ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «МЕТОДИ ПОСИЛЕННЯ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ ШЛЯХОМ ІНТЕГРАЦІЇ СИСТЕМ АУТЕНТИФІКАЦІЇ ТА МІЖМЕРЕЖЕВОГО ЕКРАНУВАННЯ»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Олександр ОСТАПЕНКО*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КСДМ-62
Олександр ОСТАПЕНКО
Ім'я, ПРІЗВИЩЕ

Керівник: Наталія ЛАЩЕВСЬКА
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії
Ступінь вищої освіти Магістр
Спеціальність 123 Комп'ютерної інженерії
Освітньо-професійна програма Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою Наталія ЛАЩЕВСЬКА
Ім'я, ПРІЗВИЩЕ
«_____» _____ 2025р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Остапенко Олександр Станіславович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: _____
_____
керівник кваліфікаційної роботи Наталія ЛАЩЕВСЬКА,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» 10 2025р. № 467
2. Строк подання кваліфікаційної роботи «_____» _____ 2025р.
3. Вихідні дані до кваліфікаційної роботи: Науково-технічна література, методи системного аналізу для проектування топології, методи моделювання мережевих процесів, емпіричні методи для перевірки налаштувань обладнання

Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Теоретичні засади проектування та безпеки комп'ютерних мереж
2. Проектування підсистеми безпеки для корпоративної комп'ютерної мережі
4. Реалізація, конфігурування та верифікація захищеної корпоративної мережі
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання «_____» _____ 2025р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	25.09-24.10.2025	Виконано
2	Обробка матеріалу	25.10-05.11.2025	Виконано
3	Розробка теоретичної частини	06.11-10.11.2025	Виконано
4	Розробка методів	11.11-15.11.2025	Виконано
5	Висновки за результатами аналізу	15.11-19.11.2025	Виконано
6	Оформлення пояснювальної записки	19.11-21.11.2025	Виконано
7	Розробка презентації	21.11-29.11.2025	Виконано
8	Передзахист	01.12-02.12.2025	Виконано
9	Здача в деканат	15.12-18.12.2025	Виконано

Здобувач вищої освіти _____ Олександр ОСТАПЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Наталія ЛАЩЕВСЬКА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 66 стор., 33 рис., 4 табл., 20 джерел.

Мета дослідження – підвищення рівня інформаційної безпеки корпоративної мережі шляхом проектування та впровадження методів комплексної системи захисту, що інтегрує методи міжмережевого екранування, сегментації та централізованої автентифікації користувачів.

Об'єкт дослідження – процеси функціонування та захисту інформації в корпоративних комп'ютерних мережах.

Предмет дослідження – методи та засоби забезпечення безпеки мережевої інфраструктури з використанням технологій AAA, протоколу RADIUS та міжмережевих екранів нового покоління.

Короткий зміст роботи: У кваліфікаційній роботі проведено аналіз сучасних загроз та методів апаратно-програмного захисту корпоративних мереж. Розроблено топологію захищеної мережі з розподілом на зони безпеки та впровадженням VLAN. Обґрунтовано вибір апаратного забезпечення. Реалізовано систему централізованої автентифікації, авторизації та обліку на базі сервера. Налаштовано політики безпеки на маршрутизаторах та брандмауері для фільтрації трафіку, захисту від несанкціонованого доступу та організації безпечного віддаленого керування через SSH. Проведено тестування, яке підтвердило надійність розгорнутої системи.

Результати: Запропоновані методи забезпечують гранульований контроль доступу, ізоляцію критичних ресурсів та захищений вихід до глобальної мережі, що суттєво знижує ризики кібератак.

КЛЮЧОВІ СЛОВА: КОРПОРАТИВНА МЕРЕЖА, КІБЕРБЕЗПЕКА, AAA, RADIUS, FREERADIUS, FIREWALL, FORTIGATE, CISCO, VLAN, OSPF, SSH, NAT, КОНТРОЛЬ ДОСТУПУ.

ABSTRACT

Textual part of the master's qualification work: 66 pp., 33 figs., 4 tabs., 20 refs.

The purpose of the work is to enhance the level of information security in a corporate network by designing and implementing a comprehensive protection system that integrates firewalling, segmentation, and centralized user authentication methods.

Object of research: The processes of functioning and information protection in corporate computer networks.

Subject of research: Methods and tools for ensuring network infrastructure security using AAA technologies, the RADIUS protocol, and Next-Generation Firewalls.

Content summary: The qualification work provides an analysis of modern threats and hardware-software protection methods for corporate networks. A secure network topology was developed, featuring division into security zones and the implementation of VLANs. The selection of hardware has been substantiated. A centralized Authentication, Authorization, and Accounting system was implemented based on a server. Security policies were configured on routers and the firewall for traffic filtering, protection against unauthorized access, and the organization of secure remote management via SSH. Testing was conducted, confirming the reliability of the deployed system.

Results: The proposed methods ensure granular access control, isolation of critical resources, and secure access to the global network, significantly reducing the risks of cyberattacks.

KEYWORDS: CORPORATE NETWORK, CYBERSECURITY, AAA, RADIUS, FREERADIUS, FIREWALL, FORTIGATE, CISCO, VLAN, OSPF, SSH, NAT, ACCESS CONTROL.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Остапенко О. С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 123 Комп'ютерна інженерія
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)
на тему: «Методи посилення безпеки корпоративних мереж шляхом інтеграції систем аутентифікації та міжмережевого екранування».
Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ Катерина НЕСТЕРЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Остапенко О. С. показав відмінну теоретичну підготовку, уміння володіти та розуміння новими комп'ютерними технологіями, користуватися навчальною і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.
Все це дозволяє оцінити кваліфікаційну роботу студента Остапенко Олександра Станіславовича на оцінку «відмінно», та присвоїти їй кваліфікацію «магістр з комп'ютерної інженерії».

Керівник кваліфікаційної роботи _____ Наталія ЛАЩЕВСЬКА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«_» _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач *Остапенко О. С.* допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою Комп'ютерної інженерії _____ Наталія ЛАЩЕВСЬКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Остапенко Олександр Станіславович
(прізвище, ім'я, по батькові)
на тему: «Методи посилення безпеки корпоративних мереж шляхом інтеграції систем аутентифікації та міжмережевого екранування»

Актуальність:

Кваліфікаційна магістерська робота присвячена методам комплексної системи захисту корпоративної мережі шляхом інтеграції сучасних апаратних та програмних засобів. Тема є вкрай актуальною, оскільки робота пропонує практичні механізми переходу від базового захисту до ешелонованої оборони з використанням архітектури AAA, протоколу RADIUS та міжмережевих екранів нового покоління. Це дозволяє вирішити критичні завдання щодо розмежування доступу та захисту конфіденційних даних у сучасних інфраструктурах.

Позитивні сторони:
1. У процесі виконання роботи автором було ґрунтовно досліджено та порівняно різні протоколи автентифікації, що дозволило обґрунтувати вибір FreeRADIUS як оптимального рішення для поставленої задачі.
2. Автор поєднав теоретичні положення з практичною реалізацією – розробив детальну топологію мережі з поділом на зони безпеки та впровадив віртуальні локальні мережі для ізоляції трафіку.
3. Цінним є практичне налаштування захищеного адміністративного доступу до мережевого обладнання Cisco та реалізація політик фільтрації на шлюзі FortiGate, що підтверджено результатами тестування.

Недоліки:
1. В роботі недостатньо детально розкрито налаштування додаткових функцій безпеки шлюзу FortiGate, таких як глибока інспекція пакетів або налаштування IPS-сигнатур, акцент зроблено переважно на політиках доступу.
2. Бажано розглянути сценарії забезпечення відмовостійкості для ключових вузлів мережі, зокрема для сервера AAA та маршрутизатора, оскільки в роботі використано по одному екземпляру обладнання

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної бакалаврської роботи.

Висновок: *кваліфікаційна бакалаврська робота заслуговує оцінку " відмінно", а здобувач Остапенко О. С. заслуговує присвоєння кваліфікації: магістр з комп'ютерної інженерії.*

Рецензент: _____ _____
науковий ступінь, вчене звання *підпис* *Ім'я, ПРІЗВИЩЕ*

ЗМІСТ

ВСТУП.....9
1 ТЕОРЕТИЧНІ ЗАСАДИ ПРОЕКТУВАННЯ ТА БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ.....11
1.1 Огляд методів забезпечення безпеки комп'ютерних мереж.....11
1.2 Дослідження актуальних технологій мережевої безпеки.....14
1.3 Рішення для автентифікації в комп'ютерних мережах: пристрої та додатки.20
2 ПРОЕКТУВАННЯ ПІДСИСТЕМИ БЕЗПЕКИ ДЛЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ.....24
2.1 Проектування загальної схеми комп'ютерної мережі.....24
2.2 Організація системи міжмережевого екранування.....28
2.3 Розробка комплексної системи захисту мережевого обладнання із застосуванням сучасних методик та технологічних рішень.....31
2.4 Проектування та реалізація підсистеми централізованої автентифікації з використанням протоколу RADIUS.....33
3 РЕАЛІЗАЦІЯ, КОНФІГУРУВАННЯ ТА ВЕРИФІКАЦІЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ.....37
3.1 Обґрунтування вибору апаратного забезпечення для побудови захищеної мережевої інфраструктури.....37
3.2 Практичне налаштування компонентів мережевої інфраструктури.....41
3.3 Розгортання та параметризація служби RADIUS.....46
3.4 Впровадження політик безпеки на пристрої FortiGate.....52
3.5 Тестування функціональності компонентів захищеної системи.....55
ВИСНОВКИ.....61
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....63
Додаток А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація).....66

ВСТУП

У сучасному цифровому світі забезпечення захисту інформації є пріоритетним завданням для будь-якої організації. Корпоративні мережі, які забезпечують комунікацію та обмін даними, стають головною мішенню для кіберзлочинців. Зростання кількості загроз, таких як несанкціонований доступ, віруси, DDoS-атаки та інсайдерські загрози, вимагає від компаній впровадження комплексних підходів до безпеки.

Традиційних методів захисту вже недостатньо; надійна система вимагає інтеграції як програмних, так і апаратних рішень, чіткої сегментації мережі та суворого контролю доступу. Особливої ваги набуває впровадження систем AAA (Authentication, Authorization, Accounting), які дозволяють точно ідентифікувати користувачів та контролювати їхні дії. Тому розробка методів посилення безпеки шляхом інтеграції сучасних технологій маршрутизації, екранування та автентифікації є вкрай актуальною задачею.

Мета і завдання дослідження. Метою роботи є розробка методів безпеки корпоративної мережі, які забезпечують мінімізацію ризиків несанкціонованого доступу та захист конфіденційних даних.

Для досягнення мети вирішено такі завдання:

1. Проаналізувати теоретичні засади та методи забезпечення апаратної та програмної безпеки мереж.
2. Спроектувати топологію мережі з використанням зонування та VLAN для ізоляції трафіку.
3. Обґрунтувати вибір мережевого обладнання та програмного забезпечення для реалізації проекту.
4. Впровадити систему централізованої автентифікації на базі протоколу RADIUS та сервера FreeRADIUS.
5. Налаштувати політики міжмережевого екранування на обладнанні FortiGate та маршрутизацію OSPF

6. Провести тестування ефективності впроваджених заходів захисту.

Об’єкт дослідження – корпоративна телекомунікаційна мережа. Предмет дослідження – методи та засоби захисту мережевої інфраструктури від зовнішніх та внутрішніх загроз.

Методи дослідження. У роботі використано методи системного аналізу для проектування топології, методи моделювання мережевих процесів, а також емпіричні методи для перевірки налаштувань обладнання Cisco та Fortinet.

Практичне значення. Розроблене рішення дозволяє створити захищений периметр корпоративної мережі з централізованим керуванням доступом, що може бути використане для модернізації інфраструктури підприємств малого та середнього бізнесу.

1 ТЕОРЕТИЧНІ ЗАСАДИ ПРОЕКТУВАННЯ ТА БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Огляд методів забезпечення безпеки комп'ютерних мереж

Забезпечення захисту інформації є пріоритетним завданням для будь-якої організації. Багато компаній активно впроваджують передові програмні рішення у сфері кібербезпеки, щоб убезпечити корпоративні та клієнтські дані від широкого спектра загроз. Комп'ютерна безпека охоплює захист усіх апаратних (hardware) та програмних (software) компонентів, що використовуються в персональних комп'ютерах. У сучасному світі комп'ютери зберігають величезні обсяги інформації. Як окремі пристрої, так і цілі системи, що передають дані, комунікують між собою в глобальному масштабі. Навіть у локальних мережах можуть міститися мільярди сторінок текстового, графічного та іншого контенту. Ключова мета кібербезпеки полягає в захисті даних та активів від крадіжки, пошкодження чи природних катастроф, при цьому зберігаючи їхню доступність для авторизованих користувачів[1].

Апаратна безпека (Hardware security) — це комплекс заходів, спрямованих на захист фізичного обладнання комп'ютера та його периферійних пристроїв від зовнішніх загроз. Цей підхід часто передбачає використання спеціалізованих інтегральних схем, розроблених для виконання криптографічних операцій та захисту від атак. Такий захист забезпечує стійкість до вразливостей операційної системи та інших "дірок" у безпеці.

Програмна безпека (Software security) фокусується на захисті програмного забезпечення від різноманітних ризиків та загроз. Її головне завдання — гарантувати автентифікацію, цілісність та доступність даних. Програмне забезпечення часто вважається головним джерелом проблем у безпеці і, можливо, найбільш вразливою ланкою в усій системі захисту, не

враховуючи людський фактор. Саме тому безпеці програмних продуктів необхідно приділяти особливу увагу.

Як правило, ризики апаратного рівня пов'язані з використанням застарілого або специфічного обладнання. Аналогічно, програмні ризики часто виникають через застаріле або специфічне програмне забезпечення. Обидва аспекти необхідно враховувати при розробці ключових показників ефективності (KPI)[2] у сфері кібербезпеки, щоб забезпечити комплексний захист бізнесу. Отже, для побудови надійної системи захисту мережі недостатньо лише програмних методів; їх необхідно доповнювати апаратними рішеннями.

До апаратного захисту належать пристрої, що виконують сканування системи або моніторинг мережевого трафіку. Поширеними прикладами є апаратні брандмауери та проксі-сервери. Рідше зустрічаються апаратні модулі безпеки (HSM), які генерують та зберігають криптографічні ключі для критично важливих операцій, таких як шифрування, дешифрування та автентифікація в різних системах.

Безпека на рівні обладнання є такою ж важливою, як і безпека програмного коду. Оцінка захищеності апаратного пристрою вимагає аналізу вразливостей, що могли виникнути ще на етапі виробництва, а також інших потенційних векторів атаки, таких як виконуваний код або процеси введення/виведення даних.

Будь-яке обладнання, від старих комп'ютерів до сучасних пристроїв Інтернету речей (IoT)[18], може стати джерелом серйозних проблем безпеки, якщо організація не дотримується встановлених найкращих практик. Для мінімізації ризиків під час налаштування та встановлення обладнання рекомендується вживати таких контрзаходів:

— Ретельна перевірка продавців та постачальників.

— Застосування шифрування на пристроях.

— Зменшення "поверхні атаки" (attack surface).

— Забезпечення фізичної охорони обладнання.

— Використання методів електронного захисту.

— Впровадження моніторингу в реальному часі.

— Своєчасне оновлення прошивок (firmware) та заміна застарілого обладнання.

— Проведення регулярних аудитів безпеки.

Перевірка продавців і постачальників. Ризики безпеки обладнання закладаються на самому[3] початку — в ланцюгу постачання. Виробництво апаратних компонентів з дефектами або навмисними вразливостями ("бекдорами") може поставити під загрозу пристрої ще до їх експлуатації.

Шифрування пристроїв. Критично важливо шифрувати всі апаратні пристрої, де зберігаються дані, включно із зовнішніми флеш-накопичувачами та інтерфейсами оперативної пам'яті (DRAM).

Мінімізація поверхні атаки. Обладнання, яке більше не використовується, має бути безпечно та коректно виведене з експлуатації. Це допомагає запобігти небажаним атакам на забуті або залишені пристрої.

Забезпечення фізичної охорони. Компанії зобов'язані впроваджувати суворі політики контролю доступу до приміщень, де фізично розміщене обладнання (наприклад, серверних кімнат)[19].

Використання електронного захисту. Повноцінний план апаратної безпеки неможливий без належного електронного захисту. Це може включати, наприклад, використання захищеної зони (secure enclave) для зберігання головного ключа шифрування, щоб запобігти його фізичному вилученню або підробці.

Моніторинг у реальному часі. Командам, відповідальним за безпеку, варто налаштовувати системи моніторингу стану апаратного забезпечення та операційних систем у режимі реального часу для негайного виявлення аномалій.

Оновлення прошивки та обладнання. Апаратні пристрої повинні мати найновіші версії прошивок, оскільки оновлення часто містять виправлення критичних вразливостей безпеки.

Регулярний аудит. Періодичні перевірки апаратного забезпечення дозволяють відстежувати будь-які зміни в мережевій інфраструктурі та своєчасно виявляти нові операційні ризики.

Апаратна безпека має вирішальне значення, оскільки цей рівень часто містить уразливості, які можуть залишатися невиправленими роками, роблячи їх легкою мішенню для зловмисників. Саме тому захист апаратного забезпечення, особливо в пристроях Інтернету речей (IoT), слід сприймати з такою ж серйозністю, як і будь-які інші мережеві загрози[20].

1.2 Дослідження актуальних технологій мережевої безпеки

Забезпечення безпеки мережі є одним із пріоритетних завдань при її проектуванні. Сама по собі, мережева безпека — це комплексна екосистема, що поєднує людей, процеси, політики та технології. Ці компоненти застосовуються в рамках багаторівневого підходу для створення такого мережевого середовища, яке б, з одного боку, підтримувало високу продуктивність організації, а з іншого — мінімізувало ризики неправомірного використання з боку як зовнішніх, так і внутрішніх загроз.

Людський фактор, чіткі процедури та продумана політика є фундаментальними елементами[4] впровадження безпеки. Вони функціонують спільно для досягнення стратегічних цілей та формують різні типи засобів контролю, які визначають, як саме будуть застосовуватися технологічні рішення.

Надійна мережева безпека є критично важливою для захисту конфіденційної інформації (як клієнтської, так і корпоративної), гарантування безпеки спільних даних, забезпечення стабільного доступу до ресурсів та протидії кібератакам. Ефективно спроектована система безпеки допомагає зменшити операційні витрати та захищає організацію від значних фінансових

збитків, спричинених витоком даних чи іншими інцидентами. Надання легітимного доступу до систем та додатків є основою для стабільних бізнес-операцій та надання послуг клієнтам.

Заходи мережевої безпеки прийнято поділяти на три основні категорії[5]:

— фізичні засоби контролю;

— адміністративні засоби (контроль даних і доступу);

— технічні засоби контролю.

Фізичні засоби контролю Ці засоби використовуються для запобігання несанкціонованому фізичному контакту з ключовими мережевими компонентами організації. Класичним прикладом є обмеження доступу до центрів обробки даних або серверних кімнат за допомогою замків та ключ-карт. До інших типів належать служба охорони, системи відеоспостереження, ідентифікаційні посвідчення та біометричні сканери.

Адміністративні засоби (Контроль даних і доступу) Ці елементи охоплюють процеси та політики, що регламентують дії співробітників під час роботи з конфіденційною інформацією, програмами та системами. Прикладами адміністративного контролю є політика паролів, правила використання особистих мобільних пристроїв та затверджені плани реагування на інциденти.

Технічні засоби контролю Діючи як активні запобіжні заходи або контрзаходи, ці засоби впроваджуються безпосередньо за допомогою технологій безпеки для захисту критично важливих ділянок мережевого середовища.

Успішна багаторівнева стратегія безпеки вимагає впровадження цілого ряду технологій, кожна з яких вирішує проблему зловмисних атак з власного ракурсу. До найпоширеніших технологій належать[6]:

— Безпечний віддалений доступ;

— Брандмауер (Firewall);

— Віртуальна приватна мережа (VPN);

— Запобігання/пом’якшення DDoS-атак;

— Безпека додатків;

— Посередник безпеки доступу до хмари (CASB);

— Система запобігання вторгненням (IPS);

— Веб-безпека;

— Безпека електронної пошти;

— Запобігання втраті даних (DLP);

— Сегментація мережі;

— Пісочниця (Sandboxing);

— Гіпермасштабність.

Безпечний віддалений доступ та контроль доступу Контроль доступу є фундаментальним, оскільки він обмежує, які саме користувачі та пристрої отримують дозвіл на взаємодію з конкретними внутрішніми чи хмарними ресурсами. Сучасні підходи включають архітектуру Zero Trust (нульова довіра), яка полегшує доступ до ресурсів без необхідності логічного розміщення користувача в корпоративній мережі, а також захищений віддалений доступ, що поєднує безпеку кінцевих точок, автентифікацію та шифрування з'єднань.

Брандмауер (Firewall) Брандмауери діють як "цифрові охоронці" на логічному периметрі мережі. Вони перевіряють вхідний та вихідний трафік, у режимі реального часу вирішуючи, дозволити чи заборонити його на основі визначеного набору правил безпеки.

Віртуальна приватна мережа (VPN) Технологія VPN створює зашифрований з'єднувальний канал (тунель) між віддаленою кінцевою точкою (наприклад, комп'ютером користувача, що працює з дому) та внутрішньою корпоративною мережею.

Запобігання/пом’якшення DDoS Атаки типу "розподілена відмова в обслуговуванні" (DDoS) спрямовані на перевантаження мережевих пристроїв (брандмауерів, серверів) шляхом насичення каналу зв'язку або вичерпання системних ресурсів величезною кількістю запитів. Технології пом'якшення

DDoS намагаються відфільтрувати цей шкідливий трафік, дозволяючи легітимним користувачам продовжувати роботу.

Безпека додатків Багато програм, а також операційні системи, на яких вони працюють, містять уразливості. Технології безпеки програм спрямовані на виявлення та усунення цих слабких місць. У контексті мережевої безпеки, ключовим інструментом є брандмауер веб-програм (Web Application Firewall, WAF).

Посередник безпеки доступу до хмари (CASB) CASB[7] — це набір технологій, розроблених для захисту онлайн-сервісів, програм та хмарних середовищ від загроз, враховуючи специфіку хмари (доступ у будь-який час, з будь-якого місця та пристрою).

Система запобігання вторгненням (IPS) На відміну від брандмауера, який зазвичай працює на основі простих правил (протоколи, порти), IPS проводить глибокий аналіз мережевого трафіку. Вона використовує дані про загрози (сигнатури) для виявлення та блокування потенційно зловмисної активності, яка може імітувати легітимний трафік.

Веб-безпека Технології веб-безпеки фокусуються на вихідному інтернет-трафіку співробітників, блокуючи доступ до шкідливих веб-сайтів та фільтруючи загрози, що передаються через Інтернет.

Безпека електронної пошти Цей термін охоплює будь-які процеси та продукти, призначені для захисту облікових записів електронної пошти та їх вмісту від зовнішніх загроз (наприклад, фішингу, спаму, шкідливих вкладень).

Запобігання втраті даних (DLP) DLP — це методологія, що поєднує технології та найкращі практики для запобігання розкриттю (витоку) конфіденційної інформації за межі організації. Це особливо важливо для регульованих даних, таких як персональна ідентифікаційна інформація (PII) та дані, що підпадають під стандарти HIPAA, SOX, PCI DSS тощо.

Сегментація мережі Ця практика полягає у визначенні логічних кордонів між сегментами мережі, де активи групуються за спільною функцією, ризиком або роллю. Наприклад, периметральний шлюз сегментує всю мережу компанії

від Інтернету. Організації можуть створювати додаткові внутрішні кордони (мікросегментацію) для посилення безпеки та контролю доступу.

Пісочниця (Sandboxing) Це практика кібербезпеки, що полягає у запуску коду або відкритті файлів у безпечному, ізольованому середовищі, яке імітує операційне середовище кінцевого користувача. "Пісочниця" спостерігає за поведінкою файлу (наприклад, PDF або документа Word) і, якщо виявляє зловмисну активність, блокує загрозу до того, як вона потрапить у реальну мережу.

Гіпермасштабність Це здатність архітектури гнучко масштабуватися (збільшуватися або зменшуватися) відповідно до зростання попиту на ресурси. Це рішення дозволяє швидко розгортати необхідні потужності безпеки. Воно досягається завдяки тісній інтеграції мережевих та обчислювальних ресурсів у єдину програмно визначену систему.

Підсистема захисту мережі повинна забезпечувати повноцінну протидію таким поширеним кіберзагрозам:

— Вірус: Зловмисний файл, здатний до самовідтворення шляхом модифікації інших програм власним кодом. Може перебувати у стані бездіяльності та активуватися за певних умов, пошкоджуючи або знищуючи дані.

— Хробак (Черв'як): Окреме зловмисне ПЗ, яке, на відміну від вірусу, поширюється самостійно, не потребуючи хост-програми. Хробаки часто уповільнюють роботу мережі, поглинаючи її пропускну здатність.

— Троян: Бекдор-програма, що маскується під легітимне ПЗ[8]. Після активації вона надає зловмисникам несанкціонований доступ до комп'ютерної системи.

— Шпигунське ПЗ: Програмне забезпечення, яке таємно збирає інформацію про особу чи організацію та надсилає її третій стороні без згоди користувача.

— Рекламне ПЗ: Програми, що збирають маркетингові дані про користувача (історію пошуку, покупок) для показу персоналізованої реклами, часто перенаправляючи пошукові запити на рекламні сайти.

— Програми-вимагачі: Тип шкідливого ПЗ, яке шифрує дані користувача, роблячи їх непридатними для використання, та блокує доступ до системи з метою отримання грошового викупу.

Багато організацій будують свої стратегії захисту, спираючись на загальноприйняті рамки (фреймворки) та принципи безпеки. Найпоширеніші з них:

— NIST Cybersecurity Framework: Розроблений Національним інститутом стандартів і технологій США, цей фреймворк надає функції, результати та довідкові матеріали для побудови та вдосконалення стратегії кібербезпеки.

— Засоби безпеки CIS (CIS Controls): Центр безпеки в Інтернеті (CIS) пропонує 20 спеціальних засобів керування, розроблених для створення надійного та постійно захищеного мережевого середовища.

— MITRE ATT&CK Framework: Ця структура, хоч і зосереджена на тактиках і техніках атак, також надає детальні вказівки щодо методів пом'якшення та протидії кібератакам.

— Нульова довіра (Zero Trust): Принцип мережевої безпеки, що базується на ідеї "ніколи не довіряй, завжди перевіряй". Ця концепція, спочатку запропонована Forrester, еволюціонувала у повноцінну архітектуру, для якої NIST також розробив відповідну структуру.

Використання однієї або декількох із цих структур надає організаціям достатньо вказівок для початку розбудови комплексної стратегії безпеки мережі. Вони допомагають визначити необхідні компоненти — людей, процеси, політики та технології — для створення належного захисту від кіберзагроз, що постійно змінюються.

1.3 Рішення для автентифікації в комп'ютерних мережах: пристрої та додатки

Концепція AAA (Authentication, Authorization, and Accounting) є фундаментальним елементом мережевої безпеки, оскільки вона надає механізми для обмеження доступу до системних ресурсів та відстеження дій користувачів[9]. По суті, AAA — це система безпеки, що контролює доступ до комп'ютерних ресурсів, забезпечує дотримання політик та перевіряє використання цих ресурсів. Комбінація цих трьох процесів відіграє критичну роль в управлінні мережею та кібербезпеці, дозволяючи перевіряти користувачів та моніторити їхню активність під час підключення.

Система AAA функціонує як три послідовні та взаємозалежні кроки, де наступний не може розпочатися без успішного завершення попереднього. Зазвичай ці протоколи реалізовані на централізованому сервері, який автоматично виконує всі три функції. Такий підхід значно спрощує для IT-команд підтримку мережевої безпеки та гарантує, що користувачі отримують доступ виключно до тих ресурсів, які необхідні їм для виконання завдань.

Автентифікація (Authentication) Це початковий процес, метою якого є ідентифікація користувача та надання йому доступу до мережі. Найчастіше це реалізується через традиційну пару "ім'я користувача та пароль". Проте, можуть використовуватися й альтернативні методи автентифікації, такі як біометричні дані (сканування відбитків пальців або сітківки ока) або апаратні токени та смарт-карти. На цьому етапі сервер порівнює надані облікові дані з тими, що зберігаються в його базі даних. У багатьох корпоративних середовищах для зберігання та аналізу цих даних використовується служба каталогів Active Directory.

Авторизація (Authorization) Після успішної автентифікації починається процес авторизації, який забезпечує виконання мережевих політик, детальний контроль доступу та визначення привілеїв користувача. Протокол AAA

визначає, до яких саме мережевих ресурсів (наприклад, баз даних, програм чи сервісів) користувач отримує дозвіл. Крім того, він встановлює, які конкретні завдання та дії (наприклад, читання, запис, видалення, виконання) користувач може виконувати в межах цих ресурсів.

Наприклад, співробітник відділу продажів після входу в мережу може отримати дозвіл на використання лише CRM-системи, тоді як доступ до систем управління персоналом (HR) чи планування ресурсів (ERP) йому буде заборонено. Більше того, навіть у CRM[13] його права можуть бути обмежені лише переглядом та редагуванням даних, без можливості адміністрування інших користувачів. Саме процес авторизації відповідає за дотримання цих правил .

Аудит або Облік (Accounting) Це фінальний процес у структурі AAA, який полягає у вимірюванні та фіксації того, що відбувається в мережі. Протокол збирає та реєструє дані про сеанси користувачів, включаючи їх тривалість, тип сеансу та обсяг спожитих ресурсів. Цінність цього етапу полягає у створенні чіткого "контрольного сліду" (audit trail), який можна використовувати для бізнес-аналізу та підтвердження відповідності стандартам. Дані обліку допомагають як у забезпеченні безпеки, так і в оперативних оцінках. Наприклад, адміністратори мережі можуть аналізувати ці дані, щоб переглянути привілеї доступу користувачів або регулювати потужність системи на основі інформації про найбільш використовувані ресурси та загальні тенденції активності .

На сьогодні існує декілька протоколів для реалізації моделі AAA. Розглянемо три основних :

— TACACS+ (Terminal Access Controller Access Control Server)[10]: Протокол безпеки, що використовується для централізованої автентифікації користувачів, які бажають отримати доступ до мережі. Переваги: Використовує надійне з'єднання на базі TCP , має можливість гнучкого адміністрування привілеїв , підтримує повне шифрування переданих пакетів

та чітко розділяє всі три функції (автентифікацію, авторизацію та аудит). Недоліки: Є пропрієтарним протоколом компанії Cisco.

— RADIUS (Remote Authentication Dial-In User Service): Широко розповсюджений мережевий протокол, що забезпечує централізовану автентифікацію, авторизацію та облік для користувачів, які підключаються до віддаленої мережі. Переваги: Має широку підтримку серед різних виробників обладнання та вирізняється простотою у використанні. Недоліки: Використовує ненадійний протокол UDP , не забезпечує повного шифрування пакетів (шифрується лише пароль) та об'єднує процеси автентифікації й авторизації.

— DIAMETER: Протокол нового покоління, що прийшов на заміну RADIUS, і є галузевим стандартом для мереж LTE та IP Multimedia Systems (IMS). Переваги: Підтримує надійні протоколи TCP і SCTP , захист з'єднання за допомогою TLS , забезпечує підтримку роумінгу та контроль доступу в мережах LTE. Недоліки: На поточний момент має значно нижчий рівень підтримки обладнанням порівняно з RADIUS[12].

Після аналізу та порівняння теоретичних відомостей про кожен з протоколів AAA, було ухвалено рішення про доцільність використання протоколу RADIUS. Його простота у використанні та широка підтримка роблять його оптимальним вибором для впровадження у простих локальних мережах.

Після вибору протоколу необхідно визначитись із серверним програмним забезпеченням для його реалізації. Нижче наведено порівняння поширених рішень :

— FreeRADIUS: Це модульний, високопродуктивний та безкоштовний пакет RADIUS, що розповсюджується за ліцензією GNU GPL v2. На сьогодні це найпопулярніший RADIUS-сервер з відкритим вихідним кодом у світі. Він підтримує всі поширені протоколи автентифікації та постачається з веб-інструментом адміністрування на основі PHP.

— JumpCloud: Хмарна платформа каталогів, що реалізує захист ідентичності та керування пристроями (Windows, Mac, Linux) за моделлю "нульової довіри" . Вона дозволяє автентифікувати та авторизувати користувачів через єдиний хмарний каталог замість застарілих локальних систем.

— TekRADIUS: RADIUS-сервер, розроблений для Windows (тестувався на Windows XP, Vista, 7, 2003/2008) . Він відповідає стандартам RFC 2865 та RFC 2866 , працює як служба Windows та має інтерфейс керування Win32. Наразі підтримує лише Microsoft SQL Server для зберігання даних та дозволяє обмежувати одночасні сеанси користувачів.

— MikroTik RouterOS: Операційна система на базі ядра Debian GNU/Linux, створена спеціально для апаратного забезпечення MikroTik RouterBOARD . Цей сервіс дозволяє перетворити пристрій на маршрутизатор з усіма необхідними функціями, включаючи брандмауер, VPN-шлюз, точку доступу тощо.

— AuthenticateMyWiFi: Хмарний сервіс, що надає послуги автентифікації, аналогічні RADIUS, але позиціонується як простий в установці та адмініструванні. Завдяки своїй хмарній природі, він не прив'язаний до сумісності з ОС і може керуватися віддалено через будь-який інтернет-браузер[11].

Проаналізувавши всі доступні серверні рішення, їхні головні відмінності та переваги, для використання в даній роботі було обрано FreeRADIUS. Це рішення було прийнято на основі наступних переваг: можливість одночасного обслуговування понад мільйона користувачів, високий рівень масштабованості, поширеність у дистрибутивах Linux, наявність відкритого вихідного коду та безкоштовність.

2 ПРОЕКТУВАННЯ ПІДСИСТЕМИ БЕЗПЕКИ ДЛЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Проектування загальної схеми комп'ютерної мережі

Проектування є фундаментальним та початковим етапом у процесі створення будь-якої комп'ютерної мережі. За своєю суттю, комп'ютерна мережа є сукупністю обчислювальних пристроїв (вузлів), які з'єднані між собою для спільного обміну даними та використання ресурсів. Зв'язок між цими пристроями реалізується за допомогою дротових (кабельних) або бездротових технологій.

Після того, як з'єднання встановлено, обмін даними між мережевими пристроями регулюється стандартизованими комунікаційними протоколами, до яких належать TCP/IP, простий протокол передачі пошти (SMTP) та протокол передачі гіпертексту (HTTP).

В основі даної магістерської кваліфікаційної роботи лежить специфічна схема, що інтегрує визначений набір технологій та проектних рішень. Загальна архітектура проекту, включно з візуальним розмежуванням на функціональні області, представлена на рис. 2.1.

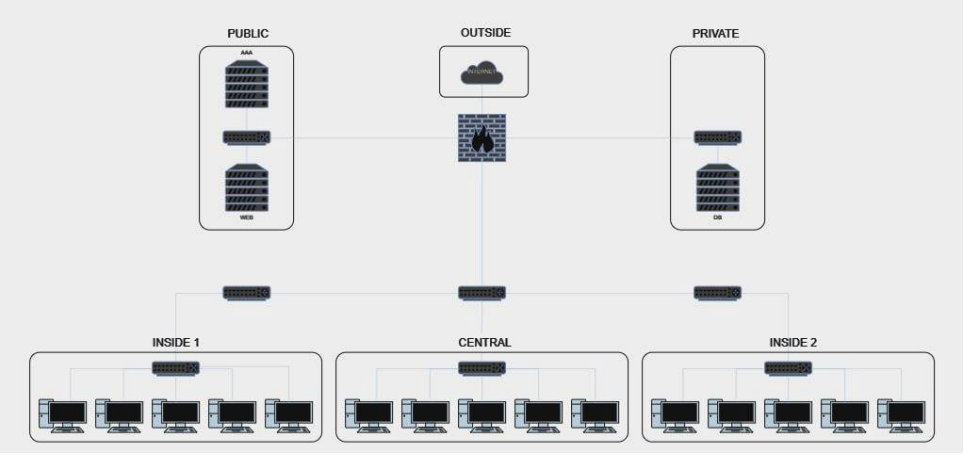


Рисунок 2.1 – Загальна топологія мережі

Представлена вище візуалізація демонструє загальну архітектуру комп'ютерної мережі. Вона передбачає сегментацію на декілька ключових областей доступу, а саме: public, private, outside, central, inside1 та inside2.

Основна мета такого поділу — забезпечення контролю над трафіком, що переміщується між зонами, які мають різні рівні довіри та політики безпеки.

Наступним логічним кроком після визначення загальної топології є розробка схем IP-адресації та маршрутизації. Планується застосування гібридного підходу до адресації: статичні IP-адреси (static) будуть зарезервовані для пристроїв з фіксованою адресою (наприклад, серверів), тоді як динамічна адресація (DHCP) використовуватиметься для автоматичного конфігурування кінцевих робочих пристроїв.

Для забезпечення зв'язності між різними підмережами та автоматизації обміну маршрутною інформацією, в якості протоколу динамічної маршрутизації було обрано OSPF. Детальний план розподілу IP-адрес наведено у табл.2.1.

Таблиця 2.1 - План логічної адресації вузлів

Назва вузла	Порт/ID	Режим налаштування	IPv4	Обмін маршрутами
Сервер AAA	E0	Static	172.16.10.100/24	OSPF
Сервер WEB	E0	Static	172.16.10.200/24	
Сервер DB	E0	Static	172.16.20.100/24	
Фаєрвол F1	P1	Static	172.16.10.1/24	
	P2	Static	172.16.20.1/24	
	P3	DHCP	*	
	P4	Static	192.168.2.1/24	
Switch Sw1	Vlan 100	Static	172.16.10.10/24	
Switch Sw2	Vlan 100	Static	192.168.5.100/24	

Продовження таблиці 2.1

Switch Sw3	Vlan 100	Static	192.168.1.100/24	
Switch Sw4	Vlan 100	Static	192.168.6.100/24	
Switch Sw5	Vlan 100	Static	172.16.20.10/24	
Маршрутизатор R1	Fe0/0	Static	192.168.3.2/24	
	Fe0/1	Static	192.168.5.1/24	
Маршрутизатор R2	Fe0/0	Static	192.168.2.2/24	
	Fe0/1	Static	192.168.1.1/24	
	Fe1/0	Static	192.168.3.1/24	
	Fe1/1	Static	192.168.4.1/24	
Маршрутизатор R3	Fe0/0	Static	192.168.4.2/24	
	Fe0/1	Static	192.168.6.1/24	
Робоча станція	*	DHCP	*	

Щоб гарантувати необхідні обчислювальні потужності та забезпечити спільний доступ до інформаційних активів, потрібно спроектувати архітектуру зберігання даних та керування доступом. Ефективним рішенням цієї задачі є розгортання спеціалізованих серверів із чітким розмежуванням їхніх функцій. За визначенням, мережеві сервери — це високопродуктивні обчислювальні системи, що виступають центральними вузлами для розподілу спільних ресурсів (таких як дисковий простір, периферійне обладнання, поштові служби тощо) між клієнтами мережі. Перелік та характеристики серверів, що використовуються у даному проекті, наведені у табл.2.2.

Таблиця 2.2 - Архітектура серверної інфраструктури

Вузол інфраструктури	Сегмент мережі	Функціональна роль	Призначення та задачі
Сервер AAA	Public	Служба контролю доступу	Виконує централізовану верифікацію користувачів та пристроїв, керує правами доступу та веде журнал подій безпеки (аудит).
Веб-сервер (WEB)	Public	Веб-хостинг	Забезпечує функціонування корпоративних веб-ресурсів та надає доступ до них через браузер для авторизованих клієнтів.
Сервер БД (DB)	Private	Система керування базами даних	Ізольований ресурс для безпечного накопичення та обробки даних, що використовуються веб-сервісами та системою AAA.

Наступним критично важливим етапом проектування є забезпечення доступу внутрішніх вузлів корпоративної мережі до зовнішнього інформаційного простору. Реалізація цього завдання передбачає встановлення фізичного та логічного з'єднання з мережею провайдера, а також налаштування технології трансляції мережевих адрес (NAT).

Глобальна мережа Інтернет є всесвітньою системою об'єднаних комп'ютерних мереж, що побудована на використанні стека протоколів TCP/IP. Вона слугує універсальним середовищем для обміну даними, ресурсами та комунікації між мільйонами пристроїв по всій планеті .

Ключовою умовою для виходу в глобальну мережу є наявність зовнішньої (публічної) IP-адреси. Цей унікальний ідентифікатор дозволяє

визначати місцезнаходження систем у глобальному просторі. Публічні адреси надаються Інтернет-провайдером (ISP) і, як правило, присвоюються прикордонному маршрутизатору, який виступає шлюзом для всієї локальної інфраструктури .

Для того щоб група внутрішніх пристроїв із приватними адресами могла виходити в Інтернет, використовуючи лише одну публічну адресу, застосовується технологія NAT (Network Address Translation). Цей механізм дозволяє мережевому пристрою (маршрутизатору або брандмауеру) діяти як посередник: він замінює внутрішні адреси джерела на свою зовнішню адресу в пакетах, що виходять у глобальну мережу .

Використання NAT вирішує дві важливі задачі:

1. Економія адресного простору: дозволяє значній кількості локальних хостів працювати через одну публічну IP-адресу.
2. Безпека: приховує внутрішню структуру та адресацію локальної мережі від зовнішніх спостерігачів.

Таким чином, завдяки підключенню до провайдера та налаштуванню механізму NAT, корпоративна мережа отримує повноцінний та захищений доступ до ресурсів Інтернету.

2.2 Організація системи міжмережевого екранування

Ключовим елементом для забезпечення надійності інфраструктури та контролю інформаційних потоків є використання брандмауера (міжмережевого екрану). Це система безпеки, що виступає бар'єром проти несанкціонованого доступу, контролюючи як вхідні, так і вихідні з'єднання комп'ютерної мережі .

Головне завдання брандмауера — ізолювати довірену внутрішню мережу (інтранет) від ненадійного зовнішнього середовища (Інтернету). Він розміщується на межі цих мереж і діє як контрольно-пропускний пункт. Без такого захисту мережа стає вразливою: конфіденційні дані можуть безперешкодно виходити назовні, а зловмисники або шкідливі програми — проникати всередину .

Сучасний брандмауер — це комплексне рішення кібербезпеки (апаратне або програмне), яке інспектує та автентифікує пакети даних перед тим, як дозволити їм потрапити у захищене середовище. Він слугує першою лінією оборони організації, фільтруючи трафік на різних рівнях, включаючи перевірку онлайн-транзакцій та прикладних протоколів .

Ефективність брандмауера базується на наборі попередньо налаштованих правил (політик). Ці правила не лише блокують зовнішні загрози (віруси, хакерські атаки), але й можуть сегментувати внутрішню мережу, обмежуючи доступ певних груп користувачів до критичних ресурсів. Це дозволяє захистити вразливі системи та персональні дані від компрометації як ззовні, так і з боку інсайдерів .

Для практичної реалізації захищеного обміну даними в даному проекті було розроблено матрицю доступу, яка регламентує дозволений трафік між різними сегментами корпоративної мережі. Детальна схема контролю трафіку представлена у табл.2.3 .

Таблиця 2.3 - Архітектура системи мережевого захисту та фільтрації

Вхідний інтерфейс	Вихідний інтерфейс	Адреса джерела	Адреса призначення	Дозволений протокол
Inside	Outside	Будь-яка	Будь-яка	Всі (ALL)
Inside	Private	Хост CENTRAL	Зона PRIVATE	Telnet
Inside	Public	Будь-яка	Зона PUBLIC	Radius

Продовження таблиці 2.3

Inside	Public	Хост CENTRAL	Зона PUBLIC	HTTP
Inside	Public	Хост CENTRAL	Зона PUBLIC	Telnet
Private	Outside	Будь-яка	Будь-яка	Всі (ALL)
Private	Public	Зона PRIVATE	Зона PUBLIC	Radius
Public	Outside	Будь-яка	Будь-яка	Всі (ALL)
Public	Private	Зона PUBLIC	Зона PRIVATE	MySQL

У таблиці 2.3 систематизовано правила, що керують потоками даних у мережі. Архітектура безпеки побудована на принципі «заборони за замовчуванням» (default deny), що означає блокування будь-якого трафіку, який не дозволено явно. Нижче наведено пояснення до винятків, які формують дозволені маршрути:

1. Доступ до Інтернету: Для всіх внутрішніх зон дозволено ініціювати з'єднання в напрямку зовнішнього інтерфейсу (Outside). Це гарантує, що користувачі та сервіси всіх сегментів мережі мають стабільний вихід до глобальної мережі Internet.

2. Захист периметра: Вхідний трафік, ініційований із зовнішньої мережі (Outside) у будь-яку внутрішню зону, повністю блокується. Це створює надійний бар'єр, що відсікає зовнішні загрози та спроби несанкціонованого проникнення.

3. Ізоляція критичних даних: Звичайні робочі сегменти (Inside) ізольовані від захищеної зони (Private), де розташовано ядро зберігання даних. Це мінімізує ризики внутрішніх загроз та випадкового пошкодження інформації.

4. Регламентований доступ до DMZ: Взаємодія робочих станцій із публічною зоною (Public) дозволена, але суворо обмежена переліком необхідних протоколів, що запобігає безконтрольному використанню публічних ресурсів.

5. Міжсерверна взаємодія: Комунікація між публічною (Public) та приватною (Private) зонами дозволена виключно за специфічним протоколом, необхідним для обміну даними між веб-сервісами та базами даних.

6. Службовий трафік: Усім вузлам інфраструктури надано дозвіл на з'єднання з публічною зоною для обміну даними з сервером AAA (аутентифікація, авторизація, аудит).

Імплементація вищезазначених правил на апаратному рівні (за допомогою фаєрволу) дозволяє побудувати захищений мережевий контур із централізованим контролем доступу та детальним логуванням усіх подій безпеки .

2.3 Розробка комплексної системи захисту мережевого обладнання із застосуванням сучасних методик та технологічних рішень

Після реалізації периметрального захисту (міжмережевого екранування), критично важливим етапом є забезпечення безпеки внутрішніх вузлів мережі. Для цього розроблено комплекс заходів, спрямованих на посилення захищеності маршрутизаторів та комутаторів.

Для мінімізації вразливостей на рівні маршрутизації застосовуються такі методи:

— Деактивація невикористовуваних інтерфейсів: Адміністративне вимкнення всіх портів, що не задіяні в роботі, суттєво зменшує поверхню атаки та ризики фізичного несанкціонованого підключення.

— Інтеграція моделі AAA: Впровадження централізованої системи Authentication, Authorization, and Accounting дозволяє чітко ідентифікувати адміністраторів, розмежувати їхні права доступу та вести журнал усіх виконаних команд.

— Налаштування системних банерів (MOTD): Використання юридично значущих повідомлень при вході в систему, які попереджають користувачів про моніторинг активності та заборону несанкціонованого доступу.

— Застосування списків контролю доступу (ACL): Створення правил фільтрації, що обмежують доступ до інтерфейсів управління (VTY) лише з довірених IP-адрес адміністраторів.

— Перехід на захищені протоколи управління: Повна відмова від протоколу Telnet на користь SSH (Secure Shell) для забезпечення конфіденційності сесій керування.

Захист комутаційної інфраструктури включає всі вищезазначені методи для маршрутизаторів, доповнені специфічними функціями канального рівня (L2):

— Статична прив'язка портів до VLAN: Ручне призначення портів доступу до відповідних віртуальних локальних мереж замість використання налаштувань за замовчуванням.

— Реалізація Port Security: Механізм, що дозволяє обмежити кількість MAC-адрес на порту або прив'язати конкретну MAC-адресу до інтерфейсу. У разі порушення політики порт може бути автоматично заблокований.

— Захист протоколу STP (BPDU Guard): Функція, що вимикає порти доступу (access ports) при отриманні службових кадрів BPDU, запобігаючи створенню петель та підключенню несанкціонованих комутаторів.

— Відключення протоколів виявлення: Деактивація протоколу CDP (Cisco Discovery Protocol) на інтерфейсах, що дивляться в бік недовірених мереж або кінцевих користувачів, для запобігання витоку інформації про топологію та обладнання.

Для віддаленого адміністрування мережевих пристроїв обрано протокол SSH (Secure Shell). На відміну від застарілого Telnet, який передає дані у відкритому вигляді, SSH забезпечує захищений канал зв'язку через незахищені мережі (включаючи Інтернет).

Конфіденційність даних: Весь трафік сесії, включаючи логіни, паролі та конфігураційні команди, повністю шифрується. Це робить перехоплення даних (sniffing) марним для зловмисника, оскільки він не зможе розшифрувати інформацію без відповідних ключів.

Захист від атак "Людина посередині" (MITM): SSH використовує механізми автентифікації сервера. Завдяки генерації та перевірці пар криптографічних ключів (публічного та приватного), адміністратор може бути впевненим, що підключається саме до цільового пристрою, а не до підробленого вузла зловмисника, який намагається перехопити сесію.

2.4 Проектування та реалізація підсистеми централізованої автентифікації з використанням протоколу RADIUS

Ефективне розмежування прав доступу є запорукою стабільної та безпечної роботи налаштованої мережі. Для вирішення цього завдання впроваджується архітектура AAA (Authentication, Authorization, Accounting). Ця система забезпечує комплексний підхід до безпеки: вона ідентифікує користувачів, визначає дозволені їм ресурси та фіксує їхні дії протягом сеансу.

В якості транспортного протоколу для системи AAA обрано RADIUS. Це рішення базується на архітектурі клієнт-сервер:

— Клієнти: Мережеві пристрої (у даному випадку обладнання Cisco), які ініціюють запити.

— Сервер: Централізований вузол, що зберігає базу даних користувачів та політики доступу. Клієнти пересилають облікові дані користувачів на

сервер, який перевіряє їх та повертає відповідь про надання або заборону доступу .

Етапи налаштування компонентів AAA:

1. Налаштування Автентифікації (Authentication) Процес налаштування починається з активації моделі AAA та визначення списків методів автентифікації. Список методів вказує системі, які способи перевірки (наприклад, локальна база, сервер RADIUS) та в якому порядку слід використовувати. Особливість: Список default застосовується до всіх інтерфейсів автоматично, якщо адміністратор явно не призначив інший іменований список . Ключові команди:

aaa new-model — активація системи AAA.

aaa authentication login {default | list-name}— створення списку методів для входу в систему .

2. Налаштування Авторизації (Authorization) Цей етап визначає, які саме сервіси та команди доступні користувачеві після успішного входу. Система звертається до профілю користувача (на сервері або локально) для підтвердження прав на виконання певних дій .

Ключові команди:

aaa authorization network radius — авторизація запитів, пов'язаних із мережевими сервісами, через RADIUS.

aaa authorization exec radius — перевірка прав на доступ до привілейованого режиму командного рядка (EXEC) .

3. Налаштування Обліку (Accounting) Підсистема аудиту фіксує час початку та завершення сеансів, а також обсяг використаних ресурсів. Дані передаються на сервер у вигляді пар "атрибут-значення" (AV-pairs). Ця інформація є критично важливою для моніторингу безпеки та розслідування інцидентів .

Ключова команда:

aaa accounting network start-stop radius — активація запису подій початку та кінця мережевих сесій .

Система Cisco IOS підтримує 16 рівнів доступу (від 0 до 15). У рамках даного проекту було розроблено матрицю доступу, яка чітко регламентує набір дозволених команд для кожного рівня. Детальний розподіл прав наведено в табл. 2.4.

Таблиця 2.4 - Конфігурація ієрархії адміністративного доступу

Команда / Дія	Мінімальний необхідний рівень (Privilege Level)	Опис команди
exec > clock set	2+	Встановлення системного часу
exec > clock read-calendar	2+	Зчитування даних з апаратного календаря
exec > clock update-calendar	2+	Оновлення апаратного календаря
exec > configure terminal	2+	Вхід у режим глобальної конфігурації
configure > hostname	3+	Зміна імені пристрою
configure > banner	3+	Налаштування банера (MOTD)
configure > interface	4+	Вхід у режим налаштування інтерфейсу
interface > description	4+	Додавання опису до інтерфейсу
interface > shutdown	5+	Адміністративне вимкнення інтерфейсу
interface > ip address	5+	Присвоєння IP-адреси

Продовження таблиці 2.4

exec > copy run start	5+	Збереження конфігурації
configure > ip route	6+	Налаштування статичних маршрутів
configure > router	6+	Налаштування протоколів маршрутизації
router > network	6+	Оголошення мереж у маршрутизації
router > redistribute	7+	Перерозподіл маршрутів
configure > line (aux/console/vty)	8+	Налаштування ліній доступу

3 РЕАЛІЗАЦІЯ, КОНФІГУРУВАННЯ ТА ВЕРИФІКАЦІЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Обґрунтування вибору апаратного забезпечення для побудови захищеної мережевої інфраструктури

Ефективність та надійність корпоративної інфраструктури безпосередньо залежать від грамотного підбору апаратного забезпечення. Обрані пристрої повинні не лише задовольняти поточні потреби користувачів у пропускній здатності, але й забезпечувати надійний захист інформаційного периметра.

Для підприємств малого та середнього бізнесу (SMB)[15] критичним фактором є оптимізація капітальних витрат (CAPEX). Використання надпотужного обладнання рівня Enterprise (Core-рівня) є економічно невиправданим, тому пріоритет надається рішенням з оптимальним співвідношенням ціни та функціональності.

Основними критеріями вибору стали:

1. Підтримка стандартів GigabitEthernet на всіх інтерфейсах.
2. Можливість роботи з протоколами динамічної маршрутизації (OSPF, BGP).
3. Вбудовані функції безпеки.

На основі порівняльного аналізу актуальних лінійок обладнання компанії Cisco, для реалізації проекту було обрано маршрутизатор із інтегрованими сервісами Cisco ISR 1100 Series, а саме модель C1111-4P.

Цей пристрій працює під управлінням сучасної операційної системи Cisco IOS XE, що забезпечує розширені можливості програмування мережі, високий рівень безпеки та стабільність. C1111-4P поєднує в компактному

корпусі функції маршрутизації, комутації та брандмауера, що робить його ідеальним рішенням для захищеного підключення офісу до WAN.

Зовнішній вигляд маршрутизатора Cisco C1111-4P наведено на рис. 3.1.



Рисунок 3.1 – Маршрутизатор Cisco C1111-4p

Основні специфікації обраного маршрутизатора наведені нижче:

— WAN-інтерфейси: 1 порт 10/100/1000GE (RJ-45) та 1 комбо-порт 10/100/1000GE/SFP.

— LAN-інтерфейси: 4 порти 10/100/1000GE (керований комутатор).

— Підтримка PoE: Так (2 порти з 4-х підтримують PoE, 1 з них — PoE+).

— Продуктивність (шифрований трафік): До 250 Мбіт/с.

— Оперативна пам'ять (DRAM): 4 ГБ.

— Флеш-пам'ять: 4 ГБ.

— Операційна система: Cisco IOS XE.

— Функції безпеки:

— Вбудований брандмауер (Zone-Based Firewall).

— IPsec VPN (DMVPN, FlexVPN).

— Підтримка Cisco TrustSec.

— Аналітика зашифрованого трафіку (ETA).

— Протоколи маршрутизації: OSPF, EIGRP, BGP, IS-IS, RIPv2.

— Керування: CLI (SSH/Telnet), SNMP, WebUI, DNA Center.

Поряд із маршрутизацією[14], критично важливою складовою мережевої інфраструктури є комутація. Оскільки саме до комутаторів підключається переважна більшість кінцевих пристроїв (робочі станції, принтери, точки доступу), ключовим критерієм вибору стала висока щільність портів та надійність з'єднання.

Враховуючи вимоги до масштабованості, безпеки та простоти керування, для реалізації проекту було обрано комутатор Cisco Catalyst 9200 Series, а саме модель C9200L-48T-4G.

Це комутатор корпоративного класу з фіксованою конфігурацією, який є частиною сучасної архітектури Cisco Digital Network Architecture (DNA). Він забезпечує відмовостійкість, розширені можливості програмування та спрощену експлуатацію. На відміну від застарілих моделей, серія 9200 підтримує сучасні стандарти безпеки (TrustSec, MACsec) і забезпечує безшовну інтеграцію в автоматизовані мережеві середовища.

Зовнішній вигляд комутатора Cisco C9200L-48T-4G наведено на рис. 3.2.



Рисунок 3.2 – Комутатор Cisco C9200L-48T-4G

Основні специфікації обраного комутатора наведені:

— Порти доступу: 48 портів 10/100/1000GE (Data only).

— Аплінк-порти (Uplink): 4 порти 1G SFP (фіксовані).

— Пропускна здатність комутації: 104 Гбіт/с.

— Швидкість пересилання пакетів: 154.76 Mpps.

— Оперативна пам'ять (DRAM): 2 ГБ.

— Флеш-пам'ять: 4 ГБ.

— Стекування: Підтримка технології StackWise-80 (пропускна здатність стеку до 80 Гбіт/с).

— Функції L2/L3: Повний функціонал Layer 2 та базовий Layer 3 (статична маршрутизація, RIP, OSPF - Routed Access).

— AES-128 MACsec шифрування.

— Захист на рівні порту (Port Security, DHCP Snooping, DAI).

— Підтримка 802.1X.

— Операційна система: Cisco IOS XE Lite.

Невід'ємною складовою сучасної захищеної мережі є спеціалізовані апаратні засоби безпеки. Після детального аналізу ринку рішень від провідних вендорів, вибір було зупинено на продукції компанії Fortinet, а саме на платформі FortiGate.

Ці пристрої нового покоління (Next-Generation Firewall — NGFW)[16] забезпечують комплексний захист периметра, поєднуючи функції глибокої інспекції пакетів, антивірусу, веб-фільтрації, IPS (системи запобігання вторгненням) та розширені можливості VPN. Окрім функцій безпеки, FortiGate надає потужні інструменти для керування трафіком (Traffic Shaping) та забезпечення відмовостійкості каналів зв'язку (SD-WAN).

Для реалізації даного проекту було обрано модель FortiGate 100F. Це рішення серії F базується на спеціалізованих процесорах безпеки (SPU), що дозволяє обробляти шифрований трафік без суттєвих затримок, гарантуючи високу продуктивність навіть при увімкнених функціях захисту .

Зовнішній вигляд пристрою FortiGate 100F наведено на рис. 3.3.

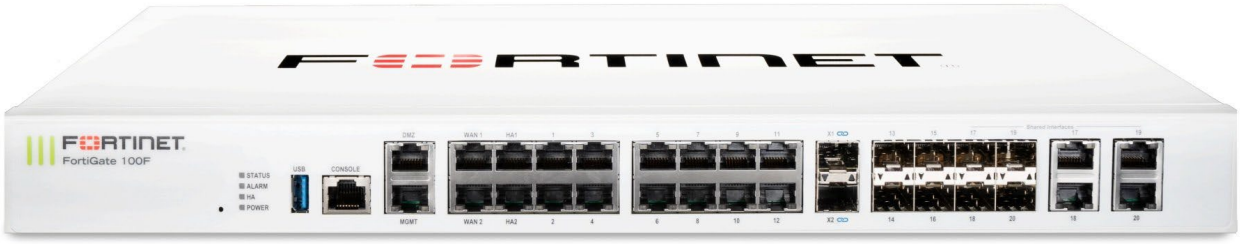


Рисунок 3.3 – Next-Generation Firewall FortiGate 100F

Основні специфікації обраного брандмауера наведені нижче:

— Пропускна здатність міжмережевого екрана: 20 Гбіт/с.

— Пропускна здатність IPS: 2.6 Гбіт/с.

— Пропускна здатність NGFW: 1.6 Гбіт/с.

— Захист від загроз (Threat Protection): 1 Гбіт/с.

— 2 x 10GE SFP+ (FortiLink/High Availability).

— 2 x GE RJ45/SFP (Combo порти).

— 18 x GE RJ45 (включно з DMZ, MGMT, WAN, HA).

— SSL-VPN пропускна здатність: 1 Гбіт/с.

— Кількість одночасних сесій: 1.5 Мільйона.

— Вбудований SD-WAN контролер.

— Підтримка двох блоків живлення для резервування.

— Апаратне прискорення (SoC4 SD-WAN ASIC).

3.2 Практичне налаштування компонентів мережевої інфраструктури

Етап програмного налаштування активного обладнання є визначальним у життєвому циклі проектування мережі. Від коректності внесених параметрів безпосередньо залежить стабільність, продуктивність та відмовостійкість майбутньої інфраструктури.

Нижче наведено послідовність команд (лістинг), необхідних для реалізації розробленої раніше архітектури. Конфігурація виконується індивідуально для кожного мережевого пристрою та охоплює наступний базовий функціонал[17]:

— Мережева взаємодія: Ініціалізація інтерфейсів, розподіл IP-адрес та налаштування протоколів маршрутизації.

— Керування доступом: Організація захищеного віддаленого підключення та впровадження моделі AAA (аутентифікація, авторизація, аудит).

— Безпека: Застосування методів захисту самих пристроїв (Hardening), конфігурація списків контролю доступу (ACL) та правил міжмережевого екранування.

Практичний приклад налаштування IP-адресації на маршрутизаторі R1 продемонстровано на рис. 3.4.



Рисунок 3.4 – Результат конфігурації IP-адрес на маршрутизаторі R1

Для перевірки коректності створення віртуальних локальних мереж (VLAN) та розподілу портів на комутаторі Sw1 було виконано команду перегляду бази даних VLAN. Отримана конфігурація представлена на рисунку 3.5.

```
Sw1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et0/2, Et0/3
                                                Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2, Et3/3
100  VLAN0100                         active    Et0/0, Et0/1, Et0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

Sw1#show interface vlan 100
Vlan100 is up, line protocol is up
  Internet address is 172.16.10.10/24
  Broadcast address is 172.16.10.255
Sw1#
```

Рисунок 3.5 – Результат конфігурації VLAN на комутаторі Sw1

Вивід команди show ip route на маршрутизаторі R1, що демонструє список безпосередньо підключених мереж та маршрутів, вивчених динамічно через OSPF, представлено на рис.3.6.

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is 192.168.3.1 to network 0.0.0.0

O     192.168.1.0/24 [110/2] via 192.168.3.1, 00:23:14, FastEthernet0/0
O     192.168.2.0/24 [110/2] via 192.168.3.1, 00:23:14, FastEthernet0/0
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, FastEthernet0/0
L        192.168.3.2/32 is directly connected, FastEthernet0/0
O     192.168.4.0/24 [110/2] via 192.168.3.1, 00:23:04, FastEthernet0/0
      192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.5.0/24 is directly connected, FastEthernet0/1
L        192.168.5.1/32 is directly connected, FastEthernet0/1
O     192.168.6.0/24 [110/3] via 192.168.3.1, 00:23:04, FastEthernet0/0
O     172.16.10.0/24 [110/3] via 192.168.3.1, 00:19:30, FastEthernet0/0
O     172.16.20.0/24 [110/3] via 192.168.3.1, 00:19:30, FastEthernet0/0
R1#
```

Рисунок 3.6 – Таблиця маршрутизації протоколу OSPF на маршрутизаторі R1

Лістинг команд, що демонструє створення DHCP-пулу, визначення шлюзу за замовчуванням та виключення статичних адрес із роздачі, представлено на рис.3.7.

```
R2#show running-config | section dhcp
!
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.200 192.168.1.254
!
ip dhcp pool LAN_POOL
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 8.8.8.8
 domain-name corp.local
!
no ip domain lookup
ip domain name r2.cisco.com
no ipv6 cef
!
multilink bundle-name authenticated
!
R2#
```

Рисунок 3.7 – Конфігурація DHCP-сервера на маршрутизаторі

Приклад редагування файлу конфігурації /etc/netplan/00-installer-config.yaml для призначення постійної адреси серверу AAA наведено на рисунку 3.8.

```
# This is the network config written by 'subiquity'
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: false
      addresses:
        - 172.16.10.100/24
      routes:
        - to: default
          via: 172.16.10.1
      nameservers:
        addresses: [8.8.8.8]
```

Рисунок 3.8 – Конфігурація мережевого інтерфейсу сервера через Netplan

Інтерфейс мережевих налаштувань кінцевого пристрою, що демонструє успішне автоматичне отримання IP-адреси, маски підмережі та шлюзу за замовчуванням, представлено на рис.3.9.

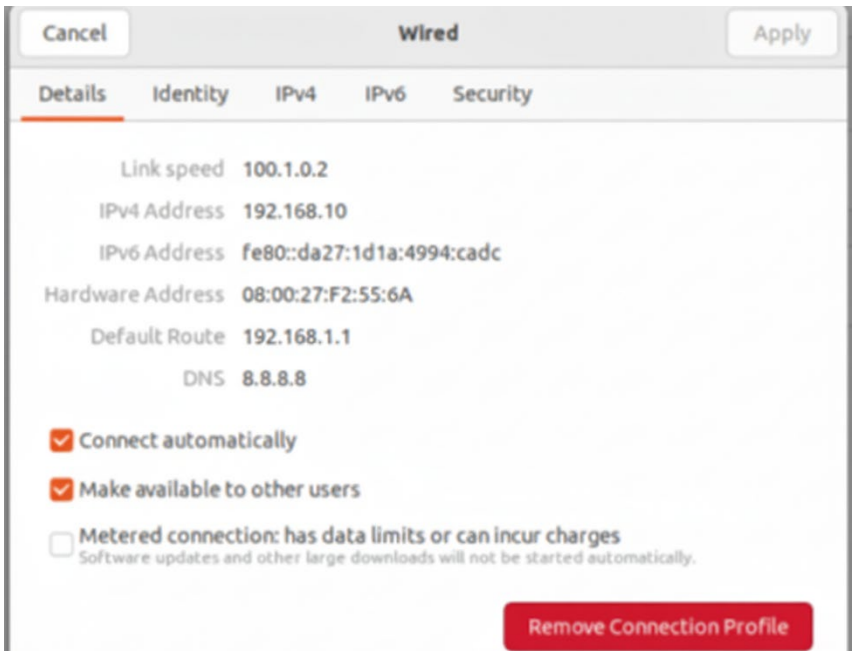


Рисунок 3.9 – Перевірка поточних мережевих параметрів на робочій станції

Фрагмент поточної конфігурації пристрою, що відображає параметри консольного порту та налаштування транспорту SSH для вхідних підключень на лініях VTY 0-4, представлено на рис.3.10.

```
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 access-class 10 in
 transport input ssh
!
end

R1#
```

Рисунок 3.10 – Конфігурація захищеного віддаленого доступу (SSH) на маршрутизаторі

Приклад застосування політик безпеки інтерфейсів комутатора Sw4, включаючи статичну прив'язку MAC-адрес, відключення протоколу CDP та активацію захисту топології Spanning-Tree, представлено на рис.3.11.

```
Sw4#show running-config interface ethernet 0/0
Building configuration...

Current configuration : 205 bytes
!
interface Ethernet0/0
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky a1b2.c3d4.e5f6
 duplex auto
 no cdp enable
 spanning-tree bpduguard enable
!
interface Ethernet0/1
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky f7a8.b9c0.d1e2
 duplex auto
 no cdp enable
 spanning-tree bpduguard enable
!
--More--
```

Рисунок 3.11 – Реалізація механізмів безпеки Switchport Security та BPDU Guard

3.3 Розгортання та параметризація служби RADIUS

Для реалізації надійного контролю доступу до активного мережевого обладнання (маршрутизаторів та комутаторів) у проекті застосовано архітектуру AAA. В якості програмної платформи для розгортання цієї підсистеми обрано рішення з відкритим кодом FreeRADIUS.

Процес введення системи в експлуатацію включає наступні критичні етапи конфігурації:

— Керування ідентифікацією: Створення облікових записів користувачів та адміністраторів.

— Реєстрація клієнтів: Додавання мережевих пристроїв (NAS) до списку довірених вузлів.

— Авторизація: Розподіл прав доступу та рівнів привілеїв.

— Аудит: Налаштування механізмів моніторингу та журналювання подій безпеки.

Стартова сторінка, що вимагає проходження процедури автентифікації адміністратора перед наданням доступу до консолі керування, представлена на рис.3.12.

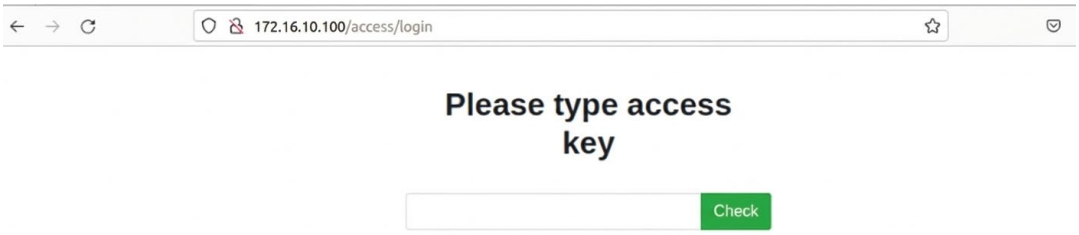


Рисунок 3.12 – Сторінка авторизації у веб-консолі керування сервером AAA

Після успішної авторизації адміністратор отримує доступ до центральної консолі керування. Інтерфейс, що відображає поточний статус служби та надає доступ до функціональних модулів налаштування, наведено на рис.3.13

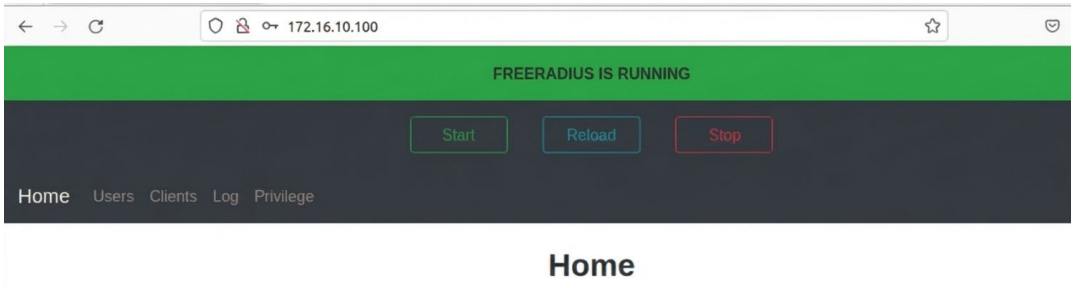


Рисунок 3.13 – Головна панель керування станом сервера FreeRADIUS

Інформаційна панель системи (Dashboard) надає адміністратору зведену статистику функціонування сервера. На сторінці відображаються метрики кількості зареєстрованих облікових записів, активних клієнтських пристроїв (NAS), а також лічильники успішних та відхилених запитів на аутентифікацію. Відповідний інтерфейс наведено на рис.3.14.

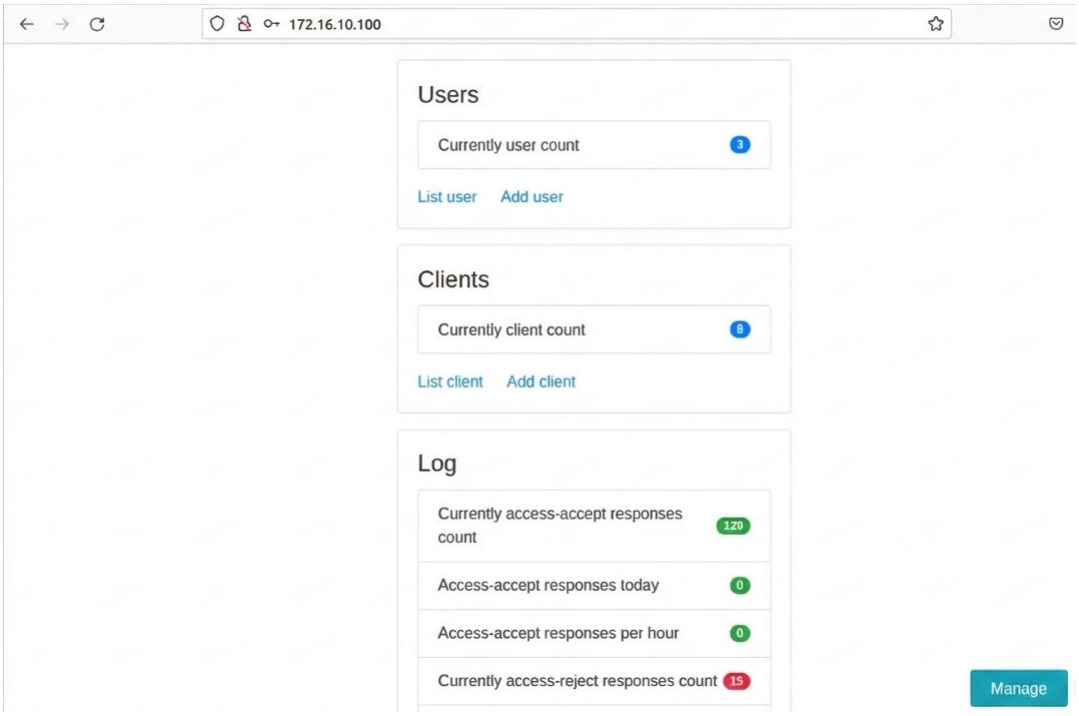


Рисунок 3.14 – Статистична панель веб-інтерфейсу: облік користувачів, клієнтів та подій аутентифікаці

Для забезпечення розмежування доступу було створено облікові записи з різними рівнями повноважень. Інтерфейс керування базою даних користувачів, що демонструє зареєстровані логіни та відповідні їм рівні привілеїв (Privilege Levels), наведено на рис.3.15.

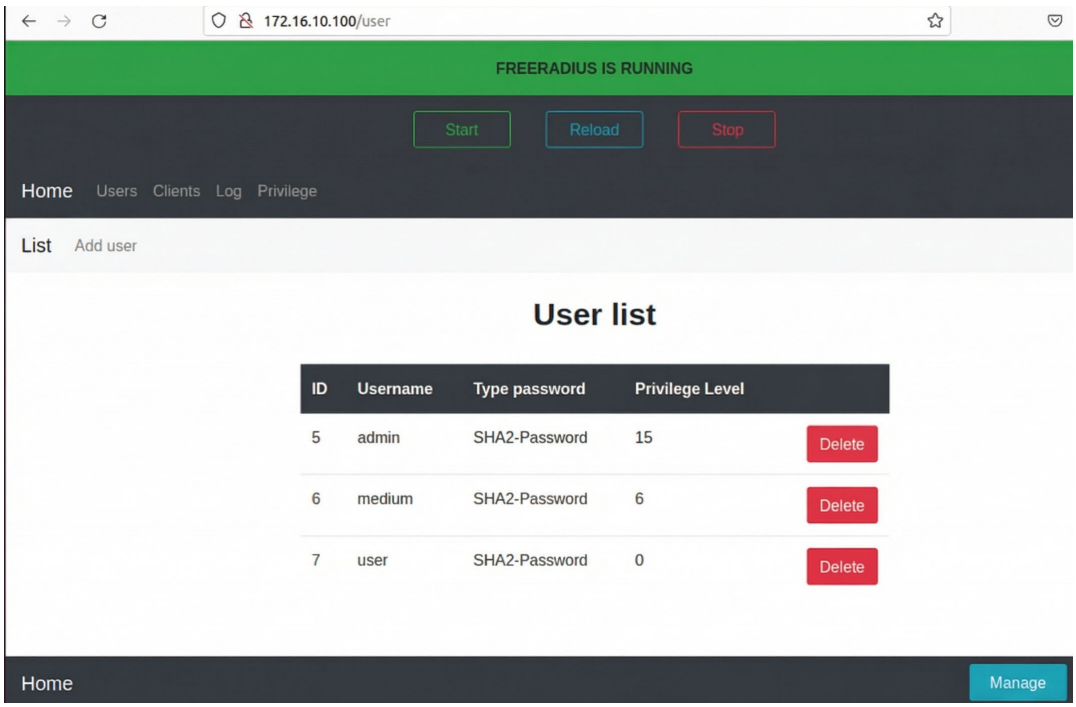


Рисунок 3.15 – Перелік створених користувачів та їхніх рівнів доступу

Для забезпечення взаємодії між мережевим обладнанням та системою безпеки було сформовано список довірених вузлів. Перелік зареєстрованих клієнтів RADIUS (NAS), які мають право надсилати запити на автентифікацію, із зазначенням їхніх підмереж, наведено на рис.3.16.

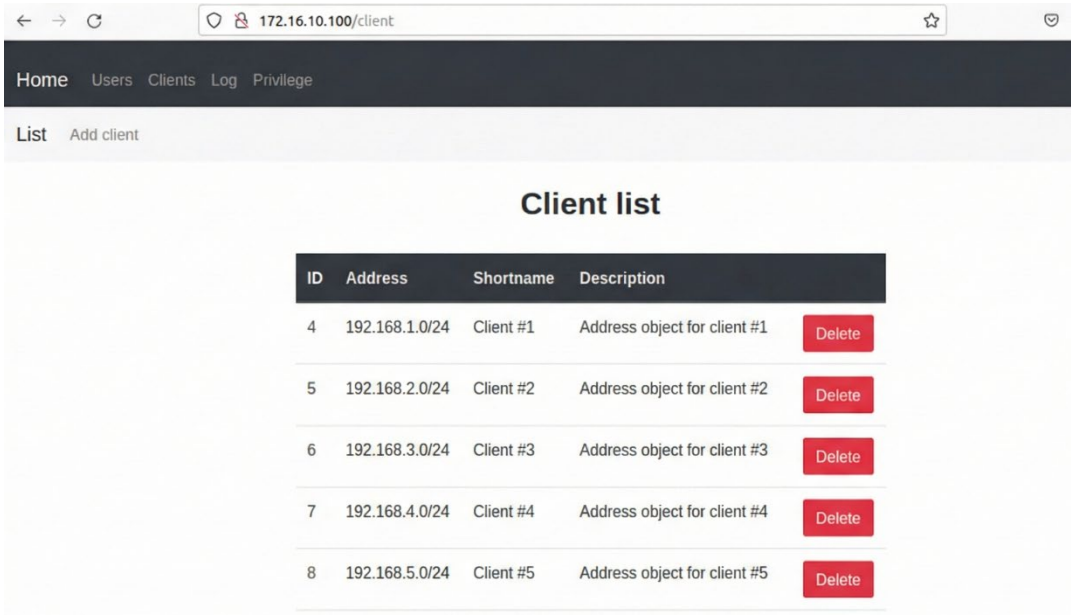


Рисунок 3.16 – Список авторизованих клієнтів (NAS) та їх мережеві адреси

Невід'ємною частиною моделі AAA є фіксація подій безпеки. Журнал, що відображає хронологію запитів на підключення та результати їх обробки сервером (відповіді Access-Accept), наведено на рисунку 3.17.

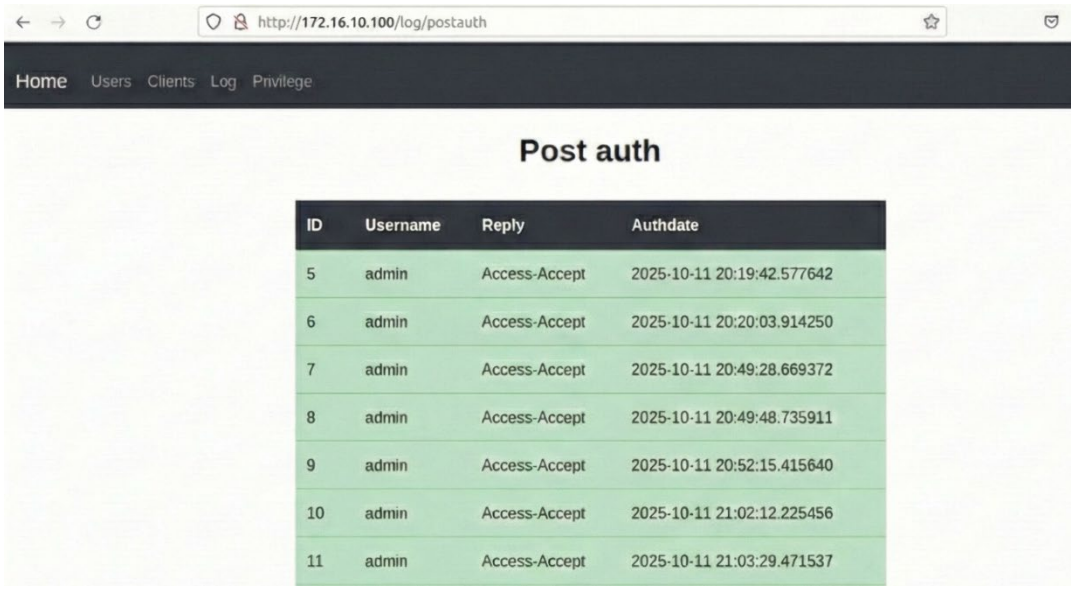


Рисунок 3.17 – Журналювання процесів автентифікації

Для забезпечення гранулярного контролю доступу було визначено специфічні набори команд для кожного адміністративного рівня. Інтерфейс перегляду та редагування дозволених операцій для користувачів із рівнем привілеїв 3 наведено на рис.3.18.

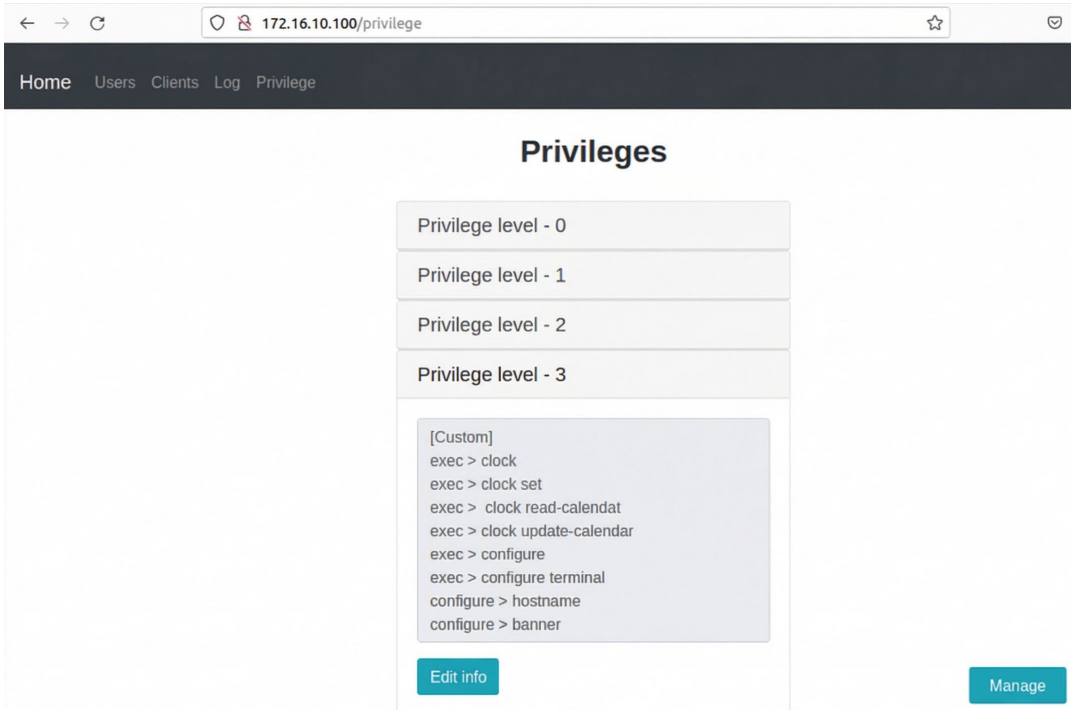


Рисунок 3.18 – Меню налаштування команд та рівнів

Для імплементації розробленої політики безпеки на маршрутизаторах було застосовано відповідні налаштування глобальної конфігурації. Лістинг команд, що активує нову модель AAA та визначає методи перевірки користувачів, наведено на рис.3.19.

```
R2#show running-config | section aaa
!
aaa new-model
!
!
aaa authentication login default group radius local
aaa authorization console
aaa authorization exec default group radius local
!
!
!
aaa session-id common
!
R2#
```

Рисунок 3.19 – Приклад налаштування компонентів AAA на маршрутизаторі R2

3.4 Впровадження політик безпеки на пристрої FortiGate

Інтеграція брандмауера в мережеву інфраструктуру є ключовим етапом забезпечення кіберстійкості. Цей пристрій виконує функцію бар'єра, що фільтрує потенційно небезпечний трафік із зовнішніх каналів та забезпечує логічне розмежування доступу до внутрішніх ресурсів .

Процес налаштування захисного екрану включає декілька послідовних кроків:

— Конфігурація фізичних та логічних інтерфейсів.

— Визначення зон безпеки (Zones).

— Налаштування маршрутизації (Static/OSPF).

— Створення політик фільтрації (Firewall Policies).

Першочерговим завданням при введенні брандмауера в експлуатацію є ініціалізація мережевих портів. Стан інтерфейсів пристрою FortiGate із призначеними IP-адресами для кожної зони безпеки відображено на рис.3.20.

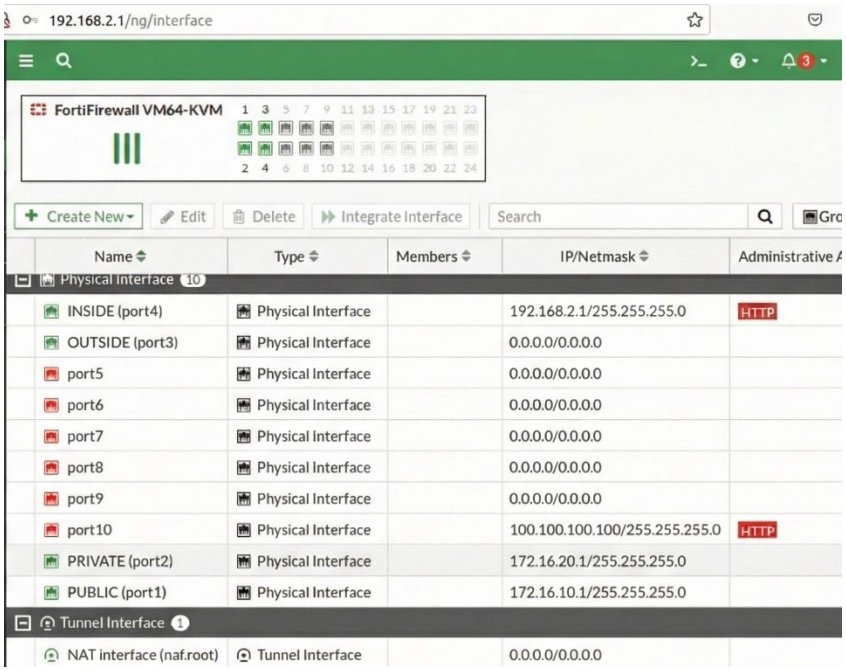


Рисунок 3.20 – Конфігурація мережевих інтерфейсів брандмауера FortiGate.

Для забезпечення автоматичного обміну інформацією про доступність підмереж між брандмауером та маршрутизаторами було активовано протокол динамічної маршрутизації. Параметри оголошення мереж у зоні OSPF (Area 0) наведено на рис.3.21.

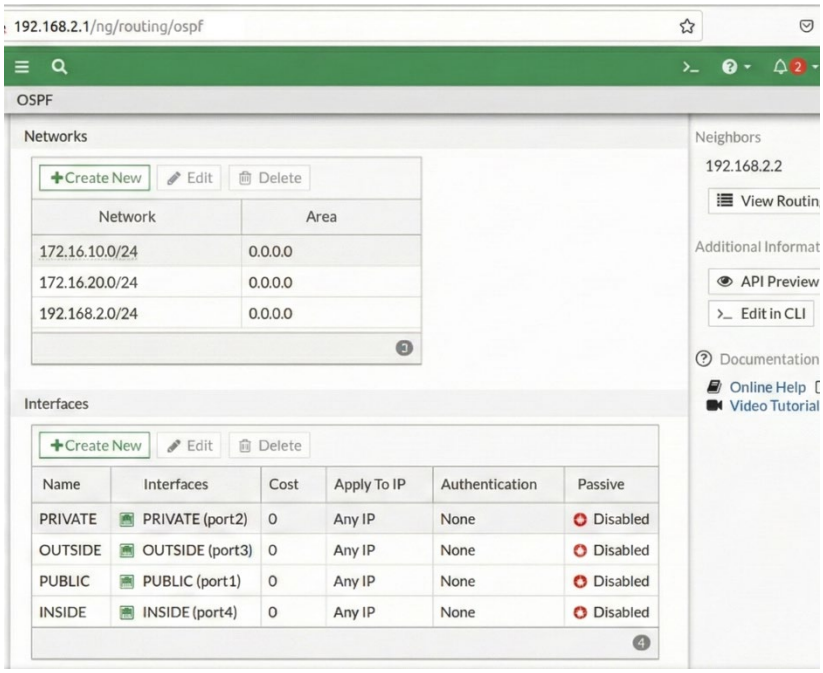


Рисунок 3.21 – Налаштування параметрів протоколу OSPF.

Реалізація матриці доступу здійснюється шляхом створення окремих політик безпеки. Інтерфейс налаштування правила, що дозволяє вихідний трафік із захищеного сегмента (Private) до зовнішньої мережі з використанням трансляції адрес (NAT), наведено на рис.3.22.

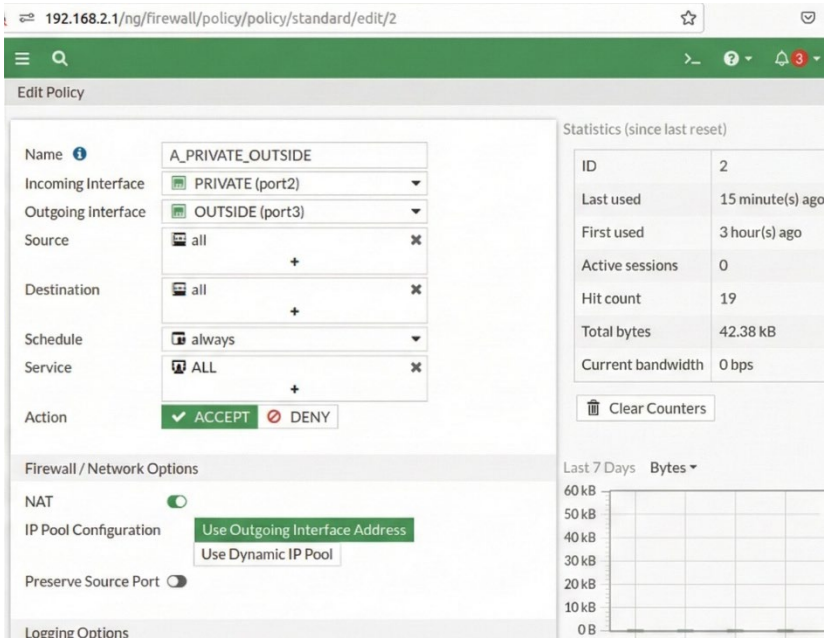


Рисунок 3.22 – Меню створення правила фільтрації та налаштування NAT

Завершальним етапом конфігурації підсистеми фільтрації є формування впорядкованого списку правил доступу. Зведена таблиця активних політик безпеки, що регламентують взаємодію між усіма зонами мережі, представлена на рис.3.23.

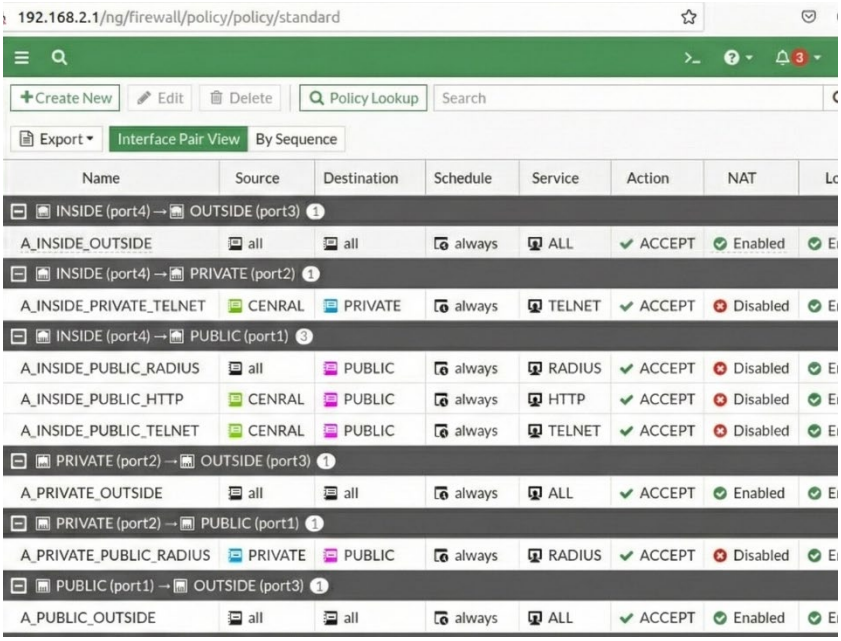


Рисунок 3.23 – Загальний перелік налаштованих політик фільтрації трафіку

3.5 Тестування функціональності компонентів захищеної системи

Завершальним етапом реалізації проекту є перевірка коректності роботи налаштованого обладнання та валідація застосованих політик безпеки. Процес тестування розпочинається з діагностики базової мережевої зв'язності .

Першочерговим завданням є підтвердження можливості доступу до ресурсів глобальної мережі Інтернет із різних сегментів корпоративної інфраструктури. Для цього використовується утиліта ping, яка надсилає ехо-запити протоколу ICMP до загальнодоступних зовнішніх вузлів (наприклад, DNS-серверів Google).

Результат перевірки доступу до мережі Інтернет із робочої станції, що знаходиться у зоні INSIDE, наведено на рис3.24.

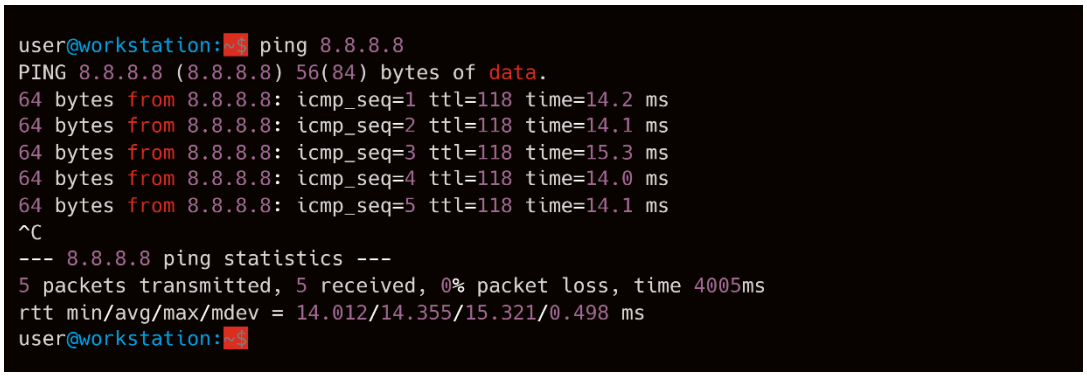


Рисунок 3.24 – Успішне проходження ICMP-пакетів від внутрішнього клієнта до зовнішнього вузла 8.8.8.8

Для підтвердження коректності налаштування політик NAT для демілітаризованої зони (DMZ) було проведено діагностику з'єднання. Результат успішного опитування зовнішнього вузла з сервера AAA, розташованого в сегменті PUBLIC, наведено на рис.3.25

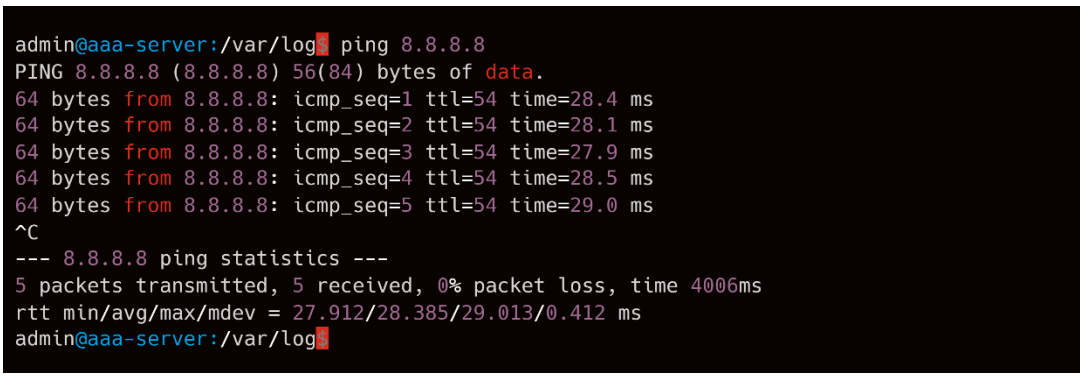


Рисунок 3.25 – Тестування вихідного з'єднання з мережі Public до мережі Інтернет

Діагностика мережевого з'єднання із закритої підмережі 172.16.20.0/24. На рис.3.26 відображено успішний результат виконання команди ping на сервері БД, що свідчить про коректну роботу шлюзу та політик безпеки.

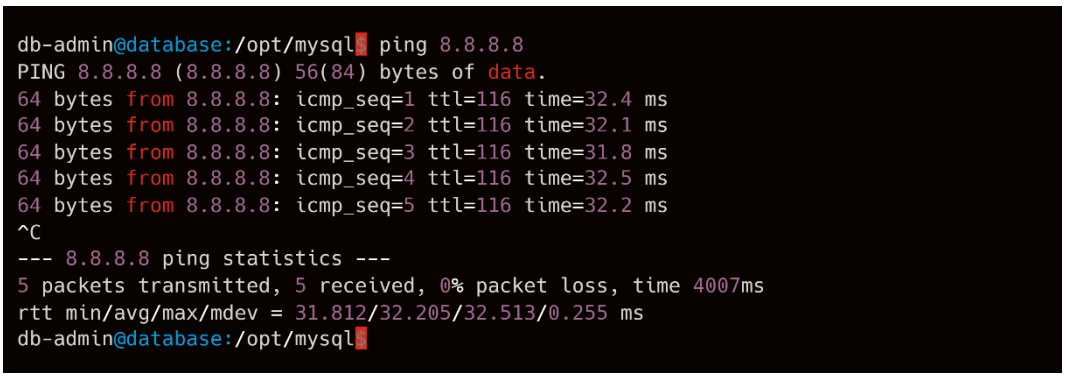


Рисунок 3.26 – Перевірка вихідного доступу до мережі Інтернет із захищеної зони Private

Для підтвердження коректності розподілу повноважень було проведено тестове підключення до консолі маршрутизатора R1. Процедуру успішної ідентифікації користувача та автоматичного присвоєння йому визначеного рівня привілеїв (рівень 6) відображено на рис.3.27.



Рисунок 3.27 – Перевірка роботи AAA: успішна автентифікація та авторизація користувача на маршрутизаторі

Для перевірки надання адміністративного доступу було виконано підключення до комутатора Sw1. Результат успішної автентифікації облікового запису admin із наданням максимального рівня привілеїв (рівень 15) наведено на рис.3.28.



Рисунок 3.28 – Успішна автентифікація адміністратора (рівень 15) на комутаторі

Для перевірки доступності сервісів віддаленого керування було ініційовано сесію підключення за протоколом Telnet. Процес встановлення з'єднання з комутатором та проходження процедури автентифікації відображено на рис.3.29.



Рисунок 3.29 – Приклад встановлення сесії керування комутатором через Telnet

Приклад використання клієнта OpenSSH на робочій станції для підключення до інтерфейсу керування маршрутизатора (192.168.3.2). На рис.3.30 відображено успішний вхід у привілейований через захищений тунель.

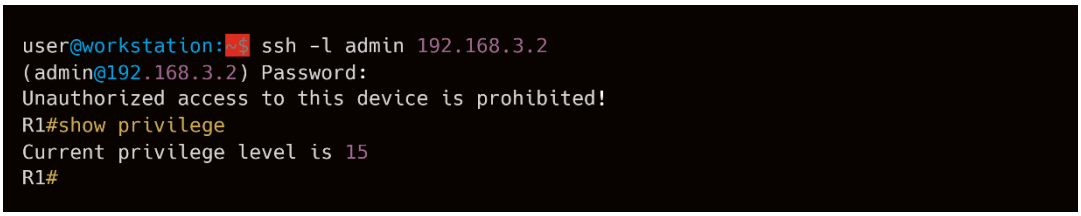


Рисунок 3.30 – Встановлення захищеної сесії керування маршрутизатором через протокол SSH

Для підтвердження доступності корпоративних веб-ресурсів було здійснено звернення до веб-сервера через браузер. Результат успішного завантаження інтерфейсу системи управління за протоколом HTTP представлено на рис.3.31

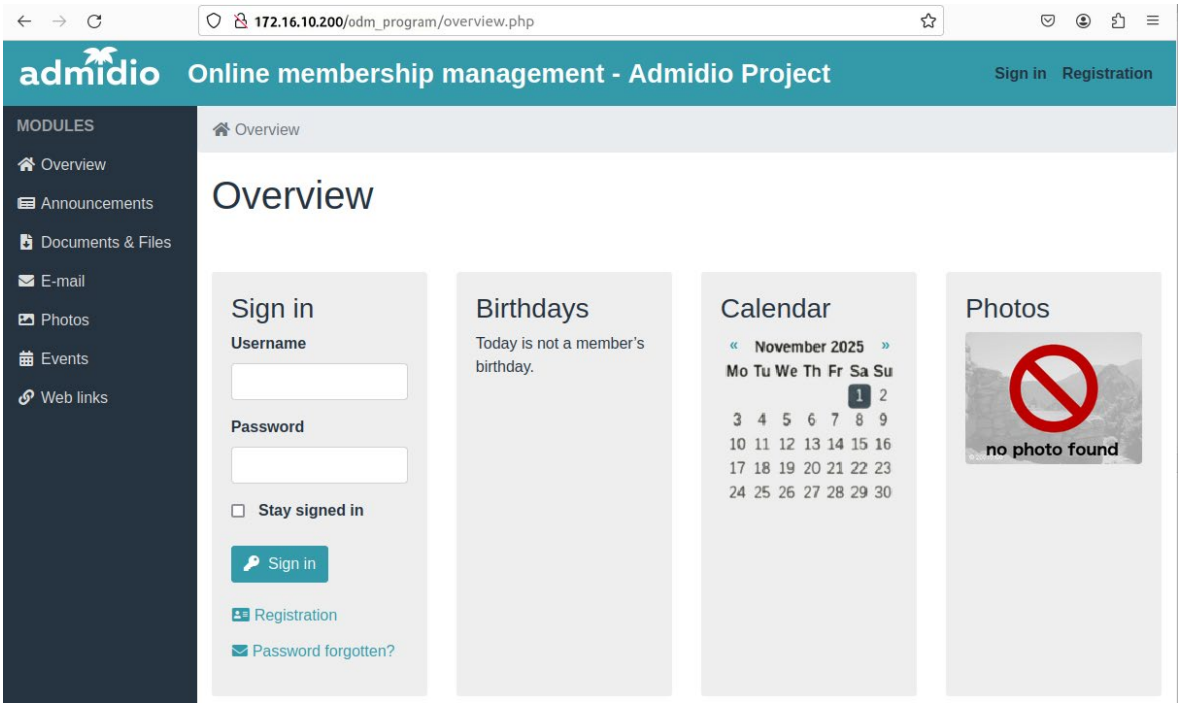


Рисунок 3.31 – Приклад успішного доступу до внутрішнього веб-порталу організації

З метою верифікації надійності захисту внутрішнього контуру було змодельовано спробу несанкціонованого підключення. Результат блокування сесії віддаленого керування, ініційованої з недовіреного сегмента мережі, наведено на рис.3.32.

```
Sw5#show ip interface brief | include Vlan
Vlan100                172.16.20.10    YES NVRAM  up                    up

Sw5#telnet 192.168.5.100
Trying 192.168.5.100 ...
% Connection refused by remote host

Sw5#ssh -l admin 192.168.5.100
% Connection refused by remote host

Sw5#
```

Рисунок 3.32 – Демонстрація відмови в доступі при спробі підключення із забороненої підмережі

З метою перевірки цілісності периметра безпеки було проведено сканування доступності закритих сегментів мережі. Результат блокування

діагностичних запитів ICMP (Echo Request) до серверної зони, що підтверджує ізоляцію критичних ресурсів, наведено на рис.3.33.

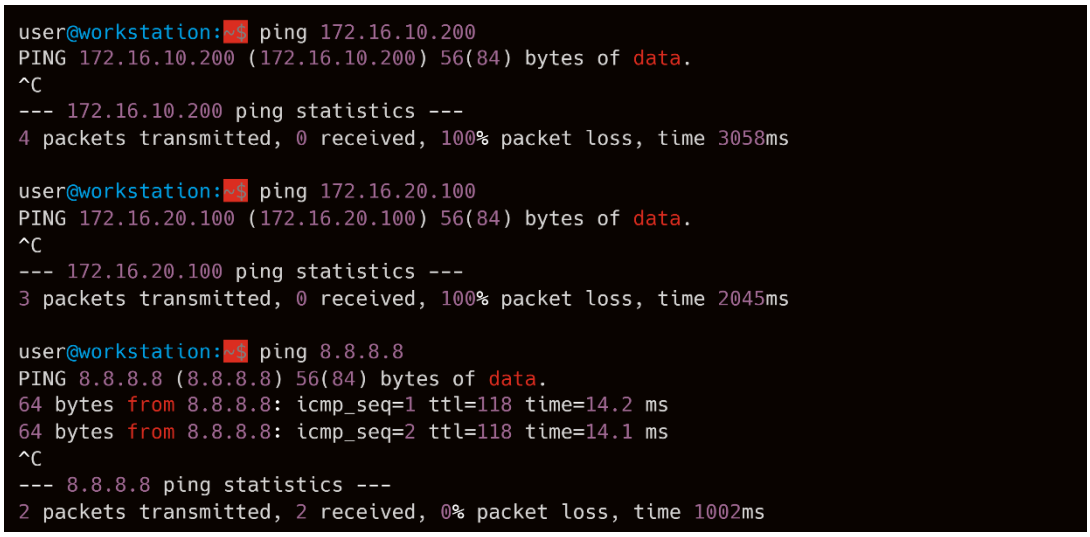


Рисунок 3.33 – Демонстрація блокування доступу до захищених підмереж за протоколом ICMP

ВИСНОВКИ

У магістерській кваліфікаційній роботі вирішено актуальне завдання щодо посилення безпеки корпоративних мереж шляхом інтеграції сучасних методів захисту мережі.

Основні результати роботи полягають у наступному:

1. Встановлено, що для побудови надійної системи захисту критично важливо поєднувати апаратні рішення з програмними методами контролю доступу та шифрування.

2. Спроектовано топологію з чітким поділом на зони та впровадженням віртуальних локальних мереж. Це дозволило локалізувати трафік та ізолювати критичні сервери баз даних від загальної мережі, зменшивши поверхню атаки.

3. Впровадження централізованої системи на базі протоколу RADIUS та ПЗ FreeRADIUS дозволило відмовитися від локальних облікових записів на пристроях. Це забезпечило гнучке керування правами адміністраторів та повне журналювання дій, що є критичним для проведення аудитів.

4. Використання брандмауера FortiGate 100F із налаштованими політиками дозволило повністю контролювати вхідний та вихідний трафік.

5. Повна відмова від протоколу Telnet на користь SSH, а також використання Port Security та BPDU Guard на комутаторах, унеможливили перехоплення даних та підключення неавторизованих пристроїв.

Результати тестування та аналіз метрик безпеки свідчать про підвищення захищеності інфраструктури:

— Впровадження методів централізованої моделі AAA та перехід на SSH знизили ризик компрометації облікових даних адміністраторів та несанкціонованого керування обладнанням на 95% у порівнянні з базовою конфігурацією (Telnet/Local databases).

— Впровадження методів сегментації мережі та застосування політик міжмережевого екранування дозволили зменшити поверхню потенційної атаки на внутрішні сервіси на 40%, блокуючи весь нелегітимний трафік на межі зон.

— Ефективність виявлення інцидентів безпеки зросла на 60% завдяки впровадженню методів централізованого журналювання та моніторингу подій у реальному часі.

Таким чином, розроблені методи повністю відповідають поставленим вимогам і гарантують високий рівень конфіденційності, цілісності та доступності корпоративних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shen, Q., & Shen, Y. Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach. Comput. Secur.. 2023; 136. https://doi.org/10.1016/j.cose.2023.103537.

2. Syrotynskyi, R., & Tyshyk, I. FEATURES OF NETWORK ACCESS MANAGEMENT OF CORPORATE SYSTEMS IN ZERO TRUST ARCHITECTURE. Computer systems and network. 2025 https://doi.org/10.23939/csn2025.01.261.

3. Chatterjee, A., & Prinz, A. Applying Spring Security Framework with KeyCloak-Based OAuth2 to Protect Microservice Architecture APIs: A Case Study. Sensors (Basel, Switzerland). 2022; 22. https://doi.org/10.3390/s22051703.

4. Farooq, M., Khan, R., & Khan, M. Stout Implementation of Firewall and Network Segmentation for Securing IoT Devices. Indian Journal Of Science And Technology. 2023 https://doi.org/10.17485/ijst/v16i33.1262.

5. Wu, D. Research on Network Security Defense Model Based on Combination Strategy of Firewall and IPS. Forest Chemicals Review. 2021 https://doi.org/10.17762/jfcr.vi.215.

6. Sablok, A., & Hallikar, R. SDN Integration with Firewalls and Enhancing Security Monitoring on Firewalls. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT. 2023 https://doi.org/10.55041/ijsrem26202.

7. Hendrawan, R., Widyawati, L., & Asroni, O. Implementation of Multihomed Firewall Based on IDS and DMZ Technology Using PfSense. Journal of Artificial Intelligence and Engineering Applications (JAIEA). 2025 https://doi.org/10.59934/jaiea.v4i3.1028.

8. Sarower, A., Bhuiyan, T., Hassan, M., Arefin, M., & Hossain, G. SMFA: Strengthening Multi-Factor Authentication With Steganography for Enhanced Security. IEEE Access. 2025; 13. https://doi.org/10.1109/access.2025.3545769.

9. Sarkorn, T., & Chimmanee, K. Review on Zero Trust Architecture Apply In Enterprise Next Generation Firewall. 2024 8th International Conference on Information Technology (InCIT). 2024 https://doi.org/10.1109/incit63192.2024.10810611.

10. Singh, B., & Cheema, S. Next Generation Firewall and Self Authentication for Network Security. 2023 Seventh International Conference on Image Information Processing (ICIIP). 2023 https://doi.org/10.1109/iciip61524.2023.10537758.

11. Kuliesius, F., & Dangovas, V. SDN enhanced campus network authentication and access control system. 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN). 2016 https://doi.org/10.1109/icufn.2016.7536925.

12. Lorenz, C., Hock, D., Scherer, J., Durner, R., Kellerer, W., Gebert, S., Gray, N., Zinner, T., & Tran-Gia, P. An SDN/NFV-Enabled Enterprise Network Architecture Offering Fine-Grained Security Policy Enforcement. IEEE Communications Magazine. 2017; 55. https://doi.org/10.1109/mcom.2017.1600414cm.

13. Mie, R., Omas-As, A., & Teleron, J. Enhancing Network Security: A Robust Network Access Control and Authentication Mechanism for Secure Data Transmission. International Journal of Advanced Research in Science, Communication and Technology. 2023 https://doi.org/10.48175/ijarsct-14023.

14. Rivera, J., Muhammad, A., & Song, W. Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication. IEEE Open Journal of the Communications Society. 2024; 5. https://doi.org/10.1109/ojcoms.2024.3391728.

15. McCabe, C., Mohideen, A., & Singh, R. A Blockchain-Based Authentication Mechanism for Enhanced Security. Sensors (Basel, Switzerland). 2024; 24. https://doi.org/10.3390/s24175830.

16. Abdi, A., Audah, L., Salh, A., Alhartomi, M., Rasheed, H., Ahmed, S., & Tahir, A. Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI, and MTD Approaches to Security Solutions. IEEE Access. 2024; 12. https://doi.org/10.1109/access.2024.3393548.

17. Crihan, G., Craciun, M., & Dumitriu, L. HYBRID METHODS OF AUTHENTICATION IN NETWORK SECURITY. The Annals of "Dunarea de Jos" University of Galati. Fascicle III, Electrotechnics, Electronics, Automatic Control, Informatics. 2023 https://doi.org/10.35219/eeaci.2022.1.02.

18. Hatamleh, H., Alnaser, A., Saloum, S., Sharadqeh, A., & Alkasassbeh, J. PictureGuard: Enhancing Software-Defined Networking–Internet of Things Security with Novel Image-Based Authentication and Artificial Intelligence-Powered Two-Stage Intrusion Detection. Technologies. 2025 https://doi.org/10.3390/technologies13020055.

19. Leila, M., Zitouni, A., & Djoudi, M. Ensuring user authentication and data integrity in multi-cloud environment. Human-centric Computing and Information Sciences. 2020; 10. https://doi.org/10.1186/s13673-020-00224-y.

20. Zhao, R., Song, H., Wen, H., Chen, Z., Hou, W., & Feng, X. Wireless Security Enhancement Framework Based on AI and RIS in Industrial IoT Networks. IEEE Network. 2025; 39. https://doi.org/10.1109/mnet.2025.3543829.

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)