

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

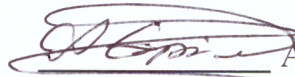
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології побудови підсистем захисту ІТ-інфраструктури на базі рішень OPNSense»

Виконав студент 2-го курсу групи КБм-23-1
спеціальності 125 «Кібербезпека та захист інформації»

 Валерій ХОМЕНКО

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

 Андрій ЄФІМЕНКО

Рецензент професор кафедри комп'ютерної інженерії та
кібербезпеки, доктор технічних наук, доцент

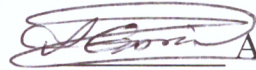
 Володимир ВОРОТНІКОВ

Житомир – 2024

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

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

17 вересня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Хоменко Валерій Ростиславович

Тема роботи: «Методи та технології побудови підсистем захисту IT-інфраструктури на базі рішень OPNSense»

затверджена Наказом університету від 17 вересня 2024 р. № 479/с

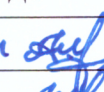
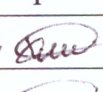
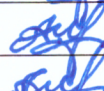
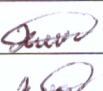
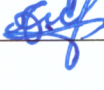
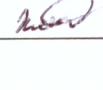
Термін здачі студентом закінченої роботи 16 грудня 2024 р.

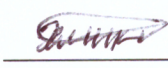
Вихідні дані роботи: об'єктом дослідження є процес побудови та впровадження методів і технологій захисту IT-інфраструктури; предметом дослідження є методи та засоби мережі, зокрема технології OPNSense для створення комплексних рішень захисту мережі.

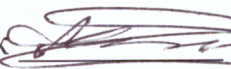
Обладнання та програмне забезпечення:

1. VirtualBox
2. ОС Linux та Windows
3. MikroTik RoutesOS
4. OPNSense

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Олексій Шелуха	25.09.2024 	25.09.2024 
2	Олексій Шелуха	15.10.2024 	15.10.2024 
3	Олексій Шелуха	01.12.2024 	01.12.2024 

Студент  Валерій Хоменко

Керівник  Андрій Єфіменко

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	12.09.2024	Виконано
2	Аналіз сучасних технологій захисту комп'ютерних мереж	25.09.2024 – 08.10.2024	Виконано
3	Аналіз існуючих технологій міжмережевого екранування	15.10.2024 – 23.10.2024	Виконано
4	Дослідження систем виявлення та попередження вторгнень	01.11.2024 – 05.11.2024	Виконано
5	Розробка структурованої моделі	06.11.2024	Виконано
6	Розробка загального проекту ІТ-інфраструктури	12.11.2024	Виконано
7	Вибір обладнання пристроїв	18.11.2024	Виконано
8	Налаштування пристроїв мережі	27.11.2024	Виконано
9	Налаштування міжмережевого екрану	01.12.2024	Виконано
10	Тестування роботи системи	04.12.2024	Виконано
11	Оформлення пояснювальної записки	05.12.2024 – 16.12.2024	Виконано
12	Захист кваліфікаційної роботи	25.12.2024	Виконано

Студент  Валерій Хоменко

Керівник  Андрій Єфіменко

АНОТАЦІЯ

Випускна кваліфікаційна робота магістра складається з проекту системи захисту корпоративної IT-інфраструктури, а також пояснювальної записки. Пояснювальна записка містить 90 сторінок друкованого тексту, 90 ілюстрацій, 9 таблиць та 25 джерел.

Метою кваліфікаційної роботи є розробка та впровадження підсистеми захисту корпоративної мережі з використанням рішення OPNsense, яке включає сучасні методи міжмережевого екранування, IDS/IPS, фільтрації трафіку, балансування навантаження та забезпечення відмовостійкості.

У процесі виконання роботи було проведено аналіз теоретичних основ захисту IT-інфраструктури, визначено актуальні загрози та виклики, досліджено можливості платформи OPNsense. У рамках проекту створено корпоративну мережу з реалізацією функцій фільтрації трафіку, виявлення і запобігання вторгненням (Suricata), а також резервування (CARP). Додатково налаштовано систему захисту від DDoS-атак, від шкідливого трафіку. Досліджено правила брандмауера OPNsense.

КЛЮЧОВІ СЛОВА: IT-ІНФРАСТРУКТУРА, OPNSENSE, МІЖМЕРЕЖЕВИЙ ЕКРАН, FIREWALL, БРАНДМАУЕР, IDS/IPS, SURICATA, ZENARMOR, DDOS, КІБЕРБЕЗПЕКА.

ANNOTATION

The master's qualification work consists of a project of a corporate IT infrastructure security system and an explanatory note. The explanatory note contains 87 pages of printed text, 90 illustrations, 9 tables and 25 sources.

The aim of the qualification work is to develop and implement a corporate network security subsystem using the OPNsense solution, which includes modern methods of firewalling, IDS/IPS, traffic filtering, load balancing and fault tolerance.

In the course of the work, the theoretical foundations of IT infrastructure protection were analysed, current threats and challenges were identified, and the capabilities of the OPNsense platform were explored. As part of the project, a corporate network was created with traffic filtering, intrusion detection and prevention (Suricata), and redundancy (CARP) functions. Additionally, a system of protection against DDoS attacks, malicious traffic. The rules of the OPNSense firewall are investigated.

KEYWORDS: IT-INFRASTRUCTURE, OPNSENSE, FIREWALL, FIREWALL, IDS/IPS, SURICATA, ZENARMOR, DDOS, CYBERSECURITY.

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1. АНАЛІЗ ТА ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІТ-ІНФРАСТРУКТУРИ	10
1.1 Аналіз сучасних загроз і викликів у захисті ІТ-інфраструктури.....	10
1.2 Технології міжмережевого екранування: огляд рішень	14
1.3 Огляд технологій безпеки в рішенні OPNsense.....	21
1.4 Принципи роботи систем виявлення та запобігання вторгненням	24
1.5 Порівняння OPNsense з іншими платформами мережевої безпеки	29
РОЗДІЛ 2. РОЗРОБКА ПРОЕКТУ ПІДСИСТЕМИ ЗАХИСТУ ІТ-ІНФРАСТРУКТУРИ	33
2.1 Розробка загального проекту ІТ-інфраструктури	33
2.2 Проектування відмовостійкого міжмережевого екранування.....	38
2.3 Вибір обладнання та програмного забезпечення	40
2.4 Визначення моделі загроз та цілей захисту ІТ-інфраструктури.....	45
РОЗДІЛ 3. РЕАЛІЗАЦІЯ, ДОСЛІЖЕННЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ	48
3.1 Налаштування міжмережевого екрану в OPNsense	48
3.2 Дослідження параметрів захисту ІТ-інфраструктури.....	56
3.3 Тестування роботи підсистеми захисту та аналіз ефективності	68
ВИСНОВКИ.....	83
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	84
ДОДАТКИ.....	87

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CARP – Common Address Redundancy Protocol
DDoS – Distributed Denial of Service
DoS – Denial of Service
HI – High Availability
HIDPS – Host-based Intrusion Detection and Prevention System
IDPS – Intrusion Detection and Prevention System
IPS – Intrusion Prevention System
LAN – Local Area Network
NAT – Network Address Translation
NBA – Network Behavior Analysis
NGFW – Next-Generation Firewall
NIDPS – Network-based Intrusion Detection and Prevention System
SIEM – Security Information and Event Management
SSL – Secure Sockets Layer
TCP – Transmission Control Protocol
TLS – Transport Layer Security
UDP – User Datagram Protocol
VHID – Virtual Host Identifier
VRPR – Virtual Router Priority Protocol
WAN – Wide Area Network

ВСТУП

Актуальність теми. У сучасному цифровому світі інформаційна безпека стає критично важливим аспектом функціонування будь-якої організації. Постійно зростаюча кількість кіберзагроз, диверсифікація методів атак та збільшення вразливостей в IT-інфраструктурі вимагають впровадження комплексних та ефективних рішень для захисту інформаційних систем.

Технології захисту IT-інфраструктури потребують інтегрованих і надійних рішень, які здатні одночасно забезпечувати контроль доступу, моніторинг активності мережі, запобігання вторгненням та інші ключові функції. В умовах обмежених бюджетів на безпеку особливого значення набувають відкриті програмні рішення, які дозволяють зменшити витрати без втрати ефективності.

Рішення OPNsense, яке є потужним open-source інструментом для побудови міжмережових екранів та забезпечення мережевої безпеки, надає широкий спектр можливостей для створення багаторівневої системи захисту. Його можливості включають управління трафіком, фільтрацію контенту, запобігання вторгненням (IDS/IPS), а також інтеграцію з іншими інструментами кібербезпеки.

Актуальність теми дослідження обумовлена необхідністю розробки універсальних, масштабованих і економічно ефективних рішень для побудови підсистем захисту корпоративних мереж, які можуть адаптуватися до сучасних умов кіберзагроз.

Метою кваліфікаційної роботи є розробка і впровадження підсистеми захисту IT-інфраструктури на базі OPNSense для забезпечення комплексної безпеки корпоративної мережі.

Для досягнення мети було поставлено такі завдання:

- Провести аналіз існуючих загроз і вразливостей мереж.
- Вивчити можливості OPNSense для побудови підсистем захисту.
- Розробити модель захищеної мережі із застосуванням технологій OPNSense.

- Налаштувати і протестувати ключові компоненти безпеки, включаючи IDS/IPS, High Availability, Web Filtering, міжмережевий екран.
- Дослідити роботу міжмережевого екрану під час атак на інфраструктуру.
- Розробити рекомендації щодо подальшого розвитку і масштабування підсистеми захисту.

Об’єктом дослідження є процес побудови та впровадження методів і технологій підсистеми захисту IT-інфраструктури.

Предметом дослідження є методи та засоби мережі, зокрема технології OPNSense для створення комплексних рішень захисту мережі.

Практичне значення одержаних результатів полягає в створенні методики, яка може бути використана організаціями різного масштабу для побудови ефективних систем інформаційної безпеки з мінімальними витратами на впровадження та подальшу підтримку.

РОЗДІЛ 1. АНАЛІЗ ТА ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІТ-ІНФРАСТРУКТУРИ

1.1 Аналіз сучасних загроз і викликів у захисті ІТ-інфраструктури

У сучасному цифровому світі захист ІТ-інфраструктури стає критично важливим завданням для організацій. переходом до цифрових технологій компанії отримують можливість автоматизувати процеси, збільшувати продуктивність і знижувати витрати. Однак цифровізація також збільшує ризики, відкриваючи доступ до важливих активів через інтернет і ускладнюючи управління безпекою. Вразливість навіть однієї складової інфраструктури може стати причиною масштабної атаки з фінансовими й репутаційними наслідками.

ІТ-інфраструктура виконує центральну роль у сучасній компанії, об'єднуючи співробітників, клієнтів і бізнес-процеси. Її компрометація може призвести до зупинки операцій, витоку конфіденційної інформації або втрати даних, що завдає компаніям значних фінансових збитків і шкодить довірі клієнтів. Зокрема, в секторах, які залежать від точності та доступності даних (наприклад, медицина чи фінанси), наслідки можуть бути катастрофічними.

Типи сучасних загроз. На ІТ-інфраструктуру впливають як зовнішні, так і внутрішні загрози. Зовнішні загрози, такі як DDoS-атаки, фішинг чи програми-видагачі, найчастіше спрямовані на дестабілізацію роботи або викрадення даних. Внутрішні загрози, зокрема халатність співробітників або зловмисна діяльність інсайдерів, можуть бути не менш руйнівними. Технологічні вразливості, пов'язані з IoT, контейнеризацією чи атаками на ланцюжок поставок, відкривають нові вектори атак для зловмисників.

Фішинг залишається одним із найпоширеніших методів атак, оскільки він націлений на людський фактор, зокрема помилки користувачів. Програми-видагачі (ransomware) паралізують операції компанії, вимагаючи викуп за розшифрування даних. DDoS-атаки, спрямовані на перевантаження мережевих ресурсів, можуть викликати значні простої. [22]

Фішингові атаки є різновидом соціальної інженерії. Багато експертів визнають фішингові атаки найпоширенішим і найефективнішим засобом злому та доступу до ресурсів компаній і організацій усіх форм власності. За різними оцінками, до 90% успішних кібератак здійснюються саме цим методом. Принцип дії досить простий: надсилається фальшивий електронний лист, текст якого спонукає жертву, наприклад, запустити вірусну програму, замасковану під офісний додаток, або перейти за посиланням на фальшивий веб-сайт, де її просять ввести логін і пароль для входу в електронну пошту або інші ресурси. Жертву заохочують це зробити. [10]

Окрім традиційних методів атак, все більшої популярності набувають загрози, що стосуються хмарних середовищ. Наприклад, згідно з дослідженнями, сучасні платформи, як-от Fortigate, дозволяють ефективно автоматизувати процеси аналізу трафіку для виявлення аномалій у хмарних мережах, що сприяє швидкій нейтралізації загроз. [1]

Незахищені IoT-пристрої, часто розроблені без врахування безпеки, стають легкою мішенню для ботнетів і атак з проникненням у мережу. У контейнеризованих середовищах, таких як Kubernetes, ризики виникають через використання ненадійних базових образів або помилки в налаштуванні оркестрації, що дозволяє зловмисникам отримувати доступ до всього кластера.



Рисунок 1.1 – Етапи злому інформаційної системи

Еволюція загроз. За останнє десятиліття кібератаки стали складнішими та більш організованими. Якщо раніше більшість атак мали випадковий характер, сьогодні зловмисники використовують автоматизацію та вдосконалені алгоритми для проведення цільових атак. Зокрема, атаки на ланцюжок поставок та програми-вимагачі стали більш поширеними через їх високу ефективність.

Організовані групи зловмисників активно використовують автоматизацію та штучний інтелект для збору даних, аналізу вразливостей і створення надзвичайно реалістичних фішингових листів. Також ШІ застосовується для автоматичного знаходження слабких місць у системах безпеки, що дозволяє зловмисникам діяти швидше, ніж традиційні засоби захисту можуть реагувати.[10]

Виклики у забезпеченні безпеки. Складність сучасних мереж, які поєднують локальні, хмарні та гібридні рішення, значно ускладнює їх захист. Узгодження політик безпеки та моніторинг таких середовищ потребує значних ресурсів і часу. Хмарні сервіси додають ризики через неправильну конфігурацію ресурсів і залежність від постачальників. Контейнеризація створює додаткові проблеми через швидкість масштабування, а IoT-пристрої залишаються вразливими через відсутність належних стандартів безпеки.

Нестача кваліфікованих кадрів у сфері кібербезпеки є серйозною перешкодою для багатьох компаній. Навіть із наявністю сучасних засобів захисту відсутність експертів для їх налаштування та підтримки значно знижує ефективність захисту. Це стає критичним, особливо для малих і середніх компаній.

Тенденції у розвитку загроз. Серед найбільш поширених загроз можна виділити атаки на хмарні середовища, програми-вимагачі, фішинг і атаки на IoT. Зростання популярності cloud-native архітектури зробило такі середовища ключовою мішенню для зловмисників.

Атаки на критичну інфраструктуру, такі як енергетика та охорона здоров'я, стають дедалі складнішими й небезпечнішими. Використання автоматизованих інструментів для пошуку вразливостей дозволяє швидше проникати в системи. Прогнози свідчать, що у найближчі 3-5 років кількість атак з використанням штучного

інтелекту та автоматизації зростатиме, а критична інфраструктура й хмарні сервіси залишатимуться серед головних цілей зловмисників.[22]

Особливу увагу слід приділяти забезпеченню безпеки трафіку, оскільки атаки на хмарні сервіси стають дедалі складнішими. Згідно з результатами досліджень, впровадження рішень Fortigate дозволяє автоматизувати процеси моніторингу та ефективно виявляти аномалії навіть у розподілених середовищах.[1]

Відомі приклади атак та їх механізм.

Одним із найбільш масштабних випадків є атака на компанію Colonial Pipeline у 2021 році. Зловмисники використовували програму-вимагач DarkSide, щоб проникнути в мережу через фішинговий лист. Після потрапляння до системи, вони зашифрували критично важливі дані компанії, вимагаючи викуп у розмірі \$4,4 мільйона. Наслідком стала тимчасова зупинка роботи трубопроводу, що забезпечує майже половину поставок пального на східному узбережжі США. Це спричинило паніку на ринку пального та збитки для компанії і споживачів.

Ще одним прикладом є витік даних із Equifax у 2017 році. Зловмисники скористалися незахищеною вразливістю у веб-додатку компанії (Apache Struts), що дозволило їм отримати доступ до персональних даних понад 147 мільйонів осіб. Компанія зазнала значних фінансових втрат і репутаційного удару, а також заплатила штрафи на сотні мільйонів доларів.

Атака на компанію SolarWinds у 2020 році демонструє, наскільки небезпечними можуть бути атаки на ланцюжок поставок. Зловмисники інтегрували шкідливий код у оновлення популярного програмного забезпечення Orion. Це дозволило їм отримати доступ до систем численних клієнтів, включаючи урядові установи США. Механізм атаки полягав у тому, що заражене оновлення поширювалося через легітимні канали, що робило його важким для виявлення. [23]

Ці інциденти підкреслюють необхідність постійного підвищення рівня кібербезпеки. Компанії, уряди і окремі особи повинні вживати заходів для захисту своїх даних і систем. Внутрішні загрози, такі як халатність співробітників чи навмисна

зловмисна діяльність, можна зменшити завдяки комбінації технічних, організаційних і освітніх заходів.

По-перше, важливо впровадити принцип найменших привілеїв (least privilege), надаючи доступ до ресурсів лише тим співробітникам, які дійсно їх потребують. Використання ролей і контроль доступу дозволяють мінімізувати ризик випадкового чи навмисного втручання.

По-друге, регулярний моніторинг дій співробітників через системи журналювання та аналізу дозволяє швидко виявляти аномальну поведінку. Встановлення політик аудиту дій на критично важливих ресурсах допоможе запобігти зловживанням.

По-третє, освітні заходи відіграють ключову роль. Навчання співробітників основам кібергігієни, таким як розпізнавання фішингових листів або безпечне поводження з конфіденційною інформацією, значно знижує ризики, пов'язані з людським фактором.

Додатково, автоматизація безпеки та використання багаторівневого захисту (наприклад, двофакторна аутентифікація) створюють додатковий бар'єр для внутрішніх загроз, зменшуючи ризики навіть у разі компрометації доступу.

1.2 Технології міжмережевого екранування: огляд рішень

Міжмережевий екран (firewall) — це система безпеки мережі, яка моніторить та контролює вхідний і вихідний трафік, базуючись на визначених правилах безпеки. Його роль в захисті мереж полягає в запобіганні несанкціонованому доступу, фільтрації шкідливого трафіку та захисті від зовнішніх і внутрішніх загроз.

Міжмережеві екрани (firewalls) є критично важливими для забезпечення кібербезпеки, оскільки вони виконують функцію першої лінії захисту від зовнішніх і внутрішніх загроз. З огляду на постійний розвиток загроз, такі як ransomware, DDoS-атаки, і соціальна інженерія, потреба в ефективному управлінні мережею стає актуальною для всіх підприємств.

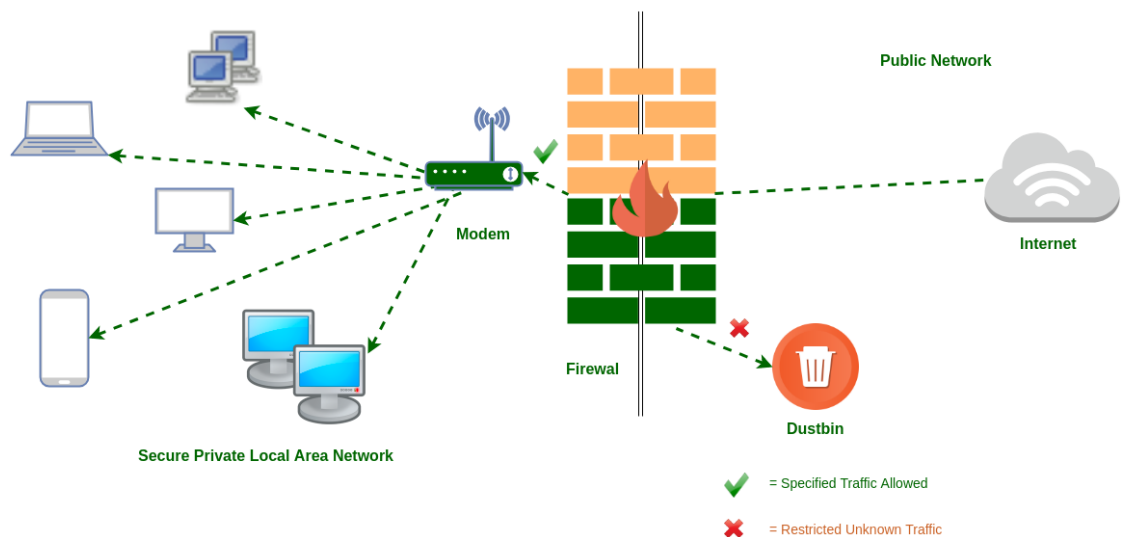


Рисунок 1.2 – Перевірка пакета брандмауером при потраплянні із зовнішньої в приватну мережу

Основні причини актуальності міжмережевих екранів:

1. Ріст обсягів кіберзагроз. У сучасному цифровому світі обсяг шкідливого трафіку стрімко зростає. Міжмережеві екрани здатні автоматично блокувати підозрілий трафік, запобігаючи вторгненням до внутрішньої мережі компанії.
2. Робота з чутливими даними. Корпоративні мережі часто працюють із конфіденційною інформацією, такою як персональні дані клієнтів, фінансова документація тощо. Міжмережеві екрани захищають ці дані від витоку.
3. Інтеграція із сучасними технологіями. Сучасні NGFW (Next-Generation Firewalls) забезпечують інтеграцію із системами виявлення та запобігання вторгненням (IDS/IPS), SIEM-платформами та хмарними сервісами, що дозволяє створити багаторівневу систему захисту.
4. Захист від атак зсередини. Міжмережеві екрани забезпечують контроль доступу для внутрішніх користувачів, запобігаючи діям потенційно шкідливих співробітників або компрометованих пристроїв.

Міжмережеві екрани виконують кілька ключових функцій, які є основою для забезпечення безпеки сучасних корпоративних мереж. Ці функції не тільки захищають інфраструктуру від зовнішніх загроз, але й допомагають дотримуватись політик доступу, забезпечуючи контроль над трафіком і захист чутливих даних.[21]

- **Фільтрація трафіку.** Фільтрація трафіку є базовою функцією міжмережових екранів, що дозволяє обмежувати доступ до мережі відповідно до визначених правил. Правила фільтрації створюються на основі IP-адрес, портів, протоколів або контенту. Адміністратор може заблокувати доступ до підозрілих IP-адрес, відомих як джерела атак, або обмежити використання певних портів, які використовуються для несанкціонованих дій.

- **Запобігання несанкціонованому доступу** — блокування спроб доступу з небезпечних або неавторизованих джерел. Це досягається за допомогою правил доступу, які дозволяють тільки авторизованим користувачам чи системам взаємодіяти з ресурсами мережі.

- **Моніторинг і ведення журналів** — дозволяє відстежувати всі події, що відбуваються в мережі. Журнали містять інформацію про джерело та пункт призначення трафіку, використані порти, протоколи, обсяг даних та статус з'єднання. Ці дані є незамінними для розслідування інцидентів безпеки, виявлення загроз та аналізу поведінки мережі. Наприклад, під час атаки типу DDoS журнали допоможуть ідентифікувати джерела підозрілого трафіку та прийняти відповідні заходи.

- **Захист від атак.** Міжмережові екрани є першою лінією оборони проти кіберзагроз, включаючи різні види атак, такі як:

- DDoS-атаки, які намагаються перевантажити сервери шляхом масового надсилання запитів;
- SQL-ін'єкції, що використовуються для доступу до баз даних;
- Фішингові атаки через шкідливі URL-адреси;
- Шкідливе програмне забезпечення, яке може поширюватися через заражений трафік.

Екрани блокують ці загрози, аналізуючи трафік на основі сигнатур, поведінкових моделей та аналізу контенту. Наприклад, глибокий аналіз пакетів (DPI) дозволяє перевіряти вміст пакетів для виявлення шкідливого коду або неналежної поведінки.

Міжмережеві екрани взаємодіють з іншими системами захисту, такими як IDS/IPS (системи виявлення і запобігання вторгненням) для більш ефективного виявлення загроз і управління інцидентами. Також вони можуть працювати з VPN (віртуальними приватними мережами), шифруючи трафік і захищаючи дані при передачі через незахищені мережі. [24]

Типи міжмережєвих екранів:

Сучасні типи міжмережєвих екранів відрізняються за принципами роботи, функціональністю та рівнями захисту, які вони забезпечують. Одним із найпростіших типів є Packet-Filtering Firewalls, які аналізують заголовки пакетів на мережевому (Layer 3) та транспортному (Layer 4) рівнях моделі OSI. Вони працюють за визначеними правилами, блокуючи або дозволяючи пакети на основі IP-адрес, портів та протоколів. Хоча ці екрани швидкі та прості у налаштуванні, вони не відстежують стан з'єднань і є вразливими до складних атак, таких як IP-спуфінг. [23]

Більш просунутий рівень захисту забезпечують Circuit-Level Gateways, які контролюють встановлення TCP/UDP-з'єднань. Вони працюють на транспортному рівні та дозволяють лише ті з'єднання, які відповідають заданим правилам. Такий підхід забезпечує схованість внутрішньої мережі, але не дозволяє аналізувати вміст трафіку, що обмежує їх функціональність.

Для більш ефективного захисту використовуються Stateful Inspection Firewalls, які враховують стан з'єднань, створюючи таблицю стану для моніторингу активних сесій. Ці екрани забезпечують динамічну фільтрацію трафіку, що значно підвищує рівень безпеки. Однак через необхідність постійного відстеження стану вони вимагають більше обчислювальних ресурсів.

Ще більш потужним інструментом є Proxy Firewalls, які працюють на рівні додатків (Layer 7). Вони виступають посередниками між користувачами та мережею, перехоплюючи запити, аналізуючи їх вміст і перенаправляючи до цільових серверів. Це дозволяє захищати мережу від атак на рівні додатків, таких як SQL-ін'єкції, і підвищувати конфіденційність, приховуючи IP-адреси користувачів.

Проте такий підхід створює затримки у передачі трафіку і потребує потужного обладнання.

Найбільш сучасними є **Next-Generation Firewalls** (NGFW), які поєднують функції традиційних фаєрволів із новітніми технологіями безпеки. Вони аналізують трафік у реальному часі за допомогою глибокого аналізу пакетів (DPI), інтегрують системи виявлення та запобігання вторгнень (IDS/IPS), а також забезпечують контроль додатків і користувачів. NGFW не лише блокують відомі загрози, а й можуть виявляти нові атаки, що робить їх ключовим компонентом кібербезпеки великих корпоративних мереж. Незважаючи на високу вартість і складність у налаштуванні, вони є стандартом у сучасному корпоративному секторі завдяки багатofункціональності та здатності адаптуватися до нових викликів.[24]

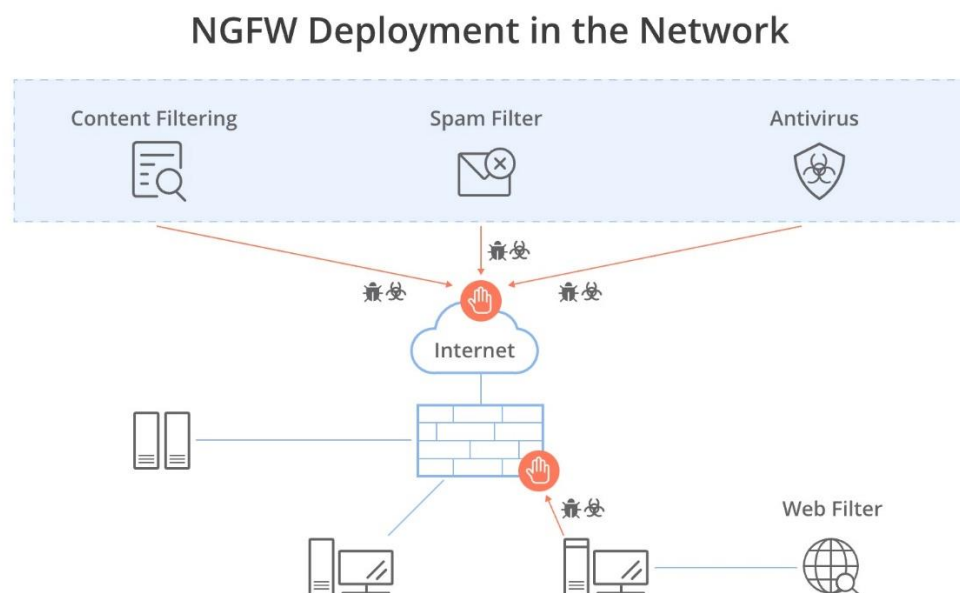


Рисунок 1.3 – Next-Generation Firewalls в мережі

Приклади рішень NGFW:

– **Palo Alto Networks:** Це одне з лідируючих рішень у галузі NGFW, яке здійснює контроль додатків, інтеграцію з хмарними платформами та виявлення загроз на основі машинного навчання. Воно пропонує високий рівень захисту завдяки глибокому аналізу трафіку, включаючи можливості для адаптивної фільтрації та запобігання загрозам в реальному часі. Однією з основних переваг є високий рівень

автоматизації у виявленні нових загроз, завдяки використанню технологій машинного навчання для аналізу поведінки трафіку.

– **Fortinet FortiGate:** Це рішення для захисту мереж з інтеграцією IDS/IPS, антивірусних технологій та функціоналу SD-WAN. FortiGate забезпечує комплексний захист завдяки вбудованій системі виявлення і запобігання вторгнень, а також автоматичному оновленню антивірусних баз. Його можливості SD-WAN дозволяють знижувати затримки та покращувати продуктивність міжмережевого з'єднання. FortiGate відомий своєю високою швидкістю обробки трафіку і підтримкою масштабованості для великих організацій.

– **Cisco ASA з Firepower:** Відоме рішення для корпоративних мереж з високим рівнем продуктивності, яке інтегрує Advanced Malware Protection (AMP) для виявлення складних атак і загроз. Cisco ASA з Firepower також включає можливості IDS/IPS та фільтрації на рівні додатків. Це рішення забезпечує надійний захист від більшості типів атак, а також інтеграцію з іншими корпоративними рішеннями Cisco для централізованого управління безпекою. [25]

– **Zenarmor:** Інноваційне рішення для фільтрації трафіку, яке спеціалізується на глибокому аналізі мережевого трафіку та поведінки додатків. Zenarmor інтегрується з OPNsense і використовує потужні алгоритми для виявлення загроз і блокування підозрілих дій в реальному часі. Це рішення добре підходить для малих і середніх підприємств завдяки своїй доступності та ефективності. Zenarmor також підтримує багаторівневий контроль трафіку, що дозволяє не лише блокувати небажані з'єднання, а й проводити розширену аналітику з метою забезпечення комплексного захисту.[21]

Таблиця 1.1 – Порівняльна характеристика NGFW

Параметр	Palo Alto Networks	Fortinet FortiGate	Cisco ASA з Firepower	Zenarmor
Контроль додатків	Так	Так	Так	Так
Інтеграція з IDS/IPS	Так	Так	Так	Так
Аналітика поведінки	Так (Machine Learning)	Так	Так (AMP)	Так (поведінковий аналіз)

Параметр	Palo Alto Networks	Fortinet FortiGate	Cisco ASA з Firepower	Zenarmor
Захист від DDoS	Так	Так	Так	Немає
Моніторинг в реальному часі	Так	Так	Так	Так
Інтеграція з хмарними платформами	Так	Так	Так	Немає
Підтримка SD-WAN	Так	Так	Немає	Немає
Складність налаштування	Висока	Середня	Висока	Середня
Ціна	Висока	Середня	Висока	Помірна

Кожен із цих типів міжмережевих екранів відіграє свою роль у захисті мережі, залежно від рівня загроз і специфіки інфраструктури, що потребує захисту. Від простих фільтрів до потужних рішень NGFW, вибір екрану визначається балансом між вартістю, складністю впровадження та необхідним рівнем безпеки.

Відкриті рішення OPNsense та pfSense надають широкий спектр можливостей для забезпечення безпеки мережі. Вони зосереджені на фільтрації трафіку, маршрутизації, VPN, IDS/IPS та інших мережевих функціях, але їх функціональність дещо відрізняється від традиційних NGFW (Next-Generation Firewall).

Однією з основних відмінностей є підхід до глибокої інтеграції з сучасними технологіями безпеки. NGFW, на відміну від OPNsense і pfSense, зазвичай має більш комплексні можливості для аналізу трафіку на рівні додатків, глибокого вивчення контенту та інтеграції з іншими системами безпеки, такими як SIEM (системи для збору та аналізу даних безпеки). NGFW також часто включає механізми для захисту від більш складних загроз, таких як атаки на рівні додатків, використовуючи глибокий аналіз пакетів і контексту, що дозволяє запобігати атакам, які звичайні брандмауери не можуть виявити.

В той час як OPNsense та pfSense забезпечують базові функції брандмауерів, такі як фільтрація за правилами, маршрутизація і VPN, їхня фокусна увага зазвичай

обмежується базовими функціями захисту, не включаючи в себе настільки глибокий аналіз трафіку та складні методи виявлення загроз. Вони можуть інтегрувати деякі функції IDS/IPS та підтримувати додаткові модулі для виявлення загроз, але їхні можливості зазвичай не зрівняються з можливостями NGFW у боротьбі зі складними атаками на рівні додатків.

OPNsense може бути чудовим вибором для малого бізнесу або стартапу, оскільки дозволяє забезпечити доступ до таких функцій, як VPN, фільтрація трафіку, виявлення загроз та журналювання, за невелику ціну. Це дозволяє малим компаніям без великих витрат на інфраструктуру зберігати належний рівень безпеки.

1.3 Огляд технологій безпеки в рішенні OPNsense

Брандмауери потребують безпеки та зміцнення, щоб успішно працювати як перша лінія захисту від кібератак. Брандмауери захищають мережу від зовнішніх загроз, таких як віруси, спроби злому та незаконний доступ. Посилення брандмауера передбачає впровадження різноманітних заходів безпеки для запобігання небажаному доступу та зниження ризику експлуатації. Регулярне оновлення програмного забезпечення, видалення непотрібних служб, встановлення обмежень доступу та прийняття надійних механізмів автентифікації - все це є частиною цього процесу.

OPNsense — це потужний відкритий фаєрвол на основі FreeBSD, що призначений для забезпечення високого рівня безпеки корпоративних мереж. Його основні особливості, які роблять його ефективним для захисту, включають гнучкість налаштувань, відкрите програмне забезпечення без ліцензійних обмежень та активну підтримку користувачами. OPNsense дозволяє детально налаштувати правила фільтрації трафіку, підтримує розширене шифрування та інтеграцію з іншими системами безпеки, що робить його ідеальним рішенням для малих та середніх підприємств. [4]

OPNsense реалізує міжмережеве екранування за допомогою фільтрації пакетів, що включає перевірку IP-адрес, портів, протоколів і навіть стану з'єднання. Він використовує stateful packet filtering для відстеження стану з'єднань і забезпечення лише дозволених з'єднань між джерелами та призначеннями. Функції фільтрації

трафіку включають можливість блокування несанкціонованих спроб доступу, контроль трафіку за допомогою правил та створення зон безпеки для різних типів трафіку, таких як веб або внутрішній корпоративний трафік.



Рисунок 1.4 – Open source firewall router OPNsense

OPNsense Traffic Shaper відстежує та оптимізує мережевий трафік. Основна мета інструменту - забезпечити ефективну роботу мережі, дозволяючи адміністраторам керувати пріоритетами, обмеженнями та розподілом пропускної здатності на основі типу даних. Це важливо для забезпечення необхідного рівня обслуговування для різних додатків і сервісів.

Traffic Shaper підтримує можливість планувати обмеження пропускної здатності за розкладом або резервувати пропускну здатність для конкретних потреб OPNsense. Це потужний інструмент для управління трафіком, особливо в ситуаціях, коли ефективність і пріоритетність мережевих ресурсів мають вирішальне значення. Він дозволяє мережевим адміністраторам тонко налаштовувати і контролювати продуктивність мережі відповідно до конкретних вимог і цілей.

OPNsense підтримує кілька протоколів для VPN, зокрема IPsec та OpenVPN. Вони забезпечують шифрування трафіку та створення безпечних з'єднань для віддалених користувачів або підключень між філіями компанії. VPN у OPNsense дозволяє захистити передавання даних через Інтернет, створюючи захищені канали для чутливої інформації, що важливо для збереження конфіденційності при віддаленому доступі.

Система IDS/IPS в OPNsense інтегрована через Suricata, яка виконує функції виявлення і запобігання вторгненням. Suricata аналізує мережевий трафік в реальному часі і здатна виявляти як відомі, так і нові загрози, застосовуючи підписи для визначення атак. Інтеграція з IDS/IPS надає додатковий рівень захисту, дозволяючи швидко реагувати на потенційно небезпечні ситуації і запобігати втручанню в мережу.

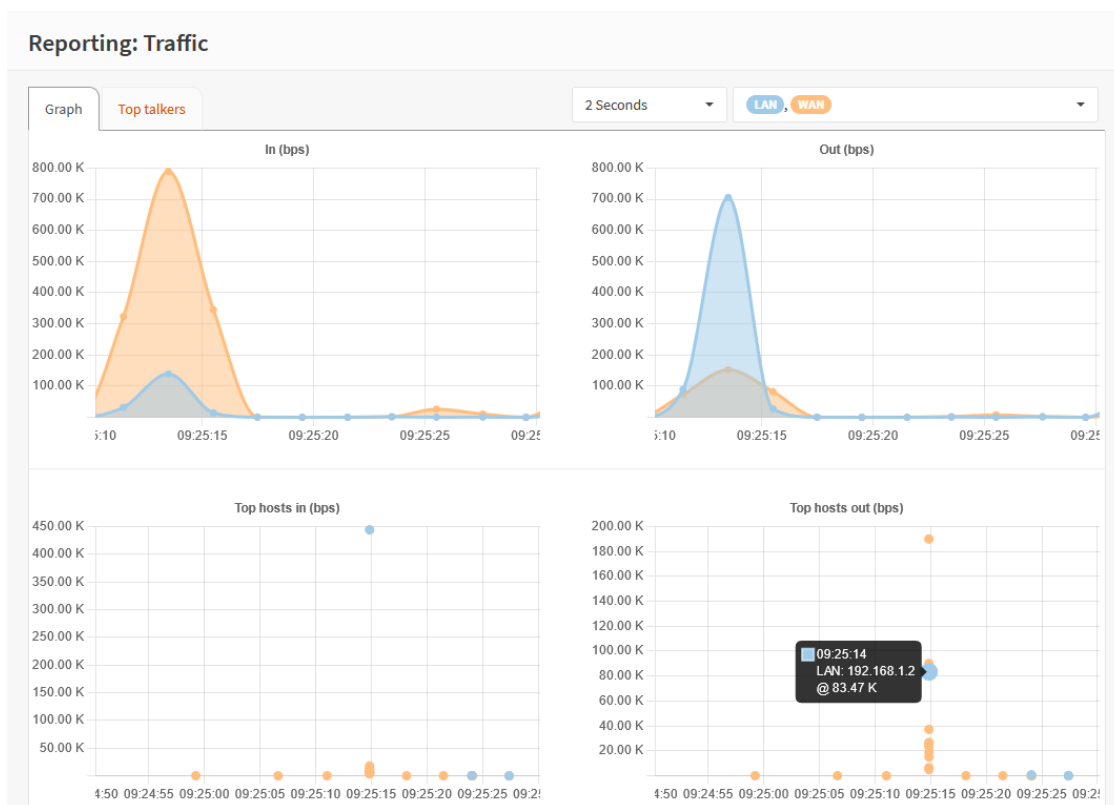


Рисунок 1.5 – Вбудована система відображення статистики в OPNsense

OPNsense має вбудовані інструменти для моніторингу подій і журналювання. Система веде детальне журналювання всіх подій, що дозволяє адміністраторам відстежувати інциденти безпеки, наприклад, спроби несанкціонованого доступу, зміни в конфігураціях та інші аномалії. За допомогою системи моніторингу можна аналізувати поведінку мережі, а також отримувати сповіщення про загрози або відмови в обслуговуванні. Дані з журналів можна інтегрувати з іншими системами моніторингу безпеки або SIEM (Security Information and Event Management).

Підтримка Netflow дозволяє аналізувати та моніторити мережевий трафік, включно з детальною інформацією про вузли та протоколи. Маршрутизатори оснащені інструментами для моніторингу стану системи, такими як завантаженість ресурсів, температура, доступна пам'ять та інші параметри. Реалізована можливість захоплення пакетів для детального аналізу мережевого трафіку в реальному часі. Крім того, доступне налаштування автоматичних сповіщень через електронну пошту або інші канали зв'язку про важливі події.[4]

OPNsense має кілька механізмів для захисту від атак типу DDoS (Distributed Denial of Service). Ці механізми включають обмеження трафіку, моніторинг підозрілих з'єднань та фільтрацію запитів, що перевищують нормальні рівні навантаження. OPNsense може також застосовувати функції rate-limiting для контролю кількості підключень і запитів до сервера, що допомагає уникнути перевантаження системи під час DDoS-атак.

OPNsense інтегрується з різними системами безпеки, що дозволяє збільшити ефективність захисту мережі. Інтеграція з іншими системами безпеки забезпечує єдиний центр керування безпекою, що дозволяє оперативно реагувати на інциденти та підвищувати рівень захисту. [5]

1.4 Принципи роботи систем виявлення та запобігання вторгненням

Процес виявлення вторгнень полягає у моніторингу подій в інформаційній чи комп'ютерній системі та їх аналізі для виявлення потенційних загроз або порушень політик безпеки. Причинами таких інцидентів можуть бути зловмисне програмне забезпечення (наприклад, віруси, шпигунські програми), неавторизований доступ зловмисників або зловживання привілеями авторизованих користувачів. Деякі інциденти можуть бути випадковими, наприклад, введення некоректної адреси комп'ютера користувачем, що призводить до несанкціонованих спроб підключення.

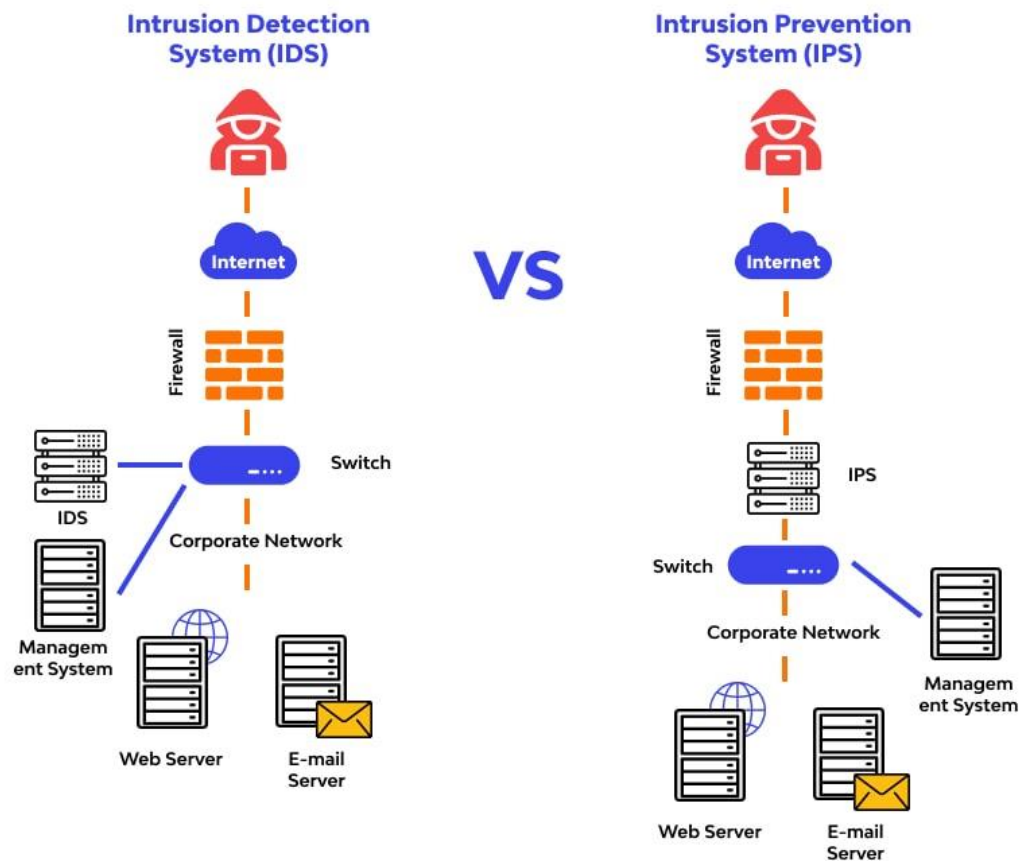


Рисунок 1.6 – Відмінності між IDS та IPS

Системи виявлення та запобігання вторгненням (IDS/IPS) — це ключові компоненти кібербезпеки, що використовуються для виявлення та запобігання атакам на корпоративні мережі. IDS (Intrusion Detection System) відповідає за виявлення вторгнень, надаючи сповіщення про потенційні загрози. IPS (Intrusion Prevention System) не тільки виявляє, але й може автоматично блокувати загрози в реальному часі, запобігаючи їхньому поширенню по мережі. Основна різниця між ними полягає в тому, що IDS обмежується моніторингом і сповіщенням про атаки, тоді як IPS активно втручається у процес, блокуючи або модифікуючи трафік для запобігання вторгненням.

Обидві зазначені системи пропонують подібні можливості, і часто адміністратори можуть використовувати IPS як систему виявлення вторгнень (IDS). Тому ці системи часто об'єднуються під загальною назвою системи виявлення та запобігання вторгненням (IDPS).

Об'єднана система виявлення та запобігання вторгнень (IDPS, Intrusion Detection and Prevention System) поєднує в собі функції IDS та IPS. Це дозволяє системі не лише виявляти загрози, але й автоматично реагувати на них, забезпечуючи більш ефективний захист мережі та систем у реальному часі. Такі системи здатні виявляти зловмисні дії та миттєво блокувати їх, не даючи зловмисникам можливості завдати шкоди. [17]

Переваги IDPS:

- Поєднання виявлення і запобігання: Можливість не лише виявити загрозу, але й автоматично вжити заходів для її запобігання.
- Реагування в реальному часі: IDPS забезпечує оперативне реагування на атаки, що дозволяє знизити час, протягом якого атака може завдати шкоди.
- Розширене виявлення атак: Завдяки інтеграції різних підходів виявлення, таких як сигнатурне та аномальне виявлення, IDPS може виявляти більш широкий спектр загроз.
- Підвищення рівня безпеки: Поєднання функцій виявлення і блокування загроз знижує ймовірність успішного вторгнення.

Недоліки IDPS:

- Витрати на ресурси: IDPS можуть вимагати значних обчислювальних ресурсів для аналізу трафіку та його обробки в реальному часі.
- Можливість помилкових спрацьовувань: Як і в IPS, існує ймовірність помилкових спрацьовувань, коли законний трафік блокується через хибне виявлення.

Системи IDPS працюють на основі моніторингу мережевого трафіку, де вони аналізують кожен пакет даних, що проходить через мережу. Вони можуть використовувати методи фільтрації пакетів для виявлення аномалій або підозрілих запитів. Використання контекстної інформації дозволяє точніше визначити, чи є певна дія атакою. Наприклад, якщо з однієї IP-адреси йде велика кількість запитів до сервера за короткий час, це може бути ознакою DDoS-атаки. Аналіз цієї поведінки в поєднанні з іншими даними дозволяє приймати обґрунтовані рішення.

IDS та IPS можуть виявляти такі загрози:

- Сканування портів, що сигналізує про спроби злому.
- DDoS-атаки, які можуть паралізувати роботу мережі.
- Шкідливе ПЗ (включаючи трояни та віруси), що передається через трафік.
- Атаки SQL-ін'єкцій чи інші спроби обходу систем авторизації.

IDPS використовують кілька основних методів для виявлення загроз:

Підписи (Signature-based detection): цей метод полягає у порівнянні мережевого трафіку з відомими підписами загроз, такими як типові шкідливі коди чи атаки. Якщо трафік збігається з підписом, система виявляє атаку.

Аномалії (Anomaly-based detection): система виявляє відхилення від нормальної поведінки трафіку або користувачів. Якщо активність виходить за межі встановлених порогових значень, це вказує на можливу атаку.

Гібридні методи (Hybrid detection): поєднання підписів і аномалій дозволяє підвищити точність виявлення. Вони дають змогу об'єднати найкращі риси обох підходів для більш ефективного захисту.

Типи IDPS.

Системи IDPS можуть бути різних типів залежно від того, де вони розгортаються і як працюють. **Мережеві системи виявлення та запобігання вторгненням (NIDS/IPS)** здійснюють моніторинг мережевого трафіку, аналізуючи його для виявлення атак. Вони зазвичай встановлюються на межі мережі та здатні працювати в реальному часі, блокуючи небажаний трафік.

Хостові системи виявлення та запобігання вторгненням (HIDS/IPS) працюють на кінцевих пристроях, таких як сервери або робочі станції. Вони аналізують активність конкретних пристроїв, що дає змогу забезпечити більш глибокий захист, оскільки моніторинг здійснюється на рівні кожної окремої машини.

Гібридні системи IDPS поєднують функціональність як мережевих, так і хостових систем, що дозволяє забезпечити більш ефективний захист, комбінуючи переваги обох підходів. [17]

Огляд популярних мережевих IDPS. Популярні рішення для виявлення та запобігання вторгненням включають як відкриті, так і комерційні системи. Snort — одна з найбільш відомих відкритих систем, яка підтримує сигнатурний і аномалійний аналіз. Це одна з найпоширеніших систем виявлення атак завдяки своїй гнучкості та налаштуванню. Snort підтримує додаткові модулі для інтеграції з іншими системами, що підвищує його ефективність у складі загальної стратегії безпеки.

Suricata — це ще одна потужна відкрита система IDPS, яка також підтримує мережеве виявлення та блокування атак у реальному часі. Вона пропонує додаткові функції, такі як глибокий аналіз пакетів (DPI) та розпізнавання аномалій.

Zeek (раніше Bro) є ще однією популярною системою для моніторингу мережевого трафіку, яка відрізняється від традиційних систем виявлення. Zeek зосереджений на аналізі поведінки і може працювати як з IDS, так і з системами управління інцидентами.

Таблиця 1.2 – Порівняння Suricata, Snort і Zeek

Функція	Suricata	Snort	Zeek (раніше Bro)
Опис	Високопродуктивний мережевий IDS, IPS та NSM	Відкрита мережева система IDS та IPS	Фреймворк аналізу мережевого трафіку
Підтримка протоколів	Широкий діапазон, включаючи IPv4, IPv6, TCP, UDP, HTTP, TLS/SSL та інше	Широкий діапазон, включаючи IPv4, IPv6, TCP, UDP, HTTP, SMTP та інше	Всебічна підтримка різних протоколів, включаючи DNS, HTTP, SSH, SSL, IRC, SMTP
Продуктивність	Багатопотоковий рушій для високої продуктивності	Однопотоковий, але ефективний	Ефективний аналіз протоколів і витяг метаданих
Механізм виявлення	Виявлення на основі сигнатур та аномалій	Виявлення на основі сигнатур	Виявлення на основі сигнатур та аномалій
Мова правил	Конфігурація на основі YAML, правила Suricata, правила ETOpen	Правила Snort	Скриптова мова Bro
Витяг файлів	Підтримується	Обмежена підтримка	Зазвичай не використовується для витягу файлів
Розшифрування TLS/SSL	Підтримується	Підтримується	Зазвичай не використовується для розшифрування TLS/SSL

Системи IDPS інтегруються з іншими технологіями безпеки для покращення загальної захищеності мережі. Наприклад, IDPS можуть взаємодіяти з фаєрволами, щоб переконатися, що трафік, що проходить через мережу, відповідає встановленим політикам безпеки. Наприклад, у хмарних середовищах, де інтенсивність трафіку є значною, застосування автоматизованих рішень, таких як Fortigate, дозволяє не лише виявляти вторгнення, а й автоматично реагувати на загрози. Система використовує аналітичні алгоритми для аналізу трафіку в режимі реального часу, забезпечуючи мінімізацію впливу загроз на функціонування сервісів. [1]

Вони також можуть бути інтегровані з системами моніторингу загроз (SIEM), що дозволяє здійснювати глибший аналіз інцидентів безпеки та швидко реагувати на виявлені загрози. Системи IDPS мають кілька переваг. Вони дозволяють оперативно виявляти вторгнення, знижують ризик поширення атак і можуть зменшити потенційні збитки від кіберзагроз. Однак, існують і певні обмеження. Наприклад, системи можуть генерувати багато помилкових спрацьовувань (false positives), що призводить до зайвих попереджень і витрат на обробку інформації. Крім того, для ефективного функціонування потрібне постійне оновлення підписів і баз даних для забезпечення актуальності захисту.

1.5 Порівняння OPNsense з іншими платформами мережевої безпеки

Порівняння OPNsense з іншими платформами мережевої безпеки дозволяє вибрати оптимальне рішення для забезпечення захисту корпоративної мережі. Кожна платформа має свої унікальні переваги, функціонал та обмеження, які можуть бути критичними в залежності від потреб організації та умов експлуатації.

OPNsense, як і pfSense, є відкритими рішеннями, які пропонують широкий функціонал для фільтрації трафіку, управління VPN, налаштування IDS/IPS та балансування навантаження. Основною перевагою цих платформ є їх безкоштовність, відкритий код і можливість розширення за рахунок модулів. OPNsense вирізняється сучасним інтерфейсом, простотою налаштування і широкими можливостями інтеграції з іншими інструментами, такими як Suricata, Zenarmor і CrowdSec.

У порівнянні з цими відкритими рішеннями, комерційні платформи, такі як Cisco ASA, FortiGate та Palo Alto, пропонують більш інтегровані та потужні інструменти для глибокого аналізу трафіку, контекстуального фільтрування, виявлення загроз на рівні додатків та масштабованості для великих підприємств. Cisco ASA спеціалізується на корпоративному рівні захисту з акцентом на продуктивність, але вимагає високого рівня підготовки для адміністрування. FortiGate пропонує багатий набір функцій для інтеграції із загрозоорієнтованими платформами через FortiGuard. Palo Alto є лідером у сегменті NGFW, пропонуючи інноваційні рішення з використанням машинного навчання для попередження загроз. OPNsense є відмінним варіантом для малих і середніх компаній, які шукають безкоштовне рішення з високою функціональністю. [25]

Таблиця 1.3 – Порівняння популярних рішень мережевої безпеки

Критерій	OPNsense	pfSense	Cisco ASA	FortiGate	Palo Alto
Міжмережеве екранування	Потужне, з фільтрацією на основі правил	Потужне, з високою налаштовуваністю	Розширена функціональність	Повний набір функцій, високий рівень захисту	Контекстуальна фільтрація, розширені функції NGFW
VPN	OpenVPN, IPSec, L2TP	OpenVPN, IPSec, L2TP	IPSec, SSL VPN	SSL VPN, IPSec	GlobalProtect, IPSec, SSL VPN
IDS/IPS	Suricata, Snort інтегровані	Snort, Suricata	Cisco Firepower IDS/IPS	FortiGuard IDS/IPS	Підтримка Threat Prevention
Зручність налаштування	Дружній інтерфейс	Простий інтерфейс	Складний, вимагає знань Cisco	Легко налаштовується через GUI	З багатьма розширеними функціями
Продуктивність	Добра для середніх мереж	Висока для малих і середніх мереж	Висока продуктивність для великих мереж	Висока продуктивність для великих підприємств	Продуктивність, орієнтована на масштабні загрози
Масштабованість	Підтримує великі мережі, з налаштуваннями	Підходить для малих і середніх мереж	Підтримує великі мережі та підприємства	Висока масштабованість для великих підприємств	Висока масштабованість для складних мереж
Вартість та ліцензування	Безкоштовно, відкритий вихідний код	Безкоштовно, відкритий вихідний код	Ліцензія з високими витратами	Платна ліцензія	Висока вартість ліцензії

При виборі платформи для забезпечення мережевої безпеки важливо враховувати її функціональність. Наприклад, pfSense, як і OPNsense, надає широкий набір інструментів для реалізації високодоступних мереж. Зокрема, функціонал балансування навантаження у pfSense дозволяє розподіляти ресурси між кількома вузлами та забезпечувати відмовостійкість, що є важливим аспектом для захисту IT-інфраструктури. [2]

Основна мета балансування навантаження – це оптимізація використання ресурсів, максимізація пропускної здатності, зменшення часу відгуку і запобігання перевантаження будь-якого одного ресурсу. Використання декількох компонентів балансування навантаження, замість одного компонента, може значно підвищити надійність і доступність за рахунок резервування. Саме балансування навантаження передбачає, зазвичай, наявність спеціального програмного забезпечення або апаратних засобів, таких як багаторівневий комутатор або система доменних імен, серверний процес. [3]

Проте, у випадку порівняння із OPNsense, pfSense має обмежені можливості інтеграції з новими модулями безпеки. Це робить OPNsense більш адаптивним для сучасних викликів, пов'язаних із складними атаками та розподіленими мережами.

Загалом, можна підсумувати основні переваги та недоліки OPNsense, що допоможе у виборі для використання в залежності від вимог та специфіки мережі

Таблиця 1.4 – Порівняльна характеристика переваг та недоліків OPNsense

Переваги	Недоліки
– OPNsense є продуктом з відкритим кодом, що дає змогу користувачам змінювати та адаптувати систему під свої потреби; – OPNsense є продуктом з відкритим кодом, що дає змогу користувачам змінювати та адаптувати систему під свої потреби; – OPNsense є продуктом з відкритим кодом, що дає змогу користувачам змінювати та адаптувати систему під свої потреби; – OPNsense є продуктом з відкритим кодом, що дає змогу користувачам змінювати та адаптувати систему під свої потреби;	– для налаштування та управління OPNsense потрібні певні знання в мережевих технологіях; – для налаштування та управління OPNsense потрібні певні знання в мережевих технологіях; – для налаштування та управління OPNsense потрібні певні знання в мережевих технологіях; – OPNsense може не підтримувати старі або специфічні моделі мережевих карт;

Переваги	Недоліки
– зручний веб-інтерфейс для адміністрування, що спрощує управління; – потужний набір інструментів для фільтрації трафіку, IDS/IPS, VPN, обмеження доступу та інших заходів безпеки – підтримка плагінів для додаткових функціональних можливостей, наприклад, моніторинг, управління брандмауером тощо; – підтримка VPN (IPSec, OpenVPN), NAT, балансування навантаження, фільтрація трафіку, VLAN; – активна підтримка з боку спільноти та регулярні оновлення з виправленнями безпеки та новими можливостями.	– при використанні віртуалізаційних середовищ або старих серверів можуть бути проблеми з продуктивністю; – хоча документація є, вона інколи може бути недостатньо детальною для новачків; – у випадку масштабних мереж OPNsense може потребувати додаткових налаштувань для забезпечення високої продуктивності; – відсутність великих компаній, які надають комерційну підтримку продукту в порівнянні з іншими рішеннями, такими як pfSense.

Висновки до першого розділу

У першому розділі роботи був проведений комплексний аналіз теоретичних основ та актуальних аспектів захисту IT-інфраструктури. Аналіз сучасних загроз показав, що з кожним роком зростає кількість та складність кібератак, що створює нові виклики для забезпечення безпеки в корпоративних мережах. Технології міжмережевого екранування, зокрема брандмауери, є одними з основних засобів захисту, проте потребують постійного вдосконалення, щоб ефективно реагувати на нові типи атак. Огляд технологій безпеки в OPNsense продемонстрував його можливості для реалізації комплексного захисту, зокрема через IDS/IPS системи, VPN, фільтрацію трафіку та SSL-інспекцію, що є важливими для захисту сучасних мереж. Принципи роботи систем виявлення та запобігання вторгненням (IDS/IPS) були описані як важливий елемент виявлення атак та захисту від них в реальному часі. Загалом, розділ дозволив сформулювати загальне розуміння актуальних методів і технологій захисту IT-інфраструктури, які можуть бути реалізовані на базі OPNsense для забезпечення надійної безпеки корпоративних мереж.

РОЗДІЛ 2. РОЗРОБКА ПРОЕКТУ ПІДСИСТЕМИ ЗАХИСТУ ІТ-ІНФРАСТРУКТУРИ

2.1 Розробка загального проекту ІТ-інфраструктури

Процес проектування підсистеми ІТ-інфраструктури базується на врахуванні потреб компанії, загроз безпеці та принципів ефективної організації мережі. Логічна топологія такої мережі дозволяє організувати взаємодію між співробітниками, підрозділами та сервісами компанії, забезпечуючи їхню стабільну і безпечну роботу. Корпоративні мережі зазвичай включають різні рівні сегментації для оптимізації трафіку, а також реалізують високий рівень захисту переданих даних. Використання трирівневої ієрархічної топології є одним із найбільш оптимальних підходів для побудови масштабованої, надійної та керованої мережі.

Трирівнева топологія складається з трьох основних рівнів: рівня ядра (Core Layer), рівня розподілу (Distribution Layer) і рівня доступу (Access Layer). Кожен із них виконує свої унікальні функції, забезпечуючи логічний поділ навантаження, відмовостійкість і можливість розширення.

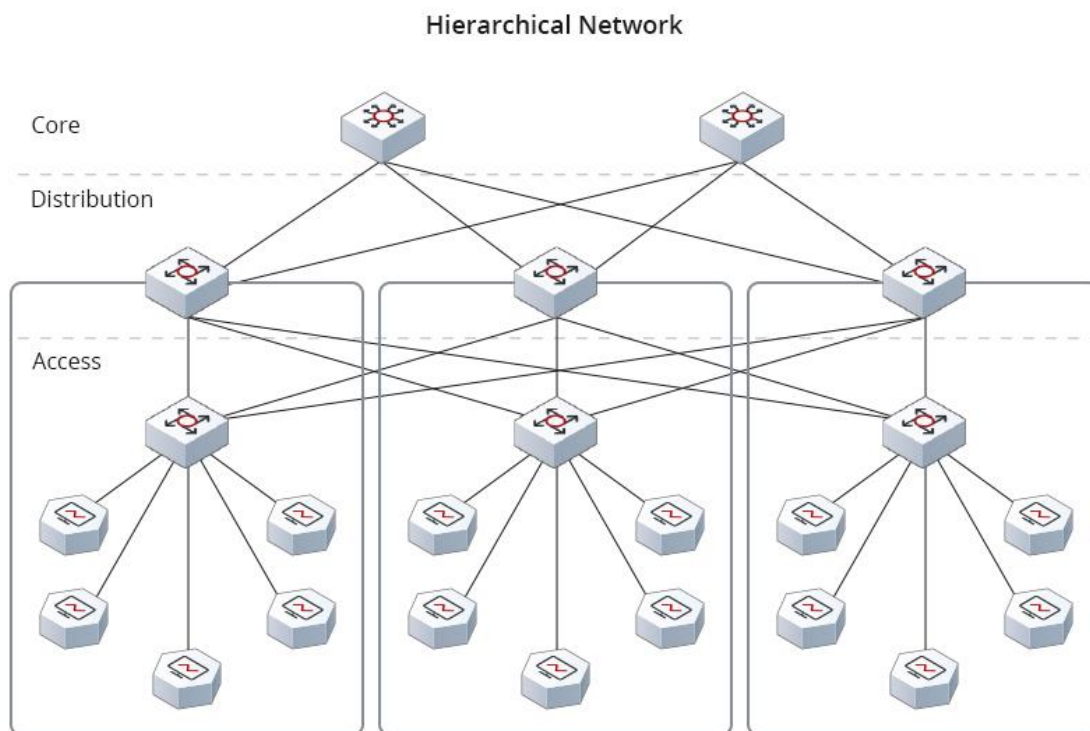


Рисунок 2.1 – Трирівнева ієрархічна модель мережі

Рівень ядра є центральною частиною мережі, яка забезпечує високошвидкісну передачу даних між іншими рівнями. На цьому рівні реалізуються найкритичніші функції маршрутизації та балансування навантаження між сегментами мережі. Для забезпечення надійності тут використовуються відмовостійкі маршрутизатори та потужні брандмауери, наприклад, OPNsense з увімкненими функціями резервування (High Availability). Основним завданням рівня ядра є швидкість і стабільність передачі трафіку, тому додаткові сервіси на цьому рівні зазвичай не розміщують.

Рівень розподілу забезпечує зв'язок між ядром і рівнем доступу. Він відповідає за виконання функцій сегментації трафіку, забезпечення відмовостійкості, застосування політик безпеки та фільтрацію даних. На цьому рівні можуть бути розміщені пристрої OPNsense для реалізації міжмережових екранів, систем виявлення та запобігання вторгненням (IDS/IPS), а також засоби шифрування трафіку, такі як VPN. Рівень розподілу часто працює з VLAN для ізоляції трафіку між підрозділами організації, що дозволяє мінімізувати ризики несанкціонованого доступу.

Рівень доступу розташований найближче до кінцевих користувачів та пристроїв. Його основною функцією є забезпечення підключення користувачів до мережі. Тут застосовуються комутатори, які підтримують функції захисту, такі як контроль доступу до портів, та забезпечують підключення пристроїв у межах сегментів. На цьому рівні також можуть впроваджуватися механізми автентифікації та контролю доступу до мережі.

Проектування трирівневої топології враховує як фізичну, так і логічну структуру мережі. Наприклад, фізичне розміщення комутаторів і маршрутизаторів узгоджується з вимогами організації, такими як кількість користувачів, географічне розташування офісів і можливе розширення мережі. Логічна структура передбачає IP-адресацію, а також налаштування правил маршрутизації між сегментами.

Така топологія дозволяє зберігати баланс між простотою адміністрування, масштабованістю та безпекою. Рівні ядра, агрегації та доступу розділяють відпові-

дальність між собою, знижуючи навантаження на кожен із компонентів і спрощуючи процеси модернізації чи усунення несправностей. Завдяки цьому трирівнева топологія є стандартом у сучасних корпоративних мережах. [16]

У межах створення моделі підмережі інфраструктури було враховано ключові аспекти, які забезпечують її надійність, масштабованість та безпеку. Для забезпечення відмовостійкості впроваджено резервування брандмауерів, а для безпеки трафіку — технології виявлення вторгнень (IDS/IPS), фільтрації та моніторингу. Завдяки цьому інфраструктура не лише вирішує існуючі проблеми, а й створює надійний фундамент для подальшого розвитку компанії.

На основі цих вимог було розроблено проект, що базується на трирівневій архітектурі мережі. У цій архітектурі ключову роль виконують брандмауери OPNsense, маршрутизатор Mikrotik, комутатори та клієнтські пристрої, які працюють у різних сегментах мережі. Сегментація дозволяє розділити трафік між адміністративною, користувацькою та гостьовою мережами, забезпечуючи оптимізацію ресурсів і підвищення рівня безпеки.

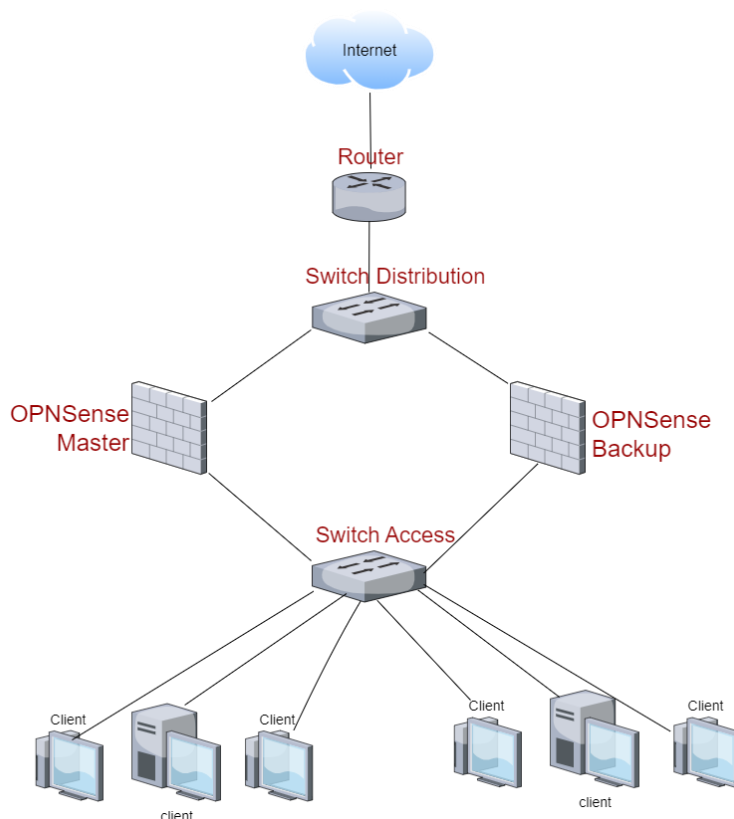


Рисунок 2.2 – Логічна топологія мережі

У представленій топології ключову роль виконують брандмауери OPNsense, маршрутизатор Mikrotik, комутатори та клієнтські пристрої, що працюють у різних сегментах мережі. Сегментація дозволяє розділити трафік між адміністративною, користувацькою та гостьовою мережами, забезпечуючи оптимізацію ресурсів і підвищення рівня безпеки.

Для розробки цієї моделі враховано наступні фактори:

- забезпечення високого рівня відмовостійкості;
- чітка сегментація мережі;
- безпечне з'єднання із зовнішніми ресурсами через Інтернет;
- посилення кібербезпеки для захисту від атак програм-вимагачів та інших загроз;
- моніторинг та захист мережі в режимі реального часу;
- можливість масштабування мережі за рахунок додавання нових користувачів та пристроїв.

Детальніше розглянемо кожен рівень. На рівня ядра розташований маршрутизатор Mikrotik, відповідає за з'єднання мережі з Інтернетом. Він виконує функцію маршрутизації глобального трафіку між зовнішньою мережею (Інтернет) і локальною мережею. Цей рівень забезпечує високу пропускну здатність і мінімальну затримку, адже через нього проходить весь трафік до/з Інтернету.

Рівень розподілу. На цьому рівні знаходить комутатор Switch Distribution. Він відповідає за об'єднання та маршрутизацію трафіку між різними мережевими сегментами, забезпечуючи їх взаємодію. А також два міжмережєвих екрани OPNsense Master і OPNsense Backup. Це два брандмауери, які працюють у режимі відмовостійкості завдяки використанню протоколу CARP. OPNsense Master є основним вузлом і приймає весь трафік на себе. OPNsense Backup перебуває в резерві й автоматично активується у разі збою основного вузла.

На цьому рівні реалізується фільтрація трафіку, забезпечення безпеки (IDS/IPS, блокування доступу), балансування навантаження та резервування.

На рівні доступу знаходиться комутатор Switch Access. Він об'єднує кінцевих користувачів, сервери та інші пристрої мережі.

Загалом, схема демонструє добре структуровану ієрархічну мережу, яка орієнтована на відмовостійкість, безпеку та продуктивність. Такий підхід дає змогу легко розширювати мережу, додавати нові пристрої та сегменти без значного впливу на поточну інфраструктуру.

IP-адресація є важливою частиною проектування мережі, яка забезпечує ефективний обмін даними між її рівнями. Для функціонування мережі передбачено використання двох основних підмереж: одна для між рівнем розподілу та ядра, інша — для локальної мережі. Усі пристрої локальної мережі мають отримати належні адреси залежно від їх функціонального призначення: статичні для мережевого обладнання та серверів, а динамічні — для клієнтських пристроїв. У наведеній топології використовуються дві основні підмережі: Мережа 172.18.0.0/24 між рівнями ядра та розподілу. Мережа 10.200.200.0/24 між рівнями розподілу та доступу.

Таблиця 2.1 – Адресація підмережі WAN

Призначення	IP-адреса (WAN)	IP-адреса (LAN)
Адреса мережі	172.18.2.0	10.200.200.0
Маска мережі	255.255.255.0/24	255.255.255.0/24
Інвертована маска	0.0.0.255	0.0.0.255
Мінімальна адреса	172.18.2.1	10.200.200.1
Максимальна адреса	172.18.1.254	10.200.200.254
Широкомовна адреса	172.18.1.255	10.200.200.255

Таблиця 2.2 – Параметри адресації маршрутизатора

Призначення	IP-адреса	Пристрій підключення
Інтерфейс Gigabit Ethernet0/0	DHCP	Інтернет
Інтерфейс Gigabit Ethernet1/0	172.18.0.1/24	Комутатор Switch Distr

Таблиця 2.3 – Параметри адресації міжмережевого екрану OPNSense Master

Призначення	IP-адреса	Пристрій підключення
LAN	10.200.200.251/24	Комутатор Switch Access
WAN	172.18.0.100/24	Комутатор Switch Distribution
pfSyns	10.0.0.1/24	OPNSense Backup

Таблиця 2.4 – Параметри адресації міжмережевого екрану OPNSense Backup

Призначення	IP-адреса	Пристрій підключення
LAN	10.200.200.252/24	Комутатор Switch Access
WAN	172.18.0.99/24	Комутатор Switch Distribution
pfSyns	10.0.0.2/24	OPNSense Master

2.2 Проектування відмовостійкого міжмережевого екранування

У цьому підрозділі розглядається реалізація відмовостійкого міжмережевого екранування в IT-інфраструктурі за допомогою OPNSense. Основна мета полягає в забезпеченні безперебійної роботи мережі навіть у разі виходу з ладу одного з брандмауерів. Завжди буде резервний, який візьме на себе навантаження. Користувач він навіть не буде знати, що один із брандмауерів вийшов з ладу. Це досягається шляхом використання технології CARP у поєднанні з pfSync для синхронізації станів.

Відмовостійкість є важливою складовою забезпечення безперебійної роботи мережі, особливо на рівні розподілу, де вирішуються питання маршрутизації між різними сегментами мережі.

Балансування навантаження є важливою функцією для високодоступних мереж, оскільки воно дозволяє розподіляти трафік між декількома серверами. Це може допомогти підвищити продуктивність мережі, оскільки трафік не надходить лише на один сервер. Балансування навантаження також може допомогти підвищити доступність мережі, оскільки якщо один сервер вийде з ладу, інший сервер зможе продовжувати обробляти трафік.[2]

В проєкті задіяно два міжмережевих екранів OPNSense. Брандмауери мають власні IP-адреси на кожному інтерфейсі (для Master і Backup) та спільну віртуальну IP-адресу (VIP) для кожної підмережі, яка використовується в CARP.

Відмовостійкість є важливою складовою забезпечення безперебійної роботи мережі, особливо на рівні розподілу, де вирішуються питання маршрутизації між різними сегментами мережі. Використання протоколу CARP (Common Address Redundancy Protocol) на цьому рівні дозволяє забезпечити автоматичне переключення між активним і резервним вузлом у разі збоїв. OPNSense використовує CARP

для відновлення апаратного забезпечення після відмови. Два або більше брендмауерів можна налаштувати як групу відновлення після відмови. Якщо один інтерфейс не працює на основному або основний повністю вимикається, вторинний стає активним. Використання цієї потужної функції OPNsense створює повністю резервованій брендмауер із автоматичним і плавним відновленням після збоїв. Під час переходу на резервну мережу підключення залишатимуться активними з мінімальними перервами для користувачів. [5]

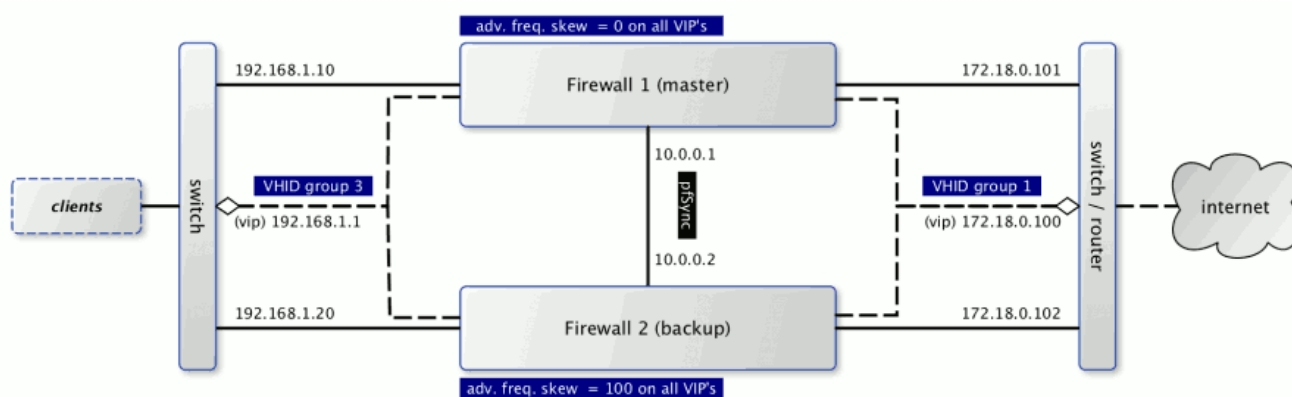


Рисунок 2.3 – Приклад мережі відмовостійкого міжмережевого екранування

Принцип роботи CARP:

CARP створює віртуальну IP-адресу (VIP), яку спільно використовують два або більше брендмауерів або маршрутизаторів. Один з них виступає активним, тоді як інші працюють у режимі очікування (standby). У разі відмови активного вузла роль автоматично переходить до резервного.

На рівні розподілу це реалізується наступним чином:

1. *Конфігурація CARP на OPNsense.* На двох вузлах (основному та резервному) налаштовуються інтерфейси з однаковими параметрами, але кожен вузол має власну фізичну IP-адресу. Додатково створюється віртуальна IP-адреса, яка буде використовуватися в мережі.

2. *Механізм синхронізації станів (pfSync).* Для забезпечення відмовостійкості на рівні з'єднань використовується протокол pfSync, який передає інформацію про стан підключень між вузлами. Це дозволяє користувачам не відчувати розриву в роботі навіть у разі аварії. Основна роль pfSync полягає в тому, щоб гарантувати,

що коли з'єднання або стан змінюється на одному брандмауері, ці зміни автоматично синхронізуються з іншими брандмауерами в кластері.

3. *Моніторинг доступності вузлів.* CARP використовує механізм "heartbeats" для перевірки стану вузлів. Якщо основний вузол перестає відповідати, резервний автоматично бере на себе його функції.

4. *Взаємодія з маршрутизаторами та комутаторами.* На рівні розподілу віртуальна IP-адреса використовується як шлюз для нижніх рівнів (доступу) і верхніх рівнів (ядра). Це дозволяє забезпечити прозорість перемикання для користувачів.

Переваги використання CARP:

- Висока доступність: забезпечується безперервна робота навіть у разі збоїв на основному вузлі.
- Простота налаштування: CARP підтримується нативно в OPNsense, що робить його інтеграцію простою.
- Масштабованість: можливість додавати більше вузлів у кластер при збільшенні вимог.

Особливості реалізації в OPNsense:

У OPNsense підтримка CARP включає графічний інтерфейс для налаштування, що спрощує процес. Достатньо налаштувати:

- інтерфейси для синхронізації (pfSync);
- віртуальну IP-адресу для CARP;
- пріоритет вузлів VHID (основний вузол має нижчий пріоритет). Протокол VRPP, який дозволяє групі маршрутизаторів працювати як один віртуальний маршрутизатор.

Використання CARP на рівні розподілу забезпечує стабільну роботу мережевої інфраструктури навіть за умов виникнення несподіваних збоїв. [12]

2.3 Вибір обладнання та програмного забезпечення

Для побудови захищеної та стабільної IT-інфраструктури важливо правильно підібрати апаратні та програмні засоби, які відповідатимуть потребам організації

та бюджету. У даному проєкті було враховано необхідність забезпечення гнучкості, надійності та доступності мережевих компонентів, а також оптимізацію витрат.

Особливу увагу приділено вибору маршрутизаторів, комутаторів і апаратного забезпечення для роботи брандмауера OPNsense. Враховуючи обмежений бюджет, обрано обладнання, яке забезпечує необхідний рівень функціональності, підтримку сучасних протоколів і можливість масштабування інфраструктури в майбутньому.

У цьому підрозділі описані конкретні пристрої, що будуть використовуватися на різних рівнях мережі: маршрутизатор для організації міжмережевої маршрутизації, комутатори для взаємодії між рівнями ядра, розподілу та доступу, а також апаратна платформа для розгортання системи OPNsense.

При виборі пристрою для встановлення міжмережевого екрану OPNsense вибір пав на недороге, але функціональне рішення для організації мережевої безпеки Protectli Vault FW4B.

Protectli Vault FW4B — це компактний і енергоефективний апаратний пристрій, призначений для роботи як мережевий брандмауер, маршрутизатор, VPN-сервер або інша мережева функція. Його гнучкість, сумісність із популярними програмними платформами (OPNsense, pfSense, Untangle тощо) і приваблива ціна роблять його ідеальним вибором для малих і середніх підприємств або домашніх лабораторій.



Рисунок 2.4-2.5 – Апаратний пристрій Protectli Vault

Protectli Vault — це ПК малого форм-фактора, створений для використання як брандмауер/маршрутизатор. FW4B базується на конструкції з 4 мережевими портами, яка використовує малопотужний, але універсальний процесор Intel Celeron J3160. Цей ЦП підтримує AES-NI, апаратне прискорення Intel для шифрування. Vault використовує стандартні компоненти Intel (включно з мережевими портами Intel), що забезпечує сумісність із різноманітними операційними системами, включаючи ряд проектів брандмауера з відкритим кодом. У Protectli Vault немає вентиляторів, тому в ньому немає рухомих частин, що створює неймовірно міцну платформу, яку можна використовувати в не ідеальних умовах. Його повністю алюмінієвий корпус (тут без пластику) є гігантським радіатором, який зберігає ЦП у холоді. FW4B може вмістити до 8 ГБ оперативної пам'яті DDR3L-1600 і 1 ТБ накопичувача mSATA. [6]

Для забезпечення надійної роботи мережі необхідно підібрати відповідне обладнання. Опираючись на кількість портів, можливості та особливості пристрою, було вирішено забезпечити організацію маршрутизатором Mikrotik.

Mikrotik RB4011iGS-RM - це гігабітний роутер на 10 Gigabit Ethernet портів і з одним оптичним портом SFP+. Маршрутизатор обладнаний 4-ох ядерним процесором. У роутері використовується потужний чіп Quad Core A15 (розроблений у лабораторії Annapurna компанії Amazon). Такий самий чип використовується в RB1100AHx4. Впроваджено підтримку PoE.



Рисунок 2.6 – Маршрутизатор Mikrotik RB4011iGS-RM

Процесором підтримується апаратне прискорення IPsec і йому надано 1 ГБ ОЗП, що дає змогу реалізувати абсолютно будь-який додаток конфігурації

RouterOS. Mikrotik RB4011iGS+RM надходить покупцеві в професійному матовому корпусі чорного кольору.

Маршрутизатор має 10 портів Gigabit Ethernet і 1 порт SFP + з метою приєднання підключення 10 Гбіт/с за рахунок модуля SFP +. Останній у комплектацію поставки не входить. RB4011iGS-RM ідеальний як для великих, так і для невеликих підприємств.

За рахунок вбудованого прискорювача маршрутизатор може працювати зі швидкостями до 2,5 Гбіт/с. Тунель моделі AES-256-CBC + SHA256 має пропускну здатність до 2 Гбіт/с, а в режимі перемикання може обробляти обсяги до 9,7 Гбіт. Роутер Mikrotik RB4011iGS+RM чудово поєднується з модулем MiniGBIC 10 Гбіт/с, щоб задіяти можливості SFP+ порту.

Всю цю потужність виробник вмістив у компактний і професійний на вигляд твердий матовий корпус чорного кольору. Модель має 2 стійкових вуха для надійного закріплення в стійці 1U. [7]

Комутатор Cisco CBS220-16T-2G-EU

Cisco CBS220-16T-2G-EU — це керований комутатор з базовими функціями рівня 2, призначений для використання в невеликих і середніх мережах. Він поєднує в собі доступну ціну, простоту налаштування та функції, які допомагають забезпечити надійність і безпеку мережевої інфраструктури. Завдяки компактным розмірам та економічності, цей комутатор є оптимальним вибором для рівня між ядром і розподілом у корпоративній мережі.



Рисунок 2.7 – Комутатор Cisco CBS220-16T-2G-EU

Cisco Business 220 Series - це доступні за ціною інтелектуальні комутатори, що відрізняються простотою використання, безпекою та надійністю для бізнес-

класу. Завдяки інтуїтивно зрозумілій панелі управління, функціям Power over Ethernet (PoE) та функціям, що налаштовуються, ці комутатори забезпечують надійну бізнес-мережу в рамках вашого бюджету. Якщо вам потрібна мережа бізнес-класу, а вартість є головним пріоритетом, Cisco Business 220 Series стане чудовим рішенням. [8]

Комутатор Cisco CBS110-16T-EU - лінійка некерованих комутаторів Cisco Business серії 110, є частиною мережевих продуктів Cisco Business. Це економічні рішення з підтримкою гігабітних підключень Ethernet для невеликих мереж. Дані комутатори Cisco розроблені спеціально для малих компаній з базовими вимогами до мережі і відрізняються високою енергоефективністю. Він забезпечує надійне підключення на рівні доступу та відмінно підходить для підключення кінцевих пристроїв, таких як робочі станції, принтери та IP-телефони. Комутатор ідеально впишеться в інфраструктуру, де немає потреби у складному адмініструванні або сегментації мережі. [9]



Рисунок 2.8 – Комутатор Cisco CBS110-16T-EU

Вибираючи одну з моделей цього сімейства, ви можете розраховувати на високу надійність мережевих підключень відповідно до вимог бізнесу, а також на додаткові функції: забезпечення якості обслуговування, виявлення циклів і діагностика кабелів. І все це в одному комутаторі, самостійне налаштування, яке займає кілька хвилин. Комутатори Cisco Business серії 110 розраховані на встановлення в невеликих офісних приміщеннях і доступні конфігурації з 5, 8, 16 і 24 портами, що

дає змогу підібрати оптимальну модель залежно від використання. Крім того, комутатори Cisco Business серії 110 Series представлені в компактному настільному виконанні та у форм-факторі для монтажу в стійку. У комутаторах відсутні вентилятори, тому вони не створюють шуму і не заважають роботі ні за яких умов.

2.4 Визначення моделі загроз та цілей захисту ІТ-інфраструктури

Модель загроз визначає потенційні небезпеки для ІТ-інфраструктури, враховуючи специфіку її побудови та функціонування. У випадку використання OPNsense як основного інструменту для захисту мережі, головна увага приділяється захисту критично важливих ресурсів, мінімізації ризиків доступу до конфіденційної інформації, а також забезпеченню відмовостійкості системи.

Аналіз ризиків та впровадження заходів для захисту мережі на основі міжмережевого екрану OPNSense можна провести, виходячи з деяких загальних загроз та рекомендацій щодо їх усунення. Ось кілька ризиків та можливих заходів для захисту мережі:

Таблиця 2.5 – Аналіз ризиків підсистеми

№	Ризик	Заходи для захисту
1	DDoS атака	Використання фільтрації на основі частоти запитів, налаштування правил на OPNsense для обмеження потоку трафіку, налаштування інструментів для виявлення і запобігання DDoS (наприклад, Suricata).
2	Сканування портів і несанкціоноване сканування мережі	Використання системи виявлення вторгнень (IDS), налаштування брандмауерів для блокування непотрібних портів, регулярне оновлення правил фільтрації на OPNsense.
3	Атаки на рівні додатків (SQL ін'єкції, XSS)	Використання web application firewall (WAF), налаштування фільтрації HTTP/HTTPS трафіку через OPNsense, регулярне оновлення ПЗ, виявлення підозрілих запитів за допомогою Suricata.\
4	Фішинг та соціальна інженерія	Навчання співробітників, використання багатофакторної автентифікації (MFA), розмежування доступу до чутливих систем, перевірка всіх зовнішніх комунікацій.
5	Втеча даних (перехоплення або витік)	Шифрування даних (VPN, SSL/TLS), використання контролю доступу до чутливих даних, зберігання паролів у зашифрованому вигляді, аудит доступу.

№	Ризик	Заходи для захисту
6	Шкідливі програми та віруси в мережі	Використання антивірусного ПЗ на всіх кінцевих пристроях, постійне оновлення програмного забезпечення, фільтрація трафіку через OPNsense, налаштування контролю за шкідливими доменами та IP-адресами.
7	Несанкціонований доступ до внутрішньої мережі	Використання багатофакторної автентифікації (MFA), впровадження політик найменших прав, сегментація мережі за допомогою VLAN, обмеження доступу до мережевих ресурсів.
8	Збої в роботі обладнання або програмного забезпечення	Використання резервних копій даних, налаштування високої доступності (HA), резервування критичних компонентів, автоматичне відновлення після відмови.
9	Зовнішні загрози через ненадійні постачальники та партнерів	Проведення аудиту безпеки постачальників, використання VPN для захищених з'єднань, перевірка систем безпеки сторонніх додатків, контроль за зовнішніми з'єднаннями.
10	Зловживання правами доступу співробітниками	Створення політики доступу на основі ролей (RBAC), моніторинг та аудит доступу, періодичний перегляд прав доступу, використання журналів доступу та сповіщень про підозрілу активність.

Для того, щоб ефективно запобігти ризикам, визначеним у таблиці, мережа повинна бути побудована з урахуванням кількох ключових принципів, що забезпечують високий рівень безпеки та стійкості до потенційних загроз.

Ризики можуть виникати як ззовні, так і всередині організації, тому важливо вчасно виявляти загрози та впроваджувати відповідні заходи для їхнього запобігання або мінімізації наслідків. Всі елементи інфраструктури повинні бути налаштовані для забезпечення високої доступності та стійкості до атак, з постійним вдосконаленням та оновленням систем захисту для адаптації до нових загроз.

Висновки до другого розділу

Другий розділ роботи зосереджений на розробці проекту підсистеми захисту ІТ-інфраструктури, що включає детальне проектування та вибір необхідних компонентів для забезпечення надійного захисту. Розробка загального проекту ІТ-інфраструктури дозволила визначити основні елементи мережі та ключові компоненти,

які повинні забезпечити ефективну взаємодію та безпеку в рамках корпоративної мережі. Проектування відмовостійкого міжмережевого екранування показало важливість забезпечення високої доступності та надійності мережевого захисту через використання механізмів резервування та балансування навантаження. Вибір обладнання та програмного забезпечення враховував вимоги до масштабованості, безпеки та ефективності. Визначення моделі загроз та цілей захисту допомогло чітко сформулювати основні уразливості системи та визначити пріоритети в захисті від можливих атак. Всього цього вдалося досягти завдяки ретельному підходу до вибору інструментів і стратегій захисту, що забезпечують ефективний рівень безпеки для організації.

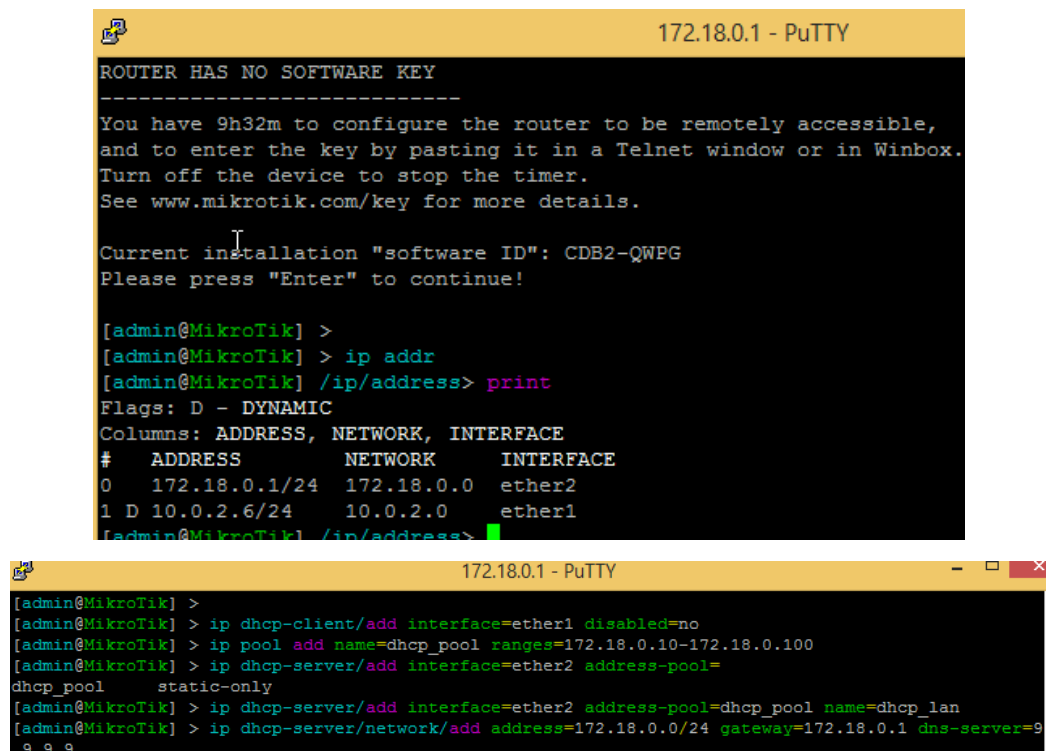
РОЗДІЛ 3. РЕАЛІЗАЦІЯ, ДОСЛІЖЕННЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ

3.1 Налаштування міжмережевого екрану в OPNsense

У цьому розділі розглядається практична реалізація підсистеми захисту IT-інфраструктури на базі рішення OPNsense. Використання віртуальних машин у середовищі VirtualBox дозволяє створити тестове середовище, що імітує реальну мережеву інфраструктуру. Такий підхід надає змогу здійснити попереднє налаштування, випробування та оптимізацію конфігурації без необхідності використання фізичного обладнання.

Основна увага приділяється налаштуванню міжмережевого екрану OPNsense, що є ключовим елементом захисту мережі. Міжмережевий екран виконує функцію фільтрації трафіку, запобігаючи несанкціонованому доступу, та контролює рух даних у мережі відповідно до визначених правил.

Базове налагодження маршрутизатора MikroTik:



```
172.18.0.1 - PuTTY
ROUTER HAS NO SOFTWARE KEY
-----
You have 9h32m to configure the router to be remotely accessible,
and to enter the key by pasting it in a Telnet window or in Winbox.
Turn off the device to stop the timer.
See www.mikrotik.com/key for more details.

Current installation "software ID": CDB2-QWPG
Please press "Enter" to continue!

[admin@MikroTik] >
[admin@MikroTik] > ip addr
[admin@MikroTik] /ip/address> print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
# ADDRESS NETWORK INTERFACE
0 172.18.0.1/24 172.18.0.0 ether2
1 D 10.0.2.6/24 10.0.2.0 ether1
[admin@MikroTik] /ip/address>

[admin@MikroTik] >
[admin@MikroTik] > ip dhcp-client/add interface=ether1 disabled=no
[admin@MikroTik] > ip pool add name=dhcp_pool ranges=172.18.0.10-172.18.0.100
[admin@MikroTik] > ip dhcp-server/add interface=ether2 address-pool=
dhcp_pool static-only
[admin@MikroTik] > ip dhcp-server/add interface=ether2 address-pool=dhcp_pool name=dhcp_lan
[admin@MikroTik] > ip dhcp-server/network/add address=172.18.0.0/24 gateway=172.18.0.1 dns-server=9
.9.9.9
```

Рисунок 3.1-3.2 – Базове налагодження маршрутизатора MikroTik

Оскільки мережа спроектована на рішенні VirtualBox. Функцію комутатора було налагоджено на ОС Linux Alpine.

```
Switch:~# apk add openssh
(1/11) Installing openssh-keygen (9.9_p1-r2)
(2/11) Installing ncurses-terminfo-base (6.5_p20241006-r3)
(3/11) Installing libncursesw (6.5_p20241006-r3)
(4/11) Installing libedit (20240808.3.1-r0)
(5/11) Installing openssh-client-common (9.9_p1-r2)
(6/11) Installing openssh-client-default (9.9_p1-r2)
(7/11) Installing openssh-sftp-server (9.9_p1-r2)
(8/11) Installing openssh-server-common (9.9_p1-r2)
(9/11) Installing openssh-server-common-openrc (9.9_p1-r2)
(10/11) Installing openssh-server (9.9_p1-r2)
(11/11) Installing openssh (9.9_p1-r2)
Executing busybox-1.37.0-r8.trigger
OK: 15 MiB in 36 packages
Switch:~# rc-update add sshd
* service sshd added to runlevel default
Switch:~# service sshd start
* Caching service dependencies ...
ssh-keygen: generating new host keys: RSA ECDSA ED25519
* Starting sshd
```

```
Switch:~# ssh valera1@10.200.200.11
valera1@10.200.200.11's password:
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <https://wiki.alpinelinux.org/>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

Switch:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:e8:e3:24 brd ff:ff:ff:ff:ff:ff
    inet 10.200.200.11/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee8:e324/64 scope link
        valid_lft forever preferred_lft forever
Switch:~$
```

Рисунок 3.3-3.4 – Базове налагодження комутатора

Першим кроком налаштування міжмережевого екрану OPNsense є визначення інтерфейсів: em0 призначається для WAN, а em1 — для LAN. Для кожного з інтерфейсів також задаються відповідні IP-адреси. Підсумок налаштування інтерфейсів наведено на рис.3.5.

```
OPNSense [Работаer] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
| Handbook:  https://docs.opnsense.org/  |  ) ) ) ) ) )  |  ( ( ( ( ( (
| Forums:    https://forum.opnsense.org/  |  |  0000///  |  \\0000
| Code:      https://github.com/opnsense  |  |  0000    |  0000
| Reddit:    https://reddit.com/r/opnsense  |  |  0000000000000000
|-----|-----|-----|
*** OPNsense.localdomain: OPNsense 24.7.11_2 (amd64) ***

LAN (em1)      -> v4: 10.200.200.251/24
OPT1 (em2)     -> v4: 10.0.0.1/24
WAN (em0)      -> v4/DHCP4: 172.18.0.100/24

SSH:  SHA256  +QAgc45m.jk1CEhV4o0ivmGE1QZVXTWqh2hA0eAZD/i0 (ECDSA)
SSH:  SHA256  0Z0dxV5MYBx2tMVdh0DUfebq0WSptieihQGGmUgHoFM (ED25519)
SSH:  SHA256  VT2LFsuHJf0qHC2P2sTHI7Qs9gdXd0Gh+k0QoBZEA6c (RSA)

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 3.5 – Налаштовані параметри інтерфейсів на OPNsense

За допомогою віртуальної машини на ОС Linux, було здійснено вхід за адресою інтерфейсу em0 міжмережевого екрану OPNsense:

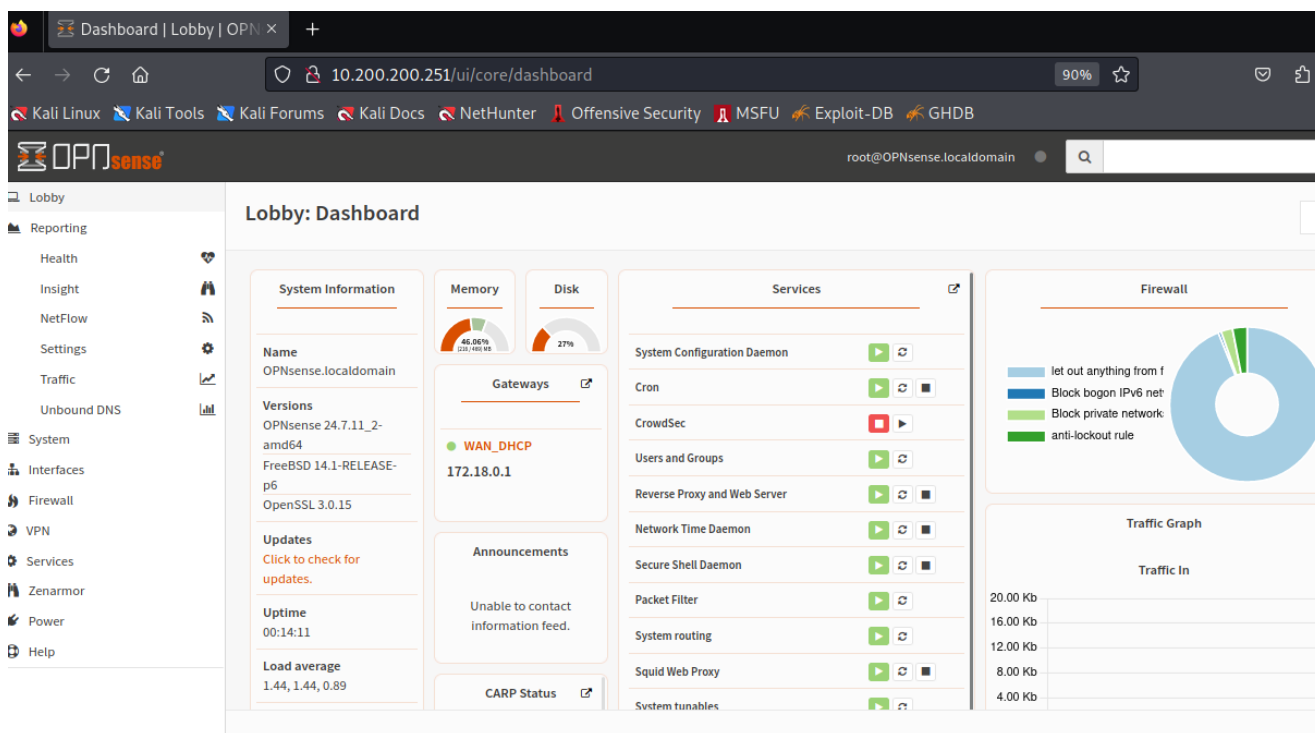


Рисунок 3.6 – Головна сторінка веб-інтерфейсу OPNsense

Базові налагодження OPNsense:

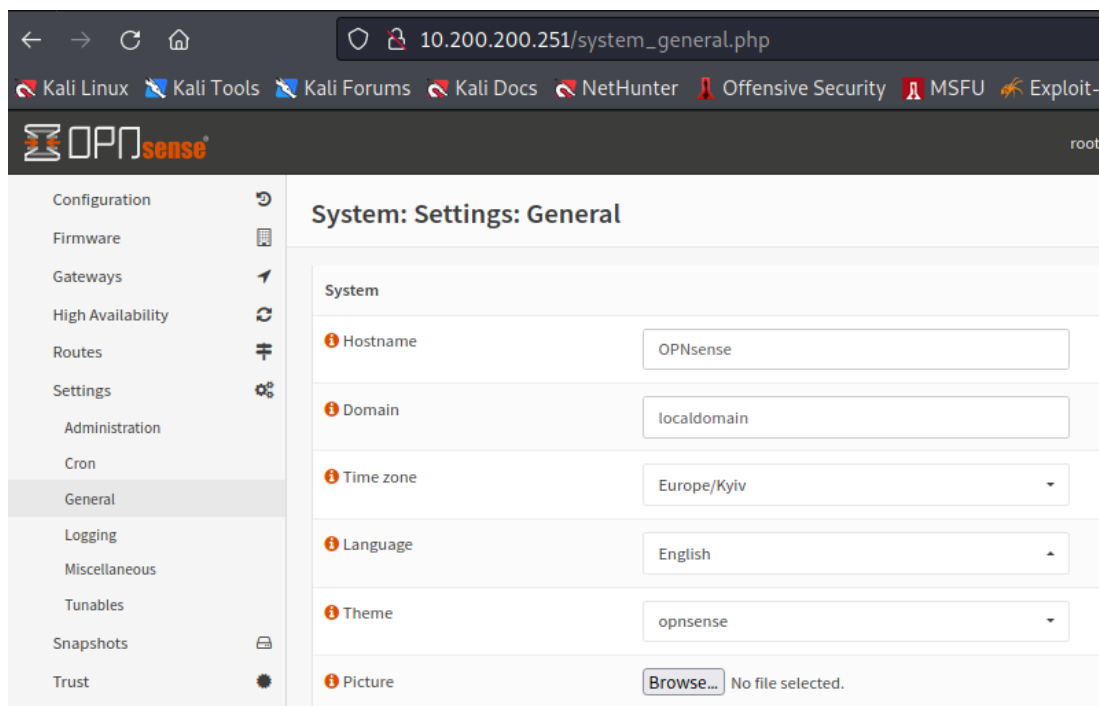


Рисунок 3.7 – Налаштування ім'я пристрою, доменного ім'я та часового поясу на OPNsense

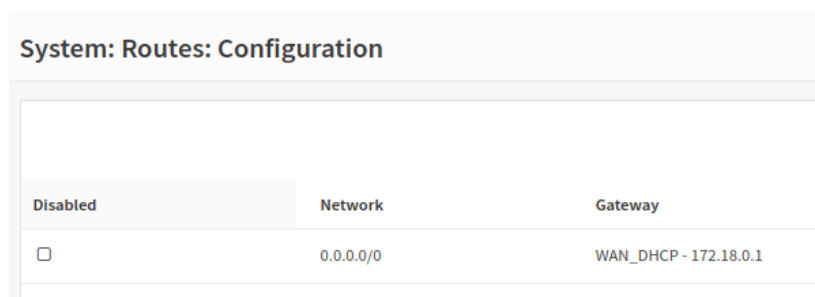


Рисунок 3.8 – Налаштування статичного маршруту за замовчуванням

IIS (Internet Information Services) — це веб-сервер від Microsoft, який використовується для розгортання та управління веб-додатками та веб-сайтами. На Windows Server 2012 IIS є однією з основних ролей, яка дозволяє організувати роботу веб-серверів у корпоративній інфраструктурі.

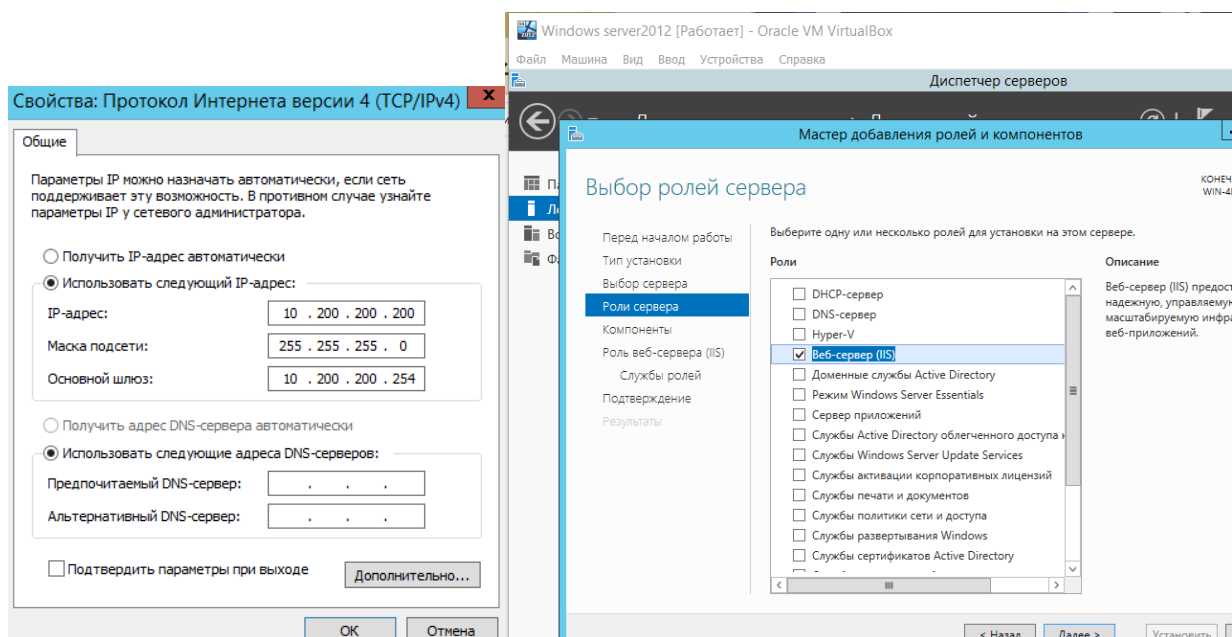


Рисунок 3.9-3.10 – Базове налагодження веб-сервера Windows Server 2012

Забезпечення високої доступності (НА) є критично важливим аспектом для захисту корпоративних мереж, особливо для інфраструктур, де простій системи може спричинити значні фінансові чи репутаційні втрати. Використання технологій Firewall НА дозволяє мінімізувати ризик втрати зв'язку з мережею через відмову одного з вузлів.

Для досягнення високої доступності в OPNsense застосовуються протоколи CARP (Common Address Redundancy Protocol) та pfSync:

- CARP забезпечує резервування IP-адрес, дозволяючи створювати віртуальні IP-адреси, які автоматично перемикаються між вузлами в разі збою.
- pfSync синхронізує правила, стани та налаштування між двома або більше брандмауерами, щоб зберігати їх ідентичність і підтримувати безперервність роботи.

ІТ-інфраструктура налаштована з двома вузлами OPNsense, що працюють у режимі активний-пасивний. Це означає, що один брандмауер виконує функції основного, тоді як другий виступає в ролі резервного. У разі виходу з ладу основного вузла, резервний автоматично перебирає на себе всі мережеві функції, забезпечуючи безперервність роботи.

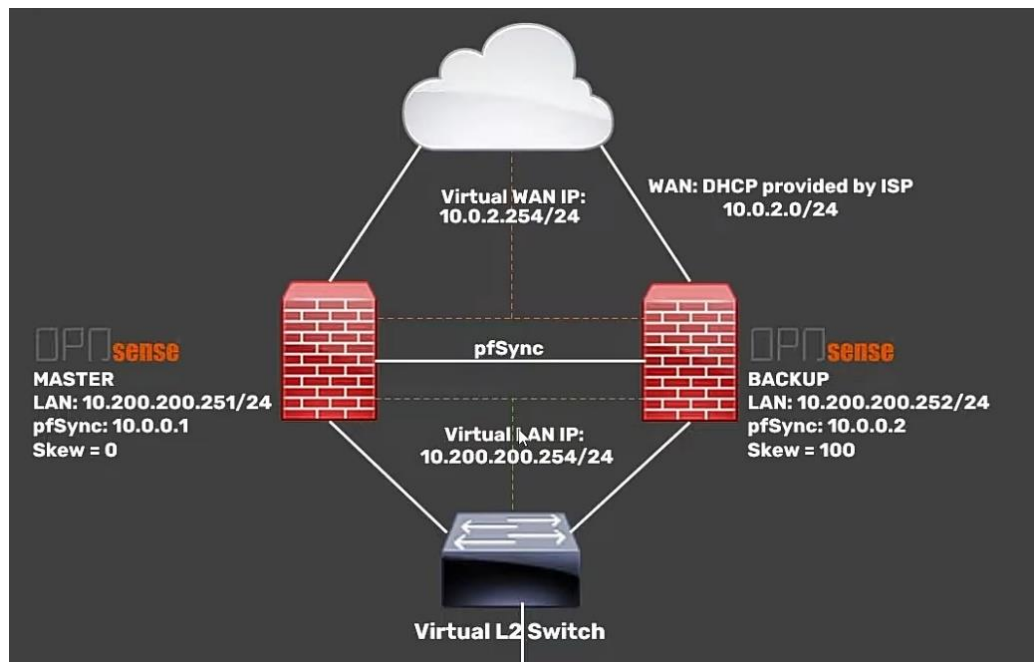


Рисунок 3.11 – Реалізація проєкту підсистеми на базі pfSync в середовищі VirtualBox

На міжмережевих екранах OPNSense було налагоджено IP-адреси інтерфейсу pfSync для синхронізації. На основному IP-адреса 10.0.0.1/24. На резервному 10.0.0.2/24.

```

OPNSense Backup [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
| Handbook:  https://docs.opnsense.org/  |  ) ) ) ) ) ) )  |  ( ( ( ( ( ( (
| Forums:    https://forum.opnsense.org/ |  | 0000///  |  \\0000
| Code:      https://github.com/opnsense |  | 0000    |  0000
| Reddit:    https://reddit.com/r/opnsense |  | 00000000000000000000
|-----|
*** OPNSense.localdomain: OPNSense 24.7.10_2 (amd64) ***

LAN (em1)      -> v4: 10.200.200.252/24
OPT1 (em2)     -> v4: 10.0.0.2/24
WAN (em0)      -> v4/DHCP4: 172.18.0.99/24

SSH:  SHA256 +QAgc4Smjk1CEhV4o0ivmGE1QZVXTWqh2hA0eAZD/i0 (ECDSA)
SSH:  SHA256 0ZDdxV5MYBx2tMVdh0DUfebq0MSptieihQGGmUgHoFM (ED25519)
SSH:  SHA256 VT2LFsuHJf0qHC2P2sTHI7Qs9gdXd0Gh+k0QoBZEA6c (RSA)

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

Enter an option:

```

Рисунок 3.12 – Налаштування резервного фаєрволу OPNSense

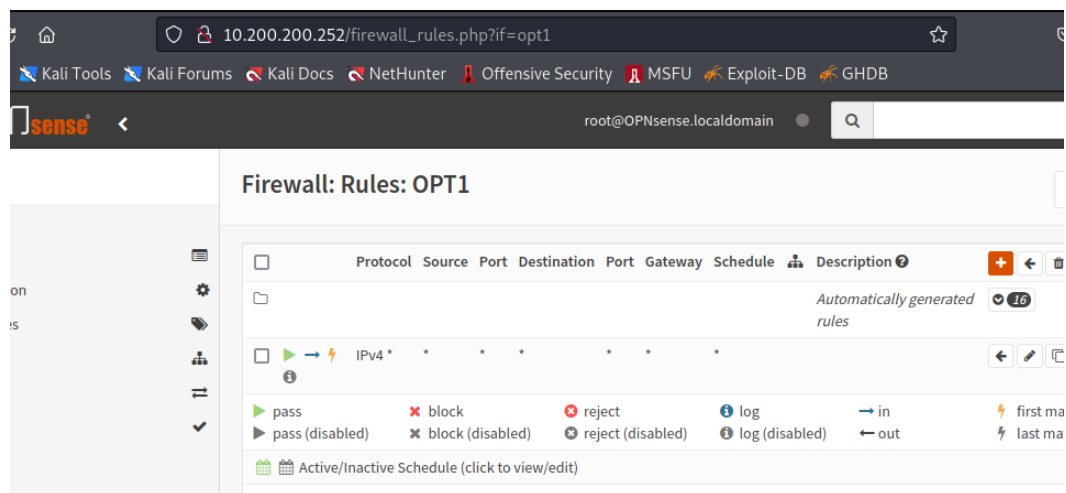


Рисунок 3.13 – Створення правила фаєрволу для інтерфейса pfSense

Віртуальні IP-адреси (Virtual IP, VIP) — це додаткові IP-адреси, які призначаються інтерфейсу для виконання специфічних завдань, таких як балансування навантаження, забезпечення високої доступності (HA) або резервування ресурсів. Вони дозволяють пристроям у мережі використовувати одну "віртуальну" адресу, яка може автоматично перемикається між пристроями у разі збоїв або для розподілу трафіку.

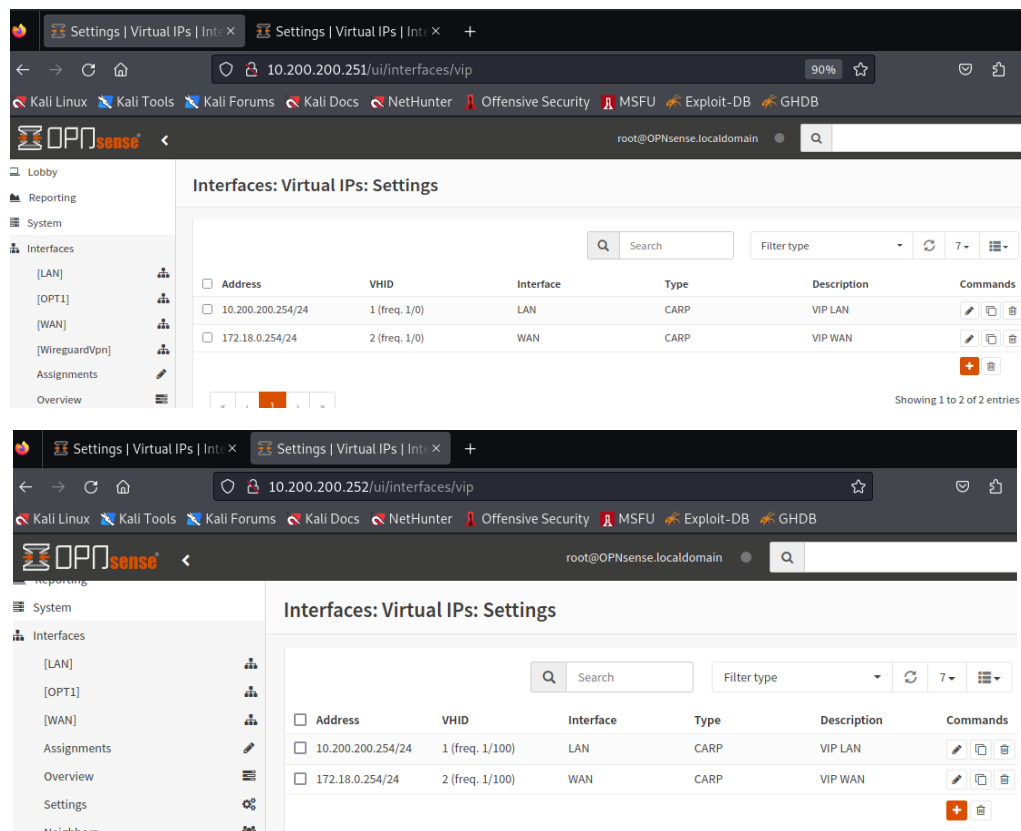


Рисунок 3.14-3.15 – Налаштування Virtual IP

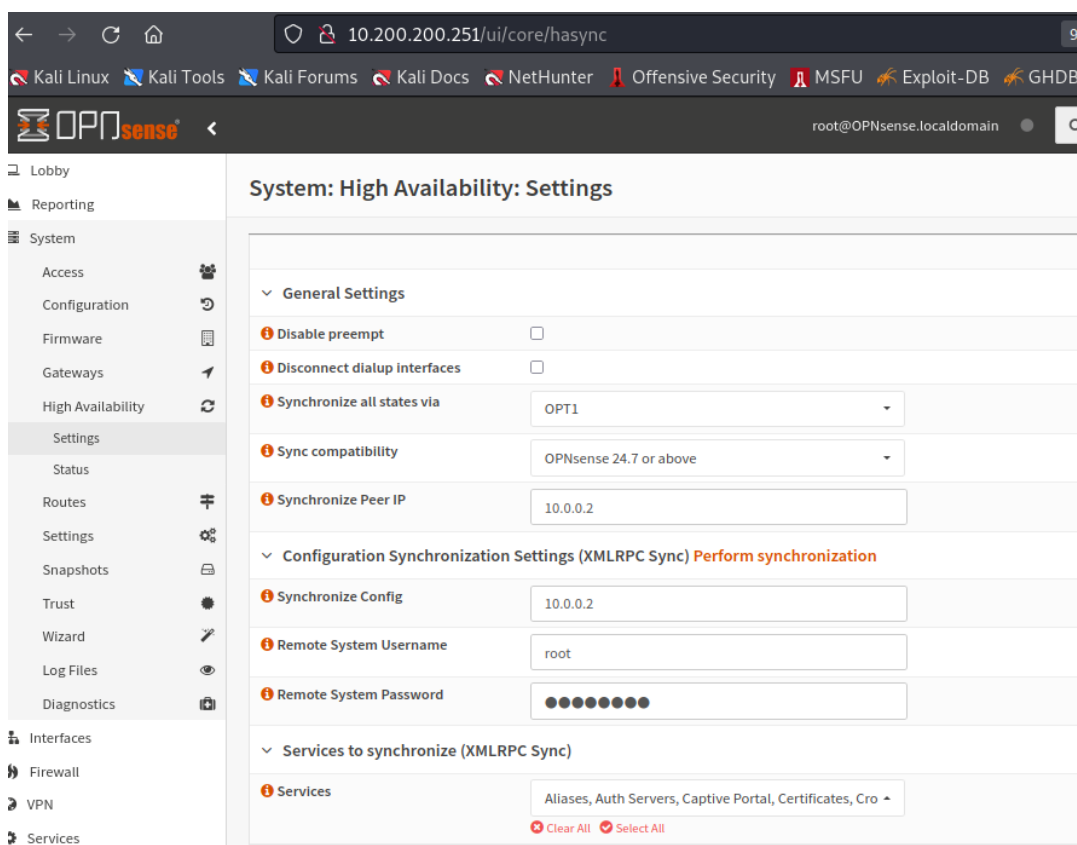


Рисунок 3.16 – Налаштування High Availability

Синхронізація конфігурації налаштовується через XML-RPC. На основному брандмауері вказується IP-адреса резервного брандмауера (pfSync) та облікові дані для синхронізації. На резервному вказується IP-адреса основного брандмауера.

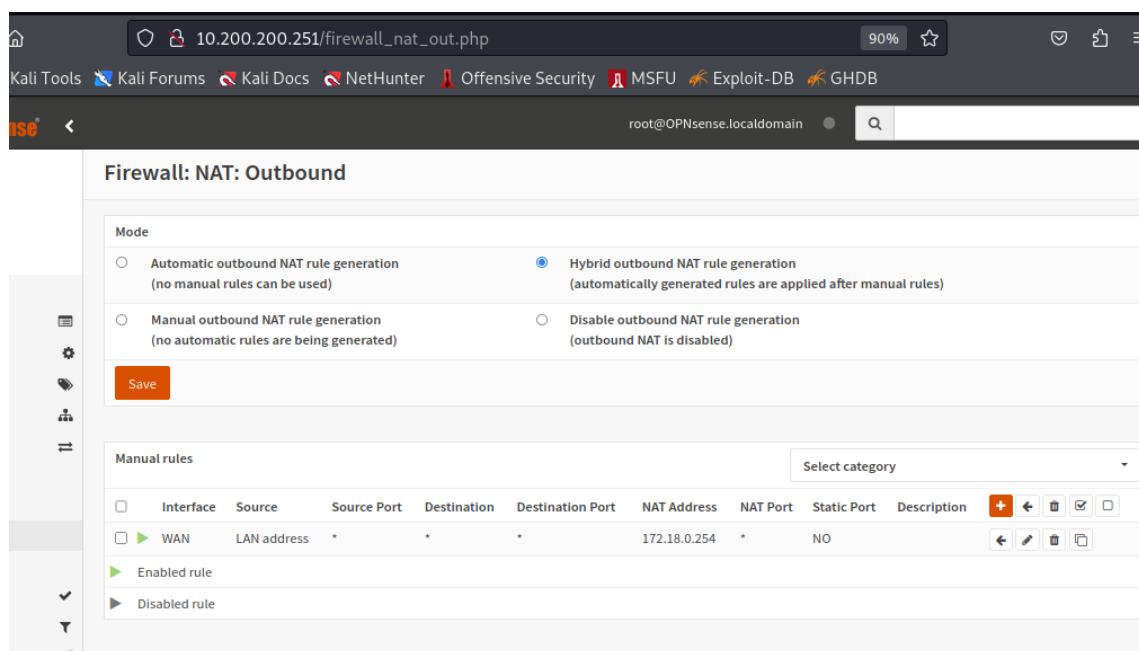


Рисунок 3.17 – Налаштування правила вихідного NAT

3.2 Дослідження параметрів захисту IT-інфраструктури

У сучасних корпоративних мережах безпека займає центральне місце. Зі зростанням кількості кібератак, таких як DDoS, сканування портів і атак на рівні додатків, необхідність виявлення і запобігання вторгненням стала важливою частиною захисту інфраструктури. Для цього все більше організацій використовують системи виявлення та запобігання вторгненням (IDS/IPS).

OPNsense надає безліч функцій для забезпечення безпеки мереж, включаючи вбудовану інтеграцію з IDS/IPS, яку можна налаштувати за допомогою Suricata. Suricata є відкритим програмним забезпеченням для виявлення вторгнень, яке дозволяє створювати власні правила та інтегрувати готові набори правил для забезпечення безпеки мережі.

Для налаштування виявлення вторгнень у вікні Services: Intrusion Detection: Administration необхідно:

- Увімкнути систему виявлення вторгнень (IDS).
- Активувати режим запобігання вторгненням (IPS).
- Увімкнути нерозбірливий режим, що дозволяє детальніше перевіряти трафік.
- Налаштувати сповіщення Syslog для повідомлень про виявлені загрози.
- Метод зіставлення шаблонів – Hyperscan.

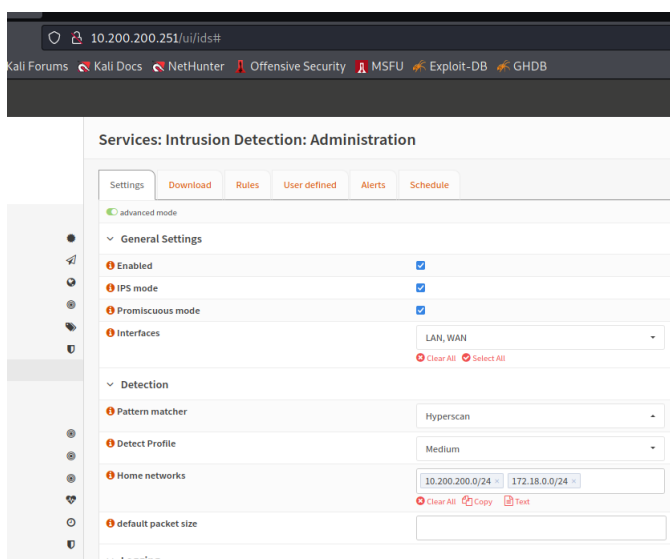


Рисунок 3.18 – Базові налаштування IDPS Suricata

Для кращої безпеки рекомендується завантажити всі запропоновані списки правил:

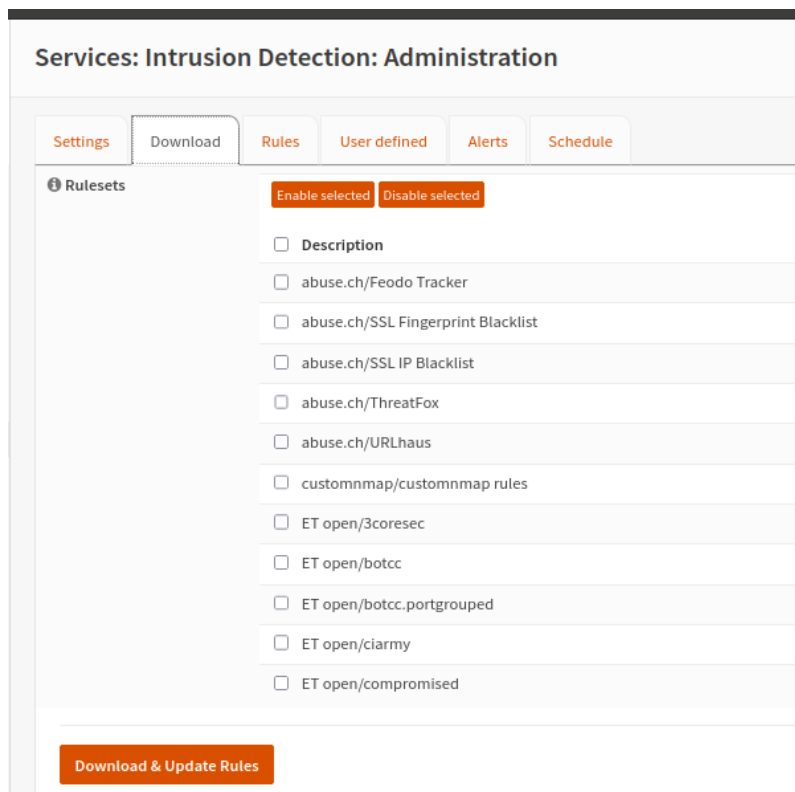


Рисунок 3.19 – Завантаження списків правил

The 'Edit job' window displays the following configuration:

- enabled:** ☒
- Minutes:** 0
- Hours:** 0
- Day of the month:** *
- Months:** *
- Days of the week:** *
- Command:** Update and reload firewall aliases
- Parameters:** (empty field)
- Description:** update and reload firewall aliases

Buttons: Cancel, Save

Рисунок 3.20 – Налаштування розкладу оновлень правил

Services: Intrusion Detection: Administration

Settings Download Rules User defined Alerts Schedule

Filters

Search

☐ sid	Action	Source	ClassType	Message	Info / Enabled
☐ 1234	alert	custommap.rules	attempted-recon	POSSIBLE NMAP SYSNTEALTH SCAN DETECTED	☒
☐ 2000005	alert	emerging-exploit.rules	attempted-dos	ET EXPLOIT Cisco Telnet Buffer Overflow	☐
☐ 2000006	alert	emerging-dos.rules	attempted-dos	ET DOS Cisco Router HTTP DoS	☐
☐ 2000007	alert	emerging-exploit.rules	attempted-dos	ET EXPLOIT Catalyst SSH protocol mismatch	☐
☐ 2000009	alert	emerging-deleted.rules	attempted-dos	ET DELETED Cisco IOS HTTP DoS	☐
☐ 2000010	alert	emerging-dos.rules	attempted-dos	ET DOS Cisco 514 UDP flood DoS	☐
☐ 2000011	alert	emerging-dos.rules	attempted-dos	ET DOS Catalyst memory leak attack	☐
☐ 2000012	alert	emerging-deleted.rules	attempted-dos	ET DELETED Cisco %u IDS evasion	☐
☐ 2000013	alert	emerging-deleted.rules	attempted-dos	ET DELETED Cisco IOS HTTP server DoS	☐
☐ 2000015	alert	emerging-p2p.rules	trojan-activity	ET P2P Phatbot Control Connection	☒

☐ Alert Drop

Showing 1 to 10 of 178855 entries

Рисунок 3.21 – Встановлені правила

Наступним етапом впровадження захисту ІТ-інфраструктури буде фільтрація трафіку, що включає створення правил для дозволу або блокування доступу до різних сегментів мережі.

В сучасних корпоративних мережах важливим аспектом є контроль доступу до інтернет-ресурсів для забезпечення продуктивності працівників, збереження конфіденційної інформації та захисту від небажаного контенту. Прозорий проксі-сервер і веб-фільтрація є ефективними інструментами для досягнення цих цілей. Компанія стикається з проблемою, коли співробітники витрачають робочий час на відвідування соціальних мереж. Для вирішення цього завдання було вирішено налаштувати прозорий проксі-сервер і веб-фільтрацію на основі OPNsense з використанням Squid Cache і SquidGuard.

10.200.200.251/ui/trust/ca

OPNsense

System: Trust: Authorities

Certificates

☐ Description	Issuer	Name	Usages	Valid from	Valid to	Commands
☐ OPNsense-webca	self-signed	/C=UA/ST=ZT/L=Zhytomyr/O=Zhytomyr Polytechnic/OU=ztu/CN=...	0	Dec 17, 2024 4:30 AM	Mar 22, 2027 5:30 AM	☐ ☐ ☐ ☐ ☐

Showing 1 to 1 of 1 entries

Рисунок 3.22 – Створення сертифікату

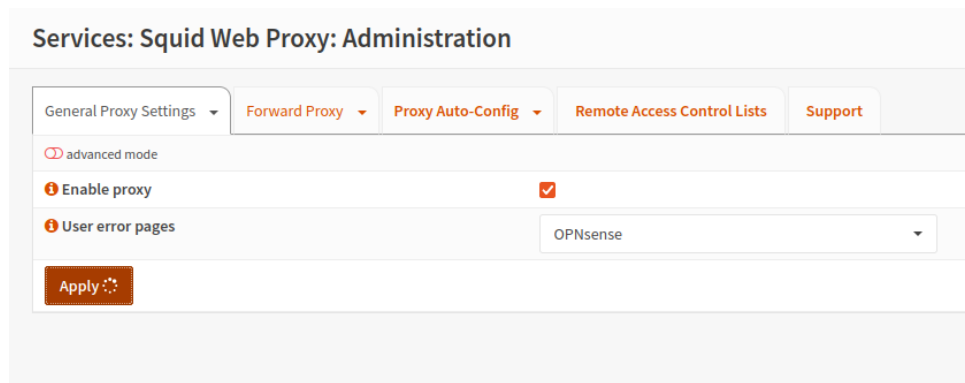


Рисунок 3.23 – Увімкнення служби

Наступним кроком є увімкнення Squid-проксі в OPNsense, активуючи режим прозорого проксі для HTTP, щоб весь HTTP-трафік автоматично проходив через проксі-сервер на порті 3128. Надалі йде правило брандмауера, яке перенаправлятиме весь HTTP-трафік з мережі на локальний проксі-сервер за адресою 127.0.0.1:3128. Після цього налаштуємо активацію SSL-інспекції, увімкнувши SSL-проксі на порту 3129, і вкажемо створений раніше сертифікат центру сертифікації (CA) для розшифрування HTTPS-запитів. Це дозволить аналізувати як HTTP, так і HTTPS-трафік через прозорий проксі.

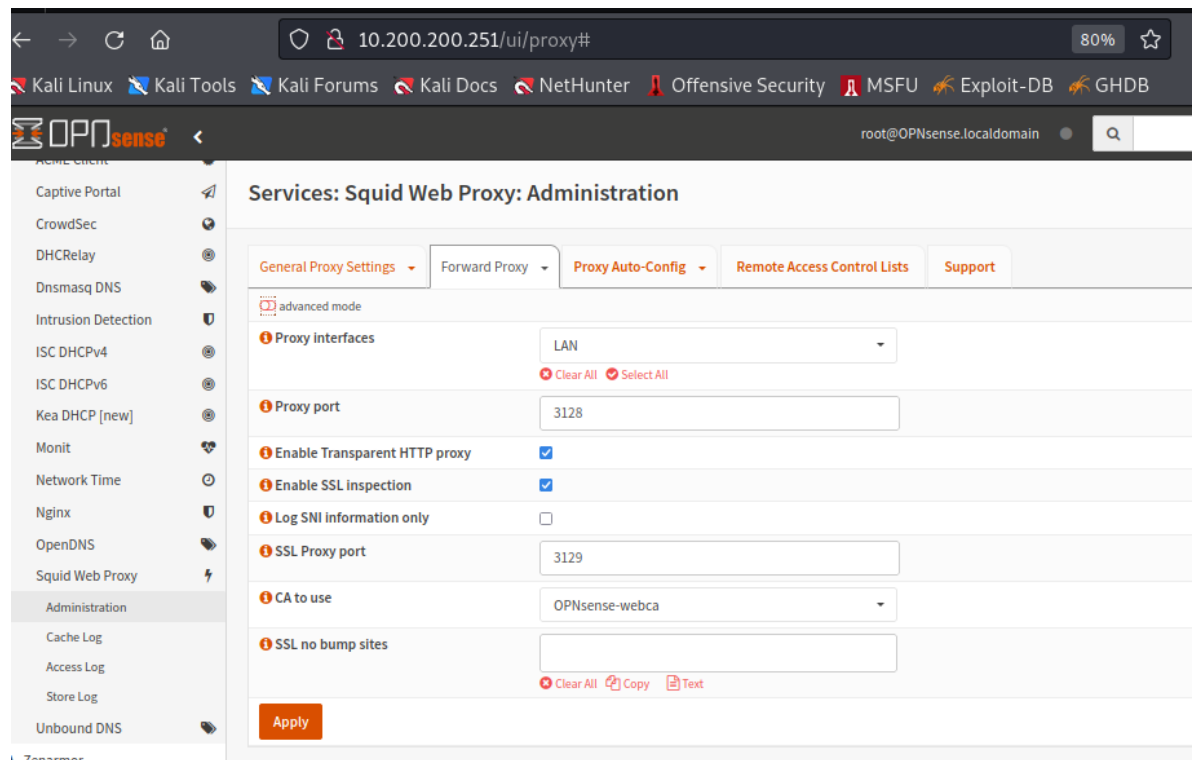


Рисунок 3.24 – Увімкнення служби

Services: Squid Web Proxy: Administration

General Proxy Settings
Forward Proxy
Proxy Auto-Config
Remote Access Control Lists
Support

Authentication method
Nothing selected
Clear All Select All

Enforce local group
Nothing selected
Clear All Select All

Authentication Prompt
OPNsense proxy authentication

Authentication TTL (hours)
2

Authentication processes
5

Apply

Рисунок 3.25 – Squid Web Proxy: Administration

Firewall: Rules: LAN

Select category Inspect

The changes have been applied successfully, remember to update your backup server in System: High availability: status

☐	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	☐	☐	☐	☐
☐	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule	☐	☐	☐	☐
☐	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule	☐	☐	☐	☐
☐	IPv4 TCP	LAN net	*	127.0.0.1	3128	*	*	redirect traffic to proxy	☐	☐	☐	☐
☐	IPv4 TCP/UDP	LAN net	*	*	80 (HTTP)	*	*	block http bypass	☐	☐	☐	☐
☐	IPv4 TCP/UDP	LAN net	*	*	443 (HTTPS)	*	*	block https bypass	☐	☐	☐	☐
☐	pass	☒ block	☒ reject	☒ log	☒ in	☒ first match						
☐	pass (disabled)	☒ block (disabled)	☒ reject (disabled)	☒ log (disabled)	☒ out	☒ last match						

Active/Inactive Schedule (click to view/edit)
Alias (click to view/edit)

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

Рисунок 3.26 – Налаштовані правила фаєрвола для інтерфейсу LAN

Надалі, було завантажено чорний список сайтів, які пропонує Université Toulouse. Серед категорій було обрано соціальні мережі:

Edit blacklist

full help

enabled
☒

Filename
UT1

URL
ftp://ftp.ut-capitole.fr/blacklist/blacklists.tar.gz

username (optional)

password (optional)

categories (if available)
social_networks
Clear All Select All

ssl ignore cert
☐

Description
UT1 web filter

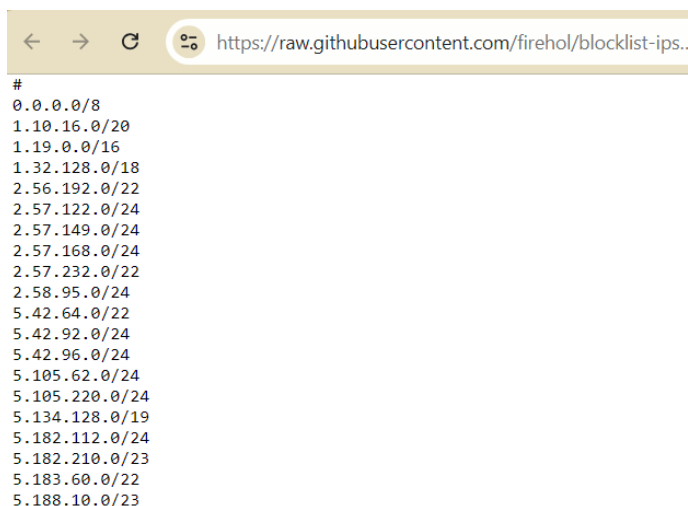
Cancel Save

Рисунок 3.27 – Налаштування чорного списку

Ще один спосіб блокування небажаного контенту є блок-листи від Firehole.

Мета полягає в тому, щоб створити чорний список, який може бути достатньо безпечним для використання в усіх системах, з брандмауером, щоб повністю блокувати доступ з і до його перерахованих IP-адрес.

Ключовою передумовою для цієї причини є відсутність помилкових спрацювань. Усі перелічені IP-адреси мають бути поганими та мають бути заблоковані без винятків. [14]



https://raw.githubusercontent.com/firehol/blocklist-ipsets

```
#
0.0.0.0/8
1.10.16.0/20
1.19.0.0/16
1.32.128.0/18
2.56.192.0/22
2.57.122.0/24
2.57.149.0/24
2.57.168.0/24
2.57.232.0/22
2.58.95.0/24
5.42.64.0/22
5.42.92.0/24
5.42.96.0/24
5.105.62.0/24
5.105.220.0/24
5.134.128.0/19
5.182.112.0/24
5.182.210.0/23
5.183.60.0/22
5.188.10.0/23
```

Рисунок 3.28 – IP-адреси, які варто заблокувати

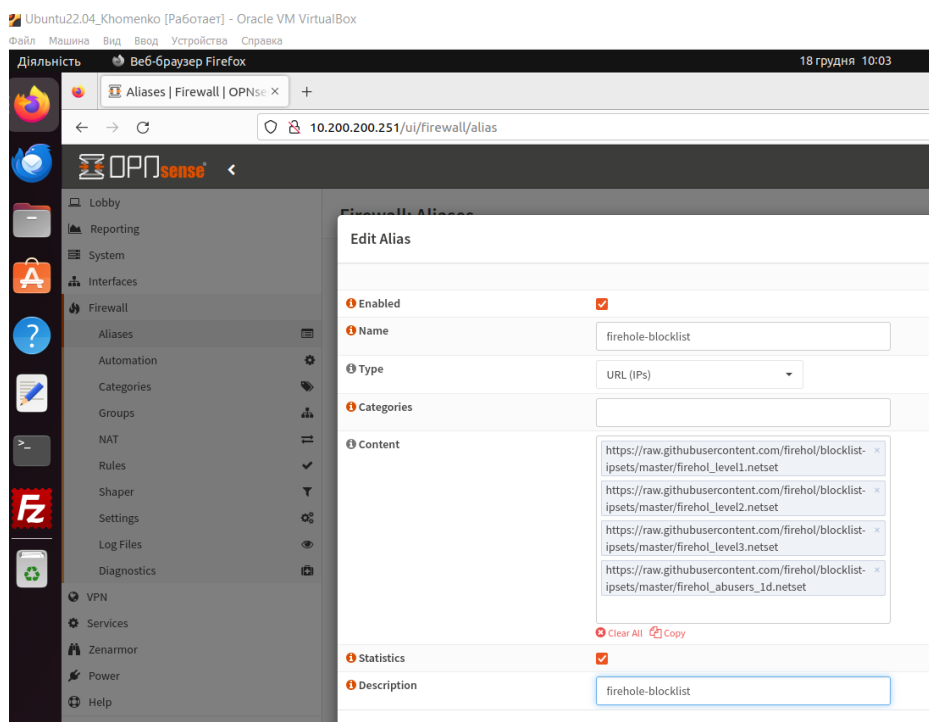


Рисунок 3.29 – Завантаження блоклистів з репозиторія

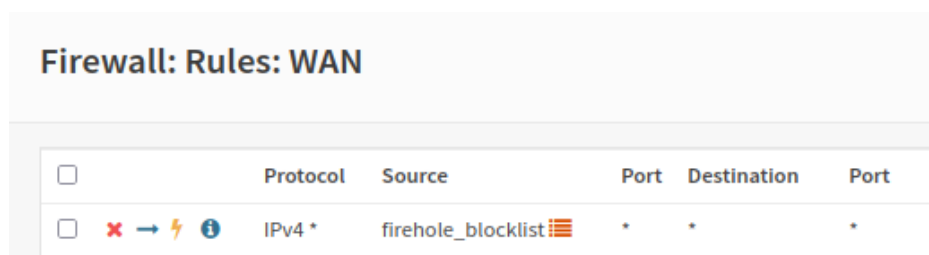


Рисунок 3.30 – Створення правила

Unbound DNS — це високопродуктивний та безпечний сервер DNS, який за замовчуванням вбудований в OPNsense і використовуються для надання DNS-послуг, таких як розв’язування доменних імен та кешування DNS-запитів.

Щоб захистити мережу від розпізнавання DNS-запитів та зменшити шанси на атаки через DNS, можна використовувати функцію DNS-over-HTTPS або DNS-over-TLS.

Quad9 - DNS резолвер, який можна використовувати як альтернативу DNS від Google або OpenDNS. Це проект Global Cyber Alliance, який створений навіть для того, щоб забезпечити додаткову безпеку користувачів, за рахунок блокування на рівні DNS запитів до проблемних доменів.

Quad9 включає також два списки — білий список, і список однозначно хороших доменів.

Білий список формується з Majestic Million проекту, що публікує найпопулярніші доменні імена, з якими користувачі працюють щодня. Список хороших доменів - це лістинг, що складається з ресурсів великих і популярних компаній (AWS, Google, Microsoft Azure), які не блокуватимуться Quad9. [13]

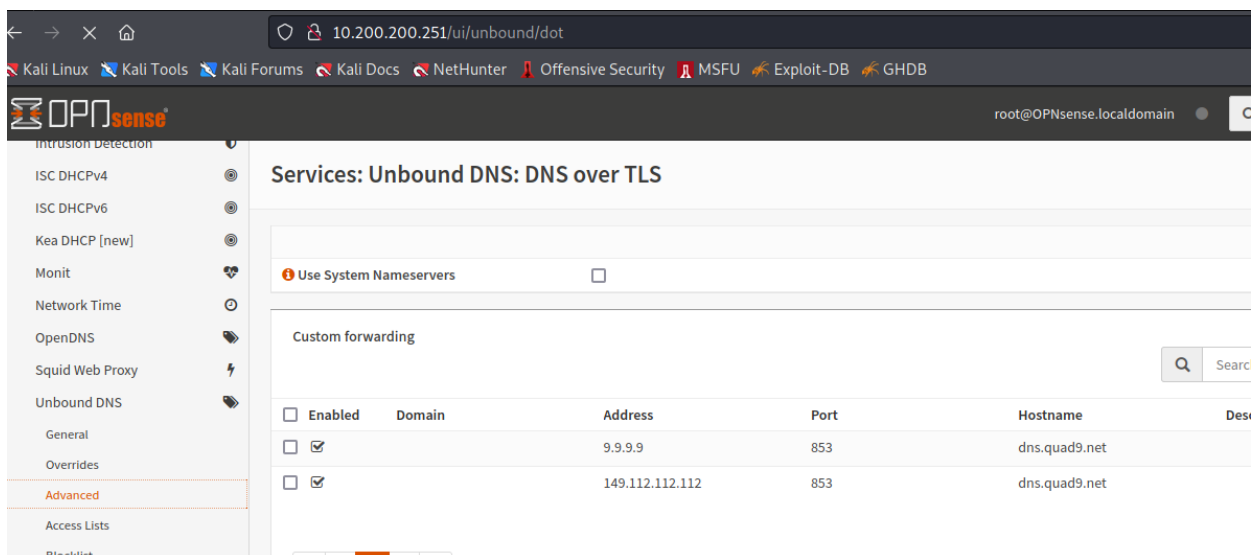


Рисунок 3.31 – Налаштування Unbound DNS

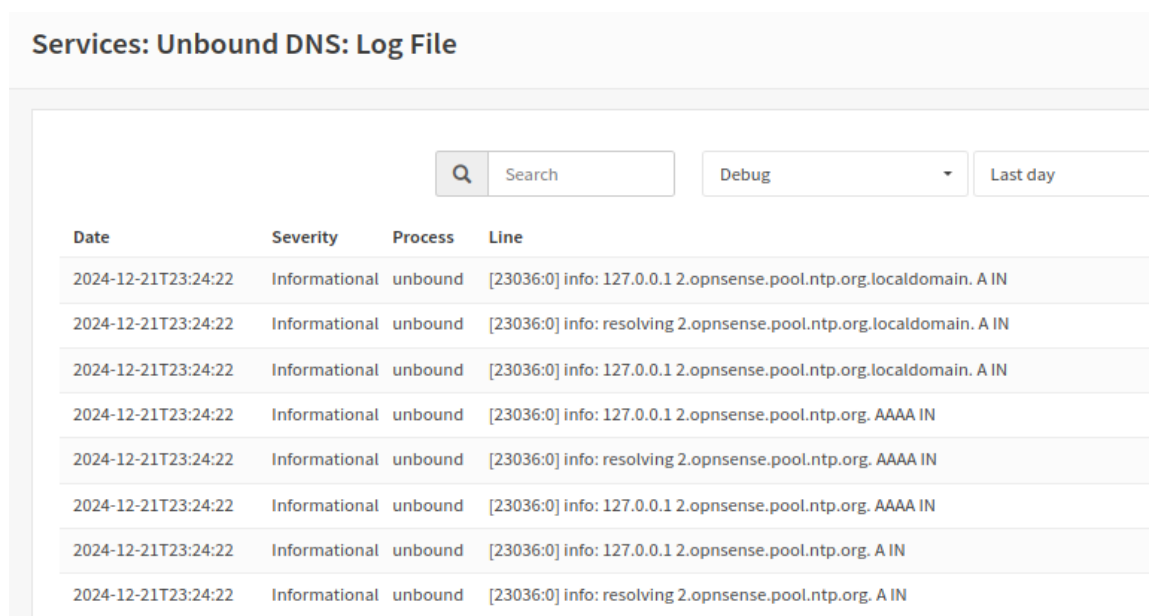


Рисунок 3.32 – Unbound DNS: Log File

Split DNS (іноді також зветься «Split-Horizon DNS») — це конфігурація DNS, яка дозволяє налаштувати різні DNS-результати для однакових доменів залежно від того, з якого мережевого інтерфейсу здійснюється запит. Це зазвичай використовується для розділення внутрішнього та зовнішнього доступу до ресурсів.

В контексті OPNsense і Unbound DNS, Split DNS може бути корисним для забезпечення доступу до різних ресурсів як для користувачів всередині мережі, так і для користувачів зовні. Наприклад, внутрішні користувачі можуть отримувати внутрішні IP-адреси для певних сервісів, тоді як зовнішні користувачі — зовнішні.

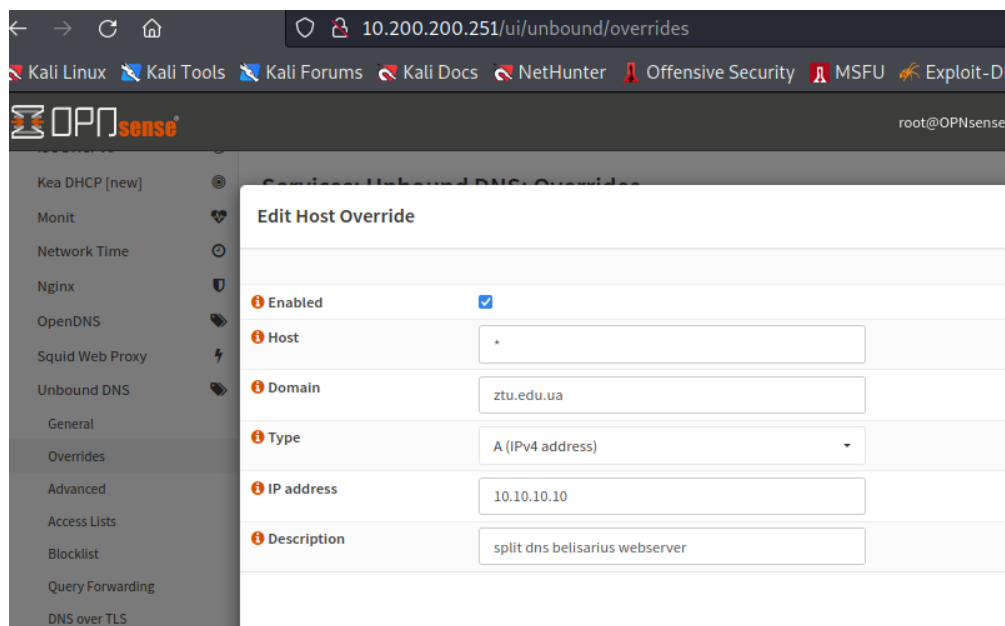


Рисунок 3.33 – Налаштування Split DNS

Блокування реклами через Unbound DNS Blocklist в OPNsense — це потужний спосіб фільтрації непотрібного або шкідливого контенту на рівні DNS. Це дозволяє значно покращити безпеку та продуктивність вашої мережі, а також зменшити кількість небажаних рекламних запитів.

OPNsense надає великий вибір обрати, що саме адміністратор хоче заблокувати в мережі:

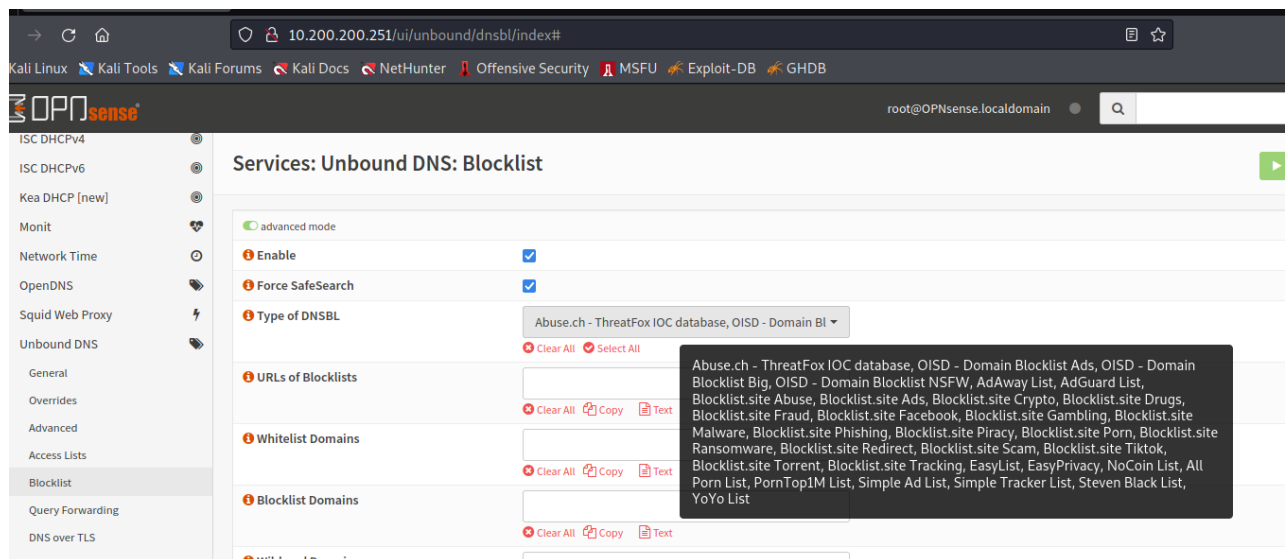


Рисунок 3.34 – Unbound DNS Blocklist

CrowdSec — це сучасна система для виявлення та блокування шкідливого трафіку та атак на основі спільного обміну інформацією між користувачами (community-driven threat intelligence). Вона використовує аналіз поведінки трафіку для виявлення підозрілих активностей, таких як brute-force атаки, DDoS, сканування портів та інші види атак. CrowdSec може працювати як IDS/IPS, фільтруючи трафік і автоматично блокуючи шкідливі IP-адреси. [20]

В OPNsense CrowdSec можна інтегрувати для посилення безпеки мережі шляхом автоматичного реагування на загрози. Це дозволяє швидко блокувати шкідливі джерела атак за допомогою різних методів (IP-блокування, брандмауерні правила, тощо).

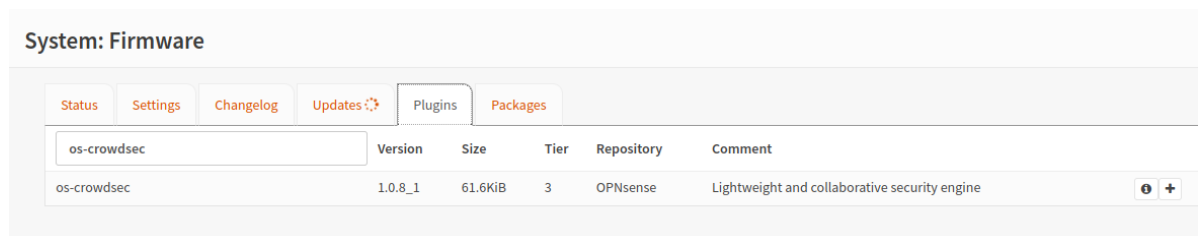


Рисунок 3.35 – Встановлення плагіну CrowdSec в OPNsense

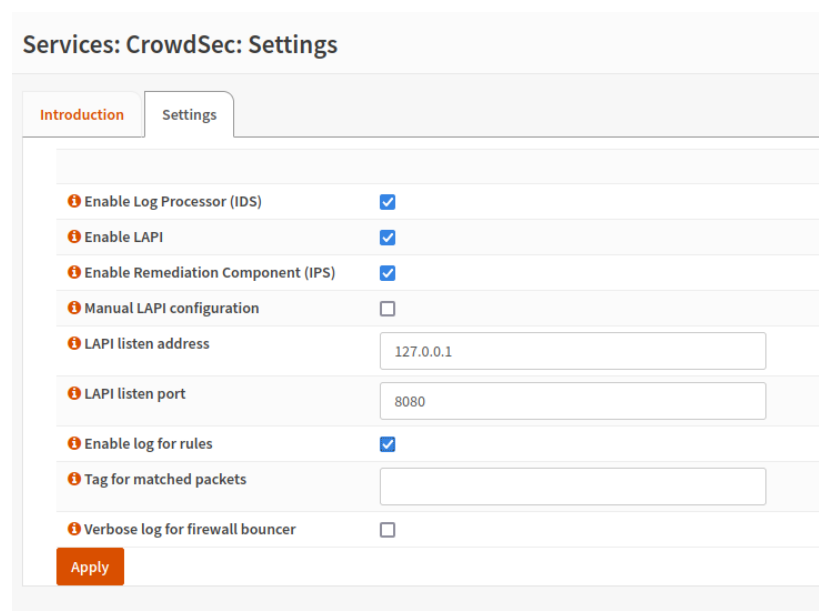


Рисунок 3.36 – Налаштування CrowdSec

Після увімкнення служби Crowdsec, було згенеровано безліч правил для фільтрації трафіку:

Status	Settings	Changelog	Updates 	Plugins	Packages			
sunny				Version	Size	Tier	Repository	Comment
os-sunnyvalley (installed)				1.4_3	2.44KiB	3	OPNsense	Vendor Repository for Zenarmor (a.k.a Sensei, Next Generation Firewall Extensions)
os-sensei				1.18.4	207MiB	3	SunnyValley	Next Generation Firewall Extensions for OPNsense (ZENARMOR)
os-sensei-agent				1.18.4	112MiB	3	SunnyValley	ZENARMOR (Sensei) Connectivity Agent for Cloud Central Management
os-sensei-updater				1.17	4.08KiB	3	SunnyValley	OPNsense ZENARMOR Plugin Updater

1 Welcome

2 Database Settings

3 Interface Settings

4 Subscription

☒ Install a local MongoDB Database
 ☐ Use a Remote Elasticsearch Database
 ☐ Use a local SQLite Database (Support up to 100 devices)

Low-end Hardware
 We have detected a low-end hardware. No worries, zenarmor will offer an optimum configuration for you.

CPU Model: Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz
 CPU Score: 239015
 Physical Memory Size: 2.0 GB

Previous

Install Database

Рисунок 3.39-3.40 – Завантаження Zenarmor

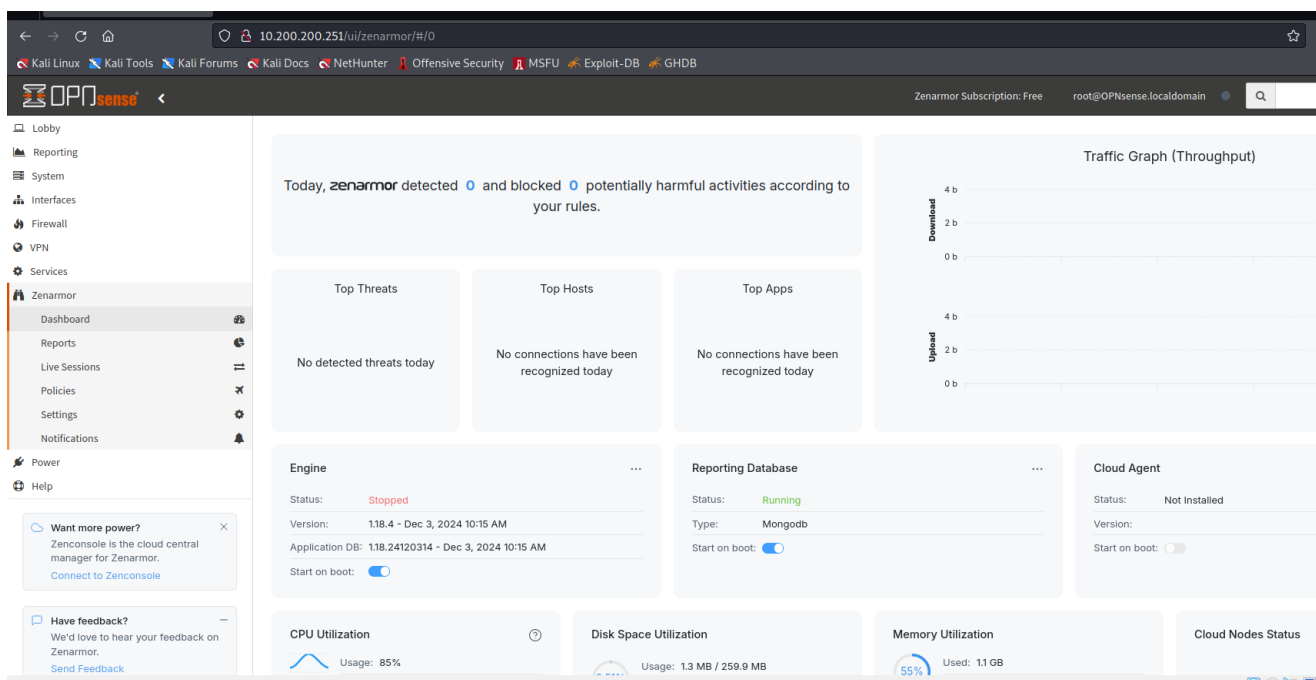


Рисунок 3.41 – Головний екран Zenarmor

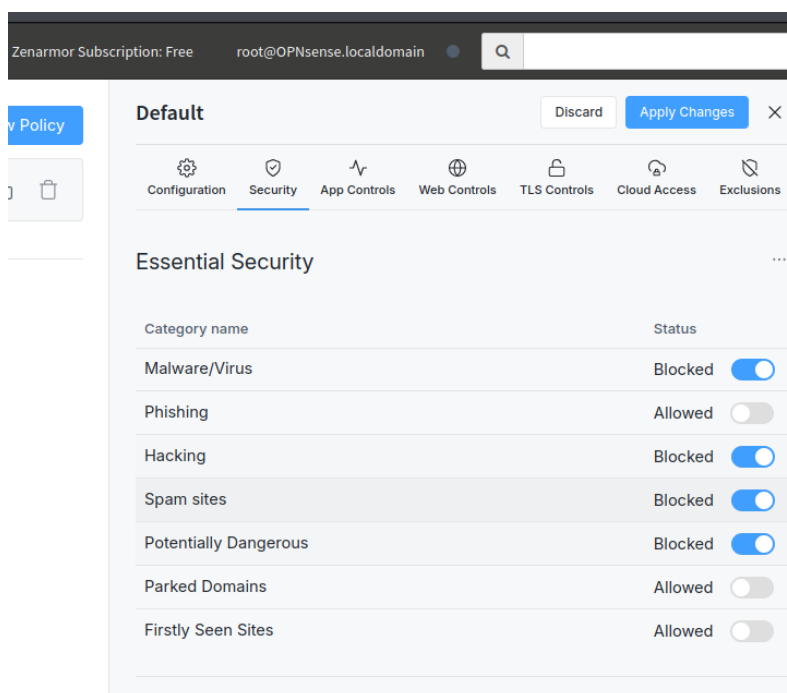


Рисунок 3.42 – Встановлення функцій для безпеки мережі

3.3 Тестування роботи підсистеми захисту та аналіз ефективності

Тестування підсистеми захисту є важливою складовою частиною забезпечення надійної безпеки інформаційних систем. Завдяки систематичному тестуванню можна оцінити, наскільки ефективно працюють засоби захисту, і виявити потенційні вразливості, які можуть бути використані зловмисниками. Оскільки кіберзагрози постійно змінюються та еволюціонують, регулярне тестування підсистем захисту необхідне для того, щоб адаптувати їх до нових видів атак і викликів.

Враховуючи важливість тестування засобів безпеки, аналіз їх ефективності має на меті визначити, чи відповідають вони вимогам до безпеки та наскільки добре вони здатні захистити інформаційні ресурси від атак. Одним з ключових етапів тестування є перевірка роботи засобів виявлення та блокування атак, таких як системи IDS/IPS, брандмауери, фільтри трафіку та інші компоненти підсистеми захисту.

Одним із ресурсів для глибокого аналізу вразливостей систем є платформи, такі як CVEDetails [15]



Рисунок 3.43 – Статистика вразливостей OPNSense

Перевірка роботи High Availability.

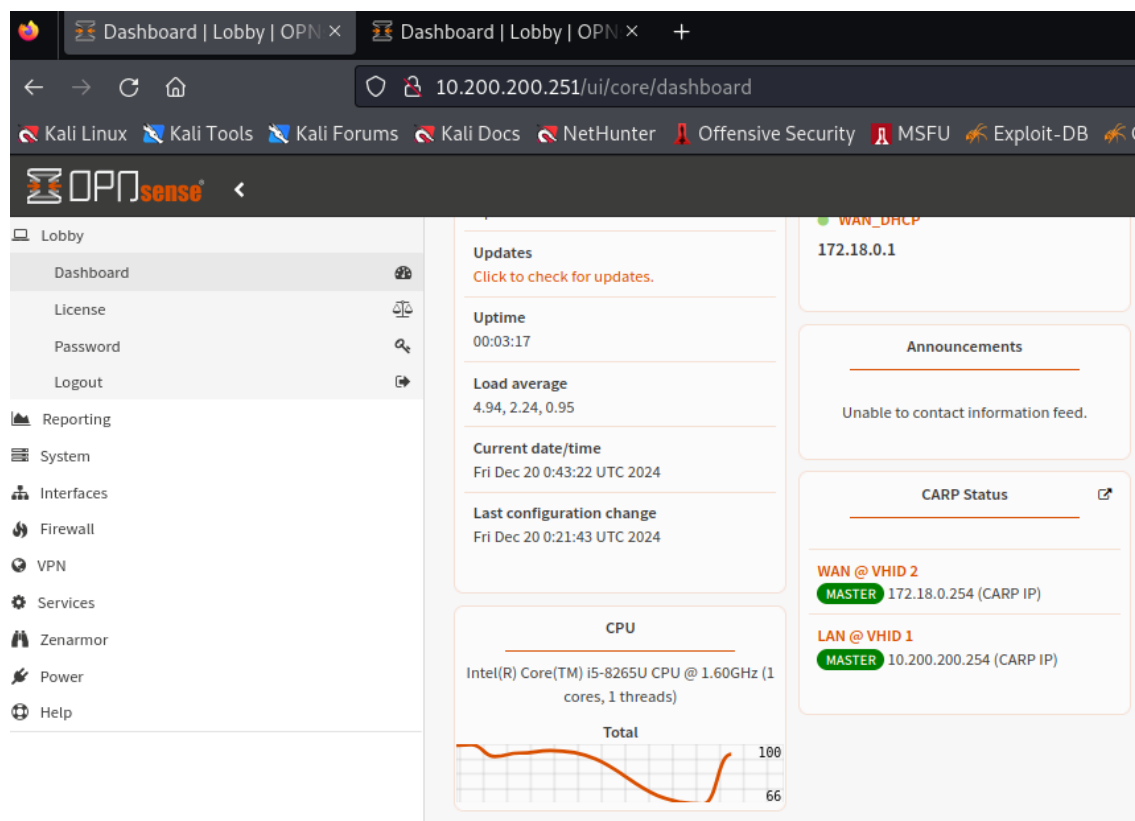


Рисунок 3.44 – Стан CARP у основного брандмауера OPNSense

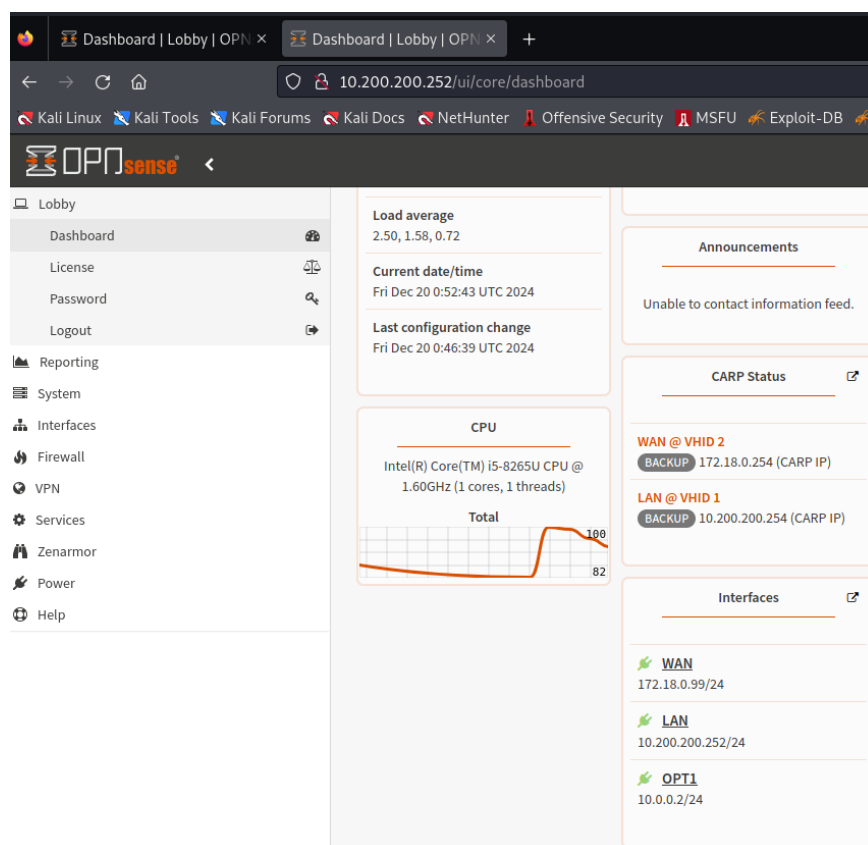


Рисунок 3.45 – Стан CARP у резервного брандмауера OPNSense

Після вимкнення основного OPNSense. Резервний став головним:

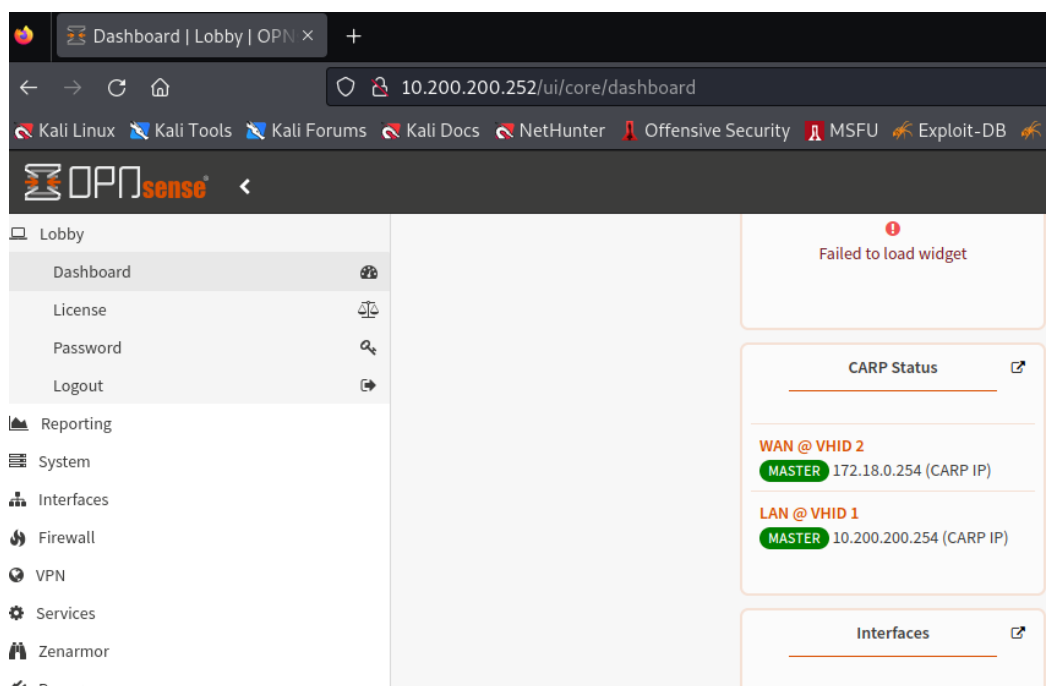


Рисунок 3.46 – Стан CARP у резервного брандмауера OPNSense після вимкнення з мережі основного

Для перевірки роботи фільтрації трафіку (Squid Web Proxy), перейдемо на сторінку Facebook. Як можна побачити на рисунку 3.60, брандмауер заблокував доступ до сайту:

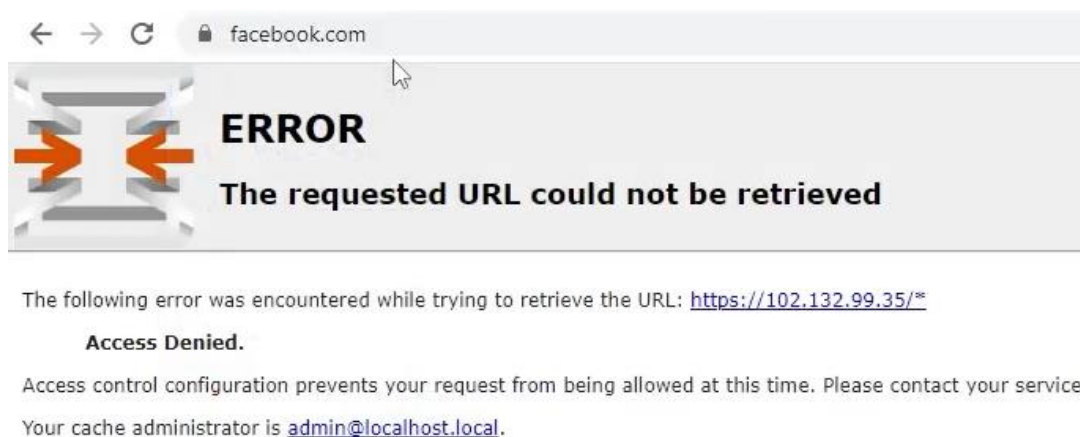


Рисунок 3.47 – Блокування фаєрволом OPNSense

Наступним етапом. Буде перевірка IDS/IPS системи. Для цього на сервер буде завантажено правило customnmap:

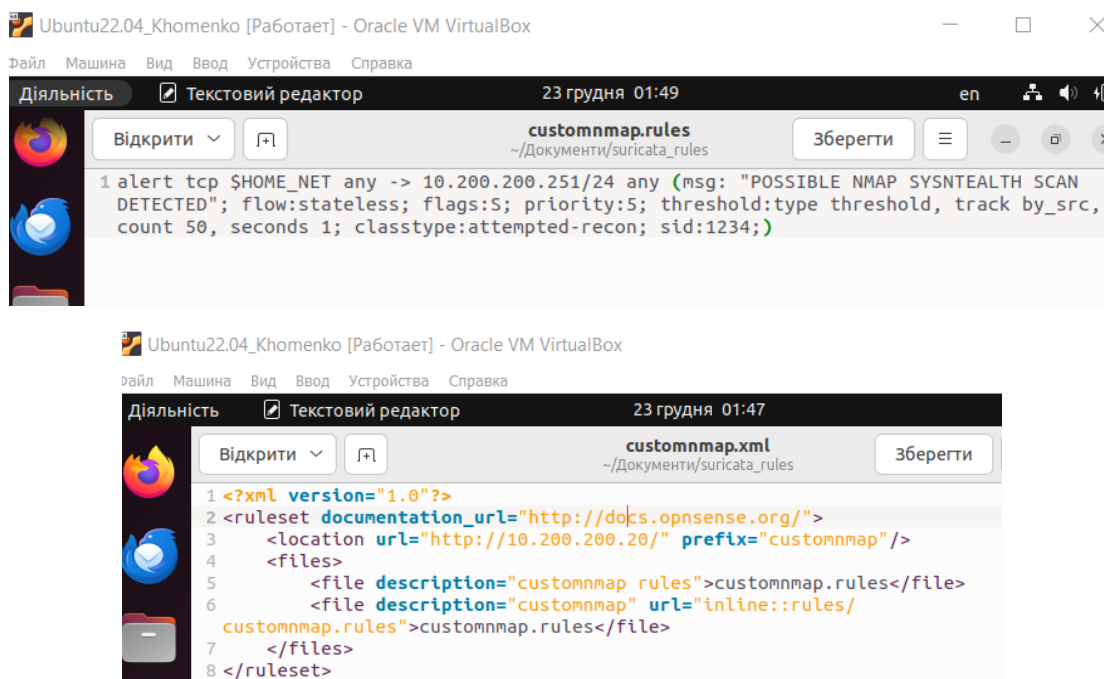


Рисунок 3.48-3.49 –Файли customnmap.rules та customnmap.xml

За допомогою FileZilla, було завантажено файл з правилами на файловий сервер OPNSense:

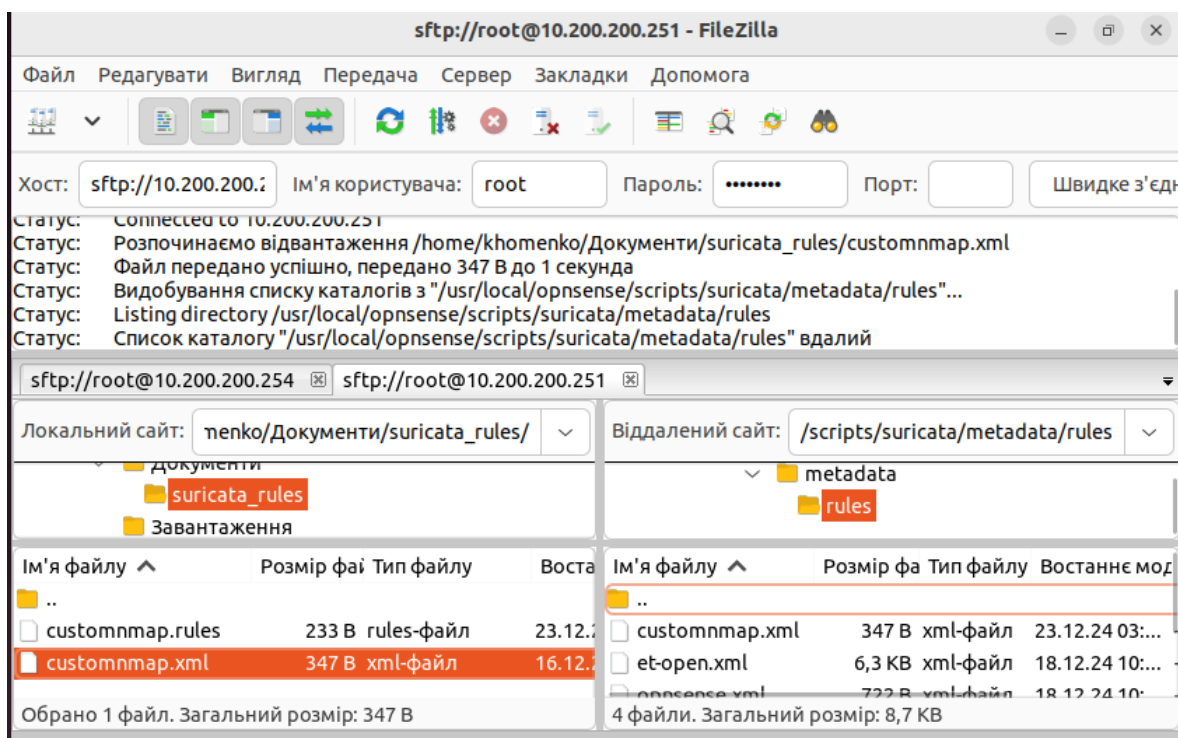


Рисунок 3.50 – FileZilla

Як можна побачити на рис. 3.51, правило custommap.rules тепер можна завантажувати на Suricata:

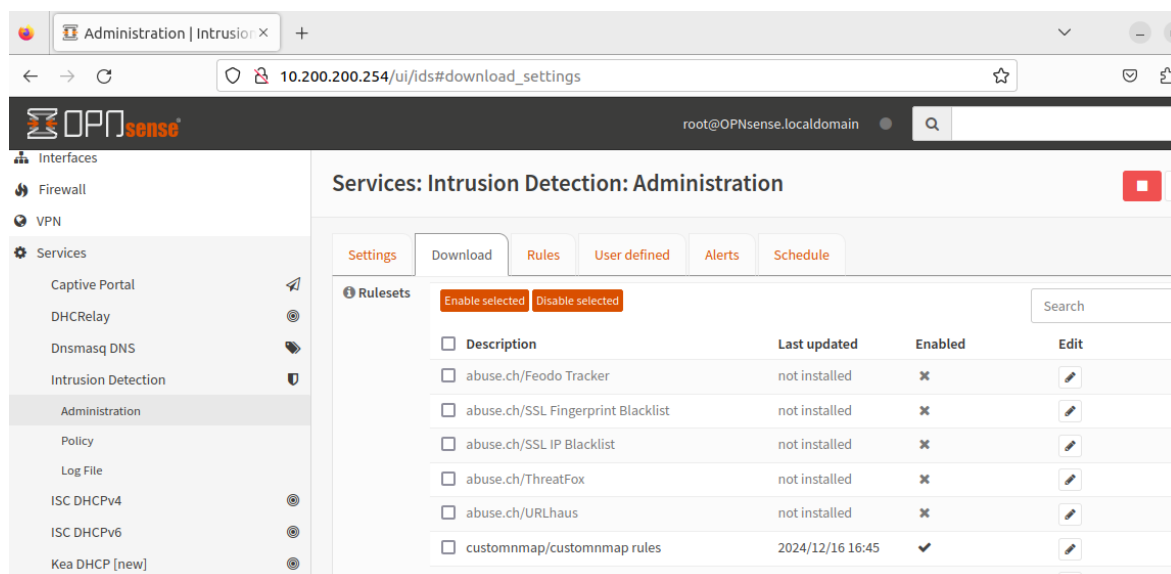


Рисунок 3.51 – Списки правил, що доступні для завантаження

Nmap (Network Mapper) — це потужний інструмент з відкритим кодом, призначений для дослідження мереж і аудиту безпеки. Він надає різноманітні методи сканування для виявлення мережевих хостів, служб і відкритих портів. Одним із

таких методів є сканування АСК (Acknowledgement), яке дозволяє здійснювати детальніший аналіз безпеки мережі.

Сканування АСК є специфічною формою TCP-сканування, при якому замість завершення стандартного встановлення TCP-з'єднання, як у випадку звичайного сканування, відправляються пакети з прапорцем АСК на цільову систему, і аналізуються отримані відповіді. Основною метою цього методу є визначення правил фільтрації трафіку та налаштувань брандмауера в цільовій мережі. [19]

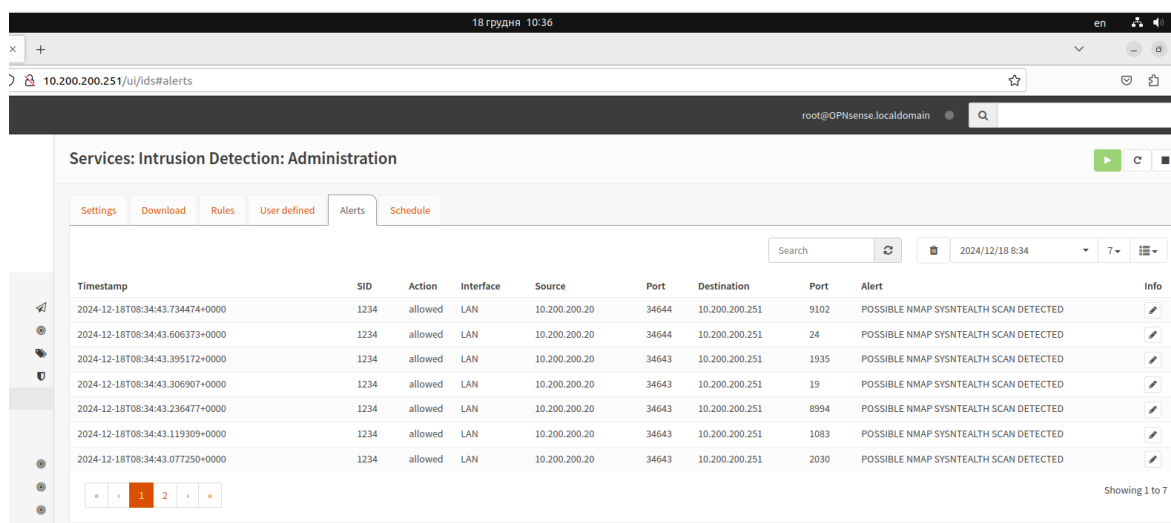
```
khomenko@virtualbox:~$ sudo nmap -sS 500 10.200.200.251
Starting Nmap 7.80 ( https://nmap.org ) at 2024-12-18 10:15 EET
Nmap scan report for 500 (0.0.1.244)
Host is up (0.0012s latency).
All 1000 scanned ports on 500 (0.0.1.244) are filtered

Nmap scan report for 10.200.200.251
Host is up (0.0070s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 08:00:27:ED:38:1D (Oracle VirtualBox virtual NIC)

Nmap done: 2 IP addresses (2 hosts up) scanned in 21.01 seconds
khomenko@virtualbox:~$
```

Рисунок 3.52 – Перевірка АСК сканування на інтерфейсі OPNSense на протоколі TCP

В результаті сканування, OPNSense залогував потенціне сканування АСК сервоміном nmap:



The screenshot shows the OPNSense web interface with the 'Alerts' tab selected. A table lists several alerts detected on 2024-12-18 at 18:08. Each alert is categorized as 'POSSIBLE NMAP SYSNHEALTH SCAN DETECTED' and shows details like the source IP (10.200.200.20), destination IP (10.200.200.251), and the specific port scanned.

Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert	Info
2024-12-18T08:34:43.734474+0000	1234	allowed	LAN	10.200.200.20	34644	10.200.200.251	9102	POSSIBLE NMAP SYSNHEALTH SCAN DETECTED	
2024-12-18T08:34:43.606373+0000	1234	allowed	LAN	10.200.200.20	34644	10.200.200.251	24	POSSIBLE NMAP SYSNHEALTH SCAN DETECTED	
2024-12-18T08:34:43.395172+0000	1234	allowed	LAN	10.200.200.20	34643	10.200.200.251	1935	POSSIBLE NMAP SYSNHEALTH SCAN DETECTED	
2024-12-18T08:34:43.306907+0000	1234	allowed	LAN	10.200.200.20	34643	10.200.200.251	19	POSSIBLE NMAP SYSNHEALTH SCAN DETECTED	
2024-12-18T08:34:43.236477+0000	1234	allowed	LAN	10.200.200.20	34643	10.200.200.251	8994	POSSIBLE NMAP SYSNHEALTH SCAN DETECTED	
2024-12-18T08:34:43.119309+0000	1234	allowed	LAN	10.200.200.20	34643	10.200.200.251	1083	POSSIBLE NMAP SYSNHEALTH SCAN DETECTED	
2024-12-18T08:34:43.077250+0000	1234	allowed	LAN	10.200.200.20	34643	10.200.200.251	2030	POSSIBLE NMAP SYSNHEALTH SCAN DETECTED	

Рисунок 3.53 – Possible Nmap sysnhealth scan detected

Rule details	
Signature Id	1234
Revision	
Message	POSSIBLE NMAP SYSNTEALTH SCAN DETECTED
classtype	attempted-recon
source	customnmap.rules
status	enabled
Action	Alert

Рисунок 3.54 – Possible Nmap sysntealth scan detected

Тестування плагіну Crowdsec. Crowdsec можна використовувати як блокування трафіку атаки від входу в мережу.

```
root@OPNsense:~ # cscli decision add -t ban -d 2m -i 10.200.200.90
INFO Decision successfully added
root@OPNsense:~ #
```

Services: CrowdSec: Overview		
Service status: crowdsec ✓ - firewall bouncer ✓		
Machines	Bouncers	Collections
Scenarios	Parsers	Postoverflows
Alerts	Decisions	
Last refresh: 3 minutes ago		
ID	Value	Reason
2	Ip:10.200.200.90	manual 'ban' from 'localhost'
« < 1 > »		

Рисунок 3.55-3.56 – Перевірка роботи Crowdsec. Користувача було заблоковано на 2хв

За допомогою команди **cscli solutions list -a** в терміналі можна побачити всі адреса, які зібрані Crowdsec:

```
root@OPNsense:~ # cscli decisions list -a
```

ID	Source	Scope:Value	Reason	Action	Country	AS	Events	expiration	Alert
1	CAPI	Ip:8.215.43.167	firewallservices/pf-scan-multi_ports	ban			0	166h49m53s	1
2	CAPI	Ip:8.219.251.250	firewallservices/pf-scan-multi_ports	ban			0	166h49m53s	1
3	CAPI	Ip:57.128.188.122	firewallservices/pf-scan-multi_ports	ban			0	166h49m53s	1
4	CAPI	Ip:157.245.45.135	firewallservices/pf-scan-multi_ports	ban			0	166h49m53s	1
5	CAPI	Ip:192.42.116.194	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
6	CAPI	Ip:192.42.116.197	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
7	CAPI	Ip:192.42.116.209	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
8	CAPI	Ip:192.42.116.211	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
9	CAPI	Ip:192.42.116.208	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
10	CAPI	Ip:192.42.116.217	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
11	CAPI	Ip:192.42.116.179	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
12	CAPI	Ip:192.42.116.218	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
13	CAPI	Ip:104.152.52.244	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
14	CAPI	Ip:80.82.77.202	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
15	CAPI	Ip:104.152.52.235	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
16	CAPI	Ip:104.152.52.146	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
17	CAPI	Ip:104.152.52.130	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
18	CAPI	Ip:104.152.52.105	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
19	CAPI	Ip:190.71.145.130	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
20	CAPI	Ip:109.202.99.36	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
21	CAPI	Ip:213.232.87.232	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
22	CAPI	Ip:109.202.99.41	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
23	CAPI	Ip:213.232.87.228	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
24	CAPI	Ip:213.232.87.230	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
25	CAPI	Ip:115.231.78.3	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
26	CAPI	Ip:206.168.34.34	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
27	CAPI	Ip:206.168.34.51	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
28	CAPI	Ip:206.168.34.40	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
29	CAPI	Ip:206.168.34.35	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
30	CAPI	Ip:206.168.34.42	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
31	CAPI	Ip:206.168.34.127	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
32	CAPI	Ip:206.168.34.53	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
33	CAPI	Ip:206.168.34.32	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
34	CAPI	Ip:150.158.45.24	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
35	CAPI	Ip:147.185.132.100	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
36	CAPI	Ip:91.238.181.35	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
37	CAPI	Ip:170.176.130.260	firewallservices/pf-scan-multi_ports	ban			0	165h49m53s	1
3415	CAPI	Ip:159.65.147.193	crowdsecurity/ssh-bf	ban			0	165h49m53s	1
3416	CAPI	Ip:170.64.134.120	crowdsecurity/ssh-bf	ban			0	165h49m53s	1
3417	CAPI	Ip:221.11.25.218	crowdsecurity/ssh-bf	ban			0	165h49m53s	1
3418	CAPI	Ip:170.64.154.53	crowdsecurity/ssh-bf	ban			0	165h49m53s	1
3419	CAPI	Ip:78.188.102.28	crowdsecurity/ssh-bf	ban			0	165h49m53s	1
3420	CAPI	Ip:119.1.156.50	crowdsecurity/ssh-bf	ban			0	165h49m53s	1
3421	CAPI	Ip:80.242.208.68	crowdsecurity/ssh-bf	ban			0	165h49m53s	1
3422	CAPI	Ip:174.138.26.166	crowdsecurity/ssh-bf	ban			0	165h49m53s	1
3423	CAPI	Ip:196.189.87.177	crowdsecurity/ssh-bf	ban			0	165h49m53s	1
3424	CAPI	Ip:101.89.210.168	crowdsecurity/ssh-bf	ban			0	165h49m53s	1
3425	CAPI	Ip:101.89.109.195	crowdsecurity/ssh-bf	ban			0	165h49m53s	1
3426	CAPI	Ip:93.113.63.8	crowdsecurity/ssh-bf	ban			0	165h49m53s	1
3427	CAPI	Ip:171.104.142.232	crowdsecurity/ssh-bf	ban			0	165h49m53s	1
3428	CAPI	Ip:119.186.61.60	crowdsecurity/ssh-cve-2024-6387	ban			0	142h49m53s	1
14988	CAPI	Ip:101.201.212.110	crowdsecurity/ssh-cve-2024-6387	ban			0	142h49m53s	1
14989	CAPI	Ip:106.75.16.124	crowdsecurity/ssh-cve-2024-6387	ban			0	142h49m53s	1
14990	CAPI	Ip:106.75.111.194	crowdsecurity/ssh-cve-2024-6387	ban			0	140h49m53s	1
14991	CAPI	Ip:106.75.67.221	crowdsecurity/ssh-cve-2024-6387	ban			0	140h49m53s	1
14992	CAPI	Ip:106.75.67.167	crowdsecurity/ssh-cve-2024-6387	ban			0	139h49m53s	1
14993	CAPI	Ip:106.75.17.42	crowdsecurity/ssh-cve-2024-6387	ban			0	138h49m53s	1
14994	CAPI	Ip:106.75.67.32	crowdsecurity/ssh-cve-2024-6387	ban			0	138h49m53s	1
14995	CAPI	Ip:103.80.87.248	crowdsecurity/ssh-cve-2024-6387	ban			0	136h49m53s	1
14997	CAPI	Ip:106.75.70.142	crowdsecurity/ssh-cve-2024-6387	ban			0	131h49m53s	1
14998	CAPI	Ip:106.75.28.12	crowdsecurity/ssh-cve-2024-6387	ban			0	130h49m53s	1
14999	CAPI	Ip:106.75.70.89	crowdsecurity/ssh-cve-2024-6387	ban			0	128h49m53s	1
15000	CAPI	Ip:120.26.230.64	crowdsecurity/ssh-cve-2024-6387	ban			0	126h49m53s	1

```
root@OPNsense:~ #
```

Рисунок 3.57-3.59 – Команда *cscli solutions list -a*

Реалізація атак на мережу з відключеним міжмережевим екраном:

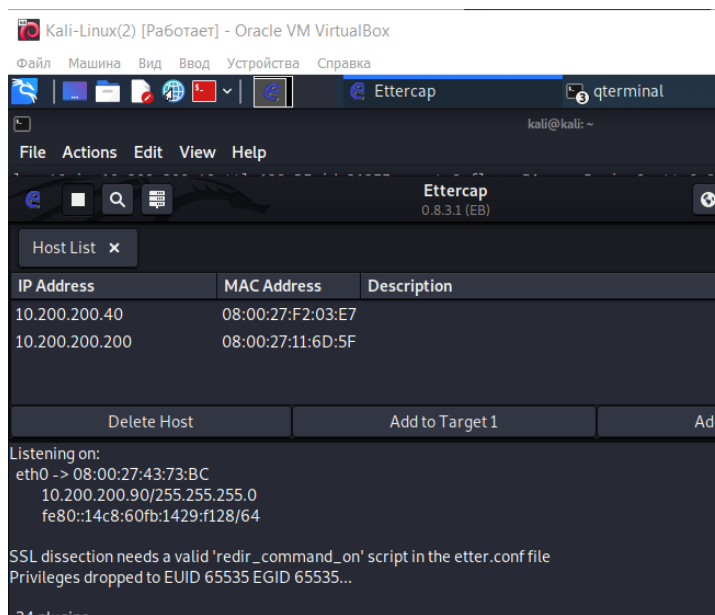


Рисунок 3.60 – Сканування мереж за допомогою Ettercap

```

(kali㉿kali)-[~]
$ nmap 10.200.200.200
Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-24 05:06 EST
Nmap scan report for 10.200.200.200
Host is up (0.0035s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49158/tcp  open  unknown
49159/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds

```

Рисунок 3.61 – Сканування nmap на відкриті порти Windows Server 2008

Реалізація атаки за допомогою Metasploit.

Metasploit Framework — це потужний інструмент для тестування безпеки, який використовується етичними хакерами та дослідниками кібербезпеки. Це платформа з відкритим кодом, яка дозволяє виконувати моделювання атак для виявлення вразливостей в системах.

За допомогою Kali Linux було здійснено реалізацію SYN Flood атаки за допомогою Metasploit. Kali Linux підробив IP-адрес Windows 7 та направляє атаку на Windows Server:

```

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > set RHOST 10.200.200.40
RHOST => 10.200.200.40
msf6 auxiliary(dos/tcp/synflood) > set RPORT 10.200.200.200
[-] The following options failed to validate: Value '10.200.200.200'
RPORT => 80
msf6 auxiliary(dos/tcp/synflood) > set RPORT 445
RPORT => 445
msf6 auxiliary(dos/tcp/synflood) > set SHOST 10.200.200.200
SHOST => 10.200.200.200
msf6 auxiliary(dos/tcp/synflood) > run
[*] Running module against 10.200.200.40

[*] SYN flooding 10.200.200.40:445 ...
^C[-] Stopping running against current target ...
[*] Control-C again to force quit all targets.
[*] Auxiliary module execution completed

```

Рисунок 3.62 – SYN Flood атака

За допомогою утиліти Wireshark можна побачити перехоплений трафік, що вказує на DoS-атаку:

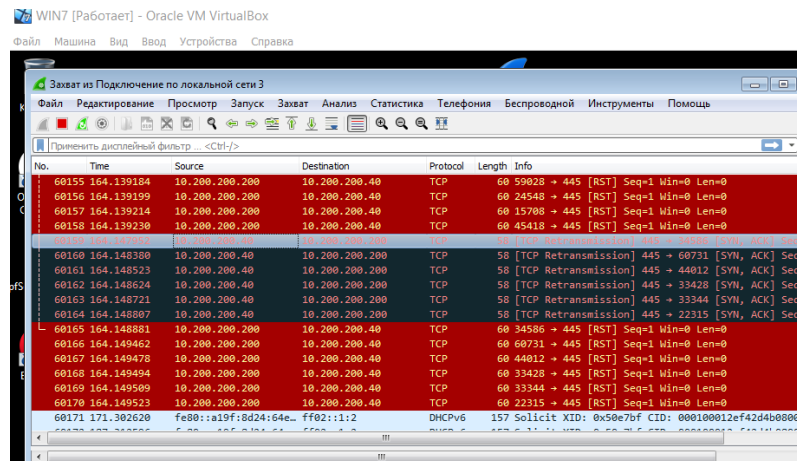


Рисунок 3.63 – Wireshark

Реалізація атаки за допомогою hping3.

hping3 — це потужний інструмент для генерації і аналізу мережевого трафіку, який працює через командний рядок. Він широко використовується в мережевому тестуванні, діагностиці та симуляції атак. Hping3 часто називають "TCP-пінгом", оскільки він підтримує перевірку доступності хоста не лише через ICMP (як стандартний ping), але й через TCP, UDP та інші протоколи.

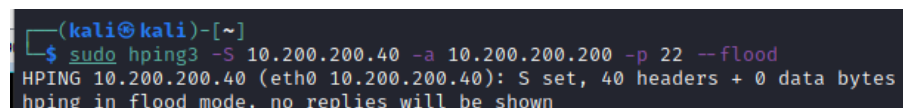


Рисунок 3.64 – SYN Flood атака

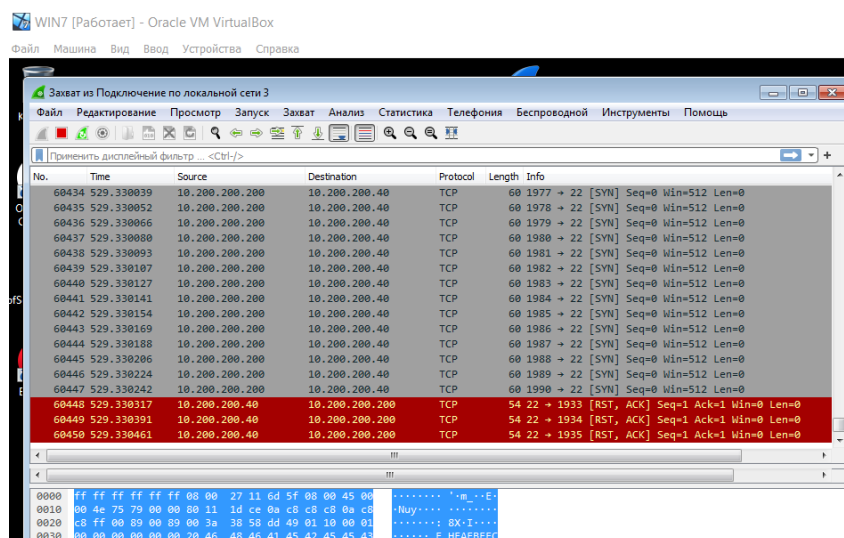
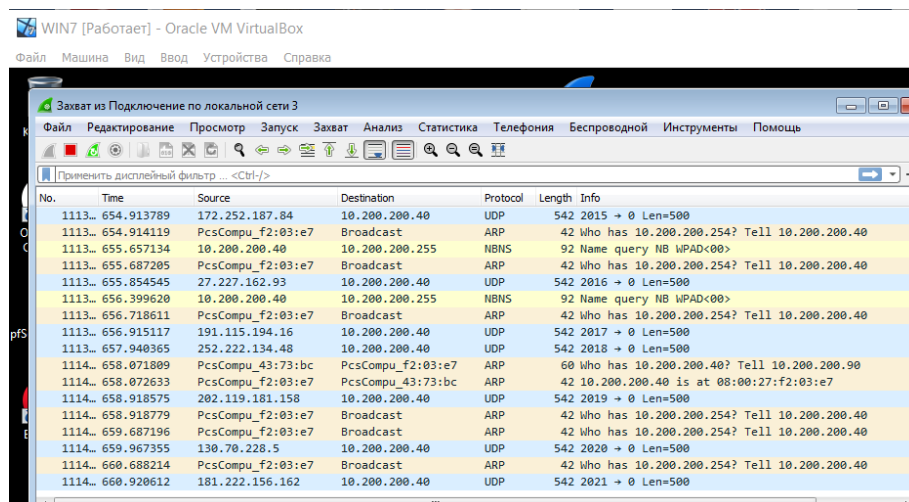


Рисунок 3.65 – Wireshark

Надсилення UDP-пакетів:

```
(kali@kali)-[~]  
$ sudo hping3 10.200.200.40 --udp --rand-source --data 500  
HPING 10.200.200.40 (eth0 10.200.200.40): udp mode set, 28 headers + 500 data bytes
```



The screenshot shows a Wireshark capture of network traffic on the interface 'Подключение по локальной сети 3'. The packet list on the left shows a series of packets. The main pane displays the details of a selected packet (No. 1113, Time 654.913789), which is a UDP packet from 172.252.187.84 to 10.200.200.40. The packet length is 542 bytes, and the info field shows '2015 → 0 Len=500'. The packet list also includes ARP requests, NBNS name queries, and other UDP packets.

No.	Time	Source	Destination	Protocol	Length	Info
1113.	654.913789	172.252.187.84	10.200.200.40	UDP	542	2015 → 0 Len=500
1113.	654.914119	PcsCompu_f2:03:e7	Broadcast	ARP	42	Who has 10.200.200.254? Tell 10.200.200.40
1113.	655.657134	10.200.200.40	10.200.200.255	NBNS	92	Name query NB WPAD<00>
1113.	655.687205	PcsCompu_f2:03:e7	Broadcast	ARP	42	Who has 10.200.200.254? Tell 10.200.200.40
1113.	655.854545	27.227.162.93	10.200.200.40	UDP	542	2016 → 0 Len=500
1113.	656.399620	10.200.200.40	10.200.200.255	NBNS	92	Name query NB WPAD<00>
1113.	656.718611	PcsCompu_f2:03:e7	Broadcast	ARP	42	Who has 10.200.200.254? Tell 10.200.200.40
1113.	656.915117	191.115.194.16	10.200.200.40	UDP	542	2017 → 0 Len=500
1113.	657.940365	252.222.134.48	10.200.200.40	UDP	542	2018 → 0 Len=500
1114.	658.071809	PcsCompu_43:73:bc	PcsCompu_f2:03:e7	ARP	60	Who has 10.200.200.40? Tell 10.200.200.90
1114.	658.072633	PcsCompu_f2:03:e7	PcsCompu_43:73:bc	ARP	42	10.200.200.40 is at 08:00:27:f2:03:e7
1114.	658.918575	202.119.181.158	10.200.200.40	UDP	542	2019 → 0 Len=500
1114.	658.918779	PcsCompu_f2:03:e7	Broadcast	ARP	42	Who has 10.200.200.254? Tell 10.200.200.40
1114.	659.687196	PcsCompu_f2:03:e7	Broadcast	ARP	42	Who has 10.200.200.254? Tell 10.200.200.40
1114.	659.967355	130.70.228.5	10.200.200.40	UDP	542	2020 → 0 Len=500
1114.	660.688214	PcsCompu_f2:03:e7	Broadcast	ARP	42	Who has 10.200.200.254? Tell 10.200.200.40
1114.	660.920612	181.222.156.162	10.200.200.40	UDP	542	2021 → 0 Len=500

Рисунок 3.66-3.67 – Реагування на UDP-пакет

Серед можливих атак на міжмережевий екран OPNSense особливою загрозою є DoS-атаки (Denial of Service). Вони спрямовані на перевантаження системи шляхом надсилення великої кількості запитів або трафіку, що може призвести до відмови в обслуговуванні та недоступності мережі.

Одним із інструментів, який можна використати для реалізації DoS-атаки на OPNSense, є програмне забезпечення Ettercap, встановлене на Kali Linux. Ettercap дозволяє здійснювати DoS-атаки через спам та перехоплення мережових пакетів. Наприклад, зловмисники можуть використовувати Ettercap для перехоплення ARP-пакетів і надсилення підроблених ARP-відповідей. Це спричиняє неправильну адресацію пристроїв у мережі, що може призвести до порушення зв'язку між ними або до їхньої повної недоступності.

Варто підкреслити, що використання Ettercap або інших інструментів для здійснення DoS-атак є незаконним і суперечить етичним нормам. Такі атаки завдають шкоди мережовій інфраструктурі, позбавляючи законних користувачів доступу до мережових ресурсів і послуг. [18]

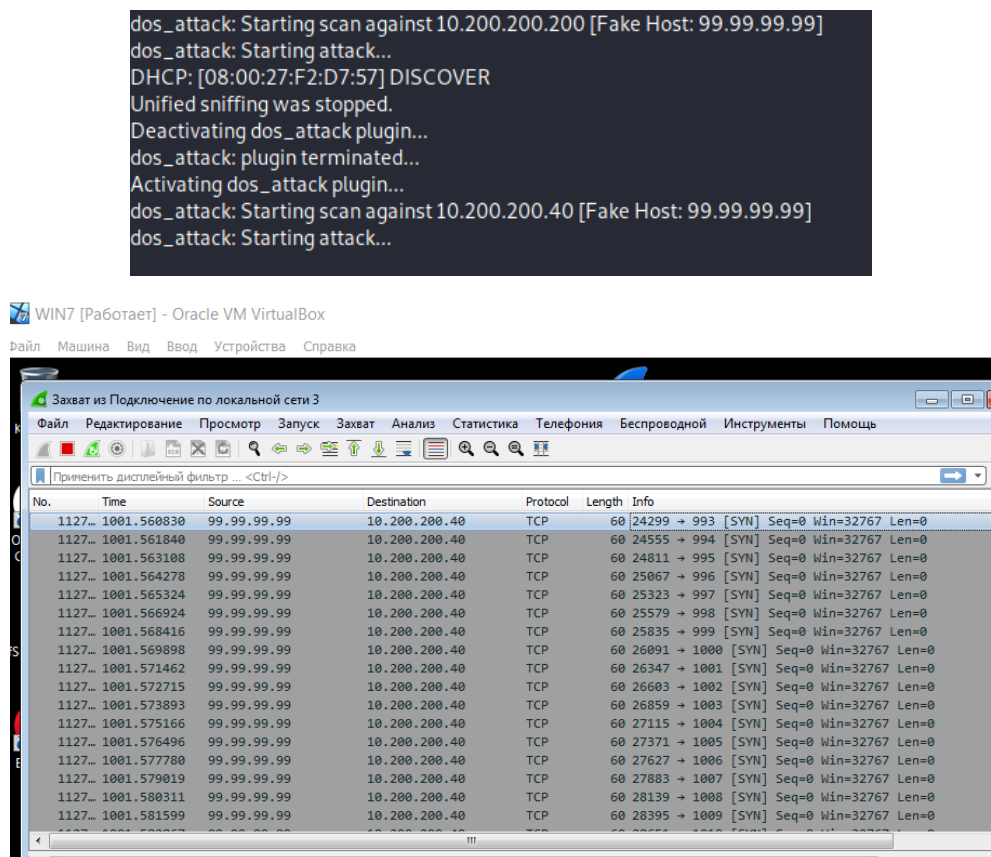


Рисунок 3.68-3.69 – DoS-атака за допомогою утиліти Ettercap

Реакція на атаки міжмережевого екрану OPNSense:

Тепер, при увімкненому та налаштованому OPNSense, Firewall блокує атаки:

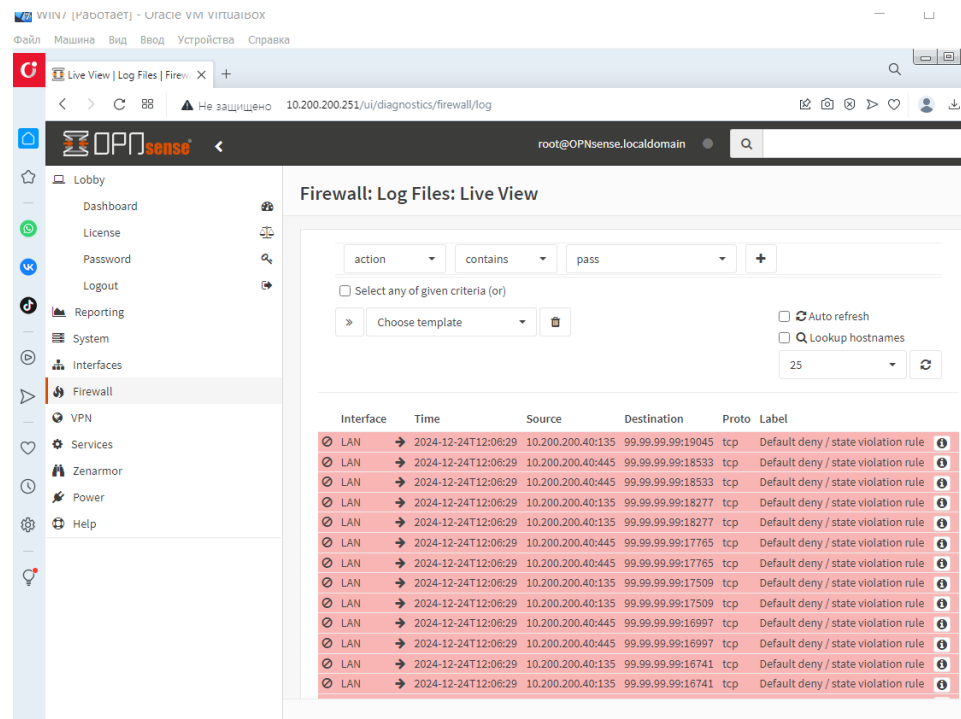


Рисунок 3.70 – Реакція на DoS-атаку

TCP retransmission вказує на блокування DoS-атаки пристроєм з адресою 10.200.200.251 (це наш міжмережвий екран OPNSense).

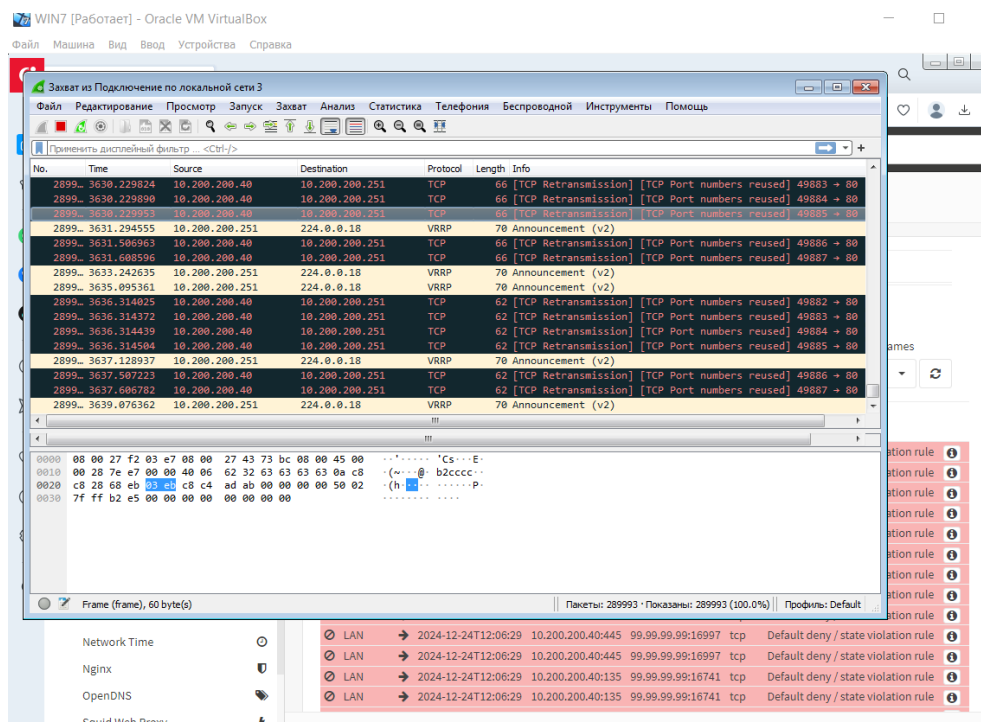


Рисунок 3.71 – Моніторинг OPNSense під час DoS-атаки

Сценарій firewallservices/pf-scan-multi_ports є одним із правил виявлення підозрілої активності, які CrowdSec застосовує для аналізу журналів мережевого трафіку. Його завдання — визначити можливу спробу сканування портів у мережі.

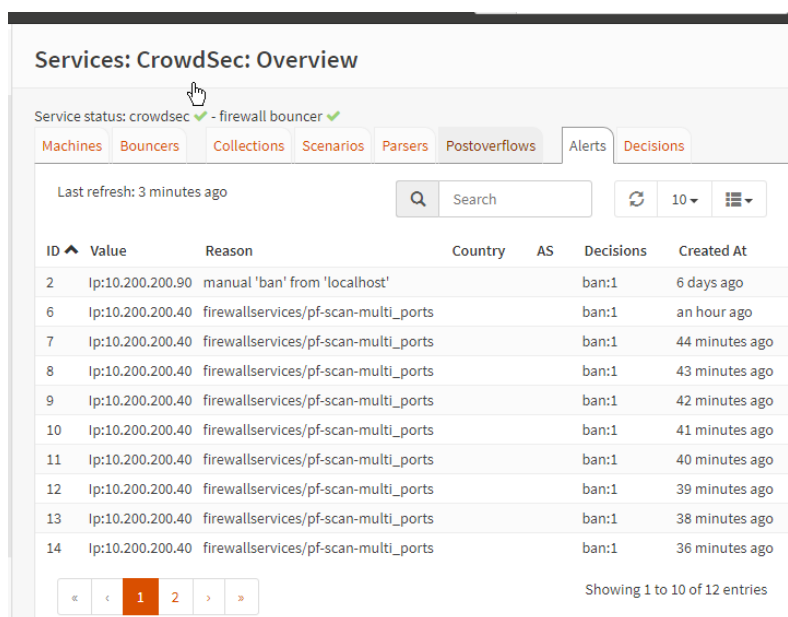


Рисунок 3.72 – CrowdSec

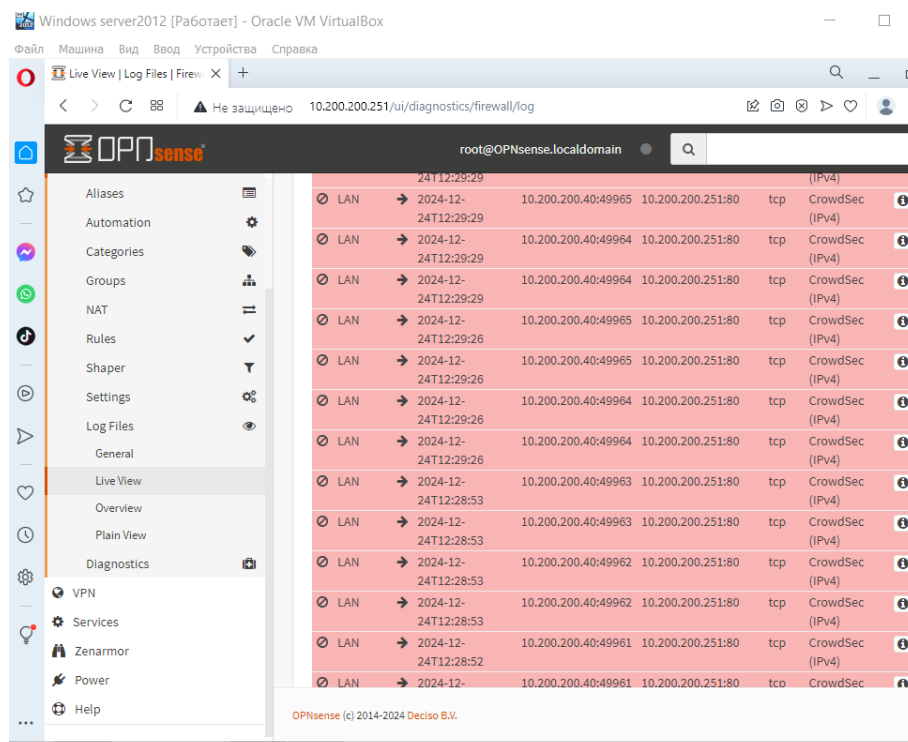


Рисунок 3.73 – CrowdSec

На далі було перевірено реагування на інциденти Suricata, виконанням атаки за допомогою Kali Linux. Для цього було проведено атаку за допомогою Ettercap.



Рисунок 3.74 – Проведення атаки DNS Spoofing за допомогою Ettercap

Лог вказує виявлення підозрілої активності в мережі: є кілька повідомлень DHCP-запитів (на UDP-порт 68), які можуть намагатися ідентифікувати хости Kali Linux, і Suricata класифікувала це як можливе порушення конфіденційності в корпоративній мережі з пріоритетом. Suricata класифікує це як порушення з пріоритетом 1.

Services: Intrusion Detection: Administration									
SettingsDownloadRulesUser definedAlertsSchedule									
Search 2024/12/18 9:127									
Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert	
2024-12-18T09:12:05.288161+0000	2022973	allowed	WAN	10.0.2.5	68	10.0.2.3	67	ET POLICY Possible Kali Linux hostname in DHCP Request Pac...	
2024-12-18T09:07:05.410117+0000	2022973	allowed	WAN	10.0.2.5	68	10.0.2.3	67	ET POLICY Possible Kali Linux hostname in DHCP Request Pac...	
2024-12-18T09:02:05.232534+0000	2022973	allowed	WAN	0.0.0.0	68	255.255.255.255	67	ET POLICY Possible Kali Linux hostname in DHCP Request Pac...	
2024-12-18T11:00:45.202476+0000	2100366	allowed	WAN	10.0.2.5	0	10.200.200.251	0	GPL ICMP_INFO PING *NIX	
2024-12-18T11:00:44.189796+0000	2100366	allowed	WAN	10.0.2.5	0	10.200.200.251	0	GPL ICMP_INFO PING *NIX	
2024-12-18T11:00:43.127305+0000	2100366	allowed	WAN	10.0.2.5	0	10.200.200.251	0	GPL ICMP_INFO PING *NIX	
2024-12-18T11:00:42.123439+0000	2100366	allowed	WAN	10.0.2.5	0	10.200.200.251	0	GPL ICMP_INFO PING *NIX	

Alert info	
Timestamp	2024-12-18T11:00:43.127305+0000
Alert	GPL ICMP_INFO PING *NIX
Alert sid	2100366
Protocol	ICMP
Source IP	10.0.2.5
Destination IP	10.200.200.251
Source port	0
Destination port	0
Interface	WAN

Alert info	
Timestamp	2024-12-18T09:02:05.232534+0000
Alert	ET POLICY Possible Kali Linux hostname in DHCP Request Packet
Alert sid	2022973
Protocol	UDP
Source IP	0.0.0.0
Destination IP	255.255.255.255
Source port	68
Destination port	67
Interface	WAN

Рисунок 3.75-3.76 – Реагування Suricata на атаку

Висновки до третього розділу

У третьому розділі було реалізовано, досліджено та протестовано підсистему захисту IT-інфраструктури на базі OPNsense. Проведено комплексне налаштування міжмережевого екрану, що включало конфігурацію правил фільтрації, впровадження технологій IDS/IPS для виявлення та запобігання загрозам, а також використання SSL-проксі для забезпечення глибокої перевірки зашифрованого трафіку. Налаштовані механізми резервування та балансування навантаження забезпечили високий рівень відмовостійкості та стабільності роботи системи.

Параметри захисту були ретельно налаштовані відповідно до визначеної моделі загроз, що дозволило знизити ризики та забезпечити належний рівень безпеки мережі. Виконане тестування продемонструвало ефективність впроваджених рішень, включаючи блокування несанкціонованого доступу, захист від атак типу DoS та мінімізацію впливу мережевих вразливостей. Аналіз результатів підтвердив, що підсистема відповідає встановленим цілям та вимогам.

Таким чином, реалізована підсистема захисту є надійним рішенням для забезпечення безпеки IT-інфраструктури, яке враховує сучасні виклики та загрози.

ВИСНОВКИ

Магістерська робота присвячена дослідженню та розробці підсистеми захисту корпоративної IT-інфраструктури на основі платформи OPNsense. Проведене дослідження підтвердило актуальність використання відкритих програмних рішень для побудови комплексних систем кіберзахисту.

У процесі виконання роботи здійснено детальний аналіз сучасних кіберзагроз, що дало змогу визначити ключові вектори атак і сформулювати вимоги до системи безпеки. Вивчення можливостей платформи OPNsense показало її ефективність у забезпеченні багаторівневого захисту, включаючи міжмережеве екранування, системи IDS/IPS, фільтрацію трафіку та механізми резервування.

Розроблений проект корпоративної мережі враховував сучасні принципи проектування, зокрема балансування навантаження та відмовостійкість. Налаштування ключових компонентів безпеки відповідало моделі загроз, що дозволило мінімізувати ризики, пов'язані з несанкціонованим доступом, атаками типу DoS та іншими загрозами.

Тестування підсистеми захисту підтвердило її здатність ефективно функціонувати в умовах, які імітують реальну корпоративну мережу. Результати роботи демонструють, що впроваджена підсистема є надійним, масштабованим і економічно ефективним рішенням, яке може бути застосоване для захисту організацій різного масштабу.

Практичне значення роботи полягає у створенні методики, яка дозволяє організаціям із різними бюджетами впроваджувати комплексні рішення безпеки на основі відкритих технологій. Отримані результати та розроблені рекомендації можуть бути використані для подальшого вдосконалення систем кіберзахисту, враховуючи постійний розвиток технологій та еволюцію загроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Хоменко В.Р. Автоматизовані рішення Fortigate для аналізу трафіку та виявлення аномалій у хмарних системах. *Комп'ютерні технології: інновації, проблеми, рішення* : VI Всеукр. науково-техн. конф., м. Житомир, 29–30 лист. 2023 р. / Наук. керівник Ю. Б. Бродський. Житомир, 2023. – Режим доступу до ресурсу: <https://conf.ztu.edu.ua/wp-content/uploads/2024/05/49.pdf>
2. Балансування навантаження та безпека: роль pfSense у високодоступних мережах. *Тези XIV Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2024»*, м. Житомир, 28–30 березня 2024 р. / Наук. керівник Ю. Б. Бродський. Житомир, 2023. – Режим доступу до ресурсу: <https://conf.ztu.edu.ua/wp-content/uploads/2024/01/116-1.pdf>
3. Динамічне балансування трафіку між декількома провайдерами. – Режим доступу до ресурсу: <http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/01/12-7.pdf>
4. OPNsense Security and Hardening Best Practice Guide – Режим доступу до ресурсу: <https://www.zenarmor.com/docs/network-security-tutorials/opnsense-security-and-hardening-best-practice-guide>
5. OPNsense® - High-End Security Made Easy™ Guide – Режим доступу до ресурсу: <https://opnsense.org/about/features/>
6. Protectli Vault FW4B 4 Port - Intel® J3160 – Режим доступу до ресурсу: <https://eu.protectli.com/wp-content/uploads/2024/07/FW4B-Datasheet-20240628.pdf>
7. MikroTik RB4011iGS+RM – Режим доступу до ресурсу: – Режим доступу до ресурсу: https://www.technotrade.com.ua/Products/MikroTik-RB4011iGSplusRM.php?srsltid=AfmBOopGP5NTrZAwWO1nB1J1SPWD2SMqVr_f4QJ7kNC3jgMfHcXeo9rI
8. Комутатор Cisco CBS220-16T-2G-EU – Режим доступу до ресурсу: – Режим доступу до ресурсу: <https://ip-tech.com.ua/cbs220-16t-2g-eu?srsltid=Afm-BOopjVXAtUXxbf4yejr5dB2X-8SH3KRKteWjHA2ephcEYFkxD0qK8>

9. Коммутатор Cisco CBS110-16T-EU – Режим доступу до ресурсу: – <https://xn--h1aemkx.com.ua/switch/cisco-sb/sb-110/cbs110-16t-eu>
10. КЛАСИФІКАЦІЯ ЗАГРОЗ І РИЗИКІВ СУЧАСНИХ ІНФОКОМУНІКАЦІЙНИХ – Режим доступу до ресурсу: – https://visn-it.uu.edu.ua/files/visnyk_2019_2_print_221-229.pdf
11. Palo Alto Alternatives: Similar Firewalls – Режим доступу до ресурсу: – <https://www.zenarmor.com/docs/network-security-tutorials/palo-alto-alternatives>
12. OpenBSD PF - Firewall Redundancy (CARP and pfsync) – Режим доступу до ресурсу: – <https://www.openbsd.org/faq/pf/carp.html>
13. Як працює Quad9? – Режим доступу до ресурсу: – Режим доступу до ресурсу: <https://sysadmin.pm/quad9/>
14. FireHOL IP Lists | IP Blacklists | IP Blocklists | IP Reputation : – Режим доступу до ресурсу: <http://iplists.firehol.org/>
15. Opnsense : Vulnerability Statistics – Режим доступу до ресурсу: <https://www.cvedetails.com/vendor/21847/>
16. How do you use the hierarchical network model for your projects ? – Режим доступу до ресурсу: <https://www.linkedin.com/advice/1/how-do-you-use-hierarchical-network-model-your>
17. Системи виявлення та запобігання вторгненням (IDPS) - <https://www.vpnunlimited.com/ua/help/cybersecurity/idps?srsId=AfmBOopkgupMUzi5QpcrpKfVBm9nwWS1Rj0O0etP30z0a7XrXC06dxs8>
18. Ettercap and middle-attacks tutorial EU [Електронний ресурс]. Режим доступу: <https://pentestmag.com/ettercap-tutorial-for-windows/>
19. Determining Firewall Rules [Електронний ресурс]. Режим доступу: <https://nmap.org/book/determining-firewall-rules.html>
20. Curated Threat Intelligence Powered by the Crowd [Електронний ресурс]. Режим доступу: <https://www.crowdsec.net/>
21. Zenarmor for Open Source Firewalls [Електронний ресурс]. Режим доступу: <https://www.zenarmor.com/zenarmor-next-generation-firewall>

22. Основні загрози безпеці ІТ інфраструктури у 2024 році [Електронний ресурс]. Режим доступу: <https://integrity.com.ua/bezpeka-v-it-infrastrukturi-zahyst-danyh/>
23. Найвідоміші хакерські атаки, про які говорив увесь світ [Електронний ресурс]. Режим доступу: <https://root-nation.com/ua/articles-ua/tech-ua/ua-naybilshihakerski-ataki/>
24. Класифікація міжмережевих екранів [Електронний ресурс]. Режим доступу <https://pejawedd.artbooks.cx.ua/articles/klasifikacija-mizhmerezhevih-ekraniv.html>
25. Next Generation Firewall (NGFW) екранів [Електронний ресурс]. Режим доступу <https://blog.infra-tech.ru/next-generation-firewall-review/>

ДОДАТКИ

Комплект постачання RB4011iGS-RM:

1 x RB4011iGS-RM

1 x 24V 1,5A блок живлення

1 x 19-дюймова стійка

Технічні характеристики Mikrotik RB4011iGS+RM:

Інтерфейс: 10 x 10/100/1000 Ethernet, 1 x SFP +

Процесор: 4 core AL21400 1,4 ГГц

Розмір оперативної пам'яті: 1 ГБ

Зберігання NAND: 512 МБ

Комутаційна чіп-модель RTL8367SB

Живлення: 12 В - 57 В (гніздо) DC 24V 1,5A, PoE IN (порт 1), PoE out (порт

10)

Максимальна споживана потужність: 18 Вт без виходу PoE, 33 Вт із виходом

PoE

Робоча температура: -40 С ... +45 С

Розміри: 228 x 120 x 30 мм

Операційна система: RouterOS, ліцензія 5

Технічні характеристики CBS220-16T-2G-EU:

16 портів 10/100/1000 Мбіт/с, 2 Gigabit SFP

Безвентиляторний

Габарити 440 x 203 x 44 мм

Вага 2,48 кг

Таблиця MAC До 8192 адресів

Флеш-пам'ять 64 МБ

Пам'ять процесора 256 МБ

Робоча температура від 0 ° до 50 ° С

Температура зберігання від -20 ° до 70 ° С

Вологість при зберіганні від 10% до 90%, при експлуатації від 10% до 90%

Технічні характеристики CBS110-16T-EU:

16 портів 10/100/1000 Мбіт/с

Безвентиляторний

Габарити 279 x 170 x 44 мм

Вага 0,97 кг

Таблиця MAC 8K адрес

Флеш-пам'ять 16 МБ

Процесор 400 МГц ARM (128 МБ)

Робоча температура від 0° до 40 °С

Температура зберігання від -20° до 70 °С

Вологість під час зберігання від 5% до 90%, під час експлуатації від 10% до 90%

Технічні характеристики FW4B:

Description 4X 1G Network Port Fanless Appliance

Processor Intel J3160 (64 Bit, 1.6 GHz, Turbo 2.24 GHz, 2MB L2 Cache)

Processor Cores 4

Processor Threads 4

Intel AES-NI Supported

Virtualization Intel Vt-x

Network 4x Intel 1G Ethernet, RJ-45

Video / Graphics Intel Clear Video HD, 2x HDMI 1.4

Audio Audio over HDMI, 1x 3.5mm Audio Jack

Memory 1x SO-DIMM DDR3L-1600, 1.35v, Max 8GB

Storage 1x mSATA

Optional Storage 1x Internal 2.5" SATA 3.0 SSD

External I/O 4x RJ-45 Ethernet

2x USB 3.2 Gen 2 Type A, 2x USB 2.0 Type A

2x HDMI

1x 3.5mm Audio Jack

1x RJ-45 COM

2x WiFi/LTE Antenna Mounting Holes

1x 12V DC Power Jack

Internal I/O 1x Mini PCIe for mSATA

1x SATA Header, 1x SATA Power

1x Full Height mPCIe (USB) for WiFi or LTE

1x USB 2.0 Header

1x CMOS Reset (2 pin)

1x Front Panel Header (9 pin)

BIOS AMI or coreboot

Indicators

1x LED Power Button (Blue), 1x LED Power Indicator (Green), 1x LED Disk Activity Indicator (Red), 1x LED Disk Activity Indicator (Yellow)

Power Input 12V DC, 1x DC Power Jack

Power Usage Max 20W