Міністерство освіти і науки України
Харківського національного університету імені В.Н. Каразіна
Навчально-наукового інституту комп'ютерних наук та штучного інтелекту
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

В.о. зав. кафедрою КІСМіТ
Марина ЄСІНА
"Допущено до захисту"

« »_____2025р.

Пояснювальна записка
до кваліфікаційної роботи бакалавра
на тему: «Засоби управління кібербезпекою мереж»

оцінка « _____ »

Голова ЕК

Мичуда Л.З.

Керівник: к.т.н. О.М. Мелкозьорова

Рецензент: д.т.н., с.н.с., Толстолузька О.Г.

Виконавець: студентка групи КБ-42
Стоянова І.В.

Харків 2025

РЕФЕРАТ

Кваліфікаційна робота складається зі 55 сторінок, включає 10 рисунків, 1 таблицю і 49 використаних джерел.

Мета роботи – дослідити принципи роботи, архітектуру та функціональні можливості мережевих засобів кібербезпеки на базі Check Point, а також реалізувати практичне налаштування компонентів системи.

У роботі застосовано методи аналізу архітектури інформаційних систем, практичне тестування функціональності систем безпеки, порівняльний аналіз засобів кіберзахисту.

Результатом роботи є сформовані рекомендації щодо оптимального налаштування інструментів SmartConsole, Security Management Server та Security Gateway у корпоративному середовищі.

Практичне значення полягає в можливості використання результатів для підвищення ефективності мережевого захисту та оперативного реагування на інциденти.

Ключові слова: CHECK POINT, МЕРЕЖЕВИЙ ЗАХИСТ, КІБЕРБЕЗПЕКА, ШЛЮЗ БЕЗПЕКИ, КОНСОЛЬ УПРАВЛІННЯ, SMARTCONSOLE, VPN, ФАЄРВОЛ.

ABSTRACT

The qualification thesis comprises 55 pages, includes 10 figures, 1 table and 49 references.

The objective of the work is to explore the operational principles, architecture, and functional capabilities of network cybersecurity tools based on Check Point, as well as to perform a practical implementation of system components.

The applied research methods include architecture analysis of IT systems, practical testing of security functionality, and comparative evaluation of cybersecurity tools.

The outcome includes practical recommendations for configuring SmartConsole, Security Management Server, and Security Gateway in corporate environments.

The practical value lies in the applicability of the results to enhance the efficiency of network protection and timely incident response.

Keywords: CHECK POINT, NETWORK PROTECTION, CYBERSECURITY, SECURITY GATEWAY, MANAGEMENT CONSOLE, SMARTCONSOLE, VPN, FIREWALL.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА СИМВОЛІВ

AES	– Advanced Encryption Standard
DDoS	– Distributed Denial of Service
DPI	– Deep Packet Inspection
IDS/IPS	– Intrusion Detection/Prevention System
IP-адреса	– Internet Protocol Address
SIEM	– Security Information and Event Management
SMS	– Security Management Server
SSL/TLS	– Secure Sockets Layer / Transport Layer Security
VPN	– Virtual Private Network
ACL	– Access Control List
IoT	– Internet of Things
SmartConsole	– інтерфейс керування продуктами Check Point
Zero Trust	– модель «нульової довіри», яка передбачає перевірку всіх користувачів та пристроїв
IPS	– Intrusion Prevention System
IDS	– Intrusion Detection System
VPN SSL	– вид VPN, що використовує SSL-протоколи, зручний для мобільного доступу

ВСТУП

У сучасну епоху цифрових технологій кібербезпека є одним із найважливіших аспектів забезпечення стабільності та надійності інформаційної інфраструктури, як у приватному секторі, так і в державних установах. Глобальна інтеграція цифрових систем, перехід на хмарні рішення, збільшення обсягу переданих даних та збільшення кількості пристроїв, підключених до мережі, створюють нові можливості для розвитку, але водночас відкривають числові вразливості для кібератак. таким чином, щороку зростає кількість загроз, як фішингові атаки, шкідливе програмне забезпечення, розподілені атаки типу «відмова в обслуговуванні» (DDoS) та витоки конфіденційної інформації. У зв’язку з цим питанням розроблення, впровадження та вдосконалення засобів контролю кібербезпеки мережі є надзвичайно актуальним.

Особливу увагу сьогодні приділено багаторівневим рішенням для моніторингу та захисту мережі. Одним із провідних інструментів у цій сфері є технології компанії Check Point, які забезпечують інтеграцію консолі управління, сервер для обробки даних та мережевого шлюзу (gateway). Це дозволяє створити єдину екосистему безпеки, яка може протидіяти сучасним складним загрозам, аналізувати мережевий трафік у реальному часі, ідентифікувати якісь небезпечні дії та реагувати на них у найкоротших рядках. Крім того, використання інструментів Check Point сприяє впровадженню політики сегментації мереж, запобіганню доступу неавторизованих користувачів, а також забезпечує безперервність роботи критично важливих систем навіть за умов зовнішнього втручання.

Важливим аспектом системи є її здатність до централізованого управління всіма елементами безпеки через консоль, що забезпечує зручність для адміністраторів і ефективність контролю. Сервер у цій структурі виконує функцію обробки великих обсягів даних про події в мережі, потім як шлюз безпеки (шлюз) виступає бар’єром між внутрішньою мережею та зовнішніми

загрозами, виконуючи фільтрацію, аналізуючи та блокуючи шкідливий трафік. Така архітектура дозволяє забезпечити комплексний захист, який адаптується до нових типів загроз і відповідає сучасним викликам у сфері інформаційної безпеки.

В умовах, коли кіберзлочинці потребують більш витончених методів атаки, компанії та організації повинні мати засоби проактивного реагування на загрози. Система Check Point дозволяє впроваджувати ефективний багаторівневий захист, який базується на сучасних технологіях, таких як машинне навчання, аналіз поведінки та інтелектуальне прогнозування атак. Реалізація таких підходів сприяє не лише запобіганню проникненню в мережу, але й мінімізації шкоди у разі успішної атаки.

Таким чином, актуальність дослідження використання засобів контролю кібербезпеки на базі Check Point зумовлена стрімким зростанням стійкості мережевої інфраструктури та забезпеченням створення ефективних, масштабованих і гнучких рішень для їхнього захисту. Реалізація таких систем забезпечує не лише безпеку даних та інформаційних процесів, а й стійкість організацій до кібервикликів, що стає критичним для сталого розвитку в умовах цифрової трансформації.

Об'єкт дослідження: системи кібербезпеки, орієнтовані на моніторинг і мережеву захисну інфраструктуру.

Предмет дослідження: інструменти кібербезпеки на базі технологій Check Point , включаючи консоль управління, сервер і шлюз (gateway), а також їх роль у забезпеченні комплексного захисту мережі.

Мета роботи: дослідити можливості та принципи функціонування технологій Check Point для забезпечення ефективного контролю та захисту мережевої інфраструктури, а також оцінити їх потенціал для реалізації сучасних вимог кібербезпеки.

Завдання роботи:

1) Проаналізувати основні концепції мережевої кібербезпеки, застосувати актуальні загрози та принципи їхнього подолання.

2) Дослідити архітектуру та функціональність системи Check Point , історію її розвитку та ключові особливості.

3) Визначте роль компонентів Check Point (консоль управління, сервер і шлюз безпеки) у забезпеченні кіберзахисту мережі.

4) Розглянути механізми реалізації захисту мережі за допомогою Check Point , включаючи принципи роботи SmartConsole , адміністрування Security Management Server та функціонування шлюзів безпеки.

5) Провести практичну реалізацію налаштування сервера безпеки та шлюзів Check Point для забезпечення кіберзахисту.

6) Оцінити ефективність інструментів Check Point виявлення, блокування та запобігання загрозам через тестування захисних механізмів.

7) Розробити рекомендації щодо оптимізації використання системи Check Point для комплексного захисту мережі.

Наукова новизна роботи відбувається в комплексному аналізі сучасних механізмів захисту мережі на основі технологій Check Point, що включає дослідження ролі та взаємодії ключових компонентів, таких як консоль управління (SmartConsole), управління (Security Management Server) та шлюзи безпеки (Security Gateway). У роботі систематизовано новітні підходи до забезпечення багаторівневого кіберзахисту, зокрема з використанням інтелектуальних інструментів моніторингу та управління, які дозволяють оперативно реагувати на загрози. Вперше акцентовано увагу на інтеграції політики безпеки та адаптації інструментів Check Point до сучасних вимог мережевої інфраструктури, що постійно змінюється через нові кіберзагрози.

Теоретичне значення роботи відбувається у поглибленні знань про концептуальні основи побудови багаторівневого захисту мережі, заснованої на інтегрованих рішеннях. У дослідженні узагальнено принципи функціонування архітектури Check Point, які раніше не систематизувалися в контексті забезпечення комплексного захисту мережевої інфраструктури. Результати роботи доповнюють сучасну теорію кібербезпеки, зокрема в питаннях ефективного моніторингу трафіку, управління подіями та

мінімізації ризиків через використання централізованих систем контролю. Узагальнені положення можуть служити основою для подальших досліджень у сфері розробки інноваційних систем мережевої безпеки.

Практичне значення роботи створено у розробці рекомендацій щодо налаштування та оптимізації роботи системи Check Point для забезпечення ефективного захисту мережі від сучасних загроз. Проведена практична реалізація механізмів кіберзахисту демонструє можливість інтеграції та використання інструментів SmartConsole, Security Management Server і шлюзів безпеки в реальних умовах. Результати роботи можуть бути використані для впровадження мережевої політики безпеки в корпоративному середовищі, освітніх установах, державних організаціях та інших структурах, що потребують захисту інформаційних ресурсів. Запропоновані рекомендації сприяють підвищенню стійкості інформаційних систем до загроз, а також ефективному виявленню, аналізу та реагуванню на кіберінциденти.

1. ТЕОРЕТИЧНІ ОСНОВИ МЕРЕЖЕВОЇ КІБЕРБЕЗПЕКИ

1.1. Основи концепції мережевої безпеки: поняття, принципи та актуальні загрози

Мережева безпека є однією з ключових складових загальної кібербезпеки, яка спрямована на захист інформаційних систем, даних і комунікаційних мереж від зовнішніх і внутрішніх загроз. Поняття мережевої безпеки охоплює всі засоби, методи та технології, які забезпечують конфіденційність, цільність і доступність даних під час їх передачі, зберігання та обробки в мережах [1]. Основна мета мережевої безпеки забезпечується у забезпеченні безпечного функціонування мережі, попередженні несанкціонованого доступу, мінімізації ризиків втрати або викрадання даних, а також від захисту від збоїв і атак [2].

Основи концепції мережевої безпеки базуються на декількох ключових принципах. По-перше, це принцип багаторівневого захисту , який використовує декілька шарів безпеки, кожен з яких працює незалежно від інших, щоб забезпечити додатковий рівень захисту навіть у разі компрометації одного з компонентів [3]. По-друге, в домені є принцип мінімізації доступу , відповідно до якого користувачам і пристроям надається лише той обсяг прав доступу, який є необхідним для виконання їх завдань [4]. По-третє, актуальним є принцип моніторингу та аналізу , який включає постійне спостереження за станом мережі, виявлення аномалій і реагування на них у режимі реального часу [5].

Сучасні мережі стикаються з різноманітними загрозами, які стають все більш складними й витонченими. Серед найбільш розширених загроз можна виділити розподілені атаки типу відмови в обслуговуванні (DDoS) , які спрямовані на перезавантаження мережевих ресурсів з метою виведення їх з ладу. Крім того, велику небезпеку становлять фішингові атаки , які використовують для викрадення облікових даних користувачів шляхом обману [6]. Витоки конфіденційної інформації, спричинені як внутрішніми,

так і зовнішніми факторами, є ще одним викликом для сучасних організацій [7]. Окремо варто зазначити загрозу використання шкідливого програмного забезпечення , яке може включати віруси, трояни, шпигунські програми та програми-вимагачі [8]. За останні роки особливої актуальності набули атаки на основі вразливостей у хмарних системах, оскільки все більше компаній переходять на використання хмарних обчислень, не завжди забезпечуючи належний рівень їх безпеки.

Захист від зазначених загроз вимагає використання низки технологій, таких як брендмауери, систем виявлення та запобігання вторгненню (IDS/IPS), засобів шифрування даних і сегментації мережі [9]. Виявлені інтелектуальні системи моніторингу, що базуються на технологіях штучного інтелекту та машинного навчання, значно підвищують ефективність аномалій у мережевому трафіку [10]. Крім того, впровадження принципів Zero Trust, які передбачають перевірку всіх користувачів і пристроїв незалежно від того, перебувають вони всередині чи поза мережею, знижують ризики.

Таким чином, концепція мережевої безпеки базується на чітко визначених принципах і сучасних технологічних підходах, які залишаються надійним захистом мережевої інфраструктури навіть у складних умовах збільшення масштабу кіберзагрози. Системний підхід до побудови багаторівневого захисту та постійне вдосконалення засобів безпеки є ключовими для протидії сучасним викликам у сфері кібербезпеки.

Для ефективного захисту мережі та даних від зазначених загроз необхідний комплексний підхід до кібербезпеки, який включає технології, методи та стратегії для зменшення виявлених ризиків. Із важливих аспектів є правильна конфігурація мережевих пристроїв та серверів, що дозволяє контролювати і фільтрувати трафік, а також відслідковувати всі спроби несанкціонованого доступу. Застосування технології VPN (віртуальні приватні мережі) дозволяє створити зашифровані канали для передачі даних, що супроводжує безпеку інформаційного обміну в мережах.

Можливі на розвиток технологій захисту, важливу роль у забезпеченні мережевої безпеки дієвий людський фактор [11]. Часто саме через неважливість або недосвідченість співробітників організацій відбуваються інциденти безпеки, такі як витоки інформації або успішні фішингові атаки. Тому для підвищення рівня безпеки необхідно регулярно проводити тренінги та навчання для працівників, щоб вони могли адекватно реагувати на можливості загрози та усвідомити важливість дотримання стандартів безпеки [12]. Впровадження корпоративних політик, які регламентують використання пристроїв та доступ до ресурсів, також хочуть знизити ймовірність несанкціонованого доступу та підвищити загальний рівень безпеки мережі.

Ще одним елементом у забезпеченні мережевої безпеки є ефективна система резервного копіювання та відновлення даних. У разі атаки програмами-вимагачами або втрати даних через технічні засоби наявність актуальних резервних копій може значно зменшити негативні слідки та допомогти організаціям відновити свої операції в найкоротші терміни. Оскільки сучасні методи шифрування, як AES (Advanced Encryption Standard), дозволяють забезпечити високий рівень захисту даних навіть при їх зберіганні в хмарних сховищах, це стає зареєстрованим інструментом для захисту корпоративних даних від несанкціонованого доступу та втрати.

Крім того, слід відзначити важливість моніторингу мережі на всіх етапах її функціонування. Системи моніторингу, які включають аналіз трафіку в реальному часі, здатні виявляти аномалії, які можуть свідчити про спроби атаки або несанкціонований доступ. Використання інтегрованих системних загроз, які аналізують дані на основі поведінки батьків, дозволяє швидко виявити нові типи атак, навіть якщо вони не будуть зафіксовані в базах даних підпису. Для підвищення ефективності таких систем часто використовують методи машинного навчання та штучного інтелекту, які дають змогу вдосконалити алгоритм виявлення загроз, зменшуючи кількість помилкових спрацьовувань і підвищуючи точність виявлення реальних атак.

Не менше є забезпечення фізичної безпеки мережевих пристроїв та серверних кімнат. Захист від фізичних загроз, таких як несанкціонований доступ до серверів або викрадення обладнання, є критичним елементом загальної стратегії кібербезпеки. Для цієї системи контролю доступу, відеоспостереження, а також застосовуються методи криптографії для захисту даних навіть у разі фізичної втрати пристрою.

Сучасні тенденції у сфері мережевої безпеки свідчать про необхідність інтеграції традиційних підходів із новітніми технологіями для більш ефективного протистояння загрозам. В умовах швидкого розвитку технологій та глобалізації Інтернету важливою складовою мережевої безпеки є адаптація до нових викликів, зокрема до загроз, пов’язаних з Інтернет-речами (IoT) та розвитком мережі 5G. Ці технології створюють нові можливості для підключення пристроїв, що вимагають від організації впровадження додаткових рівнів захисту та забезпечення безпеки на кожному етапі життєвого циклу пристроїв і мереж.

Враховуючи швидкий розвиток технологій і зростаючі загрози, майбутнє мережевої безпеки, ймовірно, буде зосереджено на використанні більш складних та інтегрованих рішень, включаючи штучний інтелект, блокчейн, а також квантову криптографію для захисту інформації. Підвищення ефективності реагування на інциденти та вдосконалення процесів відновлення після атаки стануть основними завданнями для майбутнього розвитку мережевої безпеки. Тільки таким чином можна забезпечити надійний захист інформаційних систем і зберегти цілість та конфіденційність даних у цифровому середовищі.

1.2. Основи архітектури Check Point: історія, функціональність, ключові особливості продукту

Check Point Software Technologies є однією з найбільш відомих компаній у сфері кібербезпеки, яка розробляє програмні та апаратні рішення для захисту мереж, інформаційних систем і корпоративних даних [13]. Заснована

в 1993 році в Ізраїлі, компанія швидко завоювала ринок завдяки інноваційним підходам до захисту мережі та створенню надійних продуктів для безпеки. Вже на початку своєї діяльності Check Point представила одну з перших технологій міжмережевих екранів (firewall), що стала основою для подальших розробок компанії, орієнтуючись на створення рішень для гнучкої та надійної системи захисту від зовнішніх і внутрішніх загроз. Система безпеки Check Point використовує широкий спектр інструментів для захисту периметра, а також для забезпечення безпеки в хмарних середовищах і на мобільних пристроях, що робить її однією з найбільших на ринку.

Основна функціональність архітектури Check Point забезпечує багаторівневий захист, що включає фільтрацію трафіку, захист від шкідливого ПЗ, а також технології для боротьби з атакуючими загрозами, такими як DDoS, фішинг, експлойти та інші види зловмисних атак [14]. Одна з ключових особливостей є здатністю продукту Check Point інтегруватися з іншими технологіями безпеки та забезпечити централізоване управління через єдину панель адміністрування [15]. Це дозволяє адміністраторам швидко реагувати на загрози, що з'являються, і завдяки цьому моніторинг мережевих подій у реальному часі. Крім того, Check Point активно використовує аналітику великих даних і алгоритми штучного інтелекту для виявлення аномалій у мережевому трафіку, що дозволяє точніше передавати та запобігати новим типам атак.

Продукти Check Point знають свою високу надійність та масштабність, що дозволяє заборонити їх як у малих компаніях, так і у великих корпораціях з розподіленими мережами. Основною технологією безпеки є фірмова система фільтрації трафіку, яка здатна блокувати небажаний або шкідливий трафік на основі сигнатури, а також аналізувати поведінку пакетів для створення нових типів загроз. Check Point також пропонує рішення для інтеграції з хмарними сервісами та віртуальними інфраструктурами, що є комерційним аспектом у сучасних умовах, коли все більше компаній переходять на хмарні технології та гібридні моделі [16]. Продукти включають

інструменти моніторингу хмарних середовищ, що дозволяють забезпечити високу безпеку навіть у складних і динамічних умовах.

Ще важливою особливістю є технологія SandBlast, яка дозволяє перевіряти контент на наявність шкідливих файлів і працювати на основі поведінкових патернів, знижуючи ймовірність попадання нових вірусів і шкідливого коду в мережу. Технологія SandBlast значно ефективніше захистити від нульових загроз, таких як нові троянів або варіантів програм-вимагачів, після чого вона глибоко аналізує файли та застосовує динамічну емуляцію для виявлення шкідливих дій, які не були зафіксовані раніше [17].

Важливою складовою архітектури Check Point також є система управління політиками безпеки, яка дає змогу централізовано досягти правил доступу та провести аудит мережевих подій [18]. Вона підтримує не лише стандартні правила доступу, а й більш складні стратегії захисту, включаючи захист від витоків даних та захист від нападу за допомогою технологій машинного навчання. Інтерфейс управління продуктами Check Point дозволяє адміністраторам досліджувати і коригувати політики безпеки в режимі реального часу, що важливо для забезпечення оперативної реакції на нові загрози.

Продукти Check Point також пропонують інтеграцію з іншими засобами захисту, такими як виявлення системи та запобігання інтелектуальним системам (IDS/IPS), а також рішення для забезпечення безпечних точок безпеки [19]. Це дозволяє організації створити багаторівневий захист, який лише забезпечує блокування атак на мережевому рівні, але включає моніторинг та захист пристроїв, які підключаються до корпоративної мережі. В цілому, архітектура Check Point є високофункціональною і масштабованою, що дозволяє їй ефективно захищати як дрібні підприємства, так і великі корпорації з великими і складними інфраструктурами.

Загалом, архітектура Check Point є єдиною з найбільш просунутих у сферу мережевої безпеки, що забезпечує у собі багаторівневий захист,

інноваційні технології загроз та масштабованість для різних типів організацій. Компанія активно працює над удосконаленням своїх продуктів, орієнтуючись на новітні тенденції в області кібербезпеки, як інтеграція з хмарними технологіями та використання методів штучного інтелекту для більш ефективного виявлення загроз.

Захист мережевої інфраструктури в сучасному світі стає все більш складним через постійне зростання кількості кіберзагроз і швидкий розвиток технологій. відповідно до цього, компанії, що спеціалізуються на безпеці, постійно оновлюють і вдосконалюють свої рішення для того, щоб відповідати новим вимогам і викликам кіберпростору [20].

Велике значення для Check Point має впровадження принципу Zero Trust, який обґрунтовується на постійній перевірці всіх користувачів і пристроїв, незалежно від того, чи перебувають вони всередині або за межами корпоративної мережі. Це означає, що кожен запит на доступ до ресурсів перевіряється, навіть якщо він надходить з уже автентифікованих джерел. Такий підхід забезпечує підвищений рівень безпеки, не зміг би отримати доступ до критичних ресурсів без додаткових перевірок і контролю. Впровадження Zero Trust дозволяє організації більш ефективно контролювати доступ до своїх даних, знижуючи ризик витоку інформації або її викрадання.

Ще одним аспектом, який активно впроваджує Check Point, є технологія захисту від атак на рівні додатків. Оскільки багато атак сьогодні спрямовані саме на уразливі додатки, компанія розробила спеціалізовані рішення для моніторингу та захисту додатків від різних типів атак, таких як SQL-інтеграції, кроссайтові скрипти (XSS) та інші [21]. Вони лише блокувати шкідливий трафік, але й запобігти виявленню та використанню вразливих місць у коді додатків. Це дозволяє захистити як веб-додатки, так і мобільні додатки, що є важливою складовою для сучасних компаній, після того як усі інші організації використовують додатки для забезпечення доступу до своїх сервісів і даних.

Крім того, значну увагу Check Point надає безпеці віртуальних мереж і хмарної інфраструктури, оскільки з часом все більше підприємств переходять на хмарні сервіси для зберігання даних і розгортання своїх систем. Одним із найбільш актуальних напрямків у цій сфері є захист гібридних хмарних середовищ, в яких створені як локальні, так і хмарні ресурси. Check Point пропонує рішення для виявлення загроз, які можуть виникнути при передачі даних між хмарними та локальними середовищами, а також для забезпечення захисту від можливих витоків інформації в таких системах. Система безпеки від Check Point дозволяє організаціям надійно керувати доступом до своїх даних, які зберігаються в хмарі, і мінімізувати ризики, пов’язані з хмарними обчисленнями [22].

Важливим аспектом діяльності Check Point є підтримка мобільних пристроїв, що є забезпеченням сучасних організацій, де співробітники працюють не лише в офісі, а й часто використовують мобільні телефони та планшети для доступу до корпоративних даних і додатків [23]. З цієї причини Check Point пропонує спеціальні технології для забезпечення безпеки мобільних пристроїв, що включають шифрування даних, контроль за додатками, які встановлюються на пристрої, а також захист від шкідливих програм, які можуть потрапити на мобільні пристрої через Інтернет. Ці технології забезпечують збереження високого рівня безпеки, навіть якщо співробітники використовують свої особливості пристроїв для роботи.

Важливе значення для компанії має інтеграція з системами моніторингу та управління безпекою (SIEM), що дозволяє централізувати збір та аналізувати логів з різними системами безпеки, а також оперативно реагувати на інциденти безпеки [24]. Це дозволяє адміністраторам ефективно координувати дії щодо виявлення та усунення загроз, а також забезпечувати дотримання вимог до звітності та аудиту. Усі ці рішення, спрямовані на зменшення часу реагування на загрози та підвищення оперативності в управлінні максимальною безпекою.

Також одним із напрямків розвитку архітектури Check Point є можливість розширення для управління через хмарні сервіси. Компанія надає можливість централізованого управління безпекою через хмару, що дозволяє знизити витрати на інфраструктуру та роботу персоналу, одночасно підвищуючи ефективність і гучність рішень. У зв'язку з цією компанія активно працює над удосконаленням хмарної платформи безпеки, що дозволяє організаціям швидко налагодити правила безпеки та ефективно координувати дії в різних регіонах і підрозділах. Це дозволяє швидше і точніше реагувати на зміни в середовищі безпеки, що є місцем для сучасних динамічних умов.

Таким чином, Check Point є єдиною з провідних компаній, яка пропонує високотехнологічні рішення для забезпечення безпеки сучасних мереж, від простих локальних до складних гібридних і хмарних інфраструктур. Постійне оновлення продукту та впровадження новітніх технологій дозволяє їй залишитися на передовій у галузі кібербезпеки та ефективно протистояти новим типам загроз. Інтеграція з іншими системами дозволяє створювати цільні екосистеми безпеки, де кожен елемент взаємодіє з іншими, забезпечуючи максимальний рівень захисту та спрощене адміністрування.

Велика увага в системах безпеки Check Point також приєднується до автоматизації процесів виявлення та реагування на загрози [25]. Сучасні кіберзагрози постійно змінюються, і тому важливі мати інструменти, які можуть швидко реагувати на нові типи атак. Системи, розроблені компанією, виконують технології машинного навчання та аналізу великих даних, що дозволяє автоматично виявляти аномалії в трафіку і вжити деякі заходи без участі людини. Така автоматизація дає можливість лише підвищити ефективність виявлення загрози, а й значно скоротити час на реагування, що є критичним в умовах сучасних швидких і складних атак.

Для організацій, які працюють в умовах високої волатильності та змінності навколишнього середовища, у числі аспектів є також здатність Check Point підтримувати гнучкість у налаштуваннях безпеки. Продукти

компанії повинні адаптувати налаштування безпеки до конкретних вимог кожної організації, що робить їх особливо корисними для підприємств з різноманітними видами діяльності. Це включає в себе можливість кастомізації політики безпеки, що дозволяє встановити рівень захисту в залежності від потреби конкретного відділу або групи користувачів [26]. Таким чином, Check Point забезпечує масштабованість та адаптивність своїх рішень, що робить їх ефективними в різних ситуаціях і для різних типів інфраструктури.

Ще одним аспектом є акцент на забезпеченні безпеки шляхом автоматичного оновлення баз даних та програмного забезпечення. Системи Check Point постійно підтримуються оновлення, які не можуть захистити користувачів від нових загроз, зокрема від змін у поведінці шкідливого програмного забезпечення та нових вразливостей [27]. Вони включають інтелектуальну атак на основі шаблонів поведінки, що дозволяє забезпечити ще вищий рівень безпеки, навіть якщо конкретна загроза не буде ідентифікована традиційними методами. Це дозволяє знизити ймовірність того, що система залишиться вразливою до нового нападу.

У зв’язку з глобалізацією та інтеграцією підприємств у міжнародні ринки, числом елементів є забезпечення багатомовної підтримки продукту Check Point.

Велике значення для архітектури Check Point має також під різні типи протоколів і технологій для з'єднання з іншими системами безпеки. Це включає як традиційні протоколи для роботи з мережами, так і нові стандарти для безпеки віртуальних і хмарних середовищ. Завдяки цьому рішенню компанії можуть працювати в складних і розподілених інфраструктурах, таких як дата-центри, гібридні хмари, а також забезпечувати захист IoT-пристроїв, які стають все більш розширеними в сучасних технологічних рішеннях.

Не менш важливою частиною архітектури Check Point є її можливості для глибокого аналізу мережевого трафіку, що дозволяє детально розробити

всі вхідні та вихідні з’єднання в мережі та виявити навіть найскладніші загрози, такі як зловмисний трафік, закриті канали зв’язку та спроби обходу безпеки системи. . Це дає змогу вчасно виявляти атаки, які можуть бути не помічені іншими засобами захисту. Аналіз мережевого трафіку також дозволяє компаніям отримати цінну інформацію про стан їх мережевої інфраструктури і остаточно реагувати на деякі загрози, перш ніж вони призведуть до серйозних наслідків.

Таким чином, архітектура Check Point є високоефективним комплексним рішенням для забезпечення корпоративної мережі, яке враховує всі можливості безпеки та сценарії їх реалізації. Постійне вдосконалення та оновлення технологій дозволяє продуктам Check Point залишатися актуальними та ефективними в умовах сучасного кіберпростору, що постійно змінюється і стає все більш складним.

У порівнянні з конкурентами Check Point займає сильні позиції в сегменті enterprise-безпеки. Для обґрунтування доцільності вибору цього продукту доцільно розглянути його у контексті інших рішень, які активно використовуються в інфраструктурах підприємств (таб. 1.1).

Таблиця 1.1 - Таблиця порівняльних характеристик

Критерій	Check Point	Fortinet (FortiGate)	Cisco ASA / Firepower	Palo Alto Networks
Тип архітектури	Централізована	Централізована	Модульна	Мікросервісна
Управління політиками	SmartConsole (GUI)	FortiManager	ASDM / FMC	Panorama
Виявлення загроз	ThreatCloud, SandBlast	FortiGuard, AI/ML	Snort (Cisco Talos)	WildFire, Cortex XDR
Підтримка Zero Trust	Так	Частково	Частково	Так
Пісочниця (sandboxing)	SandBlast	FortiSandbox	Частково	WildFire
Централізований журнал подій	Так (SmartEvent)	Так	Частково	Так
VPN, IPsec / SSL підтримка	Так	Так	Так	Так
Вартість (орієнтовно)	Висока	Середня	Середня	Висока
Простота впровадження	Висока	Середня	Висока	Середня
Сценарії застосування	Enterprise, хмара, SMB	SMB, MSSP, enterprise	SMB, campus	Enterprise, MSSP

З таблиці видно, що Check Point демонструє найкращу збалансованість у гнучкості, глибокому аналізі загроз та централізованому керуванні. На відміну від Fortinet, який має перевагу в ціні та швидкості розгортання в SMB-середовищах, Check Point краще адаптований для побудови єдиної системи безпеки великих організацій з географічно розподіленою інфраструктурою. У порівнянні з Cisco ASA, яке залишається популярним у корпоративному секторі, Check Point виграє за рахунок глибшої інтеграції SIEM, логіки виявлення Zero-Day та кращої підтримки інфраструктурних політик.

1.3. Роль компонентів мережевої безпеки (консоль, сервер управління, шлюз) у забезпеченні кіберзахисту

Компоненти мережевої безпеки, такі як консоль, сервер управління та шлюз, є основними елементами інфраструктури кіберзахисту, які взаємодіють між собою для забезпечення комплексного та ефективного захисту інформаційних систем та мережі від різноманітних загроз. Роль кожного з цих компонентів важко переоцінити, оскільки вони забезпечують лише фізичну та програмну безпеку мережі, а й політику функціонування, процедури та реагування на інциденти в реальному часі.

Консоль управління є ключовим елементом, який дозволяє адміністратору безпеки централізувати управління всіма процесами безпеки в мережі [28]. Це інтерфейс для моніторингу та налаштування безпеки всієї інфраструктури. Завдяки консолі можна отримати конфігурацію політики безпеки, керувати правилами фаєрволів, досягти системи моніторингу та навіть запустити сценарії для автоматичного реагування на інциденти. Консоль також дозволяє аналізувати журнали і логи безпеки, що додатково виявляють виявлені загрози та відслідковувати дії зловмисників, мінімізуючи час реакції на інциденти. З її допомогою адміністратор може отримати повний огляд стану безпеки і впроваджувати зміни в політиках, щоб забезпечити високий рівень захисту від атак і зловмисних дій.

Сервер управління виконує роль центрального вузла для зберігання та обробки даних про стан безпеки, а також для координації роботи різних елементів системи безпеки, таких як фаєрволи, системи IDS/IPS, а також інші механізми захисту [29]. Він забезпечує виконання політики безпеки, які були налаштовані через консоль, а також моніторинг моніторингу та збір статистики про діяльність мережі. Завдяки вашому серверу управління забезпечується безперервний контроль за станом безпеки, що включає відстеження змін у мережевому трафіку, наявність аномалії і виявлення негативних дій. Сервер управління також може обробляти інформацію з різних джерел і системи безпеки для виконання глибокого аналізу та

побудови звітів про стан кіберзахисту на підприємстві. Це додатково адміністраторам і керівникам організацій приймають обґрунтовані рішення про подальші кроки у напрямку забезпечення безпеки.

Шлюз мережевої безпеки є лінією захисту між внутрішньою мережею компанії та зовнішнім середовищем [30]. Його роль має змогу перевірити та фільтрувати весь трафік, який проходить між внутрішніми ресурсами та зовнішнім світом. Це включає в себе фільтр мережевого трафіку, контроль доступу, виявлення та блокування шкідливого програмного забезпечення, а також застосування принципів нульового довіри (Zero Trust) для перевірки всіх з'єднань, незалежно від того, чи є вони внутрішніми чи зовнішніми. Шлюз також виконує роль антивірусного бар'єру, перевіряючи всі вхідні дані на наявність вірусів, троянів, шпигунських програм та іншого шкідливого ПО. Він може працювати як міжмережевий екран, що запобігає несанкціонованому доступу до важливих корпоративних ресурсів, так і як система запобігання вторгненню (IPS), яка ви відображає та запобігає спробам атак з боку зловмисників. Оскільки зовнішні загрози, такі як DDoS-атаки, фішинг та інші типи злому, залишаються дедалі складнішими, шлюз стає критично важливим для забезпечення безпеки підприємства в умовах сучасних кіберзагроз.

Одним із важливих аспектів ролі шлюзує здатність працювати в умовах високої вантажопідйомності та обробляти великий обсяг трафіку без втрати продуктивності. В умовах сучасного кіберпростору де організації часто стикаються з великими обсягами даних і швидкими змінами в типах атак, шлюзи повинні мати високу пропускну здатність і швидкість обробки, щоб забезпечити надійний захист без впливу на загальну продуктивність мережі. Вони також повинні підтримувати різні протоколи і технології, включаючи VPN, SSL/TLS, а також новітні стандарти для захисту віртуальних і хмарних середовищ.

Важливою рисою цих компонентів є їх взаємодія для створення єдиної екосистеми безпеки, де кожен елемент створює свою ключову роль. Консоль

управління забезпечує централізоване управління та контроль, сервер управління забезпечує збереження та обробку даних безпеки, а шлюз виконує безпосередній захист мережевих з'єднань, фільтруючи та блокуючи загрози на рівнях трафіку. Усі ці компоненти працюють у тісній взаємодії для того, щоб забезпечити всебічний захист організацій від різноманітних кіберзагроз.

Загалом, роль цих компонентів у забезпеченні кіберзахисту є важливою для створення надійної системи безпеки, яка здатна протистояти як зовнішнім, так і внутрішнім загрозам. Їх взаємодія дозволяє організаціям забезпечити конфіденційність, цілість та доступність даних, зменшуючи ризики втрат і атак. Застосування таких рішень в умовах швидко змінюваного кіберсередовища є необхідним для стійкості та безпеки сучасних інформаційних систем і мереж.

2. МЕХАНІЗМИ РЕАЛІЗАЦІЇ ЗАХИСТУ МЕРЕЖІ ЗА ДОПОМОГОЮ CHECK POINT

2.1. Управління через SmartConsole: принципи роботи, можливості та функції

Управління через SmartConsole є одним з аспектів сучасних технологічних систем, які використовують для адміністрування та моніторингу комп'ютерних мереж та інформаційних систем. Основною метою застосування SmartConsole є забезпечення інтеграції різних функцій управління в одному інтерфейсі, що дозволяє спростити процеси адміністрування та забезпечити високий рівень безпеки. відповідно до принципів роботи SmartConsole, основним завданням є створення єдиного інтерфейсу для здійснення різноманітних операцій, що дозволяє користувачам ефективно керувати налаштуваннями без необхідності використання кількох програм чи панелей керування. Наприклад, SmartConsole дає можливість моніторити стан системи, переглядати логи подій, виконувати налаштування безпеки та керувати політиками доступу.

Ключовими можливостями SmartConsole є централізоване управління, яке забезпечує широкий спектр налаштувань і функцій. Система дозволяє адміністратору проводити моніторинг поточного стану мережі, що включає в себе аналіз трафіку, виявлення наявних загроз і вразливостей, а також управління політиками безпеки. Завдяки інтеграції різноманітних інструментів, адміністратори можуть забезпечити швидкий доступ до потрібних налаштувань і використовувати інтерфейс для виконання рутинних завдань, таких як створення або зміна облікових записів, налаштування фаєрволів, а також визначення правил доступу до різних ресурсів. Важливим елементом є також підтримка багаторазових профілів, що дозволяє організаціям мати налаштування для різних користувачів або груп.

Функціональні можливості SmartConsole включають також системи створення звітів та аналізу даних, які дозволяють отримати детальну

інформацію про стан мережі, інциденти безпеки, а також про ефективність роботи [31]. Це важливо для оперативного реагування на події та проблеми, що виникають у мережі, що сприяють підтримці належного рівня безпеки та стабільності. Із найбільш значущих аспектів є використання інтуїтивно зрозумілого інтерфейсу, що дозволяє знизити рівень стійкості виконання завдань для адміністратора, а також надає одну можливість моніторингу системи в реальному часі.

До важливих функцій SmartConsole також можна надати можливість налаштування політики, що включає в себе правила керування фаєрволом, впровадження заходів з кібербезпеки та надання доступу до безпеки певних ресурсів на основі ролей користувачів. Це дозволяє мінімізувати ризики несанкціонованого доступу та помилок при конфігурації системи, що є критичним у середовищі, де безпека є пріоритетом. Крім того, система дозволяє виконувати автоматизовані перевірки безпеки, які допомагають виявляти слабкі місця та своєчасно реагувати на поточні загрози.

Завдяки своєму високому рівню інтеграції та централізованому управлінню, SmartConsole може використовуватися для адміністрування різних типів технологічної інфраструктури. Це включає як невеликі організації, так і великі підприємства, де важливо забезпечити ефективну безпеку роботи та надійний доступ до даних. У сучасному світі де кіберзагрози залишаються дедалі складнішими, такі інструменти як SmartConsole мають важливе значення для підтримки високого рівня захисту інформації та забезпечення стабільної роботи корпоративних систем.

Управління через SmartConsole здобуло широку популярність завдяки вашій здатності забезпечувати ефективне й оперативне адміністрування технологічних та інформаційних систем. без можливості централізованого управління та налаштування параметрів мережевої безпеки, SmartConsole надає потужні інструменти для інтеграції з іншими корпоративними додатками та технологіями. Наприклад, через SmartConsole можна включити моніторинг і налаштування фаєрволів, виявлення системи та запобігання

вторгненню, а також інші засоби забезпечення безпеки, які дозволяють отримати повну картину стану захисту мережі в режимі реального часу. Однією з основних переваг цього підходу є те, що адміністратор отримує можливість лише контролювати різні аспекти мережі, а й автоматизувати багато процесів, зменшуючи тим самим ймовірність людських помилок, що є ключовим фактором для забезпечення високої надійності та безпеки системи.

Інтеграція SmartConsole з іншими інструментами та рішеннями дає можливість зібрати великий обсяг інформації про стан безпеки, продуктивність і використання ресурсів. Важливим є те, що система підтримує аналіз та звітність у реальному часі, що дозволяє швидко виявити аномалії, несанкціоновані дії чи інші інциденти безпеки, реагуючи на них майже миттєво. Ці функціональні можливості зробити SmartConsole незамінним інструментом у великих організаціях, де безпека інформаційних систем та управління доступом мають критичне значення для стабільності та безперебійної роботи.

Одним із основних аспектів ефективного використання SmartConsole є гнучкість налаштування безпеки. Система дозволяє не тільки розробляти універсальні правила для всієї організації, а й детально досліджувати параметри безпеки для конкретних відділів або груп користувачів, що значно підвищує ефективність управління доступом. Такі можливості є більшими для великих корпорацій, де доступ до ресурсів та інформації може відрізнятися залежно від функціональних обов’язків співробітників. Це дозволяє мінімізувати ризики несанкціонованого доступу до критичних даних або важливих систем, що особливо актуально в умовах швидко зростаючих кіберзагроз.

Крім того, один із важливих переваг використання SmartConsole є його здатність забезпечувати прозорість і контроль за діями адміністратора. Усі зміни в системі, включаючи налаштування політики безпеки, виконання оновлень або конфігураційних змін, фіксуються в журналах подій, що дозволяє створити детальну звітність та забезпечити аудиторський контроль.

Завдяки такому функціоналу можна проводити ретельний аналіз усіх операцій, що містяться в системі, і швидко виявляти якісь небезпечні зміни або несанкціоновані дії, що значно підвищує рівень безпеки організації в цілому.

Надійність і безпека SmartConsole також забезпечується впровадженням передових технологій шифрування даних і захисту від зовнішніх атак. Використання таких засобів захисту дозволяє забезпечити цільність і конфіденційність переданої інформації, що є масою аспектів для багатьох організацій, які працюють з чутливими даними. Також варто зазначити, що за допомогою налаштування можливостей багаторівневої аутентифікації користувачі мають можливість використовувати додаткові заходи безпеки, зокрема двофакторну атентифікацію, що додає ще один рівень захисту системи від несанкціонованого доступу.

Управління через SmartConsole також дозволяє ефективно управляти інцидентами, пов’язаними з безпекою. таким чином, система надає інструменти для автоматичного реагування на певні типи інцидентів, що значно скорочує час реагування на явно небезпечній ситуації. У випадку виявлення загрози система може автоматично блокувати доступ до вразливих ресурсів або запускати сценарії для усунення наслідків інциденту, що забезпечує високу швидкість реагування та мінімізує шкоду від нападу.

Важливою складовою ефективного використання SmartConsole є навчання персоналу та розвиток навичок роботи з цією системою. Система може бути складною для початківців, тому необхідно забезпечити кваліфіковану підготовку адміністраторів і користувачів, що дозволить їм ефективно використовувати всі функціональні можливості інтерфейсу без ризику помилок. незалежно від того, важливо регулярно проводити аудит безпеки та перевірку налаштувань систем, щоб забезпечити актуальність і ефективність усіх політик безпеки в умовах швидких змін у сфері кіберзагроз.

Таким чином, управління через SmartConsole є потужним і багатофункціональним інструментом для адміністрування сучасних інформаційних систем і мереж. Завдяки своїй універсальності та зручному інтерфейсу ця система стає незамінним інструментом для організацій, які прагнуть забезпечити високу надійність і безпеку своїх технологічних та інформаційних ресурсів.

2.2. Впровадження та адміністрування Security Management Server: політика налаштування, зберігання журналів

Впровадження та адміністрування Security Management Server (SMS) є етапом у створенні та підтримці безпеки інформаційних систем на корпоративному рівні. Цей сервер є ключовим компонентом в архітектурі управління безпекою мережі, не дозволяє централізовано керувати політиками безпеки, здійснювати моніторинг мережі, підтримувати й аналізувати журнали подій, а також використовувати оперативне реагування на деякі загрози. Основна настройка налаштування Security Management Server є створенням безпечного та стабільного середовища для корпоративних інформаційних систем, яке забезпечує контроль над усіма аспектами безпеки: від фаєрволів до захисту від кіберзагроз [32]. Для цього необхідно використовувати політику безпеки, визначати стратегії зберігання журналів та впроваджувати систему моніторингу подій.

Політика налаштування Security Management Server обхоплює декілька ключових аспектів, серед яких одним із встановлених є налаштування доступу, визначення правил для фаєрволів, а також перевірка створення правил для вразливостей. Важливо зазначити, що політика безпеки повинна бути гнучкою й адаптованою до конкретних потреб організації, з урахуванням її структури, масштабів та характеру діяльності. Встановлення чітких правил доступу, які дозволяють лише авторизованим користувачам отримувати доступ до конфіденційної інформації, є основою для забезпечення безпеки на рівні сервера. Крім того, налаштування повинні

включати визначення політики захисту мережі, яка має на мету блокувати несанкціоновані спроби доступу до системи та впровадження заходів для захисту від атак, таких як DDoS або інші типи відмови в обслуговуванні.

Одним із важливих аспектів адміністрування Security Management Server є зберігання журналів подій. Журнали безпеки використовують інструмент для аналізу інцидентів та виконання аудиту безпеки, після чого вони знають інформацію про всі дії в системі, включаючи спроби доступу, зміни в налаштуваннях, а також інші критичні події. Налаштування політики зберігання журналів є етапом у процесі адміністрування, оскільки це налаштування, як довго і в якому форматі ці журнали будуть зберігатися. Важливо, щоб журнали зберігалися в захищеному середовищі, щоб уникнути їх підробки чи видалення зловмисників, що може ускладнити розслідування інцидентів безпеки. Крім того, налаштування повинні передбачати регулярне архівування журналів, оскільки вони можуть надати важливу інформацію для довгострокового моніторингу стану безпеки організації.

Що стосується зберігання журналів, використання підходів до їх організації, зокрема централізоване зберігання або використання спеціалізованих систем управління різними журналами (SIEM). Централізоване зберігання дозволяє зберігати всі журнали в одному місці, що спрощує процес їх аналізу та відновлення інформації за потреби. З іншого боку, SIEM-системи не дозволяють автоматизувати збір, аналіз і кореляцію даних з різними джерелами, що значно ефективніше виявлення загроз і аномалій у реальному часі. Враховуючи швидкість розвитку кіберзагроз, можливість інтеграції з такими системами дозволяє забезпечити високий рівень захисту й ефективне управління журналами безпеки. Системи SIEM також можуть автоматично виключати кореляцію подій із різними джерелами та виявляти лише небезпечні або сумнівні патерни, які після цього адміністратору швидко реагують на загрози.

Налаштування зберігання журналів також має виконувати вимоги регулюючих органів, крім того, в деяких галузях (наприклад, фінансовому

секторі чи охороні здоров'я) щодо конкретних вимог до зберігання інформації про інциденти безпеки. Це може включати вимогу охорони журналу подій протягом певного періоду часу, а також обов'язково надати доступ до них у перевірці або розслідуванні. Невиконання цих вимог може призвести до юридичних наслідків або штрафів, тому правильне налаштування політики зберігання є критичним аспектом в адмініструванні Security Management Server.

Крім того, іншим аспектом адміністрування Security Management Server є проведення регулярного моніторингу стану безпеки та аналізу збережених журналів. Це дозволяє виявити деякі загрози на ранніх стадіонах і швидко реагувати на них. Такі процеси, як регулярний аудит журналів і перевірка системних налаштувань, є адресами для підтримки високого рівня безпеки в організації. Оскільки кіберзагрози постійно еволюціонують, організація повинна постійно оновлювати свої політики безпеки та адаптувати їх до нових викликів. Враховуючи це, необхідно проводити регулярні тренінги для адміністраторів і користувачів, щоб забезпечити своєчасне реагування на інциденти безпеки та підвищити загальний рівень відомості про можливість загрози.

Впровадження Security Management Server вимагає комплексного підходу, що включає налаштування політики безпеки, оптимізацію зберігання та моніторинг журналів, а також навчання персоналу для забезпечення ефективного адміністрування. Ці кроки сприяють створенню надійної та безпечної інформаційної інфраструктури, що відповідає сучасним вимогам загроз і викликів у галузі кібербезпеки.

2.3. Шлюзи безпеки (Security Gateway): механізми блокування загроз, VPN та фільтрація трафіку

Шлюз безпеки (Security Gateway) є основним елементом захисту інформаційних систем і мереж, що забезпечує контроль і моніторинг трафіку, який проходить через корпоративні мережі [33]. Вони забезпечують важливу

роль у забезпеченні безпеки по периметру мереж, блокуванні несанкціонованого доступу та зниженні ризиків від зовнішніх загроз. Шлюзи безпеки працюють на рівнях прикладного або транспортного рівня та вибирають різноманітні механізми для забезпечення захисту від атак, несанкціонованого доступу та інших кіберзагроз. Механізми блокування загроз включають аналіз і фільтрацію трафіку, а також застосування різних методів шифрування для захисту передавання даних, таких як VPN (Virtual Private Network) [34]. Технологія VPN не дозволяє створювати зашифровані канали для передачі даних через неспокійну або незахищену мережу, забезпечуючи конфіденційність і цільність інформації під час її переміщення [35].

Шлюзи забезпечують безпеку фільтрації трафіку, що є одним з основних методів захисту, що дозволяють відслідковувати і контролювати пакети даних, які проходять через мережу. Фільтрація може бути реалізована на різних рівнях, від простого контролю доступу до складніших методів, що включають аналіз вмісту пакета, перевірку наявності шкідливого коду або спробу включення. Наприклад, за допомогою перевірки IP-адреси та портів можна блокувати підключення до відомих шкідливих джерел, а використання технологій глибокого аналізу пакетів (DPI) дозволяє детектувати та блокувати трафік, який містить зловмисне програмне забезпечення або виконує атаки на веб-сервери та інші критичні компоненти мережі [36]. Крім того, одним із елементів є контроль на основі шаблонів поведінки, коли шлюз безпеки може виявити аномалії в мережевому трафіку, які є характерними для нових типів атак, зокрема для нульових вразливостей або атак типу "троян".

Одним із ключових механізмів, які реалізують шлюзи безпеки, є технологія VPN. VPN можна створити зашифровані тунелі для передачі даних через ненадійні мережі, зокрема Інтернет, що особливо важливо для віддалених співробітників або при підключенні до корпоративної мережі з публічним точком доступу. За допомогою VPN шлюзи безпеки забезпечують конфіденційність переданої інформації шляхом шифрування пакетів, що

передаються між користувачами та корпоративною мережею. Шифрування гарантує, що навіть якщо зловмисники перехоплять дані, вони не зможуть отримати доступ до їх вмісту. Важливим аспектом є вибір алгоритмів шифрування, таких як AES (Advanced Encryption Standard), який широко використовується для забезпечення високого рівня захисту, або SSL/TLS, який є стандартом для захищених об’єднань в Інтернеті.

Іншою важливою функцією шлюзів безпеки є блокування різноманітних атак, таких як атаки DDoS (Distributed Denial of Service). Шлюзи безпеки вибирають різноманітні алгоритми для здійснення таких атак, які дозволяють зменшити ризик зупинки роботи мережі чи сервісів. Вони можуть обмежувати кількість запитів, що надходять з одного джерела, або використовувати засоби фільтрації на основі аналізу аномалій у трафіку. Крім того, шлюзи безпеки здатні виявити спроби атаки через вразливість програмного забезпечення або через застарілі системи безпеки, що робить їх кінцевим інструментом для захисту мережі від нових типів загроз.

Трафік фільтрації також включає механізми блокування шкідливих добавок та програм, які намагаються використовувати мережу для передачі вірусів, троянських програм або іншого шкідливого ПЗ. Шлюзи безпеки можуть включати в себе антивірусні системи, які в реальному часі перевіряють весь вхідний і вихідний трафік, а також системи виявлення вторгнень (IDS), які аналізують трафік на наявність перевірених патернів або аномальних активностей. Ці системи дозволяють не тільки блокувати наявні загрози, а й проактивно захищати мережу від наявних атак.

Завдяки впровадженню комплексних систем безпеки, які включають шлюзи безпеки, організації можуть не лише забезпечити захист від зовнішніх атак, але й посилити контроль над внутрішнім трафіком, що забезпечує більш високий рівень безпеки. Важливо зазначити, що ефективність таких шлюзів значною мірою залежить від правильного налаштування та оновлення політики безпеки, що дозволяє адаптувати їх до нових кіберзагроз. Тому адміністрування шлюзів безпеки має включати регулярний моніторинг та

аудит їх роботи, а також остаточне оновлення програмного забезпечення для захисту від нових вразливостей.

У результаті шлюз безпеки є компонентом інфраструктури кібербезпеки, що забезпечує надійний захист інформаційних систем і мереж від різноманітних загроз, зокрема через використання VPN, фільтрацію трафіку, виявлення атаки та забезпечення конфіденційності даних. Їх застосування дозволяє значно знизити ризики несанкціонованого доступу до ресурсів організації та забезпечити стабільну роботу всієї інформаційної інфраструктури.

Шлюзи безпеки також змінюють важливу роль у забезпеченні відповідності корпоративної мережі вимогам нормативно-правових актів, таких як GDPR (Загальний регламент захисту даних) або PCI DSS (Стандарт безпеки даних платіжних карт). таким чином, вони допомагають забезпечити належну обробку та захист персональних даних, запобігаючи їх витоку або несанкціонованому доступу. У цьому контексті шлюзи безпеки можуть бути налаштовані на застосування політики фільтрації, що обмежує доступ до чутливої інформації та моніторити трафік на об’єкт можливих пошкоджень або спробувати передавати конфіденційні дані поза межами організації. Цей аспект є особливо корисним для організацій, які працюють з персональними даними клієнтів або використовують фінансові операції, де дотримання стандартів безпеки є критичним місцем.

Важливою складовою роботою шлюзів безпеки є також інтеграція з іншими компонентами системи кібербезпеки, такими як системи виявлення та запобігання вторгненню (IDS/IPS), мережеві монітори та антивірусні програми. Вони втратили всебічний контроль над мережевим трафіком та забезпечують багатоетапний захист. У поєднанні з іншими засобами безпеки шлюзи можуть автоматично реагувати на наявні загрози, блокуючи підозрілі пакети або з’єднання, а також додаючи адміністраторів пролені аномалії в мережі. Така інтеграція дозволяє створити ефективну систему моніторингу та управління безпекою, яка здатна адаптуватися до нових загроз у реальному

часі, знижуючи ризики від нападу типу «нульовий день» (нульовий день) або нових, ще не зафіксованих вразливостей.

Іншим аспектом, на який варто звернути увагу, є забезпечення високої доступності мережі при використанні шлюзів безпеки. Враховуючи критичну роль цих пристроїв у захисній інфраструктурі, забезпечення їх безвідмовної роботи є завданням. Для багатьох із цього рішення організації, які не можуть реалізувати резервування шлюзів безпеки через кластеризацію або використання кількох пристроїв на випадок збоїв. Це забезпечує безперервність захисту навіть під час технічних несправностей або у випадку атаки на інфраструктуру. Таким чином, для досягнення високої надійності мережі необхідно впроваджувати моніторинг стану шлюзів безпеки та регулярне тестування їх можливостей.

Шлюзи безпеки також здатні виконувати детальний моніторинг і аналіз поведінки користувачів у мережі, що є місцем для виявлення не тільки зовнішніх загроз, але й внутрішніх ризиків, таких як несанкціоноване використання ресурсів або зловживання доступом. Завдяки таким функціям, як управління ідентифікацією та доступом, шлюзи можуть дозволити контролювати над тими, хто має доступ до яких ресурсів у межах корпоративної мережі. Це дозволяє знизити ймовірність внутрішніх загроз і забезпечити відповідність політикам безпеки організації.

Безкоштовно, ця шлюзі безпеки можуть бути налаштовані для забезпечення безпечного доступу до хмарних сервісів та інфраструктури, що є особливо актуальним у сучасних умовах, коли підприємства активно використовують хмарні платформи для зберігання даних та управління бізнес-процесами. Для цього шлюзи безпеки забезпечують захищені з’єднання з хмарами, дозволяючи підприємствам контролювати доступ до своїх ресурсів у хмарі, а також моніторити і фільтрувати трафік, що проходить через ці з’єднання. Зменшує ризики витоку даних або кібератак через вразливості в хмарних сервісах, що є місцем для підтримки високого рівня безпеки.

Узагалі, сучасні шлюзи безпеки є потужними інструментами для комплексного захисту інформаційних систем, які включають в себе не тільки фільтрацію трафіку та блокування атак, але й інтеграцію з іншими компонентами безпеки, забезпечення високої доступності, а також можливість забезпечення захищеного доступу до хмарних ресурсів і обробки даних. Правильна настройка та регулярне оновлення цих систем є ключовими факторами для забезпечення їх ефективності та здатності протистояти новим типам загроз. Врахування всіх цих аспектів дозволяє організувати створення стійких до кіберзагроз інфраструктур, які гарантують безпеку і стабільність їх операцій.

3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХИСТУ МЕРЕЖІ ЗА ДОПОМОГОЮ CHECK POINT

3.1 Налаштування сервера безпеки та шлюзу Check Point

Для успішної реалізації комплексного і надійного захисту всієї мережевої інфраструктури, з урахуванням актуальних загроз кібербезпеки, постійно зростаючої складності атак і високих вимог до безперебійної роботи корпоративних систем, було створено спеціалізоване тестове середовище. Це середовище моделює типову архітектуру середнього підприємства або організації, де присутні щонайменше дві ізольовані підмережі — внутрішня локальна мережа (LAN) та демілітаризована зона (DMZ), а також забезпечується підключення до глобальної мережі Інтернет [37]. Додатково була змодельована низка вузлів, які відповідають за різні функції, зокрема сервер додатків, файлове сховище та сервер автентифікації. В рамках тестового стенду реалізовано сценарії для перевірки реакції системи безпеки на типові загрози, включаючи сканування портів, спроби підбору паролів та несанкціонований доступ до сервісів усередині DMZ.

Подібна структура дозволяє моделювати як внутрішні сценарії взаємодії між хостами, так і потенційні зовнішні загрози з боку мережі Інтернет. Це надзвичайно важливо для перевірки поведінки захисних механізмів Check Point у реальних умовах. У якості технологічної основи для реалізації захисту було обрано перевірені засоби компанії Check Point, зокрема Security Management Server (SMS), шлюз безпеки Security Gateway (SG), а також клієнтське програмне забезпечення SmartConsole, яке забезпечує централізоване управління всіма компонентами інфраструктури безпеки. Усі компоненти були інтегровані у віртуальне середовище UTM з ізольованими мережами, які імітують реальні сегменти корпоративної інфраструктури [38]. Це рішення дозволило забезпечити гнучке тестування політик, реалізувати змінні сценарії загроз та оперативно аналізувати ефективність відповідних контрзаходів.

Після завантаження інсталяційного образу операційної системи Check Point Gaia було створено віртуальну машину з встановленими параметрами: IP-адреса 192.168.1.10, роль – Security Management Server. Первинне налаштування здійснено через First Time Configuration Wizard, що дозволяє швидко задати параметри мережі, керування доступом, доменне ім’я та взаємодію з іншими компонентами системи (рис. 3.1) [39].

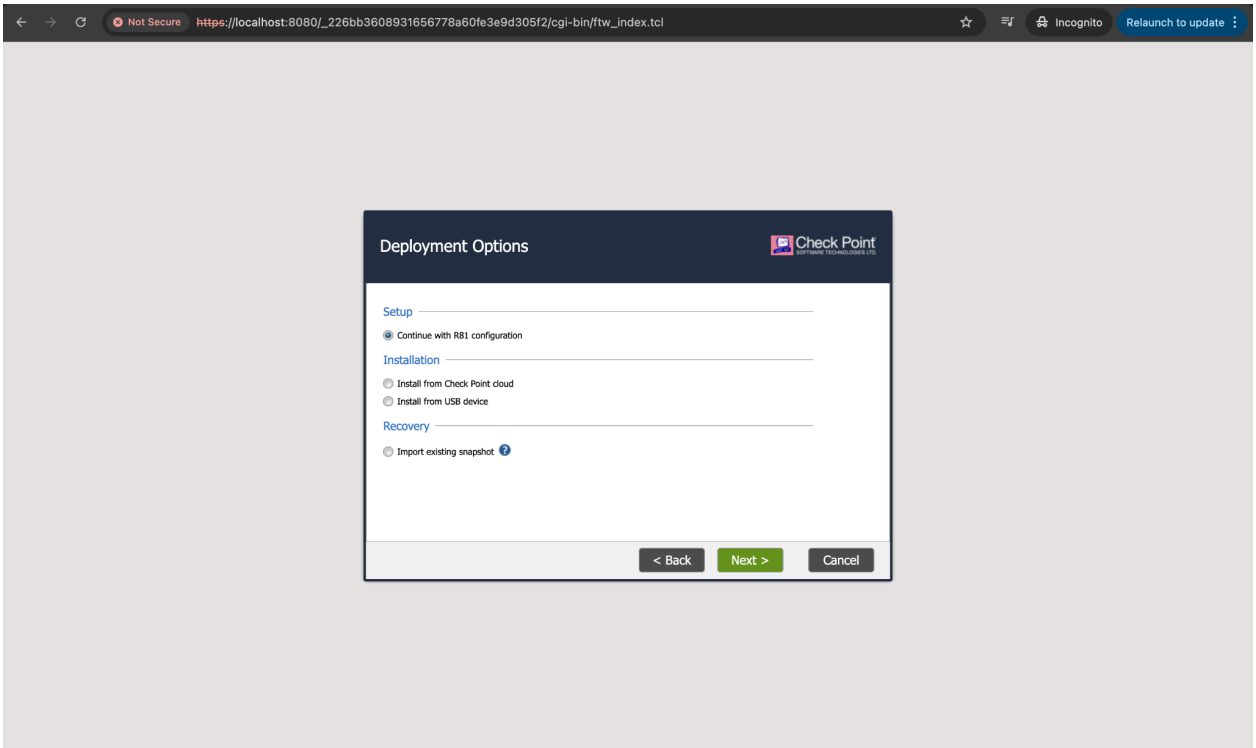

Рисунок 3.1 - First Time Configuration Wizard

Сервер був успішно зареєстрований у клієнті SmartConsole. Здійснено генерацію SIC-ключа для безпечної взаємодії з шлюзами та активацію ліцензії, а також перевірку сумісності з існуючими компонентами. Створено об’єкти мереж LAN та DMZ, хости DNS, сервера додатків та інші інфраструктурні вузли, кожен з яких був описаний у відповідній політиці доступу.

На окремій віртуальній машині було розгорнуто шлюз Security Gateway з заданими IP-адресами для інтерфейсів WAN, LAN та DMZ. У інтерфейсі Gaia WebUI задано ролі інтерфейсів, встановлено прості маршрути та виконано первинну перевірку функціональності шляхом пінгу та трасування [40].

Шлюз був доданий до SmartConsole через Secure Internal Communication (SIC), після чого система підтягнула інформацію про встановлений софт, доступні модулі безпеки та параметри апаратного середовища (рис. 3.2).

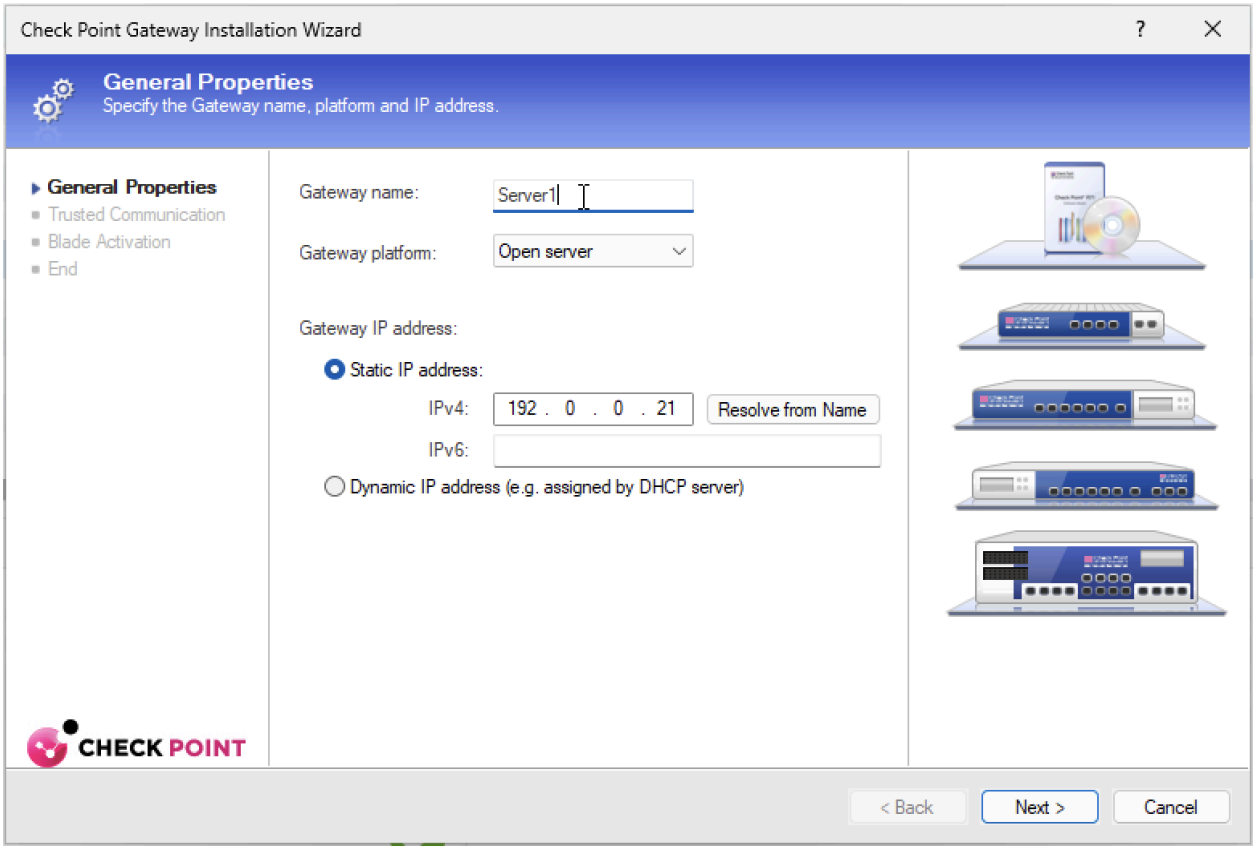

Рисунок 3.2 - Налаштування шлюз Security Gateway

Створено політику безпеки "CorporatePolicy" з трьома головними правилами (рис. 3.3):

- дозвіл трафіку з LAN до Internet по HTTP/HTTPS;
- блокування SSH-доступу до серверів;
- заборона трафіку з DMZ до LAN.

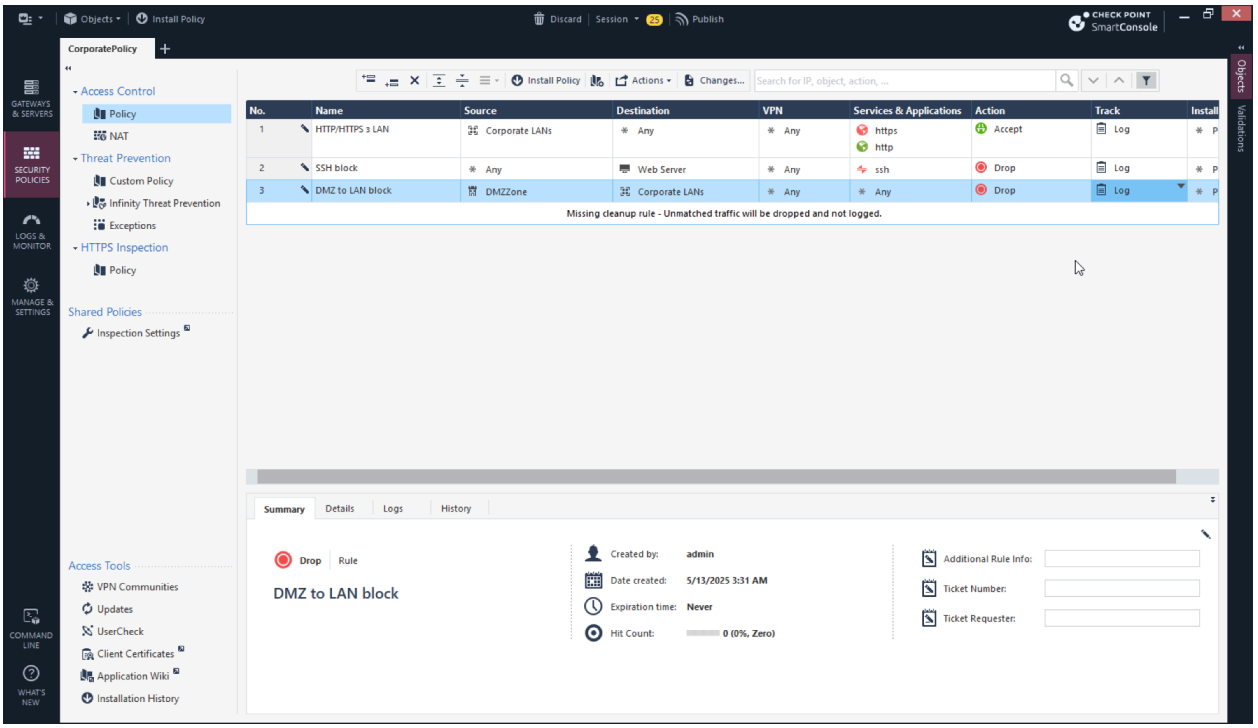

Рис 3.3 - Налаштування політики безпеки "CorporatePolicy"

Політику успішно опубліковано та застосовано до шлюза. Після застосування було виконано діагностичне тестування для перевірки коректності її виконання.

Додатково налаштовано VPN-конфігурацію для віддаленого доступу з автентифікацією через сертифікат та LDAP, обмежуючи доступ до локальної мережі. У конфігурації було враховано підтримку мобільних пристроїв та резервні сценарії підключення. Всі сервіси успішно заробили і пройшли валідацію через тестування із тестової машини, включаючи перевірку стійкості з’єднання, маршрутизації, політик доступу та логування подій в реальному часі. Це дозволило оцінити рівень надійності та функціональної гнучкості обраного рішення в умовах, максимально наближених до продуктивної експлуатації. (Рис. 3.4)

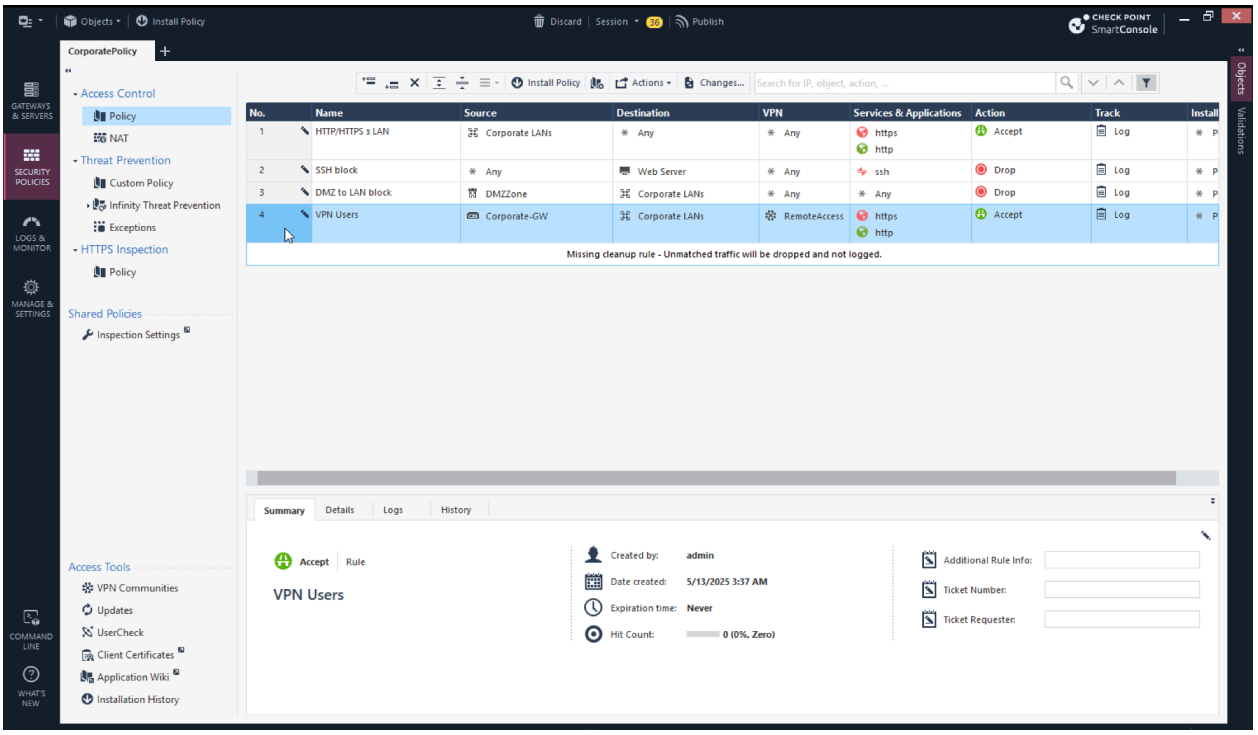

Рисунок 3.4 - Правило для користувачів VPN

3.2 Використання SmartConsole для контролю мережевих подій та реагування на інциденти

Після розгортання ключових компонентів інфраструктури захисту, надзвичайно важливим є постійний моніторинг стану мережі, оперативне виявлення загроз та своєчасне реагування на інциденти. Для цього в екосистемі Check Point передбачено зручний та функціональний інструмент управління — SmartConsole, який дозволяє реалізувати концепцію проактивного управління інформаційною безпекою.

Інтерфейс SmartConsole є інтуїтивно зрозумілим, структурованим та адаптованим до потреб адміністратора. Він дозволяє в реальному часі відслідковувати події, пов’язані з трафіком, політиками доступу, VPN-з’єднаннями, активністю користувачів, а також роботі служб фільтрації контенту, антивірусного захисту та модулів IPS/IDS. У SmartConsole реалізовано потужну систему аналітики, яка дозволяє візуалізувати мережеву активність у вигляді графіків, діаграм, часових ліній, що дає змогу швидше виявити відхилення від норми та потенційні загрози.

Після входу до SmartConsole користувач може переключитися до вкладки "Logs & Monitoring", де відображається хронологічна стрічка подій. Події можна сортувати за типом: блокування, дозволи, попередження, а також за джерелом, ціллю, сервісом, дією та іншими параметрами. Це дозволяє швидко знайти відповідь на ключове питання: яка подія викликала спрацювання захисту та як на це відреагувала система. Окрім перегляду журналів, доступна інтеграція з ThreatCloud — хмарною платформою Check Point, яка автоматично надає додаткову інформацію про IP-адреси, домени, файли, що беруть участь в підозрілих подіях (Рис. 3.5) [41].

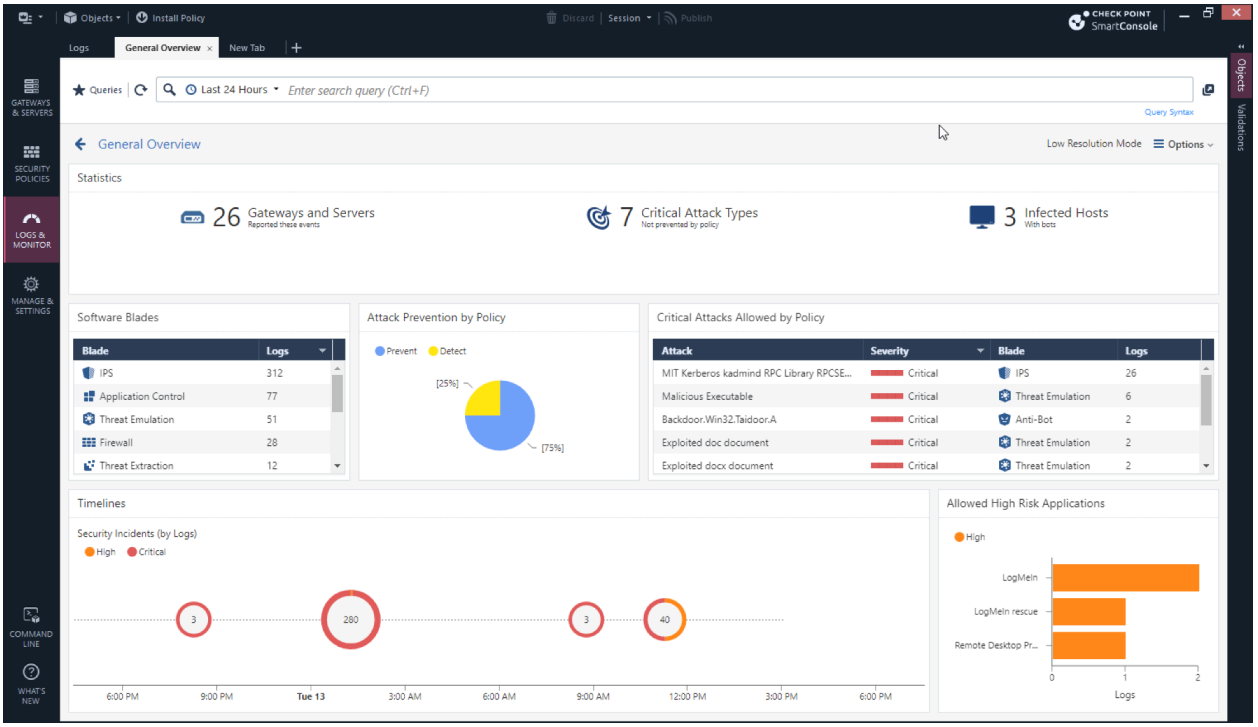

Рисунок 3.5 - Вкладки "Logs & Monitoring"

Наприклад, у випадку спроби сканування портів ззовні, SmartConsole фіксує блокування доступу до внутрішньої адреси, вказуючи джерело (IP-адресу атакувальника), ціль (внутрішній ресурс), час події, використаний протокол, а також правило політики, яке спричинило дію. Подвійне клацання на запис дозволяє переглянути детальний запис події та провести поглиблений аналіз, включаючи перегляд сесії, трасування взаємодії та

застосовані контрзаходи. У додатковому вікні можна переглянути також інформацію про географічне розташування IP-адреси джерела атаки (рис. 3.6).

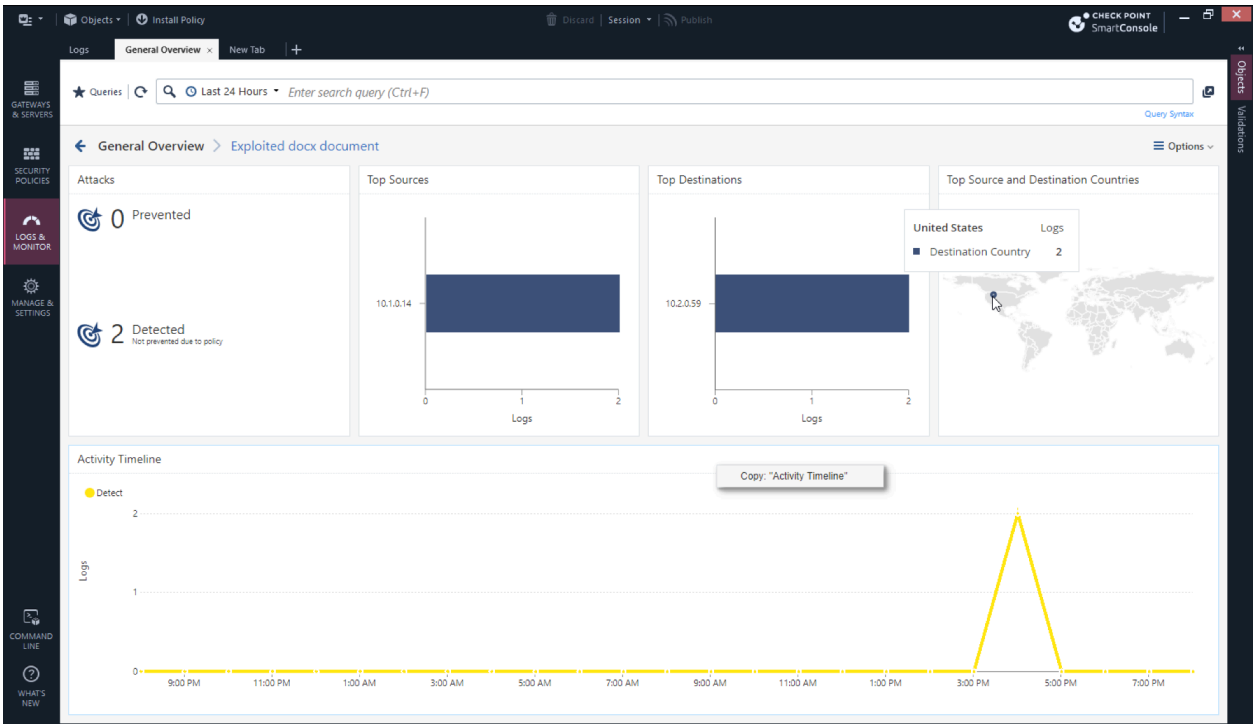

Рисунок 3.6 - Детальний запис події атаки

У межах тестового середовища було змодельовано кілька типових сценаріїв інцидентів: несанкціонована спроба SSH-доступу до шлюзу, неправильна аутентифікація через VPN, надмірна кількість підключень до внутрішнього веб-сервера, а також повторювані запити до закритих портів з одного джерела. Всі ці події були успішно зафіксовані в журналі подій і виділені кольорами згідно з рівнем критичності. Було підтверджено здатність системи автоматично виділяти події, що повторюються або відбуваються за аномальним шаблоном, і відносити їх до категорії потенційних атак.

Окремо варто зазначити можливість створення власних фільтрів та збереження їх як шаблонів для подальшого використання. Наприклад, можна створити фільтр, який автоматично виводить всі події типу "Drop" із зовнішніх IP-адрес, які повторювались більше 5 разів за останні 10 хвилин. Це особливо корисно для виявлення ботнет-активності або DoS-атак. Фільтри

дозволяють створювати індивідуальні панелі моніторингу (dashboard), що відображають тільки критичні сегменти мережі або специфічні типи загроз, що значно підвищує оперативність аналізу та прийняття рішень. (Рис. 3.7)

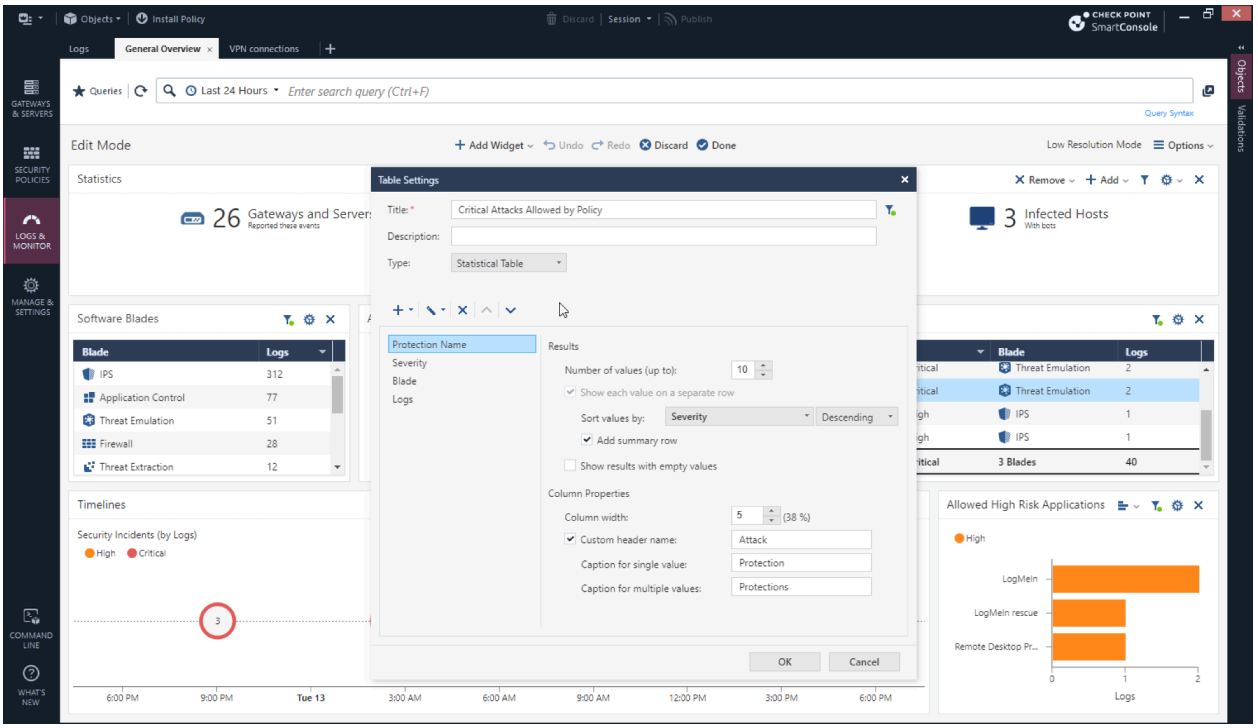

Рисунок 3.7 - Налаштування фільтрів віджету в панелі моніторингу

Також було протестовано систему сповіщень: при виникненні подій високої критичності (наприклад, кілька невдалих спроб VPN-аутентифікації з однієї адреси), адміністратор отримує повідомлення безпосередньо у інтерфейсі, а також сповіщення по електронній пошті, з можливістю дублювання у зовнішні SIEM-системи. Це значно скорочує час реагування, забезпечуючи миттєве інформування відповідальних осіб навіть за межами робочого місця.

Загалом, SmartConsole довів свою ефективність як централізований інструмент управління безпекою, який не лише спрощує адміністрування, а й забезпечує глибоку аналітику, гнучку кастомізацію звітності, візуалізацію загроз і миттєвий контроль над усіма аспектами функціонування системи захисту мережі. Результати тестування показали, що цей інструмент є

ключовим елементом ефективного реагування на загрози в сучасному середовищі, що постійно змінюється.

3.3 Тестування роботи захисних механізмів і аналіз результатів

З метою перевірки ефективності налаштованих засобів безпеки на базі Check Point було проведено розширене комплексне тестування, що охоплювало як функціональну перевірку, так і глибоку оцінку здатності системи виявляти, блокувати та логувати потенційно небезпечні дії у внутрішньому та зовнішньому трафіку. Тестування проводилося у віртуалізованому середовищі, наближеному до реальних умов корпоративного використання, із залученням ретельно змодельованих сценаріїв атак. Ці сценарії охоплювали широкий спектр загроз, що відповідають сучасним ризикам інформаційної безпеки, включаючи недбалість персоналу, помилки конфігурації, дії зловмисників із середини мережі та спроби вторгнення ззовні.

Уся процедура тестування була структурована за трьома основними напрямами: контроль доступу, протидія мережевим атакам та перевірка стабільності й безпечності VPN-з’єднань. Для кожного напряму були розроблені окремі тестові кейси із заздалегідь визначеними критеріями успішності, очікуваними результатами та метриками оцінки ефективності, серед яких: швидкість реагування системи, точність виявлення атак, рівень хибнопозитивних спрацювань, здатність до адаптації політик та легкість ведення аналітики.

У розділі перевірки контролю доступу основна увага приділялася ситуаціям, які імітують спроби доступу до критично важливих сервісів із непередбачуваних джерел. Було змодельовано кілька тестових сценаріїв, таких як спроби підключення з DMZ до внутрішніх ERP-серверів, спроби доступу до веб-інтерфейсу SmartConsole зі сторонніх IP-адрес, а також спроби внутрішнього сканування службової підмережі з гостьового Wi-Fi. Усі подібні запити були ефективно заблоковані згідно з політикою Zero Trust, а

події — зареєстровані у журналі подій з повною деталізацією: IP-джерело, порт, користувач, сесія, причина блокування та рівень критичності.

Для аналізу реакції на типові та поширені мережеві загрози було реалізовано кілька сценаріїв атак з використанням інструментів Kali Linux [42]. Проведено сканування портів із допомогою nmap, brute-force атаки через SSH за допомогою Hydra, імітацію SQL-ін'єкцій на внутрішньому веб-сервері через Metasploit, запуск DoS-атаки за допомогою LOIC та реалізацію DNS-тунелювання з використанням iodine (рис. 3.8). Крім цього, змодельовано ситуацію із застосуванням VPN-трафіку з підміною IP-адреси. IPS/IDS модулі Check Point ефективно виявили більшість спроб ідентифікувати слабкі місця, заблокували підозрілий трафік, і класифікували загрози за ступенем критичності з рекомендаціями подальших дій у інтерфейсі адміністратора.

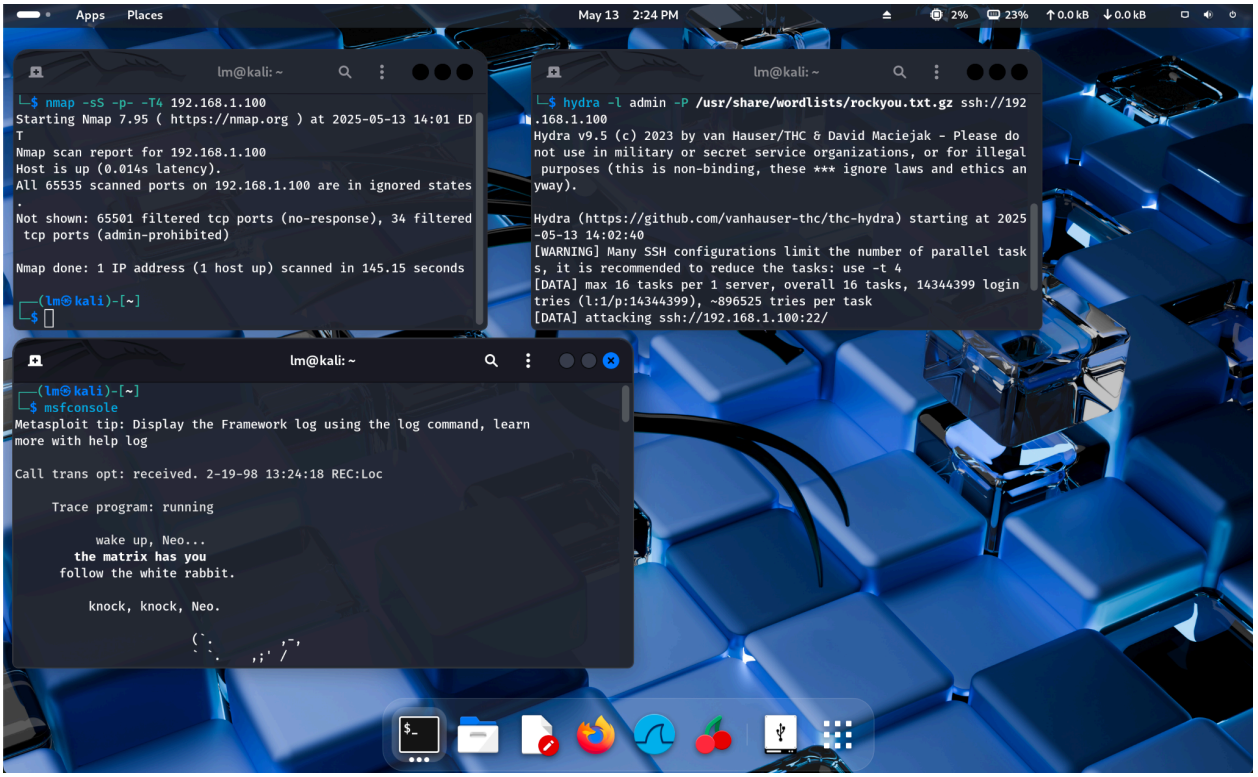

Рисунок 3.8 - Демонстрація запуску кількох утиліт для симуляції атак

У розрізі перевірки VPN-з'єднань тестувалися як стандартні сценарії авторизованого підключення до корпоративної мережі, так і спроби обходу аутентифікації з використанням прострочених сертифікатів, недійсних ключів

та невірних конфігурацій. Усі неуспішні підключення блокувалися негайно, а в логах фіксувалась інформація про причину, джерело запиту, та код помилки згідно з політикою контролю доступу. Успішні підключення здійснювалися виключно через авторизованих користувачів із використанням сертифікатів, виданих відповідним центром сертифікації та підтверджених через LDAP .

Кожен етап тестування супроводжувався детальним аудитом логів та порівнянням отриманих результатів із очікуваними. Це дозволило оцінити адекватність логіки налаштувань політик, а також виявити потенційні вузькі місця. Звіти з логів експортувалися у форматах CSV і PDF для подальшої візуалізації, аналітики та обговорення в рамках технічного аудиту. SmartConsole показала себе як ефективний та зручний інструмент для візуального аналізу, фільтрації подій, генерації кастомних звітів та контролю відповідності виявлених загроз до бази ThreatCloud.

У рамках практичних сценаріїв були виконані такі тести:

– Аудит правил фаєрволу за допомогою nmap та Zenmap: виявлено, що доступ до критичних портів (наприклад, 22, 3389, 443) ззовні заблокований, усі порушення фіксувалися в журналі з докладною інформацією про джерело сканування [43].

– Проведення SYN Flood-атаки за допомогою hping3: система змогла виявити надмірну кількість SYN-запитів до одного вузла, активувався захист від DoS і з’єднання було ізольоване [44].

– DNS-тунелювання через iodine: спроби використання нестандартного DNS-каналу були класифіковані як аномальний трафік, події миттєво заблоковані та зареєстровані у журналі [45].

– Атака SQL Injection з Kali Linux через Metasploit: інструмент використано для надсилання спеціальних запитів на веб-додаток, які були вчасно заблоковані IPS-системою, з подальшою генерацією попередження у SmartConsole [46].

– DDoS-атака через LOIC: модельована атака дозволила перевірити стійкість шлюзу до масового трафіку. Надмірна активність була обмежена

правилами обмеження пропускної здатності, а події занесені до журналу з позначкою "High Severity".

– Перевірка витоку DNS/IP через VPN за допомогою DNSleaktest та IPleak.net: усі перевірки пройдено успішно, витоків не зафіксовано, політика конфіденційності дотримана [47].

– Перехоплення SSL-трафіку за допомогою SSLsplit: спробу класифіковано як втручання у шифровану сесію, з’єднання негайно розірвано та інцидент зафіксовано з позначкою "Critical".

Додаткові приклади тестування з Kali Linux:

– Використання Nikto для виявлення уразливостей веб-серверів: Команда: nikto -h http://[IP-адреса цілі]Результат: система зафіксувала спробу сканування та класифікувала її як "Information Gathering". Подію задокументовано в логах із зазначенням сканованих портів [48].

– Тестування на XSS через XSSer: Команда: xsser --url "http://[веб-сторінка]/search.php?q=test"Результат: фаєрвол заблокував підозрілий запит, класифікувавши його як XSS-атаку. У SmartConsole згенеровано звіт з деталізацією запиту [49].

– Спроба запуску зворотного з’єднання через Netcat: На Kali: nc -lvp 4444 На цілі: bash -i >& /dev/tcp/[Kali-IP]/4444 0>&1 Результат: Check Point ідентифікував зворотне підключення як нестандартну поведінку, заблокував сесію та відобразив подію у журналі.

У підсумку, проведене тестування підтвердило високу ефективність і зрілість захисних механізмів, реалізованих у рішеннях Check Point. Усі компоненти системи, зокрема Security Gateway, SmartConsole, Security Management Server та IPS/IDS модулі, успішно справлялися зі своїми задачами. Рішення демонструє багаторівневу стійкість до атак, можливість оперативного реагування, широкі можливості для кастомізації та адаптації до змін в інфраструктурі. Це дає підстави рекомендувати його для впровадження у корпоративні мережі із підвищеними вимогами до кібербезпеки та мінімізації ризиків витоку або втрати конфіденційної інформації.

3.4 Кейси впровадження системи захисту на базі Check Point

Впровадження засобів захисту інформаційної інфраструктури на базі Check Point є доцільним у різноманітних організаційних середовищах: від малого офісу до великого розподіленого підприємства. У цьому розділі розглянуто два приклади типового впровадження.

3.4.1 Захист офісної мережі малого підприємства

Невелике підприємство, що налічує 15 співробітників, розташоване в одному офісі та використовує базові цифрові сервіси, включаючи ERP-систему, файлове сховище, електронну пошту та платформу для відеоконференцій. Частина персоналу регулярно працює дистанційно, підключаючись до офісних ресурсів із ноутбуків та мобільних пристроїв. Мережа підприємства має спрощену структуру, відсутнє розділення трафіку на сегменти, а Wi-Fi точка доступу обслуговує як внутрішніх користувачів, так і гостей, що створює підвищені ризики.

Основними викликами стали: відсутність VPN-доступу з належним рівнем захисту для віддалених працівників; спільне використання єдиного бездротового сегмента без VLAN; відкритий доступ до Інтернету з усіх пристроїв; підвищена ймовірність зараження системи шкідливим програмним забезпеченням через фішингові листи та компрометовані сайти. Також не проводився централізований аналіз подій безпеки, що унеможливлювало своєчасне реагування на інциденти.

Для розв'язання виявлених проблем було впроваджено комплексне рішення на базі Check Point Quantum Spark — шлюзу, орієнтованого на захист малих та середніх офісів. Було проведено сегментацію трафіку шляхом налаштування окремої VLAN для гостьової мережі Wi-Fi, що дозволило ізолювати зовнішній трафік від службових ресурсів. Політики фільтрації доступу були побудовані на категоріях загроз: заборонено перегляд фішингових сайтів, сайтів азартних ігор, анонімайзерів і ресурсів із поганою

репутацією. Активовано модуль IPS для виявлення експлойтів та вторгнень у режимі реального часу, а також функціональність Anti-Bot для виявлення активності бот-мереж. Антивірусний контроль було реалізовано на рівні шлюзу з оновленням сигнатур з хмарної платформи.

Окрему увагу приділено організації безпечного віддаленого доступу. Працівники, які працюють дистанційно, підключаються до офісної мережі через Remote Access VPN. Для аутентифікації використовується комбінація одноразового пароля (OTP) та цифрового сертифіката. Це дозволяє забезпечити захищене з'єднання, мінімізувати ризик несанкціонованого доступу та проконтролювати права користувачів.

Після впровадження рішень було виявлено понад 30 спроб доступу до шкідливих або небажаних ресурсів, які були заблоковані автоматично (рис. 3.9). Ізоляція гостьового трафіку забезпечила захист внутрішніх ресурсів від зовнішніх загроз. Всі підключення ззовні відбуваються виключно через VPN, що дозволяє повністю контролювати точки входу до мережі. Усі події безпеки надходять у SmartEvent, де адміністратор отримує сповіщення у реальному часі та має змогу проаналізувати інциденти. Загальна стійкість мережі до атак значно підвищилась, а IT-інфраструктура стала більш керованою, прогнозованою та захищеною від типових загроз.

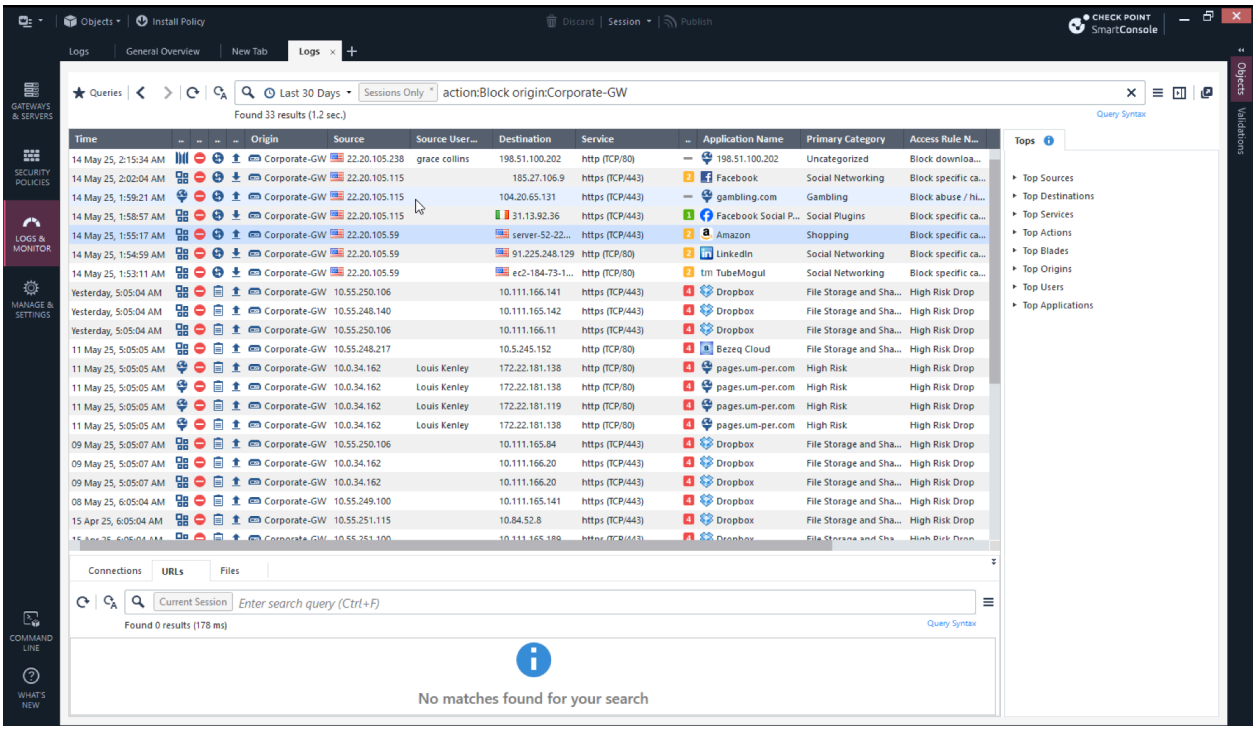

Рисунок 3.9 - Приклад заблокованих спроб доступу

3.4.2 Сегментація та захист великого підприємства

Виробниче підприємство з понад 500 працівниками використовує розгалужену IT-інфраструктуру, до складу якої входять офісні сервіси (ERP, пошта, Active Directory), SCADA-системи, хмарні рішення для зберігання даних, IoT-пристрої та гостьові точки доступу. У мережі функціонує понад 20 підмереж, однак відсутній контроль між ними. Логування подій здійснюється частково, централізований моніторинг відсутній, що суттєво ускладнює виявлення та нейтралізацію потенційних загроз.

Серед основних викликів, з якими зіткнулося підприємство, були: високий ризик горизонтального поширення загроз між підмережами через відсутність міжсегментної ізоляції; недостатній рівень виявлення атак, що потрапляють до мережі через гостьові сегменти чи пристрої підрядників; брак єдиного центру реагування на інциденти безпеки. Крім того, доступ зовнішніх підрядників до критичних служб не обмежувався ні географічно, ні часово, що створювало додаткові ризики.

Рішення полягало у впровадженні комплексної архітектури на основі Check Point, що забезпечує масштабованість, гнучкість і високу керованість усієї мережевої інфраструктури. На першому етапі реалізації було встановлено кластеризований шлюз Check Point Quantum 6200 у головному дата-центрі підприємства. Кластер працює в режимі високої доступності (High Availability), що дозволяє забезпечити безперервність захисних функцій навіть у випадку відмови одного з вузлів системи. Важливою перевагою обраного рішення є підтримка віртуалізації шлюзів безпеки, що дало змогу реалізувати кілька логічно ізольованих віртуальних систем (VSX) для різних мережевих сегментів: офісного, виробничого, гостьового, IoT-середовища та віддаленого доступу.

В рамках впровадження було проведено аудит усіх існуючих підмереж, на основі якого сформовано зони довіри з різним рівнем привілеїв доступу. Визначено та задокументовано маршрути між зонами, після чого впроваджено детальну політику міжзонного контролю. Основна увага приділялася мінімізації маршрутизації між низькодовіреними та критичними сегментами (наприклад, ізоляція IoT-пристроїв від ERP-систем). Усі політики були реалізовані відповідно до принципу найменших привілеїв (least privilege) з урахуванням актуальних ризиків та рекомендацій від Check Point.

Додатково були увімкнені й налаштовані профілі безпеки на рівні шлюзу: модулі IPS, Threat Emulation, Anti-Bot, Antivirus. Усі вони працюють у режимі активного захисту з автоматичним реагуванням на критичні інциденти. Окремо було налаштовано моніторинговий модуль SmartEvent, що забезпечує централізовану візуалізацію, сповіщення в реальному часі та генерацію періодичних звітів для аналітики інцидентів безпеки. Це дозволило адміністраторам отримувати оперативну інформацію про події в усіх зонах захисту та зменшити час реагування на загрози (Рис 3.10).

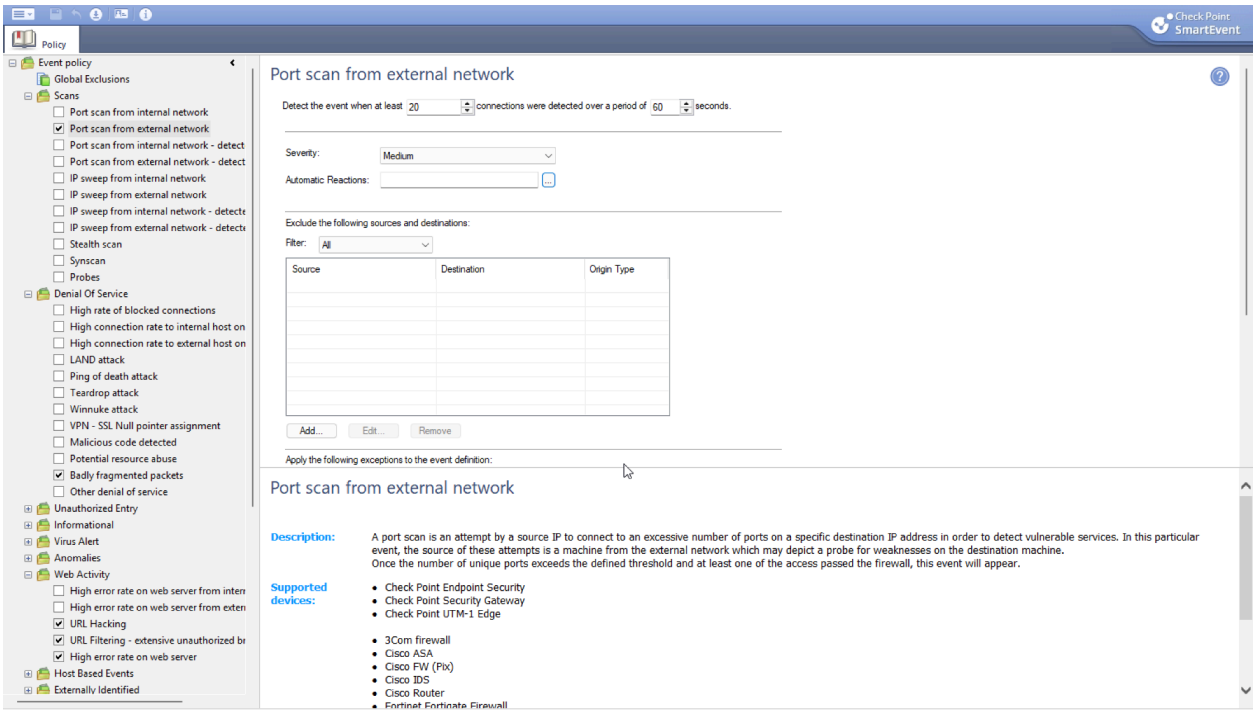

Рисунок 3.10 - Налаштування SmartEvent

Важливою складовою рішення стало впровадження контрольованого VPN-доступу для зовнішніх постачальників послуг. Доступ до внутрішніх ресурсів надається лише через шлюз з підтримкою багатофакторної автентифікації (MFA), де додатково налаштовані обмеження за IP-адресами, часом сесії та рівнем доступу. Це забезпечило не лише захищене з'єднання, а й чіткий аудит усіх дій користувачів із зовнішніх мереж.

Уже в перший тиждень після впровадження архітектури система зафіксувала понад 1000 подій у гостьовій мережі, включаючи спроби порт-сканування та атаки на вразливості протоколів SMB і DNS. Усі інциденти були успішно виявлені, ізольовані й задокументовані у SmartEvent. Завдяки зонуванню трафік між сегментами став контрольованим, а мережа — прозорою для моніторингу. Таким чином, підприємство змогло перейти від реактивного до проактивного підходу у сфері кібербезпеки, забезпечивши не лише поточний захист, але й основу для стратегічного управління безпекою в довгостроковій перспективі.

ВИСНОВКИ

У межах виконаної дипломної роботи було проведено всебічне дослідження принципів функціонування, архітектури та практичного застосування засобів мережевої кібербезпеки на базі технологій Check Point. Теоретичний розділ охопив детальний аналіз концептуальних підходів до побудови багаторівневої системи захисту, яка включає фаєрволи, VPN-з'єднання, механізми виявлення та запобігання вторгненням (IDS/IPS), системи аутентифікації, а також засоби реалізації політик доступу, сегментації трафіку і запобігання витоку даних. Окрема увага приділена питанням безперервного моніторингу, адаптивного реагування на інциденти та дотримання принципу мінімальних привілеїв у мережевому середовищі.

Розглянуто історію розвитку компанії Check Point, еволюцію її рішень, а також детально проаналізовано ключові компоненти платформи: SmartConsole, Security Management Server та Security Gateway. Акцент зроблено на їх взаємодії, функціональних особливостях та можливостях масштабування у великих корпоративних мережах. Розкрито переваги централізованого управління політиками безпеки, систем обробки подій, виявлення аномалій та інтеграції із зовнішніми джерелами загроз (threat intelligence feeds).

У практичній частині дипломної роботи здійснено повноцінну інсталяцію та конфігурацію серверів безпеки, налаштовано шлюзи, реалізовано правила фільтрації трафіку, політики доступу, VPN-з'єднання, а також механізми журналювання, логування та реагування на інциденти. Проведено низку експериментів із симуляцією мережевих атак для перевірки здатності системи виявляти і блокувати небезпечні дії. Отримані результати свідчать про високу ефективність рішень Check Point у виявленні загроз, запобіганні вторгненням та забезпеченні стабільної роботи мережевої інфраструктури. Підтверджено доцільність використання таких систем у критично важливих середовищах.

Сформовано низку рекомендацій щодо оптимізації та подальшого розвитку системи кіберзахисту: впровадження політик Zero Trust, регулярне оновлення сигнатур в системах виявлення загроз, забезпечення резервного копіювання конфігурацій, централізоване зберігання логів із підтримкою нормативних вимог, використання автоматизованих сценаріїв реагування на інциденти та інтеграція з SIEM-платформами для підвищення оперативності аналітики.

У підсумку, результати дипломної роботи мають не лише наукову і методологічну цінність, але й високу практичну значущість. Вони можуть бути застосовані для впровадження сучасних засобів кіберзахисту в реальні корпоративні мережі, підвищення загальної стійкості IT-інфраструктури до кіберзагроз, покращення управління подіями інформаційної безпеки, а також слугувати основою для подальших досліджень у сфері мережевої безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Wikipedia. Information Security [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Information_security#Security_Goals (дата звернення: 15.05.2025).

2. Imperva. Cyber Security Threats [Електронний ресурс]. – Режим доступу: https://www.imperva.com/learn/application-security/cyber-security-threats/ (дата звернення: 15.05.2025).

3. Wikipedia. Outline of Computer Security [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Outline_of_computer_security (дата звернення: 15.05.2025).

4. Cloud Security Alliance. The Risk and Impact of Unauthorized Access to Enterprise Environments [Електронний ресурс]. – Режим доступу: https://cloudsecurityalliance.org/blog/2024/05/17/the-risk-and-impact-of-unauthorized-access-to-enterprise-environments (дата звернення: 15.05.2025).

5. SentinelOne. SIEM vs. UEBA [Електронний ресурс]. – Режим доступу: https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-vs-ueba/ (дата звернення: 15.05.2025).

6. Fortinet. DDoS Attack [Електронний ресурс]. – Режим доступу: https://www.fortinet.com/resources/cyberglossary/ddos-attack (дата звернення: 15.05.2025).

7. Wikipedia. Phishing [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Phishing (дата звернення: 15.05.2025).

8. SOCRadar. Insider Threats: The Hidden Enemy of Cybersecurity [Електронний ресурс]. – Режим доступу: https://socradar.io/insider-threats-the-hidden-enemy-of-cybersecurity/ (дата звернення: 15.05.2025).

9. Wikipedia. Malware [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Malware (дата звернення: 15.05.2025).

10. Kaspersky. Firewall [Електронний ресурс]. – Режим доступу: https://www.kaspersky.com/resource-center/definitions/firewall (дата звернення: 15.05.2025).

11. Cohesity. Backup and Recovery [Електронний ресурс]. – Режим доступу: https://www.cohesity.com/glossary/backup-and-recovery (дата звернення: 15.05.2025).

12. CM Alliance. Role of Human Error in Cybersecurity Breaches and How to Mitigate It [Електронний ресурс]. – Режим доступу: https://www.cm-alliance.com/cybersecurity-blog/role-of-human-error-in-cybersecurity-breaches-and-how-to-mitigate-it (дата звернення: 15.05.2025).

13. Hoxhunt. How to Reduce Human Risk [Електронний ресурс]. – Режим доступу: https://hoxhunt.com/blog/how-to-reduce-human-risk (дата звернення: 15.05.2025).

14. Wikipedia. Check Point [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Check_Point (дата звернення: 15.05.2025).

15. Wikipedia. Infrastructure Security [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Infrastructure_security (дата звернення: 15.05.2025).

16. Wikipedia. Threat (Computer Security) [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Threat_(computer_security)#Threat_source (дата звернення: 15.05.2025).

17. Check Point. Advanced Network Threat Prevention [Електронний ресурс]. – Режим доступу: https://www.checkpoint.com/quantum/advanced-network-threat-prevention/ (дата звернення: 15.05.2025).

18. Exabeam. SIEM and Security Operations [Електронний ресурс]. – Режим доступу:

https://www.exabeam.com/explainers/siem-security/the-soc-secops-and-siem/ (дата звернення: 15.05.2025).

19. Fortinet. Unified Threat Management [Електронний ресурс]. – Режим доступу: https://www.fortinet.com/resources/cyberglossary/unified-threat-management (дата звернення: 15.05.2025).

20. Cybersecurity Guide. Environmental Protection and Cybersecurity [Електронний ресурс]. – Режим доступу: https://cybersecurityguide.org/industries/environmental-protection/ (дата звернення: 15.05.2025).

21. F5. Web Application Firewall (WAF) [Електронний ресурс]. – Режим доступу: https://www.f5.com/glossary/web-application-firewall-waf (дата звернення: 15.05.2025).

22. Check Point. CloudGuard — Cloud Security Solutions [Електронний ресурс]. – Режим доступу: https://www.checkpoint.com/cloudguard/cloud-security-solutions/ (дата звернення: 15.05.2025).

23. Check Point. Harmony Mobile Security [Електронний ресурс]. – Режим доступу: https://www.checkpoint.com/harmony/mobile-security/ (дата звернення: 15.05.2025).

24. Check Point. What Is SIEM? Security Information and Event Management [Електронний ресурс]. – Режим доступу: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-siem-security-information-and-event-management/ (дата звернення: 15.05.2025).

25. Check Point. The Check Point Threat Prevention Solution (R81.10 Admin Guide) [Електронний ресурс]. – Режим доступу: https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_ThreatPrevention_AdminGuide/Topics-TPG/The_Check_Point_Threat_Prevention_Solution.htm (дата звернення: 15.05.2025).

26. Check Point. Security Policy (R81 Next Gen Security Gateway Guide) [Електронний ресурс]. – Режим доступу: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/Topics-FWG/Security-Policy.htm (дата звернення: 15.05.2025).

27. Check Point. Threat Prevention Scheduled Updates (R81 Admin Guide) [Електронний ресурс]. – Режим доступу: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/Topics-TPG/Threat_Prevention_Scheduled_Updates.htm (дата звернення: 15.05.2025).

28. Check Point. Understanding SmartConsole (R81 Security Management Admin Guide) [Електронний ресурс]. – Режим доступу: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Understanding-SmartConsole.htm (дата звернення: 15.05.2025).

29. Check Point. Welcome (R81 Security Management Admin Guide) [Електронний ресурс]. – Режим доступу: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Welcome.htm (дата звернення: 15.05.2025).

30. Check Point. Installing Security Gateway (R81 Installation & Upgrade Guide) [Електронний ресурс]. – Режим доступу: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/Topics-IUG/Installing-Security-Gateway.htm (дата звернення: 15.05.2025).

31. Check Point. Views and Reports (R81 Logging & Monitoring Admin Guide) [Електронний ресурс]. – Режим доступу: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Views-and-reports.htm (дата звернення: 15.05.2025).

32. Check Point. Configuring the Security Management Server and Security Gateways (R81 Multi-Domain Security Management Guide) [Електронний ресурс]. – Режим доступу: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Multi-DomainSecurityManagement_AdminGuide/Topics-SECMG/Configuring_the_Security_Management_Server_and_Security_Gateways.htm (дата звернення: 15.05.2025).

33. Check Point. Enterprise Security — Next Generation Firewall [Електронний ресурс]. – Режим доступу: https://www.checkpoint.com/quantum/next-generation-firewall/enterprise-security/ (дата звернення: 15.05.2025).

34. Check Point. Remote Access VPN [Електронний ресурс]. – Режим доступу: https://www.checkpoint.com/quantum/remote-access-vpn/ (дата звернення: 15.05.2025).

35. Wikipedia. Virtual Private Network [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Virtual_private_network (дата звернення: 15.05.2025).

36. Check Point. ICS Security User Guide [Електронний ресурс]. – Режим доступу: https://sc1.checkpoint.com/documents/ICS_Security_UserGuide/html_frameset.htm?topic=documents/ICS_Security_UserGuide/202478 (дата звернення: 15.05.2025).

37. Check Point. What Is a DMZ Network? [Електронний ресурс]. – Режим доступу: https://www.checkpoint.com/cyber-hub/network-security/what-is-a-dmz-network/ (дата звернення: 15.05.2025).

38. UTM. UTM Documentation [Електронний ресурс]. – Режим доступу: https://docs.getutm.app/ (дата звернення: 15.05.2025).

39. Check Point. Running FTCW in Gaia Portal (R81 Gaia Admin Guide) [Електронний ресурс]. – Режим доступу:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/Running-FTCW-in-Gaia-Portal.htm (дата звернення: 15.05.2025).

40. Check Point. Gaia Overview (R81 Gaia Admin Guide) [Електронний ресурс]. – Режим доступу: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/Gaia-Overview.htm (дата звернення: 15.05.2025).

41. Check Point. The Check Point ThreatCloud (R81 Threat Prevention Admin Guide) [Електронний ресурс]. – Режим доступу: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/Topics-TPG/The_Check_Point_ThreatCloud.htm (дата звернення: 15.05.2025).

42. Kali Linux. Kali Linux Homepage [Електронний ресурс]. – Режим доступу: https://www.kali.org/ (дата звернення: 15.05.2025).

43. Nmap. Zenmap — GUI for Nmap [Електронний ресурс]. – Режим доступу: https://nmap.org/zenmap/ (дата звернення: 15.05.2025).

44. Kali Linux. hping3 [Електронний ресурс]. – Режим доступу: https://www.kali.org/tools/hping3/ (дата звернення: 15.05.2025).

45. Kali Linux. iodine [Електронний ресурс]. – Режим доступу: https://www.kali.org/tools/iodine/ (дата звернення: 15.05.2025).

46. Kali Linux. Metasploit Framework [Електронний ресурс]. – Режим доступу: https://www.kali.org/tools/metasploit-framework/ (дата звернення: 15.05.2025).

47. DNSLeakTest. What Is a DNS Leak? [Електронний ресурс]. – Режим доступу: https://www.dnsleaktest.com/what-is-a-dns-leak.html (дата звернення: 15.05.2025).

48. Kali Linux. Nikto [Електронний ресурс]. – Режим доступу: https://www.kali.org/tools/nikto/ (дата звернення: 15.05.2025).

49. Kali Linux. XSSer [Електронний ресурс]. – Режим доступу: https://www.kali.org/tools/xsser/ (дата звернення: 15.05.2025).