Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: " Застосування NGFW для виявлення кіберзагроз "

Виконав: студент (ка) IV курсу, групи СБ-41
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Ожинська Анастасія Олександрівна
підпис (прізвище та ініціали)

Керівник Лечаченко Т. А.
підпис (прізвище та ініціали)

Нормоконтроль Дроздова Т. В.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Ожинській Анастасії Олександрівні
(прізвище, ім'я, по батькові)

1. Тема роботи Застосування NGFW для виявлення кіберзагроз

Керівник роботи Лечаченко Тарас Анатолійович, доктор філософії, старший викладач кафедри КБ.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 02 » 05 2025 року № 4/7-361

2. Термін подання студентом завершеної роботи 12.06.2025

3. Вихідні дані до роботи Документація OPNsense та Zenarmor, вимоги до NGFW.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1. Огляд предметної області
2. Опис та налаштування компонентів тестового середовища
3. Налаштування та тестування NGFW Zenarmor
4. Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титульна сторінка. 2.Актуальність дослідження. 3. Мета, об'єкт, предмет дослідження.
4. Завдання. 5. Загальна схема тестового середовища. 6. Архітектура рішення.
7. Основні компоненти OPNsense. 8. Підключення та налаштування Zenarmor.
9. Тестування NGFW. 10. Результати тестування Zenarmor. 11. Журнал блокувань у Zenarmor
12. Блокування додатків: приклад із Gmail. 13. Звіт роботи Zenarmor. 14. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко С. Ю., к.т.н. доцент кафедри МТ		

7. Дата видачі завдання 29.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.01.2025	
2.	Опрацювання джерел в галузі дослідження	02.02 – 30.01	
3.	Оформлення розділу «Огляд предметної області»	21.02 – 10.03	
4.	Оформлення розділу «Опис та налаштування компонентів тестового середовища»	11.03 – 25.03	
5.	Оформлення розділу «Налаштування та тестування NGFW Zenarmor»	10.04 – 05.05	
6.	Оформлення розділу «Безпека життєдіяльності, основи охорони праці»	10.05 – 21.05	
7.	Оформлення кваліфікаційної роботи	23.05 – 06.06	
8.	Нормоконтроль	06.06 – 10.06	
9.	Перевірка на плагіат	11.06 – 12.06	
10.	Попередній захист кваліфікаційної роботи	14.06 – 15.06	
11.	Захист кваліфікаційної роботи	26.06.2025	

Студент _____ Ожинська А. О.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Лечаченко Т. А.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Застосування NGFW для виявлення кіберзагроз // Кваліфікаційна робота ОР «Бакалавр» // Ожинська Анастасія Олександрівна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2025 // С. 71, рис. – 36, табл. – - , кресл. – 14, додат. – .

Ключові слова: Zenarmor, NGFW, OPNsense, Hyper-V, загрози.

У кваліфікаційній роботі бакалавра було досліджено можливості брандмауерів нового покоління (NGFW) для підвищення рівня безпеки та проведено практичну реалізацію системи захисту на базі платформи OPNsense із модулем Zenarmor. Розглянуто типи й принципи роботи брандмауерів, а також особливості глибокого аналізу трафіку та виявлення сучасних кіберзагроз. Створено тестове середовище з використанням гіпервізора Hyper-V, у межах якого досліджено роботу NGFW, налаштовано правила безпеки, політики контролю додатків. За результатами тестування було підтверджено ефективність виявлення та блокування сучасних загроз (фішинг, шкідливе програмне забезпечення, нові чи запарковані домени), а також продемонстровано можливості блокування небажаних додатків. Отримані результати можуть бути використані для впровадження NGFW у корпоративних і навчальних мережах із метою підвищення рівня інформаційної безпеки та протидії актуальним кіберзагрозам.

ABSTRACT

Application of NGFW for Detecting Cyber Threats // Thesis of educational level "Bachelor"// Anastasiia Ozhynska // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБ-41 // Ternopil, 2025 // P. 69, figs. 36, tables - , drawings 14, added. -.

Keywords: Zenarmor, NGFW, OPNsense, Hyper-V, threats.

The bachelor's thesis investigated the capabilities of next-generation firewalls (NGFW) to improve security. A practical implementation of a security system based on the OPNsense platform with the Zenarmor module was carried out. The types and principles of firewalls, as well as the features of in-depth traffic analysis and detection of modern cyber threats were considered. A test environment was created using the Hyper-V hypervisor, within which the NGFW was studied, security rules and application control policies were configured. The test results confirmed the effectiveness of detecting and blocking modern threats (phishing, malware, new or parked domains), and demonstrated the ability to block unwanted applications. The results obtained can be used to implement NGFW in corporate and educational networks to improve information security and counteract current cyber threats.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

NGFW	—	Next-Generation Firewall
IDS	—	Intrusion Detection System
IPS	—	Intrusion Prevention System
WAN	—	Wide Area Network
NAT	—	Network Address Translation
DHCP	—	Dynamic Host Configuration Protocol
DPI	—	Deep Packet Inspection
LAN	—	Local Area Network
FWaaS	—	Firewall as a Service
WAF	—	Web Application Firewall
TCP	—	Transmission Control Protocol
UDP	—	User Datagram Protocol
ВМ	—	Віртуальна машина
VPN	—	Virtual Private Network

ВСТУП

Актуальність теми. Стрімке зростання кількості та складності кіберзагроз ставить під загрозу безпеку інформаційних систем організацій та окремих користувачів. Традиційні засоби захисту, такі як класичні брандмауери, виявляються недостатньо ефективними у боротьбі з новими типами атак, які використовують складні методи обходу захисту. У відповідь на ці виклики з'явилися брандмауери нового покоління (NGFW), які поєднують функціонал глибокого аналізу трафіку, виявлення додатків, систем виявлення та запобігання вторгнень (IDS/IPS) та інших механізмів для підвищення рівня кіберзахисту. Дослідження можливостей NGFW та практичної реалізації на базі сучасних платформ, таких як OPNsense, є важливим кроком для підвищення рівня інформаційної безпеки, особливо в умовах зростаючої кількості гібридних і таргетованих атак.

Мета і задачі дослідження. Метою роботи є дослідження можливостей NGFW для виявлення кіберзагроз та практична реалізація системи на базі платформи OPNsense.

Для досягнення мети були поставлені такі завдання:

- проаналізувати принципи роботи та типи брандмауерів;
- вивчити особливості та переваги NGFW у виявленні кіберзагроз;
- розробити архітектуру системи на базі OPNsense з використанням брандмауер Zenarmor;
- налаштувати основні компоненти системи: WAN, LAN, DHCP, NAT;
- провести тестування роботи брандмауера Zenarmor для виявлення кіберзагроз.

Об’єкт дослідження. Процеси забезпечення мережевої безпеки з використанням сучасних технологій фільтрації трафіку.

Предмет дослідження. Функціональні можливості брандмауера нового покоління Zenarmor у системі OPNsense для виявлення та запобігання кіберзагрозам.

Практичне значення одержаних результатів. Результати дослідження можуть бути використані для розгортання систем кіберзахисту на базі NGFW у корпоративних мережах, освітніх установах та інших організаціях. Практичні рекомендації щодо налаштування та використання OPNsense із Zenarmor сприятимуть підвищенню ефективності виявлення кіберзагроз та забезпеченню безпеки критично важливих інформаційних ресурсів.

РОЗДІЛ 1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Причини використання брандмауерів

В умовах активного розвитку інформаційних технологій, підключення до Інтернету та інтеграції систем, мережеві ресурси організацій і користувачів стають вразливими до широкого спектру кіберзагроз, таких як хакерські атаки, віруси, шкідливі програми, фішинг та інші типи зловмисних дій [1] [2].

Брандмауери відіграють одну з основних ролей у створенні бар'єра між внутрішніми мережами та зовнішнім середовищем, запобігаючи небажаному трафіку або небезпечним запитам, які можуть призвести до порушення цілісності, конфіденційності та доступності даних. Основною причиною використання брандмауерів є забезпечення контролю трафіку на основі певних правил, що дозволяє зупиняти спроби проникнення зловмисників у мережу, обмежувати доступ до потенційно небезпечних ресурсів та мінімізувати ризики для інформаційної інфраструктури.

Окрім захисту від зовнішніх загроз, брандмауери також забезпечують моніторинг і управління внутрішнім трафіком, що дозволяє уникати витоків інформації та контролювати поведінку користувачів у мережі. Це особливо важливо для організацій, де можуть виникати загрози через людський фактор, такі як випадкове відкриття шкідливих файлів чи доступ до небезпечних веб-сайтів. Іншою причиною впровадження брандмауерів є відповідність нормативним вимогам і стандартам безпеки. У багатьох галузях існують правила, які вимагають впровадження заходів із захисту даних, включно з використанням мережевих фільтрів. Брандмауери дозволяють виконувати ці вимоги, забезпечуючи розділення трафіку, блокування небезпечних з'єднань і створення журналів подій для подальшого аналізу.

Зрештою, брандмауери надають організаціям контроль над мережею, дозволяючи налаштовувати політики безпеки відповідно до потреб і специфіки роботи. Брандмауери є невід'ємним елементом комплексного захисту, здатним

забезпечити надійний рівень безпеки як для великих організацій, так і для індивідуальних користувачів.

1.2 Основні принципи роботи та проектування брандмауерів

Основні принципи роботи брандмауерів базуються на контролі та фільтрації мережевого трафіку, що проходить через них, з метою забезпечення безпеки інформаційних систем. Брандмауери виступають як перший бар’єр між внутрішньою мережею та зовнішнім світом, захищаючи ресурси від несанкціонованого доступу, шкідливих дій та небезпечного трафіку. Їх функціональність ґрунтується на кількох ключових механізмах [3] [4].

Один із основних принципів роботи брандмауерів – це аналіз мережевого трафіку на основі заданих правил. Кожен пакет даних, що проходить через брандмауер, перевіряється за різними параметрами, такими як IP-адреса відправника й отримувача, номер порту, протокол, вміст пакету тощо. На основі цієї перевірки брандмауер приймає рішення: дозволити, блокувати чи перенаправити трафік. Цей процес може бути заснований як на статичних правилах, встановлених адміністратором, так і на динамічних алгоритмах, що враховують контекст і поведінку трафіку.

Другий важливий принцип – це розмежування внутрішньої та зовнішньої зон мережі. Брандмауер розділяє мережу на сегменти, зокрема захищені (внутрішні) та незахищені (зовнішні). Такий поділ дозволяє обмежити доступ до критичних ресурсів і запобігти витоку інформації за межі довірених зон.

Брандмауери можуть працювати за принципом "дозволено все, що не заборонено" або "заборонено все, що не дозволено". Ці два підходи суттєво впливають на рівень безпеки, контроль трафіку та управління мережевими ресурсами.

Брандмауери, що працюють за принципом "дозволено все, що не заборонено" пропускають увесь трафік, окрім того, який явно заборонений набором правил. Це означає, що адміністратор мережі створює список небажаного трафіку, який блокується, а решта трафіку автоматично проходить

через брандмауер. Такий підхід може бути доцільним у мережах, де велика частина трафіку є довіреною або контрольованою, а також у випадках, коли потрібно мінімізувати обмеження на потоки даних. Однак основний недолік цього типу брандмауерів полягає в ризику пропуску небажаного трафіку, якщо він не був явно визначений у правилах фільтрації.

Брандмауери, що дотримуються принципу "заборонено все, що не дозволено" пропускають лише трафік, який відповідає попередньо визначеним правилам, блокуючи все інше. Такий підхід забезпечує значно вищий рівень безпеки, оскільки зменшує ймовірність випадкового пропуску небажаного або шкідливого трафіку. Ці брандмауери є оптимальним вибором для мереж, які пропонують послуги публічного доступу до Інтернету, або для корпоративних мереж, які потребують суворого контролю над типами дозволеного трафіку. Весь трафік, що не відповідає встановленим правилам, блокується та реєструється в журналах, що полегшує моніторинг і аналіз потенційних загроз. Основна перевага даного типу брандмауерів полягає в їх здатності забезпечувати кращий контроль як над вхідним, так і над вихідним трафіком. Це особливо важливо для захисту приватних мереж від публічного Інтернету, де велика кількість запитів може бути шкідливою. Забороняючи будь-який нерегламентований трафік, ці брандмауери мінімізують ризики, пов'язані з помилковою класифікацією даних або недоліками в правилах фільтрації. Хоча даний підхід забезпечує більшу безпеку, він може вимагати більше зусиль під час налаштування, оскільки адміністратору потрібно детально визначати всі дозволені типи трафіку. Однак цей підхід виправдовує себе в критичних системах, де безпека є пріоритетом.

Ще один важливий аспект роботи брандмауерів – це обробка трафіку в реальному часі. Для ефективного захисту необхідно, щоб перевірка пакетів даних і прийняття рішень відбувалися швидко, без затримок, які можуть негативно вплинути на продуктивність мережі. Брандмауери забезпечують швидкий аналіз даних, використовуючи різні методи, такі як глибокий аналіз пакетів (DPI) або контроль стану з’єднань (stateful inspection). Крім того, сучасні брандмауери можуть інтегруватися з іншими системами кібербезпеки,

такими як системи IDS/IPS. Це дозволяє виявляти й запобігати складним атакам, аналізуючи поведінку трафіку й зіставляючи його з відомими шаблонами атак. Важливою частиною роботи брандмауерів є ведення журналів та створення звітів. Це забезпечує моніторинг активності в мережі, аналіз подій і виявлення потенційних загроз. Завдяки цьому адміністратори можуть оперативно реагувати на інциденти безпеки та вдосконалювати політики захисту.

При проектуванні та використанні брандмауерів для забезпечення мережевої безпеки необхідно враховувати декілька ключових принципів, які дозволяють створити ефективну та надійну систему захисту [5].

Брандмауери повинні бути спроєктовані з урахуванням конкретних потреб безпеки організації. Цей процес починається з оцінки поточного стану безпеки та вимог, визначених керівництвом. На цьому етапі важливо зрозуміти, які саме ресурси та служби необхідно захищати, які загрози найбільш імовірні, та як брандмауери можуть стати бар'єром проти цих ризиків.

Один із ключових принципів – це формування чіткої політики безпеки. Вона має включати правила доступу, способи управління мережевими ресурсами та методи авторизації. Без чіткої політики безпеки робота брандмауера буде хаотичною та менш ефективною. Політика повинна враховувати доступ до внутрішніх і зовнішніх ресурсів, вразливості систем, можливі способи захисту, а також економічну ефективність обраних методів. Ще одним важливим аспектом є визначення дозволених типів комунікацій. Брандмауер повинен регулювати, хто, коли і як може використовувати мережу, а також обмежувати доступ до небажаних чи потенційно небезпечних служб. Це дозволяє уникати небажаного використання мережі та забезпечувати її продуктивність.

Розташування брандмауера в мережі також є важливим фактором. Його слід стратегічно розміщувати у вузлових точках мережі для захисту найбільш критичних ресурсів. Наприклад, фільтруючі брандмауери можуть бути встановлені на периметрі мережі для перевірки вхідного трафіку, а проксі-брандмауери – між веб-серверами та внутрішніми мережами. Іншим принципом

є багаторівневий захист. Це означає, що система безпеки повинна складатися з кількох взаємопов’язаних компонентів, кожен з яких виконує свою функцію. Якщо один рівень захисту буде скомпрометовано, інші зможуть перехопити загрозу. Контроль додатків і видимість активності в мережі є ще одним критично важливим аспектом роботи брандмауерів. Сучасні системи, такі як NGFW, здатні аналізувати трафік на рівні додатків, визначати, які програми використовуються, і регулювати їх доступ. Це допомагає як блокувати шкідливі програми, так і забезпечувати продуктивне використання мережевих ресурсів. Запобігання загрозам є основним завданням брандмауера. Використовуючи методи DPI та інтегровані системи IDS/IPS, сучасні брандмауери можуть виявляти аномалії у трафіку, ідентифікувати підозрілу поведінку та блокувати потенційно небезпечні з’єднання.

Особливу увагу варто приділяти захисту пристроїв і користувачів. Сучасні брандмауери можуть забезпечувати авторизацію користувачів не лише за IP-адресами, але й за унікальними характеристиками пристроїв або іменами користувачів. Це ускладнює для зловмисників проникнення в мережу за допомогою вкрадених або підроблених даних. Віддалені користувачі також становлять загрозу, тому важливо налаштовувати безпечний доступ для них. Брандмауери нового покоління дозволяють впроваджувати віртуальні приватні мережі (VPN), які забезпечують захищене підключення навіть у ненадійних публічних мережах.

Ефективність роботи брандмауера залежить від продуманого проектування та використання відповідних технологій. Дотримання принципів, таких як формування політики безпеки, багаторівневий захист, контроль додатків та управління доступом, дозволяє забезпечити найвищий рівень безпеки мережі та знизити ризик кібератак.

1.3 Типи брандмауерів

Брандмауери класифікуються за різними параметрами такими як системний захист, форм-фактор, мережеве розташування та метод фільтрації

даних. Ця класифікація дозволяє обрати відповідний тип брандмауера залежно від потреб і архітектури мережі [6].

1.3.1 Класифікація за системним захистом

Брандмауери на основі хоста та мережеві брандмауери мають різні підходи до забезпечення безпеки та виконують свої функції на різних рівнях мережі. Вони обидва використовуються для контролю трафіку, але їхні особливості, призначення та ефективність значно відрізняються залежно від умов використання [6].

Брандмауери на основі хоста працюють на рівні окремого пристрою або сервера, забезпечуючи захист саме для цього хоста (див. рисунок 1.1).

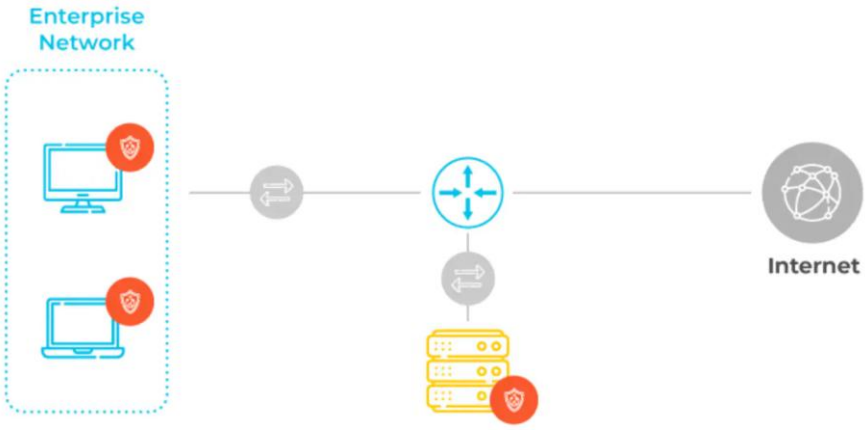

Рисунок 1.1 – Брандмауер на основі хоста

Вони є програмними рішеннями, які зазвичай інтегруються в операційну систему (наприклад, Windows Firewall) або встановлюються як додаткове програмне забезпечення. Основна мета таких брандмауерів – контроль і фільтрація вхідного та вихідного трафіку для конкретного пристрою. Вони дозволяють налаштовувати політики безпеки для додатків, процесів або портів, працюючи у вузько спрямованому режимі. Наприклад, брандмауери на основі хоста можуть дозволяти лише певним програмам доступ до Інтернету або блокувати небажані спроби з'єднань ззовні. Однією з головних переваг хостових брандмауерів є їхня гнучкість і точність. Вони дозволяють

створювати індивідуальні налаштування для кожного пристрою, враховуючи його специфіку та завдання. Це особливо важливо для захисту критичних серверів або пристроїв, які обробляють конфіденційні дані. Однак такі брандмауери мають обмеження у масштабованості, адже кожен пристрій вимагає окремого налаштування, що може бути складним у великих мережах. Також вони менш ефективні у захисті від загроз, які спрямовані на загальну мережеву інфраструктуру, оскільки працюють ізольовано від інших пристроїв.

Мережеві брандмауери, на відміну від хостових, розташовуються між різними сегментами мережі або на її межі, забезпечуючи захист для всього трафіку, який проходить через них (див. рисунок 1.2).

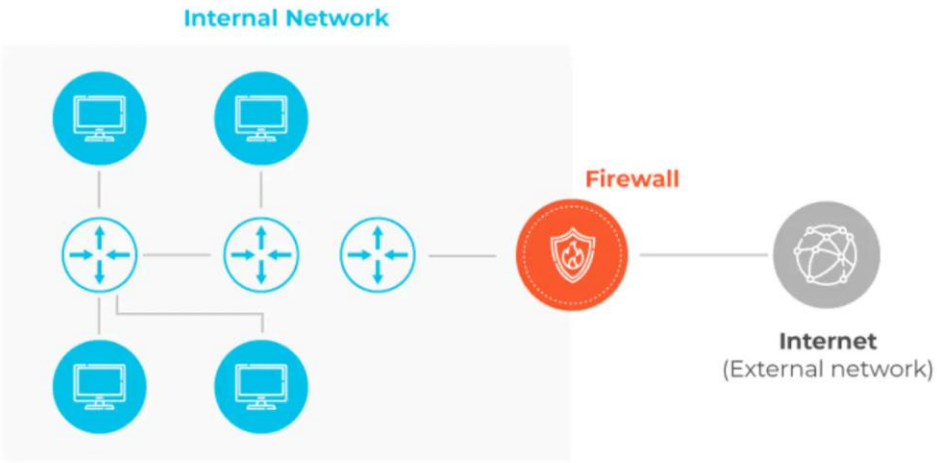

Рисунок 1.2 – Мережевий брандмауер

Вони зазвичай працюють на фізичних або віртуальних пристроях, які інтегруються в мережеву інфраструктуру. Мережеві брандмауери контролюють і фільтрують потоки даних між внутрішньою мережею та зовнішнім світом або між різними підмережами в організації. Головною перевагою мережевих брандмауерів є їхня здатність забезпечувати централізований захист для всієї мережі. Вони можуть блокувати небажаний трафік, запобігати вторгненням і створювати бар'єр, який ускладнює проникнення зловмисників. Завдяки своїй масштабованості вони ідеально підходять для великих організацій, де потрібно одночасно захищати велику кількість пристроїв. Мережеві брандмауери можуть працювати на різних рівнях: від базової фільтрації пакетів до складних систем нового покоління NGFW, які включають контроль додатків, інтеграцію з

IDS/IPS і глибокий аналіз трафіку. Проте мережеві брандмауери мають свої обмеження. Вони не можуть забезпечити такий самий рівень деталізації та гнучкості у захисті окремих пристроїв, як це роблять хостові брандмауери. Наприклад, вони можуть не виявляти шкідливі дії, що вже відбуваються на рівні конкретного хоста, якщо трафік не покидає межі внутрішньої мережі.

У багатьох сучасних мережах використовується комбінація обох типів брандмауерів. Мережеві брандмауери створюють першу лінію оборони, забезпечуючи захист на рівні всієї мережі, тоді як хостові брандмауери захищають окремі пристрої від більш специфічних загроз. Такий підхід забезпечує багаторівневий захист, який мінімізує вразливості та підвищує загальний рівень безпеки.

1.3.2 Класифікація за форм-фактором

За форм-фактором брандмауери поділяється на апаратні та програмні. Вони відрізняються своєю структурою, принципами роботи та сферою застосування. Вибір між цими типами залежить від потреб мережі, розміру організації та вимог до безпеки [6].

Апаратні брандмауери – це спеціалізовані фізичні пристрої, розроблені виключно для забезпечення безпеки мережі. Вони встановлюються на межі мережі або між її сегментами, виконуючи функції фільтрації та контролю трафіку (див. рисунок 1.3).

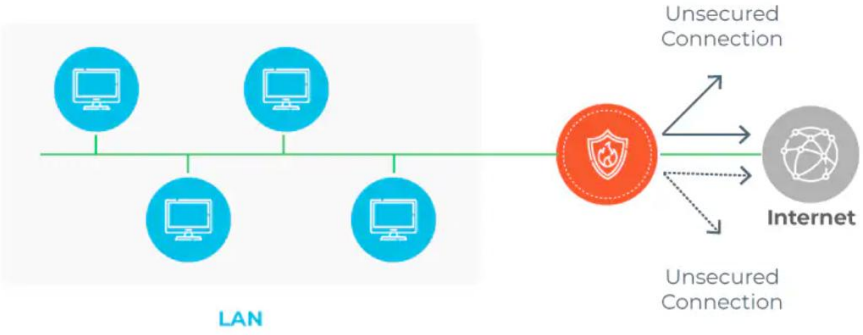

Рисунок 1.3 – Апаратний брандмауер

Апаратні брандмауери часто використовуються в корпоративних середовищах, де потрібно забезпечити захист великих обсягів даних і підтримку високої пропускної здатності. Ці пристрої працюють незалежно від інших компонентів мережі, що дозволяє мінімізувати навантаження на сервери та інші пристрої. Однією з ключових переваг апаратних брандмауерів є їхня висока продуктивність, оскільки вони мають спеціалізовані апаратні ресурси для обробки великої кількості трафіку. Вони також надають надійний фізичний захист, оскільки зловмисникам складніше отримати до них доступ без фізичного контакту. Крім того, апаратні брандмауери часто забезпечують більш високий рівень безпеки завдяки підтримці розширених функцій, таких як DPI, інтеграція з IDS/IPS. Проте апаратні брандмауери мають і свої обмеження. Вони зазвичай дорожчі, ніж програмні рішення, і потребують складнішого налаштування та обслуговування. Крім того, апаратні брандмауери менш гнучкі у масштабуванні, оскільки кожен пристрій має обмеження за кількістю оброблюваного трафіку, що може вимагати заміни обладнання при розширенні мережі.

Програмні брандмауери, на відміну від апаратних, є програмними рішеннями, які встановлюються на окремих пристроях або серверах (див. рисунок 1.4).

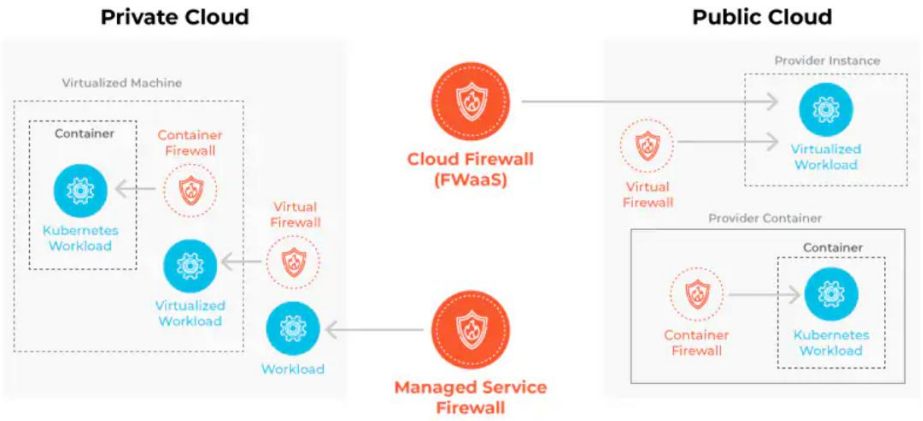

Рисунок 1.4 – Програмний брандмауер

Вони можуть працювати на базі операційної системи (наприклад, Windows, Linux) або як окремі додатки. Програмні брандмауери забезпечують

захист конкретного пристрою чи сегмента мережі, виконуючи функції моніторингу, фільтрації та блокування небажаного трафіку. Головна перевага програмних брандмауерів – це їхня гнучкість і доступність. Їх можна легко налаштовувати під конкретні потреби організації, інтегрувати з іншими програмними рішеннями та масштабувати без значних витрат. Вони є більш економічно вигідними, оскільки не потребують додаткового обладнання, а їх встановлення займає мінімум часу.

Програмні брандмауери представлені кількома типами, які орієнтовані на різні сценарії використання. Вони відрізняються своїми функціями, середовищем розгортання та призначенням. Серед основних типів виділяються контейнерні брандмауери, віртуальні брандмауери (хмарні) та брандмауери керованих служб.

Контейнерні брандмауери розроблені для роботи в сучасних контейнерних середовищах, таких як Kubernetes. Вони представляють собою програмну версію брандмауера наступного покоління (NGFW), яка інтегрується безпосередньо в інфраструктуру контейнерів. Контейнерні брандмауери вирішують специфічні завдання безпеки, які важко вирішити за допомогою традиційних брандмауерів, наприклад, захист східно-західного трафіку між контейнерами. Вони забезпечують глибоку інтеграцію з системами оркестрації Kubernetes, що дозволяє автоматично застосовувати правила безпеки до робочих навантажень контейнерів. Основне завдання таких брандмауерів – захист сучасних додатків від атак і викрадення даних.

Віртуальні брандмауери, також відомі як хмарні брандмауери, є віртуалізованими екземплярами брандмауерів, які працюють у віртуальних або хмарних середовищах. Вони забезпечують захист трафіку "північ-південь" (між користувачами та серверами) і "схід-захід" (між сегментами мережі або контейнерами). Завдяки функції мікросегментації, віртуальні брандмауери дозволяють чітко розділяти мережевий трафік у хмарних і фізичних дата-центрах, знижуючи ризик поширення атак між сегментами. Їх особливістю є здатність адаптуватися до змінної інфраструктури, характерної для хмарних середовищ, забезпечуючи динамічний контроль безпеки.

Хмарні брандмауери є варіацією віртуальних брандмауерів, які інтегруються в хмарну інфраструктуру і часто пропонуються як послуга (FWaaS). Ці брандмауери призначені для відсіювання шкідливого трафіку, захисту додатків і користувачів, які працюють у публічній хмарі. Хмарні брандмауери можуть надаватися як частина інфраструктури провайдерів хмарних послуг (наприклад, AWS, Azure або Google Cloud), або пропонуватися сторонніми постачальниками безпеки. Хмарні брандмауери забезпечують централізований контроль безпеки для розподілених додатків, що працюють у різних географічних точках.

Брандмауери керованих служб пропонуються як програмне забезпечення як послуга (SaaS). Вони забезпечують простоту використання, зменшуючи навантаження на адміністраторів завдяки автоматизації управління безпекою. Ці брандмауери часто налаштовуються та адмініструються постачальниками послуг, що дозволяє організаціям зосередитися на своїх бізнес-завданнях. Керовані брандмауери можуть забезпечувати безпеку на рівні додатків (рівень 7), масштабуватися відповідно до потреб організації та легко інтегруватися в існуючу інфраструктуру.

Вибір відповідного рішення залежить від середовища, типу загроз і вимог до безпеки. У багатьох випадках комбінування різних типів брандмауерів дозволяє створити багаторівневий захист, який відповідає сучасним викликам кібербезпеки.

1.3.3 Класифікація за розміщення у мережевій інфраструктурі

Розміщення брандмауерів у мережевій інфраструктурі визначає їхню функціональність, спосіб взаємодії з мережею та рівень захисту, який вони забезпечують. Існують три основні варіанти розташування брандмауерів у мережі: внутрішні брандмауери, розподілені брандмауери та брандмауери периметру [6]. Кожен із них виконує певні завдання та має свої особливості.

Внутрішні брандмауери розташовуються всередині мережі та призначені для захисту її окремих сегментів (див. рисунок 1.5).

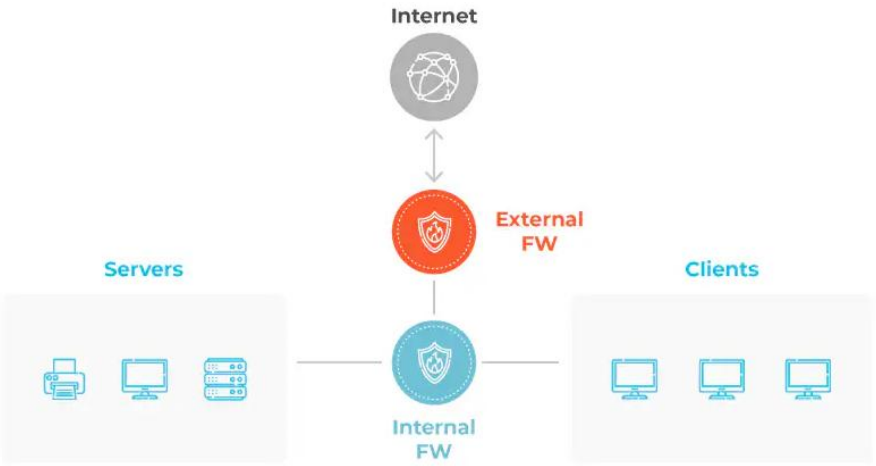

Рисунок 1.5 – Внутрішній брандмауер

Їх основна функція – запобігати поширенню загроз усередині організації. Внутрішні брандмауери часто використовуються для поділу мережі на ізольовані зони, кожна з яких має свої правила доступу та рівень безпеки. Наприклад, вони можуть захищати бази даних від несанкціонованого доступу із загальнодоступних сегментів або обмежувати доступ до критично важливих ресурсів лише для певних відділів. Такий підхід особливо корисний у великих організаціях, де необхідно суворо контролювати взаємодію між різними підрозділами або групами користувачів. Внутрішні брандмауери також допомагають запобігти загрозам, які можуть походити від зкомпрометованих внутрішніх пристроїв.

Розподілений брандмауер – це тип брандмауера, що розгортається у вигляді програмного або віртуального рішення, інтегрованого в кілька частин мережевої інфраструктури (див. рисунок 1.6).

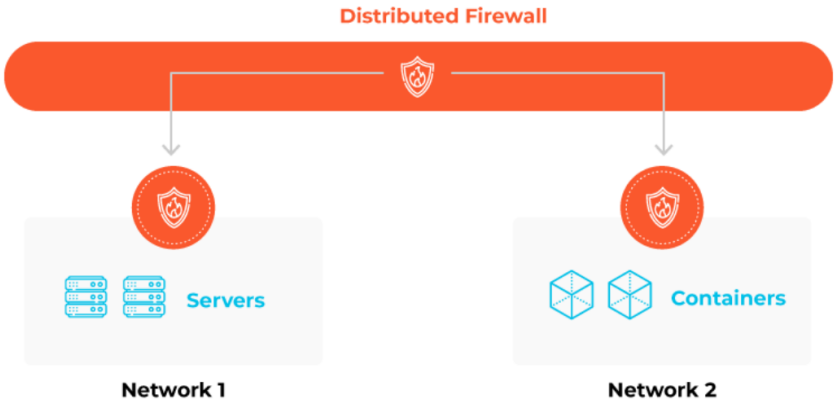

Рисунок 1.6 – Розподілений брандмауер

На відміну від традиційних брандмауерів, які працюють в одній точці, розподілені брандмауери функціонують у вигляді мережі модулів, які взаємодіють між собою, охоплюючи всю інфраструктуру.

Вони забезпечують безпеку як у фізичних мережах, так і в хмарних середовищах, контролюючи трафік на різних рівнях: між віртуальними машинами, контейнерами, мережевими сегментами та кінцевими точками. Такий підхід забезпечує високу масштабованість, дозволяючи адаптуватися до динамічних змін у сучасних інфраструктурах. Розподілені брандмауери ідеально підходять для складних мережевих середовищ, таких як гібридні або мультихмарні архітектури, де контроль і безпека потрібні на кожному етапі руху даних.

Брандмауер периметру встановлюється на межі між внутрішньою мережею організації та зовнішнім середовищем, таким як Інтернет (див. рисунок 1.7).

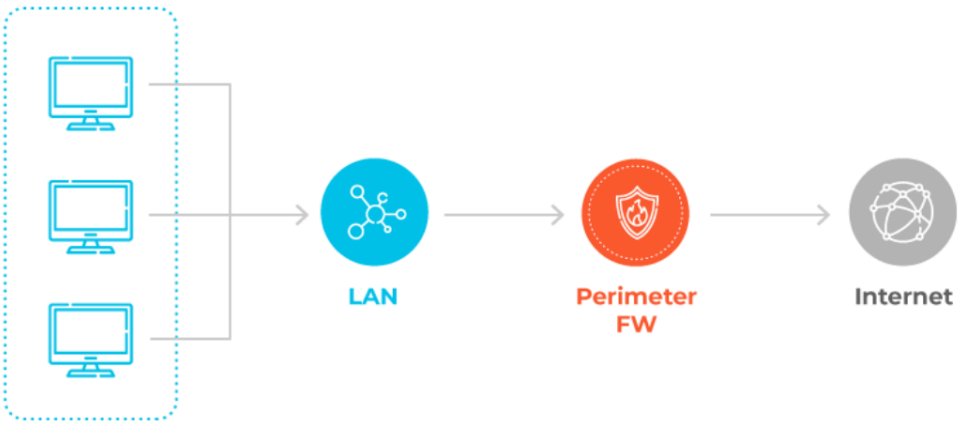

Рисунок 1.7 – Брандмауер периметру

Це перша лінія захисту, яка фільтрує весь вхідний і вихідний трафік, що проходить через мережевий периметр. Основне завдання такого брандмауера – блокувати шкідливі з'єднання, захищати мережу від несанкціонованого доступу та запобігати кіберзагрозам, які можуть надходити ззовні. Брандмауери периметру часто працюють у поєднанні з іншими засобами безпеки, такими як IDS/IPS або антивірусні рішення. Вони можуть виконувати базову фільтрацію пакетів або застосовувати складніші методи, наприклад, глибокий аналіз пакетів і контроль додатків. Периметрові брандмауери є критично важливими для захисту мережі від зовнішніх атак, особливо у випадках, коли організація надає публічний доступ до своїх сервісів.

1.3.4 Класифікація за методом фільтрації даних

Класифікація брандмауерів за методом фільтрації даних базується на різних підходах до аналізу та контролю трафіку, який проходить через мережу. Ці методи визначають, як брандмауери оцінюють, фільтрують і приймають рішення щодо пакетів даних, з'єднань або додатків [6].

Брандмауер фільтрації пакетів є найпростішим і найдавнішим типом брандмауера (див. рисунок 1.8).

Рисунок 1.8 – Брандмауер фільтрації пакетів

Він працює на мережевому рівні, аналізуючи заголовки пакетів даних, зокрема IP-адресу, порт, протокол і напрямок трафіку (вхідний або вихідний). Брандмауер приймає рішення про те, чи пропустити пакет, ґрунтуючись на

встановлених правилах. Наприклад, він може блокувати або дозволяти трафік з певних IP-адрес або портів. Оскільки цей тип брандмауера не аналізує вміст пакетів, він має обмежену здатність до виявлення складних загроз, таких як шкідливі програми, які маскуються під легітимний трафік. Однак завдяки своїй простоті та низьким вимогам до обчислювальних ресурсів брандмауери фільтрації пакетів часто використовуються як базовий рівень захисту.

Брандмауери перевірки стану (stateful inspection) є більш сучасними та складними (див. рисунок 1.9).

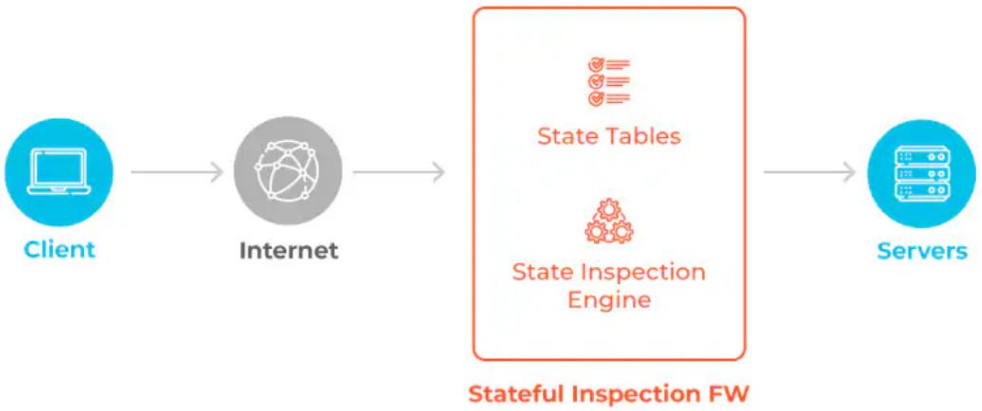

Рисунок 1.9 – Брандмауер перевірки стану

Вони працюють на рівні з’єднань і відстежують стан кожного сеансу зв’язку, включаючи всі пакети, які належать до цього з’єднання. Наприклад, якщо ініціюється з’єднання між клієнтом і сервером, брандмауер реєструє цей сеанс і дозволяє трафік, пов’язаний із ним. Якщо ж пакет не належить до відомого з’єднання, він блокується. Такий підхід дозволяє забезпечити більш точний контроль трафіку та захист від атак, які використовують несанкціоновані пакети. Брандмауери перевірки стану добре підходять для забезпечення базового рівня безпеки в багатьох мережах.

Брандмауери проксі працюють на рівні додатків, виступаючи посередниками між клієнтом і сервером (див. рисунок 1.10).

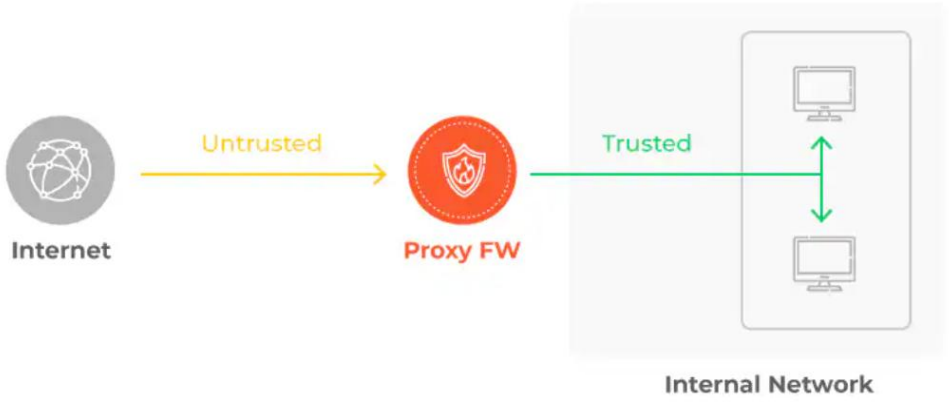

Рисунок 1.10 – Брандмауер проксі

Вони приймають запити від клієнтів, аналізують їх, а потім перенаправляють на сервери, маскуючи клієнта. Аналогічно, вони отримують відповіді від серверів і передають їх клієнту. Завдяки цьому брандмауери проксі здатні аналізувати не лише заголовки пакетів, а й їхній вміст, забезпечуючи високий рівень безпеки. Цей підхід дозволяє виявляти шкідливі додатки або загрози, приховані в даних, і запобігати їх поширенню. Брандмауери проксі ідеально підходять для захисту веб-серверів, систем електронної пошти та інших додатків, але через високі вимоги до ресурсів вони можуть знижувати продуктивність.

Брандмауери веб-додатків (WAF) спеціалізуються на захисті веб-додатків від атак, таких як SQL-ін’єкції, міжсайтовий скриптинг (XSS) і крадіжка сесій. Вони аналізують HTTP/HTTPS-запити та відповіді, застосовуючи правила для виявлення аномальної поведінки або атак (див. рисунок 1.11).

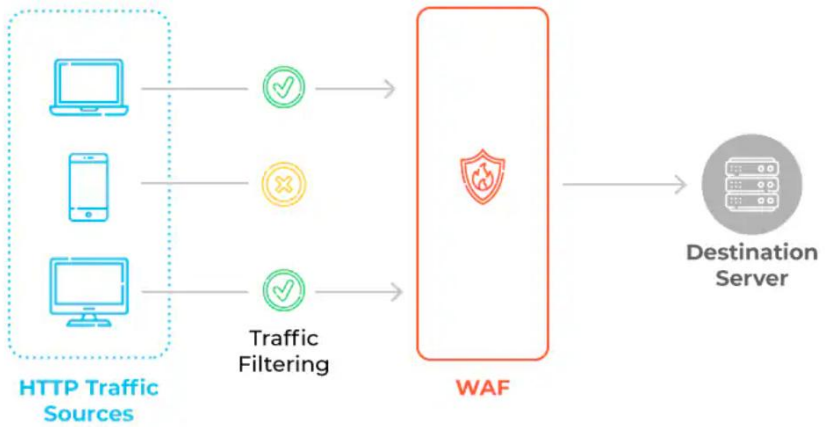

Рисунок 1.11 – Брандмауер веб-додатків

Брандмауери веб-додатків дозволяють захищати специфічні компоненти веб-додатків і забезпечують додатковий рівень безпеки для організацій, які використовують хмарні або веб-орієнтовані інфраструктури. Їх ефективність значною мірою залежить від точності правил та налаштувань.

Шлюз на рівні каналу (circuit-level gateway) працює на транспортному рівні, встановлюючи віртуальні з'єднання між клієнтом і сервером (див. рисунок 1.12).

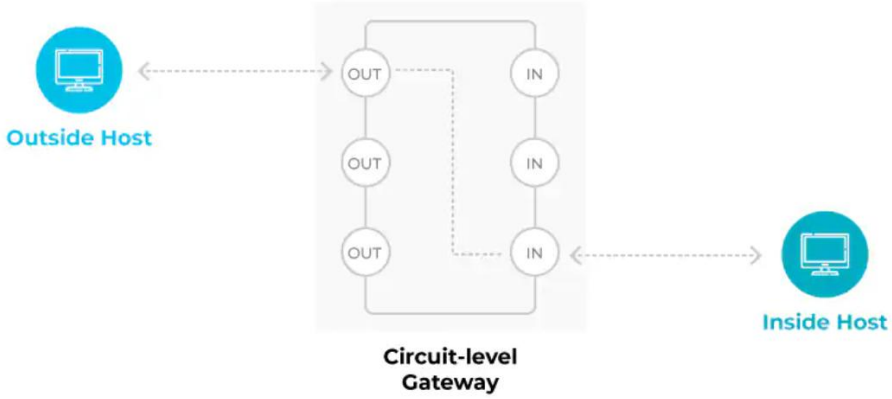

Рисунок 1.12 – Шлюз на рівні каналу

Він перевіряє легітимність TCP/UDP-сесій, але не аналізує вміст пакетів. Шлюзи на рівні каналу забезпечують базовий контроль за з'єднаннями, але мають обмежену здатність виявляти сучасні загрози. Їх часто використовують у поєднанні з іншими типами брандмауерів для створення багаторівневого захисту.

Брандмауери нового покоління представляють найсучасніший тип брандмауерів, який поєднує функціонал традиційних брандмауерів із розширеними можливостями (див. рисунок 1.13).

Рисунок 1.13 – Брандмауери нового покоління (NGFW)

Вони виконують глибокий аналіз пакетів, забезпечують контроль додатків, інтегруються з системами виявлення та запобігання вторгнень, а також дозволяють застосовувати політики безпеки на основі поведінки користувачів. NGFW здатні виявляти та блокувати складні атаки, аналізувати шкідливий трафік і забезпечувати високий рівень захисту як для фізичних, так і для віртуальних мереж. Вони ідеально підходять для захисту сучасних корпоративних інфраструктур, де загрози стають дедалі складнішими.

1.4 Висновки до першого розділу

У першому розділі було проведено огляд предметної області, який включав аналіз причин використання брандмауерів, основних принципів їхньої роботи та їх проектування, а також класифікацію різних типів брандмауерів.

Показано, що основною причиною використання брандмауерів є необхідність забезпечення безпеки мережевих ресурсів, які все більше стають вразливими до кіберзагроз через активний розвиток інформаційних технологій та Інтернету. Брандмауери дозволяють створити бар'єр між внутрішньою мережею та зовнішнім середовищем, забезпечуючи контроль трафіку та запобігаючи несанкціонованому доступу. Описано ключові принципи роботи брандмауерів, включаючи аналіз трафіку, розмежування мережевих зон і застосування різних підходів до фільтрації, таких як "дозволено все, що не заборонено" та "заборонено все, що не дозволено". Підкреслено важливість

обробки трафіку в реальному часі, інтеграції з іншими системами кібербезпеки та створення чіткої політики безпеки.

Розглянуто класифікацію брандмауерів за кількома критеріями, зокрема за системним захистом, форм-фактором, розміщенням у мережевій інфраструктурі та методом фільтрації даних. Проаналізовано функціональні особливості хостових і мережевих брандмауерів, апаратних і програмних рішень. Вивчено специфіку розташування брандмауерів у мережі, зокрема їх використання на рівні периметру, всередині мережі та у розподілених системах. Особливу увагу приділено методам фільтрації даних, які використовують традиційні брандмауери фільтрації пакетів, брандмауери перевірки стану, проксі-брандмауери, брандмауери веб-додатків, шлюзи на рівні каналу та брандмауери нового покоління (NGFW). Висвітлено їхні переваги, обмеження та галузі застосування.

Проведений аналіз підкреслює важливість вибору відповідного типу брандмауера залежно від вимог безпеки, особливостей мережевої інфраструктури та типу загроз. Комплексний підхід із застосуванням різних типів брандмауерів забезпечує багаторівневий захист мережі, мінімізуючи ризики та підвищуючи загальний рівень кібербезпеки.

РОЗДІЛ 2 ОПИС ТА НАЛАШТУВАННЯ КОМПОНЕНТІВ ТЕСТОВОГО СЕРЕДОВИЩА

2.1 Схема тестового середовища

Створення тестового середовища для дослідження використання брандмауера нового покоління для виявлення кіберзагроз є доцільним етапом і має значні переваги, особливо у контексті сучасних вимог до кібербезпеки. Таке середовище дозволяє забезпечити контрольовані умови для аналізу роботи NGFW, тестування його функціональності та оцінки ефективності у реальних сценаріях [7].

Основна доцільність створення тестового середовища полягає в тому, що воно надає можливість відтворювати різні типи кіберзагроз, які можуть бути складними, різноманітними та динамічно змінюватися. У реальних умовах виконання таких експериментів може призвести до порушення роботи мережі або навіть до компрометації даних, тому тестове середовище є безпечним способом випробування функцій NGFW без ризику для продуктивної інфраструктури. Це особливо важливо для організацій, які прагнуть впровадити NGFW, але спершу хочуть переконатися у його здатності виявляти та запобігати реальним загрозам.

Перевагою тестового середовища є його контрольованість, яка дозволяє створювати специфічні сценарії загроз, моделювати різні загроз. Завдяки цьому дослідники можуть вивчати реакцію NGFW на конкретні загрози, його можливості щодо аналізу трафіку, виявлення шкідливих дій, блокування підозрілих з'єднань і генерації відповідних журналів подій. Тестове середовище також дозволяє проводити багатократні тести за змінених умов, що допомагає оцінити стійкість та адаптивність NGFW до нових типів атак. Крім того, створення такого середовища дає змогу проводити навчання персоналу та підготовку до роботи з NGFW. Працівники, які відповідають за безпеку, отримують можливість на практиці ознайомитися з функціями брандмауера, налаштуванням політик безпеки, аналізом журналів та усуненням інцидентів.

Це сприяє підвищенню їхньої кваліфікації, а також зменшує ймовірність помилок у реальних умовах. Тестове середовище дозволяє порівнювати продуктивність і функціональність NGFW з іншими системами безпеки. Наприклад, можна оцінити, наскільки ефективно брандмауер інтегрується з існуючою інфраструктурою, чи забезпечує він потрібний рівень продуктивності при високих навантаженнях, як впливає на швидкість роботи мережі та які додаткові функції (контроль додатків, інтеграція з IDS/IPS) він пропонує порівняно з альтернативами [8] [9]. Ще однією перевагою є можливість налаштування тестового середовища для імітації специфічних умов мережі, які відповідають унікальним потребам організації. Це включає створення різних сегментів мережі, налаштування віртуальних середовищ і розгортання додаткових компонентів, таких як сервери, клієнтські пристрої. Завдяки цьому дослідники можуть отримати реалістичні результати, які максимально відповідають реальним умовам роботи.

На рисунку 2.1 показано тестове середовище для аналізу роботи брандмауера OPNsense із встановленим брандмауером Zenarmor.

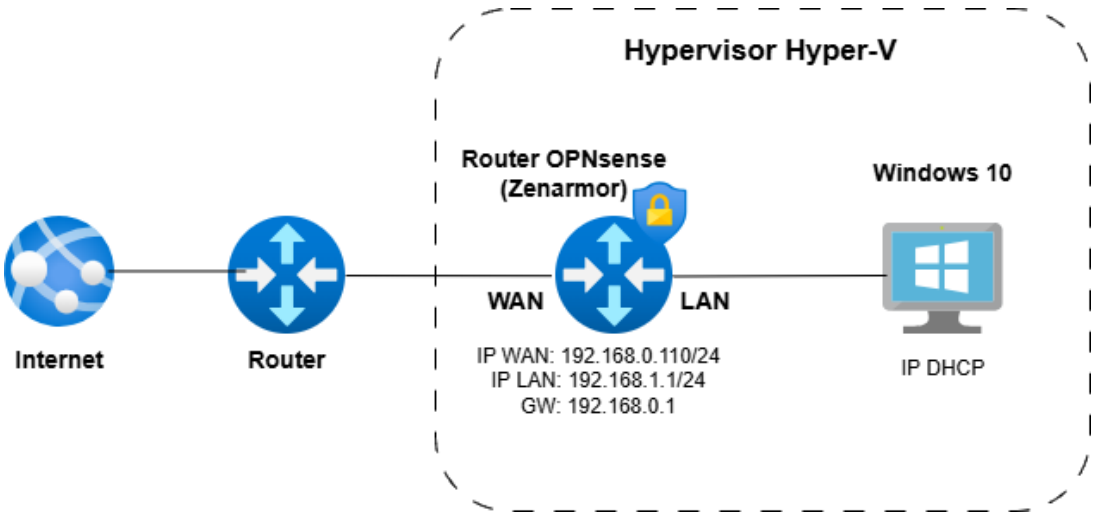

Рисунок 2.1 – Схема тестового середовища

Тестове середовище побудоване з використанням гіпервізора Hyper-V [10]. Гіпервізор використовується як платформа для розгортання віртуальних компонентів мережі. Це забезпечує ізоляцію тестового середовища, дозволяючи

експериментувати з різними сценаріями кіберзагроз, не впливаючи на продуктивну мережу.

З’єднання з Інтернет відбувається через фізичний маршрутизатор. Віртуальна машини, яка виконує функцію маршрутизатора, керованого програмним забезпеченням OPNsense від’єднує елементи тестового середовища до зовнішнього маршрутизатора. Маршрутизатор OPNsense розділяє мережу на дві основні зони: зовнішню (WAN) і внутрішню (LAN). WAN-інтерфейс має IP-адресу 192.168.0.110/24, яка призначена маршрутизатором, що підключений до зовнішньої мережі. Внутрішній інтерфейс (LAN) має адресу 192.168.1.1/24, яка використовується як шлюз для пристроїв у внутрішній мережі.

У внутрішньому сегменті мережі (LAN) знаходиться віртуальна машина з операційною системою Windows 10, яка отримує IP-адресу за допомогою DHCP, налаштованого на OPNsense. Ця конфігурація дозволяє Windows 10 взаємодіяти з внутрішньою мережею, а також використовувати брандмауер OPNsense для маршрутизації трафіку в зовнішню мережу.

OPNsense із модулем Zenarmor забезпечує функції NGFW, включаючи DPI, контроль додатків, блокування шкідливого трафіку та ведення журналів. Zenarmor працює на рівні LAN-інтерфейсу, забезпечуючи моніторинг та контроль внутрішнього трафіку, який проходить між Windows 10 і мережею.

2.2 Гіпервізор Hyper-V

Гіпервізор Hyper-V – це платформа віртуалізації, розроблена корпорацією Microsoft, яка дозволяє створювати та керувати віртуальними машинами на фізичному сервері або комп'ютері [11]. Hyper-V є одним із ключових компонентів інфраструктури Microsoft і інтегрований у серверні операційні системи Windows Server, а також у професійні редакції Windows, починаючи з Windows 8. Основна роль Hyper-V полягає в тому, щоб дозволити запуск кількох віртуальних операційних систем на одній фізичній машині, забезпечуючи при цьому ізоляцію ресурсів і гнучке управління.

Hyper-V працює як гіпервізор типу 1, що означає, що він функціонує безпосередньо на апаратному забезпеченні хоста, замінюючи операційну систему як основний контролер ресурсів [12]. Цей підхід забезпечує високу продуктивність і низьку затримку, що є важливим для корпоративних середовищ, які потребують масштабованості та ефективності. У рамках роботи гіпервізора Hyper-V виступає як посередник між апаратними ресурсами (процесором, пам'яттю, сховищем, мережевими адаптерами) та віртуальними машинами, динамічно розподіляючи їх відповідно до потреб кожної віртуальної системи.

Однією з ключових функцій Hyper-V є підтримка ізоляції віртуальних машин. Це означає, що кожна ВМ працює в окремому віртуальному середовищі, що знижує ризик впливу помилок або атак у одній ВМ на інші. Hyper-V також підтримує функції миттєвого створення знімків (snapshots) стану віртуальних машин, що дозволяє швидко відновлювати їх у разі збою або необхідності повернутися до попередньої конфігурації.

Hyper-V надає можливості управління мережею через віртуальні комутатори (Virtual Switches), які дозволяють створювати різні мережеві топології для віртуальних машин. Це особливо корисно для тестування мережевих сценаріїв, створення ізольованих середовищ і забезпечення багаторівневого захисту мережі. Крім того, Hyper-V підтримує розширені функції віртуалізації, такі як використання віртуальних мережевих адаптерів, VLAN, і маршрутизації трафіку.

Hyper-V також забезпечує високу продуктивність завдяки функціям динамічного розподілу ресурсів, таким як Dynamic Memory, яка дозволяє віртуальним машинам отримувати більше оперативної пам’яті залежно від потреб, або функція Resource Metering, яка дозволяє відстежувати використання ресурсів кожною ВМ. Це дозволяє оптимізувати використання апаратного забезпечення, що є важливим для зниження витрат у корпоративних середовищах.

Завдяки своїй масштабованості та інтеграції з екосистемою Microsoft, Hyper-V використовується для різноманітних завдань, таких як тестування

програмного забезпечення, розгортання серверних додатків, навчання, створення ізольованих середовищ для кібербезпеки та багато іншого.

Розгортання тестового середовища за допомогою Hyper-V у Windows 10 на основі наданої схеми передбачає створення віртуалізованої інфраструктури, яка імітує мережеву взаємодію між компонентами, включаючи брандмауер OPNsense із Zenarmor, операційну систему Windows 10 та інші мережеві елементи. Hyper-V дозволяє створювати віртуальні машини, які функціонують як незалежні пристрої в ізольованому середовищі. У цьому випадку використовується кілька віртуальних мережевих адаптерів для імітації мережевих сегментів WAN та LAN. Завдяки можливості створення віртуальних комутаторів у Hyper-V реалізується зв'язок між WAN і LAN інтерфейсами, а також між віртуальними машинами. Це дозволяє точно відтворити реальні мережеві умови, необхідні для тестування функцій OPNsense і Zenarmor.

На рисунку 2.2 показано консоль Hyper-V Manager, яка є інтерфейсом для управління віртуальними машинами, запущеними на Windows 10.

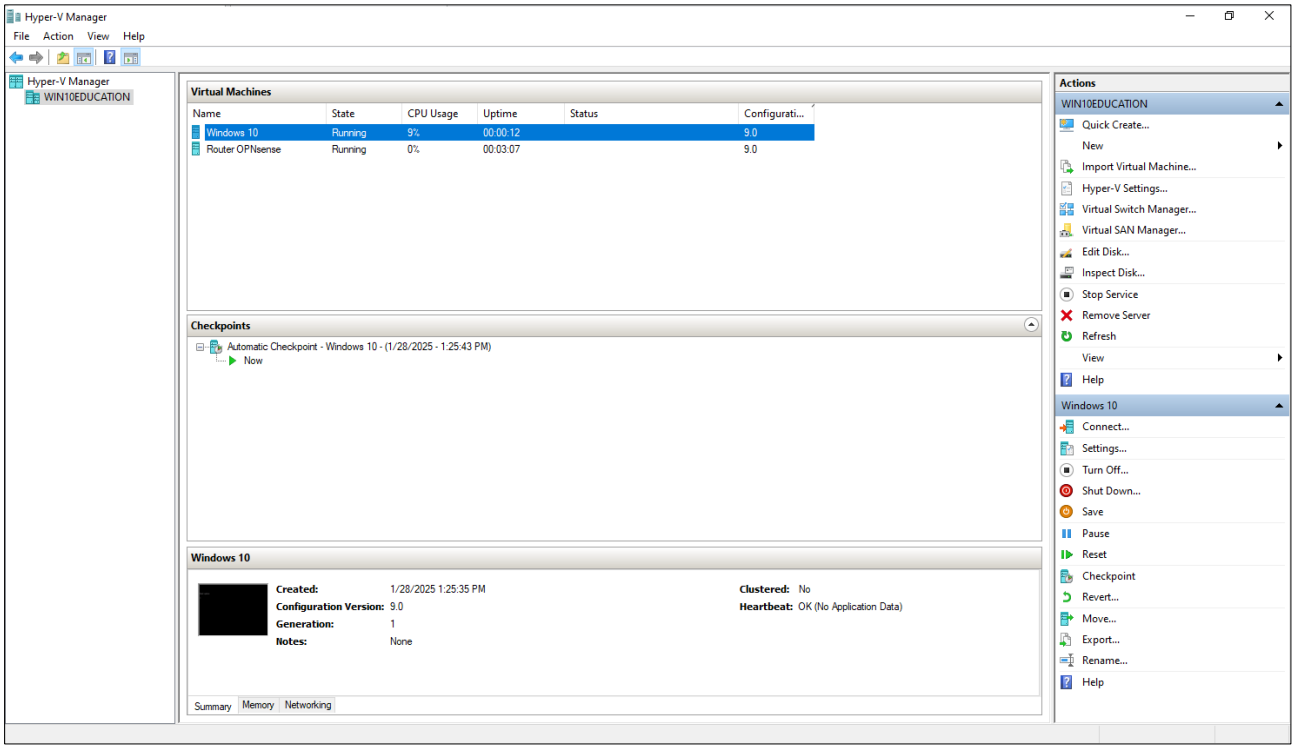

Рисунок 2.2 – Консоль Hyper-V Manager

Консоль відображає інформацію про дві активні віртуальні машини: Windows 10 і Router OPNsense, які є частиною тестового середовища для дослідження функцій брандмауера OPNsense. Віртуальна машина Router OPNsense працює як маршрутизатор і NGFW, використовуючи програмне забезпечення OPNsense із модулем Zenarmor. Віртуальна машина Windows 10 виконує роль клієнтського пристрою в LAN-сегменті мережі. Вона підключена до віртуальної мережі, створеної за допомогою Hyper-V, і взаємодіє з маршрутизатором OPNsense для отримання доступу до Інтернету та інших мережевих ресурсів. Це дозволяє тестувати функціональність брандмауера, включаючи блокування шкідливих з'єднань, контроль додатків і роботу модулів безпеки.

2.3 Брандмауер і платформа маршрутизації OPNsense

OPNsense – це платформа маршрутизації та брандмауер із відкритим вихідним кодом, розроблена для забезпечення надійного захисту мереж [14]. Вона базується на операційній системі FreeBSD і використовує сучасний мережевий стек, що забезпечує високу продуктивність та масштабованість. OPNsense є популярним вибором серед користувачів, які потребують комплексного управління мережевим трафіком, завдяки широким можливостям конфігурації, дружньому веб-інтерфейсу та підтримці розширених функцій безпеки.

Основне призначення OPNsense - забезпечення функцій маршрутизації, брандмауера та VPN. Система дозволяє налаштовувати політики маршрутизації для складних мережевих середовищ, фільтрувати трафік на основі заданих правил і створювати захищені канали зв'язку через віртуальні приватні мережі. Завдяки підтримці динамічної маршрутизації (OSPF, BGP, RIP), OPNsense може легко інтегруватися в корпоративні мережі будь-якого масштабу.

Важливою складовою OPNsense є модуль безпеки. Він включає функції DPI, IDS/IPS, контроль додатків і моніторинг трафіку в реальному часі. Платформа підтримує додаткові плагіни, такі як Zenarmor, які розширюють

можливості системи, додаючи функції аналітики трафіку, категоризації веб-сайтів і блокування загроз на рівні додатків.

Інтерфейс OPNsense розроблений для зручності використання, навіть для користувачів із базовими знаннями мережевих технологій. Веб-інтерфейс надає доступ до всіх функцій через зрозумілу структуру меню, що дозволяє швидко налаштовувати параметри без необхідності використання командного рядка (див. рисунок 2.3).

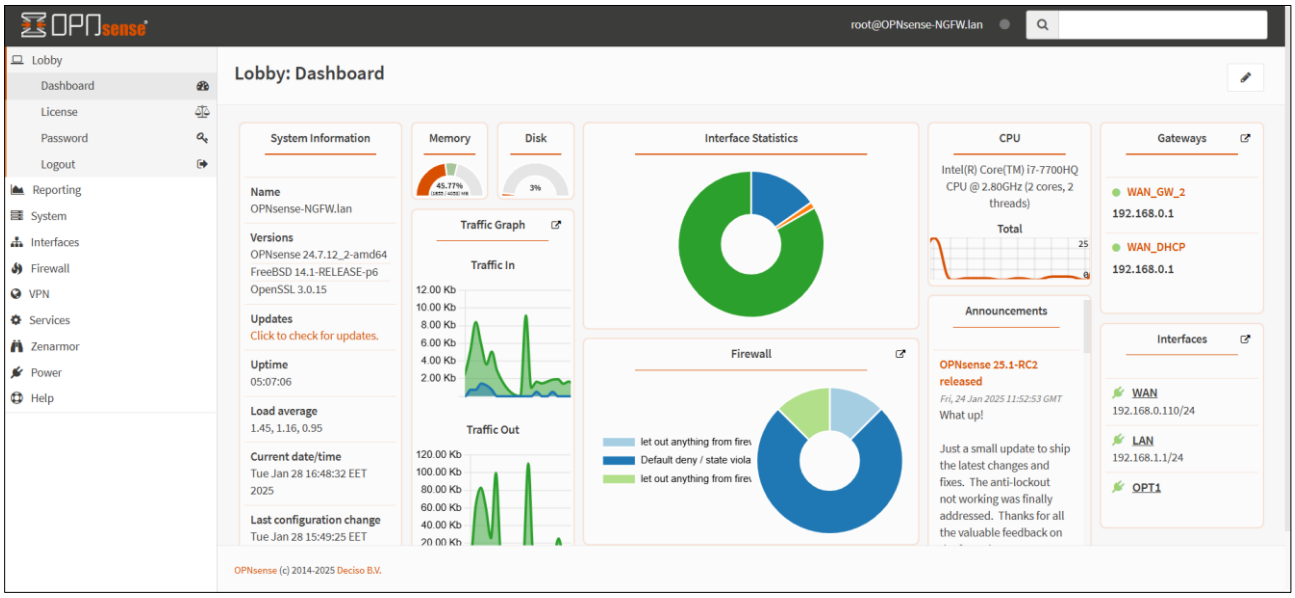

Рисунок 2.3 – Веб-інтерфейсу керування OPNsense

Для адміністраторів доступний широкий спектр інструментів моніторингу та аналізу, включаючи графічне відображення трафіку, журнали подій і сповіщення про підозрілу активність.

OPNsense забезпечує високу гнучкість завдяки своїй модульній архітектурі. Користувачі можуть додавати чи видаляти плагіни залежно від своїх потреб. Це дозволяє використовувати OPNsense як простий маршрутизатор або як потужний NGFW із розширеними функціями. Платформа підтримує широкий спектр апаратних пристроїв, включаючи сервери, міні-ПК і віртуальні машини, що робить її універсальним рішенням для різних типів інфраструктури. Безпека та оновлення є ключовими перевагами OPNsense. Розробники регулярно випускають оновлення, які

включають виправлення вразливостей, нові функції та вдосконалення продуктивності. Це дозволяє підтримувати актуальний рівень захисту мережі та відповідати сучасним викликам у сфері кібербезпеки.

На рисунку 2.4 представлений веб-інтерфейс OPNsense Interfaces: Overview, який надає огляд налаштованих мережевих інтерфейсів.

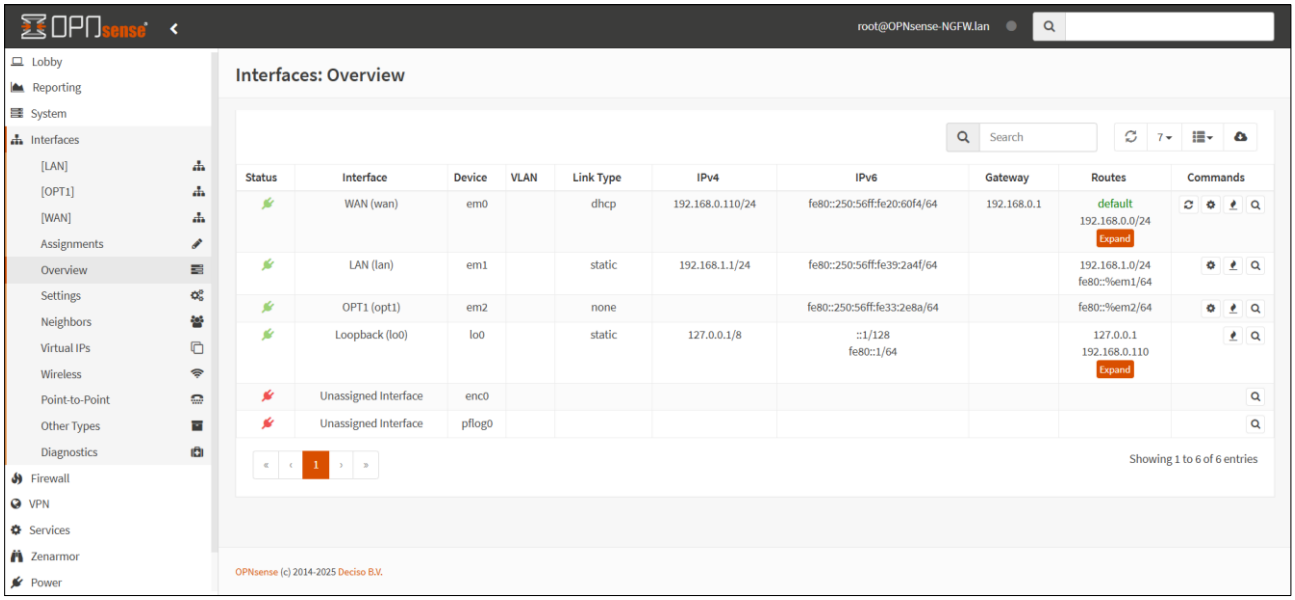

Рисунок 2.4 – Огляд налаштованих мережевих інтерфейсів в OPNsense

Ця сторінка дозволяє адміністратору переглядати поточний стан інтерфейсів, їхні конфігурації та основну інформацію, пов’язану з мережевими підключеннями [14]. На панелі відображено кілька мережевих інтерфейсів із відповідними параметрами, такими як статус, тип інтерфейсу, мережева плата, метод отримання IP-адреси, маршрутизація та шлюз. WAN - це зовнішній інтерфейс, який підключений до Інтернету. Його статус активний, а IP-адреса (192.168.0.110/24) отримана за допомогою DHCP. Для WAN-інтерфейсу шлюзом виступає IP 192.168.0.1, що вказує на доступ до зовнішньої мережі через маршрутизатор. LAN - це внутрішній інтерфейс, призначений для локальної мережі. Він має статичну IP-адресу 192.168.1.1/24, яка виступає шлюзом для пристроїв, підключених до цього сегмента мережі. Інтерфейс також активний.

На рисунку 2.5 представлений розділ Firewall: NAT Outbound у веб-інтерфейсі OPNsense, який відповідає за налаштування NAT.

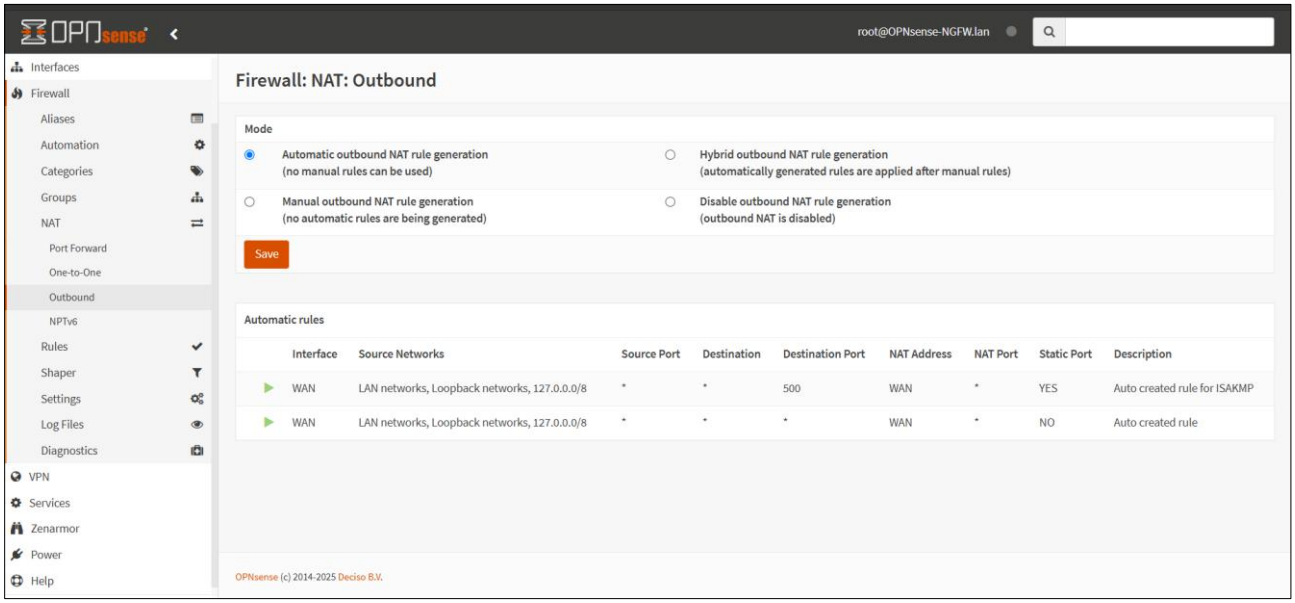

Рисунок 2.5 – Налаштування NAT в OPNsense

NAT є важливою функцією брандмауера, яка дозволяє внутрішнім пристроям у локальній мережі отримувати доступ до зовнішньої мережі Інтернету за допомогою трансляції їхніх приватних IP-адрес у публічну IP-адресу, призначену зовнішньому інтерфейсу WAN [15].

Вибраний у конфігурації Automatic outbound NAT rule generation – це автоматична генерація правил NAT. У цьому режимі OPNsense створює стандартні правила NAT для всіх вихідних підключень, що спрощує налаштування, оскільки немає необхідності вручну задавати правила. Цей режим зручний для типових конфігурацій мережі.

На рисунку 2.6 показано розділ Firewall: Rules - WAN у веб-інтерфейсі OPNsense, який відображає набір правил, застосованих до WAN-інтерфейсу брандмауера.

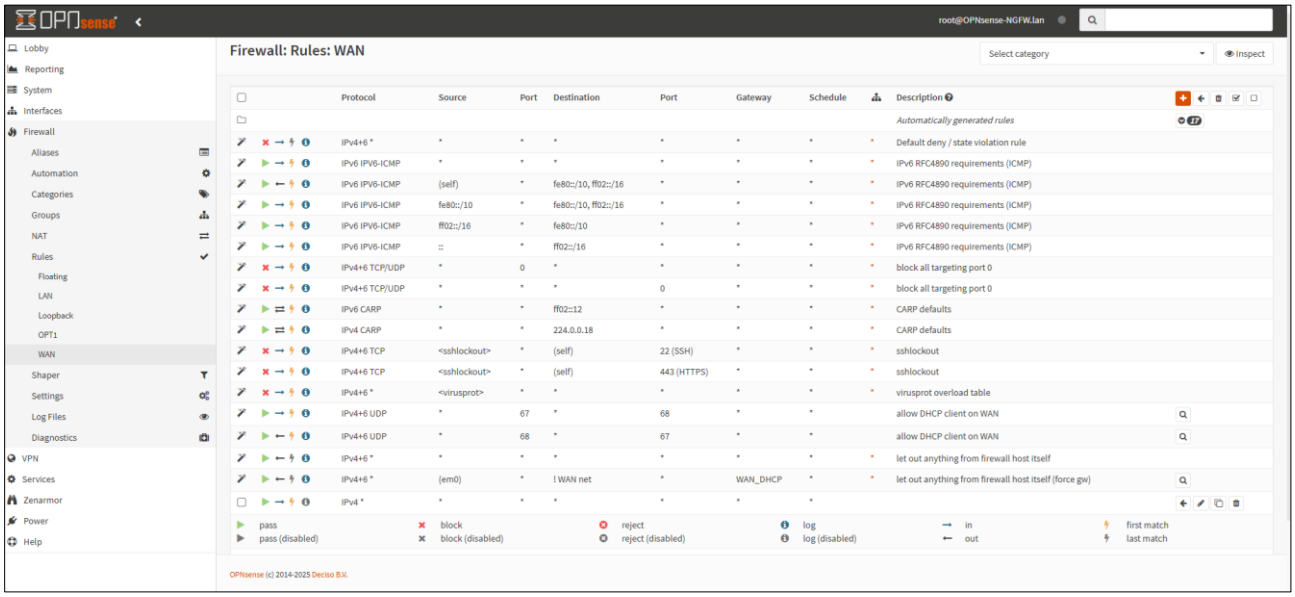

Рисунок 2.6 – Набір правил брандмауера для WAN-інтерфейсу в OPNsense

Ці правила визначають, як обробляється вхідний і вихідний трафік через WAN-інтерфейс, забезпечуючи контроль безпеки та управління мережею.

Деякі правила автоматично згенеровані системою, наприклад, для забезпечення відповідності стандартам IPv6 (RFC4890) або для роботи DHCP-клієнтів на WAN-інтерфейсі. Інші правила створені вручну для специфічних завдань, таких як доступ до SSH або HTTPS. Таблиця організована за принципом пріоритету: порядок розташування правил важливий, оскільки обробка трафіку виконується зверху вниз. Перше правило, яке відповідає параметрам трафіку, буде застосоване. Це означає, що адміністратор має ретельно планувати розташування правил, щоб уникнути конфліктів або небажаних дій.

На рисунку 2.7 представлено розділ Firewall: Rules - LAN у веб-інтерфейсі OPNsense, який відображає набір правил брандмауера, що застосовуються до LAN-інтерфейсу.

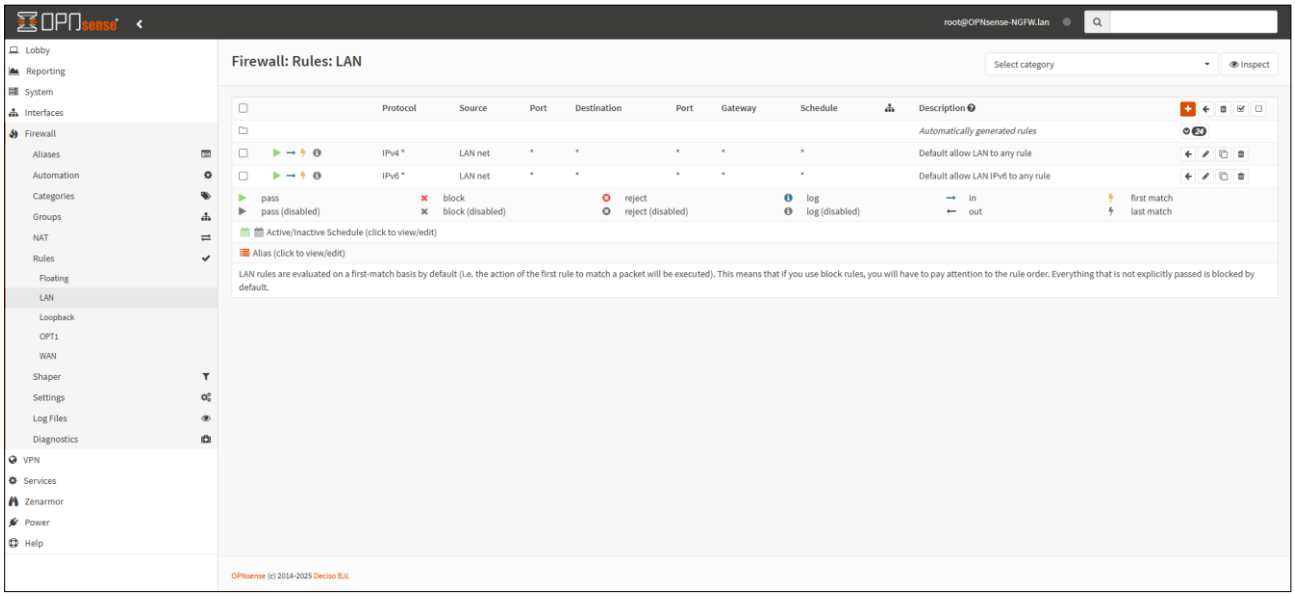

Рисунок 2.7 – Набір правил брандмауера для LAN-інтерфейсу в OPNsense

Цей розділ визначає, як обробляється трафік, що виходить з внутрішньої мережі [16].

Перше правило в таблиці дозволяє весь вихідний трафік з LAN-мережі до будь-якого пункту призначення за протоколом IPv4. Друге правило аналогічне, але застосовується до протоколу IPv6.

LAN-інтерфейс зазвичай налаштовується таким чином, щоб дозволяти всі вихідні з'єднання, водночас блокуючи небажаний вхідний трафік. Це забезпечує захист внутрішньої мережі, дозволяючи пристроям у LAN отримувати доступ до Інтернету або інших мережевих ресурсів, але не дозволяючи зовнішньому трафіку ініціювати з'єднання з пристроями в LAN.

На рисунку 2.8 показано розділ Services: Unbound DNS: General у веб-інтерфейсі OPNsense, який дозволяє налаштовувати DNS-сервер Unbound.

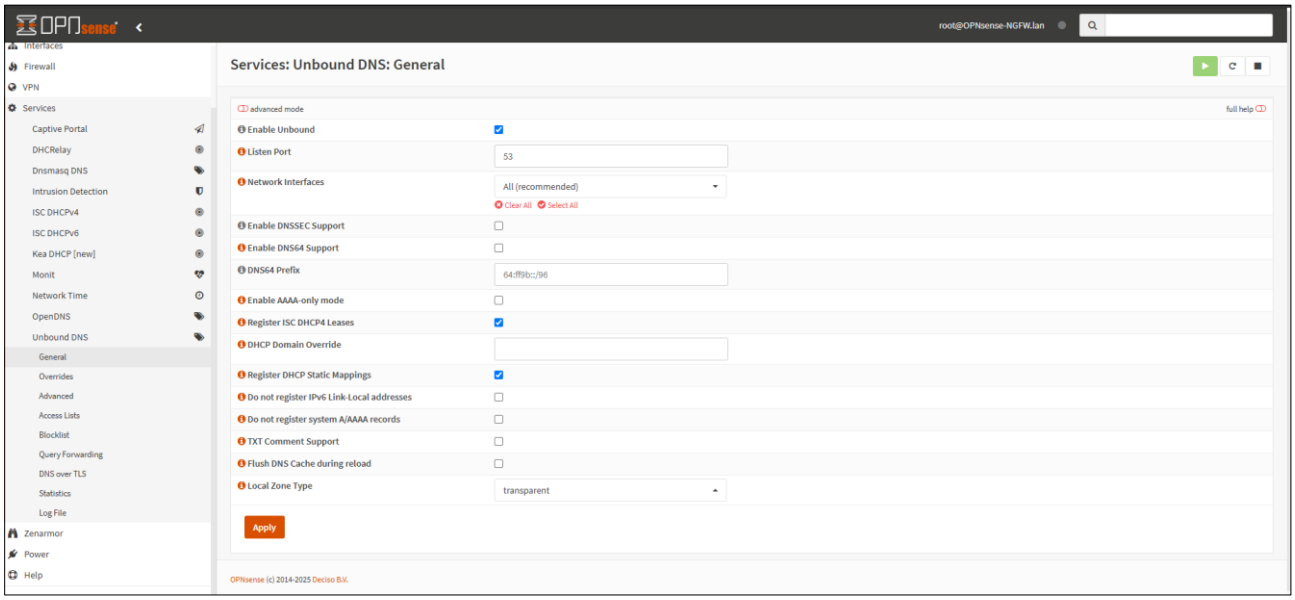

Рисунок 2.8 – Налаштування DNS-сервер Unbound в OPNsense

Unbound – це рекурсивний DNS-сервер із підтримкою кешування, який забезпечує обробку DNS-запитів для клієнтів локальної мережі [17].

Register DHCP Leases – ця опція увімкнена, що дозволяє автоматично реєструвати динамічні IP-адреси, призначені через DHCP, у локальному DNS. Це зручно для управління мережевими клієнтами, дозволяючи швидко знаходити їх за іменем. Register DHCP Static Mappings – також активована. Ця функція додає статично призначені IP-адреси з DHCP до локального DNS.

На рисунку 2.9 представлений розділ Services: ISC DHCPv4 [LAN] у веб-інтерфейсі OPNsense, який відповідає за налаштування DHCP-сервера для LAN-інтерфейсу.

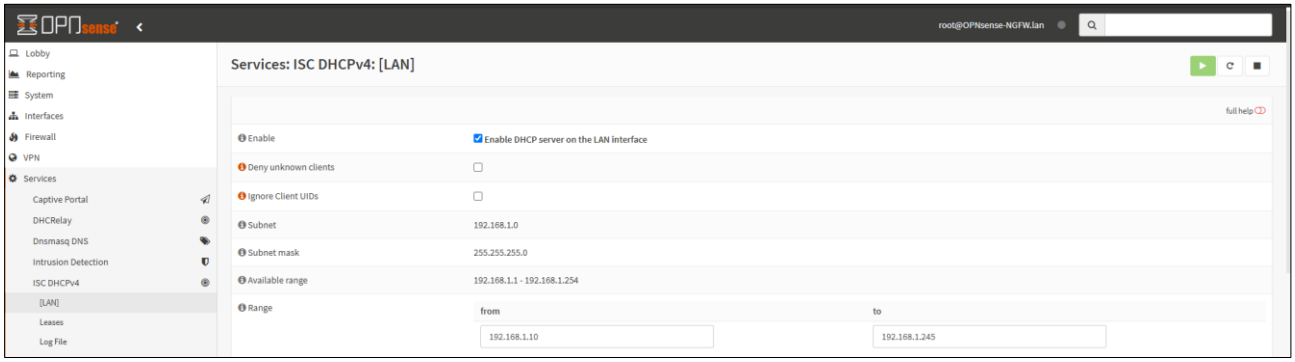

Рисунок 2.9 – Налаштування DHCP-сервера в OPNsense

DHCP (Dynamic Host Configuration Protocol) – це протокол, який автоматично призначає IP-адреси клієнтським пристроям у локальній мережі, а також надає їм додаткові мережеві параметри, такі як шлюз, маска підмережі та DNS-сервери [18]. Available range - це діапазон доступних IP-адрес, які DHCP-сервер може призначати клієнтам, визначений як 192.168.1.10–192.168.1.245. Це залишає деякі адреси поза діапазоном (наприклад, 192.168.1.1, що використовується як шлюз, або адреси, які можуть бути зарезервовані для статичного призначення).

Ця конфігурація дозволяє автоматично видавати налаштування мережі для клієнтськими пристроями у LAN-сегменті, що спрощує адміністрування мережі. Завдяки налаштованому діапазону IP-адрес адміністратор може резервувати певні адреси для статичного призначення (наприклад, для серверів). Використання DHCP значно підвищує зручність і ефективність управління мережею, забезпечуючи автоматичне конфігурування пристроїв і мінімізацію ручного втручання.

2.4 Брандмауер нового покоління Zenarmor

Брандмауер нового покоління Zenarmor – це програмно-визначене рішення для забезпечення кібербезпеки, яке працює як додатковий модуль для платформ на базі FreeBSD, таких як OPNsense [19] (див. рисунок 2.10).

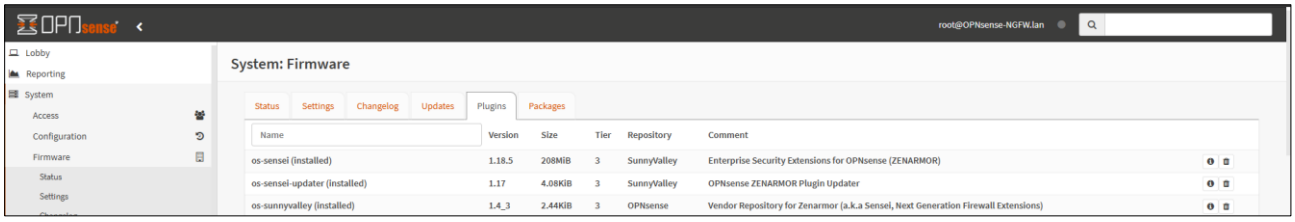

Рисунок 2.10 – Модулі Zenarmor в OPNsense

Його основна мета забезпечення глибокого аналізу мережевого трафіку та захисту мережевих середовищ від сучасних кіберзагроз, одночасно забезпечуючи простоту управління та високу продуктивність. Zenarmor є

безагентним брандмауером, що означає, що для його роботи не потрібно встановлювати додаткове програмне забезпечення на кінцевих пристроях. Він працює безпосередньо на мережевому рівні, інтегруючись із мережевими інтерфейсами системи. Це дозволяє Zenarmor здійснювати контроль за трафіком і виявляти потенційні загрози в реальному часі, аналізуючи пакети даних за допомогою DPI. Завдяки DPI Zenarmor здатний розпізнавати конкретні програми, протоколи та веб-ресурси, що забезпечує високий рівень контролю над використанням мережевих ресурсів.

Цей брандмауер підтримує класифікацію та контроль додатків, що дозволяє визначати, які програми чи сервіси можуть отримувати доступ до мережі. Наприклад, Zenarmor може блокувати небажані соціальні мережі, потокові платформи або інші ресурси, які не відповідають політикам безпеки організації. Крім того, він пропонує функціональність веб-фільтрації, яка дозволяє адміністратору обмежувати доступ до певних веб-сайтів або категорій сайтів (наприклад, фішингові ресурси чи сайти з потенційно небезпечним вмістом).

Однією з ключових переваг Zenarmor є його здатність інтегрувати сучасні механізми запобігання загрозам (Threat Prevention), які включають блокування відомих атак, зловмисного програмного забезпечення та виявлення шкідливої активності. Це забезпечується завдяки базам даних загроз, які постійно оновлюються. Zenarmor також має можливість виявляти поведінкові аномалії в мережевому трафіку, що допомагає ідентифікувати нові, раніше невідомі загрози.

Архітектура Zenarmor побудована таким чином, щоб мінімізувати вплив на продуктивність мережі. Завдяки оптимізованим алгоритмам обробки даних і використанню багатоядерних процесорів Zenarmor забезпечує високу швидкість обробки трафіку навіть у великих мережах з інтенсивним навантаженням. Крім того, він підтримує масштабованість, що робить його придатним як для малих офісів, так і для великих корпоративних мереж.

Zenarmor надає зручний інтерфейс для управління, який дозволяє адміністратору легко налаштовувати правила безпеки, переглядати детальні звіти про мережеву активність і аналізувати журнали подій (див. рисунок 2.11).

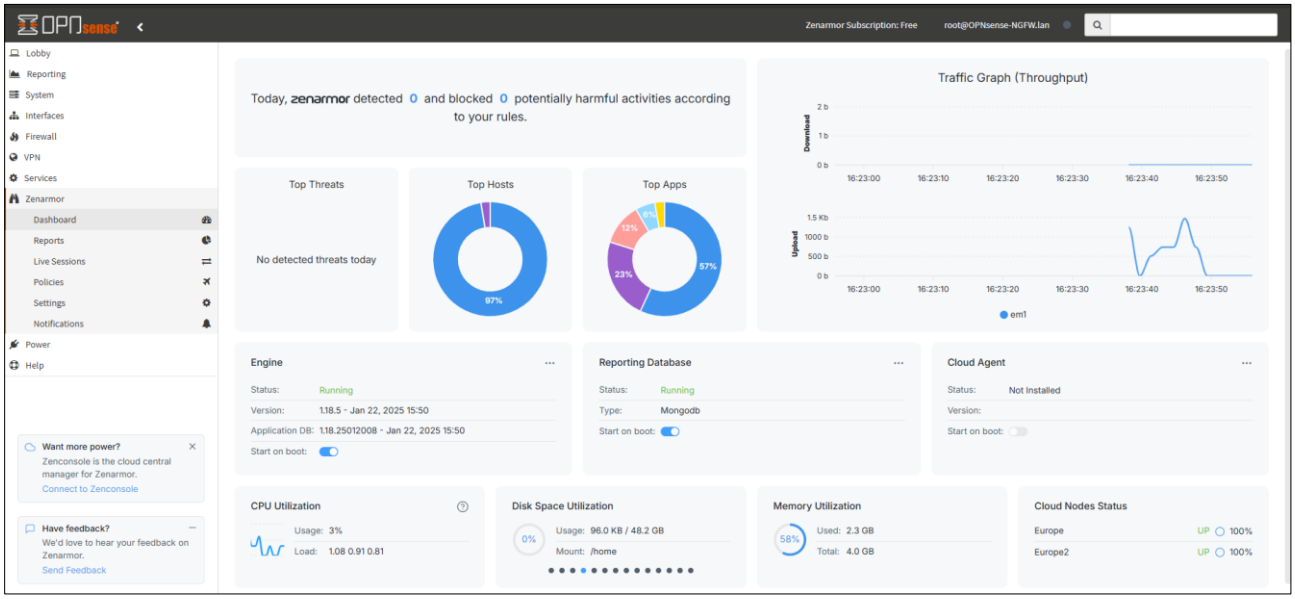

Рисунок 2.11 – Інформаційна панель Zenarmor в OPNsense

Інструменти аналітики забезпечують прозорість роботи мережі, дозволяючи швидко виявляти потенційні проблеми та усувати їх. Цей брандмауер також підтримує інтеграцію з хмарними сервісами, що розширює його можливості в області централізованого управління безпекою. Це дозволяє використовувати Zenarmor у розподілених мережах або гібридних інфраструктурах, де частина ресурсів знаходиться в хмарі.

2.5 Висновки до другого розділу

В другому розділі було описано ключові моменти створення та налаштування тестового середовища для дослідження функціональних можливостей брандмауера нового покоління Zenarmor, інтегрованого в платформу OPNsense.

Було детально описано архітектуру тестового середовища, яке побудоване на основі гіпервізора Hyper-V. Ця платформа забезпечує ізоляцію компонентів тестового середовища та дозволяє моделювати складні мережеві сценарії для аналізу роботи NGFW. Налаштування віртуальних мережевих адаптерів, зон

WAN і LAN, а також маршрутизації забезпечило реалістичне середовище для оцінки продуктивності та функціональності OPNsense із модулем Zenarmor. Особливу увагу було приділено детальному аналізу компонентів брандмауера OPNsense, таких як NAT, правила фільтрації трафіку для WAN та LAN-інтерфейсів, а також налаштування сервісів DHCP та DNS. Це дозволило створити гнучку та контрольовану інфраструктуру, яка забезпечує правильне функціонування мережі та дозволяє досліджувати поведінку мережевих пристроїв у різних умовах. Zenarmor був розглянутий як ключовий компонент тестового середовища, який забезпечує розширені можливості нового покоління брандмауерів, зокрема DPI, класифікацію додатків, блокування шкідливого трафіку та запобігання сучасним загрозам.

У підсумку, результати створення та налаштування тестового середовища підтвердили його доцільність для проведення досліджень у галузі кібербезпеки. Таке середовище дозволяє безпечно тестувати різні сценарії кіберзагроз, оцінювати ефективність функціональності брандмауера та його можливості інтеграції з іншими мережевими сервісами.

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ NGFW ZENARMOR

3.1 Налаштування Zenarmor

Налаштування Zenarmor є важливим етапом для інтеграції функціональності NGFW в інфраструктуру, яка використовує платформу OPNsense. Zenarmor додає можливості DPI, моніторингу мережевого трафіку, контролю додатків і забезпечення безпеки на рівні додатків.

Першим етапом налаштування є активація Zenarmor і вибір мережевих інтерфейсів, до яких застосовуватимуться політики безпеки (див. рисунок 3.1).

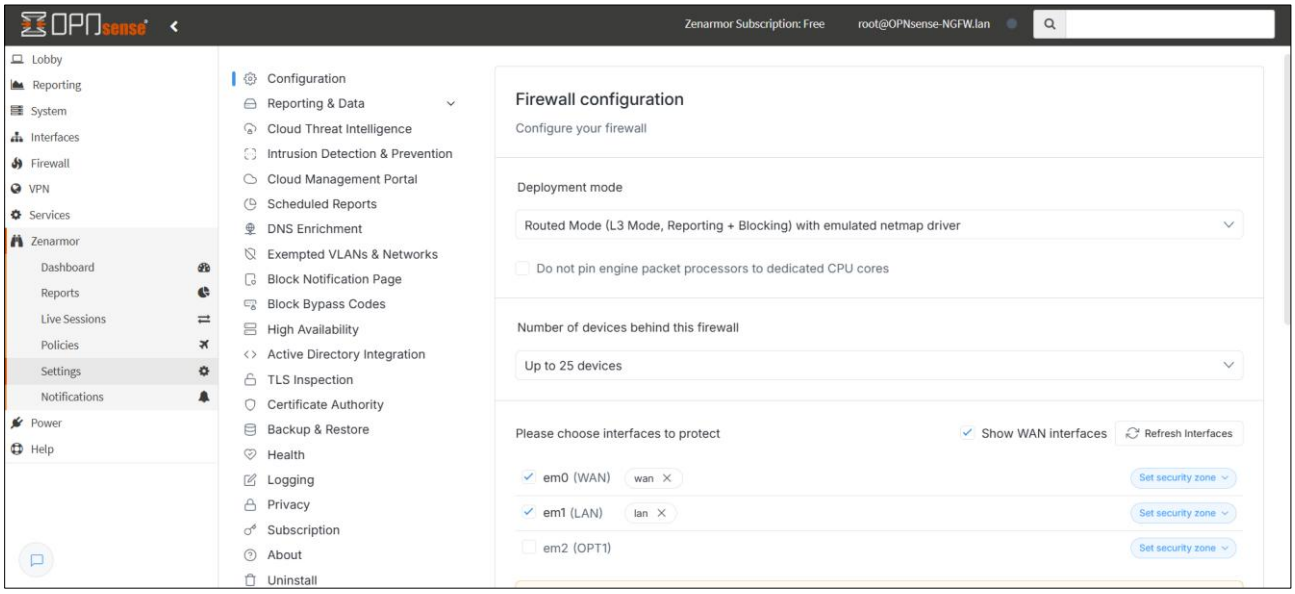

Рисунок 3.1 – Базові налаштування Zenarmor

Параметр Deployment mode визначає спосіб інтеграції Zenarmor з мережею. У цьому випадку обрано режим Routed Mode (L3 Mode, Reporting + Blocking) with emulated netmap driver. Це означає, що Zenarmor функціонує в режимі маршрутизації на рівні L3 (мережевого рівня), забезпечуючи як моніторинг трафіку, так і блокування небажаних з'єднань. Використання емуляції драйвера netmap дозволяє забезпечити підтримку сучасних функцій безпеки на платформах, які не мають апаратного прискорення. У розділі вибору інтерфейсів відображаються інтерфейси, які будуть захищені брандмауером. Тут вказано два інтерфейси: em0 (WAN) та em1 (LAN).

На рисунку 3.2 представлено розділ Cloud Threat Intelligence у налаштуваннях Zenarmor.

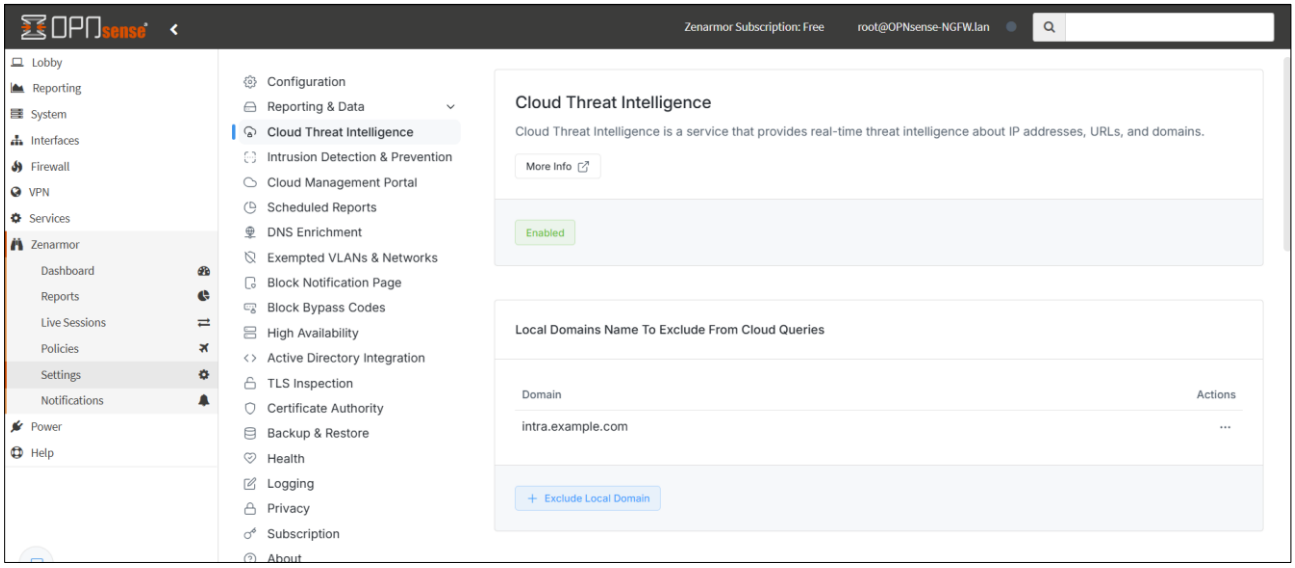

Рисунок 3.2 – Cloud Threat Intelligence в Zenarmor

Цей розділ відповідає за управління сервісом хмарної розвідки загроз, що надає актуальну інформацію про IP-адреси, URL-адреси та домени, пов’язані із загрозами.

Сервіс Cloud Threat Intelligence працює у реальному часі, забезпечуючи оновлені дані про потенційно небезпечні ресурси в Інтернеті. Це дозволяє брандмауеру швидко ідентифікувати шкідливий трафік та вживати відповідних заходів для його блокування, знижуючи ризики для мережі.

Хмарна репутація та аналіз загроз є ключовими компонентами функціональності брандмауера нового покоління Zenarmor, що забезпечується за допомогою інтегрованої системи розвідки хмарних загроз Sunny Valley Network (Zenarmor Cloud). Ця система пропонує потужний набір інструментів для виявлення та запобігання кіберзагрозам у реальному часі, що базуються на розширеній базі даних репутації веб-сайтів, доменів і IP-адрес. Zenarmor Cloud щоденно обробляє мільйони запитів, працюючи на основі бази даних, яка включає інформацію про понад 300 мільйонів веб-сайтів. Це дозволяє швидко реагувати на загрози, включаючи атаки шкідливого програмного забезпечення, фішинг та інші типи загроз у режимі реального часу. Окрім цього, платформа

забезпечує класифікацію веб-сайтів, аналіз їх репутації та рейтингування для подальшого використання з функціями, такими як чорний і білий списки для перевірки TLS.

Zenarmor Cloud здійснює аналіз у реальному часі, коли виявляє пристрої, які намагаються встановити з'єднання у мережі, що захищається. Після отримання запиту система надсилає потік даних до найближчого сервера хмари, де він аналізується на основі політик безпеки і наданої хмарною базою даних інформації. Для забезпечення безпеки зв’язку між Zenarmor і хмарними серверами використовується зашифрований протокол на основі AES-256, який працює через UDP-порти 5353, 5355 і 3478.

Розвідка хмарних загроз Zenarmor Cloud базується на кількох джерелах даних, включаючи інструменти Zenarmor для аналізу загроз, комерційні бази даних, SOC Zenarmor, відгуки партнерів і користувачів. Це дозволяє системі бути ефективною, гнучкою та надійною, забезпечуючи якісну класифікацію трафіку та виявлення загроз. Конфіденційність і безпека хмарних запитів є пріоритетом Zenarmor. Усі дані запитів обробляються анонімно, не зберігаються довше 7 днів і очищуються одразу після обробки. Політика обробки даних відповідає GDPR та закону Каліфорнії про конфіденційність споживачів.

Хмарна інфраструктура Zenarmor побудована на базі Google Cloud, що забезпечує надійність, безпеку та масштабованість сервісу. Це дозволяє платформі забезпечувати стабільний доступ до хмарної інфраструктури навіть за умов інтенсивного навантаження, надаючи користувачам високий рівень довіри до системи.

Хмарна розвідка загроз Zenarmor є одним із найбільш просунутих рішень для забезпечення мережевої безпеки. Вона поєднує в собі штучний інтелект, сучасні методи аналізу трафіку, гнучкість налаштувань і надійність для запобігання сучасним кіберзагрозам [20] [21].

Портал керування через хмару – це інструмент, що дозволяє адмініструвати пристрої з інтегрованим брандмауером Zenarmor через хмарну платформу Zenconsole https://dash.zenarmor.com/ [22] (див. рисунок 3.3).

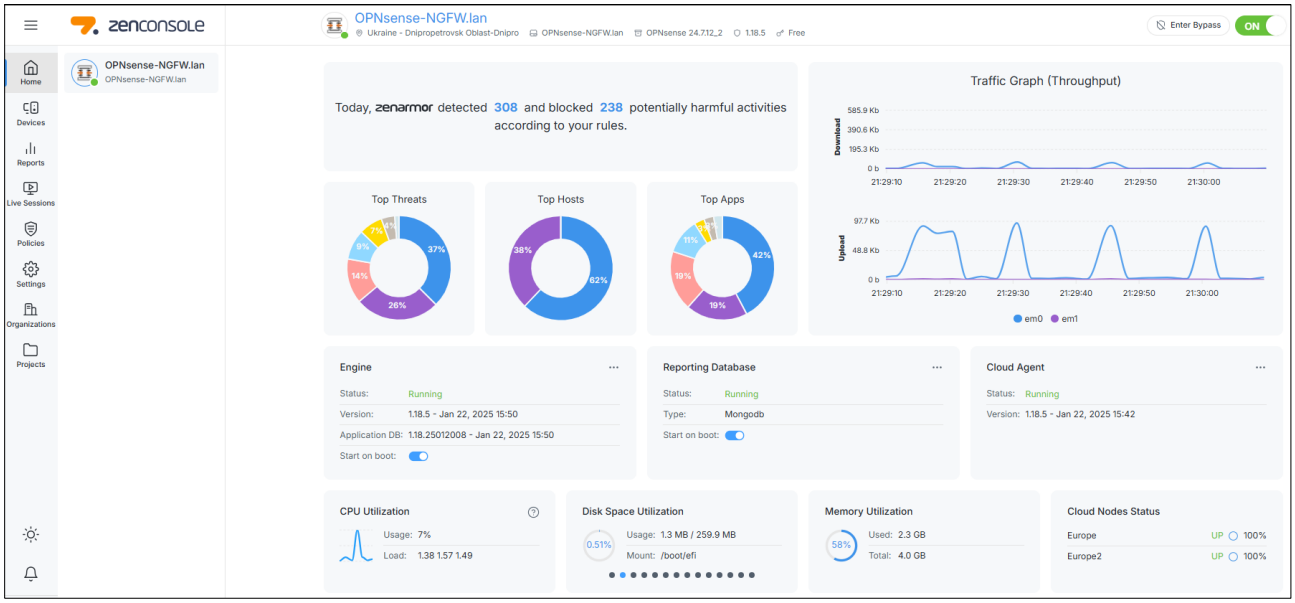

Рисунок 3.3 – Портал керування Zenarmor через хмару

Він забезпечує доступ до функцій управління та моніторингу брандмауерів, незалежно від фізичного місцезнаходження адміністратора. Це робить керування мережевою безпекою більш зручним та ефективним. Zenconsole надає централізоване хмарне середовище для управління мережею. Через цей портал адміністратори можуть легко отримувати доступ до даних і функцій, таких як управління політиками безпеки, моніторинг активності, інтеграція з хмарною розвідкою загроз та інші інструменти для забезпечення комплексної безпеки мережі.Це рисунку 3.4 відображено розділ Policies у веб-інтерфейсі Zenarmor, який використовується для налаштування політик безпеки.

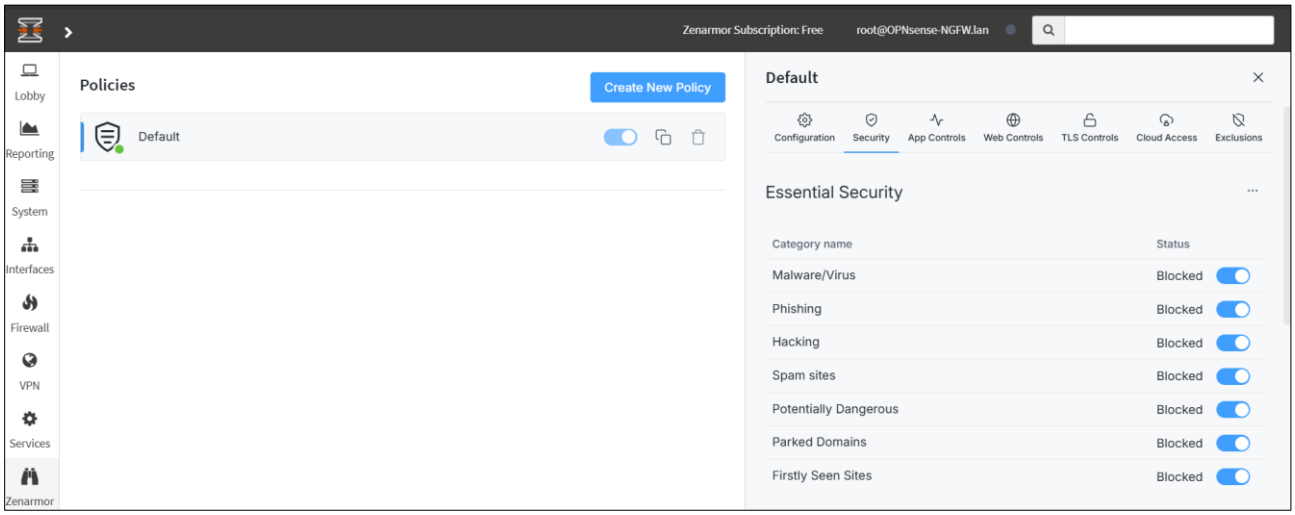

Рисунок 3.4 – Налаштування політик безпеки в Zenarmor

У цьому розділі адміністраторам надається можливість створювати, змінювати та керувати політиками, що визначають, як брандмауер обробляє певні категорії мережевого трафіку.

Використовуючи дані з об’єднаних джерел, Zenarmor блокує доступ до сайтів, які містять зловмисне програмне забезпечення, сприяють фішинговим кампаніям або поширюють небажаний контент. Блокування також застосовується до хакерських сайтів, які розповсюджують інструменти та знання для здійснення атак, а також до сайтів, які класифікуються як потенційно небезпечні чи запарковані домени. Zenarmor також підтримує функцію Firstly Seen Sites. Це дозволяє запобігати доступу до нових або невідомих веб-ресурсів, поки вони не будуть класифіковані системою. Якщо веб-сайт ще не класифіковано, його негайно ставлять у чергу для обробки системою класифікації на основі штучного інтелекту. Класифікований ресурс додається до бази даних із відповідною категорією, яка потім поширюється в системі. Особливу увагу приділено протидії DNS через HTTPS (DoH). Zenarmor відстежує та блокує всі спроби використання DoH для обходу традиційних засобів захисту, запобігаючи приховуванню дій зловмисників. Це забезпечує повний контроль над DNS-запитами у мережі.

Контроль програм у Zenarmor дозволяє забезпечити гнучке управління доступом до додатків і мережевого трафіку на основі детальної класифікації програм. Ця функція базується на використанні бази даних App DB, яка містить динамічні сигнатури для точного визначення та класифікації трафіку, що

генерується конкретними програмами. Zenarmor дозволяє адміністратору налаштовувати правила безпеки для політики контролю додатків через веб-інтерфейс OPNsense.

На вкладці App Controls політики адміністратор може переглядати список категорій додатків (див. рисунок 3.5). Кожна категорія має перемикач, який дозволяє дозволити або заблокувати весь тип додатків. У разі вибору окремих програм із певної категорії, система дозволяє деталізувати налаштування, дозволяючи чи забороняючи окремі підкатегорії або додатки.

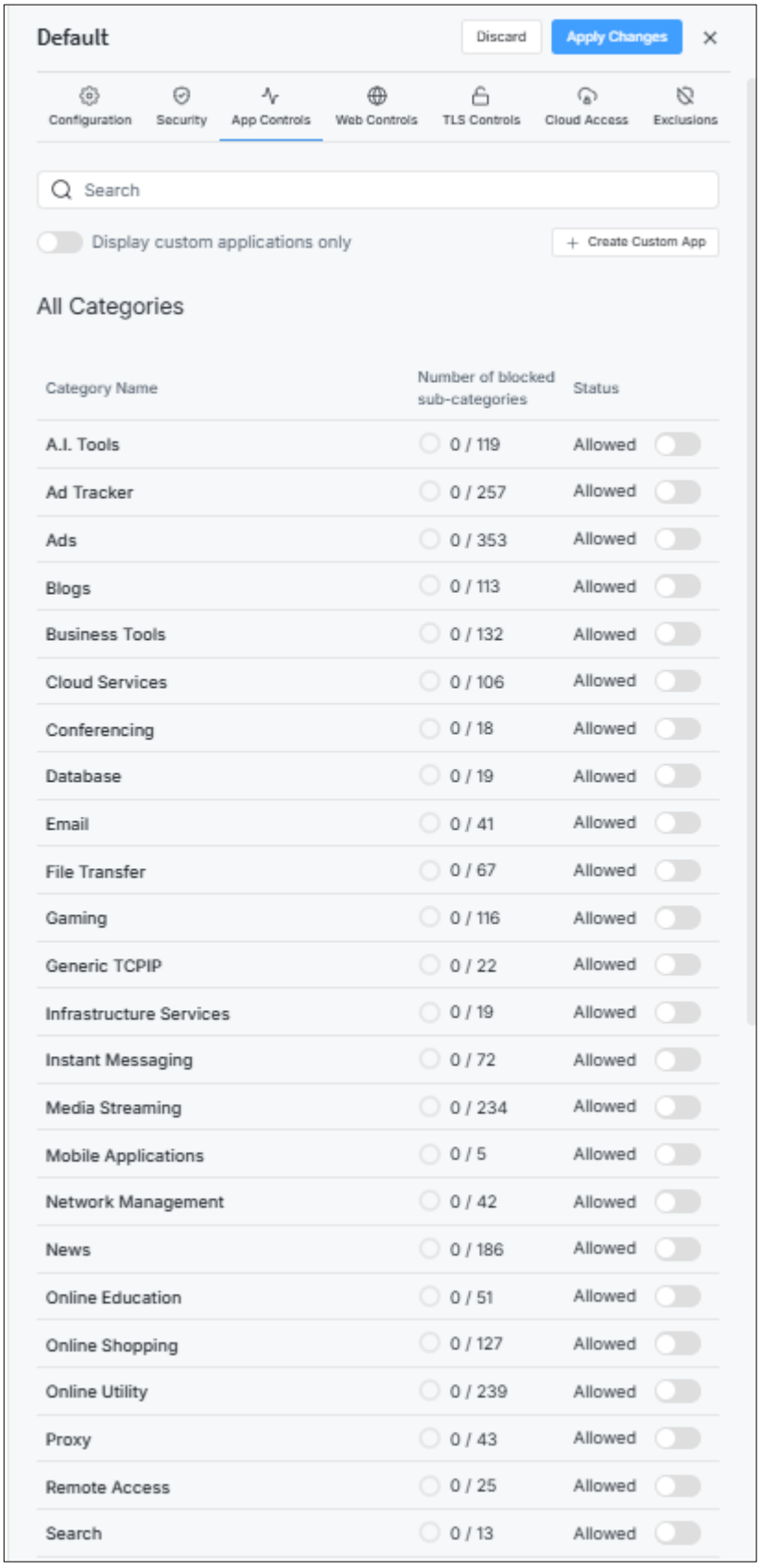

Рисунок 3.5 – Контроль програм в Zenarmor

Zenarmor підтримує функцію створення спеціальних додатків, які можуть не бути включені до стандартної бази даних.

3.2 Тестування Zenarmor

Для тестування налаштувань, виконаних у вкладках Security Rules та Application Control Rules в Zenarmor, потрібно перевірити, як ефективно вони застосовуються до мережевого трафіку. Процес тестування складається з декількох етапів.

Перевірка роботи Security Rules в Zenarmor полягає в тестуванні ефективності налаштувань, які були визначені для блокування небажаного або потенційно небезпечного трафіку. Цей процес охоплює моделювання різних сценаріїв взаємодії клієнтських пристроїв із зовнішніми ресурсами для підтвердження того, що правила безпеки працюють належним чином і захищають мережу від кіберзагроз.

Перевірка доступу проводилась до ресурсів, які мають бути заблоковані відповідно до встановлених правил безпеки. У Security Rules заблоковані категорії, такі як Malware/Virus, Phishing або Hacking. З клієнтського пристрою Windows 10 проводили спроби підключитися до відомих тестових доменів або ресурсів, які належать цим категоріям. Phishtank.org - це платформа, яка надає спільноті інструменти для обміну інформацією про фішингові атаки та боротьбу з ними. Вона була створена для виявлення та документування фішингових URL-адрес, які використовуються для обману користувачів і викрадення їхніх облікових даних або конфіденційної інформації.

PhishTank надає інструменти для звітування про фішингові атаки, перевірки підозрілих сайтів і завантаження списків підтверджених фішингових доменів (див. рисунок 3.6). Окрім того, що ці сайти є фішинговими вони також у багатьох випадках розповсюджують віруси.

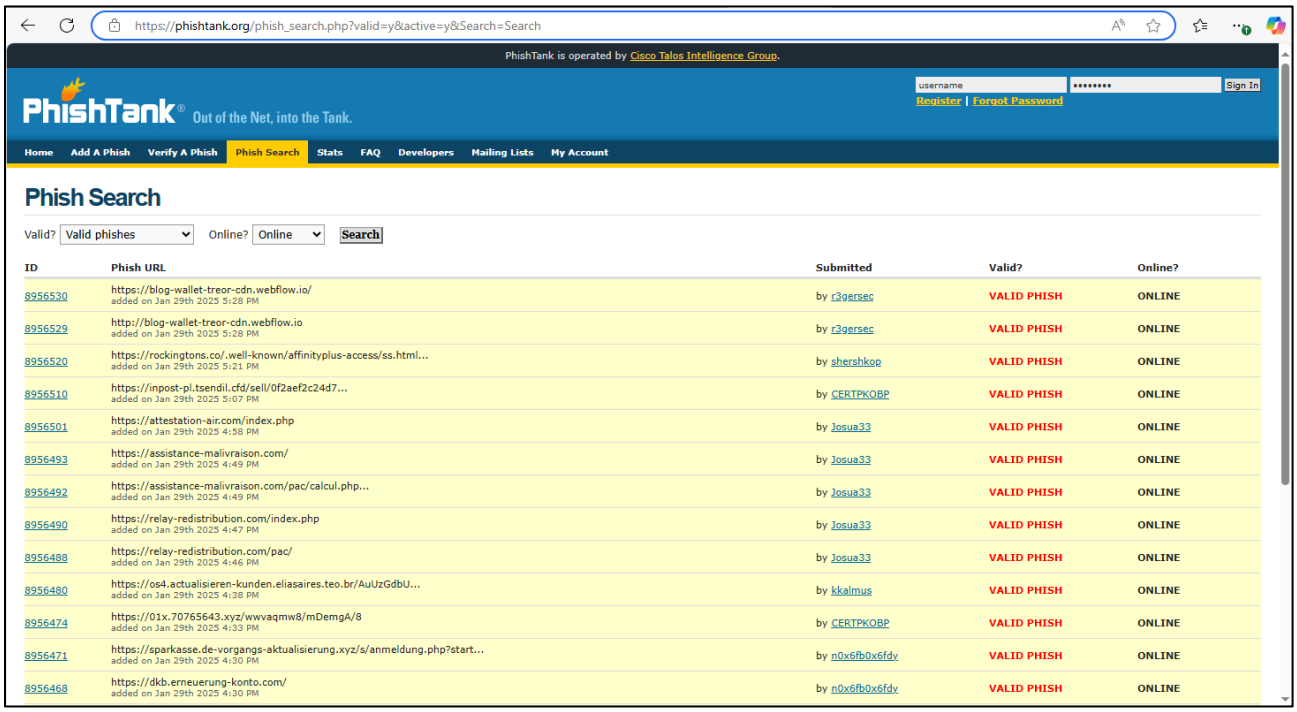

Рисунок 3.6 –Набір URL для тестування Zenarmor

PhishTank є безкоштовним і широко використовується дослідниками кібербезпеки, розробниками антивірусного програмного забезпечення, а також організаціями для захисту своїх систем від фішингових загроз. Він є корисним для тестування ефективності брандмауерів і систем виявлення загроз, таких як Zenarmor, у виявленні та блокуванні фішингових ресурсів.

На рисунку 3.7 показано інформаційну панель Zenconsole, яка надає звіт про роботу системи захисту Zenarmor. Вона відображає аналіз виявлених загроз, заблокованих загроз а також надає інформацію про заблоковані цілі. Панель надає візуалізацію у вигляді діаграм, які допомагають зрозуміти стан мережевої безпеки та активність загроз у мережі.

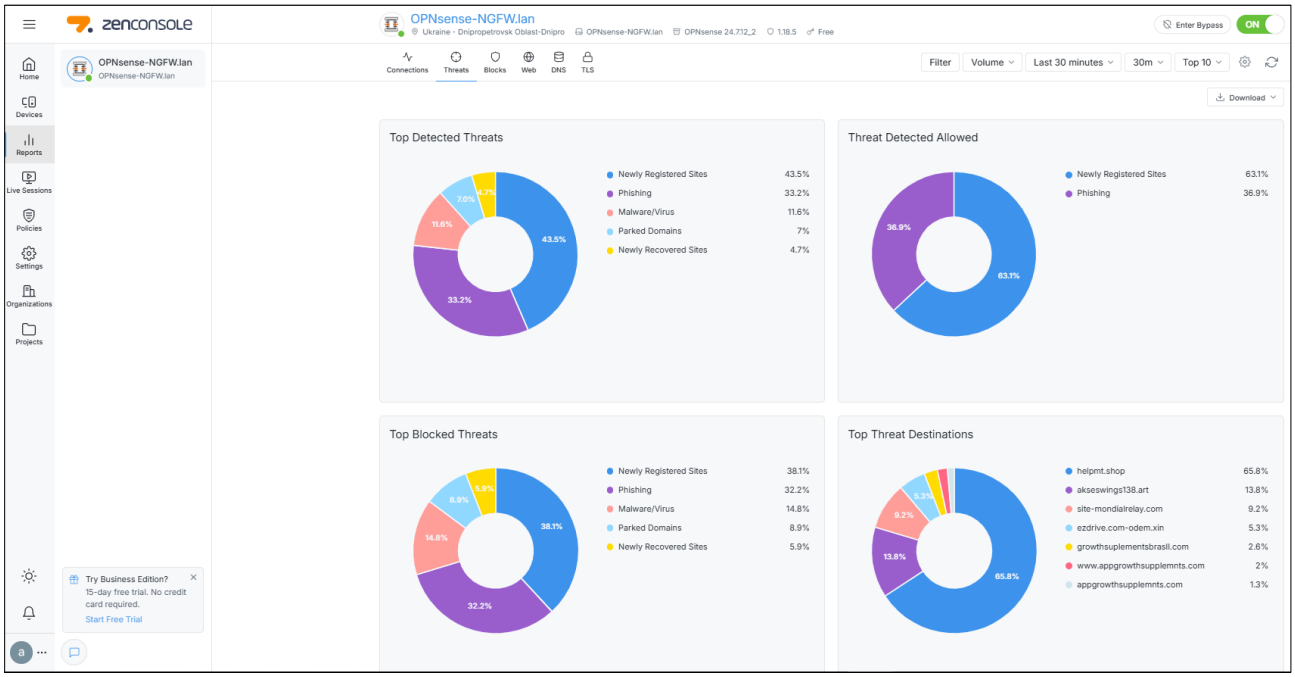

Рисунок 3.7 – Звіт про виявлені загрози в Zenarmor

На діаграмі Top Detected Threats видно, що найбільша частка загроз (43.5%) припадає на сайти з новою реєстрацією доменів. Це типова загроза, оскільки такі сайти часто створюються зловмисниками для фішингу або інших шахрайських дій. Фішинг становить значну частину загроз – 33.2 %. Інші загрози включають шкідливе програмне забезпечення та віруси (11.6%), запарковані домени (7%) і нововідновлені сайти (4.7%).

Діаграма Top Blocked Threats демонструє, що найбільше заблокованих загроз (38.1%) також припадає на нові зареєстровані домени. На другому місці знаходяться фішингові атаки (32.2%), далі йдуть шкідливе програмне забезпечення та віруси (14.8%), запарковані домени (8.9%) і нововідновлені сайти (5.9%). Це показує ефективність системи у блокуванні шкідливих дій.

Остання діаграма Top Threat Destinations показує основні джерела загроз у мережі. Найбільшою часткою серед них є сайт helpmt.shop (65.8%), який, ймовірно, є частиною фішингової кампанії або розповсюджувачем зловмисного програмного забезпечення. Інші цілі включають akseswings138.art (13.8%), site-mondialrelay.com (9.2%) та кілька інших сайтів із меншим відсотком.

На рисунку 3.8 відображено журнал активних сесій блокувань (Live Sessions > Blocks) в Zenarmor, який демонструє деталі заблокованого трафіку.

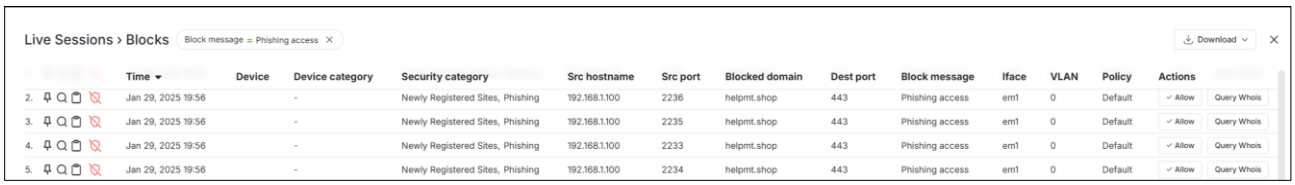

Рисунок 3.8 – Журнал блокувань (фішинг) в Zenarmor

Цей журнал демонструє ефективність налаштувань безпеки Zenarmor. Система успішно виявляє та блокує підозрілий трафік, що відповідає визначеним політикам безпеки, та надає адміністратору деталізовану інформацію для аналізу загроз.

Журнал на рисунку 3.9 демонструє ефективну роботу Zenarmor у блокуванні потенційно небезпечного трафіку. Заблоковані запити до підозрілих доменів, пов’язаних із загрозами зловмисного програмного забезпечення.

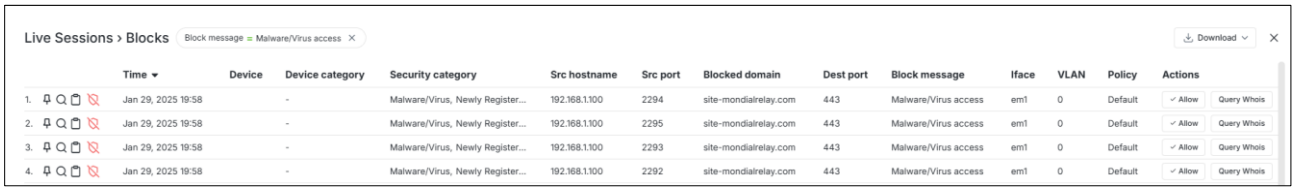

Рисунок 3.9 – Журнал блокувань (віруси) в Zenarmor

Рисунок 3.10 демонструє, як система безпеки Zenarmor успішно блокує доступ до потенційно небезпечних або підозрілих URL-адрес. На екрані браузера, відкритого на тестовій машині Windows 10, відображається повідомлення про неможливість досягти сторінки site-mondialrelay.com.

Такий тип блокування важливий для запобігання потенційним загрозам, які можуть бути приховані за підозрілими доменами, зокрема фішинговим сайтам, веб-ресурсам, що розповсюджують зловмисне програмне забезпечення, або іншим підозрілим джерелам.

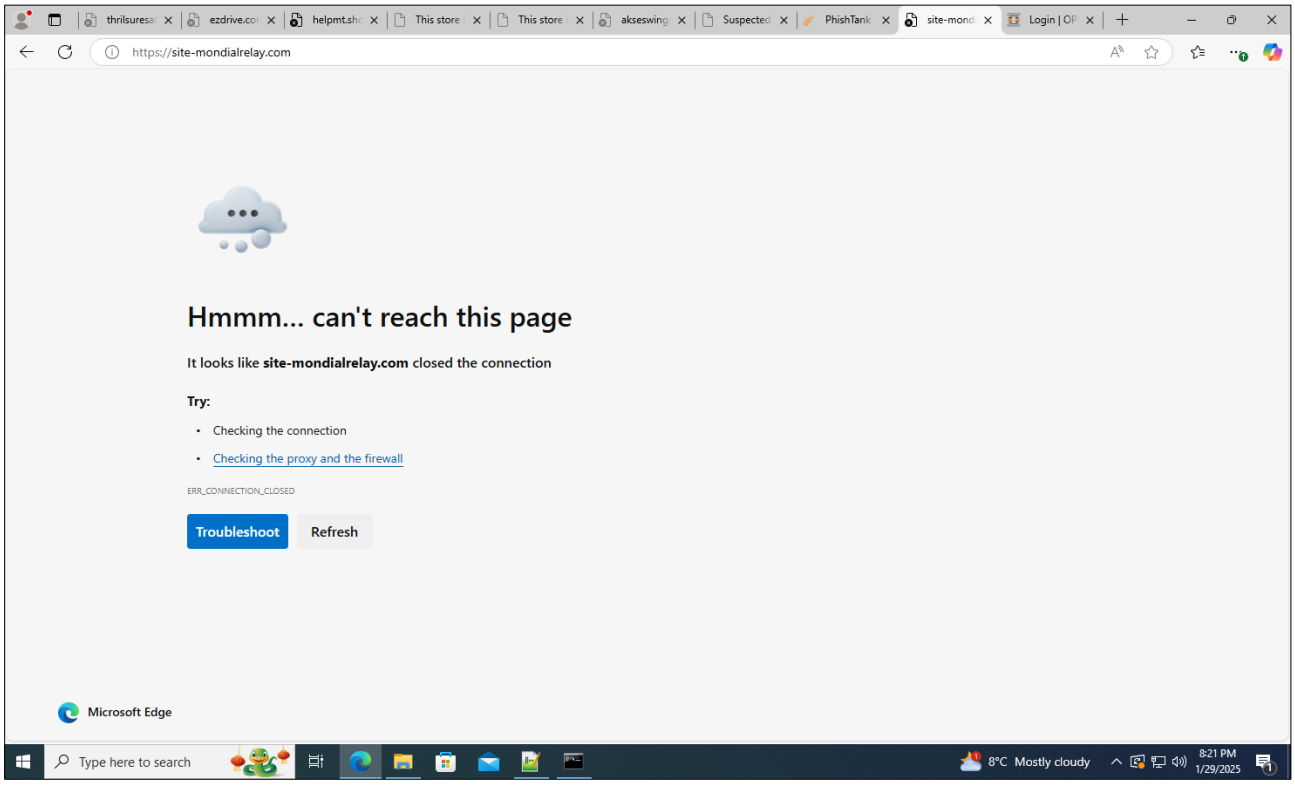

Рисунок 3.10 – Блокування доступу до підозрілих URL

Це повідомлення є прямим підтвердженням того, що правила безпеки, налаштовані в Zenarmor, активуються у відповідь на спроби підключення до сайтів, ідентифікованих як потенційно шкідливі. Блокування супроводжується відповідними налаштуваннями політики, які фільтрують такі запити та переривають з'єднання. Цей результат підкреслює ефективність застосованих заходів безпеки в тестовому середовищі, створеному для дослідження функціоналу Zenarmor на платформі OPNsense.

Для перевірки роботи функції Application Control Rules у Zenarmor було налаштовано правило, яке блокує доступ до сервісу Gmail. Цей тест є демонстрацією можливості системи виявляти та блокувати трафік, пов’язаний із певними програмами чи онлайн-сервісами, згідно з визначеними політиками.

На тестовій машині з операційною системою Windows 10 було виконано спробу доступу до веб-інтерфейсу Gmail через браузер. Після введення URL-адреси Gmail у браузері система блокувала з’єднання. Це підтверджується відображенням на екрані браузера повідомлення про неможливість доступу до сайту. Таке повідомлення є результатом дії правила в Zenarmor, яке

ідентифікувало трафік як пов'язаний із Gmail та застосувало політику блокування.

На рисунку 3.11 представлений звіт із панелі Zenconsole, який відображає результати блокувань трафіку.

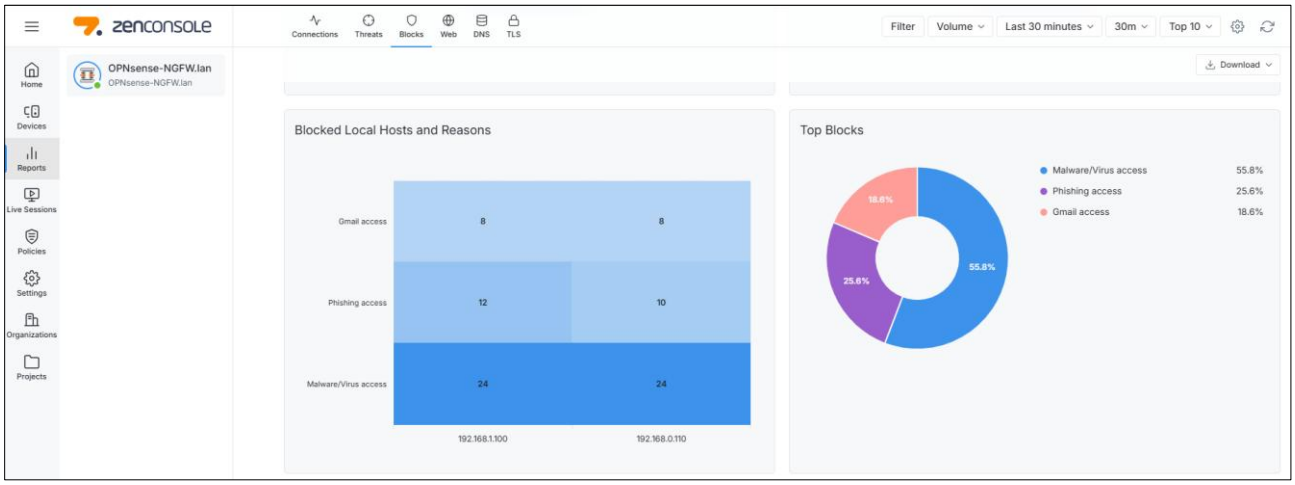

Рисунок 3.11 – Звіт про блокування доступу

Графік блоку Blocked Local Hosts and Reasons деталізує кількість заблокованих запитів за трьома основними категоріями:

Gmail access, що відповідає за спроби доступу до сервісу Gmail. Для тестової машини з IP-адресою 192.168.1.100 заблоковано 8 спроб, що свідчить про активне застосування правил контролю додатків. Phishing access демонструє блокування доступу до URL, відомих своїм фішинговим вмістом. Тут зафіксовано 12 блокувань. Malware/Virus access відповідає за блокування спроб доступу до сайтів, які містять шкідливе програмне забезпечення або відомі віруси.

Секторний графік Top Blocks узагальнює категорії блокувань у відсотковому співвідношенні:

– Malware/Virus access становить 55.8% від загальної кількості блокувань, що є найвищим показником;

– Phishing access займає 25.6% і є другою за поширеністю категорією;

– Gmail access, який було додано як тестове правило блокування додатків, складає 18.6% від загального обсягу.

Ці дані підтверджують ефективність налаштованих правил безпеки та контролю додатків у Zenarmor. Система не лише виявляє потенційно шкідливий трафік, але й успішно блокує небажані підключення, такі як спроби доступу до Gmail відповідно до вимог політики. Даний звіт дозволяє адміністратору оцінювати рівень захисту мережі та робити висновки щодо покращення конфігурації безпеки на основі детальної аналітики.

Zenarmor використовує механізми глибокого аналізу трафіку (DPI) для виявлення конкретних додатків і сервісів на основі сигнатур і характеристик мережевих пакетів. У цьому випадку система автоматично ідентифікувала з'єднання як спробу доступу до Gmail та блокувала її на рівні додатків, незалежно від методу підключення. Результати тестування також були підтверджені через Zenconsole, де в розділі Live Sessions відображаються спроби з'єднання з Gmail. Ці спроби були помічені як заблоковані, із зазначенням часу, IP-адреси джерела, цільового домену та причини блокування. Таким чином, Zenarmor продемонстрував здатність ефективно реалізовувати політики контролю додатків у реальному часі.

Цей тест показує, як система може бути налаштована для блокування доступу до певних програм або сервісів, таких як Gmail, відповідно до вимог організації чи тестового середовища. Такі можливості корисні для обмеження використання небажаних сервісів у мережі, забезпечення безпеки чи управління продуктивністю мережевих ресурсів.

На рисунку 3.12 наведений звіт за результатами роботи Zenarmor протягом 72 годин.

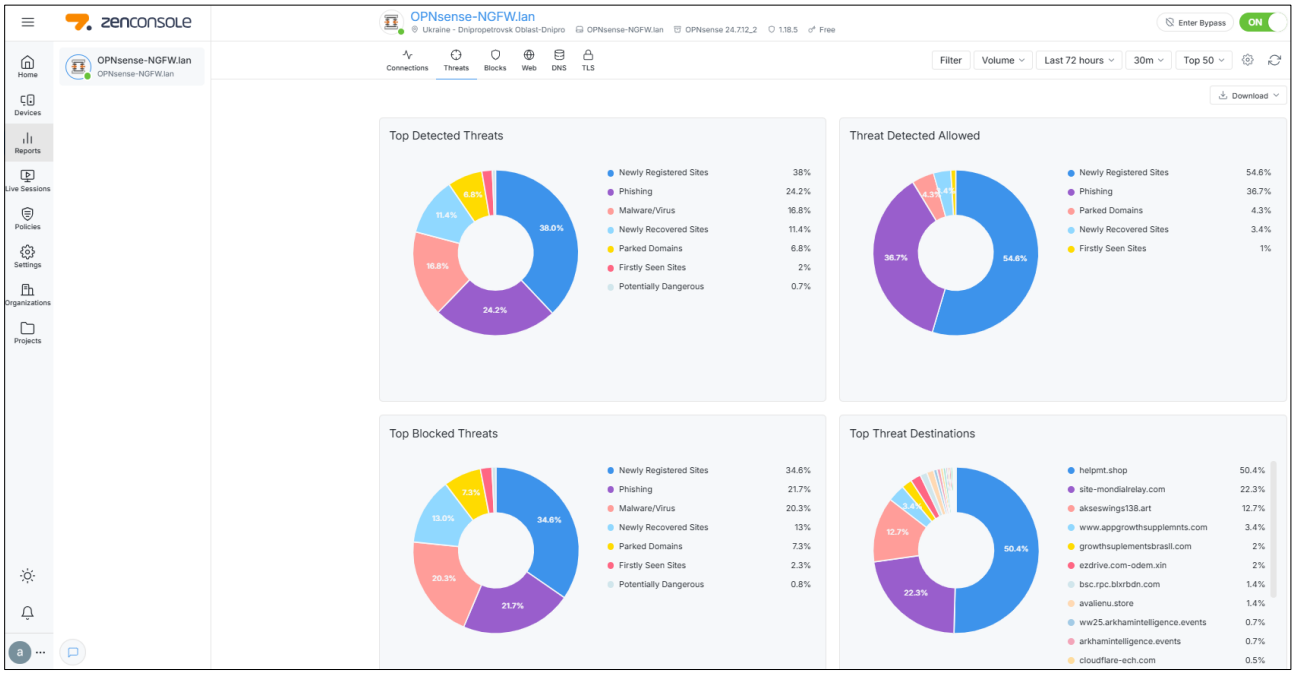

Рисунок 3.12 – Звіт за результатами роботи Zenarmor протягом 72 годин

Він включає аналітику щодо виявлених загроз, дозволеного та заблокованого трафіку, а також основних напрямків загроз.

На графіку Top Detected Threats представлений розподіл усіх виявлених загроз. Найбільшу частку складають Newly Registered Sites (38%), що свідчить про активний моніторинг нових доменів, які потенційно можуть становити загрозу. Другою за поширеністю категорією є Phishing (24.2%), що підкреслює значну кількість фішингових атак, з якими стикається мережа. Malware/Virus (16.8%) займає третю позицію, що свідчить про ефективність Zenarmor у виявленні сайтів зі шкідливим програмним забезпеченням. Інші категорії, такі як Newly Recovered Sites (11.4%), Parked Domains (6.8%), Firstly Seen Sites (2%), та Potentially Dangerous (0.7%), також представлені, але у значно меншій кількості.

Звіт демонструє ефективність Zenarmor у виявленні та блокуванні загроз.

3.3 Висновки до третього розділу

В третьому розділі було детально розглянуто процес налаштування та тестування функціональності брандмауера нового покоління Zenarmor, інтегрованого в платформу OPNsense.

Описано налаштування Zenarmor, яке включало активацію, вибір режиму роботи та мережевих інтерфейсів, а також підключення хмарної розвідки загроз (Cloud Threat Intelligence). Детально розглянуто, як хмарна платформа забезпечує аналіз трафіку в реальному часі, використовуючи розширену базу даних загроз і сучасні методи аналізу. Наголошено на високому рівні безпеки даних завдяки використанню шифрування AES-256 та відповідності стандартам GDPR.

Особливу увагу приділено налаштуванню політик безпеки (Security Rules) та контролю додатків (Application Control Rules), що дозволяє адміністраторам гнучко визначати, який трафік дозволено або заблоковано. Описано механізми роботи Zenarmor з категоріями загроз, такими як Malware/Virus, Phishing, нові домени, та функції блокування небажаних додатків або окремих категорій додатків, як у випадку з Gmail. У ході тестування підтверджено ефективність налаштувань безпеки. Перевірка Security Rules продемонструвала, що система успішно блокує доступ до сайтів із фішингом, шкідливим програмним забезпеченням та іншими загрозами, використовуючи як стандартні списки загроз, так і дані з хмари. Дані з аналітичної панелі Zenconsole підтвердили, що значна частка загроз припадає на нові домени, фішинг і шкідливе ПЗ, а також показали ефективність блокування таких загроз. У рамках тестування Application Control Rules було успішно заблоковано доступ до Gmail. Це підтвердило здатність Zenarmor точно ідентифікувати мережевий трафік, пов’язаний із конкретними сервісами, та застосовувати налаштовані політики. Результати підтверджено через інформаційні панелі Zenconsole, що відображали деталі заблокованих запитів.

Звіт за 72 години роботи Zenarmor показав ефективність системи у виявленні та блокуванні загроз, зокрема нових зареєстрованих сайтів, фішингових атак та шкідливого ПЗ. Zenarmor продемонстрував високу ефективність у забезпеченні мережевої безпеки, виявленні та блокуванні

кіберзагроз у реальному часі. Це рішення є надійним інструментом для управління безпекою завдяки широким можливостям налаштування та інтеграції з хмарними сервісами.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Вимоги пожежної безпеки при гасінні електроустановок

Електроустановки є потенційно небезпечними місцями для виникнення пожеж, так як вони містять велику кількість горючих матеріалів і речовин (ізоляційні матеріали, масла) і потенційні джерела займання (коротке замикання, скачки напруги, перевантаження, іскри). Таке поєднання пожежонебезпечних факторів призводить до того, що саме суворе дотримання норм безпеки не може повністю усунути можливість виникнення пожежі.

Основними причинами виникнення вогнищ горіння або задимлення в електроустановках є:

– аварійні ситуації, пов'язані з перевантаженням в електромережі при відсутності захисту необхідного рівня;

– коротке замикання через пошкодження обладнання або ліній електропередач;

– несправності технологічного обладнання;

– ушкодження допоміжних електромереж;

– порушення правил експлуатації і людський фактор.

Додатковим фактором небезпеки під час пожежі в електроустановках є висока напруга - найчастіше аварійні умови не дозволяють зняти напругу на охопленому вогнем ділянці, тим більше що ситуація вимагає екстрених заходів і швидких рішень. Саме тому кожному співробітнику, задіяному в роботі на такому обладнанні, необхідно точно знати - як і чим слід гасити вогнище загоряння в електроустановках до 1000 В.

Промислові електроустановки в більшості випадків мають автоматичні засоби пожежогасіння, які починають роботу при перевищенні заданих температурних параметрів в приміщенні, аварійному відключенні електроживлення обладнання та інших факторах. При відсутності такої системи виник осередок займання або задимлення необхідно ліквідувати своїми

засобами і силами до приїзду фахівців Державної служби з надзвичайних ситуацій України.

Правила пожежної безпеки України регламентують використання первинних засобів пожежогасіння на електроустановках. Згідно цих правил для гасіння електроустановок які не знаходяться під напругою можна використовувати пісок, воду і вогнегасники всіх марок. Якщо електроустановка перебуває під напругою до 1000 В - дозволено використовувати для придушення осередків займання або задимлення тільки вогнегасники порошкового, аерозольного або вуглекислотного типів з дотриманням всіх правил безпеки [23] [24].

При виникненні вогнища загоряння в щитах управління під напругою до 400В допускається використання вуглекислотних, аерозольних або порошкових типів вогнегасників. Якщо вогнище придушити не вдається, то допускається використання розпорошених водяних потоків від протипожежного водопроводу або спеціальної техніки з обов'язковим дотриманням правил безпеки - із застосуванням електроізолюючих рукавичок, взуття, індивідуальні засоби захисту, із заземленням пожежного ствола і насоса спецтехніки.

Під час гасіння пожежі електроустановок під напругою забороняється [25]:

– використання усіх видів піни;

– проводити будь-які відключення та інші операції з електричним обладнанням особовому складу пожежних підрозділів;

– використовувати воду зі змочувачами при подаванні компактних струменів води, як для гасіння, так і для охолодження електрообладнання та будівельних конструкцій;

– наближатися до машин і механізмів, які застосовуються для подачі води (вогнегасних речовин) на електроустановки під напругою, особам, безпосередньо не зайнятим на гасінні пожежі.

Ефективно застосовується вогнегасник, коли правильно вибрано його тип враховуючи клас пожежі, яку потрібно гасити. Вогнегасники, які містять вуглекислий газ, працюють на основі низькотемпературного струменя і відносяться до газового потоку. Після використання такого вогнегасника не

залишається ніяких слідів. Однак, не слід використовувати вуглекислотні вогнегасники в замкнутому просторі, так як існує ризик пошкодження шкіри і отруєння.

Гасіння електроустановок під напругою за допомогою порошкового вогнегасника вважається ефективним методом усунення загоряння. Порошок, присутній в складі, запобігає доступ кисню до матеріалу і, отже, перешкоджає поширенню полум'я, усуваючи повторні спроби загоряння.

В інструкції до вогнегасника обов’язково міститься інформація про дату виготовлення та час проведення його останнього техобслуговування.

4.2 Проведення інструктажів з охорони праці

Проведення інструктажів з охорони праці є важливим елементом забезпечення безпеки на робочих місцях. Інструктажі з охорони праці спрямовані на ознайомлення працівників з потенційними небезпеками, методами їх запобігання, а також правилами поведінки в надзвичайних ситуаціях. Регулярне проведення таких заходів сприяє зниженню рівня виробничого травматизму та забезпечує відповідність діяльності підприємства чинному законодавству у сфері охорони праці.

Працівники, включаючи керівний персонал, які не пройшли інструктаж та перевірку знань з охорони праці, не можуть бути допущені до виконання роботи. На підприємстві перевірка знань працівників щодо охорони праці здійснюється спеціальною комісією, склад якої затверджується керівником за допомогою відповідного наказу. Роботодавець несе відповідальність за організацію та проведення інструктажів.

За характером і часом проведення інструктажі з охорони праці поділяються на вступні, первинні, повторні, позапланові та цільові, причому кожен з них проводиться для конкретних категорій працівників і за певних обставин [26].

Вступний інструктаж з охорони праці проводиться спеціалістом або іншим кваліфікованим фахівцем. Працівники проходять цей інструктаж у кабінеті

охорони праці або в спеціально обладнаному для цього місці, згідно з програмою та тривалістю, затвердженими роботодавцем. Інструктаж проводиться в перший робочий день працівника або напередодні, якщо існує наказ про його прийняття на роботу [27]. Інформація про проведення вступного інструктажу з питань охорони праці реєструється у відповідному журналі реєстрації. Цей вид інструктажу з охорони праці на підприємстві проводиться:

– працівникам, які приймаються на постійну або тимчасову роботу, незалежно від їх освіти, стажу роботи чи посади;

– працівникам інших організацій, які прибули на підприємство для участі у виробничому процесі або виконання інших робіт для підприємства;

– учням і студентам, які проходитимуть на підприємстві трудове або професійне навчання;

– учасникам екскурсії на підприємство.

Первинний інструктаж проводиться керівником робіт (начальником цеху, майстром) або фізичною особою. Первинний інструктаж проводять з:

– новоприйнятими на постійну або тимчасову роботу працівниками;

– відрядженими працівниками з інших підприємств;

– працівниками, яких перевели з іншого структурного підрозділу підприємства;

– працівниками, які будуть виконувати нову роботу.

Для учнів, студентів, курсантів та слухачів, які проходитимуть трудове або професійне навчання і будуть використовувати різноманітні інструменти, механізми, матеріали також необхідно проводити первинний інструктаж з охорони праці індивідуально або для групи осіб одночасно [27].

Повторний інструктаж є важливим, оскільки дозволяє працівнику відновити знання, отримані під час первинного інструктажу, повторити основні аспекти та уникнути помилок у подальшій роботі. Тому спеціалісти повинні відповідально підходити до розроблення документів з охорони праці, включаючи програми інструктажів, щоб кожен працівник отримав необхідну інформацію та міг своєчасно скористатися набутими знаннями. Терміни проведення повторного інструктажу працівникам:

– які виконують роботи з підвищеною небезпекою –раз на три місяці;

– які виконують інші роботи – раз на пів року.

Позаплановий інструктаж з охорони праці проводять у разі:

введення в дію нових або зміни наявних нормативних документів з охорони праці;

– модифікації технічного обладнання, технологічного процесу або матеріалів, які змінюють алгоритми виробництва;

– випадків недотримання вимог нормативних документів з охорони праці, що спричинили травми, аварії, пожежі тощо;

– у разі перерви в роботі виконавця робіт з підвищеною небезпекою, яка триває понад 30 календарних днів;

– у разі перерви в роботі виконавця інших робіт, яка триває понад 60 календарних днів.

Цільові інструктажі з охорони праці проводяться у випадку необхідності ліквідації аварії або оформлення наряду-допуску, наказу чи розпорядження та не завжди включаються до журналу реєстрації, якщо вони вже узгоджені в наряді-допуску.

Відповідно до вимог, керівник підприємства, відповідальний спеціаліст або безпосередній керівник відділу, ділянки або цеху повинні своєчасно інформувати співробітників про заходи з безпеки. Розробка інструкцій покладається на роботодавця з урахуванням думки професійних фахівців. Обов'язки інструктора включають навчання персоналу, перевірку засвоєних знань та ведення відповідної документації.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи бакалавра було досліджено можливості брандмауерів нового покоління (NGFW) для виявлення й запобігання кіберзагрозам, а також проведено практичне розгортання такої системи на базі платформи OPNsense із використанням модуля Zenarmor. У результаті вдалося досягти мети роботи та виконати всі поставлені завдання.

У роботі проаналізовано принципи роботи та класифікації брандмауерів. Окреслено причини їхнього застосування, а також наведено основні види (за методом фільтрації даних, системним захистом, розташуванням у мережі та форм-фактором). Показано еволюцію від традиційних засобів до NGFW, які поєднують декілька рівнів контролю та інтеграцію з системами IDS/IPS. Вивчено особливості й переваги NGFW у виявленні кіберзагроз. З’ясовано, що глибокий аналіз пакетів, контроль додатків і застосування хмарної розвідки загроз роблять ці рішення ефективними проти сучасних складних атак, зокрема фішингу, шкідливих програм, таргетованих вторгнень. Розроблено архітектуру тестового середовища на базі платформи OPNsense. Для реалізації рішення використано гіпервізор Hyper-V та побудовано двозонну схему мережі (WAN/LAN). Конфігурація включала налаштування WAN, LAN, DHCP, NAT і служб DNS, що імітувало реальну організаційну мережу. Досліджено функціональні можливості Zenarmor як складової NGFW. Виконано інтеграцію Zenarmor в OPNsense, налаштовано політики контролю додатків і безпеки, підключено сервіс хмарної розвідки загроз (Cloud Threat Intelligence), протестовано механізми блокування шкідливих сайтів, фішингу, вірусів, а також заборону доступу до певних сервісів.

Проведено тестування та аналіз ефективності виявлення і блокування загроз. Результати підтвердили спроможність Zenarmor запобігати широкому спектру сучасних кіберзагроз, застосовуючи гнучкі політики безпеки та контролю додатків. Аналітика з інструментів Zenarmor (звіти Zenconsole) продемонструвала успішну ідентифікацію загроз у реальному часі, високу швидкість реагування та вичерпну статистику щодо блокованого трафіку.

Практичне значення отриманих результатів полягає в можливості впровадження розглянутої архітектури NGFW на базі OPNsense у корпоративних і навчальних мережах для підвищення безпеки. Налаштовані методи фільтрації трафіку та система хмарного аналізу забезпечують проактивний захист від складних атак, мінімізуючи ризики витоку конфіденційних даних і збоїв у роботі мережевої інфраструктури.

Поставлену мету було досягнуто, а результати дослідження засвідчили ефективність підходу з використанням Zenarmor для глибокого аналізу пакетів, блокування фішингу, вірусів та інших кіберзагроз. Запропонований комплекс налаштувань і методів діагностики може бути застосований в організаціях, які прагнуть зміцнити кібербезпеку та підвищити стійкість своїх інформаційних систем до сучасних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What are the benefits of a firewall? | fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/benefits-of-firewall

2. Kirbtech. (2022, August 22). Why are firewalls important? | network firewall security. Kirbtech LLC - IT Tech Support, Computer Repair, Networking, Phone |. https://kirbtech.com/benefits-of-firewalls

3. What is a firewall? (n.d.). Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html

4. What are firewall rules? | firewall rules explained. (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-are-firewall-rules

5. 5 firewall design principles in network security | fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/firewall-design-principles

6. Types of firewalls defined and explained. (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/types-of-firewalls

7. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.

8. Tymoshchuk, V., Vantsa, V., Karnaukhov, A., Orlovska, A., & Tymoshchuk, D. (2024). COMPARATIVE ANALYSIS OF INTRUSION DETECTION APPROACHES BASED ON SIGNATURES AND ANOMALIES. Матеріали конференцій МЦНД, (29.11. 2024; Житомир, Україна), 328-332.

9. Tymoshchuk, V., Mykhailovskyi, O., Dolinskyi, A., Orlovska, A., & Tymoshchuk, D. (2024). OPTIMISING IPS RULES FOR EFFECTIVE DETECTION OF MULTI-VECTOR DDOS ATTACKS. Матеріали конференцій МЦНД, (22.11. 2024; Біла Церква, Україна), 295-300.

10. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.

11. Hyper-V technology overview. (n.d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/about

12. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ. Матеріали конференцій МЦНД, (24.05. 2024; Запоріжжя, Україна), 145-146.

13. Introduction — OPNsense documentation. (n.d.). OPNsense documentation. https://docs.opnsense.org/intro.html

14. Interfaces — OPNsense documentation. (n.d.). OPNsense documentation. https://docs.opnsense.org/interfaces.html

15. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп’ютерні мережі. Книга 1. [навчальний посібник] - Львів, "Магнолія 2006", 2013. – 256 с.

16. Firewall — OPNsense documentation. (n.d.). OPNsense documentation. https://docs.opnsense.org/firewall.html

17. Unbound DNS — OPNsense documentation. (n.d.). OPNsense documentation. https://docs.opnsense.org/manual/unbound.html

18. DHCP — OPNsense documentation. (n.d.). OPNsense documentation. https://docs.opnsense.org/manual/dhcp.html

19. Zenarmor. (n.d.). Welcome to the zenarmor user guide for opnsense - zenarmor.com. Zenarmor - Agile Service Edge Security. https://www.zenarmor.com/docs/opnsense

20. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N. & Tymoshchuk, V.(2024). Detection and classification of DDoS flooding attacks by machine learning method. CEUR Workshop Proceedings, 3842, 184–195.

21. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.

22. Zenarmor. (n.d.-a). Cloud management portal for opnsense - zenarmor.com. Zenarmor - Agile Service Edge Security.

https://www.zenarmor.com/docs/opnsense/configuring/cloud-management-portal-for-opnsense

23. ZAGORODNA, N., STADNYK, M., LYPA, B., GAVRYLOV, M., & KOZAK, R. (2022). Network Attack Detection Using Machine Learning Methods. Challenges to national defence in contemporary geopolitical situation, 2022(1), 55-61.

24. Nedzelky, D., Derkach, M., Skarga-Bandurova, I., Shumova, L., Safonova, S., & Kardashuk, V. (2021, September). A Load Factor and its Impact on the Performance of a Multicore System with Shared Memory. In *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (Vol. 1, pp. 499-503). IEEE.

25. Sachenko, A. O., Kochan, V. V., Bykovyy, P. Y., Zahorodnia, D. I., Osolinskyy, O. R., Skarga-Bandurova, I. S., ... & Fesenko, H. V. Internet of Things for intelligent transport systems.

26. Sedinkin, O., Derkach, M., Skarga-Bandurova, I., & Matiuk, D. (2024). Система для відстеження руху очей на основі машинного навчання. *COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION*, (55), 199-205.

27. Стручок В.С. Техноекологія та цивільна безпека. Частина «Цивільна безпека». Навчальний посібник. Тернопіль: ТНТУ. 2022. 150 с.

28. Про затвердження Інструкції з гасіння пожеж на енергетичних об'єктах України. (n.d.). Офіційний вебпортал парламенту України. https://zakon.rada.gov.ua/laws/show/z0013-12

29. Костюк В. Гасіння пожеж на електричних об’єктах під напругою // Охорона праці і пожежна безпека. 2018.

30. Види інструктажів з охорони праці - Охорона праці і пожежна безпека. (n.d.). Охорона праці і пожежна безпека. https://oppb.com.ua/articles/vydy-instruktazhiv-z-ohorony-pratsi

31. Profiteh. (2020, July 7). Інструктажі з охорони праці в Україні — види й порядок проведення | Профітех. ПРОФІТЕХ. https://profiteh.ua/instruktazhi-z-okhorony-pratsi-v-ukraini/