ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту корпоративної мережевої інфраструктури на базі рішення Fortigate»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Максим КИРКАЧ
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
КИРКАЧ Максим
(прізвище, ім'я)

Керівник д-р філос., доц., МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD — Active Directory

API — Application Programming Interface

DoS — Denial of Service

DDoS — Distributed Denial of Service

DNS — Domain Name System

FW — Firewall

IPS — Intrusion Prevention System

IDS — Intrusion Detection System

NAT — Network Address Translation

NGFW — Next Generation Firewall

OSI — Open Systems Interconnection

SD-WAN — Software Defined Wide Area Network

SPU — Security Processing Unit

SSL — Secure Sockets Layer

TLS — Transport Layer Security

UTM — Unified Threat Management

VPN — Virtual Private Network

WAN — Wide Area Network

LAN — Local Area Network

DMZ — Demilitarized Zone

ВСТУП

Стрімкий розвиток інформаційних технологій та цифровізація процесів зумовили суттєве зростання ролі корпоративних мереж у діяльності сучасних організацій. Корпоративна мережева інфраструктура сьогодні є основою для функціонування інформаційних систем, обміну даними, віддаленої роботи співробітників, доступу до хмарних сервісів та інтеграції з зовнішніми партнерами. Водночас підвищення рівня залежності бізнесу від мережевих технологій призводить до зростання кількості кіберзагроз, складності атак та потенційних наслідків порушення безпеки.

Сучасний склад загроз усе більше характеризується переходом від одиничних несфокусованих атак до складних, багатоступеневих і тривалих кампаній, які спрямовані на підрив корпоративної інфраструктури, викрадення конфіденційної інформації або дестабілізацію процесів. Зловмисники активно експлуатують слабкі місця мережевих протоколів, помилки конфігурації, методи соціальної інженерії, а також шкідливе програмне забезпечення, здатне обходити традиційні засоби захисту.

Актуальність даної роботи зумовлена необхідністю впровадження сучасних технологій захисту корпоративної мережевої інфраструктури, які поєднують у собі багаторівневий підхід, глибокий аналіз трафіку, централізоване управління політиками безпеки та високу продуктивність. Одним із найбільш поширених і технологічно розвинених рішень у цій сфері є платформа FortiGate компанії Fortinet, яка належить до класу міжмережевих екранів нового покоління та інтегрує широкий спектр механізмів захисту в межах єдиної операційної системи FortiOS.

FortiGate використовується як у невеликих корпоративних мережах, так і в інфраструктурах великих підприємств та дата-центрів, забезпечуючи захист на периметрі, між сегментами мережі, а також у середовищах із віддаленими філіями та хмарними ресурсами.

Мета роботи: дослідження технологій захисту корпоративної мережевої інфраструктури на базі рішення FortiGate, аналіз його архітектурних особливостей та функціональних можливостей, а також розробка практичних рекомендацій щодо застосування даної платформи для підвищення рівня мережевої безпеки.

Для досягнення поставленої мети у роботі передбачається вирішення таких завдань: дослідити еволюцію векторів атак та актуальні загрози для корпоративних мереж; проаналізувати обмеження традиційних підходів до мережевої безпеки; розглянути сучасні концепції багаторівневого захисту; проаналізувати архітектуру та ключові технології платформи FortiGate; розробити модель сегментації мережі з використанням FortiGate; надати рекомендації щодо практичного впровадження технологій захисту в корпоративному середовищі.

Об'єкт дослідження: корпоративна мережева інфраструктура організації.

Предмет дослідження: технології та методи захисту корпоративної мережевої інфраструктури на базі рішення FortiGate.

Практична цінність цієї роботи полягає у можливості використання отриманих результатів та рекомендацій під час проєктування, впровадження та експлуатації систем мережевої безпеки в реальних корпоративних мережах з використанням технологій сучасних міжмережевих екранів FortiGate.

1 ДОСЛІДЖЕННЯ СУЧАСНИХ ЗАГРОЗ ТА МЕТОДОЛОГІЙ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Дослідження еволюції векторів атак та актуальних загроз для сучасної корпоративної інфраструктури

Сучасні корпоративні мережі зазнали суттєвих змін у порівнянні з класичними ізольованими інфраструктурами минулих років. Масове впровадження хмарних сервісів, віддаленого доступу, мобільних пристроїв та інтеграція з зовнішніми інформаційними системами призвели до значного розширення поверхні атаки. Внаслідок цього вектори атак стали більш різноманітними, а самі атаки — складнішими та менш помітними для традиційних засобів захисту.

На початкових етапах розвитку корпоративних мереж основна увага приділялася захисту периметра. Типові атаки були спрямовані на відкриті мережеві сервіси, такі як FTP, Telnet, SMTP або HTTP, з використанням відомих вразливостей або слабких паролів [1]. Захист будувався переважно на основі статичних правил фільтрації трафіку за IP-адресами та портами. У таких умовах міжмережевий екран виконував роль основного і часто єдиного засобу безпеки.

З розвитком вебтехнологій та зростанням популярності прикладних сервісів зловмисники почали активно використовувати атаки на рівні застосунків. З’явилися масові експлуатації вразливостей вебдодатків, зокрема SQL-ін’єкції, міжсайтовий скриптинг, підміна сесій та атаки на механізми автентифікації. У таких сценаріях мережевий трафік формально відповідав дозволеним правилам доступу, що унеможливлювало його блокування класичними firewall.

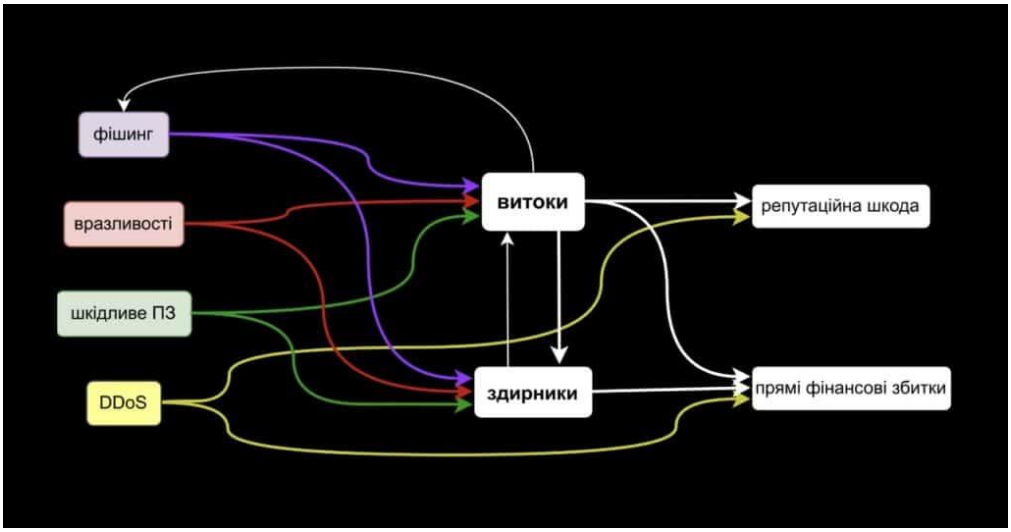

Рис. 1.1 Види та наслідки кібератак [5]

Подальша еволюція векторів атак пов’язана з появою цільових атак та складних багатоступеневих сценаріїв. Атаки типу Advanced Persistent Threat характеризуються тривалим перебуванням зловмисника в мережі, використанням декількох етапів проникнення, закріплення та розширення привілеїв. Початковий доступ часто реалізується через фішингові листи, заражені вкладення або скомпрометовані облікові дані, після чого здійснюється горизонтальне переміщення мережею та збір конфіденційної інформації.

Окрему категорію загроз становлять атаки з використанням зашифрованого трафіку. З поширенням протоколів TLS більшість корпоративного трафіку передається у зашифрованому вигляді, що ускладнює аналіз його вмісту. Зловмисники активно використовують цей факт для приховування команд керування шкідливим програмним забезпеченням, ексфільтрації даних та обходу систем виявлення атак. За відсутності механізмів інспекції зашифрованого трафіку значна частина загроз залишається непоміченою.

Суттєвий вплив на сучасний ландшафт загроз мають також атаки, спрямовані на доступність ресурсів. Розподілені атаки типу DDoS здатні призводити до повної недоступності корпоративних сервісів, що безпосередньо впливає на безперервність

бізнесу. Такі атаки часто комбінуються з іншими векторами, зокрема з метою відволікання уваги служб безпеки під час реалізації проникнення.

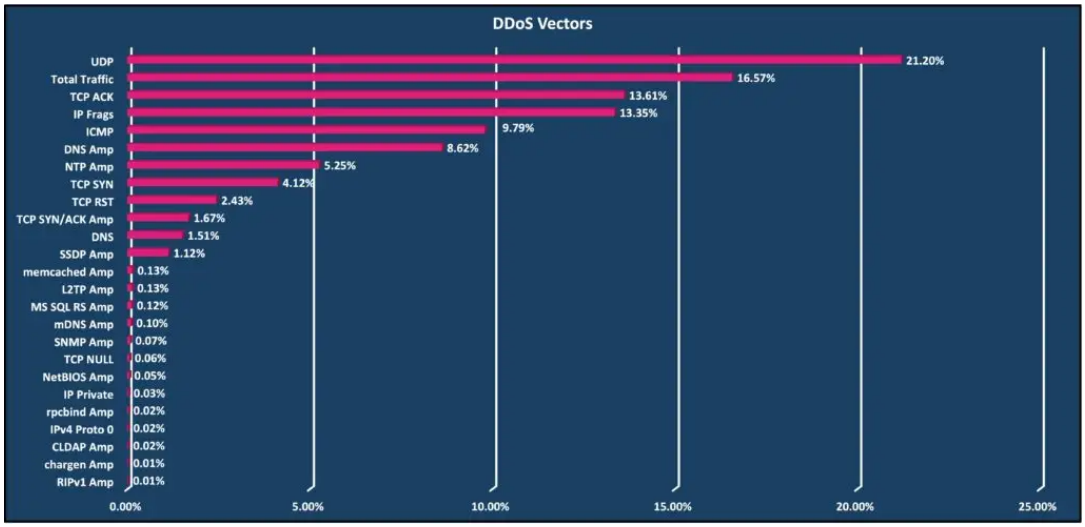

Рис 1.2 Вектори DDoS атак та їх статистика[4]

Не менш актуальними залишаються внутрішні загрози, пов’язані з діями користувачів або скомпрометованих внутрішніх пристроїв. В умовах недостатньої сегментації мережі компрометація одного вузла може призвести до поширення загрози на критичні сервіси та інформаційні ресурси організації. Саме тому сучасні атаки все частіше орієнтуються не на периметр, а на внутрішні сегменти мережі.

У відповідь на еволюцію векторів атак сформувалися сучасні підходи до захисту корпоративних мереж, які базуються на принципах багаторівневості, постійного моніторингу та контекстного аналізу трафіку. Рішення класу NGFW, до яких належить FortiGate, поєднують функції міжмережевого екрану, системи запобігання вторгненням, контролю застосунків та інспекції зашифрованого трафіку, що дозволяє ефективно протидіяти більшості актуальних загроз.

Date/Time	User	Source	Action	URL	Category	Initiator	Sent / Received
2025/12/22 11:04:08	[redacted]	[redacted]	Blocked	https://kl89regular.com/	Phishing		2.13 kB / 0 B
2025/12/22 11:04:08	[redacted]	[redacted]	Blocked	https://kl89regular.com/	Phishing		2.13 kB / 0 B
2025/12/22 11:03:58	[redacted]	[redacted]	Blocked	https://kl89regular.com/	Phishing		2.13 kB / 0 B
2025/12/22 11:03:46	[redacted]	[redacted]	Blocked	https://kl89regular.com/	Phishing		2.03 kB / 0 B
2025/12/22 11:03:45	[redacted]	[redacted]	Blocked	https://kl89regular.com/	Phishing		2.13 kB / 0 B
2025/12/22 11:03:39	[redacted]	[redacted]	Blocked	https://kl89regular.com/	Phishing		2.09 kB / 0 B
2025/12/22 11:03:24	[redacted]	[redacted]	Blocked	https://kl89regular.com/	Phishing		2.09 kB / 0 B
2025/12/22 11:03:19	[redacted]	[redacted]	Blocked	https://kl89regular.com/	Phishing		1.82 kB / 0 B

Рис 1.3 Заблокований перехід на фішингове посилання

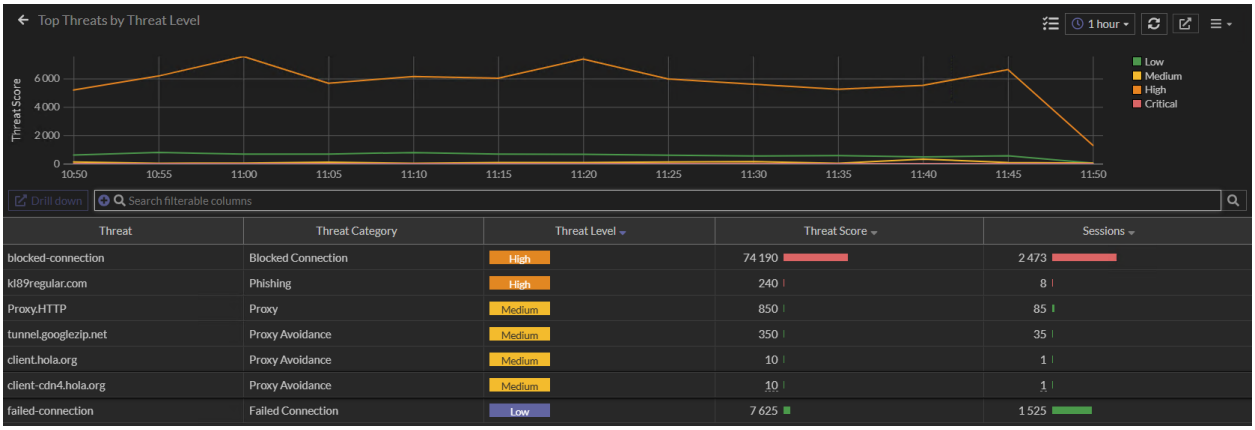

Рис 1.4 Статистика загроз вебінтерфейсу FortiGate

Це дослідження еволюції векторів атак підтверджує необхідність переходу від класичних периметрових моделей безпеки до комплексних рішень, здатних забезпечити захист на всіх рівнях корпоративної мережевої інфраструктури.

1.2 Аналіз обмежень традиційних підходів до мережевої безпеки

Традиційні підходи до забезпечення мережевої безпеки корпоративних інфраструктур формувалися в умовах, коли мережі мали чітко визначений периметр, обмежену кількість сервісів та мінімальну взаємодію із зовнішніми системами. Основою захисту виступали класичні міжмережеві екрани, які здійснювали фільтрацію трафіку на основі IP-адрес, портів та протоколів. Така модель довгий час залишалася ефективною, однак із розвитком сучасних інформаційних технологій вона виявила низку критичних обмежень.

Одним із ключових недоліків традиційних firewall є відсутність глибокого аналізу мережевого трафіку. Класичні правила доступу не враховують контекст застосунків, вміст переданих даних та поведінкові характеристики з’єднань. У результаті шкідливий трафік, який використовує дозволені порти та протоколи, може

безперешкодно проходити через систему захисту. Це особливо актуально для вебатак, які маскуються під легітимні HTTP або HTTPS-з’єднання.

Іншим суттєвим обмеженням є орієнтація виключно на периметровий захист. У традиційній моделі передбачається, що внутрішня мережа є довіреним середовищем, а основна загроза надходить ззовні. Такий підхід не враховує внутрішні загрози, зокрема компрометацію робочих станцій, зловмисні дії інсайдерів або поширення шкідливого програмного забезпечення між сегментами мережі. За відсутності внутрішньої сегментації одна успішна атака може призвести до повної компрометації інфраструктури.

Традиційні системи безпеки також мають обмежені можливості реагування на сучасні багатоступеневі атаки. Вони, як правило, не забезпечують кореляцію подій, аналіз поведінки та виявлення аномалій у режимі реального часу. Це ускладнює виявлення тривалих атак, під час яких зловмисник поступово розширює свої привілеї та переміщується мережею. У таких сценаріях атака може залишатися непоміченою протягом тривалого часу.

Окремою проблемою є недостатня ефективність традиційних підходів у роботі з зашифрованим трафіком. Класичні міжмережеві екрани не виконують розшифрування SSL або TLS-з’єднань, що робить неможливим аналіз вмісту пакетів. З урахуванням того, що переважна більшість сучасних сервісів використовує шифрування, це створює значну «сліпу зону» в системі безпеки, яку активно використовують зловмисники.

Необхідність використання окремих засобів для реалізації різних функцій безпеки також є суттєвим недоліком традиційного підходу. Для захисту мережі часто застосовуються різні продукти від різних виробників, такі як firewall, IDS, VPN-шлюзи та системи фільтрації контенту. Це ускладнює адміністрування, призводить до фрагментації політик безпеки та підвищує ймовірність помилок конфігурації.

Ще одним обмеженням є низька масштабованість класичних рішень. Зі зростанням обсягів трафіку та кількості користувачів традиційні міжмережеві екрани

часто стають вузьким місцем інфраструктури, оскільки не здатні забезпечити необхідну продуктивність без значних апаратних оновлень. Це особливо критично для організацій із розгалуженою мережею філій або високими вимогами до доступності сервісів.

Традиційні підходи до мережевої безпеки не відповідають сучасним вимогам щодо захисту корпоративних мереж. Їхні обмеження зумовлюють необхідність переходу до більш гнучких та інтегрованих рішень, які забезпечують глибокий аналіз трафіку, багаторівневий захист та централізоване управління. Саме ці вимоги стали основою для розвитку концепції міжмережевих екранів нового покоління та комплексних платформ безпеки, зокрема FortiGate.

1.3 Дослідження сучасних підходів до побудови багаторівневого захисту

Сучасні підходи до захисту корпоративної мережевої інфраструктури базуються на концепції багаторівневого захисту, яка передбачає використання декількох взаємодоповнювальних механізмів безпеки на різних рівнях мережі та інформаційних систем. Такий підхід дозволяє знизити ймовірність успішної атаки, а також мінімізувати наслідки компрометації окремих компонентів інфраструктури.

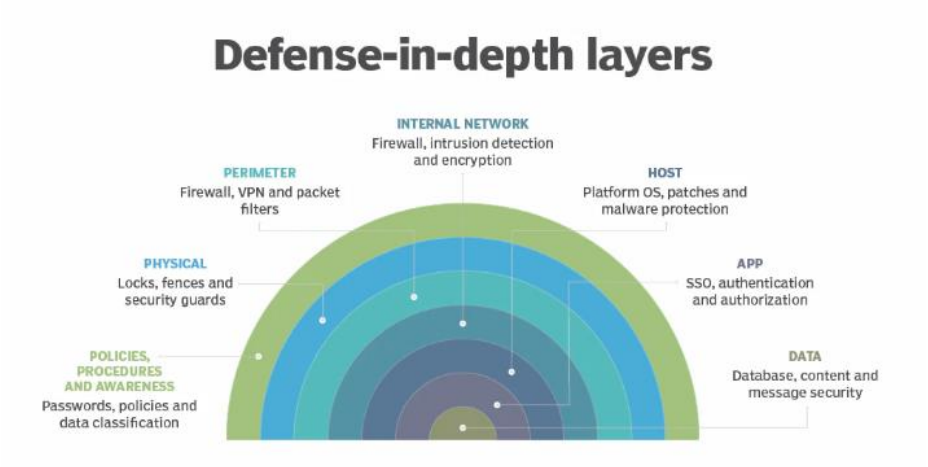

Рис 1.5 Концепція багаторівневого захисту[7]

Одним із ключових принципів багаторівневого захисту є відмова від моделі повної довіри до внутрішньої мережі. Замість цього впроваджується контроль доступу між усіма сегментами, включаючи внутрішні зони, серверні сегменти, зони віддаленого доступу та демілітаризовані зони. Кожне з'єднання розглядається як потенційно небезпечне та підлягає перевірці відповідно до визначених політик безпеки.

Важливу роль у сучасних моделях захисту відіграє сегментація мережі. Поділ інфраструктури на логічні зони з обмеженим доступом дозволяє локалізувати інциденти безпеки та запобігти поширенню загроз. Сегментація може реалізовуватися на основі VLAN, віртуальних інтерфейсів, а також за допомогою міжсегментних політик безпеки, які контролюються міжмережевими екранами нового покоління.

Наступним рівнем багаторівневого захисту є глибока інспекція мережевого трафіку. Аналіз пакетів на рівні застосунків дозволяє виявляти шкідливу активність, замасковану під легітимні сервіси. Для цього використовуються системи запобігання вторгненням, контроль застосунків, антивірусна перевірка та фільтрація вебконтенту. У сучасних рішеннях ці механізми працюють у режимі реального часу та інтегруються в єдину політику безпеки.

Окрему увагу приділяють захисту зашифрованого трафіку. Багаторівневий підхід передбачає використання механізмів SSL та TLS інспекції, які дозволяють тимчасово розшифровувати трафік для його аналізу з подальшим повторним шифруванням. Це забезпечує виявлення загроз, які передаються через захищені канали зв'язку, без порушення логіки роботи застосунків.

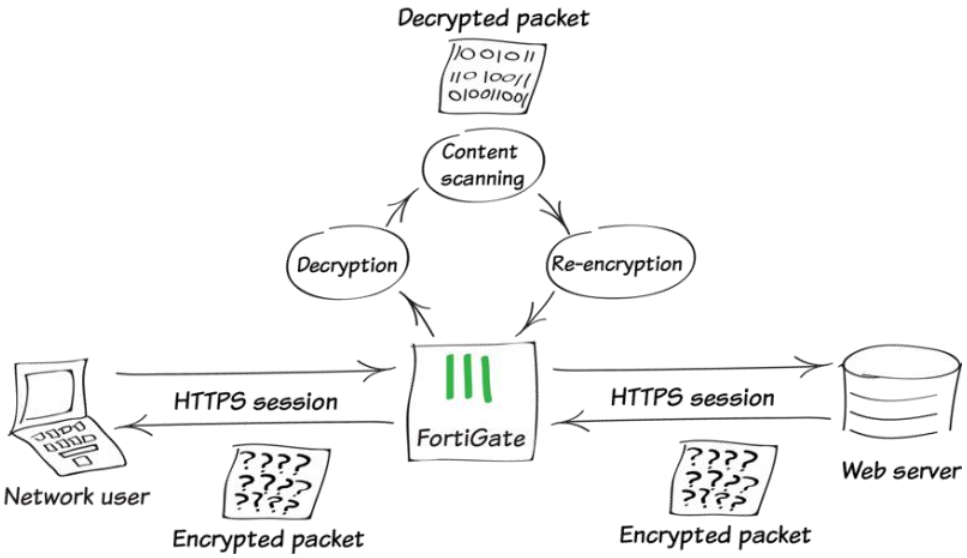

Рис 1.6 Процес глибокої перевірки шифрованого трафіку[1]

Сучасні концепції захисту також включають використання поведінкового аналізу та кореляції подій. Замість реагування на окремі сигнатури система безпеки аналізує загальну картину активності в мережі, виявляє аномалії та нетипову поведінку користувачів або пристроїв. Такий підхід особливо ефективний для виявлення цільових атак та внутрішніх загроз.

Важливою складовою багаторівневого захисту є централізоване управління та автоматизація. Сучасні платформи безпеки дозволяють керувати політиками доступу, профілями захисту та журналами подій з єдиного інтерфейсу. Це знижує ризик помилок конфігурації, підвищує швидкість реагування на інциденти та забезпечує узгодженість політик безпеки на всіх рівнях інфраструктури.

Значного поширення набуває концепція Zero Trust, яка є логічним розвитком багаторівневого підходу. Вона ґрунтується на принципі постійної перевірки користувачів, пристроїв та сервісів незалежно від їхнього розташування в мережі[4]. Доступ надається виключно на основі мінімально необхідних прав та з урахуванням контексту з’єднання, що суттєво знижує ризики несанкціонованого доступу.

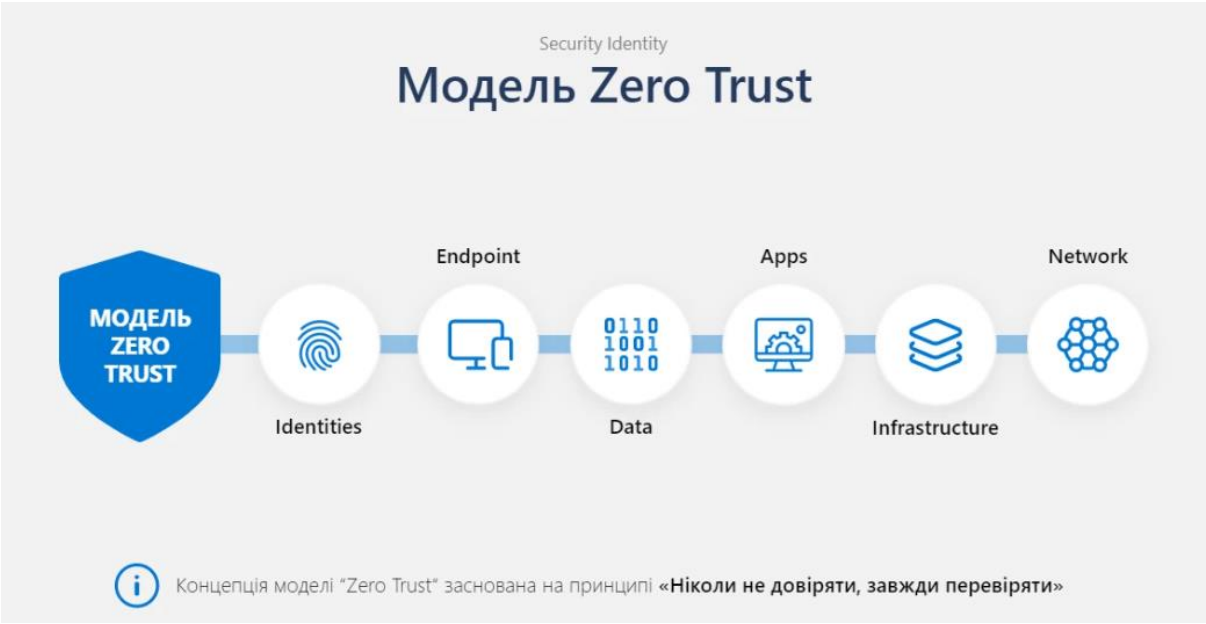

Рис 1.7 Модель Zero Trust[2]

Реалізація багаторівневого захисту корпоративної мережевої інфраструктури вимагає використання комплексних рішень, здатних об'єднувати різні механізми безпеки в межах єдиної, узгодженої архітектури. Такий підхід дозволяє забезпечити захист не лише на периметрі мережі, а й на рівні внутрішніх сегментів, користувацьких підключень і мережевого трафіку між критичними ресурсами. Платформа FortiGate повністю відповідає цим вимогам, оскільки інтегрує функції міжмережевого екрану, системи запобігання вторгненням, захисту мережевих застосунків, глибокої інспекції зашифрованого трафіку та засобів логічної сегментації мережі в межах єдиного рішення з централізованим керуванням[1].

Застосування багаторівневого захисту на базі FortiGate дозволяє реалізувати принцип «захисту в глибину», за якого кожен рівень безпеки доповнює інші та компенсує їх можливі обмеження. Навіть у разі обходу або компрометації одного з механізмів загроза може бути виявлена та заблокована на іншому рівні. Сучасні підходи до побудови багаторівневого захисту, що поєднують сегментацію мережі, контекстний контроль доступу та постійний аналіз трафіку, суттєво підвищують загальний рівень захищеності корпоративної мережевої інфраструктури. Це створює

надійну основу для ефективного впровадження та експлуатації платформ класу NGFW, зокрема FortiGate, у середовищах із підвищеними вимогами до безпеки та безперервності процесів.

Висновки до розділу

У результаті дослідження встановлено, що сучасні корпоративні мережі функціонують в умовах постійної еволюції кіберзагроз, які характеризуються багатоступеневістю, прихованістю та активним використанням зашифрованого трафіку. Традиційні периметрові підходи до безпеки не забезпечують належного рівня захисту, оскільки не враховують внутрішні загрози, атаки на рівні застосунків та складні сценарії проникнення.

Сучасні методології захисту базуються на принципах багаторівневості, сегментації мережі та постійного аналізу трафіку. Використання міжмережевих екранів нового покоління дозволяє поєднати класичні механізми фільтрації з глибокою інспекцією, що є необхідною умовою ефективного захисту корпоративної мережевої інфраструктури.

2 АНАЛІЗ АРХІТЕКТУРИ ТА ТЕХНОЛОГІЧНИХ МОЖЛИВОСТЕЙ ПЛАТФОРМИ FORTIGATE

2.1 Аналіз архітектури FortiGate: операційна система FortiOS, процесори безпеки та їх роль у продуктивності

Платформа FortiGate є апаратно-програмним комплексом, призначеним для реалізації функцій міжмережевого екрану нового покоління та комплексного захисту корпоративної мережевої інфраструктури. Архітектура FortiGate побудована з урахуванням вимог до високої продуктивності, масштабованості та можливості обробки значних обсягів мережевого трафіку з одночасним застосуванням декількох механізмів безпеки.

Основою програмної частини FortiGate є операційна система FortiOS, яка розроблена компанією Fortinet спеціально для задач інформаційної безпеки[3]. FortiOS забезпечує єдине середовище для реалізації всіх функцій захисту, включаючи міжмережевий екран, систему запобігання вторгненням, контроль застосунків, антивірусний захист, фільтрацію вебконтенту, VPN-з’єднання та механізми централізованого управління. Єдина операційна система дозволяє уникнути конфліктів між модулями безпеки та забезпечує узгоджену обробку трафіку на всіх етапах.

FortiOS побудована за модульним принципом, що дозволяє гнучко активувати або деактивувати окремі функції залежно від потреб організації. Усі політики безпеки обробляються в рамках єдиного потоку інспекції, що суттєво зменшує затримки та підвищує ефективність аналізу трафіку. Такий підхід відрізняє FortiGate від традиційних рішень, у яких кожна функція безпеки може працювати як окремий сервіс із власною логікою обробки пакетів.

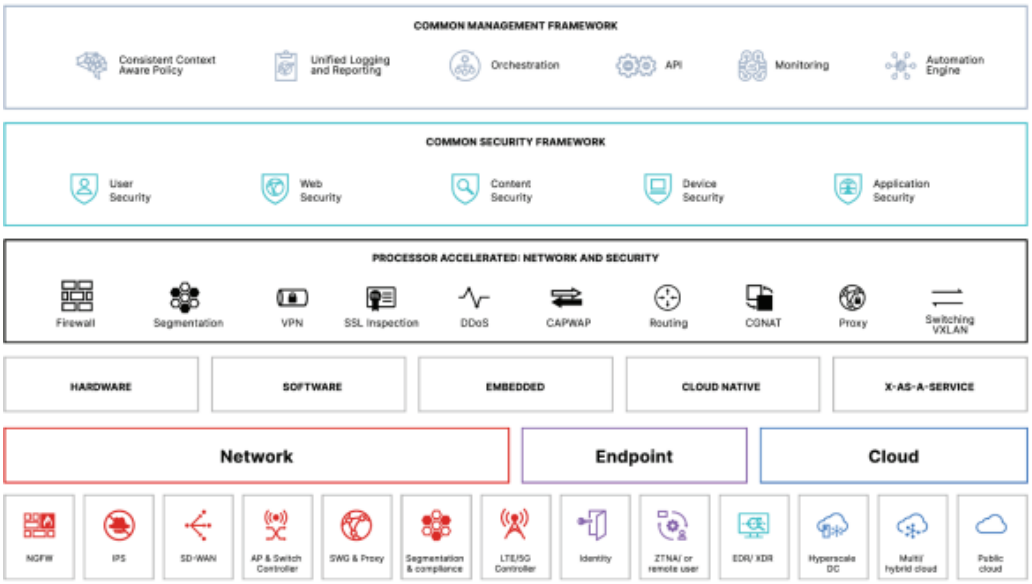

Рис. 2.1 «Зони відповідальності» FortiOS[3]

Важливою особливістю архітектури FortiGate є використання спеціалізованих апаратних процесорів безпеки, об’єднаних під загальною назвою SPU. До складу SPU входять різні типи процесорів, кожен з яких виконує окремі завдання, пов’язані з обробкою мережевого трафіку та криптографічними операціями. Такий підхід дозволяє зняти навантаження з центрального процесора та забезпечити високу продуктивність навіть при активному використанні всіх механізмів захисту.

Процесори NP призначені для прискорення мережевих операцій, таких як маршрутизація, фільтрація пакетів та трансляція адрес. Вони забезпечують обробку трафіку на канальному та мережевому рівнях без залучення центрального процесора, що суттєво знижує затримки та підвищує пропускну здатність пристрою. Завдяки NP-процесорам FortiGate здатен обробляти великі обсяги трафіку з мінімальним впливом на загальну продуктивність системи.

Процесори CP відповідають за виконання криптографічних операцій, зокрема шифрування та розшифрування VPN-з’єднань, а також обробку SSL та TLS трафіку. Використання апаратного прискорення криптографії дозволяє FortiGate ефективно працювати з великою кількістю захищених з’єднань без значного зниження

швидкодії. Це є критично важливим у сучасних корпоративних мережах, де значна частина трафіку передається у зашифрованому вигляді.

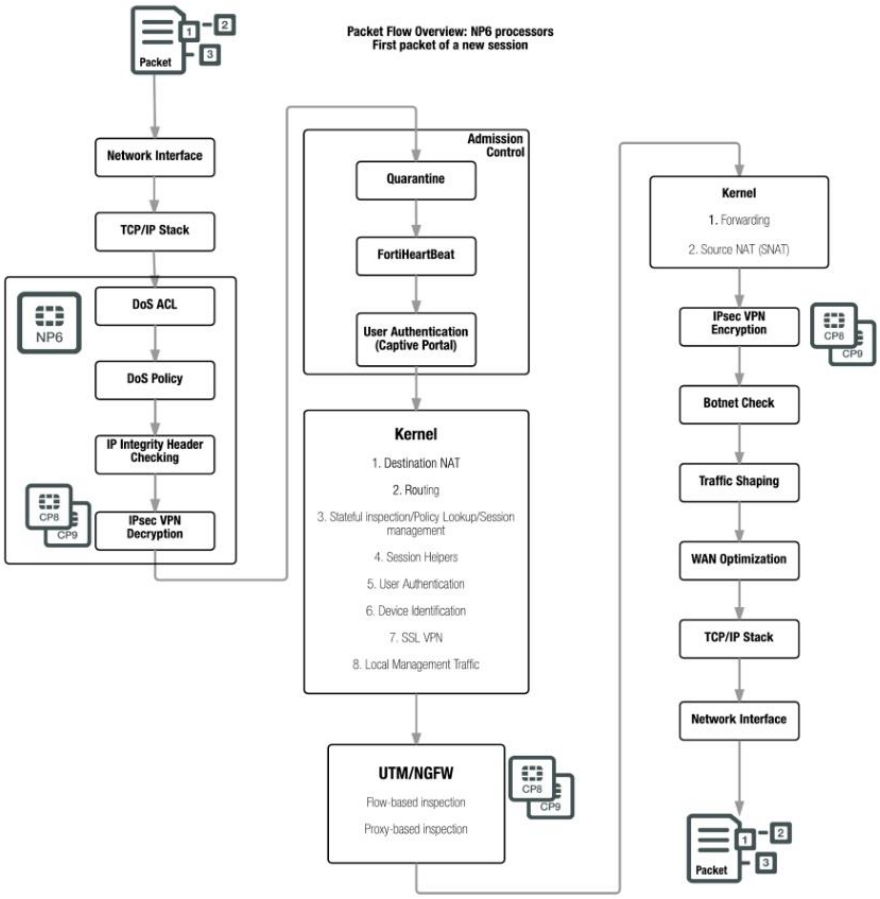

Рис. 2.2 Схема роботи CP-процесорів [3]

Окрему роль відіграють процесори SP, які забезпечують прискорення глибокої інспекції трафіку, включаючи перевірку сигнатур IPS, антивірусний аналіз та контроль застосунків. Завдяки апаратній реалізації цих функцій FortiGate здатен виконувати повноцінну перевірку трафіку в режимі реального часу без суттєвого зниження пропускної здатності.

Поєднання FortiOS та апаратних процесорів безпеки формує архітектуру, оптимізовану для комплексного захисту мережі. На відміну від програмних рішень, які покладаються виключно на ресурси центрального процесора, FortiGate забезпечує стабільну продуктивність навіть при одночасному застосуванні IPS, антивірусу, SSL-інспекції та контролю застосунків.

Таблиця 2.1 Порівняння програмної та апаратно-прискореної обробки трафіку

Критерій порівняння	**Програмна обробка трафіку (CPU)**	**Апаратно прискорена обробка трафіку (SPU)**
Основний елемент обробки	Центральний процесор загального призначення	Спеціалізовані процесори безпеки NP та CP
Пропускна здатність	Обмежена ресурсами CPU, знижується при ввімкненні профілів безпеки	Висока та стабільна навіть при активних механізмах захисту
Затримки обробки	Збільшуються при глибокій інспекції та SSL-перевірці	Мінімальні завдяки апаратному офлоадингу
Обробка firewall-трафіку	Виконується програмно при складних правилах або винятках	Основний трафік обробляється NP6 без участі CPU
IPS та контроль застосунків	Високе навантаження на CPU	Частково офлоадиться на SPU, що підвищує продуктивність
SSL VPN	Значне навантаження на CPU при великій кількості сесій	Криптографічні операції прискорюються CP9
IPsec VPN	Обмежена кількість тунелів без деградації продуктивності	Висока кількість тунелів завдяки апаратному шифруванню
Стабільність роботи	Залежить від загального навантаження системи	Стабільна при пікових навантаженнях
Масштабованість	Потребує збільшення потужності CPU або заміни пристрою	Забезпечується за рахунок апаратної архітектури

Поєднання FortiOS та апаратних процесорів безпеки формує архітектуру, оптимізовану для комплексного захисту мережі. На відміну від програмних рішень, які покладаються виключно на ресурси центрального процесора, FortiGate забезпечує стабільну продуктивність навіть при одночасному застосуванні IPS, антивірусу, SSL-інспекції та контролю застосунків.

Архітектура FortiGate також підтримує масштабування як у вертикальному, так і в горизонтальному напрямках. Залежно від потреб організації можуть використовуватися різні апаратні моделі, а також кластеризація пристроїв для підвищення доступності та продуктивності. Це дозволяє адаптувати рішення до інфраструктур різного масштабу — від невеликих офісів до великих корпоративних мереж і дата-центрів.

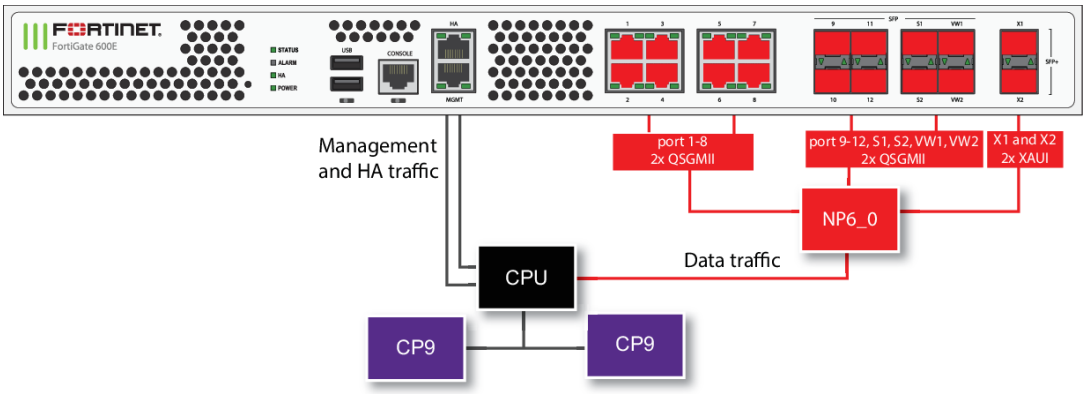

Рис 2.3 Архітектура FortiGate-600e з розподілом CPU,NP,CP

Таким чином, архітектура FortiGate, побудована на базі операційної системи FortiOS та спеціалізованих процесорів безпеки, забезпечує високий рівень продуктивності та надійності, що є ключовим фактором для ефективного захисту сучасної корпоративної мережевої інфраструктури.

2.2 Дослідження ключових технологій захисту, інтегрованих у FortiGate

Платформа FortiGate реалізує комплексний підхід до захисту корпоративної мережевої інфраструктури шляхом інтеграції декількох ключових технологій безпеки в межах єдиної операційної системи FortiOS. Така інтеграція дозволяє забезпечити узгоджену політику захисту, зменшити складність адміністрування та підвищити ефективність протидії сучасним кіберзагрозам.

Однією з базових технологій захисту є міжмережевий екран нового покоління. FortiGate забезпечує фільтрацію трафіку не лише на основі IP-адрес та портів, але й з урахуванням застосунків, користувачів та контексту з'єднання. Контроль застосунків дозволяє ідентифікувати тисячі різних сервісів і протоколів незалежно від використовуваного порту, що особливо важливо для сучасних вебзастосунків та хмарних сервісів.

Система запобігання вторгненням є ключовим компонентом захисту FortiGate. IPS здійснює глибоку інспекцію пакетів та порівнює трафік із сигнатурами відомих атак, а також застосовує поведінкові методи виявлення загроз. Регулярне оновлення сигнатур дозволяє оперативно реагувати на нові вразливості та експлойти, що з'являються в сучасних інформаційних системах.

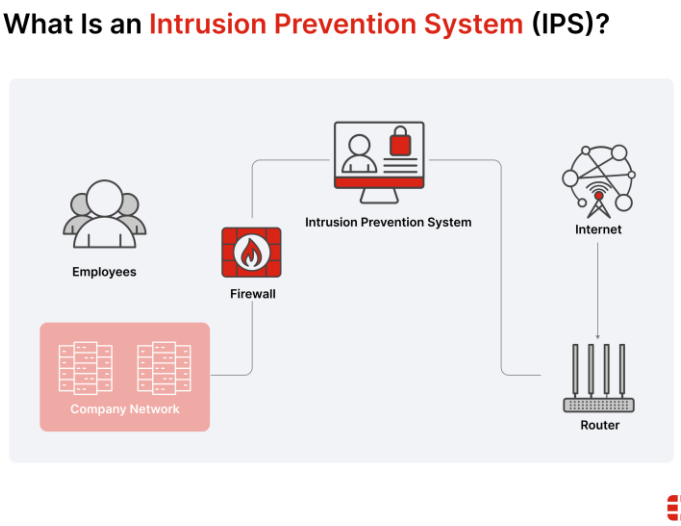

Рис 2.4 Принцип роботи IPS[3]

Антивірусний захист у FortiGate забезпечує перевірку файлів, що передаються мережею, з метою виявлення шкідливого програмного забезпечення. Аналіз виконується для різних протоколів, включаючи HTTP, HTTPS, SMTP, POP3 та FTP. У поєднанні з інспекцією зашифрованого трафіку це дозволяє блокувати шкідливі об’єкти ще на етапі їхнього завантаження в корпоративну мережу.

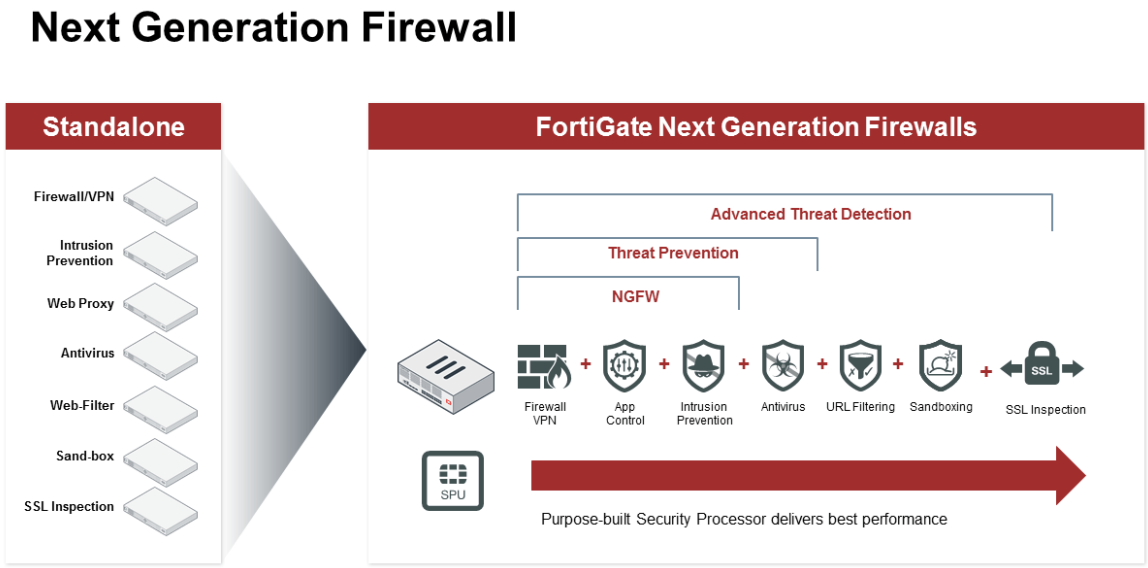

Рис. 2.5 FortiGate NGFW. [3]

Фільтрація вебконтенту є важливою технологією захисту, спрямованою на обмеження доступу користувачів до небажаних або потенційно небезпечних ресурсів мережі Інтернет. FortiGate використовує категоризацію вебсайтів та політики доступу для зниження ризиків зараження шкідливим програмним забезпеченням, а також для підвищення продуктивності роботи персоналу.

Особливе значення має інспекція SSL та TLS трафіку, яка дозволяє FortiGate аналізувати зашифровані з’єднання без втрати контролю над вмістом переданих даних. У рамках цієї технології трафік тимчасово розшифровується, проходить перевірку антивірусом та IPS, після чого знову шифрується та передається адресату. Такий підхід дозволяє усунути «сліпі зони» в системі безпеки. Технології VPN, реалізовані у FortiGate, забезпечують захищений віддалений доступ

користувачів та безпечне з'єднання між філіями організації. Підтримка IPsec та SSL VPN дозволяє адаптувати рішення до різних сценаріїв використання, а апаратне прискорення криптографічних операцій забезпечує високу продуктивність навіть при великій кількості одночасних підключень.

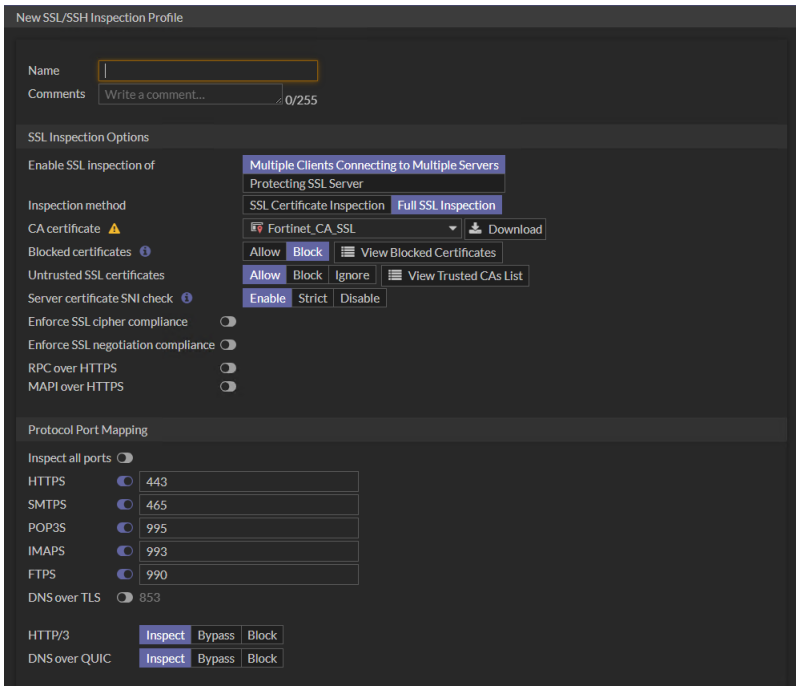

Рис 2.6 Налаштування SSL інспекції

Окрему роль відіграє інтеграція FortiGate з сервісами глобальної розвідки загроз FortiGuard. Вони є важливим складником екосистеми безпеки Fortinet і забезпечують актуальну інформаційну підтримку для механізмів захисту, інтегрованих у платформи FortiGate.

Вони базуються на глобальній інфраструктурі збору та аналізу даних про кіберзагрози, що включає центри обробки загроз, сенсори та аналітичні платформи. Завдяки цьому FortiGate отримує постійно оновлювані бази сигнатур для систем запобігання вторгненням, антивірусного захисту, вебфільтрації, контролю застосунків та репутаційних сервісів, що дозволяє оперативно реагувати на нові та модифіковані загрози.

Використання сервісів FortiGuard дає змогу реалізувати динамічний підхід до мережевої безпеки, за якого політики захисту адаптуються до актуального рівня загроз. Зокрема, сервіси репутації IP-адрес і доменів дозволяють блокувати підозрілий трафік ще на початкових етапах з'єднання, а сервіси аналізу вебконтенту та застосунків — обмежувати доступ до потенційно небезпечних ресурсів. Така інтеграція хмарних сервісів загроз з локальними механізмами FortiGate підвищує загальну ефективність захисту корпоративної мережевої інфраструктури без істотного зниження продуктивності.

Рис 2.7 Сервіси FortiGuard

Окрім функцій виявлення та блокування загроз, сервіси FortiGuard відіграють важливу роль у забезпеченні централізованого та уніфікованого підходу до управління безпекою. Використання єдиних джерел аналітичних даних дозволяє узгоджувати роботу різних механізмів захисту, зменшувати кількість помилкових спрацювань та спрощувати адміністрування політик безпеки.

Таблиця 2.2 Сервіси FortiGuard та їх опис

Сервіс FortiGuard	Призначення	Короткий опис функціоналу	Практичне застосування у FortiGate
Antivirus	Захист від шкідливого ПЗ	Виявлення та блокування відомих і нових зразків шкідливого програмного забезпечення	Перевірка файлів у вебтрафіку, пошті, FTP та зашифрованих сесіях
Intrusion Prevention	Запобігання вторгненням	Виявлення та блокування мережевих атак на основі сигнатур і поведінки	Захист серверів і робочих станцій від експлойтів та сканування
Mobile Security	Захист мобільних пристроїв	Аналіз загроз, пов’язаних із мобільними платформами та застосунками	Контроль доступу мобільних пристроїв до корпоративної мережі
Threat Intelligence Service	Глобальна розвідка загроз	Збір і кореляція даних про актуальні кіберзагрози з усього світу	Актуалізація політик безпеки та реакція на нові загрози
Antispam	Захист від спаму	Фільтрація небажаної та фішингової електронної пошти	Захист поштових серверів від спаму та соціальної інженерії
Vulnerability Management	Управління вразливостями	Аналіз відомих вразливостей програмного забезпечення та систем	Пріоритизація ризиків і посилення політик захисту
Virus Outbreak Protection Service	Захист від масових спалахів вірусів	Швидке реагування на глобальні епідемії шкідливого ПЗ	Оперативне блокування zero-day та масових атак
IP Reputation	Репутація IP-адрес	Оцінка надійності IP-адрес на основі глобальної статистики	Блокування трафіку з ботнетів і зловмисних хостів
Content Disarm & Reconstruction	Безпечна обробка контенту	Видалення потенційно небезпечного активного вмісту з файлів	Захист від прихованих загроз у документах
Industrial Security	Захист промислових мереж	Захист SCADA та OT-протоколів	Безпека промислових та критичних інфраструктур
Cloud Access Security Broker	Контроль хмарних сервісів	Моніторинг і контроль використання хмарних застосунків	Захист даних при роботі з SaaS та хмарними платформами

Продовження таблиці 2.2

Application Control	Контроль застосунків	Ідентифікація та управління мережевими застосунками	Обмеження небажаних або ризикованих сервісів
Web Filtering	Фільтрація вебконтенту	Категоризація та блокування небезпечних сайтів	Захист користувачів від фішингу та malware
Security Rating Service	Оцінка рівня безпеки	Аналіз конфігурації та відповідності best practices	Аудит та підвищення загального рівня безпеки
Web Security	Захист вебдоступу	Комплексний захист HTTP/HTTPS трафіку	Запобігання вебатакам і зараженню через браузер
Indicators of Compromise	Індикатори компрометації	Дані про ознаки зараження та атак	Швидке виявлення скомпрометованих хостів

Централізоване управління та моніторинг є важливою складовою технологій захисту FortiGate. Вебінтерфейс FortiOS надає засоби для аналізу журналів подій, перегляду статистики трафіку та налаштування політик безпеки. Це забезпечує повну видимість стану мережі та дозволяє оперативно виявляти підозрілу активність.

2.3 Порівняльний аналіз функціонала FortiGate з альтернативними рішеннями

Для обґрунтування доцільності використання платформи FortiGate у корпоративній мережевій інфраструктурі важливо провести порівняльний аналіз її функціональних можливостей з альтернативними рішеннями класу міжмережевих екранів нового покоління. До найбільш поширених конкурентних продуктів у цьому сегменті належать рішення Palo Alto Networks, Check Point та Cisco Firepower, які також використовуються для захисту корпоративних мереж різного масштабу.

Однією з ключових відмінностей FortiGate є тісна інтеграція програмних механізмів захисту з апаратним прискоренням. Завдяки використанню власних процесорів безпеки SPU FortiGate забезпечує стабільну високу продуктивність навіть при активному застосуванні IPS, антивірусу, контролю застосунків та інспекції SSL. У багатьох альтернативних рішеннях значна частина цих функцій реалізується

програмно, що призводить до зниження пропускної здатності при зростанні навантаження.

FortiGate вирізняється єдиною операційною системою FortiOS, у межах якої реалізовані всі функції безпеки. Це забезпечує узгоджену логіку обробки трафіку та спрощує адміністрування. У деяких альтернативних платформах окремі модулі безпеки можуть мати різні механізми керування або залежати від додаткових компонентів, що ускладнює підтримку та оновлення системи.

З точки зору масштабованості FortiGate підтримує широкий спектр апаратних моделей — від пристроїв для малих офісів до високопродуктивних рішень для дата-центрів. Можливість побудови кластерів високої доступності дозволяє забезпечити безперервність роботи мережевої інфраструктури. Альтернативні рішення також підтримують масштабування, однак у деяких випадках це потребує значних фінансових витрат або складнішої архітектури.

Особливу увагу варто приділити співвідношенню функціональності та вартості. FortiGate, як правило, пропонує широкий набір функцій безпеки в межах однієї платформи без необхідності придбання значної кількості окремих ліцензій. У конкурентних продуктах деякі функції можуть вимагати додаткового ліцензування або окремих апаратних модулів, що збільшує загальну вартість володіння.

FortiGate також має перевагу у вигляді інтеграції з екосистемою Fortinet Security Fabric, яка дозволяє об’єднувати міжмережеві екрани, системи аналізу подій, захист кінцевих пристроїв та інші компоненти в єдину систему безпеки. Це забезпечує кращу видимість подій та централізоване реагування на інциденти. У альтернативних виробників подібні екосистеми також існують, однак часто мають вищий поріг складності впровадження.

Разом із тим слід зазначити, що деякі альтернативні рішення мають власні сильні сторони. Наприклад, окремі платформи відомі розвинутими механізмами аналізу застосунків або зручними інструментами управління політиками у великих розподілених мережах

Таблиця 2.3 Порівняння функціональних можливостей FortiGate та альтернативних рішень класу NGFW.

Критерій порівняння	FortiGate	Palo Alto Networks	Check Point	Cisco Firepower
Апаратне прискорення	Власні SPU процесори	Обмежене	Обмежене	Частково
Єдина ОС	FortiOS	PAN-OS	Gaia	FXOS
IPS та AV	Інтегровані	Інтегровані	Інтегровані	Інтегровані
SSL inspection	Апаратно прискорена	Програмна	Програмна	Програмна
Threat Intelligence	FortiGuard	WildFire	ThreatCloud	Talos
Масштабованість	Висока	Висока	Висока	Висока
Вартість володіння	Помірна	Висока	Висока	Висока
Простота адміністрування	Висока	Середня	Середня	Середня

Порівняльний аналіз свідчить, що платформа FortiGate є конкурентоспроможним рішенням для захисту корпоративної мережевої інфраструктури та забезпечує ефективне поєднання продуктивності, функціональності та економічної доцільності, що робить її доцільним вибором для впровадження в сучасних корпоративних мережах.

Висновки до розділу

Дане рішення забезпечує комплексний підхід до мережевої безпеки за рахунок використання єдиної операційної системи FortiOS та спеціалізованих апаратних процесорів безпеки. Така архітектура дозволяє зберігати високу продуктивність навіть при активному використанні механізмів захисту.

Порівняльний аналіз із альтернативними рішеннями підтвердив конкурентоспроможність FortiGate завдяки оптимальному поєднанню функціональності, продуктивності та вартості володіння.

3 ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

3.1 Розробка моделі мережевої сегментації на базі FortiGate для ізоляції критичних активів та стримування загроз

Мережева сегментація є одним із найбільш ефективних практичних підходів до підвищення безпеки корпоративної інфраструктури, оскільки дозволяє обмежити поширення загроз, зменшити поверхню атаки та забезпечити контрольований доступ до критичних ресурсів. У сучасних умовах, коли значна частина інцидентів починається з компрометації звичайної робочої станції, сегментація виконує роль механізму стримування, який не дозволяє зловмиснику вільно переміщатися мережею та досягати серверних або управлінських сегментів.

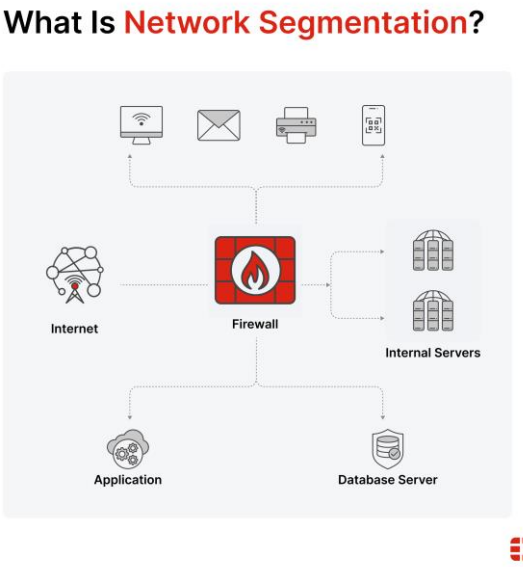

Рис. 3.1 Схема мережевої сегментації [3]

Побудова моделі сегментації на базі FortiGate має низку переваг, оскільки платформа FortiOS забезпечує одночасно маршрутизацію між підмережами, фільтрацію трафіку, застосування профілів безпеки та централізоване керування політиками. Це дозволяє реалізувати логічну архітектуру мережі, де FortiGate

виступає контрольним вузлом для всіх міжсегментних взаємодій. Таким чином, будь-який трафік між сегментами проходить через політики безпеки, що унеможливлює неконтрольоване переміщення загроз.

Першим етапом розробки моделі сегментації є визначення сегментів мережі на основі функцій, рівнів довіри та критичності активів. Для типової корпоративної інфраструктури доцільно формувати такі основні сегменти: сегмент користувачів, серверний сегмент, сегмент керування, зона публічних сервісів, гостьова мережа, сегмент віддаленого доступу та, за потреби, окремий сегмент для IoT або периферійних пристроїв. Кожен із цих сегментів має різні рівні ризику та різні вимоги до доступу.

Сегмент користувачів включає робочі станції співробітників і є найбільш уразливим через людський фактор, фішинг, заражені файли та помилки користувачів. Основне завдання сегментації в цьому випадку полягає в тому, щоб не дозволити компрометації робочої станції перерости в компрометацію серверів або систем керування. Тому доступ користувачів до серверного сегмента має бути обмежений лише конкретними сервісами та лише для визначених груп. Наприклад, доступ до файлового сервера може бути дозволений по SMB, доступ до ERP-системи по конкретному TCP-порту, а доступ до адміністративних сервісів на кшталт RDP чи SSH має бути заборонений звичайним користувачам.

Рис. 3.2 Створений окремий VLAN для користувачів

Серверний сегмент включає системи, що зберігають або обробляють критичну інформацію. До таких належать доменні контролери, сервери баз даних, файлові сховища, сервери додатків та інші ключові компоненти. Для серверного сегмента важливою є мінімізація доступу з інших зон, а також захист від мережевих атак через застосування IPS, антивірусу та контролю застосунків. Важливою практикою є

розділення серверного сегмента на підсегменти, якщо це необхідно, наприклад окремо для серверів автентифікації, окремо для баз даних, окремо для прикладних серверів, оскільки ризики та необхідні правила доступу можуть відрізнятися.

Сегмент керування призначений для адміністрування мережевого обладнання, серверів та систем безпеки і є одним із найбільш критичних елементів корпоративної мережевої інфраструктури. Компрометація цього сегмента може призвести до повної втрати контролю над мережею, зміни політик безпеки або відключення захисних механізмів. Саме тому сегмент керування повинен бути максимально ізольованим від користувацьких, серверних і публічних сегментів, а будь-які прямі з’єднання з ним мають бути заборонені за замовчуванням.

Доступ до сегмента керування надається виключно адміністративному персоналу з використанням захищених протоколів, таких як HTTPS, SSH або SNMPv3, із застосуванням додаткових механізмів автентифікації. У моделі сегментації на базі FortiGate контроль доступу до керування може здійснюватися за кількома критеріями одночасно, зокрема за IP-адресами адміністративних станцій, ролями користувачів, належністю до визначених груп та часовими обмеженнями. Такий підхід дозволяє обмежити адміністративний доступ лише необхідними сценаріями та зменшити ризик несанкціонованого підключення.

Крім того, FortiGate надає можливість застосовувати окремі політики безпеки для керуючого трафіку, що дозволяє вести детальне журналювання адміністративних дій і здійснювати їх подальший аудит. Поєднання ізоляції сегмента керування, суворого контролю доступу та постійного моніторингу адміністративної активності забезпечує високий рівень захисту критичних елементів корпоративної мережевої інфраструктури та відповідає сучасним вимогам до побудови захищених мереж.

Зона DMZ використовується для розміщення публічних сервісів, які повинні бути доступні з мережі Інтернет або інших зовнішніх мереж, таких як партнерські чи філіальні підключення. Основною метою створення DMZ є ізоляція

зовнішньодоступних серверів від внутрішньої корпоративної мережі з метою мінімізації ризиків у разі їх компрометації. Сервери, розміщені в DMZ, зазвичай надають вебсервіси, поштові шлюзи, VPN-портали або інші публічні служби, які потенційно є першою ціллю для атак з боку зловмисників.

Навіть у разі успішної атаки на сервер у DMZ зловмисник не повинен отримати прямий або неконтрольований доступ до внутрішніх ресурсів організації. У середовищі FortiGate це досягається за рахунок чіткого розмежування мережевих сегментів та застосування принципу мінімальних привілеїв. Для обробки вхідних з'єднань із зовнішніх мереж налаштовуються механізми Virtual IP або port forwarding, які дозволяють перенаправляти трафік лише на конкретні сервери та сервіси в DMZ. При цьому створюються окремі політики доступу з напрямку WAN до DMZ, у яких визначаються дозволені протоколи, порти та джерела підключення.

Додатково FortiGate надає можливість застосовувати до трафіку в зоні DMZ профілі безпеки, такі як система запобігання вторгненням, антивірусний захист і вебфільтрація, що дозволяє виявляти та блокувати атаки ще на етапі їх спроби реалізації. Обмеження вихідних з'єднань із DMZ до внутрішньої мережі або Інтернету, детальне логування подій та постійний моніторинг активності забезпечують підвищений рівень контролю й безпеки публічних сервісів, розміщених у зоні DMZ.

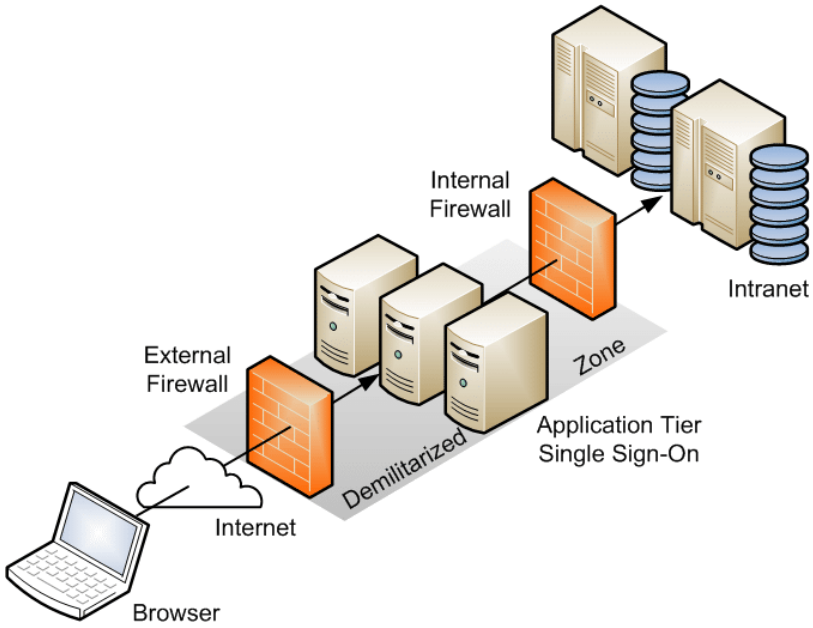

Рис.3.3 Механіка роботи DMZ-зони

Гостьовий сегмент призначений для відвідувачів або персональних пристроїв, які не повинні мати доступу до внутрішніх ресурсів. Найбільш правильним підходом є повна ізоляція гостьового сегмента від корпоративних підмереж та надання доступу лише до Інтернету

Рис. 3.3 Приклад створення гостьової мережі WI-FI

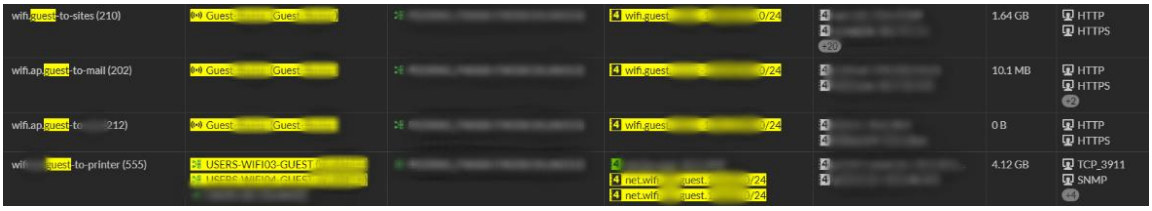

Рис 3.4 Правила для ізольованого доступу сегменту

На цих рисунках можна побачити успішну практику відділення гостьової частини мережі.

Рисунок 3.2 показує наявність гостьової мережі, яка виступає об’єктом для впровадження відповідних правил доступу. Рисунок 3.3 відображає створені правила доступу. Перша колонка – назва правила, друга колонка – вхідний інтерфейс, третя колонка – вихідний інтерфейс, четверта колонка – джерела/об’єкти інтерфейсу, п’ята колонка – адреса призначення(конкретна адреса на вихідному інтерфейсі), шоста колонка – кількість трафіку, який пройшов за цим правилом, сьома колонка – сервіси(порти), на які трафік може потрапити.

Сегмент віддаленого доступу формується для користувачів, які підключаються до корпоративної мережі за допомогою технологій IPsec або SSL VPN, і є важливим елементом сучасної мережевої інфраструктури. Такі підключення зазвичай здійснюються з неконтрольованих або частково контрольованих середовищ, що підвищує ризики для безпеки внутрішньої мережі. У зв’язку з цим у моделі сегментації доцільно розглядати VPN-користувачів як окрему зону з обмеженим рівнем довіри, а не прирівнювати їх до повноцінних внутрішніх користувачів корпоративної мережі.

У середовищі FortiGate сегмент віддаленого доступу ізолюється шляхом створення окремих інтерфейсів або тунельних зон для VPN-з’єднань та застосування спеціалізованих політик доступу. Контроль доступу для таких користувачів здійснюється на основі належності до визначених груп користувачів, що дозволяє реалізувати рольову модель доступу. Наприклад, користувачам бухгалтерії може бути надано доступ виключно до фінансових сервісів і баз даних, адміністраторам — до серверів керування та інфраструктурних ресурсів, а підрядникам — лише до окремого сервера або вебресурсу, необхідного для виконання конкретних завдань.

Крім того, FortiGate дозволяє застосовувати до VPN-трафіку додаткові профілі безпеки, включаючи антивірусний захист, контроль застосунків і систему запобігання вторгненням, що знижує ризик проникнення шкідливого трафіку у внутрішні

сегменти мережі. Поєднання сегментації VPN-користувачів, рольового контролю доступу та багаторівневого аналізу трафіку забезпечує безпечну організацію віддаленого доступу без порушення принципів ізоляції та мінімальних привілеїв у корпоративній мережевій інфраструктурі.

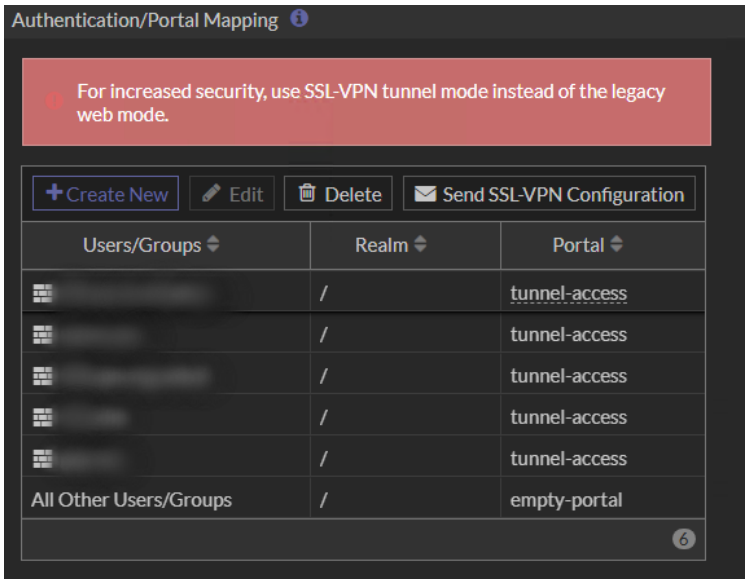

Рис 3.5 Конфігурація доступу до VPN за групами користувачів

Після визначення сегментів формується матриця доступу, яка описує, які сегменти можуть взаємодіяти між собою і які сервіси дозволені. Матриця доступу є практичним інструментом для уникнення надмірних дозволів, оскільки дозволяє одразу побачити зайві зв’язки та скоротити їх до мінімуму.

Таблиця 3.1 Приклад матриці доступу

Джерело	Призначення	Дозволені сервіси	Дія
Users	Internet	HTTP/HTTPS, DNS, NTP	allow
Users	Servers	RDP/SSH лише для адмінів, доступ до сервісів	allow/deny
Guest	Internet	HTTP/HTTPS, DNS	allow
Guest	Internal	будь-що	deny
Mgmt	FortiGate/Servers/Switches	HTTPS, SSH, SNMP, RDP	allow
DMZ	Internal	тільки необхідні з’єднання (наприклад до DB)	allow мінімально

Далі визначається технічний спосіб реалізації сегментів. У FortiGate найчастіше застосовується VLAN-сегментація, коли кожен сегмент має власний VLAN ID, власну IP-підмережу, а FortiGate виступає шлюзом для кожного VLAN. У такому сценарії між FortiGate та комутатором налаштовується trunk, після чого на FortiGate створюються VLAN-інтерфейси для кожної підмережі.

Після створення інтерфейсів налаштовується адресація і, за потреби, DHCP для сегментів. Важливим є коректне налаштування маршрутизації, зокрема default route у напрямку провайдера, та при наявності кількох каналів, політики маршрутизації або SD-WAN.

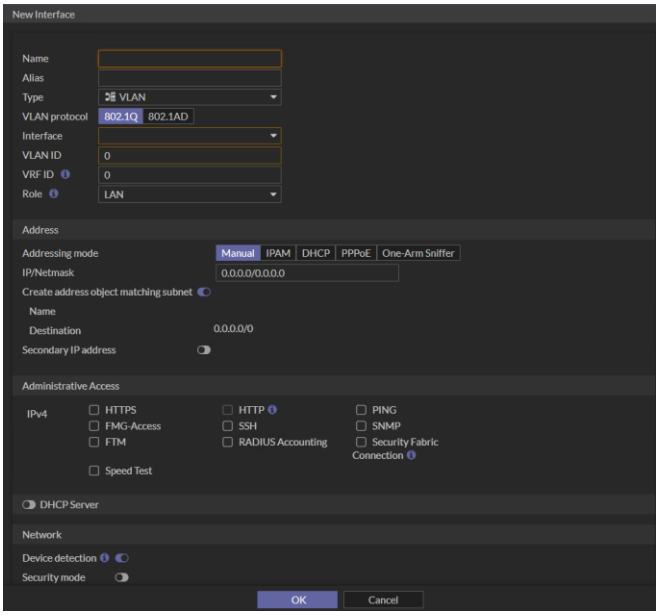

Рис 3.6 Меню створення нового інтерфейсу (VLAN)

Центральним елементом реалізації сегментації в корпоративній мережі є коректне формування політик безпеки у FortiGate. Саме політики визначають логіку взаємодії між сегментами мережі та забезпечують контроль доступу відповідно до вимог процесів. Основним принципом побудови таких політик є дозвіл лише

необхідних мережевих з’єднань і явна заборона всього іншого трафіку, що відповідає концепції мінімальних привілеїв та значно знижує ризик несанкціонованого доступу.

На практиці це означає, що для кожного дозволеного процесу створюється окрема політика з чітко визначеними параметрами, зокрема джерелом трафіку, його призначенням, переліком дозволених сервісів і, за потреби, належністю користувачів до відповідних груп. Такий підхід дозволяє легко відслідковувати призначення кожного правила, спрощує аналіз конфігурації та зменшує ймовірність помилок під час адміністрування.

Для підвищення якості, структурованості та читабельності конфігурації широко використовуються адресні об’єкти для опису підмереж і окремих вузлів, об’єкти сервісів для портів і протоколів, а також групи об’єктів для об’єднання однотипних елементів. Застосування стандартизованих і зрозумілих назв правил і об’єктів полегшує подальший супровід системи, аудит політик і масштабування мережевої інфраструктури, що є особливо важливим для корпоративних середовищ із великою кількістю сегментів та складною логікою доступу.

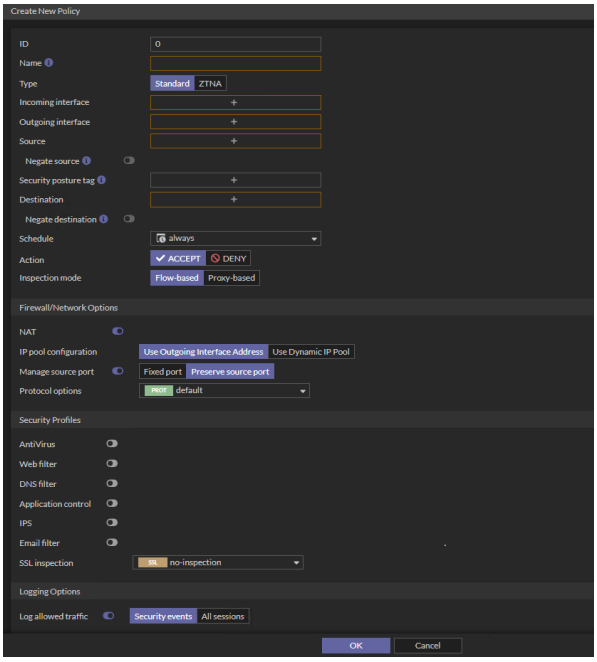

Рис. 3.7 Вікно створення сегментаційних політик

Окремо важливо зазначити, що сегментація мережі лише на рівні дозволу або заборони трафіку не забезпечує повноцінного захисту корпоративної мережевої інфраструктури. Практика кіберінцидентів свідчить, що більшість сучасних атак реалізуються саме через дозволені канали зв'язку, зокрема через вебдоступ, електронну пошту або легітимні застосунки. У таких випадках зловмисний трафік формально відповідає правилам доступу, але містить шкідливий вміст або експлуатує вразливості на рівні застосунків, що робить просту фільтрацію недостатньою.

З огляду на це в середовищі FortiGate до міжсегментних політик доцільно застосовувати профілі безпеки, які забезпечують глибоку інспекцію дозволеного трафіку. Для користувацького сегмента у напрямку Інтернету зазвичай використовуються профілі вебфільтрації, антивірусного захисту, системи запобігання вторгненням та контролю застосунків, а за необхідності - механізми інспекції зашифрованого SSL-трафіку. Такий набір дозволяє блокувати доступ до шкідливих або небажаних ресурсів, виявляти шкідливе програмне забезпечення та обмежувати використання ризикових застосунків без порушення роботи легітимних сервісів.

Для трафіку між користувацьким і серверним сегментами доцільно застосовувати IPS-профілі, орієнтовані на захист серверних служб і прикладних протоколів, а також суворо обмежувати перелік дозволених сервісів відповідно до реальних потреб. Це дозволяє зменшити ризик lateral movement у разі компрометації робочої станції та підвищує захищеність критичних серверних ресурсів. У зоні DMZ обов'язковим є застосування IPS і максимально жорстких правил доступу, а також розділення політик для вхідного та вихідного трафіку. Такий підхід дозволяє контролювати як доступ зовнішніх користувачів до публічних сервісів, так і ініційовані з DMZ з'єднання, мінімізуючи ризик використання публічних серверів як точки входу у внутрішню мережу.

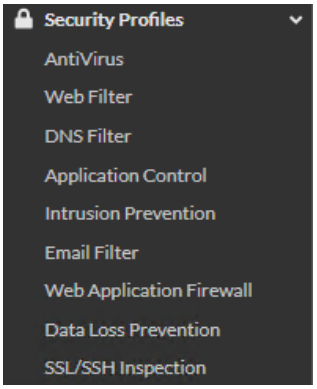

Рис. 3.8 Перелік профілів безпеки

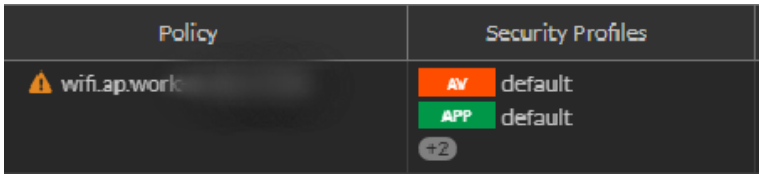

Рис 3.9 Увімкнені профілі безпеки на правилі доступу

Після налаштування політик виконується тестування та валідація сегментації. На практиці перевіряється, що клієнти отримують адреси в правильних VLAN, що дозволені зв'язки працюють, а заборонені блокуються. Додатково аналізуються журнали трафіку, щоб підтвердити роботу правил. У разі виявлення проблем застосовуються вбудовані діагностичні інструменти, зокрема перевірка відповідної політики для з'єднання та аналіз причин блокування.

У процесі експлуатації сегментація повинна підтримуватися шляхом регулярного перегляду політик, видалення застарілих правил, мінімізації широких дозволів та контролю міжсегментного трафіку за журналами. Будь-які зміни виконуються з попереднім резервним копіюванням конфігурації та подальшою перевіркою процесів.

Розробка моделі мережевої сегментації на базі FortiGate базується на послідовному визначенні сегментів та матриці доступу, технічній реалізації сегментів через VLAN або фізичні інтерфейси, побудові міжсегментних політик з принципом мінімальних привілеїв, застосуванні профілів безпеки до дозволеного трафіку та постійній валідації за допомогою журналів і діагностики. Така модель забезпечує

ізоляцію критичних активів та ефективне стримування загроз у корпоративній мережевій інфраструктурі.

3.2 Технологія застосування FortiGate

Технологія застосування FortiGate у корпоративній мережевій інфраструктурі ґрунтується на використанні платформи як центрального елемента контролю, фільтрації та аналізу мережевого трафіку. FortiGate у цій моделі виконує роль не лише периметрового міжмережевого екрана, а й універсального вузла безпеки, через який проходять усі критично важливі з'єднання між сегментами мережі, зовнішніми ресурсами та віддаленими користувачами. Такий підхід дозволяє реалізувати єдину політику безпеки та забезпечити повну видимість подій у корпоративній мережі.

Практичне впровадження FortiGate починається з його інтеграції в мережеву архітектуру організації. Найчастіше FortiGate встановлюється на периметрі мережі як шлюз між внутрішньою інфраструктурою та мережею Інтернет. У цьому сценарії пристрій забезпечує маршрутизацію, трансляцію адрес, фільтрацію вхідного та вихідного трафіку, а також контроль доступу між внутрішніми сегментами. При використанні VLAN або зон FortiGate стає центральною точкою міжсегментного контролю, що дозволяє реалізувати модель Zero Trust у межах корпоративної мережі.

Ключовим елементом технології застосування FortiGate є побудова політик доступу відповідно до принципу мінімальних привілеїв. Усі правила формуються з чітким визначенням джерела, призначення та дозволених сервісів. Для підвищення керованості та зменшення ризику помилок використовуються об'єкти адрес, групи сервісів, зони безпеки та стандартизовані назви політик. Такий підхід дозволяє забезпечити прозорість конфігурації та спрощує подальшу підтримку системи.

Важливою складовою запропонованої технології захисту є застосування профілів безпеки до дозволеного мережевого трафіку, оскільки саме через легітимні з'єднання найчастіше реалізуються сучасні кіберзагрози. Платформа FortiGate надає

можливість інтегрувати антивірусний захист, систему запобігання вторгненням, контроль мережевих застосунків, вебфільтрацію та DNS-фільтрацію безпосередньо в політики доступу, що дозволяє виконувати глибоку інспекцію трафіку на всіх етапах його проходження через мережу.

Застосування таких профілів забезпечує виявлення шкідливого коду, спроб експлуатації вразливостей, небажаних або ризикових застосунків навіть у тих випадках, коли з'єднання є формально дозволеним з точки зору правил доступу. Особливу роль у цьому процесі відіграє інспекція зашифрованого трафіку, яка дозволяє усунути так звані сліпі зони безпеки, пов'язані з активним використанням протоколів SSL та TLS. Завдяки можливості аналізу зашифрованих з'єднань FortiGate забезпечує підвищений рівень видимості мережевих потоків і дозволяє ефективно протидіяти загрозам, що маскуються під захищений легітимний трафік, не порушуючи при цьому логіку побудови політик доступу та стабільність роботи мережі.

У межах технології застосування FortiGate важливе місце займає організація захищеного віддаленого доступу. Платформа підтримує технології IPsec та SSL VPN, що дозволяє забезпечити безпечне підключення співробітників і партнерів до корпоративних ресурсів із зовнішніх мереж. VPN-користувачі інтегруються в загальну модель сегментації та отримують доступ до ресурсів відповідно до своїх ролей і груп, що мінімізує ризики несанкціонованого доступу.

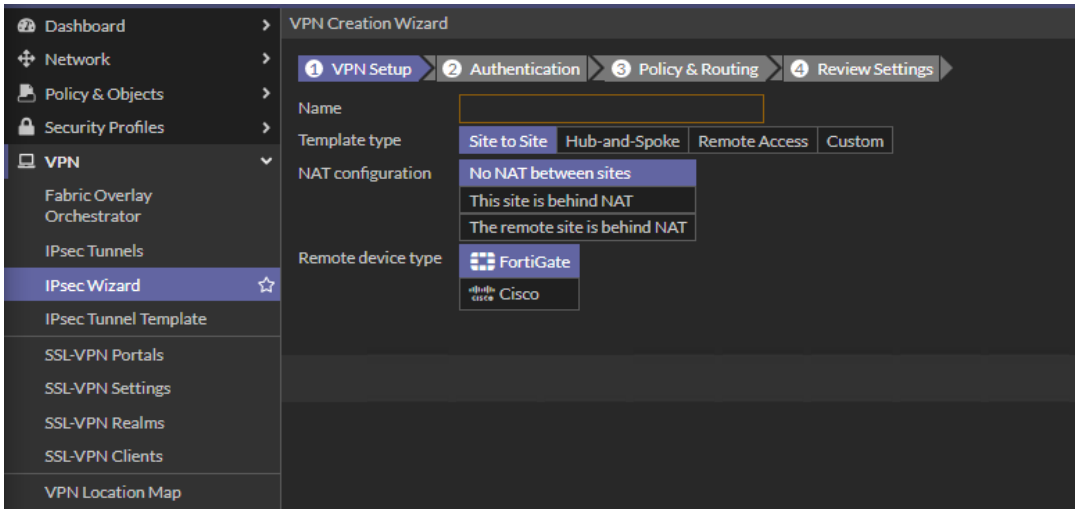

Рис 3.10 Вікно створення IPsec тунелю

Суттєвим розширенням функціональності FortiGate є інтеграція з системою централізованого аналізу та кореляції подій FortiAnalyzer. FortiAnalyzer використовується для збору, зберігання та аналізу журналів безпеки з FortiGate та інших рішень Fortinet[10]. Інтеграція FortiGate з FortiAnalyzer дозволяє зменшити навантаження на сам міжмережевий екран, підвищити рівень контролю та забезпечити відповідність вимогам аудиту й нормативних стандартів.

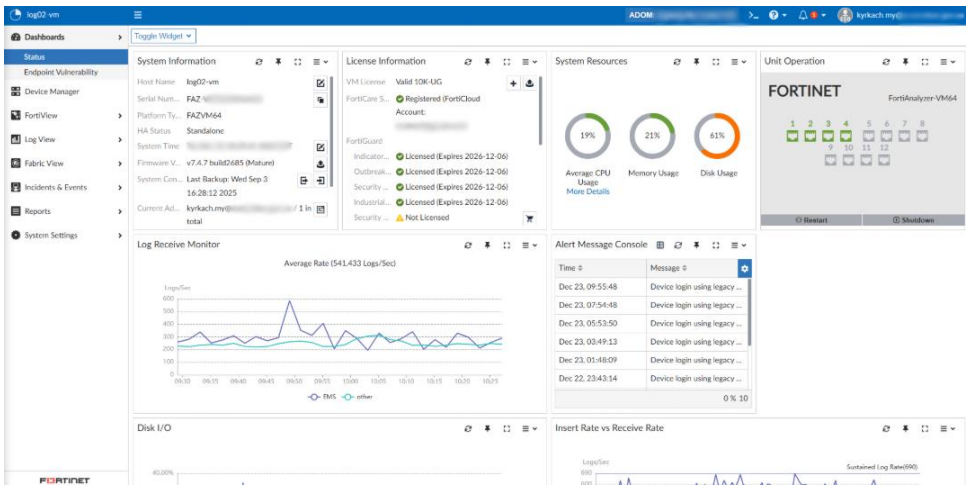

Рис 3.11 Дашборд FortiAnalyzer

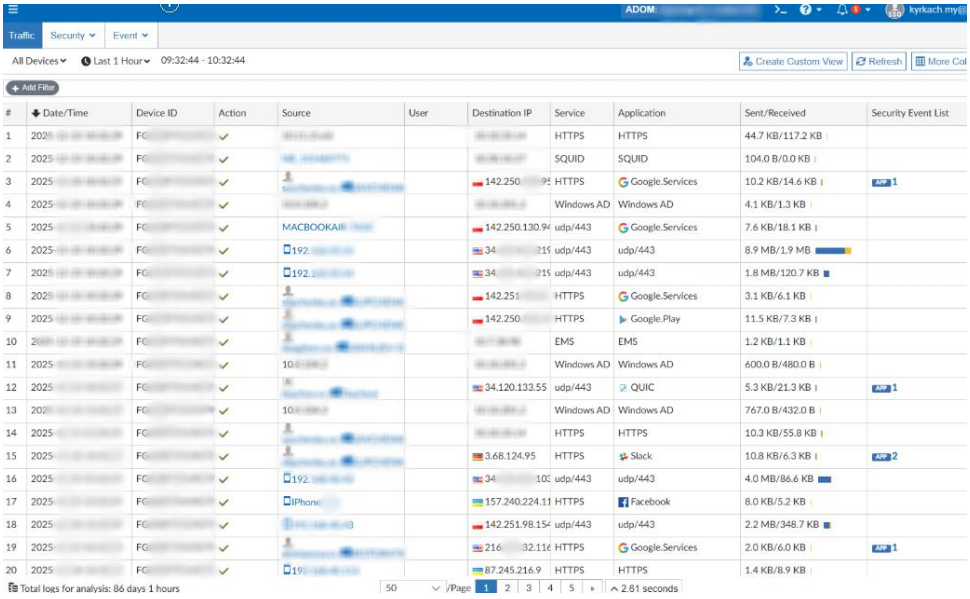

Рис 3.12 Логування трафіку з FortiGate

Окрему роль у технології застосування FortiGate відіграє інтеграція з FortiEMS, який використовується для централізованого управління захистом кінцевих пристроїв. FortiEMS забезпечує керування агентами FortiClient, контроль стану робочих станцій, перевірку відповідності політикам безпеки та застосування принципів Zero Trust Network Access[13]. У поєднанні з FortiGate це дозволяє реалізувати сценарії, коли доступ до мережі або окремих сегментів надається лише пристроям, що відповідають визначеним вимогам безпеки, наприклад наявності актуальних оновлень або активного антивірусного

Інтеграція FortiGate з FortiAnalyzer та FortiEMS формує єдину екосистему безпеки, у межах якої мережеві події, стан кінцевих пристроїв та політики доступу взаємопов’язані. Такий підхід дозволяє не лише виявляти загрози, а й автоматично обмежувати доступ скомпрометованих або невідповідних пристроїв до корпоративних ресурсів, що значно підвищує рівень загального захисту.

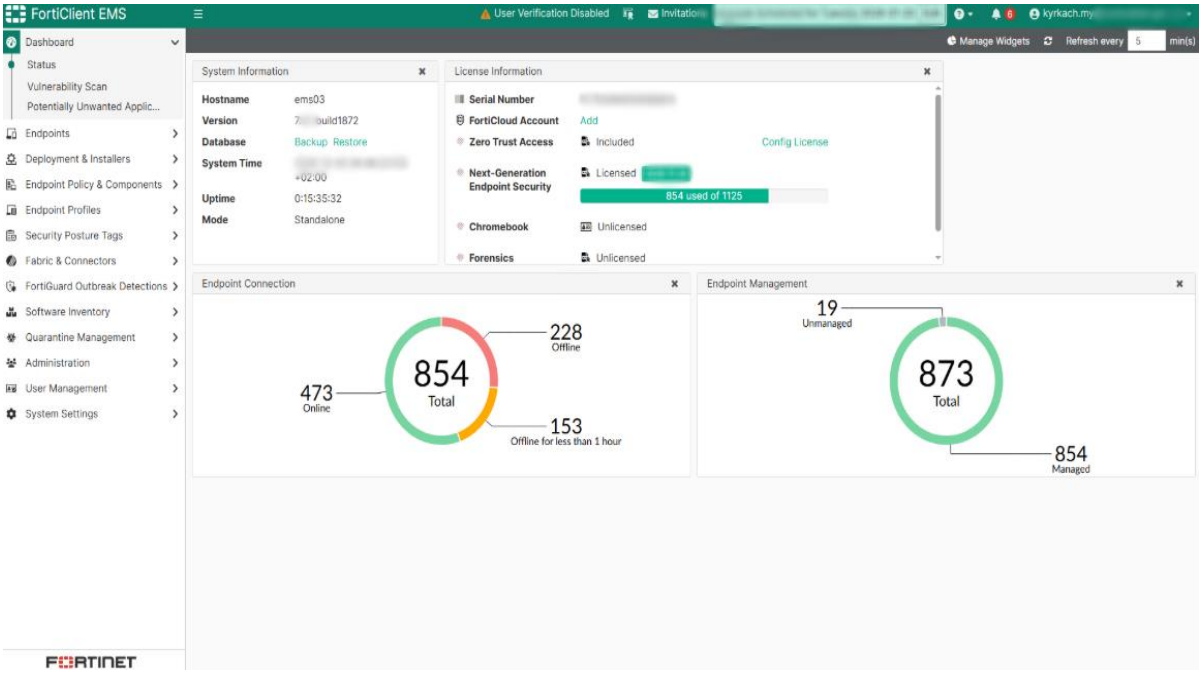

Рис 3.13 Дашборд FortiEMS

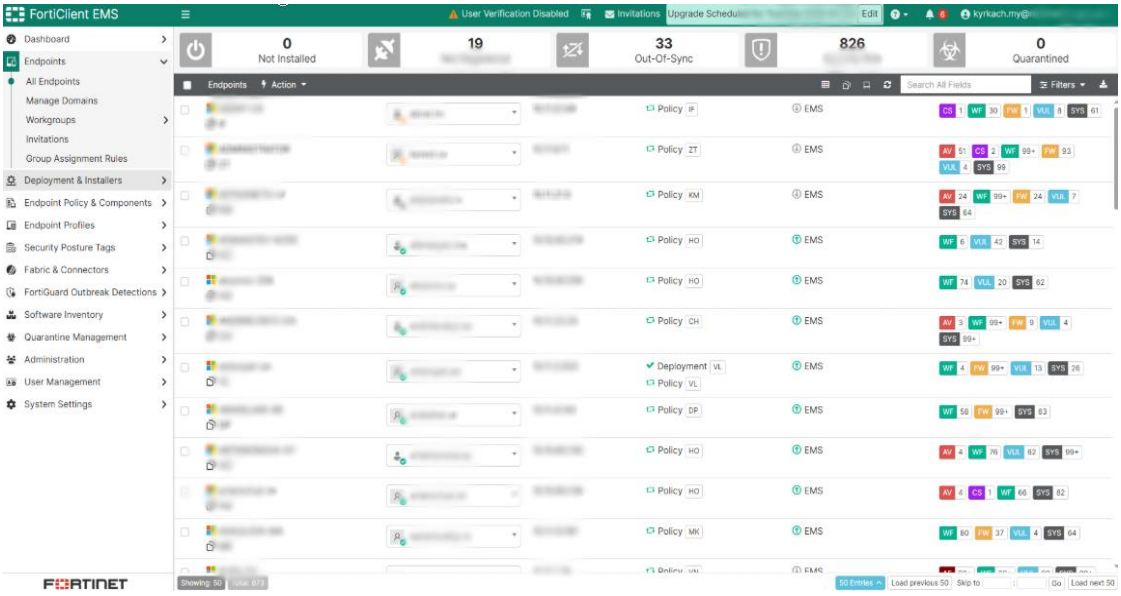

Рис 3.14 Адміністрування користувачів з FortiEMS

Для забезпечення безперервності роботи корпоративної мережі FortiGate підтримує механізми високої доступності, які дозволяють об’єднувати декілька пристроїв у кластер. У разі відмови одного з вузлів керування трафіком автоматично

переходить до резервного пристрою, що забезпечує стабільну роботу сервісів. У поєднанні з централізованим аналізом подій у FortiAnalyzer це дозволяє оперативно реагувати на інциденти навіть у складних мережевих середовищах. [10]

У процесі експлуатації важливим аспектом є постійний моніторинг, аналіз журналів та актуалізація політик безпеки. FortiGate у поєднанні з FortiAnalyzer надає повну видимість мережевої активності, а інтеграція з FortiEMS дозволяє враховувати стан кінцевих пристроїв при прийнятті рішень щодо доступу. Регулярне оновлення FortiOS та сервісів FortiGuard забезпечує відповідність системи актуальному рівню загроз.

Таким чином, технологія застосування FortiGate полягає у комплексному використанні платформи як центрального елемента мережевої безпеки з інтеграцією засобів аналізу подій та контролю кінцевих пристроїв. Поєднання FortiGate, FortiAnalyzer та FortiEMS дозволяє реалізувати багаторівневий захист, підвищити керованість корпоративної мережевої інфраструктури та забезпечити ефективне реагування на сучасні кіберзагрози.

3.3 Рекомендації щодо застосування технології захисту корпоративної мережевої інфраструктури на базі рішення FortiGate

Побудова ефективної системи захисту корпоративної мережевої інфраструктури на базі FortiGate повинна здійснюватися поетапно, з поступовим підвищенням рівня контролю доступу та складності механізмів безпеки. Такий підхід дозволяє спочатку усунути базові та найбільш критичні вектори атак, а надалі підсилювати захист шляхом ідентифікації пристроїв, користувачів і контексту доступу.

Етап 1. Формування базової архітектури та сегментації мережі

Першим і найбільш критичним етапом є побудова правильної мережевої архітектури, у якій FortiGate виконує роль центральної точки маршрутизації та міжсегментного контролю. Усі ключові сегменти корпоративної мережі — користувацькі, серверні, гостьові, DMZ, сегмент керування та віддалений доступ — повинні бути логічно відокремлені та взаємодіяти між собою виключно через FortiGate.

На цьому етапі реалізується VLAN-сегментація або поділ за фізичними інтерфейсами, визначаються IP-підмережі та формується матриця доступу між сегментами. Сегментація створює базовий рівень ізоляції та запобігає неконтрольованому поширенню загроз у разі компрометації окремих вузлів.

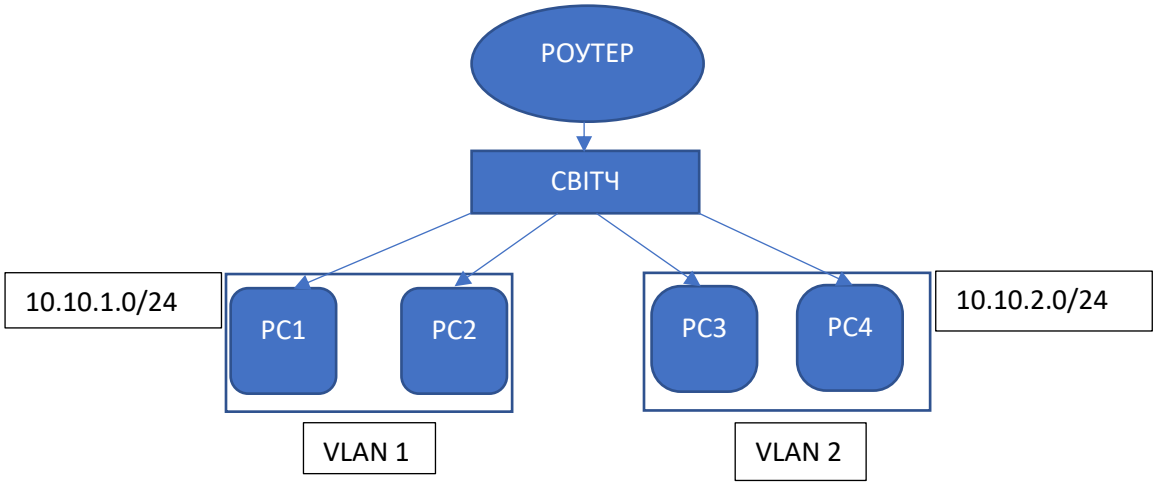

Рис.3.15 Принцип VLAN-сегментації

Таблиця 3.1 Стандартна матриця доступу між сегментами

Джерело сегмента	Призначення сегмента	Дозволений доступ	Основні сервіси	Рівень контролю
Users	Internet	дозволено	HTTP, HTTPS, DNS, NTP	AV, IPS, Web Filter, App Control
Users	Servers	обмежено	ERP, SMB, SQL (за потреби)	IPS, AV, Identity
Users	Management	заборонено	–	–
Users	Guest	заборонено	–	–
Guest	Internet	дозволено	HTTP, HTTPS, DNS	Web Filter, Rate Limit

Продовження таблиці 3.1

Guest	Internal	заборонено	–	–
Servers	Internet	обмежено	HTTP, HTTPS, NTP, Update	IPS, AV
Servers	Users	обмежено	Response traffic	IPS
Servers	Management	обмежено	SSH, RDP, HTTPS	Identity, IPS
Internet	DMZ	дозволено	HTTP, HTTPS (VIP)	IPS, WAF
DMZ	Internal	мінімально	DB, API (точково)	IPS, AV
Management	All	дозволено	SSH, HTTPS, SNMP, RDP	Identity, MFA
VPN	Internal	за ролями	За потребою	IPS, Identity
VPN	Internet	дозволено	HTTP, HTTPS	Web Filter

Етап 2. Реалізація міжсегментних політик доступу

Після формування логічних і фізичних сегментів корпоративної мережі наступним етапом є впровадження міжсегментних політик доступу, які визначають правила взаємодії між окремими зонами безпеки. Саме на цьому рівні формується контроль над потоками трафіку між сегментами, з урахуванням напрямків з’єднань, переліку дозволених сервісів і необхідного рівня доступу. Усі політики будуються відповідно до принципу мінімальних привілеїв та повинні відображати реальні процеси організації, що дозволяє забезпечити баланс між безпекою та функціональністю мережі.

На даному етапі здійснюється блокування будь-яких надлишкових, неявних або небажаних з’єднань, зокрема прямих доступів із гостьових або публічних сегментів до внутрішніх корпоративних ресурсів. Для критично важливих політик доступу активується журналювання подій, що забезпечує базову видимість мережевої активності та створює підґрунтя для подальшого аналізу інцидентів безпеки. Такий підхід дозволяє не лише зменшити ризики несанкціонованого доступу, але й спрощує аудит політик та контроль відповідності конфігурації вимогам інформаційної безпеки.

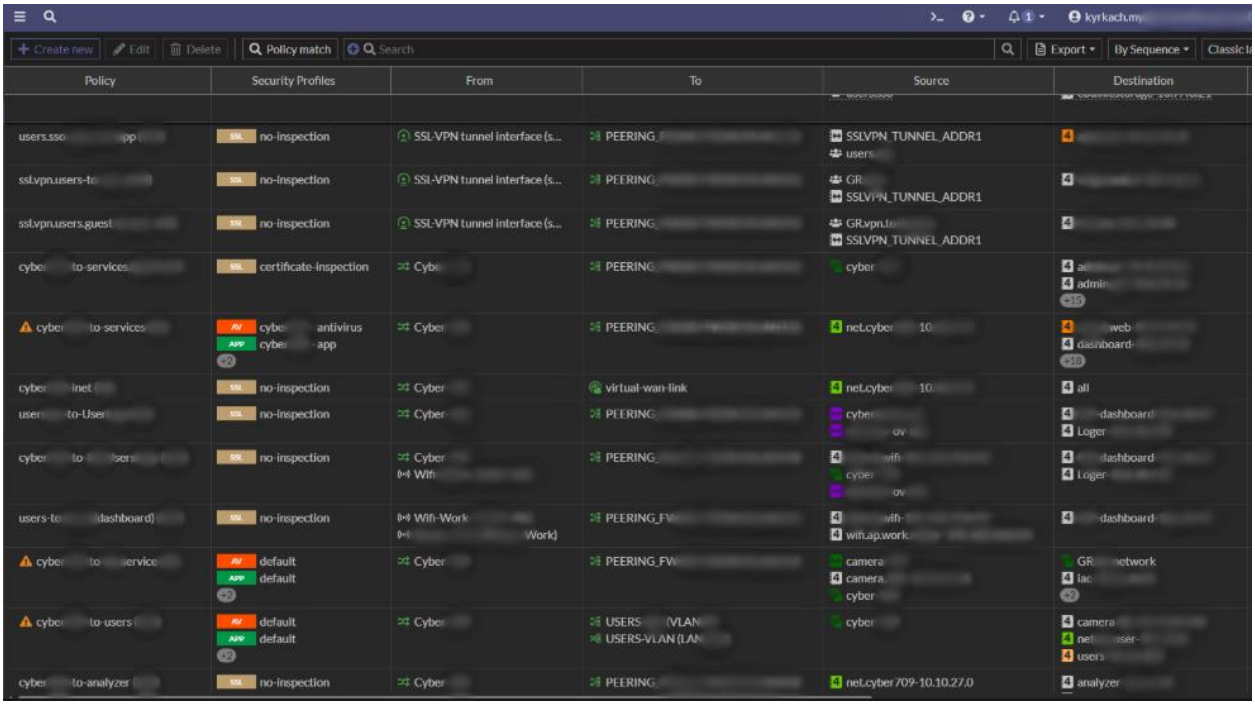

Рис 3.16 Міжсегментні Firewall policies в FortiGate. [7]

Eman 3.. Захист дозволеного трафіку за допомогою профілів безпеки

Після обмеження доступу між сегментами стає очевидно, що навіть дозволений трафік може бути носієм загроз. Тому наступним логічним етапом є застосування профілів безпеки до дозволених з'єднань.

У політиках FortiGate активуються IPS, антивірусний захист, контроль застосунків, вебфільтрація та DNS-фільтрація[7]. Особливу увагу слід приділяти трафіку між користувацьким і серверним сегментами, оскільки саме ці з'єднання найчастіше використовуються для lateral movement після компрометації робочих станцій.

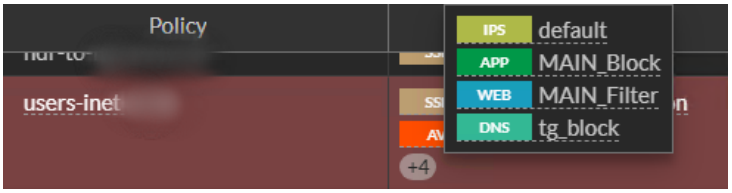

Рис 3.17 Увімкнення профілів безпеки для правила виходу в інтернет

Eman 4. Контроль доступу пристроїв на основі MAC-адрес

Після впровадження аналізу трафіку наступним рівнем захисту стає контроль підключення пристроїв до мережі. На цьому етапі доцільно використовувати механізми фільтрації доступу на основі MAC-адрес.

FortiGate дозволяє ідентифікувати пристрої та застосовувати до них окремі політики доступу, що є особливо актуальним для обладнання, яке не підтримує автентифікацію користувачів. Це дозволяє обмежити доступ таких пристроїв до окремих сегментів та зменшити ризик несанкціонованого підключення[11].

Водночас MAC-адреса не є криптографічно захищеним ідентифікатором, що зумовлює необхідність подальшого підсилення цього механізму.

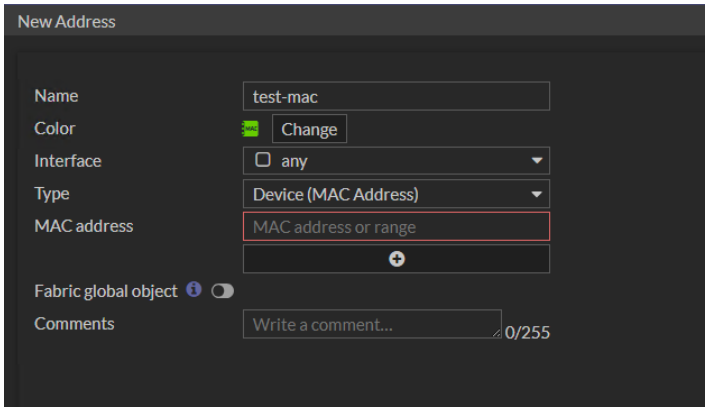

Рис 3.17 Створення адресного об’єкту за MAC-адресою

Eman 5. Підсилення контролю пристроїв за рахунок технології єдиного входу(опціонально)

Логічним продовженням контролю доступу на основі MAC-адрес є впровадження ідентифікації користувачів. На цьому етапі FortiGate інтегрується з провайдером технології єдиного входу, який забезпечує централізовану автентифікацію та управління обліковими записами.

Поєднання контролю пристрою та ідентифікації користувача дозволяє реалізувати контекстний доступ до ресурсів, коли рішення про надання доступу приймається з урахуванням як типу пристрою, так і ролі користувача. Такий підхід

значно підвищує ефективність мережевого контролю доступу та знижує ризик зловживань у разі компрометації одного з факторів.

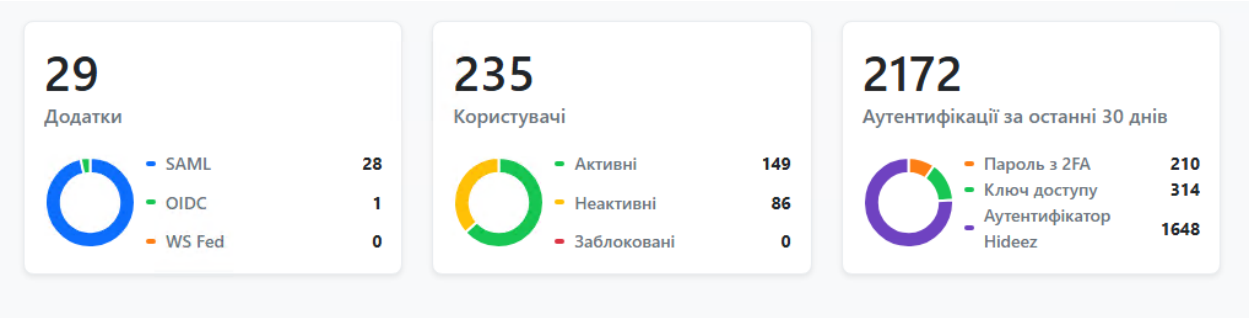

Рис 3.18 Показники успішної інтеграції єдиного входу

Приклад додавання SSO провайдера можна побачити нижче. Це CLI-код для консолі FortiGate[14].

```
config user ldap
    edit "SSO_Provider"
        set server "192.168.1.10"
        set cnid "sAMAccountName"
        set dn "dc=corp,dc=local"
        set type regular
        set username "CN=ldapbind,OU=ServiceAccounts,DC=corp,DC=local"
        set password ENC <encrypted_password>
        set secure ldaps
        set port 636
    next
end
```

Етап 6. Централізований моніторинг і кореляція подій безпеки

Після впровадження багаторівневого контролю доступу та застосування різних механізмів захисту виникає об’єктивна потреба у централізованому зборі й аналізі подій безпеки. На цьому етапі доцільно інтегрувати FortiGate з системою

централізованого моніторингу та аналізу логів, що дозволяє об’єднати інформацію про мережеві з’єднання, дії користувачів і спрацювання профілів безпеки в єдиному аналітичному просторі. Така інтеграція значно спрощує контроль за станом безпеки корпоративної мережі та підвищує керованість інфраструктури.

Централізований моніторинг забезпечує можливість кореляції подій доступу, результатів роботи системи запобігання вторгненням, антивірусного захисту та інших механізмів безпеки з ознаками аномальної активності. Це дозволяє оперативно виявляти підозрілі дії, відстежувати ланцюги інцидентів та скорочувати час реагування на загрози. Крім того, накопичення та аналіз журналів подій створюють основу для проведення аудиту, оцінки ефективності політик безпеки та вдосконалення технології захисту корпоративної мережевої інфраструктури в цілому.

До прикладу, візьмемо FortiAnalyzer. Прив’язка FortiGate до FortiAnalyzer забезпечує централізований збір і довготривале зберігання журналів подій, розширені можливості кореляції та формування аналітичних звітів. Це дозволяє не лише оперативно реагувати на інциденти, а й здійснювати комплексний аналіз стану безпеки мережі, оцінювати ефективність налаштованих політик і виявляти тенденції розвитку загроз. Використання рішень одного виробника створює цілісну екосистему безпеки, у межах якої всі компоненти доповнюють один одного та підвищують загальний рівень захищеності корпоративної мережевої інфраструктури.

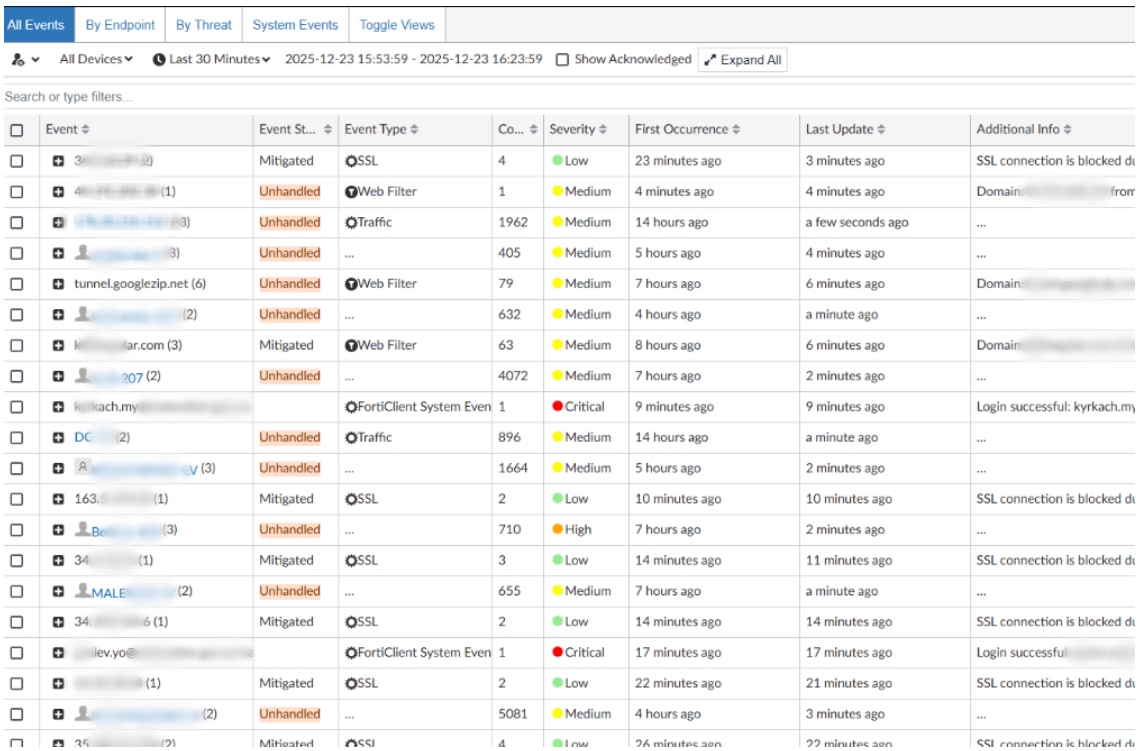

Рис 3.19 Моніторинг трафіку за допомогою FortiAnalyzer

Етап 7. Забезпечення безперервності роботи та відмовостійкості

Оскільки FortiGate виступає центральним елементом контролю доступу та безпеки, його стабільна робота є критичною для всієї інфраструктури. На цьому етапі доцільно впроваджувати механізми високої доступності шляхом об’єднання пристроїв у кластер.

Це дозволяє зберегти працездатність мережі у разі апаратних або програмних збоїв.

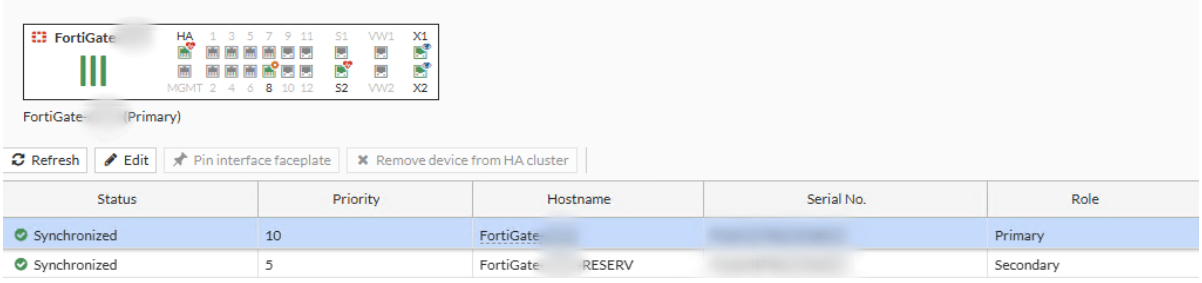

Рис 3.20 Приклад успішного налаштування відмовостійкості через HA

Етап 8. Експлуатація, аудит та розвиток системи безпеки

Завершальним етапом реалізації технології захисту є постійна експлуатація та розвиток системи безпеки корпоративної мережевої інфраструктури. На цьому етапі особлива увага приділяється регулярному оновленню програмного забезпечення FortiOS і баз сигнатур, що дозволяє підтримувати актуальний рівень захищеності та своєчасно реагувати на появу нових типів загроз і вразливостей.

Важливим складником експлуатації є систематичний аудит політик доступу та їх відповідність поточним процесам організації. Аналіз журналів подій і звітів безпеки дає змогу виявляти аномальну активність, оцінювати ефективність налаштованих механізмів захисту та вносити коригування до конфігурації системи. Окрему роль відіграє регулярне резервне копіювання конфігурації FortiGate, яке забезпечує можливість швидкого відновлення працездатності мережевої інфраструктури у разі збоїв, помилкових змін або аварійних ситуацій. Крім того, актуалізація інтеграцій із зовнішніми сервісами ідентифікації та іншими компонентами екосистеми безпеки створює основу для подальшого розвитку та масштабування системи захисту без порушення стабільності корпоративної мережі.

Додатково в процесі експлуатації системи захисту доцільно приділяти увагу документуванню змін конфігурації та регламентуванню адміністративних процедур. Ведення журналу змін, опис налаштованих політик і сценаріїв доступу спрощують супровід системи, підвищують прозорість адміністрування та зменшують залежність від окремих спеціалістів. Регулярне тестування резервних копій конфігурації та перевірка сценаріїв відновлення дозволяють переконатися в готовності системи до аварійних ситуацій і забезпечують безперервність роботи корпоративної мережевої інфраструктури навіть у разі серйозних інцидентів безпеки.

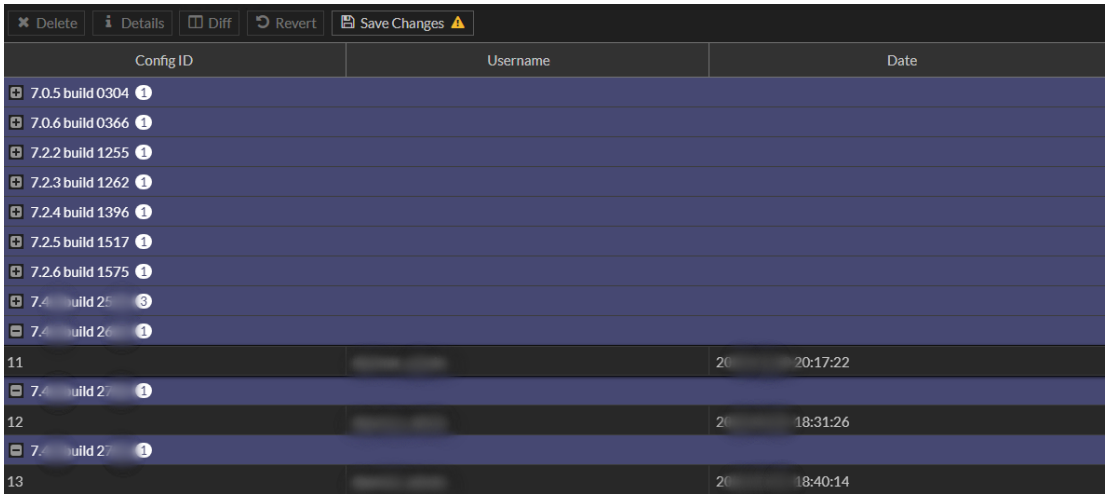

Рис 3.21 Наявні резервні копії конфігу для відновлення в критичних випадках[11]

Поетапне впровадження технологій захисту на базі FortiGate дозволяє послідовно й логічно перейти від базової сегментації мережі до комплексної моделі контролю доступу, у межах якої поєднуються мережеві, пристроєві та користувацькі механізми безпеки. Такий підхід дає змогу на кожному етапі зосереджуватися на усуненні найбільш критичних ризиків, поступово розширюючи функціональні можливості системи захисту без необхідності кардинальних змін у мережевій архітектурі.

Застосування цієї моделі впровадження сприяє збереженню стабільності та безперервності процесів, оскільки кожен новий механізм безпеки вводиться з урахуванням уже налаштованих політик і реальних потреб організації. У результаті формується гнучка та масштабована система захисту корпоративної мережевої інфраструктури, здатна адаптуватися до змін у мережевому середовищі та ефективно протидіяти сучасним кіберзагрозам.

Висновки до розділу

У даному розділі розглянуто основні практичні підходи до побудови технології захисту корпоративної мережевої інфраструктури на базі рішення FortiGate. Показано, що ефективний захист мережі потребує комплексного підходу, який поєднує сегментацію мережі, міжсегментний контроль доступу та багаторівневий аналіз мережевого трафіку.

Установлено, що логічна сегментація корпоративної мережі та застосування детальних політик доступу дозволяють суттєво зменшити поверхню атаки та обмежити поширення загроз у разі компрометації окремих сегментів. Застосування профілів безпеки до дозволеного трафіку забезпечує додатковий рівень захисту та підвищує ефективність виявлення мережевих атак.

Обґрунтовано доцільність поєднання контролю доступу пристроїв із ідентифікацією користувачів на основі технології єдиного входу, що дозволяє враховувати контекст доступу та підвищувати рівень безпеки. Таким чином, використання платформи FortiGate дає змогу реалізувати керовану та масштабовану модель захисту корпоративної мережевої інфраструктури, стійку до сучасних кіберзагроз.

ВИСНОВКИ

У межах даної кваліфікаційної роботи здійснено всебічне дослідження проблематики захисту корпоративної мережевої інфраструктури в умовах стрімкого розвитку інформаційних технологій та зростання кількості й складності кіберзагроз. Установлено, що сучасні корпоративні мережі характеризуються складною архітектурою, наявністю великої кількості сегментів, використанням віддаленого доступу та зашифрованих протоколів, що суттєво ускладнює забезпечення належного рівня інформаційної безпеки традиційними методами.

У роботі проведено аналіз сучасних загроз корпоративним мережам і показано обмеженість класичних периметрових підходів до захисту. Обґрунтовано необхідність переходу до багаторівневих моделей безпеки, які передбачають сегментацію мережі, жорсткий контроль міжсегментного трафіку та постійний аналіз дозволених з’єднань. Особливу увагу приділено ролі міжмережевих екранів нового покоління у забезпеченні комплексного захисту мережевої інфраструктури.

Значну частину роботи присвячено дослідженню архітектури та функціональних можливостей платформи FortiGate. Показано, що використання єдиної операційної системи FortiOS та апаратного прискорення дозволяє поєднати високу продуктивність із широким набором механізмів безпеки. Застосування FortiGate як центрального елемента мережевої інфраструктури забезпечує централізоване управління політиками доступу, сегментацію мережі та ефективний контроль мережевих з’єднань.

На основі проведених досліджень розроблено варіант технології захисту корпоративної мережевої інфраструктури на базі рішення FortiGate, який передбачає поетапне впровадження механізмів безпеки з урахуванням їх критичності. Запропонована технологія поєднує сегментацію мережі, детальні політики міжсегментного доступу, застосування профілів безпеки до дозволеного трафіку, а

також контроль доступу користувачів і пристроїв. Такий підхід дозволяє зменшити поверхню атаки, обмежити поширення загроз та підвищити стійкість мережі до інцидентів безпеки.

Отримані результати свідчать про доцільність та практичну ефективність застосування платформи FortiGate для побудови комплексної системи захисту корпоративної мережевої інфраструктури. Запропоновані у роботі підходи та рекомендації можуть бути використані під час проєктування, впровадження та експлуатації систем мережевої безпеки в організаціях різного масштабу та сприятимуть підвищенню рівня захищеності інформаційних ресурсів і стабільності процесів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Fortinet. Types of cyber attacks. – URL: https://www.fortinet.com/uk/resources/cyberglossary/types-of-cyber-attacks (дата звернення: 13.11.2025).

2. Smart IT. Zero Trust та багаторівнева модель безпеки для сучасного бізнесу . – URL: https://cloud.smart-it.com/news-post/zero-trust-bagatorivneva-model-bezpeky-dlya-suchasnogo-biznesu/ (дата звернення: 13.11.2025).

3. Fortinet. Fortinet Documentation . – URL: https://docs.fortinet.com/ (дата звернення:13.11.2025).

4. DigiCert. 2023 DDoS statistics and trends. – URL: https://vercara.digicert.com/resources/2023-ddos-statistics-and-trends (дата звернення: 13.11.2025).

5. H-X Technology. Прогноз кіберзагроз на 2024 рік . – URL: https://www.h-x.technology/ua/blog-ua/cyber-threats-forecast-2024-ua (дата звернення: 13.11.2025).

6. Wiz. Defense in Depth. – URL: https://www.wiz.io/academy/cloud-security/defense-in-depth (дата звернення: 19.11.2025).

7. Fortinet. FortiGate Administration Guide. Policy and objects. Version 7.6.5 . – URL: https://docs.fortinet.com/document/fortigate/7.6.5/administration-guide/728881/policy-and-objects (дата звернення: 19.11.2025).

8. Fortinet. FortiSwitch devices managed by FortiOS. Configuring FortiSwitch VLANs and ports. Version 7.0.8 . – URL: https://docs.fortinet.com/document/fortiswitch/7.0.8/devices-managed-by-fortios/173294/configuring-fortiswitch-vlans-and-ports (дата звернення: 19.11.2025).

9. Fortinet. FortiSwitch devices managed by FortiOS. Configuring VLANs. Version 7.0.8 . – URL: https://docs.fortinet.com/document/fortiswitch/7.0.8/devices-managed-by-fortios/546342/configuring-vlans (дата звернення: 7.12.2025).

10. Fortinet. FortiAnalyzer Administration Guide. Logs. Version 7.6.5 . – URL: https://docs.fortinet.com/document/fortianalyzer/7.6.5/administration-guide/381919/logs (дата звернення:7.12.2025).

11. Fortinet. FortiAnalyzer Administration Guide. Device Manager. Version 7.6.5 . – URL: https://docs.fortinet.com/document/fortianalyzer/7.6.5/administration-guide/781928/device-manager (дата звернення: 7.12.2025).

12. Fortinet. FortiSIEM External Systems Configuration Guide. FortiClient EMS. Version 7.4.2 . – URL: https://docs.fortinet.com/document/fortisiem/7.4.2/external-systems-configuration-guide/153523/fortinet-forticlient-ems (дата звернення: 23.12.2025).

13. Fortinet. FortiGate Ports and Protocols. FortiClient EMS Endpoint Management Server. Version 6.4.0 . – URL: https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/35450/forticlient-ems-endpoint-management-server (дата звернення: 23.12.2025).

14. Fortinet. FortiGate Ports and Protocols. Fortinet Single Sign-On (FSSO). Version 6.4.0 . – URL: https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/879117/fsso-fortinet-single-sign-on (дата звернення: 23.12.2025).

ДЕМОНСТРАЦІЙНИЙ МАТЕРІАЛ (Презентація)