне апаратне забезпечення MikroTik, так і на віртуальні машини, що дозволяє розгортати повноцінні маршрутизатори у віртуалізованому середовищі [12].

Маршрутизатор MikroTik поєднує в собі функціонал класичного маршрутизатора, міжмережевого екрана, DHCP-сервера, VPN-шлюзу, проксі-

сервера, точки доступу та багатьох інших компонентів у єдиному пристрої. Завдяки широкому набору функцій, доступності та простому ліцензуванню, MikroTik здобув популярність серед малого та середнього бізнесу та провайдерів.

Керування маршрутизатором MikroTik може здійснюватися через кілька інтерфейсів: графічна утиліта Winbox [13] (див. рисунок 2.2), веб-інтерфейс, командний рядок (CLI) через SSH-доступ. Це забезпечує зручність як для початківців, так і для досвідчених системних адміністраторів.

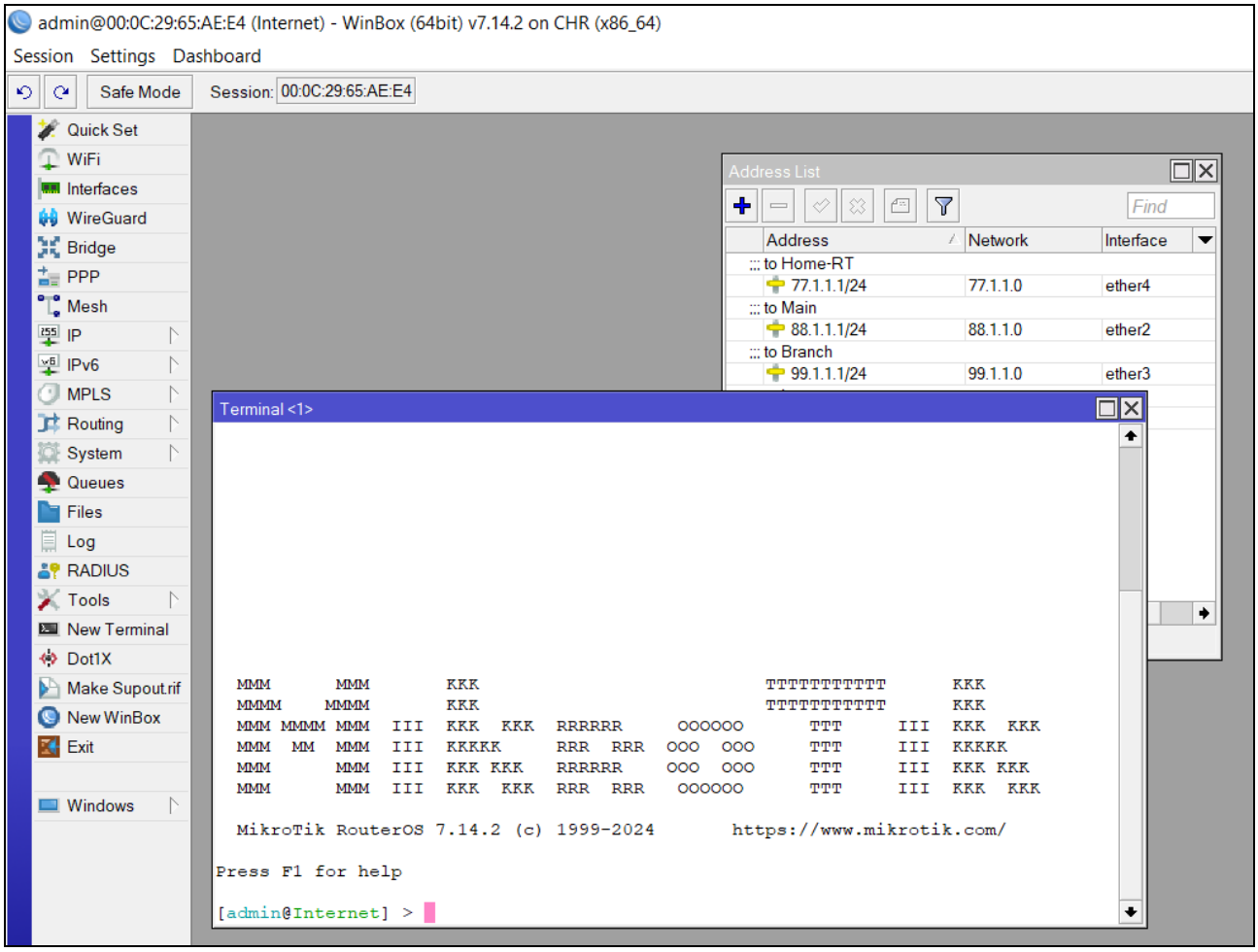

Рисунок 2.2 – Інтерфейс Winbox для управляння MikroTik

У системі MikroTik можливо детально налаштувати маршрутизацію - як статичну, так і динамічну (OSPF, BGP, RIP). Окрім того, пристрій підтримує створення віртуальних локальних мереж (VLAN), NAT, політики маршрутизації, queue для управління трафіком, брандмауер, захист від DoS-

атак [14] [15], журналювання подій та багато іншого. Завдяки підтримці VPN-протоколів, таких як L2TP/IPSec, PPTP, SSTP, OpenVPN та WireGuard, MikroTik може бути використаний як шлюз для віддаленого доступу або як маршрутизатор для побудови Site-to-Site тунелів.

У лабораторних середовищах MikroTik у вигляді CHR дозволяє легко емулювати багатосегментну мережу. MikroTik CHR - це спеціалізована версія операційної системи MikroTik RouterOS, розроблена для розгортання у віртуальному середовищі [16]. На відміну від фізичних пристроїв MikroTik, CHR не прив’язаний до конкретного апаратного забезпечення, а працює як віртуальна машина на базі гіпервізорів типу VMware Workstation, ESXi, VirtualBox, Hyper-V або в хмарних інфраструктурах, таких як Amazon AWS, Microsoft Azure, Google Cloud та інших [17]. Основною метою створення CHR є забезпечення гнучкості, масштабованості та економії ресурсів при побудові маршрутизованих середовищ, зокрема для задач VPN, брандмауера, маршрутизації трафіку, балансування навантаження та лабораторного тестування.

MikroTik CHR має повноцінний функціонал RouterOS і включає всі ключові можливості. Це означає, що віртуальний MikroTik CHR здатен повністю замінити апаратний маршрутизатор в умовах, де фізична інфраструктура або бюджет обмежені. Його функціональність не урізана - вона ідентична до RouterOS Level 7, і відрізняється лише пропускною здатністю, яка залежить від ліцензії. MikroTik CHR розповсюджується у підготовленого шаблону, який імпортується до гіпервізора. Після розгортання йому можна призначити потрібну кількість інтерфейсів, CPU, оперативної пам’яті та дискового простору. Завдяки цьому CHR ідеально підходить для лабораторних стендів, коли потрібно змоделювати мережу з декількома сегментами, філіями або для тестування VPN-тунелів. Це особливо зручно в поєднанні з віртуальними машинами на базі Windows, Linux або серверних ОС, які можуть взаємодіяти з маршрутизатором, виконуючи роль клієнтів або внутрішніх серверів. Для керування MikroTik CHR можна використовувати ті самі засоби,

що й для фізичного обладнання. Після встановлення CHR не потребує складної активації - його можна запустити з пробною ліцензією P1 на 60 днів, яка обмежує пропускну здатність до 1 Гбіт/с, чого цілком достатньо для більшості лабораторних задач. При потребі у високопродуктивних середовищах можна активувати ліцензії P10, P-Unlimited тощо.

Суттєвою перевагою MikroTik CHR є його незалежність від фізичних інтерфейсів: замість апаратних портів він використовує віртуальні мережеві адаптери гіпервізора, які можуть бути підключені до віртуальних комутаторів, NAT-сегментів або до фізичного мережевого інтерфейсу хост-машини. Це відкриває широкі можливості для створення складних топологій, включаючи ізольовані VLAN, тунелі VPN, DMZ-сегменти, системи моніторингу трафіку тощо. MikroTik CHR також активно використовується у виробничих середовищах, коли потрібно швидко розгорнути маршрутизатор у хмарі або організувати резервне рішення без закупівлі обладнання. Його також можна використовувати для тестування нових конфігурацій, скриптів або оновлень без ризику для основної мережі.

Таким чином, MikroTik CHR - це повноцінний, універсальний, програмно-визначений маршрутизатор, який поєднує потужність RouterOS з гнучкістю віртуалізації. Він ідеально підходить для навчання, тестування, віддаленого управління інфраструктурою, побудови VPN-сервісів і для продуктивної роботи у хмарних і гібридних мережах.

2.2.1 Налаштування маршрутизатора головного офісу

На рисунку 2.3 представлено результат виконання команди `interface print` у командному рядку RouterOS на маршрутизаторі MikroTik Main-RT. Ця команда виводить список усіх інтерфейсів, які налаштовані в системі, із зазначенням їх типу, фактичного MTU (Maximum Transmission Unit), а також MAC-адреси.

```
[admin@Main-RT] > interface/print
Flags: R - RUNNING
Columns: NAME, TYPE, ACTUAL-MTU, MAC-ADDRESS
#    NAME         TYPE       ACTUAL-MTU  MAC-ADDRESS
;;; WAN
0 R ether1       ether            1500  00:0C:29:85:7F:AD
;;; LAN
1 R ether2       ether            1500  00:0C:29:85:7F:B7
;;; DMZ
2 R ether3       ether            1500  00:0C:29:85:7F:C1
3 R lo           loopback        65536  00:00:00:00:00:00
4 R wireguard1   wg                1420
[admin@Main-RT] >
```

Рисунок 2.3 – Результат виконання команди `interface print` на маршрутизаторі MikroTik Main-RT

У системі наявні п’ять активних інтерфейсів. Три з них є фізичними Ethernet-інтерфейсами, один - віртуальний VPN-інтерфейс, і один - системний loopback-інтерфейс. Кожному інтерфейсу призначено логічне ім’я, яке відповідає певній частині мережевої архітектури, що дозволяє чітко розмежувати функції і призначення кожного з них.

Інтерфейс wireguard1 має тип wg, що означає, що це VPN-інтерфейс, створений для тунелювання трафіку за допомогою протоколу WireGuard. MTU цього інтерфейсу - 1420 байт, що нижче за стандартний Ethernet, оскільки частина простору кадру використовується для службових заголовків шифрування та тунелювання. WireGuard-інтерфейс використовується для реалізації Site-to-Site VPN-з’єднання між основним офісом і філією, що дозволяє передавати трафік між мережами через зашифрований тунель.

Усі інтерфейси мають префікс R, що означає, що вони фізично підключені, активні та готові до передавання трафіку. Це підтверджує правильне налаштування мережевої топології на маршрутизаторі та свідчить про успішне функціонування основних компонентів лабораторного середовища.

На рисунку 2.4 показано результат виконання команди `ip address print` у командному рядку MikroTik RouterOS на маршрутизаторі Main-RT. Ця команда виводить список IP-адрес, які призначені кожному інтерфейсу маршрутизатора.

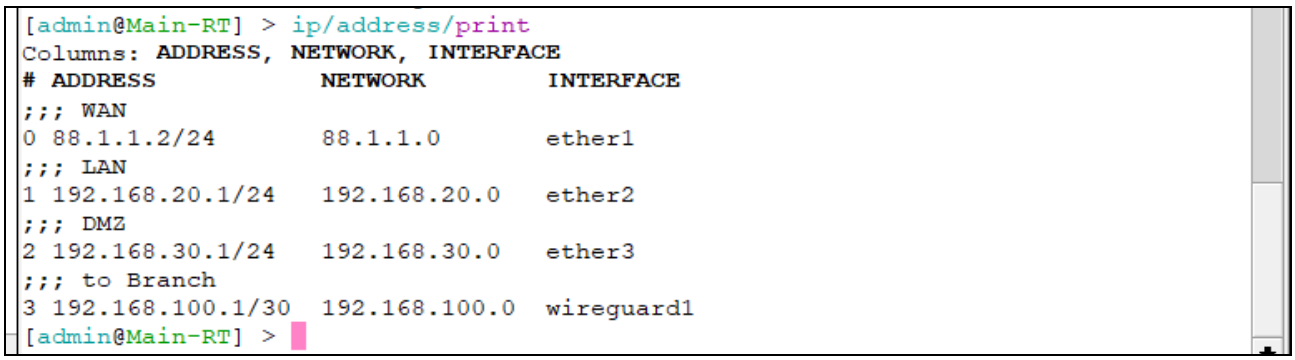

Рисунок 2.4 – Результат виконання команди `ip address print` на маршрутизаторі MikroTik Main-RT

Перший запис вказує, що інтерфейс ether1 (WAN-інтерфейс) має адресу 88.1.1.2/24, що відповідає зовнішній публічній мережі з ідентифікатором 88.1.1.0. WAN-сегмент використовують для комунікації з зовнішнім світом, включаючи встановлення VPN-з'єднань з віддаленими користувачами або іншими вузлами.

Другий запис - це інтерфейс ether2, який підключено до локальної мережі головного офісу (LAN Main Office). Йому присвоєна адреса 192.168.20.1/24, що є шлюзом для всіх пристроїв у підмережі 192.168.20.0/24. Цей інтерфейс забезпечує зв'язок між внутрішніми користувачами головного офісу та іншими сегментами, включно з DMZ і VPN-клієнтами.

Третій запис стосується інтерфейсу ether3, який підключений до DMZ-зони. Тут використовується IP-адреса 192.168.30.1/24, що є шлюзом для мережі 192.168.30.0/24. У цьому сегменті розташований сервер Windows Server 2022 з RDS, який має IP-адресу 192.168.30.2. DMZ-сегмент, як правило, ізольований від внутрішньої мережі та використовується для доступних сервісів з обмеженим контролем доступу.

Останній запис відображає VPN-інтерфейс wireguard1, призначений для тунелю WireGuard Site-to-Site. Адреса 192.168.100.1/30 належить до точки з'єднання між головним офісом і віддаленою філією. Підмережа 192.168.100.0/30 створена спеціально для тунельного з'єднання між двома

маршрутизаторами: основний офіс отримав IP 192.168.100.1, а філія — 192.168.100.2. Через цей інтерфейс здійснюється маршрутизація трафіку між підмережами головного офісу та філії у зашифрованому вигляді.

У сукупності з таблицею маршрутизації (див. рисунок 2.5), ця конфігурація свідчить про правильно реалізоване налаштування маршрутизатора MikroTik CHR у межах лабораторного середовища.

```
[admin@Main-RT] > ip/route/print
Flags: D - DYNAMIC; A - ACTIVE; c - CONNECT, s - STATIC
Columns: DST-ADDRESS, GATEWAY, DISTANCE
#      DST-ADDRESS        GATEWAY     DISTANCE
0  As  0.0.0.0/0          88.1.1.1           1
   DAc 88.1.1.0/24        ether1             0
   DAc 192.168.20.0/24    ether2             0
   DAc 192.168.30.0/24    ether3             0
1  As  192.168.40.0/24    wireguard1         1
   DAc 192.168.100.0/30   wireguard1         0
[admin@Main-RT] >
```

Рисунок 2.5 – Результат виконання команди `ip route print` на маршрутизаторі MikroTik Main-RT

Таблиця маршрутизації відображає набір правил, за якими маршрутизатор визначає шлях пересилання IP-пакетів до інших мереж. Загальна картина таблиці маршрутизації свідчить про повністю налаштовану інфраструктуру, де трафік до локальних мереж маршрутизується напряму, доступ до Інтернету здійснюється через статичний маршрут за замовчуванням, а передавання даних до філії реалізовано через захищений VPN-тунель WireGuard. Така конфігурація дозволяє реалізувати як внутрішню комунікацію, так і безпечний обмін трафіком між офісами.

На рисунку 2.6 показано налаштування DHCP-сервера на маршрутизаторі MikroTik Main-RT, який виконує автоматичну видачу IP-адрес у локальній мережі головного офісу, а також відповідні пули IP-адрес для DHCP та VPN.

```
[admin@Main-RT] > ip/dhcp-server/print
Columns: NAME, INTERFACE, ADDRESS-POOL, LEASE-TIME
# NAME                INTERFACE  ADDRESS-POOL  LEASE-TIME
0 DHCP-main-server1   ether2     DHCP-POOL     30m
[admin@Main-RT] > ip/dhcp-server/network/print
Columns: ADDRESS, GATEWAY, DNS-SERVER, DOMAIN
# ADDRESS           GATEWAY       DNS-SERVER    DOMAIN
0 192.168.20.0/24   192.168.20.1  192.168.20.1  main.kn.lan
[admin@Main-RT] > ip/pool/print
Columns: NAME, RANGES
#   NAME              RANGES
0   DHCP-POOL         192.168.20.100-192.168.20.200
1   L2TP-IPSEC-POOL   192.168.50.100-192.168.50.200
[admin@Main-RT] >
```

Рисунок 2.6 – Параметри налаштування DHCP сервера та пулів IP-адрес на маршрутизаторі MikroTik Main-RT

Пул DHCP-POOL охоплює діапазон від 192.168.20.100 до 192.168.20.200, тобто містить 101 адресу. Цей пул використовується для надання IP-адрес клієнтам локальної мережі через DHCP-сервер. Другий пул L2TP-IPSEC-POOL визначає діапазон 192.168.50.100 – 192.168.50.200. Він призначений для призначення IP-адрес користувачам, які підключаються до маршрутизатора через L2TP/IPSec Remote Access VPN. Коли віддалений користувач проходить автентифікацію і встановлює VPN-з'єднання, йому динамічно призначається адреса з цього діапазону, що дозволяє йому логічно стати частиною внутрішньої інфраструктури і отримати доступ до ресурсів мережі.

Загалом, така конфігурація забезпечує повністю автоматизовану систему розподілу адрес як для внутрішньої мережі головного офісу, так і для віддалених користувачів, які підключаються через захищений VPN-тунель. Це дозволяє спростити адміністрування, знизити кількість помилок при конфігурації та централізовано контролювати використання IP-простору [18].

На рисунку 2.7 показано вивід правил фільтрації трафіку [19] з таблиці filter в брандмауері маршрутизатора MikroTik Main-RT.

```
[admin@Main-RT] > ip/firewall/filter/print
Flags: X - disabled, I - invalid; D - dynamic
 0    ;;; accept established
      chain=input action=accept connection-state=established

 1    ;;; accept related
      chain=input action=accept connection-state=related

 2    ;;; drop invalid
      chain=input action=drop connection-state=invalid log=no log-prefix=""

 3    ;;; allow ICMP
      chain=input action=accept protocol=icmp in-interface=ether1

 4    ;;; allow Winbox
      chain=input action=accept protocol=tcp in-interface=ether1 port=8291

 5    ;;; allow SSH
      chain=input action=accept protocol=tcp in-interface=ether1 port=22

 6    ;;; allow IPSec
      chain=input action=accept protocol=udp in-interface=ether1 port=500

 7    ;;; allow IPSec
      chain=input action=accept protocol=udp in-interface=ether1 port=4500

 8    ;;; allow L2TP
      chain=input action=accept protocol=udp in-interface=ether1 port=1701

 9    ;;; allow WireGuard
      chain=input action=accept protocol=udp in-interface=ether1 port=13231

10    ;;; block everything else
      chain=input action=drop in-interface=ether1 log=no log-prefix=""
[admin@Main-RT] >
```

Рисунок 2.7 – Правила фільтрації трафіку з таблиці filter в брандмауері маршрутизатора MikroTik Main-RT

Перші три правила забезпечують базову обробку з'єднань за станом. Перше правило дозволяє трафік, який є частиною вже встановлених з'єднань (стан established). Це необхідно для збереження зворотного трафіку, наприклад, у відповідь на запити зсередини мережі. Друге правило дозволяє пов’язані з’єднання (related), наприклад, динамічно відкриті порти для FTP або VoIP. Третє правило блокує всі з’єднання зі станом invalid, тобто некоректні або пошкоджені пакети, які не відповідають жодному відомому сеансу. Це типова практика для захисту від некоректного або потенційно шкідливого трафіку.

Четверте правило дозволяє ICMP-пакети, зокрема ping, які часто використовуються для перевірки доступності хоста. Правило обмежене інтерфейсом ether1, тобто WAN, що дає змогу здійснювати діагностику ззовні,

якщо це потрібно. П'яте правило дозволяє підключення до Winbox (порт 8291 tcp) - фірмової утиліти для керування MikroTik, шосте - SSH (порт 22 tcp), що дозволяє керування через CLI. Обидва ці сервіси дозволені на вхід через інтерфейс ether1.

Наступні три правила дозволяють використання портів, необхідних для VPN-протоколів. Сьоме та восьме правила відповідають за IPsec - порти 500 udp (IKE) і 4500 (NAT-T), дев’яте правило дозволяє L2TP-протокол (порт 1701 udp). Таким чином, вони забезпечують можливість встановлення L2TP/IPSec Remote Access VPN. Десяте правило відкриває порт 13231 udp, який використовується для WireGuard, що застосовується в Site-to-Site VPN з’єднанні.

Останнє правило є загальним правилом блокування всього іншого трафіку на вхід через інтерфейс ether1. Усі пакети, які не відповідають попереднім умовам, будуть відкинуті без логування. Це правило завершує політику «дозволити явно, заборонити все інше» і є основою захисту від несанкціонованого доступу ззовні. Така політика є важливою для мінімізації площини атаки на маршрутизатор.

На рисунку 2.8 показано конфігурацію правил у таблиці nat брандмауера [20] маршрутизатора MikroTik Main-RT, отриману за допомогою команди `ip firewall nat print`.

```
[admin@Main-RT] > ip/firewall/nat/print
Flags: X - disabled, I - invalid; D - dynamic
 0    chain=srcnat action=masquerade src-address=192.168.20.0/24
      out-interface=ether1 log=no log-prefix=""

 1    chain=srcnat action=masquerade src-address=192.168.30.0/24
      out-interface=ether1 log=no log-prefix=""

 2    chain=srcnat action=masquerade src-address=192.168.50.0/24
      out-interface=ether1 log=no log-prefix=""
[admin@Main-RT] >
```

Рисунок 2.8 – Правила nat в брандмауері маршрутизатора MikroTik Main-RT

Ці правила використовуються для трансляції адрес джерела (Source NAT) і виконання маскараду - автоматичної підстановки зовнішньої IP-адреси

маршрутизатора замість локальної адреси клієнта при виході в Інтернет. Такий підхід дає змогу пристроям із приватними IP-адресами передавати дані у глобальну мережу, використовуючи публічну IP-адресу маршрутизатора [21].

У наведеному прикладі присутні три правила, які відповідають за NAT для різних локальних підмереж. Усі вони виконують дію masquerade, тобто автоматично підставляють IP-адресу інтерфейсу, через який здійснюється вихід у зовнішню мережу (в даному випадку - ether1, який має публічну адресу 88.1.1.2). Перше правило стосується підмережі 192.168.20.0/24, яка відповідає за локальну мережу головного офісу (LAN). Друге правило для підмережі 192.168.30.0/24, яка належить до DMZ-зони, де розташований сервер Windows Server 2022 з RDS. Третє правило обслуговує підмережу 192.168.50.0/24, яка використовується для VPN Remote Access (L2TP/IPSec).

На рисунку 2/9 показано детальну конфігурацію інтерфейсу WireGuard [22] на маршрутизаторі MikroTik Main-RT, включаючи налаштування самого інтерфейсу (interface wireguard) та параметри peer-з'єднань (interface wireguard peers), яке реалізує VPN-зв'язок Site-to-Site між головним офісом і філією.

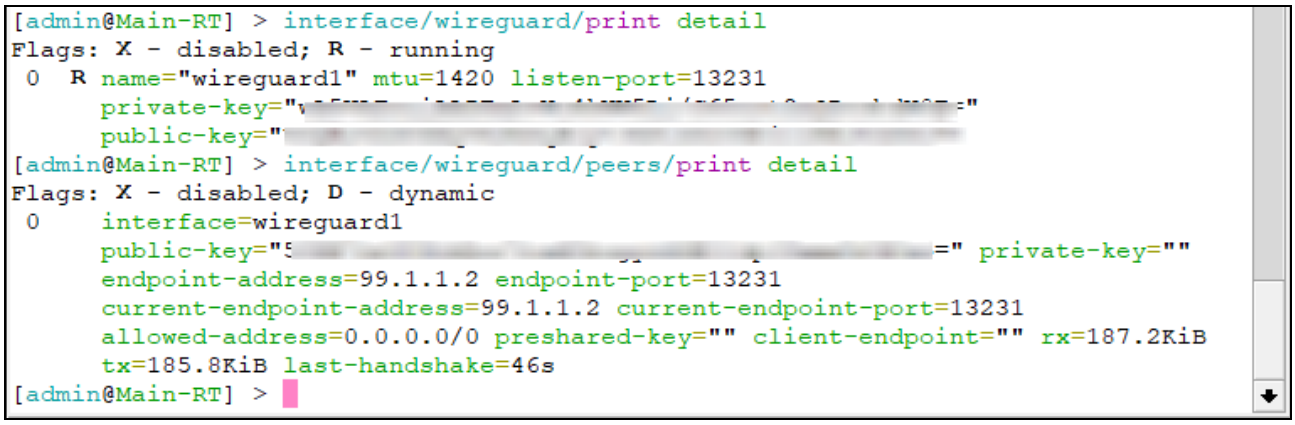

Рисунок 2.9 – Детальна конфігурація інтерфейсу WireGuard на маршрутизаторі MikroTik Main-RT

У першій частині виводу видно, що інтерфейс має назву wireguard1, він активний, має MTU 1420 байт і слухає порт 13231 для вхідних UDP-з'єднань. Це означає, що інтерфейс відкритий до прийому тунельного трафіку з боку

іншого вузла (філії) і здатний встановлювати VPN-з'єднання. Також присутні записи private-key та public-key, які ідентифікують цей вузол у криптографічному обміні. У другій частині вказані параметри VPN peer, з яким встановлено з'єднання. Вказано його public-key, що використовується для аутентифікації віддаленого вузла. Поле endpoint-address вказує на реальну IP-адресу філії, а endpoint-port - на udp-порт.

Представлена конфігурація демонструє правильно налаштовану Site-to-Site VPN інфраструктуру між головним офісом і філією за допомогою WireGuard, з повноцінною аутентифікацією, обміном ключами, тунельним маршрутом і активною передачею даних [23]. Це рішення забезпечує шифрування, високу продуктивність і сучасний рівень безпеки при мінімальній складності конфігурації.

На рисунку 2.10 показано детальний вивід команди `ppp profile print`, яка використовується в MikroTik RouterOS для перегляду налаштувань профілів PPP (Point-to-Point Protocol). У контексті конфігурації L2TP/IPSec Remote Access VPN, ці профілі визначають параметри IP-адресації, шифрування та поведінки VPN-клієнтів під час підключення до маршрутизатора Main-RT.

```
[admin@Main-RT] > ppp/profile/print detail
Flags: * - default
 0 * name="default" bridge-learning=default use-ipv6=yes use-mpls=default
     use-compression=default use-encryption=default only-one=default
     change-tcp-mss=yes use-upnp=default address-list="" on-up="" on-down=""

 1   name="VPN_PROFILE" local-address=192.168.50.1 remote-address=L2TP-IPSEC-POOL
     bridge-learning=default use-ipv6=yes use-mpls=default
     use-compression=default use-encryption=default only-one=default
     change-tcp-mss=default use-upnp=default address-list="" on-up=""
     on-down=""

 2 * name="default-encryption" bridge-learning=default use-ipv6=yes
     use-mpls=default use-compression=default use-encryption=yes
     only-one=default change-tcp-mss=yes use-upnp=default address-list=""
     on-up="" on-down=""
[admin@Main-RT] >
```

Рисунок 2.10 – Детальний вивід команди `ppp profile print` на маршрутизаторі MikroTik Main-RT

Присутність профілю VPN_PROFILE дозволяє централізовано керувати параметрами з'єднання для всіх VPN-користувачів, які підключаються через L2TP. Це дає змогу легко масштабувати систему, призначати динамічні адреси, контролювати політику. Він забезпечує правильний розподіл адрес і дозволяє користувачам, які підключаються ззовні (наприклад, із домашньої мережі), ставати частиною логічного внутрішнього сегменту - 192.168.50.0/24 зі шлюзом 192.168.50.1. У поєднанні з IPsec-тунелем, це гарантує захищений доступ до ресурсів головного офісу.

На рисунку 2.11 наведено конфігурацію L2TP-сервера на маршрутизаторі MikroTik Main-RT, отриману за допомогою команди `interface l2tp-server server print`.

```
[admin@Main-RT] > interface/l2tp-server/server/print
                  enabled: yes
                  max-mtu: 1450
                  max-mru: 1450
                     mrru: disabled
           authentication: mschap2
       keepalive-timeout: 30
             max-sessions: unlimited
          default-profile: VPN_PROFILE
                use-ipsec: yes
              ipsec-secret: [redacted]
           caller-id-type: ip-address
    one-session-per-host: no
          allow-fast-path: no
       l2tpv3-circuit-id:
    l2tpv3-cookie-length: 0
      l2tpv3-digest-hash: md5
  accept-pseudowire-type: all
    accept-proto-version: all
[admin@Main-RT] >
```

Рисунок 2.11 – Вивід команди `interface l2tp-server server print` на маршрутизаторі MikroTik Main-RT

Аутентифікація здійснюється методом MS-CHAPv2, який є поширеним і підтримується більшістю операційних систем. Це забезпечує безпечний обмін обліковими даними користувачів VPN під час підключення. Ключовим елементом є VPN_PROFILE, який визначає IP-адресацію клієнтів та шлюз

VPN-сервера. Цей профіль, як показано раніше, призначає віддаленим користувачам адреси з пулу 192.168.50.100–200.

Параметр `use-ipsec: yes` активує шифрування тунелю, тобто весь L2TP-трафік додатково захищений за допомогою IPsec. У полі ipsec-secret встановлено попередньо узгоджений ключ (pre-shared key), який є обов'язковим елементом автентифікації на етапі встановлення тунелю. Це забезпечує надійний захист від спроб підключення неавторизованих клієнтів.

На рисунку 2.13 показано результат виконання команди `ip ipsec proposal print detail` на маршрутизаторі MikroTik Main-RT, яка відображає налаштування IPsec пропозиції (proposal) - тобто параметри криптографії, які будуть запропоновані при встановленні VPN-тунелю з використанням протоколу IPsec.

```
[admin@Main-RT] > ip/ipsec/proposal/print detail
Flags: X - disabled; * - default
 0  * name="default" auth-algorithms=sha256,sha1 enc-algorithms=aes-256-cbc
      lifetime=30m pfs-group=modp2048
[admin@Main-RT] >
```

Рисунок 2.12 – Вивід команди `ip ipsec proposal print detail` на маршрутизаторі MikroTik Main-RT

У параметрі `auth-algorithms=sha256,sha1` вказано два хеш-алгоритми, які відповідають за перевірку автентичності даних [24]. Першим у списку стоїть SHA-256, який є сильнішим і сучаснішим варіантом, і саме він буде пріоритетним при узгодженні параметрів тунелю. SHA-1 вказано як резервний варіант, який підтримується для сумісності зі старими клієнтами або системами. Поле `enc-algorithms=aes-256-cbc` визначає алгоритм шифрування - в даному випадку використовується AES із довжиною ключа 256 біт у режимі CBC [25]. Це дуже надійна комбінація, яка забезпечує високий рівень захисту для VPN-трафіку і відповідає сучасним стандартам криптографічної стійкості. Параметр `lifetime=30m` вказує, що криптографічний ключ, сформований у рамках даної сесії, діє протягом 30

хвилин, після чого має бути оновлений. Це дозволяє регулярно оновлювати ключі, знижуючи ризик їхнього компрометування.

Значення `pfs-group=modp2048` означає використання групи Perfect Forward Secrecy з використанням 2048-бітного ключа. Це забезпечує додатковий рівень захисту шляхом незалежної генерації ключів шифрування для кожної сесії. У разі, якщо один із ключів буде скомпрометований, інші сесії залишаться захищеними. Modp2048 (Modular Exponentiation Group 2048-bit) - це одна з груп для алгоритму обміну ключами Diffie-Hellman (DH) [26], що використовується в протоколах IPsec для захищеного узгодження криптографічних ключів між двома сторонами VPN-з'єднання. Основна ідея полягає в тому, щоб дві сторони могли узгодити спільний секретний ключ, не передаючи його напряму через мережу. Для цього використовується обчислення на основі модульної арифметики - так званий обмін Диффі-Гелмана. Група modp2048 означає, що для обчислень використовується просте число довжиною 2048 біт і відповідний первісний корінь (генератор), які зафіксовані в стандарті RFC 3526 (Group 14) [27]. Група modp2048 відповідає так званому груповому рівню безпеки 112–128 біт, що є визнаним порогом сучасної криптостійкості для захищених каналів комунікації. Це означає, що зламати згенерований ключ методом перебору або криптоаналізу за допомогою сучасних обчислювальних засобів є надзвичайно складно. Обчислювально це еквівалентно зламу AES-128.

Застосування групи modp2048 у конфігурації IPsec має кілька важливих переваг. Вона підтримується більшістю сучасних операційних систем та мережевих пристроїв (Windows, Linux, Android, MikroTik, Cisco, pfSense тощо), що забезпечує високу сумісність при побудові VPN-тунелів. Вона дозволяє реалізувати Perfect Forward Secrecy (PFS) - властивість криптографічної системи, за якої компрометація одного сесійного ключа не дозволяє розшифрувати трафік з інших сесій, оскільки ключі щоразу генеруються заново [28]. Водночас modp2048 вимагає більше обчислювальних ресурсів, ніж

коротші групи (наприклад modp1024), однак сучасні процесори без проблем обробляють це навантаження.

На рисунку 2.13 представлено вивід команди `ppp secret print`, яка показує список користувачів PPP-сервісів, у тому числі користувачів L2TP/IPSec Remote Access VPN на маршрутизаторі MikroTik Main-RT.

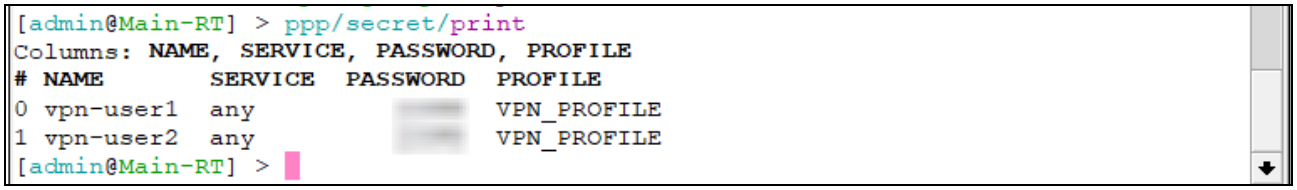

Рисунок 2.13 – Вивід команди `ppp secret print` на маршрутизаторі MikroTik Main-RT

Ці облікові записи використовуються для автентифікації клієнтів при підключенні до VPN.

Повний файл конфігурації маршрутизаторі MikroTik Main-RT наведено в додатку А.

2.2.2 Налаштування маршрутизатора філії

Конфігурація маршрутизатора філії MikroTik Branch-RT формує повноцінний вузол мережі, який одночасно обслуговує локальний сегмент 192.168.40.0/24, надає абонентам доступ до Інтернету через статичне WAN-підключення 99.1.1.2/24 і підтримує захищений тунель WireGuard до головного офісу. Повний файл конфігурації маршрутизаторі MikroTik Branch-RT наведено в додатку Б.

У блоці interface ethernet перший порт ether1 позначено як WAN, другий порт ether2 використовуються для внутрішньої мережі LAN. Інтерфейс wireguard1 із MTU 1420 та udp портом 13231 використовується для обміни трафіком між філією й центральним маршрутизатором. Інтерфейс ether1 має IP-адресу 99.1.1.2/24, ether2 - 192.168.40.1/24, а wireguard1 - 192.168.100.2/30. Для

локальних клієнтів налаштовано DHCP-сервіс: пул DHCP-POOL охоплює діапазон 192.168.40.100–200, сервер DHCP-branch-server1 прив’язано до ether2, а в параметрах мережі клієнтам автоматично роздаються шлюз 192.168.40.1, внутрішній DNS. Запит до зовнішніх DNS маршрутизатор переадресовує на 99.1.1.1 і резервний 8.8.8.8, дозволяючи одночасно локальний рекурсивний режим (allow-remote-requests=yes). Секція interface wireguard peers описує VPN Site-to-Site. Віддалений вузол має IP-адресу 88.1.1.2 та udp порт 13231. Змінну allowed-address виставлено 0.0.0.0/0, що спрощує маршрутизацію будь-яких підмереж через тунель. Статичні маршрути у розділі ip route спрямовують три внутрішні підмережі головного офісу - 192.168.20.0/24 (LAN), 192.168.30.0/24 (DMZ) та 192.168.50.0/24 (пул L2TP-клієнтів) через інтерфейс wireguard1, тоді як шлях за замовчуванням 0.0.0.0/0 вказує на зовнішній шлюз 99.1.1.1. Отже, локальні станції мають прозорий доступ і до ресурсів центрального офісу, і до зовнішнього Інтернету.

Брандмауер у ланцюгу input реалізує класичну модель «дозволити необхідне - заборонити решту». Перші два правила пропускають established і related з’єднання, третє відсікає invalid трафік, далі вибірково відкрито icmp для діагностики, tcp 8291 для Winbox, tcp 22 для SSH адміністрування та udp 13231 для WireGuard. Завершальне правило блокує будь-який інший вхідний трафік на WAN. У ланцюгу srcnat єдине правило виконує NAT усіх пакетів з підмережі 192.168.40.0/24, що прямують у зовнішній інтерфейс ether1, підмінюючи їх IP-адресою 99.1.1.2 та забезпечуючи NAT-доступ до Інтернету.

Конфігурація забезпечує DHCP та DNS сервіси у філії та захищений канал WireGuard до головного офісу з повним обміном внутрішніми підмережами, а також мінімально необхідний перелік відкритих сервісів для керування й діагностики.

2.2.3 Налаштування домашнього маршрутизатора

Конфігурація маршрутизатора MikroTik Home-RT представляю собою типову схему домашньої мережі з єдиним зовнішнім підключенням і внутрішнім сегментом 172.16.1.0/24. Повний файл конфігурації маршрутизаторі MikroTik Home -RT наведено в додатку В.

Перший фізичний порт ether1 позначено як WAN і йому призначено статичну публічну IP-адресу 77.1.1.2/24. Другий порт ether2 слугує локальним інтерфейсом LAN з IP-адресою 172.16.1.1/24. Для динамічного розподілу IP-адрес в середині мережі створено пул DHCP-POOL із діапазоном 172.16.1.100–172.16.1.200. Сервер DHCP-home-server1 прив'язано безпосередньо до ether2 і налаштовано роздавати клієнтам не лише саму адресу, а й параметри DNS та шлюзу 172.16.1.1.

Модуль брандмауера у ланцюгу input реалізує базову політику безпеки. Спочатку пропускається трафік зі станом established і related, потім відкидаються пакети, що RouterOS класифікує як invalid. Із допустимих сервісів на WAN відкрито ICMP для діагностики, tcp порт 8291 для Winbox і tcp 22 для SSH-керування; усі інші запити ззовні одразу блокуються останнім правилом, тим самим мінімізуючи поверхню атаки. У ланцюгу srcnat єдина дія – здіснити NAT усього вихідного трафіку з приватної мережі 172.16.1.0/24 через зовнішній інтерфейс ether1, тобто внутрішні IP-адреси підмінюються IP-адресою 77.1.1.2, що гарантує коректний доступ до Інтернету. Таблиця маршрутів містить лише один статичний маршрут за замовчуванням на шлюз провайдера 77.1.1.1.

У такому налаштуванні маршрутизатор забезпечує стабільне підключення з централізованим DHCP, кешованим DNS, захищеним NAT-шлюзом і мінімальним набором відкритих сервісів для віддаленого адміністрування.

2.2.4 Налаштування Windows Server 2022 RDS

Windows Server 2022 - це серверна операційна система від Microsoft, що прийшла на зміну Windows Server 2019 і фокусується на безпеці ядра, тісній інтеграції з хмарними службами Azure та розвитку сучасних робочих навантажень, передусім контейнеризації і віртуалізації [29]. Система доступна в редакціях Standard, Datacenter і Datacenter Azure Edition; перші дві призначені для локальних або гібридних цодів, тоді як Azure Edition оптимізовано під розгортання у хмарній інфраструктурі. Усі редакції пропонуються як із класичним графічним середовищем Desktop Experience, так і в мінімальному варіанті Server Core, що зменшує поверхню атаки та навантаження на ресурси.

Remote Desktop Services у Windows Server 2022 залишаються центральною платфомою Microsoft для публікації робочих столів [30], окремих програм і графічних середовищ у мережі, але зосереджуються на підвищеній безпеці ядра, покращеній підтримці графіки та тіснішій інтеграції з Azure Virtual Desktop. Базова архітектура не змінилася. Роль RDS, як і раніше, складається з компонентів RD Session Host, RD Connection Broker, RD Gateway, RD Licensing, RD Web Access і RD Virtualization Host для VDI-ферм.

На рисунку 2.14 показано вікно Server Manager в операційній системі Windows Server 2022 Standard, вкладка Local Server, яка надає загальну інформацію про конфігурацію та стан локального сервера, що виконує роль RDS.

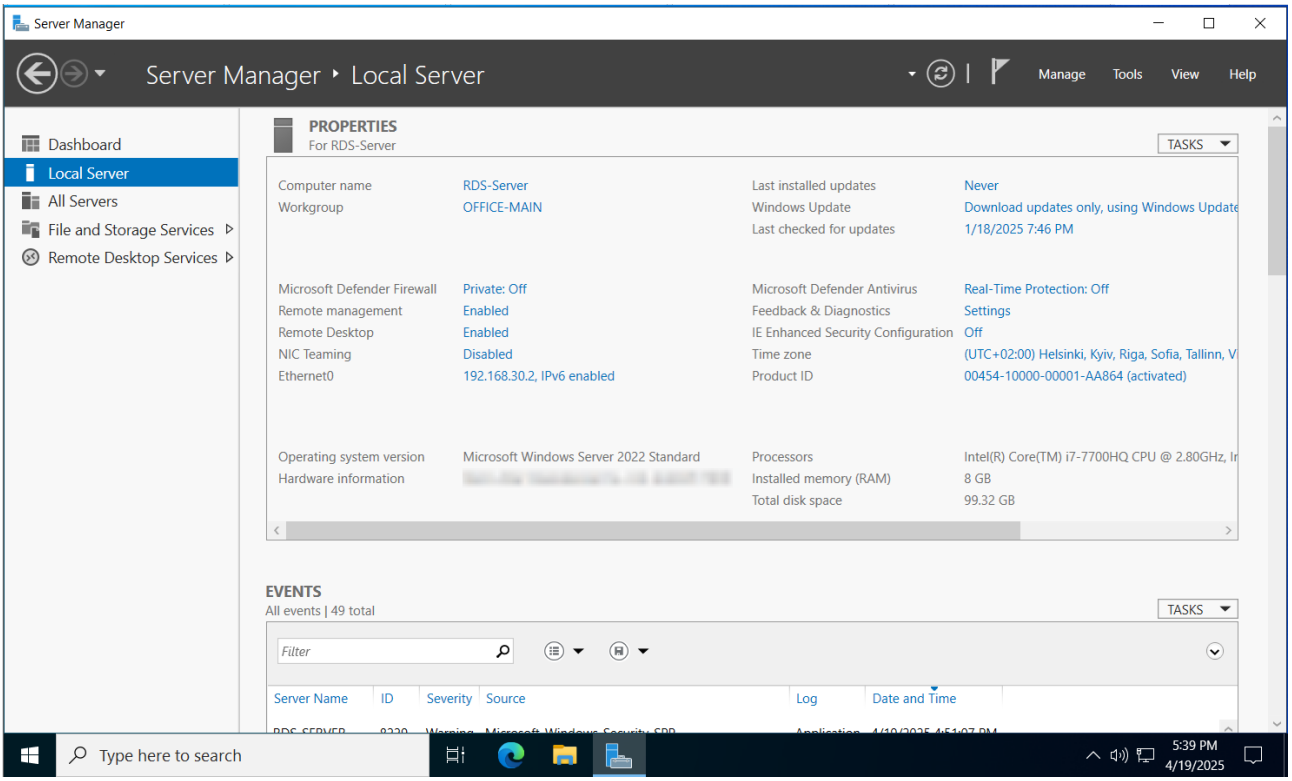

Рисунок 2.14 – Вікно Server Manager в операційній системі Windows Server 2022 Standard

Сервер має активовану функцію `Remote Desktop (Enabled)`, що дозволяє користувачам підключатися до цього вузла віддалено по RDP-протоколу. Також активовано Remote management, тобто керування сервером може здійснюватися з інших систем через Windows Admin Center, PowerShell або Server Manager. У полі мережевого інтерфейсу Ethernet0 призначену IP-адресу 192.168.30.2, що вказує на розміщення сервера в DMZ сегменті головного офісу.

На рисунку 2.15 представлено результат виконання PowerShell-команди `Get-WindowsFeature -Name RDS* | Where-Object Installed`.

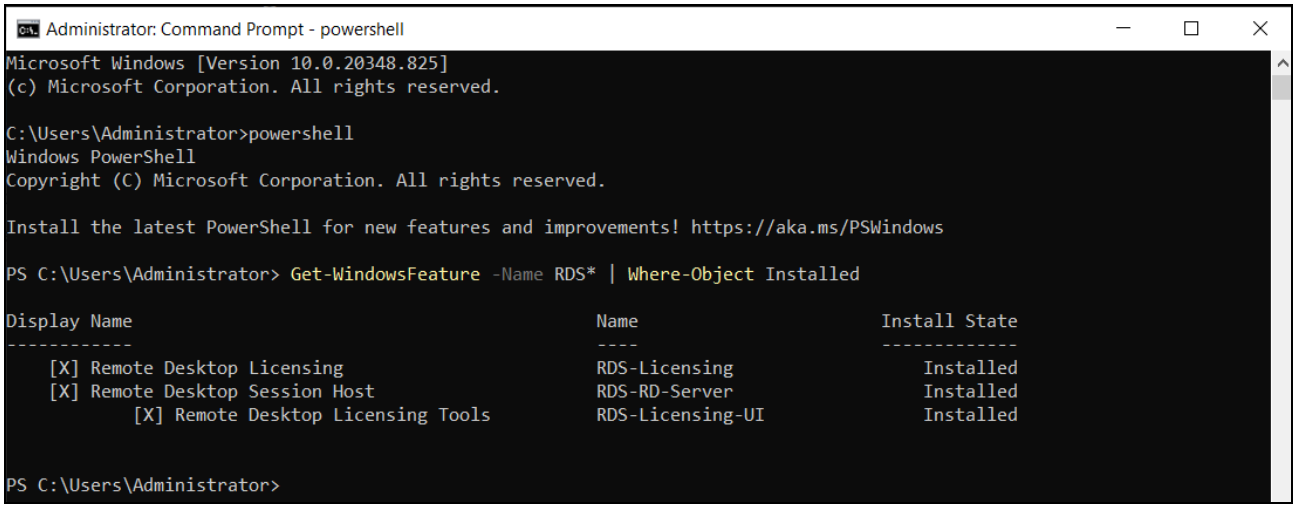

Рисунок 2.15 – Результат виконання команди `Get-WindowsFeature -Name RDS* | Where-Object Installed` в Windows Server 2022

Ця команда виводить список встановлених ролей і компонентів, пов’язаних із RDS на сервері під управлінням Windows Server. Усі ролі мають статус Installed, що свідчить про те, що сервер повністю готовий для роботи як вузол термінального доступу (RDS Session Host) із можливістю ліцензування користувачів і пристроїв. Це дозволяє адміністратору централізовано керувати виданими ліцензіями, забезпечити легітимне використання сервісу та надавати віддалений доступ до робочих столів для співробітників організації. Така конфігурація є типовою для невеликих або лабораторних розгортань RDS, де одна система одночасно виконує роль як сеансного хоста, так і ліцензійного сервера. Це спрощує адміністрування і дозволяє швидко впровадити віддалений робочий стіл для тестування або малого підприємства.

На рисунку 2.16 представлено результат виконання PowerShell-команди `Get-LocalUser -Name "dmytro_kudryk" | Select-Object -Property *`.

Рисунок 2.16 – Результат виконання команди `Get-LocalUser -Name "dmytro_kudryk" | Select-Object -Property *` в Windows Server 2022

Ця команда надає повну інформацію про локального користувача з ім’ям dmytro_kudryk у системі Windows Server 2022. Обліковий запис є активним і використовується для підключення до віддалених сесій у середовищі RDS (див.рисунок 2.17).

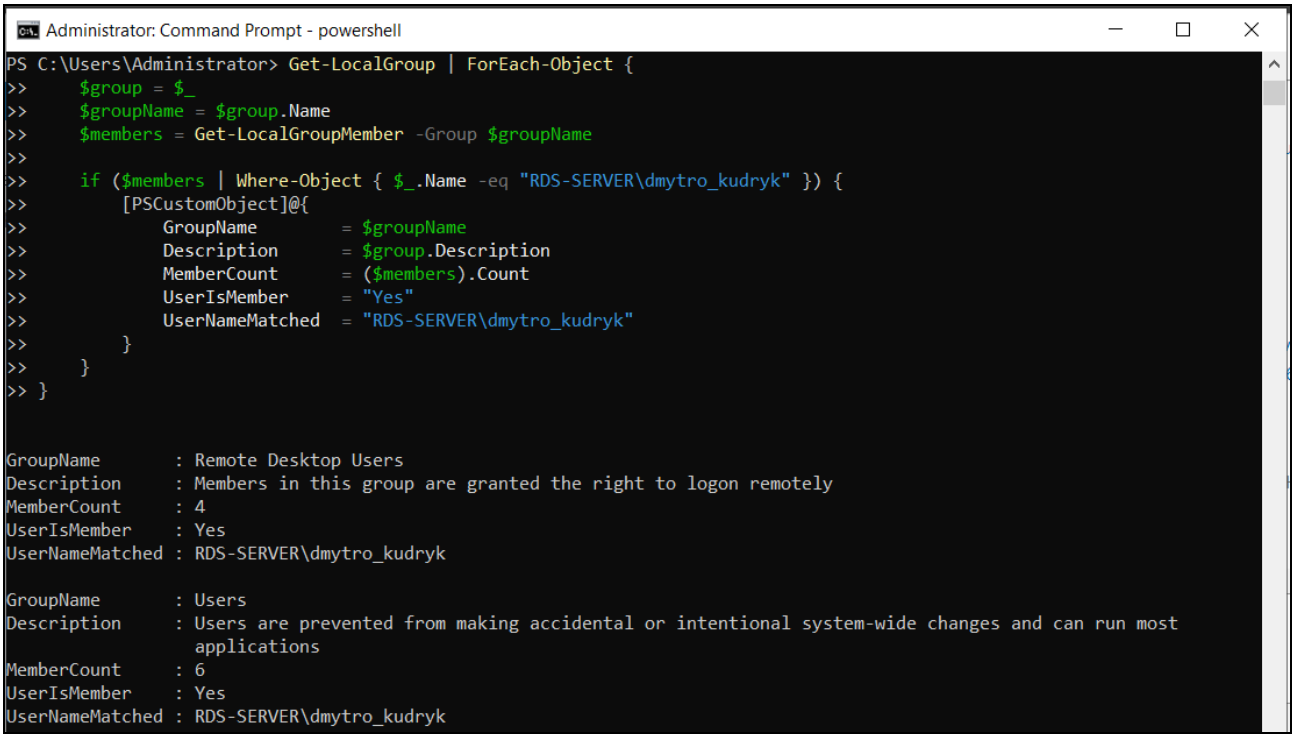

Рисунок 2.17 – Результат виконання команди PowerShell скрипта в Windows Server 2022

На рисунку 2.17 показано результат виконання PowerShell-скрипта, який перебирає всі локальні групи на сервері та перевіряє, чи входить локальний користувач RDS-SERVER\dmytro_kudryk до їхнього складу. Виведено інформацію по тих групах, де цей користувач є членом, із зазначенням назви групи, опису, кількості учасників та підтвердженням, що користувач справді знайдений. Перша група Remote Desktop Users надає право на віддалений вхід до системи за допомогою протоколу RDP.

2.3 Висновок до другого розділу

У другому розділі було розглянуто реалізацію VPN мережі на основі програмно-визначених маршрутизаторів MikroTik у віртуальному лабораторному середовищі. Детально описано побудову інфраструктури з трьома сегментами - головним офісом, віддаленою філією та віддаленим користувачам, які з’єднуються між собою за допомогою двох типів VPN: L2TP/IPSec Remote Access VPN для безпечного підключення індивідуальних користувачів і WireGuard Site-to-Site VPN для створення постійного захищеного каналу між офісами. У якості VPN-сервера обрано MikroTik CHR, розгорнутий у середовищі VMware Workstation Pro, що дозволило ефективно змоделювати всі компоненти корпоративної інфраструктури без потреби у фізичному обладнанні. Описано покрокове налаштування інтерфейсів, IP-адресації, маршрутів, пулів адрес, правил брандмауера та NAT, а також реалізацію VPN-тунелів з урахуванням криптографічних параметрів і механізмів безпеки. Було встановлено та налаштовано сервер Windows Server 2022, який виступає RDS-хостом. Це дозволяє перевірити реальну функціональність тунелювання VPN з подальшим RDP-підключенням до сервера.

Усі представлені конфігурації підтверджують працездатність запропонованої інфраструктури, її здатність забезпечувати конфіденційність, цілісність та захищений доступ до внутрішніх ресурсів незалежно від фізичного розташування користувачів чи офісів.

РОЗДІЛ 3. ПРАКТИЧНЕ ТЕСТУВАННЯ VPN МЕРЕЖІ

3.1 Тестування Remote Access VPN

3.1.1 Операційна система Windows

Тестування Remote Access VPN з операційної системи Windows 10 має на меті перевірити працездатність конфігурації L2TP/IPSec Remote Access VPN, реалізованої на маршрутизаторі MikroTik Main-RT. В якості клієнта виступає ПК з Windows 10, розміщений у сегменті домашньої мережі Home LAN з адресним простором 172.16.1.0/24. Пристрій отримує IP-адресу динамічно через DHCP-сервер, розгорнутий на маршрутизаторі Home-RT, а доступ до Інтернету здійснювався через шлюз з IP-адресою 77.1.1.1 (див. рисунок 3.1).

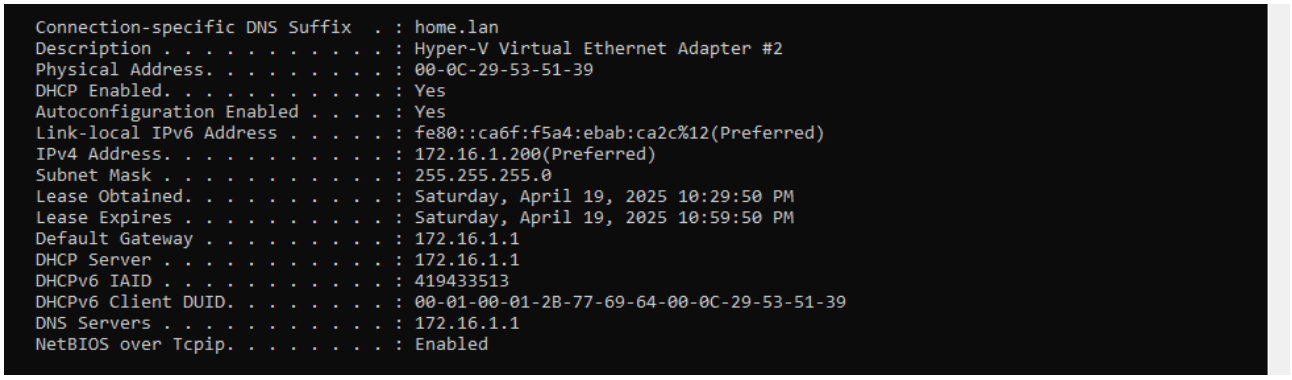

Рисунок 3.1 – Результат виконання команди `ipconfig /all` в операційній системі Windows 10

Наявність цих параметрів свідчить про правильне налаштування Windows 10, стабільне функціонування DHCP-інфраструктури та готовність пристрою до встановлення віддаленого VPN-з'єднання. Адреса 172.16.1.200 є останньою в пулі, що також підтверджує ефективну видачу IP із діапазону, налаштованого на маршрутизаторі Home-RT. Це є підготовчим етапом перед підключенням до L2TP/IPSec VPN сервера, де після успішної аутентифікації клієнт отримає іншу

IP-адресу вже з внутрішнього пулу 192.168.50.0/24, що стане ознакою логічного включення до мережі головного офісу.

На стороні клієнта VPN-підключення здійснювалося штатними засобами Windows 10 (див. рисунок 3.2).

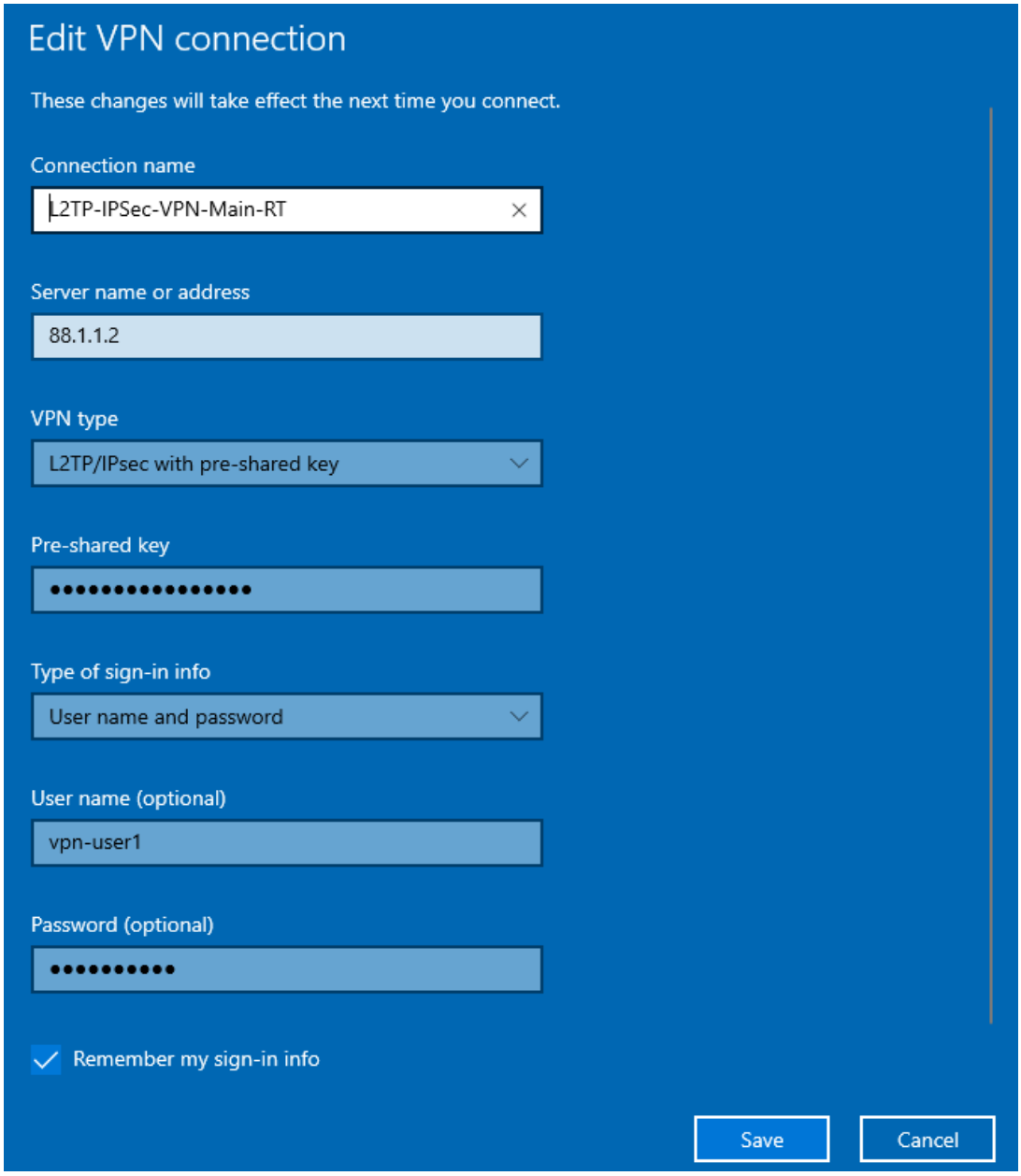

Рисунок 3.2 – Налаштування L2TP/IPSec VPN в операційній системі Windows 10

Після збереження конфігурації й ініціалізації підключення, клієнт Windows 10 встановлює тунель до маршрутизатора MikroTik Main-RT (див. рисунок 3.3).

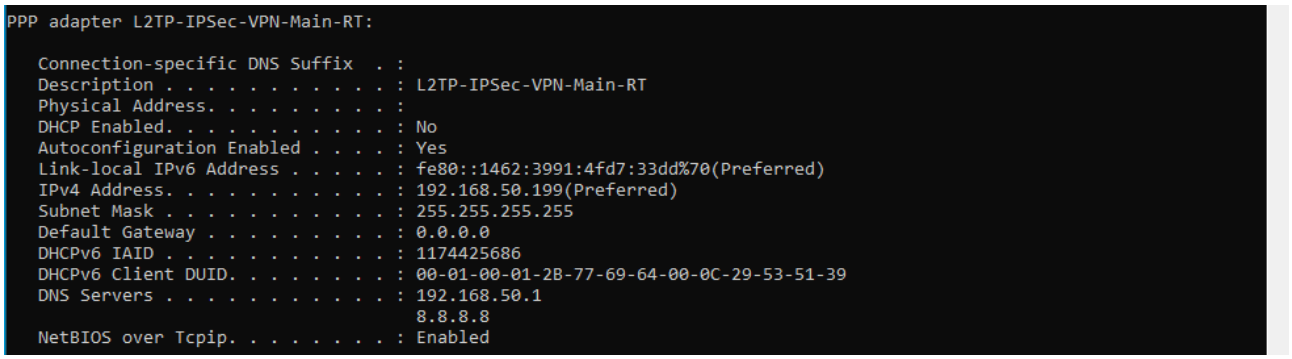

Рисунок 3.3 Результат виконання команди `ipconfig /all` в операційній системі Windows 10 після встановлення VPN-з’єднання

Після встановлення VPN-з'єднання було проведено перевірку доступності сервера Windows Server 2022 RDS у локальній мережі головного офісу (див. рисунок 3.4).

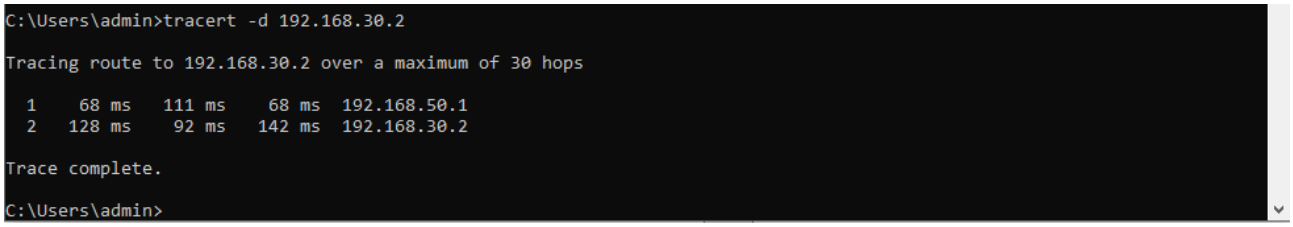

Рисунок 3.3 – Результат виконання результат виконання команди `tracert -d 192.168.30.2` на Windows 10

Факт завершення трасування з успішним результатом означає, що клієнт має доступ до сервера RDS через VPN-тунель, і вся мережна інфраструктура, включаючи маршрутизацію, тунелювання, NAT і міжмережеві екрани, налаштована правильно. Це також підтверджує, що клієнт отримав дійсну IP-адресу з пулу VPN, сервер відповідає, а трафік в обох напрямках проходить без обмежень або блокувань.

На рисунку 3.4 представлено активну сесію віддаленого підключення за допомогою RDP до сервера з IP-адресою 192.168.30.2, що розташований у DMZ-сегменті головного офісу.

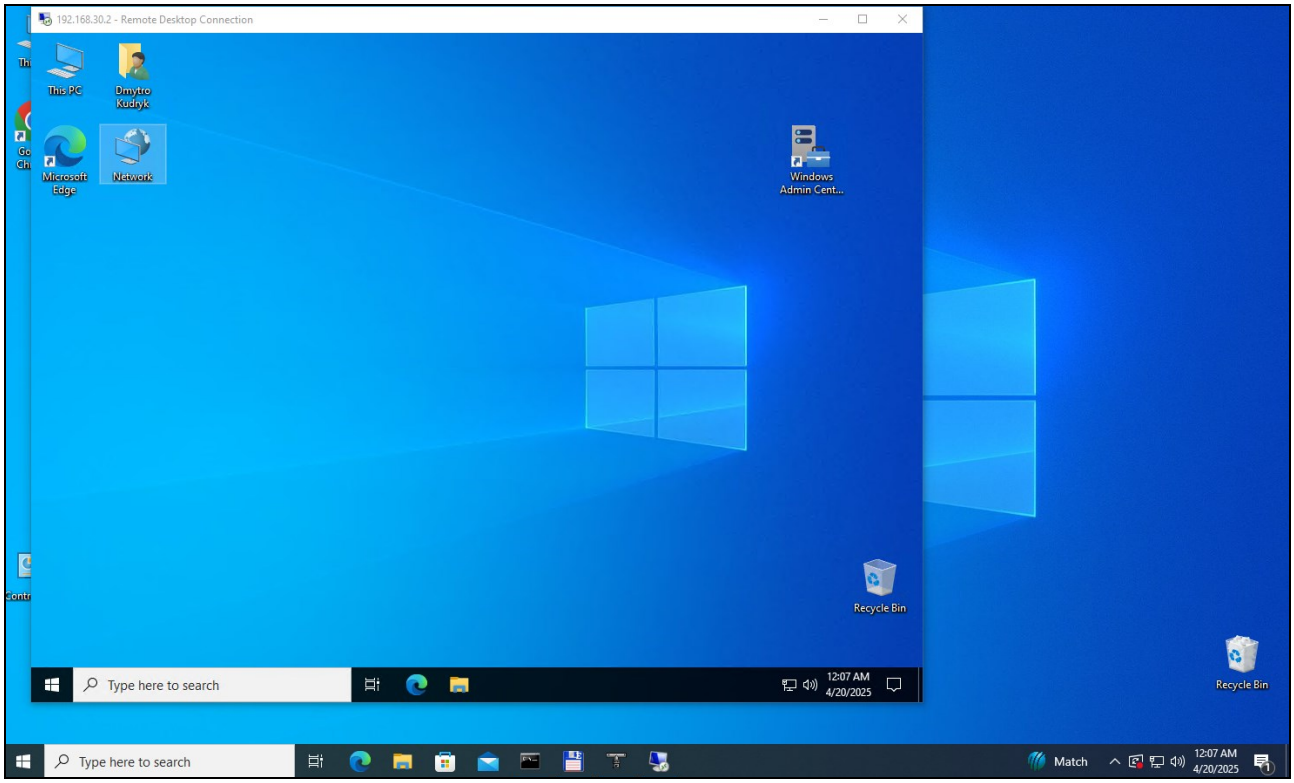

Рисунок 3.4 – Успішне підключення до Windows Server 2022 RDS

Підключення здійснене з клієнтського комп’ютера під керуванням Windows 10, який попередньо встановив L2TP/IPSec VPN-з’єднання з маршрутизатором MikroTik Main-RT. Факт успішного запуску сеансу RDP підтверджує, що тунель VPN працює стабільно, маршрутизація налаштована коректно, а брандмауер на сервері й маршрутизаторі дозволяє вхідні з’єднання по tcp-порту 3389.

Таким чином, тестування доступу до внутрішніх сервісів головного офісу через L2TP/IPSec Remote Access VPN з Windows 10 завершилося успішно. Це доводить повну функціональність лабораторного середовища, зокрема можливість безпечного, зашифрованого підключення до корпоративних ресурсів із віддаленого розташування.

3.1.2 VPN L2TP/IPSec сервер MikroTik

На рисунку 3.5 показано результат виконання команди `ppp active print detail` на маршрутизаторі MikroTik Main-RT, яка виводить детальну інформацію про активні PPP-з'єднання, зокрема L2TP/IPSec VPN підключення.

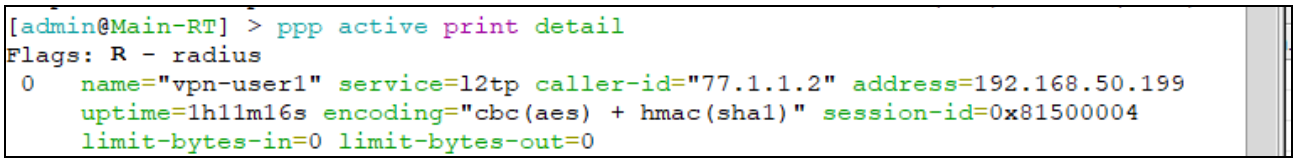

Рисунок 3.5 – Результат виконання команди `ppp active print detail` на маршрутизаторі MikroTik Main-RT

В даному випадку активне VPN-з’єднання встановлене користувачем vpn-user1, який підключився до сервісу l2tp. Значення `caller-id="77.1.1.2"` вказує на публічну IP-адресу клієнта - це домашній маршрутизатор (Home-RT), через який здійснюється тунелювання. Користувачеві призначено внутрішню IP-адресу 192.168.50.199 з пулу L2TP-IPSEC-POOL, що свідчить про логічне включення клієнта до внутрішньої мережі головного офісу.

Поле `encoding="cbc(aes) + hmac(sha1)"` описує використовувані криптографічні алгоритми: AES у режимі CBC для шифрування трафіку та HMAC з SHA-1 для перевірки цілісності даних. Така комбінація є типовою для L2TP/IPSec тунелів і забезпечує належний рівень безпеки при збереженні сумісності з клієнтськими ОС.

На рисунку 3.6 показано результат виконання команди `ip address print detail` на маршрутизаторі MikroTik Main-RT, яка надає повну інформацію про призначення IP-адрес кожному інтерфейсу пристрою, включно з динамічно створеними тунелями.

```
[admin@Main-RT] > ip address print detail
Flags: X - disabled, I - invalid, D - dynamic
 0    ;;; WAN
      address=88.1.1.2/24 network=88.1.1.0 interface=ether1
      actual-interface=ether1

 1    ;;; LAN
      address=192.168.20.1/24 network=192.168.20.0 interface=ether2
      actual-interface=ether2

 2    ;;; DMZ
      address=192.168.30.1/24 network=192.168.30.0 interface=ether3
      actual-interface=ether3

 3    ;;; to Branch
      address=192.168.100.1/30 network=192.168.100.0 interface=wireguard1
      actual-interface=wireguard1

 4 D address=192.168.50.1/32 network=192.168.50.199 interface=<l2tp-vpn-user1>
      actual-interface=<l2tp-vpn-user1>
```

Рисунок 3.6 – Результат виконання команди `ip address print detail` на маршрутизаторі MikroTik Main-RT

Окрім чотирьох раніше налаштованих статичних інтерфейсів - ether1 (WAN) з IP-адресою 88.1.1.2/24, ether2 (LAN) з адресою 192.168.20.1/24, ether3 (DMZ) з 192.168.30.1/24 та wireguard1 для тунелю Site-to-Site з адресою 192.168.100.1/30 - у списку з'явився п'ятий запис, позначений прапором D, тобто динамічно створений. Цей запис відповідає VPN-підключенню користувача vpn-user1, який підключився до маршрутизатора через L2TP/IPSec Remote Access VPN. Йому автоматично призначено адресу 192.168.50.199/32, яка відображається як частина інтерфейсу <l2tp-vpn-user1>. Це віртуальний інтерфейс, створений автоматично в процесі встановлення L2TP-сесії.

На рисунку 3.7 показано результат виконання команди і`p ipsec policy print detail` на маршрутизаторі MikroTik Main-RT, яка відображає активну політику IPsec, що використовується для шифрування VPN-з'єднання з клієнтами L2TP/IPSec Remote Access VPN.

```
[admin@Main-RT] > ip/ipsec/policy/print detail
Flags: T - template; B - backup;
X - disabled, D - dynamic, I - invalid, A - active; * - default
 0 T  * group=default src-address=::/0 dst-address=::/0 protocol=all
        proposal=default template=yes

 1   D  peer=l2tp-in-server tunnel=no src-address=88.1.1.2/32 src-port=1701
        dst-address=77.1.1.2/32 dst-port=1701 protocol=udp action=encrypt
        level=unique ipsec-protocols=esp proposal=default ph2-count=2
        ph2-state=established
[admin@Main-RT] >
```

Рисунок 3.7 – Результат виконання команди `ipsec policy print detail` на маршрутизаторі MikroTik Main-RT

Запис із прапором D (dynamic) свідчить про те, що ця політика була створена автоматично під час встановлення VPN-з'єднання з конкретним користувачем. Поле `peer=l2tp-in-server` вказує на те, що політика пов'язана з підключенням до L2TP-сервера, а не до Site-to-Site тунелю. Параметр `tunnel=no` означає, що IPsec не створює окремий тунель, а використовується для захисту L2TP-трафіку. Пара портів src-port=1701 і dst-port=1701 підтверджує, що політика стосується протоколу L2TP (udp 1701). Дія `action=encrypt` вказує, що трафік між цими вузлами має бути зашифрований. Поле `level=unique` означає, що політика застосовується лише до унікальної пари IP-адрес і портів. Встановлено використання `ipsec-protocols=esp`, тобто шифрування трафіку виконується з використанням протоколу ESP (Encapsulating Security Payload), який є основним методом шифрування в IPsec.

Важливим є параметр `proposal=default`, який визначає набір криптографічних алгоритмів - відповідно до попередніх налаштувань, це `aes-256-cbc + sha256/sha1`. Значення `ph2-state=established` свідчить про те, що друга фаза IPsec завершена успішно, ключі шифрування згенеровано, і тунель активний та готовий до передавання захищеного трафіку.

Отже, з'єднання встановлено коректно, шифрування працює, і користувач успішно інтегрований у VPN-сегмент корпоративної мережі. Це підтверджує повну функціональність L2TP/IPSec Remote Access VPN на маршрутизаторі MikroTik Main-RT.

3.2 Тестування Site-to-Site VPN

3.2.1 Маршрутизатор MikroTik

Перевірка працездатності WireGuard VPN між маршрутизаторами MikroTik Main-RT і Branch-RT проводиться для підтвердження встановлення захищеного Site-to-Site з'єднання, коректної маршрутизації між підмережами та успішного обміну трафіком через тунель. Основна мета перевірки - впевнитися, що тунель стабільно функціонує, peer-з'єднання активне, а пристрої з обох сторін можуть взаємодіяти на рівні 3-го рівня моделі OSI (IP-рівень).

На рисунку 3.8 показано вивід команди `interface wireguard peers print detail` на маршрутизаторі MikroTik Main-RT.

```
[admin@Main-RT] > interface wireguard peers print detail
Flags: X - disabled; D - dynamic
 0    interface=wireguard1
      public-key="53RB7hzTORikAu/2csA3kugytAfWl1QpI5wxxLfQDwo=" private-key=""
      endpoint-address=99.1.1.2 endpoint-port=13231
      current-endpoint-address=99.1.1.2 current-endpoint-port=13231
      allowed-address=0.0.0.0/0 preshared-key="" client-endpoint="" rx=585.2KiB
      tx=544.4KiB last-handshake=57s
[admin@Main-RT] >
```

Рисунок 3.8 – Результат виконання команди `interface wireguard peers print detail` на маршрутизаторі MikroTik Main-RT

Вивід команди підтверджує, що тунель WireGuard успішно функціонує та обмін даними між вузлами відбувається у режимі реального часу. Параметри конфігурації, наведені на зображенні, свідчать про активну сесію між Main-RT та віддаленим маршрутизатором Branch-RT.

Пара `endpoint-address=99.1.1.2` та `endpoint-port=13231` вказує на фактичну зовнішню IP-адресу та udp-порт віддаленого маршрутизатора Branch-RT, через які здійснюється з'єднання. Ці ж значення дублюються в параметрах

current-endpoint-address та current-endpoint-port, що підтверджує встановлений активний зв'язок.

Наявність полів rx=585.2 KiB та tx=544.4 KiB підтверджує двосторонній обмін трафіком. Це означає, що обидві сторони тунелю не лише ініціювали handshake, але й активно обмінюються даними. Параметр last-handshake=57s вказує на те, що нещодавній обмін криптографічною інформацією відбувся менш ніж хвилину тому, що відповідає типовому keepalive-інтервалу в WireGuard.

На рисунку 3.9 показано вивід команди tracer на маршрутизаторі MikroTik Main-RT.

```
[admin@Branch-RT] > tool/tracer  192.168.20.1 interface=wireguard1
Columns: ADDRESS, LOSS, SENT, LAST, AVG, BEST, WORST, STD-DEV
#  ADDRESS        LOSS  SENT  LAST  AVG  BEST  WORST  STD-DEV
1  192.168.20.1   0%      72  1ms   1.4  0.6   13.4   1.5
```

Рисунок 3.9 – Результат виконання команди tracer на маршрутизаторі MikroTik Branch-RT

Результати виконання команди tool/tracer на маршрутизаторі MikroTik Branch-RT з параметром interface=wireguard1 та цільовою IP-адресою 192.168.20.1 підтверджують працездатність тунелю WireGuard Site-to-Site VPN між філією та головним офісом. Цільова адреса 192.168.20.1 належить головному офісу. У звіті видно, що втрат пакетів (LOSS) не зафіксовано, що свідчить про стабільність з'єднання. Загальна кількість відправлених запитів - 72, всі досягли призначення, тобто маршрут до головного офісу через VPN-тунель активний і доступний без збоїв.

Таким чином, тести демонструють повністю працездатне VPN-з'єднання між головним офісом і філією з використанням WireGuard. Тунель шифрує весь переданий трафік, а маршрутизатори здійснюють повноцінну маршрутизацію між відповідними сегментами мережі.

3.2.2 Операційна система Ubuntu Linux

Тестування VPN Site-to-Site між головним офісом і філією з боку клієнта, що працює під управлінням операційної системи Ubuntu Linux [31], дозволяє перевірити коректність маршрутизації та доступність Windows Server 2022 RDS. Такий підхід демонструє, як пристрої у філії (192.168.40.0/24) можуть прозоро комунікувати з ресурсами головного офісу (192.168.20.0/24 та 192.168.30.0/24), використовуючи захищений VPN-канал, реалізований на основі протоколу WireGuard.

Після запуску віртуальної машини з Ubuntu Linux система автоматично отримує IP-адресу з пулу DHCP, налаштованого на маршрутизаторі MikroTik Branch-RT (див. рисунок 3.10).

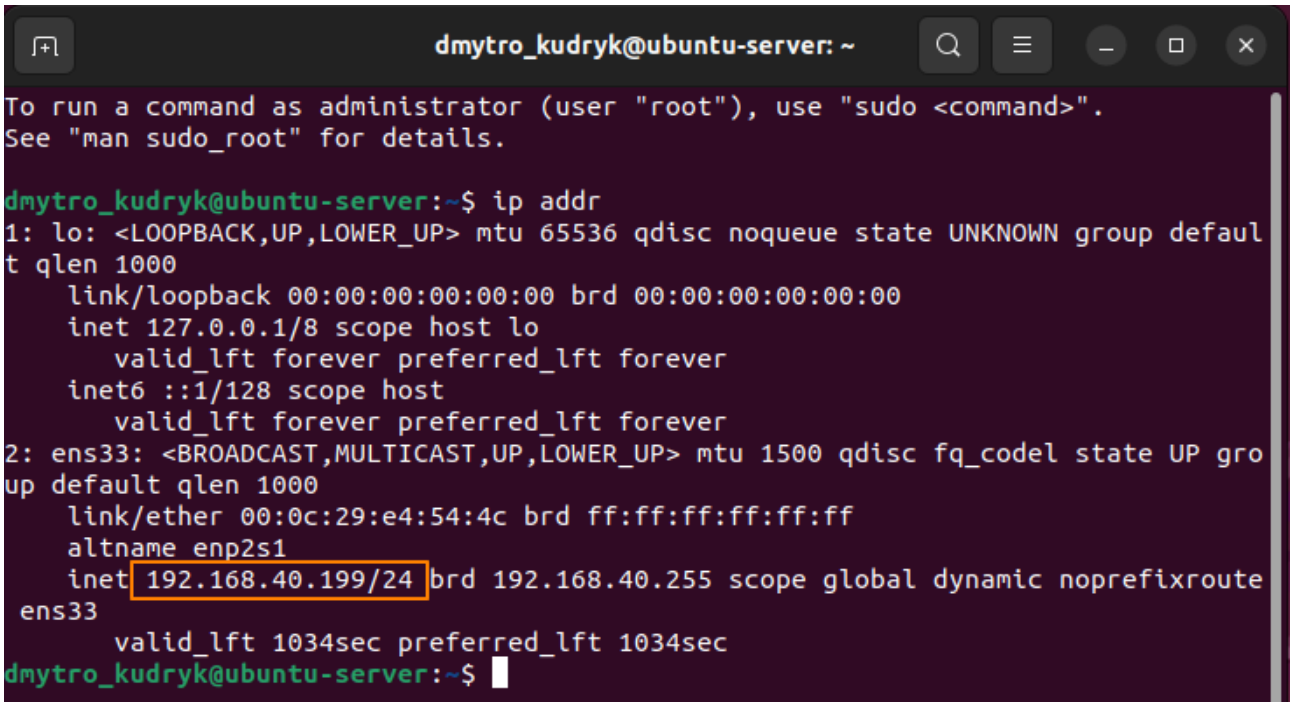

Рисунок 3.10 – Результат виконання команди `ip addr` в Ubuntu Linux

Усі запити до підмереж головного офісу маршрутизатор автоматично пересилає через інтерфейс wireguard1, що створює захищений тунель до Main-RT, завдяки статичним маршрутам, прописаним на рівні маршрутизатора (див. рисунок 3.11).

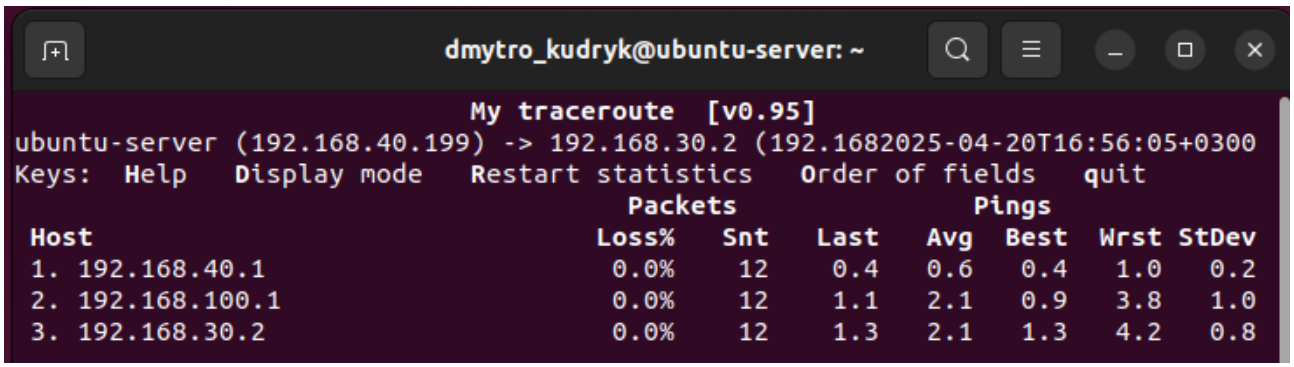

Рисунок 3.11 – Результат виконання команди `mtr 192.168.30.2 -n` в Ubuntu Linux

На рисунку показано результат виконання команди traceroute в Ubuntu Linux із локальною IP-адресою 192.168.40.199, що розташований у мережі філії та використовує тунель WireGuard Site-to-Site VPN для доступу до IP-адреси 192.168.30.2, яка належить серверу Windows Server 2022 RDS у сегменті DMZ головного офісу. Таким чином, трасування підтверджує, що трафік з хоста у філії через інтерфейс WireGuard успішно досягає внутрішніх ресурсів головного офісу. Усі проміжні маршрути відповідають очікуваній схемі: спочатку локальний шлюз, потім VPN-шлюз (Main-RT), і нарешті - Windows Server 2022 RDS в DMZ-сегменті. Це демонструє правильну маршрутизацію, активність тунелю WireGuard, а також доступність внутрішніх служб головного офісу з філії через захищене VPN-з’єднання.

На рисунку 3.12 показано результат виконання команди traceroute з Ubuntu Linux у філії до зовнішнього ресурсу ukr.net (IP-адреса 35.186.218.67).

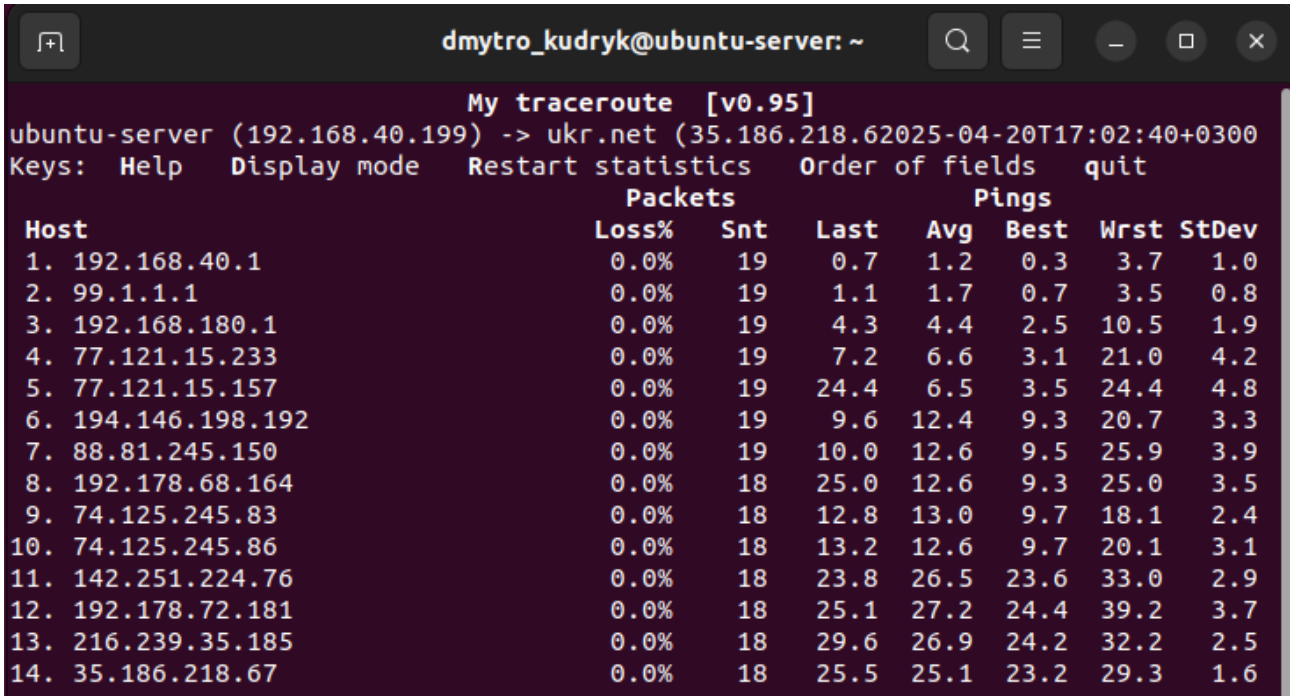

Рисунок 3.12 – Результат виконання команди `mtr ukr.net -n` в Ubuntu Linux

Трасування демонструє успішну реалізацію NAT на MikroTik Branch-RT та правильну маршрутизацію. Це підтверджує, що внутрішні клієнти філії можуть безперешкодно виходити в Інтернет, при цьому локальний доступ до ресурсів головного офісу відбувається через WireGuard VPN, а зовнішній трафік - через фізичне підключення до мережі Інтернет.

На рисунку 3.13 показано успішне встановлення з'єднання по протоколу RDP з Ubuntu-клієнта до сервера Windows Server 2022 RDS. Підключення здійснюється через програму Remmina [32], яка є популярним клієнтом віддаленого робочого столу для середовищ на базі Linux.

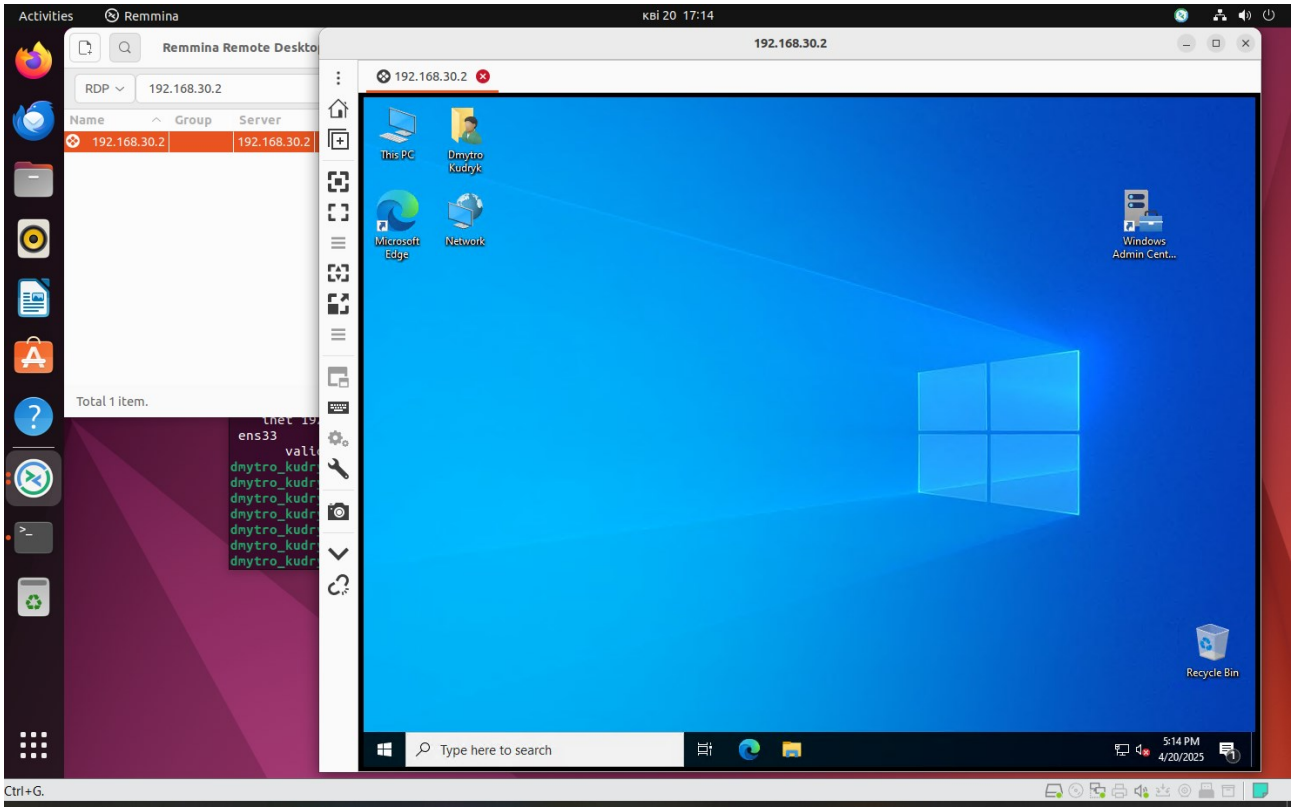

Рисунок 3.13 – З'єднання по протоколу RDP з Ubuntu до сервера Windows Server 2022 RDS

Таким чином, продемонстровано повну функціональність Site-to-Site VPN через WireGuard: від маршрутів і тунелювання до фактичного доступу до сервісів на кінцевих вузлах у віддаленій підмережі. Це підтверджує надійну інтеграцію мережевих сегментів через захищений VPN-канал.

3.5 Висновок до третього розділу

В третьому розділі було проведено практичне тестування функціональності VPN-з’єднань у лабораторному середовищі з використанням маршрутизаторів MikroTik та двох основних типів тунелювання - Remote Access VPN (L2TP/IPSec) і Site-to-Site VPN (WireGuard).

Для перевірки L2TP/IPSec Remote Access VPN було здійснено підключення з клієнтського ПК під керуванням Windows 10, що знаходився у віддаленій домашній мережі. Було підтверджено правильну роботу DHCP,

успішне встановлення VPN-тунелю, динамічне призначення IP-адреси з внутрішнього пулу 192.168.50.0/24, а також доступ до внутрішніх ресурсів головного офісу. Завдяки трасуванню, тестуванню з'єднання до сервера Windows Server 2022 RDS та запуску сеансу Remote Desktop було доведено, що маршрутизація, IPsec-шифрування, політики безпеки та міжмережеві екрани функціонують належним чином. Перевірка активних сесій на маршрутизаторі MikroTik Main-RT та IPsec-політик додатково підтвердила, що трафік зашифрований, а тунель повністю відповідає очікуваним параметрам безпеки.

У другій частині тестування було оцінено працездатність WireGuard Site-to-Site VPN між головним офісом та філією. На рівні маршрутизаторів MikroTik Main-RT та Branch-RT підтверджено наявність активного тунелю, обмін трафіком у обох напрямках, відсутність втрат пакетів та стабільне підтримання сесій. Статичні маршрути забезпечили прозорий доступ до підмереж головного офісу з філії. З боку клієнта, що працює під управлінням Ubuntu Linux у мережі Branch, було проведено трасування до сервера RDS у DMZ-сегменті головного офісу. Вивід команд mtr показав правильну маршрутизацію через WireGuard-тунель. Паралельно було підтверджено можливість виходу в Інтернет без використання WireGuard-тунель. Найбільш наочним підтвердженням працездатності Site-to-Site VPN стала успішна сесія підключення по протоколу RDP з Ubuntu Linux до Windows Server 2022 через програму Remmina.

Загалом тестування підтвердило, що конфігурація VPN у середовищі на основі MikroTik реалізована коректно. Обидва типи тунелів забезпечують надійну, стабільну та захищену комунікацію. Це створює передумови для масштабування рішення в умовах реального підприємства.

РОЗДІЛ 4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при переломах

Переломи є одними з найпоширеніших травм, які можуть виникати у людей будь-якого віку. Розуміння основних причин переломів допоможе не лише уникнути їх, але й надасть можливість краще підготуватися до їхнього лікування. Нижче наведено основні причини переломів:

Падіння є однією з найпоширеніших причин переломів, особливо серед дітей та літніх людей. Вдома падіння можуть статися через слизькі поверхні, неправильно розташовані предмети, відсутність поручнів на сходах або невідповідне освітлення. Зовні причиною падінь можуть бути нерівні тротуари, лід, сніг або інші перешкоди.

ДТП часто спричиняють важкі травми, включаючи переломи. Учасники аварій можуть отримати переломи різних кісток через силу удару, здавлювання або різке гальмування. Це одна з головних причин переломів серед молодих дорослих.

Активні види спорту, такі як футбол, хокей, гірські лижі, велосипедний спорт і навіть біг, можуть призвести до переломів через високий рівень фізичних навантажень, падіння або зіткнення. Особливо високий ризик мають спортсмени, які займаються контактними видами спорту.

Сильні удари або зіткнення, наприклад, під час бійок або нещасних випадків на виробництві, можуть спричинити переломи кісток. Високий ризик отримання таких травм мають люди, які працюють на будівництві, у важкій промисловості або займаються екстремальними видами діяльності.

Остеопороз – це стан, при якому кістки стають крихкими і більш схильними до переломів. Це особливо актуально для літніх людей, особливо жінок після менопаузи. Навіть незначні удари або падіння можуть спричинити перелом у людей з остеопорозом.

Механічні травми. Механічні травми, такі як удари важкими предметами, можуть призвести до переломів. Наприклад, падіння важкого предмета на ногу або руку може зламати кістку.

Переломи від перенапруження, або так звані "стресові переломи", можуть виникати через тривалі повторювані навантаження на певні кістки. Це часто зустрічається у бігунів, військовослужбовців та інших людей, які постійно піддаються великим фізичним навантаженням.

Деякі захворювання, такі як рак, інфекції або метаболічні розлади, можуть ослаблювати кістки, роблячи їх більш вразливими до переломів. Наприклад, кісткові метастази раку можуть призвести до переломів навіть при незначному впливі.

Професійні травми є частою причиною переломів. Робітники, які працюють у небезпечних умовах або з важким обладнанням, мають підвищений ризик отримати перелом через випадкові удари або падіння.

Насильницькі дії, такі як удари під час бійок або напади, можуть призвести до переломів різних кісток, особливо якщо удар був спрямований на череп, ребра або кінцівки.

Перш за все, необхідно забезпечити спокій та нерухомість потерпілого. Слід уникати будь-яких спроб самостійно виправити положення кісток або рухати кінцівкою, оскільки це може спричинити додаткові пошкодження м’яких тканин, нервів і судин. Якщо перелом відкритий (видно кістку), важливо зупинити кровотечу, застосувавши стерильну пов’язку. Накладіть її обережно, не натискаючи занадто сильно, щоб не пошкодити виступаючу кістку [33] .

Забезпечення іммобілізації є одним з найважливіших кроків у долікарській допомозі при переломах. Для цього можна використовувати підручні засоби, такі як дошки, палиці або будь-які жорсткі предмети, які можна зафіксувати бинтами або тканинами. Іммобілізація допомагає запобігти подальшому зміщенню уламків кістки та зменшує біль. При цьому важливо фіксувати не лише місце перелому, а й сусідні суглоби [33].

У випадку з переломами кінцівок, слід забезпечити їх підняття, якщо це можливо, для зменшення набряку. Застосування холодного компресу до місця травми також допомагає зменшити набряк і біль. Варто пам’ятати, що холодний компрес потрібно тримати не більше 20 хвилин, а між шкірою та компресом має бути тканина, щоб уникнути обмороження [33] .

При підозрі на перелом хребта або шиї потерпілого ні в якому разі не можна переміщати, оскільки це може призвести до пошкодження спинного мозку і паралічу. Слід забезпечити нерухомість голови та шиї до прибуття медичної допомоги, використовуючи підручні засоби для фіксації .

Щодо переломів ребер, основним завданням є забезпечення спокою потерпілому та зменшення рухів грудної клітки [33]. Потерпілому можна надати напівсидяче положення і накласти тугу пов'язку на грудну клітку для обмеження її рухливості. Однак, потрібно бути обережними, щоб не перетягнути грудну клітку і не утруднити дихання.

Найголовніше правило при наданні долікарської допомоги при переломах – це збереження спокою та мінімізація рухів потерпілого.

4.2 Рекомендації щодо естетичного оформлення інтер’єру цеху, дільниці

Естетичне оформлення інтер'єру цеху чи дільниці є важливим аспектом, який впливає на продуктивність працівників, їхнє здоров'я та загальне враження від підприємства. Одним із перших кроків у створенні привабливого інтер'єру є вибір кольорової гами. Використання яскравих і теплих кольорів може стимулювати енергію і мотивацію працівників. Наприклад, жовтий колір сприяє підвищенню настрою та креативності, тоді як зелений заспокоює та сприяє концентрації. Важливо уникати надмірно яскравих кольорів, які можуть викликати втому очей та знижувати продуктивність [34].

Наступним важливим аспектом є освітлення. Природне світло є найбільш сприятливим для робочого середовища, тому варто забезпечити максимальний

доступ до нього. Це можна зробити за допомогою великих вікон або світлових люків. Якщо природне світло обмежене, варто використовувати якісне штучне освітлення з нейтральними відтінками, яке не викликатиме напруги очей [34]. Освітлення повинно бути рівномірним, без тіней, щоб забезпечити комфортні умови для роботи.

Організація простору також відіграє важливу роль в естетичному оформленні інтер'єру цеху чи дільниці. Простір повинен бути добре організованим та максимально зручним для працівників. Це включає правильне розташування обладнання, робочих місць і зон відпочинку. Важливо уникати захаращення простору, що може призвести до стресу та зниження продуктивності [34].

Значну увагу слід приділити вибору меблів та обладнання. Вони повинні бути зручними, функціональними та відповідати ергономічним вимогам. Використання якісних матеріалів забезпечить довговічність меблів та обладнання, а також сприятиме створенню позитивного враження про підприємство [35]. Ергономічні стільці, столи і робочі станції допоможуть знизити ризик професійних захворювань і підвищити продуктивність працівників.

Декоративні елементи також можуть значно вплинути на загальний вигляд інтер'єру. Це можуть бути картини, плакати, зелень або інші елементи, які додають індивідуальності та стилю. Використання зелених рослин створює приємну атмосферу, покращує якість повітря і сприяє зниженню стресу. Варто також використовувати декоративні елементи, які відповідають тематиці підприємства або його продукції [35].

Звукова атмосфера є ще одним важливим аспектом естетичного оформлення. Надмірний шум може викликати стрес та знижувати продуктивність працівників [35]. Тому важливо забезпечити звуковий комфорт за допомогою звукоізоляційних матеріалів та обладнання, яке працює тихо. Використання музики або звуків природи може створити приємну атмосферу і покращити настрій працівників.

Температурний режим і вентиляція також важливі для створення комфортного робочого середовища. Оптимальна температура і свіже повітря сприяють підвищенню продуктивності та зниженню втоми. Варто забезпечити достатню кількість вентиляційних отворів або встановити кондиціонери для підтримання комфортної температури та забезпечення циркуляції повітря.

Оформлення зон відпочинку є важливою складовою естетичного оформлення інтер'єру. Вони повинні бути зручними і привабливими, щоб працівники могли повноцінно відпочити під час перерви. Зручні меблі, зелень і приємна атмосфера сприяють відновленню сил і підвищенню мотивації.

Важливим аспектом є також чистота та порядок у цеху чи дільниці. Регулярне прибирання і підтримка чистоти сприяють створенню приємної атмосфери і знижують ризик нещасних випадків та професійних захворювань. Варто встановити системи управління відходами та забезпечити працівників засобами для підтримки чистоти на робочих місцях.

Нарешті, варто звернути увагу на безпеку та доступність інтер'єру. Всі робочі місця повинні бути безпечними і відповідати стандартам безпеки. Доступність до всіх зон повинна бути забезпечена для всіх працівників, включаючи тих, хто має обмежені фізичні можливості [35]. Це можна досягти за допомогою спеціальних пандусів, ліфтів та інших засобів.

Естетичне оформлення інтер'єру цеху чи дільниці є важливим елементом, який впливає на продуктивність працівників, їхнє здоров'я та загальний імідж підприємства. Правильний вибір кольорової гами, освітлення, організація простору, вибір меблів та обладнання, декоративні елементи, звукова атмосфера, температурний режим і вентиляція, оформлення зон відпочинку, підтримка чистоти і порядку, а також забезпечення безпеки та доступності допоможуть створити привабливий і комфортний робочий простір.

4.3 Висновок до четвертого розділу

У четвертому розділі було розглянуто основи надання долікарської допомоги при переломах та рекомендації щодо естетичного оформлення інтер’єру цеху або дільниці.

Перший підрозділ детально охоплює основні причини виникнення переломів, серед яких падіння, дорожньо-транспортні пригоди, спортивні травми, професійні та побутові ушкодження. Було акцентовано увагу на важливості правильних дій при наданні першої допомоги потерпілому, зокрема забезпеченні спокою, іммобілізації пошкодженої ділянки, зменшенні болю та набряку, а також дотриманні заходів безпеки при підозрі на переломи хребта чи ребер. Надання грамотної долікарської допомоги дозволяє мінімізувати ускладнення та забезпечити ефективну подальшу медичну допомогу.

Другий підрозділ присвячений рекомендаціям щодо естетичного та функціонального оформлення виробничого середовища. Було підкреслено значення вибору кольорової гами, організації освітлення, ергономічності меблів, температурного режиму, озеленення зон відпочинку, а також підтримання чистоти та безпеки. Раціональний підхід до оформлення інтер’єру позитивно впливає на продуктивність працівників, знижує рівень стресу, покращує фізичне і психологічне самопочуття та формує привабливий імідж підприємства.

Таким чином, розділ підкреслює взаємозв’язок між фізичним здоров’ям працівника та умовами його праці, наголошуючи на необхідності комплексного підходу до забезпечення безпечного, комфортного й естетично привабливого робочого середовища.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи бакалавра було розглянуто, реалізовано та протестовано рішення щодо організації захищених VPN-з’єднань у корпоративному середовищі із використанням обладнання MikroTik. У роботі послідовно проаналізовано теоретичні основи технологій віртуальних приватних мереж, здійснено проєктування архітектури мережі з урахуванням різних типів тунелювання, а також проведено повноцінне практичне тестування в лабораторних умовах.

У першому розділі було охарактеризовано основні принципи побудови VPN, виділено ключові протоколи та типи тунелювання, включно з L2TP/IPSec і WireGuard. Також було розглянуто переваги та недоліки кожного з варіантів, питання безпеки, аутентифікації та шифрування, що дозволило обґрунтувати вибір конкретних рішень для практичного впровадження. Особливу увагу приділено технологіям маршрутизації, побудові DMZ-сегменту, механізмам міжмережевого екранування та адмініструванню на базі MikroTik RouterOS.

У другому розділі було виконано проєктування VPN-інфраструктури для організації доступу як з боку мобільних користувачів, так і для об’єднання двох віддалених офісів. Розроблено схему мережі з розподіленням на логічні сегменти, визначено IP-адресний простір, реалізовано налаштування тунелів Remote Access VPN (L2TP/IPSec) і Site-to-Site VPN (WireGuard). Також було проведено детальну конфігурацію міжмережевих екранів, маршрутизації, NAT та IPsec-політик, що забезпечує ізоляцію трафіку та підвищення рівня інформаційної безпеки.

У третьому розділі було здійснено практичне тестування функціональності обох типів VPN. Підключення клієнта з віддаленої домашньої мережі до L2TP/IPSec Remote Access VPN підтвердило правильну роботу DHCP, динамічне призначення IP, коректне шифрування трафіку та доступ до внутрішніх ресурсів головного офісу. Для Site-to-Site VPN через WireGuard було показано стабільність тунелю між філією та центральним

офісом, відсутність втрат пакетів і прозорий доступ до DMZ-сегменту з Ubuntu Linux у філії. Усі проведені перевірки, включно з трасуванням, тестуванням RDP та аналізом активних сесій, засвідчили правильність функціонування всієї побудованої інфраструктури.

У результаті проведеного дослідження було успішно реалізовано та перевірено на практиці побудову VPN-мережі на базі маршрутизаторів MikroTik. Створена інфраструктура забезпечує захищене з’єднання між користувачами і сегментами мережі підприємства, використовуючи як L2TP/IPSec для віддаленого доступу, так і WireGuard для з’єднання філій через Site-to-Site VPN. Запропоноване рішення забезпечує надійний, масштабований та захищений канал зв’язку між офісами та користувачами, що відповідає сучасним вимогам корпоративної безпеки і може бути впроваджене у реальному виробничому середовищі.

ПЕРЕЛІК ДЖЕРЕЛ

1. What is a virtual private network (VPN)? (n.d.). Retrieved from https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-virtual-private-network-vpn.html

2. 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.

3. How does a VPN work? (n.d.). Retrieved from https://www.paloaltonetworks.com/cyberpedia/how-does-a-vpn-work

4. 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.

5. What is a remote access VPN? (n.d.). Retrieved from https://www.paloaltonetworks.com/cyberpedia/what-is-a-remote-access-vpn

6. What Is a Site-to-Site VPN? (n.d.). Retrieved from https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn

7. What are the different types of VPN protocols? (n.d.). Retrieved from https://www.paloaltonetworks.com/cyberpedia/types-of-vpn-protocols

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

9. 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.

10. MikroTik. (n.d.). Retrieved from https://mikrotik.com/aboutus

11. RouterOS - RouterOS - MikroTik Documentation. (n.d.). Retrieved from https://help.mikrotik.com/docs/spaces/ROS/pages/328059/RouterOS

12. 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. https://doi.org/10.62731/mcnd-24.05.2024.001

13. WinBox - RouterOS - MikroTik Documentation. (n.d.). Retrieved from https://help.mikrotik.com/docs/spaces/ROS/pages/328129/WinBox

14. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). СИСТЕМА ЗМЕНШЕННЯ ВПЛИВУ DOS-АТАК НА ОСНОВІ MIKROTIK. Матеріали конференцій МЦНД, (17.05. 2024; Ужгород, Україна), 198-200.

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

16. Cloud hosted router, CHR - routeros - mikrotik documentation. (n.d.). Retrieved from https://help.mikrotik.com/docs/spaces/ROS/pages/18350234/Cloud+Hosted+Router+CHR

17. Тимощук, В., & Тимощук, Д. (2022). Віртуалізація в центрах обробки даних-аспекти відмовостійкості. Матеріали X науково-технічної конференції „Інформаційні моделі, системи та технології “Тернопільського національного технічного університету імені Івана Пулюя, 95-95.

18. Tymoshchuk, V., Pakhoda, V., Dolinskyi, A., Karnaukhov, A., & Tymoshchuk, D. (2024). MODELLING CYBER THREATS AND EVALUATING THE PERFORMANCE OF INTRUSION DETECTION SYSTEMS. Grail of Science, (46), 636–641. https://doi.org/10.36074/grail-of-science.29.11.2024.081

19. Firewall - RouterOS - MikroTik Documentation. (n.d.). Retrieved from https://help.mikrotik.com/docs/spaces/ROS/pages/250708066/Firewall

20. NAT - RouterOS - MikroTik Documentation. (n.d.). Retrieved from https://help.mikrotik.com/docs/spaces/ROS/pages/3211299/NAT

21. Tymoshchuk, V., Vantsa, V., Karnaukhov, A., Orlovska, A., & Tymoshchuk, D. (2024). COMPARATIVE ANALYSIS OF INTRUSION DETECTION APPROACHES BASED ON SIGNATURES AND ANOMALIES. Матеріали конференцій МЦНД, (29.11. 2024; Житомир, Україна), 328-332.

22. WireGuard - RouterOS - MikroTik Documentation. (n.d.). Retrieved from https://help.mikrotik.com/docs/spaces/ROS/pages/69664792/WireGuard

23. WireGuard: Fast, modern, secure VPN tunnel. (n.d.). Retrieved from https://www.wireguard.com/

24. Zagorodna, N., Skorenkyy, Y., Kunanets, N., Baran, I., & Stadnyk, M. (2022). Augmented Reality Enhanced Learning Tools Development for Cybersecurity Major. In ITTAP (pp. 25-32).

25. RFC 3826: The advanced encryption standard (AES) cipher algorithm in the SNMP user-based security model. (n.d.). Retrieved from https://datatracker.ietf.org/doc/html/rfc3826

26. RFC 2631: Diffie-hellman key agreement method. (n.d.). Retrieved from https://datatracker.ietf.org/doc/html/rfc2631

27. RFC 3526: More modular exponential (MODP) diffie-hellman groups for internet key exchange (IKE). (n.d.). Retrieved from https://datatracker.ietf.org/doc/html/rfc3526

28. What is perfect forward secrecy? Definition & faqs | vmware. (n.d.). Retrieved from https://www.vmware.com/topics/perfect-forward-secrecy

29. Windows Server documentation. (n.d.). Retrieved from https://learn.microsoft.com/en-us/windows-server/

30. Remote desktop services overview in windows server. (n.d.). Retrieved from https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/

31. Ubuntu Server documentation. (n.d.). Retrieved from https://documentation.ubuntu.com/server/

32. Remmina remote desktop client. (n.d.). Retrieved from https://remmina.org/

33. Посібник " Надання першої медичної допомоги при переломах". (n.d.). Retrieved from https://naurok.com.ua/posibnik-nadannya-persho-medichno-dopomogi-pri-perelomah-200976.html

34. 7 секретів від дизайнера інтер'єру робочих просторів | Продизайн. (n.d.). Retrieved from https://prodesign.in.ua/2023/08/7-sekretiv-vid-dyzajnera-interyeru-robochyh-prostoriv/

35. 5 підказок щодо оформлення інтер'єру робочого місця - Видавництво ArtHuss. (n.d.). Retrieved from https://www.arthuss.com.ua/books-blog/5-pidkazok-shchodo-oformlennya-interyeru-robochoho-mistsya

ДОДАТКИ

Додаток А

Файл конфігурації MikroTik Main-RT

```
# RouterOS 7.14.2
# software id =
#
/interface ethernet
set [ find default-name=ether1 ] comment=WAN disable-running-check=no
set [ find default-name=ether2 ] comment=LAN
set [ find default-name=ether3 ] comment=DMZ
/interface wireguard
add listen-port=13231 mtu=1420 name=wireguard1
/ip ipsec proposal
set [ find default=yes ] auth-algorithms=sha256,sha1 enc-algorithms=\
    aes-256-cbc pfs-group=modp2048
/ip pool
add name=DHCP-POOL ranges=192.168.20.100-192.168.20.200
add name=L2TP-IPSEC-POOL ranges=192.168.50.100-192.168.50.200
/ip dhcp-server
add address-pool=DHCP-POOL interface=ether2 name=DHCP-main-server1
/port
set 0 name=serial0
set 1 name=serial1
/ppp profile
add local-address=192.168.50.1 name=VPN_PROFILE remote-address=\
    L2TP-IPSEC-POOL
/interface l2tp-server server
set authentication=mschap2 default-profile=VPN_PROFILE enabled=yes use-ipsec=\
    yes
/interface wireguard peers
add allowed-address=0.0.0.0/0 endpoint-address=99.1.1.2 endpoint-port=13231 \
```

```
    interface=wireguard1 public-key=\
    "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
/ip address
add      address=88.1.1.2/24      comment=WAN      interface=ether1
network=88.1.1.0
add     address=192.168.20.1/24     comment=LAN     interface=ether2
network=192.168.20.0
add     address=192.168.30.1/24     comment=DMZ     interface=ether3
network=192.168.30.0
add       address=192.168.100.1/30       comment="to       Branch"
interface=wireguard1 \
    network=192.168.100.0
/ip dhcp-client
add disabled=yes interface=ether1
/ip dhcp-server network
add         address=192.168.20.0/24         dns-server=192.168.20.1
domain=main.kn.lan \
    gateway=192.168.20.1 netmask=24
/ip dns
set allow-remote-requests=yes servers=8.8.8.8,88.1.1.1
/ip firewall filter
add   action=accept   chain=input   comment="accept   established"
connection-state=\
    established
add action=accept chain=input comment="accept related" connection-
state=\
    related
add  action=drop  chain=input  comment="drop  invalid"  connection-
state=invalid
add   action=accept   chain=input   comment="allow   ICMP"   in-
interface=ether1 \
    protocol=icmp
add   action=accept   chain=input   comment="allow   Winbox"   in-
interface=ether1 \
    port=8291 protocol=tcp
```

```
add action=accept chain=input comment="allow SSH" in-
interface=ether1 port=22 \
    protocol=tcp
add action=accept chain=input comment="allow IPSec" in-
interface=ether1 port=\
    500 protocol=udp
add action=accept chain=input comment="allow IPSec" in-
interface=ether1 port=\
    4500 protocol=udp
add action=accept chain=input comment="allow L2TP" in-
interface=ether1 port=\
    1701 protocol=udp
add action=accept chain=input comment="allow WireGuard" in-
interface=ether1 \
    port=13231 protocol=udp
add action=drop chain=input comment="block everything else" in-
interface=\
    ether1
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1 src-
address=\
    192.168.20.0/24
add action=masquerade chain=srcnat out-interface=ether1 src-
address=\
    192.168.30.0/24
add action=masquerade chain=srcnat out-interface=ether1 src-
address=\
    192.168.50.0/24
/ip route
add disabled=no dst-address=0.0.0.0/0 gateway=88.1.1.1 routing-
table=main \
    suppress-hw-offload=no
add disabled=no distance=1 dst-address=192.168.40.0/24
gateway=wireguard1 \
```

```
    pref-src="" routing-table=main scope=30 suppress-hw-offload=no
\
    target-scope=10
/ppp secret
add name=vpn-user1 profile=VPN_PROFILE
add name=vpn-user2 profile=VPN_PROFILE
/system identity
set name=Main-RT
/system note
set show-at-login=no
```

Додаток Б

Файл конфігурації MikroTik Branch-RT

```
# RouterOS 7.14.2
# software id =
#
/interface ethernet
set [ find default-name=ether1 ] comment=WAN disable-running-check=no
set [ find default-name=ether2 ] comment=LAN
/interface wireguard
add listen-port=13231 mtu=1420 name=wireguard1
/ip pool
add name=DHCP-POOL ranges=192.168.40.100-192.168.40.200
/ip dhcp-server
add address-pool=DHCP-POOL interface=ether2 name=DHCP-branch-server1
/port
set 0 name=serial0
set 1 name=serial1
/interface wireguard peers
add allowed-address=0.0.0.0/0 endpoint-address=88.1.1.2 endpoint-port=13231 \
    interface=wireguard1 public-key=\
    "YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY"
/ip address
add address=99.1.1.2/24 comment=WAN interface=ether1 network=99.1.1.0
add address=192.168.40.1/24 comment=LAN interface=ether2 network=192.168.40.0
add address=192.168.100.2/30 comment="to Main" interface=wireguard1 network=\
    192.168.100.0
/ip dhcp-client
add disabled=yes interface=ether1
```

```
/ip dhcp-server network
add address=192.168.40.0/24 dns-server=192.168.40.1
domain=branch.kn.lan \
    gateway=192.168.40.1 netmask=24
/ip dns
set allow-remote-requests=yes servers=99.1.1.1,8.8.8.8
/ip firewall filter
add action=accept chain=input comment="accept established"
connection-state=\
    established
add action=accept chain=input comment="accept related" connection-
state=\
    related
add action=drop chain=input comment="drop invalid" connection-
state=invalid
add action=accept chain=input comment="allow ICMP" in-
interface=ether1 \
    protocol=icmp
add action=accept chain=input comment="allow Winbox" in-
interface=ether1 \
    port=8291 protocol=tcp
add action=accept chain=input comment="allow SSH" in-
interface=ether1 port=22 \
    protocol=tcp
add action=accept chain=input comment="allow WireGuard" in-
interface=ether1 \
    port=13231 protocol=udp
add action=drop chain=input comment="block everything else" in-
interface=\
    ether1
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1 src-
address=\
    192.168.40.0/24
/ip route
```

```
add disabled=no dst-address=192.168.20.0/24 gateway=wireguard1
routing-table=\
    main suppress-hw-offload=no
add disabled=no dst-address=192.168.30.0/24 gateway=wireguard1
routing-table=\
    main suppress-hw-offload=no
add disabled=no dst-address=0.0.0.0/0 gateway=99.1.1.1 routing-
table=main \
    suppress-hw-offload=no
add disabled=no dst-address=192.168.50.0/24 gateway=wireguard1
routing-table=\
    main suppress-hw-offload=no
/system identity
set name=Branch-RT
/system note
set show-at-login=no
```

Додаток В

Файл конфігурації MikroTik Home-RT

```
# RouterOS 7.14.2
# software id =
#
/interface ethernet
set [ find default-name=ether1 ] comment=WAN disable-running-check=no
set [ find default-name=ether2 ] comment=LAN
/ip pool
add name=DHCP-POOL ranges=172.16.1.100-172.16.1.200
/ip dhcp-server
add address-pool=DHCP-POOL interface=ether2 name=DHCP-home-server1
/port
set 0 name=serial0
set 1 name=serial1
/ip address
add address=172.16.1.1/24 comment=LAN interface=ether2 network=172.16.1.0
add address=77.1.1.2/24 comment=WAN interface=ether1 network=77.1.1.0
/ip dhcp-client
add disabled=yes interface=ether1
/ip dhcp-server network
add address=172.16.1.0/24 dns-server=172.16.1.1 domain=home.lan gateway=\
    172.16.1.1 netmask=24
/ip dns
set allow-remote-requests=yes servers=172.168.1.1,8.8.8.8
/ip firewall filter
add action=accept chain=input comment="accept established" connection-state=\
    established
```

```
add action=accept chain=input comment="accept related" connection-
state=\
    related
add action=drop chain=input comment="drop invalid" connection-
state=invalid
add action=accept chain=input comment="allow ICMP" in-
interface=ether1 \
    protocol=icmp
add action=accept chain=input comment="allow Winbox" in-
interface=ether1 \
    port=8291 protocol=tcp
add action=accept chain=input comment="allow SSH" in-
interface=ether1 port=22 \
    protocol=tcp
add action=drop chain=input comment="block everything else" in-
interface=\
    ether1
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1 src-
address=\
    172.16.1.0/24
/ip route
add disabled=no dst-address=0.0.0.0/0 gateway=77.1.1.1 routing-
table=main \
    suppress-hw-offload=no
/system identity
set name=Home-RT
/system note
set show-at-login=no
```