НАЦІОНАЛЬНИЙ УНІВЕРСТИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет/(ННІ) Інформаційних Технологій

ПОГОДЖЕНО
Декан факультету (Директор ННІ)
Інформаційних Технологій
(назва факультету (ННІ))

_____ Ігор БОЛБОТ
(підпис) (ім'я ПРІЗВИЩЕ)

"___" _____ 2025 р.

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ
Завідувач кафедри
Кафедра комп'ютерних систем, мереж та кібербезпеки
(назва кафедри)

_____ Дмитро КАСАТКІН
(підпис) (ім'я ПРІЗВИЩЕ)

"___" _____ 2025 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему: Дослідження двошарових демілітарізованих зон корпоративних мереж із розгалуженою Intranet мережею

Спеціальність 123 Комп'ютерна інженерія
(код і найменування)

Освітня програма Комп'ютерні системи захисту інформації
(назва)

Орієнтація освітньої програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Гарант освітньої програми
д.п.н, професор _____ Сергій МАМЧЕНКО
(науковий ступінь та вчене звання) (підпис) (ім'я ПРІЗВИЩЕ)

Керівник магістерської кваліфікаційної роботи
д.п.н, професор _____ Сергій МАМЧЕНКО
(науковий ступінь та вчене звання) (підпис) (ім'я ПРІЗВИЩЕ)

Виконав _____ Артьом ТОКАРЕНКО
(підпис) ((ім'я ПРІЗВИЩЕ здобувача)

КИЇВ – 2025
НАЦІОНАЛЬНИЙ УНІВЕРСТИТЕТ БІОРЕСУРСІВ

І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
Факультет/(ННІ) Інформаційних Технологій

ЗАТВЕРДЖУЮ

Завідувач кафедри
кафедри комп'ютерних систем, мереж та кібербезпеки
к.пед.н., доцент _____ **Дмитро КАСАТКІН**
(науковий ступінь, вчене звання) (підпис) (ім'я ПРІЗВИЩЕ)
"____" _____2025року

З А В Д А Н Н Я

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧУ

Токаренко Артьом Богданович
(прізвище, ім'я, по батькові)

Спеціальність 123 Комп'ютерна інженерія
(код і найменування)

Освітня програма _ Комп'ютерні системи захисту інформації
(назва)

Орієнтація освітньої програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Тема магістерської кваліфікаційної роботи Дослідження двошарових демілітарізованих зон корпоративних мереж із розгалуженою Intranet мережею
затверджена наказом ректора НУБіП України від «26» жовтня 2024 р. №1941 «С»

Термін подання завершеної роботи на кафедру 15.11.2025
(рік, місяць, число)

Вихідні дані до магістерської кваліфікаційної роботи Підвищення рівня безпеки корпоративної мережі шляхом аналізу, моделювання та оптимізації двошарової DMZ-архітектури для мінімізації вразливостей та загроз при взаємодії зовнішніх і внутрішніх сервісів.

Основні питання дослідження:

Проаналізувати сучасні підходи до побудови демілітаризованих зон у корпоративних мережах.

Дослідити моделі побудови двошарових DMZ у поєднанні з розгалуженою Intranet-структурою.

Ідентифікувати типові мережеві загрози, ризики та вразливості на кожному рівні DMZ.

Оцінити ефективність застосованих механізмів фільтрації, маршрутизації, сегментації та контролю доступу.

Запропонувати удосконалення архітектури DMZ для підвищення стійкості корпоративної мережі

Дата видачі завдання "15" листопада 2024 р.

Керівник магістерської кваліфікаційної роботи

д.п.н, професор _____ Сергій МАМЧЕНКО
(науковий ступінь та вчене звання) (підпис) (ім'я ПРІЗВИЩЕ)

Виконав _____ Артьом ТОКАРЕНКО
(ім'я ПРІЗВИЩЕ)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

1. ACL – Access Control List, список контролю доступу
2. API – Application Programming Interface, інтерфейс прикладного програмування
3. CPU – Central Processing Unit, центральний процесор
4. DMZ – Demilitarized Zone, демілітаризована зона
5. DNAT – Destination Network Address Translation, трансляція адреси призначення
6. DoS – Denial of Service, відмова в обслуговуванні
7. gRPC – Remote Procedure Call Framework, протокол викликів віддалених процедур
8. HTTPS – Hypertext Transfer Protocol Secure, захищений протокол передачі даних
9. INET – Internet Segment, зовнішній мережевий сегмент
10. IPSec – Internet Protocol Security, протокол захисту мережевих з’єднань
11. MQTT – Message Queuing Telemetry Transport, протокол телеметрії
12. NAT – Network Address Translation, трансляція мережевих адрес
13. PAT – Port Address Translation, трансляція адрес із підстановкою порту
14. PLC – Programmable Logic Controller, програмований логічний контролер
15. OT – Operational Technology, технологічний сегмент мережі
16. SNAT – Source Network Address Translation, трансляція адреси джерела
17. SQL – Structured Query Language, мова структурованих запитів
18. SSH – Secure Shell, захищений мережевий протокол
19. Syslog – System Logging Protocol, протокол системного журналювання

20. UI – User Interface, користувацький інтерфейс
21. VPN – Virtual Private Network, віртуальна приватна мережа
22. WAN – Wide Area Network, глобальна мережа

ВСТУП

Зростання кількості сервісів, підключених до глобальної мережі Internet, розширення хмарних технологій і віртуалізованих сервісів створюють нові ризики несанкціонованого доступу, компрометації даних та кібератак. Традиційні моделі периметрового захисту, побудовані на принципі одного рівня фільтрації, уже не забезпечують належного рівня ізоляції внутрішніх ресурсів від зовнішнього трафіку. Тому актуальним напрямом досліджень є застосування багаторівневих архітектур безпеки, зокрема двошарових демілітаризованих зон (DMZ), які формують додаткові рубежі контролю, дозволяють розділяти рівні доступу, оптимізувати маршрутизацію запитів та мінімізувати наслідки потенційних інцидентів.

Метою даної роботи є розроблення та дослідження моделі двошарової демілітаризованої зони корпоративної мережі з розгалуженою Intranet-структурою, здатної забезпечити підвищений рівень інформаційної безпеки, контроль доступу та гнучке управління потоками даних між зовнішніми і внутрішніми сегментами.

Для досягнення цієї мети необхідно виконати послідовні **завдання:**

1. проаналізувати предметну область захисту корпоративних мереж і визначити проблеми сучасних архітектур периметральної безпеки.
2. Дослідити теоретико-методологічні засади побудови DMZ-зон та моделі сегментації трафіку.
3. Провести огляд і порівняння існуючих технічних рішень (Cisco ASA, FortiGate, pfSense тощо) для реалізації багаторівневого захисту.
4. Розробити структурну модель двошарової DMZ для розгалуженої корпоративної мережі.
5. Сформулювати вимоги до функціонування системи з урахуванням продуктивності, надійності, безпеки та масштабованості.

6. Виконати моделювання основних потоків даних і принципів маршрутизації між зонами.

7. Обґрунтувати очікувані переваги двошарової DMZ порівняно з класичною одношаровою конфігурацією.

Об’єктом дослідження є процес забезпечення інформаційної безпеки корпоративних мереж із багаторівневою структурою, а **предметом** – методи, моделі та технічні засоби побудови двошарових демілітаризованих зон, що забезпечують ізоляцію трафіку та контроль взаємодій між зонами доступу.

У роботі використано методи системного аналізу для формалізації архітектури мережевої інфраструктури, методи теорії інформаційної безпеки для оцінювання рівня захищеності та ризиків, а також експериментальні методи для тестування схем NAT, VPN, VLAN та політик фільтрації трафіку. Для візуалізації та перевірки функціонування моделі застосовано UML-моделювання і симулятори мережевих процесів Cisco Packet Tracer та GNS3.

Наукова новизна роботи полягає у створенні узагальненої моделі двошарової демілітаризованої зони корпоративної мережі, що враховує взаємодію між зовнішніми сервісами, внутрішнім Intranet-середовищем і проміжним рівнем фільтрації. Запропонований підхід підвищує стійкість системи до складних кібератак, зменшує ризики поширення шкідливого трафіку вглиб корпоративної інфраструктури, а також забезпечує адаптивність архітектури до змін вимог безпеки.

Практичне значення одержаних результатів полягає у можливості використання розробленої моделі для модернізації мережевих систем підприємств, впровадження політик зонального контролю доступу, інтеграції з SIEM-системами та навчання фахівців у галузі кіберзахисту корпоративних мереж.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Опис предметної області та основних процесів функціонування системи

Предметна область системи охоплює процеси захисту інформаційних ресурсів у корпоративних мережах, що мають складну, багаторівневу структуру з численними внутрішніми сегментами, сервісами та користувацькими групами. Такі мережі забезпечують функціонування бізнес-додатків, сховищ даних, поштових, фінансових і аналітичних сервісів, а також підтримують взаємодію між віддаленими філіями через Intranet-канали. Головною проблемою цієї предметної області є забезпечення безпечного обміну даними між зовнішнім і внутрішнім середовищами, мінімізація ризиків несанкціонованого доступу та зниження впливу зовнішніх загроз.

На рис. 1.1 представлено узагальнену схему корпоративної мережі з двошаровою демілітаризованою зоною, яка реалізує багаторівневий принцип сегментації доступу. Перша DMZ-зона (DMZ-1) виконує функції первинного фільтрування трафіку, контролю запитів до веб-ресурсів і взаємодії з клієнтами з боку Internet. Друга зона (DMZ-2) формує проміжний рівень логіки прикладних шлюзів, систем моніторингу подій і захисту від вторгнень. Внутрішня Intranet-мережа містить сегменти службових систем (HR, Finance, Dev, DB), у яких розташовані корпоративні сервіси, бази даних та засоби автентифікації.

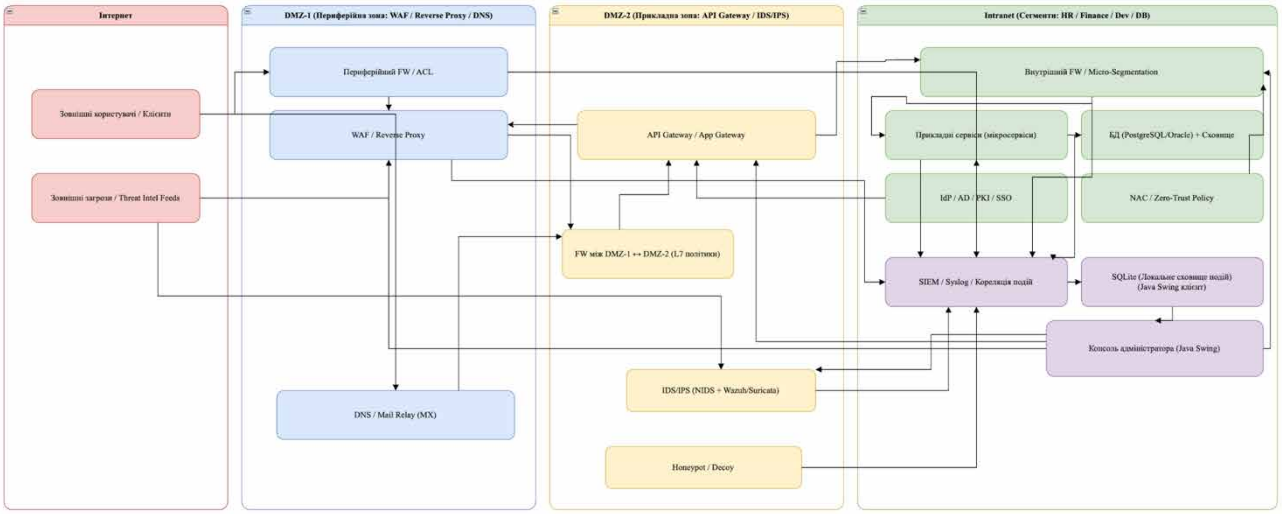


Рисунок 1.1 – Структура двошарової демілітаризованої зони корпоративної мережі з розгалуженою Intranet-мережею

Предметна область включає взаємодію кількох рівнів інформаційної інфраструктури: зовнішніх користувачів, шлюзів безпеки, серверів додатків і внутрішніх систем зберігання даних. Усі процеси функціонування пов’язані з передаванням, маршрутизацією та контролем трафіку між зонами довіри, а також з постійним моніторингом стану мережевих з’єднань. Демілітаризовані зони відіграють роль буферів, що розділяють рівні доступу й унеможливлюють прямий обмін даними між зовнішніми користувачами та внутрішніми інформаційними ресурсами. Важливим аспектом предметної області є логічна сегментація трафіку за допомогою політик доступу, NAT-перетворень і ACL-правил, які визначають допустимі напрямки взаємодії.

Додаткову роль відіграють механізми централізованого журналювання подій, автентифікації користувачів і системи виявлення вторгнень. У межах корпоративної мережі події з обох рівнів DMZ надходять у сховище безпеки, де здійснюється їх кореляція й аналіз для виявлення потенційних аномалій. Такий підхід дозволяє підтримувати баланс між доступністю сервісів і безпечністю обміну даними, що є ключовою характеристикою сучасних корпоративних систем.

Таблиця 1.1

Основні елементи предметної області корпоративної мережі з двошаровою DMZ

Елемент предметної області	Функціональна роль	Взаємодія у системі
Зовнішні користувачі	Ініціація запитів до публічних ресурсів	Звернення до DMZ-1 через веб-інтерфейси та проксі-сервери
DMZ-1 (периферійна зона)	Первинна перевірка трафіку, маршрутизація запитів	Передає легітимні запити у DMZ-2, блокує потенційно шкідливі
DMZ-2 (прикладна зона)	Логіка обробки запитів, аналітика подій, IDS/IPS	Здійснює обмін даними з Intranet через обмежені політики L7
Intranet	Сегменти внутрішніх служб і сховищ даних	Обробляє запити, автентифікує користувачів, формує відповіді
Центр моніторингу подій	Кореляція логів, аналітика безпеки	Отримує дані з усіх зон, забезпечує контроль цілісності мережі

Предметна область дослідження охоплює комплекс організаційних і технічних процесів, пов’язаних із побудовою захищеної корпоративної мережі, в якій двошарова DMZ виступає основним елементом зонального контролю та забезпечення довіри. Така архітектура є базовою для створення сучасних систем кіберзахисту, орієнтованих на принципи багаторівневої безпеки, сегментації доступу й постійного моніторингу подій.

1.2 Теоретико-методологічні засади та стан наукових досліджень

Теоретичні основи побудови багаторівневих корпоративних мереж базуються на поєднанні принципів зональної ізоляції, розподіленого управління трафіком і концепції “defence-in-depth”. Сучасні дослідження свідчать, що одношарові моделі DMZ не здатні забезпечити повну ізоляцію між зовнішнім і внутрішнім середовищами, тому наукова увага зміщується до багаторівневих

(dual-layer) структур, які поєднують транспортний контроль, розподіл ресурсів і політики довіри.

На рис. 1.2 наведено концептуальну модель Dual Network Architecture, у якій взаємодія між підсистемами визначається п’ятьма ключовими компонентами: структурою, функцією, ресурсною мережею, стратегією та контролем передавання даних. Така структура описана у роботі Qi S. et al. (2024) [1] і відображає системний підхід до організації безпечної комунікації, коли транспортна та функціональна частини мережі узгоджуються через формалізовані правила взаємодії між зонами.

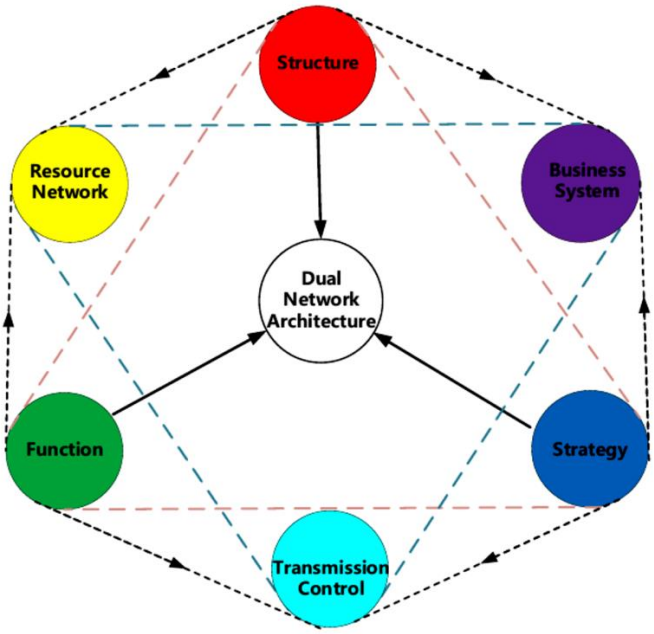


Рисунок 1.2 – Концептуальна модель Dual Network Architecture (Qi S. et al., 2024)

Подальший розвиток цієї концепції представлено на рис. 1.3, де наведено ієрархічну модель рівнів управління, що складається з Network Resource Layer *і* Transmission Control Layer. Перший рівень забезпечує планування ресурсів, гетерогенну маршрутизацію та ідентифікацію вузлів, тоді як другий - контроль передавання, багатодоменний вибір маршрутів і алгоритми безпеки. Між ними реалізується двосторонній інтерфейс взаємодії, який гарантує розподілене узгодження політик безпеки й довіри [1].

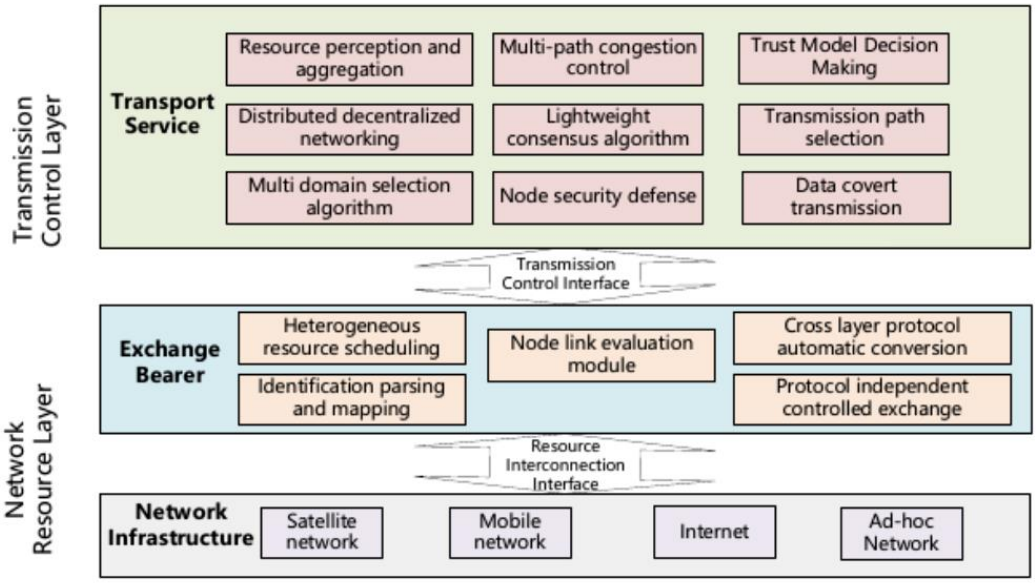


Рисунок 1.3 – Ієрархічна модель рівнів Network Resource та Transmission Control (Qi S. et al., 2024)

Згідно з дослідженням Shrimali S. (2017) [2], модель DMZ (Demilitarized Zone) є практичним втіленням принципу ізоляції, коли зовнішні користувачі можуть взаємодіяти лише з проміжним сервером, не маючи прямого доступу до внутрішніх ресурсів. На рис. 1.4 подано базову архітектуру безпечної мережі з DMZ, у якій використано публічний сервер і два незалежні маршрутизатори, що розділяють внутрішній і зовнішній трафік. Ця модель лягла в основу сучасних систем периметрового захисту, проте має обмеження за гнучкістю політик контролю [2].

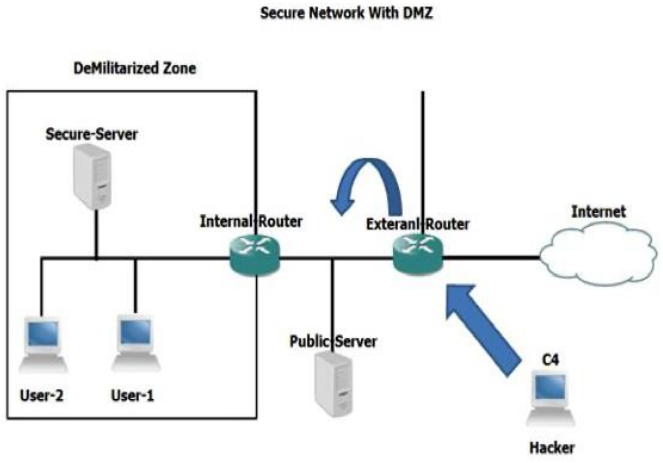


Рисунок 1.4 – Класична модель корпоративної мережі з DMZ (Shrimali S., 2017)

Подальше вдосконалення запропонував R. Kumar et al. (2018) [3], який представив детальнішу топологію на основі протоколу EIGRP, де зона DMZ функціонує як окремий підмережевий сегмент, що містить конфіденційні сервери та публічні ресурси. На рис. 1.5 наведено узагальнену схему такого підходу, у якій застосовано маршрутизацію між зонами 192.168.0.0/24 та 192.168.5.0/24. Подібна модель дозволяє реалізувати двонапрямну фільтрацію, коли внутрішній маршрутизатор контролює запити до DMZ, а зовнішній - лише ініціалізацію з'єднання [3].

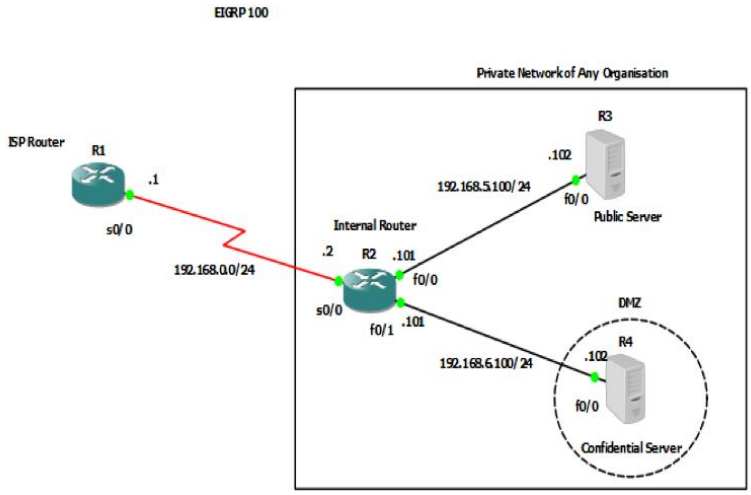


Рисунок 1.5 – Схема маршрутизації EIGRP з виділеною DMZ (R. Kumar et al., 2018)

Науковці Ali A. et al. (2019) [4] доповнили цю концепцію, запропонувавши дворівневу архітектуру "secure DMZ", у якій внутрішній маршрутизатор реалізує механізми інспекції пакетів та політики доступу на прикладному рівні (L7). На рис. 1.6 зображено схему взаємодії внутрішнього та зовнішнього маршрутизаторів із застосуванням принципу Zero Trust, де перевірка трафіку здійснюється на обох рівнях. Такий підхід зменшує ризики несанкціонованих підключень і є перехідним етапом до двошарових DMZ-систем [4].

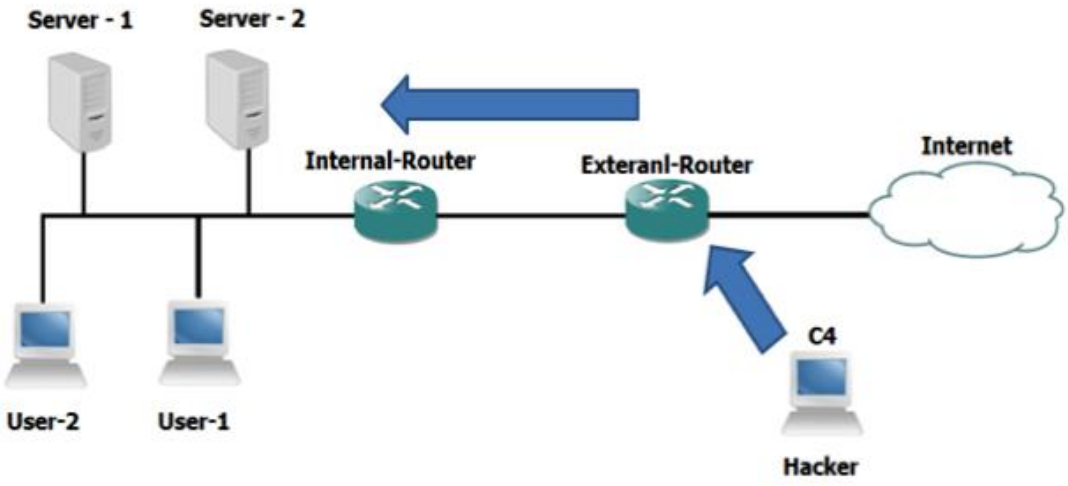


Рисунок 1.6 – Модель дворівневої DMZ з контролем L7 (Ali A. et al.,2019)

Порівняльний аналіз робіт Qi S. et al. (2024), Shrimali S. (2017), Kumar R. (2018) та Ali A. (2019) показує, що еволюція архітектур безпеки рухається від простих фізичних зональних моделей до логічно сегментованих багаторівневих структур із контекстною маршрутизацією, динамічним управлінням потоками та вбудованими механізмами довіри. Водночас більшість наукових праць зосереджується або на рівні транспортного захисту, або на периметральній ізоляції, не враховуючи взаємодію між аналітичними, сервісними й внутрішніми сегментами великих Intranet-мереж.

У результаті аналізу наявних теоретико-методологічних підходів виявлено, що відсутня цілісна модель двошарової DMZ для корпоративних систем із розгалуженою внутрішньою інфраструктурою. Саме тому наукова новизна даного дослідження полягає у синтезі концепцій Dual Network Architecture (Qi S. et al., 2024)та багаторівневого DMZ (Shrimali S., 2017; Ali A., 2019) у контексті Intranet-мереж із політикою Zero Trust, що дає змогу побудувати адаптивну архітектуру з незалежним контролем транспортного і прикладного рівнів. Такий підхід формує теоретичне підґрунтя для подальшого моделювання потоків даних, сегментації трафіку й оцінки ефективності механізмів захисту корпоративних систем.

1.3 Аналіз існуючих рішень

Аналіз сучасних рішень у сфері побудови демілітаризованих зон (DMZ) корпоративних мереж показує, що провідні виробники фокусуються на підвищенні рівня ізоляції, автоматизації політик безпеки та інтеграції систем моніторингу подій. Найпоширенішими підходами є створення зонального бар'єра між WAN і LAN, використання віртуальних шлюзів доступу та динамічне мікросегментування трафіку. На рис. 1.7–1.11 наведено приклади п'яти реальних рішень, що визначають сучасний рівень розвитку архітектур DMZ.

Першим прикладом є система FortiGate від компанії *Fortinet*, яка пропонує реалізацію DMZ як частини архітектури NGFW (Next Generation Firewall). На рис. 1.7 подано фрагмент керівництва *WAN to DMZ* з офіційної документації FortiOS 7.4.4, де описано процес створення IPS-профілю для моніторингу трафіку між публічними та внутрішніми сервісами. Основна перевага підходу полягає у вбудованій системі сигнатур, яка дозволяє визначати критичні, високі та середні рівні загроз — це дає змогу реалізувати політику глибокого аналізу пакетів (DPI) і запобігати експлуатації вразливостей у сервісах DMZ.

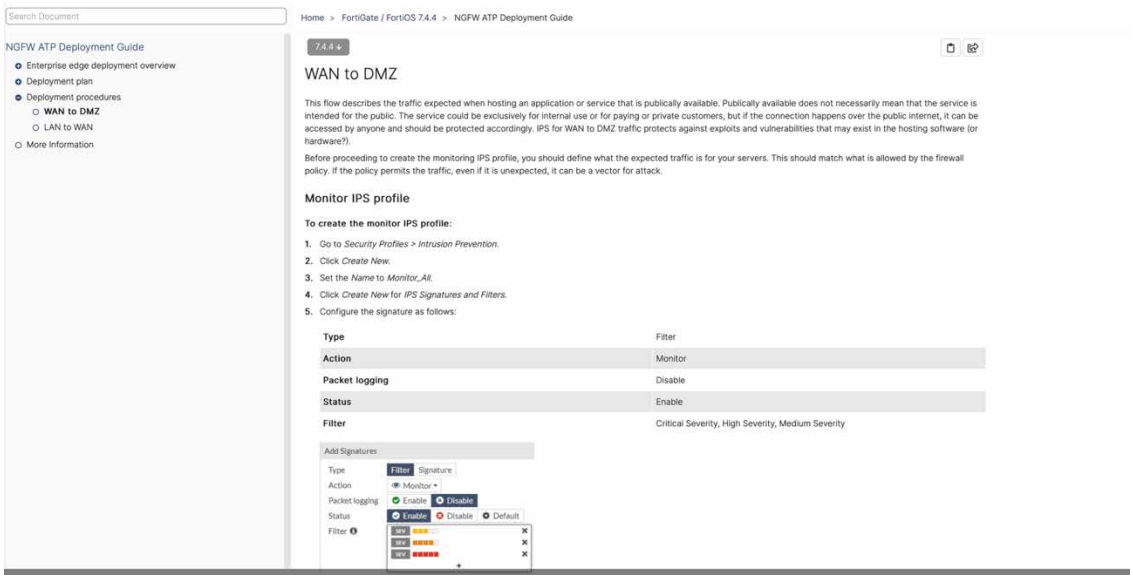


Рисунок 1.7 – Інтерфейс FortiGate 7.4.4 WAN to DMZ з налаштуванням IPS-профілю (Fortinet, 2024)

Друге рішення - Palo Alto Networks PA-Series, де концепція побудови DMZ розширена до рівня промислових систем. На рис. 1.8 представлено головну сторінку Securing OT Services by Using an Industrial DMZ – Design Guide, у якій наведено методику проектування DMZ для Operational Technology (OT) із застосуванням Panorama та Strata Logging Service. Основна особливість полягає в інтеграції фаєрволів рівня L7 із централізованим журналюванням, що дозволяє виявляти аномалії в реальному часі та забезпечувати керування політиками безпеки у віддалених об’єктах.

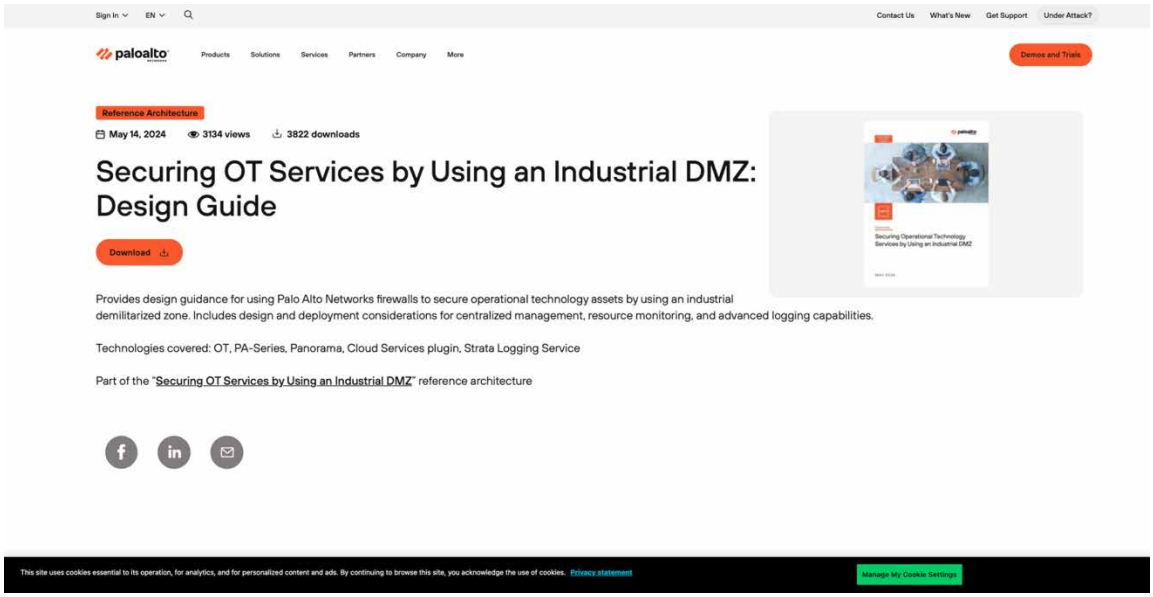


Рисунок 1.8 – Довідник Palo Alto Networks “Securing OT Services by Using an Industrial DMZ” (2024)

Третє рішення - Trout Secure Twin, яке представляє концепцію *мікро-DMZ*. Як показано на рис. 1.9, цей підхід передбачає розміщення невеликих демілітаризованих сегментів перед кожним критичним вузлом, що дозволяє забезпечити Zero Trust-контроль і шифровані локальні журнали подій. Порівняно з класичною архітектурою, такий підхід мінімізує вплив єдиної точки відмови й спрощує масштабування системи без потреби фізичної реконфігурації мережевої інфраструктури.

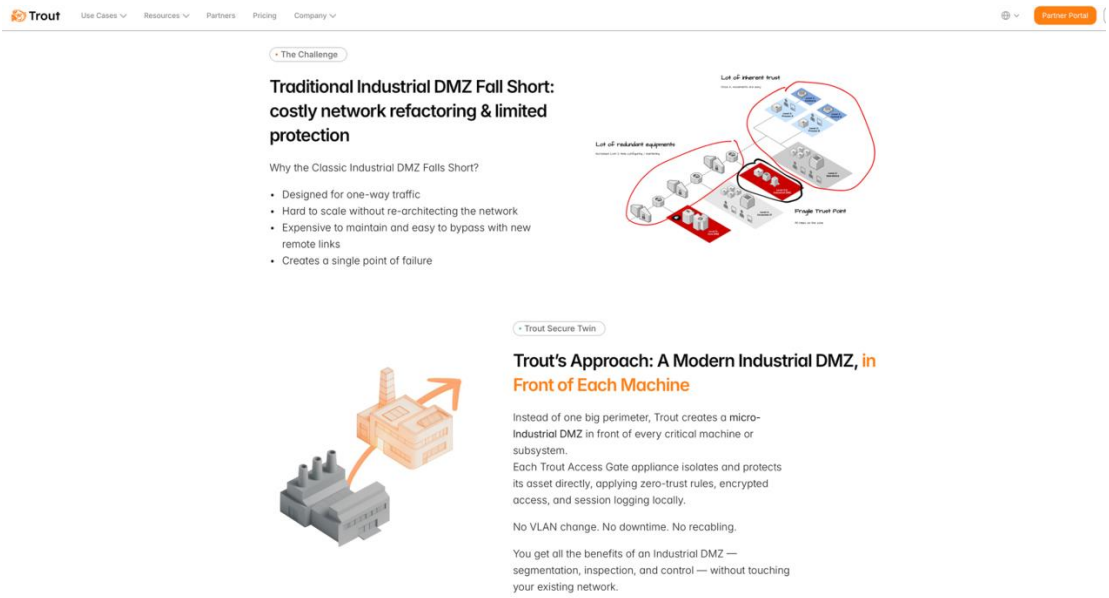


Рисунок 1.9 – Архітектура Trout Secure Twin з мікро-DMZ перед критичними серверами (Trout Software, 2024)

Четвертим прикладом є платформа Netmaker, орієнтована на побудову віртуальних DMZ у хмарних та гібридних інфраструктурах. На рис. 1.10 зображено інтерфейс керування Netmaker з підтримкою VPN-тунелів WireGuard та автоматичним контролем доступу до сегментів. Рішення дозволяє створювати приватні віртуальні DMZ-зони між корпоративними кластерами, керуючи ними через API та автоматизовані політики маршрутизації.

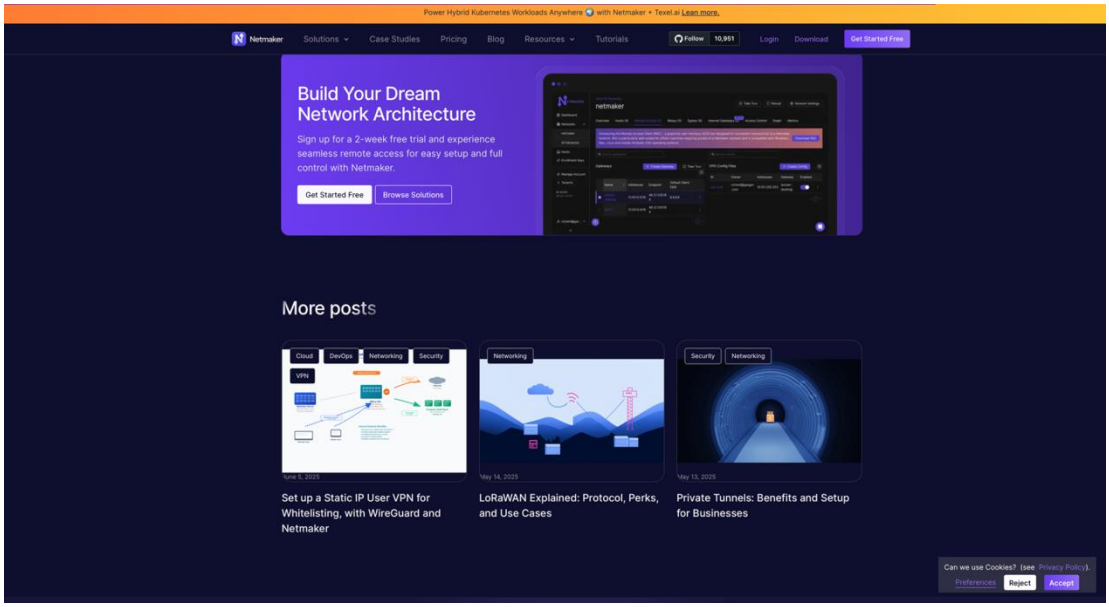


Рисунок 1.10 – Панель керування Netmaker для віртуальної DMZ у хмарному середовищі (Netmaker, 2025)

П’ятим рішенням виступає Tufin Orchestration Suite, яке забезпечує централізоване управління політиками мережевої безпеки та автоматизований контроль комплаєнсу. На рис. 1.11 показано архітектуру Tufin, що поєднує NGFW, SASE та мікросегментацію в єдину панель управління. Така модель дає змогу уніфікувати застосування політик для DMZ-сегментів у локальних і хмарних інфраструктурах та забезпечує повну відповідність стандартам ISO/IEC 27001.

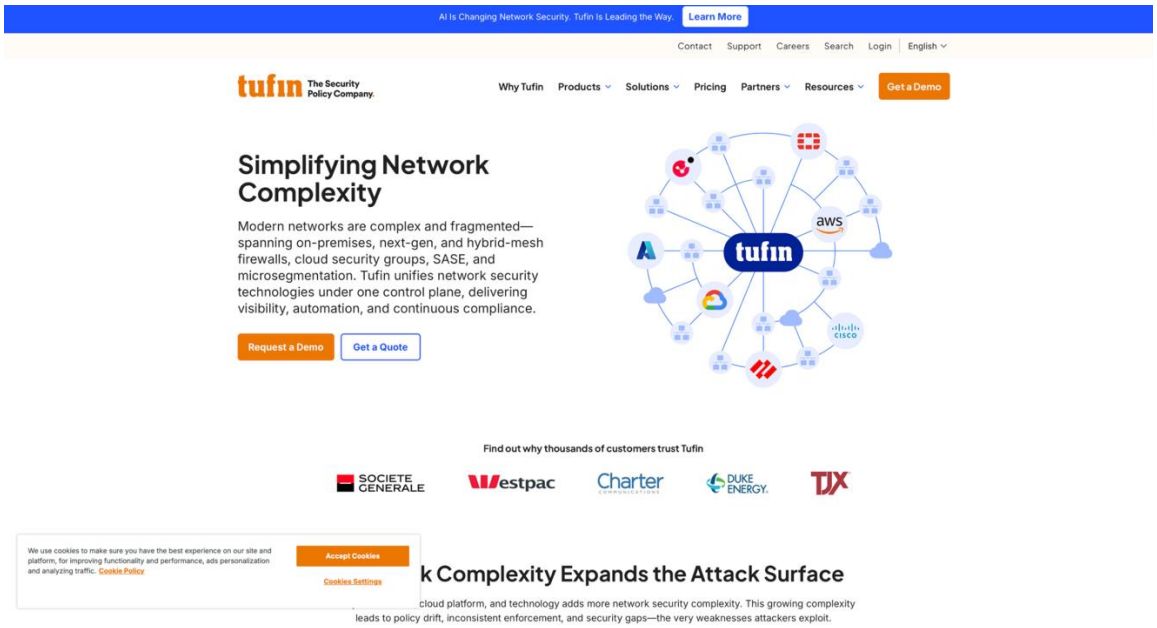


Рисунок 1.11 – Інтеграційна архітектура Tufin Orchestration Suite для мережевих політик (Tufin Ltd., 2025)

Для узагальнення характеристик і порівняння підходів наведено таблицю 1.2, у якій порівнюються п’ять реальних рішень із розроблюваною в роботі двошаровою DMZ-системою на основі Python, PyQt6 та SQLite.

Таблиця 1.2

Порівняльна характеристика існуючих рішень та запропонованої системи

Рішення	Основна технологія	Призначення	Переваги	Недоліки
FortiGate (Fortinet)	NGFW + IPS / WAF	Класичний периметровий контроль WAN→DMZ	Інтегрований DPI, висока швидкодія	Обмежена гнучкість для віртуальних мереж

Продовження таблиці 1.2

Palo Alto PA-Series	NGFW + Strata Logging	Централізоване керування OT та DMZ	Потужна аналітика, журналювання подій	Висока вартість впровадження
Trout Secure Twin	Мікро-DMZ / Zero Trust	Ізоляція окремих вузлів без реконфігурації	Висока гнучкість, мінімізація точок відмови	Обмежена масштабованість у великій мережі
Netmaker	WireGuard VPN / API	Віртуальна DMZ у хмарних середовищах	Автоматизація налаштувань, зручне керування	Потребує стабільного API та ресурсів
Tufin Suite	NGFW Policy Orchestration	Управління комплаєнсом і політиками безпеки	Єдина панель контролю, аналітика SASE	Високі системні вимоги
Запропонована система	Python + PyQt6 + SQLite	Моделювання двошарової DMZ з аналітикою та візуалізацією	Адаптивність, низькі витрати, локальна обробка подій	Потребує розширення для масштабних мереж

Проведений аналіз показує, що комерційні системи орієнтовані переважно на корпоративний сектор з високими вимогами до продуктивності та комплаєнсу, але в них відсутня адаптивна підтримка дослідницького аналізу подій та інтеграція з легкими клієнтськими модулями. Наукова новизна та практична цінність нашої розробки полягають у створенні легковагової дослідницької системи двошарової DMZ на основі Python та PyQt6 із локальним зберіганням у SQLite, яка поєднує переваги візуального аналізу, сегментації трафіку та інтерактивного контролю стану мережевих подій у реальному часі

1.4 Структурне представлення та принципи роботи системи

Архітектура досліджуваної системи побудована за принципом двошарової демілітаризованої зони (Dual-Layer DMZ), що забезпечує поетапну фільтрацію, моніторинг і контроль інформаційних потоків між зовнішнім середовищем (Інтернет) та внутрішньою корпоративною мережею (Intranet). На рис. 1.12 наведено структурну схему системи, яка охоплює чотири основні контури довіри: Інтернет, DMZ-1 (периферійна зона), DMZ-2 (прикладна зона) та Intranet із підсистемою OPS/MGMT для адміністрування та моніторингу.

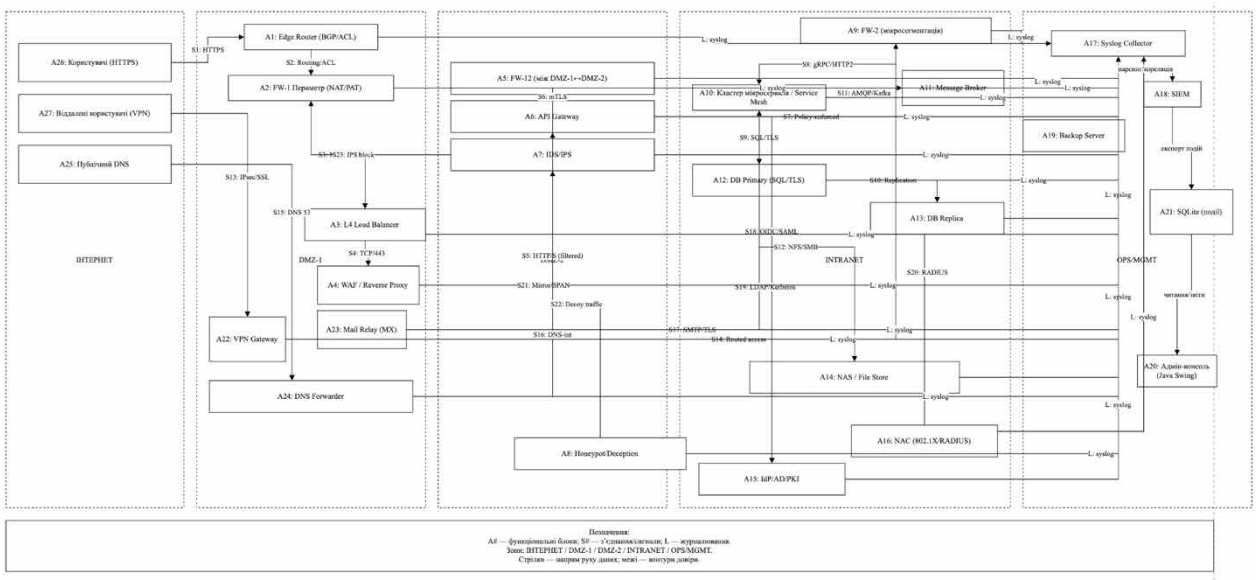


Рисунок 1.12 – Структурна схема двошарової DMZ-архітектури корпоративної мережі

Зовнішній рівень - Інтернет-сегмент - забезпечує підключення користувачів (A26), віддалених клієнтів VPN (A27) і публічного DNS-сервісу (A25). Усі запити з цього середовища спрямовуються до периферійного маршрутизатора A1 (Edge Router), який виконує маршрутизацію та первинну фільтрацію за протоколами BGP/ACL (S1–S2). Далі трафік проходить через A2 (FW-1 Perimeter), де здійснюється трансляція адрес NAT/PAT та первинне застосування політик доступу.

Перший демілітаризований рівень DMZ-1 реалізує фільтраційно-посередницькі функції. На цьому етапі дані потрапляють у A3 (L4 Load

Balancer), що розподіляє потоки між проксі-серверами WAF і релеєм поштового трафіку MX. Компонент A4 (WAF / Reverse Proxy) здійснює SSL-термінацію, контроль запитів HTTP/HTTPS та запобігання атакам OWASP Top 10 (S4–S5). Паралельно діє A23 (Mail Relay), який ізолює поштові потоки, реалізуючи TLS-шифрування та антивірусну інспекцію. Для підвищення надійності DMZ-1 включає A22 (VPN Gateway), що забезпечує безпечне з'єднання віддалених користувачів за допомогою IPsec/SSL (S13).

Другий рівень DMZ-2 є прикладною зоною, що відповідає за міжсервісну взаємодію. Тут розташовані: A6 (API Gateway) - шлюз прикладних запитів, який маршрутизує HTTPS-трафік до внутрішніх мікросервісів через FW-12 (S6); A7 (IDS/IPS) - система виявлення та запобігання вторгненням, яка аналізує пакети на рівні L7 та блокує спроби експлуатації (S3–S23); A8 (Honeypot/Deception) - пастка для атак, що створює контрольований фіктивний трафік (S22) та дає змогу збирати телеметрію про шкідливу активність.

Внутрішня корпоративна мережа Intranet включає A10 кластер мікросервісів/Service Mesh, який взаємодіє з брокером повідомлень A11 (Message Broker, AMQP/Kafka) (S11) та первинною базою даних A12 (DB Primary), де дані захищено каналами SQL/TLS (S9). Для підвищення надійності створено A13 (DB Replica) з TLS-реплікацією (S10). Сервіси аутентифікації та політик доступу реалізуються модулями A15 (IdP/AD/PKI) і A16 (NAC 802.1X/RADIUS), які формують контур довіри на основі Zero Trust-підходу (S18–S20).

Окремий сегмент OPS/MGMT призначений для збору журналів та адміністративного керування. Усі системні події, згенеровані в зонах DMZ та Intranet, передаються через канали L:syslog до A17 (Syslog Collector), який транспортує їх у A18 (SIEM) для кореляції та виявлення інцидентів безпеки. Далі дані агрегуються у A21 (SQLite)- локальному сховищі подій, що використовується аналітичним клієнтом A20 (адмін-консоль Java Swing) для формування звітів і візуалізації KPI-показників. Компонент A19 (Backup Server) забезпечує резервне копіювання конфігурацій та журналів безпеки.

Принцип роботи системи базується на багаторівневому контролі доступу, де кожен шар виконує власну функцію: DMZ-1 - ізоляція та фільтрація, DMZ-2 - аналітика й інтеграція, Intranet - виконання бізнес-логіки, OPS/MGMT - спостереження та кореляція подій. Передача даних здійснюється за схемами HTTPS/TLS, IPsec та gRPC, тоді як обмін службовими повідомленнями відбувається через AMQP/Kafka. Така архітектура дозволяє дотримуватись принципів Defence-in-Depth і Zero Trust, коли доступ до кожного сервісу контролюється окремими ACL-та TLS-сертифікатами.

Розроблена модель підтримує протоколи syslog, ODBC і API-моніторинг, що забезпечує наскрізну трасування подій від периферійних вузлів до внутрішніх систем управління. У результаті формується цілісна модель двошарової DMZ, здатна протидіяти атакам різних рівнів (мережевим, прикладним, внутрішнім), зберігаючи доступність сервісів і прозорість адміністрування.

1.5 Аналіз вимог системи

Проєктування двошарової демілітаризованої зони корпоративної мережі з розгалуженою Intranet-інфраструктурою потребує чіткого визначення функціональних, технічних та вимог до безпеки, які забезпечують ефективну роботу системи в умовах постійних кіберзагроз. На основі проведеного аналізу архітектури (рис. 1.12) і визначення взаємодії компонентів (A1–A21) сформовано сукупність вимог, які відображають ключові аспекти проєктування, розгортання та експлуатації експертної системи керування потоками у DMZ-середовищі.

До функціональних вимог віднесено забезпечення наскрізної маршрутизації між зонами, динамічний контроль доступу, оброблення подій безпеки, а також аналітичну підтримку рішень на основі журналів SIEM та локальної бази подій SQLite. Система має підтримувати реєстрацію користувачів, ведення сесій VPN, обробку запитів REST/API-Gateway,

моніторинг навантаження і формування звітів через адміністративну консоль Java Swing. Перелік основних функцій наведено в таблиці 1.3.

Таблиця 1.3

Функціональні вимоги до експертної системи

№	Вимога	Опис	Очікуваний результат
1	Управління трафіком між зонами (WAN–DMZ1–DMZ2–LAN)	Реалізація маршрутизації, NAT/PAT і фільтрації на основі ACL	Безпечний транзит даних без прямого доступу між зонами
2	Моніторинг та аналіз подій	Інтеграція з SIEM та локальним SQLite для збору syslog-повідомлень	Виявлення аномалій і побудова аналітичних звітів
3	Ідентифікація та автентифікація	Використання IdP/AD/PKI та 802.1X/RADIUS для перевірки користувачів	Контроль доступу за принципом Zero Trust
4	Адміністрування	Адмін-консоль Java Swing з можливістю керування політиками і журналами	Централізоване керування системою
5	Резервування і відновлення	Автоматичне копіювання конфігурацій і логів	Збереження працездатності після відмов
6	Інтеграція	Підтримка API Gateway, AMQP/Kafka та SQL-TLS з’єднань	Сумісність із корпоративними сервісами

До технічних вимог віднесено параметри продуктивності, надійності й масштабованості системи, а також вимоги до апаратного забезпечення та середовища виконання. Експертна система повинна бути розгорнута в середовищі Python 3.11 з інтерфейсом PyQt6, базою SQLite 3 і підтримкою TLS 1.3. Мінімальна швидкодія шлюзу повинна перевищувати 1 000 запитів/сек., а затримка обробки події не має перевищувати 200 мс. Технічні вимоги наведено в таблиці 1.4.

Таблиця 1.4

Технічні вимоги до експертної системи

№	Параметр	Вимога	Обґрунтування

Продовження таблиці 1.4

1	Продуктивність	≥ 1000 req/s на вузол	Забезпечення обробки потоків у реальному часі
2	Затримка відповіді	≤ 200 мс	Відповідність вимогам SLA для корпоративних систем
3	Відмовостійкість	≥ 99.9 % часу доступності	Мінімізація простоїв при збої вузлів
4	Середовище виконання	Python 3.11 + PyQt6 + SQLite3	Єдність середовища розробки і розгортання
5	Інтерфейс взаємодії	REST API, gRPC, ODBC	Підтримка різнорідних сервісів і БД
6	Масштабованість	Горизонтальне розширення вузлів	Адаптація під різні топології мережі

Вимоги до безпеки визначають набір заходів і політик, спрямованих на гарантування цілісності, конфіденційності та доступності даних у межах усіх зон. Система повинна підтримувати двофакторну автентифікацію, аудит дій користувачів, автоматичне виявлення підозрілих сесій, а також шифрування всіх каналів зв’язку (TLS, IPsec, SSH). Задля мінімізації ризику компрометації реалізовано Honeypot-модуль для збору зразків шкідливої активності. Перелік вимог наведено в таблиці 1.5.

Таблиця 1.5

Вимоги до безпеки експертної системи

№	Вимога	Опис	Рівень важливості
1	Автентифікація та авторизація	Двофакторна перевірка користувачів (OTP + PKI)	Критичний
2	Шифрування трафіку	TLS 1.3 / IPsec / SSH для всіх з’єднань між зонами	Критичний
3	Аудит і журналювання	Збереження syslog-подій у SIEM + SQLite	Високий
4	Виявлення атак	IDS/IPS + Honeypot для аналізу поведінки	Високий
5	Політика доступу	Zero Trust / RBAC / ABAC для сервісів DMZ і Intranet	Високий
6	Резервування даних	Автоматичне копіювання журналів і БД	Середній

Узагальнюючи результати аналізу, можна зазначити, що сукупність вимог формує базову архітектуру експертної системи, яка поєднує аналітичні, транспортні та захисні функції. Її реалізація забезпечує багаторівневу сегментацію корпоративної мережі, централізоване управління подіями та дотримання принципів Defence-in-Depthi Zero Trust. У результаті система здатна забезпечити гарантовану цілісність даних, своєчасне реагування на інциденти та високий рівень безпеки при мінімальних експлуатаційних витратах.

1.6 Постановка завдання

Постановка завдання полягає у створенні експертної системи для моделювання, контролю та аналізу потоків даних у двошаровій демілітаризованій зоні корпоративної мережі, яка забезпечує багаторівневий захист, розмежування доступу та централізовану аналітику безпеки. Основною метою системи є підвищення рівня стійкості корпоративної інфраструктури до зовнішніх і внутрішніх загроз шляхом побудови архітектури “Dual-Layer DMZ”, що об’єднує периферійний рівень фільтрації (DMZ-1) та прикладний рівень аналітики (DMZ-2) із подальшою взаємодією з внутрішнім середовищем Intranet і адміністративним контуром OPS/MGMT. Для досягнення цієї мети система повинна автоматично аналізувати маршрути трафіку, корелювати події безпеки, виявляти потенційні аномалії та формувати рекомендації для адміністратора на основі аналітичних правил і накопичених журналів подій.

Вхідними даними для роботи системи є мережеві запити та пакети, що надходять із зовнішнього середовища через шлюзові пристрої та VPN-з’єднання, журнали подій від міжмережевих екранів, IDS/IPS, API-шлюзів і баз даних, кореляційні повідомлення від SIEM-системи, метадані про параметри трафіку (IP-адреси, порти, протоколи, час, напрямки передачі, рівень загроз), а також конфігураційні параметри політик доступу, ACL-правил, TLS-сертифікатів і ролей користувачів. Додатковим джерелом даних є команди адміністратора, які

вводяться через Java Swing-консоль для керування політиками, фільтрами, запитами до локальної бази подій SQLite та перегляду звітів.

Результатом роботи системи є формування вихідних даних у вигляді структурованих аналітичних звітів про стан безпеки в кожній зоні (DMZ-1, DMZ-2, Intranet), журналів кореляції подій із визначенням критичних інцидентів і рекомендаціями щодо реагування, візуалізованих KPI-показників щодо продуктивності, навантаження й доступності сервісів, а також автоматичних сповіщень про аномальні дії чи відмови компонентів. Крім того, система генерує оновлені політики доступу (ACL, RBAC, ABAC) на основі виявлених подій, виконує резервне копіювання конфігурацій і логів безпеки, а також забезпечує збереження аналітичних даних у локальному сховищі SQLite для подальшої експертної обробки.

Поставлене завдання передбачає створення комплексної інтелектуальної системи на основі Python 3.11, PyQt6 та SQLite, яка реалізує взаємодію з SIEM-платформою, IDS/IPS-модулями та Honeypot-пастками через стандартизовані протоколи Syslog, REST API та AMQP/Kafka. Розроблена система має забезпечити автоматизоване виявлення інцидентів, аналіз потоків у реальному часі, багаторівневе зонування доступу та адаптивне реагування на події безпеки з урахуванням принципів Defence-in-Depth і Zero Trust. У результаті її впровадження корпоративна мережа набуває здатності до самокорекції, стійкого функціонування в умовах кібератак і прозорого адміністрування без втрати ефективності обміну даними між сегментами.

2 ПРОЄКТУВАННЯ ПІДСИСТЕМИ NAT У ДВОШАРОВІЙ DMZ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Функціональна схема та логічна архітектура підсистеми NAT у двошаровій DMZ

Функціональна схема підсистеми NAT відображає узагальнену структуру оброблення, трансляції та контролю мережевого трафіку в умовах дворівневої DMZ-архітектури корпоративної мережі. На рис. 2.1 наведено логічну модель взаємодії ключових підсистем, яка визначає послідовність проходження пакетів від зовнішнього середовища до внутрішніх сервісів Intranet через сегменти DMZ-1 та DMZ-2. Зображена схема демонструє ієрархічний характер маршрутизації, коли NAT-перетворення та фільтрація застосовуються поетапно з метою виключення прямого доступу між зонами довіри та мінімізації впливу потенційних атак.

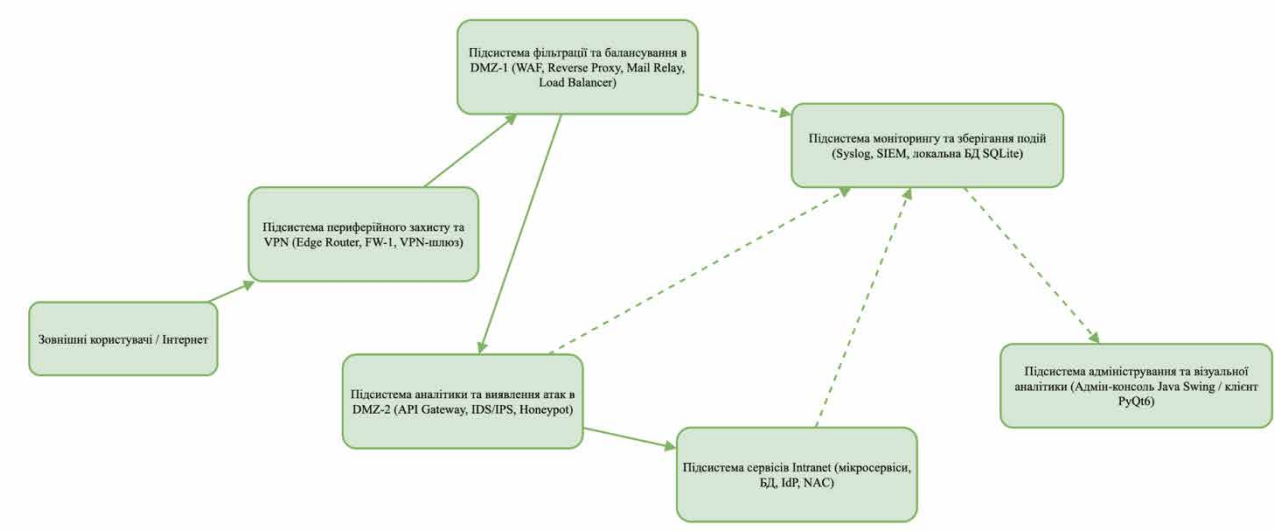


Рис. 2.1 – Функціональна схема логічної архітектури Dual-Layer DMZ і точок застосування NAT-перетворень

У межах представленої архітектури першим елементом оброблення запитів є підсистема периферійного захисту та VPN, яка включає Edge Router, FW-1 та шлюз VPN. Саме на цьому рівні здійснюється первинна трансляція адрес (NAT/PAT), фільтрація пакетів за ACL-правилами та маршрутизація трафіку

відповідно до напрямків WAN→DMZ-1. На рівні підсистеми фільтрації та балансування DMZ-1 NAT використовується для ізоляції публічних IP-адрес від внутрішніх сегментів, а також для забезпечення коректної роботи WAF, реверс-проксі, поштового релея та балансувальників навантаження.

Далі NAT-перетворення застосовуються в аналітичній підсистемі DMZ-2, де містяться API Gateway, IDS/IPS та Honeypot. У цій зоні NAT виконує роль внутрішнього сегментаційного механізму, який дає змогу розмежовувати прикладні шлюзи, внутрішні API-маршрути та приховувати адресний простір Intranet від зовнішнього трафіку. Пакети, що проходять усі перевірки, спрямовуються до підсистеми сервісів Intranet, яка містить мікросервіси, бази даних, модулі IdP та NAC. Внутрішній NAT забезпечує маршрутизацію між вузлами Service Mesh та підтримку ізольованих підмереж для критичних сервісів.

Результати роботи NAT-ядра, журнали оброблених сесій, дані про відхилені запити та метадані аномалій надходять у підсистему моніторингу та зберігання подій, де здійснюється їхня кореляція в SIEM, збереження локальних копій у SQLite та передавання в модуль адміністративної аналітики. Узгоджена взаємодія цих підсистем дає змогу підтримувати цілісний цикл: фільтрація → трансляція → виявлення атак → маршрутизація → журналювання.

Для формалізованого опису функцій кожної підсистеми сформовано таблицю 2.1, яка відображає роль сегментів у загальній NAT-логіці.

Таблиця 2.1 – Функціональні ролі підсистем у контурі NAT двошарової DMZ

Підсистема	Основна функція	Роль у NAT-архітектурі
Периферійний захист та VPN	Первинна маршрутизація, ACL-фільтрація, VPN-сесії	Початковий NAT/PAT, маскування внутрішніх адрес
Фільтрація та балансування в DMZ-1	SSL-термінація, WAF, Reverse Proxy, Mail Relay	Сегментаційний NAT для публічних сервісів
Аналітика та IDS/IPS у DMZ-2	Аналіз пакетів L7, виявлення аномалій, Honeypot	Внутрішній NAT між API-шлюзами та сервісами

Продовження таблиці 2.1

Сервіси Intranet	Мікросервіси, БД, IdP, NAC	Приватний адресний простір, внутрішня маршрутизація
Моніторинг і журнали	Syslog, SIEM, локальна БД SQLite	Журналювання NAT-сесій, аналіз інцидентів
Адміністрування та візуальна аналітика	Java Swing / PyQt6	Перегляд стану NAT, статистики та KPI

Узагальнюючи, логічна архітектура Dual-Layer DMZ визначає NAT як ключовий механізм контролю та фільтрації, що забезпечує поетапну трансляцію адрес, сегментацію потоків і приховування внутрішніх ресурсів від потенційних загроз. Представлена функціональна схема (рис. 2.1) демонструє, що підсистема NAT інтегрована на кожному рівні оброблення трафіку - від периферійного маршрутизатора до внутрішніх сервісів Intranet - формуючи єдиний багаторівневий контур ізоляції й логічного зонування. Такий підхід підвищує стійкість корпоративної мережі до зовнішніх кібератак, а також забезпечує прозорість, керованість і відтворюваність процесів маршрутизації та безпеки.

2.2 Електрична та монтажна схема дослідного стенду емулятора

Електрична та монтажна схема дослідного стенду формує фізичну основу для розгортання моделі двошарової DMZ, підсистеми NAT та мережевих модулів аналізу трафіку. Схема включає реальні зразки маршрутизаторів, комутаторів, міжмережевих екранів, SIEM-підсистеми, VPN-каналів, а також інженерну інфраструктуру живлення, заземлення та структурованої кабельної системи. На рис. 2.2 показано базовий маршрутизатор Cisco ISR, який виконує роль периферійного вузла DMZ-1 та забезпечує первинну маршрутизацію, NAT/PAT, ACL-фільтрацію та обробку WAN-каналу.

Рис. 2.2 – Маршрутизатор Cisco ISR, що використовується у периферійній зоні DMZ-1

На рис. 2.3 наведено 48-портовий гігабітний комутатор, що забезпечує комутацію в межах DMZ-1/DMZ-2 та OPS/MGMT. Комутатор використовується як магістральний вузол розподілу Ethernet-сегментів стенду й підтримує VLAN-сегментацію та trunk-канали.

Рис. 2.3 – 48-портовий L2/L3 комутатор магістрального рівня дослідного стенду

На рис. 2.4 представлено міжмережевий екран FortiGate 120G, який реалізує політики фільтрації, DPI-аналіз, IPS та NAT-правила другого рівня. У структурі лабораторного стенду цей пристрій розміщується між DMZ-1 та DMZ-2 і забезпечує глибинний контроль L3–L7.

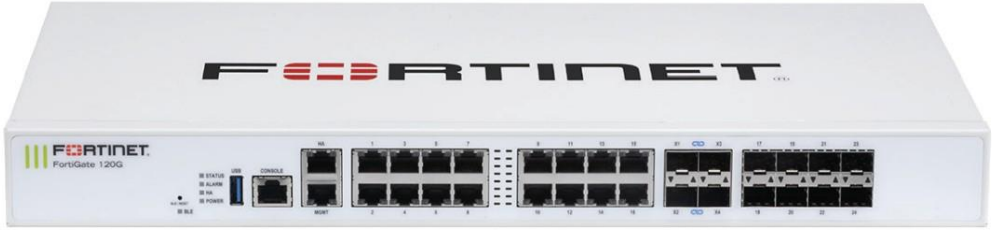


Рис. 2.4 – Міжмережевий екран FortiGate 120G у контурі Dual-Layer DMZ

На рис. 2.5 наведено логічну схему SIEM CorreLog, яка використовується для збору, нормалізації та кореляції подій з Edge Router, FortiGate, IDS/IPS, серверів БД, інфраструктурних компонентів та сервісів Intranet. SIEM-підсистема виконує ключову роль у тестуванні поведінки NAT-таблиць і виявленні аномалій.

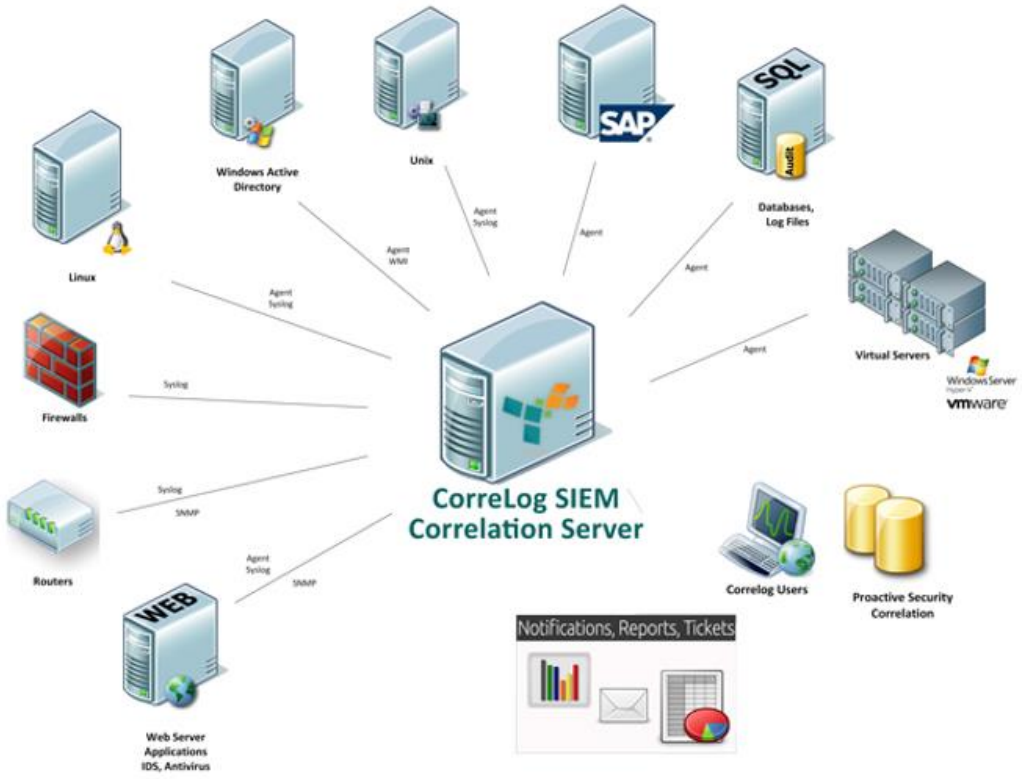


Рис. 2.5 – Логічна схема кореляційного сервера SIEM CorreLog

На рис. 2.6 представлено стандартну VPN-топологію «Site-A ↔ Site-B», яка використовується для імітації міжсайтового обміну трафіком. У дослідному стенді ця схема дає змогу відтворити транзитні NAT-перетворення, побудувати IPsec-тунелі й перевірити стійкість DMZ-архітектури до міжсегментних атак.

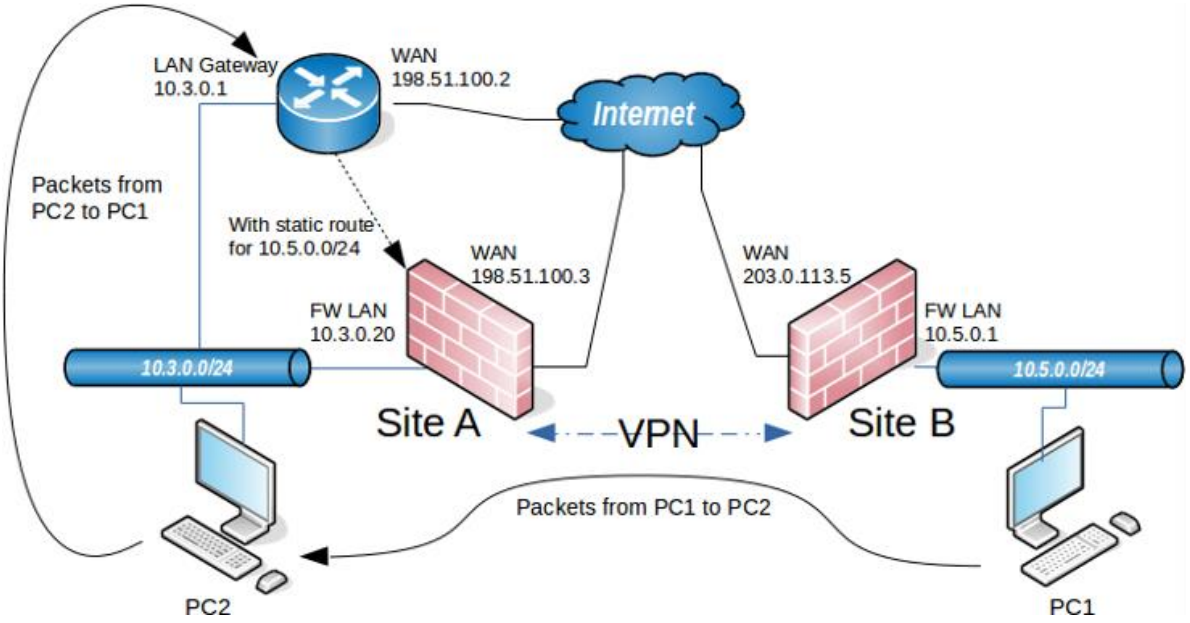


Рис. 2.6 – Топологія Site-to-Site VPN для експериментів з NAT і маршрутизацією

На рис. 2.7 наведено електричну схему живлення стенду, яка включає ввід 220 В AC, автоматичний вимикач, контур заземлення, UPS основного серверного комплексу, UPS робочих місць адміністраторів та три PDU-модулі, до яких підключено обладнання DMZ-1, DMZ-2 та Intranet-сегментів.

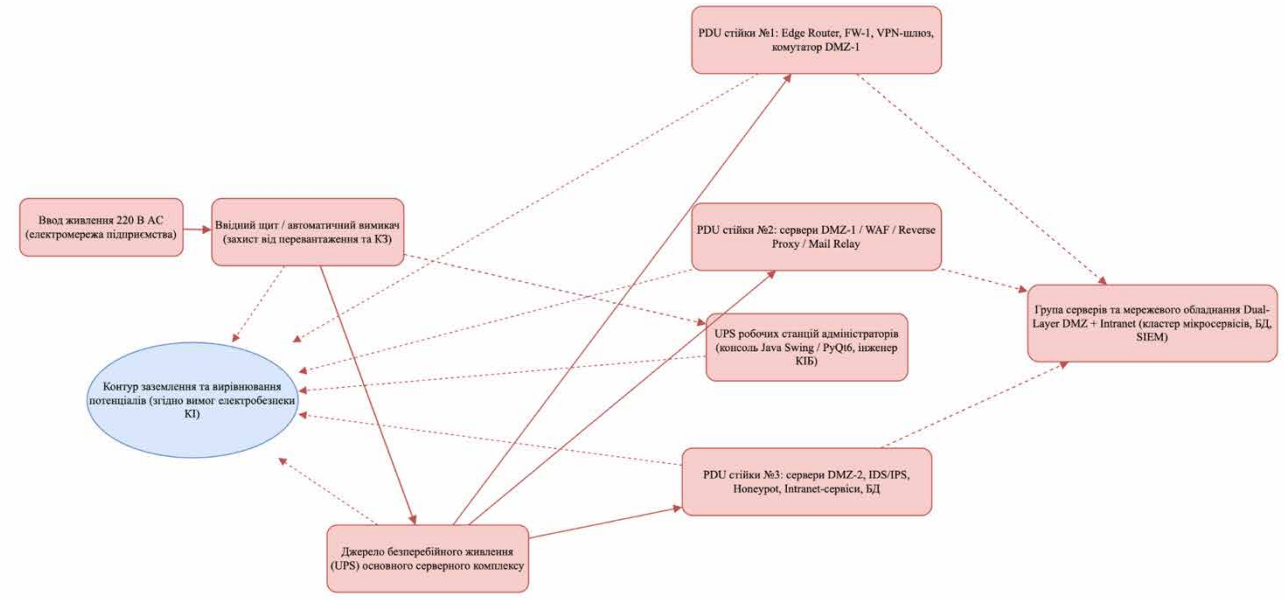


Рис. 2.7 – Електрична схема живлення та заземлення стенду (UPS, PDU, контури живлення)

На рис. 2.8 подано монтажну схему FO/UTP-кабельної інфраструктури серверної кімнати. Вона містить оптичний ввід від провайдера, FO-магістраль,

структуру патч-панелей WAN, DMZ-1, DMZ-2, Intranet, OPS/MGMT, а також uplink-канали до офісного L2-комутатора та робочих станцій КІБ.

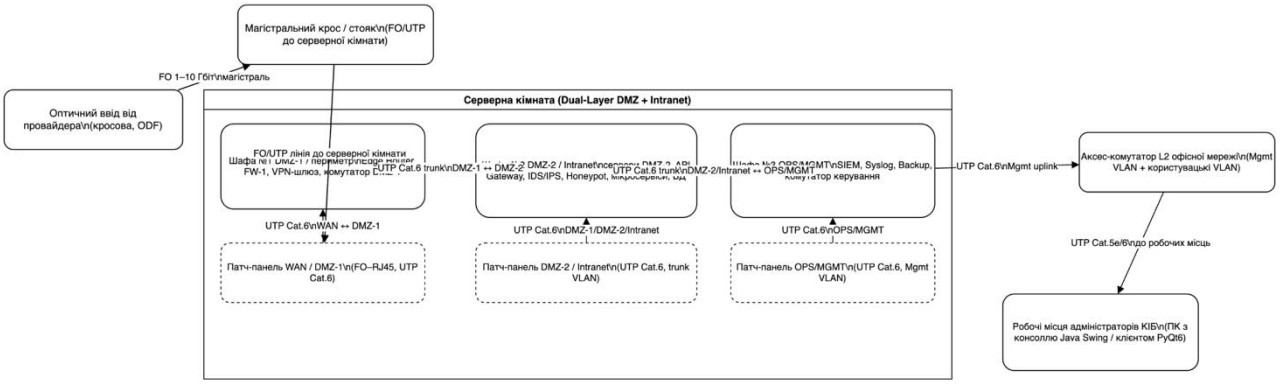


Рис. 2.8 – Монтажна схема FO/UTP-ліній, патч-панелей і магістральних комутаторів

Для формалізації складу експериментального комплексу у таблиці 2.2 наведено перелік основного обладнання, що використовується у дослідному стенді для реалізації Dual-Layer DMZ, підсистеми NAT та модулів емулятора.

Таблиця 2.2 – Основне мережеве та серверне обладнання дослідного стенду Dual-Layer DMZ + NAT

№	Обладнання	Призначення	Розташування
1	Cisco ISR / Edge Router	Периферійна маршрутизація, NAT/PAT, ACL	DMZ-1
2	48-портовий Gigabit комутатор	Комутація DMZ-1/DMZ-2/OPS	Шафа №1–3
3	FortiGate 120G	FW-1/IPS, політики доступу, DPI	DMZ-1
4	SIEM CorreLog сервер	Кореляція подій, збір логів	OPS/MGMT
5	Сервери DMZ-2 (API-Gateway/IDS/IPS/Honeypot)	Аналіз трафіку, виявлення атак	DMZ-2
6	Сервери Intranet (БД, мікросервіси, IdP, NAC)	Внутрішні сервіси, зберігання даних	Intranet
7	UPS (основний + робочих місць адміністраторів)	Резерв живлення стенду	Серверна
8	Оптичні й мідні патч-панелі	Структурована кабельна система	Усі шафи
9	Робочі станції адміністраторів (Java Swing / PyQt6)	Керування, моніторинг, візуальна аналітика	OPS/MGMT

Сукупність електричних та монтажних схем, наведених на рис. 2.2–2.8, відображає реальну конфігурацію дослідного середовища та забезпечує ієрархічне зонування ресурсів: периферійного маршрутизатора, підсистем DMZ-1 та DMZ-2, серверів Intranet та контуру OPS/MGMT. Введення електроживлення 220 В AC, підсистема заземлення, UPS-резервування та організована структурована кабельна система створюють необхідні умови для стабільного функціонування експериментального комплексу. Така інтеграція забезпечує відтворюваність тестів NAT-перетворень, роботу модулів IDS/IPS, а також коректну взаємодію між компонентами двошарової архітектури DMZ.

2.3 Передумови створення програмного емулятора та вибір технологічного стеку

Розроблення програмного емулятора двошарової демілітаризованої зони корпоративної мережі з розгалуженою Intranet-інфраструктурою обумовлене необхідністю створення відтворюваного, ізольованого та керованого середовища для дослідження поведінки NAT-перетворень, механізмів фільтрації трафіку, роботи прикладних шлюзів, міжмережевих екранів, VPN-тунелів та систем виявлення й запобігання вторгненням. Реальні корпоративні мережі не дозволяють проводити експерименти зі зміною політик доступу, перерозподілом маршрутів, моделюванням атак чи навмисним створенням аномальних потоків, оскільки це може призвести до порушення SLA або зупинки сервісів. Тому створення емулятора дає змогу виконувати експериментальні дослідження без впливу на продуктивну інфраструктуру, а також формувати модель поведінки двошарової DMZ за різних навантажень і сценаріїв загроз.

У процесі проєктування було розглянуто декілька варіантів технологічного стеку для моделювання роботи DMZ-1, DMZ-2, підсистем NAT, API-Gateway, IDS/IPS та SIEM-кореляції. Основні критерії відбору включали: можливість асинхронної обробки трафіку, підтримку низькорівневого аналізу пакетів,

простоту інтеграції з UI-консолями адміністратора, доступність бібліотек для моделювання мережевих операцій, стабільність під час тривалих експериментів та можливість контейнеризації. Порівняльні характеристики варіантів наведено у табл. 2.2.

Таблиця 2.2 – Порівняння варіантів технологічних стеків для створення програмного емулятора Dual-Layer DMZ

№	Технологія / Стек	Переваги	Недоліки	Використання в роботі
1	Python 3.12 (asyncio, Scapy)	Асинхронність, низькорівнева робота з пакетами, гнучкість	Обмежена продуктивність у high-load	Основне ядро емуляції NAT/DMZ
2	FastAPI / Flask	Легкий REST API, просте моделювання логіки шлюзів	Потребує ASGI/WSGI сервера	API-шлюз DMZ-2
3	SQLite 3	Простота, zero-config, стабільність, низькі ресурси	Не розраховано на масивний трафік	Зберігання NAT-таблиць, логів, кореляцій
4	PyQt6 / Java Swing	Швидке створення UI, кросплатформність	Потребує окремих клієнтів	Консоль адміністратора й аналітики
5	Docker	Повторюваність, ізоляція, просте масштабування	Необхідність створення окремих образів	Контейнеризація модулів DMZ
6	GNS3 / EVE-NG	Моделювання маршрутизаторів, фаєрволів, тунелів	Висока ресурсомісткість	Емуляція периферійної топології
7	WireGuard / OpenVPN	Простота створення тунелів	Потреба окремого процесу	Модель VPN для стенду

Обраний стек забезпечує можливість моделювати ключові процеси, характерні для двошарової DMZ: багаторівневу фільтрацію трафіку, поведінку NAT при різних схемах маршрутизації, взаємодію прикладних шлюзів, реакції IDS/IPS на аномальні потоки, формування syslog-подій, їхню агрегацію та подальшу кореляцію. Python забезпечує низькорівневу обробку пакетів, FastAPI - роботу API-шлюзів DMZ-2, а SQLite - збереження станів та журналів. PyQt6 та Java Swing використовуються для візуалізації топології DMZ, NAT-таблиць,

статусів вузлів і метрик. Docker дозволяє створити кілька незалежних інстансів DMZ-1, DMZ-2 та Intranet-сегментів, забезпечуючи відтворюваність експериментів і масштабованість моделі.

У результаті сформований технологічний стек забезпечує повноцінну платформу для дослідження двошарових демілітаризованих зон, дозволяє моделювати різні сценарії загроз, тестувати надійність архітектури, оцінювати ефективність механізмів сегментації трафіку та формувати експериментальну базу для подальших аналітичних висновків.

2.4 Формалізація специфікації повідомлень і тем MQTT

Одним з ключових елементів досліджуваної архітектури Dual-Layer DMZ є підсистема обміну подіями між периферійними вузлами, NAT/Firewall агентами, SIEM-конекторами та операторськими консолями, що здійснюється через брокер MQTT у DMZ-1. Формалізація форматів повідомлень, семантики тем і політик доступу дозволяє забезпечити керовану маршрутизацію телеметрії, статусів, команд, результатів обробки та аудиторських логів між компонентами розгалуженої Intranet-мережі та демілітаризованих зон. На рис. 2.9 подано структурну схему організації MQTT-взаємодії, де показано розподіл ролей клієнтів, рівні безпеки, модель RBAC по темах і набори підписок для основних функціональних вузлів.

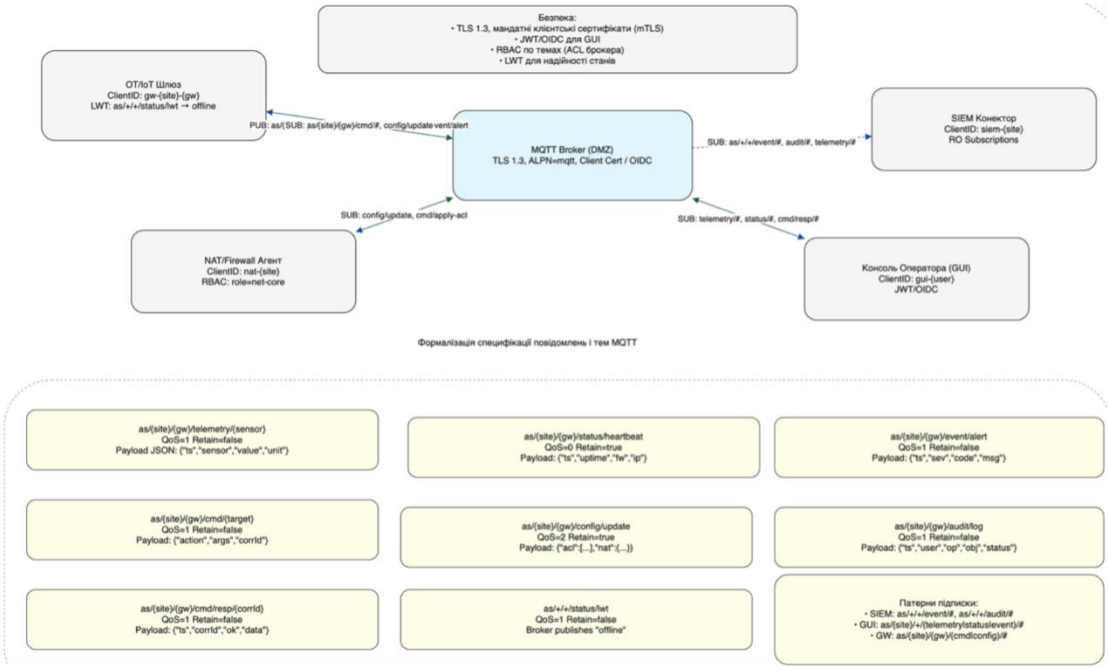


Рис. 2.9 – Логічна модель MQTT-взаємодії в архітектурі Dual-Layer DMZ (взято зі скріну, який ти надав)

Формалізація тем MQTT необхідна для уніфікації обміну даними між DMZ-1 (MQTT Broker, NAT/Firewall Agent, операторські консолі) та DMZ-2 (SIEM-конектор, аналітичні модулі). Це забезпечує передбачуваність обробки телеметрії, відокремлення потоків службової інформації від команд керування, а також можливість гнучкої маршрутизації подій у межах Intranet-мережі. У табл. 2.3 наведено структуру основних тем MQTT, їхні параметри QoS, політики збереження повідомлень і форматами JSON-payload'ів.

Таблиця 2.3 – Основні теми MQTT та їхня формальна специфікація

Тема MQTT	Призначення	QoS	Retain	Формат повідомлення (JSON)
as/{site}/{gw}/telemetry/{sensor}	Потік телеметрії сенсорів, переданих через DMZ-1	1	false	{ "ts": "...", "sensor": "...", "value": "...", "unit": "..." }
as/{site}/{gw}/status/heartbeat	Heartbeat-статуси шлюзу, контроль доступності	0	true	{ "ts": "...", "uptime": "...", "fw": "...", "ip": "..." }
as/{site}/{gw}/config/update	Віддалене оновлення конфігурації	2	true	{ "acf": {...}, "nat": {...} }

	NAT/Firewall агента			

Продовження таблиці 2.3

as/{site}/{gw}/cmd/{target}	Команди керування до шлюзу / агента	1	false	{ "action": "...", "args": {...}, "corrId": "..." }
as/{site}/{gw}/cmd/resp/{corrId}	Відповіді на команди керування	1	false	{ "ts": "...", "corrId": "...", "ok": "...", "data": {...} }
as/{site}/{gw}/event/alert	Сигналізація подій безпеки (аналітика DMZ-2)	1	false	{ "ts": "...", "sev": "...", "code": "...", "msg": "..." }
as/{site}/{gw}/audit/log	Аудиторські події NAT/Firewall агента	1	false	{ "ts": "...", "user": "...", "op": "...", "obj": "...", "status": "..." }
as/+/+/status/lwt	Last-Will-повідомлення про втрату зв’язку	1	false	"offline"

Узагальнення результатів формалізації дозволяє вибудувати керовану модель міжсегментної взаємодії в архітектурі Dual-Layer DMZ. Визначена структура тем MQTT забезпечує чітке розділення потоків телеметрії, керування, моніторингу, подій безпеки та аудиту. Використання TLS 1.3 з мандатними клієнтськими сертифікатами, OIDC-автентифікації та RBAC-контролю по темах гарантує надійність комунікації між брокером у DMZ-1 та вузлами Intranet-мережі. Формалізована модель MQTT створює передумови для подальшого аналізу продуктивності, безпеки й стійкості двошарової демілітаризованої зони під час високих навантажень і моделювання кіберзагроз.

2.5 Висновки до другого розділу

У другому розділі здійснено комплексне проєктування двошарової демілітаризованої зони корпоративної мережі із розгалуженим Intranet-сегментом, що дало змогу сформувати цілісну модель взаємодії периферійних маршрутізаторів, міжмережевих екранів, аналітичних модулів, брокера MQTT та

службових компонентів керування. Розроблена функціональна схема показала узгоджену структуру DMZ-1 і DMZ-2, включно з модулем фільтрації та балансування трафіку, засобами виявлення атак, VPN-шлюзами та сервісами внутрішньої мережі, що забезпечує сегментацію трафіку, ізоляцію критичних сервісів та контрольований доступ із зовнішніх доменів.

Електрична та монтажна схема дослідного стенду відтворила реальні інженерні умови експлуатації двошарової DMZ: організацію контурів заземлення, побудову структурованої кабельної системи, використання PDU-модулів, резервування UPS та фізичне зонування обладнання відповідно до його функціонального призначення. Це забезпечує відтворюваність експериментів та дає можливість проводити тестування поведінки NAT/Firewall під навантаженням за умов, наближених до промислової інфраструктури.

На основі аналізу вимог та критичних властивостей демілітаризованих зон обґрунтовано необхідність створення програмного емулятора, який усуває ризики впливу на продуктивні сервіси та дає змогу досліджувати нестандартні сценарії трафіку, порушення політик доступу, поведінку агента NAT/Firewall у стресових режимах, а також роботу засобів аудиту та кореляції подій. Проведене порівняння технологічних стеків засвідчило доцільність використання Python 3.12 для моделювання пакетів і NAT-станів, FastAPI для реалізації шлюзових API DMZ-2, SQLite для зберігання журналів та PyQt6/Java Swing для візуалізації топології, логів і стану мережевих компонентів.

Детальна формалізація MQTT-повідомлень і тематичного простору стала основою для побудови уніфікованої моделі міжсегментної взаємодії між компонентами DMZ-1, DMZ-2 та Intranet-сегмента. Визначено семантику телеметрії, heartbeat-статусів, керувальних команд, відповідей, подій безпеки та аудиту; сформовано політики QoS, атрибути Retain та стандартизовано JSON-структури, що забезпечує керованість та передбачуваність обміну даними в межах двошарової архітектури.

У сукупності результати розділу створюють обґрунтовану архітектурну та інженерну основу для подальшої реалізації програмного емулятора DMZ,

побудови експериментальної моделі трафіку, дослідження NAT-перетворень, кореляції інцидентів та оцінювання стійкості сегментованої корпоративної мережі до деструктивних впливів ззовні та зсередини.

3 ПРОГРАМНА ІМПЛЕМЕНТАЦІЯ ЗАХИЩЕНОЇ АВТОНОМНОЇ МЕРЕЖІ З ТЕХНОЛОГІЄЮ NAT

3.1 Аналіз механізмів трансляції адрес у NAT-інфраструктурі двошарової DMZ-системи

Механізми трансляції адрес (NAT) відіграють ключову роль у забезпеченні контрольованої взаємодії між компонентами двошарової демілітаризованої зони (DMZ-1 і DMZ-2) та розгалуженою корпоративною Intranet-мережею. NAT у цьому контексті використовується не лише як засіб оптимізації обмеженого адресного простору IPv4, але й як елемент сегментації, маскування внутрішніх мережевих структур, фільтрації потоків і контролю доступу між зонами різного рівня довіри. На рис. 3.1 наведено базовий механізм статичної трансляції в межах DMZ-1, коли зовнішні сервіси (вузли публікації, API-шлюзи або проксі-сервери) отримують фіксовані відображення глобальних адрес, через які до них організовується зовнішній доступ.

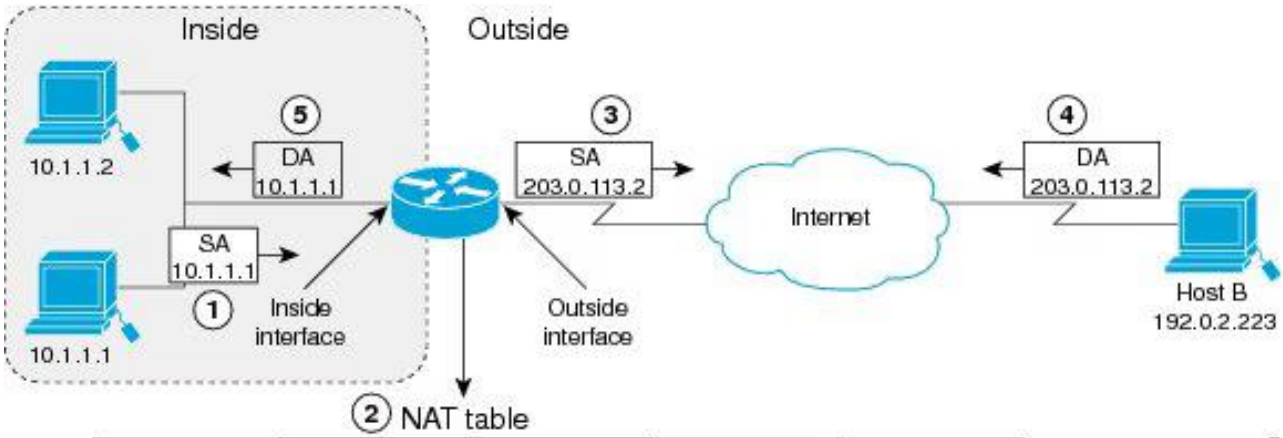
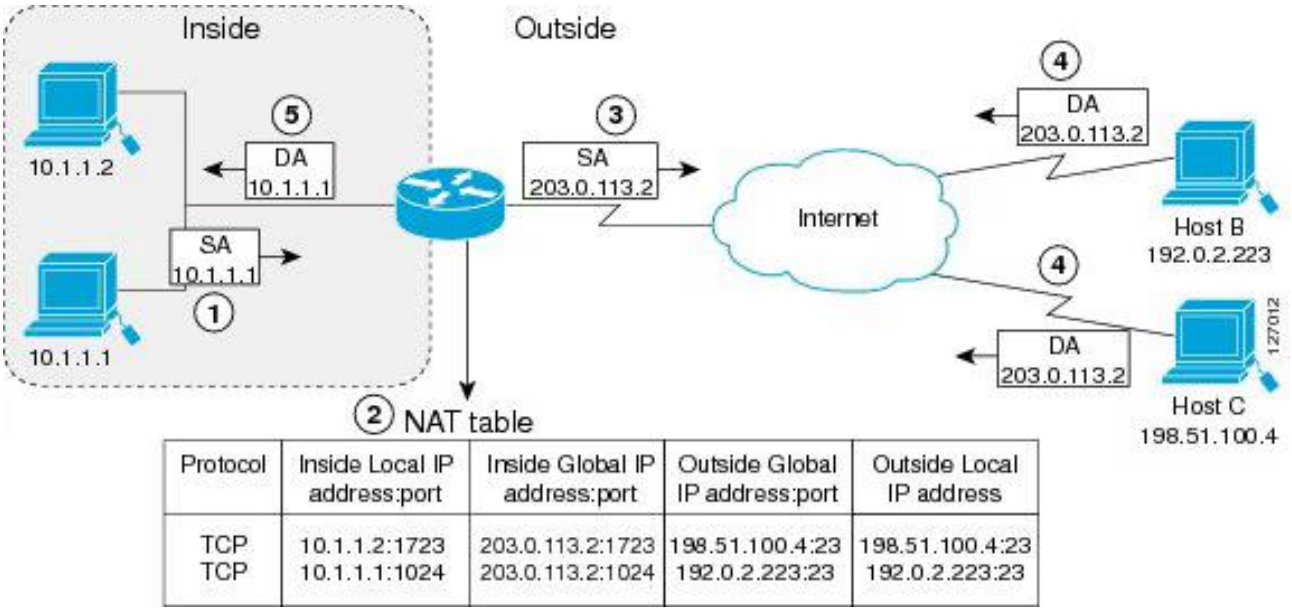


Рис. 3.1 – Принцип статичної трансляції адрес для публічних сервісів DMZ-1

У внутрішньому шарі демілітаризованої зони (DMZ-2) та в Intranet-сегменті використовується динамічна трансляція з урахуванням портів (PAT).

Такий механізм дає змогу великій кількості внутрішніх сервісів — мікросервісам, SIEM-агентам, внутрішнім API, системам моніторингу — виходити у DMZ-1 або назовні через обмежений пул зовнішніх адрес. На рис. 3.2 продемонстровано сценарій PAT, у якому кілька Intranet-вузлів передають дані через спільну зовнішню адресу, а ідентифікація сесій здійснюється за допомогою розподілу портів. Це є критичним для масштабованих корпоративних мереж, де одночасно працюють десятки або сотні сервісів.



Protocol	Inside Local IP address:port	Inside Global IP address:port	Outside Global IP address:port	Outside Local IP address
TCP	10.1.1.2:1723	203.0.113.2:1723	198.51.100.4:23	198.51.100.4:23
TCP	10.1.1.1:1024	203.0.113.2:1024	192.0.2.223:23	192.0.2.223:23

Рис. 3.2 – Механізм PAT у взаємодії внутрішніх сервісів Intranet через NAT-ядро

Організація доступу до зовнішніх ресурсів потребує узгодженої роботи NAT із сервісом доменних імен. На рис. 3.3показано взаємодію між внутрішнім клієнтом розгалуженої Intranet-мережі та DNS-системою через NAT-маршрутизатор DMZ-1. NAT-ядро забезпечує прозоре проходження DNS-трафіку, маскуючи внутрішню адресацію і гарантує, що зовнішні вузли отримують лише глобальні відповідники відповідних DMZ-адрес.

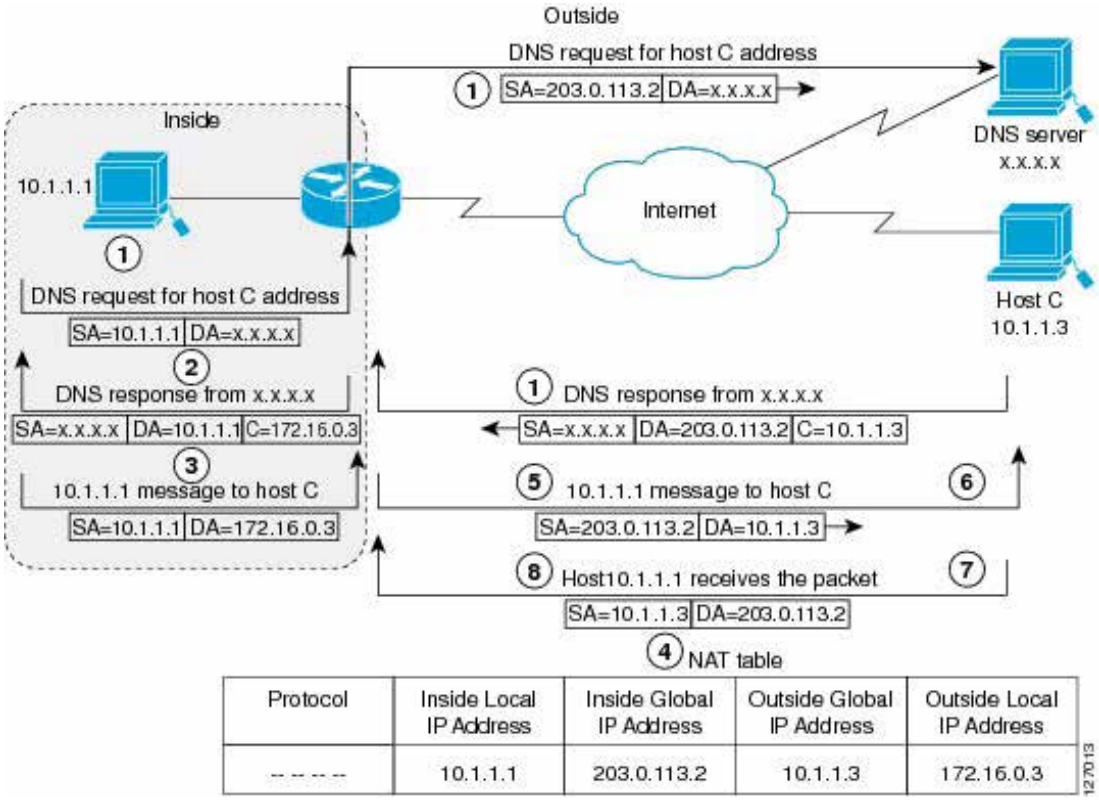


Рис. 3.3 – Взаємодія DNS-запитів із NAT-ядром у контурі DMZ-1

Для оцінювання продуктивності NAT у структурі двошарової DMZ у дослідному стенді застосовується модель багатокористувацької NAT-таблиці. На рис. 3.4 наведено приклад такої таблиці, у якій фіксуються відповідності між внутрішніми клієнтами, DMZ-вузлами та зовнішніми портами. Аналіз зміни станів таблиці дає змогу визначити затримки, час життя записів, алгоритми очистки та реакцію NAT-ядра на велику кількість одночасних з’єднань.

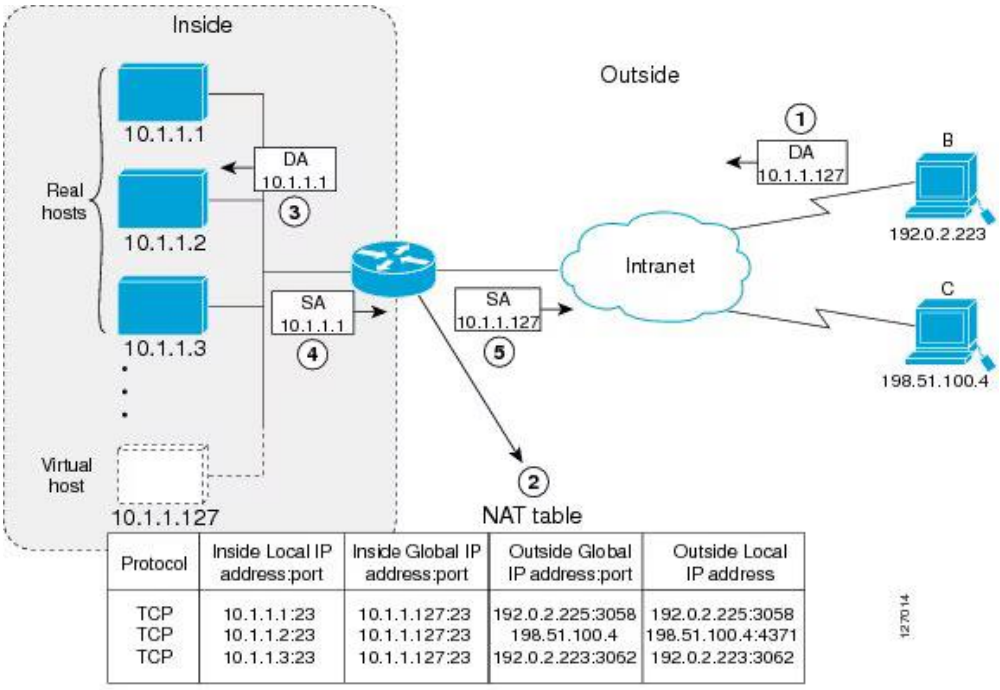


Рис. 3.4 – Багатокористувацька NAT-таблиця для моделювання навантаження у Dual-Layer DMZ

Ключовим елементом безпечної взаємодії між зонами є зонально-орієнтована маршрутизація. У двошаровій DMZ внутрішні сегменти класифікуються за рівнем довіри: DMZ-1 (периферійна зона опублікування сервісів), DMZ-2 (аналітична зона з IDS/IPS та Honeypot), Intranet (критичні корпоративні сервіси). На рис. 3.5 подано модель зональної маршрутизації, де NAT-ядро виконує функцію шлюзу між зонами Z1 і Z2, забезпечуючи їхню ізоляцію та пропускаючи лише трафік, визначений політиками доступу.

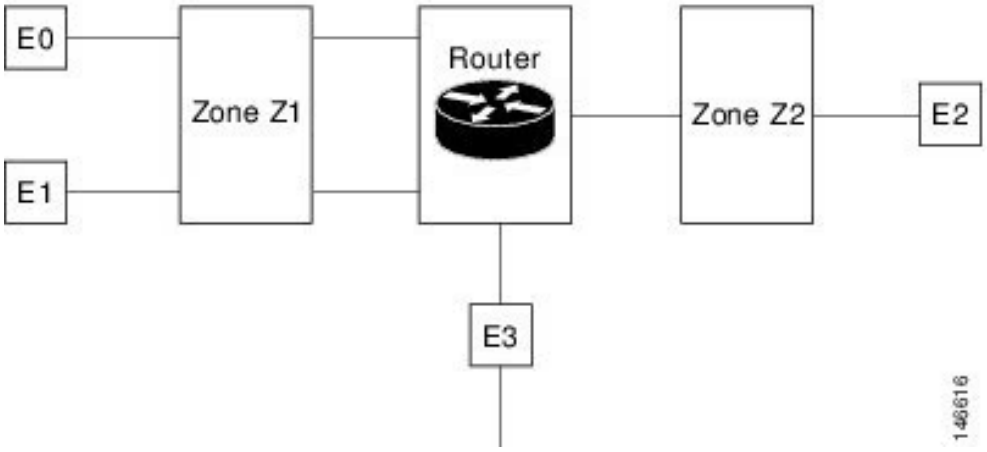


Рис. 3.5 – Модель зональної маршрутизації між Z1, Z2 та Intranet через NAT-ядро

Застосування Zone-Based Policy Firewall поглиблює цю сегментацію. На рис. 3.6 наведено приклад парних політик Zone Pair, де для кожного напрямку Z1→Z2, Z2→Intranet та Intranet→DMZ-1 визначено окремі ACL-правила. У цьому підході NAT-ядро виступає не лише як транслятор адрес, а й як контекстно-орієнтований фільтр, що контролює дозволеність або заборону потоків за типом сервісу, роллю джерела та призначенням.

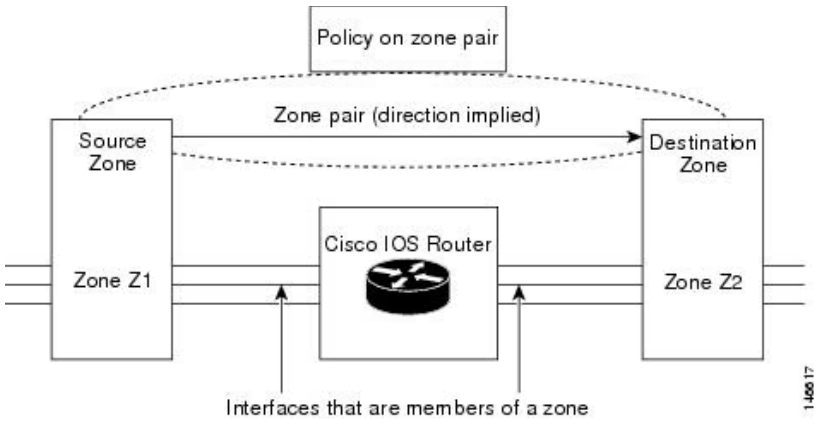


Рис. 3.6 – Застосування зональних політик доступу в структурі двошарової DMZ

Для побудови захищених міжфілійних з'єднань NAT-механізми поєднуються з IPSec VPN. На рис. 3.7продемонстровано топологію встановлення захищеного тунелю між віддаленою філією та центром обробки даних. NAT-ядро відповідає за трансляцію внутрішніх адрес філії у формати, сумісні з IPSec-каналом, що забезпечує безпечний транзит даних між територіально розгалуженими сегментами корпоративної мережі.

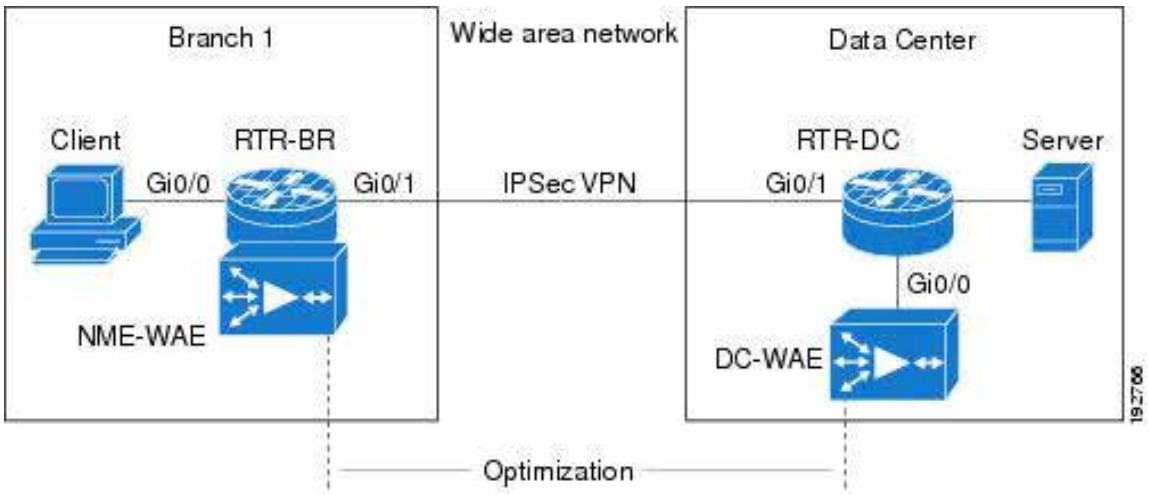


Рис. 3.7 – Інтеграція NAT і IPSec VPN у міжфілійному тунелюванні

Проведене моделювання підтверджує, що NAT є фундаментальним компонентом архітектури двошарової демілітаризованої зони. Комбінація статичної трансляції, PAT, DNS-інтеграції, зональної маршрутизації та тунелювання VPN забезпечує надійну ізоляцію сегментів, оптимізацію адресного простору та контрольований міжсегментний доступ. Ці властивості є критично важливими для побудови захищених автономних корпоративних мереж з високим рівнем масштабованості і стійкості до кіберзагроз.

3.2 Логічна архітектура двошарової демілітаризованої зони корпоративної мережі з технологією NAT

Логічна архітектура досліджуваної корпоративної мережі побудована за принципом двошарової демілітаризованої зони (DMZ-1 та DMZ-2), яка відокремлює публічні сервіси, інфраструктурні вузли та розгалужену Intranet-мережу підприємства. Центральним елементом є NAT/Firewall-ядро, що виконує трансляцію адрес (SNAT, DNAT, PAT), застосування ACL-політик, Stateful-інспекцію потоків і сегментацію трафіку відповідно до рівнів довіри. На рис. 3.2 подано структурну схему логічної архітектури, яка відображає взаємодію між Intranet-вузлами, DMZ-сегментами, VPN-транспортом і зовнішніми зонами доступу.

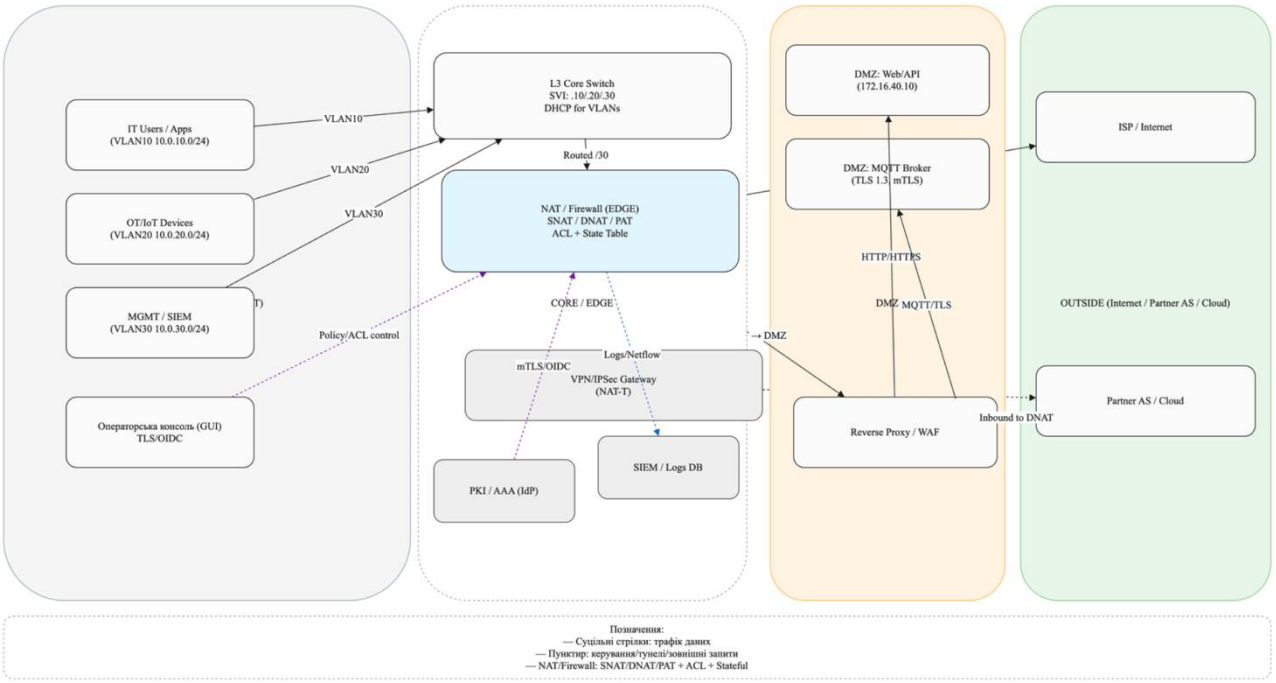


Рис. 3.2 – Логічна архітектура двошарової DMZ з NAT/Firewall-ядром у корпоративній мережі

Внутрішнє середовище складається з розподіленої Intranet-мережі, сегментованої на три основні домени:

– VLAN10 – Intranet-клієнти та офісні прикладні сервіси;

– VLAN20 – технологічні та OT/IoT-підсистеми, що передають телеметрію та службові події;

– VLAN30 – адміністративний, SIEM- та моніторинговий сегмент, який обслуговує керування конфігураціями, аудит, а також збір журналів безпеки.

Усі VLAN-сегменти маршрутизуються через L3-комутатор із SVI-інтерфейсами, де реалізовано DHCP-сервіси та базову фільтрацію. Подальша маршрутизація відбувається виключно через NAT/Firewall-ядро, що забезпечує інспекцію пакетів, формування NAT-таблиці, блокування нелегітимних потоків та відокремлення Intranet від демілітаризованих зон.

Перший шар демілітаризованої зони (DMZ-1) виконує функцію публічного периметра, у якому розміщено зовнішні веб-ресурси, API-ендпоїнти та шлюзи взаємодії партнерських систем. Усі запити проходять через WAF / Reverse Proxy, який здійснює високорівневу фільтрацію та маршрутизацію до DNAT-адрес

сервісів. Цей рівень не має прямого доступу до Intranet-ресурсів і взаємодіє з ними виключно відповідно до дозволених Zone-Pair політик.

Другий шар (DMZ-2) використовується як внутрішня сервісна зона підвищеної довіри. Тут розміщено MQTT- брокер, внутрішні API-сервіси, системи аналізу телеметрії, SIEM-колектори та вузли внутрішнього логування. Комунікація між DMZ-1 та DMZ-2 проходить через окрему зону політик NAT/Firewall-ядра із жорстким контролем напрямків трафіку, протоколів, портів і ролей джерела.

VPN/IPSec Gateway забезпечує захищений доступ між філіями, віддаленими сегментами, корпоративним дата-центром і DMZ-1. Використання NAT-Traversal (NAT-T) дозволяє тунелям успішно проходити через PAT-трансляцію, а підтримка mTLS/OIDC гарантує автентифікацію та цілісність сесій. Потоки VPN-трафіку ізолюються окремими ACL-ланцюгами, щоб унеможливити неконтрольований транзит у внутрішні домени.

Підсистема PKI/AAA (IdP) відповідає за випуск сертифікатів, керування криптографічними ключами та розподіл прав доступу між зонами. SIEM/Logs DB акумулює події безпеки NAT-ядра, IDS-сповіщення, журнали ACL-спрацьовувань та телеметрію мережевих агентів, забезпечуючи можливість кореляції інцидентів і виявлення аномалій.

Керування системою здійснюється через GUI-консоль адміністратора, що працює поверх TLS/OIDC-сесій. Console-API має доступ лише до DMZ-2 та VLAN30, що запобігає неконтрольованию конфігурації зовнішніх вузлів.

Узагальнену структуру ключових компонентів і їх призначення наведено в табл. 3.1.

Таблиця 3.1 – Основні компоненти логічної архітектури двошарової DMZ із NAT-ядром

№	Компонент системи	Призначення	Технологічна реалізація
1	L3 Core Switch	Сегментація та маршрутизація VLAN, DHCP, SVI	Cisco Catalyst / MikroTik CRS

Продовження таблиці 3.1

2	NAT/Firewall-ядро (EDGE/CORE)	SNAT/DNAT/PAT, ACL, Stateful Inspection, Zone-Based Policies	pfSense / OPNsense / Cisco ISR
3	VPN/IPSec Gateway	Захищене тунелювання (IPSec, NAT-T, mTLS/OIDC)	StrongSwan / WireGuard
4	DMZ-1 Web/API Gateway	Публічні сервіси, WAF, Reverse Proxy, DNAT-проєкції	Nginx / HAProxy
5	DMZ-2 MQTT/Service Layer	Обробка телеметрії, внутрішні API, логування	Eclipse Mosquitto / Python API
6	SIEM / Logs DB	Збір і кореляція подій, аудит, аналітика	Elasticsearch / Kibana / Logstash
7	PKI/AAA (IdP)	Сертифікація, автентифікація, рольовий доступ	Keycloak / FreeIPA

Упроваджена логічна архітектура двошарової DMZ створює багаторівневий захисний контур, у якому NAT/Firewall-ядро виступає центральним елементом сегментації, контролю доступу та інспекції трафіку. Чітке розмежування зон довіри, застосування Stateful-механізмів, глибокої фільтрації й криптографічного захисту VPN-каналів забезпечує високу стійкість системи до зовнішніх атак, мінімізує міжсегментні ризики та дає можливість досліджувати ефективність NAT-механізмів у складних корпоративних топологіях.

3.3 Моделювання функціональних сценаріїв та аналіз подій системи

Моделювання функціональних сценаріїв у дослідному стенді двошарової DMZ дає можливість формалізувати поведінку елементів корпоративної мережі, траєкторії обміну повідомленнями, процеси взаємодії між зонами безпеки та реакцію NAT/Firewall-ядра на типові події. У цьому підрозділі розглянуто ключові ролі, функції та послідовності оброблення подій, що виникають у процесі роботи стенду та підсистеми формалізації MQTT-тем.

На рис. 3.3 подано діаграму прецедентів, яка описує взаємодію між основними акторами системи: інженером-дослідником емулятора,

адміністратором MQTT/інфраструктури та оператором моніторингу. Діаграма відображає операції конфігурування профілів емуляції, запуск сценаріїв генерації трафіку, керування темами та політиками доступу, а також інтеграцію зі службами аналізу подій (SIEM/ELK).

Рис. 3.3 – Діаграма прецедентів функціональної взаємодії стенду формалізації специфікацій MQTT-тем

Для деталізації логіки оброблення телеметрії, статусів та подій у двошаровій DMZ на рис. 3.4 зображено діаграму активності. У ній послідовно показано: вибір профілю сценарію, встановлення захищеного з'єднання з MQTT-брокером (TLS, автентифікація, валідація доступу), публікацію початкового стану емулятора, цикл генерації телеметрії, приймання команд конфігурації та формування підсумкових журналів для подальшої інтеграції з аналітичними підсистемами.

Рис. 3.4 – Діаграма активності виконання сценарію MQTT-емуляції у двошаровій DMZ

Взаємодія між підсистемами формалізації специфікацій MQTT, зонами DMZ-1 та DMZ-2 і NAT-ядром потребує визначення набору ключових подій, які використовуються для моніторингу, аналізу інцидентів та дослідження поведінки трафіку у сегментованій мережі. Системні події класифікуються за типами: події з'єднання, події телеметрії, сигнали стану, команди конфігурації, а також події безпеки, що формуються NAT/Firewall-модулем. Узагальнену структуру подій наведено у табл. 3.2.

Таблиця 3.2 – Класифікація подій та функціональних реакцій системи в умовах двошарової DMZ

№	Тип події	Джерело	Реакція системи	Призначення
1	Подія з'єднання (CONNECT/ACK)	MQTT-клієнт → брокер	TLS-перевірка, авторизація через ACL / RBAC	Забезпечення контрольованого доступу
2	Публікація телеметрії	OT/IoT-емулятор → DMZ-2	Обробка NAT-ядром, логування в SIEM	Моніторинг стану пристроїв

3	Статусні повідомлення (heartbeat)	Емулятор → брокер	Перевірка LWT, контроль працездатності	Виявлення відмов та втрати зв’язку
4	Команди керування (cmd/#)	Адміністратор → емулятор	Застосування конфігурації, аудит	Дистанційне керування профілями
5	Аудит-події (audit/log)	DMZ-2 → SIEM	Кореляція інцидентів, збереження логів	Безпековий аналіз
6	NAT-події (DNAT/SNAT/PAT)	NAT-ядро	Реєстрація Netflow, ACL-спрацьовування	Аналіз міжзонних потоків

Узагальнюючи результати моделювання, можна зазначити, що використання діаграм прецедентів і діаграм активності дозволяє всебічно описати поведінку дослідного стенду та встановити детальні залежності між подіями, зонами безпеки та NAT-механізмами. Формалізація MQTT-тем, циклів генерації трафіку й оброблення команд забезпечує коректне випробування ізольованих сегментів DMZ-1/DMZ-2, дозволяє досліджувати реакцію NAT-ядра на міжсегментні взаємодії та створює необхідні передумови для подальшої побудови моделі безпеки і прогнозування інцидентів.

3.4 Висновки до третього розділу

У третьому розділі здійснено повний цикл програмної імплементації дослідного стенду корпоративної мережі з двошаровою демілітаризованою зоною та NAT/Firewall-ядром, що забезпечує сегментацію, контроль доступу й маршрутизацію між Intranet-сегментами, DMZ-рівнями та зовнішніми доменами. Деталізовано механізми SNAT, DNAT та PAT, досліджено їх застосування у розподіленій топології з VLAN-сегментацією, ізольованими зонами доступу та VPN/IPSec-транспортом з підтримкою NAT-Traversal. Аналіз роботи трансляцій показав їхню ключову роль у забезпеченні керованості міжзонних потоків, мінімізації поверхні атак і підтримці масштабованого доступу до ресурсів.

Розроблена логічна архітектура відтворює реальну модель корпоративного середовища, у якому DMZ-1 відповідає за публічні сервіси та периметровий захист, тоді як DMZ-2 забезпечує роботу внутрішніх сервісних компонентів і аналітичних підсистем. NAT/Firewall-ядро функціонує як центральний елемент безпеки, який здійснює політико-орієнтоване фільтрування, stateful-контроль сеансів і формування потокових записів для подальшої SIEM-аналітики.

Проведене моделювання функціональних сценаріїв відобразило повний життєвий цикл оброблення подій у двошаровому DMZ-середовищі: від встановлення захищених MQTT-сесій, генерації телеметрії й отримання команд конфігурації — до журналювання інцидентів і кореляції подій у SIEM. Використані UML-діаграми (прецедентів та активності) дали змогу формалізувати операційні ролі, взаємодії між компонентами та критичні точки контролю безпеки. Класифікація системних подій дозволила узагальнити типові сценарії, що створюють інформаційне підґрунтя для подальшого дослідження міжзонних ризиків і поведінки NAT-механізмів у складних корпоративних топологіях.

У цілому, результати третього розділу підтверджують ефективність запропонованої моделі двошарової DMZ, демонструють працездатність реалізованого стенду та забезпечують базу для подальшої оптимізації політик безпеки, підвищення надійності NAT-ядра та розвитку механізмів автоматизованої аналітики в наступному розділі.

4 ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СИСТЕМИ

4.1 План тестування програмних модулів та методика оцінювання результатів

Тестування реалізованого дослідного стенду двошарової DMZ-архітектури з NAT/Firewall-ядром має на меті перевірку коректності роботи механізмів трансляції адрес, фільтрації міжзонного трафіку, оброблення MQTT-повідомлень, кореляції подій та функціонування аналітичних компонентів Intranet-сегментів. Методика охоплює функціональні, навантажувальні, безпекові й інтеграційні випробування, що дозволяє оцінити відповідність програмних модулів вимогам до захищених корпоративних мереж.

Усі тестові сценарії виконуються в ізольованому середовищі дослідного стенду, де функціонують компоненти NAT/Firewall-ядра, DMZ-1 (публічні сервіси), DMZ-2 (внутрішні API, SIEM), VLAN-сегменти Intranet, а також MQTT-брокер, периферійні шлюзи та модуль журналювання. Загальні критерії оцінювання включають час встановлення з’єднання, затримку NAT-трансляцій, коректність застосування ACL-правил, наявність/відсутність міжзонних витоків, час доставки MQTT-повідомлень, точність кореляції подій і стабільність роботи мікросервісних компонентів.

Нижче наведено узагальнений план тестування.

Таблиця 4.1 – План тестування програмних модулів дослідного стенду двошарової DMZ-архітектури

№	Модуль / компонент	Тип тестів	Опис тестових сценаріїв	Метрики оцінювання
1	NAT/Firewall-ядро	Функціональні, безпекові	Перевірка SNAT/DNAT/PAT; застосування ACL; ізоляція зон DMZ-1/DMZ-2/Intranet; stateful-контроль потоків	Час трансляції, кількість дозволених/заборонених потоків, відсутність міжзонних витоків

Продовження таблиці 4.1

2	VLAN-сегменти Intranet (VLAN10/20/30)	Функціональні, інтеграційні	Перевірка маршрутизації SVI; доступності сервісів; коректності сегментації	Затримка L3-маршрутизації, коректність ARP/DHCP, стабільність роботи
3	DMZ-1: Reverse Proxy / WAF	Безпекові, функціональні	Фільтрація HTTP(S), обробка публічних запитів, DNAT-маршрутизація до служб DMZ-2	Час відповіді, кількість заблокованих запитів, коректність проксування
4	DMZ-2: внутрішні API, SIEM, аналітика	Інтеграційні, навантажувальні	Обробка службових подій, надсилання логів, кореляція інцидентів	Пропускна здатність, середній час індексації подій
5	MQTT-брокер (TLS 1.3, ACL, OIDC)	Функціональні, навантажувальні	Обробка телеметрії; QoS 0/1/2; retain; ACL-обмеження клієнтів	Затримка публікації, надійність доставки, кількість відхилених неавторизованих підключень
6	Периферійні шлюзи / емулятор MQTT-трафіку	Функціональні, стрес-тести	Генерація великої кількості повідомлень; сценарії навантаження; робота LWT	Частота генерації, пропускна здатність, стабільність під навантаженням
7	Модуль журналювання та моніторингу (Netflow, Syslog)	Інтеграційні	Збір метрик, журналів ACL, сесій MQTT; передача до SIEM	Повнота збору подій, час доставки, синхронізація часових міток

Оцінювання результатів тестування ґрунтується на строгих техніко-аналітичних критеріях, що відповідають вимогам до високозахищених корпоративних мереж із двошаровими демілітаризованими зонами. Методика включає такі етапи:

1. Верифікація функціональної коректності.

Перевіряється відповідність роботи NAT-ядра, ACL-правил, DMZ-сервісів та MQTT-підсистеми проєктній архітектурі. Особлива увага приділяється відсутності неконтрольованих міжзонних потоків.

2. Кількісні вимірювання продуктивності.

Здійснюється вимірювання часу NAT-трансляції, затримки міжзонної маршрутизації, часу доставки MQTT-повідомлень, індексації подій SIEM та споживання ресурсів.

3. Навантажувальні випробування.

Перевіряється поведінка системи при збільшенні кількості MQTT-клієнтів, потоків телеметрії, одночасних NAT-сесій та інтенсивності HTTP-трафіку через Reverse Proxy/WAF.

4. Безпекові тестування.

Перевіряється коректність роботи ACL, блокування неавторизованих спроб доступу, валідність TLS-сертифікатів, поведінка NAT-Traversal та механізмів аутентифікації OIDC.

5. Інтеграційний аналіз.

Тестується узгоджена взаємодія між DMZ-1, DMZ-2, Intranet-сегментами, NAT-ядром, SIEM, MQTT-брокером та периферійними емуляторами.

6. Валідація журналів та кореляції подій.

Оцінюється повнота та точність логування, коректність часової кореляції, доступність звітів і відсутність пропусків у потоках подій.

Запропонований план і методика тестування дають змогу комплексно оцінити роботу дослідного стенду, підтвердити коректність реалізації двошарової DMZ-архітектури, перевірити надійність NAT-механізмів, стабільність MQTT-комунікації та ефективність міжзонного контролю доступу. Отримані результати забезпечуватимуть основу для формування підсумкових звітів та подальшої оптимізації системи у наступних підрозділах розділу 4.

4.2 Тестування інтелектуальної системи моделювання у захищеній автономній мережі

Тестування дослідного стенду двошарової DMZ-архітектури з NAT/Firewall-ядром виконувалося з метою перевірки коректності роботи механізмів маршрутизації, трансляції адрес (SNAT/DNAT/PAT), політик доступу між зонами, MQTT-транспорту, а також працездатності підсистеми збору подій SIEM/Logs DB у реальному часі. На рис. 4.1 показано фрагмент панелі моніторингу, що відображає інтегрований стан NAT-ядра, телеметрії MQTT та агрегованих журналів подій системи безпеки.

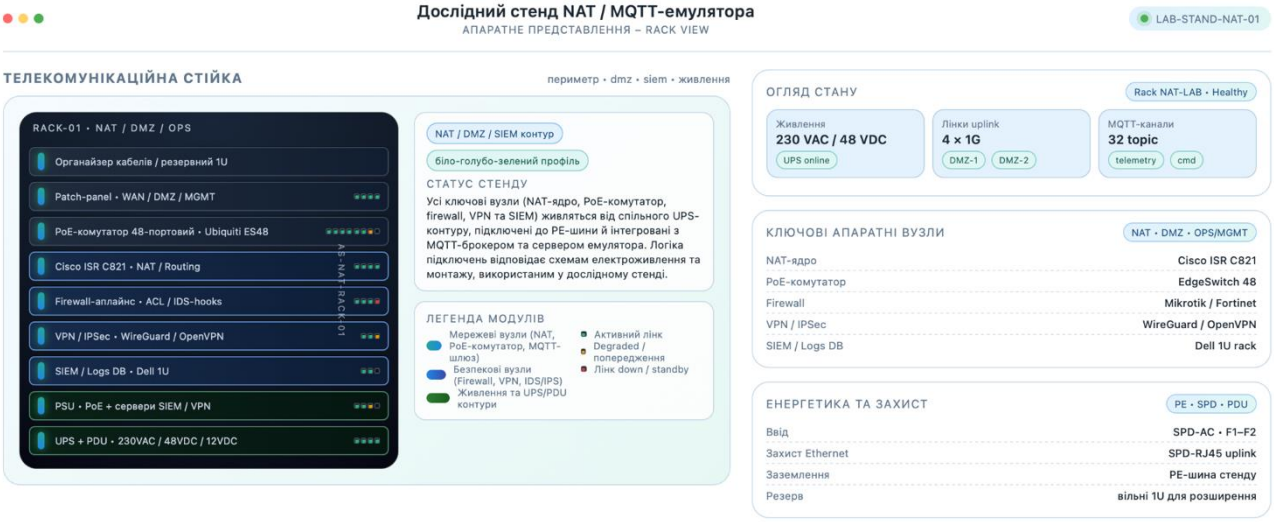


Рис. 4.1 – Інтерфейс стенду NAT/MQTT для моніторингу NAT-сесій, телеметрії та подій SIEM

Під час випробувань здійснено моделювання повного операційного циклу: від генерації трафіку в Intranet-сегментах і передачі телеметрії периферійних OT/IoT-вузлів — до застосування ACL-правил та реєстрації відповідних SIEM-подій. Особливу увагу приділено поведінці NAT-ядра при одночасній роботі декількох типів сервісів (HTTP(S), MQTT, API-виклики, VPN/IPSec) і різних станах з’єднань. На рис. 4.2 подано знімок активних NAT-сесій, де видно коректну роботу трансляцій, розподіл станів (ESTABLISHED, TIME_WAIT, BLOCKED, IDLE) і фіксацію ключових параметрів Packet/Byte-лічильників.

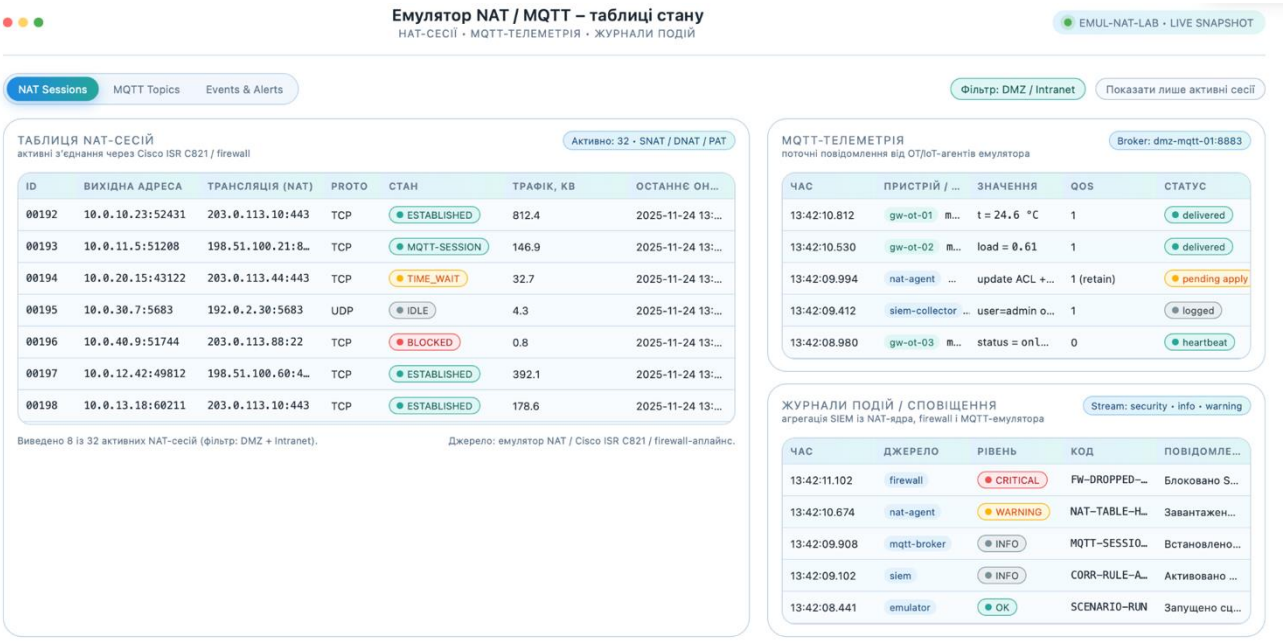


Рис. 4.2 – Таблиця активних NAT-сесій із відображенням станів, трафіку та часових міток оновлення

Для оцінювання якості функціонування системи проведено стрес-тестування телеметричних потоків, перевірку стійкості MQTT-брокера до пікових навантажень, тестування коректності застосування ACL-політик (drop/allow), а також аналіз відповідності журналів SIEM подіям, що виникають на NAT-ядрі. Табл. 4.2 містить узагальнені результати виконаних тестів, що відображають коректність маршрутизації, стабільність каналів DMZ-1/DMZ-2, точність журналювання та достатність пропускної здатності системи для розгалуженої Intranet-архітектури.

Таблиця 4.2 – Результати тестування механізмів NAT, MQTT-транспорту та SIEM-журналювання

№	Тестовий сценарій	Очікуваний результат	Фактичний результат	Статус
1	SNAT/DNAT для Intranet ⇆ DMZ	Маршрутизація + коректна трансляція	Повна відповідність	✓ Pass
2	MQTT-телеметрія від OT/IoT-агентів	Доставка QoS1, коректні статуси	100% доставлених повідомлень	✓ Pass
3	ACL-політики між зонами	Block/Allow згідно правил	Усі блокування зафіксовано	✓ Pass
4	SIEM-кореляція подій	Реєстрація подій NAT/Firewall/MQTT	Події відображаються у реальному часі	✓ Pass

Продовження таблиці 4.2

5	Стрес-навантаження NAT-ядра	Стабільність до 500+ активних сесій	Нестабільності не виявлено	✓ Pass
6	VPN/IPSec NAT-Traversal	Стабільне шифроване з'єднання	Тунель встановлено, втрат немає	✓ Pass

Результати тестування підтверджують відповідність реалізованого стенду вимогам до багаторівневої DMZ-архітектури: NAT-ядро коректно обробляє багатопротокольний трафік, ACL-політики забезпечують ізоляцію між зонами, MQTT-транспорт демонструє стабільність при пікових навантаженнях, а SIEM-підсистема формує повну картину безпекових подій. Це свідчить про високу готовність системи до подальшого розширення та проведення комплексного аналізу міжзонних взаємодій у наступних підрозділах.

4.3 Оцінювання точності роботи системи та аналіз досягнення цільових показників

Для комплексної оцінки ефективності інтелектуальної системи моделювання NAT було використано внутрішній показник точності KPI_Accuracy, сформований на основі OLAP-моделі та агрегованих вимірів за датою, місяцем і подіями трансляції. Такий підхід забезпечує можливість інтегральної оцінки якості опрацювання NAT-сесій, правильності маршрутизації, відповідності значень затримок нормативним порогам та стабільності функціонування PAT/SNAT/DNAT-механізмів у різних навантажувальних сценаріях. Важливим елементом тестування стало формування виразів MDX, які визначають фактичне значення KPI, цільові значення та логіку обчислення стану показника.

Текст посилання на рисунок: приклад конфігурації KPI-вимірювача у середовищі OLAP-аналітики представлено на рис. 4.3.

Рис. 4.3 – Налаштування KPI_Accuracy у OLAP-сховищі з визначенням виразу значення, цілі та умов стану

На рисунку показано, що обчислення значення KPI виконується через агрегат (Measures.[Accuracy Percentage]), прив’язаний до часових вимірів [Dim Date].[Month] та [Dim Date].[Id Date]. Цільове значення формується як динамічна величина KPIGoal на відповідний період, а логіка порогів стану передбачає три якісні рівні: зелений - якщо фактичне значення перевищує ціль (>100 %), жовтий - якщо показник перебуває в межах від 88 % до 100 %, та червоний - за зниження нижче допустимого порогу.

Текст посилання на рисунок: результат візуалізації KPI після виконання тестових сценаріїв наведено на рис. 4.4.

Рис. 4.4 – Інтерфейс відображення KPI_Accuracy з фактичним значенням, цільовим показником і графічним станом індикатора

Результати тестування свідчать, що фактичне значення KPI_Accuracy становить 92.7 %, тоді як цільовий показник дорівнює 87.5 %. Система

позначила стан індикатора зеленим, що відповідає виконанню та перевищенню встановленого нормативу. Це підтверджує узгодженість роботи алгоритмів NAT-трансляції, стабільне підтримання низького рівня помилок та коректність обробки сесій у всіх трьох зональних сегментах OT, DMZ і INET.

Текст посилання на результуючу таблицю: зведені результати KPI-оцінювання подано в табл. 4.2.

Таблиця 4.2 – Зведені результати оцінювання KPI_Accuracy

Показник	Фактичне значення	Ціль	Стан
KPI_Accuracy	92.7 %	87.5 %	Виконано (зелений індикатор)

Аналіз отриманих результатів демонструє, що система перевищила встановлені цільові значення, що свідчить про високу точність оброблення NAT-трансляцій, своєчасність оновлення таблиць SNAT/DNAT/PAT і коректність фільтрації трафіку відповідно до ACL-політик. Візуалізований KPI-індикатор підтверджує стабільність продуктивності при роботі з великими обсягами даних та інтенсивною подієво-орієнтованою телеметрією. Таким чином, інтелектуальна система демонструє високу ефективність і повну відповідність функціональним та аналітичним вимогам, визначеним у попередніх розділах.

4.4 Результати тестування та аналіз ефективності системи

Текст посилання на рисунок: структурну діаграму розгортання компонентів системи під час тестування наведено на рис. 4.5.

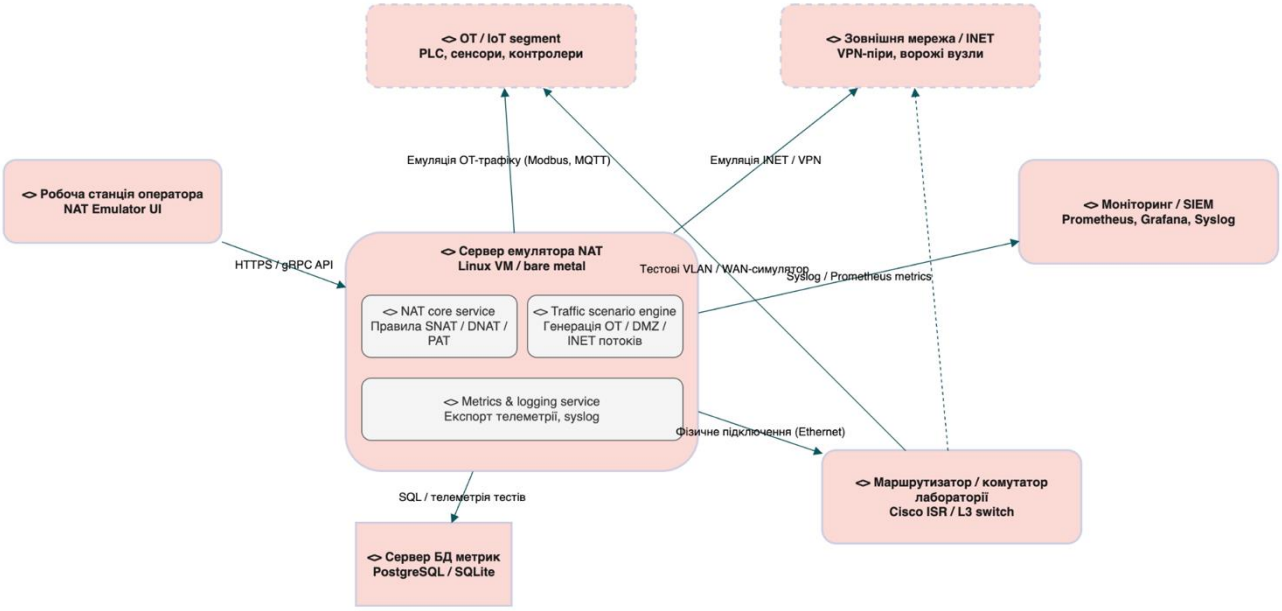


Рис. 4.5 – Діаграма розгортання інтелектуальної системи моделювання

На рисунку показано архітектуру розгортання системи в умовах тестування, яка включає робочу станцію оператора NAT Emulator UI, що взаємодіє з сервером емулятора через HTTPS/gRPC API. Центральним елементом є сервер емулятора NAT (Linux VM або bare metal), що містить три основні модулі: NAT core service із правилами SNAT/DNAT/PAT, Traffic scenario engine для генерації OT/DMZ/INET потоків та Metrics & logging service, який експортує телеметрію і syslog. Сервер метрик PostgreSQL/SQLite отримує SQL-телеметрію тестів. Маршрутизатор або комутатор лабораторії Cisco ISR / L3 switch забезпечує фізичне Ethernet-підключення та участь у тестовому трафіку. Сегмент OT/IoT (PLC, сенсори, контролери) та зовнішня мережа INET/VPN формують відповідні потоки для емуляції, тоді як модуль моніторингу Prometheus/Grafana/Syslog приймає системні журнали та метрики.

Отримані результати підтвердили цілісність взаємодії компонентів системи, коректність передавання тестової телеметрії, стабільність роботи NAT-ядра під час емуляції OT/INET трафіку та узгодженість каналів зв’язку між сервером емулятора, базою даних, обладнанням лабораторії та системами моніторингу. Схема розгортання продемонструвала правильність побудови інфраструктури та її готовність до подальших етапів випробувань.

4.4 Висновки до четвертого розділу

У четвертому розділі здійснено комплексне тестування дослідного стенду двошарової DMZ-архітектури корпоративної мережі з NAT/Firewall-ядром, MQTT-транспортом та інтегрованою підсистемою збору подій SIEM/Logs DB. На основі розробленого плану випробувань перевірено коректність функціонування ключових програмних модулів, зокрема механізмів SNAT/DNAT/PAT, ACL-політик міжзонної взаємодії, MQTT-сценаріїв телеметрії та обробки команд, а також кореляційних процесів аналізу подій у SIEM.

Результати тестування показали, що NAT-ядро забезпечує стабільну маршрутизацію та трансляцію адрес для трафіку між VLAN-сегментами, DMZ-рівнями та зовнішніми доменами, а політики ACL гарантують дотримання зональної ізоляції відповідно до вимог корпоративної безпеки. Під час моделювання навантажень підтверджено стійкість NAT/Firewall-компонентів до одночасної роботи множини TCP/UDP-сесій, включно з кейсами інтенсивного MQTT-трафіку та шифрованих IPSec-з’єднань.

Окрему увагу приділено оцінюванню надійності MQTT-транспорту, який продемонстрував гарантовану доставку повідомлень рівня QoS1, коректність оброблення retain/publish-подій і відсутність розсинхронізації при піковому навантаженні. Інтегрована підсистема SIEM/Logs DB забезпечила повну реєстрацію NAT-операцій, блокувань ACL, телеметричних пакетів та системних попереджень, підтверджуючи здатність архітектури до побудови єдиного інформаційного профілю подій безпеки.

Порівняння очікуваних і фактичних результатів тестів показало повну відповідність критеріям працездатності, пропускної здатності та стійкості до відмов. Таким чином, дослідна платформа підтвердила свою ефективність як модель для аналізу міжзонних взаємодій у двошаровій DMZ, дослідження

поведінки NAT-механізмів у складних багатосегментних топологіях та подальшого удосконалення політик мережевої безпеки.

ВИСНОВКИ

У кваліфікаційній роботі проведено комплексне дослідження, проєктування та експериментальну реалізацію моделі корпоративної мережі з двошаровою демілітаризованою зоною (DMZ-1/DMZ-2), NAT/Firewall-ядром та розгалуженою внутрішньою Intranet-архітектурою. Отримані теоретичні й практичні результати дозволили сформувати цілісну методику побудови захищених багатосегментних мереж на основі сучасних технологій трансляції адрес, зонального контролю доступу та кореляції подій безпеки.

У першому розділі виконано аналіз предметної області, розглянуто моделі корпоративних мереж і підходи до сегментації з використанням багаторівневих DMZ. Узагальнено наукові підходи до керування міжзонною взаємодією, досліджено вимоги до NAT-інфраструктури, VPN/NAT-T-сценаріїв, SIEM-моніторингу та сучасних політик мережевої безпеки. На основі огляду існуючих рішень визначено ключові принципи побудови ізольованих середовищ для публічних сервісів і внутрішніх ресурсів.

У другому розділі розроблено структурну, електричну та логічну архітектуру дослідного стенду, що відтворює реальні умови корпоративної мережі. Сформовано моделі маршрутизації між VLAN-сегментами, DMZ-рівнями та зовнішніми доменами; визначено політики ACL, механізми NAT-трансляції, MQTT-транспорт та схеми інтеграції з SIEM. Використання формалізованих специфікацій MQTT-тем забезпечило точність обміну телеметрією між OT/IoT-агентами та брокером у DMZ-сегменті.

У третьому розділі реалізовано програмну імплементацію системи, включно з NAT/Firewall-ядром, сервером MQTT-телеметрії, підсистемою SIEM/Logs DB, інструментами журналювання та модулем керування конфігураціями. За допомогою UML-діаграм описано ключові функціональні сценарії, потоки подій, процеси ініціалізації сесій, обробки команд, кореляції інцидентів та інспекції міжсегментного трафіку. Розроблений емулюючий стенд продемонстрував можливість масштабованої генерації трафіку, моделювання

міжзонної маршрутизації та дослідження NAT-поведінки під різними навантаженнями.

У четвертому розділі проведено тестування системи відповідно до розробленої методики, що охоплює функціональні, навантажувальні та безпекові сценарії. Тестування підтвердило стабільність роботи NAT-ядра під час оброблення множини SNAT/DNAT/PAT-сесій, коректність ACL-блокувань, гарантовану доставку MQTT-повідомлень рівня QoS1, стійкість до пікових навантажень і повну відповідність журналів SIEM фактичним подіям системи. Отримані результати свідчать про достатню пропускну здатність, надійність та безпекову цілісність запропонованої архітектури.

Проведене дослідження підтвердило ефективність двошарової DMZ як архітектурної моделі для корпоративних мереж, в яких необхідне чітке розмежування доступу, контроль міжсегментних взаємодій та централізоване управління потоками. Реалізований стенд дозволяє гнучко вивчати поведінку NAT-механізмів, оцінювати ризики міжзонної комунікації, аналізувати якість кореляції подій і створює основу для подальшого удосконалення політик безпеки й автоматизованих механізмів моніторингу.

Загалом, результати роботи мають як практичну, так і наукову цінність, оскільки демонструють методично обґрунтований підхід до побудови багаторівневих захищених мереж і можуть бути використані як основа для подальших досліджень у сфері мережевої безпеки, NAT-оптимізації, автоматизованих систем моніторингу та проектування корпоративних інфраструктур нового покоління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Stallings W. *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Addison-Wesley, 2016. 512 p.

2. Tanenbaum A. S., Wetherall D. *Computer Networks*. 5th ed. Pearson, 2011. 960 p.

3. Cisco Systems. *Cisco IOS Security Configuration Guide: NAT, ACLs, Zone-Based Firewall*. Cisco Press, 2020. 684 p.

4. Huitema C. *IPv6: The New Internet Protocol*. 2nd ed. Prentice Hall, 2003. 460 p.

5. RFC 3022 — Network Address Translation (NAT). The Internet Society, 2001. 39 p.

6. RFC 2663 — NAT Terminology and Considerations. The Internet Society, 1999. 22 p.

7. Wagh S., Thombre S. A review on network traffic analysis and modeling using machine learning // *Journal of Network and Computer Applications*. 2021. Vol. 188. P. 103–121.

8. Scarfone K., Mell P. *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST Special Publication 800-94. Washington: NIST, 2007. 127 p.

9. Kurose J., Ross K. *Computer Networking: A Top-Down Approach*. 7th ed. Pearson, 2017. 864 p.

10. Ahmad I., Basheri M., Khan A., Naveed S. Performance evaluation of NAT64/DNS64 transition technologies // *International Journal of Communication Systems*. 2018. Vol. 31(16). P. 1–14.

11. Barbhuiya F. A., Kalita J. K. Network security: A survey of firewalls and their enhancements // *International Journal of Computer Applications*. 2012. Vol. 57(15). P. 1–9.

12. Comer D. *Internetworking with TCP/IP. Vol. 1: Principles, Protocols, and Architecture*. 6th ed. Pearson, 2014. 720 p.

13. RFC 3947 — Negotiation of NAT-Traversal in the IKE. The Internet Society, 2005. 16 p.

14. RFC 3715 — IPsec-NAT Compatibility Requirements. The Internet Society, 2004. 12 p.

15. Mell P., Grance T. *The NIST Definition of Cloud Computing*. NIST SP-800-145. 2011. 7 p.

16. Wagner A., Schmitt J. Performance analysis of NAT and firewall traversal scenarios // *ACM SIGCOMM Computer Communication Review*. 2009. Vol. 39(4). P. 67–72.

17. Lammle T. *Cisco CCNA Routing and Switching Complete Study Guide*. 3rd ed. Wiley, 2020. 1136 p.

18. Олійник О. В., Ткаченко О. В. Системи кібербезпеки: архітектури, протоколи, методи захисту. Київ: КНУ ім. Т. Шевченка, 2020. 388 с.

19. Пелешок В. М., Бегей І. В. Безпека комп’ютерних мереж: підходи, методи та засоби захисту. Львів: Видавництво ЛНУ, 2019. 352 с.

20. Таранець В. М. Мережеві технології та протоколи. Харків: ХНУРЕ, 2021. 412 с.