

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

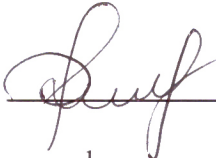
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології захисту корпоративної
мережі організації на базі рішень Mikrotik і OpenVPN»

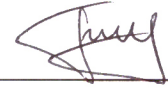
Виконав студент 2-го курсу групи КБм-23-1
спеціальності 125 «Кібербезпека та захист інформації»

 Д.І. Плитус

Керівник старший викладач кафедри комп'ютерної
інженерії та кібербезпеки

 Є.М. Трокоз

Рецензент старший викладач кафедри комп'ютерної
інженерії та кібербезпеки

 О.А. Покотило

Житомир – 2024

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

17 вересня 2024 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу магістра

Студент: Плитус Денис Іванович

Тема роботи: **«Методи та технології захисту корпоративної мережі
організації на базі рішень Mikrotik і OpenVPN»**

затверджена Наказом університету від 17 вересня 2024 р. № 479/с

Термін здачі студентом закінченої роботи 25 грудня 2024 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Топологія локальної корпоративної мережі.
2. Рішення Mikrotik та OpenVPN.

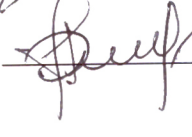
Обладнання та програмне забезпечення:

1. GNS3 v.2.2.52
2. Oracle VM VirtualBox 7.0.10
3. ОС Windows 10
4. ОС Windows Server 2019
5. ОС RouterOS v.7.16.2

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Д.С. Морозов	17.09.2024 	08.10.2024 
2	Д.С. Морозов	09.10.2024 	11.11.2024 
3	Д.С. Морозов	12.11.2024 	15.12.2024 

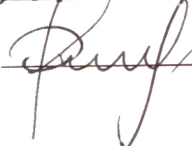
Студент  Д.І. Плитус

Керівник  Є.М. Трокоз

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	17.09.2024	Виконано
2	Розробка плану роботи	24.09.2024	Виконано
3	Огляд теоретичних відомостей стосовно Mikrotik та RouterOS	01.10.2024	Виконано
4	Аналіз використання VPN	08.10.2024	Виконано
5	Розробка топології мережі та схеми адресації	15.10.2024	Виконано
6	Розробка підсистеми захисту мережі	22.10.2024	Виконано
7	Вибір обладнання	11.11.2024	Виконано
8	Створення та налаштування проєкту мережі та обраних рішень	20.11.2024	Виконано
9	Тестування роботи мережі	30.11.2024	Виконано
10	Написання пояснювальної записки	15.12.2024	Виконано
11	Підготовка презентації	20.12.2024	Виконано
12	Захист	25.12.2024	Виконано

Студент  Д.І. Плитус

Керівник  Є.М. Трокоз

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему «Методи та технології захисту корпоративної мережі організації на базі рішень Mikrotik і OpenVPN» складається зі вступу, трьох розділів, висновків, списку використаної літератури, додатків і має 96 сторінок основного тексту, 77 рисунки, 4 таблиці, 8 сторінок додатків. Список використаних джерел містить 20 найменувань і займає 2 сторінки. Загальний обсяг роботи – 104 сторінки.

Метою роботи є дослідження методів та технологій захисту корпоративної мережі організації на базі рішень Mikrotik і OpenVPN, проєктування та налаштування корпоративної мережі та використання визначених рішень.

В ході роботи було визначено призначення корпоративних мереж та основні типи атак, що спрямовані на них. Виконано опис різних методів і технологій захисту корпоративних мереж. Проаналізовано теоретичні відомості стосовно Mikrotik та ОС RouterOS, досліджено переваги використання VPN та проаналізовано різновиди протоколів VPN в ході якого визначено, що OpenVPN найкраще задовольняє всі вимоги до мережі.

Розроблено топологію корпоративної мережі організації, наведено схему адресації, визначено технології та функції захисту мережі, які будуть використані при налагодженні та виконано підбір відповідного обладнання.

Проведено практичне налаштування мережі з використанням емулятора GNS3 та гіпервізора Oracle VirtualBox з використанням визначених технологій захисту мережі. Проведене тестування проєкту показали його повну працездатність та відповідність всім поставленим задачам даної роботи.

КЛЮЧОВІ СЛОВА: МЕРЕЖА, МІКРОТІК. OPENVPN, ЗАХИСТ, ШИФРУВАННЯ.

ANNOTATION

The graduate qualification work on the topic "Methods and Technologies for Protecting the Corporate Network of an Organization Based on Mikrotik and OpenVPN Solutions" consists of an introduction, three chapters, conclusions, a list of references, appendices, and contains 96 pages of main text, 77 figures, 4 tables, and 8 pages of appendices. The list of used sources includes 20 entries and occupies 2 pages. The total volume of the work is 104 pages.

The aim of the work is to research the methods and technologies for protecting the corporate network of an organization based on Mikrotik and OpenVPN solutions, design and configure the corporate network and use the selected solutions.

During the work, the purpose of corporate networks and the main types of attacks targeting them were identified. Various methods and technologies for protecting corporate networks were described. The theoretical aspects regarding Mikrotik and RouterOS were analyzed, the advantages of using VPN were researched, and the different types of VPN protocols were analyzed and it was found that OpenVPN best meets all network requirements.

A corporate network topology for the organization was developed, an addressing scheme was provided, and the network protection technologies and functions to be used for setup were determined. The appropriate equipment was selected.

Practical configuration of the network was carried out using the GNS3 emulator and Oracle VirtualBox hypervisor with the selected network protection technologies. Testing of the project demonstrated its full functionality and compliance with all the objectives of the work.

KEYWORDS: NETWORK, MIKROTIK, OPENVPN, PROTECTION, ENCRYPTION.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ВИКОРИСТАННЯ МІКРОТІК ТА OPENVPN ДЛЯ ЗАХИСТУ МЕРЕЖІ	10
1.1 Теоретичні аспекти захисту корпоративних мереж	10
1.2 Особливості та функціональні можливості Mikrotik RouterOS.....	15
1.3 Загальні аспекти роботи VPN та їх класифікація	18
1.4 Сценарії використання VPN.....	23
1.5 Різновид технологій VPN	27
1.6 Відомості щодо OpenVPN	35
РОЗДІЛ 2 РОЗРОБКА ПРОЄКТУ МЕРЕЖІ ТА ВИБІР ОБЛАДНАННЯ.....	41
2.1 Розробка загальної структури мережі	41
2.2 Розробка схеми адресації.....	46
2.3 Розробка підсистеми захисту корпоративної мережі	49
2.4 Вибір обладнання	51
РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ПЕРЕВІРКА РОБОТИ МЕРЕЖІ ТА ВИКОРИСТАНИХ РІШЕНЬ.....	56
3.1 Базове налагодження проєкту мережі	56
3.2 Налаштування OpenVPN на пристроях.....	67
3.3 Налagodження додаткових функцій захисту та їх перевірка	83
ВИСНОВКИ.....	93
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	95
ДОДАТКИ.....	1

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VPN – Virtual Private Network
ОС – Операційна Система
IP – Internet Protocol
APT – Advanced Persistent Threats
NGFW – Next-generation firewall
EDR – Endpoint Detection and Response
OSPF – Open Shortest Path First
BGP – Border Gateway Protocol
RIP – Routing Information Protocol
NAT – Network Address Translation
IPsec – IP Security
QoS – Quality of Service
PPTP – Point-to-Point Tunneling Protocol
L2TP – Layer 2 Tunneling Protocol
IKEv2 – Internet Key Exchange version 2
SSTP – Secure Socket Tunneling Protocol
TCP – Transmission Control Protocol
SSL/TLS – Sockets Layer/Transport Layer Security
UDP – User Datagram Protocol
AES – Advanced Encryption Standard

ВСТУП

Актуальність. Сучасні корпоративні мережі є невід'ємною частиною інфраструктури будь-якої організації, які забезпечують обмін даними, взаємодію між її компонентами, доступ до хмарних сервісів і підтримку віддаленої роботи. Проте із розвитком інформаційних технологій виникає все більше викликів у забезпеченні відповідної безпеки. Зростання кількості віддалених працівників, процес глобалізації, активне впровадження IoT-пристроїв, збільшення кількості та їх складність кіберзагроз створюють нові ризики для конфіденційності, цілісності та доступності даних.

За даними звітів про кібербезпеку, кількість атак на корпоративні мережі продовжують збільшуватись, а фінансові втрати від таких інцидентів досягають мільйонів доларів. Серед основних ризиків – несанкціонований доступ до мережі, перехоплення трафіку та витоки конфіденційної інформації. Водночас багато організацій стикаються з обмеженими фінансовими можливостями, що ускладнює впровадження дорогих рішень для забезпечення захисту [1].

Технології Mikrotik та OpenVPN пропонують ефективні, економічні та гнучкі засоби для побудови захищених корпоративних мереж. Mikrotik забезпечує широкий функціонал для маршрутизації, управління доступом і фільтрації трафіку, тоді як OpenVPN дозволяє створювати віртуальні приватні мережі (VPN) для шифрування даних і захисту з'єднань з віддаленими вузлами. Ці рішення особливо актуальні для організацій, які прагнуть підвищити безпеку своєї мережі без значних витрат.

Метою дослідження є створення та забезпечення захисту корпоративної мережі організації шляхом впровадження відповідних рішень на базі Mikrotik та використання OpenVPN для створення захищених каналів передачі даних.

Визначена мета обумовлює наступні завдання:

- Аналіз і дослідження принципу роботи VPN та їх класифікація.

- Вивчення функціональних можливостей обладнання Mikrotik та програмного забезпечення OpenVPN у контексті забезпечення мережевої безпеки.

- Розробка топології мережі та вибір необхідного обладнання для її реалізації.

- Налаштування маршрутизаторів Mikrotik.

- Організація віддаленого доступу з використання рішення OpenVPN та впровадження додаткових функцій захисту.

- Проведення тестування налаштованих рішень з метою оцінки їхньої працездатності, продуктивності та надійності.

Об'єктом дослідження є процес проєктування та налаштування корпоративної мережі та її захист з використанням відповідних рішень.

Предметом дослідження є методи та технології захисту корпоративної мережі організації на базі рішень Mikrotik і OpenVPN.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ВИКОРИСТАННЯ МІКРОТІК ТА OPENVPN ДЛЯ ЗАХИСТУ МЕРЕЖІ

1.1 Теоретичні аспекти захисту корпоративних мереж

Корпоративні мережі – це складні інфраструктури, що забезпечують взаємодію та обмін даними між різними пристроями та системами всередині організації. Вони включають в себе локальні мережі (LAN), а також підключення до глобальних мереж (WAN), що дозволяють з'єднувати віддалені філії чи офіси компанії [2]. Корпоративні мережі можуть включати сервери, робочі станції, мережеві пристрої, такі як маршрутизатори, комутатори, точки доступу, а також різноманітні програмні рішення для управління та моніторингу трафіку. Завдяки чому працівники організації можуть ефективно взаємодіяти з корпоративними додатками та використовувати ресурси, такі як бази даних або сервери [3].

Корпоративні мережі часто інтегруються з хмарними платформами та сторонніми сервісами, що дає можливість розширювати їх функціональність і зменшувати витрати на обслуговування. Однак це також створює нові виклики для безпеки, оскільки дані можуть зберігатися та оброблятися поза межами компанії, що вимагає додаткових заходів для захисту цих даних. Враховуючи постійно змінювані технології та зростаючі загрози, компанії повинні постійно вдосконалювати свої стратегії кібербезпеки для мінімізації ризиків, пов'язаних з використанням корпоративних мереж.

Типові способи атак

У сучасному світі корпоративні мережі стикаються зі значною кількістю кіберзагроз, які можуть викликати серйозні проблеми у їх роботі. Щоб захистити інфраструктуру від можливих атак, адміністратор мережі повинен постійно проводити роботи з виявлення наявних вразливостей, на основі чого визначити адекватні заходи для підвищення інформаційної безпеки та мінімізації наслідків можливих атак (ризик-менеджмент).

Зловмисники, як правило, мають обмежену інформацію про цільову мережу, тому їхньою основною задачею стає збір цієї інформації. Після збору

даних зломисники можуть організувати різні типи атак. Серед способів збору інформації можуть використовуватися інструменти на зразок WHOIS для отримання доменних імен та IP-адрес цільової мережі.

Атаки на корпоративні мережі можуть включати, як зовнішні дії з боку кіберзлочинців, так і внутрішні загрози, пов'язані з діяльністю працівників. Різні типи атак мають різні механізми здійснення, але всі вони мають спільну мету – отримати доступ до мережі та її ресурсів, а також завдати шкоди організації [4].

- Розвідувальні атаки спрямовані на несанкціоноване виявлення систем, служб або вразливостей цільової мережі. Зломисники можуть використовувати інструменти, такі як ping-запити, сканування портів або аналізатори пакетів. Ці атаки тривалий час залишаються непоміченими, оскільки не впливають безпосередньо на роботу мережі. Після виявлення активних IP-адрес і портів зломисники можуть отримати інформацію про операційні системи, типи програмного забезпечення та конфігурації, що використовуються в мережі.

- DoS-атаки та DDoS-атаки спрямовані на виведення з ладу мережевих ресурсів, що унеможлиблює доступ легітимних користувачів до сервісів. Ці атаки здійснюються через перевантаження серверів запитамі або інші механізми, що створюють надмірне навантаження на інфраструктуру.

- Атаки "людина посередині" (Man-in-the-middle, MitM) базуються на перехопленні та потенційному зміні комунікації між двома сторонами без їхнього відома. Зломисник може, наприклад, отримати доступ до конфіденційної інформації, коли співробітник використовує незахищену публічну мережу Wi-Fi для входу в корпоративну електронну пошту. Це дозволяє викрасти облікові дані або внести зміни в передану інформацію, наприклад, підмінити реквізити платежу. Для запобігання MitM-атакам широко застосовуються шифрування трафіку, використання HTTPS та VPN, а також забезпечення доступу до мереж лише через захищені з'єднання.

- Атаки типу фішинг базуються на використанні людського фактору, вводячи в оману за допомогою підроблених електронних листів, які виглядають

як легітимні. Зловмисники можуть використовувати цю інформацію для інсталяції шкідливого програмного забезпечення, викрадення облікових даних або здійснення несанкціонованих фінансових операцій. Наприклад, співробітник може випадково надати доступ до конфіденційних даних або фінансових систем, відповівши на підроблений лист від імені довіреної особи чи керівника. Компрометація облікових даних дозволяє зловмисникам отримати доступ до корпоративної мережі, підвищувати привілеї та переміщуватися в мережі для досягнення своїх цілей.

- Вразливості "нульового дня" (Zero-day exploits) дозволяють зловмисникам використовувати недоліки програмного забезпечення, про які розробники ще не знають. Через відсутність доступного виправлення, такі атаки є надзвичайно складними для виявлення та усунення. Зазвичай вони супроводжуються встановленням систем виявлення вторгнень (IDS), які аналізують підозрілі дії в мережі та допомагають запобігти цим атакам.

- Шкідливе програмне забезпечення, таке як віруси, черви та трояни, також становлять серйозну загрозу для корпоративних мереж. Віруси можуть поширюватися через заражені файли або електронну пошту, тоді як черви мають здатність самостійно розповсюджуватися мережею, впливаючи на всі підключені пристрої. Трояни, у свою чергу, маскуються під корисні програми, але завдають шкоди після встановлення.

- Інсайдерські загрози, як ненавмисні, так і навмисні, становлять серйозну небезпеку для безпеки мережі. Співробітник, який випадково натисне на фішингове посилання, може завантажити програму-шифрувальник, що призведе до простою мережі або витоку даних. У випадку навмисної загрози, невдоволений працівник може свідомо передавати конфіденційну інформацію конкурентам чи відкривати доступ до систем для третіх сторін.

- Атаки типу Advanced Persistent Threats (APT) використовуються для довготривалого та непомітного доступу до мережі. Зловмисники можуть залишатися непоміченими протягом тривалого часу, збираючи конфіденційну

інформацію або розробляючи більш масштабну атаку. Такі дії можуть включати систематичне викрадення великих обсягів даних упродовж років, завдаючи колосальних збитків організаціям.

Захист

Захист корпоративної мережі вимагає комплексного підходу, який включає використання різноманітних інструментів для виявлення атак і підвищення безпеки [5].

- Фаєрвол. Фаєрволи є одним з основних засобів захисту, контролюючи вхідний і вихідний трафік на основі встановлених правил безпеки. Проксі-фаєрволи забезпечують додатковий рівень безпеки, блокуючи прямі з'єднання з зовнішніх мереж, тоді як фаєрволи з урахуванням контексту (stateful) відстежують активні з'єднання та здійснюють аналіз трафіку в реальному часі. Наступне покоління фаєрволів (NGFW) поєднує функції виявлення вторгнень і аналізу додатків, що дозволяє протидіяти сучасним загрозам.

- IDPS. Системи виявлення та запобігання вторгненням (IDPS) здійснюють постійний моніторинг мережевого трафіку та виявляють підозрілі активності, зокрема, на основі аналізу трафіку в реальному часі. Сучасні системи IDPS можуть не тільки виявляти загрози, але й активно блокувати їх, що дозволяє зупиняти атаки на ранніх етапах. Завдяки використанню машинного навчання такі системи можуть ефективно реагувати на нові типи загроз, які ще не були внесені в бази даних підписів.

- Моніторинг та аналіз мережевого трафіку. Моніторинг мережевого трафіку є ключовим елементом виявлення та запобігання загрозам. Це дозволяє системним адміністраторам вчасно виявляти аномалії в поведінці мережі, такі як несанкціоновані спроби доступу або аномальні піки трафіку, що можуть свідчити про наявність атаки. Використання спеціалізованих інструментів для аналізу трафіку допомагає виявляти уразливості та потенційні загрози на ранніх етапах.

- EDR (Endpoint Detection and Response). EDR – це рішення для моніторингу та реагування на загрози на кінцевих пристроях у реальному часі. Воно забезпечує безпеку шляхом постійного аналізу активності на комп'ютерах, мобільних пристроях та інших терміналах. EDR-системи здатні виявляти аномальні або підозрілі дії, такі як спроби проникнення, запуск шкідливих програм чи несанкціоновані зміни в налаштуваннях системи. У разі виявлення загрози, EDR може автоматично реагувати, блокуючи шкідливу активність, або надавати адміністратору інструменти для оперативного реагування. Це дає змогу швидко локалізувати і знешкоджувати загрози на ранніх етапах, мінімізуючи потенційні наслідки для організації. EDR також забезпечує детальну звітність та аналіз подій, що дозволяє створювати ефективні стратегії захисту та покращувати безпеку кінцевих пристроїв.

- VPN. Віртуальні приватні мережі (VPN) дозволяють захищати з'єднання віддалених працівників через публічні мережі, забезпечуючи шифрування трафіку, що робить його недоступним для злоумисників, навіть якщо вони мають доступ до мережі. Це особливо важливо при роботі в громадських місцях, де використовується незахищене Wi-Fi з'єднання.

- Аудит безпеки та управління патчами. Регулярні аудити безпеки та управління патчами є важливими аспектами захисту мережі. Перевірка мережі на вразливості та своєчасне застосування оновлень допомагає запобігти експлуатації відомих уразливостей. Проводити регулярні перевірки безпеки необхідно для виявлення нових загроз і вдосконалення захисних механізмів.

- Централізоване збирання журналів подій. Централізоване збирання і зберігання журналів подій дозволяє адміністратору оперативно відслідковувати стан мережі, виявляти потенційні проблеми та аномалії, а також здійснювати аналіз критичних інцидентів. Це дає змогу швидко реагувати на загрози, забезпечуючи високу стабільність і безпеку мережі.

- Централізоване управління доступом. Централізоване управління доступом до ресурсів мережі дозволяє детально відслідковувати активність

користувачів, включаючи час підключень та інші параметри. Це допомагає виявляти підозрілу поведінку та знижувати ризик несанкціонованого доступу до критичних даних.

- **Захищений віддалений доступ.** Для забезпечення захищеного віддаленого доступу до мережевих пристроїв слід використовувати методи, які забезпечують зашифроване з'єднання, захищаючи дані від перехоплення та атак. Ці технології дозволяють здійснювати віддалене керування мережею без необхідності передавати чутливу інформацію в незашифрованому вигляді, що підвищує рівень безпеки.

- **Шифрування даних.** Шифрування є важливою частиною стратегії захисту корпоративної мережі. Всі важливі комунікації та дані, що передаються через мережу, повинні бути зашифровані, щоб уникнути їх перехоплення та витоку. Використання сильних алгоритмів шифрування гарантує, що дані залишаються конфіденційними та доступними лише для авторизованих користувачів.

В загалом комплексний захист корпоративних мереж вимагає використання сучасних технологій і методів, які дозволяють мінімізувати можливі втрати від атак. Розуміння теоретичних аспектів роботи мереж і характеру загроз є ключовим для забезпечення надійної інформаційної безпеки.

1.2 Особливості та функціональні можливості Mikrotik RouterOS

MikroTik – це латвійська компанія, що базується в Ризі та спеціалізується на розробці маршрутизаторів і систем для інтернет-провайдерів, поставляючи обладнання по всьому світу. Основними продуктами компанії є операційна система RouterOS і серія апаратних пристроїв RouterBOARD. Вся продукція компанії супроводжується обширною документацією, що робить їх надійним кандидатом для використання в мережевій інфраструктурі будь-якого розміру [6].

MikroTik RouterBOARD є апаратною платформою від MikroTik, яка являє собою маршрутизатори на базі операційної системи RouterOS. Широкий вибір

модифікацій мережевої платформи RouterBOARD дозволяє використовувати їх для вирішення багатьох задач, пов'язаних з мережевими технологіями. На обладнанні MikroTik можна легко реалізувати, як просту бездротову точку доступу, так і маршрутизатор [7].

Mikrotik RouterOS – це спеціалізована операційна система розроблена компанією MikroTik для обладнання MikroTik RouterBOARD, однак може бути встановлена на будь-який інший комп'ютер, що перетворить його на повноцінний маршрутизатор. RouterOS базується на ядрі Linux і забезпечує широкий спектр функціональних можливостей для налаштування та управління мережами, що включає маршрутизацію, фавол, керування пропускну здатністю, бездротову точку доступу, VPN-сервер і багато іншого. Дана платформа відома своєю стабільністю, високою якістю контролю та гнучкістю для роботи з різними типами пакетів даних і обробкою.

Можливості RouterOS включають все, що стосується адресації в Інтернеті та управлінням трафіком. Більшість маршрутизаторів та мережних пристроїв виконують лише певні функції. Один пристрій може бути PPPoE-сервером або концентратором, а інший контролювати пропускну здатність і регулювати потік даних у мережі. RouterOS же включає всі вищезгадані функції. У деяких випадках пристрої та програмне забезпечення RouterOS можуть коштувати менш ніж чверть від вартості аналогічних пристроїв, пропонуючи при цьому більше функціональних можливостей, ніж ці дорожчі пристрої.

У поєднанні з надійним і потужним обладнанням RouterOS може швидко перевершити багато маршрутизаторів, доступних на ринку. Багато компаній та інших кінцевих користувачів виявили, що економія коштів, яку пропонує RouterOS є ключовим фактором для вибору обладнання MikroTik.

Можливості RouterOS включають:

- Маршрутизація. RouterOS підтримує різноманітні методи маршрутизації для оптимізації мережевого трафіку. Це включає як статичну, так і динамічну маршрутизацію. Динамічна маршрутизація забезпечує автоматичне оновлення маршрутів через протоколи, такі як OSPF (Open Shortest Path First), BGP (Border

Gateway Protocol), і RIP (Routing Information Protocol). Це дозволяє пристроям автоматично адаптуватися до змін у мережі.

- Брандмауер і безпека. RouterOS надає потужні інструменти для забезпечення безпеки мережі, включаючи фільтрацію трафіку за допомогою правил брандмауера. Це дозволяє контролювати вхідний і вихідний трафік, блокуючи небажані або небезпечні з'єднання. Крім того, підтримуються різні методи NAT (Network Address Translation) та IPsec для створення захищених з'єднань між мережами або для захисту даних у мережі.

- QoS (Quality of Service). QoS у RouterOS дозволяє управляти якістю обслуговування мережі шляхом пріоритезації трафіку. Це особливо важливо для забезпечення стабільної роботи критичних додатків, таких як голосові чи відео конференції. Ви можете налаштувати обмеження пропускної здатності для різних видів трафіку та створити правила для управління чергами трафіку.

- Бездротові мережі. Дана ОС підтримує різні бездротові технології, включаючи стандарти 802.11a/b/g/n/ac. Це дозволяє налаштовувати бездротові точки доступу, клієнти, репітри та інші типи бездротових з'єднань. Система також підтримує різні режими безпеки, такі як WPA2/WPA3, для захисту бездротових мереж від несанкціонованого доступу.

- Віртуальні приватні мережі (VPN). RouterOS забезпечує підтримку кількох протоколів VPN, включаючи PPTP, L2TP, OpenVPN, SSTP, Wireguard.

- Скрипти та автоматизація. Існують можливості створення скриптів, які дозволяють автоматизувати рутинні завдання. Це включає резервне копіювання конфігурацій, виконання регулярних оновлень та інших адміністративних задач. Також можна налаштувати завдання, що виконуються за розкладом, для автоматичного запуску скриптів у визначений час.

- Моніторинг та управління. RouterOS надає інструменти для моніторингу мережевого трафіку та продуктивності системи, що включає статистику трафіку, виявлення збоїв та проблем у мережі. Підтримуються інтерфейси для

віддаленого моніторингу через веб-інтерфейс, SNMP (Simple Network Management Protocol) та графічний інтерфейс Winbox.

- Віртуалізація. Може бути розгорнутий, як віртуальна машина на різних гіпервізорах, таких як VMware, VirtualBox або Hyper-V, що може бути корисний для тестування певних функцій, навчанню або впровадження віртуальних мережеских рішень.

1.3 Загальні аспекти роботи VPN та їх класифікація

Загальні відомості

Віртуальна приватна мережа (VPN) є розширенням внутрішньої корпоративної мережі через публічні мережі, такі як Інтернет, створюючи захищене приватне з'єднання у вигляді "тунелю". VPN дозволяє безпечно передавати інформацію через Інтернет, об'єднуючи віддалених користувачів, філії та бізнес-партнерів в єдину корпоративну мережу [8].

Простіше кажучи, VPN дозволяє адміністратору створити «локальну» мережу між кількома комп'ютерами, які знаходяться в різних сегментах мережі. У деяких випадках ці комп'ютери можуть перебувати в одній локальній мережі (LAN), знаходитися на значній відстані один від одного через Інтернет, або навіть бути підключеними через різноманітні з'єднання, такі як бездротові підключення, супутникові канали, комутовані мережі тощо. Мережеский трафік, що проходить через VPN, часто називають трафіком всередині (VPN) тунелю, у порівнянні з усім іншим трафіком, який знаходиться поза тунелем. Розберемо, що вбачає кожне слово даної технології:

Віртуальна. Термін "віртуальна" означає, що фізична інфраструктура мережі повинна бути прозорою для будь-якого з'єднання VPN. Зазвичай це також означає, що фізична мережа не належить користувачеві VPN, а є публічною мережею, яку ділять багато інших користувачів. Для забезпечення прозорості на вищих рівнях мережі застосовуються техніки тунелювання протоколів. Оскільки фізична мережа не контролюється користувачем, слід укласти угоди про рівень

обслуговування з провайдерами, щоб забезпечити відповідну продуктивність та доступність, необхідні для VPN.

Приватна. "Приватна" у контексті VPN стосується конфіденційності трафіку, який передається через мережу. Часто трафік VPN проходить через публічні мережі, тому необхідно вживати заходів для забезпечення необхідної безпеки для конкретного профілю трафіку. Ці заходи включають: шифрування даних, аутентифікацію джерела даних, захищене створення та своєчасне оновлення криптографічних ключів для шифрування та аутентифікації, захист від повторної передачі пакетів і підміни адрес.

Мережа. Хоча VPN фізично не існує, дане визначення необхідно сприймати і трактувати як розширення інфраструктури корпоративної мережі. Це означає, що VPN повинна бути доступна решті мережі, або їй певній частині, включаючи пристрої та додатки.

Переваги використання

Користувачі зазвичай використовують VPN-сервіси для безперешкодного доступу до Інтернету приховуючи свою діяльність від сторонніх осіб і обходячи різного роду обмеження.

В умовах глобалізації економіки компанії шукають можливості географічного розподілу, що може бути пов'язане з податковими стимулами або з розширенням бізнесу. В цьому випадку співробітники потребують свободи у виконанні своїх завдань без географічних обмежень та забезпечення безпеки переданої інформації.

Концепція віртуальної приватної мережі (VPN) виникла як економічна альтернатива захищеним комунікаціям через публічні канали зв'язку, такі як Інтернет, і швидко стала популярною технологією безпеки, що забезпечує цілісність, конфіденційність і доступність інформації.

Переваги використання VPN:

- Зручність для віддаленої роботи: VPN забезпечує безпечний доступ до корпоративних сервісів і документації, що робить роботу з дому чи з іншого віддаленого місця безпечною і захищеною від перехоплення даних.

- Низька вартість установки та експлуатації: відсутність потреби в оренді або організації власних ліній зв'язку.
- Майже необмежена масштабованість: можливість розширення мережі без значних витрат.
- Простота налаштування і зміни конфігурації мережі: легкість в управлінні та адаптації.
- Доступність для користувачів і додатків: широке застосування і зручність для кінцевих користувачів.
- Об'єднання різних частин організації: VPN дозволяє з'єднати офіси, які знаходяться на великій відстані один від одного.
- Безпечне підключення до публічних мереж: Використання VPN у загальнодоступних мережах, таких як Wi-Fi у кафе або метро, захищає дані від можливого перехоплення або видозміни.
- Доступ до заблокованих сайтів: VPN дозволяє обходити блокування доступу до сайтів, які можуть бути заборонені у вашій країні чи регіоні.
- Анонімність в Інтернеті: Використання VPN дозволяє залишатися анонімним, приховуючи відстеження відвіданих сайтів і вашу геолокацію.

Недоліки:

- Зниження швидкості Інтернету: Шифрування даних може значно знижувати швидкість Інтернету, а також це може залежати від відстані до VPN-сервера.
- Відсутність підтримки IPv6: Деякі VPN-сервіси не підтримують протокол IPv6, що може обмежувати їх використання в сучасних мережах.

Зі стрімким зростанням Інтернету компанії все частіше задаються питанням, як можна найкраще використати Інтернет для бізнесу. Спочатку підприємства використовували Інтернет для просування свого іміджу, продуктів та послуг через надання доступу до корпоративних веб-сайтів. Однак сьогодні потенціал Інтернету безмежний, і фокус змістився на електронний бізнес, який використовує глобальні можливості Інтернету для забезпечення легкого доступу

до ключових бізнес-додатків і даних, що зберігаються в традиційних ІТ-системах. Компанії шукають найкращі рішення для безпечного та економічно ефективного розширення доступу до своїх додатків і даних по всьому світу. Хоча для цього можна використовувати веборієнтовані додатки, віртуальна приватна мережа пропонує більш комплексні та безпечні рішення.

VPN забезпечує безпечну передачу інформації через Інтернет, з'єднуючи віддалених користувачів, філії та бізнес-партнерів у розширену корпоративну мережу.

Незважаючи на те, що технологія впровадження цих віртуальних приватних мереж використовується вже давно, але правильне рішення VPN має визначатися відповідно до ваших потреб, враховуючи наступні аспекти:

- Бізнес-потреби;
- Безпека;
- Продуктивність;
- Взаємодія рішення з поточними системами.

Ключем до максимізації ефективності VPN є здатність компаній розвивати свої VPN відповідно до зміни їхніх бізнес-потреб і легко оновлювати їх до нових технологій. Постачальники, які підтримують широкий спектр апаратних і програмних продуктів VPN, забезпечують гнучкість, необхідну для задоволення цих вимог. Сьогодні рішення VPN переважно працюють у середовищі IPv4, але важливо, щоб вони мали можливість оновлення до IPv6, щоб залишатися сумісними з рішеннями VPN бізнес-партнера та/або постачальника. Так само важливо працювати з постачальником, який розуміє проблеми впровадження VPN. Успішна реалізація VPN включає більше, ніж просто технологію; досвід постачальника в мережевій інфраструктурі має велике значення.

Безпека

Використання VPN піднімає кілька проблем безпеки, які виходять за межі тих, що були в традиційних корпоративних мережах. Типовий шлях передачі даних від кінця до кінця може включати:

- Проміжні вузли, які не контролюються організацією (наприклад, доступ до ISP та маршрутизатори в межах Інтернету).
- Шлюз безпеки (брандмауер або маршрутизатор), який розташований на межі між внутрішнім і зовнішнім сегментами.
- Внутрішній сегмент (інтранет), який містить хости та маршрутизатори, які оброблятимуть як внутрішній, так і міжмережевий трафік.
- Зовнішній сегмент (Інтернет), який передає трафік не лише з мережі вашої компанії, а й з інших джерел.

Різновиди

Існують два основних типи підключень VPN: Remote Access VPN і VPN типу "Site-to-Site".

Remote Access VPN використовується для забезпечення безпечного доступу співробітникам компанії до корпоративної мережі та її ресурсів через публічну мережу Інтернет. Це особливо важливо, коли підключення до Інтернету здійснюється через загальнодоступні точки доступу Wi-Fi або інші небезпечні способи з'єднання. Для використання Remote Access VPN необхідно, щоб на пристрої було встановлено клієнтське програмне забезпечення VPN. Це програмне забезпечення взаємодіє зі шлюзом VPN, де відбувається автентифікація та авторизація користувача і створюється захищений «віртуальний» тунель між локальною мережею та шлюзом. Після успішного завершення цієї процедури користувач отримує доступ до внутрішніх мережевих ресурсів (файлові сервери, бази даних, принтери та інші) так, ніби він підключений безпосередньо до локальної мережі. Remote Access VPN дозволяє користувачам підключатися до приватної мережі та віддалено користуватися її ресурсами. З'єднання між користувачем і приватною мережею здійснюється через Інтернет і забезпечує безпеку та конфіденційність даних.

Site-to-Site VPN забезпечує з'єднання між мережами, розташованими в різних географічних точках, і зазвичай використовується в корпоративних середовищах. Site-to-Site VPN використовується для з'єднання локальних мереж,

розташованих в різних географічних точках. Це часто застосовується для з'єднання віддалених філій з центральним офісом або дата-центром компанії. В цьому випадку не потрібно встановлювати VPN-клієнти на кінцевих пристроях користувачів, оскільки з'єднання обробляється VPN-шлюзом. Дані передаються між пристроями в різних мережах прозоро. У цьому типі VPN шлюз одного віддаленого офісу взаємодіє зі шлюзом іншого офісу для створення безпечного тунелю. Схема Site-to-Site VPN зображена. У VPN типу "Site-to-Site" один маршрутизатор виконує роль VPN-клієнта, а інший — VPN-сервера. З'єднання між маршрутизаторами починається тільки після успішної автентифікації.

1.4 Сценарії використання VPN

Трафік у межах VPN може включати будь-які дані, які надсилаються через локальну або глобальну мережу: веб-трафік, електронну пошту, текстові повідомлення, графічні дані тощо. Приклади застосування VPN включають:

- Банкомати. Банкомати можуть використовувати VPN для безпечнішого підключення до банківських систем.
- Публічний Wi-Fi. З розповсюдженням безкоштовних або відкритих бездротових мереж, звичайні користувачі можуть використовувати VPN для захисту всієї своєї активності в Інтернеті.
- GeoIP/сервіси на основі геолокації. Деякі сервіси надають контент на основі географічного розташування, використовуючи бази даних GeoIP та інші записи. VPN дозволяє вам «перескочити» на інший сервер, розташований ближче до бажаного контенту.
- Обхід інтернет-цензури. У країнах із суворими обмеженнями інтернету VPN використовується для обходу цензури та доступу до глобального інтернету.
- Забезпечення конфіденційності та анонімності. Використання VPN допомагає приховати вашу IP-адресу та інші особисті дані під час перегляду вебсайтів, що забезпечує додатковий рівень конфіденційності.

- Корпоративні мережі. Корпорації та інші організації можуть використовувати VPN для підключення кількох офісів або навіть цілих центрів обробки даних.

З'єднання між віддаленими офісами

У сценарії з філією йдеться мова про надійне з'єднання двох довірених інтранетів в межах організації. Основний акцент на безпеку робиться на захист інтранету компанії від зовнішніх злоумисників та забезпечення безпеки даних компанії під час їх передачі через публічний Інтернет. Припустимо, що головний офіс компанії прагне мінімізувати витрати, пов'язані зі зв'язком зі своїми філіями. Використовуючи Інтернет, VPN-з'єднання для філій можуть бути легко встановлені для задоволення потреб компанії. Окрім безпеки, така архітектура дозволяє значно знизити витрати, уникаючи використання дорогих виділених каналів зв'язку. Це робить рішення фінансово вигідним і масштабованим, адже філії можуть підключатися до головного офісу незалежно від їхнього географічного розташування.

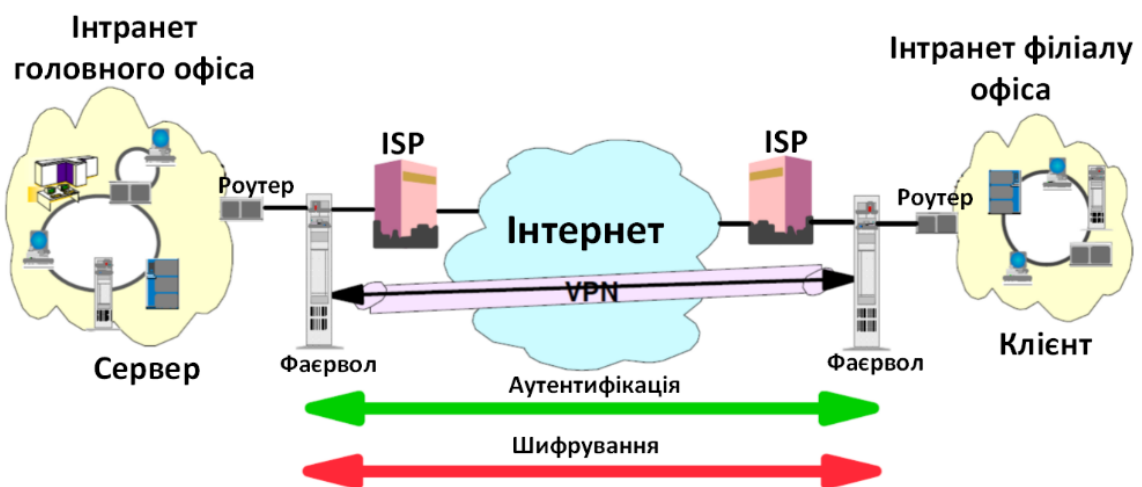


Рисунок 1.1 – З'єднання мереж головного офісу і філіалу через VPN

Одним із способів реалізації цього VPN-з'єднання між головним офісом компанії та однією з її філій полягає у отриманні доступу до Інтернету через інтернет-провайдера (ISP). На межі кожного з інтранетів встановлюються брандмауери або маршрутизатори з інтегрованими функціями брандмауера для

захисту корпоративного трафіку від інтернет-хакерів. Завдяки такому підходу будь-яка конфіденційна інформація буде прихована від ненадійних користувачів Інтернету, а брандмауер відхилятиме доступ потенційних зловмисників.

Завдяки встановленню VPN-з'єднань головний офіс і філія компанії зможуть безпечно та економічно ефективно мати зв'язок між собою, незалежно від того, знаходяться вони локально чи на віддаленій відстані. Завдяки технології VPN кожна філія також може розширити свій існуючий інтранет, щоб включити інтранети інших філій, створюючи розширену корпоративну мережу на рівні всього підприємства. І ця компанія може легко розширити це новостворене середовище, включивши в нього своїх бізнес-партнерів, постачальників і віддалених користувачів використовуючи VPN.

Мережа бізнес-партнерів/постачальників

Компанії-лідери галузі будуть тими, хто зможе недорого і безпечно спілкуватися зі своїми бізнес-партнерами, дочірніми компаніями та постачальниками. Раніше багато компаній обирали для цього придбання орендованих ліній для досягнення такої взаємодії, але це дорога послуга, а географічні можливості можуть бути обмеженими. Технологія VPN пропонує альтернативу для компаній, дозволяючи створювати приватну та економічно ефективну розширену корпоративну мережу з глобальним охопленням, використовуючи Інтернет або інші публічні мережі.

Припустимо, що компанія є основним постачальником деталей для виробника. Для ефективної роботи виробничої фірми важливо мати точні деталі у потрібній кількості в потрібний час, тому необхідно постійно бути в курсі стану запасів і графіків виробництва. Якщо ця взаємодія здійснюється вручну, вона може бути трудомісткою, дорогою та потенційно неточною. Існує потреба в простішому, швидшому та ефективнішому способі спілкування. Однак, через конфіденційність та часову чутливість цієї інформації, виробник може не бажати публікувати ці дані на корпоративному веб-сайті або розповсюджувати цю інформацію за допомогою зовнішніх звітів.

Щоб вирішити ці проблеми, постачальник деталей і виробник можуть впровадити VPN. Можна створити VPN між робочою станцією клієнта в інтранеті постачальника деталей і сервером, що знаходиться в інтранеті виробника. Клієнти можуть пройти аутентифікацію через брандмауер або маршрутизатор, що захищає інтранет виробника, безпосередньо на сервері виробника (підтверджуючи свою особу) або на обох, залежно від політики безпеки. Після цього можна встановити тунель, шифруючи всі пакети даних від клієнта через Інтернет до потрібного сервера.

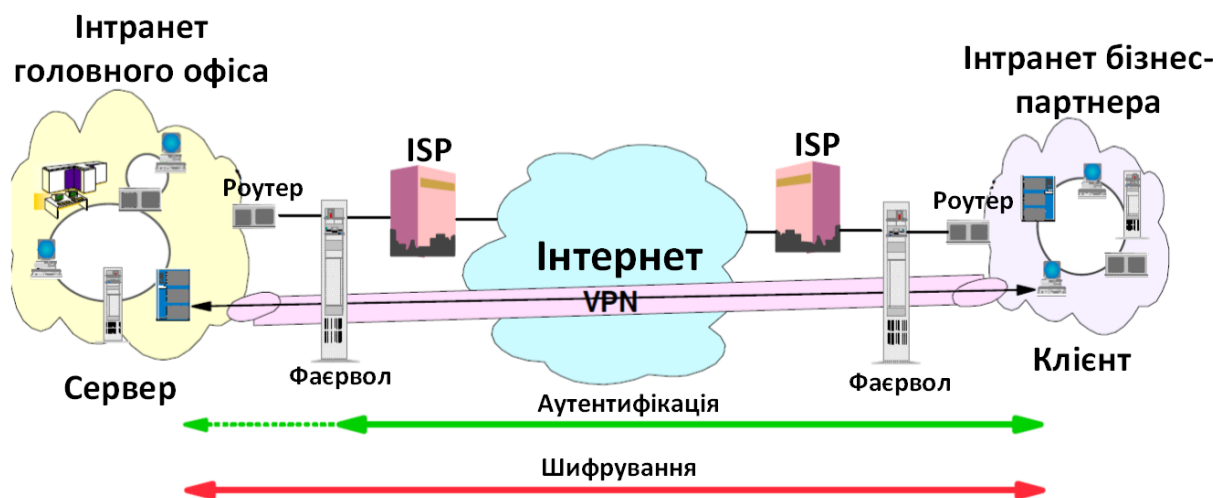


Рисунок 1.2 – З'єднання мереж головного офісу і бізнес-партнера через VPN

За бажанням тунелі в інтранет можуть завершуватися на спеціальному VPN-шлюзі в зоні DMZ. Це дозволить виконувати додаткові перевірки безпеки, такі як захист від вірусів і інспекцію контенту, перед тим як дані з зовнішньої системи будуть допущені до корпоративної мережі.

Один зі способів реалізації цього сценарію полягає в тому, щоб компанії отримали доступ до Інтернету, а потім впровадили брандмауер або маршрутизатор із підтримкою VPN. Це дозволяє забезпечити безпечне підключення віддалених співробітників, захистити внутрішні ресурси від несанкціонованого доступу та забезпечити сегментацію мережі.

Завдяки використанню технології VPN виробник зможе легко розширити свою існуючу корпоративну інтранет-мережу для включення одного або декількох бізнес-партнерів (фактично створюючи розширену корпоративну

мережу), водночас використовуючи Інтернет, як економічно вигідний засіб. І завдяки гнучкості відкритої технології VPN, можливість залучення додаткових партнерів є необмеженою.

Підключення віддаленого працівника

Віддалений користувач, будь то вдома чи в дорозі, хоче мати можливість безпечно й економічно ефективно підключатися до корпоративного інтранету. Наприклад, ви перебуваєте вдома або в дорозі, але вам потрібен конфіденційний файл на сервері в вашому офісі. Отримавши доступ до Інтернету ви можете зв'язатися з сервером в головному офісі та отримати необхідний файл.

Один зі способів реалізації цього сценарію – використання протоколу тунелювання для віддаленого доступу. Клієнт підключається до Інтернету через комутоване підключення до ISP, а потім встановлює автентифікований і зашифрований тунель між собою та брандмауером на межі інтранету.

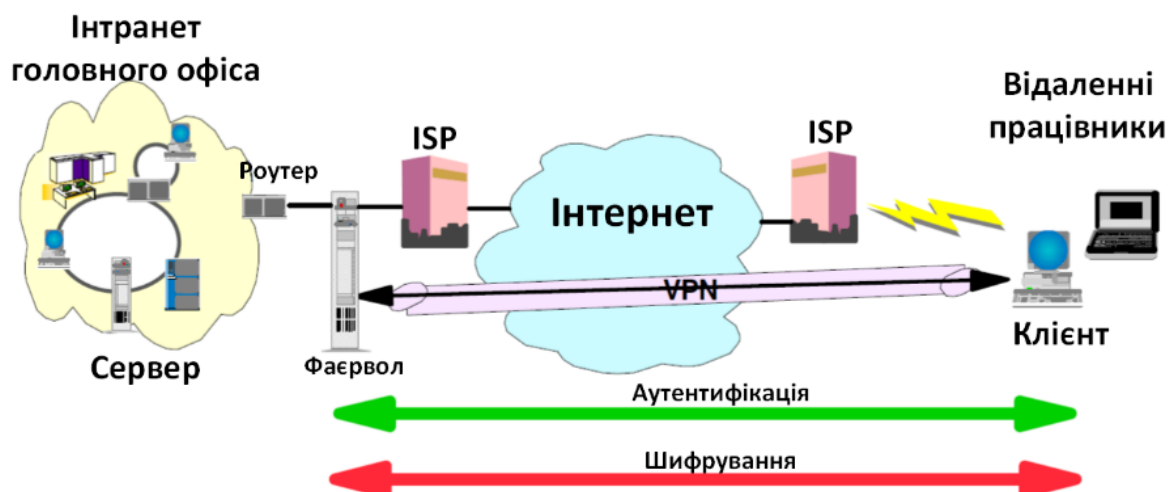


Рисунок 1.3 – З'єднання мережі головного офісу і пристрою клієнта через VPN

1.5 Різновид технологій VPN

Сучасні технології VPN відіграють ключову роль у забезпеченні безпечного та надійного з'єднання між користувачами і корпоративними мережами, а також між різними сегментами мережі. Нині існує ряд протоколів VPN, кожен з яких має свої переваги та обмеження, що впливають на вибір

відповідного рішення для конкретних завдань. Тому розглянемо основні різновиди VPN-технологій, їх характеристики та особливості використання [9].

1) PPTP (Point-to-Point Tunneling Protocol) — це тунельний протокол, що працює за принципом з'єднання точка-точка. Він дає можливість встановити безпечний канал зв'язку з сервером через створення спеціального тунелю у відкритій мережі. PPTP дозволяє інкапсулювати (обгортати або приховувати) пакети протоколу PPP у пакети протоколу Internet Protocol (IP) і передавати їх через IP-мережі, включно з Інтернетом. Цей протокол популярний через те, що вже вбудований у більшість пристроїв і платформ, простий у налаштуванні, ефективний і не потребує додаткового програмного забезпечення. Для встановлення безпечного з'єднання достатньо мати лише ім'я користувача, пароль та адресу сервера.

При першому випуску з Windows 95, PPTP мав численні проблеми з безпекою. Сьогодні протокол оновив свої методи шифрування до 128-бітного шифрування з ключем, що є прийнятним, але якщо безпека є критично важливою, можливо, слід розглянути інші варіанти. Навіть Microsoft рекомендує користувачам, які шукають вищі стандарти безпеки, використовувати SSTP або L2TP. Низький рівень шифрування робить PPTP одним з найшвидших VPN-протоколів.

Плюси PPTP:

- Висока швидкість з'єднання.
- Вбудований у більшість платформ.
- Простота налаштування.

Мінуси PPTP:

- Проблеми з безпекою (один з найменш захищених протоколів VPN).
- Може бути заблокований брандмауерами.

2) L2TP/IPsec. L2TP (Layer 2 Tunneling Protocol) — це протокол VPN, який сам по собі не забезпечує шифрування або захисту даних, що передаються через з'єднання. Тому його зазвичай використовують разом з IPSec, що є протоколом

шифрування. L2TP є розширенням PPTP, яке використовує технологію подвійної інкапсуляції, що сприяло його початковій популярності. Перша інкапсуляція встановлює з'єднання PPP, а друга забезпечує шифрування через IPSec.

L2TP підтримує алгоритм шифрування AES-256, які є одним з найзахищеніших. Однак підвищене шифрування може знижувати продуктивність з'єднання. Протокол вбудований у більшість настільних і мобільних операційних систем, що полегшує його впровадження. Проте L2TP використовує тільки UDP-порт 500 для з'єднання, що може легко блокуватися брандмауерами. Це вимагає додаткової конфігурації при використанні за брандмауером. L2TP може бути повільнішим, оскільки трафік спочатку перетворюється в форму L2TP і додається додатковий рівень шифрування. Це менш ефективне рішення порівняно з OpenVPN, але просте у налаштуванні [10].

Плюси L2TP/IPsec:

- Доступний на більшості пристроїв і операційних систем.
- Процес налаштування простий.
- Забезпечує високий (хоча і ослаблений) рівень безпеки.
- Підтримує багатопоточність для підвищення продуктивності.

Мінуси L2TP/IPsec:

- Гірша швидкість з'єднання через подвійне інкапсулювання.
- Може бути заблокований брандмауерами.

3) IKEv2/IPSec. IKEv2 (Internet Key Exchange version 2) базується на IPSec і був розроблений спільно Microsoft та Cisco. Хоча технічно це не є VPN-протоколом, він функціонує, як такий і відповідає за управління обміном ключами IPSec. В даний час IKEv2 вбудований у всі версії Windows починаючи з Windows 7, а також має реалізації для Linux, пристроїв Blackberry та інших платформ. Для користувачів Blackberry це один з небагатьох підтримуваних VPN-протоколів.

IKEv2 корисний для забезпечення постійного VPN-з'єднання, навіть при перемиканні між мережами. Він підтримує VPN-з'єднання, навіть якщо інтернет

або з'єднання зникає. Протокол відзначається стабільністю, безпекою та високою продуктивністю, зокрема для мобільних користувачів, які потребують безпечного і приватного з'єднання. Підтримка MOBIKE робить IKEv2 стійким до змін у мережевих умовах, тому з'єднання залишається стабільним під час перемикання між Wi-Fi та мобільними даними. Хоча він не підтримується на всіх пристроях, IKEv2 пропонує вищий рівень безпеки порівняно з L2TP, а також кращу швидкість і стабільність.

Плюси IKEv2/IPSec:

- Дуже безпечний, підтримує широкий спектр протоколів шифрування.
- Висока стабільність, навіть при втраті мережевого з'єднання.
- Простий у налаштуванні.
- Один з найшвидших протоколів VPN.

Мінуси IKEv2/IPSec:

- Обмежена підтримка платформ.
- Може бути заблокований брандмауерами.

4) SSTP (Secure Socket Tunneling Protocol) — це протокол захищеного тунелювання сокетів, розроблений Microsoft. Він є частиною їхніх операційних систем, починаючи з Windows 2008 та Windows Vista SP1. SSTP встановлює з'єднання через HTTPS на порті 443, використовуючи SSL для шифрування та поєднуючи SSL з PPP для автентифікації. SSTP (Secure Socket Tunneling Protocol) забезпечує механізм інкапсуляції трафіку PPP (Point-to-Point Protocol) через SSL (Secure Sockets Layer) протоколу HTTPS. Використання PPP дозволяє підтримувати методи строгої автентифікації, такі як EAP-TLS (Extensible Authentication Protocol-Transport Layer Security). SSL-протокол забезпечує безпеку на транспортному рівні завдяки покращеному узгодженню ключів, шифруванню та перевірці цілісності даних.

Плюси SSTP:

- Високий рівень безпеки завдяки SSL.
- Підтримується на Windows.

- Працює через порт HTTPS (TCP 443), тому менш імовірно буде виявлений і заблокований брандмауером.

Мінуси SSTP:

- Обмежена підтримка на не-Windows платформах.
- Приватний протокол Microsoft, що знижує прозорість.

5) OpenVPN — найбільш популярний протокол VPN, який реалізує створення захищених з'єднань за принципом «точка-точка» або «сайт-сайт» у маршрутизованих чи мостових мережах, а також для забезпечення віддаленого доступу [11]. OpenVPN використовує власний протокол безпеки, що базується на SSL/TLS для обміну ключами. Завдяки цьому протоколу однорангові вузли можуть автентифікувати один одного за допомогою секретного ключа, сертифіката або пари «ім'я користувача — пароль». Більшість VPN-провайдерів, що використовують OpenVPN, впроваджують пряму секретність для підвищення безпеки.

Хоча OpenVPN заснований на відкритому коді, багато хто вважає його одним із найбезпечніших VPN-протоколів. Він стабільний, надійний і гнучко налаштовується для роботи на будь-якому порту, підтримує апаратне прискорення для підвищення швидкості, здатний обходити брандмауери та NAT і використовує бібліотеки OpenSSL для шифрування. Однак для його роботи необхідне стороннє клієнтське програмне забезпечення.

Переваги OpenVPN:

- Протокол здатен обходити більшість мережевих екранів.
- Є проєктом з відкритим вихідним кодом.
- Забезпечує дуже високий рівень безпеки.
- Підтримує декілька методів шифрування.
- Має гнучкі налаштування.

Недоліки OpenVPN:

- Процес встановлення є досить складним.
- Для роботи необхідне стороннє програмне забезпечення.

6) WireGuard — це сучасний протокол VPN, який був розроблений для забезпечення високого рівня безпеки, швидкості та простоти використання. Його мета — бути швидшим, простішим і ефективнішим за IPsec. WireGuard також призначений для забезпечення вищої продуктивності порівняно з OpenVPN. Розроблений для універсального використання, він підходить як для вбудованих інтерфейсів, так і для суперкомп'ютерів, і підтримує різноманітні платформи, включаючи Linux, Windows, macOS, BSD, iOS та Android. Хоча протокол все ще активно розробляється, він вже може вважатися одним з найбільш безпечних, зручних у використанні та простих у налаштуванні рішень на ринку VPN.

Завдяки легшій та ефективнішій реалізації WireGuard забезпечує такий самий або навіть кращий рівень безпеки, ніж інші протоколи, але при цьому працює швидше та навантажує пристрої менше. Раніше розробникам доводилося обирати між безпекою та швидкістю при використанні VPN-протоколів, але WireGuard майже повністю усуває цей компроміс.

WireGuard почав набувати популярності кілька років тому і з тих пір став одним із основних стандартів для надійних VPN. Багато VPN-сервісів перейшли з OpenVPN на WireGuard, оскільки він поєднує в собі безпеку, швидкість і простоту впровадження в одному рішенні, що робить їхні послуги кращими.

Плюси WireGuard:

- Висока швидкість роботи завдяки легкому та ефективному коду.
- Високий рівень безпеки з використанням сучасних методів шифрування.
- Простий у налаштуванні та впровадженні.
- Низьке навантаження на пристрої через невелику кількість рядків коду.
- Мінуси WireGuard:
- Відносно нова технологія, яка може мати менше підтримки на деяких платформах.
- WireGuard не може динамічно призначати IP-адреси, замість цього використовується статична IP-адресація.

Основні відмінності вищезгаданих рішень наведено в табл.1.1.

Загальна характеристика технологій VPN

	PPTP	L2TP /IPSec	IKEv2 /IPSec	SSTP	OpenVPN	Wireguard
Безпека	Низька	Висока	Висока	Висока	Висока	Висока
Швидкість	Висока	Середня	Висока	Середня	Середня	Висока
Сумісність з різними ОС	Вбудована у більшості	Вбудована у більшості	Відносно сумісна	Переважно на Windows	Кросплатформенна	Кросплатформенна
Простота налаштування	Дуже проста	Проста	Проста	Проста	Складніша	Проста
Номер порта	TCP 1723	UDP 1701, UDP 500, UDP 4500,	UDP 500, UDP 4500	TCP 443	TCP 443, UDP 1194	Так
Можливість легко змінити номер порта	Ні	Ні	Ні	Ні	Так	Так
Динамічне призначення IP-адрес	Так	Так	Так	Так	Так	Ні
Стабільність з'єднання	Дуже стабільне	Стабільне	Стабільне	Дуже стабільне	Стабільне	Стабільне
Популярність	Низька	Середня	Середня	Середня	Висока	Стрімко зростаюча

Отже, підсумовуючи всі вище згадані протокол, можна сказати наступне:

PPTP простий у налаштуванні і швидкий, оскільки використовується слабе шифрування. Однак він має вкрай серйозні проблеми з безпекою і не рекомендований до використання.

L2TP/IPSec має стійкий алгоритм шифрування, не потребує додаткового програмного забезпечення для пристроїв, оскільки інтегрований у більшість настільних і мобільних операційних систем, легко реалізується та не має відомих серйозних вразливостей. Проте L2TP/IPSec має в порівнянні з іншими протоколами має гіршу швидкість через подвійну інкапсуляцію даних.

IKEv2/IPSec, який є частиною реалізації IPSec у Windows, простий у використанні. Водночас, існують певні проблеми сумісності між різними платформами.

SSTP забезпечує надійне шифрування, його важко виявити та заблокувати, і він повністю підтримується на пристроях з Windows, але має обмежену сумісність з іншими пристроями, крім Windows.

OpenVPN відомий своєю високою безпекою і гнучкістю налаштувань. Працює з різними методами шифрування і може обійти блокування брандмауера. Однак його налаштування може бути складним для початківців і для роботи потрібне стороннє програмне забезпечення.

WireGuard новий, швидкий, безпечний і простий для налаштування протокол. Однак він не підтримує динамічне присвоєння IP-адрес і є відносно новим протоколом.

Отже, виходячи з усіх вищенаведених характеристик та відмінностей вирішено, що OpenVPN буде кращим вибором для організації роботи VPN в корпоративній мережі завдяки поєднанню високого рівня безпеки, широкої сумісності та гнучкості. Даний протокол підтримує різні методи шифрування, що забезпечує надійний захист даних. До того ж OpenVPN є відкритим проєктом з активною спільнотою розробників, які постійно оновлюють і вдосконалюють протокол, що забезпечує швидке виправлення вразливостей і надійний рівень безпеки. Крім того, OpenVPN є кросплатформним, що дозволяє використовувати його на різних пристроях і операційних системах, однак для цього необхідно встановити стороннє програмне забезпечення. Він також пропонує можливість налаштовувати порти, що дозволяє обходити блокування брандмауера і працювати в умовах обмеженого доступу до мережі. Єдиним суттєвим недоліком є важкість налаштування, однак у відкритому доступі є безліч документацій та інструкцій по налаштування протоколу на тих чи інших платформах з відповідними налаштуваннями. Всі ці характеристики роблять OpenVPN універсальним та надійним рішенням для організацій, які шукають оптимальне поєднання безпеки та зручності використання.

1.6 Відомості щодо OpenVPN

OpenVPN – це VPN з відкритим вихідним кодом на основі SSL/TLS, оскільки він використовує протоколи SSL і TLS для забезпечення захищеного з'єднання [12].

OpenVPN застосовує HMAC у поєднанні з алгоритмом хешування для гарантування цілісності пакетів даних. Цей протокол може бути налаштований для використання, як попередньо спільних ключів (PSK, Pre-Shared Key), так і сертифікатів, що зазвичай недоступно в інших VPN на основі SSL.

OpenVPN використовує віртуальний мережевий адаптер (пристрої tun або tap) для зв'язку між програмним забезпеченням OpenVPN та операційними системами. Як правило, будь-яка операційна система, яка підтримує tun або tap, може працювати з OpenVPN, що включає майже всі відомі ОС, як Windows, Linux, Mac OS, FreeBSD, Solaris, AIX, iOS та Android. Однак для всіх згаданих платформ необхідно встановлювати клієнтське програмне забезпечення.

Хоча OpenVPN не визначений у стандарті RFC, протокол є загальнодоступним завдяки тому, що має відкритий вихідним кодом. Відкритий код підвищує безпеку, оскільки його регулярно перевіряють різні розробники, що зменшує ймовірність наявності прихованих вразливостей. OpenVPN має окремі канали для управління та передачі даних, кожен із яких шифрується та захищається окремо. Весь трафік проходить через одне з'єднання за протоколом UDP або TCP, причому канал управління шифрується та захищається за допомогою SSL і TLS, а дані — за допомогою спеціального протоколу шифрування. За замовчуванням OpenVPN використовує UDP порт 1194, однак досить легко можна змінити на будь-який інший UDP чи TCP порт.

Історія виникнення

Згідно з інтерв'ю опублікованому в 2003 році, розробник OpenVPN, Джеймс Йонан, подорожував Центральною Азією та підключався до свого офісу через азійських або російських інтернет-провайдерів. Те, що ці з'єднання встановлювалися через сервери в країнах із сумнівною ситуацією з безпекою,

дедалі більше усвідомлювало його проблеми безпеки. Дослідження Йонана показали, що в технології VPN існують два основні підходи: один орієнтований на безпеку, інший — на зручність використання. Жодне з рішень, доступних на той час, не пропонувало ідеального поєднання обох цілей. IPsec та його різні реалізації були складними у налаштуванні, але пропонували прийнятний рівень безпеки. Однак їхня складна структура робила їх вразливими до атак, помилок і недоліків у безпеці. Тому мережевий підхід, який Йонан виявив у деяких рішеннях, орієнтованих на зручність використання, здавався йому більш логічним. Це спонукало його створити модульну мережеву модель, використовуючи віртуальні мережеві пристрої TUN/TAP, які надавав ядро Linux.

Вибір моделі мережі на основі пристроїв TUN/TAP одразу забезпечив гнучкість, якої не могли запропонувати інші VPN-рішення. У той час як інші VPN на основі SSL/TLS потребували браузера для встановлення з'єднань, OpenVPN створював майже реальні (але все ще віртуальні) мережеві пристрої, на яких можна виконувати практично всі мережеві операції.

Йонан вирішив назвати свій проєкт OpenVPN на честь бібліотек і програм проєкту OpenSSL, а також через зрозумілий меседж, що це програмне забезпечення з відкритим кодом і безкоштовне.

Переваги та функціональні можливості

OpenVPN представляє нове покоління VPN. На відміну від багатьох інших рішень, що часто використовують власні або нестандартні механізми, OpenVPN використовує надійні й перевірені механізми SSL/TLS для автентифікації та шифрування. Він пропонує можливості, які перевершують можливості інших VPN:

- VPN другого і третього рівня. OpenVPN може працювати як на другому, так і на третьому рівні моделі OSI, що дозволяє йому передавати не тільки звичайні IP-пакети, а й Ethernet-кадри, IPX-пакети та NETBIOS-запити, з якими зазвичай виникають труднощі в інших VPN рішеннях.

- Захист віддалених працівників через внутрішній фаїрвол організації. Віддалений працівник, підключений до центрального офісу компанії через VPN, може налаштувати свій ноутбук так, щоб весь його трафік йшов лише через цей тунель. Після налагодження тунелю OpenVPN центральний фаїрвол компанії захищатиме ноутбук віддаленого працівника так, ніби він перебуває в локальній мережі. Це означає, що для роботи з локальною мережею (наприклад, клієнтською) працівнику потрібно відкрити лише один мережевий порт, а весь інший трафік буде надійно захищений.

- Можливість тунелювання в обхід правил фаїрволів. OpenVPN здатний проходити через майже будь-який фаїрвол завдяки легкій можливості змінити TCP або UDP порту.

- Підтримка IPv6. Даний протокол забезпечує можливість передачі трафіку через VPN-тунель у мережах, що використовують протокол IPv6, що робить його актуальним для сучасної інфраструктури.

- Підтримка проксі-серверів та різноманітних конфігурацій. OpenVPN можна налаштувати для роботи як у режимі TCP, так і UDP, при цьому він може функціонувати як сервер або клієнт. У режимі сервера OpenVPN чекає на запити від клієнтів, а в режимі клієнта — сам ініціює підключення відповідно до налаштувань.

- Потрібен відкрити лише один порт у фаїрволі для дозволу вхідних підключень. З моменту виходу OpenVPN 2.0, серверний режим дозволяє обробляти декілька вхідних підключень через один TCP або UDP порт, при цьому для кожного підключення можуть використовуватися різні конфігурації.

- Гнучкість завдяки можливостям сценаріїв OpenVPN надає широкі можливості для налаштування завдяки підтримці сценаріїв, які можна запускати під час підключення. Це дозволяє виконувати різноманітні завдання — від автентифікації до резервного перемикання.

- Динамічна адресація. OpenVPN підтримує автоматичне призначення IP-адрес клієнтам, що спрощує адміністрування мережі та забезпечує ефективне використання адрес у великих і змінних мережах.

- Модульна архітектура. OpenVPN відрізняється високим ступенем гнучкості та простоти як у налаштуваннях безпеки, так і в управлінні мережею. Жодне інше рішення VPN не пропонує такої ж кількості можливостей із аналогічним рівнем безпеки.

Захист в протоколі

Безпека в OpenVPN забезпечується за допомогою криптографічної бібліотеки OpenSSL, яка надає високий рівень захисту через протокол Secure Sockets Layer/Transport Layer Security (SSL/TLS) використовуючи стандартні алгоритми, такі як Advanced Encryption Standard (AES), Blowfish або Triple DES (3DES).

Комунікація в OpenVPN забезпечується за допомогою SSL/TLS. Це та ж технологія, яка використовується для захисту даних, що передаються на HTTPS веб-сайти та з них. Це є великою перевагою у випадку, якщо потрібно обійти брандмауер або інші блокування VPN, оскільки досить складно визначити, що використовує VPN, оскільки онлайн-активність виглядає як звичайний веб-трафік HTTPS.

OpenVPN використовує багато функцій SSL/TLS, таких як підтвердження того, що підключення відбувається до легітимного сервера, а також перевірка того, що дані не були змінені. Коректна імплементація сучасного веб-шифрування є величезним завданням, і, на щастя, OpenVPN не намагається це зробити самостійно, а передає більшість завдань шифрування бібліотеці OpenSSL.

Для аутентифікації використовуються сертифікати, а для шифрування – симетричні та асиметричні алгоритми шифрування. Кожен такий алгоритм має кілька характеристик: довжину ключа, розмір блоку та режим роботи. Довжина ключа визначає міцність шифру, розмір блоку – скільки даних шифрується в

одному блоці, а режим роботи—як саме використовується шифр. Інші важливі фактори – розповсюдження ключів і криптографічна стійкість шифру. OpenSSL використовує симетричні та асиметричні шифри як частину загальної безпеки. Проте безпека всієї системи настільки сильна, наскільки сильна її найслабша ланка. Наприклад, якщо використовується 40-бітний симетричний ключ і 2048-бітний асиметричний ключ, то найімовірніше, 40-бітний ключ буде найслабшою ланкою, що робить використання 2048-бітного асиметричного ключа надмірним.

В OpenSSL для симетричного шифрування використовуються блочні шифри, які можуть працювати в різних режимах. OpenVPN застосовує режим під назвою Cipher Block Chaining (CBC), що робить шифротекст поточного блоку залежним від шифротексту попереднього блоку. Це запобігає тому, щоб злоумисник міг побачити шаблони між блоками з ідентичними текстовими повідомленнями та маніпулювати одним або кількома з цих блоків.

Висновки до першого розділу

В даному розділі було розглянуто основні принципи та теоретичні аспекти, обраних рішень Mikrotik та OpenVPN для забезпечення захисту корпоративної мережі.

В ході розробки даного розділу було визначено призначення корпоративних мереж, їх інфраструктуру та основні види атак що спрямовані на них. Виконано опис різних методів і технологій захисту корпоративних мереж.

Розглянуто можливості та особливості обладнання виробництва Mikrotik латвійської компанія, яка спеціалізується на розробці мережевого обладнання та програмного забезпечення, зокрема операційної системи RouterOS. Сама RouterOS заснована на Linux та підтримує широкий спектр функцій, включаючи маршрутизацію, брандмауери, VPN, QoS та автоматизацію. Це робить її економічно вигідним рішенням для побудови складних мереж, зберігаючи при цьому високу продуктивність і безпеку.

Далі були розглянуті теоретичні основи роботи з VPN-технологіями, їх класифікація та різновиди. Основні типи VPN, такі як IPsec, L2TP і OpenVPN,

були розглянуті в контексті вибору найбільш підходящих рішень для різних вимог щодо безпеки та продуктивності. Вибір типу VPN залежить від конкретних потреб, таких як захищені з'єднання для віддалених працівників або безпечний обмін даними між філіями організації.

Визначено, що віртуальна приватна мережа (VPN) є важливою технологією для забезпечення безпеки при передачі даних через публічні мережі, такі як Інтернет, і широко використовується для з'єднання віддалених користувачів та офісів, об'єднуючи їх в єдину корпоративну мережу. VPN надає численні переваги, зокрема забезпечує безпечний доступ до корпоративних ресурсів, знижує витрати на зв'язок і масштабованість, а також дозволяє підключати віддалені мережі та користувачі незважаючи на їх географічну віддаленість. VPN використовує різні методи захисту даних, такі як шифрування і аутентифікація, що забезпечує конфіденційність і цілісність інформації при передачі через Інтернет, що робить її незамінною для віддалених працівників і глобальних корпоративних мереж.

Далі було наведено детальну характеристика основних VPN-протоколів, їх особливостей, переваг та недоліків. Було проаналізовано протоколи PPTP, L2TP/IPSec, IKEv2/IPSec, SSTP, OpenVPN та WireGuard, зокрема їх безпеку, швидкість, сумісність з різними операційними системами та простоту налаштування. Порівняння цих протоколів дозволило виявити сильні та слабкі сторони кожного з них у контексті використання в корпоративних мережах. Було зроблено висновок, що OpenVPN є оптимальним рішенням для організації VPN-з'єднань в корпоративній мережі завдяки поєднанню високої безпеки, гнучкості налаштувань і широкої сумісності з різними платформами.

РОЗДІЛ 2. РОЗРОБКА ПРОЄКТУ МЕРЕЖІ ТА ВИБІР ОБЛАДНАННЯ

2.1 Розробка загальної структури мережі

Корпоративна мережа – це інформаційна інфраструктура організації, яка забезпечує доступ до внутрішніх ресурсів, хмарних сервісів та обмін даними між офісами, філіями та віддаленими користувачами. Основними завданнями перед розробкою корпоративної мережі є забезпечення її високої продуктивності, можливість масштабованості, достатній рівень безпеки та надійності.

Архітектура корпоративної мережі може передбачати поділ на такі ключові компоненти:

- **Головний офіс** – центральний вузол мережі, де розташовані основні сервери, системи управління та брандмауери. Головний офіс виконує функцію об'єднуючого центру для філій та віддалених користувачів. Також він часто відповідає за централізоване управління мережею, обробку та зберігання критично важливих даних, резервне копіювання інформації та інше в залежності від потреб та специфіки роботи організації.

- **Філії** – це регіональні або територіально віддалені офіси, які можуть підключатися до головного офісу через захищені канали зв'язку з використанням технологій VPN. У філіях можуть розташовуватись локальні сервери для оперативного доступу до ресурсів, кінцеві пристрої користувачів (робочі станції, принтери тощо).

- **Віддалені користувачі** включають працівників, які працюють з дому, перебувають у відрядженнях або працюють за межами офісу. Доступ до корпоративної мережі для таких користувачів забезпечується через використання VPN, що дозволяє шифрувати трафік, аутентифікувати користувачів та надавати доступ лише до необхідних для них ресурсів.

Нижче на рис.2.1 наведено приклад підключення філіалу, бізнес-партнеру та віддаленого користувача до корпоративної мережі центрального офісу з використанням VPN-тунелів.

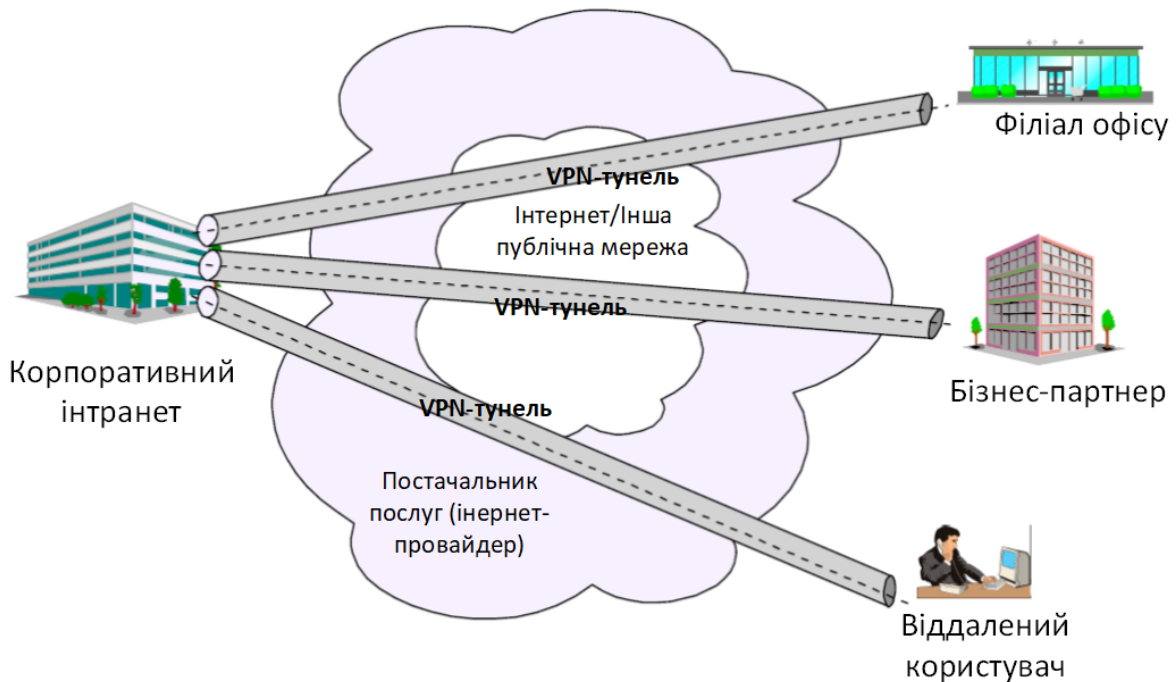


Рисунок 2.1 – Приклад підключення до корпоративної мережі різних компонентів з використанням VPN-тунелів

Трирівнева модель

Трирівнева (ієрархічна) модель мережі – це стандартна архітектура, яка забезпечує масштабованість, структурованість і високу продуктивність [13]. Вона складається з трьох рівнів: доступу (Access layer), агрегації (Distribution layer) та ядра (Core layer), рис.2.2. Використання даної моделі при розробці мережі головного офісу дозволить забезпечити оптимальний баланс між продуктивністю, безпекою та гнучкістю. Така архітектура дозволяє легко адаптувати мережу до потреб організації, інтегрувати нові технології та гарантувати безпечний і стабільний зв'язок між усіма її компонентами.

Рівень доступу (Access layer) – це рівень, на якому кінцеві пристрої, такі як комп'ютери, принтери та локальні сервери, підключаються до мережі. Цей рівень також називають «Рівнем робочих станцій», оскільки він дозволяє користувачам отримувати доступ до внутрішніх ресурсів і даних мережі. Рівень доступу є точкою входу в мережу для кінцевих пристроїв і включає в себе точки доступу для бездротових пристроїв, комутатори та кінцеві станції.

Рівень агрегації (Distribution layer) – це проміжний рівень, який відповідає за політики підключення та контролює межі між іншими рівнями мережі. На цьому рівні здійснюється маршрутизація і фільтрація трафіку, що дозволяє організувати ефективний потік даних між сегментами мережі. Цей рівень часто називають «Рівнем робочих груп», оскільки він забезпечує передачу трафіку з нижчих рівнів до рівня ядра, а також забезпечує управління доступом до мережі.

Рівень ядра (Core layer) – це основа мережі, яка забезпечує високу швидкість передачі даних між комутаторами на рівні агрегації. Цей рівень обробляє високошвидкісний трафік і забезпечує зв'язок між різними частинами мережі. Рівень ядра відповідає за маршрутизацію та передачу даних з мінімальною затримкою, що дозволяє мережі працювати стабільно та ефективно, навіть при високих навантаженнях.

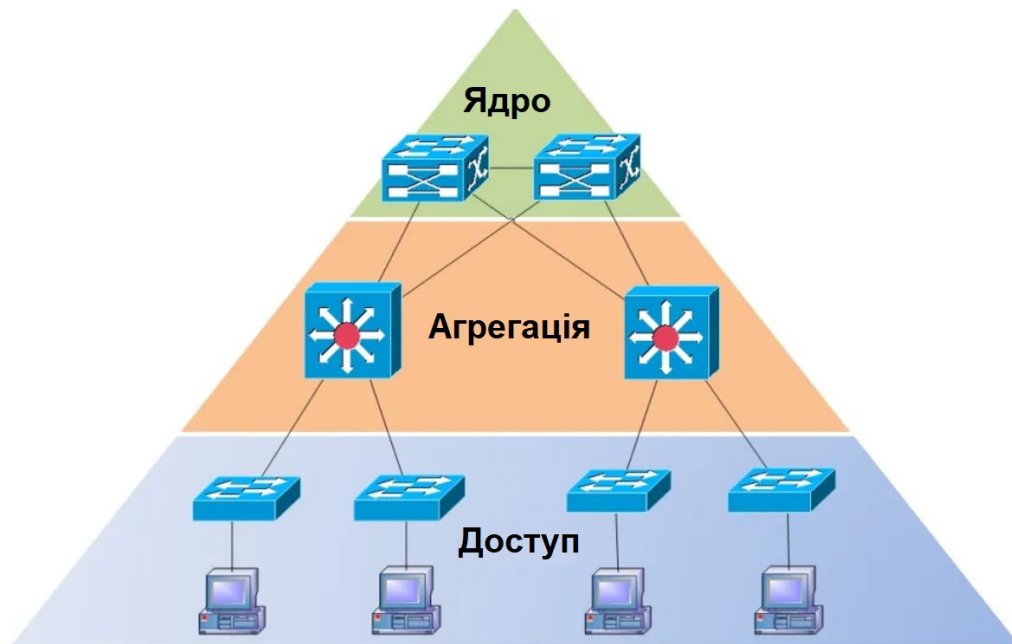


Рисунок 2.2 – Трирівнева модель мережі

Переваги використання даної моделі:

- Продуктивність. Ієрархічна мережа передбачає використання високопродуктивних комутаторів на рівнях ядра та розподілу. Це забезпечує швидшу передачу даних через мережу, оскільки інформація маршрутизується

через агреговані порти з мінімальною затримкою, що покращує загальну ефективність.

- **Надійність.** Завдяки модульній структурі мережі, сегменти, що вийшли з ладу, можна швидко ізолювати не порушуючи роботу решти мережі. Резервування на рівнях доступу, розподілу та ядра гарантує, що мережа залишатиметься доступною навіть при виникненні відмови в окремих її частинах.

- **Масштабованість.** Трирівнева модель дозволяє безпечно і без значних збоїв додавати нові елементи та сегменти. Завдяки структурованому підходу кожен новий компонент можна додавати, не порушуючи загальну архітектуру, що дозволяє легко розширювати мережу в міру зростання організації..

- **Безпека.** Завдяки чітко визначеним рівням доступу та можливості створювати складні списки контролю доступу дане проектування дозволяє більш ефективно контролювати трафік і виявляти потенційні загрози. Політики безпеки можна застосовувати на різних рівнях мережі, що дає змогу точно налаштувати захист для кожного користувача або відділу.

- **Управління.** Кожен рівень мережі виконує конкретну функцію, що спрощує адміністрування та технічне обслуговування. Оскільки комутатори на кожному рівні мають схожі налаштування, зміни можна здійснювати централізовано, що знижує ймовірність помилок і спрощує процес обслуговування.

- **Економічність.** Використання даної структури дозволяє зменшити витрати на обладнання завдяки можливості додавати нові елементи лише за необхідністю. Модульність дозволяє організації додавати нові компоненти без великих капітальних витрат, що робить таку архітектуру економічно вигідною.

- **Легкість у відновленні та усуненні несправностей.** Завдяки чітко структурованим рівням мережі, адміністратори можуть швидко ідентифікувати проблеми та визначати джерела несправностей. Кожен рівень мережі має свої чіткі функції, що дозволяє локалізувати проблему на конкретному рівні і вирішити її без значних затримок.

На рисунку 2.3 наведена розроблена загальна топологія мережі організації, що складається з головного офісу організації, її філіалу А та віддаленого користувача. Філіал та віддалений користувач підключені до головного офісу через використання VPN-тунелів і разом формують одну цілісну корпоративну мережу. Головний офіс, в свою чергу, спроектований з дотриманням трирівневої моделі мережі, що включає рівні ядра, агрегації та доступу.

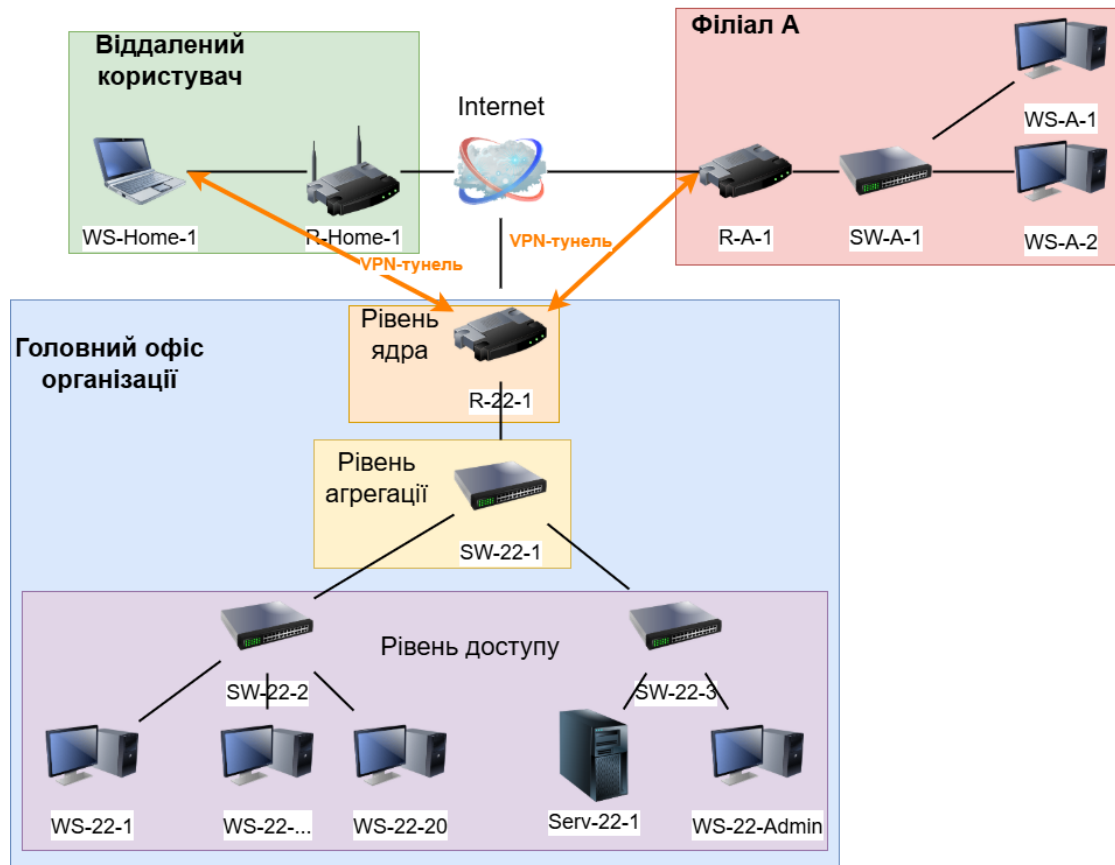


Рисунок 2.3 – Загальна топологія мережі

Розглянемо детальніше кожен компонент:

Головний офіс є центром управління мережею, у якому реалізована багаторівнева архітектура: ядро, агрегація і доступ.

- Рівень ядра представлений маршрутизатором R-22-1, що слугую центральним маршрутизатор і є точкою підключення головного офісу до Інтернету. Він забезпечує обробку вхідного/вихідного трафіку та передачу даних між зовнішніми вузлами (філіалами, віддаленими користувачами) і внутрішніми рівнями. Він також відповідає за маршрутизацію трафіку між рівнями агрегації і

виконує роль VPN-сервера, що забезпечує підключення віддаленого користувача та філіалу.

- Рівень агрегації представлений комутатором SW-22-1, що виконує роль проміжної ланки між ядром і рівнем доступу. Його основне завдання – оптимізація трафіку та підключення нових сегментів мережі.

- Рівень доступу включає комутатори SW-22-2 та SW-22-3 і кінцеве обладнання. Комутатори слугують точкою входу до мережі для комп'ютерів та серверів. Кінцеве обладнання представлене 20 комп'ютерами працівників на ОС Windows 10, 1 комп'ютером головного адміністратора теж на Windows 10 та 1 сервером на Windows Server 2019.

Філіал А представлений маршрутизатором R-A-1, комутатором SW-A-1 та 2 робочими станціями. R-A-1 слугує точкою виходу локальної мережі до Інтернету, а також забезпечує зв'язок з головним офісом через використання VPN-тунелю для організації підключення типу «Site-to-site».

Віддалений працівник представлений домашнім маршрутизатором R-Home-1 та ноутбуком WS-Home-1. R-Home-1 забезпечує лише вихід користувача до Інтернету, а з'єднання з головним офісом організовано прямо з комп'ютера WS-Home-1 за допомогою VPN-тунелю для підключення типу «Remote Access».

2.2 Розробка схеми адресації

Адресація мережі є важливою частиною проєктування корпоративної мережі. Від правильного вибору і структурування IP-адрес залежить ефективність роботи мережі, її масштабованість, безпека та простота управління. Схема адресації дозволяє оптимізувати використання IP-простору, забезпечує логічну організацію підмереж, полегшує маршрутизацію та підтримує інтеграцію із зовнішніми мережами.

Для зв'язку між маршрутизаторами на Інтернетом необхідно 3 підмережі:

R-22-1 – Internet –136.22.1.0/30

R-A-1 – Internet –136.22.2.0/30

R-Home-1 – Internet –136.22.3.0/30

Для роботи VPN-тунелів необхідно 1 підмережа, при чому адреси для клієнтів VPN будуть видаватись динамічно зі створеного пулу:

R-22-1 – VPN – 10.22.1.0/24

В таблиця 2.1 – 2.3 наведено розподіл IP-адрес для кожної локальної мережі.

Таблиця 2.1

Адресація локальної мережі LAN-HEAD-OFFICE

Призначення адрес	IP-адреса
Адреса мережі	192.168.1.0
Маска мережі	255.255.255.0
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.1.1
Максимальна адреса	192.168.1.254
Шлюз за замовчуванням	192.168.1.1
Призначені комутаторам	192.168.1.2 – 192.168.1.4
Призначені комп'ютеру адміністратора та серверу	192.168.1.10 – 192.168.1.11
Діапазон адрес майбутніх пристроїв	192.168.1.50 – 192.168.1.69
Діапазон вільних адрес	192.168.1.70 – 192.168.1.254

Таблиця 2.2

Адресація локальної мережі LAN-BRANCH-A

Призначення адрес	IP-адреса
Адреса мережі	192.168.2.0
Маска мережі	255.255.255.0
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.2.1
Максимальна адреса	192.168.2.254
Шлюз за замовчуванням	192.168.2.1
Призначені комутаторам	192.168.2.2
Діапазон адрес майбутніх пристроїв	192.168.2.10 – 192.168.2.11
Діапазон вільних адрес	192.168.2.12 – 192.168.2.254

Адресація локальної мережі LAN-HOME

Призначення адрес	IP-адреса
Адреса мережі	192.168.100.0
Маска мережі	255.255.255.0
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.100.1
Максимальна адреса	192.168.100.254
Шлюз за замовчуванням	192.168.100.1
Діапазон адрес майбутніх пристроїв	192.168.100.10
Діапазон вільних адрес	192.168.100.11 – 192.168.100.254

Для зручності нанесемо призначені адреси на топологію мережі, рис.2.4.
Це значно полегшить видимість мережі та її подальше налаштування.

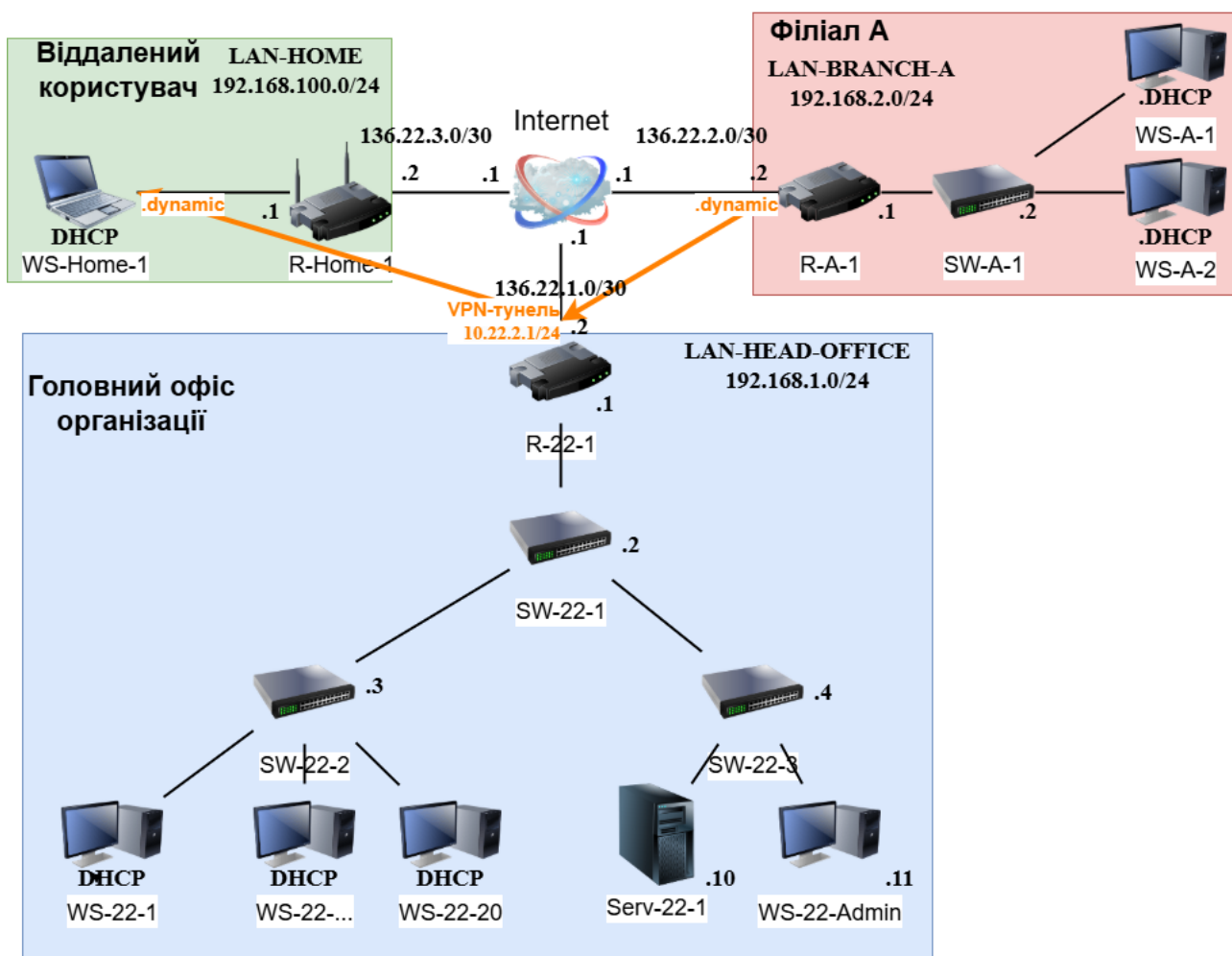


Рисунок 2.4 – Загальна топологія мережі з адресацією пристроїв

2.3 Розробка підсистеми захисту корпоративної мережі

Зростання загроз інформаційній безпеці та ризиків, пов'язаних із несанкціонованим доступом, вимагає впровадження ефективних методів захисту даних, моніторингу безпеки та забезпечення безпечного віддаленого доступу, що включає використання ряду наступних функцій та технологій:

1) Використання та налаштування роботи VPN, а саме OpenVPN, є ключовим аспектом для забезпечення безпечного підключення віддалених філій та користувачів до корпоративної мережі. Використання маршрутизатору Mikrotik у центральному офісі дозволяє налаштувати на ньому OpenVPN-сервер, до якого через захищені тунелі підключаються віддалені філії та користувачі. Це забезпечуватиме шифрування трафіку, аутентифікацію за допомогою сертифікатів, а також централізований та зручний доступ до ресурсів центрального офісу. Такий підхід мінімізує ризики перехоплення даних, забезпечуючи безпечну роботу з корпоративними ресурсами незалежно від місцезнаходження філії чи співробітника, що працює віддалено.

2) Всі Mikrotik, а саме їх ОС RouterOS, мають вбудований функціонал налаштування фаєрволу, що є важливим елементом для забезпечення безпеки корпоративної мережі, дозволяючи контролювати та фільтрувати трафік між сегментами мережі, а також захищати її від зовнішніх загроз. Використовуючи інструменти брандмауер, можна реалізувати необхідні політики доступу, блокувати підозрілий трафік, обмежувати доступ до певних ресурсів та запобігати несанкціонованому проникненню. На додачу до цього фаєрвол в Mikrotik включає налаштування NAT, фільтрацію пакетів, маркування трафіку та механізми протидії DDoS-атакам. Це дозволяє не лише ефективно захищати мережу від потенційних атак, а й підвищити продуктивність мережі, оптимізуючи її використання та управління ресурсами.

3) Syslog – це протокол для централізованого збору, зберігання та моніторингу журналів подій з різних пристроїв і додатків у мережі. Він дозволяє системним адміністраторам збирати важливу інформацію про стан мережі,

апаратне забезпечення та безпеку з одного або декількох джерел, що допомагає швидко виявляти і усувати проблеми, а також здійснювати аналіз подій. За допомогою Syslog можна централізовано зберігати логи, що включають різні повідомлення про помилки, попередження, критичні інциденти та інші події, важливі для безпеки й стабільності мережі.

4) RADIUS (Remote Authentication Dial-In User Service) є ключовим компонентом для централізованої автентифікації, авторизації та обліку (Authentication, Authorization, Accounting, AAA) в корпоративній мережі, що дозволяє ефективно і безпечно керувати доступом до ресурсів. Використання даного протоколу також надає деталізований облік активності, включаючи час підключення дозволяючи виявляти підозрілу поведінку. Завдяки цьому RADIUS забезпечує безпеку, масштабованість і зручність управління доступом у великих корпоративних мережах. Маршрутизатори Mikrotik підтримують інтеграцію з RADIUS-серверами, що дозволяє зручно реалізувати політики доступу на основі облікових записів і прав користувачів.

5) Використання SSH (Secure Shell) для доступу до мережевих пристроїв є критично важливим елементом для віддаленого та безпечного підключення до пристроїв. SSH дозволяє здійснювати захищений доступ до таких пристроїв, як маршрутизатори, комутатори та сервери, через зашифроване з'єднання, що захищає від перехоплення даних і атак "посередника". Завдяки використанню ключів для автентифікації, SSH забезпечує надійний механізм доступу без необхідності передавати паролі у відкритому вигляді. У корпоративних мережах SSH дозволяє адміністраторам ефективно керувати пристроями на відстані, здійснюючи налаштування, моніторинг та діагностику безпечно через зашифровані канали зв'язку. Для забезпечення безпеки рекомендується вимикати інші менш захищені методи доступу, такі як Telnet, і використовувати тільки SSH для доступу до мережевих пристроїв.

6) Відключення незадіяних інтерфейсів на комутаторах та призначення їм окремої VLAN є важливим заходом для підвищення безпеки мережі. Відключення інтерфейсів дозволяє знизити ризик несанкціонованого доступу, а

присвоєння окремої визначеної для них VLAN дозволяє ізолювати їх від основної мережі. Цей підхід не тільки зменшує ймовірність атак через неактивні порти, але й дає змогу ефективно керувати та контролювати доступ у мережі, зберігаючи ресурси та підвищуючи її безпеку.

2.4 Вибір обладнання

Наступним не менш важливим етапом в розробці проєкту мережі є вибір обладнання.

При виборі маршрутизаторів слід звернути увагу на пропускну здатність WAN/LAN, яка визначає швидкість обробки трафіку між інтерфейсами. Так для великого офісу потрібна пропускну здатність не менше 1 Гбіт/с. Важливою є наявність підтримки роботи OpenVPN для шифрування трафіку між віддаленими офісами та користувачами. Також слід врахувати кількість одночасних з'єднань, бо якщо мережа розрахована на 50+ користувачів, потрібен маршрутизатор із відповідним процесором та об'ємом оперативної пам'яті. Також можна звернути увагу на можливість масштабування, а також наявність базових функцій захисту, такого як брандмауер.

Тому на роль маршрутизаторів головного офісу та філіалу доцільно розглянути MikroTik CCR1009-7G-1C-1S+, рис.2.5. Це збалансоване рішення для корпоративних мереж, де потрібна висока продуктивність та надійність. Він оснащений 9-ядерним процесором TILE-Gx9 із тактовою частотою 1 ГГц та 2 ГБ оперативної пам'яті, що забезпечує стабільну обробку великих обсягів трафіку навіть у складних мережових середовищах [14].



Рисунок 2.5 – Маршрутизатор MikroTik CCR1009-7G-1C-1S+

Пристрій має сім портів Ethernet із пропускнуою здатністю до 1 Гбіт/с, один комбінований порт Ethernet/SFP для універсальності підключень і один порт SFP+ для швидкості до 10 Гбіт/с. Завдяки цьому маршрутизатор підходить для мереж, що вимагають обробки високошвидкісного трафіку та масштабування інфраструктури.

CCR1009-7G-1C-1S+ підтримує OpenVPN, що дозволяє налаштовувати захищені тунелі для з'єднання між офісами або віддаленими користувачами. Разом із іншими популярними протоколами VPN, такими як IPsec та L2TP, маршрутизатор забезпечує високий рівень захисту переданих даних. RouterOS, яка є операційною системою пристрою, пропонує широкий функціонал для керування мережею: брандмауери, фільтрація трафіку, QoS. Підтримка можливості резервного живлення через PoE забезпечує стабільність роботи пристрою навіть у випадку перебоїв із електроживленням. Тому CCR1009-7G-1C-1S+ є ідеальним вибором для корпоративних мереж із високими вимогами до швидкості, надійності й безпеки.

Для вибору комутаторів перш за все необхідно враховувати кількість портів, яка залежить від кількості підключених пристроїв. Швидкість портів також є важливою, адже сучасний стандарт – це гігабітні порти (1 Гбіт/с). Якщо потрібно підключати IP-камери, точки доступу чи VoIP-телефони, слід вибирати комутатори з підтримкою PoE. Варто враховувати пропускну здатність, яка визначає, наскільки швидко комутатор обробляє одночасний трафік. Для мереж на рівні агрегації бажана наявність uplink-портів зі швидкістю 10 Гбіт/с.

Цим параметрам добре відповідає Cisco WS-C2960X-24PD-L, рис.2.6. Даний пристрій є ефективним рішенням для мереж малого та середнього бізнесу, а також для корпоративних підрозділів. Він оснащений 24 портами Gigabit Ethernet, що забезпечують високу швидкість підключення для робочих станцій, серверів або інших пристроїв. Завдяки підтримці двох портів SFP, він дозволяє підключати оптоволоконні лінії для магістрального зв'язку або резервування [15].



Рисунок 2.6 – Комутатор Cisco WS-C2960X-24PD-L

Комутатор має підтримку PoE+ із загальною потужністю до 370 Вт, що робить його ідеальним вибором для підключення точок доступу, IP-камер та інших пристроїв, які живляться через Ethernet. Пристрій працює на рівні Layer 2 із базовими функціями Layer 3, що дозволяє виконувати маршрутизацію між VLAN та використовувати додаткові засоби управління трафіком.

Його пропускну здатність до 216 Гбіт/с забезпечує швидку обробку даних навіть у мережах із великим трафіком. Крім того, комутатор підтримує функції енергозбереження завдяки технології Energy Efficient Ethernet (EEE) і має резервне живлення для підвищення надійності. Тому дана модель є чудовим вибором для корпоративних мереж, де потрібна висока швидкість, зручність та підключення великої кількості пристроїв.

На роль домашнього маршрутизатора для віддаленого працівника доцільно обирати модель, яка забезпечить високу швидкість передачі даних, стабільне покриття та сучасні функції безпеки. Важливими параметрами є підтримка стандартів Wi-Fi 5 або Wi-Fi 6, які дозволяють досягти швидкості понад 100 Мбіт/с. Одним з таких популярних варіантів є TP-Link Archer AX50. Він підтримує стандарт Wi-Fi 6, забезпечує швидкість до 3 Гбіт/с, має чотири гігабітні LAN-порти для провідних підключень і оснащений сучасними технологіями безпеки, включаючи WPA3. Пристрій також підтримує мобільний додаток для легкого налаштування та управління мережею. Ця модель оптимально поєднує високу продуктивність, доступну ціну та функціонал, необхідний для домашньої мережі.

При виборі робочого комп'ютера з ОС Windows 10 для корпоративної мережі слід звернути увагу на наступні характеристики. Продуктивність процесора має забезпечувати швидку роботу з багатозадачними програмами, тому процесори Intel Core i5 або AMD Ryzen 5 є оптимальним вибором для більшості офісних завдань. Обсяг оперативної пам'яті відіграє не менш важливу роль. Мінімумально рекомендується 8 ГБ RAM, але для ефективної роботи з сучасним програмним забезпеченням краще мати 16 ГБ. Важливо також врахувати тип накопичувача. Сучасні SSD забезпечують швидке завантаження системи та програм, тому доречно обирати носій SSD на 256 ГБ або більше. Графічна складова залежить від специфіки завдань. Для базових офісних робіт достатньо вбудованої графіки, тоді як для графічного дизайну, обробки відео чи 3D-моделювання потрібна дискретна відеокарта. І на кінець, комп'ютер повинен підтримувати підключення до швидкісного Ethernet (1 Гбіт/с) і за бажанням сучасних стандартів Wi-Fi (Wi-Fi 5 або Wi-Fi 6).

При виборі сервера для корпоративної мережі на ОС Windows Server 2019 слід врахувати наступні параметри. Для стабільної роботи необхідно обрати серверний процесор, наприклад, Intel Xeon або AMD EPYC, які забезпечують багатоядерну обробку даних. Рекомендовано використовувати не менше 16 ГБ оперативної пам'яті, з можливістю розширення до 64 ГБ або більше. Сховище даних має бути швидким і надійним. Рекомендується SSD для основних операцій, доповнений HDD для архівних даних. Система зберігання повинна підтримувати масиви RAID для підвищення продуктивності та забезпечення резервування даних. Сервер повинен мати інтерфейс зі швидкість передачі даних 1 Гбіт/с. На майбутнє слід подбати про можливість розширення сервера, як от додавання оперативної пам'яті, дискових накопичувачів чи мережевих карт.

Висновки до другого розділу

В ході виконання даного розділу розглянуті основні принципи створення корпоративної мережі. Обґрунтовано вибір трирівневої моделі архітектури, яка забезпечує високу масштабованість, продуктивність та безпеку. Особливу увагу

було приділено функціональному поділу на рівні доступу, розподілу та ядра, що дозволяє забезпечити ефективне управління трафіком та підвищити надійність роботи мережі. Це рішення дає змогу створити інфраструктуру корпоративної мережі, яка відповідає потребам сучасних організацій, включаючи інтеграцію філій та віддалених користувачів.

У другому підрозділі було розроблено схему адресації мережі, яка враховує вимоги до логічного структурування трафіку, ізоляції сегментів та економії адресного простору. Було обрано підмережі, які дозволяють забезпечити гнучке розподілення IP-адрес для кожного сегмента мережі, враховуючи можливості масштабування в майбутньому.

В 3 розглянуто основні технології захисту корпоративної мережі які будуть використані у проєкті, зокрема застосування OpenVPN для безпечного віддаленого доступу, фаєрволу для контролю трафіку та захисту від зовнішніх загроз. Використання Syslog і RADIUS забезпечує централізоване зберігання логів та управління доступом. SSH гарантує безпеку віддаленого доступу, а відключення незадіяних інтерфейсів підвищує безпеку мережі. Використання даних технологій забезпечить надійний захист корпоративної мережі.

І в останньому підрозділі було детально розглянуто критерії вибору обладнання для корпоративної мережі, враховуючи особливості маршрутизаторів, комутаторів, домашніх маршрутизаторів для віддалених працівників, робочих комп'ютерів та серверів. В ході аналізу було підібрано оптимальні моделі пристроїв, які відповідають сучасним вимогам продуктивності, надійності, безпеки та масштабованості. Ретельний та комплексний підхід до вибору обладнання забезпечить високу продуктивність, надійність та безпеку корпоративної мережі, що дозволить організації ефективно виконувати свої завдання.

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ПЕРЕВІРКА РОБОТИ МЕРЕЖІ ТА ВИКОРИСТАНИХ РІШЕНЬ

3.1 Базове налагодження проєкту мережі

Для налаштування корпоративної мережі обрано мережевий емулятор GNS3 із використанням Oracle VirtualBox. Це рішення дозволяє створити віртуальне середовище, що максимально наближене до реальних умов і забезпечити повну інтеграцію з образами операційних систем та мережевого обладнання. GNS3 забезпечує гнучкість у моделюванні топологій, а VirtualBox дозволяє запускати віртуальні машини для тестування взаємодії між різними компонентами мережі. При цьому кількість кінцевих станцій у моделі буде зменшено для оптимізації ресурсів, що дозволить зосередитися на ключових аспектах налаштування та функціонування мережі. Використання такого підходу дозволяє відтворити повний цикл налаштування, тестування та оптимізації мережі, мінімізуючи витрати на реальне обладнання.

Перши етапом в налагодженні будуть маршрутизатори Mikrotik, а саме R-22-1 та R-A-1. В загальному виділяють наступні способи підключення до обладнання Mikrotik:

- Термінал (CLI) – конфігурування через командний рядок у самому маршрутизаторі. Це один із найпотужніших способів налаштування, який надає доступ до всіх команд RouterOS. CLI можна використовувати через.
- WinBox – це офіційна утиліта від MikroTik для налаштування маршрутизаторів через графічний інтерфейс. WinBox дозволяє виконувати всі конфігурації зручним чином і підтримує підключення через IP-адресу або MAC-адресу. Цей спосіб популярний завдяки інтуїтивному інтерфейсу та високій швидкості роботи [16].
- Веб-інтерфейс – вбудований веб-інтерфейс маршрутизатора, який дозволяє виконувати налаштування через браузер.

Тому для початку базове налаштування адресації буде виконано через термінальне підключення, однак надалі буде використовуватись WinBox,

оскільки це зручний і інтуїтивно зрозумілий інструмент для роботи з обладнанням MikroTik. Нижче на рис.3.1 наведено приклад налагодження адресації на маршрутизаторі R-22-1, однак на R-A-1 це відбувається схожим чином. В даному прикладі використовується команда `system identity set`, щоб задати ім'я маршрутизатора, тобто R-22-1. Потім через `ip address add` додається зовнішня IP-адреса на інтерфейс ether1 (підключений до Інтернету) і внутрішня IP-адреса на інтерфейс ether2 для локальної мережі. За допомогою `ip route add` налаштовується маршрут за замовчуванням, який спрямовує трафік через шлюз провайдера.

```
[admin@MikroTik] > system identity set name=R-22-1
[admin@R-22-1] > ip address add interface=ether1 address=136.22.1.2/30
[admin@R-22-1] > ip route add dst-address=0.0.0.0/0 gateway=136.22.1.1
[admin@R-22-1] > ip address add interface=ether2 address=192.168.1.1/24
```

Рисунок 3.1 – Налагодження параметрів адресації R-22-1

Подальше конфігурування маршрутизаторів буде здійснюватися через графічний інтерфейс WinBox. Для цього на сервер Serv-22-1 заздалегідь було виконано встановлення програмного забезпечення WinBox. Після запуску програми відображається перелік пристроїв до яких можна підключитись, в даному випадку це лише R-22-1. Тому обираємо відповідний пристрій, вводимо логін та пароль на натискаємо кнопку «Connect» рис.3.2.

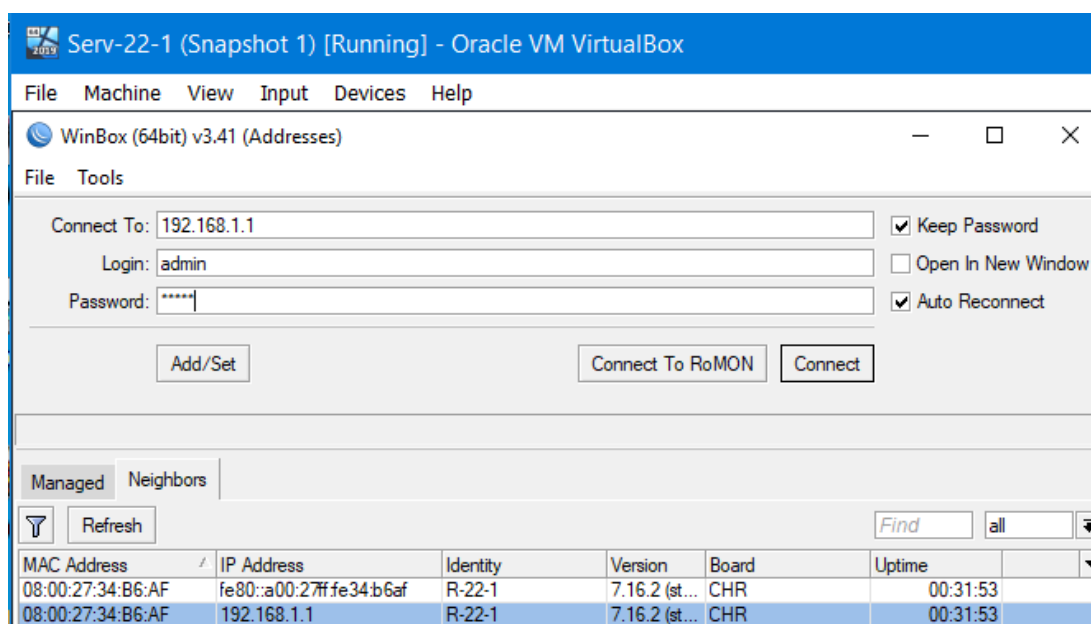


Рисунок 3.2 – Вибір маршрутизатора для підключення у WinBox

Якщо підключення відбулося успішно, то побачимо наступне вікно зі вкладками налаштування, рис.3.3. Аналогічно підключення виконується і для R-A-1.

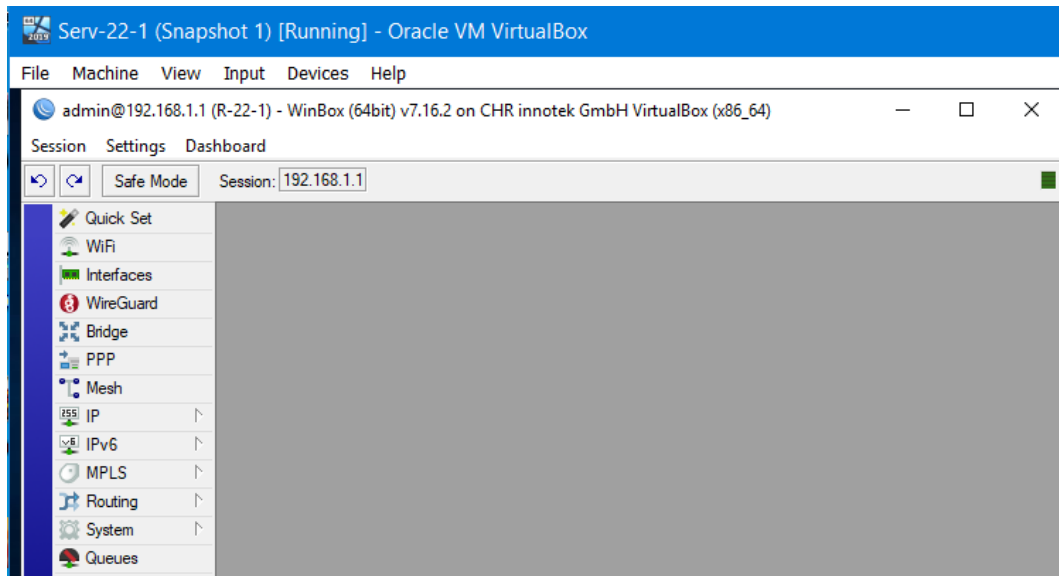


Рисунок 3.3 – Успішне підключення до R-22-1

Для філії А виконуємо налагодження DHCP-сервера на маршрутизаторі R-A-1 з використанням WinBox, рис.3.4. DHCP-сервер для мережі головного офісу буде налаштовано на сервері Serv-22-1 і буде виконано згодом.

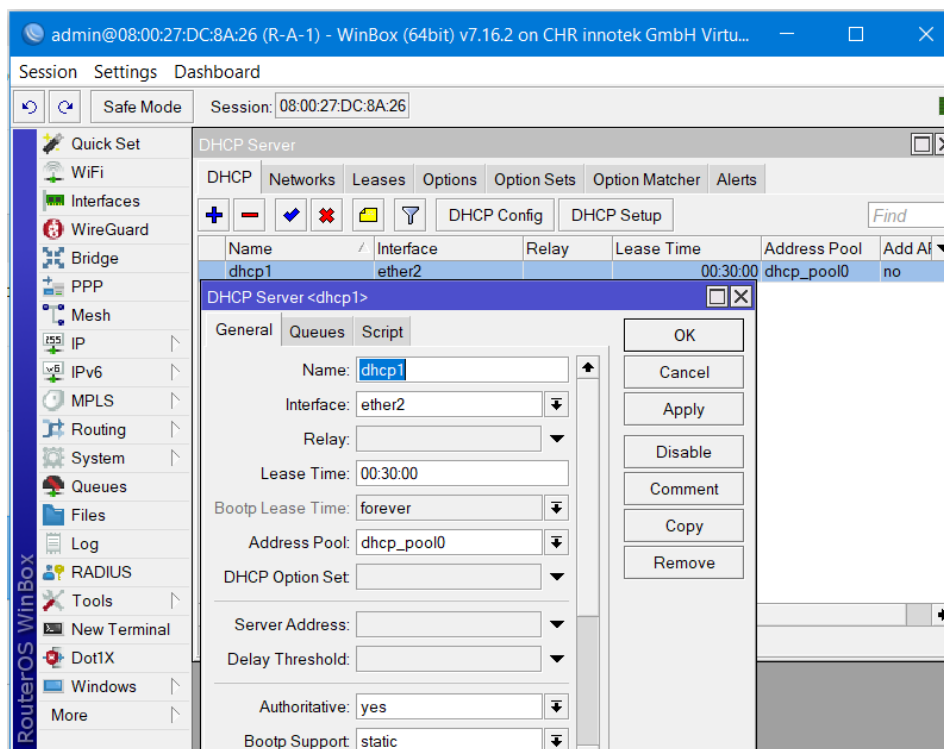


Рисунок 3.4 – Налаштування DHCP-сервера на R-A-1

Далі налаштовуємо параметри адрес DNS-серверів обох маршрутизаторах R-22-1 та R-1, аби пристрої локальних мереж могли використовувати дані маршрутизатори для доступу до Інтернету, рис.3.5.

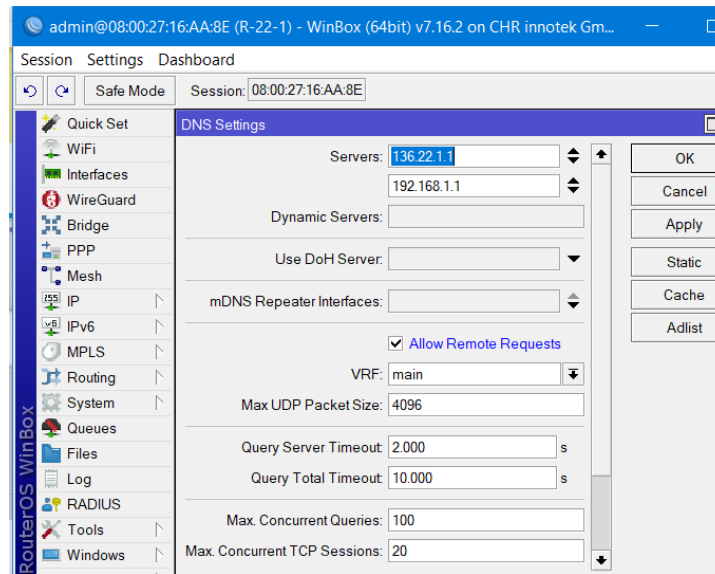


Рисунок 3.5 – Налаштування адреси DNS-серверів на Mikrotik

Для того, щоб пристрої в локальній мережі могли використовувати один публічний IP для підключення до Інтернету, потрібно налаштувати NAT в конфігурації PAT (Port Address Translation) на R-22-1 та R-A-1. Тут дія «masquerade» використовується для маскування IP-адрес. Вона замінює приватні IP-адреси вхідного трафіку на публічну IP-адресу маршрутизатора, коли трафік виходить з локальної мережі в Інтернет. Це дозволяє всім пристроям у локальній мережі використовувати одну публічну IP-адресу для доступу до Інтернету, рис.3.6.

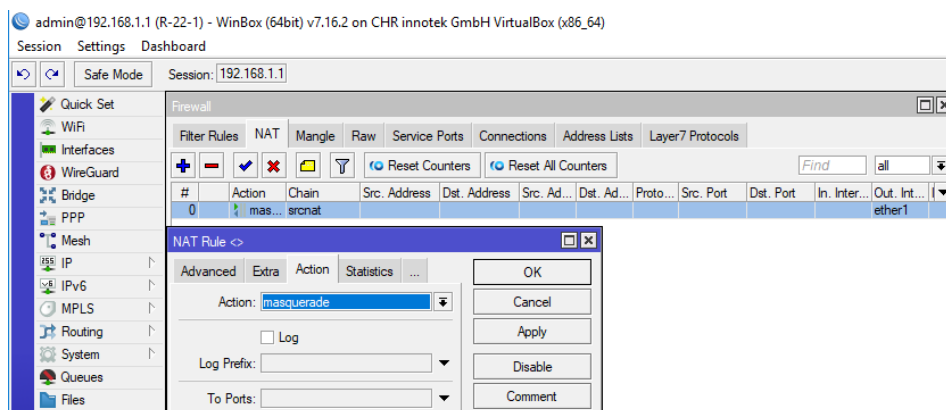
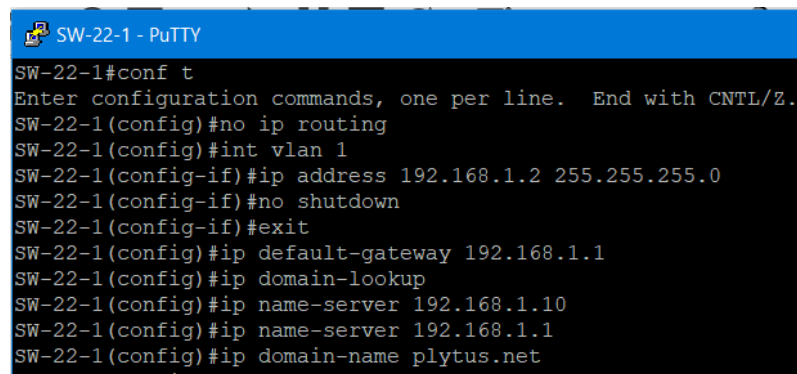


Рисунок 3.6 – Налаштування NAT на R-22-1

Тепер перейдемо до налаштування адресації на комутаторах. Спочатку з використанням `configure terminal` входим у режим глобальної конфігурації. За допомогою `int vlan 1` активується інтерфейс VLAN 1, а `ip address 192.168.1.2 255.255.255.0` присвоює йому статичну IP-адресу. Команда `no shutdown` активує інтерфейс. Для задання адреси шлюзу за замовчуванням використовується `ip default-gateway 192.168.1.1`, а `ip domain-lookup` вмикає DNS-пошук. Адреси DNS-серверів задаються командами `ip name-server`, а `ip domain-name plytus.net` задає доменне ім'я. Нижче на рис.3.7 наведено сценарій налаштувань для SW-22-1, однак на інших комутаторах це виконується подібним чином.



```
SW-22-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-22-1(config)#no ip routing
SW-22-1(config)#int vlan 1
SW-22-1(config-if)#ip address 192.168.1.2 255.255.255.0
SW-22-1(config-if)#no shutdown
SW-22-1(config-if)#exit
SW-22-1(config)#ip default-gateway 192.168.1.1
SW-22-1(config)#ip domain-lookup
SW-22-1(config)#ip name-server 192.168.1.10
SW-22-1(config)#ip name-server 192.168.1.1
SW-22-1(config)#ip domain-name plytus.net
```

Рисунок 3.7 – Базове налагодження комутатора SW-22-1

Переходим до налаштувань сервера Serv-22-1 та основних сервісів на ньому. Для цього задамо статичну адресу згідно виконаного розподілу, рис.3.8.

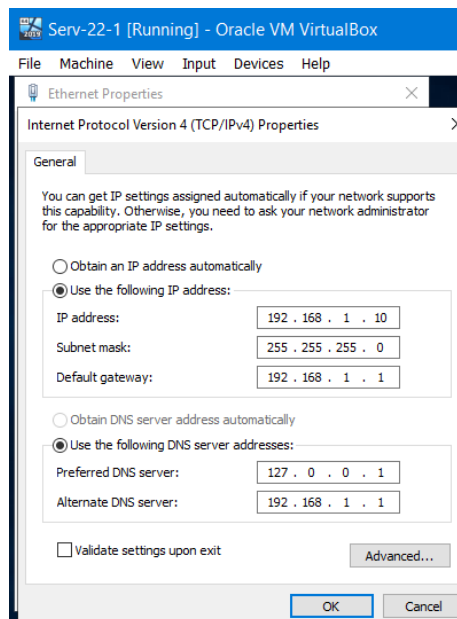


Рисунок 3.8 – Задання адресації на сервері

Далі в ході розгортання Active Directory зазначаємо ролі та функції, які необхідно встановити та згодом створюємо домен plytus.net, рис.3.9-3.11.

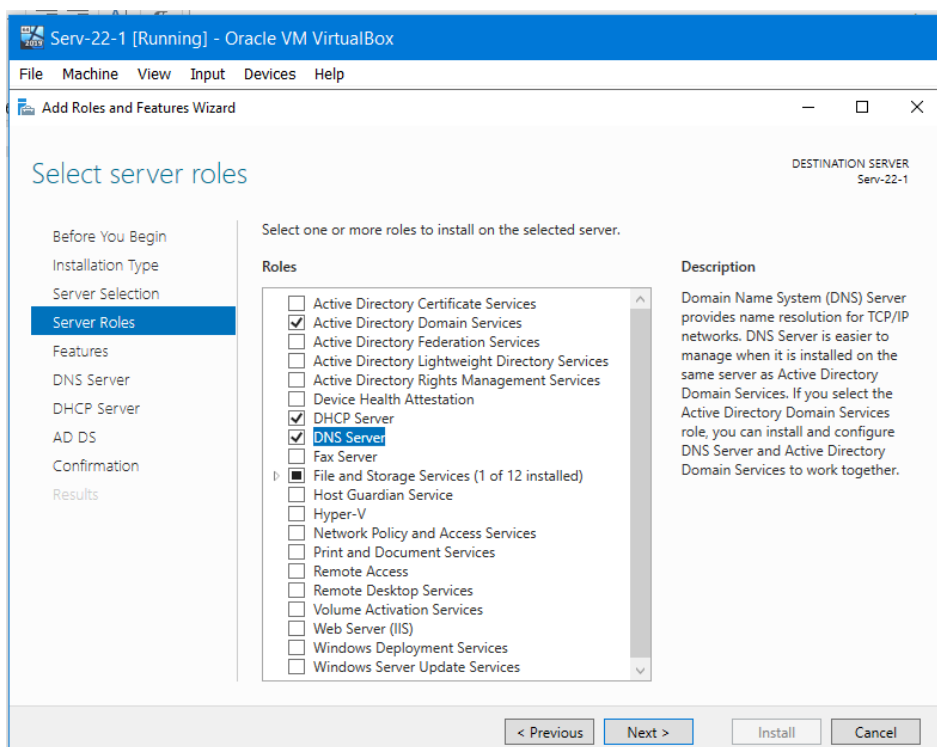


Рисунок 3.9 – Встановлення ролей

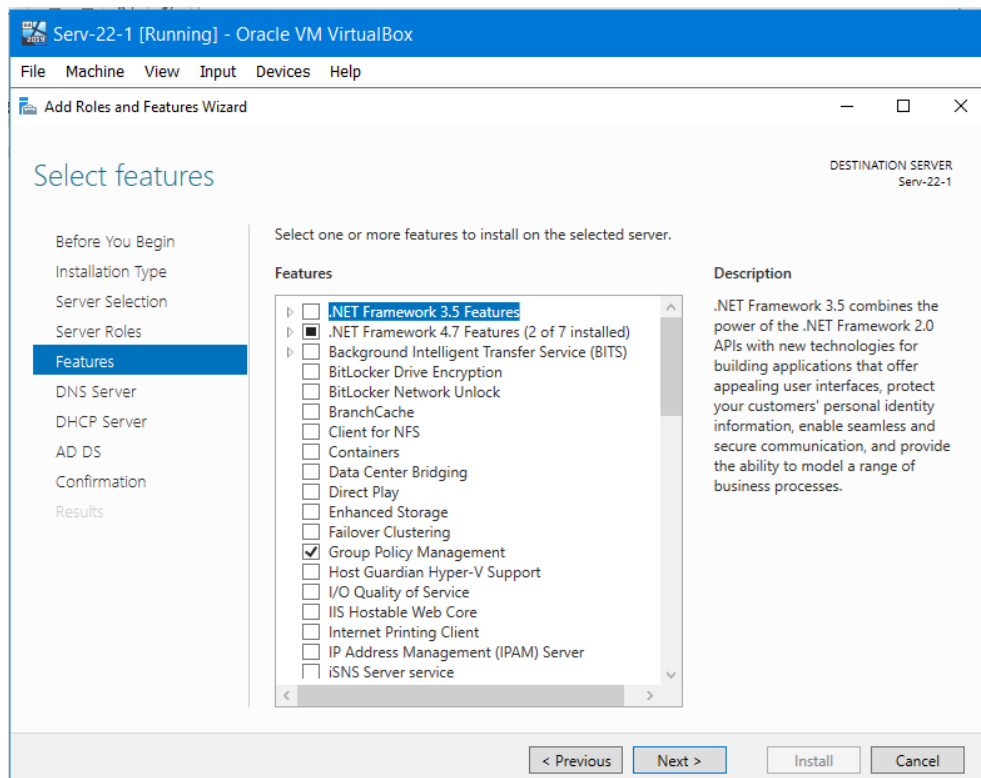


Рисунок 3.10 – Встановлення функцій

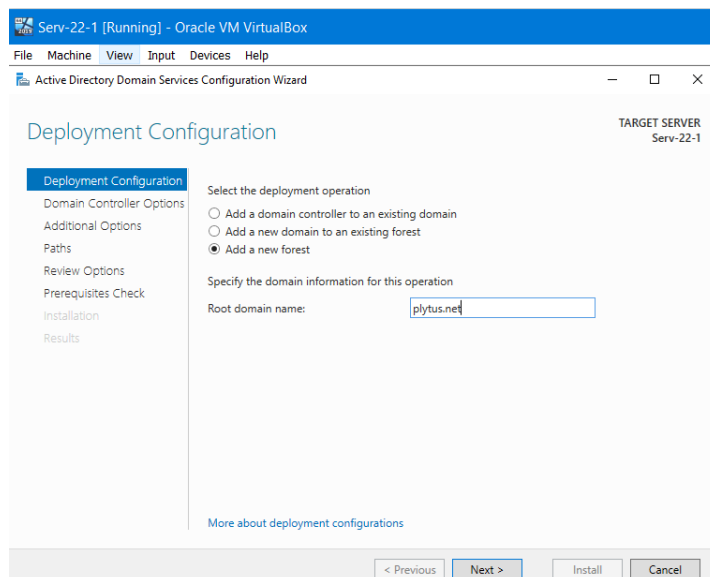


Рисунок 3.11 – Створення домену plytus.net

DHCP (Dynamic Host Configuration Protocol) служить для автоматичного призначення IP-адрес клієнтським пристроям в мережі. Без налаштування DHCP адміністратору доведеться вручну задавати IP-адреси для кожного пристрою, що є трудомістким і неефективним, особливо в великих мережах. Тому виконаємо налаштування роботи DHCP-сервера, рис.3.12.

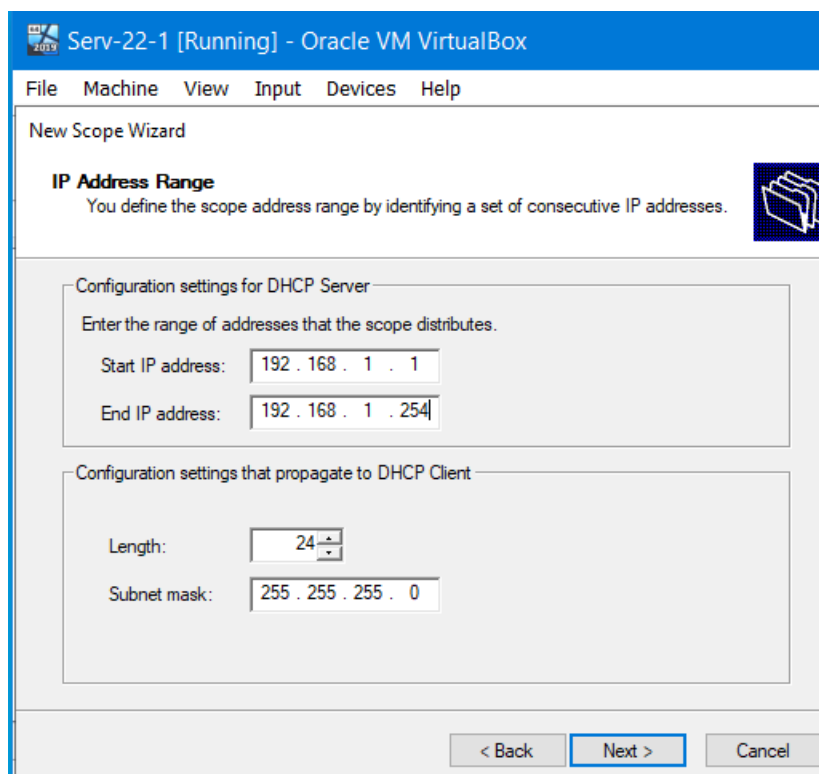


Рисунок 3.12 – Створення та налаштування пулу роздачі адрес

DNS (Domain Name System) служить для перетворення доменних імен на IP-адреси, що дозволяє користувачам звертатися до ресурсів за їхніми доменними іменами, замість запам'ятовування числових IP-адрес, що значно спрощує користування та адміністрування мережі. Нижче на рис.3.13 наведено процес додання статичних DNS-записів типу А для мережевих пристроїв мережі.

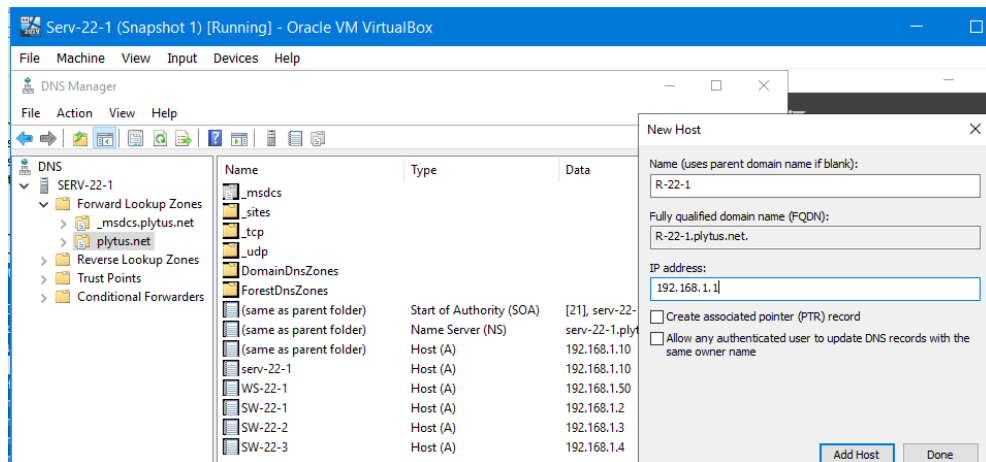


Рисунок 3.13 – Додання статичних DNS-записів типу А мережевих пристроїв

Створення користувачів на Windows Server дозволяє централізовано керувати доступом до мережевих ресурсів, забезпечувати безпеку і контролювати активність користувачів. Зрештою, це підвищує ефективність, зручність і безпеку мережі. Нижче на рис.3.14-3.15 наведено приклад створення одного з користувачів.

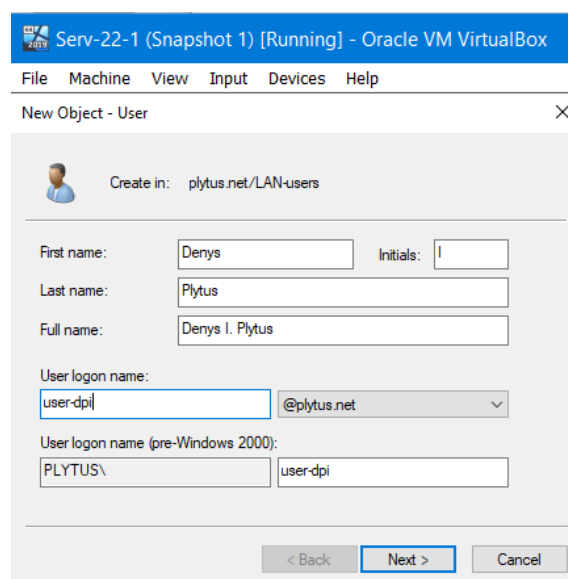


Рисунок 3.14 – Створення облікового запису користувача

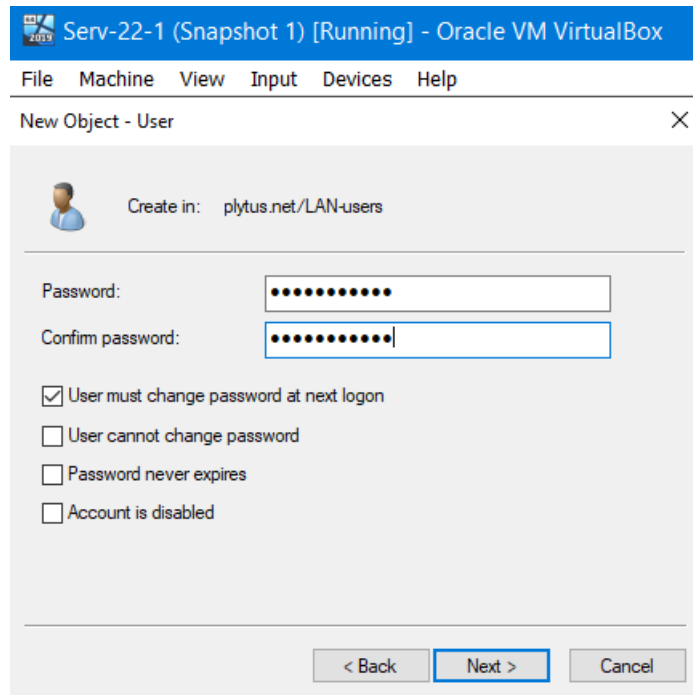


Рисунок 3.15 – Створення пароля облікового запису користувачів

Переходимо до налаштувань робочих станцій. Перш за все на всіх кінцевих пристроях виставляємо динамічне отримання адрес від DHCP-сервера. Нижче наведено приклад налаштувань для WS-22-1, однак те саме виконується на всіх кінцевих комп'ютерах.

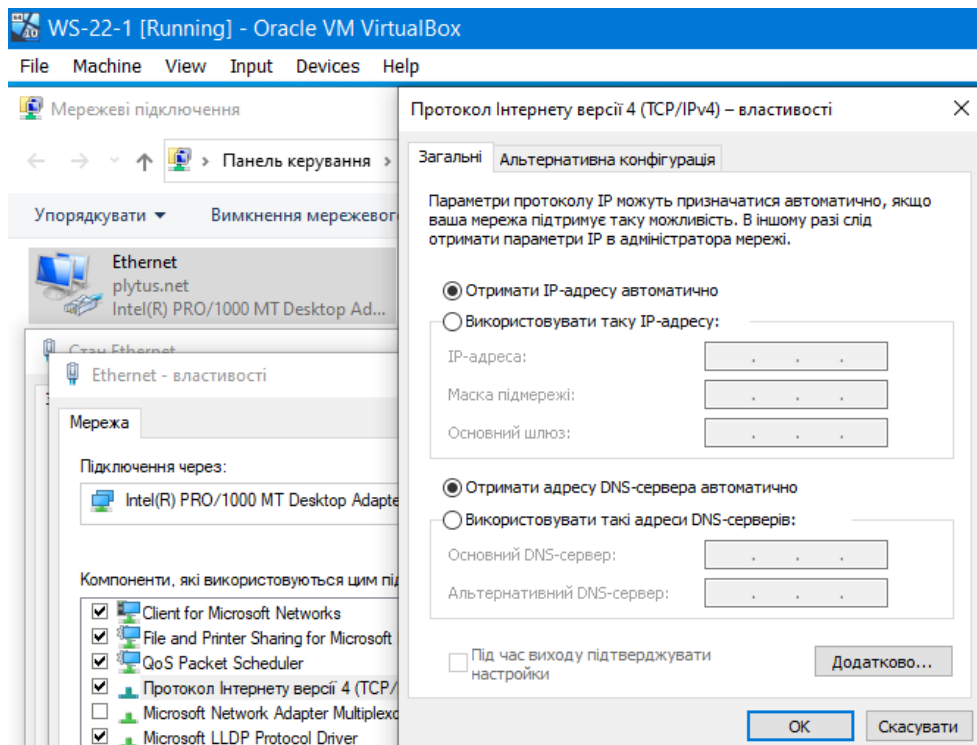


Рисунок 3.16 – Налаштування адресації на робочій станції WS-22-1

І відразу можемо перейти до DHCP-сервера Serv-22-1, щоб переконатись у правильності роздачі адрес, рис.3.17.

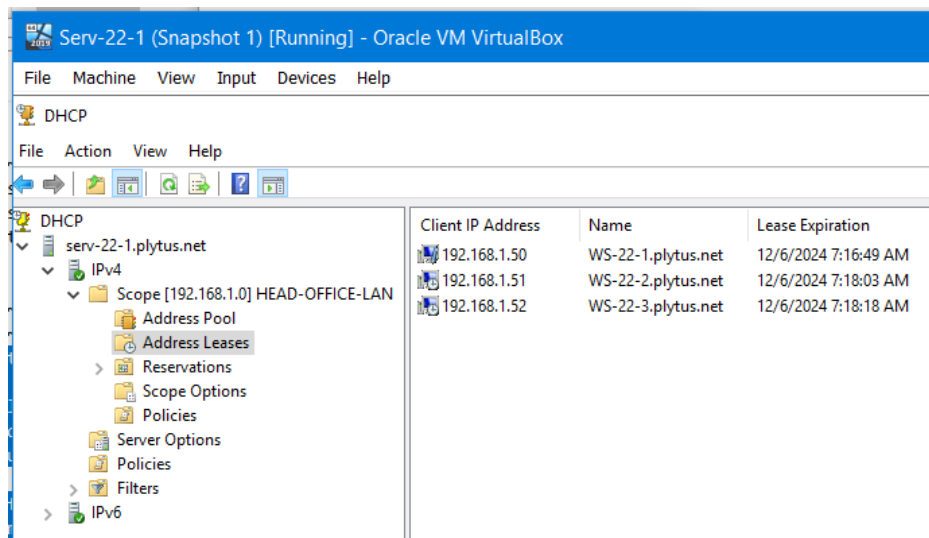


Рисунок 3.17 – Перевірка розданих адрес на DHCP-сервері Serv-22-1

Підключення пристроїв до домену дозволяє централізовано управляти доступом, безпекою та налаштуваннями на всіх пристроях, спрощує аутентифікацію користувачів і забезпечує стандартизацію політик у мережі. Нижче на рис.3.18 наведено підключення WS-22-1 до домену, однак всі інші кінцеві пристрої організації підключаються тим же чином.

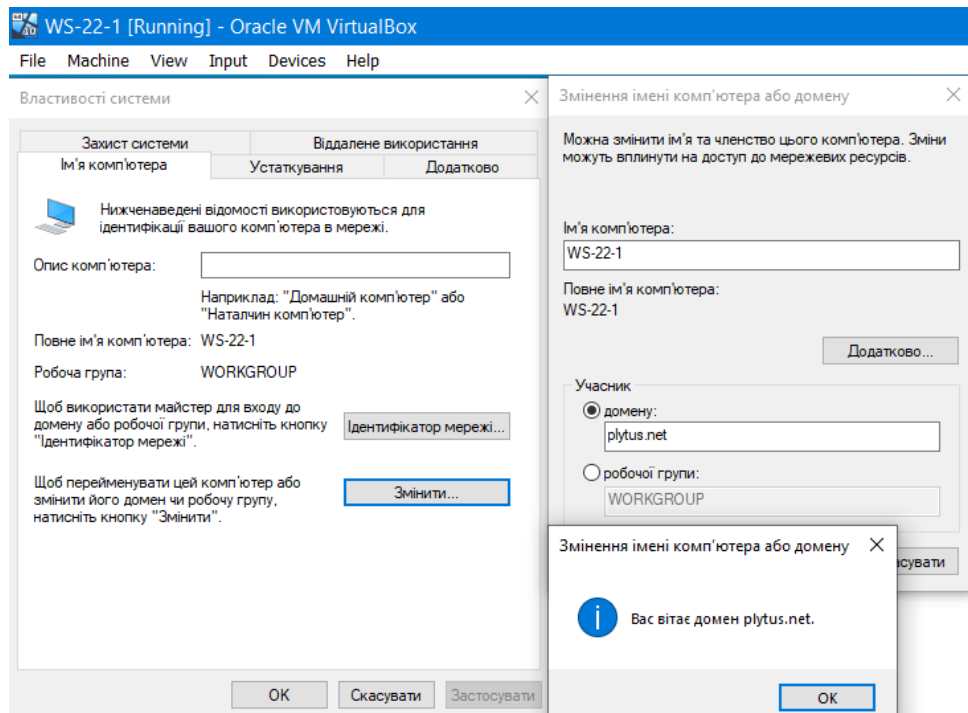


Рисунок 3.18 – Долучення робочої станції WS-22-1 до домену plytus.net

Після перезапуску виконуємо вхід в систему з використанням логіну та паролю облікового запису користувача, що був створений раніше на Serv-22-1, рис.3.19.

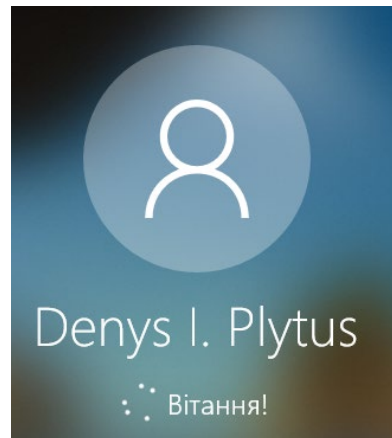


Рисунок 3.19 – Вхід в систему під користувачем Denys Plytus

Після успішного входу в систему перевіряємо зв'язок з пристроями локальної мережі та публічних ресурсів в мережі Інтернет з використанням команди ping, рис.3.20. Як видно з рисунку було отримано відповіді зі всіх пропінгованих вузлів, а це значить, що базові налаштування мережі були виконані успішно.

```
WS-22-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Windows PowerShell
PS C:\Users\user-dpi> ping serv-22-1

Pinging Serv-22-1.plytus.net [192.168.1.10] with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time=2ms TTL=128
Reply from 192.168.1.10: bytes=32 time=4ms TTL=128
Reply from 192.168.1.10: bytes=32 time=4ms TTL=128
Reply from 192.168.1.10: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 3ms
PS C:\Users\user-dpi> ping sw-22-2

Pinging sw-22-2.plytus.net [192.168.1.3] with 32 bytes of data:
Request timed out.
Reply from 192.168.1.3: bytes=32 time=1ms TTL=255
Reply from 192.168.1.3: bytes=32 time=2ms TTL=255
Reply from 192.168.1.3: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
PS C:\Users\user-dpi> ping google.com

Pinging google.com [142.250.186.206] with 32 bytes of data:
Reply from 142.250.186.206: bytes=32 time=41ms TTL=112
Reply from 142.250.186.206: bytes=32 time=38ms TTL=112
Reply from 142.250.186.206: bytes=32 time=45ms TTL=112
Reply from 142.250.186.206: bytes=32 time=35ms TTL=112

Ping statistics for 142.250.186.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 45ms, Average = 39ms
PS C:\Users\user-dpi>
```

Рисунок 3.20 – Використання ping для перевірки зв'язку

3.2 Налаштування OpenVPN на пристроях

Перш ніж приступити налаштування OpenVPN, важливо перевірити кілька основних аспектів конфігурації маршрутизатора. Це включає в себе налаштування часу на маршрутизаторі, перевірку доступу до Інтернету, а також налаштування основних мережевих інтерфейсів [17]. Перевірка доступу до Інтернету та налаштування інтерфейсів було виконано в попередньому розділі, тому лишається лише час.

Для коректної роботи SSL/TLS сертифікати необхідно, щоб час на маршрутизаторі був коректний та синхронізований. Для цього на обох маршрутизаторах Mikrotik налаштовується робота NTP-клієнта, який дозволяє автоматично синхронізувати час з публічним NTP-сервером, для прикладу 0.ua.pool.ntp.org. Виконані налаштування NTP на R-22-1 і його перевірка роботи наведено нижче на рис.3.21, однак та сама дія виконується і на R-A-1.

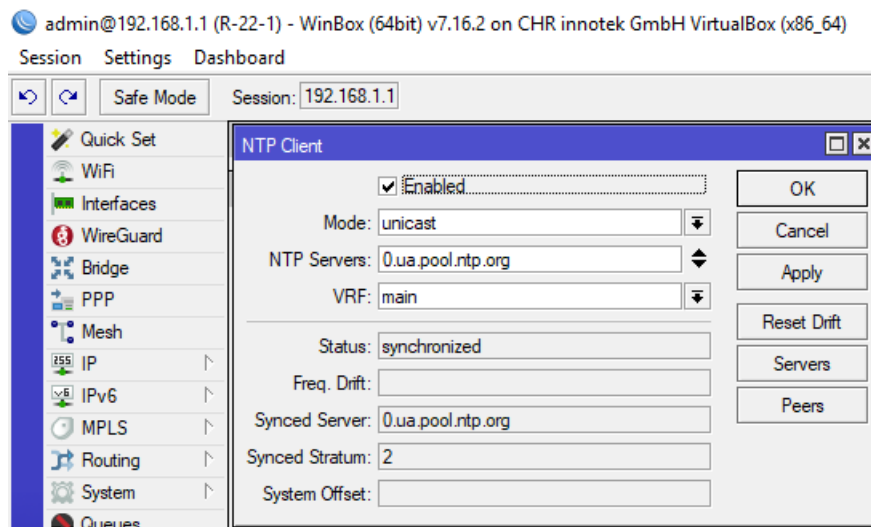


Рисунок 3.21 – Налаштування роботи NTP-клієнта

Налаштування сервера OpenVPN

Як було згадано, OpenVPN в своїй роботі використовує сертифікати для шифрування трафіку та забезпечення автентифікації користувачів і серверів [18]. Сертифікати можна згенерувати кількома способами, залежно від потреб і доступних інструментів. Найпоширеніші методи включають використання внутрішніх засобів MikroTik, програмного забезпечення OpenSSL, утиліти Easy-

RSA або сертифікаційних центрів (CA). Однак найпростішим та зручним є використання вбудованих засобів MikroTik, які забезпечуються простотою, швидкістю та не потребують використання сторонніх інструментів.

Отже, для початку необхідно створити кореневий сертифікат (CA), а потім на основі цього сертифіката генерувати сертифікати для сервера і клієнтів. Для цього переходимо у вкладку System – Certificate і заповнюємо відомості стосовно сертифікату, що включає його назву та відомості про власника. Розмір ключа задається в полі Key Size, а термін дії (дні) в Days Valid. За замовчуванням термін дії становить 365 днів, однак для кореневого сертифікату це значення можна збільшити до 3650 (10 років). Процес створення наведено на рис.3.22.

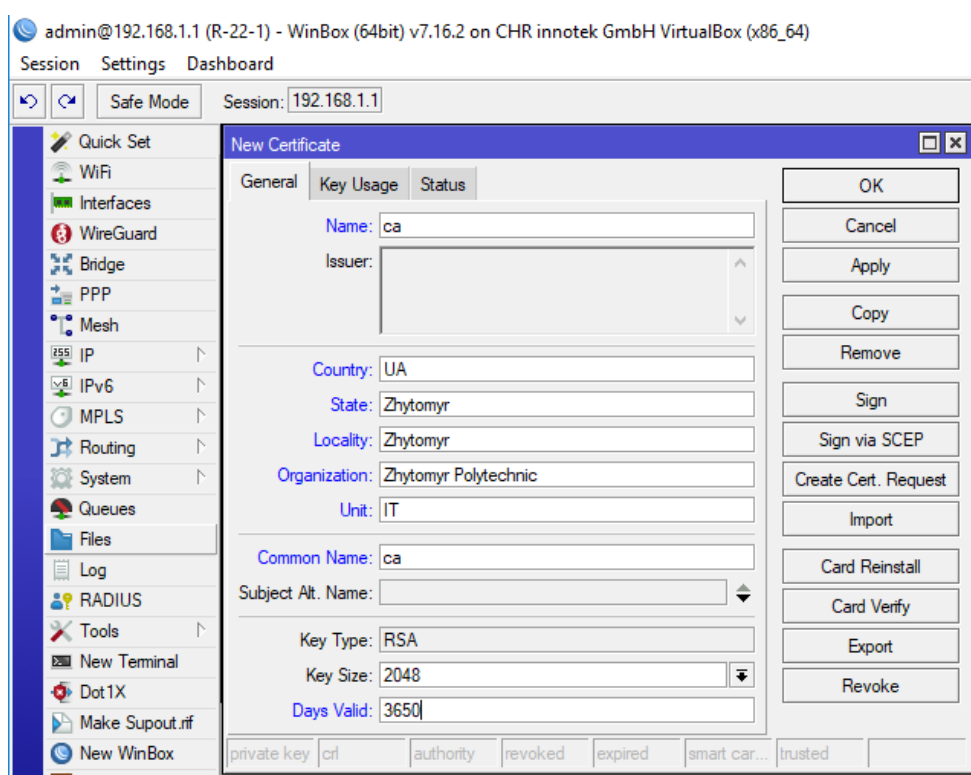


Рисунок 3.22 – Створення кореневого сертифікату (ca)

Далі в цьому ж вікні перейдемо у вкладку Key Usage і ставимо відмітки лише напроти «crl sign» та «key cert. sign» і натискаємо Apply. Тепер підпишемо сертифікат натиснувши на кнопку Sign. В новому вікні заповнюємо поле CA CRL Host де вказуємо публічну адресу маршрутизатора, тобто 136.22.1.2 і натискаємо Start, рис.3.23. Створення кореневого сертифікату завершено.

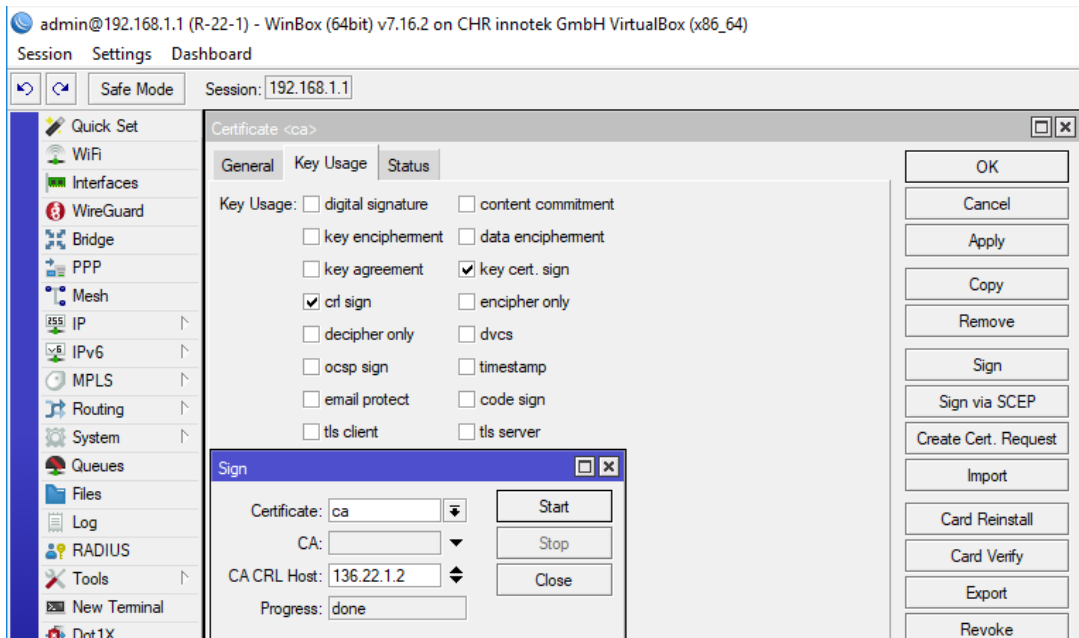


Рисунок 3.23 – Підпис кореневого сертифікату (ca)

Наступним кроком є створення сертифіката для OpenVPN сервера (ovpn-server). Даний процес подібний на створення кореневого сертифікату (ca). Єдиною відмінністю є інші відмітки в полі Key Usage, де треба поставити відмітки лише біля digital-signature, key-encipherment і tls-server. А під час підпису в полі CA вказується раніше створений кореневий сертифікат (ca), рис.3.24-3.25.

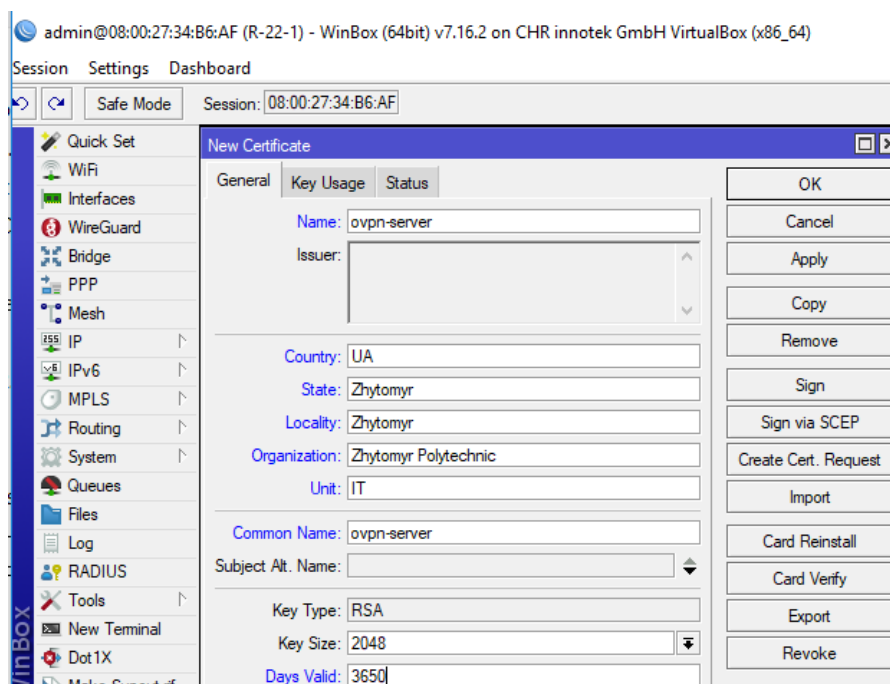


Рисунок 3.24 – Створення сертифікату сервера (ovpn-server)

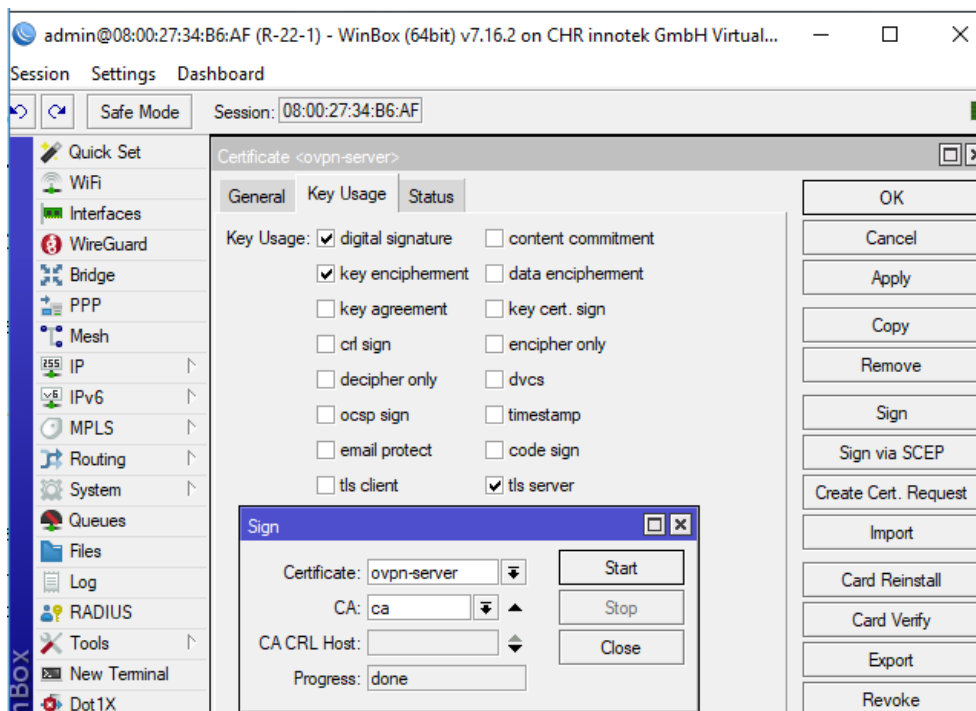


Рисунок 3.25 – Підпис сертифікату сервера (ovpn-server)

Для кожного клієнта, який підключатиметься до OpenVPN сервера, необхідно створити окремий сертифікат. Тобто сертифікат для філії А (client-branch-a) та віддаленого працівника (client-remote-user-1). Процес виконання подібний, відмінністю є зменшення терміну дії сертифікату для віддаленого працівника до 365 днів і у вікні Key Usage ставиться відмітка напроти «tls-client». Процес створення та підпису сертифікатів наведено на рис.3.26-3.29.

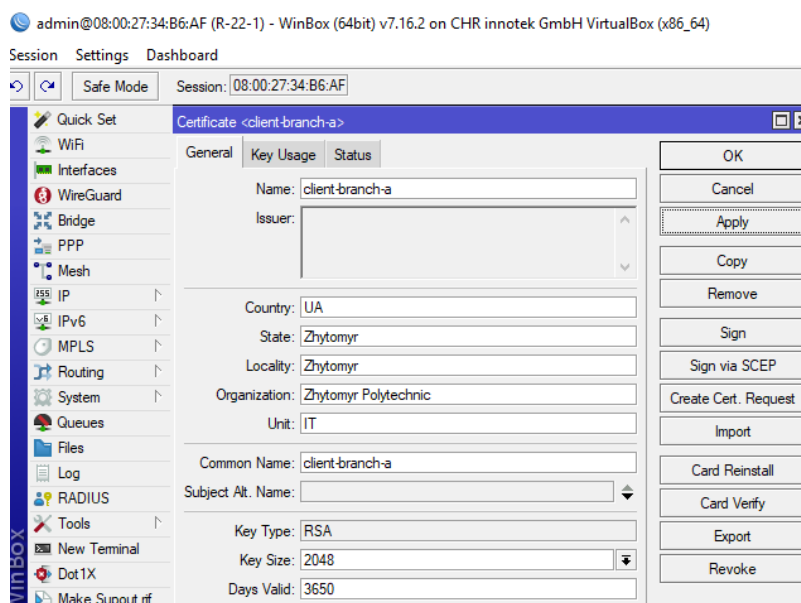


Рисунок 3.26 – Створення сертифікату клієнта для філії А (client-branch-a)

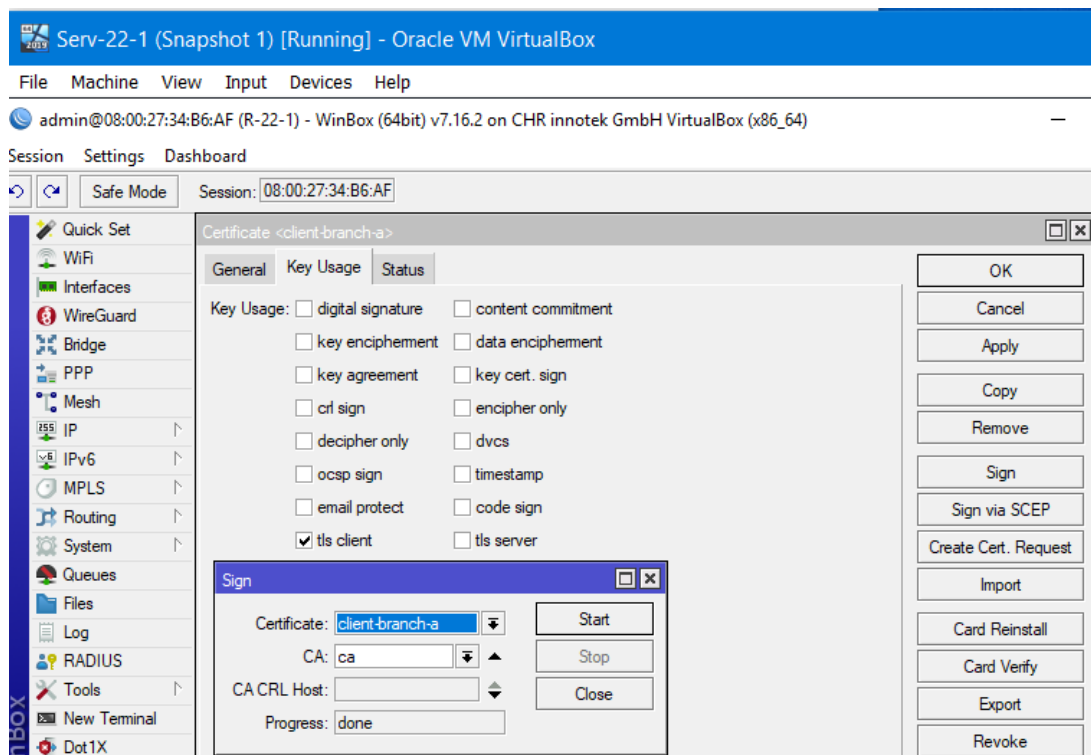


Рисунок 3.27 – Підпис сертифікату клієнта для філії А (client-branch-a)

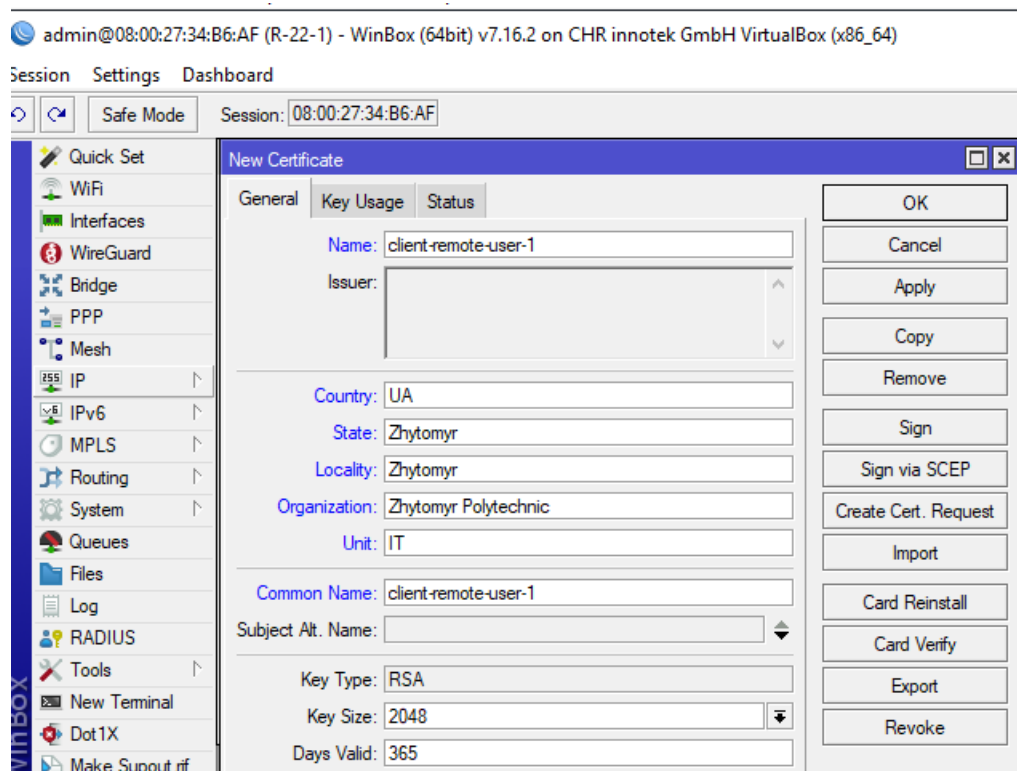


Рисунок 3.28 – Створення сертифікату клієнта віддаленого користувача (client-remote-user-1)

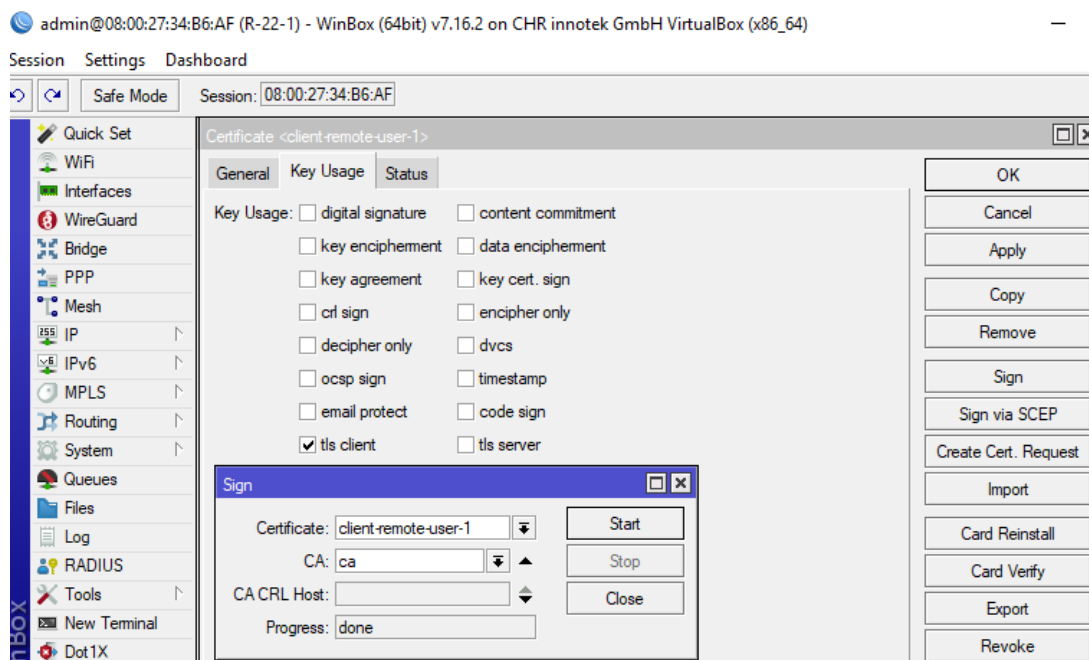


Рисунок 3.29 – Підпис сертифікату клієнта віддаленого користувача (client-remote-user-1)

Після генерації сертифікатів, необхідно налаштувати роботу OpenVPN сервера. Кожен клієнт VPN повинен отримати свою IP-адресу з певного пулу, тобто з 10.22.1.0/24. При цьому слід врахувати, що перша адреса діапазону (10.22.1.1), буде належати серверу OpenVPN, тобто R-22-1, тому її не слід включати до діапазону. Створення пулу адрес наведено нижче, рис.3.30:

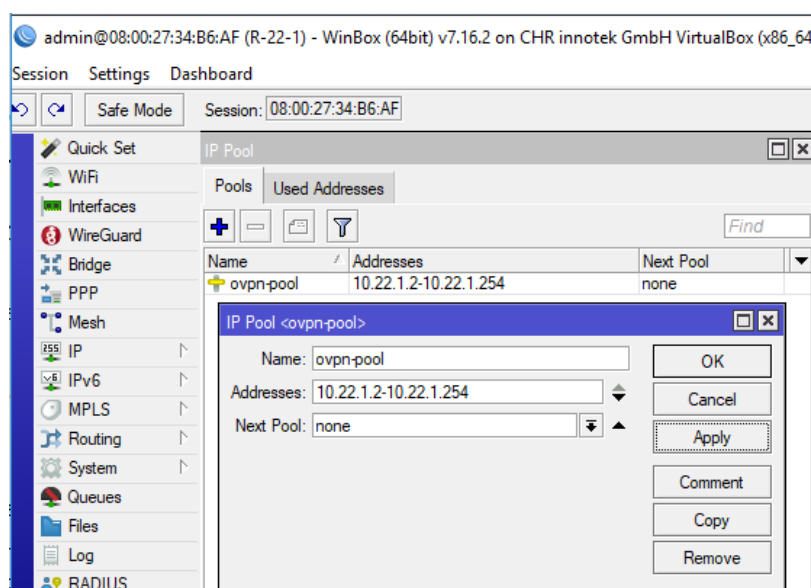


Рисунок 3.30 – Створення пулу адрес для клієнтів VPN

OpenVPN використовує профілі для визначення параметрів підключення. Нижче на рис.3.31 наведено процес створення профілю, в якому вказуються ім'я профілю, локальна адреса сервера, створений пул адрес для клієнтів та адреси DNS-серверів.

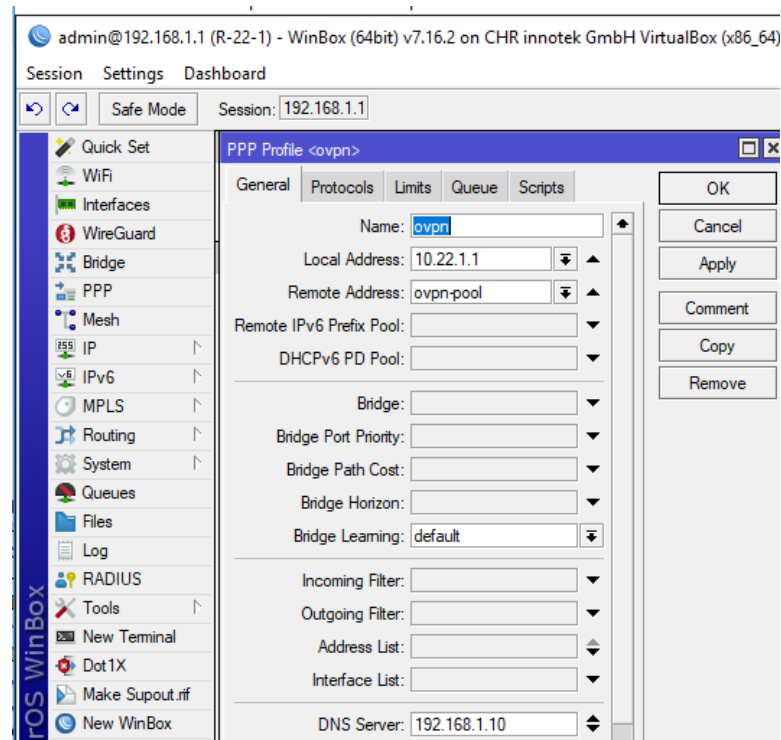


Рисунок 3.31 – Створення профілю PPP для OpenVPN

Кожен клієнт, який підключатиметься до OpenVPN сервера, повинен мати свій обліковий запис. З метою зручності доречно давати такі самі імена, що і при створенні відповідних сертифікатів. Також тут вказується пароль, тип сервісу – оvpn та ім'я створеного профілю PPP, рис.3.32-3.33.

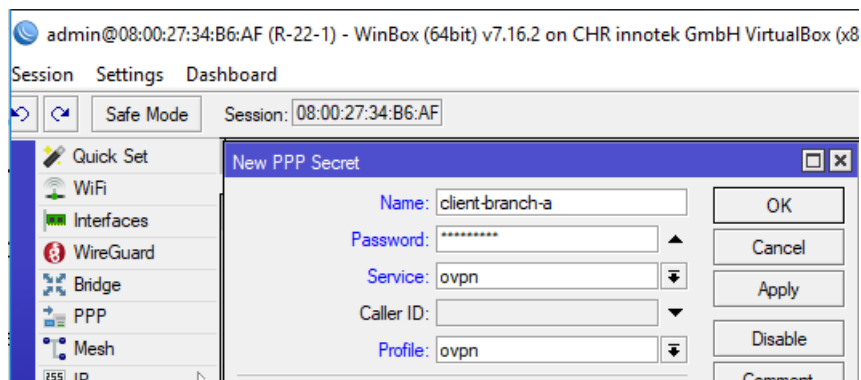


Рисунок 3.32 – Створення облікового запису для філії А

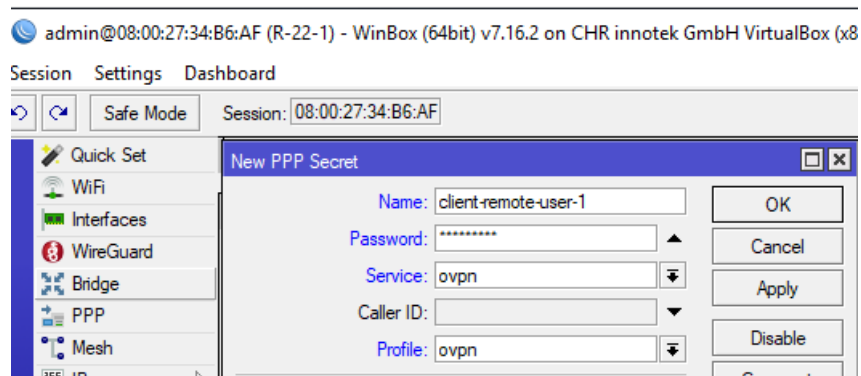


Рисунок 3.33 – Створення облікового запису для віддаленого користувача

Для налаштування сервера OpenVPN потрібно вказати ім'я профілю PPP (ovpn), створений сертифікат сервера OpenVPN (ovpn-server), підтримувані алгоритми хешування, шифрування та маршрут, рис.3.34.

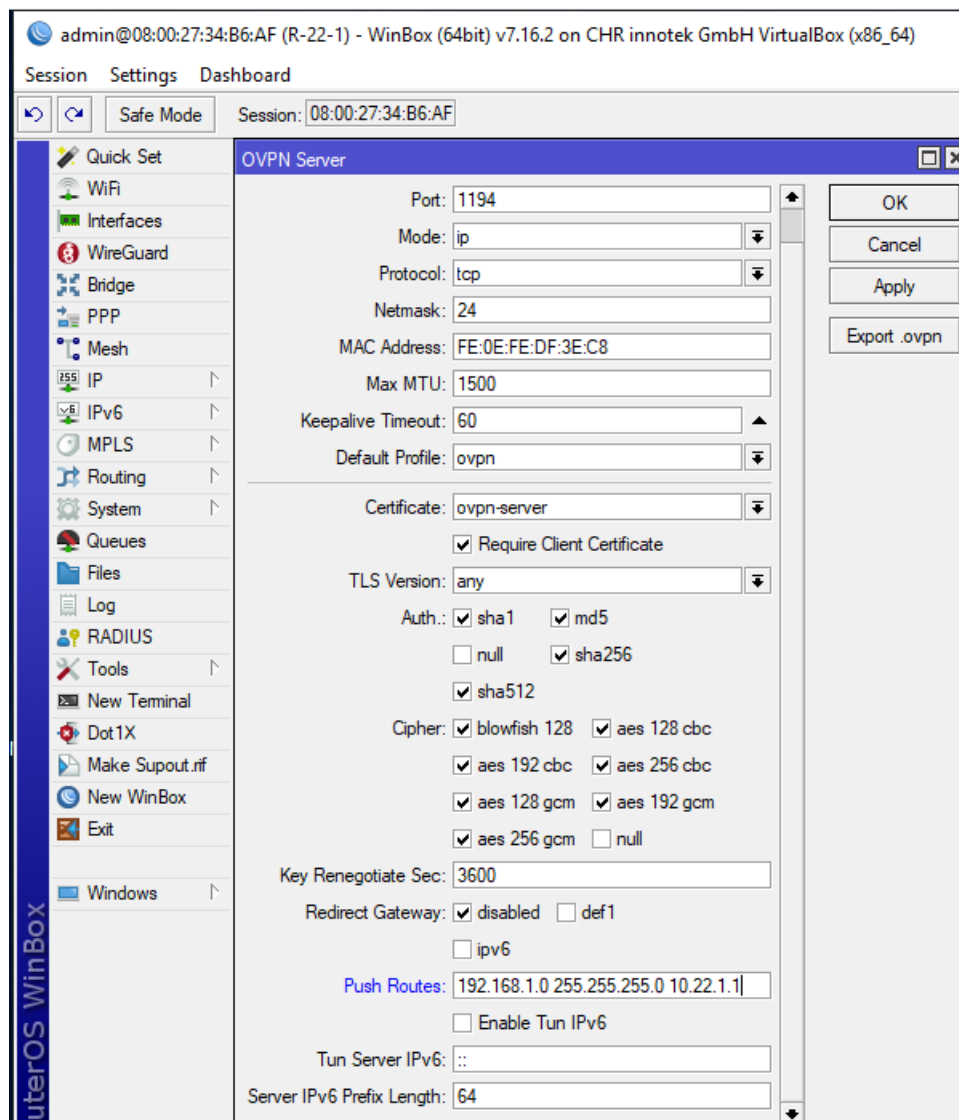


Рисунок 3.34 – Налаштування OpenVPN сервера

Щоб клієнти могли підключатися до OpenVPN сервера, потрібно дозволити трафік через порт 1194, що використовується для OpenVPN. Для цього додається відповідне правило у фаєрвол, рис.3.35.

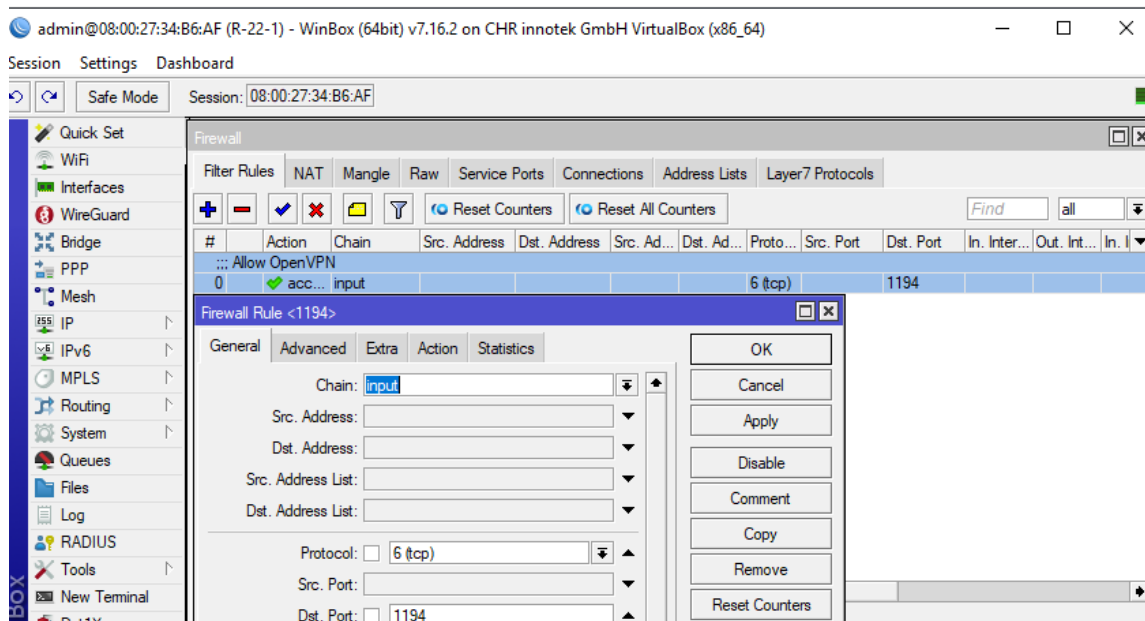


Рисунок 3.35 – Створення правила фаєрволу для трафіку OpenVPN

Налаштування клієнта VPN на маршрутизаторі Mikrotik

Для налаштування клієнта перш за все необхідно експортувати кореневий сертифікат (ca), сертифікат клієнта та його закритий ключ (client-branch-a). Найбільш зручно використовувати для цього формат PKCS12. При чому при експортуванні сертифікату клієнта доцільно вказати пароль, рис.3.36-3.37.

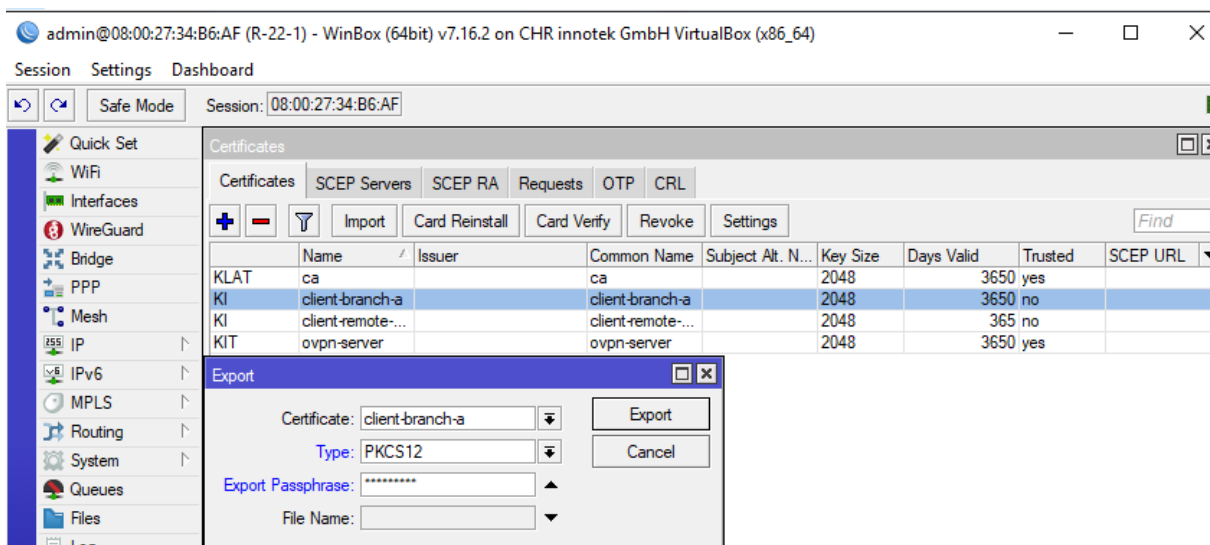


Рисунок 3.36 – Експортування кореневого сертифікату

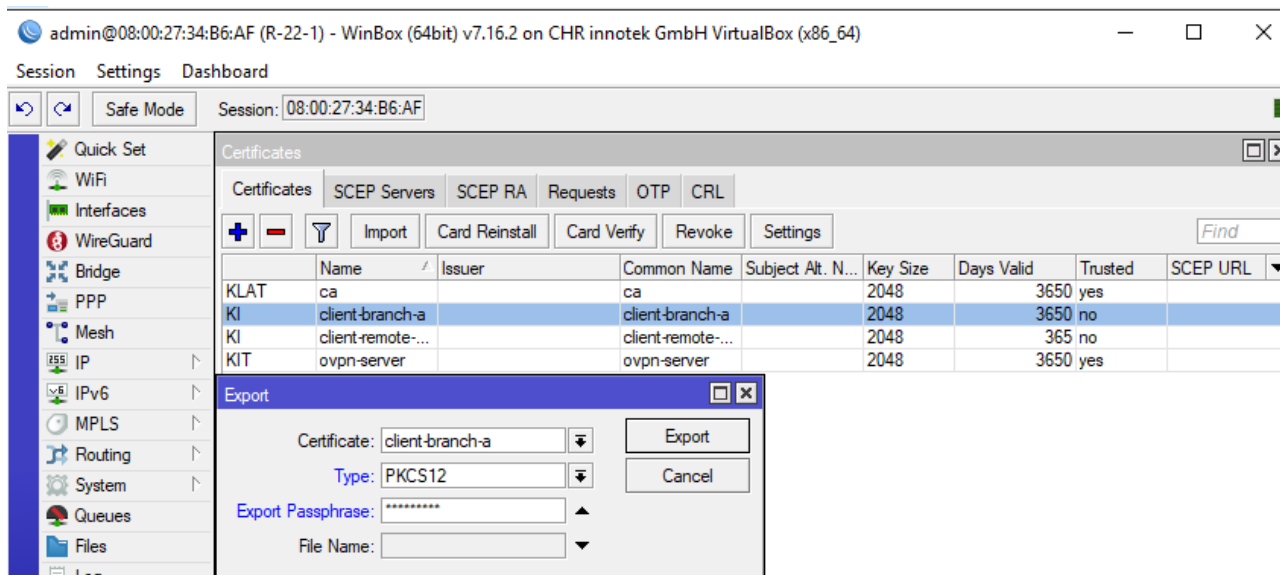


Рисунок 3.37 – Експортування сертифікату клієнта

Далі експортовані сертифікати необхідно перемістити з Mikrotik на комп'ютер і передати будь-яким захищеним каналом до маршрутизатора R-A-1, рис.3.38.

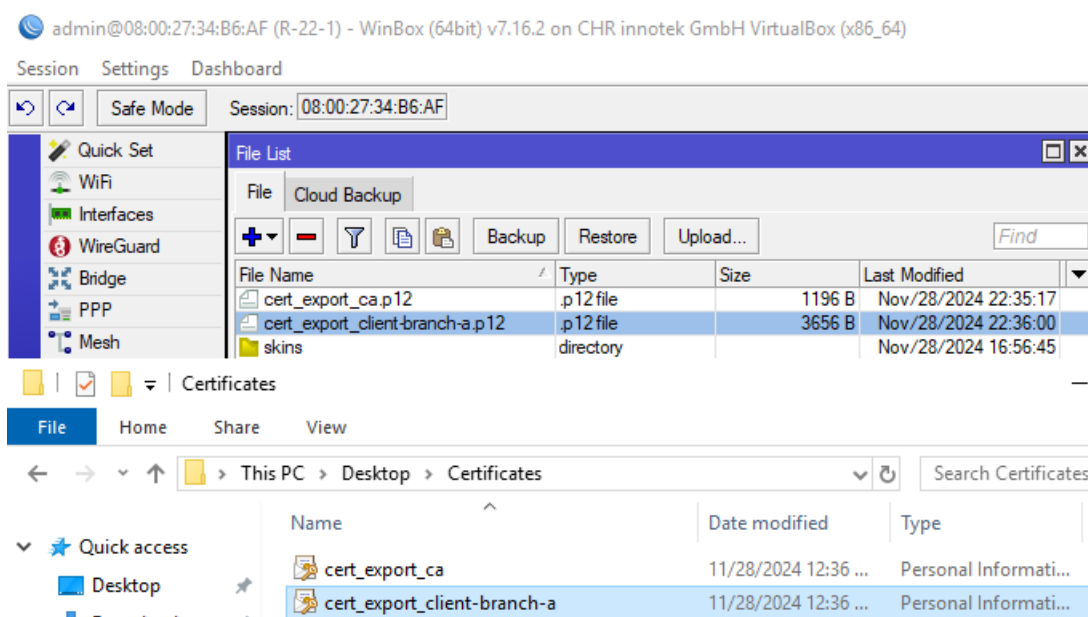


Рисунок 3.38 – Копіювання експортованих сертифікатів на комп'ютер

На клієнтський маршрутизатор, тобто R-A-1, потрібно перенести дані сертифікати та виконати їх імпортування. Слід не забувати, що при імпортуванні клієнтського сертифікату слід ввести пароль, рис.3.39-3.41.

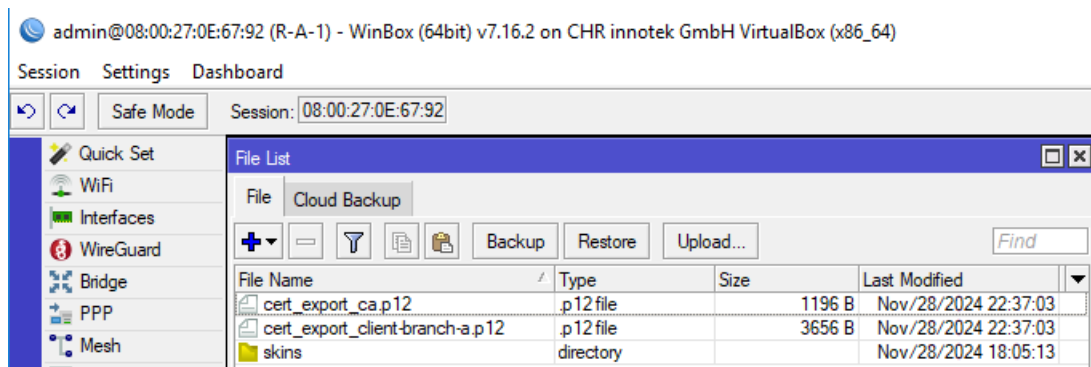


Рисунок 3.39 – Копіювання файлів сертифікатів на R-A-1

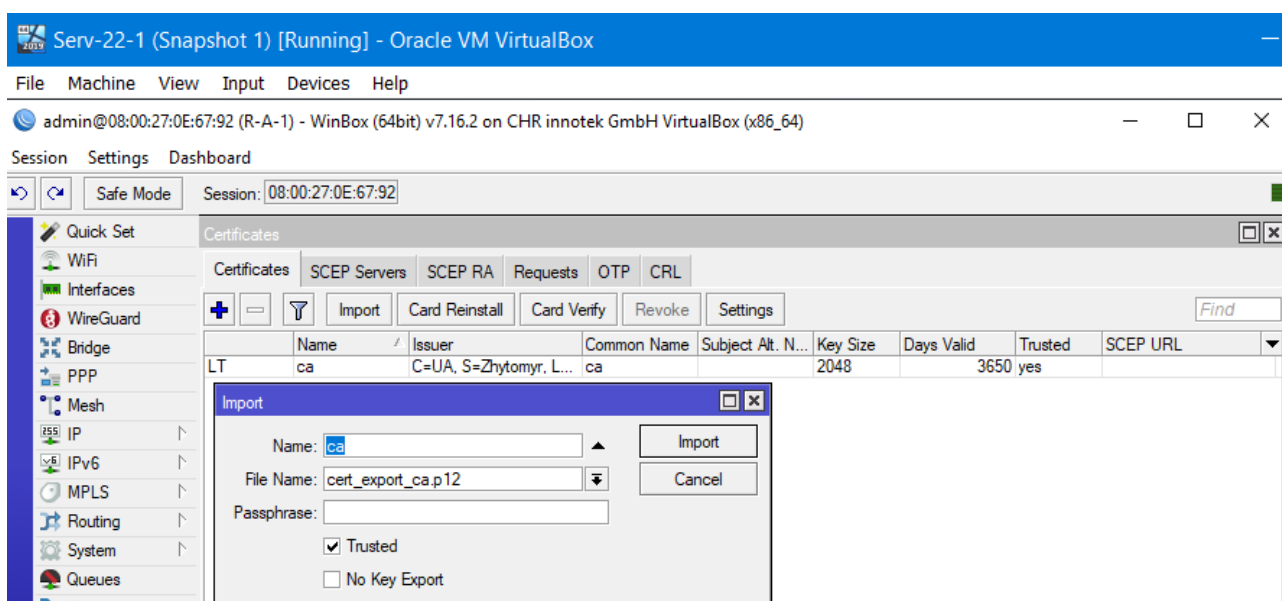


Рисунок 3.40 – Імпортування кореневого сертифікату на R-A-1

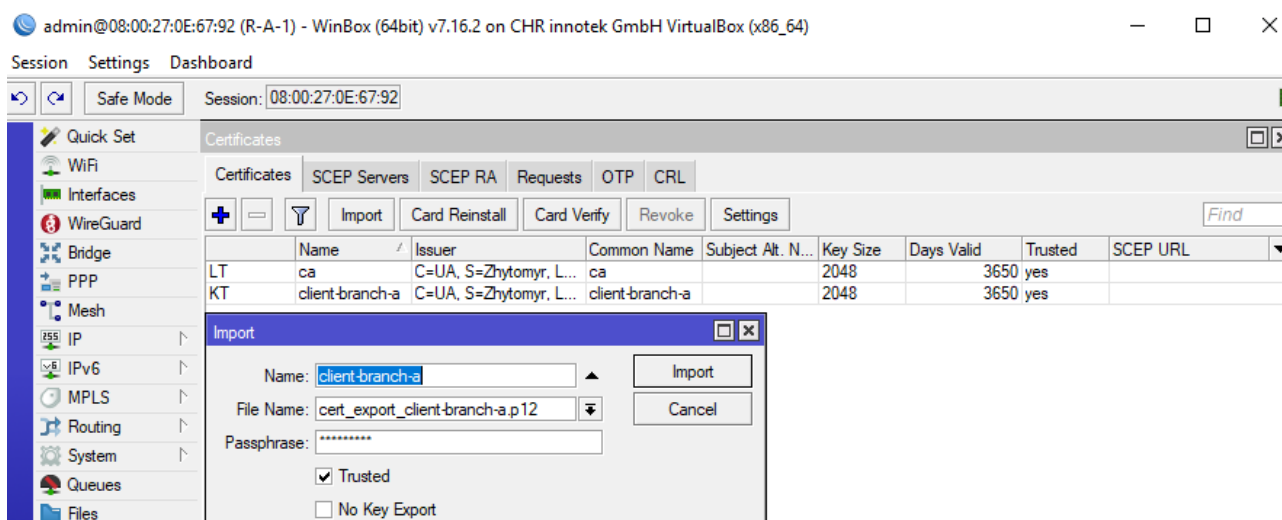


Рисунок 3.41 – Імпортування клієнтського сертифікату на R-A-1

І тепер створюємо новий інтерфейс типу «OpenVPN Client». Тут вказуємо публічну адресу R-22-1, ім'я користувача та його пароль, сертифікат клієнту, алгоритм хешування та шифрування, рис.3.42.

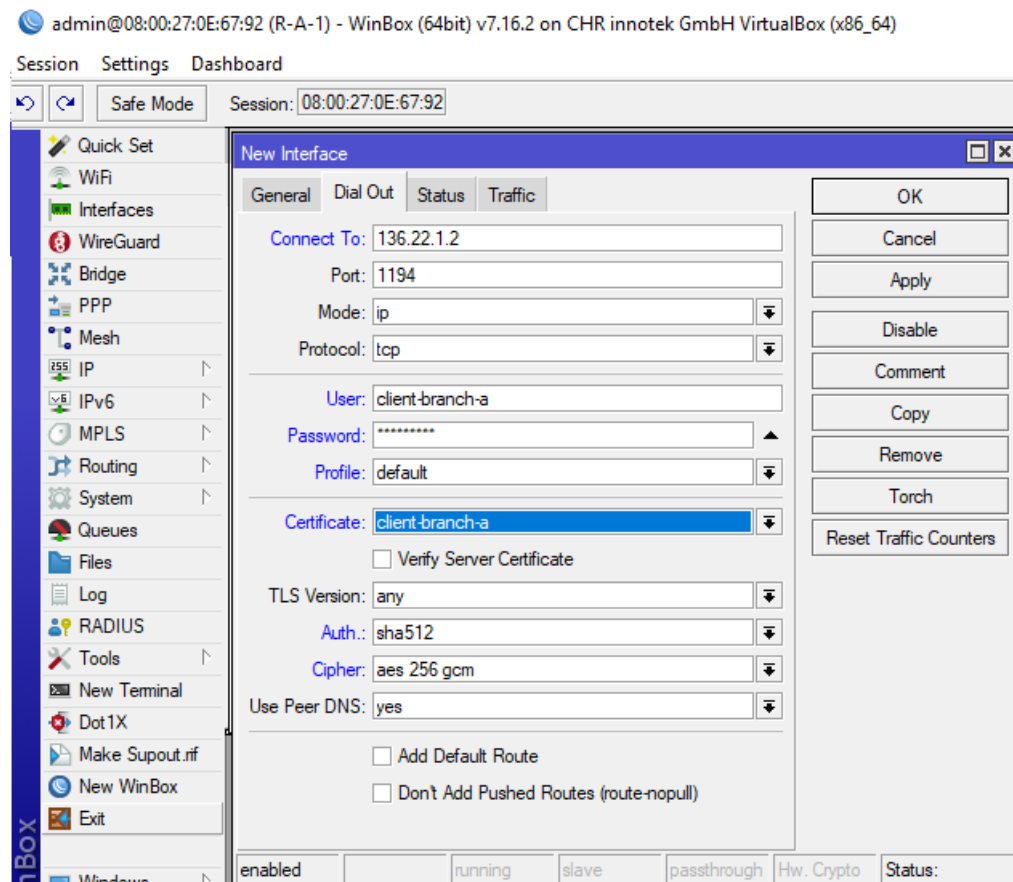


Рисунок 3.42 – Налаштування клієнтського інтерфейсу OpenVPN

Коли клієнт підключається до OpenVPN-сервера, автоматично створюється відповідний динамічний інтерфейс (D). Основна проблема динамічного інтерфейсу полягає в тому, що його існування залежить від стану з'єднання клієнта. Якщо клієнт відключиться, інтерфейс видаляється, і маршрути, прив'язані до нього, також припиняють працювати. Це унеможливує стабільну маршрутизацію між мережами. Для вирішення цієї проблеми необхідно створити постійний інтерфейс для конкретного клієнта і після чого створити статичний маршрут, рис.3.43-3.44.

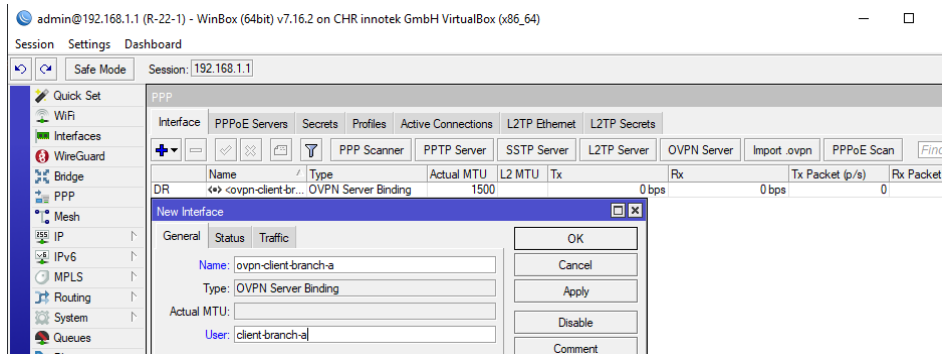


Рисунок 3.43 – Створення постійного інтерфейсу типу OVPN Server Binding

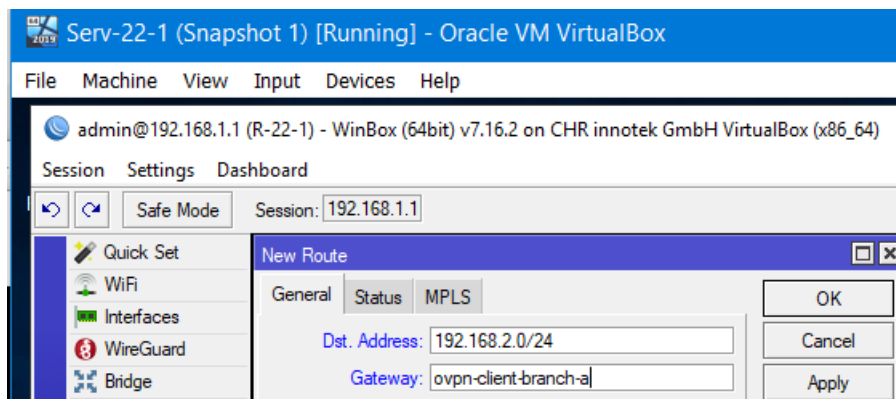


Рисунок 3.44 – Створення статичного маршруту до локальної мережі філіалу

Якщо все було виконано правильно, то пінги до пристроїв локальної мережі філії А від пристроїв головного офісу проходять успішно, рис.3.45.

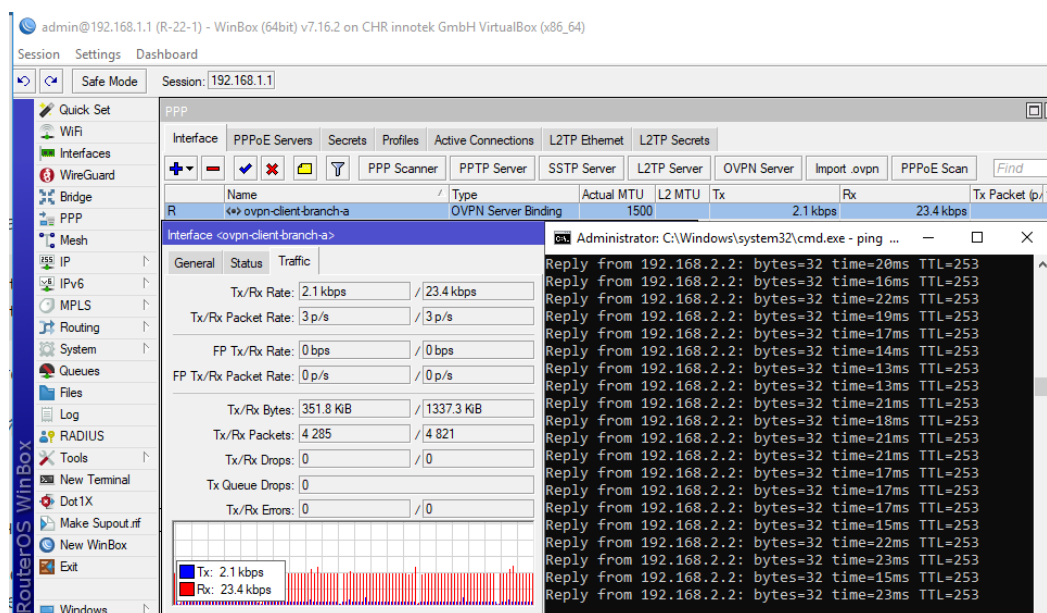


Рисунок 3.45 – Перевірка роботи OpenVPN та зв'язку з пристроєм віддаленої філії А зі станції Serv-22-1

Налаштування клієнта VPN на комп'ютері віддаленого працівника

Для налаштування клієнтів OpenVPN доцільно виконати експортування файлу конфігурацій в форматі .ovpn. Тут зазначається публічна адреса R-22-1, кореневий сертифікат, сертифікат клієнта та його закритий ключ і натискається кнопка Start, рис.3.46. Згенерований файл необхідно передати на комп'ютер клієнта будь-яким зручним та захищеним каналом зв'язку.

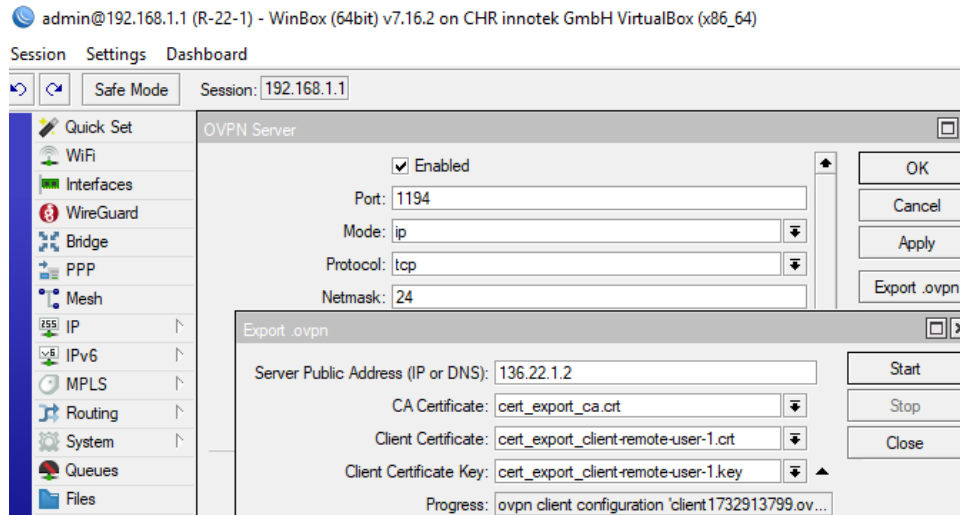


Рисунок 3.46 – Експортування файлу конфігурації .ovpn

Переходимо до комп'ютера віддаленого користувача WS-Home-1. В файлі конфігурацій необхідно прописати маршрут до локальної мережі організації, аби віддалений користувач міг отримувати доступ до внутрішніх ресурсів, рис.3.47.

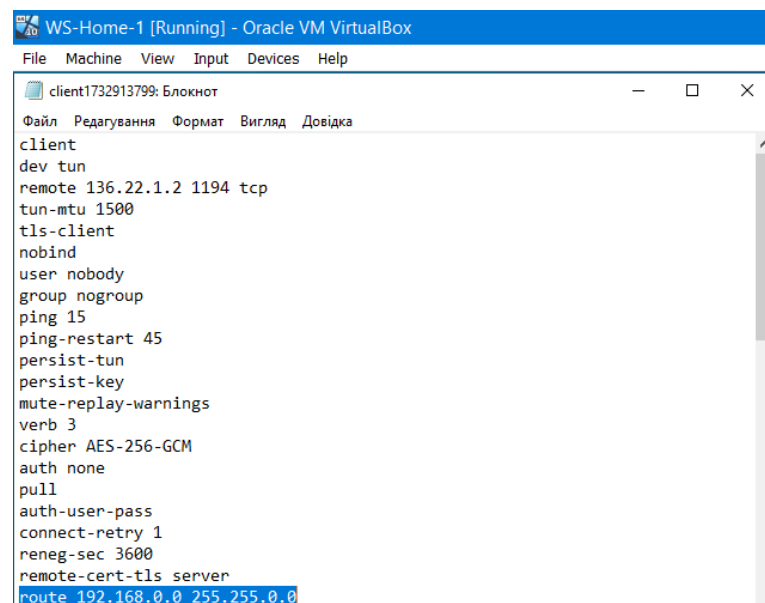


Рисунок 3.47 – Додання маршруту до локальної мережі організації

В заздалегідь встановленій програмі «OpenVPN Connect» необхідно обрати даний файл конфігурацій в форматі .ovpn, ввести ім'я користувача та пароль від нього і пароль від файлу сертифіката клієнта, рис.3.48.

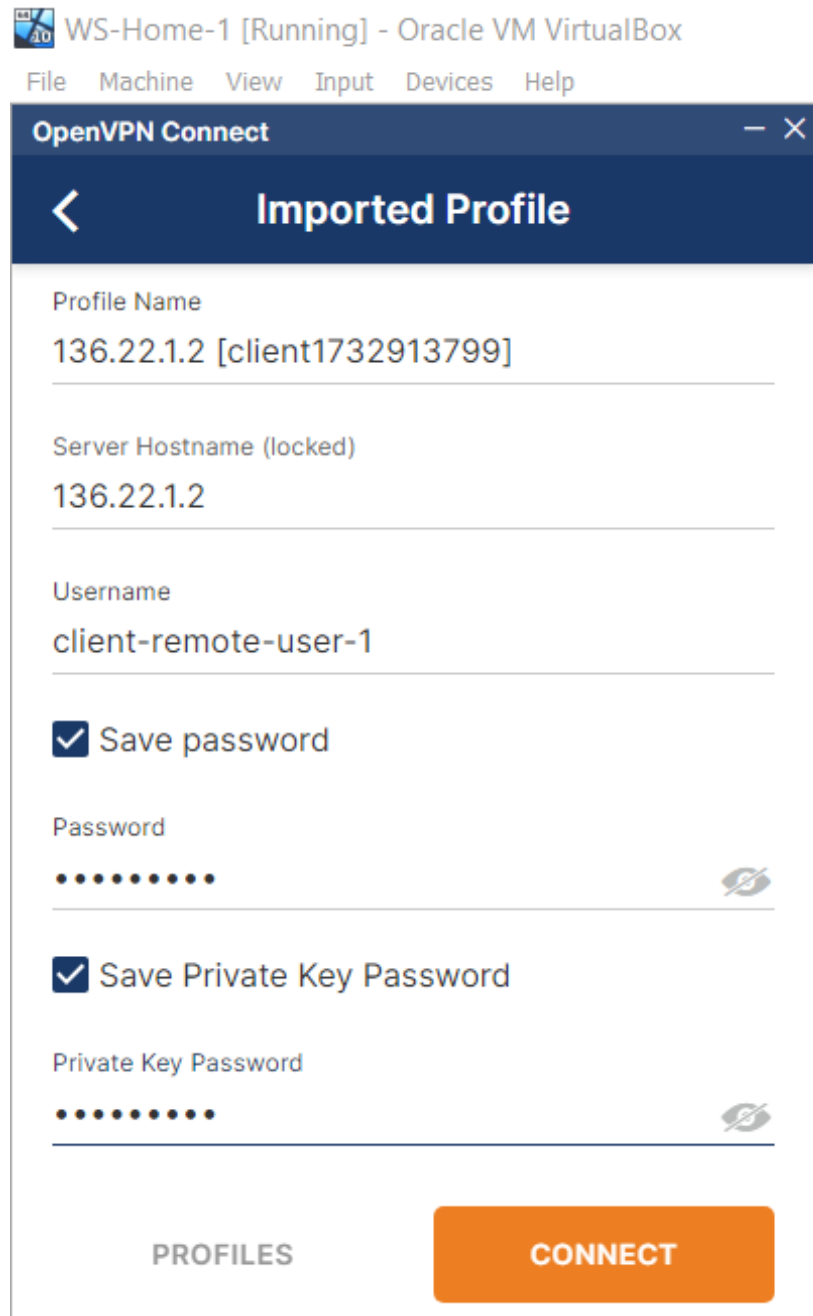


Рисунок 3.48 – Підключення до сервера OpenVPN

І після цього перевіримо доступність внутрішніх ресурсів організації для віддаленого користувача виконавши відповідні пінги до пристроїв локальної мережі за їх доменними іменами, рис.3.49.

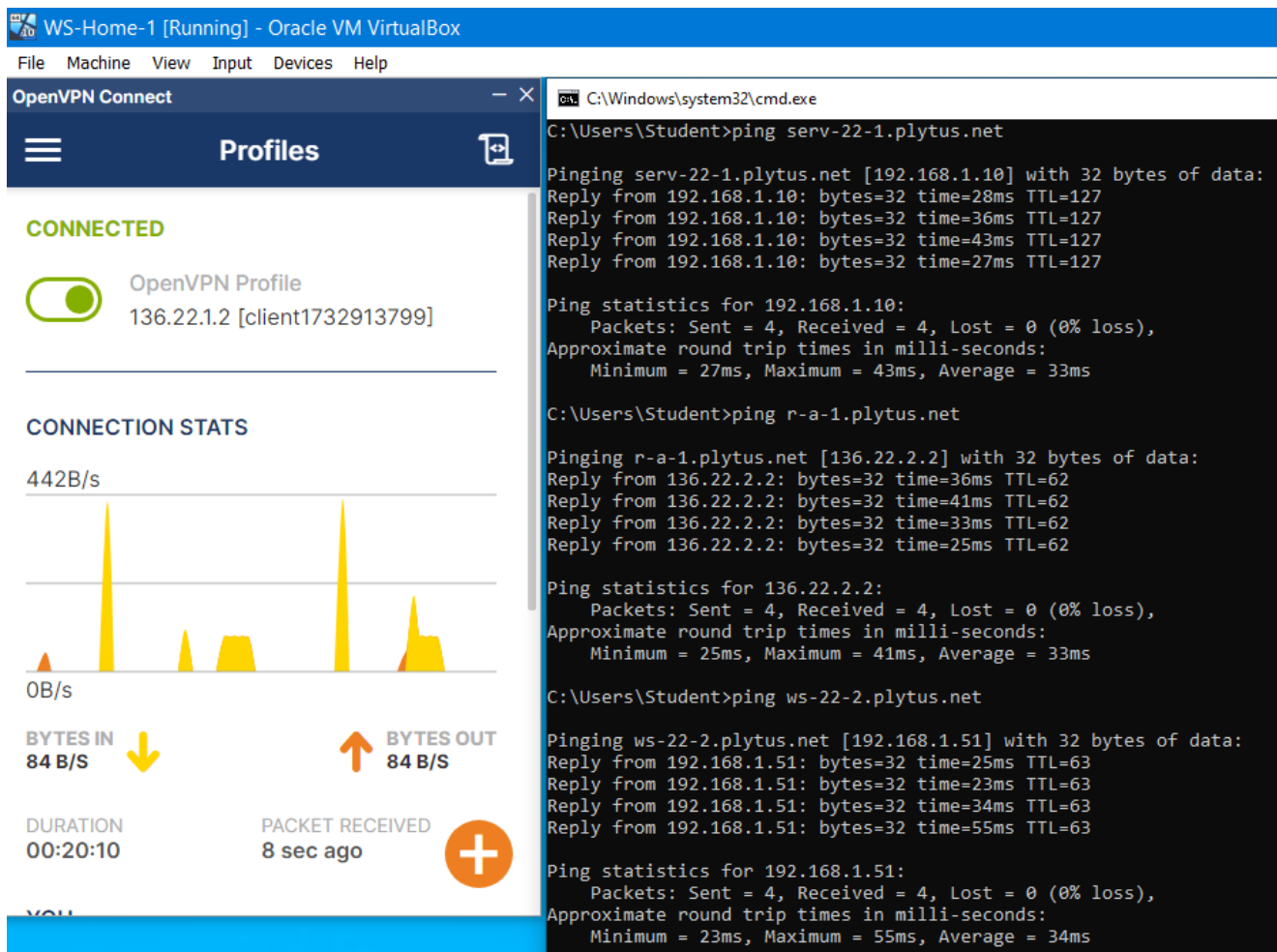


Рисунок 3.49 – Перевірка зв'язку з пристроями локальної мережі організації

На рис.3.50 наведено створені інтерфейси VPN до клієнтів та таблиця маршрутизації R-22-1.

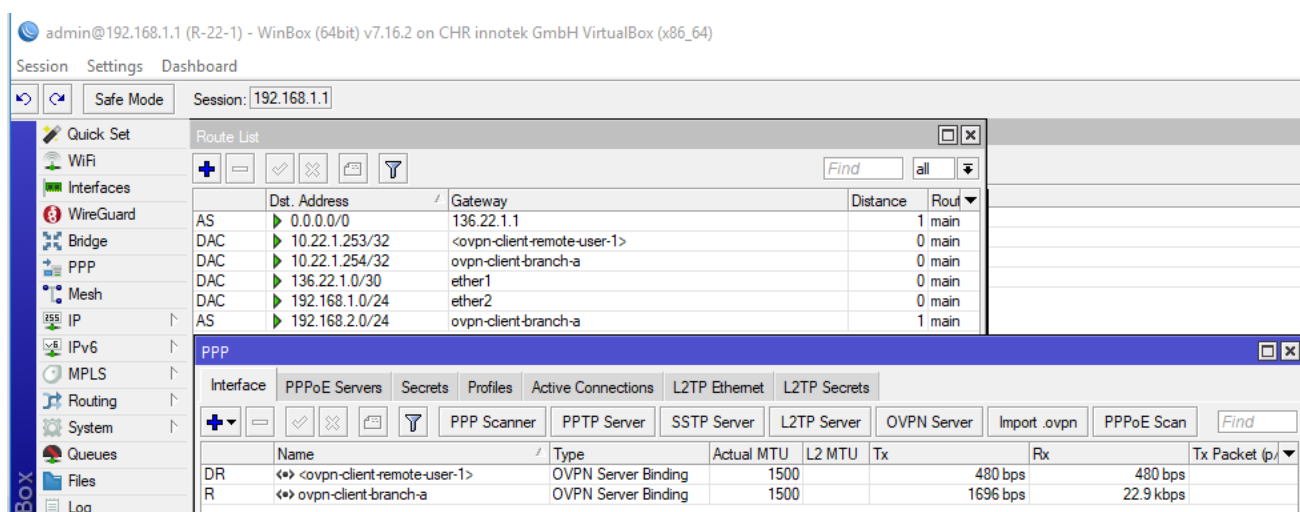


Рисунок 3.50 – Створені інтерфейси VPN до клієнтів та таблиця маршрутизації

Для наочної перевірки роботи протоколу виконаємо перехоплення пакетів із зовнішнього інтерфейсу маршрутизатора R-22-1 і відфільтруємо пакети за адресами відправлення та призначення, рис.3.51. Як видно з рисунку переважна більшість пакетів відноситься до протоколу OpenVPN в яких інформація передається у зашифрованому вигляді. Таким чином перевірка роботи протоколу OpenVPN була виконана успішно.

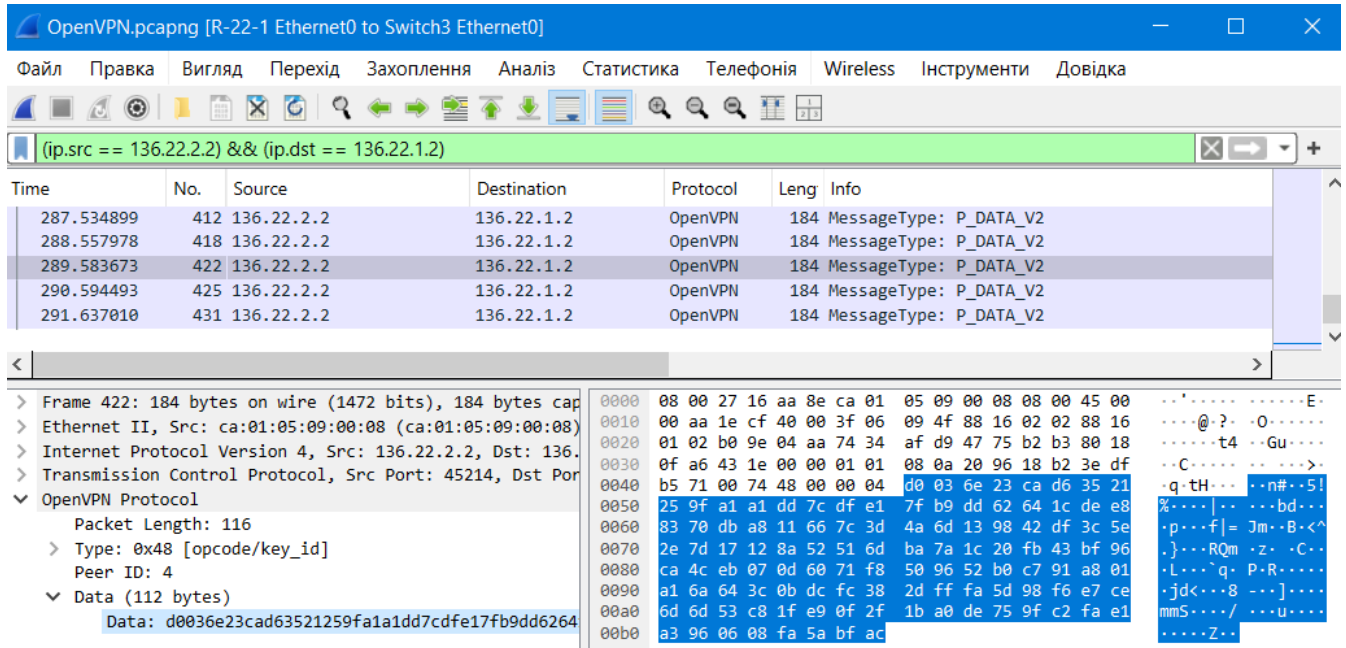


Рисунок 3.51 – Перехоплені пакети OpenVPN

3.3 Налаштування додаткових функцій захисту та їх перевірка

За замовчуванням на маршрутизаторах Mikrotik вже налаштовані базові правила фаєрвол, які забезпечують початковий рівень безпеки [19]. Вони включають дозвіл на вихідний трафік із локальної мережі в Інтернет і блокування вхідного трафіку з Інтернету, якщо він не підпадає під налаштоване правило NAT, наприклад, перенаправлення портів. Також заблоковані з'єднання, які не є частиною вже існуючого з'єднання, що допомагає захистити мережу від несанкціонованих доступів ззовні, рис.3.52. Однак за потреби користувач може легко додати свої правила до вже існуючих.

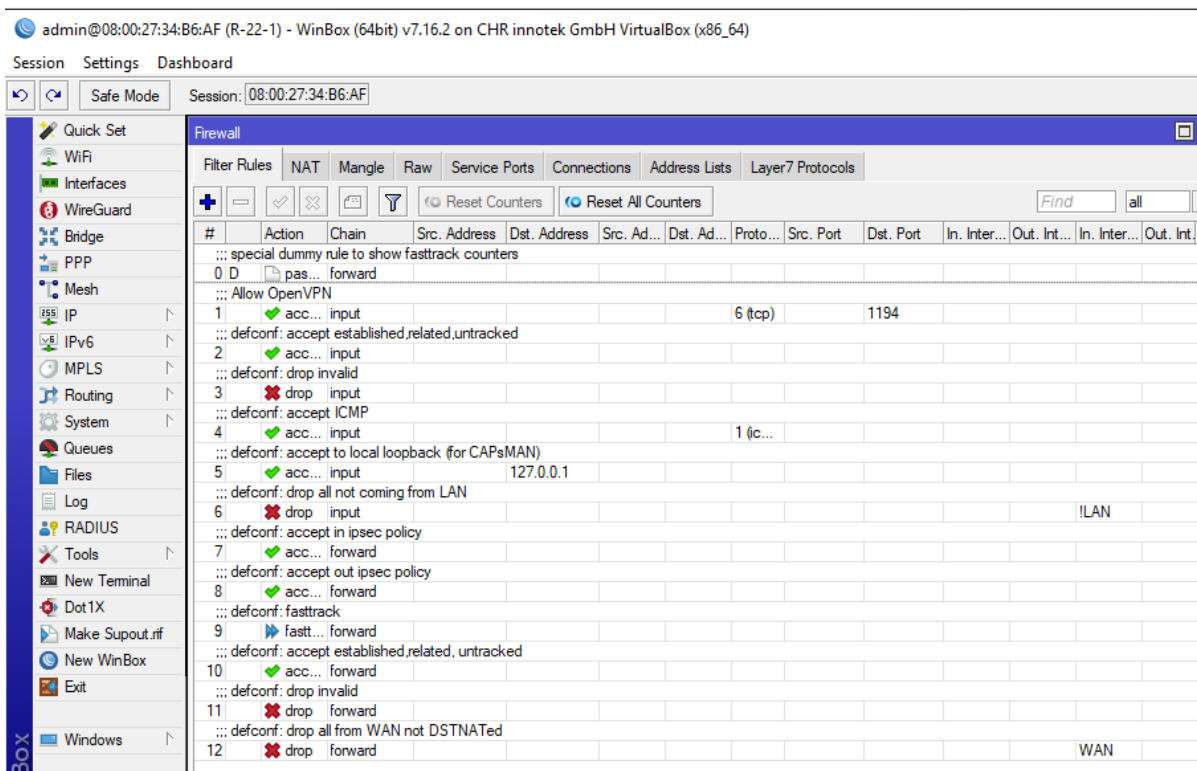


Рисунок 3.52 – Налаштовані правила Firewall за замовчуванням

RADIUS (Remote Authentication Dial-In User Service) — це мережевий протокол, який використовується для централізованої аутентифікації, авторизації та обліку доступу користувачів до мережевих ресурсів, тому виконаємо розгортання серверу RADIUS на комп'ютері Serv-22-1 з використання вбудованих можливостей Windows Server, рис.3.53-3.55.

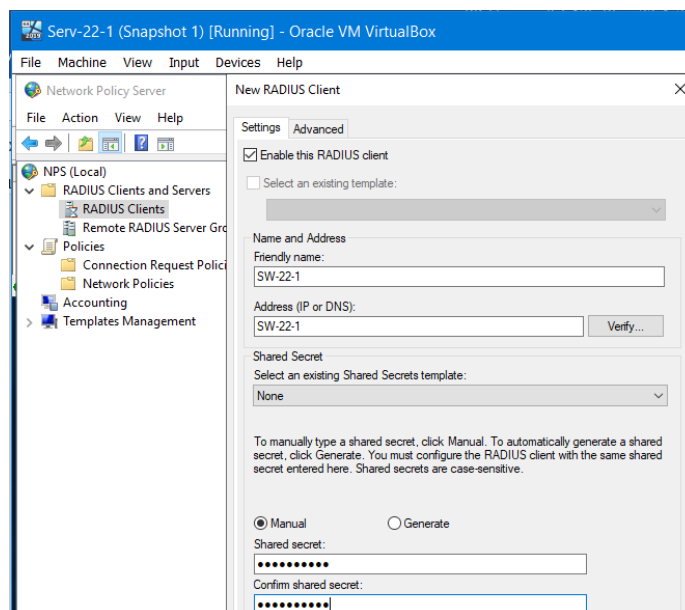


Рисунок 3.53 – Додання клієнта RADIUS

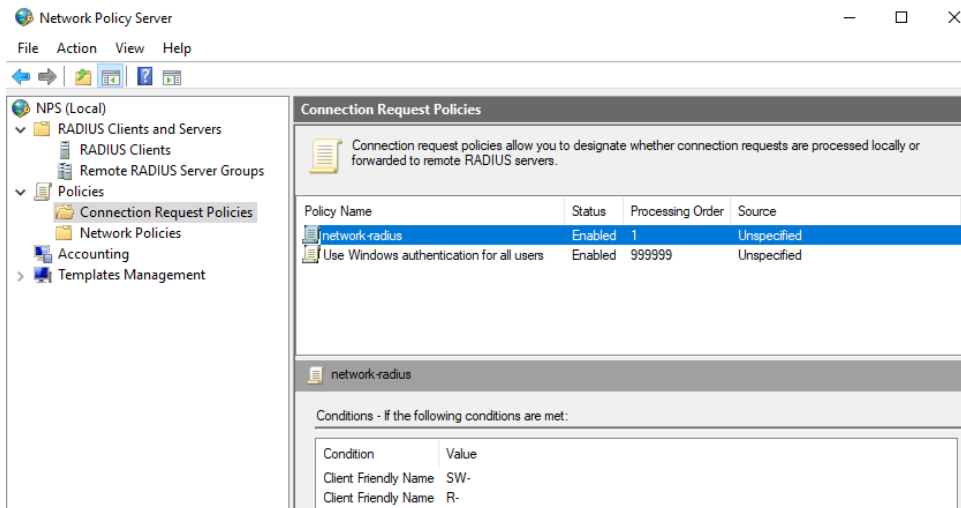


Рисунок 3.54 – Налаштування політик підключення до серверу RADIUS

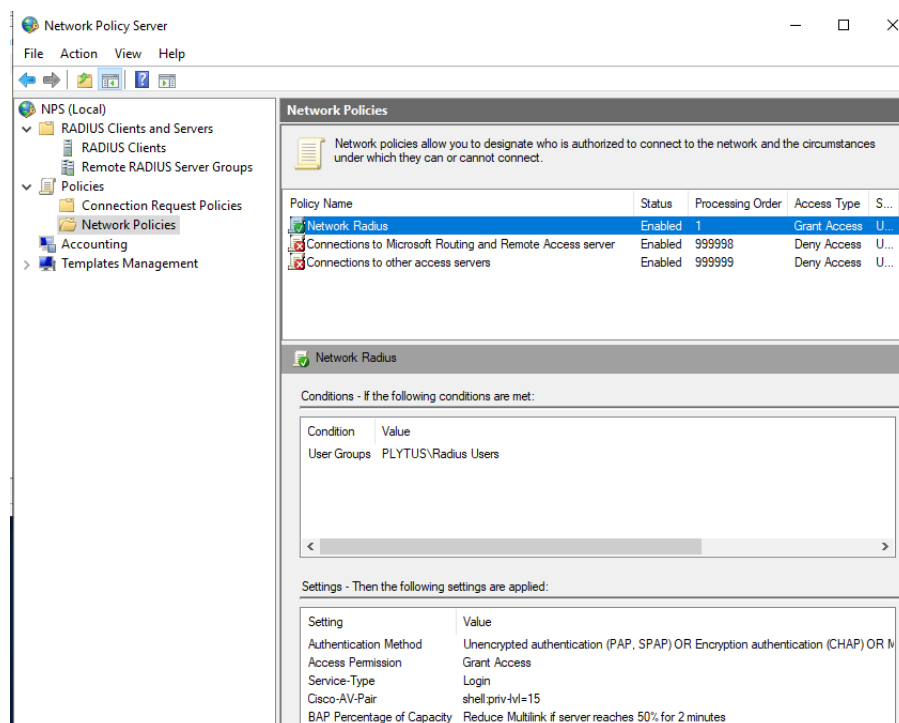


Рисунок 3.55 – Налаштування мережевих політик

Тепер налаштовуємо аутентифікацію з використанням серверу RADIUS на комутаторах. Для цього спершу активуємо режим AAA (Authentication, Authorization, Accounting) за допомогою команди `aaa new-model`, після чого створюється локальний обліковий запис адміністратора командою `username`. Для доступу до привілейованого режиму задається пароль через команду `enable secret`. Далі налаштовується сервер RADIUS командою `radius server`, з визначенням його

IP-адреси, портів аутентифікації (1812) та обліку (1813), а також задається секретний ключ (який було визначено на сервері RADIUS) через key win-radius. Командами `aaa authentication login default group Radius local` і `aaa authorization exec default group Radius local if-authenticated` встановлюється порядок аутентифікації та авторизації: спершу через сервер RADIUS, а якщо він недоступний — через локальний обліковий запис. Для лінії консолі за допомогою `line cons 0` задається використання даної схеми аутентифікації командою `login authentication default`, рис.3.56.

```
SW-22-1(config)#aaa new-model
SW-22-1(config)#username Admin privilege 15 secret pass-admin
SW-22-1(config)#enable secret enable-pass
SW-22-1(config)#radius server Serv-22-1
SW-22-1(config-radius-server)#address ipv4 Serv-22-1 auth-port 1812 acct-port 1813
SW-22-1(config-radius-server)#key win-radius
SW-22-1(config-radius-server)#exit
SW-22-1(config)#aaa authentication login default group Radius local
SW-22-1(config)#aaa authorization exec default group Radius local if-authenticated
SW-22-1(config)#line cons 0
SW-22-1(config-line)#login authentication default
SW-22-1(config-line)#line vty 0 4
```

Рисунок 3.56 – Налаштування аутентифікації через сервер RADIUS

Далі налаштовуємо маршрутизатор Mikrotik, тобто R-22-1, на роль клієнта RADIUS, рис.3.57-3.58 [20].

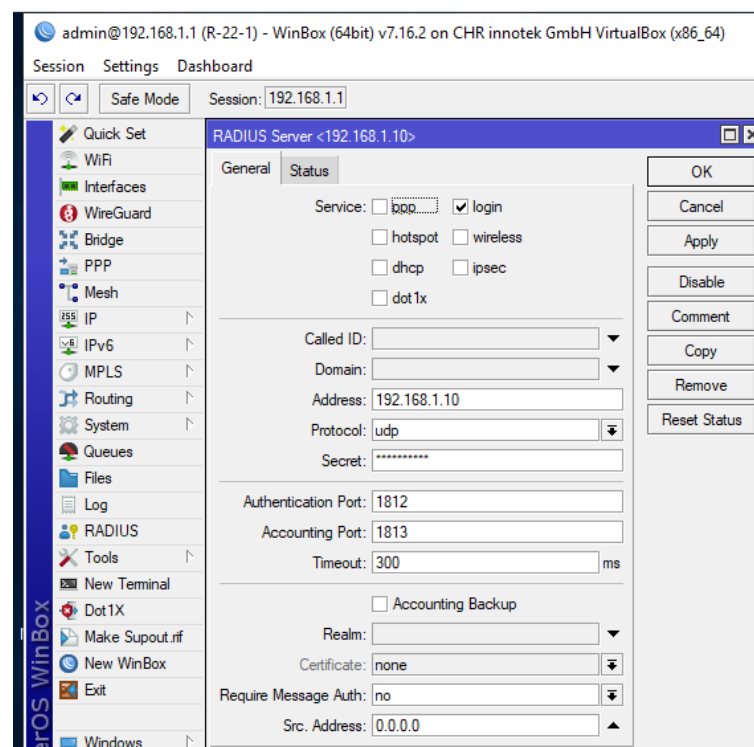


Рисунок 3.57 – Налаштування роботи клієнта RADIUS на Mikrotik

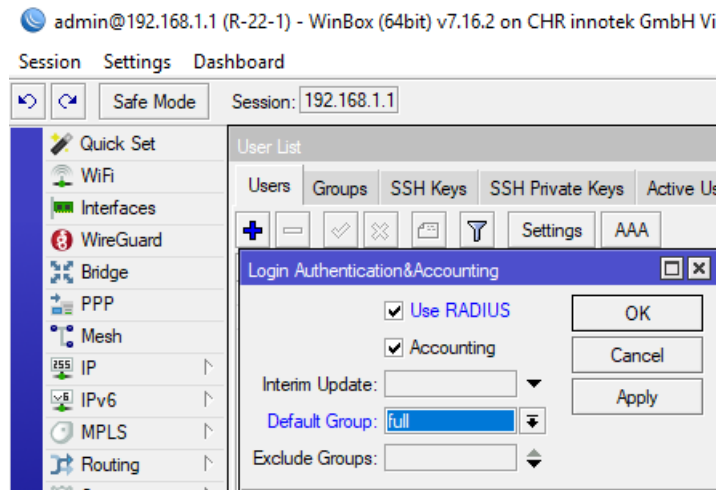


Рисунок 3.58 – Налаштування роботи клієнта RADIUS на Mikrotik

SSH (Secure Shell) — це протокол для безпечного віддаленого доступу до комп'ютерних систем через зашифроване з'єднання. Він забезпечує захищений канал для виконання команд, передачі файлів та адміністрування мережевих пристроїв. Тому на всіх комутаторах мережі здійснимо налаштування роботи даного протоколу, рис.3.59. Команда `crypto key generate rsa modulus 1024` генерує пару RSA-ключі. Далі задається використання другої версії протоколу SSH через команду `ip ssh version 2`, що підвищує рівень безпеки. Налаштовується час очікування для сеансів SSH за допомогою `ip ssh time-out 30`. Для ліній віддаленого доступу VTY командою `line vty 0 4` активується підтримка лише SSH-з'єднань через `transport input ssh`, а також прив'язується попередньо налаштована схема аутентифікації командою `login authentication default`.

```

SW-22-1 - PuTTY
SW-22-1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: SW-22-1.plytus.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

SW-22-1(config)#ip ssh version 2
SW-22-1(config)#ip ssh time-out 30
SW-22-1(config)#line vty 0 4
SW-22-1(config-line)#transport input ssh
SW-22-1(config-line)#login authentication default

```

Рисунок 3.59 – Налаштування SSH на комутаторі

Syslog використовується для централізованого збирання, зберігання та аналізу логів з різних пристроїв і систем у мережі. Тому на всіх комутаторах виконаємо налагодження передачі повідомлень до сервера Syslog на, рис.3.60.

```
SW-22-1(config)#service timestamps log datetime
SW-22-1(config)#logging Serv-22-1
SW-22-1(config)#logging trap notifications
```

Рисунок 3.60 – Налаштування відправки подій до серверу Syslog на комутаторах

Те саме слід зробити і на пристроях Mikrotik. Спочатку тут слід зазначити адресу віддаленого сервера з відповідним портом, а далі вказати які типи сповіщень слід надсилати до сервера Syslog, рис.3.61-3.62.

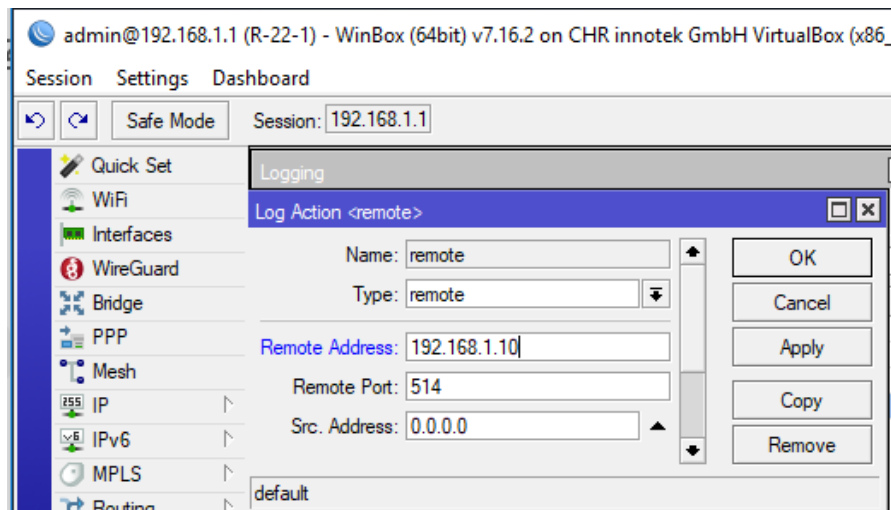


Рисунок 3.61 – Налаштування відправки подій до серверу Syslog на Mikrotik

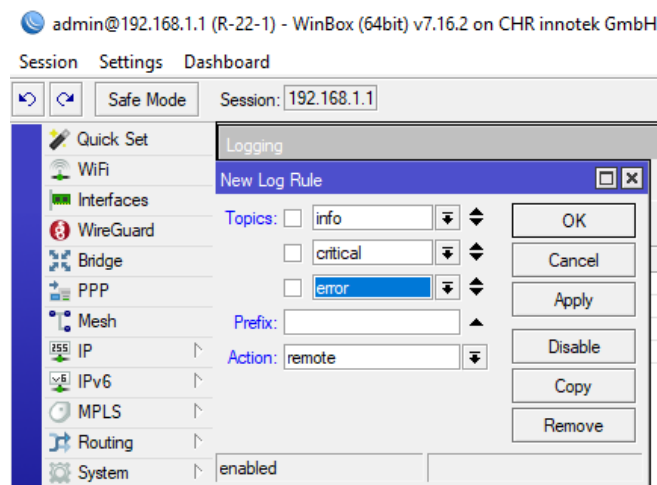


Рисунок 3.62 – Налаштування типів сповіщень для відправки до серверу Syslog

Тепер на самому сервері, тобто комп'ютері Serv-22-1, необхідно встановити і налагодити роботу Syslog, рис.3.63.

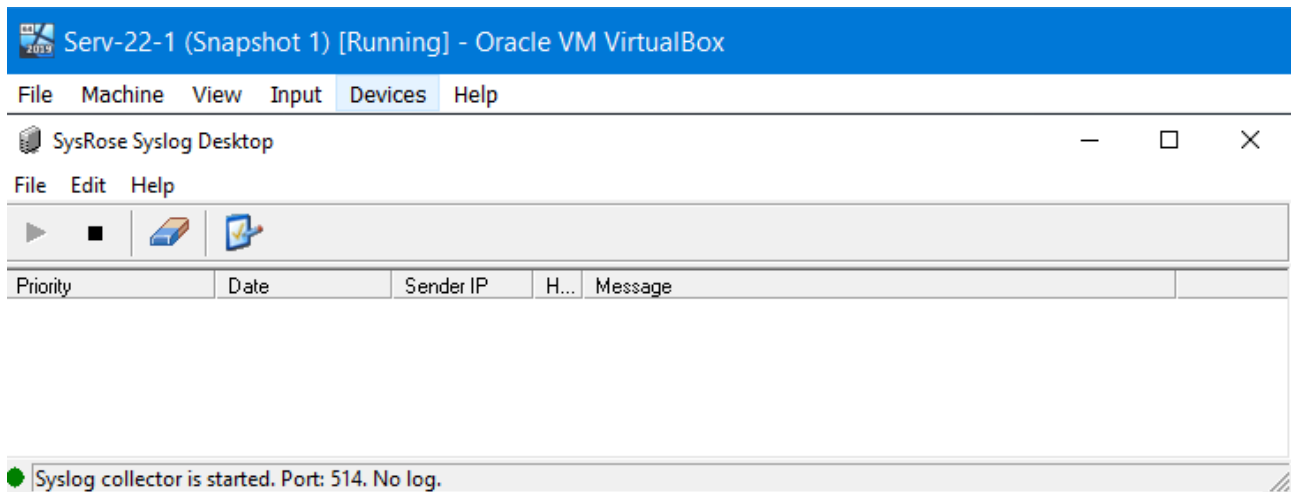


Рисунок 3.63 – Налагодження сервера Syslog

Лишається тепер тільки відімкнути незадіяні інтерфейси на комутаторах та призначити їм окрему VLAN 1001, рис.3.64. Командою `switchport mode access` обрані інтерфейси переводяться в режим доступу, а `switchport access vlan 1001` здійснює прив'язку цих інтерфейсів до VLAN 1001 задля їх ізолювання.

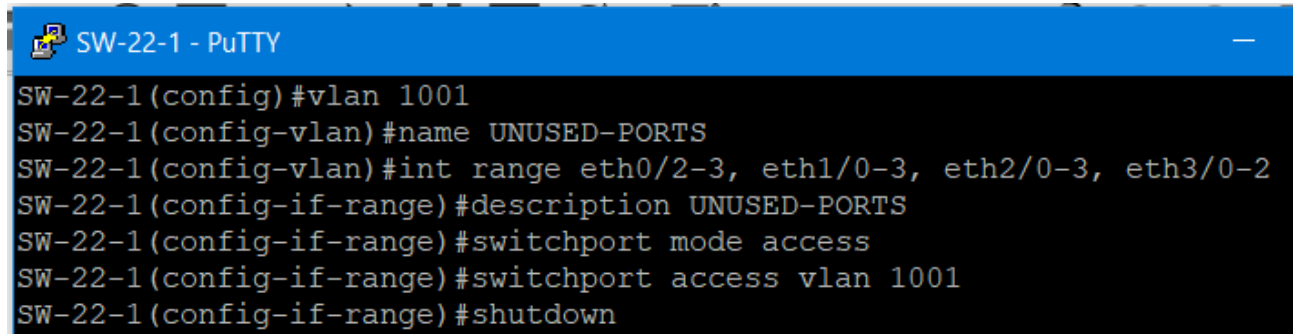


Рисунок 3.64 – Відключення незадіяних інтерфейсів та призначення їм окремої незадіяної VLAN

Тепер виконаємо перевірку використаних функцій. З Windows Server виконаємо віддалене підключення через SSH до комутатора SW-22-1 та відімкнемо один з інтерфейсів. Одразу після цього на Syslog сервері з'явилися відповідні сповіщення про відімкнення одного з інтерфейсів пристроїв, рис.3.65.

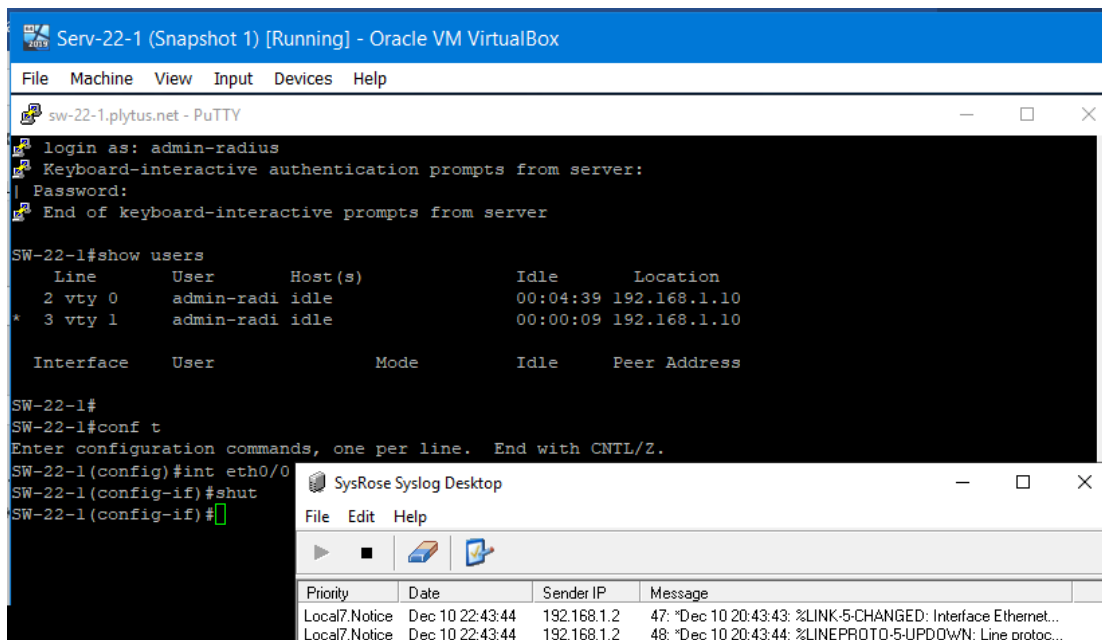


Рисунок 3.65 – Підключення через SSH до комутатора SW-22-1 та перегляд сповіщень на Syslog сервері

Можемо переглянути сповіщення, що стосуються RADIUS сервера та помітити подію входу до SW-22-1 з використанням користувача admin-radius, рис.3.66, що і було виконано на минулому рисунку.

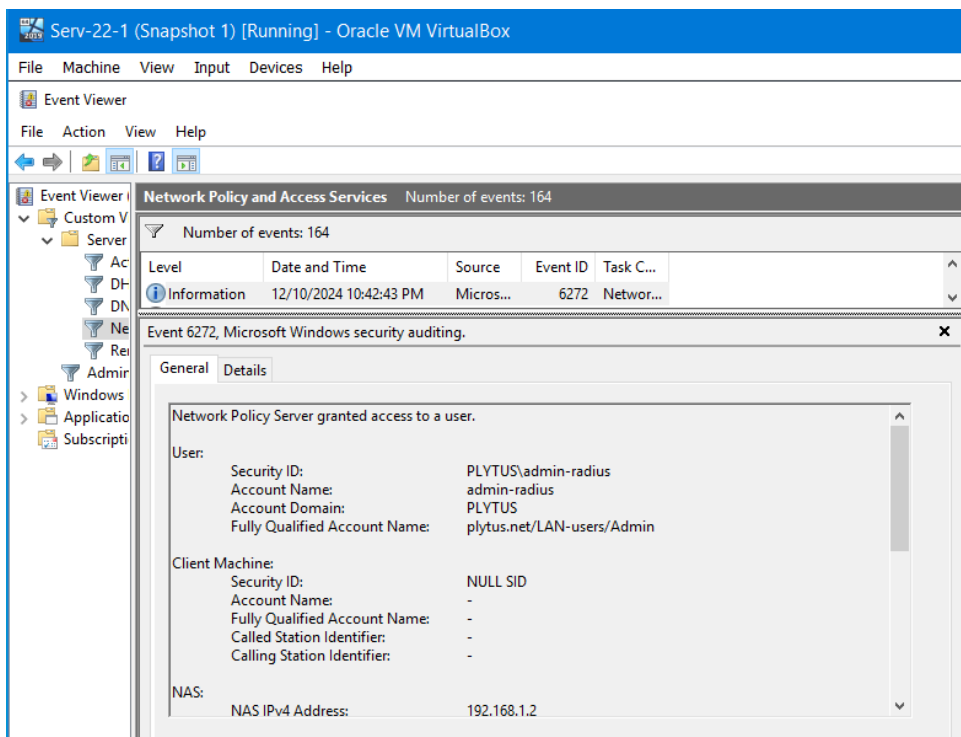


Рисунок 3.66 – Подія входу на SW-22-1 з використання облікового користувача RADIUS admin-radius

Так само облікові записи RADIUS можуть бути використані для підключення до маршрутизатора Mikrotik, рис.3.67.

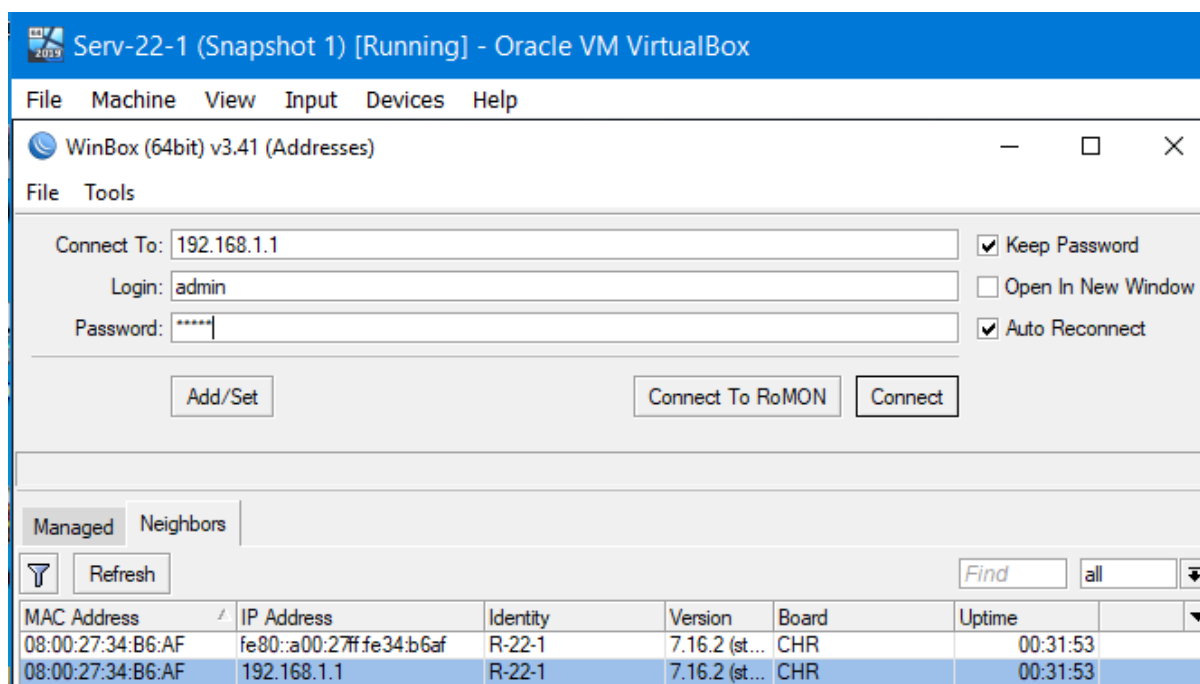


Рисунок 3.67 – Підключення до R-22-1 з використання облікового користувача RADIUS admin-radius

І як бачимо активним користувачем R-22-1 нині є admin-radius. Якщо повернемось до сервера Syslog, то побачимо нове сповіщення про щойно виконане підключення до Mikrotik через WinBox, рис.3.68.

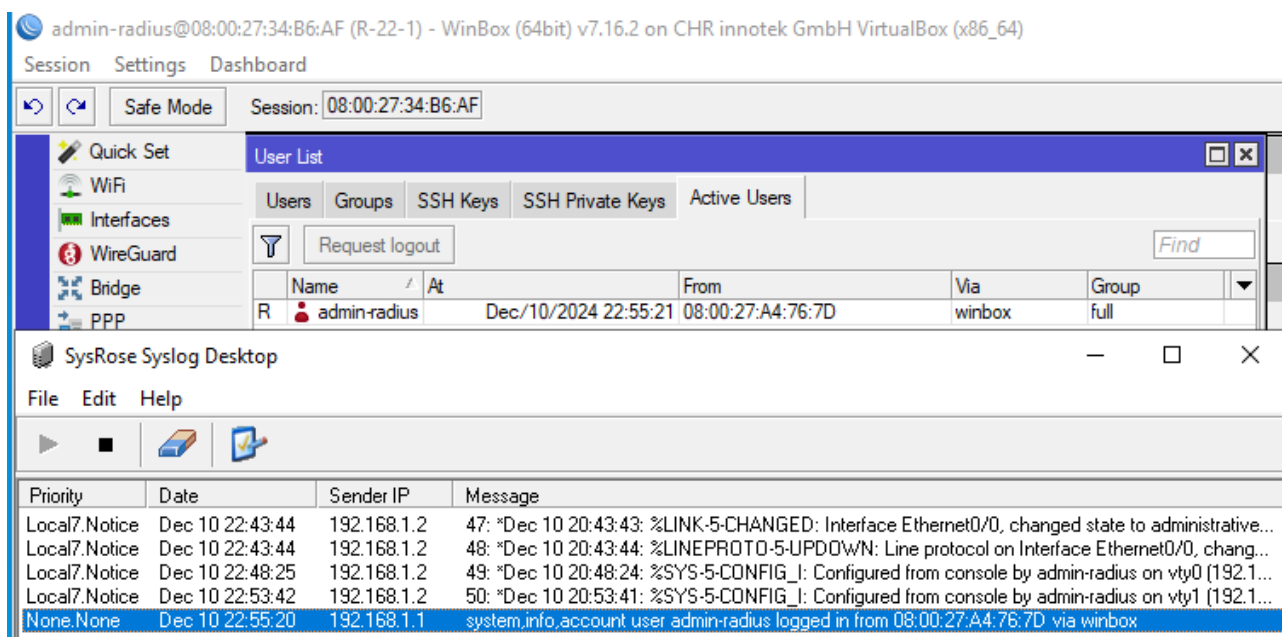


Рисунок 3.68 – Використання користувача admin-radius на Mikrotik

Висновки до третього розділу

В першому підрозділі було виконано базове налаштування мережі із використанням емулятора GNS3 та Oracle VirtualBox. Налаштування почалося з маршрутизаторів Mikrotik, на яких через термінал було задано базові параметри адресації та маршрутизації. Надалі для налаштування Mikrotik використано інструмент WinBox, через який було налагоджено NAT, DHCP та DNS. Аналогічно виконано базове налагодження комутаторів. На сервері Serv-22-1 розгорнуто Active Directory, DHCP, DNS і створено домен plytus.net. Кінцеві пристрої були налаштовані на динамічне отримання IP-адрес і підключені до домену. Перевірка зв'язку між вузлами та виходу в Інтернет підтвердила коректність виконаних налаштувань.

В наступному підрозділі виконано налаштування OpenVPN тунелів для підключення віддаленої філії та користувача. Процес налаштування включав включення роботи NTP-клієнтів створення сертифікатів за допомогою вбудованих засобів MikroTik, конфігурацію сервера OpenVPN із відповідними профілями PPP, пулом IP-адрес і правилами фаєрволу. Для клієнтів VPN виконано відповідне імпортування налаштувань зі серверу OpenVPN та перевірено доступність між усіма вузлами мережі, яка підтвердила коректність виконаних налаштувань. Додатково виконано перехоплення трафіку, яке наочно підтвердило правильність роботи OpenVPN та шифрування даних.

В останньому підрозділі виконано налаштування додаткових функцій захисту мережі, включаючи RADIUS для централізованої аутентифікації, налаштування протоколу, SSH для безпечного віддаленого доступу, Syslog для централізованого моніторингу подій і відключення незадіяних інтерфейсів на комутаторах. Роботу усіх функцій було перевірено.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було досліджено методи та технології захисту корпоративної мережі організації з використанням рішень Mikrotik і OpenVPN. Визначена мета обумовлювала виконання наступних завдань.

У першому розділі було розглянуто основні принципи та теоретичні аспекти використання технологій Mikrotik і OpenVPN для забезпечення захисту корпоративної мережі. Перш за все було визначено призначення корпоративних мереж та основні типи атак, що спрямовані на них. Виконано опис різних методів і технологій захисту корпоративних мереж. Визначено, що Mikrotik, завдяки своїй операційній системі RouterOS, забезпечує високу продуктивність, безпеку і гнучкість для побудови складних мереж. Визначено, що VPN є необхідною і вкрай актуальною технологією для забезпечення безпеки передачі даних через публічні мережі, а правильний вибір VPN-протоколу залежить від вимог щодо безпеки та продуктивності. Також були проаналізовані різні типи VPN, серед яких зазначено, що OpenVPN є найбільш оптимальним рішенням для використання корпоративних мереж завдяки своїй високій безпеці, гнучкості налаштувань і сумісності з різними платформами.

У другому розділі було розглянуто ключові принципи створення корпоративної мережі, що включають вибір трирівневої архітектури, яка забезпечує масштабованість, продуктивність і безпеку. Розроблено схему адресації, що дозволяє гнучко розподіляти IP-адреси та враховувати майбутнє масштабування. Також були наведено опис і призначення основних технологій захисту мережі, що будуть використані у проєкті мережі, зокрема OpenVPN, фаєрвол, Syslog, RADIUS і SSH. Остання частина розділу присвячена вибору обладнання для мережі, що відповідає вимогам безпеки, надійності та продуктивності, що дозволить організації ефективно функціонувати в умовах сучасних загроз.

У третьому розділі було виконано практичне налаштування мережі з використанням емулятора GNS3 та гіпервізора Oracle VirtualBox. Базове налаштування мережі було здійснено на маршрутизаторах Mikrotik, з використанням WinBox для налаштування NAT, DHCP і DNS. На сервері Serv-22-1 розгорнуто Active Directory, DHCP та DNS, а також створено домен. Далі було налаштовано OpenVPN для підключення віддалених філій і користувачів. Створено відповідні сертифікати, виконано їх експортування на клієнтські пристрої VPN і перевірено працездатність мережі. Також налаштовано додаткові функції захисту, такі як RADIUS, SSH та Syslog для централізованого моніторингу та аутентифікації. Перевірка налаштувань показала їх правильність і надійність, що забезпечило безпечне та стабільне функціонування корпоративної мережі.

Результатом виконання даної кваліфікаційної роботи є створення безпечної та ефективною корпоративної мережі на базі рішень Mikrotik і OpenVPN, що відповідає сучасним вимогам безпеки та продуктивності. Тестування роботи мережі довело працездатність та ефективність обраних рішень та технологій безпеки в межах корпоративної мережі організації. Всі поставлені цілі та завдання було виконано в повному обсязі.

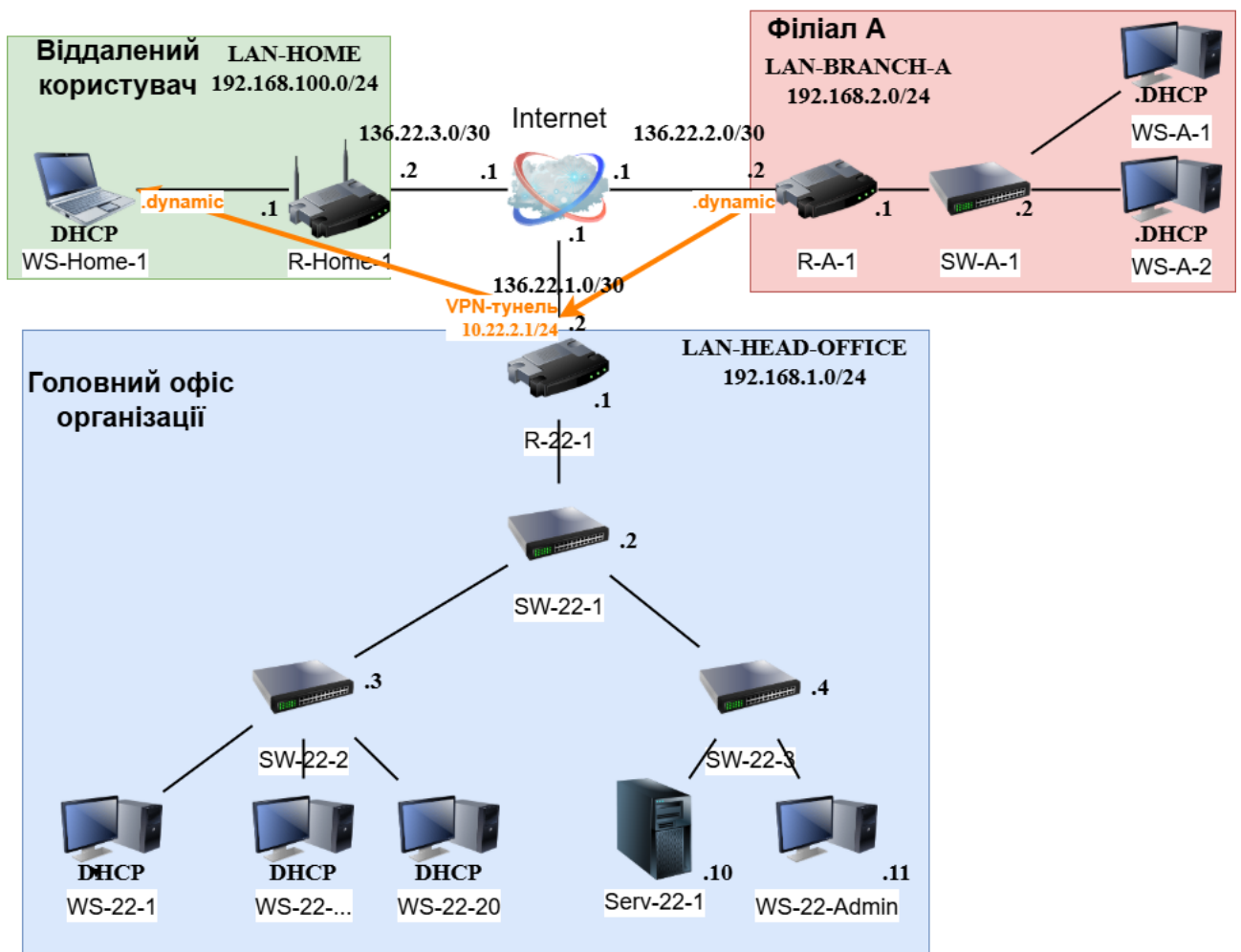
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. TOP 10 Cybersecurity Threats to Businesses in 2023 [Електронний ресурс]. – Режим доступу: <https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/top-10-cybersecurity-threats-to-businesses-in-2023>
2. Olifer N, Olifer V. Computer Networks: Principles, Technologies and Protocols for Network Design (2005).
3. James F. Kurose, Keith W. Ross. Computer Networking: A Top-Down Approach (2012).
4. Corporate Network Security: How to Detect & Prevent Attacks [Електронний ресурс]. – Режим доступу: <https://www.netmaker.io/resources/network-security>
5. 9 Techniques To Improve Your Business Network Security | ClearNetwork [Електронний ресурс]. – Режим доступу: <https://www.clearnetwork.com/cybersecurity-advice-to-secure-your-business-network/>
6. Плитус Д. І., Трокоз Є. М. Переваги використання обладнання Mikrotik в інфраструктурі корпоративної мережі // Тези доповідей VII Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 02-03 грудня 2024 року – Житомир: Житомирська політехніка, 2024.
7. What is the MikroTik RouterOS? Features & Capabilities [Електронний ресурс]. – Режим доступу: https://www.netmaker.io/resources/mikrotik-routerosLearn_Router_OS_2nd_Edition
8. Плитус Д. І., Трокоз Є. М. Сценарії використання VPN в корпоративних мережах // Тези доповідей VII Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 02-03 грудня 2024 року – Житомир: Житомирська політехніка, 2024.
9. Best VPN Protocols Compared in 2024 [Електронний ресурс]. – Режим доступу: <https://operavps.com/blog/different-protocols-of-vpn/>

10. Types of VPN Protocols: Explained and Compared 2024 [Электронный ресурс]. – Режим доступа: https://zoogvpn.com/vpn-protocols/?srsId=AfmBOorKYAuGARCeDY6zsqbX0Q7KjtL2Ro3liX81Juk_u4B3uiVW2uCE
11. What is OpenVPN? Capabilities [Электронный ресурс]. – Режим доступа: <https://www.techradar.com/vpn/what-is-openvpn>
12. Feilner, Markus OpenVPN: Building and Integrating Virtual Private Networks/ Markus Feilner – Packt Publishing, 2006;
13. Network Topology [Электронный ресурс]. – Режим доступа: <https://networkhope.in/network-topology/>
14. CCR1009-7G-1C-1S+ [Электронный ресурс]. – Режим доступа: <https://mikrotik.com/product/CCR1009-7G-1C-1Splus>
15. Cisco Catalyst 2960-X Series Switches [Электронный ресурс]. – Режим доступа: <https://www.cisco.com/c/en/us/support/switches/catalyst-2960-x-series-switches/series.html>
16. WinBox - MikroTik Documentation [Электронный ресурс]. – Режим доступа: <https://help.mikrotik.com/docs/spaces/ROS/pages/328129/WinBox>
17. OpenVPN - MikroTik Documentation [Электронный ресурс]. – Режим доступа: <https://help.mikrotik.com/docs/spaces/ROS/pages/2031655/OpenVPN>
18. Configuring openVPN on a Mikrotik router [Электронный ресурс]. – Режим доступа: <https://ltesocks.io/blog/configuring-openvpn-on-a-mikrotik-router/>
19. MikroTik Security: Built-in Default Configuration [Электронный ресурс]. – Режим доступа: https://mum.mikrotik.com/presentations/KH19/presentation_6541_1548340815.pdf
20. RADIUS - MikroTik Documentation [Электронный ресурс]. – Режим доступа: <https://help.mikrotik.com/docs/spaces/ROS/pages/328097/RADIUS>

ДОДАТКИ

Топологія мережі з адресацією



Конфігураційні файли пристроїв мережі

Маршрутизатор R-22-1:

```

# 2024-12-11 14:03:54 by RouterOS 7.16.2
# software id =
#
/interface ovpn-server
add name=ovpn-client-branch-a user=client-branch-a
/interface list
add name=WAN
add name=LAN
/ip pool
add name=ovpn-pool ranges=10.22.1.2-10.22.1.254
/port
set 0 name=serial0
/ppp profile
add dns-server=192.168.1.10 local-address=10.22.1.1 name=ovpn remote-address=\
    ovpn-pool
/system logging action
set 3 remote=192.168.1.10
/interface list member
add interface=ether1 list=WAN
add interface=ether2 list=LAN
/interface ovpn-server server
set certificate=ovpn-server
cipher="blowfish128,aes128-cbc,aes192-cbc,aes256-c\
    bc,aes128-gcm,aes192-gcm,aes256-gcm"
default-profile=ovpn enabled=yes \
    push-routes="192.168.1.0 255.255.255.0"
require-client-certificate=yes
/ip address
add address=136.22.1.2/30 interface=ether1 network=136.22.1.0
add address=192.168.1.1/24 interface=ether2 network=192.168.1.0
/ip dhcp-client
add interface=ether1
/ip dns
set servers=136.22.1.1,192.168.1.1
/ip firewall filter
add action=accept chain=input src-address=127.0.0.1
add action=accept chain=input comment=\
    "defconf: accept to local loopback (for CAPsMAN)" dst-address=127.0.0.1
add action=accept chain=input comment="Allow OpenVPN" dst-port=1194 protocol=\
    tcp
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=drop chain=forward comment=\
    "defconf: drop all from WAN not DSTNATed" connection-nat-state=!dstnat \
    connection-state=new in-interface-list=WAN
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 hw-offload=yes
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 disabled=yes
/ip firewall nat
add action=masquerade chain=srcnat out-
interface=ether1
/ip route
add dst-address=0.0.0.0/0
gateway=136.22.1.1
add disabled=no distance=1 dst-
address=192.168.2.0/24 gateway=\
    ovpn-client-branch-a routing-table=main
scope=30 suppress-hw-offload=no \
    target-scope=10
/ppp secret
add name=client-remote-user-1 profile=ovpn
service=ovpn
add name=client-branch-a profile=ovpn
service=ovpn
/radius

```

```

add address=192.168.1.10 require-message-
auth=no service=login
/system clock
set time-zone-name=Europe/Kyiv
/system identity
set name=R-22-1
/system logging
add action=remote topics=info
add action=remote topics=critical
add topics=error
/system note
set show-at-login=no
/system ntp client
set enabled=yes
/system ntp client servers
add address=0.ua.pool.ntp.org
/tool romon
set enabled=yes
/user aaa
set default-group=full use-radius=yes

```

Маршрутизатор R-A-1:

```

# 2024-12-11 14:10:18 by RouterOS 7.16.2
# software id =
#
/interface ovpn-client
add auth=md5 certificate=client-branch-a
cipher=aes256-cbc connect-to=\
    136.22.1.2 mac-
address=02:EE:FF:D9:88:2C name=ovpn-
out1 user=\
    client-branch-a
/ip pool
add name=dhcp_pool0 ranges=192.168.2.10-
192.168.2.254
/ip dhcp-server
add address-pool=dhcp_pool0
interface=ether2 name=dhcp1
/port
set 0 name=serial0
/ip address
add address=136.22.2.2/30 interface=ether1
network=136.22.2.0
add address=192.168.2.1/24 interface=ether2
network=192.168.2.0
/ip dhcp-client
add interface=ether1

```

```

/ip dhcp-server network
add address=192.168.2.0/24 dns-
server=192.168.2.1,192.168.1.10 gateway=\
    192.168.2.1
/ip dns
set allow-remote-requests=yes
servers=136.22.2.1,8.8.8.8
/ip firewall nat
add action=masquerade chain=srcnat out-
interface=ether1
/ip route
add disabled=no dst-address=0.0.0.0/0
gateway=136.22.2.1 routing-table=main \
    suppress-hw-offload=no
/system clock
set time-zone-name=Europe/Kyiv
/system identity
set name=R-A-1
/system note
set show-at-login=no
/system ntp client
set enabled=yes
/system ntp client servers
add address=0.ua.pool.ntp.org
vmn

```

Комутатор SW-22-1:

! Last configuration change at 20:41:46 UTC
Tue Dec 10 2024 by Admin

```
!  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime  
no service password-encryption  
service compress-config  
!  
hostname SW-22-1  
!  
boot-start-marker  
boot-end-marker  
!  
!  
logging discriminator EXCESS severity drops  
6 msg-body drops EXCESSCOLL  
logging buffered 50000  
logging console discriminator EXCESS  
enable secret 5  
$1$TYXk$0h50wKlt0oM4ZusJTaYB4.  
!  
username Admin privilege 15 secret 5  
$1$yWcq$GSCgYzu9Dsia7FeyXQSgF1  
aaa new-model  
!  
!  
aaa authentication login default group radius  
local  
aaa authorization exec default group radius  
local if-authenticated  
!  
!  
!  
aaa session-id common  
!  
!  
!  
!  
!  
no ip routing  
no ip icmp rate-limit unreachable  
!  
!  
!  
ip domain-name plytus.net  
ip name-server 192.168.1.10  
ip name-server 192.168.1.1  
no ip cef
```

```
no ipv6 cef  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Ethernet0/0  
!  
interface Ethernet0/1  
!  
interface Ethernet0/2  
description UNUSED-PORTS  
switchport access vlan 1001  
switchport mode access  
shutdown  
!  
interface Ethernet0/3  
description UNUSED-PORTS  
switchport access vlan 1001  
switchport mode access  
shutdown  
!  
interface Ethernet1/0  
description UNUSED-PORTS  
switchport access vlan 1001  
switchport mode access  
shutdown  
!  
interface Ethernet1/1  
description UNUSED-PORTS  
switchport access vlan 1001  
switchport mode access  
shutdown  
!  
interface Ethernet1/2
```

```

description UNUSED-PORTS
switchport access vlan 1001
switchport mode access
shutdown
!
interface Ethernet1/3
description UNUSED-PORTS
switchport access vlan 1001
switchport mode access
shutdown
!
interface Ethernet2/0
description UNUSED-PORTS
switchport access vlan 1001
switchport mode access
shutdown
!
interface Ethernet2/1
description UNUSED-PORTS
switchport access vlan 1001
switchport mode access
shutdown
!
interface Ethernet2/2
description UNUSED-PORTS
switchport access vlan 1001
switchport mode access
shutdown
!
interface Ethernet2/3
description UNUSED-PORTS
switchport access vlan 1001
switchport mode access
shutdown
!
interface Ethernet3/0
description UNUSED-PORTS
switchport access vlan 1001
switchport mode access
shutdown
!
interface Ethernet3/1
description UNUSED-PORTS
switchport access vlan 1001
switchport mode access
shutdown
!
interface Ethernet3/2
description UNUSED-PORTS
switchport access vlan 1001
switchport mode access
shutdown
!
interface Ethernet3/3
description UNUSED-PORTS
switchport access vlan 1001
switchport mode access
shutdown
!
interface Vlan1
ip address 192.168.1.2 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.1.1
ip forward-protocol nd
!
ip tcp synwait-time 5
ip http server
!
ip ssh time-out 30
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
!
!
logging trap notifications
logging host 192.168.1.10
!
!
radius server Serv-22-1
address ipv4 192.168.1.10 auth-port 1812
acct-port 1813
key win-radius
!
!
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
transport input ssh
!
!
!
End

```

Вміст конфігураційного файлу OpenVPN «client1732913799.ovpn»

```
client
dev tun
remote 136.22.1.2 1194 tcp
tun-mtu 1500
tls-client
nobind
user nobody
group nogroup
ping 15
ping-restart 45
persist-tun
persist-key
mute-replay-warnings
verb 3
cipher AES-256-GCM
auth none
pull
auth-user-pass
connect-retry 1
reneg-sec 3600
remote-cert-tls server
route 192.168.0.0 255.255.0.0
<ca>
-----BEGIN CERTIFICATE-----
MIIDvzCCAqegAwIBAgIIWYYcOOVi62gwDQYJKoZIhvcNAQELBQAwZjELMAkGA1UE
BhMCMVUEXETAPBgNVBAGMCFpoeXRvbXlyMREwDwYDVQQHDAhaaHl0b215cjERMA8G
A1UECgwIWmh5dG9teXlXETAPBgNVBAsMCFpoeXRvbXlyMQswCQYDVQQDDAJjYTAe
Fw0yNDEzMjg0MjE0MDFaFw0zNDEzMjg0MjE0MDFaMGYxCzAJBgNVBAYTAiVBMREw
DwYDVQQIDAhaaHl0b215cjERMA8GA1UEBwwIWmh5dG9teXlXETAPBgNVBAoMCFpo
eXRvbXlyMREwDwYDVQQQLDAhaaHl0b215cjELMAkGA1UEAwwCY2EwggeiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC9JHNAoDkQIUJuVtqBtOQ6+HhtvFnF0EE4
UMKpgxcGdNvIa/lACOLk4i4yJhu7Fn7xrFlwKfE4araAt25BKK/xp9+rc/MSyczt
fuiECiBQyXln4tOltH13wOXKtngs2HtB7pjRoq5S/9Zy23JwuBdy1NZy02BfAu1k
/Xte4Z9+QfiiyUpZk7fWGPq9+XEBUIU9IXKXzDjO6R3uRwKMceIDpid65XHPZ8/
c3w6cUzuXv5B4UMUg4yJlTrNe+oqbbQLwXOeEm2VR6m2ohX8htCPOgz/6NK5LyC8
QpczKt145T+ftOlukgKB9I3Pg/aGnx0dJjpgTQztsxM9GrLGhfajAgMBAAAgjcTBv
MA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBTaVcyW
Lp3VSKMgiqO18GFkh8xWFjAtBgNVHR8EJjAkMCKgIKAehhxodHRwOi8vMTM2Ljly
LjEuMi9jcmVwMTEuY3JsMA0GCSqGSIb3DQEBCwUAA4IBAQBiJJPpDjDh0CsKsx2T
RrCfSJFtvvOkoro2WQndg6mAoZLvllrxv2xkBPi1m3IVXO3WbvhtwzX+x7nZv7r
Ws9hEmSTgs8dMK9sACXERY90/0QNpnW7wi146S3vA66bYgEh9Adys0Sn9omcxJoJ
rY8ZZQkFImptWgyFkNsMiwT9o+cdELUVF5MEf2i//VVgTrMWPcNFYPICeEYz6q+w
+RvqfwqjObU+hQJXdfRxnKwg4FeGetBxL6/Xyqk2CvTcSx8ft7DabXW7I32sRphs
XRvZfys9yjGVbb3278a/n2RG6eN1xMJrdbB+JgToYbDBcdZpHwaviXS4gziov5t
z2g8
-----END CERTIFICATE-----
</ca>
<cert>
-----BEGIN CERTIFICATE-----
MIIDvTCCAqWgAwIBAgIICgudEoL47gkwDQYJKoZIhvcNAQELBQAwZjELMAkGA1UE
BhMCMVUEXETAPBgNVBAGMCFpoeXRvbXlyMREwDwYDVQQHDAhaaHl0b215cjERMA8G
A1UECgwIWmh5dG9teXlXETAPBgNVBAsMCFpoeXRvbXlyMQswCQYDVQQDDAJjYTAe
```

Fw0yNDExMjgxNzExMjBaFw0yNTEExMjgxNzExMjBaMH4xCzAJBgNVBAYTAIVBMREw
DwYDVQQIDAAH10b215cjERMA8GA1UEBwwIWmh5dG9teXlHTAbBgNVBAoMFFpo
eXRvbXlyIFBvbH10ZWNoYmMjMQswCQYDVQQLDAJJVDEdMBsGA1UEAwwUY2xpZW50
LXJlbW90ZS1lc2VyLTFEwggEiMA0GCSqGSIb3DQEBAAQUAA4IBDwAwggEKAoIBAQC0
Op3u+tkfmyiMYCjRHH2CnhRGYjddG57LN4a/qHendFIYzwqvLR8dv+cPaAC251k7
Cp20mxgcdJKRbviwwdIr+7lA7z+iJlgavU181HeyuMI7t/gD3aLfhjUIsKTKQyT
BPHHNquJCi1DE+o7XLVq6/sW637fMUjPWvuBQ/MnDIgnPbI3ypyv+IWkOsUXo7sS
WtO1JH4jJo6ZF1b2QsPhEfvMGGCBC5tI9KUKCFnt9QSnmhBusQkWOBzvhpzSJduN
7JAx7kK+1lBf7A8X5IUcj/q5XjGxNk3U/OTY3Gmir8SWgVlSmPuE3sKcxlAfa5
hT152x7J24u4uwlHc2cXAgMBAAGjVzBVMBMGA1UdJQQMMAoGCCsGAQUFBwMCMB0G
A1UdDgQWBBTtX8xpJQkuEiO+mG5XJeebev7dADAFBgNVHSMEGDAWgBTaVcyWLP3V
SKMgiqO18GFkh8xWFjANBgkqhkiG9w0BAQsFAAOCAQEAS8b8padjlhBHLooqoCBo
wD61OpFORBU7kyEpa7kpMOv6oyXtzkVQdrWf7Ho95BnkV8/yvzfV1J6vaxi2LEX9
KtzQCphnFiUHMMyWrqR+Ver+JMic1TQWVQqy4kLVfBmO5fw9M8AmvRegaTF1AWAh7
VbibBNGvTwY1QSOyQsCP5jvPJX/xM6rwwLYM0tho5S+FN82vnUpv6OLXIFU31pF
fClo6ZXl0xGCOWHwmSJg5NwlsXktIRbBLqI16K8FRbIK6JISXWPAMsq953V17QPf
k5Ec0FPTlc1CBn4nb4I3XWso31LUv6maXOp1NgBRcL2M+x2g3xwqO0wW9N2Lwu4k
wA==

-----END CERTIFICATE-----

</cert>

<key>

-----BEGIN ENCRYPTED PRIVATE KEY-----

MIIFNTBfBgkqhkiG9w0BBQ0wUjAxBgkqhkiG9w0BBQwwJAQQcehAjRkeBc9Jw5M6
BLMAOAICJxAWDAYIKoZIHvcNAgkFADAdBgglghkgBZQMEASoEECsVKdAJZkqI3tJH
myVm4WgEggTQAIgGVXEJ2ADuFvUpt0MGFF1ni/DSdZ+FkXRKEZnerKZ8UFyhBO9v
8DdoJSVcyHcKlJQRvjPM8dK5KyLH7gs9qwoOcr/fSiBHwR/RfIdUTujfabzyCjCN
yWuZQBKf63vNbUIfmU9SeZBJIHgZupqB+2do9Sx1AwSzR57Xwm1DvP2KD+MA4Bz8
Eng2B7DHjhl7Y66PE1jIJ+y35j/FEgJWzBQJKB4+v+WVU+C+aqeZTwrwHsrcdMhU
QdRk6YtxUmmzStm0vYmtoZ7BucVEkAuyaKEurEEIJX4MrLCWkEQdMnBDVgqx9svV
qCTDq1zvfqpmSXTM9YXuMXeqbJSIJq4d8uN99dCaM6HeC6V/CfRV/5G9S9y+5in
PVegqrgD3zfC8OoR5vDqAScGXZLF1q0GBaRcArOT4gs5t89TqLFhL2yQ/gJSp2Jt
GeewEzRUId2SBy5+gPJmx3IdbwpaltXVQyFwY/XjofabRIoX60PYIQkDfxQnLOre
o1T/oLBItS+JWpRzck3J8K5g3ZVWNHVjR+qiU3Q3LeGjvYjCPQRjP6AK9+nYfi8
6v3791Pa041Ir5nRmJRxo/CU6QHSM7w2fwKEuy6zqJ5RPyV+yL7B2RFgMmK21TA2
qFI/BEhpNvIZfoxywbgkrKhLqcvLqZOD5d/MnvAyliB42ld5fKaZfeVPfphxSeR/
MCF8K6TdeB7WYdBk2S3A9cAeXaRaT8N2zIB1ZdfbEj4Vlr0yzRNhHk3fdG2ZlCIP
SsnB6R3ejkVrcC9pPjd42O/5n4SYECWW+12Mv0sJehQxgePt8agfx8/jhLPBq7Cm
IMdD2URzfYCUm80I6hhY6P2w4K4pbj7JwreIbfpDvfFA3QwTTilqlLDXS6z2G85g
eKc8qMTxi7w2PEH0yjNmiegNLU6HEcF9GZ+wBhbt6MvIhKgUDb5CkPBNLWYsHy
5GMf3zx0jvwMSL9YLdN9TmMeEXB9Pmd7rcH9u0bLmuwtBy6ZWBzgyhtlOB18csBf
T42sQv7Ox4eb1nq0NFhZSAvVxjaTTS2/rMBrABQ+cEgzaJXoVYCVXQ1jKsyouM97
JFV58a1DsACFTVxkOM6ULxmDG8rY2IQDjuhGKFy7rOPDOv+8N+IWf7DfjQRUu8sd
0AVzccBER03XtN8M8esHq/mmRBcKT6ZzYdL1nG55QPU5Dfxvi++JBmk7xLnF43/v
6QhRw1MiH56z4BCrIev5ME9bun9/KwpLF6tl2idMFZ1EZu9yUOsfzAKheuHeQ+IL
obtlennptvtcE7Xf2qrp9VTEtnGKJRnPeVpwOwP3SHRDKABbf33MzjCCWuDMFUR2
uEtAmNg4ngzp/CXxQFZeVUQbNhTHFhV0O6UcR620iTAryEwLD+dFKNbIWOWThVi
nFC9XHV0ZxSBKul9qjW+tYdkSgV1PdoVThMkUoEil880CIH6g+E2lO/BKyuEYHTV
CyJzHUwtsZi81PK45yak2W5CuB6+hVHOGJFCtB7gs/S4rJuxZs0UP8rIHpH+FIxt
zkeC18rTHWMUOGKch38cG+miYbOKSV1CRgmmb70/ZMYp0IgTZOSup1UzdBQ5ZqD
E0m/ZgK4CAahoWm/VsJ+bs7lNQZzzRgfdVQELwnqocZh6GheGV7Naws=

-----END ENCRYPTED PRIVATE KEY-----

</key>