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

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: " Використання Site-to-Site VPN у побудові захищених мереж підприємств "

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

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

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

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

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2025

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

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

Кафедра кібербезпеки
(повна назва кафедри)

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

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Вдовиній Даяні Юріївні
(прізвище, ім'я, по батькові)

1. Тема роботи Використання Site-to-Site VPN у побудові захищених мереж підприємств

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

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

2. Термін подання студентом завершеної роботи 12.06.2025

3. Вихідні дані до роботи Маршрутизатор Mikrotik, вимоги до безпеки Site-to-Site VPN. Windows Server 2022 RDS, ОС Windows 11, методичні вимоги

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1. Огляд предметної області
2. Розгортання тестового лабораторного середовища
3. Тестування інформаційно-телекомунікаційної 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 та завдання. 4. Об'єкт, предмет і методи. 5. Технології та компоненти. 6. Схема лабораторного середовища. 7. Конфігурація VPN та брандмауера. 8. Windows Server 2022. 9. Тестування VPN-тунелю. 10. Тестування wireguard site-to-site VPN. 11. Тестування доступу до Windows Server 2022 з Windows 11 через VPN. 12. Перевірка можливості підключення до Windows Server 2022 через RDP. 13. Висновки. 14. Завершальний.

6. Консультанти розділів роботи

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

7. Дата видачі завдання 29.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

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

Студент _____ Вдовина Д. Ю.
(підпис) (прізвище та ініціали)

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

АНОТАЦІЯ

Використання Site-to-Site VPN у побудові захищених мереж підприємств // Кваліфікаційна робота ОР «Бакалавр» // Вдовина Даяна Юріївна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2025 // С. 80, рис. – 32, табл. – - , кресл. – 14, додат. – .

Ключові слова: WireGuard, MikroTik, VPN, RDP, Windows Server.

У кваліфікаційній роботі бакалавра досліджено сучасні підходи до побудови безпечних корпоративних мереж на основі VPN-рішень із використанням протоколу WireGuard. Проаналізовано переваги та недоліки існуючих технологій, охарактеризовано особливості маршрутизації, брандмауера, налаштування DHCP і NAT на обладнанні Mikrotik. У ході практичної частини розгорнуто тестову мережу, що моделює роботу головного офісу та віддаленої філії, налаштовано Site-to-Site VPN-тунель WireGuard для захищеного обміну даними. Перевірено стабільність, пропускну здатність і безпеку з'єднання, а також налаштовано доступ до Windows Server 2022 RDS, розташованого в DMZ. Результати підтверджують ефективність і надійність запропонованого рішення, що дає змогу підприємствам забезпечити конфіденційність корпоративної інформації й оптимізувати витрати на побудову та підтримку віддалених з'єднань.

ABSTRACT

Use of Site-to-Site VPN in Building Secure Enterprise Networks // Thesis of educational level "Bachelor"// Daiana Vdovyna // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБ-41 // Ternopil, 2025 // P. 80, figs. 32, tables -, drawings 14, added. -.

Keywords: WireGuard, MikroTik, VPN, RDP, Windows Server.

The bachelor's thesis explores modern approaches to building secure corporate networks based on VPN solutions using the WireGuard protocol. The advantages and disadvantages of existing technologies were analysed, and the features of routing, firewall, DHCP and NAT configuration on Mikrotik equipment were described. During the practical part, a test network was deployed to simulate the operation of the main office and a remote branch, and a WireGuard Site-to-Site VPN tunnel was configured for secure data exchange. The stability, bandwidth, and security of the connection were checked, and access to Windows Server 2022 RDS located in the DMZ was configured. The results confirm the effectiveness and reliability of the proposed solution, which allows enterprises to ensure the confidentiality of corporate information and optimise the cost of building and maintaining remote connections.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

VPN	—	Virtual Private Network
MPPE	—	Microsoft Point-to-Point Encryption
GRE	—	Generic Routing Encapsulation
IPSec	—	Internet Protocol Security
PPP	—	Point-to-Point Protocol
RDP	—	Remote Desktop Protocol
PPTP	—	Point-to-Point Tunneling Protocol
LAN	—	Local Area Network
WAN	—	Wide Area Network
RDS	—	Remote Desktop Services
TCP	—	Transmission Control Protocol
TLS	—	Transport Layer Security
SSTP	—	Secure Socket Tunneling Protocol
DHCP	—	Dynamic Host Configuration Protocol
NAT	—	Network Address Translation
CHR	—	Cloud Hosted Router
DMZ	—	Demilitarized Zone
ICMP	—	Internet Control Message Protocol
ESP	—	Encapsulating Security Payload
AES	—	Advanced Encryption Standard
SSL VPN	—	Secure Sockets Layer Virtual Private Network
SSL	—	Secure Sockets Layer
UDP	—	User Datagram Protocol
SHA	—	Secure Hash Algorithm
L2TP	—	Layer 2 Tunneling Protocol
IKEv2	—	Internet Key Exchange version 2

ВСТУП

Актуальність теми. В умовах швидкого розвитку цифрових технологій та збільшення кіберзагроз безпечний обмін даними між офісами, особливо у географічно розподілених структурах, є пріоритетним завданням для підприємств. Зростаюча кількість кіберзагроз та необхідність безпечного обміну даними між віддаленими офісами вимагають впровадження надійних рішень для забезпечення конфіденційності та цілісності інформації. Використання технології Site-to-Site VPN дозволяє створювати захищені канали зв'язку між офісами підприємства, забезпечуючи безпечну передачу даних через загальнодоступні мережі. Особливо актуальним є застосування сучасних протоколів, таких як WireGuard, які поєднують високу швидкість роботи з високим рівнем безпеки.

Мета і задачі дослідження. Метою даної роботи є дослідження та практична реалізація захищеної корпоративної мережі з використанням Site-to-Site VPN на базі протоколу WireGuard.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– дослідити виклики, пов’язані з побудовою безпечних корпоративних мереж;

– описати переваги використання VPN для створення корпоративних мереж;

– провести огляд існуючих типів VPN та їх особливостей;

– дослідити протокол WireGuard та його переваги у порівнянні з іншими VPN-рішеннями;

– розробити та налаштувати мережу VPN на базі Mikrotik CHR для головного офісу та філії з використанням WireGuard;

– налаштувати доступ з локальної мережі філії до Windows Server 2022 RDS у головному офісі;

– провести тестування та оцінити ефективність впровадженого рішення.

Об’єкт дослідження. Об'єктом дослідження є процес побудови захищених корпоративних мереж з використанням технології Site-to-Site VPN.

Предмет дослідження. Предметом дослідження є практична реалізація Site-to-Site VPN на базі протоколу WireGuard з використанням обладнання Mikrotik CHR для забезпечення безпечного з'єднання між офісами підприємства.

Практичне значення одержаних результатів. Результати даного дослідження можуть бути використані підприємствами для впровадження ефективних та надійних рішень з побудови захищених корпоративних мереж. Розроблені рекомендації та практичні налаштування дозволять забезпечити безпечний обмін даними між віддаленими офісами, підвищити загальний рівень інформаційної безпеки та оптимізувати витрати на впровадження та підтримку VPN-рішень.

РОЗДІЛ 1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Проблематика побудови безпечних корпоративних мереж

Проблематика побудови безпечних корпоративних мереж полягає у складності забезпечення конфіденційності, цілісності та доступності даних у цифровому середовищі. Зі зростанням обсягів корпоративної інформації та інтенсивності її обміну, підприємства стикаються з кіберзагрозами, що постійно еволюціонують [1].

Додатковий виклик створює необхідність інтеграції географічно розподілених офісів у єдину мережу, що вимагає ефективного рішення для передачі даних через загальнодоступні мережі, такі як Інтернет. Однак використання Інтернету як основного транспортного середовища підвищує ризик несанкціонованого доступу до даних, що потребує впровадження додаткових рівнів захисту. Відсутність належного шифрування даних може призвести до перехоплення конфіденційної інформації, такої як фінансові дані, особисті дані клієнтів чи стратегічно важливі корпоративні документи. Це особливо актуально для компаній з розподіленою інфраструктурою, де віддалені офіси або працівники потребують доступу до корпоративних ресурсів.

Крім того, підприємства стикаються з проблемами інтеграції різнорідних систем і пристроїв у єдину захищену мережу. Використання різних операційних систем, мережевого обладнання та програмного забезпечення може ускладнювати налаштування безпеки та створювати вразливості. Не менш важливим є людський фактор. Недостатнє навчання персоналу щодо правил безпечного користування мережевими ресурсами часто стає причиною порушення безпеки.

Ще однією складністю є дотримання вимог законодавства та стандартів інформаційної безпеки, що регламентують обробку даних, особливо в галузях, які працюють із конфіденційною інформацією, наприклад фінансовий сектор, охорона здоров'я чи державні установи. Крім того, підприємства часто

стикаються з обмеженнями бюджету, необхідністю збереження продуктивності мережі та забезпечення безперебійного доступу до ресурсів.

Для вирішення цих проблем використовуються технології віртуальних приватних мереж (VPN), які дозволяють створювати захищені канали зв'язку між офісами. Однак вибір відповідного протоколу VPN та його налаштування є складним завданням, яке потребує глибоких знань і досвіду. Сучасні VPN-рішення пропонують високий рівень безпеки, однак їхня ефективність залежить від правильної інтеграції з корпоративною інфраструктурою, включаючи налаштування брандмауера, політик доступу та моніторингу.

1.2 Переваги використання VPN для створення корпоративних мереж

Використання VPN для створення корпоративних мереж має низку переваг, які роблять цю технологію ключовим інструментом для забезпечення безпеки, ефективності та гнучкості роботи підприємств у цифровому середовищі [2].

Захист даних і безпека зв’язку у корпоративних мережах, побудованих з використанням VPN, є одними з ключових аспектів, що забезпечують надійне функціонування підприємства. VPN-технології дозволяють шифрувати переданий трафік, забезпечуючи його конфіденційність навіть у випадках використання загальнодоступних мереж, таких як Інтернет. Усі дані, що передаються між кінцевими точками VPN-з'єднання, інкапсулюються в зашифровані пакети.

Шифрування є основою безпеки VPN. Сучасні криптографічні алгоритми, такі як AES із довжиною ключа 128 або 256 біт, забезпечують високий рівень захисту. Навіть за умови перехоплення зашифрованих даних, розшифрувати їх без відповідного ключа практично неможливо через високу обчислювальну складність алгоритмів. Крім того, протоколи VPN, такі як WireGuard, використовують новітні криптографічні алгоритми, такі як ChaCha20, які поєднують високу продуктивність із надійним шифруванням. Інкапсуляція даних є ще одним важливим механізмом захисту, який реалізується у VPN. Передані дані поміщаються в тунель, що забезпечує ізоляцію інформації від

загального трафіку мережі. Це дозволяє приховати зміст даних і навіть інформацію про типи трафіку, що передається, від потенційних зловмисників. Завдяки цьому VPN забезпечує захист від атак типу Man-in-the-Middle, у яких зловмисники намагаються перехопити або змінити дані під час їхнього проходження через мережу [3]. Для додаткового захисту VPN використовує механізми перевірки цілісності даних. Ці механізми дозволяють переконатися, що дані не були змінені під час передачі, шляхом застосування криптографічних хеш-функцій. У разі виявлення змін у даних з'єднання може бути автоматично перервано, що запобігає можливому компрометуванню системи. Важливим аспектом безпеки є також аутентифікація. VPN-системи забезпечують перевірку особи користувача або пристрою перед наданням доступу до мережі. Це досягається за допомогою цифрових сертифікатів, облікових даних (логінів і паролів) або більш сучасних методів, таких як двофакторна аутентифікація. Ці заходи запобігають несанкціонованому доступу до корпоративної мережі навіть у випадках компрометації одного з рівнів безпеки. Додатковий рівень захисту забезпечується функцією приховування реальної IP-адреси. VPN замінює IP-адресу користувача на адресу VPN-сервера, що приховує місцезнаходження користувача і унеможливлює ідентифікацію його реальної мережі [4].

З'єднання віддалених офісів і мобільних працівників через VPN є важливим елементом сучасної корпоративної мережі, який забезпечує ефективний, безпечний і безперебійний доступ до ресурсів організації незалежно від фізичного розташування користувачів. За допомогою VPN можна створити єдину захищену мережу, яка об'єднує всі офіси компанії, розташовані в різних регіонах чи країнах, а також надає можливість співробітникам підключатися до неї віддалено, працюючи з дому чи під час відряджень.

Основним завданням такого підходу є забезпечення конфіденційності та безпеки переданих даних. VPN створює зашифровані тунелі між кінцевими точками - наприклад, між віддаленим офісом та головним сервером компанії [5]. Це дозволяє використовувати публічні мережі, такі як Інтернет, для передачі даних без ризику їх перехоплення. Інтеграція віддалених офісів у єдину мережу дозволяє обмінюватися даними між різними підрозділами компанії так, ніби

вони знаходяться в одному фізичному офісі. Це значно підвищує продуктивність та ефективність бізнес-процесів, дозволяючи співробітникам без затримок отримувати доступ до спільних ресурсів, таких як бази даних, документи чи програмне забезпечення, розташовані на центральних серверах.

Для мобільних працівників VPN є ключовим інструментом, який забезпечує доступ до корпоративної мережі незалежно від того, де вони знаходяться. Наприклад, співробітники, які працюють з дому або підключаються до мережі під час поїздок, можуть використовувати VPN для безпечного доступу до необхідних файлів і систем. Це особливо важливо в умовах, коли співробітники працюють у загальнодоступних мережах Wi-Fi, таких як кафе чи готелі. Використання VPN гарантує, що весь трафік, який проходить через ці мережі, залишається зашифрованим і недоступним для зловмисників. Зручність і простота налаштування VPN є важливою перевагою для мобільних працівників. Сучасні VPN-рішення дозволяють автоматично встановлювати з’єднання при підключенні до Інтернету, мінімізуючи технічні труднощі для кінцевих користувачів.

З’єднання віддалених офісів та мобільних працівників через VPN також дозволяє оптимізувати витрати на інфраструктуру. Використання загальнодоступних мереж як транспортного середовища є значно дешевшим, ніж побудова окремих фізичних каналів зв’язку. У той же час захист, який забезпечується за допомогою VPN, є еквівалентним до захисту приватних мереж.

Економічність використання VPN для створення корпоративних мереж є однією з ключових переваг цієї технології, яка дозволяє підприємствам оптимізувати витрати на побудову та підтримку мережевої інфраструктури без шкоди для її безпеки та продуктивності. Основна економія досягається завдяки використанню загальнодоступного Інтернету як транспортного середовища для передачі даних між офісами, співробітниками та корпоративними ресурсами.

Традиційні методи створення захищених мереж, наприклад, за допомогою виділених ліній зв’язку, є значно дорожчими. Вони вимагають великих капітальних вкладень у фізичну інфраструктуру, включаючи прокладання кабелів, встановлення апаратного забезпечення та підтримку роботи цих ліній. У

той же час VPN дозволяє використовувати вже існуючі загальнодоступні мережі для створення захищених каналів зв’язку, значно зменшуючи витрати на інфраструктуру. Додаткову економію забезпечує можливість масштабування VPN-з'єднань без значних фінансових витрат. У випадку розширення бізнесу та відкриття нових офісів чи філій впровадження VPN не потребує прокладання нових фізичних ліній або встановлення складного обладнання. Налаштування нових підключень може бути виконане за допомогою вже існуючих ресурсів компанії, таких як сервери VPN або маршрутизатори. Це дозволяє швидко інтегрувати нові підрозділи у корпоративну мережу, зберігаючи стабільність і безпеку з’єднання. Економічність VPN також проявляється в його здатності зменшувати витрати на технічне обслуговування та підтримку. Завдяки автоматизації багатьох процесів, таких як оновлення програмного забезпечення, налаштування політик безпеки та моніторинг мережі, знижується потреба у великих командах IT-спеціалістів. Крім того, простота налаштування сучасних VPN-протоколів дозволяє суттєво скоротити час і витрати на впровадження.

Ще одним аспектом економічності VPN є його гнучкість у використанні. Компанії можуть вибирати між різними моделями розгортання VPN, такими як локальні сервери або хмарні платформи, залежно від своїх потреб і фінансових можливостей [6]. Хмарні VPN-рішення дозволяють уникнути капітальних витрат на апаратне забезпечення, пропонуючи модель "оплати за використання".

Забезпечення безпечного та швидкого доступу до корпоративних ресурсів через VPN надає співробітникам можливість працювати віддалено, що значно підвищує гнучкість бізнес-процесів. Завдяки використанню зашифрованих тунелів та сучасних протоколів VPN компанії можуть гарантувати конфіденційність переданих даних та захист від несанкціонованого доступу, навіть якщо працівники підключаються до мережі з незахищених точок, наприклад, публічних Wi-Fi. Ця можливість особливо важлива у кризових ситуаціях, таких як пандемії, природні катаклізми чи інші форс-мажорні обставини, коли фізичний доступ до офісів може бути обмеженим або неможливим. В умовах, коли віддалена робота стає необхідністю, VPN забезпечує стабільний і безпечний канал для доступу до внутрішніх ресурсів

компанії, таких як документи, бази даних, програмне забезпечення або хмарні платформи. Додатково, VPN дозволяє компаніям швидко адаптуватися до змін, надаючи новим співробітникам чи підрядникам доступ до потрібних ресурсів без необхідності фізичної присутності. Це сприяє безперервності бізнес-процесів, підтримці продуктивності та збереженню конкурентних переваг навіть у нестабільних умовах.

Сукупність цих механізмів робить VPN одним із найефективніших рішень для забезпечення безпеки корпоративного трафіку, дозволяючи компаніям захищати свої дані від зовнішніх загроз і зберігати стабільність своєї інформаційної інфраструктури. Усе це сприяє безпечному обміну інформацією між офісами, віддаленими працівниками та корпоративними ресурсами, забезпечуючи високий рівень захисту даних навіть у складних умовах сучасного кіберпростору.

1.3 Існуючі типи VPN та їх особливості

1.3.1 Типи VPN

Типи VPN класифікуються залежно від призначення, способу побудови та рівня функціонування. Кожен тип має свої особливості, які роблять його придатним для певних задач і сценаріїв [7].

VPN Site-to-Site є типом віртуальної приватної мережі, яка забезпечує захищене з'єднання між двома або більше географічно розподіленими мережами. Ця технологія дозволяє об’єднати різні офіси, філії або дата-центри компанії в єдину логічну мережу, забезпечуючи безпечний і прозорий доступ до корпоративних ресурсів. У такій конфігурації пристрої, що знаходяться в різних мережах, взаємодіють так, ніби вони підключені до однієї локальної мережі, без потреби у додатковому налаштуванні для кожного пристрою.

Основним принципом роботи Site-to-Site VPN є використання шифрування та тунелювання для захисту даних, які передаються через загальнодоступні мережі, такі як Інтернет. Трафік з однієї мережі інкапсулюється в зашифровані

пакети, які передаються через тунель до іншої мережі, де вони розшифровуються (див. рисунок 1.1).

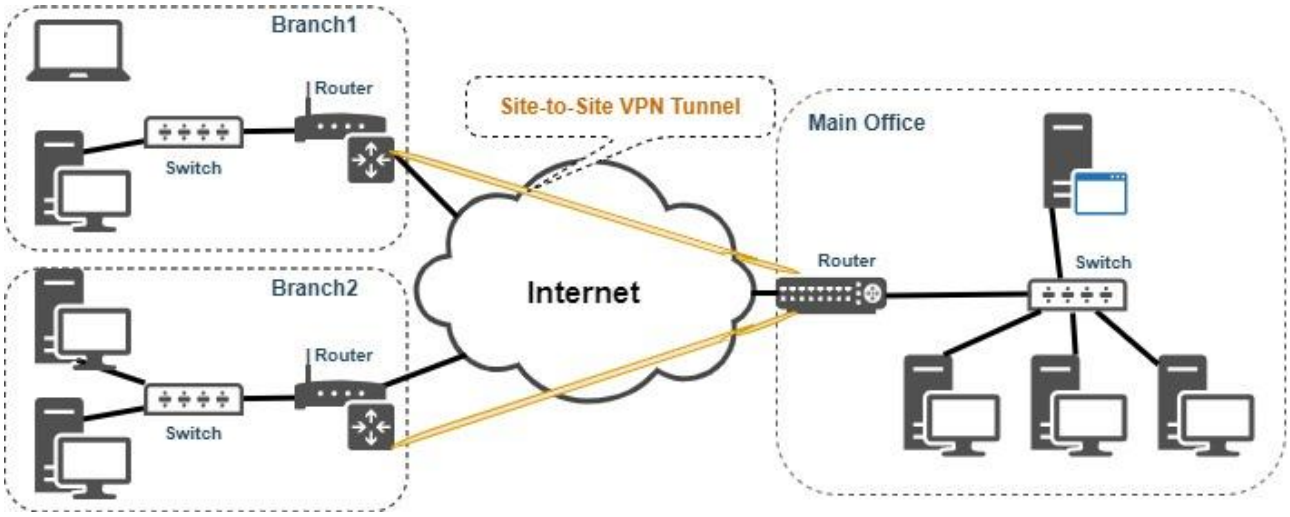

Рисунок 1.1 – VPN типу Site-to-Site

Site-to-Site VPN зазвичай налаштовується на рівні мережевих пристроїв, таких як маршрутизатори або спеціалізовані VPN-шлюзи. Це забезпечує централізоване управління і мінімізує потребу в ручному налаштуванні на кожному кінцевому пристрої. Однією з важливих переваг такого підходу є те, що підключення встановлюється автоматично і не потребує участі користувачів, що робить його зручним для великих корпоративних середовищ.

Цей тип VPN є ідеальним для організацій, які мають постійну необхідність у обміні великими обсягами даних між своїми офісами. Наприклад, головний офіс компанії може зберігати основні корпоративні дані та додатки, а віддалені офіси отримують до них доступ через Site-to-Site VPN, не порушуючи безпеку або продуктивність мережі. Крім того, використання VPN-тунелів дозволяє уникнути витрат на створення та підтримку виділених фізичних ліній зв’язку, використовуючи натомість існуючу інфраструктуру Інтернету.

Безпека є ключовим аспектом Site-to-Site VPN. Окрім шифрування, часто використовуються додаткові механізми захисту, такі як двофакторна автентифікація для VPN-шлюзів, динамічні ключі шифрування та фільтрування трафіку за певними політиками безпеки. Це дозволяє мінімізувати ризик несанкціонованого доступу до мережі навіть у разі перехоплення даних.

Site-to-Site VPN також має певні виклики. Вони включають потребу в належному налаштуванні обладнання, яке може бути складним і вимагати участі досвідчених IT-фахівців. Крім того, для забезпечення стабільного з'єднання важливо мати надійне інтернет-з'єднання в кожній точці, де розгорнута мережа. У разі поганої якості Інтернету з'єднання може бути нестабільним, що впливатиме на ефективність роботи систем. Загалом, Site-to-Site VPN є ефективним і економічним рішенням для організацій, які прагнуть інтегрувати свої розподілені офіси в єдину мережу з високим рівнем безпеки і стабільності, забезпечуючи безперебійний доступ до корпоративних ресурсів для всіх працівників.

Remote Access VPN є типом віртуальної приватної мережі, яка забезпечує індивідуальним користувачам безпечний доступ до корпоративної мережі через загальнодоступний Інтернет. Ця технологія широко використовується для підключення співробітників, які працюють віддалено, з дому, під час відряджень або з інших місць, до внутрішніх ресурсів організації, таких як файли, бази даних, сервери, корпоративні програми чи внутрішні веб-сайти.

Основним принципом роботи Remote Access VPN є створення зашифрованого тунелю між пристроєм користувача та сервером VPN, розташованим у корпоративній мережі (див. рисунок 1.2).

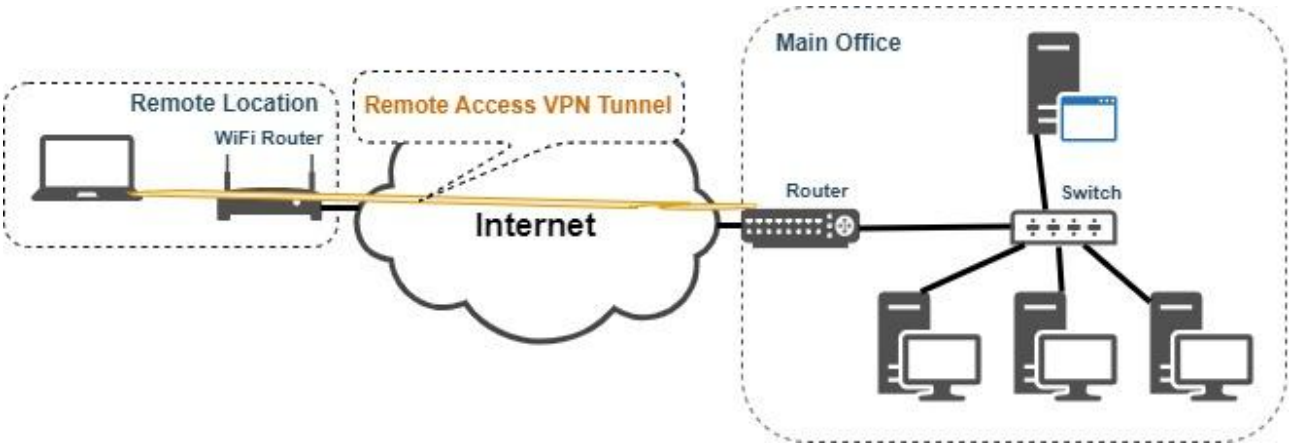

Рисунок 1.2 – VPN типу Remote Access

Усі дані, що передаються через цей тунель, шифруються, що гарантує конфіденційність і безпеку навіть у разі використання незахищених мереж, таких

як публічний Wi-Fi у кафе чи готелях. Це захищає інформацію від перехоплення або модифікації третіми сторонами, зокрема в умовах потенційних атак типу MITM.

Remote Access VPN зазвичай реалізується через спеціалізоване програмне забезпечення -VPN-клієнти, які встановлюються на пристрої користувача, такі як ноутбуки, смартфони чи планшети. VPN-клієнт підключається до VPN-сервера, розташованого в корпоративній мережі, і забезпечує автентифікацію користувача, використовуючи логін, пароль або більш безпечні методи, такі як двофакторна автентифікація. Цей тип VPN дозволяє користувачам підключатися до корпоративної мережі з будь-якої точки світу, якщо у них є доступ до Інтернету. Це особливо корисно для мобільних працівників або співробітників, які працюють на умовах гнучкого графіка. Наприклад, співробітник може отримати доступ до корпоративної бази даних або фінансової звітності, перебуваючи за межами офісу, без необхідності фізичної присутності в локальній мережі. Remote Access VPN також забезпечує гнучкість у налаштуванні доступу. Адміністратори мережі можуть визначати, до яких саме ресурсів користувачі матимуть доступ залежно від їхніх ролей у компанії. Наприклад, співробітники фінансового відділу можуть отримувати доступ до бухгалтерських програм, а IT-фахівці - до серверів і систем моніторингу.

Однією з головних переваг Remote Access VPN є економічність. Компаніям не потрібно створювати спеціалізовані фізичні канали зв’язку для кожного співробітника, що працює віддалено. Замість цього використовується вже існуюча інфраструктура Інтернету, що значно знижує витрати. Крім того, цей тип VPN легко масштабувати - додавання нових користувачів виконується швидко і не потребує значних витрат чи змін у мережевій інфраструктурі. Безпека Remote Access VPN є ключовим аспектом. Крім шифрування даних, забезпечується перевірка автентичності користувачів та їхніх пристроїв. Використання багатофакторної автентифікації, цифрових сертифікатів та фільтрації IP-адрес дозволяє мінімізувати ризик несанкціонованого доступу.

Попри численні переваги, Remote Access VPN має певні виклики. Одним із них є залежність від швидкості та якості Інтернет-з’єднання. Якщо у користувача

низька швидкість Інтернету, це може вплинути на продуктивність роботи. Також збільшення кількості одночасно підключених користувачів може створити додаткове навантаження на сервер VPN, що потребує належного планування та управління ресурсами. Remote Access VPN є ефективним і гнучким інструментом для забезпечення безпечного доступу до корпоративних мереж. Він дозволяє організаціям підтримувати продуктивність співробітників незалежно від їхнього місцезнаходження, водночас забезпечуючи високий рівень безпеки даних.

SSL VPN - це тип віртуальної приватної мережі, яка використовує протоколи TLS для забезпечення захищеного доступу до корпоративних ресурсів через загальнодоступні мережі, такі як Інтернет. Основна особливість SSL VPN полягає в тому, що доступ до мережі можна отримати безпосередньо через веб-браузер, що робить його зручним і гнучким для користувачів. На відміну від традиційних VPN-рішень, які потребують встановлення спеціалізованого клієнтського програмного забезпечення, SSL VPN забезпечує доступ через HTTPS-з’єднання, використовуючи стандартний веб-браузер. Це дозволяє користувачам легко підключатися до корпоративної мережі з будь-якого пристрою, навіть якщо вони не мають адміністративних прав для встановлення додаткових програм. Завдяки цьому SSL VPN є особливо корисним для мобільних працівників, партнерів або підрядників, які потребують тимчасового або обмеженого доступу до ресурсів компанії. SSL VPN створює захищений тунель між клієнтом і сервером VPN, у якому шифруються всі дані, що передаються (див. рисунок 1.3).

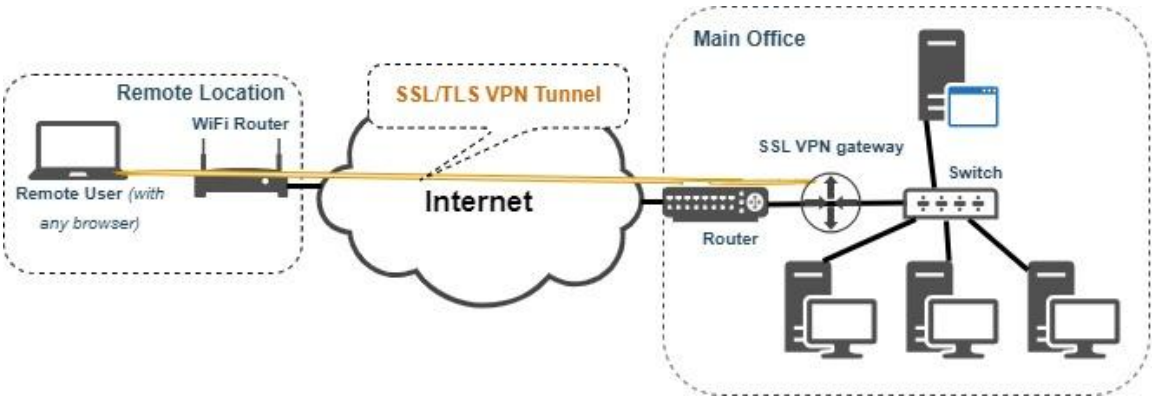

Рисунок 1.3 – SSL VPN

Протокол HTTPS забезпечує шифрування на основі SSL/TLS, що гарантує захист від перехоплення трафіку та атак типу MITM. Для додаткової безпеки SSL VPN зазвичай підтримує автентифікацію користувачів, використовуючи логін і пароль, цифрові сертифікати або багатофакторну автентифікацію. Однією з переваг SSL VPN є його сумісність із різними пристроями та операційними системами. Оскільки для підключення використовується веб-браузер, користувачі можуть отримувати доступ до корпоративної мережі з комп'ютерів, планшетів або смартфонів без необхідності налаштування складного обладнання чи програмного забезпечення. Це спрощує управління доступом і знижує витрати на підтримку інфраструктури.

SSL VPN підтримує два основних режими роботи: портал-доступ і тунель-доступ. У режимі портал-доступу користувачі отримують доступ до корпоративних веб-додатків або файлів через веб-інтерфейс, що дозволяє працювати безпосередньо через браузер.

У режимі тунель-доступу SSL VPN створює зашифрований тунель, який дозволяє доступ до ширшого спектра ресурсів, включаючи програми, які працюють не тільки через веб-браузер.

Окрім гнучкості, SSL VPN пропонує високий рівень безпеки. Забезпечується конфіденційність переданих даних, а також їхня цілісність. Механізми перевірки цілісності дозволяють виявляти та запобігати будь-яким змінам у переданій інформації. Крім того, SSL VPN дозволяє налаштовувати детальні політики доступу для кожного користувача або групи користувачів, обмежуючи доступ до певних ресурсів або дозволяючи його лише в певні часові проміжки. SSL VPN також є зручним рішенням для обходу мережевих обмежень. Оскільки він використовує HTTPS-з'єднання через порт 443, SSL VPN легко працює в середовищах, де доступ до інших портів може бути заблоковано. Це робить його особливо ефективним для користувачів, які працюють у країнах із суворими обмеженнями доступу до Інтернету або з корпоративних мереж, де обмежено використання інших протоколів.

Однак SSL VPN має певні обмеження. Наприклад, його продуктивність може залежати від навантаження на сервер та кількості одночасно підключених

користувачів. Крім того, для доступу до деяких ресурсів, які не є веб-орієнтованими, може знадобитися встановлення додаткового клієнтського програмного забезпечення, що знижує його універсальність.

SSL VPN ідеально підходить для організацій, які потребують гнучкого і безпечного доступу до своїх ресурсів. Він забезпечує надійний захист даних, простоту впровадження та масштабування, а також можливість знижувати витрати на підтримку інфраструктури. Це робить SSL VPN популярним вибором для підприємств будь-якого розміру, які прагнуть забезпечити безпечну віддалену роботу своїх співробітників.

Кожен із цих типів VPN має своє призначення і особливості, що дозволяють вибирати найбільш підходяще рішення залежно від потреб підприємства, його розміру та специфіки бізнес-процесів.

1.3.2 Типи протоколів VPN

Протоколи VPN є основою роботи віртуальних приватних мереж, оскільки саме вони визначають, як встановлюється і шифрується з'єднання між клієнтом і сервером VPN. Кожен протокол має свої особливості, переваги та недоліки, що робить їх придатними для різних завдань і сценаріїв використання.

PPTP є одним із найстаріших протоколів для побудови VPN, розробленим компанією Microsoft у 1990-х роках [8]. Його основна мета - створення зашифрованого тунелю між клієнтом і сервером через Інтернет для забезпечення безпечного доступу до мережевих ресурсів. PPTP працює на основі протоколу PPP, який відповідає за автентифікацію користувача та управління з’єднанням. Протокол PPTP широко підтримується багатьма операційними системами, включаючи Windows, macOS, Linux та мобільні пристроями, що забезпечує його зручність і простоту впровадження. Підключення через PPTP виконується швидко, оскільки він використовує відносно просте шифрування. Для захисту переданих даних PPTP застосовує 128-бітний алгоритм шифрування MPPE, який забезпечує базовий рівень конфіденційності.

Однією з головних переваг PPTP є його висока швидкість роботи. Оскільки протокол має невисокі вимоги до обчислювальних ресурсів, він забезпечує швидке встановлення з’єднання та передачу даних. Це робить PPTP придатним для задач, де швидкість є важливішою за високий рівень безпеки.

Однак PPTP має серйозні недоліки, які обмежують його використання в сучасних умовах. Головною проблемою є застарілі методи шифрування, які більше не відповідають сучасним стандартам безпеки. Протокол вразливий до різних типів атак, включаючи розшифрування переданих даних та компрометацію автентифікації. Це робить PPTP непридатним для задач, де потрібен високий рівень конфіденційності, наприклад, для передачі конфіденційних корпоративних даних. Ще одним недоліком PPTP є його залежність від протоколу GRE, який використовується для інкапсуляції даних. GRE-пакети можуть бути заблоковані брандмауерами або мережевими адміністраторами, що ускладнює використання PPTP в обмежених мережах. Крім того, PPTP не підтримує сучасні функції захисту, такі як перевірка цілісності даних або багатофакторна автентифікація.

Станом на сьогодні PPTP рідко використовується для серйозних задач через низький рівень безпеки. Хоча він залишається привабливим для новачків завдяки простоті налаштування і сумісності з різними платформами, його використання обмежується лише сценаріями, де безпека не є пріоритетом. Сучасні протоколи, такі як OpenVPN, WireGuard або IKEv2, значно перевершують PPTP за рівнем захисту і продуктивності, тому PPTP поступово втратив свою актуальність і замінюється більш надійними рішеннями.

L2TP/IPsec - це комбінація двох протоколів, що використовуються для створення захищених віртуальних приватних мереж. L2TP відповідає за інкапсуляцію і передачу даних через тунель [9], а IPsec забезпечує шифрування, автентифікацію та цілісність переданих даних [10]. Разом ці протоколи забезпечують високий рівень безпеки, що робить їх популярним вибором для створення як корпоративних, так і особистих VPN. Основна роль L2TP полягає в створенні тунелю, через який передаються дані. Цей протокол працює на рівні 2 моделі OSI (канальному рівні) і дозволяє інкапсулювати різні типи мережевих

протоколів. Однак сам L2TP не забезпечує шифрування даних, що передаються. Саме тому він використовується в поєднанні з IPsec, який шифрує трафік, захищає від несанкціонованого доступу та забезпечує перевірку цілісності даних.

IPsec додає кілька рівнів безпеки до L2TP-з'єднання. Він використовує шифрування для захисту даних, які передаються через тунель, і автентифікацію для перевірки ідентичності обох сторін з'єднання. Зазвичай IPsec працює в режимі транспортного або тунельного режиму. У випадку з L2TP/IPsec найчастіше використовується тунельний режим, який інкапсулює та шифрує весь IP-пакет, забезпечуючи максимальний захист. L2TP/IPsec є сумісним із більшістю сучасних операційних систем, таких як Windows, macOS, Linux, iOS і Android, що робить його доступним для використання на різних пристроях. Налаштування цього протоколу зазвичай просте для кінцевих користувачів, оскільки більшість сучасних платформ мають вбудовану підтримку L2TP/IPsec.

Однією з головних переваг L2TP/IPsec є високий рівень безпеки. Завдяки комбінації шифрування IPsec і тунелювання L2TP забезпечується захист даних навіть у разі їхнього перехоплення зловмисниками. IPsec використовує сучасні криптографічні алгоритми, такі як AES-256, що гарантують надійне шифрування. Крім того, механізми перевірки цілісності, такі як HMAC, дозволяють виявляти будь-які спроби зміни переданих даних.

Однак L2TP/IPsec має і свої недоліки. Одним із головних є його відносно низька швидкість у порівнянні з більш сучасними протоколами, такими як WireGuard або OpenVPN. Це зумовлено тим, що L2TP/IPsec використовує подвійне інкапсулювання: спочатку дані інкапсулюються за допомогою L2TP, а потім шифруються IPsec. Такий підхід створює додаткове навантаження на процесор і збільшує затримки при передачі даних. Ще одним викликом є потенційна складність налаштування у мережах із суворими правилами брандмауера. L2TP/IPsec використовує порти UDP 500 і 4500, а також протокол ESP, які можуть блокуватися мережевими адміністраторами. Це може обмежити можливість встановлення з'єднання в певних середовищах.

L2TP/IPsec часто використовується для забезпечення безпечного віддаленого доступу до корпоративних ресурсів або для підключення між філіями компаній. Завдяки своїй безпеці та сумісності, цей протокол залишається популярним вибором для організацій, які потребують захищеного з'єднання, навіть якщо він поступається в продуктивності деяким новітнім рішенням. Загалом, L2TP/IPsec забезпечує ефективний баланс між безпекою та універсальністю, що робить його придатним для широкого спектра задач, хоча його продуктивність і складність у певних умовах можуть бути обмеженням.

OpenVPN - це популярний і універсальний протокол VPN з відкритим вихідним кодом, який забезпечує високий рівень безпеки, гнучкість і сумісність із різними платформами [11]. Він використовує бібліотеку OpenSSL для шифрування даних і підтримує широкий спектр криптографічних алгоритмів, таких як AES-256, що гарантує конфіденційність і захист переданих даних. OpenVPN працює як на UDP, так і на TCP протоколах, що дозволяє налаштовувати з'єднання під різні сценарії використання, включаючи обхід мережевих обмежень і брандмауерів.

Головною перевагою OpenVPN є його висока гнучкість. Завдяки відкритому вихідному коду, його можна налаштовувати відповідно до специфічних вимог організації. OpenVPN дозволяє використовувати як точка-точка з'єднання, так і масштабовані багатокористувацькі конфігурації. Він також підтримує різні методи автентифікації, включаючи облікові дані користувачів, цифрові сертифікати та багатофакторну автентифікацію, що додає додатковий рівень безпеки.

OpenVPN підтримує динамічний обмін ключами, що ускладнює злом навіть у разі тривалого перехоплення трафіку. Для перевірки цілісності даних використовуються криптографічні хеш-функції, такі як HMAC, які дозволяють виявляти будь-які зміни у переданих пакетах.

OpenVPN є кросплатформеним і сумісним із більшістю операційних систем, включаючи Windows, macOS, Linux, iOS і Android. Це дозволяє використовувати його на будь-яких пристроях, забезпечуючи універсальність і зручність для користувачів. Для налаштування клієнтів і серверів OpenVPN надає

конфігураційні файли, які можуть бути адаптовані до конкретних потреб, що робить процес впровадження відносно простим для досвідчених адміністраторів.

Попри всі переваги, OpenVPN має певні недоліки. Одним із них є відносно високе навантаження на систему через складність криптографічних обчислень, що може впливати на продуктивність з'єднання, особливо на слабких пристроях. Крім того, налаштування OpenVPN може бути складним для недосвідчених користувачів, оскільки воно вимагає знань у галузі мережевих технологій та роботи з сертифікатами.

OpenVPN зазвичай використовується в корпоративних середовищах, де необхідний високий рівень безпеки і гнучкість. Він також підходить для особистого використання, особливо для обходу географічних обмежень або захисту трафіку в незахищених мережах, таких як публічні Wi-Fi. Завдяки своїй універсальності, OpenVPN підтримує різні сценарії, включаючи Site-to-Site VPN, Remote Access VPN і навіть складні багатосегментні конфігурації.

SSTP - це протокол VPN, розроблений Microsoft, який забезпечує захищене тунелювання даних через загальнодоступні мережі, такі як Інтернет [12]. Він використовує SSL/TLS для шифрування та автентифікації, що гарантує високий рівень безпеки та конфіденційності переданих даних. SSTP був представлений у Windows Vista і з того часу підтримується всіма основними версіями Windows, що робить його природним вибором для середовищ на базі цієї операційної системи.

Однією з ключових переваг SSTP є його здатність працювати через порт 443, який використовується для HTTPS-з'єднань. Завдяки цьому SSTP здатний обходити більшість брандмауерів і мережевих фільтрів, оскільки його трафік виглядає як звичайний веб-трафік. Це робить протокол особливо корисним у середовищах зі строгими обмеженнями доступу до Інтернету або в країнах із жорстким контролем мережевого трафіку. SSTP використовує SSL/TLS для встановлення захищеного з'єднання між клієнтом і сервером. SSL/TLS забезпечує надійне шифрування трафіку, автентифікацію обох сторін з'єднання та перевірку цілісності даних. SSTP інтегрований у Windows, що спрощує процес його налаштування та використання для користувачів цієї операційної системи.

Завдяки цьому користувачі можуть створювати з'єднання без встановлення додаткового програмного забезпечення, використовуючи лише вбудовані інструменти Windows. Хоча SSTP спочатку був розроблений для Windows, існують сторонні реалізації, які дозволяють використовувати його на інших платформах, таких як Linux.

SSTP пропонує високий рівень безпеки, що робить його придатним для передачі конфіденційних даних у корпоративних середовищах. Автентифікація сервера виконується за допомогою цифрових сертифікатів, що гарантує, що клієнт підключається саме до авторизованого сервера. Для додаткової безпеки SSTP може використовувати сертифікати клієнта, що забезпечує автентифікацію обох сторін з'єднання.

Однак SSTP має деякі обмеження. Його вихідний код не є відкритим, оскільки протокол розроблений і підтримується Microsoft. Це викликає побоювання у деяких користувачів щодо можливих прихованих вразливостей або бекдорів. Крім того, SSTP не є настільки гнучким, як OpenVPN або WireGuard, у питаннях налаштування та підтримки різних платформ. Хоча сторонні реалізації протоколу існують, їхня інтеграція з іншими операційними системами може бути складною. Продуктивність SSTP зазвичай хороша, але через складність криптографічних операцій швидкість може бути дещо нижчою, ніж у простіших протоколів, таких як PPTP. Водночас, завдяки оптимізації під Windows, SSTP забезпечує стабільну роботу без значного впливу на продуктивність мережі. SSTP часто використовується для забезпечення віддаленого доступу до корпоративних ресурсів у середовищах Windows, особливо там, де потрібно обійти мережеві обмеження. Завдяки високому рівню безпеки, простоті використання та здатності працювати через порт 443, SSTP є ефективним рішенням для організацій, які прагнуть забезпечити захищений і надійний доступ до своїх мереж. Однак його використання в багатоплатформних середовищах може бути обмеженим через відсутність підтримки деяких операційних систем.

IKEv2/IPsec - це сучасний протокол VPN, який поєднує у собі надійність, безпеку та високу продуктивність [13]. IKEv2/IPsec був розроблений спільно

Microsoft і Cisco для забезпечення швидкого, стійкого та захищеного з'єднання між клієнтським пристроєм і сервером VPN. Протокол є особливо популярним у мобільних середовищах завдяки своїй здатності швидко відновлювати з’єднання після зміни мережі, наприклад, при переході з Wi-Fi на мобільний Інтернет.

IKEv2 є протоколом, який працює в рамках IPsec для створення тунелів і управління ключами шифрування. Його основна функція - ініціалізація та встановлення захищеного з'єднання між клієнтом і сервером, а також регулярне оновлення ключів для підтримки високого рівня безпеки. IPsec, у свою чергу, забезпечує шифрування даних, перевірку їхньої цілісності та автентифікацію кінцевих точок з'єднання. У поєднанні ці два компоненти створюють потужний механізм для передачі даних у VPN.

Однією з найбільших переваг IKEv2/IPsec є його швидкість і продуктивність. Протокол оптимізований для використання сучасного обладнання, що дозволяє мінімізувати затримки і забезпечує високі швидкості передачі даних навіть при складному шифруванні. IKEv2 підтримує потужні алгоритми шифрування, такі як AES-256, а також протоколи перевірки цілісності, такі як SHA-256, що робить його надзвичайно надійним для захисту конфіденційної інформації.

IKEv2/IPsec також відомий своєю стійкістю до мережевих збоїв. Завдяки функції MOBIKE (Mobility and Multihoming), протокол дозволяє автоматично відновлювати VPN-з'єднання у разі зміни IP-адреси або типу підключення. Це робить його ідеальним для мобільних користувачів, які можуть перемикатися між мережами Wi-Fi і стільникового зв'язку, не втрачаючи доступу до VPN. Протокол широко підтримується сучасними операційними системами, включаючи Windows, macOS, iOS, Android і Linux. Його вбудована підтримка в багатьох ОС спрощує налаштування та використання, оскільки користувачам зазвичай не потрібно встановлювати додаткове програмне забезпечення. Це робить IKEv2/IPsec зручним вибором як для корпоративних, так і для індивідуальних користувачів.

Безпека IKEv2/IPsec базується на сучасних криптографічних методах і перевірених алгоритмах. Протокол забезпечує сильне шифрування, що захищає

дані навіть у разі їхнього перехоплення. Крім того, IKEv2/IPsec підтримує багатофакторну автентифікацію, що додає додатковий рівень захисту. Для автентифікації можуть використовуватися цифрові сертифікати, ключі попереднього спільного використання (PSK) або інші методи, що забезпечують високу гнучкість у налаштуванні.

Проте IKEv2/IPsec має деякі обмеження. Одним із недоліків є залежність від UDP-портів 500 і 4500, які можуть блокуватися в мережах зі строгими правилами брандмауера. Це може ускладнити використання протоколу в середовищах із жорсткими мережевими обмеженнями. Крім того, хоча IKEv2/IPsec є дуже безпечним, його налаштування може бути складним для недосвідчених користувачів, оскільки воно вимагає глибокого розуміння мережевих технологій і шифрування. IKEv2/IPsec є популярним вибором для корпоративних мереж завдяки своїй надійності, безпеці та мобільності. Він також широко використовується приватними користувачами, які хочуть забезпечити конфіденційність своїх даних в Інтернеті або обійти географічні обмеження.

WireGuard - це сучасний VPN-протокол з відкритим вихідним кодом, розроблений для забезпечення максимальної продуктивності, простоти використання та високого рівня безпеки [14]. Він був створений з акцентом на мінімалістичний дизайн і ефективність, що робить його однією з найшвидших і найнадійніших VPN-технологій, доступних на сьогодні. WireGuard працює на рівні ядра операційної системи, що дозволяє знизити затримки та підвищити швидкість обробки трафіку. Це досягається завдяки його невеликій кодовій базі, яка значно менша за інші VPN-протоколи, такі як OpenVPN або IPsec. Невелика кодова база не лише підвищує продуктивність, але й забезпечує легший процес перевірки та підтримки, знижуючи ймовірність наявності вразливостей або помилок у коді.

WireGuard використовує новітні криптографічні алгоритми, такі як ChaCha20 для шифрування, Poly1305 для автентифікації повідомлень і Curve25519 для обміну ключами. Ці алгоритми забезпечують високу швидкість і водночас гарантують надійний захист переданих даних. Завдяки цьому WireGuard вважається більш безпечним і сучасним у порівнянні з традиційними

протоколами, такими як OpenVPN або IPsec, які використовують старіші криптографічні стандарти.

Однією з унікальних особливостей WireGuard є його простота налаштування. Кожен вузол у мережі має унікальні криптографічні ключі, які використовуються для автентифікації і встановлення з'єднання. Це усуває необхідність у складній інфраструктурі сертифікатів, характерній для інших протоколів. Усі налаштування здійснюються через прості конфігураційні файли, що робить процес встановлення швидким і зручним. WireGuard підтримує технологію roaming, яка дозволяє клієнтам безперебійно змінювати IP-адресу без втрати з'єднання. Це особливо корисно для мобільних пристроїв, які можуть переходити між різними мережами, такими як Wi-Fi і стільниковий зв'язок, не перериваючи VPN-з'єднання. Завдяки цьому WireGuard є ідеальним вибором для мобільних користувачів, які потребують стабільного та безпечного доступу до мережі. Протокол також відзначається високою продуктивністю. Завдяки ефективному використанню ресурсів і оптимізації на рівні ядра, WireGuard забезпечує низькі затримки і високі швидкості передачі даних навіть на слабкому обладнанні. Це робить його привабливим для використання як у корпоративних мережах, так і для особистого захисту трафіку. WireGuard є кросплатформним і доступним для більшості сучасних операційних систем, включаючи Linux, Windows, macOS, iOS і Android. Крім того, його інтеграція в ядро Linux (починаючи з версії 5.6) робить його нативною частиною системи, що ще більше підвищує продуктивність і зручність використання на цій платформі. Безпека WireGuard підсилюється його дизайном, орієнтованим на мінімізацію поверхні атаки. Наприклад, протокол не підтримує динамічну зміну налаштувань у реальному часі або складних механізмів відновлення з'єднання, які могли б створити додаткові вразливості. Замість цього він покладається на простоту та прозорість, які знижують ймовірність помилок і підвищують довіру до технології. Однак WireGuard має деякі обмеження. Наприклад, він не забезпечує шифрування метаданих трафіку, таких як IP-адреси вузлів, що може бути проблемою для користувачів, які шукають максимальну анонімність.

WireGuard підходить для широкого спектра задач: від захисту персонального трафіку у публічних мережах Wi-Fi до створення корпоративних VPN для віддаленого доступу або з'єднання між офісами. Завдяки поєднанню швидкості, безпеки та простоти, WireGuard стає стандартом нового покоління VPN, який поступово замінює старіші та менш ефективні протоколи.

1.4 Висновки до першого розділу

У першому розділі було проведено огляд предметної області, пов’язаної з побудовою безпечних корпоративних мереж. Було визначено основні проблеми, з якими стикаються підприємства у процесі забезпечення конфіденційності, цілісності та доступності даних. Зокрема, розглянуто питання зростання кіберзагроз, інтеграції географічно розподілених офісів у єдину мережу, дотримання стандартів інформаційної безпеки та обмежень бюджету. Окрему увагу приділено перевагам використання VPN для створення корпоративних мереж. Розглянуто механізми захисту, які забезпечують сучасні VPN-рішення, включаючи шифрування, інкапсуляцію даних, перевірку цілісності та автентифікацію. Також було висвітлено значення VPN для з’єднання віддалених офісів та мобільних працівників, що дозволяє забезпечити безпечний доступ до корпоративних ресурсів незалежно від фізичного місцезнаходження користувачів. У розділі проведено аналіз існуючих типів VPN, таких як Site-to-Site, Remote Access і SSL VPN, їхніх особливостей, переваг і викликів. Site-to-Site VPN продемонстровано як ефективне рішення для інтеграції офісів у єдину мережу, а Remote Access VPN і SSL VPN визнані зручними інструментами для мобільних працівників та організацій з динамічними потребами в доступі до ресурсів. Додатково було розглянуто основні протоколи VPN: PPTP, L2TP/IPsec, OpenVPN, SSTP, IKEv2/IPsec і WireGuard. Було проведено детальний аналіз їхніх технічних характеристик, безпекових можливостей, продуктивності та сумісності. Виявлено, що сучасні протоколи, такі як WireGuard та IKEv2/IPsec, забезпечують високу швидкість і безпеку, тоді як застарілі, наприклад PPTP, втрачають актуальність через низький рівень захисту.

Таким чином, перший розділ заклав теоретичну основу для розуміння ключових аспектів побудови безпечних корпоративних мереж за допомогою VPN-технологій. Це створило базу для подальших практичних досліджень та реалізації ефективних рішень для інтеграції, захисту та оптимізації корпоративної мережевої інфраструктури.

РОЗДІЛ 2 РОЗГОРТАННЯ ТЕСТОВОГО ЛАБОРАТОРНОГО СЕРЕДОВИЩА

Налаштування тестового лабораторного середовища є важливим етапом для моделювання та перевірки функціонування корпоративної VPN мережі. Це середовище дозволить імітувати роботу основних компонентів корпоративної інфраструктури, оцінити ефективність застосованих рішень, перевіряти політики безпеки. У цьому розділі описано етапи створення тестового середовища, його архітектуру та ключові компоненти [15] [16].

2.1 Схема лабораторного середовища

Схема лабораторного середовища ілюструє процес побудови захищеного зв’язку між головним офісом та віддаленою філією за допомогою VPN-технологій. Для цього використано протокол WireGuard у конфігурації Site-to-Site VPN, що забезпечує надійне шифрування та високу продуктивність передачі даних через публічний Інтернет. Лабораторне середовище відображає реальну корпоративну мережу з усіма необхідними компонентами, включаючи маршрутизатори, сервери, робочі станції та сегментовані мережі.

Ця модель дозволяє проводити тестування VPN-рішень, перевіряти доступність корпоративних ресурсів, а також аналізувати продуктивність і безпеку з’єднань у різних сценаріях. Випробування такого середовища є важливим кроком перед впровадженням технологій у реальну корпоративну інфраструктуру.

На рисунку 2.1 показано тестове лабораторне середовище побудоване для моделювання корпоративної мережі з можливістю забезпечення безпечного віддаленого доступу через VPN.

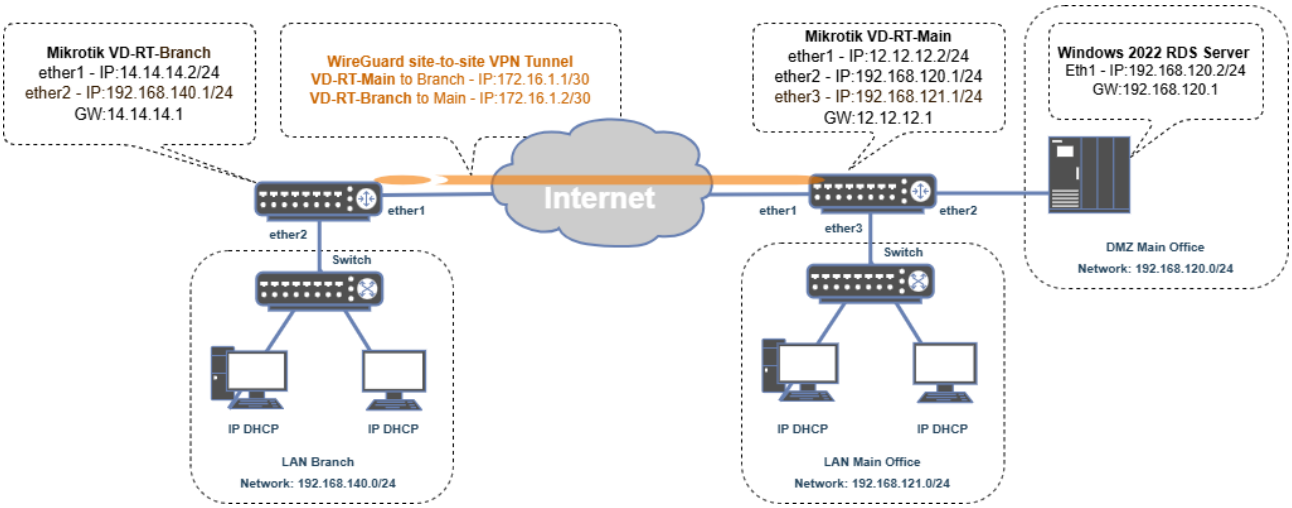

Рисунок 2.1 – Схема тестового лабораторного середовища

Схема лабораторного середовища ілюструє структуру тестування VPN-рішень з використанням протоколу WireGuard у конфігурації Site-to-Site VPN. У цьому середовищі налаштовано дві основні мережі: LAN Main Office (головний офіс) і LAN Branch (віддалена філія), які з'єднані через публічний Інтернет за допомогою зашифрованого тунелю WireGuard. Основною метою цієї конфігурації є забезпечення безпечного з'єднання між двома офісами, що дозволяє передавати дані без ризику їхнього перехоплення.

У головному офісі встановлено маршрутизатор Mikrotik (VD-RT-Main), який виконує роль VPN-шлюзу.

На цьому маршрутизаторі налаштовано інтерфейси:

– ether1 з IP-адресою 12.12.12.2/24, який підключений до Інтернету;

– ether2 з локальною IP-адресою 192.168.120.1/24, який з'єднаний із сервером Windows 2022 RDS;

– ether3 для підключення до локальної мережі офісу (192.168.121.0/24).

Сервер Windows 2022 RDS, розташований у зоні DMZ, має IP-адресу 192.168.120.2 і забезпечує віддалений доступ до корпоративних ресурсів для працівників.

У віддаленій філії розгорнуто маршрутизатор Mikrotik (VD-RT-Branch) із схожою конфігурацією. Інтерфейс ether1 має IP-адресу 14.14.14.2/24 для підключення до Інтернету, а ether2 обслуговує локальну мережу філії (192.168.140.0/24).

З’єднання між головним офісом і віддаленою філією реалізоване через WireGuard Site-to-Site VPN. Тунель має наступну конфігурацію: VD-RT-Main призначено IP-адресу 172.16.1.1/30, а VD-RT-Branch – IP-адресу 172.16.1.2/30. Це забезпечує безпечний обмін даними між двома офісами через Інтернет.

На кожному маршрутизаторі налаштовані правила брандмауера, які забезпечують фільтрацію трафіку і додатковий захист мережі. У локальних мережах використовується DHCP для автоматичного призначення IP-адрес клієнтським пристроям, що спрощує адміністрування мережі.

Ця лабораторна конфігурація дозволяє тестувати роботу VPN-тунелю, перевіряти доступність корпоративних ресурсів, таких як сервер RDS, із локальної мережі філії, а також виявляти можливі проблеми в налаштуваннях безпеки чи продуктивності. Схема забезпечує надійний і реалістичний сценарій для оцінки ефективності VPN-рішень у корпоративному середовищі.

2.2 Маршрутизатор Mikrotik

Mikrotik - це компанія, яка спеціалізується на створенні мережевого обладнання та програмного забезпечення, відомого своєю гнучкістю, функціональністю та доступністю [17]. Вона пропонує широкий спектр продуктів, які підходять як для малого бізнесу, так і для великих корпоративних мереж. Основним елементом продуктів Mikrotik є операційна система RouterOS, яка забезпечує багатий набір функцій для управління мережею.

RouterOS є потужною платформою, яка підтримує маршрутизацію, налаштування VPN, управління брандмауером, фільтрацію трафіку, VLAN, а також моніторинг і контроль якості обслуговування (QoS). Вона дозволяє налаштовувати як статичну, так і динамічну маршрутизацію, використовуючи протоколи OSPF, BGP і RIP. Завдяки вбудованій підтримці VPN-протоколів, таких як WireGuard, L2TP/IPsec, OpenVPN і SSTP, Mikrotik забезпечує захищений доступ до мережевих ресурсів і передачу даних через публічні мережі.

Апаратне забезпечення Mikrotik охоплює широкий спектр рішень, включаючи маршрутизатори серії RouterBOARD, високопродуктивні Cloud Core Router (CCR) і компактні точки доступу для домашнього використання. Крім того, компанія пропонує CHR, який дозволяє використовувати RouterOS у віртуалізованих середовищах, таких як VMware або Hyper-V. Це робить Mikrotik ідеальним для організацій, які використовують хмарні технології.

Однією з головних переваг Mikrotik є його підтримка широкого спектра інструментів для моніторингу і налаштування. Інтерфейс управління включає графічну програму WinBox [18], веб-інтерфейс, текстову консоль CLI, а також API для автоматизації задач. Це забезпечує високу гнучкість і дозволяє адміністраторам обирати зручний спосіб роботи з пристроями. Крім того, Mikrotik підтримує інструменти для аналізу трафіку.

На рисунку 2.2 показано інтерфейс програми WinBox, яка використовується для управління маршрутизаторами Mikrotik через графічний інтерфейс.

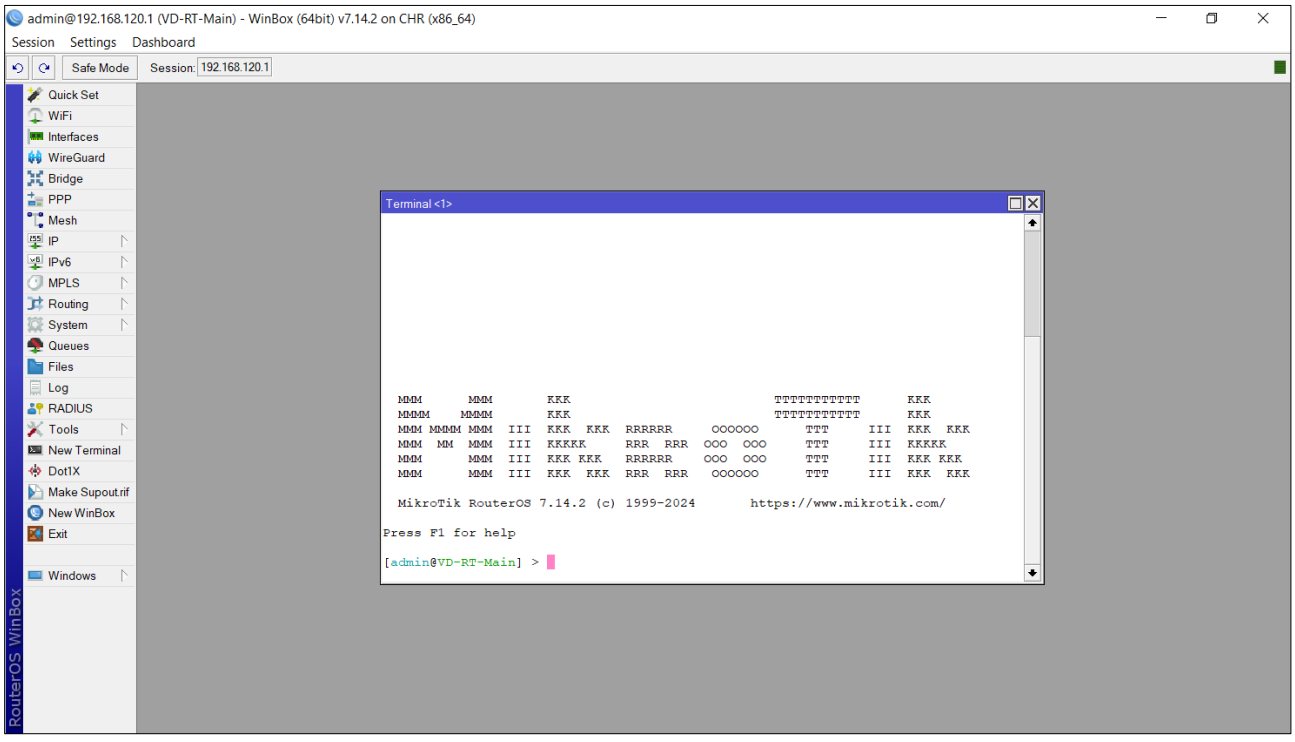

Рисунок 2.2 – Інтерфейс графічного управління Mikrotik

Інтерфейс WinBox дозволяє користувачеві виконувати налаштування як через графічний інтерфейс, так і через текстові команди. Це зручно для

адміністраторів, які віддають перевагу різним способам управління. Завдяки своїй інтуїтивній структурі WinBox полегшує доступ до складних функцій RouterOS, таких як VPN, брандмауери, моніторинг трафіку та управління користувачами. Це робить його основним інструментом для роботи з маршрутизаторами Mikrotik.

Mikrotik відзначається масштабованістю, що дозволяє використовувати його обладнання як у малих мережах, так і у великих корпоративних інфраструктурах. Завдяки підтримці багатопроцесорної архітектури та можливості роботи у віртуалізованих середовищах, пристрої Mikrotik здатні обробляти великі обсяги трафіку з мінімальними затримками. Вбудовані функції, такі як QoS, дозволяють пріоритизувати трафік, забезпечуючи стабільну роботу критично важливих додатків.

Брандмауер у RouterOS [19] надає розширені можливості для захисту мережі, включаючи фільтрацію пакетів, перенаправлення портів і контроль доступу до ресурсів. Це дозволяє забезпечити високий рівень безпеки, необхідний у сучасних умовах, коли кіберзагрози постійно еволюціонують. Продукти Mikrotik також відомі своєю економічністю. Вони пропонують функціональність, яка зазвичай доступна в дорожчому обладнанні, за значно нижчою ціною.

Велика кількість налаштувань і параметрів може бути перевагою для професіоналів, але для тих, хто не має достатнього досвіду, це може стати викликом.

Mikrotik є універсальним і потужним рішенням для побудови мереж різної складності. Його багатофункціональність, висока продуктивність і доступна вартість роблять його ідеальним вибором для організацій, які шукають ефективні способи забезпечення комунікації, безпеки і управління мережею. Завдяки постійним оновленням RouterOS і підтримці, Mikrotik залишається одним із провідних рішень на ринку мережевого обладнання.

2.2.1 Налаштування маршрутизатора філії

На з рисунку 2.3 показано вкладку Interface List програми WinBox, яка використовується для управління інтерфейсами маршрутизатора Mikrotik філії.

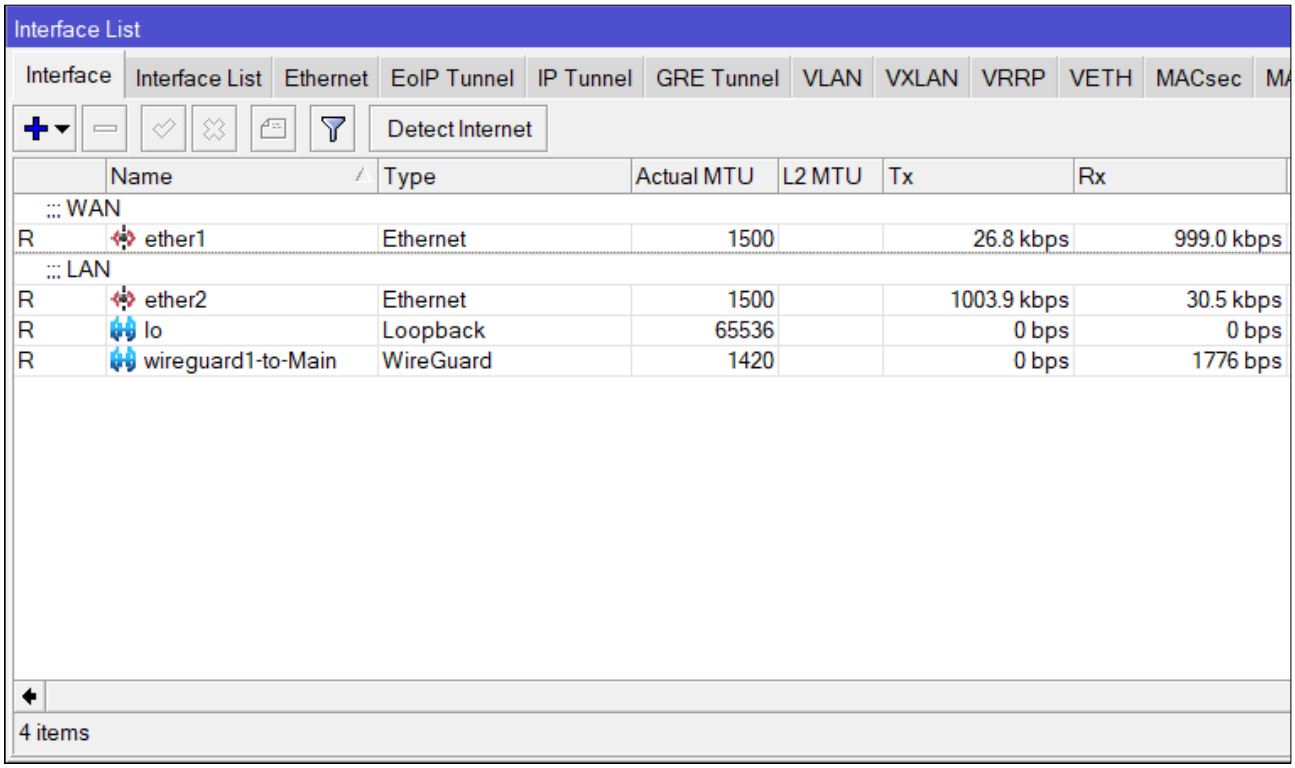

Рисунок 2.3 – Interface List маршрутизатора VD-RT-Branch

Інтерфейс ether1 позначений як WAN. Це Ethernet-інтерфейс, який використовується для підключення маршрутизатора до зовнішньої мережі. Інтерфейс ether2 позначений як LAN і використовується для локальної мережі. Це також Ethernet-інтерфейс. Інтерфейс lo є віртуальним інтерфейсом типу Loopback. Loopback використовується для внутрішньої комунікації маршрутизатора, наприклад, для тестування чи обслуговування. Інтерфейс wireguard1-to-Main позначений як WireGuard, що вказує на його використання для VPN-з'єднання.

На рисунку 2.4 представлено вкладку Address List програми WinBox, яка відображає IP-адреси, призначені різним інтерфейсам маршрутизатора Mikrotik.

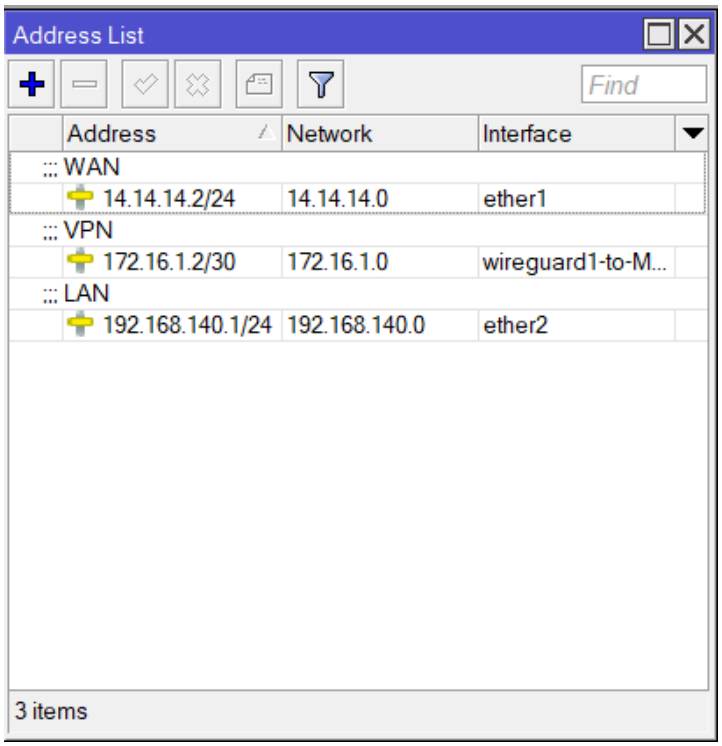

Рисунок 2.4 – Address List маршрутизатора VD-RT-Branch

Перша IP-адреса 14.14.14.2/24 прив’язана до інтерфейсу ether1, який позначений як WAN. Це публічна IP-адреса, яка використовується для підключення маршрутизатора до Інтернету. Цей інтерфейс забезпечує зв’язок із зовнішнім світом і є основним шлюзом для зовнішніх підключень. Друга IP-адреса 172.16.1.2/30 прив’язана до інтерфейсу wireguard1-to-Main, який є VPN-тунелем, налаштованим за допомогою протоколу WireGuard. Цей тунель забезпечує захищене з’єднання між маршрутизатором і віддаленим вузлом (головним офісом). Мережа з маскою /30 вказує на те, що вона використовується для Point-to-Point з’єднання між двома вузлами. Третя IP-адреса 192.168.140.1/24 прив’язана до інтерфейсу ether2, який використовується для локальної мережі (LAN). Цей інтерфейс виконує роль шлюзу для локальної мережі.

На рисунку 2.5 представлено вкладку Route List програми WinBox, яка відображає таблицю маршрутизації маршрутизатора Mikrotik.

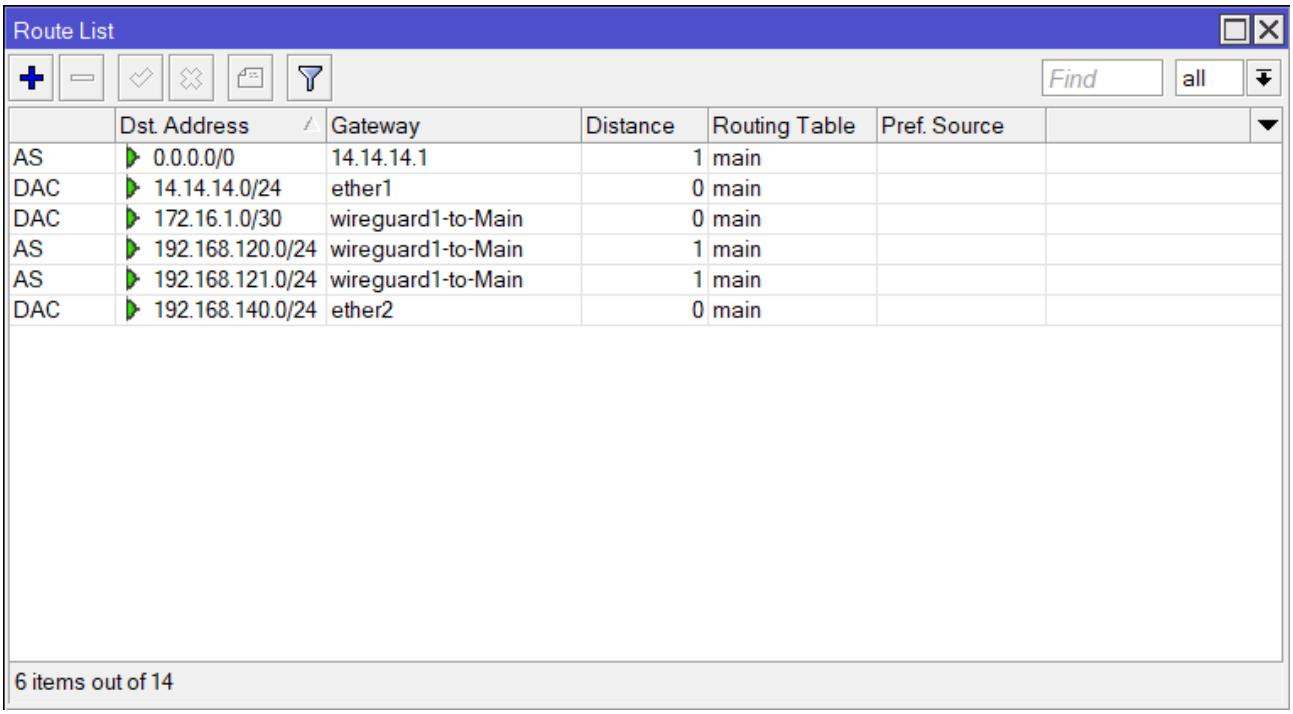

Рисунок 2.5 – Route List маршрутизатора VD-RT-Branch

У таблиці наведені маршрути, які вказують, як і куди маршрутизатор має передавати мережевий трафік.

Перше правило в таблиці - маршрут 0.0.0.0/0 (default route). Цей маршрут використовується для передачі трафіку до будь-якої мережі, яка не визначена в інших маршрутах таблиці. Шлюз для цього маршруту вказано як 14.14.14.1, що є зовнішнім шлюзом через інтерфейс ether1 (WAN). Це забезпечує вихід трафіку в Інтернет. Другий маршрут 14.14.14.0/24 автоматично доданий для локальної підмережі інтерфейсу ether1, який використовується для підключення до WAN. Маршрут має відстань (Distance) 0, що вказує на його високий пріоритет у таблиці маршрутизації. Третій маршрут 172.16.1.0/30 належить до VPN-з'єднання через інтерфейс wireguard1-to-Main. Це забезпечує передачу трафіку через захищений тунель WireGuard між локальним маршрутизатором і віддаленим вузлом. Відстань 0 свідчить про те, що маршрут безпосередньо пов'язаний із локальним інтерфейсом. Четвертий маршрут 192.168.120.0/24 також передає трафік через інтерфейс wireguard1-to-Main, що дозволяє доступ до цієї підмережі через VPN. Цей маршрут потрібен для передачі даних між локальною мережею та головним офісом. П'ятий маршрут 192.168.121.0/24 призначений для ще однієї підмережі, доступної через VPN. Він також

використовує інтерфейс wireguard1-to-Main, що забезпечує доступ до цієї мережі через зашифрований тунель. Усі маршрути через VPN мають відстань 1, що забезпечує їхній пріоритет при передачі трафіку. Шостий маршрут 192.168.140.0/24 пов’язаний із локальною мережею (LAN), яка використовує інтерфейс ether2. Цей маршрут додається автоматично для передачі трафіку між маршрутизатором і пристроями у локальній мережі.

Ця таблиця маршрутизації демонструє чітко налаштовану структуру мережі, яка забезпечує доступ до локальних мереж, з'єднання через VPN та вихід в Інтернет. Кожен маршрут оптимізований для відповідної підмережі чи точки призначення, що дозволяє ефективно розподіляти трафік між різними сегментами мережі. Маршрутизатор Mikrotik використовує ці маршрути для управління рухом даних, дотримуючись правил пріоритету, визначених у колонці Distance.

На рисунку 2.6 показана вкладка IP Pool програми WinBox, яка використовується для управління пулом IP-адрес, доступних для автоматичного призначення клієнтським пристроям через DHCP-сервер.

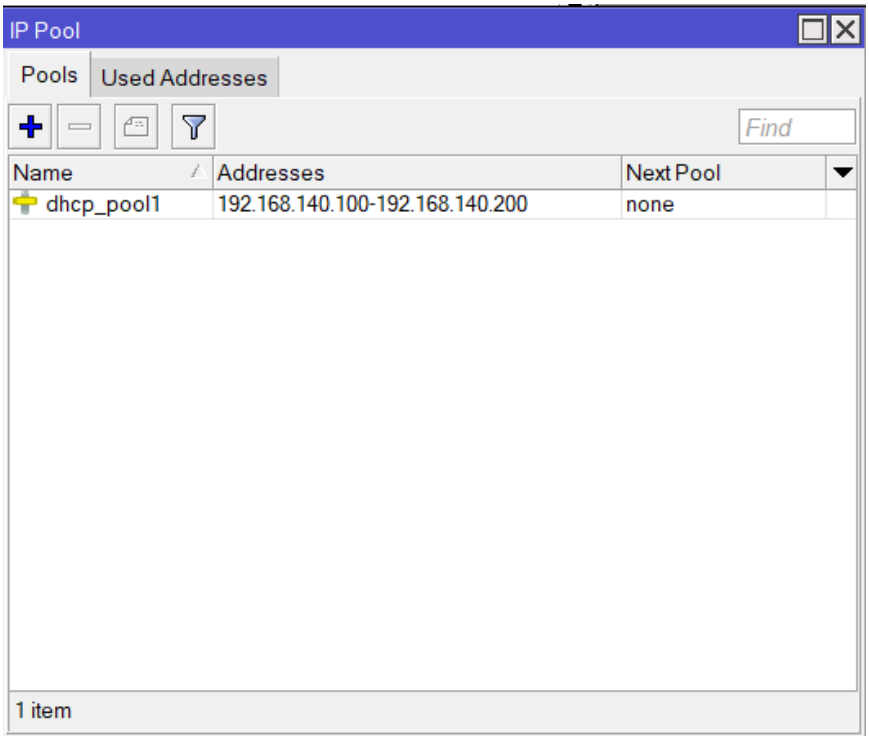

Рисунок 2.6 – IP Pool маршрутизатора VD-RT-Branch

У списку відображено один пул IP-адрес під назвою dhcp_pool1. Пул dhcp_pool1 включає діапазон адрес від 192.168.140.100 до 192.168.140.200. Цей діапазон використовується для автоматичного призначення IP-адрес клієнтським пристроям у локальній мережі, яка прив'язана до інтерфейсу з підмережею 192.168.140.0/24. Кожному пристрою в мережі, який запитує IP-адресу через DHCP, буде видано одну з адрес із цього діапазону. Ця конфігурація пулу є стандартною практикою для налаштування DHCP у локальних мережах. Вона забезпечує централізоване управління IP-адресами, запобігає конфліктам адрес і спрощує адміністрування мережі. Вказаний діапазон адрес зазвичай не включає IP-адресу шлюзу (192.168.140.1), яка використовується маршрутизатором, а також виключає майбутні статичні IP-адреси.

На рисунку 2.7 відображено налаштування DHCP-сервера в програмі WinBox на маршрутизаторі Mikrotik.

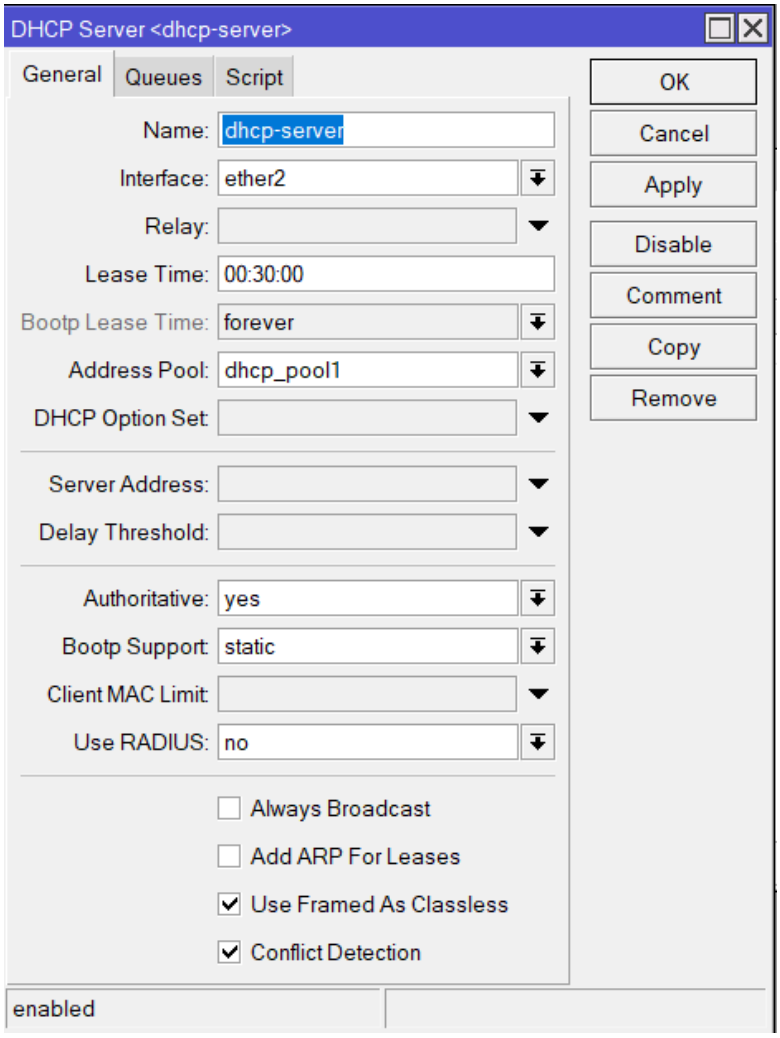

Рисунок 2.7 – Налаштування DHCP-сервера маршрутизатора VD-RT-Branch

DHCP-сервер прив’язаний до інтерфейсу ether2, який, згідно з попередньою інформацією, використовується для локальної мережі (LAN). Це означає, що DHCP-сервер буде обслуговувати клієнтів, підключених до цього інтерфейсу. Параметр Lease Time встановлено на 30 хвилин. Це означає, що IP-адреса, видана клієнту, залишатиметься зарезервованою за цим клієнтом протягом вказаного часу, після чого може бути перевидана іншому клієнту, якщо поточний не подасть запит на її продовження. Bootp Lease Time встановлено на "forever", що вказує на постійне збереження виданих адрес для клієнтів, які використовують BOOTP. Для призначення адрес DHCP-сервер використовує пул адрес dhcp_pool1, який містить діапазон IP-адрес, доступних для автоматичного розподілу. Це гарантує, що всі видані адреси будуть з цього пулу. Параметр Authoritative має значення yes, що означає, що цей DHCP-сервер є головним для зазначеного інтерфейсу. Усі запити клієнтів будуть оброблятися саме цим сервером, навіть якщо є інші DHCP-сервери. У розділі опцій увімкнено Use Framed As Classless, що вказує на використання сучасного методу обробки підмереж, і Conflict Detection, яка дозволяє виявляти конфлікти IP-адрес перед їх призначенням.

На рисунку 2.8 представлено налаштування параметрів DHCP у програмі WinBox.

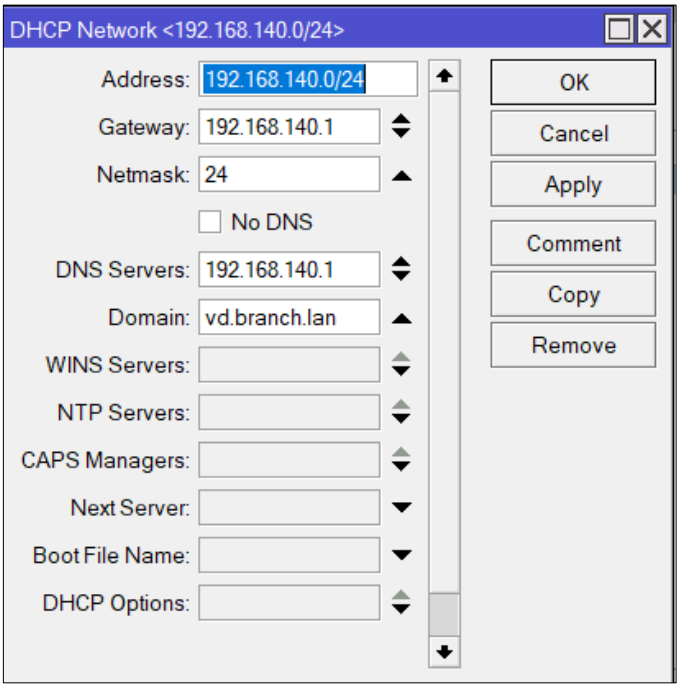

Рисунок 2.8 – Налаштування параметрів DHCP маршрутизатора VD-RT-Branch

Це налаштування визначає параметри, які DHCP-сервер використовує для автоматичної конфігурації клієнтських пристроїв у локальній мережі. Поле Address містить значення 192.168.140.0/24, яке визначає підмережу, для якої працює DHCP-сервер. Поле Gateway має значення 192.168.140.1. Це IP-адреса шлюзу, яка буде надана клієнтським пристроям. У цьому випадку маршрутизатор виконує роль шлюзу для підключення клієнтів до інших мереж, таких як Інтернет або VPN. Поле Netmask має значення 24, що відповідає стандартній масці для локальних мереж із 256 адресами (255.255.255.0). Ця маска використовується для визначення меж локальної мережі. Поле DNS Servers містить значення 192.168.140.1, що вказує на IP-адресу DNS-сервера, який використовується для перетворення доменних імен у IP-адреси. У цьому випадку маршрутизатор також виконує функцію DNS-сервера для клієнтів у локальній мережі. Поле Domain має значення vd.branch.lan, що задає доменне ім’я локальної мережі. Це корисно для ідентифікації мережі та полегшення роботи з внутрішніми DNS-запитами.

На рисунку 2.9 відображена вкладка Firewall у програмі WinBox, яка показує список правил брандмауера для маршрутизатора Mikrotik.

Ці правила визначають, як маршрутизатор обробляє вхідний трафік на різних рівнях і за різними критеріями. Правило з номером 0 має дію accept і стосується з'єднань у стані established (вже встановлених). Це означає, що трафік, який є частиною вже створеного з'єднання, буде дозволено. Правило з номером 1 також має дію accept і застосовується до з'єднань у стані related. Це дозволяє трафік, пов'язаний із уже дозволеним з'єднанням (наприклад, для FTP або інших протоколів, які створюють додаткові з'єднання). Правило з номером 2 має дію drop і застосовується до з'єднань у стані invalid. Це означає, що будь-який некоректний трафік, який не відповідає станам з'єднання, буде відхилено. Це правило забезпечує базовий рівень захисту від потенційно шкідливого трафіку.

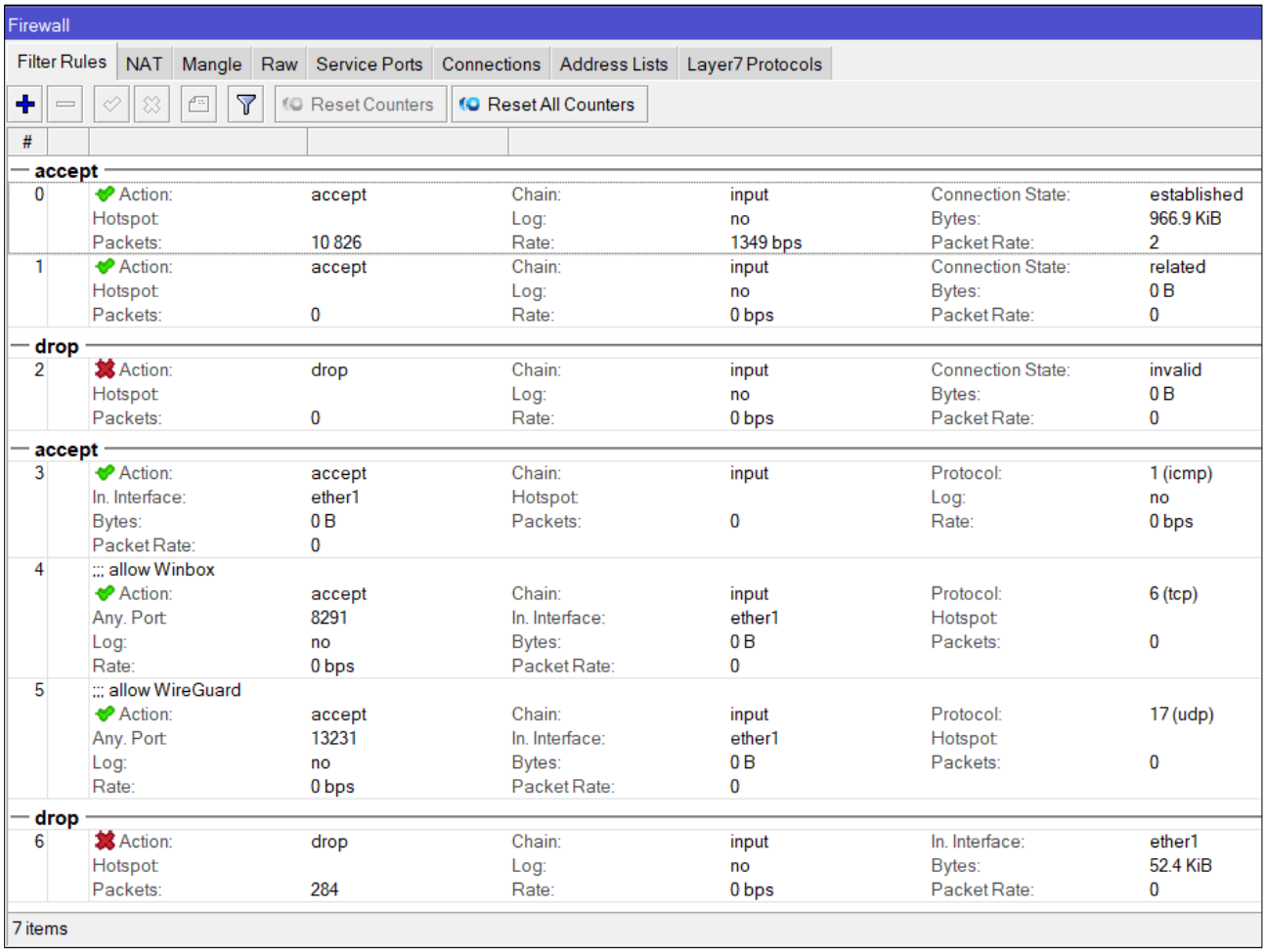

Рисунок 2.9 – Вкладка Firewall маршрутизатора VD-RT-Branch

Правило з номером 3 має дію accept і застосовується до вхідного ICMP трафіку через інтерфейс ether1. Правило з номером 4 має дію accept і дозволяє доступ до маршрутизатора через порт 8291 протоколу TCP. Цей порт використовується для управління маршрутизатором через WinBox. Це правило забезпечує доступ адміністратора до інтерфейсу управління. Правило з номером 5 має дію accept і дозволяє трафік через порт 13231 протоколу UDP. Це правило використовується для обробки VPN-з'єднань через WireGuard. Правило з номером 6 має дію drop і застосовується до вхідного трафіку через інтерфейс ether1. Це правило блокує весь решту трафік, який не відповідає попереднім правилам. Це створює додатковий рівень безпеки, відхиляючи будь-який небажаний трафік.

Ця конфігурація брандмауера забезпечує базовий захист мережі, дозволяє необхідний трафік для управління та VPN-з'єднань, і блокує потенційно

шкідливий або небажаний трафік. Всі правила виконуються послідовно, що дозволяє чітко контролювати потік даних.

На рисунку 2.10 показана вкладка NAT у програмі WinBox, яка відображає список правил для трансляції адрес на маршрутизаторі Mikrotik.

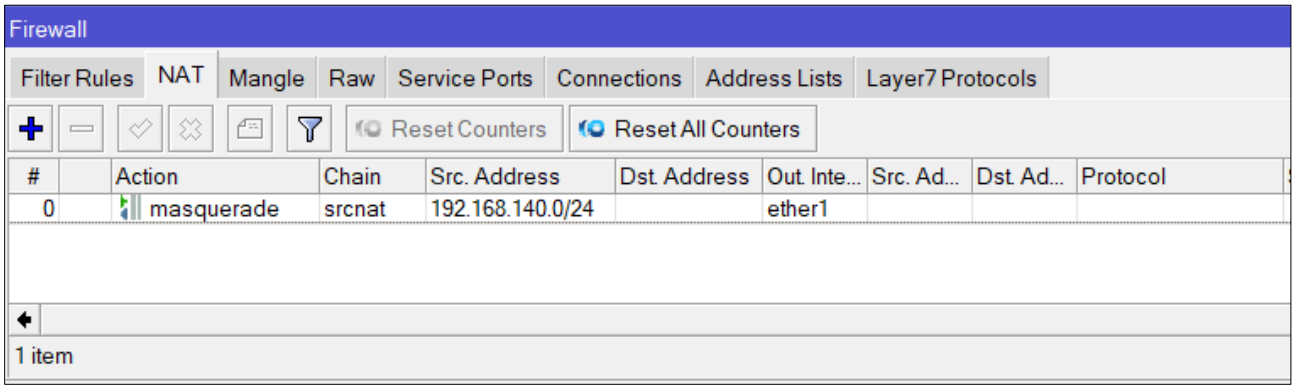

Рисунок 2.10 – Вкладка NAT маршрутизатора VD-RT-Branch

Дія masquerade означає, що для вихідного трафіку з локальної мережі маршрутизатор змінює IP-адресу джерела на свою власну зовнішню адресу (IP-адресу інтерфейсу WAN). Це забезпечує доступ пристроїв локальної мережі до зовнішніх ресурсів через один загальний зовнішній IP. Цей NAT використовується в ланцюзі srcnat (source NAT). Поле Src. Address має значення 192.168.140.0/24, що вказує на локальну підмережу, для якої застосовується це правило. Це означає, що всі пристрої в локальній мережі з IP-адресами в цьому діапазоні будуть підпадати під дію цього правила. Поле Out. Interface має значення ether1, що вказує на інтерфейс, через який трафік виходить у зовнішню мережу. Це гарантує, що правило NAT буде застосовуватися лише до трафіку, що виходить через цей інтерфейс.

На рисунку2.11 показано налаштування інтерфейсу WireGuard у програмі WinBox.

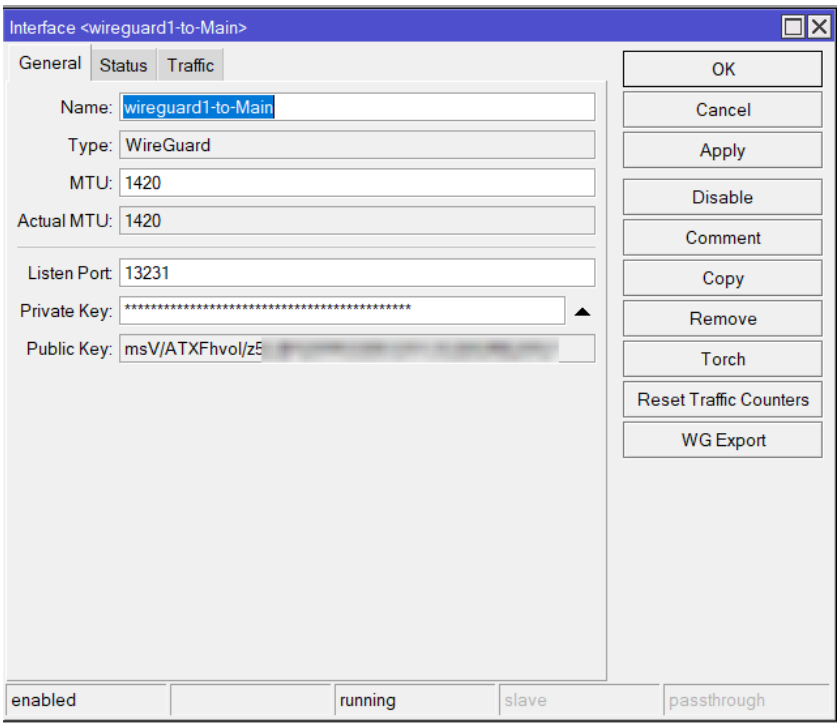

Рисунок 2.11 – Налаштування інтерфейсу WireGuard маршрутизатора VD-RT-Branch

Інтерфейс має назву wireguard1-to-Main і використовується для налаштування VPN-з'єднання через протокол WireGuard, що забезпечує швидкий і захищений тунель для передачі даних. Поле Type вказує, що це інтерфейс типу WireGuard. Це спеціалізований тип інтерфейсу для роботи з VPN-з'єднаннями, побудованими на цьому сучасному протоколі. Поле Listen Port встановлено на 13231, що означає, що інтерфейс прослуховує цей порт для вхідних VPN-з'єднань. Це дозволяє іншим пристроям встановлювати тунель із цим маршрутизатором через зазначений порт. Поле Private Key містить закритий ключ (захищений, тому на зображенні відображається лише маска), який використовується для автентифікації і шифрування трафіку. Цей ключ є унікальним для цього маршрутизатора і є критичним компонентом безпеки WireGuard-з'єднання. Поле Public Key відображає публічний ключ, який використовується для встановлення з'єднання з іншими вузлами. Інші пристрої, що підключаються до цього тунелю, використовують цей публічний ключ для аутентифікації.

На рисунку2.12 показано налаштування WireGuard Peer у програмі WinBox для інтерфейсу wireguard1-to-Main, що використовується для встановлення з'єднання між вузлами через протокол WireGuard.

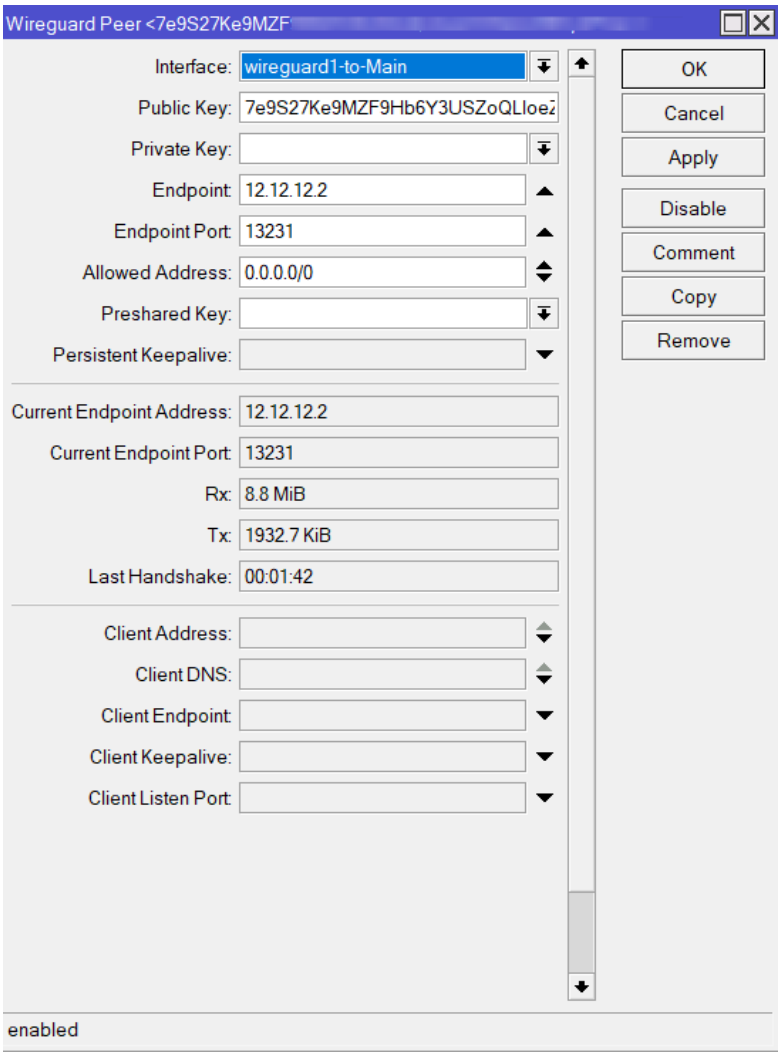

Рисунок 2.12 – Налаштування WireGuard Peer маршрутизатора VD-RT-Branch

Поле Interface вказує, що цей peer (вузол) прив’язаний до інтерфейсу wireguard1-to-Main, який вже налаштований для роботи з WireGuard. Поле Public Key містить публічний ключ віддаленого вузла, який використовується для автентифікації та встановлення шифрованого з'єднання. Це ключ, наданий віддаленим вузлом для обміну зашифрованим трафіком. Поле Endpoint містить IP-адресу 12.12.12.2, що вказує на адресу віддаленого вузла, з яким встановлюється тунель. Поле Endpoint Port має значення 13231, що є портом, на якому віддалений вузол слухає трафік для VPN-з'єднання. Поле Allowed Address

вказує значення 0.0.0.0/0, що означає, що весь трафік, який проходить через цей тунель, дозволений і спрямовується до віддаленого вузла. Це типово для налаштувань, коли весь трафік локальної мережі проходить через VPN.

2.2.2 Налаштування маршрутизатора головного офісу

На з рисунку 2.13 представлено список інтерфейсів маршрутизатора Mikrotik головного офісу.

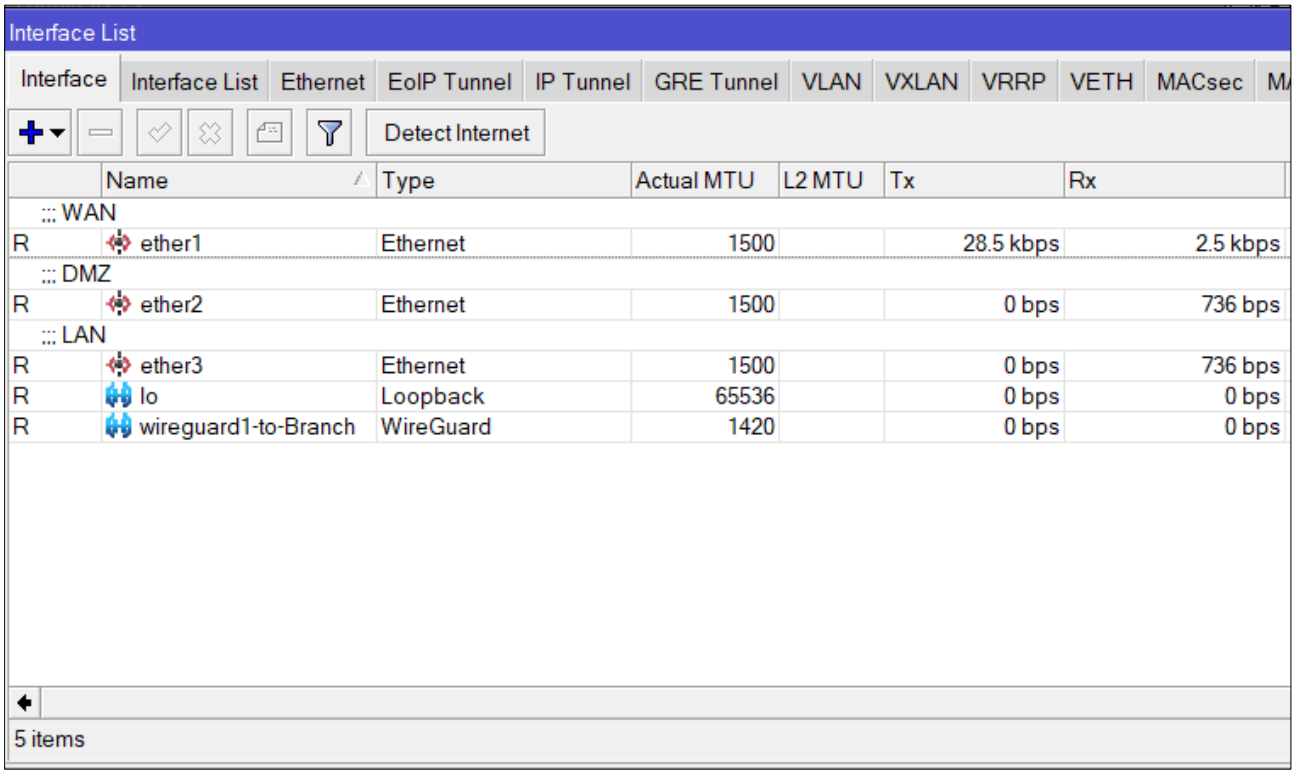

Рисунок 2.13 – Interface List маршрутизатора VD-RT-Main

Ця конфігурація демонструє призначення інтерфейсів для різних зон і завдань маршрутизатора. Інтерфейс WAN використовується для підключення до Інтернету, DMZ - для Windows Server 2022 RDS, LAN - для локальної мережі, а WireGuard - для захищеного з'єднання між вузлами через VPN.

На рисунку 2.14 відображена вкладка Address List у програмі WinBox, яка показує список IP-адрес, призначених інтерфейсам маршрутизатора Mikrotik.

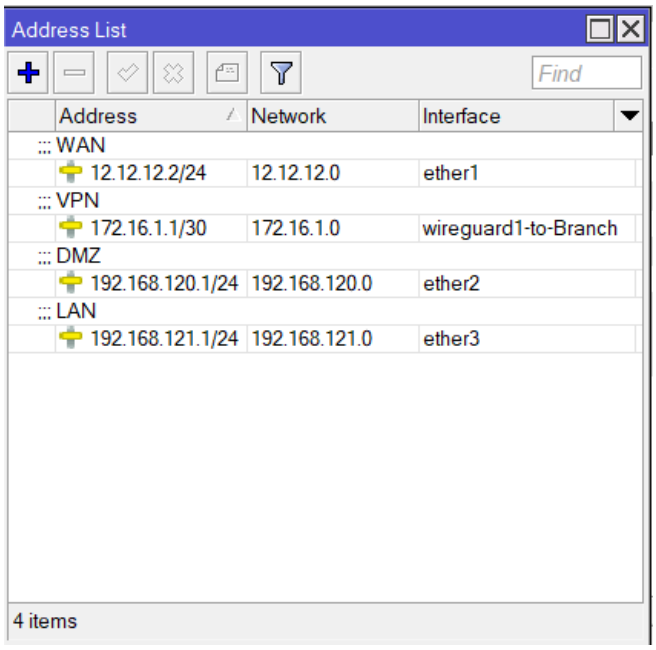

Рисунок 2.14 – Address List маршрутизатора VD-RT-Main

В налаштуваннях вказано IP-адресу, мережу, до якої вона належить, та інтерфейс, до якого вона прив’язана.

На рисунку 2.15 представлено вкладку Route List програми WinBox, яка відображає таблицю маршрутизації маршрутизатора Mikrotik.

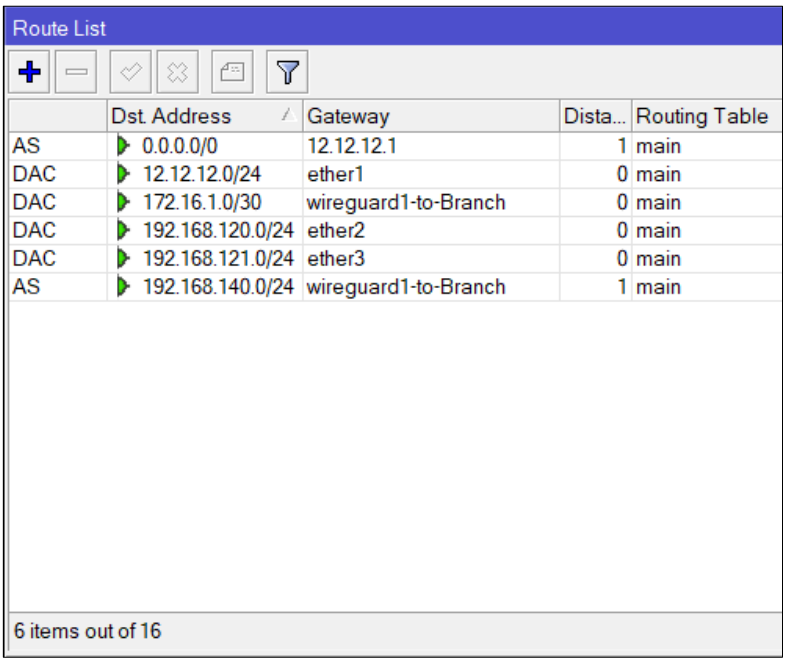

Рисунок 2.15 – Route List маршрутизатора VD-RT-Main

Ця конфігурація маршрутизації забезпечує чіткий розподіл трафіку між локальною мережею, DMZ, VPN-з'єднанням і зовнішньою мережею. Динамічні маршрути автоматично створюються відповідно до підключених інтерфейсів і мереж.

На рисунку 2.16 представлено налаштування пулу IP-адрес у вкладці IP Pool програми WinBox.

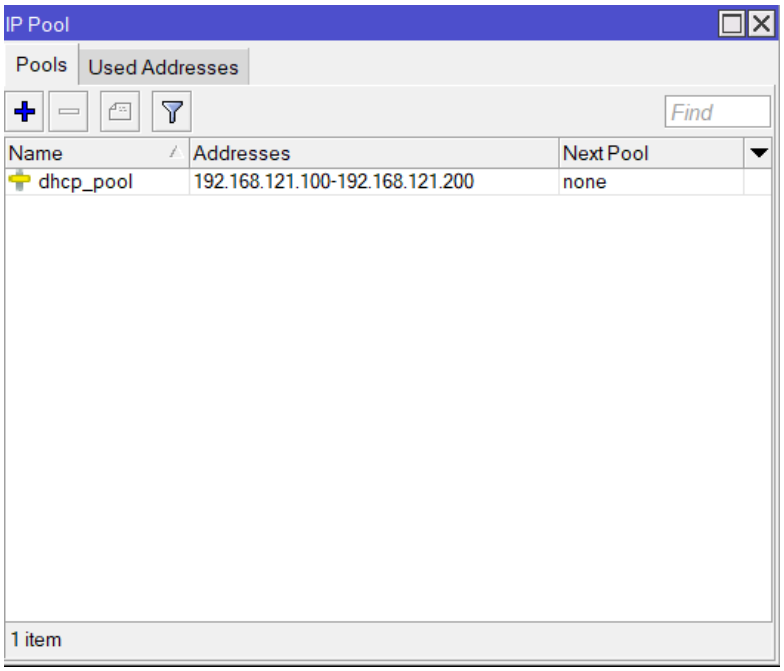

Рисунок 2.16 – IP Pool маршрутизатора VD-RT-Main

Цей пул використовується для автоматичної видачі IP-адрес клієнтам через DHCP-сервер у мережі. Ця конфігурація забезпечує ефективний розподіл IP-адрес серед пристроїв у локальній мережі, спрощуючи управління мережею та мінімізуючи потребу в ручному налаштуванні кожного пристрою. Пул є частиною підмережі 192.168.121.0/24, що відповідає адресі інтерфейсу LAN маршрутизатора, забезпечуючи сумісність і правильну маршрутизацію трафіку.

Налаштування брандмауера аналогічні, як на маршрутизаторі філії. Правила визначають, як маршрутизатор обробляє вхідний трафік на різних рівнях і за різними критеріями. Ця конфігурація брандмауера забезпечує базовий захист мережі, дозволяє необхідний трафік для управління та VPN-з'єднань, і блокує

потенційно шкідливий або небажаний трафік. NAT нат також налаштовано аналогічно, як на маршрутизаторі філії.

На рисунку 2.17 представлено налаштування інтерфейсу WireGuard під назвою wireguard1-to-Branch у програмі WinBox.

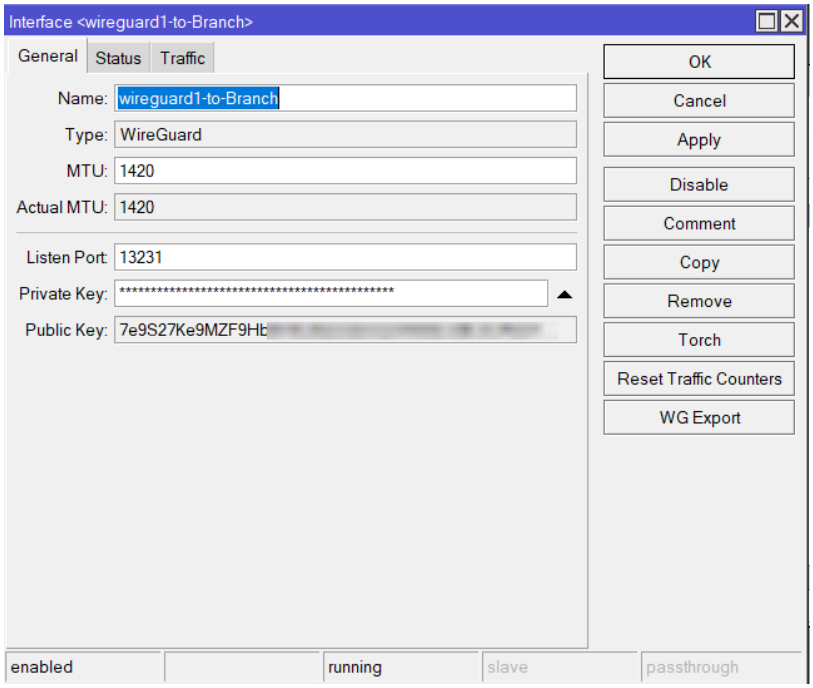

Рисунок 2.17 – Налаштування інтерфейсу WireGuard маршрутизатора VD-RT-Main

Цей інтерфейс використовується для організації VPN-з'єднання через протокол WireGuard між локальним маршрутизатором і віддаленою точкою (Branch). Інтерфейс має тип WireGuard, що означає, що він налаштований для роботи з сучасним VPN-протоколом, який забезпечує високу швидкість, безпеку та ефективність передачі даних. Максимальний розмір передаваного пакета (MTU) встановлено на значення 1420, яке є стандартним для WireGuard-з'єднань і забезпечує оптимальну передачу даних у межах VPN-тунелю. Поле Actual MTU також вказує на значення 1420, що підтверджує, що це налаштування успішно застосовано. Поле Listen Port містить значення 13231, яке визначає порт, на якому інтерфейс слухає вхідні підключення для VPN-з'єднання. Це порт, який використовується віддаленим вузлом для передачі даних через тунель. Поле Private Key відображає закритий ключ інтерфейсу, який використовується для

автентифікації та шифрування трафіку. Для забезпечення безпеки ключ замаскований. Поле Public Key містить публічний ключ, який використовується для автентифікації цього маршрутизатора іншими вузлами в тунелі WireGuard. Інші вузли використовують цей ключ для шифрування трафіку, адресованого до цього маршрутизатора. Статус інтерфейсу вказаний як enabled і running, що підтверджує його активність і готовність до передачі даних через VPN-з'єднання.

На рисунку2.18 показане налаштування WireGuard Peer для інтерфейсу wireguard1-to-Branch у програмі WinBox.

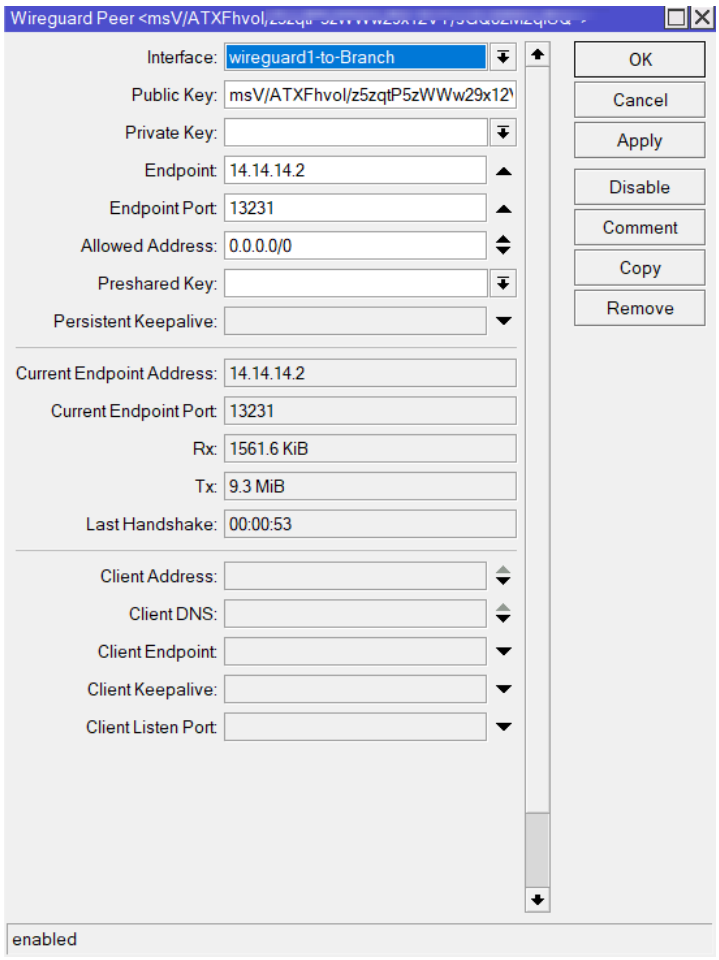

Рисунок 2.18 – Налаштування WireGuard Peer маршрутизатора VD-RT-Main

Поле Interface вказує, що цей Peer належить до інтерфейсу wireguard1-to-Branch, який відповідає за VPN-з’єднання між локальним маршрутизатором і віддаленим вузлом. Поле Public Key містить публічний ключ віддаленого вузла, який використовується для автентифікації та встановлення захищеного з'єднання. Цей ключ є унікальним і обов'язково повинен відповідати ключу,

наданому віддаленим вузлом. Поле Endpoint вказує IP-адресу 14.14.14.2, яка є адресою віддаленого вузла, з яким встановлюється VPN-з'єднання. Поле Endpoint Port має значення 13231, що є портом на віддаленому вузлі, через який встановлюється тунель WireGuard. Поле Allowed Address містить значення 0.0.0.0/0, що означає, що цей вузол дозволяє передавати весь трафік через VPN-тунель.

Ця конфігурація забезпечує ефективне та безпечне VPN-з’єднання через WireGuard, використовуючи сучасні криптографічні методи для забезпечення конфіденційності та цілісності переданих даних.

2.3 Налаштування Windows Server 2022 RDS

Windows Server 2022 - це потужна серверна операційна система, розроблена Microsoft, яка забезпечує високу продуктивність, безпеку та інтеграцію з сучасними хмарними технологіями [19]. Вона розроблена для використання в корпоративних середовищах, надаючи широкий спектр інструментів для управління інфраструктурою, сервісами та додатками. Windows Server 2022 пропонує розширені можливості безпеки, включаючи багаторівневий захист через функцію Secured-core server, підтримку протоколу TLS 1.3 та інтеграцію з Azure Defender для виявлення і запобігання кіберзагрозам. Операційна система підтримує сучасне апаратне забезпечення, здатна працювати з великими обсягами пам’яті та багатоядерними процесорами, що робить її ідеальною для обслуговування великих робочих навантажень. Операційна система також пропонує вдосконалення у віртуалізації завдяки Hyper-V, що забезпечує стабільну роботу віртуальних машин з високою продуктивністю та можливістю масштабування. Мережеві функції, такі як SMB over QUIC і Storage Replica, дозволяють забезпечити швидкий і захищений доступ до даних навіть у віддалених середовищах. Active Directory надає централізоване управління користувачами, групами та доступом до ресурсів, що спрощує управління мережею.

Windows Server 2022 підтримує роль Remote Desktop Services для віддаленого доступу до ресурсів і додатків, що робить її ідеальною для організації віддаленої роботи [20]. Завдяки інноваційним рішенням у сфері збереження даних, таким як Storage Spaces Direct і ReFS, система гарантує надійність, масштабованість та стійкість до збоїв. Це рішення підходить для підприємств, які прагнуть забезпечити стабільність, продуктивність і захист своєї IT-інфраструктури, інтегруючи її з сучасними хмарними технологіями.

На рисунку2.19 панель управління Server Manager для локального сервера під управлінням Windows Server 2022 Standard.

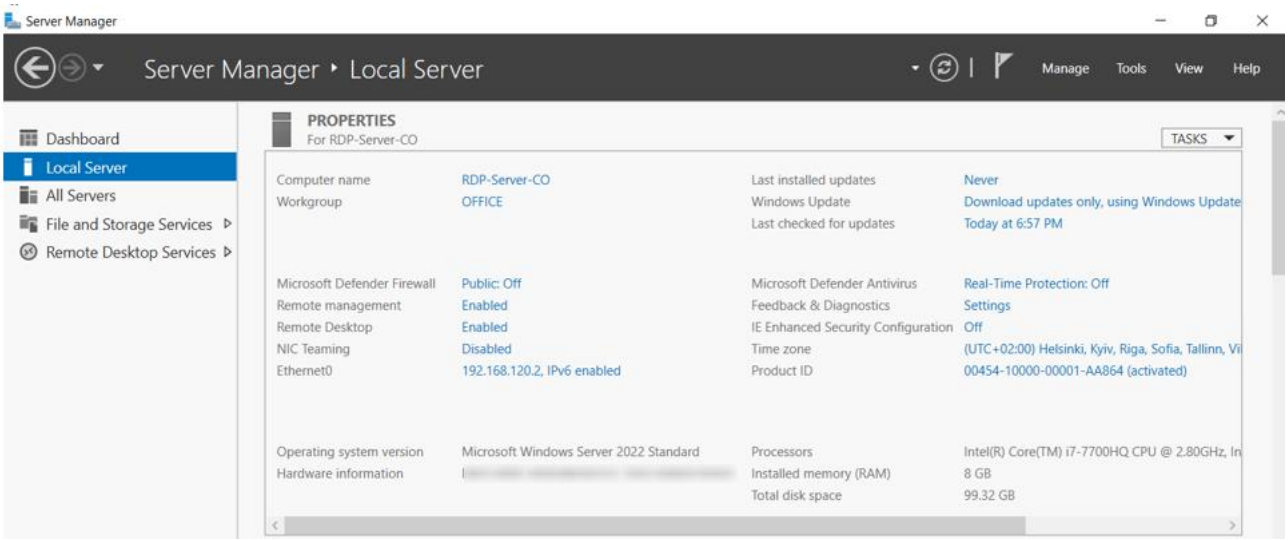

Рисунок 2.19 – Панель управління Server Manager

Сервер має ім'я RDP-Server-CO і знаходиться у робочій групі OFFICE. Microsoft Defender Firewall увімкнено, що забезпечує базовий захист від небажаних мережевих з'єднань. Remote Management також увімкнено, що дозволяє керувати сервером віддалено через інструменти Microsoft, такі як PowerShell чи Server Manager. Підтримка Remote Desktop активована, що дозволяє користувачам підключатися до сервера через протокол RDP. Основний мережевий інтерфейс Ethernet0 має IP-адресу 192.168.120.2.

На рисунку 2.20 представлено результат виконання команди Get-WindowsFeature у PowerShell, яка використовується для перевірки встановлених компонентів і ролей сервера.

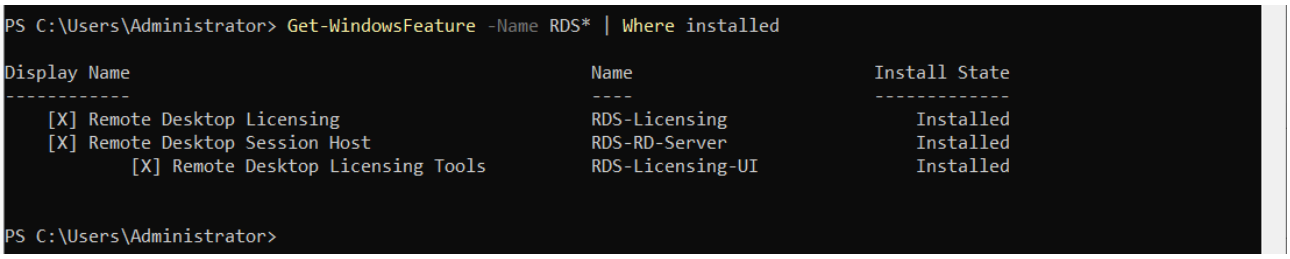

Рисунок 2.20 – Результат виконання команди Get-WindowsFeature у PowerShell

У даному випадку команда з параметром -Name RDS* відфільтровує лише функції, пов’язані з RDS, і показує встановлені компоненти. На сервері активовано три ключові функції, які забезпечують роботу сервісів віддаленого робочого столу (RDS). Встановлена роль Remote Desktop Licensing, яка відповідає за управління ліцензіями для користувачів та пристроїв, що підключаються через RDS. Наявність цього компонента дозволяє адмініструвати ліцензії, необхідні для роботи Remote Desktop Services відповідно до політики Microsoft. Роль Remote Desktop Session Host також встановлена, що свідчить про те, що сервер налаштований як хост сеансів віддаленого робочого столу. Ця роль дозволяє користувачам підключатися до серверу та виконувати завдання у віддаленому середовищі. Це особливо корисно для надання доступу до додатків або ресурсів компанії для співробітників, які працюють дистанційно. Також встановлений компонент Remote Desktop Licensing Tools, що включає інструменти для управління ліцензіями через графічний інтерфейс (RDS-Licensing-UI). Це забезпечує адміністраторам зручний доступ до налаштувань і управління RDS Licensing через відповідні графічні інтерфейси Windows Server.

Ці ролі та компоненти підтверджують, що сервер налаштований для підтримки віддалених підключень із забезпеченням ліцензування, і готовий до використання в середовищі, яке передбачає багатокористувацьку роботу через RDS. Інформація про стан встановлених компонентів (Installed) свідчить, що всі функції успішно активовані та доступні для використання.

На рисунку 2.21 представлено вивід команди Get-LocalUser у PowerShell, яка використовується для отримання інформації про користувачів на сервері.

```
PS C:\Users\Administrator> Get-LocalUser -Name  "daiana" | Select -Property *


AccountExpires         :
Description            :
Enabled                : True
FullName               : Daiana Vdovyna
PasswordChangeableDate : 1/11/2025 4:54:25 PM
PasswordExpires        :
UserMayChangePassword  : False
PasswordRequired       : True
PasswordLastSet        : 1/11/2025 4:54:25 PM
LastLogon              : 1/11/2025 5:51:05 PM
Name                   : daiana
SID                    : S-1-5-21-1629928194-966319733-2993158006-1001
PrincipalSource        : Local
ObjectClass            : User



PS C:\Users\Administrator>
```

Рисунок 2.21 – Результат виконання команди Get-LocalUser у PowerShell

У даному випадку команда запитує детальну інформацію про користувача з іменем daiana. Обліковий запис активний, що підтверджується параметром Enabled: True.

На рисунку 2.22 зображено PowerShell-скрипт, який виконує перевірку членства користувача в локальних групах на сервері.

```
PS C:\Users\Administrator> Get-LocalGroup | ForEach-Object {
>>
>>     $groupName = $_.Name
>>
>>     if ((Get-LocalGroupMember -Group $groupName | Where-Object {$_.Name -eq "RDP-SERVER-CO\daiana"})) {
>>
>>         $groupName
>>
>>     }
>>
>> }
Remote Desktop Users
Users
PS C:\Users\Administrator>
```

Рисунок 2.22 – Вивід груп користувача

Скрипт використовує командлет Get-LocalGroup для отримання списку всіх локальних груп. Результат виконання скрипта показує, що користувач RDP-SERVER-CO\daiana є членом двох груп: Remote Desktop Users та Users. Це свідчить про те, що обліковий запис має дозволи на підключення до сервера через RDS і належить до базової групи користувачів системи.

Windows Server 2022 повністю готовий до надання послуг RDS. Усі необхідні компоненти, включаючи Remote Desktop Session Host, Remote Desktop Licensing і Licensing Tools, встановлені та активні. Сервер налаштований для

роботи з віддаленими користувачами, що підтверджується присутністю облікового запису користувача в групі Remote Desktop Users, яка надає необхідні права для підключення через RDP. Конфігурація сервера виконана без помилок, а операційна система функціонує стабільно, забезпечуючи надійність і продуктивність.

2.4 Висновки до другого розділу

В другому розділі було детально описано процес розгортання тестового лабораторного середовища для налаштування корпоративної VPN-мережі. Середовище було спроєктовано таким чином, щоб максимально наблизити його до реальних умов корпоративної інфраструктури, включаючи сегментацію мереж, використання протоколу WireGuard для захищеного з'єднання між головним офісом і віддаленою філією, а також налаштування Windows Server 2022 для надання послуг віддаленого доступу через RDS. Було представлено архітектуру лабораторного середовища, що включає маршрутизатори Mikrotik, Windows Server 2022, робочі станції. Показано налаштування маршрутизації, брандмауера, NAT. У головному офісі та віддаленій філії було налаштовано VPN-тунель WireGuard із забезпеченням шифрування трафіку, що дозволить безпечно передавати дані між сегментами мережі через публічний Інтернет. Окрему увагу приділено налаштуванню DHCP-серверів, які забезпечують автоматичне призначення IP-адрес у локальних мережах, та брандмауерам, які забезпечують безпеку трафіку. Windows Server 2022 було налаштовано як хост для Remote Desktop Services, що дозволяє надавати віддалений доступ до корпоративних ресурсів через RDP. Встановлені ключові компоненти RDS, такі як Remote Desktop Licensing та Remote Desktop Session Host, гарантують готовність сервера до обслуговування віддалених користувачів. Проведені перевірки підтвердили, що сервер відповідає всім вимогам для стабільної роботи та безпеки.

Лабораторне середовище успішно налаштовано для тестування VPN-рішень, перевірки доступності корпоративних ресурсів та аналізу продуктивності з'єднань у різних сценаріях.

РОЗДІЛ 3 ТЕСТУВАННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ VPN МЕРЕЖІ

3.1 Тестування WireGuard site-to-site VPN

3.1.1 Маршрутизатор Mikrotik

Для перевірки роботи WireGuard Site-to-Site VPN між маршрутизаторами Mikrotik у головному офісі (VD-RT-Main) і віддаленій філії (VD-RT-Branch) було проведено тестування. WireGuard VPN був налаштований відповідно до схеми, в якій головний офіс має IP-адресу тунелю 172.16.1.1/30, а філія – 172.16.1.2/30. Для перевірки доступності тунелю між вузлами використовувалася команда ping на маршрутизаторі VD-RT-Main (див. рисунок 3.1).

На рисунку 3.1 показано вкладка Ping у програмі WinBox маршрутизатора Mikrotik, яка використовується для тестування доступності мережевих вузлів.

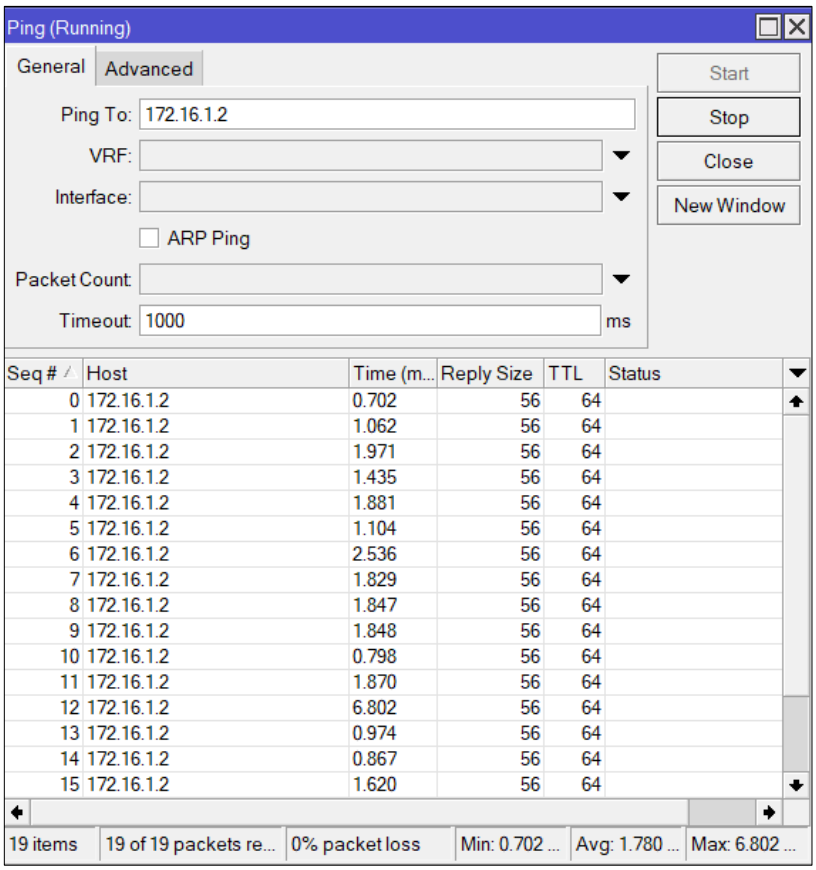

Рисунок 3.1 – Тест доступності IP-адресу тунелю 172.16.1.2

У полі Ping To вказана IP-адреса 172.16.1.2, що відповідає віддаленому вузлу у VPN-тунелі WireGuard. Результати тесту демонструють успішну передачу 7 пакетів, без втрат. Величина часу відповіді (Round Trip Time) коливається від 0.702 мс до 6.802 мс, із середнім значенням 1.780 мс. Це вказує на стабільне з’єднання з невеликою затримкою, що є очікуваним для тестування VPN-з'єднання в лабораторних умовах.

На рисунку 3.2 показано інструмент Traceroute маршрутизатора Mikrotik, який використовується для перевірки маршруту до до IP-адреси 192.168.120.1, яка є шлюзом для DMZ зони маршрутизатора Mikrotik у головному офісі.

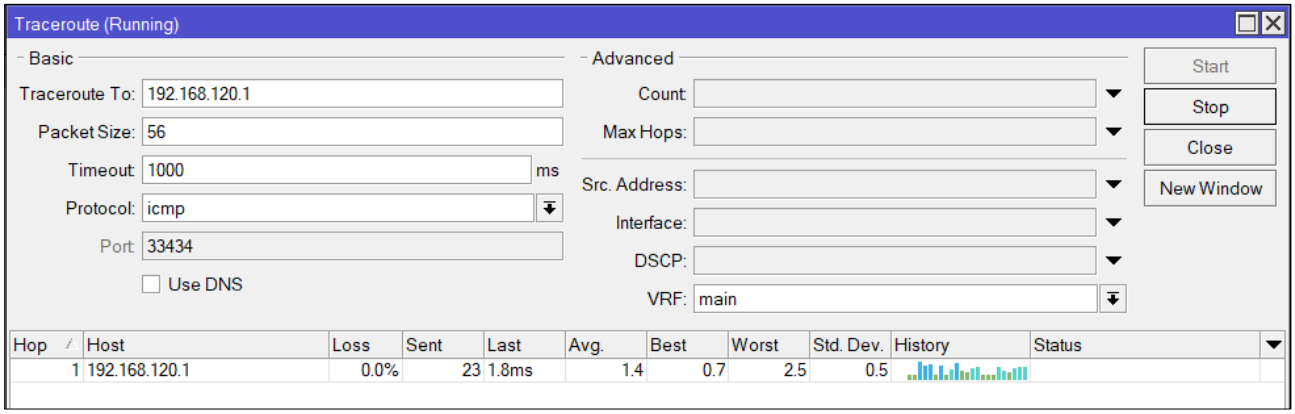

Рисунок 3.2 – Тест доступності IP-адресу 192.168.120.1

Результат виконання команди traceroute показує, що з’єднання до IP-адреси 192.168.120.1 досягається за один крок (Hop). Це вказує на те, що цільова IP-адреса коректно маршрутизується через VPN тунель. Поле Loss вказує на нульову втрату пакетів, що підтверджує надійність з’єднання. Цей результат підтверджує, що IP-адреса 192.168.120.1 є досяжною з маршрутизатора, а мережевий шлях не має жодних перешкод чи додаткових вузлів. Стабільна низька затримка підтверджує якість VPN тунелю.

На маршрутизаторах Mikrotik, які використовують протокол WireGuard, немає можливості вручну вказувати криптографічні параметри, такі як алгоритми шифрування або хешування. Це обумовлено особливістю самого протоколу WireGuard, який націлений на простоту, мінімалізм і максимальну безпеку завдяки жорстко заданим параметрам криптографії.

Основна концепція WireGuard полягає у використанні лише добре перевірених, ефективних і безпечних криптографічних механізмів, що робить протокол простим у використанні, а його реалізацію - стійкою до помилок.

WireGuard використовує ChaCha20, сучасний потоковий симетричний алгоритм шифрування, відомий своєю швидкістю і надійністю [21]. ChaCha20 забезпечує 256-бітну безпеку і працює швидше за AES на багатьох платформах, особливо там, де відсутні апаратні прискорювачі AES. ChaCha20 гарантує, що всі дані, які передаються через тунель, залишаються зашифрованими та недоступними для перехоплення.

Для забезпечення цілісності та автентичності даних використовується Poly1305, алгоритм аутентифікації повідомлень [22]. Він працює у парі з ChaCha20, перевіряючи, що дані не були змінені під час передачі. Poly1305 генерує криптографічний тег для кожного блоку даних, який перевіряється на стороні отримувача.

Для хешування ключів у WireGuard використовується BLAKE2s, який є швидким, безпечним і більш ефективним, ніж традиційні алгоритми, такі як SHA-256. BLAKE2s використовується для генерації ключів, автентифікації та забезпечення цілісності [23].

WireGuard використовує алгоритм обміну ключами на основі кривої Curve25519, яка забезпечує швидку та безпечну генерацію загальних секретних ключів [24]. Алгоритм забезпечує безпечний обмін ключами навіть через незахищені канали, завдяки своїм властивостям стійкості до атак.

Отже, на маршрутизаторах Mikrotik неможливо вказувати криптографічні параметри WireGuard, оскільки вони зафіксовані на рівні протоколу. Це рішення базується на принципах WireGuard, що спрямовані на простоту, безпеку та оптимальність. Всі з'єднання через WireGuard на Mikrotik автоматично відповідають найвищим сучасним стандартам криптографії, що робить цей протокол надійним вибором для Site-to-Site VPN.

3.1.2 Операційна система Windows

Наступний етап тестування передбачає перевірку функціональності VPN-з'єднання, налаштованого на маршрутизаторах Mikrotik філії та головного офісу з тестового комп’ютера з операційною системою Windows11, який розміщений в локальній мережі філії.

На рисунку 3.3 представлено вивід команди ipconfig для мережевого адаптера Ethernet0 комп’ютера в локальній мережі філії.

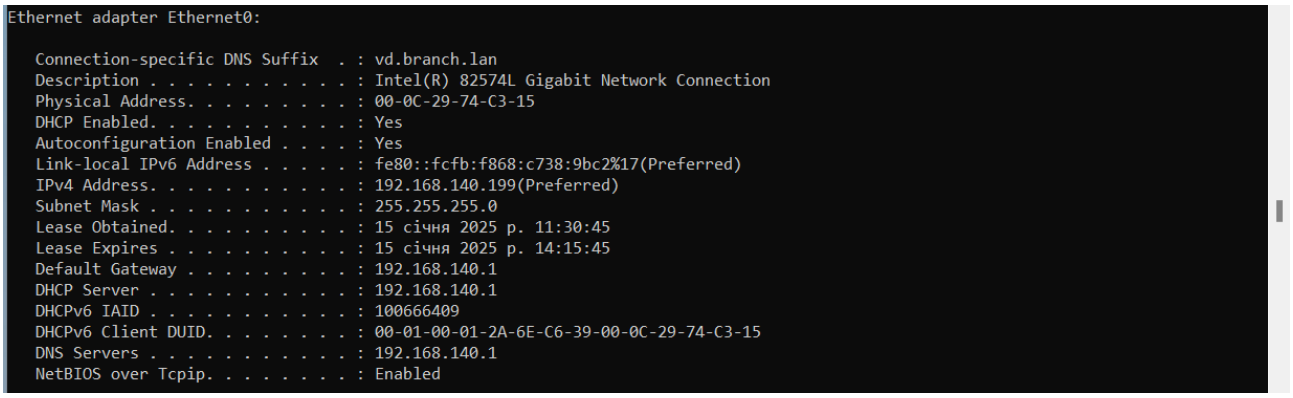

Рисунок 3.3 – Мережеві налаштування комп’ютера в локальній мережі філії

Конфігурація свідчить, що комп’ютер отримав мережеві параметри через DHCP-сервер, налаштований на маршрутизаторі Mikrotik у філії. Мережевий адаптер має IP-адресу 192.168.140.199 з маскою підмережі 255.255.255.0, що підтверджує належність пристрою до локальної мережі філії з підмережею 192.168.140.0/24. Шлюз за замовчуванням вказаний як 192.168.140.1, що відповідає IP-адресі інтерфейсу ether2 маршрутизатора Mikrotik у філії. Це підтверджує, що трафік з комп'ютера спрямовується через маршрутизатор для доступу до інших мереж. DHCP-сервер також має IP-адресу 192.168.140.1, що вказує на те, що маршрутизатор виконує роль DHCP-сервера в цій мережі. DNS-сервер встановлений як 192.168.140.1, що свідчить про те, що маршрутизатор також виконує роль DNS-проксі, перенаправляючи запити на зовнішні DNS-сервери.

Локальна мережа у філії повинна мати доступ до локальної мережі головного офісу та серверів DMZ через VPN тунель. Решту трафік через VPN тунель не проходить (див. рисунок 3.3).

На рисунку 3.4 відображено результати трасування до веб-сайту www.tntu.edu.ua із використанням програмного забезпечення PingPlotter Pro [25].

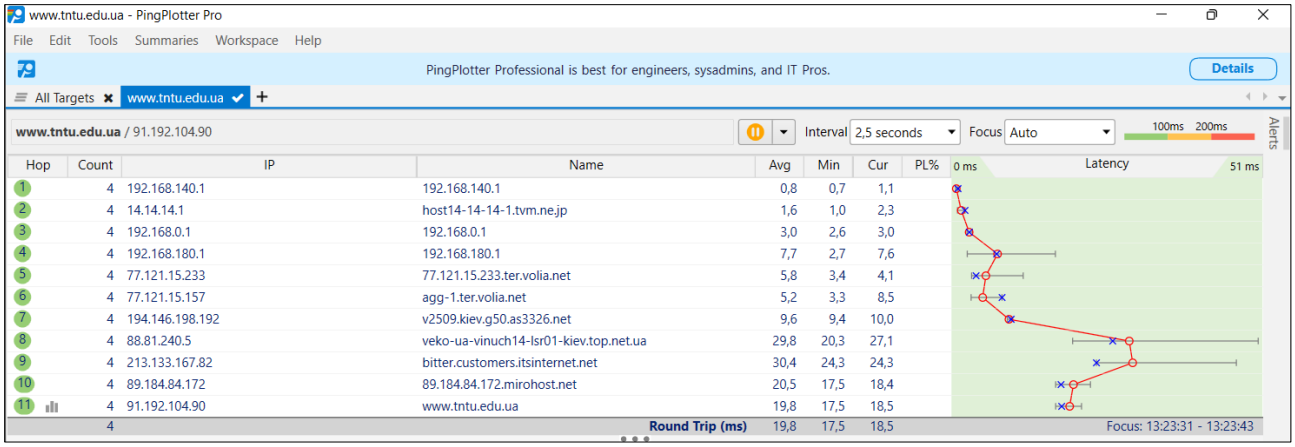

Рисунок 3.4 – Трасування маршруту до www.tntu.edu.ua

Цей інструмент дозволяє аналізувати маршрути пакунків через мережу до зазначеної IP-адреси 91.192.104.90, вимірюючи затримку (latency) на кожному вузлі маршруту. Вихідний IP-адрес локального пристрою - 192.168.140.1, що належить локальній мережі філії.

Результати тестування демонструють, що трафік не проходить через VPN тунель, налаштований між філією та головним офісом. Це підтверджується тим, що перший вузол маршруту (hop 1) - це шлюз локальної мережі філії (192.168.140.1), а подальші вузли маршруту показують передачу трафіку через зовнішню інфраструктуру провайдерів, починаючи з вузла 14.14.14.1, що відповідає шлюзу маршрутизатора філії.

Ця поведінка відповідає заданій конфігурації, де трафік, що направляється до зовнішніх ресурсів, таких як www.tntu.edu.ua, повинен проходити безпосередньо через WAN-з'єднання маршрутизатора філії, минаючи VPN-тунель. Таким чином, VPN використовується виключно для трафіку, що прямує до локальної мережі головного офісу або його DMZ.

Тест та рисунку 3.5 також підтверджує правильність налаштувань маршрутизації на маршрутизаторі Mikrotik філії.

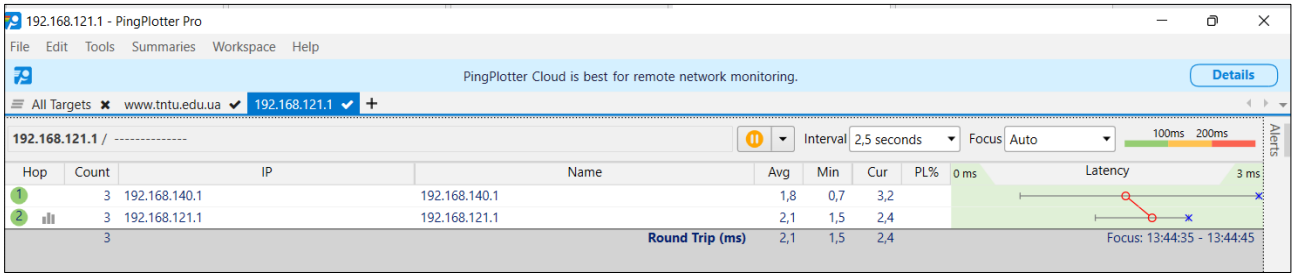

Рисунок 3.5 – Трасування маршруту до локальної мережі головного офісу

Згідно з таблицею маршрутизації, лише трафік, призначений для локальних мереж головного офісу або DMZ (192.168.120.0/24, 192.168.121.0/24), спрямовується через VPN-тунель. Усі інші запити, зокрема до зовнішніх веб-ресурсів, таких як www.tntu.edu.ua, проходять через WAN-інтерфейс без використання тунелю.

Результати трасування маршруту до IP-адреси 192.168.121.1, яка належить локальній мережі головного офісу, підтверджують, що трафік проходить через VPN тунель, налаштований між маршрутизаторами філії та головного офісу. Першим вузлом маршруту є IP-адреса шлюзу локальної мережі філії (192.168.140.1), що свідчить про коректну передачу даних від комп'ютера з операційною системою Windows через локальний шлюз. Другим вузлом є IP-адреса 192.168.121.1, яка відповідає шлюзу локальної мережі головного офісу. Це підтверджує, що трафік передається через VPN тунель між філією та головним офісом, оскільки VPN забезпечує прямий та захищений доступ до цієї підмережі. Жодні інші вузли маршруту, такі як зовнішні шлюзи або маршрутизатори провайдерів, у цьому випадку не залучаються, що є характерною ознакою використання VPN.

Ці результати демонструють коректну маршрутизацію трафіку через VPN тунель для доступу до локальної мережі головного офісу. Це підтверджує, що VPN забезпечує безпечний і прямий доступ до ресурсів головного офісу з локальної мережі філії.

Ця схема є типовою для Split Tunnel VPN, коли лише певний трафік передається через захищений тунель, а решта - напряму через зовнішній інтернет-шлюз, щоб уникнути зайвого навантаження на VPN і зменшити затримки для трафіку, який не потребує шифрування [26].

Ці тести підтверджують, що тунель WireGuard між маршрутизаторами VD-RT-Main і VD-RT-Branch працює стабільно, забезпечуючи передачу даних із невеликою затримкою і без втрат пакетів.

3.2 Тестування доступу до Windows Server 2022 RDS через VPN

На заключному етапі тестування перевіряється можливість встановлення віддаленого підключення до Windows Server 2022, розташованого у головному офісі, через протокол RDP з комп’ютерів локальної мережі філії. Сервер Windows Server 2022 у головному офісі, розташований у зоні DMZ, має роль RDS і доступний через протокол RDP.

Сервіс RDS у Windows Server є технологією, яка забезпечує доступ до робочих столів і додатків, що працюють на віддалених серверах. RDS дозволяє користувачам підключатися до серверів, використовувати їхні ресурси та працювати з додатками так, ніби вони встановлені на локальних пристроях. Основною метою сервісу є забезпечення централізованого доступу до корпоративних ресурсів із будь-якого місця, підвищення ефективності використання обчислювальних потужностей та оптимізація роботи організації. Сервіс RDS надає компаніям можливість централізувати обробку даних і зберігання інформації, що дозволяє знизити витрати на управління та обслуговування інфраструктури. Завдяки RDS користувачі можуть отримувати доступ до своїх робочих місць, додатків та корпоративних файлів із будь-якого пристрою, який підтримує клієнт RDP, забезпечуючи мобільність і продуктивність. Це робить RDS важливим інструментом для організацій, які впроваджують політику дистанційної роботи або намагаються зменшити залежність від фізичної інфраструктури.

RDS широко використовується в корпоративному середовищі для забезпечення доступу до бізнес-додатків і даних. Сервіс активно застосовується для організації робочих місць у віртуалізованих середовищах, де користувачі працюють на легких клієнтах, а обробка даних виконується на сервері. RDS також є ключовим компонентом хмарних сервісів, надаючи доступ до віртуальних робочих столів через платформи Microsoft Azure Virtual Desktop або інші аналогічні рішення.

З точки зору безпеки RDS забезпечує ізольоване середовище для роботи, де всі дані зберігаються на сервері, а не на локальних пристроях користувачів. Це зменшує ризики витоку інформації та полегшує дотримання політик безпеки. Додаткові функції, такі як підтримка багатофакторної аутентифікації, шифрування трафіку та інтеграція з Active Directory, роблять RDS надійним рішенням для захисту корпоративних ресурсів. Сервіс також підтримує масштабування, що дозволяє організаціям збільшувати або зменшувати кількість підключень залежно від потреб.

На рисунку 3.6 представлено результат трасування маршруту до Windows Server 2022, який розташований у головному офісі з IP-адресою 192.168.120.2.

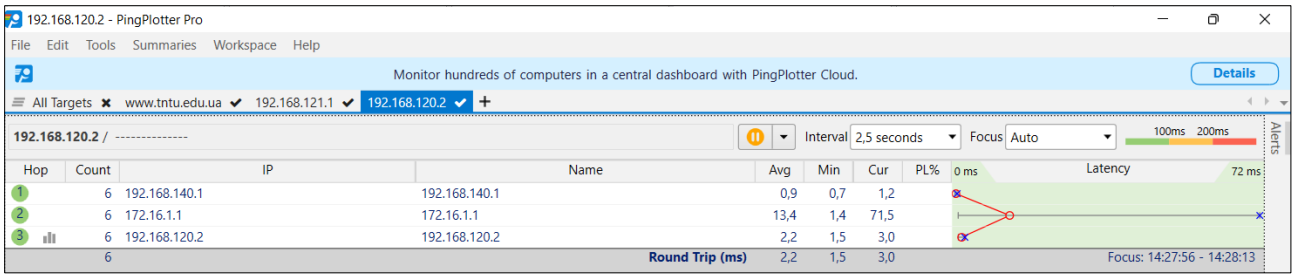

Рисунок 3.6 – Трасування маршруту до Windows Server 2022

Результати показують три вузли (hops), через які проходить трафік. Перший вузол має IP-адресу 192.168.140.1. Це локальний шлюз у мережі філії, який є інтерфейсом маршрутизатора Mikrotik філії. Другий вузол має IP-адресу 172.16.1.1. Це внутрішня IP-адреса тунелю WireGuard маршрутизатора головного офісу. Третій вузол має IP-адресу 192.168.120.2. Це сервер Windows Server 2022, який розташований у зоні DMZ головного офісу. Графік затримок

демонструють стабільну передачу даних із мінімальними затримками на всіх етапах. Зелений графік свідчить про відсутність втрати пакетів та низький рівень затримок, що підтверджує ефективність VPN-з'єднання.

Ці результати підтверджують, що комп'ютер із локальної мережі філії має доступ до сервера в головному офісі через VPN-тунель WireGuard.

На рисунку 3.7 демонструється успішне підключення до сервера Windows Server 2022 через протокол RDP із комп’ютера, розташованого в локальній мережі філії.

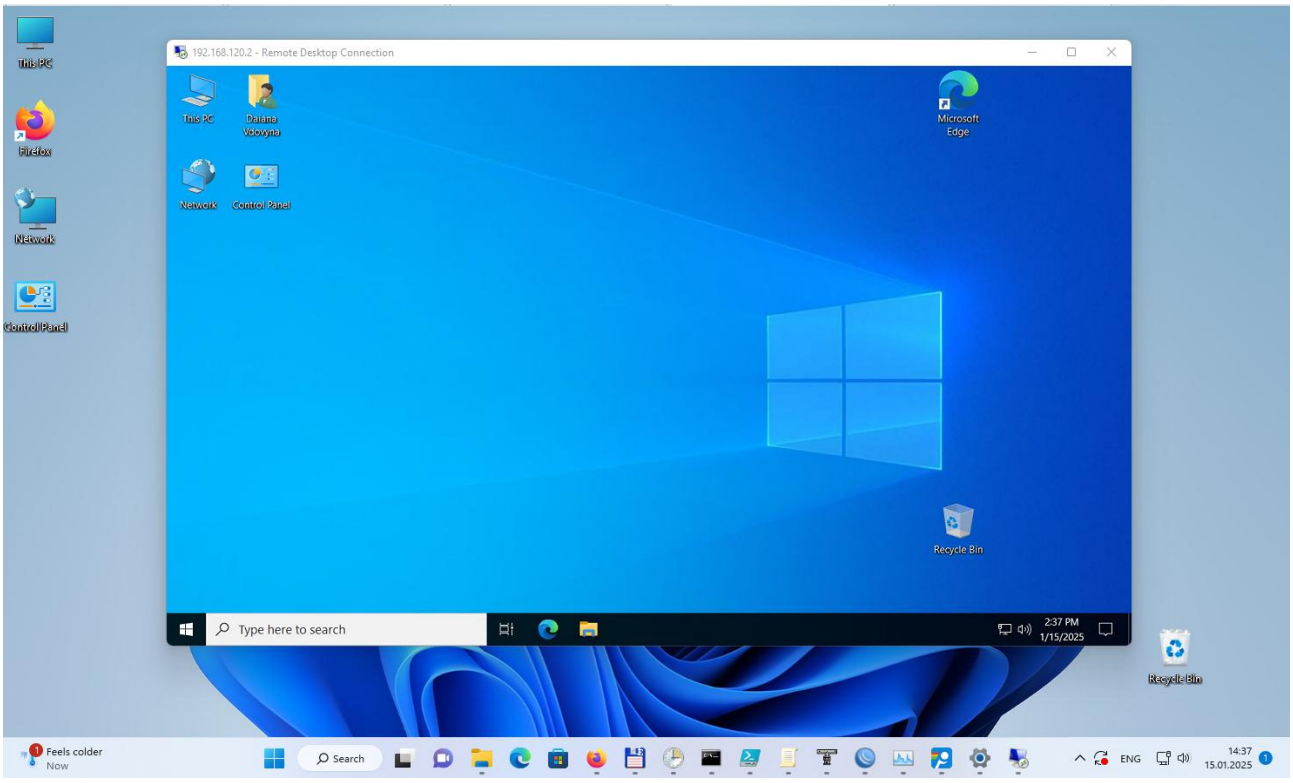

Рисунок 3.7 – Перевірка можливості підключення до Windows Server 2022 через RDP

Віддалений робочий стіл відображає інтерфейс сервера, включаючи робочий стіл із стандартними елементами. IP-адреса сервера, до якого здійснено підключення, 192.168.120.2, відповідає серверу, розташованому в зоні DMZ головного офісу. Успішне з'єднання свідчить про те, що тунель WireGuard, налаштований між маршрутизаторами філії та головного офісу, працює належним чином, забезпечуючи безпечний доступ до ресурсів головного офісу через зашифроване VPN-з'єднання.

Інтерфейс віддаленого робочого столу виглядає стабільним, без жодних ознак помилок чи проблем із продуктивністю. Це підтверджує, що мережеве з'єднання через VPN забезпечує необхідну якість для віддаленого доступу, включаючи низькі заримки і достатню пропускну здатність.

На рисунку 3.8 представлено інструмент Torch, який використовується на маршрутизаторі Mikrotik головного офісу для аналізу мережевого трафіку.

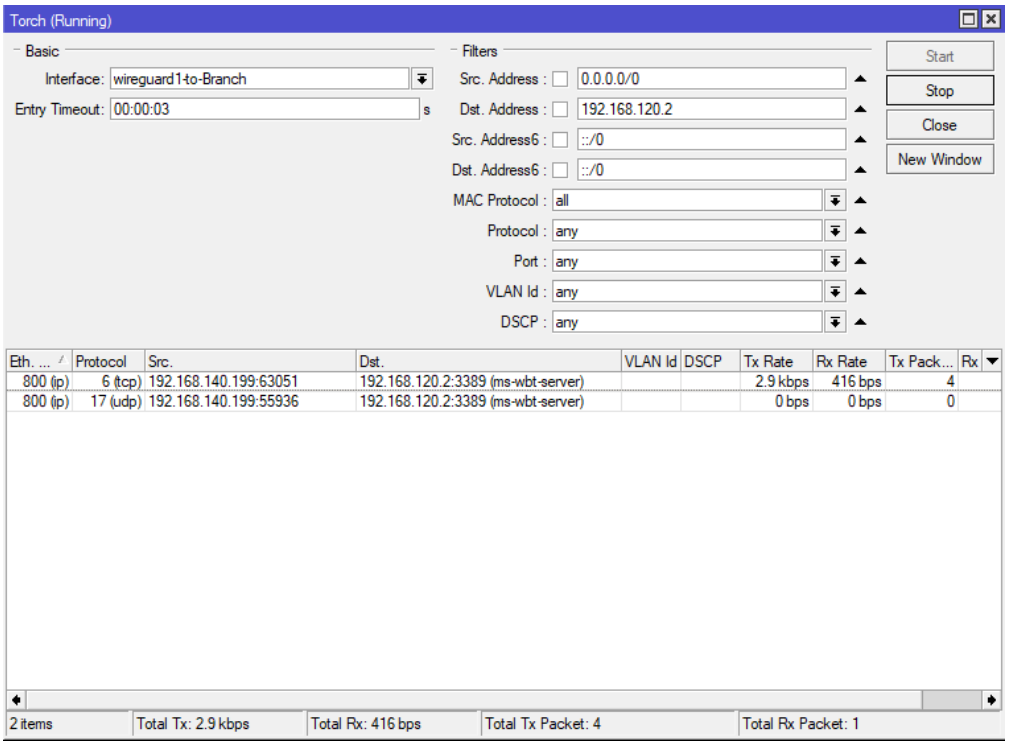

Рисунок 3.8 – Аналізу мережевого трафіку VPN тунелю

Torch запущений на інтерфейсі wireguard1-to-Branch, який є VPN-інтерфейсом, налаштованим для зв'язку між головним офісом та філією за допомогою WireGuard. Інструмент дозволяє відстежувати мережеву активність, фільтруючи трафік за різними параметрами, такими як джерело, призначення, протокол, порт і VLAN. У секції фільтрів вказано, що трафік аналізується з будь-якої IP-адреси до конкретного призначення 192.168.120.2. Це IP-адреса сервера, який розташований у зоні DMZ головного офісу. Сервер відповідає за обробку підключень по протоколу RDP, оскільки порт призначення 3389 асоційований із цим сервісом.

У таблиці результатів Torch видно два активних потоки трафіку. Перший потік використовує протокол TCP з IP-адреси 192.168.140.199 до сервера 192.168.120.2 на порту 3389. Другий запис у таблиці відображає протокол UDP із тими ж IP-адресами джерела та призначення, але наразі трафік у цьому потоці відсутній.

Ці дані свідчать про активну сесію RDP між клієнтом у філії та сервером у головному офісі через VPN-тунель WireGuard. Інструмент Torch дає можливість детально аналізувати мережевий трафік і виявляти особливості його маршрутизації, використовуючи фільтрацію за вказаними критеріями. У цьому випадку аналіз підтверджує, що передача даних для RDP-сесії проходить через захищений VPN-тунель.

Ці тести підтверджують, що VPN-з'єднання забезпечує повний доступ до серверних ресурсів головного офісу для користувачів із локальної мережі філії, що є необхідною умовою для виконання корпоративних завдань і використання ресурсів компанії через безпечний канал зв'язку.

3.3 Висновки до третього розділу

В третьому розділі було проведено комплексне тестування інформаційно-телекомунікаційної VPN мережі, побудованої на основі протоколу WireGuard для забезпечення захищеного з'єднання між головним офісом та віддаленою філією. Основним завданням тестування було перевірити функціональність і продуктивність VPN-з'єднання, налаштованого на маршрутизаторах Mikrotik, а також забезпечення доступу до корпоративних ресурсів через захищений тунель.

На першому етапі було протестовано WireGuard Site-to-Site VPN між маршрутизаторами головного офісу та філії. Тести доступності IP-адрес тунелю (ping) та маршрутизації (traceroute) підтвердили стабільність VPN-з'єднання, низьку затримку передачі даних та відсутність втрат пакетів. Конфігурація VPN, яка використовує WireGuard, забезпечила надійний зв’язок між локальними мережами обох офісів. На другому етапі проводилася перевірка роботи VPN-з'єднання з тестового комп’ютера, розташованого в локальній мережі філії, із

використанням операційної системи Windows 11. Конфігурація мережевого адаптера підтвердила коректну роботу DHCP-сервера на маршрутизаторі філії. Було підтверджено, що трафік, спрямований до підмереж головного офісу, коректно маршрутизується через VPN-тунель, тоді як решту трафік виходить напряму через WAN-інтерфейс маршрутизатора філії, відповідно до принципу Split Tunnel VPN. На заключному етапі тестування було перевірено доступ до Windows Server 2022, розташованого в зоні DMZ головного офісу, через протокол RDP. Успішне підключення до сервера з комп'ютера в локальній мережі філії підтвердило коректну роботу сервісу Remote Desktop Services через VPN-тунель WireGuard. Аналіз мережевого трафіку за допомогою інструменту Torch на маршрутизаторі головного офісу продемонстрував, що всі дані для RDP-сесії передаються через зашифрований VPN-тунель, забезпечуючи безпеку та конфіденційність передачі інформації.

Результати тестування підтвердили стабільність і надійність роботи WireGuard Site-to-Site VPN, а також відповідність налаштувань VPN сучасним вимогам безпеки. VPN-тунель забезпечує захищений доступ до ресурсів головного офісу для користувачів із філії, мінімізуючи ризики витоку даних і забезпечуючи продуктивну роботу корпоративної мережі. Таким чином, тестова VPN-мережа відповідає вимогам до корпоративного середовища та готова до впровадження в реальній інфраструктурі.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Значення адаптації в трудовому процесі

Праця людини безпосередньо пов’язана із виробничим середовищем. Працівник може нормально здійснювати трудову діяльність лише тоді, коли умови зовнішнього середовища відповідають оптимальним. Якщо вони змінюються, стають несприятливими, то на протидію їм організм людини включає спеціальний механізм, який зберігає постійність внутрішньою середовища, або змінює його в межах допустимого. Такий механізм називається адаптацією. Адаптація є важливим засобом попередження травмування, виникнення нещасних випадків у трудовому процесі і відіграє значну роль в охороні праці [27].

Адаптація – це динамічний процес пристосування організму та його органів до мінливих умов зовнішнього середовища.

Адаптація в трудовій діяльності поділяється на фізіологічну, психічну, соціальну та професійну.

Фізіологічна адаптація – це сукупність фізіологічних реакцій, які є в основі пристосування організму до змін зовнішніх умов, і направлені на збереження відносної постійності його внутрішнього середовища – гомеостазу.

Гомеостаз – це відносна динамічна постійність складу та властивостей внутрішнього середовища і стійкість основних фізіологічних функцій організму людини. Гомеостаз в організмі підтримується на усіх рівнях його організації і забезпечує динамічну рівновагу організму і зовнішнього середовища.

Суть механізму адаптації полягає у змінах меж чутливості аналізаторів, розширенні діапазону фізіологічних резервів організму та зміні в певних межах параметрів фізіологічних функцій. Завдяки фізіологічній адаптації фізичні та біохімічні параметри, які визначають життєдіяльність організму, змінюються у вузьких межах порівняно із значними змінами зовнішніх умов: підвищується стійкість організму до холоду, тепла, недостачі кисню, змін барометричного тиску та інших факторів. Велике значення у фізіологічній адаптації має

реактивність організму, його початковий функціональний стан (вік, тренованість тощо), в залежності від якого змінюються і відповідні реакції організму на різні дії. Процес фізіологічної адаптації до незвичайних, екстремальних умов проходить декілька стадій, або фаз: спочатку переважають явища декомпенсації (порушення функцій), потім неповного пристосування (активний пошук організмом стійких станів, що відповідають новим умовам середовища) і, нарешті, фаза відносного стійкого пристосування.

Фізіологічна адаптація до праці має активний характер і за сприятливих умов виробничого середовища та оптимальних навантажень веде до підвищення стійкості та працездатності організму, збільшення його резервних можливостей, зменшення захворювань і травматизму. Проте коливання умов середовища, в яких відбувається фізіологічна адаптація, має певну межу, характерну для кожного організму. Якщо працівник потрапляє в умови, коли інтенсивність впливу чинників виробничого середовища переважає можливості його адаптації, настають патологічні зміни фізіологічних систем, захворювання організму.

Психічна адаптація – це процес встановлення оптимальної відповідності особистості до навколишнього середовища в процесі діяльності. Зрозуміло, що такі властивості, як гальмування мислення та низька швидкість переробки інформації, обмежений діапазон сприйняття, порушення функції пам’яті гальмують адаптацію; висока рухливість нервових процесів, навпаки, її підвищує.

Психічна адаптація в процесі праці залежить від психічних властивостей працівника, його психічного стану, психологічних реакцій на стреси, що виникають на роботі, кваліфікації та культури людини, особливостей професійної діяльності, конкретних умов праці тощо.

Соціальна адаптація – це пристосування працюючої людини до системи відносин у робочому колективі з його нормами, правилами, традиціями, ціннісними орієнтаціями. Під час соціальної адаптації працівник поступово отримує різнобічну інформацію про колектив, де він працює, про систему ділових та особистих взаємовідносин.

При несприятливому протіканні соціальної адаптації підвищується рівень стресу на роботі, наслідки якого позначаються на поведінці працівника та можуть призвести до міжособових конфліктів, нещасних випадків.

Професійна адаптація – це адаптація до трудової діяльності з усіма її складовими: адаптація до робочого місця, знарядь та засобів праці, об'єктів та предметів праці, особливостей технологічного процесу, часових параметрів роботи тощо.

Професійна адаптація виражається у розвитку стійкого позитивного ставлення працівника до своєї професії, певного рівня оволодіння ним специфічними навичками та уміннями, у формуванні необхідних для якісного виконання роботи властивостей. Професійна адаптація визначається необхідним мінімумом знань та навичок, яких працівник набув при одержанні спеціальності, ступенем відповідальності, практичністю, діловитістю тощо. Адаптація вважається завершеною тоді, коли працівник досягає кваліфікації, відповідної існуючим стандартам.

Кожен із розглянутих видів адаптації впливає на працездатність та здоров'я працівника, формує у нього певний рівень чутливості та стійкості до психоемоційних перевантажень, внаслідок розвитку яких може істотно змінитися надійність професійної діяльності.

4.2 Техніка безпеки при роботі з ПК

В умовах сьогодення багато видів виробничої, наукової та навчальної діяльності, пов'язані з підвищеним навантаженням на зорову систему. У комбінації з гіподинамією та нервово-емоційною напругою тривале збереження основної робочої пози нерідко стає причиною розвитку зорового й загального стомлення, що може привести до зниження працездатності. Зорова система людини погано пристосована до розглядання зображення на екрані монітора. Тому у користувача персонального комп'ютера може виникати головний біль і запаморочення, очі починають сльозитися, з'являється втома, двоїння

зображення. Це явище отримало назву «комп'ютерний зоровий синдром». Як же уникнути шкідливого впливу монітора на очі і знизити їхню втомлюваність?

Як з'ясувалося, максимальний час, протягом якого людина безпечно може працювати на комп'ютері, становить не більше п'яти годин. Тим, хто сидить за комп'ютером довше, проблем зі здоров'ям не уникнути. А ось перелік найбільш частих порушень і симптомів, що виникають у результаті тривалої роботи за комп'ютером:

Неясність зору, коли людина дивиться вдалину;

– двоїння в очах;

– утрудненість концентрації уваги;

– хворобливі відчуття в очах, сверблячка, різь і сльозотеча, печіння, стомлення;

– головний біль у надбрівній частині чола, в потиличній, тім'яний і скроневих частинах голови;

– пропуски в наборі, зсув слів або цифр, перескакування з рядка в рядок, повторення знаків у тексті;

– відчуття поколювання й біль в руках, зап'ясті, долонях, напруга у верхній або нижній частині тулуба.

Усе це – симптоми перенапруги. Вони виникають через недотримання принципів ергономіки (ергономіка – наука, яка комплексно вивчає особливості виробничої діяльності людини в системі «людина-техніка-довкілля» задля її ефективності, безпеки та комфорту). Головний привід для занепокоєння й найбільша загроза здоров'ю - статичність пози, нерухомість, особливо м'язів голови, які потребують динамічного режиму роботи [27]. Тому при роботі на комп'ютері насамперед потрібно подумати про створення комфортного робочого місця та спеціального рухового режиму для м'язів усього тіла й особливо очей.

Воно має бути гарно освітлене. У кімнаті повинно бути стільки світла, скільки вдень на вулиці. Займатися потрібно при верхньому або настільному світлі, промені світла не повинні потрапляти прямо в очі. Природне світло має падати зліва збоку. Відстань від екрана до очей має бути не меншою 50

сантиметрів, при цьому екран повинен розташовуватися на рівні очей або трохи нижче. Корисно, час від часу, робити гімнастику для очей. І ще одне правило: моргайте кожні 3-5 секунд – це природній спосіб «змащення», очищення поверхні ока та захист від неприємних відчуттів, таких як сверблячка та печіння очей, їх почервоніння. Особливо це відчувають люди, що носять контактні лінзи.

Не слід також забувати про «спеціальне харчування» для очей. Варто вживати продукти, що зміцнюють судини сітківки ока: чорниці, чорну смородину, моркву. Корисні для очей також вітаміни (особливо комплексні полівітаміни, у яких вітаміни сполучаються з мікроелементами: цинком, кальцієм).

Дотримуючись цих порад, ви значно зменшите долю ризику погіршення стану свого здоров’я, а зокрема зору, під час тривалої роботи за комп’ютером.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи бакалавра було проаналізовано існуючі VPN-рішення для побудови безпечних корпоративних мереж та визначено їхні основні переваги й недоліки. Особливу увагу приділено протоколу WireGuard, який зарекомендував себе як сучасне, високопродуктивне та безпечне рішення для організації VPN-з'єднань. На базі лабораторного середовища з маршрутизаторами Mikrotik CHR здійснено практичну реалізацію Site-to-Site VPN, що дало змогу відтворити роботу корпоративної мережі у типовому сценарії з головним офісом та віддаленою філією.

У процесі роботи було розгорнуто дві ізольовані підмережі, з'єднані через публічний Інтернет за допомогою зашифрованого тунелю WireGuard. Налаштування маршрутизаторів підтвердило, що трафік між офісами передається без втрат і з мінімальними затримками. Тестування на рівні брандмауера й маршрутизації засвідчило правильну роботу механізмів NAT і DHCP, а також коректний розподіл трафіку (Split Tunnel VPN) для різних напрямів (внутрішні підмережі та Інтернет).

Додатково перевірено доступ до Windows Server 2022, налаштованого як RDS-сервер у DMZ головного офісу. Результати показали, що користувачі з локальної мережі філії можуть успішно підключатися до віддаленого робочого столу та безпечно працювати з корпоративними ресурсами, оскільки весь трафік RDP проходить захищеним тунелем WireGuard.

Отримані результати підтверджують, що:

– протокол WireGuard забезпечує високу швидкість і стабільність з'єднання, що відповідає потребам сучасних розподілених офісних систем;

– використання маршрутизаторів Mikrotik дає змогу гнучко налаштовувати параметри безпеки, брандмауера, маршрутизацію та DHCP;

– побудована мережа є масштабованою, оскільки до неї легко додавати нові вузли або розширювати кількість офісів, використовуючи вже існуючий VPN.

Безпека передавання даних ґрунтується на сучасних криптографічних алгоритмах ChaCha20, Poly1305 і Curve25519, які за замовчуванням підтримуються протоколом WireGuard.

Таким чином, розгорнуте та протестоване рішення Site-to-Site VPN на базі WireGuard підтвердило свою ефективність для безпечного з’єднання між віддаленими підрозділами компанії та захищеного доступу до ресурсів у головному офісі. Впровадження результатів даного дослідження дасть змогу підприємствам підвищити рівень інформаційної безпеки й оптимізувати витрати на розгортання та підтримку мережевої інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Three key network challenges every enterprise should address in the post-pandemic era. (n.d.). The Cisco News Network - APJC. https://news-blogs.cisco.com/apjc/2021/09/27/three-key-network-challenges-that-every-enterprise-should-address-now

2. Benefits of VPNS: Advantages of using a virtual private network | fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/benefits-of-vpn

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

4. What are the benefits of a VPN (virtual private network)? (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/vpn-benefits

5. 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.

6. Fearn, N. (2024, December 23). What is a VPN and how does it work? New York Post. https://nypost.com/shopping/what-is-a-vpn-and-how-does-it-work/

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

8. What is the PPTP (Point-to-Point Tunneling Protocol)? | NordVPN. (n.d.). NordVPN. https://nordvpn.com/uk/blog/what-is-pptp-protocol/

9. What is the layer two tunneling protocol (L2TP)? Overview. (n.d.). Network security platform for business | NordLayer. https://nordlayer.com/learn/vpn/l2tp/

10. What is ipsec? How does ipsec work? - huawei. (n.d.). Huawei. https://info.support.huawei.com/info-finder/encyclopedia/en/IPsec.html

11. What is OpenVPN, and how does it work? | NordVPN. (n.d.). NordVPN. https://nordvpn.com/uk/blog/what-is-openvpn/

12. What is SSTP? - VPN protocol | proofpoint US. (n.d.). Proofpoint. https://www.proofpoint.com/us/threat-reference/sstp

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

14. WireGuard: Fast, modern, secure VPN tunnel. (n.d.). WireGuard: fast, modern, secure VPN tunnel. https://www.wireguard.com/

15. 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.

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

17. User manuals - mikrotik documentation. (n.d.). MikroTik Routers and Wireless - Support. https://help.mikrotik.com/docs/spaces/UM/pages/8978698/User+Manuals

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

19. Windows Server documentation. (n.d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/windows-server/

20. Remote desktop services overview in windows server. (n.d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/remote-desktop-services-overview

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

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

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

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

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

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

27. Stadnyk, M., Zagorodna, N., Lypa, B., Gavrylov, M., Kozak, R. (2022). Network Attack Detection Using Machine Learning Methods. Challenges to national defense in contemporary geopolitical situation 2022, no. 1, 55-61.

28. Karpinski, M., Kushnerov, O., Akhiiezer, O., Sokol, V., Korchenko, A., & Muzh, V. (2025, April). Protection of Neural Networks from Attacks on Their Structure. In Annual International Congress on Computer Science: the Proceedings Book (p. 16). Oxford, United Kingdom: Published by Computer Science Research Training Center.

29. 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.

30. Mishko O., Matiuk D., Derkach M. (2024) Security of remote iot system management by integrating firewall configuration into tunneled traffic. Scientific Journal of TNTU (Tern.), vol 115, no 3, pp. 122–129.

31. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.

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

33. Захист населення і територій від надзвичайних ситуацій – WikiLegalAid. Платформа правових консультацій - WikiLegalAid. URL: https://wiki.legalaid.gov.ua/index.php/Захист_населення_і_територій_від_надзвичайних_ситуацій.