

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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

**«Технологія забезпечення безпеки комп'ютерних мереж на основі рішення
CISCO»**

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

Кирило БРИКСА

(підпис)

Виконав: здобувач вищої освіти групи БСДМ-63

БРИКСА Кирило

(прізвище, ім'я)

Керівник

д.ф. СОБЧУК Андрій

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

Рецензент

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

Київ 2026

ЗМІСТ

	Стор.
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	3
ВСТУП.....	4
1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ	6
1.1. Аналіз основних загроз та вразливостей комп'ютерних мереж	6
1.2. Аналіз підходів до забезпечення безпеки комп'ютерних мереж	11
1.3 Аналіз існуючих рішень щодо забезпечення безпеки комп'ютерних мереж	19
2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ РІШЕННЯ CISCO.....	26
2.1. Призначення та основні функції Cisco Secure Firewall.....	26
2.2. Основні компоненти архітектури Cisco Secure Firewall	36
2.3. Інтеграція Cisco Secure Firewall	42
3 ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ РІШЕННЯ CISCO.....	47
3.1. Варіант розгортання Cisco Secure Firewall у корпоративній мережі.....	47
3.2. Налаштування політик безпеки та механізмів контролю трафіку в Cisco Secure Firewall.....	56
3.3. Розробка рекомендацій щодо забезпечення безпеки комп'ютерних мереж	69
ВИСНОВКИ	74
ПЕРЕЛІК ПОСИЛАНЬ	76
ДЕМОНТРАЦІЙНІ МАТЕРІАЛИ (Презентація).....	80

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ACP — Access Control Policy

API — Application Programming Interface

CISA — Cybersecurity and Infrastructure Security Agency

CVE — Common Vulnerabilities and Exposures

DDoS — Distributed Denial of Service

DMZ — Demilitarized Zone

DNS — Domain Name System

ENISA — European Union Agency for Cybersecurity

FMC — Firepower Management Center F

TD — Firepower Threat Defense

HA — High Availability

HTTP — HyperText Transfer Protocol

HTTPS — HyperText Transfer Protocol Secure

IDS — Intrusion Detection System

IPS — Intrusion Prevention System

NAT — Network Address Translation

NGFW — Next-Generation Firewall

SIEM — Security Information and Event Management

SSH — Secure Shell

VPN — Virtual Private Network

XDR — Extended Detection and Response

ВСТУП

Актуальність дослідження. Комп'ютерні мережі сучасних організацій характеризуються розподіленістю інфраструктури, наявністю віддалених філій і користувачів, інтеграцією локальних сегментів із зовнішніми сервісами та зростанням частки шифрованого трафіку. За цих умов мережеві атаки еволюціонують від простих спроб проникнення через периметр до комплексних сценаріїв із використанням уразливостей сервісів, компрометації облікових записів, бічного переміщення між сегментами та прихованої передачі даних. Традиційні периметрові підходи, що спираються на мінімальну сегментацію та фрагментовані засоби захисту, ускладнюють централізований контроль, знижують видимість подій безпеки та підвищують ризик неконтрольованих змін у конфігурації мережі. У зв'язку з цим першочергового значення набуває побудова технології мережевого захисту, яка забезпечує контроль між мережевими зонами, сегментацію, інспекцію трафіку та керовану експлуатацію засобів захисту.

У цьому контексті актуальними є рішення класу NGFW, що поєднують функції мережевого контролю та інспекції трафіку з можливістю централізованого управління конфігурацією і журналюванням подій. Використання Cisco Secure Firewall як основи технології захисту комп'ютерних мереж дає змогу сформувати керований периметр, підвищити рівень ізоляції між сегментами, забезпечити контрольоване внесення змін і підтримати процеси моніторингу та реагування на інциденти. Тому дослідження технології забезпечення безпеки комп'ютерних мереж на основі рішення Cisco є актуальним як у теоретичному, так і в прикладному аспектах.

Об'єкт дослідження – процес забезпечення безпеки комп'ютерних мереж організації.

Предмет дослідження – технологія забезпечення безпеки комп'ютерної мережі організації.

Мета роботи – розробити варіант застосування технології забезпечення безпеки комп'ютерних мереж на основі рішення Cisco.

Наукові завдання:

проаналізувати основні загрози та вразливості комп'ютерних мереж організації, що впливають на порушення конфіденційності, цілісності та доступності;

узагальнити підходи до побудови мережевого периметра та внутрішньої сегментації, визначити їх значення для протидії проникненню та бічному переміщенню;

дослідити функціональні можливості рішень класу NGFW у контексті контролю міжзонової взаємодії, інспекції трафіку та журналювання подій;

проаналізувати архітектуру Cisco Secure Firewall та її компоненти з позиції побудови керованого контуру мережевого захисту;

сформувати варіант розгортання технології мережевого захисту на основі Cisco та розробити практичні рекомендації щодо її впровадження в організаційній інфраструктурі.

Методи дослідження – опрацювання наукової та технічної літератури, аналіз сучасних підходів до побудови мережевого захисту, системний аналіз архітектури мережі та зон безпеки, порівняння варіантів розгортання NGFW і моделей централізованого управління, узагальнення практик моніторингу та журналювання подій.

Практичне значення одержаних результатів: запропоновано варіант застосування технології забезпечення безпеки комп'ютерних мереж на основі рішення Cisco, а також сформовано рекомендації для фахівців з кібербезпеки щодо впровадження периметрового захисту, сегментації та організації керованої експлуатації мережевих засобів захисту.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 29 жовтня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1. Аналіз основних загроз та вразливостей комп'ютерних мереж

Комп'ютерні мережі формують базову інфраструктуру сучасних організацій, оскільки забезпечують транспорт даних і доступ до прикладних сервісів у межах локальних, розподілених та гібридних середовищ. Ускладнення мережевих архітектур, збільшення частки віддаленого доступу та зростання кількості інтеграцій із зовнішніми провайдерами об'єктивно розширюють площу атаки. За таких умов забезпечення належного рівня захищеності потребує системного аналізу загроз і вразливостей, який дозволяє пов'язати джерела небезпеки з конкретними слабкими місцями інфраструктури та визначити пріоритети реагування на ризики. Методологічно загроза розглядається як потенційна причина небажаної події, що може реалізуватися через певний вектор атаки, тоді як вразливість трактується як слабкість компонента, конфігурації або процесу, яка робить можливим використання загрози. Такий підхід є практично значущим через динамічність ландшафту: змінюються тактики та техніки атак, з'являються нові дефекти програмного забезпечення, а також накопичуються ризики внаслідок конфігураційних помилок і технічного боргу. У результаті аналіз має поєднувати класифікацію типових загроз, ідентифікацію релевантних вразливостей та пріоритезацію ризиків на основі ймовірності реалізації та масштабу наслідків, що узгоджується з рекомендаціями NIST щодо проведення оцінювання ризиків.

У сучасних оглядах кіберзагроз наголошується на домінуванні категорій, які безпосередньо впливають на мережеву інфраструктуру та мережево-орієнтовані сервіси: атаки на доступність (DoS/DDoS), кампанії ransomware, поширення шкідливого програмного забезпечення, соціальна інженерія, а також атаки на ланцюги постачання та залежності. Такі загрози мають міжсекторальний характер і проявляються як у публічних сервісах, так і у внутрішніх сегментах мереж. У свою чергу, нормативні підходи до ризик-менеджменту підкреслюють необхідність

формалізованого зв'язку між загрозами, вразливостями, наслідками та наявними контролями безпеки, оскільки саме цей зв'язок забезпечує відтворюваність управлінських рішень і прозорість пріоритезації заходів захисту.

Об'єктом аналізу доцільно визначати корпоративні комп'ютерні мережі, що охоплюють мережеве обладнання (маршрутизатори, комутатори, точки доступу Wi-Fi, міжмережеві екрани), серверну інфраструктуру, робочі станції, доменні служби, засоби віддаленого доступу, системи моніторингу та журналювання подій, а також канали взаємодії з Інтернетом і хмарними провайдерами. Для таких мереж типовими є сегментація на підмережі (користувацькі, серверні, DMZ, гостьові), застосування VLAN, VPN, проксі-рішень, NAT і політик доступу. Уразливості в межах цього об'єкта формуються як на рівні програмних дефектів, так і на рівні конфігурацій та процесів експлуатації, а наслідки інцидентів проявляються у порушенні конфіденційності, цілісності та доступності даних і сервісів.

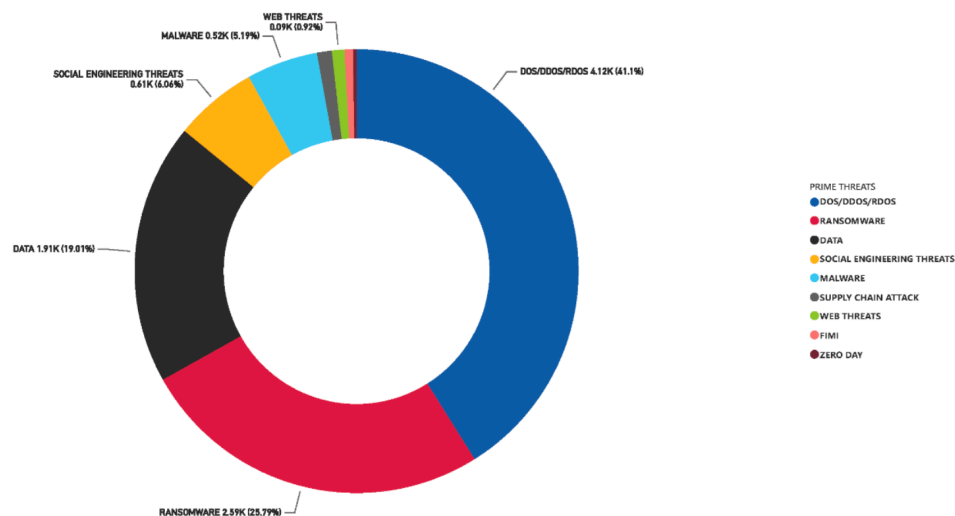


Рис.1.1. Основні загрози комп'ютерних мереж

Сценарії компрометації мережевих середовищ зазвичай мають фазовий характер, що дозволяє формалізувати точки контролю та виявляти критичні вузли ризику. Типова послідовність включає: розвідку та картографування периметра (виявлення адрес, сервісів, доменів і залежностей); первинний доступ (експлуатація вразливостей, компрометація облікових даних, фішинг, помилки конфігурації); закріплення та підвищення привілеїв (зловживання правами доступу, експлуатація уразливостей служб, викрадення токенів); латеральне

переміщення (використання стандартних протоколів адміністрування та довірених зв'язків між сегментами); досягнення цілі (екфільтрація даних, шифрування, саботаж, порушення доступності, підміна інформації). Така логіка підкреслює, що загрози не обмежуються лише периметром: після первинного доступу вирішальними стають внутрішні комунікації, контроль ідентичностей, якість сегментації та здатність виявляти аномалії за телеметрією. Концептуально це узгоджується з підходом zero trust, у межах якого захист зміщується від статичних мережеских периметрів до фокусу на користувачах, активах і ресурсах, а неявна довіра на підставі мережевого розташування вважається недостатньою.

Атаки на доступність реалізуються як навмисне створення умов, за яких мережеві сервіси не можуть обслуговувати легітимні запити або працюють у деградованому режимі. До типових проявів належать DoS та DDoS-атаки на мережеві канали, DNS-інфраструктуру, веб-ресурси й інтерфейси керування. Сучасні кампанії нерідко поєднують об'ємні атаки (перевантаження пропускної здатності) з протокольними й прикладними атаками, спрямованими на виснаження станів, сесій та ресурсомістких операцій. Уразливість підсилюється залежністю від зовнішніх провайдерів (хостинг, CDN, DNS, хмарні балансувальники), оскільки відмова критичної ланки може спричинити каскадний ефект для бізнес-процесів, включно з недоступністю автентифікації, пошти, корпоративних порталів або API, що відображено в узагальненнях ландшафту загроз на рівні ЄС.

Ransomware доцільно розглядати як багатофазну атаку, що поєднує проникнення в мережу, розвідку внутрішніх ресурсів, зловживання засобами адміністрування, шифрування даних і часто екфільтрацію з подальшим шантажем. Критичність для мережі визначається тим, що ransomware активно використовує латеральне переміщення та централізовані служби (каталоги, файлові сховища, системи резервного копіювання), а помилки сегментації й надмірні привілеї прискорюють масштабування інциденту від локального до організаційного рівня. У технічному вимірі поєднуються експлуатація публічно доступних сервісів, слабкість парольної політики, недостатність багатофакторної автентифікації, помилки конфігурації VPN/VDI та ризики ланцюга оновлень. Відповідно, мережа виступає не лише точкою входу, а й середовищем поширення та керування атакою.

Шкідливе програмне забезпечення у мережевому контексті охоплює трояни, бекдори, інфостілери, проксі-боти, криптомайнери та завантажувачі наступних стадій атаки. Мережева небезпека полягає у формуванні прихованих каналів керування та екфільтрації (C2), застосуванні DNS-тунелювання та HTTPS-каналів, а також у використанні легітимних хмарних сервісів як транспортного рівня. Наслідками стають компрометація облікових даних, збір конфіденційних файлів, підміна транзакцій і створення передумов для більш масштабних атак. За наявності централізованих доменних служб критичною стає протидія викраденню секретів і токенів, оскільки це перетворює локальний інцидент на компрометацію доменного рівня.

Соціальна інженерія зберігає роль універсального вектора первинного доступу, оскільки дозволяє обійти частину технічних бар'єрів через вплив на поведінку користувачів. У мережевих сценаріях це проявляється як фішинг із викраденням облікових даних, встановленням шкідливих компонентів, отриманням доступу до віддалених сесій або зловживанням механізмами підтвердження MFA. Наслідком є не лише компрометація окремого облікового запису, а й створення точки входу у внутрішні сегменти, де можуть діяти менш жорсткі політики безпеки. Узагальнення загрозливих категорій на рівні ЄС також фіксує стабільну присутність соціальної інженерії серед пріоритетних категорій.

Загрози даним охоплюють витік через зовнішні канали та внутрішню компрометацію через некоректні права доступу, публічні сховища, помилки ізоляції та неконтрольований обмін файлами. Для мережевої інфраструктури принциповим є те, що екфільтрація часто маскується під звичайний вихідний трафік через HTTPS, хмарні диски, API інтеграцій, поштові сервіси та інші дозволені канали. Модифікація даних може виконуватися як безпосередньо у сховищах, так і шляхом перехоплення або підміни трафіку за відсутності належного шифрування та верифікації цілісності. Окрему небезпеку становлять атаки на конфігураційні репозиторії, системи CI/CD та служби керування інфраструктурою, оскільки зміна одного артефакту може спричинити множинні компрометації залежних вузлів.

Атаки на ланцюг постачання в мережевому контексті проявляються як компрометація оновлень постачальників, бібліотек, агентів адміністрування, віддалених сервісів, провайдерів ідентичностей або підрядників із доступом до мережі. Специфіка полягає у перенесенні довіри на зовнішній суб'єкт: компрометація такого суб'єкта призводить до проникнення шкідливих змін у мережу під виглядом легітимних операцій. У зв'язку з цим у сучасних оглядах загроз підкреслюється пріоритетність контролю ризиків постачальників, верифікації оновлень та застосування принципу мінімальних привілеїв для інтеграцій.

Систематизація вразливостей мережевих середовищ показує, що найбільшу практичну частку становлять конфігураційні слабкості: відкриті інтерфейси керування (SSH, RDP, веб-панелі), надмірно широкі правила доступу, відсутність сегментації, помилки NAT і маршрутизації, використання застарілих криптографічних налаштувань у VPN або TLS, тестові облікові записи та невідключені непотрібні служби. Додатковим фактором є неконсистентність політик між сегментами та середовищами, коли частина інфраструктури має посилені правила, а інша залишається з дефолтними налаштуваннями, що створює умови для обходу захисту через найслабшу ланку. Вразливості програмного забезпечення та мережевих сервісів охоплюють дефекти ОС, мережевих служб, веб-серверів, служб каталогів, клієнтських застосунків і агентських компонентів адміністрування, при цьому ризик посилюється затримками в оновленнях та залежностями сумісності. Окремо виділяються уразливості, що забезпечують віддалене виконання коду в сервісах на периметрі, підвищення привілеїв на критичних серверах, обхід автентифікації та авторизації, а також можливість внутрішнього руху без взаємодії з користувачем.

Суттєва частина інцидентів зумовлюється компрометацією облікових даних, що підкреслює критичність вразливостей ідентичностей та доступу: слабкі або повторно використані паролі, відсутність MFA для критичних доступів, застарілі протоколи автентифікації, помилки довірених зв'язків між доменами, надмірні привілеї сервісних акаунтів, неконтрольовані API-ключі та токени. Навіть без експлуатації CVE доступ може бути отриманий через підбір пароля, використання

витоків, перехоплення сесій або соціальну інженерію, тобто формально система може працювати коректно, але модель довіри є порушеною. Водночас шифрування та верифікація цілісності трафіку залишаються фундаментом захисту передавання даних, а слабкості криптографічної конфігурації (застарілі алгоритми, помилки TLS, неправильне управління сертифікатами) створюють умови для перехоплення облікових даних, атак посередника та непомітної екфільтрації через незахищені протоколи.

Окремою вразливістю мережесередовищ є недостатня спостережуваність: відсутність централізованого журналювання, мала глибина зберігання логів, невизначеність відповідальних за кореляцію подій, відсутність сенсорів у ключових точках трафіку, некоректні налаштування синхронізації часу та неузгодженість ідентифікаторів активів. За таких умов інцидент може тривати тривалий час, оскільки індикатори компрометації не реєструються або не аналізуються, а розслідування ускладнюється браком даних. У цьому контексті ризик-орієнтований підхід, запропонований у NIST SP 800-30 Rev.1, є методологічною основою для пріоритезації, оскільки передбачає послідовну ідентифікацію активів, загроз і вразливостей, оцінювання ймовірності та впливу, а також визначення залишкового ризику й пріоритетів обробки.

З урахуванням наведеного, ключовий висновок полягає в тому, що зниження мережесередовищеских ризиків вимагає поєднання організаційної пріоритезації та технічних контрольних механізмів, які забезпечують керований примус політик доступу і трафіку, обмежують небажані взаємодії між сегментами та створюють умови для виявлення аномалій. У цьому сенсі особливо значущим є клас рішень, що контролює потоки трафіку між мережами або хостами з різними безпековими позиціями та реалізує формалізовану політику обробки потоків, оскільки саме він забезпечує базову структурну основу сегментації та зменшення площі атаки.

1.2. Аналіз підходів до забезпечення безпеки комп'ютерних мереж

Забезпечення безпеки комп'ютерних мереж розглядають як системний комплекс підходів, у межах якого технічні механізми захисту поєднуються з

керованими процесами, правилами експлуатації та контролем ефективності. Мережа в цьому контексті є не лише каналом передавання даних, а й середовищем взаємодії активів, ідентичностей та сервісів, де будь-яка помилка в архітектурі, конфігурації чи моделі доступу може перетворитися на масштабне порушення конфіденційності, цілісності або доступності. Тому аналіз підходів має фокусуватися на тому, як організація формує керовану безпекову позицію мережі, зменшує площу атаки, контролює доступ і трафік, забезпечує спостережуваність та здатність до реагування і відновлення.

Ключовим методологічним підходом у мережевій безпеці є ризик-орієнтоване управління, коли вибір заходів захисту визначається не переліком популярних технологій, а пріоритетами активів і сценаріями загроз для конкретної мережевої архітектури. Такий підхід забезпечує обґрунтованість рішень щодо сегментації, розміщення контрольних точок, вимог до віддаленого доступу, політик фільтрації, моніторингу та резервування. Практичне значення ризик-орієнтованості проявляється у можливості узгоджувати мережеві зміни з бізнес-вимогами, формувати прийнятний рівень залишкового ризику та обирати компенсуючі контролю там, де повна нейтралізація загрози економічно або технологічно недоцільна. Для формування такої керованості застосовуються рамкові моделі, що задають цільові результати безпеки, підтримують пріоритезацію та вимірювання прогресу. У цьому сенсі доречним є використання NIST Cybersecurity Framework 2.0 як орієнтира для побудови узгодженого циклу управління кіберризиками, у межах якого мережеві контрзаходи розглядаються як частина цілісної програми, а не як ізольований набір налаштувань або засобів [5].

Наступним фундаментальним підходом є архітектурна безпека мережі, тобто проектування структури та правил взаємодії компонентів так, щоб мережа за замовчуванням обмежувала небезпечні траєкторії атаки. Архітектурний підхід передбачає розділення мережі на зони з різними рівнями довіри, керування маршрутами та потоками між зонами, винесення критичних сервісів у ізольовані сегменти, обмеження площини адміністрування та мінімізацію експонованих назовні сервісів. У традиційній логіці периметр міг розглядатися як головний рубіж оборони, однак сучасні гібридні середовища, віддалена робота та інтеграція з

хмарними сервісами роблять периметр умовним і змінним. У результаті зростає роль підходу, за якого довіра не базується на розташуванні вузла в мережі, а формується через перевірку ідентичності, контексту та політик доступу до конкретного ресурсу. Ця ідея системно описується в NIST SP 800-207, де Zero Trust Architecture визначається як концептуальна рамка з акцентом на політико-орієнтований контроль доступу та мінімізацію неявної довіри, зокрема всередині мережі [6].

У практиці мережевої безпеки підхід Zero Trust реалізується як сукупність рішень щодо ідентичностей, доступу, сегментації та контролю трафіку, які в комплексі зменшують імовірність успішного первинного доступу та ускладнюють розвиток атаки після проникнення. Центальною категорією стає сильна автентифікація й авторизація, де доступ до мережевих ресурсів прив'язується до конкретного суб'єкта, його ролі та контексту сесії. Мережеві рішення в такому випадку мають підтримувати контроль не лише на вході в мережу, а й у внутрішніх взаємодіях, особливо для адміністративних протоколів, доступу до доменних сервісів, файлових сховищ, систем керування конфігураціями та інших вузлів, компрометація яких викликає каскадні наслідки. Важливо, що ефективність Zero Trust в мережі залежить від якості інвентаризації активів і ідентичностей, оскільки політика не може бути коректно застосована, якщо не визначено, які вузли існують, які з них критичні та які типові маршрути і потоки між ними є допустимими.

Сегментація в рамках сучасних підходів розглядається не як одноразовий поділ на кілька VLAN, а як керована модель мінімально необхідних взаємодій, яка обмежує латеральне переміщення та зменшує радіус ураження при компрометації вузла. У технічному сенсі доцільним є поєднання макросегментації (користувачькі, серверні, DMZ, гостьові зони) та мікросегментації, коли політики застосовуються до конкретних груп сервісів або навіть до окремих робочих навантажень. Такий підхід переводить мережеву безпеку в режим контролю east-west трафіку, де найбільш небезпечними вважаються не лише зовнішні спроби доступу, а й внутрішні нетипові взаємодії, сканування, спроби підбору облікових даних або використання адміністративних протоколів поза регламентом. При цьому сегментація є ефективною лише за умови, що правила між сегментами підкріплені

принципом найменших привілеїв, а винятки з політик обґрунтовані, документовані та регулярно переглядаються, інакше сегментація деградує до формального поділу без реальних обмежень.

Важливою групою підходів є периметровий і транспортний контроль трафіку, який, попри умовність периметра, все ще залишається критичним елементом. Він включає політики фільтрації вхідних і вихідних потоків, обмеження непотрібних сервісів, контроль адміністративних інтерфейсів, застосування принципу мінімальної експонованості, а також керування віддаленим доступом. У сучасній практиці обґрунтованим вважається зниження кількості прямого публічного доступу до внутрішніх сервісів і перенесення доступу через керовані шлюзи з сильною автентифікацією, короткоживучими сесіями та контекстними політиками. Для мережі це означає, що VPN або інші канали доступу мають розглядатися як частина моделі довіри: важливими стають криптографічна стійкість, контроль налаштувань, видимість сесій, аудит дій та можливість швидкого відкликання доступу. Паралельно важливим є контроль вихідного трафіку, оскільки сучасні атаки часто використовують легітимні канали екфільтрації через HTTPS та хмарні сервіси, і без політик egress-control мережа втрачає здатність обмежувати витік даних навіть при наявності захисту на вході.

Криптографічний підхід у мережевій безпеці охоплює забезпечення конфіденційності та цілісності даних у транзиті та зниження ризику перехоплення облікових даних. Він реалізується через коректне застосування TLS для сервісів, захищені тунелі для віддалених сегментів, політики щодо шифрів і протоколів, а також управління сертифікатами та ключовим матеріалом. У мережевому контексті критичним є те, що криптографія не компенсує помилки доступу, але значно зменшує ефективність атак посередника, пасивного прослуховування та підміни трафіку. Практичні проблеми виникають через використання застарілих алгоритмів, некоректне налаштування перевірки сертифікатів, слабе управління життєвим циклом ключів та неузгодженість політик між середовищами. Тому криптографічний підхід має реалізовуватися не фрагментарно, а як частина конфігураційних базових ліній для мережеских компонентів і сервісів.

Безпека бездротових сегментів є окремою прикладною площиною мережових підходів, оскільки Wi-Fi поєднує ризики радіоефіру, мобільності клієнтів і потенційної відсутності фізичного контролю над середовищем. У рамках загальної логіки підходів доцільним є застосування сильних режимів автентифікації, ізоляція гостьових і корпоративних сегментів, мінімізація перетинів між бездротовими мережами та критичними ресурсами, контроль доступу за профілями пристроїв та моніторинг аномалій підключень. Безпека бездротових мереж у практиці не зводиться лише до вибору режиму шифрування, оскільки значна частина інцидентів пов'язана з неправильними політиками доступу, спільними паролями, неконтрольованим підключенням неавторизованих пристроїв і появою тіньових точок доступу, що обходять політики організації.

Окремою групою є конфігураційна безпека та керування змінами в мережі. Вразливості мережевої інфраструктури часто формуються не через складні протокольні атаки, а через помилки адміністратора, надмірно широкі правила фільтрації, відкриті керуючі інтерфейси, дефолтні облікові дані, невідключені сервіси та розбіжності між фактичною та задокументованою конфігурацією. Тому якісна практика забезпечення безпеки мереж передбачає інвентаризацію обладнання та сервісів, побудову базових конфігураційних профілів, контроль відхилень, формалізовані процедури внесення змін, регулярний аудит правил доступу та систематичне вилучення технічного боргу. Результативність цього підходу суттєво зростає при переході до автоматизації та керованих шаблонів, оскільки ручне адміністрування на масштабі створює неминучі помилки, а розрізнені зміни з часом руйнують логіку сегментації і доступу. У підходах CIS Controls акцент робиться на пріоритезованих практиках, які підтримують саме керованість і вимірюваність захисних дій, що є важливим для мережевої дисципліни конфігурацій і контролю [7].

Підхід управління вразливостями в мережевому середовищі полягає у безперервному циклі виявлення, оцінювання та усунення слабких місць у мережевому обладнанні, сервісах і кінцевих вузлах, що впливають на мережеву безпеку. Практично це означає підтримку актуальності прошивок і ОС на мережових пристроях, контроль версій сервісів, управління експонованими

портами, а також тестування змін до впровадження. У межах цього підходу важливим є скорочення часу до усунення критичних вразливостей, особливо для компонентів, доступних з Інтернету, а також забезпечення того, щоб оновлення не порушували доступність ключових сервісів. Типовою проблемою є конфлікт між вимогами безпеки та вимогами безперервності, тому ефективна практика включає планування вікон обслуговування, резервування, тестові контури та контроль зворотного відкату. При цьому слід враховувати, що мережеві інциденти часто стартують із компрометації облікових даних або помилок доступу без експлуатації CVE, а тому управління вразливостями має доповнюватися посиленням ідентичностей і політик доступу.

Підходи до контролю ідентичностей і доступу мають особливе значення саме для мереж, оскільки мережа об'єднує різні домени довіри та часто забезпечує транспорт для адміністративних протоколів. Практичний фокус включає багатофакторну автентифікацію для критичних доступів, мінімізацію постійних привілеїв, жорсткі правила для адміністративних облікових записів, сегментацію адміністративного трафіку та контроль віддаленого адміністрування. Додатково важливим є захист сервісних облікових записів і секретів, оскільки вони часто використовуються для автоматизації й інтеграцій і можуть стати механізмом непомітної ескалації привілеїв. У рамках Zero Trust підкреслюється потреба в явній перевірці та політико-орієнтованому доступі, що зменшує ризики, пов'язані з неявною довірою до внутрішніх сегментів [6].

Неможливо забезпечити стійку мережеву безпеку без підходу спостережуваності, що включає моніторинг, журналювання та аналітику подій. Оскільки жодна мережа не може бути повністю ізольована від інцидентів, важливими стають час виявлення, якість даних для розслідування та здатність до швидкого реагування. У мережевій площині спостережуваність базується на централізованому збиранні журналів із мережевих пристроїв, сервісів доступу, систем автентифікації та критичних вузлів, на підтримці коректної синхронізації часу, на контролі змін конфігурацій і на аналізі мережевих потоків. Перевага підходу полягає у можливості виявляти аномальні патерни, зокрема нетипові внутрішні підключення, сканування сегментів, підозрілі обсяги вихідного трафіку,

повторювані невдалі спроби автентифікації та інші індикатори компрометації. Практична результативність спостережуваності залежить від того, чи перетворюється телеметрія на керовані процедури: визначення порогів, правил кореляції, маршрутів ескалації та сценаріїв реагування.

Підхід реагування на інциденти та мережевої стійкості полягає у створенні умов, за яких мережа здатна локалізувати інцидент, зберегти керованість, підтримати відновлення сервісів і мінімізувати наслідки. У мережевому контексті критичною є можливість швидко відокремити уражений сегмент, змінити політики доступу, відкликати скомпрометовані облікові дані, перекрити канали керування атакувальника, а також забезпечити коректне функціонування резервних каналів і критичних сервісів. Стійкість також включає підхід до забезпечення доступності, що передбачає резервування, контроль пропускнуої здатності, керування навантаженням і готовність до протидії атакам на доступність. Хоча ці заходи часто асоціюються з експлуатаційною інженерією, у межах мережевої безпеки вони є частиною контролю ризику простою та відмови сервісів, тому мають бути інтегровані в загальну програму управління безпекою.

Автоматизація та стандартизація є окремим підходом, який підвищує якість мережевої безпеки через зменшення людського фактора та забезпечення відтворюваності контролів. У практиці це проявляється як використання шаблонів конфігурацій, політик як коду, централізованого управління правилами доступу та процедур контролю змін. Автоматизація не замінює аналізу ризиків і архітектурного проєктування, але забезпечує масштабованість і стабільність: мережеві правила легше перевіряти, узгоджувати, документувати та швидко змінювати під час інцидентів. Водночас автоматизація створює нові вимоги до контролю доступу до систем керування інфраструктурою, до аудиту змін і до ізоляції адміністративних площин, оскільки компрометація системи автоматизації може мати системний ефект на всю мережу.

Підхід пріоритезованих практик, орієнтованих на зупинення найбільш типових атак, у мережевій безпеці є корисним інструментом для узгодження технічних дій із реальними загрозами та ресурсними обмеженнями. CIS Controls v8 позиціонується як набір прескриптивних і спрощених найкращих практик, що

формують чіткий шлях для підвищення кіберзахисту організації [7]. Для мережеских команд практична цінність такого підходу полягає в тому, що пріоритетні заходи допомагають уникати ситуації, коли розбудова безпеки перетворюється на нескінченне додавання розрізнених вимог. Натомість формується послідовність: спочатку інвентаризація та контроль конфігурацій, потім контроль доступу й сегментація, далі моніторинг, реагування та підвищення зрілості. Узгодження таких практик із рамковим ризик-орієнтованим управлінням забезпечує вимірюваність прогресу та підзвітність: стає можливим оцінювати не лише факт наявності технологій, а й реальний стан виконання контрольних дій, їх повноту та ефективність.

Суттєвим аспектом аналізу підходів є їх взаємодоповнюваність і потреба в узгодженій інтеграції. Жоден підхід не є самодостатнім. Периметрова фільтрація без сегментації створює ризик швидкого латерального руху після проникнення. Сильна автентифікація без журналювання й контролю сесій ускладнює розслідування та не гарантує виявлення зловживань. Шифрування каналів без контролю доступу не запобігає несанкціонованому використанню легітимних облікових даних. Автоматизація без контролю адміністративних доступів може підвищити масштаб наслідків при компрометації. Саме тому сучасна мережево-орієнтована безпека обґрунтовано опирається на комбінацію ризик-орієнтованого управління, архітектурних принципів, Zero Trust логіки доступу, конфігураційної дисципліни, управління вразливостями, спостережуваності та готовності до реагування. У NIST SP 800-207 така логіка відображається через акцент на політико-орієнтованому контролі доступу й мінімізації неявної довіри, що є визначальним для сучасних гібридних мереж [6]. У NIST CSF 2.0, своєю чергою, підкреслюється необхідність перетворення безпеки на керований процес із пріоритезацією та комунікацією результатів, що дозволяє системно впроваджувати і підтримувати мережеві контролі на рівні організації [5].

Отже, аналіз підходів до забезпечення безпеки комп'ютерних мереж показує, що найстійкіша модель досягається не максимальною кількістю точкових засобів, а керованою системою, де архітектурні рішення, політики доступу та контроль трафіку підкріплюються процесами конфігураційного управління, управління

вразливостями, моніторингом і планами реагування. Така система зменшує площу атаки, обмежує поширення інцидентів у мережі, забезпечує видимість подій і дозволяє підтримувати прийнятний рівень ризику в умовах змінної інфраструктури та еволюції загроз. При цьому джерельні орієнтири на кшталт NIST CSF 2.0, NIST SP 800-207 і CIS Controls v8 задають узгоджену логіку: від управління і результатів до конкретних контрольних дій і архітектурних принципів [5–7].

1.3 Аналіз існуючих рішень щодо забезпечення безпеки комп'ютерних мереж

Аналіз існуючих рішень щодо забезпечення безпеки комп'ютерних мереж варто будувати через розуміння двох взаємопов'язаних площин: керування кіберризиком на рівні організації та реалізація технічних контролів на рівні мережевої архітектури, протоколів і сервісів. У сучасних умовах мережа рідко є статичною: користувачі працюють віддалено, застосунки мігрують у хмару, а значна частина критичних бізнес-процесів залежить від веб-сервісів і API. Через це мережевий захист уже не зводиться до одного периметрового бар'єра; він формується як система взаємодоповнювальних засобів, які одночасно обмежують доступ, відстежують аномалії, забезпечують шифрування каналів, збирають телеметрію та підтримують відновлення після інцидентів. Узагальнену логіку такої системи зручно описувати через функції управління кібербезпекою, визначені в NIST Cybersecurity Framework 2.0: Govern, Identify, Protect, Detect, Respond, Recover [8].

З позиції управління безпекою мережі першочерговими є завдання формалізації очікувань і правил: які дані та сервіси вважаються критичними, хто має право доступу, який рівень журналювання потрібний для розслідувань, які показники визначають прийнятний рівень ризику. Саме на цьому рівні виникає потреба в узгодженні технічних рішень із політиками та процесами, оскільки без регламенту змін і контролю конфігурацій навіть найсучасніші інструменти деградують у набір випадкових винятків. CSF 2.0 окремо підкреслює роль функції Govern як основи для управління ризиком, політиками і відповідальністю, що

безпосередньо впливає на дисципліну налаштувань мережевих контролів і їх перевірку [8].

У технічній площині найстійкіший підхід до мережевого захисту базується на принципі багатошаровості, де кожен шар виконує окрему функцію та компенсує обмеження інших. Одним із базових механізмів є сегментація, яка зменшує площину атаки і стримує поширення компрометації всередині організації. Сегментація вводить логічні межі між користувацькими, серверними, DMZ-сегментами, середовищем керування та іншими зонами, а доступ між ними здійснюється за контрольованими правилами. CISA у своїх матеріалах підкреслює, що сегментація додає контроль і зменшує ризик або масштаб наслідків кібератаки, оскільки обмежує «вільне» переміщення між частинами мережі. У сучасній практиці сегментація доповнюється мікросегментацією, яка зменшує довіру навіть усередині одного сегмента і дозволяє будувати політики на рівні робочих навантажень і конкретних з'єднань. Це узгоджується із загальною логікою Zero Trust, де довіра не надається «за фактом перебування в мережі», а формується на основі контексту, ідентичності та політик для конкретного ресурсу, а CISA окремо публікує методичні матеріали щодо мікросегментації як одного з ключових мережевих контролів у Zero Trust-підході [11].

Окремою великою групою існуючих рішень є засоби керування доступом і фільтрації трафіку, де центральну роль відіграють фаєрволи. Фаєрволи реалізують політику пропуску або блокування трафіку між мережами чи хостами з різними рівнями довіри та забезпечують контроль напрямків, протоколів, портів, адрес і, у сучасних варіантах, контексту застосунків. NIST розглядає фаєрвол як механізм контролю потоку трафіку між мережами/хостами з різними безпековими «позами» та наголошує на критичності саме політики фаєрвола, яка визначає, як обробляються вхідні й вихідні потоки, а також на важливості процесів вибору, налаштування, тестування, розгортання і супроводу [9]. У реальних мережах фаєрволи застосовуються в різних точках: на периметрі (Internet edge), у DMZ, між внутрішніми зонами (east-west контроль), а також у вигляді хостових фаєрволів на серверах і робочих станціях. Така багатоточкова модель зменшує залежність від одного периметра і робить мережу стійкішою до помилок конфігурації або

компрометації окремого сегмента. Разом із цим, ефективність фаєрвола визначається не кількістю правил, а їх узгодженістю з архітектурою сегментації та принципом мінімально необхідних дозволів: усе, що не описано явними дозволами, має бути забороненим, а винятки повинні мати обґрунтування і підлягати регулярному перегляду [9].

У межах фаєрвол-підходу сформувалася еволюція від базової фільтрації пакетів до stateful-контролю і далі до NGFW-функціональності, коли рішення враховує стан з'єднання, може пов'язувати трафік із конкретними застосунками, застосовувати політики інспекції та підтримувати інтеграцію з механізмами запобігання вторгненням. Утім, навіть NGFW не закриває всі сценарії: шифрування TLS ускладнює глибоку інспекцію, а значний відсоток атак використовує легітимні канали (наприклад, веб-доступ) і потребує додаткових детекційних рівнів. Це підводить до іншої великої групи рішень — систем виявлення та запобігання вторгненням.

IDS/IPS (або ширше IDPS) розглядаються як засоби, що фіксують підозрілу активність, атаки чи порушення політик і, залежно від режиму роботи, або сигналізують, або блокують небезпечні дії. NIST надає огляд технологій IDPS, підкреслюючи необхідність проектування, налаштування, захисту, моніторингу та супроводу таких систем, а також описує типові класи продуктів і підходи до детекції [10]. На практиці мережеві IDS/IPS розміщують на межі критичних зон і на напрямках з найбільшим ризиком: Internet→DMZ, доступ до серверних сегментів, керуючі протоколи, міжсегментні потоки до служб автентифікації, баз даних тощо. Окремий клас рішень пов'язаний із поведінковим аналізом трафіку (network behavior analysis) та NDR-підходами, де акцент робиться на аномаліях і кореляції ознак, а не лише на сигнатурах. У цьому сегменті ключовим фактором якості є не тільки механізм детекції, а й наявність коректної базової моделі нормальної активності та процес тюнінгу, без якого система або генерує надмірні хибні спрацювання, або пропускає важливі події. NIST у матеріалах про IDPS також звертає увагу на операційну складову: потрібні процедури аналізу тривоги, актуалізація правил, розмежування доступів до керування і контроль змін [10].

Захист мережі неможливо повноцінно розглядати без безпечного віддаленого доступу і захищених каналів між майданчиками. Найпоширенішим технологічним класом залишаються VPN-рішення, зокрема IPsec для site-to-site та окремі технології для віддалених користувачів. NIST SP 800-77 Rev.1 описує IPsec VPN як механізм захисту мережових комунікацій і надає рекомендації щодо підготовки, експлуатації та безпеки таких розгортань. На практиці ефективність VPN визначається не самим фактом тунелювання, а політиками того, який трафік через тунель дозволено, як керуються ключі та криптографічні параметри, чи обмежується доступ користувача до мінімально потрібних ресурсів, і чи існує журналювання сесій. У сучасних архітектурах VPN дедалі частіше поєднується із принципами Zero Trust та ідеєю ZTNA, де доступ формується навколо конкретного ресурсу і контексту користувача, а не навколо «підключення до мережі». NIST SP 800-207 визначає Zero Trust як набір парадигм, що зміщують захист із статичного периметра на користувачів, активи і ресурси, та описує загальні кроки переходу до Zero Trust-архітектури [11].

Ще один базовий клас рішень — керування доступом на рівні ідентичності та підключення до мережі, яке часто реалізується через NAC-підходи, контроль портів (802.1X), профілювання пристроїв, ізоляцію невідомих вузлів і застосування політик залежно від ролі користувача або стану пристрою. Хоча конкретні механізми можуть відрізнятися, їхня мета спільна: не допускати, щоб будь-який пристрій, який фізично або логічно підключився до мережі, автоматично отримував доступ до чутливих сегментів. У практичних програмах безпеки це тісно пов'язано з управлінням активами, обліковими записами, багатофакторною автентифікацією та контрольованими привілеями. У CIS Controls ця логіка відображається як пріоритизований набір safeguards, що починається з інвентаризації активів і подальшого контролю конфігурацій, доступів і захисту даних [10].

Важливе місце серед існуючих рішень посідають засоби безпеки для веб-доступу та доменних взаємодій, оскільки значний обсяг корпоративної активності проходить через HTTP/HTTPS і DNS. До таких рішень належать secure web gateway, DNS-фільтрація, категоризація контенту, репутаційні списки та

інструменти, які блокують доступ до відомо шкідливих доменів/адрес або небажаних категорій сервісів. Ці механізми не замінюють фаєрвол або IDS/IPS, але створюють додатковий бар'єр проти фішингу, шкідливих завантажень і командно-керуючих комунікацій, які часто використовують веб і DNS як транспорт. У Zero Trust-підході контроль доступу до ресурсів доповнюється політиками для сесій, пристроїв і контексту, що підсилює ефективність мережевих контролів у гібридних середовищах.

Окремої уваги потребують рішення, пов'язані з журналюванням, моніторингом та централізованою аналітикою, оскільки без телеметрії мережеві політики не можуть бути ані перевірені, ані вдосконалені. NIST SP 800-92 розглядає лог-менеджмент як набір практик розробки, впровадження і підтримки ефективного журналювання в масштабі організації та підкреслює важливість повного циклу роботи з логами, включно зі збиранням, зберіганням, аналізом і захистом журналів [8]. У цій групі рішень розміщуються SIEM-платформи, системи кореляції подій, засоби збагачення даних threat intelligence та оркестрація реагування. Практична цінність SIEM визначається пріоритизацією джерел і якістю подій: потрібні логи з мережевих контрольних точок, систем автентифікації, критичних серверів, DNS/DHCP, VPN-шлюзів, а також дані про зміни конфігурацій. CISA також надає матеріали з базових практик журналювання і детекції загроз, які можна використовувати як орієнтир для мінімального набору та якості подій [9].

Моніторинг у сучасних мережах переходить від періодичних перевірок до постійної обізнаності щодо стану активів, вразливостей і загроз. NIST SP 800-137 визначає Information Security Continuous Monitoring як підтримання постійної обізнаності щодо безпеки, вразливостей і загроз на підтримку рішень з управління ризиком [11]. У практичному сенсі це означає регулярне сканування вразливостей, контроль конфігурацій, відстеження змін топології, оновлення сигнатур, аналіз аномалій трафіку, контроль доступів і ротацію ключових секретів. Змістовно ці процеси добре узгоджуються з пріоритизованими заходами CIS Controls, де акцент робиться на видимості активів, контрольованості конфігурацій, керуванні вразливостями, захисті даних та здатності до реагування [12].

Окремим виміром аналізу існуючих рішень виступає те, як вони інтегруються в модель загроз і як забезпечують вимірюваність покриття. Тут широко використовується MITRE ATT&CK як знаннєва база тактик і технік противника, яка допомагає співвідносити можливості засобів захисту з реальними сценаріями атак і формувати вимоги до журналювання та детекцій. ATT&CK описується як загальнодоступна база знань, сформована на основі спостережень у реальному світі, і застосовується для побудови моделей загроз і методологій у різних секторах [13]. У мережевому контексті це дозволяє перевіряти, чи є видимість і детекції для ключових етапів атаки: первинний доступ, встановлення командно-керуючих каналів, латеральний рух, викрадення облікових даних, ексфільтрація. Відповідно, рішення з мережевого захисту оцінюються не лише за «наявністю функції», а за тим, чи дають вони контрольовані політики, які можна підтвердити телеметрією, і чи підтримують керований цикл удосконалення.

Порівняльний аналіз існуючих рішень показує, що різні класи інструментів мають різні сильні сторони та обмеження. Фаєрволи сильні в політиках і сегментації, але обмежені там, де потрібна глибока видимість за умов масового TLS-шифрування або де атака використовує легітимні протоколи й сервіси без явних сигнатур. IDS/IPS забезпечують детекцію й запобігання відомим класам атак, але потребують тюнінгу, актуалізації правил і якісного процесу реагування на спрацювання. VPN вирішує задачу шифрування каналу, проте не гарантує правильного розмежування доступу без додаткових політик і контролю ідентичності. Zero Trust-підхід змінює логіку побудови доступу, зменшуючи роль «внутрішньої довіри», але для практичного переходу потребує інвентаризації ресурсів, коректної ідентифікації та перебудови політик на рівні ресурсів і контексту. Сегментація і мікросегментація обмежують поширення атак, але потребують якісної моделі потоків і дисципліни в керуванні правилами. Лог-менеджмент і SIEM забезпечують видимість і доказовість, але їхня ефективність прямо залежить від правильного відбору джерел, структури подій і процесів аналізу. Continuous monitoring дозволяє підтримувати актуальність контролів, але потребує метрик і регулярності, інакше перетворюється на нерегулярні перевірки без керованого результату [11].

Узагальнюючи, існуючі рішення щодо забезпечення безпеки комп'ютерних мереж формують «конструктор» із різних класів контролів, які мають бути зібрані під конкретну архітектуру організації та її ризики. Ядром технічної частини найчастіше виступають сегментація та контроль доступу, де фаєрвол забезпечує політики між зонами, IDS/IPS доповнює це детекціями та запобіганням атакам, VPN і Zero Trust-механізми керують захищеним доступом у гібридних сценаріях, а централізоване журналювання та безперервний моніторинг підтримують керованість, аудит і розвиток детекцій. Така композиція відповідає логіці CSF 2.0, у якій технічні заходи мають бути пов'язані з управлінням ризиком, практиками експлуатації та відновленням, а не існувати як набір розрізнених налаштувань [8].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ РІШЕННЯ CISCO

2.1. Призначення та основні функції Cisco Secure Firewall

У сучасній мережевій інфраструктурі міжмережевий екран розглядається як базовий механізм контролю мережевого трафіку між сегментами з різним рівнем довіри, що забезпечує реалізацію політик доступу, зменшення площі атаки та підтримку керованості безпеки. У рекомендаціях NIST підкреслюється, що фаєрволи призначені для контролю потоків трафіку між мережами або вузлами з різними безпековими профілями, а також мають застосовуватися в рамках визначеної політики та процесів адміністрування, тестування й супроводу. У цьому контексті Cisco Secure Firewall використовується як платформний засіб мережевого захисту, що поєднує функції класичного станового фаєрвола та механізми наступного покоління, зокрема ідентифікацію застосунків, інтегроване запобігання вторгненням і використання джерел загрозової інформації [14].

З практичної точки зору Cisco Secure Firewall доцільно розглядати як один із ключових контрольних пунктів на межі мережі організації та всередині її сегментів. Його призначення проявляється у двох взаємодоповнювальних режимах: периметровий захист (north-south трафік) і міжсегментний контроль (east-west трафік). У периметровому сценарії фаєрвол виступає бар'єром між недовіреним середовищем (Інтернет, партнерські мережі, віддалені користувачі) та внутрішніми ресурсами, забезпечуючи фільтрацію, інспекцію протоколів і застосування політик доступу. У міжсегментному сценарії він використовується для ізоляції критичних підсистем, контролю доступу між VLAN або зонами, обмеження латерального переміщення зловмисника та локалізації наслідків інциденту. Такий підхід узгоджується з архітектурним принципом багатошарового захисту, де сегментація і контроль між шарами зменшують ризик компрометації всієї інфраструктури через один слабкий елемент [16].

Периметровий захист зазвичай концентрується на тому, щоб публічні з'єднання не створювали прямого шляху до внутрішніх ресурсів, а доступ до сервісів, що експонуються назовні, відбувався через обмежені та контрольовані контури. У довідкових архітектурах Cisco SAFE для Secure Edge підкреслюється, що край мережі є небезпечним через концентрацію атак, які походять з Інтернету або координуються через зовнішні сервіси, і тому потребує набору контрольних можливостей на кшталт фаєрволінгу, запобігання вторгненням і керованої DMZ. Практично це означає, що Secure Firewall часто розміщується в зоні периметрових сервісів і демілітаризованій зоні, де саме відбувається відсікання недоречного трафіку, обмеження ініціації з'єднань, контроль публікацій сервісів і захист від типових класів атак на вебрівні (наприклад, компрометація сесій, маніпуляції з HTTP, зловживання протоколами прикладного рівня), які, у свою чергу, можуть бути пов'язані з експлуатацією вразливостей вебзастосунків [16].

Окрему вагу має міжсегментний контроль трафіку всередині організації (east-west). У традиційних мережах значна частина захисту історично концентрувалася на периметрі, тоді як внутрішні сегменти вважалися умовно довіреними. У сучасних сценаріях така модель є ризикованою, оскільки після первинного проникнення зловмисник прагне рухатися всередині інфраструктури, підбираючи облікові дані, досліджуючи сервіси та виконуючи горизонтальне переміщення. Унаслідок цього фаєрвол починає виконувати функцію внутрішнього контрольного бар'єра, який примусово реалізує розмежування доступу між сервісами, підсистемами та середовищами (корпоративний доступ, серверні сегменти, середовища розробки/тестування, інфраструктурні служби). Така сегментація підтримує принцип мінімальних привілеїв на рівні мережових взаємодій та суттєво знижує наслідки інциденту, обмежуючи домени поширення шкідливої активності.

У контексті захисту на рівні застосунків важливо, що наступне покоління фаєрволів переходить від суто портово-протокольного контролю до контекстного контролю, де рішення про дозвіл або блокування враховує тип застосунку, характер сесії, пов'язані ризики та індикатори загроз. Cisco визначає NGFW як мережовий засіб безпеки, що виходить за межі традиційного станового фаєрвола, додаючи

принаймні ідентифікацію та контроль застосунків, інтегроване запобігання вторгненням і використання хмарно-доставленої загрозової інформації [14]. Саме ця сукупність властивостей робить Secure Firewall придатним не лише для грубої фільтрації трафіку, а і для протидії атакам прикладного рівня та сучасному шкідливому ПЗ, яке використовує легітимні протоколи як транспорт.

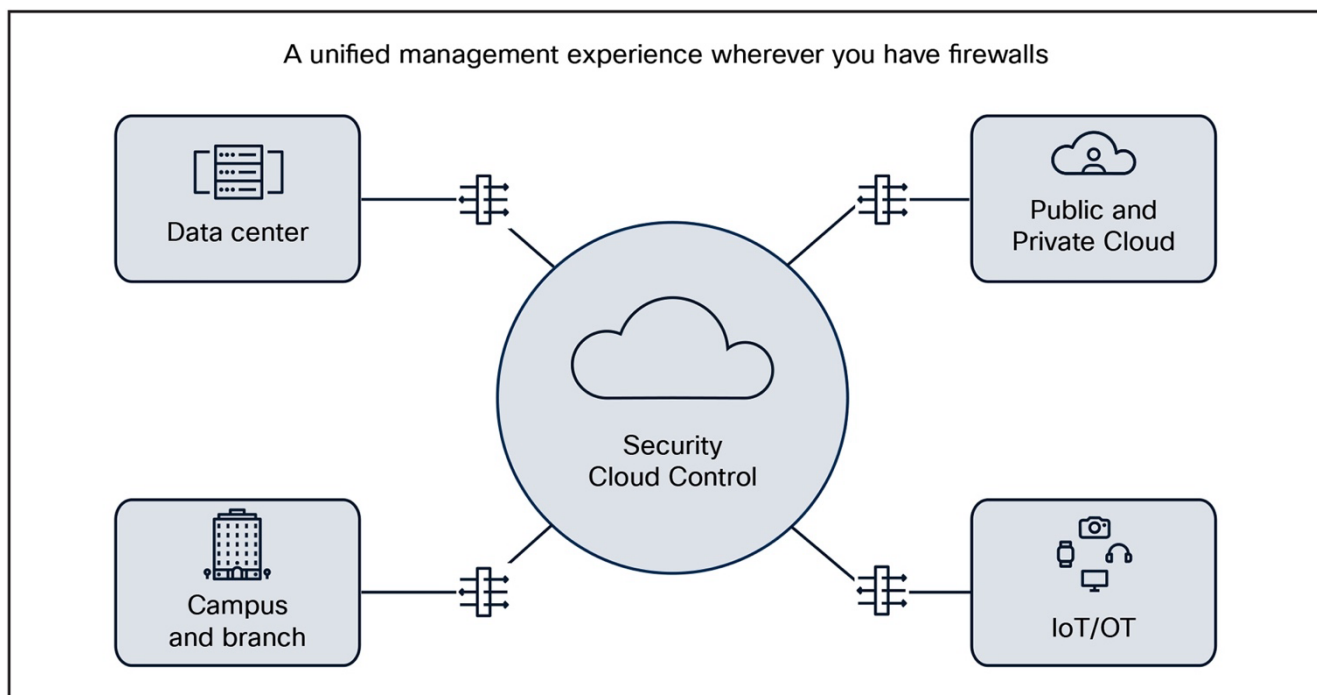


Рис.2.1. Приклад уніфікованого підходу до керування фаєрволами в різних середовищах (централізоване керування)

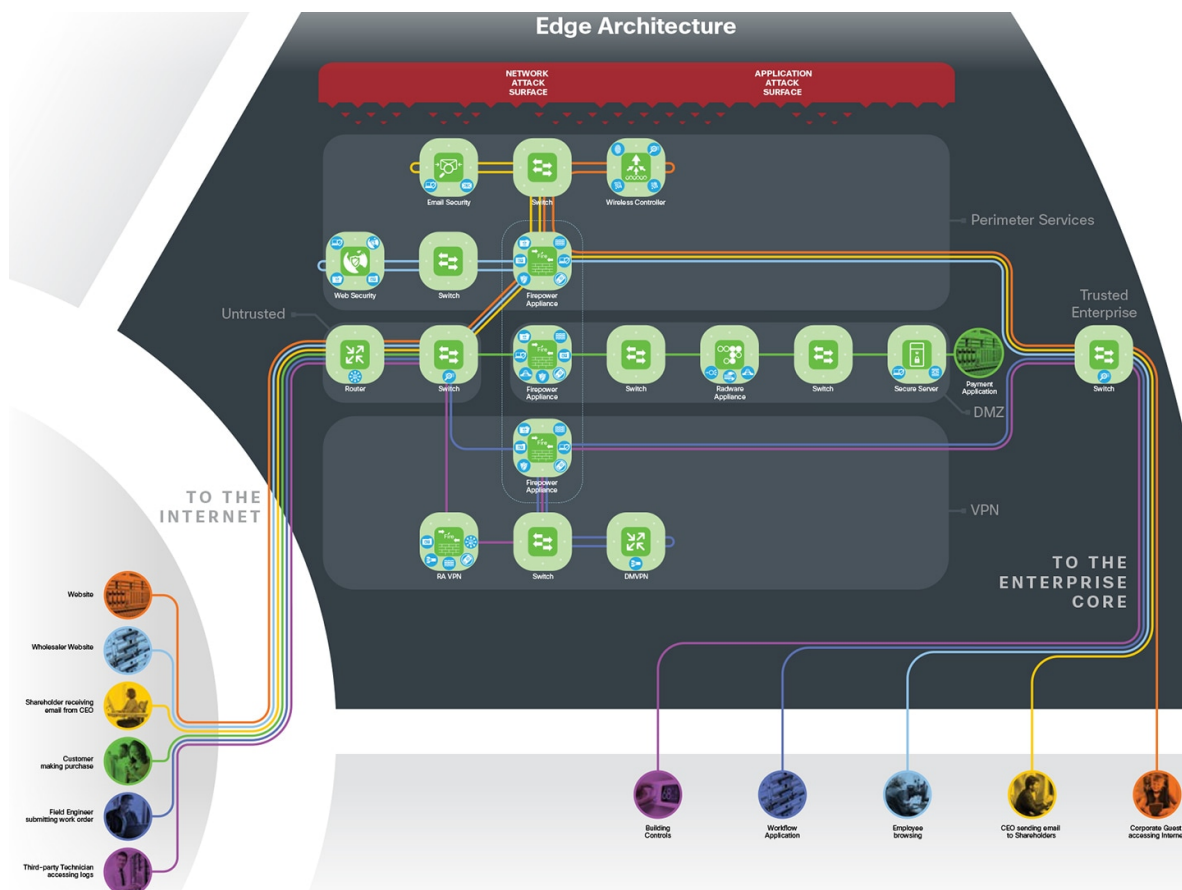


Рис.2.2. Логічне розміщення засобів захисту в архітектурі Secure Edge (периметр, DMZ, VPN), де фаєрвол є базовою контрольованою точкою інспекції

Ключовою ідеєю NGFW є розширення можливостей традиційного фаєрвола (який виконує стану інспекцію і фільтрацію за адресами, портами та протоколами) до рівня, де контроль спирається на зміст і контекст мережових взаємодій. Cisco описує, що традиційний фаєрвол, як правило, дозволяє або блокує трафік на основі стану, порту та протоколу й правил адміністратора, тоді як NGFW зберігає ці базові функції, але доповнює їх механізмами, необхідними для протидії сучасним загрозам, включно з атаками прикладного рівня [14]. Для організації це означає можливість формувати політики не лише у форматі дозволити TCP 443, а у форматі дозволити необхідний бізнес-застосунок або категорію сервісу за визначених умов.

На практиці політика NGFW зазвичай базується на принципі зонування: мережові інтерфейси, підмережі або сегменти групуються в зони, що відображають рівні довіри та призначення, після чого правила доступу формуються як взаємодія зона-до-зони. Такий підхід робить політики читабельними, формалізує кордони

довіри та спрощує аудит. NIST підкреслює необхідність побудови й підтримки firewall policy, оскільки саме політика визначає, який трафік є допустимим, як виконуються винятки та як забезпечується контроль змін. У випадку Secure Firewall це проявляється в систематизованому підході до правил доступу, де будь-яке розширення дозволів має бути обґрунтованим бізнес-потребою, мінімізованим за обсягом та підкріпленим журналюванням.

Контроль сесій є суттєвою властивістю станового фаєрвола та продовжує бути основою NGFW. Під контролем сесій слід розуміти відстеження стану мережеских з'єднань, коректності послідовності пакетів, часу життя сесій і відповідності трафіку очікуваним шаблонам. Це забезпечує можливість блокувати або обмежувати нетипові мережескі взаємодії, які можуть свідчити про спроби обходу політик, сканування або підготовку до атаки. Оскільки NGFW доповнює становий контроль ідентифікацією застосунків, з'являється можливість коректніше обмежувати довготривалі або високоризикові сесії (наприклад, тунелювання всередині дозволених протоколів), що підвищує якість мережескої гігієни та зменшує канали прихованого обміну даними.

Журналювання та подієва телеметрія є необхідною умовою практичного застосування політик. Сам факт блокування або дозволу трафіку не має достатньої цінності без подальшого аналізу, кореляції, реагування та аудиту. З позиції керованості безпеки журнали дозволяють підтвердити виконання політик доступу, відстежити аномалії, відновити ланцюжок подій під час інциденту й оцінити ефективність налаштувань. NIST окремо наголошує на необхідності управління фаєрволами як процесу, що включає супровід, тестування та контроль змін, а не одноразову конфігурацію. Для Secure Firewall це означає практику керування правилами як життєвим циклом: створення, обґрунтування, тестування, застосування, моніторинг наслідків, періодичний перегляд і оптимізація.

Фільтрація трафіку є базовою функцією фаєрвола, але її значення виходить за межі простого блокування портів. У сучасній мережі фільтрація має реалізовувати політику доступу, тобто формалізовані правила того, які суб'єкти (користувачі, системи, сегменти) можуть взаємодіяти з якими об'єктами (сервіси, підмережі, застосунки) і за яких умов. У визначенні NIST акцент зроблено на

контролі потоків трафіку між мережами або вузлами з різними безпековими профілями, що прямо відповідає задачі розмежування доступу.

Для організації практична цінність керування доступом на фаєрволі полягає у зменшенні площі атаки. Якщо публікація сервісів або внутрішні взаємодії не обмежені політикою, будь-яка компрометація одного вузла відкриває широкий спектр шляхів для ескалації та латерального переміщення. Водночас грамотно сформована політика зони-до-зони дозволяє обмежити взаємодії лише тими потоками, які необхідні для бізнес-процесів.

Cisco підкреслює, що NGFW забезпечує не тільки доступ-контроль, але й здатність блокувати сучасні загрози, включно з атаками прикладного рівня [14]. Це важливо для фільтрації, оскільки реальні атаки часто приховані в дозволеному трафіку: використання HTTP(S) як транспортного каналу, зловживання API, маскування команд і контролю під легітимні запити. У таких умовах ефективність контролю визначається не стільки кількістю заборонених портів, скільки здатністю коректно розпізнавати дозволений бізнес-трафік і відсікти небезпечні варіації взаємодій.

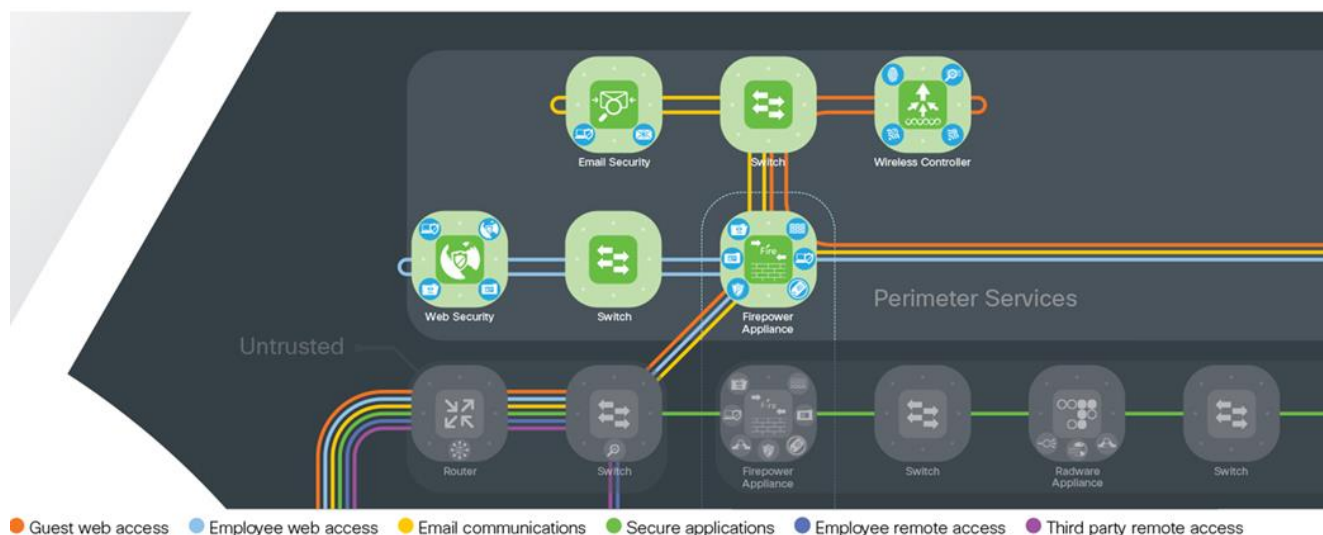


Рис.2.3. Архітектура Perimeter Services як місця застосування фаєрволу та інспекції трафіку на межі з недовіреним середовищем

Інтегровані механізми IDS/IPS є однією з характеристик NGFW, на якій робиться акцент у визначенні Cisco: NGFW включає інтегроване запобігання вторгненням [14]. У прикладному значенні IDS/IPS виконує задачу виявлення та

блокування атак, що мають виражені мережеві ознаки: експлойти протоколів, аномальні послідовності запитів, відомі шаблони шкідливих навантажень, спроби сканування та підбору.

В архітектурному описі Cisco SAFE у контексті edge-рівня прямо зазначається, що intrusion prevention забезпечує блокування атак на основі сигнатур та аналізу аномалій, а також є відповіддю на загрози, пов'язані з черв'яками, вірусами й іншими техніками [16]. Це важливо з методичної точки зору, тому що підкреслює: IPS не замінює політику доступу, а доповнює її. Якщо політика визначає, який трафік дозволений у принципі, то IPS аналізує дозволений трафік на предмет ознак атаки, підвищуючи стійкість до загроз, що використовують легітимні канали.

Задача запобігання експлуатації вразливостей полягає у зменшенні ймовірності успішного виконання атаки до моменту, коли вразливість буде усунута організаційними або технічними заходами (патчинг, зміна конфігурації, ізоляція сервісу). У реальних умовах усунення вразливостей завжди має часовий лаг, тому мережеві компенсувальні контрзаходи у вигляді IPS часто застосовуються як тимчасова або додаткова лінія оборони. Водночас слід враховувати, що якість IPS залежить від коректності налаштувань, актуальності правил детекції, контролю хибних спрацювань і узгодженості з політикою доступу. Саме тому керування IPS має включати постійний моніторинг подій і налаштування, а не бути разовим увімкненням. Такий підхід узгоджується з рекомендаціями NIST щодо необхідності постійного управління фаєрволами та їх політиками.

Контроль застосунків є однією з головних відмінностей NGFW від традиційного фаєрвола. Cisco прямо зазначає, що NGFW включає application awareness and control, тобто здатність бачити та блокувати ризикові застосунки [14]. Для організації це означає перехід від керування мережевими атрибутами до керування бізнес-діяльністю у мережі: які саме сервіси використовуються, чи відповідають вони політикам, чи не створюють каналів обхідного доступу або витоку даних.

Cisco Secure Firewall у матеріалах оглядового рівня акцентує можливість видимості великої кількості застосунків, що дає змогу точніше ідентифікувати

трафік і застосовувати політики контролю [15]. З практичної точки зору контроль застосунків закриває кілька важливих задач. По-перше, зменшується ризик використання небажаних сервісів, які можуть містити підвищені загрози (тіньові месенджери, несанкціоновані файлообмінники, проксі/тунелі). По-друге, знижується ймовірність обходу політик через використання дозволених протоколів як контейнера для забороненого функціоналу, наприклад, коли всередині HTTPS трафіку приховується небажана взаємодія. По-третє, з'являється можливість формалізувати й контролювати політики використання Інтернету та корпоративних сервісів не на рівні загальних заборон, а на рівні конкретних категорій трафіку та застосунків.

Важливою методичною вимогою є узгодженість контролю застосунків із бізнес-процесами. Якщо політики формуються без розуміння операційних потреб, вони або будуть надто жорсткими, що призведе до обходів і деградації довіри до контролів, або надто м'якими, що не дасть ефекту. Тому контроль застосунків має супроводжуватися інвентаризацією сервісів, визначенням дозволених і заборонених категорій, процесом погодження винятків і періодичним переглядом. У цій частині знову актуальними є принципи NIST щодо побудови політик і їх управління як процесу.

Захищене з'єднання віддалених користувачів і майданчиків є однією з найтипівіших і найкритичніших задач у мережах організацій, особливо за умов гібридної роботи, географічної розподіленості та співпраці з підрядниками. В архітектурному описі Cisco SAFE прямо вказано, що VPN layer з'єднує віддалені місця і людей, які використовують недовірені публічні з'єднання, та потребує криптографічних механізмів для захисту, а також що виділяються два типи VPN-з'єднань: site-to-site і remote access.

У цьому контексті Cisco Secure Firewall може виконувати роль VPN-шлюзу, через який реалізуються тунелі між філіями/майданчиками, захист каналів до партнерів або підключення віддалених користувачів. При цьому VPN не слід розглядати як окрему функцію, відірвану від політик доступу. Безпека VPN визначається не лише фактом шифрування, а й тим, які ресурси стають доступними після встановлення тунелю, як виконується автентифікація, чи застосовується

розмежування доступу до сегментів, як контролюється трафік всередині тунелю та як ведеться журналювання. Cisco SAFE у розділі про VPN layer підкреслює, що цей шар має основні можливості безпеки та інспекції, необхідні для захисту компанії, а також що доступ віддалених користувачів потребує аутентифікації й політик контролю, інтегрованих з ресурсами автентифікації організації.

Таким чином, VPN у складі Secure Firewall доцільно розглядати як механізм безпечного транспорту, який обов'язково доповнюється політиками: визначенням дозволених напрямків доступу, контролем сервісів, інспекцією трафіку та моніторингом подій. Це особливо важливо для remote access сценарію, де ризики значною мірою пов'язані з компрометацією кінцевих пристроїв, фішингом облікових даних або використанням незахищених мереж доступу.

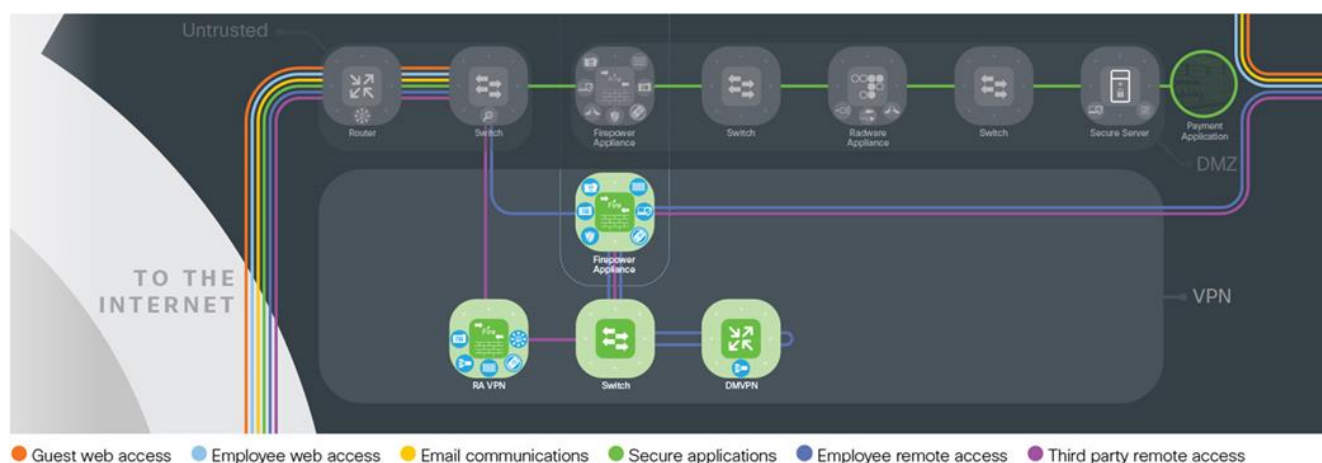


Рис.2.4. Приклад виділення VPN шару в Secure Edge

Окремою групою функцій є забезпечення централізованої видимості та контрольованості. У практичній експлуатації фаєрвол є не лише пристроєм блокування, а й джерелом телеметрії, на основі якої формується розуміння стану безпеки, виявляються інциденти та перевіряється дотримання політик. Cisco в матеріалах щодо Secure Firewall підкреслює напрям уніфікованого керування, коли фаєрволи можуть управлятися з єдиного інтерфейсу в різних середовищах розгортання, а також важливість централізованого менеджменту для підвищення операційної ефективності [15]. У архітектурному сенсі це означає, що політики застосовуються узгоджено, зміни відстежуються, а інциденти аналізуються з урахуванням контексту.

Централізована видимість подій включає принаймні три аспекти. Перший аспект полягає у збиранні журналів і подій доступу, блокувань, спрацювань IPS, змін конфігурації та адміністративних дій. Другий аспект пов'язаний із кореляцією та пріоритизацією: обсяг телеметрії у великих мережах є значним, тому важливо виділяти події, що мають ознаки інциденту або порушення політики. Третій аспект стосується доказовості та аудиту: у випадку розслідування інциденту необхідно відтворити часову послідовність подій, визначити, які правила спрацювали, хто вносив зміни та чи відповідали вони процедурі.

NIST у своїх рекомендаціях розглядає управління фаєрволами як цикл, що включає підбір, налаштування, тестування, розгортання та постійне адміністрування, підкреслюючи значення політик і контролю експлуатації. Звідси випливає, що централізоване керування та аудит адміністраторів не є додатковою опцією, а є необхідним елементом надійності безпекового контролю. Якщо немає прозорості змін і можливості перевірити їх вплив, зростає ризик конфігураційних помилок, надмірних дозволів, неконтрольованих винятків і деградації політик.

Узагальнюючи, Cisco Secure Firewall доцільно визначати як мережевий контрольний засіб, що виконує роль бар'єра між зонами з різним рівнем довіри та реалізує політики доступу, інспекцію трафіку й підтримку керованості безпеки. Його призначення розкривається через периметровий захист і внутрішню сегментацію, що відповідає підходам до зниження ризиків компрометації та локалізації інцидентів. Концепція NGFW у даному випадку проявляється в поєднанні станового контролю, ідентифікації застосунків, інтегрованого запобігання вторгненням і використання джерел загрозової інформації, що дозволяє протидіяти сучасним атакам, які маскуються під легітимні протоколи. Додаткову практичну цінність забезпечують VPN-сценарії (site-to-site і remote access) як основа безпечної взаємодії з віддаленими майданчиками та користувачами, а також централізована видимість подій і аудит адміністративних дій, без яких неможливе системне управління політиками та доказовість у розслідуваннях.

2.2. Основні компоненти архітектури Cisco Secure Firewall

Архітектура Cisco Secure Firewall доцільно розглядати як сукупність взаємопов'язаних компонентів, які забезпечують проходження трафіку через пристрій із застосуванням політик безпеки, централізоване керування конфігураціями та подіями, а також підтримку різних режимів функціональності (сучасний стек NGFW або спадковий фаєрвол/VPN). У практичному розгортанні це реалізується через розділення на площину даних (data plane), площину керування (control/management plane) та виконавче середовище пристрою (FTD або ASA), що разом формують повний цикл: політика → застосування → телеметрія/події → кореляція/аудит → інтеграція із зовнішніми системами.

Площина даних відповідає за безпосереднє оброблення мережевого трафіку, що проходить через Cisco Secure Firewall, та за застосування правил контролю доступу і механізмів інспекції. На цьому рівні пристрій виступає одночасно:

- шлюзом між мережевими зонами (наприклад, Internet ↔ DMZ ↔ LAN або сегментація між VLAN/підмережами),
- точкою примусового виконання політик (policy enforcement point),
- сенсором, який формує події безпеки й телеметрію для подальшого аналізу.

У межах NGFW ключовою ідеєю є те, що рішення не обмежується статичною фільтрацією IP/портів, а застосовує політики на рівні контексту з'єднань, сервісів та поведінкових ознак трафіку: визначення застосунків, контроль сесій, інспекція корисного навантаження (де це дозволено політикою), а також формування подій про спроби атак і аномалії. При цьому ефективність площини даних напряду залежить від того, як у площині керування описані правила й які об'єкти/зони/винятки створені для інфраструктури.

З погляду поділу відповідальностей, площина даних реалізує виконання політик і збір результатів інспекції, а всі рішення щодо того, які саме правила потрібно застосувати, централізовано задаються в системі керування (FMC) і доставляються на пристрої. Це дозволяє зберігати єдині стандарти контролю доступу та однотипну реєстрацію подій у розподілених розгортаннях [17].

Площина керування побудована навколо Cisco Secure Firewall Management Center (FMC) як централізованого засобу адміністрування. FMC виконує роль єдиного пункту, де:

- створюються та супроводжуються політики,
- здійснюється розгортання політик на керовані пристрої,
- збираються події, дані виявлення (discovery) та статистика,
- забезпечується моніторинг стану (health) і аудит адміністративних дій.

Принципова логіка взаємодії FMC з керованими пристроями полягає у двосторонньому захищеному каналі зв'язку: FMC передає політики та конфігурації, а пристрої повертають події, дані виявлення і статистику роботи. Це базова модель, яка дозволяє не змішувати виконання політики (на фаєрволі) та її життєвий цикл (у FMC), зменшуючи ризик локально неконсистентних налаштувань [17].

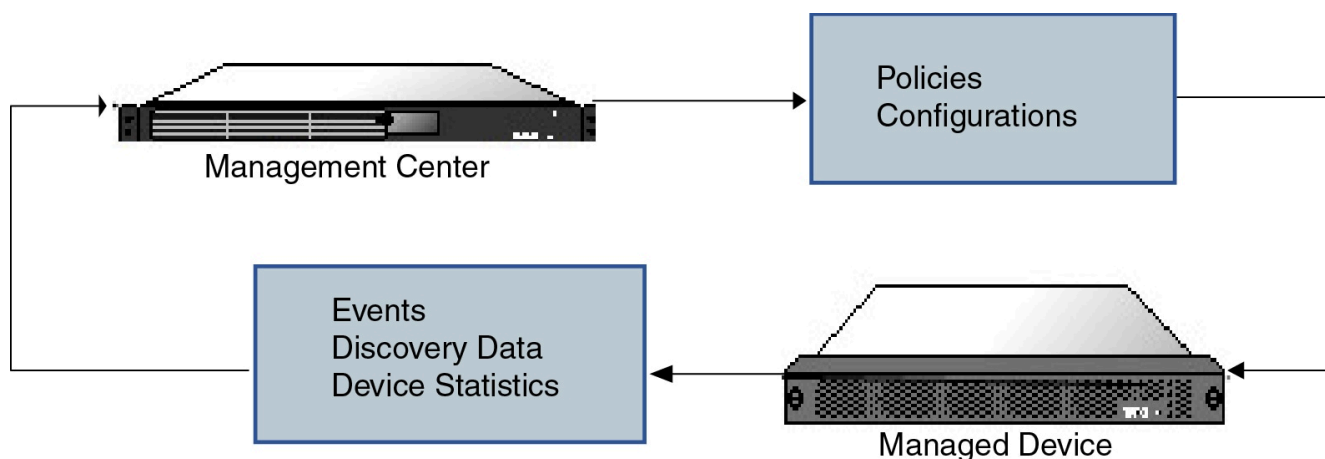


Рис. 2.5. Схема обміну даними між FMC та керованим пристроєм

Окремо важливо, що площина керування включає не лише створення правил доступу, а й операційні функції: централізовані оновлення, керування об'єктами/шаблонами, контроль стану пристроїв та подій, а також експорт даних назовні через інтеграційні механізми. Зокрема, FMC описується як централізований менеджер подій і політик для Secure Firewall Threat Defense і суміжних функцій безпеки, а також як компонент, що підтримує інтеграції та сценарії передачі подій у зовнішні платформи (наприклад, SIEM) через стандартні механізми й API [18].

Архітектурно управління пристроями передбачає наявність менеджмент-з'єднання між FMC та Secure Firewall. Для цього використовується захищений канал, який застосовується і для доставки політик, і для повернення подій.

У межах типового проектування мережі менеджменту практично важливими є два рішення:

1. чи використовувати один менеджмент-інтерфейс (де керування та події йдуть одним шляхом),
2. чи розділяти менеджмент-трафік і event-трафік (де події/журнали можуть бути винесені на окремий інтерфейс/шлях).

Такі варіанти потрібні, щоб масштабувати збір подій, розвантажити канали, ізолювати керування від продуктивного трафіку та зменшити вплив інцидентів у робочих сегментах на стабільність адміністрування.

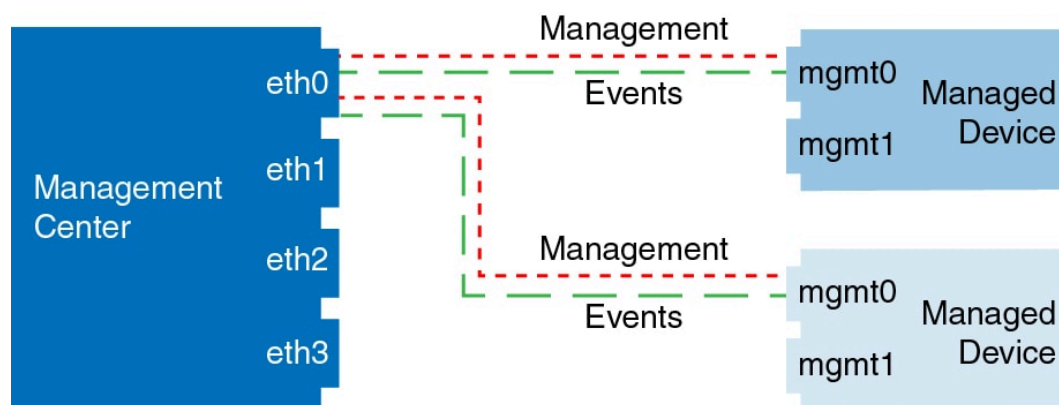


Рис. 2.6. Приклад: один менеджмент-інтерфейс на FMC (eth0) і стандартні менеджмент-інтерфейси на керованих пристроях

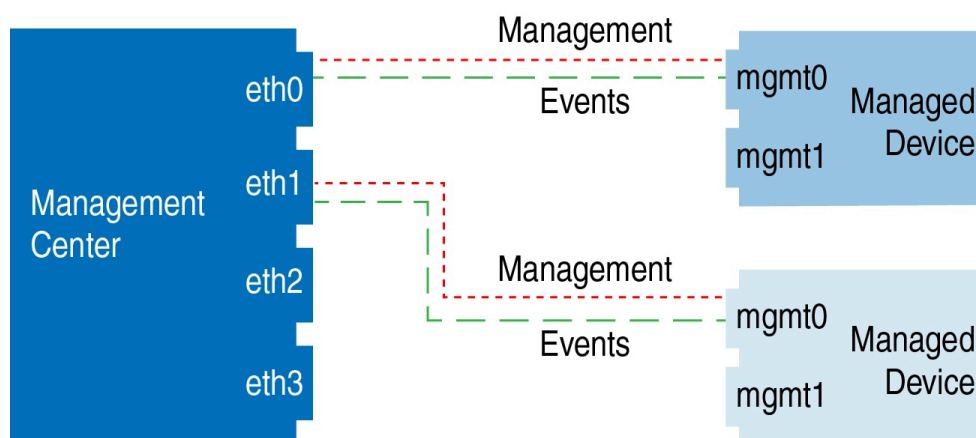


Рис. 2.7. Приклад: декілька менеджмент-інтерфейсів на FMC для підключення до різних мереж керування

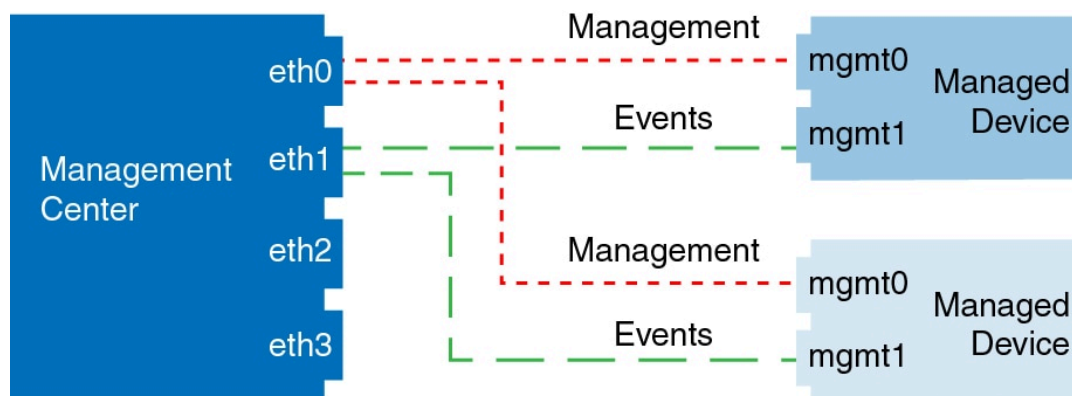


Рис. 2.8. Приклад: виділений інтерфейс/шлях для event-трафіку (розділення management та events)

У контексті безпеки адміністрування важливо, що в документації наголошується на захищеному характері каналу керування (шифрування) та на необхідності забезпечення стабільного менеджмент-шляху, оскільки порушення доступності цього каналу ускладнює централізований контроль і збір подій [17].

У межах Cisco Secure Firewall пристрої можуть працювати в різних програмних режимах, що визначає набір доступних можливостей та підхід до керування.

FTD (Firepower Threat Defense) розглядається як основний сучасний стек NGFW, де функції фаєрвола, інспекції та керування політиками інтегровані в єдину логіку. Це спрощує реалізацію сценаріїв, де потрібні одночасно сегментація, IDS/IPS-можливості, контроль застосунків, кореляція подій та централізована видимість через FMC.

ASA (Adaptive Security Appliance) доречно описувати як класичний фаєрвол/VPN-підхід, який зустрічається в організаціях як спадкове рішення або як середовище, з якого виконують міграцію до FTD для уніфікації NGFW-функцій і централізованого управління. Практичний сенс згадки ASA у розділі архітектури полягає в поясненні сумісності, різниці підходів та організаційного процесу переходу.

Процедурно міграція ASA до FTD у Cisco описується як окремий керований процес із визначеними передумовами, що підкреслює: ASA і FTD є різними

виконавчими середовищами, а не просто різними наборами галочок у тій самій системі [20].

Для коректного опису FTD важливо показати, що пристрій має внутрішню структуру, де управління та частина діагностичних функцій реалізуються через логічні компоненти. У матеріалах Cisco наведено приклад еволюції підходу до менеджменту: у старіших реалізаціях використовувалось розділення діагностичного логічного інтерфейсу та менеджмент-логіки, тоді як у новіших версіях реалізовано зближення (merge) для спрощення експлуатації [19].

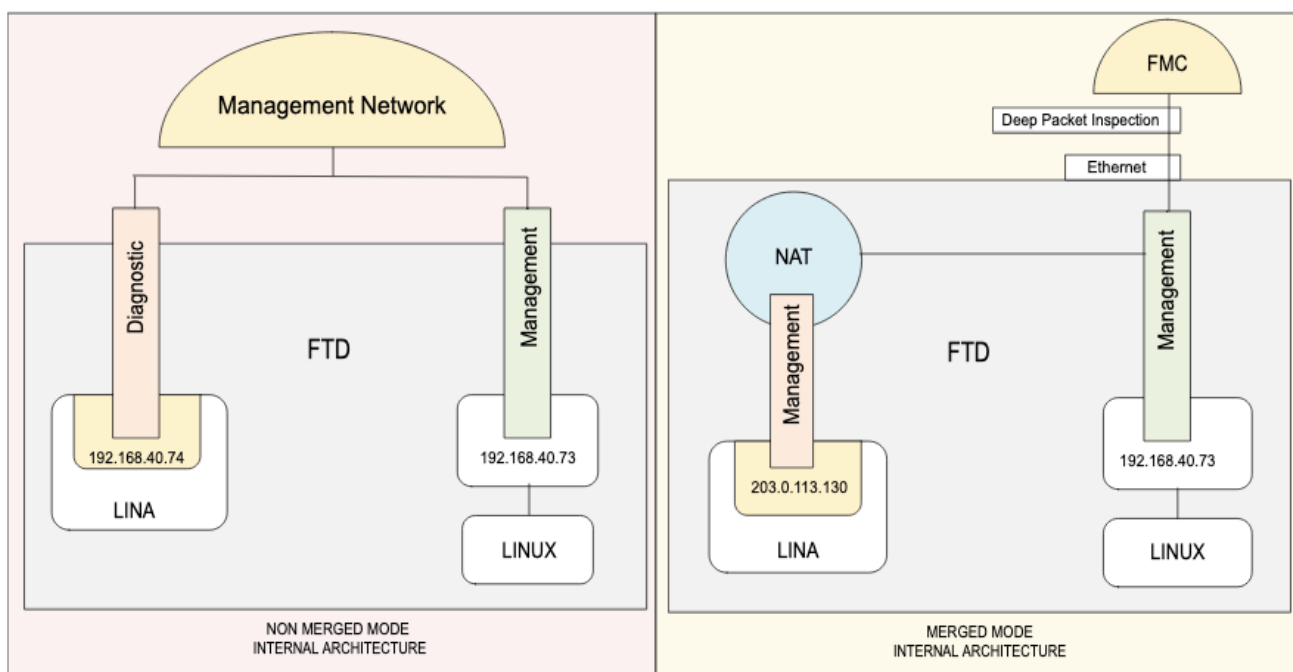


Рис. 2.9. Внутрішня архітектура FTD до та після об'єднання management і diagnostic

Рис.2.9. демонструє, що менеджмент-мережа та доступність каналу керування не є лише організаційною домовленістю, а відображаються у внутрішній реалізації пристрою та його режимах роботи [19].

Логіка взаємодії компонентів: життєвий цикл політики та подій

Узагальнений цикл роботи архітектури Cisco Secure Firewall у керованому (FMC) сценарії доцільно описувати як послідовність операцій:

1. Моделювання політики в FMC. Адміністратор формує зони/мережеві об'єкти/правила, а також параметри інспекції та журналювання. FMC виступає

точкою, де політика набуває стандартизованого вигляду і може бути масштабована на декілька пристроїв.

2. Доставка політики на пристрої. Політики й конфігурації передаються з FMC на керовані Secure Firewall у межах захищеного менеджмент-каналу (двостороння взаємодія).

3. Застосування політики в площині даних. Пристрій аналізує трафік згідно з отриманими правилами, виконує дозволи/заборони, застосовує інспекцію, формує журнали про спрацювання правил і підозрілі події.

4. Повернення подій і телеметрії в FMC. Події, дані виявлення (discovery) та статистика надходять назад у FMC, що відображено як базова модель обміну даними.

5. Кореляція, моніторинг, аудит. FMC агрегує дані та надає засоби перегляду контексту, стану пристроїв і керованих політик; додатково підкреслюється роль FMC як централізованого менеджера подій/політик та платформи інтеграції.

6. Інтеграція із зовнішніми системами. За потреби події експортуються в SIEM або інші системи моніторингу/реагування через доступні механізми інтеграції (наприклад, API та стандартні канали передавання подій), що описується як один зі сценаріїв використання FMC [18].

У практичних мережах архітектура Cisco Secure Firewall зазвичай реалізується в одному або кількох шаблонах розміщення, які визначають, де саме працює площина даних і як організований менеджмент:

- Периметровий захист. Один або кластер фаєрволів на межі організації контролює зовнішні з'єднання, публічні сервіси (DMZ) та канали VPN.
- Міжсегментний контроль east-west. Фаєрволи встановлюються між ключовими VLAN/сегментами, щоб реалізувати мікросегментацію та зменшити радіус поширення атаки.
- Дата-центр/філії. У філіях пристрій забезпечує локальний контроль трафіку та VPN-зв'язність, а централізоване керування й видимість реалізуються через FMC, що дозволяє уніфікувати політики для географічно розподілених майданчиків.

Для всіх схем спільним є те, що централізоване управління спрощує підтримання однакових принципів доступу, журналювання та контролю змін, а менеджмент-мережа має бути спроектована як стійкий канал, від якого залежить життєвий цикл політик і збір подій.

2.3. Інтеграція Cisco Secure Firewall

Інтеграції для Cisco Secure Firewall потрібні не як додаткова опція, а як спосіб побудувати єдиний контур спостереження та реагування: події з NGFW мають потрапляти в системи кореляції, збагачуватися контекстом і перетворюватися на інциденти, з якими зручно працювати аналітику SOC. На практиці інтеграції можна умовно поділити на два напрями: інтеграція з хмарними сервісами Cisco для консолідації подій та керування (зокрема Cisco XDR), а також інтеграція з SIEM-платформами для довгострокового зберігання, пошуку, кореляції та звітності (Splunk, QRadar та інші). Обидва напрями можуть використовувати різні транспортні механізми, але спільна мета одна — уніфіковане отримання та обробка телеметрії безпеки [21].

Cisco XDR у цьому ланцюгу виступає як хмарний рівень, який агрегує та корелює події від різних джерел телеметрії, зводить окремі спрацювання до інцидентів і допомагає пріоритезувати реагування. Для Cisco Secure Firewall (Threat Defense) документація описує два базові методи підключення до Cisco XDR: пряму інтеграцію та інтеграцію через syslog. Вибір методу залежить від версії ПЗ, вимог до доступу в інтернет, а також того, які типи подій потрібно передавати [22].

Пряма інтеграція логічно виглядає як канал, де керуючий компонент (FMC/Management Center) та керовані пристрої Threat Defense забезпечують передавання керуючих і подієвих даних у Cisco Security Cloud (через компоненти Cisco Security Services Exchange), після чого події стають доступними у Cisco XDR як інциденти для SOC-аналітика. Такий підхід орієнтований на більш тісну зв'язку з хмарними можливостями Cisco та уніфіковану обробку подій.

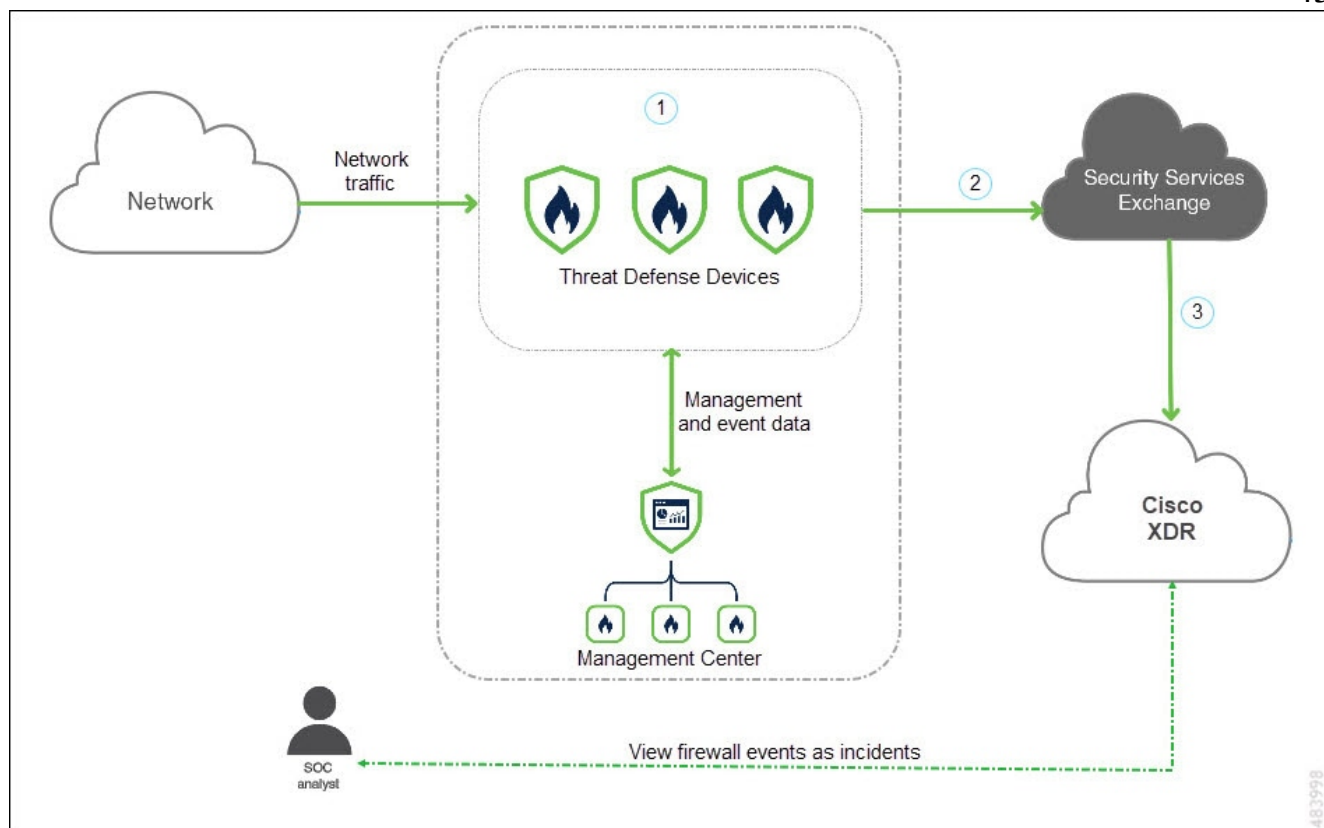


Рис.2.10. Схема прямої інтеграції Cisco Secure Firewall з Cisco XDR

Інтеграція через syslog застосовується як більш універсальний варіант, де пристрій Threat Defense генерує події та надсилає їх у хмарні сервіси Cisco з використанням syslog-ланцюга. У типовій схемі між фаєрволом і хмарию може використовуватись проміжний компонент (Cisco Security Services Proxy), який забезпечує доставку в Security Services Exchange і далі в Cisco XDR. Це важливо як компромісний варіант у сценаріях, коли потрібен контроль вихідних з'єднань або спрощене підключення.

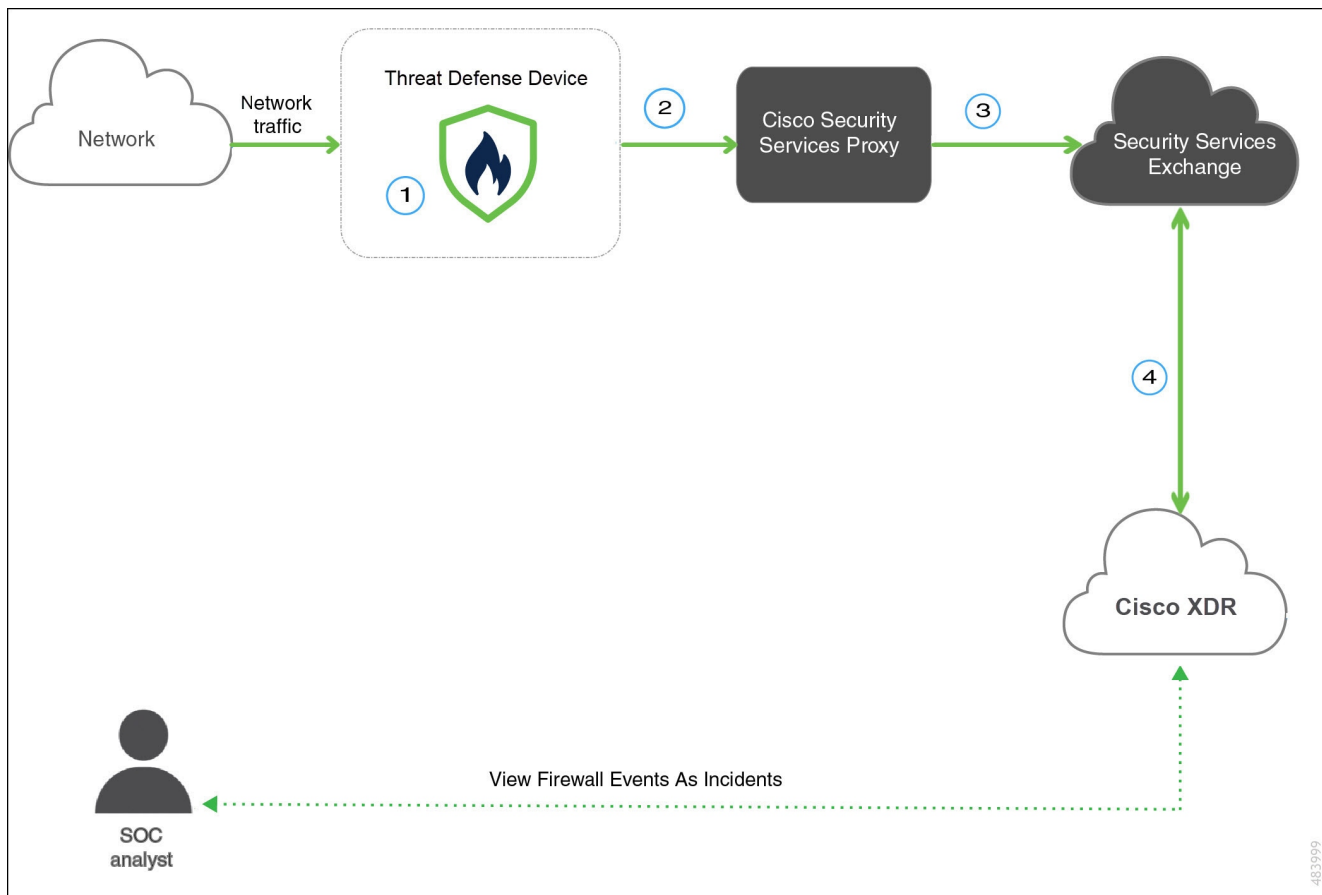


Рис.2.11. Схема інтеграції Cisco Secure Firewall з Cisco XDR через syslog

З погляду операцій SOC результат інтеграції з Cisco XDR доцільно описувати як перехід від перегляду окремих подій NGFW до роботи з інцидентами, де кореляція може включати додаткові джерела (наприклад, endpoint-телеметрію чи дані про шкідливі об'єкти) та де аналітик отримує більш цілісний контекст атаки. Окремо підкреслюється, що інтеграція з Cisco XDR є ліцензованою можливістю, а підтримувані методи передавання подій (direct або syslog) мають версійні обмеження [22].

Інтеграція із SIEM: кореляція, довгострокове зберігання, пошук і звітність

На рівні SIEM головна задача — забрати події з Secure Firewall у стандартизованому вигляді й забезпечити їх нормалізацію, пошук, кореляцію з іншими джерелами (AD/IdP, EDR, DNS, проксі, пошта тощо), а також звіти й ретеншн. Для Cisco Secure Firewall на практиці найтипівіші два підходи доставки даних у SIEM — syslog або eStreamer-потік (через інструменти/клієнти, які забирають події з FMC і передають у SIEM).

Підхід через eStreamer часто використовують там, де потрібні більш повні та збагачені події, а також підтримка широких класів івентів (мережеві з'єднання, intrusion із пакетними даними, file/malware, correlation тощо). У матеріалах Cisco Live для зв'язки Splunk + Firewall показано типову логіку: FMC виступає джерелом подій, а на стороні Splunk працює eStreamer Client Add-On, який отримує enriched events via eStreamer та віддає їх у Splunk для подальшого аналізу [23].

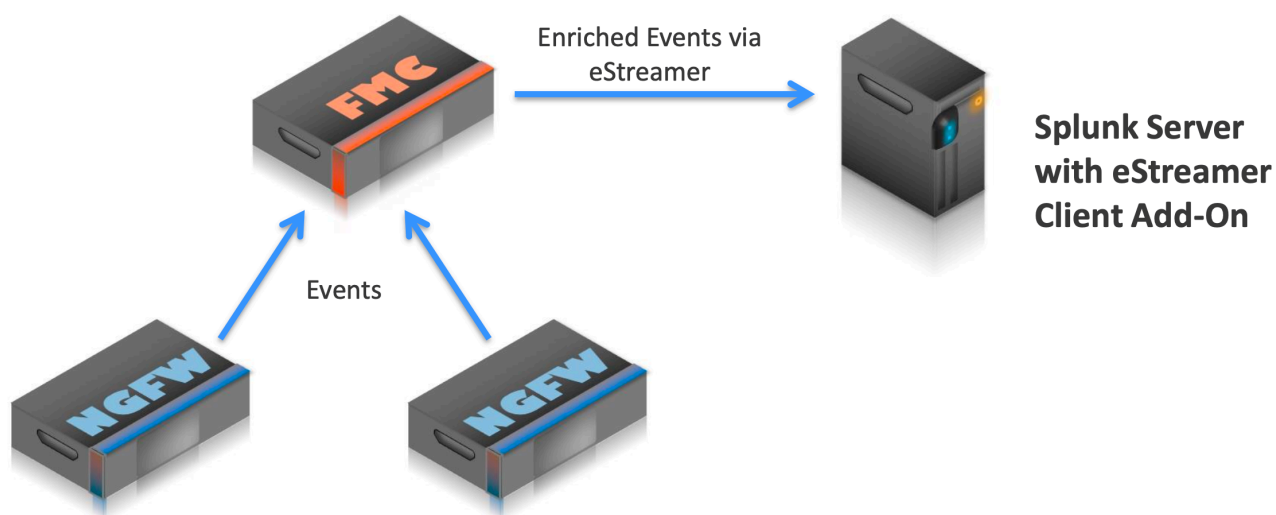


Рис.2.12. Приклад архітектури інтеграції Splunk з Cisco Secure Firewall через eStreamer

Для QRadar в офіційній документації IBM інтеграція з Cisco Firepower Management Center також описується через eStreamer: на боці FMC створюються сертифікати, які імпортуються в QRadar Event Collector/Console, після чого QRadar збирає eStreamer event data та підтримує низку типів подій (зокрема intrusion, connection, malware/file, discovery та інші). Така модель інтеграції важлива для обґрунтування того, що SIEM може отримувати не лише загальні повідомлення, а структуровані категорії подій для подальшого мапінгу та кореляції [24].

У результаті SIEM-інтеграція дає практичні ефекти, які зручно формувати як задачі: побудова правил кореляції між мережевими подіями та подіями з інших систем, централізований аудит безпеки, зберігання даних для розслідувань, формування звітів для контролю ефективності політик доступу та IDS/IPS, а також можливість threat hunting по історичних даних. При цьому доцільно окремо

зазначати, що вибір механізму доставки (syslog або eStreamer) впливає на повноту подій, витрати на обробку та вимоги до продуктивності інфраструктури логування.

На рівні процесу безпеки інтеграції слід трактувати як послідовний конвеєр: Secure Firewall генерує телеметрію й застосовує політики, FMC централізовано керує й акумулює події, далі події або передаються в Cisco XDR для інцидент-орієнтованої роботи SOC, або надходять у SIEM для кореляції, ретеншну та аналітики (а в зрілій моделі — одночасно в обидва контури з чітким розподілом ролей). Концептуально Cisco XDR зводить фокус до оперативного пріоритезованого реагування на інциденти, тоді як SIEM закриває задачі широкої кореляції, довгого зберігання, комплаєнсу й аналітики.

3 ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ РІШЕННЯ CISCO

3.1. Варіант розгортання Cisco Secure Firewall у корпоративній мережі

У межах варіанту розгортання мережа організації розділяється на щонайменше три логічні зони: зовнішній сегмент провайдера, внутрішній сегмент локальної мережі та окремий сегмент керування. Прикордонний міжмережевий екран Cisco Secure Firewall (наприклад, серії 3100 з образом Threat Defense) встановлюється на периметрі та забезпечує контроль проходження трафіку між зовнішнім і внутрішнім сегментами, а також централізоване керування через Secure Firewall Management Center (FMC). Архітектурний принцип полягає в тому, що робочий (продуктивний) трафік проходить через інтерфейси даних, тоді як керування, оновлення та реєстрація виконуються через виділений інтерфейс керування і окрему мережу керування, що зменшує ризик впливу подій у користувацьких сегментах на керуючу площину.

На початковому етапі визначається місце встановлення пристрою, схема підключень і параметри мережі керування. Для FMC обирається вузол, який має стабільний доступ до мережі керування та, за потреби, доступ до Інтернету для оновлень. Для firewall визначаються як мінімум адреса інтерфейсу керування, шлюз керування, DNS та синхронізація часу. Синхронізація часу вважається обов'язковою умовою коректної кореляції подій і журналів, тому часові налаштування виконуються під час первинного майстра ініціалізації.

Фізичне підключення реалізується так, щоб інтерфейс Management 1/1 був під'єднаний до мережі керування, а консольний доступ був доступний для аварійних сценаріїв. Типова схема підключення для введення в експлуатацію показує паралельне використання: керуючого інтерфейсу до management-мережі, порту консолі до керуючого ПК та інтерфейсів inside/outside для трафіку даних. На рис.3.1 показано приклад, де FMC і керуючий комп'ютер знаходяться в management-сегменті, а вихід у зовнішню мережу під'єднаний окремо. Така

топология забезпечує керованість і дає можливість виконувати первинну реєстрацію та діагностику незалежно від стану політик обробки трафіку.

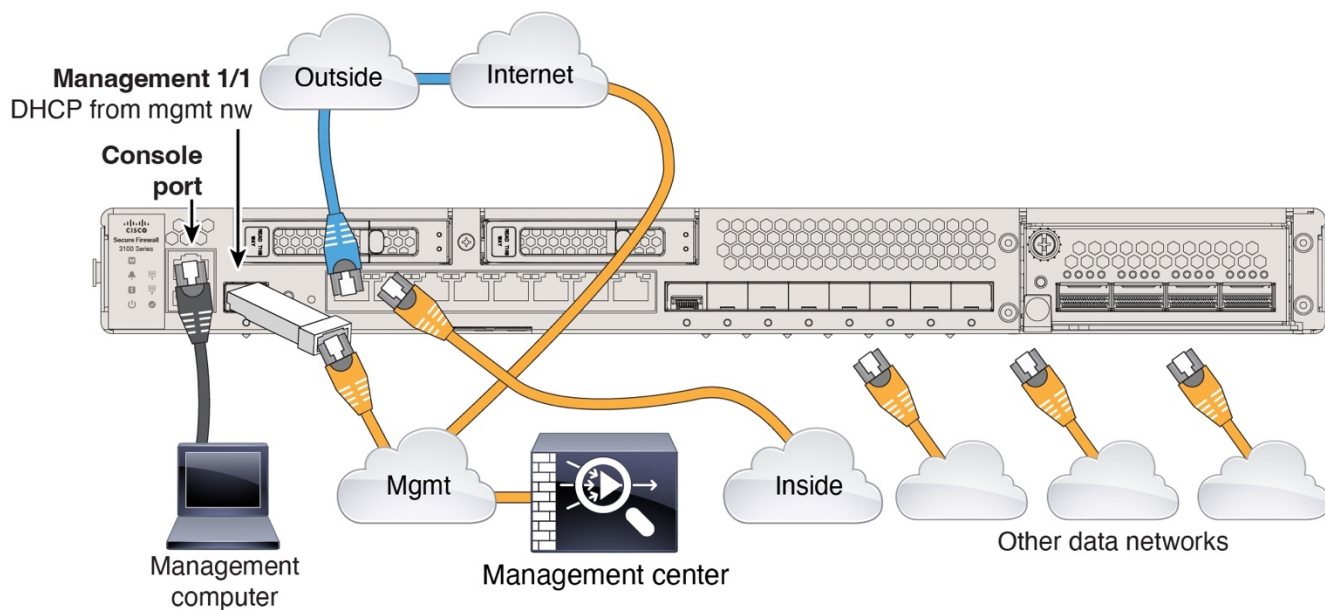


Рис.3.1. Приклад кабелювання мережі керування та підключень під час введення в експлуатацію

Після подачі живлення та перевірки апаратної готовності виконується первинна ініціалізація через локальний вебінтерфейс Secure Firewall Device Manager, який використовується саме як стартовий майстер для bootstrap-налаштувань (без побудови повноцінних політик). На цьому етапі уточнюється базова мережна зв'язність пристрою, зокрема можливість отримання адреси (DHCP або статична конфігурація), базова досяжність шлюзу та доступ до служб DNS. Узагальнений вигляд майстра, який послідовно проводить через первинні кроки, наведено на рис.3.2. Важливо, що з цього майстра зазвичай починається формування базової керуючої площини: пристрій має отримати коректні параметри часу та мережі, перш ніж його буде під'єднано до централізованого керування [25].

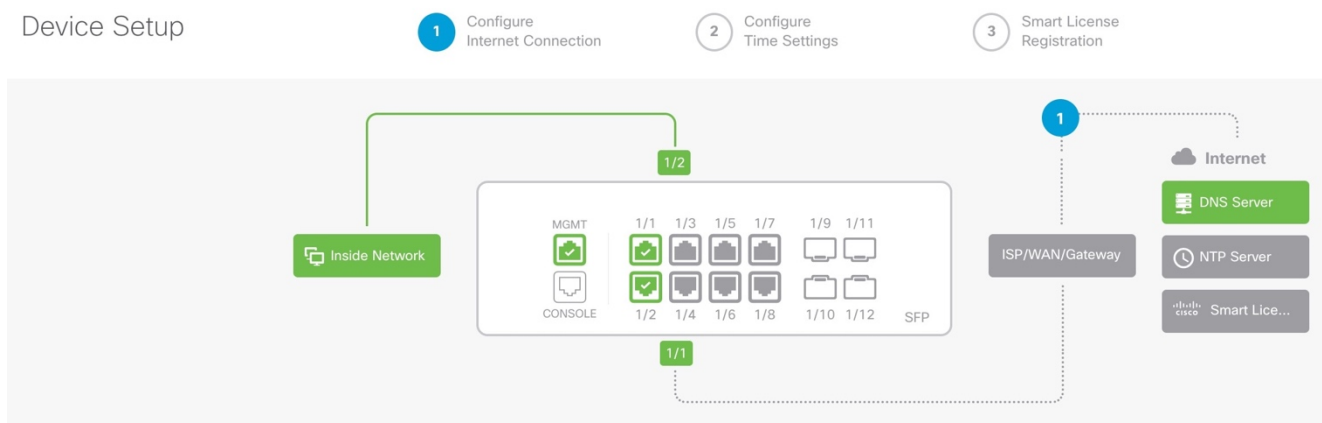


Рис.3.2. Фрагмент майстра первинного налаштування Device Setup

Налаштування часу виконується в межах первинного майстра: обирається часовий пояс, джерело NTP і перевіряється, що система коректно застосовує отримані параметри. Приклад екрану налаштувань часу наведено на рис.3.3. Роль цього кроку технічно критична, оскільки неправильний час призводить до некоректної валідації сертифікатів, розсинхронізації журналів, помилок під час реєстрації та складнощів під час розслідування інцидентів.

Time Setting (NTP)

System Time: 11:56:20AM October 03 2024 -06:00

Time Zone for Scheduling Tasks

(UTC+00:00) UTC

NTP Time Server

Default NTP Servers

Server Name

0.sourcefire.pool.ntp.org

1.sourcefire.pool.ntp.org

2.sourcefire.pool.ntp.org

NEXT

Рис.3.3. Налаштування часу (NTP) під час первинної ініціалізації

Після завершення первинної ініціалізації пристрій переводиться в режим, що дозволяє централізоване керування через FMC. На практиці це виглядає як перехід від стартового майстра до стану готовності, де пристрій очікує під'єднання до системи керування. Приклад екрана готовності показано на рис.3.4, де фіксується, що пристрій готовий до подальших конфігураційних дій. На цьому етапі принциповим є те, що подальша конфігурація пристрою (включно з об'єктами, правилами та розгортанням змін) виконується вже з FMC як з централізованої керуючої системи.

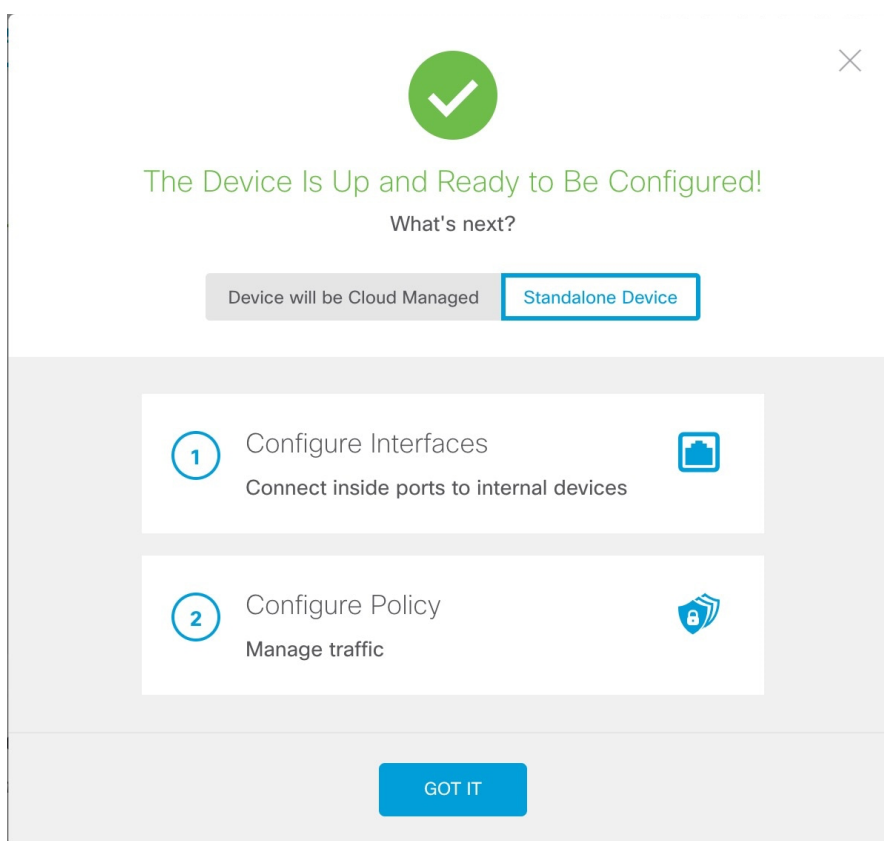


Рис.3.4. Стан готовності після первинного майстра

Далі виконується встановлення зв'язку між Threat Defense та FMC. З боку пристрою вказуються параметри FMC: адреса або ім'я, реєстраційний ключ і, за потреби, NAT ID для сценаріїв, де реєстрація проходить через трансляцію адрес або коли безпосередня маршрутизація між вузлами відсутня. Візуальний приклад сторінки, де вказуються ці параметри, наведено на рис.3.5. З технічної точки зору, реєстраційний ключ використовується як спільний секрет для встановлення довіри між керованим пристроєм та керуючим центром, а NAT ID виконує роль додаткового ідентифікатора для коректного зіставлення пристрою в складних

топологіях. Після введення параметрів ініціюється підключення, а система відображає статус з'єднання та етапи, які пройдені успішно.

Management Center/SCC Details

Do you know the Management Center/SCC hostname or IP address?

☒ Yes ☐ No

Threat Defense

 10.89.5.4
 fe80::6a87:c6ff:fea6:5480/64

→

Management Center/SCC

 10.89.5.35

Management Center/SCC Hostname or IP Address

10.89.5.35

Management Center/SCC Registration Key

.... 

NAT ID

Required when the management center/SCC hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/SCC hostname or IP address.

11204

Connectivity Configuration

Threat Defense Hostname

1120-4

DNS Server Group

CustomDNSServerGroup ▼

Management Center/SCC Access Interface

management (Management1/1) ▼

Type: Static | **IP Address:** 10.89.5.4 / 255.255.255.192 [Edit](#)

CANCEL

CONNECT

Рис.3.5. Введення параметрів підключення до FMC (Management Center Details)

Після того як з боку пристрою ініційовано під'єднання, дія продовжується у вебінтерфейсі FMC. У межах централізованого керування обирається сценарій

додавання пристрою, де як метод реєстрації використовується показаний у документації підхід через Registration key або, альтернативно, за серійним номером (в залежності від моделі та процесів постачання). Для типової локальної схеми, коли пристрій вже знаходиться в мережі керування, реєстрація через Registration key є прямим шляхом і не потребує додаткових механізмів. Приклад вибору методу наведено на рис.3.6.

Add device

1 Device registration method

2 Device details

3 Initial device configuration

Device registration method

Registration key
Identify the same one-time registration key on the device and in the management center.

Serial number
Identify the device by serial number. On the device, you don't have to configure anything (zero-touch provisioning).

Choose the initial device configuration method:

☒ **Basic**
Apply basic configuration, including the access control policy.

☐ **Device template**
Preconfigure settings using a template. A compatible **template** must exist (either a default template or one you added) before continuing.

[Cancel](#) [Next](#)

Рис.3.6. Вибір методу додавання пристрою в FMC (Add device, Device registration method)

На наступному екрані FMC запитується мінімальний набір ідентифікаційних параметрів керованого пристрою: домен (у випадку багатодоменого розгортання), IP або hostname, відображуване ім'я, реєстраційний ключ і NAT ID (якщо застосовується). Зміст цього кроку полягає в тому, що FMC отримує реквізити для встановлення каналу керування та подальшої інвентаризації можливостей пристрою. Приклад форми введення показаний на рис.3.7. Після підтвердження FMC виконує верифікацію heartbeat і, у випадку успіху, додає пристрій у список керованих.

Add device

1 Device registration method

2 Device details

3 Initial device configuration

Device details

Domain *

Global/Leaf1

Hostname or IP address

10.89.5.41

e.g. server.example.com or 192.168.1.1

Display name *

3110-1

Registration key *

....

Enter the same registration key you set on the device. This key doesn't have to be unique per device. Use alphanumeric characters (A-Z, a-z, 0-9) and the hyphen (-), between 2 and 36 characters.

Unique NAT ID

31101

Enter the same NAT ID if you set one on the device. This key needs to be unique per device. Use alphanumeric characters (A-Z, a-z, 0-9) and the hyphen (-), between 2 and 36 characters.

☐ **Analytics-only management center**

When using Security Cloud Control as your primary manager, you can use an On-Prem management center for analytics.

[Cancel](#) [Back](#) [Next](#)

Рис.3.7. Введення даних пристрою під час додавання в FMC (Device details)

Після реєстрації та появи пристрою в FMC виконується розгортання змін конфігурації на керований пристрій. Цей крок є формальною фазою переходу від стану редагування об'єктів і параметрів у FMC до стану застосування їх на пристрої. Навіть коли мова йде про базовий варіант введення в експлуатацію без детального налаштування політик, сам факт централізованого керування передбачає застосування змін через механізм Deploy. У FMC для цього використовується інтерфейс швидкого розгортання, де обирається пристрій або група пристроїв і запускається Deploy. Приклад екрану Quick Deploy показано на рис.3.8.

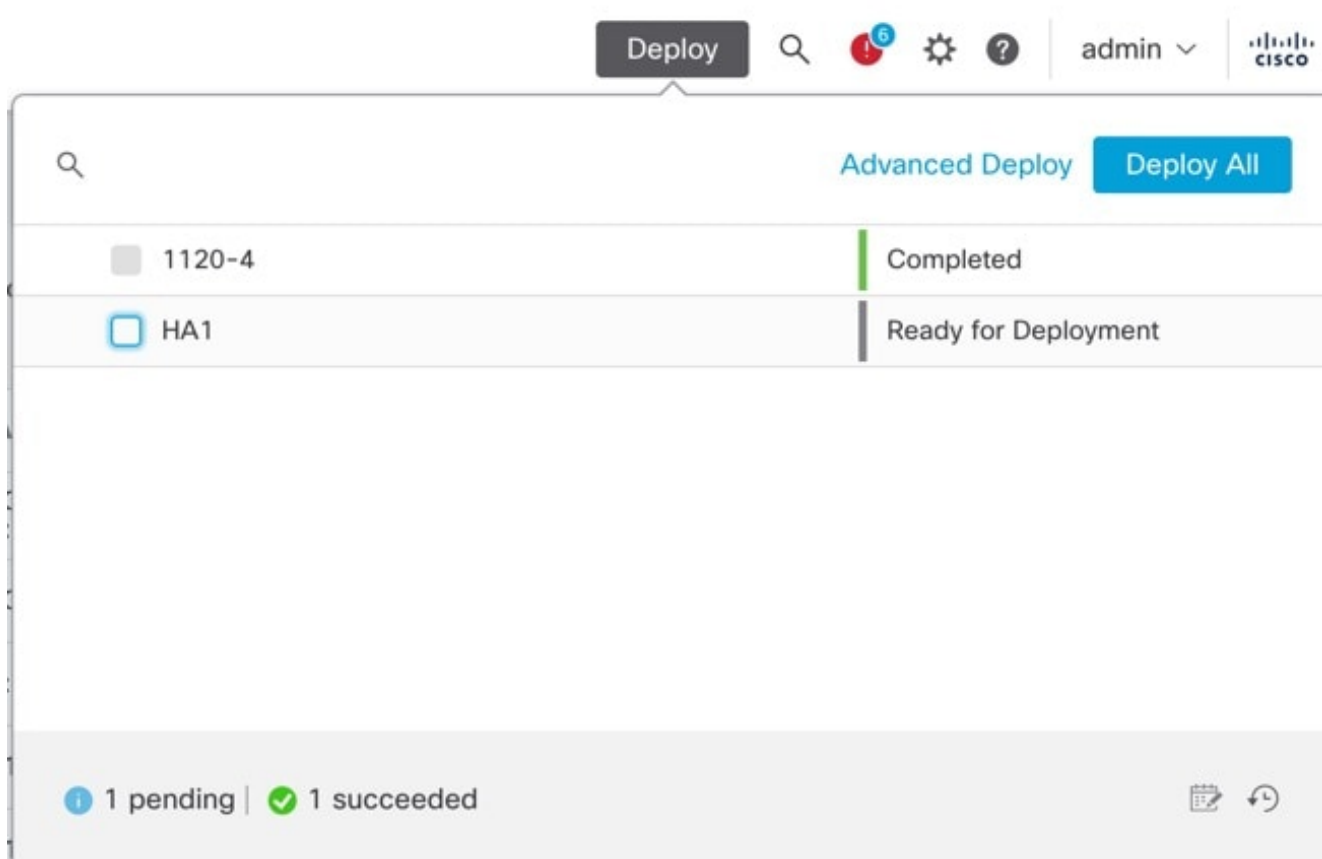


Рис.3.8. Екран Quick Deploy у FMC

У сценаріях, де важлива керованість процесу, застосовується Advanced Deploy, який дозволяє переглянути склад змін, статус готовності та службові параметри розгортання. Це корисно як мінімум для контролю того, що зміни відправляються на правильний пристрій, а також для розуміння стадій виконання. Приклад екрана Advanced Deploy наведено на рис.3.9. Такий підхід покращує відтворюваність процесу введення в експлуатацію, тому що фіксує, які конфігураційні зміни були підготовлені в FMC і коли саме вони були застосовані на пристрої.

Search using device name, user name, type, group or status							
Generate Reports							
☐ Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
> ☐ HA1	System, admin		FTD		-		Ready for Deployment
> ☐ 1120-4	System		FTD		Oct 17, 2023 10:47 ...		Ready for Deployment

Рис.3.9. Екран Advanced Deploy у FMC

Після завершення Deploy виконується перевірка стану керованості та цілісності керуючого каналу. Перевіряється, що пристрій відображається як

керований, має актуальний стан зв'язку, а також що FMC не показує помилок реєстрації або деградації. На цьому ж етапі в реальному розгортанні зазвичай виконують мінімальні перевірки мережної досяжності між management-інтерфейсами, оскільки саме через цей канал відбуваються подальші зміни та оновлення [26].

Для підвищення відмовостійкості керуючої площини може розгортатися FMC у режимі High Availability. У такому варіанті існують два вузли FMC з ролями primary та secondary, між якими синхронізуються конфігураційні дані, а у випадку відмови активного вузла відбувається перемикання керуючої ролі. З практичної позиції це зменшує ризик втрати керованості периметра під час інцидентів або технічних збоїв. У вебінтерфейсі FMC вибирається роль, вводяться параметри реєр-вузла та реєстраційні дані для зв'язування пари. Приклад сторінки, де задаються role та peer details для HA, наведений на рис.3.10. У контексті варіанту розгортання важливо, що HA стосується саме керуючої системи, а не є частиною налаштування політик; це інфраструктурний механізм забезпечення безперервності керування.

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

☐ Standalone (No High Availability)

☐ Primary

☒ Secondary

Peer Details:

After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Primary Firewall Management Center Host:

192.0.2.0

Registration Key*:

Unique NAT ID:

Register

† Either host or NAT ID is required.

484161

Рис.3.10. Налаштування High Availability для FMC (вибір ролі та параметрів peer)

У підсумку, варіант розгортання Cisco Secure Firewall для захисту комп'ютерної мережі реалізується як послідовність інфраструктурних кроків: підготовка сегменту керування і схеми підключень, первинна ініціалізація Threat Defense через стартовий майстер, встановлення коректних параметрів часу та мережі, ініціювання реєстрації пристрою до FMC через реєстраційні реквізити, додавання пристрою в FMC із заповненням ідентифікаційних полів, та застосування змін механізмом Deploy. За потреби підвищення стійкості керування додається НА для FMC як окремий інфраструктурний шар. Такий підхід забезпечує керованість периметра, відокремлення керуючого трафіку від користувацького та відтворюваність процесу введення в експлуатацію за рахунок централізованого життєвого циклу конфігурації [27].

3.2. Налаштування політик безпеки та механізмів контролю трафіку в Cisco Secure Firewall

У Cisco Secure Firewall контроль трафіку реалізується не однією налаштувальною формою, а ланцюжком політик, що послідовно застосовуються до потоку пакетів і сесій: від первинної класифікації та раннього блокування відомих загроз до детального контролю доступу, інспекції застосунків/URL і IPS-захисту. На практиці це означає, що якість захисту залежить не тільки від того, чи існує правило дозволу або блокування, а від того, як побудована політика в цілому, як визначені об'єкти (зони, мережі, сервіси), як виставлене логування, як підібрана IPS-політика та як узгоджені NAT/VPN із правилами доступу. Такий підхід дозволяє реалізувати принцип мінімально необхідних дозволів і забезпечити відтворюваність налаштувань при масштабуванні на філії/сегменти/датацентр.

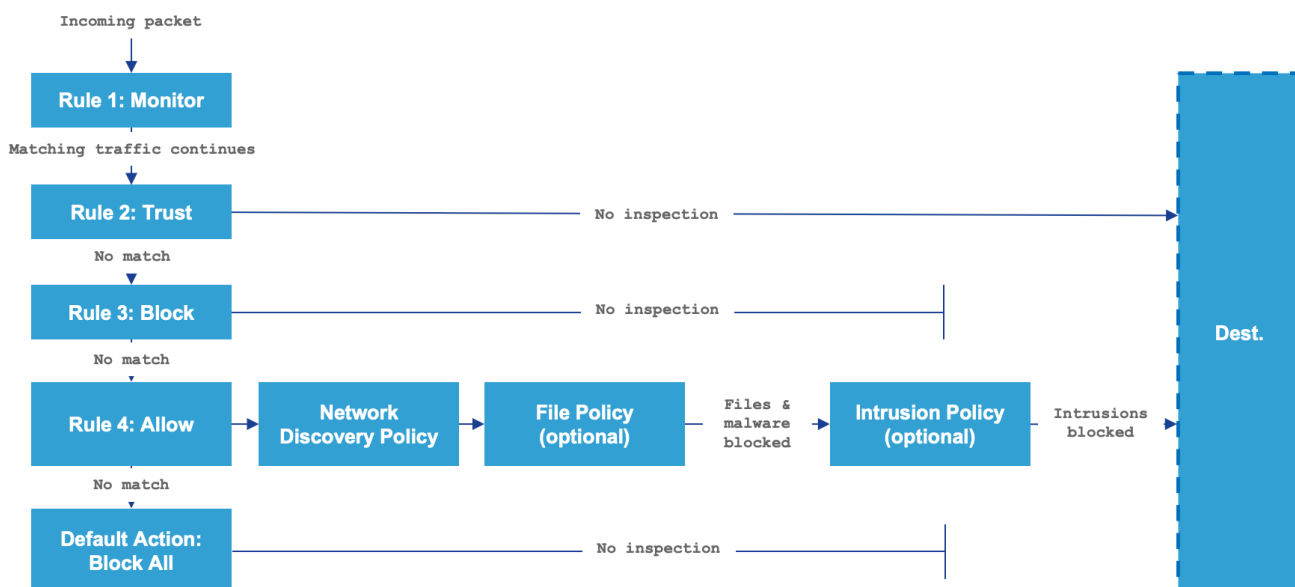


Рис.3.11. Приклад робочого лланцюжка політик

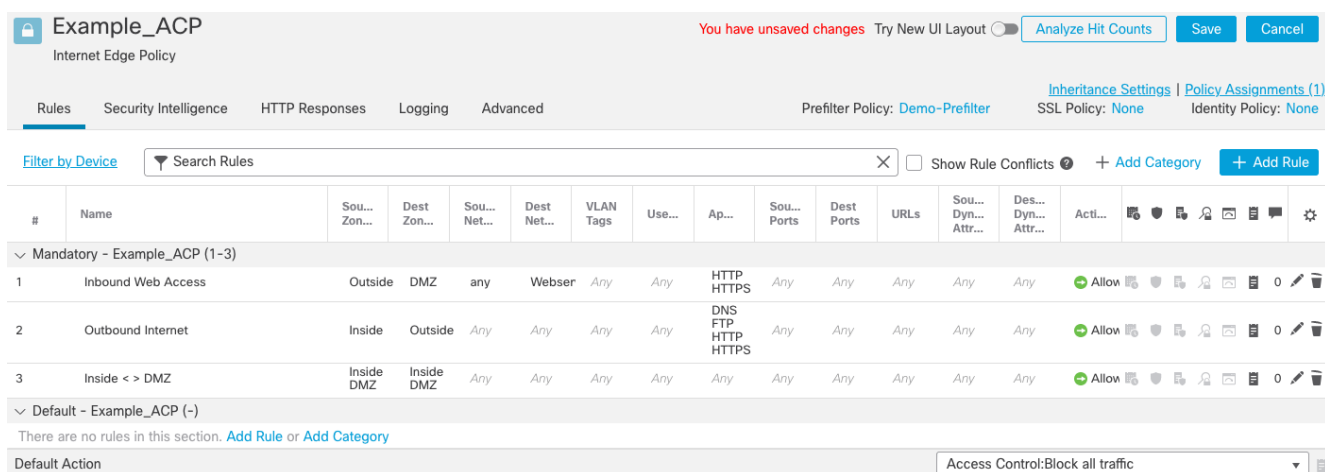


Рис.3.12. Екран Access Control Policy з базовою структурою та правилами

Ключовим елементом керування доступом є Access Control Policy (ACP). У межах ACP формуються правила, які описують хто, звідки, куди, яким сервісом/застосунком, до яких URL/категорій може передавати трафік, а також які режими інспекції та логування треба застосувати. Типова робоча практика — мати окремі категорії правил для обов'язкових обмежень (наприклад, заборона тіньових сервісів або небажаних категорій URL) і для бізнес-дозволів (наприклад, доступ користувачів до веб-ресурсів, доступ сервісів до API, міжсегментна взаємодія конкретних VLAN/зон). Важливий принцип — default action доцільно встановлювати як блокування всього, що не описане явними правилами, а дозволи формувати вузько та контрольовано. Це прямо підтримує модель мінімально

необхідних дозволів і зменшує ризик несанкціонованого доступу через пропущені винятки.

New Policy

Name:

Example_ACP

Description:

Internet Edge Policy

Select Base Policy:

None

Default Action:

☒ Block all traffic

☐ Intrusion Prevention

☐ Network Discovery

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Search by name or value

alc_ftd1

Add to Policy

Selected Devices

Cancel

Save

Рис.3.13. Створення правила в АСР (Add Rule, базові поля)

Add Rule

Name: ☒ Enabled

Insert:

Action: +

Time Range: +

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Available Zones

- DMZ
- EPG1
- EPG2
- EPG3
- Inside
- Out
- Outside

Source Zones (1):

Destination Zones (1):

Рис.3.14. Вибір зон джерела/призначення (Zones)

Add Rule

Name: ☒ Enabled

Insert:

Action: +

Time Range: +

Networks Zones VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Available Networks

Networks Geolocation

- Partner_DMZ
- smc721
- SNMP-Server
- Webserver_Private
- Webserver_Public
- win10_172.16.22.10
- win2016_172.16.24.10

Source Networks (0):

Destination Networks (1):

Рис.3.15. Вибір мереж/хостів (Networks)

Add Rule

Name: Inbound Web Access ☒ Enabled Insert: below rule 1

Action: Allow Time Range: None

Zones Networks VLAN Tags **Users** Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Application Filters Clear All Filters X Available Applications (13) Selected Applications and Filters (2)

Search by name: HTTP

- User-Created Filters
- Risks (Any Selected)
- Business Relevance (Any Selected)
- Types (Any Selected)
- Categories (Any Selected)
- Tags (Any Selected)

- HTTP
- HTTP 2.0
- HTTP RPC Ep Map
- HTTP Tunnel
- HTTP/SSL Tunnel
- HTTPMGT
- HTTPS
- Multimedia HTTP

Add to Rule

Applications: HTTP, HTTPS

Cancel Add

Рис.3.16. Вибір застосунків (Applications) як рівень контролю поверх портів

З технічної точки зору, АСР працює як комбінація матчінг-умов і дії, де умови збираються з бібліотеки об'єктів (network objects, port objects, URL категорії/репутації, користувачі/групи, атрибути тощо). Саме тому у виробничих конфігураціях критично важливою є дисципліна створення об'єктів: назви мають бути однозначними, об'єкти — перевикористовуваними, а логіка зони/сегментації — стабільною. Якщо в правилах постійно використовуються разові значення IP/портів без нормалізації в об'єкти, політика швидко деградує: з'являються дублікати, суперечливі винятки й складнощі з аудитом.

Окремий рівень якості АСР — контроль застосунків і URL. У корпоративній мережі часто недостатньо дозволити 80/443, оскільки тоді в межах дозволу «веб» можуть пройти небажані сервіси (від несанкціонованих проксі до конкретних SaaS-категорій). Тому на практиці доцільно комбінувати: зони/мережі + застосунки (HTTP/HTTPS, DNS, FTP тощо) + URL категорії/репутації, а вже потім накладати інспекцію та IPS.

Editing Rule - Outbound Internet

Name: Outbound Internet ☒ Enabled [Move](#)

Action: Time Range: None

Zones Networks VLAN Tags **Users** Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Categories and URLs Reputations

Search for a category

Category	URLs
Non-governmental Organizations	
Non-sexual Nudity	
Not Actionable	
Online Communities	
Online Meetings	
Online Storage and Backup	
Online Trading	

Reputations

Any
5 - Trusted
4 - Favorable
3 - Neutral
2 - Questionable
1 - Untrusted

Selected URLs (3)

Computers and Internet (Any Reputation)	Remove
Education (Reputation 5)	Remove
Online Communities (Reputations 4-5)	Remove

Enter URL

Cancel Save

Рис.3.17. Налаштування URL-категорій та репутації в правилі ACP (URLs)

Логування в Secure Firewall має дві типові задачі: операційна (швидко бачити, що відбувається зараз, чому трафік не проходить/чому проходить) і доказова (відтворити ланцюжок подій після інциденту, провести аудит змін, забезпечити кореляцію в SIEM). У контексті ACP базовою практикою є ввімкнення логів на початку та/або в кінці з'єднання (залежно від сценарію), а також визначення, куди саме відправляти події: у перегляд подій (Event Viewer), на syslog, через SNMP-пастки тощо. Важливо, що логування повинно бути керованим: для критичних правил (доступ до DMZ, адміністративні протоколи, міжсегментний доступ) логування треба робити детальнішим і стабільним, для масового «користувачького веба» — часто достатньо логувати завершення сесії або лише відхилення/аномалії, інакше обсяг подій стає надмірним.

Add Rule

Name: ☒ Enabled

Insert:

Action: ☒ ☐ ☐ ☐ ☐

Time Range: +

Zones Networks VLAN Tags **Users** Applications Ports URLs SGT/ISE Attributes Inspection **Logging** Comments

☒ Log at Beginning of Connection

☒ Log at End of Connection

File Events:

☐ Log Files

Send Connection Events to:

☒ Event Viewer

☐ Syslog Server (Using default syslog configuration in Access Control Logging) [Show Overrides](#)

☐ SNMP Trap +

Рис.3.18. Налаштування логування в правилі ACP: Log at Beginning/End, напрямки подій (Event Viewer, Syslog, SNMP)

На рівні вимог до логування в корпоративному середовищі зазвичай фіксуються мінімальні атрибути події: час, джерело/призначення, зони, дія (allow/block), застосунок/протокол, URL/категорія (для веб), користувач (за наявності ідентифікації), ідентифікатор правила, а також контекст інспекції (чи застосовувалась IPS-політика, чи було розшифрування TLS, чи працювали списки Security Intelligence). Це дає змогу в SIEM будувати кореляції «користувач → сесія → домен/URL → індикатор компрометації», а також робити відокремлений аудит «хто і коли змінив політику, і як це вплинуло на трафік».

Механізми Security Intelligence використовуються для того, щоб відсікати трафік до відомо шкідливих IP/DNS/URL якнайраніше, ще до витратних етапів аналізу. Це важливо з двох причин. По-перше, зменшується навантаження на інспекцію, оскільки значна частина шкідливих звернень може бути відхилена на ранньому кроці. По-друге, зростає швидкість реакції на загрози, якщо використовується актуальна розвідка (threat intelligence) та списки блокування, синхронізовані з джерелами на кшталт Talos/Umbrella. У політиці зазвичай підтримуються два ключові набори: Block List (що блокується) та Do-Not-Block List

(винятки), щоб уникати збоїв бізнес-процесів через помилкові спрацювання або специфічні корпоративні домени.

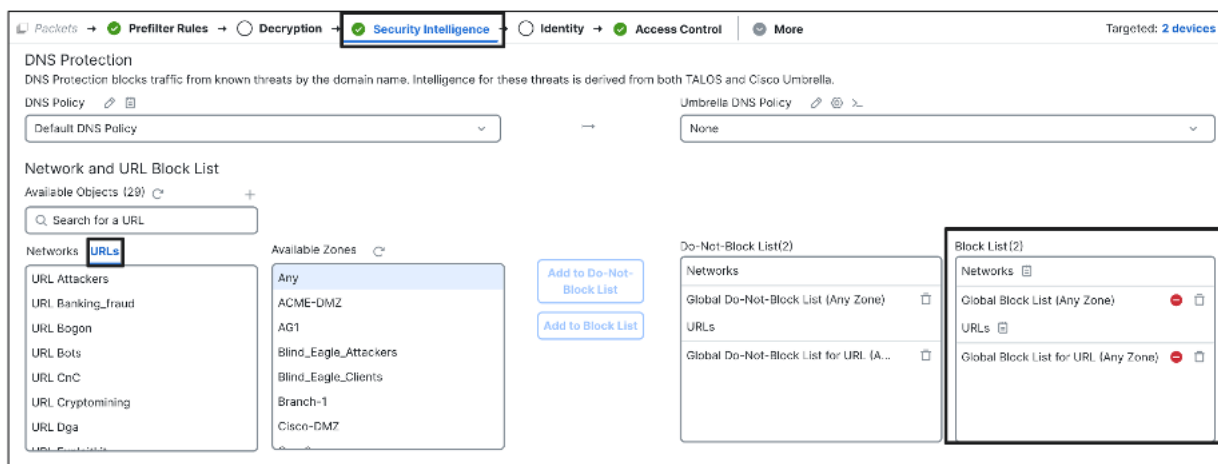


Рис.3.19. Security Intelligence у FMC: DNS Policy та списки блокування/винятків

Практично важливо, що Security Intelligence не замінює АСР або IPS. Це саме швидкий фільтр за репутаційними/розвідувальними ознаками, тоді як АСР визначає дозволи за контекстом мережі й застосунків, а IPS відловлює експлуатації та атаки на рівні вмісту/патернів. Тому правильна інженерна логіка виглядає так: максимально чітка сегментація та мінімально необхідні дозволи в АСР, раннє відсікання завідомо шкідливого трафіку через Security Intelligence, і окремо — IPS/інспекція там, де це потрібно за ризиком і критичністю сегмента [28].

IPS-функціональність у Cisco Secure Firewall реалізується через Intrusion Policy, яку можна застосувати до трафіку (зазвичай через прив'язку в правилі АСР на вкладці Inspection). Політика IPS визначає, які сигнатури та методи аналізу активні, у якому режимі вони працюють (виявлення або запобігання), а також як саме трактуються спрацювання (alert/drop тощо). З погляду керування ризиками, IPS налаштовується не «вмиканням усього», а вибором базової політики (наприклад, збалансованої) і подальшим тюнінгом під конкретний сегмент, щоб зменшити false positive і не зламати легітимний трафік.

Create Intrusion Policy

Name*

Inline IPS Policy

Description

Inspection Mode

☐ Detection ☒ Prevention

Intrusion rule actions are always applied. Connections that match a drop rule are blocked.

Base Policy

Balanced Security and Connectivity

Cancel Save

Рис.3.20. Створення Intrusion Policy: режим Detection або Prevention, вибір базової політики

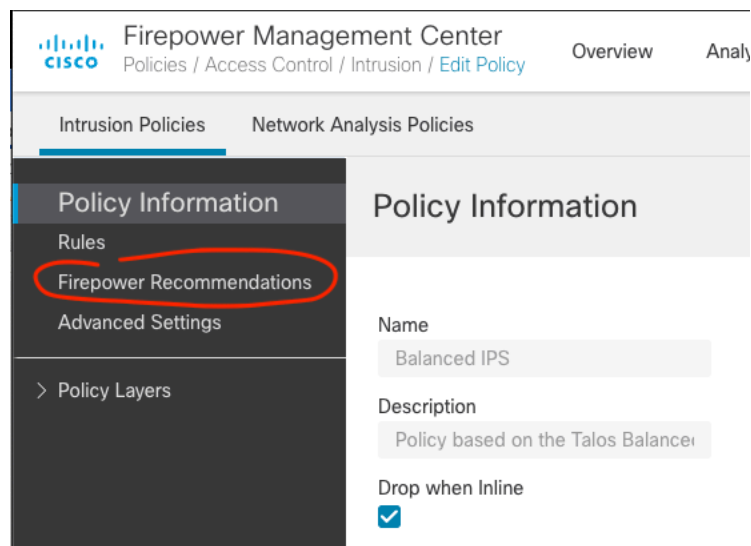


Рис.3.21. Firepower Recommendations як механізм рекомендацій для правил IPS

Рис.3.22. Параметри Firepower Recommended Rules Configuration: поріг, мережі для аналізу, прийняття рекомендацій

З практичної точки зору, IPS-політика має бути прив'язана до контексту, тобто до тих потоків, де вона справді дає користь. Наприклад, для периметра (інтернет → DMZ) доцільно мати суворіші профілі, для сегментів із застарілими сервісами — обережніші, щоб не провокувати помилкові блокування. Також важливий Variable Set, який адаптує правила до мережевого середовища (наприклад, внутрішні адресні простори, сервіси, що вважаються внутрішніми). На рівні процесу керування політикою це виглядає як: базовий профіль → обмеження за рекомендаціями/контекстом → контроль спрацювань → корекція винятків/дій [29].

Рис.3.23. Вкладка Inspection у правилі ACP: вибір Intrusion Policy та Variable Set

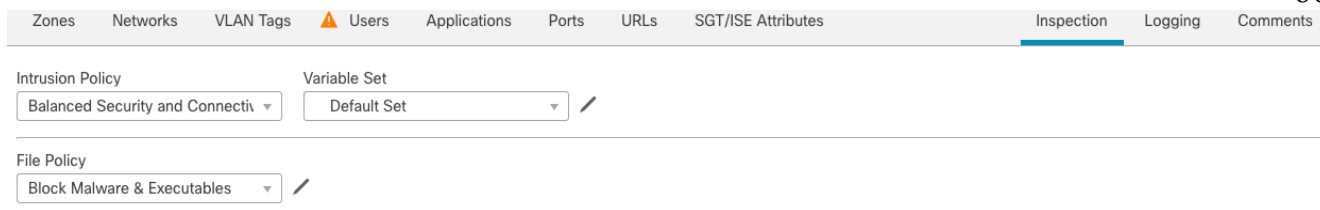


Рис.3.24. Приклад: одночасний вибір Intrusion Policy і File Policy в правилі ACP

NAT у Cisco Secure Firewall впливає на те, які адреси видно правилам і як узгодити зовнішню публічну адресацію із внутрішніми сегментами. В FMC для FTD NAT реалізується як окрема NAT Policy, у межах якої існують секції на кшталт правил до (NAT Rules Before), автоматичних (Auto NAT Rules) та після (NAT Rules After), що концептуально відповідає секціям NAT у класичній ASA-парадигмі. Це важливо для передбачуваності: наприклад, винятки NAT (exemption) або специфічні двосторонні трансляції мають опинитися в правильній секції, інакше конфігурація може працювати формально, але некоректно для частини потоків.

Для корпоративних сценаріїв типові класи NAT-налаштувань такі: статичний NAT для публічних сервісів у DMZ, динамічний PAT для виходу користувачів у інтернет, NAT exemption для VPN або для специфічних міжсегментних маршрутів, а також pool NAT у випадках, коли потрібно розподіляти вихідні адреси з пулу. Важливий момент: навіть правильно налаштований NAT не означає, що трафік дозволений — для проходження потоку потрібні відповідні правила ACP (і часто саме тут виникають типові помилки). У практичній роботі контроль коректності реалізується через перевірку, що для необхідних напрямків існують дозволяючі правила і що адреси/зони, які матчатся, відповідають реальному потоку після/до трансляції згідно логіки обробки [30].

Додатково, в реальних середовищах NAT потрібно узгоджувати з вимогами журналювання. Якщо в логах фіксується лише «перекладена» адреса без контексту, розслідування інцидентів ускладнюється. Тому на рівні політик і SIEM-кореляцій зазвичай налаштовується збереження полів, які дозволяють відтворити первинний і транслований контекст потоку (original/translated), а також зону входу/виходу [28].

67

Edit NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Static

☒ Enable

Interface Objects **Translation** PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* Webserver_Private	Translated Source: Address
Original Port: TCP	Translated Source: Webserver_Public
	Translated Port:

Cancel OK

Рис.3.25. Редагування статичного NAT (Edit NAT Rule, Static)

New Network Object

Name
Example_NAT_Pool

Description

Network
☐ Host ☒ Range ☐ Network ☐ FQDN

209.165.201.20-209.165.201.30

☐ Allow Overrides

Cancel Save

Рис.3.26. Створення об'єкта для NAT pool (New Network Object)

Edit NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Dynamic

☒ Enable

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:*	Translated Source:
IPv4-Private-10.0.0.0-8 +	Address
Original Port:	Translated Port:
TCP	Example_NAT_Pool +

Рис.3.27. Динамічний NAT з пулом (Edit NAT Rule, Dynamic + NAT Pool)

VPN у Cisco Secure Firewall використовується як для site-to-site сценаріїв, так і для віддаленого доступу (Remote Access VPN). У контексті механізмів контролю трафіку важливо, що VPN — це не лише створення тунелю. Це також: правила доступу для трафіку з пулів VPN-клієнтів до внутрішніх ресурсів, винятки NAT (коли потрібно), вимоги до журналювання і додаткові захисні опції для запобігання підміні адрес (anti-spoofing/uRPF тощо). У FMC налаштування віддаленого доступу часто виконується через майстер (Remote Access VPN Policy Wizard), але навіть після проходження майстра потрібна інженерна перевірка АСР/NAT/логування.

З погляду політик контролю трафіку, критичний момент у Remote Access VPN — як саме обробляється трафік з пулу клієнтів. Якщо дозволити його надто широко, VPN стає «пропуском» у внутрішню мережу без сегментації. Якщо ж не створити потрібних правил АСР, користувач може успішно підключитися, але не матиме доступу до ресурсів (що також є типовим інцидентом експлуатації). Тому правильна практика — створювати окремі правила АСР для VPN-пулу до конкретних внутрішніх сервісів, з явним логуванням і, за потреби, із застосуванням IPS до найбільш критичних потоків. Окремо враховується, чи потрібно робити NAT exemption для доступу у внутрішні сегменти або для взаємодії з site-to-site тунелями.

У документації також підкреслюється аспект безпеки: за замовчуванням опції, які можуть «обійти» інспекцію або змінити логіку пропуску трафіку, треба застосовувати обережно. Наприклад, опція `bypass` для `decrypted traffic` (`sysopt permit-vpn`) впливає на те, чи проходить трафік через ACP/IPS. З погляду керування ризиками, більш контрольований підхід — забезпечити антиспуфінг на інтерфейсі, де термінується VPN, і залишити стандартний контроль політиками доступу [31].

У корпоративних мережах з Cisco Secure Firewall найбільш типові проблеми виникають не через відсутність окремої функції, а через неузгодженість політик. Наприклад, NAT налаштований, але ACP не дозволяє потрібний напрямок; VPN-майстер завершений, але не створені адресні об'єкти й правила доступу для пулу; IPS увімкнений занадто агресивно на сегменті зі спадковими сервісами і провокує збої; URL-контроль застосовується без винятків і блокує необхідні бізнес-категорії; логування або вимкнене, або настільки надмірне, що події стають непридатними для аналізу. В інженерній практиці це вирішується введенням правил побудови політики: окремі категорії правил, контроль пріоритетів, регулярний перегляд `hit counts`, маркування правил за власниками/сервісами, і тестування змін через контрольовані вікна впровадження з можливістю швидкого відкату.

Ще один аспект — доказовість та аудит. Якщо політика дозволу існує, але не логуються ключові атрибути, організація фактично втрачає можливість довести, що саме відбулося під час інциденту, або швидко встановити причину збою. Тому навіть у сценаріях, де дозволяється великий обсяг веб-трафіку, логування повинно бути налаштоване так, щоб у разі інциденту можна було відокремити «норму» від аномалії: блокування Security Intelligence, спрацювання IPS, повторювані відмови доступу, зростання частки невідомих застосунків або звернень до небезпечних категорій. [28]

3.3. Розробка рекомендацій щодо забезпечення безпеки комп'ютерних мереж

Забезпечення безпеки комп'ютерних мереж доцільно розглядати як комплекс організаційних і технічних заходів, спрямованих на зниження ймовірності

компрометації мережевої інфраструктури, обмеження наслідків інцидентів та підтримання контрольованості змін упродовж життєвого циклу мережі. Практична реалізація такого підходу базується на попередньому описі активів, сервісів і мережевих потоків, оскільки саме розуміння того, які вузли є критичними, які дані ними обробляються та які протоколи використовуються для міжсегментної взаємодії, визначає коректність подальшого проектування політик доступу. У мережі має бути сформовано актуальну модель потоків, де відображено допустимі напрямки обміну трафіком, мінімально необхідні сервіси та залежності інфраструктурного рівня, зокрема DNS, NTP та служби автентифікації. Така модель забезпечує можливість переходу від фрагментарних налаштувань до системного керування доступом, коли правила визначаються потребами бізнес-процесів і властивостями ризиків, а не випадковими винятками.

Ключовим елементом підвищення стійкості мережі є сегментація, що передбачає поділ інфраструктури на зони з різним рівнем довіри та різними вимогами до контролю трафіку. Доцільним є виокремлення принаймні користувачьких сегментів, серверних сегментів, демілітаризованої зони для публічних сервісів, окремого середовища керування (management), гостьових мереж та мереж для пристроїв із обмеженими можливостями захисту, зокрема IoT-компонентів. Між такими зонами має реалізовуватися керований периметр, у межах якого встановлюються та застосовуються політики міжсегментного доступу. З позиції протидії поширенню атак важливо, що сегментація повинна охоплювати не лише напрямки взаємодії з зовнішніми мережами, але й внутрішній east-west трафік, який часто використовується для латерального переміщення після первинної компрометації. Для критичних сервісів доцільним є застосування мікросегментації, коли доступ дозволяється лише для визначених сервісних ланцюжків, а будь-які інші спроби взаємодії між сегментами блокуються та реєструються для подальшого аналізу.

Політики мережевого доступу мають формуватися відповідно до логіки мінімально необхідних дозволів, що передбачає блокування всього трафіку, який не описано явними правилами, і надання доступу лише для конкретних джерел, призначень і сервісів. У цьому контексті якість політики визначається ступенем

конкретизації правил, де обмеження задаються за зонами, мережами, протоколами або застосунками, а також за потреби доповнюються часовими чи рольовими умовами. Надмірно широкі дозволи збільшують площину атаки та ускладнюють аудит, тому винятки мають бути обґрунтованими, формалізованими та такими, що підлягають регулярному перегляду. Для публічних сервісів доцільним є використання DMZ як буферної зони, у межах якої зовнішній доступ дозволяється лише до необхідних ресурсів, а взаємодія між DMZ та внутрішніми сегментами обмежується мінімальним набором залежностей. Адміністрування таких сервісів має здійснюватися через захищені канали та керовані точки доступу, що зменшує ризик компрометації через прямі адміністративні підключення з робочих сегментів.

Значущим напрямом є контроль віддаленого доступу, оскільки саме він розширює периметр мережі на пристрої користувачів і підрядників. Віддалений доступ доцільно реалізовувати з багатофакторною автентифікацією та розмежуванням прав, забезпечуючи окремі профілі доступу для різних категорій користувачів і мінімізацію доступних ресурсів відповідно до функціональних обов'язків. При цьому політики для трафіку віддалених користувачів повинні бути узгоджені з міжсегментними правилами, а також із вимогами до журналювання, щоб унеможливити появу неконтрольованих маршрутів до критичних сегментів. Для взаємодії між майданчиками організації актуальним є застосування site-to-site з'єднань із чітким визначенням допустимих напрямків і сервісів, що знижує ризики несанкціонованого транзиту та неочікуваного доступу між філіями.

Підвищення ефективності захисту потребує використання механізмів виявлення та блокування загроз на мережевому рівні, зокрема засобів IDS/IPS, що дозволяють протидіяти експлуатації відомих вразливостей і типовим атакам на протоколи та застосунки. Доцільним є застосування таких механізмів на найбільш ризикових напрямках, включно з доступом до публічних сервісів та критичних серверів, а також у міжсегментних потоках, де компрометація може призвести до масштабних наслідків. Разом із цим механізми фільтрації вихідного трафіку та репутаційного блокування відомо шкідливих доменів і адрес забезпечують раннє відсікання типових командно-контрольних взаємодій і фішингових ресурсів, зменшуючи навантаження на глибоку інспекцію та підвищуючи швидкість реакції

на масові загрози. У серверних сегментах доцільно застосовувати egress-обмеження, оскільки невиправдано широкий доступ серверів до зовнішніх ресурсів підвищує ризики витоку даних і прихованої взаємодії зі шкідливою інфраструктурою.

Невід'ємною умовою керованості безпеки мережі є централізоване журналювання та моніторинг. Події від мережевих пристроїв, засобів контролю доступу, VPN-підсистем, DNS/DHCP, проксі та критичних серверів мають збиратися централізовано із забезпеченням достатнього терміну зберігання для потреб розслідувань і аудитів. Для мережевих подій доцільним є фіксування часу, джерела та призначення, зон, дії політики, ідентифікатора правила, параметрів застосунка або сервісу, а за можливості також ідентичності користувача та результатів інспекції. Окремого значення набуває аудит адміністративних дій і змін конфігурацій, оскільки саме контроль змін дозволяє встановити причинно-наслідкові зв'язки між оновленням політик та появою інцидентів або деградацією доступності сервісів.

Захист площини керування мережевою інфраструктурою має реалізовуватися шляхом ізоляції керуючих інтерфейсів у спеціальному сегменті, обмеження доступу до нього, використання захищених протоколів керування, централізованої автентифікації адміністраторів і розмежування привілеїв. Такий підхід знижує ризики несанкціонованих змін і компрометації мережевих пристроїв через слабкі облікові дані або небезпечні канали адміністрування. Паралельно необхідно забезпечувати актуальність програмного забезпечення мережевих компонентів, регулярне оновлення сигнатур, списків репутацій та сертифікатів, а також реалізацію відмовостійкості для критичних елементів інфраструктури, зокрема резервування каналів, високої доступності контрольних вузлів і наявності планів відновлення після інцидентів.

Підтримання ефективності мережевих контролів у часі вимагає періодичного перегляду політик доступу, аналізу їхньої фактичної застосовності та видалення невикористовуваних або надмірно широких правил. Регулярний аналіз спрацювань механізмів детекції, відхилень доступу та загальних тенденцій у мережевій активності дає змогу своєчасно виявляти аномалії, коригувати налаштування та

запобігати накопиченню технічного боргу в політиках. Документування схеми сегментації, матриці доступу між зонами, вимог до логування, порядку внесення змін і процедур реагування є необхідною умовою повторюваності та керованості мережевої безпеки, оскільки дозволяє забезпечити однозначне трактування налаштувань і зберігати цілісність підходу під час масштабування або змін персоналу.

ВИСНОВКИ

У кваліфікаційній роботі вирішено актуальне науково-прикладне завдання щодо розробки та обґрунтування технології забезпечення безпеки комп'ютерних мереж організації на основі рішень класу Next-Generation Firewall (NGFW), зокрема екосистеми Cisco Secure Firewall.

Встановлено, що сучасний ландшафт кіберзагроз характеризується зміщенням акцентів від прямих атак на периметр до складних сценаріїв, що включають використання легітимних каналів (HTTPS, DNS), компрометацію облікових даних та латеральне (горизонтальне) переміщення всередині мережі. Традиційні підходи до захисту, що базуються лише на портовій фільтрації, втратили ефективність в умовах шифрованого трафіку та розмитого периметра. Визначено, що для протидії актуальним загрозам (Ransomware, атаки на ланцюг постачання, приховані канали керування) критично необхідним є перехід до архітектури Zero Trust із глибокою інспекцією трафіку та сегментацією.

Дослідження функціональних можливостей Cisco Secure Firewall підтвердило, що це рішення є комплексною платформою, яка поєднує можливості станового міжмережевого екрана, системи запобігання вторгненням (IPS), контролю застосунків (AVC) та захисту від шкідливого ПЗ (AMP). Визначено, що архітектурний поділ на площину даних (Cisco Threat Defense) та площину керування (Cisco Secure Firewall Management Center — FMC) є оптимальним для корпоративних мереж, оскільки забезпечує централізовану політику безпеки, уніфікацію конфігурацій та незалежність процесів збору телеметрії від навантаження на канали передачі даних.

Запропоновано варіант розгортання Cisco Secure Firewall, який передбачає фізичне та логічне відокремлення мережі керування (Management Network) від продуктивного трафіку. Розроблено алгоритм введення пристрою в експлуатацію, що включає первинну ініціалізацію, налаштування синхронізації часу (NTP), реєстрацію в FMC та перевірку цілісності каналу керування. Обґрунтовано

доцільність використання механізмів High Availability (HA) для центру керування з метою забезпечення безперервності процесів моніторингу та адміністрування.

Розроблено методику формування багаторівневої системи політик, де ключовим елементом є Access Control Policy (ACP). Доведено, що ефективний захист досягається шляхом послідовного застосування контролів: раннього відсікання загроз через Security Intelligence (блокування за репутацією IP/URL/DNS), контекстної фільтрації застосунків і користувачів, та глибокої інспекції IPS для дозволеного трафіку. Сформовано рекомендації щодо налаштування NAT та VPN, які наголошують на необхідності створення окремих правил доступу для VPN-пулів та уникнення надмірно широких винятків (bypass), що можуть знизити рівень захищеності.

Показано, що ізольована робота NGFW не забезпечує повної ситуаційної обізнаності. Обґрунтовано необхідність інтеграції Cisco Secure Firewall із системами кореляції подій (SIEM) та платформами реагування (XDR) через механізми syslog або eStreamer. Це дозволяє перетворити розрізнені події безпеки на контекстні інциденти, забезпечити довгострокове зберігання журналів для розслідувань та реалізувати проактивний підхід до виявлення атак.

На основі проведеного аналізу сформовано перелік рекомендацій для підвищення рівня безпеки комп'ютерних мереж. Ключовими заходами визначено: впровадження мікросегментації для обмеження внутрішніх загроз, застосування принципу мінімальних привілеїв у правилах ACP, обов'язкове детальне логування критичних з'єднань та регулярний аудит політик для усунення застарілих правил.

Отже, запропонована технологія на основі рішення Cisco дозволяє побудувати масштабовану, керовану та стійку систему захисту, що відповідає сучасним вимогам стандартів кібербезпеки та забезпечує безперервність бізнес-процесів організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. ENISA Threat Landscape 2024 [Електронний ресурс] / European Union Agency for Cybersecurity (ENISA). URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> (дата звернення: 10.12.2025).
2. Guide for Conducting Risk Assessments (NIST SP 800-30 Rev. 1) [Електронний ресурс] / Joint Task Force. URL: <https://csrc.nist.gov/pubs/sp/800/30/r1/final> (дата звернення: 10.12.2025).
3. Rose S. Zero Trust Architecture (NIST SP 800-207) [Електронний ресурс] / S. Rose, O. Borchert, S. Mitchell, S. Connelly. URL: <https://csrc.nist.gov/pubs/sp/800/207/final> (дата звернення: 10.12.2025).
4. Scarfone K. A. Guidelines on Firewalls and Firewall Policy (NIST SP 800-41 Rev. 1) [Електронний ресурс] / K. A. Scarfone, P. Hoffman. URL: <https://csrc.nist.gov/pubs/sp/800/41/r1/final> (дата звернення: 10.12.2025).
5. The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29) [Електронний ресурс] / National Institute of Standards and Technology. URL: <https://doi.org/10.6028/NIST.CSWP.29> (дата звернення: 10.12.2025).
6. Rose S. Zero Trust Architecture (NIST SP 800-207) [Електронний ресурс] / S. Rose, O. Borchert, S. Mitchell, S. Connelly. URL: <https://doi.org/10.6028/NIST.SP.800-207> (дата звернення: 10.12.2025).
7. CIS Critical Security Controls v8 [Електронний ресурс] / Center for Internet Security. URL: <https://www.cisecurity.org/insights/white-papers/cis-controls-v8> (дата звернення: 10.12.2025).
8. The NIST Cybersecurity Framework (CSF) 2.0 [Електронний ресурс] / NIST. URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> (дата звернення: 15.12.2025).
9. Guidelines on Firewalls and Firewall Policy (NIST SP 800-41 Rev. 1) [Електронний ресурс] / NIST. URL: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-41r1.pdf> (дата звернення: 15.12.2025).

10. Guide to Intrusion Detection and Prevention Systems (IDPS) (NIST SP 800-94) [Электронный ресурс] / NIST. URL: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf> (дата звернения: 15.12.2025).
11. Zero Trust Architecture (NIST SP 800-207) [Электронный ресурс] / NIST. URL: <https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf> (дата звернения: 15.12.2025).
12. Layering Network Security Through Segmentation [Электронный ресурс] / CISA. URL: <https://www.cisa.gov/resources-tools/resources/layering-network-security-through-segmentation-infographic> (дата звернения: 15.12.2025).
13. MITRE ATT&CK knowledge base [Электронный ресурс] / MITRE. URL: <https://attack.mitre.org/> (дата звернения: 15.12.2025).
14. What Is a Next-Generation Firewall (NGFW)? [Электронный ресурс] / Cisco. URL: <https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-next-generation-firewall.html> (дата звернения: 15.12.2025).
15. Cisco Secure Firewall At-a-Glance [Электронный ресурс] / Cisco. URL: <https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/secure-firewall-aag.html> (дата звернения: 15.12.2025).
16. SAFE Secure Edge Architecture Guide [Электронный ресурс] / Cisco. URL: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/safe-secure-edge-architecture-guide.html> (дата звернения: 15.12.2025).
17. Cisco Secure Firewall Management Center Device Configuration Guide, 7.6: Get Started with Device Management [Электронный ресурс] / Cisco. URL: <https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/get-started-device-management.html> (дата звернения: 15.12.2025).
18. Cisco Firepower Management Center Datasheet [Электронный ресурс] / Cisco. URL: <https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html> (дата звернения: 15.12.2025).
19. Configure the Merge of Management and Data Interfaces [Электронный ресурс] / Cisco. URL: <https://www.cisco.com/c/en/us/support/docs/security/secure->

[firewall-threat-defense/222873-configure-the-merge-of-management-and-di.html](https://www.cisco.com/c/en/us/support/docs/security/secure-firewall/222873-configure-the-merge-of-management-and-di.html) (дата
звернення: 15.12.2025).

20. Migrate ASA to Firepower Threat Defense with the Firepower Migration Tool [Електронний ресурс] / Cisco. URL: <https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-asa/222707-migrate-asa-to-firepower-threat-defense.html> (дата звернення: 15.12.2025).

21. Cisco Secure Firewall Integrations Overview Guide [Електронний ресурс] / Cisco. URL: <https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/consolidated-integration-guide/integration-overview.html> (дата звернення: 14.12.2025).

22. Cisco Secure Firewall Threat Defense and Cisco XDR Integration Guide [Електронний ресурс] / Cisco. URL: <https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/xdr/secure-firewall-threat-defense-and-xdr-integration-guide.pdf> (дата звернення: 14.12.2025).

23. Splunk + Firewall, DEVNET-2245 (Cisco Live) [Електронний ресурс] / Cisco. URL: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2023/pdf/DEVNET-2245.pdf> (дата звернення: 14.12.2025).

24. Cisco Firepower Management Center integration (QRadar DSM guide) [Електронний ресурс] / IBM Docs. URL: <https://www.ibm.com/docs/en/dsm?topic=cisco-firepower-management-center> (дата звернення: 14.12.2025).

25. Cisco Secure Firewall 3100 Getting Started Guide [Електронний ресурс] / Cisco. URL: https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hw/3100/getting-started/b_3100_gsg.html (дата звернення: 15.12.2025).

26. Cisco Secure Firewall Management Center Device Configuration Guide, 7.4: Configuration Deployment [Електронний ресурс] / Cisco. URL: <https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/740/management-center-device-config-74/configuration-deployment.html> (дата звернення: 15.12.2025).

27. Cisco Secure Firewall Management Center Administration Guide, 7.6: High Availability [Электронный ресурс] / Cisco. URL: <https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/760/management-center-admin-76/high-availability.html> (дата звернения: 15.12.2025).
28. Access Control Policy [Электронный ресурс] / Cisco Secure Firewall Documentation. URL: <https://secure.cisco.com/secure-firewall/docs/access-control-policy> (дата звернения: 15.12.2025).
29. Intrusion Policy [Электронный ресурс] / Cisco Secure Firewall Documentation. URL: <https://secure.cisco.com/secure-firewall/docs/intrusion-policy> (дата звернения: 15.12.2025).
30. Configure and Verify NAT on FTD [Электронный ресурс] / Cisco Support. URL: <https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212702-configure-and-verify-nat-on-ftd.html> (дата звернения: 15.12.2025).
31. Configure AnyConnect Remote Access VPN on FTD [Электронный ресурс] / Cisco Support. URL: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212410-configure-anyconnect-vpn-client-on-ftd.html> (дата звернения: 15.12.2025).

ДЕМОНТРАЦІЙНІ МАТЕРІАЛИ (Презентація)