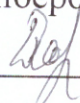


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту IT-
інфраструктури організації на базі рішень OPNsense»

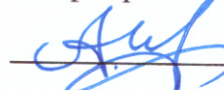
Виконав: студент 4-го курсу групи КБ-21-1
спеціальності 125 «Кібербезпека»

 Денис КЛИМЕНКО

Керівник: доцент кафедри КІ та КБ, к.пед.н., доцент

 Олена ГОЛОВНЯ

Рецензент: доцент кафедри КІ та КБ, к.т.н.

 Олексій ШЕЛУХА

Житомир – 2025

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

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
 Андрій Єфіменко
3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Клименко Денис Олександрович

Тема роботи: «Проект підсистеми захисту IT-інфраструктури організації на базі рішень OPNsense»

затверджена Наказом університету від 3 березня 2025 р. №80/с

Термін здачі студентом закінченої роботи 27 червня 2025 р.

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

1. Топологія мережевої інфраструктури.
2. Підсистема захисту на базі рішень OPNsense.

Обладнання та програмне забезпечення:

1. Емулятор GNS3
2. Oracle VirtualBox
3. ОС Windows Server 2019
4. ОС Windows 10
5. OPNsense (v.25.1.7)
6. Комутатори Cisco

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1			
2			
3			

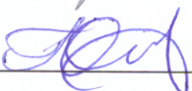
Студент  Денис КЛИМЕНКО

Керівник  Олена ГОЛОВНЯ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	03.03.2025	Виконано
2	Аналіз принципу роботи міжмережевих екранів та їх класифікація	10.03.2025	Виконано
3	Порівняння безкоштовних фаєрволів для мережевого захисту	17.03.2025	Виконано
4	Дослідження можливостей і архітектури OPNsense	24.03.2025	Виконано
5	Аналіз можливостей системи виявлення та запобігання вторгненням Suricata	31.03.2025	Виконано
6	Розробка топології мережі та IP-адресація	07.04.2025	Виконано
7	Вибір засобів захисту в OPNsense	14.04.2025	Виконано
8	Визначення та підбір апаратного забезпечення	17.04.2025	Виконано
9	Проведення налаштування пристроїв мережі	28.04.2025	Виконано
10	Тестування роботи пристроїв мережі та підсистеми захисту	10.05.2025	Виконано
11	Оформлення пояснювальної записки	21.05.2025	Виконано
12	Захист	27.05.2025	Виконано

Студент  Денис КЛИМЕНКО

Керівник  Олена ГОЛОВНЯ

АНОТАЦІЯ

Пояснювальна записка до випускної кваліфікаційної роботи бакалавра складається зі вступу, трьох розділів, висновків, списку використаної літератури та додатків. Текстова частина викладена на 79 сторінках друкованого тексту. Пояснювальна записка має 8 сторінок додатків. Список використаних джерел містить 26 найменувань і займає 2 сторінки. В роботі наведено 63 рисунки та 4 таблиці. Загальний обсяг роботи – 87 сторінок.

Метою роботи є розробка проєкту підсистеми захисту ІТ-інфраструктури організації на базі рішень OPNsense із застосуванням сучасних методів і технологій кібербезпеки, що забезпечить ефективний захист від мережевих загроз, централізоване управління доступом і моніторинг безпеки.

У роботі розглянуто теоретичні засади захисту ІТ-інфраструктури на базі OPNsense, проаналізовано основні мережеві загрози, класифікацію фаєрволів і можливості безкоштовних рішень, обґрунтовано вибір OPNsense як основної платформи для використання в проєкті. Розроблено логічну топологію мережі відповідно до трирівневої моделі, підібрано обладнання, визначено схему IP-адресації та засоби захисту, включаючи фаєрвол, IDPS Suricata, DNS-фільтрацію і двофакторну аутентифікацію. Реалізовано проєкт у середовищі GNS3, виконано конфігурацію серверів, мережевих служб, пристроїв і компонентів OPNsense, протестовано функціонування мережі, а також перевірено ефективність роботи підсистеми захисту.

Ключові слова: OPNSENSE, ІНФОРМАЦІЙНА БЕЗПЕКА, ФАЄРВОЛ, IDPS, SURICATA, МЕРЕЖЕВИЙ ЕКРАН, GNS3, ACTIVE DIRECTORY, DNS, SYSLOG, ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ, МЕРЕЖЕВА ІНФРАСТРУКТУРА.

					ККІКБ.КР.Б – 125 – 08 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту ІТ-інфраструктури організації на базі рішень OPNsense	Літ.	Арк.	Аркушів
Розроб.		Клименко Д.О.		26.06.25				
Керівник		Головня О.С.		26.06.25			4	87
Реценз.		Шелуха О.О.		26.06.25		ФІКТ, Гр. КБ-21-1		
Н. контр.		Головня О.С.		26.06.25				
Затверд.		Єфіменко А.А.		26.06.25				

ANNOTATION

The explanatory note to the bachelor's qualification thesis consists of an introduction, three chapters, conclusions, a list of references, and appendices. The textual part spans 79 pages of printed text. The explanatory note includes 8 pages of appendices. The list of references contains 26 sources and takes up 2 pages. The thesis includes 63 figures and 4 tables. The total volume of the work is 87 pages.

The objective of the thesis is to develop a project of an IT infrastructure protection subsystem for an organization based on OPNsense solutions, applying modern cybersecurity methods and technologies to ensure effective protection against network threats, centralized access management, and security monitoring.

The thesis explores the theoretical foundations of IT infrastructure protection using OPNsense, analyzes key network threats, firewall classifications, and the capabilities of free solutions, and justifies the choice of OPNsense as the primary platform for the project. A logical network topology was designed according to a three-tier model, equipment was selected, an IP addressing scheme and protection tools were defined, including a firewall, Suricata IDPS, DNS filtering, and two-factor authentication. The project was implemented in the GNS3 environment, with configuration of servers, network services, devices, and OPNsense components carried out. The network functionality and effectiveness of the protection subsystem were successfully tested.

Keywords: OPNsense, information security, firewall, IDPS, Suricata, network firewall, GNS3, Active Directory, DNS, Syslog, two-factor authentication, network infrastructure.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	7
ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИСТУ ІТ-ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯ OPNSENSE	10
1.1 Класифікація міжмережевих екранів та принцип їх роботи	10
1.2 Порівняння популярних безкоштовних фаєрволів для захисту мереж.....	20
1.3 Можливості, переваги та архітектура OPNsense	24
1.4 Огляд системи виявлення і запобігання вторгненням	27
1.5 Suricata – система виявлення та запобігання вторгненням у складі OPNsense	31
РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ ІТ-ІНФРАСТРУКТУРИ	35
2.1 Розробка мережевої топології та адресації	35
2.2 Вибір технологій та засобів захисту на основі OPNsense	40
2.3 Вибір апаратного забезпечення.....	41
РОЗДІЛ 3. ВПРОВАДЖЕННЯ, НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ	45
3.1. Базове налаштування мережі ІТ-інфраструктури.....	45
3.2 Встановлення та налаштування OPNsense.....	54
3.3 Тестування, моніторинг та діагностика роботи підсистеми захисту	66
ВИСНОВКИ.....	77
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	78
ДОДАТКИ.....	80

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

VPN – Virtual Private Network

TCP – Transmission Control Protocol

NFS – Network File System

SMTP – Simple Mail Transfer Protocol

DNS – Domain Name System

MITM – Man-in-the-Middle

FISMA – Federal Information Security Management Act

PCI DSS – Payment Card Industry Data Security Standard

NAT – Network Address Translation

APT – Advanced Persistent Threat

DLP – Data Loss Prevention

SIEM – Security Information and Event Management

ACL – Access Control List

WAF – Web Application Firewall

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

IDPS – Intrusion Detection and Prevention System

AD – Active Directory

DHCP – Dynamic Host Configuration Protocol

LAN – Local Area Network

WAN – Wide Area Network

QR – Quick Response

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Актуальність теми. У сучасних умовах розвитку інформаційних технологій забезпечення безпеки IT-інфраструктури організацій є пріоритетним завданням через постійне зростання кількості та складності кіберзагроз. Розгортання комплексних підсистем захисту на основі ефективних і гнучких рішень стає необхідністю для мінімізації ризиків несанкціонованого доступу, втрати даних та збоїв у роботі корпоративних мереж.

OPNsense – відкрите програмне забезпечення з широкими можливостями налаштування мережевого захисту, яке включає функції маршрутизатора, фаєрвола, VPN, систем виявлення вторгнень (IDS/IPS) та інших засобів безпеки – набуває дедалі більшої популярності як основа для побудови підсистем захисту. Завдяки відкритому коду та активній спільноті користувачів і розробників, рішення OPNsense постійно оновлюється і вдосконалюється, що забезпечує високу адаптивність до нових кіберзагроз. Впровадження такої системи дозволить організації значно підвищити рівень контролю за мережевим трафіком і швидко реагувати на потенційні загрози, що особливо важливо в умовах динамічних змін у кіберпросторі.

Крім того, використання відкритих платформ, таких як OPNsense, сприяє зниженню загальних витрат на захист інформаційних систем без шкоди для їх ефективності. Це особливо актуально для організацій із обмеженим бюджетом, які прагнуть впровадити сучасні засоби безпеки без залучення дорогого комерційного програмного забезпечення. Гнучкість конфігурацій та можливість інтеграції з іншими інструментами роблять OPNsense потужним інструментом для створення надійного багаторівневого захисту, що відповідає вимогам сучасного кібербезпекового середовища.

Метою роботи є розробка проєкту підсистеми захисту IT-інфраструктури організації на базі рішень OPNsense із застосуванням сучасних методів і технологій кібербезпеки, що забезпечить ефективний захист від мережевих загроз, централізоване управління доступом і моніторинг безпеки.

Робота передбачає виконання таких завдань:

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

- Проаналізувати принцип роботи міжмережевих екранів та їх класифікація
- Порівняти популярні безкоштовні фаєрволи для мережевого захисту.
- Проаналізувати можливості та архітектуру OPNsense.
- Розглянути функції IDPS Suricata в OPNsense.
- Розробити мережеву топологію та адресацію.
- Обрати технології і засоби захисту на базі OPNsense.
- Визначити необхідне апаратне забезпечення.
- Провести базове налаштування мережі та конфігурування безпекових функцій.
- Провести тестування та моніторинг підсистеми захисту.

Об'єктом дослідження є IT-інфраструктура організації та її захист за допомогою мережевих засобів безпеки.

Предметом дослідження виступають методи, технології та інструменти, реалізовані в рішенні OPNsense, які забезпечують захист мережі, виявлення та запобігання вторгненням.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИСТУ ІТ-ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯ OPNSENSE

1.1 Класифікація міжмережевих екранів та принцип їх роботи

Сучасні організації зазвичай мають внутрішню мережу, що об'єднує їхні комп'ютерні системи, де існує високий рівень довіри між пристроями, особливо в ізольованому середовищі. Однак все більше компаній мають підключення до Інтернету, що відкриває доступ до нових сервісів, але водночас і створює ризики, оскільки Інтернет за своєю природою є незахищеним середовищем.

До основних загроз, пов'язаних доступом до мережі, належать наступні загрози.

- Слабка або відсутня автентифікація. Частина сервісів, зокрема rlogin, взагалі не вимагає введення пароля при підключенні. Інші, такі як анонімний FTP чи загальнодоступні веб-ресурси, дозволяють доступ без належної перевірки користувача. Протоколи типу TCP та UDP покладаються на довіру до IP-адреси віддаленого вузла, а служби на кшталт NFS можуть надавати надто широкі права доступу. У багатьох випадках паролі передаються у незашифрованому вигляді, що полегшує їх перехоплення.

- Небезпечне або вразливе програмне забезпечення. Багато доступних в Інтернеті додатків – особливо безкоштовних чи умовно безкоштовних – містять помилки або недоліки в архітектурі через низьку якість розробки та тестування. Такі програми можуть стати вектором для вторгнення або несанкціонованого доступу до системи.

- Сканери трафіку (сніфери). Програми цього типу дозволяють перехоплювати мережеві пакети з обліковими даними користувачів. Відомі випадки, коли тисячі систем було зламано через встановлення таких утиліт на вразливі вузли.

- Програми для підбору паролів. Словникові атаки дозволяють зловмисникам автоматично підбирати паролі, порівнюючи хеші з заздалегідь

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

підготовленими значеннями. Успішне виконання таких атак може призвести до масового доступу до акаунтів.

- Сканери портів. Ці інструменти дозволяють зловмисникам визначити, які порти на віддаленому хості відкриті, а відтак – знайти потенційно вразливі служби для подальшого вторгнення.
- Маскування (spoofing). Через відсутність автентифікації у низці протоколів, таких як SMTP, можливе підроблення IP-адрес або заголовків електронної пошти. Зловмисник може, наприклад, скористатися маршрутизацією IP source routing для встановлення зворотного з'єднання з підробленої адреси.
- Наявність прихованих каналів обміну. Деякі протоколи та служби можуть мимоволі створювати можливість для обходу стандартних засобів контролю – наприклад, через ICMP або нестандартне використання служб DNS.
- Вразливість до атак типу «людина посередині» (man-in-the-middle, MITM). За відсутності шифрування з'єднання можуть бути перехоплені й змінені в реальному часі, що особливо небезпечно при передачі авторизаційних даних або конфіденційної інформації.

Зрештою, враховуючи ці загрози, підключення до Інтернету вимагає надійного захисту. Одним з основних рішень є впровадження міжмережевих екранів, які слугують бар'єром між внутрішньою мережею та Інтернетом, забезпечуючи контроль за трафіком згідно з політиками безпеки та виявленням потенційно шкідливої активності.

Міжмережеві екрани (також називають фєсрволами або брандмауерами) – це пристрої або програми, які керують потоком мережевого трафіку між мережами або хостами з різними рівнями безпеки [1]. Хоча зазвичай їх розглядають у контексті підключення до Інтернету, вони також застосовуються в інших типах мереж. Наприклад, у корпоративних мережах фєсрволи використовують для обмеження доступу до внутрішніх сегментів, що обслуговують критично важливі функції. Завдяки контролю з'єднань з такими зонами, організація може запобігти несанкціонованому доступу до своїх систем та ресурсів. Наявність належно

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

налаштованого фаєрвола забезпечує додатковий рівень захисту. Часто використання міжмережевих екранів є обов'язковим відповідно до нормативних вимог (наприклад, FISMA). Деякі з них, як-от стандарт безпеки даних індустрії платіжних карток (PCI DSS), прямо передбачають використання фаєрволів.

Використання фаєрволів надає, зокрема, наступні переваги.

- Блокування небезпечних або вразливих сервісів. Фаєрвол може зупиняти вхідні запити до потенційно небезпечних служб.
- Гнучке керування доступом. Можна обмежити доступ до ресурсів за IP-адресами, протоколами або портами. Наприклад, дозволити тільки читання через FTP, заборонити вхід з певних країн або мереж, чи дозволити доступ лише до визначених доменів.
- Приховування внутрішньої структури мережі. Фаєрвол може маскувати IP-адреси внутрішніх хостів, використовувати NAT (трансляцію мережесих адрес) і відкривати лише мінімально необхідні сервіси, тим самим знижуючи ризик розвідки з боку зловмисників.
- Централізований контроль безпеки. Замість того, щоб окремо захищати кожен вузол, достатньо налаштувати один або кілька мережесих фаєрволів, що суттєво знижує витрати на адміністрування.
- Зменшення кількості точок входу. Фаєрволи дозволяють централізовано контролювати трафік і блокувати небажані з'єднання ще до того, як вони досягнуть внутрішньої мережі, зменшуючи кількість потенційних векторів атак.
- Моніторинг та звітність. Сучасні міжмережесі екрани ведуть детальні журнали подій, що дозволяє виявляти підозрілу активність, будувати політики безпеки на основі статистики та проводити розслідування інцидентів.
- Підтримка політик доступу. Фаєрволи дають змогу реалізовувати політики, що відображають потреби бізнесу та вимоги регуляторів – наприклад, обмеження доступу до певних ресурсів у позаробочий час.
- Інтеграція з іншими засобами захисту. Міжмережесі екрани можуть працювати спільно з IDS/IPS, системами аутентифікації, VPN, антивірусами та

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

іншими компонентами захищеної інфраструктури, посилюючи загальний рівень безпеки.

Хоча фаєрволи є важливим компонентом захисту мережі, вони мають низку суттєвих обмежень [2], зокрема наступні.

- Централізована точка атаки. Якщо зловмиснику вдається обійти фаєрвол, він може отримати майже необмежений доступ до внутрішньої мережі. Вся безпека тоді залежить від одного компонента.

- Не захищає від фізичних атак на пристрій. Якщо користувачі мають змогу підключатися напряду (через модеми, USB-накопичувачі або інші обхідні канали), то фаєрвол втрачає контроль над трафіком. Такі шляхи також можуть бути використані для перенесення вірусів чи крадіжки даних.

- Неможливість фільтрації вмісту без додаткових засобів. Фаєрвол самостійно не аналізує вміст файлів або листів. Це дозволяє переносити заборонені файли, шкідливе ПЗ або віруси через дозволені канали, як-от електронна пошта або HTTPS.

- Відсутність захисту від внутрішніх загроз. Фаєрвол не може в повній мірі запобігти діям недобросовісних співробітників, які мають доступ до ресурсів зсередини – наприклад, копіювання конфіденційної інформації на знімні носії.

- Не виявляє складні атаки. Фаєрвол не може розпізнати багатоетапні цільові атаки (APT), фішингові повідомлення або зловмисну активність у дозволеному трафіку без допомоги додаткових систем (IDS/IPS, DLP, SIEM).

Тобто фаєрвол – лише один із основних компонентів системи захисту. Без надійної політики безпеки, навчання користувачів, контролю доступу та моніторингу він не зможе ефективно захистити всю інфраструктуру.

Загальний принцип роботи

Фаєрвол може бути розгорнутий як на мережевому рівні (наприклад, між зовнішньою мережею та внутрішньою), так і безпосередньо на окремих хостах. У будь-якому випадку він діє як контрольна точка, через яку проходить увесь трафік, що підлягає аналізу. Адміністратори створюють так звані вузькі місця (choke

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

points), де фаєрвол перевіряє всі пакети даних, що входять до системи або виходять з неї [3].

Пакет – це одиниця даних, сформована для передавання в мережі, яка містить:

- корисне навантаження (payload) – власне вміст;
- заголовок (header) – інформацію про джерело та призначення пакета.

Фаєрвол аналізує ці пакети згідно з заздалегідь заданими правилами, щоб визначити, чи є трафік допустимим. Основні параметри перевірки:

- IP-адреси джерела та одержувача;
- вміст пакета;
- мережеві протоколи (TCP, UDP тощо);
- прикладні протоколи (HTTP, FTP, SSH, DNS та інші);
- сигнатури атак або характерні шаблони шкідливого трафіку.

Пакети, що не відповідають політиці безпеки, блокуються. Це може відбуватися двома способами:

- ігнорування (відкидання) запиту;
- відправлення повідомлення про помилку.

У більшості випадків використовується перший варіант, щоб зловмисник не міг отримати зворотну інформацію про систему або мережу.

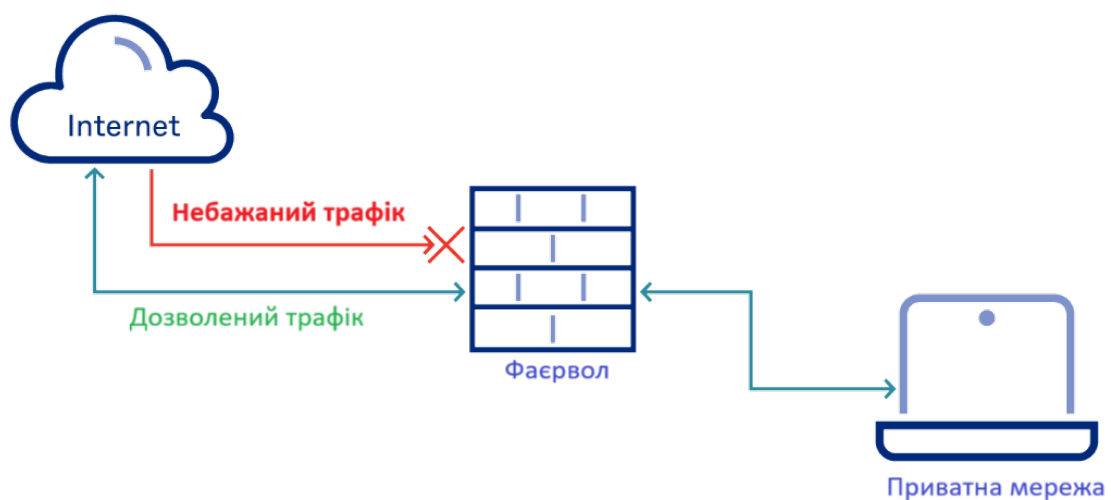


Рисунок 1.1 – Загальний принцип роботи міжмережевого екрану

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

Класифікація

Міжмережеві екрани класифікуються за способом їх впровадження на три основні типи: програмні, апаратні та хмарні [4].

1) Апаратні фаєрволи (Hardware Firewalls). Це окремі фізичні пристрої, які фільтрують трафік на межі мережі. Вони мають власні ресурси й не навантажують клієнтські пристрої. Такі пристрої доцільно використовувати у великих організаціях з кількома підмережами.

Переваги:

- захищають одразу декілька пристроїв;
- забезпечують якісний периметровий захист;
- не впливають на продуктивність кінцевих пристроїв;
- централізоване управління.

Недоліки:

- вища вартість у порівнянні з програмними рішеннями;
- вразливість до внутрішніх загроз;
- вимагають вищої кваліфікації для налаштування та підтримки.

2) Програмні фаєрволи (Software Firewalls). Ці фаєрволи встановлюються безпосередньо на хост-пристрій (ПК, сервер, ноутбук тощо) і захищають лише конкретний пристрій. Адміністратору потрібно встановити окрему копію програмного забезпечення на кожен пристрій, який підлягає захисту. Через це програмні фаєрволи споживають ресурси системи, зокрема оперативну пам'ять та процесор.

Переваги:

- забезпечують точковий захист конкретного пристрою;
- дозволяють ізолювати вузли один від одного;
- гнучке налаштування доступу до програм;
- широко доступні.

Недоліки:

- завантажують ресурси пристрою;

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

- потребують індивідуального налаштування для кожного хоста;
- щоденне обслуговування може бути складним;
- не всі фаєрволи сумісні з усіма ОС і платформами.

Hardware Firewall vs Software Firewall

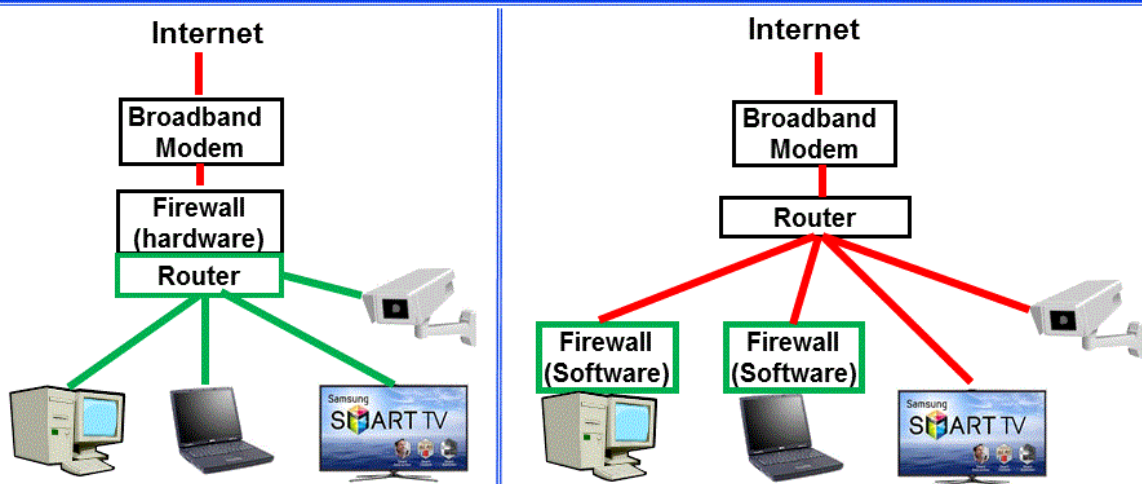


Рисунок 1.2 – Різниця розташування апаратного та програмного фаєрвола [5]

3) Хмарні фаєрволи (Cloud-Based Firewalls / Firewall-as-a-Service). Дані рішення надаються у вигляді послуги через Інтернет і управляються зовнішнім постачальником. Підходять для компаній з розподіленою інфраструктурою або обмеженими ІТ-ресурсами.

Переваги:

- усі адміністративні задачі виконує постачальник;
- масштабування відповідно до навантаження;
- не потребують власного обладнання;
- висока доступність.

Недоліки:

- обмежена прозорість внутрішньої роботи фаєрволу;
- складна міграція на іншого провайдера;
- можливе зростання затримок і ризик втрати конфіденційності через сторонній трафік;
- висока загальна вартість при тривалому використанні.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

Класифікація фаєрволів за методом роботи

Існує кілька основних типів фаєрволів, які класифікуються за принципом функціонування та рівнем моделі OSI [6]. Усі вони можуть бути реалізовані як апаратні пристрої, програмні рішення або у хмарному середовищі.

1) Фільтрація пакетів (Packet-Filtering Firewall). Працює на мережевому рівні OSI, перевіряє заголовки пакетів за заданими правилами, не аналізує вміст.

Переваги:

- низька вартість реалізації;
- висока швидкість обробки трафіку;
- мінімальне навантаження на систему;
- не впливає на швидкодію мережі;
- може реалізовувати складні політики доступу на основі заголовків;
- добре підходить для внутрішнього трафіку між сегментами;
- перший базовий рівень захисту.

Недоліки:

- не аналізує вміст пакетів (payload);
- уразливий до складних атак (IP-спуфінг, обхід правил);
- не підтримує прикладний рівень;
- не має аутентифікації та журналювання;
- складність у конфігурації списків доступу (ACL).

2) Мережеві шлюзи сесійного рівня (Circuit-Level Gateway) Контроль TCP-handshake на рівні сеансу, дозволяє або блокує з'єднання на основі встановлення сесії.

Переваги:

- простота налаштування та супроводу;
- ефективне блокування несанкціонованих з'єднань;
- низькі вимоги до ресурсів;
- захист від розкриття внутрішніх адрес;
- мінімальний вплив на користувачів.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Недоліки:

- не аналізує зміст трафіку;
- не забезпечує повноцінного захисту без додаткових засобів;
- потребує зміни конфігурації мережевих протоколів.

3) Фаєрвол з підтримкою стану з'єднання (Stateful Inspection Firewall).

Поєднує перевірку пакетів і контроль стану з'єднань, працює на мережевому та транспортному рівнях.

Переваги:

- враховує історію трафіку при прийнятті рішень;
- зменшує кількість відкритих портів;
- захищає від атак на протоколи;
- ведення детального журналу подій;
- менша вразливість до сканування портів.

Недоліки:

- вища вартість у порівнянні з простими фаєрволами;
- складність конфігурації;
- може викликати затримки в мережі;
- немає захисту від IP-спуфінгу;
- уразливий до TCP flood-атак.

4) Проксі-фаєрвол (Proxy Firewall або Application firewall). Функціонує на прикладному рівні, виступає посередником, проводить глибоку перевірку вмісту.

Переваги:

- глибокий аналіз пакетів (заголовків і вмісту);
- приховує внутрішні IP-адреси;
- виявляє атаки на прикладному рівні;
- забезпечує додаткову ізоляцію між клієнтом і сервером;
- підтримує точне налаштування правил;
- може обходити географічні обмеження.

Недоліки:

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

- високе навантаження на систему;
- затримки через додаткові кроки обробки;
- складність у налаштуванні;
- несумісність з деякими мережевими протоколами.

5) WAF (Web Application Firewall). Даний тип працює на прикладному рівні й спеціально призначений для захисту вебзастосунків від атак, спрямованих на вразливості HTTP/HTTPS-трафіку. WAF аналізує вхідні запити, зокрема параметри URL, заголовки, cookies і тіла запитів, щоб блокувати спроби SQL-ін'єкцій, XSS, CSRF та інших web-загроз.

Переваги:

- захист від специфічних веб-атак (SQLi, XSS, CSRF тощо);
- працює з популярними вебпротоколами та платформами;
- можливість кастомізації правил під особливості вебзастосунку;
- захист у режимі реального часу;
- веде журнали подій, що корисно для аудиту та реагування;
- може функціонувати як частина хмарної інфраструктури.

Недоліки:

- не захищає інші частини мережі (лише HTTP/HTTPS-трафік);
- висока вартість ліцензії для преміум-функцій;
- можливість помилкового блокування (false positives);
- потребує регулярного оновлення правил і налаштувань;
- вимагає технічної експертизи для ефективного впровадження.

6) Міжмережевий екран нового покоління (Next-Generation Firewall, NGFW) Об'єднує можливості попередніх типів і доповнюється IDS/IPS, антивірусом, аналізом загроз тощо.

Переваги:

- комплексне поєднання захисних механізмів;
- аналіз трафіку від канального до прикладного рівня;
- потужні можливості журналювання;

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

- інтеграція з сучасними механізмами виявлення загроз.

Недоліки:

- висока вартість придбання та обслуговування;
- потенційна точка відмови в системі;
- тривалий час впровадження;
- необхідність високої кваліфікації персоналу;
- зниження продуктивності при великому обсязі трафіку.

1.2 Порівняння популярних безкоштовних фаєрволів для захисту мереж

Деякі безкоштовні фаєрволи дозволяють реалізувати ефективний захист мережі без значних фінансових витрат, зберігаючи при цьому широкий набір функцій, таких як фільтрація трафіку, VPN, IDS/IPS та моніторинг. Вибір конкретного рішення залежить від особливостей середовища, рівня технічної підготовки адміністратора та вимог до гнучкості й масштабованості. Нижче наведено порівняння популярних безкоштовних міжмережевих екранів [7].

1) pfSense – популярний фаєрвол, заснований на FreeBSD з власним ядром, доступний як програмне забезпечення або як апаратне рішення [8]. Забезпечує гнучке конфігурування, підтримку VPN, NAT, IDS/IPS, балансування навантаження, інтеграцію з хмарними сервісами (AWS, Azure) та безпеку корпоративного рівня..

Переваги:

- зручний веб-інтерфейс для адміністрування;
- високий рівень стабільності та активна спільнота;
- VPN, Wi-Fi підтримка;
- потужна система фільтрації, SPI;
- балансування навантаження;
- гнучкість розгортання.

Недоліки:

- відсутність офіційної підтримки для безкоштовної версії;

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

- застарілий інтерфейс у деяких версіях.

2) OPNsense – це безкоштовний фаєрвол з відкритим кодом, створений на основі HardenedBSD (форк FreeBSD, орієнтований на безпеку) [9]. Він поєднує найкращі риси pfSense та Monowall, пропонує сучасний веб-інтерфейс, підтримку плагінів, VPN, IDS/IPS, маршрутизацію, балансування навантаження, а також captive portal.

Переваги:

- сучасний та зручний веб-інтерфейс;
- щотижневі оновлення;
- інтегрований веб-проксі з доступом до чорних списків;
- підтримка OSPF, BGP, 2FA;
- inline-IPS із глибокою інспекцією пакетів.

Недоліки:

- обмежена документація.

3) IPFire – незалежний Linux-дистрибутив, що виступає як фаєрвол, VPN-шлюз та проксі-сервер [10]. Має графічний інтерфейс, простий у використанні, особливо для початківців. Забезпечує SPI-фільтрацію, контент-фільтрацію та базові можливості IDS/IPS..

Переваги:

- працює як фаєрвол, VPN і проксі.;
- віртуалізація через Xen, KVM, VMWare;
- просте налаштування;
- контент-фільтрація.

Недоліки:

- відносно обмежений функціонал;
- Linux-конфігурація може бути складною.

4) VyOS – фаєрвол з CLI-інтерфейсом на базі Debian, орієнтований на досвідчених адміністраторів [11]. Його можна розгорнути як на фізичних серверах,

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

так і у віртуальних середовищах. Підтримує BGP, VPN, тунелювання, балансування навантаження, а також функції маршрутизатора й фаєрвола.

Переваги:

- підтримка VPN, тунелювання, BGP, MPLS;
- інтегрує функції маршрутизатора й фаєрвола;
- балансування навантаження;
- надійність у великих мережах.

Недоліки:

- CLI без GUI;
- немає підтримки сторонніх модулів;
- обмежена кількість портованих архітектур.

5) Sophos XG Firewall Home Edition – це безкоштовна програмна версія міжмережевого екрана для домашнього використання, яка встановлюється на окремий комп'ютер з двома мережевими інтерфейсами [12]. Вона забезпечує повний захист мережі, включаючи антивірус, веб-фільтрацію, контроль додатків, VPN, IPS.

Переваги:

- повний функціонал корпоративного класу;
- інтуїтивний веб-інтерфейс;
- вбудовані IPS, АТР, веб-фільтрація, VPN;
- централізований моніторинг та контроль додатків;
- підтримка Sandstorm-сервісу для захисту від нульового дня.

Недоліки:

- не можна використовувати в комерційних цілях;
- не всі функції доступні, як у комерційній версії.

Для узагальнення інформації та виділення основних переваг і недоліків кожного з продуктів представлена порівняльна таблиця нижче (табл. 1.1), яка дозволяє наочно оцінити функціональні можливості, особливості реалізації, а

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

також визначити доцільність використання кожного рішення в тій чи іншій мережевій інфраструктурі.

Таблиця 1.1

Порівняльна характеристика безкоштовних міжмережевих екранів

Параметр	pfSense	OPNsense	IPFire	VyOS	Sophos XG Firewall Home
Базова ОС	FreeBSD	HardenedBSD	Linux	Debian	Пропрієтарна (на базі Linux)
Інтерфейс	Веб, CLI	Сучасний веб-інтерфейс, CLI	Веб-інтерфейс	CLI (без GUI)	Інтуїтивний веб-інтерфейс
VPN	IPsec, OpenVPN, WireGuard	IPsec, OpenVPN, WireGuard	IPsec, OpenVPN	IPsec, OpenVPN, тунелі GRE, L2TP, BGP VPN	IPsec, SSL VPN, L2TP
IDS/IPS	Snort, Suricata (через плагіни)	Вбудований Suricata	Базова підтримка	Залежить від CLI конфігурації	Вбудований IPS
Цільова аудиторія	Малі та середні організації	Малі та середні організації	Домашні користувачі, малі офіси	Професіонали, провайдери, дата-центри	Домашні користувачі
Ліцензія	BSD (вільна)	BSD (вільна)	GPL	Відкрита, офіційні збірки можуть потребувати підписки	Безкоштовна, некомерційна

На основі проведеного аналізу, можна зробити висновок, що OPNsense вирізняється серед інших безкоштовних міжмережевих екранів завдяки сучасному і зручному веб-інтерфейсу, регулярним оновленням безпеки та розширеній підтримці протоколів. Потужні функції захисту, зокрема інтегрований веб-проксі

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

та IPS з глибокою інспекцією пакетів, забезпечують високий рівень гнучкості, надійності та простоти адміністрування, що робить OPNsense оптимальним вибором для захисту малої та середньої корпоративної мережі.

1.3 Можливості, переваги та архітектура OPNsense

OPNsense – це відкрите, безкоштовне та функціонально насичене рішення для захисту мереж, яке базується на FreeBSD. Вперше було представлено у січні 2015 року після відгалуження від проєктів pfSense і m0n0wall. Завдяки постійній еволюції та активному розвитку, OPNsense швидко перетворився на одну з найпотужніших open-source платформ для маршрутизації та захисту мережі [13].

OPNsense є популярним рішенням для малих і середніх підприємств, навчальних закладів, офісів та організацій, які потребують надійного, гнучкого і одночасно економічно вигідного рішення для захисту мережі. Воно буде корисним як для досвідчених системних адміністраторів, що цінують широкі можливості кастомізації та розширення функціоналу через плагіни, так і для користувачів із базовими знаннями завдяки інтуїтивно зрозумілому інтерфейсу та регулярним оновленням безпеки. Рішення може бути розгорнуте як на фізичному обладнанні, так і у віртуальних середовищах, забезпечуючи гнучкість у виборі платформи – від домашніх серверів і офісних пристроїв до віртуальних машин у дата-центрах, що дозволяє адаптуватися до різних масштабів і вимог мережевої інфраструктури.

Однією з ключових переваг OPNsense є його функціональність, яка не поступається, а часто й перевищує можливості дорогих комерційних рішень. Програмне забезпечення надає щотижневі оновлення безпеки, дотримується чіткого циклу релізів із двома основними оновленнями на рік, а також має відкриту розробку з високими стандартами якості коду. Такий підхід забезпечує стабільність, надійність і передбачуваність для користувачів та бізнесу.

У плані безпеки OPNsense включає потужні механізми захисту від шкідливого ПЗ, фішингу, атак на IoT-пристрої, а також можливості для реалізації VPN-з'єднань. Інтегровані системи виявлення та запобігання вторгненням (IDPS) дозволяють своєчасно виявляти підозрілу активність, а DNS- і email-фільтрація

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

забезпечують захист від шкідливих вебресурсів і листів. Також підтримується резервне копіювання та розширене шифрування, що знижує ризики, пов'язані з програмами-вимагачами.

Інтерфейс користувача доступний через вебпанель, яка має зручну навігацію та підтримує гнучке налаштування, рис.1.3. Основні елементи інтерфейсу – це панель меню, вікно навігації та інформаційна панель, що відображає поточний стан системи. Через відповідні розділи користувачі можуть керувати інтерфейсами, створювати правила фаєрволу, налаштовувати VPN, запускати сервіси тощо.

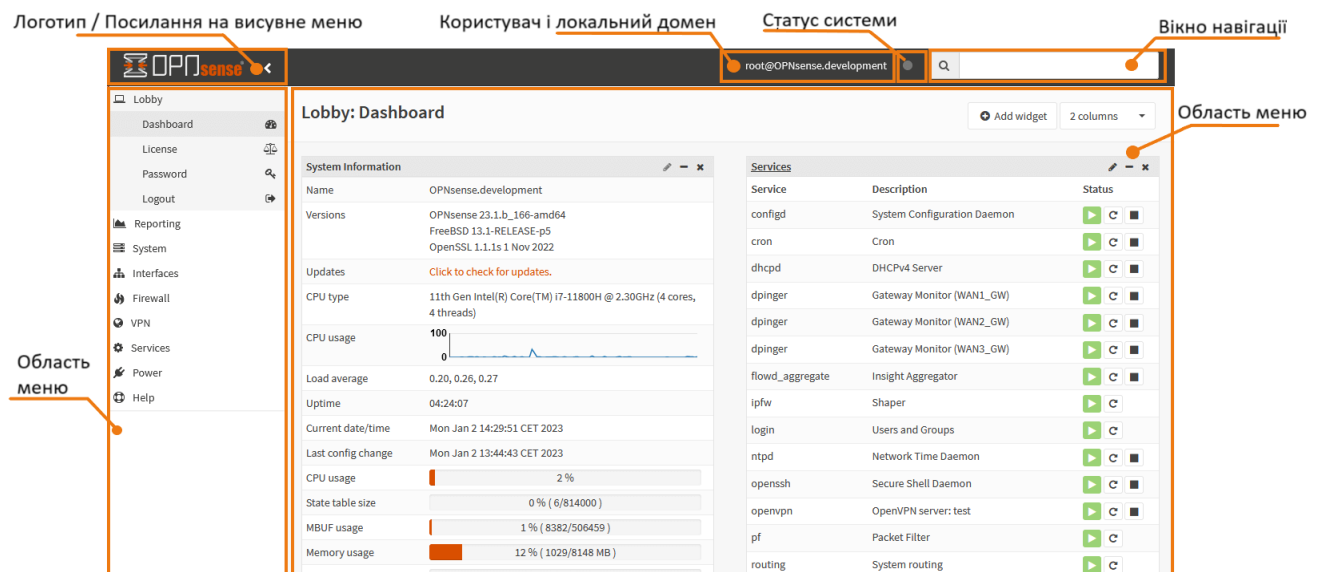


Рисунок 1.3 – Користувацький веб-інтерфейс OPNsense

Фаєрвол у OPNsense функціонує як основний механізм контролю доступу – правила чітко визначають, який трафік дозволено чи заборонено. Завдяки цьому забезпечується захист від DDoS-атак, сканування портів, несанкціонованого доступу та шкідливих протоколів. Також можливе створення політик NAT, порт-форвардингу та контент-фільтрації.

Мінімальні системні вимоги для інсталяції OPNsense включають двоядерний процесор з тактовою частотою від 1 ГГц, 4 ГБ оперативної пам'яті, SSD-диск від 40 ГБ і хоча б один мережевий інтерфейс. Система може бути розгорнута як на фізичних пристроях, так і у віртуальному середовищі. Для підвищення продуктивності та надійності рекомендується використання 64-бітного процесора, окремого інтерфейсу для WAN і накопичувача SSD.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

Ключові функції безпеки OPNsense є наступними.

- Фаєрвол із відстеженням стану (Stateful Firewall). Для захисту мережі від небажаного трафіку фаєрвол OPNsense є першою і найкращою лінією оборони. Він ретельно перевіряє всі вхідні та вихідні дані і відкидає пакети, які не відповідають його правилам. Правила фаєрволу можна легко налаштувати навіть без попереднього досвіду завдяки інтуїтивному веб-інтерфейсу. Окрім цього, підтримується геоблокінг – обмеження доступу на основі географічного розташування IP-адрес, що додатково підвищує рівень безпеки мережі.

- IDS/IPS. OPNsense використовує Suricata в ролі системи IDS/IPS, яка забезпечує високоефективний аналіз мережевого трафіку з метою виявлення та запобігання мережевим загрозам. Suricata виконує глибоку інспекцію пакетів у режимі реального часу, розпізнає відомі атаки, такі як сканування портів, DoS/DDoS, експлойти та інші шкідливі активності, а також дозволяє застосовувати політики блокування або сповіщення для забезпечення безпеки мережі. Вбудована інтеграція Suricata в OPNsense дозволяє ефективно підвищити рівень захисту корпоративної мережі шляхом автоматичного виявлення та нейтралізації загроз.

- VPN (Віртуальна приватна мережа). OPNsense підтримує кілька VPN-протоколів, зокрема IPsec, OpenVPN і WireGuard. Це дозволяє створювати безпечні тунелі між пристроями і фаєрволом OPNsense. Ця функція забезпечує доступ до мережевих ресурсів з віддалених місць, захищаючи дані від злому чи перехоплення. Вбудовані майстри налаштування та зручний інтерфейс спрощують процес підключення і налаштування VPN.

- Фільтрація веб-контенту. OPNsense надає потужні можливості для фільтрації веб-контенту, що дозволяє блокувати доступ до шкідливих і небажаних сайтів. Ця функція слугує щитом проти шкідливого ПЗ, фішингових атак і різних онлайн-загроз. Налаштування правил фільтрації здійснюється через зручний веб-інтерфейс. Найпопулярніший плагін Zenarmor використовує системи штучного інтелекту для захисту користувачів від шкідливого контенту в Інтернеті.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

- 2FA (Двофакторна аутентифікація). Для посилення безпеки OPNsense підтримує двофакторну аутентифікацію, що додає додатковий рівень захисту облікових записів користувачів. Для входу користувачам потрібно вводити пароль і код із телефону. Цей надійний механізм запобігає несанкціонованому доступу навіть у випадку компрометації паролів.
- Логування та моніторинг. OPNsense забезпечує детальне логування всієї мережевої активності, що дозволяє відслідковувати події, аналізувати інциденти та вести аудит безпеки. Вбудовані інструменти для візуалізації статистики і побудови графіків допомагають своєчасно виявляти аномалії у трафіку.
- Резервне копіювання і відновлення конфігурації. Можливість створення автоматичних резервних копій налаштувань для швидкого відновлення роботи після збою або атаки.
- Балансування навантаження та відмовостійкість. OPNsense підтримує балансування трафіку між кількома інтернет-з'єднаннями і механізми failover, що забезпечують безперервність роботи мережі.
- Підтримка VLAN та сегментації мережі. Ця функція дозволяє ефективно ізолювати різні підмережі та підвищувати безпеку шляхом розмежування трафіку.
- Інтеграція з зовнішніми системами аутентифікації, наприклад LDAP, RADIUS, що спрощує централізоване управління доступом.

1.4 Огляд системи виявлення і запобігання вторгненням

Система виявлення і запобігання вторгненням (IDPS) – це програмне забезпечення, яке автоматизує моніторинг і аналіз подій у комп'ютерних системах або мережах для своєчасного виявлення та блокування потенційних загроз. Основна мета такої системи полягає у швидкому розпізнаванні підозрілої активності, що може свідчити про спроби несанкціонованого доступу, атак або інших шкідливих дій, та негайному реагуванні для захисту інформаційної інфраструктури. Крім того, IDPS забезпечує важливу інформацію для подальшого аналізу безпеки та допомагає у розслідуванні інцидентів. Сучасні системи можуть інтегруватися з іншими засобами безпеки, що підвищує загальну ефективність

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

захисту. Впровадження IDPS дозволяє знизити час реагування на атаки та мінімізувати потенційні збитки.

Принцип роботи системи виявлення і запобігання вторгненням базується на постійному аналізі мережевого трафіку й системних подій із застосуванням методів детекції за сигнатурами, аналізу аномалій і контролю протоколів. У разі виявлення загрози система може миттєво сповістити адміністратора, зафіксувати інцидент або автоматично блокувати шкідливу активність у режимі реального часу. Це дозволяє забезпечити проактивний захист мережі та мінімізувати ризики виникнення інцидентів безпеки [14].

Система виявлення і запобігання вторгненням (IDPS) об'єднує в собі функції двох типів систем: IDS (система виявлення вторгнень) та IPS (система запобігання вторгненням).

Система виявлення вторгнень (IDS) зазвичай розміщується пасивно в мережі, наприклад, на окремому вузлі або в точці мережевого моніторингу, де вона аналізує копії трафіку без впливу на його проходження, рис.1.4. Такий підхід дозволяє виявляти загрози без втручання в роботу мережі, але не забезпечує автоматичного блокування шкідливого трафіку [15].

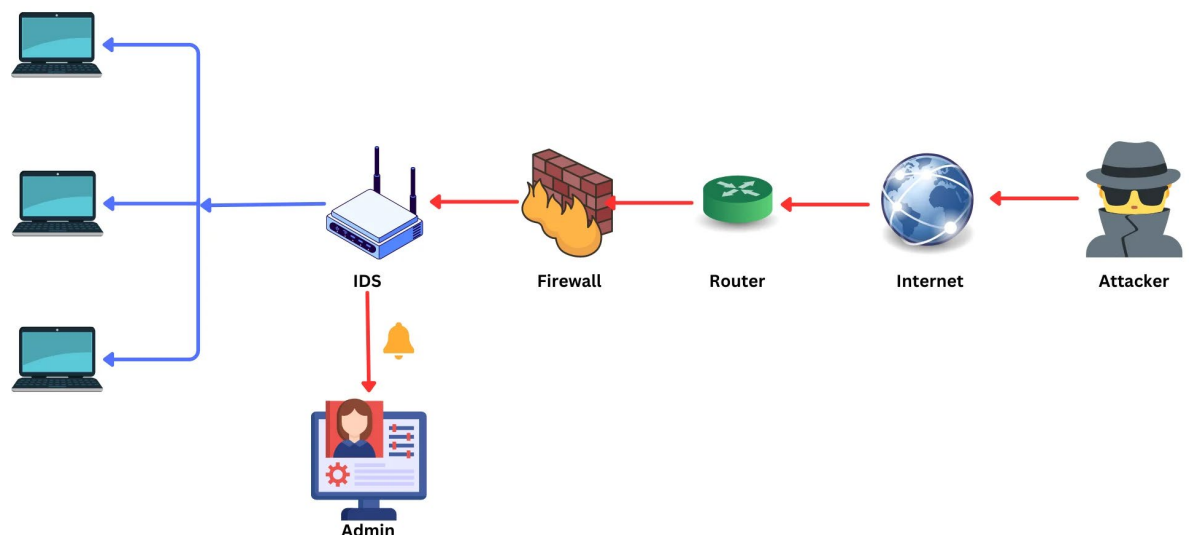


Рисунок 1.4 – Розміщення IDS в мережі

На відміну від IDS, система запобігання вторгненням (IPS) розміщується безпосередньо у мережевому шляху, через який проходить трафік, рис.1.5. Це дає

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

їй можливість не лише виявляти загрози, а й миттєво блокувати або модифікувати шкідливі пакети, запобігаючи можливим атакам. Така інтеграція IPS безпосередньо впливає на продуктивність мережі, але забезпечує більш активний захист.

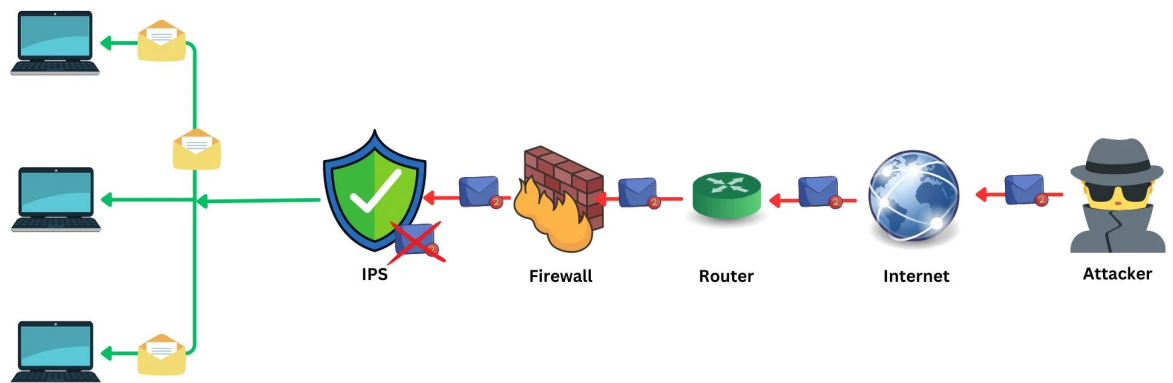


Рисунок 1.5 – Розміщення IPS в мережі

Термін IDPS використовується для підкреслення поєднання можливостей обох систем в одному комплексному рішенні – воно одночасно виявляє загрози (IDS) і запобігає їм (IPS).

Класифікація

Системи виявлення і запобігання вторгненням поділяються на кілька основних типів залежно від місця розміщення та сфери застосування. Кожен має свої особливості і призначений для контролю певного середовища.

- Мережева система виявлення і запобігання вторгненням (Network-based IDPS) розміщується на периферії мережі, наприклад, на маршрутизаторі чи фаєрволі, і виконує моніторинг усього вхідного та вихідного трафіку. Така система здатна виявляти шкідливу активність на рівні мережевих з'єднань і блокувати її до того, як вона досягне цільових пристроїв.

- Хостова система виявлення і запобігання вторгненням (Host-based IDPS) встановлюється безпосередньо на сервер або робочу станцію, де аналізує локальні процеси, журнали подій і трафік, що проходить через цей конкретний хост. Вона забезпечує більш глибокий аналіз дій на рівні операційної системи та може ефективно реагувати на спроби атак саме на цьому пристрої.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

- Бездротова система виявлення і запобігання вторгненням (Wireless IDPS) спеціально призначена для захисту бездротових мереж. Вона зазвичай інтегрується у точки доступу або контролери Wi-Fi й виконує аналіз трафіку у повітряному інтерфейсі, виявляючи несанкціоновані пристрої, спроби вторгнень або порушення політик безпеки у бездротовому середовищі.

- Системи аналізу поведінки мережі (Network Behavior Analysis, NBA) – це різновид IDPS, що виявляє загрози на основі відхилень від типової активності в мережі. На відміну від класичних методів, NBA не покладається лише на відомі сигнатури атак, а аналізує мережевий трафік у реальному часі, виявляючи аномалії, які можуть свідчити про зловмисну діяльність. Завдяки цьому такі системи особливо ефективні проти нових, складних або малопомітних загроз.

Методи виявлення в IDPS

IDPS-системи застосовують різні методи виявлення загроз, які умовно поділяються на три основні категорії [16].

1) Виявлення на основні сигнатур (Signature-based detection). Виявлення здійснюється шляхом порівняння мережевої активності з базою відомих сигнатур – унікальних шаблонів вже зафіксованих загроз. Цей підхід ефективний проти відомих атак, але не здатний виявити нові, ще не задокументовані загрози.

2) Виявлення на основні аномалій (Anomaly-based detection). Засноване на порівнянні випадкових фрагментів трафіку з типовим (еталонним) профілем мережевої активності. Значні відхилення від норми трактуються як потенційна загроза. Цей метод краще виявляє нові атаки, але має вищий рівень хибних спрацювань.

3) Протокольне або політико-орієнтоване виявлення (Protocol-based або Policy-based detection). Оцінює активність на відповідність заздалегідь визначеним мережевим протоколам або політикам безпеки, створеним фахівцем. Будь-яке порушення цих правил розцінюється як підозріла поведінка.

Основні переваги використання системи виявлення і запобігання вторгненням (IDPS) є наступними.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

- Виявлення загроз у реальному часі. IDPS постійно моніторить мережевий трафік і події в системі, оперативно виявляючи підозрілу активність. Це дозволяє вчасно реагувати на загрози й запобігати ескалації інцидентів, що є ключовою вимогою багатьох стандартів безпеки, таких як NIS2, DORA або NIPAA.
- Автоматичне реагування на інциденти. У разі виявлення шкідливої активності система може самостійно вжити заходів – заблокувати трафік, завершити сесію або виконати інші дії згідно з заданими політиками безпеки. Це мінімізує людський фактор і підвищує ефективність захисту.
- Покращена видимість мережі. IDPS забезпечує глибоке розуміння того, що відбувається в мережі, допомагаючи ідентифікувати вразливості, нестандартну поведінку або потенційні точки атак. Завдяки цьому адміністратори можуть своєчасно коригувати політики безпеки та зміцнювати захист інфраструктури.
- Відповідність вимогам нормативно-правових актів. Багато галузевих стандартів вимагають наявності механізмів контролю безпеки. Використання IDPS допомагає дотримуватись цих вимог та підтверджувати відповідність аудиторам.
- Оптимізація роботи служби безпеки. Завдяки автоматизації моніторингу та реагування, IDPS зменшує навантаження на команду кіберзахисту, дозволяючи спеціалістам зосередитися на стратегічних завданнях замість рутинного аналізу подій.

1.5 Suricata – система виявлення та запобігання вторгненням у складі OPNsense

У дистрибутиві OPNsense Suricata використовується як основний рушій для глибокого аналізу мережевого трафіку та реалізації механізмів виявлення вторгнень [17]. Завдяки підтримці роботи в режимах IDS та IPS, Suricata дозволяє застосовувати сигнатурне виявлення та блокування загроз, а також інтегрується зі сторонніми системами журналювання й візуалізації подій.

Suricata – це високопродуктивна система аналізу мережевого трафіку з відкритим вихідним кодом, яка підтримує функції виявлення (IDS) та запобігання (IPS) вторгнень, а також ведення журналів і аналізу мережеских потоків [18]. Вона

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

розроблена консорціумом Open Information Security Foundation (OISF) та орієнтована на гнучке налаштування правил, ефективну обробку трафіку й масштабованість. Suricata підтримує багатопоточність, що дозволяє їй працювати з великими обсягами даних без значного зниження продуктивності системи.

Крім того, Suricata підтримує використання як сторонніх сигнатурних баз, так і правил, написаних вручну відповідно до потреб конкретної мережі. Це дає змогу адаптувати систему до унікальних загроз, що можуть виникати в організації та оперативно реагувати на нові вектори атак.

Принцип роботи

Робота Suricata базується на аналізі мережевого трафіку в режимі реального часу з метою виявлення загроз на основі визначених сигнатур. Вона працює в режимі прослуховування (promiscuous mode), що дозволяє їй фіксувати увесь трафік, який проходить через заданий мережевий інтерфейс, незалежно від того, кому він призначений [19].

Після захоплення пакетів Suricata виконує їх аналіз, виділяючи заголовки, корисні навантаження та специфічні дані для кожного мережевого протоколу. Далі відбувається порівняння вмісту пакетів з базою сигнатур – наборами правил, що описують характерні ознаки відомих атак. При наявності збігу Suricata ідентифікує відповідну загрозу.

Крім сигнатурного аналізу, Suricata підтримує глибоку інспекцію пакетів (DPI), що дозволяє перевіряти вміст на прикладному рівні та виявляти загрози, які приховуються у середині даних. У разі виявлення підозрілої активності система виконує задану дію: ведення журналу, створення сповіщення або блокування трафіку (в режимі IPS).

Створення правил

Правила Suricata – це інструкції, які визначають, який мережевий трафік потрібно ідентифікувати та яку дію слід виконати при його виявленні. Кожне правило має стандартну структуру, що складається з трьох основних частин [20].

1. Дія (Action) – визначає, що робити при спрацюванні правила. Типовими діями є:

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

- alert – створити сповіщення;
- pass – припинити подальшу перевірку пакета і пропустити пакет;
- drop – відкинути пакет і створити сповіщення;
- reject – надіслати RST або ICMP повідомлення про недосяжність відправнику пакета, що відповідає правилу;
- rejectsrc – те саме, що reject (відправнику пакета);
- rejectdst – надіслати RST або ICMP повідомлення про помилку отримувачу пакета, що відповідає правилу;
- rejectboth – надіслати RST або ICMP повідомлення про помилку обом сторонам спілкування.

2. Заголовок (Header): описує тип трафіку, до якого застосовується правило:

- протокол (TCP, UDP, ICMP тощо);
- IP-адреса джерела і призначення (можуть використовуватись діапазони або any);
- порт джерела і призначення;
- напрямок трафіку (->, => або <>).

3. Опції (Options): додаткові умови, що уточнюють правило, наприклад:

- msg – повідомлення про подію;
- content – пошук конкретного рядка у тілі пакета;
- sid – унікальний ідентифікатор правила;
- rev – номер ревізії;
- classtype, priority, flow, depth, offset тощо.

Для прикладу, нижче наведено наступне правило

alert tcp any any -> 192.168.1.0/24 80 (msg:"HTTP GET request detected"; content:"GET"; http_method; sid:100001; rev:1;)

Це правило Suricata означає:

- alert – при спрацьовуванні правила буде створено сповіщення (alert);
- tcp – правило застосовується до TCP-трафіку;
- any any – джерело може бути будь-яким IP і будь-яким портом;

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

- -> 192.168.1.0/24 80. Символ -> означає, що правило застосовується до трафіку, що прямує до підмережі 192.168.1.0/24 та порту 80 (HTTP);
- msg:"HTTP GET request detected" – повідомлення, яке з'явиться у сповіщенні, якщо правило спрацює;
- content:"GET" – у пакеті шукається текст "GET";
- http_method – перевірка, чи слово "GET" є HTTP-методом (тобто в заголовку HTTP-запиту);
- sid:100001 – унікальний ідентифікатор правила;
- rev:1 – версія правила.

Тобто, дане правило виявляє HTTP GET-запити, спрямовані на веб-сервери в локальній мережі 192.168.1.0/24 на порт 80, і при їх виявленні генерує сповіщення.

Висновки до першого розділу

У ході роботи над розділом було проаналізовано загрози, що виникають при підключенні до Інтернету, досліджено роль міжмережевих екранів як одного з ключових засобів захисту мережевої інфраструктури, розглянуто принцип їхньої роботи, класифікацію за способом реалізації, основні переваги, обмеження та можливості інтеграції з іншими системами безпеки.

У результаті аналізу безкоштовних фаєрволів було визначено, що більшість з них мають широкий функціонал для захисту мережі, включаючи підтримку VPN, систему виявлення вторгнень та контроль доступу. Найбільш збалансованим за критеріями зручності, функціональності та гнучкості налаштувань виявився OPNsense, що робить його доцільним вибором для побудови безпечної мережевої інфраструктури.

У результаті аналізу можливостей та архітектури OPNsense було встановлено, що це гнучке та багатфункціональне рішення для побудови захищеної мережевої інфраструктури. Платформа поєднує широкий набір сучасних засобів захисту, таких як фаєрвол, IDS/IPS, VPN, фільтрація контенту, 2FA та резервне копіювання, з інтуїтивним веб-інтерфейсом і можливістю розгортання як на фізичному, так і на віртуальному обладнанні. Завдяки відкритому коду,

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

регулярним оновленням і підтримці плагінів OPNsense є ефективним вибором для малого й середнього бізнесу, що прагне забезпечити високий рівень мережевої безпеки без значних фінансових витрат.

Також було виконано аналіз принципів роботи, класифікації та методів виявлення загроз у системах виявлення і запобігання вторгненням (IDPS), а також розглянуто особливості реалізації такої системи на прикладі Suricata в середовищі OPNsense. Проаналізовано різні типи IDPS, їх переваги та роль у забезпеченні безпеки інформаційної інфраструктури, що стало основою для подальшого впровадження даного механізмів захисту у рамках проєкту.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ ІТ-ІНФРАСТРУКТУРИ

2.1 Розробка мережевої топології та адресації

Вибір топології мережі є одним із важливих етапів проєктування ІТ-інфраструктури, оскільки саме від неї залежать надійність, продуктивність, масштабованість та подальше адміністрування системи. Правильно обрана топологія дозволяє ефективно організувати обмін даними між усіма вузлами мережі, оптимізувати навантаження, забезпечити резервування критичних

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

компонентів та реалізувати засоби захисту відповідно до сучасних вимог інформаційної безпеки.

З огляду на зростання обсягів даних, кількості користувачів і різноманіття сервісів, сучасна мережа має бути не лише функціональною, а й здатною до швидкої адаптації і вимог безпеки. Тому нині актуальним стає використання структурованих підходів до побудови топології, які дозволяють легко масштабувати інфраструктуру, ізолювати проблемні ділянки та централізовано впроваджувати засоби контролю та моніторингу. Такий підхід підвищує ефективність обслуговування мережі та спрощує інтеграцію нових технологій.

Трирівнева модель побудови мережі є однією з найпоширеніших архітектур у корпоративних інфраструктурах [21]. Її перевага полягає в логічному поділі функцій між окремими рівнями, що сприяє підвищенню масштабованості, керованості та надійності мережі. Такий підхід дозволяє централізовано впроваджувати політики безпеки, розгортати нові сервіси без порушення роботи мережі та гнучко адаптувати її до структурних змін.

Рівень ядра (core) відповідає за високошвидкісну маршрутизацію між ключовими сегментами мережі. На цьому рівні мінімізується оброблення трафіку – здійснюється лише швидка передача даних з максимальною пропускну здатністю та мінімальними затримками. Його основне завдання забезпечення надійного та стабільного з'єднання між критично важливими компонентами мережі і забезпечення виходу до інших мереж, таких як Інтернет.

Рівень розподілу (distribution) виконує функції агрегації трафіку з нижчого рівня, маршрутизації між підмережами, застосування політик безпеки та фільтрації доступу. На цьому рівні реалізуються механізми контролю доступу, сегментації мережі за допомогою VLAN, міжмережева маршрутизація.

Рівень доступу (access) забезпечує підключення кінцевих користувачів і пристроїв до локальної мережі. Тут відбувається автентифікація користувачів, базова фільтрація трафіку та реалізація політик контролю доступу. До цього рівня підключаються комп'ютери, принтери, IP-телефони, точки бездротового доступу

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

та інші клієнтські пристрої. Даний рівень відповідає за первинну обробку трафіку перед його передачею до рівня розподілу.

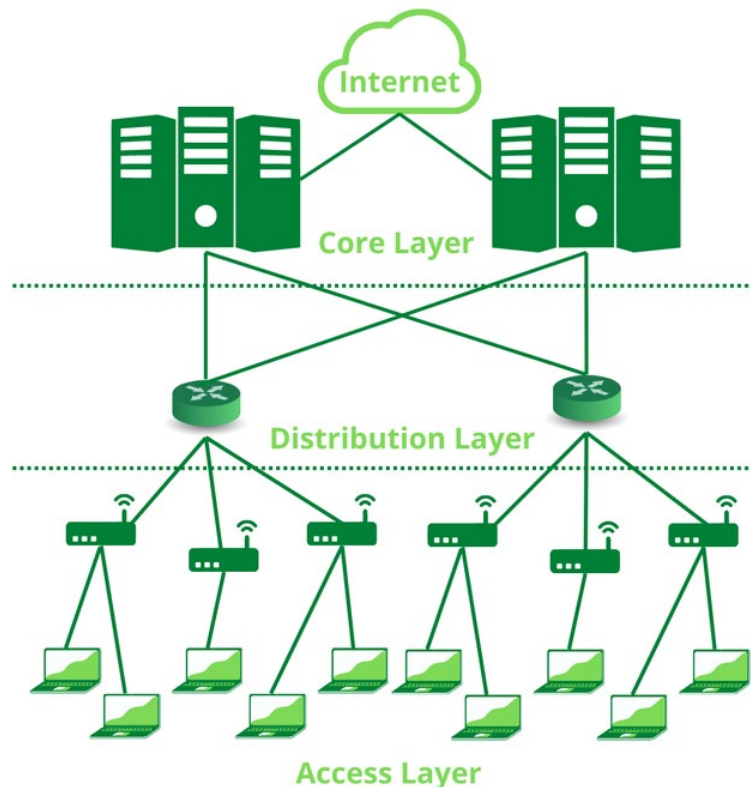


Рисунок 2.1 – Схематичне зображення трирівневої моделі мережі

Тому, зважаючи на очевидні переваги трирівневої моделі мережі – чітке розмежування функцій, спрощене адміністрування, високу масштабованість і підтримку політик безпеки – саме ця модель буде обрана як основа для проєктування мережевої ІТ-інфраструктури. Її використання дозволить створити гнучку, надійну, масштабовану та ефективну архітектуру.

На рис.2.2 представлена спроектована логічна топологія ІТ-інфраструктури організації. Детальніше розглянемо кожен рівень.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

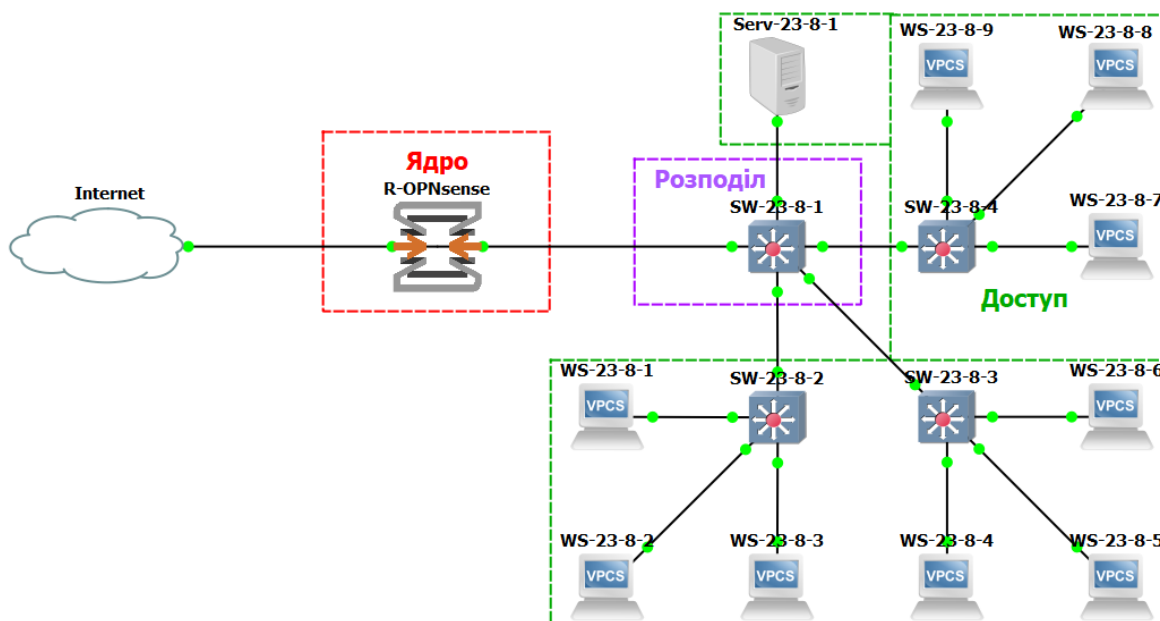


Рисунок 2.2 – Логічна топологія мережі IT-інфраструктури

Рівень ядра складається з маршрутизатора R-OPNSense, який виконуватиме базові функції маршрутизації трафіку до Інтернету і водночас забезпечуватиме можливості фільтрації трафіку та захисту мережі.

Рівень розподілу представлений комутатором SW-23-8-1, який з'єднаний з рівнем ядра, тобто з R-OPNSense.

Рівень доступу представлений комутаторами SW-23-8-2, SW-23-8-3, SW-23-8-4 та кінцевим обладнанням у вигляді комп'ютерів працівників.

Комутатор SW-23-8-4 підключений до маршрутизатора R-OPNSense через виту пару Gigabit Ethernet. В свою чергу до даного комутатора підключено серверне обладнання, а саме Windows Server 2019 (Serv-23-8-1). Підключення серверу саме на цьому рівні забезпечить кращий контроль доступу і централізованість.

Комутатори SW-23-8-2 та SW-23-8-3 підключені до комутатора рівня розподілу SW-23-8-1 через виту пару Gigabit Ethernet. В свою чергу до SW-23-8-2 та SW-23-8-3 під'єднані кінцеві пристрої користувачів, що включає комп'ютери та ноутбуки.

Таким чином в мережі буде використано 1 маршрутизатор, 4 комутатори та 50 кінцевих пристроїв у вигляді комп'ютерів та ноутбуків, що рівномірно розподілені між комутаторами SW-23-8-2 - SW-23-8-4.

Наступним етапом розробки є визначення схеми IP-адресації мережі з урахуванням раціонального використання адресного простору. У проєкті передбачено одну мережу 25.23.8.0/30 для каналу зв'язку між маршрутизатором та Інтернетом і одну локальну мережу 192.168.1.0/24. Всі мережеві пристрої та сервери матимуть статичні IP-адреси, тоді як кінцеві пристрої отримуватимуть параметри адресації від DHCP-сервера. Крім того, усі пристрої мережі будуть приєднані до домену klymenko.net.

На табл.2. наведено таблицю адресації пристроїв IT-інфраструктури. Більш детальна схема топології мережі представлена у додатку А.

Таблиця 2.1

Параметри адресації пристроїв мережі

Мережа/Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска	Префікс
WAN	—	25.23.8.0	255.255.255.252	/30
LAN	—	192.168.1.0	255.255.255.0	/24
R-OPNsense	Eth0	25.23.8.2	255.255.255.252	/30
	Eth1	192.168.1.254	255.255.255.0	/24
Комутатор SW-23-8-1	Інтерфейс Vlan 1	192.168.1.253	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.254	—	
Комутатор SW-23-8-2	Інтерфейс Vlan 1	192.168.1.252	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.254	—	
Комутатор SW-23-8-3	Інтерфейс Vlan 1	192.168.1.251	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.254	—	
Комутатор SW-23-8-4	Інтерфейс Vlan 1	192.168.1.251	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.254	—	
Сервер Serv-23-8-1	Eth0	192.168.1.200	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.254	—	
Робочі станції WS-23-8-1 – WS-23-8-50	Eth0	DHCP		
	Шлюз за замовчуванням			

2.2 Вибір технологій та засобів захисту на основі OPNsense

У процесі реалізації підсистеми захисту на базі OPNsense виконаємо обґрунтування доцільності використання низки вбудованих механізмів і сервісів, які забезпечуватимуть базову та розширену безпеку мережевої інфраструктури. До ключових технологій, які буде обрано для впровадження, належатимуть правила фаєрвола, система виявлення вторгнень Suricata з пересилкою подій до Syslog-сервера, сервіс Unbound DNS із функцією блокування небажаних доменів, а також механізм двофакторної аутентифікації для захищеного доступу до панелі керування OPNsense. Кожне з рішень виконуватиме окрему функцію в загальній системі безпеки, доповнюючи одне одного та формуючи багаторівневий захист.

- **Правила фаєрвола.** OPNsense автоматично генерує базові правила фаєрвола для інтерфейсів WAN і LAN, що включають блокування приватних та зарезервованих підмереж на зовнішньому інтерфейсі, дозволи на вихідний трафік з внутрішньої мережі, а також спеціальні правила захисту, такі як anti-lockout для доступу до веб-інтерфейсу. Це дозволяє забезпечити початковий рівень безпеки одразу після встановлення системи без потреби ручного налаштування всіх правил.
- **Suricata.** Система виявлення та запобігання вторгненням Suricata інтегрована в OPNsense та забезпечує фільтрацію мережевого трафіку з виявленням відомих шаблонів мережевих атак. Події про спрацювання Suricata можуть автоматично пересилатись на Syslog-сервер, де вони можуть централізовано зберігатись і дозволяти адміністратору швидко і оперативно вижити необхідних заходів
- **Unbound DNS.** Вбудований рекурсивний DNS-сервер Unbound у OPNsense виконує локальне розв'язання DNS-запитів, що підвищує швидкість і безпеку. Його розширення через функцію Blocklist дозволяє блокувати небажані домени, а також можливе використання функцій, як-от примусове застосування SafeSearch, що актуально для фільтрації вмісту в освітніх чи корпоративних мережах [22].

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

- Двофакторна аутентифікація на вхід. Для посилення контролю доступу OPNsense підтримує двофакторну аутентифікацію, яка реалізується через Google Authenticator або інші TOTP-сумісні програми. Після активації користувач повинен вводити одноразовий код зі свого смартфона разом із паролем при вході в систему, що значно знижує ризик несанкціонованого доступу навіть у випадку витоку облікових даних [23].

2.3 Вибір апаратного забезпечення

При виборі пристрою для розгортання дистрибутиву OPNsense слід звертати увагу на такі технічні параметри, як кількість і швидкість мережевих інтерфейсів (не менше двох Gigabit Ethernet портів), обсяг оперативної пам'яті (рекомендовано від 4 ГБ), тип і ємність накопичувача (SSD для швидшої роботи), а також продуктивність процесора – бажано використовувати багатоядерні x86-сумісні процесори з підтримкою апаратного прискорення шифрування для забезпечення стабільної роботи фаєрвола, IPS, VPN та інших сервісів.

Тому для розгортання OPNsense в мережу було обрано міні-ПК Protectli FW2B Vault 2 на базі процесора Intel® Celeron® J3060, рис.2.3. Цей компактний мережевий шлюз має два гігабітні мережеві порти, що забезпечує надійне з'єднання з зовнішніми та внутрішніми сегментами мережі. Процесор J3060 з двома ядрами і тактовою частотою до 2,48 ГГц забезпечує достатню обчислювальну потужність для стабільної роботи фаєрвола, NAT, VPN та інших сервісів безпеки. Пристрій оснащено 4 ГБ оперативної пам'яті DDR3L, чого цілком достатньо для невеликої або середньої мережі, а також накопичувачем SSD, що забезпечує швидке завантаження системи та обробку журналів. Низьке енергоспоживання, пасивне охолодження і компактні розміри роблять FW2B оптимальним вибором для побудови безпечного і ефективного мережевого вузла на базі OPNsense для організації невеликого розміру [24].

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

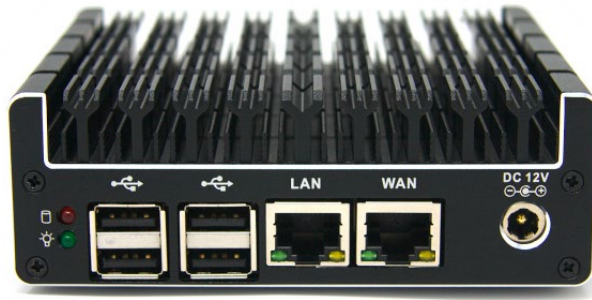


Рисунок 2.3 – Міні-ПК Protectli FW2B Vault 2

При виборі комутатора слід звертати увагу на кількість портів і їх тип (Fast Ethernet або Gigabit Ethernet). Важливими є наявність функцій керування (у разі вибору керованого комутатора), пропускна здатність і швидкість комутації. Додатково варто враховувати тип живлення (звичайне або PoE) та можливість монтажу в стійку.

Тому для побудови мережевої інфраструктури було обрано комутатор Cisco Cisco Catalyst WS-C2960X-24TS-LL, рис.2.4. Комутатори даної серії є популярним рішенням для середнього бізнесу, що поєднують високу надійність, продуктивність і розширені функції керування. Дана модель має 24 порти Gigabit Ethernet і 2 порти SFP для підключення оптичних лінків або аплінків до інших мережевих пристроїв. Комутатор підтримує основні функції рівня 2, зокрема VLAN, STP, EtherChannel, а також функції безпеки, як-от контроль доступу (Port Security) та контроль автентифікації 802.1X. Пристрій має пропускну здатність до 50 Гбіт/с і швидкість пересилання до 41,7 млн пакетів за секунду, що дозволяє ефективно обробляти мережевий трафік. Даний вибір обумовлений надійністю даних пристроїв, енергоефективністю, зручним керуванням через Cisco IOS та сумісністю з іншими пристроями Cisco, що спрощує адміністрування всієї мережі [25].



Рисунок 2.4 – Cisco Catalyst WS-C2960X-24TS-LL

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

При виборі комп'ютера для розгортання Windows Server 2019 важливо враховувати вимоги до обчислювальних ресурсів, а також масштабованість і надійність обраного апаратного забезпечення. Ключовими критеріями є кількість процесорних ядер, обсяг оперативної пам'яті, тип і ємність накопичувачів, підтримка віртуалізації, наявність резервування (наприклад, RAID), а також типи мережевих інтерфейсів.

Тому для розгортання ОС Windows Server 2019 доцільно обирати серверне обладнання з багатоядерним процесором (наприклад, Intel Xeon), не менше 32–64 ГБ оперативної пам'яті з можливістю розширення, швидкісними накопичувачами SSD із підтримкою RAID, а також підтримкою апаратної віртуалізації (Intel VT-x або AMD-V). Важливою є наявність кількох мережевих інтерфейсів (мінімум 1×1GbE), модульної побудови, резервування живлення і підтримки віддаленого адміністрування. Такий підхід забезпечує високу продуктивність, стабільність і масштабованість інфраструктури для реалізації основних ролей Windows Server 2019.

Висновки до другого розділу

В ході роботи над розділом було розроблено логічну топологію IT-інфраструктури на основі трирівневої моделі, яка забезпечує чіткий поділ функціональності між рівнями ядра, розподілу та доступу, що сприяє високій масштабованості, керованості та безпеці мережі. Для побудови мережі обрано один маршрутизатор, чотири комутатори та 50 кінцевих пристроїв, розподілених по рівнях відповідно до їх функцій. Визначено схему IP-адресації в якій статичні адреси призначені мережевим пристроям та серверу, а кінцеві пристрої отримують адреси через DHCP. Усі компоненти мережі будуть інтегровані в єдиний домен, що забезпечить централізоване керування та контроль доступу.

Обґрунтовано вибір технологій та механізмів захисту мережі на базі OPNsense, що забезпечать багаторівневу безпеку IT-інфраструктури. Зокрема, використання правил фаєрвола дозволяє встановити базові обмеження доступу, а інтеграція системи виявлення вторгнень Suricata із пересиланням подій на Syslog-сервер забезпечить моніторинг і реагування на загрози. Вбудований DNS-сервер

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

Unbound із функцією блокування доменів підвищить безпеку та керованість запитів до зовнішніх ресурсів, а впровадження двофакторної аутентифікації значно посилить захист адміністративного доступу. Сукупне використання цих засобів сформує цілісну систему захисту.

Також в ході аналізу було обґрунтовано вибір апаратного забезпечення для розгортання основних компонентів мережевої інфраструктури, а саме маршрутизатора з функціями фаєрвола на базі OPNsense, комутаторів та сервера з ОС Windows Server 2019. Вибір здійснювався з урахуванням вимог до продуктивності, надійності та підтримки сучасних мережевих технологій.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

РОЗДІЛ 3. ВПРОВАДЖЕННЯ, НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ

3.1. Базове налаштування мережі IT-інфраструктури

Подальше налаштування мережевої інфраструктури та тестування її функціональності буде виконано у віртуальному середовищі за допомогою емулятора GNS3. Для запуску віртуальних машин, зокрема OPNsense, Windows Server та Windows 10, використовуватиметься VirtualBox у поєднанні з GNS3. Такий підхід дає змогу створити гнучке й реалістичне тестове середовище, яке імітує роботу фізичної мережі, водночас усуваючи потребу у використанні реального обладнання. Це дозволяє ефективно виконати необхідні налаштування, перевірити конфігурації та тестувати взаємодію мережевих компонентів у безпечних і контрольованих умовах.

Почнемо налаштування з комутаторів мережі. В рамках конфігурації комутаторів було налаштовано основні мережеві параметри. Задано IP-шлюз за замовчуванням, визначено домен (klymenko.net), призначено IP-адресу для VLAN 1 як основного інтерфейсу. Нижче на рис.3.1 наведено приклад налаштувань на SW-23-8-1.

```
SW-23-8-1(config)#no ip routing
SW-23-8-1(config)#ip default-gateway 192.168.0.254
SW-23-8-1(config)#ip domain-name klymenko.net
SW-23-8-1(config)#ip domain-lookup
SW-23-8-1(config)#ip name-server 192.168.0.200
SW-23-8-1(config)#int vlan 1
SW-23-8-1(config-if)#ip address 192.168.0.253 255.255.255.0
SW-23-8-1(config-if)#no shutdown
```

Рисунок 3.1 – Налагодження SW-23-8-1

Далі перейдемо до сервера Windows Server 2019, тобто до Serv-23-8-1. Першим кроком в налаштуванні буде задання адресації згідно виконаного розподілу адрес, рис.3.2.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

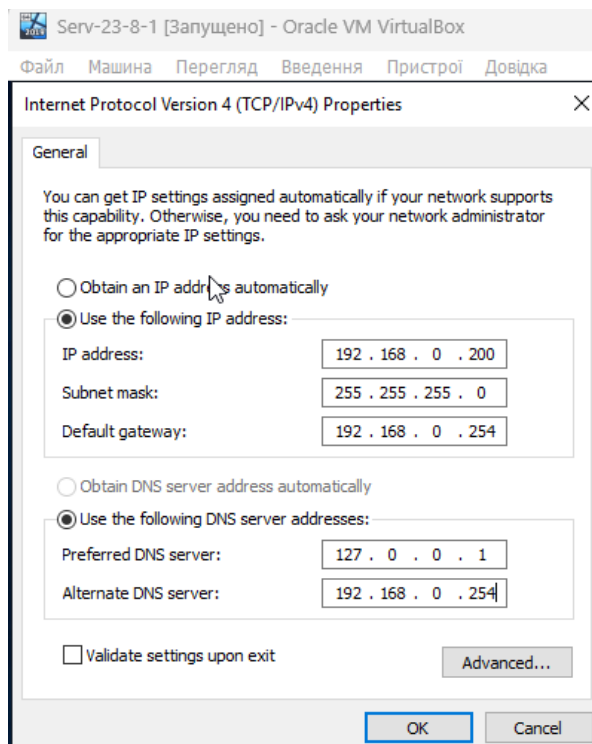


Рисунок 3.2 – Налаштування адресації Serv-23-8-1

Наступним етапом є розгортання Active Directory із встановленням необхідних ролей і функцій, а також створенням домену klumenko.net, рис.3.3-3.5.

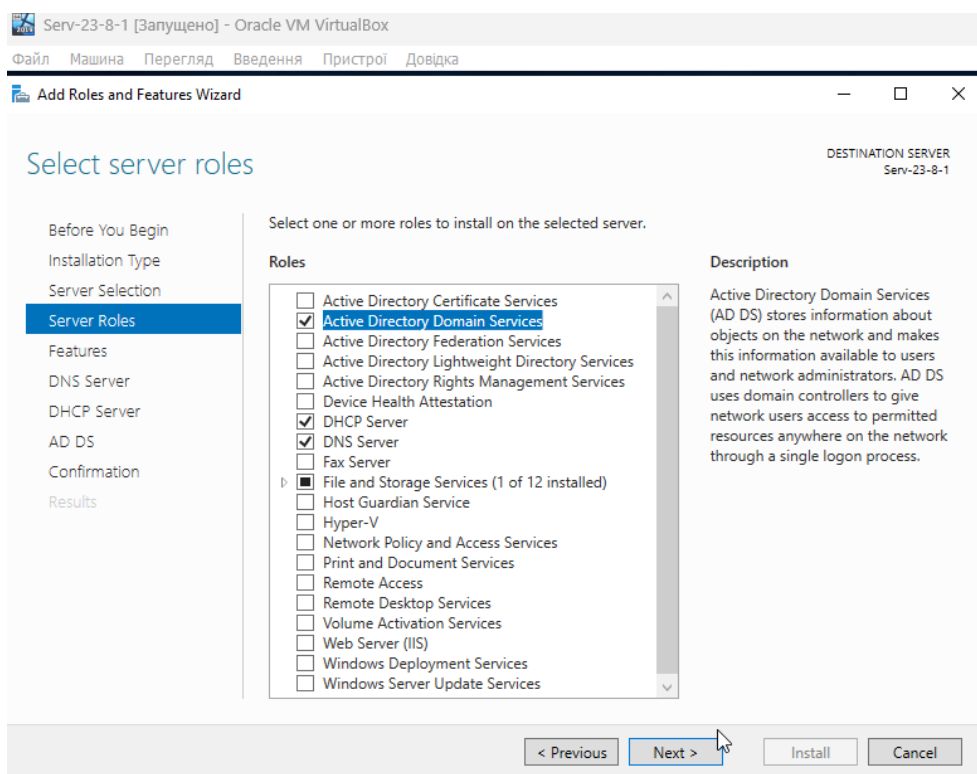


Рисунок 3.3 – Додавання ролей і компонентів Windows Server

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

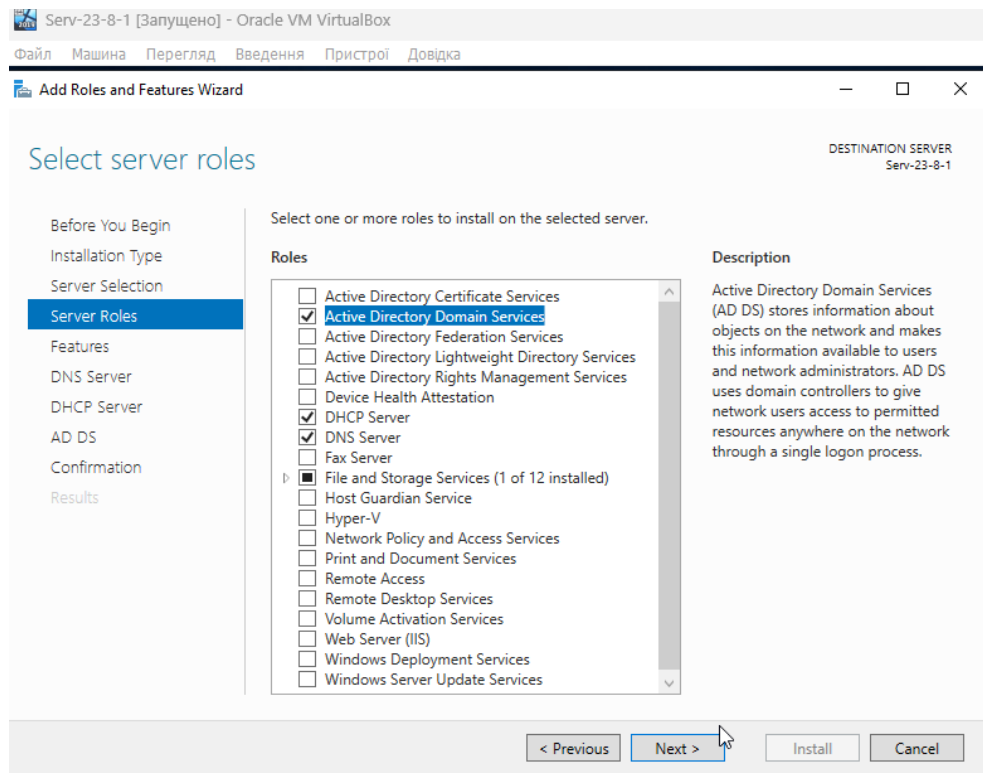


Рисунок 3.4 – Результати успішного встановлення ролей і компонентів на сервері

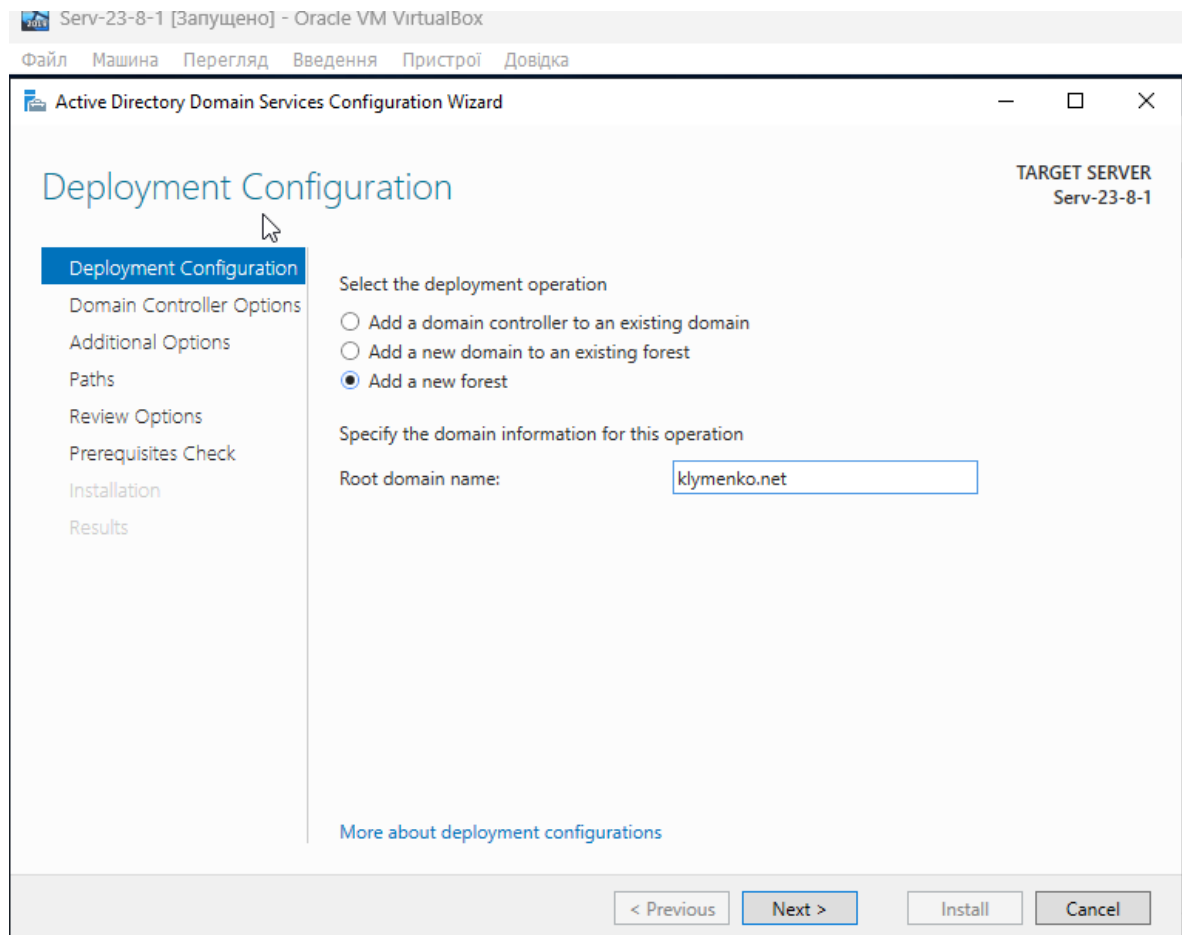


Рисунок 3.5 – Розгортання нового домену klymenko.net

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк. 47
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		

На сервері виконується налаштування служби DHCP, яка забезпечить автоматичну видачу IP-адрес кінцевим пристроям у локальній мережі. Для цього створюється новий пул адрес, задаються параметри мережі, включаючи шлюз, DNS-сервер і тривалість оренди, що дозволить централізовано керувати адресацією та зменшити ризик конфліктів IP-адрес, рис.3.6-3.10.

Serv-23-8-1 [Запущено] - Oracle VM VirtualBox

Файл Машина Перегляд Введення Пристрої Довідка

New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 0 . 1

End IP address: 192 . 168 . 0 . 254

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

Рисунок 3.6 – Визначення пулу видачі адрес

Serv-23-8-1 [Запущено] - Oracle VM VirtualBox

Файл Машина Перегляд Введення Пристрої Довідка

New Scope Wizard

Add Exclusions and Delay
Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: . . . End IP address: . . . Add

Excluded address range:
192.168.0.200 to 192.168.0.254 Remove

Subnet delay in milli second:
0

< Back Next > Cancel

Рисунок 3.7 – Виключення незадіяних адрес

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

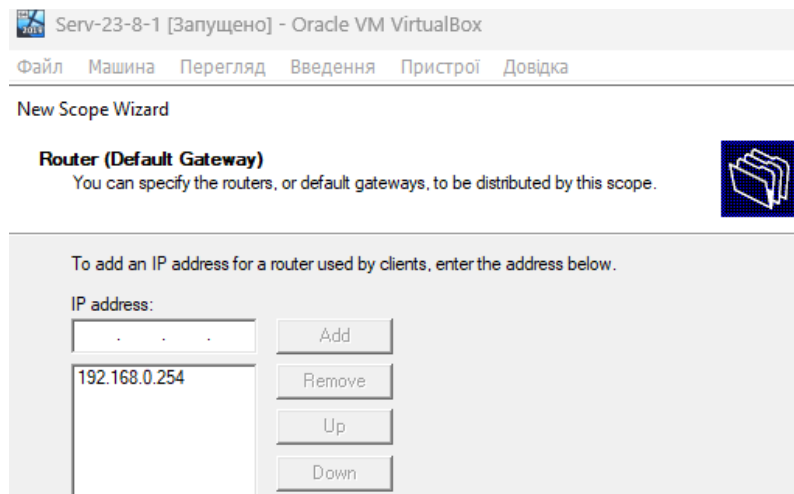


Рисунок 3.8 – Шлюз за замовчуванням

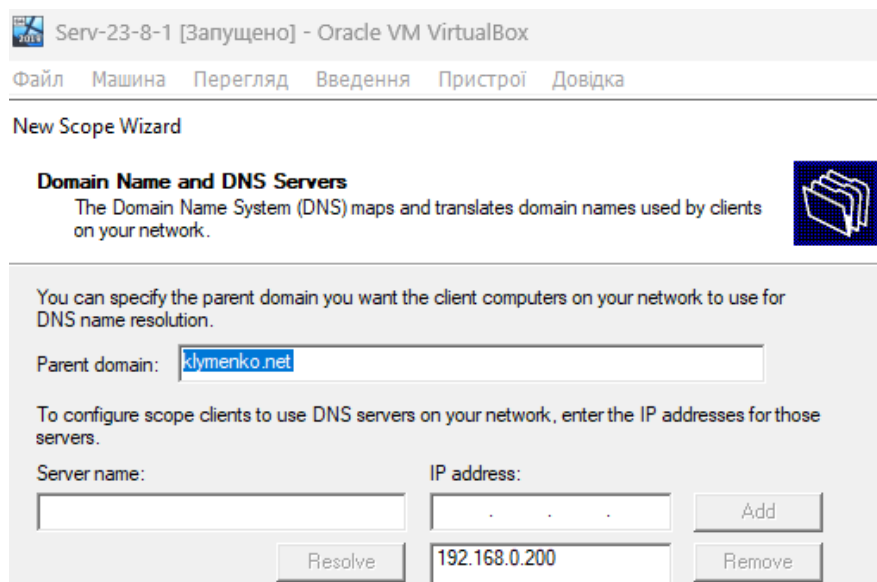


Рисунок 3.9 – Домене ім'я та адреса DNS-серверу

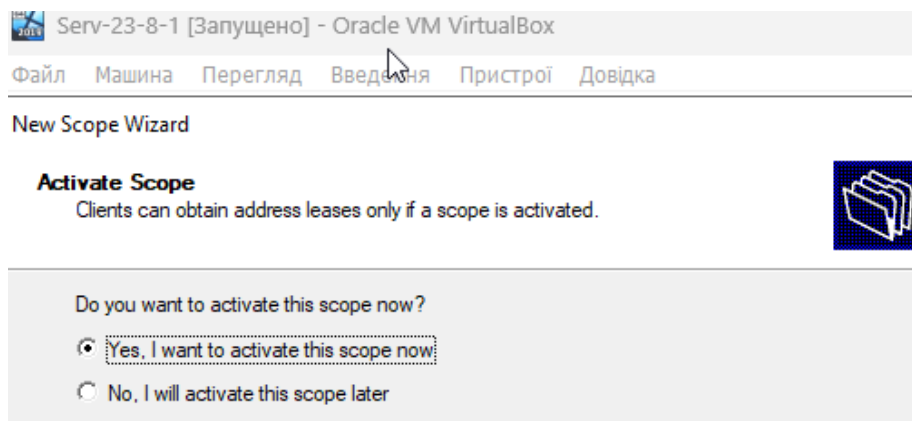


Рисунок 3.10 – Активація налаштованої області DHCP

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

Виконується налаштування служби DNS із доданням записів типу А для основних мережевих пристроїв. Це дає змогу зіставити доменні імена з відповідними IP-адресами, що спрощує адресацію в мережі та забезпечує стабільну роботу внутрішніх сервісів, рис.3.11-3.12.

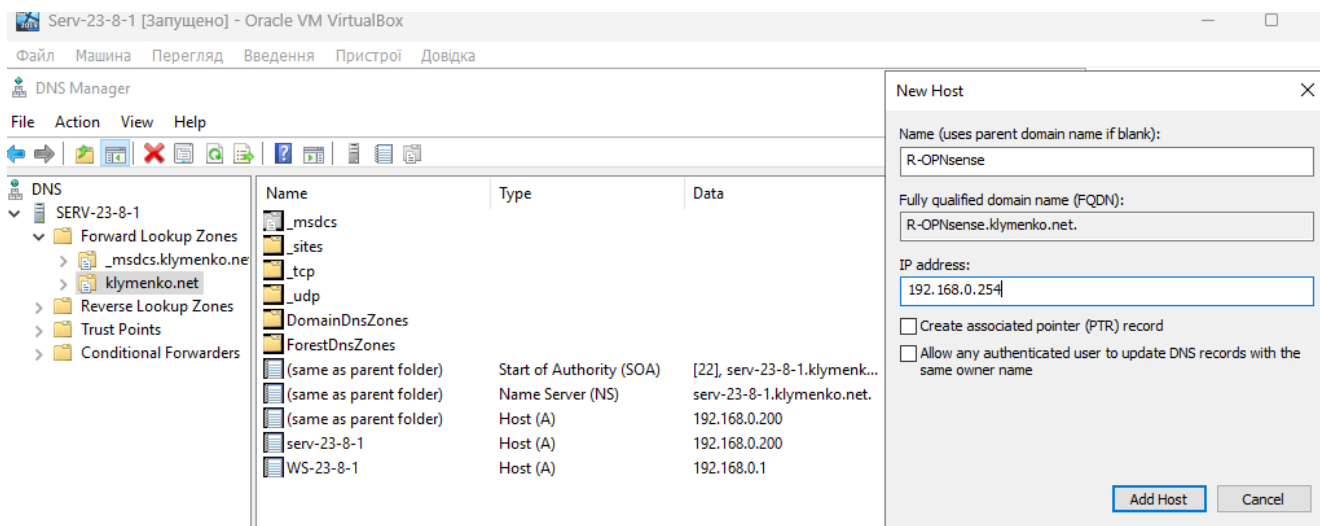


Рисунок 3.11 – Додання DNS-записів мережевих пристроїв типу А

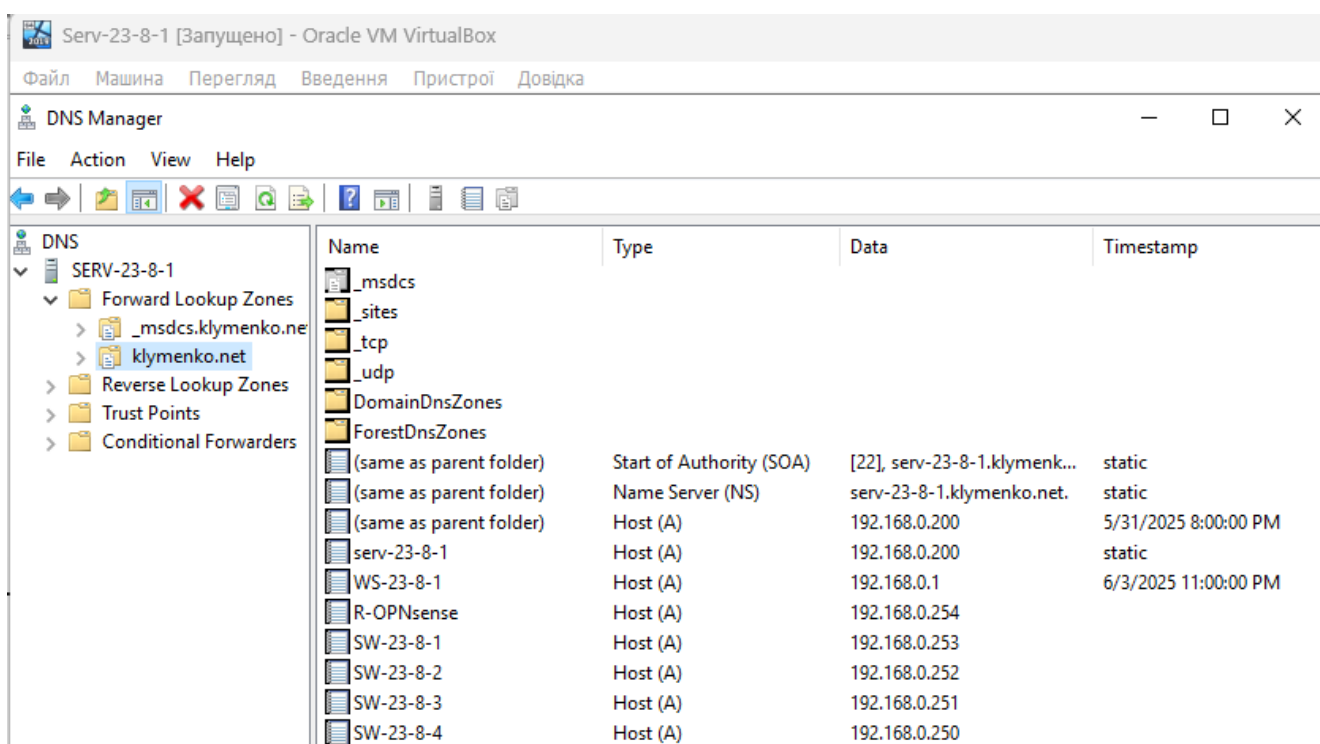


Рисунок 3.12 – Додання DNS-записів мережевих пристроїв типу А

На завершальному етапі конфігурації служб AD створюються облікові записи користувачів у доменній структурі. Для кожного користувача задаються унікальні імена входу, паролі. Це дозволяє централізовано керувати доступом до ресурсів мережі та забезпечити контроль за правами користувачів.

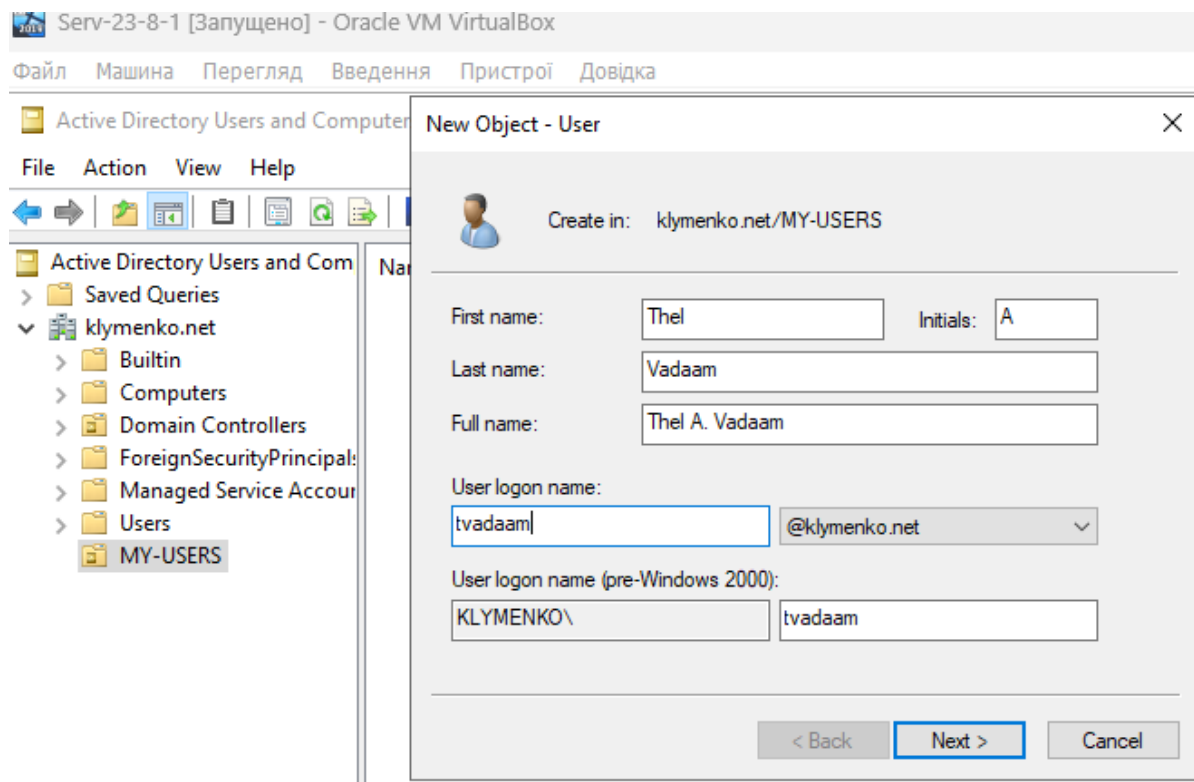


Рисунок 3.13 – Створення користувача в організаційній структурі MY-USERS

Для збору та моніторингу системних журналів у мережі буде використано застосунок Syslog Watcher, який виконуватиме роль syslog-сервера на Windows Server. Дане програмне забезпечення дає змогу приймати, зберігати та аналізувати повідомлення з різних мережевих пристроїв. Використання Syslog Watcher [26] дозволяє централізувати логування, оперативно виявляти потенційні проблеми та підвищити рівень контролю за станом мережевої інфраструктури, рис.3.14.

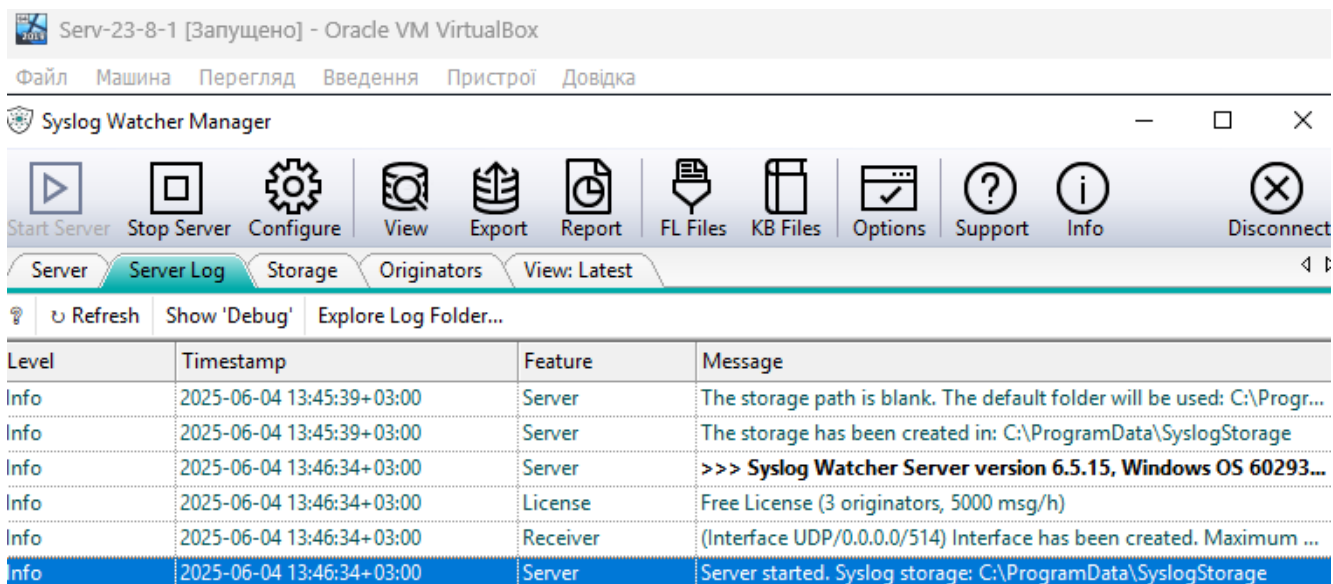


Рисунок 3.14 – Встановлений і запущений застосунок Syslog Watcher

Перейдемо до комутаторів. На цих пристроях виконується налаштування надсилання системних журналів на Syslog-сервер. Це дозволяє фіксувати важливі події з боку мережевого обладнання в централізованому журналі для подальшого аналізу. Також виконується налаштування синхронізації часу за протоколом NTP, що забезпечує точність часових позначок у логах, необхідну для коректного аналізу подій та усунення неспівпадінь у часі між пристроями, рис.3.15.

```
SW-23-8-1(config)#ntp server serv-23-8-1
SW-23-8-1(config)#ntp update-calendar
SW-23-8-1(config)#clock timezone UA 2 0
SW-23-8-1(config)#clock summer-time UA recurring last Sun Mar 3:00 last Sun Oct 4:00
SW-23-8-1(config)#logging serv-23-8-1
SW-23-8-1(config)#logging trap informational
SW-23-8-1(config)#service timestamps log datetime show-timezone msec
SW-23-8-1(config)#service timestamps debug datetime show-timezone msec
SW-23-8-1(config)#logging on
```

Рисунок 3.15 – Налаштування роботи Syslog та NTP на комутаторах

На всіх кінцевих станціях з ОС Windows 10 виконується налаштування мережевих адаптерів на автоматичне отримання IP-адреси та параметрів DNS-сервера за допомогою DHCP, рис.3.16. Це дає змогу централізовано керувати адресацією клієнтських пристроїв, спрощує адміністрування мережі та зменшує ризик конфліктів IP-адрес. Станції автоматично отримуватимуть відповідні мережеві параметри від DHCP-сервера, розгорнутого на Windows Server.

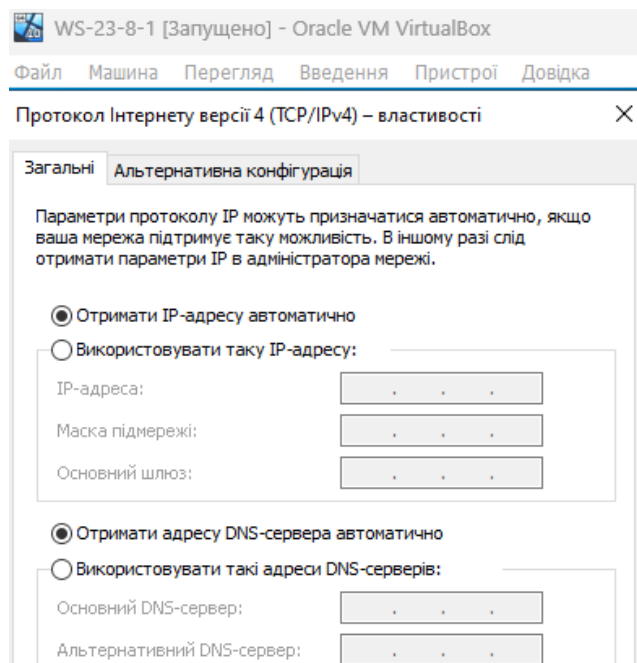


Рисунок 3.16 – Налаштування динамічної адресації на Windows 10

На кожній кінцевій станції після успішного отримання мережевих параметрів виконується приєднання до домену klymenko.net. Для цього в параметрах системи задається доменне ім'я, після чого вводяться облікові дані адміністратора домену, рис.3.17. Після успішного приєднання комп'ютер перезавантажується, і користувачі можуть виконувати вхід до системи з доменними обліковими записами.

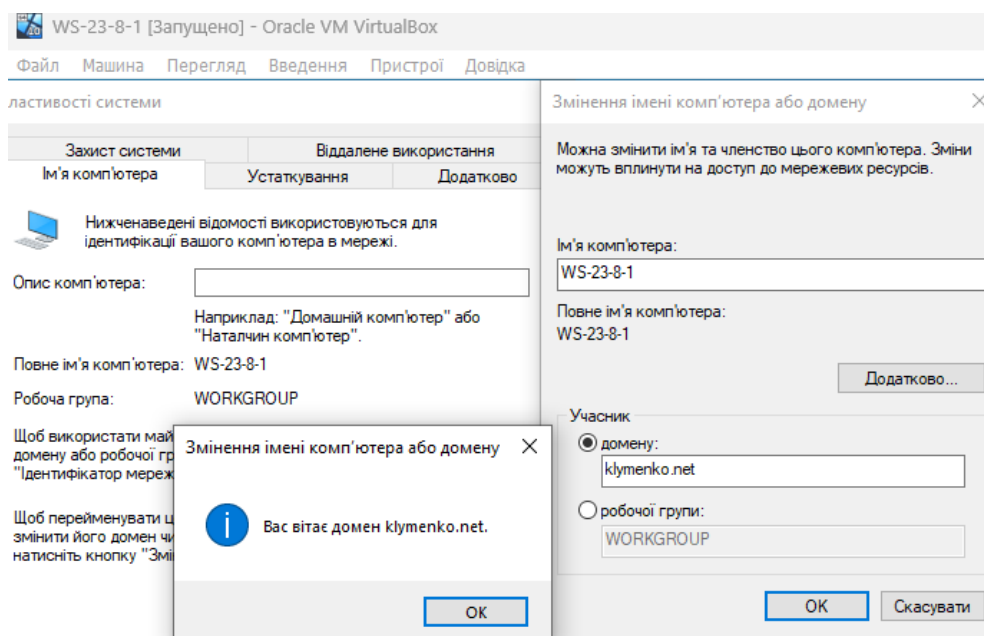
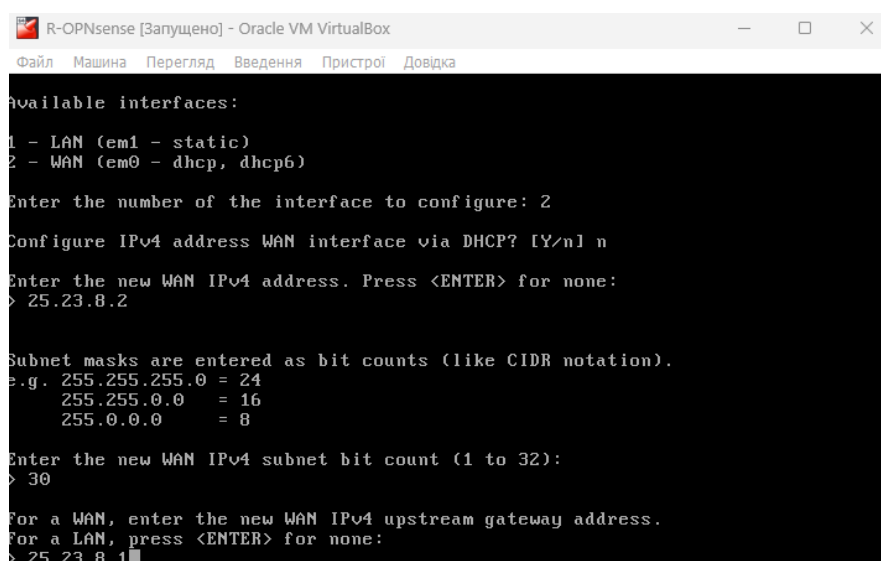


Рисунок 3.17 – Приєднання комп'ютера до домену klymenko.net

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

3.2 Встановлення та налаштування OPNsense

Переходимо до розгортання і налаштування OPNsense. Після успішного встановлення образу здійснюється первинне налаштування інтерфейсів. Для WAN-інтерфейсу задається фіксована IP-адреса, що використовується для з'єднання з зовнішньою мережею (Інтернетом). LAN-інтерфейс отримує статичну IP-адресу з внутрішнього діапазону та виконує роль шлюзу для локальної мережі. Також налаштовується маршрут за замовчуванням через зовнішній шлюз, а NAT і базові правила фаєрвола активуються автоматично для забезпечення захищеного виходу пристроїв локальної мережі в Інтернет.



```
R-OPNsense [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

Available interfaces:
1 - LAN (em1 - static)
2 - WAN (em0 - dhcp, dhcp6)

Enter the number of the interface to configure: 2

Configure IPv4 address WAN interface via DHCP? [Y/n] n

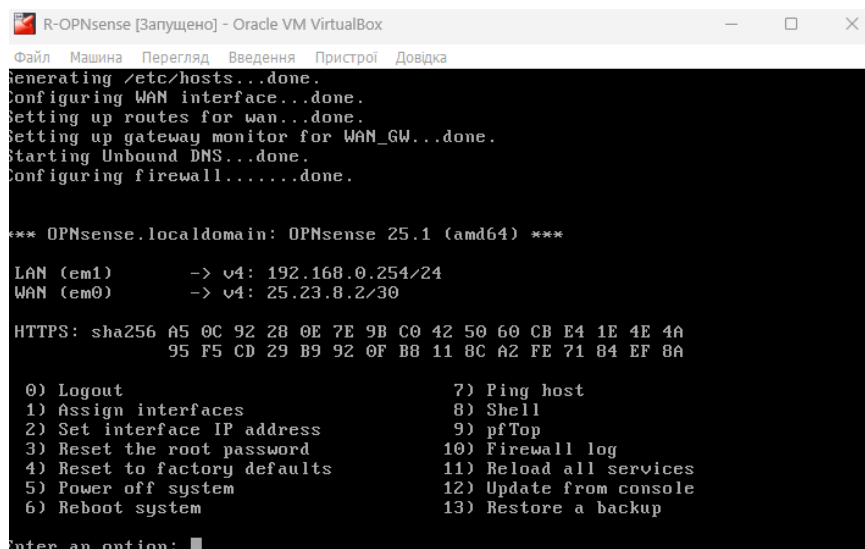
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 25.23.8.2

Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 30

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 25.23.8.1
```

Рисунок 3.18 – Налаштування параметрів адресації WAN-інтерфейсу OPNsense



```
R-OPNsense [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

generating /etc/hosts...done.
configuring WAN interface...done.
setting up routes for wan...done.
setting up gateway monitor for WAN_GW...done.
Starting Unbound DNS...done.
configuring firewall.....done.

*** OPNsense.localdomain: OPNsense 25.1 (amd64) ***

LAN (em1)      -> v4: 192.168.0.254/24
WAN (em0)      -> v4: 25.23.8.2/30

HTTPS: sha256 A5 0C 92 28 0E 7E 9B C0 42 50 60 CB E4 1E 4E 4A
          95 F5 CD 29 B9 92 0F B8 11 8C A2 FE 71 84 EF 8A

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

Enter an option: 
```

Рисунок 3.19 – Параметри інтерфейсів OPNsense

Після налаштування базових параметрів OPNsense здійснюється підключення до веб-інтерфейсу керування з боку Windows Server. Для цього у веб-браузері вводиться домене ім'я даного маршрутизатора або його IP-адреса LAN інтерфейсу, після чого відбувається авторизація за допомогою стандартних облікових даних адміністратора (логін:root, пароль:opnsense), рис.3.20-3.21. Під час першого підключення браузер повідомляє про незахищене з'єднання, оскільки OPNsense використовує самопідписаний SSL-сертифікат, який не був виданий довіреним центром сертифікації. Це стандартне попередження, яке можна обійти. Однак в реальному середовищі доцільно встановити і налаштувати довірений сертифікат.

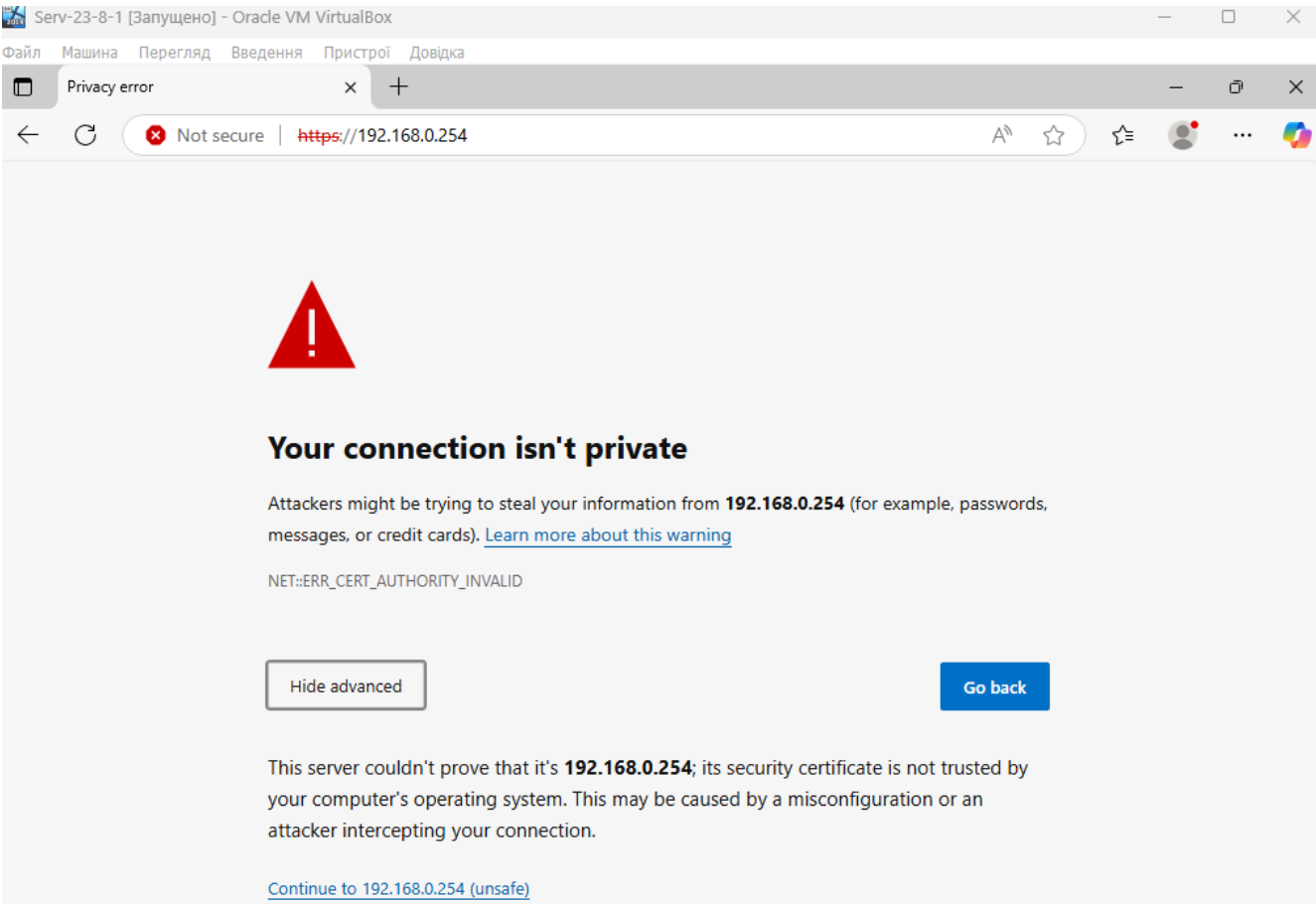


Рисунок 3.20 – Перехід у веб-інтерфейс OPNsense

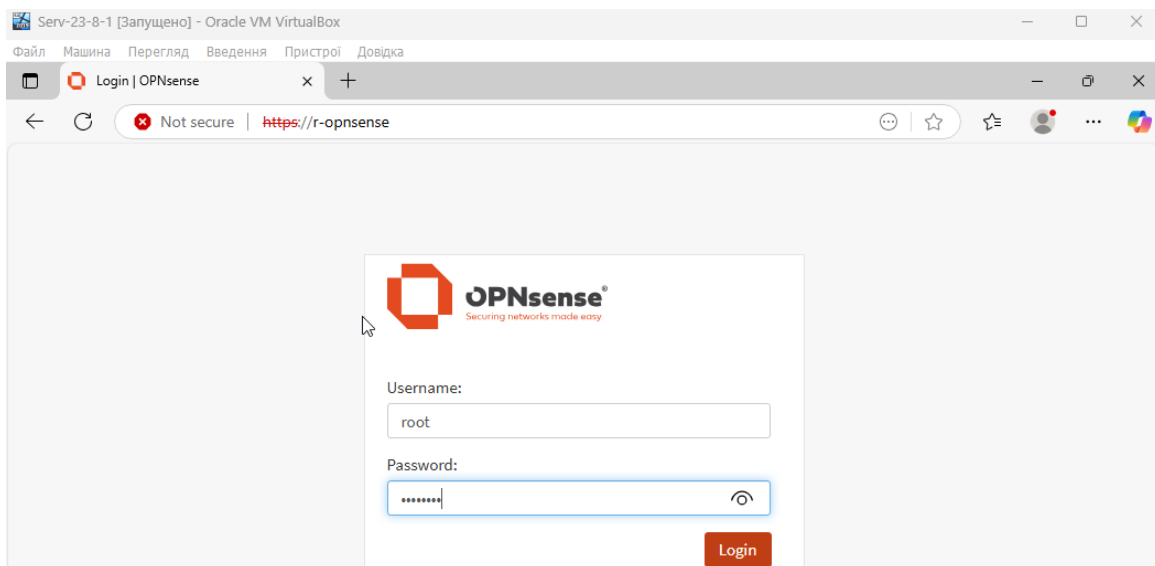


Рисунок 3.21 – Аутентифікація у веб-інтерфейсі

Після успішного входу до веб-інтерфейсу OPNsense автоматично відкривається майстер первинного налаштування (Wizard), який дозволяє покроково задати ключові параметри системи. За допомогою цього майстра виконується налаштування загальних параметрів, пароля користувача, конфігурація WAN- та LAN-інтерфейсів, налаштування DNS-серверів, часу та інших базових параметрів, рис.3.22-3.24. Після чого пристрій перезавантажиться.

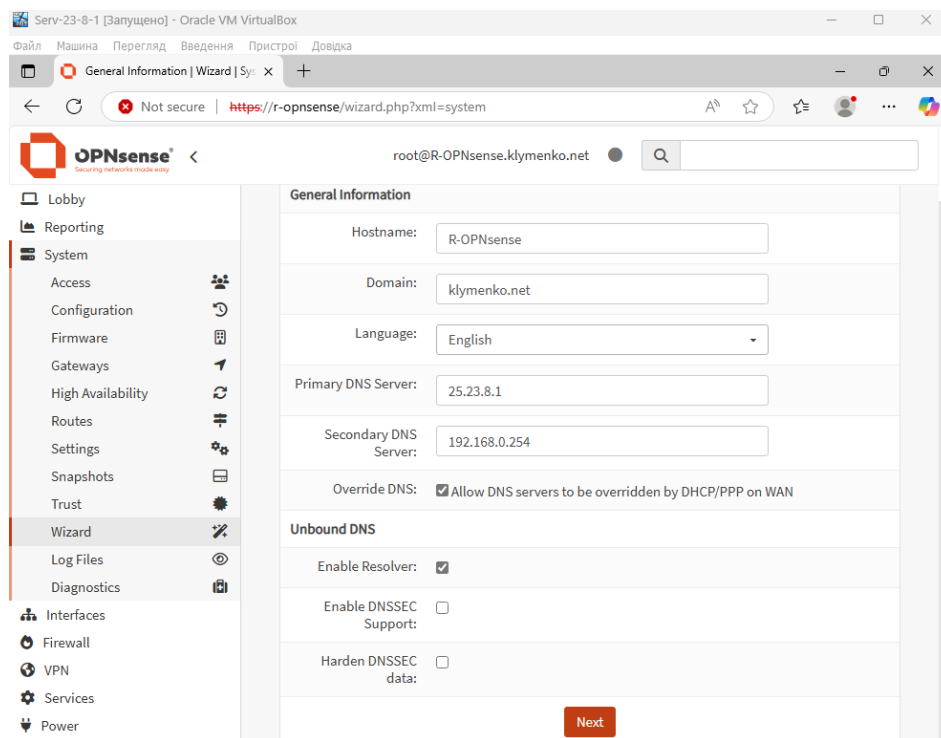


Рисунок 3.22 – Майстер налаштувань загальної інформації про пристрій

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

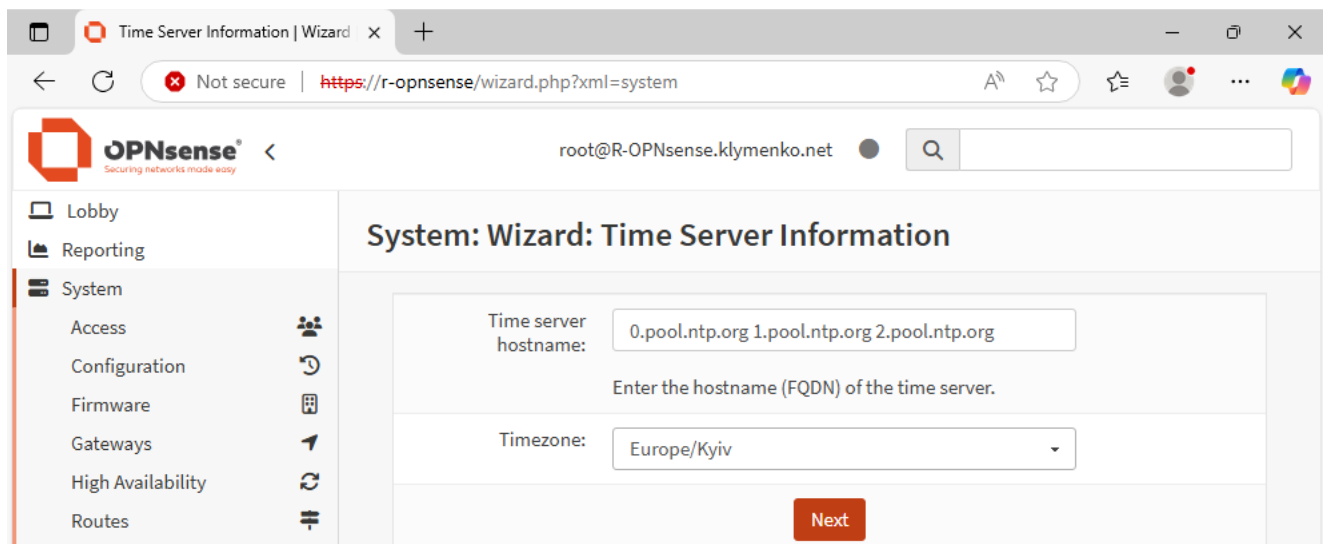


Рисунок 3.23 – Майстер налаштувань часових параметрів

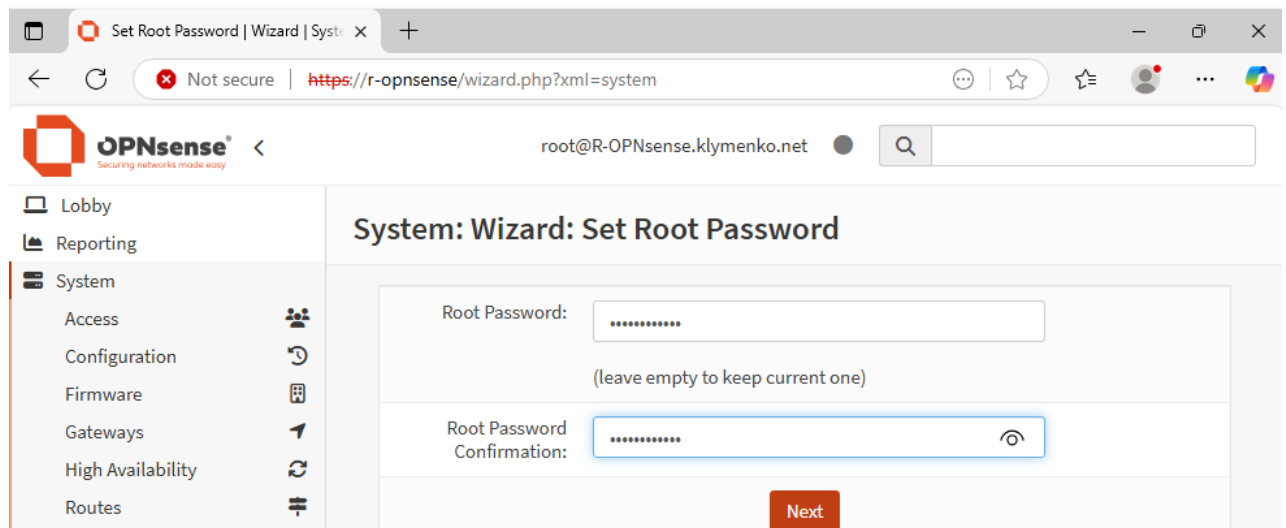


Рисунок 3.24 – Майстер налаштувань паролю для root користувача

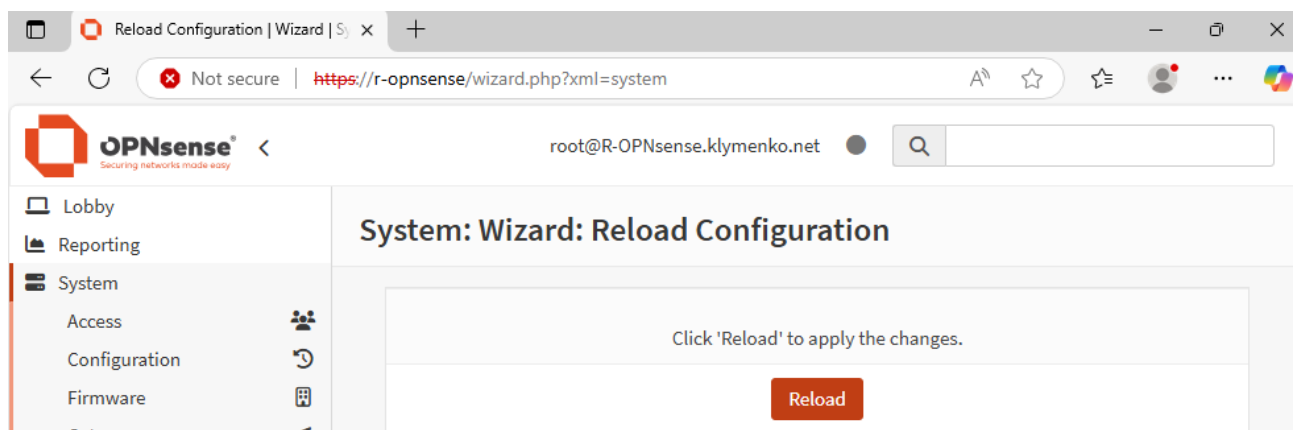


Рисунок 3.25 – Перезапуск пристрою для застосування налаштувань

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

Після перезавантаження система автоматично застосувала всі внесені зміни та повернула нас до головного меню веб-інтерфейсу OPNsense. Тут відображається основна інформація про стан системи, завантаження, мережеві інтерфейси, активні служби та системні повідомлення. З цього розділу можна перейти до повного набору функцій для подальшого налаштування фаєрвола, маршрутизації, VPN, IPS та інших компонентів, рис.3.26.

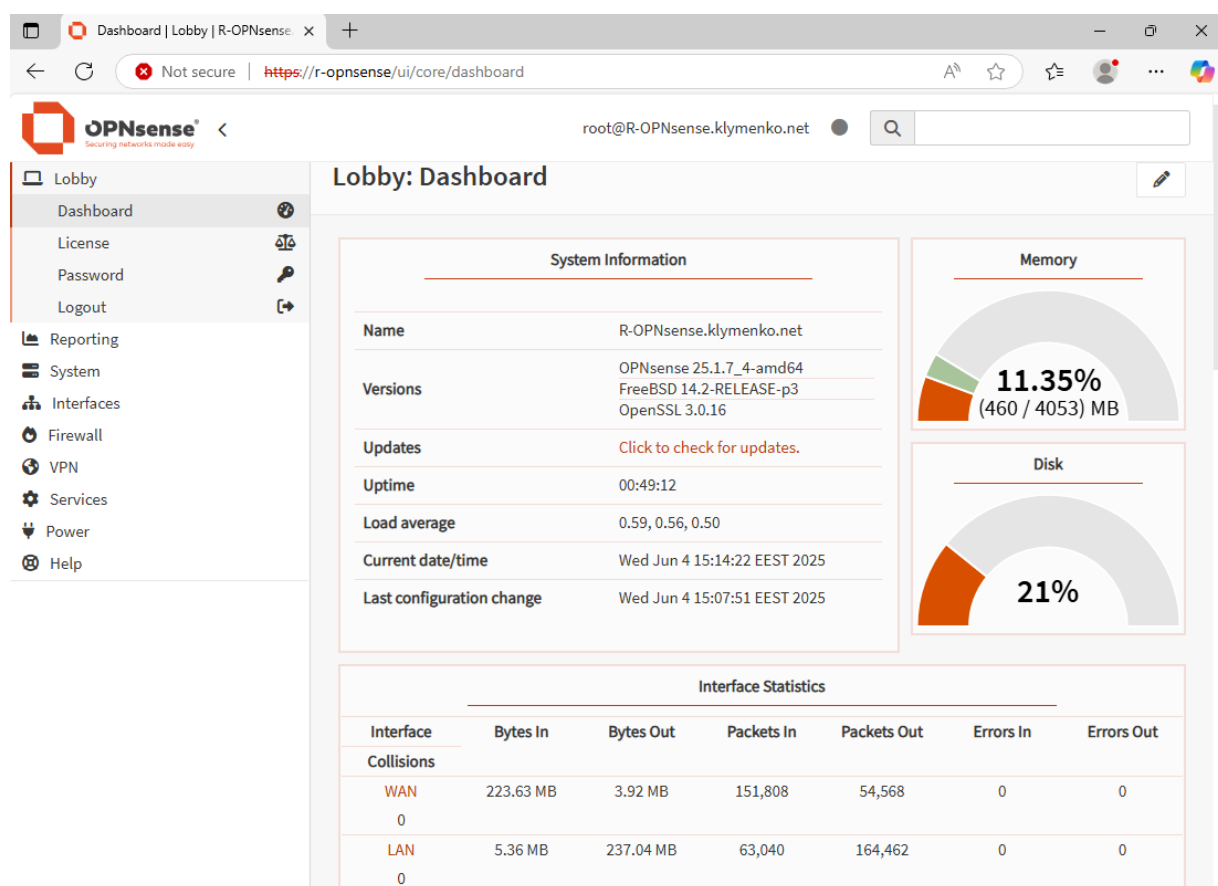


Рисунок 3.26 – Головне вікно OPNsense

Переходимо до налаштування брандмауера, а саме до правил на інтерфейсі WAN. Тут вже за замовчуванням створено набір системних правил, які забезпечують базовий рівень безпеки, рис.3.27. Серед них – правила блокування приватних і зарезервованих мереж, захист від трафіку з недійсними або забороненими адресами, дозволи на службові ICMP-запити, обмеження для підозрілих з'єднань, а також дозволи для вихідного трафіку з самого фаєрвола. Ці правила автоматично застосовуються для запобігання типових загроз зі сторони Інтернету й не потребують ручного втручання на початковому етапі налаштування.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

Однак за потреби користувач може власноруч дозволити доступ до тих чи інших портів чи IP-адрес.

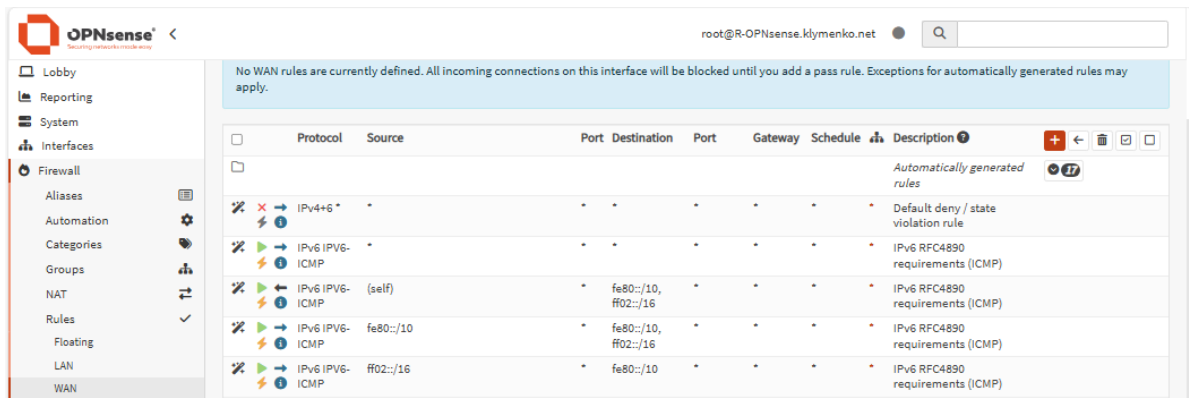


Рисунок 3.27 – Частина правил для інтерфейсу WAN

На інтерфейсі LAN також присутній набір автоматично створених правил, призначених для забезпечення базової роботи локальної мережі, рис.3.28. Зокрема, дозволено повний доступ з локальної мережі до будь-яких зовнішніх ресурсів. Також додано спеціальні правила для запобігання блокуванню доступу до веб-інтерфейсу фаєрвола (anti-lockout), правила вихідного трафіку від самого фаєрвола, ICMP для IPv6, обмеження на порт 0, а також захист від підозрілих підключень через sshlockout і virusprot. Така конфігурація дозволяє користувачам локальної мережі вільно і безпечно виходити в Інтернет і взаємодіяти з фаєрволом. Всі згенеровані правила для інтерфейсів WAN та LAN наведені в додатку Б.1 та Б.2.

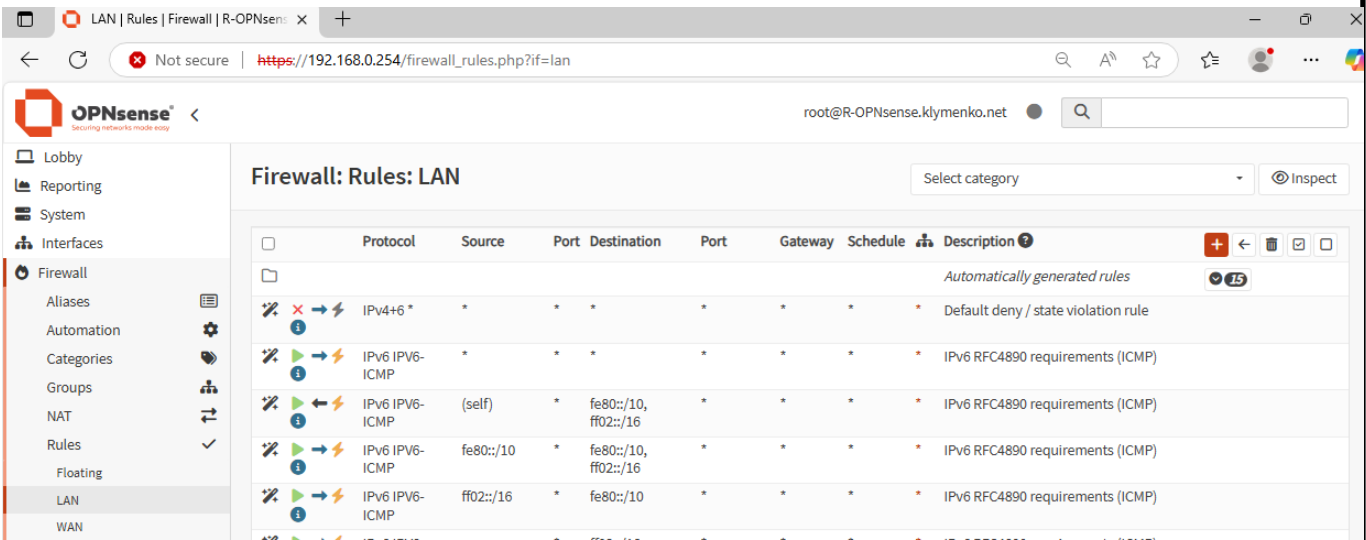


Рисунок 3.28 – Частина правил для інтерфейсу LAN

Далі виконаємо налаштування пересилки повідомлень про виявлені порушення системи виявлення вторгнень Suricata на Syslog-сервер. У веб-інтерфейсі OPNsense перейдемо до розділу Sytem – Settings – Logging та активуємо опцію надсилання подій. Після цього вкажемо домене ім'я Syslog-сервера, тип подій які слід надсилати та рівень сповіщень, рис.3.29.

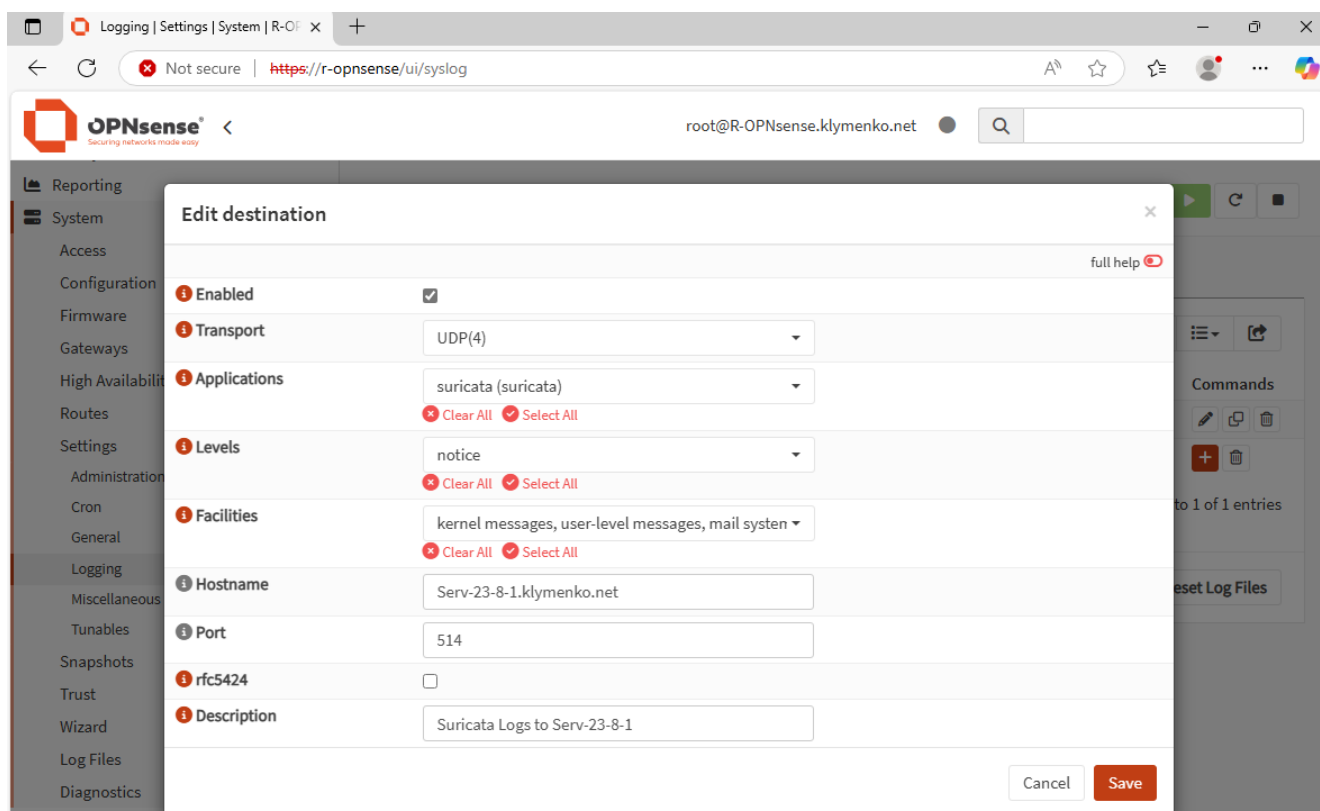


Рисунок 3.29 – Налаштування відправки сповіщень Suricata на Syslog-сервер

Тепер перейдемо до налаштувань Suricata на сторінці Services – Intrusion Detection – Administration. У цьому розділі активуємо опцію «Enabled», а також «IPS Mode» для забезпечення активного виявлення і блокування трафіку. Зазначимо інтерфейси, на яких здійснюватиметься перевірка (LAN та WAN), виберемо режим сканування «Nmapscan» і включимо логування подій, рис.3.30.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

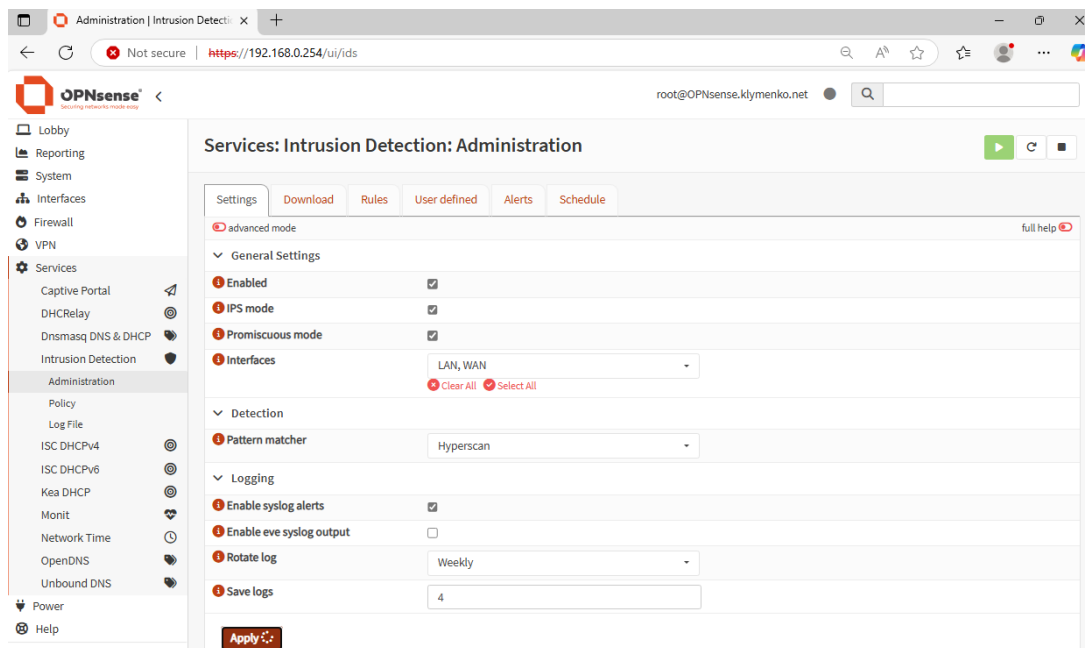


Рисунок 3.30 – Базові налаштування Suricata

Наступним етапом є завантаження та активація правил виявлення загроз. Для цього слід перейти до розділу Services – Intrusion Detection – Download і обрати відповідні набори правил. Після вибору виконується їх завантаження, а потім – активація у вкладці Rules. В даному випадку завантажимо і активуємо всі доступні набори правил, рис.3.31-3.32. На цьому базова робота Suricata налагоджена.

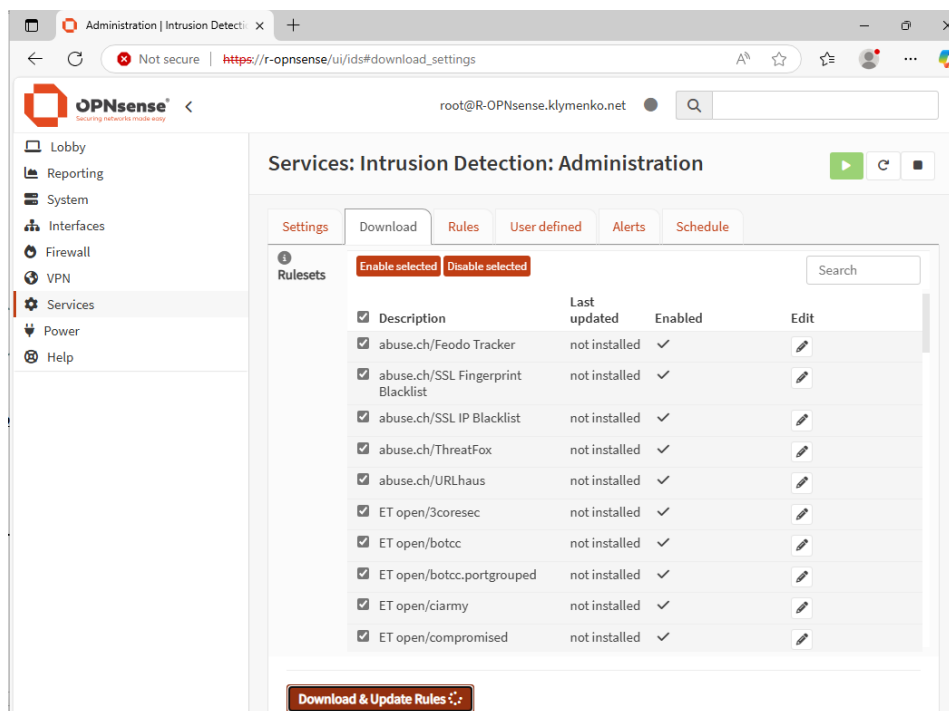


Рисунок 3.31 – Завантаження категорій правил

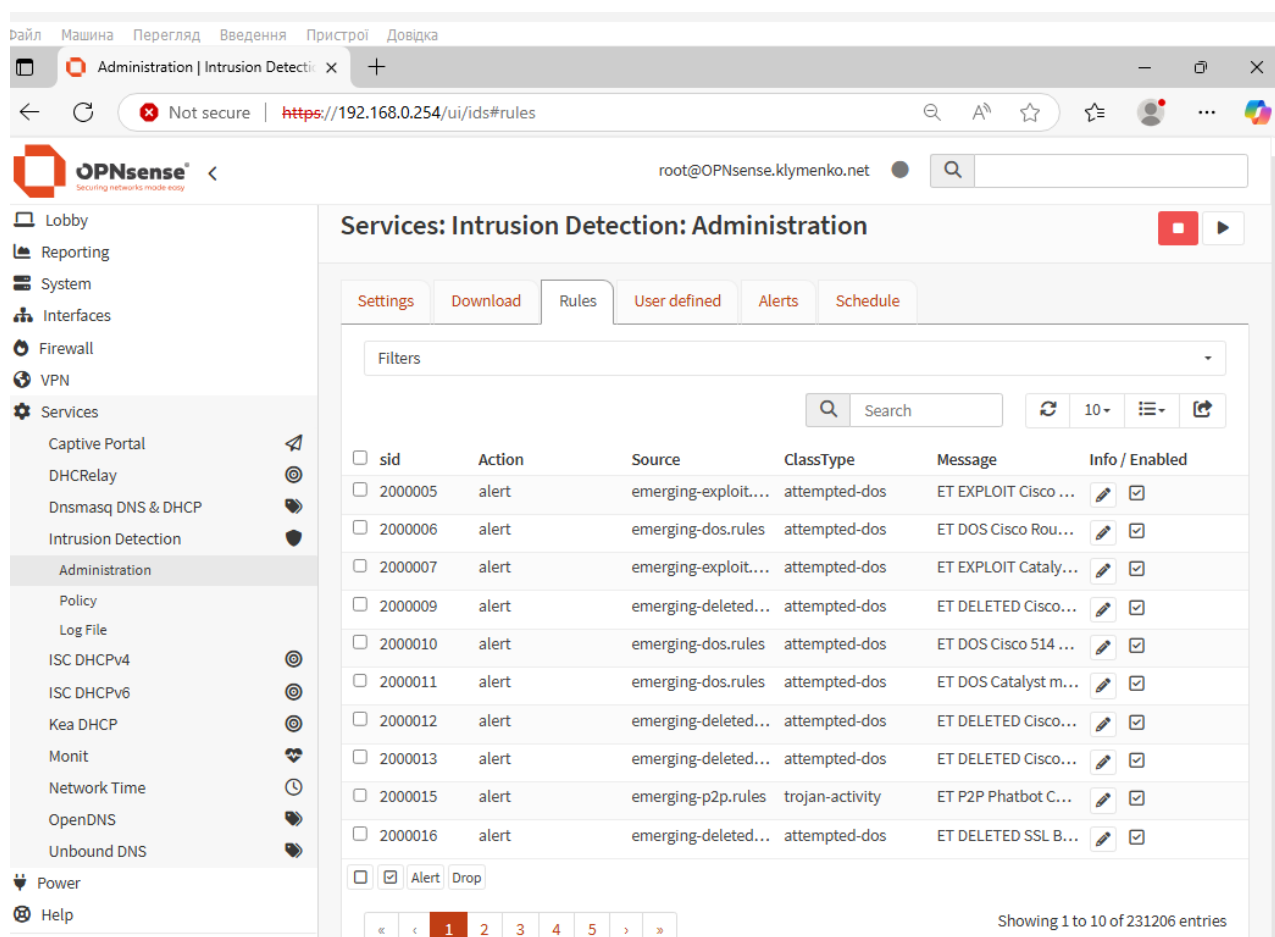


Рисунок 3.32 – Активація правил

Unbound DNS – це рекурсивний DNS-сервер, вбудований в OPNsense, який забезпечує розв’язання DNS-запитів напряму, без необхідності звернення до провайдерського DNS. Це підвищує швидкість, контроль і безпеку DNS-обробки в мережі. Завдяки інтеграції з DNSBL (DNS Blocklist), Unbound DNS дозволяє блокувати запити до відомих шкідливих, рекламних або трекінгових доменів, що підвищує загальний рівень захисту користувачів. У розділі Services – Unbound DNS – Blocklist можна додати відповідні списки блокування, після чого DNS-сервер автоматично блокуватиме запити до цих доменів. Додатково також була активована функція Force SafeSearch, яка примусово вмикає фільтрацію пошукового контенту на популярних платформах, таких як Google, YouTube та Bing, що особливо актуально в навчальних або корпоративних мережах, рис.3.33.

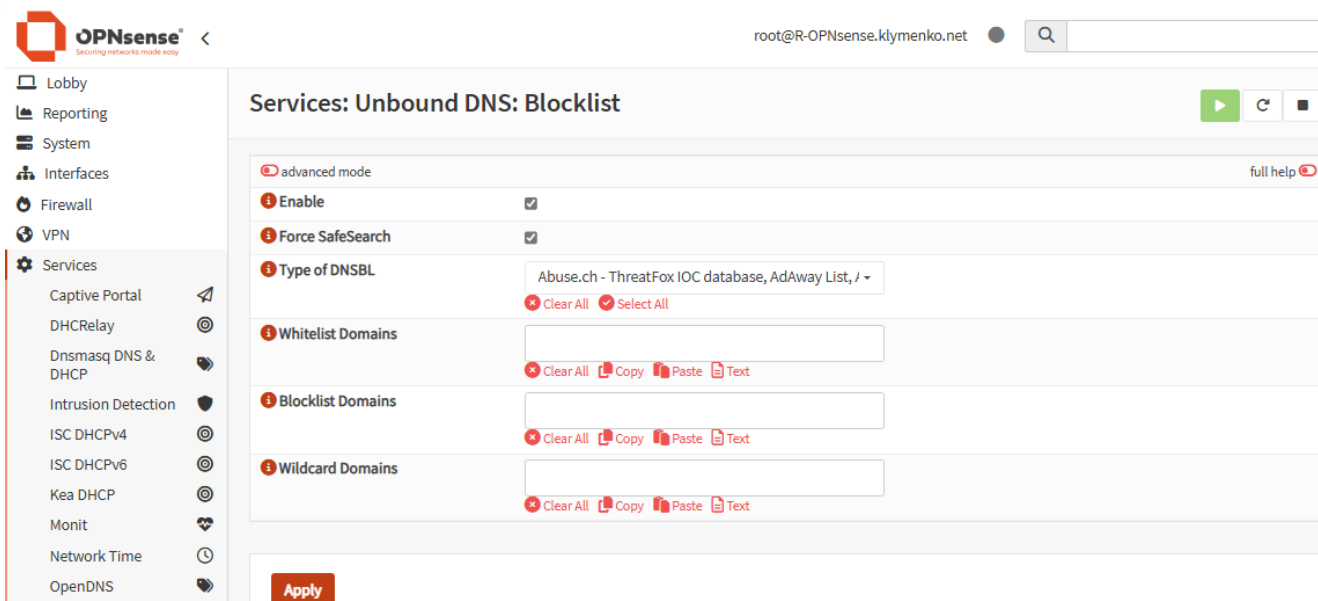


Рисунок 3.33 – Вибір списків блокування доменів

Для підвищення рівня безпеки доступу до веб-інтерфейсу OPNsense виконаємо налаштування двофакторної автентифікації (2FA) з використанням мобільного автентифікатора, наприклад Google Authenticator. Для цього в меню System – Access – Servers створюємо новий сервер типу «Local + Timebased One Time Password». Інші поля не змінюємо, рис.3.34.

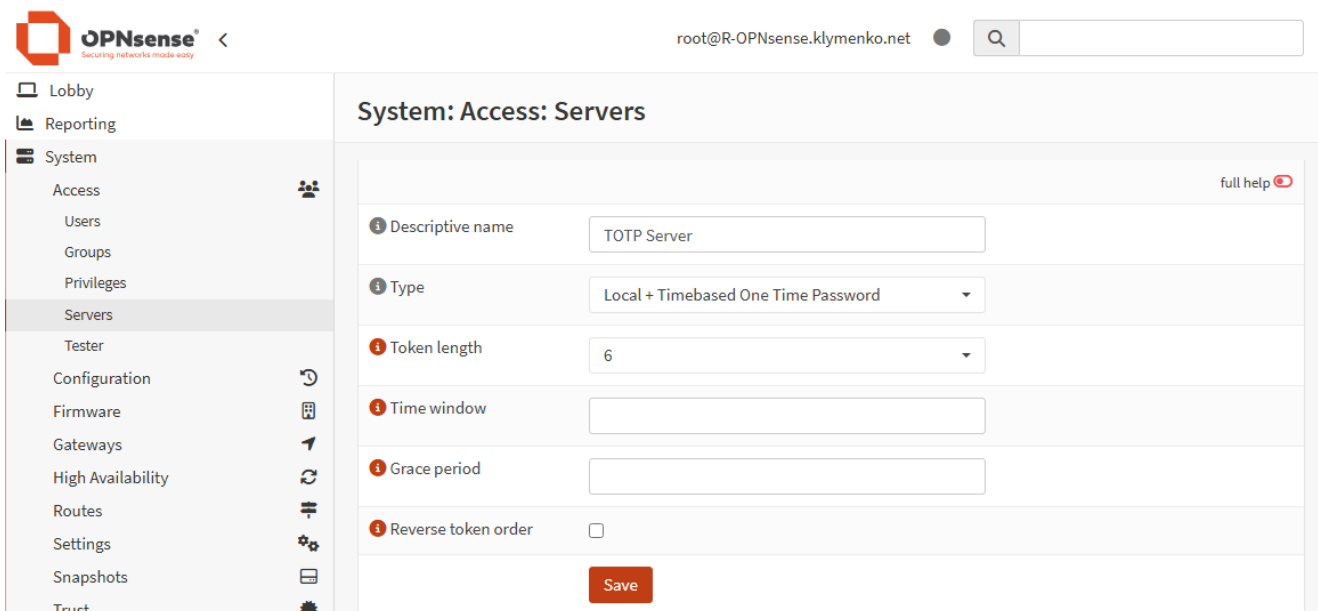


Рисунок 3.34 – Створення серверу типу Timebased One Time Password(TOTP)

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі у розділі System – User Manager додаємо новий обліковий запис адміністратора, рис.3.35, та активуємо опцію TOTP, після чого буде згенеровано QR-код, рис.3.36, який потрібно просканувати мобільним автентифікатором.

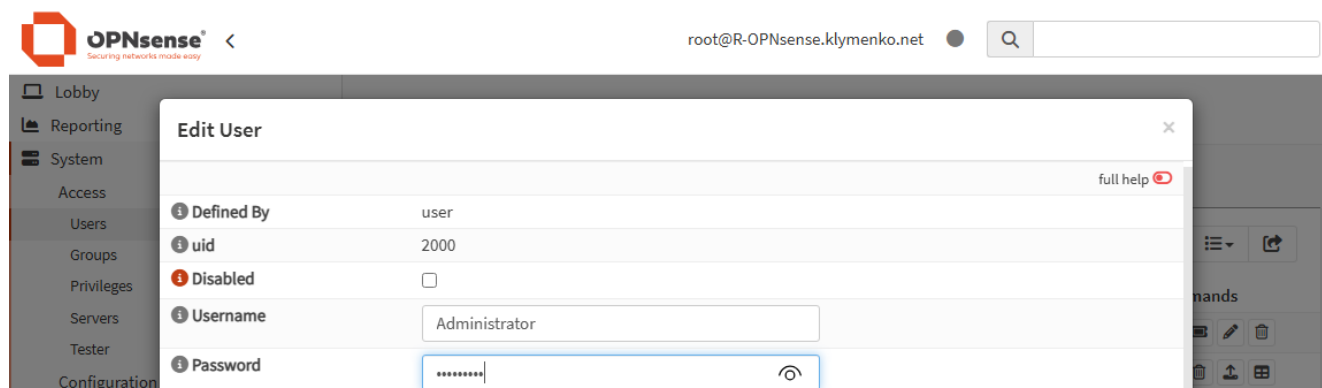


Рисунок 3.35 – Задання логіну та паролю нового користувача

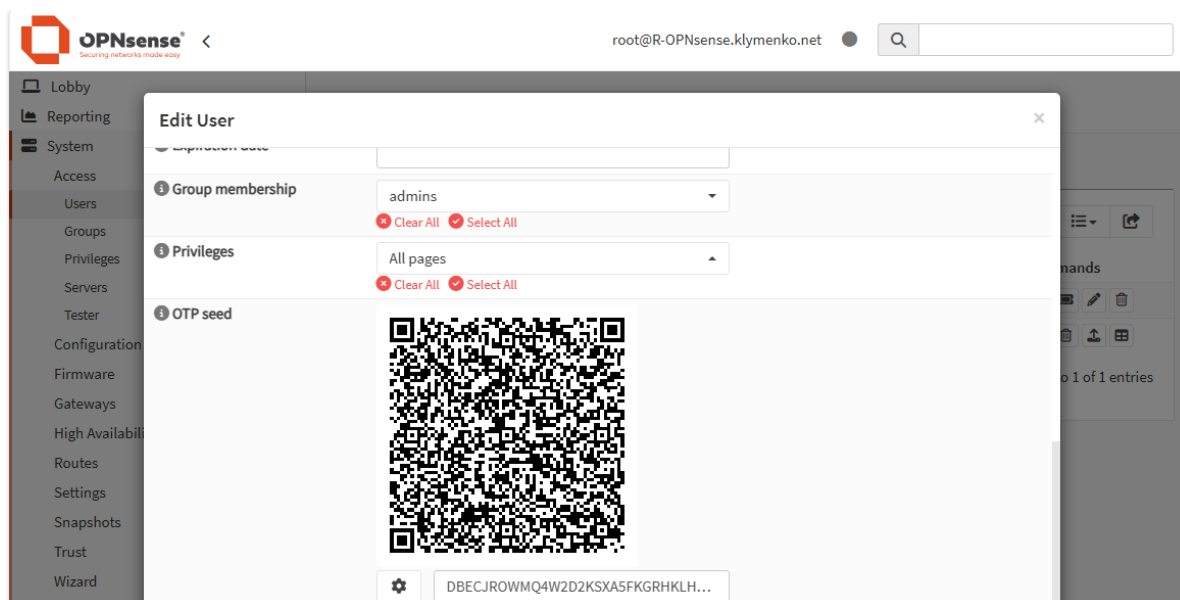


Рисунок 3.36 – Генерація QR коду

На цьому етапі відкриваємо мобільний додаток Google Authenticator (або інший сумісний автентифікатор) на смартфоні, натискаємо кнопку додавання облікового запису (плюсик), обираємо варіант "Сканувати QR-код" і наводимо камеру на екран монітора. Додаток автоматично зчитає код і додасть новий запис, який буде відображати шестизначні одноразові паролі, що оновлюються кожні 30 секунд, рис.3.37-3.38.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

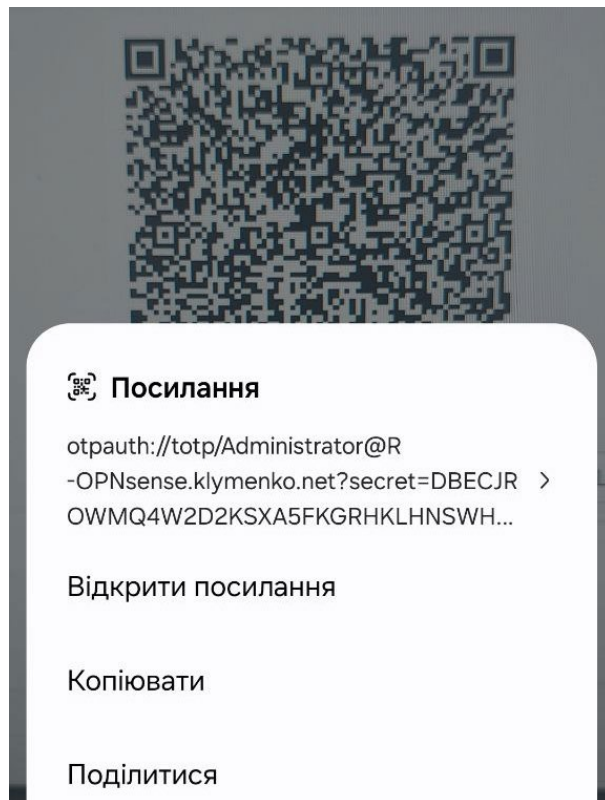


Рисунок 3.37 – Сканування QR коду з персонального телефону

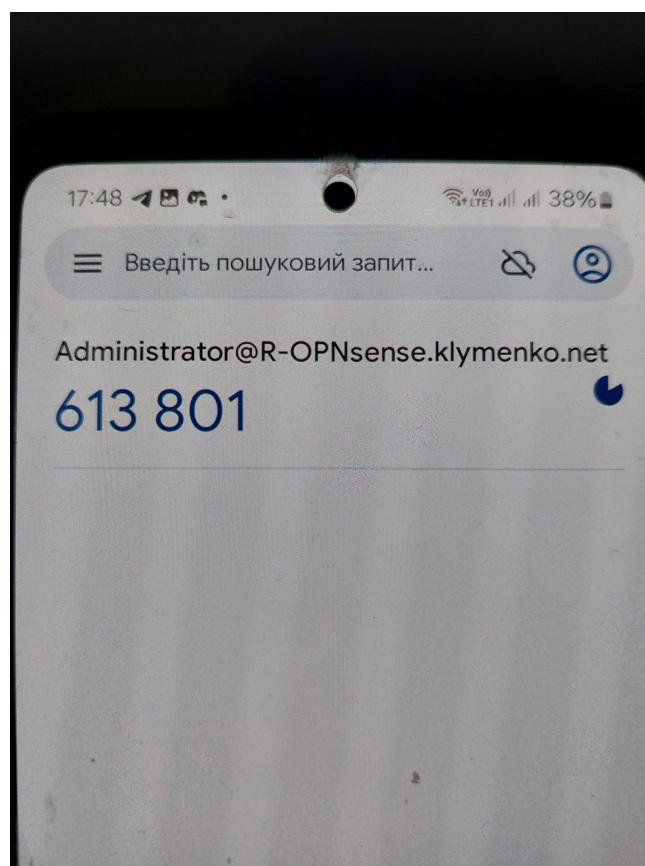


Рисунок 3.38 – Доданий запис в Google Authenticator

		Клименко Д.О.			ККІКБ.КР.Б - 125 - 08 - ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

Останнім етапом налаштування в OPNsense стане використання механізму Snapshots, який дозволяє вручну зберігати бажаний стан конфігурації системи. Через розділ System – Snapshots можна створити знімок поточних налаштувань, що стане точкою відновлення у разі помилкових змін або збоїв, рис.3.39. Кожен snapshot зберігає копію конфігураційного файлу, яку за потреби можна легко відновити. Це зручно при внесенні критичних змін у систему або перед оновленням компонентів.

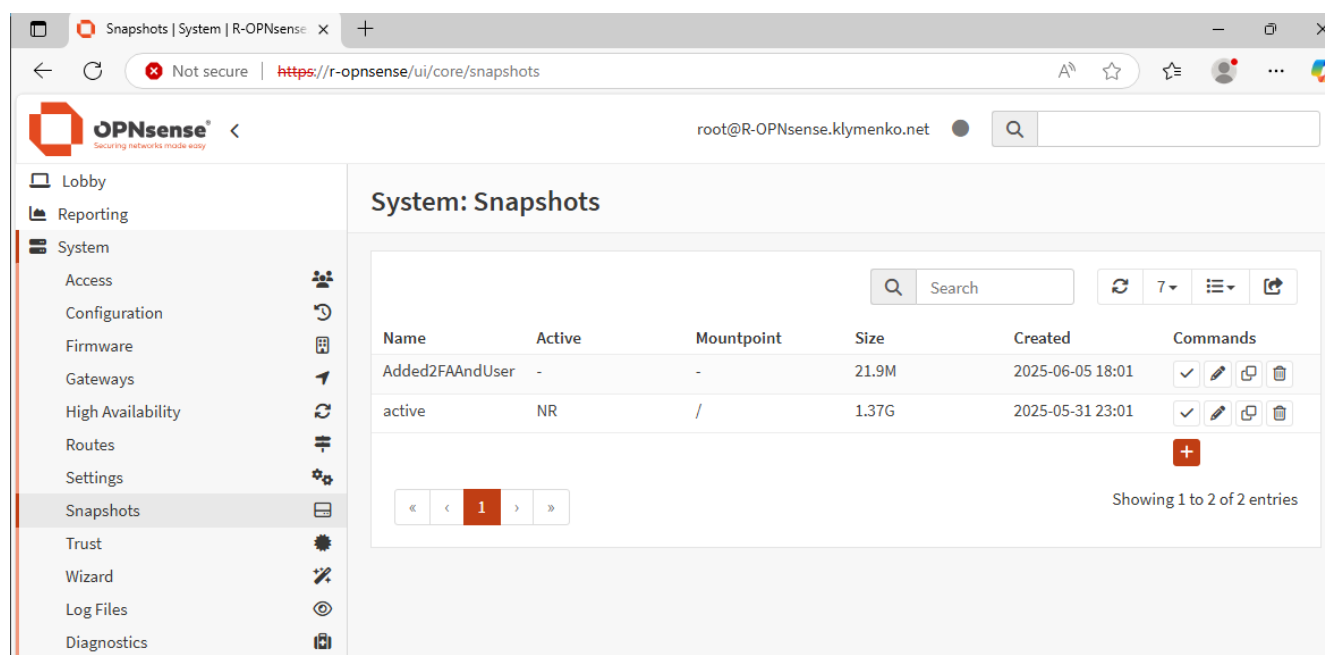


Рисунок 3.39 – Створення снєпшоту під назвою «Added2FAAndUser»

3.3 Тестування, моніторинг та діагностика роботи підсистеми захисту

Приступаємо до перевірки працездатності мережі та впроваджених рішень. Спершу з однієї з кінцевих станцій виконаємо вхід до операційної системи під обліковим записом користувача, створеним у службі Active Directory, рис.3.40. Успішна авторизація засвідчить правильну роботу механізмів доменної автентифікації, доступність контролера домену, а також коректну роботу DNS-сервера, який забезпечує розпізнавання імені домену. Це також підтвердить, що мережеві налаштування клієнтської станції, зокрема отримання IP-адреси через DHCP.

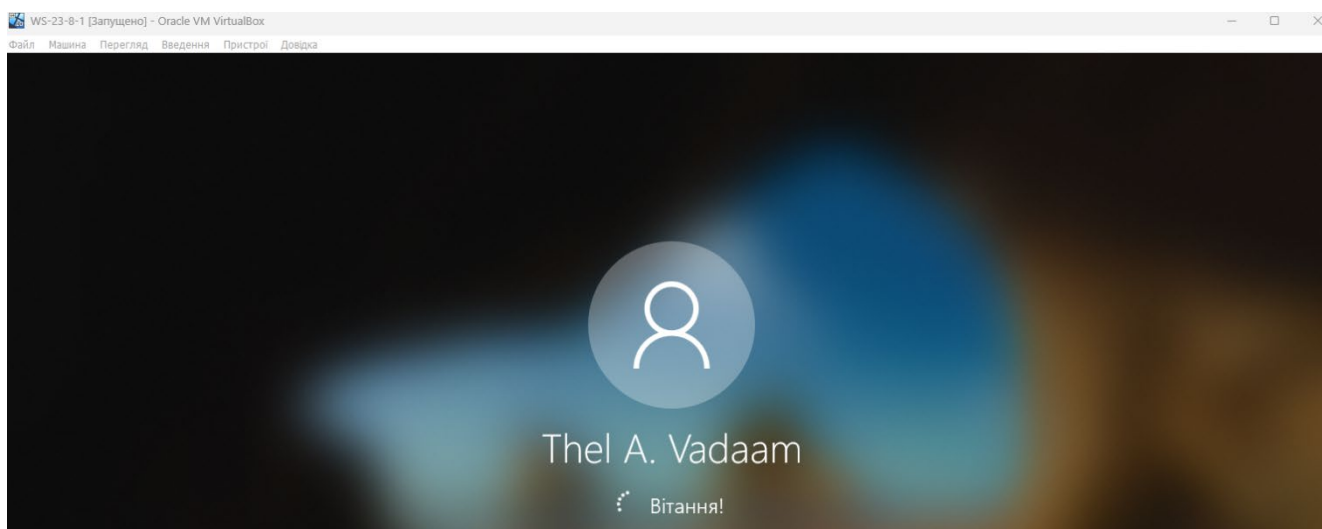


Рисунок 3.39 – Вхід в систему робочої станції

Далі на клієнтській станції виконаємо перевірку зв'язку з іншими пристроями мережі та ресурсами Інтернету за допомогою їх доменних імен. Це дозволить пересвідчитись у коректній роботі служби DNS. Зокрема, буде здійснено пінг до маршрутизатора та комутатора, а також до зовнішніх ресурсів, таких як google.com та ztu.edu.ua, що також підтвердить наявність доступу до Інтернету та правильну налаштовану роботу маршрутизації та NAT, рис.3.41.

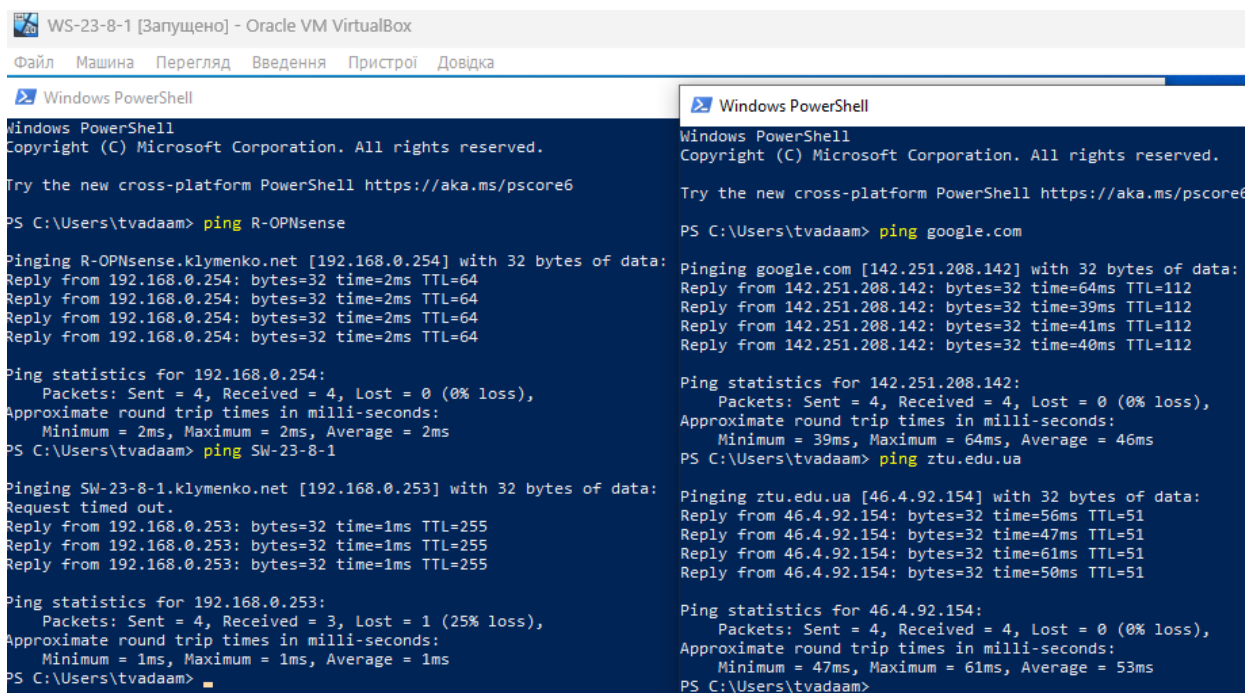


Рисунок 3.41 – Результат успішного пінгування

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

Переконавшись у працездатності кінцевих робочих станцій і наявності доступу до Інтернету, переходимо до перевірки OPNsense. Для входу в інтерфейс керування під обліковим записом адміністратора необхідно врахувати особливості використання двофакторної автентифікації. У полі Password слід ввести спочатку шестизначний код, згенерований мобільним додатком-автентифікатором і одразу після нього основний пароль користувача. Наприклад, якщо код – 123456, а пароль – MyPass, у поле вводиться 123456MyPass, рис.3.42. Таке поєднання перевіряється системою як єдиний рядок автентифікації.

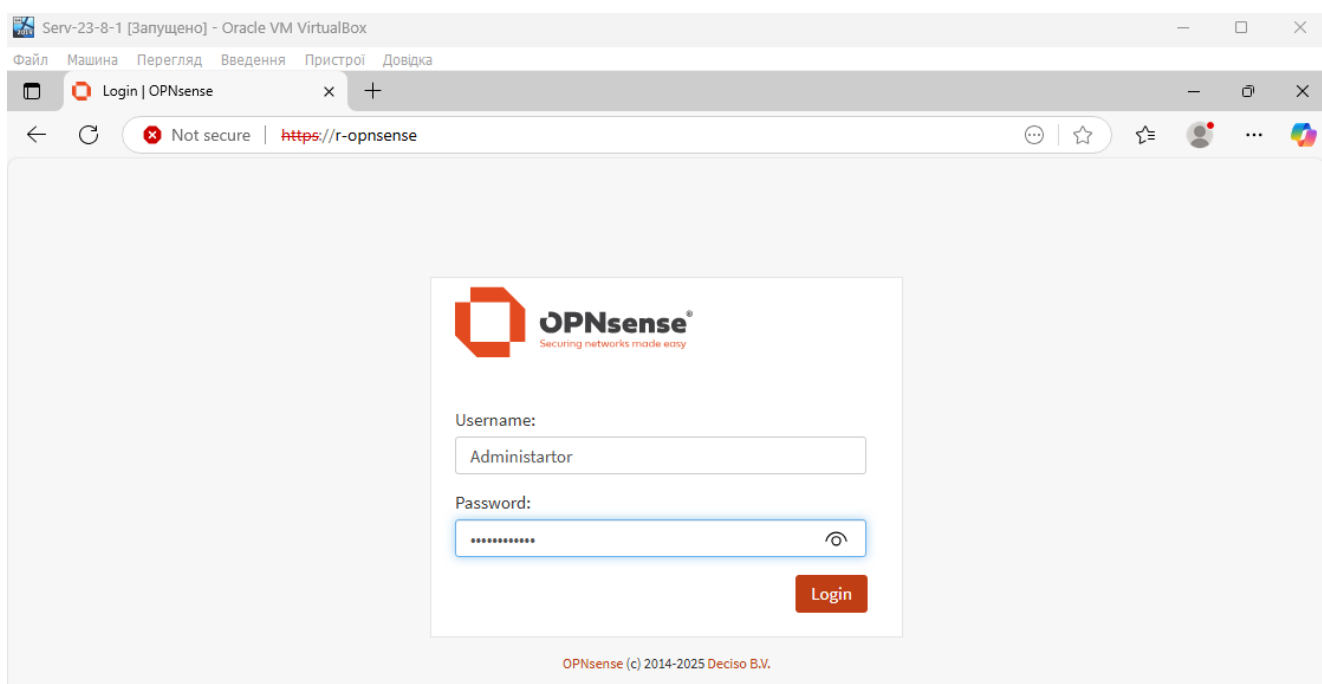


Рисунок 3.42 – Вхід в систему з використанням двофакторної автентифікації

Після входу в систему відкривається головне меню OPNsense, де відображається зведена інформація про стан системи. Зокрема, на головній панелі можна побачити дані про аптайм, завантаженість процесора, використання оперативної пам'яті, статус мережевих інтерфейсів, а також інформацію про наявні оновлення та стан служб. Це дозволяє швидко оцінити поточний стан роботи системи та перейти до подальшого адміністрування, рис.3.43.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

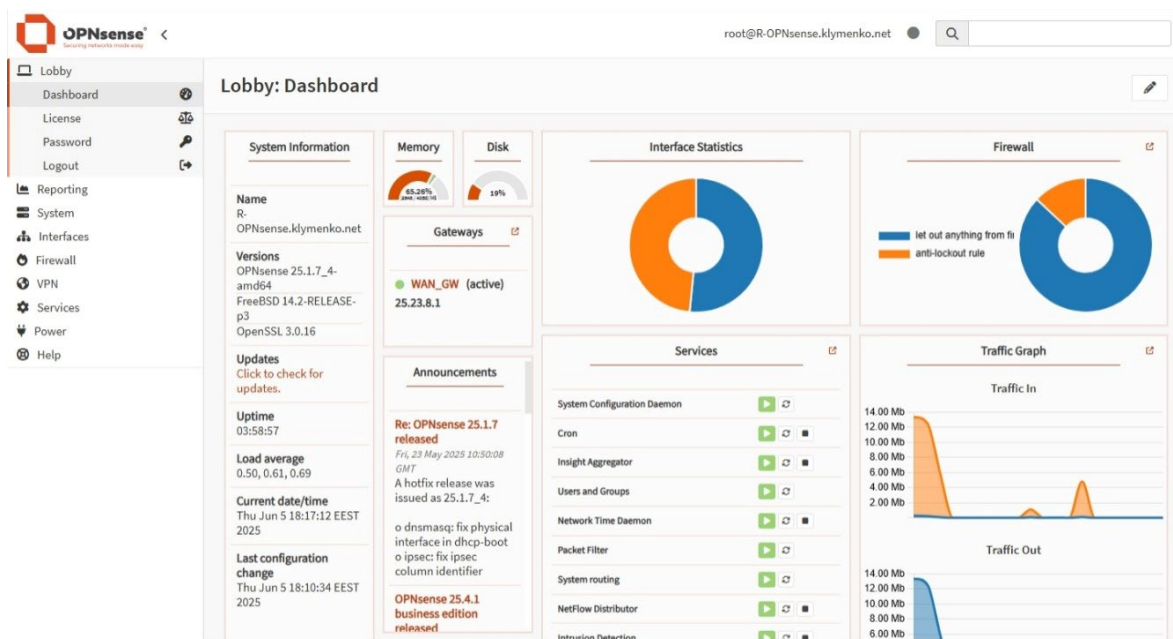


Рисунок 3.43 – Головне меню OPNsense

Першим механізмом захисту для перевірки буде IPS Suricata. Виконаємо це шляхом імітації внутрішньої мережевої атаки зі станції зловмисника, оскільки правила фایрвол для інтерфейсу WAN забороняють майже всі зовнішні підключення. Отже, для цього додамо і підключимо віртуальну машину з Kali Linux до одного з комутаторів локального сегмента мережі та за допомогою утиліти Nmap виконаємо сканування пристрою OPNsense. Виконаємо команду `nmap -A 192.168.0.254`, яка виконає розширене сканування хоста OPNsense з визначенням відкритих портів, операційної системи та іншої інформації рис.3.44.

```
(kali@kali)~$ nmap -A 192.168.0.254
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-04 16:07 EDT
Nmap scan report for OPNsense.klymenko.net (192.168.0.254)
Host is up (0.0033s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Unbound 1.23.0
| dns-nsid:
|   id.server: OPNsense.klymenko.net
|   bind.version: unbound 1.23.0
80/tcp    open  http         OPNsense
|_ http-server-header: OPNsense
|_ fingerprint-strings:
|_   DNSVersionBindReqTCP:
|_     HTTP/1.0 400 Bad Request
|_     Content-Type: text/html
|_     Content-Length: 162
|_     Connection: close
|_     Date: Wed, 04 Jun 2025 20:07:47 GMT
|_     Server: OPNsense
|_     <!DOCTYPE html>
|_     <html lang="en">
|_     <head>
|_       <meta charset="UTF-8" />
|_       <title>400 Bad Request</title>
|_     </head>
|_     <body>
|_       <h1>400 Bad Request</h1>
|_     </body>
|_     </html>
|_   FourOhFourRequest:
|_     HTTP/1.0 400 Bad Request
```

Рисунок 3.44 – Результат виконання команди `nmap -A 192.168.0.254`

Після виконання сканування командою nmap -A 192.168.0.254 на OPNsense у журналі Suricata з'явилося сповіщення ET SCAN Possible Nmap User-Agent Observed з дією Action: Allowed. Це свідчить про те, що система виявила ознаки використання Nmap для збору інформації про систему, однак відповідний трафік не було заблоковано і лише зафіксовано як подію безпеки, рис.3.45.

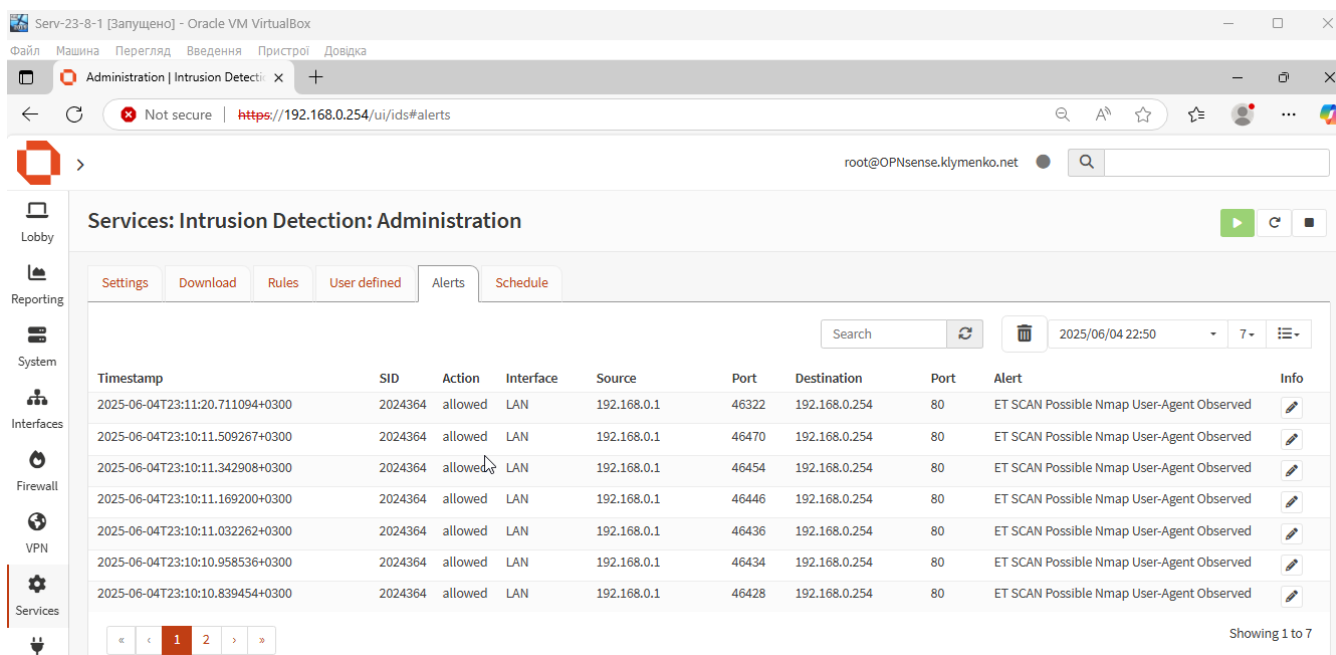


Рисунок 3.45 – Виконання команди nmap -A 192.168.0.254

У цьому випадку адміністратор може змінити дію відповідних правил на Drop, що забезпечить автоматичне блокування схожого трафіку в майбутньому. Крім цього, за потреби можна вручну заблокувати увесь трафік від джерела, з якого було зафіксовано активність, за допомогою відповідного правила у фаєрвол.

Тому в даному випадку ми виконаємо зміну дій для виявлених подій Suricata з простого виявлення (Alert) на відкидання (Drop). Перейдемо до вкладки Rules, та оберемо необхідні правила, для яких слід виставити дію блокування. Для прикладу змінимо дію для правил зі списку «emerging-scan.rules» на Drop – замість Alert, рис.3.46. Після цього слід перезапустити Suricata, щоб зміни набрали чинності. Дані зміни дозволять не лише виявляти, а й автоматично блокувати шкідливу активність у мережі.

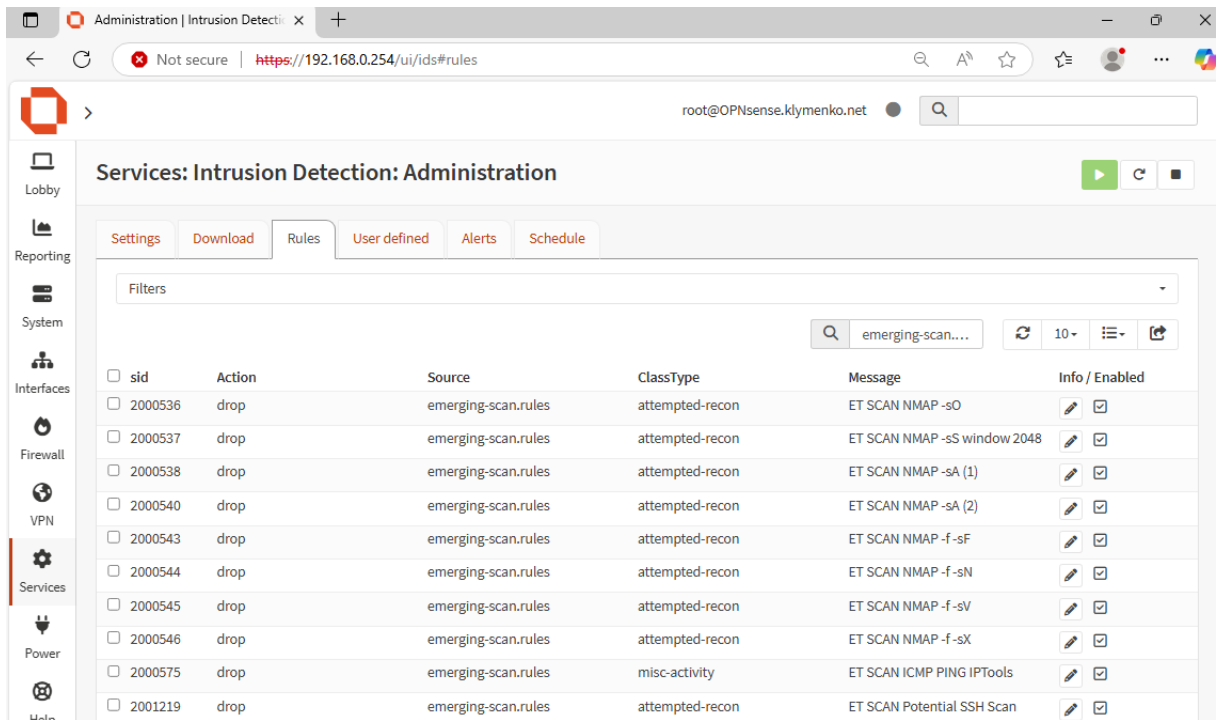


Рисунок 3.46 – Зміна дії правил з Alert на Drop

Після зміни дії правил на Drop повторимо атаку зі станції Kali. Цього разу Suricata знову виявила спробу сканування, однак у полі дії вже відображається Blocked, що свідчить про успішне застосування змін. Система не лише зафіксувала підозрілу активність, а й автоматично заблокувала відповідний трафік, рис.3.47. Це підтверджує ефективність налаштованої системи виявлення.

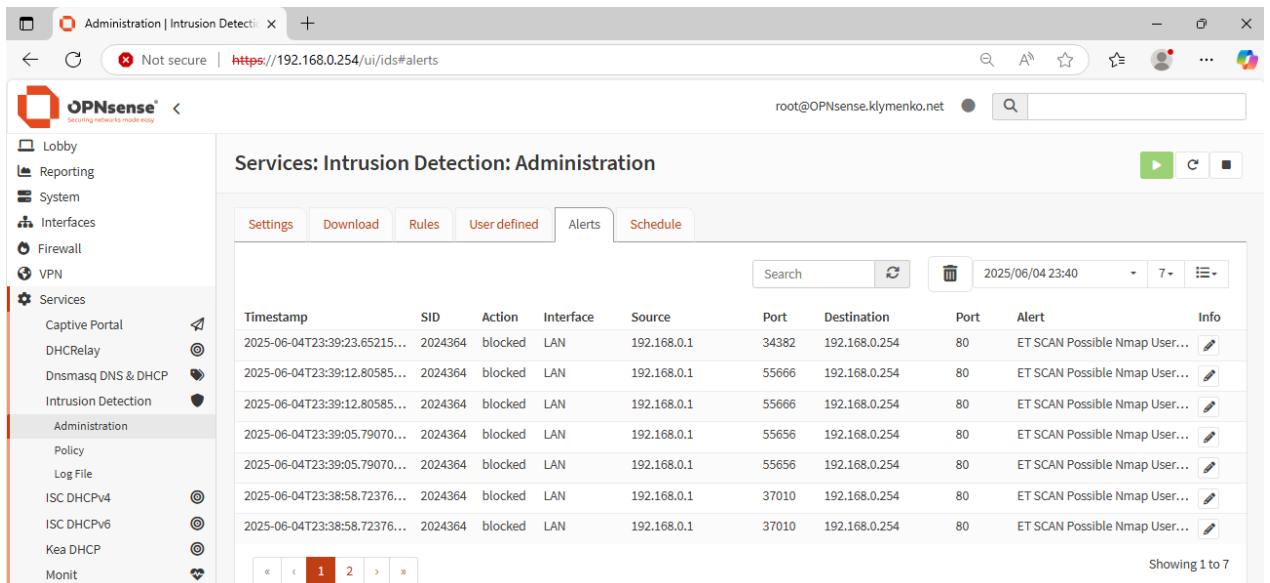


Рисунок 3.47 – Отримані сповіщення

Аналогічні сповіщення можна переглянути на Syslog-сервері, що був раніше налаштований на Windows Server 2019, рис.3.48.

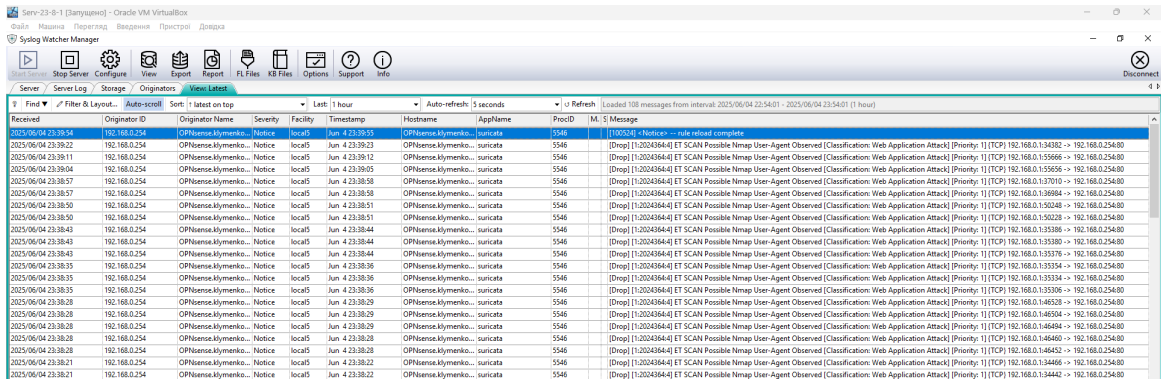


Рисунок 3.48 – Отримані сповіщення на Syslog-сервері

Для перевірки роботи функції безпечного пошуку в Unbound DNS було введено пошуковий запит "NSFW". Однак в результаті жодних небажаних посилань та рисунків не відобразилось, а отримані результати мали допустимий вміст. Це свідчить коректну роботу примусової функції безпечного пошуку (SafeSearch), яка була попередньо налаштована в Unbound DNS. Саме ця функція автоматично перенаправляє запити до пошукових систем із активованим режимом безпечного перегляду, забезпечуючи додатковий рівень контент-фільтрації, рис.3.49.

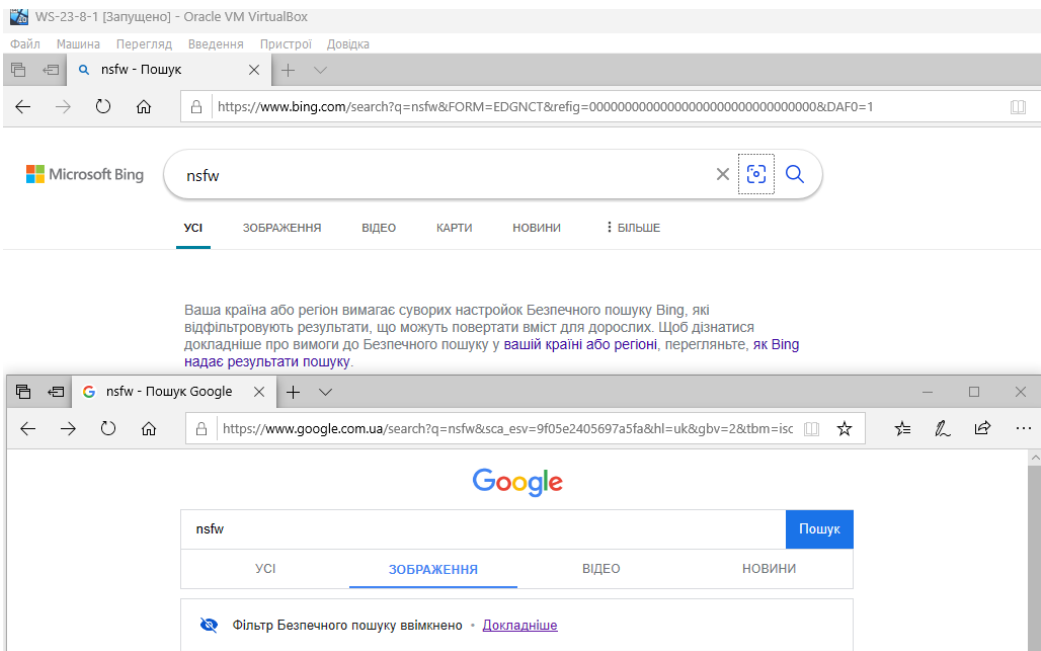


Рисунок 3.49 – Робота примусового безпечного пошуку

Для перевірки роботи Unbound DNS зі станції було виконано тестове відкриття вебсайтів, що містять піратський контент та входять до категорій, зазначених у списках DNS-блокування. Як результат, доступ до піратських сайтів було успішно заблоковано. Водночас освітні сайти відкривались без обмежень, що свідчить про коректну роботу фільтрації DNS-запитів та належну фільтрацію дозволених і заборонених ресурсів, рис.3.50.

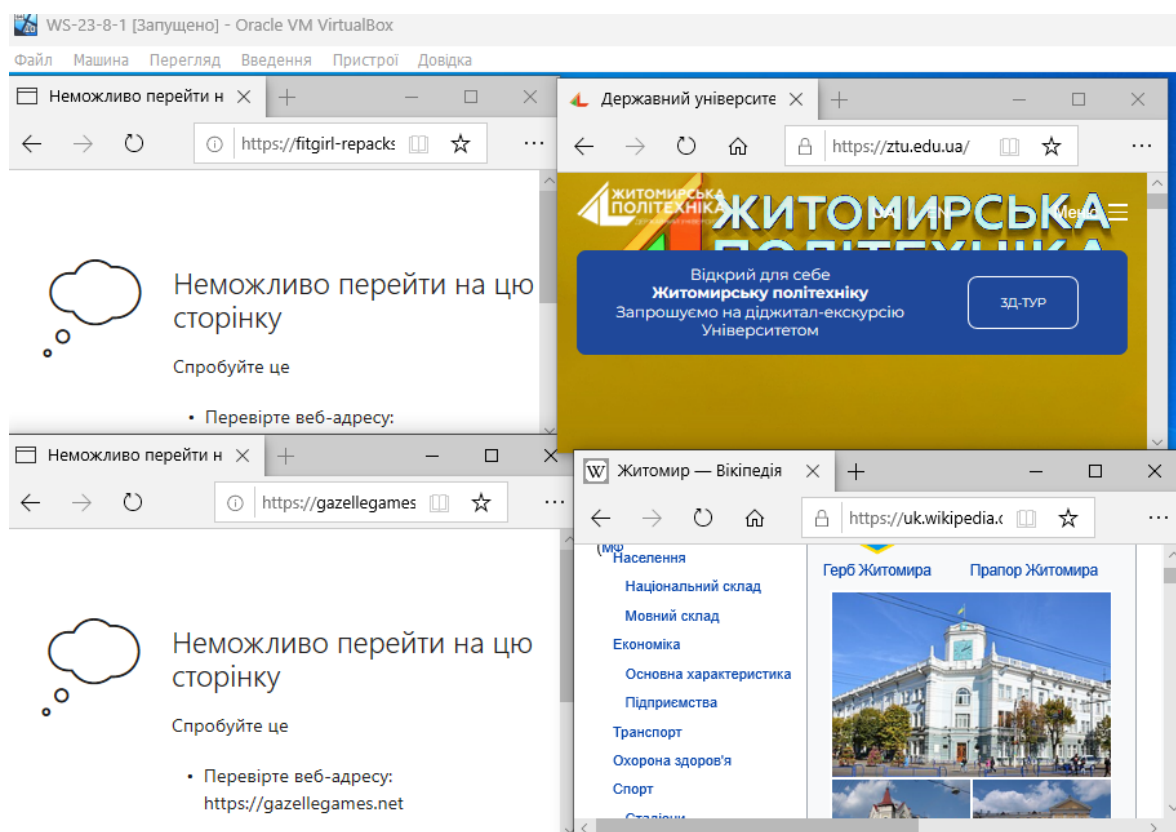


Рисунок 3.50 – Спроба відкриття піратських (зліва) та освітніх ресурсів (справа)

На сторінці Unbound DNS доступна статистика його роботи, яка включає інформацію про кількість виконаних DNS-запитів, кількість заблокованих доменів, джерела блокування, а також останні звернення. Це дозволяє контролювати ефективність фільтрації, виявляти потенційно небажану активність у мережі та оперативно реагувати на загрози та вживати відповідні заходи щодо блокування доменів та IP-адрес. На рис.3.51 наведена графік запитів та заблокованих DNS-запитів. Повна версія сторінки представлена на додатку Б.3.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		73

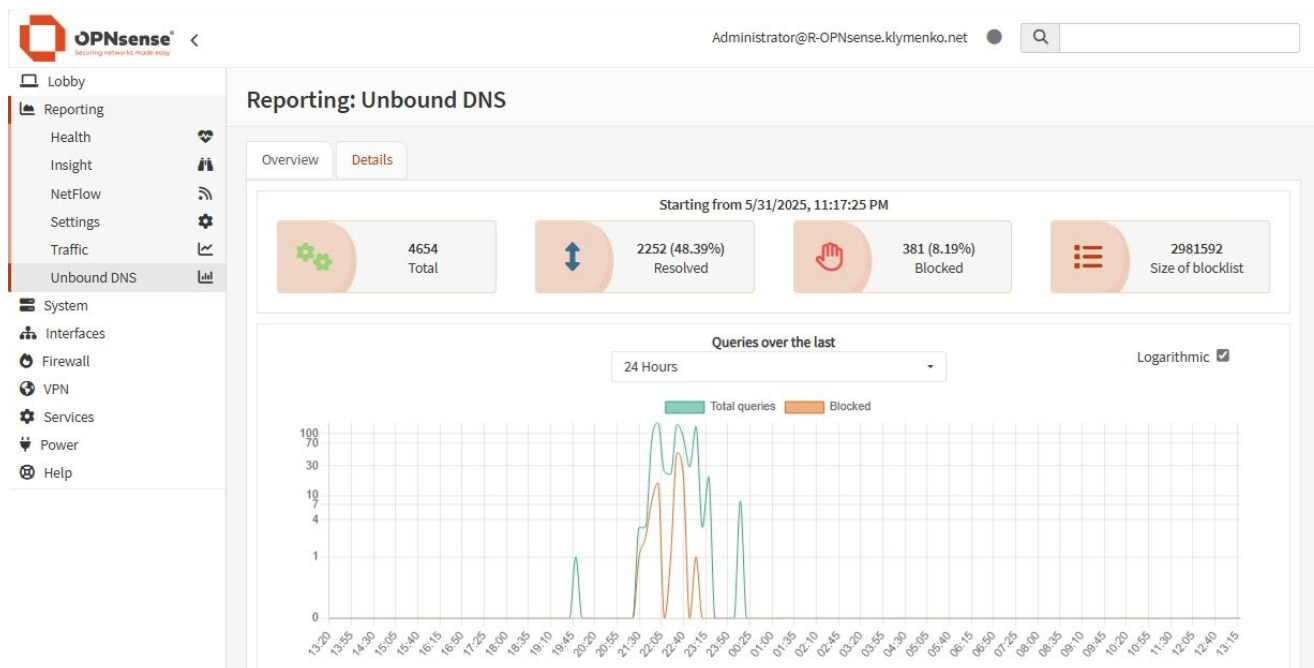


Рисунок 3.51 – Графік роботи DNS Unbound

Наостанок виконаємо перегляд графіків та статистики роботи OPNsense у розділі Reporting. Тут доступні візуалізації трафіку за інтерфейсами, завантаження процесора, використання оперативної пам'яті, активність фаєрволу, статистика IDS/IPS та інші ключові показники. Це дозволяє отримати наочне уявлення про поточний стан системи, виявляти пікові навантаження або підозрілу активність у мережі, рис.3.52-3.54 та додатки Б.4-Б.5.

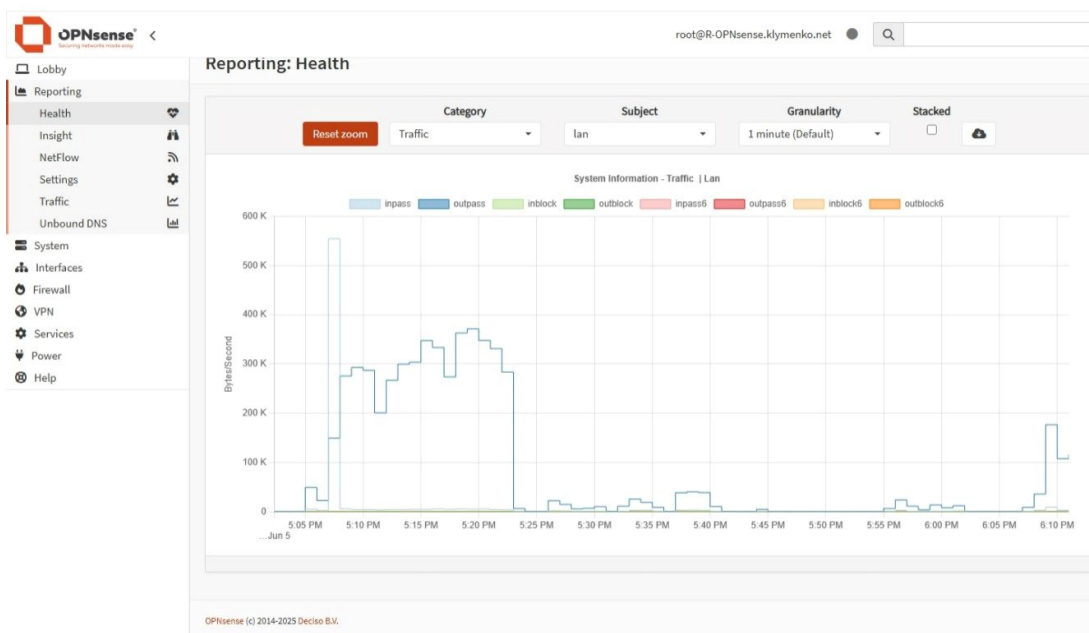


Рисунок 3.52 – Статистика проходження трафіку

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		74

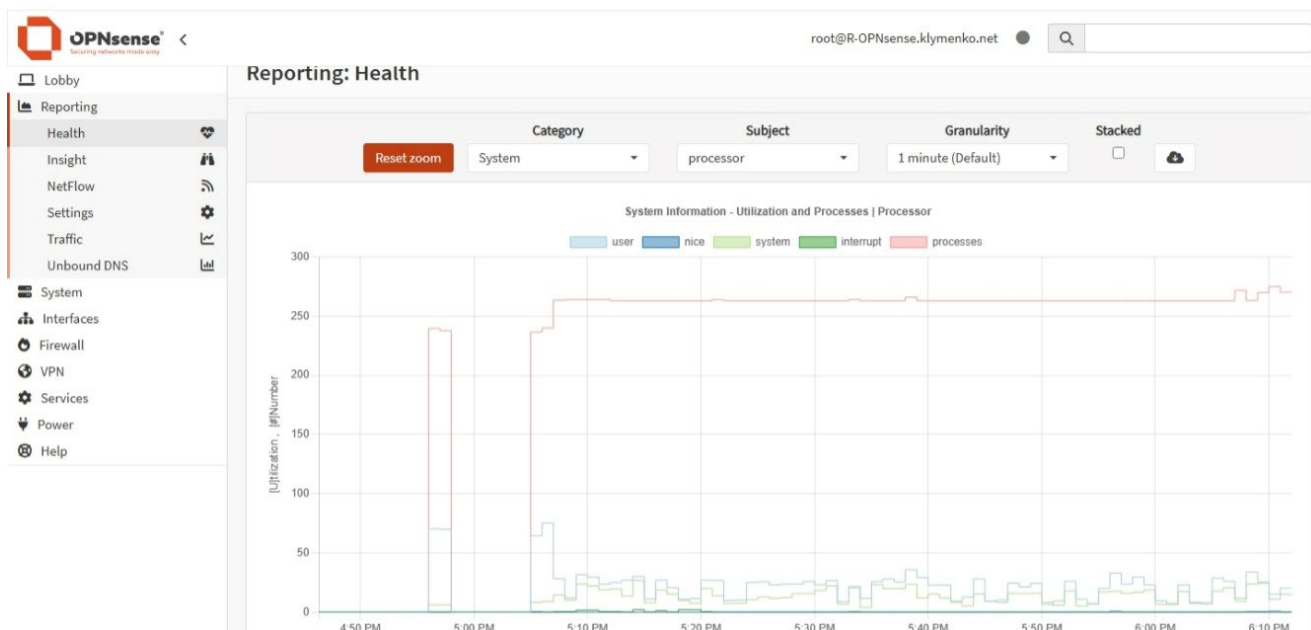


Рисунок 3.53 – Статистика роботи процесора

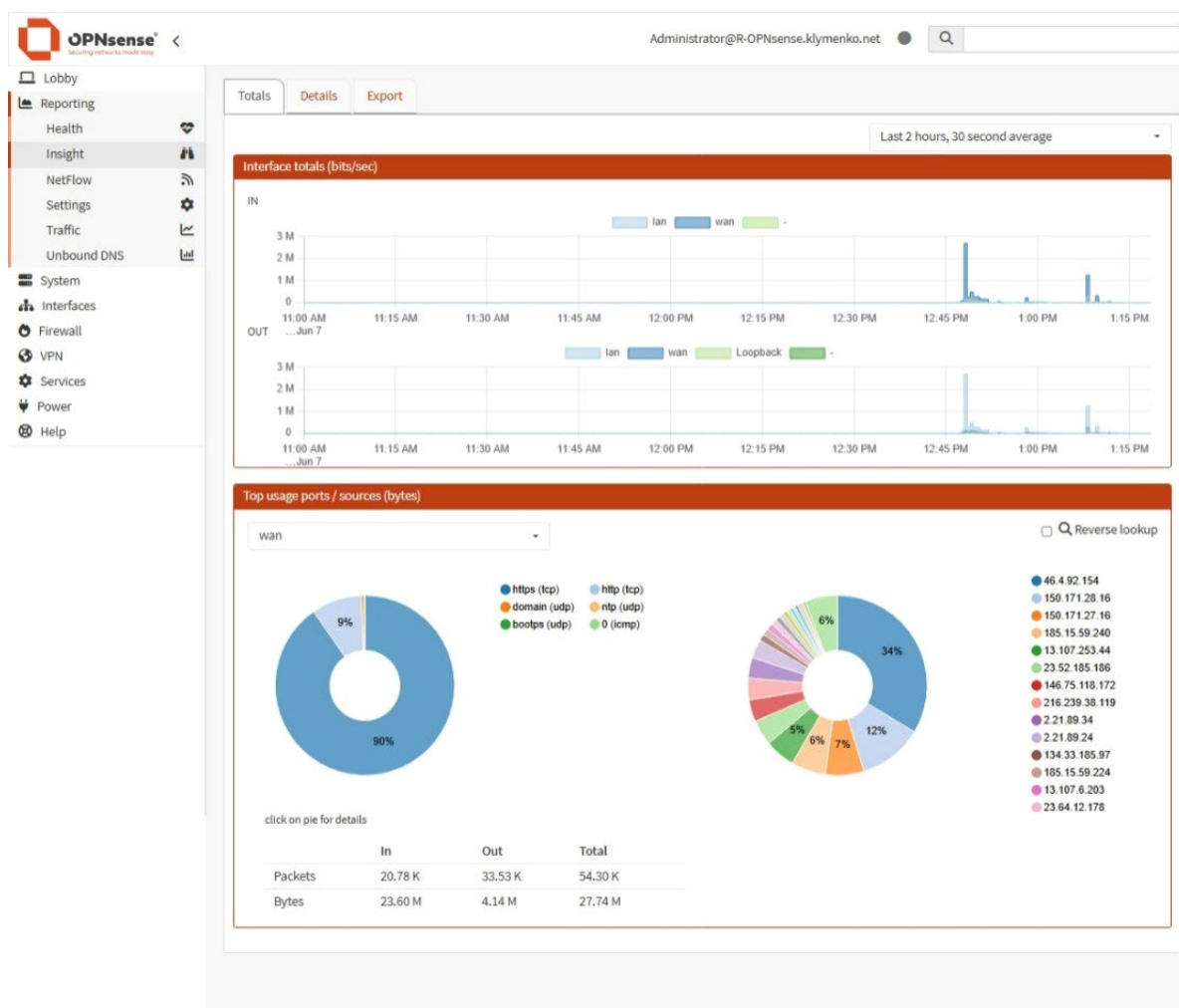


Рисунок 3.54 – Статистика проходження трафіку та протоколів через інтерфейси

Висновки до третього розділу

В ході роботи над розділом було створено проєкт мережі в віртуальному середовищі в GNS3 з використанням VirtualBox, у якому розгорнуто ключові компоненти інфраструктури. Виконано конфігурацію комутаторів, налаштування IP-адресації, розгортання Active Directory, служб DHCP і DNS, централізоване логування через Syslog Watcher, а також приєднання клієнтських станцій до домену.

Було виконано встановлення та базове налаштування системи OPNsense у віртуальному середовищі. Здійснено конфігурацію мережевих інтерфейсів, налаштовано доступ до веб-інтерфейсу та проведено первинне налаштування системи. Реалізовано початкові правила фаєрвола для інтерфейсів WAN і LAN, налаштовано систему виявлення вторгнень Suricata із пересиланням повідомлень на Syslog-сервер, активовано Unbound DNS з функцією блокування небажаних доменів, а також увімкнено двофакторну автентифікацію для підвищення рівня захисту доступу до системи. Для забезпечення гнучкого керування конфігурацією створено знімки стану системи (snapshots).

Наостанок було проведено комплексне тестування працездатності підсистеми захисту мережі. Успішна авторизація користувача в домені підтвердила коректну роботу служби Active Directory, DNS та DHCP. За допомогою перевірки зв'язку з внутрішніми та зовнішніми ресурсами було засвідчено правильне функціонування маршрутизації і NAT. У ході перевірки механізму виявлення загроз Suricata було зафіксовано мережеву атаку, після чого відповідні правила було модифіковано для автоматичного блокування шкідливого трафіку. Надсилання сповіщень на Syslog-сервер підтвердило працездатність журналювання подій безпеки. DNS-фільтрація в Unbound DNS ефективно обмежила доступ до небажаних ресурсів відповідно до заданих політик. Статистичні дані та графіки в розділі моніторингу OPNsense дозволили оцінити навантаження системи та ефективність її роботи, що засвідчило стабільне функціонування підсистеми захисту та моніторингу стану.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

ВИСНОВКИ

У межах кваліфікаційної роботи було розроблено проєкт підсистеми захисту IT-інфраструктури організації на базі рішень OPNsense.

У першому розділі було розглянуто теоретичні аспекти захисту IT-інфраструктури з використанням OPNsense. Проведено аналіз типових мережевих загроз, принципів роботи та класифікації міжмережевих екранів, здійснено порівняння популярних безкоштовних фаєрволів і обґрунтовано вибір OPNsense як найбільш оптимального рішення. Також детально досліджено функціональні можливості даної платформи, зокрема окрема увага приділена Suricata, як ефективному механізму виявлення та запобігання вторгненням.

У другому розділі розроблено логічну топологію IT-інфраструктури за трирівневою моделлю. Обрано пристрої мережі із відповідною схемою IP-адресації: статичні адреси для мережевих пристроїв і сервера, динамічні – для користувачів, а всі елементи інтегровані в єдиний домен для централізованого управління. Вибрано засоби захисту на базі OPNsense, зокрема фаєрвол, IDS Suricata із пересиланням подій на Syslog, DNS-сервер Unbound із блокуванням доменів і двофакторну аутентифікацію. Обґрунтовано вибір маршрутизатора з OPNsense, комутаторів і сервера на базі операційної системи Windows Server 2019.

У третьому розділі створено проєкт мережі у віртуальному середовищі GNS3, розгорнуто компоненти інфраструктури, виконано конфігурацію пристроїв, IP-адресації, Active Directory, служб DHCP і DNS, логування через Syslog Watcher та приєднання клієнтських станцій до домену. Встановлено та налаштовано OPNsense, початкові правила фаєрвола для WAN і LAN, систему виявлення вторгнень Suricata з пересиланням подій на Syslog, Unbound DNS із блокуванням небажаних доменів і двофакторну автентифікацію. Проведено комплексне тестування підсистеми захисту мережі, підтверджено коректну роботу Active Directory, DNS, DHCP, маршрутизації та NAT. Було виявлено мережеву атаку, яка була заблокована модифікованими правилами Suricata, перевірено працездатність журналювання подій безпеки, ефективність DNS-фільтрації і стабільне функціонування інструментів моніторингу OPNsense.

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Guidelines on Firewalls and Firewall Policy [Електронний ресурс]. Режим доступу до ресурсу: <https://csrc.nist.gov/pubs/sp/800/41/r1/final>
2. The 8 Types of Firewalls [Електронний ресурс]. Режим доступу до ресурсу: <https://phoenixnap.com/blog/types-of-firewalls>
3. How does a firewall work? [Електронний ресурс]. Режим доступу до ресурсу: <https://nordlayer.com/learn/firewall/how-firewall-work/>
4. Firewall Definition: What Is A Network Firewall? [Електронний ресурс]. Режим доступу до ресурсу: <https://www.fortinet.com/resources/cyberglossary/firewall>
5. Hardware Firewall vs Software Firewall? [Електронний ресурс]. Режим доступу до ресурсу: <https://navigators.com/firewall.html>
6. The 5 different types of firewalls explained [Електронний ресурс]. Режим доступу до ресурсу: <https://www.techtarget.com/searchsecurity/feature/The-five-different-types-of-firewalls>
7. Top 15 Best Open Source Firewalls for Linux / Windows [Електронний ресурс]. Режим доступу до ресурсу: <https://cloudinfrastructureservices.co.uk/top-15-best-open-source-firewalls-for-linux-windows/>
8. pfSense [Електронний ресурс]. Режим доступу до ресурсу: <https://www.pfsense.org/>
9. OPNsense [Електронний ресурс]. Режим доступу до ресурсу: <https://opnsense.org/>
10. IPFire [Електронний ресурс]. Режим доступу до ресурсу: <https://www.ipfire.org/>
11. VyOS [Електронний ресурс]. Режим доступу до ресурсу: <https://vyos.io/>
12. Free Firewall Home Edition [Електронний ресурс]. Режим доступу до ресурсу: <https://www.sophos.com/en-us/free-tools/sophos-xg-firewall-home-edition>
13. Getting Started with OPNsense [Електронний ресурс]. Режим доступу до ресурсу: <https://www.zenarmor.com/docs/network-security-tutorials/what-is-opnsense>
14. What is IDPS? [Електронний ресурс]. Режим доступу до ресурсу: <https://www.twingate.com/blog/glossary/idps>

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

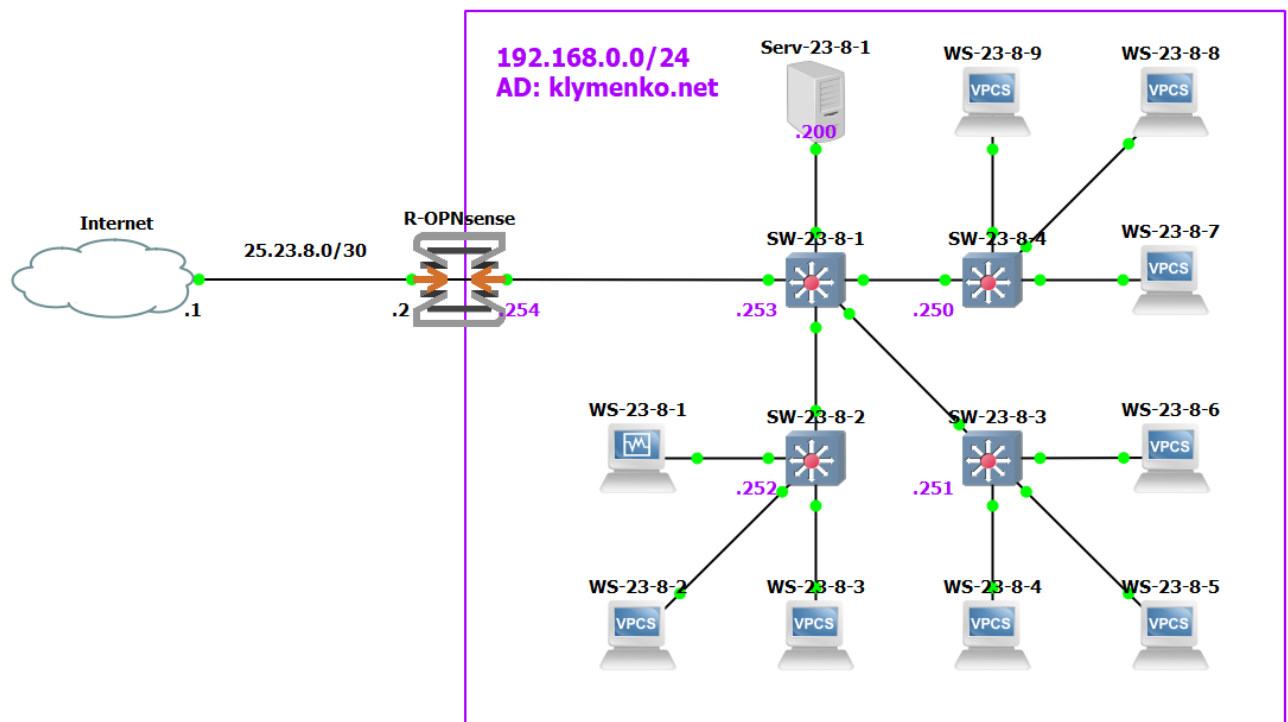
15. What is Intrusion Detection System | What is Intrusion Prevention System | IDS vs IPS [Електронний ресурс]. Режим доступу до ресурсу: <https://techofide.com/blogs/what-is-intrusion-detection-system-what-is-intrusion-prevention-system-ids-vs-ips/>
16. What is an intrusion detection and prevention system (IDPS)? [Електронний ресурс]. Режим доступу до ресурсу: <https://www.redhat.com/en/topics/security/what-is-an-IDPS>
17. Intrusion Prevention System [Електронний ресурс]. Режим доступу до ресурсу: <https://docs.opnsense.org/manual/ips.html>
18. Suricata [Електронний ресурс]. Режим доступу до ресурсу: <https://suricata.io/>
19. How does Suricata work? [Електронний ресурс]. Режим доступу до ресурсу: <https://www.stamus-networks.com/blog/how-does-suricata-work>
20. Suricata Rules [Електронний ресурс]. Режим доступу до ресурсу: <https://docs.suricata.io/en/latest/rules/index.html>
21. Cisco Three Layer / Three-tier Hierarchical Network Model [Електронний ресурс]. Режим доступу до ресурсу: <https://www.omnisecu.com/cisco-certified-network-associate-ccna/three-tier-hierarchical-network-model.php>
22. Unbound DNS [Електронний ресурс]. Режим доступу до ресурсу: <https://docs.opnsense.org/manual/unbound.html>
23. Two-factor authentication [Електронний ресурс]. Режим доступу до ресурсу: https://docs.opnsense.org/manual/two_factor.html
24. FW2B – 2 Port Intel® J3060 [Електронний ресурс]. Режим доступу до ресурсу: <https://eu.protectli.com/product/fw2b/>
25. Cisco Catalyst 2960-X and 2960-XR Series Switches Data Sheet [Електронний ресурс]. Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/datasheet_c78-728232.html
26. Syslog Watcher [Електронний ресурс]. Режим доступу до ресурсу: <https://ezfive.com/syslog-watcher/>

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		79

ДОДАТКИ

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		80

Додаток А – Топологія проєкту мережі в GNS3



		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток Б.1 – Згенерований набір правил для інтерфейсу WAN

OPNsense

Securing networks made easy

Lobby

Reporting

System

Interfaces

Firewall

Aliases

Automation

Categories

Groups

NAT

Rules

Floating

LAN

WAN

Shaper

Settings

Log Files

Diagnostics

VPN

Services

Power

Help

root@R-OPNsense.klymenko.net

Firewall: Rules: WAN

Select category

Inspect

No WAN rules are currently defined. All incoming connections on this interface will be blocked until you add a pass rule. Exceptions for automatically generated rules may apply.

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	
								Automatically generated rules	17
	IPv4+6	*	*	*	*	*	*	Default deny / state violation rule	
	IPv6	IPv6-ICMP	*	*	*	*	*	IPv6 RFC4890 requirements (ICMP)	
	IPv6	IPv6-ICMP (self)	*	fe80::/10, ff02::/16	*	*	*	IPv6 RFC4890 requirements (ICMP)	
	IPv6	IPv6-ICMP fe80::/10	*	fe80::/10, ff02::/16	*	*	*	IPv6 RFC4890 requirements (ICMP)	
	IPv6	IPv6-ICMP ff02::/16	*	fe80::/10	*	*	*	IPv6 RFC4890 requirements (ICMP)	
	IPv6	IPv6-ICMP ::	*	ff02::/16	*	*	*	IPv6 RFC4890 requirements (ICMP)	
	IPv4+6	TCP/UDP	0	*	*	*	*	block all targeting port 0	

OPNsense (c) 2014-2025 Deciso B.V.

	TCP/UDP							0	
	IPv4+6	TCP	<sshlockout>	(self)	22 (SSH)	*	*	sshlockout	
	IPv4+6	TCP	<sshlockout>	(self)	443 (HTTPS)	*	*	sshlockout	
	IPv4+6	*	<virusprot>	*	*	*	*	virusprot overload table	
	IPv4	*	<bogons>	*	*	*	*	Block bogon IPv4 networks from WAN	
	IPv6	*	<bogonsv6>	*	*	*	*	Block bogon IPv6 networks from WAN	
	IPv4	*	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 127.0.0.0/8, 100.64.0.0/10, 169.254.0.0/16	*	*	*	*	Block private networks from WAN	
	IPv6	*	fd00::/8, fe80::/10, ::/128	*	*	*	*	Block private networks from WAN	
	IPv4+6	*	*	*	*	*	*	let out anything from firewall host itself	
	IPv4+6	(em0)	*	! WAN net	*	WAN_GW	*	let out anything from firewall host itself (force gw)	

pass

pass (disabled)

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

block

block (disabled)

reject

reject (disabled)

log

log (disabled)

in

out

first match

last match

WAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

		Клименко Д.О.		
		Головня О.С.		
Змн.	Арк.	№ докум.	Підпис	Дата

ККІКБ.КР.Б - 125 - 08 - ПЗ

Арк.
82

Додаток Б.2 – Згенерований набір правил для інтерфейсу LAN

Lobby

Reporting

System

Interfaces

Firewall

Aliases

Automation

Categories

Groups

NAT

Rules

Floating

LAN

WAN

Shaper

Settings

Log Files

Diagnostics

VPN

Services

Power

Help

root@R-OPNsense.klymenko.net

Firewall: Rules: LAN

Select category

Inspect

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
Automatically generated rules								
	IPv4+6	*	*	*	*	*	*	Default deny / state violation rule
	IPv6 IPv6-ICMP	*	*	*	*	*	*	IPv6 RFC4890 requirements (ICMP)
	IPv6 IPv6-ICMP	(self)	*	fe80::/10, ff02::/16	*	*	*	IPv6 RFC4890 requirements (ICMP)
	IPv6 IPv6-ICMP	fe80::/10	*	fe80::/10, ff02::/16	*	*	*	IPv6 RFC4890 requirements (ICMP)
	IPv6 IPv6-ICMP	ff02::/16	*	fe80::/10	*	*	*	IPv6 RFC4890 requirements (ICMP)
	IPv6 IPv6-ICMP	::	*	ff02::/16	*	*	*	IPv6 RFC4890 requirements (ICMP)
	IPv4+6 TCP/UDP	*	0	*	*	*	*	block all targeting port 0
	IPv4+6 TCP/UDP	*	*	*	0	*	*	block all targeting port 0
	IPv4+6 TCP	<sshlockout>	*	(self)	22 (SSH)	*	*	sshlockout
	IPv4+6 TCP	<sshlockout>	*	(self)	443 (HTTPS)	*	*	sshlockout
	IPv4+6	<virusprot>	*	*	*	*	*	virusprot overload table
	IPv4+6	*	*	*	*	*	*	let out anything from firewall host itself
	IPv4+6 TCP	*	*	(self)	80 (HTTP)	*	*	anti-lockout rule
	IPv4+6 TCP	*	*	(self)	443 (HTTPS)	*	*	anti-lockout rule

OPNsense (c) 2014-2025 Deciso B.V.

IPv4	LAN net	*	*	*	*	*	Default allow LAN to any rule
IPv6	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule

pass

pass (disabled)

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

block

block (disabled)

reject

reject (disabled)

log

log (disabled)

in

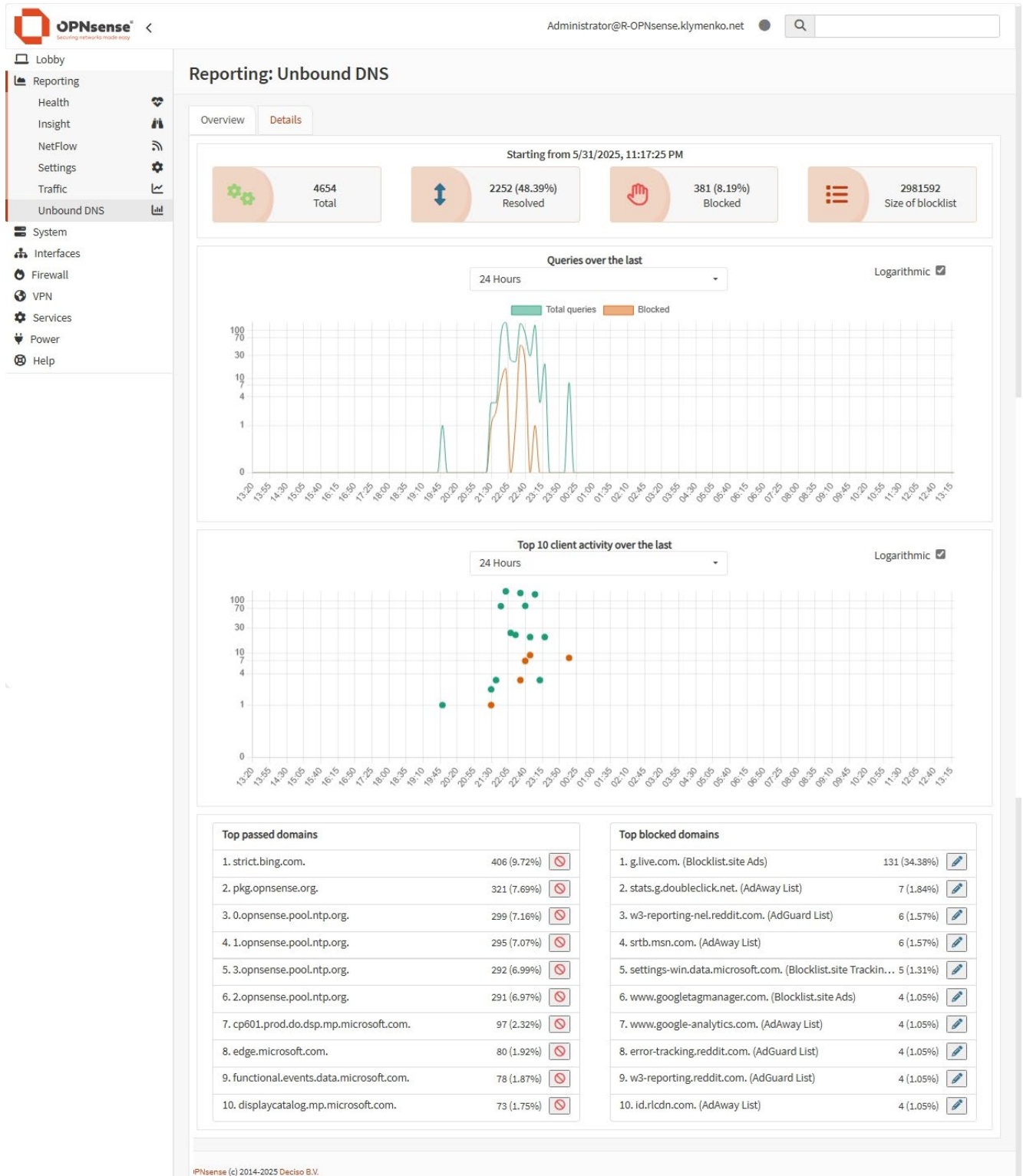
out

first match

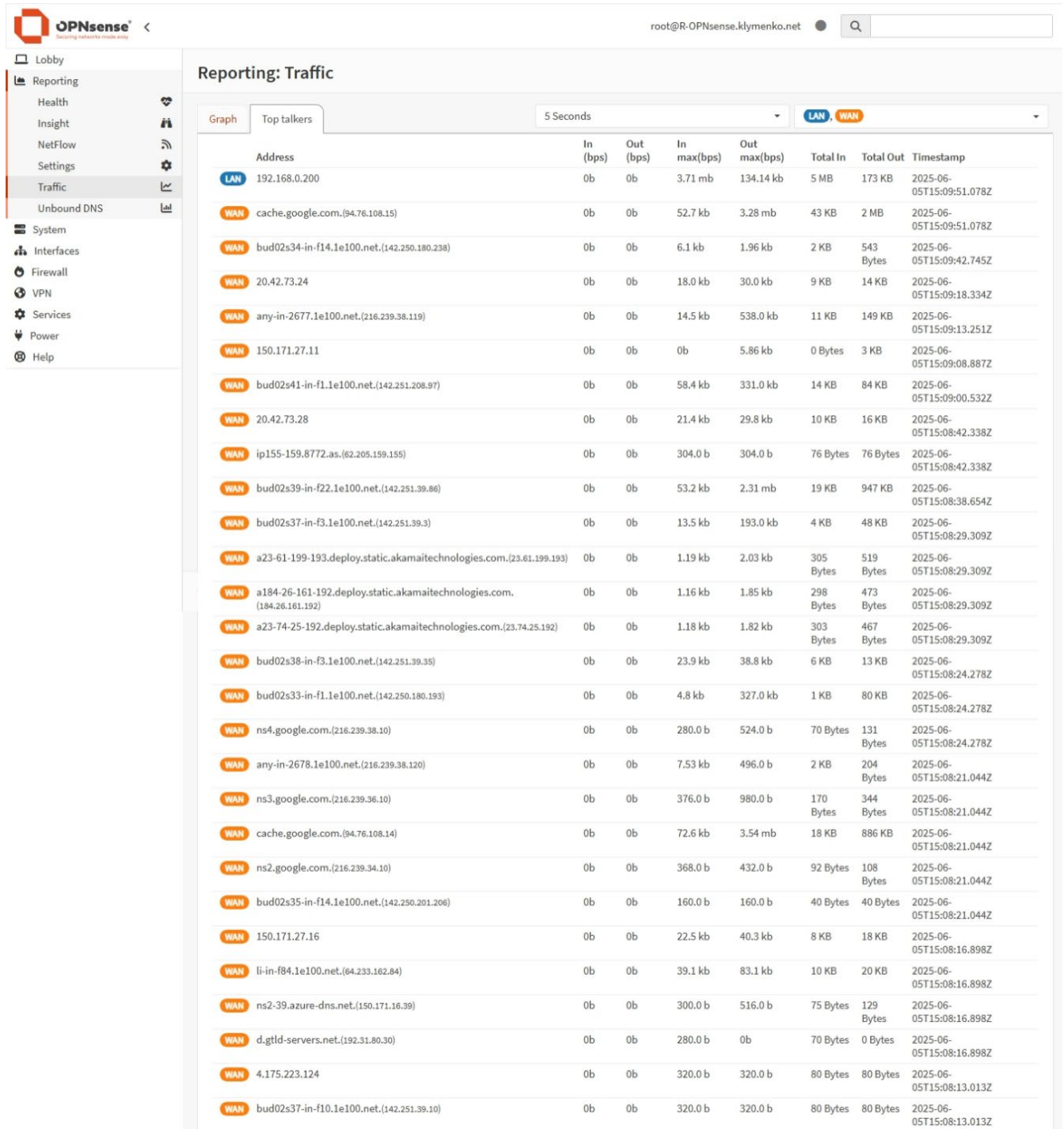
last match

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

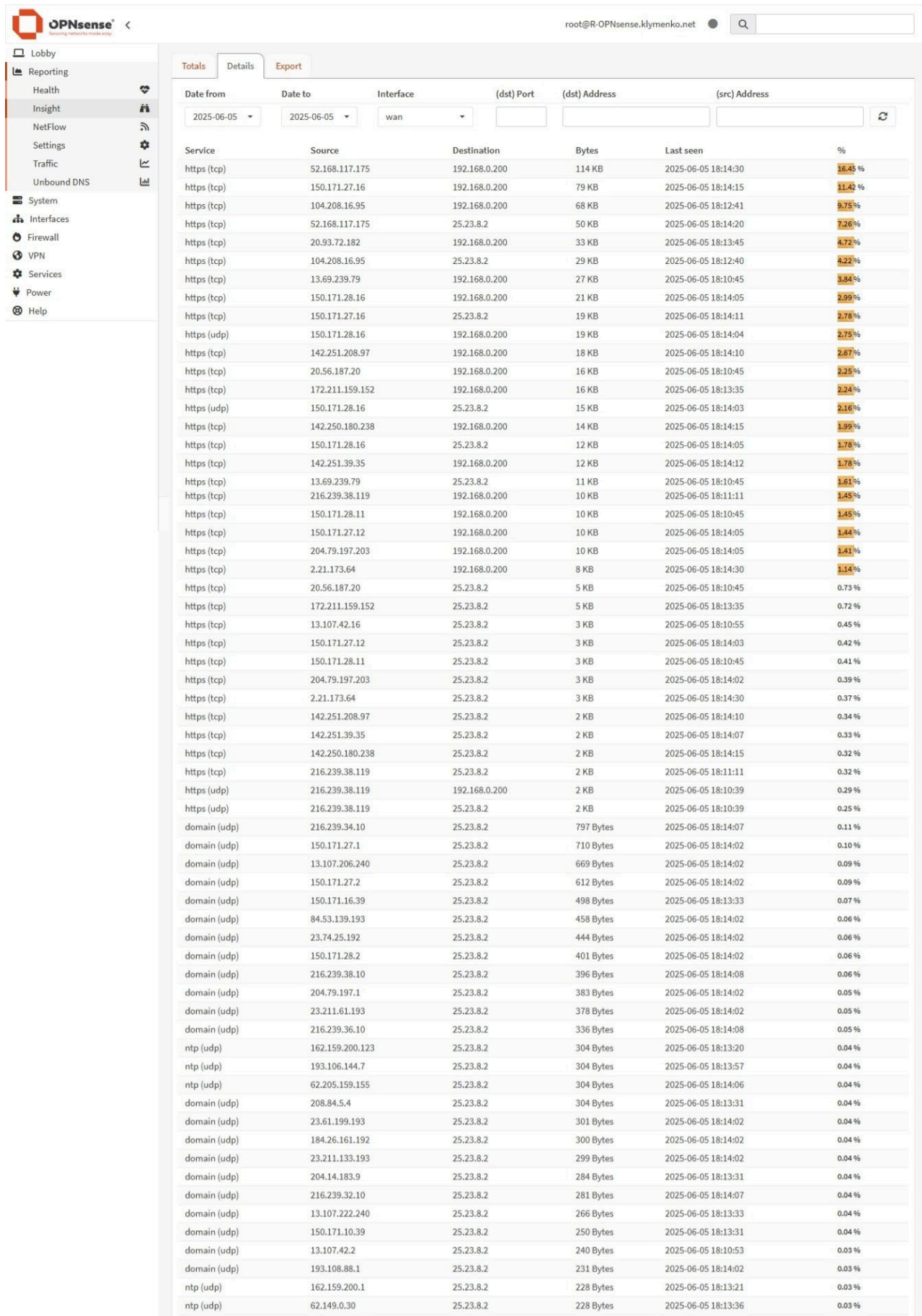
Додаток Б.3 – Статистика роботи Unbound DNS



Додаток Б.4 – Перелік найактивніших джерел трафіку в мережі.



Додаток Б.5 – Детальна аналітика мережевого трафіку



Додаток В – Конфігураційні файл комутатора SW-23-8-1

```

! Last configuration change at 21:55:01 UA Wed Jun 4 2025
!
version 15.2
service timestamps debug datetime msec show-timezone
service timestamps log datetime msec show-timezone
no service password-encryption
service compress-config
!
hostname SW-23-8-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops
EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
clock timezone UA 2 0
clock summer-time UA recurring last Sun Mar 3:00 last Sun Oct 4:00
!
!
no ip routing
no ip icmp rate-limit unreachable
!
!
!
ip domain-name klymenko.net
ip name-server 192.168.0.200
no ip cef
no ipv6 cef
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
interface Ethernet0/0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 192.168.0.253 255.255.255.0

no ip route-cache
!
ip default-gateway 192.168.0.254
ip forward-protocol nd
!
ip tcp synwait-time 5
ip http server
!
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
!
logging host 192.168.0.200
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
ntp update-calendar
ntp server serv-23-8-1
!
!
end

```

		Клименко Д.О.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		87