Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп’ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проєкт захищеної мережної інфраструктури організації на базі обладнання MikroTik і рішення L2TP/IPsec»

Виконала: студентка 4-го курсу групи КБ-22-2
спеціальності 125 «Кібербезпека»
_____ Вероніка КЛИМЧУК
Керівник: доцент кафедри КІ та КБ, к.т.н.
_____ Олексій ШЕЛУХА
Рецензент: доцент кафедри КІ та КБ, к.т.н., доцент
_____ Юрій РОССІНСЬКИЙ

Житомир – 2026

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
Андрій Єфіменко
2 лютого 2026 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу бакалавра

Студентка: Климчук Вероніка Сергіївна
Тема роботи: «Проєкт захищеної мережної інфраструктури організації на базі обладнання MikroTik і рішення L2TP/IPsec»
затверджена Наказом університету від 2 лютого 2026 р. №58/с
Термін здачі студентом закінченої роботи 8 червня 2026 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
1. Топологія захищеної мережної інфраструктури організації;
2. Обладнання MikroTik;
3. Рішення L2TP/Ipsec VPN.

Обладнання та програмне забезпечення:
1. Гіпервізор Oracle VirtualBox;
2. Емулятор GNS3.
3. ОС Windows Server;
4. ОС Windows;
5. Маршрутизатори Mikrotik RouterOS;
6. Комутатори Cisco.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Хохлов М.О.	02.02.2026	02.02.2026
2	Хохлов М.О.	02.02.2026	02.02.2026
3	Хохлов М.О.	02.02.2026	02.02.2026

Студентка _____ Вероніка КЛИМЧУК

Керівник _____ Олексій ШЕЛУХА

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	02.02.2026	Виконано
2	Пошук літературних джерел	02.03.2026	Виконано
3	Аналіз існуючих рішень	02.03.2026	Виконано
4	Побудова моделі мереже	23.03.2026	Виконано
5	Аналіз та вибір обладнання	30.03.2026	Виконано
6	Налаштування проєкту мережі	06.04.2026	Виконано
7	Тестування працездатності та аналіз результатів	20.04.2026	Виконано
8	Написання пояснювальної записки	01.06.2026	Виконано
9	Підготовка матеріалів до захисту	08.06.2026	Виконано

Студентка _____ Вероніка КЛИМЧУК

Керівник _____ Олексій ШЕЛУХА

АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра складається з пояснювальної записки, що містить вступ, три розділи, висновки, список використаної літератури та додатки. Текстова частина викладена на 98 сторінках. Пояснювальна записка містить 91 рисунок, 4 таблиці та 4 сторінки додатків. Список використаних джерел містить 32 найменування і займає 3 сторінки. Загальний обсяг роботи – 102 сторінки.

Метою роботи є дослідження особливостей функціонування рішень захисту розподілених корпоративних мереж та розробка проєкту захищеної мережі з віддаленими підрозділами та користувачами на основі рішень MikroTik та L2TP/IPsec.

У першому розділі досліджено базові принципи безпеки корпоративних мереж, обгрунтовано вибір обладнання MikroTik та технології L2TP/IPsec для реалізації захищених тунелів, а також сформовано постановку завдань для захищеної розподіленої інфраструктури.

У другому розділі на основі трирівневої моделі розроблено логічну й фізичну топології мережі, схему IP-адресації, підібрано апаратну базу та спроєктовано комплексну підсистему захисту, що поєднує централізоване керування доступом через RADIUS з Active Directory, роботу брандмауера MikroTik, моніторинг подій через Syslog, використання SSH та відключення незадіяних портів комутаторів.

У третьому розділі в середовищі емулятора GNS3 виконано практичне розгортання та конфігурування спроєктованої інфраструктури, реалізовано доменні служби Windows Server, налаштовано тунелі L2TP/IPsec типу Site-to-Site та Remote Access, а також проведено комплексне тестування мережі й аналіз передачі зашифрованого трафіку з використанням утиліти Wireshark.

КЛЮЧОВІ СЛОВА: КОРПОРАТИВНА МЕРЕЖА, МЕРЕЖНА БЕЗПЕКА, MIKROTIK, CISCO, L2TP, IPSEC, RADIUS, ACTIVE DIRECTORY, GNS3, ШИФРУВАННЯ.

ANNOTATION

The Bachelor's graduation qualification thesis consists of an explanatory note containing an introduction, three chapters, conclusions, a list of references, and appendices. The text part is presented on 98 pages. The explanatory note contains 91 figures, 4 tables, and 4 pages of appendices. The list of references includes 32 items and occupies 3 pages. The total volume of the thesis is 102 pages.

The aim of the work is to investigate the operational features of security solutions for distributed corporate networks and to develop a project for a secure network with remote branches and users.

The first chapter investigates the basic principles of corporate network security, substantiates the choice of MikroTik equipment and L2TP/IPsec technology for implementing secure tunnels, and defines the task statement for the secure distributed infrastructure.

The second chapter develops the logical and physical network topologies and the IP addressing scheme based on a three-tier model, selects the hardware base, and designs a comprehensive security subsystem that combines centralized access management via RADIUS with Active Directory, MikroTik firewall operation, event monitoring via Syslog, the use of SSH, and disabling unused switch ports.

The third chapter performs the practical deployment and configuration of the designed infrastructure within the GNS3 emulator environment, implements Windows Server domain services, configures Site-to-Site and Remote Access L2TP/IPsec tunnels, and conducts comprehensive network testing alongside encrypted traffic analysis using the Wireshark utility.

KEYWORDS: CORPORATE NETWORK, NETWORK SECURITY, MIKROTIK, CISCO, L2TP, IPSEC, RADIUS, ACTIVE DIRECTORY, GNS3, ENCRYPTION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 7
ВСТУП 8
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ ЗАХИЩЕНИХ КОРПОРАТИВНИХ МЕРЕЖ НА БАЗІ ОБЛАДНАННЯ MIKROTIK 10
1.1 Основні принципи безпеки сучасних корпоративних мереж 10
1.2 Аналіз ринку мережного обладнання та обгрунтування вибору платформи MikroTik RouterOS 12
1.3 Архітектурні принципи побудови та порівняльна характеристика протоколів VPN 17
1.4 Аналіз принципів функціонування та архітектури L2TP/IPsec 25
1.5 Постановка завдання дослідження 27
РОЗДІЛ 2. ПРОЄКТУВАННЯ ІНФРАСТРУКТУРИ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ 31
2.1 Розробка мережної топології та адресації 31
2.2 Механізм централізованої автентифікації RADIUS для VPN 37
2.3 Вибір апаратної бази мережі 38
2.4 Вибір механізмів захисту мережної інфраструктури 41
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ MIKROTIK ТА ТЕХНОЛОГІЇ L2TP/IPSEC 44
3.1 Базова конфігурація пристроїв мережі 44
3.2 Налаштування L2TP/IPsec між головним офісом та підрозділом 58
3.3 Налаштування L2TP/IPsec між головним офісом та віддаленим користувачем 65
3.4 Налаштування додаткових механізмів захисту 74
3.5 Перевірка роботи мережі і впроваджених засобів 83
ВИСНОВКИ 95
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 96
ДОДАТКИ 99

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AAA — Authentication, Authorization, and Accounting

AES — Advanced Encryption Standard

DHCP — Dynamic Host Configuration Protocol

DNS — Domain Name System

ESP — Encapsulating Security Payload

FWD — DNS Forwarding

GNS3 — Graphical Network Simulator-3

HQ — Headquarters

ICMP — Internet Control Message Protocol

IP — Internet Protocol

IPsec — Internet Protocol Security

L2TP — Layer 2 Tunneling Protocol

LAN — Local Area Network

MS-CHAP v2 — Microsoft Challenge Handshake Authentication Protocol

NAT — Network Address Translation

NGFW – Next-Generation Firewall

NPS — Network Policy Server

NTP — Network Time Protocol

OS — Operating System

PPP — Point-to-Point Protocol

RADIUS — Remote Authentication in Dial-In User Service

SVI — Switch Virtual Interface

SFP — Small Form-factor Pluggable

SSH — Secure Shell

VLAN — Virtual Local Area Network

VPN — Virtual Private Network

WAN — Wide Area Network

ВСТУП

Актуальність теми. Стрімкий перехід організацій на віддалений і гібридний формати роботи висувають нові вимоги до архітектури корпоративних мереж. Традиційне розуміння локальної мережі, як замкнутого фізичного периметра вже давно застаріло. Сьогодні мережна інфраструктура підприємства має бути гнучким, масштабованим і безпечним середовищем, що інтегрує територіально рознесені підрозділи та хмарні сервіси. У цьому контексті побудова відмовостійкої, масштабованої та захищеної мережної архітектури стає важливим кроком для забезпечення безперервності бізнес-процесів і захисту корпоративних даних [1].

Використання публічних каналів зв'язку, зокрема мережі Інтернет, для передачі корпоративної інформації створює значні ризики починаючи перехопленням трафіку і аж до несанкціонованого доступу до внутрішніх ресурсів мережі. Тому використання технології віртуальних приватних мереж (VPN) на базі бюджетного, надійного та функціонального обладнання, такого як MikroTik, є найбільш раціональним підходом для малих та середніх бізнесів на сьогодні. Використання рішення L2TP/IPsec дозволяє створити криптографічно захищений тунель, який поєднує універсальність підключення з достатнім рівнем безпеки, що забезпечується сучасними алгоритмами шифрування.

Метою кваліфікаційної роботи є проведення аналізу особливостей функціонування існуючих рішень захисту розподілених корпоративних мереж та розробка проєкту захищеної мережі з віддаленими підрозділами та користувачами на базі платформи MikroTik RouterOS з використанням технології L2TP/IPsec.

Визначена мета обумовлює наступні завдання:

- провести аналіз підходів до побудови захищеної мережної інфраструктури організації з віддаленими підрозділами з використанням технологій VPN;
- розробити проєкт топології корпоративної мережі організації, провести аналіз обладнання та програмних засобів для реалізації проєкту захищеної мережної інфраструктури;

- провести розгортання розробленого проєкту захищеної мережної інфраструктури організації із використанням обраних рішень та обладнання;
- провести тестування працездатності проєкту захищеної мережної інфраструктури організації та аналізу отриманих результатів.

Об’єктом дослідження є процес побудови та захисту розподіленої мережної інфраструктури організації.

Предметом дослідження є методи, технології та засоби розробки захищеної мережної інфраструктури організації, зокрема метод комп’ютерного моделювання, обладнання MikroTik та рішення L2TP/IPsec.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ ЗАХИЩЕНИХ КОРПОРАТИВНИХ МЕРЕЖ НА БАЗІ ОБЛАДНАННЯ MIKROTIK

1.1 Основні принципи безпеки сучасних корпоративних мереж

В умовах переходу бізнес-процесів до гібридних моделей роботи, мережна інфраструктура стає базовим активом будь-якої організації, що зрештою перетворює її на головну мішень для кібератак. Забезпечення безпеки корпоративної мережі сьогодні не обмежується лише захистом периметра, воно вимагає створення комплексної екосистеми, здатної протидіяти як масовим автоматизованим загрозам, так і складним цілеспрямованим атакам. Побудова такої системи базується на розумінні того, що мережна безпека є не кінцевою точкою, а динамічним процесом адаптації до нових методів компрометації даних, де ключову роль відіграє поєднання стійких криптографічних протоколів із суворими політиками контролю доступу [2].

Побудова сучасної безпечної мережної інфраструктури базується на комплексному підході, що виходить за межі простого встановлення засобів захисту і розглядається як безперервний процес, що складається з етапів захисту, виявлення та реагування. Згідно з дослідженнями, ефективна стратегія безпеки повинна передусім забезпечувати фундаментальну тріаду CIA, що включає [3]:

- Конфіденційність (Confidentiality) – гарантія доступу до даних лише авторизованим особам;
- Цілісність (Integrity) – захист від несанкціонованої модифікації інформації;
- Доступність (Availability) – забезпечення безперебійного доступу до сервісів для легітимних користувачів.

Нехтування будь-яким із цих компонентів створює критичні вразливості, які можуть бути використані зловмисниками для дестабілізації бізнес-процесів або викрадення інтелектуальної власності.

Типові загрози та їх протидія

Ефективне проектування захисту неможливе без розуміння актуального ландшафту загроз, які можуть бути ініційовані як зовнішніми зловмисниками, так і внутрішніми факторами. Серед найбільш критичних можна виділити наступні [4]:

- Атаки на відмову в обслуговуванні (DoS/DDoS). Спрямовані на перевантаження мережних ресурсів надмірною кількістю запитів, що призводить до повної або часткової зупинки робот бізнес-служб;
- Фішинг та соціальна інженерія. Використання людського фактора для отримання персональних даних (наприклад логіни та паролі) часто стає точкою входу зловмисника у внутрішню мережу;
- Шкідливе програмне забезпечення. Віруси, трояни та програми-вимагачі, що здатні шифрувати дані або створювати «бекдори» для віддаленого управління;
- Атаки типу Man-in-the-Middle (MitM). Перехоплення та можлива підміна трафіку між двома вузлами мережі, що є особливо небезпечним при використанні нешифрованих протоколів (наприклад HTTP, FTP, Telnet);
- Експлуатація вразливостей програмного забезпечення. Використання помилок у коді операційних систем або прошивок мережного обладнання, зокрема вразливостей «нульового дня», для отримання несанкціонованого доступу;
- Атаки на паролі. Brute force, dictionary attacks, credential stuffing та password spraying, спрямовані на підбір або повторне використання скомпрометованих облікових даних;
- SQL-ін’єкції та крос-сайтове скриптинг (XSS). Експлуатація вразливостей веб-додатків для отримання доступу до баз даних або виконання шкідливого коду в браузері користувача.

Для протидії цим загрозам необхідно впроваджувати комплексну стратегію захисту, засновану на таких наступних принципах:

- Багаторівневий захист (Defense in Depth). Створення ешелонованої оборони, де кожен рівень інфраструктури має власні механізми захисту (фізичний доступ, сегментація мереж, міжмережні екрани, системи запобігання вторгненням,

антивіруси), що гарантує, що компрометація одного елемента не призведе до повного зламу всієї мережі;

- Концепція «Нульової довіри» (Zero Trust Architecture). Відмова від поняття «довіреного периметра». Кожен запит на доступ до ресурсів піддається суворій автентифікації, авторизації та перевірці незалежно від розташування джерела, що мінімізує ризики внутрішніх загроз та горизонтального переміщення зловмисників [5].

- Протидія актуальним загрозам та вразливостям. Регулярний аудит прошивок і програмного забезпечення, використання криптографічно стійких протоколів передачі даних (наприклад, TLS 1.3, IPsec), впровадження систем аналізу трафіку в реальному часі та моніторингу аномалій.

- Управління доступом та автентифікація. Впровадження багатофакторної автентифікації (MFA), рольових моделей доступу (RBAC), шифрування каналів зв'язку при віддаленому підключенні (VPN) та принципів найменших привілеїв.

- Моніторинг та аналіз інцидентів. Розбір і аналіз журналів подій, впровадження SIEM-систем, регулярне тестування на проникнення та проведення розслідування інцидентів для запобігання повторним атакам.

- Сегментація мережі. Розподіл корпоративної мережі на окремі зони за допомогою віртуальних локальних мереж (VLAN), що обмежує вільне переміщенню зловмисника всередині інфраструктури.

Загалом, побудова сучасної корпоративної мережі вимагає переходу до створення цілісної екосистеми, де технічні параметри обладнання тісно інтегровані з політиками безпеки. Тільки поєднання регулярного моніторингу, аудиту вразливостей та використання перевірених архітектурних рішень дозволяє забезпечити стійкість мережі до постійно зростаючих кіберзагроз.

1.2 Аналіз ринку мережного обладнання та обгрунтування вибору платформи MikroTik RouterOS

Сучасний ринок мережного обладнання для малого та середнього бізнесу характеризується широким спектром рішень від корпоративних систем преміум-

класу до бюджетних платформ. Вибір платформи визначається балансом між функціональністю, вартістю, зручністю управління, надійністю та можливостями масштабування. Для реалізації захищеної корпоративної інфраструктури з акцентом на VPN, гнучкістю налаштувань та економічність було проведено порівняльний аналіз п’яти ключових вендорів: Cisco, Juniper, Fortinet та та MikroTik.

Cisco Systems. Будучи багаторічним лідером ринку, Cisco пропонує найбільш комплексні рішення (наприклад, серії ISR та Catalyst), що відрізняються високим рівнем надійності та розвиненою екосистемою технічної підтримки. Проте для багатьох організацій критичним недоліком є висока вартість як самого обладнання, так і складних схем ліцензування функцій безпеки, що значно підвищує загальні витрати на інфраструктуру [6].

Juniper Networks займає провідні позиції в сегменті високонавантажених мереж та великих центрів обробки даних, пропонуючи потужну операційну систему Junos OS, яка базується на модульній архітектурі та забезпечує виняткову стабільність і безпеку. Ключовою перевагою рішень Juniper є їхня орієнтованість на автоматизацію та підтримку відкритих стандартів, що робить це обладнання ідеальним для побудови складних магістральних мереж, проте висока вартість пристроїв та сервісних контрактів, а також складність налаштування через спеціалізований інтерфейс командного рядка (CLI) зміщують фокус їх використання переважно на рівень великих корпорацій та інтернет-провайдерів [7].

Fortinet. Вендор спеціалізується на рішеннях у сфері кібербезпеки, де серія FortiGate виступає як потужний міжмережний екран наступного покоління (NGFW). Продукція Fortinet демонструє високу продуктивність при аналізі загроз у реальному часі, проте повний функціонал безпеки доступний лише за умови придбання дорогих щорічних підписок FortiGuard, що може бути економічно недоцільним для малих та середніх підприємств [8].

MikroTik. Обладнання латвійського вендора займає унікальну нішу завдяки операційній системі RouterOS, яка надає функціонал професійного рівня (протоколи динамічної маршрутизації, складні VPN-конфігурації) за бюджетною

ціною обладнання. Ключовою перевагою є відсутність прихованих ліцензій та повний контроль над параметрами мережі, що робить MikroTik гарною платформою для досліджень та побудови захищених мереж у проєктах з обмеженим бюджетом, але високими вимогами до гнучкості конфігурації [9].

Нижче на табл.1.1 наведено порівняльний аналіз ключових характеристик мережних вендорів на сучасному ринку.

Таблиця 1.1

Порівняння характеристик мережних вендорів

	Cisco Systems	**Juniper Networks**	**Fortinet**	**MikroTik (RouterOS)**
Цільовий сегмент	Великі корпорації	Середній та великий бізнес	Середні та великі корпорації	Малий та середній бізнес
Рівень складності	Високий (CLI)	Високий (Junos CLI + Mist AI)	Середній (Web)	Середній (WinBox/CLI)
Гнучкість ОС	Пропрієтарна, закрита	Пропрієтарна, закрита	Орієнтована на UTM	Максимальна (Linux-based)
Ліцензування	Платне (окремі функції)	Платне (Juniper Care, Mist AI)	Платне (FortiGuard)	Відсутнє
Цінова категорія	Висока	Висока	Середня	Бюджетна
Оновлення ПЗ	Платні (SmartNet)	Платні (Juniper Care)	Платні (Support)	Безкоштовні
Підтримка та спільнота	Висока	Висока	Висока	Висока

Проаналізувавши дані отримані в ході порівняння основних характеристик було встановлено, що MikroTik забезпечує оптимальне співвідношення

функціональності, вартості та гнучкості для реалізації захищеної корпоративної інфраструктури в сегменті малого та середнього бізнесу. На відміну від Cisco та Juniper Networks, які пропонують вищу надійність, SD-WAN та інтегровані рішення безпеки, але за значно вищу ціну, MikroTik не поступається їм за базовими можливостями при мінімальних витратах на обладнання та повній відсутності ліцензійних платежів. Fortinet лідирує в UTM-функціоналі, але також вимагає дорогих підписок. Таким чином, вибір MikroTik обумовлений необхідністю поєднати необхідний рівень захисту з економічністю та високою адаптивністю до вимог розподіленої корпоративної мережі.

Компанія MikroTik, заснована у 1995 році в Ризі (Латвія), пройшла шлях від розробника програмного забезпечення для бездротових систем до одного з провідних світових виробників мережного обладнання. Ключовим етапом розвитку став 2002 рік, коли компанія розпочала випуск власної апаратної лінійки під брендом RouterBOARD. Ці пристрої орієнтовані на широкий спектр споживачів – від домашніх користувачів до великих інтернет-провайдерів пропонуючи високу продуктивність та багатий набір функцій за відносно низької вартості [10].

Основою екосистеми MikroTik є операційна система RouterOS, яка базується на ядрі Linux. Це спеціалізоване програмне забезпечення здатне перетворити будь-яку апаратну платформу, будь то фірмовий пристрій RouterBOARD, звичайний персональний комп'ютер архітектури x86, чи віртуальну машину на повноцінний маршрутизатор. RouterOS надає адміністратору інструментарій для гнучкого керування пропускною здатністю, налаштування прозорих пакетних фільтрів, створення бездротових точок доступу та побудови складних VPN-мереж.

Важливою перевагою платформи є універсальність налаштування. Доступ до системи можна отримати через вебінтерфейс, командний рядок (CLI) або спеціалізовану графічну утиліту WinBox. У контексті побудови захищених мереж, RouterOS підтримує широкий спектр протоколів тунелювання та апаратне прискорення IPsec, що робить її ефективним рішенням для реалізації VPN-з'єднань з використанням сучасних алгоритмів шифрування даних.

Операційна система RouterOS вирізняється гнучкістю та широким набором інструментів, що дозволяють адаптувати мережне обладнання під конкретні потреби бізнесу. Основними функціональними можливостями системи є [11]:

- Розширені можливості маршрутизації. Система підтримує більшість сучасних протоколів динамічної маршрутизації, таких як OSPF, BGP та RIP. Це дозволяє інтегрувати пристрої MikroTik у складні розподілені мережі, забезпечуючи автоматичний вибір оптимального шляху для даних. Крім того, підтримується технологія MPLS (Multiprotocol Label Switching) для створення ізольованих віртуальних приватних мереж у межах однієї фізичної інфраструктури, а також VRF для логічного сегментування таблиць маршрутизації.

- Підтримка VPN-технологій та протоколів тунелювання. RouterOS пропонує один із найширших переліків протоколів для організації захищеного віддаленого доступу. Система забезпечує повноцінну роботу з класичними VPN-рішеннями, такими як L2TP (у зв'язці з IPsec), PPTP, SSTP та OpenVPN, а також підтримує сучасні протоколи WireGuard та ZeroTier. Для створення складних мережних топологій доступні інструменти інкапсуляції GRE, IPIP, 6to4, а також унікальний фірмовий EoIP (Ethernet over IP). Важливою перевагою є глибока інтеграція з IPsec та підтримка PPPoE, що забезпечує сумісність пристроїв MikroTik із будь-якою сучасною мережною архітектурою [12].

- Мережний екран (Firewall). Брандмауер RouterOS базується на технології Stateful Packet Inspection, що дозволяє відстежувати стан активних з'єднань. Система підтримує фільтрацію на рівні деяких протоколів прикладного рівня (Layer-7), що є важливим для блокування небажаного трафіку. Адміністратор має можливість гнучко налаштовувати правила NAT для організації доступу до внутрішніх сервісів ззовні та маскування локальних адрес.

- Модульність та пакетна система. RouterOS має модульну структуру, що дозволяє адміністратору кастомізувати систему під конкретні завдання. Користувачі можуть завантажувати та встановлювати додаткові пакети (наприклад, dude, mpls, wireless, iot, advanced-tools) з офіційного сайту MikroTik,

що дозволяє розширювати функціонал без необхідності перевстановлення всієї системи.

- Керування трафіком та QoS. Завдяки вбудованим механізмам Quality of Service (QoS) та інструментам пріоритезації (наприклад, Queue Trees), RouterOS дозволяє виділяти гарантовану смугу пропускання для важливих додатків, таких як IP-телефонія або відеоконференції, запобігаючи затримкам під час пікових навантажень.

- Універсальність розгортання та Cloud Hosted Router (CHR). Окрім апаратних рішень RouterBOARD, MikroTik пропонує версію CHR, яка дозволяє розгорнути RouterOS у вигляді віртуалізованого маршрутизатора для роботи у хмарних середовищах або на серверах. Це дозволяє компаніям масштабувати свою мережну інфраструктуру в хмарі, зберігаючи єдиний інтерфейс керування та ідентичний набір функцій безпеки.

- Адміністрування. Для налаштування доступні як командний рядок (CLI), так і графічні інтерфейси, як ось веб-панель WebFig та більш професійна і традиційна утиліта WinBox.

- Централізований моніторинг за допомогою The Dude. Для моніторингу інфраструктури MikroTik пропонує безкоштовну утиліту The Dude, яка автоматично сканує мережу, будує карту зв’язків та моніторить стан кожного пристрою.

1.3 Архітектурні принципи побудови та порівняльна характеристика протоколів VPN

Віртуальна приватна мережа (Virtual Private Network, VPN) – це логічна мережа, яка будується поверх уже існуючої фізичної інфраструктури (зазвичай Інтернету) і створює захищений канал між двома вузлами або мережами. Хоча трафік фізично передається через публічні мережі, для учасників VPN він виглядає наче як передача всередині приватної мережі. Дані в тунелі шифруються, забезпечується їхня цілісність і автентичність, а доступ отримують лише авторизовані користувачі. Такі тунелі дозволяють об’єднувати віддалені офіси,

організовувати безпечний доступ співробітників до корпоративних ресурсів, а також захищати передавання конфіденційної інформації у хмарних сервісах [13].

Переваги впровадження VPN:

- використання публічних каналів зв'язку замість оренди виділених ліній дозволяє суттєво знизити витрати на розгортання та підтримку інфраструктури;
- застосування сучасних алгоритмів шифрування (AES-256 та інші) механізмів автентифікації та перевірки цілісності гарантують високий рівень захисту даних від несанкціонованого доступу та модифікації;
- забезпечення високої масштабованості за рахунок швидкого підключення нових сегментів мережі або віддалених користувачів;
- можливість централізованого управління доступом та політиками безпеки.

Недоліки та експлуатаційні обмеження:

- процеси інкапсуляції та криптографічної обробки пакетів створюють додаткові накладні витрати, що впливає на пропускну здатність та затримку сигналу;
- надійність та швидкість з’єднання безпосередньо залежать від стабільності та характеристик мережі Інтернет-провайдера;
- керування складними топологіями потребує високої кваліфікації адміністраторів для належного налаштування політик безпеки та управління ключами;
- можливість блокування VPN-трафіку провайдерами або корпоративними фаєрволами (особливо для UDP-протоколів);
- додаткове навантаження на апаратні ресурси (CPU, пам’ять) VPN-сервера при великій кількості одночасних з’єднань.

Загалом, за призначенням та архітектурою VPN поділяють на Remote Access VPN та Site-To-Site.

Remote Access VPN призначений для підключення окремих користувачів до корпоративної мережі через Інтернет. На кінцевому обладнанні (комп’ютер, ноутбук чи смартфон) встановлюється VPN-клієнт, який створює зашифрований

тунель до VPN-шлюзу організація. Після проходження аутентифікації та підключення користувач може обмінюватись з внутрішні ресурсами (файлові сервери, бази даних, застосунки) так, ніби він знаходиться в локальній мережі офісу. Такий підхід особливо важливий у сценаріях віддаленої роботи, BYOD (Bring Your Own Device) та хмарних сервісів, коли співробітникам потрібно безпечно працювати будь-де і з будь-якого пристрою, рис.1.1

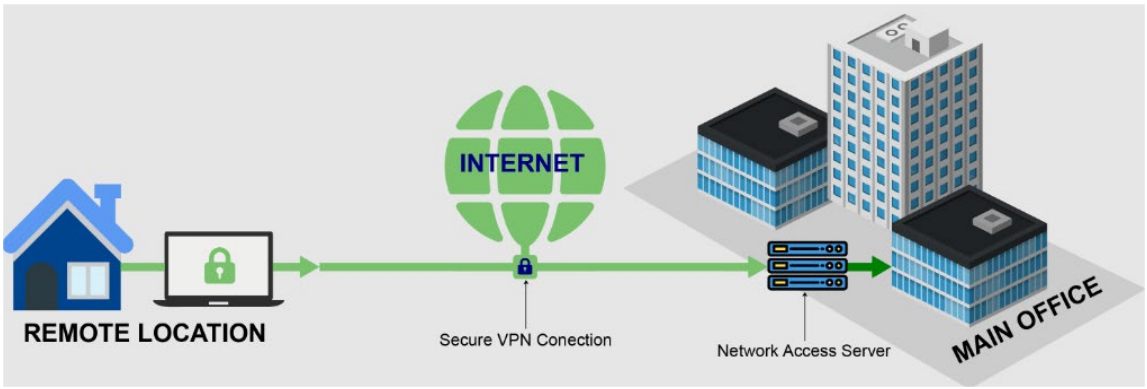


Рисунок 1.1 – Топологія корпоративної мережі з використанням Remote Access VPN [14]

Site-to-site VPN використовується для з'єднання двох або більше локальних мереж. Наприклад головного офісу та філій, дата-центрів, майданчиків у різних містах чи країнах. На периферійних маршрутизаторах або VPN-шлюзах налаштовується постійний тунель, через який передається весь або частина міжмережного трафіку. Для внутрішніх хостів така взаємодія виглядає як звичайна корпоративна WAN-мережа. На відміну від Remote Access, тут не потрібно налаштовувати VPN-клієнт на кожному пристрої, що спрощує адміністрування і масштабування для великих організацій, наприклад банків, університетів чи компаній з багатьма філіями, рис.1.2

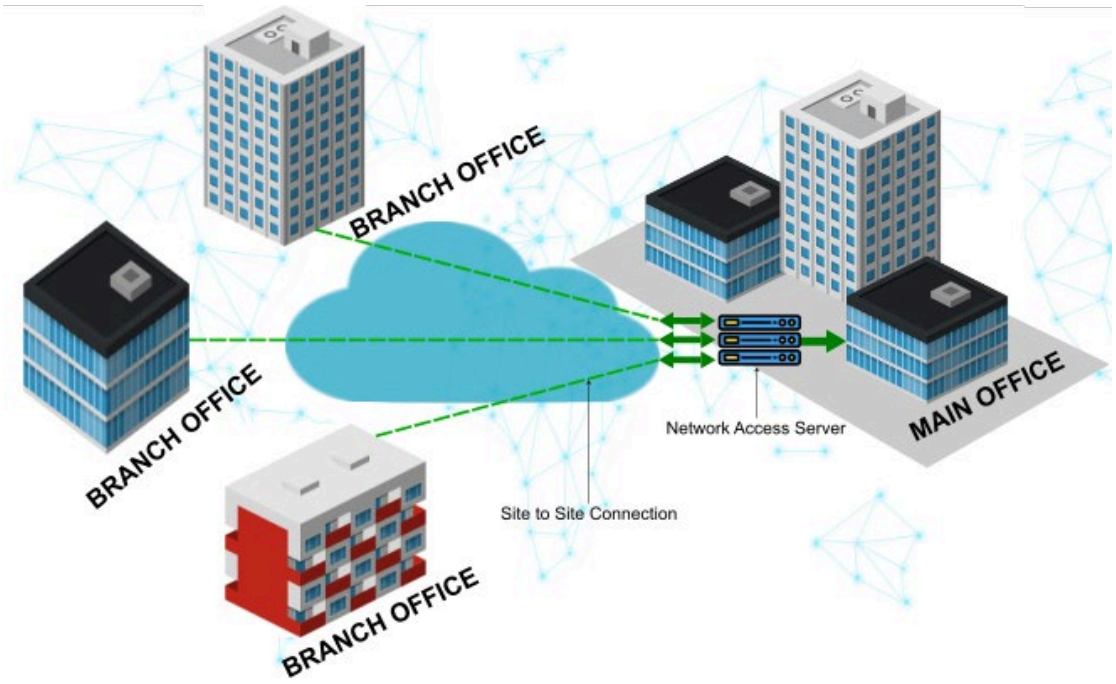


Рисунок 1.2 – Топологія корпоративної мережі з використанням Site-to-site VPN

Додатково можна виділити Personal (Private) VPN, який є підтипом Remote access адаптованим для індивідуального використання на персональних комп'ютерах та мобільних пристроях. Технологія забезпечує захист мережної активності шляхом створення зашифрованого тунелю між пристроєм користувача та сервером постачальника послуг, що дозволяє мінімізувати ризики відстеження та несанкціонованого збору даних. З технічної точки зору, весь вихідний трафік проходить через проміжний вузол, завдяки чому кінцеві веб-ресурси ідентифікують IP-адресу VPN-сервера замість реальних мережних параметрів користувача. Це сприяє підвищенню рівня безпеки під час використання Інтернету в публічних мережах, рис.1.3.

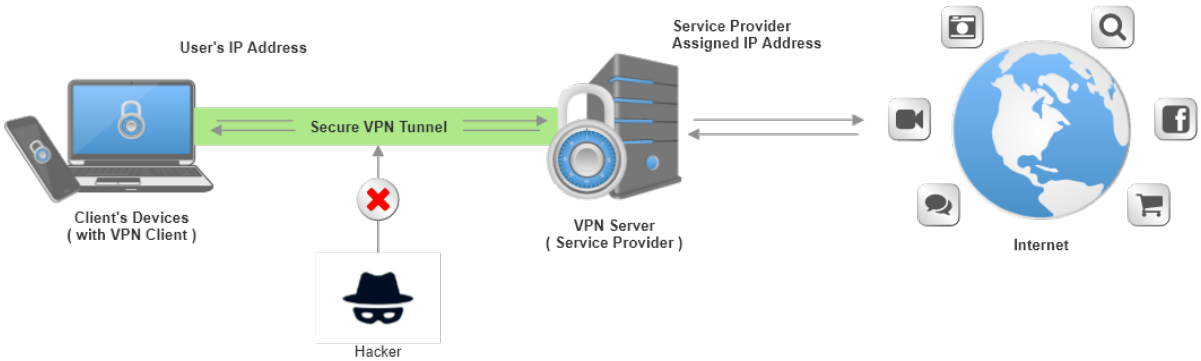


Рисунок 1.3 – Топологія з використанням Personal VPN [15]

Існують різні протоколи VPN, кожен з яких має свої особливості щодо механізму тунелювання, шифрування, продуктивності та рівня безпеки. Серед найпоширеніших та тими що підтримуються RouterOS, можна виділити SSTP, IKEv2/IPsec, L2TP/IPsec, OpenVPN та Wireguard. Остаточний вибір протоколу залежить від вимог до безпеки, сумісності з платформами, продуктивності та здатності обходити мережні обмеження [16].

1. SSTP розроблений Microsoft і використовує SSL/TLS для створення захищеного тунелю між клієнтом і сервером. Він працює на порті TCP 443 (HTTPS), що робить його подібним до звичайного веб-трафіку, дозволяючи легко обходити фаєрволи. SSTP інтегрується з Windows, забезпечуючи надійне шифрування з використанням алгоритму AES-256. Він добре підходить для корпоративних середовищ, де потрібна сумісність з Windows, але менш поширений поза екосистемою Microsoft [17].

Переваги:

- сильне шифрування і інтеграція з TLS для високої безпеки;
- легко обходить фаєрволи, оскільки використовує TCP порт 443 (HTTPS);
- вбудована підтримка в Windows;
- стабільний на нестабільних мережах через TCP.

Недоліки:

- обмежена сумісність з іншими ОС;
- закритий код;
- відсутня підтримка UDP.

2. IKEv2/IPsec поєднує протокол обміну ключами IKEv2 із захистом IPsec, забезпечуючи конфіденційність, цілісність і автентифікацію даних. Він був розроблений Microsoft та Cisco насамперед для мобільних пристроїв, забезпечуючи швидке відновлення з'єднання після переривань (наприклад, зміна між Wi-Fi і мобільним інтернетом). IKEv2 використовує шифрування AES-256. Рішення добре підходить для смартфонів і планшетів, де потрібна стабільність, але менш є менш гнучким для додаткових налаштувань [18].

Переваги:

- стабільність з’єднання при зміні мереж;
- високий рівень безпеки завдяки Ipsec;
- швидке встановлення тунелю;
- вбудована підтримка в iOS, Android, Windows і macOS.

Недоліки:

- складність налаштування;
- менш гнучкий для конфігурації порівняно з OpenVPN.
- закритий код.

3. L2TP/IPsec це гібридний протокол, де L2TP створює тунель, а IPsec забезпечує шифрування та аутентифікацію. L2TP/IPsec підтримує AES-256, але є повільнішим через подвійне інкапсуляцію. Проте суттєвою перевагою є відсутність необхідності встановлення додаткового програмного забезпечення. Дане рішення досить поширене для використання в корпоративних мережах і мобільних ОС [19].

Переваги:

- широка підтримка платформ;
- не потребує додаткового клієнтського ПЗ;
- високий рівень безпеки завдяки IPsec.

Недоліки:

- подвійна інкапсуляція збільшує накладні витрати трафіку та затримки;
- може бути заблокований фаєрволами;
- нижча пропускна здатність в порівнянні з WireGuard або OpenVPN.

4. OpenVPN є універсальним рішенням з відкритим вихідним кодом, що використовує бібліотеку OpenSSL для шифрування. OpenVPN дозволяє проводити гнучку конфігурацію використовуючи різні методи аутентифікації (certificates, pre-shared keys). Протокол вирізняється здатністю працювати як через UDP для швидкості, так і через TCP. OpenVPN працює на будь-якому порту, обходячи обмеження фаєрволів і тому ідеально для приватності та безпеки. Він повільніший за WireGuard через великий код, але дуже надійний [20].

Переваги:

- висока гнучкість конфігурації;
- сильне шифрування та надійний захист даних;
- прозорість програмного коду;
- можливість використання будь-якого порту.

Недоліки:

- складніша конфігурація порівняно з іншими протоколами;
- висока ресурмомісткість.

5. WireGuard базується на використанні сучасного алгоритму шифрування ChaCha20 та мінімізованому обсязі програмного коду. Він функціонує на базі протоколу UDP і спрямований на забезпечення високої пропускної здатності за низьких затримок. Завдяки лаконічній архітектурі, дане рішення демонструє високу ефективність на пристроях забезпечуючи миттєве з'єднання та мінімальні затримки [21].

Переваги:

- висока пропускна здатність;
- найвища швидкість серед усіх існуючих протоколів;
- легкість налаштування та низьке навантаження на процесор;
- стабільність при зміні мережних інтерфейсів.

Недоліки:

- відсутність динамічного розподілу IP-адрес;
- менша гнучкість налаштувань;
- може бути заблокований фаєрволами.

Вибір оптимального VPN-протоколу для впровадження в мережу вимагає балансу між рівнем захищеності даних та пропускною здатністю каналів зв'язку. З метою обгрунтування фінального архітектурного рішення було наведено порівняльний аналіз згаданих рішень, табл.1.2.

Таблиця 1.2

Порівняльна характеристика основних протоколів VPN

Характеристика	SSTP	IKEv2/IPsec	L2TP/IPsec	OpenVPN	WireGuard
Порт	TCP 443	UDP 500, 4500	UDP 1701, 500, 4500	UDP або TCP (будь-який)	UDP (будь-який)
Підтримка платформ	Windows (нативно)	Windows, iOS, Android, macOS	Windows, iOS, Android, macOS	Всі (клієнт)	Всі (нативно/клієнт)
Відкритий код	Ні (Microsoft)	Ні (частково)	Ні (частково)	Так	Так
Швидкість / Ефективність	Середня / Низька	Висока	Низька (подвійна інкапсуляція)	Середня	Найвища
Обхід фаєрволів	Відмінний (порт 443)	Середній	Слабкий	Відмінний (будь-який порт)	Середній
Складність налаштування	Низька (Windows)	Середня	Низька	Висока	Низька
Підтримка в RouterOS	Повна	Повна	Повна	Повна	Повна
Навантаження на CPU	Середня	Низька	Висока	Висока	Найнижча
Ключові переваги	Обходить фаєрволи, стабільний на TCP, вбудований у Windows	Швидке відновлення, мобільність, нативна підтримка	Широка сумісність, без додаткового ПЗ	Гнучкість, відкритий код, обхід обмежень	Найвища швидкість, низьке нанантаження, Простий код
Ключові недоліки	Закритий код, тільки TCP, повільний	Блокується UDP, складне налаштування	Подвійна інкапсуляція, повільний	Повільніший за WireGuard, складна конфігурація	Статичні IP, менша гнучкість, блокується UDP

Виходячи з проведеного аналізу вибір на користь L2TP/IPsec для реалізації захищеної мережної інфраструктури обумовлений оптимальним співвідношенням між універсальною сумісністю та відносною простотою впровадження в корпоративному середовищі. Нативна підтримка цього протоколу більшістю сучасних операційних систем дозволяє організувати віддалений доступ без необхідності встановлення додаткового програмного забезпечення на кінцеві пристрої користувачів, що суттєво спрощує адмініструванн. Застосування апаратного прискорення шифрування IPsec на обладнанні MikroTik дозволяє ефективно компенсувати обчислювальні витрати, пов’язані з подвійною

інкапсуляцією трафіку, забезпечуючи стабільну пропускну здатність каналів зв’язку. Хоча сучасніші протоколи (WireGuard, IKEv2/IPsec, OpenVPN) є кращими за L2TP/IPsec в швидкості, мобільності чи гнучкості, але L2TP/IPsec оптимально поєднує універсальність, надійність, безпеку і перевірену часом надійність архітектури. Тому вибір даного протоколу є раціональним рішенням для побудови захищених тунелів у гетерогенних корпоративних мережах із високими вимогами до конфіденційності даних.

1.4 Аналіз принципів функціонування та архітектури L2TP/IPsec

L2TP/IPsec є однією з класичних технологій побудови віртуальних приватних мереж, яка поєднує протокол тунелювання другого рівня L2TP (Layer Two Tunneling Protocol) та засоби криптографічного захисту IPsec. L2TP призначений для транспортування кадрів PPP через IP-мережу, інкапсулюючи їх у UDP-датаграми, що дозволяє створювати логічні віртуальні канали. Сам по собі L2TP не забезпечує шифрування даних і не гарантує їх конфіденційність чи цілісність, тому на практиці його поєднують із IPsec, який додає шифрування, автентифікацію та захист від підміни й повторної передачі пакетів.

Процес встановлення захищеного каналу зв’язку між клієнтом та VPN-шлюзом відбувається у декілька послідовних етапів, де кожен рівень відповідає за свою частину захисту та транспортування даних [22]:

1. На першому етапі між вузлами (клієнтом та сервером) ініціюється обмін даними за протоколом IKE (Internet Key Exchange). Сторони узгоджують криптографічні алгоритми шифрування (наприклад, AES-256), методи хешування (наприклад, SHA-256), групи Diffie-Hellman (для генерації ключів), методи автентифікації (pre-shared key, сертифікати або RSA) та генерують спільні ключі безпеки.

Це відбувається у дві підфази:

- IKE Phase 1. Створюється захищений канал ISAKMP SA для управління. Обмін включає пропозиції політик, обмін ключами Diffie-Hellman, nonce та аутентифікацію сторін.

- IKE Phase 2. Узгоджуються параметри IPsec SA (для даних), включаючи протоколи ESP/AH та ключі для шифрування трафіку.

2. Створення логічного тунелю L2TP. Після того, як IPsec-з'єднання успішно встановлено і канал став захищеним, всередині нього запускається протокол L2TP (над UDP портом 1701). Він створює логічний між L2TP Access Concentrator (LAC, тобто клієнт) та L2TP Network Server (LNS, тобто сервер). Обмін контрольними повідомленнями (SCCRQ, SCCRP, SCCCN) включає аутентифікацію тунелю (за спільним секретом) та присвоєння ID тунелю.

3. Встановлення сесії L2TP та аутентифікація користувача. Усередині тунелю створюється сесія (session) для кожного PPP-з'єднання. Обмін (ICRQ, ICRP, ICCN) дозволяє проксі-аутентифікацію та перехід до узгодження параметрів PPP. На цьому етапі відбувається аутентифікація користувача через PPP (наприклад, MS-CHAPv2, CHAP або PAP), призначення IP-адреси та інших параметрів.

4. Транспортування PPP-кадрів. Всередині сформованого L2TP-тунелю передаються PPP-кадри, які містять безпосередній корисний трафік користувача. Це дозволяє використовувати стандартні механізми автентифікації та інкапсулювати трафік канального рівня (L2), роблячи його прозорим для мережі.

5. Забезпечення конфіденційності та цілісності (через IPsec з використанням ESP). Для захисту переданих пакетів використовується протокол ESP (Encapsulating Security Payload) в transport mode. Він забезпечує повне шифрування вмісту пакетів (включаючи L2TP + PPP), їх автентичність (HMAC), захист від повторного відтворення та інтеграцію з IPsec headers.

Нижче на рис.1.2 показано формат даних у захищеному L2TP/IPsec-тунелі. Можна побачити, що ESP інкапсулює L2TP-пакет, забезпечуючи шифрування та автентифікацію вмісту корисного навантаження, рис.1.4.

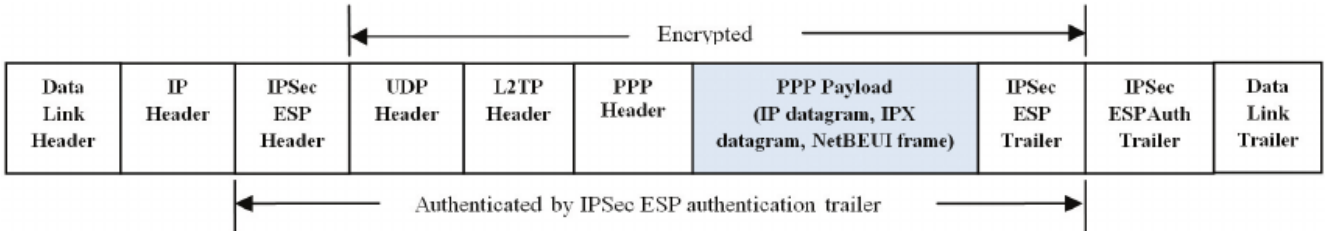


Рисунок 1.4 – Формат даних у тунелі L2TP/IPsec [23]

L2TP/IPsec активно застосовується для організації як віддаленого доступу користувачів, так і «site-to-site» з'єднань між філіями підприємства через публічний Інтернет. Порівняльні дослідження з іншими VPN-технологіями показують, що L2TP/IPsec забезпечує вищий рівень безпеки, ніж PPTP, завдяки більш стійким криптографічним засобам і продвинутим засобам захисту трафіку, хоча ці переваги досягаються ціною збільшення накладних витрат, більшої затримки та зниження пропускної здатності [24]. Попри це L2TP/IPsec залишається поширеним рішенням у корпоративних мережах, оскільки дозволяє використовувати існуючу інфраструктуру Інтернету, створюючи поверх неї логічно ізольовані й криптографічно захищені тунелі [25].

1.5 Постановка завдання дослідження

Сучасні корпоративні мережі функціонують в умовах постійного зростання кількості кібератак, переходу працівників на гібридні формати роботи та розширенням бізнесу і часто стикаються з питанням забезпечення безпечного, швидкого та гнучкого доступу до внутрішніх ресурсів. Це зрештою породжує низку викликів та важливих аспектів, які треба врахувати при розробці інфраструктури:

- запобігання перехопленню та витоку конфіденційної інформації в публічних мережах. Для прикладу, передача трафіку через канали MPLS, GRE або в чистому L2TP у відкритому вигляді створює високий ризик атак типу MitM, а застосування застарілих протоколів (PPTP) не гарантує криптографічної стійкості;
- оптимізація обчислювальних ресурсів та уникнення надмірного навантаження на системні ресурси маршрутизаторів, що вимагає обов'язкового використання платформ із підтримкою апаратного прискорення;
- централізація контролю доступу та інтеграцію мережних протоколів із корпоративними службами Active Directory для створення єдиної точки автентифікації користувачів та аудиту подій безпеки;
- економічну доцільність та мінімізацію витрат при масштабуванні.

Тому задля вирішення цих проблем запропоновано дослідити, спроєктувати та реалізувати захищену інфраструктуру розподіленої корпоративної мережі

організації на базі мережного обладнання MikroTik та технології тунелювання L2TP/IPsec. Використання L2TP у поєднанні з IPsec дозволить створити надійні захищені канали зв'язку, які мають широку сумісність із більшістю сучасних операційних систем без необхідності встановлення стороннього ПЗ.

Для досягнення поставленої мети передбачено виконання наступних завдань:

1. Аналіз підходів до побудови захищеної мережної інфраструктури організації з віддаленими підрозділами з використанням технологій VPN. Необхідно проаналізувати принципи роботи, класифікацію та архітектурні моделі VPN, провести порівняльну характеристику сучасних протоколів тунелювання та обгрунтувати переваги використання стеку L2TP/IPsec для забезпечення конфіденційності й цілісності даних в межах корпоративної мережі.

2. Розробка проєкту топології корпоративної мережі організації, вибір обладнання та програмних засобів. Завдання охоплює проєктування логічної та фізичної топологій розподіленої мережі організації, що охоплює віддалені філіали і користувачів та провести розробку схеми IP-адресації. Також необхідно обгрунтувати вибір мережного обладнання, серверу та кінцевих робочих станцій користувачів. Спроєктувати підсистему централізованої аутентифікації користувачів на базі Active Directory та RADIUS.

3. Розгортання проєкту захищеної мережної інфраструктури організації із використанням обраних рішень. Етап передбачає конфігурацію пристроїв інфраструктури в середовищі мережного емулятор GNS3, що включає: налаштування IP-адресації пристроїв, створення тунелів L2TP/IPsec між офісами та для віддаленими клієнтами, інтеграцію з Acitve Directory та RADIUS-сервером, а також налаштування механізмів безпеки та аудиту.

4. Тестування працездатності проєкту мережної інфраструктури та аналізу отриманих результатів. Наприкінці необхідно провести комплексне тестування мережної доступності між усіма сегментами організації, перевірити успішність автентифікації користувачів через Active Directory, а також проаналізувати криптографічний захист тунелів L2TP/IPsec за допомогою аналізатора трафіку Wireshark.

Висновки до першого розділу

У ході роботи над розділом встановлено, що безпека сучасної корпоративної мережі є динамічним процесом, який грунтується на фундаментальній тріаді CIA та вимагає відмови від застарілих моделей захисту периметра на користь архітектури «нульової довіри». І лише комплексна інтеграція політик контролю доступу та безпекових рішень дозволяє забезпечити стійкість бізнес-інфраструктури до складних цілеспрямованих кібератак.

У ході аналізу ринку мережного обладнання встановлено, що вибір оптимального рішення для малого та середнього бізнесу базується на балансі між вартістю, функціональністю та гнучкістю налаштувань. Порівняння ключових вендорів Cisco, Juniper, Fortinet та MikroTik показало, що продукція MikroTik займає унікальну нішу завдяки відсутності ліцензійних платежів та відкритій операційній системі RouterOS на базі Linux. Дослідження функціональних можливостей платформи підтвердило її високу ефективність у побудові захищених корпоративних мереж, а саме підтримка сучасних протоколів тунелювання, наявність брандмауера та інструментів QoS дозволяє реалізувати складні топології без значних витрат. Універсальність розгортання від апаратних рішень RouterBOARD до віртуалізованих систем CHR робить MikroTik найбільш адаптивною платформою для реалізації будь-яких проєктів.

В ході аналізу VPN-рішень було встановлено, що віртуальні приватні мережі є ключовим інструментом забезпечення безпеки в сучасних гетерогенних корпоративних середовищах. Порівняльний аналіз протоколів (SSTP, IKEv2/IPsec, OpenVPN, WireGuard та L2TP/IPsec) дозволив визначити L2TP/IPsec як найбільш оптимальне рішення для малого та середнього бізнесу завдяки його універсальній сумісності з основними операційними системами без додаткового ПЗ та підтримці роботи на обладнанні MikroTik. Незважаючи на додаткові обчислювальні витрати, пов’язані з подвійною інкапсуляцією, гнучкість у реалізації топологій Remote Access та Site-to-Site робить L2TP/IPsec перевіреним рішенням для побудови захищених тунелів поверх публічних каналів зв’язку.

Було виконано постановку завдання дослідження, що включало визначення актуальних викликів та важливих аспектів проєктування розподілених мереж, зокрема захисту, врахування системних ресурсів маршрутизаторів, централізації контролю доступу та економічної доцільності рішення. Сформовано перелік ключових завдань, які охоплюють повний цикл розробки проєкту від теоретичного аналізу підходів VPN до практичного розгортання топології в середовищі емулятора GNS3 та подальшому тестуванні розробленої мережі.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ІНФРАСТРУКТУРИ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Розробка мережної топології та адресації

Для проєктування захищеної корпоративної мережі організації часто застосовується трирівнева ієрархічна модель. Цей підхід є галузевим стандартом, який забезпечує необхідний рівень масштабованості, відмовостійкості та керованості. Модель традиційно визначається трьома шарами: ядро (Core), розподіл (Distribution) та доступ (Access). Ключовий принцип ієрархічного дизайну полягає в тому, що кожен елемент має чітко визначену роль і набір функцій, рис.2.1 [27].

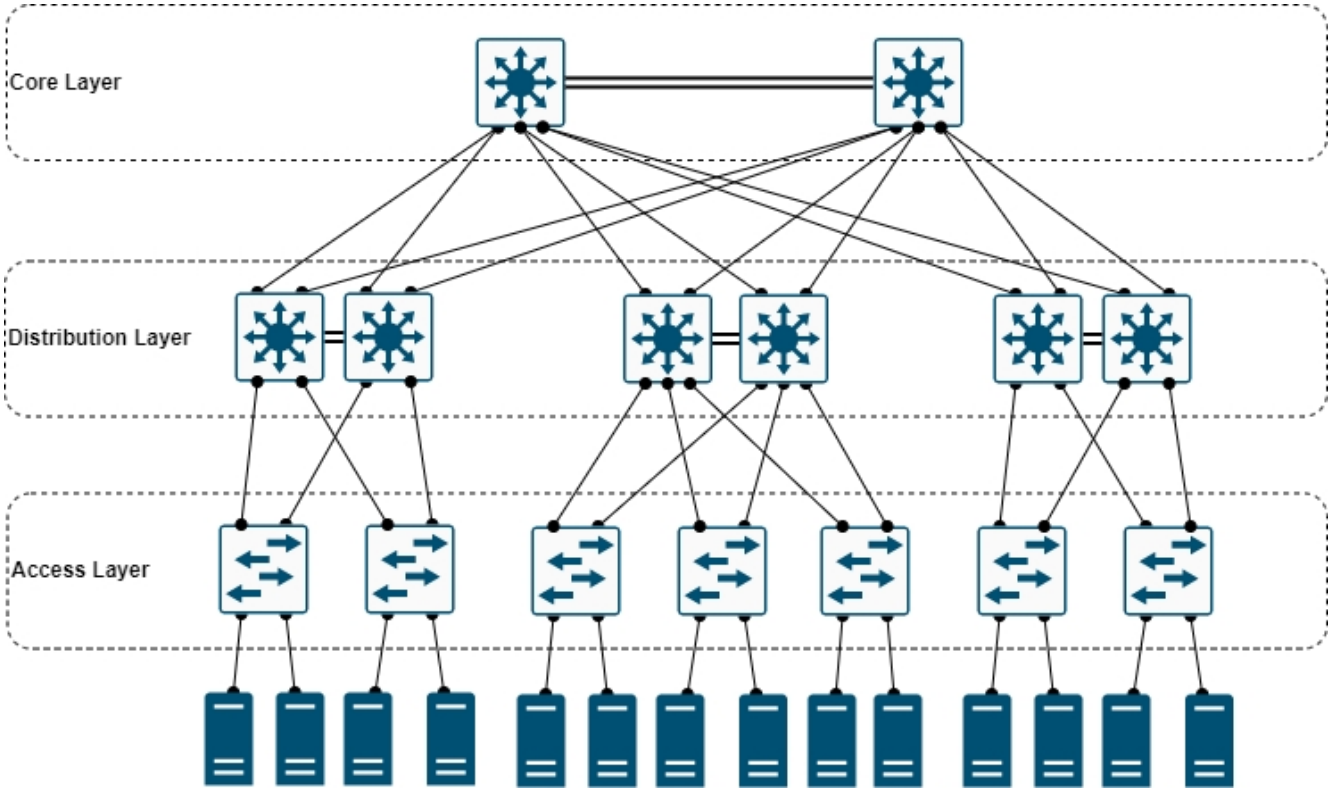


Рисунок 2.1 – Загальний приклад трирівневої ієрархічної моделі мережі

Рівень ядра є основою ієрархічної мережі, його головне призначення – забезпечення максимально швидкого та надійного транспортування трафіку між зовнішньою мережею та рівнем розподілу. Пристрої на цьому рівні (зазвичай високопродуктивні маршрутизатори або комутатори) повинні бути оптимізовані виключно для швидкості та відмовостійкості. Основні вимоги до рівня ядра

включають високу пропускну здатність, низьку затримку та відмовостійкість для забезпечення максимальної доступності.

Рівень розподілу виступає як межа між рівнем доступу та ядром. Його ключова функція здійснювати агрегацію трафіку з рівня доступу та застосувати мережні політики. На цьому рівні може виконуватись маршрутизація між різними локальними мережами, реалізуються політики якості обслуговування (QoS), а також ключові функції безпеки, включаючи фільтрацію трафіку за допомогою списків доступу. Крім того, пристрої рівня розподілу мають забезпечувати достатню надмірність каналів зв’язків для мережі доступу.

Рівень доступу є найнижчим рівнем ієрархії, що безпосередньо взаємодіє з кінцевими пристроями – робочими станціями, IP-телефонами, серверами та бездротовими точками доступу. Основне його завдання забезпечити підключення користувачів та контроль доступу до мережі. Функції, які тут реалізуються, включають комутацію Layer 2, а також початкові механізми безпеки, накшталт Port Security. Саме на цьому рівні закладаються основи для сегментації мережі, що є важливим для мінімізації поширення загроз.

Віртуальна приватна мережа (VPN) є концепцією, що дозволяє корпоративним компаніям із розподіленими офісами безпечно об'єднувати свої локальні мережі (LAN) через публічну мережу Інтернет. VPN дозволяє розширити корпоративну мережу до філій та віддалених місць, створюючи зашифровані тунелі, що забезпечують захищений доступ до корпоративних ресурсів у головному офісі. Основними перевагами використання VPN є безпека, масштабованість та економічна ефективність. Використання Інтернету для створення VPN-тунелів є значно дешевшою альтернативою, ніж дорогі приватні канали зв'язку, такі як орендовані лінії [28].

У корпоративній мережі використовують два основні типи VPN. Site-to-Site VPN забезпечує постійне безпечне з'єднання цілих мереж між головним офісом та віддаленими філіями. Це дозволяє філіям отримати доступ до центральних ресурсів, ніби вони є частиною внутрішньої LAN. З іншого боку, Remote Access VPN призначений для підключення окремих віддалених співробітників. Для цього

користувача на своїх комп’ютерах використовують спеціалізоване вбудований чи сторонній VPN-клієнт або стандартний браузер (для SSL VPN), що гарантує безперервність процесів та гнучкість підключення, дозволяючи організовувати зв’язок незалежно від фізичного розташування працівників.

Виходячи з проведеного аналізу було здійснено проєктування логічної топології організації, що складається центрального офісу, підрозділу А та віддаленого користувача, рис.2.2.

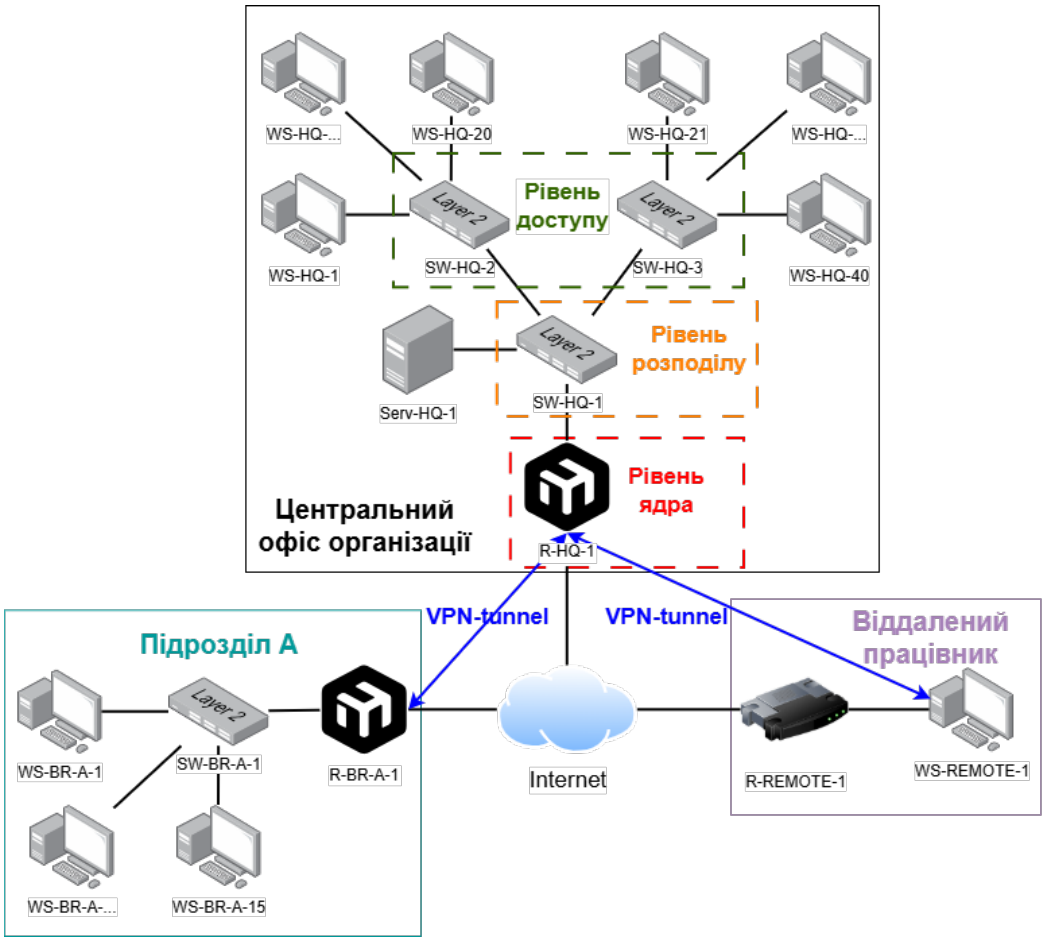


Рисунок 2.2 – Логічна топологія мережі

Центральний офіс побудований за принципами ієрархічної моделі та чітко розділений на три функціональні рівні.

- Рівень ядра представлений маршрутизатором R-HQ-1. Цей рівень забезпечує високошвидкісну комунікацію між рівнями розподілу та зовнішніми мережами. Він є точкою виходу до Інтернету та слугує VPN-сервером (VPN-шлюзом) для підключення віддаленого підрозділу А та користувача.

- Рівень розподілу представлений комутатором SW-HQ-1. Його функція виконувати агрегацію трафікк з рівня доступу та застосовувати політики безпеки перед передачею трафіку до ядра.
- Рівень доступу складається з комутаторів SW-HQ-2 та SW-HQ-3. Вони безпосередньо підключають кінцеві робочі станції співробітників (WS-HQ-…) загальною кількістю 20 одиниць.

Підрозділ А являє собою віддалену філію організації, яка інтегрована в корпоративну мережу через постійний захищений VPN-тунель типу «Site-To-Site». Інфраструктура підрозділу складається з маршрутизатора R-BR-A-1 та комутатора SW-BR-A-1, до якого підключені кінцеві робочі станції (WS-BR-A-…) кількість 10 одиниць. Для захищеного з'єднання з центральним офісом використовується L2TP/IPsec VPN-тунель. Цей тунель встановлюється між маршрутизатором R-BR-A-1 та маршрутизатором R-HQ-1, що дозволяє вільно і безпечно обмінюватись інформацією між усіма пристроями корпоративної мережі.

Віддалений користувач представляє собою індивідуального співробітника, який знаходиться в себе вдома та інтегрований в мережу організації через захищений VPN-тунель типу «Remote Access». Мережа користувача представляє собою домашній маршрутизатор R-REMOTE-1, який забезпечує вихід до Інтернету та комп'ютера WS-Remote-1. Для доступу до корпоративної мережі використовується L2TP/IPsec VPN-тунель, при цьому підключення ініціюється прямо з робочої станції WS-Remote-1 використовуючи вбудований VPN-клієнт.

Загальна кількість мережних пристроїв в проєкті становить 8 одиниць (3 маршрутизатори та 5 комутаторів), які обслуговують мінімум 31 робочу станцію у трьох різних локаціях. Спроєктована архітектура дозволяє швидко і зручно виконати масштабування мережі організації за рахунок використання трирівневої моделі мережі в центральному офісі та можливості долучення нових віддалених компонентів через створення L2TP/IPsec VPN-тунелів.

Адресація мережі є важливим етапом проєктування корпоративної інфраструктури, оскільки саме вона визначає логічну організацію всіх підключень. Правильний підхід до вибору та структурування IP-адрес забезпечує

продуктивність та масштабованість мережі, а також має прямий вплив на її безпеку та ефективність адміністрування.

Для каналів зв’язку з мережею Інтернет буде виділено 3 підмережі:

25.222.1.0/30 – канал R-HQ-1 та Internet;

25.222.2.0/30 – канал R-BR-A-1 та Internet

25.222.3.0/30 – канал R-REMOTE-1 та Internet

І також необхідно 3 локальні підмережі:

172.22.1.0/24 – в центральному офісі;

172.22.2.0/24 – в підрозділі А;

192.168.22.0/24 – у віддаленого працівника.

Для роботи VPN відведено мережу 10.222.22.0/24. При чому маршрутизатор головного офісу R-HQ-1 матиме постійну адресу 10.222.22.1, а пристрій філіалу R-BR-A-1 адресу 10.222.22.2. Віддалені користувачі отримуватимуть параметри мережні параметри динамічно з визначеного пулу.

Розрахунок IP-адрес для центрального офісу та підрозділу А наведено нижче на табл. 2.1-2.2.

Таблиця 2.1

Адресація локальної мережі центрального офісу

Призначення адрес	IP-адреса
Адреса мережі	172.22.1.0
Маска мережі	255.255.255.0
Мінімальна адреса	172.22.1.1
Максимальна адреса	172.22.1.254
Шлюз за замовчуванням	172.22.1.1
Призначені комутаторам	172.22.1.2 – 172.22.1.4
Призначені серверу	172.22.1.99
Діапазон адрес робочих станцій	172.22.1.100 – 172.22.1.119
Діапазон незайнятих адрес	172.22.1.5 – 192.168.1.99, 172.22.1.121 – 192.168.1.254,

Таблиця 2.2

Адресація локальної мережі підмережі А

Призначення адрес	IP-адреса
Адреса мережі	172.22.2.0
Маска мережі	255.255.255.0
Мінімальна адреса	172.22.2.1
Максимальна адреса	172.22.2.254
Шлюз за замовчуванням	172.22.2.1
Призначені комутаторам	172.22.2.2
Діапазон адрес робочих станцій	172.22.2.100 – 172.22.2.109
Діапазон незайнятих адрес	172.22.2.3 – 192.168.1.99, 172.22.2.111 – 192.168.1.254,

Повна фізична топології мережі представлена нижче на рис.2.3.

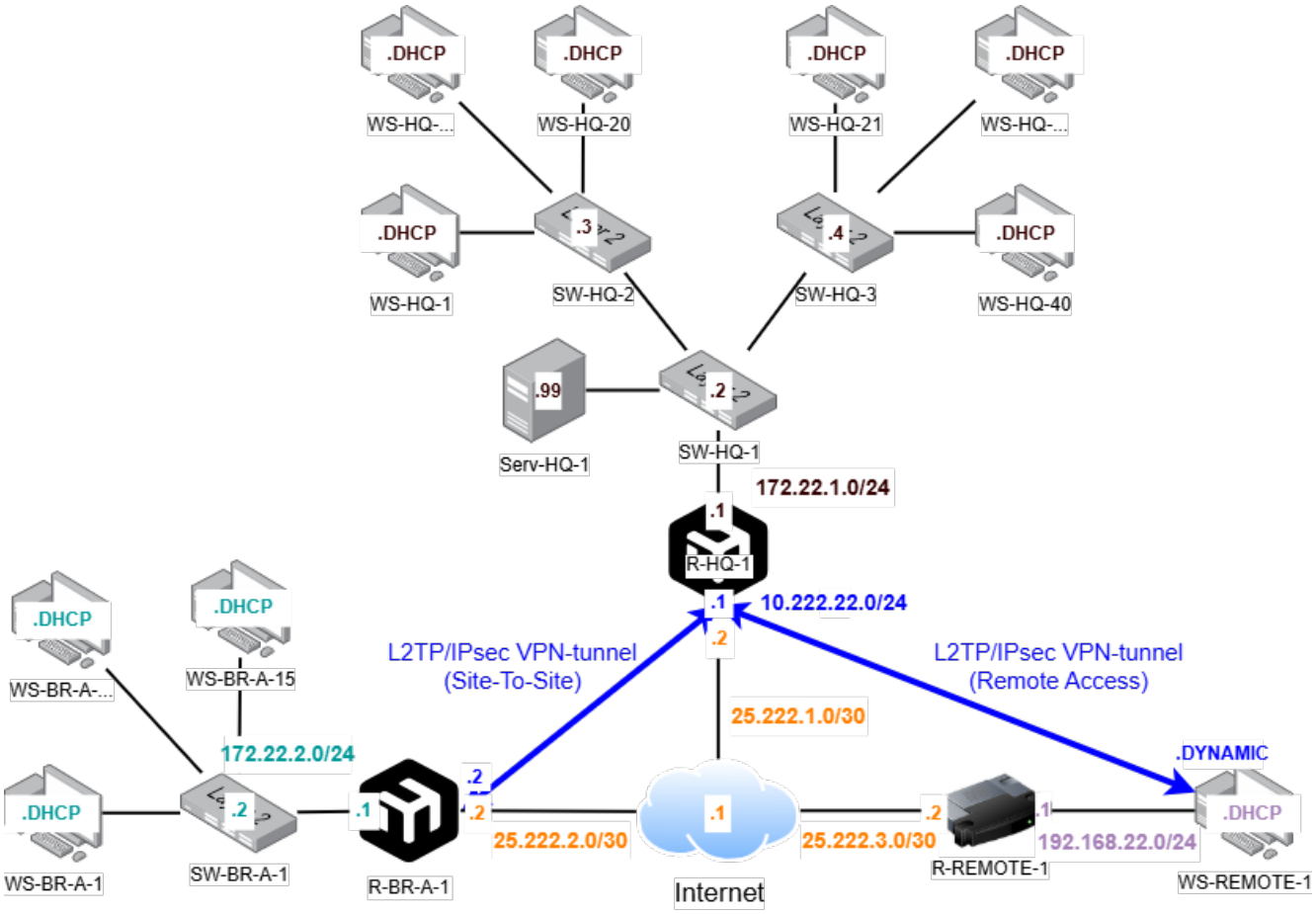


Рисунок 2.3 – Фізична топологія мережі з адресацією

2.2 Механізм централізованої автентифікації RADIUS для VPN

Для забезпечення масштабованості та високого рівня безпеки в проєкті мережі передбачено використання механізму централізованої автентифікації RADIUS, де процес створення кожного VPN-тунелю віддаленого користувача керується внутрішнім сервером. Згідно з розробленою схемою, рис.2.4, взаємодія між компонентами мережі базується на делегуванні повноважень перевірки користувачів від маршрутизатора R-HQ-1 до контролера домену, тобто Serv-HQ-1.

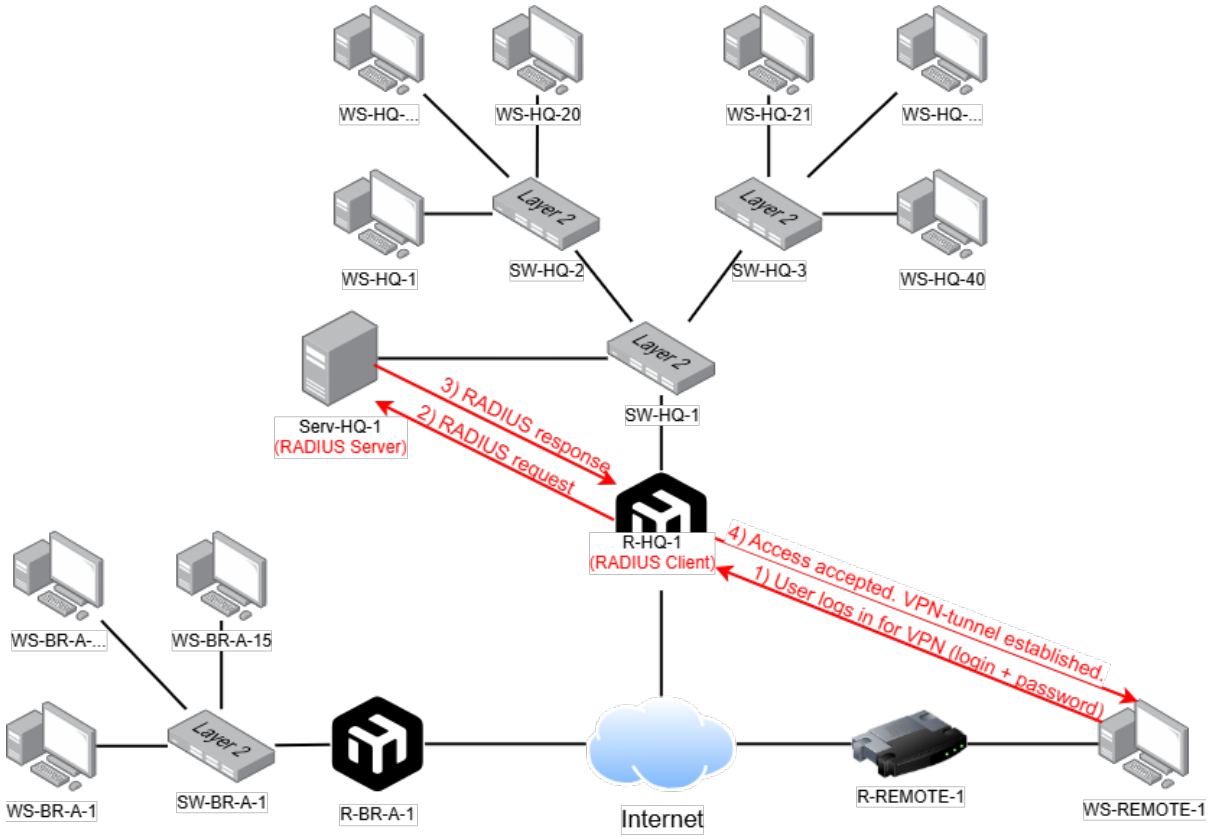


Рисунок 2.4 – Фізична топологія мережі з адресацією

Покроково розберемо загальний принцип роботи даного механізму на прикладі підключення віддаленої станції WS-REMOTE-1.

Кроки 1-2. Віддалений користувач WS-REMOTE-1 ініціює запит на встановлення L2TP/IPsec з'єднання, надсилаючи відповідні ідентифікаційні дані (логін та пароль) до маршрутизатора R-HQ-1. Отримавши цей запит, роутер, що виступає в ролі RADIUS-клієнта, призупиняє процес формування тунелю та інкапсулює отримані дані у пакет RADIUS Request, який перенаправляється на

сервер Serv-HQ-1. Сервер виконує валідацію облікового запису через Active Directory, перевіряючи не лише пароль, а й відповідність політикам доступу.

Крок 3. Після перевірки сервер повертає роутеру пакет RADIUS Response. Саме ця відповідь слугує командою для R-HQ-1 завершити переговори за протоколом L2TP та запустити роботу віртуального інтерфейсу. Окрім дозволу, RADIUS-сервер може передавати специфічні атрибути для тунелю, зокрема фіксовану внутрішню IP-адресу для конкретного співробітника, привілеї доступу або параметри маршрутизації, що дозволяє динамічно керувати конфігурацією кожного окремого VPN-підключення.

Крок 4. Завершальний етап створення тунелю супроводжується активацією захисту тунелю за допомогою стеку IPsec, що гарантує конфіденційність та цілісність переданих даних. Такий підхід до планування дозволяє розв'язати проблему розрізненого керування користувачами, оскільки всі операції з автентифікації при створенні L2TP-тунелів зосереджені в єдиній точці керування на сервері Serv-HQ-1, що значно підвищує керованість та аудит безпеки всієї корпоративної мережі.

Застосування даного механізму взаємодії з RADIUS дозволяє централізовано керувати доступом, швидко долучати нових віддалених користувачів до мережі та мінімізувати ризики компрометації облікових даних. А в разі чого мати можливість швидко обмежити доступ підключення для того чи іншого користувача.

2.3 Вибір апаратної бази мережі

При виборі маршрутизаторів для центрального офісу (R-HQ-1) та Підрозділу А (R-BR-A-1) важливо враховувати їхню здатність підтримувати протоколи L2TP/IPsec та забезпечувати достатню швидкість передачі даних через VPN-тунелі. Основними критеріями є продуктивність IPsec, оскільки шифрування та дешифрування трафіку вимагає значних обчислювальних ресурсів процесора. Також необхідно врахувати достатня пропускна здатність інтерфейсів (не менше 1 Гбіт/с) для швидкої обробки локального та зовнішнього трафіку. Також пристрої

повинні мати достатній обсяг оперативної пам'яті (RAM) та потужний багатоядерний центральний процесор.

Тому на роль маршрутизаторів було обрано модель Mikrotik RB4011iGS, рис.2.5. Це високопродуктивний гігабітний маршрутизатор, розроблений для великих і малих підприємств, що вимагають значної пропускної здатності та надійності. Він оснащений потужним 4-ядерним процесором AL21400 (1.4 ГГц) від Annapurna Labs (Amazon), ідентичним тому, що використовується в RB1100AHx4, та має 1 ГБ оперативної пам'яті, що забезпечує гнучкість для реалізації будь-яких конфігурацій RouterOS . Маршрутизатор пропонує достатню кількість інтерфейсів: 10 гігабітних Ethernet-портів і один оптичний порт SFP+ для підключення 10 Гбіт/с (модуль SFP+ купується окремо). Пристрій також підтримує функціонал PoE. Завдяки апаратному прискоренню IPsec пристрій може досягати швидкості тунелю AES-256-CBC + SHA256 до 2 Гбіт/с, а загальна пропускна здатність комутації може сягати 9.7 Гбіт/с. І вся це розміщено в компактному, матовому чорному корпусі, який постачається з двома стійковими вухами для встановлення у стійку 1U [29].



Рисунок 2.5 – Маршрутизатор MikroTik RB4011iGS

При виборі моделі комутатора слід звернути увагу, щоб вона підтримувати хоча б Fast Ethernet (100 Мбіт/с) на портах доступу для підключення робочих станцій, забезпечуючи при цьому достатню швидкість Uplink-портів (бажано 1 Гбіт/с) для зв'язку з маршрутизатором і серверами. Важливим є і підтримка технології VLAN (IEEE 802.1Q) для можливості логічного розділення мережі та ефективного контролю широкомовного трафіку. Додатковими важливими параметрами є підтримка PoE (Power over Ethernet) для живлення IP-телефонів чи

точок доступу та загальна комутаційна ємність, достатня для обробки сукупного трафіку всіх підключених пристроїв.

Тому, зважаючи на наведені характеристики, було обрано модель комутатора Cisco CBS350-24T-4X-EU, що належить до нової серії Cisco Business 350, рис.2.6. Вибір обладнання Cisco замість комутаторів компанії MikroTik зумовлений зумовлений його вищою продуктивністю та архітектурними особливостями систем захисту на рівні доступу. Комутатори Cisco традиційно мають апаратно інтегрований та стандартизований набір функцій локальної безпеки (таких як Port Security, DHCP Snooping, Dynamic ARP Inspection). Лінійка Cisco Business 350 є продовженням високопродуктивних, безпечних та керованих комутаторів, спеціально розроблених для малого та середнього бізнесу. Комутатори серії 350 є ідеальним рішенням для швидкого створення ефективної та захищеної корпоративної мережі, оскільки вони прості у розгортанні, мають інтуїтивно зрозумілу панель моніторингу, що спрощує налаштування, та підтримують розширені функції, які прискорюють цифрову інтеграцію. Модель CBS350-24T-4X-EU оснащена 24 портами Fast Ethernet / Gigabit Ethernet (10/100/1000 Мбіт/с), що забезпечує достатню кількість портів для підключення робочих станцій, а також чотирма портами 10G SFP+ для високошвидкісних Uplink-з'єднань із маршрутизатором та серверами. Пристрій підтримує комутацію 2-го рівня, технологію VLAN, розширений захист від загроз IPv6 та статичну маршрутизацію IPv4/IPv6, що дозволяє йому ефективно виконувати роль керованого комутатора доступу з підтримкою SVI (Switch Virtual Interface) і QoS (якість обслуговування). Крім того, конструкція без вентиляторів забезпечує його тиху роботу та можливість встановлення в офісних приміщеннях [30].



Рисунок 2.6 – Комутатор Cisco CBS350-24T-4X-EU

Для головного сервера корпоративної мережі, представленого на схемі як Serv-HQ-1, у ролі серверної операційної системи обрано Windows Server. Вибір даної платформи дозволить забезпечити стабільну роботу критично важливих служб, таких як контролер домену (Active Directory), DHCP, DNS та файлові сервіси, пропонуючи при цьому сучасні механізми захисту даних і багаторівневу систему безпеки. Для стабільного функціонування сервера доцільно обрати наступну апаратна конфігурацію, що має включає чотириядерний або шестиядерний серверний процесор (наприклад, Intel Xeon Silver), не менше 32 ГБ оперативної пам'яті, а також накопичувачі на базі NVMe SSD об'єднаних у RAID-масив для забезпечення відмовостійкості та високої швидкості обробки запитів. Використання такої конфігурації гарантує необхідну продуктивність для обслуговування запитів кінцевих користувачів.

В якості операційної системи для робочих станцій обрано ОС Windows 11 Pro, оскільки ці версії забезпечують високий рівень безпеки, необхідний для корпоративного середовища, підтримують ключові мережні функції (як-от можливість приєднання до домену), а також мають широку сумісність із програмним забезпеченням. Для забезпечення комфортної та продуктивної роботи співробітників у мережі, мінімальні технічні параметри комп'ютерів мають включати: чотириядерний процесор (наприклад, Intel Core i3 або AMD Ryzen 3), не менше 8 ГБ оперативної пам'яті (RAM), а також твердотільний накопичувач (SSD) об'ємом від 256 ГБ. Використання SSD є критичним для прискорення завантаження системи та застосунків, що безпосередньо впливає на швидкість виконання робочих завдань.

2.4 Вибір механізмів захисту мережної інфраструктури

Для забезпечення високого рівня інформаційної безпеки та надійності корпоративної мережі планується впровадження комплексної системи захисту, яка охоплюватиме як канальний, так і прикладний рівні мережної моделі. Основна увага буде приділена створенню захищених каналів зв'язку для віддалених точок, централізації механізмів автентифікації та розгортанню засобів безперервного

моніторингу, що дозволить мінімізувати ризики несанкціонованого втручання та забезпечити цілісність переданих даних.

- L2TP/IPsec. Для побудови захищених VPN-каналів з головним буде налаштовано протокол L2TP з шифруванням IPsec, що дозволить безпечно інкапсулювати корпоративний трафік і захистити його від перехоплення в публічних мережах за допомогою стійкого алгоритму шифрування AES.
- Active Directory. У проекті передбачено розгортання служби каталогів як єдиного центру керування ідентифікацією, що дозволить системним адміністраторам централізовано впроваджувати політики безпеки та керувати правами доступу користувачів до всіх вузлів домену klymchuk.net.
- RADIUS. Для інтеграції мережного обладнання з доменною структурою буде використано протокол RADIUS, який забезпечуватиме перевірку повноважень користувачів при підключенні до VPN або SSH, усуваючи необхідність локального збереження конфіденційних даних на маршрутизаторах і комутаторах.
- Syslog. З метою оперативного реагування на інциденти буде розгорнуто сервер Syslog для централізованого збору та аналізу журналів подій, що дозволить зберігати повну історію дій користувачів, спроб входу в систему та змін у конфігурації обладнання.
- SSH. Віддалене адміністрування пристроїв здійснюватиметься виключно через протокол SSH версії 2, який забезпечить надійне шифрування сесій керування та захистить від мережного прослуховування.
- Firewall. На всіх маршрутизаторах MikroTik за замовчуванням уже встановлено базовий набір правил міжмережного екрана, які працюють за принципом «заборонити все, що не дозволено явно». Це включає блокування всіх зовнішніх запитів та дозволятиме проходження трафіку лише через зазначені порти та протоколи.
- Відключення незадіяних портів. На фізичному рівні безпеки буде проведено аудит усіх комутаторів з подальшим програмним вимкненням вільних

портів, що унеможливить несанкціонований фізичний доступ сторонніх пристроїв до локальної мережі компанії.

Висновки до другого розділу

У ході розробки другого розділу було спроєктовано захищену ієрархічну структуру корпоративної мережі, що базується на трирівневій моделі. Сформовано логічну та фізичну топології. Було розроблено схему адресації відповідно до необхідної кількості пристроїв. Встановлено, що використання протоколу RADIUS дозволяє реалізувати централізовану систему керування доступом, де делегування повноваження перевірки користувачів передається серверу. Запропонований механізм взаємодії забезпечує безпечну передачу ідентифікаційних даних віддалених станцій до контролера домену Active Directory, що дозволяє не лише валідувати паролі, а й динамічно призначати VPN-атрибути.

Було проведено підбір апаратної бази для реалізації проєкту мережі. Це включало маршрутизатори MikroTik RB4011iGS, комутатори Cisco CBS350-24T-4X-EU, сервер на базі Windows Server та робочі станції під управлінням Windows, що разом формують цілісну екосистему.

Завершуючи розробку другого розділу, визначено комплекс механізмів захисту, що формують захист корпоративної інфраструктури. Основою безпеки трафіку є використання протоколу L2TP/IPsec із шифруванням AES для захищених тунелів, централізовану автентифікацію RADIUS, інтегровану зі службою каталогів Active. Технічна реалізація передбачає використання міжмережного екрану на пристроях MikroTik за принципом «Default Deny» і використання захищеного протоколу SSH версії 2 для адміністрування. Впровадження Syslog для централізованого логування дозволяє забезпечити прозорий аудит усіх процесів усередині мережі.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ MIKROTIK ТА ТЕХНОЛОГІЇ L2TP/IPSEC

3.1 Базова конфігурація пристроїв мережі

Подальше налагодження та перевірка функціональної працездатності спроєктованої мережної інфраструктури, зокрема образів маршрутизаторів MikroTik, буде виконано з використанням мережного емулятора GNS3. Даний емулятор дає змогу змоделювати та протестувати комп'ютерну топологію інтегруючи реальні образи операційних систем обладнання, зокрема Cisco IOS, MikroTik RouterOS, Windows. Використання GNS3 дозволить покроково провести налаштування параметрів пристроїв мережу, схему адресації та налаштувати та перевірити коректність функціонування VPN-тунелів Цей підхід дасть можливість найбільш точніше відтворити робоче середовище без використання фізичний мережних пристроїв. Складений проєкт мережі наведено нижче на рис.3.1.

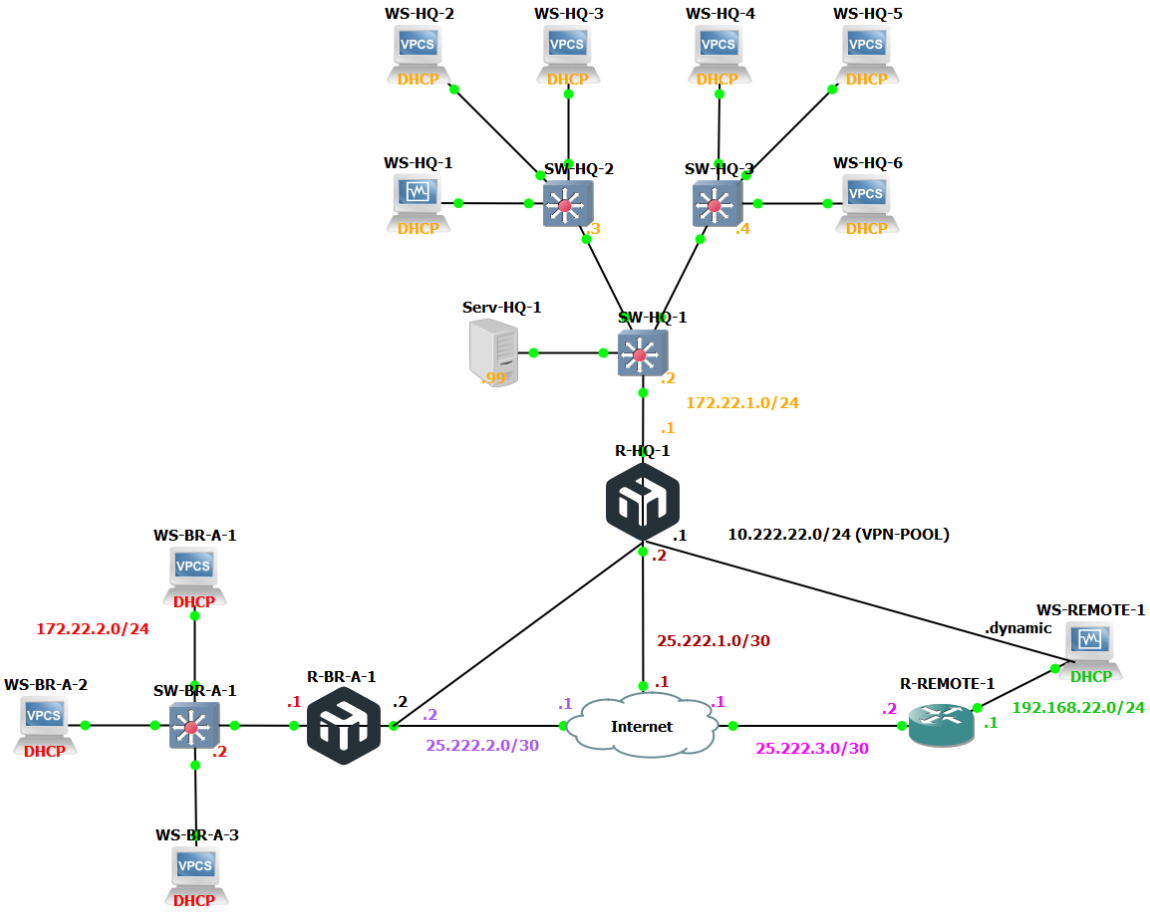


Рисунок 3.1 – Складена схема проєкту мережі в емуляторі GNS3

Почнемо налаштування з комутаторів. Для прикладу розглянемо цей процес на комутаторі SW-HQ-1, але інші пристрої налаштовуються подібним чином. Для початку слід задати відповідне ім’я, що полегшить його ідентифікацію в мережі. Після цього виконується конфігурація інтерфейсу VLAN 1 як інтерфейсу управління, якому присвоюється IP-адреса 172.22.1.2 з маскою 255.255.255.0. Для забезпечення зв’язку з іншими сегментами мережі вказується шлюз за замовчуванням (172.22.1.1), а для коректного вирішення мережних імен активується функція domain-lookup, задається доменне ім’я klymchuk.net та вказується адреса DNS-сервера 172.22.1.99, роль якого в мережі виконує сервер Serv-HQ-1, рис.3.2.

```
SW-HQ-1(config)#no ip routing
SW-HQ-1(config)#hostname SW-HQ-1
SW-HQ-1(config)#int vlan 1
SW-HQ-1(config-if)#ip address 172.22.1.2 255.255.255.0
SW-HQ-1(config-if)#no shutdown
SW-HQ-1(config-if)#exit
SW-HQ-1(config)#ip default-gateway 172.22.1.1
SW-HQ-1(config)#ip domain-lookup
SW-HQ-1(config)#ip domain-name klymchuk.net
SW-HQ-1(config)#ip name-server 172.22.1.99
```

Рисунок 3.2 – Налаштування комутатора SW-HQ-1

Перейдемо до сервера головного офісу, тобто Serv-HQ-1. Йому було присвоєно статичну IP-адресу 172.22.1.99 із маскою 255.255.255.0. Як основний шлюз вказано адресу 172.22.1.1, що відповідає внутрішньому інтерфейсу R-HQ-1, рис.3.3.

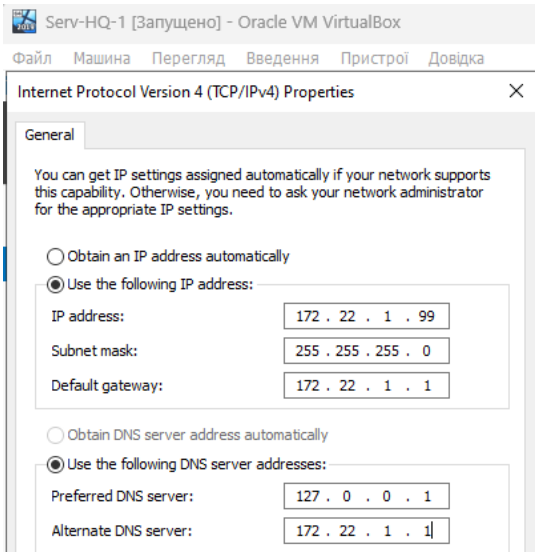


Рисунок 3.3 – Налаштування станції WS-HQ-1

Продовжуючи налаштування сервера, через майстра «Add Roles and Features Wizard» було обрано наступні ролі, а саме Active Directory Domain Services для керування користувачами, а також DHCP та DNS Server для автоматизації адресації та вирішення імен у домені klymchuk.net. Також було активовано роль Network Policy and Access Services (NPS), яка забезпечуватиме роботу RADIUS-сервера, рис.3.4.

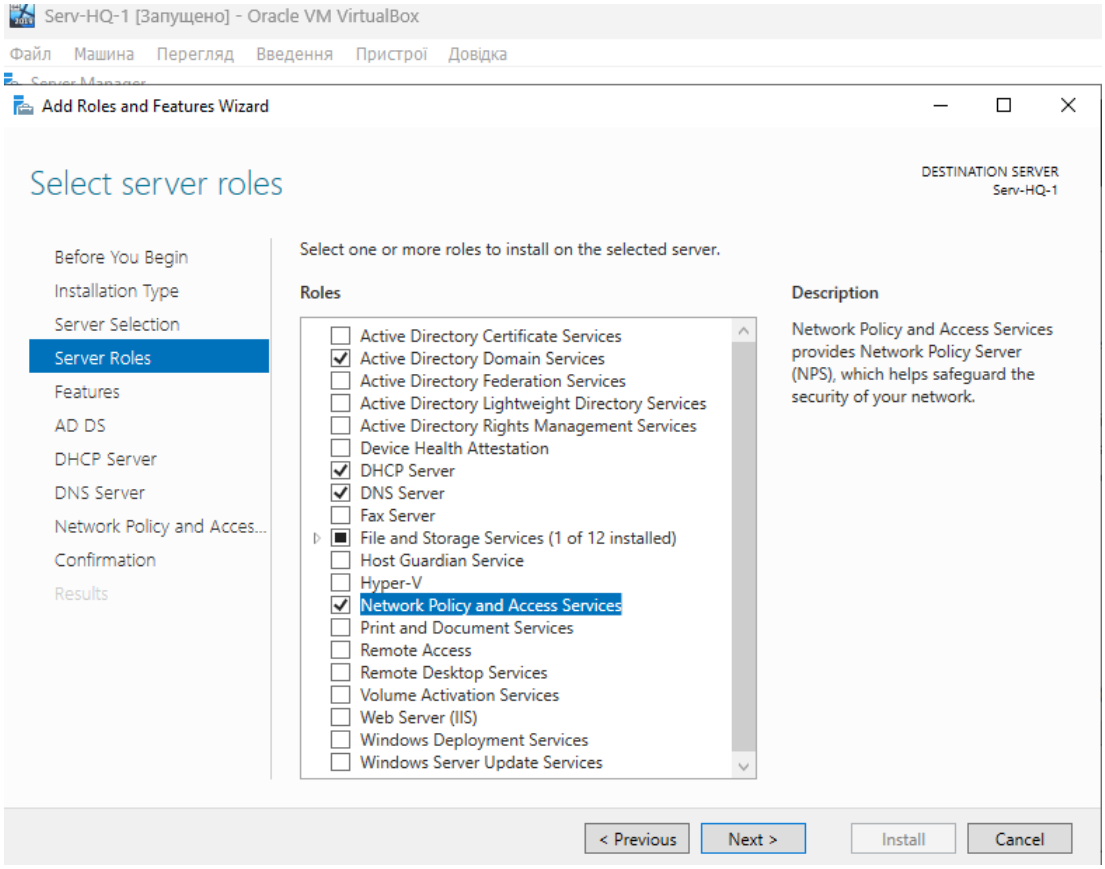


Рисунок 3.4 – Вибір серверних ролей

Після інсталяції необхідних ролей та перезавантаження серверу, наступним етапом є безпосередня конфігурація доменного середовища. За допомогою майстра «Active Directory Domain Services Configuration Wizard» було ініційовано створення нового лісу (Add a new forest) з кореневим доменним іменем klymchuk.net, рис.3.5. Створення власного доменного простору є необхідною умовою для коректної взаємодії мережних сервісів, групових політик, ідентифікації користувачів і адміністрування ресурсів в корпоративному середовищі.

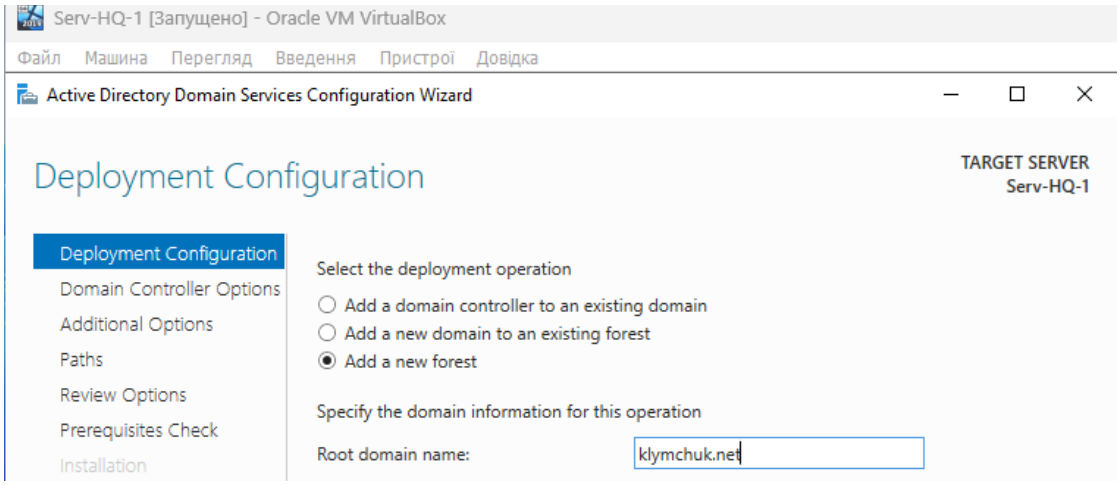


Рисунок 3.5 – Розгортання нового доменного лісу klymchuk.net.

Наступним кроком стала конфігурація сервісу DHCP. В рамках цього на сервері було створено область HQ-LAN-POOL. Задля запобігання конфліктам адрес було встановлено діапазон виключень для статичних IP від 172.22.1.1 до 172.22.1.99, а також визначено шлюз за замовчуванням 172.22.1.1 та параметри DNS-сервера з адресою 172.22.1.99, рис.3.6-3.9. Правильне налаштування DHCP-сервера дозволяє автоматизувати процес підключення клієнтських станцій до доменного середовища, що є важливим для надійної роботи корпоративної інфраструктури.

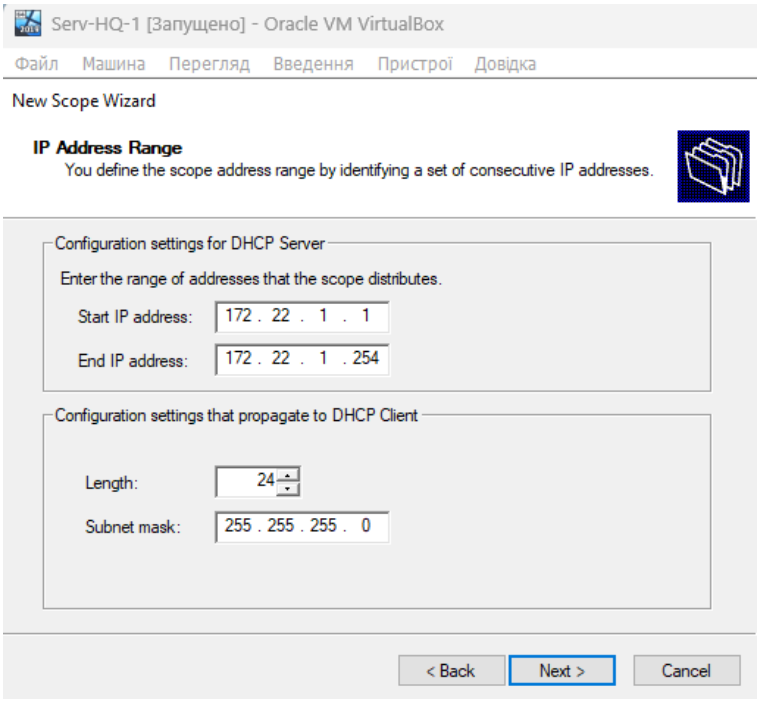


Рисунок 3.6 – Визначення діапазону адрес та маски підмережі

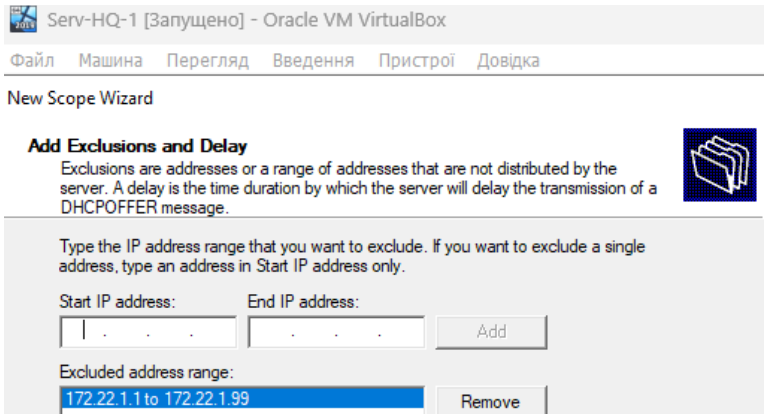


Рисунок 3.7 – Конфігурація діапазону виключень для статичних IP-адрес

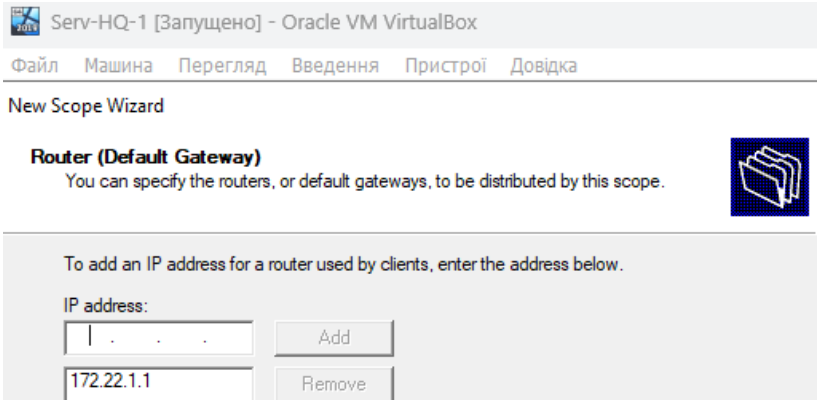


Рисунок 3.8 – Налаштування шлюзу за замовчуванням для клієнтів

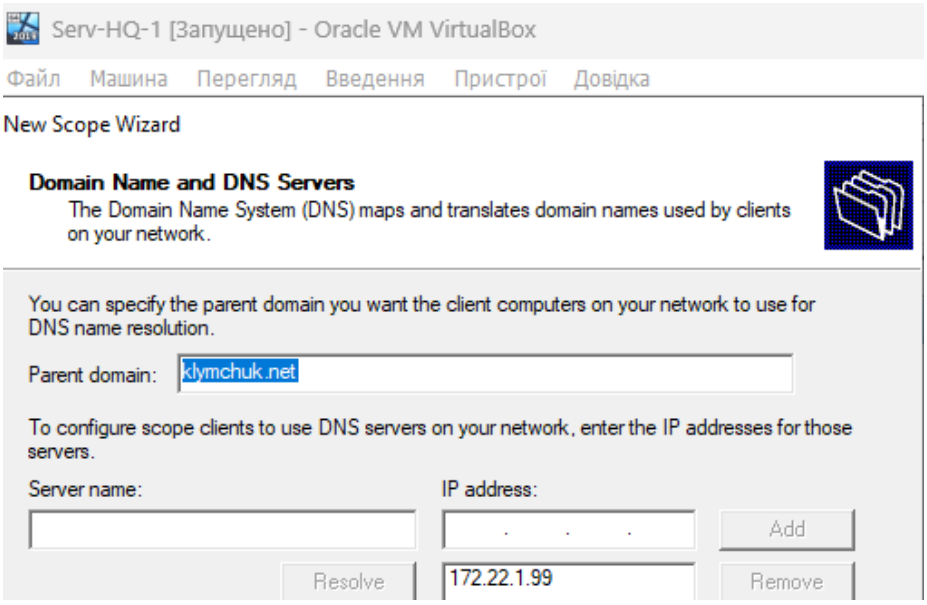


Рисунок 3.9 – Налаштування DNS-серверу для клієнтів

Далі було виконано наповнення зони прямого перегляду в DNS Manager для забезпечення коректної роздільної здатності імен у домені klymchuk.net. В ході цього було створено статичні записи типу Host (A) для всіх ключових вузлів інфраструктури, зокрема для комутаторів та маршрутизаторів. Це дозволяє мережним службам та адміністраторам звертатися до обладнання за їх іменами замість IP-адрес, що спрощує процес взаємодії між обладнанням, рис.3.10.

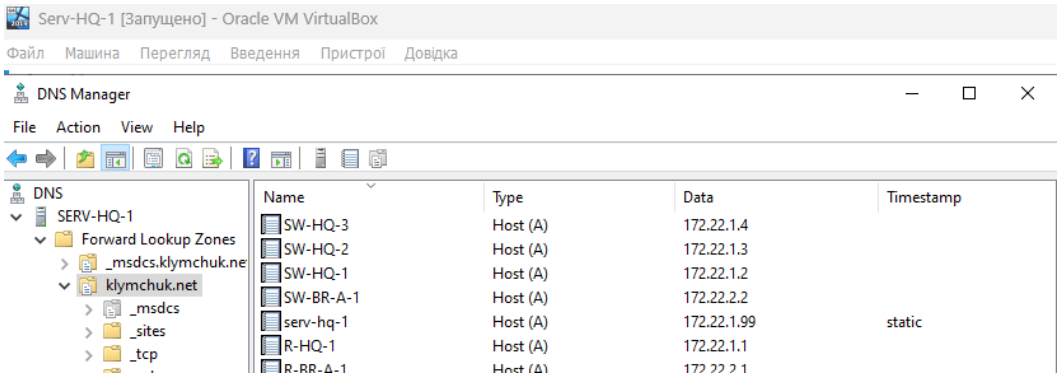


Рисунок 3.10 – Створення записів типу Host (A) для статичних пристроїв

На завершальному було створено організаційний підрозділ DOMAIN-USERS, у якому сформовано базу облікових записів співробітників. Створення облікових записів дозволяє гнучко налаштовувати групові політики безпеки та використовувати ці дані при вході в систему на робочих станціях, рис.3.11-3.12.

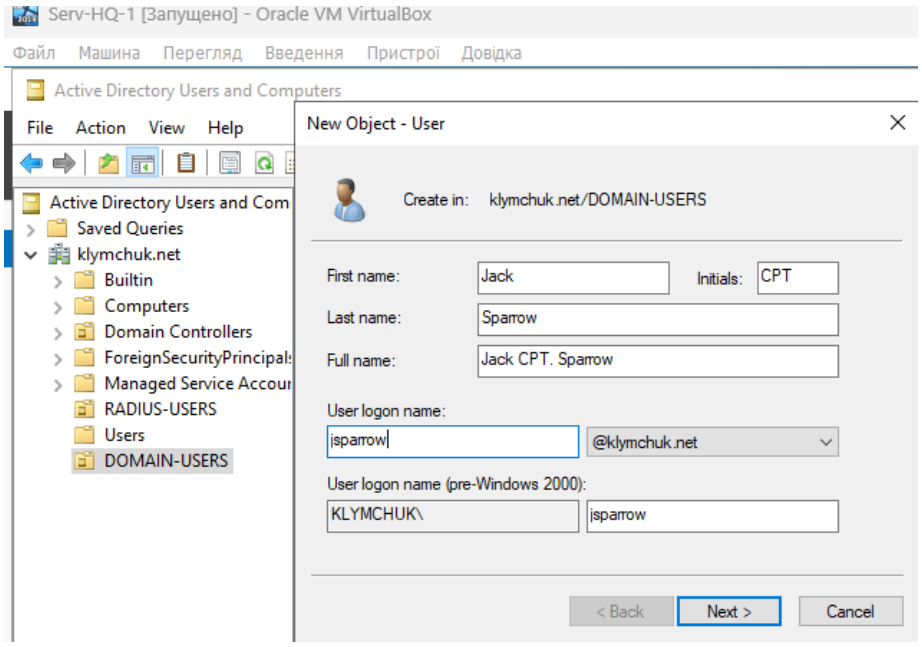


Рисунок 3.11 – Створення нового користувача

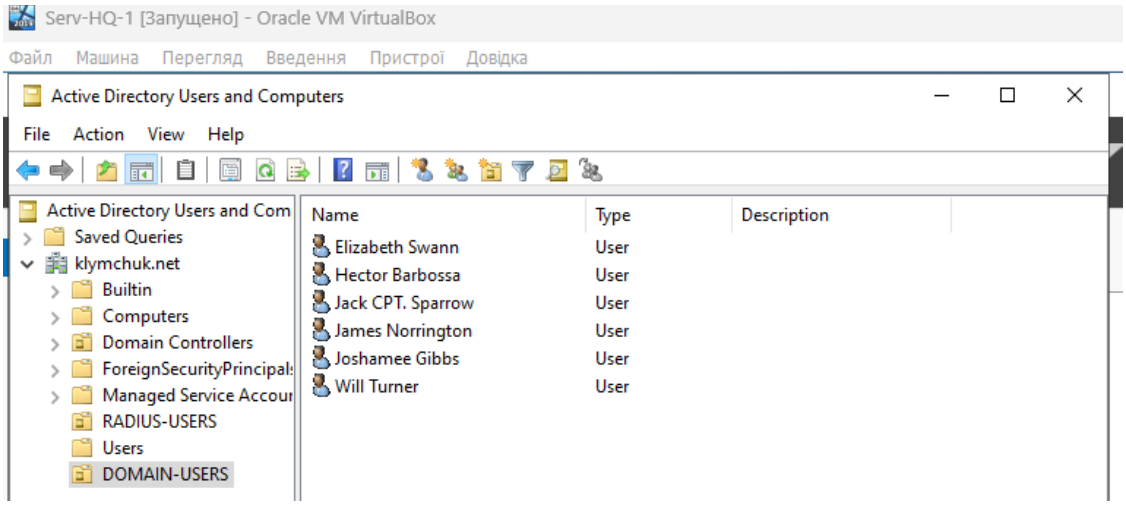


Рисунок 3.12 – Перелік облікових записів користувачів у домені

Перейдемо до робочих станцій в головному офісі, для прикладу розглянемо WS-HQ-1. Завдяки роботі розгорнутого раніше DHCP-сервера, пристрій автоматично отримав IP-адресу 172.22.1.100 із відповідною маскою підмережі 255.255.255.0, рис.3.13.

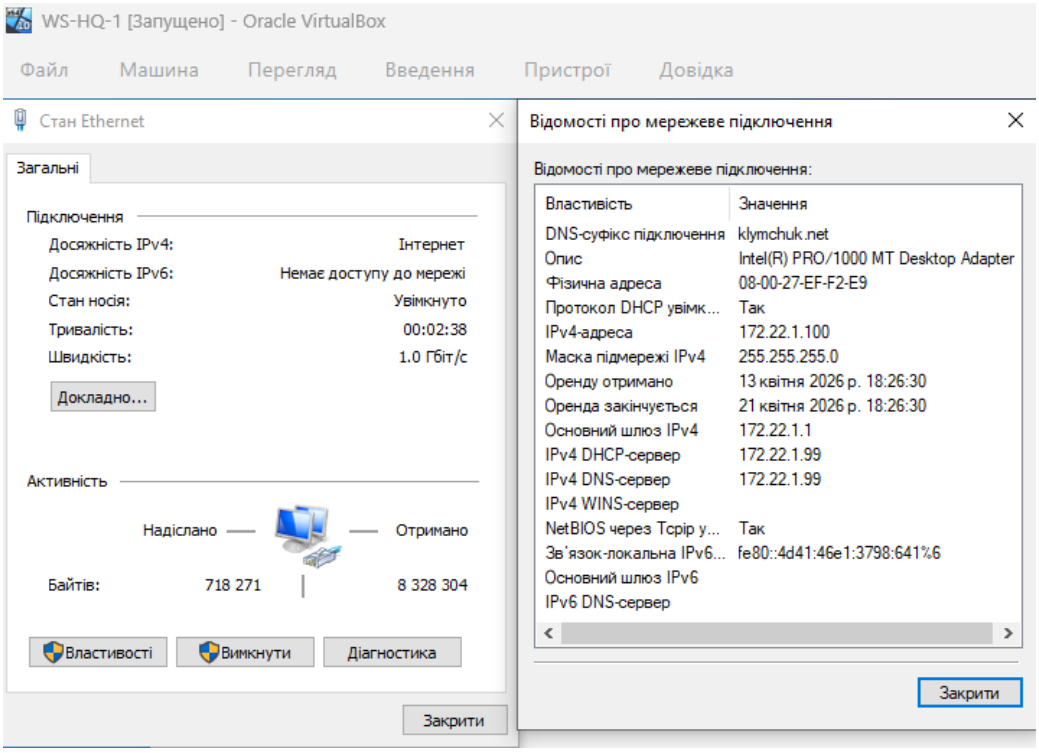


Рисунок 3.13 – Перевірка мережних параметрів робочої станції

Після успішного отримання мережних параметрів робочі станції готові до приєднання до домену. На прикладі станції WS-HQ-1 було змінено її участь з

робочої групи на домен klymchuk.net, рис.3.15. Після перезавантаження комп'ютера було виконано вхід в систему з використання раніше створеного доменного облікового запису користувача, що свідчить про повноцінне та успішне підключення станції до домену, рис.3.15.

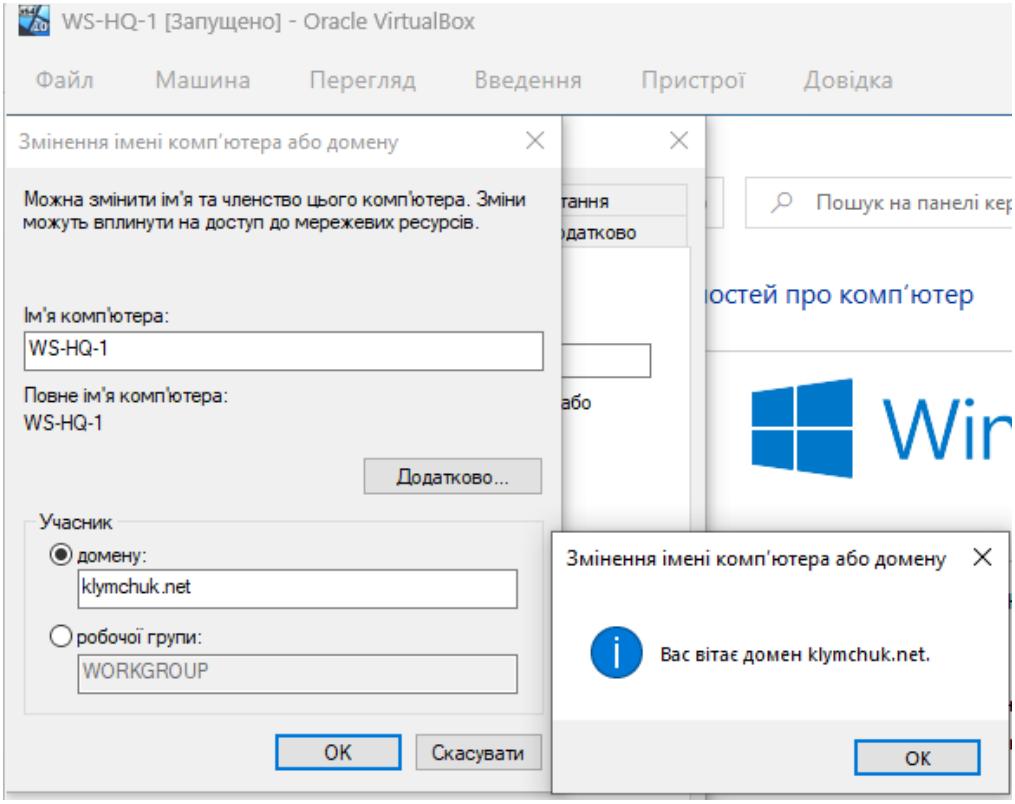


Рисунок 3.14 – Приєднання робочої станції WS-HQ-1 до домену klymchuk.net

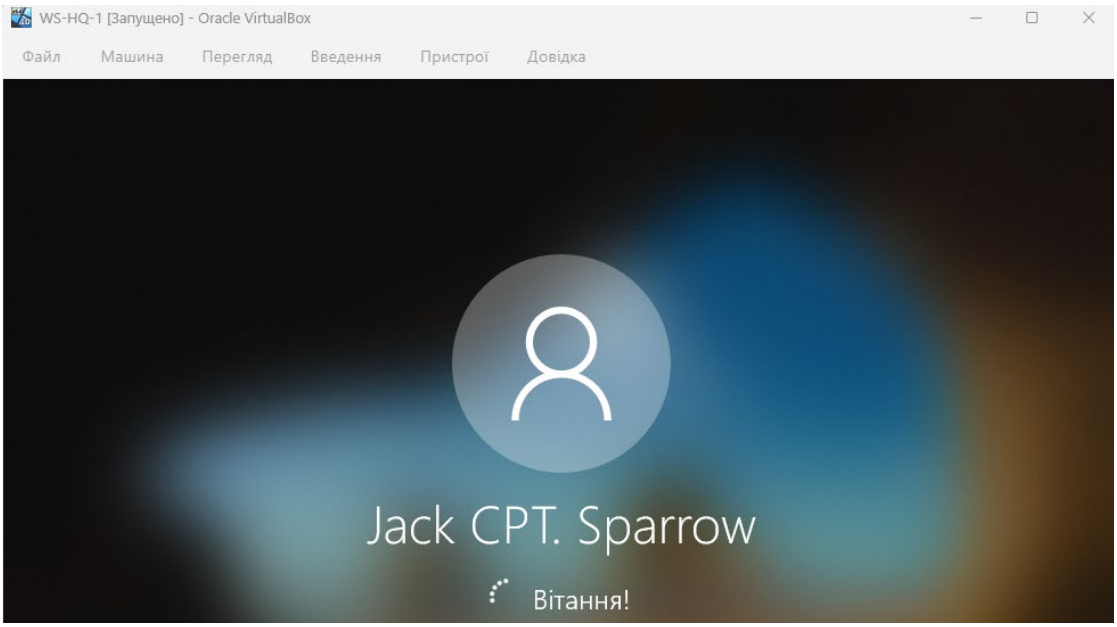


Рисунок 3.15 – Успішний вхід в систему станції під доменним користувачем

На цьому базове налаштування сервера і робочих станцій завершено. Тепер можем приступати до налагодження маршрутизатора MikroTik (R-HQ-1) в головному офісі через спеціалізоване програмне забезпечення WinBox. У вікні «Neighbors» слід обрати MAC-адресу бажаного пристрою та натиснути кнопку «Connect». Після успішного підключення автоматично з'явиться вікно зі запитом на зміну пароля для облікового запису «admin», рис.3.16-3.17.

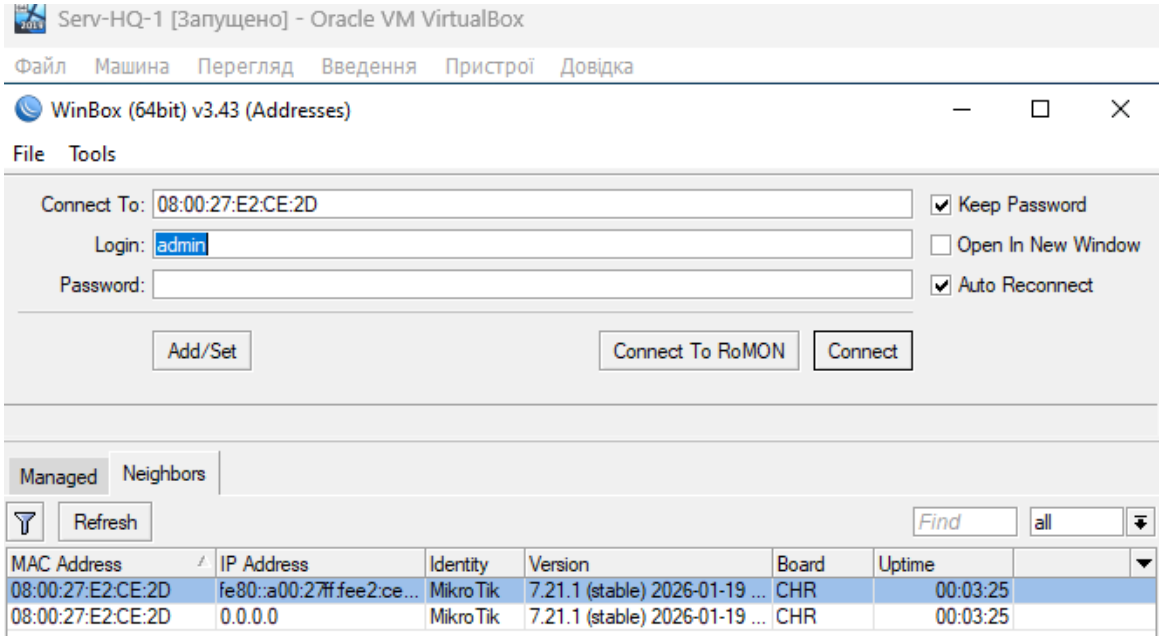


Рисунок 3.16 – Підключення до R-HQ-1 через утиліту WinBox

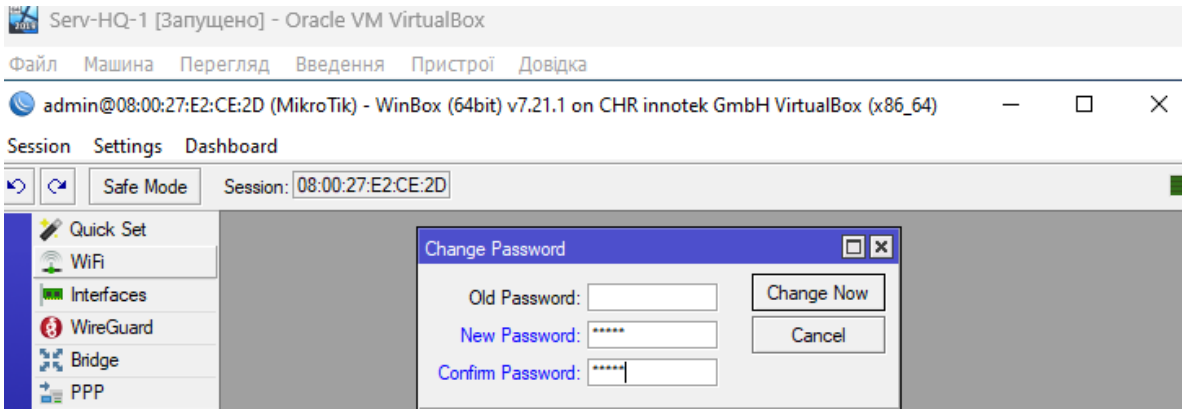


Рисунок 3.17 – Зміна паролю користувача admin на R-HQ-1

Після цього переходимо до налаштування основних параметрів маршрутизатора, що розпочалося зі встановлення коректного системного ідентифікатора пристрою, рис.3.18. Було виконано налаштування інтерфейсів, де

порт ether1 визначено як зовнішній інтерфейс (WAN), а ether2 – як інтерфейс локальної мережі (LAN), рис.3.19. Відповідно до розробленого плану адресації, для зазначених інтерфейсів було призначено статичні IP-адреси 25.222.1.2/30 та 172.22.1.1/24 відповідно, рис.3.20.

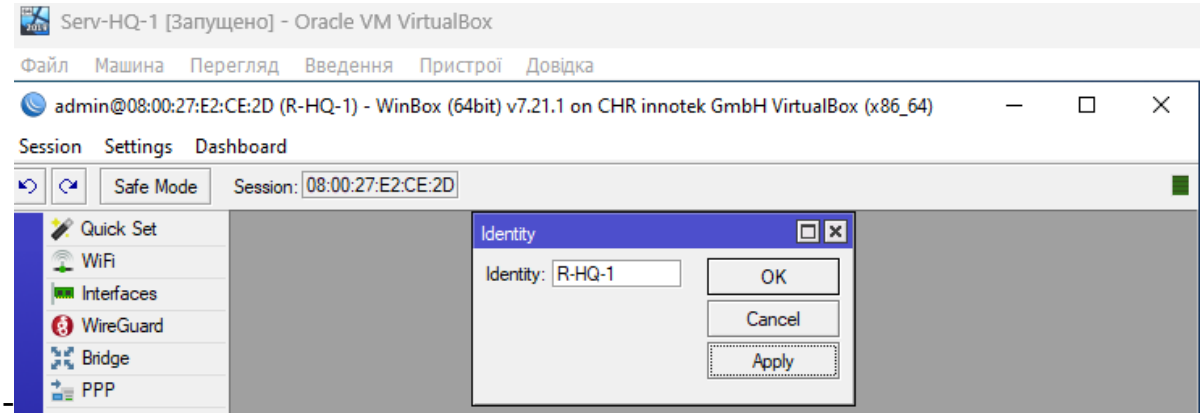


Рисунок 3.18 – Зміна системного ідентифікатора маршрутизатора

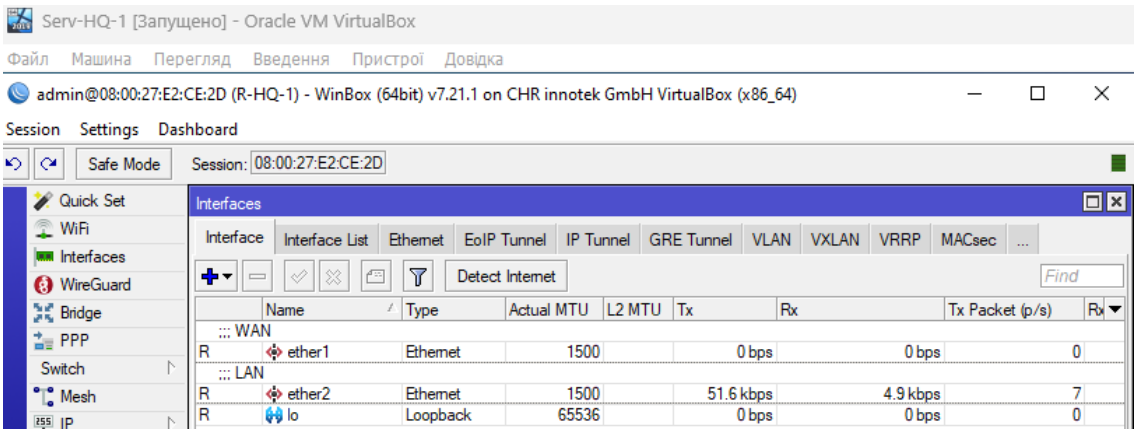


Рисунок 3.19 – Конфігурування назв мережних інтерфейсів

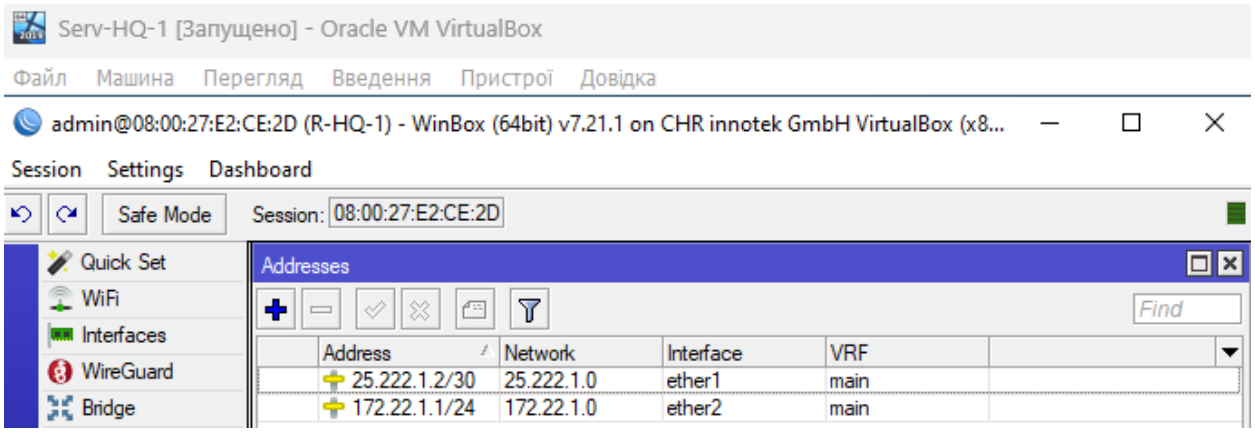


Рисунок 3.20 – Призначення IP-адрес мережним інтерфейсам

Для забезпечення доступу хостів локальної мережі до зовнішніх ресурсів та коректної обробки вихідного трафіку було виконано створення маршруту за замовчуванням. Для мережі призначення 0.0.0.0/0 було встановлено шлях до зовнішнього інтерфейсу маршрутизатора, тобто ether1, рис.3.21. Для коректної обробки пакетів при доступі до зовнішніх ресурсів було налаштовано механізм трансляції мережних адрес. У розділі Firewall на вкладці NAT було впроваджено правило для ланцюжка srcnat, згідно з яким для всього вихідного трафіку з підмережі 172.22.1.0/24, що проходить через зовнішній інтерфейс ether1, застосовується дія masquerade, яка дозволяє виконувати динамічну трансляцію багатьох внутрішніх локальних адрес в одну зовнішню, рис.3.22.

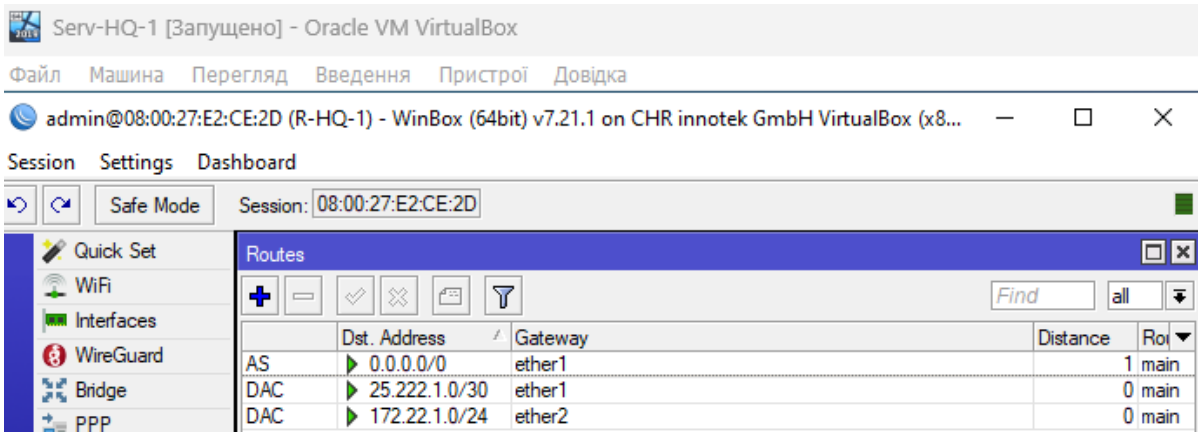


Рисунок 3.21 – Налаштування маршрутизації за замовчуванням

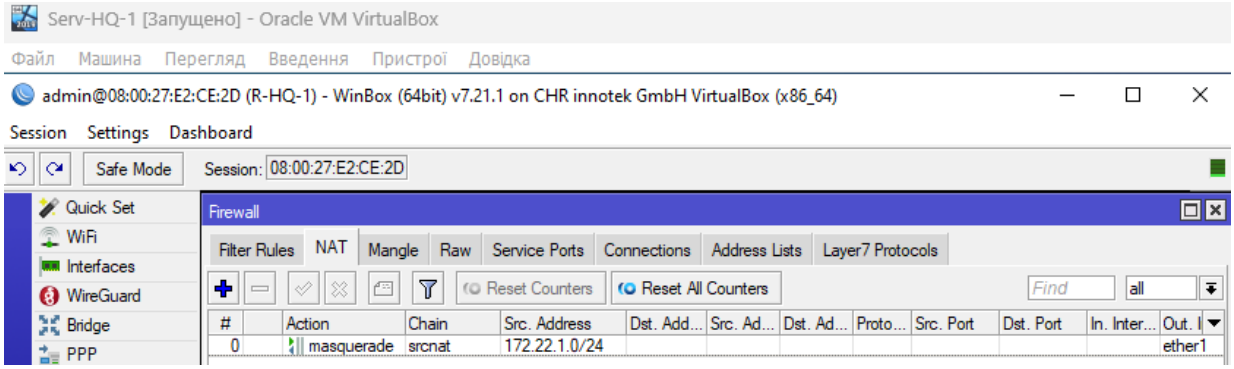


Рисунок 3.22 – Налаштування правила механізму трансляції мережних адрес

З метою забезпечення коректного вирішення доменних імен на маршрутизаторі було додано параметри DNS-серверу, а саме 8.8.8.8 та 8.8.4.4, що гарантує стабільний доступ до зовнішніх мережних ресурсів. Для надання

можливості пристроям локальної мережі використовувати маршрутизатор як рекурсивний DNS-сервер було активовано Allow Remote Requests, рис.3.23.

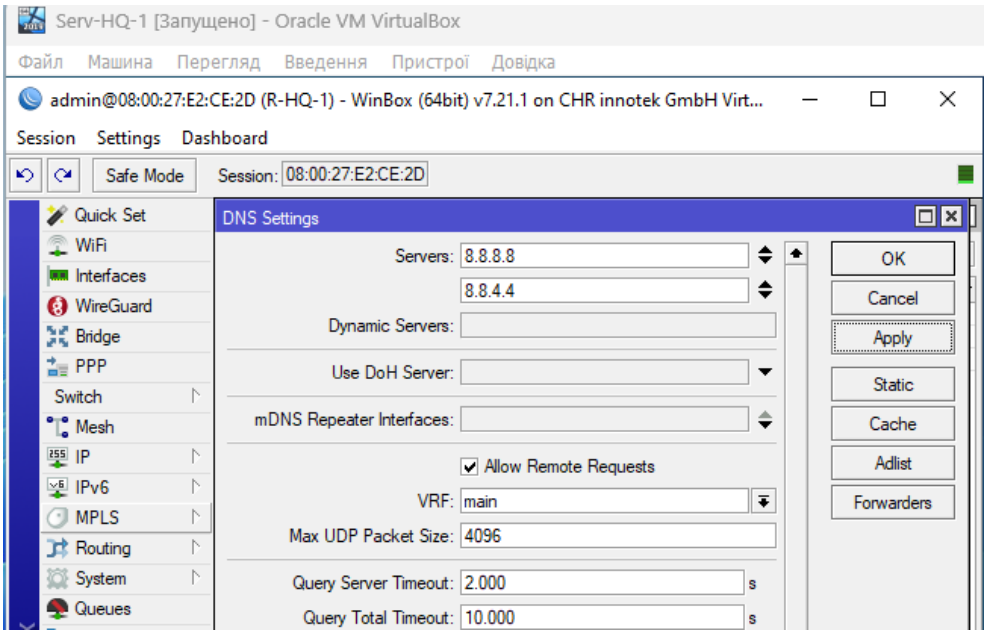


Рисунок 3.23 – Налаштування параметрів DNS-сервера на маршрутизаторі

Для забезпечення коректного перенаправлення DNS-запитів на внутрішній сервер домену було додано статичний запис, де для доменного імені klymchuk.net було створено запис типу FWD. В параметрах було призначено IP-адресу 172.22.1.99, що відповідає адресі серверу Serv-HQ-1 та встановлено позначку біля «Match Subdomain», рис.3.24.

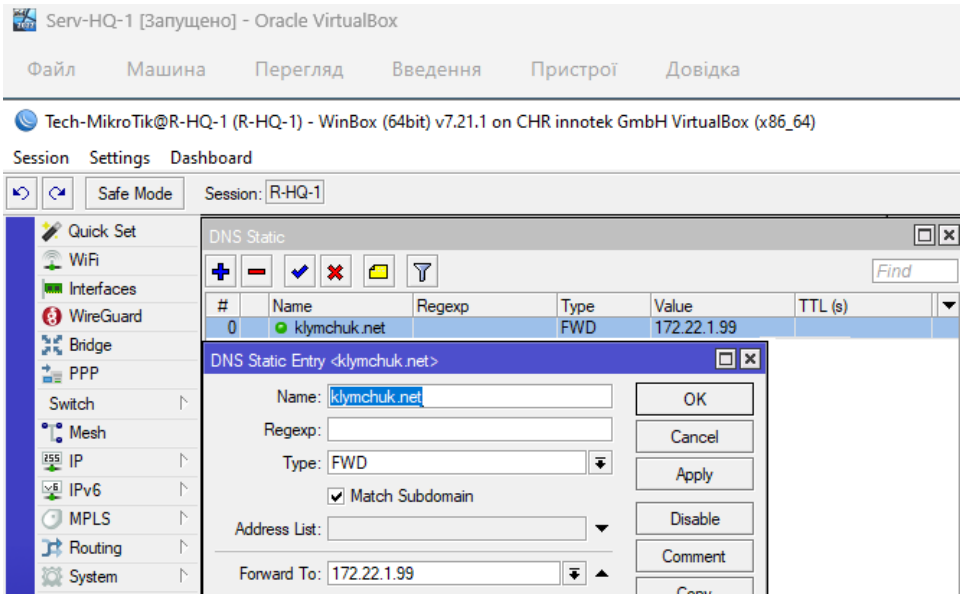


Рисунок 3.24 – Додання статичного DNS-запису до klymchuk.net

Для забезпечення точності реєстрації системних подій було налагоджено механізм автоматичної синхронізації часу. У розділі NTP Client було вказано адресу сервера синхронізації time.in.ua після чого статус роботи NTP перевівся у стан «synchronized». Паралельно з цим, у меню Clock було проведено налаштування часового поясу Europe/Kyiv та поставлено відмітку про автоматичний перехід на літній/зимовий час та забезпечити відповідність часових міток у журналах маршрутизатора реальному поточному часу, рис.3.25-3.26 На цьому базове налаштування маршрутизатора R-HQ-1 завершено.

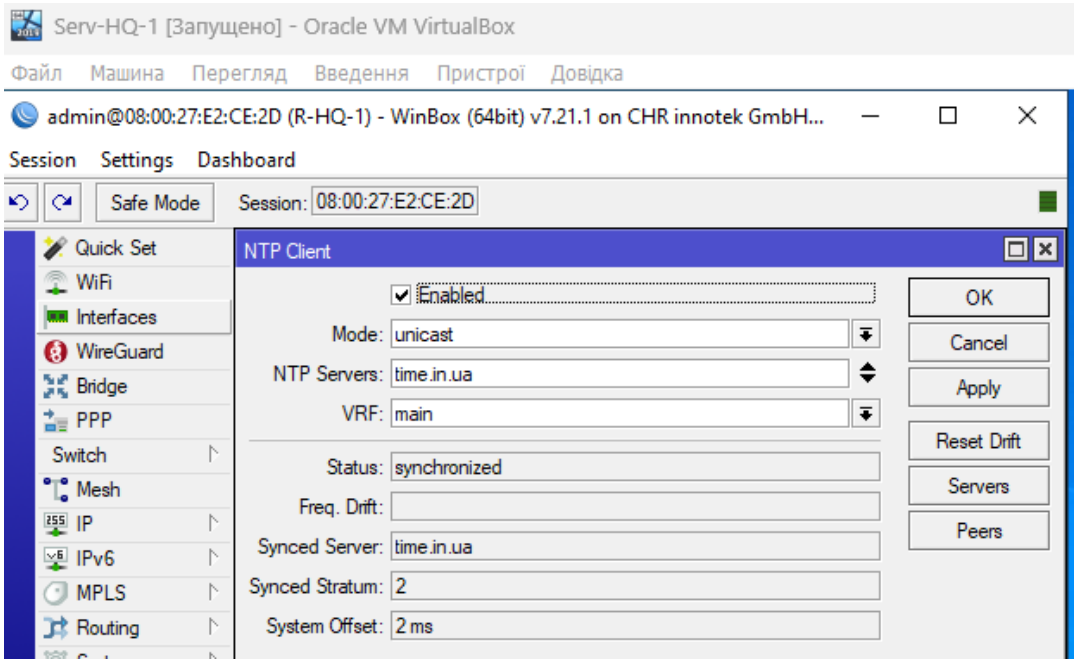


Рисунок 3.25 – Налаштування роботи NTP-клієнту

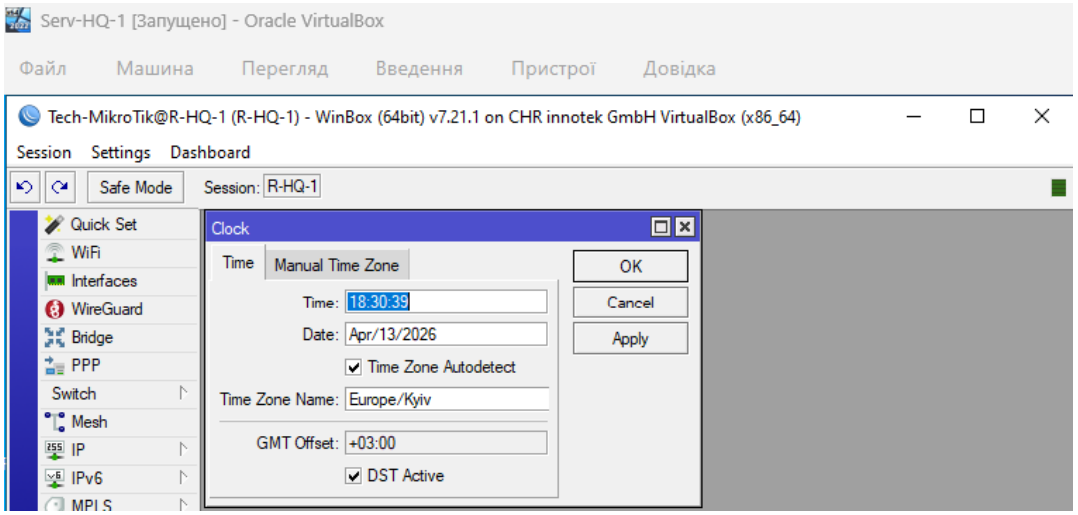


Рисунок 3.26 – Налаштування параметру часового поясу

Тепер перейдемо до маршрутизатора MikroTik в підрозділі А (R-BR-A-1). Тут загальний процес налагодження аналогічний до виконаних налаштування на R-HQ-1. Нижче на рис.3.27 наведено встановлені параметри адресації інтерфейсів на R-BR-A-1.

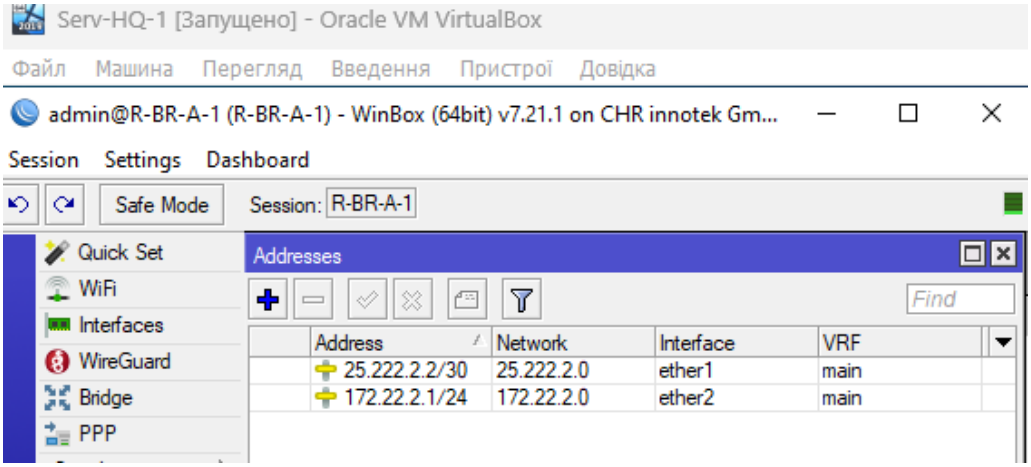


Рисунок 3.27 – Параметри адресації інтерфейсів R-BR-A-1

Але також на R-BR-A-1 слід налаштувати роботу DHCP-сервер. За допомогою вбудованого майстра налаштування DHCP Setup було зафіксовано, що роздача відбуватиметься на локальному інтерфейсі ether2. Було встановлено мережу 172.22.2.0/24 та сформовано пул доступних IP-адрес у діапазоні від 172.22.2.100 до 172.22.1.109. Додатково було вказано адресу основного шлюзу та DNS-сервера (172.22.2.1), що загалом дозволить забезпечити клієнтські робочі станції всіма необхідними параметрами для роботи, рис.3.28-3.29.

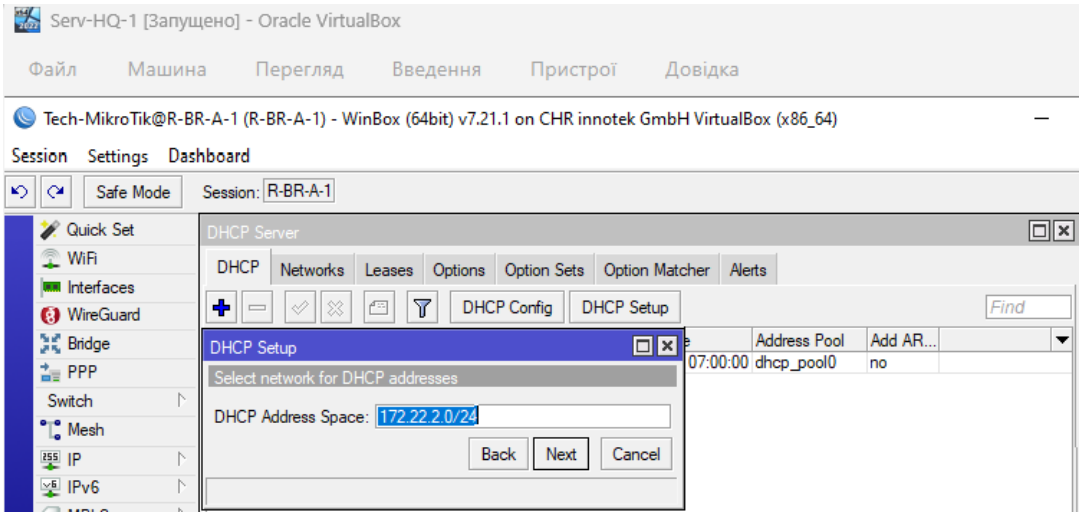


Рисунок 3.28 – Визначення мережі роздачі для DHCP-сервера

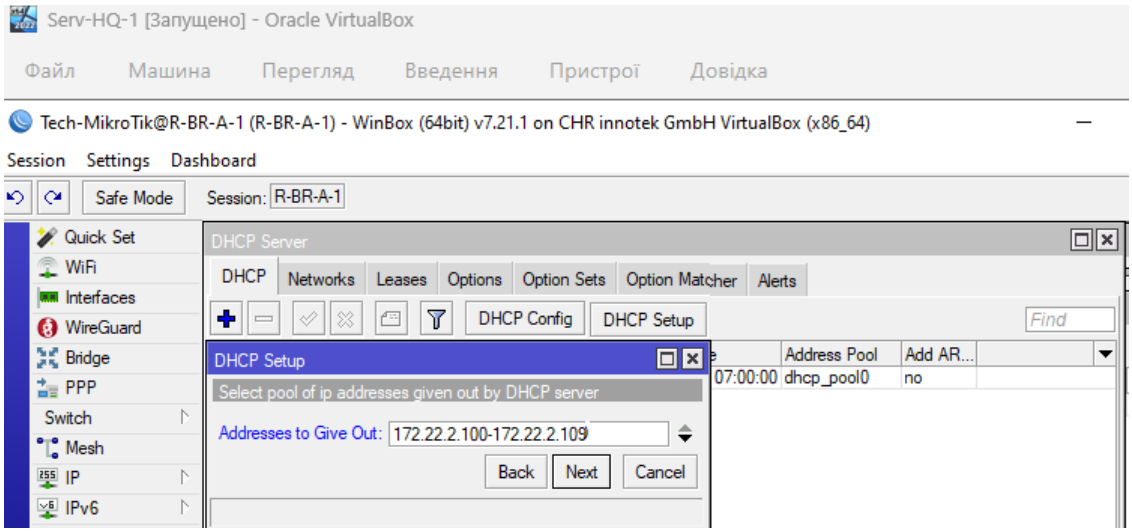


Рисунок 3.29 – Визначення адрес до видачі для DHCP-сервера

3.2 Налаштування L2TP/IPsec між головним офісом та підрозділом

Після успішного налагодження базових параметрів мережі перейдемо до налаштування L2TP/IPsec на R-HQ-1. З метою забезпечення автоматичної видачі мережних параметрів для вузлів, що підключатимуться до мережі через VPN, було проведено налаштування адресного простору. Для цього створено пул адрес L2TP-pool з діапазоном IP-адрес від 10.222.22.10 до 10.222.22.254, рис.3.30.

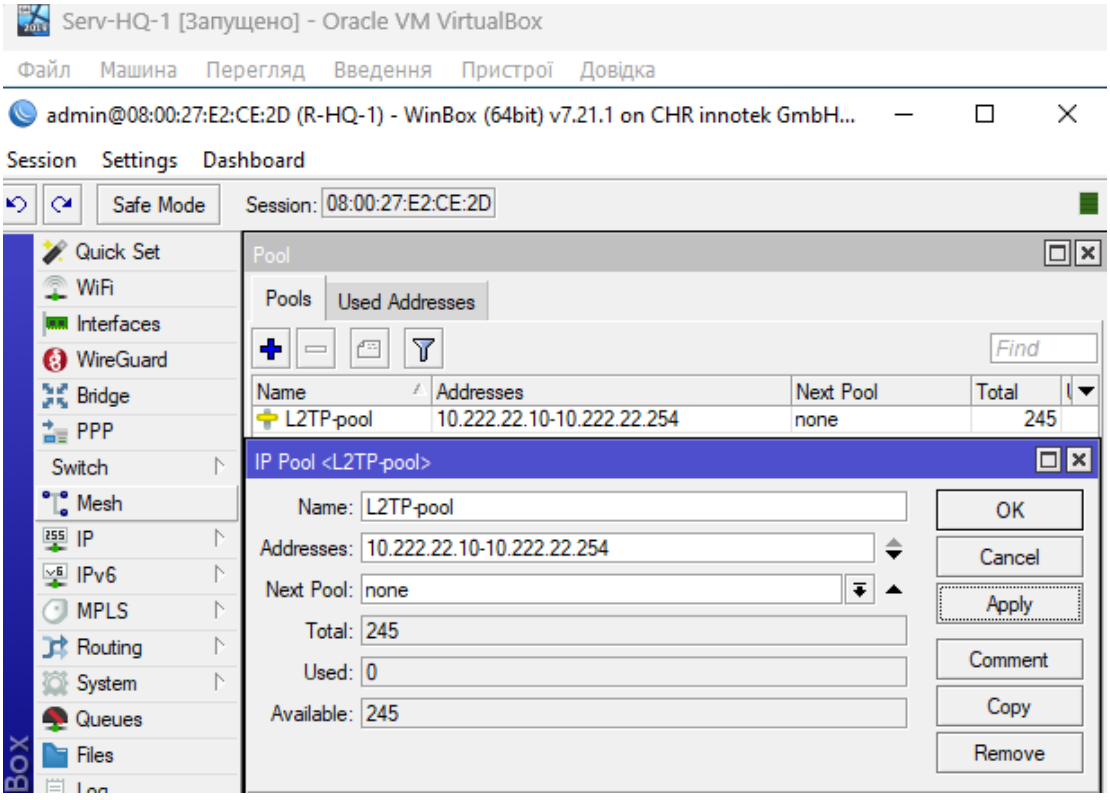


Рисунок 3.30 – Створення пулу динамічних адрес для VPN-клієнтів

Після пулу адрес було створено новий PPP-профіль з назвою L2TP-profile. Для нього визначено локальну IP-адресу сервера 10.222.22.1, а для віддалених клієнтів обрано раніше створений пул L2TP-pool. Додатково у налаштуваннях профілю було вказано адресу DNS-сервера (172.22.1.99), що дозволить клієнтам після встановлення VPN-з'єднання коректно використовувати внутрішній сервер організації для розв'язання доменних імен, рис.3.31.

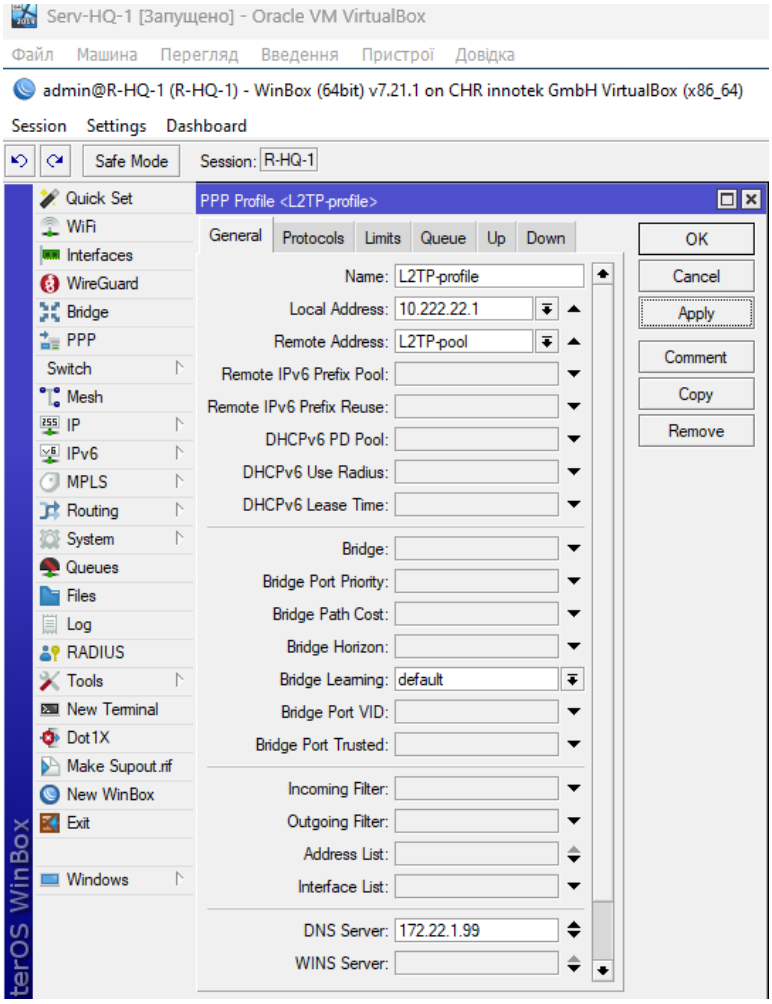


Рисунок 3.31 – Налаштування профілю PPP для L2TP-підключень

Для забезпечення автентифікації з маршрутизатором підрозділу А було створено відповідний обліковий запис користувача із прив'язкою до профілю L2TP-profile. Для цього було налаштовано запис R-BR-A-1-VPN-user, де окрім пароля та сервісу l2tp, було зафіксовано локальну адресу сервера (10.222.22.1) та віддалену адресу клієнта (10.222.22.2). Крім цього також було зазначено віддалену локальну мережу філіалу (172.22.2.0/24), рис.3.32.

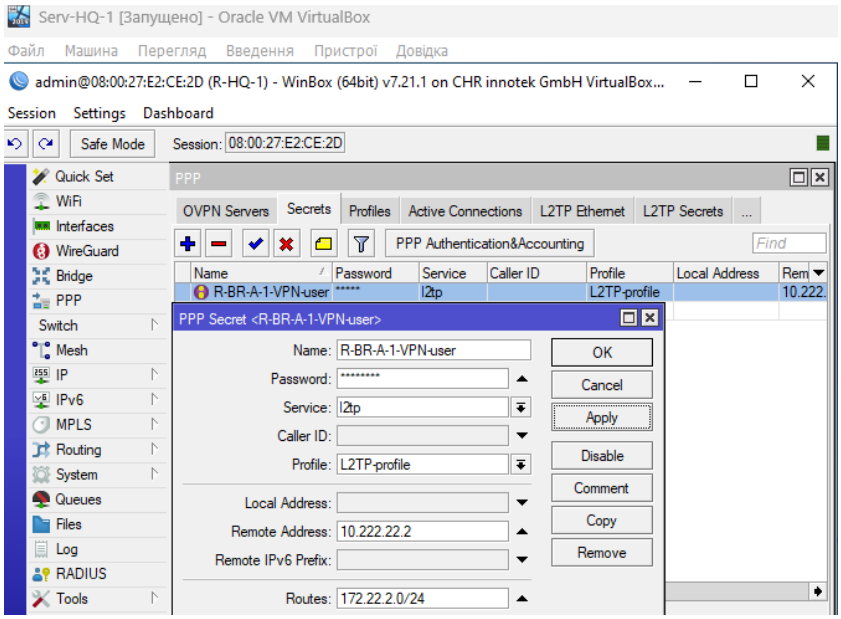


Рисунок 3.32 – Створення облікового запису L2TP клієнта для R-BR-A-1

Далі було виконано налаштування параметрів безпеки IPsec. У розділах «Proposals» та «Profile» визначено алгоритми шифрування, хешування та встановлено групи Diffie-Hellman для безпечного обміну ключами, рис.3.33-3.34.

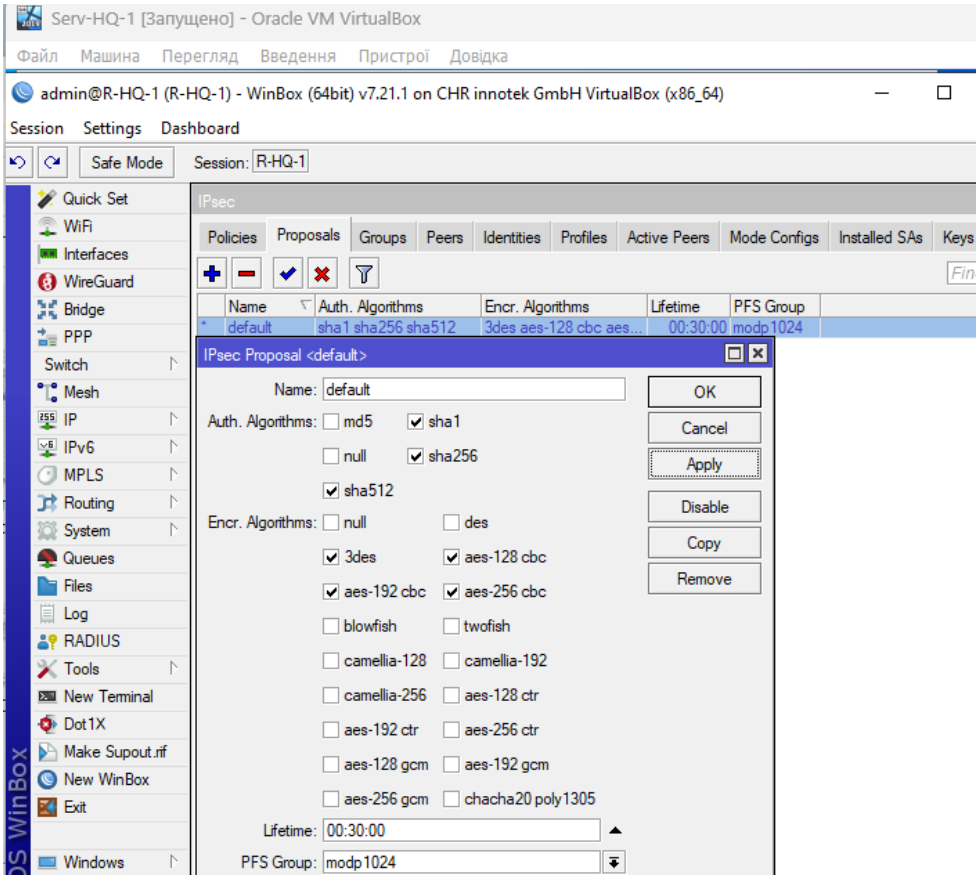


Рисунок 3.33 – Налаштування параметрів IPsec Proposal

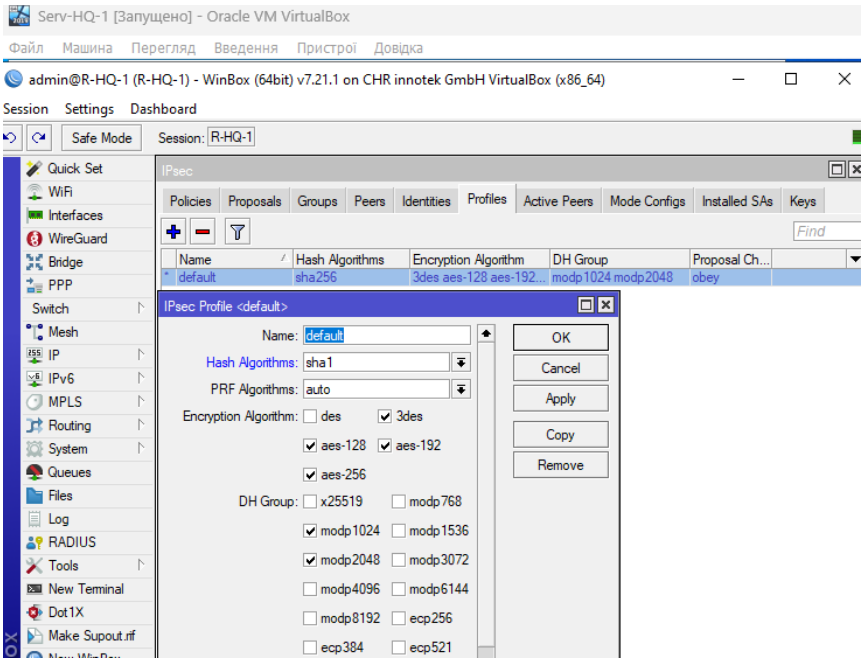


Рисунок 3.34 – Налаштування параметрів IPsec Profile

Після чого переходимо до безпосередньої активації L2TP-сервера. У ході налагодження встановлено створений раніше L2TP-profile, як профіль за замовчуванням та обрано безпечні протоколи автентифікації mschap2 і chap. Вкрай важливо тут ввімкнути шифрування IPsec та задати ключ доступу у полі IPsec Secret, рис.3.35.

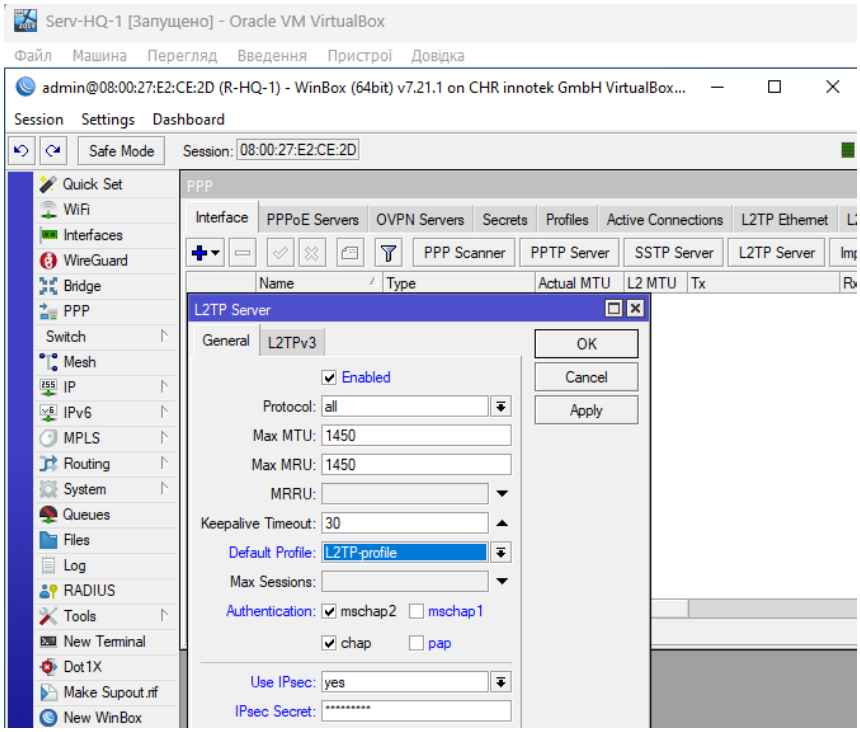


Рисунок 3.35 – Активація L2TP-сервера

Також для забезпечення успішного проходження трафіку до VPN-сервера для фарєвола було створено два дозвільні правила для ланцюжка input. Першим правилом було дозволено вхідні пакети за протоколом UDP через порти 500, 1701 та 4500, що необхідно для ініціалізації L2TP-тунелю та обміну ключами. Друге правило забезпечило проходження пакетів протоколу ipsec-esp, який відповідає за безпосереднє транспортування зашифрованих даних усередині захищеного каналу. Для обох правил було визначено вхідний інтерфейс ether1 (WAN-порт маршрутизатора R-HQ-1) та переміщено на самий верх списку, рис.3.36-3.37.

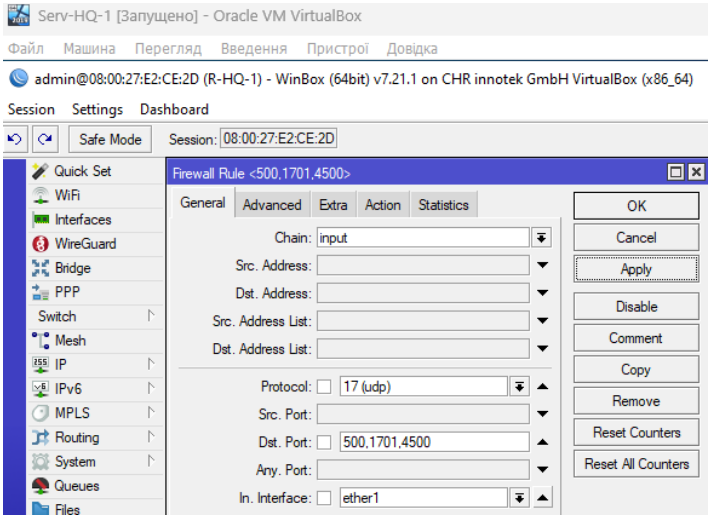


Рисунок 3.36 – Налаштування правила фаєрволу для вхідних пакетів з портами призначенням UDP 500, 1701, 4500

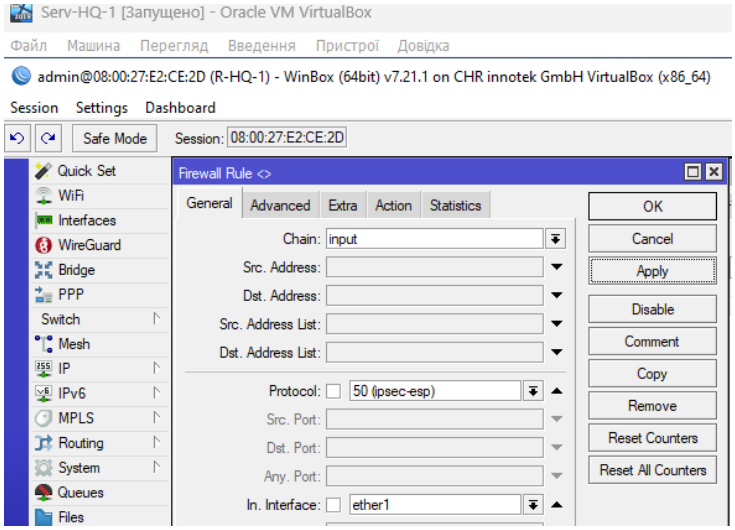


Рисунок 3.37 – Налаштування правила фаєрволу для вхідних пакетів з протоколом ipsec-esp

Налаштування L2TP/IPsec на клієнті R-BR-A-1

Для встановлення зв'язку з центральним офісом на маршрутизаторі підрозділу, тобто R-BR-A-1, було налаштовано інтерфейс L2TP-клієнта. Основне налагодження з'єднання виконано на вкладці Dial Out, де у полі вказано зовнішню IP-адресу маршрутизатора R-HQ-1 (25.222.1.2), а також введено дані облікового запису R-BR-A-1-VPN-user та відповідний пароль. З метою створення зашифрованого з'єднання було введено пароль IPsec, рис.3.38-3.39.

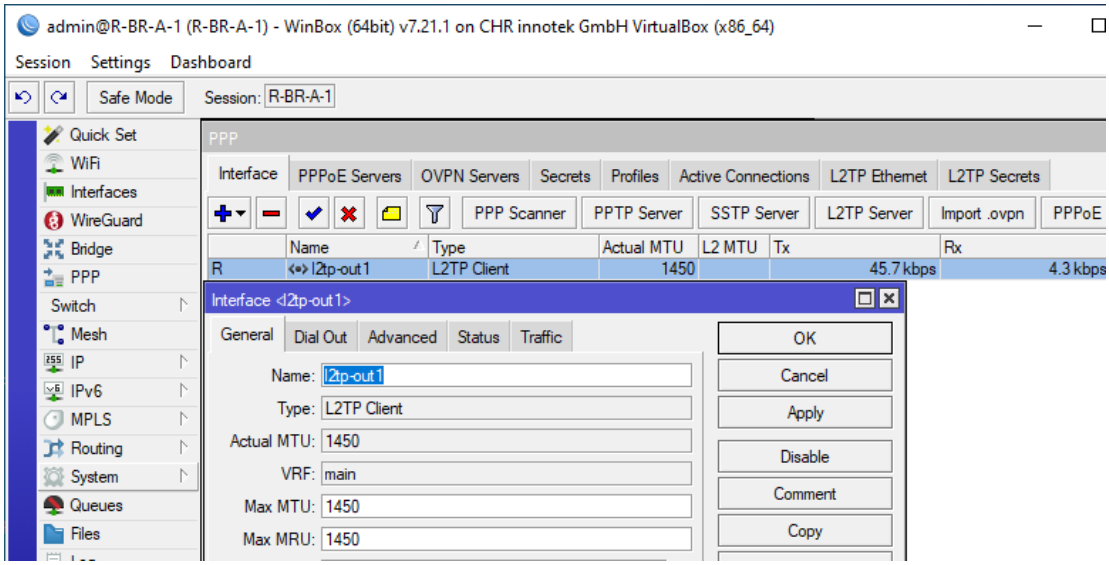


Рисунок 3.38 – Налаштування інтерфейсу L2TP-клієнта на R-BR-A-1

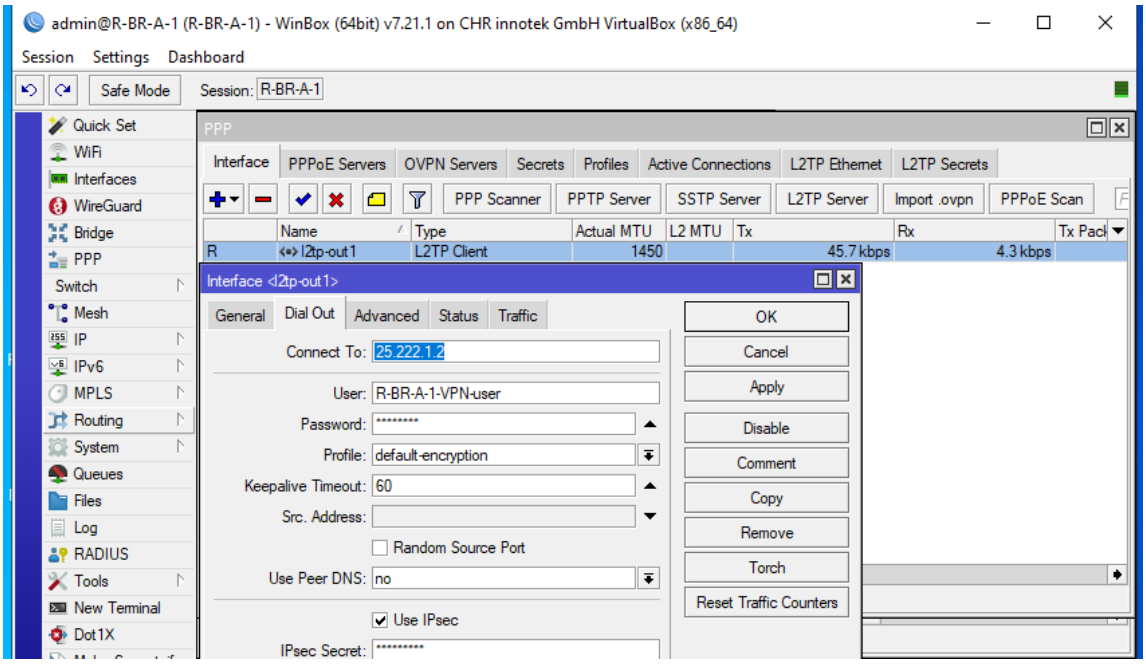


Рисунок 3.39 – Налаштування інтерфейсу L2TP-клієнта на R-BR-A-1

Аналогічно до налаштувань центрального офісу, на маршрутизаторі R-BR-A-1 було створено дозвільні правила для коректного функціонування VPN-тунелю з боку зовнішнього інтерфейсу ether1, рис.3.40-3.41.

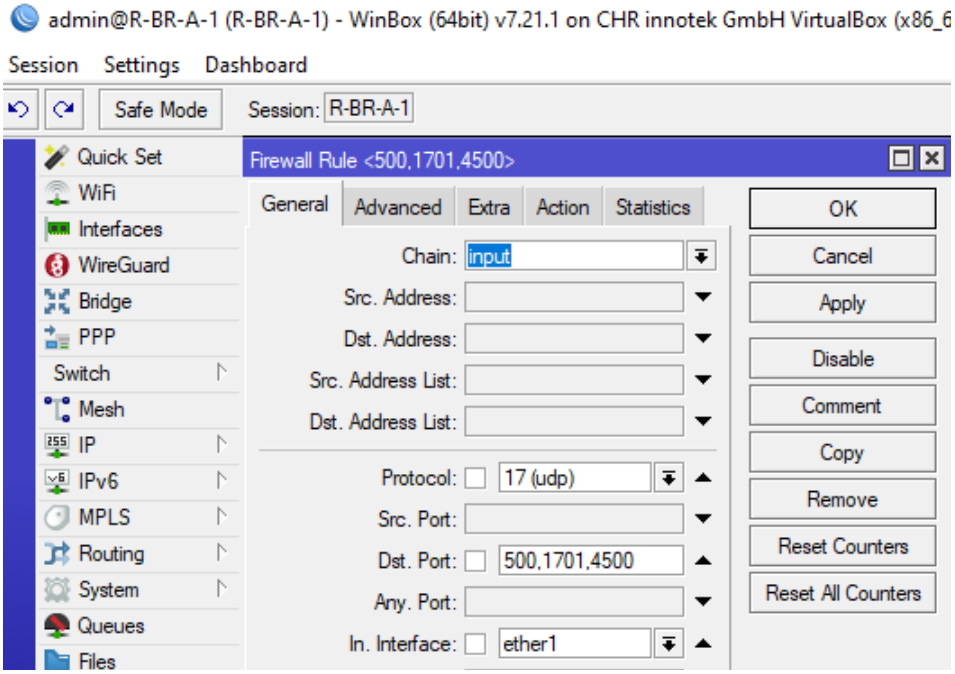


Рисунок 3.40 – Налаштування правила фаєрволу для вхідних пакетів з портами призначенням UDP 500, 1701, 4500

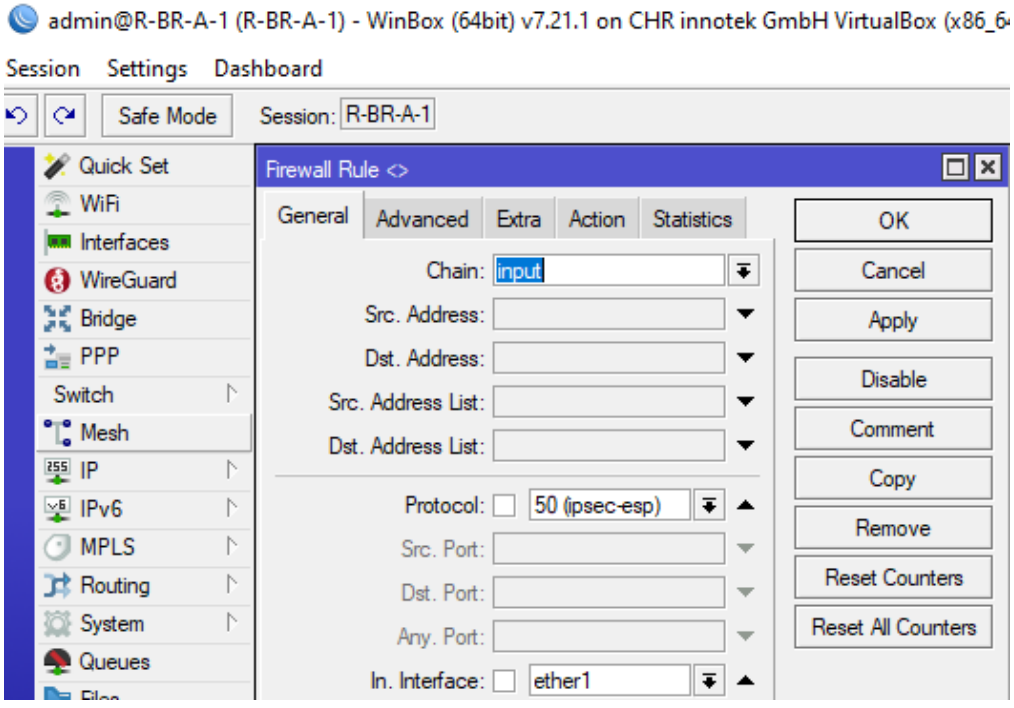


Рисунок 3.41 – Налаштування правила фаєрволу для вхідних пакетів з протоколом ipsec-esp

Також для забезпечення доступу з локальної мережі філії до ресурсів головного офісу було додано два статичних маршрути. Перший маршрут до VPN-клієнтів (10.222.22.0/24) проходитиме через шлюз l2tp-out1 (10.222.22.1). А другий маршрут до локальної мережі центрального офісу (172.22.1.0/24) проходитиме теж через інтерфейс l2tp-out1 (10.222.22.1). Таке налаштування гарантує, що до інших компонентів корпоративної мережі проходитимуть виключно через встановлене L2TP-з'єднання, рис.3.42.

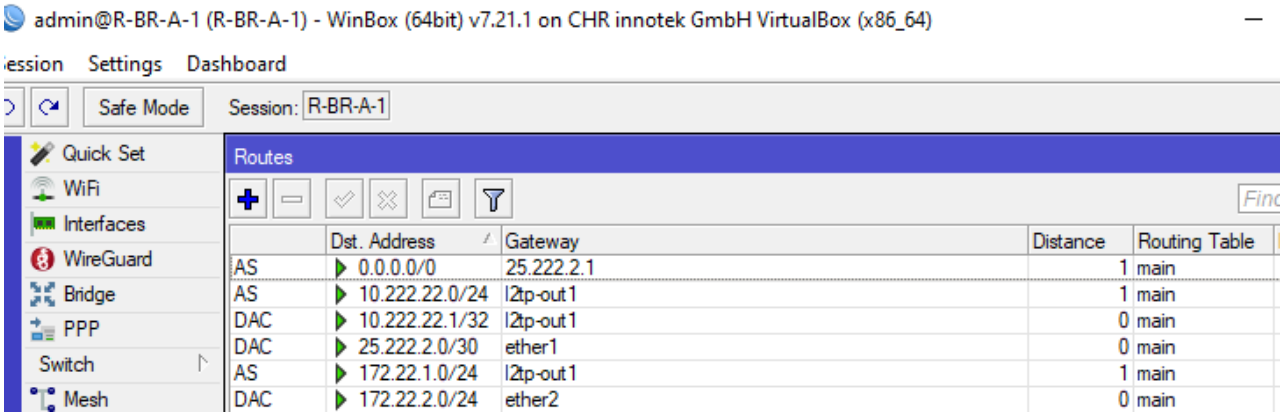


Рисунок 3.42 – Налаштування статичних маршрутів до підмереж

3.3 Налаштування L2TP/IPsec між головним офісом та віддаленим користувачем

Для можливості аутентифікації віддалених працівників з використання облікових записів на сервері Serv-HQ-1 було створено спеціалізований організаційний підрозділ RADIUS-USERS. У цій папці було створено групу безпеки vpn-group, яка в подальшому слугуватиме фільтром для надання доступу до мережі, а також створено окремий обліковий запис WS-REMOTE-1-user, рис.3.43. В подальшому це дозволить налаштовувати політики на сервері, що дозволить відокремити звичайних офісних користувачів від тих, хто має право на встановлення захищеного з’єднання з маршрутизатором через RADIUS.

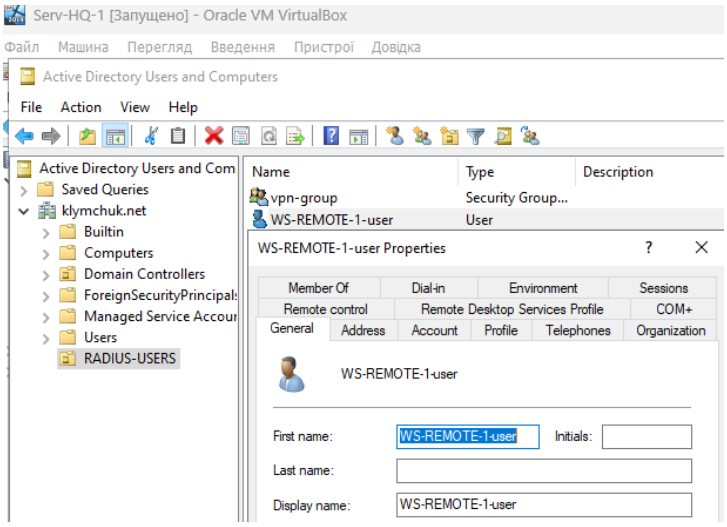


Рисунок 3.43 – Створення користувача WS-REMOTE-1-user та додання його до групи vpn-group

Тепер безпосередньо перейдемо до конфігурації ролі Network Policy Server (NPS). У консолі керування NPS створюється новий RADIUS-клієнт, де вказується дружня назва пристрою (R-HQ-1), його IP-адреса 172.22.1.1 та спільний секретний ключ, що має збігатися з налаштуваннями на маршрутизаторі MikroTik для встановлення зв'язку.

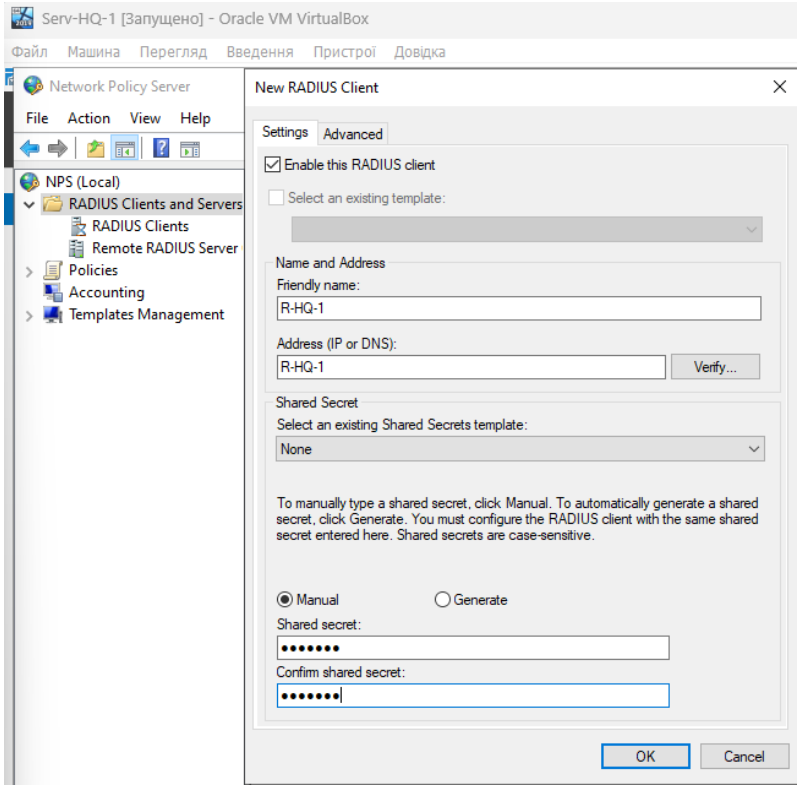


Рисунок 3.44 – Додання RADIUS-клієнта R-HQ-1 у консолі NPS

Далі в консолі Network Policy Server (NPS) було створено нову мережну політику з назвою VPN-policy, яка визначає алгоритми доступу для віддалених з'єднань. В якості обов'язкових умов для виконання політики було вказано приналежність користувача до доменної групи безпеки KLYMCHUK\vpn-group, а також ідентифіковано пристрій запиту за дружньою назвою R-HQ-1. Фінальна конфігурація політики передбачає надання доступу за протоколами MS-CHAP v1/v2 для сервісів типу Framed (VPN) через протокол PPP, що дозволяє серверу NPS приймати рішення про авторизацію віддалених працівників на основі їхніх облікових даних у Active Directory, рис.3.45-3-46.

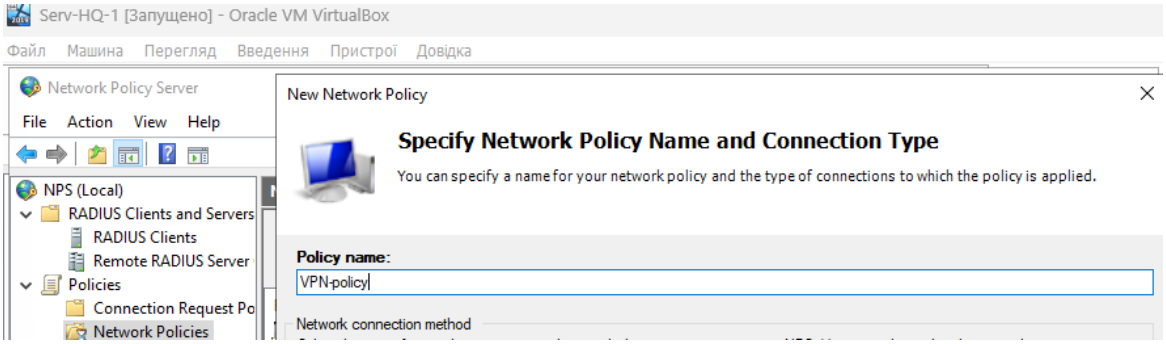


Рисунок 3.45 – Створення та нової мережної політики VPN-policy в консолі NPS.

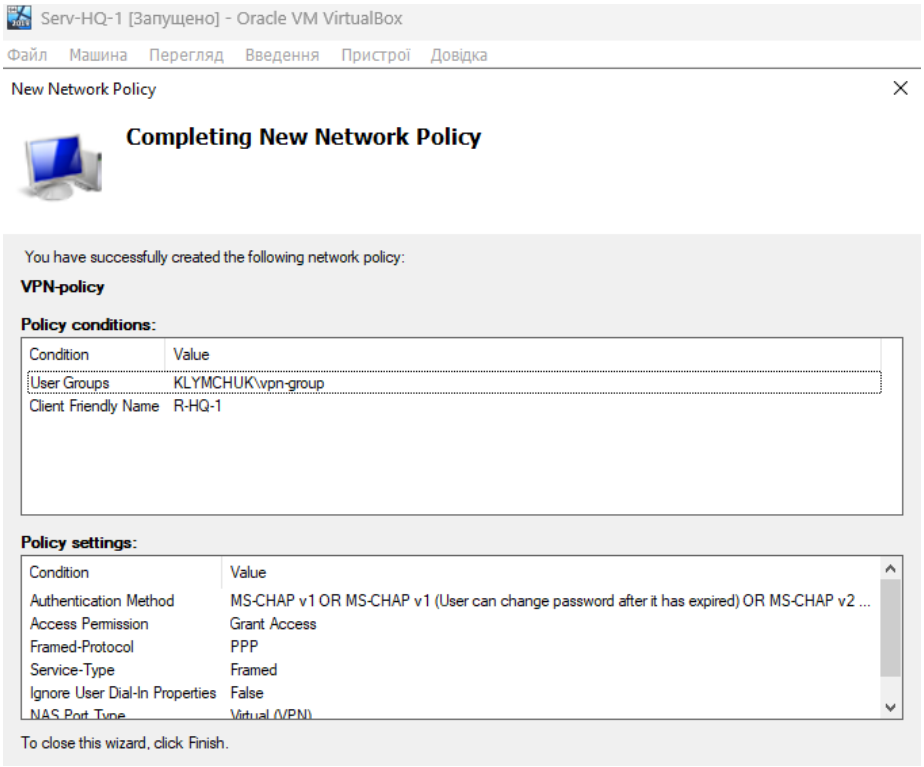


Рисунок 3.46 – Перегляд параметрів створеної політики VPN-policy

Аби мережні пристрої могли звертатись до Serv-HQ-1 було виконано додаткове налаштування в брандмауері Windows. Для цього створено правило для вхідного трафіку з назвою «Allow RADIUS», яке дозволяє проходження пакетів через UDP-порти 1812 (для автентифікації) та 1813 (для обліку) і тим самим дає змогу обробляти запити від RADIUS-клієнтів, рис.3.47.

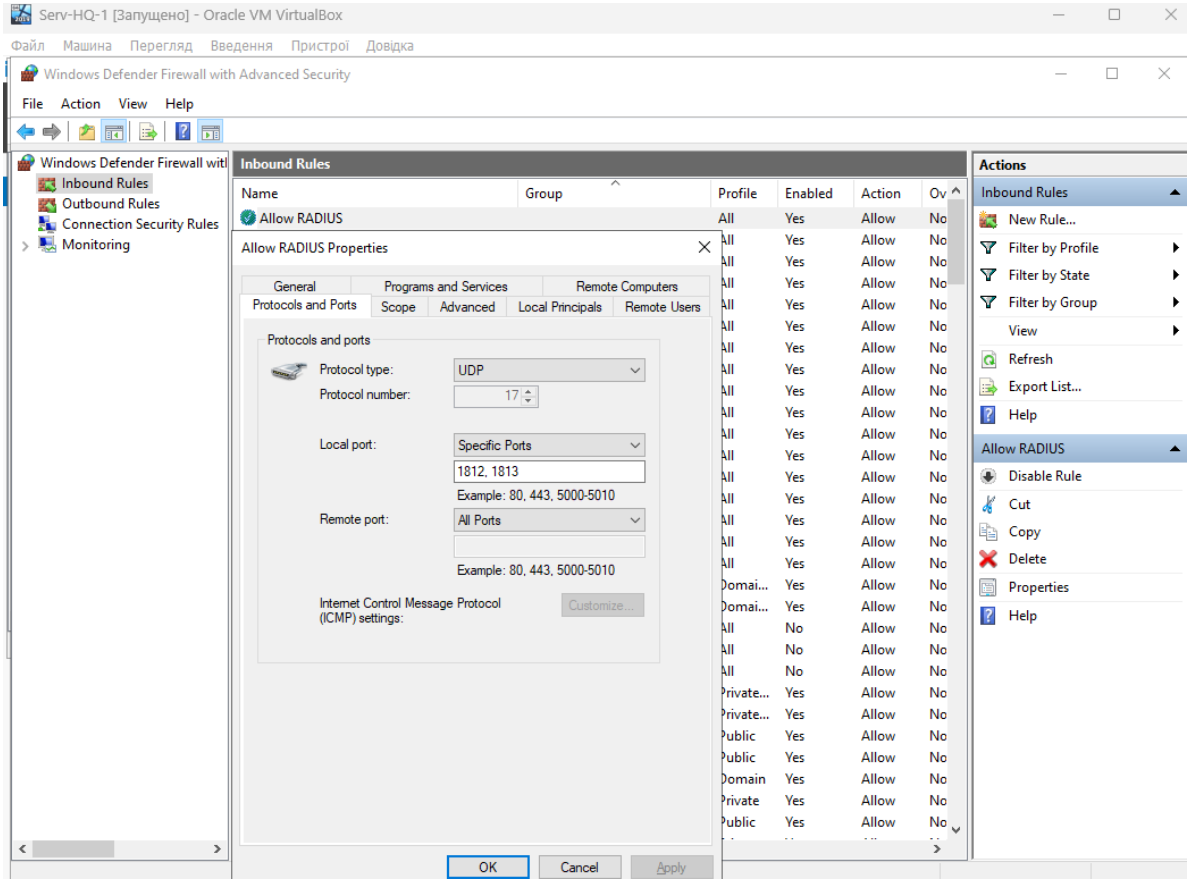


Рисунок 3.47 – Створення дозвільного правила для трафіку RADIUS у брандмауері Windows

Повернемось до маршрутизатора головного офісу. Для забезпечення захищеного підключення віддалених працівників через VPN на R-HQ-1 було налаштовано взаємодію з централізованим сервером автентифікації через протокол RADIUS. У розділі PPP -> Secrets було активовано використання протоколу RADIUS для перевірки облікових даних користувачів, що дозволяє динамічно звіряти облікові записи із базою Active Directory, рис.3.48.

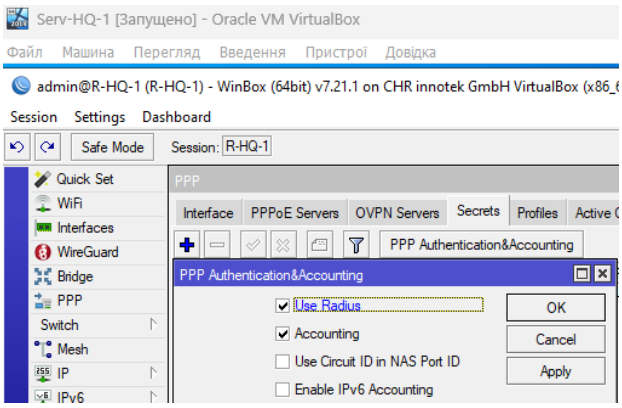


Рисунок 3.48 – Активація використання RADIUS для автентифікації PPP-з’єднань

У налаштуваннях RADIUS-клієнта було обрано сервіс ppp, вказано домен klymchuk.net та IP-адресу сервера 172.22.1.99, а також задано секретний ключ та порти аутентифікації і авторизації (UDP 1812 та 1813). Дане налаштування гарантує, що кожен віддалений співробітник при спробі підключення до мережі проходитиме централізовану перевірку на сервері Serv-HQ-1, що дозволяє адміністратору гнучко керувати правами доступу без необхідності локального створення облікових записів на маршрутизаторі, рис.3.49.

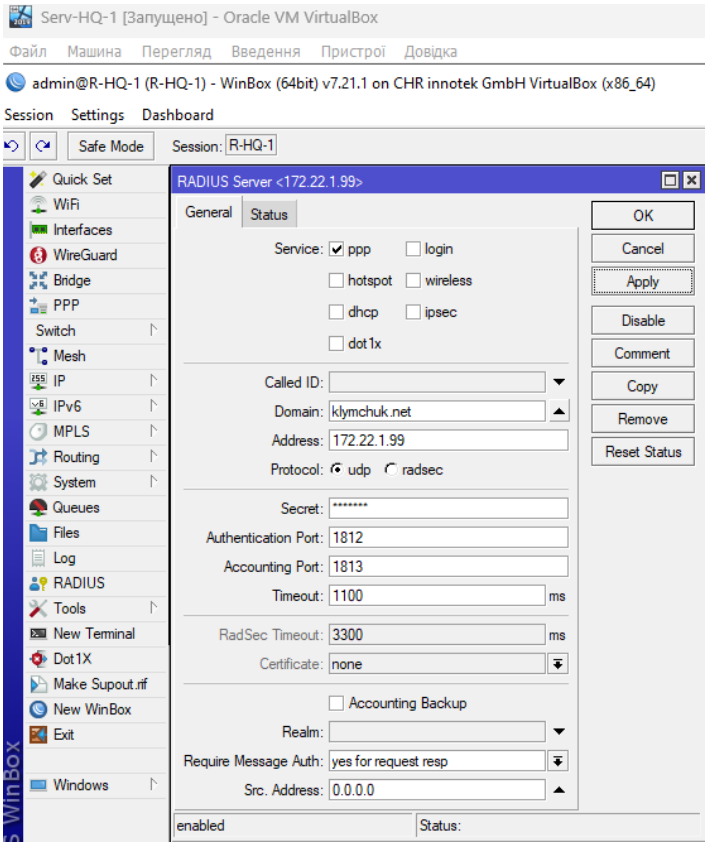


Рисунок 3.49 – Активація використання RADIUS для автентифікації PPP-з’єднань

Налаштування L2TP/IPsec клієнта WS-Remote-1

Для підготовки робочої станції WS-Remote-1 до встановлення VPN-з'єднання перевіримо поточні мережні параметри за допомогою команди ipconfig /all. Згідно з цим мережний адаптер отримав IPv4-адресу 192.168.22.51 від DHCP-сервера домашнього маршрутизатора R-REMOTE-1. Також підтверджено коректне призначення шлюзу за замовчуванням та DNS-сервера з адресою 192.168.22.1, що свідчить про готовність ініціалізації VPN-тунелю, рис.3.50.

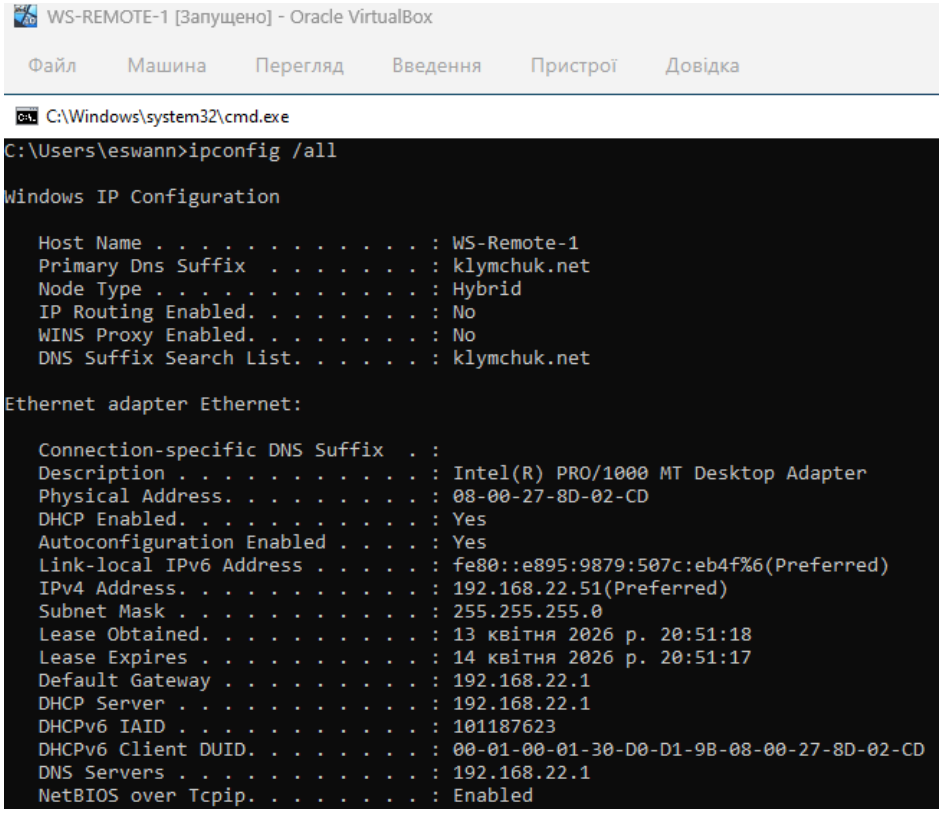


Рисунок 3.50 – Мережні параметри станції WS-Remote-1

Після цього виконуємо підключення віддаленої станції до корпоративної мережі за допомогою відповідних команд в терміналі PowerShell. Спершу за допомогою команди Add-VpnConnection було створено новий профіль «L2TP-TO-HQ», де визначено VPN-сервер 25.222.1.2, тип тунелю L2tp та спільний ключ для забезпечення безпеки на рівні IPsec. У параметрах команди було зафіксовано використання методу автентифікації MSChapv2 та обов'язковий рівень шифрування (EncryptionLevel Required). Для доступу до конкретних підмереж головного офісу та підрозділу було використано команду Add-VpnConnectionRoute,

за допомогою якої до інтерфейсу «L2TP-TO-HQ» було додано статичні маршрути до мереж 172.22.1.0/24 та 172.22.2.0/24. Після цього виконується безпосереднє підключення ви користанням команди rasdial та введенням логіну користувача у форматі WS-REMOTE-1-user@klymchuk.net. Після чого отримуємо підтвердження «Successfully connected to L2TP-TO-HQ», що свідчить про успішне підключення станції до корпоративної мережі через VPN, рис.3.51-3.52.

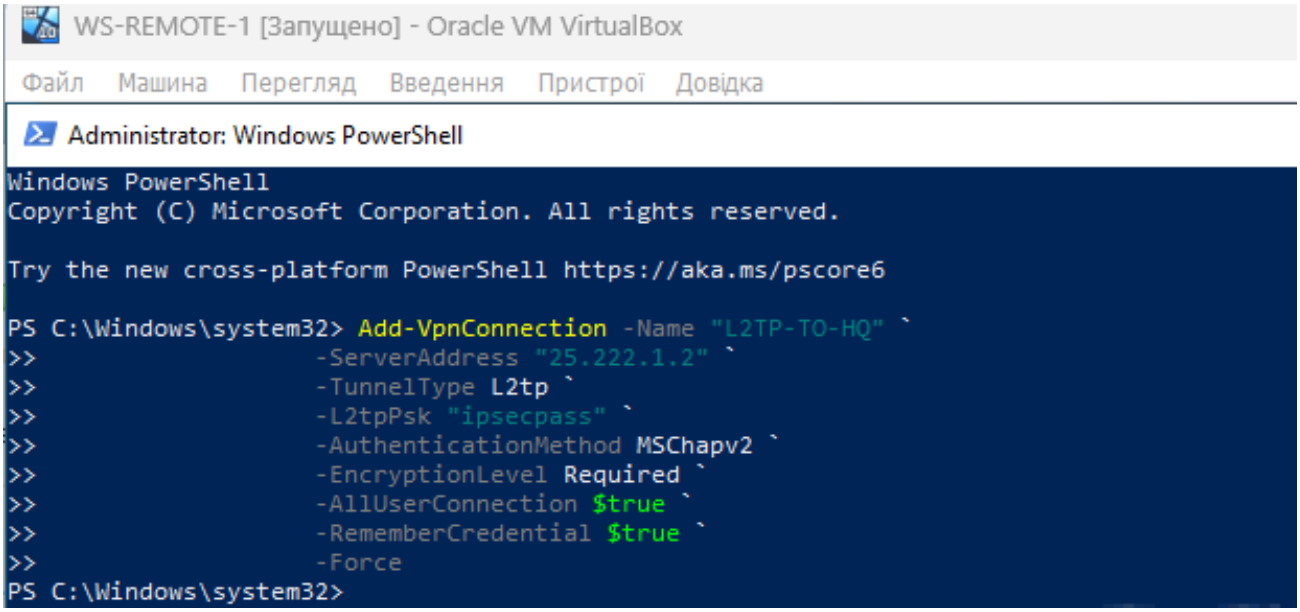


Рисунок 3.51 – Процес створення VPN-інтерфейсу

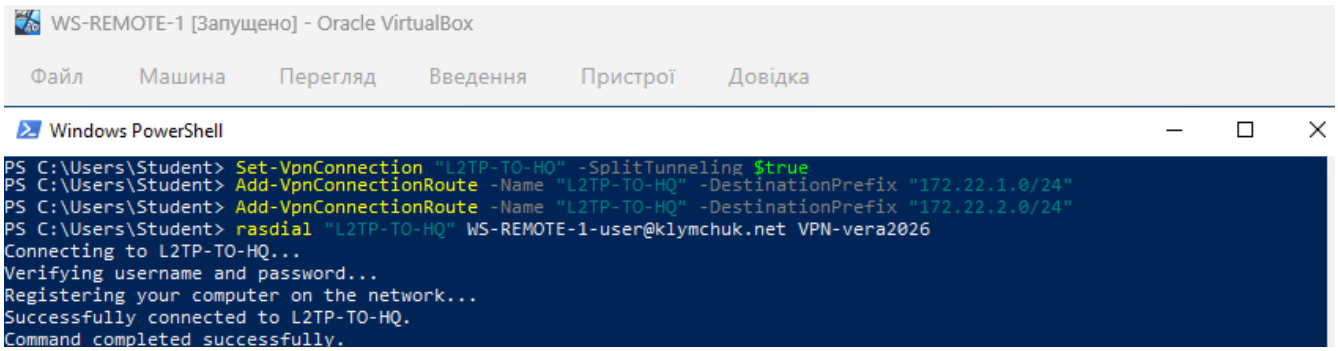


Рисунок 3.52 – Додання статичних маршрутів та ініціалізація VPN-сесії через PowerShell

Для забезпечення автоматизації процесу підключення віддаленої робочої станції відразу після запуску комп'ютера було створено заплановане завдання в «Task Scheduler» з назвою Auto_VPN_L2TP-TO-HQ. У налаштуваннях як основні

тригери обрано запуск під час старту ОС (At startup) та входу будь-якого користувача (At log on), що гарантує постійну наявність зв'язку з корпоративною мережею. Основною дією завдання є запуск системної утиліти C:\Windows\System32\rasdial.exe з аргументами, що містять назву профілю L2TP-TO-HQ, ім'я користувача WS-REMOTE-1-user та відповідний пароль, що дозволяє автоматично підіймати тунель. Це зрештує забезпечує безшовну інтеграцію віддаленого комп'ютера в доменну інфраструктуру klymchuk.net відразу після включення живлення пристрою, рис.3.53-3.55.

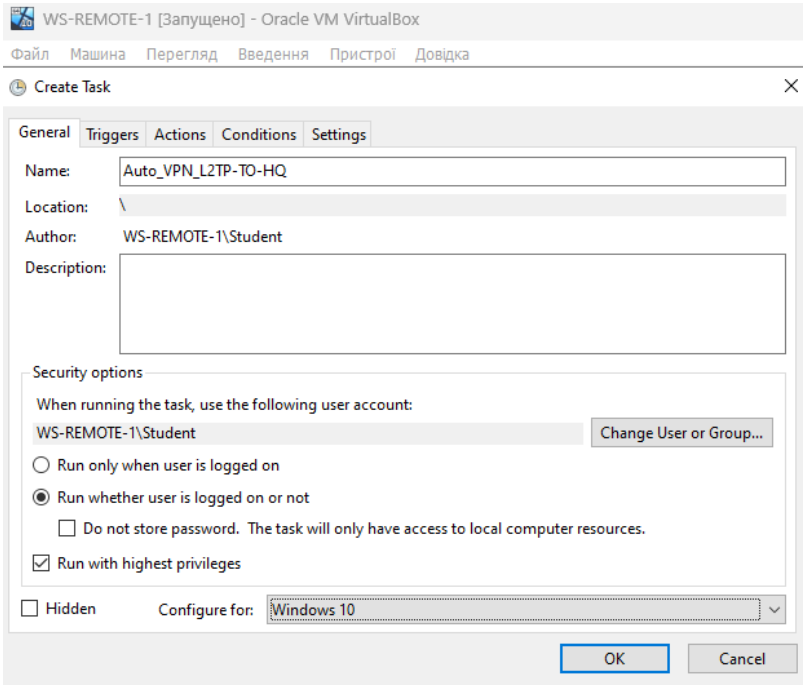


Рисунок 3.53 – Створення та конфігурація загальних параметрів автоматичного завдання Auto_VPN_L2TP-TO-HQ

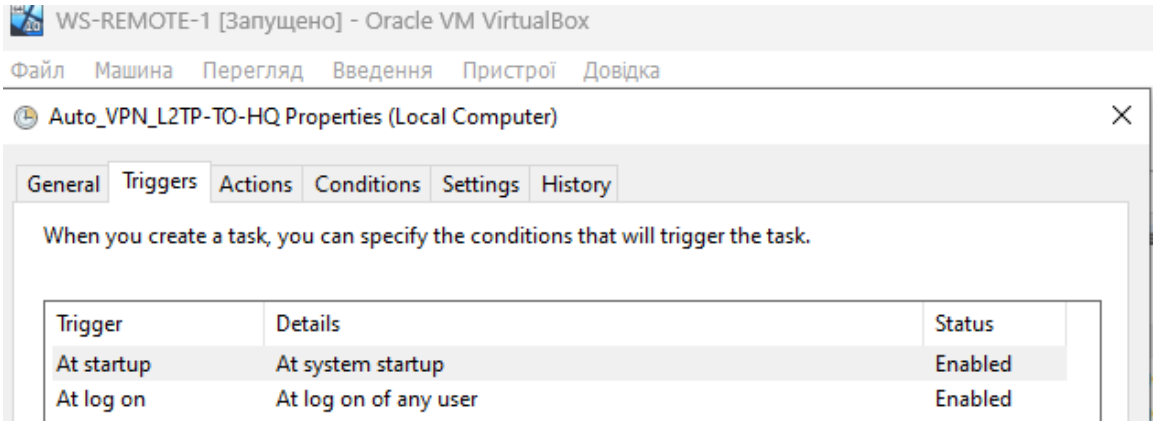


Рисунок 3.54 – Налаштування тригерів запуску завдання

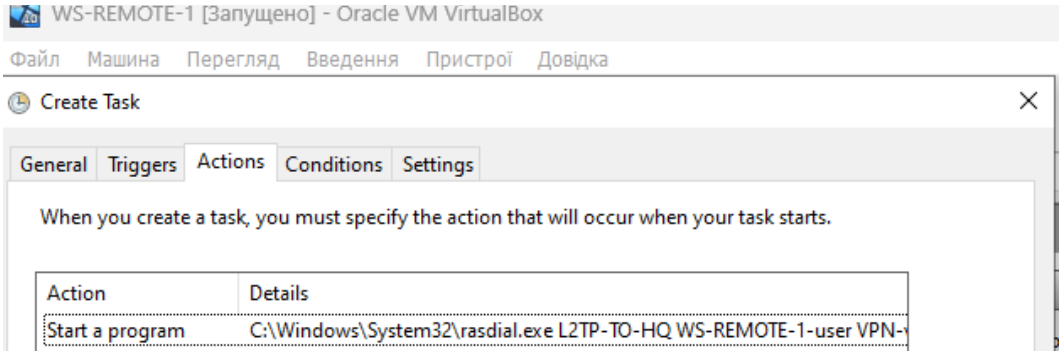


Рисунок 3.55 – Визначення виконуваної дії для автоматичної автентифікації через rasdial.exe

Після успішної конфігурації VPN-з'єднання на пристрої було успішно виконано вхід у систему під доменним обліковим записом користувача. Привітання користувача свідчить про те, що віддалена станція повноцінно інтегрована в корпоративну інфраструктуру, а налаштовані маршрути до мереж 172.22.1.0/24 та 172.22.2.0/24 забезпечують доступ до внутрішніх ресурсів домену, рис.3.56.

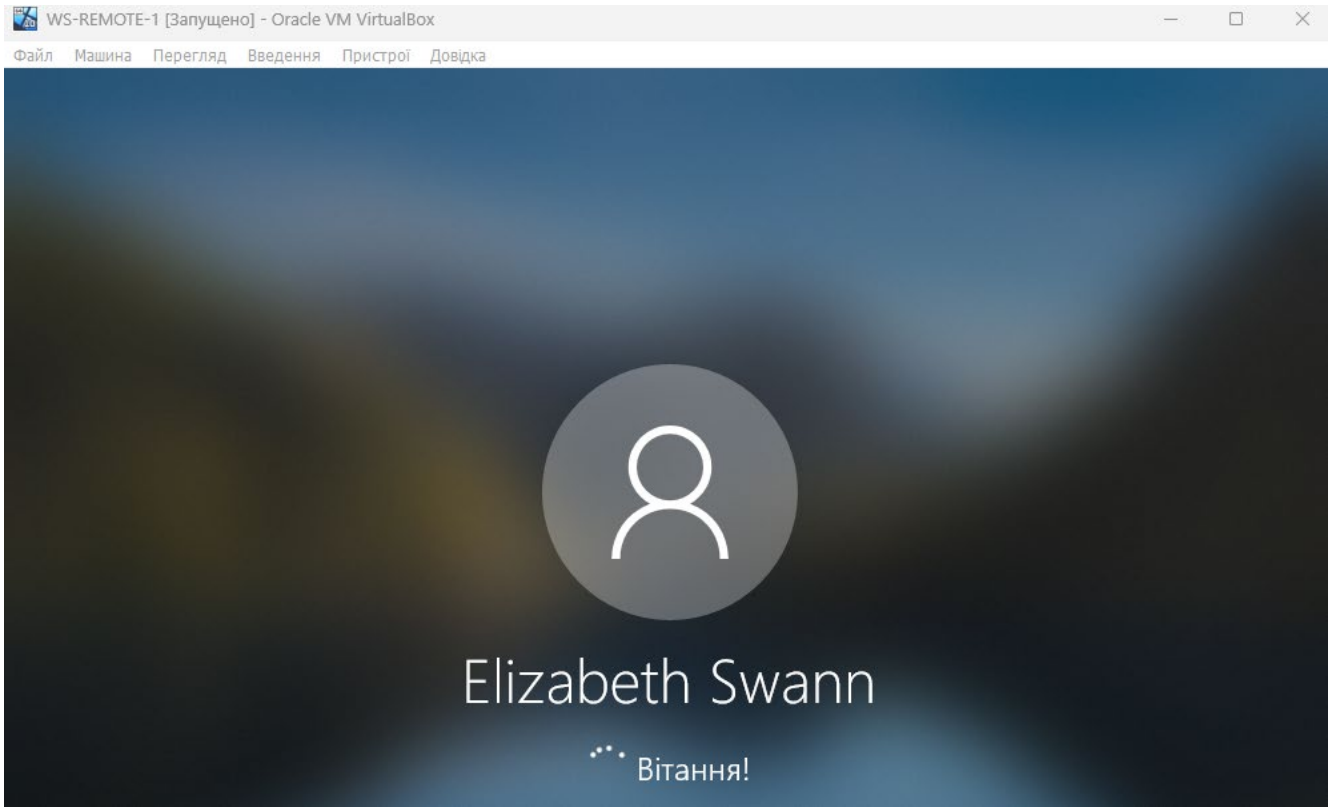


Рисунок 3.56 – Вхід у систему під доменним користувачем

3.4 Налаштування додаткових механізмів захисту

Для забезпечення централізованої автентифікації на мережних пристроях на сервері головного офісу було створено користувачів Tech-Cisco та Tech-Mikrotik, які були додані до групу безпеки network-admins, рис.3.57.

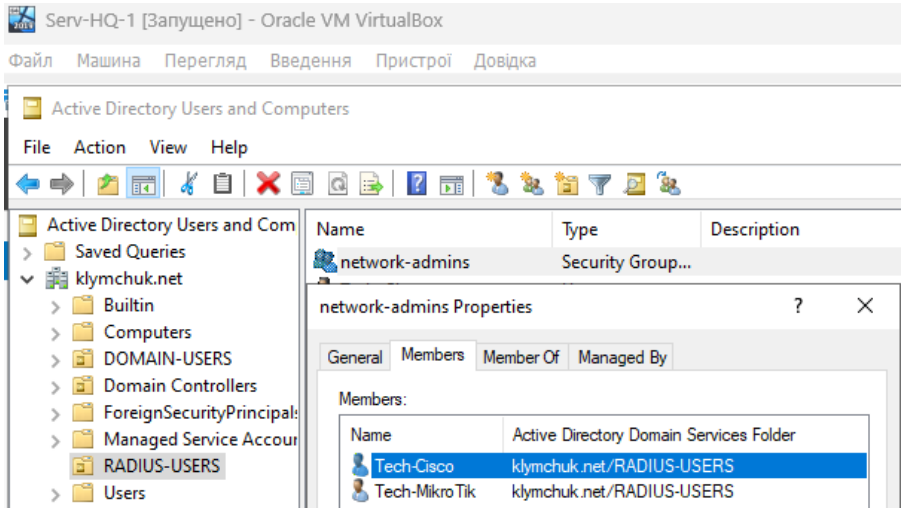


Рисунок 3.57 – Створення окремих користувачів та групи для аутентифікації на мережних пристроях

У консолі Network Policy Server (NPS) було виконано реєстрацію переліку всіх мережних пристроїв як RADIUS-клієнтів для забезпечення централізованої автентифікації в усій інфраструктурі, рис.3.58.

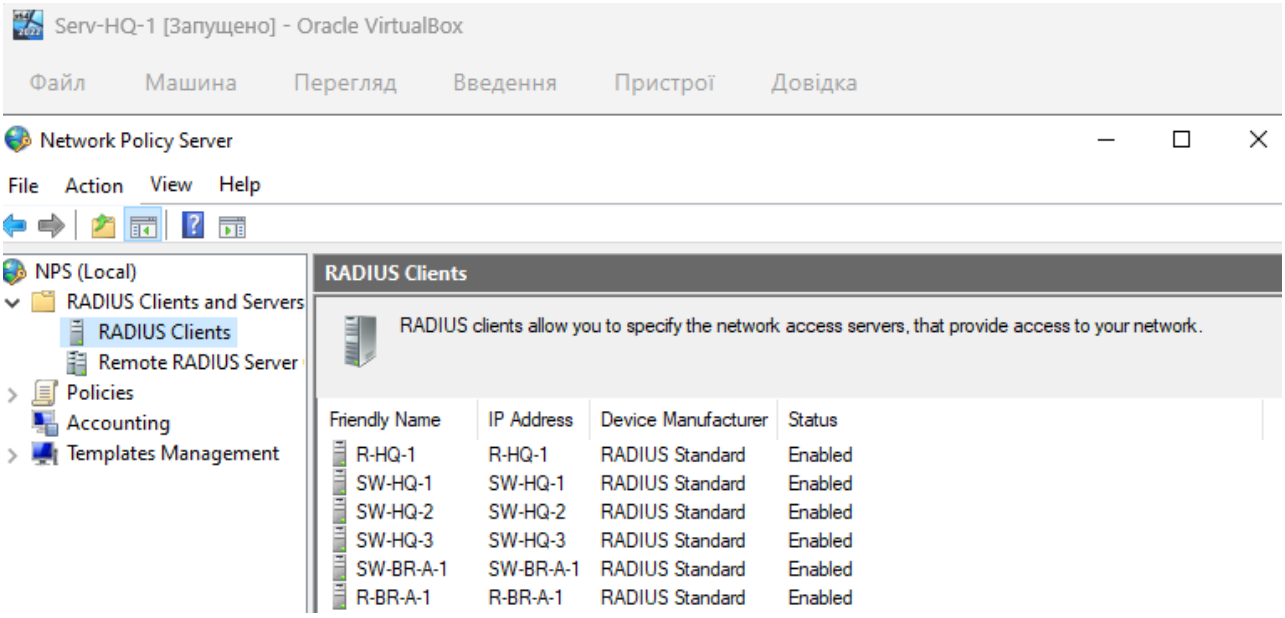


Рисунок 3.58 – Додання мережних пристроїв в ролі RADIUS-клієнтів

Для забезпечення розмежування прав доступу в консолі Network Policy Server (NPS) було створено дві спеціалізовані мережні політики Cisco-policy та Mikrotik-policy, які дозволяють розділяти правила доступу залежно від обладнання. Для політики Cisco-policy встановлено умову перевірки приналежності до групи network-admins та відповідність імені клієнта шаблону SW-, а в налаштуваннях додано специфічний атрибут Cisco-AV-Pair зі значенням shell:priv-lvl=15 для автоматичного надання максимальних привілеїв. Аналогічно для MikroTik-policy визначено умови для пристроїв з іменами, що починаються на R-, та налаштовано параметри протоколу PPP із використанням методів автентифікації MS-CHAP v1/v2. Таке налаштування гарантує, що сервер NPS не просто дозволяє вхід, а й передає пристроям конкретні інструкції щодо рівня доступу для кожного підключеного користувача, рис.3.59-3.60.

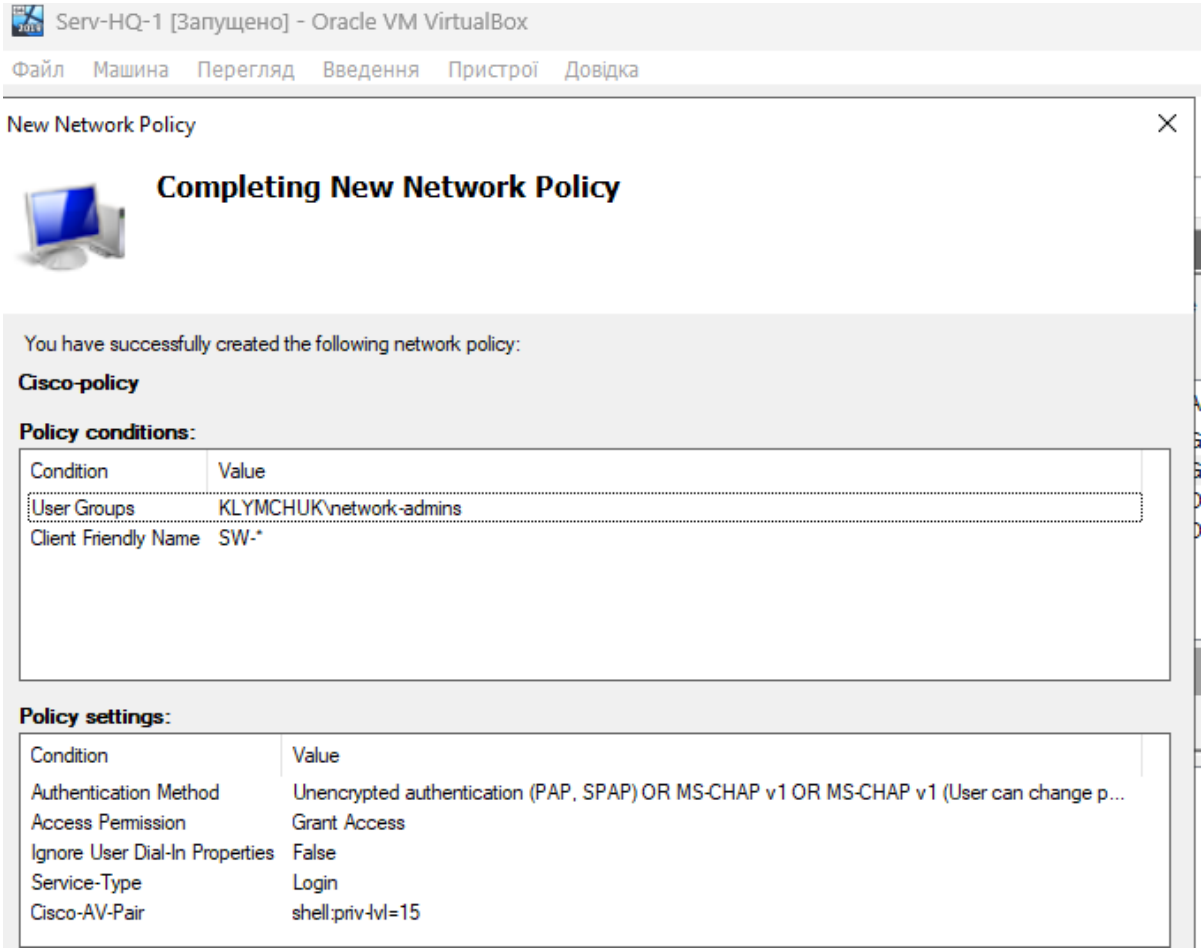


Рисунок 3.59 – Створення політики Cisco-policy з атрибутом Privilege Level 15

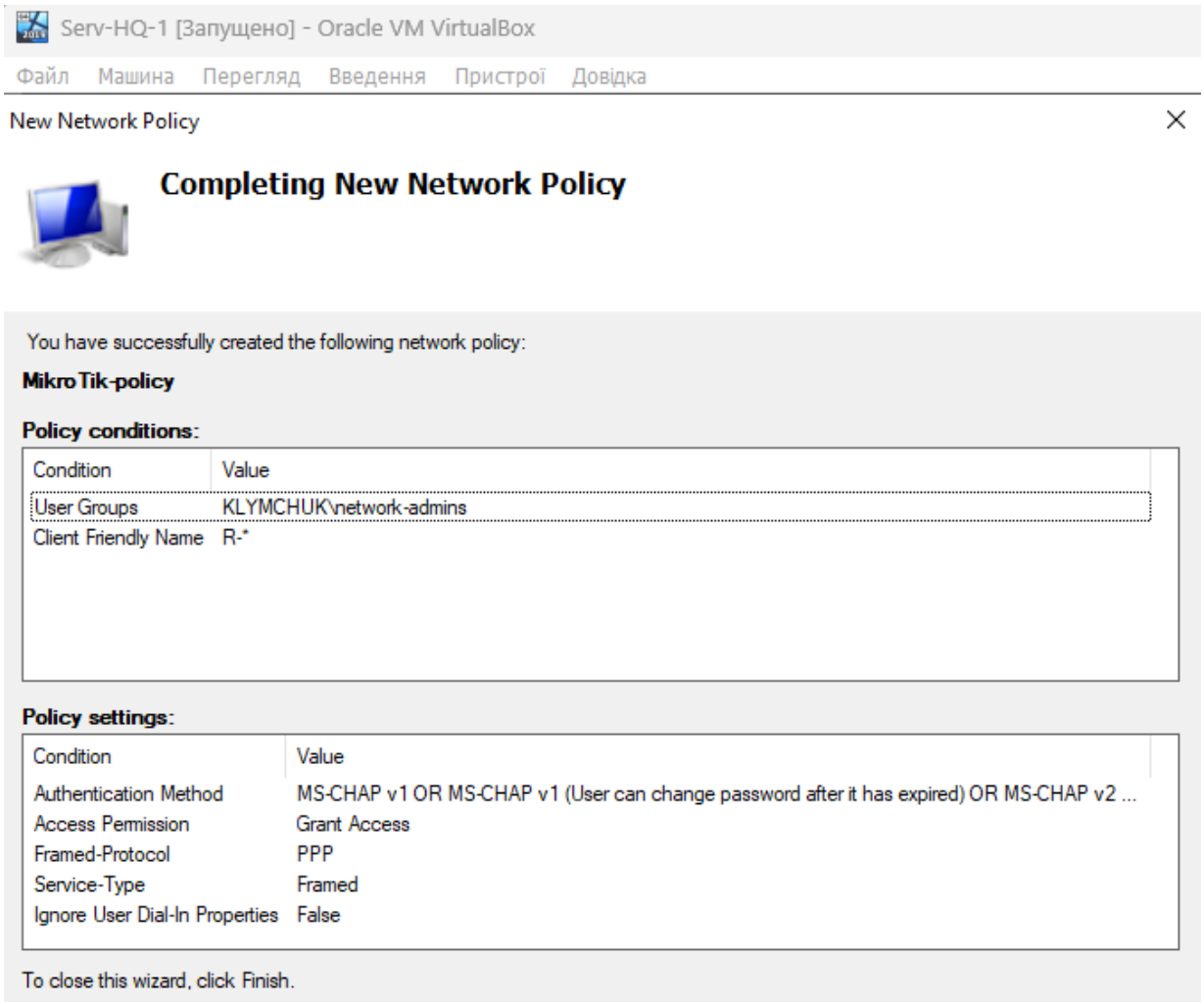


Рисунок 3.60 – Створення політики MikroTik-policy

Перейдемо до налаштування RADIUS на комутаторах Cisco. Спочатку командою aaa new-model активовано модель безпеки, після чого створено локальний резервний обліковий запис та пароль на режим enable для доступу у разі відсутності зв'язку з сервером. Наступним кроком налаштовано взаємодію з RADIUS-сервером Serv-HQ-1, де вказано порти 1812/1813 та спільний секрет radpass. За допомогою команд aaa authentication, authorization та accounting визначено пріоритетність RADIUS-сервера для входу користувачів та виконання команд, а також активовано передачу даних про дії адміністраторів (accounting). Для забезпечення можливості безпечного захищеного з’єднання через SSH було згенеровано RSA-ключі модулем 1024 біт, активовано SSH версії 2 з таймаутом 30 секунд та обмежено вхід на лініях vty 0 4 виключно через протокол SSH, рис.3.61.

```
SW-HQ-1(config)#aaa new-model
SW-HQ-1(config)#username local-admin privilege 15 secret admin-pass
SW-HQ-1(config)#enable secret enable-pass
SW-HQ-1(config)#radius server Serv-HQ-1
SW-HQ-1(config-radius-server)#address ipv4 Serv-HQ-1 auth-port 1812 acct-port 1813
SW-HQ-1(config-radius-server)#key radpass
SW-HQ-1(config-radius-server)#exit
SW-HQ-1(config)#aaa authentication login default group radius local
SW-HQ-1(config)#aaa authorization exec default group radius local
SW-HQ-1(config)#aaa accounting exec default start-stop group radius
SW-HQ-1(config)#aaa authorization console
SW-HQ-1(config)#line cons 0
SW-HQ-1(config-line)#authorization exec default
SW-HQ-1(config-line)#exit
SW-HQ-1(config)#crypto key generate rsa modulus 1024
% You already have RSA keys defined named SW-HQ-1.klymchuk.net.
% They will be replaced.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

SW-HQ-1(config)#ip ssh version 2
SW-HQ-1(config)#ip ssh time-out 30
SW-HQ-1(config)#line vty 0 4
SW-HQ-1(config-line)#transport input ssh
```

Рисунок 3.61 – Налаштування механізму AAA та протоколу SSH на комутаторах Cisco

На обох маршрутизаторах MikroTik (R-HQ-1 та R-BR-A-1) було виконано налаштування RADIUS-клієнта, де у розділі RADIUS додано новий сервер із адресою 172.22.1.99, активовано сервіс login та вказано спільний секрет, що відповідає UDP-портам 1812 та 1813, рис.3.62. Паралельно з цим у розділі System -> Users у вікні налаштувань AAA активовано параметри Use RADIUS та Accounting, що дозволяє пристрою перенаправляти запити на авторизацію до сервера NPS та вести облік дій користувачів. Це зрештою дозволяє адміністраторам з доменної групи network-admins використовувати свої облікові записи для входу на пристрої, рис.3.63.

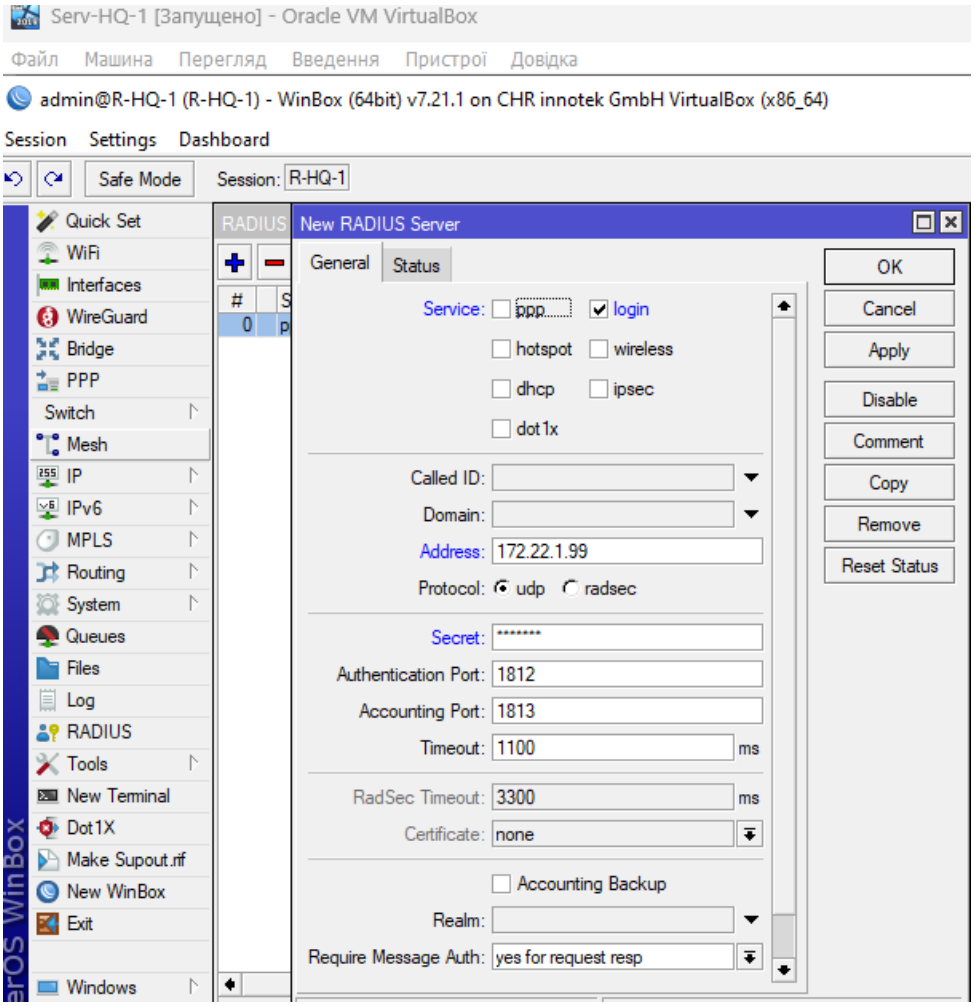


Рисунок 3.62 – Конфігурація підключення до RADIUS-сервера в RouterOS

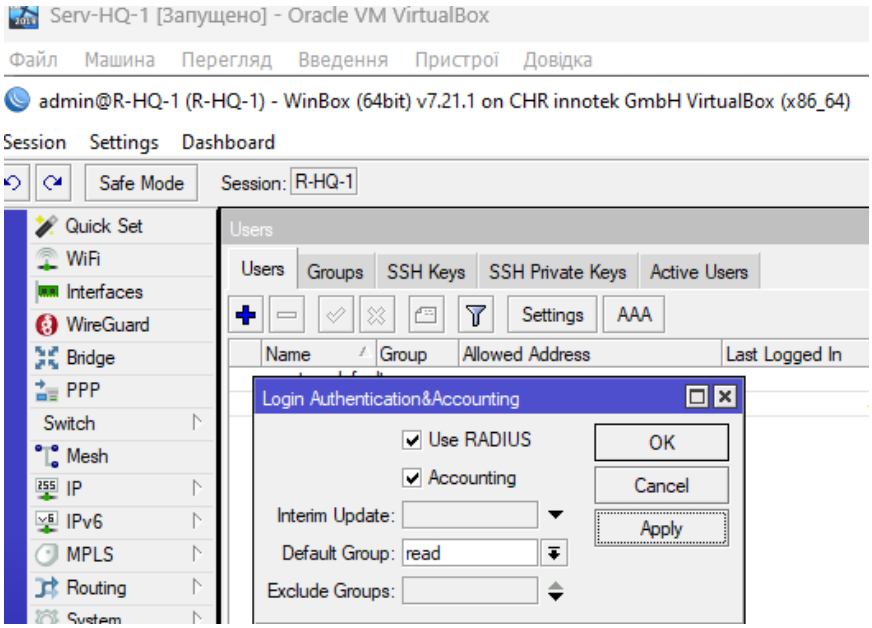


Рисунок 3.63 – Активація використання RADIUS для автентифікації та обліку користувачів MikroTik

Syslog

Для організації централізованого збору та аналізу системних подій у мережній інфраструктурі на сервері Serv-HQ-1 було встановлено безкоштовне програмне забезпечення Visual Syslog Server, яке дозволяє в реальному часі відстежувати повідомлення від пристроїв, рис.3.64 [31].

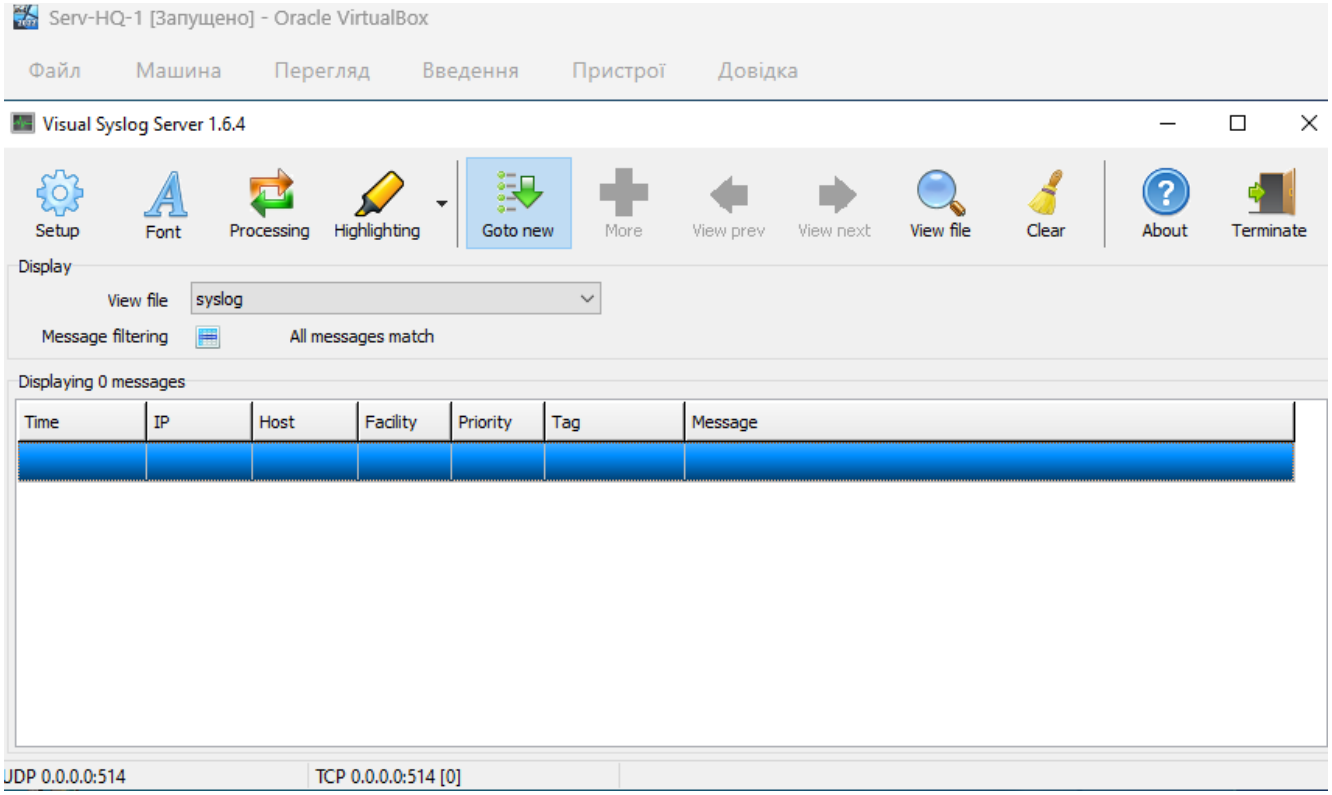


Рисунок 3.64 – Активація використання RADIUS для автентифікації та обліку користувачів MikroTik

Далі на обох маршрутизаторах MikroTik у меню System -> Logging було відредаговану дію з назвою remote, де було вказано адресу сервера Serv-HQ-1.klymchuk.net, порт 514 та протокол UDP для передачі даних у форматі BSD syslog. Після цього у вкладці Rules додано відповідні правила, які перенаправляють системні повідомлення типів account, critical, error, info, system та warning на створений віддалений сервер, що повну видимість ключових подій на пристрої, рис.3.65-3.66.

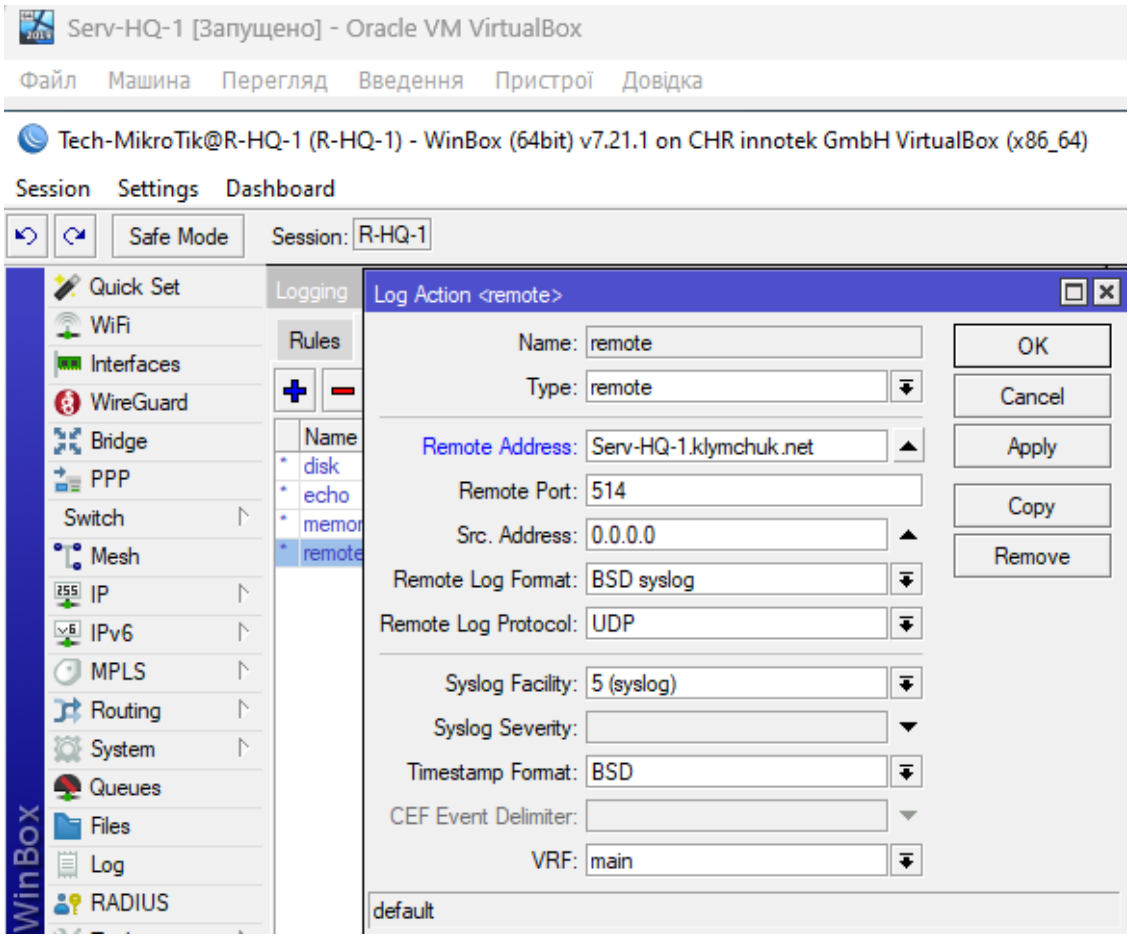


Рисунок 3.65 – Налаштування параметрів віддаленого логування в MikroTik

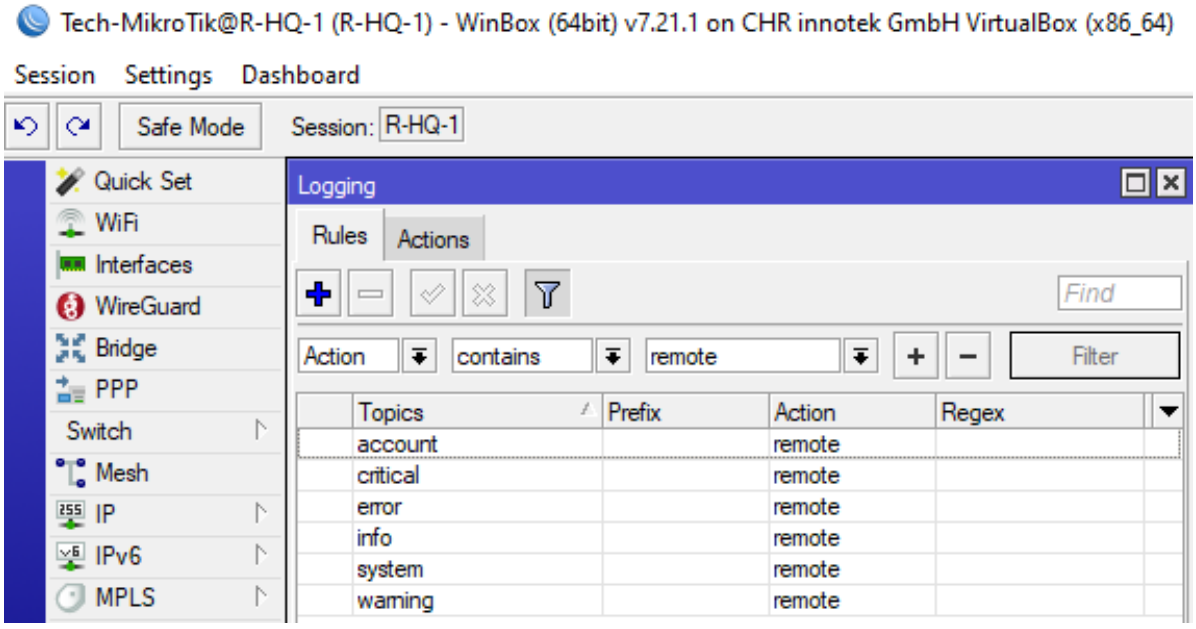


Рисунок 3.66 – Вибір типу системних подій для відправки на сервер

Перейдемо до комутаторів. Для забезпечення точності часових міток у системних журналах на всіх комутаторах Cisco було виконано синхронізацію часу. Спочатку командами clock timezone EEST 2 та clock summer-time встановлено часовий пояс і правила переходу на літній час, а за допомогою ntp server time.in.ua активовано синхронізацію з зовнішнім сервером точного часу. Для інформативності звітів налаштовано сервіс міток часу service timestamps log datetime msec localtime show-timezone, що дозволяє фіксувати події з точністю до мілісекунди. На завершення встановлено рівень деталізації logging trap informational та вказано адресу сервера збору повідомлень logging host Serv-HQ-1, що в поєднанні з командою logging on гарантує миттєву передачу всіх важливих системних подій на раніше розгорнутий Visual Syslog Server, рис.3.67.

```
SW-HQ-1(config)#clock timezone EEST 2
SW-HQ-1(config)#clock summer-time EET recurring last Sun Mar 3:00 last Sun Oct 4:00
SW-HQ-1(config)#ntp update-calendar
SW-HQ-1(config)#ntp server time.in.ua
SW-HQ-1(config)#service timestamps debug datetime msec localtime show-timezone
SW-HQ-1(config)#service timestamps log datetime msec localtime show-timezone
SW-HQ-1(config)#login on-failure log
SW-HQ-1(config)#login on-success log
SW-HQ-1(config)#logging trap informational
SW-HQ-1(config)#logging host Serv-HQ-1
SW-HQ-1(config)#logging on
```

Рисунок 3.67 – Налаштування синхронізації часу (NTP) та параметрів відправки системних логів на комутаторах Cisco

Firewall

Для забезпечення безпеки пристроїв «із коробки» маршрутизатори MikroTik під керуванням RouterOS вже мають ряд передвстановлених правил міжмережного екрана, які захищають пристрій від зовнішніх загроз. Ці правила включають дозвіл на вхідний трафік для вже встановлених з'єднань (established, related, untracked), дозвіл протоколу ICMP для діагностики та специфічних служб на кшталт IPsec, тоді як підозрілі або невалідні пакети автоматично відкидаються. Особливо важливою є наявність правила drop all not coming from LAN, яке за замовчуванням блокує будь-які спроби несанкціонованого доступу до маршрутизатора з боку зовнішньої мережі (WAN), дозволяючи при цьому взаємодію з напрямку локальної мережі до Інтернету, рис.3.68.

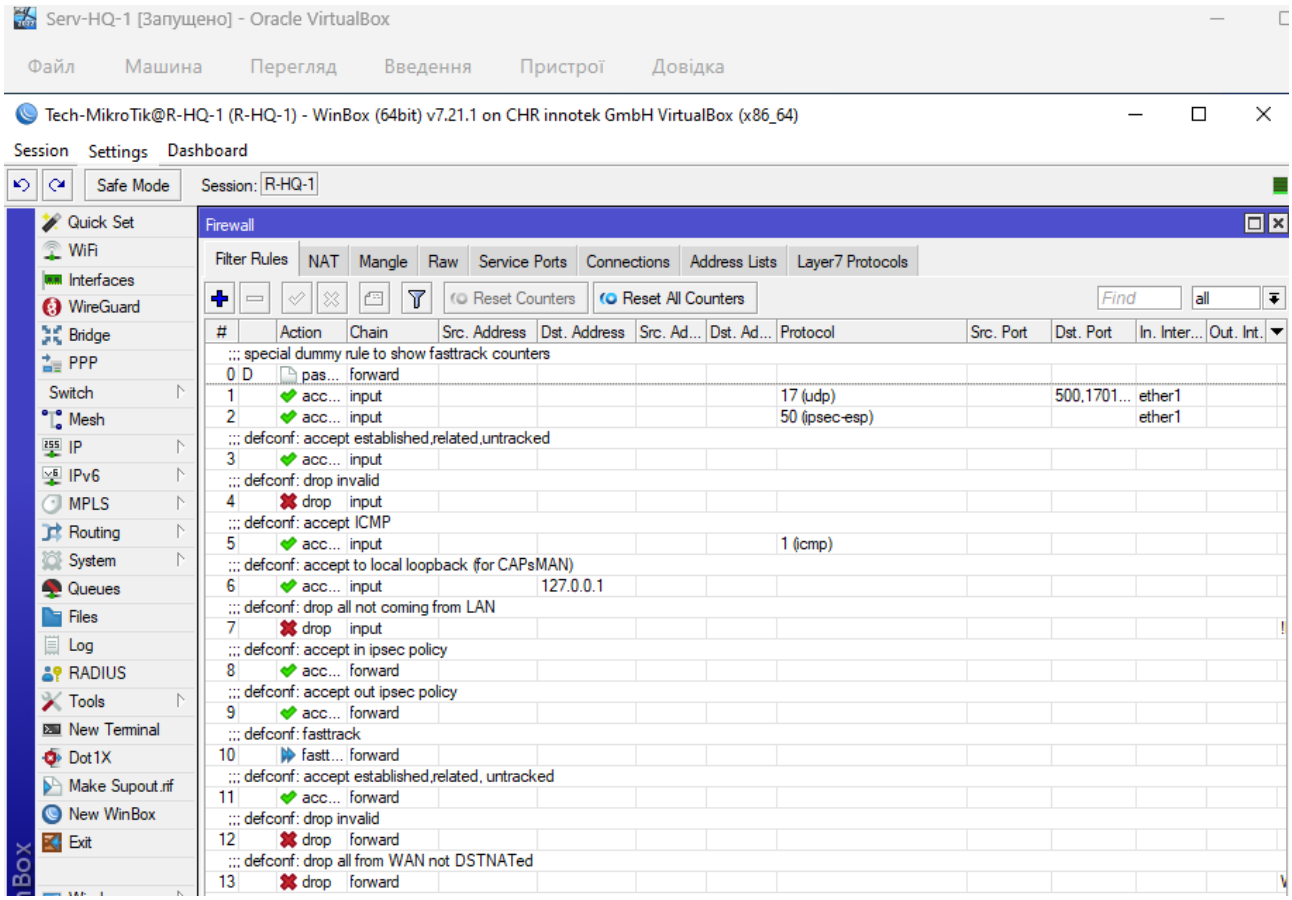


Рисунок 3.68 – Стандартний набір передвстановлених правил фаєрвола MikroTik

Відключення незадіяних портів

Для посилення фізичної безпеки мережної інфраструктури на всіх комутаторах Cisco було створено окрему ізольовану VLAN 1001 з назвою UNUSED-PORTS, до якої було переведено всі незадіяні інтерфейси у режимі доступу (switchport mode access). І далі дані порти були примусово вимкнені командою shutdown, що гарантує неможливість їх використання у разі підключення невідомого обладнання, рис.3.69.

```
SW-HQ-1(config)#vlan 1001
SW-HQ-1(config-vlan)#name UNUSED-PORTS
SW-HQ-1(config-vlan)#exit
SW-HQ-1(config)#interface range eth0/2-3, eth1/0-3, eth2/0-3, eth3/0-1
SW-HQ-1(config-if-range)#switchport mode access
SW-HQ-1(config-if-range)#switchport access vlan 1001
SW-HQ-1(config-if-range)#shutdown
```

Рисунок 3.69 – Ізоляція та деактивація незадіяних портів на комутаторах Cisco

3.5 Перевірка роботи мережі і впроваджених засобів

Перейдемо до перевірки роботи мережі. Для початку підключимось до маршрутизатора R-HQ-1 за допомогою спеціального доменного облікового запису Tech-MikroTik. Під час авторизації через утиліту WinBox було використано доменні облікові дані, після чого RADIUS-сервер (NPS) успішно верифікував користувача та надав йому доступ до керування пристроєм. У розділі System -> Users -> Active Users зафіксовано активну сесію користувача Tech-MikroTik, де вказано, що вхід здійснено з IP-адреси сервера 172.22.1.99 через сервіс winbox, що підтверджує працездатність механізмів авторизації з використанням RADIUS-сервера, рис.3.70-3.71.

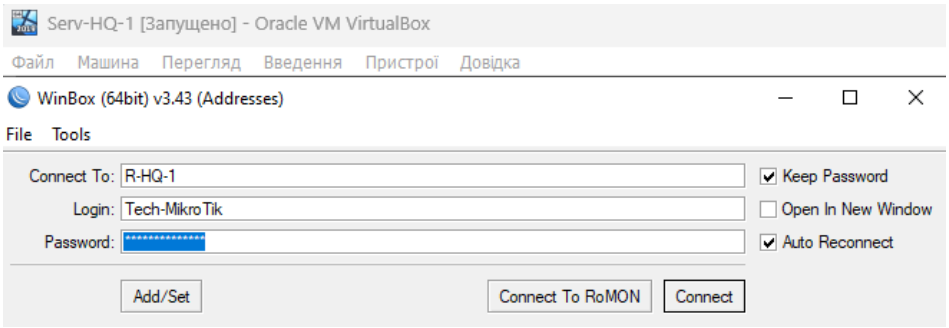


Рисунок 3.70 – Підключення до маршрутизатора R-HQ-1 за допомогою доменного облікового запису Tech-MikroTik

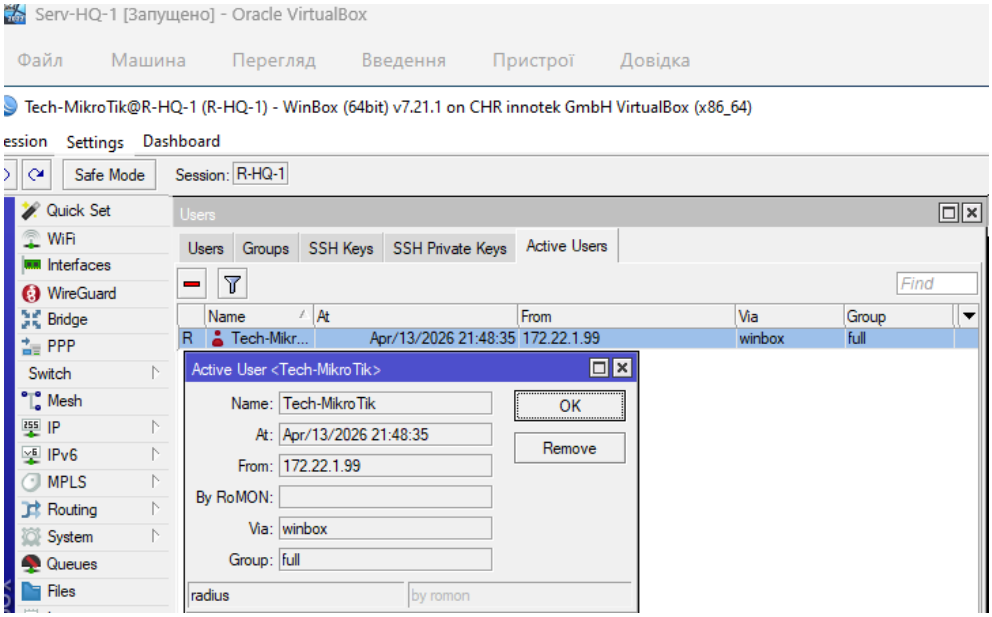


Рисунок 3.71 – Відображення активної сесії RADIUS-користувача Tech-MikroTik

Додатковим підтвердженням коректності аутентифікації користувача Tech-MikroTik є перегляд подій через Windows Event Viewer, де зафіксовано подію з ID 6272, яка свідчить про успішне надання доступу сервером NPS для користувача KLYMCHUK\Tech-MikroTik, рис.3.72. Паралельно в інтерфейсі Visual Syslog Server з'явилося інформаційне повідомлення від хоста R-HQ-1, що доводить повну працездатність системи відправки подій до SYSLOG-сервера та аутентифікації з використанням RADIUS, рис.3.73.

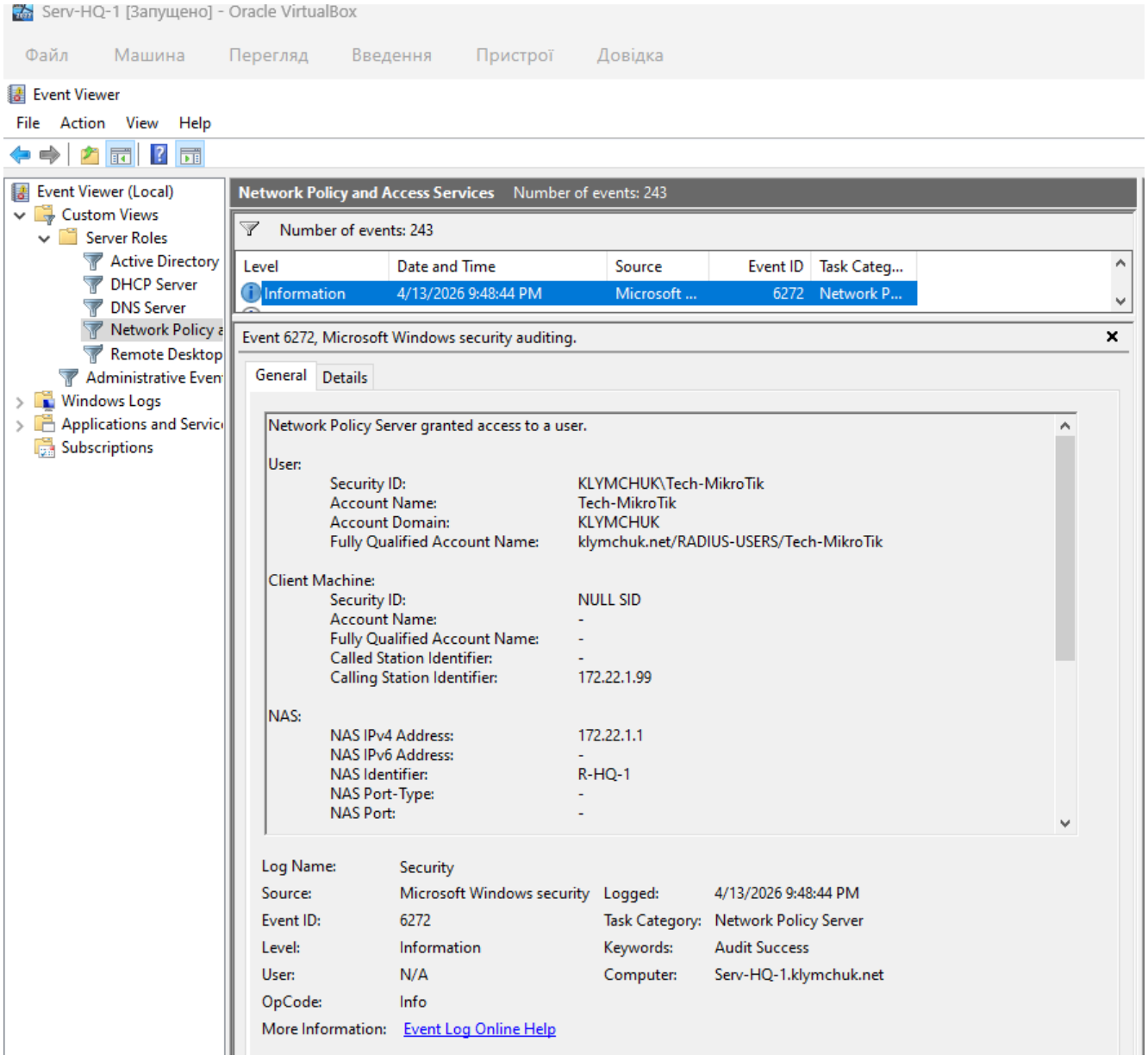


Рисунок 3.72 – Журнал подій NPS про успішну автентифікацію Tech-MikroTik

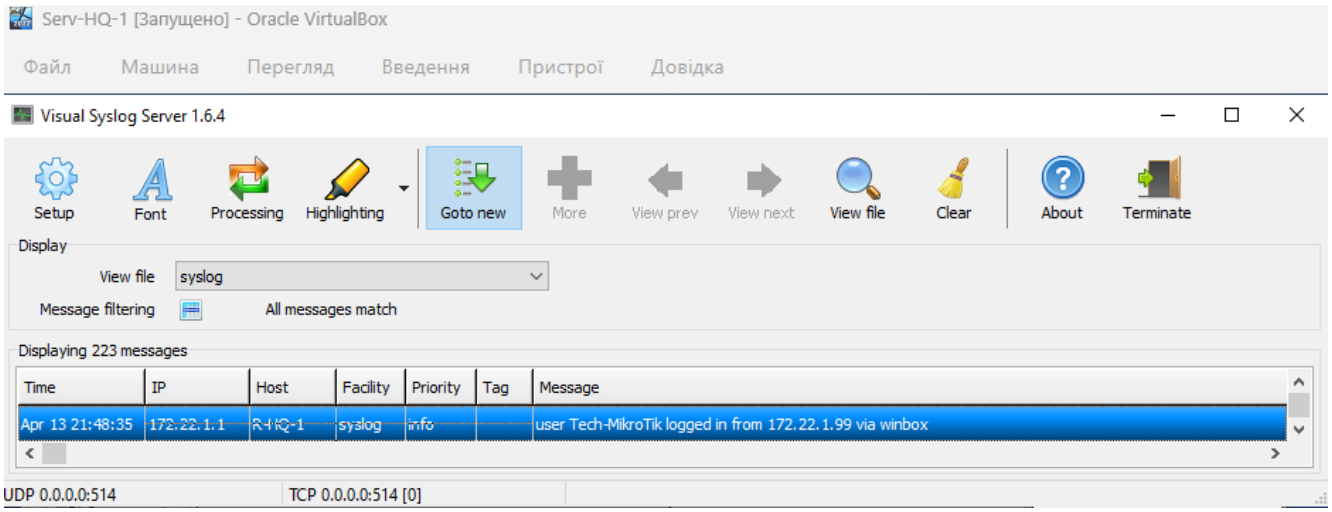


Рисунок 3.73 – Реєстрація події входу в Visual Syslog Server

Перевірка роботи DHCP та DNS

Далі перевіримо коректність роботи DHCP-серверів на сервері головного офісу (Serv-HQ-1) та маршрутизаторі віддаленого підрозділу (R-BR-A-1). Для цього виведемо призначені IP-адреси кінцевим пристроям, рис.3.74-3.75.

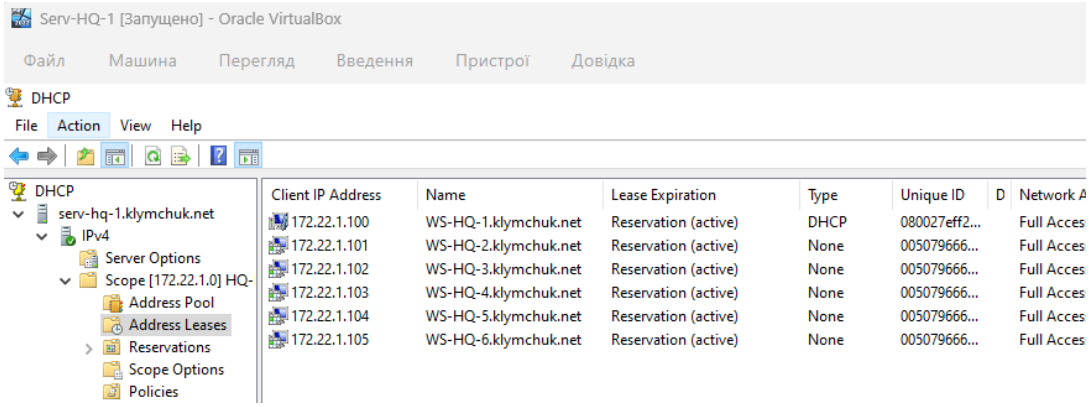


Рисунок 3.75 – Перевірка виданих адрес DHCP-сервером на Serv-HQ-1

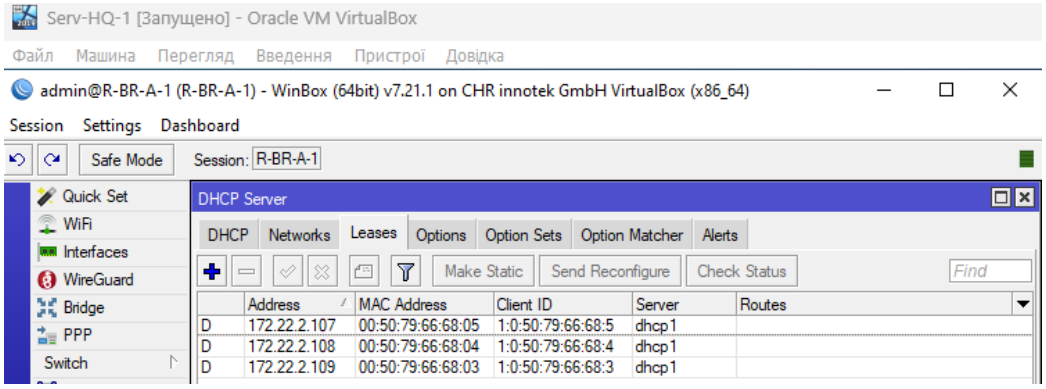


Рисунок 3.75 – Перевірка виданих адрес DHCP-сервером на R-BR-A-1

Після чого проведемо перевірку зв'язку між усіма сегментами мережі використовуючи доменні імена пристроїв, рис.3.76-3.78.

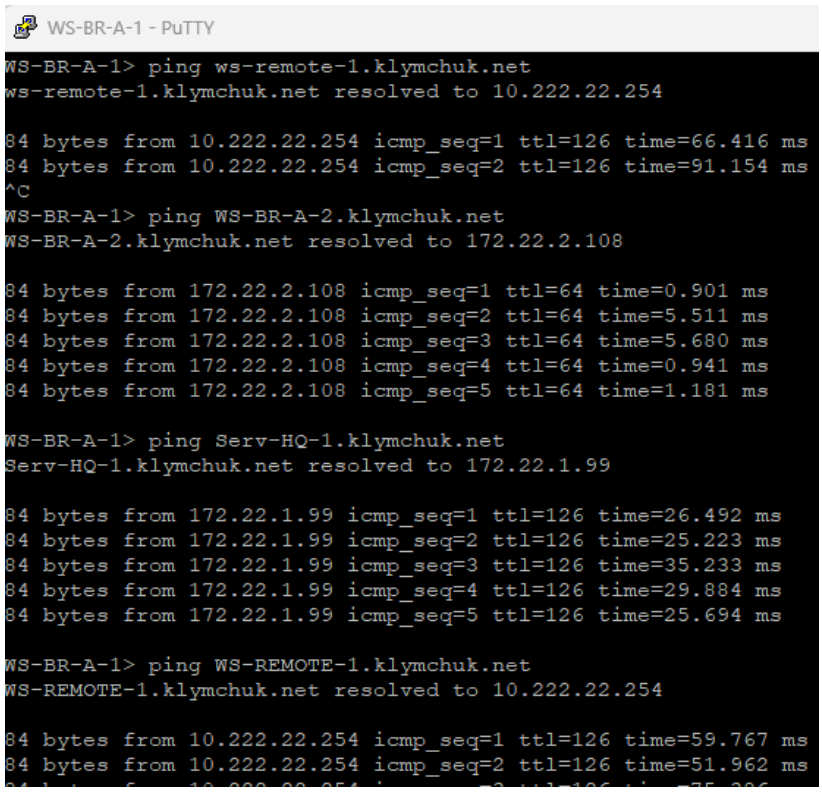


Рисунок 3.76 – Перевірка зв'язку зі станції підрозділу А

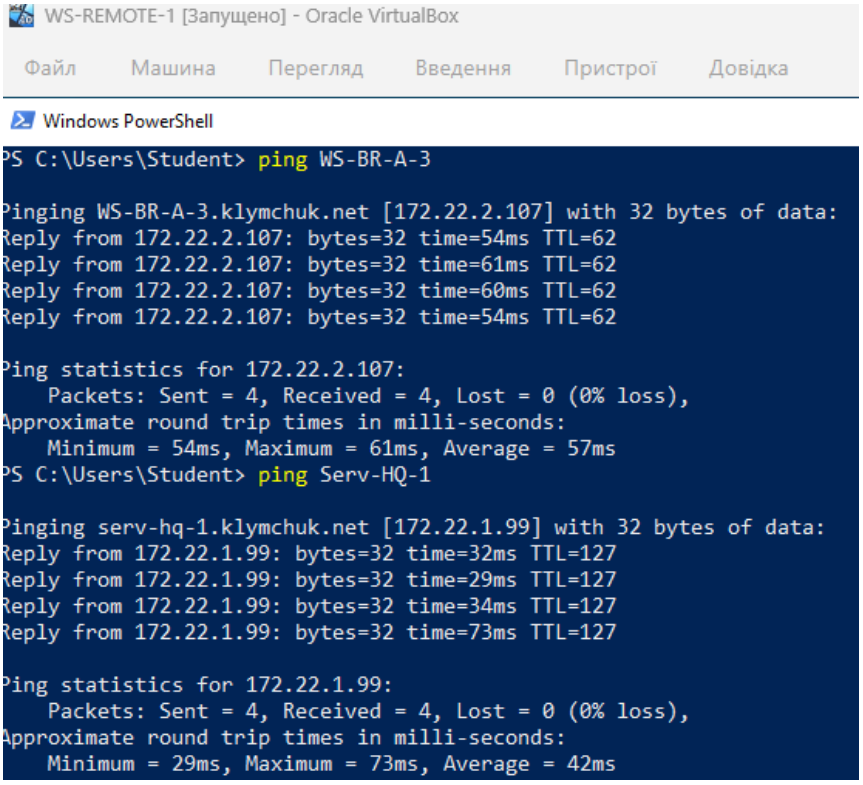


Рисунок 3.77 – Перевірка зв'язку зі станції віддаленого користувача

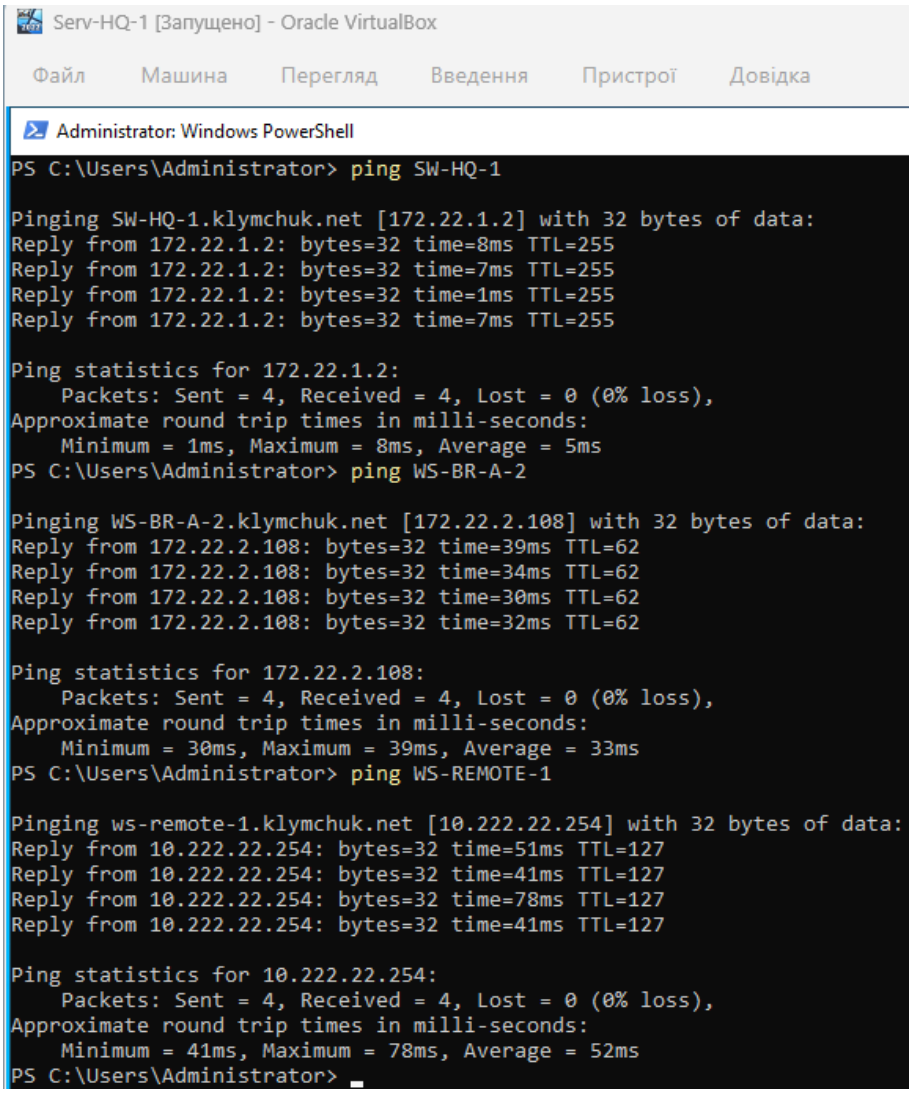


Рисунок 3.78 – Перевірка зв'язку зі серверу головного офісу

SSH

Тепер проведемо перевірку можливості віддаленого підключення до комутаторів через SSH. Для цього з використанням утиліти PuTTY виконаємо підключення до пристрою SW-HQ-1 під користувачем Tech-Cisco. Після успішного підключення перевіряємо рівень привілеїв командою show privileges, а show users підтверджує активну сесію на лінії vty 0 з IP-адреси сервера 172.22.1.99. Паралельно з цим, на у вікні Visual Syslog Server відображаються системні повідомлення від хоста 172.22.1.2, які свідчать, що користувач Tech-Cisco успішно підключився, а потім відключився від пристрою, рис.3.79-3.80.

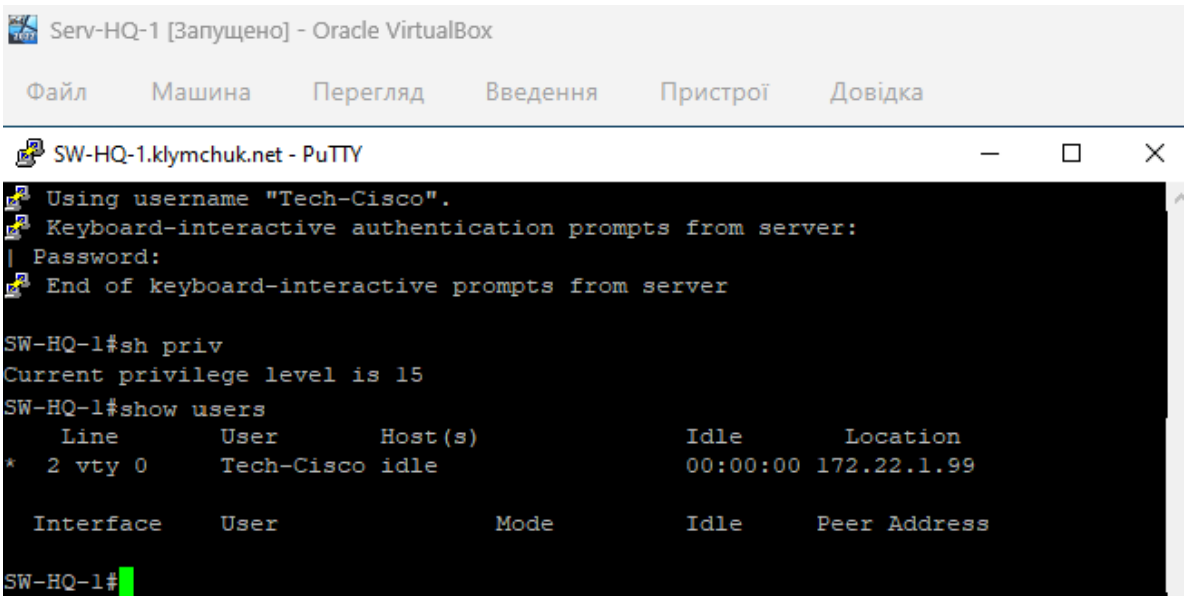


Рисунок 3.79 – Підключення до SW-HQ-1 через SSH

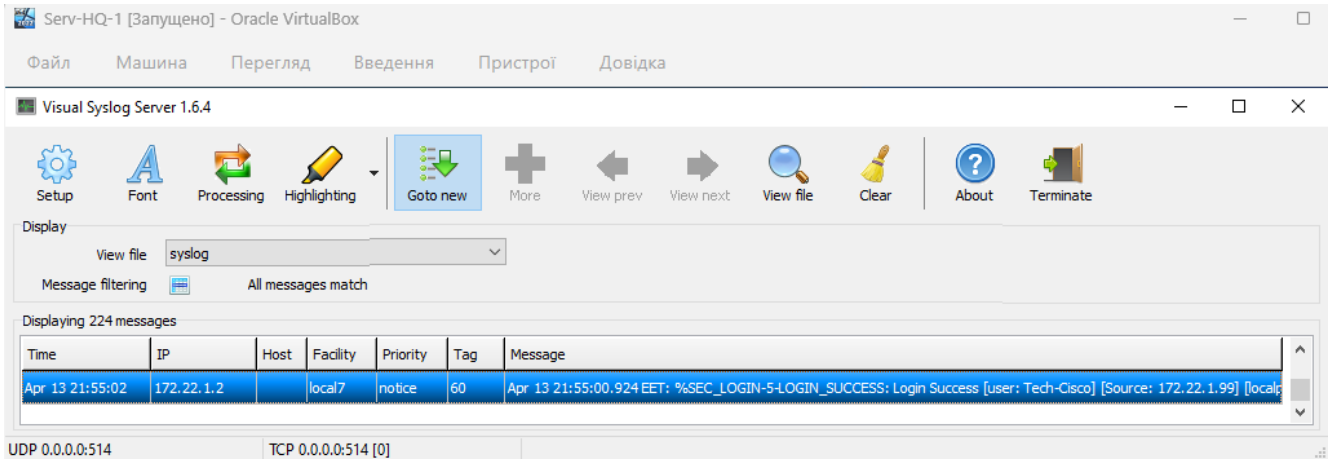


Рисунок 3.80 – Логування подій аутентифікації користувача

L2TP/IPsec

Переглянемо детальну інформацію про роботу VPN-сервера. На пристроїв R-HQ-1 у розділі PPP на вкладці Interface наявно два активних тунельних інтерфейсів <l2tp-R-BR-A-1-user> та <l2tp-WS-REMOTE-1-user klymchuk.net>. Тут можна отримати детальну інформацію про дату останнього підключення, час безперервної роботи (Uptime), використаний логін користувача, тип шифрування, параметри MTU/MRU та переглянути IP-адресацію клієнтів VPN, рис.3.81.

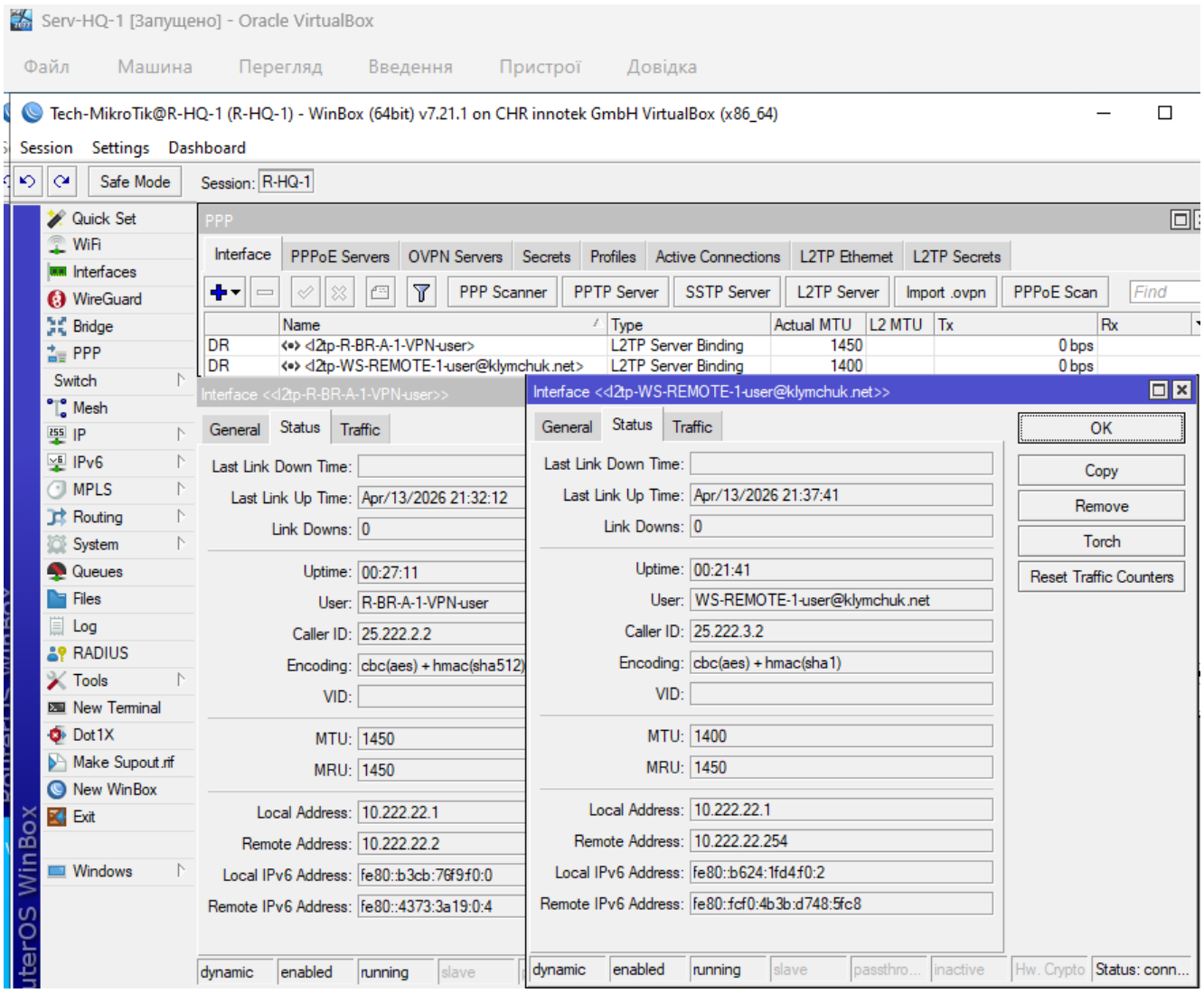


Рисунок 3.81 – Детальна інформація про статус L2TP-сесії та параметри шифрування на інтерфейсі сервера.

Водночас на вкладці Active Connections зафіксовано сесії для користувачів R-BR-A-1-VPN-user та WS-REMOTE-1-user@klymchuk.net, для яких використовується шифрування cbc(aes) + hmac(sha512/sha1). Зокрема, у вікні параметрів можна переглянути назву активного з'єднання, тип сервісу (l2tp), отриману адресу, час роботи сесії (Uptime). Також значення Caller ID містить IP-адресу клієнта, яка була зафіксована під час його підключення, рис.3.82.

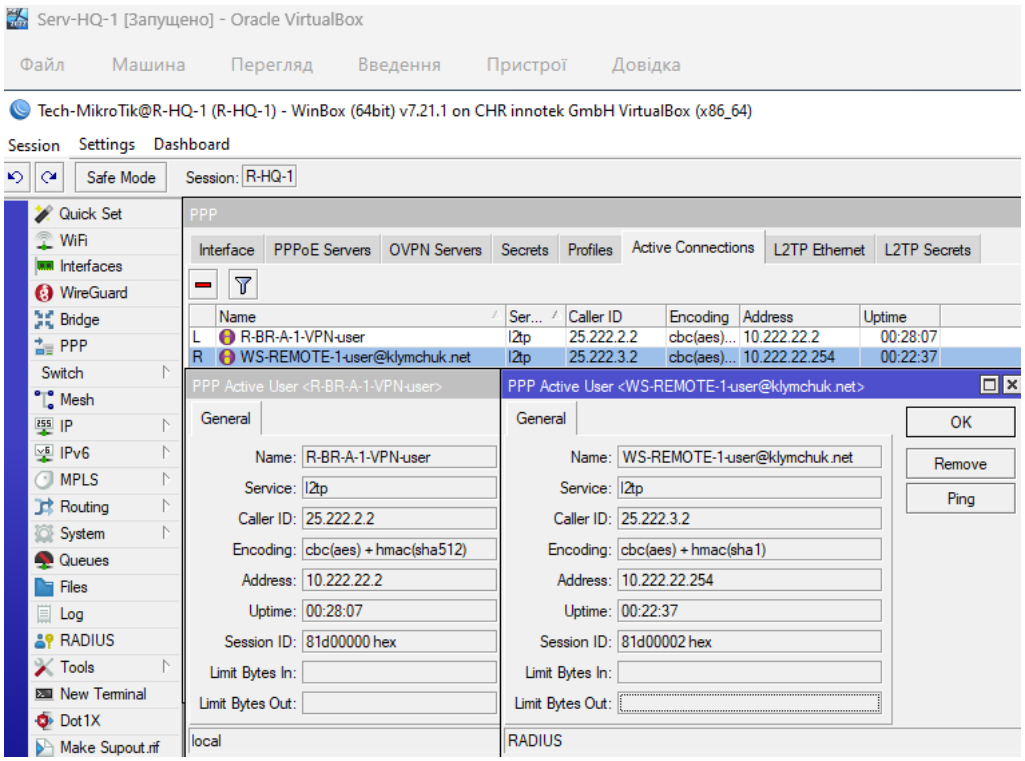


Рисунок 3.82 – Список активних VPN-підключень користувачів

На маршрутизаторі підрозділу R-BR-A-1 у розділі PPP на вкладці Interface можна переглянути статус інтерфейсу l2tp-out1, рис.3.83.

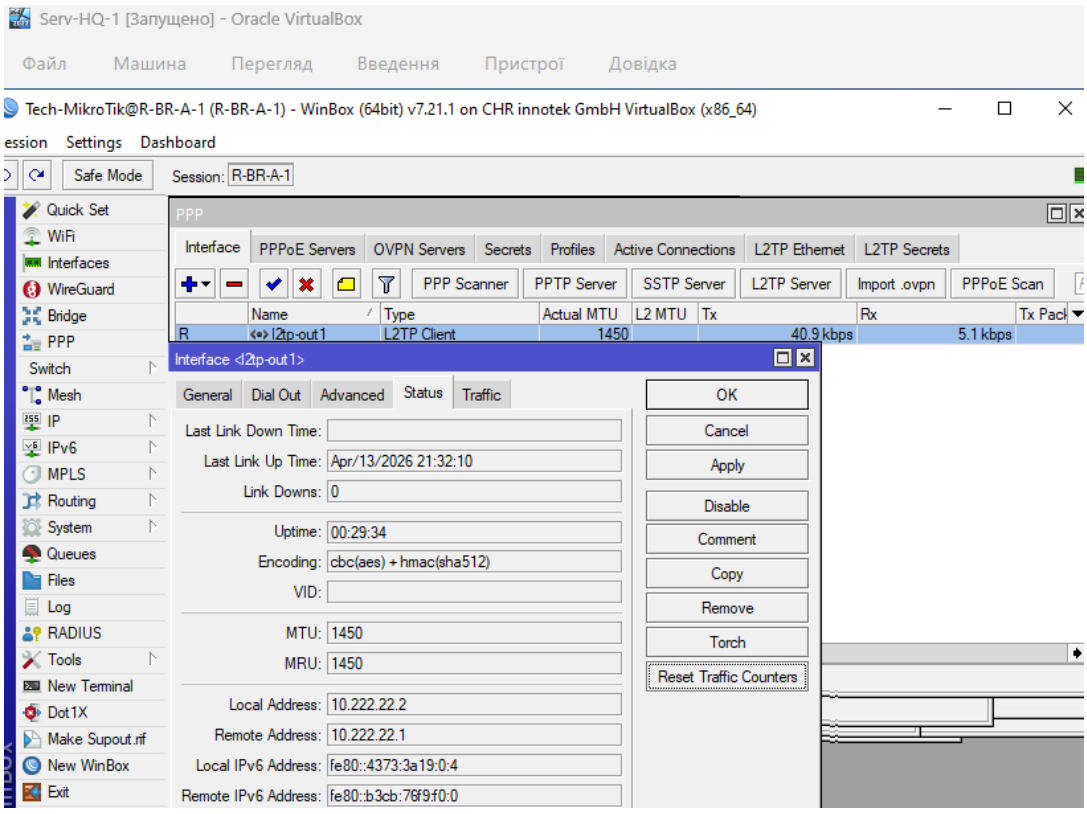


Рисунок 3.83 – Статус та параметри L2TP-клієнта на маршрутизаторі R-BR-A-1

Лишається перевірити параметри віддаленої робочої станції WS-REMOTE-1. Через консоль PowerShell було виведено параметри віртуально VPN-інтерфейсу (L2TP-TO-HQ). Можна побачити, що комп'ютером від VPN-серверу було отримано IPv4-адресу 10.222.22.254 із маскою підмережі 255.255.255.255. Також перевірено призначення DNS-сервера з адресою 10.222.22.1, що відповідає внутрішній VPN-адресі головного маршрутизатора, рис.3.84.

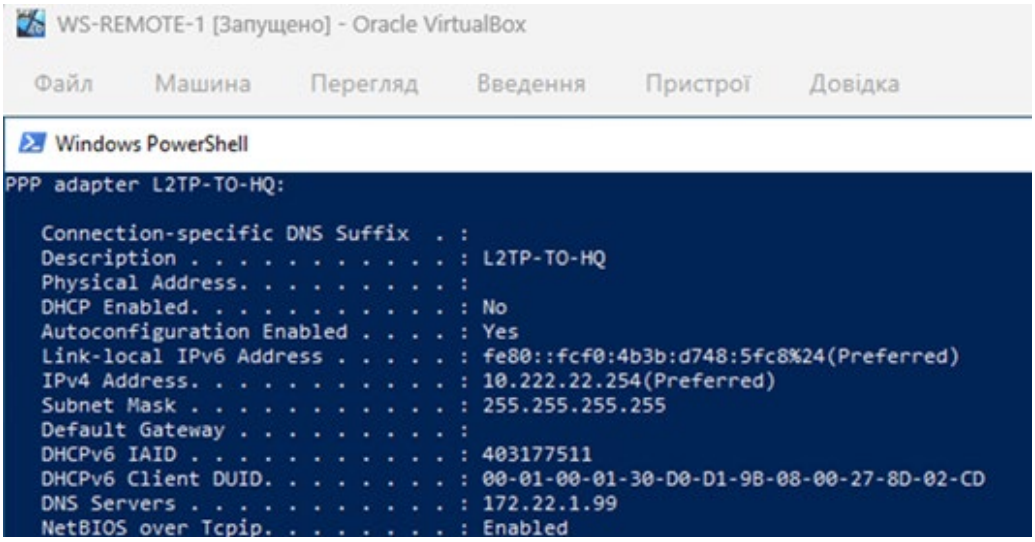


Рисунок 3.84 – Перевірка мережних параметрів VPN-адаптера

Виконання команди Get-NetRoute -InterfaceAlias "L2TP-TO-HQ" підтверджує, що маршрути до мережі головного офісу (172.22.1.0/24) та підрозділу А (172.22.2.0/24) були успішно додані до таблиці маршрутизації VPN, рис.3.85.

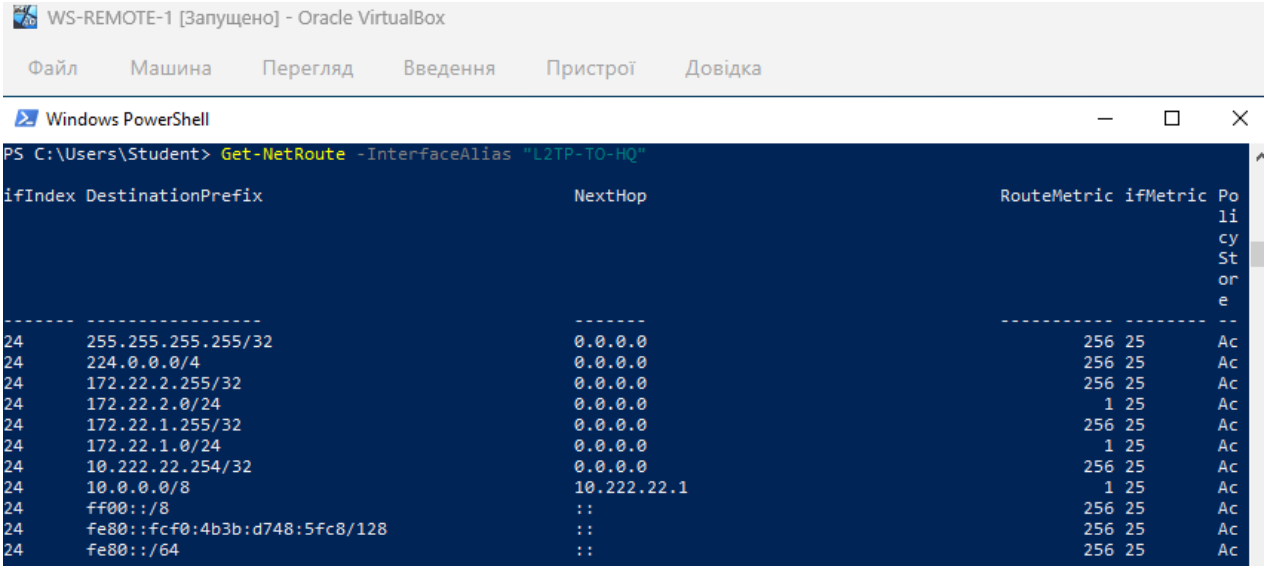


Рисунок 3.85 – Перевірка таблиці маршрутизації для VPN-з'єднання

Наостанок проаналізуємо структуру пакетів, які проходять через VPN-тунель. Для цього виконаємо пінг від віддаленої станції до сервера Serv-HQ-1 і паралельно з цим виконаємо перехоплення пакетів на виході з комп'ютера з використанням Wireshark. Як можна помітити усі пакети, що прямували до корпоративної мережі були ідентифіковані, як протокол ESP (Encapsulating Security Payload), що підтверджує роботу IPsec у транспортному режимі. Вміст пакетів повністю зашифрований, а для ідентифікації зашифрованих пакетів використовуються значення SPI, що зрештує унеможливлює перегляд переданих даних без відповідних ключів шифрування, рис.3.86.

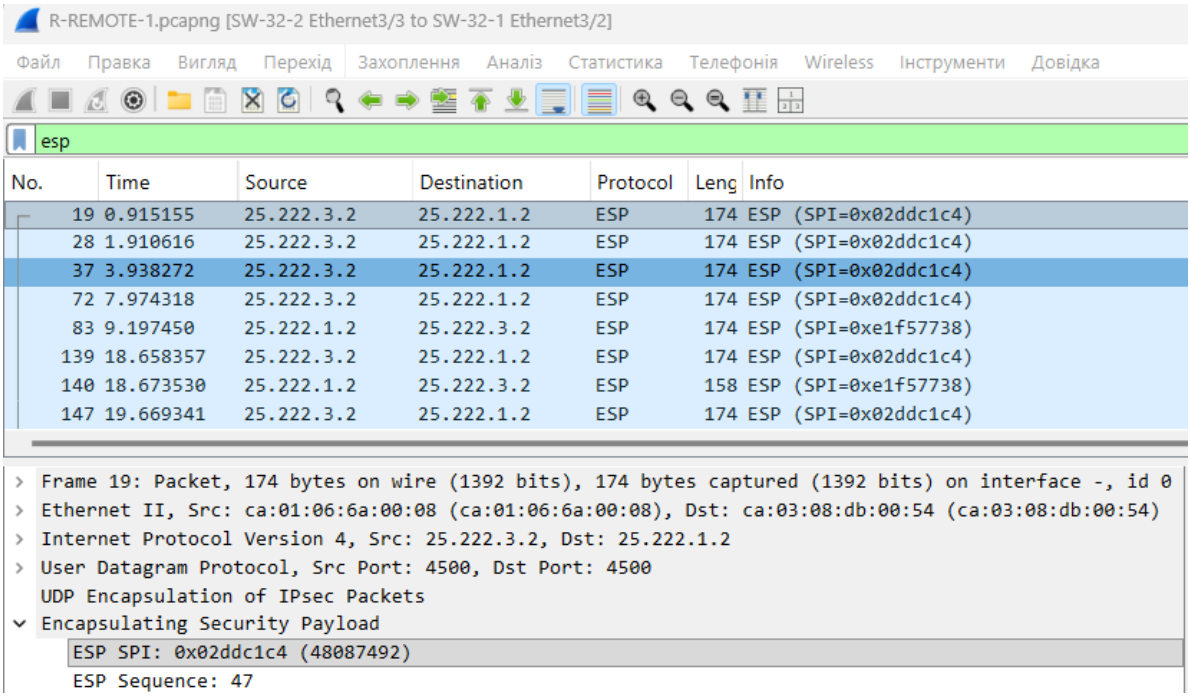


Рисунок 3.86 – Аналіз перехопленого IPsec-трафіку від віддаленої станції до серверу головного офісу з використанням Wireshark

Водночас з цим виконаємо перехоплення пакетів вже на сервері головного офісу, тобто вже після розшифрування пакетів на маршрутизаторі. Аналіз перехоплення показує, що пакети, які надсилаються з віддаленої станції з IP-адресою 10.222.22.254 (VPN-адреса), досягають сервера і отримують відповіді, при цьому протокол ідентифікується вже як чистий ICMP, а не зашифрований ESP. Це свідчить про те, що VPN-шлюз MikroTik на вході в центральну мережу HQ успішно знімає шифрування та направляє трафік у локальний сегмент у розшифрованому

стані, що дозволяє системним сервісам та аналізаторам трафіку бачити вміст запитів усередині локальної мережі, рис.3.87.

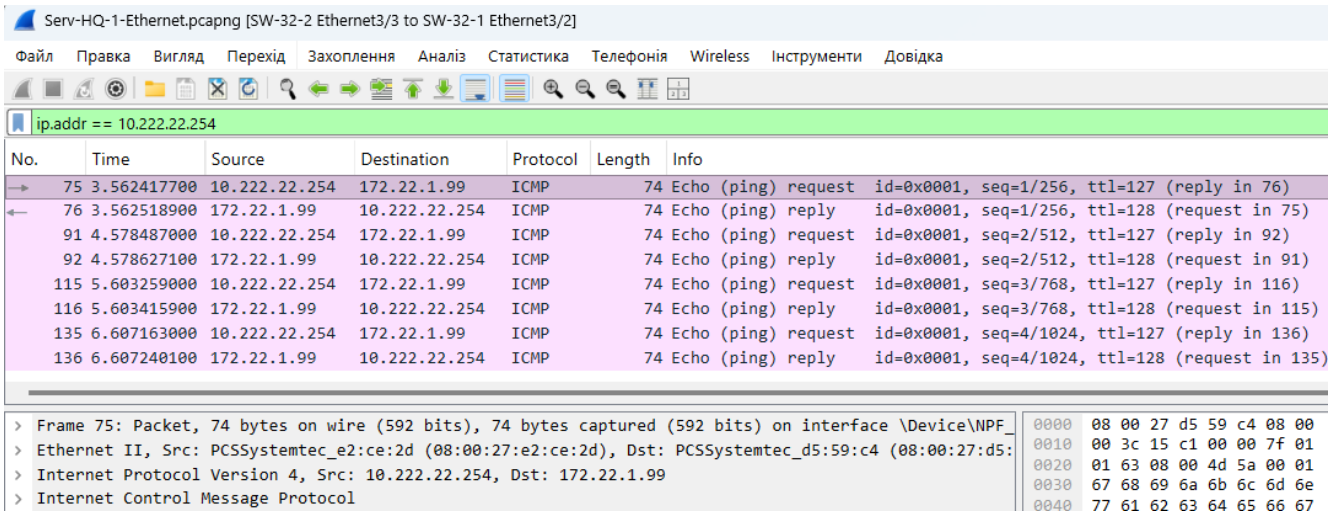


Рисунок 3.87 – Аналіз декапсульованого ICMP-трафіку від VPN-клієнта на Serv-HQ-1 з використанням Wireshark

Висновки до третього розділу

У ході реалізації третього розділу було проведено розгортання та базову конфігурацію спроєктованої мережі в середовищі емулятора GNS3. На базі Windows Server було успішно ініціалізовано доменну інфраструктуру klymchuk.net, розгорнуто ролі Active Directory, DNS та DHCP, а також налаштовано RADIUS-сервер для майбутньої автентифікації VPN-з'єднань. Процес налаштування маршрутизаторів MikroTik (R-HQ-1 та R-BR-A-1) охопив конфігурування інтерфейсів, встановлення статичної адресації, налаштування маршрутизації за замовчуванням та правил NAT для забезпечення виходу в Інтернет. Результатом цього стало успішне приєднання робочих станцій до домену.

Для забезпечення захищеної взаємодії між локаціями було сконфігуровано тунель L2TP/IPsec типу Site-to-Site, що дозволило об'єднати ресурси головного офісу та філії в єдиний. Паралельно з цим реалізовано модель Remote Access для віддалених працівників, де завдяки інтеграції ролі Network Policy Server було впроваджено централізовану автентифікацію через протокол RADIUS, що дозволило звіряти облікові дані користувачів з базою Active Directory.

Було реалізовано комплекс заходів із захисту та моніторингу інфраструктури. Центральною ланкою безпеки стало впровадження моделі AAA через протокол RADIUS. Налаштовано роботу Syslog на сервері, на який налаштовано передачу системних логів з усіх вузлів мережі. Фізичний та мережний рівні захисту посилено шляхом активації SSH v2, впровадження суворих правил фаєрволів на пристроях MikroTik за принципом «заборонити все, що не дозволено явно» та програмної ізоляції незадіяних портів комутаторів.

Етап верифікації підтвердив повну функціональну відповідність розгорнутої мережі вимогам безпеки та доступності. Тестування механізмів RADIUS засвідчило успішну автентифікацію на обладнанні Cisco та MikroTik та миттєвою реєстрацією подій у журналах Windows Event Viewer і Visual Syslog Server. Перевірка мережних служб продемонструвала стабільну роботу DHCP та коректне розв'язання доменних імен у зоні klymchuk.net для всіх сегментів інфраструктури. Аналіз трафіку за допомогою Wireshark показав, що пакети між сегментами мережі в публічній мережі передаються виключно у зашифрованому вигляді, тоді як усередині локального сегмента трафік успішно декансулюється. Це свідчить про повну реалізацію головних цілей проєкту, а саме створення цілісної, керованої та захищеної розподіленої інфраструктури.

ВИСНОВКИ

У межах виконання кваліфікаційної роботи було здійснено дослідження, проєктування та практичну реалізацію захищеної інфраструктури розподіленої корпоративної мережі організації.

Проведено теоретичний аналіз сучасних технологій VPN та порівняльну характеристику протоколів тунелювання. Обгрунтовано вибір стеку L2TP/IPsec як найбільш раціонального рішення, що забезпечує високу криптографічну стійкість та має кросплатформенну сумісність. За результатами аналізу ринку мережного обладнання доведено економічну та функціональну доцільність рішень MikroTik

На основі трирівневої ієрархічної моделі розроблено фізичну та логічну топології розподіленої мережі, розраховано схему IP-адресації та підібрано апаратне забезпечення. Спроєктовано підсистему централізованого контролю доступу на базі протоколу RADIUS та служби Active Directory та динамічного призначення VPN-атрибутів користувачам.

Здійснено практичне розгортання спроєктованої архітектури в емуляційному середовищі GNS3, де на базі Windows Server реалізовано доменні ролі. На маршрутизаторах MikroTik налаштовано NAT, правила фаєрвола, логування Syslog та успішно побудовано зашифровані тунелі L2TP/IPsec типу Site-to-Site та Remote Access з використанням RADIUS та Active Directory. Всі кінцеві станції Windows успішно додані до єдиного домену.

Проведено комплексне тестування мережі, яке підтвердило роботу доменних сервісів у всіх сегментах та успішну автентифікацію локальних та віддалених користувачів. Успішна тестування роботи мережі та аналіз перехопленого у Wireshark трафіку підтвердили роботу служб домену, автентифікацію користувачів і шифрування пакетів у публічній мережі через тунелі L2TP/IPsec.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Birru NK (2025) The Future of Work in a Secure, Always-On World, European Journal of Computer Science and Information Technology, 13 (30), 111-121

2. Network Security Concepts, Dangers, and Defense Best Practical. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/369739760_Network_Security_Concepts_Dangers_and_Defense_Best_Practical

3. What Is the CIA Triad? [Електронний ресурс]. – Режим доступу: https://www.fortinet.com/resources/cyberglossary/cia-triad

4. Defense in Depth: A Guide to Layered Cybersecurity. [Електронний ресурс]. – Режим доступу: https://www.datacamp.com/fr/tutorial/defense-in-depth

5. Aslan, Ö.; Aktuğ, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics 2023, 12, 1333.

6. What is Zero Trust architecture? [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/en-us/security/business/security-101/what-is-zero-trust-architecture

7. Cisco Networking. [Електронний ресурс]. – Режим доступу: https://www.cisco.com/site/us/en/products/networking/index.html

8. Juniper zero trust data center solution brief. [Електронний ресурс]. – Режим доступу: https://www.juniper.net/content/dam/www/assets/solution-briefs/us/en/juniper-zero-trust-data-center-solution-brief.pdf

9. Fortinet. [Електронний ресурс]. – Режим доступу: https://www.fortinet.com/corporate/about-us/about-us

10. Mikrotik. [Електронний ресурс]. – Режим доступу: https://mikrotik.com/aboutus

11. Stephen Discher. RouterOS by Example, 2nd Edition: B&W, 2016 - 440 pages.

12. What is the MikroTik RouterOS? Features & Capabilities. [Електронний ресурс]. – Режим доступу: https://www.netmaker.io/resources/mikrotik-routeros

13. MikroTik Documentation. [Електронний ресурс]. – Режим доступу: https://help.mikrotik.com/docs/spaces/ROS/pages/119144597/Virtual+Private+Networks

14. Virtual Private Network: Survey and Research Challenges. (2025). International Journal of Latest Technology in Engineering Management & Applied Science, 14(6), 211-226

15. What Is Site-to-Site VPN and How It Works? [Електронний ресурс]. – Режим доступу: https://www.anyviewer.com/how-to/what-is-site-to-site-vpn-2578.html

16. Personal VPN. [Електронний ресурс]. – Режим доступу: https://www.hkcert.org/blog/learn-about-personal-vpn-services-protect-online-privacy-and-security

17. Comparing VPN Protocols on MikroTik. [Електронний ресурс]. – Режим доступу: https://mikrotikusers.com/comparing-vpn-protocols-on-mikrotik-routers/

18. Types of VPN Protocols. [Електронний ресурс]. – Режим доступу: https://zoogvpn.com/vpn-protocols

19. VPN protocols comparison. [Електронний ресурс]. – Режим доступу: https://nordlayer.com/learn/vpn/protocols-comparison/

20. Який протокол VPN є найкращим? [Електронний ресурс]. – Режим доступу: https://surfshark.com/uk/blog/vpn-protocols

21. Types of VPN Protocols. [Електронний ресурс]. – Режим доступу: https://www.security.org/vpn/protocols/

22. What Is WireGuard? [Електронний ресурс]. – Режим доступу: https://www.paloaltonetworks.com/cyberpedia/what-is-wireguard

23. RFC 3193. [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc3193

24. Simion, D., Ursuleanu, M., Graur, A., Potorac, A., Lavric, A. (2013). Efficiency Consideration for Data Packets Encryption within Wireless VPN Tunneling for Video Streaming. China: International Journal of computers communications & control.

25. J. Luo and Q. Ji, "Password Acquisition and Traffic Decryption Based on L2TP/IPSec," 2020 IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China, 2020, pp. 1567-1571

26. Angelo, R. (2019). Secure Protocols And Virtual Private Networks: An Evaluation. Issues in Information Systems, 20(3).

27. RADIUS Active Directory. [Електронний ресурс]. – Режим доступу: https://www.inkbridgenetworks.com/blog/blog-10/radius-active-directory-166

28. Alarbad, Abdulhadi Hasan, Anas Mohammed Alsharif, and Salem Omar SatI. "Campus Network Design for Information Technology Faculty." International Journal of Advanced Networking and Applications 15, no. 06 (2024): 6211–17.

29. What is VPN. [Електронний ресурс]. – Режим доступу: https://www.fortinet.com/resources/cyberglossary/what-is-a-vpn

30. RB4011iGS+RM. [Електронний ресурс]. – Режим доступу: https://mikrotik.com/product/rb4011igs_rm

31. Cisco Business 350 Series. [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/switches/business-350-series-managed-switches/datasheet-c78-744156.htm

32. Visual Syslog Server for Windows. [Електронний ресурс]. – Режим доступу: https://maxbelkov.github.io/visualsyslog/

ДОДАТКИ

Конфігураційні файли пристроїв

R-HQ-1:

```
/interface ethernet
set [ find default-name=ether1 ] auto-
negotiation=no comment=WAN \
    disable-running-check=no
set [ find default-name=ether2 ] comment=LAN
disable-running-check=no
/interface list
add name=WAN
add name=LAN
/ip dns forwarders
add disabled=yes dns-servers=172.22.1.99
name=klymchuk.net verify-doh-cert=no
/ip ipsec proposal
set [ find default=yes ] auth-
algorithms=sha512,sha256,sha1 enc-algorithms=\
    aes-256-cbc,aes-192-cbc,aes-128-cbc,3des
/ip pool
add name=L2TP-pool ranges=10.222.22.10-
10.222.22.254
add name=dhcp_pool4 ranges=172.22.1.100-
172.22.1.119
/ppp profile
add change-tcp-mss=yes dns-server=172.22.1.99
local-address=10.222.22.1 name=\
    L2TP-profile remote-address=L2TP-pool
/system logging action
set 3 remote=Serv-HQ-1.klymchuk.net remote-
log-format=syslog src-address=\
    172.22.1.1 syslog-facility=syslog
/ipv6 settings
set max-neighbor-entries=16384 min-neighbor-
entries=4096 \
    soft-max-neighbor-entries=8192
/interface l2tp-server server
set accept-proto-version=l2tpv2
authentication=chap,mschap1,mschap2 \
    default-profile=L2TP-profile enabled=yes
use-ipsec=yes
/interface list member
add interface=ether1 list=WAN
add interface=ether2 list=LAN
/ip address
add address=25.222.1.2/30 interface=ether1
network=25.222.1.0
add address=172.22.1.1/24 interface=ether2
network=172.22.1.0
/ip dhcp-client
add interface=ether1
/ip dhcp-server
add address-pool=dhcp_pool4 interface=ether2
lease-time=7h name=dhcp1
/ip dhcp-server network
add address=172.22.1.0/24 dns-
server=172.22.1.1 gateway=172.22.1.1
/ip dns
set allow-remote-requests=yes
servers=8.8.8.8,8.8.4.4
/ip dns static
add address=172.22.1.99 match-subdomain=yes
name=klymchuk.net type=A
/ip firewall filter
add action=accept chain=input dst-
port=500,1701,4500 in-interface=ether1 \
    protocol=udp
add action=accept chain=input in-
interface=ether1 protocol=ipsec-esp
add action=accept chain=input comment=\
    "defconf: accept
established,related,untracked" connection-
state=\
    established,related,untracked
add action=drop chain=input comment="defconf:
drop invalid" connection-state=\
    invalid
add action=accept chain=input
comment="defconf: accept ICMP" protocol=icmp
add action=accept chain=input comment=\
    "defconf: accept to local loopback (for
CAPsMAN)" dst-address=127.0.0.1
add action=drop chain=input comment="defconf:
drop all not coming from LAN" \
    in-interface-list=!LAN
add action=accept chain=forward
comment="defconf: accept in ipsec policy" \
    ipsec-policy=in,ipsec
add action=accept chain=forward
comment="defconf: accept out ipsec policy" \
    ipsec-policy=out,ipsec
add action=fasttrack-connection chain=forward
comment="defconf: fasttrack" \
    connection-state=established,related
add action=accept chain=forward comment=\
    "defconf: accept established,related,
untracked" connection-state=\
    established,related,untracked
add action=drop chain=forward
comment="defconf: drop invalid" \
    connection-state=invalid
add action=drop chain=forward comment=\
    "defconf: drop all from WAN not DSTNATed"
connection-nat-state=!dstnat \
    connection-state=new in-interface-list=WAN
/ip firewall nat
add action=masquerade chain=srcnat out-
interface=ether1 src-address=\
    172.22.1.0/24 to-addresses=25.222.1.2
/ip ipsec profile
set [ find default=yes ] enc-algorithm=aes-
256,aes-192,aes-128,3des
/ip route
add disabled=no dst-address=0.0.0.0/0
gateway=25.222.1.1 routing-table=main
/ipv6 nd
set [ find default=yes ] advertise-dns=yes
/ppp aaa
set use-radius=yes
/ppp secret
add name=R-BR-A-1-VPN-user profile=L2TP-
profile remote-address=10.222.22.2 \
    routes=172.22.2.0/24 service=l2tp
/radius
add address=172.22.1.99 domain=klymchuk.net
service=ppp
```

```
add address=172.22.1.99 service=login
/system clock
set time-zone-name=Europe/Kyiv
/system identity
set name=R-HQ-1
/system logging
add action=remote topics=critical
add action=remote topics=error
add action=remote topics=info
add action=remote topics=warning
add action=remote topics=account
add disabled=yes topics=radius
add action=remote topics=system
/system ntp client
set enabled=yes
/system ntp client servers
add address=time.in.ua
/tool romon
set enabled=yes
/user aaa
set default-group=full use-radius=yes
```

R-BR-A-1:

```
/interface ethernet
set [ find default-name=ether1 ] comment=WAN
disable-running-check=no
set [ find default-name=ether2 ] comment=LAN
disable-running-check=no
/interface l2tp-client
add allow=chap,mschap2 connect-to=25.222.1.2
disabled=no name=l2tp-out1 \
    use-ipsec=yes user=R-BR-A-1-VPN-user
/interface list
add name=WAN
add name=LAN
/ip ipsec proposal
set [ find default=yes ] auth-
algorithms=sha512,sha256,sha1 enc-algorithms=\
    aes-256-cbc,aes-192-cbc,aes-128-cbc,3des
/ip pool
add name=dhcp_pool0 ranges=172.22.2.100-
172.22.2.109
/ip dhcp-server
add address-pool=dhcp_pool0 interface=ether2
lease-time=7h name=dhcp1
/system logging action
set 3 remote=Serv-HQ-1.klymchuk.net remote-
log-format=syslog syslog-facility=\
    syslog
/ipv6 settings
set max-neighbor-entries=16384 min-neighbor-
entries=4096 \
    soft-max-neighbor-entries=8192
/interface list member
add interface=ether1 list=WAN
add interface=ether2 list=LAN
/ip address
add address=25.222.2.2/30 interface=ether1
network=25.222.2.0
add address=172.22.2.1/24 interface=ether2
network=172.22.2.0
/ip dhcp-client
add interface=ether1
/ip dhcp-server lease
add address=172.22.2.109 client-
id=1:0:50:79:66:68:3 mac-address=\
    00:50:79:66:68:03 server=dhcp1
add address=172.22.2.108 client-
id=1:0:50:79:66:68:4 mac-address=\
    00:50:79:66:68:04 server=dhcp1
add address=172.22.2.107 client-
id=1:0:50:79:66:68:5 mac-address=\
    00:50:79:66:68:05 server=dhcp1
/ip dhcp-server network
add address=172.22.2.0/24 dns-
server=172.22.2.1 gateway=172.22.2.1
/ip dns
set allow-remote-requests=yes
servers=8.8.8.8,8.8.4.4
/ip dns static
add address=172.22.1.99 match-subdomain=yes
name=klymchuk.net type=A
add address=172.22.2.109 name=WS-BR-A-
1.klymchuk.net type=A
add address=172.22.2.108 name=WS-BR-A-
2.klymchuk.net type=A
add address=172.22.2.107 name=WS-BR-A-
3.klymchuk.net type=A
/ip firewall filter
add action=accept chain=input dst-
port=500,1701,4500 in-interface=ether1 \
    protocol=udp
add action=accept chain=input in-
interface=ether1 protocol=ipsec-esp
add action=accept chain=input in-
interface=l2tp-out1 src-address=\
    172.22.1.0/24
add action=accept chain=input comment=\
    "defconf: accept
established,related,untracked" connection-
state=\
    established,related,untracked
add action=drop chain=input comment="defconf:
drop invalid" connection-state=\
    invalid
add action=accept chain=input
comment="defconf: accept ICMP" protocol=icmp
add action=accept chain=input comment=\
    "defconf: accept to local loopback (for
CAPsMAN)" dst-address=127.0.0.1
add action=drop chain=input comment="defconf:
drop all not coming from LAN" \
    in-interface-list=!LAN
add action=accept chain=forward
comment="defconf: accept in ipsec policy" \
    ipsec-policy=in,ipsec
add action=accept chain=forward
comment="defconf: accept out ipsec policy" \
    ipsec-policy=out,ipsec
add action=fasttrack-connection chain=forward
comment="defconf: fasttrack" \
    connection-state=established,related
add action=accept chain=forward comment=\
    "defconf: accept established,related,
untracked" connection-state=\
    established,related,untracked
add action=drop chain=forward
comment="defconf: drop invalid" \
    connection-state=invalid
add action=drop chain=forward comment=\
    "defconf: drop all from WAN not DSTNATed"
connection-nat-state=!dstnat \
    connection-state=new in-interface-list=WAN
/ip firewall nat
```

```
add action=masquerade chain=srcnat out-
interface=ether1 src-address=\
    172.22.2.0/24
/ip ipsec profile
set [ find default=yes ] enc-algorithm=aes-
256,aes-192,aes-128,3des
/ip route
add dst-address=0.0.0.0/0 gateway=25.222.2.1
add disabled=no dst-address=172.22.1.0/24
gateway=l2tp-out1 routing-table=\
    main
add disabled=no distance=1 dst-
address=10.222.22.0/24 gateway=l2tp-out1 \
    routing-table=main scope=30 target-
scope=10
/ipv6 nd
set [ find default=yes ] advertise-dns=yes
/radius
add address=172.22.1.99 service=login src-
address=172.22.2.1
/radius incoming
set accept=yes
/system clock
set time-zone-name=Europe/Kyiv
/system identity
set name=R-BR-A-1
/system logging
add action=remote topics=error
add action=remote topics=critical
add action=remote topics=info
add action=remote topics=warning
add action=remote topics=system
/system ntp client
set enabled=yes
/system ntp client servers
add address=time.in.ua
/user aaa
set default-group=full use-radius=yes
```

SW-HQ-1:

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-HQ-1
!
boot-start-marker
boot-end-marker
!
logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
clock timezone EEST 2 0
clock summer-time EET recurring last Sun Mar
3:00 last Sun Oct 4:00
!
no ip routing
no ip icmp rate-limit unreachable
!
ip name-server 172.22.1.1
no ip cef
no ipv6 cef
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Ethernet0/0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
 ip address 172.22.1.2 255.255.255.0
 no ip route-cache
!
ip default-gateway 172.22.1.1
ip forward-protocol nd
!
ip tcp synwait-time 5
ip http server
!
ip ssh server algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
ntp update-calendar
ntp server time.in.ua
end
```