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

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Розробка тестового середовища для оцінки ефективності NGFW у виявленні та блокуванні загроз

Виконав: студент IV курсу, групи СН-42
спеціальності 122 Комп'ютерні науки
(шифр і назва спеціальності)

_____ Паращук Н.М.
(підпис) (прізвище та ініціали)

Керівник _____ Никитюк В.В.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Шимчук Г.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ _____
(підпис) (прізвище та ініціали)

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 комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«___» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

Студенту Паращуку Назарію Михайловичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка тестового середовища для оцінки ефективності NGFW у виявленні та блокуванні загроз

Керівник роботи Никитюк Вячеслав Вячеславович, к.т.н., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*07*» *травня* *2025* року № *4/7-444*

2. Термін подання студентом завершеної роботи 20 червня 2025р.

3. Вихідні дані до роботи Методи та засоби побудови тестових середовищ. Документація по маршрутизатору OPNsense, NGFW Zenarmor та VMware ESXi. Документація по операційний системі Oracle Linux.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1) Аналіз предметної області
2) Проектування та розгортання тестового середовища
3) Практична реалізація та оцінка ефективності NGFW
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 дослідження. 5. Брандмауер нового покоління. 6. Архітектура тестового середовища. 7. Платформа віртуалізації VMware ESXi. 8. Маршрутизатор OPNsense. 9. Zenarmor як модуль NGFW в OPNsense. 10. Політики фільтрації трафіку в Zenarmor. 11. Тестування NGFW Zenarmor: сайт PhishTank. 12. Тестування NGFW Zenarmor: журнал подій. 13. Тестування NGFW Zenarmor: аналітична панель. 14. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Окіпний Ігор Богданович, к.т.н. зав. кафедри МТ		

7. Дата видачі завдання 29 січня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	30.01.2025	*Виконано*
2.	Підбір джерел по темі кваліфікаційної роботи	31.01.2025-03.02.2025	*Виконано*
3.	Опрацювання джерел по темі кваліфікаційної роботи	04.02.2025-06.02.2025	*Виконано*
4.	Виконання дослідження щодо розробка тестового	07.02.2025-11.02.2025	*Виконано*
	середовища для оцінки ефективності NGFW у		
	виявленні та блокуванні загроз		
5.	Оформлення розділу «Аналіз предметної області»	03.06.2025-05.06.2025	*Виконано*
6.	Оформлення розділу «Проектування та розгортання	06.06.2025-08.06.2025	*Виконано*
	тестового середовища»		
6.	Оформлення розділу «Практична реалізація та оцінка	09.06.2025-11.06.2025	*Виконано*
	ефективності NGFW»		
7.	Виконання завдання до розділу «Безпека життєдіяльності»	12.06.2025-13.06.2025	*Виконано*
8.	Виконання завдання до підрозділу «Основи охорони	14.06.2025-15.06.2025	*Виконано*
	праці»		
9.	Оформлення кваліфікаційної роботи	16.06.2025-17.06.2025	*Виконано*
10.	Нормоконтроль	18.06.2025-19.06.2025	*Виконано*
11.	Перевірка на плагіат	20.06.2025	*Виконано*
12.	Попередній захист кваліфікаційної роботи	21.06.2025	*Виконано*
13.	Захист кваліфікаційної роботи	23.06.2025	

Студент _____ Паращук Н.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Никитюк В.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка тестового середовища для оцінки ефективності NGFW у виявленні та блокуванні загроз // Кваліфікаційна робота освітнього рівня «Бакалавр» // Паращук Назарій Михайлович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СН-42 // Тернопіль, 2025 // С.64, рис. – 24, табл. – 1, кресл. – 14, додат. – 0, бібліогр. – 35.

Ключові слова: OPNSense, NGFW, Zenarmor, VMware ESXi, віртуалізація.

У кваліфікаційній роботі бакалавра бакалавра було розроблено, налаштовано та протестовано віртуальне тестове середовище, яке призначене для дослідження можливостей міжмережевого екрана нового покоління Zenarmor на основі маршрутизатор OPNsense.

Метою роботи було створення тестового середовища на базі гіпервізора VMware ESXi, що дало змогу моделювати реальні корпоративні мережі, генерувати як легітимний, так і зловмисний трафік та оцінювати можливості NGFW у режимі реального часу. Здійснено налаштування Zenarmor та активовано Cloud Threat Intelligence, сформовано політики безпеки, керування додатками та веб-контентом.

Практичні випробування проведено з використанням актуальних фішингових доменів сервісу PhishTank. Zenarmor продемонстрував стійку здатність виявляти й блокувати фішингові ресурси, що підтвердилось журналами Live Sessions і аналітичними панелями ZenConsole. Отримані результати доводять доцільність впровадження NGFW Zenarmor у корпоративних мережах як ключового елемента багаторівневого захисту, а розроблена методика тестування може бути використана для попередньої валідації мережевих рішень, навчання персоналу SOC та подальших наукових досліджень продуктивності систем виявлення й запобігання загрозам.

ANNOTATION

Development of a Test Environment to Assess NGFW Efficiency in Threat Detection and Blocking // Qualification work of the educational level "Bachelor" // Nazarii Parashchuk // Ternopil Ivan Pulyu National Technical University, Computer and Information Systems and Software Engineering Faculty, Computer Sciences Department, group SN-42 // Ternopil, 2025 // P. 64, fig. - 24, tabl. - 1, drawings - 14, annexes. – 0, references - 35.

Keywords: OPNSense, NGFW, Zenarmor, VMware ESXi, virtualisation.

In the bachelor's thesis, a virtual test environment was developed, configured and tested to investigate the capabilities of Zenarmor's NGFW based on the OPNsense router.

The goal was to create a test environment based on the VMware ESXi hypervisor, which allowed us to simulate real corporate networks, generate both legitimate and malicious traffic, and evaluate the capabilities of NGFW in real time. Zenarmor was configured and Cloud Threat Intelligence was activated, and security policies and application and web content management were created.

Practical tests were conducted using the latest phishing domains of the PhishTank service. Zenarmor demonstrated a strong ability to detect and block phishing resources, which was confirmed by Live Sessions logs and ZenConsole dashboards. These results prove the feasibility of implementing Zenarmor NGFW in corporate networks as a key element of multi-level protection, and the developed testing methodology can be used for preliminary validation of network solutions, training of SOC personnel, and further research into the performance of threat detection and prevention systems.

ПЕРЕЛІК СКОРОЧЕНЬ

NGFW (англ. Next-Generation Firewall) – Брандмауер нового покоління.

DPI (англ. Deep Packet Inspection) – Глибока інспекція пакетів.

IDS (англ. Intrusion Detection System) – Система виявлення вторгнень.

IPS (англ. Intrusion Prevention System) – Система запобігання вторгненням.

OSI (англ. Open Systems Interconnection) – Модель взаємодії відкритих систем.

DoS (англ. Denial of Service) – Атака на відмову в обслуговуванні.

TCP (англ. Transmission Control Protocol) - Протокол керування передачею

UDP (англ. User Datagram Protocol) - Протокол дейтаграм користувача.

WAN (англ. Wide Area Network) - Глобальна мережа.

LAN (англ. Local Area Network) - Локальна мережа.

HTTP (англ. HyperText Transfer Protocol) — Протокол передавання гіпертексту.

NAT (англ. Network Address Translation) – Трансляція мережевих адрес.

PF (англ. Packet Filter) – Фільтрація пакетів.

DHCP (англ. Dynamic Host Configuration Protocol) – Протокол динамічної конфігурації хостів.

SOC (англ. Security Operations Center) – Центр операцій кібербезпеки.

ЗМІСТ

ВСТУП

Актуальність теми. З кожним роком мережеві інфраструктури стають дедалі складнішими та вразливішими до кіберзагроз, що постійно еволюціонують як за технічним рівнем, так і за масштабом впливу. Це зумовлює зростання вимог до засобів інформаційної безпеки, зокрема до брандмауерів. Класичні брандмауери вже не можуть ефективно протистояти складним атакам, які маскуються під легітимний трафік або використовують особливості протоколів прикладного рівня. У зв'язку з цим все ширше застосовуються міжмережеві екрани нового покоління (NGFW), які поєднують традиційні механізми контролю доступу з глибоким аналізом трафіку (DPI), інтеграцією з IDS/IPS, функціями виявлення додатків та поведінкової аналітики. Для обґрунтованого вибору та налаштування таких рішень необхідно створити тестове середовище, здатне імітувати реальні загрози та забезпечити повноцінну оцінку ефективності NGFW у виявленні й блокуванні атак.

Мета і задачі дослідження. Метою кваліфікаційної роботи є розробка віртуального тестового середовища на основі гіпервізора та брандмауера OPNsense з модулем Zenarmor для аналізу ефективності NGFW у виявленні та блокуванні різних типів кіберзагроз.

Для досягнення мети були поставлені наступні завдання:

- провести аналіз типів брандмауерів та особливостей NGFW;
- дослідити роль тестових середовищ в оцінці ефективності кіберзахисту;
- створити віртуальну інфраструктуру на основі гіпервізора VMware ESXi;
- налаштувати маршрутизатор OPNsense з інтеграцією модуля NGFW Zenarmor;
- здійснити тестування NGFW із внутрішнього сегменту мережі;
- провести оцінку ефективності NGFW з точки зору виявлення та блокування загроз.

Об’єкт дослідження. Об’єктом дослідження є віртуалізовані тестові середовища, призначені для оцінки ефективності NGFW у виявленні та нейтралізації різноманітних кіберзагроз.

Предмет дослідження. Предметом дослідження є процес побудови та використання віртуалізованого тестового середовища для аналізу методів виявлення і блокування кіберзагроз з використанням NGFW Zenarmor, інтегрованого в маршрутизатор OPNsense.

Практичне значення одержаних результатів. Результати даного дослідження можуть бути використані для побудови та тестування корпоративних рішень мережевої безпеки, зокрема для перевірки функціональності NGFW перед їх впровадженням у реальні мережі. Запропоноване тестове середовище дозволяє ефективно оцінювати здатність брандмауера до виявлення та блокування сучасних загроз, що підвищує надійність систем інформаційної безпеки.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Стан інформаційної безпеки в корпоративних мережах

Стан інформаційної безпеки в корпоративних мережах залишається критичним питанням для більшості організацій у всьому світі [1]. Зі зростанням цифрової трансформації бізнес-процесів, розширенням використання хмарних технологій, віддаленого доступу та мобільних пристроїв, корпоративні мережі стають дедалі складнішими, а їх поверхня атаки ширшою. Це призводить до значного зростання кількості кіберінцидентів, витоків даних, атак на IT-інфраструктуру та системи управління.

Сучасні кіберзагрози є високотехнологічними, організованими та часто підтримуються на державному рівні, що створює серйозну загрозу навіть для добре захищених компаній. Традиційні методи захисту, такі як класичні брандмауери або антивіруси, вже не здатні ефективно виявляти складні атаки, які використовують шифрування, обфускацію або легітимний мережевий трафік для проникнення в систему [2].

Особливу небезпеку становлять цілеспрямовані атаки, програми-вимагачі, фішингові атаки, експлойти нульового дня та атаки на ланцюги постачання. Часто такі атаки залишаються непоміченими тривалий час, що дозволяє зловмисникам отримувати контроль над внутрішніми системами та викрадати чутливу інформацію. Крім того, вразливості в конфігурації мережевих пристроїв, недостатній контроль за доступом, використання застарілих протоколів і відсутність сегментації мережі призводять до того, що навіть один скомпрометований вузол може стати точкою входу для подальшого розповсюдження атаки в мережі.

У відповідь на зростання ризиків компанії дедалі частіше впроваджують комплексні рішення для кіберзахисту, серед яких важливе місце займають системи IDS/IPS, а також брандмауери нового покоління. Останні здатні

проводити глибокий аналіз трафіку, контролювати доступ до додатків, виявляти аномалії в поведінці користувачів і автоматично блокувати підозрілу активність у режимі реального часу [3].

Таким чином, попри суттєвий прогрес у розвитку засобів захисту, рівень інформаційної безпеки в корпоративних мережах багато в чому залежить від інтеграції сучасних технологій захисту, грамотної побудови мережевої архітектури, безперервного моніторингу та періодичного тестування захисних механізмів в умовах, максимально наближених до реального середовища загроз.

1.2 Причини використання брандмауерів у корпоративному середовищі

Використання брандмауерів у корпоративному середовищі є фундаментальним елементом забезпечення інформаційної безпеки та контролю за мережевими потоками [4]. Головна причина їхнього впровадження полягає в необхідності обмеження несанкціонованого доступу до внутрішніх ресурсів організації з боку зовнішнього світу, зокрема з глобальної мережі Інтернет. Брандмауери дозволяють фільтрувати мережевий трафік на основі визначених політик безпеки, блокуючи підозрілу або шкідливу активність ще на рівні входу до мережі [5].

У корпоративному середовищі завжди існує потреба чітко розмежовувати доступ між різними сегментами мережі - наприклад, між серверами, робочими станціями, гостьовими зонами Wi-Fi та віддаленими підключеннями. Без належної фільтрації мережевого трафіку будь-який вузол може стати як джерелом витоку даних, так і точкою проникнення зловмисників. Саме брандмауери забезпечують ізоляцію окремих мережевих зон і виконують функції контролю за дозволеними протоколами, портами, IP-адресами, що значно знижує ризик внутрішнього та зовнішнього вторгнення.

Крім цього, у зв’язку з поширенням складних атак, які використовують стандартні протоколи та легітимні додатки для прикриття, компаніям необхідні засоби глибшого аналізу трафіку, ніж просто перевірка заголовків пакетів. Сучасні брандмауери, такі як NGFW здатні розпізнавати типи додатків, виявляти аномальну поведінку, здійснювати перевірку вмісту трафіку, інтегруватися з системами аутентифікації та централізованого журналювання. Це дозволяє дотримуватись політик доступу на основі ролей користувачів, пристроїв або додатків.

Ще однією причиною використання брандмауерів є необхідність дотримання вимог нормативних документів, стандартів інформаційної безпеки та галузевих регламентів - таких як ISO 27001, GDPR, PCI DSS тощо. Вони вимагають впровадження технічних засобів контролю, серед яких брандмауер займає ключове місце.

Таким чином, брандмауери відіграють не лише роль першої лінії захисту від зовнішніх загроз, а й стають складовою політики безпечного доступу, захисту конфіденційних даних та дотримання вимог регуляторів. Їх використання є обов’язковим для побудови надійної та масштабованої системи захисту інформаційних ресурсів.

1.3 Типи брандмауерів

Існує кілька основних типів брандмауерів, кожен з яких має свої особливості, рівень захисту та сценарії використання [6]. Розвиток цих рішень відображає еволюцію методів фільтрації трафіку у відповідь на дедалі складніші кіберзагрози.

Найпростішими є брандмауери, що здійснюють фільтрацію пакетів (Packet Filtering Firewalls) (див. рисунок 1.1). Вони працюють на мережевому та транспортному рівнях моделі OSI (L3–L4) і аналізують заголовки пакетів без вивчення їх вмісту [7].

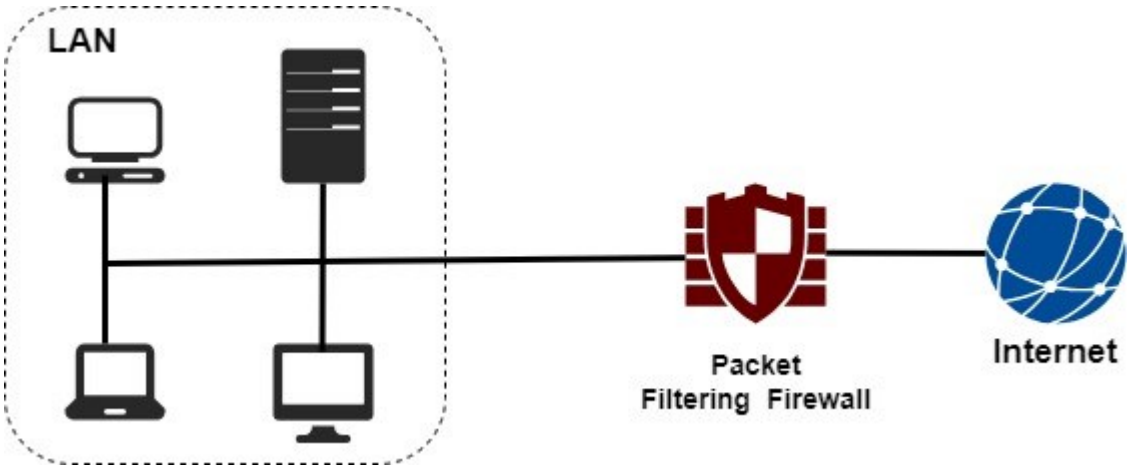

Рисунок 1.1 – Брандмауер із фільтрацією пакетів

Такі брандмауери ухвалюють рішення про дозвіл чи блокування трафіку на основі IP-адреси джерела і призначення, номера порту, типу протоколу (TCP, UDP тощо). Хоча вони мають високу швидкість обробки трафіку, їхній рівень безпеки обмежений, оскільки відсутній контекст попередніх з'єднань, а глибокий аналіз даних недоступний.

Наступним етапом розвитку стали брандмауери з перевіркою стану з’єднання (Stateful Inspection Firewalls) (див. рисунок 1.2).

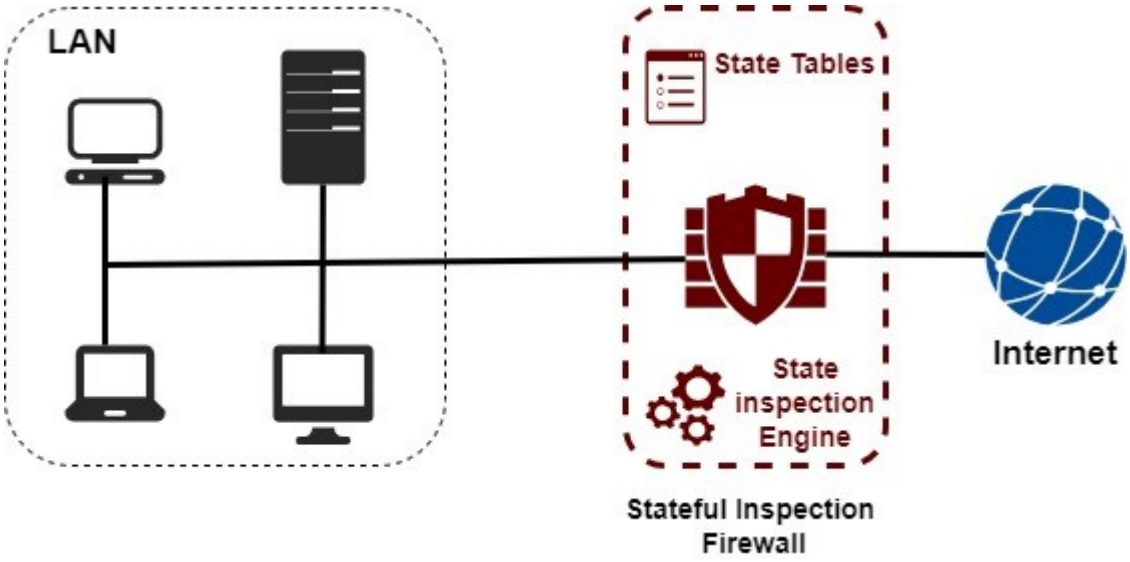

Рисунок 1.2 – Брандмауер із перевіркою стану з’єднання

Вони також працюють на L3–L4 рівнях, але вже підтримують стан з'єднань, тобто пам'ятають попередні пакети сесії та аналізують, чи є новий

пакет частиною встановленого з'єднання [8]. Це дозволяє ефективніше виявляти підозрілий трафік, уникати атак, що використовують спуфінг або інші методи маніпуляції TCP-з'єднаннями. Stateful-фільтрація забезпечує вищий рівень захисту в порівнянні з простим Packet Filtering.

Іншим типом є брандмауери на основі проксі (Application Proxy Firewalls). Вони працюють на прикладному рівні моделі OSI (L7) і діють як посередник між клієнтом і сервером. Проксі-брандмауери повністю розривають з'єднання, аналізують вміст запитів і відповідей, здійснюють перевірку протоколів (HTTP, FTP, DNS тощо) та можуть виявляти атаки, які базуються на аномаліях у поведінці додатків. Завдяки повному контролю трафіку вони забезпечують високий рівень безпеки, проте можуть знижувати продуктивність через значні обчислювальні витрати.

Подальший розвиток отримали брандмауери нового покоління, які поєднують функціональність stateful-брандмауерів і проксі-фільтрації з новими можливостями: DPI, інспекція за протоколами прикладного рівня, ідентифікація додатків, інтеграція з антивірусами, системами IDS/IPS, контроль користувачів, шифруваного трафіку (SSL inspection) та інше (див. рисунок 1.3).

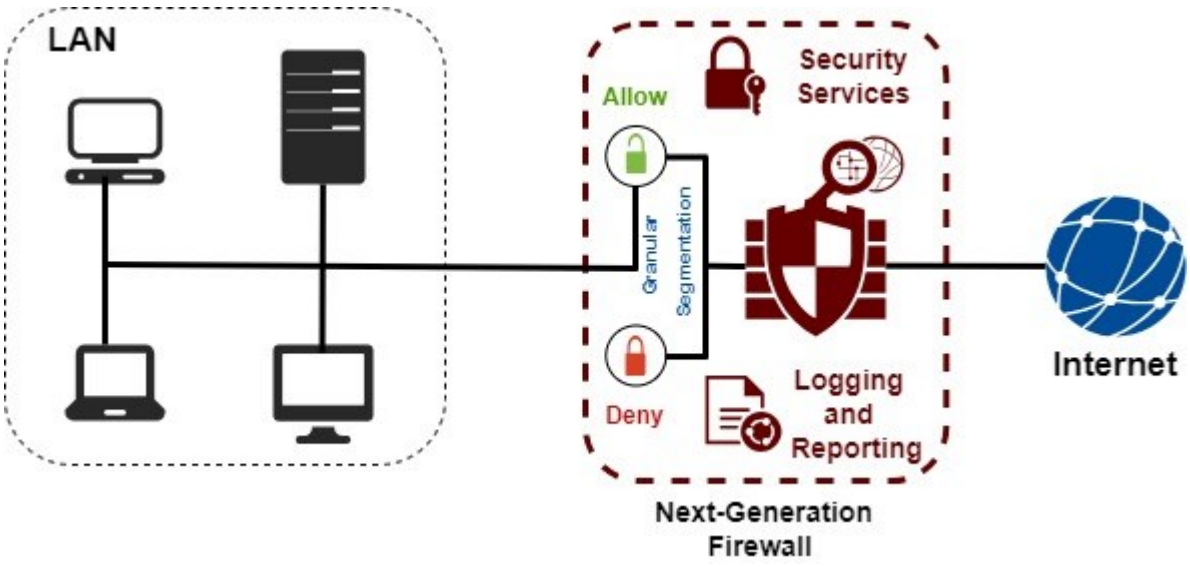

Рисунок 1.3 – Брандмауер нового покоління

Однією з головних особливостей NGFW є інтеграція механізму DPI, який дозволяє аналізувати не лише заголовки, а й вміст трафіку [9]. Завдяки цьому брандмауер може розпізнавати конкретні додатки, навіть якщо вони працюють через нестандартні порти або зашифрований трафік, а також відстежувати поведінку користувача або пристрою, який генерує мережеву активність. Ще одна важлива характеристика - це розпізнавання та контроль додатків (application-aware firewalling). NGFW дозволяє створювати політики безпеки не тільки на основі IP-адрес чи портів, а з урахуванням того, який саме додаток використовується - наприклад, Facebook, Dropbox, Skype, BitTorrent тощо. Це дає змогу блокувати або обмежувати окремі функції додатків, знижуючи ризик витоку даних або порушення політик компанії. Крім цього, NGFW часто включає вбудовані функції систем IDS/IPS [10], що дозволяють виявляти відомі атаки на основі сигнатур, а також виявляти аномалії в трафіку. У сучасних брандмауерах ці функції тісно інтегровані з DPI, що дозволяє не лише фіксувати загрозу, а й негайно її блокувати до того, як вона завдасть шкоди. Ще одна особливість полягає в підтримці SSL/TLS-інспекції [11], яка дозволяє NGFW розшифровувати зашифрований HTTPS-трафік. NGFW також підтримує ідентифікацію користувачів та інтеграцію з системами контролю доступу (наприклад, Active Directory), що дозволяє застосовувати політики безпеки не лише на рівні IP-адрес, а й для конкретних користувачів або груп. Це особливо корисно в корпоративних середовищах, де потрібен гнучкий контроль за поведінкою співробітників та дотриманням внутрішніх регламентів.

Багато NGFW-рішень мають функції централізованого моніторингу та аналітики, що дозволяють не лише переглядати журнали подій, а й будувати графіки трафіку, аналізувати статистику загроз, отримувати повідомлення про інциденти в реальному часі та здійснювати кореляцію подій з різних джерел. Це значно полегшує роботу аналітиків SOC та дозволяє швидше реагувати на потенційні загрози. Слід також відзначити можливість динамічного оновлення сигнатур загроз за допомогою хмарних сервісів, що дозволяє NGFW залишатись актуальним у боротьбі з новими загрозами, такими як zero-day

експлойти, ботнети, шкідливе ПЗ тощо. Деякі рішення також підтримують машинне навчання або поведінкову аналітику, що дозволяє виявляти нові загрози без використання попередньо визначених сигнатур.

За місцем розташування брандмауери можна розділити на два основних типи: мережеві брандмауери (network firewalls) та брандмауери на основі хостів (host-based firewalls). Обидва типи виконують одну з головних функцій кіберзахисту - контроль мережевих з'єднань, але мають різну зону застосування, архітектуру та особливості реалізації (див. рисунок 1.4).

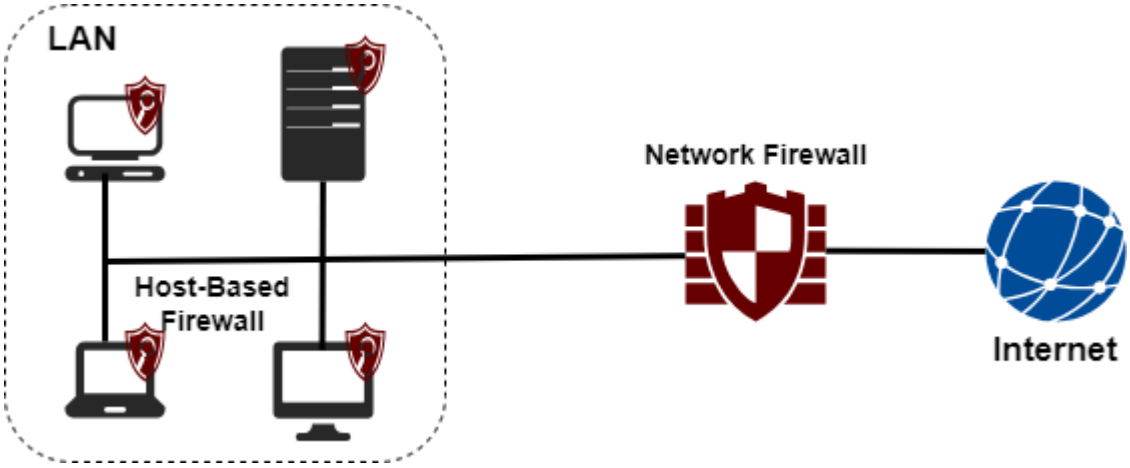

Рисунок 1.4 – Мережевий брандмауери та брандмауери на основі хостів

Мережеві брандмауери зазвичай розгортаються на межі між внутрішньою корпоративною мережею та зовнішніми мережами або між окремими сегментами мережі. Вони можуть бути реалізовані у вигляді окремого апаратного пристрою, віртуального середовища (наприклад, в хмарних інфраструктурах), або як програмне забезпечення на спеціалізованих маршрутизаторах чи шлюзах безпеки. Основне завдання мережевого брандмауера - централізований контроль усього вхідного та вихідного трафіку, який проходить через межі підконтрольної мережі. Такі брандмауери можуть працювати на різних рівнях моделі OSI. Мережева модель забезпечує масштабованість і дозволяє впроваджувати політики безпеки в централізований спосіб для всієї організації. Проте, мережеві брандмауери можуть не мати

повного доступу до подій всередині вузлів мережі, особливо у випадках, коли трафік залишається локальним або йде в обхід шлюзів.

На відміну від них, брандмауери на основі хостів працюють на рівні окремих кінцевих пристроїв - серверів, робочих станцій або навіть мобільних пристроїв. Це програмні рішення, вбудовані в операційні системи (наприклад, Windows Defender Firewall, Nftables у Linux), або додаткові інструменти, які забезпечують локальний контроль вхідних та вихідних з'єднань безпосередньо на конкретному пристрої. Брандмауери на основі хоста фільтрують трафік ще до того, як він досягне або вийде з самого вузла, на якому вони працюють.

Головна перевага таких брандмауерів полягає в їхній здатності забезпечити детальний контроль за процесами, які ініціюють мережеву активність. Вони можуть перевіряти, який саме додаток чи служба генерує трафік, дозволяти або забороняти його залежно від політики безпеки, вести журнали подій та виявляти потенційно небажану активність, навіть якщо вона залишається локалізованою в межах підмережі. Брандмауери на основі хоста також важливі для пристроїв, які підключаються до зовнішніх або незахищених мереж - наприклад, ноутбуки з віддаленим доступом або BYOD-пристрої. Водночас, основним обмеженням є їх децентралізований характер: адміністратору потрібно забезпечити окреме налаштування, моніторинг і оновлення для кожного вузла, що вимагає додаткових зусиль у великих інфраструктурах. Обидва типи брандмауерів не виключають один одного, а доповнюють. Мережеві брандмауери створюють зовнішній периметр захисту, тоді як на основі хоста - забезпечують глибинний контроль та внутрішню ізоляцію. Їхнє спільне використання дозволяє реалізувати багаторівневий захист (defense-in-depth), який значно ускладнює проникнення та горизонтальне розповсюдження атак у корпоративному середовищі.

Також слід згадати хмарні брандмауери (Cloud Firewalls або Firewall-as-a-Service), які надають аналогічну функціональність у вигляді віддалених сервісів, без потреби в локальному обладнанні. Такі рішення широко використовуються в умовах переходу на хмарну інфраструктуру, гібридні та

мультихмарні середовища. Вони інтегруються з сервісами IaaS/PaaS і забезпечують захист трафіку між хмарними та локальними сегментами.

1.4 Роль тестових середовищ в оцінці кіберзахисту.

Тестові середовища відіграють ключову роль в оцінці ефективності засобів кіберзахисту, оскільки дозволяють відтворити поведінку реального мережевого середовища в контрольованих умовах, не наражаючи на ризик продуктивну інфраструктуру [12]. Оскільки зловмисники використовують дедалі складніші та динамічніші методи атак, вкрай важливо мати можливість моделювати як типові, так і нестандартні сценарії вторгнень. Саме тестові середовища дають змогу не лише перевірити роботу брандмауерів, IDS/IPS, систем захисту кінцевих точок або NGFW, а й оцінити їхню здатність своєчасно реагувати на реальні загрози [13].

Завдяки таким середовищам можна ретельно протестувати політики безпеки, правила фільтрації, процедури виявлення аномалій і перевірити, наскільки ефективно система блокує небажаний або шкідливий трафік. Це особливо важливо для NGFW, які повинні виконувати не лише базову перевірку пакетів, а й проводити аналіз додатків, виявляти експлойти, контролювати користувачів та реалізовувати поведінкову аналітику. У тестовому середовищі можна створити точні сценарії атаки - наприклад, порт-сканування, DoS, експлуатацію вразливостей у додатках і спостерігати за реакцією захисної системи без ризику порушення роботи корпоративної мережі [14].

Окрім цього, тестові середовища широко застосовуються для верифікації оновлень, які можуть вплинути на стабільність роботи мережевих пристроїв або служб безпеки. Перед тим як застосовувати нову версію прошивки, змінювати сигнатури IPS чи інтегрувати нові функції, адміністратори можуть протестувати зміни в ізольованому середовищі. Це значно зменшує ризик конфліктів і збоїв у продуктивній мережі. Тестове середовище також є

важливим інструментом для навчання та тренувань персоналу з кібербезпеки. Спеціалісти можуть відпрацьовувати реагування на інциденти, шукати шляхи обфускації трафіку, тестувати нові способи атак, при цьому розуміючи, як їх можна виявити й заблокувати. Це розвиває як технічні навички, так і стратегічне мислення щодо побудови ефективної системи захисту.

У процесі впровадження нових рішень або оновлення архітектури безпеки тестові середовища є незамінними для порівняльного аналізу різних продуктів - наприклад, NGFW від різних виробників. В однакових умовах можна оцінити швидкодію, точність виявлення загроз, рівень false positives, підтримку протоколів, зручність адміністрування та гнучкість політик.

З технічної точки зору, сучасні тестові середовища зазвичай реалізуються у віртуалізованій формі, використовуючи гіпервізори [15] на кшталт VMware ESXi, KVM, XEN, Hyper-V або хмарні платформи [16]. Це дозволяє швидко масштабувати інфраструктуру, моделювати складні мережеві топології, створювати ізольовані підмережі та використовувати шаблони систем для автоматизованого розгортання.

Загалом, роль тестових середовищ у сфері кіберзахисту є фундаментальною. Вони забезпечують надійний простір для експериментів, удосконалення захисту, зниження ризиків та підвищення впевненості в працездатності впроваджених рішень [17]. Без такого середовища неможливо повноцінно оцінити реальну ефективність навіть найпотужнішого інструменту безпеки в умовах реальних загроз.

1.5 Висновок до першого розділу

В першому розділі було проведено всебічний аналіз предметної області, що стосується інформаційної безпеки в корпоративних мережах, ролі брандмауерів у захисті інформаційних ресурсів, класифікації міжмережевих екранів, їхніх особливостей, а також значення тестових середовищ для оцінки ефективності засобів кіберзахисту. Розглянуто сучасний стан інформаційної

безпеки в умовах стрімкого зростання кількості та складності кіберзагроз. Показано, що традиційні засоби захисту втрачають ефективність у боротьбі зі складними та цілеспрямованими атаками, що змушує організації впроваджувати більш гнучкі та інтелектуальні засоби контролю трафіку, зокрема NGFW. У ході дослідження визначено основні причини використання брандмауерів у корпоративному середовищі, серед яких – потреба в захисті від несанкціонованого доступу, ізоляція мережевих сегментів, забезпечення відповідності нормативним вимогам і створення єдиної політики контролю доступу. Було проаналізовано типи брандмауерів: від простих пакетних фільтрів до NGFW, які поєднують глибоку інспекцію трафіку, поведінковий аналіз, розпізнавання додатків, контроль користувачів та інтеграцію з IDS/IPS. Описано функціональні особливості мережевих брандмауерів та брандмауерів на основі хоста, які відіграють взаємодоповнюючу роль у багаторівневому захисті інфраструктури.

Окрема увага приділена тестовим середовищам, які є незамінним інструментом як для перевірки працездатності систем захисту, так і для симуляції атак та аналізу їх впливу. Було встановлено, що тестові середовища дозволяють безпечно моделювати загрози, перевіряти ефективність політик безпеки, проводити порівняльний аналіз NGFW-рішень і навчати персонал методам протидії інцидентам.

Таким чином, отримані в першому розділі теоретичні результати закладають основу для подальшої практичної реалізації тестового середовища та оцінки ефективності NGFW у наступних розділах роботи.

РОЗДІЛ 2. ПРОЕКТУВАННЯ ТА РОЗГОРТАННЯ ТЕСТОВОГО СЕРЕДОВИЩА

2.1 Архітектура тестового середовища

Розробка архітектури є ключовим етапом створення тестового середовища для проведення достовірного й репрезентативного тестування ефективності NGFW. Вона визначає топологію, взаємозв'язки між віртуальними компонентами, сегментацію мережі та сценарії передачі трафіку, які імітують реальну корпоративну інфраструктуру. У даній роботі тестове середовище реалізовано на основі гіпервізора VMware ESXi, що забезпечує можливість створення ізольованих віртуальних машин, незалежних мережевих сегментів і гнучке налаштування інтерфейсів (див. рисунок 2.1).

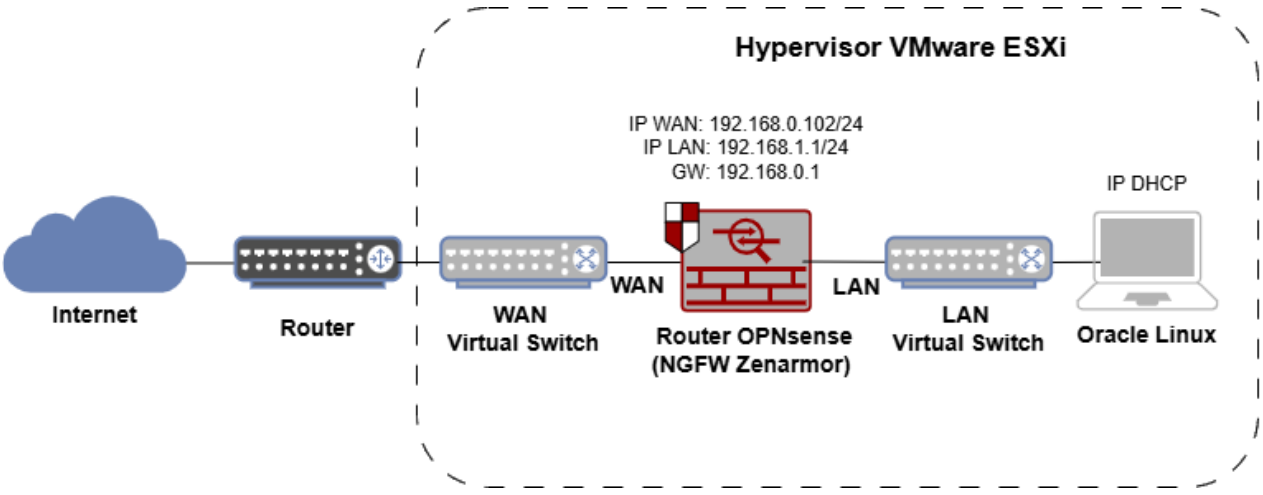

Рисунок 2.1 – Схема тестового середовища

У центрі тестового середовища розташовано Zenarmor NGFW на базі маршрутизатора OPNsense, який виконує функції глибокого аналізу трафіку, інспекції додатків та моніторингу мережевої активності. OPNsense має два основні інтерфейси: WAN та LAN, які логічно розділяють зовнішній і внутрішній сегменти віртуальної мережі.

Інтерфейс WAN з’єднаний з фізичним маршрутизатором з доступом до мережі Інтернет. Інтерфейс LAN є внутрішнім сегментом мережі, де розташовані захищені вузли. Віртуальна машина Oracle Linux у LAN-сегменті виступає в ролі легітимного користувача корпоративної мережі. Цей хост піддається тестам із моделювання внутрішніх загроз, а також генерує звичайний користувацький трафік для аналізу поведінки NGFW у реальних умовах. На LAN-інтерфейсі також працює DHCP-сервер, розгорнутий на OPNsense, що забезпечує автоматичне надання IP-адрес у внутрішньому сегменті.

Zenarmor, інтегрований як плагін у систему OPNsense, відповідає за аналіз трафіку в LAN-сегменті. Він здійснює глибоку інспекцію даних, класифікацію додатків, фільтрацію HTTPS/HTTP-запитів, ідентифікацію сесій та виявлення підозрілої активності. Важливою перевагою є можливість перегляду повної статистики з детальними логами, аналітикою за типами трафіку, користувачами та пристроями.

Мережеві налаштування елементів тестового середовища показано в таблиці 2.1.

Таблиця 2.1 – Мережеві налаштування елементів тестового середовища

Елемент	Інтерфейс	IP-адреса	Мережева маска	Шлюз
Router	eth1	DHCP	DHCP	DHCP
	eth2	192.168.0.1	255.255.255.0	
Router OPNsense	eth1	192.168.0.102	255.255.255.0	192.168.0.1
	eth2	192.168.1.1	255.255.255.0	
Oracle Linux	eth1	192.168.1.101	255.255.255.0	192.168.1.1
Hypervisor VMware ESXi	eth1	192.168.0.200	255.255.255.0	192.168.0.1

Віртуальні мережі на базі VMware ESXi створюються ізольовано, що дозволяє повністю контролювати передачу даних, конфігурувати маршрутизацію, застосовувати NAT, ізолювати сегменти та забезпечувати

безпечне середовище для моделювання реалістичних атак без загрози для зовнішньої інфраструктури.

Загальна архітектура забезпечує повноцінний цикл тестування: від генерування загроз до фіксації подій брандмауером і аналізу результатів. Такий підхід дозволяє не лише оцінити здатність NGFW до виявлення та блокування кіберзагроз, а й перевірити його стійкість до навантаження, точність класифікації трафіку, гнучкість у налаштуванні політик безпеки, а також зручність використання системи адміністрування. У результаті створена архітектура дозволяє проводити якісне, багатоаспектне тестування, наближене до реальних умов експлуатації корпоративного захисту.

2.2 Платформа віртуалізації VMware ESXi

VMware ESXi є високопродуктивним гіпервізором типу 1 (bare-metal), який дозволяє безпосередньо запускати віртуальні машини на фізичному сервері без потреби в проміжній операційній системі [18]. Це ядро віртуалізаційної екосистеми VMware, що широко використовується в корпоративному секторі для побудови надійних, масштабованих та керованих інфраструктур [19]. Завдяки своїй архітектурі ESXi забезпечує високий рівень стабільності, безпеки та продуктивності, що є критично важливим для розгортання тестових середовищ з метою дослідження кібербезпеки.

Однією з головних переваг VMware ESXi є його мікроядро ядро, яке містить лише базові функції, необхідні для запуску та керування віртуальними машинами. Такий підхід зменшує поверхню атаки, підвищує рівень захисту платформи та знижує вимоги до обслуговування. ESXi не потребує встановлення традиційної операційної системи. Після інсталяції гіпервізор працює автономно, взаємодіючи з апаратними ресурсами через власні драйвери та низькорівневі сервіси.

Платформа підтримує широке коло гостьових операційних систем, включаючи Windows, Linux, Unix а також спеціалізовані дистрибутиви для

мережевих і безпекових задач - наприклад, Kali Linux, pfSense, OPNsense. Кожна віртуальна машина ізольована від інших, що дозволяє моделювати безпечні сценарії атак і експериментів без ризику для основної інфраструктури.

У тестовому середовищі для оцінки ефективності NGFW ESXi виконує роль центральної платформи, на якій розгортається вся інфраструктура: NGFW на основі віртуального маршрутизатора OPNsense, клієнтська машина Oracle Linux, віртуальні комутатори для сегментів LAN і WAN. Кожна з операційних систем існує у вигляді окремої віртуальної машини з налаштованими мережевими інтерфейсами, обсягом пам’яті та процесорними ядрами.

Інтерфейс керування ESXi надається через вебпанель (див. рисунок 2.2).

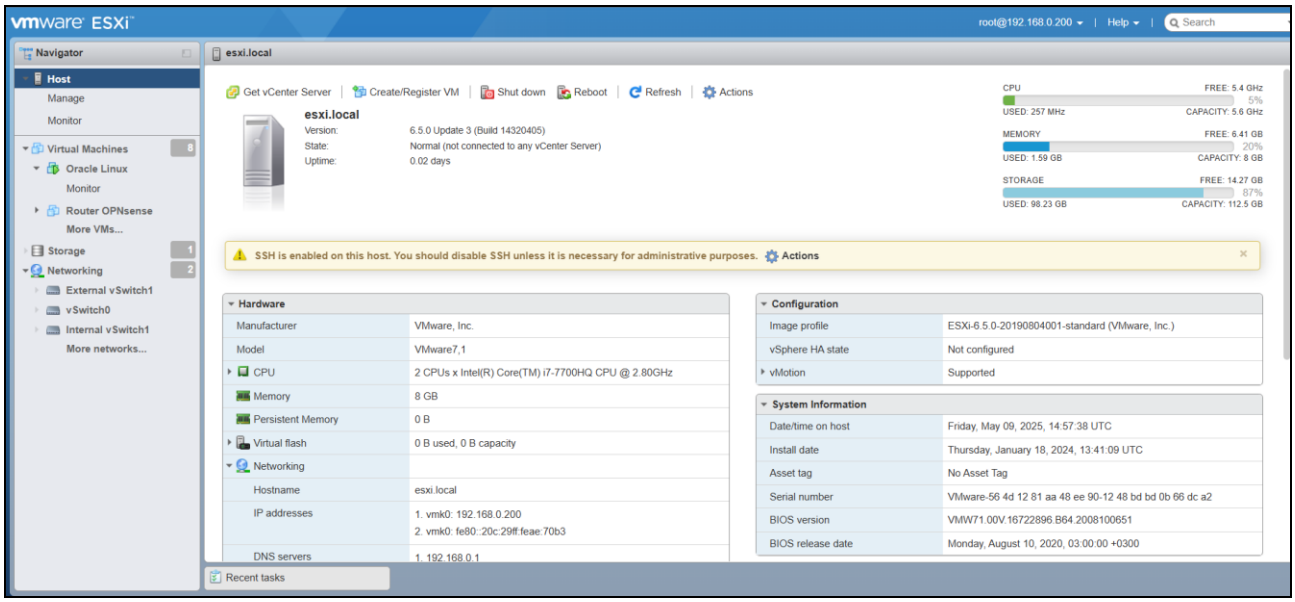

Рисунок 2.2 – Вебпанель керування VMware ESXi

Адміністратор має змогу запускати, зупиняти, клонувати віртуальні машини, переглядати системні логи, створювати шаблони, змінювати параметри ресурсів і оперативно перемикатися між мережевими сценаріями. Це спрощує керування середовищем і дозволяє швидко реагувати на потреби тестування або зміни топології. ESXi підтримує створення знімків стану (snapshots), що дозволяє зберегти поточний стан системи перед виконанням критичних змін або запуском небезпечного коду. У випадку збоїв або

небажаних наслідків адміністратор може швидко повернути систему до попереднього стабільного стану, що є надзвичайно корисним під час симуляції атак чи тестування оновлень NGFW.

Підтримка апаратної віртуалізації, зокрема технологій Intel VT-x та AMD-V, є критичним компонентом сучасних платформ віртуалізації, таких як VMware ESXi. Ці апаратні функції вбудовані на рівні центрального процесора й забезпечують можливість ефективного запуску віртуальних машин із мінімальними накладними витратами, вищою продуктивністю та кращою ізоляцією гостьових середовищ. У традиційній (програмній) віртуалізації гіпервізору необхідно було перехоплювати й емітувати всі інструкції гостьової операційної системи, які могли вплинути на апаратні ресурси. Це створювало суттєве навантаження на систему, призводило до втрати продуктивності й обмежувало функціональність гостьових ОС. З появою апаратної віртуалізації виробники процесорів надали механізми, які дозволяють гіпервізору безпосередньо делегувати виконання критичних інструкцій процесору без потреби в їхній емуляції.

Технологія Intel VT-x надає набір інструкцій і апаратні розширення, що дозволяють створювати середовище, у якому гостьова ОС вважає, що працює безпосередньо на фізичному обладнанні [20]. Основною складовою VT-x є механізм VMX (Virtual Machine Extensions), який дозволяє процесору перемикатися між двома режимами - VMX root (для гіпервізора) і VMX non-root (для гостьових систем). Завдяки цьому гіпервізор може запускати віртуальні машини майже без накладних витрат, а також перехоплювати лише ті події, які дійсно вимагають його втручання - наприклад, доступ до апаратних пристроїв, зміна таблиць сторінок тощо. Аналогічно, технологія AMD-V реалізує апаратну підтримку віртуалізації на процесорах AMD [21]. Вона базується на SVM (Secure Virtual Machine) - наборі розширень, що забезпечують подібний поділ привілеїв між гіпервізором та гостьовими ОС. AMD-V, як і Intel VT-x, дозволяє уникнути накладних витрат програмної

віртуалізації, значно зменшуючи затримки при обробці системних викликів і прискорюючи загальну роботу віртуальної машини.

У контексті VMware ESXi підтримка VT-x або AMD-V є обов'язковою вимогою для запуску сучасних гостьових систем, особливо тих, що потребують високої продуктивності або використовують складні архітектурні механізми. Більше того, апаратна віртуалізація дозволяє запускати nested virtualization - тобто розгортання гіпервізора всередині віртуальної машини. Це особливо важливо в тестових лабораторіях, де досліджується робота NGFW або інших мережевих сервісів у багаторівневих топологіях. Для коректної роботи VT-x або AMD-V в BIOS/UEFI налаштуваннях хост-системи обов'язково має бути активована відповідна функція, як правило позначена як Intel Virtualization Technology або SVM Mode. Без її увімкнення гіпервізор не зможе запускати віртуальні машини, що потребують повноцінного доступу до апаратних ресурсів.

Завдяки цим технологіям сучасні платформи віртуалізації, включно з VMware ESXi, змогли досягти рівня продуктивності, який майже не поступається роботі систем на фізичному обладнанні, забезпечити високу стабільність, покращити управління пам'яттю через механізми EPT/SLAT, а також гарантувати безпечну ізоляцію між віртуальними машинами - що критично важливо в тестових середовищах для дослідження кіберзахисту.

Завдяки усім цим можливостям, VMware ESXi є ідеальним вибором для побудови тестового середовища. Він забезпечує ізольованість, гнучкість конфігурації, стабільність роботи та широкі можливості для моделювання складних мережевих сценаріїв.

2.3 Маршрутизатор OPNsense

OPNsense - це потужний модульний маршрутизатор та брандмауер, який базується на операційній системі FreeBSD і є форком популярного проєкту pfSense [22]. Вперше представлений у 2015 році компанією Deciso, OPNsense

швидко здобув популярність серед спільноти мережевих адміністраторів завдяки поєднанню високого рівня безпеки, сучасного веб-інтерфейсу керування та активної підтримки.

Архітектурно OPNsense реалізований як повноцінна мережева операційна система, призначена для використання на апаратних пристроях шлюзів безпеки, віртуальних машинах або серверних платформах. Він підтримує роботу з різними інтерфейсами, VLAN, тунельними протоколами та VPN, забезпечуючи широкі можливості для побудови як простих, так і складних мережевих топологій. Завдяки мікромодульному підходу, користувач може встановлювати тільки ті компоненти, які необхідні для конкретної задачі - від звичайного NAT-маршрутизатора до повноцінного NGFW із DPI, IDS/IPS [23], проксі, captive portal і моніторингом трафіку.

OPNsense має інтуїтивно зрозумілий вебінтерфейс, який дозволяє адміністратору повністю керувати всіма параметрами системи (див. рисунок 2.3).

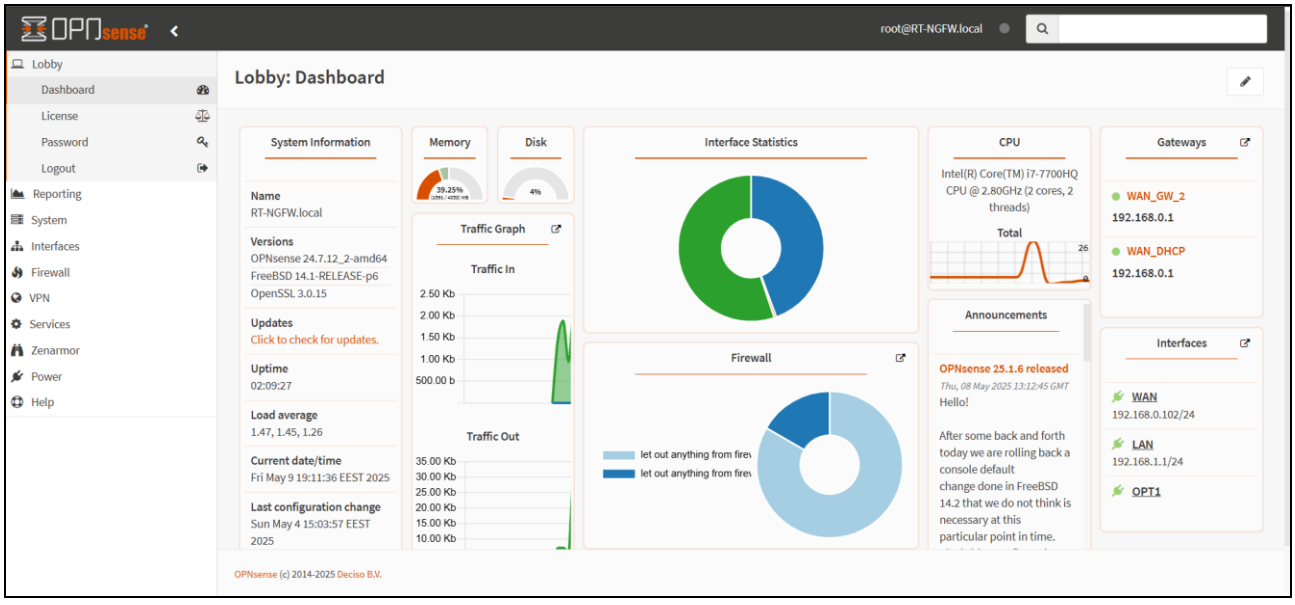

Рисунок 2.3 – Вебінтерфейс керування OPNsense

Вебінтерфйс дозволяє налаштовувати правила фільтрації трафіку (брандмауер PF), таблиці маршрутизації, параметри інтерфейсів, VPN-

з’єднання, DHCP-сервер, SNMP, QoS (Traffic Shaper), динамічний DNS, моніторинг у режимі реального часу, резервне копіювання та оновлення.

Однією з найважливіших функцій є брандмауер, заснований на PF - потужному та надійному механізмі фільтрації пакетів, що забезпечує контроль вхідного, вихідного та міжмережевого трафіку на основі заданих правил. Адміністратор може створювати політики, що базуються на IP-адресах, портах, протоколах, інтерфейсах або комбінаціях критеріїв, з можливістю пріоритизації трафіку, ведення журналів, створення груп, макросів, правил NAT та переадресації портів. OPNsense також має інтегровану підтримку VPN-сервісів, включаючи IPsec, OpenVPN, WireGuard. Це дозволяє створювати як віддалені доступи для працівників, так і захищені тунелі між філіями компанії або хмарною інфраструктурою. Конфігурація VPN здійснюється через графічний інтерфейс з системою аутентифікації, сертифікатами, групами користувачів та ключами.

Завдяки відкритій структурі, OPNsense активно підтримує розширення через плагіни. Одним із найпоширеніших є Zenarmor - модуль NGFW. Zenarmor надає можливості аналізу HTTPS/HTTP, класифікації додатків, поведінкового моніторингу, блокує шкідливі запити, рекламу, трекери, а також збирає розширену статистику з візуалізацією через веб-інтерфейс. Zenarmor працює у прозорому режимі (без потреби в проксі), що значно спрощує інтеграцію у вже існуючі мережі [24].

У тестових або продуктивних середовищах OPNsense може працювати на фізичних пристроях, гіпервізорах або хмарних хостингах. У рамках тестування NGFW OPNsense виконує роль центрального маршрутизатора з функціями DPI та фільтрації трафіку між сегментами WAN та LAN. Вбудовані механізми NAT, DHCP, DNS-релей, графіки навантаження та логування дають змогу створити повноцінне середовище для відтворення сценаріїв атаки та аналізу реакції системи.

На рисунку 2.4 показано вебінтерфейс OPNsense у розділі Interfaces: Overview, де наведено перелік усіх мережевих інтерфейсів системи, їхній поточний стан, конфігурацію, IP-адреси, тип з'єднання та маршрути.

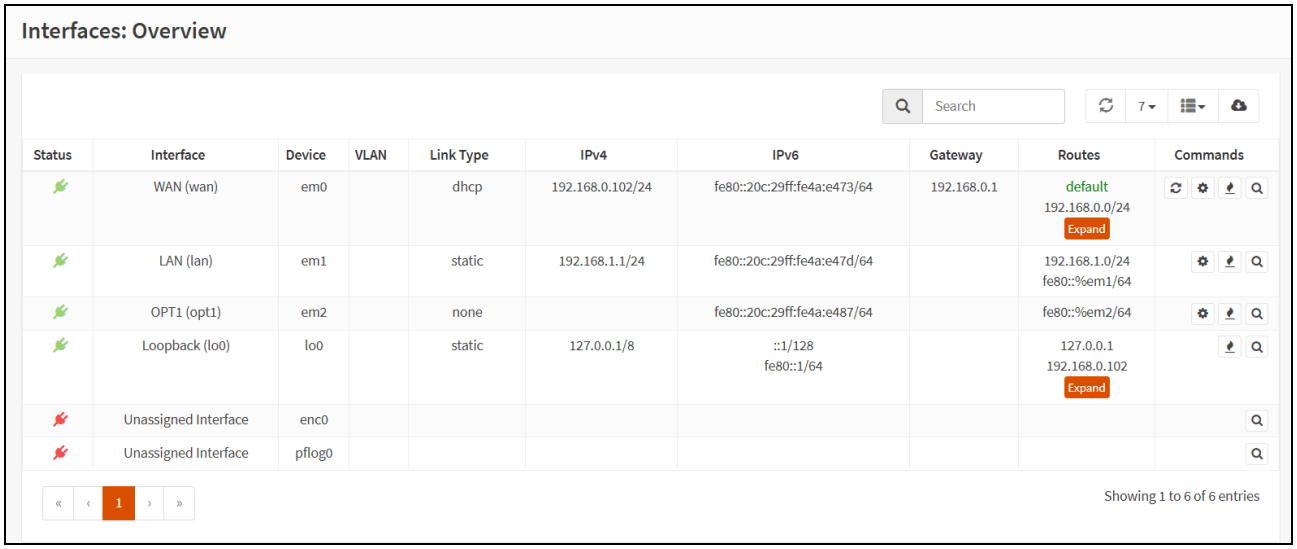

Рисунок 2.4 – Мережеві налаштування OPNsense

WAN-інтерфейс прив'язаний до мережевої плати em0 і використовує динамічну конфігурацію IP через DHCP. Він отримав адресу 192.168.0.102/24, а вказаним шлюзом виступає 192.168.0.1. LAN-інтерфейс (em1) налаштований статично і має адресу 192.168.1.1/24. Він слугує внутрішнім інтерфейсом для підключення локальних пристроїв.

Загалом, дана конфігурація демонструє типову двосегментну архітектуру: WAN для зовнішніх з'єднань і LAN для внутрішньої мережі, з можливістю подальшого розширення. Вона є ідеальною основою для побудови тестового середовища для перевірки роботи NGFW Zenarmor, фільтрацією трафіку та моніторингом безпеки в умовах, наближених до реального корпоративного середовища.

На рисунку 2.5 представлено конфігурацію DHCP-сервера в системі OPNsense для інтерфейсу LAN. DHCP - це служба, яка автоматично призначає IP-адреси клієнтам у мережі.

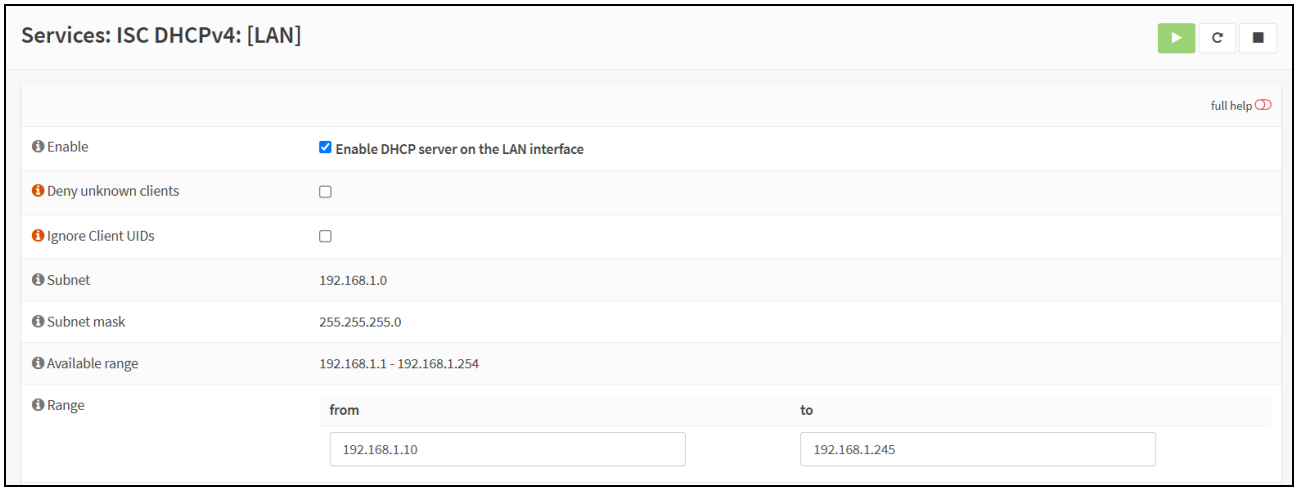

Рисунок 2.5 – Конфігурація DHCP-сервера в OPNsense

Значення в Available range відображає повний можливий діапазон для роздачі - тобто всі IP-адреси, що належать до мережі, окрім мережевої адреси (192.168.1.0) і широкомовної адреси (192.168.1.255), які зарезервовані. Проте фактично активний діапазон роздачі IP-адрес обмежено вручну до 192.168.1.10 – 192.168.1.245. Це дозволяє виключити з автоматичної роздачі адреси, які можуть бути зарезервовані для критичних пристроїв з фіксованими IP Опція Deny unknown clients залишена вимкненою, тобто DHCP-сервер надає IP-адреси будь-якому пристрою, що звертається до нього. Це зручно в тестовому середовищі, але може бути небезпечно в продуктивній мережі, оскільки дозволяє підключення будь-якого пристрою.

Налаштування DHCP на цьому етапі повністю відповідає базовим вимогам для формування стабільного середовища із динамічною роздачею адрес у LAN-сегменті. Завдяки чітко заданому діапазону IP, адміністратор зберігає контроль над адресним простором і має змогу уникнути конфліктів між статичними й динамічними адресами. Така конфігурація є типовою для внутрішніх корпоративних або навчальних мереж, де централізоване керування підключеннями клієнтів забезпечує зручність, масштабованість і безпеку.

На рисунку 2.6 представлено конфігураційне меню Unbound DNS у веб-інтерфейсі системи OPNsense, розділ General Settings.

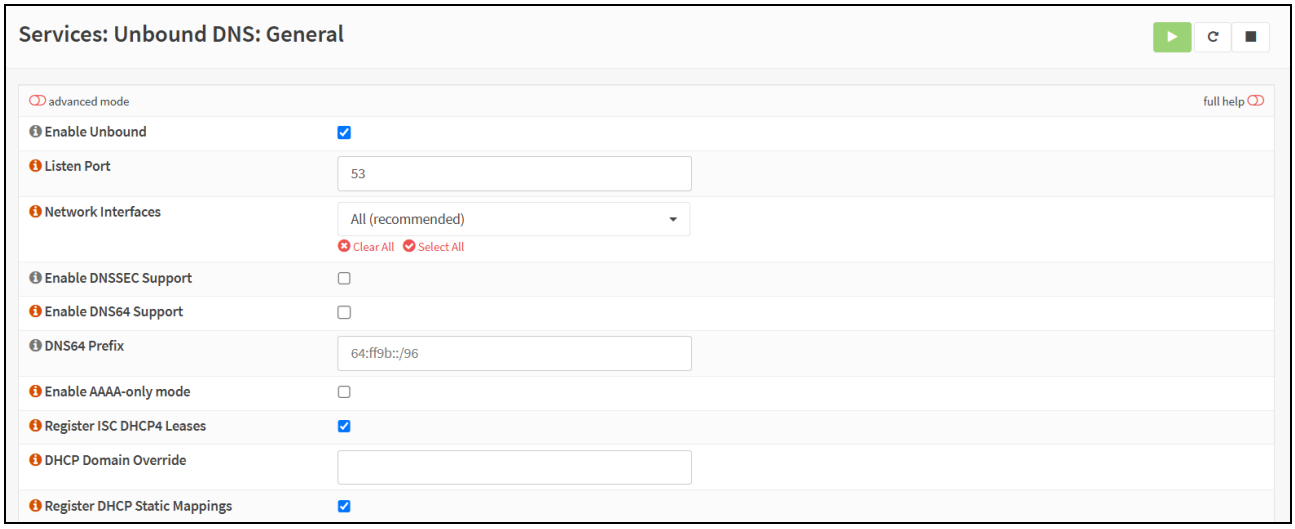

Рисунок 2.6 – Конфігурація Unbound DNS в OPNsense

Unbound DNS - це рекурсивний DNS-сервер, який дозволяє локально обробляти запити доменних імен для клієнтів у мережі без потреби у зовнішніх DNS. Це значно підвищує швидкодію, надає контроль над DNS-трафіком і дозволяє централізовано впроваджувати фільтрацію або перенаправлення запитів.

У поточній конфігурації DNS-сервер буде обробляти запити з усіх інтерфейсів, включаючи LAN. Це забезпечує гнучкість і гарантує, що запити з будь-якого підключеного пристрою в межах локальної мережі будуть оброблені коректно.

Важливими є активовані параметри Register ISC DHCP Leases та Register DHCP Static Mappings. Це означає, що Unbound автоматично реєструє у своїй локальній зоні DNS-імена пристроїв, які отримують IP-адреси через DHCP, а також ті, що мають статичні відповідники

Представлена конфігурація показує правильно налаштований DNS-сервер у внутрішньому LAN-сегменті. Він обслуговує DNS-запити з усіх інтерфейсів, використовує кешування, інтегрується з DHCP. Така реалізація є базовою, проте повністю функціональною для більшості внутрішніх мережевих середовищ, зокрема тестових для аналізу трафіку NGFW.

OPNsense є потужним, надійним і відкритим рішенням для створення гнучких систем мережевого захисту. Його глибока модульність, підтримка

сучасних технологій, стабільність і простота керування роблять його ідеальним вибором як для тестування, так і для використання в реальних умовах підприємств будь-якого масштабу.

2.4 Zenarmor як модуль NGFW в OPNsense

Zenarmor - це програмне розширення до OPNsense, яке надає розширену функціональність міжмережевого екрану нового покоління [25]. Його головна мета - перетворити класичний брандмауер на повноцінну інтелектуальну платформу для аналізу та контролю мережевого трафіку. Zenarmor працює у прозорому режимі без необхідності конфігурування проксі-сервера, що дозволяє йому здійснювати глибоку інспекцію трафіку на рівні додатків, не змінюючи архітектуру існуючої мережі.

На рисунку 2.7 представлено розділ System: Firmware у вебінтерфейсі OPNsense.

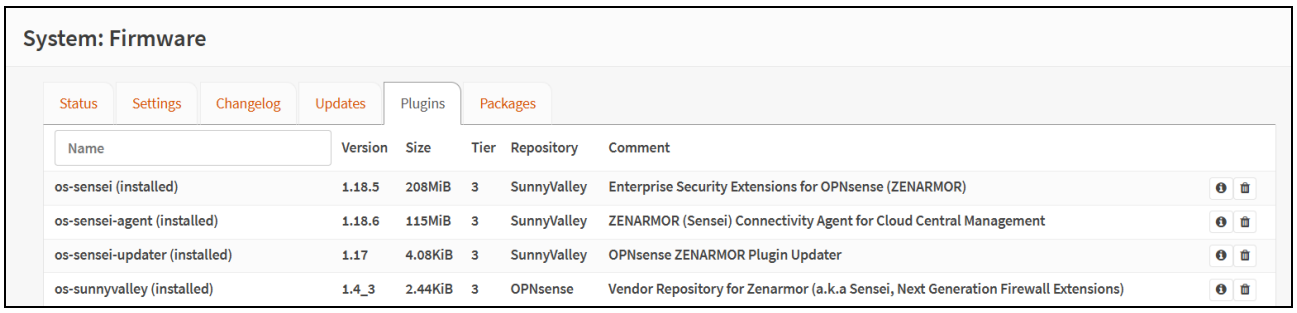

Рисунок 2.7 – System: Firmware в OPNsense

У вкладці Plugins відображено встановлені плагіни, що стосуються системи Zenarmor. Цей набір компонентів є основою для розгортання та стабільної роботи функціоналу NGFW на базі OPNsense.

Архітектура Zenarmor базується на спеціальних пакетах (модулях), які інтегруються безпосередньо у стек FreeBSD, що лежить в основі OPNsense. Zenarmor аналізує всі TCP/UDP з'єднання в реальному часі, розпізнає прикладні протоколи (наприклад, Facebook, YouTube, Dropbox, Telegram, BitTorrent тощо)

навіть у випадках, коли ці сервіси використовують нестандартні порти або шифрування. Таким чином, Zenarmor забезпечує контроль додатків (application visibility), що є однією з ключових характеристик NGFW.

Окрім DPI, Zenarmor виконує функції поведінкової аналітики, фільтрації за категоріями, блокування небажаних сайтів, реклами а також виявлення шкідливих активностей. Він надає детальну аналітику трафіку в режимі реального часу, з можливістю побудови графіків, перегляду топ-джерел і споживачів трафіку, активних сесій, геолокацій підключень і розподілу за типами сервісів.

Zenarmor інтегрується з DHCP та DNS-сервісами OPNsense, що дозволяє ідентифікувати пристрої в мережі не лише за IP-адресою, а й за іменем хоста. Це забезпечує додатковий рівень читабельності та контрольованості трафіку. Крім того, він підтримує створення розширених політик фільтрації, які можуть застосовуватись до окремих інтерфейсів, груп пристроїв або часових діапазонів. У більшості випадків DPI працює в LAN-сегменті, де OPNsense виступає в ролі шлюзу. Zenarmor не потребує окремих апаратних ресурсів, окрім вільного CPU і оперативної пам’яті. У режимі блокування він працює надзвичайно швидко та ефективно, оскільки оптимізований для FreeBSD.

Плагін os-sensei - це основний компонент Zenarmor, який містить всі базові модулі для роботи з DPI, аналітикою трафіку, категоризацією додатків і блокуванням контенту. Цей плагін відповідає за інтеграцію розширених функцій захисту рівня підприємства в систему.

Плагін os-sensei-agent - це агент взаємодії Zenarmor з централізованою хмарною платформою Sunny Valley, яка використовується для керування політиками, перегляду глобальної статистики, ліцензування, хмарного оновлення та інтеграції з іншими інсталяціями.

Плагін os-sensei-updater - це модуль, що відповідає за оновлення компонентів Zenarmor у фоновому режимі. Він слугує для синхронізації з офіційним репозиторієм, завантаження нових версій DPI-баз, сигнатур, фільтрів і самої програми

Плагін os-sunnyvalley додає до OPNsense доступ до плагінів від Sunny Valley Networks - розробника Zenarmor. Цей плагін відповідає за джерело всіх оновлень і пакетів, пов'язаних з NGFW-розширеннями.

Для зручності керування Zenarmor надає вебінтерфейс, інтегрований у OPNsense (див. рисунок 2.8).

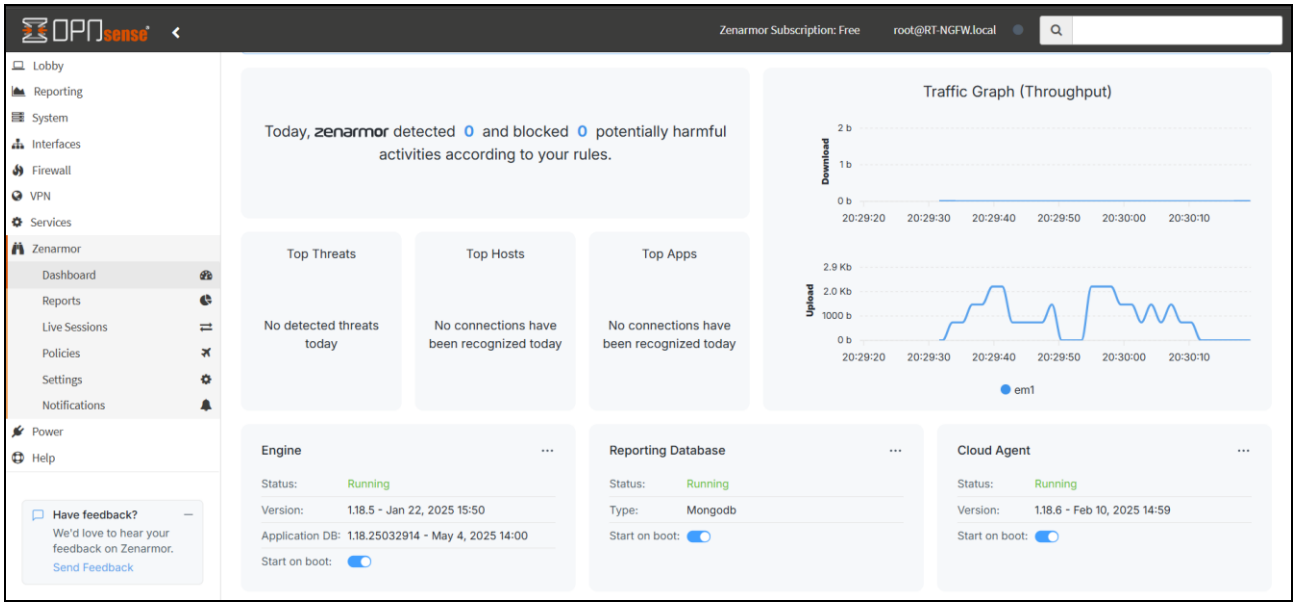

Рисунок 2.8 – Вебінтерфейс керування Zenarmor в OPNsense

Інтерфейс керування Zenarmor - це зручний та інформативний інструмент, що дозволяє візуалізувати стан кіберзахисту, спостерігати за навантаженням, ідентифікувати джерела потенційних загроз і керувати системою у реальному часі. У ньому реалізовано розділи для аналітики трафіку, перегляду сесій, налаштування політик, оновлення категорій загроз і створення списків виключень. Водночас користувач може створювати власні категорії блокування, дозволяти або забороняти доступ до певних сервісів або доменів.

Таким чином, Zenarmor - це повноцінне рішення NGFW, яке значно розширює можливості стандартного брандмауера OPNsense. Його використання в тестовому середовищі дозволяє моделювати та виявляти сучасні типи атак, аналізувати поведінку пристроїв у мережі, контролювати доступ до вебресурсів і оцінювати ефективність політик безпеки з точністю до

сесії або хоста. Це робить його незамінним інструментом для дослідників, аналітиків SOC і мережевих адміністраторів, що прагнуть мати під контролем кожен біт трафіку.

2.5 Операційна система Oracle Linux

Oracle Linux - це корпоративна операційна система на базі Red Hat Enterprise Linux, яку підтримує компанія Oracle. Вона розроблена з урахуванням високих вимог до стабільності, безпеки та масштабованості й зазвичай використовується на серверних платформах, у дата-центрах та хмарних середовищах [26]. Водночас Oracle Linux також може ефективно використовуватись як робоча станція - зокрема в тестових середовищах, лабораторіях інформаційної безпеки або у корпоративному IT-секторі, де потрібне середовище з високим рівнем контролю над системою.

Операційна система підтримує як класичне ядро Red Hat Compatible Kernel, так і вдосконалене ядро Unbreakable Enterprise Kernel, розроблене Oracle. Ядро від Oracle відрізняється покращеною продуктивністю, оптимізацією для роботи з базами даних, мережевими стеком і сучасними апаратними платформами. Для робочої станції це означає стабільну та швидку реакцію системи під навантаженням, ефективну підтримку багатоядерних процесорів, SSD-дисків та сучасних драйверів. Як робоче середовище Oracle Linux використовує GNOME, як сучасний інтерфейс користувача. Система надає повний набір базових утиліт, офісних програм, браузерів, інструментів розробки, а також підтримку багатьох додаткових програм, які можна встановити через менеджер пакетів DNF. Завдяки спільності з RHEL, користувач має доступ до великої кількості репозиторіїв, як офіційних, так і спільнотних.

У сфері інформаційної безпеки Oracle Linux може бути використаний як вузол у тестовому середовищі у сегменті LAN, для моделювання поведінки легітимного користувача, створення мережевого трафіку, запуску клієнтських

застосунків, тестування політик NGFW тощо. Система чудово взаємодіє з DHCP-серверами, DNS, що дозволяє швидко інтегрувати її в інфраструктуру OPNsense із Zenarmor.

На рисунку 2.9 показано вивід команди ifconfig та route -n, виконаних на робочій станції з операційною системою Oracle Linux.

```
[root@oracle9u4 /]# ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.101  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fe1a:174b  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:1a:17:4b  txqueuelen 1000  (Ethernet)
        RX packets 545457  bytes 826651896 (788.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 124288  bytes 9464352 (9.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 132  bytes 13138 (12.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 132  bytes 13138 (12.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@oracle9u4 /]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    100    0        0 ens160
192.168.1.0     0.0.0.0         255.255.255.0   U     100    0        0 ens160
[root@oracle9u4 /]#
```

Рисунок 2.9 – Вивід команди ifconfig та route -n в Oracle Linux

Дані команди надають детальну інформацію про стан мережевих інтерфейсів і таблицю маршрутизації. Ця конфігурація підтверджує, що робоча станція Oracle Linux успішно інтегрована в мережеву інфраструктуру в сегменті LAN, отримала IP-адресу з діапазону, що роздається DHCP-сервером на OPNsense, має зв’язок з локальним маршрутизатором і здатна здійснювати вихід в Інтернет через шлюз.

2.6 Висновок до другого розділу

В другому розділі було здійснено проєктування архітектури та розгортання тестового середовища призначеного для дослідження ефективності NGFW Zenarmor на основі маршрутизатор OPNsense. У ході проєктування було сформовано двосегментну мережеву інфраструктуру з логічним поділом на внутрішній та зовнішній сегменти, що відтворює реальні умови корпоративної мережі. Центральним компонентом архітектури виступає маршрутизатор OPNsense, який забезпечує маршрутизацію, фільтрацію трафіку, функції DHCP та DNS, а також інтеграцію модуля Zenarmor.

В якості платформи віртуалізації використано гіпервізор VMware ESXi, що надає високу стабільність, ізоляцію, підтримку апаратної віртуалізації та можливість гнучкого керування віртуальними машинами. Це дозволило створити незалежне, контрольоване середовище для моделювання мережевої взаємодії та перевірки механізмів захисту NGFW без загрози зовнішній інфраструктурі. В межах середовища розгорнуто робочу станцію на базі Oracle Linux, яка імітує легітимну активність користувача в LAN-сегменті. Завдяки використанню DHCP-сервера OPNsense забезпечено автоматичне конфігурування IP-параметрів клієнта. Особлива увага була приділена інтеграції Zenarmor, який виконує функції глибокого аналізу трафіку, класифікації додатків, виявлення потенційно шкідливої активності, ведення журналів та формування аналітики у режимі реального часу.

У результаті було реалізовано гнучке, масштабоване тестове середовище, здатне забезпечити повноцінний цикл перевірки роботи NGFW: від створення трафіку та моделювання загроз - до візуалізації результатів, що дозволяє ефективно аналізувати поведінку системи безпеки в умовах максимально наближених до реальних мереж.

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ NGFW

3.1 Налаштування NGFW Zenarmor

Налаштування NGFW Zenarmor в OPNsense - це процес інтеграції та конфігурації розширеного функціоналу мережевого захисту, який перетворює стандартний брандмауер OPNsense у повноцінний NGFW.

Після встановлення компонентів Zenarmor наступним етапом є первинне налаштування NGFW [27].

На рисунку 3.1 показано конфігураційне меню Zenarmor у вебінтерфейсі керування ZenConsole [28].

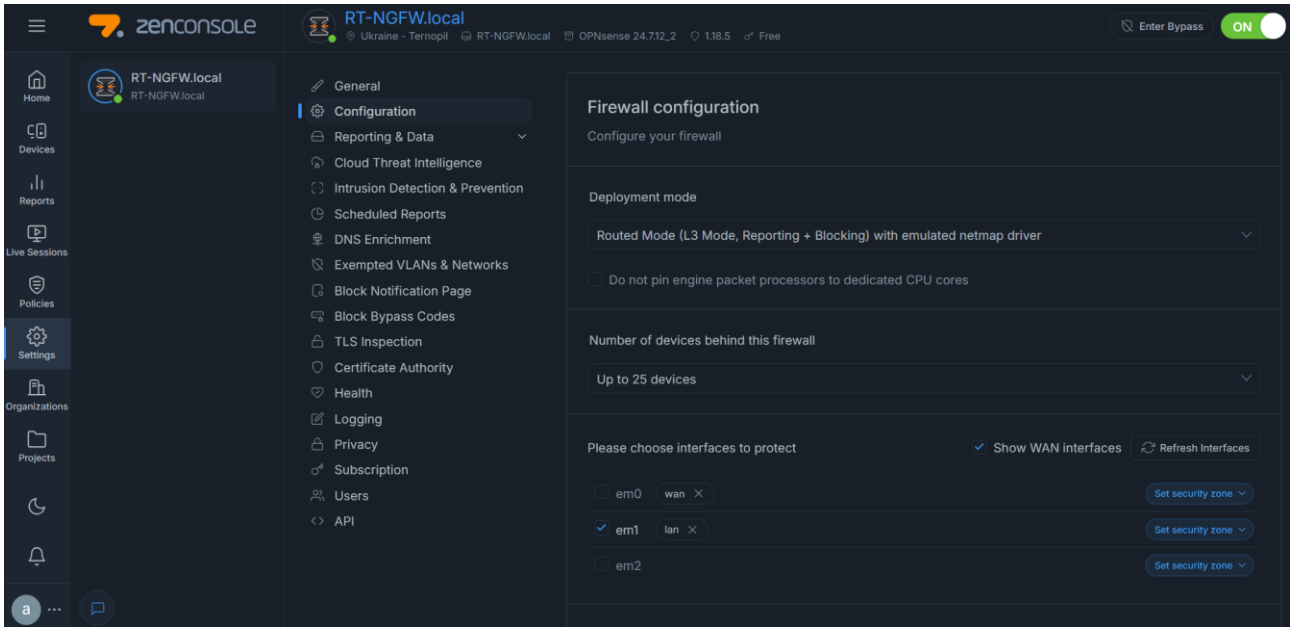

Рисунок 3.1 – Конфігураційне меню Zenarmor у вебінтерфейсі керування ZenConsole

Параметр Deployment mode встановлено на Routed Mode (L3 Mode, Reporting + Blocking) with emulated netmap driver, що означає, що Zenarmor працює у режимі маршрутизатора рівня 3 моделі OSI. У цьому режимі він має доступ до повного аналізу трафіку, дозволяє вести детальну аналітику та

здійснювати блокування з'єднань на основі політик безпеки. Використовується емулятор драйвера Netmap, що дозволяє Zenarmor інтегруватись із мережевим стеком FreeBSD без необхідності у фізичному мережевому розриві або bridge-режимі. При виборі інтерфейсів для захисту активовано лише інтерфейс em1, позначений як lan. Це внутрішній мережевий сегмент, де розташовані кінцеві пристрої, і саме через нього проходить основний користувацький трафік. Тому логічно, що саме його обрано як об'єкт для DPI, моніторингу та фільтрації. Інтерфейс em0, позначений як wan, не активовано. Це відповідає рекомендаціям Zenarmor щодо фокусування DPI на LAN, оскільки фільтрація вхідного трафіку з WAN зазвичай здійснюється через класичні правила брандмауера PF, а не через DPI. Окрім того, DPI на WAN може створити надлишкове навантаження або дублювання подій.

На рисунку 3.2 показано розділ Cloud Threat Intelligence, який є компонентом для підвищення рівня захисту в реальному часі за допомогою хмарної аналітики загроз.

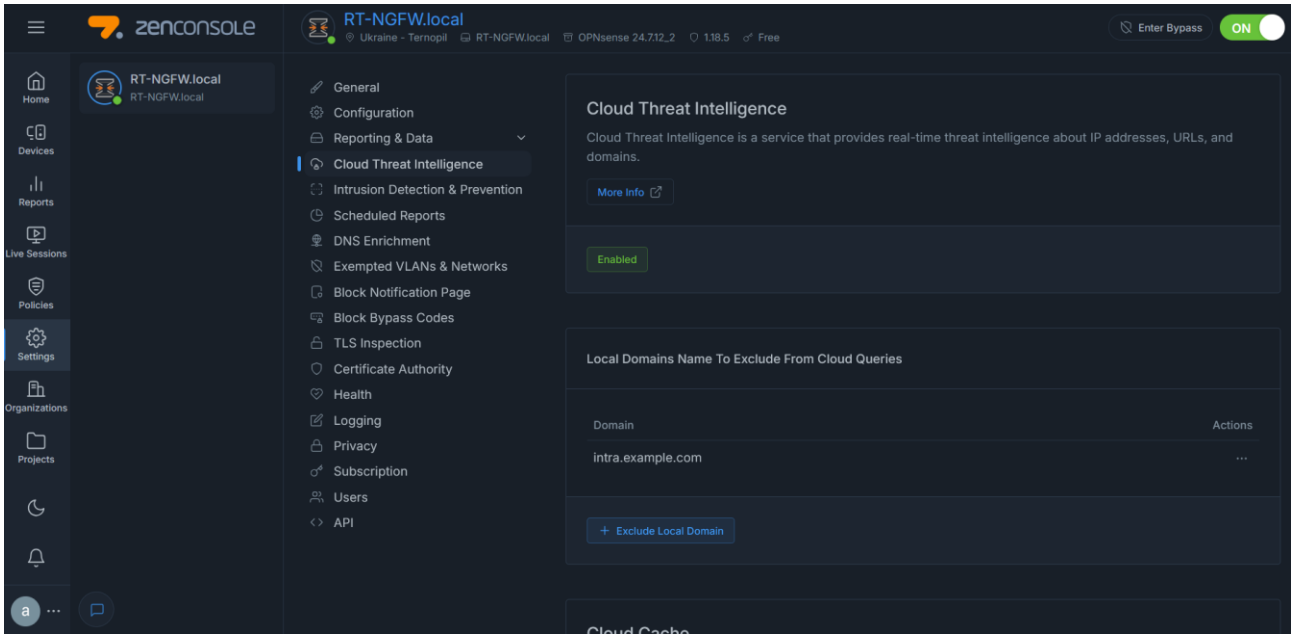

Рисунок 3.2 – Розділ Cloud Threat Intelligence у Zenarmor

Cloud Threat Intelligence є однією з ключових складових системи мережевої безпеки нового покоління, інтегрованої у Zenarmor. Вона забезпечує

розширений рівень захисту, використовуючи хмарні аналітичні механізми для оцінки репутації IP-адрес, доменів і URL в режимі реального часу. Цей сервіс, відомий як Zenarmor Cloud, побудований на основі масштабованої інфраструктури Google Cloud і здатен обробляти мільйони запитів щодня з усього світу, забезпечуючи миттєву реакцію на нові загрози, шкідливі вебресурси, фішингові кампанії та аномальну активність в мережі.

Під час кожного звернення пристрою з внутрішньої мережі до зовнішнього ресурсу, Zenarmor перехоплює мережевий потік і виконує його перевірку за допомогою розподілених хмарних серверів, розташованих у Північній Америці, Європі, Азії та Австралії. Інформація про запитану IP-адресу або домен порівнюється з базою знань, що постійно оновлюється за допомогою штучного інтелекту, машинного навчання [29] та даних, отриманих від партнерів, комерційних аналітичних провайдерів, власного SOC та зворотного зв’язку від користувачів. У залежності від поточного рейтингу репутації, категорії ресурсу і встановлених політик безпеки, система вирішує - дозволити, блокувати або журналювати доступ до вказаного ресурсу.

Сама взаємодія між Zenarmor і Zenarmor Cloud відбувається через захищене власне з’єднання з використанням UDP портів 5353, 5355 і 3478, а передача даних шифрується за допомогою протоколу AES-256 [30]. Особливу увагу приділено конфіденційності. Запити не містять персональних даних, а зібрана інформація автоматично очищується після обробки та зберігається не більше семи днів. Вся політика обробки даних відповідає вимогам GDPR і CCPA.

Усі версії Zenarmor, включно з безкоштовною, мають доступ до базового рівня Zenarmor Cloud. Інтерфейс керування Zenarmor дозволяє адміністратору налаштовувати параметри хмарної репутації, вмикати або вимикати механізм класифікації, очищати кеш запитів, додавати винятки для локальних доменів, які не потребують перевірки, а також вибирати оптимальний географічний регіон хмарного сервера для мінімізації затримок. Уся ця екосистема формує високоефективну платформу для превентивного захисту корпоративної мережі.

Zenarmor Cloud не лише виявляє загрози - він аналізує поведінку, класифікує контент, оптимізує політики, і робить це без перерв і затримок, використовуючи обчислювальні можливості хмари для масштабованого аналізу. У результаті адміністратор отримує динамічний, завжди актуальний механізм фільтрації, який дозволяє керувати мережею з позиції повного контролю і розуміння поточних ризиків.

На рисунку 3.3 показано розділі Block Bypass Codes, який дозволяє створювати спеціальні обхідні коди для доступу до сторінок або ресурсів, які були заблоковані відповідно до встановлених політик фільтрації.

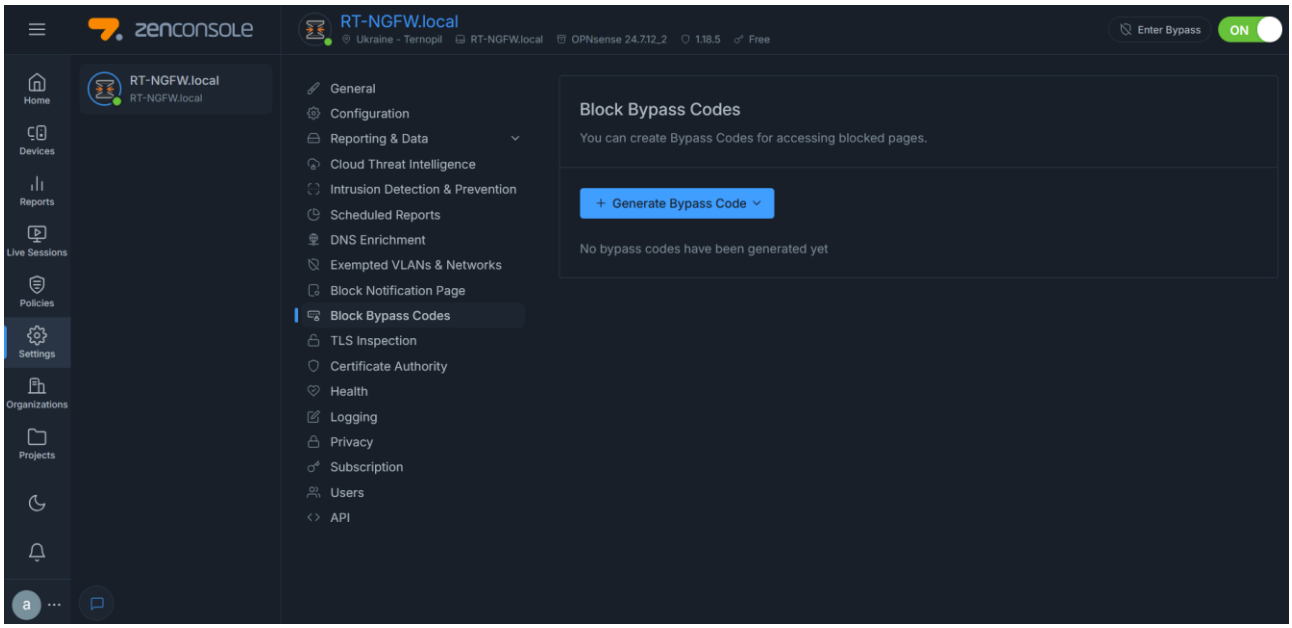

Рисунок 3.3 – Розділ Block Bypass Codes у Zenarmor

Функціональність Block Bypass Codes реалізується через генерацію унікальних кодів. Після створення код може бути переданий користувачу або технічному персоналу, який має обґрунтовану потребу в доступі до певного ресурсу. Це може бути корисно в ситуаціях, коли сайт помилково заблокований через категоризацію, але потрібен для робочих цілей, або ж коли обмеження потрібно тимчасово зняти для діагностики, тестування чи навчання.

На рисунку 3.4 показано розділ Policies у Zenarmor, який надає засоби керування політиками фільтрації трафіку.

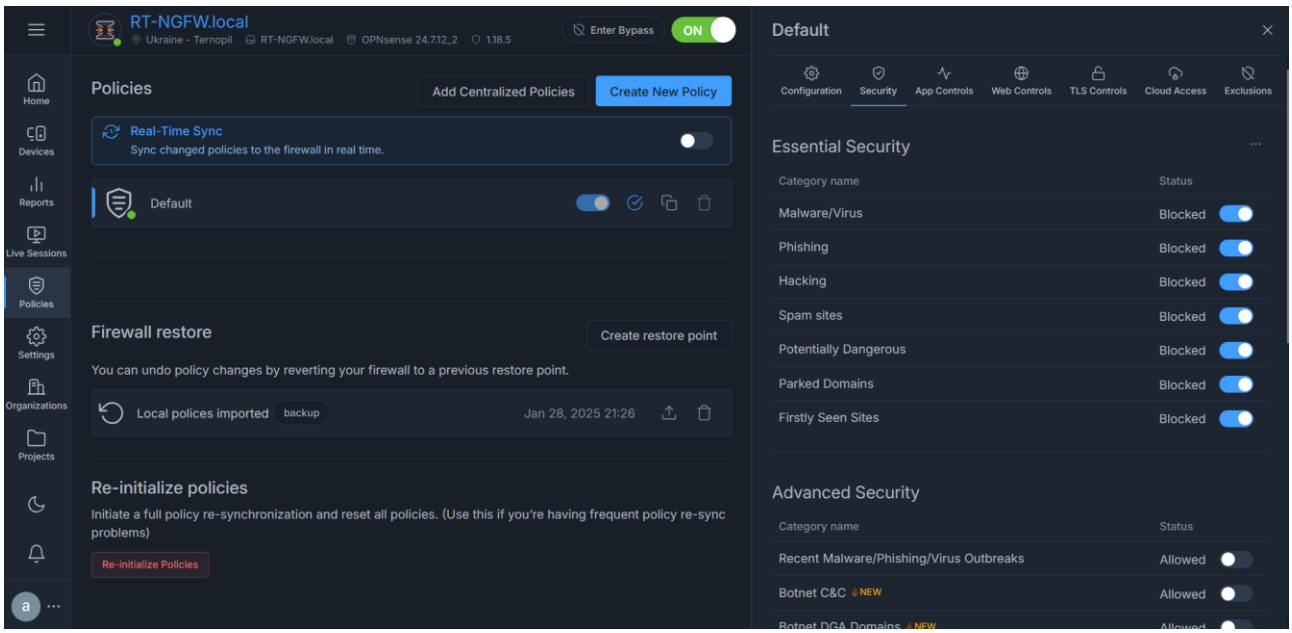

Рисунок 3.4 – Інтерфейс керування політиками фільтрації трафіку у Zenarmor

Вкладка Security відповідає за основні параметри безпеки. Тут активовано блокування для широкого спектру критичних категорій, таких як шкідливе ПЗ (Malware/Virus), фішинг (Phishing), хакінг (Hacking), спам-ресурси, потенційно небезпечні сайти, запарковані домени та ресурси, що вперше з'явилися в мережі. Це означає, що будь-який трафік, який відповідає цим категоріям, буде автоматично заблокований Zenarmor. Таким чином забезпечується високий рівень захисту від найпоширеніших класів загроз. Розділ Advanced Security, який включає більш специфічні категорії - наприклад, виявлення нових спалахів шкідливих програм або фішингових кампаній, ботнет-активність (C&C), домени, створені алгоритмічно (DGA), та інші загрози.

На рисунку 3.5 представлено вкладку App Controls у політиці фільтрації Zenarmor. Цей розділ дозволяє адміністратору керувати доступом до програмних категорій та сервісів на прикладному рівні.

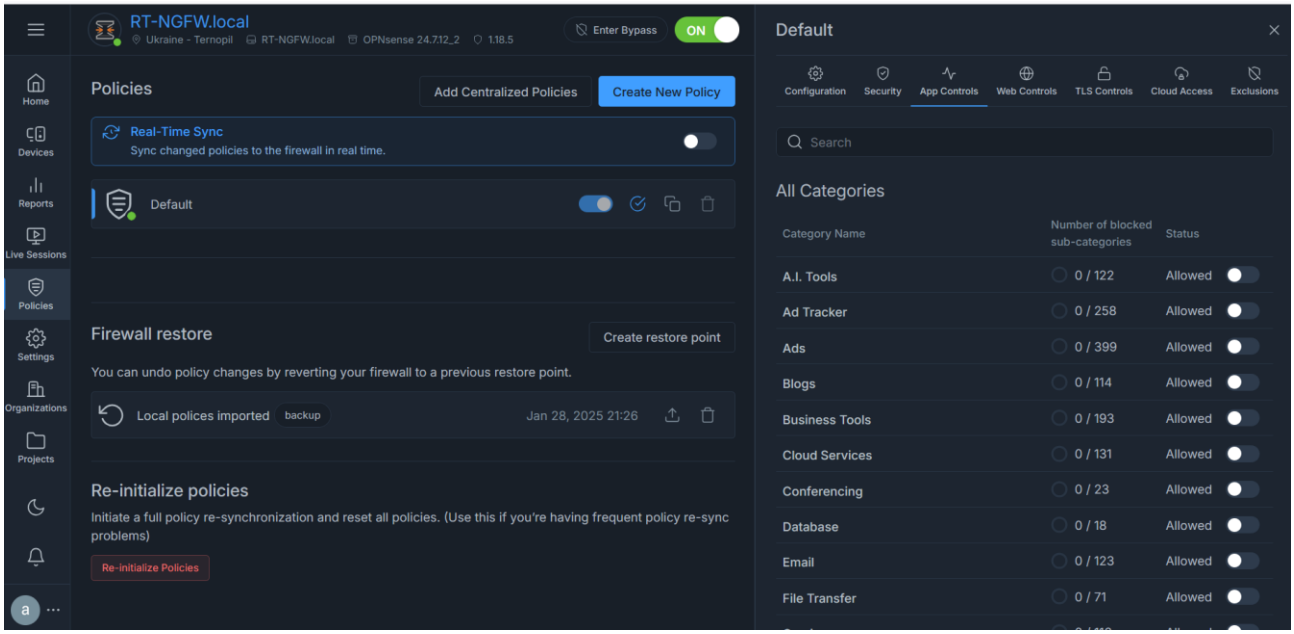

Рисунок 3.5 – Розділ App Controls у Zenarmor

У списку справа відображено перелік категорій додатків, до яких належать інструменти штучного інтелекту, трекери реклами, рекламні платформи, блоги, бізнес-додатки, хмарні сервіси, засоби конференцзв’язку, поштові клієнти, бази даних, сервіси передачі файлів тощо. Кожна категорія містить інформацію про загальну кількість підкатегорій та кількість тих, що заблоковані. У разі необхідності адміністратор має можливість швидко активувати блокування будь-якої категорії або окремих підкатегорій, натиснувши перемикач статусу. Це дозволяє миттєво обмежити доступ до конкретних класів застосунків, наприклад, до всіх інструментів передачі файлів, засобів конференцзв’язку чи комерційної реклами.

Інтерфейс App Controls надає інструменти для реалізації application-aware фільтрації трафіку, що є однією з основних відмінностей між традиційними брандмауерами та NGFW. Він дозволяє здійснювати контроль не лише за IP-адресами чи портами, а й за типами додатків, протоколами прикладного рівня та користувацькою активністю. Це особливо корисно у складних корпоративних мережах, де потрібен детальний контроль над тим, які саме сервіси дозволено використовувати працівникам, а які слід обмежити з міркувань безпеки, продуктивності або політики організації.

На рисунку 3.6 представлено розділ Web Controls у конфігурації політик Zenarmor, що дозволяє управляти доступом до вебконтенту через категоризацію сайтів.

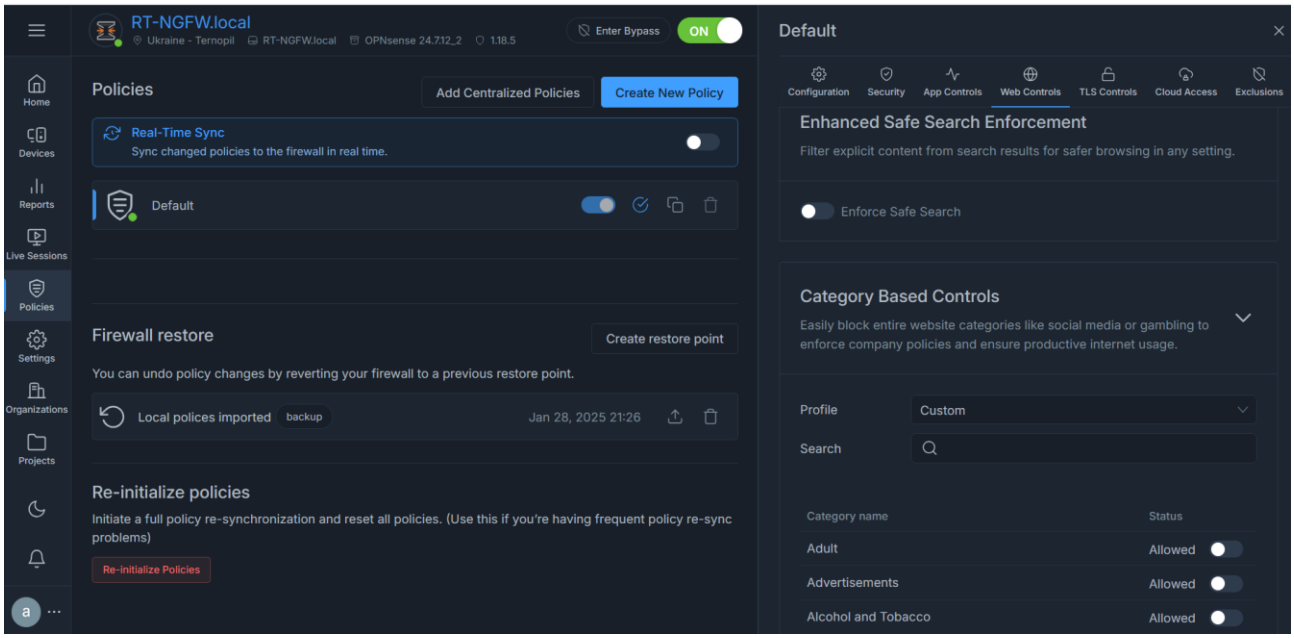

Рисунок 3.6 – Розділ Web Controls у Zenarmor

У верхній частині відображено модуль Enhanced Safe Search Enforcement, який відповідає за активацію фільтрації небажаного контенту в результатах пошукових систем, зокрема Google, Bing або YouTube. Це дозволяє обмежити відображення матеріалів для дорослих та інших небажаних тем при стандартному використанні інтернету. Основну частину інтерфейсу займає секція Category Based Controls, яка дозволяє адміністратору блокувати або дозволяти цілі категорії вебсайтів. У списку нижче видно кілька категорій, таких як Adult, Advertisements та Alcohol and Tobacco.

Zenarmor надає можливість змінити статус кожної категорії та дозволяє миттєво заблокувати всі сайти, які належать до певної тематики. Це забезпечує гнучке реагування на зміни в інформаційній політиці компанії або виявлені інциденти. Наприклад, у навчальних установах або організаціях із жорсткими вимогами до етики інтернет-доступу категорії Adult, Gambling, Drugs або Social Media можуть бути повністю заблоковані.

Цей механізм є частиною широкої системи контентної фільтрації, яка базується на хмарній базі знань Zenarmor і дозволяє виявляти не лише конкретні сайти, а й цілі доменні зони, IP-адреси та ресурси, які постійно оновлюються. Завдяки цьому адміністратор може забезпечити високий рівень захисту від небажаного контенту без необхідності вручну додавати сайти до чорного списку.

На рисунку 3.7 представлено інтерфейс налаштування виключень у політиці фільтрації трафіку Zenarmor.

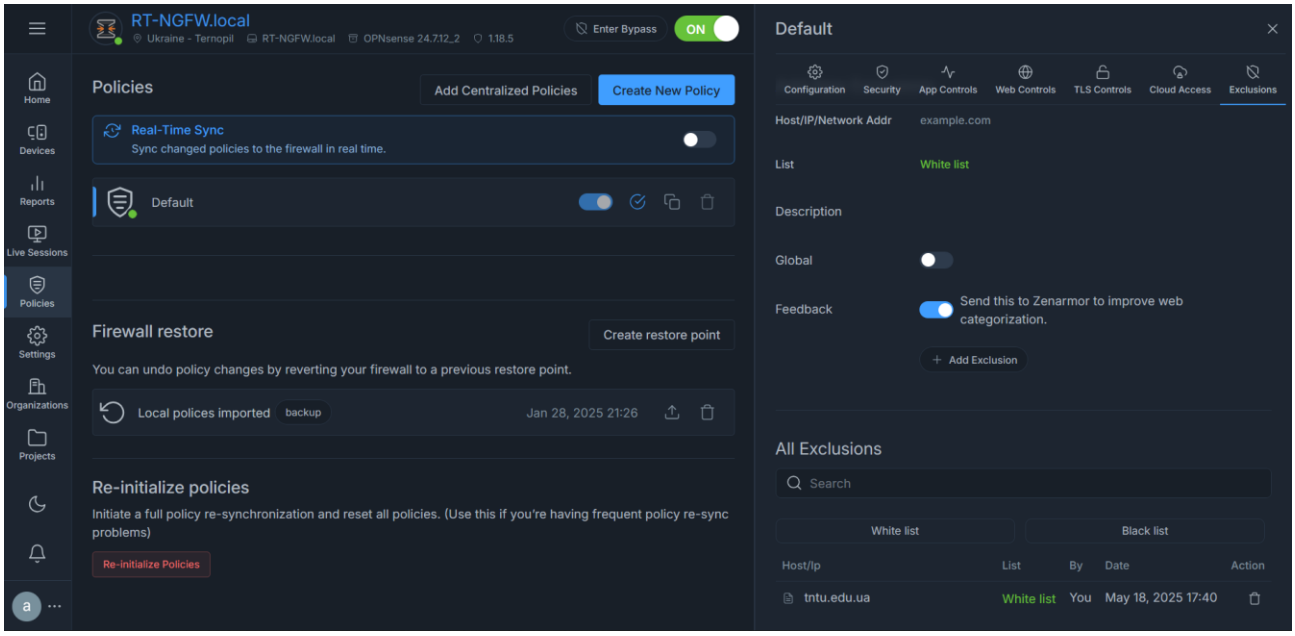

Рисунок 3.7 – Інтерфейс налаштування виключень у Zenarmor

Розділ Exclusions дозволяє адміністратору створювати так звані білі та чорні списки - переліки доменів, IP-адрес або мереж, які мають бути або завжди дозволені, або завжди заблоковані, незалежно від загальних політик фільтрації. У розділі All Exclusions показано поточний активний запис. Домен tntu.edu.ua внесено до White list вручну користувачем. Цей механізм критично важливий для уникнення випадкових блокувань легітимних сайтів або забезпечення стабільного доступу до корпоративних сервісів. Крім того, він дозволяє швидко реагувати на інциденти, коли окремі сайти були некоректно класифіковані або помилково заблоковані, зберігаючи баланс між безпекою та функціональністю.

Конфігурація, показана на зображеннях, демонструє базову, але функціонально завершену інсталяцію Zenarmor. Вона повністю відповідає вимогам до тестового середовища для оцінки ефективності NGFW, забезпечуючи гнучке масштабування, зручне адміністрування і потужну платформу для подальшого аналізу трафіку, створення політик та виявлення аномалій.

3.2 Тестування NGFW Zenarmor

Тестування NGFW Zenarmor в OPNsense проводиться з метою оцінки його здатності виявляти, аналізувати та блокувати потенційно небезпечні дії в мережі в умовах, максимально наближених до реальних. Це включає перевірку роботи механізмів DPI, категоризації трафіку, виявлення шкідливих ресурсів, блокування фішингових сайтів, небажаних додатків, а також загроз, що маскуються під легітимну активність.

У тестовому середовищі, розгорнутому на базі VMware ESXi, було створено повноцінну віртуальну мережу з двома сегментами: WAN та LAN. У ролі NGFW виступає маршрутизатор на базі OPNsense із встановленим і налаштованим модулем Zenarmor. До внутрішнього сегмента підключено робочу станцію з ОС Oracle Linux, яка використовується для моделювання поведінки типового користувача - ініціації вихідних з’єднань, доступу до різних категорій сайтів і генерування легітимного трафіку.

Для перевірки ефективності NGFW Zenarmor в OPNsense у частині фільтрації фішингових сайтів було використано відкрите репутаційне джерело PhishTank [31]. Цей сервіс підтримується спільнотою і містить актуальний список підтверджених фішингових URL-адрес, які постійно оновлюються. Дані з PhishTank були використані для моделювання реальних атак з метою тестування функцій виявлення та блокування шкідливих веб-ресурсів.

На рисунку 3.8 представлено вебінтерфейс сайту PhishTank із переліком активних підтверджених фішингових URL-адрес.

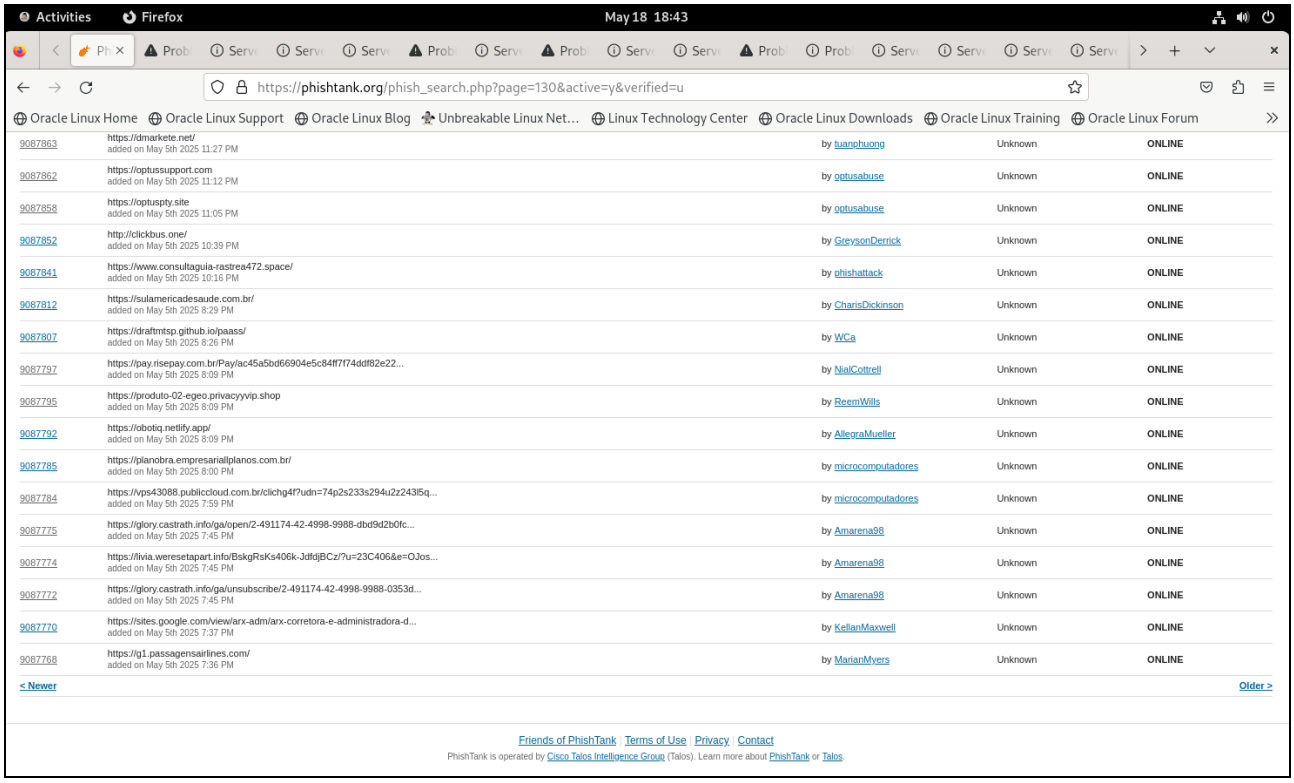

Рисунок 3.8 – Вебінтерфейс сайту PhishTank

Для цілей тестування NGFW Zenarmor цей список фішингових посилань використовується як репрезентативне джерело загроз. На тестовій машині з Oracle Linux у сегменті LAN пробували відкрити ці URL-адреси через браузер.

Zenarmor, працюючи в режимі DPI [32] і маючи активовану функцію Cloud Threat Intelligence, аналізує запити до доменів у реальному часі. Якщо домен або IP-адреса запиту відповідає сигнатурам або репутаційним записам з бази фішингових сайтів, з’єднання негайно блокується.

У вебінтерфейсі Zenconsole ця подія буде зафіксована в Live Sessions або Reports, з відповідною позначкою категорії, зазначенням IP-адреси клієнта, часу, URL, категорії ресурсу та дії (див. рисунок 3.9).

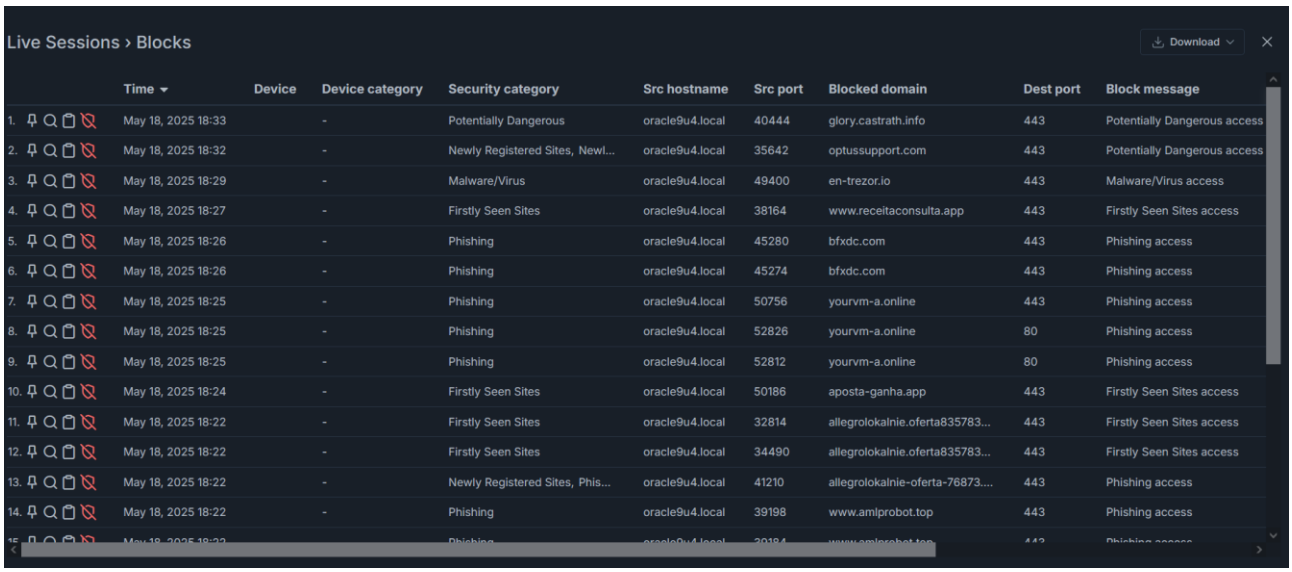

Рисунок 3.9 – Журнал Live Sessions у Zenarmor

На рисунку 3.10 представлено аналітичну панель звітування Zenarmor в інтерфейсі Zenconsole.

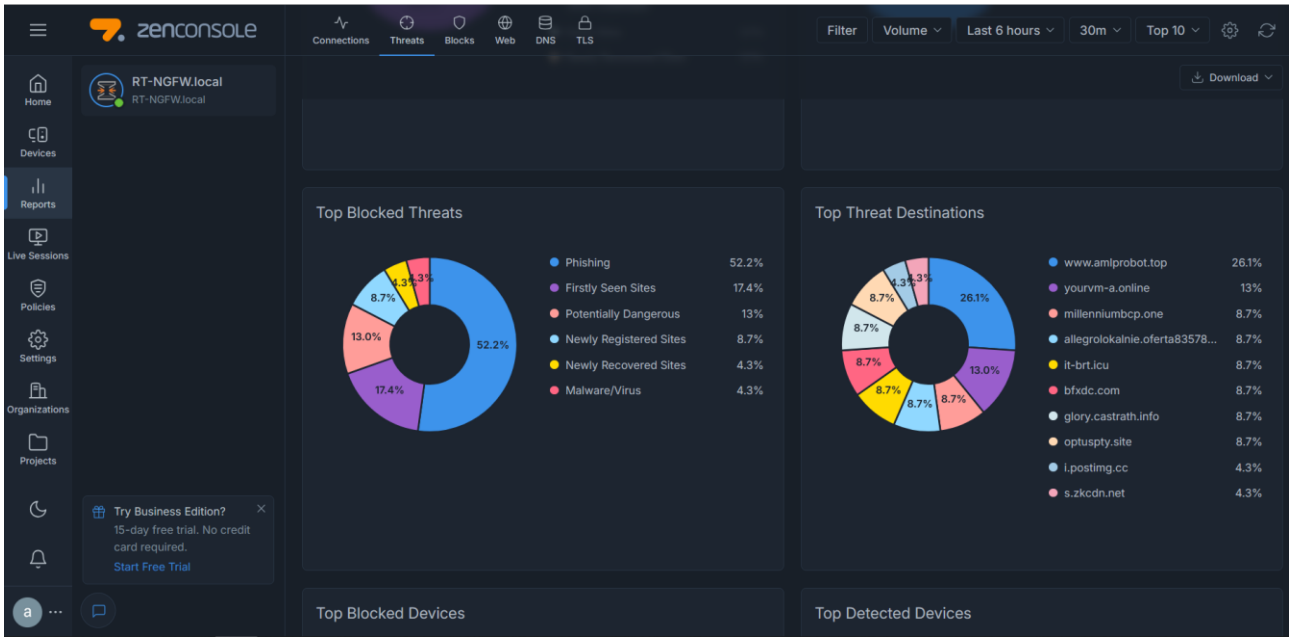

Рисунок 3.10 – Аналітична панель звітування Zenarmor

Інтерфейс демонструє розділ Threats, який візуалізує статистику заблокованих загроз за останні 6 годин. Сектор із заголовком Top Threat Destinations містить діаграму найпопулярніших доменів, які були визначені як загроза та до яких здійснювалися спроби доступу. Панель демонструє надійну

роботу NGFW Zenarmor у режимі DPI, аналітики загроз, класифікації сайтів і активної фільтрації шкідливих запитів. Це дозволяє не лише оперативно реагувати на нові типи загроз, а й бачити загальну тенденцію атак, джерела небезпеки та їхню категорію, що є важливим для аналітиків SOC [33].

На рисунку 3.11 представлено вкладку Blocks у вебінтерфейсі Zenconsole.

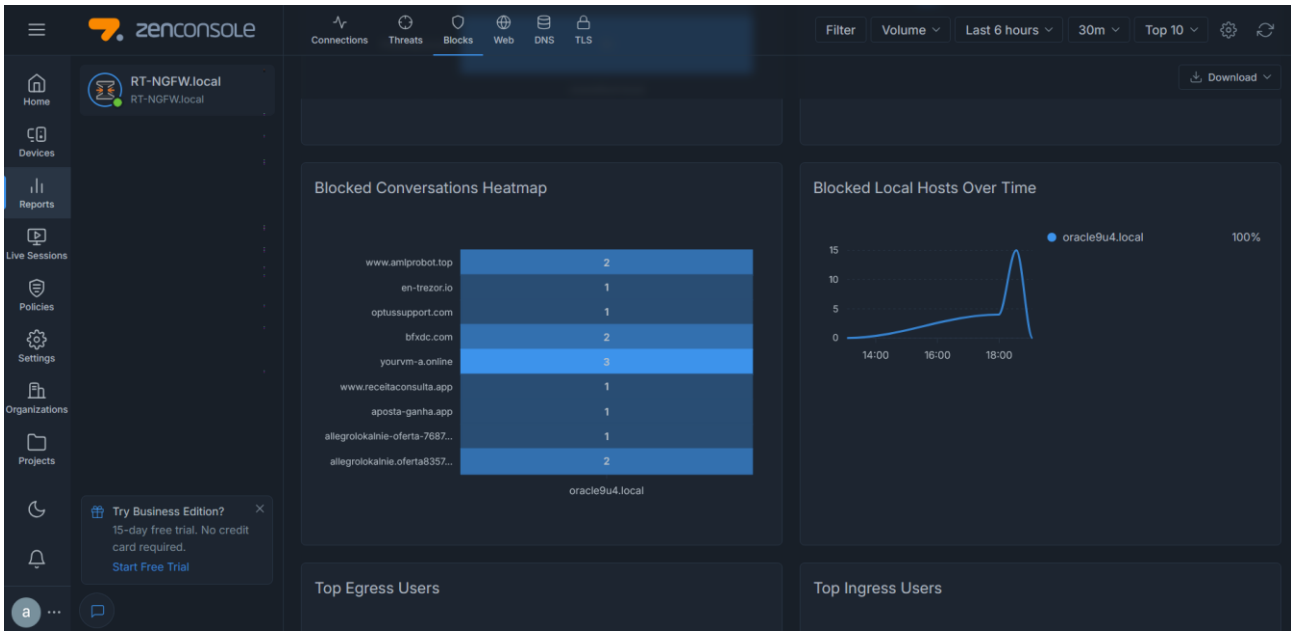

Рисунок 3.11 – Вкладка Blocks у вебінтерфейсі Zenconsole

Панель візуалізації розділена на два блоки, що дозволяє оцінити як інтенсивність блокувань за доменами, так і активність клієнтських пристроїв у часі. У лівій частині розташовано теплову карту заблокованих спроб з'єднання, яка показує перелік доменів, до яких було здійснено спробу підключення з локального вузла oracle9u4.local, і які були заблоковані механізмами фільтрації Zenarmor. У правій частині рисунку знаходиться графік, який відображає часову динаміку заблокованих підключень з боку локального пристрою. Увесь блокований трафік був з одного джерела - вузла oracle9u4.local, що, є клієнтською машиною в тестовому середовищі.

Такий результат демонструє, що тестування NGFW Zenarmor із використанням доменів з ресурсу PhishTank було успішним: небезпечні ресурси було виявлено, з'єднання заблоковано, а події зафіксовано для подальшого

аналізу. Це свідчить про здатність системи ефективно протистояти актуальним загрозам у мережі. Це також підтверджує ефективність налаштувань Zenarmor. Система успішно блокує шкідливі запити на основі категорій загроз у реальному часі, навіть для новостворених або ще не класифікованих доменів. Виявлені ресурси класифіковано як потенційно небезпечні або фішингові, і всі спроби доступу до них було припинено, що є свідченням належної роботи DPI, Cloud Threat Intelligence та політик безпеки.

3.3 Висновок до третього розділу

В третьому розділі було проведено практичну реалізацію та тестування міжмережевого екрану нового покоління Zenarmor у складі системи OPNsense, що дозволило всебічно оцінити його функціональність та ефективність. На етапі налаштування було здійснено конфігурацію основних параметрів Zenarmor: вибір режиму розгортання у Routed Mode із підтримкою емуляції Netmap-драйвера, активацію захисту для LAN-інтерфейсу, ввімкнення хмарного аналітичного модуля Cloud Threat Intelligence, налаштування категорій політик безпеки, керування програмними сервісами на рівні прикладного трафіку, вебфільтрацією за категоріями та створенням списків виключень. Було проведено тестування можливостей Zenarmor щодо виявлення та блокування загроз з використанням репутаційного джерела - PhishTank. Активні URL-адреси фішингових ресурсів було використано для моделювання сценарію доступу до шкідливих сайтів з робочої станції в LAN-сегменті. Після здійснення спроби підключення до фішингових ресурсів, Zenarmor, застосовуючи DPI та хмарну аналітику загроз, автоматично блокував з’єднання та реєстрував відповідні події в системному журналі. Результати аналізу Live Sessions, звітів та графіків показали, що Zenarmor коректно класифікував шкідливі домени за категоріями Phishing, Potentially Dangerous, Malware/Virus тощо. Візуалізація заблокованих доменів, часових діапазонів активності та розподілу загроз у вебінтерфейсі Zenconsole продемонструвала ефективність

механізмів реального часу, що дозволяють не лише фіксувати, а й оперативно реагувати на загрози.

Таким чином, отримані результати засвідчують, що Zenarmor NGFW у складі OPNsense є надійним рішенням для забезпечення мережевої безпеки. Його функціонал дозволяє впроваджувати політики доступу, контролювати застосунки, блокувати шкідливий трафік, виявляти загрози та здійснювати аналітику на основі актуальної інформації. В умовах тестового середовища інструмент виявив себе як високоефективний компонент захисту корпоративних мереж і довів свою здатність виявляти сучасні загрози без затримок.

РОЗДІЛ 4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при масивній зовнішній кровотечі

Масивна зовнішня кровотеча є надзвичайно небезпечним станом, який може призвести до серйозної загрози життю постраждалої особи. Невідкладна надання домедичної допомоги може врятувати життя і запобігти подальшій крововтраті.

Долікарська допомога постраждалим при кровотечі є важливою процедурою, яку можуть виконувати особи без медичної освіти.

Ознаками масивної зовнішньої кровотечі є будь-що з нижченаведеного:

- швидке, інтенсивне витікання крові з рани;
- пульсуючий характер кровотечі (кров б’є фонтаном);
- пляма крові біля постраждалого, яка швидко збільшується;
- значне просякнення одягу постраждалого кров’ю;
- порушення або втрата свідомості у постраждалого без ознак черепно-мозкової травми, при наявності зовнішньої кровотечі;
- бліда шкіра, холодні кінцівки тощо, при наявності зовнішньої кровотечі.

Наказ Міністерства охорони здоров'я України від 09.03.2022 р. № 441 " Про затвердження порядків надання домедичної допомоги особам при невідкладних станах" встановлює порядки надання домедичної допомоги постраждалим при при масивній зовнішній кровотечі. У цьому порядку термін “тепловий удар” вживаються у такому значенні - невідкладний стан, викликаний дією високої температури навколишнього середовища, що спричиняє системні розлади у постраждалого [34].

Надання домедичної допомоги постраждалим при масивній зовнішній кровотечі передбачає такі кроки:

- переконайтесь що небезпеки для вас немає;
- закличте оточуючих на допомогу;

- перед початком надання допомоги, за можливості, захистіть себе за допомогою індивідуальних засобів захисту, таких як рукавички, маска і захист для очей;
- якщо є кровотеча з рани на кінцівці, і вона видно:
  а) здійсніть максимальний тиск на рану руками;
  б) накладіть пов'язку, що чинитиме тиск на рану, і оцініть її ефективність;
  в) якщо кровотеча зупинилась, заспокойте постраждалого, викличте екстрену медичну допомогу та слідуйте вказівкам диспетчера;
  г) якщо кровотеча не зупинилась, накладіть кровоспинний джгут на відстані 5-7 см вище рани;
  д) уникайте накладання джгута безпосередньо на суглоби ліктя або коліна;
  е) перевірте ефективність накладеного кровоспинного джгута.
- при кровотечі з рани кінцівки без можливості її чіткої візуалізації:
  а) накладіть кровоспинний джгут якомога вище на кінцівку;
  б) заспокойте постраждалого та поясніть подальші кроки;
  в) якщо можливо, розріжте одяг на кінцівці;
  г) оцініть ефективність накладання кровоспинного джгута.

Якщо кровотеча зупинилась, зафіксуйте точний час накладання джгута на самому джгуті або видимому місці. Якщо неможливо зафіксувати час, повідомте медичному персоналу та переконайтеся, що ця інформація буде внесена до медичних записів. Якщо у вас є навик перевірки пульсу на кінцівці нижче джгута, перевірте його. Якщо пульс присутній, збільште тиск кровоспинного джгута або накладіть додатковий джгут. Якщо кровотеча не зупинилась, збільште тиск на кровоспинному джгуті або накладіть ще один джгут в залежності від місця рани. Якщо другий джгут не є ефективним або неможливо його накласти, продовжуйте чинити прямий тиск на рану руками до прибуття медичної бригади або тампонуйте рану. Не знімайте або не послабляйте кровоспинний джгут до прибуття медичної бригади.

При кровотечі з рани, розташованої в пахвових ділянках, сідницях або основі шиї растосуйте максимальний тиск на рану, заспокойте постраждалого та поясніть подальші дії, тампонуйте рану тугим гемостатичним засобом або марлевим бинтом. Після тампонування продовжуйте здійсніть прямий тиск на рану протягом 3 хвилин (з гемостатиком) або 10 хвилин (з марлевим бинтом) та оцініть ефективність тампонування рани.

Якщо кровотеча зупинилась, продовжуйте надавати іншу домедичну допомогу, передбачену процедурою. Якщо кровотеча не зупинилась, спробуйте повторно тампонувати рану. Якщо це неможливо, продовжуйте чинити максимальний тиск на рану руками до прибуття швидкої медичної допомоги.

Це загальна послідовність дій, яку слід виконати, але завжди важливо дотримуватись інструкцій медичних фахівців та адаптувати допомогу до конкретної ситуації. Виконання цих кроків допоможе забезпечити постраждалому першу необхідну допомогу та зберегти його життя до прибуття медичних фахівців.

4.2 Забезпечення захисту працівників суб’єкта господарювання від іонізуючого випромінювання

Працівники, які виконують роботи з радіоактивними речовинами, повинні перебувати під постійним медичним наглядом, використовувати засоби індивідуального захисту від радіації та прилади індивідуального дозиметричного контролю (універсальні радіометри) для своєчасного виявлення і вимірювання рівня випромінювання [35].

Захищаючись від зовнішнього іонізуючого опромінювання при роботах із закритими джерелами випромінювання, тобто такими, які виключають можливість потрапляння радіоактивних речовин у навколишнє середовище, перш за все необхідно не допустити переопромінення працівників.

Основним способами захисту від цього є:

- зменшення активності джерела, з яким контактують працівники під час конкретного технологічного процесу – досягається шляхом використання речовин із меншою активністю;
- зменшення часу контакту з джерелом випромінювання – досягається шляхом вдосконалення організації робіт і технологічного виробничого процесу та проведення попередніх тренінгів працівників;
- збільшення відстані між людиною і джерелом – використовується, як правило, при контакті з точковим джерелом випромінювання шляхом використання дистанційних універсальних маніпуляторів та інших автоматизованих пристроїв;
- розташування між людиною і джерелом захисного екрану (стаціонарного, пересувного, розбірного, настільного тощо), тобто пристрою, який зменшує інтенсивність випромінювання до безпечного рівня [35].

Для виготовлення екранів, а також для захисту працівників в стаціонарних спорудах, використовується бетон, чавун, сталь, алюміній, скло, свинець та інші матеріали. Від дії рентгенівських променів застосовують екрани зі сталевого листа товщиною 0,5-1 мм або алюмінію товщиною 3 мм, спеціальної гуми. Оглядові вікна виконують з плексигласу товщиною 30 мм або з покритого оловом скла товщиною 9 мм.

Для захисту шкіри від забруднень радіоактивними речовинами та запобігання їх попаданню всередину організму, захисту від альфа і бета-випромінювання передусім застосовуються засоби індивідуального захисту (ЗІЗ) від радіації.

Отже, засоби захисту від радіації використовуються у тих випадках, коли інші заходи недостатньо ефективні: при переході через зони збільшеної інтенсивності випромінювання, при ремонтних та налагоджувальних роботах у аварійних ситуаціях, під час короткочасного контролю та при зміні інтенсивності опромінення.

З урахуванням зазначеного прогнозу на території області може виникнути складна радіаційна обстановка наслідки якої вимагатимуть від органів

виконавчої влади, органів місцевого самоврядування, суб'єктів господарювання, на які покладено виконання завдань щодо захисту населення і територій від надзвичайних ситуацій, оперативного реагування та дій [35].

Місцеві органи виконавчої влади, органи місцевого самоврядування, суб'єкти господарювання здійснюють для забезпечення захисту людей від впливу іонізуючих випромінювань наступні заходи:

- приймають згідно з законодавством України рішення щодо застосування на підвідомчій території заходів втручання у разі радіаційних аварій;
- організовують проведення в установленому порядку щорічні обстеження з метою оцінки стану захисту людини від впливу іонізуючих випромінювань та ведення екологічного паспорта підвідомчої території;
- здійснюють організаційне керівництво системою обліку та контролю доз опромінення населення на підвідомчій території;
- організовують контроль за виконанням заходів щодо захисту людини від впливу радіонуклідів, що містяться у будівельних матеріалах;
- затверджують відповідні плани щодо захисту населення від радіаційних аварій та їх наслідків;
- забезпечують постійну готовність засобів оповіщення населення на підвідомчій території про виникнення радіаційної аварії;
- організовують контроль за виконанням заходів щодо захисту населення від радіаційних аварій та їх наслідків;
- забезпечують населення, в місцях його проживання, інформацією щодо рівнів опромінення людини та заходів захисту від впливу іонізуючих випромінювань, що виконуються на підвідомчій території;
- розроблюють та впроваджують програми захисту людей від впливу іонізуючих випромінювання;
- здійснюють оповіщення населення у разі виникнення радіаційної аварії та інформування про рятувальні та профілактичні заходи у зв’язку з цим.

Для виконання вищезазначених заходів залучаються органи управління, сили і засоби обласної територіальної та функціональних підсистем єдиної державної системи цивільного захисту (далі – ЄДС ЦЗ), порядок дій яких визначено Планом реагування на надзвичайні ситуації, пов'язаних з викидом радіоактивних речовин.

Режими захисту робітників і службовців на суб'єктах господарювання вводяться в дію рішенням керівників об'єктів. Незалежно від місця розміщення суб'єкту господарювання (в населеному пункті або за його межами) на його території вводиться в дію свій режим захисту з урахуванням рівнів радіації, виміряних на об'єкті, і реального ступеню захисту працівників і службовців.

При виникненні комунальної радіаційної аварії окрім термінових робіт щодо стабілізації радіаційного стану (включаючи відновлення контролю над джерелом) місцеві органи виконавчої влади, органи місцевого самоврядування, суб'єкти господарювання одночасно здійснюють заходи, спрямовані на:

- зведення до мінімуму кількості осіб з населення, які зазнають аварійного опромінення;
- запобігання чи зниження індивідуальних і колективних доз опромінення населення;
- запобігання чи зниження рівнів радіоактивного забруднення продуктів харчування, питної води, сільськогосподарської сировини і сільгоспугідь, об'єктів довкілля (повітря, води, ґрунту, рослин тощо), а також будівель і споруд.

Для населення, робітників та службовців суб'єктів господарювання, які можуть потрапити в зону випадіння радіоактивних опадів, доцільно завчасно, виходячи з конкретних місцевих умов, розрахувати варіанти режимів радіаційного захисту [35].

З урахуванням вищезазначеного, режими радіаційного захисту вводяться в дію місцевими органами виконавчої влади, органами місцевого самоврядування, суб'єктами господарювання з метою захисту людей від впливу

іонізуючого випромінювання у разі загрози або виникнення надзвичайних ситуацій, пов'язаних з радіаційними аваріями.

4.3 Висновок до четвертого розділу

В четвертому розділі було розглянуто ключові моменти безпеки життєдіяльності та охорони праці в умовах надзвичайних ситуацій, зосереджені на домедичній допомозі при масивній зовнішній кровотечі та заходах захисту працівників від іонізуючого випромінювання.

Питання домедичної допомоги при кровотечі є критично важливим у надзвичайних обставинах, зокрема під час бойових дій, аварій чи нещасних випадків. У розділі детально описано алгоритм дій у разі масивної зовнішньої кровотечі, відповідно до чинного наказу МОЗ України. Особливу увагу приділено правильному накладанню пов’язки та кровоспинного джгута, тампонуванню ран, фіксації часу. Це знання дозволяє рятувати життя ще до прибуття медиків і повинно бути обов’язковим для персоналу об’єктів критичної інфраструктури.

Окремо вивчено вимоги до захисту працівників від іонізуючого випромінювання, що є важливою складовою охорони праці в умовах роботи з радіоактивними джерелами або в разі радіаційної аварії. Захист працівників забезпечується за рахунок обмеження часу контакту, збільшення відстані до джерела, екранування, використання засобів індивідуального захисту та дозиметричного контролю. Належне виконання організаційних та інженерно-технічних заходів дозволяє звести ризик опромінення до мінімуму. Важливим елементом є й система цивільного захисту, що забезпечує координацію дій органів влади, суб’єктів господарювання та населення в умовах загрози або настання радіаційної аварії. Впровадження режимів захисту, інформування населення, екологічний моніторинг та формування планів реагування є запорукою ефективного зниження ризиків для здоров’я та життя людей.

Проаналізовані питання мають важлива значення для безпеки працівників. Вони формують основу для підвищення рівня готовності до надзвичайних ситуацій і підкреслюють важливість превентивних дій, навчання персоналу та дотримання чинних стандартів у сфері охорони праці та цивільного захисту.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи бакалавра було розроблено, налаштовано та протестовано віртуальне тестове середовище, яке призначене для дослідження можливостей міжмережевого екрана нового покоління Zenarmor на основі маршрутизатор OPNsense.

У першому розділі проведено аналіз сучасного стану інформаційної безпеки корпоративних мереж. Розглянуто обмеження класичних пакетних фільтрів і stateful-брандмауерів, показано, як складні атаки маскуються під легітимний трафік та використовують шифрування, соціальну інженерію й особливості протоколів прикладного рівня. Обґрунтовано необхідність використання NGFW, які поєднують глибоку інспекцію пакетів, поведінкову аналітику, контроль додатків і хмарні механізми репутації. Значну увагу приділено концепції тестових середовищ: описано їх роль у безпечній симуляції вторгнень, оцінці оновлень, навчанні персоналу та порівняльному аналізі продуктів безпеки.

У другому розділі здійснено детальне проєктування та розгортання тестового середовища на базі гіпервізора VMware ESXi, що забезпечує ізольованість, гнучке керування ресурсами та підтримку апаратної віртуалізації VT-x / AMD-V. Побудовано двосегментну топологію: зовнішній WAN інтерфейс під’єднаний до фізичного маршрутизатора з виходом у мережу Інтернет, а внутрішній LAN містить захищені вузли й служить основним об’єктом DPI. Центральним елементом виступає OPNsense із двома мережевими інтерфейсами, який виконує маршрутизацію та функції NAT, DHCP, DNS а також містить плагін Zenarmor. Робочу станцію Oracle Linux розгорнуто в LAN-сегменті, вона імітує легітимну діяльність користувачів, генерує типовий вебтрафік і слугує джерелом тестових запитів. В межах архітектури передбачено можливість швидкого масштабування з додаванням нових віртуальних машин, сегментів чи симуляторів атак, що дозволяє

варіювати навантаження та відтворювати комплексні сценарії корпоративної інфраструктури.

Третій розділ присвячено практичній конфігурації міжмережевого екрана. Активовано хмарний сервіс Cloud Threat Intelligence, що на основі машинного навчання та репутації оцінює домени й IP-адреси у режимі реального часу. В інтерфейсі ZenConsole сформовано комплексні політики безпеки. Надалі проведено серію тестів з використанням бази підтверджених фішингових URL-адрес сервісу PhishTank. Робоча станція Oracle Linux ініціювала HTTP- і HTTPS-запити до цих доменів, а Zenarmor виконував репутаційну перевірку, блокував з'єднання, реєстрував подію та відображав її в Live Sessions. Аналіз інтерактивних панелей Threats і Blocks засвідчив, що всі спроби доступу до фішингових ресурсів були негайно зупинені, причому система коректно визначила категорію загрози, джерело трафіку, часову мітку і кількість спроб без фіксації хибнопозитивних спрацьовувань для легітимного вебсерфінгу.

Сукупність теоретичних і практичних результатів демонструє успішне виконання поставленої мети і завдань, підтверджує доцільність застосування NGFW Zenarmor у корпоративних мережах і доводить ефективність розробленої методики тестування. Створене середовище можна використовувати для попередньої валідації брандмауерів перед впровадженням, розробки сценаріїв реагування на інциденти, підготовки фахівців SOC, а також для наукових експериментів, пов'язаних із порівнянням продуктивності та точності різних систем виявлення загроз.

ПЕРЕЛІК ДЖЕРЕЛ

1. What is network security? Definition and types | fortinet. (n.d.). Fortinet. https://www.fortinet.com/fr/resources/cyberglossary/what-is-network-security-

2. IBM. (n.d.). What is network security? | IBM. IBM - United States. https://www.ibm.com/think/topics/network-security

3. Corporate network security: How to detect & prevent attacks. (n.d.). Netmaker: Zero Trust Platform for Secure Networking. https://www.netmaker.io/resources/network-security

4. 6 reasons why your company needs a firewall | WatchGuard Technologies. (n.d.). WatchGuard | Comprehensive Cybersecurity Solutions. https://www.watchguard.com/wgrd-news/blog/6-reasons-why-your-company-needs-firewall

5. Tymoshchuk, V., Karnaukhov, A., & Tymoshchuk, D. (2024). USING VPN TECHNOLOGY TO CREATE SECURE CORPORATE NETWORKS. Collection of scientific papers «ΛΌГОΣ», (June 21, 2024; Seoul, South Korea), 166-170.

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

7. GeeksforGeeks. (2021, October 10). Types of network firewall - geeksforgeeks. https://www.geeksforgeeks.org/types-of-network-firewall/

8. What is a firewall? Definition and types of firewall | fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/firewall

9. Understanding the main types of firewalls. (n.d.). Network security platform for business | NordLayer. https://nordlayer.com/learn/firewall/types-of-firewalls/

10. 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.

11. Karnaukhov, A., Tymoshchuk, V., Orlovska, A., & Tymoshchuk, D. (2024). USE OF AUTHENTICATED AES-GCM ENCRYPTION IN VPN. Матеріали конференцій МЦНД, (14.06. 2024; Суми, Україна), 191-193.

12. The role of test environments: Types, benefits, and QA best practices. (n.d.). APIs Accelerated: Ambassador Redefines API Development Process. https://www.getambassador.io/blog/test-environment-explained

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

14. 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.

15. What is a hypervisor? (n.d.). VMware by Broadcom - Cloud Computing for the Enterprise. https://www.vmware.com/topics/hypervisor

16. 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. https://doi.org/10.62731/mcnd-24.05.2024.001

17. Pandey, B., & Ahmad, S. (2022). Roles of cyber ranges: Testing, training, and research. In Introduction to the cyber ranges (pp. 67–78). Chapman and Hall/CRC. https://doi.org/10.1201/9781003206071-5

18. VMware vsphere | virtualization platform. (n.d.). VMware by Broadcom - Cloud Computing for the Enterprise. https://www.vmware.com/products/cloud-infrastructure/vsphere

19. Тимощук, В., & Тимощук, Д. (2022). Віртуалізація в центрах обробки даних-аспекти відмовостійкості. Матеріали X науково-технічної конференції „Інформаційні моделі, системи та технології “Тернопільського національного технічного університету імені Івана Пулюя, 95-95.

20. Intel® virtualization technology - 001 - ID:655258 | 12th generation intel® core™ processors datasheet, volume 1 of 2. (n.d.). https://edc.intel.com/content/www/us/en/design/ipla/software-development-platforms/client/platforms/alder-lake-desktop/12th-generation-intel-core-processors-datasheet-volume-1-of-2/001/intel-virtualization-technology

21. AMD virtualization - glossary. (n.d.). DevX. https://www.devx.com/terms/amd-virtualization/

22. Welcome to OPNsense documentation. (n.d.). OPNsense documentation. https://docs.opnsense.org/

23. 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.

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

25. Zenarmor (sensei): Installing via web interface. (n.d.). OPNsense documentation. https://docs.opnsense.org/vendor/sunnyvalley/zenarmor_install.html

26. Oracle linux - oracle linux. (n.d.). Oracle Help Center. https://docs.oracle.com/en/operating-systems/oracle-linux/

27. Zenarmor. (n.d.). Installation - zenarmor.com. Zenarmor - Agile Service Edge Security. https://www.zenarmor.com/docs/installing/installation

28. 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

29. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.

30. Everything you need to know about AES-256 encryption. (n.d.). Kiteworks | Your Private Data Network. https://www.kiteworks.com/risk-compliance-glossary/aes-256-encryption/

31. PhishTank | Join the fight against phishing. (n.d.). PhishTank | Join the fight against phishing. https://phishtank.org

32. What is deep packet inspection (DPI)? | fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/dpi-deep-packet-inspection

33. Tymoshchuk, V., Vorona, M., Dolinskyi, A., Shymanska, V., & Tymoshchuk, D. (2024). SECURITY ONION PLATFORM AS A TOOL FOR DETECTING AND ANALYSING CYBER THREATS. Collection of scientific papers «ΛΌГОΣ», (December 13, 2024; Zurich, Switzerland), 232-237.

34. Про затвердження порядків надання домедичної допомоги особам при невідкладних станах. (n.d.). Офіційний вебпортал парламенту України. https://zakon.rada.gov.ua/laws/show/z0356-22#n769

35. Желібо Є. П., Сагайдак І. С. Безпека життєдіяльності. Навчальний посібник для аудиторної та практичної роботи. К.:ЕКОМЕН. 2011. 200 с.