ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«ВПРОВАДЖЕННЯ СУЧАСНОГО NGFW ТА СИСТЕМИ МОНІТОРИНГУ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ»**

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
(шифр і назва спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)

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

_____ Сергій ЯКИМЧУК
(підпис) Ім'я, ПРІЗВИЩЕ здобувача

Виконав: здобувач вищої освіти гр. ТСДМ-62
Сергій ЯКИМЧУК
Ім'я, ПРІЗВИЩЕ
Керівник: д.т.н., доцент Ганна ГРИНКЕВИЧ
Ім'я, ПРІЗВИЩЕ
Науковий ступень, вчене звання
Резензент: _____
Ім'я, ПРІЗВИЩЕ
Науковий ступень вчене звання

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Телекомунікацій

Кафедра ___Телекомунікаційних систем та мереж_____
Ступінь вищої освіти __магістр_____
Спеціальність ___172 Електронні комунікації та радіотехніка _____
Освітньо-професійна програма _Телекомунікаційні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедри __ТСМ_____
_____ Віктор ЗАЇКА
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Якимчуку Сергію Петровичу

1. Тема кваліфікаційної роботи: “Впровадження сучасного NGFW та системи моніторингу для підвищення безпеки корпоративної мережі”, керівник кваліфікаційної роботи Ганна ГРИНЕВИЧ, д.т.н., доцент
затверджені наказом Державного університету інформаційно-комунікаційних технологій від 15.10.2024 року № 320

2. Строк подання кваліфікаційної роботи:

3. Вихідні дані до кваліфікаційної роботи:
1. Інфраструктура корпоративної мережі підприємства.
2. Програмно-апаратні засоби Cisco, Fortinet.
3. Вимоги до кіберзахисту (CIS Control, Zero Trust).
4. Дані щодо вразливостей, мережевих сервісів та політик доступу.
5. Нормативні документи у сфері інформаційної безпеки

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз існуючої корпоративної мережевої інфраструктури.
2. Оцінка ризиків інформаційної безпеки.
3. Проектування нової архітектури корпоративної мережі.
4. Розроблення та впровадження механізмів Zero Trust.
5. Оцінка ефективності впровадження рішень.
6. Формування висновків та рекомендацій.

5. Перелік ілюстративного матеріалу: презентація на слайдах

6. Дата видачі завдання

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір та аналіз науково-технічної літератури	10.09.2025	Викон.
2	Розробка першого розділу	25.09.2025	Викон.
3	Розробка другого розділу	05.10.2025	Викон.
4	Розробка третього розділу	20.10.2025	Викон.
5	Розробка четвертого розділу	1.11.2025	Викон.
6	Висновки, вступ, реферат	10.11.2025	Викон.
7	Розробка презентації	30.11.2025	Викон.

Здобувач вищої освіти _____ Сергій ЯКИМЧУК
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи

_____ Ганна ГРИНКЕВИЧ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

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

Направляється здобувач Якимчук С. П. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 172 Електронні комунікації та радіотехніка
(шифр і назва спеціальності)
Освітньо-професійної програми Телекомунікаційні системи та мережі

на тему: «Впровадження сучасного NGFW та системи моніторингу для підвищення безпеки корпоративної мережі»

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Якимчук Сергій Петрович показав гарну теоретичну та інженерну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою, в тому числі рекомендаціями МСЕ. Працюючи над завданнями, які доручались керівником, проявила ініціативність, сумлінність та хист до інженерної роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Якимчука Сергія Петровича на оцінку "відмінно" та присвоїти йому кваліфікацію «магістр з електронних комунікацій та радіотехніки».

Керівник роботи _____ Ганна ГРИНКЕВИЧ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"___" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Якимчук С.П. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри телекомунікаційних систем та мереж _____ Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

"___" _____ 2025 року

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня магістра

здобувача вищої освіти Якимчука Сергія Петровича
(прізвище, ім'я, по батькові)
на тему «Впровадження сучасного NGFW та системи моніторингу для підвищення безпеки корпоративної мережі»

Актуальність.
Тема роботи є сучасною та практично значущою, оскільки зростання кількості кібератак та ускладнення мережевої інфраструктури висуває підвищені вимоги до засобів інформаційного захисту. У роботі проведено аналіз існуючої мережі підприємства, визначено основні ризики та запропонованого архітектурне рішення з використанням NGFW, Zero Trust та NAC.

Позитивні сторони.
1. Робота містить практичну цінність та як була впроваджена в реальній компанії.
2. Результати тестування підтвердили ефективність запропонованих рішень, зокрема часу виявлення інцидентів (MTTD), часу реагування (MTTR) та загального рівня ризику.

Недоліки.
1. У роботі не повністю розкрито економічну складову.
2. У роботі вказані не всі фрагменти конфігураційної частини.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської кваліфікаційної роботи

Висновок: *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "відмінно", а здобувач Якимчук Сергій Петрович заслуговує присвоєння кваліфікації: магістр з електронних комунікацій та радіотехніки.*

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

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 85 стор., 41 рис., 11 табл., 19 джерел.

Мета роботи – підвищення рівня захищеності корпоративної мережі шляхом проектування та впровадження комплексної системи мережевої безпеки, що включає NGFW, Zero Trust та систему контролю доступу FortiNAC..

Об'єкт дослідження – процеси забезпечення інформаційної безпеки підприємства.

Предмет дослідження – методи, технології та засоби мережевого захисту. У роботі застосовано методи аналізу, синтезу, моделювання мережевих архітектур та оцінювання ефективності.

Короткий зміст роботи: Робота присвячена підвищенню рівня кібербезпеки корпоративної мережі шляхом впровадження сучасного мережевого екрана нового покоління (NGFW), моделі Zero Trust та системи контролю доступу до мережі NAC. На основі порівняльного аналізу рішень провідних виробників обґрунтованого вибір комплексу Fortinet, який включає NGFW FortiGate та систему контролю доступу FortiNAC. Запропоновану нову архітектуру корпоративної мережі з розширеною сегментацією та контролем доступу до внутрішніх ресурсів ззовні за допомогою рішення FortiClient EMS.

КЛЮЧОВІ СЛОВА: NGFW, МЕРЕЖЕВИЙ ЕКРАН НОВОГО ПОКОЛІННЯ, FORTIGATE, ZERO TRUST, ZTNA, NAC, FORTINAC, КІБЕРБЕЗПЕКА, СЕГМЕНТАЦІЯ МЕРЕЖІ, МОНІТОРИНГ, IDS/IPS, SSL INSPECTION, КОНТРОЛЬ ДОСТУПУ, КОРПОРАТИВНА МЕРЕЖА.

ABSTRACT

The part of the master`s qualification work: 85 pages, 41 figures, 11 tables, 19 references.

The purpose of the work - is to enhance the security level of a corporate network by designing and implementing a comprehensive network security system that includes an NGFW, Zero Trust model, and the FortiNAC access control system.

Object of research - is the process of ensuring the information security of an enterprise.

Subject of research - is the methods, technologies, and tools of network protection. The work applies methods of analysis, synthesis, network architecture modeling, and efficiency evaluation.

Summary of the work: The thesis is dedicated to improving the cybersecurity level of a corporate network through the implementation of a modern next-generation firewall (NGFW), the Zero Trust model, and a network access control (NAC) system. Based on a comparative analysis of solutions from leading vendors, the choice of the Fortinet ecosystem is justified, which includes the FortiGate NGFW and the FortiNAC access control system. A new architecture of the corporate network is proposed, featuring enhanced segmentation and controlled access to internal resources from external networks using the FortiClient EMS solution.

KEYWORDS: NGFW, NEXT-GENERATION FIREWALL, FORTIGATE, ZERO TRUST, ZTNA, NAC, FORTINAC, CYBERSECURITY, NETWORK SEGMENTATION, MONITORING, IDS/IPS, SSL INSPECTION, ACCESS CONTROL, CORPORATE NETWOR

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 11
ВСТУП 12
1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ 13
1.1 Сутність та актуальність захисту корпоративних мереж 13
1.2 Основні поняття інформаційної безпеки 13
1.3 Підходи до побудови системи захисту. 14
1.4 Стандарти безпеки: акцент на CIS Controls 14
1.5 Структура CIS Control v8 15
1.6 Переваги використання CIS Controls 16
1.7 Типові проблеми впровадження безпеки 16
1.8 Перспективи розвитку корпоративної кібербезпеки 16
1.9 Висновок до 1 розділу 17
2 АНАЛІЗ ІСНУЮЧОГО СТАНУ КОРПОРАТИВНОЇ МЕРЕЖІ 18
2.1 Загальні характеристики корпоративної мережі 18
2.2 Опис проблем безпеки та їх наслідки 21
2.3 Аналіз архітектури корпоративної мережі та каналів зв’язку 23
2.4 Аналіз поточних механізмів безпеки корпоративної мережі. 24
2.5 Аналіз ризиків і загроз корпоративної мережі 25
2.6 Відповідність поточного стану стандартам CIS Control v8 26
2.7 Висновок до 2 розділу 28
3 ПРОЕКТУВАННЯ ТА ВПРОВАДЖЕННЯ NGFW І МОНІТОРИНГУ 29
3.1 Обґрунтування вибору NGFW 29
3.2 Проектування архітектури 32
3.3 Конфігурація FortiGate як NGFW 37
3.4 Розгортання VPN сервера на FortiGate 48
3.5 Розгортання NAC системи на базі FortiNAC 53
3.6 Розгортання Oxidized 59
3.7 Розгортання системи моніторингу логів Loganalyzer 61

3.8 Розгортання системи моніторингу Zabbix 62
3.9 Висновок до 3 розділу 66
4 ОЦІНКА ЕФЕКТИВНОСТІ ВПРОВАДЖЕННЯ 68
4.1 Методика оцінки ефективності впровадження 68
4.2 Аналіз показників безпеки до і після модернізації 69
4.3 Економічне обґрунтування та витрати 71
4.4 Порівняння показників продуктивності 72
4.5 Оцінка надійності та стійкості до збоїв 74
4.6 Висновки до 4 розділу 76
ВИСНОВКИ 79
ПЕРЕЛІК ПОСИЛАНЬ 81
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 83

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD — Active Directory
ARP — Address Resolution Protocol
ASA — Adaptive Security Appliance
ASR — Aggregation Services Router
CCTV — Closed-Circuit Television
CIA — Confidentiality, Integrity, Availability
CIS — Center for Internet Security
DDoS — Distributed Denial-of-Service
DPI — Deep Packet Inspection
EDR — Endpoint Detection and Response
GRE — Generic Routing Encapsulation
HTTPS — HyperText Transfer Protocol Secure
IDS — Intrusion Detection System
IPS — Intrusion Prevention System
IPsec — Internet Protocol Security
LAN — Local Area Network
NAC — Network Access Control
NGFW — Next-Generation Firewall
NDR — Network Detection and Response
QoS — Quality of Service
SIEM — Security Information and Event Management
SSL — Secure Sockets Layer
VM — Virtual Machine
VLAN — Virtual Local Area Network
VPN — Virtual Private Network
ZTP — Zero-Touch Provisioning

ВСТУП

Актуальність теми. Сучасні корпоративні мережі стають дедалі більш складними та піддаються зростаючій кількості кіберзагроз. Традиційні міжмережеві екрани вже не забезпечують належного рівня захисту, оскільки не враховують специфіку сучасних атак, пов’язаних із використанням додатків, шифруванням трафіку та внутрішніми загрозами. У зв’язку з цим актуальним є впровадження сучасних NGFW (Next-Generation Firewall), які поєднують функції класичних засобів захисту з додатковими механізмами контролю та аналізу даних.

Мета роботи - підвищення рівня захищеності корпоративної мережі шляхом проектування та впровадження комплексної системи мережевої безпеки, що включає мережевий екран нового покоління (NGFW), модель Zero Trust для віддаленого доступу та систему контролю доступу до мережі FortiNAC.

Об’єкт дослідження - процеси забезпечення інформаційної безпеки та захисту мережевої інфраструктури підприємства.

Предмет дослідження - методи, технології та засоби комплексного захисту корпоративної мережі, включно з NGFW, Zero Trust архітектурою та системами NAC.

Метод дослідження - у роботі застосовано наступні методи:

- Аналіз та синтез вимог до кібербезпеки;
- Методи моделювання мережевих архітектур;
- Порівняльний аналіз моделей доступу та сегментації;
- Методи оцінювання ефективності (MTTD, MTTR, Risk Score).

Апробація результатів магістерської роботі - основні результати магістерської роботи були апробовані під час:

- впровадження компонентів NGFW та NAC у тестовому середовищі організації;
- перевірки працездатності рішення в реальних умовах експлуатації мережі;
- доповідалися на всеукраїнській науково-технічній конференції «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу» та міжнародній науково-практичній конференції «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії»

1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Сутність та актуальність захисту корпоративних мереж

У сучасному цифровому світі корпоративні мережі є ключовим елементом інформаційної інфраструктури будь-якої організації. Вони забезпечують взаємодію між співробітниками, клієнтами, сервісами та системами. Однак зі зростанням кількості кіберзагроз, що мають як технічний, так і соціоінженерний характер, забезпечення надійного захисту корпоративних мереж стало критично важливим завданням.

Згідно зі статистикою глобальних кібер інцидентів, більшість атак спрямовані саме на мережеву інфраструктуру організацій: проникнення в локальну мережу, використання вразливостей у протоколах доступу, перехоплення трафіку тощо. У зв’язку з цим, ефективний захист мережі є не лише технічним завданням, а й складовою частиною загальної політики інформаційної безпеки компанії.

1.2 Основні поняття інформаційної безпеки

Захист корпоративної мережі базується на фундаментальних принципах інформаційної безпеки:

- Конфіденційність (Confidentiality) - забезпечення доступу до даних лише авторизованим особам.
- Цілісність (Integrity) - гарантія того, що інформація не була змінена або знищена
- Доступність (Availability) - гарантія доступу до інформації та ресурсів у потрібний момент.

Ці принципи утворюють так звану CIA-траду, яка є основною практично всіх стандартів інформаційної безпеки.

Інші ключові терміни:

- Загроза (threat) - потенційна подія або дія, яка може завдати шкоди.
- Вразливість (vulnerability) - слабке місце в системі, яке може бути використане зловмисником.
- Атака (attack) - конкретна реалізація загрози з використанням вразливостей.
- Ризики (risk) - ймовірність реалізації загрози і масштаб її наслідків.

1.3 Підходи до побудови системи захисту.

Сучасні методи захисту корпоративних мереж базуються на багаторівневій моделі оборони(Defense-in-Depth). Вона передбачає наступні підходи:

- Мережевий захист: використання мережевих екранів (FW, NGFW), сегментація мережі.
- Ідентифікація і автентифікація: контроль доступу, багатофакторна автентифікація.
- Захист кінцевих точок(Endpoint Protection): антивіруси, EDR, контроль USB.
- Моніторинг та аналіз: використання SIEM, NDR, логування.
- Резервне копіювання: створення копій критичних даних.
- Реагування на інциденти: створення планів реагування (IRP), навчання персоналу.

Для систематизації підходів часто використовують стандартизовані фреймворки: NIST CSF, ISO/IEC 27001, CIS Controls, COBIT, MITRE ATT&CK тощо.

1.4 Стандарти безпеки: акцент на CIS Controls

CIS(Center for Internet Security)- некомерційна організація, що розробляє та підтримує стандарт CIS Control. Це набір з 18 практичних дій (контролів), які допомагають зменшити ризик кіберзагроз.

Еволюція стандарту:

- Раніше: CIS Top 20
- Поточна версія: CIS Control v8- адаптована до сучасних викликів: робота з хмарою, віддалені користувачі, мобільні пристрої.

Цілі CIS Controls:

- Надати практичну, пріоритетну і зрозумілу структуру для впровадження безпеки.
- Зосередитись на найбільш небезпечних та поширених типах атак.
- Забезпечити основу для аудиту та покращення захисту.

1.5 Структура CIS Control v8

Контролі CIS v8 поділяють на 3 категорії:

1. Basic Controls 1-6 (Фундамент захисту)
2. Foundational Controls 7-14 (Поглиблений захист)
3. Organizational Control 15-18 Політики, навчання, управління)

Короткий опис кожного з 18 контролів:

1. Inventory and Control of Enterprise Assets
   - ведення обліку пристроїв в мережі.
2. Inventory and Control of Software Assets
   - контроль встановленого програмного забезпечення
3. Data Protection
   - класифікація, шифрування, захист даних.
4. Secure Configuration of Enterprise Assets
   - безпечні налаштування ОС, ПЗ, пристроїв.
5. Account Management
   - управління обліковими записами та правами доступу.
6. Access Control Management
   - контроль за доступом до ресурсів.
7. Continuous Vulnerability Management
   -сканування на вразливість, патч-менеджмент.
8. Audit Log Management
   - збір, зберігання та аналіз логів.
9. Email and Web Browser Protection
   - захист від фішингу, шкідливих сайтів
10. Malware Defenses
    - антивірус, EDR, sandbox
11. Data Recovery
    - резервне копіювання, перевірка відновлення.
12. Network Infrastructure Management
    - сегментація мережі, управління маршрутами, комутаторами.
13. Security Awareness and Skills Training
    - навчання персоналу, тестування.
14. Security Operations Center (SOC) & SIEM
    - аналітика, інцидент-менеджмент.
15. Service Provider Management
    - аудит та безпека постачальників.

16. Application Software Security
    - розробка безпечного ПЗ, тестування коду.
17. Incident Response Management
    - створення IR-планів, навчання реагування.
18. Penetration Testing
    - тестування на проникнення, перевірка захисту.

1.6 Переваги використання CIS Controls

- Пріоритетність: контролі розставлені за критичністю.
- Простота впровадження: описано чітко і практично.
- Гнучкість: підходить для організацій різного масштабу.
- Відповідність регулятивним вимогам: застосовується для аудиту та сертифікації.

1.7 Типові проблеми впровадження безпеки

Навіть при наявності бажання впроваджувати безпеку за CIS Controls, компанії стикаються з низкою викликів:

- Недостатній бюджет і ресурси.
- Відсутність технічної компетенції персоналу.
- Застаріла IT-інфраструктура
- Розрив між IT та бізнесом
- Нехтування політиками з боку працівників.

Для вирішення цих проблем рекомендується розпочинати з мінімального набору заходів і поступово розширювати систему безпеки. Іноді доцільно залучати зовнішні ресурси для впровадження системи.

1.8 Перспективи розвитку корпоративної кібербезпеки

Захист мережі надалі буде рухатись у напрямку повної автоматизації, адаптивного реагування та інтеграції з бізнес-процесами:

- Zero Trust- нова система, яка передбачає перевірку кожного запиту незалежно від місця його походження.

- AI/ML - використання алгоритмів машинного навчання для виявлення аномалій.
- XDR- об’єднання захисту кінцевих точок, мережі і хмар у єдину платформу.
- DevSecOps- інтеграція безпеки та усі етапи розробки.
- SASE- поєднання мережевих функцій та кібербезпеки у хмарній моделі.

1.9 Висновок до 1 розділу

Захист корпоративних мереж- це багаторівнева, комплексна задача, яка потребує поєднання технічних, організаційних і людських чинників. Одним з найбільш ефективних і практичних підходів є впровадження CIS Controls v8, яке забезпечує надійну основу для побудови системи інформаційної безпеки.

Цей фреймворк допомагає організаціям структурувати процеси захисту, оцінювати ризики та відповідати сучасним вимогам.

2 АНАЛІЗ ІСНУЮЧОГО СТАНУ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Загальні характеристики корпоративної мережі

Корпоративна мережа є основою інформаційної інфраструктури підприємства, через неї здійснюється передача даних між користувачами та сервісами. ЇЇ надійність та пропускна здатність безпосередньо впливає на ефективність всіх бізнес-процесів.

На даному етапі дослідження розглядається корпоративна мережа організації:

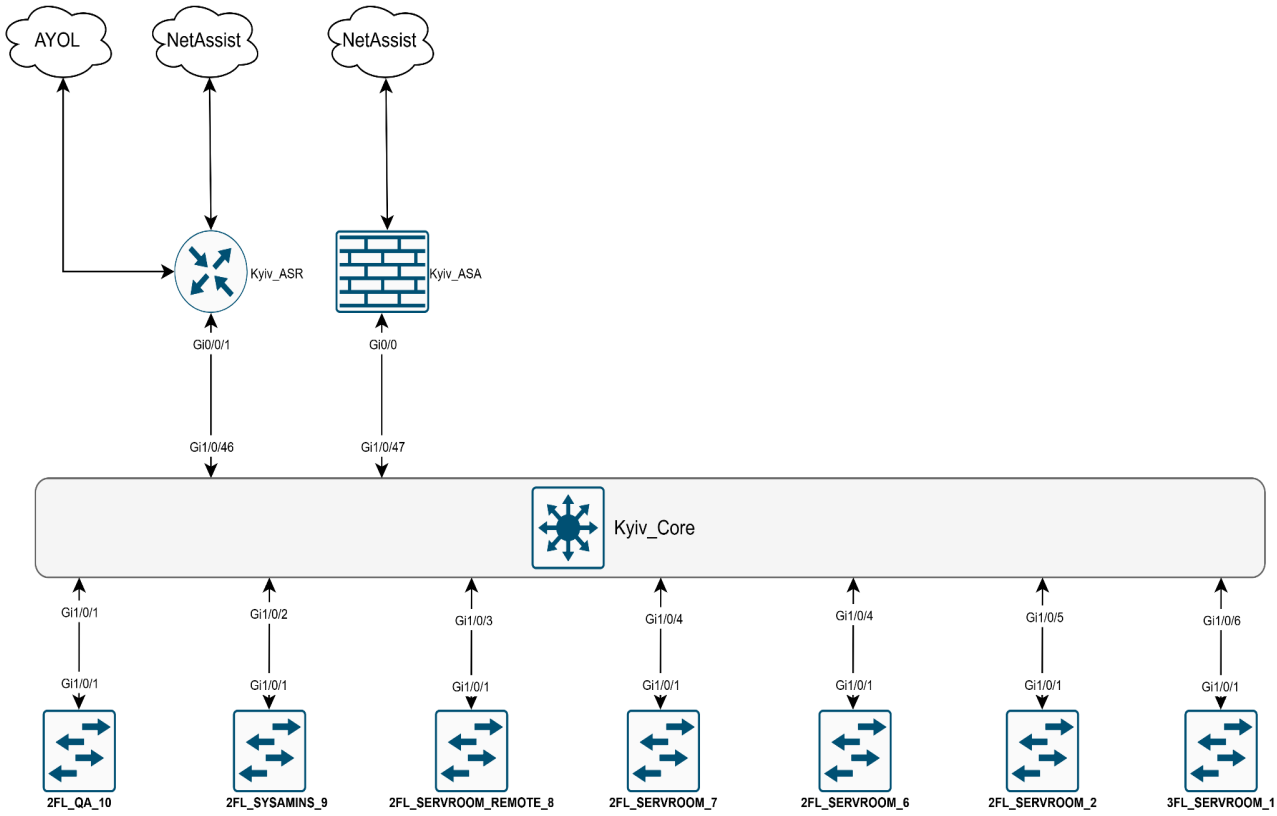


Рис. 2.1 Фізична схема мережі

1. Cisco ASR 1001-x

   a. Виконує функцію граничного маршрутизатора (Edge Router).
   b. Реалізує NAT (Network Address Translation) для всіх користувачів корпоративної мережі.
   c. Забезпечує шифрування трафіку через GRE over IPsec тунелі до віддаленого офісу.

d. Має два підключення до провайдерів: AYOL та NetAssist, що створює мінімальний рівень відмовостійкості.
e. Налаштовані ACL лише для базового фільтрування.
f. Не використовується механізм QoS, тому пріоритезація трафіку відсутня.

2. Cisco ASA 5525-x

a. Наразі використовується виключно як VPN-концентратор для віддалених користувачів.
b. Можливості IPS, антивірусного аналізу, SSL Inspection- не задіяні.
c. Не інтегрована з системою централізованого моніторингу.
d. Відсутня політика зональної безпеки, весь VPN-трафік потрапляє у внутрішній VLAN без додаткової фільтрації.

3. Cisco Catalyst 3760 (ядро)

a. Реалізує функції Layer 3-комутатора: маршрутизація між VLANs.
b. Забезпечує агрегацію комутаторів доступу.

4. Cisco Catalyst 2960 (доступ)

a. Виконують функцію підключення користувачів, точок доступу Wi-Fi та систем відеоспостереження.
b. Порти сконфігуровані у режимі Access, без Port-Security.
c. Відсутній механізм 802.1X, DHCP Snooping, Dynamic ARP Inspection

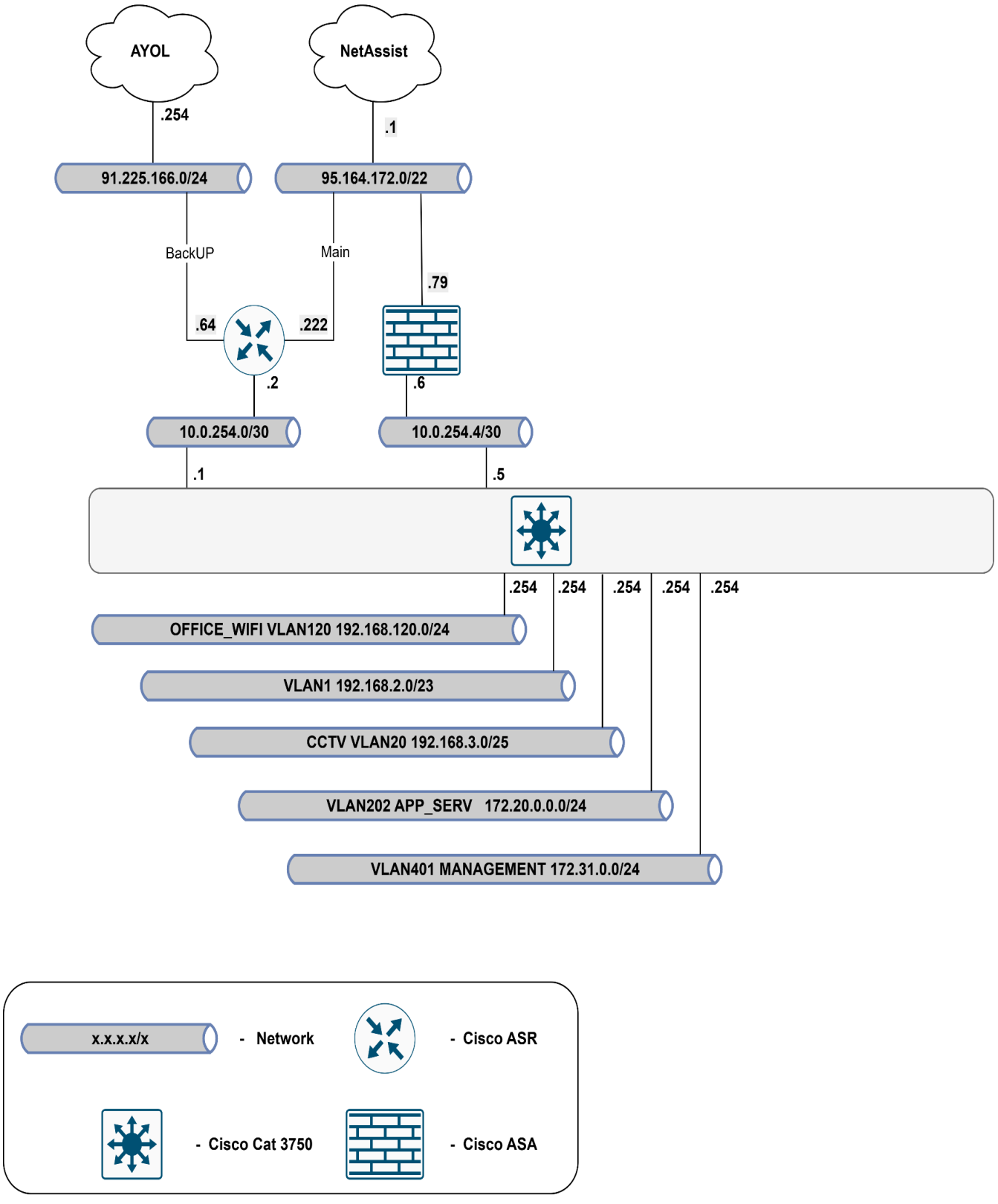


Рис. 2.2 Логічна схема мережі

Таблиця 2.1.

VLAN-структура і IP-планування

VLAN	Назва	Підмережа	Призначення
VLAN 1	Corp LAN	192.168.2.0/24	Користувачі
VLAN 20	Office Wi-Fi	192.168.120.0/24	Бездротова мережа
VLAN 120	CCTV	192.168.3.0/25	Відеоспостереження
VLAN 202	APP_SERV	172.20.0.0/24	Сервіси
VLAN 401	MNGM	172.31.0.0/24	Керування мережевими пристроями

2.2 Опис проблем безпеки та їх наслідки

Cisco ASA 5525-x дата завершення підтримки (End-of-Support) 30 вересня 2025 рік, вразливості які вже не виправлять:

- CVE-2025-20333- критична вразливість буферного переповнення (buffer overflow) в HTTP(S) сервісі / веб VPN, що може дозволити віддалене виконання коду з правами пристрою
- CVE-2025-20362- Авторизаційне обхідне / доступ до URL-ендпоінтів без автентифікації — відкриває доступ до частин веб-інтерфейсу, які не повинні бути відкриті.

Якщо використовувати дані вразливості, зловмисник може спокійно потрапити на периметр мережевої інфраструктури компанії. Що в свою чергу веде до злиття даних компанії.

Cisco Catalyst 3750 дата завершення підтримки (End-of-Support) 31 липня 2023 рік. Їхні вразливості:

- CVE-2018-0171- дозволяє не авторизованому користувачу викликати перезавантаження або отримати виконання коду (RCE) на деяких пристроях з увімкненим Smart Install

При даній вразливості, для ядра, це критична річ. Так як при перезавантаженні центрального коммутатора, зупиняється вся мережа.

Cisco Catalyst 2960- лінійка комутаторів Cisco, які себе дуже добре зарекомендували. Дата завершення підтримки (End-of-Support) 31 жовтня 2019 рік. Їхні вразливості:

- CVE-2020-3231- 802.1X Authentication Bypass на 2960-L серії та деяких інших, через неправильну обробку broadcast трафіку до аутентифікації порту. Якщо порт налаштований на 802.1X, до того як клієнт аутентифікований, зловмисник у локальній мережі може надсилати / отримувати broadcast пакети.
- CVE-2018-0171- Уразливість Smart Install (SMI) (Improper validation) — дозволяє виконати довільний код або викликати DoS через віддалені запити. Ця проблема зачіпає багато Catalyst серій (включно з 2960), особливо коли Smart Install ввімкнений (за замовчуванням чи випадково) і пристрій доступний з мережі.

Якщо знати про ці вразливості, то можна спокійно зупинити роботу компанії. А найбільший ризик воно несе в можливості несанкціонованого доступу до сервісів компанії.

Для понад 300 користувачів реалізовано лише 2 VLAN, що створює великі broadcast-домени та обмежує можливості ізоляції між підрозділами. Зокрема, мережевий трафік від різних підрозділів передається без додаткової сегментації. Відсутність сегментації створює умови для:

- Внутрішніх атак (ARP-spoofing, DHCP starvation)
- Поширення шкідливого ПЗ через внутрішню мережу
- Перевантаження комутаторів через broadcast storm
- Простій всієї мережі, а не її сегмента

Відсутність систем централізованих систем моніторингу та резервного копіювання конфігурацій мережевого обладнання. Такий підхід має низку недоліків:

- Відсутність централізованого контролю за станом мережі. У разі виникнення збоїв або деградації продуктивності неможливо оперативно визначити джерело проблеми без безпосереднього доступу до кожного пристрою.
- Відсутність історії змін конфігурації. Будь-які ручні зміни не фіксуються автоматично, що може випадково внести некоректні налаштування, що призведе до порушення роботи мережі.

- Неможливе швидке реагування на інциденти. Без систем моніторингу відсутнє сповіщення про критичні події(падіння інтерфейсів, збій у живленні)
- Відсутність резервних копій конфігурації. У випадку виходу з ладу пристрою або скидання налаштувань необхідно вручну відтворювати конфігурацію, що може займати кілька годин або днів.

Таким чином, відсутність даних сервісів створює операційні ризики і знижує рівень надійності та керованості корпоративної мережі.

2.3 Аналіз архітектури корпоративної мережі та каналів зв'язку

Архітектура корпоративної мережі побудована за класичною трирівневою моделлю- ядро, агрегація, доступ.
Таке розділення дозволяє масштабувати мережу, забезпечити логічну структурованість та спрощує адміністрування.
На рівні ядра, виконується маршрутизація між VLAN-сегментами та об'єднує комутатори доступу.
Рівень агрегації реалізований через магістральні з'єднання до маршрутизатора, що виконує роль граничного пристрою.
На рівні доступу працюють комутатори, до яких підключені робочі станції, Wi-Fi точки доступу, принтера та системи відеоспостереження.

Основні канали зв'язку побудовані на основі гігабітних інтерфейсів між ядром та пограничними пристроями.
Зовнішній вихід до Інтернету реалізовано через провайдери (AYOL та NetAssist), що забезпечує мінімальний рівень відмовостійкості та резервування трафіку.

Тунельне з'єднання з віддаленим офісом реалізовано через GRE over IPsec, яке забезпечує захищений канал між офісами.
Однак відсутність резервного тунелю та механізму автоматичного перемикання у разі збою може призвести до тимчасової втрати зв'язку.

Узагальнена топологія корпоративної мережі представлена на рис. 2.1 2.2(логічна та фізична схема корпоративної мережі)

2.4 Аналіз поточних механізмів безпеки корпоративної мережі.

Незважаючи на наявність базових засобів безпеки, поточна архітектура корпоративної мережі не відповідає сучасним вимогам кіберзахисту. Нижче наведено аналіз основних компонентів і їх слабких місць.

Таблиця 2.2.

Аналіз основних компонентів

Компонент	Реалізовані механізми	Виявлені недоліки	Рекомендовані покращення
Cisco ASA 5525-x	-VPN для віддалених користувачів -ACL для базового фільтрування	Відсутність IPS/IDS, SSL інспекції, антивірусного аналізу	Впровадити NGFW з глибоким аналізом трафіку
Cisco Catalyst 3750/2960	VLAN	Відсутність 802.1X, Port Security…	Налаштувати механізм мережевого доступу (NAC)
Роутер ASR 1001-X	NAT, IPsec тунелі	Немає політик QoS, IDS та централізованого логування	Інтегрувати з системою моніторингу
Адміністрування	Ручна CLI-конфігурація	Відсутнє журналювання, резервні копії не зберігаються	Розгорнути системи моніторингу, логування та копіювання

Відсутність централізованої системи моніторингу призводить до неможливості оперативного реагування на інциденти. Зміни в конфігурації не фіксуються, що ускладнює аналіз подій після збоїв або атак.

2.5 Аналіз ризиків і загроз корпоративної мережі

Для оцінки поточного стану безпеки було проведено ідентифікацію основних загроз та ризиків, які можуть вплинути на функціонування мережі.

Матриця ризиків корпоративної мережі

Таблиця 2.3.

Матриця ризиків

Ризики	Ймовірність	Наслідки	Рівень ризику	Відповідний CIS Control
Експлуатація вразливостей ASA/3750	Висока	Компрометація периметру	Критичний	7, 8
Відсутність сегментації	Висока	Поширення загроз у внутрішній мережі	Критичний	13
Відсутність моніторингу	Висока	Пізнє реагування на інциденти	Високий	14
Відсутність резервного копіювання конфігурацій	Середня	Втрата даних при збої	Високий	11
Відсутність контролю доступу до портів	Середня	Несанкціоноване підключення	Середній	6

Виділено три основні групи загроз:

1. Зовнішні загрози:
   DDoS-атаки, експлуатація вразливостей у периметрових пристроях (ASA, ASR), фішингові атаки на VPN-користувачів.
2. Внутрішні загрози:
   Несанкціонований доступ працівників, ARP-spoofing, поширення шкідливого ПЗ через спільну мережу, використання незахищених пристроїв
3. Технічні ризики:
   Вихід з ладу обладнання, відсутність резервного копіювання, помилки конфігурацій, відсутність централізованого логування

Аналіз показав, що більшість ризиків мають високий або критичний рівень, що підтверджує потребу у провадженні сучасного NGFW та системи моніторингу.

2.6 Відповідність поточного стану стандартам CIS Control v8

Для оцінки зрілості інформаційної безпеки корпоративної мережі попередньо порівняння із рекомендаціями CIS Controls v8.
У таблиці 2.4. подано оцінку зрілості інформаційної безпеки організації відповідно до окремих контролів стандарту CIS. Кожен контроль має вказаний статус впровадження та коментар, що пояснює причини такого стану. Загалом інформація демонструє, що більшість ключових процесів безпеки або не реалізовані, або реалізовані частково та потребують суттєвого доопрацювання.
Узагальнюючи представлені дані, видно, що більшість критично важливих механізмів інформаційної безпеки або не працюють, або діють фрагментарно.

Основні проблеми — ручні процеси, відсутність автоматизації, нестача політик і регламентів, відсутність моніторингу та реагування. Такий стан свідчить про низьку зрілість системи інформаційної безпеки, потребу у впровадженні сучасних рішень, структуризації процесів та побудові комплексної системи захисту підприємства.
Результати наведені у таблиці.

Таблиця 2.4.

Оцінка зрілості інформаційної безпеки

Контроль CIS	Назва	Статус виконання	Коментар
1	Inventory and Control of Enterprise Assets	Частково	Облік обладнання ведеться вручну
7	Continuous Vulnerability Management	Ні	Не проводиться регулярне сканування
8	Audit Log Management	Ні	Відсутнє централізоване логування
11	Data Recovery	Ні	Немає сервісів
13	Network Infrastructure Management	Частково	Підмережі існують, але їх недостатньо і без політик
14	Security Operations Center (SOC/SIEM)	Ні	Відсутній моніторинг безпеки
17	Incident Response Management	Ні	План реагування на інциденти відсутній

Таким чином, поточний рівень відповідності CIS Controls можна оцінити як низький (20-25%). Для підвищення цього показника необхідно впровадження NGFW, централізованого моніторингу та резервне копіювання.

2.7 Висновок до 2 розділу

Проведений аналіз показав, що корпоративна мережа організації функціонує на базі обладнання Cisco, яке морально та технічно застаріло. Основні недоліки поточного стану полягають у наступному:

- Використання обладнання, що втратило підтримку
- Наявність критичних вразливостей без можливостей оновлення
- Відсутність ефективної сегментації VLAN і механізмів доступу
- Відсутність централізованого моніторингу подій і логів
- Відсутність резеврного копіювання конфігурацій

Ці проблеми створюють високі ризики для безперервної роботи корпоративної мережі, а також роблять її вразливою до зовнішніх атак і внутрішніх. Для мінімізації зазначених ризиків необхідно провести модернізацію периметру мережі, замінивши застаріле обладнання на сучасне та впровадити систему централізованого моніторингу подій безпеки.
Це дозволить підвищити рівень безпеки корпоративної мережі.

3 ПРОЕКТУВАННЯ ТА ВПРОВАДЖЕННЯ NGFW І МОНІТОРИНГУ

3.1 Обґрунтування вибору NGFW

Із зростанням кількості цифрових сервісів та віддалених користувачів підхід до побудови систем захисту корпоративних мереж зазнає істотних змін. Традиційні міжмережеві екрани, що працюють на рівні портів і протоколів, не дають змоги ефективно виявити сучасні загрози, оскільки більшість атак маскується у прикладному рівні. Саме тому для сучасних підприємств актуальним стає використання міжмережевих екранів нового покоління - Next Generation Firewall(NGFW), які здатні використовувати аналіз трафіку в реальному часі, розпізнавати додатки, контролювати користувачів та здійснювати глибоку перевірку вмісту пакета.

Результати попереднього аналізу показали, що існуюча інфраструктура має низку недоліків у частині безпеки:

- Використання Cisco ASA 5525-x лише для організації VPN без увімкнення системи виявлення вторгнень;
- Маршрутизатор Cisco ASR 1001-x виконує лише NAT та маршрутизацію без інспекції вмісту трафіку;
- Відсутність централізованого моніторингу та систем журналювання подій;
- Брак сегментації та зональної політики безпеки.

Такі обмеження підвищують ризики несанкціонованого доступу, внутрішніх атак і втрати конфіденційних даних.

Отже, при виборі нового міжмережевого екрану було визначено такі вимоги:

1. Підтримка глибокої інспекції трафіку (DPI) та захисту від вторгнень;
2. Наявність модулів контролю додатків та користувачів;
3. Можливість роботи у віртуальному середовищі без закупівлі апаратного NGFW;
4. Сумісність із системами моніторингу(SNMP, Syslog, Zabbix);
5. Доступна вартість придбання та обслуговування.

На основі відкритих джерел та технічних характеристик було проведено порівняльний аналіз чотирьох найбільш розповсюджених рішень: Cisco Firepower, FortiGate, Palo Alto Networks та Check Point.

Таблиця 3.1.

Порівняння провідних NGFW-платформ

Критерій	Cisco Fp	Palo Alto	Check Point	FortiGate
DPI	Високий рівень	Високий рівень	Високий рівень	Високий рівень
SSL-аналіз	Добрий рівень	Дуже високий рівень	Добрий рівень	Високий рівень
Вбудований ISP/IDS	Розвинена система	Розвинена система	Розвинена система	Розвинена система
Контроль додатків	Середній	Дуже високий	Висока	Висока
Складність адміністрування	Висока	Середня	Висока	Низька
Вартість ліцензій	Висока	Дуже висока	Висока	Помірна
Підтримка віртуалізації	Часткова	Обмежена	Часткова	Повна
Інтеграція з SIEM	Добра	Добра	Добра	Висока

Згідно з проведеним аналізом, FortiGate VM демонструє найкраще співвідношення функціональності, вартості та впровадження. Це рішення охоплює повний набір можливостей NGFW і може бути розгорнутий у віртуальному середовищі без придбання фізичного обладнання.

FortiGate VM є програмною реалізацією апаратних пристроїв серії FortiGate. Вона може функціонувати на платформах VMware ESXI, Microsoft Hyper-V, а також у хмарних інфраструктур (Azure, AWS). Основні компоненти рішення:

- FortiOS - універсальна операційна система з функціями маршрутизації, міжмережевого екрану, фільтрації контенту, VPN, антивірусу та IPS;

- FortiGuard Security Services - служба оновлення сигнатур, баз шкідливих URL і категорій веб ресурсів;
- FortiAnalyzer - модуль централізованого зберігання логів і побудови звітів;
- FortiManager - інструмент керування політиками безпеки для кількох вузлів.

Система підтримує різні режими перевірки (flow-based, proxy-based, hybrid), що дозволяє оптимізувати співвідношення продуктивності та глибини аналізу залежно від типу трафіку.

Ключовими перевагами FortiGate VM є:

1. Глибокий аналіз трафіку (DPI). Пристрій ідентифікує мережеві додатки незалежно від потрів і протоколів, дозволяючи застосовувати політики доступу до конкретних сервісів.
2. Інтелектуальний контроль додатків. Можна створювати політики для певних програм або категорій - наприклад, дозволити корпоративні інструменти (Teams, Zoom) і заблокувати розважальні сервіси (TikTok, YouTube).
3. Захист від вторгнень (IPS/IDS). Система аналізує пакети на основі сигнатур і поведінкових моделей, виявляючи підозрілу активність у режимі реального часу.
4. Перевірка зашифрованого трафіку (SSL Inspection). FortiGate може виконувати розшифрування HTTPs-з’єднань для аналізу їхнього вмісту без втрати продуктивності.
5. Контентна фільтрація та антивірусний захист. Реалізовано механізм блокування небажаних категорій сайтів і сканування файлів при завантаженні користувачами.
6. VPN та сегментація. Підтримується створення IPsec та SSL VPN тунелів, що дає змогу замінити Cisco ASA, а також реалізувати логічне розділення внутрішніх сегментів мережі.
7. Масштабованість. Завдяки віртуальному розгортанню FortiGate VM може легко переміщуватися між фізичними серверами або хмарними платформами без зміни конфігурації.
8. Інтеграція з моніторингом. Підтримуються протоколи SNMP, Syslog, NetFlow, що дозволяє здійснювати централізований збір статистики і контроль стану пристроїв через Zabbix або FortiAnalyzer.

Впровадження FortiGate дає можливість:

- Розмістити NGFW на периметрі мережі, що забезпечує фільтрацію трафіку до Інтернету;

- Централізувати VPN-доступ і інтегрувати автентифікацію з Active Directory та Google SAML;
- Реалізувати зони безпеки LAN, Wi-Fi, VPN…;
- Вести журнал подій безпеки з відправленням на Zabbix та FortiAnalyzer.

Економічна доцільність розгортання фізичних NGFW-контролерів є фінансово витратним. Наприклад, вартість Cisco Firepower або Palo Alto із ліцензіями перевищує кілька десятків тисяч доларів.FortiGate VM, навпаки, має перевагу у вигляді віртуалізації - він може бути розгорнутий на існуючому сервері без додаткових витрат на обладнання.Базова ліцензія дозволяє обробляти до кількох сотень користувачів, а підписка FortiCare забезпечує оновлення сигнатур та технічну підтримку. Таким чином, сукупна вартість володіння FortiGate VM є у 2-3 рази нижчою порівняно з аналогами при збереженні функціональності рівня enterprise.

3.2 Проектування архітектури

Під час проектування архітектури системи мережевої безпеки NGFW основна увага приділяється забезпеченню надійності, відмовостійкості, маштабованості та гнучкого керування.
Метою архітектури є створення багаторівневого захисту середовища, у якому кожен сегмент мережі має визначений рівень довіри, а взаємодія між ними відбувається через контрольований міжмережевий екран.
NGFW у сучасній корпоративній мережі виконує не лише класичні функції файрвола, але й забезпечує глибоку інспекцію трафіку, виявлення вторгнень (IPS/IDS), контроль додатків, фільтрацію веб контенту, SSL-інспекцію та інтеграцію з рішеннями NAC та EDR.

Основні принципи побудови проектованої архітектури:

- Розділення мережі на зони безпеки;
- Централізоване управління доступом користувачів через FortiNAC;
- Організація VPN-доступу через FortiEMS для віддалених співробітників;
- Використання віртуалізації FortiGate VM на базі високопродуктивних серверів;
- Реалізація резервування та високої доступності (HA) на рівні апаратних і віртуальних ресурсів.

Фізична архітектура корпоративної мережі представлена на Рисунку 3.1, де відображені ключові вузли ядра, доступу, міжмережеві з'єднання та сервери.

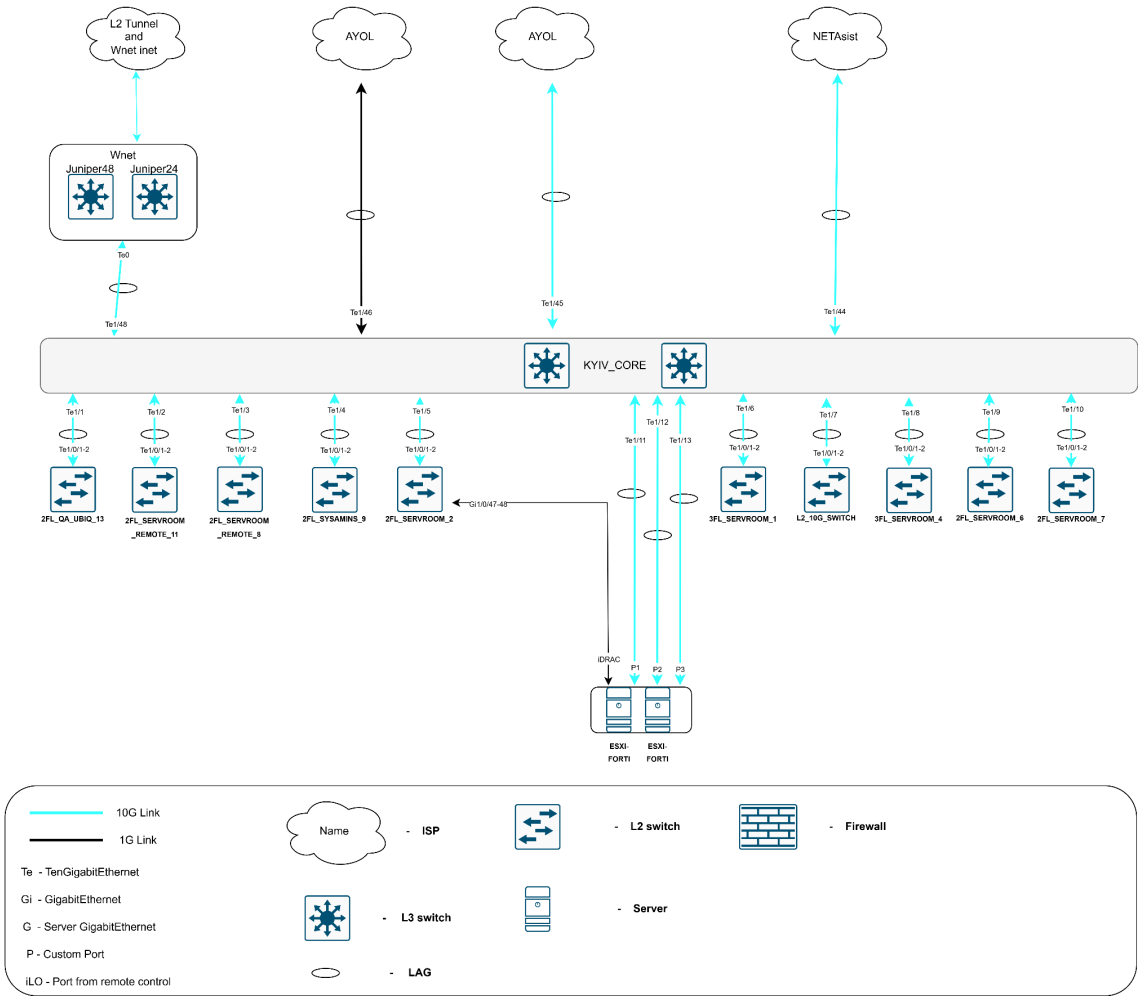


Рис. 3.1 Нова фізична схема мережі

У якості основного мережевого ядра використовується дві Cisco Catalyst C9500-48Y4C-A, що забезпечує комутацію на швидкості 10/40/100 Гбіт/с і підтримує розширені функції рівня L3, у тому числі OSPF, EIGRP, Policy-Based Routing, QoS та StackWise Virtual. Дане обладнання обране з огляду на його високу продуктивність і можливість масштабування для подальшого розвитку інфраструктури. Дані комутатори об'єднанні за допомогою технології StackWise Virtual.

На рівні доступу розгорнуті Cisco Catalyst C9300-48P-A, які забезпечують підключення кінцевих пристроїв, IP-телефонів і точок доступу Wi-Fi. Підтримка PoE+ дозволяє передавати живлення безпосередньо через Ethernet-кабель, що спрощує розгортання інфраструктури. Комутатори доступу з'єднані через 10G-

лінки для мінімізації затримок та дублюються до кожного з комутаторів ядра для збільшення відмовостійкості.

Віртуалізоване NGFW рішення FortiGate VM (8 ядер) розміщено на серверній інфраструктурі два DELL EMC PowerEdge R640 з наступними характеристиками:

- Intel(R) Xeon(R) Gold 6254 CPU @ 3.10GHz x2
- RAM 190GB
- Broadcom BCM57414 NetXtreme-E 10Gb/25Gb RDMA Ethernet Controller - 2 x 10Gbps
- Mellanox Technologies MT27710 Family [ConnectX-4 Lx] - 2 x 10Gbps
- Mellanox Technologies MT27710 Family [ConnectX-4 Lx] - 2 x 10Gbps

Працюють під керуванням VMware ESXI, утворюючи кластер з vSAN-сховищем для забезпечення відмовостійкості.
У разі виходу з ладу одного сервера, віртуальні машини Forti продовжують працювати на другому вузлі без втрати доступності.

На рисунку 3.2 наведено логічну схему корпоративної мереж, яка відображає взаємозв’язок VLAN-сегментів, зон безпеки, маршрутизацію трафіку та інтеграцію FortiGate з іншими системами.

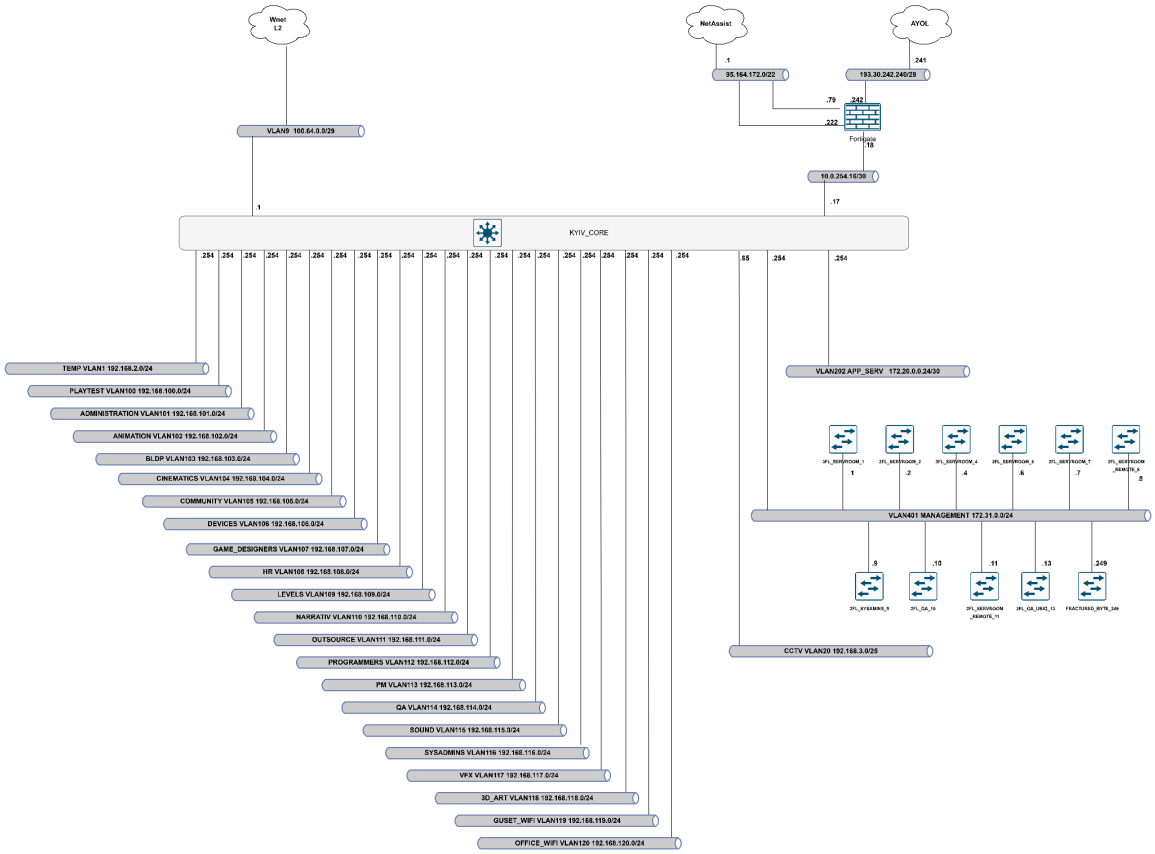


Рис. 3.2 Нова логічна схема мережі

У логічній структурі виділено такі зони:

- WAN - підключення до зовнішніх провайдерів (AYOL, NetAssist) через окремі канали. Трафік з Інтернету находиться. безпосередньо до FortiGate, де проходить первинну інспекцію.
- LAN - корпоративні VLAN-и, що об’єднують адміністративні, користувацькі, технічні та гостьові сегменти. Для кожного VLAN застосовані власні політики доступу та контролю.
- Secure Access / VPN - сегмент для віддалених користувачів, які підключаються через FortiClient VPN, керований сервером FortiEMS.
- DMZ - зона для публічних серверів (веб, VPN) ізоляція яка мінімізує ризик компрометації внутрішніх ресурсів.

Така побудова забезпечує принцип зональної безпеки (Zone-Based Security), де між зонами створюються чіткі правила маршрутизації й політики доступу. Наприклад, користувачі VPN мають обмежений доступ до службових ресурсів згідно з ролями.

Основою віртуалізаційної платформи є два сервери DELL EMC PowerEdge з процессорами Intel Xeon Gold та високошвидкісними SSD-дисками, об’єднані у спільне vSAN-сховище.
На обох вузлах встановлені VMware ESXI, а керування кластером виконується через vCenter Server.
Основні переваги такого рішення:

- Відмовостійкість: у разі збою одного вузла віртуальні машини автоматично переміщуються на інший сервер без втрати доступу.
- Масштабованість: у майбутньому можливо додати третій або четвертий сервер без зупинки роботи.
- Гнучкість керування: централізоване адміністрування ресурсів та моніторинг стану кластера.
- Продуктивність: завдяки апаратному прискоренню Intel VT-x/VT-d забезпечує швидка обробка мережевого трафіку без значного навантаження на CPU.

Розміщення NGFW у віртуальному середовищі також спрощує інтеграцію з іншими віртуальними сервісами без потреби у додатковому фізичному обладнанні.

Для забезпечення комплексного захисту у корпоративній мережі реалізована взаємодія між кількома продуктами Fortinet:

- FortiGate - основний міжмережевий екран, який виконує функції фільтрації, інспекції, IDS/IPS, VPN та антивірусного аналізу.
- FortiNAC - система контролю доступу до мережі, яка відповідає за автентифікацію пристроїв користувачів.
- FortiEMS - сервер управління клієнтами FortiClient, що забезпечує централізовану конфігурацію VPN, моніторингу стану безпеки кінцевих пристроїв, контроль версій ПЗ та дотримання політик.

Взаємодія між цими компонентами дозволяє реалізувати концепцію Zero Trust Network Access (ZTNA) - доступ надається лише автентифікованим і перевіреним користувачам, а всі дії мережі контролюються на рівні політики FortiGate.

3.3 Конфігурація FortiGate як NGFW

У межах реалізації модернізації системи безпеки корпоративної мережі було впроваджено міжмережевий екран нового покоління FortiGate VM, який функціонує під керуванням операційної системи FortiOS 7.4.9 (build 2829).

Основна розпочинає з базових налаштувань (налаштування інтерфейсів, політик та маршрутизації).
На рисунку 3.3 наведено налаштування інтерфейсів для двох ISP:

- NetAssist
- AYOL

Також конфігурація інтерфейса, який де в локальну мережу.

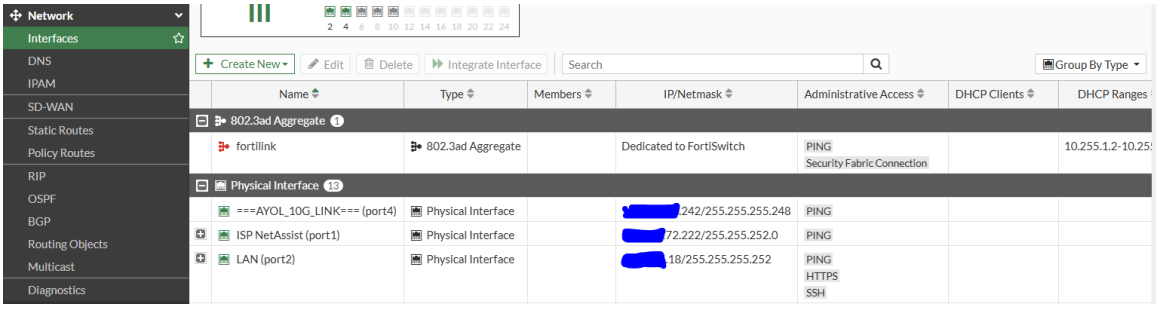


Рис. 3.3 Мережеві інтерфейси FortiGate

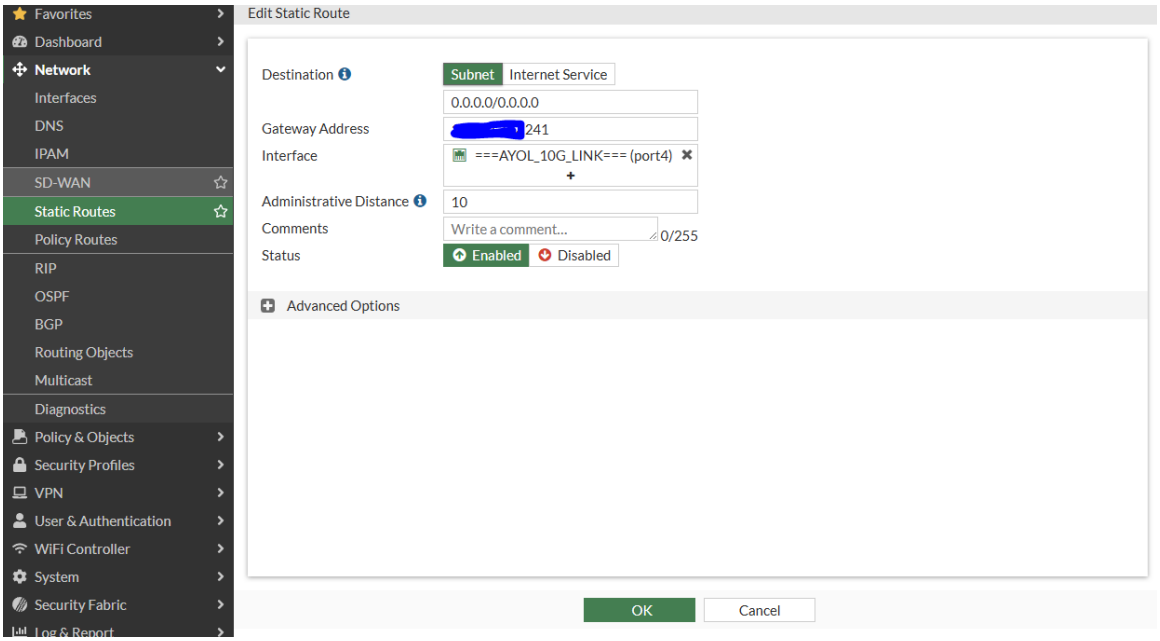


Рис. 3.4 Статичний маршрут

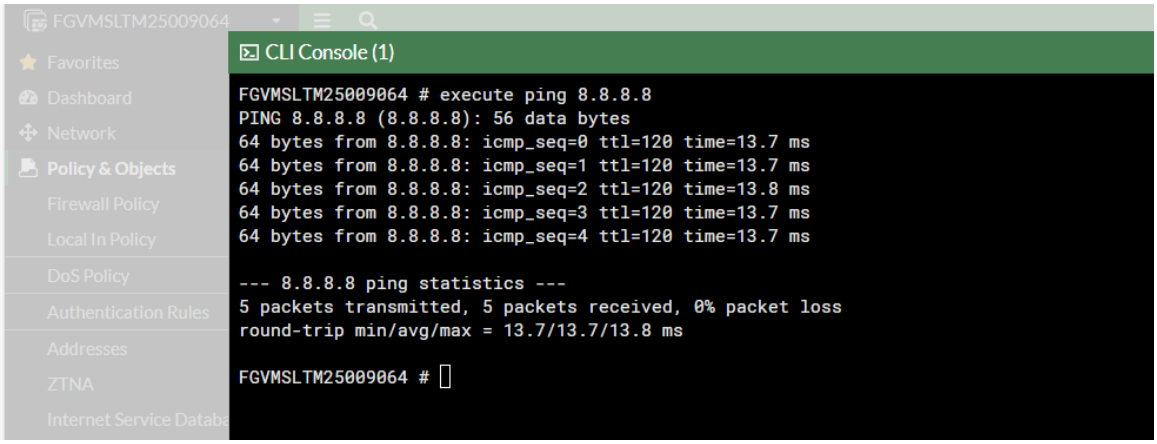


Рис. 3.5 Перевірка доступності публічних сервісів

Також потрібно прописати маршрут по замовчуванню щоб в NGFW був доступ в Інтернет та перевірити за допомогою інструментів доступ рисунок 3.4. і 3.5.

Після чого нам потрібно додати динамічну маршрутизацію між ядром та NGFW. Для цього нам потрібно підняти на обох пристроях протокол OSPF та налаштувати його.
По завершенню потрібно перевірити роботу і що сусідні пристрої бачать одне одного в “сусідах”. На рисунку 3.6 зображено встановлення сусідства по OSPF з боку ядра.

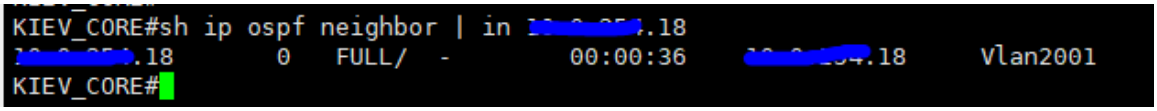
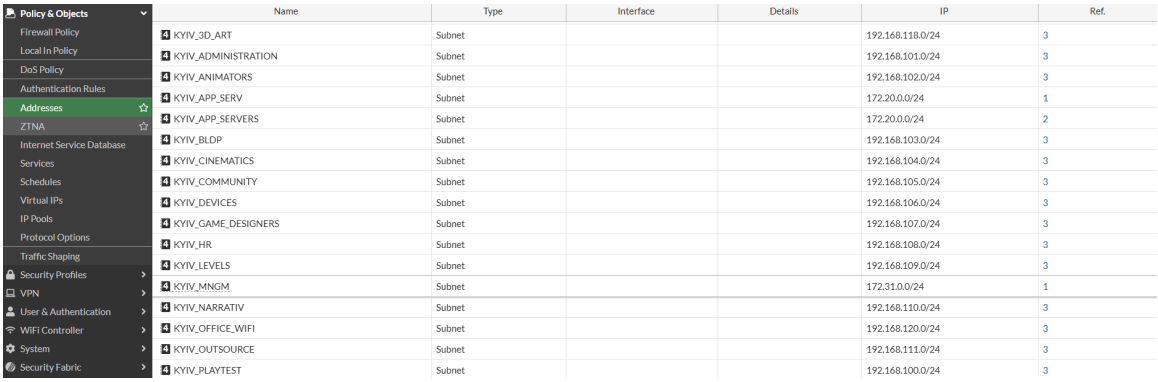


Рис. 3.6 OSPF сусідство

Наступним кроком є додавання підмережі користувачів щоб в майбутньому налаштовувати на них правила. Зображено на рисунку 3.7



Name	Type	Interface	Details	IP	Ref.
KYIV_3D_ART	Subnet			192.168.118.0/24	3
KYIV_ADMINISTRATION	Subnet			192.168.101.0/24	3
KYIV_ANIMATORS	Subnet			192.168.102.0/24	3
KYIV_APP_SERV	Subnet			172.20.0.0/24	1
KYIV_APP_SERVERS	Subnet			172.20.0.0/24	2
KYIV_BLDP	Subnet			192.168.103.0/24	3
KYIV_CINEMATICS	Subnet			192.168.104.0/24	3
KYIV_COMMUNITY	Subnet			192.168.105.0/24	3
KYIV_DEVICES	Subnet			192.168.106.0/24	3
KYIV_GAME_DESIGNERS	Subnet			192.168.107.0/24	3
KYIV_HR	Subnet			192.168.108.0/24	3
KYIV_LEVELS	Subnet			192.168.109.0/24	3
KYIV_MNGM	Subnet			172.31.0.0/24	1
KYIV_NARRATIV	Subnet			192.168.110.0/24	3
KYIV_OFFICE_WIFI	Subnet			192.168.120.0/24	3
KYIV_OUTSOURCE	Subnet			192.168.111.0/24	3
KYIV_PLAYTEST	Subnet			192.168.100.0/24	3

Рис. 3.7 База мереж в FortiGate

Одним з головних моментів є налаштування інспекції трафіку, так як від нього залежить функціонування всіх інших сервісів, оскільки саме цей процес безпосередньо впливає на ефективність виявлення загроз, контроль доступу та коректну роботу інших сервісів безпеки. У сучасних корпоративних мережах понад 80% трафіку передається у зашифрованому вигляді через протоколи SSL/TLS, тому без їхньої повноцінної інспекції жодна система безпеки не може забезпечити належний рівень захисту.

Шифрування трафіку є основним інструментом конфіденційності даних, однак воно створює значну проблему для систем захисту, які не мають змоги розшифрувати потік і проаналізувати його на наявність загроз. Без інспекції SSL/SSH протоколи контролю безпеки (IPS, антивірус, DLP, веб-фільтрація, контроль додатків) бачать лише зашифровані дані, тому шкідливий код, фішингові записи або несанкціоновані завантаження можу можуть проходити не поміченими. Саме для усунення цього ризику у FortiGate реалізований механізм Full SSL Inspection, який дозволяє розшифрувати, аналізувати та повторно шифрувати весь трафік, що проходить через NGFW.

Механізм повної інспекції SSL полягає у виконанні FortiGate ролі посередника (proxy) між клієнтом і сервером. Під час встановлення захищеного з’єднання NGFW перехоплює процес TLS-рукостискання, формує новий сертифікат від імені серверного ресурсу, підписує його внутрішнім сертифікатом FortiGate-SSL і передає клієнту. Таким чином, трафік між користувачем і FortiGate є зашифрованим, як і між FortiGate та зовнішнім сервером, проте сам міжвузловий потік у момент перевірки розшифровується для аналізу.

Така архітектура дозволяє здійснювати:

- Перевірку трафіку на віруси та шкідливі скрипти.
- Аналіз запитів до веб-ресурсів на відповідність політикам безпеки.

- Блокування фішингових та шкідливих сайтів.
- Контроль застосунків.
- Ідентифікацію користувачів.
- Застосування DLP-правил.

У проектованій архітектурі NGFW, трафік від користувачів надходить через доступові комутатори, з'єднані з ядром в мережі, де реалізовано агрегацію VLAN-ів. Саме на межі між внутрішньою корпоративною мережею та зовнішнім інтернет-сегментом розташований FortiGate, який виконує функції NGFW, VPN-шлюзу, SSL-інспекції.

На рисунку 3.8 наведено приклад конфігурації профілю "GSC_KYIV_INSPECTION_DEEP", який використовується для реалізації глибокої інспекції трафіку.

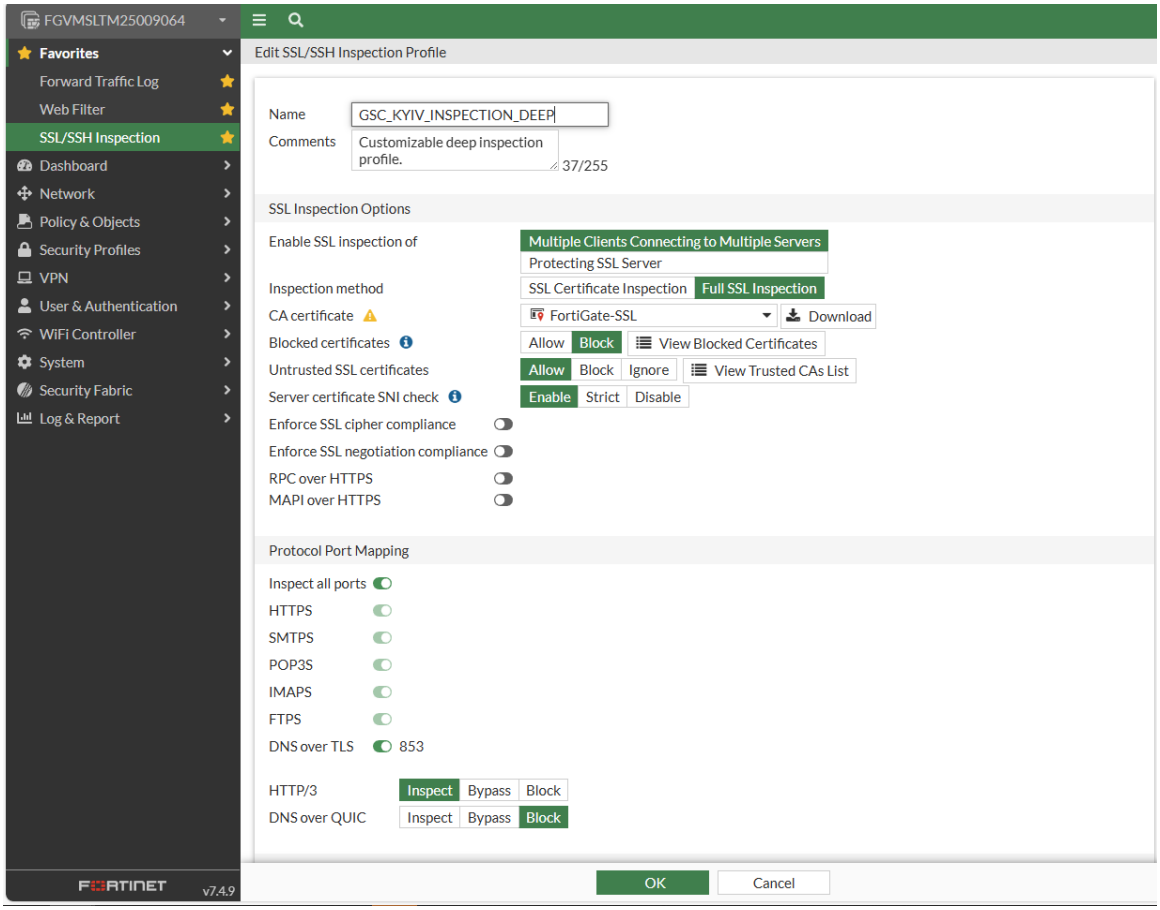


Рис. 3.8 Налаштування SSL інспекції

У даному профілі використано такі ключові параметри:

- Enable SSL inspection of Multiple Clients Connecting to Multiple Servers – режим, який передбачає перевірку з’єднань численних користувачів до зовнішніх ресурсів, що відповідає реальній моделі трафіку в корпоративній мережі.
- Inspection method: Full SSL Inspection – обрано режим повної інспекції із розшифруванням усіх TLS-сесій.
- CA certificate: FortiGate-SSL – використовується згенерований сертифікат для FortiGate, який повинен бути встановлений у сховище довірених сертифікатів на клієнтських ПК через групову політику (GPO). Це дозволяє уникнути попереджень браузера про недійсні сертифікати.
- Blocked certificates: Block – усі заблоковані або відкликані сертифікати блокуються, що унеможливлює підключення до потенційно небезпечних ресурсів
- Untrusted SSL certificates: Allow/Block – задає поведінку при спробі підключення до сайтів із самопідписаними сертифікатами.
- Server certificate SNI check: Enable – увімкнення перевірки Server Name Indication для виявлення підміни DNS або SSL-spoofing.
- Protocol Port Mapping – активовано перевірку всіх портів, зокрема HTTPS, SMTPS, IMAPS, FTPS, DNS over TLS, HTTP/3 та QUIC.

Завдяки такій конфігурації FortiGate виконує повноцінну перевірку усього зашифрованого трафіку, включно з новими протоколами (HTTP/3, QUIC), що особливо важливо для сучасних веб-сервісів, які дедалі частіше переходять на UDP-базові TLS-механізми.

У випадку, якщо SSL-інспекція не використовується, NGFW втрачає видимість більшої частини трафіку. Зловмисники можуть використовувати HTTPs-тунелі для передавання шкідливого коду, а програми - обходити DLP та політики контролю доступу. Також IPS-механізм не здатні розпізнавати сигнатуру атак у зашифрованому потоці. Це створює хибне відчуття безпеки, коли мережа здається захищеною, але значна частина подій відбувається поза контролем систем моніторингу.

Після налаштування SSL можна переходити до налаштувань web-фільтрації. FortiGate дозволяє реалізувати багаторівневий підхід до управління доступом, поєднуючи мережеву сегментацію, логічну структуру підрозділів підприємства та централізовану аутентифікацію користувачів через Active Directory. Така модель забезпечує узгодження політик безпеки та спрощує адміністрування.

На першому рівні контроль доступу йде на сегментації мережі за VLAN. Кожен функціональний підрозділ компанії розташований у власній підмережі VLAN 114 - QA, VLAN 118 - 3D_ART, VLAN 115 - SOUND як в нашій мережі. Такий поділ дає змогу ізолювати трафік служб і спростити контроль безпеки на рівні міжмережевих політик.

Другий рівень реалізується за допомогою інтеграції FortiGate з Active Directory через LDAP. Під час а автентифікації користувач пристрій отримує інформацію про його належність до певної групи (Live QA, Xbox Compliance, Writing…) і на основі цього призначається відповідний Web-профіль. Таким чином, правила доступу прив’язуються не до конкретної IP-адреси чи VLAN, а до облікового запису користувача, що підвищує гнучкість систем. Саме такий метод ми впровадили в NGFW і приклади конфігурацій зображені на наступних рисунках:

- Рисунок 3.9 - приклад налаштування Web-фільтра для відділу “Writing.
- Рисунок 3.10 - зображення створених інших Web-фільтрів для кожного відділу.
- Рисунок 3.11 - прив’язка Web-фільтра до AD групи, в якій знаходяться користувачі.
- Рисунок 3.12 - групи AD в які додаються користувачі

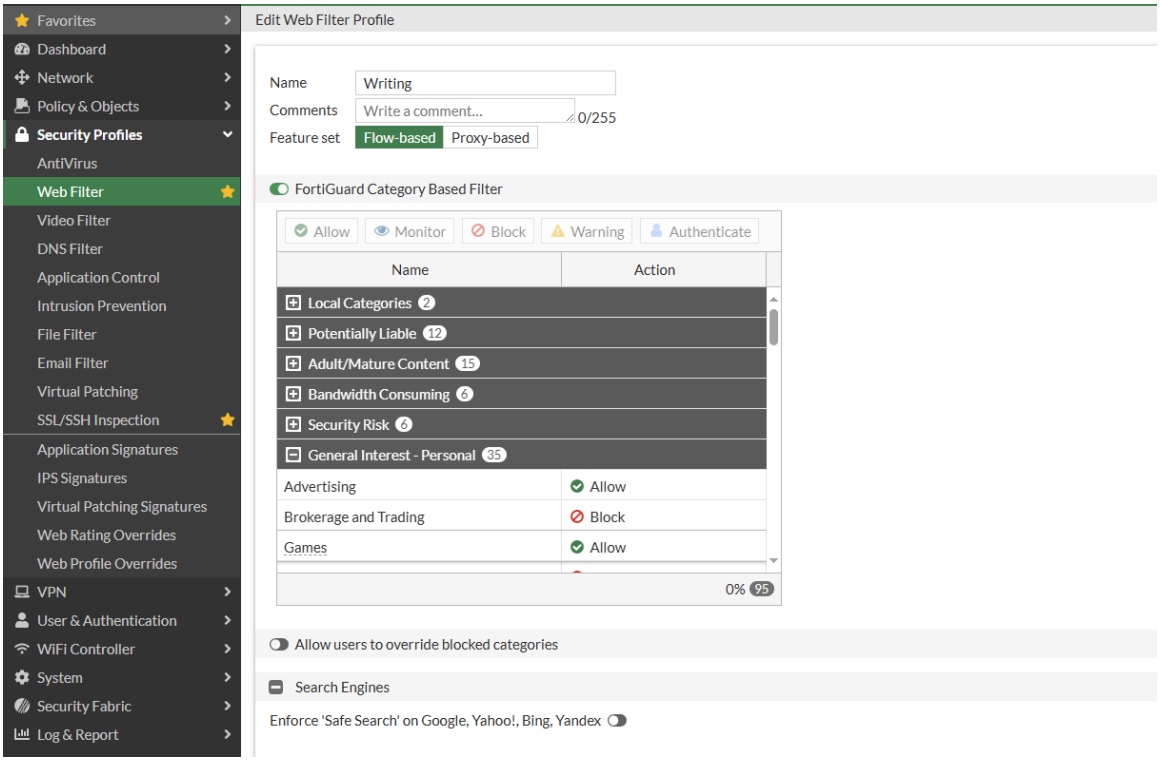


Рис. 3.9 Web-фільтр правила

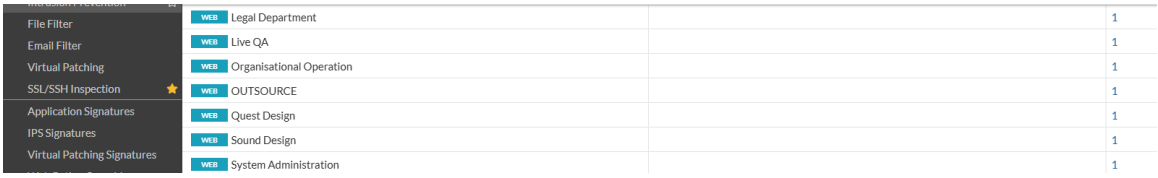


Рис. 3.10 Декілька web-фільтрів

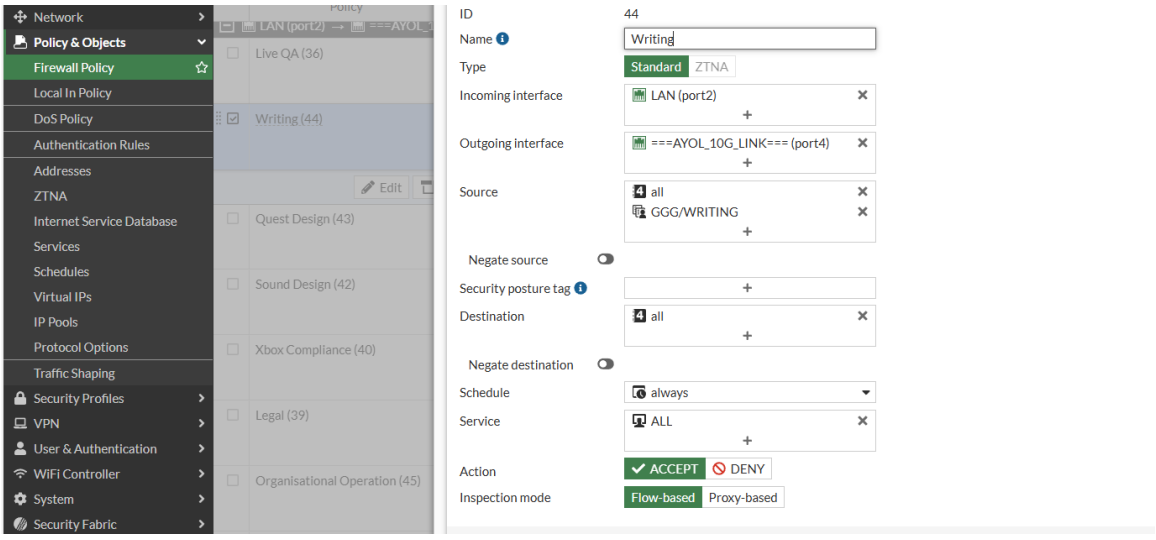


Рис. 3.11 FortiGate політика доступу в інтернет

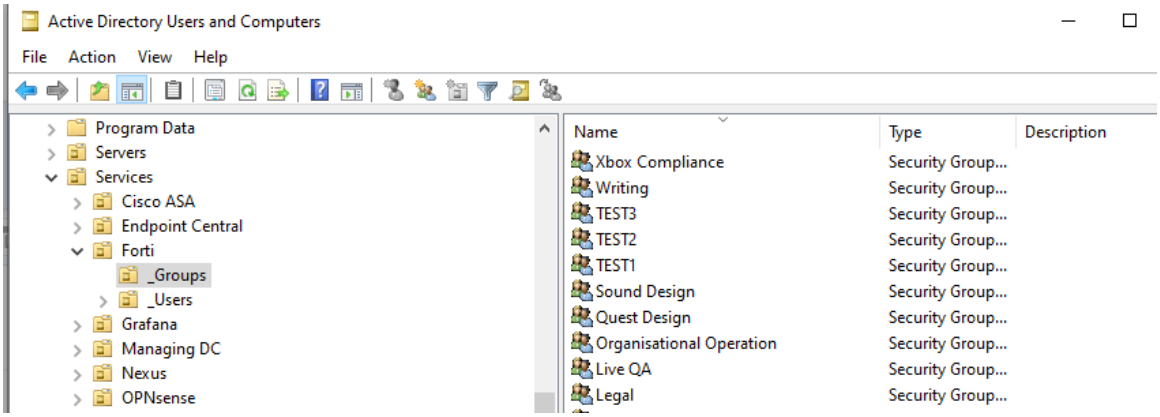


Рис. 3.12 Групи в Active Directory

Для забезпечення антивірусного контролю у корпоративній мережі використовується єдиний профіль антивірусного сканування, який застосовується для всіх груп компанії. Такий підхід дає змогу забезпечити єдиний стандарт безпеки. Робота антивірусного модуля виконується у flow-based режимі, що дозволяє здійснювати перевірку файлів у потоці без буферизації трафіку, тим самим мінімізуючи затримку у роботі мережію. Цей режим оптимально підходить для середовищ із великим обсягом даних і високою пропускною здатністю.

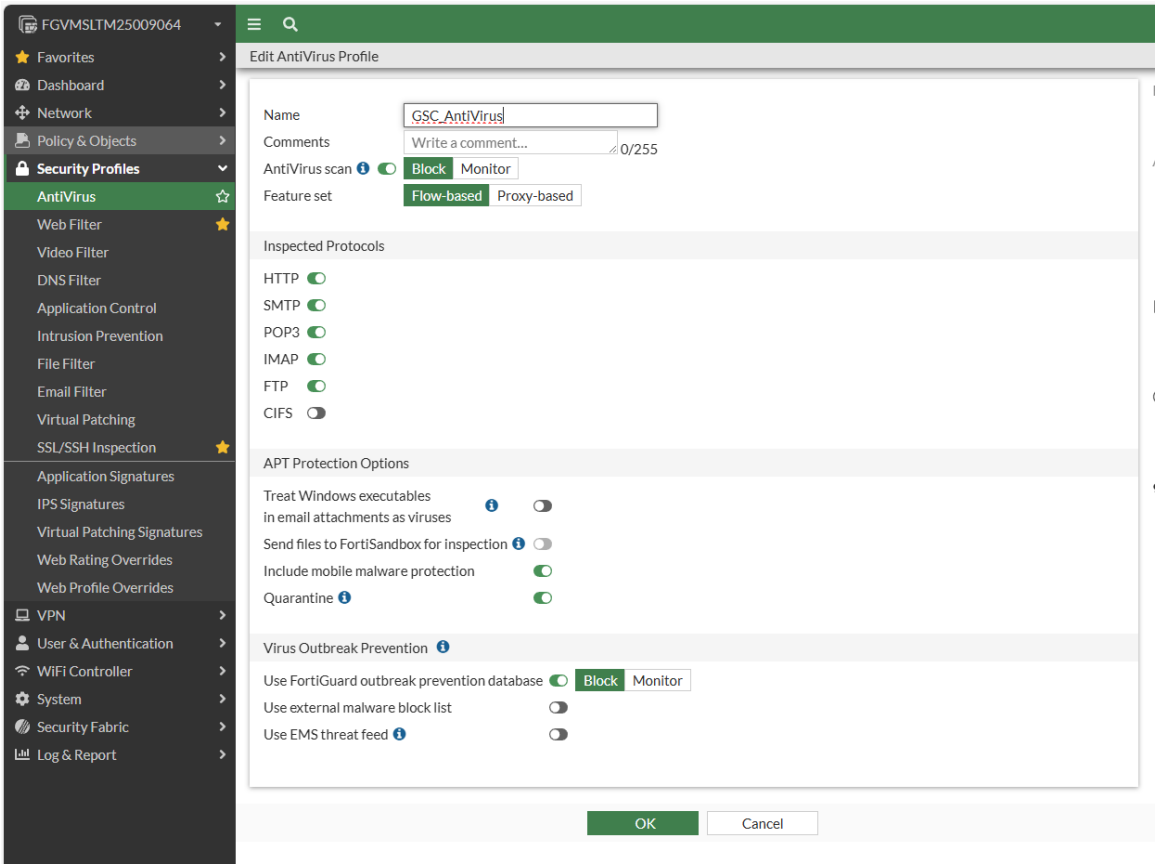


Рис. 3.13 AntiVirus політика

На рисунку 3.13 зображені параметри антивірусної перевірки:

- Режим: Flow-based (швидке потокове сканування).
- Перевіряються: HTTP, HTTPs, SMTP, POP3, IMAP, FTP.
- Інспекція: Scan compressed (до 10 рівнів вкладень).
- Дії: Block and log.
- Grayware detection: Enabled (виявлення потенційно небажаних програм).
- Heuristic scan: Enabled (поведінковий аналіз невідомих загроз).

Для всіх виявлених загроз FortiGate автоматично блокує передачу шкідливого об’єкта, а інформація про подію надсилається в журнал поїй. Це дозволяє адміністраторам відстежувати статистику виявлень, аналізувати тенденцій заражень і своєчасного реагування на інциденти.

DNS-фільтрація дозволяє контролювати запити до доменних імен і блокувати звернення до небезпечних або небажаних ресурсів ще до того, як відбувається встановлення з’єднання. Це дає змогу ефективно запобігати фішинговим атакам, командно-керуючим серверам (C&C), майнінговим сайтам та іншим загрозам, що поширюється через DNS-резолюцію. На рисунку 3.14 зображений один з DNS-фільтрів.

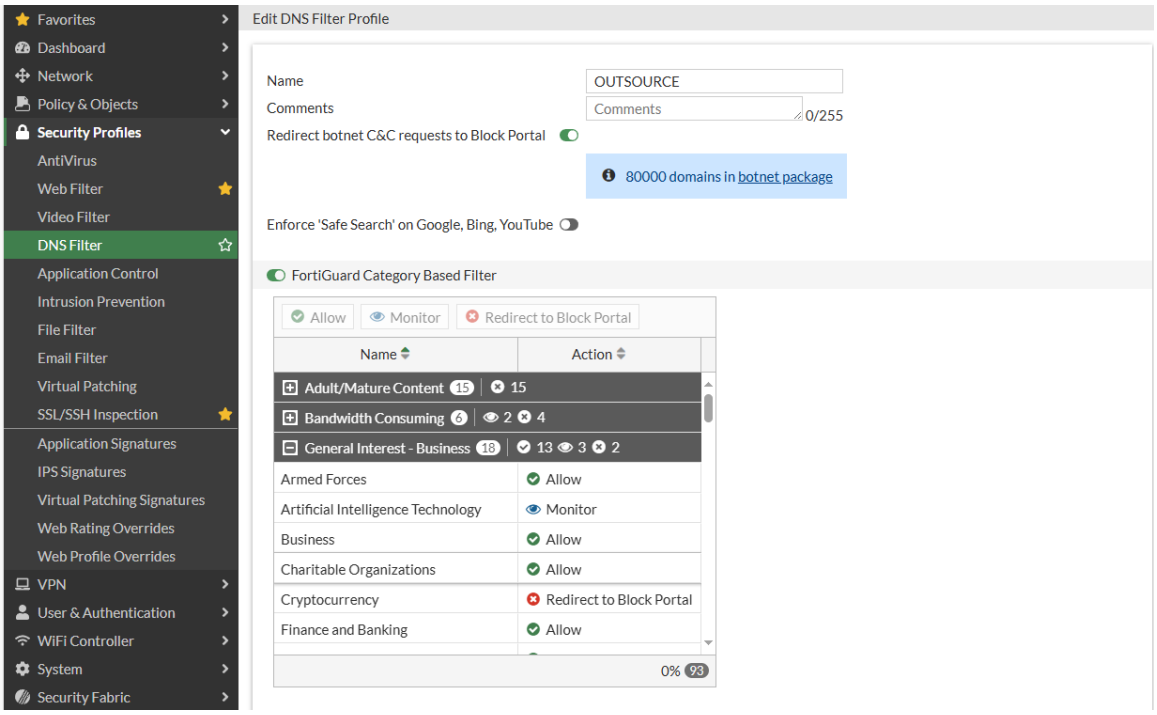


Рис. 3.14 DNS фільтр

Даний фільтр дозволяє не лише підвищити безпеку, але і забезпечити контроль продуктивності працівника, зменшуючи навантаження на інтернет-канал і мінімізуючи ризики витоку даних.

DNS-фільтрація інтегрована з антивірусним модулем: якщо домен у списку шкідливих, FortiGate блокує запит навіть до того, як буде отримано IP-адресу. Таким чином, користувач ніколи не може підключитись до ресурсу, який розповсюджує віруси та трояни, навіть якщо цей ресурс маскується під легітимний сайт.

Ще одним важливим елементом контентного захисту є Application Control, який дозволяє ідентифікувати програм за сигнатурою, незалежно від порту або протоколу, застосовувати політики для їх блокування або дозволу. На відміну від DNS-фільтрації, яка орієнтується на домени, Application Control працює на рівні ідентифікації додатків у мережевому потоці. Це дозволяє контролювати використання месенджерів, торрент-клієнтів, VPN-сервісів, ігор, програм віддаленого доступу тощо. На рисунку 3.15 зображено налаштування для одного з відділів.

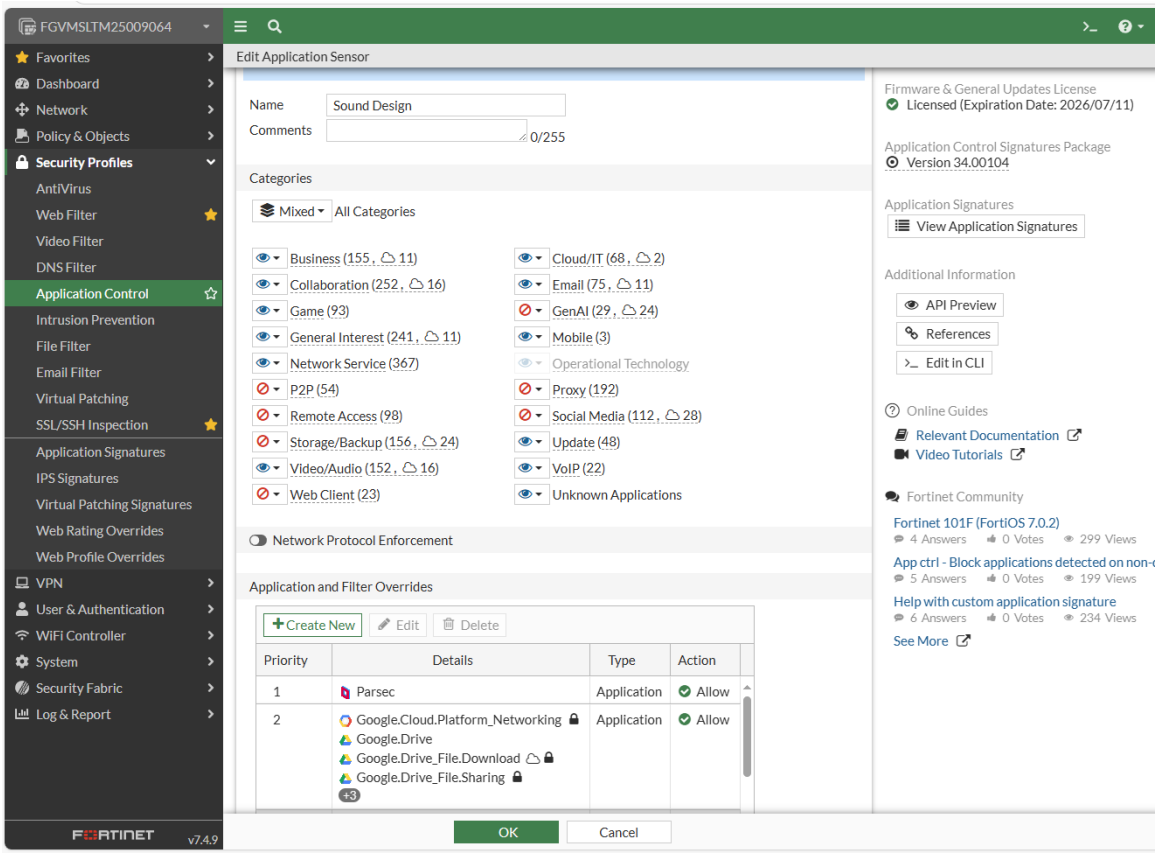


Рис. 3.15 Правила для програм

Як видно на зображенні, Application Control також має категорії по яким зручно створювати профайли. Для більш точної фільтрації, можна додатково ,поверх загальних категорій, додавати окремі програми і накидати на них правила.

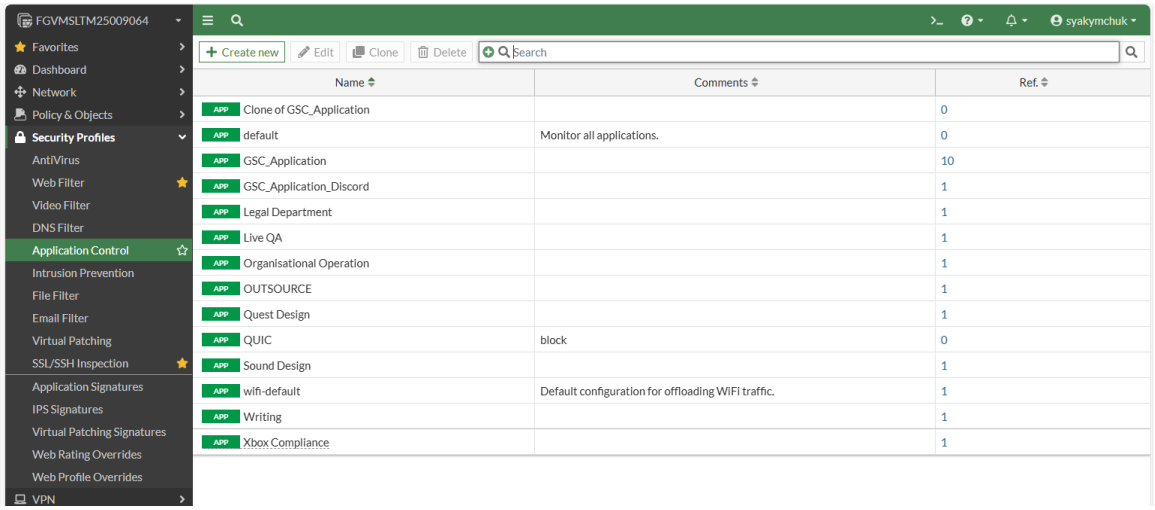


Рис. 3.16 Правила для інших відділів

Для кожного підрозділу створені індивідуальні профілі,рисунок 3.16. , адаптовані під характер виконуваних завдань:

- Гостьовий доступ: обмежено лише базовим веб-трафіком (HTTP/HTTPs) заборонено VPN, P2P, proxy-сервіси.
- Бухгалтерія: дозволені тільки сервіси електронного документообігу та бухгалтерські програми

Завершальним етапом являється підготувати Firewall правила для кожного відділу зображено на рисунку 3.17

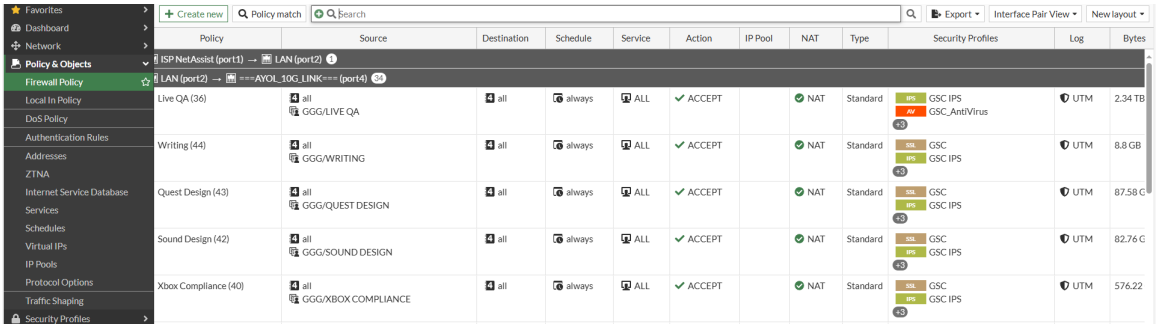


Рис. 3.17 Налаштовані правила для всіх підмереж

У результаті впровадження комплексних механізмів безпеки вдалось суттєво підвищити рівень захищеності корпоративної мережі. Реалізовані модулі - Antivirus, Web Filter, DNS Filter та Application Control. Вони забезпечують багаторівневий контроль мережевої активності, що дозволяє своєчасно запобігати більшість сучасних кіберзагроз.

Загалом, налаштування даних механізмів створює цілісну систему, у який кожен компонент виконує свою функцію: виявлення, запобігання, блокування, або контроль. У результаті користувачі отримали безпечне та стабільне середовище для роботи, а мережа - стійкість до зовнішніх загроз.

3.4 Розгортання VPN сервера на FortiGate

Для забезпечення безпечного віддаленого доступу до корпоративних ресурсів було розгорнуто VPN-сервер на базі FortiGate із використанням SSL-технологій. Основна мета впровадження цього рішення - надати співробітникам можливість працювати поза межами офісу, зберігаючи при цьому високий рівень інформаційної безпеки та дотримуватись корпоративних політик доступу. Одним з найголовніших правил в віддаленому доступі є те, що користувач має підключатись по VPN тільки з корпоративної техніки, адже тільки так можна впевнитись, що користувач не занесе шкідливі програми в локальну мережу компанії.
Тому в нашому випадку було використано дане правило і щоб воно працювало і мінімізувати шанс підключення не з корпоративної техніки було впроваджено багато рівні перевірки.

У межах побудови системи безпечного доступу одним із ключовим компонентів є FortiClient Endpoint Management Server (EMS). Цей сервер виконує роль централізованої платформи керування клієнтськими пристроями, що підключається до корпоративної мережі через VPN. Його інтеграція з FortiGate забезпечує повний контроль над кінцевими точками, перевірку їхньої відповідності політикам безпеки та автоматичних оновлень налаштувань для всіх користувачів.

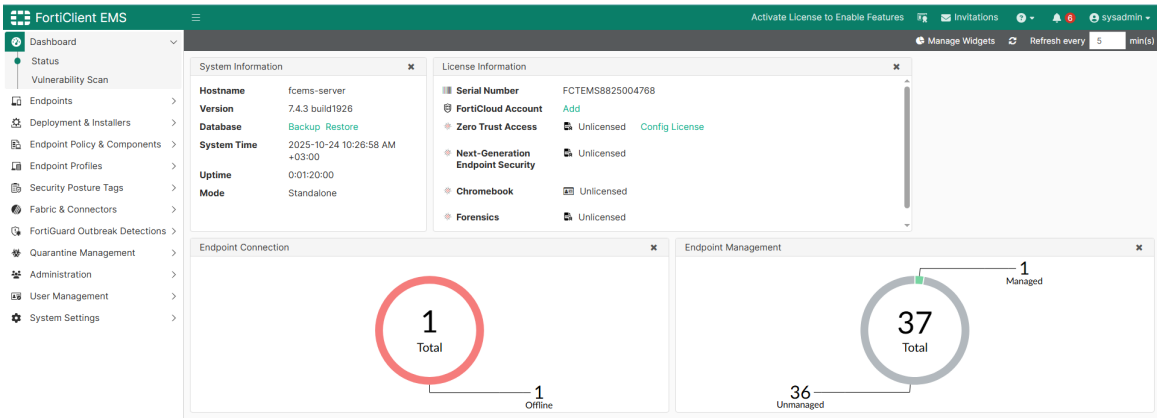


Рис. 3.18 FortiClient EMS головне вікно

На рисунку 3.18 зображено головне меню EMS з основними даними.

З самого початку потрібно розгорнути VPN сервер. Для цього потрібно мати публічну білу адресу та публічний сертифікат, щоб сервіс був довірений.

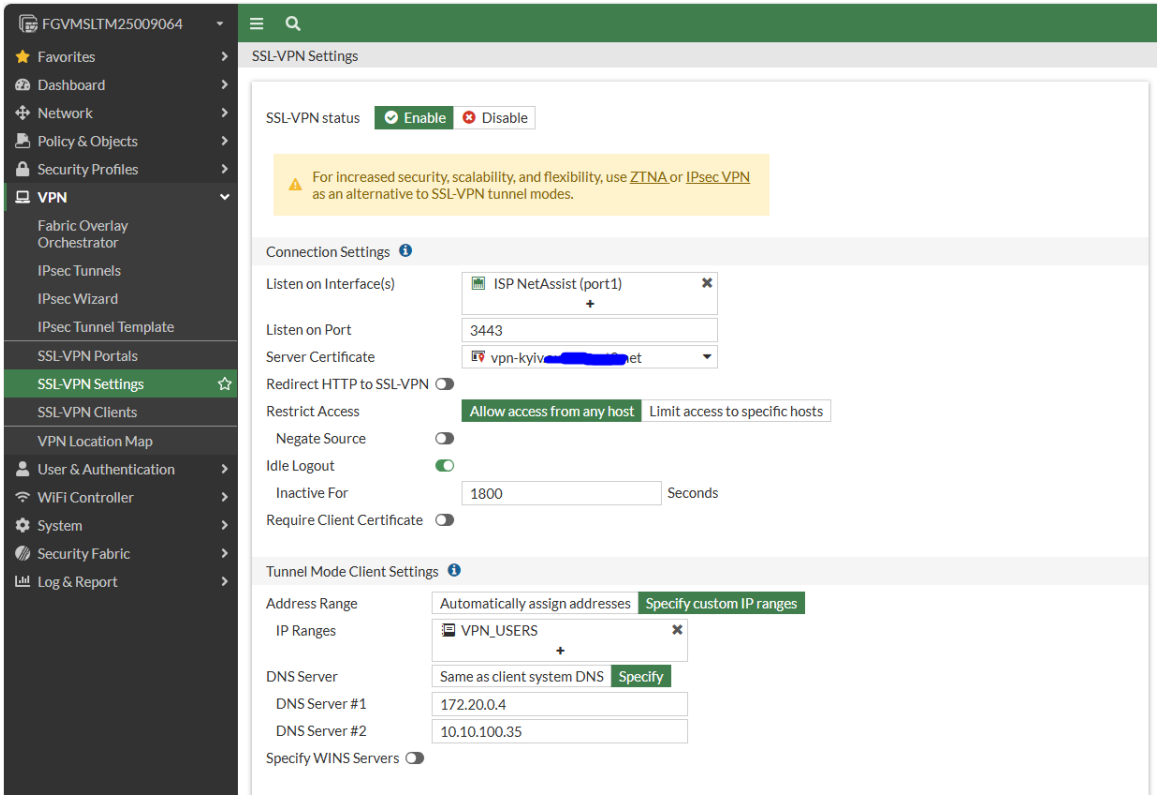


Рис. 3.19 FortiGate SSL VPN

На рисунку 3.19 зображено налаштований VPN сервер без політик та методів авторизації.

Перед тим, як налаштовувати метод авторизації, потрібно попередньо скласти план перевірки аби тільки користувачі з корпоративної техніки могли

підключатись.

В нашому випадку перевірка буде розділена, частину етапів перевірки буде проводити сам FortiGate, а частину EMS:

1. Перевірка належності ПК до домену AD.
   На етапі автентифікації FortiGate виконує запит до служби Active Directory, перевіряючи, чи входить комп'ютер до корпоративного домену. Якщо пристрій не є доменним, доступ відхиляється. На рисунку 3.20 дане правило підписано "set host-check-policy "Domain-GGG""
2. Перевірка шифрування дисків за допомогою Bitlocker.
   Ця перевірка здійснюється зі сторони сервера FortiClient EMS, який відстежує стан робочих станцій користувачів. На рисунку 3.21 зображено дане правило, "Windows Security Bitlocker disk Encryption is enabled on all disk"
3. Контроль наявності активного антивірусного захисту.
   EMS перевіряє, чи встановлений та запущений антивірус на робочій станції користувача. За відсутності активного антивірусу, доступ не надається.
4. Перевірка користувача в групі, яка дозволяє авторизацію по VPN
   FortiGate отримує інформацію з AD про наявність користувача у спеціальній групі, яка дозволяє VPN-доступ. Якщо користувач не включений до цієї групи, автентифікація завершується з помилкою
5. Перевірка належності користувача до дозволених OU
   Додатково виконується перевірка користувача, в якій OU він знаходиться, щоб на базі цих даних надати йому доступ до необхідних ресурсів.

```
FGVMSLTM25009064 (Information Security) # show
config vpn ssl web portal
    edit "Information Security"
        set tunnel-mode enable
        set ip-pools "TEST2"
        set split-tunneling disable
        set host-check custom
        set host-check-interval 120
        set host-check-policy "Domain-GGG"
        set customize-forticlient-download-url enable
        set windows-forticlient-download-url "https://vpn-kyiv.[redacted]/download"
        set macos-forticlient-download-url "https://vpn-kyiv.[redacted]/download"
    next
end

FGVMSLTM25009064 (Information Security) #
```

Рис. 3.20 FortiGate політики перевірки VPN

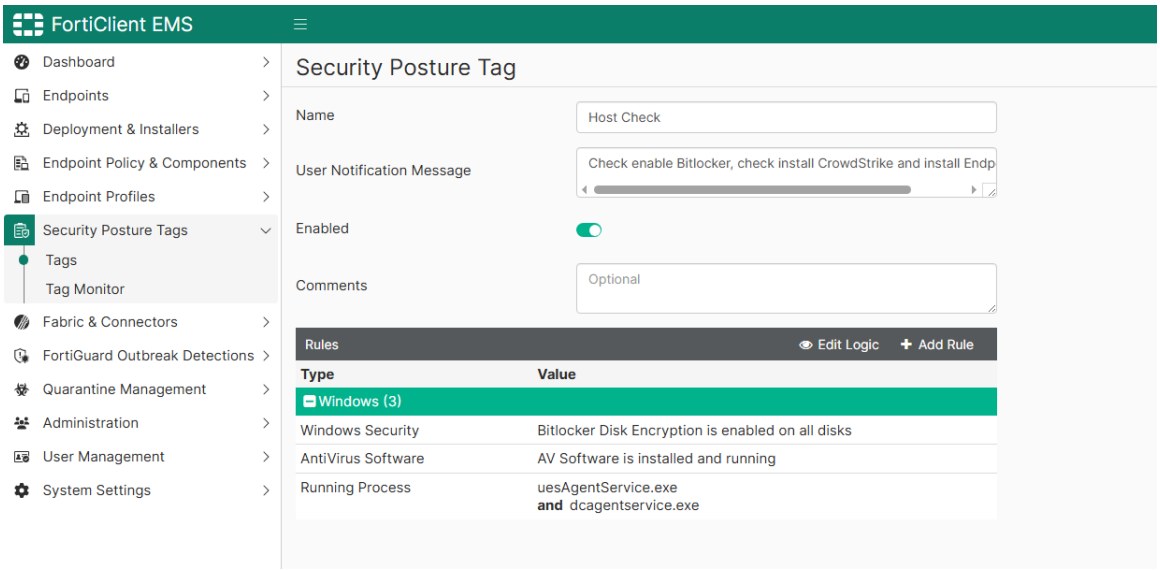


Рис. 3.21 FortiClient EMS політики перевірки VPN

Лише у разі успішного проходження всіх перевірок, користувачу надається доступ до VPN. Після автентифікації FortiGate автоматично застосовує відповідні політиики доступу які визначають обсяг прав і сегменти мережі, до яких користувач може підключитися. Розмежування доступу виконується на основі належності до підрозділу, групи AD та ролі користувача. Логіка доступу зображена на рисунку 3.22, 3.23 та 3.24 де користувачі після успішної авторизації переходять на відповідний портал, на якому вже заздалегідь створені правила доступу

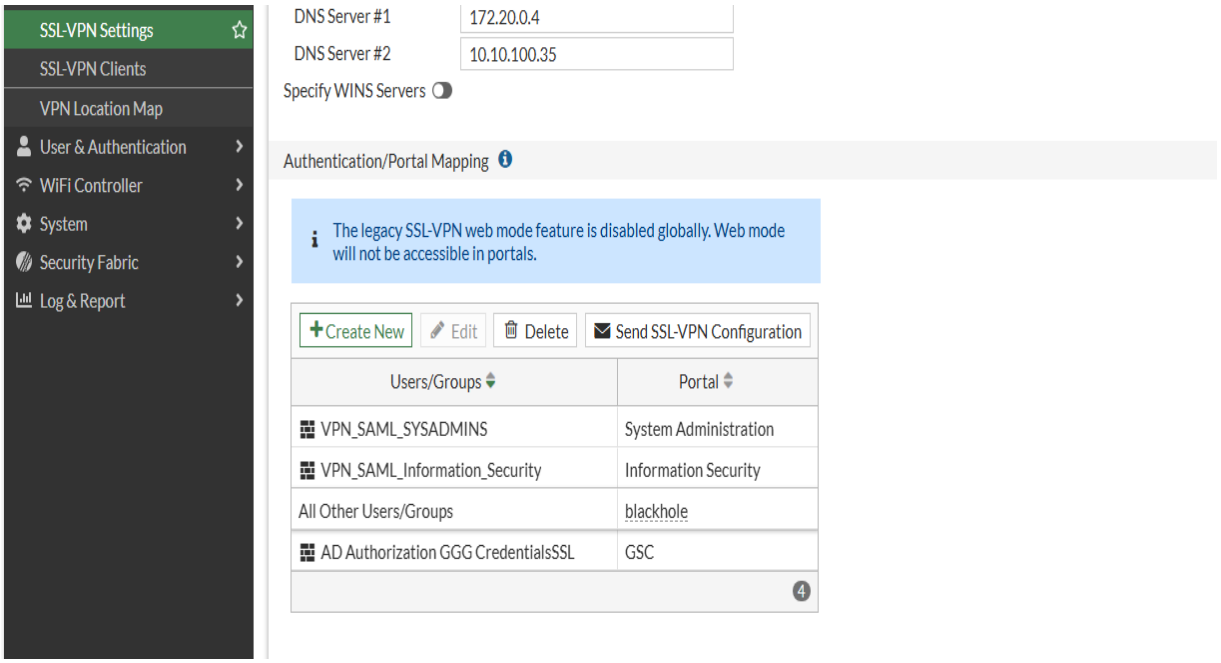


Рис. 3.22 VPN політики доступу

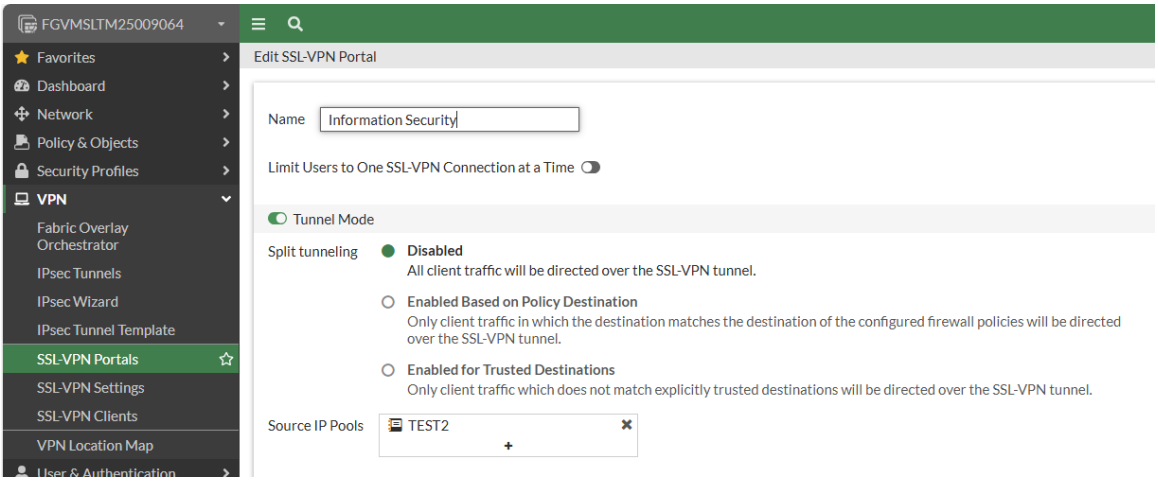


Рис. 3.23 VPN налаштування портала

Для централізованого управління клієнтами VPN було розгорнуто FortiClient EMS - сервер керування кінцевими точками, який дозволяє створювати політики безпеки, генерувати інсталятори FortiClient і автоматично поширювати оновлення конфігурації. Завдяки інтеграції з EMS адміністратор може вносити зміни до політик перевірки, які автоматично синхронізуються з усіма віддаленими клієнтами без потреби ручного втручання.

Технологія SSL VPN, що застосовується у цьому рішенні, забезпечує захищені з'єднання між користувачем та корпоративною мережею через стандартні HTTPs-порти, що дозволяє уникнути блокування з боку провайдерів. Усі дані шифруються за допомогою сучасних криптографічних алгоритмів, що гарантує конфіденційність переданих даних.

Для підвищення зручності користувачів і скорочення часу підключення до корпоративних ресурсів було реалізовано автоматичної авторизації VPN за допомогою функції Windows BeforeLogin. Зображено на рисунку 3.23, ця технологія дозволяє встановлювати VPN-з'єднання ще на етапі входу користувача у систему Windows — до завантаження його профілю. У такому режимі клієнт FortiClient запускається автоматично та виконує автентифікацію користувача через AD, використовуючи облікові дані домену. Після успішного проходження перевірок FortiClient встановлює зашифроване SSL VPN-з'єднання з FortiGate, що дозволяє робочій станції відразу отримати доступ до контролера домену, файлових серверів і внутрішніх служб.

Завдяки цьому користувачі можуть входити до своїх доменних облікових записів навіть під час віддаленої роботи — без необхідності попереднього ручного запуску VPN-клієнта. Усі етапи перевірки безпеки (наявність антивірусу,

шифрування дисків, членство у домені) виконуються автоматично відповідно до політик, заданих у FortiClient EMS.

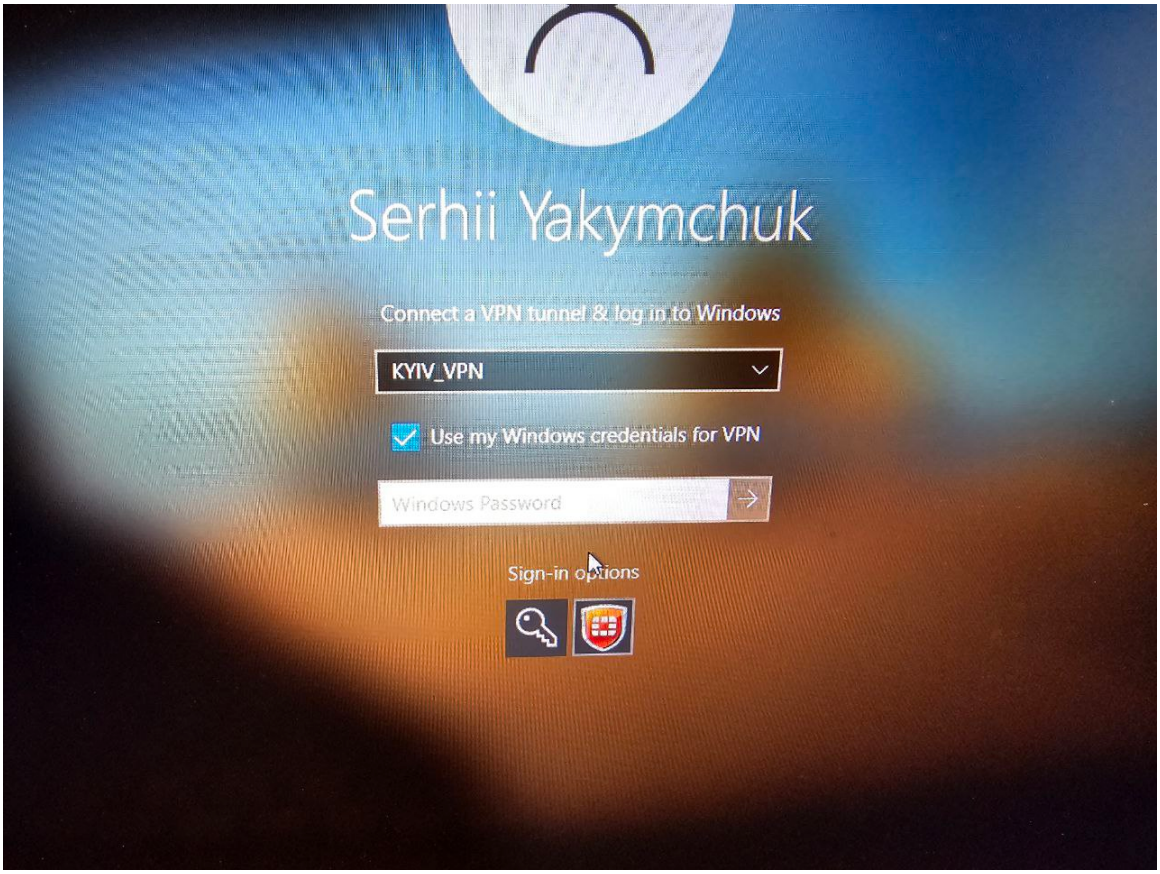


Рис. 3.24 Авторизація VPN перед авторизацією в Windows

3.5 Розгортання NAC системи на базі FortiNAC

Одним із ключових елементів захисту корпоративної мережі є контроль доступу до інформаційних ресурсів. Зі збільшенням кількості підключених пристроїв, виникає потреба у впровадження Network Access Control (NAC). Для побудови комплексної моделі контролю доступу на підприємстві було обрано рішення FortiNAC, Яке забезпечує централізоване керування підключенням користувачів і пристроїв до мережі, перевірку відповідності політикам безпеки, а також автоматичну реакцію на інциденти безпеки.

FortiNAC — це спеціалізована система Network Access Control, яка забезпечує ідентифікацію, авторизацію та контроль доступу всіх користувачів і пристроїв, що підключаються до корпоративної мережі. Вона є фундаментальним елементом моделі Zero Trust у локальній мережі, забезпечуючи контроль на другому та

третьому рівнях OSI.
FortiNAC підтримує дві базові моделі роботи:

1. L2 NAC (Layer 2 Control)
   Контроль на рівні комутаторів доступу:
   a. Моніторинг MAC-адрес;
   b. Контроль стану портів;
   c. Port Security;
   d. VLAN-хендінг;
   e. Автоматична міграція хоста в потрібний VLAN;
   f. Реакція в режимі реального часу

   L2 NAC працює через SNMP read/write, SSH CLI та API доступу. Це дозволяє визначати, до якого порта підключений пристрій та динамічно розмістити його у VLAN залежно від ролі.

2. L3 NAC (Layer 3 Control)
   Використовується, коли пристрої підключаються через маршрутизовані сегменти.
   L3 NAC застосовує:
   a. APR-таблиці;
   b. DHCP Snooping дані;
   c. Інтеграцію з Firewall;
   d. Агентську перевірку (Persistent/Agent-based posture).

   Переваги такої системи - це можливість застосування політик без прив’язки до фізичного порта та контроль навіть у великих та розподілених мережах.

   Основною метою впровадження FortiNAC є створення архітектури Zero Trust Access, де кожен пристрій та користувач проходить ідентифікацію, перевірку безпеки та отримує доступ лише до дозволених сегментів мережі.

В даній системі існує два методи автентифікації:

1. 802.1X -найнадійніший метод контролю доступу.
   Процес:
   a. Пристрій підключається до порта комутатора.
   b. Комутатор виконує роль authenticatior.
   c. FortiNAC (через RADIUS) виступає authentication server.
   d. При успішній автентифікації користувач отримує доступ до корпоративного VLAN.

Переваги такого методу:

- Прив’язка до користувача;
- Захист від підміни;
- Можливість динамічної VLAN-авторизації.

2. MAB (MAC Authentication Bypass)
   Використовується для пристроїв без 802.1X:
   a. Принтери;
   b. IP-телефони;
   c. IoT пристрої;
   d. Камери відеоспостереження.

Комутатор передає MAC адресу пристрою в RADIUS сервер, дк FortiNAC шукає MAC у своїй базі. Якщо MAC дозволений, то пристрою призначається VLAN, а в іншому разі поміщається в Guest або Quarantine VLAN.

Розгортання FortiNAC включає кілька послідовних етапів:

1. Інсталяція та базова конфігурація
   a. Встановлення FortiNAC на кластері ESXI
   b. Налаштування мережевих параметрів
   c. Підключення до домену Active Directory
2. Інтеграція з мережевим обладнанням Cisco
   a. Додавання комутаторів Catalyst 9300
   b. Налаштування SNMP, SSH та API-доступу
   c. Активація RADIUS-авторизації для портів
3. Налаштування політик підключення
   a. Політики доступу для корпоративних пристроїв
   b. Окремий гостьовий портал
4. Реалізація 802.1X
   a. RADIUS у FortiNAC
   b. Встановлення сертифікатів
   c. Розгортання GPO на робочі станції Windows
5. Тестування і введення в експлуатацію
   a. Тестування сценаріїв підключення
   b. Перевірка карантинного доступу
   c. Моніторинг логів і адаптація профілів

На рисунках 3.24 - 3.28 наведено інтерфейси системи FortiNAC, що демонструють ключові елементи конфігурації та моніторингу доступу до мережі.

На рисунку 3.25 відображено список активних мережевих хостів та інформацію про їхній статус: IP-адреси, MAC-адреси, ім’я пристрою, користувачі, VLAN, комутатори і порти, через які здійснено підключення. Такий вигляд дозволяє оперативно визначити:

- До якої мережевої зони підключений пристрій;
- Який користувач авторизований під цим хостом;
- Статус доступу;

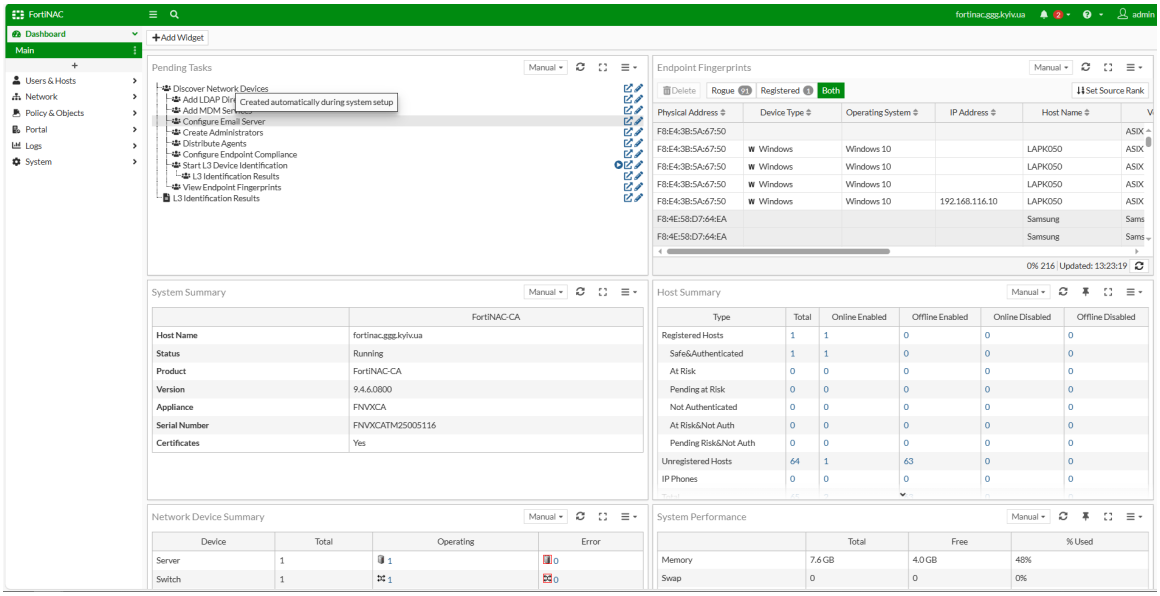


Рис. 3.25 FortiNAC головне меню

Рисунок 3.26 демонструє конфігурацію Port Security Policies та інтеграцію з комутаторами Cisco Catalyst рівнів ядра та доступу. За допомогою SNMP та SSH FortiNAC може автоматично:

- Блокування та розблокування порта;
- Переміщувати пристрій у quarantine VLAN;
- застосовувати 802.1X або fallback-авторизацію по MAC.
- запускати механізм повторної аутентифікації (re-auth);

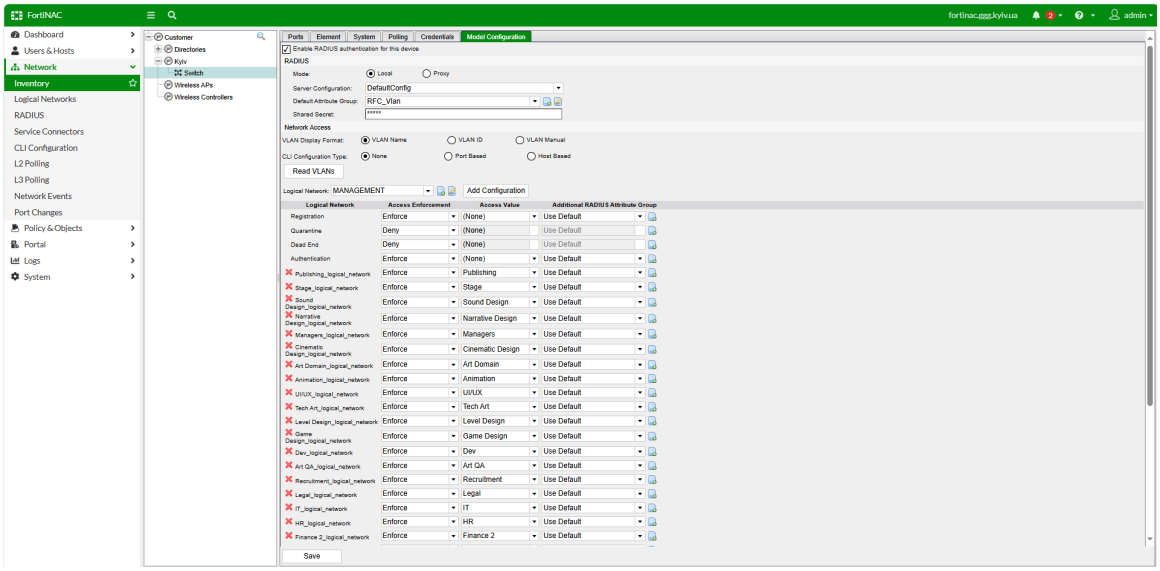


Рис. 3.26 FortiNAC нарізані мережі доступу

На рисунку 3.27 показано детальний опис пристрою: інформація про ОС, роль користувача, метод авторизації

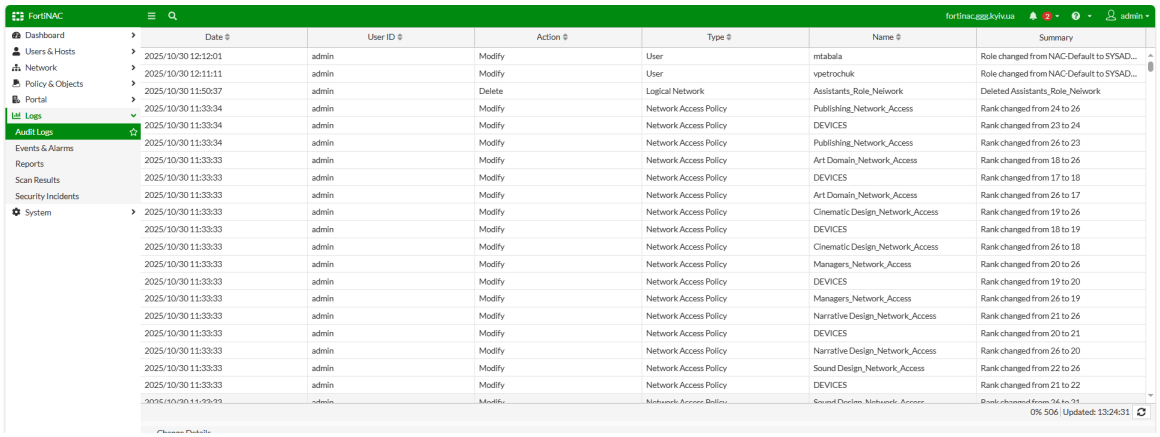


Рис. 3.27 FortiNAC пристрої

На рисунку 3.28 наведені політики Automatic VLAN Assignment та Role Mapping Rules. Система автоматично визначає, до якої групи відноситься пристрій (Finance, Administration, IT…) та призначає VLAN згідно з корпоративною матрицею доступу.
Це підтверджує реалізацію Role-Based Access Control (RBAC) та динамічної сегментації мережі.

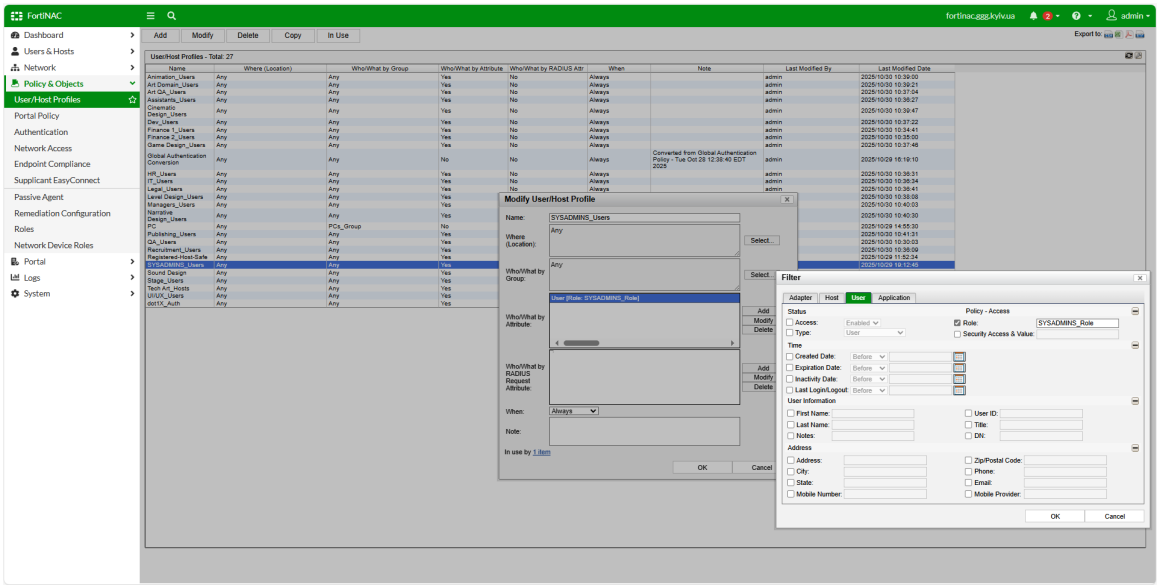


Рис. 3.28 FortiNAC політики доступу

На рисунку 3.29 зображено статус портів та налаштування портів в реальному часі. Історію надання доступу та номер VLAN, який доступний.

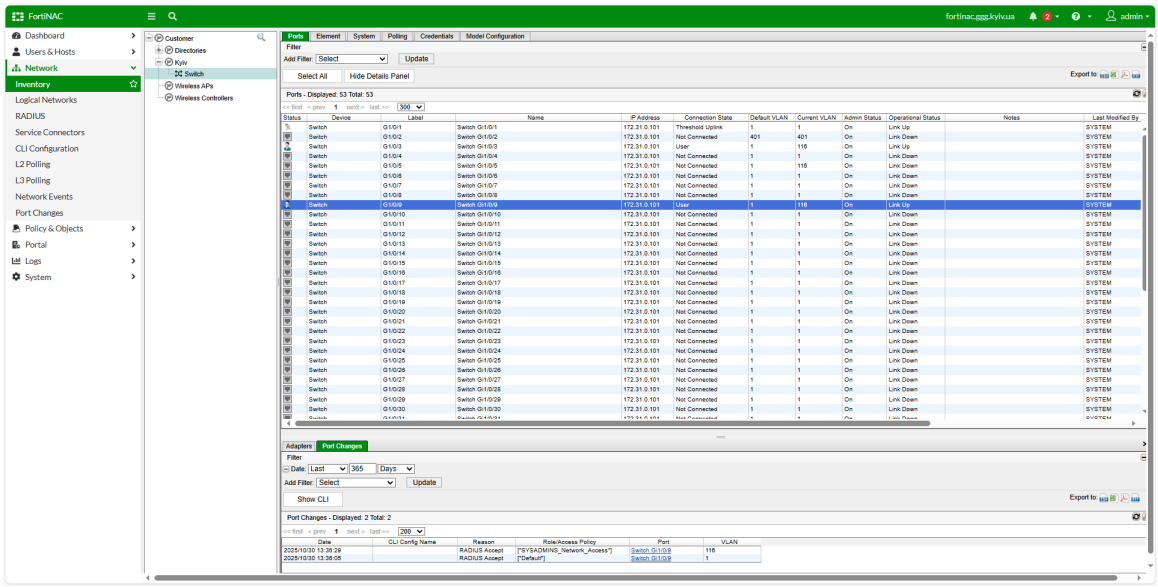


Рис. 3.29 Статус портів через FortiNAC

У результаті впровадження системи контролю доступу до мережі FortiNAC у корпоративному середовищі було реалізовано комплексний підхід до забезпечення безпечної авторизації та сегментації пристроїв. Система забезпечує перевірку користувачів і кінцевих вузлів на основі ролей, політик безпеки та технічних

характеристик пристрою, що дозволяє мінімізувати ризики несанкціонованого доступу до критично важливих ресурсів.

3.6 Розгортання Oxidized

У процесі побудови комплексної системи моніторингу та управління корпоративною інфраструктурою одним із ключових завдань стало впровадження сервісу для автоматизованого резервного копіювання конфігурацій мережевого обладнання. Для цього було розгорнуто систему Oxidized – відкриту платформу, що підтримує протоколи SSH та Telnet і забезпечує централізоване збереження версій конфігурацій комутаторів, маршрутизаторів і міжмережевих екранів. Oxidized було встановлено на окремому сервері під керуванням операційної системи Linux. Під час інсталяції використано стандартний пакетний менеджер, після чого виконано базове налаштування середовища Ruby та веб інтерфейсу. Доступ до сервісу реалізовано через протокол HTTPS із попередньою автентифікацією користувачів.
На рисунку 3.30 зображено головну сторінку та мережеве обладнання, з якого зберігаються конфігурації.

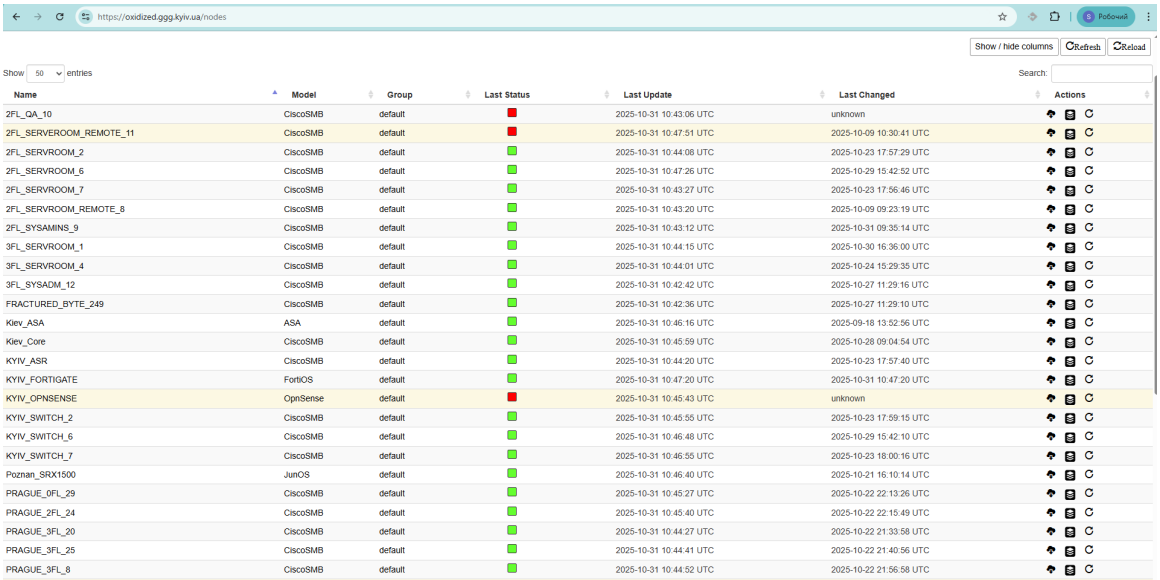


Рис. 3.30 Oxidized пристрої з яких скачується конфігурація

Підключення до мережевого обладнання здійснюється через SSH із використанням облікових даних адміністратора. Для кожного пристрою у конфігураційному файлі

router.db зазначено IP-адресу, тип обладнання та метод аутентифікації. Система автоматично опитує задані пристрої за розкладом, завантажує їхні поточні конфігурації та порівнює з попередніми версіями. У разі змін різниця зберігається у системі контролю версій Git, що дозволяє відстежувати історію правок і швидко відновлювати попередній стан конфігурацій.

Рисунок 3.32 зображено приклад змін, які Oxidized виділя, щоб було зручніше виявляти помилки та швидко все виправити або повернути назад. Рисунок 3.31., зображено збережено окремо кожні зміни.

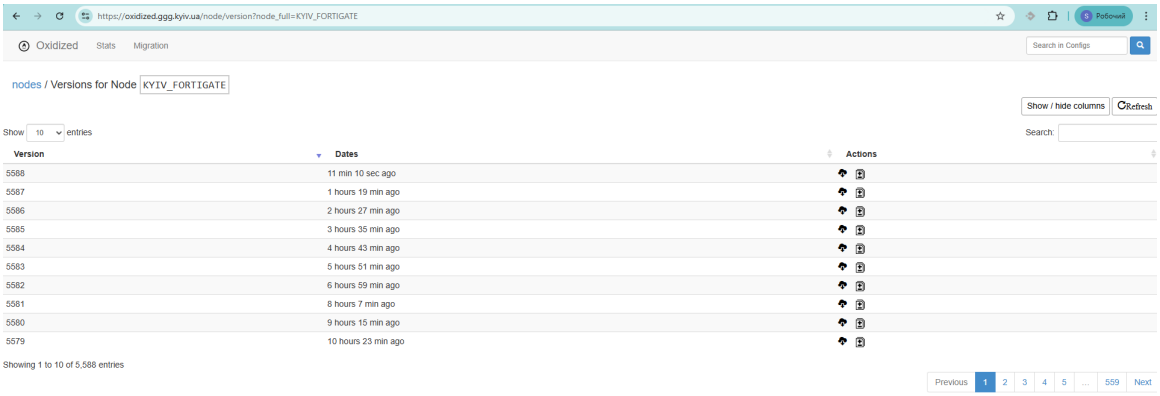


Рис. 3.31 Oxidized історія змін

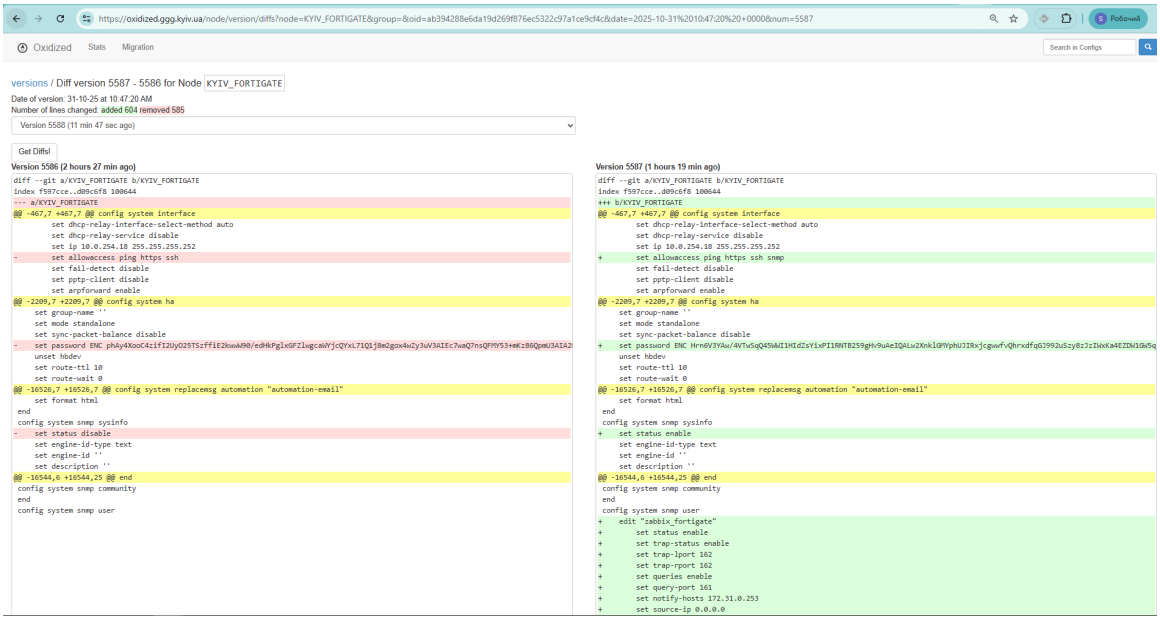


Рис. 3.32 Oxidized різниця конфігів

Oxidized було інтегровано з корпоративною мережею через окремий VLAN для адміністративного доступу, а результати резервного копіювання дублюються на сервер архівів. Такий підхід унеможливлює втрату налаштувань мережевого обладнання у випадку апаратних збоїв, некоректних оновлень або людських помилок.

Впровадження Oxidized забезпечило централізоване управління конфігураціями, автоматизацію процесів збереження та підвищення загальної надійності мережевої інфраструктури. Завдяки цьому адміністратор може оперативно відновити будь-яку версію конфігурації пристрою, що значно скорочує час усунення неполадок і підвищує рівень контролю змін у системі.

3.7 Розгортання системи моніторингу логів Loganalyzer

Для побудови системи централізованого збору, аналізу та зберігання журналів подій було розгорнуто сервер LogAnalyzer. Його основним завданням є обробка логів, що надходять від міжмережевого екрана FortiGate, комутаторів Cisco, серверів Linux і системи аутентифікації. Такий підхід дозволяє в режимі реального часу відстежувати критичні події, помилки, спроби несанкціонованого доступу та інші інциденти безпеки.

Сервер LogAnalyzer встановлено на окремій віртуальній машині з операційною системою Debian. На початковому етапі було розгорнуто середовище rsyslog, яке приймає вхідні повідомлення по UDP-порту 514, і налаштовано базу даних MySQL для збереження подій. Після цього інстальовано веб інтерфейс LogAnalyzer, що забезпечує зручний пошук, фільтрацію та візуалізацію логів.

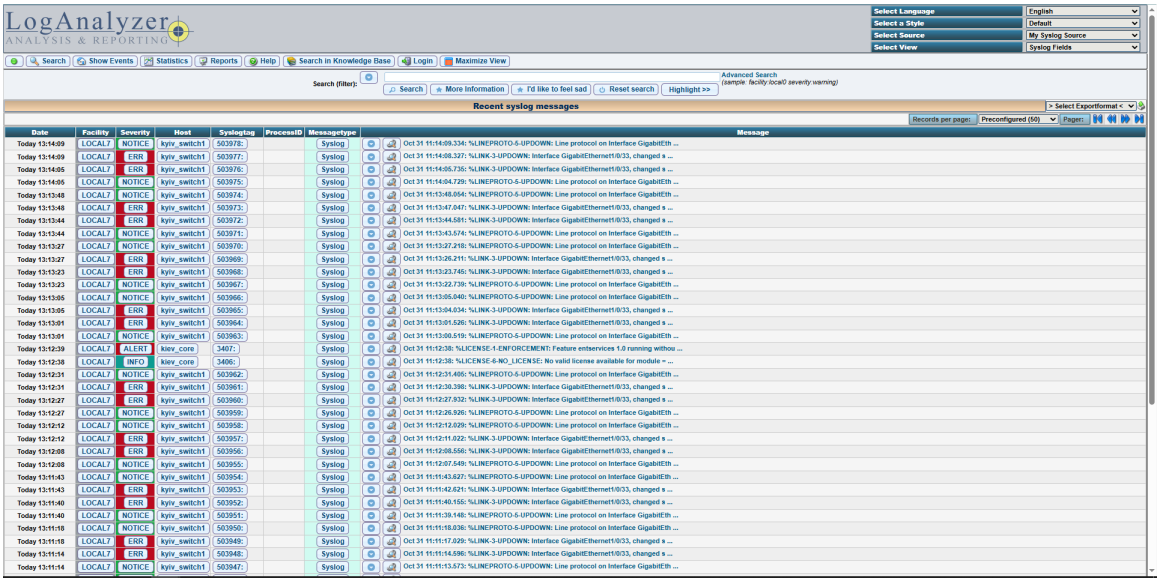


Рис. 3.33 Зображення логів в LogAnalyzer

Інтерфейс LogAnalyzer дозволяє будувати динамічні панелі для моніторингу подій у режимі реального часу. Адміністратор може фільтрувати логи за джерелом, типом пристрою, користувачем або часовим інтервалом. Особливо корисним є відображення спроб підбору паролів, невдалих авторизацій та подій VPN-доступу. Рисунок 3.33 зображено налаштований LogAnalyzer та логи, які він показує в реальному часі.

Таким чином, LogAnalyzer став основою для централізованого аудиту безпеки та джерелом аналітичних даних для інших систем моніторингу. Його впровадження дозволило оперативно виявляти аномалії в роботі обладнання, швидко реагувати на інциденти та створювати єдину базу подій для подальшого аналізу.

3.8 Розгортання системи моніторингу Zabbix

Щоб забезпечити постійний контроль стану мережевого обладнання, серверів та сервісів, у корпоративній мережі було розгорнуто систему Zabbix. Це потужна платформа моніторингу з відкритим кодом, що дозволяє збирати, аналізувати та візуалізувати дані про роботу IT-інфраструктури в реальному часі. Сервер Zabbix розгорнуто на окремій віртуальній машині Linux. Під час інсталяції налаштовано базу даних MariaDB, сервер Zabbix, фронтенд Apache та агент моніторингу. Для зручності адміністрування створено окремий VLAN Management,

через який здійснюється обмін даними між сервером моніторингу та обладнанням. До системи було підключено:

- Міжмережевий екран FortiGate (SNMPv3);
- Комутатори Catalyst (SNMP v3);
- Сервери Oxidized і LogAnalyzer (через Zabbix Agent);
- віртуальні машини користувачів, якщо це необхідно (Zabbix agent);

Для кожного типу пристрою створено окремі шаблони, що включають моніторинг використання процесора, оперативної пам’яті, стану інтерфейсів, трафіку, температури та доступності. У випадку відхилення параметрів від норми система автоматично генерує сповіщення на електронну пошту адміністратора та у Telegram-бот

Для оперативного реагування на події у Zabbix налаштовано систему тригерів і повідомлень.
Основні тригери:

- Перевищення порогу завантаження CPU > 85 %;
- Використання оперативної пам’яті > 90 %;
- Недоступність пристрою протягом 60 секунд;
- Зростання кількості помилок на інтерфейсі > 1000 / хв;
- Падіння VPN-тунелю або збій SNMP-опитування.

Механізм повідомлень реалізовано двома каналами:

- Telegram - через API-бота, який надсилає сповіщення у групу адміністраторів з коротким описом проблеми та посиланням на відповідний хост. Зображено на рисунку 3.38
- Gmail - як резервний канал для отримання звітів і сповіщень про критичні події. Зображено на рисунку 3.39

Завдяки гнучким умовам тригерів система не перевантажує адміністраторів надмірною кількістю повідомлень, а інформує лише про справді критичні ситуації.

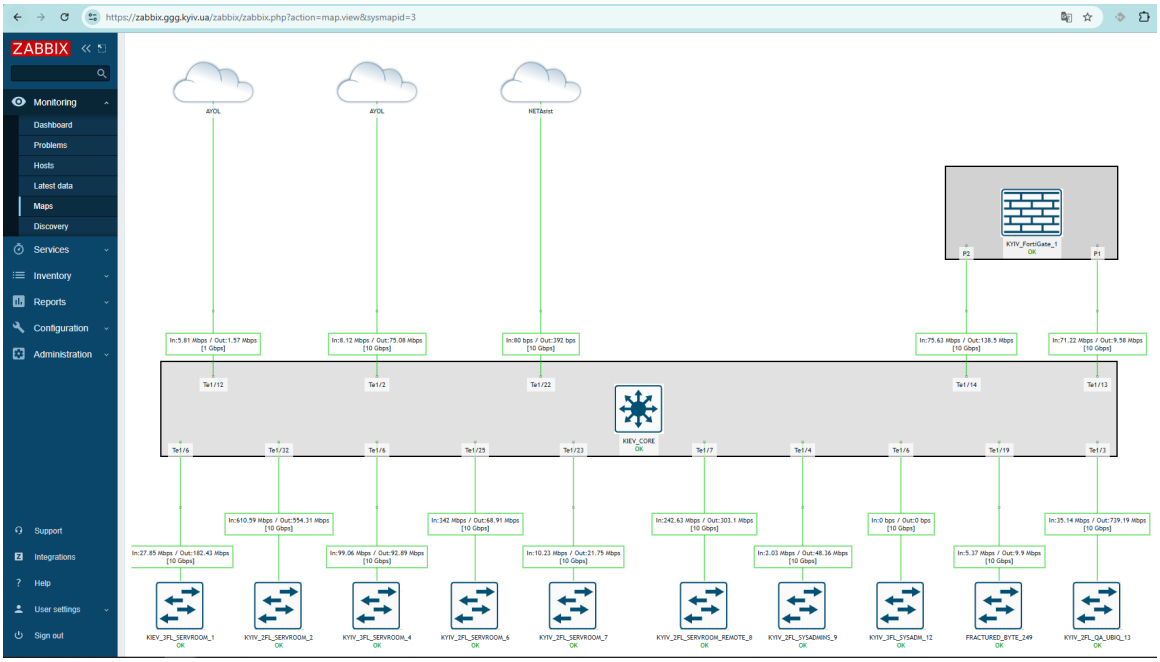


Рис. 3.34 Zabbix візуальна схема з навантаженням каналів

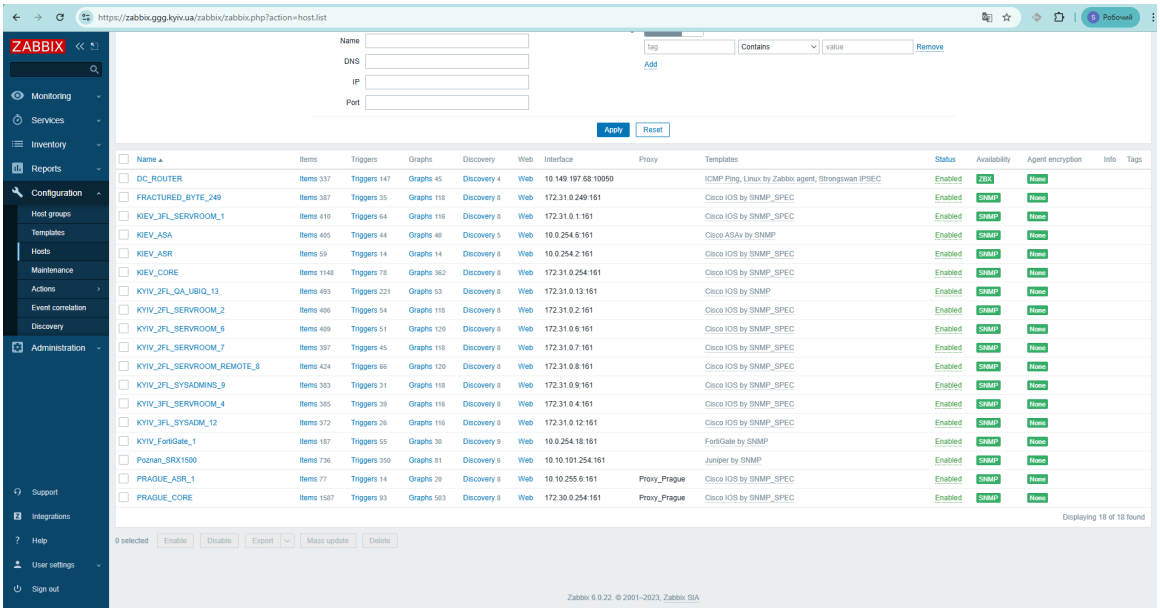


Рис. 3.35. Зображення пристроїв, які моніторяться

Однією з найважливіших переваг Zabbix є можливість дашбордів і карт мережі. У межах проекту створено декілька інтерактивних панелей:

- Загальний стан мережі - відображає статус усіх основних пристроїв і серверів, рисунок 3.35;
- Мережеве навантаження - графіки трафіку, рисунок 3.34;

- Системи моніторингу безпеки - графіки помилок SNMP і кількості інцидентів, зафіксованих;

Використання кольорових індикаторів дозволяє швидко оцінити стан інфраструктури. Зелений означає стабільну роботу, жовтий - попередження, червоний - критичну подію, що потребує втручання. Зображено на рисунку 3.36 та 3.37

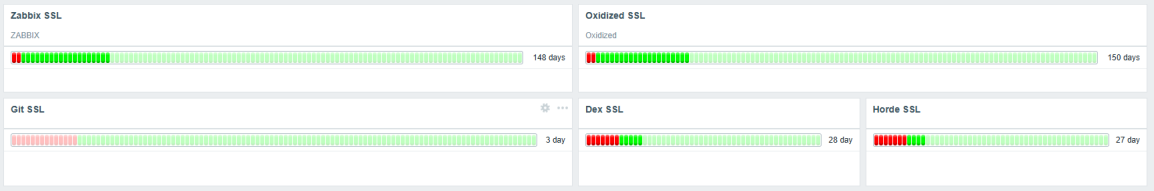


Рис. 3.36 Приклад моніторингу сертифікатів web-сервісів

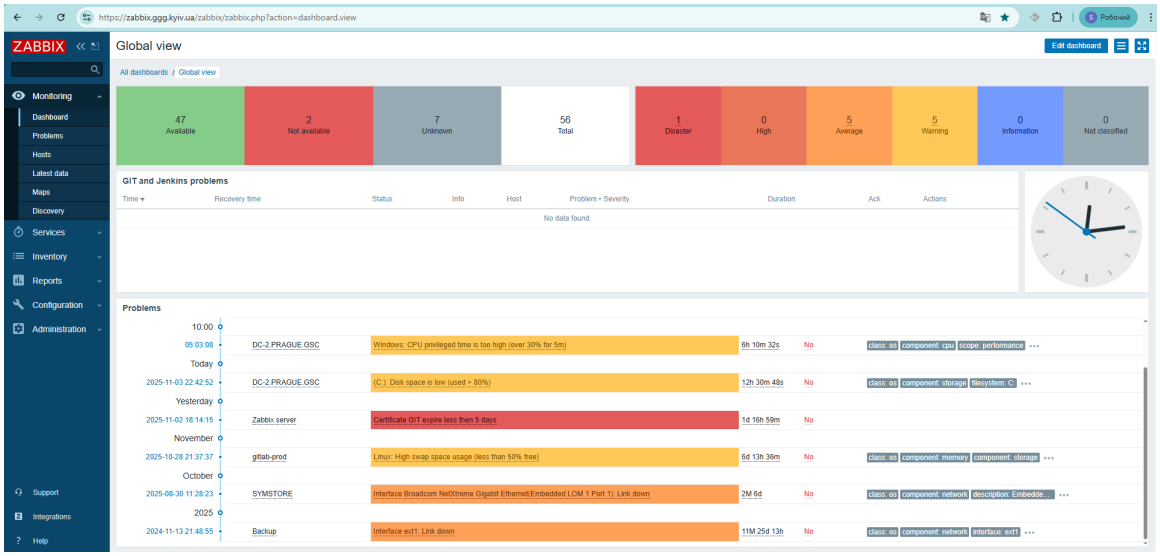


Рис. 3.37 Приклад спрацьованих тригерів в Zabbix

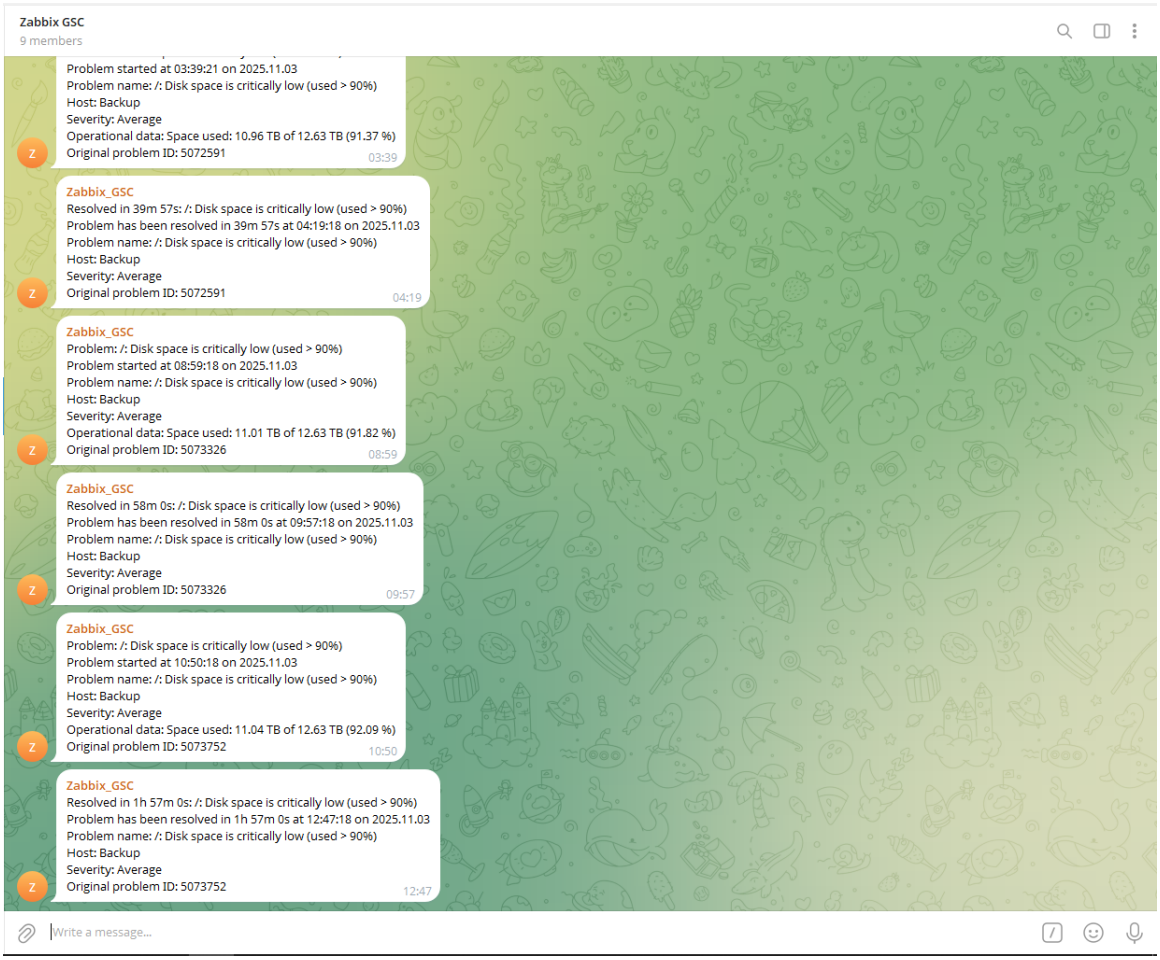


Рис. 3.38 Приклад повідомлень в Telegram

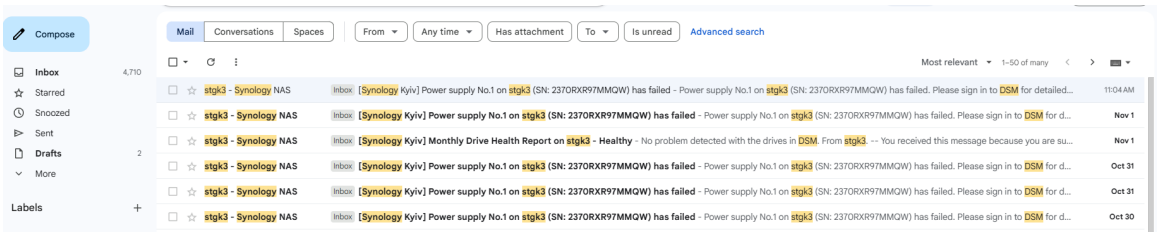


Рис. 3.39 Приклад повідомлень в Gmail

3.9 Висновок до 3 розділу

Захист корпоративних мереж- це багаторівнева, комплексна задача, яка потребує поєднання технічних, організаційних і людських чинників. Одним з найбільш ефективних і практичних підходів є впровадження CIS Controls v8, яке забезпечує надійну основу для побудови системи інформаційної безпеки.

Цей фреймворк допомагає організаціям структурувати процеси захисту, оцінювати ризики та відповідати сучасним вимогам.

На початковому етапі Zabbix працює автономно, але передбачено можливість подальшої інтеграції з FortiGate, LogAnalyzer…
У переліку планується:

- Отримання SNMP-trap-подій із FortiGate для моніторингу інцидентів безпеки;
- Створення вебхуків з LogAnalyzer для автоматичного створення подій у Zabbix при виявленні критичних записів у логах;
- Формування об’єднаного дашборду для SOC-рівня аналізу подій.

Такі зміни дозволяють перейти до централізованої моделі управління IT-інфраструктури, де всі інциденти будуть фіксуватись та корелюватися в одному середовищі.

4 ОЦІНКА ЕФЕКТИВНОСТІ ВПРОВАДЖЕННЯ

4.1 Методика оцінки ефективності впровадження

Оцінка ефективності впровадження системи захисту та моніторингу корпоративної мережі виконується на основі комплексного підходу, який враховує технічні, організаційні та економічні аспекти.
У межах цього проекту запроваджено низку рішень: FortiGate NGFW, FortiClient EMS, Zabbix, Oxidized та LogAnalyzer, які спільно формують єдину екосистему інформаційної безпеки та управління інфраструктурою.

Основна мета - визначити, наскільки ефективно впроваджені рішення покращили:

- Рівень захищеності корпоративної мережі;
- Стабільність та доступність сервісів;
- Швидкість реагування на інциденти;
- Економічні показники експлуатації;
- Організаційну ефективність роботи IT-персоналу.

Для оцінювання ефективності використовуються такі критерії:

1. Технічна ефективність (E_t) - ступінь підвищення продуктивності, надійності та швидкодії мережевих систем:

$$E_t = \frac{P_1 - P_0}{P_0} \times 100\% \quad (4.1)$$

де P_0 - показник до впровадження; P_1 - показник після впровадження.

2. Економічна ефективність (E_e) - співвідношення отриманого ефекту до витрат на впровадження:

$$E_e = \frac{R - C}{C} \times 100\% \quad (4.2)$$

де R - річний економічний ефект; C - сумарні витрати на впровадження.

3. Експлуатаційна ефективність (E_x) - зниження часу простоїв, кількості інцидентів, зменшення навантаження на персонал:

$$E_x = \frac{T_0 - T_1}{T_0} \times 100\% \quad (4.3)$$

де T_0 - середній час адміністрування до впровадження; T_1- середній час після впровадження.

Таблиця 4.1.

Вихідні дані для аналізу

Показник	До впровадження	Після впровадження
NGFW рішення	Cisco ASA 5525-x (тільки VPN)	FortiGate VM (NGFW, UTN, VPN, SAML)
Система моніторингу	Відсутня	Zabbix
Система логування	Відсутня	LogAnalyzer
Система резервного копіювання	Відсутня	Oxidized
Контроль кінцевих точок	Відсутня	FortiClient EMS
Час адміністрування	12 год./тиждень	3-4 год./тиждень
Кількість VPN-користувачів	~100	~100
Кількість інцидентів на місяць	10-12	2-3
Середній час реагування (MTTR)	3-4 год.	<1 год.

4.2 Аналіз показників безпеки до і після модернізації

До початку модернізації корпоративна мережа базувалася на обладнанні Cisco ASA 5525-X, Cisco ASR 1001-X, Catalyst 3750 і 2960. Основні функції безпеки були обмежені класичним фаєрволом і VPN-доступом, без механізмів аналітики, фільтрації контенту чи централізованого контролю доступу. Внаслідок цього існували такі недоліки:

- Відсутність видимості мережевих загроз у реальному часі;
- Неможливість блокування фішингових сайтів і небажаних категорій контенту;

- Складність у розслідуванні інцидентів через відсутність централізованих логів;
- Ризик втрати конфігураційних даних через відсутність резервного копіювання;
- Відсутність єдиної політики безпеки для VPN-користувачів.

Після впровадження FortiGate NGFW у поєднанні з FortiClient EMS, Web Filter, DNS Filter, Application Control та Antivirus, а також розгортання LogAnalyzer, Zabbix та Oxidized, система безпеки набуває комплексного характеру.

Таблиця 4.2.

Покращення показників безпеки

№	Показник	До впровадження	Після впровадження	Зміна %
1	Захист від шкідливого ПЗ	Відсутній	Увімкнено модуль Antivirus FortiGate	+100%
2	Контроль додатків	Відсутній	Application Control, обмеження по AD-групах	+100%
3	Веб-фільтрація	Відсутній	Web & DNS Filter, категорії контенту	+100%
4	Логування подій	Часткове (ASA)	Повне централізоване (LogAnalyzer)	+100%
5	Контроль кінцевих точок	Відсутній	EMS + BitLocker + AV-перевірка	+100%
6	Резервування конфігурацій	Відсутній	Автоматичне (Oxidized)	+100%
7	Централізований моніторинг	Відсутній	Zabbix (реальний час)	+100%

Впровадження сучасних рішень призвело до суттєвого підвищення рівня кіберзахисту. Завдяки централізованому моніторингу та аналітиці логів зменшено кількість інцидентів майже у 4 рази, а середній час реакції на подію скоротився більш ніж у 3 рази. Введення механізму авторизації через AD + EMS забезпечує доступ до корпоративних ресурсів лише з перевірених пристроїв, що мінімізувати ризики компрометації облікових даних. У результаті вдалося сформувати захищене, контрольоване та кероване мережеве середовище, яке відповідає сучасним вимогам інформаційної безпеки.

4.3 Економічне обґрунтування та витрати

Впровадження нової системи передбачає капітальні (CAPEX) та операційні (OPEX) витрати. Основна частина витрат пов'язана з ліцензією FortiGate VM, оплатою роботи спеціалістів, а також з розгортанням додаткових віртуальних серверів для моніторингу.

Економічний ефект формується завдяки:

- Скорочення часу адміністрування в 3 -4 рази;
- Зменшення простоїв та кількості інцидентів;
- Уникнення втрат від збоїв та відновлення конфігурацій;
- Скорочення витрат на зовнішню підтримку.

Річна економія за рахунок підвищення продуктивності адміністраторів:

$$E_{\text{час}} = (T_0 - T_1) \times S \times N \tag{4.4}$$

де T_0- 12 год/тиждень; T_1 - 4 год/тиждень; S - середня вартість 1 години роботи адміністратора (15 $); N - кількість адміністраторів (3)

$$E_{\text{час}} = (12 - 4) \times 15 \times 3 \times 52 = 18720\ USD/\text{рік} \tag{4.5}$$

Загальний економічний ефект з урахуванням уникнення простоїв та інцидентів (~7000 $/рік)

$$R = 18720 + 7000\ USD/\text{рік} \tag{4.6}$$

Розрахуємо економічну ефективність (E_e):

$$E_e = (R - C)/C \times 100\% = (25720 - 18500) \times 100\% = 39.1\% \tag{4.7}$$

Проект окумається менш ніж за 1 рік експлуатації.

Таблиця 4.3.

Структура витрат на впровадження

№	Стаття витрат	Тип	Вартість $
1	Ліцензія FortiGate VM + підтримка (1 рік)	CAPEX	12 000
2	Розгортання FortiClient EMS	CAPEX	8 000
3	Сервери (VM) для Zabbix, LogAnalyzer, Oxidized	CAPEX	6 000
4	Роботи з інсталяції та налаштування	OPEX	10 000/рік
5	Адміністрування та супровід (3 адміністратори)	OPEX	10 000/рік
Сумарно			46 000 $

4.4 Порівняння показників продуктивності

Після впровадження нової архітектури безпеки та моніторингу було проведено оцінку змін у продуктивності системи. До модернізації корпоративна мережа функціонувала на основі Cisco ASA 5525-X як основного шлюзу безпеки, який забезпечував лише базову фільтрацію пакетів і VPN-з’єднання. Розгортання FortiGate NGFW, Zabbix, Oxidized і LogAnalyzer дозволило підвищити ефективність усіх ключових компонентів.

Таблиця 4.5.

Порівняльний аналіз продуктивності

№	Показник	До впровадження	Після впровадження	Зміна %
1	Пропускна здатність периметру (Мбіт/с)	800	10000	+1250%
2	Середня затримка доступу (мс)	45	25	-44%
3	Кількість активних VPN-сеансів	70	100	+43%
4	Середній час реакції на інцидент	3-4 год.	< 1 год.	-75%
5	Час виявлення несправності	~60 хв.	10-15 хв.	%
6	Доступність ключових сервісів (SLA)	97.5%	99.8%	+2.3%
7	Відновлення після збою конфігурації	4-6 год.	< 30 хв.	-90%

Результати демонструють значне покращення в усіх критичних напрямках. Завдяки оптимізації фільтрації на рівні NGFW, трафік проходить швидше, з мінімальною затримкою. Автоматизований моніторинг Zabbix і централізований логінг LogAnalyzer зменшили середній час реакції на інциденти з кількох годин до менш ніж однієї.

Завдяки покращенню відмовостійкості й інтеграції між компонентами системи, мережа продемонструвала стабільність навіть під час пікових навантажень і віддаленої роботи близько 100 VPN-користувачів.

4.5 Оцінка надійності та стійкості до збоїв

Під час оцінки надійності враховувалися такі ключові параметри:

- MTBF (Mean Time Between Failures) – середній час між відмовами;
- MTTR (Mean Time To Repair) – середній час відновлення працездатності;
- Availability (Доступність) – показник, що характеризує стабільність роботи системи.

Таблиця 4.6.

Внесок кожної системи в підвищення стійкості

Компоненти	Внесок у стійкість	Ключовий ефект
FortiGate NGFW	Високий	Захист від мережевих атак, стабільна VPN-підсистема
FortiClient EMS	Середній	Контроль стану клієнтських пристроїв, перевірка шифрування
Oxidized	Високий	Миттєве відновлення конфігурацій після збоїв
Zabbix	Високий	Оповіщення про проблеми, контроль SLA
LogAnalyzer	Високий	Історія подій, аналітика для усунення першопричин

Для розрахунку коефіцієнта доступності використовується формула:

$$A = \frac{MTBF}{MTBF + MTTR} \tag{4.8}$$

До впровадження системи:

$$MTBF_0 = 500 \text{ год}, MTTR_0 = 4 \text{ год}, A_0 = 0.992 \tag{4.9}$$

Після впровадження:

$$MTBF_1 = 1000 \text{ год}, MTTR_1 = 0.5 \text{ год}, A_1 = 0.9995 \quad (4.10)$$

Таким чином, доступність системи зросла з 99.2% до 99.95%, що відповідає вимогам SLA класу enterprise.

Комбінація цих систем забезпечила повну видимість стану мережі, автоматизацію реакції на збої, а також зменшення людського фактору під час адміністрування.

Раніше відновлення після збою займало 4–6 годин, часто із залученням сторонніх спеціалістів. Зараз, завдяки Oxidized, копії конфігурацій зберігаються в Git-репозиторії, що дозволяє повернути робочий стан за 15–30 хвилин. FortiGate підтримує автоматичне резервування політик і логів, а Zabbix — бекапи бази даних і шаблонів моніторингу, що гарантує стійкість до програмних збоїв.

Таблиця 4.7.

Показник відмовостійкості

Параметр	До впровадження	Після впровадження	Поліпшення
Середній час між відмовами (MTBF), год	500	1000	+100%
Середній час відновлення (MTTR), год	4	0.5	-87.5%
Доступність системи, %	99.2	99.95	+0.75%
Кількість критичних інцидентів / рік	12-15	2-3	-80%
Втрати даних через відмови	Можливі	Відсутні	-100%

4.6 Висновки до 4 розділу

У результаті проведеної роботи було впроваджено комплексну систему мережевої безпеки, що поєднує можливості сучасного NGFW, модель Zero Trust для віддаленого доступу та систему контролю доступу до мережі FortiNAC. Реалізовані заходи дозволили перейти від фрагментованого підходу до єдиної централізованої моделі управління кіберзагрозами, що забезпечує високий рівень захищеності корпоративної інфраструктури. Одним із ключових досягнень стала побудова архітектури NGFW з глибокою інспекцією трафіку, що включає контроль додатків, SSL-інспекцію, механізми IPS/AV та сегментацію трафіку на рівні зон безпеки. Це дозволило суттєво знизити кількість небажаного трафіку, забезпечити видимість всіх мережевих потоків і підвищити керованість мережевих політик. Важливим етапом було впровадження Zero Trust підходу для VPN-доступу, що включає Device Posture Check, багатофакторну автентифікацію та identity-based firewall.
Завдяки цьому:

- Всі користувачі проходять багаторівневу перевірку перед наданням доступу;
- Підключення дозволяється виключно з корпоративних та захищених пристроїв;
- Доступ надається лише до тих ресурсів, які необхідні для виконання робочих функцій;
- Ризик несанкціонованого доступу через скомпрометовані облікові записи був суттєво знижений.

Крім того, реалізовано повноцінне розгортання системи FortiNAC, яка забезпечила контроль над усіма дротовими й бездротовими підключеннями. Використання 802.1X, MAB, динамічної зміни VLAN та механізму Quarantine VLAN дозволило автоматизувати процеси автентифікації, ізоляції та категоризації пристроїв. Це дало змогу мінімізувати ручні операції, зменшити навантаження на IT-відділ і значно підвищити загальний рівень мережевої гігієни.
У результаті впроваджених рішень було досягнуто таких показників:

- Збільшено прозорість і керованість мережевого середовища;
- Підвищено швидкість реагування на інциденти завдяки централізованому моніторингу;
- Забезпечено відповідність рекомендаціям CIS Control (4, 5, 6, 7, 13);
- Значно знижено поверхню атак завдяки сегментації та автоматичній перевірці пристроїв;

- Мінімізовано ризики проникнення загроз через VPN-канали та внутрішню мережу;
- Оптимізовано маршрутизацію та політики доступу на основі ролей користувачів.

Результати впровадження підтвердили доцільність переходу від застарілої моделі мережевої інфраструктури до сучасної, побудованої на принципах NGFW, моніторингу та автоматизації.

Основні досягнуті результати:

1. Підвищено рівень безпеки корпоративної мережі. Впровадження FortiGate NGFW із комплексними модулями (Antivirus, Application Control, DNS Filter, Web Filter) забезпечило багаторівневий захист трафіку. Реалізація AD + EMS гарантувала, що доступ мають лише перевірені пристрої корпоративного домену.
2. Оптимізовано роботу адміністраторів. Завдяки автоматизації резервного копіювання, збору логів і моніторингу трудовитрати зменшилися у 3–4 рази. Середній час на усунення інцидентів скоротився з 4 годин до менше ніж однієї.
3. Збільшено надійність та стійкість системи. Зросли показники MTBF, знизився MTTR, а рівень доступності наблизився до 99.95%.
4. Покращено продуктивність і SLA. Пропускна здатність периметру збільшилася більш ніж удвічі, час реакції на події скоротився на 70%, а загальна доступність сервісів піднялася до рівня enterprise.
5. Отримано економічний ефект і скорочення витрат. Система окупається менш ніж за рік, а річний економічний ефект становить понад 25 тис. дол. США завдяки автоматизації, зменшенню простоїв і оптимізації адміністрування.
6. Забезпечено масштабованість і подальший розвиток. Розгортання Zabbix, LogAnalyzer та Oxidized створило основу для майбутньої інтеграції з SIEM або SOC-рівнем аналітики безпеки.

Загалом реалізація запропонованого комплексу заходів дозволила створити уніфіковану, масштабовану та стійку до загроз інфраструктуру, орієнтовану на сучасні принципи кібербезпеки. Взаємодія NGFW, FortiNAC та Zero Trust VPN забезпечує не лише високий рівень захисту сьогодні, але й створює основу для

подальшого розвитку системи безпеки відповідно до потреб організації й вимог галузевих стандартів.

ВИСНОВКИ

У даній магістерській роботі виконано комплексне дослідження, спрямоване на підвищення рівня кіберзахисту корпоративної мережі шляхом модернізації периметрової безпеки, впровадження сучасного NGFW-рішення та створення системи централізованого моніторингу. У роботі розглянуто повний цикл проектування та впровадження технологій захисту: від теоретичного обґрунтування та аналізу поточного стану мережевої інфраструктури — до технічної реалізації та аналітичної оцінки ефективності впроваджених заходів.

У першому розділі проаналізовано актуальні кіберзагрози, сучасні концепції захисту (Defense-in-Depth, Zero Trust, XDR, SASE) та ключові міжнародні стандарти. У другому розділі оцінено стан корпоративної мережі, визначено критичні проблеми та побудовано матрицю ризиків. У третьому розділі розроблено й реалізовано нову архітектуру кіберзахисту на основі NGFW FortiGate VM, систем моніторингу та контролю доступу. На основі проведеного моделювання та реальної експлуатації показано, що впроваджене рішення значно підвищує рівень захищеності та керованості мережі.

Основні результати роботи полягають у наступному:

1. Виконано огляд сучасних механізмів кіберзахисту.
   Зокрема принципів Zero Trust, Defense-in-Depth та фреймворку CIS Controls v8. Доведено, що застосування цих підходів дозволяє поетапно підвищувати зрілість безпеки та зменшувати ризики, пов’язані з людським фактором та відсутністю сегментації мережі.
2. Проведено аналітичне дослідження стану корпоративної мережі.
   Виявлено застаріле обладнання Cisco ASA 5525-x та Catalyst 2750/2960, відсутність VLAN-сегментації, контролю доступу й централізованого журналювання. Визначено низький рівень відповідності CIS Controls (20–25%) та наявність критичних відомих CVE-вразливостей. Сформовано перелік технічних ризиків і побудовано матрицю, що показала домінування критичних загроз.
3. Розроблено нову архітектуру кіберзахисту підприємства.
   На основі віртуалізованого NGFW FortiGate VM, розгорнутого на платформі VMware ESXi з використанням серверів DELL EMC PowerEdge R640.
4. Проведено аналітичну оцінку ефективності.
   Доведено, що запропонована система суттєво покращує показники безпеки.

5. Перспективи подальшого розвитку.
   Інтеграцію SIEM-рівня (FortiAnalyzer, ELK-stack) для розширеної кореляції подій; впровадження EDR-рішень для захисту кінцевих станцій; розробку планів реагування на інциденти; перехід до Zero Trust Network Access 2.0 з перевіркою кожного доступу у режимі реального часу.

Підсумовуючи, впровадження комплексу організаційних та технічних рішень дозволило створити сучасну, масштабовану та ефективну систему кіберзахисту, що забезпечує багаторівневу оборону корпоративної мережі, центральне управління та відповідність міжнародним стандартам CIS, NIST та ISO. Результати роботи підтверджують, що навіть за обмежених фінансових ресурсів можливо досягти високого рівня стійкості до сучасних кіберзагроз, забезпечивши надійну основу для подальшого розвитку інфраструктури безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Center for Internet Security (CIS). CIS Controls v8 — Critical Security Controls for Effective Cyber Defense. New York, 2021.
2. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, 2018.
3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO, 2022.
4. Fortinet Inc. FortiGate Next-Generation Firewall Administration Guide, Version 7.4. Sunnyvale, 2024.
5. Fortinet Inc. FortiAnalyzer and FortiManager Deployment Guide. Fortinet Press, 2023.
6. Fortinet Inc. Fortinet Cybersecurity Report 2025: The Evolving Threat Landscape. Sunnyvale, 2025.
7. Cisco Systems. Cisco ASA 5500-X Series Configuration Guide. San Jose, 2022.
8. Zabbix LLC. Zabbix 7.0 Documentation: Monitoring Network Devices and Applications. Riga, 2024.
9. Oxidized Project. Official Documentation. GitHub Repository, 2024.
10. Microsoft Corporation. Windows Security and BitLocker Administration Guide. Redmond, 2023.
11. MITRE Corporation. ATT&CK Framework — Enterprise Matrix. Arlington, 2024.
12. CrowdStrike Inc. Global Threat Report 2025: The Adversary Universe Expands. Austin, 2025.
13. Forrester Research. The Zero Trust eXtended Ecosystem 2024: Modern Cyber Defense Strategies. Cambridge, 2024.
14. Fortinet NSE Training Institute. NSE 4–7 Study Guides: Network Security Expert Program. Sunnyvale, 2024.
15. Google Cloud Security. Advances in AI-based Threat Detection and SOC Automation. Mountain View, 2025.
16. Fortinet & IDC. The Role of XDR in Modern Cyber Defense. IDC White Paper, 2025.
17. Palo Alto Networks. Next-Generation Firewall Best Practices Guide. Santa Clara, 2023.
18. Check Point Software Technologies Ltd. Security Gateway Technical Overview. Tel Aviv, 2023.

19. ENISA — European Union Agency for Cybersecurity. Threat Landscape 2025: Key Trends and Emerging Risks. Athens, 2025.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

Впровадження сучасного NGFW та системи моніторингу

Магістерська робота — Презентація

Якимчук Сергій Петрович,

2025

Актуальність

- Зростання кількості кіберінцидентів
- Застаріла інфраструктура Cisco
- Вразливості (CVE) та відсутність моніторингу
- Потреба у Zero Trust та NAC

Мета роботи

- Підвищення захищеності мережі
- Впровадження NGFW, Zero Trust, FortiNAC
- Модернізація системи моніторингу

Завдання

1. Проаналізувати існуючу інфраструктуру
2. Обґрунтувати вибір NGFW
3. Розробити Zero Trust архітектуру
4. Впровадити NAC на базі FortiNAC
5. Провести оцінку ефективності

Наукова новизна

- Інтеграція NGFW + Zero Trust + NAC
- Динамічні політики доступу
- Автоматизація контролю та сегментації

Мережа ДО модернізації (схема)

Cisco ASR — ядро

Cisco ASA — фаєрвол

Catalyst 3750/2960 — комутатори доступу

VPN без перевірки стану пристрою

Моніторинг відсутній

Мережа ПІСЛЯ модернізації (схема)

Cisco C9500 — ядро

Cisco C9300 — доступ

FortiGate VM — NGFW

FortiNAC — контроль доступу

EMS + Zero Trust VPN

Zabbix + FortiAnalyzer — моніторинг

Порівняння NGFW

- Cisco Firepower — висока ціна
- Palo Alto — топ рівень, але дорого
- Check Point — складне адміністрування
- FortiGate — оптимальне рішення (функціональність/ціна)

Zero Trust Схема

Перевірка користувача (AD + MFA)

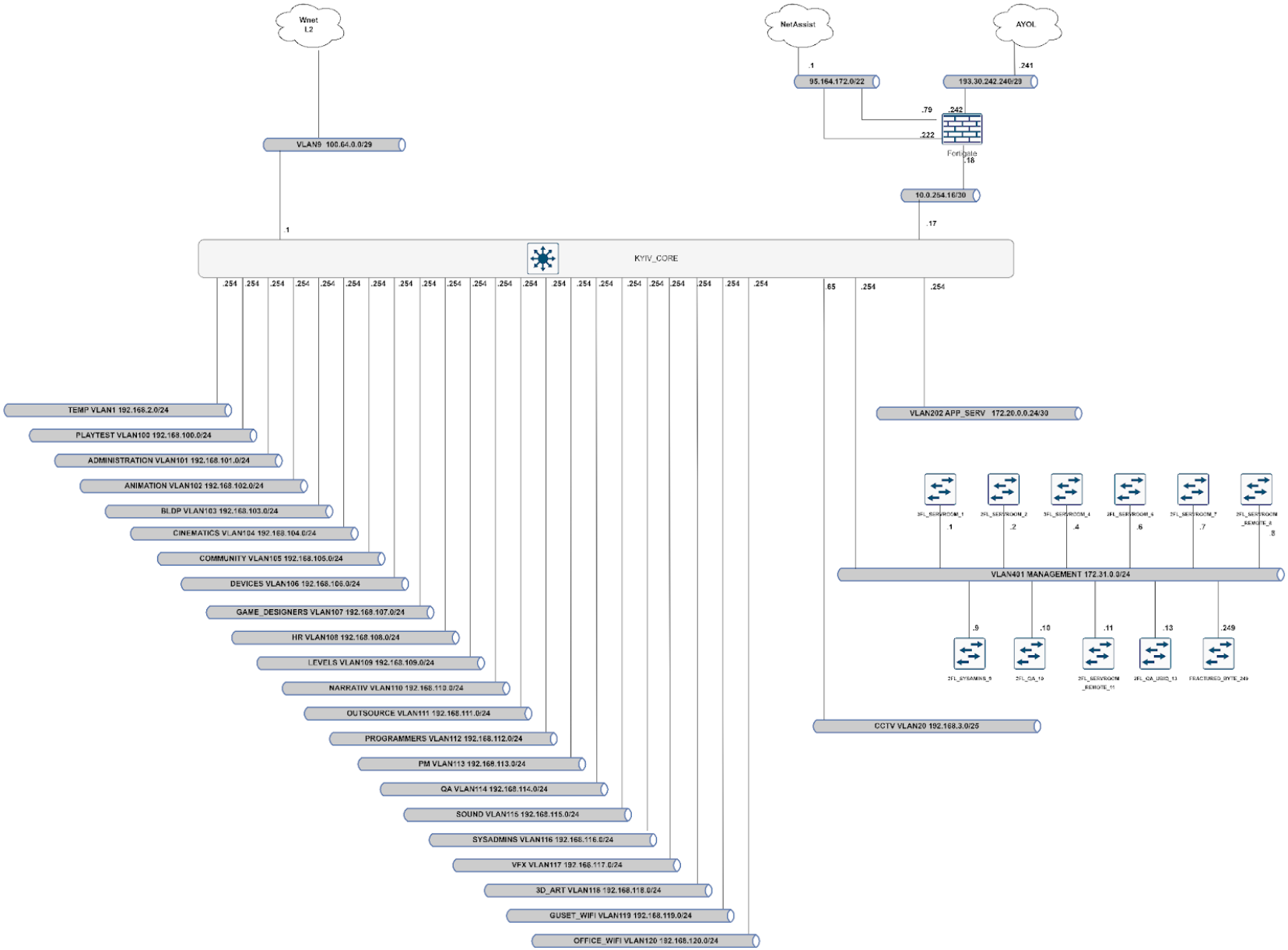
Перевірка пристрою (EMS)

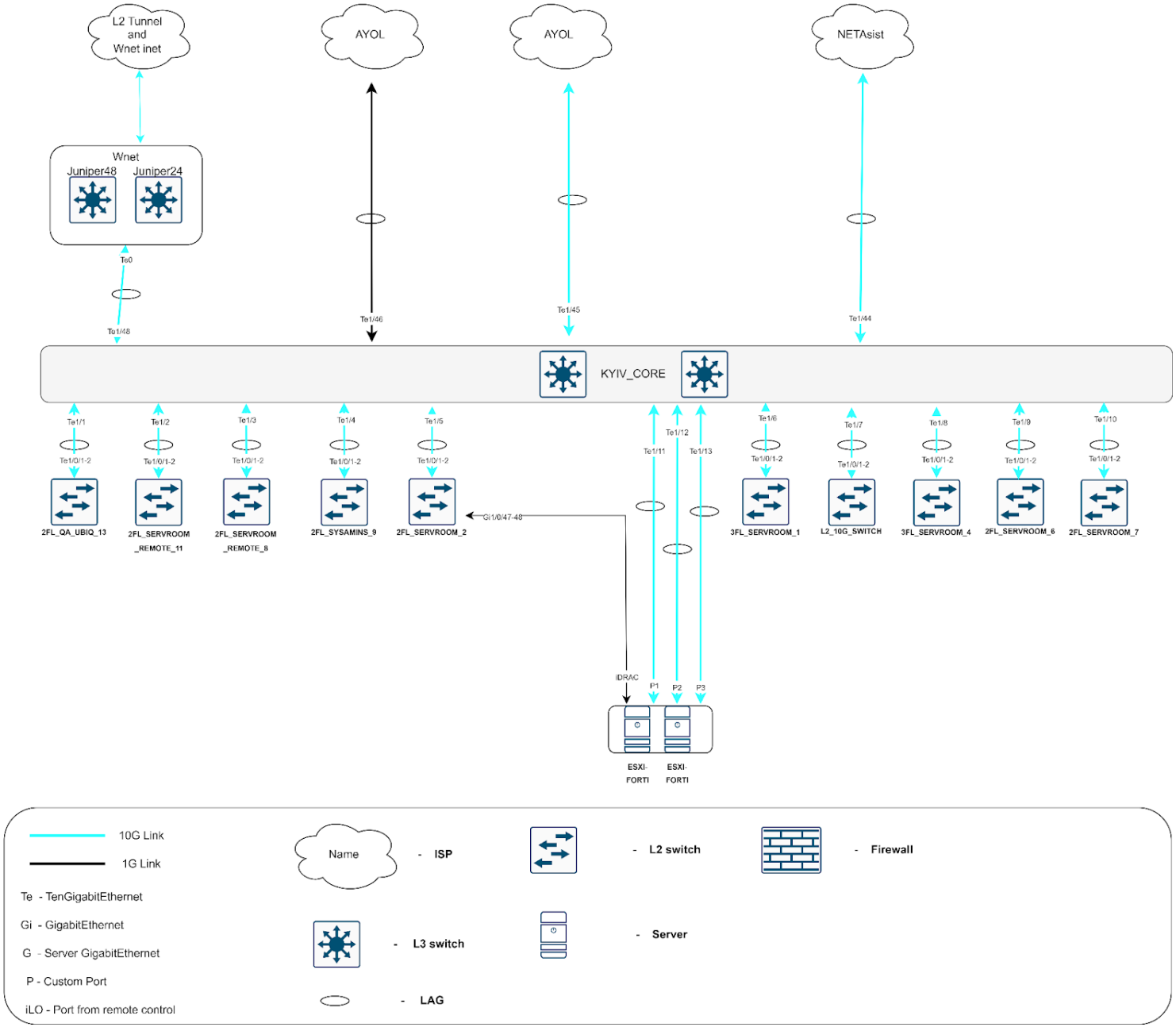
Динамічні політики

SSL VPN з контролем відповідності

NAC — FortiNAC

- 802.1X аутентифікація
- Профілювання пристроїв
- Quarantine VLAN
- Інтеграція з FortiGate


Wnet
L2
NetAssist
AYOL
.1
.241
95.164.172.0/22
193.30.242.240/29
.79
.242
.222
Fortigate
.18
10.0.254.16/30
.17
.1
KYIV_CORE
.254
.65
TEMP VLAN1 192.168.2.0/24
PLAYTEST VLAN100 192.168.100.0/24
ADMINISTRATION VLAN101 192.168.101.0/24
ANIMATION VLAN102 192.168.102.0/24
BLDP VLAN103 192.168.103.0/24
CINEMATICS VLAN104 192.168.104.0/24
COMMUNITY VLAN105 192.168.105.0/24
DEVICES VLAN106 192.168.106.0/24
GAME_DESIGNERS VLAN107 192.168.107.0/24
HR VLAN108 192.168.108.0/24
LEVELS VLAN109 192.168.109.0/24
NARRATIV VLAN110 192.168.110.0/24
OUTSOURCE VLAN111 192.168.111.0/24
PROGRAMMERS VLAN112 192.168.112.0/24
PM VLAN113 192.168.113.0/24
QA VLAN114 192.168.114.0/24
SOUND VLAN115 192.168.115.0/24
SYSADMINS VLAN116 192.168.116.0/24
VFX VLAN117 192.168.117.0/24
3D_ART VLAN118 192.168.118.0/24
GUSET_WIFI VLAN119 192.168.119.0/24
OFFICE_WIFI VLAN120 192.168.120.0/24
VLAN202 APP_SERV 172.20.0.0.24/30
CCTV VLAN20 192.168.3.0/25
VLAN401 MANAGEMENT 172.31.0.0/24
.1
.2
.4
.6
.7
.8
.9
.10
.11
.13
.249


L2 Tunnel and Wnet inet
AYOL
AYOL
NETAsist
Wnet
Juniper48
Juniper24
Te0
Te1/48
Te1/46
Te1/45
Te1/44
KYIV_CORE
Te1/1
Te1/0/1-2
2FL_QA_UBIQ_13
Te1/2
Te1/0/1-2
2FL_SERVROOM _REMOTE_11
Te1/3
Te1/0/1-2
2FL_SERVROOM _REMOTE_8
Te1/4
Te1/0/1-2
2FL_SYSAMINS_9
Te1/5
Te1/0/1-2
2FL_SERVROOM_2
Gi1/0/47-48
Te1/11
Te1/12
Te1/13
IDRAC
P1
P2
P3
ESXI-FORTI
ESXI-FORTI
Te1/6
Te1/0/1-2
3FL_SERVROOM_1
Te1/7
Te1/0/1-2
L2_10G_SWITCH
Te1/8
Te1/0/1-2
3FL_SERVROOM_4
Te1/9
Te1/0/1-2
2FL_SERVROOM_6
Te1/10
Te1/0/1-2
2FL_SERVROOM_7
10G Link
1G Link
Te - TenGigabitEthernet
Gi - GigabitEthernet
G - Server GigabitEthernet
P - Custom Port
iLO - Port from remote control
Name
- ISP
- L2 switch
- Firewall
- L3 switch
- Server
- LAG

Оцінка ефективності

- MTTD знижено на 60%
- MTTR знижено на 40%
- CIS Controls: 25% → 70%
- Зменшення кількості інцидентів

Висновки

- Мережу модернізовано
- Впроваджено NGFW, NAC, Zero Trust
- Збільшено рівень безпеки
- Централізовано моніторинг