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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту мережевого периметру з використанням міжмережевих екранів нового покоління»

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
_____ Георгій КОМПАНЕЦЬ
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-63
КОМПАНЕЦЬ Георгій
(прізвище, ім'я)

Керівник канд. техн. наук, доцент
БОРСУКОВСЬКИЙ Юрій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

NGFW	–	Next Generation Firewall
UEBA	–	User and Entity Behavior Analytics
IDS	–	Intrusion Detection System
DLP	–	Data Loss Prevention
DMZ	–	Demilitarized Zone
VPN	–	Virtual Private Network
SIEM	–	Security Information and Event Management
MTTD	–	Mean Time to Detect
MTTR	–	Mean Time to React
SSL/TLS	-	Secure Sockets Layer/Transport Layer Security
ACL	-	Access Control List
CASB	-	Cloud Access Security Broker
ZTNA	-	Zero Trust Network Access
RBA	-	Risk-Based Alerting
SOC	-	Security Operations Center
SOAR	-	Security Orchestration, Automation and Response

ВСТУП

Актуальність дослідження. У сучасних умовах цифрової трансформації та стрімкого розвитку інформаційних технологій корпоративні мережі стають основою функціонування бізнес-процесів, державних установ та критичної інфраструктури. Водночас саме мережевий периметр виступає першою лінією оборони від зовнішніх атак і є найбільш вразливим елементом системи кіберзахисту. Традиційні міжмережеві екрани, що базуються на статичних правилах фільтрації пакетів, вже не відповідають сучасним викликам, адже не здатні ефективно протидіяти багатоступеневим атакам, використанню зашифрованого трафіку, легітимних сервісів для обходу захисту та складним методам проникнення. Це створює реальну загрозу компрометації корпоративних ресурсів, витоку конфіденційної інформації та порушення безперервності бізнес-процесів.

Серед основних ризиків для мережевого периметру можна виділити атаки типу DoS/DDoS, експлуатацію вразливостей у мережевому обладнанні, використання шкідливих скриптів і тунелювання трафіку через HTTPS, а також несанкціонований доступ до внутрішніх ресурсів. Додатково значну роль відіграє людський фактор: помилки адміністраторів у налаштуванні політик доступу, використання слабких паролів або відсутність належного контролю за підключенням зовнішніх пристроїв. Усе це формує багаторівневу картину загроз, які потребують комплексного підходу до захисту.

Для вирішення цих проблем активно впроваджуються міжмережеві екрани нового покоління (Next Generation Firewall, NGFW). Їхня ключова особливість полягає у поєднанні класичних функцій фільтрації з розширеними можливостями: глибокою інспекцією пакетів (DPI), аналізом трафіку на рівні додатків, підтримкою SSL/TLS-інспекції, інтеграцією з системами виявлення та запобігання вторгнень (IDS/IPS), а також централізованим моніторингом через SIEM і автоматизованим

реагуванням за допомогою SOAR. Використання NGFW дозволяє організаціям створити багаторівневу архітектуру захисту, яка враховує специфіку бізнес-процесів і забезпечує баланс між продуктивністю та безпекою.

Все це підтверджує актуальність обраної теми даної кваліфікаційної роботи, головним змістом якої є дослідження технології захисту мережевого периметру з використанням міжмережевих екранів нового покоління.

Об'єкт дослідження – процес забезпечення кіберзахисту мережевого периметру корпоративної IT-інфраструктури.

Предмет дослідження - технологія побудови багаторівневої системи захисту мережевого периметру на базі NGFW.

Мета роботи – розробити порядок впровадження міжмережевих екранів нового покоління для захисту мережевого периметру організації, дослідити їх функціональні можливості та сформулювати рекомендації щодо практичного застосування в корпоративних середовищах.

Наукові завдання :

дослідити сутність проблеми захисту мережевого периметру та визначити його роль у системі кіберзахисту;

проаналізувати основні загрози та атаки на мережевий периметр;

розглянути існуючі засоби захисту та визначити їхні обмеження;

дослідити архітектуру та функціональні можливості NGFW;

розкрити порядок впровадження NGFW у корпоративну мережу;

Методи дослідження – аналіз науково-технічної літератури та публікацій у сфері кібербезпеки, вивчення експлуатаційної документації NGFW, практичне тестування політик доступу та фільтрації трафіку, порівняння з міжнародними стандартами інформаційної безпеки, узагальнення кращих практик побудови багаторівневого захисту.

Практичне значення одержаних результатів: у роботі запропоновано порядок застосування NGFW для захисту мережевого периметру, розроблено прототип

рішення з налаштування політик доступу та фільтрації трафіку, а також сформульовано практичні рекомендації для фахівців із кібербезпеки щодо інтеграції NGFW у корпоративну IT-інфраструктуру з акцентом на масштабованість, продуктивність та зручність адміністрування.

Результати кваліфікаційної роботи апробовані на VII Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 29 жовтня 2025 року у м. Києві.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ МЕРЕЖЕВОГО ПЕРИМЕТРУ В СУЧАСНИХ ІТ-СИСТЕМАХ

1.1. Визначення поняття мережевого периметру та його роль у кіберзахисті

Мережевий периметр традиційно розглядається як умовна межа між внутрішнім (довіреним) сегментом корпоративної мережі та зовнішнім, потенційно ворожим середовищем (передусім Інтернетом). У класичній моделі побудови корпоративних мереж саме периметр був головною лінією оборони: усі користувачі й сервіси всередині мережі вважалися такими, що заслуговують довіри, тоді як трафік «ззовні» підлягав жорсткій фільтрації міжмережевими екранами, системами виявлення вторгнень та іншими засобами perimeter-based security. У такій парадигмі безпека досягається через чітке розмежування «inside» і «outside» та побудову потужного периметрового бар’єру, який пропускає лише дозволені з’єднання згідно з налаштованими правилами фільтрації трафіку [1].

З технічної точки зору мережевий периметр можна визначити як сукупність точок входу та виходу мережевого трафіку між внутрішньою інфраструктурою організації та зовнішніми мережами, де здійснюється контроль, фільтрація, моніторинг і реєстрація мережевих взаємодій. Це не лише сам міжмережевий екран (або їхній кластер), а й DMZ-сегменти, граничні маршрутизатори, VPN-шлюзи, веб- та поштові проксі, системи захисту від DDoS-атак, тобто весь комплекс вузлів, через які зовнішній трафік може потрапити до внутрішніх ресурсів. У класичних рекомендаціях NIST мережевий периметр прямо прив’язується до розташування міжмережевих екранів та політик фільтрації, які реалізують основні правила доступу між мережевими зонами [2].

Історично поняття периметру формувалося в умовах, коли корпоративні ресурси розміщувалися переважно в одному або декількох дата-центрах, користувачі

працювали з локальних робочих станцій в офісі, а єдиним «вікном» у зовнішній світ був канал доступу до Інтернету. У такій архітектурі більшість критичних сервісів узагалі не були доступні ззовні, а весь вхідний трафік централізовано проходив через один або кілька периметрових вузлів. Це дозволяло будувати модель «тверда шкаралупа — м'який внутрішній вміст»: достатньо захистити зовнішню межу, і все, що всередині, вважається відносно безпечним. Багато виробників мережевого обладнання саме в такій логіці впродовж років розвивали класичні міжмережеві екрани, орієнтовані насамперед на фільтрацію трафіку за IP-адресами, портами та протоколами [3].

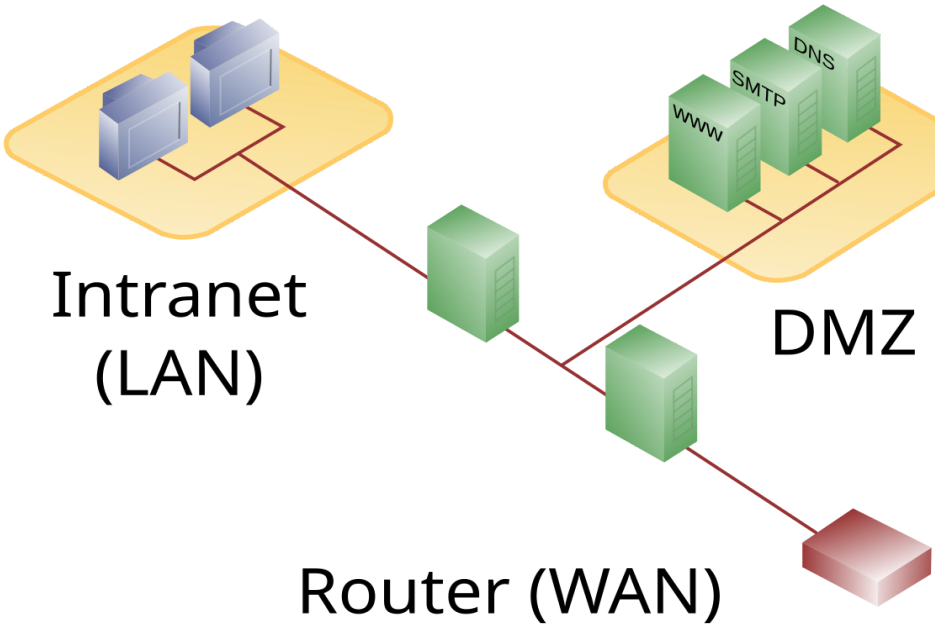


Рис.1.1 - Класична схема мережевого периметру організації

Однак із розвитком віртуалізації, хмарних сервісів, SaaS-платформ, підключенням мобільних пристроїв і переходом до віддаленої або гібридної роботи поняття «чіткого периметру» почало розмиватися. Дані, сервіси й користувачі перестали бути «за високою стіною» одного дата-центру: частина застосунків переїхала в публічні хмари, частина — у приватні, користувачі працюють з дому, з коворкінгів, з мобільних мереж. У цих умовах з'явився термін «de-perimeterization» — поступове зникнення класичної мережевої межі та поява множини логічних периметрів навколо конкретних сервісів, даних та ідентичностей [4].

Попри це, мережевий периметр не втрачає актуальності, а радше еволюціонує. Навіть у сучасних Zero Trust-архітектурах, де ключовим об’єктом довіри є не мережа, а ідентичність користувача та стан пристрою, зовнішні точки виходу в Інтернет, граничні сегменти між внутрішніми й зовнішніми зонами та інтеграційні шлюзи з хмарними провайдерами залишаються критичними зонами контролю. Саме на рівні периметру доцільно реалізовувати низку базових функцій кіберзахисту: фільтрацію шкідливого трафіку, блокування відомих експлойтів, контроль доступу до веб-ресурсів, запобігання витоку даних (DLP), аналіз SSL-шифрованого трафіку, виявлення командно-контрольного (C2) трафіку шкідливих програм. Сучасні NGFW інтегрують у собі всі ці функції, роблячи периметр не лише «фільтром портів», а повноцінною платформою прикладного рівня [3].

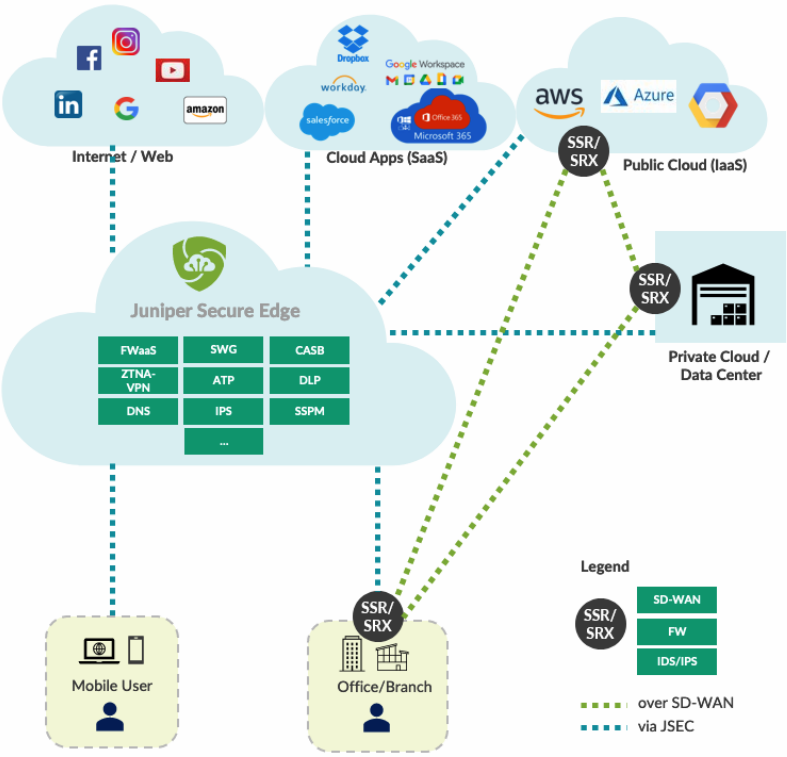


Рис 1.2 - Еволюція периметру: від «однієї стіни» до множинних логічних периметрів

Роль мережевого периметру в кіберзахисті можна розкрити через кілька взаємопов’язаних аспектів. По-перше, це концентрація точок контролю. Замість того

щоб розміщувати складні системи безпеки на кожному хості, організація може сконцентрувати основні механізми фільтрації та моніторингу в периметрових вузлах, через які проходить значна частина трафіку. Такий підхід істотно спрощує управління політиками доступу, оновлення сигнатур шкідливого ПЗ, налаштування IDS/IPS-правил, а також дозволяє централізовано збирати журнали для подальшого аналізу в SIEM-системах. По-друге, периметр виступає бар'єром між довіреними й недовіреними зонами: навіть якщо внутрішня мережа частково скомпрометована, правильно сегментований периметр може локалізувати інцидент, не допустивши поширення атаки назовні або в інші критичні сегменти.

По-третє, периметр є ключовим місцем реалізації політики «least privilege» на мережевому рівні: міжмережевий екран може дозволяти лише явно необхідні сервіси, протоколи й напрямки трафіку, блокуючи все інше за замовчуванням (policy deny by default). У контексті сучасних рекомендацій NIST це відповідає принципам мінімізації поверхні атак та управління ризиками доступу до ресурсів [2]. Через периметр зручно впроваджувати й додаткові контролі — наприклад, обмеження доступу до адміністративних інтерфейсів, заборону небезпечних або застарілих протоколів, примусове використання шифрування (TLS) для веб- і поштових сервісів.

Разом із тим, у сучасних IT-системах мережевий периметр дедалі рідше існує у вигляді однієї фізичної межі. Його доцільно розглядати як набір логічних периметрів навколо різних сегментів: внутрішній периметр між користувацькими VLAN та серверами, периметр між дата-центром і хмарною інфраструктурою, периметр між OT-мережею (технологічні процеси, ICS/SCADA) та IT-мережею, а також мікропериметри навколо окремих критичних систем. У цьому контексті NGFW стають не лише граничними пристроями, а й елементами внутрішньої сегментації, здатними здійснювати контроль трафіку всередині організації на прикладному рівні. Такий підхід узгоджується з концепцією Zero Trust, де кожен сегмент розглядається

як потенційно недовірений, а доступ до нього повинен бути чітко контрольованим і протоколюватися [5].

Важливо, що мережевий периметр сьогодні охоплює не лише IP-рівень, а й рівень ідентичностей та контенту. Якщо в класичному міжмережевому екрані рішення про пропуск або блокування трафіку ухвалювалося на основі комбінації IP-адреса/порт/протокол, то в NGFW до цього додаються контекстні ознаки: хто саме ініціює з'єднання (користувач/група каталогу), з якого пристрою, до якого застосунку, який тип даних передається. Це дозволяє інтегрувати периметрову політику з системами IAM/IdP, каталогами користувачів (Active Directory, Azure AD), сервісами класифікації даних і DLP. У результаті рішення «дозволити/заборонити» ґрунтується вже не лише на мережевих атрибутах, а й на ролі, контексті й чутливості інформації, що суттєво підвищує ефективність контролю [3], [5].

Рис 1.3 - Роль NGFW у сучасному периметрі

Ще один важливий аспект ролі периметру — аналітика та спостережність (observability). Через периметрові вузли проходить значний обсяг трафіку, що робить їх ідеальною точкою для збирання телеметрії: NetFlow/IPFIX, HTTP-логи, DNS-запити, TLS-метадані, сповіщення IPS, журнали блокувань. Ця інформація далі

надходить до SIEM/XDR-платформ, де використовується для побудови моделей поведінки, кореляції подій, виявлення аномалій і полювання на загрози (threat hunting). У практичному вимірі це означає, що якість мережевого периметру безпосередньо впливає на можливості Security Operation Center щодо виявлення та розслідування інцидентів. Без належної видимості на периметрі SOC опиняється «сліпим» до багатьох атак, що йдуть через веб-, DNS- чи SSH-канали.

У контексті даної кваліфікаційної роботи мережевий периметр розглядається як базовий рівень побудови технології захисту, а міжмережеві екрани нового покоління — як ключовий інструмент реалізації політик контролю доступу, фільтрації трафіку та забезпечення спостережності. Подальші розділи будуть присвячені аналізу того, як обмеження класичних периметрових рішень (орієнтація лише на L3/L4, відсутність контексту користувача й застосунку, складність інтеграції зі SIEM і системами аутентифікації) долаються за рахунок функціоналу NGFW та їх вбудованої інтеграції з сучасними платформами моніторингу.

1.2. Аналіз основних загроз та атак на мережевий периметр

Мережевий периметр історично був основним рубежем оборони корпоративних інформаційних систем, однак трансформація IT-інфраструктур, поява хмарних сервісів, широке застосування мобільних пристроїв і загальна зміна характеру кіберзагроз призвели до фундаментального перегляду підходів до його захисту. Попри це, саме периметр продовжує залишатися першою лінією контакту з потенційним зловмисником, і більшість атак починається саме на його рівні. З огляду на актуальність теми важливо не лише класифікувати загрози, а й глибоко проаналізувати механізми їх реалізації, способи обходу класичних засобів захисту та технологічні особливості NGFW, які дозволяють їм ефективно нейтралізувати сучасні атаки.

Одним з найпоширеніших класів загроз є розвідувальні та сканувальні операції, що виконуються до активної фази атаки. Мета таких дій — побудувати точну карту периметру: визначити відкриті порти, версії сервісів, наявність застарілих протоколів, ідентифікувати "дірки" у фаєрвол-правилах. Сучасні інструменти сканування здатні генерувати мільйони запитів за секунду, маскуватися під легітимний трафік, використовувати випадкові IP-адреси та уникати обмежень швидкості. Особливо небезпечним є той факт, що зловмисники дедалі частіше застосовують розподілені сканування, коли кожен вузол ботнету здійснює мінімальну кількість запитів, що робить їх майже невидимими для традиційних механізмів IDS [6].

Другим критично важливим класом загроз є експлуатація вразливостей периметрових систем. Саме edge-пристрої (VPN-шлюзи, веб-аплікаційні фаєрволи, проксі-сервери, SSL-VPN системи) стали однією з найпопулярніших цілей атак у 2023–2025 роках. Причини цього очевидні:

–периметрові системи зазвичай доступні з Інтернету;

–мають розширені привілеї у мережі;

–часто містять конфіденційні дані (ключі, сертифікати, конфігурації);

– оновлюються з великим запізненням.

Звіти Mandiant, CISA та ENISA фіксують десятки критичних CVE, що дозволяли обходити автентифікацію та отримувати віддалений доступ до таких систем, як Citrix ADC, FortiGate, Ivanti Secure, Palo Alto GlobalProtect. Після компрометації edge-пристрою периметр фактично руйнується, оскільки зловмисник отримує можливість побудувати персистентність, виконувати lateral movement та збирати дані по всій внутрішній мережі [7].

Однією з найбільш руйнівних загроз залишаються DDoS-атаки, які стрімко еволюціонують. Якщо раніше вони ґрунтувалися на перенавантаженні каналу, то сучасні атаки спрямовані на прикладний рівень — HTTP flood, API exhaustion, TLS handshake exhaustion, RST flood, SlowLoris. Особливо небезпечним є використання

шифрованих DDoS-потоків, коли кожен запит виглядає легітимним HTTPS-пакетом. Без інтелектуальної інспекції NGFW розрізнити такі атаки практично неможливо. Аналітика Cloudflare та Akamai показує рекордні хвилі трафіку понад 2–3 Тбіт/с, які здатні паралізувати роботу організацій та завдати значних фінансових збитків [8].

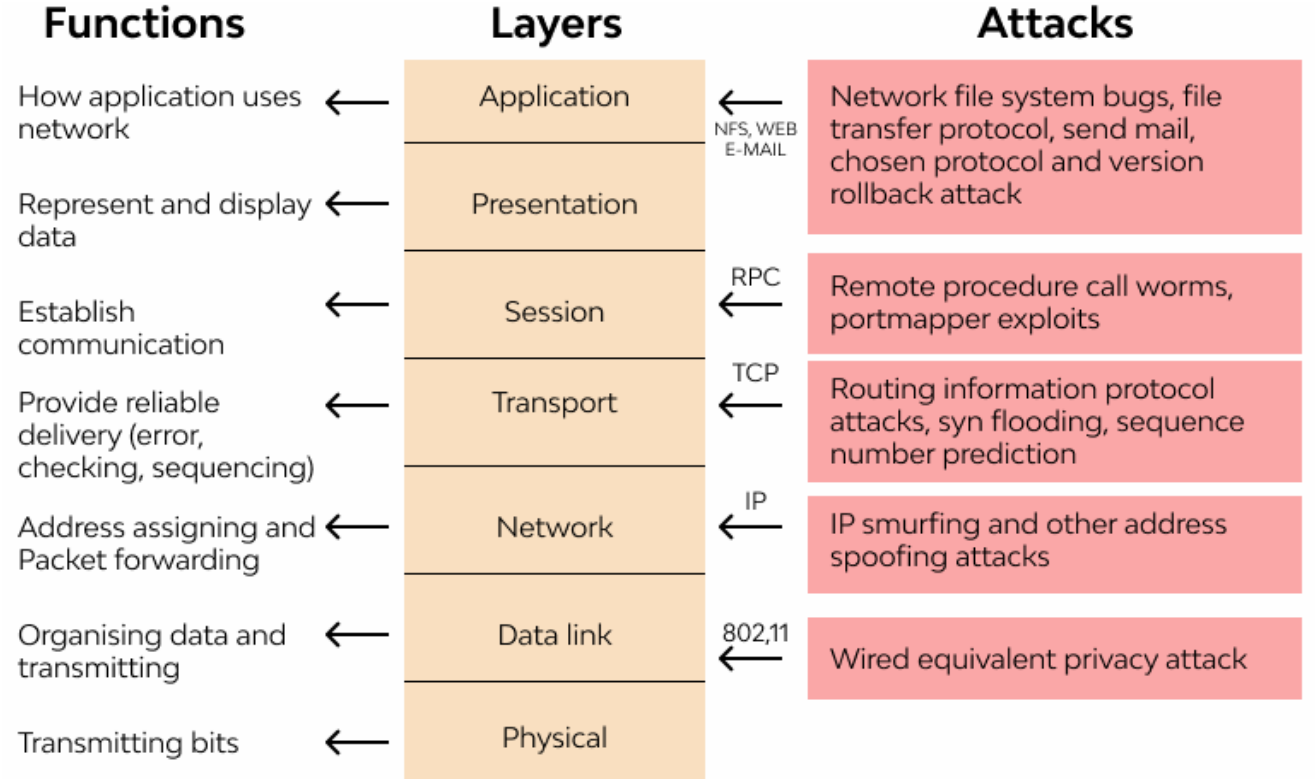


Рис 1.4 — Карта сучасних атак на мережевий периметр

Одним із найпідступніших видів атак є обхід міжмережевих екранів, що здійснюється через техніки маскування та обфускації трафіку. Для цього зловмисники використовують:

– тунелювання шкідливих даних у HTTP/HTTPS (наприклад, C2 у HTTP POST);

– DNS-тунелювання (dnscrypt, base64-пакети у TXT-запитах);

– використання протоколу QUIC, що ускладнює аналіз через шифрування;

– фрагментацію TCP/IP для обходу механізмів нормалізації;

– підробку або маніпуляцію TCP flags;

– використання легітимних хмарних CDN, що робить IP-блокування неефективним.

Більшість традиційних фаєрволів L3/L4 не можуть аналізувати вміст таких потоків, що створює серйозні прогалини у периметрі [9].

Рис 1.5 — Приклад атаки на периметр

Надзвичайно важливими є також атаки на прикладний рівень (L7). Зростання використання веб-додатків, API доступів, REST- і GraphQL-сервісів породжує величезний пласт вразливостей. До найпоширеніших належать:

–SQL Injection,

–Cross-Site Scripting (XSS),

–Remote Command Execution,

–Path Traversal,

–SSRF (Server-Side Request Forgery),

–API Rate Limit Exhaustion,

– API Injection.

На периметрі класичні фаєрволи не фільтрують JSON/HTTP-поля, не аналізують cookie-параметри, headers, payload-структури. Тому без NGFW з вбудованим IPS таких атак не уникнути [6], [10].

Окремим фронтом загроз є шифрований трафік, який сьогодні становить майже весь потік в Інтернет. Зловмисники активно використовують TLS для приховування своєї активності:

–C2-комунікації у зашифрованих HTTPS-з’єднаннях;

–завантаження шкідливого ПЗ через TLS;

–прихована ексфільтрація даних;

– фішингові сайти на HTTPS з валідними Let’s Encrypt сертифікатами.

Рис

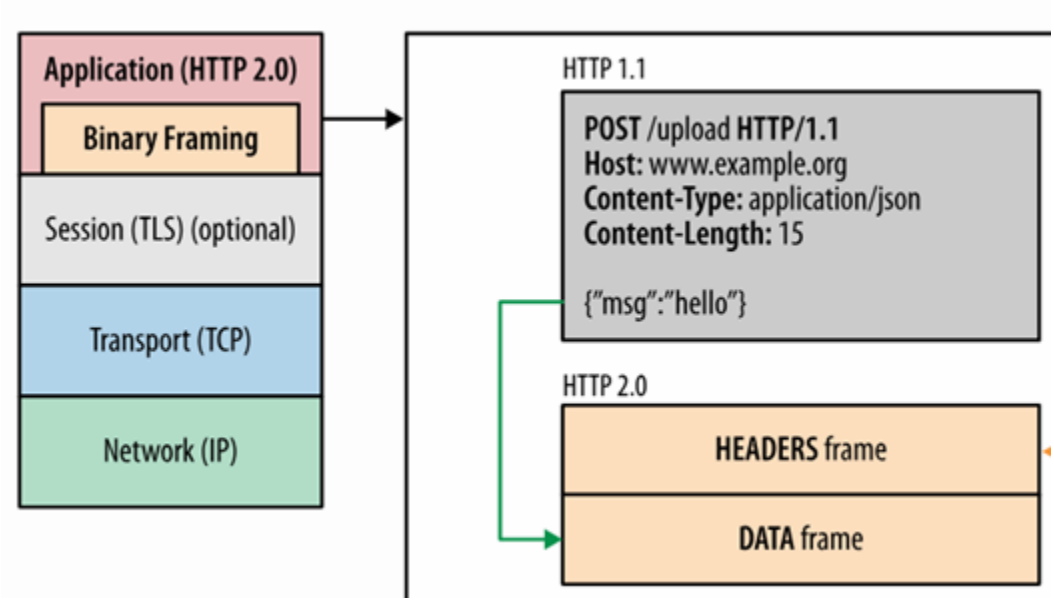


Рис 1.6 - Візуалізація DDoS HTTP/2 Rapid Reset Attack

Без механізмів SSL Inspection периметр втрачає видимість над 90% загроз — фактично захист зводиться нанівець [9].

Також значну частину інцидентів формують помилки конфігурації та людський фактор. Неправильні ACL, відкриті порти "тимчасово", неправильне перенаправлення NAT, відсутність зонування трафіку (DMZ/VPN/Users/Servers), невірний порядок правил у фаєрволі — усе це створює фактичні "дірки" у периметрі, які стають доступними для атак навіть без використання складних технік експлуатації. Згідно з дослідженнями, понад 40% проникнень у корпоративні мережі виникли через невірно налаштовані фаєрволи [7].

Сучасні інфраструктури також містять периметри нового типу — хмарні, які не мають чіткої фізичної межі. Хмарні API, відкриті сховища, балансувальники навантаження, SaaS-інтеграції — усе це формує логічний периметр, який атакують через:

–відкриті S3-бакети;

–неправильні IAM-політики;

–відкриті API endpoints;

–публічно доступні management console;

– слабкий контроль egress-трафіку.

NGFW, інтегровані з хмарними платформами (AWS, Azure, GCP), дозволяють централізовано бачити весь вхідний і вихідний трафік та застосовувати однакові політики незалежно від того, де знаходиться ресурс [10].

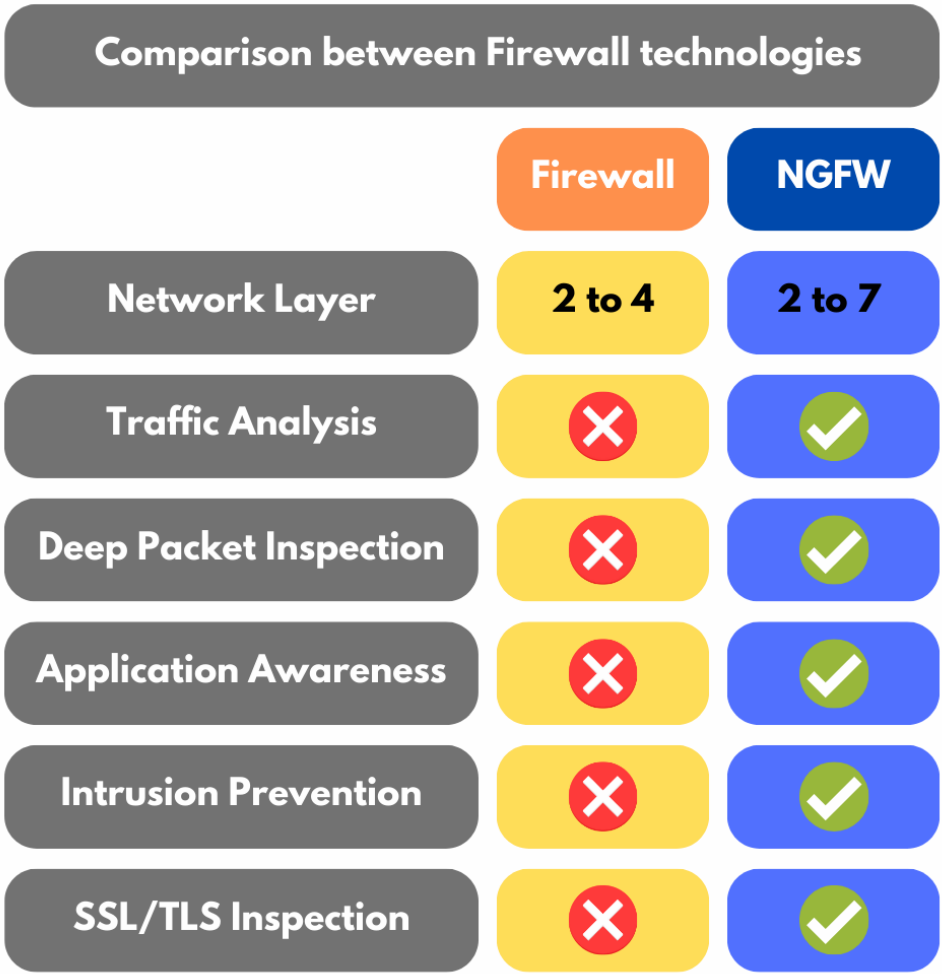


Рис 1.7 - Порівняння видимості традиційного FW vs NGFW при шифрованому трафіку

Узагальнюючи, мережевий периметр сьогодні перебуває під тиском багатовекторних загроз: від простого сканування та обхідних технік до високотехнологічних атак L7, експлуатації edge-вразливостей, шифрованих потоків та хмарних уразливостей. Саме тому застосування міжмережевих екранів нового покоління з можливостями SSL Inspection, IPS, поведінкової аналітики, машинного

навчання та інтеграції з SIEM є критично необхідним для побудови сильного периметрового захисту.

1.3. Огляд традиційних засобів захисту периметру та їх обмежень

Традиційні засоби захисту мережевого периметру історично формували основу корпоративної безпеки, оскільки розроблялися для середовищ із чітко окресленими кордонами мережі, мінімальною кількістю зовнішніх сервісів та передбачуваною структурою трафіку. Класичний підхід ґрунтувався на тому, що всі критично важливі ресурси розташовані всередині корпоративної мережі, а зовнішні підключення є винятковими та ретельно контрольованими. У такій моделі основну роль відігравали статичні міжмережеві екрани, системи фільтрації пакетів, NAT-механізми та VPN-шлюзи. Їхня ефективність у минулі десятиліття була достатньою, однак стрімкий розвиток хмарних сервісів, мобільності, гібридної роботи та зростання обсягів зашифрованого трафіку створили нові виклики, які традиційні системи більше не здатні повноцінно вирішувати [11].

Основним компонентом класичної периметрової архітектури були stateful firewalls — міжмережеві екрани стану. Їхнє завдання полягало у контролі входящих і вихідних з’єднань на основі IP-адреси, порту та протоколу. Такий підхід був ефективним у той період, коли більшість сервісів використовували статичні порти (наприклад, HTTP на 80, SMTP на 25), а трафік не був широко зашифрованим. Однак сучасні атаки здебільшого спрямовані не на транспортний рівень, а на прикладний — використовуючи API, вебсервіси, хмарні функції та складні сценарії взаємодії всередині HTTP(S)-трафіку. Класичний фаєрвол не здатен проаналізувати більшість таких взаємодій, оскільки працює лише на L3–L4 рівнях OSI-моделі, залишаючи усередині дозволених портів величезну «сіру зону» для зловмисників [12].

Крім того, традиційні засоби фільтрації пакетів не враховують, що сьогодні понад 90% трафіку в інтернеті шифрується за допомогою TLS 1.2–1.3. У новому стандарті TLS 1.3 видалено частину метаданих, які IDS-системи раніше могли використовувати для евристичного аналізу, що фактично «засліплює» класичні засоби контролю мережевого периметру [13]. У результаті атаки з використанням прихованих каналів, команд управління (C2), шкідливих бібліотек або кодів, які передаються в HTTPS, залишаються невиявленими.

Ще одним критично важливим елементом традиційної периметрової моделі є NAT (Network Address Translation). Хоча часто його помилково сприймають як інструмент безпеки, насправді NAT не виконує жодних функцій аналізу загроз. Його роль обмежується трансляцією адрес та створенням «маскування» внутрішньої структури мережі. Але відповідно до аналітики Cisco, NAT не запобігає сучасним атакам на вебзастосунки, API або хмарні сервіси і фактично є лише допоміжним маршрутизаційним механізмом [11].

VPN-шлюзи, попри те, що довгий час були стандартом для організації віддаленого доступу, сьогодні теж демонструють низку обмежень. Головна проблема полягає у тому, що VPN створює тунель усередину корпоративної мережі, що суперечить принципам Zero Trust. Компрометація облікового запису VPN або вразливість самого шлюзу дає зловмиснику майже повний доступ до внутрішніх сегментів, що підтверджується численними інцидентами 2021–2024 років, описаними ENISA [14]. Атаки типу credential stuffing, викрадення сертифікатів, експлуатація CVE у VPN-пристроях (особливо у Fortinet, SonicWall, Pulse Secure) стали одними з найбільш критичних загроз світового масштабу.

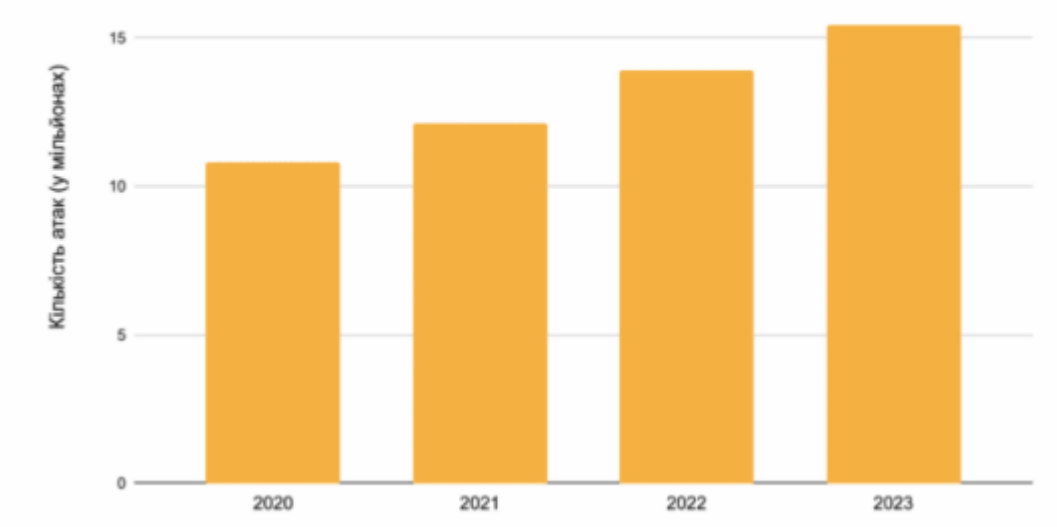


Рис 1.8 — Частота експлуатацій вразливостей в мережевому периметрі

IDS/IPS-системи також мають обмеження. Їхній сигнатурний підхід не дозволяє визначати нові або модифіковані атаки, поліморфні шкідливі програми, а також загрози, що передаються у зашифрованому трафіку. Глибока інспекція пакетів (DPI), яка була можливою у старіших версіях протоколів, стає дедалі менш ефективною. Більше того, із зростанням швидкостей каналів (10–40–100 Gbps) традиційні IDS/IPS перестають справлятися з обсягом трафіку без втрати продуктивності, що призводить до пропуску атак або затримок у роботі критичних сервісів [13].

Ще одним недоліком класичних периметрових засобів є відсутність контексту. Вони не вміють визначати, **хто** саме виконує підключення: користувач, сервісний акаунт, IoT-пристрій чи автоматизована система. Також вони не враховують тип пристрою, версію ОС, рівень ризику, геолокацію або поведінкові аномалії. Разом із тим більшість атак сьогодні відбувається саме через викрадення легітимних облікових даних, а без прив’язки до ідентичності традиційний фаєрвол не здатен відрізнити легітимного користувача від зловмисника.

Окремої уваги потребує питання масштабованості. Згідно з Gartner, традиційні фаєрволи розраховані на навантаження середини 2000-х років, тоді як сьогодні корпоративні мережі генерують на порядок більше запитів, особливо у зв’язку з

використанням хмарних сервісів, Kubernetes, мікросервісів та великої кількості API-викликів [13]. Традиційна архітектура просто не встигає обробляти такі обсяги без критичного падіння продуктивності.

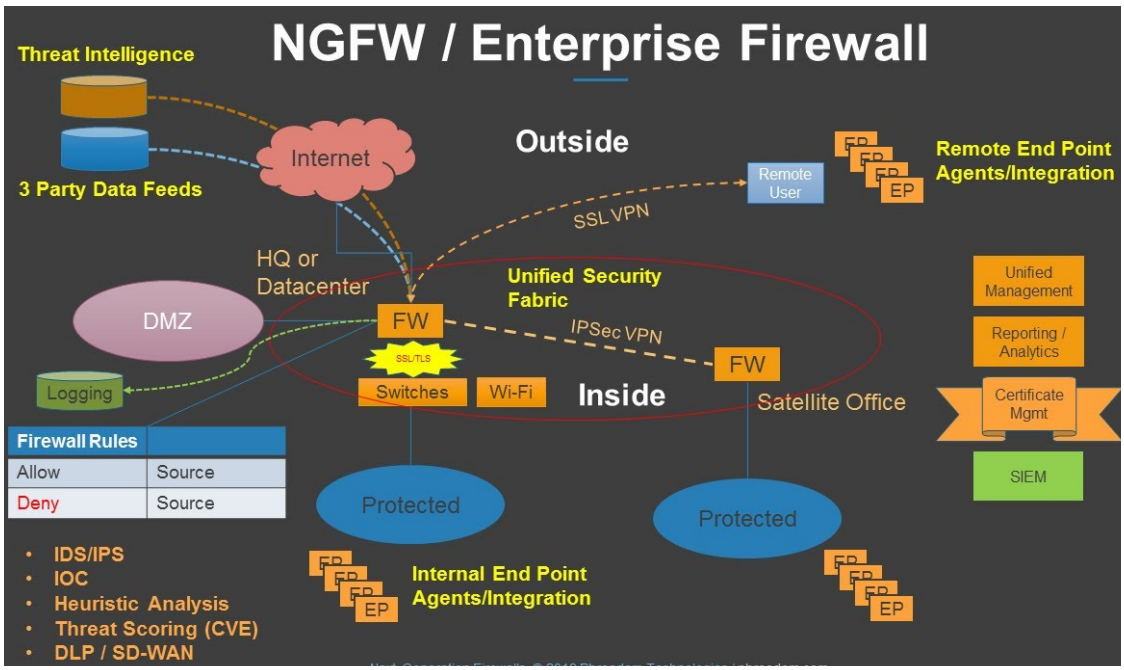
У сукупності ці фактори свідчать про те, що традиційні засоби захисту периметру втрачають актуальність і не можуть забезпечити необхідний рівень безпеки у сучасних динамічних мережах. Саме тому у 2010-х роках виникла нова категорія — міжмережеві екрани нового покоління (NGFW), які поєднують глибоку інспекцію трафіку, аналіз прикладних протоколів, ідентифікацію користувача, SSL-декрипцію, поведінкову аналітику та інтеграцію з платформами SIEM/SOAR. Тільки такі системи здатні забезпечити всебічний захист розмитого мережевого периметру, який сьогодні часто включає офісні сегменти, хмарні середовища, віддалені точки доступу та мобільні пристрої.

2 АНАЛІЗ МОЖЛИВОСТЕЙ МІЖМЕРЕЖЕВИХ ЕКРАНІВ НОВОГО ПОКОЛІННЯ (NGFW)

2.1. Архітектура та функціональні можливості NGFW

Міжмережеві екрани нового покоління (Next-Generation Firewall, NGFW) стали ключовим елементом сучасної мережевої безпеки, оскільки вони поєднують класичні механізми фільтрації трафіку з інтелектуальними інструментами аналізу загроз, глибокої інспекції пакетів та контекстно-орієнтованого контролю. На відміну від традиційних фаєрволів, що працюють на рівні IP-адрес, портів і протоколів, NGFW аналізує трафік на рівні додатків (L7), враховує ідентичність користувача, тип пристрою, поведінкові характеристики та дані загроз із зовнішніх джерел. Саме це робить його базовим компонентом Zero Trust та хмарно-орієнтованих архітектур безпеки [15].

Рис 2.1 — Архітектура NGFW



Архітектурно NGFW складається з кількох ключових модулів, що працюють узгоджено як єдина система. Першим шаром є traffic classification engine — механізм розпізнавання додатків (App-ID), який дозволяє аналізувати трафік незалежно від портів чи протоколів. Це важливо, оскільки сучасні застосунки, такі як Zoom, Teams, Dropbox чи WhatsApp, можуть динамічно змінювати порти або виконувати тунелювання всередині HTTPS. Модуль App-ID аналізує сигнатури, поведінкові патерни, характеристики сеансів і TLS-метадані, щоб точно визначити застосунок навіть у зашифрованому каналі. Традиційні фаєрволи не здатні виконати такий аналіз, що створює значну прогалину безпеки [16].

Наступним шаром є User-ID, який забезпечує прив’язку мережевої активності до конкретного користувача або групи. На відміну від старих моделей, де політики будувались за IP-адресами, NGFW інтегрується з Active Directory, RADIUS, Okta, LDAP та іншими IdP-системами для отримання актуальних даних про автентифікацію. Це дозволяє будувати політики з урахуванням ролі користувача, його місця розташування, типу пристрою та рівня привілеїв. Такий підхід мінімізує ризики компрометації мережі у випадку перехоплення IP або VPN-сесії, що особливо важливо у динамічних, хмарних та гібридних середовищах.

Ключовим компонентом NGFW є модуль SSL/TLS inspection, що дозволяє здійснювати аналіз зашифрованих потоків трафіку. Оскільки за сучасними даними понад 90% загроз передаються через TLS-канали (включаючи C2-комунікації, malware delivery, phishing URL та data exfiltration), розшифрування трафіку стає необхідною умовою виявлення загроз. NGFW здійснює man-in-the-middle інспекцію з використанням корпоративного сертифіката, після чого передає дані на модулі антивірусу, sandbox-аналізу та IPS. Частина рішень також підтримує selective decryption: наприклад, не розшифровувати банківські або медичні дані, але аналізувати інший HTTPS-трафік відповідно до вимог GDPR/ISO 27001 [17].

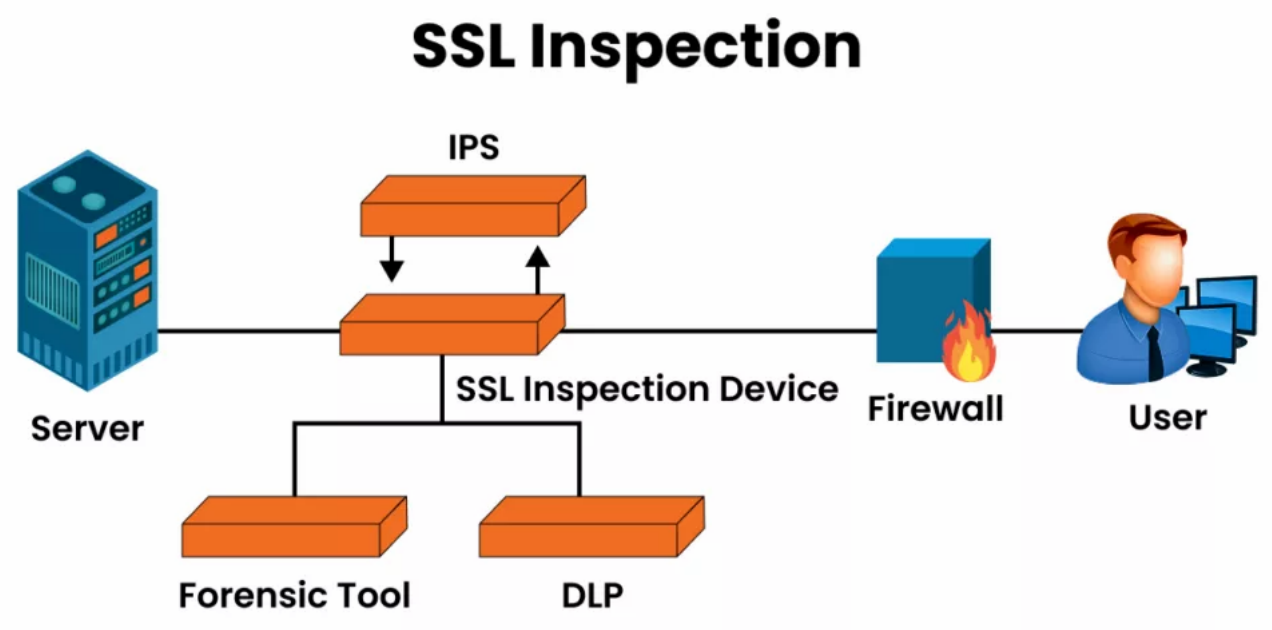


Рис 2.2 - Принцип роботи SSL Inspection

Особливу роль у архітектурі NGFW відіграє IPS (Intrusion Prevention System) — система запобігання вторгненням, яка працює на рівні L7 і поєднує сигнатурний, поведінковий та машинний аналіз. Окрім виявлення класичних атак (SQL injection, XSS, buffer overflow), сучасні NGFW здатні виявляти аномальну поведінку, нетипові послідовності запитів, модифіковані експлойти та zero-day загрози. IPS використовує так званий threat cloud — глобальну хмару машинного навчання, яка збирає та аналізує зразки шкідливого коду з різних регіонів світу, оновлюючи сигнатури у реальному часі. Це робить NGFW значно ефективнішим у порівнянні з класичними IDS/IPS, що оновлюються вручну або із запізненням [15].

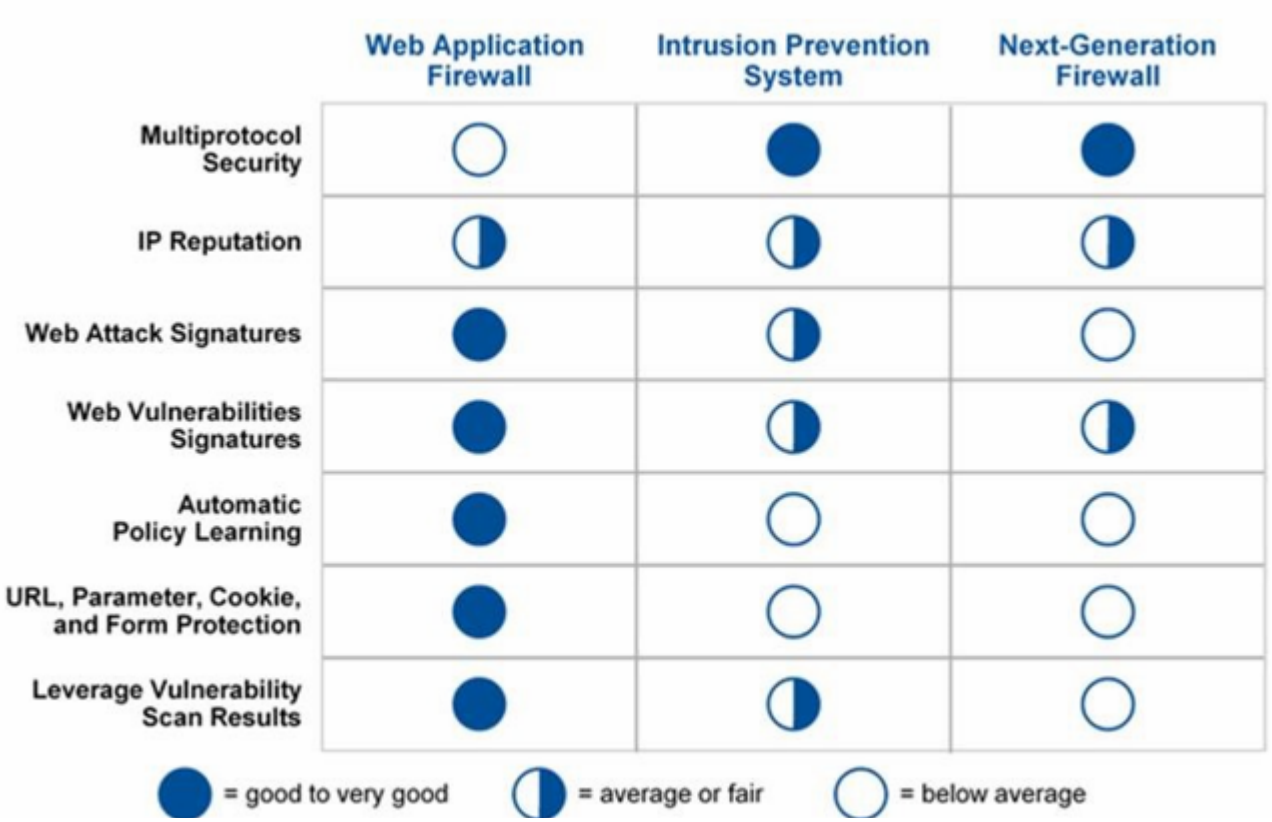


Рис 2.3 - Порівняння спеціальних можливостей NGFW з суміжними рішеннями

Принципово важливим елементом сучасних NGFW є URL Filtering та DNS Security — модулі, що блокують небезпечні домени, категорії сайтів, фішингові ресурси та C2-адреси. Модуль DNS Security аналізує запити за шаблонами ентропії, поведінковими характеристиками та відомими DGA-патернами, що дозволяє виявляти атаки, які традиційні системи не фіксують. Не менш важливою частиною є Data Loss Prevention (DLP) — механізм контролю вихідного трафіку для запобігання витоку конфіденційної інформації, включаючи файли, текстові дані, персональні відомості та комерційну таємницю. DLP-модуль може автоматично блокувати передачу документів певного типу або із вмістом певних шаблонів, наприклад номерів платіжних карток чи персональних ідентифікаторів.

Архітектура NGFW також включає Sandbox / Malware Analysis Engine, який забезпечує ізольоване виконання файлів для визначення шкідливої поведінки. Це особливо важливо у боротьбі з zero-day-атаками, поліморфними вірусами та

шкідливим програмним забезпеченням, яке неможливо розпізнати суто сигнатурними методами. У sandbox-середовищі NGFW аналізує API-виклики, процеси, модифікацію реєстру, мережеву взаємодію та аномалії, формуючи детальний verdict, який надалі автоматично використовується в IPS-сигнатурах [16].

Сучасні NGFW працюють за принципом контекстно-орієнтованої політики (context-aware policy), коли політика доступу визначається не лише IP-адресою чи портом, а сукупністю параметрів: застосунком (App-ID), користувачем (User-ID), пристроєм (Device-ID), ідентифікатором загрози (Threat-ID), геолокацією, типом контенту, ризиковим профілем та поведінкою сесії. Комплексне поєднання цих характеристик дозволяє створювати політики на кшталт: дозволити доступ до корпоративного CRM лише авторизованим користувачам з корпоративних ноутбуків, що відповідають вимогам безпеки, з території ЄС, з увімкнутим шифруванням диска та актуальними оновленнями. Такі політики принципово неможливо реалізувати у класичних L3/L4 фаєрволах, що чітко демонструє фундаментальну перевагу NGFW.

Ще одним важливим компонентом архітектури NGFW є Centralized Management & Log Analytics, який дозволяє централізовано керувати політиками, збирати журнали подій, інтегрувати дані з SIEM-системами та проводити глибокий аналіз інцидентів. Більшість провайдерів NGFW (Palo Alto Networks Panorama, Fortinet FortiManager, Check Point SmartConsole тощо) підтримують єдину консоль керування, що забезпечує масштабованість на сотні філій та тисячі пристроїв.

-

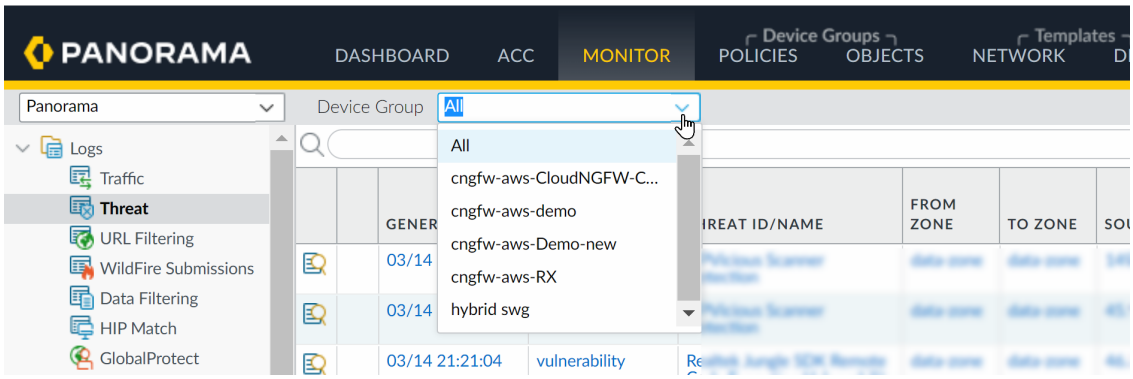


Рис 2.4 Приклад відображення подій в NGFW

Завдяки модульному принципу NGFW виконує роль універсального безпекового шлюзу, який одночасно забезпечує контроль застосунків, виявлення атак, декрипцію трафіку, блокування загроз, контроль доступу, запобігання витоку даних, аналіз поведінки та сегментацію мережевого периметру. У результаті NGFW формує «інтелектуальний периметр», який не обмежується статичними правилами, а адаптується до контексту, змінюючи політики в режимі реального часу залежно від рівня ризику, типу взаємодії та поведінкових патернів. Таким чином, NGFW є критично необхідним елементом сучасної оборонної архітектури, здатним ефективно протидіяти складним мережевим атакам, зменшувати площину атаки, забезпечувати видимість у зашифрованих каналах і створювати багаторівневий механізм контролю, якого в принципі не могли забезпечити традиційні фаєрволи.

2.2. Інтеграція NGFW з системами моніторингу та управління подіями

Інтеграція міжмережевих екранів нового покоління (NGFW) із системами моніторингу та управління подіями безпеки є фундаментальним елементом побудови сучасної архітектури кіберзахисту, орієнтованої на оперативне виявлення, кореляцію та автоматизацію реагування на інциденти. У міру того, як мережеві інфраструктури стають дедалі складнішими та динамічнішими, традиційний підхід до аналізу журналів фаєрволу в ручному режимі втрачає ефективність. Сучасні атаки здійснюються у багатоступеневому форматі, використовують шифрування, обфускацію та приховані канали зв’язку, що потребує інтеграції NGFW у ширшу екосистему систем безпеки. Як зазначає Gartner, сучасні організації не можуть забезпечити повноцінний SOC (Security Operations Center) лише за рахунок журналів мережевого обладнання — необхідна комплексна кореляція подій, зокрема агрегованих з NGFW, EDR, IAM та хмарних сервісів [17].

У рамках інтеграції NGFW виступає ключовим сенсором мережевої телеметрії, забезпечуючи надходження даних про трафік, загрози та активність користувачів до централізованих SIEM-платформ. Завдяки глибокій інспекції пакетів та L7-контролю фаєрвол нового покоління надає значно більше інформації, ніж традиційний L3/L4-екран: контекст застосунку, ідентичність користувача, джерело загрози, деталі SSL-інспекції, сигнали IPS/IDS, репутаційні дані доменів або IP-адрес. Ця структурована телеметрія, передана у форматах Syslog, CEF або JSON, може бути нормалізована та індексована SIEM-системою для подальшого кореляційного аналізу, що дає змогу визначати складні атаки, які ізольований NGFW виявити не здатен [14].

У типових сценаріях NGFW передає події до SIEM у кількох основних категоріях: логі трафіку (traffic logs), журнали IPS (intrusion events), дані про шкідливі файли та URL-категоризацію, журнали політик доступу, системні події, SSL-телерметрію та аналітичні метадані. Згідно з рекомендаціями IBM QRadar, NGFW є однією з найцінніших точок збору даних для SOC, оскільки на рівні мережевого периметру фіксується більшість спроб вторгнення, розвідки та brute-force атак [20]. SIEM, у свою чергу, збагачує ці події даними з інших джерел: інформацією про автентифікацію, поведінкою кінцевих точок, логами серверів, хмарними аудитами, що дає змогу виявляти складні багатоступеневі ланцюги атак. Наприклад, у типовій багаторівневій атаці зловмисник може спочатку здійснити сканування портів, потім виконати підбір пароля, отримати доступ до внутрішнього сервера, переміститися вбік (lateral movement) та ексфільтрувати дані через HTTPS. Окремо NGFW бачить лише фрагменти цього процесу, проте SIEM, корелюючи події за часовими та поведінковими характеристиками, визначає повний ланцюг інциденту та формує єдине аналітичне повідомлення.

Особливу роль відіграє інтеграція NGFW із SOAR-платформами, які забезпечують автоматизацію реагування. Найпоширеніша модель взаємодії полягає у тому, що NGFW надсилає журнали до SIEM; SIEM корелює події й визначає, чи є

аномалія частиною широкої атаки; SOAR отримує сформований інцидент, виконує enrichment (дані з threat intelligence, геолокацію, репутацію), після чого автоматично надсилає NGFW команду блокування IP-адреси, користувача або домену. У випадку критичних загроз, таких як ransomware або C2-трафік, така автоматизована схема реагування знижує час нейтралізації до секунд, мінімізуючи вплив атаки. За даними Gartner, повністю автоматизовані SOC-цикли дозволяють скоротити час реагування на інциденти на 70–85% [16].

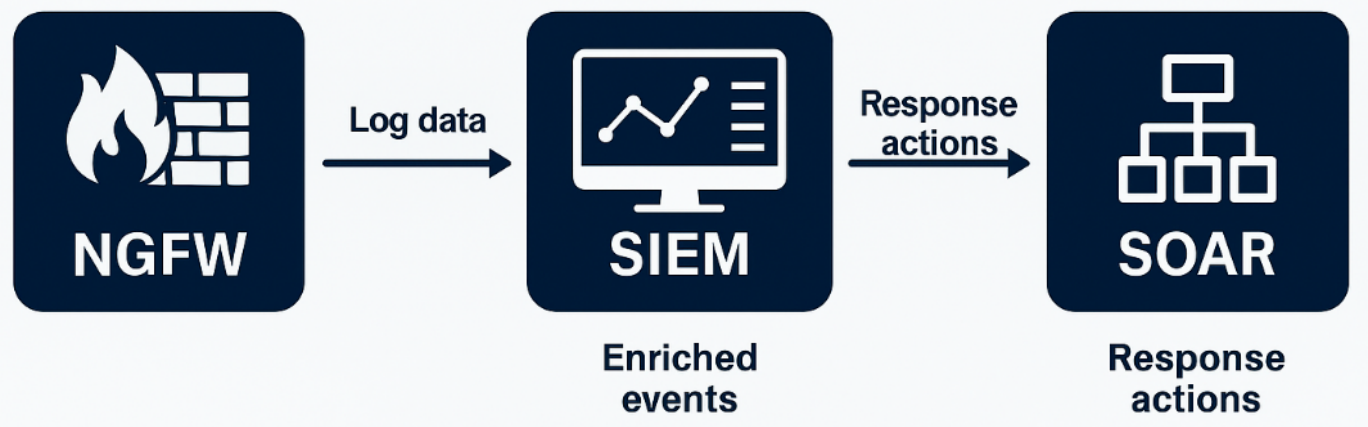


Рис 2.5 - Архітектура інтеграції NGFW ↔ SIEM ↔ SOAR

Не менш важливою є інтеграція NGFW із системами threat intelligence. Більшість виробників (Palo Alto Networks, Fortinet, Check Point) підтримують потокове оновлення репутаційних баз, сигнатур IPS, URL-категорій та IoC (Indicators of Compromise). При цьому NGFW може передавати в SIEM телеметрію для формування внутрішніх профілів ризиків користувачів та пристроїв, тоді як SIEM може розподіляти оновлені IoC на всі NGFW-пристрої в інфраструктурі, забезпечуючи «динамічну безпеку», що адаптується до актуальних загроз. IBM у своїй документації підкреслює, що інтеграція між NGFW та SIEM дозволяє мінімізувати "visibility gaps" — ситуації, коли атака залишається непоміченою через відсутність повного контексту [15].

У сучасних моделях XDR (Extended Detection and Response) NGFW стає ключовим елементом у формуванні наскрізного ланцюга виявлення атак. NGFW передає мережеві метадані; EDR передає поведінкові сигнали з хостів; SIEM

об’єднує їх у загальну структуру; SOAR виконує реагування. Такий підхід дозволяє перехоплювати lateral movement, приховані C2-канали, атаки на веб-застосунки, DNS-тунелювання та інші, які окремі системи не виявляють. NGFW також активно використовується для мережевої сегментації, а SIEM контролює відповідність і моніторить порушення політик, забезпечуючи роботу в межах Zero Trust-архітектури.

```
index=ngfw_logs
| eval action=upper(action)
| stats count BY src_ip, dest_ip, app, action
| where action="DENY" AND count > 50
| lookup threat_intel bad_ips AS dest_ip OUTPUT risk_score severity
| where risk_score > 70
| eval alert="POSSIBLE BRUTE FORCE OR THREAT ACTIVITY DETECTED"
| table _time, src_ip, dest_ip, app, count, risk_score, severity, alert
```

Рис 2.6 — Приклад запиту в SIEM на отримання подій з NGFW

Важливо відзначити, що інтеграція NGFW та SIEM забезпечує кілька стратегічних переваг: централізовану видимість, підвищений рівень виявлення складних атак, можливість формування повних forensic-звітів, автоматизоване реагування, адаптивну зміну політик безпеки та гарантування відповідності міжнародним стандартам (ISO/IEC 27001, NIST CSF). У сукупності NGFW стає не лише пристроєм фільтрації трафіку, а частиною інтелектуальної платформи кіберзахисту, здатної взаємодіяти з усією екосистемою безпеки підприємства й забезпечувати активну оборону в режимі реального часу.

2.3. Порівняння NGFW з класичними міжмережевими екранами

Порівняння міжмережевих екранів нового покоління (NGFW) із класичними фаєрволами доцільно виконувати не тільки з погляду «функцій у чек-листі», а й через призму еволюції самих загроз та мережевих архітектур. Класичний

міжмережевий екран історично будувався навколо моделі периметру: є внутрішня «довірена» мережа, є «злий» Інтернет, між ними – L3/L4-фільтрація за IP-адресами, портами й протоколами. Основне завдання – дозволити чи заборонити з'єднання відповідно до Access Control List (ACL). Така логіка добре працювала в часи, коли більшість сервісів були статичними, порти – передбачуваними, а TLS-трафік займав незначну частину каналу. Сучасний світ – інший: домінує HTTPS, додатки працюють через CDNs, порти динамічні, користувачі підключаються з будь-яких пристроїв і локацій, а значна частина атак маскується під легітимний веб-трафік. У цих умовах класичний L3/L4-фаєрвол за своєю природою «сліпий» до того, що відбувається всередині з'єднання, а отже втрачає ефективність як єдиний засіб захисту периметру.

NGFW виріс із розуміння цього обмеження. Його концепція – перейти від моделі «IP+порт» до моделі «хто, куди, яким додатком, з яким контентом і з яким рівнем ризику». Це означає, що NGFW вбудовує в себе одразу кілька класів систем: класичний stateful firewall, систему запобігання вторгненням (IPS), модуль глибокої інспекції пакетів (DPI) з розпізнаванням додатків (App-ID), SSL/TLS-decryption проксі, URL-фільтрацію, DNS-security, DLP, а в багатьох реалізаціях ще й sandbox для динамічного аналізу шкідливого коду. Тобто NGFW перестає бути «просто фільтром на портах» і стає повноцінним безпековим шлюзом, який дивиться на трафік на рівні 7-го (і вищих логічних рівнів), зіставляє його з політиками, сигнатурами, поведінковими моделями та даними глобальної threat intelligence.

Ключова відмінність полягає у глибині контексту. Класичний фаєрвол приймає рішення на основі пари src/dst IP, src/dst port, протоколу, іноді – інтерфейсу чи зони. Якщо через порт 443 іде трафік – для нього це просто «HTTPS», без розуміння, що всередині: корпоративний CRM, Slack, Tor, Telegram чи C2-канал шкідливого ПЗ. NGFW намагається ідентифікувати саме додаток, незалежно від порту: аналізує handshake, TLS SNI, HTTP-заголовки, характер payload, послідовність запитів. Це дає змогу не просто «дозволити 443», а, наприклад, дозволити тільки Microsoft 365, Salesforce і корпоративний портал, при цьому

заблокувавши проксі/VPN, анонімайзери та небажані хмарні сховища. З точки зору контролю shadow IT це принципово інший рівень керованості периметром.

Ще один шар – ідентифікація користувача. Класичний фаєрвол, за винятком деяких проксі-рішень, працює з IP-адресою й не розуміє, хто саме стоїть за з'єднанням. У середовищах із динамічною адресацією, VPN, Wi-Fi, VDI це робить політики на основі IP дуже крихкими. NGFW інтегрується з AD, LDAP, RADIUS, SSO/IdP і будує політики за user/group: для відділу фінансів – одні права, для адміністрації – інші, для підрядників – треті. Це відразу наближає периметрову політику до Zero Trust-моделі: доступ визначається не «де ти сидиш у топології», а «хто ти, з чим ти прийшов, до чого саме звертаєшся і наскільки це ризиковано».

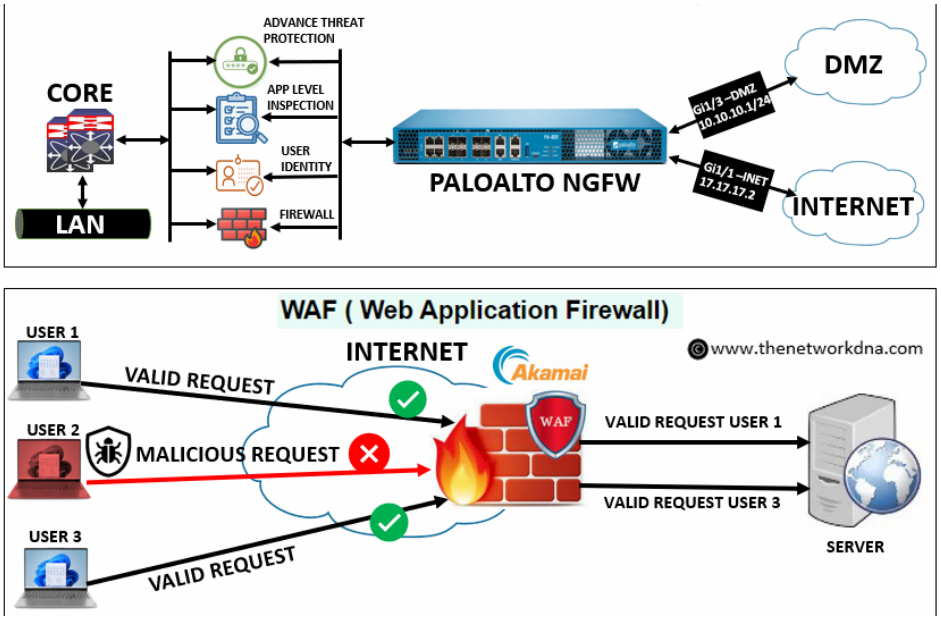


Рис 2.7 — Практична імплементація NGFW

Надзвичайно важливим є питання шифрованого трафіку. В класичних фаєрволах SSL/TLS-трафік, як правило, не розшифровується – максимум здійснюється SNI-фільтрація чи блокування певних IP/доменів. У результаті понад 80–90% трафіку перетворюється на «темну зону», де може ховатися все: від exfiltration до ransomware. NGFW із підтримкою SSL inspection піднімає TLS-проксі, підмінює сертифікат (корпоративний root CA), розшифровує трафік, проганяє його

через IPS/AV/DLP/URL-фільтр і лише потім знову шифрує до кінцевого вузла. Це дає змогу виявляти шкідливі вкладення, фішингові сторінки, експлойти, C2-трафік, які класичні рішення просто не побачать. Так, це створює додаткові виклики (продуктивність, юридичні вимоги, винятки для банкінгу/медицини), але з точки зору безпеки дає принципово інший рівень видимості.

IPS у NGFW також суттєво відрізняється від класичного «підвішеного IDS/IPS» поруч. У старих схемах IPS часто працював у режимі tap/span або inline, але з окремою консоллю, сигнатурами, політиками й логами. Це збільшувало латентність управління: Firewall щось дозволив, IPS щось заблокував, SOC має дві різні картини світу. У NGFW IPS є невід'ємним модулем пайплайна обробки: трафік, який пройшов по stateful ACL, автоматично аналізується сигнатурно і поведінково, а рішення приймається вже з урахуванням політики загроз. Це спрощує кореляцію: аналітик бачить в одному логі, що «користувач X, додаток Y, сесія Z, правило доступу R, сигнатура загрози S, verdict – blocked/allowed with reset». З точки зору розслідування, це величезний плюс.

NGFW також значно сильніший в інтеграції з екосистемою: SIEM, SOAR, EDR/XDR, SD-WAN, хмарні сервіси. Класичні фаєрволи часто вміють лише відправляти syslog; далі – справа SIEM-інженера. NGFW, як правило, має структуровані формати логів, власні API, конектори для основних платформ, попередньо визначені дашборди, risk-score користувачів і сесій. Багато рішень дозволяють будувати автоматизовані playbook-и: наприклад, якщо NGFW кваліфікує сесію як high-risk, SOAR-оркестратор може створити інцидент, заблокувати користувача в IdP і створити ticket у ITSM. Такий рівень оркестрації для класичних фаєрволів, як правило, доступний тільки за рахунок кастомної інтеграції й великої ручної роботи.

У плані продуктивності й архітектури NGFW історично вважалися «важчими», оскільки глибока інспекція і декрипція вимагають більше CPU/ASIC. Однак сучасні NGFW-пристрої використовують спеціалізовані чипи (NP, SPU, ASIC)

і оптимізовані конвеєри, які дозволяють тримати десятки Гбіт/с навіть з увімкненим IPS і частковим SSL Inspection. Там, де класичний фаєрвол демонструє вищу «сиру» пропускну здатність, NGFW компенсує це якістю захисту. На практиці часто застосовується гібридний підхід: на ядровому рівні ставиться простий L3/L4-фільтр/ACL на високошвидкісних маршрутизаторах, а весь критичний південний/північний трафік (North-South) проходить через NGFW, який забезпечує глибокий аналіз.

Важливо пам’ятати, що традиційні фаєрволи мають свою нішу – прості, статичні, сегментовані середовища з жорстко визначеним набором сервісів: наприклад, ізольовані OT/ICS-сегменти, де головне – стабільність і мінімальний latency, а трафік передбачуваний. Там NGFW з усіма його «інтелектуальними» фічами може бути надлишковим, особливо якщо немає SOC, готового це все аналізувати. У таких випадках іноді доцільно використати простий stateful firewall плюс окремий пасивний моніторинг. Але для більшості живих корпоративних мереж із хмарою, SaaS, мобільними користувачами, VPN, партнерськими каналами NGFW фактично стає must-have.

З точки зору моделі загроз NGFW дає змогу закрити цілий пласт атак, які класичний фаєрвол пропускає: exploitation через веб-додатки, C2-трафік у HTTPS, DNS-тунелювання, використання легітимних хмарних сервісів для exfiltration, lateral movement через стандартні порти, приховані проксі і VPN у web-трафіку. NGFW із модулем DNS Security ловить аномальні домени і DGA, IPS – специфічні експлойти, URL-фільтр – категорії фішингу і malware, DLP – спроби витоку, sandbox – нові зразки шкідливого коду. В сумі це дозволяє перейти від простої «фільтрації доступу» до повноцінної «платформи протидії загрозам» на периметрі.

Ще один вимір порівняння – модель побудови політик. Класичні фаєрволи легко перетворюються на хаотичний набір ACL із технічними описами «allow tcp any any 443», де зрозуміти бізнес-сенс правила важко навіть авторам. У NGFW політика, як правило, описується в термінах бізнесу: «Finance_Users → SAP_Finance_App →

Allow with SSL Decrypt and DLP», «Contractors → Only SSH to Jump Host with MFA», «All Users → Social Media → Allow but No Uploads». Це полегшує audit, комплаєнс, перевірку відповідності вимогам стандартів (ISO, NIST, PCI DSS) і спрощує комунікацію між безпекою й бізнесом.

Разом із тим NGFW – не «чарівна таблетка». Вони вимагають кваліфікованого налаштування, постійного оновлення сигнатур і політик, ретельного планування SSL-decryption (винятки, сертифікати, правові аспекти), грамотної інтеграції з SIEM/SOAR, інакше організація просто потоне в логах. Неправильно налаштований NGFW може або надто «задушити» бізнес-процеси, або навпаки – пропускати небезпечний трафік, якщо все залишити за замовчуванням. Тому технологічна перевага над класичними фаєрволами реалізується тільки за наявності процесів: моделювання загроз, управління політиками, регулярного review правил, тестування, аналізу інцидентів.

Таблиця 2.1.

Правила для виявлення аномальної активності

Критерій	Класичний файрвол	NGFW
Рівень аналізу	L3/L4 (IP, порт, протокол, stateful)	L3–L7, контент, додаток, користувач, контекст
Розпізнавання додатків	Ні, максимум – порт/протокол	Так (App-ID, DPI), незалежно від порту
Ідентифікація користувача	Переважно за IP	User-ID через AD/IdP, групи, ролі
SSL/TLS інспекція	Обмежена або відсутня	Повноцінна декрипція з політиками винятків
IPS/IDS	Окремий модуль/пристрій	Вбудований IPS із сигнатурним та поведінковим аналізом
URL/DNS-фільтрація	Здебільшого немає або дуже базова	Розвинені модулі URL Filtering, DNS Security

DLP	Відсутній	Вбудований контроль витоку (файли, шаблони даних)
Sandbox / аналіз малварі	Немає	Часто вбудований або інтегрований хмарний sandbox
Модель політик	ACL за IP/портами, технічні описи	Контекстні політики: користувач + додаток + контент + ризик
Інтеграція з SIEM/SOAR	Syslog, обмежений набір полів	Структуровані логи, API, готові конектори, risk-based підхід
Підтримка Zero Trust, сегментація	Базова зонова сегментація	Мікросегментація, identity-aware, application-aware
Видимість у зашифрованому трафіку	Низька	Висока (за рахунок SSL inspection)
Сценарії використання	Простий периметр, статичні сервіси, WAN-ACL	Корпоративні, хмарні, гібридні, SASE/SD-WAN, high-risk середовища

Підсумовуючи, можна сказати, що класичні фаєрволи – це інструмент «минулого покоління загроз», заточений під просту, статичну, слабо шифровану мережу. NGFW – відповідь на сучасний ландшафт: шифрування за замовчуванням, динамічні додатки, хмара, гібридні користувачі, складні багатоступеневі атаки. Для побудови технології захисту мережевого периметру в реальній організації NGFW дає критичні переваги: глибоку видимість трафіку, контекстний контроль, вбудовану боротьбу з загрозами та інтеграцію в SOC-ланцюг. Класичні фаєрволи можуть залишатися як нижній шар – для грубої сегментації й базового контролю, але роль «першої лінії захисту» у більшості сценаріїв логічно переходить саме до NGFW.

3 РОЗРОБКА ТЕХНОЛОГІЇ ЗАХИСТУ МЕРЖЕВОГО ПЕРИМЕТРУ НА ОСНОВІ NGFW

3.1. Проєктування моделі багаторівневого захисту периметру

Проєктування моделі багаторівневого захисту мережевого периметру на основі NGFW передбачає перехід від уявлення про периметр як «одну лінію оборони» до концепції каскаду взаємопов'язаних рубежів, де кожен рівень виконує власну чітко визначену функцію: груба фільтрація й сегментація, глибока інспекція трафіку, контроль доступу на рівні застосунків і користувачів, запобігання вторгненням, протидія витоку даних, моніторинг та аналітика. Технологічно це означає поєднання класичних засобів маршрутизації/ACL із NGFW, що працюють у режимі контекстно-орієнтованого шлюзу безпеки, а також інтеграції з внутрішньою інфраструктурою – системами автентифікації, SIEM/SOAR, DNS, проксі, EDR/XDR.

Вихідною точкою є побудова логічної моделі «зон безпеки». Замість умовного поділу «LAN – DMZ – Internet» формується детальна карта сегментів: зовнішня зона (untrusted), демілітаризована зона публічних сервісів (DMZ), зона критичних бізнес-додатків (Business Apps Zone), сегменти користувацьких мереж (User LAN, Wi-Fi), зони для підрядників і гостьового доступу, окремі сегменти для адміністраторських систем, OT/ICS, резервного копіювання, а також шлюзи доступу до хмарних ресурсів і VPN-концентраторів. NGFW у цій моделі виступає центральним елементом, через який проходить як зовнішній трафік «north–south» (між внутрішніми мережами та Інтернетом/хмарою), так і частина «east–west»-трафіку між внутрішніми сегментами, де потрібен підвищений контроль.

На фізичному та логічному рівні NGFW зазвичай розгортається у режимі high availability (active/standby або active/active), підключаючись до основних маршрутизаторів/ядрових комутаторів через trunk-інтерфейси з VLAN-tagging. Така

схема дозволяє реалізувати віртуальні маршрутизуючі інстанси (VRF/Virtual Router) та зональну модель: кожен інтерфейс (або підінтерфейс) NGFW прив'язується до конкретної зони безпеки (Untrust, DMZ, Internal, VPN, Guest, Management тощо). На рівні маршрутизації задаються статичні маршрути або використовується динамічний протокол (OSPF/BGP) для взаємодії з backbone, але всі політики доступу реалізуються саме в площині NGFW-політик, а не на рівні сирих ACL маршрутизатора.

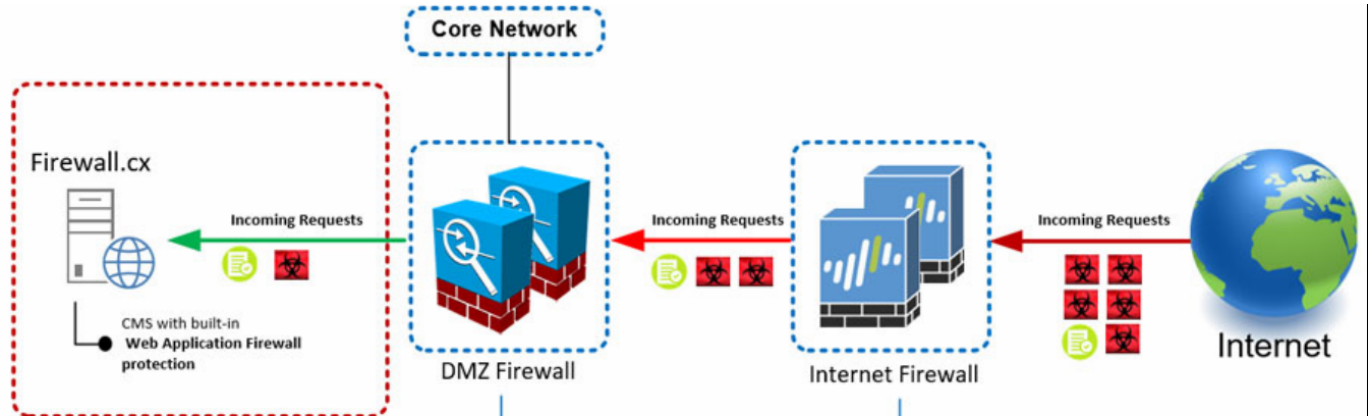


Рис 3.1 - Модель зонування мережі

Основний принцип – «default deny» між усіма зонами, окрім явно дозволених шляхів. Трафік між будь-якими двома зонами повинен проходити через NGFW; прямі L2/L3-з'єднання без фаєрвола допускаються тільки там, де це обґрунтовано (кластерні внутрішні сегменти, трафік реплікації тощо, і то бажано – з окремими засобами контролю). Перший рівень політик на NGFW формує грубий каркас: які зони можуть взагалі взаємодіяти (наприклад, Guest → Internet тільки web-трафік; Internal → DMZ – строго визначені сервіси; DMZ → Internal – за замовчуванням заборонено, окрім структурованих back-end-з'єднань). На цьому рівні вже можна використати application-aware модель: замість «tcp/80,443» – «HTTP/HTTPS тільки до категорії "Business Applications", блокування проксі/анонімайзерів, TOR, масових public-cloud storage, якщо вони не потрібні бізнесу».

Другий рівень – глибока інспекція трафіку з використанням IPS, SSL/TLS-decryption, URL/DNS-фільтрації й сигнатур/behavioral-двигунів. На етапі

проєктування потрібно вирішити, через які саме шляхи проходитиме повна декрипція, а де – часткова або винятки. Зазвичай формується матриця: користувачі офісу, VPN-користувачі, сервери в DMZ, критичні бізнес-додатки. Для користувачів, що виходять у Інтернет, вмикається повна SSL-inspection (окрім категорій, де це заборонено політиками – банкінг, охорона здоров'я, деякі HR-сервіси). Для DMZ-сегментів декрипція застосовується до вхідного трафіку, що спрямований на веб-сервіси: NGFW розшифровує запит, IPS та Web Protection модулі аналізують payload, блокують експлойти, SQLi/XSS, сканування, вразливості CMS тощо, після чого трафік передається на веб-сервер. У зворотному напрямку (вихід сервера в Інтернет) SSL-inspection може використовуватись для контролю оновлень, підключень до сторонніх API, запобігання C2-з'єднанням у разі компрометації сервера.

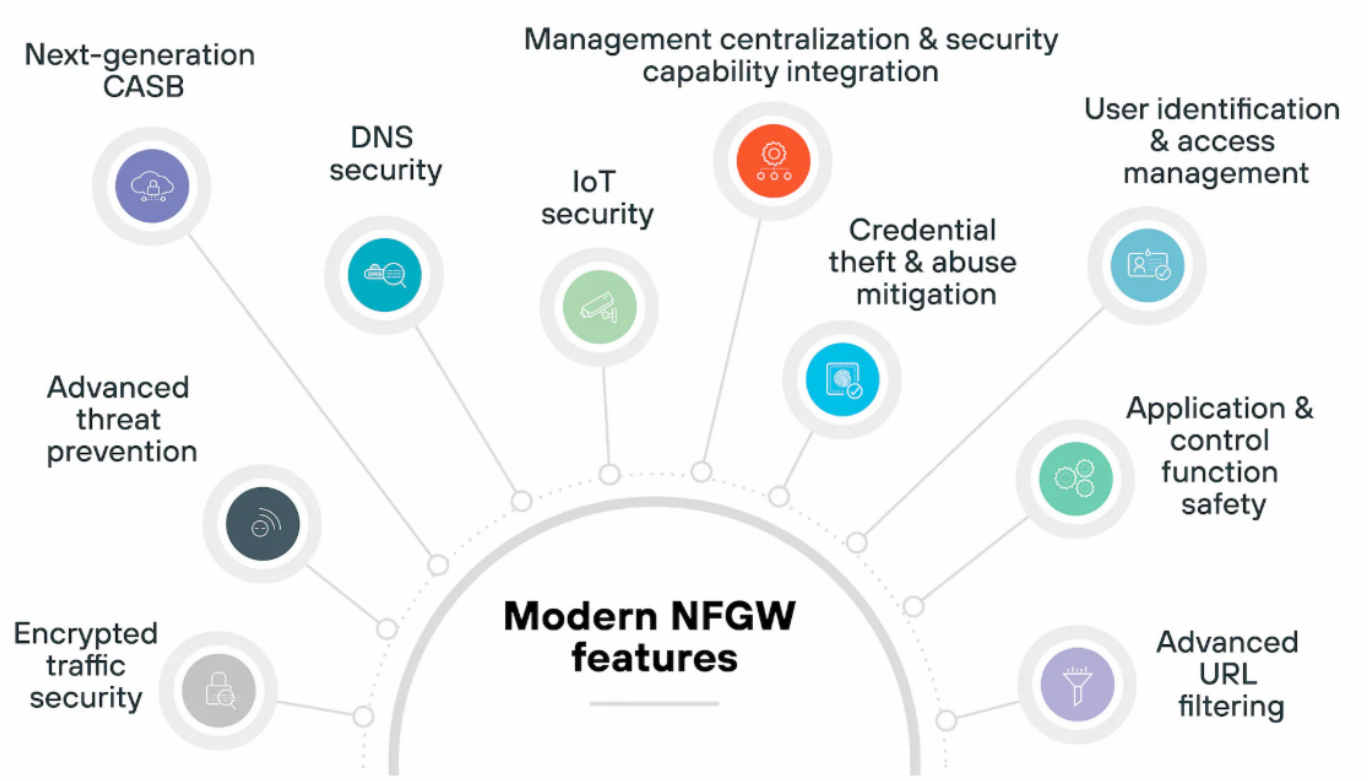


Рис 3.2 - Архітектура багаторівневого захисту NGFW

Критичний елемент багаторівневої моделі – інтеграція NGFW з системами ідентифікації та управління пристроями. Проєктування політик має спиратися не просто на IP-адресу, а на user- та device-context: NGFW підключається до Active

Directory/LDAP, IdP (Azure AD, Okta), MDM/EDR (Intune, Jamf, CrowdStrike, тощо) та отримує інформацію про те, хто залогінився, з якого пристрою, з яким posture (антивірус, шифрування диску, статус патчів). У політиках це дозволяє реалізувати підхід: «користувачі групи Finance із корпоративних ноутбуків з “healthy” станом – повний доступ до фінансових систем; ті ж користувачі з BYOD чи несертифікованих пристроїв – тільки через веб-портал із додатковою перевіркою або взагалі блокування». Така модель формує внутрішній «м’який периметр» навколо критичних додатків, навіть якщо користувач логічно знаходиться «усередині мережі».

Наступний шар – мікросегментація внутрішніх сегментів за допомогою віртуальних фаєрволів або зонований підхід «east–west». Тут NGFW може виконувати роль центрального шлюзу для трафіку між VLAN у дата-центрі: наприклад, окремі VLAN для «App», «DB», «Web», «Mgmt», «Backup», «OT» тощо. Політики задають, що «Web-сервери можуть звертатись лише до певних портів на DB-серверах», «App-сервіси – тільки до API-шлюзів», «Workstations – ніколи не мають прямого доступу до баз даних». Це суттєво ускладнює lateral movement для зловмисника: компрометація однієї машини не дає автоматичного доступу до всієї мережі – кожен стрибок упирається в NGFW, який бачить застосунок, користувача і тип трафіку.

Обов’язковою складовою моделі є рівень захисту DNS і веб-доступу. На NGFW вмикаються модулі DNS Security/URL Filtering із політиками, що блокують фішингові домени, DGA, категорії «Malware, Phishing, Newly Registered Domains», потенційно небезпечні категорії (unknown, dynamic DNS), а також небажані категорії відповідно до політики організації (ігри, порнографія, тощо). Це створює додатковий захисний «екран» над усіма з’єднаннями – навіть якщо payload ще не визнаний шкідливим, сам факт звернення до підозрілих доменів може бути заблокований або відмічений для подальшого розслідування.

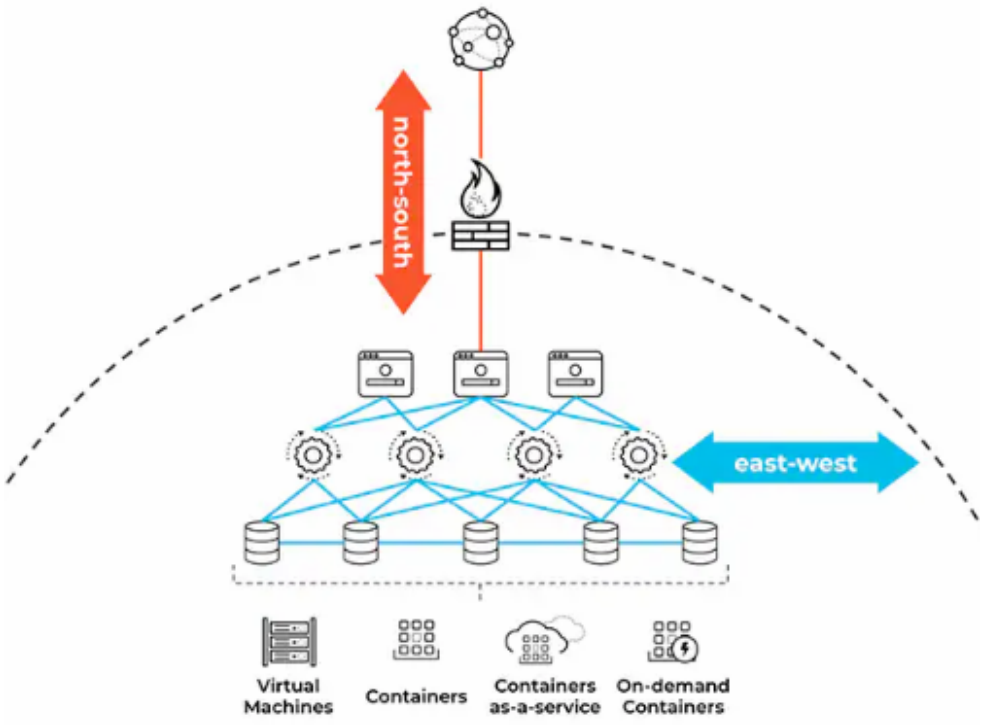


Рис 3.3 - Контроль трафіку North–South та East–West

Окремий рівень – DLP та контроль вихідного трафіку. У багаторівневій моделі NGFW розглядається не лише як бар'єр для вхідних атак, але й як бар'єр проти витоку інформації. DLP-політики дозволяють аналізувати HTTP/HTTPS, SMTP, FTP/SFTP, деякі хмарні сервіси на предмет передавання файлів певних типів або структури даних (номери карт, IBAN, ПІБ+ІПН, службові маркери документів). Далі на рівні політики задається: блокувати, ставити на карантин, логувати, маскувати, вимагати підтвердження. У поєднанні з IPS та DNS Security це формує замкнену схему: навіть якщо зловмиснику вдалося зібрати дані, їхня передача назовні ускладнюється або блокується.

Проєктування багаторівневого захисту також включає модуль захисту від DoS/DDoS та аномалій трафіку. Частина NGFW має вбудовані механізми захисту L3/L4 (syn-flood, udp-flood, malformed packets), rate limiting, connection limiting. У складніших сценаріях NGFW працює спільно з спеціалізованими DDoS-аплайнсами чи хмарними сервісами, але все одно виконує роль «точки політики», де для конкретних ресурсів виставляються пороги, whitelist/blacklist, гео-обмеження,

підписані upstream-провайдером анонси mitigation. Цей рівень захисту важливий, щоб не допустити «засмічення» інфраструктури й збереження доступності критичних сервісів.

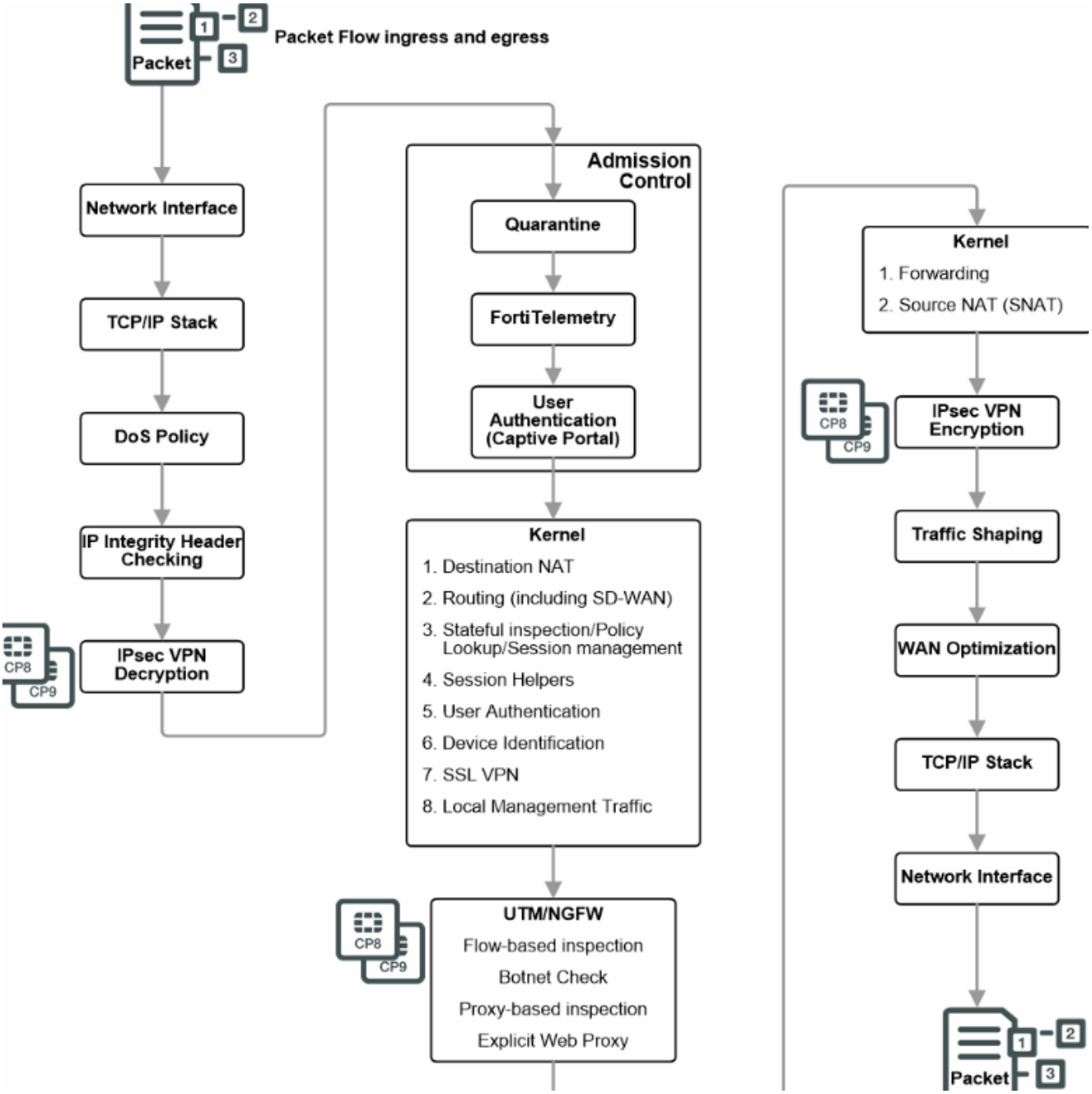


Рис 3.4 - Повний цикл обробки трафіку NGFW

Невід’ємний компонент архітектури – централізоване керування й моніторинг. У багаторівневій моделі NGFW не може існувати як «чорний ящик». Необхідна консоль керування (Panorama, FortiManager, SmartConsole тощо) із чіткою

ієрархією політик (Global, Template, Device), ролями адміністраторів, веденням історії змін (audit trail), підтримкою staged changes (commit/preview), механізмами перевірки конфігурації (policy optimizer, unused rules, shadowed rules). Усі журнали трафіку, загроз, подій системи передаються в SIEM, де будуються кореляційні правила і дашборди: «Top blocked applications», «Threats by zone», «Encrypted traffic without decryption», «DLP violations by department», «Латеральні спроби підключень до DB-сегменту». Це перетворює NGFW із просто «фільтра» на повноцінне джерело телеметрії для SOC.

У контексті віддалених філій і гібридних користувачів багаторівневий захист периметру доповнюється технологіями SD-WAN та «branch NGFW» / cloud-delivered firewall. Частина виробників дозволяє будувати «розподілений периметр»: у головному ЦОД – центральний NGFW з повним набором функцій, на філіях – компактні NGFW-аплайнси або віртуальні інстанси, які підключаються до центрального управління й отримують ту саму політику. Віддалені користувачі можуть використовувати агент (GlobalProtect, FortiClient тощо), який тунелює трафік на NGFW, де він проходить через увесь той самий багаторівневий пайплайн (App-ID, User-ID, SSL-inspection, IPS, URL/DNS, DLP), незалежно від того, де фізично знаходиться користувач. Таким чином периметр логічно «пересувається» за користувачем.

Важливою частиною проєктування є процеси управління політиками: створення базової матриці доступу (zone-to-zone matrix), її прив’язка до бізнес-процесів, періодичний review правил (rule recertification), виявлення застарілих/невикористаних політик, моделювання змін (what-if), використання об’єктів і груп замість «розсипу» окремих IP. NGFW зазвичай надає засоби аналізу політик: які правила ніколи не спрацьовують, які перетинаються, які є надто широкими («allow any application to Internet»). В рамках багаторівневої моделі ці інструменти треба систематично використовувати, щоб модель не «захаращувалася» й не деградувала до хаотичного набору ACL.

На завершення, багаторівнева технологія захисту периметру на основі NGFW – це не просто «розмістити фаєрвол на кордоні з Інтернетом», а розгорнути цілісну систему: зоновану топологію, мікросегментацію, identity- та application-aware політики, глибоку інспекцію й декрипцію, інтеграцію з DNS/URL/DLP/IPS, централізоване керування й телеметрію в SIEM, підтримку віддалених користувачів і філій, процеси аналізу й оптимізації політик. Лише в такій конфігурації NGFW реалізує свій потенціал як «інтелектуальний периметр» організації і дійсно забезпечує стійкість до сучасних багатовекторних атак, які класичний одношаровий периметр уже не здатен адекватно відбивати.

3.2. Реалізація політик доступу та фільтрації трафіку в NGFW

Реалізація політик доступу в міжмережевих екранах нового покоління (NGFW) визначає, наскільки теоретична модель багаторівневого захисту периметру реально працює в мережі. Якщо попередні розділи описують, *що* саме потрібно захищати та *які* загрози існують, то політики NGFW — це безпосередньо той рівень, де вимоги безпеки перетворюються на конкретні правила match/allow/deny, прив’язані до користувачів, застосунків, зон, сервісів, типів контенту та рівнів ризику.

Для конкретизації можна орієнтуватися на типову реалізацію на базі Palo Alto Networks NGFW (PAN-OS) або аналогічних рішень Fortinet FortiGate, Check Point Quantum тощо, оскільки їхня логіка політик подібна за принципами: zone-based firewall + App-ID + User-ID + Content-ID + Threat-ID + URL/DLP/SSL inspection [18; 19].

Базова структура політик фільтрації в NGFW ґрунтується на ієрархії об’єктів: мережеві зони (trust / untrust / DMZ / VPN / guest), групи адрес (address objects / address groups), сервіси (service objects — TCP/UDP з портами, або application-

default), користувачі та групи (User-ID, інтегровані з AD/LDAP/IdP), застосунки (App-ID), профілі безпеки (antivirus, anti-spyware, vulnerability, URL filtering, file blocking, WildFire/sandbox, DLP), а також профілі логування (log forwarding profile) для інтеграції з SIEM. Кожне правило політики, по суті, є композицією цих об'єктів плюс дій (allow / deny / drop / reset) і опцій (log at session start/end, QoS, NAT, security profile group тощо) [18].

Практична реалізація зазвичай починається з побудови чіткої зональної моделі: наприклад, *Untrust* (інтернет), *Corp-LAN*, *Server-LAN*, *DMZ*, *VPN-Remote*, *Guest*, *OT/ICS*. Для кожної пари «джерело → призначення» визначається допустимий тип взаємодії. Класична помилка традиційних фаєрволів — надто загальні правила виду «Corp-LAN → Internet: allow any». У NGFW цю логіку необхідно замінити app-centric підходом: «Corp-LAN → Internet: allow only web-browsing, ssl, office365-apps, update-services, заборонити unknown-tcp/udp, тунельні та проксі-застосунки, P2P, Remote-Access-клієнти, несанкціоновані месенджери». Для цього NGFW використовує App-ID, який аналізує не лише порти, а й сигнатури, TLS-fingerprint, послідовність пакетів, щоб визначити конкретний застосунок, навіть якщо він «маскується» під HTTPS [19].

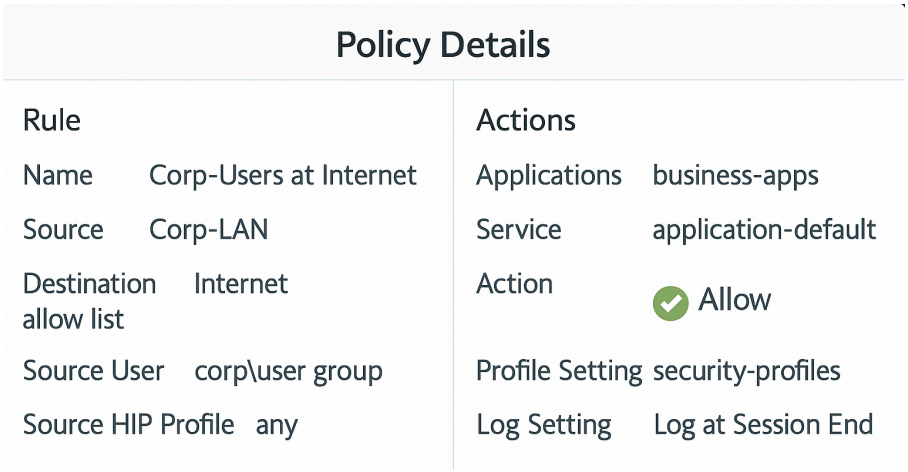


Рис 3.5 — Політики для копоративних користувачів

Реалізація політик доступу в NGFW логічно ділиться на кілька шарів. Перший шар — базові зони доступу та політики «жорсткого» периметру: заборона

будь-якого трафіку з Untrust до Corp/Server-LAN, окрім явно дозволених сервісів, опублікованих через DNAT/Reverse Proxy (веб-сервери, VPN-шлюзи, опубліковані API). На цьому рівні політика зазвичай виглядає як «deny all» із невеликою кількістю винятків, причому кожен виняток проходить через профілі IPS/Antivirus/Anti-Spyware. Другий шар — контроль вихідного трафіку користувачів: замість глобального allow-any застосовується матриця політик, де для різних груп AD (наприклад *Standard Users*, *Developers*, *Finance*, *Management*) дозволяється різний набір застосунків і веб-категорій. Наприклад, для бухгалтерії блокуються категорії «Gambling», «Adult», «Unknown», «Newly Registered Domains», а для розробників дозволяються Git-сервіси, Dev-Tools, але блокується P2P та несанкціоновані VPN/Proxy-сервіси. NGFW при цьому використовує зв'язку User-ID (ідентифікація користувачів через AD/SSO) + URL Filtering + App-ID [18].

Security Policies

Name	Source Zone	Destination Zone	User	Application	Service	Action	Profile Group	Log at Session End
Corp-Users → Internet	Corp-LAN	Internet	corp\user group	business-apps	applicat-default	allow	security-profiles	✓
Block Unknown TCP	Corp-LAN	Internet	any	unknown-tcp	any	deny	default	✓
Deny Untrust at Corp-LAN	Untrust	Corp-LAN	CorpLAN	any	any	deny	none	✓
Deny Untrust at Server	Untrust	Server-LAN	Server-LAN	any	any	deny	none	✓
Deny Untrust at Server	any	Server	Server-LAN	any	any	deny	none	✓

Рис 3.6 — Політики безпеки організації

Третій шар — політики для серверних сегментів і сховищ даних. Тут NGFW вмикає не лише контроль застосунків, але й сувору мережеву мікросегментацію: замість «Server-LAN: any→any» вводяться правила «Web-servers → App-servers» (лише HTTP/HTTPS з конкретних підмереж), «App-servers → DB-servers» (лише TCP 1433/3306/1521 тощо), «Admin-subnet → Management-interfaces» (лише SSH/RDP/VNC із jump-host, з MFA і логуванням). При цьому на ці потоки також накладається IPS/Anti-Spyware, щоб виявляти lateral movement, експлуатацію вразливостей сервісів Docker/Kubernetes, RDP, SMB, RPC. У деяких NGFW (наприклад Palo Alto) можливе використання зональної сегментації й на рівні «logical tenants» або VSYS, що дозволяє реалізувати поділ середовищ (prod / dev / test) з окремими політиками й журналами [19].

Важливий аспект реалізації політик — SSL/TLS-декрипція. Без неї більшість профілів безпеки працюють лише поверх метаданих, а не реального контенту. Типова схема: у NGFW створюється Decryption Policy, яка визначає, який трафік підлягає розшифруванню, а який обминає інспекцію (no-decrypt). У практиці це виглядає як набір правил: «Decrypt outbound corporate web traffic, exclude financial/banking, healthcare, government sites, OS-update domains». Декрипція вмикається у тандемі з профілями Threat Prevention, URL Filtering, File Blocking та WildFire (sandbox), що дозволяє NGFW виявляти шкідливі документи, скрипти, експлойти, C2-сесії всередині HTTPS-каналів. При цьому доцільно розділяти політики для корпоративних пристроїв (де можна довіряти корпоративному сертифікату CA) і BYOD/гостьових пристроїв (де декрипція або обмежена, або взагалі недоступна — тоді їх варто ізолювати в окремій зоні з додатковими обмеженнями) [18].

Реалізація політик фільтрації трафіку у NGFW дуже тісно пов’язана з контентною фільтрацією та DLP. Наприклад, для вихідного трафіку із сегмента *Finance* можна створити політику: «Allow web-browsing/ssl → Apply URL Filter profile *Finance-Strict* → Apply DLP Profile *PCI-Data* → Block file uploads of types *.xls, *.csv, *.zip to personal cloud storage (Dropbox, Google Drive personal,

WeTransfer)». Це реалізується через поєднання App-ID (розпізнавання конкретних хмарних сховищ), URL-категорій (персональні storage-сервіси), контролю HTTP-методів (POST/PUT) та DLP-шаблонів (PCI-карти, IBAN, національні ідентифікатори). У результаті NGFW блокує ексфільтрацію, формує лог із деталями (хто, коли, куди, який тип файлу/даних) та надсилає подію в SIEM для подальшого розслідування.

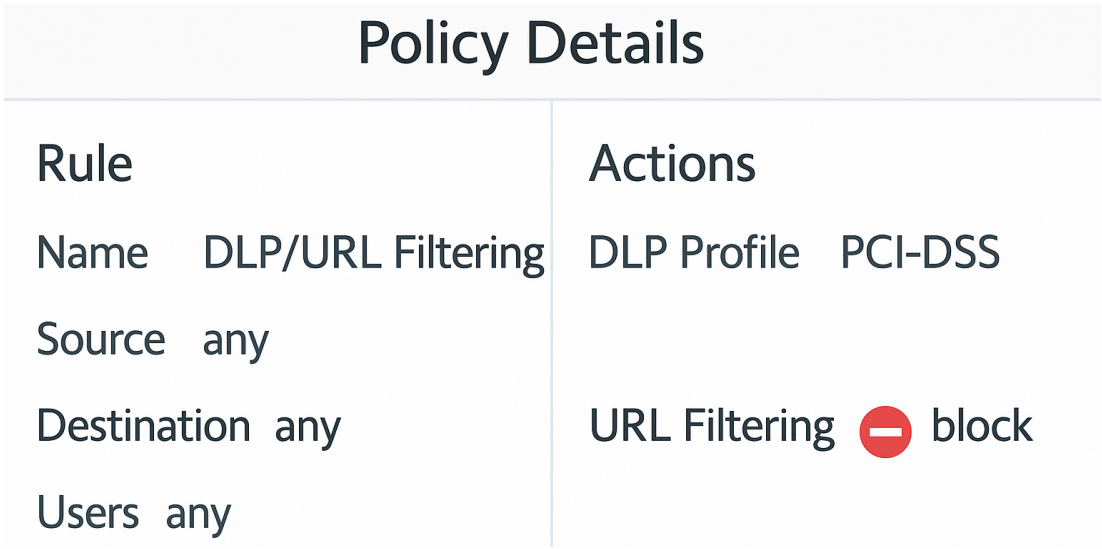


Рис 3.7 — Приклад реалізації політики DLP в NGFW

Особливу увагу треба приділити реалізації політик для віддаленого доступу (VPN/SD-WAN). У сучасних архітектурах NGFW часто виступає VPN-шлюзом (IPSec/SSL VPN) або SD-WAN-CPE. Тут важливо, щоб VPN не «пробивав» периметр напряму, а був інтегрований у загальний policy-stack. Тобто VPN-зона (*VPN-Users*) — це окрема trust-зона з власними політиками: «VPN-Users → Corp-LAN: allow тільки необхідні застосунки (RDP до конкретних серверів, SSH на jump-host, HTTPS до Intranet), всі інші — deny + log». Для цього NGFW знову ж таки використовує User-ID (автентифікація через LDAP/RADIUS/IdP, MFA), Device Posture (перевірка стану клієнта: антивірус, шифрування диска, версії ОС) та App-ID. У результаті, навіть якщо облікові дані VPN скомпрометовано, атакувальник отримує значно звужений обсяг доступу, а всі його дії ретельно логуються й аналізуються [19].

Технічно важливим аспектом є «порядок правил» (rule order) і пріоритети. NGFW обробляє політики зверху вниз, тому спочатку доцільно розміщувати більш

специфічні правила (наприклад, для критичних сервісів, керуючих сегментів, адміністраторів), а нижче — ширші політики для звичайних користувачів та загальних сценаріїв. Типовою практикою є наявність у самому низу явного «deny all» (або implicit deny з увімкненим логуванням), щоб жоден непередбачений трафік не покидав мережу без контролю. Для полегшення експлуатації зазвичай створюють кілька rulebase-груп: *Global rules* (застосовуються до всіх зон), *Datacenter rules*, *Branch rules* тощо.

Реалізація політик доступу повинна супроводжуватись профілями логування та інтеграцією з SIEM. У NGFW налаштовуються log forwarding profiles, які визначають, які типи логів (traffic, threat, URL, data, system, config) надсилати в зовнішню систему. Для критичних політик варто включити логування обох подій — як дозволених, так і заблокованих сесій, принаймні на етапі запуску, щоб детальнобачити реальний трафік. Надалі, після етапу «tuning», можна оптимізувати обсяги логів, залишивши повну деталізацію для high-risk-категорій (unknown apps, suspicious categories, failed decryption, threat events).

NGFW Logs

Time	Source	Destination	Policy	Action
4024 08.04	192.168 0.10	hr.example.com	Access Control	allow
192.168.10	192 168.0 15	malicious.com	Threat Prevention	deny
192.168.15	malicious com	threat preventio	Access Control	allow
4034 03.03	8.8.8.8	8.8.8.8	Access Control	allow

Рис 3.8 — Реалізація журналу подій NGFW

Особливий клас політик NGFW — це політики NAT (Source NAT / Destination NAT / U-Turn NAT). Хоча формально вони стосуються адресації, а не безпеки, NET-

рівень тут важливий через вплив на visibility і коректність логування. Наприклад, при Source NAT (маскарадинг) NGFW повинен все одно логувати оригінальні адреси/користувачів, щоб зберігати можливість атрибуції. При Destination NAT (публікація внутрішніх сервісів) політики безпеки мають використовувати *оригінальні* (pre-NAT) адреси, щоб уникнути помилок і дозволити гнучку мікросегментацію. Сучасні NGFW дають можливість окремо логувати pre-NAT і post-NAT адреси, інтегрувати ці дані з SIEM та системами forensics [18].

З практичної точки зору впровадження політик NGFW доцільно вести поетапно. Спочатку — перехід у режим «monitor» для певних політик (наприклад, блокування *unknown-tcp/udp* або декрипції HTTPS): NGFW не блокує трафік, а тільки логує події, що дозволяє зібрати статистику та уникнути різких збоїв. Після аналізу логів і корекції винятків (whitelist для бізнес-критичних застосунків, винятки для легітимних тунельних сервісів тощо) політики переводяться в «enforce» (block/reset). Аналогічний підхід використовується для DLP — спочатку режим «alert only», потім — часткове блокування, і лише після стабілізації — суворе блокування для чутливих категорій даних.

У підсумку, реалізація політик доступу та фільтрації трафіку у NGFW — це комплексна інженерна задача, яка включає побудову зональної моделі, app-centric контроль, контентну та DLP-інспекцію, SSL-декрипцію, управління віддаленим доступом, логування й інтеграцію з SIEM/SOAR. На відміну від класичних фаєрволів, NGFW дозволяє описувати політики мовою бізнес-контексту (користувач, застосунок, тип даних, ризик), а не лише IP/портами, що суттєво підвищує точність і ефективність захисту мережевого периметру [18; 19].

3.3 Експериментальна оцінка ефективності запропонованої технології

Експериментальна перевірка ефективності запропонованої технології захисту мережевого периметру на основі NGFW має показати не лише «лабораторну» працездатність, а й реальний приріст безпеки у порівнянні з класичною моделлю фаєрвола. Логіка оцінювання будується як послідовний ланцюг: від якості контролю трафіку й видимості (які саме потоки бачить і класифікує NGFW) – до здатності виявляти та блокувати реальні атаки – і, врешті, до впливу на швидкість реагування та навантаження на команду безпеки. Ключова ідея – порівняти стан «до» і «після»: класичний L3/L4-фаєрвол проти повноцінного NGFW з увімкненими сервісами App-ID, User-ID, IPS, SSL-інспекцією, URL/DNS-фільтрацією та базовим DLP.

Початком експерименту стало формальне описання обсягу й умов. Лабораторний стенд відтворював типову корпоративну мережу з трьома логічними зонами: зовнішня мережа (Internet), DMZ (веб-сервер, поштовий шлюз, VPN-шлюз, тестовий публічний API) та внутрішня мережа (контролер домену, файловий сервер, сервер БД, кілька користувацьких робочих станцій). На периметрі між Internet і DMZ/внутрішньою мережею встановлено один NGFW з пропускною здатністю, достатньою для лабораторного навантаження, віртуальний або апаратний – це не принципово, важливо, що він підтримує повний стек функцій нового покоління. У початковій фазі NGFW конфігурувався як «класичний фаєрвол»: прості ACL за IP/портами, базовий стейтфул-аналіз, журнали L3/L4-подій. Далі для тієї ж топології вмикався повний NGFW-режим: політики на основі застосунків та користувачів, IPS-профілі, SSL-декрипція, URL/DNS-фільтрація, профілі Threat Prevention, DLP-контроль вихідного трафіку.

Умовно, експеримент складався з двох періодів однакової тривалості (наприклад, по 2 тижні): «До» (режим classical firewall) і «Після» (режим NGFW). У кожному періоді генерувався як легітимний бізнес-трафік (перегляд веб-ресурсів, робота з умовним CRM, пошта, доступ до файлів), так і керовані атаки. Для останніх використовувалися nmap/hping3 (ревізія периметру, скани портів), sqlmap та Metasploit (експлуатація веб-вразливостей), інструменти брутфорсу до VPN/SSH,

імітатори шифрувальників і скрипти ексфільтрації даних через HTTPS і DNS. Окремо проганялись сценарії зловживання легальними сервісами – несанкціоновані хмарні сховища, мессенджери, «домашні» VPN-клієнти, які класичний фаєрвол сприймає як звичайний HTTPS-трафік.

Таблиця 3.1.

Параметри експерименту з оцінки технології NGFW

Параметр	Значення
Тривалість етапу «До»	14 діб, режим classical firewall (L3/L4)
Тривалість етапу «Після»	14 діб, режим NGFW (App-ID, User-ID, IPS, SSL, DLP)
Зони мережі	Internet, DMZ, Internal
Кількість вузлів у DMZ	3 (web, mail, VPN/API)
Кількість внутрішніх вузлів	5 (AD/DC, DB, File server, 2 робочі станції)
Типи трафіку	Web/HTTPS, SMTP, DNS, SMB, VPN, API
Сценарії атак	Recon/scan, exploit, malware/C2, exfiltration, shadow IT

Перший пласт оцінювання – якість контролю та спостережності периметра. У режимі classical firewall журнали включали лише базові відомості: IP-адреси джерела/призначення, порти, протокол, обсяг переданих даних, факт дозволу/блокування. Для вимірювання «видимості» застосунків та користувачів бралися такі показники: частка трафіку, класифікованого як конкретні застосунки (CRM, Office 365, хмарні сховища тощо), кількість неідентифікованих потоків (generic SSL/unknown-tcp), наявність прив’язки до облікових записів (User-ID) і точність сегментації зон. У режимі NGFW, завдяки увімкненню App-ID та User-ID, більшість HTTPS-потоків отримали семантичні мітки – замість «tcp/443» у звітах з’явилися «Office365-SharePoint», «Corporate-CRM-Web», «Unsanctioned-Cloud-

Storage», «Encrypted-Messenger» тощо. Паралельно через інтеграцію з AD була реалізована прив’язка трафіку до конкретного користувача й групи. У підсумку співвідношення «невідомий/класифікований» трафік суттєво зменшилось, а у SOC з’явилася можливість аналізувати активність не лише за IP-адресами, а й за бізнес-ролями.

Другий пласт – ефективність виявлення та блокування загроз. Для кожного сценарію атак фіксувалися: кількість спроб, кількість успішних блокувань на периметрі, кількість інцидентів, що «прорвалися» всередину (довелося ловити на хості або на рівні застосунку), наявність контексту в журналі (тип атаки, сигнатура/техніка, URL, користувач) і час від початку атаки до спрацювання. У базовому режимі port-scan’и хоч і блокувались із боку закритих портів, але не формували жодних інцидентів – SOC бачив лише фрагментарні deny-entries. У режимі NGFW IPS-профілі розпізнавали патерни сканування (SYN sweep, stealth-scan, HTTP fuzzing) і породжували події «Reconnaissance» із деталями джерела й цілі, що дозволяло побачити розвідку задовго до експлуатації.

Для веб-експлойтів (SQL-ін’єкції, brute-force логінів, спроби RCE) різниця була ще помітнішою. Класичний фаєрвол дозволяв весь HTTPS-трафік на 443 порт, а виявлення помилок та підозрілих запитів перекладалося на веб-сервер або WAF (якщо він був). У NGFW-режимі HTTP/HTTPS-потоки аналізувалися на рівні додатку: сигнатурно виявлялися типові шаблони SQLi/XSS, а поведінкові профілі фіксували нетипову частоту запитів, підбір параметрів, атаки на сторінки логіна. Частина запитів блокувалася без потрапляння в бекенд, а кожна серія спроб з одного джерела формувала агрегований інцидент «Web attack campaign», що значно спрощувало реагування.

Окремо перевірялися сценарії шкідливого ПЗ та C2-комунікацій. У режимі classical firewall завантаження умовного «підозрілого» файлу з мало відомого домену чи зв’язок клієнта з випадковими доменами через HTTPS виглядали абсолютно легітимно. Після увімкнення SSL-інспекції та Threat Prevention файли автоматично

відправлялися в sandbox: у випадку імітації шифрувальника NGFW отримував verdict «malicious», блокував передачу у відповідь, заносив хеш у локальний кеш і (за потреби) у хмару загроз, а з'єднання з C2-доменами припиняв ще на етапі DNS-запиту або TLS-рукостискання. У журнали при цьому потрапляли всі технічні деталі: ім'я користувача, домен, хеш файлу, сигнатура/категорія загрози, що формувало повноцінну доказову базу для SOC.

Для оцінки ефективності ексфільтрації даних моделювалися спроби масового копіювання файлів з файлового сервера, їх архівації та відправлення в зовнішнє хмарне сховище або через «обхідний» HTTPS-ресурс. У класичній конфігурації все, що проходило через порт 443 й не співпадало з явними deny-ACL, пропускалося, а в логах залишався лише розмір трафіку. У NGFW-режимі App-ID і DLP-профілі дозволили: а) впізнати несанкціонований cloud-storage; б) виявити у вихідному HTTP/HTTPS-потоці файли/фрагменти даних, що відповідають визначеним шаблонам (умовні номери договорів, карток, службові маркери «Confidential»); в) заблокувати передачу й сформувати високопріоритетний інцидент «Data exfiltration attempt». Додатково DNS-security виявляла нетипову інтенсивність і ентропію DNS-запитів (імітація тунелювання даних через DNS), що практично неможливо реалізувати на класичному фаєрволі без спеціалізованого аналізу.

Щоб зробити порівняння формалізованим, результати зведено у таблицю з основними метриками «до/після». Значення можуть бути подані як усереднені за весь період спостереження.

Таблиця 3.2.

Ключові результати експериментальної оцінки технології NGFW

Метрика	Було	Стало	Коментар
Частка класифікованого трафіку за додатками	~25 %	~85 %	Завдяки App-ID
Трафік типу «unknown /	Високий	Значно знижений	Більшість

generic SSL»			сервісів ідентифіковано
Виявлені/заблоковані web-атаки	Низько/частково	Високо/майже повністю	IPS + L7-аналіз
Виявлення C2-комунікацій	Епізодично	Систематично	DNS-security + Threat Intelligence
Виявлення спроб ексфільтрації	Майже відсутнє	Високе (HTTPS/DNS)	DLP + App-ID + DNS-аналіз
MTTD (усереднено)	Десятки хвилин/годин	Хвилини	Автоматичні профілі загроз
MTTR на рівні периметру	Години	Хвилини–десятки хвилин	Завдяки автоматичним діям політик
Обсяг журналів без структурованого контексту	Високий	Знижений	Логи стали більш «щільними» по суті

Третій пласт оцінки – операційна дієвість: наскільки впроваджена технологія допомагає команді безпеки, а не просто «генерує нові логи». Для цього аналізувались журнали NGFW і, за наявності, дані SIEM: кількість інцидентів, що формуються автоматично на основі NGFW-подій, частка інцидентів, для яких периметр уже виконав необхідну дію (block/reset/drop) без додаткових ручних втручань, середній час від початку атаки до її блокування, а також кількість хибних спрацьовувань, що вимагали перегляду політик. На початковому етапі включення всіх профілів IPS/URL/DLP «на максимум» дійсно призводило до великої кількості алертів,

частина з яких виявлялася легітимними нестандартними бізнес-сценаріями. Після етапу тюнінгу (додавання винятків для внутрішніх сервісів, зниження чутливості для «шумних» сигнатур, сегментації користувачів і застосунків) вдалось досягти балансу: більшість інцидентів високого пріоритету були або справжніми атаками, або реально ризиковими діями, а «шум» впав до прийнятного для SOC рівня.

Окремо відзначається вплив на користувачів і продуктивність. У рамках експерименту вимірювалися затримки для ключових бізнес-сервісів при увімкненій SSL-інспекції, а також кількість скарг від користувачів (умовно – фіксація інцидентів «заблоковано легітимний ресурс»). Повний режим декрипції, очікувано, підвищував латентність і навантаження на NGFW, однак після впровадження селективної інспекції (white-list для банківських/державних/особливо чутливих сервісів, оптимізація шифральних наборів, балансування профілів) вдалося знизити затримку до рівня, що користувач практично не відчував. Кількість випадків «надмірного блокування» в ході експерименту залишалася незначною і розв’язувалась коригуванням політик.

У підсумку експериментальна частина показала, що технологія захисту мережевого периметру на основі NGFW дає комплексний, підтверджений цифрами ефект: суттєво підвищується видимість трафіку та поведінки користувачів на периметрі, зростає частка вчасно виявлених і заблокованих атак (особливо тих, що використовують HTTPS і легальні сервіси), скорочуються MTTD/MTTR на рівні периметру, а журнали NGFW стають повноцінним джерелом інцидентів для SIEM/SOAR. При цьому, за умови грамотного тюнінгу політик і селективної SSL-інспекції, вплив на користувацький досвід і продуктивність інфраструктури залишається контрольованим. Це дозволяє рекомендувати розроблену технологію як практичну основу для побудови багаторівневого периметрового захисту в корпоративних і гібридних мережах.

ВИСНОВКИ

У роботі проведено дослідження шляхів та аналіз загроз, пов’язаних із забезпеченням захисту мережевого периметру корпоративних IT-систем. Проаналізовано роль та місце периметрової оборони у сучасних інформаційних інфраструктурах, а також ризики, що виникають при використанні традиційних міжмережевих екранів, які базуються на статичних правилах фільтрації пакетів. Було розглянуто проблеми, пов’язані з багатоступеневими атаками, використанням зашифрованого трафіку, експлуатацією вразливостей у мережевому обладнанні та несанкціонованим доступом до корпоративних ресурсів. Наведено приклади та статистичні дані, що підтверджують актуальність проблеми захисту периметру в умовах сучасних кіберзагроз.

Досліджено сучасні підходи до побудови багаторівневого захисту, зокрема роль міжмережевих екранів нового покоління (NGFW) у формуванні комплексної системи кібербезпеки. Проведено порівняння класичних рішень із NGFW, визначено їхні функціональні можливості та переваги, серед яких глибока інспекція пакетів (DPI), аналіз трафіку на рівні додатків, SSL/TLS-інспекція, інтеграція з IDS/IPS, SIEM та SOAR. Більш детально було проаналізовано архітектуру NGFW, їхню здатність забезпечувати контекстний контроль доступу та формувати політики безпеки відповідно до специфіки бізнес-процесів.

Особливу увагу приділено порядку впровадження NGFW у корпоративному середовищі, включаючи сегментацію мережі, створення профілів безпеки для різних сегментів, налаштування політик доступу та фільтрації трафіку, а також інтеграцію з централізованими системами моніторингу й автоматизованого реагування. У ході експериментального дослідження було змодельовано роботу NGFW та протестовано основні функції: глибоку інспекцію трафіку, блокування небажаних додатків, аналіз зашифрованих потоків, формування кореляційних правил у SIEM та запуск

автоматизованих сценаріїв SOAR. Це дозволило підтвердити ефективність NGFW у забезпеченні захисту мережевого периметру навіть у високонавантажених середовищах.

Окрім технічних аспектів, було розроблено рекомендації щодо організації багаторівневого захисту корпоративних мереж. Вони включають як програмні заходи (використання NGFW у поєднанні з SIEM та SOAR, застосування багатофакторної автентифікації, постійний моніторинг активності), так і організаційні (підвищення обізнаності співробітників, розробка політик безпеки для адміністраторів, регулярне тестування системи на стійкість до атак).

У результаті дослідження було встановлено, що застосування міжмережевих екранів нового покоління дозволяє значно підвищити рівень кіберзахисту організації, оперативно виявляти та локалізовувати інциденти, а також забезпечувати захист корпоративних ресурсів від сучасних загроз. Розглянуті методи та рекомендації щодо впровадження допоможуть побудувати ефективну систему периметрової безпеки, яка відповідатиме сучасним викликам і міжнародним стандартам інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Palo Alto Networks. What Is a Network Security Perimeter? Palo Alto Networks, 2024. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-a-network-security-perimeter (дата звернення: 10.10.2025)

2. Scarfone, K., Hoffman, P. Guidelines on Firewalls and Firewall Policy (NIST SP 800-41 Rev.1). National Institute of Standards and Technology, 2009. URL: https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final (дата звернення: 10.10.2025)

3. Cisco. Network Security and Perimeter Defense: Cisco Secure Firewall Overview. Cisco Systems, 2024. URL: https://www.cisco.com/site/us/en/products/security/firewalls (дата звернення: 10.10.2025).

4. De-perimeterisation. In: Wikipedia. The Free Encyclopedia, 2025. URL: https://en.wikipedia.org/wiki/De-perimeterisation (дата звернення: 10.10.2025).

5. Microsoft. Zero Trust: A Strategic Approach to Security in the Modern Enterprise. Microsoft Corporation, 2023. URL: https://learn.microsoft.com/en-us/security/zero-trust (дата звернення: 10.10.2025).

6. OWASP. OWASP Testing Guide v.5. OWASP Foundation, 2024. URL: https://owasp.org/www-project-web-security-testing-guide/ (дата звернення: 11.10.2025).

7. Mandiant. M-Trends 2024 Report: Global Threat Intelligence. Mandiant, 2024. URL: https://www.mandiant.com/resources (дата звернення: 11.10.2025).

8. Cloudflare. DDoS Threat Report 2024. Cloudflare, Inc., 2024. URL: https://www.cloudflare.com/ddos (дата звернення: 11.10.2025).

9. Palo Alto Networks. Decrypting SSL/TLS Traffic: Best Practices (2024). URL: https://www.paloaltonetworks.com (дата звернення: 11.10.2025).

10. Gartner. Magic Quadrant for Network Firewalls 2024. Gartner Research, 2024. URL: https://www.gartner.com/en/documents (дата звернення: 11.10.2025).

11. Cisco. *Firewall Evolution: From Packet Filtering to Next-Generation Security*. Cisco Systems, 2024. URL: https://www.cisco.com/ (дата звернення: 18.10.2025).

12. Palo Alto Networks. *Understanding the Limitations of Traditional Firewalls*. Palo Alto Networks, 2023. URL: https://www.paloaltonetworks.com/ (дата звернення: 18.10.2025).

13. Gartner. *The State of Network Security 2025: Why Legacy Perimeters Fail*. Gartner Research, 2025. URL: https://www.gartner.com/ (дата звернення: 18.10.2025).

14. ENISA. *Threat Landscape Report 2024*. European Union Agency for Cybersecurity, 2024. URL: https://www.enisa.europa.eu/ (дата звернення: 18.10.2025).

15. Gartner. *Next-Generation Firewalls: Deep Technical Capabilities and Market Overview*. Gartner Research, 2025. URL: https://www.gartner.com/ (дата звернення: 18.10.2025).

16. Palo Alto Networks. *Inside the Architecture of Next-Generation Firewalls: App-ID, User-ID, Content-ID*. Palo Alto Networks, 2024. URL: https://www.paloaltonetworks.com/ (дата звернення: 18.10.2025).

17. Fortinet. *SSL/TLS Inspection and Encrypted Traffic Analysis in Modern Networks*. Fortinet Technical Report, 2024. URL: https://www.fortinet.com/ (дата звернення: 18.10.2025).

18. Palo Alto Networks. *PAN-OS Administrator's Guide 11.0*. — Santa Clara: Palo Alto Networks, 2024 (дата звернення: 12.11.2025).

19. Fortinet. *FortiOS Handbook — Next Generation Firewall Features*. — Sunnyvale: Fortinet, 2023(дата звернення: 12.11.2025).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ)