Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____*Інфокомунікацій*_____
(повна назва)
Кафедра _____*Інформаційно-мережної інженерії*_____
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____

_____*Побудова системи комплексного захисту мережі з використанням IDS/IPS модулів*_____
(тема)

Виконав:
студент _2_ курсу, групи ____*ІМІм-22-1*____
_____*Скляров О.М.*_____
(прізвище, ініціали)

Спеціальність _*172. Телекомунікації та радіотехніка*_____
(код і повна назва спеціальності)
Тип програми _____*освітньо-професійна*_____
(освітньо-професійна або освітньо-наукова)
Освітня програма _*Інформаційно-мережна інженерія*_____
(повна назва освітньої програми)

Керівник _____*ст.викл. Твердохліб В.В.*_____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ _____*Безрук В.М.*_____
(підпис) (прізвище, ініціали)

2024 р.

Не містить відомостей, заборонених
до відкритого публікування

Керівник _____ /*В.В.Твердохліб*

Студент _____ / *О.М. Скляров*

Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*

Кафедра *Інформаційно-мережної інженерії*

Рівень вищої освіти другий (магістерський)

Спеціальність *172. Телекомунікації та радіотехніка*
(код і повна назва)

Тип програми *Освітньо-професійна*
(освітньо-професійна або освітньо-наукова)

Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«_23_»*жовтня* 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Склярову Олександру Миколайовичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Побудова системи комплексного захисту мережі з використанням IDS/IPS модулів*

затверджена наказом університету від _23_ жовтня 2023 р. № 1233 Ст
2. Термін подання студентом роботи до екзаменаційної комісії 24 січня 2024 р.
3. Вихідні дані до роботи *Дослідити інструменти побудови системи захисту мережі з використанням IDS/IPS компонент (з відкритим кодом) для випадку, коли мережа містить до 200 кінцевих пристроїв та знаходиться під управлінням Active Directory. Обгрунтувати вибір та дослідити процес налаштування інструментарію захисту периметру, внутрішньої мережі та окремих вузлів.Розглянути випадки протидії зовнішнім та внутрішнім загрозам*

4. Перелік питань, що потрібно опрацювати в роботі *Вступ*
1. Актуальні питання побудови системи комплексного захисту мережі від зловмисних впливів
2. Використання NGFW для захисту периметру мережі
3. Захист від зловмисних впливів на базі IDS/IPS модулів усередині мережі
4. Захист ресурсів мережі від загроз, зумовлених внутрішніми ризиками
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____
слайди презентації в форматі Power Point (назва та мета роботи, актуальні питання побудови системи комплексного захисту мережі від зловмисних впливів, використання NGFW для захисту периметру мережі, IDS/IPS Suricata, захист від внутрішніх ризиків, висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Вступ	24.10.23-26.10.23	виконано
2	Актуальні питання побудови системи комплексного захисту мережі від зловмисних впливів	27.10.23-8.11.23	виконано
3	Використання NGFW для захисту периметру мережі	9.11.23-18.11.23	виконано
4	Захист від здовмисних впливів на базі IDS/IPS модулів усередині мережі	19.11.23-27.11.23	виконано
5	Захист ресурсів мережі від загроз, зумовлених внутрішніми ризиками	28.11.23-16.12.23	виконано
6	Висновки	17.12.23-19.12.23	виконано
7	Оформлення пояснювальної записки	20.12.23-5.1.24	виконано

Дата видачі завдання *24 жовтня* 2023 р.

Студент _____
(підпис)

Керівник роботи _____ *ст. викл. Твердохліб В.В.*
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 72 с., 44 рис., 20 джерел, 2 додатки

SNORT, CHECK POINT, IDPS, SURICATA, NGFW, GPO, ГРУПОВА ПОЛІТИКА, URL FILTERING

Об'єкт дослідження – методи та засоби побудови комплексного захисту мережевої інфраструктури від зловмисних впливів.

Мета роботи – дослідити ключові компоненти та механізми системи захисту мережі.

Виконується вибір засобів захисту мережевої інфраструктури на рівні периметру, на рівні внутрішнього середовища та окремих вузлів. Досліджується процес розгортання та налаштування обраних засобів. Здійснюється дослідження процедур активації та налаштування групових політик, спрямованих на протидію можливим зловмисним впливам, випадково чи спрямовано ініційованим внутрішніми користувачами мережі.

THE ABSTRACT

Explanatory note: 72 p., 44 fig., 20 sources, 2 apps.

SNORT, CHECK POINT, IDPS, SURICATA, NGFW, GPO, GROUP POLICY, URL FILTERING

The object of research is Methods and tools for building a comprehensive protection of network infrastructure from malicious influences.

The aim of research is to investigate the key components and mechanisms of the network security system.

Network infrastructure security tools are selected at the perimeter level, at the internal environment level, and at individual nodes. The process of deploying and configuring selected tools is investigated. The investigation of procedures for activating and configuring group policies aimed at countering possible malicious influences accidentally or directed by internal network users is carried out.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

NGFW– (Next Generation Firewall) – міжмережевий екран наступного покоління;
IDS – (Intrusion Detection System) – система виявлення вторгнень;
IPS – (Intrusion Prevention System) – система протидії вторгненням;
IDPS – (Intrusion Detection and Prevention System) – система, що поєднує функції IDS та IPS;
APT – (Advanced Persistent Threat) – розвинута стійка загроза;
DPI – (Deep Packet Inspection) – глибоке дослідження пакетів, технологія безпеки даних;
SSL – (Secure Sockets Layer) – протокол мережевої безпеки на базі засобів криптографії;
VPN – (Virtual Private Network) – віртуальна приватна мережа;
DMZ – (Demilitarized Zone) – сегмент мережі, що містить загальнодоступні сервіси та відокремлює їх від приватних;
DHCP – (high definition) – відео високої роздільної здатності;
NAT – (Network Address Translation) – механізм перетворення транзитних IP-пакетів;
SMB – (Server Message Block) – протокол прикладного рівня доступу до мережевих ресурсів;
UUID – (Universally Unique IDentifier) – універсальний унікальний ідентифікатор;
GPO – (Group Policy Object) – об’єкт групової політики;
HASP – (Hardware Against Software Piracy) – апаратно-програмна система захисту даних та програм.

ВСТУП

Розвиток інфокомунікацій в існуючому базисі технологічних рішень сприяє не лише розвитку чисельних мережевих сервісів, але також надає додаткові інструменти та можливості потенційному зловмиснику. Це, у свою чергу, сприяє тому, що останнім часом інформаційне середовище перетворюється на простір змагання, з одного боку, технологій зловмисного впливу а з іншого боку – технологій інформаційної безпеки [1, 2].

При цьому, захист від кіберзагроз, у загальному випадку, реалізується на превентивному (запобігаючому) та пост-прецендентному рівнях, та включає у себе [3]:

- методи та засоби блокування можливості доступу зловмисника до цільової мережі/вузла;
- методи та засоби виявлення та усунення зловмисних агентів усередині мережі/вузла з подальшим блокуванням каналу їх надходження;
- методи та засоби моніторингу потенційних вразливостей мережі та/або вузла, які потенційно може бути використано зловмисником.

У випадках, коли зловмисник реалізує цілеспрямовану кібератаку на конкретний мережевий ресурс, з його боку у різних варіаціях може бути задіяно такі методи впливу, як:

- апаратні;
- програмно-технічні;
- соціальні.

Водночас, оскільки методи апаратного впливу сьогодні, у загальному випадку, мають лімітований діапазон ефективного використання (зокрема, можливість прямого доступу до приміщень цільової мережі та/або фізичних ліній зв’язку мережевої інфраструктури, що є об’єктом атаки), тому, у першу чергу, необхідно брати до уваги методи соціального та програмно-технічного впливу.

Так, методи соціального впливу сьогодні представлені категорією «соціальна інженерія», головним завданням якої є забезпечення виконання користувачем дій. потрібних зловмиснику. При цьому такі дії, по-перше, не виглядають підозрілими та потенційно небезпечним а по-друге – сприяють отриманню зловмисником прямого чи опосередкованого доступу до цільової

інформації, або інструментарію управління цільовою мережевою інфраструктурою.

Разом з тим, певним чином поєднуючи засоби соціального та програмно-технічного впливу, а також – беручи до уваги специфіку побудови мережевої інфраструктури, що є об’єктом потенційної атаки, зловмисник може реалізувати найбільш небезпечний на сьогодні тип втручання, що отримав на сьогодні назву «розвинута стійка загроза».

На відміну від будь-яких атак класичного типу розвинуту стійка загроза фактично неможливо ідентифікувати традиційним засобами кіберзахисту. При цьому, тривалість такої атаки з супутньою крадіжкою/заміною даних та впливом у роботу інформаційної системи може мати досить велику тривалість.

Таким чином, у зазначених умовах дослідження інструментів протидії програмно-технічним та соціальним засобам зловмисного впливу є актуальним прикладним питанням.

1. АКТУАЛЬНІ ПИТАННЯ ПОБУДОВИ СИСТЕМИ КОМПЛЕКСНОГО ЗАХИСТУ МЕРЕЖІ ВІД ЗЛОВМИСНИХ ВПЛИВІВ

1.1 Потенційні об’єкти зловмисного впливу

Ключовими чинниками, що зумовлюють планування та реалізацію будь-якої кібератаки найчастіше є [2]:

- особисті мотиви (помста, заздрість тощо);
- фінансові мотиви;
- недобросовісна конкуренція у тих чи інших нішах діяльності;
- політичні та релігійні мотиви.

При цьому, залежно від мотивів, які зумовлюють факт атаки, головні завдання, які може ставити перед собою зловмисник, це (рис.1.1):

- виведення з ладу інформаційної системи атакованої мережевої інфраструктури чи її окремих складових (підсистеми, робочі станції, сервери тощо);
- видалення чи модифікація інформації баз даних у системі, що є об’єктом атаки;
- крадіжка чи копіювання певної інформації;
- отримання управління над інформаційними ресурсами цільової мережі;
- отримання доступу до фінансових акаунтів юридичних чи фізичних осіб;

Рисунок 1.1 – Головні завдання, які ставить перед собою зловмисних

- формування бот-нету, тобто, множини інфікованих вузлів, які далі може бути використано для реалізації наступних атак різного характеру та спрямованості.

З аналізу завдань, які ставить перед собою зловмисник, можемо бачити, що:

- більшість завдань є комплексними, тобто, містять у собі декілька етапів реалізації;

- майже всі завдання, окрім останніх двох пунктів, є апріорі спрямованими – тобто, атаки плануються та надалі виконуються відносно певної інформаційної системи.

Очевидно, що усе вищезазначене дозволяє визначити першочергові об’єкти зловмисного впливу, серед яких (рис.1.2) [2, 3]:

- офіційні та приватні облікові записи осіб, афільованих з інформаційними системами – потенційними об’єктами зловмисного впливу;

- мережеве програмне забезпечення, яке використовується у межах інформаційної системи, що є об’єктом атаки;

- прикладне програмне забезпечення робочих станцій;

- бази даних та СУБД;

- файлосховища;

- системи управління веб-ресурсами (CMS).

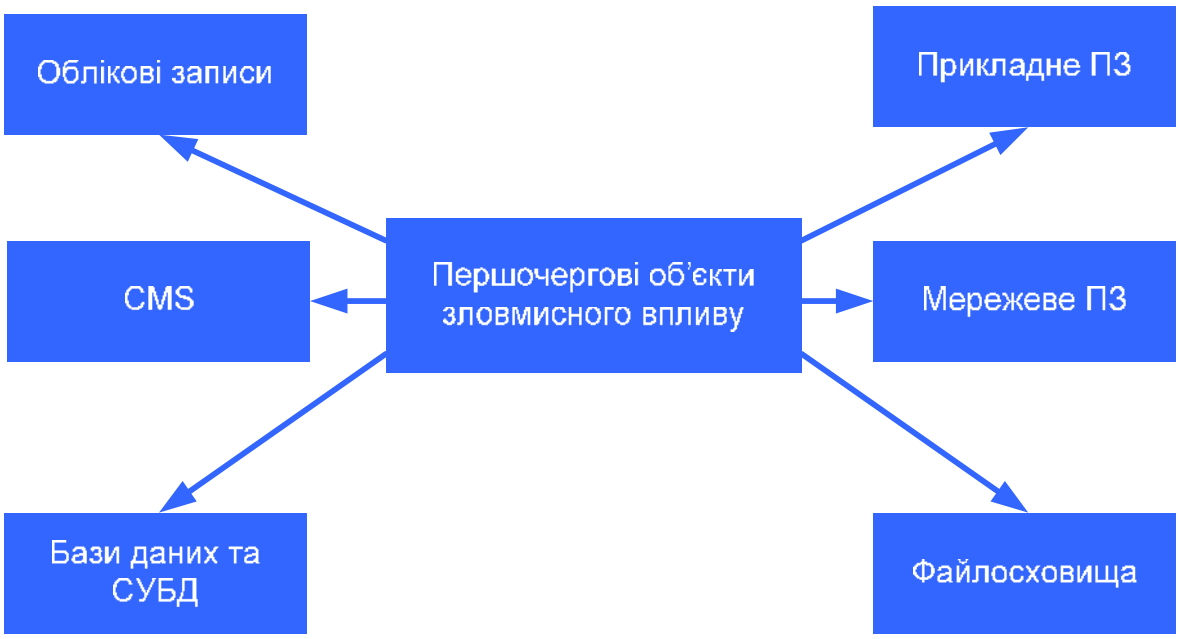

Рисунок 1.2 – Першочергові об’єкти зловмисного впливу

1.2 Загальна стратегія побудови комплексного захисту мережі

З усіх методів зловмисного впливу, які може бути здійснено на мережу/вузол, у ході як цілеспрямованої, так і незумовленої атаки, раніше було виділено апаратні, програмно-технічні та соціальні як такі, що:

- повною мірою характеризують перебіг атаки, специфіку та особливості її реалізації;
- можуть використовуватися комбінативно у різних варіаціях; це, у свою чергу, з одного боку, суттєво розширює їхні можливості а з іншого боку – утруднює процеси їх виявлення та протидії;
- потребують різних, нерідко – діаметрально протилежних підходів щодо виявлення та протидії;
- у ряді випадків ефективною протидією може розглядатися запобігання, а не реагування на інциденти, які вже реалізовано (є актуальним для соціальних методів).

Відповідно, будь-яка стратегія захисту мережевої інфраструктури має ураховувати зазначені методи.

При цьому, ураховуючи, що будь-яка система комплексного захисту мережевої інфраструктури являє собою сукупність програмно-апаратних засобів, слід взяти до уваги, що [4]:

1. Існує ймовірність компрометації апаратного забезпечення за рахунок:

- можливості інтеграції закладок на рівні прошивки;
- існування закладок на апаратному рівні.

2. Можливою є компрометація програмного забезпечення (зокрема, через уразливість використовуваного ПЗ з відкритим кодом або такого, яке завантажено з недовіреного джерела).

3. Може бути скомпрометовано складні алгоритми – наприклад, алгоритми криптографії. Зазвичай, закладки у даному випадку складно а деколи – практично неможливо виявити, але досить легко використовувати.

Таким чином, стратегія побудови системи захисту мережевої інфраструктури має ґрунтуватися на [4, 5]:

- використанні довірених джерел ПЗ та апаратного забезпечення довірених виробників, отриманих з нескомпрометованих джерел;
- побудові багаторівневої системи, яка, по-перше, забезпечує захист мережевої інфраструктури на рівні периметру а по-друге – дозволяє

захищати окремі вузли мережі, формуючи, у сутності, додатковий оівень захисту;

- використанні організаційно-технічних заходів з захисту.

У свою чергу, на рівні периметру мережі для її захисту може бути використано:

- NGFW (Next Generation Firewall);
- роутер з функціями NGFW;
- проксі-вузол, що утілює у собі функції як роутеру, так і NGFW.

При цьому, для побудови системи захисту мережевої інфраструктури усередині периметру, доцільніше за все зараз використовувати IDS та IPS-системи.

Дані засоби спрямовані на виявлення та блокування впливу зловмисних модулів, які з тих чи інших причин не було виявлено на рівні NGFW, або впливів/модулів, джерело яких знаходиться усередині контрольованої мережі.

Разом з тим, для нівелювання впливу соціальних методів, необхідно розробити комплекс організаційно-технічних заходів.

Сюди можна віднести:

- заходи з навчання персоналу;
- встановлення відповідного режиму функціонування мережі як у цілому, так і на рівні додатків та/або служб кожного окремого клієнтського вузла.

Разом з тим, для того, щоб уникнути (або мінімізувати) впливу загроз, зумовлених теоретичною можливістю існування апаратних закладок, може бути використано комплекс заходів, як:

- використання апаратних та програмних модулів, отриманих виключно з довірених джерел;
- тестовий моніторинг програмних та апаратних модулів у ізольованому захищеному середовищі (наприклад – sandbox, або – пісочниця, де засіб може проявити усі відкриті та приховані функції без можливості впливу на систему).

Виходячи з усього вищезазначеного, може бути розглянуто ряд рівнів захисту мережі від зловмисних впливів.

1.3 Рівні побудови захисту

Зрозуміло, що за аналогією зі зловмисними впливами, захисту мережі може бути утілено на апаратному, програмно-технічному та організаційному рівнях [5].

Разом з тим, керуючись стратегією побудови комплексного захисту мережі, а також приймаючи до уваги архітектуру мережі у цілому, можемо виокремити такі рівні, як:

1. Рівень кінцевого вузла. Тут необхідно запровадити інструменти, що здатні виявляти та блокувати зловмисні механізми, які, у свою чергу:

- початково містилися у межах вузла у вигляді апаратних чи програмних закладок;
- отримані з зовнішньої мережі, та з тих чи інших причин не були виявлені на рівні периметру (глибоке інкапсулювання, мають нетипову архітектуру, що робить неефективним застосування сигнатурних чи евристичних підходів, можуть проявлюватися лише у специфічних умовах, що знижує ефективність «Пісочниці»);
- отримані зі змінного носія у наслідок цілеспрямованих чи некваліфікованих дій персоналу;
- є наслідком усвідомлених зловмисних дій користувача.

Для реалізації функціоналу комплексного захисту кінцевого вузла доцільно використати IDS/IPS системи.

2. Рівень периметру мережі. У цьому випадку виконується моніторинг мережевої активності та здійснюється аналіз процесів взаємодії внутрішніх служб та користувачів з об’єктами зовнішньої мережі. Тут може бути реалізовано [5, 6]:

- повне або часткове блокування чи обмеження трафіку, який находить ззовні;
- повне або часткове блокування чи обмеження доступу користувачам мережі назовні;
- глибоке дослідження пакетів;
- антивірусний моніторинг тощо.

Отже, на даному рівні реалізуються заходи, що, з одного боку, спрямовані на перешкоджання розповсюдженню зловмисних модулів усередину мережі а з іншого боку – заходи, які блокують взаємодію користувачів з потенційно небезпечними об’єктами ззовні.

Традиційно для захисту периметру використовується між мережевий екран або його удосконалена версія – екран нового покоління NGFW.

3. Рівень мережі. У даному разі використовуються механізми та методи, що дозволяють виявляти аномальну поведінку окремих служб та додатків. Даний рівень є дублюючим для інструментарію IDS/IPS систем, та може реалізуватися на базі мережевих версій означених систем, які вже функціонують на рівні вузлів [5-7].

4. Загальносистемний рівень. Тут формуються внутрішньо мережеві протоколи функціонування об’єктів інфраструктури, зокрема [6]:

- встановлюється загальний регламент мережі та її окремих складових;
- розробляються організаційні заходи захисту з урахуванням топології мережі, програмного та апаратного базису, завдань, що мають виконуватися та найбільш актуальних загроз;
- на базі попередньо створених організаційних заходів захисту, виконується призначення та розподіл привілеїв користувачів. Фактично, це являє собою обмеження доступу для окремих категорій користувачів до тих чи інших ресурсів мережевої інфраструктури на програмному та/або апаратному рівнях;
- створюється ресурс відповідних навчальних матеріалів та формується певний порядок інструктажу користувачів.

При цьому, структурна схема комплексної системи захисту мережі, яка ураховує ієрархію окремих рівнів побудови захисту, буде такою, як зображено на рис. 1.3.

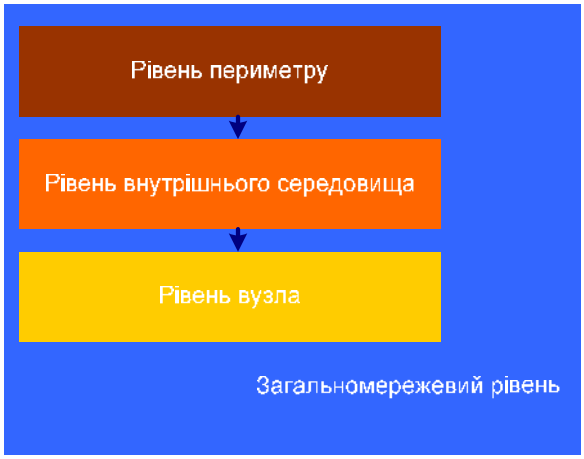

Рисунок 1.3 - Структурна схема комплексної системи захисту мережі

Схема захисту, що відповідає структурі, зображеній на рис. 1.3, потенційно здатна забезпечити достатньо високий рівень інформаційної безпеки.

Разом з тим, виключення зі структури хоча б однієї компоненти, суттєвим чином зменшує її ефективність.

Далі виконаємо дослідження принципів та закономірностей механізмів та інструментів захисту, що відносяться до перелічених рівнів.

2 ВИКОРИСТАННЯ NGFW ДЛЯ ЗАХИСТУ ПЕРИМЕТРУ МЕРЕЖІ

2.1 Функціонал NGFW та його відмінності з класичними міжмережевими екранами

Міжмережеві екрани нового покоління, або NGFW, у сутності являють собою брандмауери, що функціонують на прикладному рівні моделі OSI, виконуючи функції захисту на рівні периметру мережі [3-7].

NGFW забезпечують захист мережі від внутрішніх та зовнішніх загроз, виконуючи фільтрацію мережевого трафіку.

Однією з відмінностей NGFW від класичних між мережевих екранів, є можливості більш глибокої перевірки вмісту пакетів, разом з підтримкою ключових функцій міжмережевих екранів з перевіркою стану (фільтрація пакетів, підтримка IPsec та SSL, VPN) моніторинг мережі та зіставлення IP-адрес. Ці можливості дозволяють виявляти атаки, потенційно небезпечне програмне забезпечення, а також дозволяють міжмережевим екранам нового покоління блокувати виявлені загрози.

До базових функцій NGFW відносяться (рис.2.1):

1. Application Control. Забезпечує відстежування міток додатків, що використовуються у мережі. При цьому, у випадку запуску невідомого додатку, NGFW блокує виконання цієї операції та сповіщує адміністратора.
2. DPI – здійснює перевірку пакетів на рівні додатків, а також у межах інспекції портів і протоколів.
3. IPS – забезпечує блокування небезпечного трафіку у режимі реального часу на базі сигнатур. Функціонал IPS NGFW за замовчуванням орієнтований на превентивний режим роботи – тобто, блокує будь-які додатки чи служби, які не внесено у перелік дозволених.
4. Веб-фільтр, що виконує контроль URL-адрес, до яких звертаються користувачі. Зазвичай URL-адреси поділені на різні категорії, доступ до яких може бути дозволено чи навпаки - заборонено адміністратором мережі.
5. Аутентифікація користувачів. Дана функція дозволяє NGFW ідентифікувати користувачів за їх IP-адресами.

У свою чергу, базовий функціонал NGFW може бути розширено за рахунок додавання [6]:

1. Модулів антивірусного захисту. Такі модулі можуть являти собою, фактично, повноцінний антивірусний засіб. При цьому, перевірка трафіку виконується на рівні периметру, перешкоджаючи проникненню усередину вірусів, шпигунського ПЗ, trojan та worm's. Як і у випадку традиційного антивірусу, сигнатури для нього оновлюються в онлайн-режимі.
2. Антиспам.

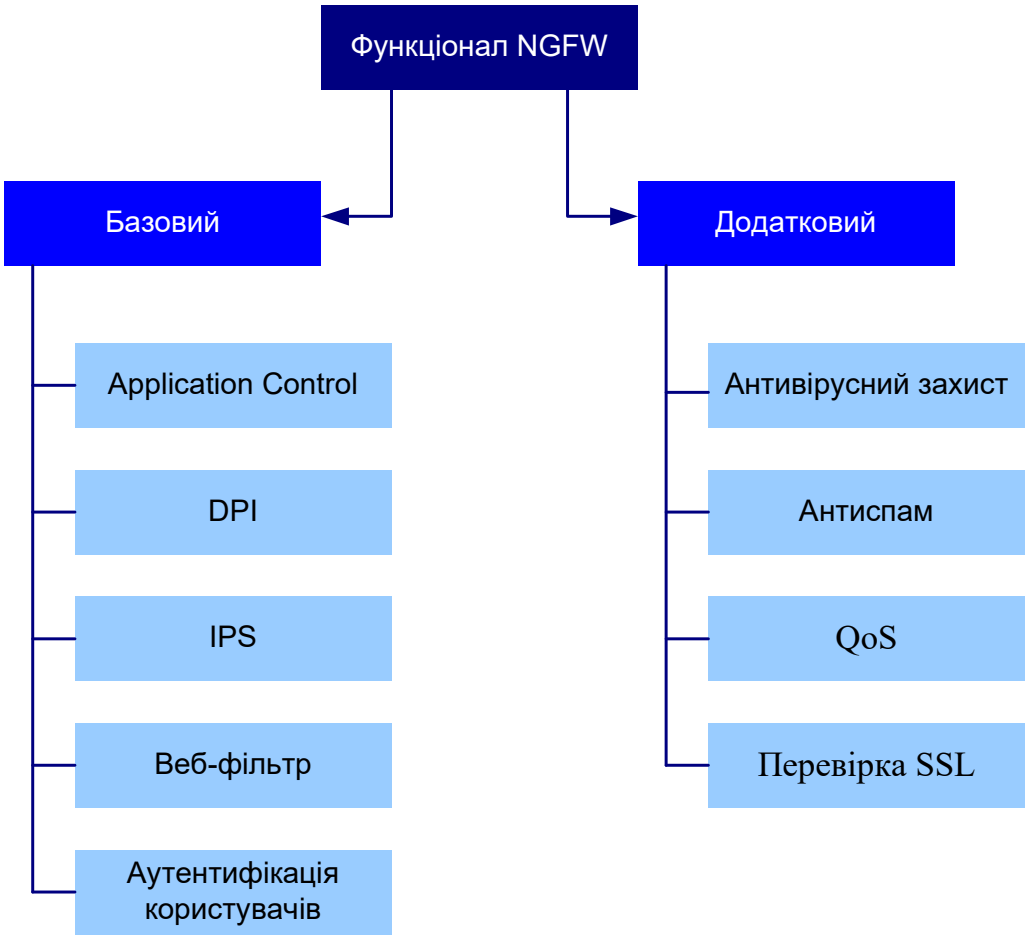

Рисунок 2.1 – Базові та додаткові функції NGFW

3. Модуль QoS. Підтримка технологій, що надають різним класам трафіку різні пріоритети в обслуговуванні, що спрощує контроль над потоками даних, чим збільшує загальну продуктивність NGFW.
4. Перевірка SSL, що дозволяє розривати SSL-тунель протоколів типу HTTPS і перевіряти зашифрований трафік.

З урахуванням цього, схему мережі з n робочими групами, захист якої побудовано на базі NGFW, може бути зображено, як показано рис.2.2.

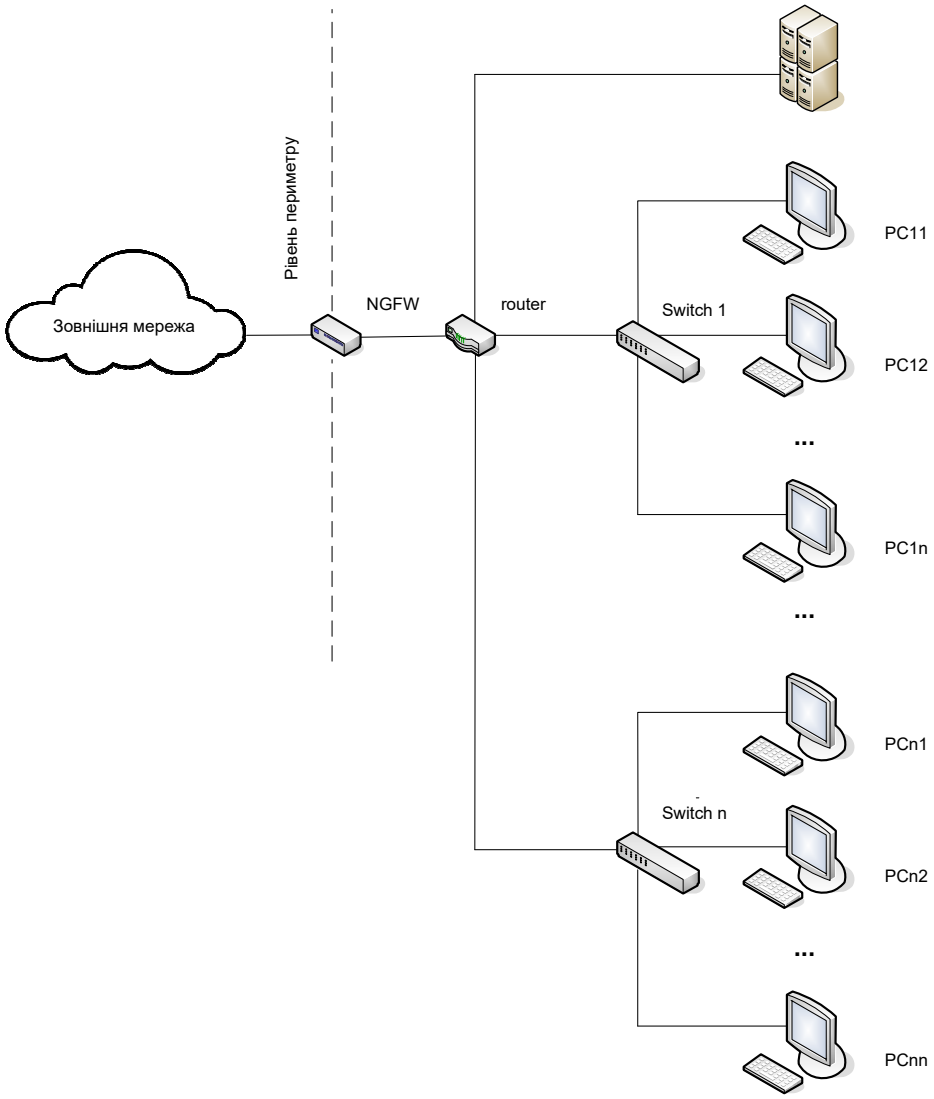

Рисунок 2.2 – Загальна схема мережі з n робочими групами, захист якої побудовано на базі NGFW

2.2 Вибір NGFW для застосування у схемі захисту мережі

Розглянемо ряд популярних рішень для побудови захисту периметру мережі, а саме – Comodo Firewall [8], Forti Gate NGFW [9] та Check Point NGFW [10]. Тут Comodo Firewall являє собою апаратне рішення, яке передбачає використання на базі апаратного проксі, що використовується спільно з граничним маршрутизатором. У свою чергу, як Forti Gate NGFW та

Check Point NGFW – програмно-апаратні модулі, що можуть також повноцінно реалізовувати функції маршрутизатора.

З іншого боку, як показало дослідження оцінок та відгуків, залишених користувачами, що порівнювали між собою лінійки продуктів Forti Gate NGFW та Check Point NGFW [11], за рядом показників Check Point NGFW демонструє вищу результативність. Це, зокрема, показники:

- легкості використання та порогу входження;
- функціоналу мережевого екрану;
- якості технічної підтримки;
- загального рівня захищеності;
- функціоналу роутеру

При цьому, Forti Gate NGFW відзначається порівняно вищою легкістю розгортання та адміністрування.

Таким чином, у нашому випадку більш доцільним для використання є Check Point NGFW.

2.3 Розгортання NGFW CheckPoint на рівні периметру мережі

Процес розгортання NGFW з наступним його налаштуванням розглянемо на прикладі обладнання CheckPoint серії 1500, як такого, що, з одного боку, містить повний функціонал NGFW а іншого – призначений для використання у мережах середнього масштабу [12].

Типовим представником серії є CheckPoint 1590 NGFW. Однією з переваг 1590 NGFW є уніфікований набір провідних та безпровідних інтерфейсів, серед яких (рис.2.2):

- інтерфейси для підключення 2 антен WiFi (2.4 ГЦ та 5 ГЦ) та 2 антен LTE
- 2 слоти для роботи з Micro/Nano SIM у режимі LTE та слот для карти SD;
- Порт WAN (rj-45);
- 8 портів LAN (rj-45);
- порт для DMZ-зони (rj-45);
- USB 3.0 для синхронізації з ПК.

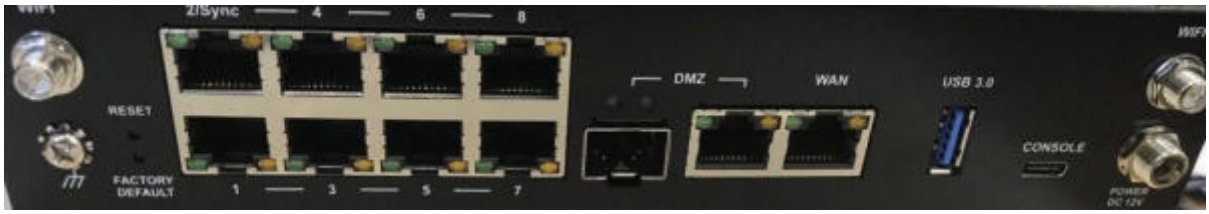

Рисунок 2.2 – Панель інтерфейсів CheckPoint 1590 NGFW

2.3.1 Первинна ініціалізація пристрою

Для того щоб приступити до ініціалізації пристрою, попередньо необхідно виконати такі дії, як [12]:

1. З’єднати ПК, який далі буде відігравати роль керуючого, мережевим кабелем «вита пара» з портом LAN-1 на шлюзі.

2. Забезпечити умови для можливості виходу до зовнішнього мережевого оточення, для чого відповідний кабель з’єднується з інтерфейсом WAN пристрою.

3. Перейти до веб-інтерфейсу управління пристроєм (так званий портал Gaia Embedded), виконавши наступний URL-запит: https://192.168.1.1:4434/

Далі, після переходу на стартову сторінку порталу Gaia, необхідно підтвердити відкриття сторінки з недовіреним сертифікатом.

За результатами виконання цієї операції далі буде активуватися майстер налаштувань порталу.

У першу чергу, виконуються налаштування облікового запису (рис.2.3).

При цьому, у систему вносяться стандартні відомості про користувача, як-то пароль та ім’я для адміністратора, та країна, де буде використовуватися шлюз.

Також до стандартних налаштувань відноситься встановлення дати та часу, що необхідно для коректної синхронізації.

При цьому, дані параметри або вносяться вручну, або використовується NTP-сервер компанії.

Наступний крок конфігурування пристрою передбачає задання його імені та вказівку домену компанії для коректної роботи служб шлюзу в Інтернеті (рис.2.4).

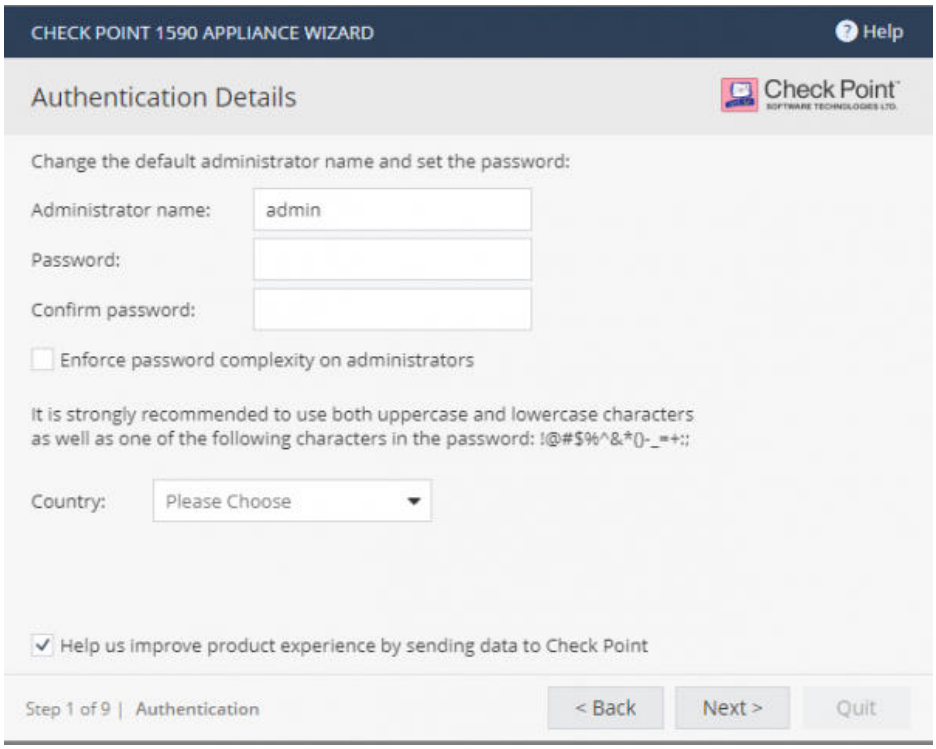

Рисунок 2.3 – Інтерфейс налаштування облікового запису адміністратора

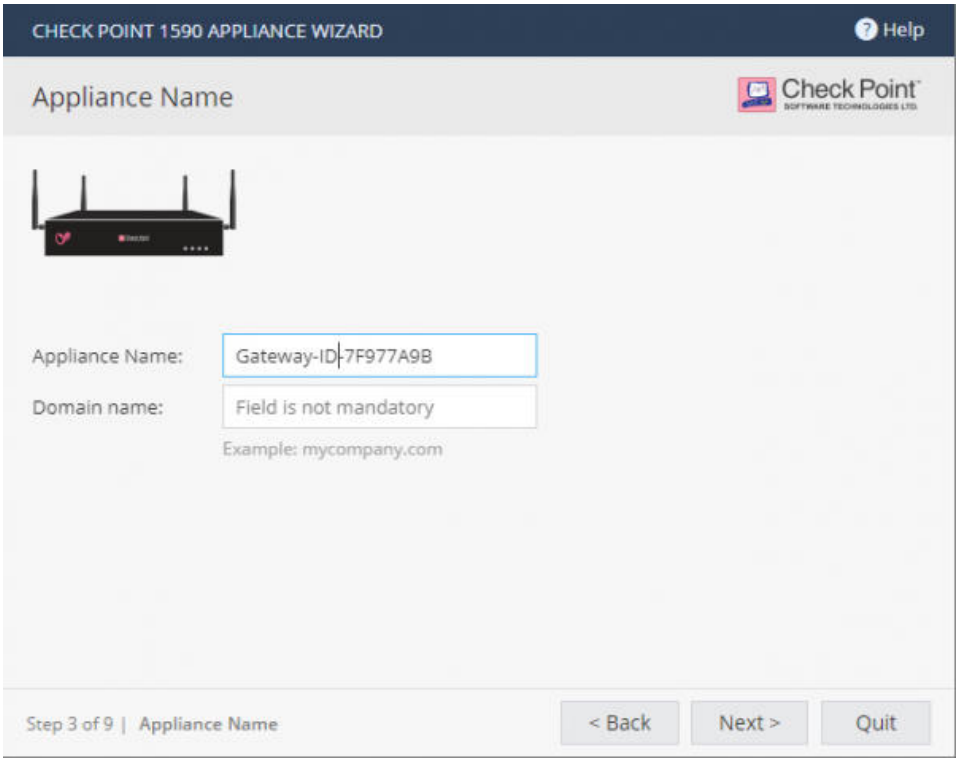

Рисунок 2.4 – Діалогове вікно встановлення імені пристрою та домену компанії

Наступний крок налаштувань полягає у виборі типу управління NGFW, а саме - Local Management, або Central Management, як показано на рисунку 2.5.

Ключові відмінності між зазначеними типами управління полягають у тому, що [12, 13]:

- Local Management являє собою варіант управління, у якому взаємодія зі шлюзом є доступною через веб-інтерфейс Gaia Portal. Інакше кажучи, даний варіант управління шлюзом CheckPoint 1590 NGFW є суто локальним;
- Central Management передбачає створення виділеного Management серверу CheckPoint, синхронізацію з хмарою Smart1-Cloud або з SMP (сервіс управління для SMB).

У нашому випадку конфігурування шлюзу буде виконуватися з вибором способу управління Local Management.

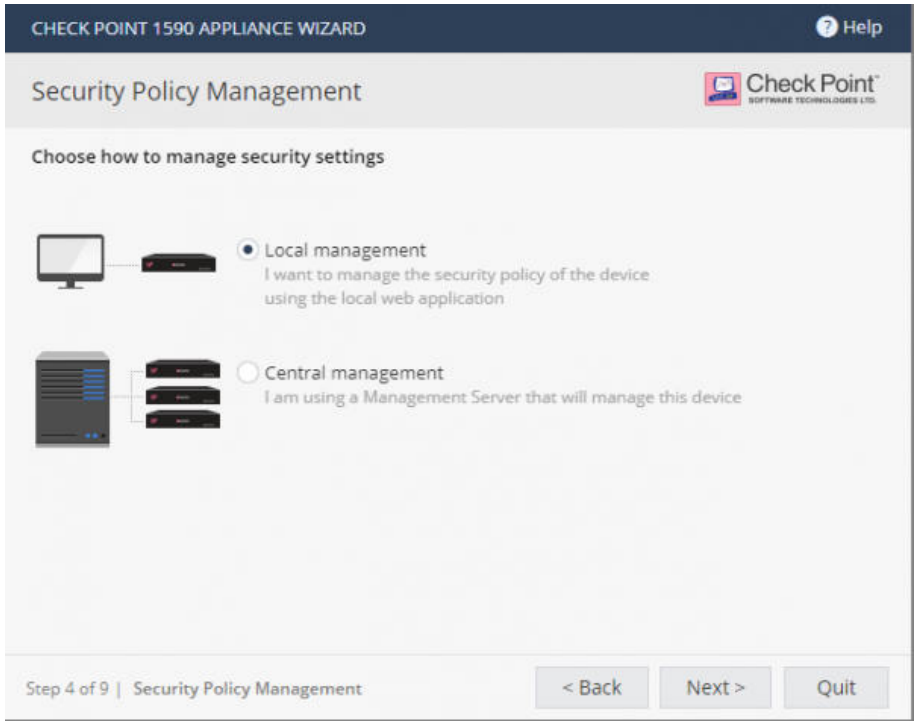

Рисунок 2.5 – Інтерфейс вибору типу управління шлюзом

Після того, як обрано необхідний режим управління, далі необхідно обрати режим функціонування інтерфейсів шлюзу. Діалогове вікно, яке дозволяє визначити режими роботи інтерфейсів, представлене на рис.2.6.

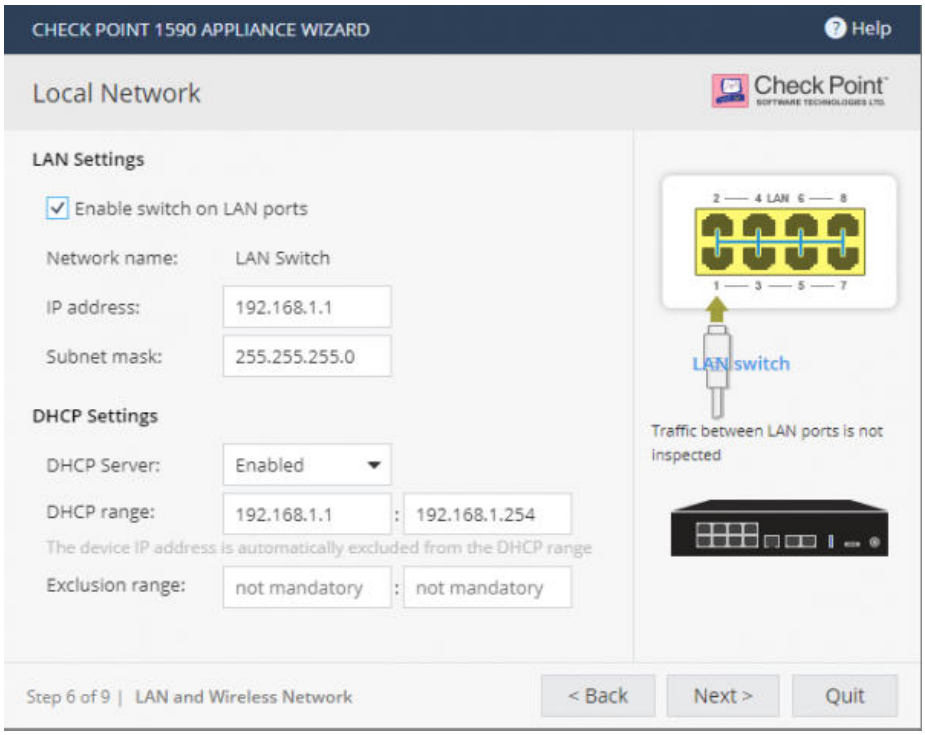

Рисунок 2.6 – Діалогове вікно вибору режиму роботи інтерфейсів

У свою чергу, обраний у якості NGFW пристрій може підтримувати такі режими, як:

- режим Switch, що передбачає доступність підмережі від одного інтерфейсу до підмережі іншого інтерфейсу.
- Режим Disable Switch, який, відповідно, деактивує режим Switch, у цьому випадку кожен порт маршрутизує трафік, як окремий фрагмент мережі.

Інтерфейс, який, у свою чергу, ілюструється на рисунку 2.6., також пропонує користувачеві встановити пул DHCP адрес, які надалі будуть використовуватися адміністратором/користувачем при підключенні до локальних інтерфейсів шлюзу.

Далі система пропонує виконати налаштування роботи шлюзу в бездротовому режимі.

При цьому, може бути створено нову бездротову точку доступу, встановлено пароль для підключення до неї а також задано режим роботи бездротового каналу (2.4 Гц або 5 Гц) [13].

Після цього, слідуючи черговості кроків конфігурування шлюзу з Gaia Portal, виконуємо налаштування доступу до шлюзу для адміністраторів мережі.

При цьому зазначимо, що, за замовчуванням, права доступу до шлюзу дозволені, у таких випадках, якщо доступ здійснюється у зазначені далі способи (рис.2.7):

- з внутрішньої мережі компанії;
- з довіреної бездротової мережі;
- через VPN-тунель.

Водночас, можливість доступу до шлюзу через мережу Інтернет за замовчуванням деактивована.

Це, у свою чергу, зумовлюється тим фактом, що можливість входження до інтерфейсу керування шлюзом завжди несе у собі суттєві потенційні ризики.

Разом з тим, інтерфейс налаштування дає можливість вказати, які саме IP-адреси можуть бути дозволені (як такі, що не несуть загроз) для підключення до шлюзу [13].

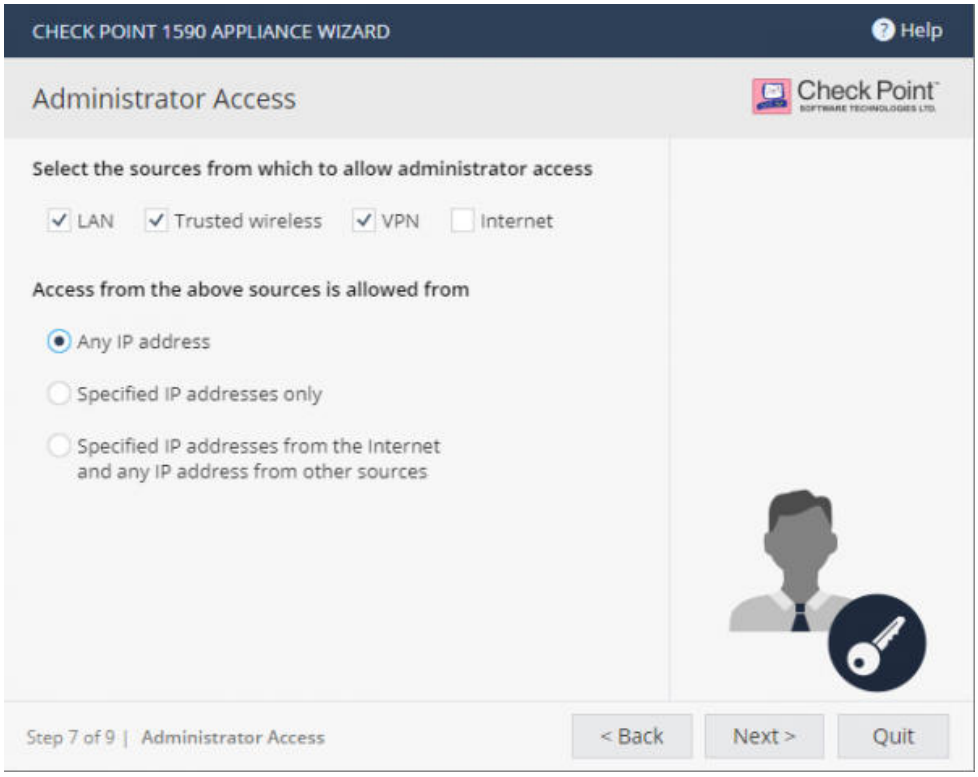

Рисунок 2.7 – Інтерфейс налаштування адміністраторського доступу CheckPoint 1590 NGFW

Після того, як адміністраторський доступ налаштовано, необхідно активувати ліцензії на користування пристроєм.

У загальному випадку, при первинній ініціалізації пристрою, розробником надається 30-денний період користування (trial mode).

При цьому, передбачено можливість застосування одного з двох існуючих способів активації, а саме [13]:

1. З існуючим підключенням до Інтернету. У цьому випадку ліцензія активується в автоматичному режимі.
2. Офлайн-активація, без доступу до інтернету.

У зазначеному випадку, коли онлайн-активація з тих чи інших причин неможлива, для здійснення активації офлайн, користувач має виконати такі дії:

- завантажити ліцензію з UserCenter;
- зареєструвати пристрій на порталі розробника.

Як у першому, так і у другому випадках, користувачеві необхідно буде імпортувати вручну завантажену ліцензію.

Нарешті, останній діалог конфігурування NGFW у майстрі налаштувань пропонує обрати блейди, що будуть використовуватися далі, як показано на рис. 2.8.

Тут слід зазначити, що особливий у рамках системи блейд, а саме – QoS, буде активовано виключно після первинної ініціалізації [12].

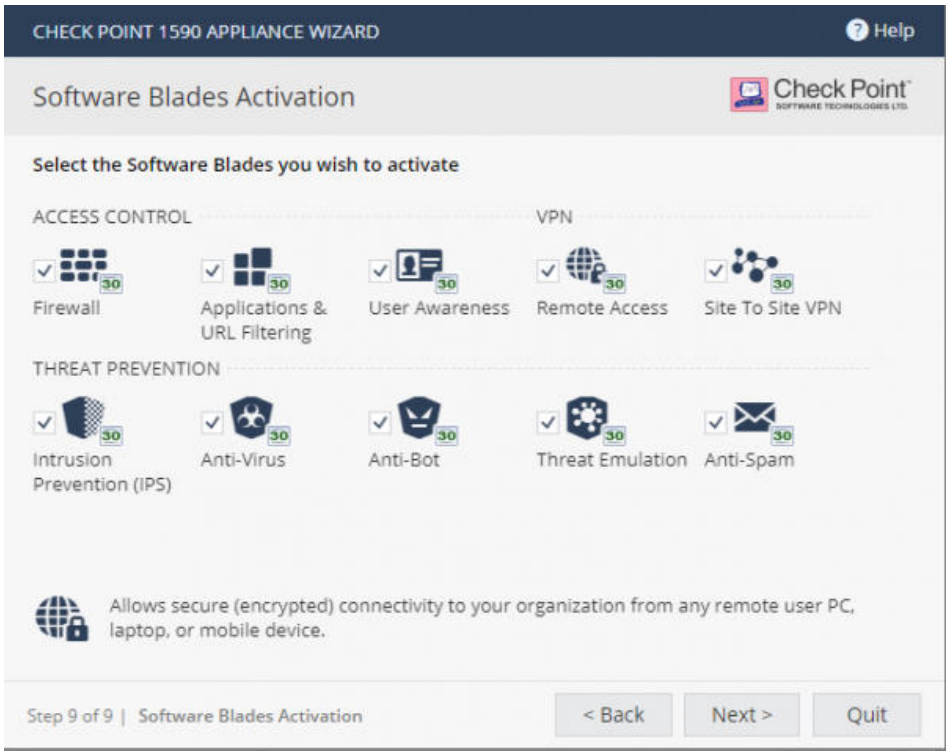

Рисунок 2.8 – Вибір блейдів для активації

2.3.2 Налаштування NGFW

У першу чергу, на стадії початкового налаштування NGFW, розробник продукту рекомендує попередньо виконати перевірку стану наявних ліцензій.

Даний крок є одним з ключових у налаштуванні, оскільки від нього залежатиме сненарій подальшого налаштування.

При цьому, для виконання зазначеної вище перевірки спершу необхідно звернутися до наступної локації Home → License, як показує рисунок 2.9 [12].

Якщо виконана перевірка свідчить про те, що ліцензії активовані, далі необхідно виконати оновлення системи до останньої актуальної прошивки. Для реалізації зазначеної операції потрібно перейти у локацію Device → System Operations (рис.2.10).

Сам інструментарій оновлення системи знаходяться у пункті Firmware Upgrade. У нашому випадку, як показано рис.2.10, встановлена актуальна та остання версія прошивки.

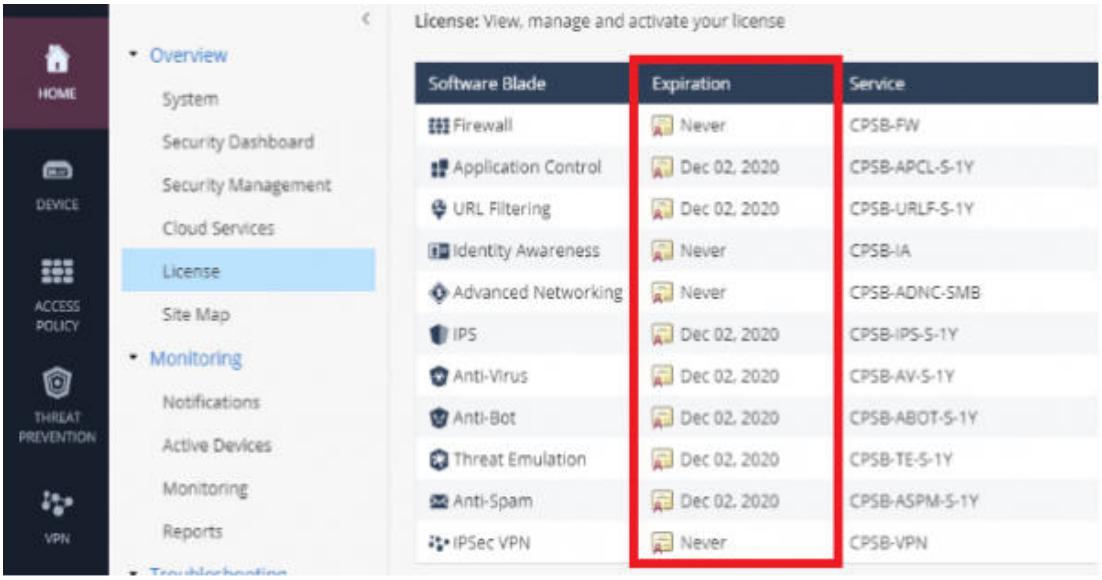

Рисунок 2.9 – Перевірка встановлених ліцензій

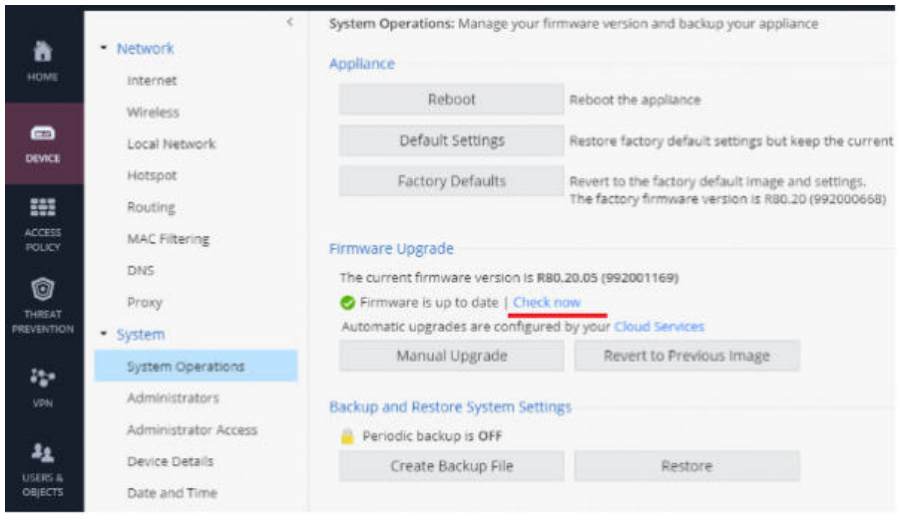

Рисунок 2.10 – Діалогове вікно оновлення прошивки шлюзу

Далі розглянемо можливості та особливості конфігурування блейдів системи.

Логічно їх може бути розділено на [12, 13]:

- політики рівня Access (Firewall, Application Control, URL Filtering)
- Threat Prevention (IPS, Antivirus, Anti-Bot, Threat Emulation).

Спершу виконаємо перехід на вкладку Access Policy → Blade Control, як зазначено на рисунку 2.11.

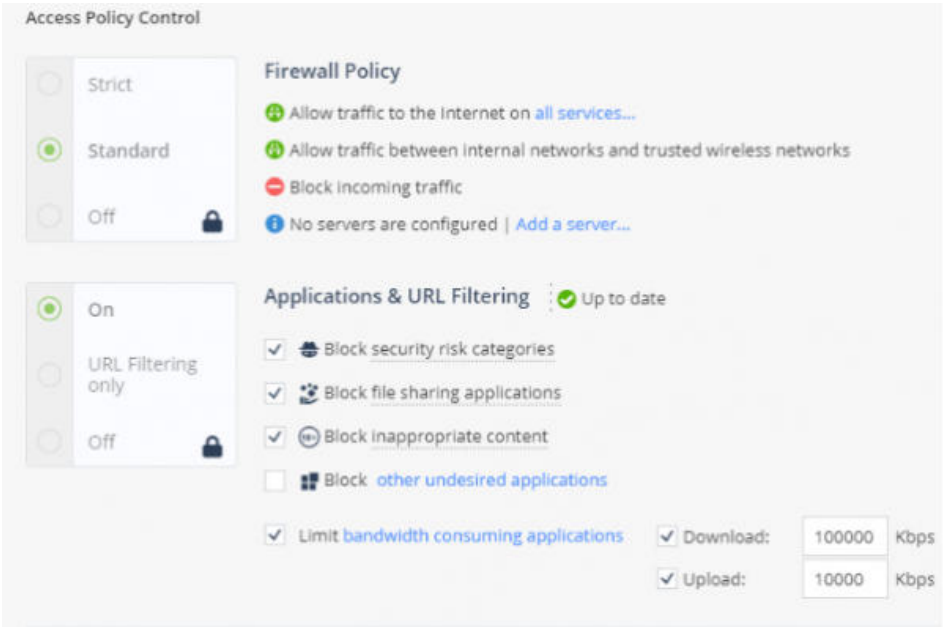

Рисунок 2.11 – Опції режиму Standard за замовчуванням

Як бачимо, за замовчуванням використовується режим Standard, який дозволяє у рамках Firewall Policy наступне:

- надходження вихідного трафіку до зовнішньої мережі;
- циркуляцію трафіку усередині локальної мережі.

Разом з тим, виконується блокування вхідного трафіку з Інтернету.

У свою чергу, що стосується блейдів Applications & URL Filtering, то за замовчуванням для них встановлюється опція блокування сайтів, яким відповідає високий рівнем небезпеки, блокування програм обміну даними на кшталт Torrent, File Storage тощо.

Окрім цього, також додатково можна заблокувати інші небажані сайти вручну.

Тут виконаємо вибір опції для користувацького трафіку "Limit bandwidth consuming applications", яка надає можливість обмежувати швидкість вихідного та вхідного трафіку для груп додатків. За замовчуванням пропонуються показники швидкості, рівні 100 Мб/с на завантаження та 10 Мб/с на вивантаження назовні [12].

Далі, після встановлення обмежень для користувацького трафіку, відкриємо локацію Policy, щоб переглянути чинні налаштування. За умовчанням правила згенеровані автоматично згідно з раніше описаними опціями.

У свою чергу, підрозділ NAT за замовчуванням функціонує у режимі в Global Hide Nat Automatic, тобто всі внутрішні хости будуть мати доступ в Інтернет через публічну IP-адресу. При цьому, за необхідності система надає можливість встановити правила NAT вручну для публікації потрібних веб-додатків або сервісів (рис.2.12).

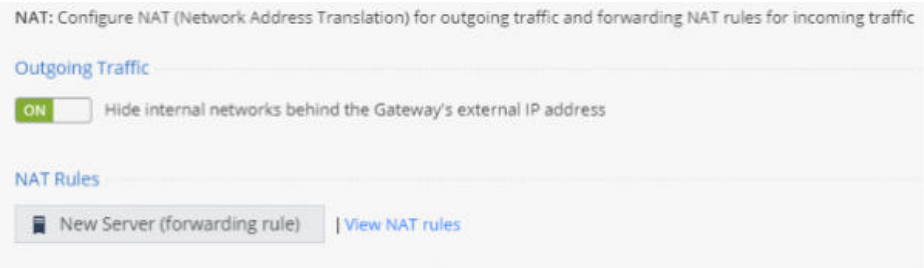

Рисунок 2.12 – Діалогове вікно налаштування NAT

Після цього у розділі, що відноситься до процедури аутентифікації користувачів у мережі (розділ Blade Control), система пропонує виконати

вибір одного з двох доступних варіантів аутентифікування користувача, а саме (рис. 2.13):

- Active Directory Queries (на той випадок, коли у складі мережевої інфраструктури використовується Active Directory, передбачається інтеграція з даною службою);
- Browser-Based-Authentication (користувач вводить доменні облікові дані у порталі).

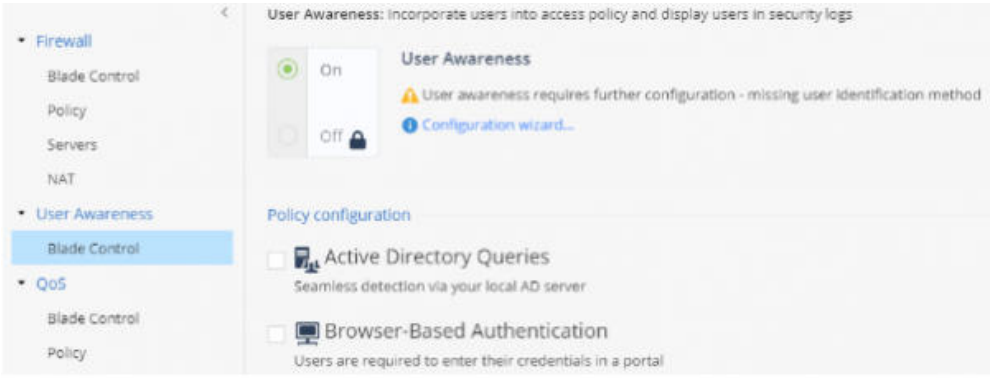

Рисунок 2.13 – Встановлення типу аутентифікації користувача

Також далі необхідно розглянути інструменти SSL-інспекції.

Дане питання є актуальним з тієї причини, що загальна частка загального HTTPS-трафіку у загальносвітовому масштабі невпинно поступово зростає.

У зв’язку з вищезазначеним, виконаємо огляд можливостей, які пропонує CheckPoint для рішень SMB [12, 13].

Для цього необхідно перейти у локацію SSL-Inspection → Policy (рис.2.14).

У данному меню опцій є можливість встановити режим інспектування HTTPS-трафіку.

При цьому для того, щоб мати змогу реалізувати зазначену можливість, попередньо необхідно виконати імпорт сертифікату а далі - встановити його до центру довірених сертифікатів на кінцевих машинах користувачів.

Разом з тим, зручною опцією можна вважати режим Bypass для встановлених категорій.

Це, у свою чергу, сприяє значному заощадженню часу при активації інспекції.

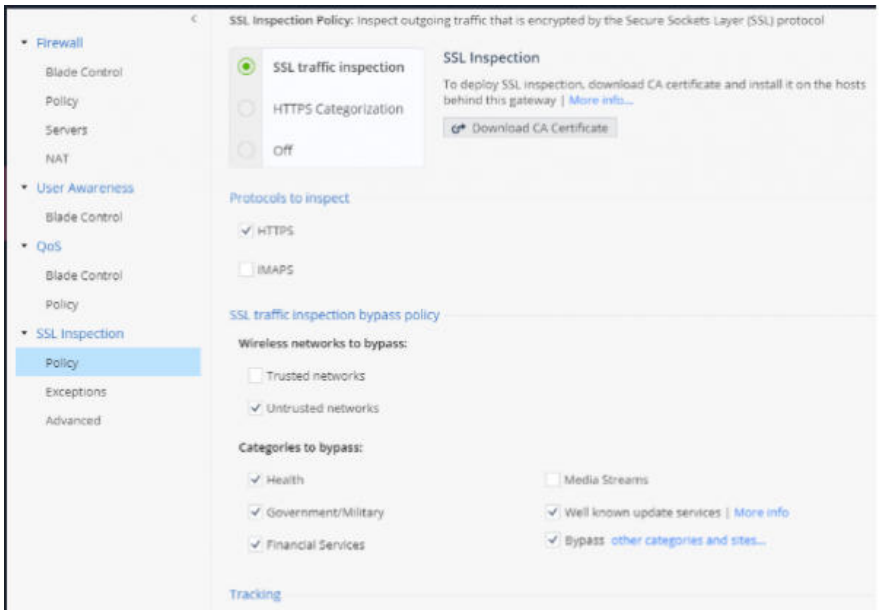

Рисунок 2.14 – Вікно налаштування SSL-Inspection

Далі, за стандартним сценарієм конфігурування системи, виконується налаштування правил на рівні Firewall/Application. Після цього необхідно перейти до встановлення опцій для політик безпеки (Threat Prevention).

Зазначені операції виконуються у відповідному розділі, як показує рисунок 2.15.

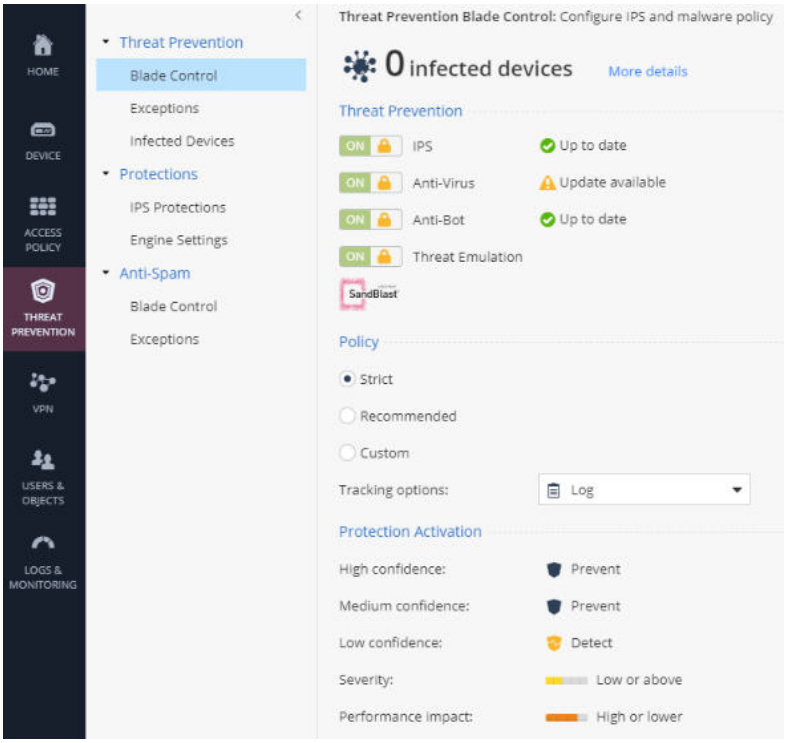

Рисунок 2.15 – Інтерфейс налаштування політик безпеки NGFW

Як видно з рисунку 2.15, на даній сторінці наводиться перелік активованих блейдів, а також статуси оновлень сигнатур та баз по кожному з них. Окрім цього, дане діалогове вікно дозволяє також обрати необхідний профіль для захисту периметру мережі, відображаючи відповідні налаштування.

У свою чергу, конфігурування дій на ту чи іншу подію безпеки виконується у розділі IPS Protections інтерфейсу Threat Prevention (рис.2.16).

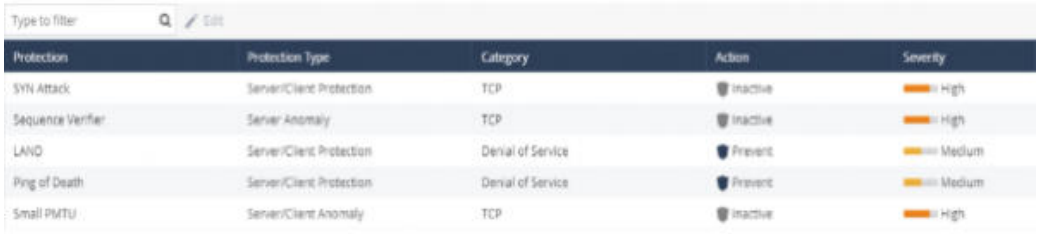

Рисунок 2.16 – Інтерфейс налаштування реакції системи

Після того, як попередньо здійснено ініціалізацію пристрою та виконано налаштування системи, перевіримо її функціональність. Для цього, наприклад, необхідно упевнитися у її можливості детектування та реагування на вразливості, виявлені відносно Розглянемо для прикладу, вже згущувану вразливість DNS серверів на базі Windows Server – SigRed.

У даному випадку, по-перше, необхідно упевнитися щодо наявності відповідної сигнатури у Gaia Embedded 80.20. Для цього достатньо ввести запит “CVE-2020-1350” у формі пошуку розділу IPS Protections (рис. 2.17).

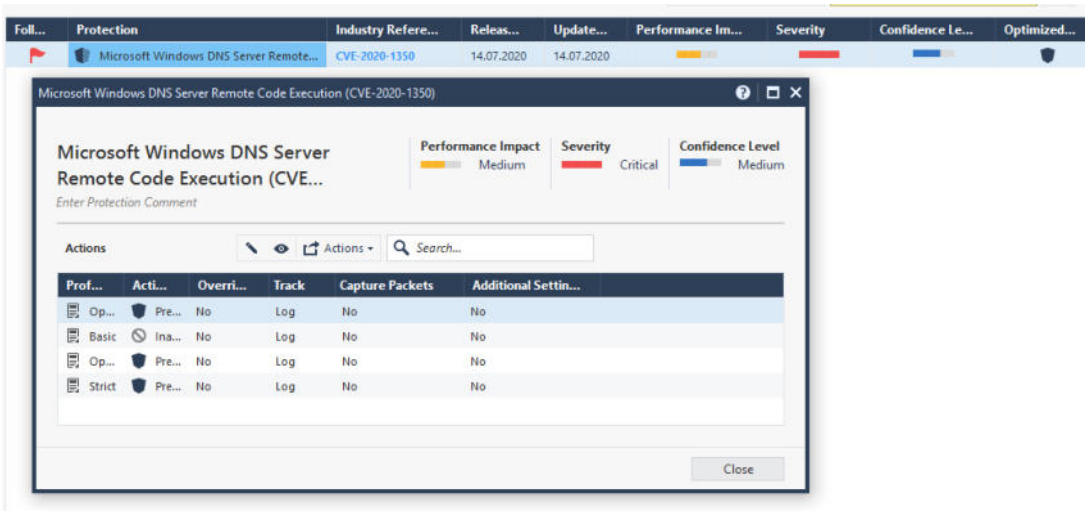

Рисунок 2.17 – Перевірка наявності сигнатур SigRed

Як видно з рисунку 2.17, відповідну сигнатуру у системі знайдено. При цьому, подано також перелік дій, які можна застосувати до цієї загрози (за умовчанням Prevent для рівня небезпеки - Critical).

2.4 Додатковий інструментарій NGFW

Окрім засобів IPS3, антивірусних інструментів та інших засобів підтримки безпеки, CheckPoint 1590 надає ряд додаткових інструментів діагностики, які може бути використано для усунення можливих проблем під час ініціалізації та розгортання засобу, а також у процесі функціонування мережі [12].

Зазначені інструменти знаходяться у розділі HOME → Tools. Вони, зокрема, надають можливість (рис.2.18):

- моніторингу системних ресурсів;
- перегляду таблиць маршрутизації;
- перевірки доступності хмарних сервісів CheckPoint;
- генерації CPinfo;

Також користувачеві доступні вбудовані мережеві команди: Ping, Traceroute, Traffic Capture тощо.

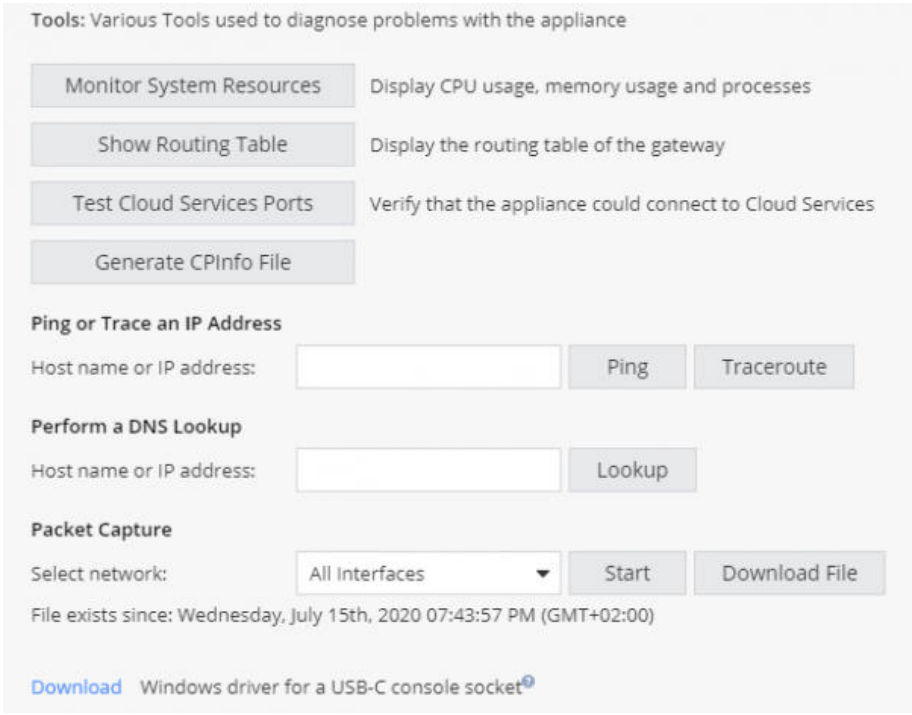

Рисунок 2.18 – Додатковий інструментарій NGFW CheckPoint 1590

Важливим є те, що розглянуті опції для CheckPoint 1590 є аналогічними для усієї серії пристроїв 1590. Таким чином, досвід роботи з одним пристроєм дозволяє адміністратору ефективно використовувати весь зазначений модельний ряд.

3. ЗАХИСТ ВІД ЗДОВМИСНИХ ВПЛИВІВ НА БАЗІ IDS/IPS МОДУЛІВ УСЕРЕДИНІ МЕРЕЖІ

3.1 Вибір засобу протидії зловмисним втручанням

За умовами технічного завдання, основою протидії зловмисним впливам усередині мережі має бути IDPS-система з відкритим кодом. При цьому, мережа, яка є об'єктом захисту, має у своєму складі не більше, ніж 200 кінцевих вузлів (клієнтські ПК, сервери тощо).

Виходячи з вищезазначеного, для захисту мережі є потенційно прийнятними засоби Snort [14] (рис.3.1) та Suricata [15] (рис. 3.2). Як Snort, так і Suricata, дозволяють виявляти ознаки зловмисної присутності шляхом виявлення системних аномалій.

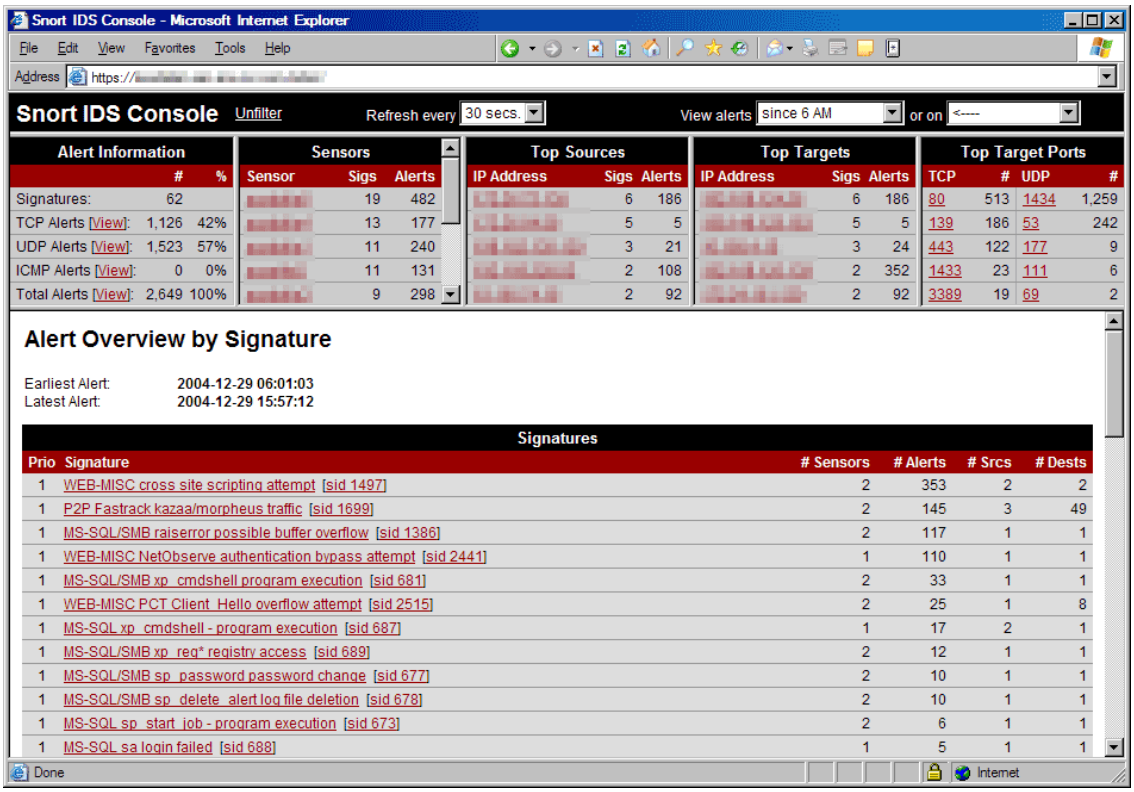

Рисунок 3.1 - Основне робоче вікно Snort

Засіб Snort - класична IDS-система, яка свого часу виникла, як проект з з відкритим кодом (1998 р.), Зараз партнером, а також розробником проекту є Cisco, що напряму може свідчити про його потенційну ефективність.

Від самого початку розробка Snort ведеться у парадигмі незалежного ПЗ.

Серед численних інструментів, які має у своєму складі засіб - сніфер пакетів, що, зокрема має функціонал налаштування та підтримки правил і багато іншого. У цілому, Snort зараз позиціонується як інструмент, що надає зрозумілу та досить функціональну систему виявлення зловмисних втручань.

У свою чергу, на відміну від системи Snort, Suricata не містить великої кількості legacy-коду. У підсумку, завдяки цьому, а також за рахунок використання новітніх розробок, система характеризується вищою швидкодією, ніж більшість аналогічних.

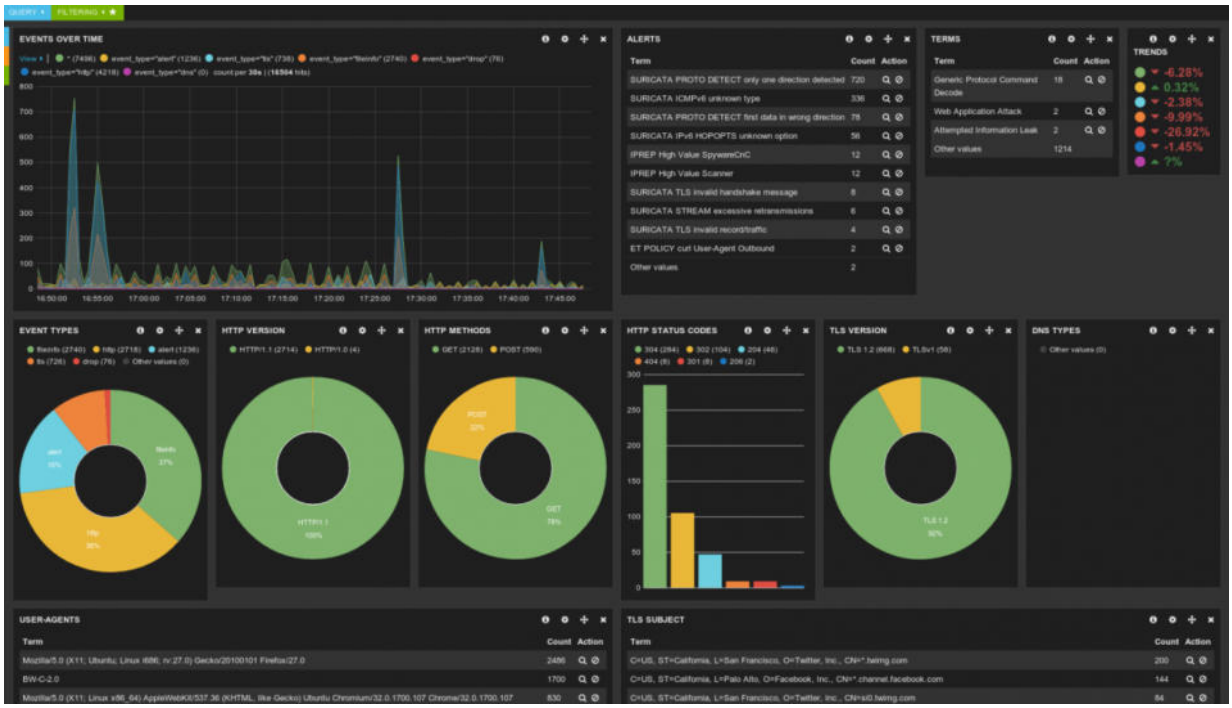

Рисунок 3.2 - Головне робоче вікно IDS/IPS Suricata

Разом з тим, розробники системи забезпечили її сумісність зі стандартизованими утилітами аналізу результатів. Інакше кажучи, це свідчить про те, що Suricata може підтримувати такі саме модулі, як і засіб Snort. Система орієнтована на виявлення загроз на базі сигнатурного підходу.

Засіб показав себе досить ефективно для інформаційних систем середніх і великих компаній.

З точки зору функціональності, засоби Snort та Suricata є, за великим рахунком, аналогічними. Разом з тим, засіб Suricata характеризується рядом переваг, зокрема:

- Suricata на сьогодні є більш user-friendly засобом (базова інструкція з використання Suricata займає приблизно 20 сторінок формату А4, тоді як інструкція для Snort – близько 200) [16];
- Snort може функціонувати виключно в однопотоковому режимі, тоді як Suricata може запускатися у мультипотокових сценаріях, що, у свою чергу, дозволяє обробляти більше трафіку фактично миттєво;
- засіб Snort позиціонується саме як IDS-засіб, тоді як останні релізи Suricata є, у сутності, повноцінна IDS/IPS (IDPS)-система.

Таким чином, беручи до уваги усе вищезазначене, далі у ролі засобу протидії зловмисним втручанням усередині мережі будемо розглядати IDPS Suricata.

3.2 Схеми включення IDPS Suricata

IDPS Suricata може використовуватися у наступних режимах [17]:

- у локальному режимі (тобто, на рівні кінцевих вузлів);
- у режимі шлюзу (у «розрив»)

На рисунку 3.3 зображено приклад схеми підключення IDPS у «розрив».

Як видно зі схеми на рис. 3.3, між цільовим веб-сервером та зовнішньою мережею встановлено IDPS Suricata.

Таким чином, функції як маршрутизації, так і прокидання портів реалізує проксі-вузол з встановленою IDPS-системою.

У зазначених умовах, якщо систему попередньо було налаштовано коректно, може бути забезпечено можливість блокування трафіку у разі спрацьовування сигнатур.

Отже, у сутності, Suricata частково реалізує функції міжмережевого екрану (firewall).

У свою чергу, локальний режим розгортання Suricata передбачає, що засіб забезпечує:

- виявлення та протидію втручанням на рівні окремого вузла, виконуючи моніторинг функціонування внутрішніх служб та систем;
- виявлення та протидію втручанням на рівні окремого вузла, виконуючи моніторинг трафіку, який захоплюється мережевою картою.

У нашому випадку виконується розгортання Suricata за схемою у «розрив» на рівні периметру, а також на рівні окремого клієнтського вузла.

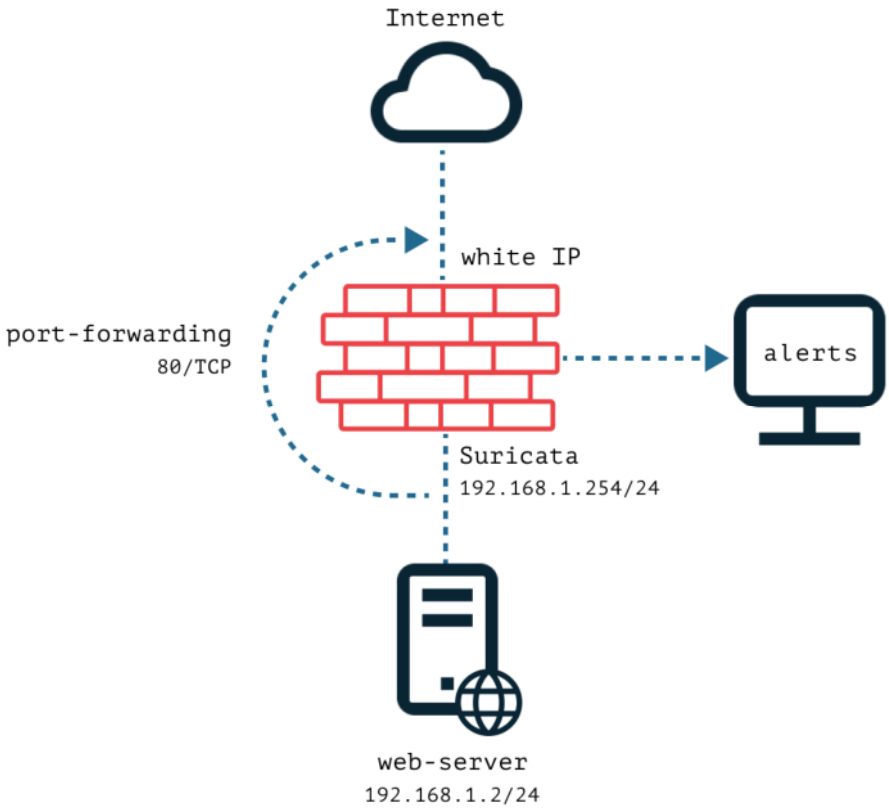

Рисунок 3.3 - Приклад включення Suricata у «розрив»

Виконаємо налаштування Suricata для випадку кожної зі схем включення.

3.3 Налаштування IDPS Suricata

3.3.1 Розгортання Suricata для випадку включення у «розрив»

Спершу виконаємо розгортання віртуального серверу на базі Ubuntu – хосту для IDPS Suricata [17].

Дана процедура включає у себе ряд кроків налаштування, а саме:

- реєстрації та входу до панелі управління;

- входу до розділу «Хмарна платформа», де обирається пункт «Сервери»;

- безпосередньо конфігурування хосту (рис.3.4).

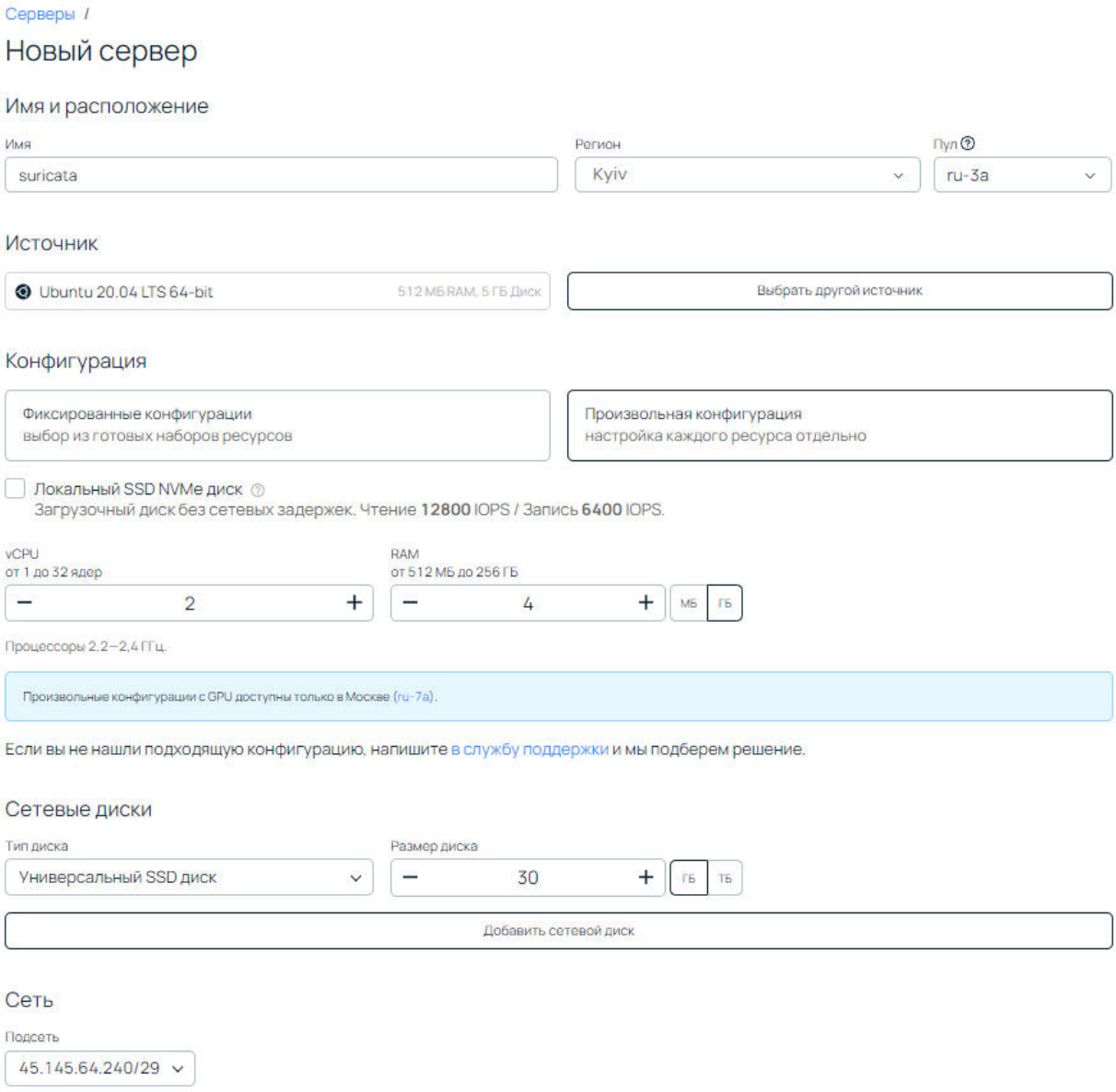

Рисунок 3.4 - Вікно розгортання віртуального серверу на базі Ubuntu

У першу чергу, вносимо ідентифікатори доступних мережевих інтерфейсів. При цьому, щонайменше один з них використовуватиметься для доступу до зовнішньої мережі, а ще, принаймні, один - до локальної мережі, тому для цього необхідно призначити відповідну адресу:

```
eth1: inet 192.168.1.252/24 brd 192.168.1.255 scope global eth1
```

```
$ sudo iptables -t nat -A PREROUTING -p tcp -i eth0 --dport 80 -
j DNAT --to-destination 192.168.1.3:80
$ sudo iptables -A FORWARD -p tcp -d 192.168.1.3 --dport 80 -m
state --state NEW,ESTABLISHED,RELATED -j ACCEPT
$ sudo iptables-save > /etc/iptables/rules.v4
```

Далі необхідно виконати налаштування для локальної мережі з виходом назовні, та заздалегідь опублікувати веб-сервер, наприклад:

```
$ sudo echo 1 > /proc/sys/net/ipv4/ip_forward
$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Після цього виконується розгортання хосту для веб-сервера, на який встановлюється Nginx і далі виконується перевірка доступность ззовні, приклад, як показано далі:

```
$ sudo apt install nginx -y
$ curl http://45.145.64.242
```

У випадку, якщо налаштування хосту та встановлення Nginx було виконано коректно, у результаті здійснення URL-запиту до серверу, у браузер завантажується відповідне діалогове вікно (рис.3.5):

Рисунок 3.5 - Вікно Nginx

При цьому, у випадку коли Nginx налаштовано коректно, далі у ході перегляду його логів може бути виявлено наявність записів про звернення, які у загальному випадку подібні до наступного:

```
$ tail -f /var/log/nginx/access.log
- - [25/Oct/2023:10:05:15 +0000] "PROPFIND / HTTP/1.1" 400 166
"-" "-"
- - [25/ Oct /2023:10:05:15 +0000] "TRACE / HTTP/1.0" 405 166 "-
"     "Mozilla/5.00     (Nobody     /2.1.5)     (Evasions:None)
(Test:httpoptions: TRACE)"
- - [25/ Oct /2023:10:05:15 +0000] "TRACE / HTTP/1.0" 405 166 "-
"       "Mozilla/5.00       (Nobody/2.1.5)       (Evasions:None)
(Test:httpoptions: TRACE)"
- - [25/ Oct /2023:10:05:15 +0000] "TRACK / HTTP/1.0" 405 166 "-
"       "Mozilla/5.00       (Nobody/2.1.5)       (Evasions:None)
(Test:httpoptions: TRACK)"
- - [25/ Oct /2023:10:05:15 +0000] "TRACK / HTTP/1.0" 405 166 "-
"       "Mozilla/5.00       (Nobody/2.1.5)       (Evasions:None)
(Test:httpoptions: TRACK)"
-     -     [25/     Oct     /2023:10:05:15     +0000]     "GET
/TiVoConnect?Command=QueryServer    HTTP/1.1"    404    162    "-"
"Mozilla/5.00 (Nobody/2.1.5) (Evasions:None) (Test:000001)"
-     -     [25/     Oct     /2023:10:05:15     +0000]     "GET
/TiVoConnect?Command=QueryContainer&Container=/&Recurse=Yes
HTTP/1.1"    404    162    "-"    "Mozilla/5.00    (Nobody/2.1.5)
(Evasions:None) (Test:000002)"
- - [25/ Oct /2023:10:05:15 +0000] "GET /cfappman/index.cfm
HTTP/1.1"    404    162    "-"    "Mozilla/5.00    (Nobody/2.1.5)
(Evasions:None) (Test:000013)"
-     -     [25/     Oct     /2023:10:05:15     +0000]     "GET
/cfdocs/examples/cvbeans/beaninfo.cfm   HTTP/1.1"   404   162   "-"
"Mozilla/5.00 (Nobody/2.1.5) ( Evasions:None) (Test:000014)"
-     -     [25/     Oct     /2023:10:05:15     +0000]     "GET
/cfdocs/examples/parks/detail.cfm    HTTP/1.1"    404    162    "-"
"Mozilla/5.00 (Nobody/2.1.5) ( Evasions:None) (Test:000015)"
```

Зрозуміло, що такі записи, у першу чергу, напряму свідчать про функціональність серверу.

Разом з тим, зазначена інформація свідчить також про те, що сервер зазнає сканування ззовні. Таким чином, далі необхідно виконати оперативне налаштування IDPS. Після цього система буде виконувати відстежування та наступне блокування запитів, що мають спільні риси з відомими сигнатурами атак [17].

Далі розглянемо процес встановлення засобу Suricata на хост.

Перед початком процедури встановлення засобу попередньо слід завантажити необхідні залежності, для чого використовується команда [18]:

```
$ sudo apt install libpcre3 libpcre3-dbg libpcre3-dev build-essential libpcap-dev libnet1-dev libyaml-0-2 libyaml-dev pkg-config zlib1g zlib1g-dev libcap-ng-dev libcap-ng0 make lib libnss3-dev libgeoip-dev liblua5.1-dev libhiredis-dev libevent-dev python-yaml rustc cargo
```

Програмний засіб Suricata можемо встановити на хост такими способами, як:

- завантаження архіву, розпакування та подальша інсталяція;
- інсталяція засобу з PPA.

Перший з зазначених способів є достатньо простим. Для інсталяції Suricata усі операції завантаження та подальшого встановлення засобу необхідно виконати стандартний перелік команд, який може різнитися виключно параметрами – локацією інсталяційного пакету, та, власне, його назвою. У нашому випадку маємо наступний лістинг команд:

```
$wget https://www.openinfosecfoundation.org/download/suricata-6.0.13.tar.gz
$ls
suricata-6.0.13.tar.gz
$ tar xzvf suricata-6.0.13.tar.gz
$ cd suricata-6.0.13
$ sudo ./configure --prefix=/usr/ --sysconfdir=/etc/ --localstatedir=/var/
$ sudo make
$ sudo make install
```

У свою чергу, інсталяція з PPA передбачає звернення до Personal Package Archive, PPA, що являє собою спеціалізований репозиторій, який містить open-source-проекти різних компаній, у т. ч. також і розробників Suricata (OSIF). Для реалізації даного сценарію інсталяції потрібно виконати наступний перелік команд:

```
$ sudo add-apt-repository ppa:oisf/suricata-stable
$ sudo apt-get update
```

```
$ sudo apt-get install suricata
```

При цьому, для того, щоб перевірити успішність інсталяції засобу, в обох випадках необхідно виконати спеціалізовану команду `suricata -v`. У випадку, коли інсталяцію виконано успішно, зазначена команда поверне версію встановленої системи.

Оновлення системи

Перший крок одразу після інсталяції Suricata полягає в оновленні переліку доступних сигнатур та їх джерел. Дану операцію виконуємо наступною командою [19]:

```
root@suricata:~/suricata-6.0.12# suricata-update
```

Після цього у файлі /etc/default/suricata виконується перевірка значення існуючого параметру IFACE з ім'ям зовнішнього інтерфейсу хоста:

```
$cat /etc/default/suricata | grep IFACE
IFACE=eth0
$ ip a
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
fq_codel state UP group default qlen 1000
link/ether fa:16:3e:29:e3:e3 brd ff:ff:ff:ff:ff:ff
inet 45.145.64.242/29 brd 45.145.64.247 scope global eth0
valid_lft forever preferred_lft forever
inet6 fe80::f816:3eff:fe29:e3e3/64 scope link
valid_lft forever preferred_lft forever
```

У випадку, якщо назви інтерфейсів збігаються, далі виконуються дії з підготовки до конфігурування системи.

Зокрема, виконаємо перевірку умови існування запису про зовнішній інтерфейс хоста у файлі /etc/suricata/suricata.yaml, а саме - у блоках pcap, pfring та af-packet. При цьому, за замовчуванням там встановлено eth0 – що частіше за все збігається з ім'ям зовнішнього інтерфейсу [17, 19].

Конфігурування системи

Ключовим конфігураційним файлом Suricata є /etc/suricata/suricata.yaml.

Більша частина налаштувань системи при цьому зводиться до внесення відповідних змін у зазначений файл. Для цього файл відкривається будь-яким редактором (VI, Nano тощо) для редагування.

У першу чергу виконуємо активацію виведення даних у блоці outputs:

```
# a line based alerts log similar to Snort's fast.log
- Fast: enabled: yes
filename: fast.log
append: yes
- eve-log: enabled: yes
filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
filename: eve.json
types:
- alert:
payload: yes # enable dumping payload in Base64
# payload-buffer-size: 4kb # max size of payload buffer to
output in eve-log
# payload-printable: yes # enable dumping payload in printable
(lossy) format
# packet: yes # enable dumping of packet (without stream
segments)
# metadata: no # включення app layer metadata with alert.
Default yes
http-body: yes # Requires metadata; enable dumping of HTTP body
in Base64
- http-log:
enabled: yes
filename: http.log
append: yes
```

Після цього здійснюємо перевірку валідності файлу конфігурацій. Для цього використовується наступна команда [19]:

```
suricata-T-c/etc/suricata/suricata.yaml-v
```

Приклад результату перевірки конфігурації наведено далі:

```
25/9/2023 - 12:26:54 - <Info> - Running suricata under test mode
25/9/2023 - 12:26:54 - <Notice> - Version 6.0.13 RELEASE running
in SYSTEM mode
```

```
25/9/2023 - 12:26:54 - <Info> - CPUs/cores online: 2
25/9/2023 -- 12:26:54 - <Info> - Setting engine mode to IDS mode by default
25/9/2023 - 12:26:54 - <Info> - fast output device (regular) initialized: fast.log
25/9/2023 - 12:26:54 - <Info> - eve-log output device (regular) initialized: eve.json
25/9/2023 - 12:26:54 - <Info> - http-log output device (regular) initialized: http.log
25/9/2023 -- 12:26:54 - <Info> - alert-debug output device (regular) initialized: alert-debug.log
25/9/2023 -- 12:26:54 - <Info> - stats output device (regular) initialized: stats.log
25/9/2023 -- 12:27:05 - <Info> - 2 rule files processed. 34519 rules success loaded, 0 rules failed
25/9/2023 -- 12:27:05 - <Info> - Threshold config parsed: 0 rule(s) found
25/9/2023 - 12:27:06 - <Info> - 34522 signatures processed. 1280 є IP-one rules, 5229 is inspecting packet payload, 27806 inspect application layer, 108 are decoder event only
25/9/2023 - 12:27:20 - <Notice> - Configuration provided was success loaded. Exiting.
25/9/2023 -- 12:27:20 - <Info> - cleaning up signature grouping structure... complete
```

Далі, при зверненні до лог-файлу, можемо побачити сеанси звернення до веб-серверу, які, у свою чергу, фіксує Suricata. Це з урахуванням того, що у більшості правил цієї IDPS-системи за замовчуванням зазначено дію alert.

Водночас, для того, щоб на базі Suricata не лише виконувалося логування підозрілого трафіку, але також здійснювалося його блокування, виконуємо додавання дії drop у сигнатури, які знаходяться у локації /var/lib/suricata/rules. Також у даній директорії можна створювати файли зі своїми правилами [17-19].

```
$ tail -f /var/log/suricata/http.log
06/25/2023-12:33:15.638309     45.145.64.242[**]/[**]Mozilla/5.00 (Nobody/2.1.5)  (Evasions:None)  (Test:Port  Check)[**]109.207.173.75:51566 -> 45.145.64.242:80
06/25/2023-12:33:15.763447     45.145.64.242[**]/[**]Mozilla/5.00 (Nobody/2.1.5)  (Evasions:None)  (Test:getinfo)[**]109.207.173.75:51566 -> 45.145.64.242:80
```

```
06/25/2023-12:33:15.799758     45.145.64.242[**]/[**]Mozilla/5.00
(Nobody/2.1.5)  (Evasions:None)  (Test:map_codes)[**]109.207.173.
:51566 -> 45.145.64.242:80
06/25/2023-12:33:15.836635
45.145.64.242[**]/dpyyI9SK.link[**]Mozilla/5.00    (Nobody/2.1.5)
(Evasions:None)   (Test:map_codes)[**]   109.207.173.75:51566   ->
45.145.64.242:80
06/25/2023-12:33:15.873426
45.145.64.242[**]/dpyyI9SK.de[**]Mozilla/5.00      (Nobody/2.1.5)
(Evasions:None)   (Test:map_codes)[**]   109.207.173.75:51566   ->
45.145.64.242:80
06/25/2023-12:33:15.909272
45.145.64.242[**]/dpyyI9SK.nlm[**]Mozilla/5.00     (Nobody/2.1.5)
(Evasions:None)   (Test:map_codes)[**]   109.207.173.75:51566   ->
45.145.64.242:80
06/25/2023-12:33:15.945103
45.145.64.242[**]/dpyyI9SK.var[**]Mozilla/5.00     (Nobody/2.1.5)
(Evasions:None)   (Test:map_codes)[**]   109.207.173.75:51566   ->
45.145.64.242:80
06/25/2023-12:33:15.980823
45.145.64.242[**]/dpyyI9SK.pm[**]Mozilla/5.00      (Nobody/2.1.5)
(Evasions:None)   (Test:map_codes)[**]   109.207.173.75:51566   ->
45.145.64.242:80
06/25/2023-12:33:16.016680
45.145.64.242[**]/dpyyI9SK.config[**]Mozilla/5.00  (Nobody/2.1.5)
(Evasions:None)   (Test:map_codes)[**]   109.207.173.75:51566   ->
45.145.64.242:80
06/25/2023-12:33:16.053655
45.145.64.242[**]/dpyyI9SK.jsp[**]Mozilla/5.00     (Nobody/2.1.5)
(Evasions:None)   (Test:map_codes)[**]   109.207.173.75:51566   ->
45.145.64.242:80
06/25/2023-12:33:16.089380
45.145.64.242[**]/dpyyI9SK.pwd[**]Mozilla/5.00     (Nobody/2.1.5)
(Evasions:None)   (Test:map_codes)[**]   109.207.173.75:51566   ->
45.145.64.242:80
```

3.3.2 Розгортання Suricata за локальною схемою

За умовою технічного завдання, клієнтські вузли функціонують під управлінням ОС сімейства Windows. Тому процес розгортання IDPS у даному випадку має декілька відмінностей від попередньо розглянутого, а саме [17]:

- попередньо необхідно інсталювати бібліотеку pcap. Зокрема, у нашому випадку, це може бути npcap win;
- необхідно завантажити файли правил Suricata та виконати їх активацію.

Активація та налаштування правил Suricata

Так як усі процедур з перевірки трафіку Suricata реалізує на базі правил, перед початком використання системи потрібно щонайменше обрати та активувати необхідний їх перелік.

Правила Suricata є поняттям, еквівалентним сигнатурам загроз. Проте, на відміну від сигнатур більшості IDS/IPS систем, правила Suricata являють собою сигнатури, орієнтовані та ті чи інші класи додатків, сервісів чи умов, поєднані з відповідними діями системи.

Зазвичай правила знаходяться у директоріїі «[розділ з інстальованим засобом]\rules». Якщо необхідно завантажити правила у довільний каталог, шлях до їх розміщення слід вказати у головному файлі конфігурації - suricata.yaml.

Так як більшість збірок Suricata не містять правил за замовчуванням у складі інсталяційного пакету, після встановлення самого додатку виконується завантаження правил. Зокрема, це може бути:

- набір ETPro (ProofPoint (Нові потоки - набір правил ETPro)), що містить скупність специфічних правил, створених для забезпечення максимальної продуктивності системи за рахунок використання її розширених та специфічних функцій;
- набір ETOpen, до складу якого входить уніфікований перелік сигнатур, достатній для рішення більшості типових завдань з виявлення потенційних загроз усередині мережі;
- набір самостійно створених правил; дане рішення є доцільним у тому випадку, коли необхідно, щоб система лише певний трафік у специфічних умовах.

При цьому, набір ETPro містить кількість правил, яка є надмірною для більшості конфігурацій корпоративних мереж, а їх налаштування може потребувати значного часу.

У свою чергу, створення власних правил потребує від адміністратора певного досвіду роботи з системою. За цих умов для швидкого розгортання

системи найбільш продуктивним можна вважати набір ETOpen, який містить перелік сигнатур, достатній для більшості випадків.

Далі, після завантаження правил у відповідну директорію, виконуємо активацію тих, що є актуальними у нашому випадку і навпаки – вимикаємо правила, використання яких у поточній конфігурації є недоцільним.

Сутність зазначених операцій полягає у тому, що за рахунок деактивації правил, асоційованих з відсутнім (неактивним) у системі сервісом, додатком чи роллю, забезпечуються умови для росту швидкодії системи у цілому а відтак – збільшення захищеності мережі.

Для вимкнення правила достатньо закоментувати його символом «#» на початку рядка у файлі suricata.yaml (рис. 3.6):

```
1123  # Set the default rule path here to search for the files.
1124  # if not set, it will look at the current working dir
1125  default-rule-path: C:\\Program Files (x86)\\Suricata\\rules\\
1126  rule-files:
1127   - botcc.rules
1128   - ciarmy.rules
1129   - compromised.rules
1130   - drop.rules
1131   - dshield.rules
1132   - emerging-activex.rules
1133   - emerging-attack_response.rules
1134   - emerging-chat.rules
1135   - emerging-current_events.rules
1136  # - emerging-dns.rules
1137  # - emerging-dos.rules
1138  # - emerging-exploit.rules
1139  # - emerging-ftp.rules
1140  # - emerging-games.rules
1141  # - emerging-icmp_info.rules
1142  # - emerging-icmp.rules
1143   - emerging-imap.rules
```

Рисунок 3.6 - Увімкнення та вимкнення правил у конфігураційному файлі Suricata

У свою чергу, для активації правила достатньо прибрати символ коментаря.

Створення базової конфігурації Suricata

Файл конфігурації Suricata (suricata.yaml) містить у собі, окрім переліку правил, необхідний перелік конфігураційних змінних - мережі, інтерфейси, розташування файлів журналу/каталоги з правилами тощо. Має специфічний

синтаксис. Даний файл після інсталяції Suricata буде містити параметри конфігурації за замовчуванням [19].

Так, запис про розміщення директорії логів задається наступним рядком:

```
”default-log-dir:C:\Suricata\log
-file:
  enabled:yes
  filename:C:\\Suricata\\suricata.log
```

Приклад оголошення директорії логів за замовчуванням у suricata.yaml показано на рисунку 3.7.

```
47  ##
48  ## Step 2: select outputs to enable
49  ##
50
51  # The default logging directory.  Any log or output file will be
52  # placed here if its not specified with a full path name. This can be
53  # overridden with the -l command line parameter.
54  default-log-dir: C:\\Program Files\\Suricata\\log
55
```

Рисунок 3.7 - Запис про директорію логів за замовчуванням у файлі suricata.yaml

У свою чергу, запис шляху до правил за замовчуванням має наступний вигляд:

```
default-rule-path:
C:\\Suricata\\rules\\
classification-file:
C:\\Suricata\\classification.config
```

При цьому, якщо завантажується стандартний перелік правил, не використовується кілька пакетів правил паралельно (наприклад, для різних режимів роботи мережі) а також не передбачається створення власних правил, для файлу правил використовується локація за замовчуванням [17].

Наступним кроком налаштування є зазначення ідентифікатору мережі, трафік якої система має перевіряти. Такий ідентифікатор встановлюється

аргументом поля HOME_NET у файлі suricata.yaml та має наступний формат:

```
HOME_NET: "[192.168.1.0/24]"
```

Активація Suricata

Запуск Suricata здійснюється з командного рядку (cmd), для чого попередньо необхідно перейти до каталогу, де знаходиться виконуваний файл Suricata. Для запуску необхідно виконати команду вигляду [17, 19]:

```
suricata.exe -c suricata.yaml -i [IP-адреса/інтерфейс, який має прослуховувати Suricata, тобто IP-адреса, на яку налаштовано мережеву карту]
```

У нашому випадку, оскільки Suricata використовується як IDPS-система рівня локального вузла, то вказується IP-адреса мережевої карти самого клієнтського пристрою, наприклад – 192.168.1.2 (рис. 3.8.).

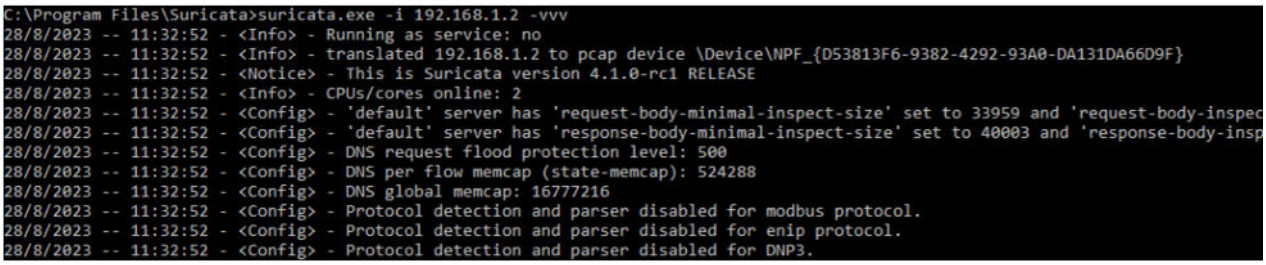

Рисунок 3.8 - Запуск Suricata з командного рядку

Далі розглянемо випадок, коли може виникнути необхідність запуску Suricata у прив’язці до інтерфейсу без IP. У цьому разі маємо попередньо отримати UUID мережевої карти. Дану задачу може бути виконано різними способами, серед яких найпростішим є використання команди для WMIC, як показано далі:

```
wmic nicconfig get ipaddress,SettingID
```

Результати виконання команди можемо бачити далі (рис.3.9):

Рисунок 3.9 - Результати виконаного запиту щодо UUID мережевих карт

У свою чергу для того, щоб виключити з видачі мережеві адаптери з призначеними IP-адресами, виконаємо фільтрацію результатів за допомогою функції findstr [19]. Для цього випадку команда буде наступною:

```
wmic nicconfig get ipaddress,SettingID | findstr [IP-адреси, що підлягають фільтрації]
```

Таким чином, отримуємо перелік UUID мережевих карт, які далі можемо використовувати у якості аргументу інтерфейсу, наприклад:

```
C:\Program Files\Suricata>suricata.exe -
i\\DEVICE\\NPF_\{FAE18080-E94C-4F73- 9CDA-
91188C071973\}
```

Таким чином, обрано IDPS систему для захисту мережі на рівні локальних вузлів та на рівні периметру.

Досліджено процес розгортання, та виконано базове налаштування IDPS Suricata для схем включення у «розрив» та для локальної схеми.

Здійснені налаштування передбачають, що моніторинг мережевого трафіку на системних процесів на рівні вузлів буде виконуватися на базі правил та асоційованих з ними дій за замовчуванням.

У свою чергу, вибір та налаштування певного набору правил, що забезпечить максимально ефективне функціонування IDPS-системи, потребує відомостей про переділ служб, додатків та протоколів, що використовуються у мережі.

4. ЗАХИСТ РЕСУРСІВ МЕРЕЖІ ВІД ЗАГРОЗ, ЗУМОВЛЕНИХ ВНУТРІШНІМИ РИЗИКАМИ

4.1 Класи загроз, що надходять від внутрішніх користувачів

У цілому, всі загрози, які можуть надходити від внутрішніх користувачів, викликані або їх некомпетентністю, або існуючим наміром.

У свою чергу, у разі існування наміру, його першоосновою може бути або конфліктна ситуація, або початкова зацікавленість користувача у заподіянні шкоди інформаційній системі та її компонентам, спричинена ідеологічними чи фінансовими чинниками (користувач є свідомим агентом зловмисника).

При цьому загрози, що існують у кожній із розглянутих ситуацій, можна віднести до одного з таких класів, як [4, 6]:

- видалення/зміна інформації у сховищах;
- крадіжка інформації з обмеженим доступом;
- крадіжка облікових записів.

У той же час, для того, щоб мати можливість реалізації зазначених класів загроз, для користувача має існувати можливість:

- прямого доступу до інформаційних ресурсів, які становлять інтерес для зловмисника;
- користування знімними пристроями для зберігання інформації з метою копіювання даних та/або запуску додатків/скриптів;
- інсталяції, налаштування та запуску програм із зовнішньої мережі.

Таким чином, для того, щоб забезпечити захист мережевої інфраструктури від загроз перерахованих класів, необхідно:

- обмежити можливість інсталяції програмного забезпечення для користувачів;
- обмежити можливість використання знімних носіїв;
- використовувати регламент взаємодії користувачів з ресурсами зовнішньої мережі, у сутності обмежуючи доступ до них;
- розробити та впровадити навчальні курси для користувачів, спрямовані на підвищення їх обізнаності з питань інформаційної безпеки.

При цьому, інструментарій, що забезпечує обмеження доступу до ряду ресурсів зовнішньої мережі було розглянуто у п 2.3.

4.2 Обмеження використання знімних носіїв внутрішніми користувачами мережі

Одним з елементів захисту мережевої інфраструктури, а також даних, що містяться в сховищах, є обмеження використання зовнішніх носіїв, насамперед USB, за рахунок чого забезпечується [7]:

- захист від навмисного або випадкового запуску шкідливого коду, розміщеного на зовнішніх носіях;
- захист від викрадення критично важливої інформації за допомогою зовнішніх накопичувачів.

4.2.1 Блокування доступу до USB у середовищі Windows

Процедура блокування доступу до USB може у Windows-оточенні може бути реалізована різними шляхами.

У нашому випадку, оскільки в мережі розгорнуто ActiveDirectory, заборона на використання USB доцільно реалізувати за допомогою групових політик [7].

При цьому в умовах, коли необхідно налаштувати політику обмеження використання USB портів на окремому комп'ютері, може бути використаний локальний редактор групових політик (gpedit.msc). Однак, у нашому випадку, коли теоретично необхідно заборонити використання носіїв USB для великої кількості робочих станцій, цей спосіб є недоцільним.

Разом з тим, також недоцільно застосовувати політику заборони використання USB до всього домену, оскільки це буде також стосуватися серверу та інші технологічних пристроїв. Тому розглянемо блокування USB накопичувачів на всіх комп'ютерах у OU домену з ім'ям Workstations.

Цей процес виконується у ході наступних технологічних кроків [6]:

1. Створити нову політику. Для цього потрібно в консолі управління доменними GPO (msc) перейти до структури Organizational Unit і викликати відповідний пункт меню для контейнера Workstations, як показано рис. 4.1.

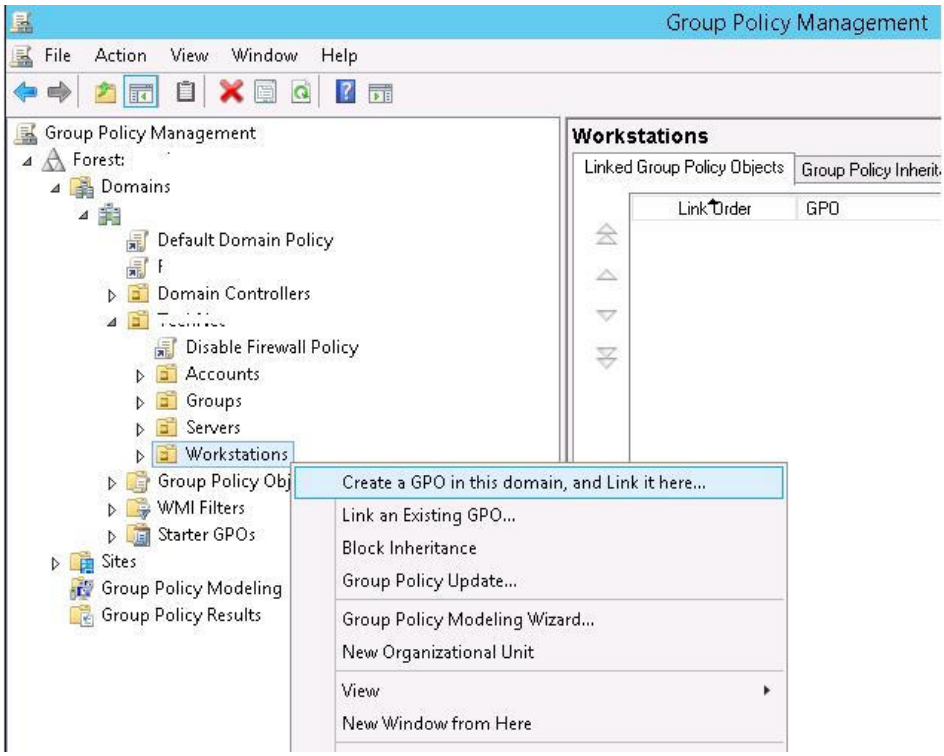

Рисунок 4.1 - Створення нової політики у менеджері групових політик

2. Створити ідентифікатор нової політики. У нашому випадку це - Disable USB Access (рис.4.2).

Рисунок 4.2 – Створення ідентифікатора політики

3. Налаштувати створену політику. Для цього потрібно перейти в режим редагування GPO (Edit) (рис. 4.3).

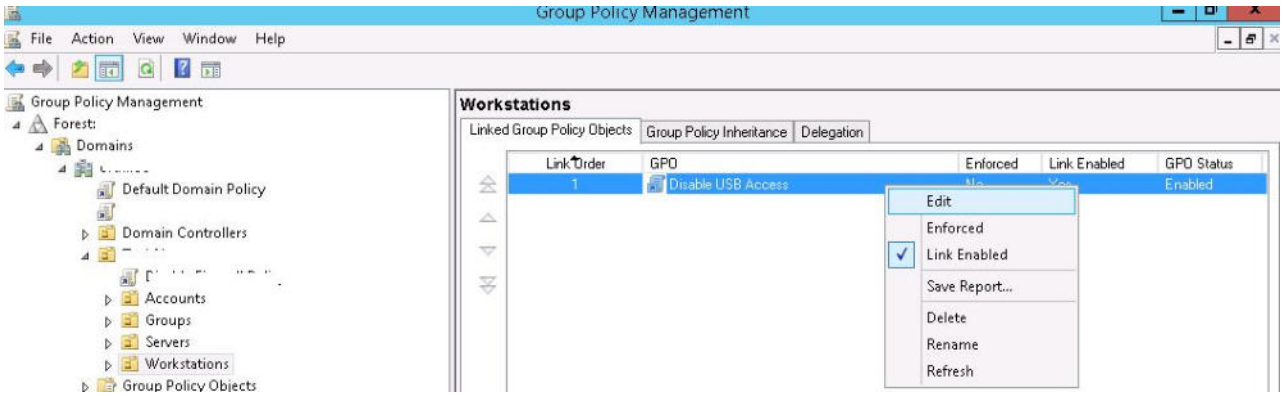

Рисунок 4.3 - Перехід у режим редагування політики

Налаштування блокування зовнішніх пристроїв є як у користувацькому, так і в комп'ютерних розділах GPO, а саме – в локаціях:

- User Configuration → Policies → Administrative Templates → System → Removable Storage Access;
- Computer Configuration → Policies → Administrative Templates → System → Removable Storage Access.

При цьому, якщо необхідно здійснити блокування USB-накопичувачів для всіх користувачів робочої станції, потрібно налаштувати відповідні параметри в розділі Computer Configuration.

У свою чергу, розділ Removable Storage Access містить ряд політик, що дають можливість блокувати використання різних класів пристроїв зберігання (рис. 4.4): CD/DVD дисків, флоппі дисків (FDD), USB пристроїв тощо. У нашому випадку актуальними є політики [5, 6]:

- Знімні диски: Заборонити виконання (Removable Disks: Deny execute access).
- Знімні диски: Заборонити читання (Removable Disks: Deny read access).
- Знімні диски: Заборонити запис (Removable Disks: Deny write access).

Таким чином, для кожного класу пристроїв може бути заборонено запуск файлів, що виконуються (захист від вірусів), заборонено читання даних і запис/редагування інформації на зовнішньому носії.

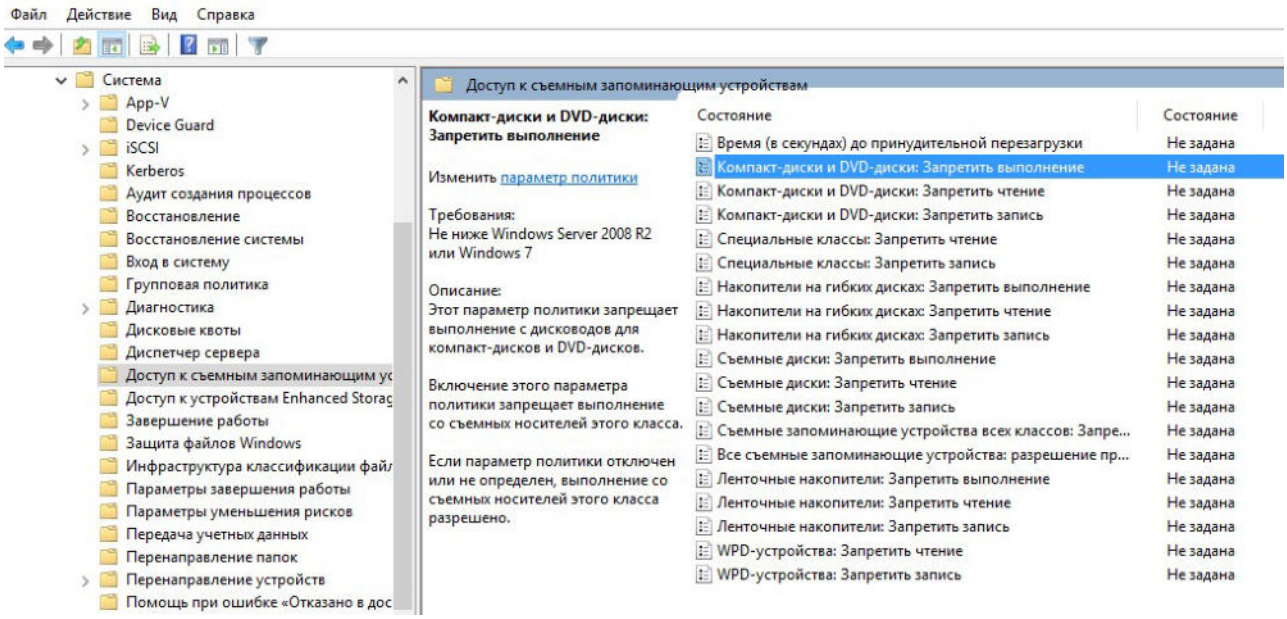

Рисунок 4.4 - Перелік політик управління використанням різних класів пристроїв зберігання

При цьому, максимальні обмеження використання пристроїв зберігання встановлює політика All Removable Storage Classes: Deny All Access (рис.4.5).

У цьому випадку забезпечується повна заборона доступу до будь-яких типів зовнішніх пристроїв зберігання.

Щоб увімкнути цю політику, необхідно відкрити її налаштування та встановити стан Enable.

Для того, щоб активувати обрану політику після її налаштування, необхідно оновити параметри GPO на клієнтах [7].

У цьому разі, оскільки політика застосовується на рівні робочих станцій, а не користувачів, оновлення параметрів виконується командою:

```
gpupdate /target:computer /force
```

У результаті виконаних дій всі зовнішні пристрої, що підключаються (не тільки USB пристрої, але і будь-які зовнішні накопичувачі) будуть визначатися ОС, але при спробі їх відкрити з'явиться помилка доступу, як показано рис. 4.6.

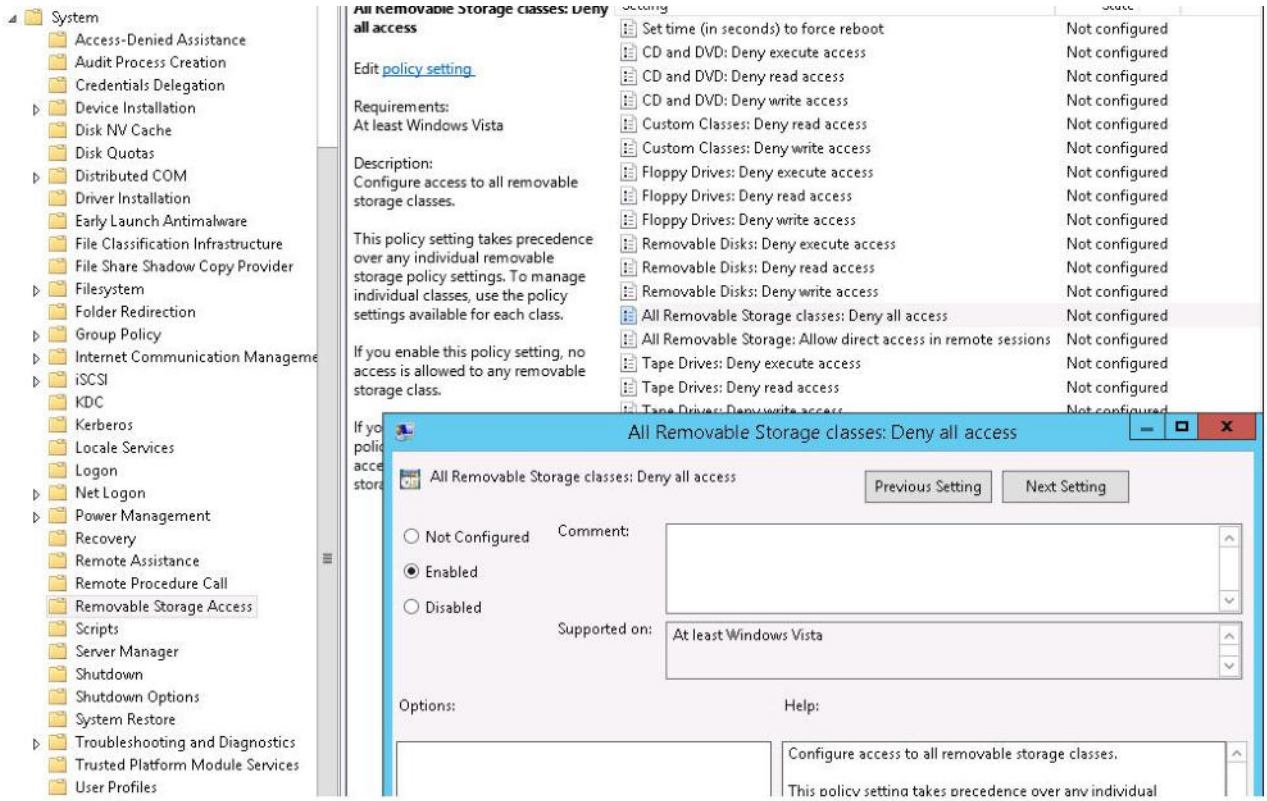

Рисунок 4.5 –Активація політикиAll Removable Storage Classes: Deny All Access

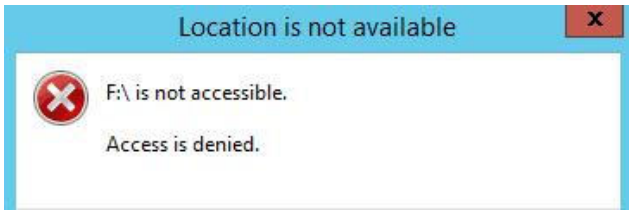

Рисунок 4.6 - Інформування системи про неможливість доступу до зовнішнього пристрою

4.2.2 Застосування гнучких політик щодо використання зовнішніх USB накопичувачів

У ряді випадків розглянутий спосіб блокування USB може бути неприйнятним для забезпечення штатного режиму функціонування мережі, зокрема [5, 7]:

- якщо користувачі використовують USB-HASP;

- регламент передбачає, що USB-носії обмежено використовуються при реалізації робочих процесів усередині мережі і т.д.

У розглянутих випадках може бути використана політика, що забороняє запис даних на USB-носія, а саме – RemovableDisk: Deny write access (рис.4.7).

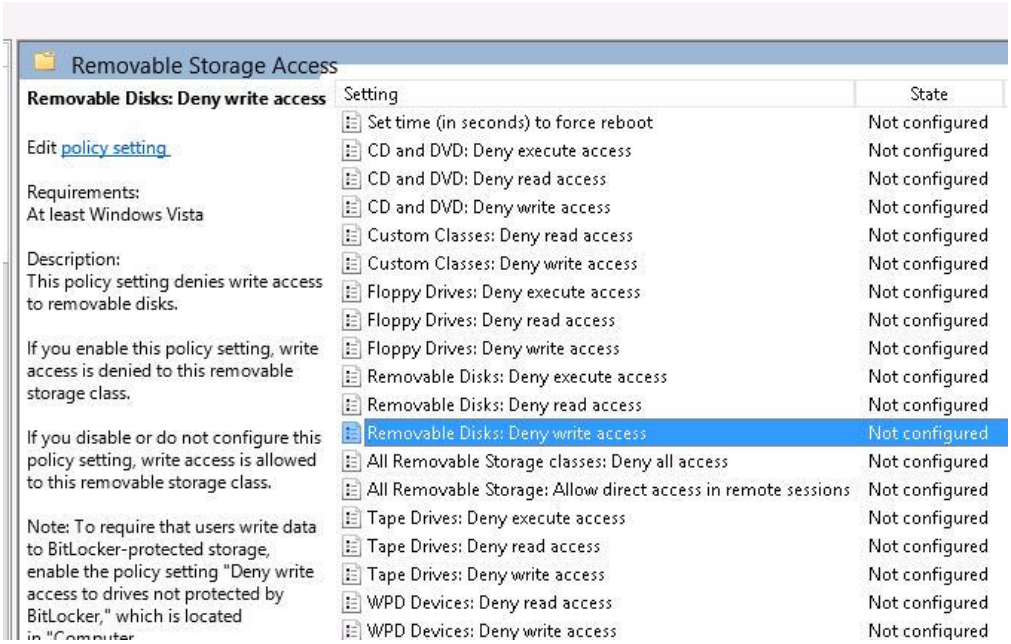

Рисунок 4.7 - Встановлення політики, що забороняє запис даних на носії USB

Внаслідок встановлення та активації згаданої політики, користувачі зможуть читати дані з USB-носія, однак у разі спроб запису, система інформує про помилку, як показано на рисунку 4.8.

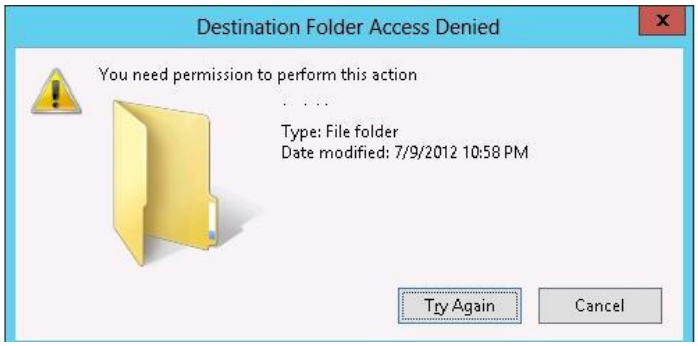

Рисунок 4.8 - Вікно Alert, видане системою під час спроби запису на носій USB з активованою політикою Removable Disk: Deny write access

Далі виконаємо блокування можливості запуску виконуваних файлів та скриптів із USB-дисків.

Для цього використовується політика Removable Disks: Deny execute access (рис.4.9).

Рисунок 4.9 - Налаштування політики, що блокує запуск виконуваних файлів та скриптів з USB-дисків

4.2.3 Налаштування можливості використання USB-накопичувачів залежно від привілеїв користувачів

У ряді випадків необхідно заборонити використовувати USB-носії усім користувачам комп'ютера, крім ряду категорій, що мають підвищені привілеї. Найчастіше це стосується керівників підрозділів та адміністраторів.

Найпростіше встановити виняток у політиці за допомогою Security Filtering GPO.

Розглянемо випадок, коли потрібно заборонити використання політики блокування USB до групи адміністраторів домену. У цій ситуації потрібно виконати такі кроки:

1. Звернутися до активованої політики Disable USB Access у консолі Group Policy Management.
2. Додати групу Domain Admins у розділі Security Filtering (рис.4.10).
3. Встановити заборону застосування для групи Domain Admins налаштування даної GPO. Для цього потрібно перейти на вкладку Delegation, далі перейти в розділ Advanced, натиснувши відповідну кнопку.

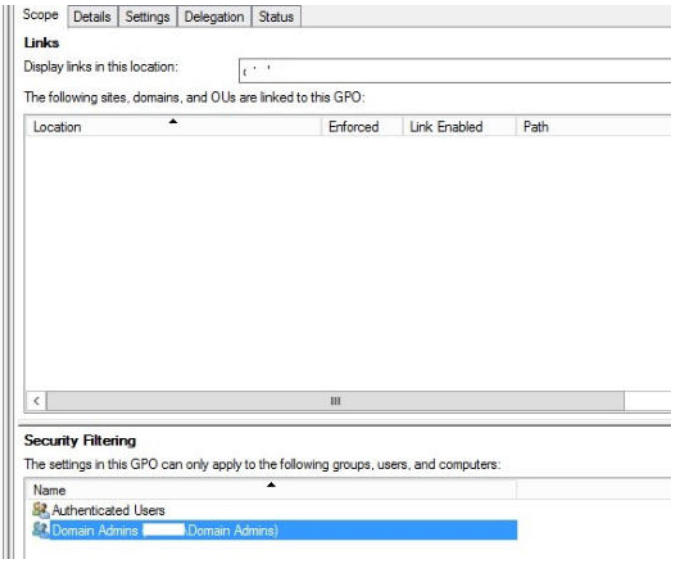

Рисунок 4.10 – Додавання групи Domain Admins

Після цього в редакторі налаштувань безпеки потрібно вказати те, що для групи Domain Admins заборонено застосовувати налаштування даної GPO (Apply group policy – Deny), як показано на рисунку 4.11.

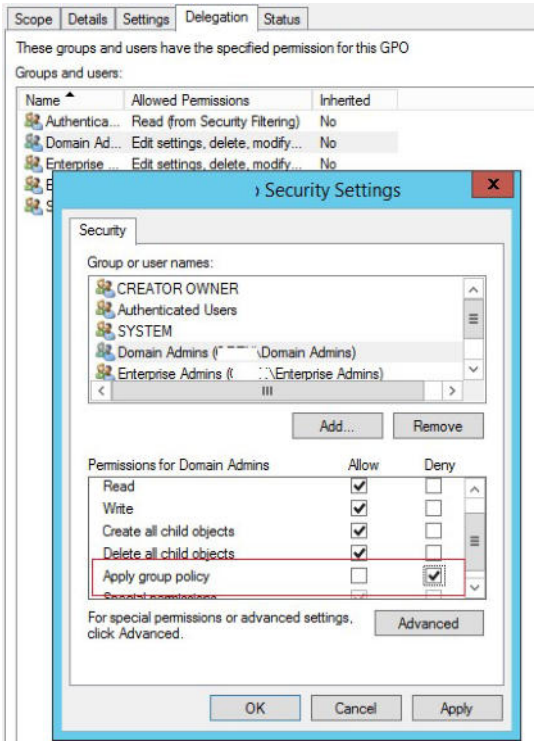

Рисунок 4.11 – Встановлення заборони застосування GPO до групи Domain Admins

Далі розглянемо розв'язання зворотного завдання. Припустимо, що потрібно встановити дозвіл на використання зовнішніх USB-накопичувачів для всіх користувачів, крім тих, що входять до певної групи [6].

Ця задача може бути вирішена наступним чином. Спочатку створюється група безпеки “Deny USB”, після чого ця група додається у налаштуваннях політики безпеки. Для цієї групи встановлюється дозвіл на читання та застосування GPO, для груп Authenticated Users або Domain Computers встановлюється лише дозвіл на читання (потрібно поставити галку у пункті Apply group policy), як показано на рис. 4.12.

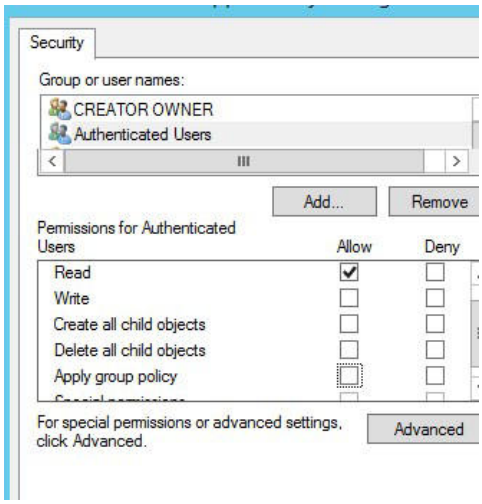

Рисунок 4.12 – Налаштування обмежень для групи

Після цього користувачі, яким потрібно заблокувати доступ до зовнішніх носіїв, додаються до створеної групи AD.

4.2.4 Встановлення дозволу на використання зареєстрованого USB-носія

Розглянемо механізм ініціалізації USB-носія у середовищі Windows.

При підключенні будь-якого USB-накопичувача до комп'ютера, драйвер USBSTOR встановлює пристрій і створює у гілці реєстру HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR окрему гілку, в якій міститься інформація про накопичувач (наприклад, Disk&Ven_Kingstom&0_1), як показує рис. 4.13.

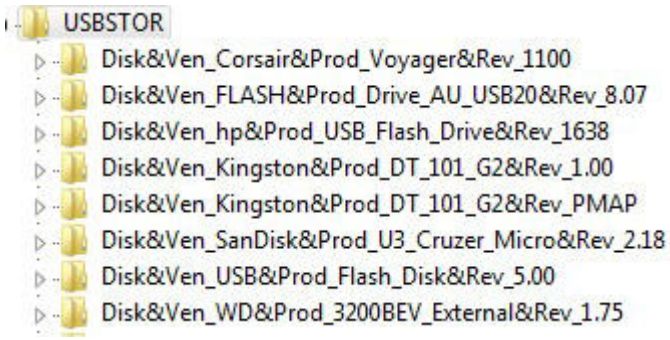

Рисунок 4.13 – Процес ініціалізації USB-носія

Наявність цього механізму у складі Windows дає можливість отримати список USB-накопичувачів, які будь-коли підключалися до цього комп'ютера. Для цього може бути використана наступна команда PowerShell:

```
Get-ItemProperty –Path
HKLM:\SYSTEM\CurrentControlSet\Enum\USBSTOR\*\*| select
FriendlyName
```

Результат виконання команди бачимо на рис.4.14.

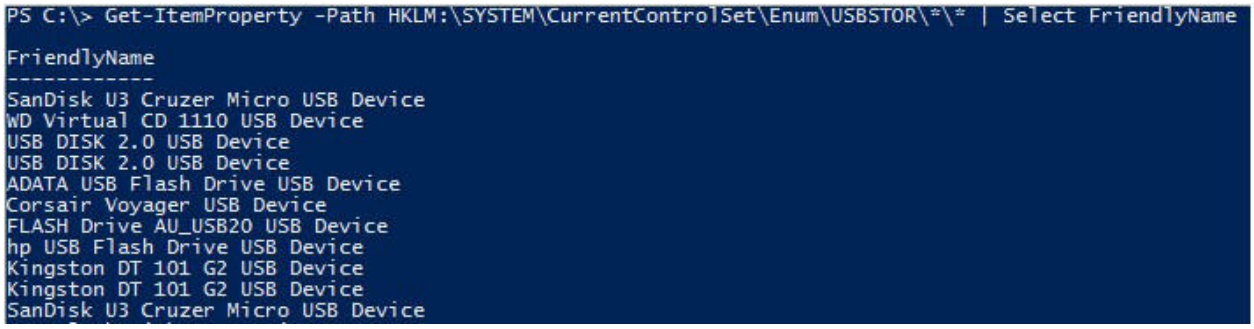

Рисунок 4.14 – Отримання списку USB-накопичувачів, для яких було виконано ініціалізацію в системі

Далі виконується видалення всіх записів для раніше підключених USB-носіїв, крім тих, для яких потрібно забезпечити можливість підключення. Після цього дозволи для гілки реєстру USBSTOR змінюються таким чином, щоб у всіх користувачів, у тому числі SYSTEM та адміністраторів, були лише права на читання. У результаті таких дій, при спробі підключення будь-

якого USB-накопичувача, крім дозволеного, Windows не зможе встановити пристрій [6].

Крім того, може бути створене завдання Task Sheduler, з прив'язкою до події EventID підключення USB-диска до комп'ютера, яке активує виконання скрипту перевірки нового носія.

У випадку, якщо серійний номер пристрою відсутній у списку дозволених, виконується автоматичне вимкнення будь-яких USB-накопичувачів.

Наприклад, розглянемо відповідний скрипт:

```
$usbdev = get-wmiobject win32_volume | where{$_.DriveType -eq
'2'}If ($usbdev.SerialNumber –notlike
“32SM32846AD”){$usbdev.DriveLetter =
$null$usbdev.Put()$usbdev.Dismount($false,$false) | Out-Null
}
```

У цьому скрипті wmi-клас Win32_Volume представляє області зберігання даних. Клас повертає відомості про всі локальні томи незалежно від статусу (відформатовані, неформатовані, змонтовані або відключені від мережі). У свою чергу, властивість DriveType у значенні 2 вказує на знімні пристрої.

Таким чином, до знімного пристрою, серійний номер якого не відповідає дозволеному, автоматично застосовуватиметься метод Dismount з його подальшим вимкненням.

4.3 Аналіз функціонування блокуючих політик

Для того, щоб відстежити результативність раніше застосованих політик щодо обмеження використання знімних носіїв, потрібно отримати інформацію про історію їх підключення до ПК [5].

У найпростішому випадку, щоб отримати список USB накопичувачів, підключених до комп'ютера, необхідно виконати таку команду PowerShell (рис.4.15):

```
Get-PnpDevice -PresentOnly | Where-Object { $_.deviceId
-match '^USBSTOR'}
```

```
PS C:\Windows\system32> Get-PnpDevice -PresentOnly | Where-Object { $_.deviceId -match '^USBSTOR' }

Status     Class          FriendlyName                                                  Ins
------     -----          ------------                                                  ---
OK         DiskDrive      UFD 2.0 Silicon-Power16G USB Device                           USB
```

Рисунок 4.15 – отримання списку USB-накопичувачів, підключених у поточний момент

Тут статус «OK» вказує на те, що цей пристрій підключено та функціонує штатно.

Крім розглянутого способу, відстежувати факти підключення/відключення USB-накопичувачів дозволяє журнал подій Windows.

Доступ до цих подій знаходиться в журналі Event Viewer → Application and Services Logs → Windows → Microsoft-Windows-Driver Frameworks-User Mode → Operational.

У той же час, оскільки за замовчуванням Windows не зберігає історію про підключення, попередньо необхідно активувати ведення даного логу вручну (EnableLog) або через GPO (рис.4.16).

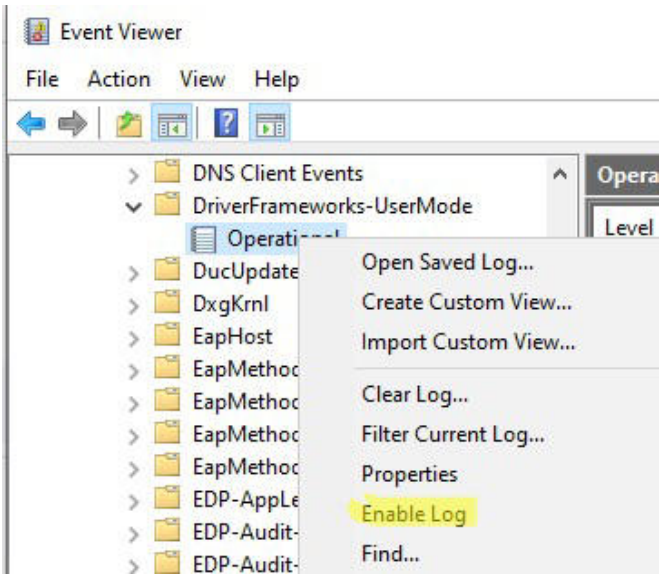

Рисунок 4.16 – Увімкнення логування події підключень знімних носіїв

Після цього з'являється можливість використовувати подію з EventID 2003 для отримання інформації про час підключення USB накопичувача і Event ID 2102 про час відключення (рис.4.17):

```
Forwarded finished Pnp or Power operation (27, 2) to the lower
driver for device
SWD\WPDBUSENUM\_??_USBSTOR#DISK&VEN_UFD_2.0&PROD_SILICON-
POWER16G&REV_PMAP#12010208030E6C1 B6BF-11D0-94F2-00A0C91EFB8B} з
status 0x0.
```

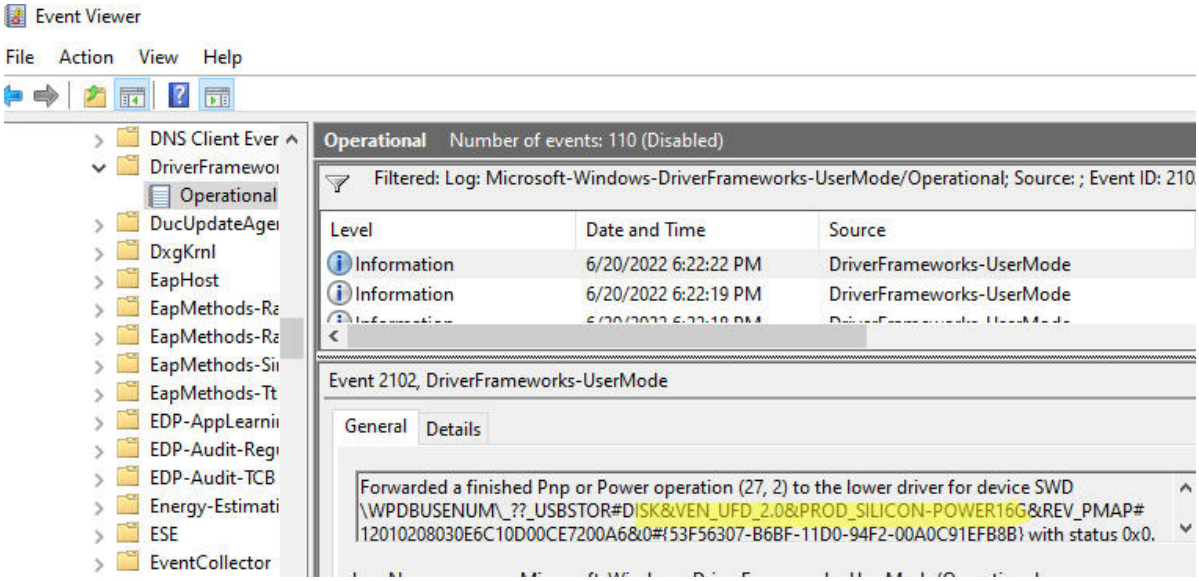

Рисунок 4.17 – Отримання відомостей про підключення/вимкнення USB накопичувача в Event Viewer

4.4 Розробка заходів щодо підвищення рівня обізнаності персоналу з питань інформаційної безпеки

Заходи щодо навчання персона слід класифікувати на планові та ситуативні. Тут до першої групи належать такі заходи, як [7]:

- первинні (ввідні);
- періодичні (щорічні, квартальні і т.д.).

У свою чергу, заходи другої групи це:

- інструктаж, який проводиться за фактом зміни регламенту роботи мережі або її окремих компонентів;
- інструктаж, що проводиться у разі впровадження нових апаратних/програмних засобів захисту;
- інстуктаж, присвячений інцидентам.

У ході планових навчальних заходів до персоналу доводяться відомості щодо:

- основ інформаційної безпеки з позиції специфіки діяльності підприємства;

- чинного законодавства, що регулює питання інформаційної безпеки;

- найчастіших видів загроз, їх ознак та наслідків.

Окремо звертається увага на методи соціальної інженерії, зокрема – фішинг. У рамках цього розглядаються класичні механізми фішингу, виконується аналіз реалізованих фішинг-атак. Аналізуються дії користувачів, що сприяють успішній реалізації атак на основі фішингу.

ВИСНОВКИ

У відповідності до технічного завдання, було обрано інструментарій та досліджено схему комплексного захисту мережі від зловмисних впливів.

При цьому, ураховувалась ймовірність існування як зовнішніх, так і внутрішніх загроз.

Схема захисту мережі містить у собі компоненти наступних рівнів:

- рівень периметру;
- рівень внутрішньої мережі;
- рівень вузла;
- загально мережевий рівень.

Це, у свою чергу, дозволяє забезпечити захист мережевої інфраструктури за рахунок:

- обмеження або блокування підозрілого трафіку та трафіку з потенційно небезпечних джерел;
- виявлення та блокування зловмисних агентів на рівні периметру, окремих кінцевих та мережевих вузлів усередині периметру за аномаліями поведінки, а також на базі сигнатурного та евристичного підходів;
- обмеження можливостей спрямованого чи випадкового впливу на елементи мережевої інфраструктури з боку користувачів.

При цьому, захист мережі на рівні периметру побудовано на базі апаратно-програмного модулю Check Point 1590 NGFW, що виступає у ролі міжмережевого екрану нового покоління, а також граничного маршрутизатора.

У свою чергу, для захисту внутрішнього мережевого простору на базі окремого ПК розгорнуто IDPS Suricata, що також може забезпечувати функції між мережевого екрану у доповнення до NGFW.

Водночас, на рівні кінцевих вузлів використовується IDPS Suricata у локальному форматі налаштування.

Виходячи з того, що за початковими умовами адміністрування мережі здійснюється на базі Windows Server з Active Directory, це дає змогу:

- реалізувати заходи, спрямовані на обмеження використання знімних носіїв користувачами, на базі групових політик GPO, без залучення додаткового інструментарію;

- виконати гнучке налаштування політик використання знімних зовнішніх носіїв у залежності від привілеїв користувача, а також дозволити використання зареєстрованих пристроїв;

- налаштувати моніторинг спроб доступу до знімних накопичувачів.

Таким чином, усі пункти технічного завдання виконано у повному обсязі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Microsoft security report [Електронний ресурс] – Режим доступу: https://microsoft.com/securityinsights.

2. Antivirus and Cybersecurity Statistics & Facts 2021 [Електронний ресурс] – Режим доступу: https://wethegeek.com/antivirus-statistics-facts/

3. Stood, A. Targeted Cyber Attacks. — Elsevier Inc.. — 2014. — ISBN 978-0-12-800604-7.

4. Шаньгін В.Ф. Захист інформації в розподілених корпоративних мережах і системах [Текст]: підручник / В.Ф. Шаньгин, А.В. Соколов. – М.: ДМК Пресс, 2002. – 656 с.

5. Шаньгін В.Ф. Інформаційна безпека та захист інформації. ДМК-Прес., 2017, 702 с.

6. El-Monem A., El-Bawab A. Untangle Network Security. – Packt Publishing, - 2014. – 564 p. ISBN: 9781849517720.

7. Sadiqui A. Computer Network Security. - Wiley-ISTE, - 2020. - pp: 655 p. ISBN: 9781786305275.

8. Comodo Firewall | Get Best Personal Firewall Software [Електронний ресурс] Режим доступу: https://personalfirewall.comodo.com/

9. FortiGate: Next Generation Firewall (NGFW) ~ PT. Network Data Sistem [Електронний ресурс] Режим доступу: https://nds.id/en/products/networks-en/firewall-en/fortigate-next-generation-firewall-ngfw-en/

10. Check Point Next Generation Firewalls (NGFW) [Електронний ресурс] Режим доступу: https://www.checkpoint.com/quantum/next-generation-firewall/

11. Compare Comodo Firewall and Check Point Next Generation Firewalls (NGFWs) | G2 [Електронний ресурс] Режим доступу: https://www.g2.com/compare/comodo-firewall-vs-check-point-next-generation-firewalls-ngfws

12. NGFW for small businesses. Unpacking and setup [Електронний ресурс] Режим доступу: https://tech-en.netlify.app/articles/en511462/?ysclid=lpxtgqak6t651875595

13. Check Point 1500 Security Gateway Datasheet [Електронний ресурс] Режим доступу: https://www.checkpoint.com/downloads/products/1500-security-gateway-datasheet.pdf

14. Snort – Network Intrusion Detection System [Електронний ресурс] Режим доступу: https://snort-org.herokuapp.com/

15. Home - Suricata [Електронний ресурс] Режим доступу: https://suricata.io/

16. Documentation - Suricata [Електронний ресурс] Режим доступу: https://docs.suricata.io/

17. User Guide - Suricata [Електронний ресурс] Режим доступу: https://docs.suricata.io/en/latest/

18. 3. Installation — Suricata 8.0.0-dev documentation [Електронний ресурс] Режим доступу: https:// docs.suricata.io/en/latest/install.html

19. The Security Analyst’s Guide to Suricata [Електронний ресурс] Режим доступу: https://github.com/StamusNetworks/suricata-4-analysts

20. Emerging Threat Intelligence - Cyber Threat Solutions | Proofpoint US [Електронний ресурс] Режим доступу: https://www.proofpoint.com/us/products/advanced-threat-protection/et-intelligence