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 ПОБУДОВИ ПІДСИСТЕМИ ЗАХИСТУ ПЕРИМЕТРУ КОРПОРАТИВНОЇ МЕРЕЖІ**»

Виконав студент 2-го курсу групи КІм-23-1
спеціальності 123 «Комп’ютерна інженерія»
_____ Б.С. Фальковський

Керівник завідувач кафедри КІ та КБ, к.т.н., доцент
_____ А.А. Єфіменко

Рецензент професор кафедри КІ та КБ, д.т.н., доцент
_____ В.В. Воротніков

Житомир – 2024

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кіберебзпеки
Андрій Єфіменко
17 вересня 2024 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу магістра

Студент: Фальковський Богдан Сергійович

Тема роботи: **«Методи та технології побудови підсистеми захисту периметру корпоративної мережі»**

затверджена Наказом університету від 17 вересня 2024 р. № 478/с

Термін здачі студентом закінченої роботи 16.12 2024 р.

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

1. Розроблені фізична топологія мережі
2. Розроблена логічна топологія мережі
3. Проведені налаштування відповідно від поставлених задач
4. Здійснено тестування мережі

Обладнання та програмне забезпечення:

1. Міжмережевий екран FortiGate 60F
2. Комутатори MikroTik

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Россінський Ю.М.	17.09.24	17.09.24
2	Россінський Ю.М.	17.09.24	17.09.24
3	Россінський Ю.М.	17.09.24	17.09.24

Студент _____ Б.С. Фальковський

Керівник _____ А.А. Єфіменко

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Постановка завдання	17.09.2024	**Виконано**
2	Пошук, огляд та аналіз літературних джерел щодо організації периметрового захисту мережі	20.09.2024 – 30.09.2024	**Виконано**
3	Аналіз технологій периметрового захисту на основі міжмережного екрану	1.10.2024 – 7.10.2024	**Виконано**
4	Аналіз можливостей мережного обладнання MikroTik для гетерогенності мережі	8.10.2024 – 14.10.2024	**Виконано**
5	Розробка загального проекту мережі організації	15.10.2024	**Виконано**
6	Проектування мережі та вибір обладнання для її реалізації	16.10.2024 – 21.10.2024	**Виконано**
7	Проектування таблиці маршрутизації	22.10.2024	**Виконано**
8	Проектування сценарію тестування мережі	23.10.2024 25.10.2024	**Виконано**
9	Базове налагодження пристроїв мережі	26.10.2024 – 11.11.2024	**Виконано**
10	Налагодження гетерогенної мережі	12.11.2024 – 18.11.2024	**Виконано**
11	Тестування роботи гетерогенної мережі	19.11.2024 – 22.11.2024	**Виконано**
12	Аналіз результатів тестування	23.11.2024 – 25.11.2024	**Виконано**
13	Написання пояснювальної записки	26.11.2024 – 20.12.2024	**Виконано**
14	Підготовка презентації та виступу	21.12.2024 – 25.12.2024	**Виконано**
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	26.12.2024	**Виконано**
9	Захист		**Виконано**

Студент _____ Б.С. Фальковський

Керівник проекту _____ А.А. Єфіменко

АНОТАЦІЯ

Випускна кваліфікаціна робота магістра складається з проекту комплексної системи захисту інформації та пояснювальної записки. Пояснювальна записка до випускної роботи містить 69 сторінок, 46 ілюстрацій та 5 таблиць.

Метою роботи є розробка підсистеми периметрового захисту корпоративної мережі організації, яка включає в себе аналіз сучасних приладів та вибір структури мережі, вибір ПЗ для реалізації мережі, реалізація підсистеми захисту.

Проект складатиметься з трьох розділів, в яких буде продемонстровано розробку логічної та фізичної структури мережі, вибір обладнання та ПЗ, конфігурація пристроїв. В додатках буде вказано конфігурації Fortinet Fortigate 60F та комутаторів мережі.

КЛЮЧОВІ СЛОВА: КІБЕРБЕЗПЕКА, КОРПОРАТИВНА МЕРЕЖА, ПЕРИМЕТРОВИЙ ЗАХИСТ, FORTINET FORTIGATE 60F, MIKROTIK, БАГАТОРІВНЕВИЙ ЗАХИСТDHCP-СЕРВЕР, ІЄРАРХІЧНА МОДЕЛЬ МЕРЕЖІ, ФАЄРВОЛ, МАРШРУТИЗАЦІЯ, ФІЛЬТРАЦІЯ ТРАФІКУ, WIRESHARK, АНТИВІРУСНИЙ ЗАХИСТ, КІБЕРЗАГРОЗИ, ІНФОРМАЦІЙНА БЕЗПЕКА.

ANNOTATION

The master's qualification thesis consists of a comprehensive information protection system project and an explanatory note. The explanatory note for the thesis includes 69 pages, 46 illustrations, and 5 tables.

The goal of the thesis is to develop a subsystem for perimeter protection of the corporate network of an organization, which includes the analysis of modern devices and the selection of the network structure, the choice of software for network implementation, and the realization of the protection subsystem.

The project will consist of three sections, demonstrating the development of the logical and physical structure of the network, the selection of equipment and software, and the configuration of devices. The appendices will include configurations for the Fortinet FortiGate 60F firewall and network switches.

KEYWORDS: Cybersecurity, corporate network, perimeter protection, Fortinet FortiGate 60F, MikroTik, multilayer protection, DHCP server, hierarchical network model, firewall, routing, traffic filtering, Wireshark, antivirus protection, cyber threats, information security.

ЗМІСТ

АНОТАЦІЯ 4
ANNOTATION 5
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 7
ВСТУП 8
РОЗДІЛ 1 ОСНОВИ ТА ВИМОГИ ДО КОРПОРАТИВНИХ МЕРЕЖ: КОНЦЕПЦІЯ І СТРУКТУРА 11
1.1 Конструювання корпоративних мереж: ключові аспекти 11
1.2 Структурні моделі корпоративних мереж 14
1.3 Модуль доступу до Інтернету в корпоративних мережах 15
1.4 Серверний модуль 18
РОЗДІЛ 2 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ З СИСТЕМАМИ ЗАХИСТУ 22
2.1 Основи функціонування корпоративної мережі 22
2.2 Формування логічної інфраструктури мережі 25
2.3 Підбір технічних засобів і програмного забезпечення. 30
РОЗДІЛ 3 НАЛАШТУВАННЯ І ТЕСТУВАННЯ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ 37
3.1 Процес налаштування корпоративної мережі 37
3.2 Оцінка ефективності проведених налаштувань. 54
3.3 Аналіз результатів перевірок 56
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 60
ДОДАТКИ 61

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПЗ – програмне забезпечення

ПК – персональний комп'ютер

КМ – комп'ютерна мережі

ОС – операційна система

FORTINET FORTIGATE 60F – міжмережний екран

ВСТУП

Актуальність теми. У сучасному світі корпоративні мережі стали основою для ефективного функціонування організацій у різних сферах діяльності. Водночас, з огляду на постійно зростаючі загрози, захист периметру корпоративної мережі є однією з найбільш важливих та актуальних проблем у сфері кібербезпеки. Загрози, що виникають у результаті зовнішніх атак, зловмисних проникнень, а також внутрішніх помилок, можуть призвести до значних фінансових і репутаційних втрат, а іноді й до повного знищення критичних даних компанії. Саме тому вибір правильних методів і технологій для побудови надійної системи захисту периметру корпоративної мережі стає ключовим завданням для спеціалістів з інформаційної безпеки.

Технологічний прогрес сприяє значному збільшенню кількості і складності кіберзагроз. Атаки на корпоративні мережі стають дедалі більш складними та хитромудрими, що вимагає постійної адаптації систем захисту. Кіберзлочинці використовують різноманітні методи для проникнення в корпоративні мережі, серед яких: фішинг, віддалене виконання кодів, DDoS-атаки, використання шкідливого програмного забезпечення та інші. Периметр мережі є найбільш уразливою частиною системи, оскільки саме через нього здійснюється більшість спроб несанкціонованого доступу.

Захист периметру має на меті блокування зовнішніх загроз до того, як вони потраплять до внутрішньої корпоративної мережі. Це вимагає застосування різноманітних інструментів та методів для контролю за трафіком, моніторингу активності і реагування на інциденти. Одним із ключових аспектів є створення багаторівневого захисту, де кожен рівень виконує специфічну роль у відсіченні потенційних загроз.

Захист периметру корпоративної мережі традиційно передбачає використання таких засобів, як міжмережеві екрани (фаєрволи), системи виявлення та запобігання вторгнень (IDS/IPS), проксі-сервери, а також VPN-мережі. Однак, з розвитком технологій і зміною характеру загроз, виникає потреба в більш ефективних і гнучких підходах до захисту.

Сучасні технології, такі як «Zero Trust» (нульове довір'я), принципи сегментації мережі, використання інтелектуальних систем моніторингу на базі машинного навчання та штучного інтелекту, стали важливими інструментами для захисту периметру. Зокрема, концепція Zero Trust полягає в тому, щоб жодна частина мережі не вважалася «надійною», і кожен запит до системи проходить перевірку незалежно від того, чи перебуває користувач чи пристрій всередині чи поза мережею.

Серед основних переваг сучасних методів захисту периметру варто зазначити їх здатність до швидкої адаптації до нових типів атак, а також інтеграцію з іншими аспектами кібербезпеки, що дозволяє створювати комплексні системи захисту. Такі підходи дозволяють не лише попереджати зовнішні загрози, а й ефективно виявляти аномальні дії в мережі, що може свідчити про внутрішнє порушення безпеки.

Проте впровадження таких технологій може бути складним через високу вартість обладнання, потребу в кваліфікованих спеціалістах та необхідність постійного оновлення систем. Окрім того, існують виклики, пов'язані з інтеграцією нових систем захисту в існуючі інфраструктури та управлінськими процесами компаній.

Оскільки кіберзагрози постійно еволюціонують, технології захисту периметру також будуть вдосконалюватися. Важливими напрямами є використання більш потужних аналітичних інструментів для виявлення і блокування складних атак, покращення інтеграції систем захисту з іншими компонентами корпоративної інформаційної системи, а також підвищення ефективності методів виявлення загроз на основі штучного інтелекту та великих даних.

Загалом, захист периметру корпоративної мережі є стратегічно важливим напрямом для забезпечення безпеки будь-якої організації. Вибір правильних методів і технологій є основою для створення стійкої та безпечної інфраструктури, здатної витримати різноманітні загрози і забезпечити належний рівень безпеки для користувачів і даних.

Отже, актуальність теми захисту периметру корпоративної мережі безпосередньо пов'язана з постійним розвитком нових методів атак та необхідністю удосконалення підходів до захисту. Впровадження ефективних технологій і методів захисту, багаторівневий захист та інтеграція сучасних інтелектуальних систем, є основою для надійної та безпечної роботи корпоративних мереж у майбутньому.

Метою кваліфікаційної роботи є розробка підсистеми периметрового захисту корпоративної мережі організації.

Встановлена мета створює наступні завдання:

– аналіз сучасних приладів та вибір структури мережі;

– вибір ПЗ для реалізації мережі;

– реалізація підсистеми захисту;

Об'єктом дослідження є процес налаштування захисту комп'ютерної мережі від зловмисників.

Предметом дослідження методи і засоби захисту корпоративної мережі.

Апробація результатів:

1. Фальковський Б.С., Байлюк Є.М., Вакалюк Т.А. Система запобігання вторгнень IPS // Тези доповідей V Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 01-02 грудня 2022 р. – Житомир: Житомирська політехніка, 2022.

2. Фальковський Б.С., Байлюк Є.М., Вакалюк Т.А. Модуль територіальних мереж(WAN EDGE) // Тези доповідей V Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 01-02 грудня 2022 р. – Житомир: Житомирська політехніка, 2022.

РОЗДІЛ 1 ОСНОВИ ТА ВИМОГИ ДО КОРПОРАТИВНИХ МЕРЕЖ: КОНЦЕПЦІЯ І СТРУКТУРА

1.1 Конструювання корпоративних мереж: ключові аспекти

Корпоративна мережа - це мережа, основною функцією якої є підтримка діяльності компанії, що володіє мережею. Єдиними користувачами мережі є співробітники компанії.[1]

Простіше кажучи, корпоративна мережа - це мережа, яка закрита від зовнішнього світу, забезпечує надійний захист від вторгнення і вирішує всі завдання, які можуть бути поставлені перед підприємством.

Операційна потужність корпоративної мережі — це здатність мережі обробляти дані та виконувати операції в межах її інфраструктури. Ось кілька аспектів, що впливають на операційну потужність:

Швидкість обробки запитів: Включає час, необхідний для обробки запитів користувачів або системи, а також для виконання складних обчислювальних задач. Може бути важливим для баз даних, що підтримують реальний час (наприклад, фінансові звіти).

Продуктивність зберігання даних: Сюди входять ефективність зберігання великих обсягів даних, наприклад, через використання швидких жорстких дисків або SSD, а також механізми резервного копіювання та відновлення.

Паралельна обробка: Важливий аспект для корпоративних мереж, де одночасно працює кілька користувачів з великою кількістю запитів.

Чим вища операційна потужність мережі, тим швидше і з меншою кількістю затримок вона виконує операції, що критично важливо для великих компаній або організацій з великими обсягами даних.

Час доставки повідомлень визначає, наскільки швидко інформація передається в межах мережі. Це залежить від таких факторів:

Технології передачі даних: Наприклад, якщо мережа використовує швидкий оптоволоконний зв'язок, час доставки повідомлень буде значно меншим, ніж при використанні звичайних телефонних ліній.

Навантаження на мережу: Якщо в певний момент часу кількість запитів і переданих повідомлень велика, це може вплинути на час доставки.

Мережеві шари та протоколи: Протоколи, такі як TCP/IP, зокрема механізми управління потоком і підтвердження отримання, також можуть впливати на час затримки повідомлення.

Час доставки може мати важливе значення в реальному часі для організацій, що здійснюють онлайн операції або користуються хмарними рішеннями.

Продуктивність мережі — це сумарна здатність мережі передавати дані за певний проміжок часу. Ось деякі аспекти, які впливають на продуктивність:

Пропускна здатність каналу зв'язку: Мережева інфраструктура, включаючи сервери, маршрутизатори і мережеві комутатори, повинна мати достатню пропускну здатність для обміну даними без значних затримок.

Оптимізація навантаження: Залишкове навантаження на мережу, яке виникає через неправильний баланс між серверними запитами і реальними ресурсами, може значно знизити ефективність. Сучасні мережі зазвичай використовують технології балансування навантаження для підтримки стабільної роботи.

Системи моніторингу: Важливо мати засоби для моніторингу продуктивності, щоб виявляти та усувати потенційні проблеми в процесі обміну даними між користувачами та серверами.

Висока продуктивність мережі дозволяє швидко обробляти і передавати дані без затримок, що є важливим для інтенсивних обчислювальних задач або в компаніях, що працюють з великими масивами інформації.

Витрати на обробку даних складаються з багатьох компонентів:

Інфраструктура (апаратне забезпечення): Включає витрати на сервери, мережеві пристрої (комутатори, маршрутизатори), пристрої зберігання даних. Вартість обладнання і його обслуговування відіграють важливу роль.

Програмне забезпечення: Витрати на ліцензії для ОС, антивірусних програм, засобів шифрування, систем управління базами даних, а також на інші програмні продукти.

Енергоспоживання: Підтримка інфраструктури мережі потребує значної кількості енергії, тому енергоефективність серверних ферм є важливим фактором для зниження витрат.

Загальна вартість на обробку даних визначає ефективність витрат компанії на підтримку мережевої інфраструктури. Зниження витрат є одним із пріоритетів при розробці мережевої архітектури.

Модульна архітектура є ключовим елементом, який дозволяє адаптувати мережу під конкретні задачі компанії. Ось як вона працює:

Модульність як принцип проектування: Всі компоненти мережі поділяються на незалежні частини або модулі, які можуть бути замінені чи оновлені без необхідності змінювати всю структуру.

Простота управління та масштабування: Модульність дозволяє значно спростити управління мережею та додавання нових функцій. Наприклад, якщо компанія вирішить розширити сервери або впровадити нові служби, можна просто додати новий модуль без порушення роботи всієї системи.

Зниження ризиків: Кожен модуль можна тестувати і впроваджувати окремо, що знижує ризики при модернізації. Це також дозволяє швидко реагувати на зміни в бізнес-потребах.

Забезпечення масштабованості: Масштабованість мережі дозволяє швидко реагувати на зростання компанії. Якщо потрібно збільшити кількість користувачів або додати нові офіси, це можна зробити без необхідності змінювати всю мережу.

Гнучкість для інтеграції нових технологій: Поява нових технологій (наприклад, хмарних рішень, нових комунікаційних протоколів) може бути інтегрована в корпоративну мережу завдяки модульній архітектурі.

Відмовостійкість: Система повинна гарантувати безперервну роботу навіть у разі відмови одного з компонентів. Наприклад, сервери повинні працювати в режимі високої доступності (HA).

Безпека: Системи безпеки повинні включати засоби шифрування, аутентифікацію користувачів, захист від зовнішніх атак, а також моніторинг для виявлення будь-яких підозрілих дій у мережі.

Централізоване управління мережою дозволяє швидко виявляти проблеми та забезпечувати безперервність її роботи. Автоматизовані системи керування, такі як оркестрація мережі або використання програмного забезпечення для моніторингу, є важливою частиною архітектури корпоративної мережі.

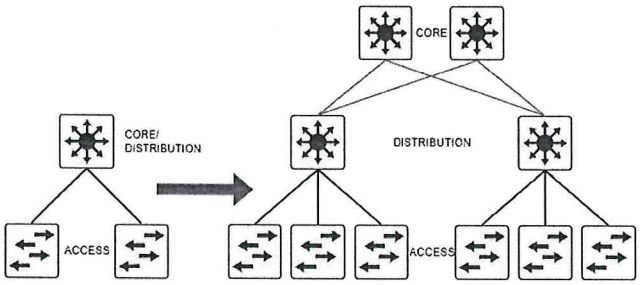


Рисунок 1.1 – Приклад модернізації мережі

1.2 Структурні моделі корпоративних мереж

Ієрархічна модель призначена для побудови надійних, масштабованих та ефективних мереж. Цей підхід забезпечує економічно ефективний, модульний, структурований і простий спосіб задоволення поточних і майбутніх потреб зростання мережі. Кожна з цих ієрархій має свої унікальні характеристики і функції, що ще більше спрощує структуру мережі.[9]

Ієрархічна модель поділяє мережу на три основні рівні [10]:

1. рівень доступу - забезпечує користувачам і пристроям доступ до мережі.

Основні характеристики:

- Комутація 2-го рівня;
- Висока доступність;
- Безпека портів;
- Класифікація та маркування;
- Межі довіри;
- Списки контролю доступу (ACL); - Магістраль;

2. Рівень розподілу - об'єднує рівні доступу та забезпечує доступ до різних сервісів організації. . Розташований між рівнем доступу та основним рівнем, його основною функцією є забезпечення маршрутизації та фільтрації, а також створення зв'язків між рівнем доступу та основним рівнем.

Основні функції:

- Агрегація каналів LAN/WAN;

- Контроль доступу та фільтрація;

- Маршрутизація між локальними мережами;

- Балансування навантаження;

- Агрегація шляхів до граничного/ядерного рівня;

- Управління широкомовними доменами.

3. рівень ядра - великі мережі Рівень розподілу об'єднує наступні рівні розподілу Магістральний рівень відповідає за забезпечення високошвидкісного трафіку між розподільчими комутаторами всередині організації.

Основні характеристики:

- Високопродуктивна наскрізна комутація

- Забезпечує надійність і відмовостійкість

- Масштабованість.

1.3 Модуль доступу до Інтернету в корпоративних мережах

Неможливо уявити сучасний бізнес без доступу до Інтернету. Сьогодні багато бізнес-процесів використовують інтернет-ресурси, такі як веб-сайти та електронна пошта. Тому для роботи в мережі необхідний Internet Edge.

Internet Edge розділений на кілька блоків, кожен з яких виконує свою функцію і надає необхідні сервіси. Поділ на кілька модулів полегшує розширення, управління та налаштування, а нові функції можна додавати відповідно до можливостей і потреб організації, щоб використовувати тільки ті модулі, які потрібні.

Інтернет-модуль - це частина мережі, яка з'єднує локальну мережу з глобальною мережею. Іншими словами, це межа між загальнодоступною мережею компанії та її приватними ресурсами, де встановлюється брандмауер для захисту мережі від зовнішніх загроз, таких як віруси, атаки та шкідливе програмне забезпечення, шляхом фільтрації небажаного та непотрібного трафіку.

Модуль Інтернет повинен включати в себе наступний модуль:

- Міжмережний екран - дозволяє або забороняє доступ до мережі (списки доступу) і надає такі функції, як NAT і DMZ.[8]

В якості міжмережного екрану під час написання дипломної роботи в побудованій віртуальній мережі використовувався Firewall Fortinet FG-60F.

Fortinet FortiGate 60F — це наступник популярної серії фаєрволів FortiGate, що належить до лінійки апаратних брандмауерів малого та середнього бізнесу. Цей пристрій пропонує потужні можливості безпеки, які поєднуються з високою продуктивністю та простотою в управлінні. Він забезпечує комплексний захист від загроз, включаючи віруси, шкідливе програмне забезпечення, вторгнення, фішинг, а також дозволяє ефективно управляти мережею.

Основні характеристики FortiGate 60F:

Продуктивність:

- IPSec VPN: до 5 Гбіт/с;
- Firewall Throughput: до 10 Гбіт/с;
- IPS Throughput: до 1,4 Гбіт/с;
- SSL Inspection Throughput: до 800 Мбіт/с;
- NGFW Throughput: до 3,5 Гбіт/с;
- Threat Protection Throughput: до 700 Мбіт/с.

FortiGate 60F оснащений потужним процесором на базі спеціалізованої архітектури, що дозволяє йому ефективно обробляти трафік та забезпечувати високий рівень безпеки без зниження продуктивності мережі.

Порти та підключення:

- GE RJ45 порти
- 1 x GE SFP слот
- 1 x USB порт для управління
- 1 x Console порт

Фаєрвол має достатню кількість портів для підключення різних мережевих пристроїв, включаючи сервери, комутатори, або інші мережеві елементи.

Вбудовані сервіси безпеки: FortiGate 60F інтегрує широкий спектр функцій захисту, включаючи:

- Антивірусний захист (FortiGuard Antivirus)
- Анти-спам та фільтрація контенту
- Фільтрація веб-трафіку
- Захист від вторгнень (IPS): виявлення і блокування атак на мережу в реальному часі.
- SSL-інспекція: аналіз і фільтрація зашифрованих з'єднань для виявлення загроз у HTTPS-трафіку.
- VPN (IPSec та SSL VPN): підтримка безпечних віддалених з'єднань для користувачів.

Інтерфейс управління: FortiGate 60F підтримує кілька методів для адміністрування та моніторингу, включаючи:

- Web GUI (графічний інтерфейс користувача)
- CLI (Command Line Interface) — командний рядок
- FortiManager — централізоване управління для великих середовищ
- FortiCloud — хмарне управління та звітність

Користувачі можуть налаштовувати і контролювати політики безпеки, переглядати звіти та моніторити стан мережі за допомогою простого в управлінні інтерфейсу.

Переваги FortiGate 60F:

- Висока продуктивність: Завдяки оптимізованому апаратному забезпеченню та потужному процесору, FortiGate 60F забезпечує високу швидкість обробки трафіку навіть за умов інтенсивного використання засобів захисту, таких як IDS/IPS, антивірусний захист та SSL-інспекція.
- Інтегровані функції безпеки: Всі основні функції безпеки вбудовані в саму платформу, що дозволяє забезпечити всеосяжний захист без необхідності впровадження додаткових рішень.

– Надійність та масштабованість: FortiGate 60F підтримує масштабовані налаштування для зростаючих організацій, дозволяючи безперешкодно збільшувати можливості системи безпеки в міру розвитку бізнесу.

– Легкість у впровадженні та управлінні: Завдяки інтуїтивно зрозумілому інтерфейсу та простим налаштуванням, пристрій зручний у впровадженні та підтримці, що робить його відмінним вибором для малих і середніх підприємств.

– Підтримка хмарних рішень: Завдяки підтримці інтеграції з FortiCloud, адміністратори можуть отримувати звіти і моніторинг в реальному часі, а також мати можливість віддаленого управління мережею.Застосування та сфери використання.

FortiGate 60F є ідеальним рішенням для малих і середніх підприємств, а також для відділів IT в організаціях, які шукають потужне, але економічно ефективне рішення для забезпечення безпеки мережі. Його можна використовувати для:

– Захисту офісних мереж від зовнішніх атак
– Забезпечення безпеки віддалених робочих місць через VPN
– Виявлення та блокування шкідливих атак в реальному часі
– Фільтрації інтернет-трафіку для запобігання шкідливому доступу

1.4 Серверний модуль

Сервер – це виділений або спеціалізований комп’ютер із групи персональних комп’ютерів для виконання сервісних задач без безпосередньої участі людини у цьому. Сервер і робоча станція можуть мати одинаку апаратну конфігурацію, єдина відмінність між ними у участі в роботі людини за консоллю.

Сервер - це виділений або спеціалізований комп'ютер у групі персональних комп'ютерів для виконання сервісних завдань без безпосереднього втручання людини. Сервери та робочі станції можуть мати однакову апаратну конфігурацію, різниця лише в тому, чи знаходиться людина за пультом чи ні.

Деякі сервісні завдання можуть виконуватися на робочих станціях паралельно з роботою користувачів. Такі робочі станції традиційно називають невиділеними серверами.

Консолі та втручання людини необхідні для серверів лише на етапі початкового встановлення, на етапі апаратного та технічного обслуговування, а також під час управління аварійними ситуаціями.

У цій дипломній роботі використовується сервер DHCP.

DHCP-сервер необхідний для великих мереж і для комфортної роботи з великою кількістю робочих станцій під час розширення мережі Основна роль DHCP-сервера полягає в автоматичному налаштуванні мережевих адаптерів робочих станцій, в даній роботі він розміщений на одному з мережевих пристроїв Mikrotik.

Протокол DHCP працює за принципом клієнт-сервер [4]. При запуску клієнтська робоча станція надсилає запит на отримання IP-адреси в мережу, а сервер у відповідь надсилає основні параметри конфігурації мережевого адаптера.

DHCP дозволяє автоматично встановити такі основні параметри:

- IP-адреса
- мережева маска
- шлюз за замовчуванням
- доменне ім'я
- DNS-сервер [3].

Розглянемо детальніше процес отримання даних від DHCP-сервера. DHCP-запит дозволяє клієнту вибрати IP-адресу для включення в DHCP-запит, надсилає IP-адресу, що міститься в DHCP-запиті.

Вибраний клієнтом сервер надсилає DHCPPACK, завершуючи розподіл IP-адреси. DHCPPACK містить адресу і час оренди, позначаючи сервер як такий, що вже використовує цю адресу, тобто недоступний для інших пристроїв.

Якщо клієнт відповідає на пакет DHCPDISCOVER, сервер надсилає DHCPREQUEST, якщо DHCPREQUEST відхилено, сервер надсилає клієнту

DHCPPACK і клієнт повинен повторно знайти адресу. [4] Формат, якщо DHCP-сервер успішно виділив IP-адресу (рис. 1.2).

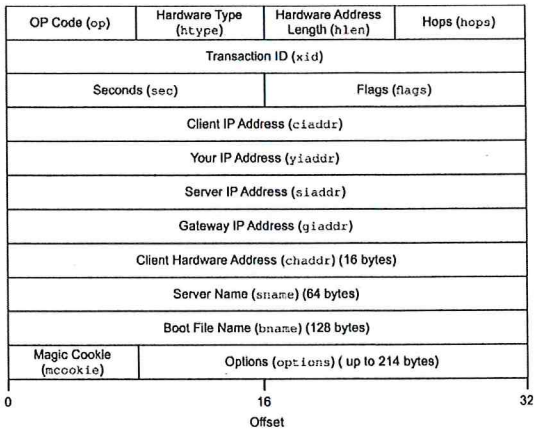


Рисунок 1.2 – Формат DHCP пакету

Тепер давайте розглянемо кожний елемент цього пакету:

– Op–тип повідомлення, може приймати значення BOOTREQUEST та BOOTREPLY.

– Htype – тип адреси.

– hlen – довжина адреси.

– Hops –кількість проміжних машрутизаторів.

– Xid – унікальний ідентифікатор процесу, що генерується клієнтом.

– Secs (час операції) –час в секундах, який був потрачений з моменту початку отримання адреси.

– Flags – спеціальні параметри DHCP.

– Ciaddr –IP-адреса клієнта.

– Yiaddr – нова IP-адрес клієнта.

– Siaddr – IP-адреса серверу.

– Giaddr – IP-адреса за замовчуванням.

– Chaddr – адреса обладнання.

– Sname – ім’я сервера.

– bname – завантажувальний файл.

– Options - додаткові налаштування.

DHCP-сервер працює в одному із трьох режимів:

– Статичний розподіл – аналогічний ручному введенню адрес для кожного пристрою.

– Автоматичний розподіл – сервер постійно призначає IP-адресу кожному клієнту в регіоні

– Динамічний розподіл – адмін мережі призначає діапазон адрес на сервері і кожен клієнтський пристрій повинен запитувати IP-адресу окремо.

Висновки до 1-го розділу:

У розглянутому розділі було детально охарактеризовано основні аспекти побудови корпоративної мережі, її архітектуру та вимоги до інфраструктури, яка повинна забезпечити надійний, безпечний та ефективний обмін даними для підтримки діяльності підприємства. Окрему увагу було приділено принципам побудови мережі, таким як модульність, гнучкість, масштабованість та відмовостійкість, які дозволяють адаптувати мережу до змін та забезпечувати стабільну роботу навіть в умовах зростання організації.

Також була розглянута ієрархічна модель мережі, що включає три основні рівні: рівень доступу, рівень розподілу та рівень ядра. Кожен з цих рівнів має свої функції і характеристики, які забезпечують ефективне функціонування корпоративної мережі.

Важливою складовою сучасних корпоративних мереж є інтернет-модуль, що з'єднує приватну мережу з глобальною мережею, а також використання спеціалізованих пристроїв, таких як фаєрволи, для захисту від зовнішніх загроз.

Додатково в тексті описано серверний модуль, який виконує важливі функції в управлінні мережевими пристроями, зокрема за допомогою DHCP-сервера, що автоматизує процес налаштування мережевих параметрів для робочих станцій, що значно спрощує управління великими мережами.

Отже, для створення ефективної та безпечної корпоративної мережі необхідно враховувати як технічні вимоги до її архітектури, так і інтеграцію з інтернет-сервісами, використання сучасних засобів захисту, а також забезпечення масштабованості та зручності в управлінні мережевою інфраструктурою.

РОЗДІЛ 2 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ З СИСТЕМАМИ ЗАХИСТУ

2.1 Основи функціонування корпоративної мережі

Спершу, перед розробкою мережі, вказано, що важливо розділити її на логічні модулі. Що дозволить, легко розширювати мережу при необхідності, додаючи нові компоненти або змінюючи наявні, не порушуючи цілісність всієї інфраструктури. Створити зручну і чітку структуру, яка спростить налаштування, управління та обслуговування мережі.

Модульний підхід дозволяє розглядати кожен блок окремо, що важливо для забезпечення масштабованості і зручності в подальшому розвитку мережі. Інтернет-модуль виконує роль шлюзу між корпоративною мережею і зовнішнім світом. Який включатиме, налаштований доступ в Інтернет: Це означає, що мережа буде підключена до глобальної мережі через спеціальний шлюз або канал зв'язку. Спеціальний зв'язок з дружньою організацією: Це додатковий канал для з'єднання з дружньою організацією, що забезпечує надійний та безпечний доступ між мережами через приватні лінії або інші типи зв'язку. Fortinet FortiGate 60F: Це фаєрвол, що забезпечує надійний захист від різноманітних загроз, таких як атаки або шкідливе програмне забезпечення, фільтруючи небажаний трафік і запобігаючи несанкціонованому доступу.

Для забезпечення автоматизації процесу розподілу IP-адрес у мережі буде використано DHCP-сервер. Оскільки мережа складається з великої кількості робочих станцій з різними операційними системами, важливо, щоб кожна станція отримувала унікальну IP-адресу для коректної роботи в мережі. DHCP-сервер автоматично надає IP-адреси, що спрощує адміністрування мережі і забезпечує безпеку.

DHCP-сервер на базі MikroTik: Цей сервер використовується для автоматичного присвоєння IP-адрес станціям в мережі. Налаштований DHCP-relay на рівні розподілу дозволяє передавати DHCP-запити між клієнтами та сервером, що важливо для налаштування зв'язку між різними сегментами мережі.

Мережа розділена на різні рівні для забезпечення ефективного зв'язку та доступу до ресурсів:

Рівень доступу: Це рівень, на якому підключаються кінцеві користувачі та їхні пристрої. Робочі станції на цьому рівні взаємодіють з іншими пристроями через комутатори рівня доступу.

Рівень розподілу: Цей рівень забезпечує зв'язок між ядром (основними серверами) та кінцевими пристроями. Тут здійснюється маршрутизація та агрегація трафіку, а також здійснюється передача даних між підмережами.

Рівень розподілу також включає налаштування IP-адресації для забезпечення правильного маршрутування трафіку між різними підмережами та модулями мережі.

Далі зазначається необхідність розробки IP-топології мережі, що передбачає правильне налаштування адресації для кожного сегмента мережі. Враховуючи наявність підключень до сторонніх організацій, важливо налаштувати специфічну адресу для кожного з підключених пристроїв та підмереж. Це також включає в себе визначення діапазонів IP-адрес для різних частин мережі та налаштування відповідних параметрів маршрутизації.

Таблиця з детальними параметрами адресації (зазначено в таблиці 2.1) містять конкретні дані щодо розподілу IP-адрес, які дозволяють коректно налаштувати з'єднання між модулями та підмережами.

Таблиця 2.1

Параметри адресації мережі

Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Інтернет модуль				
Мережевий екран Fortinet FortiGate 60F	int	Зовнішня IP-адреса	255.255.255.0	/24
	int	192.168.***.1	255.255.255.0	/24
	int	172.31.***.6	255.255.255.0	/24

Продовження таблиці 2.1

Параметри адресації мережі

Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Ядро				
Комутатор MikroTik DHCP_Server	int e0/0	192.168.***.2	255.255.255.0	/24
	int e1/0	192.168.***.3	255.255.255.0	/24
	int e1/1	192.168.***.4	255.255.255.0	/24
	int e1/2	192.168.***.5	255.255.255.0	/24
Рівень розподілу				
Комутатор MikroTik	int e1/0	192.168.***.*	255.255.255.0	/24
	int e2/0	192.168.***.*	255.255.255.0	/24
	int e3/0	192.168.***.*	255.255.255.0	/24
	int e0/0	192.168.***.*	255.255.255.0	/24
	int e0/1	192.168.***.*	255.255.255.0	/24
Комутатор MikroTik	int e1/1	192.168.***.*	255.255.255.0	/24
	int e2/1	192.168.***.*	255.255.255.0	/24
	int e3/1	192.168.***.*	255.255.255.0	/24
	int e0/0	192.168.***.*	255.255.255.0	/24
	int e0/1	192.168.***.*	255.255.255.0	/24
Комутатор MikroTik	int e1/2	192.168.***.*	255.255.255.0	/24
	int e2/2	192.168.***.*	255.255.255.0	/24
	int e3/2	192.168.***.*	255.255.255.0	/24
	int e0/0	192.168.***.*	255.255.255.0	/24
	int e0/1	192.168.***.*	255.255.255.0	/24
Комутатор MikroTik	int e1/2	192.168.***.*	255.255.255.0	/24
	int e2/2	192.168.***.*	255.255.255.0	/24
	int e3/2	192.168.***.*	255.255.255.0	/24
	int e0/0	192.168.***.*	255.255.255.0	/24

Продовження таблиці 2.1

Параметри адресації мережі

Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Рівень доступу				
Комутатор	Vlan	192.168.***.*	255.255.255.0	/24
Комутатор	Vlan	192.168.***.*	255.255.255.0	/24
Комутатор	Vlan	192.168.***.*	255.255.255.0	/24
Комутатор	Vlan	192.168.***.*	255.255.255.0	/24
Комутатор	Vlan	192.168.***.*	255.255.255.0	/24
Усі робочі станції	int e0	DHCP		

2.2 Формування логічної інфраструктури мережі

Трирівнева модель є однією з найбільш популярних архітектур для побудови корпоративних і великих організаційних мереж. Вона дозволяє забезпечити надійність, масштабованість та високопродуктивність завдяки чітко структурованому розподілу функцій на різних рівнях мережі. Кожен рівень має свою роль і відповідальність, що дозволяє покращити управління мережею та її ефективність.

У даному контексті, мережа буде складатися з трьох основних рівнів: ядра, розподілу, доступу, а також включатиме інтернет-модуль, який зв'язує мережу з зовнішнім світом.Ядро мережі є серцем інфраструктури, яке відповідає за швидку та ефективну маршрутизацію даних між різними сегментами мережі. Це рівень, який забезпечує:

Надійність: Ядро мережі зазвичай має високопродуктивне обладнання з максимальною надійністю, яке підтримує великі обсяги трафіку.

Швидкість: Оскільки ядро мережі займається лише маршрутизацією трафіку, необхідно, щоб воно працювало з дуже високою пропускною здатністю, щоб підтримувати високі швидкості передачі даних між іншими рівнями.

Централізоване управління: Ядро здійснює маршрутизацію між різними частинами мережі, що дозволяє централізовано контролювати зв'язки між підмережами та іншими ресурсами.

На рівні ядра будуть розміщені потужні маршрутизатори, які керують основними потоками даних і забезпечують зв'язок між різними частинами мережі та з зовнішніми мережами (наприклад, Інтернетом або іншими організаціями).Розподільчий рівень відіграє важливу роль у забезпеченні зв'язку між ядром і рівнем доступу. Він займається:

Маршрутизацією між підмережами: Розподільчий рівень забезпечує маршрутизацію трафіку між різними підмережами та дозволяє управляти політиками доступу і безпеки.

Ізоляцією трафіку: Цей рівень також відповідає за ізоляцію різних підмереж та обмеження трафіку між ними в разі необхідності (наприклад, для покращення безпеки).

Політики доступу та фільтрація: На цьому рівні можуть бути налаштовані правила доступу (ACL), фільтрація даних та інші засоби для контролю трафіку.

Окрім того, розподільчі комутатори або маршрутизатори можуть мати додаткові функції, такі як QoS (Quality of Service) для керування пріоритетами трафіку або VPN-шлюзи для забезпечення безпечного віддаленого доступу до мережі.

Рівень доступу безпосередньо взаємодіє з кінцевими користувачами та їх пристроями. На цьому рівні підключаються робочі станції, сервери, принтери, камери спостереження та інші кінцеві пристрої. Ось основні функції цього рівня:

Підключення кінцевих пристроїв: Рівень доступу забезпечує підключення різноманітних пристроїв до мережі через комутатори доступу (access switches).

Безпека: На рівні доступу можуть бути налаштовані механізми безпеки, такі як аутентифікація користувачів за допомогою 802.1X або фільтрація по MAC-адресах.

DHCP-розподіл: Рівень доступу може бути оснащений DHCP-ретрансляторами (DHCP-relay), які допомагають автоматично розподіляти IP-адреси кінцевим пристроям через сервер DHCP на рівні розподілу або ядра.

Цей рівень є найближчим до користувача, тому він також відповідає за збирання та управління даними, що надходять від кінцевих пристроїв.

Інтернет-модуль забезпечує підключення мережі до зовнішнього світу, тобто до Інтернету та інших мереж. Цей модуль є важливою частиною мережевої інфраструктури, оскільки він забезпечує:

Шлюз до Інтернету: Інтернет-модуль керує доступом до глобальної мережі Інтернет, може включати проксі-сервери, фаєрволи та системи фільтрації трафіку для забезпечення безпеки і контролю за доступом до Інтернету.

З'єднання з іншими організаціями: Інтернет-модуль може також забезпечувати з'єднання з іншими підприємствами або організаціями через спеціальні канали зв'язку, що дозволяє зберігати конфіденційність та безпеку даних.

Мережевий захист: За допомогою таких рішень як FortiGate 60F (вказаного раніше в тексті), інтернет-модуль може також виконувати функції фаєрволу, контролю за трафіком, виявлення та запобігання вторгненням (IDS/IPS), а також VPN-з'єднань для віддаленого доступу.

Інтернет-модуль також включає системи, які можуть підтримувати балансування навантаження та високу доступність для забезпечення безперебійного підключення до Інтернету та зовнішніх ресурсів.

Розглянемо кожен рівень окремо. Рівень ядра відповідає за високошвидкісний транспорт між пристроями розподільчого рівня, тобто між мережевими комутаторами, на яких налаштовані DHCP-сервери. На рівні ядра використовуються комутатори MicroTik.

Рівень розподілу знаходиться між рівнем ядра і рівнем доступу. Роль цього рівня полягає у забезпеченні мережевої маршрутизації та з'єднанні основного рівня і рівня доступу. Крім того, комутатори діють як DHCP-реле для розподілу IP-адрес.

Рівень доступу включає в себе комутатор, робочі станції та невиділений сервер для моніторингу та зручної роботи мережі, на якому встановлений мережевий антивірус.

Загальний вигляд мережі зображено схематично разом із зазначенням вищевказаних рівнів на рисунку 2.1.

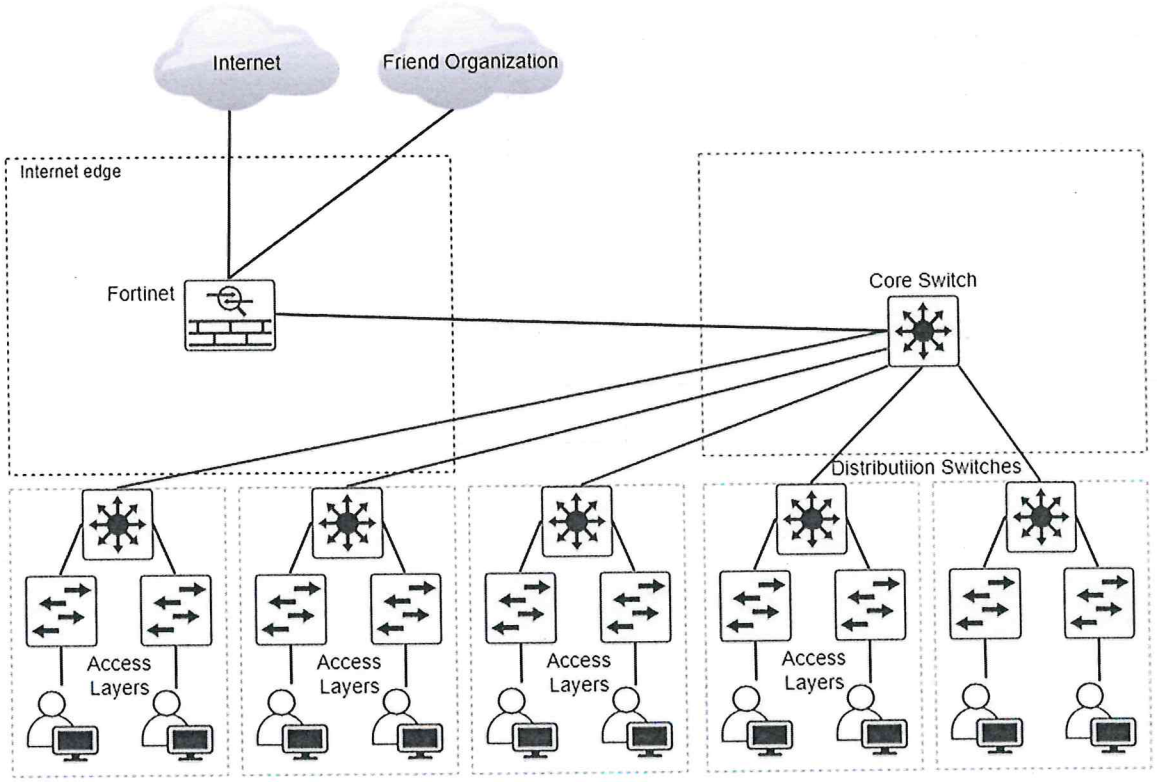


Рисунок 2.1 – Трирівнева ієрархічна модель мережі

Детально розглянемо кожен з рівнів окремо, зовнішній яких наведено на рисунках 2.2-2.5, пристрої, що входять до складу підмереж, зазначені в табл. 2.2-2.5.

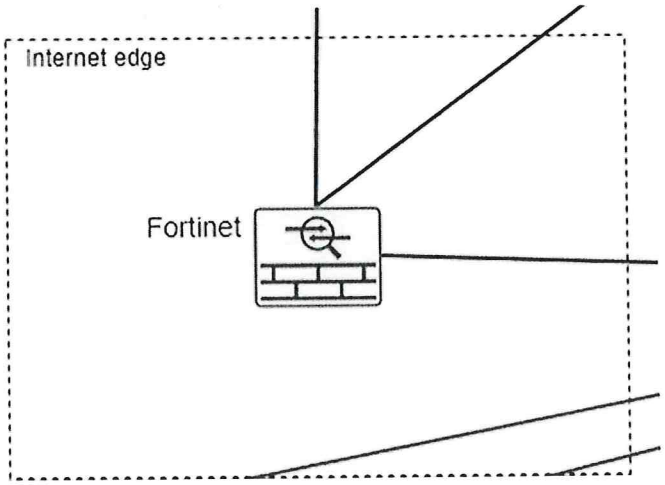


Рисунок 2.2 – Інтернет модуль

Таблиця 2.2

Інтернет модуль

Мережевий екран	Fortinet FortiGate 60F

Задля забезпечення надійної безпеки мережі в інтернет модулі був встановлений Fortinet FortiGate 60F [7].

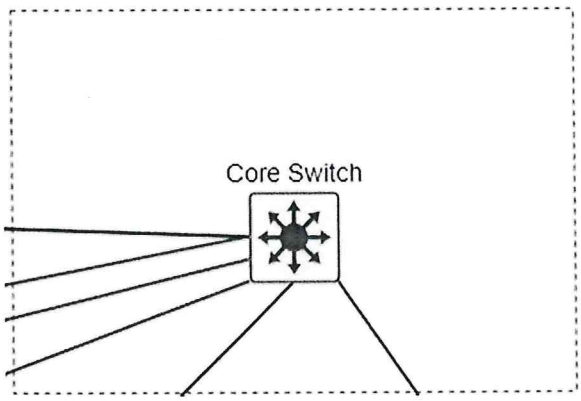


Рисунок 2.3 – Ядро з DHCP-сервером

Таблиця 2.3

Ядро з DHCP-сервером

Комутатор MikroTik	DHCP-сервер

Створено модуль ядра для забезпечення маскованої роботи мережі. Для спрощення процесу налаштування мережевих адаптерів на робочих станціях у мережі впроваджено DHCP-сервер.

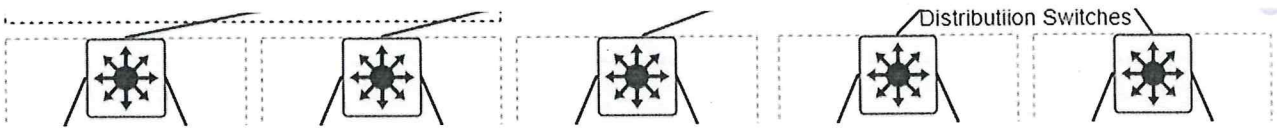


Рисунок 2.4 – Рівень розподілу

Таблиця 2.4

Рівень розподілу

Комутатори	MikroTik

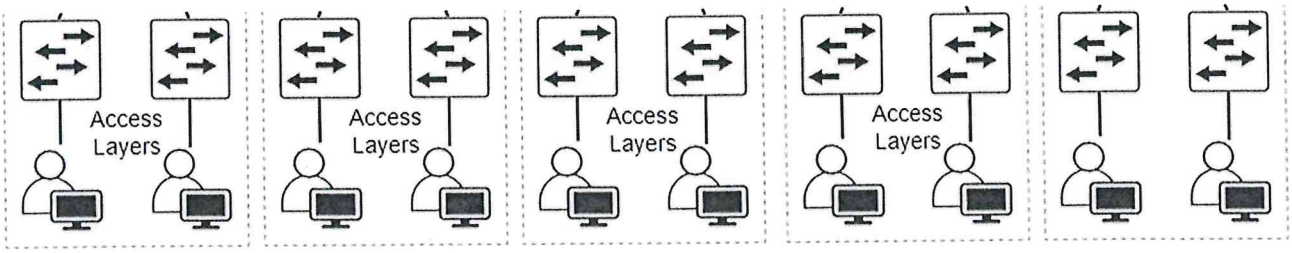


Рисунок 2.5 – Рівень доступу з робочими станціями

Також були встановлені дві робочі станції Windows10[5] з встановленим Log-сервером у якості невиділеного серверу на базі мережевого антивірусу.

Таблиця 2.5

Рівень доступу

Комутатори	Пустишки
Робочі станції	Windows11, 10, 7, XP.

Для забезбечення зв'язку між дружніми мережами було налаштовано адресацію.

2.3 Підбір технічних засобів і програмного забезпечення.

Відповідно до потреб, що зазначені вище, сформовано такі вимоги до програмно-апаратного забезпечення:

1. Використання робочих станцій Windows11, 10, 7, XP.
2. Невиділений сервер Windows10 з встановленим мережеви антивірусом.
3. Налаштування DHCP-серверу.
4. Наявність віддаленого захищеного доступу до пристроїв за допомогою WinBox.
5. Налаштування Fortinet FortiGate 60F, задля забезпечення надійного захисту мережі.

Захищеність мережі буде забезпечуватися: парольним доступом до пристроїв мережі, , створенням списків доступу, налаштуванням FortiGate 60F.

Для реалізації схеми будемо використовувати обладнання фірми MikroTik. Основними перевагами MikroTik перед іншими компаніями є:

1. Висока якість та надійність при розумних цінах. MikroTik пропонує обладнання, яке має високу якість виготовлення та стабільну роботу, проте ціна на його продукцію значно нижча порівняно з конкурентами. Це робить їх ідеальним вибором для організацій, які хочуть отримати надійне обладнання за помірну ціну. Такий баланс між ціною та якістю дозволяє зберігати ефективність мережі без значних капіталовкладень у закупівлю дорогих рішень.

2. Гнучкість і налаштування. Однією з ключових переваг MikroTik[2] є їх операційна система RouterOS, яка забезпечує велику кількість можливостей для налаштувань. Ця операційна система дозволяє детально налаштовувати всі параметри маршрутизації, безпеки, фільтрації трафіку та багато інших функцій. За допомогою RouterOS можна легко налаштувати:

- Маршрутизацію (включаючи статичні маршрути, RIP, OSPF, BGP);
- VPN-з'єднання (PPTP, L2TP, IPSec, OpenVPN);
- Фаєрволи та фільтрацію трафіку;
- QoS (Quality of Service) для управління трафіком;
- NAT (Network Address Translation);
- DHCP-сервери та DHCP-ретранслятори;
- Системи моніторингу та аналізу трафіку.

Це дозволяє створювати надзвичайно гнучкі та масштабовані мережі з деталізованим контролем над кожним аспектом їх функціонування.

3. Масштабованість. Продукти MikroTik підтримують різні рівні масштабування, що робить їх чудовим вибором для компаній будь-якого розміру — від малих офісів до великих підприємств та постачальників інтернет-послуг. В залежності від потреб, можна вибирати маршрутизатори та комутатори з різними характеристиками, які дозволяють створювати як невеликі локальні мережі, так і великі корпоративні інфраструктури.

Наприклад:

- RouterBoard та Cloud Core Router забезпечують високу продуктивність та достатньо потужні можливості для великих підприємств.

– MikroTik Switches підтримують великі обсяги трафіку та можуть бути налаштовані для використання в різних топологіях, таких як VLAN, Spanning Tree Protocol (STP), і т. п.

4. Висока продуктивність. MikroTik використовує сучасні компоненти та архітектуру для досягнення високої продуктивності в мережах різного масштабу. Наприклад, моделі таких пристроїв як CCR (Cloud Core Routers) оснащені багатоядерними процесорами та мають велику пропускну здатність, що дозволяє забезпечити стабільну роботу навіть при високих навантаженнях.

Продукти MikroTik мають оптимізовану обробку трафіку, що забезпечує швидку маршрутизацію і фільтрацію на високих швидкостях, що є важливим для організацій, які працюють з великими обсягами даних.

5. Широкий асортимент продуктів. MikroTik пропонує величезний вибір обладнання для різних типів мереж: від малих домашніх маршрутизаторів до потужних маршрутизаторів і комутаторів для великих підприємств або інтернет-провайдерів. Це дає можливість підібрати оптимальне обладнання для будь-якої організації, з урахуванням її специфічних потреб і бюджету.

– Маршрутизатори (RouterBoards, CCR) для централізованої маршрутизації;

– Комутатори (Switches) для підключення пристроїв до мережі;

– Бездротові точки доступу (Access Points) для організації Wi-Fi мережі;

– IP-телефонія та інші периферійні пристрої для повного інтегрованого рішення.

6. Підтримка VPN і безпеки. MikroTik забезпечує потужні функції для організації віртуальних приватних мереж (VPN), що дає змогу безпечно підключати віддалені офіси або співробітників до корпоративної мережі. Операційна система RouterOS підтримує такі протоколи, як IPSec, PPTP, L2TP, OpenVPN, що дозволяє створювати високозахищені з'єднання.

Що важливо, MikroTik активно розвиває функції безпеки, зокрема для фільтрації трафіку, побудови фаєрволів, контролю доступу та виявлення вторгнень.

7. Документація та підтримка спільноти. MikroTik має велике і активне співтовариство користувачів та розробників, що забезпечує обмін досвідом, допомогу в налаштуванні обладнання та оптимізації мереж. Крім того, компанія надає детальну документацію, навчальні матеріали, а також сертифікаційні курси (MTCNA, MTCRE, MTCWE тощо), що дозволяє швидко освоїти налаштування та адміністрування обладнання.

8. Підтримка автоматизації та моніторингу. Обладнання MikroTik дозволяє реалізувати автоматизацію задач і моніторинг стану мережі. Можна налаштувати автоматичне реагування на різні ситуації (наприклад, на зміни в мережевій топології або стані пристроїв) за допомогою скриптів на RouterOS. Це дає змогу швидко налаштувати безперервний моніторинг мережі і забезпечити своєчасне виявлення та усунення проблем.

9. Надійна підтримка SNMP і інших стандартів. MikroTik підтримує SNMP (Simple Network Management Protocol), що дозволяє організувати централізоване управління мережею, а також інтегрувати її з іншими системами моніторингу та управління.

З цього, виходить висновок, прилади MikroTik є найкращими у сферах захисту, налаштувань та надійності. У ході роботи будуть використовуватися образи комутатори MikroTik CRS326-24G-2S+IN та FortiGate 60F (рис. 2.6-7).

Для перевірки трафіку та вразливостей в мережі буде використовуватися WireShark.

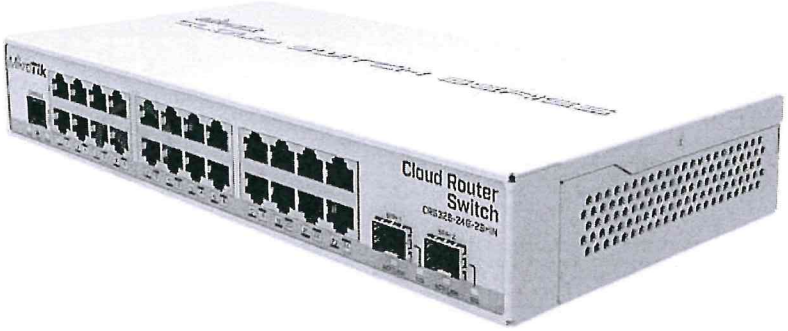


Рисунок 2.6 – Комутатор MikroTik CRS326-24G-2S+IN

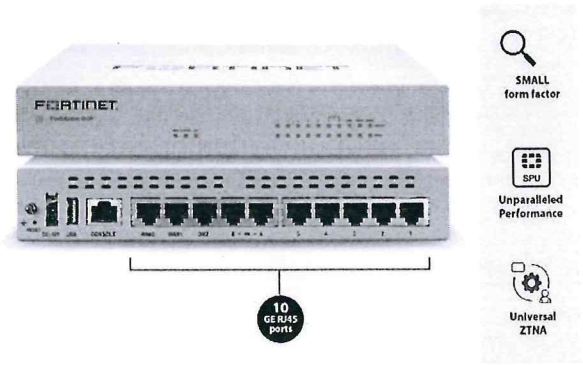


Рисунок 2.7 – Мережевий екран (FortiGate 60F)

Wireshark — це потужний та широко використовуваний інструмент для захоплення та аналізу мережевих пакетів. Він дозволяє досліджувати деталі мережевого трафіку в реальному часі, що робить його незамінним інструментом для мережевих адміністраторів, спеціалістів із безпеки та розробників.[11]

Основні характеристики та можливості Wireshark:

Захоплення мережевого трафіку: Wireshark може перехоплювати пакети, які проходять через мережевий інтерфейс вашого пристрою. Це можуть бути як дротові, так і бездротові мережі (наприклад, Ethernet, Wi-Fi).

Підтримка великої кількості протоколів: Wireshark підтримує аналіз понад 2000 різних мережевих протоколів, серед яких:

- Ethernet
- TCP, UDP
- IP, IPv6
- HTTP, HTTPS, FTP, DNS
- SMB, ICMP, ARP та багато інших.

Програма дозволяє детально аналізувати кожен пакет, включаючи заголовки, дані та метадані.

Інтерфейс та зручність використання: Wireshark має зручний графічний інтерфейс, у якому пакети відображаються у вигляді списків, і можна переглядати деталі кожного пакета. Це включає інформацію про протоколи, адреси відправника та отримувача, порти та інші характеристики.

Фільтрація пакетів: Wireshark надає потужні можливості для фільтрації захоплених даних як під час захоплення, так і після збору даних. Це дозволяє

швидко знаходити потрібну інформацію серед великої кількості пакетів. Приклад фільтрів:

- Фільтрація за IP-адресою, портом, протоколом.
- Вибірка тільки TCP або UDP пакетів.
- Пошук пакетів з помилками або втрачених.

Реконструкція протоколів: Wireshark може відновлювати та аналізувати послідовності мережевих сесій, наприклад, для аналізу HTTP-запитів і відповідей або відстеження з'єднань TCP.

Аналіз у реальному часі: Wireshark дозволяє відстежувати трафік у реальному часі, що допомагає оперативно виявляти проблеми в мережі або підозрілу активність.

Розширена статистика: Wireshark надає статистику по трафіку, включаючи:

- Кількість переданих пакетів по протоколах.
- Графіки розподілу пакетів за часом.
- Аналіз потоків даних та помилок у передачі.

Робота з великими об'ємами даних: Wireshark підтримує роботу з великими файлами захоплених пакетів і дозволяє ефективно шукати та аналізувати дані, навіть якщо трафік був дуже інтенсивним.

Портативність і кросплатформність: Wireshark доступний для різних операційних систем, таких як Windows, Kali Linux[6] та macOS, що робить його зручним інструментом для різних користувачів і сценаріїв.

Відкритий вихідний код: Wireshark — це безкоштовна програма з відкритим вихідним кодом. Вона постійно розвивається та підтримується спільнотою, що дозволяє регулярно оновлювати інструмент і додавати нові можливості.

Застосування Wireshark:

Діагностика та вирішення мережевих проблем: Wireshark допомагає визначити причини мережевих проблем, таких як втрата пакетів, затримки, проблеми з з'єднанням або неправильно налаштовані пристрої.

Безпека та аналіз загроз: Інструмент використовується для аналізу мережевих атак, таких як перехоплення даних (сніффінг), атаки "man-in-the-middle" або для виявлення аномалій у мережевому трафіку.

Аналіз продуктивності: Wireshark допомагає моніторити та оптимізувати продуктивність мережевих додатків, а також вивчати ефективність використання мережевих ресурсів.

Wireshark — це незамінний інструмент для професіоналів у галузі мережевих технологій та інформаційної безпеки.

Висновки до 2-го розділу:

Мережу поділяють на кілька логічних модулів для зручності управління та масштабування. Інтернет-модуль відповідає за підключення до зовнішнього світу через шлюз, а для забезпечення безпеки використовують фаєрвол FortiGate 60F, який контролює трафік і фільтрує непотрібні чи шкідливі з'єднання. Відповідальність за автоматичну видачу IP-адрес до робочих станцій лежить на DHCP-сервері MikroTik, що значно полегшує адміністрування.

Мережа поділяється на кілька рівнів: рівень доступу (який містить робочі станції та кінцеві пристрої), рівень розподілу (для обробки та маршрутизації трафіку) та рівень ядра, що забезпечує високошвидкісне з'єднання між основними мережевими пристроями. Правильне налаштування IP-адресації для кожного сегмента є важливим для ефективної роботи мережі.

Для забезпечення маршрутизації та фільтрації трафіку використовуються комутатор MikroTik та фаєрвол FortiGate 60F. MikroTik дає змогу налаштовувати мережу гнучко і ефективно, а FortiGate надає додатковий рівень безпеки, захищаючи мережу від несанкціонованого доступу, атак та іншого шкідливого трафіку.

Для моніторингу та аналізу мережевих проблем використовують інструмент Wireshark, який дозволяє детально аналізувати мережеві пакети, перевіряти трафік на наявність вразливостей і знаходити потенційні проблеми в роботі мережі.

РОЗДІЛ 3 НАЛАШТУВАННЯ І ТЕСТУВАННЯ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ.

3.1 Процес налаштування корпоративної мережі

В даному пункті буде розглянуто основні налаштування пристроїв мережі. Спочатку повністю складемо схему, яку спроектували в попередньому розділі (рис.3.1).

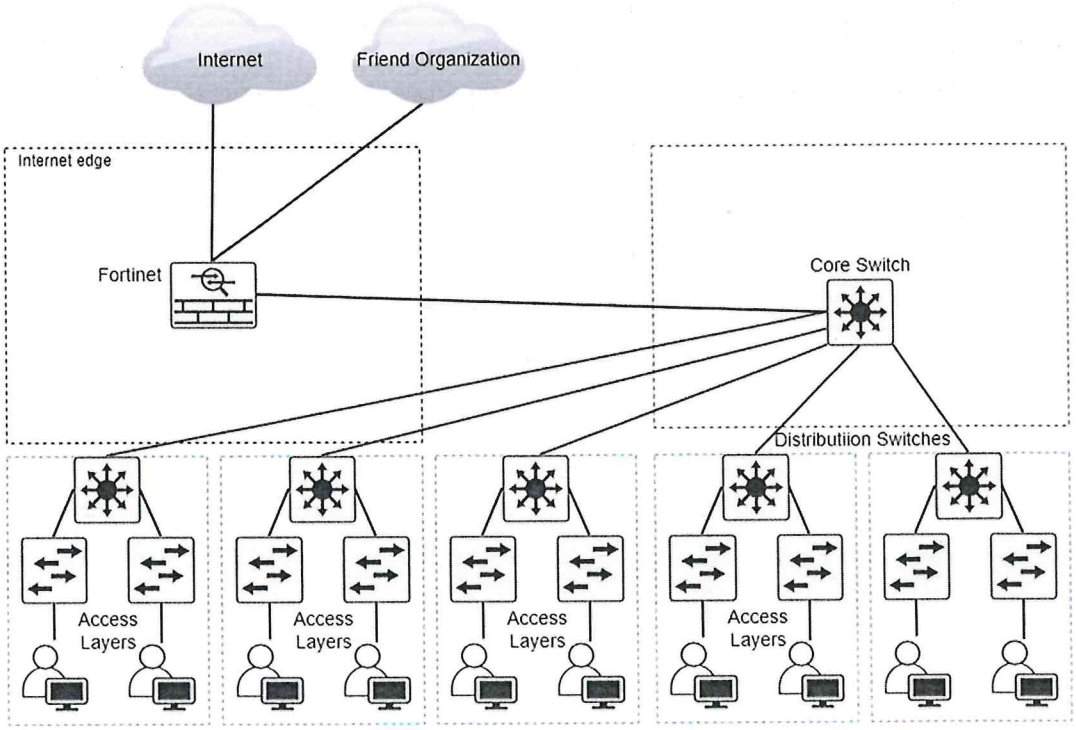


Рисунок 3.1 – Повна схема мережі

По-перше, перед початком базової конфігурації пристрій повинен бути надійно захищений як від віддаленого, так і від фізичного доступу: Оскільки існує два варіанти входу в пристрій MikroTik, консольний і віддалений, кожен з цих способів повинен бути надійно захищений. Без цього зловмисник за допомогою декількох команд, зможе зібрати достатньо інформації про мережу і тип самим знайти її слабкості(рис.3.2).

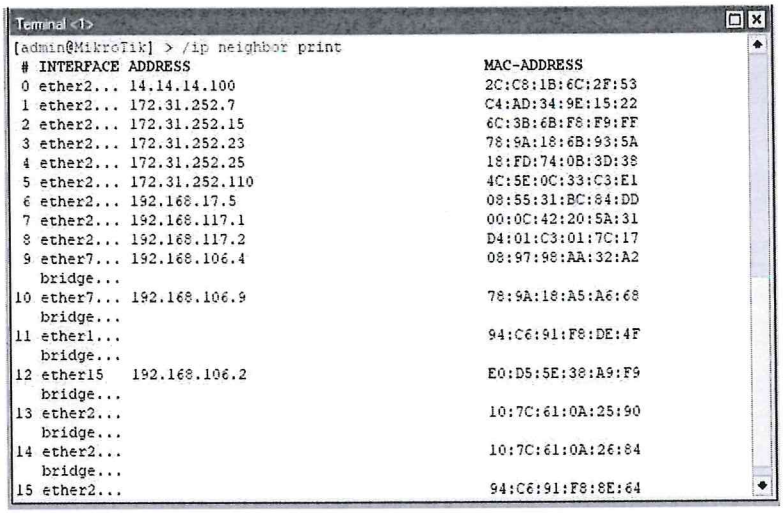


Рисунок 3.2 – Виконання команди /ip neighnor print

Отже, зловмисник може знати IP-адресу мережевого адаптера і версію пристрою, тому доступ до консолі слід заборонити навіть у режимі користувача. Тепер перейдемо до налаштування.(рис. 3.3)

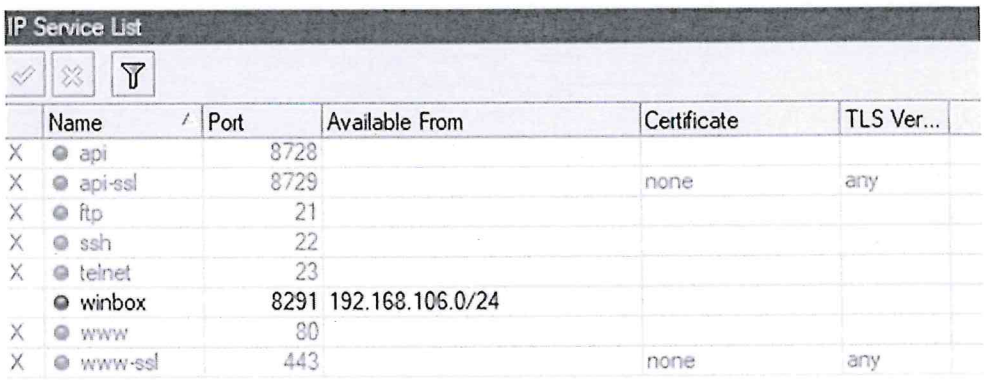


Рисунок 3.3 – Налаштування доступу тільки через Winbox лише для відповідної мережі

Тепер необхідно пояснити, чому необхідні подібні налаштування, покажемо це все на прикладі(рис. 3.4).

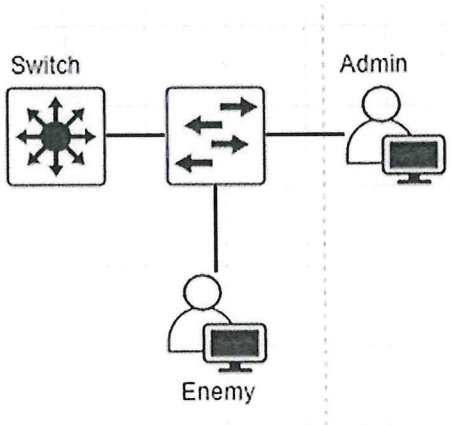


Рисунок 3.4 – Приклад мережі

Уявимо, зловмисник підключається до нашої мережі, а адміністратор не знає про це. В цей час зловмисник перехопить весь цей трафік.

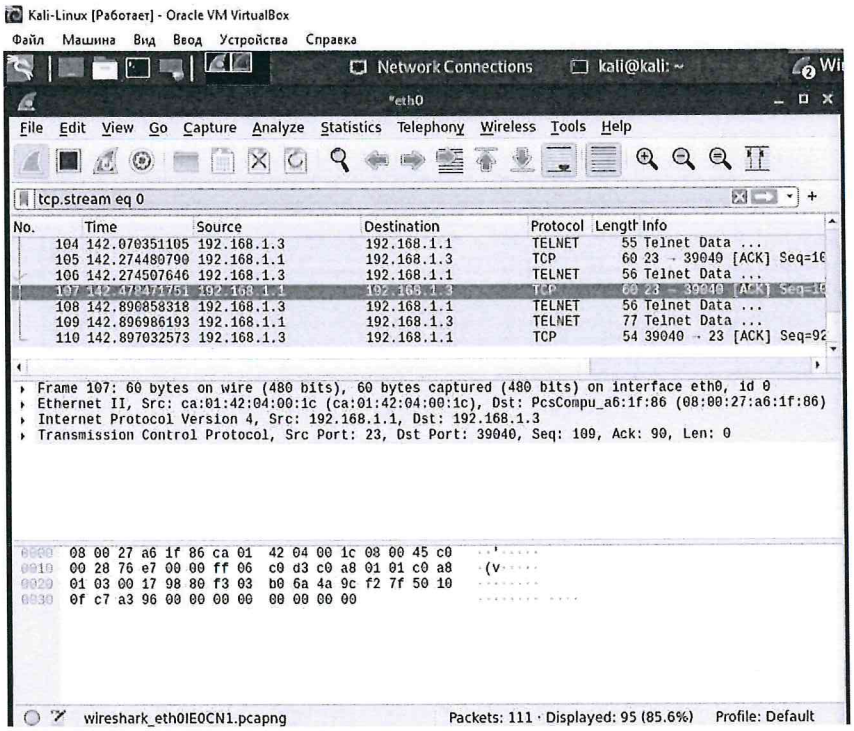


Рисунок 3.5 – Перехоплені пакети на інтерфейсі

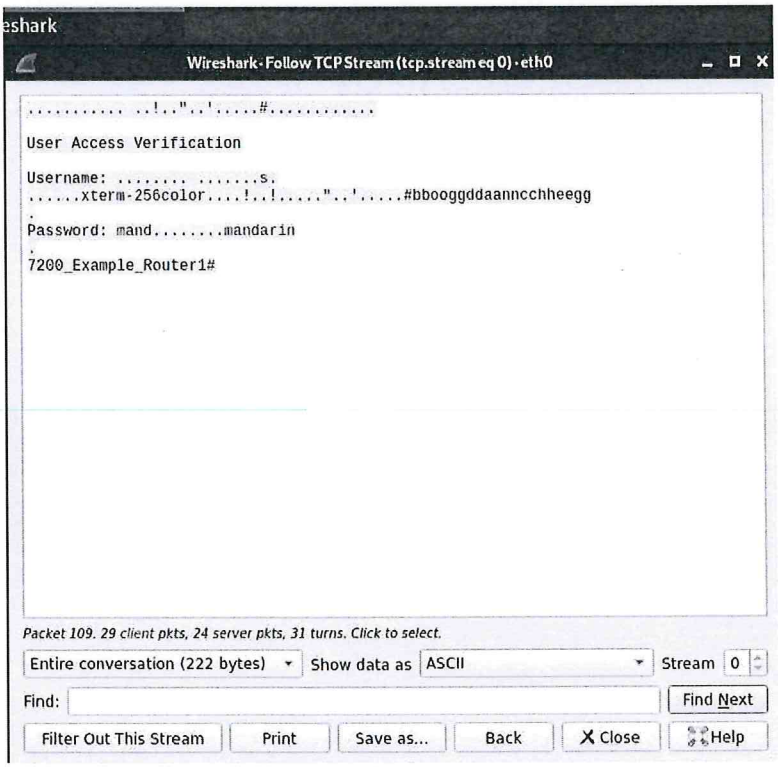


Рисунок 3.6 – Перехоплений пакет

Як видно з рисунків 3.5 та 3.6, зловмисник перехопив пакети та дізнався ім'я користувача та пароль. З цієї причини під час налаштування мережі було заборонено використовувати всі протоколи віддаленого підключення, окрім графічного інтерфейсу Wirtualbox, лише на необхідних мережах.

У цьому випадку зловмисник не зможе побачити логін і пароль і нейтралізувати блокування трафіку.

Після отримання віддаленого доступу до пристрою необхідно налаштувати списки доступу до пристрою та захист від перебору, щоб звичайні користувачі мережі не змогли втрутитися в конфігурацію пристрою та пошкодити мережу. Відповідні налаштування показані на рисунку 3.7.

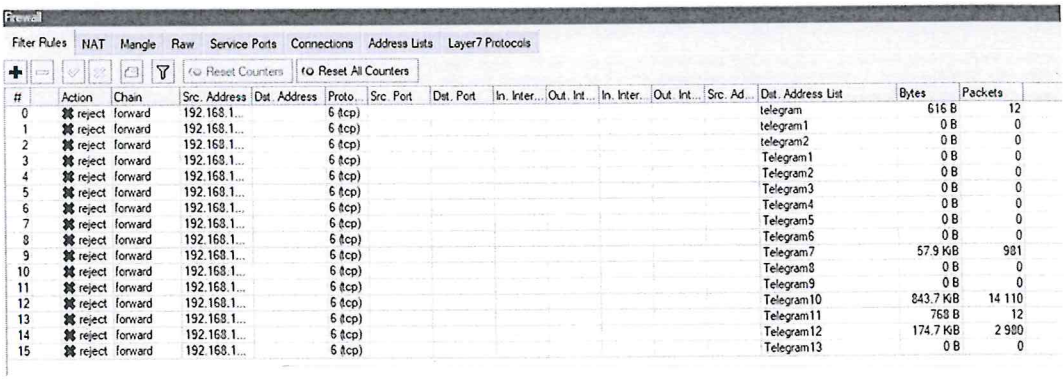
```
/ip firewall filter
add action=drop chain=input comment="drop ssh brute forcers" dst-port=22 protocol=tcp src-address-list=ssh_blacklist
add action=add-src-to-address-list address-list=ssh_blacklist address-list-timeout=1h chain=input connection-state=new dst-
port=22 protocol=tcp src-address-list=ssh_stage3
add action=add-src-to-address-list address-list=ssh_stage3 address-list-timeout=20s chain=input connection-state=new dst-
port=22 protocol=tcp src-address-list=ssh_stage2
add action=add-src-to-address-list address-list=ssh_stage2 address-list-timeout=20s chain=input connection-state=new dst-
port=22 protocol=tcp src-address-list=ssh_stage1
add action=add-src-to-address-list address-list=ssh_stage1 address-list-timeout=20s chain=input connection-state=new dst-
port=22 protocol=tcp
add action=drop chain=input comment="Protected - WinBox Access" src-address-list="Black List Winbox"
add action=add-src-to-address-list address-list="Black List Winbox" address-list-timeout=none-dynamic chain=input connection-
state=new dst-port=8291 in-interface-list=WAN log=\
yes log-prefix="BLACK WINBOX" protocol=tcp src-address-list="Winbox Stage 3"
add action=add-src-to-address-list address-list="Winbox Stage 3" address-list-timeout=1m chain=input connection-state=new dst-
port=8291 in-interface-list=WAN protocol=tcp \
src-address-list="Winbox Stage 2"
add action=add-src-to-address-list address-list="Winbox Stage 2" address-list-timeout=1m chain=input connection-state=new dst-
port=8291 in-interface-list=WAN protocol=tcp \
src-address-list="Winbox Stage 1"
add action=add-src-to-address-list address-list="Winbox Stage 1" address-list-timeout=1m chain=input connection-state=new dst-
port=8291 in-interface-list=WAN protocol=tcp
add action=accept chain=input dst-port=8291 in-interface-list=WAN protocol=tcp
```

Рисунок 3.7 – Налаштування списків доступу та захисту від brute force

Логіка процесу тут наступна: Коли ви підключаєтеся до роутера через порт 8291, ви переходите в новий стан з'єднання, і правило додає IP-адресу до списку 1-го рівня. Якщо ви відключаєтеся без входу в систему і намагаєтеся підключитися знову, ви знову переходите в новий стан підключення. У цьому випадку IP-адреса вже знаходиться в списку 1. Тому IP-адреса додається до списку 2 і залишається в цьому стані, поки не буде заблокована правилом 13, а правило 12 не заблокує нове з'єднання з роутером через порт 8291. Після входу в систему

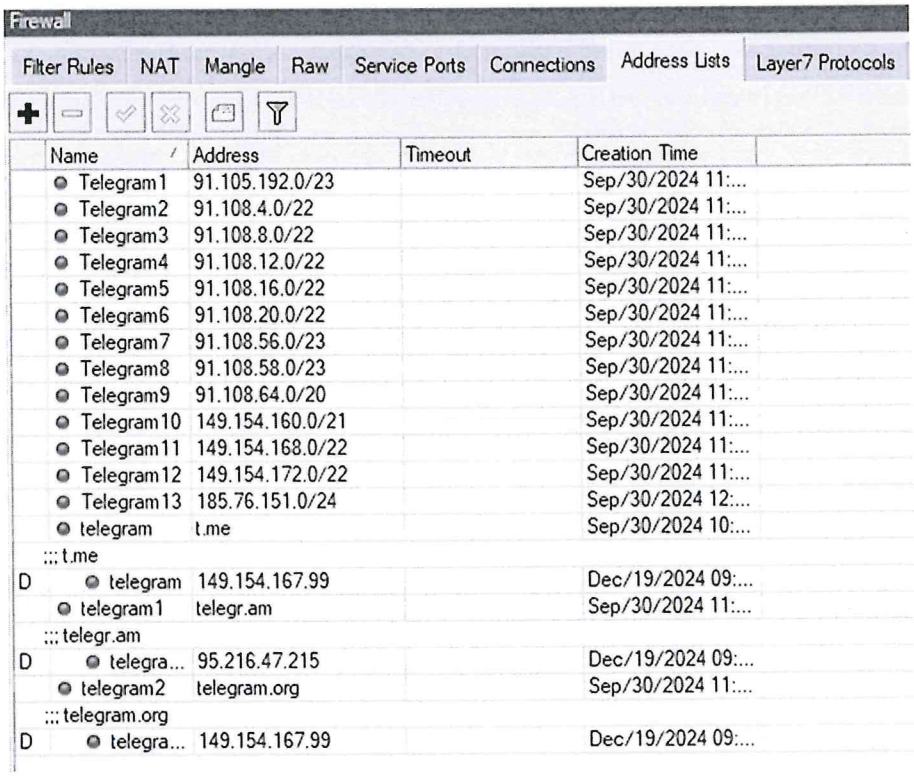
з'єднання перемикається з нового стану на встановлений, і воно вже обробляється за допомогою правил найвищого рівня 2, які дозволяють все. Коротше кажучи, у зловмисника є лише чотири можливості увійти до роутера через порт WinBox.

Також оскільки робочим органом Ради національної безпеки і оборони України – Національним координаційним центром кібербезпеки за результатами розгляду 19 вересня 2024 року питань щодо мінімізації кіберзагроз, пов'язаних із месенджером Telegram, було прийняте відповідне протокольне рішення про обмеження доступу до месенджеру в організаціях, були проведені відповідні налаштування за допомогою пристроїв MikroTik та мережевого антивірусу, що зображено на рисунках 3.8-14.



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter.	Out. Int...	Src. Ad...	Dst. Address List	Bytes	Packets
0	reject	forward	192.168.1...		6 (tcp)								telegram	616 B	12
1	reject	forward	192.168.1...		6 (tcp)								telegram1	0 B	0
2	reject	forward	192.168.1...		6 (tcp)								telegram2	0 B	0
3	reject	forward	192.168.1...		6 (tcp)								Telegram1	0 B	0
4	reject	forward	192.168.1...		6 (tcp)								Telegram2	0 B	0
5	reject	forward	192.168.1...		6 (tcp)								Telegram3	0 B	0
6	reject	forward	192.168.1...		6 (tcp)								Telegram4	0 B	0
7	reject	forward	192.168.1...		6 (tcp)								Telegram5	0 B	0
8	reject	forward	192.168.1...		6 (tcp)								Telegram6	0 B	0
9	reject	forward	192.168.1...		6 (tcp)								Telegram7	57.9 KiB	981
10	reject	forward	192.168.1...		6 (tcp)								Telegram8	0 B	0
11	reject	forward	192.168.1...		6 (tcp)								Telegram9	0 B	0
12	reject	forward	192.168.1...		6 (tcp)								Telegram10	843.7 KiB	14 110
13	reject	forward	192.168.1...		6 (tcp)								Telegram11	768 B	12
14	reject	forward	192.168.1...		6 (tcp)								Telegram12	174.7 KiB	2 980
15	reject	forward	192.168.1...		6 (tcp)								Telegram13	0 B	0

Рисунок 3.8 – Налаштування фільтрів Firewall



	Name	Address	Timeout	Creation Time
	Telegram1	91.105.192.0/23		Sep/30/2024 11:...
	Telegram2	91.108.4.0/22		Sep/30/2024 11:...
	Telegram3	91.108.8.0/22		Sep/30/2024 11:...
	Telegram4	91.108.12.0/22		Sep/30/2024 11:...
	Telegram5	91.108.16.0/22		Sep/30/2024 11:...
	Telegram6	91.108.20.0/22		Sep/30/2024 11:...
	Telegram7	91.108.56.0/23		Sep/30/2024 11:...
	Telegram8	91.108.58.0/23		Sep/30/2024 11:...
	Telegram9	91.108.64.0/20		Sep/30/2024 11:...
	Telegram10	149.154.160.0/21		Sep/30/2024 11:...
	Telegram11	149.154.168.0/22		Sep/30/2024 11:...
	Telegram12	149.154.172.0/22		Sep/30/2024 11:...
	Telegram13	185.76.151.0/24		Sep/30/2024 12:...
	telegram	t.me		Sep/30/2024 10:...
	;;; t.me			
D	telegram	149.154.167.99		Dec/19/2024 09:...
	telegram1	telegr.am		Sep/30/2024 11:...
	;;; telegr.am			
D	telegra...	95.216.47.215		Dec/19/2024 09:...
	telegram2	telegram.org		Sep/30/2024 11:...
	;;; telegram.org			
D	telegra...	149.154.167.99		Dec/19/2024 09:...

Рисунок 3.9 – Створення відповідних списків для блокування

988	Dec/25/2024 10:11:42	memory	firewall, info	forward: in:bridge-local out:ether1-INTERNET, src-mac 94:c6:91:f8:dc:9a, proto TCP (SYN), 192.168.106.208:59117->149.154.167.220:443, len 52
989	Dec/25/2024 10:11:50	memory	firewall, info	forward: in:bridge-local out:ether1-INTERNET, src-mac 94:c6:91:f8:dc:9a, proto TCP (SYN), 192.168.106.208:59117->149.154.167.220:443, len 52
990	Dec/25/2024 10:13:38	memory	firewall, info	forward: in:bridge-local out:ether1-INTERNET, src-mac 94:c6:91:f8:dc:9a, proto TCP (SYN), 192.168.106.208:59162->149.154.167.220:443, len 52
991	Dec/25/2024 10:13:39	memory	firewall, info	forward: in:bridge-local out:ether1-INTERNET, src-mac 94:c6:91:f8:dc:9a, proto TCP (SYN), 192.168.106.208:59162->149.154.167.220:443, len 52
992	Dec/25/2024 10:13:41	memory	firewall, info	forward: in:bridge-local out:ether1-INTERNET, src-mac 94:c6:91:f8:dc:9a, proto TCP (SYN), 192.168.106.208:59162->149.154.167.220:443, len 52
993	Dec/25/2024 10:13:45	memory	firewall, info	forward: in:bridge-local out:ether1-INTERNET, src-mac 94:c6:91:f8:dc:9a, proto TCP (SYN), 192.168.106.208:59162->149.154.167.220:443, len 52
994	Dec/25/2024 10:13:53	memory	firewall, info	forward: in:bridge-local out:ether1-INTERNET, src-mac 94:c6:91:f8:dc:9a, proto TCP (SYN), 192.168.106.208:59162->149.154.167.220:443, len 52
995	Dec/25/2024 10:15:40	memory	firewall, info	forward: in:bridge-local out:ether1-INTERNET, src-mac 94:c6:91:f8:dc:9a, proto TCP (SYN), 192.168.106.208:59207->149.154.167.220:443, len 52
996	Dec/25/2024 10:15:41	memory	firewall, info	forward: in:bridge-local out:ether1-INTERNET, src-mac 94:c6:91:f8:dc:9a, proto TCP (SYN), 192.168.106.208:59207->149.154.167.220:443, len 52
997	Dec/25/2024 10:15:43	memory	firewall, info	forward: in:bridge-local out:ether1-INTERNET, src-mac 94:c6:91:f8:dc:9a, proto TCP (SYN), 192.168.106.208:59207->149.154.167.220:443, len 52
998	Dec/25/2024 10:15:47	memory	firewall, info	forward: in:bridge-local out:ether1-INTERNET, src-mac 94:c6:91:f8:dc:9a, proto TCP (SYN), 192.168.106.208:59207->149.154.167.220:443, len 52
999	Dec/25/2024 10:15:55	memory	firewall, info	forward: in:bridge-local out:ether1-INTERNET, src-mac 94:c6:91:f8:dc:9a, proto TCP (SYN), 192.168.106.208:59207->149.154.167.220:443, len 52

Рисунок 3.10 – Перегляд Log файлу

Тепер перейдемо безпосередньо до налаштування мережевого антивірусу ESET.

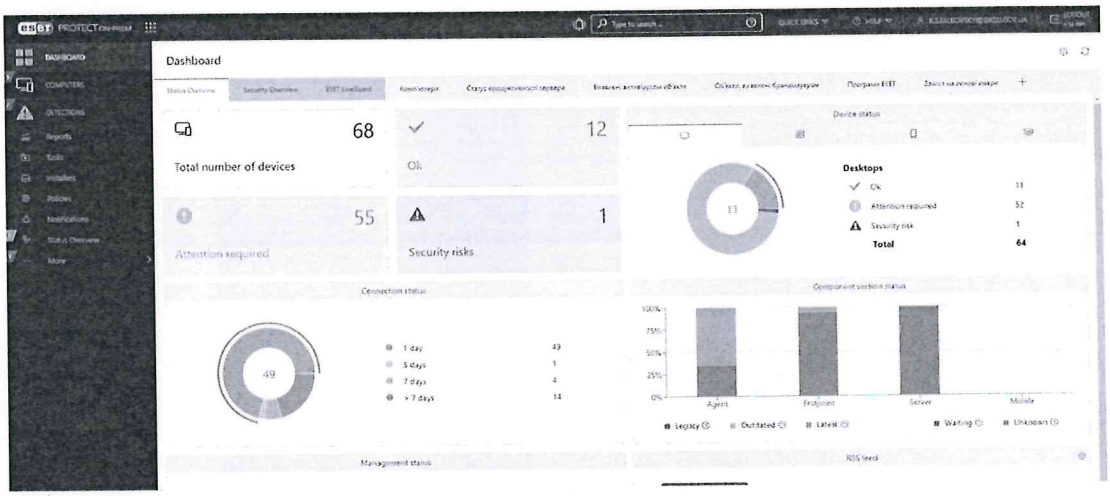


Рисунок 3.11 – Головна панель антивірусу

Після успішного входу, необхідно створити нову політику. Налаштування якої відбувається на рис.3.12-14.

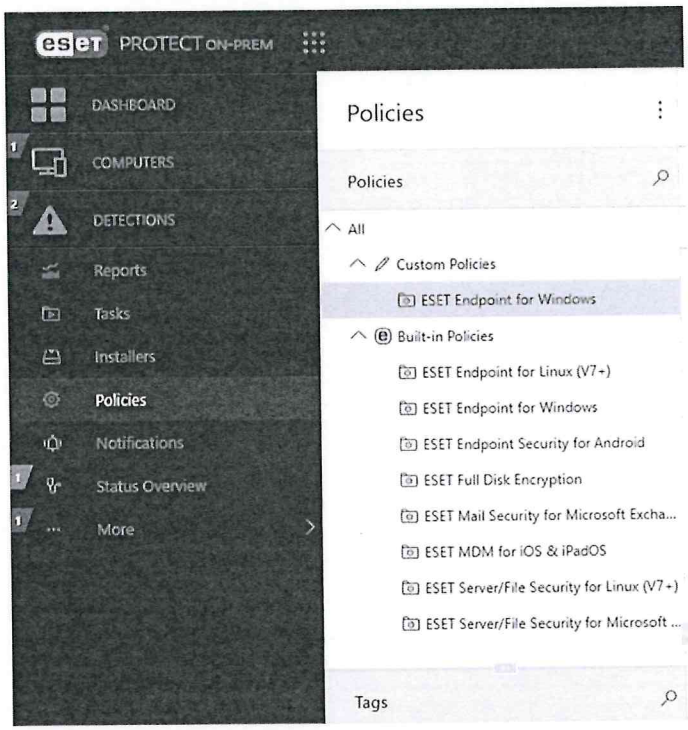


Рисунок 3.12 – Створення нової політики

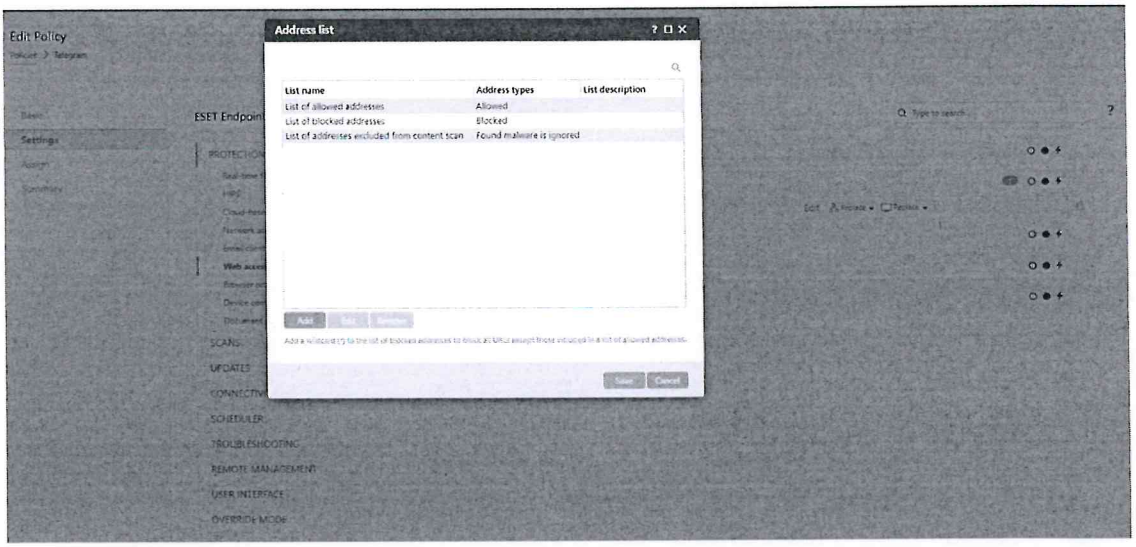


Рисунок 3.13 – Додавання обмежень для підключення

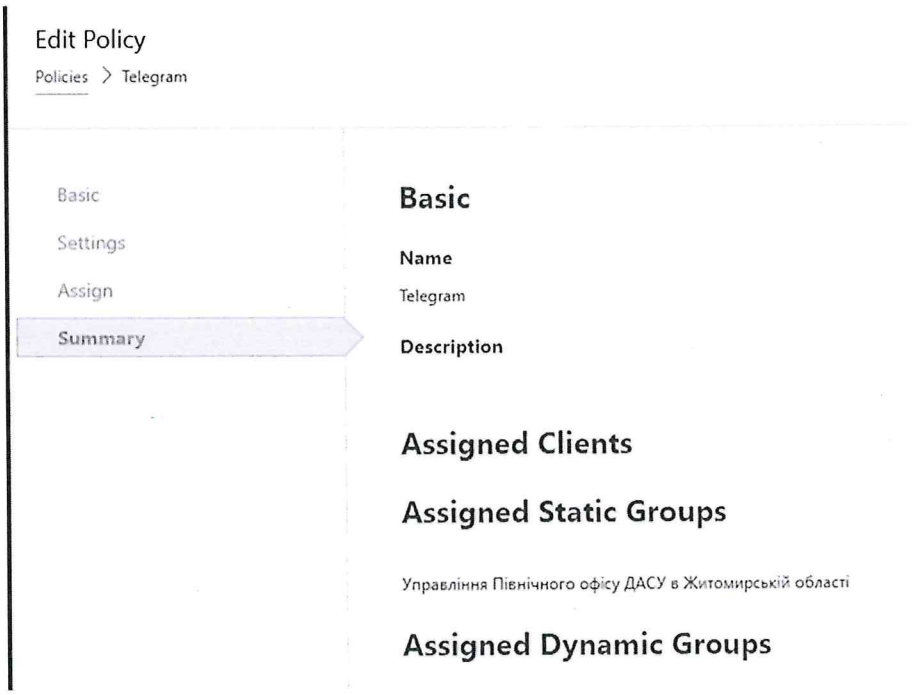


Рисунок 3.14 – Успішне додавання обмежень для підключення

Далі налаштуємо DHCP-сервер на базі комутатора MikroTik.(рис.3.15-3.20).

Для початку потрібно зайти в меню налаштувань DHCP-сервера. Для цього відкриваємо меню MikroTik і вибираємо пункт DHCP Server. Після цього натискаємо кнопку DHCP Setup, щоб розпочати процес налаштування DHCP-сервера.

У вікні налаштування DHCP-сервера потрібно вказати інтерфейс, через який сервер буде роздавати IP-адреси. Зазвичай це інтерфейс, підключений до локальної мережі, наприклад, інтерфейс LAN.

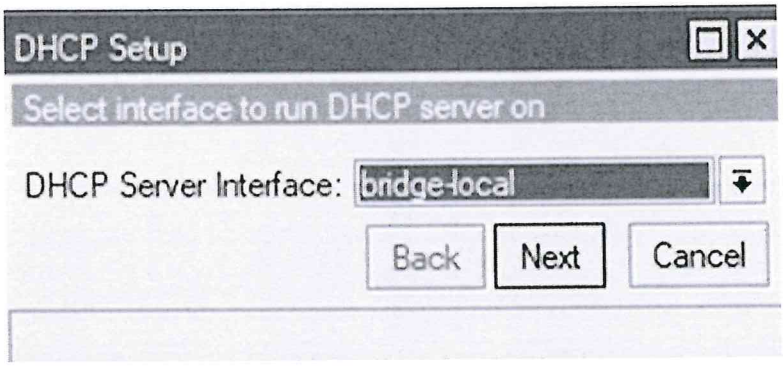


Рисунок 3.15 – Додаємо інтерфейс на які DHCP Server буде роздавати адреси

На наступньому етапі вказуємо мережу, в якій буде працювати DHCP-сервер. Це важливий крок, оскільки DHCP-сервер повинен працювати в конкретній підмережі.

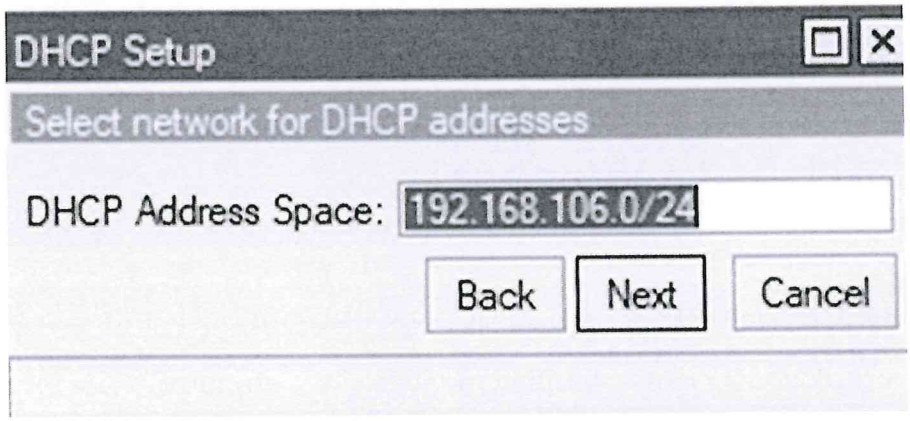


Рисунок 3.16 – В цьому вікні обирається мережа

Тепер потрібно визначити діапазон IP-адрес, які DHCP-сервер буде роздавати клієнтам. Вказуємо мінімальну та максимальну IP-адреси, щоб сервер знав, в якому діапазоні видавати адреси.

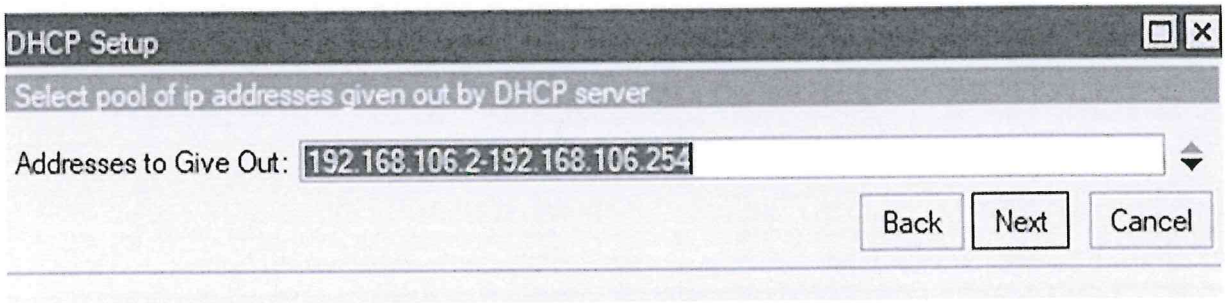


Рисунок 3.17 – Прописуємо діапазон адрес які будуть роздаватися

Наступним кроком є налаштування DNS-серверів, які будуть використовувати клієнти, що підключатимуться через DHCP.

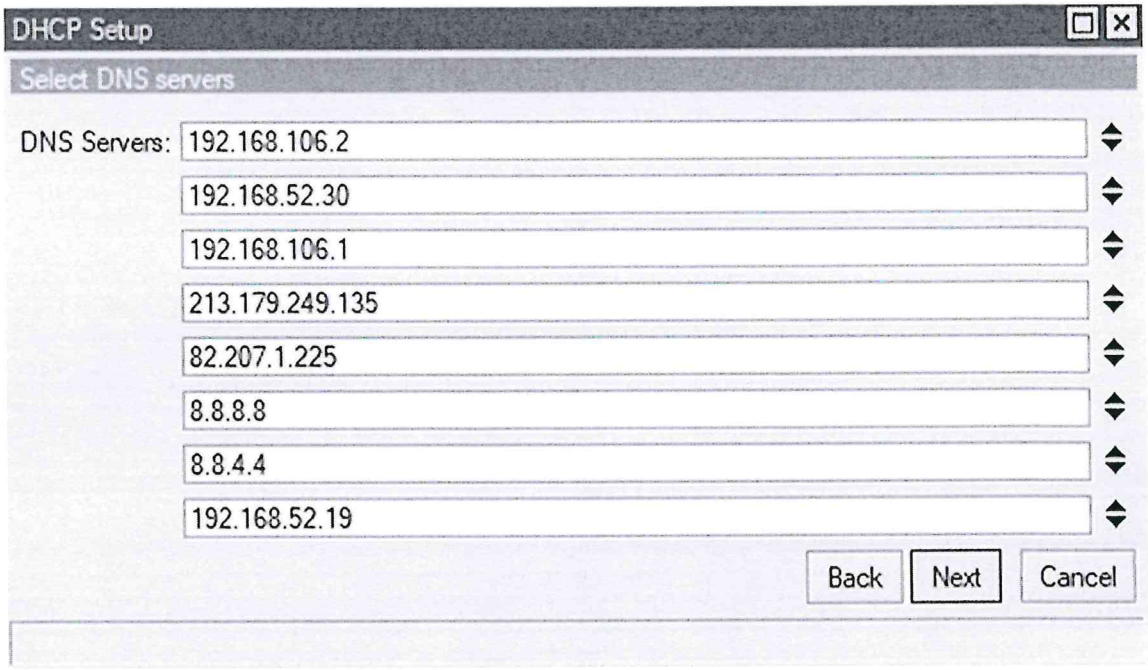


Рисунок 3.18 – Проводимо налаштування DNS

Останнім кроком налаштовуємо час резервування IP-адрес для клієтів. Це дозволяє гарантувати, що клієнт отримає одну й ту саму IP-адресу при кожному наступному підключенні, якщо адресу не була зайнята або ще не був вичерпаний час оренди.

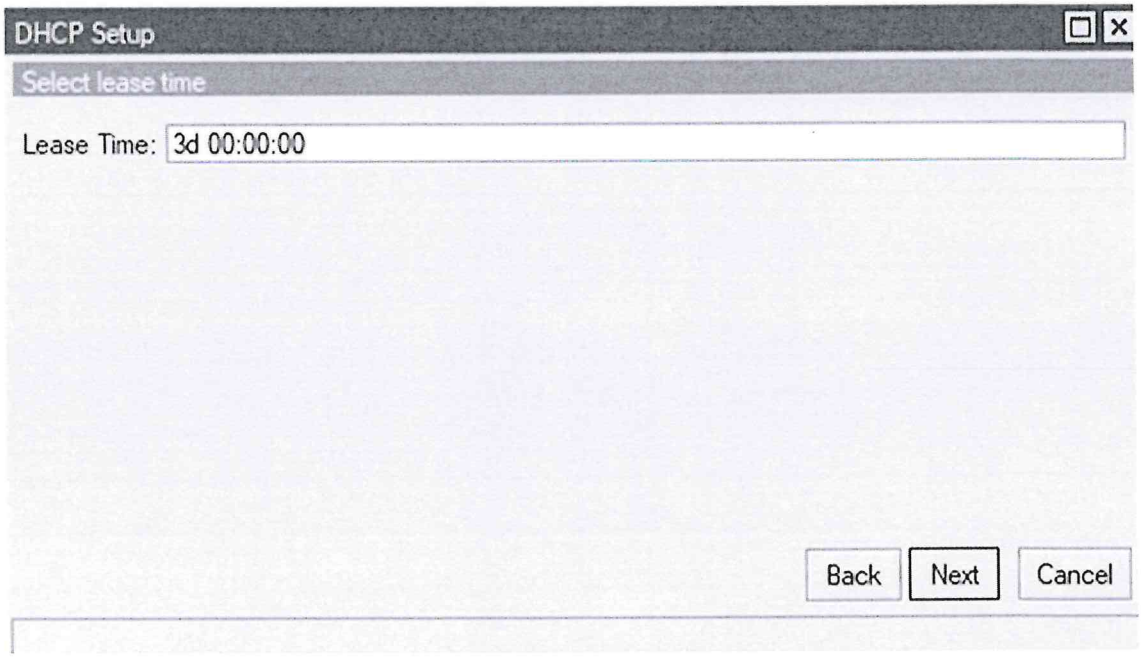


Рисунок 3.19 – Задаємо час резервування IP-адрес

Після виконання всіх кроків, DHCP-сервер успішно налаштовано і він готовий до роботи. Тепер він автоматично роздаватиме IP-адреси вказаного діапазону для всіх клієтів мережі.

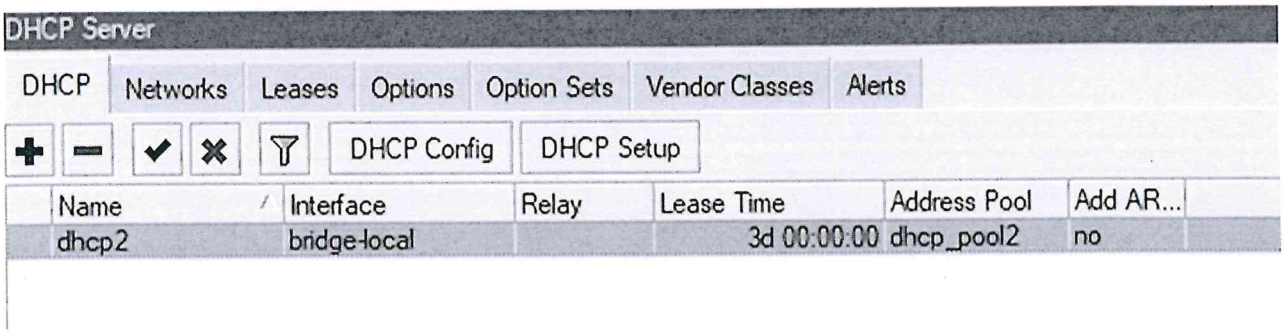


Рисунок 3.20 – DHCP Server успішно налаштовано

Перевіримо налаштування DHCP Server, як можна побачити на рисунку 3.21, DHCP Server успішно налаштовано і пристрої отримали свої адреси, за допомогою функціоналу MikroTik деяким пристроям в мережі були призначені статичні IP-адреси для зручності в керуванні.

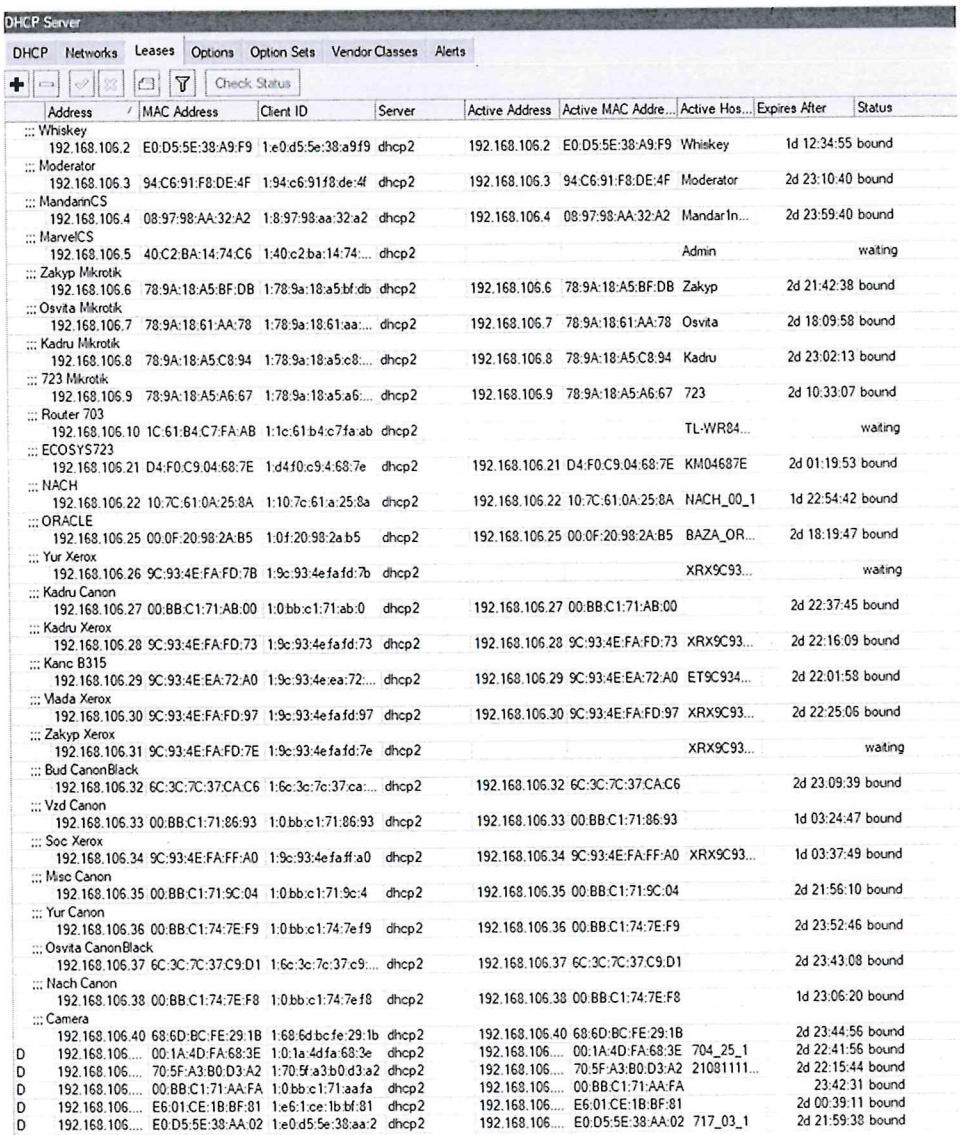


Рисунок 3.21 – Список підключених клієнтів

Тепер перейдемо до налаштування інтернет модуля, необхідно налагодити підключення до мережі інтернет та до дружної організації, а також забезпечити захист від зовнішніх втручань за допомогою FortiGate 60F.

Спочатку налаштуємо отримання IP-адреси від провайдера через DHCP. Для цього переходимо в меню IP- DHCP Client в інтерфейсі MikroTik. Це дозволить нашому пристрою автоматично отримати адресу від провайдера.

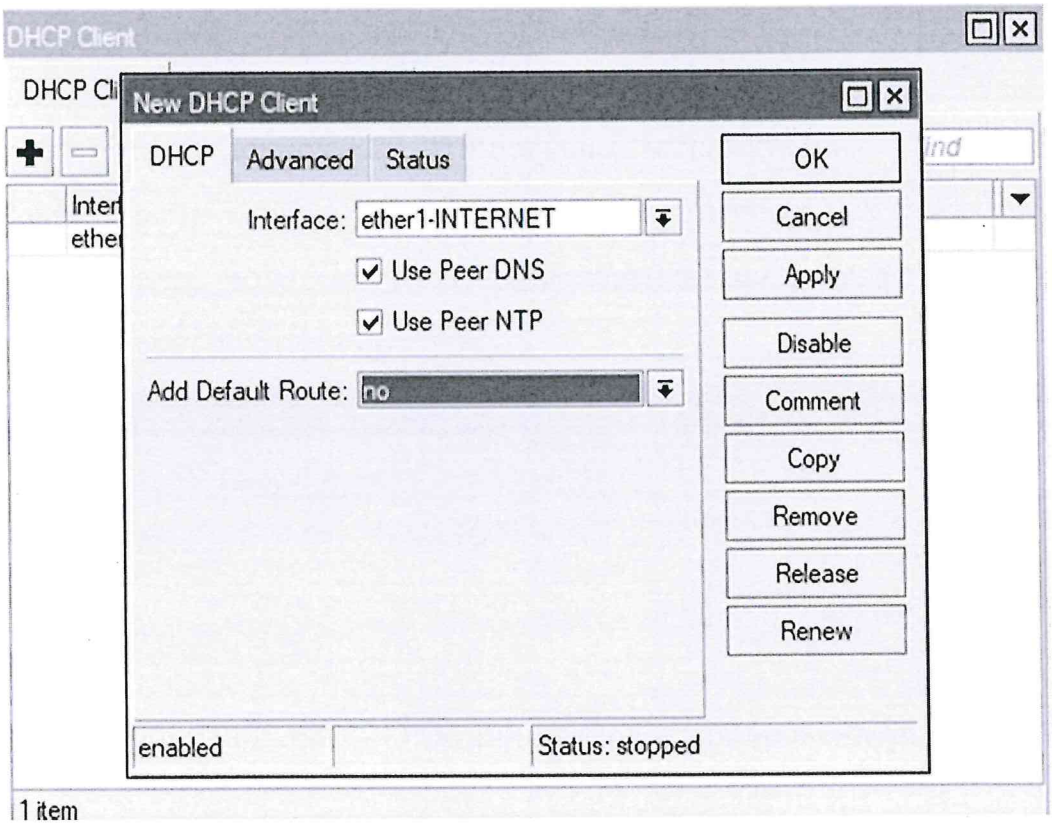


Рисунок 3.22 – Проведення налаштувань

Після цього пристрій автоматично отримає IP-адресу, надану провайдером, після чого потрібно переконатися що інтерфейсу призначена адреса, що можна побачити на рисунку 3.23.

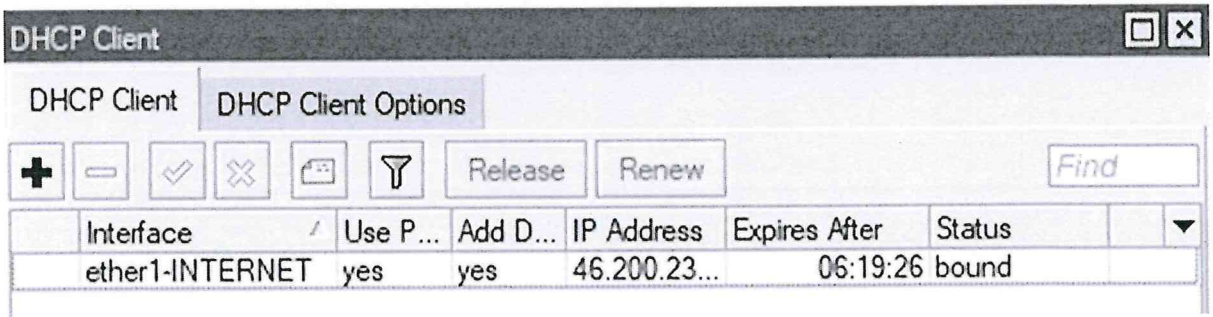


Рисунок 3.23 – Отримання адреси від провайдера

Після налаштування DHCP-клієнта важливо перевірити, чи є доступ до інтернету. Для цього можна виконати команду ping на будь який публічний сервер, наприклад 8.8.8.8, або перевірити чи з'явився доступ до веб-ресурсів через браузер.

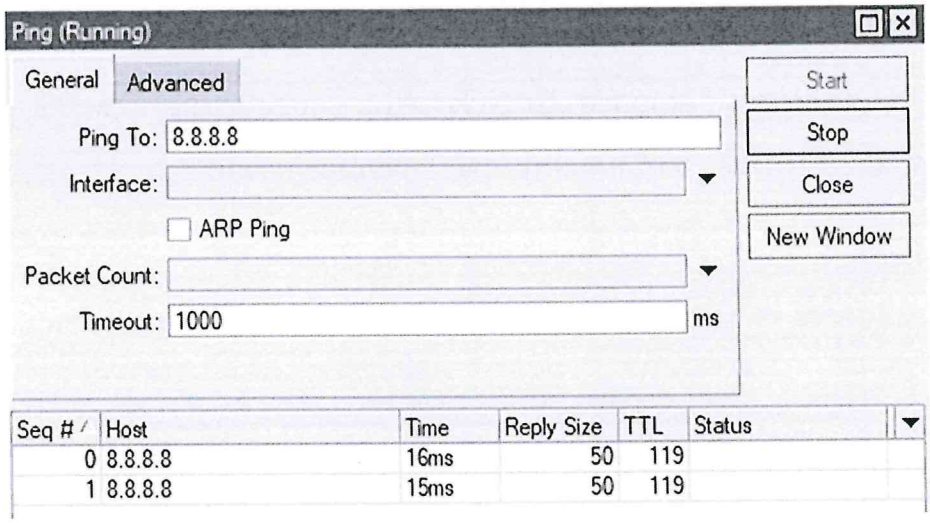


Рисунок 3.24 – Перевірка зв'язку з мережею інтернет

Тепер приступаємо до налаштування зв'язку з дружньою організацією. Для цього потрібно налаштувати статичну IP-адресу для підключення через спеціальний канал зв'язку.

Це довзволить комутатору MikroTik мати певну, незмінну IP-адресу, яка була надана дружньою організацією і яка використовуватиметься для зв'язку з їхньою мережею.

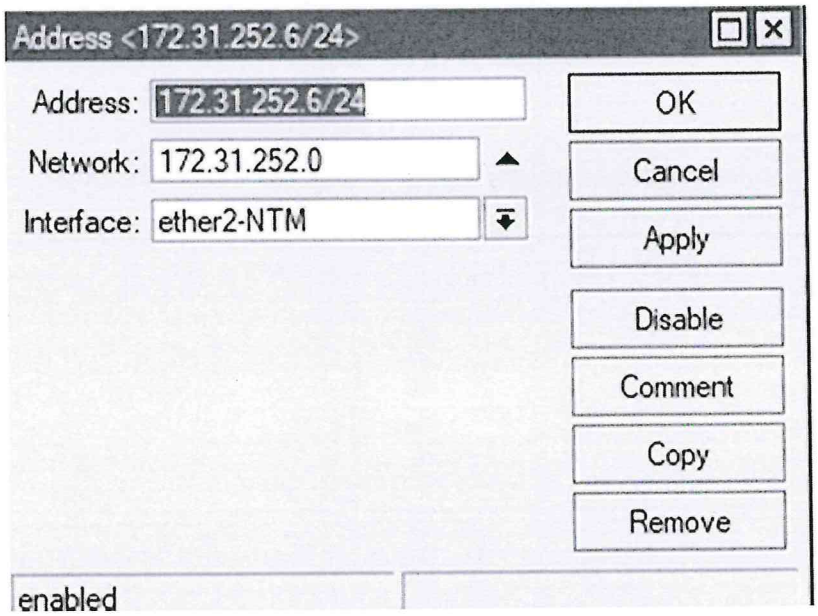


Рисунок 3.25 – Налаштування адреси для підключення через спецзв'язок

Після того, як статична адреса налаштована, необхідно налаштувати шлюзи для правильної маршрутизації трафіку через статичну IP-адресу. Це означає, що потрібно вказати шлюз за замовчуванням для трафіку, що виходить до дружньої організації, та інші шлюзи для локальних мереж.

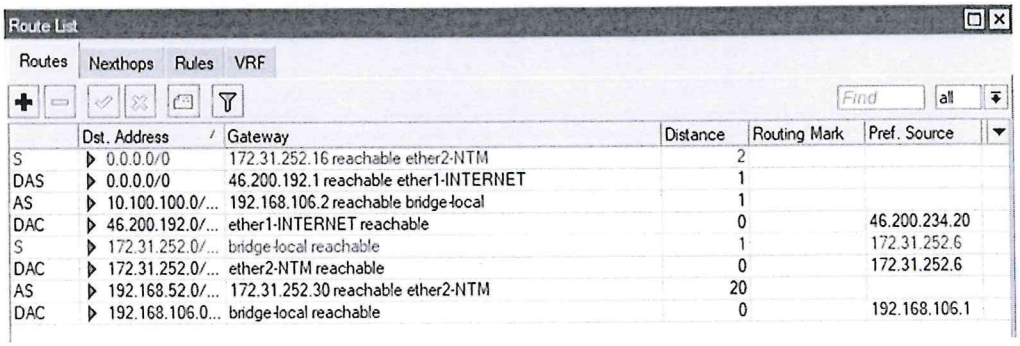


Рисунок 3.26 – Налаштування відповідних шлюзів.

Щоб всі пристрої в нашій мережі могли отримати доступ до Інтернету та ресурсів дружньої організації, потрібно налаштувати NAT. NAT дозволяє перетворювати приватні IP-адреси, використовувані в локальній мережі, на публічні адреси, які можна використовувати для доступу до Інтернету. Налаштування які були проведені зображені на рисунках 3.27-29.

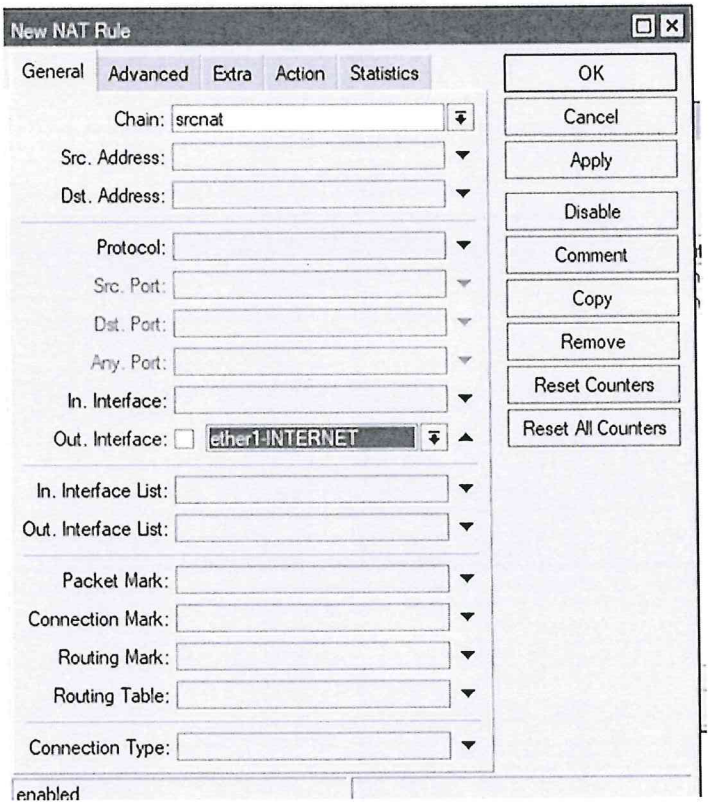


Рисунок 3.27 – Створення правила NAT

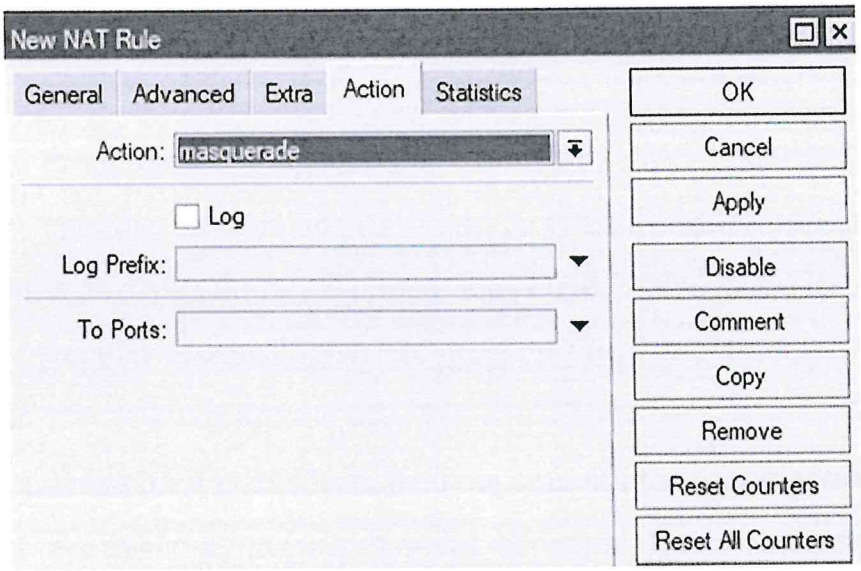


Рисунок 3.28 – Створення правила NAT

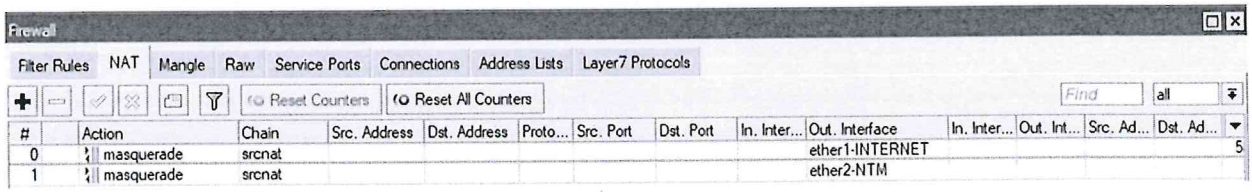


Рисунок 3.29 – Перевірка створених NAT правил

Останнім кроком налаштування є конфігурація інших пристроїв MikroTik для автоматичного отримання IP-адрес від DHCP-сервера. Це дозволяє усім пристроям в мережі отримувати IP-адреси без необхідності вручну їх налаштовувати.

Після налаштування DHCP-клієнта, адреси, які отримують пристрої, можна зафіксувати як статичні в налаштуваннях сервера. Це дозволить зберегти IP-адреси за кожним пристроєм, що полегшить управління мережею.

Закінчивши з налаштування мережевих пристроїв MikroTik, перейдемо до інтернет модуля, а саме до Fortigate 60F на якому необхідно забезпечити зихист від зовнішніх втручань.

Простими словами, трафіку який ініціалізований на зовнішньому інтерфейсі заборонено потрапляти в мережу і навпаки трафік який буде відбуватися всередині мережі повинен мати доступ до мережі інтернет.

Окрім цього потрібно налаштувати статичний маршрут за замовчуванням, щоб дістатися до хостів в Інтернеті.

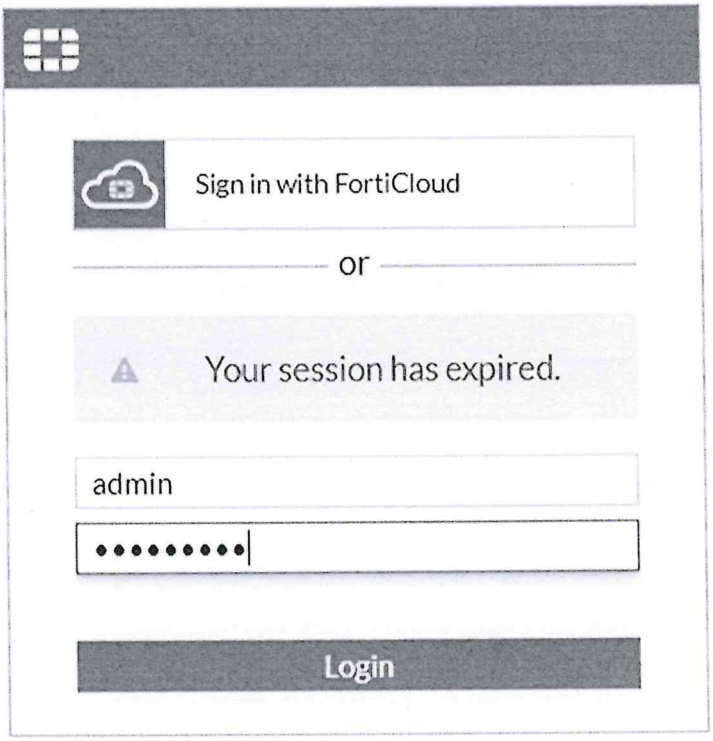


Рисунок 3.30 – Вікно входу

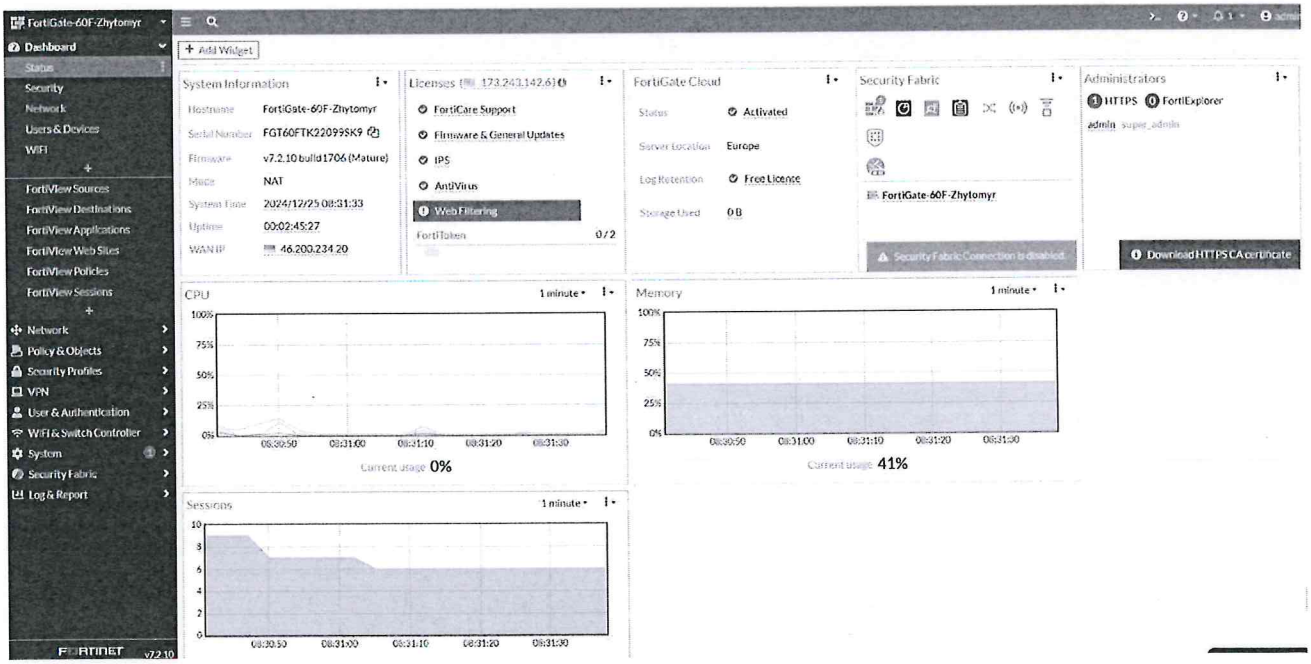


Рисунок 3.31 – Головне меню

Спершу налаштуємо адресацію на пристрої, проведені налаштування зображено на рисунках 3.32-34.

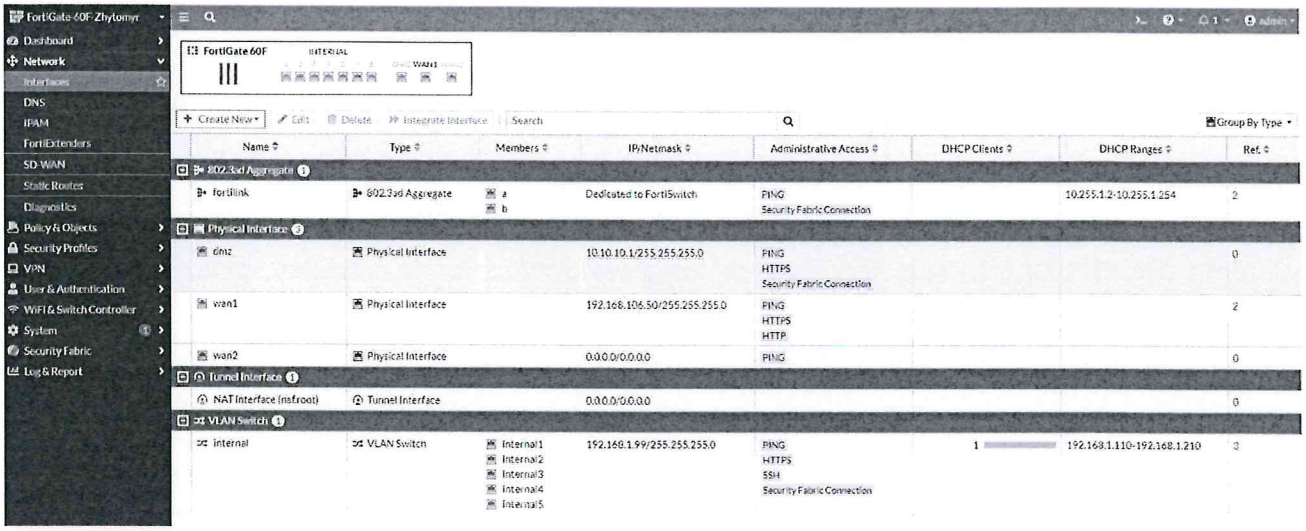


Рисунок 3.32 – Налаштування інтерфейсів

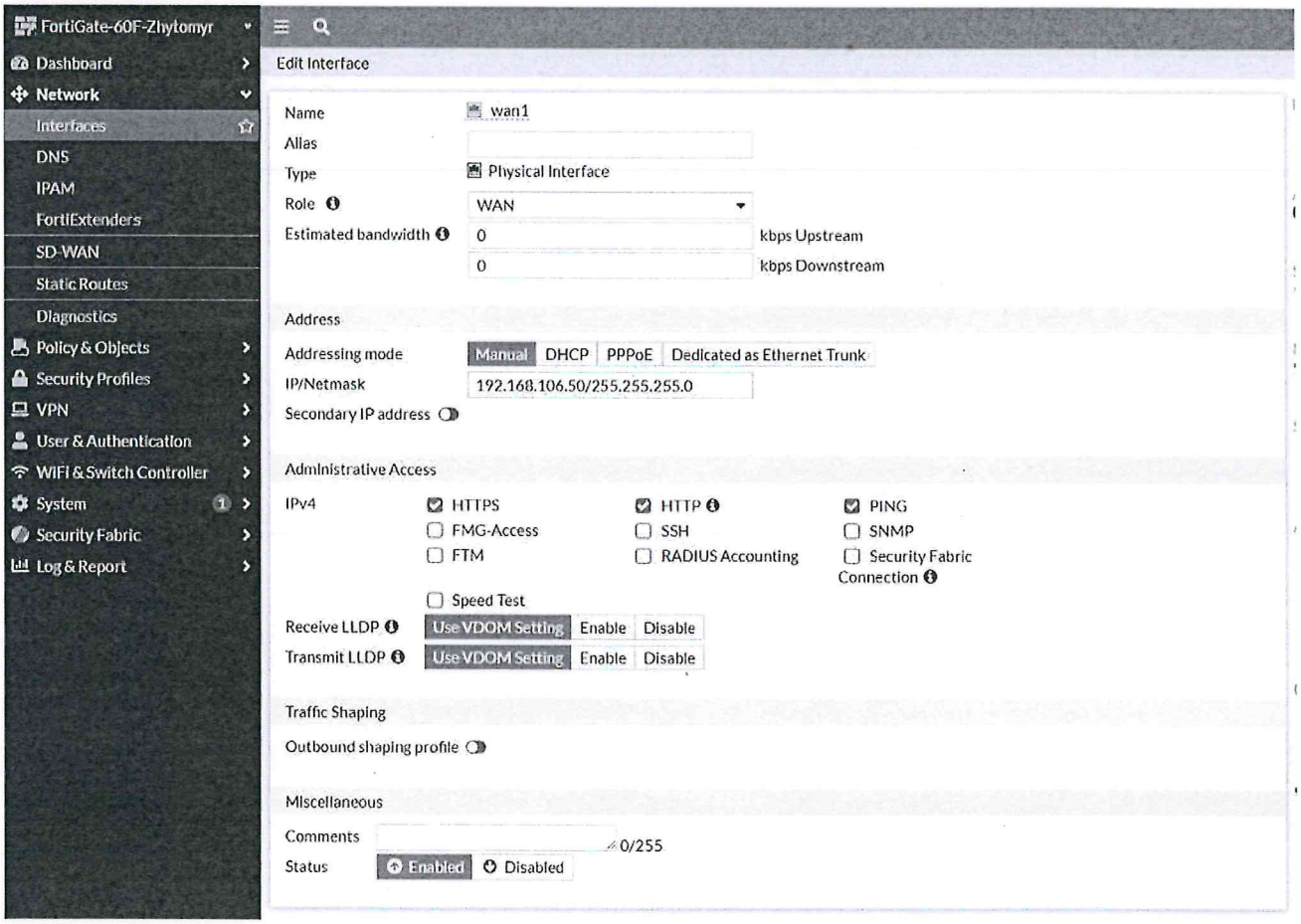


Рисунок 3.33 – Налаштування IP-адреси

Після цього необхідно додати маршрут за замовченням. Для цього в лівому меню обираємо Network - Static Routes та натискаємо Create New для створення нового маршруту.

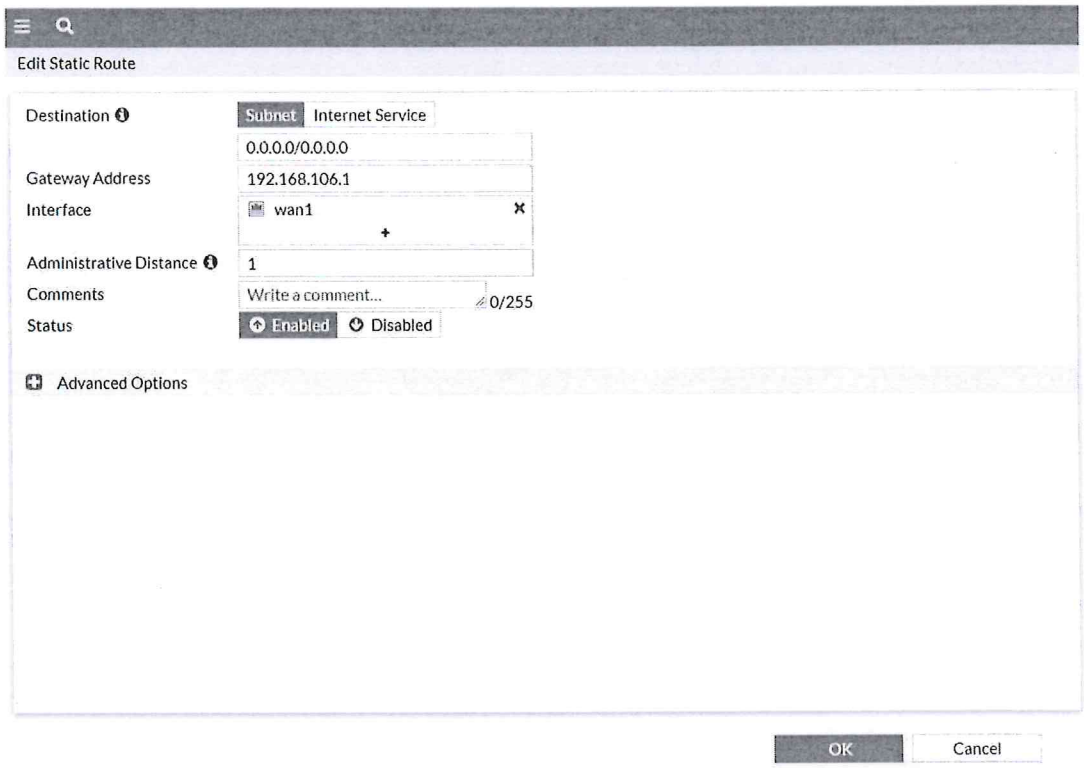


Рисунок 3.34 – Налаштування маршруту за замовчуванням

Після того як провели налаштування показані вище приступаємо до налаштування блокування вхідного трафік, але при цьому дозволяємо виходити всьому вихідному трафіку у Інтернет.

Нище показано відповідний скрипт який був застосований на пристрої.

```
config firewall policy
    edit 1
        set name "Allow-Outbound"
        set srcintf "internal"
        set dstintf "wan1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
    edit 2
        set name "Block-Inbound"
        set srcintf "wan1"
        set dstintf "internal"
        set action deny
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
    edit 1
        set name "Allow-Outbound"
        set srcintf "internal"
```

```
        set dstintf "wan1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable    # Включаємо NAT для вихідного трафіку
    next
end
```

Ці налаштування дозволять всім користувачам у внутрішній мережі мати доступ до Інтернету через інтерфейс WAN, окрім цього ці політики заблокують всі вхідні з'єднання з Інтернету в локальну мережу. Також був налаштований NAT (Network Address Translation) для того, щоб всі вихідні з'єднання з LAN використовували IP-адресу інтерфейсу WAN.

Після налаштування, було перевірено, чи всі політики та налаштування виконані правильно командою show firewall policy.

```
# show firewall policy
Policy ID  Name             Src Intf   Dst Intf   Action   Schedule  Service  Src Address  Dst Address  NAT     Log
---------  ---------------  ---------  ---------  -------  --------  -------  -----------  -----------  ------  ----
1          Allow-Outbound   internal   wan1       accept   always    ALL      all          all          enable  all
2          Block-Inbound    wan1       internal   deny     always    ALL      all          all          disable none
```

Рисунок 3.35 – Виконання політики show firewall policy

3.2 Оцінка ефективності проведених налаштувань.

Тестування підсистеми периметрового захисту мережі організації є важливим етапом для перевірки ефективності налаштувань безпеки та відповідності їх поставленим вимогам. Метою тестування є виявлення можливих вразливостей і перевірка того, чи налаштовані параметри захисту та доступу відповідають заданим стандартам безпеки та вимогам бізнес-процесів організації.

Першим етапом тестування є перевірка налаштувань DHCP-сервера, оскільки він відповідальний за автоматичне надання IP-адрес пристроям в мережі. Правильна конфігурація DHCP-сервера є ключовою для забезпечення коректної роботи всіх пристроїв, які підключаються до мережі(рис.3.30-3.32).

Для перевірки DHCP-сервера необхідно перевірити, чи коректно він роздає IP-адреси пристроям в мережі. Це можна зробити, підключивши комп'ютери та

інші пристрої до мережі і перевіривши, чи отримують вони IP-адреси з правильного діапазону.

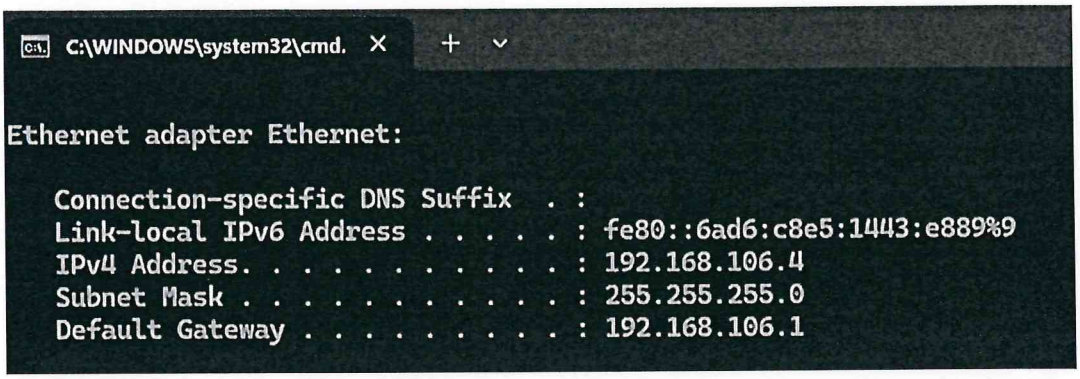


Рисунок 3.36 – Перевірка видання IP-адреси сервером

Після того, як налаштування DHCP-сервера перевірено, наступним кроком є перевірка зв'язку між робочими станціями та іншими пристроями в мережі. Це необхідно для того, щоб упевнитися, що всі пристрої можуть успішно спілкуватися між собою в межах локальної мережі.

Перевірка зв'язку між робочими станціями здійснюється за допомогою інструментів типу ping або traceroute, які дозволяють тестувати доступність мережевих пристроїв. Також можна перевірити правильність налаштування маршрутизації для локальних мереж.

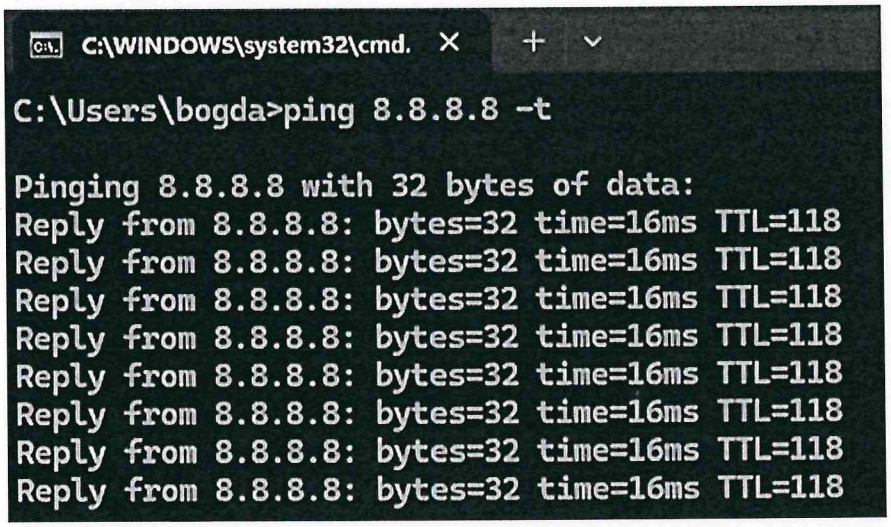


Рисунок 3.37 – Перевірка зв’язку з робочих станцій

Наступним етапом є перевірка доступу до Інтернету. Це важливо для підтвердження того, що підсистема периметрового захисту, зокрема шлюзи та NAT (Network Address Translation), налаштовані правильно та не блокують зовнішні з'єднання.

Перевірка зв'язку з Інтернетом може бути здійснена шляхом ping запиту до публічного сервера (наприклад, Google DNS 8.8.8.8) або за допомогою веб-браузера для перевірки доступу до зовнішніх веб-ресурсів. Якщо з'єднання встановлене, це означає, що налаштування маршрутизації та NAT працюють коректно.

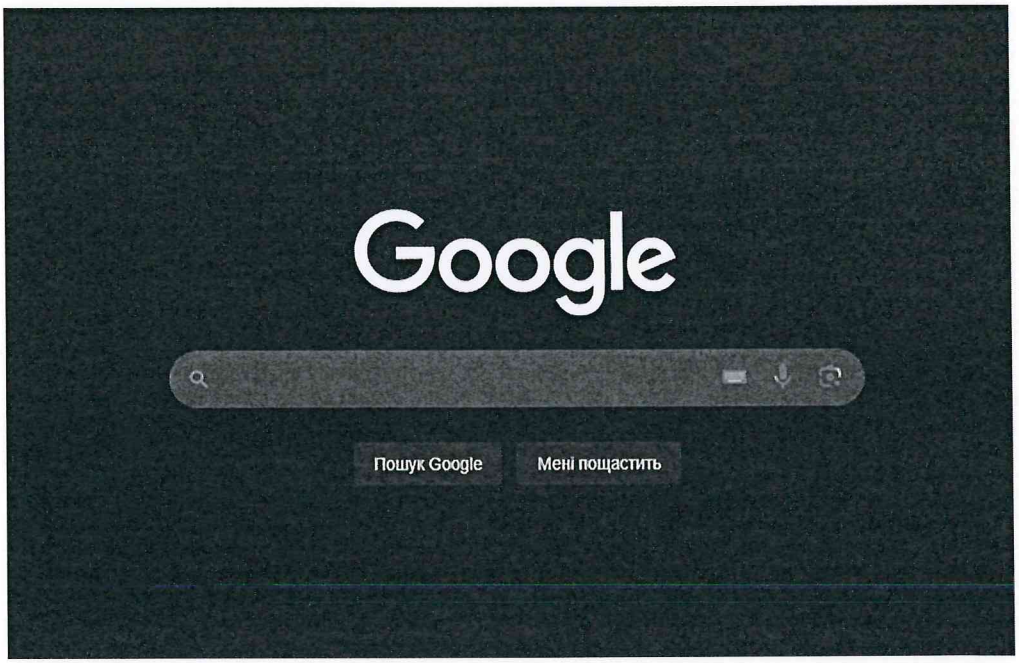


Рисунок 3.38 – Перевірка наявності зв'язку до мережі Інтернет

3.3 Аналіз результатів перевірок

Як і планувалося, всі раніше згадані вимоги були виконані. У майбутньому ця мережа може бути розширена та вдосконалена під конкретні завдання. Для цього є всі можливості: DHCP допомагає налаштовувати нові робочі станції та пристрої, сервер допомагає конфігурувати та контролювати нові пристрої, а рівень ядра є гнучким для майбутніх налаштувань по мірі використання пристроїв MikroTik.

В інтернет-модулі встановлено Fortigate 60F, який надійно захищає мережу від зловмисників з Інтернету.

Недоліком цієї мережі є те, що професійне, якісне обладнання коштує дорожче. Це означає, що комутатори MikroTik досить дорогі через свою надійність, якість і гарантію заміни обладнання та комплектуючих в разі їх виходу

з ладу в короткі терміни, що досить вигідно для великих компаній, де кожна хвилина на рахунку.

Висновки до 3-го розділу:

Для налаштування мережі необхідно дотримуватись кількох етапів. Початково потрібно обмежити доступ до пристроїв MikroTik через консоль, забезпечивши безпеку мережі. Це включає в себе налаштування дозволів лише для доступу через Winbox, обмеження доступу до SSH[10] та інших віддалених протоколів. Важливо налаштувати списки доступу, а також активувати блокування перебору паролів для підвищення рівня захисту. З метою підвищення безпеки мережі на MikroTik також налаштовуються антивірусні політики.

Далі налаштовується DHCP-сервер для автоматичного розподілу IP-адрес, що дозволяє ефективно керувати підключеннями пристроїв у мережі. Наступним кроком здійснюється підключення до Інтернету через статичні IP-адреси та налаштування шлюзу. Задаються правила NAT для маршрутизації трафіку, щоб він міг коректно проходити через мережу та досягати Інтернету.

Окрім цього, важливо встановити додаткові правила безпеки для блокування небажаного вхідного трафіку з Інтернету. Це включає конфігурацію брандмауера та фільтрацію пакетів для захисту внутрішньої мережі від потенційних загроз.

Після завершення налаштувань проводиться тестування, щоб перевірити коректність роботи мережі, підключення до Інтернету та функціонування всіх налаштувань безпеки.

ВИСНОВКИ

У дипломному проекті була описані методи та технології побудови підсистеми захисту периметру корпоративної мережі. Для побудови мережі використовувалися технології від компанії MikroTik та Fortinet.

Для початку було проведено аналіз та вибір існуючих технологій побудови сучасних гетерогенних мереж.

Було всебічно проаналізовано основні принципи проектування та налаштування корпоративних мереж, що дозволяють забезпечити їх ефективну, безпечну та масштабовану роботу також акцентовано увагу на ключових аспектах архітектури корпоративної мережі, включаючи модульність, гнучкість, масштабованість і відмовостійкість. Ці принципи є основою для побудови стабільної і продуктивної мережі, здатної адаптуватися до змін і забезпечити безперебійний обмін даними між усіма структурними підрозділами підприємства. Окрему увагу було приділено ієрархічній моделі мережі, яка включає рівні доступу, розподілу та ядра, кожен з яких має свої функції, що оптимізують загальну ефективність та стабільність мережі. Крім того, розглянуто важливість використання інтернет-модуля для підключення до глобальної мережі та спеціалізованих пристроїв, таких як фаєрволи для забезпечення безпеки.

Надано детальний опис архітектури мережі з точки зору її розподілу на логічні модулі для полегшення управління та масштабування. Інтернет-модуль виступає ключовим елементом, що з'єднує внутрішню мережу з зовнішнім середовищем, а для забезпечення безпеки використовуються фаєрволи (зокрема FortiGate 60F), що фільтрують непотрібні чи шкідливі з'єднання, забезпечуючи захист від потенційних загроз з боку Інтернету. Налаштування DHCP-сервера на базі MikroTik автоматизує розподіл IP-адрес серед робочих станцій, що значно полегшує адміністрування та знижує ймовірність помилок. Крім того, важливою складовою налаштувань є використання сучасних інструментів для моніторингу та аналізу мережевих з'єднань, таких як Wireshark, який дозволяє оперативно виявляти проблеми з трафіком, аналізувати вразливості і коригувати налаштування для забезпечення безперебійної роботи.

Розглянуто практичні аспекти налаштування мережі, зокрема, початкові кроки для забезпечення безпеки доступу до мережевих пристроїв MikroTik. Це включає налаштування обмежень на доступ через консоль, активацію блокування перебору паролів та використання антивірусних політик для підвищення рівня захисту. Крім того, важливо налаштувати автоматичний розподіл IP-адрес через DHCP-сервер, підключення до Інтернету та налаштування шлюзу для коректної маршрутизації трафіку. Забезпечення додаткових заходів безпеки, таких як фільтрація вхідного трафіку через брандмауер, є необхідним для захисту внутрішньої мережі від зовнішніх загроз. Після завершення налаштувань важливо провести тестування мережі для перевірки коректності роботи всіх компонентів і безпечного підключення до Інтернету.

Проведено налаштування пристроїв та аналіз результатів, сформовано висновки стосовно модернізації та вдосконалення роботи. Реалізована мережа є готовим макетом реальної реалізації проекту, а конфігурації можуть застосовуватися для реального обладнання.

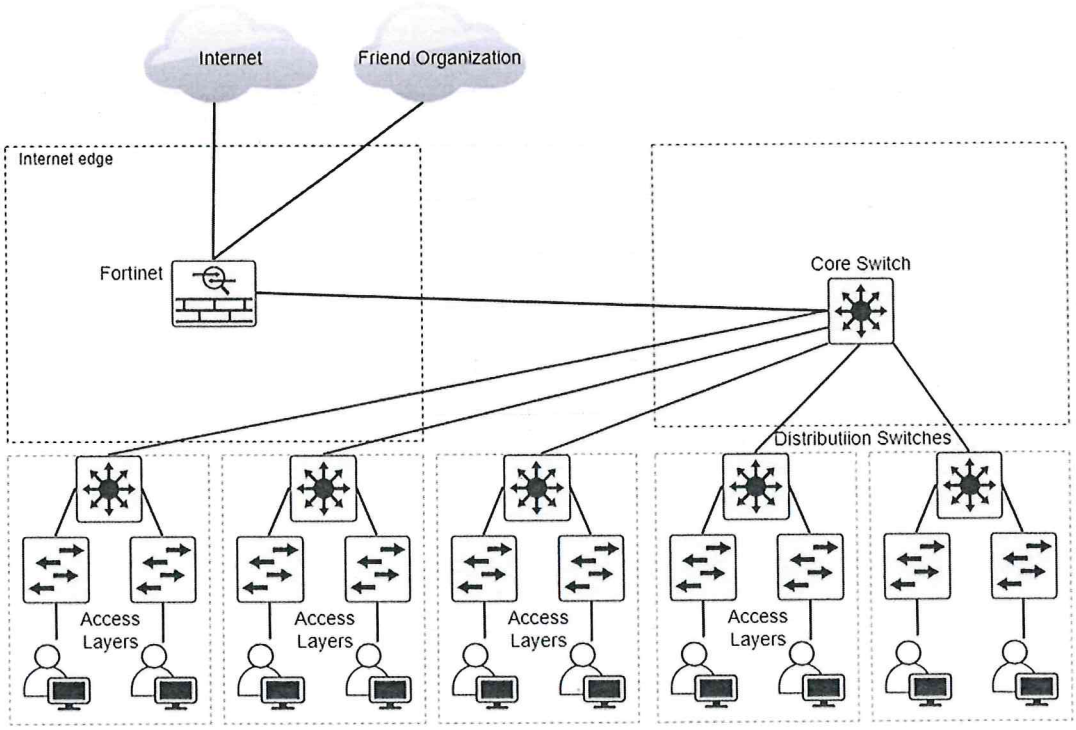
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Корпоративна мережа [Електронний ресурс] – https://uk.wikipedia.org/wiki/Корпоративна_мережа
2. Налаштування MikroTik [Електронний ресурс] –https://настройка-микротик.укр/kak-nastroit-router-mikrotik-bazovaya-konfiguracziya/
3. DNC сервер [Електронний ресурс] – https://ru.wikipedia.org/wiki/DNS
4. DHCP relay [Електронний ресурс] – https://ixnfo.com/dhcp-relay-cisco.html
5. Windows 10 [Електронний ресурс] – https://www.microsoft.com/uk-ua/software-download/windows10
6. Kali Linux [Електронний ресурс] – https://www.kali.org/get-kali/#kali-virtual-machines
7. Fortinet Fortigate 60f [Електронний ресурс] – https://www.fortsoft.com.ua/ua/catalog/mezhsetevye-ekrany/mezhsetevoy-ekran-fortinet-fg
8. Налаштування NAT [Електронний ресурс] – http://commonerrors.blogspot.com/2011/07/nat-configuration-on-gns3.html
9. Ієрархічна модель мережі[Електронний ресурс] - http://www.telesphera.net/blog/model-mereghi-vid-cisco.html
10. Протокол SSH [Електронний ресурс] – https://uk.wikipedia.org/wiki/SSH
11. Wireshark [Електронний ресурс] – https://www.wireshark.org/docs/wsug_html_chunked/ChAdvExpert.html

ДОДАТКИ

ДОДАТОК А

Мережевий проект



ДОДАТОК Б

Конфігураційні файли пристроїв мережі

Конфігураційни файл комутатора MikroTik

```
[admin@RouterOS] > export
# jan/02/1970 04:38:35 by RouterOS 6.48.7
# software id = VBTQ-U294
#
# model = CRS326-24G-2S+
# serial number = HF30985SD49
/interface bridge
add admin-mac=78:9A:18:61:AA:78 auto-mac=no comment=defconf name=bridge
/interface list
add name=WAN
add name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip hotspot profile
set [ find default=yes ] html-directory=hotspot
/interface bridge port
add bridge=bridge comment=defconf interface=ether1
add bridge=bridge comment=defconf interface=ether2
add bridge=bridge comment=defconf interface=ether3
add bridge=bridge comment=defconf interface=ether4
add bridge=bridge comment=defconf interface=ether5
add bridge=bridge comment=defconf interface=ether6
add bridge=bridge comment=defconf interface=ether7
add bridge=bridge comment=defconf interface=ether8
add bridge=bridge comment=defconf interface=ether9
add bridge=bridge comment=defconf interface=ether10
add bridge=bridge comment=defconf interface=ether11
add bridge=bridge comment=defconf interface=ether12
add bridge=bridge comment=defconf interface=ether13
add bridge=bridge comment=defconf interface=ether14
add bridge=bridge comment=defconf interface=ether15
add bridge=bridge comment=defconf interface=ether16
add bridge=bridge comment=defconf interface=ether17
add bridge=bridge comment=defconf interface=ether18
add bridge=bridge comment=defconf interface=ether19
add bridge=bridge comment=defconf interface=ether20
add bridge=bridge comment=defconf interface=ether21
add bridge=bridge comment=defconf interface=ether22
add bridge=bridge comment=defconf interface=ether23
add bridge=bridge comment=defconf interface=ether24
add bridge=bridge comment=defconf interface=sfp-sfpplus1
add bridge=bridge comment=defconf interface=sfp-sfpplus2
/interface list member
add interface=ether1 list=WAN
add interface=ether2 list=LAN
add interface=ether3 list=LAN
add interface=ether4 list=LAN
add interface=ether5 list=LAN
add interface=ether6 list=LAN
add interface=ether7 list=LAN
add interface=ether8 list=LAN
add interface=ether9 list=LAN
add interface=ether10 list=LAN
add interface=ether11 list=LAN
add interface=ether12 list=LAN
add interface=ether13 list=LAN
add interface=ether14 list=LAN
add interface=ether15 list=LAN
add interface=ether16 list=LAN
add interface=ether17 list=LAN
add interface=ether18 list=LAN
add interface=ether19 list=LAN
add interface=ether20 list=LAN
add interface=ether21 list=LAN
add interface=ether22 list=LAN
add interface=ether23 list=LAN
add interface=ether24 list=LAN
add interface=sfp-sfpplus1 list=LAN
add interface=sfp-sfpplus2 list=LAN
/ip address
```

```
add address=110.110.110.51/24 comment=defconf interface=ether2 network=110.110.110.0
/system identity
set name=RouterOS
/system routerboard settings
set boot-os=router-os
[admin@RouterOS] >
```

Конфігураційни файл комутатора MikroTik

```
[admin@RouterOS] > export
# jan/02/1970 04:38:35 by RouterOS 6.48.7
# software id = VBTQ-U294
#
# model = CRS326-24G-2S+
# serial number = HF30985SD49
/interface bridge
add admin-mac=78:9A:18:61:AA:78 auto-mac=no comment=defconf name=bridge
/interface list
add name=WAN
add name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip hotspot profile
set [ find default=yes ] html-directory=hotspot
/interface bridge port
add bridge=bridge comment=defconf interface=ether1
add bridge=bridge comment=defconf interface=ether2
add bridge=bridge comment=defconf interface=ether3
add bridge=bridge comment=defconf interface=ether4
add bridge=bridge comment=defconf interface=ether5
add bridge=bridge comment=defconf interface=ether6
add bridge=bridge comment=defconf interface=ether7
add bridge=bridge comment=defconf interface=ether8
add bridge=bridge comment=defconf interface=ether9
add bridge=bridge comment=defconf interface=ether10
add bridge=bridge comment=defconf interface=ether11
add bridge=bridge comment=defconf interface=ether12
add bridge=bridge comment=defconf interface=ether13
add bridge=bridge comment=defconf interface=ether14
add bridge=bridge comment=defconf interface=ether15
add bridge=bridge comment=defconf interface=ether16
add bridge=bridge comment=defconf interface=ether17
add bridge=bridge comment=defconf interface=ether18
add bridge=bridge comment=defconf interface=ether19
add bridge=bridge comment=defconf interface=ether20
add bridge=bridge comment=defconf interface=ether21
add bridge=bridge comment=defconf interface=ether22
add bridge=bridge comment=defconf interface=ether23
add bridge=bridge comment=defconf interface=ether24
add bridge=bridge comment=defconf interface=sfp-sfpplus1
add bridge=bridge comment=defconf interface=sfp-sfpplus2
/interface list member
add interface=ether1 list=WAN
add interface=ether2 list=LAN
add interface=ether3 list=LAN
add interface=ether4 list=LAN
add interface=ether5 list=LAN
add interface=ether6 list=LAN
add interface=ether7 list=LAN
add interface=ether8 list=LAN
add interface=ether9 list=LAN
add interface=ether10 list=LAN
add interface=ether11 list=LAN
add interface=ether12 list=LAN
add interface=ether13 list=LAN
add interface=ether14 list=LAN
add interface=ether15 list=LAN
add interface=ether16 list=LAN
add interface=ether17 list=LAN
add interface=ether18 list=LAN
add interface=ether19 list=LAN
add interface=ether20 list=LAN
add interface=ether21 list=LAN
add interface=ether22 list=LAN
add interface=ether23 list=LAN
add interface=ether24 list=LAN
add interface=sfp-sfpplus1 list=LAN
add interface=sfp-sfpplus2 list=LAN
/ip address
```

```
add address=110.110.110.52/24 comment=defconf interface=ether2 network=110.110.110.0
/system identity
set name=RouterOS
/system routerboard settings
set boot-os=router-os
[admin@RouterOS] >
```

Конфігураційни файл комутатора MikroTik

```
[admin@RouterOS] > export
# jan/02/1970 04:38:35 by RouterOS 6.48.7
# software id = VBTQ-U294
#
# model = CRS326-24G-2S+
# serial number = HF30985SD49
/interface bridge
add admin-mac=78:9A:18:61:AA:78 auto-mac=no comment=defconf name=bridge
/interface list
add name=WAN
add name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip hotspot profile
set [ find default=yes ] html-directory=hotspot
/interface bridge port
add bridge=bridge comment=defconf interface=ether1
add bridge=bridge comment=defconf interface=ether2
add bridge=bridge comment=defconf interface=ether3
add bridge=bridge comment=defconf interface=ether4
add bridge=bridge comment=defconf interface=ether5
add bridge=bridge comment=defconf interface=ether6
add bridge=bridge comment=defconf interface=ether7
add bridge=bridge comment=defconf interface=ether8
add bridge=bridge comment=defconf interface=ether9
add bridge=bridge comment=defconf interface=ether10
add bridge=bridge comment=defconf interface=ether11
add bridge=bridge comment=defconf interface=ether12
add bridge=bridge comment=defconf interface=ether13
add bridge=bridge comment=defconf interface=ether14
add bridge=bridge comment=defconf interface=ether15
add bridge=bridge comment=defconf interface=ether16
add bridge=bridge comment=defconf interface=ether17
add bridge=bridge comment=defconf interface=ether18
add bridge=bridge comment=defconf interface=ether19
add bridge=bridge comment=defconf interface=ether20
add bridge=bridge comment=defconf interface=ether21
add bridge=bridge comment=defconf interface=ether22
add bridge=bridge comment=defconf interface=ether23
add bridge=bridge comment=defconf interface=ether24
add bridge=bridge comment=defconf interface=sfp-sfpplus1
add bridge=bridge comment=defconf interface=sfp-sfpplus2
/interface list member
add interface=ether1 list=WAN
add interface=ether2 list=LAN
add interface=ether3 list=LAN
add interface=ether4 list=LAN
add interface=ether5 list=LAN
add interface=ether6 list=LAN
add interface=ether7 list=LAN
add interface=ether8 list=LAN
add interface=ether9 list=LAN
add interface=ether10 list=LAN
add interface=ether11 list=LAN
add interface=ether12 list=LAN
add interface=ether13 list=LAN
add interface=ether14 list=LAN
add interface=ether15 list=LAN
add interface=ether16 list=LAN
add interface=ether17 list=LAN
add interface=ether18 list=LAN
add interface=ether19 list=LAN
add interface=ether20 list=LAN
add interface=ether21 list=LAN
add interface=ether22 list=LAN
add interface=ether23 list=LAN
add interface=ether24 list=LAN
add interface=sfp-sfpplus1 list=LAN
add interface=sfp-sfpplus2 list=LAN
/ip address
```

```
add address=110.110.110.53/24 comment=defconf interface=ether2 network=110.110.110.0
/system identity
set name=RouterOS
/system routerboard settings
set boot-os=router-os
[admin@RouterOS] >
```

Конфігураційни файл комутатора MikroTik

```
[admin@RouterOS] > export
# jan/02/1970 04:38:35 by RouterOS 6.48.7
# software id = VBTQ-U294
#
# model = CRS326-24G-2S+
# serial number = HF30985SD49
/interface bridge
add admin-mac=78:9A:18:61:AA:78 auto-mac=no comment=defconf name=bridge
/interface list
add name=WAN
add name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip hotspot profile
set [ find default=yes ] html-directory=hotspot
/interface bridge port
add bridge=bridge comment=defconf interface=ether1
add bridge=bridge comment=defconf interface=ether2
add bridge=bridge comment=defconf interface=ether3
add bridge=bridge comment=defconf interface=ether4
add bridge=bridge comment=defconf interface=ether5
add bridge=bridge comment=defconf interface=ether6
add bridge=bridge comment=defconf interface=ether7
add bridge=bridge comment=defconf interface=ether8
add bridge=bridge comment=defconf interface=ether9
add bridge=bridge comment=defconf interface=ether10
add bridge=bridge comment=defconf interface=ether11
add bridge=bridge comment=defconf interface=ether12
add bridge=bridge comment=defconf interface=ether13
add bridge=bridge comment=defconf interface=ether14
add bridge=bridge comment=defconf interface=ether15
add bridge=bridge comment=defconf interface=ether16
add bridge=bridge comment=defconf interface=ether17
add bridge=bridge comment=defconf interface=ether18
add bridge=bridge comment=defconf interface=ether19
add bridge=bridge comment=defconf interface=ether20
add bridge=bridge comment=defconf interface=ether21
add bridge=bridge comment=defconf interface=ether22
add bridge=bridge comment=defconf interface=ether23
add bridge=bridge comment=defconf interface=ether24
add bridge=bridge comment=defconf interface=sfp-sfpplus1
add bridge=bridge comment=defconf interface=sfp-sfpplus2
/interface list member
add interface=ether1 list=WAN
add interface=ether2 list=LAN
add interface=ether3 list=LAN
add interface=ether4 list=LAN
add interface=ether5 list=LAN
add interface=ether6 list=LAN
add interface=ether7 list=LAN
add interface=ether8 list=LAN
add interface=ether9 list=LAN
add interface=ether10 list=LAN
add interface=ether11 list=LAN
add interface=ether12 list=LAN
add interface=ether13 list=LAN
add interface=ether14 list=LAN
add interface=ether15 list=LAN
add interface=ether16 list=LAN
add interface=ether17 list=LAN
add interface=ether18 list=LAN
add interface=ether19 list=LAN
add interface=ether20 list=LAN
add interface=ether21 list=LAN
add interface=ether22 list=LAN
add interface=ether23 list=LAN
add interface=ether24 list=LAN
add interface=sfp-sfpplus1 list=LAN
add interface=sfp-sfpplus2 list=LAN
/ip address
```

```
add address=110.110.110.54/24 comment=defconf interface=ether2 network=110.110.110.0
/system identity
set name=RouterOS
/system routerboard settings
set boot-os=router-os
[admin@RouterOS] >
```

Конфігураційни файл комутатора MikroTik

```
[admin@RouterOS] > export
# jan/02/1970 04:38:35 by RouterOS 6.48.7
# software id = VBTQ-U294
#
# model = CRS326-24G-2S+
# serial number = HF30985SD49
/interface bridge
add admin-mac=78:9A:18:61:AA:78 auto-mac=no comment=defconf name=bridge
/interface list
add name=WAN
add name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip hotspot profile
set [ find default=yes ] html-directory=hotspot
/interface bridge port
add bridge=bridge comment=defconf interface=ether1
add bridge=bridge comment=defconf interface=ether2
add bridge=bridge comment=defconf interface=ether3
add bridge=bridge comment=defconf interface=ether4
add bridge=bridge comment=defconf interface=ether5
add bridge=bridge comment=defconf interface=ether6
add bridge=bridge comment=defconf interface=ether7
add bridge=bridge comment=defconf interface=ether8
add bridge=bridge comment=defconf interface=ether9
add bridge=bridge comment=defconf interface=ether10
add bridge=bridge comment=defconf interface=ether11
add bridge=bridge comment=defconf interface=ether12
add bridge=bridge comment=defconf interface=ether13
add bridge=bridge comment=defconf interface=ether14
add bridge=bridge comment=defconf interface=ether15
add bridge=bridge comment=defconf interface=ether16
add bridge=bridge comment=defconf interface=ether17
add bridge=bridge comment=defconf interface=ether18
add bridge=bridge comment=defconf interface=ether19
add bridge=bridge comment=defconf interface=ether20
add bridge=bridge comment=defconf interface=ether21
add bridge=bridge comment=defconf interface=ether22
add bridge=bridge comment=defconf interface=ether23
add bridge=bridge comment=defconf interface=ether24
add bridge=bridge comment=defconf interface=sfp-sfpplus1
add bridge=bridge comment=defconf interface=sfp-sfpplus2
/interface list member
add interface=ether1 list=WAN
add interface=ether2 list=LAN
add interface=ether3 list=LAN
add interface=ether4 list=LAN
add interface=ether5 list=LAN
add interface=ether6 list=LAN
add interface=ether7 list=LAN
add interface=ether8 list=LAN
add interface=ether9 list=LAN
add interface=ether10 list=LAN
add interface=ether11 list=LAN
add interface=ether12 list=LAN
add interface=ether13 list=LAN
add interface=ether14 list=LAN
add interface=ether15 list=LAN
add interface=ether16 list=LAN
add interface=ether17 list=LAN
add interface=ether18 list=LAN
add interface=ether19 list=LAN
add interface=ether20 list=LAN
add interface=ether21 list=LAN
add interface=ether22 list=LAN
add interface=ether23 list=LAN
add interface=ether24 list=LAN
add interface=sfp-sfpplus1 list=LAN
add interface=sfp-sfpplus2 list=LAN
/ip address
```

```
add address=110.110.110.55/24 comment=defconf interface=ether2 network=110.110.110.0
/system identity
set name=RouterOS
/system routerboard settings
set boot-os=router-os
[admin@RouterOS] >
```