ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ
КАФЕДРА КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Пояснювальна записка

до кваліфікаційної роботи

бакалавра
(освітньо-кваліфікаційний рівень)

на тему *Розробка комплексної системи захисту інфраструктури Інтернет-провайдера*

Development of an integrated security system for the Internet provider infrastructure

Виконав: студент *4* курсу, групи *4КІБ*
напряму підготовки (спеціальності)
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)

Мартинюк І.С.
(прізвище та ініціали)

Керівник *Козел В.М.*
(прізвище та ініціали)

Рецензент *Вороненко М. О.*
(прізвище та ініціали)

Хмельницький – 2026 року

ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Інститут, факультет, відділення *інформаційних технологій та дизайну*
Кафедра, циклова комісія *комп'ютерних систем та мереж*
Освітньо-кваліфікаційний рівень *бакалавр*
Напрям підготовки *12 Інформаційні технології*
(шифр і назва)
Спеціальність *125 «Кібербезпека»*
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри *комп'ютерних систем та мереж*
Анжела ГРИГОРОВА
«___» _____202__ року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Мартинюка Івана Сергійовича
(прізвище, ім'я, по батькові)

1. Тема проєкту (роботи) *Розробка комплексної системи захисту інфраструктури Інтернет-провайдера*
Development of an integrated security system for the Internet provider infrastructure
керівник проєкту (роботи) *Козел Віктор Миколайович к.т.н., доцент*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від «13» січня 2026 року № 47-С
2. Строк подання студентом проєкту (роботи) 1 червня 2026 року
3. Вихідні дані до проєкту (роботи) *Методичні рекомендації до дипломного проєкту, звіт про проходження практики*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. *Аналіз об'єкта захисту*
2. *Обґрунтування вибору засобів для побудови системи безпеки*
3. *Проєктування та реалізація системи безпеки*
4. *Практичне тестування та перевірка системи захисту*

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	***Видача завдання, підбір та огляд літературних джерел, аналіз об'єкта захисту***	***16.02.2026 – 23.02.2026***	
2	***Обґрунтування вибору програмно-технічних засобів для побудови системи безпеки***	***23.02.2026 – 28.02.2026***	
3	***Розробка топології, проєктування та програмно-технічна реалізація системи захисту***	***01.03.2026 – 12.04.2026***	
4	***Практичне тестування системи захисту, симуляція мережевих атак та аналіз результатів***	***21.04.2026 – 24.04.2026***	
5	***Формування вступу, загальних висновків, підготовка додатків***	***26.04.2026 – 29.04.2026***	
6	***Оформлення пояснювальної записки та подання роботи на перевірку***	***до 01.06.2026***	

Студент _____ Мартинюк І.С.
(підпис) (прізвище та ініціали)

Керівник проєкту (роботи) _____ *Козел В.М.*
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Кваліфікаційна робота містить: 87 сторінок , 41 рисунок, не містить таблиць, не містить формул, має 63 посилання, 2 додатки.

Об'єкт дослідження – процеси забезпечення інформаційної безпеки та безперервності надання послуг у телекомунікаційних мережах інтернет-провайдерів.

Ціль роботи – розробка, програмно-технічна реалізація та практичне тестування ешелонованої системи захисту мережевого ядра та клієнтських сегментів телекомунікаційної інфраструктури.

У даній кваліфікаційній роботі бакалавра розроблено ієрархічну модель мережі з жорстким апаратним та логічним розмежуванням на зони довіри. Побудовано відмовостійке магістральне ядро на базі кластера pfSense з використанням протоколів CARP та pfsync. Для проактивного захисту периметра від атак прикладного рівня та мережевих перевантажень розгорнуто систему запобігання вторгненням IPS Suricata та механізми управління смугою пропускання. Забезпечено багаторівневий захист серверного сегмента DMZ шляхом загартовування ОС, налаштування локального міжмережевого екрана та системи динамічного блокування. Для безперервного аудиту та контролю цілісності файлів впроваджено SIEM-платформу Wazuh.

Проведено комплексне практичне тестування розробленого інженерного стенда. Емпірично доведено здатність системи автоматично відновлювати маршрутизацію при апаратних збоях, а також успішно відбивати спроби атак.

Розроблена комплексна система захисту може бути використана для підвищення кіберстійкості та надійності реальних мереж інтернет-провайдерів.

ІНФОРМАЦІЙНА БЕЗПЕКА, ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА, ВІДМОВОСТІЙКІСТЬ, МІЖМЕРЕЖЕВИЙ ЕКРАН, PFSENSE, IPS, SIEM, WAZUH, VLAN

АНОТАЦІЯ

Дипломну роботу присвячено проєктуванню та практичній реалізації ешелонованої системи захисту телекомунікаційної мережі провайдера. Метою роботи є забезпечення відмовостійкості та кібербезпеки магістрального ядра й клієнтських сегментів. У ході виконання роботи спроектовано архітектуру з апаратно-логічною ізоляцією VLAN, розгорнуто кластер високої доступності на базі pfSense, впроваджено систему запобігання вторгненням Suricata та підсистему централізованого моніторингу подій безпеки Wazuh. Ефективність запропонованих рішень емпірично підтверджено шляхом тестування стійкості інфраструктури до DDoS-атак, мережевої розвідки та експлойтів прикладного рівня. Практичні результати можуть бути використані для підвищення безпеки реальних мереж інтернет-провайдерів.

ABSTRACT

The diploma thesis is devoted to the design and practical implementation of a defense-in-depth security system for an ISP telecommunication network. The aim of the work is to ensure the fault tolerance and cybersecurity of the backbone core and client segments. During the work, an architecture with hardware-logical isolation VLAN was designed, a high-availability cluster based on pfSense was deployed, an intrusion prevention system Suricata and a centralized security event monitoring subsystem Wazuh were implemented. The effectiveness of the proposed solutions is empirically confirmed by testing the infrastructure's resilience to DDoS attacks, network reconnaissance, and application-layer exploits. The practical results can be used to enhance the security of real-world internet service provider networks.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧОК, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ОС – операційна система

ПЗ – програмне забезпечення

КСЗІ – комплексна система захисту інформації

СУІБ – система управління інформаційною безпекою

ACL (Access Control Lists) –списки контролю доступу

ARP (Address Resolution Protocol) – протокол визначення адрес

BGP (Border Gateway Protocol) – протокол граничного шлюзу

Brute-force – метод перебору паролів грубою силою

CARP (Common Address Redundancy Protocol) – протокол резервування спільних адрес

CPE (Customer Premises Equipment) – клієнтське обладнання

DDoS (Distributed Denial of Service) – розподілена атака на відмову в обслуговуванні

DHCP (Dynamic Host Configuration Protocol) – протокол динамічного налаштування вузла

Dictionary Attack – атака перебору за словником

DMZ (Demilitarized Zone) – демілітаризована зона

DNS (Domain Name System) – система доменних імен

DPI (Deep Packet Inspection) – глибока інспекція пакетів

EDR (Endpoint Detection and Response) – виявлення та реагування на кінцевих точках

FIM (File Integrity Monitoring) – моніторинг цілісності файлів

HA (High Availability) – кластер високої доступності (відмовостійкості)

HTTP (HyperText Transfer Protocol) – протокол передачі гіпертексту

HTTPS (HyperText Transfer Protocol Secure) – безпечний протокол передачі гіпертексту

IDS (Intrusion Detection Systems) – системи виявлення вторгнень

IP (Internet Protocol) – міжмережевий протокол

IPsec (IP Security) – набір протоколів для захисту даних

IPoE (IP over Ethernet) – технологія авторизації та передачі IP-трафіку поверх Ethernet

IPS (Intrusion Prevention System) – система запобігання вторгненням

ISP (Internet Service Provider) – Інтернет-провайдер

MAC (Media Access Control) – унікальний апаратний ідентифікатор мережевого інтерфейсу

MPLS (Multiprotocol Label Switching) – багатопротокольна комутація за мітками

NAT (Network Address Translation) – трансляція мережевих адрес

OSI (Open Systems Interconnection) – базова еталонна модель взаємодії відкритих систем

OSPF (Open Shortest Path First) – протокол динамічної маршрутизації

PAM (Pluggable Authentication Modules) – модулі автентифікації, що підключаються

PPPoE (Point-to-Point Protocol over Ethernet) – тунельний протокол канального рівня поверх Ethernet

QoS (Quality of Service) – якість обслуговування (технології пріоритезації трафіку)

SIEM (Security Information and Event Management) – система управління інформаційною безпекою та подіями

SSH (Secure Shell) – безпечний протокол віддаленого управління операційною системою

TCP (Transmission Control Protocol) – протокол управління передачею даних

UDP (User Datagram Protocol) – протокол користувацьких датаграм

UFW (Uncomplicated Firewall) – локальний міжмережевий екран операційної системи Ubuntu

VIP (Virtual IP) – віртуальна IP-адреса

VLAN (Virtual Local Area Network) – віртуальна локальна комп'ютерна мережа

VPN (Virtual Private Network) – віртуальна приватна мережа

WAF (Web Application Firewall) – міжмережевий екран для захисту веб-додатків
WAN (Wide Area Network) – глобальна обчислювальна мережа (зовнішній канал зв'язку)

ВСТУП

Швидке поширення та розвиток інформаційно-комунікаційних технологій та цифровізація сучасного суспільства перетворили телекомунікаційні мережі на критично важливу складову національної та глобальної інфраструктури. Інтернет-провайдери відіграють важливу роль, забезпечуючи безперервний доступ до глобальної мережі, цілісність переміщення великих обсягів даних, а також збереження конфіденційності користувачів. Через свою масштабність та значущість, інфраструктура провайдерів стає однією з пріоритетних цілей для кіберзлочинців.

Сучасні проблеми захисту ISP-інфраструктури характеризуються постійним зростанням кількості та складності загроз. Якщо раніше основна увага приділялась атакам мережевого та транспортного рівнів, то сьогодні значна частина загроз спрямована на прикладний рівень та серверну інфраструктуру. Значна кількість провайдерських мереж побудована на базі застарілих архітектурних рішень з недостатнім рівнем безпеки. Ефективна система захисту повинна включати комплекс взаємопов’язаних компонентів, серед яких системи виявлення та запобігання вторгненням, механізми сегментації мережі, централізований моніторинг подій безпеки, засоби аналізу трафіку, технології контролю доступу, системи захисту серверної інфраструктури та інструменти захищеного віддаленого управління. Окрему увагу необхідно приділяти забезпеченню відмовостійкості мережевих вузлів та безперервності надання послуг абонентам.

Актуальність теми зумовлена необхідністю переходу від традиційних підходів до побудови комплексних, надійних систем, що базуються на принципах багаторівневої оборони та нульової довіри. Використання лише окремих засобів фільтрації трафіку або класичних міжмережевих екранів вже не дає достатнього рівня безпеки. Компрометація мережі провайдера може призвести до порушення роботи критично важливих сервісів, втрати даних або створення загроз для великої кількості користувачів. Тому розробка системи, яка чітко розмежовує ресурси та захищає інфраструктуру як від зовнішніх, так і від внутрішніх загроз, є необхідністю для забезпечення стабільної роботи.

Об’єктом дослідження є мережева інфраструктура Інтернет-провайдера як об’єкт інформаційної безпеки.

Предмет дослідження – методи, технології та програмно-технічні засоби забезпечення комплексного захисту інфраструктури провайдера від сучасних загроз.

Метою роботи є розробка комплексної системи захисту інфраструктури Інтернет-провайдера із використанням сучасних засобів мережевої безпеки, централізованого моніторингу, сегментації мережі, технологій виявлення вторгнень та механізмів захисту серверного сегмента.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Провести аналіз інфраструктури Інтернет-провайдера як об’єкта інформаційної безпеки;
2. Дослідити сучасні загрози та вразливості телекомунікаційних мереж;
3. Виконати аналіз існуючих технологій та засобів захисту;
4. Обґрунтувати вибір програмно-технічних рішень для побудови системи безпеки;
5. Розробити логічну архітектуру комплексної системи захисту;
6. Реалізувати механізми захисту та провести експериментальні дослідження ефективності функціонування розробленої системи;
7. Оцінити ефективність впроваджених механізмів захисту.

Практичне значення. Результати кваліфікаційної роботи можуть бути безпосередньо використані для модернізації інфраструктури Інтернет-провайдерів, а також підвищення загального рівня захищеності складних корпоративних мереж.

Взаємозв'язок з іншими роботами. Дане дослідження ґрунтується на сучасних розробках у галузі мережевої безпеки та розвиває підходи до використання концепції відмовостійкості і комплексних інструментів з відкритим вихідним кодом для потреб критичної інфраструктури.

1 АНАЛІЗ ОБ’ЄКТА ЗАХИСТУ

1.1 Характеристика інфраструктури Інтернет-провайдера

Сучасні Інтернет-провайдери є технічною основою для функціонування глобальної мережі. З інженерної точки зору, інфраструктура провайдера — це масштабна система, яка об'єднує маршрутизатори, комутатори та магістральні канали зв'язку, які забезпечують безперервну передачу даних між кінцевими користувачами й рештою світу. За своєю структурою та принципами роботи мережа ISP суттєво відрізняється від звичайних корпоративних чи локальних мереж підприємств. Головна відмінність полягає в тому, що вона побудована як відкрита транзитна система. У такій інфраструктурі немає єдиного захищеного периметра, оскільки обладнання повинно щомиті обробляти трафік із тисяч клієнтських пристроїв та суміжних систем.

Для забезпечення масштабованості та стабільної обробки потоків даних інфраструктуру сучасного провайдера розділяють на чотири основні послідовні рівні:

1. **Граничний рівень** — це зовнішній кордон мережі, який забезпечує взаємодію з магістральними операторами вищого рівня та точками обміну трафіком. На цьому етапі встановлюються високопродуктивні маршрутизатори, які обробляють глобальні таблиці маршрутів за протоколом BGP. Обладнання підбирає оптимальні напрямки для передачі трафіку та взаємодії із зовнішніми мережами.

2. **Рівень ядра** — центральна магістраль провайдера. Його функція зводиться до максимально швидкого пересилання великих обсягів даних між ключовими вузлами мережі з мінімальними затримками. На цьому рівні використовуються потужні комутатори та протоколи внутрішньої динамічної маршрутизації, зокрема OSPF, які часто поєднуються з технологією MPLS. Будь-які ресурсномісткі операції, що вимагають глибокої інспекції пакетів, на рівні ядра не проводяться, трафік просто має йти далі.

3. **Рівень агрегації або розподілу** — проміжний етап, на якому збирається трафік з багатьох вузлів доступу для його подальшої передачі в ядро.

На цьому рівні працюють широкосмугові шлюзи віддаленого доступу BRAS/BNG. Вони виконують основну логіку керування користувачами: керування абонентськими сесіями, автентифікацію, видачу мережевих адрес, збір статистики для білінгу та обмеження швидкості згідно з тарифними планами.

4. **Рівень доступу** — це безпосереднє підключення кінцевого абонентського обладнання. Фізично цей рівень реалізується на базі комутаторів доступу у будинках або оптичних лінійних терміналів у випадку пасивних оптичних мереж PON. Цей сегмент є найбільшим за кількістю пристроїв і безпосередньо контактує з неконтрольованим клієнтським середовищем [12].

Крім транспортної ієрархії, в архітектурі провайдера обов'язково виділяють окремі логічні та функціональні зони. Так звана демілітаризована зона потрібна для розміщення критично важливих сервісів, що забезпечують життєдіяльність мережі. Сюди входять офіційні веб-сайти, сервери DNS, служби автоматичного налаштування DHCP, RADIUS чи TACACS-сервери автентифікації та білінгові системи. Також створюється окрема мережа управління, яка повністю ізольована від клієнтських потоків даних і використовується інженерами виключно для налаштування, моніторингу та збору телеметрії з активного обладнання. Така багаторівнева фізична та логічна архітектура робить мережу стійкою до високих навантажень. Проте ця складність створює величезну площу для атаки. Кожен рівень та сегмент містить специфічні активи, компрометація яких може призвести до різних за масштабом наслідків: від відключення окремого будинку до глобального падіння мережі цілого регіону.

Для побудови ефективної комплексної системи захисту необхідно чітко визначити перелік активів провайдера, які підлягають охороні. Багаторівнева архітектура мережі передбачає наявність великої кількості елементів, що вимагає їхньої систематизації. Інфраструктурні активи Інтернет-провайдера доцільно класифікувати за чотирма основними групами.

До першої групи належить апаратне забезпечення мережі. Це активні мережеві пристрої на всіх ієрархічних рівнях: магістральні маршрутизатори ядра, широкосмугові шлюзи агрегації, комутатори доступу, оптичні лінійні термінали та

фізичні сервери у центрах обробки даних. Фізичне пошкодження або програмне виведення з ладу цих компонентів призводить до миттєвої деградації сервісів.

Другу групу становлять програмні комплекси та мережеві сервіси. До цієї категорії входять операційні системи мережевого обладнання, протоколи динамічної маршрутизації, а також критичні служби демілітаризованої зони, такі як сервери доменних імен, системи автоматичної конфігурації хостів, сервери автентифікації клієнтів та білінгові системи.

У третю групу входять інформаційні активи. Цей блок включає конфігураційні файли обладнання, таблиці маршрутизації, бази персональних даних абонентів, журнали реєстрації подій та безпосередньо масиви транзитного трафіку.

Четверта група активів об'єднує канали управління та адміністрування. Сюди відноситься виділена мережа управління, протоколи віддаленого доступу та облікові записи інженерного персоналу. Компрометація цих каналів дозволяє зловмисникам отримати повний контроль над інфраструктурою оператора незалежно від надійності зовнішнього захисту [8].

Визначивши ключові активи, необхідно адаптувати класичну тріаду інформаційної безпеки до специфіки телекомунікаційної мережі. Розподіл пріоритетів між доступністю, цілісністю та конфіденційністю для Інтернет-провайдера має виражені відмінності від стандартних корпоративних моделей.

Найвищим і безумовним пріоритетом для оператора зв'язку є доступність сервісів. Згідно з галузевими стандартами та угодами про рівень обслуговування, телекомунікаційна інфраструктура повинна забезпечувати безперервну передачу даних. Будь-які простої внаслідок технічних збоїв або цілеспрямованих атак на відмову в обслуговуванні спричиняють прямі фінансові збитки та репутаційні втрати.

Наступним за важливістю критерієм виступає цілісність інфраструктури та даних. Для провайдера критично важливо гарантувати незмінність конфігурацій обладнання та коректність таблиць маршрутизації. Несанкціонована зміна

маршрутних даних може призвести до масштабного перехоплення трафіку, утворення мережевих петель або ізоляції цілих автономних систем.

На третьому місці серед пріоритетів конфіденційність. Провайдер безпосередньо не відповідає за шифрування користувацького трафіку, оскільки це завдання вирішується на прикладному рівні самими клієнтами за допомогою криптографічних протоколів. Проте оператор зобов'язаний забезпечувати сувору конфіденційність персональних даних абонентів у білінг системах та захищати технологічну інформацію, зокрема конфігурації та журнали аудиту, від витоків.

1.2 Класифікація загроз та аналіз вразливостей

Серед об’єктів кібератак провайдери є однією з найпривабливіших цілей для кіберзлочинців, оскільки вона виступають єдиною точкою доступу до мережі для тисяч користувачів і корпоративних клієнтів. Успішна атака на вузли ISP дозволяє зловмисникам не лише порушити доступність послуг, але й отримати можливість перехоплення конфіденційного транзитного трафіку. Усі мережеві атаки на телекомунікаційну інфраструктуру доцільно розділяти на зовнішні, що ініціюються з глобальної мережі, та внутрішні, що походять з абонентського сегмента. Аналіз зовнішніх загроз демонструє, що найвищу небезпеку для працездатності провайдера становлять атаки на відмову в обслуговуванні DoS/DDoS. За вектором впливу їх поділяють на дві основні категорії:

1. **Об'ємні атаки.** Спрямовані на повне вичерпання пропускної здатності магістральних каналів зв'язку. Найчастіше реалізуються через методи ампліфікації, коли зловмисники використовують вразливі публічні сервери (DNS, NTP) для відправлення масиву підроблених запитів із підміненою IP-адресою цілі. У результаті граничні маршрутизатори провайдера отримують відповіді, розмір яких багаторазово перевищує початковий запит, що призводить до перевантаження вхідних інтерфейсів.

2. **Атаки спрямовані на вичерпання ресурсів.** Їхньою метою є вичерпання оперативної пам'яті та переповнення таблиць станів на граничних маршрутизаторах та міжмережевих екранах. Класичним прикладом є TCP SYN

Flood, який генерує величезну кількість напіввідкритих з'єднань. Це призводить до того, що мережеве обладнання втрачає здатність встановлювати нові легітимні сесії для абонентів.

Другим значним зовнішнім вектором є сканування та атаки типу Brute-force. Зовнішній периметр ISP постійно піддається автоматизованому скануванню спеціалізованими інструментами та ботнетами. Метою такої розвідки є пошук відкритих портів управління, залишених без належного захисту стандартних інтерфейсів керування маршрутизаторами або вразливих VPN-шлюзів. Після виявлення такої точки входу ініціюється масований словниковий перебір паролів для отримання несанкціонованого доступу з правами адміністратора.

Третій вектор загроз фокусується на експлуатації вразливостей прикладного рівня. Ці загрози спрямовані переважно на сервіси демілітаризованої зони, які вимушено залишаються відкритими для глобальної мережі. Зловмисники застосовують техніки SQL-ін'єкцій для отримання несанкціонованого доступу до баз даних білінгових систем, а також атаки типу Cross-Site Scripting (XSS) і Remote Code Execution (RCE) для захоплення контролю над публічними веб-серверами та порталами самообслуговування абонентів.

Успішна реалізація будь-якого з цих зовнішніх векторів здатна завдати критичної шкоди системі. Проте практика експлуатації мереж провайдерів показує, що не менш руйнівними, а іноді й значно складнішими для виявлення, є внутрішні загрози, джерелом яких виступає безпосередньо клієнтське обладнання. Традиційні моделі мережевої безпеки, що базувалися на принципі довіри до внутрішньої мережі, в умовах телекомунікаційного підприємства є нерелевантними. Клієнтське обладнання перебуває поза зоною прямого адміністрування оператора зв'язку, проте має пряме підключення до інфраструктури, що породжує низку специфічних векторів атак.

Перша група внутрішніх загроз пов'язана з маніпуляцією базовими протоколами канального та мережевого рівнів. До цієї категорії належать:

— Підміна мережевих ідентифікаторів MAC/IP Spoofing: Спроби абонентів змінити свої фізичні або логічні адреси на адреси інших легітимних клієнтів з метою обходу білінгових систем чи уникнення блокувань.

— ARP Spoofing: Відправлення фальшивих ARP-відповідей у локальну мережу для перенаправлення трафіку сусідніх вузлів і реалізації атак типу «людина посередині».

— Несанкціоновані сервери конфігурації Rogue DHCP: Навмисне або випадкове розгортання стороннього DHCP-сервера, який видає абонентам хибні IP-адреси та адреси DNS-серверів, що призводить до відмови в обслуговуванні або перенаправлення трафіку на фішингові ресурси.

Друга група загроз виходить від масово скомпрометованого клієнтського обладнання. Домашні маршрутизатори із застарілими прошивками та слабкими паролями автоматизовано інфікуються і об'єднуються у ботнети. Такі пристрої функціонують як автономні одиниці, генеруючи величезні обсяги паразитного трафіку в напрямку внутрішніх вузлів провайдера, або здійснюють масову розсилку спаму. Це швидко призводить до потрапляння публічних IP-адрес провайдера до міжнародних чорних списків і блокування легітимної пошти інших клієнтів.

Третя група — загроза горизонтального переміщення. За відсутності належної логічної ізоляції та функцій ізоляції портів на комутаторах доступу, інфекція з одного скомпрометованого пристрою безперешкодно поширюється на обладнання сусідів. Крім того, відсутність мікросегментації дозволяє зловмисникам здійснювати пряме сканування серверів управління мережею провайдера.

Для систематизації описаних зовнішніх та внутрішніх загроз формується профіль потенційного порушника. Критеріями поділу виступають розташування щодо периметра мережі та рівень наявних привілеїв:

1. **Зовнішній порушник (з глобальної мережі).** Володіє кваліфікацією від середнього до дуже високого рівня, часто має у розпорядженні значні

обчислювальні потужності. Мотивований фінансовим збагаченням або політичним хактивізмом; атакує граничні маршрутизатори та публічні сервіси у DMZ.

2. **Внутрішній легітимний порушник (інсайдер).** Це системний адміністратор або інженер із легальним доступом до мережі управління та детальним знанням топології. Дії інсайдера найважче виявити, оскільки він використовує штатні інструменти адміністрування.

3. **Внутрішній нелегітимний порушник (абонентський сегмент).** Клієнт провайдера або інфіковане обладнання. Мотивація зводиться до обходу обмежень швидкості, отримання безкоштовного доступу або генерування паразитного трафіку [20].

Сформована модель переконливо доводить, що інфраструктура провайдера перебуває під постійним тиском з усіх векторів. Класичний підхід, за якого мережа вважається довіреною зсередини, є неефективним. Для нейтралізації цих профілів порушників необхідний перехід до архітектури, що базується на суворій ізоляції сегментів та глибокому аналізі трафіку.

1.3 Огляд існуючих технологій та систем захисту мережевої інфраструктури

Історично розвиток мережевої безпеки розпочався з концепції захисту периметра, яку часто порівнюють з моделлю «замку та рову». Суть цього підходу зводилася до створення жорсткої межі між «довіреною» внутрішньою мережею підприємства та «недовіреним» глобальним середовищем. У такій парадигмі всі ресурси всередині периметра за замовчуванням наділялися високим рівнем довіри, тоді як транзитний трафік, що надходив ззовні, підлягав обов'язковій перевірці. Для реалізації такого класичного захисту Інтернет-провайдери традиційно спиралися на кілька базових технологій фільтрації, які сьогодні складають лише первинний рубіж оборони [19].

Статична пакетна фільтрація. Першим рівнем контролю доступу традиційно виступають магістральні маршрутизатори, що використовують списки контролю доступу. Цей метод функціонує на мережевому та транспортному рівнях

моделі OSI, приймаючи рішення щодо пересилання пакетів виключно на основі статичних параметрів: IP-адрес джерела та призначення, номерів портів і типів протоколів. Головною перевагою пакетної фільтрації є надзвичайно висока швидкість обробки, що не створює затримок на магістральних каналах провайдера. Водночас цей механізм є абсолютно сліпим до безпосереднього вмісту трафіку. Для обходу такого захисту зловмиснику достатньо помістити свій шкідливий код у дозволений протокол, наприклад, відправивши навантаження через стандартний відкритий порт вебсервера.

Динамічна інспекція станів та NAT. Для компенсації недоліків статичної маршрутизації впроваджуються міжмережеві екрани, які відстежують життєвий цикл кожного мережевого з'єднання від моменту ініціалізації до його завершення. Вони динамічно відкривають порти для зворотного трафіку лише за умови, що сесія була легітимно ініційована зсередини мережі, що ефективно захищає вузли від зовнішнього автоматизованого сканування. Додатковою лінією приховування топології тривалий час вважалася трансляція мережевих адрес NAT, яка ховає внутрішні підмережі абонентів за публічними адресами шлюзу оператора. Проте ані NAT, ані Stateful-екрани не здійснюють глибокого аналізу на рівні додатків. Вони не здатні відрізнити звичайний HTTP-запит користувача від цілеспрямованої атаки типу SQL-ін'єкції, оскільки обидва потоки проходять через один легітимний канал.

З огляду на особливості сучасних Інтернет-провайдерів, традиційна периметральна модель має фундаментальні недоліки. По-перше, вона не забезпечує захисту від внутрішніх загроз, залишаючись безсилою проти інфікованих клієнтських пристроїв, які вже знаходяться в системі. По-друге, плоска топологія дозволяє зловмиснику, який подолав зовнішній бар'єр, безперешкодно переміщуватися між серверами та підмережами. По-третє, масовий перехід глобальної мережі на протоколи з наскрізним шифруванням робить класичні міжмережеві екрани неспроможними аналізувати транзитні потоки, перетворюючи їх на прості маршрутизатори зашифрованих даних. Наявність цих недоліків вимагає концептуальної зміни парадигми безпеки. Тому на зміну застарілим

підходам прийшла архітектура Zero Trust, що базується на принципі відсутності довіри за замовчуванням. Згідно з рекомендаціями NIST SP 800-207, жоден вузол мережі, незалежно від його фізичного розташування, не вважається безпечним. Будь-яка спроба взаємодії між серверами управління, маршрутизаторами ядра або клієнтськими пристроями вимагає обов'язкової автентифікації, авторизації та безперервного моніторингу. Кожному суб'єкту мережі надається лише мінімально необхідний обсяг привілеїв [17]. Практична реалізація моделі нульової довіри в інфраструктурі провайдера базується на глибокій сегментації мережі. Замість створення єдиних великих широкомовних доменів, де заражений комп'ютер одного клієнта може безперешкодно сканувати сусідів, мікросегментація розбиває мережу на жорстко ізольовані зони. У абонентському сегменті це досягається шляхом виділення клієнтів у власні віртуальні канали за допомогою технології VLAN. Натомість для інших критично важливих зон застосовується суворе фізичне розділення інтерфейсів. Це гарантує контроль доступу та унеможливлює горизонтальне переміщення зловмисника у разі локальної компрометації одного з вузлів.

Впровадження концепцій Zero Trust та мікросегментації дозволяє створити стійку до компрометації інфраструктуру, де успішна атака на один елемент не призводить до ефекту доміно і не ставить під загрозу всю мережу провайдера. Проте, для повноцінного захисту самої лише ізоляції недостатньо — необхідні інструменти, які здатні заглядати всередину пакетів та розуміти їхній вміст.

Глибока інспекція пакетів. Основою такого аналізу є технологія DPI. На відміну від традиційних міжмережевих екранів, які перевіряють лише заголовки пакетів: IP-адреси та порти, DPI виконує повну реконструкцію сесії та аналізує корисне навантаження кожного пакету.

Технологія DPI лежить в основі сучасних систем виявлення та запобігання вторгненням:

1. Системи виявлення вторгнень. працюють у пасивному режимі. Вони отримують копію мережевого трафіку і аналізують його на наявність відомих загроз. У разі виявлення підозрілої активності IDS генерує сповіщення для

адміністратора безпеки, але не втручається в сам процес передачі даних. Головна перевага IDS полягає в тому, що система не створює затримок у мережі і не може випадково заблокувати легітимний трафік. Однак для мереж Інтернет-провайдерів, де атаки розгортаються за лічені секунди, простого сповіщення вже недостатньо.

2. Системи запобігання вторгненням. На відміну від IDS, системи IPS встановлюються «в розрив» і є активним елементом мережі. Весь трафік проходить крізь процесор інспекції системи. Використовуючи комбінацію сигнатурних баз даних та евристичного аналізу, сучасні IPS безперервно сканують транзитний трафік у пошуках відомих вразливостей, спроб виконання ін'єкцій коду або звернень до шкідливих доменів. У разі виявлення загрози система здатна автоматично заблокувати з'єднання або внести IP-адресу нападника до чорного списку.

Системи централізованого моніторингу та кореляції подій. Ефективна реалізація багатошарової оборони вимагає наявності єдиного центру управління безпекою. Оскільки пристрої розташовані на різних рівнях інфраструктури провайдера, аналіз логів окремо робить фізично неможливим завданням. Для вирішення цієї проблеми впроваджуються SIEM, які об’єднують інформацію з магістральних маршрутизаторів, комутаторів агрегації, серверів демілітаризованої зони та систем запобігання вторгненню. Замість простого зберігання логів, SIEM-системи автоматично нормалізують дані та виконують їх кореляцію. Це дозволяє виявляти складні, розподілені в часі багатовекторні атаки, які залишаються непомітними для окремих вузлів захисту, і миттєво сповіщати інженерний персонал про інциденти. Невід'ємною складовою систем моніторингу є механізми контролю цілісності файлів. Для провайдера критично важливо гарантувати незмінність конфігурацій активного мережевого обладнання та системних файлів серверів DMZ. Модулі FIM безперервно хешують та відстежують стан конфігураційних файлів і політик доступу. Будь-яка несанкціонована зміна, незалежно від того, чи була вона викликана діями зовнішнього зловмисника, чи помилкою інсайдера, негайно фіксується системою. У поєднанні з локальними міжмережевими екранами на серверах та системами

динамічного аналізу логів, технології FIM забезпечують надійний захист кінцевих хостів та мережі управління від прихованої компрометації [60].

Автентифікація абонентів та управління доступом. Забезпечення безпеки на границі між клієнтською мережею й інфраструктурою провайдера залежить від обраної технології авторизації користувачів. Історично базовим рішенням для більшості операторів зв'язку був протокол PPPoE. Його механізм полягає у створенні віртуального тунелю між домашнім роутером абонента та шлюзом BRAS/BNG на рівні агрегації. PPPoE інкапсулює IP-пакети у кадри канального рівня, що дозволяє легко виконувати процедури автентифікації через централізовані RADIUS-сервери, вести чіткий облік сесій для білінгу та динамічно застосовувати політики обмеження швидкості. З точки зору безпеки, цей протокол захищає від багатьох атак канального рівня, оскільки абоненти ізольовані всередині своїх тунелів. Проте використання PPPoE створює серйозні системні недоліки: додаткові заголовки протоколу зменшують корисний розмір пакета MTU, що вимагає налаштування фрагментації, а процес інкапсуляції та деінкапсуляції трафіку створює високе навантаження на центральні процесори маршрутизаторів розподілу. [33]

Сучасною і більш продуктивною альтернативою є технологія IPoE. У цій архітектурі абонентський пристрій не будує жодних тунелів, а отримує доступ до мережі нативно, за допомогою стандартного протоколу динамічного налаштування вузлів DHCP. Захист та ідентифікація користувачів при використанні IPoE переноситься на рівень доступу за допомогою механізму DHCP Snooping та опції Option 82. Коли клієнтський роутер відправляє запит на отримання IP-адреси, найближчий керований комутатор доступу перехоплює цей пакет і впроваджує в нього додаткове поле Option 82, яке містить унікальний ідентифікатор самого комутатора та номер фізичного порту, до якого підключено кабель. Шлюз агрегації спільно з RADIUS-сервером аналізує цю інформацію, перевіряє прив'язку порту до конкретного договору в білінгу та видає легітимні мережеві налаштування. Перехід на IPoE повністю знімає проблему заголовків та знижує навантаження на ядро

мережі, проте вимагає суворого впровадження функцій захисту на комутаторах доступу для запобігання підміні адрес [33].

Віртуальні приватні мережі. Захист каналів адміністрування інфраструктури провайдера є критично важливою ланкою, оскільки компрометація інтерфейсів керування означає втрату контролю над усією мережею. Для організації безпечного доступу інженерного персоналу до виділеної мережі управління використовуються технології віртуальних приватних мереж. Традиційне використання протоколу SSH без додаткового захисту на межі мережі створює ризики підбору паролів або експлуатації вразливостей нульового дня у самих службах віддаленого доступу. Впровадження VPN дозволяє повністю приховати порти управління від зовнішнього сканування глобальної мережі та абонентського сегмента, створюючи шифрований тунель через недовірене середовище передачі даних.

При проектуванні вузлів доступу для адміністраторів зазвичай розглядають два типи архітектурних рішень VPN. Класичний стек протоколів IPsec функціонує на мережевому рівні та забезпечує найвищий рівень захисту завдяки суворому шифруванню та автентифікації кожної датаграми. IPsec є стандартом для побудови захищених каналів зв'язку типу Site-to-Site між віддаленими технологічними майданчиками чи серверами провайдера. Проте для підключення окремих робочих станцій інженерів Client-to-Site частіше розгортають рішення на базі OpenVPN або сучасного протоколу WireGuard. Завдяки шифруванню VPN-тунелів провайдер повністю нівелює загрозу перехоплення адміністративних облікових даних, навіть якщо зловмисник має фізичний доступ до проміжних ліній зв'язку.

1.4 Нормативно-правове регулювання та міжнародні стандарти у сфері кібербезпеки

Побудова надійної системи захисту Інтернет-провайдера не обмежується виключно вибором апаратних чи програмних рішень. Будь-яка архітектура має відповідати суворим вимогам міжнародних стандартів та чинного законодавства. Саме нормативно-правова база формує критерії оцінки захищеності та визначає

міру юридичної відповідальності оператора за збереження даних абонентів і безперебійність надання послуг.

Міжнародні стандарти серії ISO/IEC 27000. Фундаментом для організації управління безпекою є стандарти Міжнародної організації зі стандартизації. Ключову роль тут відіграє ISO/IEC 27001, який регламентує створення та підтримку системи управління інформаційною безпекою. Цей стандарт вимагає від провайдера застосування ризик-орієнтованого підходу: спочатку проводиться інвентаризація активів, потім оцінюються ризики для кожного активу, і лише після цього обираються адекватні технічні та організаційні засоби контролю. Впровадження СУІБ гарантує, що безпека інфраструктури є безперервним процесом, а не одноразовою дією [15].

Окрім того, увагу звертають на окремий стандарт стандарт ISO/IEC 27032, який безпосередньо стосується кіберпростору та визначає механізми обміну інформацією про мережеві інциденти [16].

Концептуальна модель NIST Cybersecurity Framework. Якщо стандарти ISO дають загальну управлінську рамку, то еталоном для практичного інженерного проектування вважається фреймворк Національного інституту стандартів і технологій США (NIST). Він пропонує гнучку структуру, побудовану на п'яти безперервних функціях:

1. Ідентифікація: розуміння того, яке обладнання та дані існують у мережі
2. Захист: впровадження механізмів контролю доступу, сегментації мережі та шифрування.
3. Виявлення: розгортання систем моніторингу трафіку та виявлення аномалій.
4. Реагування: автоматизоване або ручне блокування виявлених загроз.
5. Відновлення: забезпечення резервування та відмовостійкості.

З інженерної точки зору цей підхід є максимально прагматичним. Він вимагає, щоб оператор не просто встановив мережевий екран для захисту мережі, але й обов'язково розгорнув систему глибокого моніторингу трафіку для фіксації аномалій. Крім того, інженери повинні мати задокументований алгоритм

перемикання маршрутів BGP або використання резервних каналів зв'язку у разі успішної DDoS-атаки. Така комплексна модель гарантує швидке відновлення працездатності магістралі навіть за умов часткової компрометації обладнання.

Національне законодавство та статус об'єктів критичної інфраструктури, нормативні документи з технічного захисту інформації (НД ТЗІ). У правовому полі України діяльність Інтернет-провайдерів регулюється низкою нормативно-правових актів, які визначають їхні обов'язки щодо захисту інформації та забезпечення безперервності надання послуг. Базовим є Закон України “Про електронні комунікації”, який встановлює правову основу діяльності постачальників електронних комунікаційних мереж [2]. Ключовим документом є Закон України «Про основні засади забезпечення кібербезпеки України». Згідно з його положеннями, магістральні мережі великих операторів зв'язку можуть класифікуватися як об'єкти критичної інформаційної інфраструктури. Набуття такого статусу суттєво посилює вимоги: провайдер зобов'язаний регулярно проходити незалежні аудити інформаційної безпеки та оперативно передавати інформацію про серйозні кіберінциденти урядовій команді реагування CERT-UA [4]. Окрім транзитного трафіку, провайдер оперує великими масивами даних у білінгових системах, через що підпадає під дію Закону України «Про захист персональних даних». Це робить обов'язковим впровадження криптографічних засобів та жорсткої ізоляції для запобігання витоку клієнтської інформації. Практична побудова захисних комплексів також спирається на вимоги НД ТЗІ, які встановлюють жорсткі архітектурні критерії для проектування комплексних систем захисту інформації [5].

1.5 Необхідність розробки комплексної системи захисту та постановка задачі

Специфіка інфраструктури Інтернет-провайдера як відкритої транзитної системи унеможливлює використання класичної периметральної моделі безпеки. Постійне зростання масштабів атак, доводять необхідність побудови проактивної комплексної системи захисту інформації. Така система повинна реалізувати

концепцію ешелонованої оборони на всіх чотирьох ієрархічних рівнях мережі, забезпечуючи безперервність сервісів та глибокий аналіз навантаження.

Комплексна система захисту має відповідати таким ключовим вимогам:

— **Архітектурна ізоляція:** логічна мікросегментація в абонентському сегменті для ізоляції клієнтів. Для активів провайдера фізичне розділення середовищ передачі даних за допомогою виділених інтерфейсів. Це повністю нівелює ризики компрометації систем управління через вразливості логічних тегів.

— **Фільтрація та відмовостійкість:** побудова відмовостійкого кластера високої доступності з автоматичним перемиканням шлюзів та синхронізацією сесій, інтеграція багатопотокової системи запобігання вторгненням на прикладному рівні та застосування засобів автоматизованої репутаційної фільтрації трафіку.

— **Моніторинг та управління:** розгортання централізованої системи моніторингу подій безпеки SIEM для серверів сервісної зони, а також організація віддаленого адміністрування інфраструктури виключно через шифровані віртуальні приватні мережі VPN.

Метою роботи є проєктування, програмно-технічна реалізація та експериментальне тестування моделі комплексної системи захисту інфраструктури Інтернет-провайдера.

Для її досягнення необхідно вирішити такі завдання:

1. Розробити структурно-логічну схему мережі провайдера з фізичним розділенням критичних зон та мікросегментацією абонентського рівня.
2. Налаштувати відмовостійкий кластер міжмережевого екранування.
3. Інтегрувати IPS та додаткові модулі автоматизованої репутаційної фільтрації.
4. Розгорнути підсистему централізованого моніторингу SIEM.
5. Організувати віддалене адміністрування за допомогою технології віртуальних приватних мереж.
6. Провести практичне тестування спроектованої системи в умовах симуляції мережевих атак та оцінити її ефективність.

2 ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ ДЛЯ ПОБУДОВИ СИСТЕМИ БЕЗПЕКИ

2.1 Міжмережевий екран та маршрутизація трафіку

Центральним вузлом транзитної інфраструктури провайдера є магістральний маршрутизатор, який одночасно виконує функції міжмережевого екрана. Оскільки через цей вузол проходить увесь клієнтський трафік та запити до публічних сервісів, до нього висуваються критичні вимоги щодо пропускної здатності, стабільності мережевого стека та здатності забезпечувати безперервність надання послуг. Традиційним підходом для великих телекомунікаційних компаній є використання спеціалізованих апаратних комплексів рівня Cisco ASA або Juniper SRX. Вони забезпечують гарантовану продуктивність, проте є закритими системами із надзвичайно високою вартістю ліцензування за кожну додаткову функцію. Це робить їх економічно недоцільними для регіональних операторів зв'язку. Іншою популярною альтернативою є обладнання латвійського виробника MikroTik під управлінням RouterOS. Попри свою доступність та гнучкість маршрутизації, RouterOS має суттєві архітектурні обмеження при побудові відмовостійких кластерів. Зокрема, у цій системі відсутні повноцінні механізми миттєвої синхронізації таблиць станів з'єднань між двома фізичними маршрутизаторами, що є критичним недоліком при проектуванні глибокої фільтрації [23].

Для реалізації ядра мережі у розроблюваній системі обрано платформу pfSense. Це рішення з відкритим вихідним кодом, яке базується на операційній системі FreeBSD, яка відзначається стабільністю та продуктивністю мережевої маршрутизації. На відміну від комерційних аналогів, pfSense надає повний доступ до функціоналу корпоративного рівня без додаткових ліцензійних платежів, дозволяючи гнучко масштабувати продуктивність шляхом простої заміни фізичних компонентів сервера. Вбудований пакетний фільтр PF гарантує надшвидку обробку правил статичної та динамічної фільтрації безпосередньо на рівні ядра ОС Вирішальним фактором на користь pfSense стала нативна підтримка кластеризації. Мережа провайдера не може дозволити собі простоїв через апаратний збій одного

маршрутизатора. Тому архітектура системи будується у вигляді відмовостійкого HA-кластера, що працює за допомогою зв'язки двох протоколів: CARP та pfsync [24].

Протокол CARP дозволяє об'єднати два фізичні маршрутизатори під єдиною віртуальною IP-адресою, яка виступає шлюзом замовчуванням для абонентів. У разі виходу з ладу основного пристрою, резервний маршрутизатор миттєво бере на себе віртуальний IP і продовжує маршрутизацію. Своєю чергою, протокол pfsync через виділений фізичний інтерфейс безперервно синхронізує таблицю станів мережевих сесій між пристроями. Завдяки цьому прозорому механізму абоненти навіть не помітять моменту аварійного перемикання: усі активні завантаження файлів, потокові відео або відкриті SSH-сесії залишаться активними, оскільки резервний маршрутизатор вже має відомості про них і продовжить їхню обробку [25].

2.2 Технології сегментації мережі

Розподіл мережевих потоків та ізоляція різних груп користувачів і сервісів є базовою умовою для забезпечення стійкості інфраструктури оператора зв'язку. У плоскій мережевій топології, де абоненти та технологічні сервери знаходяться в одному широкомовному домені, компрометація навіть одного клієнтського пристрою дозволяє зловмиснику проводити сканування всієї мережі, перехоплювати чужий трафік через атаки на канальному рівні або викликати широкомовний шторм. Для проектування надійної архітектури у роботі обрано комбінований підхід: логічна мікросегментація для масового абонентського вузла та суворе апаратне розділення для критичних зон.

Для ізоляції клієнтського трафіку на рівні доступу та агрегації обрано технологію віртуальних локальних мереж VLAN стандарт IEEE 802.1Q. Використання логічного розділення є єдино можливим інженерним рішенням для абонентського сегменту провайдера. Альтернативний підхід у вигляді виділення окремого фізичного порту чи кабелю під кожного клієнта на всьому шляху до ядра мережі є економічно та технічно неможливим через колосальні витрати на

обладнання. Технологія VLAN дозволяє інкапсулювати трафік кожного абонента або окремого будинку у виділений логічний канал шляхом додавання 4-байтового тегу в Ethernet-кадр. Ключова перевага цього методу — повна ізоляція абонентів один від одного на канальному рівні в межах одного фізичного кабелю чи магістрального Trunk-порту [39]. Це повністю вирішує проблему безпеки «сусідського» середовища: клієнти не можуть перехоплювати чужі дані або здійснювати деструктивний вплив на пристрої інших абонентів мережі.

Попри високу ефективність для масового сегмента, технологія VLAN має відомі архітектурні вразливості. За наявності специфічного програмного забезпечення зловмисник може реалізувати атаки типу VLAN Hopping або Double Tagging, які дозволяють штучно ін'єктувати деструктивні пакети з одного віртуального сегмента в інший в обхід правил фільтрації. З цієї причини використання логічних VLAN для захисту внутрішньої інфраструктури самого провайдера є критичним ризиком.

Для захисту стратегічних активів оператора обрано метод фізичного розділення інтерфейсів. Це означає, що зовнішній транзитний канал, сервери публічних служб та мережа віддаленого адміністрування підключаються до абсолютно різних, незалежних апаратних портів центрального шлюзу захисту. Такий підхід створює нездоланний фізичний бар'єр. Навіть якщо зловмисник повністю скомпрометує абонентське обладнання на рівні доступу і зможе маніпулювати тегами VLAN, він апаратно не здатний надіслати кадр безпосередньо у серверну зону чи мережу управління. Будь-яка взаємодія між цими середовищами стає можливою виключно через ядро пакетного фільтра, яке аналізує трафік на вищих рівнях моделі OSI.

2.3 Метод авторизації клієнтів

Процедура автентифікації та контролю доступу абонентів у мережі визначає не лише рівень захищеності інфраструктури, але й безпосередньо впливає на її продуктивність та швидкість надання послуг. Оскільки оператор зв'язку взаємодіє з великою кількістю неконтрольованих кінцевих пристроїв, обраний метод

авторизації повинен ефективно вирішувати три інженерні завдання: однозначно ідентифікувати користувача згідно з його договором, автоматизувати видачу мережевих налаштувань та повністю блокувати спроби несанкціонованого доступу або підміни адрес на канальному рівні.

В свій час базовим рішенням у телекомунікаційній сфері був протокол PPPoE. Його популярність зумовлювалася простотою впровадження на застарілому обладнанні: протокол створює віртуальний тунель від клієнта до шлюзу доступу, що дозволяє легко виконувати авторизацію через RADIUS-сервери за логіном і паролем та ізолювати користувачів. Проте в умовах сучасних високошвидкісних мереж PPPoE створює серйозні системні проблеми. По-перше, інкапсуляція кожного IP-пакета в заголовки PPP та PPPoE створює додатковий оверхед 8 байт, що зменшує стандартний розмір пакета MTU з 1500 до 1492 байт. Це вимагає обов'язкового налаштування MSS Clamping на маршрутизаторах для запобігання фрагментації, що часто стає причиною некоректного завантаження деяких веб-ресурсів у клієнтів. По-друге, і це найголовніше, процес пакування та розпакування тунельного трафіку виконується на центральному процесорі маршрутизатора агрегації, що при високих навантаженнях призводить до деградації пропускної здатності всього ядра мережі.

Для вирішення проблем продуктивності у даному проєкті обрано нативний підхід: технологію IPoE . У цій архітектурі абонентський пристрій не будує жодних логічних тунелів, а взаємодіє з мережею оператора нативно, використовуючи стандартний стек протоколів Ethernet та IP. Видача мережевих реквізитів відбувається автоматично через службу DHCP. Це повністю знімає проблему зменшення MTU, мінімізує затримки при передачі пакетів та знижує навантаження на центральний процесор головного шлюзу, оскільки комутація трафіку виконується на повній швидкості інтерфейсів. Головним архітектурним викликом при переході на IPoE є захист від підміни мережевих ідентифікаторів. Оскільки середовище є нативним, зловмисник в абонентському сегменті може вручну прописати чужу IP-адресу або MAC-адресу, атаки IP/MAC Spoofing, щоб отримати безкоштовний доступ до Інтернету або перехопити чужі пакети [35].

Для нівелювання цієї загрози для системи буде реалізовано механізм захисту, який базується на суворій зв'язці двох методів:

— **DHCP Static Mapping:** Центральний сервер автоматичної конфігурації провайдера не видає адреси з випадкового динамічного пулу. За кожним абонентом або його пристроєм у базі даних закріплюється унікальна, фіксована IP-адреса, яка видається лише у відповідність до його унікальної фізичної MAC-адреси.

— **Static ARP:** Самого лише DHCP-мапінгу недостатньо, адже клієнт може прописати адресу вручну в обхід DHCP-сервера. Тому на магістральному маршрутизаторі впроваджується режим жорсткої перевірки таблиці ARP. При звичайному динамічному ARP маршрутизатор вірить будь-яким повідомленням із мережі та оновлює записи відповідності IP-MAC автоматично. У режимі Static ARP таблиця відповідностей стає повністю статичною та стійкою до змін із мережі [38].

Завдяки такій інженерній схемі, якщо пристрій абонента надсилає пакет, маршрутизатор перевіряє, чи відповідає поточна пара IP та MAC жорстко зафіксованому запису в його пам'яті. Якщо зловмисник змінить MAC-адресу або спробує підставити чужий IP, пакет буде миттєво відкинутий пакетним фільтром на найнижчому рівні обробки. Це повністю ліквідує загрозу несанкціонованого доступу та крадіжки сервісів усередині мережі провайдера.

2.4 Глибокий аналіз та контроль трафіку

В умовах відкритої транзитної мережі оператор зв'язку щомиті стикається з масивами небажаного трафіку: від цілеспрямованих спроб сканування до паразитної активності інфікованих клієнтських пристроїв. Використання виключно систем глибокого аналізу IDS/IPS для обробки кожного пакета є нераціональним, оскільки це призводить до швидкого вичерпання обчислювальних ресурсів маршрутизатора. Тому ефективна архітектура вимагає впровадження механізмів префільтрації, які відсікають очевидні загрози на найбільш ранніх етапах, а також інструментів управління пропускною здатністю для нівелювання наслідків об'ємних атак.

Механізми репутаційної фільтрації та DNS-Sinkhole. Для вирішення задачі префільтрації у проєкті обґрунтовано використання інтегрованого модуля pfBlockerNG. На відміну від класичних правил міжмережевого екрана, які налаштовуються вручну, pfBlockerNG працює за принципом автоматизованої репутаційної фільтрації Threat Intelligence. Він динамічно агрегує глобальні бази даних відомих шкідливих IP-адрес: ботнетів, спам-мереж, вузлів Tor і блокує з'єднання з ними ще до того, як вони досягнуть підсистеми маршрутизації ядра. Важливою перевагою pfBlockerNG є можливість розгортання технології DNS Sinkhole. Оскільки більшість сучасних шкідливих програм звертаються до своїх командних серверів за доменними іменами, DNS-фільтрація дозволяє заблокувати загрозу ще на етапі перетворення імені в IP-адресу. Якщо клієнтський пристрій намагається перейти на фішинговий сайт або зв'язатися з командним центром ботнету, система підміняє відповідь DNS, перенаправляючи запит в нікуди. Це дозволяє не лише захистити абонентів від зараження, але й критично знизити обсяг сміттєвого трафіку, який генерують уже інфіковані домашні роутери, не навантажуючи при цьому процесор.

Управління пропускною здатністю Traffic Shaping. Другим найважливішим вектором контролю є забезпечення якості обслуговування та захист магістральних каналів від перевантажень. Навіть за ідеально налаштованої фільтрації, один скомпрометований клієнт, що генерує UDP-флуд на максимальній швидкості свого порту, здатен вичерпати ресурси апаратних інтерфейсів і спричинити відмову в обслуговуванні для інших абонентів мережі. Для запобігання таким інцидентам застосовуються вбудовані механізми Limiters, що працюють безпосередньо в pfSense.

2.5 Засоби виявлення та запобігання вторгненням

Базові механізми міжмережевого екранування є неефективними проти атак прикладного рівня, коли зловмисник використовує вразливості легітимних сервісів. Для виявлення таких загроз необхідне впровадження систем глибокої інспекції пакетів DPI, які здатні аналізувати корисне навантаження кожного

мережевого кадру. Враховуючи специфіку мережі провайдера, обрана система повинна не лише виявляти загрози, але й автоматично блокувати їх у реальному часі, не створюючи при цьому вузьких місць для транзитного трафіку.

Стандартом у сфері IDS/IPS є система Snort. Проте її архітектура має фундаментальний недолік при використанні у високошвидкісних мережах: Snort є однопотоковим додатком. Весь трафік з інтерфейсу буде оброблятися лише одним ядром процесора маршрутизатора, що неминуче призведе до перевантаження апаратної платформи та катастрофічного падіння пропускної здатності для абонентів. Для забезпечення необхідного рівня продуктивності та безпеки обрано сучасну систему виявлення вторгнень Suricata. Її ключовою інженерною перевагою є повноцінна підтримка багатопотоковості. Suricata здатна динамічно розподіляти навантаження з аналізу пакетів на всі доступні ядра процесора. Це дозволяє здійснювати глибоку інспекцію транзитного трафіку на повній швидкості інтерфейсів без внесення відчутних затримок. Крім архітектурної переваги, Suricata забезпечує високий рівень захисту завдяки свої можливостям:

— Аналіз на прикладному рівні та функціонал WAF: Система здатна розпізнавати специфічні протоколи та застосовувати сигнатурний аналіз безпосередньо до їхнього вмісту. Це дозволяє використовувати Suricata як своєрідний міжмережевий екран веб-додатків (Web Application Firewall, WAF), здатний блокувати складні атаки на інфраструктуру.

— Інтеграція з базами Threat Intelligence: Ефективність роботи IPS безпосередньо залежить від актуальності її правил. Suricata підтримує динамічне завантаження глобальних баз даних індикаторів компрометації. Це дозволяє системі розпізнавати сигнатури відомих шкідливих програм та блокувати цілеспрямовані атаки ще на периметрі мережі, до того як вони досягнуть цільових серверів або абонентського обладнання.

— Робота в режимі Inline IPS: Завдяки тісній інтеграції з пакетним фільтром операційної системи, Suricata налаштовується в режимі запобігання Inline mode. При виявленні збігу із сигнатурою загрози, зловмисний пакет миттєво

відкидається, а IP-адреса нападника може бути автоматично занесена до чорного списку фаєрвола для тимчасового або постійного блокування [44].

2.6 Захист серверного сегмента мережі

Демілітаризована зона є найбільш вразливим елементом інфраструктури провайдера, оскільки розміщені в ній сервери за визначенням повинні приймати вхідні з'єднання з глобальної мережі. Покладатися виключно на магістральний міжмережевий екран є небезпечним: у разі експлуатації вразливості нульового дня або помилки в конфігурації маршрутизатора, зловмисник отримає безперешкодний доступ до сервера. Тому архітектура безпеки вимагає реалізації концепції ешелонованої оборони, де кожен хост має власну автономну підсистему захисту.

Хостове екранування UFW. Першим рівнем локального захисту серверів під управлінням ОС Ubuntu є впровадження хостового міжмережевого екрана Uncomplicated Firewall. Його використання є необхідністю для створення жорсткої політики «Default Deny» безпосередньо на рівні ядра операційної системи сервера. Навіть якщо магістральний шлюз пропустить небажаний трафік у DMZ, UFW заблокує будь-які звернення до закритих технологічних портів. Крім того, хостовий фаєрвол є критично важливим для запобігання горизонтальному переміщенню: якщо зловмисник якимось чином скомпрометує один із серверів у DMZ, UFW не дозволить йому ініціювати несанкціоновані з'єднання з сусідніми машинами у тому ж фізичному сегменті [49].

Динамічна протидія перебору паролів Fail2Ban. Магістральні системи IDS/IPS ефективно відбивають масовані мережеві атаки, проте вони можуть пропускати низькоінтенсивні атаки прикладного рівня, такі як повільний перебір паролів до служб віддаленого адміністрування SSH. Для вирішення цієї проблеми обрано інструмент Fail2Ban. Його перевага полягає у принципі локального парсингу: програма в реальному часі аналізує системні журнали сервера і, виявивши серію невдалих спроб авторизації з однієї IP-адреси, автоматично створює блокуюче правило в UFW на заданий проміжок часу. Це робить сервер

здатним самостійно та динамічно реагувати на цілеспрямовані атаки без втручання адміністратора [47].

Політики та криптографічний захист доступу. Найбільш надійним методом захисту від крадіжки облікових даних є повна відмова від використання паролів. У рамках розробки системи безпеки обґрунтовано впровадження жорстких політик для служб адміністрування. Доступ до серверів DMZ по протоколу SSH через паролі повністю вимикається на рівні конфігурації демона. Натомість авторизація здійснюється виключно за допомогою асиметричної криптографії з використанням алгоритму Ed25519. Вибір саме цього стандарту на основі еліптичних кривих зумовлений його значними перевагами над застарілим RSA: ключі Ed25519 генеруються швидше, мають значно менший розмір, забезпечують вищий рівень криптостійкості та є апаратно стійкими до атак побічними каналами.

2.7 Система централізованого моніторингу та аудиту

Інфраструктура провайдера створює величезні масиви телеметричних даних. Мережеве обладнання, системи запобігання вторгненням та локальні сервери генерують тисячі журналів подій щосекунди. За таких умов ручний аналіз логів адміністраторами є фізично неможливим, що призводить до несвоєчасного виявлення кіберінцидентів. Для забезпечення проактивної безпеки архітектура мережі повинна включати єдиний центр управління подіями безпеки SIEM, який здатен автоматично збирати, нормалізувати та корелювати дані з усіх ешелонів захисту.

Для реалізації системи централізованого аудиту обрано платформу Wazuh. Це сучасне рішення з відкритим вихідним кодом, яке концептуально відрізняється від класичних збирачів логів. Wazuh поєднує в собі функціонал традиційної SIEM-системи та системи виявлення загроз на кінцевих точках. Його архітектура базується на використанні легковагових агентів, які встановлюються безпосередньо на цільові сервери та передають уже частково оброблену телеметрію на центральний сервер управління по захищеному каналу зв'язку [63]. Вибір Wazuh для захисту інфраструктури провайдера обґрунтовується наявністю трьох

критично важливих підсистем, які ідеально закривають потреби моніторингу:

— **Безперервний контроль цілісності файлів:** Агенти Wazuh безперервно відстежують стан критичних конфігураційних файлів системи. Будь-яка несанкціонована зміна, видалення файлу або модифікація прав доступу миттєво фіксується і передається на сервер моніторингу як інцидент високого рівня критичності.

— **Автоматизований аудит безпеки:** Система регулярно проводить сканування серверів на відповідність глобальним стандартам безпеки. Вона автоматично виявляє слабкі місця в конфігурації операційної системи і надає інженерам готові рекомендації щодо їх усунення.

— **Автоматичне виявлення вразливостей:** Wazuh інтегрується з глобальними базами даних CVE (Common Vulnerabilities and Exposures). Система здатна інвентаризувати всі встановлені пакети на серверах Ubuntu і в реальному часі сигналізувати, якщо для певного програмного забезпечення (наприклад, старої версії веб-сервера) була опублікована критична вразливість.

Завдяки впровадженню цієї системи, інженерний персонал отримує єдину консоль, де корелюються події з міжмережевого екрана pfSense, системи виявлення вторгнень Suricata та локальних серверів, що дозволяє миттєво реагувати на складні, багаторівневі кібератаки.

2.8 Захищений віддалений доступ

Безпека адміністративного доступу до обладнання є складовою загальної стійкості мережі. Виведення портів управління безпосередньо у глобальну мережу є критичним порушенням політик безпеки, оскільки це миттєво робить їх мішенню для автоматизованого сканування та атак типу Brute-force. Згідно з розробленою архітектурою, управління інфраструктурою провайдера має здійснюватися виключно через ізольований сегмент. Щоб надати інженерам можливість віддалено та безпечно потрапляти до нього через недовірене середовище, необхідно впровадити надійний механізм віртуальних приватних мереж VPN.

Індустріальними стандартами для побудови адміністративних тунелів залишалися протоколи IPsec та OpenVPN. Проте їх використання у сучасних

високонавантажених системах має низку недоліків. Протокол IPsec є надзвичайно складним у конфігуруванні, складається з багатьох під протоколів часто має проблеми з проходженням транзитного трафіку через пристрої, що виконують трансляцію адрес NAT [56]. OpenVPN є рішенням, яке працює у просторі користувача. Це означає, що кожен зашифрований пакет змушений проходити багаторазове перемикання контексту між ядром операційної системи та простором користувача, що вносить помітні мережеві затримки при інтерактивному адмініструванні. OpenVPN має кодову базу з сотні тисяч рядків, що робить її повноцінний аудит на наявність вразливостей вкрай складним завданням [57].

Для організації захищеного каналу віддаленого адміністрування обрано сучасний протокол WireGuard. Головною архітектурною перевагою цього рішення є його інтеграція безпосередньо в простір ядра операційної системи шлюзу. Завдяки цьому маршрутизація та шифрування пакетів відбуваються на максимально можливій швидкості без затримок, що є критично важливим для комфортної роботи інженерів у командному рядку. Вибір WireGuard обґрунтовується також його безкомпромісним підходом до криптографії та безпеки. На відміну від застарілих протоколів, які підтримують сотні комбінацій різних шифрів, він використовує фіксований набір найсучасніших криптографічних мотедів. Для симетричного шифрування застосовується високошвидкісний алгоритм ChaCha20 з автентифікацією Poly1305, а для безпечного обміну ключами еліптична крива Curve25519. Важливою інженерною особливістю є і мінімалістичність протоколу: уся його логіка вміщується приблизно у 4000 рядків коду. Це мінімізує площу атаки і дозволяє легко верифікувати безпеку тунелю [58].

У межах розробленої системи WireGuard розгортається на базі pfSense і функціонує за скритним принципом: його слухаючий UDP-порт не відповідає на неавторизовані запити, залишаючись абсолютно невидимим для зовнішніх сканерів мережі. Успішно ініціювавши з'єднання за допомогою асиметричних ключів, інженер отримує маршрутизацію у фізично виділену підмережу управління, звідки може безпечно адмініструвати всі вузли провайдера.

3 ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ СИСТЕМИ БЕЗПЕКИ

3.1 Опис структурно-логічної топології реалізованої мережі

Основою для програмно-технічної реалізації комплексної системи захисту стала розроблена модель мережі, що базується на принципах суворого апаратного та логічного розмежування зон довіри. Загальна топологія побудованого інженерного стенда, яка ілюструє взаємодію ключових вузлів, маршрутизацію трафіку та точки підключення засобів безпеки, наведена на рисунку 3.1

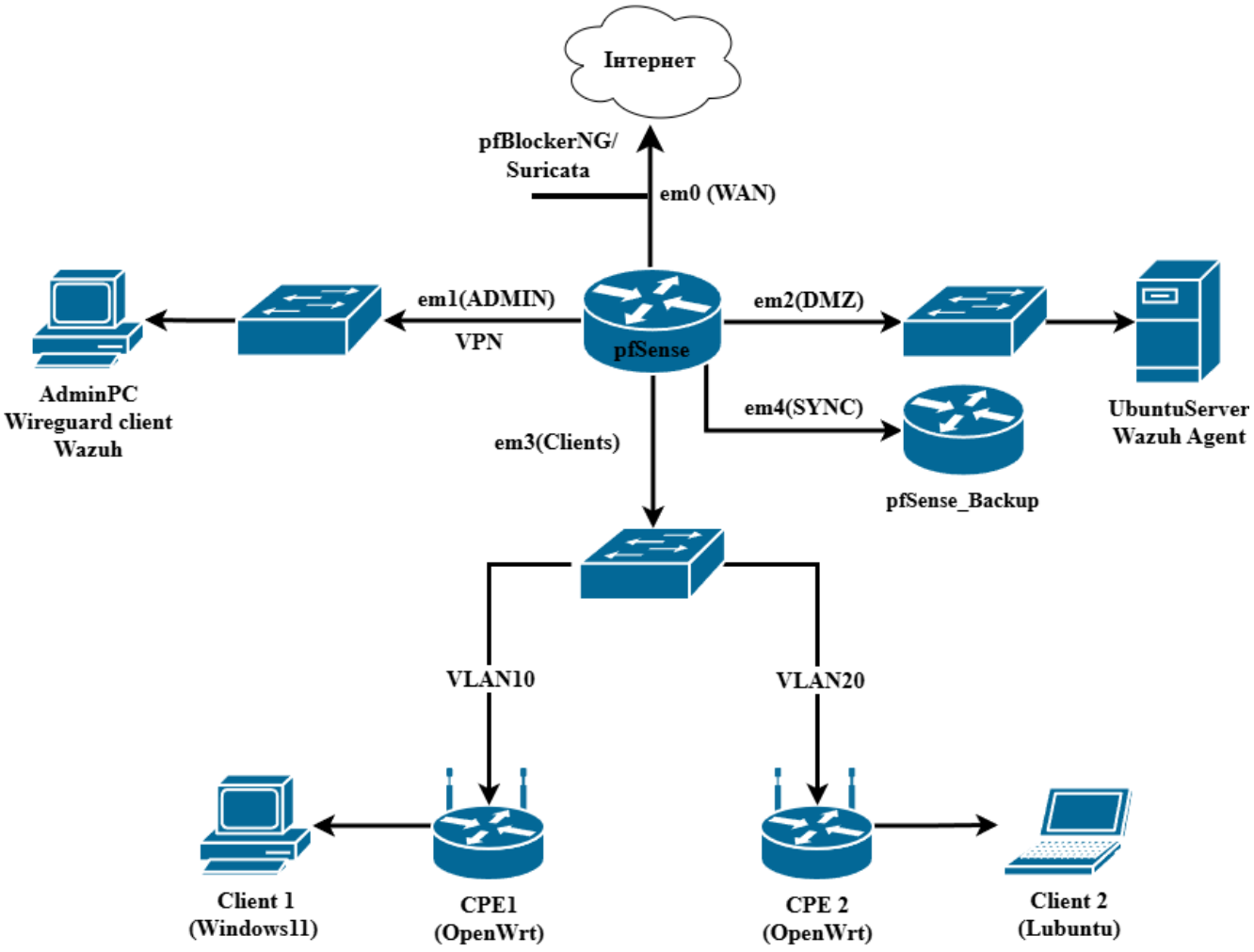

Рисунок 3.1 – Структурно-логічна топологія мережі провайдера та розподіл зон безпеки

Центральним маршрутизуючим ядром інфраструктури виступає відмовостійкий HA-кластер на базі комплексу pfSense. Він складається з основного Master та резервного Backup вузлів, виконуючи роль головного шлюзу

замовчуванням для всіх підмереж. Підключення до інтернету реалізовано через транзитний фізичний інтерфейс em0 WAN, на якому розгорнуто первинні ешелони захисту та підсистеми запобігання вторгненням.

Відповідно до концепції ізоляції критичних активів, сервісна зона та сегмент управління апаратно відокремлені від абонентів. Демілітаризована зона DMZ виведена на окремий інтерфейс em2. Тут розміщено цільовий сервер під управлінням ОС Ubuntu Server , який обслуговує публічні вебсервіси Nginx та виступає кінцевою точкою для моніторингу SIEM. Управління всім активним обладнанням здійснюється виключно через ізольовану мережу, закріплену за портом em1 ADMIN. Для забезпечення роботи технології High Availability задіяно інтерфейс em4 SYNC. Винесення службового трафіку кластеризації на окремий фізичний лінк дозволяє уникнути перевантаження та захищає інфраструктуру від перехоплення. Зв'язок із клієнтським сегментом організовано через високошвидкісний магістральний порт em3 CLIENTS, що працює в режимі Trunk-каналу. Абонентська мережа побудована виключно з використанням логічної мікросегментації. Клієнтські пристрої на базі OpenWrt забезпечують підключення віртуальних каналів VLAN 10 та VLAN 20. Це гарантує повну ізоляцію кінцевого обладнання абонентів на канальному рівні та дозволяє шлюзу індивідуально застосовувати політики контролю доступу.

3.2 Розгортання та базова конфігурація магістрального міжмережевого екрана

Процес ініціалізації магістрального шлюзу розпочинається з базового апаратного розподілу портів через локальну консоль управління. На цьому етапі фізичні інтерфейси маршрутизатора були попередньо прив'язані до відповідних логічних зон: зовнішній транзитний канал закріплено за em0, мережу управління за em1, демілітаризовану зону за em2, а магістральний канал агрегації абонентів за em3 [25]. На рисунку 3.2 відображено первинний розподіл базових інтерфейсів маршрутизатора.

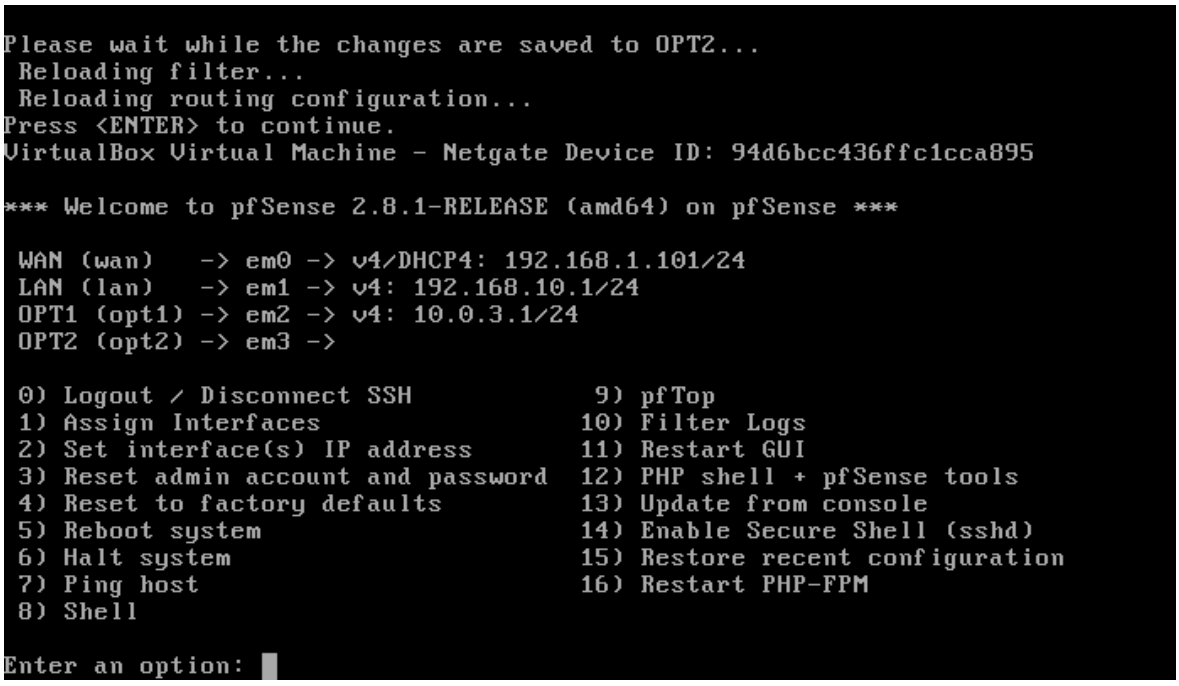

Рисунок 3.2 – Первинний розподіл базових інтерфейсів маршрутизатора

Після первинного налаштування та отримання доступу до графічного веб-інтерфейсу pfSense через ізольовану мережу управління em1, конфігурацію було розширено. Для забезпечення безперервності надання послуг було розпочато розгортання кластера високої доступності. Для ізоляції службового трафіку синхронізації від абонентського середовища, через веб-інтерфейс було додатково ініційовано п'ятий фізичний інтерфейс em4 SYNC. Архітектура відмовостійкості будується на синхронній роботі основного та резервного вузлів. Для резервування шлюзу замовчуванням налаштовано протокол CARP. У межах кожної підмережі було створено віртуальні IP-адреси, які є спільними для обох маршрутизаторів [26]. Загальний вигляд панелі веб-інтерфейсу pfSense наведено на рисунку 3.3, а конфігурування віртуальних IP-адрес протоколу CARP продемонстровано на рисунку 3.4.

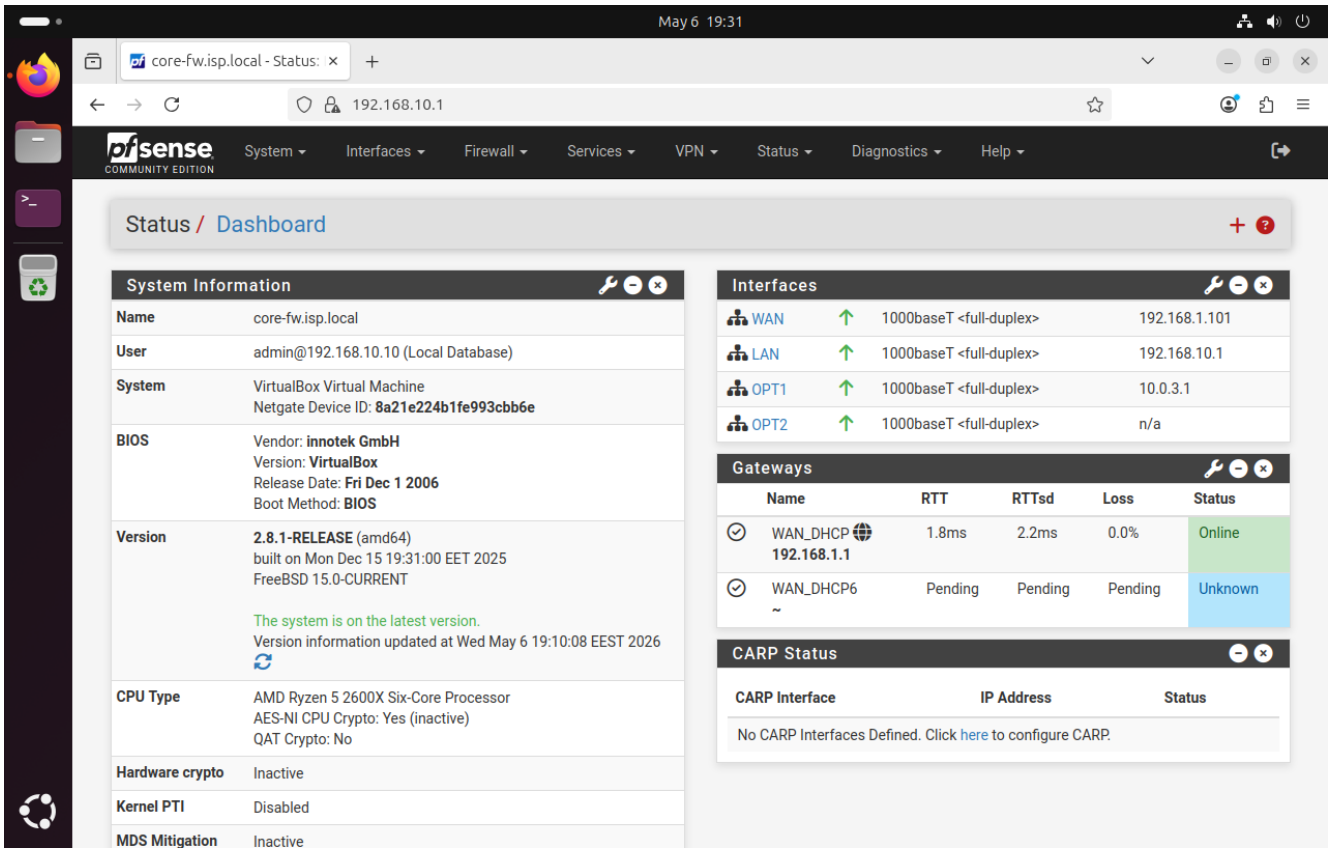

Рисунок 3.3 – Веб-інтерфейс pfSense

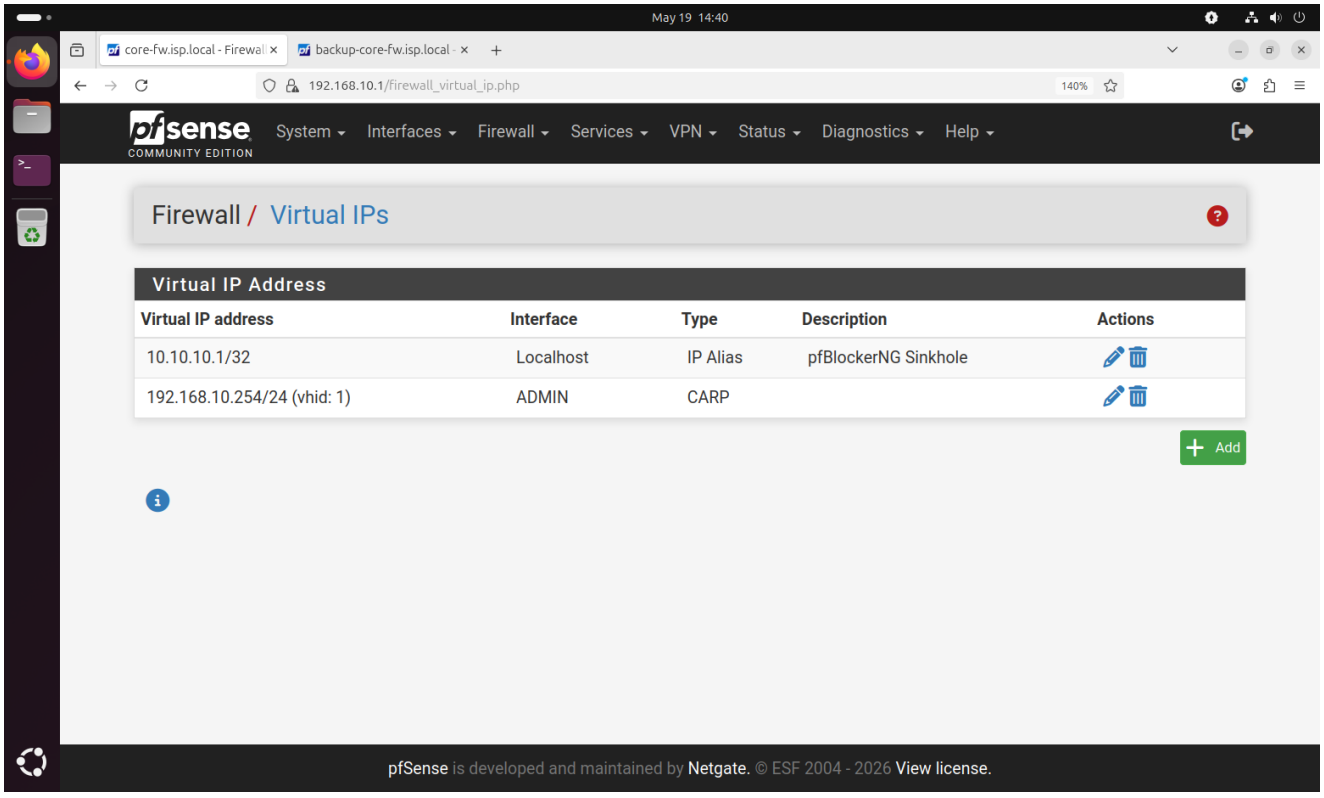

Рисунок 3.4 – Конфігурування віртуальних IP-адрес протоколу CARP

Щоб аварійне перемикання маршрутів відбувалося без розриву активних з'єднань, через виділений лінк em4 було активовано динамічну реплікацію таблиць станів pfsync та синхронізацію конфігурацій XMLRPC Sync. Завершальним етапом розгортання магістрального ядра стала верифікація роботи протоколу CARP на обох вузлах кластера [26].

Під час перевірки статусів було підтверджено, що основний маршрутизатор успішно перебрав на себе віртуальні IP-адреси та перейшов у стан обробки трафіку «MASTER». На рисунку 3.5 відображено статус CARP на основному вузлі кластера.

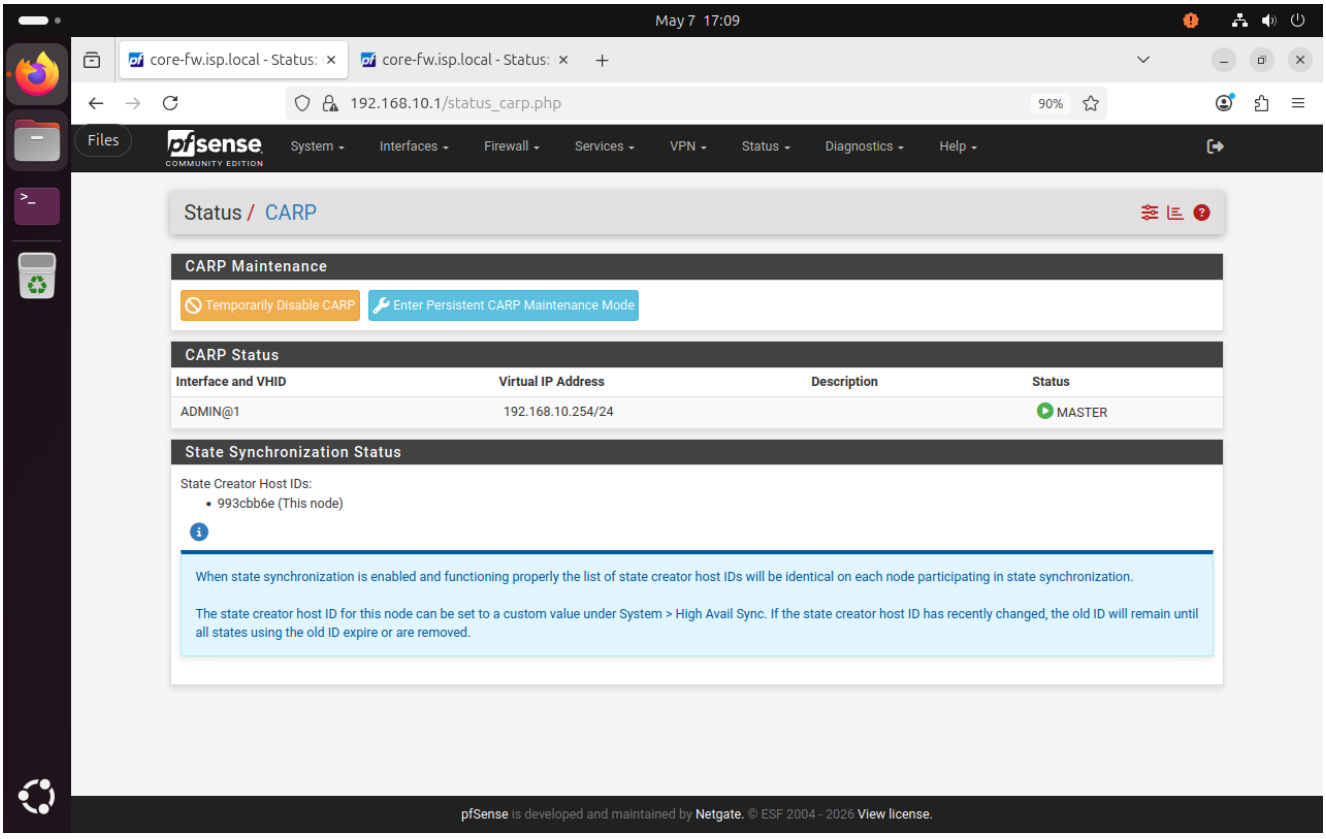

Рисунок 3.5 – Статус CARP на основному вузлі кластера

Перевірка резервного вузла показала, що механізми синхронізації працюють коректно: пристрій отримав актуальну конфігурацію та зафіксував свою готовність до миттєвого перехоплення трафіку у стані «BACKUP». На рисунку 3.6 наведено статус CARP на резервному вузлі кластера.

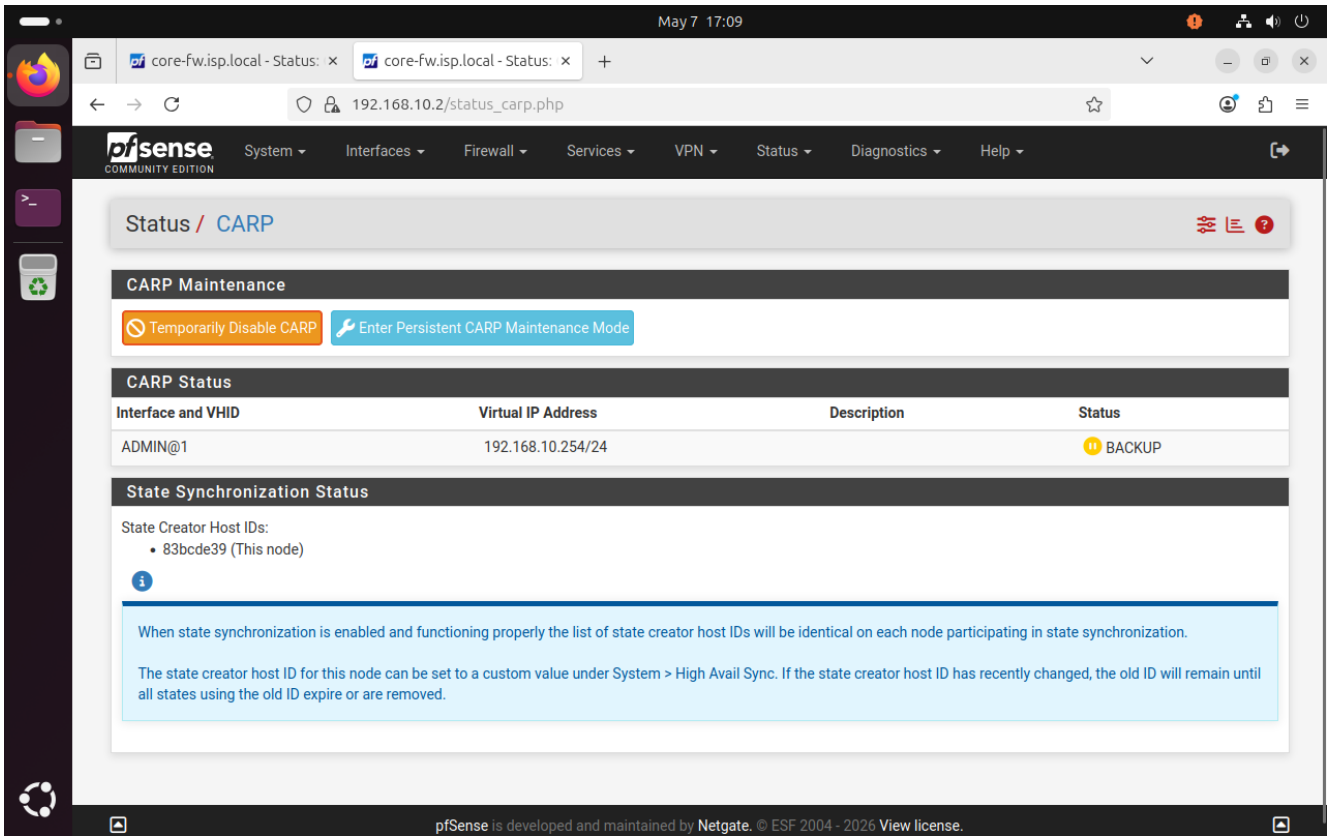

Рисунок 3.6 – Статус CARP на резервному вузлі кластера

3.3 Реалізація сегментації трафіку та IPoE-авторизації абонентів

Після завершення базового налаштування магістрального ядра наступним етапом є конфігурування абонентського сегмента мережі. Відповідно до розробленої архітектури, для забезпечення ізоляції клієнтських потоків на канальному рівні було реалізовано технологію віртуальних локальних мереж VLAN. Базою для створення логічних каналів виступає магістральний інтерфейс em3, який функціонує в режимі Trunk-порту. У веб-інтерфейсі pfSense було проведено ініціалізацію двох віртуальних мереж з унікальними тегами: VLAN 10 та VLAN 20. Кожен створений логічний інтерфейс був прив'язаний до батьківського порту em3 та отримав власну унікальну IP-адресацію, що дозволило повністю розділити широкомовні домени різних абонентських груп. Трафік, який надходить від клієнтських пристроїв, маркується відповідними тегами і передається в ядро мережі, де підлягає незалежній маршрутизації та фільтрації. Конфігурування віртуальних локальних мереж на магістральному інтерфейсі відображено на рисунку 3.7.

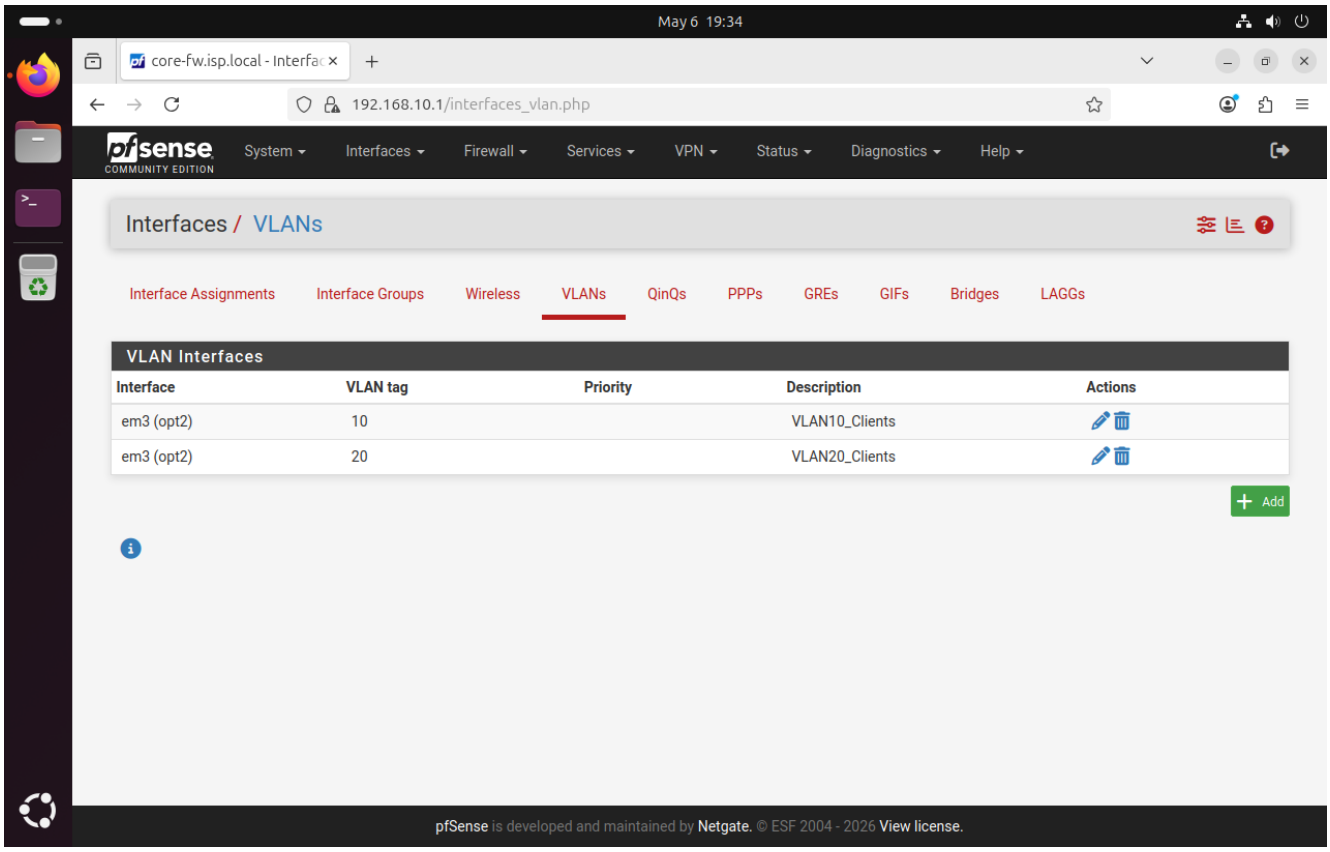

Рисунок 3.7 – Віртуальні локальні мережі на магістральному інтерфейсі

Після ініціалізації віртуальних мереж, нові логічні інтерфейси були закріплені в системі та активовані. Підсумкова конфігурація всіх мережевих інтерфейсів магістрального шлюзу, яка включає як базові фізичні порти: WAN, ADMIN, DMZ, SYNC, так і створені логічні абонентські підмережі на базі Trunk-каналу, відображає повністю сформовану топологію маршрутизатора. Підсумкову таблицю призначених фізичних та логічних інтерфейсів системи наведено на рисунку 3.8.

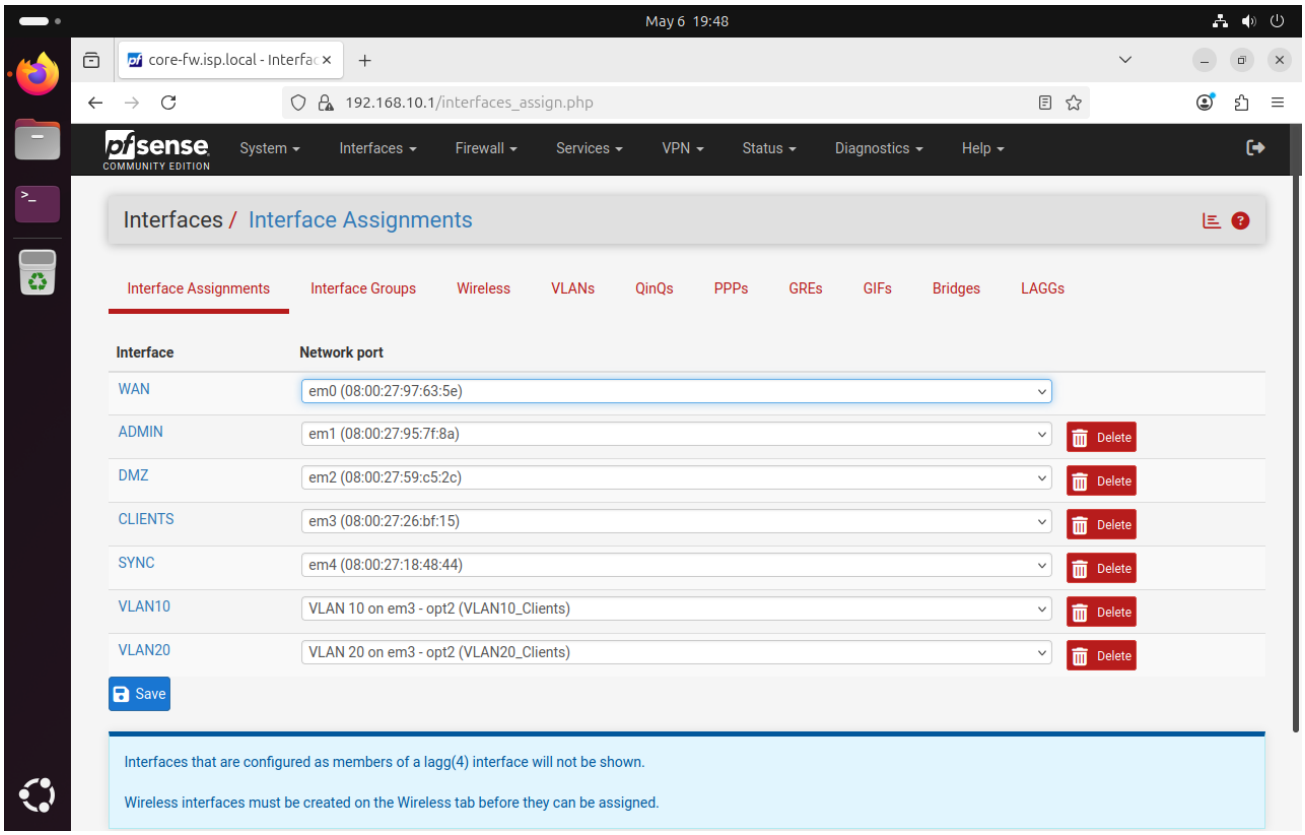

Рисунок 3.8 – Підсумкова таблиця призначених фізичних та логічних інтерфейсів системи

Для автоматизації видачі адресної інформації абонентам у межах створених VLAN-сегментів було активовано та налаштовано службу DHCP. З метою реалізації технології безтунельної авторизації IPoE та запобігання несанкціонованому доступу, видача IP-адрес із випадкового динамічного пулу була повністю обмежена. Замість цього для кожної клієнтської робочої було створено жорсткі статичні прив'язки. У конфігурації DHCP-сервера для кожного абонента було зафіксовано унікальну пару: фізична MAC-адреса мережевої карти клієнтського пристрою та відповідна їй фіксована IP-адреса із дозволеного провайдером підмережевого діапазону [37]. На рисунку 3.9 відображено формування таблиці статичних прив'язок IP та MAC-адрес абонентів.

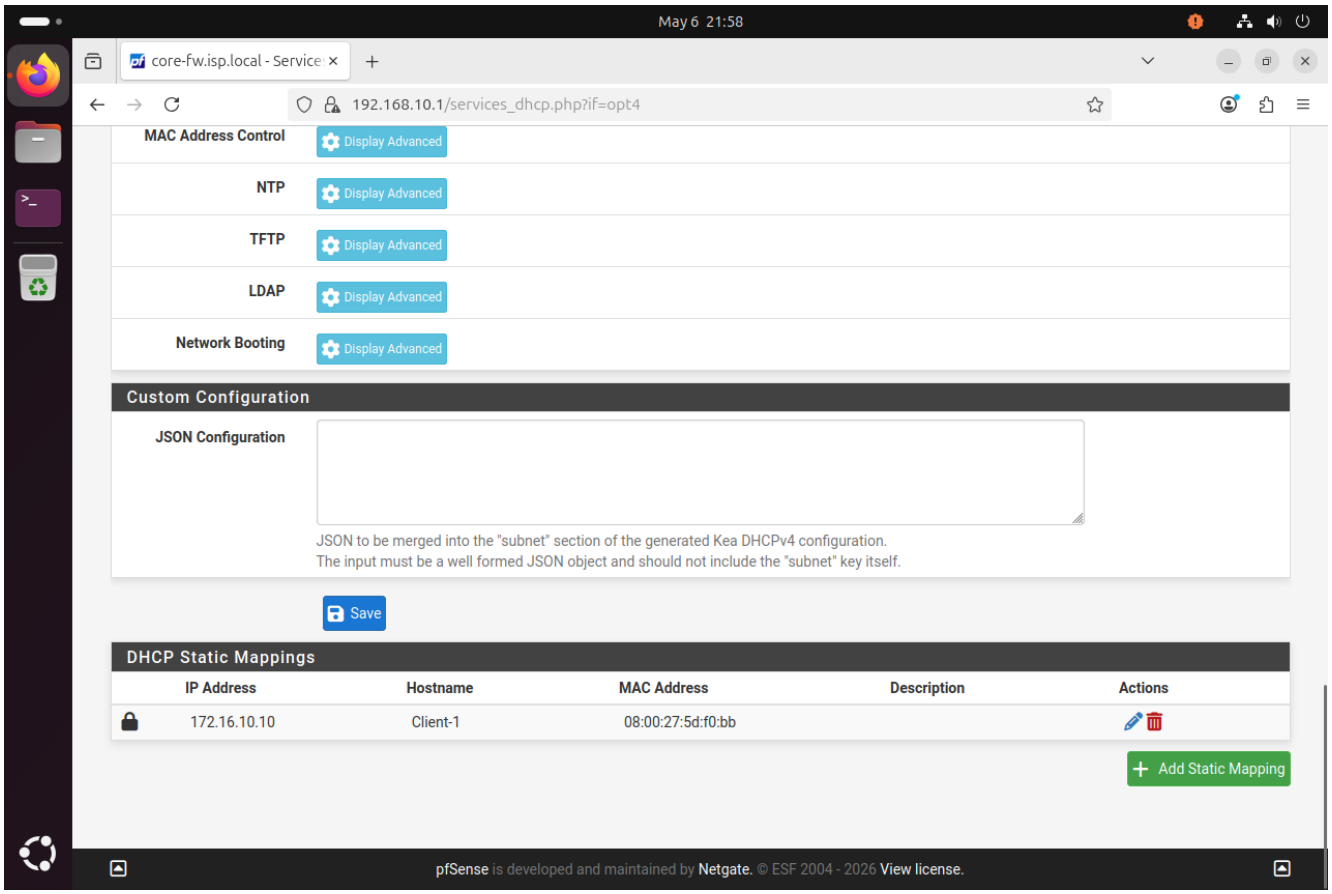

Рисунок 3.9 –Таблиця статичних прив'язок IP та MAC-адрес абонентів

Самого лише створення таблиці DHCP-мапінгів недостатньо для повного захисту мережі, оскільки зловмисник може прописати легітимну IP-адресу на своєму пристрої вручну, в обхід запитів до DHCP-сервера. Для нівелювання цього вектора загрози на налаштованих абонентських інтерфейсах маршрутизатора було активовано режим суворої перевірки Static ARP. Після увімкнення цієї опції пакетний фільтр pfSense повністю припиняє динамічне оновлення таблиці ARP з мережі та ігнорує будь-які сторонні ARP-відповіді. Маршрутизатор приймає та обробляє пакети лише від тих пристроїв, чия пара IP-MAC чітко зафіксована у таблиці DHCP Static Mapping. Трафік від будь-яких незареєстрованих конфігурацій або спроби підміни ідентифікаторів миттєво відкидаються на рівні мережевого драйвера. Активацію режиму суворої перевірки таблиці Static ARP на абонентському інтерфейсі продемонстровано на рисунку 3.10.

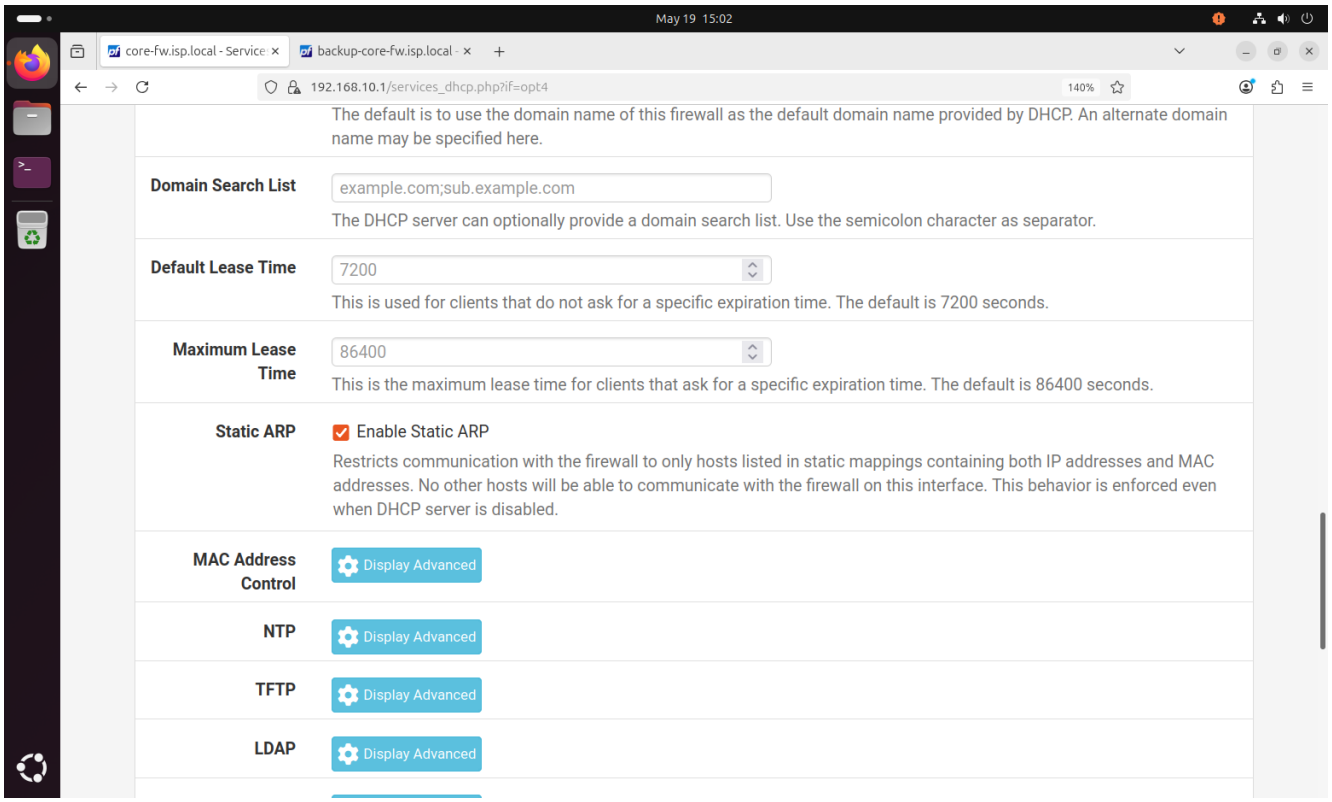

Рисунок 3.10 – Активація режиму суворої перевірки таблиці Static ARP на абонентському інтерфейсі

3.4 Конфігурування правил фільтрації та аліасів міжмережевого екрана

Після формування таблиці з інерфейсами та створення віртуальних абонентських сегментів критично важливою задачею є конфігурування базової політики міжмережевого екранування. За замовчуванням пакетний фільтр pfSense блокує весь транзитний трафік між підмережами. Для оптимізації процесу адміністрування, уникнення дублювання правил та створення гнучкої системи розмежування доступу на першому етапі було реалізовано механізм об'єктів фільтрації Aliases.

У веб-інтерфейсі маршрутизатора було створено спеціалізовані аліаси, які об'єднують групи адрес у логічні блоки. Зокрема, було сформовано об'єкт, який містить діапазони приватних IP-адрес, що використовуються в інфраструктурі провайдера. Використання таких об'єктів дозволяє одним правилом описувати політику ізоляції абонентських VLAN від внутрішніх технологічних ресурсів оператора. Процес створення адресних аліасів у pfSense наведено на рисунку 3.11.

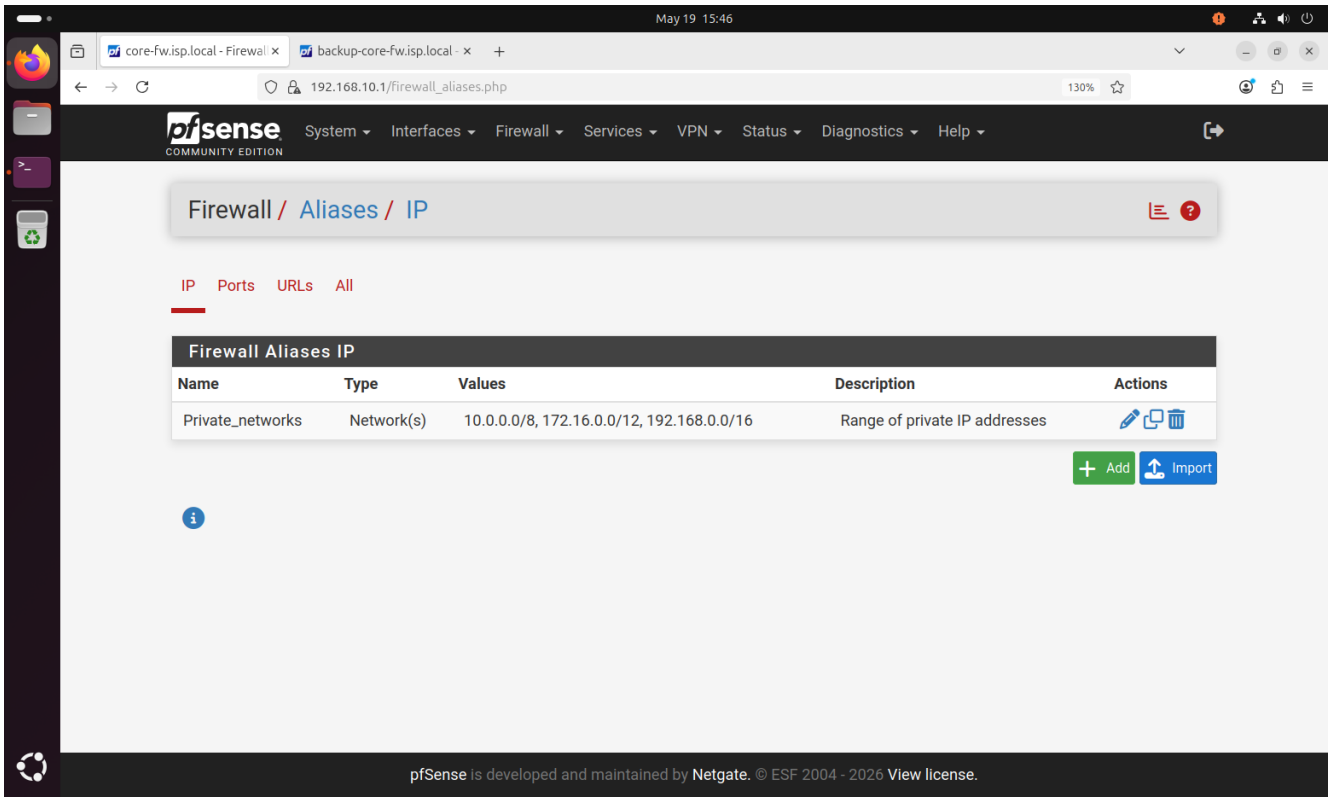

Рисунок 3.11 – Створення адресних аліасів у pfSense

Конфігурування правил виконувалося індивідуально для кожного інтерфейсу на основі принципу мінімальних привілеїв:

1. Зовнішній інтерфейс WAN

Політика зовнішнього інтерфейсу налаштована на суворе відсікання будь-яких неініційованих зсередини з'єднань. У набір правил додано лише два винятки для забезпечення працездатності інфраструктури:

— Дозвіл вхідного UDP-трафіку на порт 51820 для забезпечення підключення адміністраторів до сервера WireGuard VPN.

— Дозвіл вхідного TCP-трафіку на порт 80 HTTP із подальшою трансляцією мережевих адрес на внутрішню IP-адресу цільового сервера в демілітаризованій зоні.

На рисунку 3.12 відображено правила для зовнішнього інтерфейсу WAN.

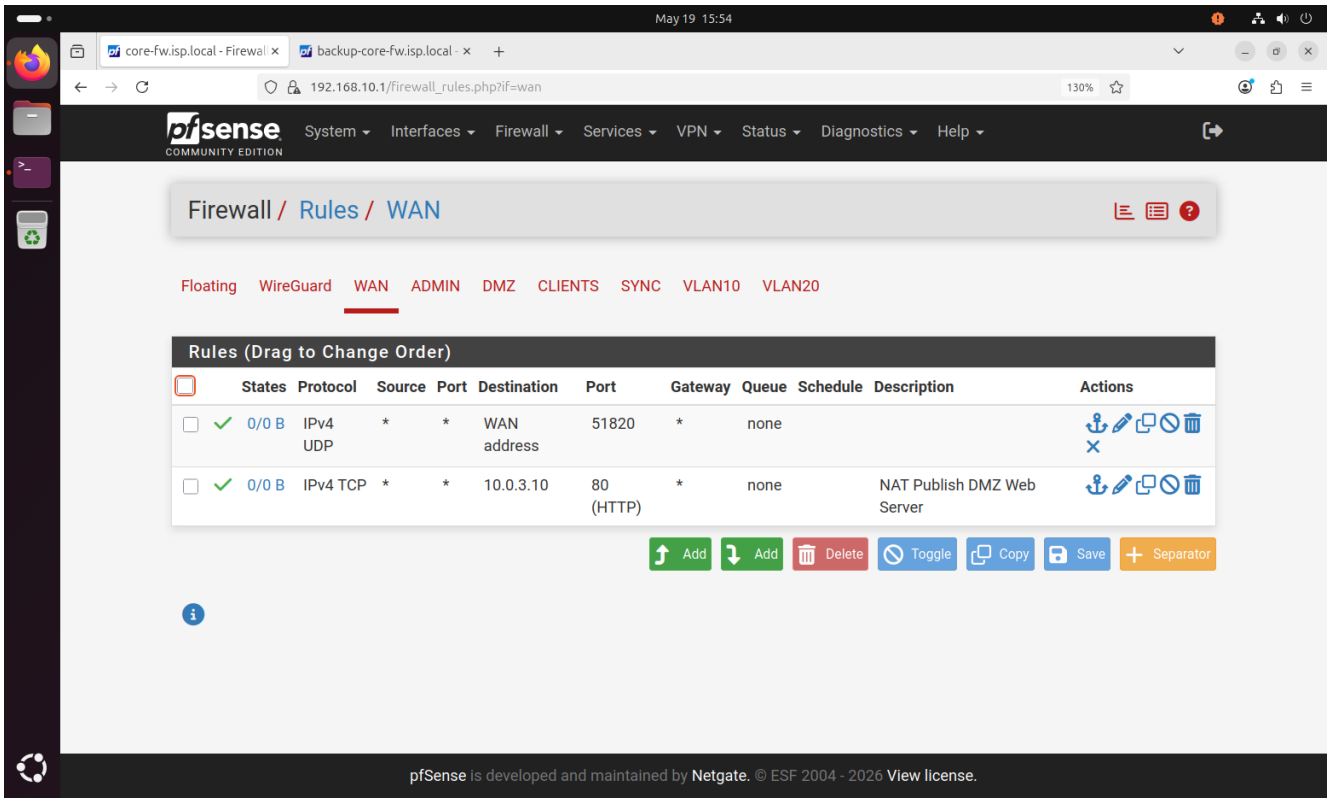

Рисунок 3.12 – Правила для зовнішнього інтерфейсу WAN

2. Сегмент управління ADMIN

Оскільки цей сегмент є ізольованим для управління для нього створено специфічну політику доступу. Робочій станції адміністратора дозволено ініціювати з'єднання з глобальною мережею та технологічними вузлами, проте встановлено жорстке правило блокування будь-якого доступу з підмережі ADMIN до клієнтського адресного простору. Це унеможливлює горизонтальне переміщення зловмисника в абонентські мережі у разі гіпотетичної компрометації комп'ютера адміністратора. Сформовані правила для сегмента ADMIN наведено на рисунку 3.13.

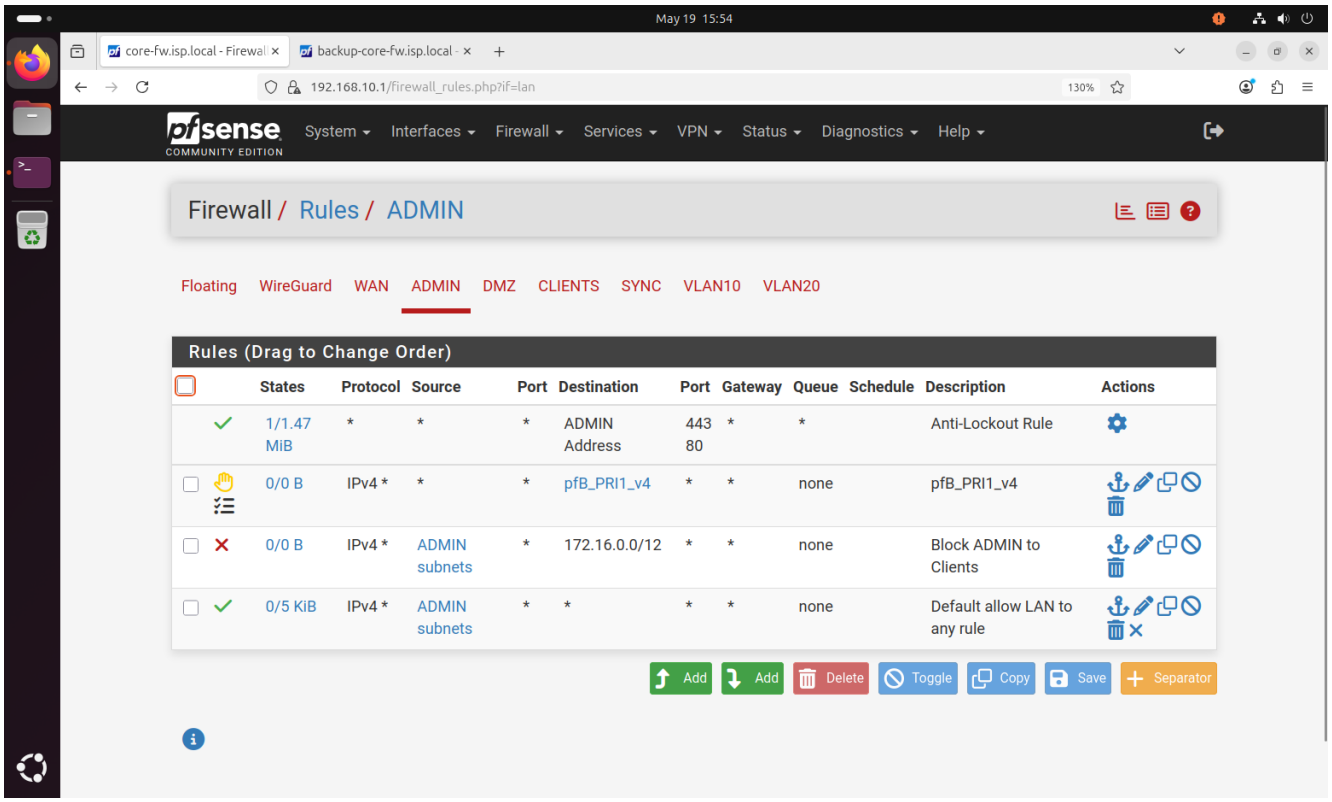

Рисунок 3.13 – Правила для ADMIN

3. Демілітаризована зона DMZ

Для серверного сегменту діє сувора політика ізоляції. Серверам дозволено ініціювати вихідні з'єднання в мережу Інтернет для завантаження оновлень ПЗ. Також створено точкове правило, яке дозволяє локальному агенту Wazuh на Ubuntu Server відправляти телеметрію на центральний менеджер по протоколу TCP порти 1514-1515. Будь-які інші спроби трафіку з DMZ потрапити у внутрішні підмережі провайдера беззастережно блокуються. Правила для DMZ продемонстровано на рисунку 3.14.

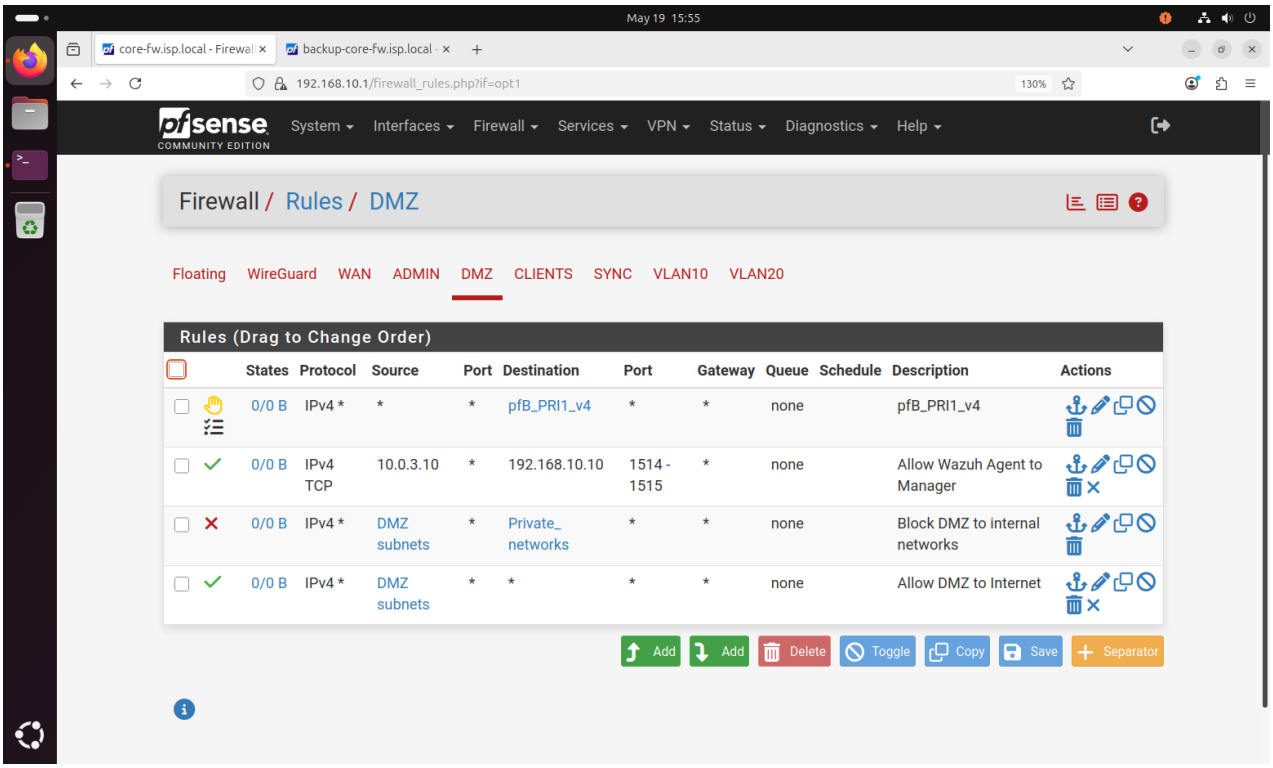

Рисунок 3.14 – Правила для DMZ

4. Абонентські сегменти VLAN 10 та VLAN 20

Для клієнтських віртуальних мереж реалізовано ідентичну, жорстко регламентовану логіку доступу. На кожному з логічних інтерфейсів налаштовано три послідовні правила:

— Дозвіл на доступ до підмережі DMZ для отримання абонентами публічних послуг локального вебсервера.

— Ультимативне блокування доступу до будь-яких інших локальних мереж. Це правило гарантує, що клієнти з VLAN 10 не зможуть потрапити у VLAN 20, а також не матимуть доступу до технологічної мережі управління.

— Дозвіл на вільний доступ до глобальної мережі Інтернет для легітимного абонентського трафіку.

Правила для абонентського сегмента VLAN 10 відображено на рисунку 3.15, а правила для абонентського сегмента VLAN 20 наведено на рисунку 3.16.

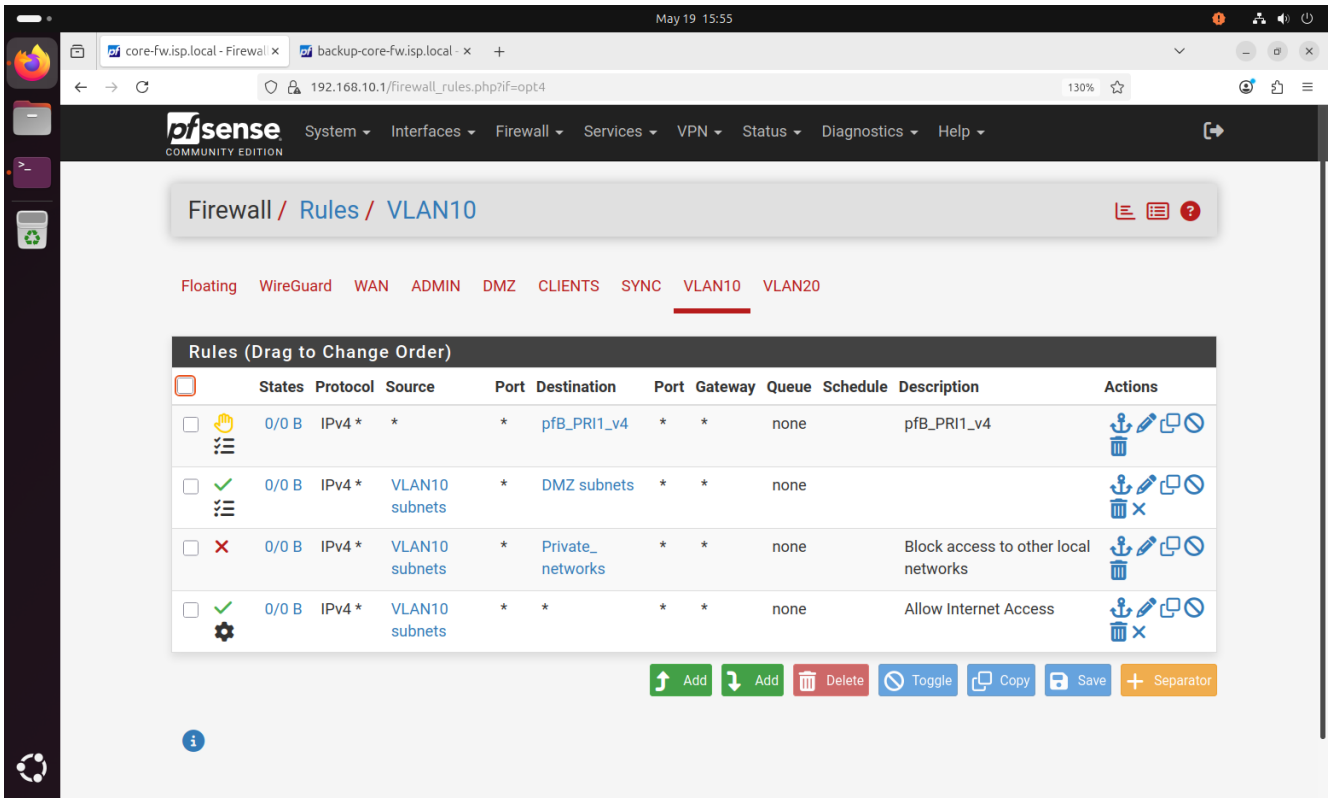

Рисунок 3.15 – Правила для абонентського сегмента VLAN 10

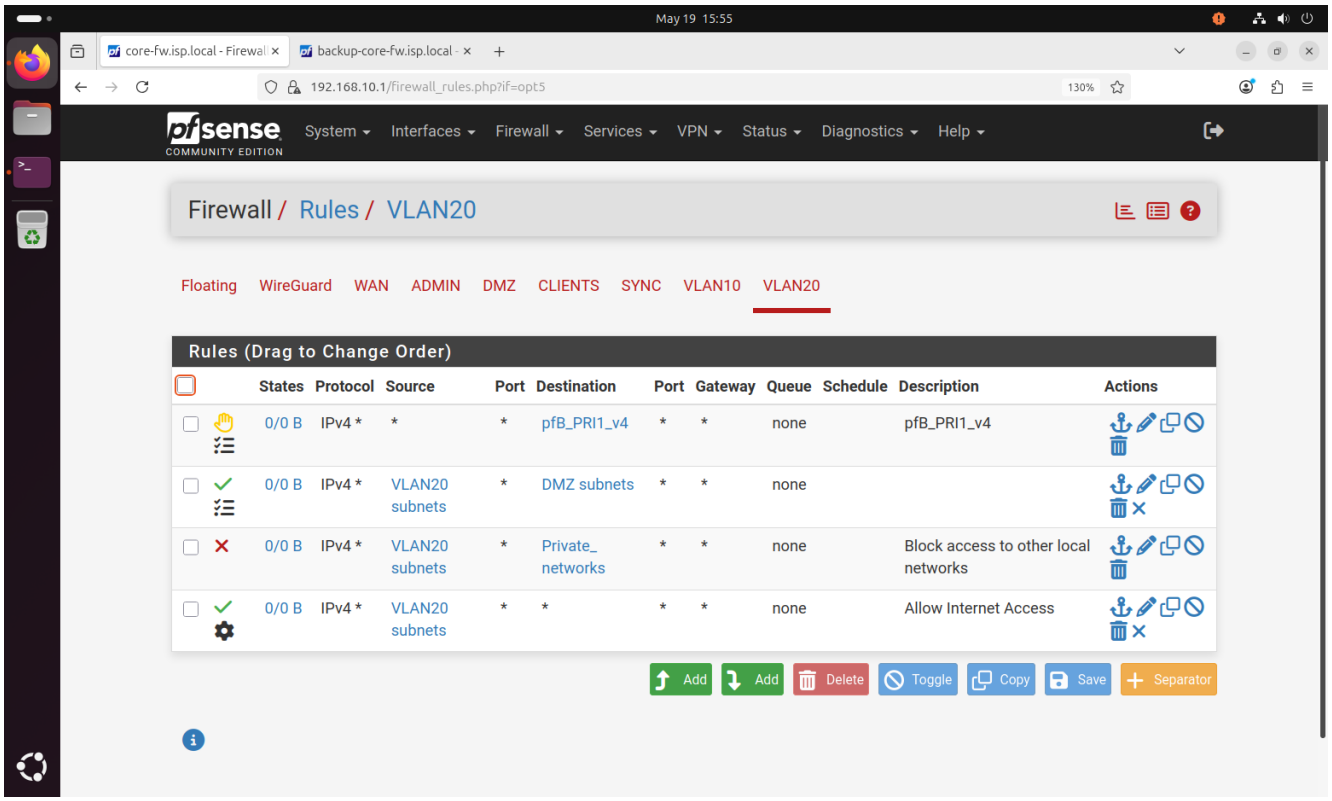

Рисунок 3.16 – Правила для абонентського сегмента VLAN 20

3.5 Налаштування систем інспекції трафіку та обмеження смуги пропускання

Для організації проактивного захисту периметра мережі та контролю транзитних потоків даних було реалізовано комплекс засобів глибокого аналізу пакетів DPI та механізми динамічного керування пропускною здатністю. Конфігурування цих інструментів у межах системи pfSense дозволяє мінімізувати площу атак на сервіси провайдера та захистити інфраструктуру від об'ємних перевантажень.

На першому етапі було виконано розгортання та інтеграцію багатопотокової системи виявлення та запобігання вторгненням Suricata. На відміну від класичних засобів фільтрації, Suricata була активована безпосередньо на інтерфейсах шлюзу для інспекції корисного навантаження пакетів на прикладному рівні. Під час налаштування сервісу інтерфейси були переведені в режим Inline IPS, що дозволяє системі не просто фіксувати аномалії в журналах, а миттєво відкидати шкідливі пакети до того, як вони пройдуть у внутрішні сегменти мережі. Перелік та поточний статус активованих інтерфейсів у системі Suricata наведено на рисунку 3.17.

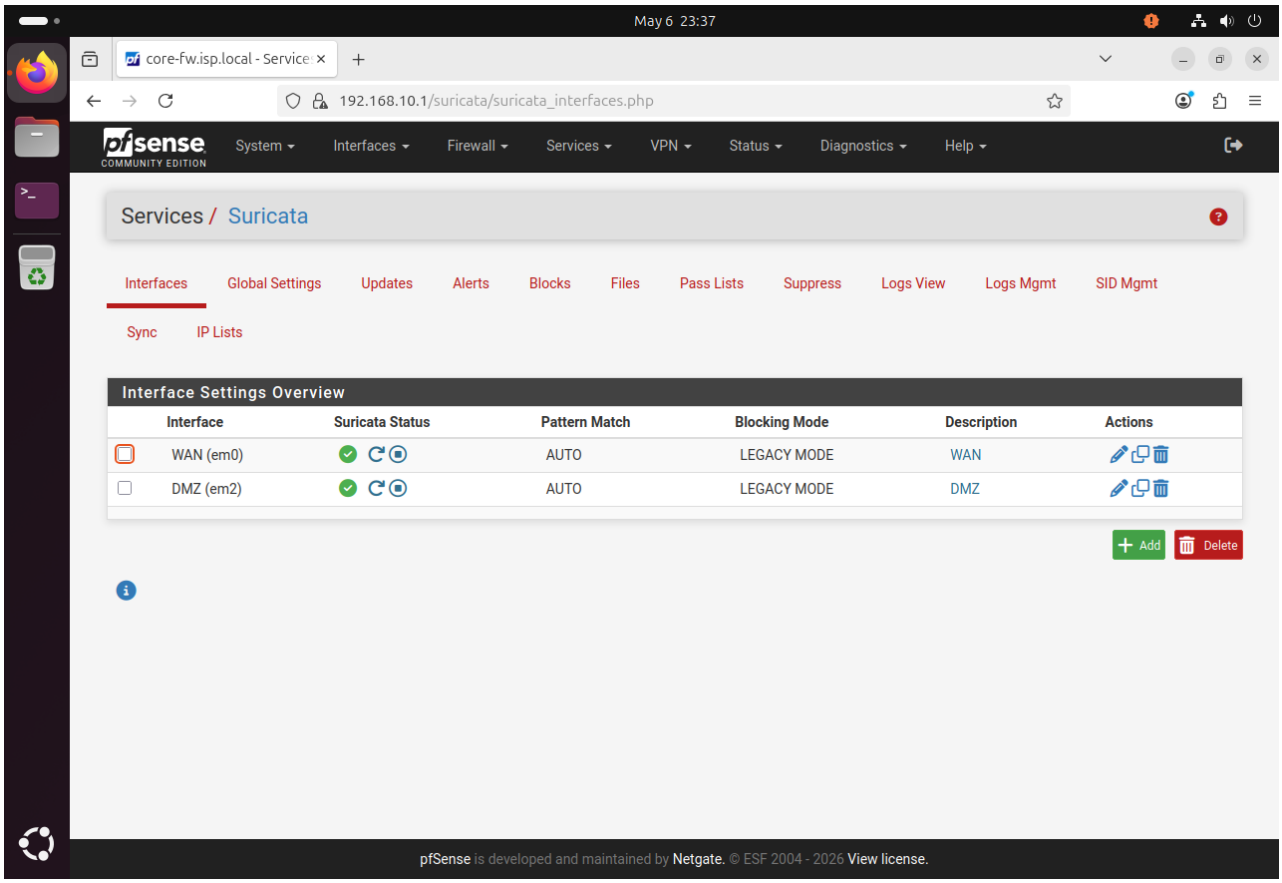

Рисунок 3.17 – Перелік та поточний статус активованих інтерфейсів у системі Suricata

Ефективність функціонування IPS-модуля забезпечується підключенням актуальних сигнатурних наборів. У внутрішніх параметрах Suricata було активовано інтеграцію з глобальними базами даних Threat Intelligence, зокрема правилами Emerging Threats ET Open. Для захисту внутрішніх ресурсів та демілітаризованої зони було увімкнено специфічні категорії сигнатур, орієнтовані на виявлення сканування мережі, експлуатацію вразливостей вебсерверів та ідентифікацію аномальних сплесків трафіку. Конфігурування категорій сигнатурних правил глибокого аналізу трафіку на WAN-інтерфейсі відображено на рисунку 3.18, а на DMZ-інтерфейсі рисунок 3.19.

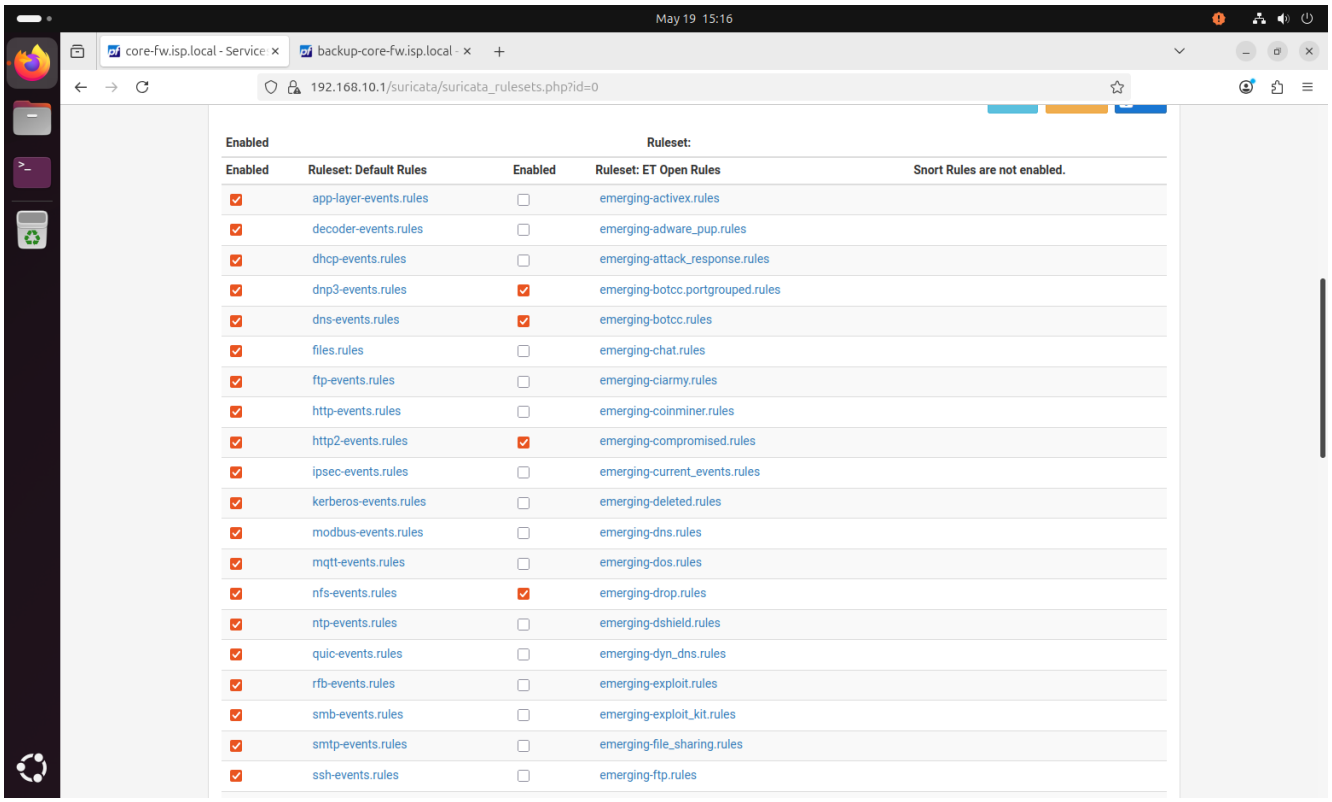

Рисунок 3.18 – Категорії сигнатурних правил глибокого аналізу трафіку на WAN інтерфейс

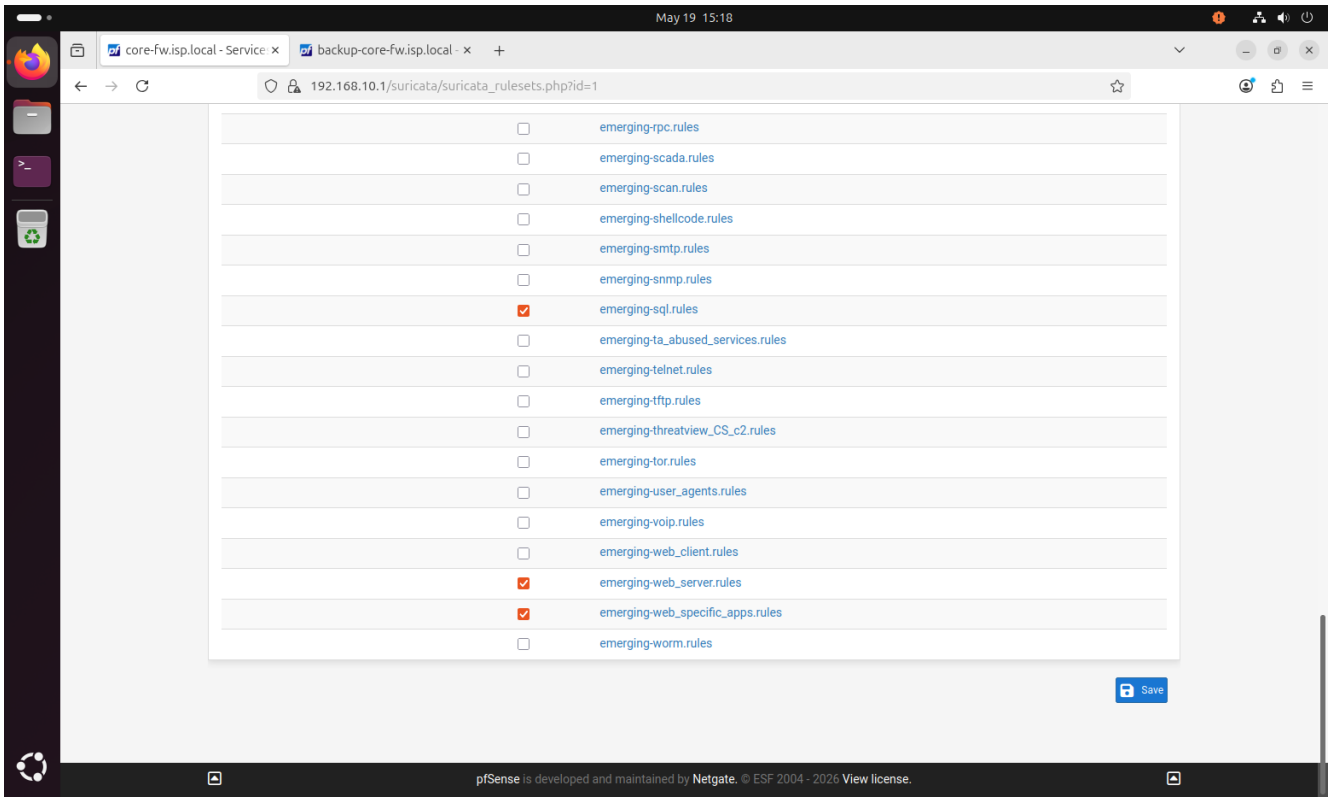

Рисунок 3.19 – Конфігурування категорій сигнатурних правил глибокого аналізу трафіку на DMZ інтерфейс

Для префільтрації шкідливого або паразитного трафіку та захисту клієнтського сегмента від фішингу було задіяно можливості пакета pfBlockerNG. На базі цього інструменту реалізовано технологію DNS Sinkhole. Система аналізує всі DNS-запити, що надходять від абонентів, і у разі спроби звернення до відомих зловмисних чи фішингових доменів, автоматично підміняє IP-адресу у відповіді, спрямовуючи запит на ізольований локальний хост Sinkhole. Це дозволяє заблокувати загрозу ще на етапі ініціалізації з'єднання і суттєво знижує навантаження на процесор маршрутизатора [45]. Конфігурування репутаційних списків та технології DNS Sinkhole продемонстровано на рисунку 3.20.

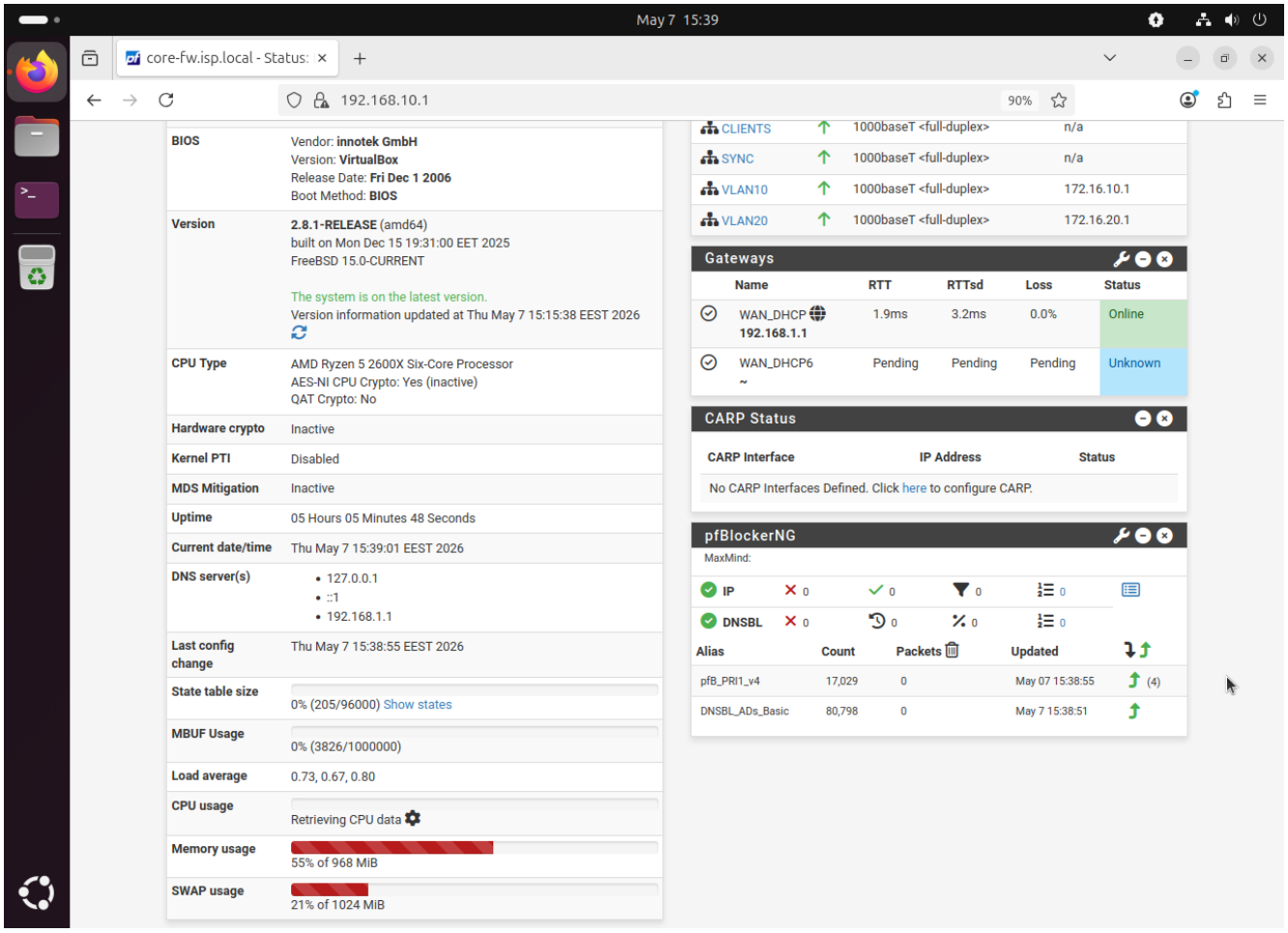

Рисунок 3.20 –Репутаційні списки та технології DNS Sinkhole

Завершальним етапом контролю магістральних каналів стало налаштування підсистеми обмеження швидкості та забезпечення якості обслуговування QoS. Для захисту від об'ємного флуду та гарантування доступності критичних сервісів, у

розділі Traffic Shaper було створено віртуальні обмежувачі Limiters. Через алгоритми безпосередньо в ядрі операційної системи шлюзу було сформовано окремі черги для вхідного Download та вихідного Upload абонентського трафіку. Створені ліміти жорстко обмежують максимальну смугу пропускання для абонентських VLAN, не дозволяючи аномальним сплескам трафіку з клієнтського сегмента перевантажити фізичні інтерфейси ядра мережі чи DMZ. На рисунку 3.21 наведено конфігурування черг Limiters, а на рисунку 3.22 відображено їх додавання до правил для управління пропускною здатністю клієнтських каналів.

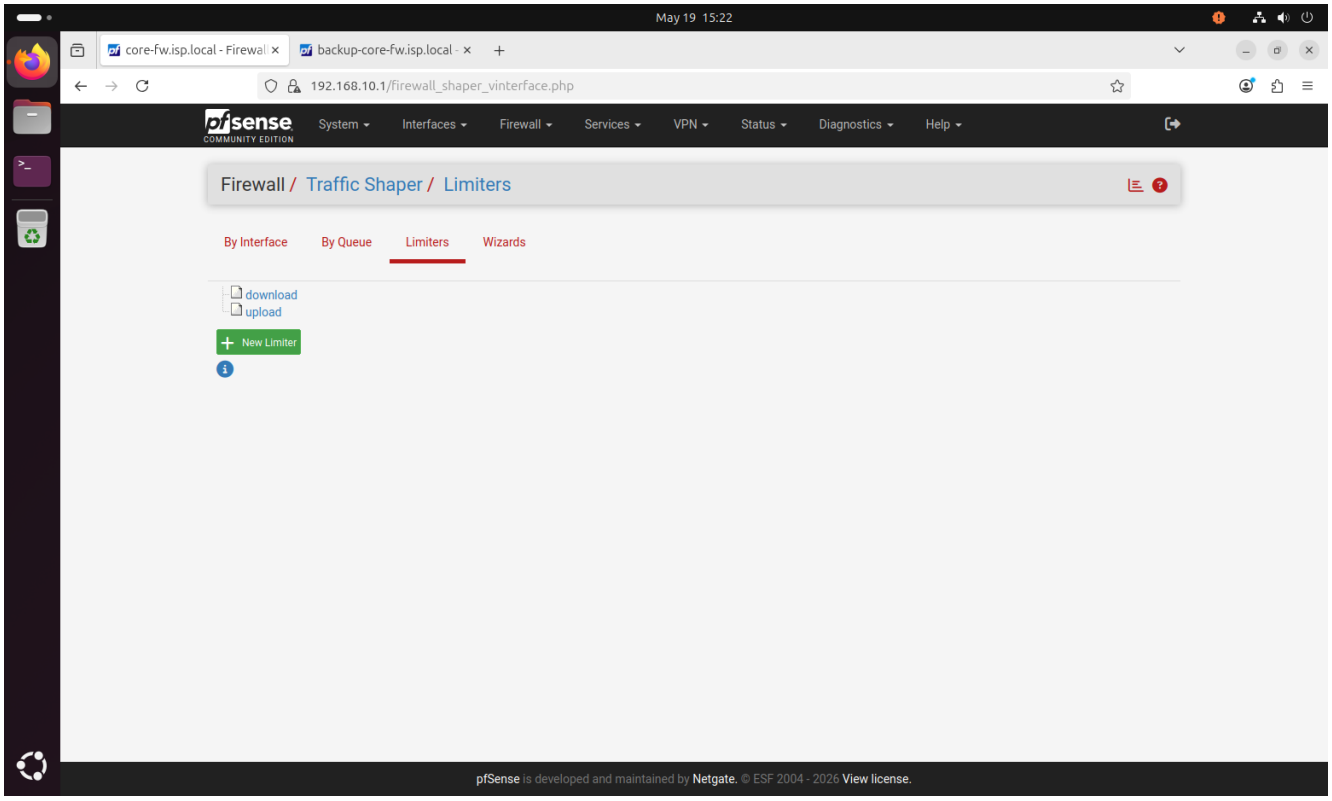

Рисунок 3.21 – Конфігурування черг Limiters для управління пропускною здатністю каналів

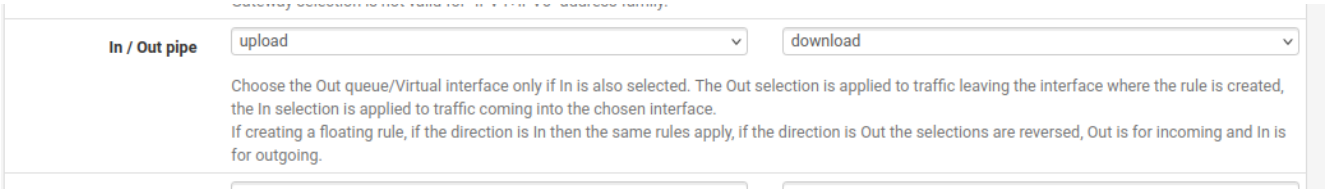

Рисунок 3.22 – Додавання черг Limiters до клієнтів для управління пропускною здатністю каналів

3.6 Конфігурування ешелонованого захисту серверного сегмента

Попри наявність потужних систем інспекції трафіку на магістральному шлюзі, архітектура безпеки вимагає реалізації концепції ешелонованої оборони Демілітаризована зона є найбільш вразливим сегментом мережі, оскільки розташовані в ній сервери приймають вхідні з'єднання з глобальної мережі. Для забезпечення автономної стійкості цільового вузла сервера було впроваджено комплекс заходів хостового захисту.

На початку було розгорнуто та налаштовано локальний міжмережевий екран UFW. Базовою політикою безпеки для сервера було обрано парадигму «Default Deny», тобто заборона всього вхідного трафіку за замовчуванням. У конфігурації UFW було створено винятки лише для критично необхідних служб: дозволено транзит HTTP/HTTPS-трафіку для вебсервера Nginx та обмежено доступ до порту служби SSH. Такий підхід гарантує, що у разі компрометації інших вузлів або прориву периметра зловмисник не зможе отримати доступ до закритих технологічних портів сервера. Конфігурацію правил UFW наведено на рисунку 3.23.

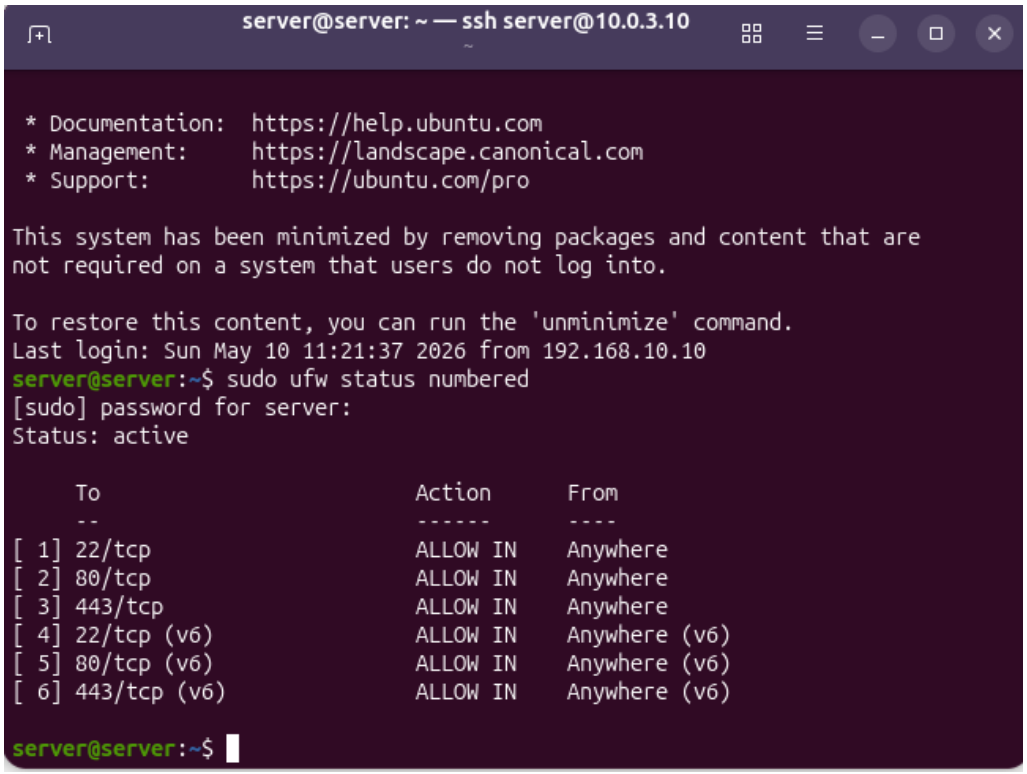

Рисунок 3.23 – Конфігурація правил хостового міжмережевого екрана UFW

Для захисту від автоматизованих низько інтенсивних атак, таких як перебір паролів до служби віддаленого управління, було інтегровано сервіс динамічного блокування Fail2Ban. Система налаштована на безперервний парсинг системних журналів автентифікації. У разі фіксації серії невдалих спроб авторизації з однієї IP-адреси, Fail2Ban автоматично генерує тимчасове блокуюче правило в UFW. Це дозволяє серверу самостійно відбивати атаки прикладного рівня без втручання адміністратора [47]. Статус роботи підсистеми динамічного блокування Fail2Ban відображено на рисунку 3.24.

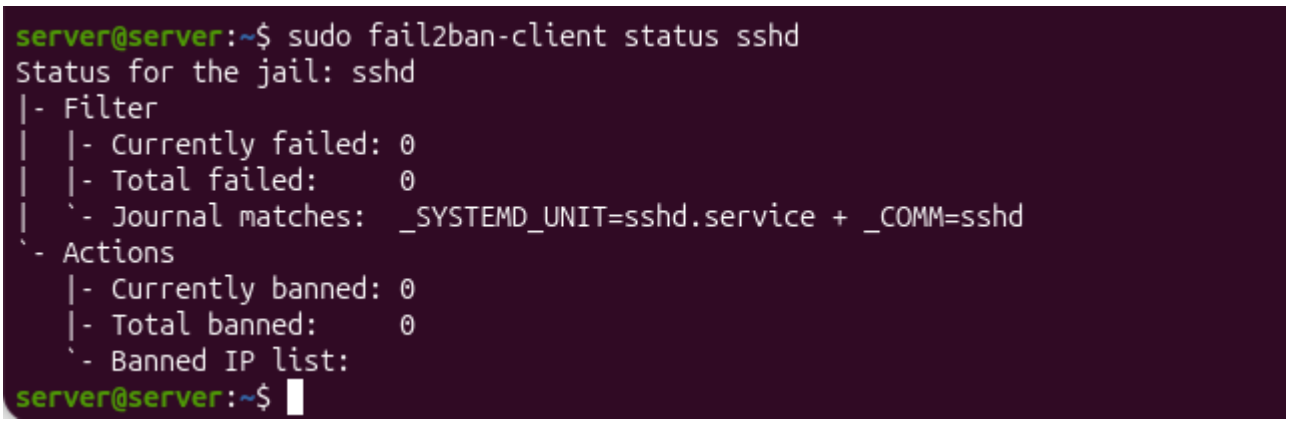

Рисунок 3.24 – Статус роботи підсистеми динамічного блокування Fail2Ban

Найбільш критичним вектором атак на серверну інфраструктуру залишається компрометація облікових даних. З метою повного нівелювання цього ризику було проведено зміцнення служби SSH. У головному конфігураційному файлі демона було деактивовано можливість входу за паролем. Натомість єдиним дозволеним методом авторизації стала асиметрична криптографія з використанням сучасного стандарту ключів Ed25519. Відмова від паролів робить будь-які атаки типу Brute-force чи Dictionary Attack математично недоцільними [52]. Налаштовані параметри захисту служби SSH продемонстровано на рисунку 3.25.

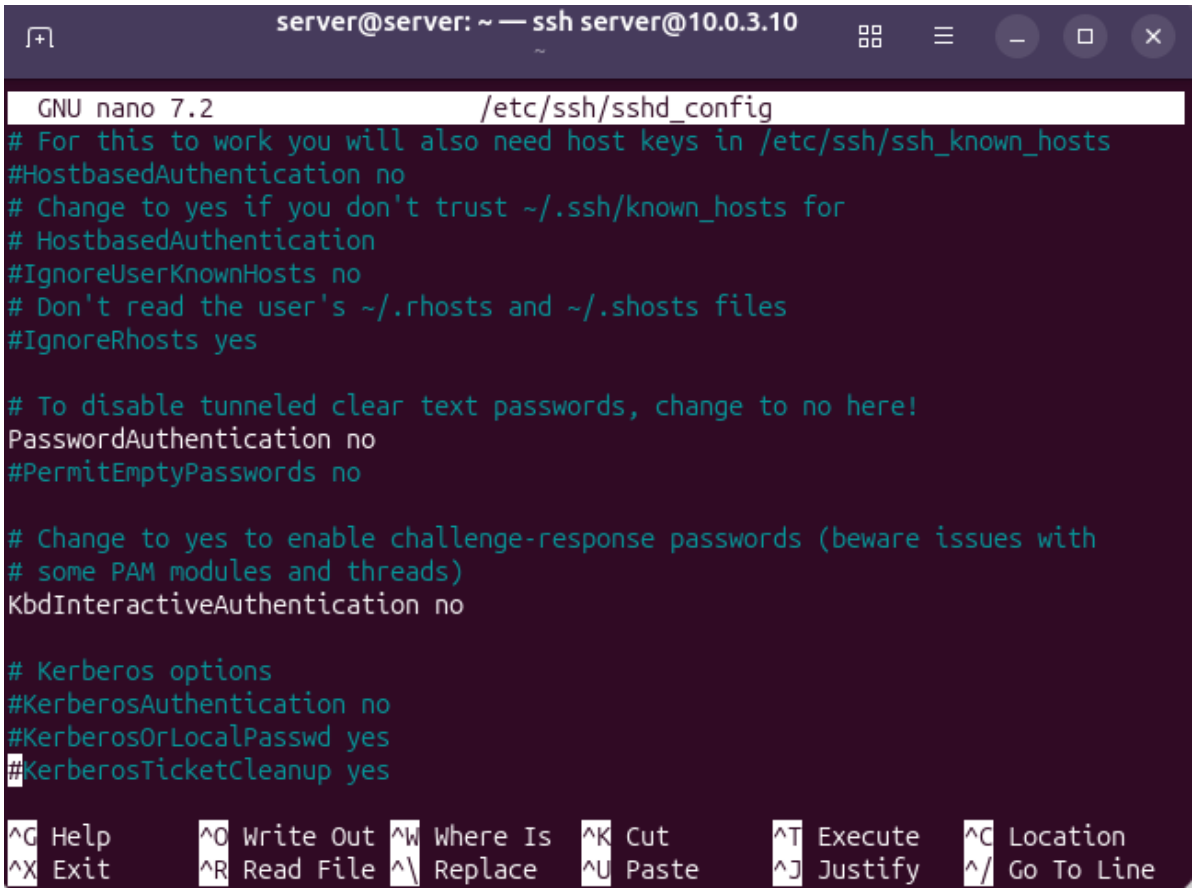

Рисунок 3.25 – Параметри захисту служби SSH

3.7 Інтеграція підсистеми моніторингу та аудиту на базі SIEM Wazuh

Для забезпечення наскрізного контролю безпеки інфраструктури та централізованого аналізу подій у демілітаризованій зоні було реалізовано інтеграцію системи моніторингу класу SIEM/EDR на базі платформи Wazuh. Основним завданням цього етапу є розгортання легковагових агентів на цільових хостах для збору телеметрії, відстеження цілісності конфігурацій та проактивного виявлення ознак компрометації системи.

На першому етапі було виконано встановлення та первинну ініціалізацію Wazuh Agent на цільовому хості під управлінням операційної системи Ubuntu Server. Процес інтеграції включав імпорт офіційного репозиторію, встановлення пакету та внесення змін до конфігураційного файлу, де було чітко визначено IP-адресу центрального менеджера управління Wazuh, що знаходиться у технологічному сегменті. Після запуску служби автентифікація агента відбулася за допомогою криптографічних ключів, а перевірка статусу у веб-консолі SIEM-

системи підтвердила успішне встановлення захищеного каналу зв'язку та перехід хоста у стан активного моніторингу [62]. Верифікацію підключення та поточного статусу агента безпеки в консолі Wazuh наведено на рисунку 3.26.

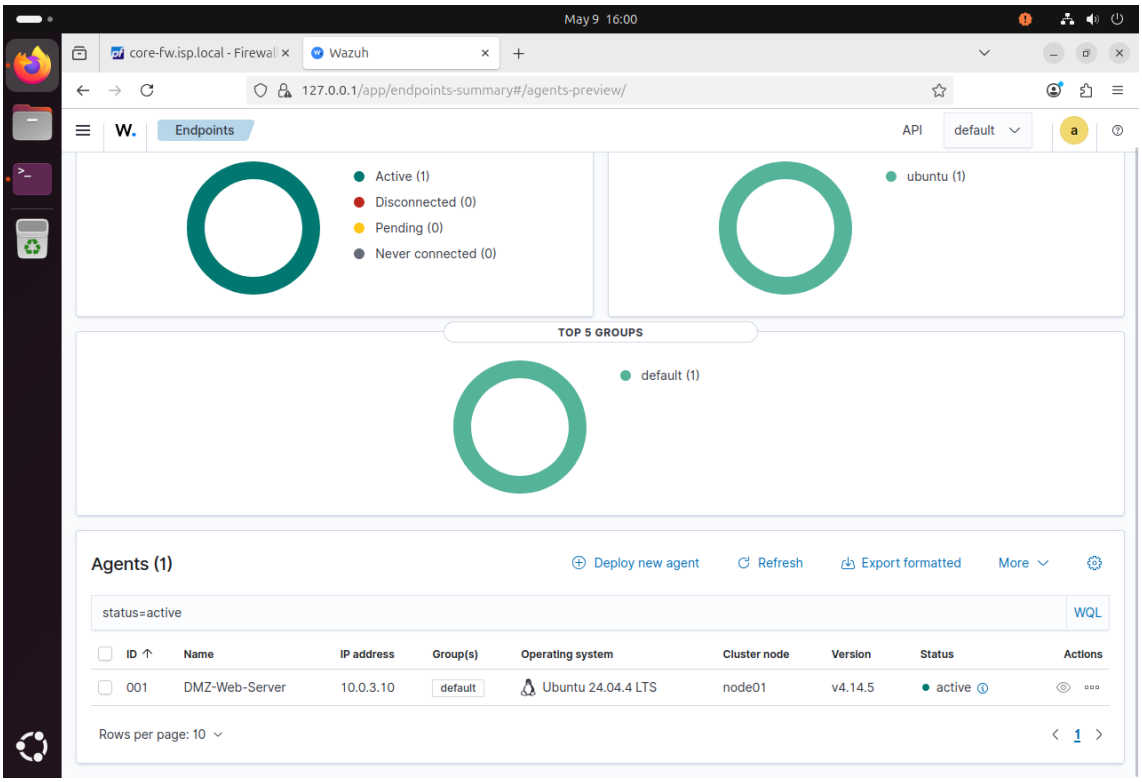

Рисунок 3.26 – Підключення та поточного статусу агента безпеки в консолі Wazuh

Наступним етапом налаштування проактивної оборони хоста стало конфігурування модуля безперервного контролю цілісності файлів FIM. У підсистемі на боці агента було визначено перелік критичних каталогах і файлів конфігурацій, які підлягають регулярному скануванню та перевірці контрольних сум. Будь-яка несанкціонована модифікація, зміна прав доступу або поява сторонніх об'єктів миттєво генерує сповіщення високого рівня критичності у SIEM-системи, дозволяючи адміністраторам миттєво локалізувати спроби несанкціонованого втручання. Процес моніторингу цілісності файлів серверної інфраструктури відображено на рисунку 3.27.

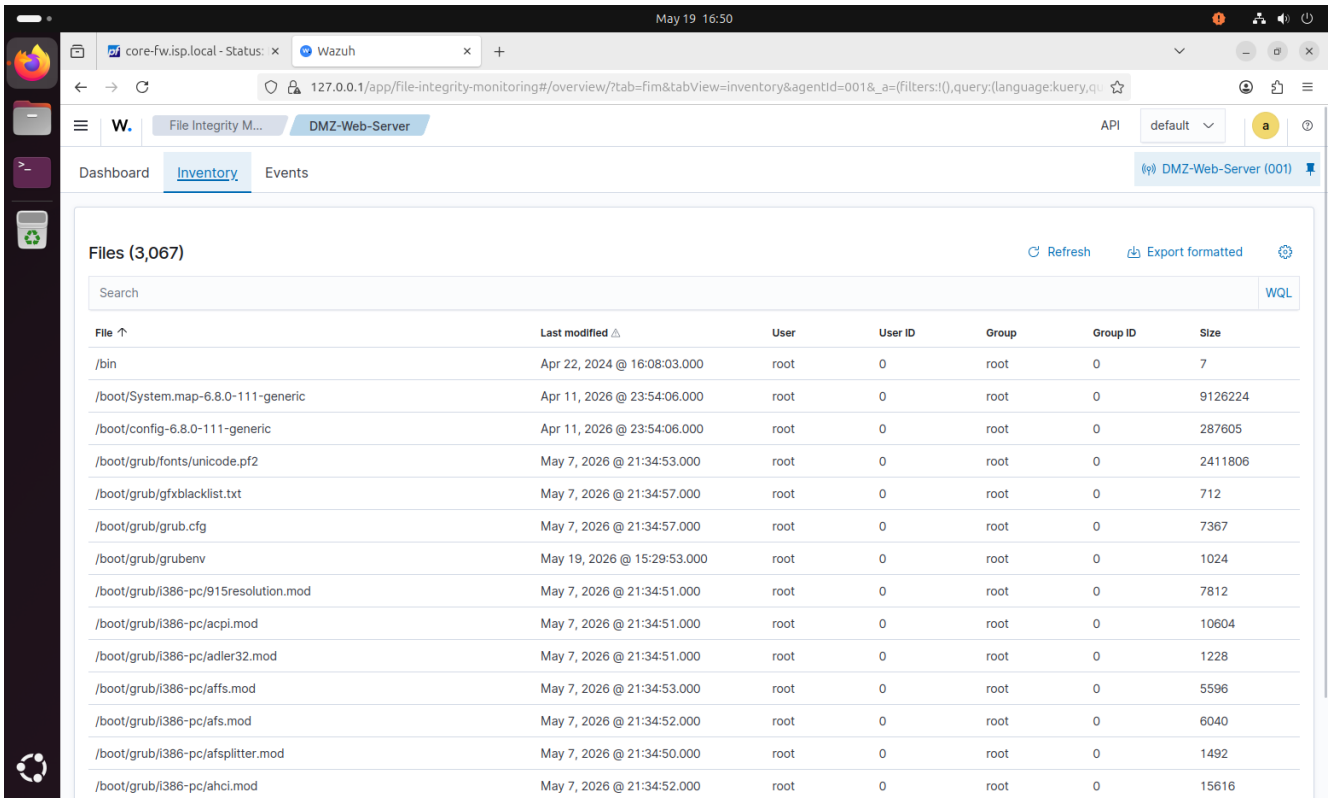

Рисунок 3.27 – Моніторинг цілісності файлів серверної інфраструктури

3.8 Організація захищеного віддаленого доступу через WireGuard VPN

Завершальним етапом реалізації системи захисту є конфігурування безпечного каналу для віддаленого адміністрування мережевої інфраструктури. Оскільки будь-який прямий доступ до портів управління з глобальної мережі суворо заборонений політикою міжмережевого екрана, для авторизації інженерного персоналу з недовірених середовищ було розгорнуто віртуальну приватну мережу VPN на базі сучасного протоколу WireGuard. Цей механізм забезпечує криптографічно захищений вхід виключно до ізольованого сегменту управління.

Процес розгортання розпочався зі створення серверного тунелю у відповідному модулі pfSense. Під час ініціалізації віртуального інтерфейсу tun_wg0 було згенеровано унікальну пару асиметричних криптографічних ключів на базі еліптичної кривої Curve25519. Для маршрутизації VPN-трафіку тунелю було призначено окрему ізольовану транзитну підмережу. Слухаючий порт служби було закріплено за нестандартним UDP-портом, який функціонує в скритому режимі, він

не відповідає на неавторизовані мережеві сканування, залишаючись невидимим для потенційних зловмисників. Конфігурування тунелю WireGuard на магістральному шлюзі продемонстровано на рисунку 3.28.

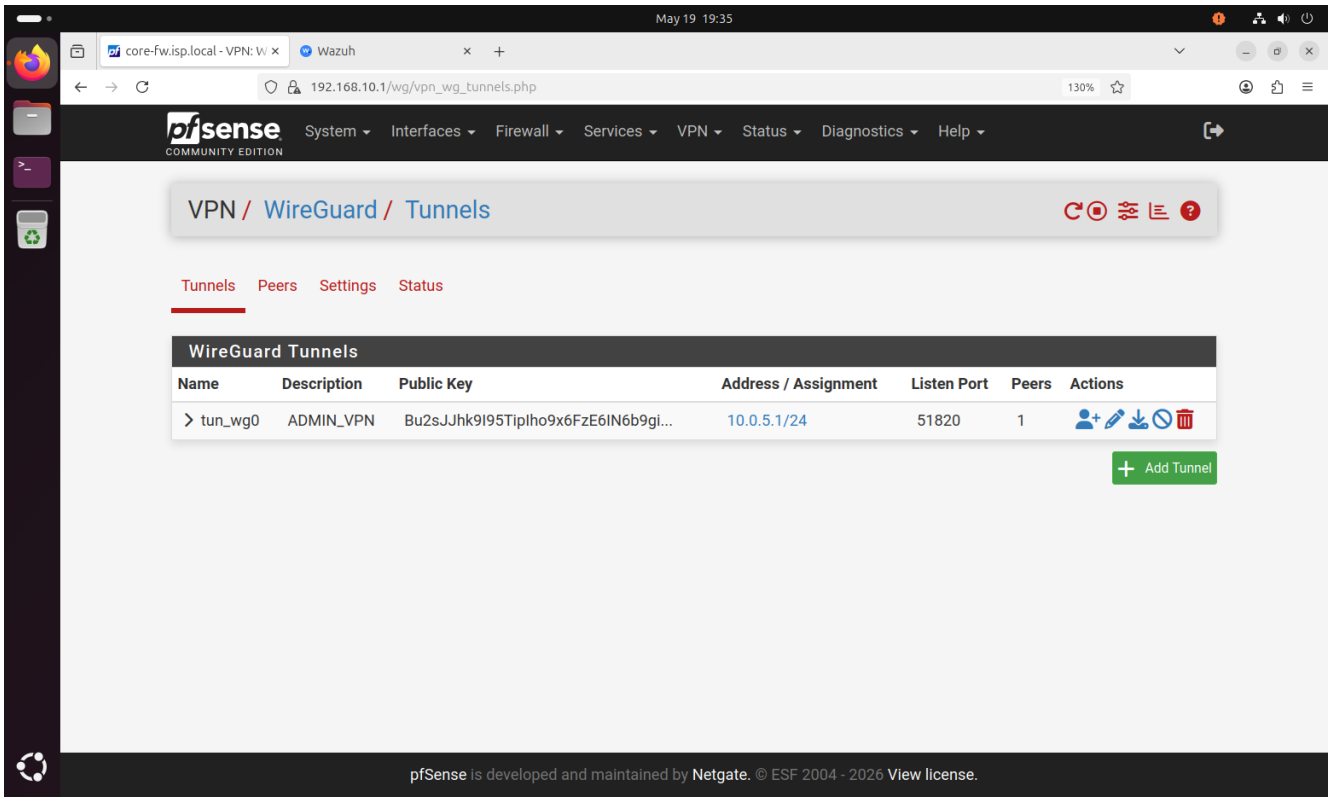

Рисунок 3.28 –Тунель WireGuard на магістральному шлюзі

Для авторизації адміністраторів у системі було сформовано профілі Peers. Кожному авторизованому пристрою було згенеровано власну пару ключів та виділено статичну IP-адресу з транзитної підмережі VPN. У налаштуваннях пірів на шлюзі було застосовано фундаментальну для WireGuard концепцію Cryptokey Routing. Параметр Allowed IPs було жорстко прив'язано до конкретної клієнтської IP-адреси, що повністю унеможливлює спроби підміни адрес всередині зашифрованого тунелю: маршрутизатор приймає пакети від клієнта лише в тому випадку, якщо вони розшифровуються правильним відкритим ключем і мають дозволену IP-адресу джерела [59]. Створення профілю для адміністратора відображено на рисунку 3.29.

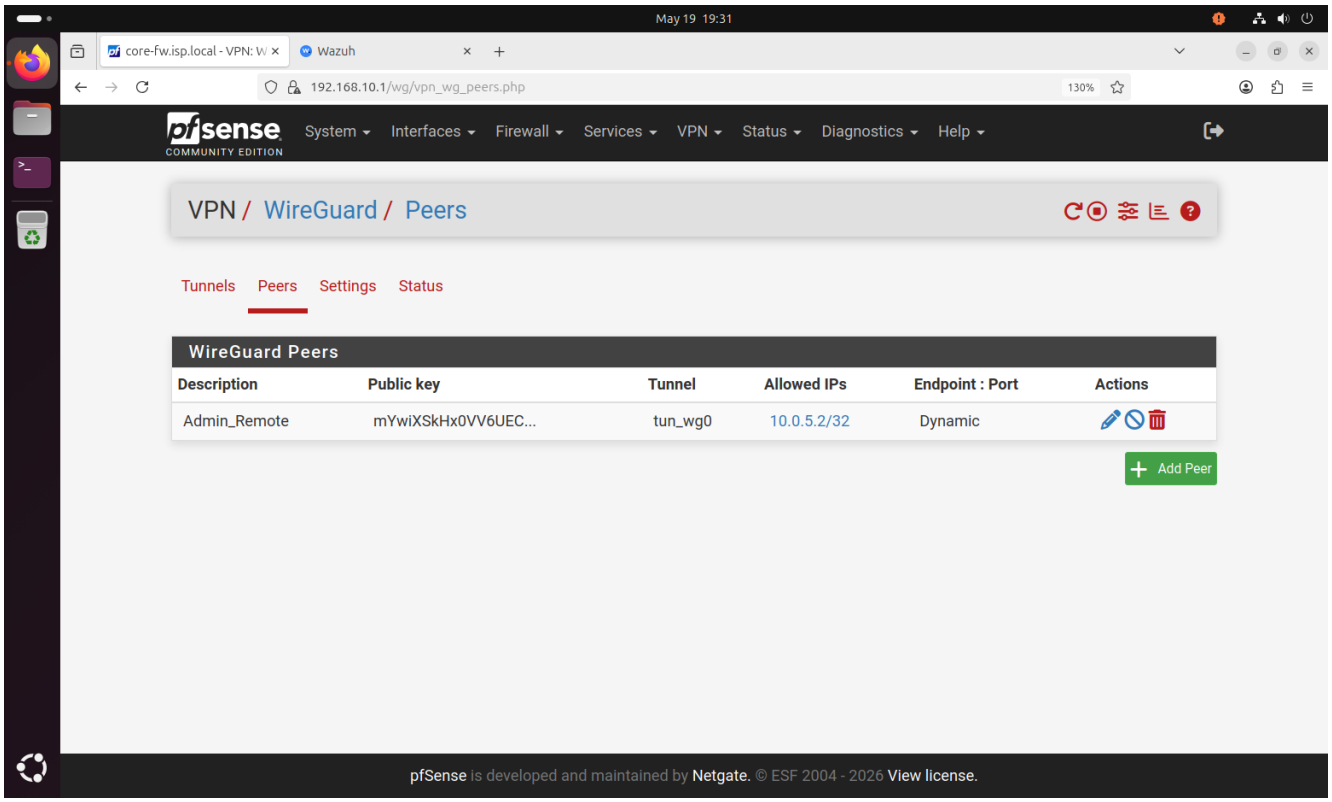

Рисунок 3.29 –Профіль для адміністратора

Фінальним кроком стала верифікація встановлення захищеного з'єднання з робочої станції адміністратора, яка знаходиться за межами мережі провайдера. Після ініціалізації тунелю на клієнтському пристрої, у веб-консолі pfSense було зафіксовано успішний криптографічний обмін ключами. Аналіз таблиці маршрутизації та лічильників трафіку підтвердив, що двосторонній обмін зашифрованими пакетами відбувається коректно, а адміністратор отримав безпечний доступ до технологічних вузлів мережі управління. Перевірку роботи VPN з віддаленого пристрою наведено на рисунку 3.30, а статус підключення на стороні ядра мережі продемонстровано на рисунку 3.31.

Рисунок 3.30 – Перевірка роботи VPN з віддаленого пристрою

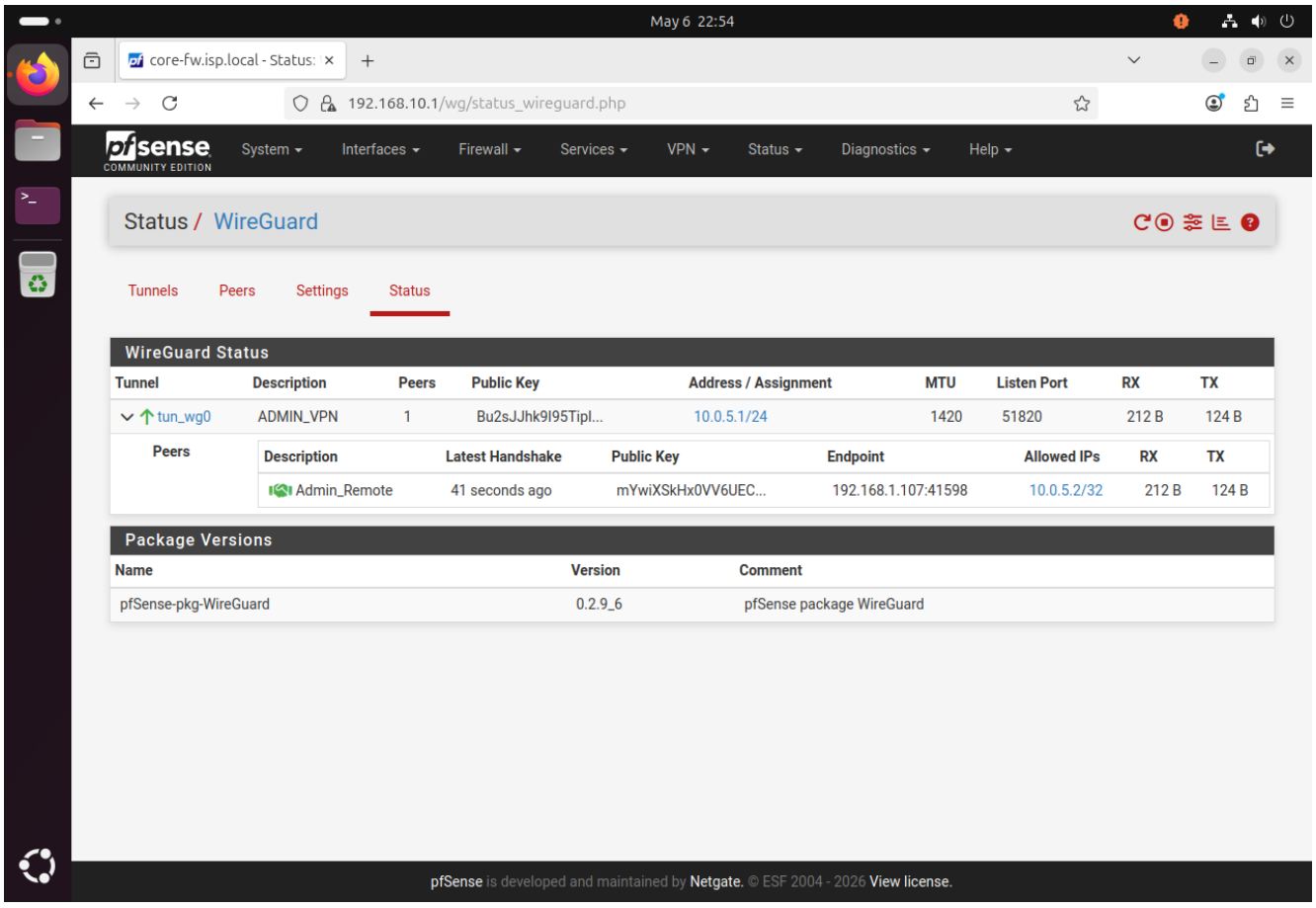

Рисунок 3.31 – Перевірка роботи VPN на сторонні ядра мережі

4 ПРАКТИЧНЕ ТЕСТУВАННЯ ТА ПЕРЕВІРКА СИСТЕМИ ЗАХИСТУ

4.1 Аудит мережевого доступу та логічної ізоляції сегментів

Першим етапом практичного тестування розробленої комплексної системи захисту стала верифікація політик міжмережевого екранування, перевірка стійкості периметра до мережевої розвідки та аудит логічної ізоляції внутрішніх сегментів VLAN.

Для імітації дій зовнішнього зловмисника, який намагається зібрати інформацію про відкриті порти та доступні сервіси магістрального шлюзу, було застосовано спеціалізований інструмент мережевого аудиту Nmap. З умовної машини атакуючого ОС Kali Linux було ініційовано «невидиме» SYN-сканування першої тисячі найпопулярніших TCP-портів на зовнішньому інтерфейсі маршрутизатора. Результати сканування підтвердили коректність налаштувань периметра: єдиним відкритим портом виявився порт 80 HTTP, який легітимно прокинутий у демілітаризовану зону для роботи вебсервера. Всі інші 999 портів отримали статус «filtered», що свідчить про успішне відкидання пакетів фаєрволом. Результати зовнішнього сканування портів маршрутизатора утилітою Nmap наведено на рисунку 4.1.

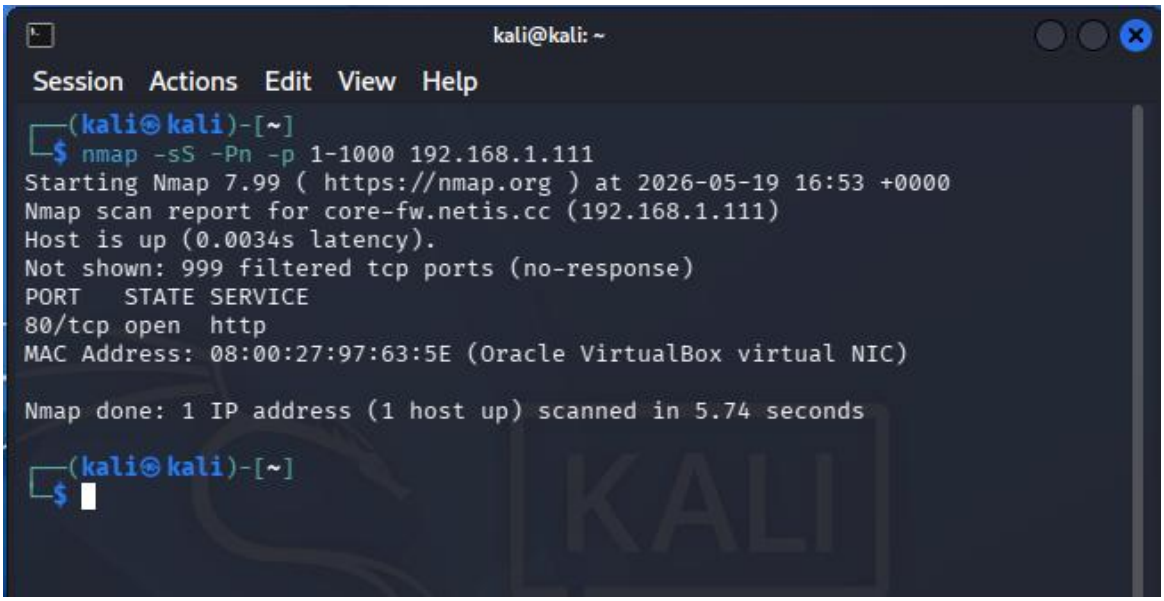

Рисунок 4.1 –Зовнішнє сканування портів маршрутизатора утилітою Nmap

Аналіз системних журналів міжмережевого екрана pfSense продемонстрував проактивну реакцію системи безпеки на спробу масованого сканування. Замість базового відкидання пакетів правилом за замовчуванням, система виявила аномальну активність і спрацював механізм динамічного блокування. IP-адреса атакуючого була автоматично занесена до системної таблиці порушників, після чого всі подальші спроби підключення блокувалися превентивним правилом «Block snort2c hosts». Це повністю ізолює зловмисника та унеможливлює подальший збір топологічної інформації. Динамічне блокування IP-адреси зловмисника в системних журналах фаєрвола відображено на рисунку 4.2.

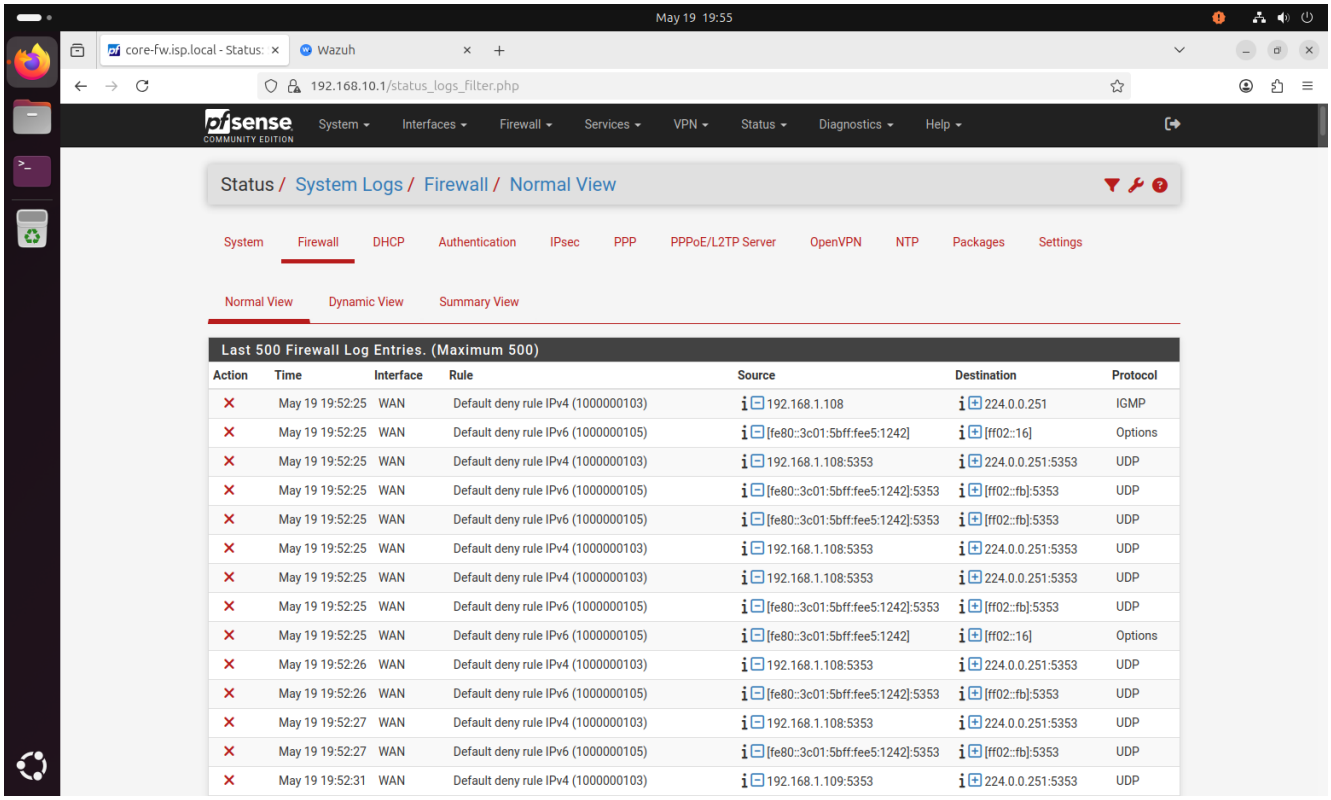

Рисунок 4.2 – Системні журнали фаєрвола

Наступним кроком стала перевірка ефективності внутрішньої сегментації абонентської мережі. Відповідно до закладеної архітектури, клієнтські пристрої з різних віртуальних мереж не повинні мати можливості прямої взаємодії. Для верифікації цього правила з ПК під управлінням ОС Windows, яка знаходиться в одній ізольованій підмережі, було відправлено ping на IP-адресу клієнта з

підмережі VLAN 20. В результаті 100% втрата пакетів із повідомленням «Request timed out». Це доводить, що правила фільтрації на магістральному Trunk-інтерфейсі успішно блокують несанкціоновану горизонтальну маршрутизацію між абонентами. Тестування логічної ізоляції абонентських підмереж на канальному та мережевому рівнях продемонстровано на рисунку 4.3.

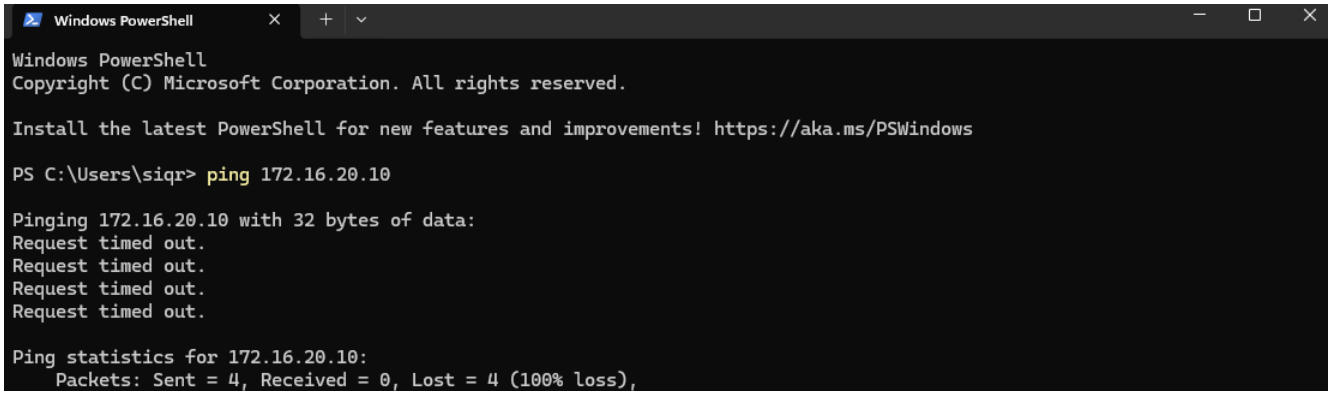

Рисунок 4.3 – Логічна ізоляції абонентських підмереж на канальному та мережевому рівнях

4.2 Верифікація роботи системи запобігання вторгненням IPS

Другим етапом практичних випробувань став аудит працездатності сигнатурного аналізу та підсистеми глибокого аналізу пакетів на прикладному рівні. Головною метою цього тесту була перевірка ефективності налаштованої системи Suricata, яка функціонує в режимі Inline IPS на інтерфейсах магістрального шлюзу, щодо своєчасного виявлення та автоматичного блокування спроб експлуатації вразливостей вебдодатків у демілітаризованій зоні.

Для симуляції цілеспрямованої атаки на вебсервер з хоста зовнішнього зловмисника було реалізовано спробу експлуатації уразливості типу Directory Traversal, тобто вихід за межі кореневого каталогу вебсервера. За допомогою консольної утиліти curl було сформовано та відправлено шкідливий HTTP-запит до публічної IP-адреси шлюзу, який містив специфічний відносний шлях із метою несанкційонованого зчитування критичного системного файлу операційної системи. Спробу атаки за допомогою утиліти curl відображено на рисунку 4.4.

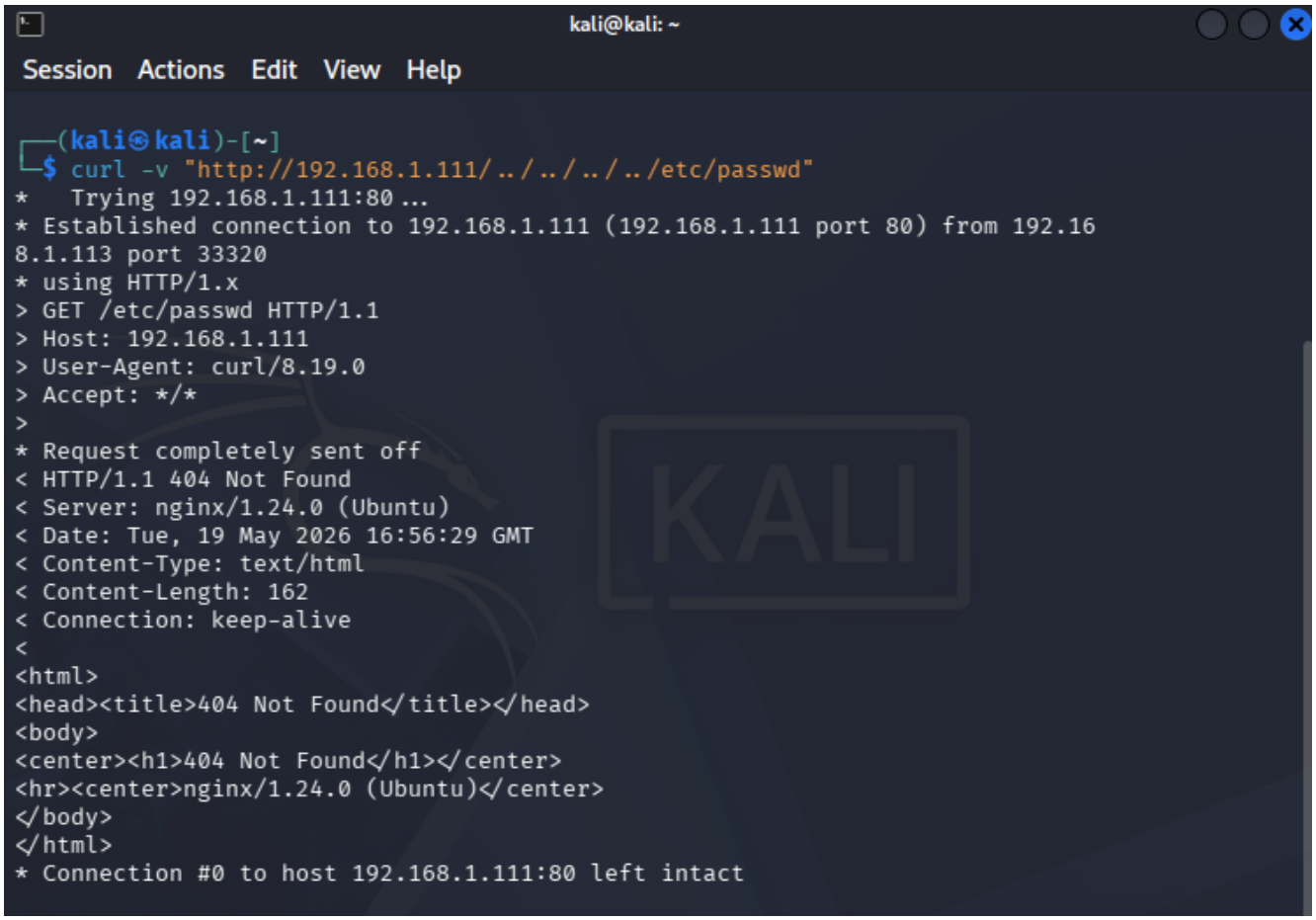

Рисунок 4.4 – Атака за допомогою утиліти curl

Аналіз журналів сповіщень та інтерфейсу моніторингу сигнатурного захисту в pfSense підтвердив миттєву реакцію. Система інспекції трафіку Suricata успішно декодувала вміст HTTP-пакета в реальному часі та ідентифікувала аномальну структуру запиту. У результаті аналізу корисного навантаження спрацювало специфічне сигнатурне правило з підключеного репутаційного набору Emerging Threats, а саме правило класу ET WEB_SERVER /etc/passwd. Оскільки інтерфейс брандмауера було переведено в режим Inline IPS, система безпеки не просто зафіксувала інцидент у журналах, а миттєво змінила дію для цього потоку даних на «Drop», повністю заблокувавши передачу шкідливих пакетів до цільового Ubuntu Server. Зловмисник при цьому не отримав доступу до даних, що підтверджує ефективність захисту веб-периметра. Фіксацію інциденту безпеки та автоматичне відкидання шкідливого пакета системою Suricata наведено на рисунку 4.5.

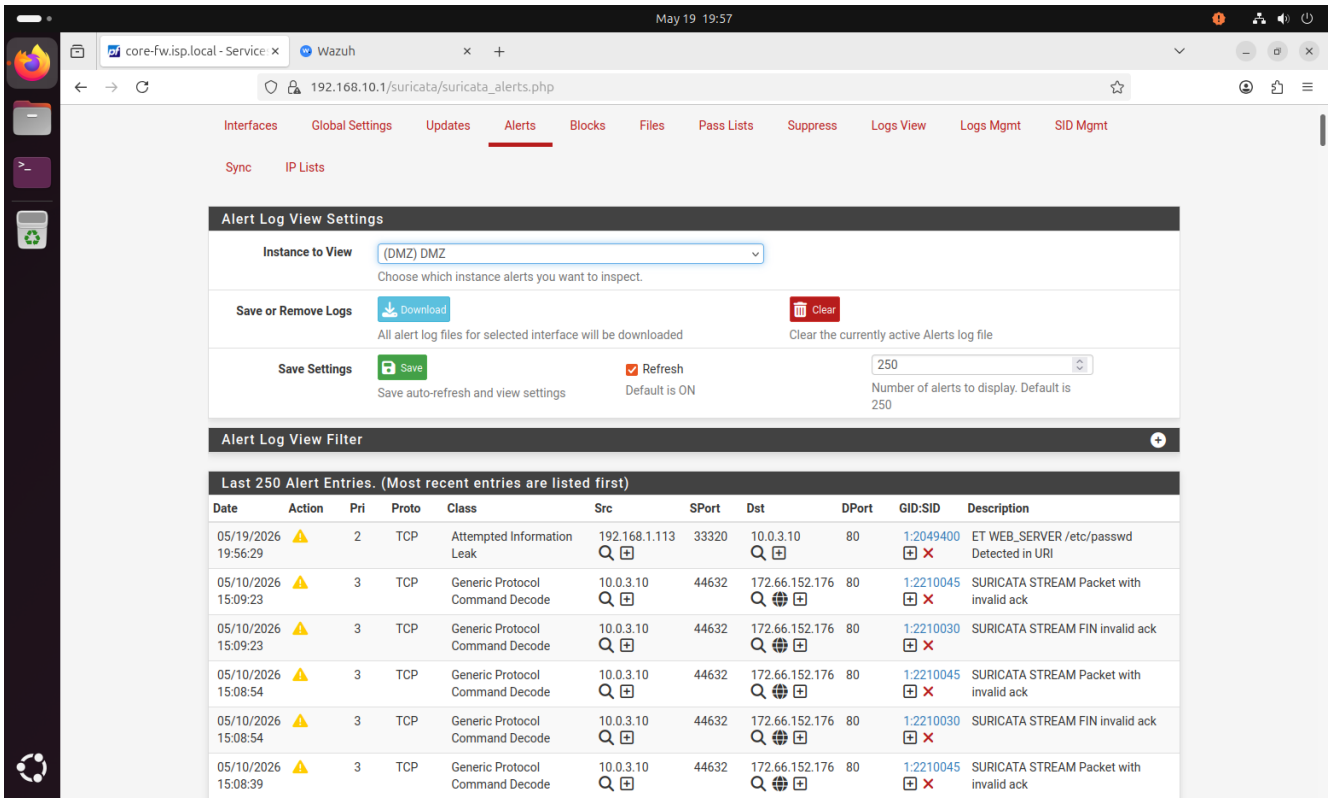

Рисунок 4.5 – Системні журнали Suricata

4.3 Тестування стійкості до мережевих перевантажень

Третім етапом практичного тестування стала перевірка стійкості інфраструктури до об'ємних мережевих атак типу DoS/DDoS, метою яких є вичерпання обчислювальних ресурсів магістрального маршрутизатора або пропускної здатності каналів зв'язку. Згідно з розробленою політикою захисту, основним інструментом протидії таким загрозам виступають налаштовані раніше обмежувачі швидкості Limiters підсистеми Traffic Shaper.

Для симуляції масованого мережевого перевантаження з боку зовнішнього зловмисника було використано утиліту hping3, яка дозволяє генерувати кастомні TCP/IP пакети з високою інтенсивністю. Атаку було спрямовано на відкритий порт 80 HTTP вебсервера, що знаходиться у демілітаризованій зоні. У консолі атакуючої машини було запущено генерацію класичного SYN-флуду, який відправляє тисячі запитів на ініціалізацію з'єднання щосекунди, не чекаючи на відповідь від сервера. Симуляцію масованої SYN-Flood атаки за допомогою утиліти hping3 продемонстровано на рисунку 4.6.

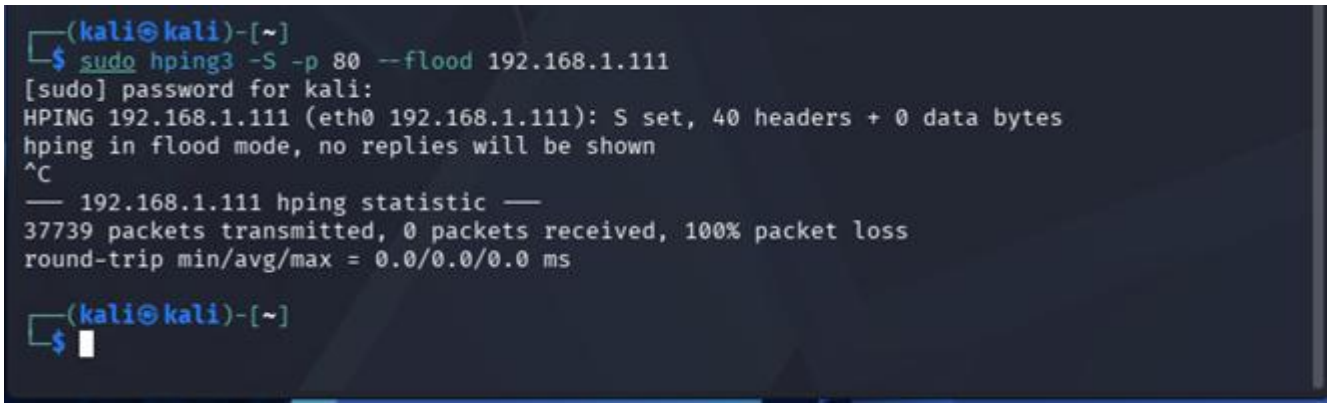

Рисунок 4.6 –Атака за допомогою утиліти hping3

Моніторинг стану магістрального шлюзу під час атаки підтвердив високу ефективність налаштованих механізмів управління трафіком. Завдяки жорстким лімітам пропускної здатності, виділеним для відповідних підмереж, весь надлишковий паразитний трафік, що перевищував встановлені квоти, автоматично відкидався пакетним фільтром ще на етапі входу в інтерфейс маршрутизатора. Це дозволило уникнути переповнення глобальної таблиці станів та вичерпання ресурсів процесора pfSense. Таким чином, незважаючи на безперервну генерацію флуду зловмисником, інфраструктура зберегла свою працездатність, а легітимні клієнти в інших ізольованих VLAN-сегментах не відчули погіршення якості обслуговування.

4.4 Перевірка хостового захисту та підсистеми моніторингу SIEM

Четвертим етапом практичних випробувань став аудит локальної безпеки цільового сервера, розміщеного в демілітаризованій зоні, а також верифікація працездатності підсистеми централізованого моніторингу та аудиту на базі Wazuh.

Для перевірки політик зміцнення операційної системи було здійснено спробу несанкціонованої авторизації до служби віддаленого управління SSH. З машини атакуючого було ініційовано підключення з використанням стандартного методу автентифікації за паролем, що є типовим вектором для атак типу Brute-force або використання словників. Результат тестування підтвердив коректність налаштувань, впроваджених на етапі конфігурування: сервер миттєво відхилив

запит із повідомленням Permission denied (publickey). Це доводить, що повна заборона парольної автентифікації на користь криптографічних ключів робить сервер абсолютно стійким до спроб підбору облікових даних. Відхилення несанкціонованої спроби підключення до служби віддаленого доступу SSH відображено на рисунку 4.7.

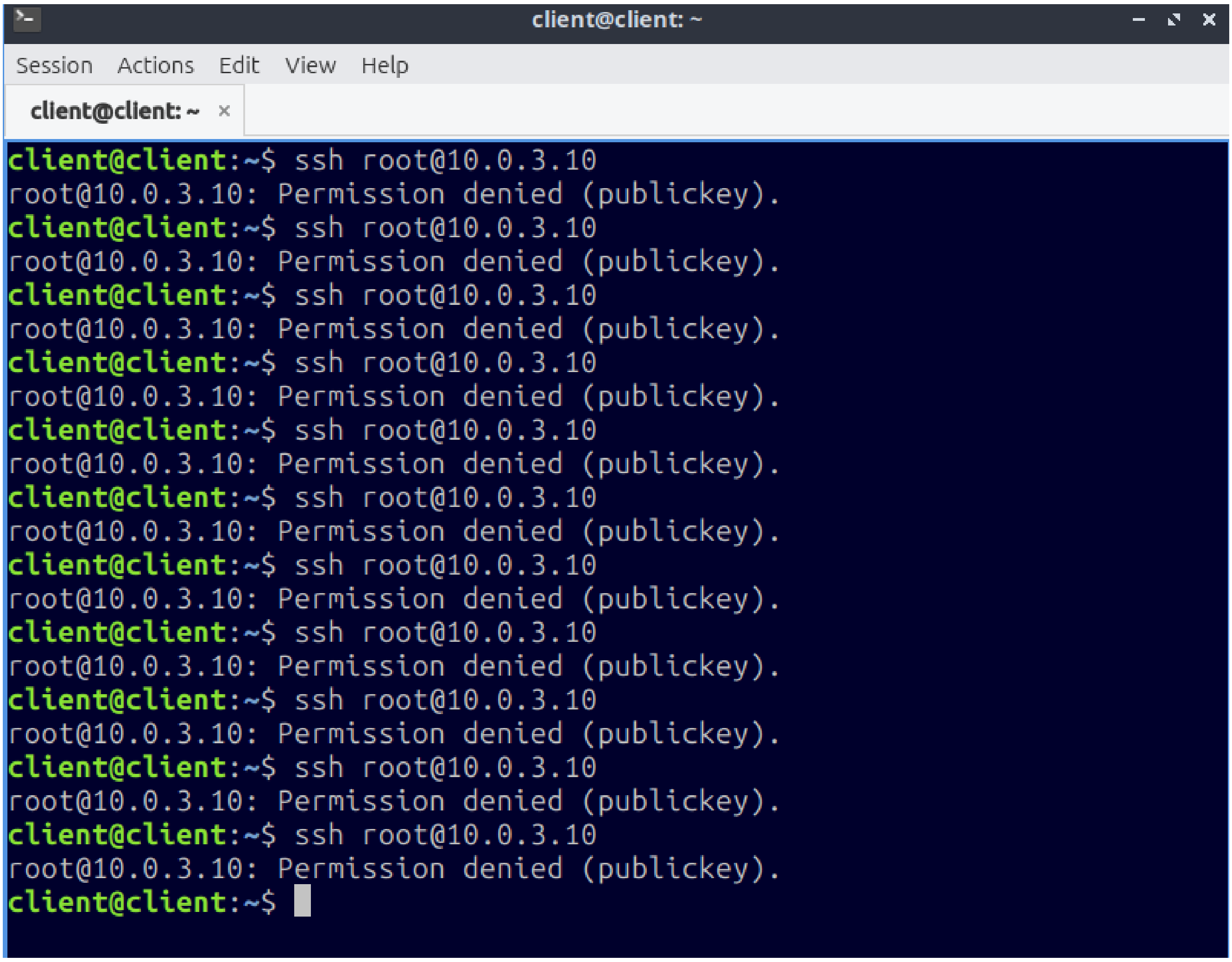

Рисунок 4.7 – Спроба підключення до служби віддаленого доступу SSH

Наступним кроком стала перевірка функціонування підсистеми аудиту та моніторингу подій безпеки. Важливою вимогою до SIEM-системи є здатність фіксувати не лише мережеві аномалії, а й локальні дії користувачів на захищених хостах. Після легітимної авторизації адміністратора на сервері за допомогою криптографічного ключа було виконано серію команд із підвищенням привілеїв

через утиліту sudo. Аналіз інформаційної панелі Threat Hunting у центральній консолі Wazuh продемонстрував, що встановлений на сервері агент успішно збирає та передає системну телеметрію в режимі реального часу. SIEM-система коректно зафіксувала відкриття та закриття сесій PAM: Login session opened/closed, а також усі факти використання підвищених привілеїв. Це гарантує безперервний аудит дій інженерного персоналу та дозволяє оперативно виявляти нетипову або зловмисну активність безпосередньо всередині операційної системи захищеного вузла. Фіксацію локальних подій безпеки та аудиту привілеїв у системі моніторингу Wazuh наведено на рисунку 4.8.

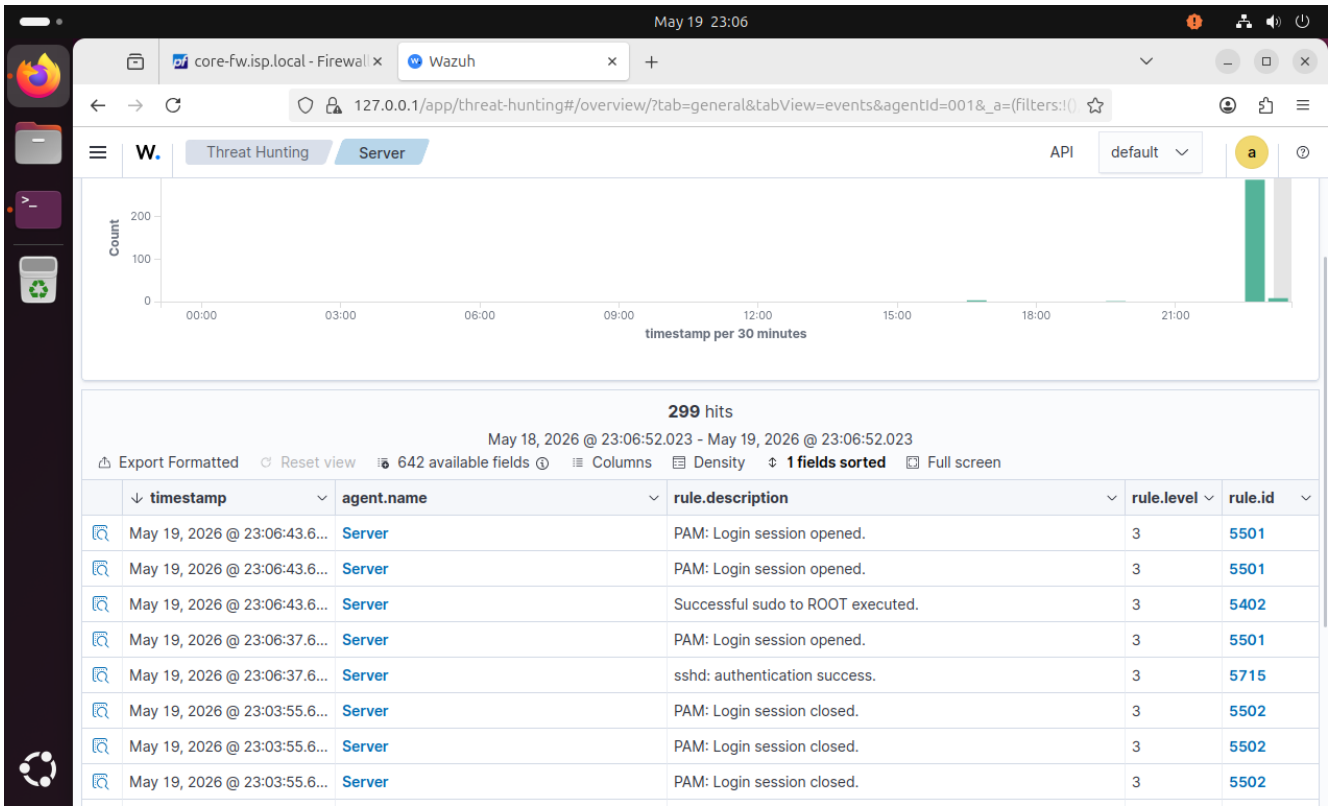

Рисунок 4.8 – Локальні події безпеки та аудиту привілеїв у системі моніторингу Wazuh

4.5 Тестування механізмів відмовостійкості магістрального ядра

Фінальним етапом практичного тестування стала верифікація роботи кластера високої доступності, побудованого на базі протоколів CARP та pfsync. Головною метою цього випробування було підтвердження здатності мережевої

інфраструктури зберігати працездатність та забезпечувати безперервність надання послуг у разі критичного апаратного збою основного магістрального маршрутизатора.

Для проведення тесту було розгорнуто сценарій імітації відмови: з абонентської робочої станції було запущено безперервну передачу ping до DNS-сервера. У процесі обміну мережевими пакетами було здійснено примусове відключення основного шлюзу pfSense Master, що імітувало раптову апаратну відмову або знеструмлення. Аналіз результатів виконання команди ping показав, що в момент відключення відбулася передбачувана короткочасна затримка в маршрутизації, яка призвела до втрати частини транзитних пакетів. Проте вже за кілька секунд передача даних повністю та автоматично відновилася. Це підтверджує, що завдяки технології pfsync таблиці мережевих станів були заздалегідь синхронізовані, і клієнтські сесії не розірвалися остаточно. Фіксацію короткочасного переривання зв'язку в момент аварійного перемикання шлюзів продемонстровано на рисунку 4.9.

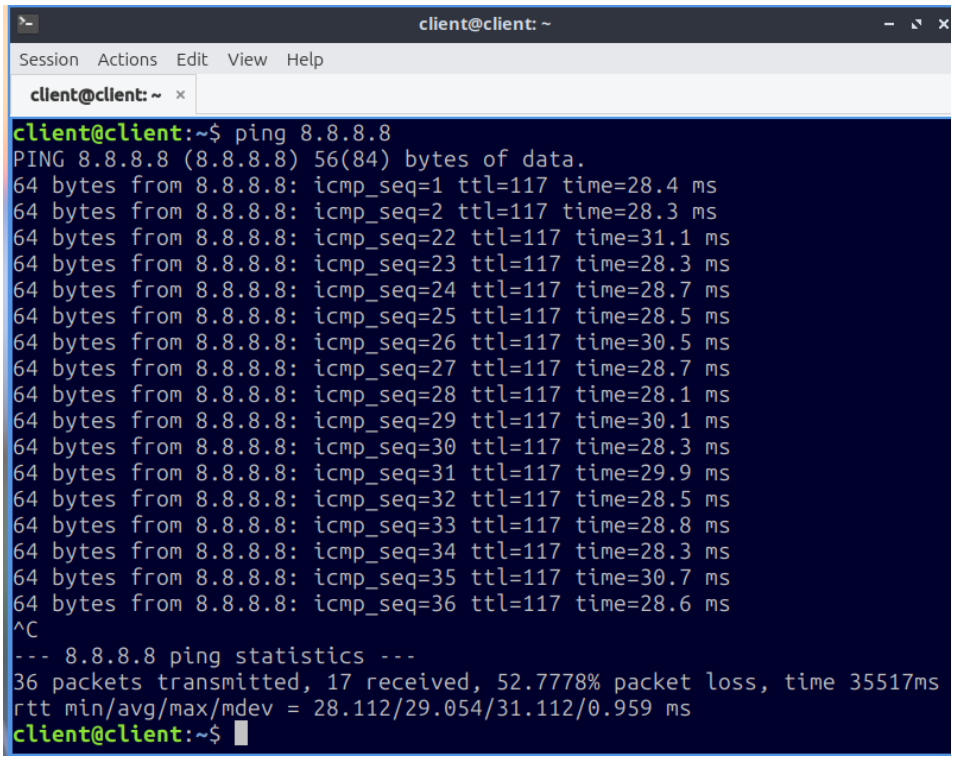

Рисунок 4.9 – Короткочасне переривання зв'язку в момент аварійного перемикання шлюзів

Одночасно з відновленням зв'язку було перевірено логіку роботи протоколу резервування на боці мережевого обладнання. У веб-консолі управління резервного маршрутизатора pfSense_Backup було проведено аудит станів віртуальних інтерфейсів. Оскільки резервний вузол перестав отримувати широкомовні сигнали від основного пристрою через виділений лінк синхронізації, він штатно відпрацював аварійний сценарій та перехопив управління всіма віртуальними IP-адресами протоколу CARP. Статус усіх задіяних інтерфейсів у системі миттєво змінився з «BACKUP» на «MASTER», після чого резервний пристрій повністю взяв на себе функції магістрального ядра розробленої мережі. Успішне перехоплення віртуальних IP-адрес та перехід резервного вузла у стан MASTER відображено на рисунку 4.10.

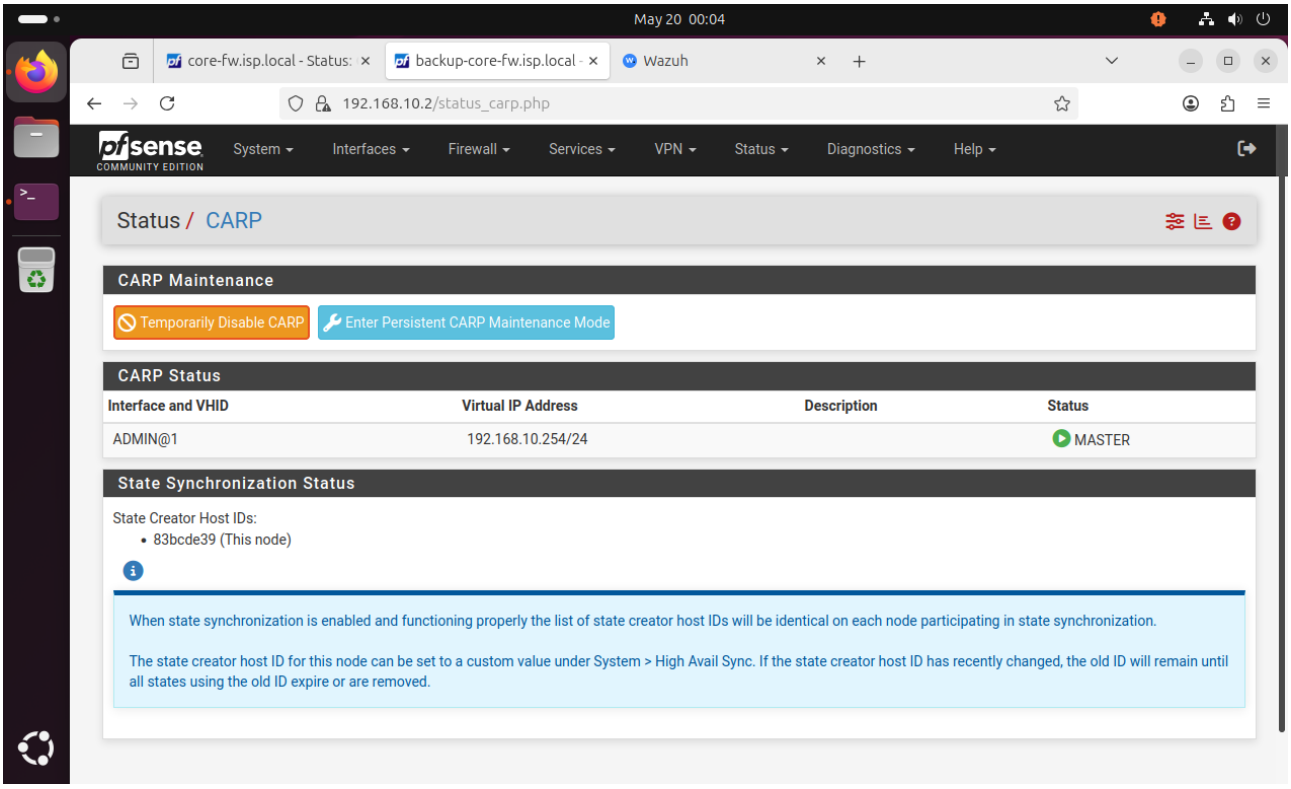

Рисунок 4.10 – Перехід резервного вузла у стан MASTER

Проведене практичне тестування та верифікація програмно-апаратного стенда повністю підтвердили ефективність розробленої архітектури комплексної системи захисту. У ході випробувань було доведено, що впроваджена політика

логічної сегментації та міжмережевого екранування успішно ізолює критичні вузли та блокує несанкціоновану розвідку. Тестування підсистеми запобігання вторгненням Suricata підтвердило її здатність в режимі реального часу. Імітація об'ємних мережевих перевантажень продемонструвала надійність механізмів шейпінгу у збереженні ресурсів ядра мережі. Крім того, верифікація хостового захисту в поєднанні з SIEM-системою Wazuh підтвердила неможливість компрометації серверів через підбір паролів та довела високу результативність безперервного аудиту дій усередині демілітаризованої зони. Фінальний тест механізмів відмовостійкості засвідчив високу надійність інфраструктури та її здатність до автоматичного відновлення після критичних апаратних збоїв із мінімальним часом простою.

ВИСНОВКИ

Під час виконання роботи вирішено актуальне науково-практичне завдання з проєктування, розгортання та тестування комплексної системи захисту телекомунікаційної інфраструктури провайдера. Використання комплексного підходу, що поєднує методи логічної ізоляції, глибокої інспекції трафіку та централізованого моніторингу, дозволило створити відмовостійке та захищене мережеве середовище. У результаті отримано:

1. Проведено комплексний аналіз об'єкта захисту та актуальних загроз. Визначено критичні вектори атак на мережі провайдерів. На основі моделювання загроз обґрунтовано вибір технологічного стека та методів протидії, що базуються на концепції глибоко ешелонованого захисту.

2. Розроблено та впроваджено ієрархічну архітектуру мережі з суворим розмежуванням доступу. На базі магістрального шлюзу реалізовано жорсткий апаратний та логічний розподіл на зони довіри. Створено ізольований сегмент управління, демілітаризовану зону для публічних сервісів та абонентський сегмент із мікросегментацією за допомогою технології VLAN. Застосування політики мінімальних привілеїв та суворих правил міжмережевого екранування унеможливило несанкціоновану маршрутизацію між клієнтськими та технологічними підмережами.

3. Побудовано відмовостійке магістральне ядро мережі. Для забезпечення безперервності надання послуг розгорнуто кластер високої доступності на базі програмно-апаратного комплексу pfSense. Використання протоколів CARP та pfsync із виділеним фізичним каналом синхронізації дозволило реалізувати механізм миттєвого аварійного перемикання зі збереженням таблиць станів активних клієнтських сесій.

4. Реалізовано систему проактивного захисту та інспекції трафіку. Інтеграція системи Suricata в режимі Inline IPS забезпечила здатність мережі в реальному часі аналізувати трафік на прикладному рівні та автоматично відкидати експлойти. Для захисту від мережевих перевантажень успішно впроваджено

механізми управління смугою пропускання, що гарантує стабільність роботи ядра навіть в умовах масованих атак.

5. Забезпечено багаторівневий захист серверного сегмента. Для цільових вузлів у DMZ налаштовано локальні міжмережеві екрани UFW, інтегровано системи динамічного блокування Fail2Ban та переведено служби віддаленого доступу на сувору криптографічну автентифікацію, що повністю нівелює ризики компрометації через підбір паролів.

6. Впроваджено підсистему централізованого моніторингу та аудиту SIEM. На базі платформи Wazuh організовано збір телеметрії як з магістрального шлюзу, так і з серверу через Wazuh Agents. Активація модулів контролю цілісності файлів FIM та аудиту подій безпеки дозволила створити єдину точку контролю за станом інфраструктури.

7. Проведено емпіричне тестування ефективності розробленої системи. Практичні випробування за допомогою спеціалізованого програмного забезпечення повністю підтвердили заявлені характеристики. Система успішно заблокувала спроби атак без порушення роботи магістралі та продемонструвала автоматичне відновлення маршрутизації під час імітації відмови основного шлюзу.

Розроблена та практично реалізована комплексна система захисту повністю відповідає сучасним стандартам інформаційної безпеки. Запропоновані архітектурні та програмно-технічні рішення довели свою ефективність і можуть бути рекомендовані для впровадження в реальні телекомунікаційні мережі інтернет-провайдерів та корпоративні інфраструктури з високими вимогами до відмовостійкості й безпеки.

СПИСОК ДЖЕРЕЛ

1. Системи захисту інформації : підручник / Ю.В. Костюк, П.М. Складанний, Г.М. Гулак, Б.Т. Бебешко, К.В. Хорольська, С.Л. Рзаєва. – Київ : Київський столичний університет імені Бориса Грінченка, 2025. – 887 с (дата звернення: 05.03.2026).

2. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX : станом на 27 лют. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 16.03.2026).

3. Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 20 січ. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 16.03.2026).

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 16.03.2026).

5. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 16.03.2026).

6. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Каб. Міністрів України від 19.06.2019 № 518 : станом на 20 листоп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (дата звернення: 17.03.2026).

7. Mistry N. SLAs: how isps and carriers agree on service levels. *Quadrang Systems*. URL: https://quadrang.com/slas-how-isps-and-carriers-agree-on-service-levels/ (дата звернення: 01.03.2026).

8. ISP network architecture. *ZPE Systems*. URL: https://zpesystems.com/isp-network-architecture-zs/ (дата звернення: 01.03.2026).

9. Rief J., Wiedner F. W. ISP networks- differences and challenges. *TUM Info VIII: Homepage*. URL: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2024-09-1/NET-2024-09-1_04.pdf (дата звернення: 01.03.2026).

10. Cisco. ISP network design. *Home | Network Startup Resource Center*. URL: https://nsrc.org/wrc/data/2003/9642836473fa01ff7e00d9/d1-1up.pdf (date of access: 01.03.2026).

11. ISP architecture & components. *Note Sack – A Better Way To Success*. URL: https://notesack.wordpress.com/wp-content/uploads/2017/07/isp-architecture.pdf (дата звернення: 02.03.2026).

12. GeeksforGeeks. Hierarchical network design. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/computer-networks/hierarchical-network-design/ (дата звернення: 02.03.2026).

13. Contributors to Wikimedia projects. Internet service provider - Wikipedia. *Wikipedia, the free encyclopedia*. URL: https://en.wikipedia.org/wiki/Internet_service_provider (дата звернення: 02.03.2026).

14. What is a DMZ network and why would you use it?. *Fortinet*. URL: https://www.fortinet.com/resources/cyberglossary/what-is-dmz (дата звернення: 03.0.2026).

15. What is ISO/IEC 27001? |IBM. *IBM*. URL: https://www.ibm.com/products/cloud/compliance/iso-27001 (дата звернення: 17.03.2026).

16. ISO/IEC 27032 cybersecurity. *Standards Explained*. URL: https://standardsexplained.com/iso-iec-27032-cybersecurity/ (date of access: 17.03.2026).

17. What Is NIST SP 800-207? Zero trust Architecture Framework. *Palo Alto Networks*. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-nist-sp-800-207 (дата звернення: 18.03.2026).

18. GeeksforGeeks. What is OSI model | 7 layers explained. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/computer-networks/open-systems-interconnection-model-osi/ (дата звернення: 20.02.2026).

19. What is the castle-and-moat network security model?. *Cloudflare*. URL: https://www.cloudflare.com/learning/access-management/castle-and-moat-network-security/ (дата звернення: 19.03.2026).

20. What is an insider threat?. *Cloudflare*. URL: https://www.cloudflare.com/learning/access-management/what-is-an-insider-threat/ (дата звернення: 19.03.2026).

21. Філіпов О. Типи кібератак – 4 класифікації кібератак. *Datami.ee*. URL: https://datami.ee/ua/blog/types-of-cyberattacks-4-classifications-of-cyber-threats/ (дата звернення: 07.03.2026).

22. VirtualBox documentation. *VirtualBox* URL: https://www.virtualbox.org/wiki/Documentation (дата звернення: 21.02.2026).

23. Morrison A. Mikrotik vs. pfsense: a comprehensive comparison of features, performance, and security. *1Gbits*. URL: https://1gbits.com/blog/mikrotik-vs-pfsense/ (дата звернення: 21.02.2026).

24. Getting started with pfsense software. *pfSense® - World's Most Trusted Open Source Firewall*. URL: https://www.pfsense.org/getting-started/ (дата звернення: 21.02.2026).

25. PfSense documentation | pfsense documentation. *Netgate Documentation | Netgate Documentation*. URL: https://docs.netgate.com/pfsense/en/latest/ (дата звернення: 21.02.2026).

26. DeepWiki. High Availability Configuration | pfsense/docs | DeepWiki. *DeepWiki*. URL: https://deepwiki.com/pfsense/docs/4.2-high-availability-configuration (дата звернення: 21.02.2026).

27. Ubuntu Desktop documentation. *Ubuntu Desktop*. URL: https://documentation.ubuntu.com/desktop/en/latest/ (дата звернення: 21.02.2026).

28. GeeksforGeeks. How to install Ubuntu on VirtualBox? - GeeksforGeeks. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/linux-unix/how-to-install-ubuntu-on-virtualbox/ (дата звернення: 21.02.2026).

29. Rendek L. Installing VirtualBox Guest Additions on Ubuntu 24.04. *Linuxconfig.org*. 21.09.2025. URL: https://linuxconfig.org/installing-virtualbox-guest-additions-on-ubuntu-24-04 (дата звернення: 21.02.2026).

30. Ubuntu Server documentation. *Ubuntu Server*. URL: https://ubuntu.com/server/docs/ (дата звернення: 21.02.2026).

31. Hibbard J. How to install ubuntu server on virtualbox. *Hibbard.eu*. URL: https://hibbard.eu/install-ubuntu-virtual-box// (дата звернення: 21.02.2026).

32. Nwezeaku C. Understanding firewall rules: a beginner's guide. *SecureMyOrg*. URL: https://securemyorg.com/understanding-firewall-rules-a-beginners-guide/ (дата звернення: 22.02.2026).

33. What Is the RADIUS Protocol?. *Fortinet*. URL: https://www.fortinet.com/resources/cyberglossary/radius-protocol (дата звернення: 20.05.2026).

34. Tianshu W. What Is IPoE? How Does IPoE Differ from PPPoE?. *Huawei*. URL: https://info.support.huawei.com/info-finder/encyclopedia/en/IPoE.html (дата звернення: 24.02.2026).

35. Gokhankosem. IP over ethernet | ipoe vs pppoe | pppoe vs ipoe | ipcisco.com. *IPCisco*. URL: https://ipcisco.com/ip-over-ethernet-and-ipoe-versus-pppoe/ (дата звернення: 24.02.2026).

36. GeeksforGeeks. Dynamic host configuration protocol (DHCP). *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/computer-networks/dynamic-host-configuration-protocol-dhcp/ (дата звернення: 24.02.2026).

37. Dhandala N. How to Set Up DHCP on pfSense. *OneUptime | One Complete Observability platform.* URL: https://oneuptime.com/blog/post/2026-03-20-set-up-dhcp-pfsense/view (дата звернення: 26.03.2026).

38. What is ARP (address resolution protocol)? How does it work?. *Fortinet*. URL: https://www.fortinet.com/uk/resources/cyberglossary/what-is-arp (дата звернення: 24.02.2026).

39. GeeksforGeeks. Virtual LAN (VLAN). *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/computer-networks/virtual-lan-vlan/ (дата звернення: 25.02.2026).

40. Lubuntu – The official Lubuntu home. *Lubuntu – The official Lubuntu home*. URL: https://lubuntu.me/ (дата звернення: 26.02.2026).

41. Cooper S. Deep packet inspection (DPI) guide including 8 best DPI tools. *Comparitech*. URL: https://www.comparitech.com/net-admin/deep-packet-inspection/ (дата звернення: 15.03.2026).

42. Suricata Documentation. *Suricata Documentation*. URL: https://suricata.io/documentation/ (дата звернення: 15.03.2026).

43. What is Snort?. *Snort*. URL: https://www.snort.org/ (дата звернення: 15.03.2026).

44. Vasileiadis A. Suricata vs snort: detailed guide to the programs. *Medium*. 27.08.2024. URL: https://medium.com/@redfanatic7/suricata-vs-snort-detailed-guide-to-the-programs-c331cff452a1 (дата звернення: 15.03.2026).

45. William K. PfSense: Setting up pfBlockerNG. *Substack*. URL: https://opensourceisfun.substack.com/p/pfsense-setting-up-pfblockerng (дата звернення: 15.03.2026).

46. Brester S. fail2ban: Daemon to ban hosts that cause multiple authentication errors. *GitHub*. URL: https://github.com/fail2ban/fail2ban (дата звернення: 12.03.2026).

47. Gómez R. Fail2ban cheat sheet for sysadmins. *Geeksta*. URL: https://geeksta.net/geeklog/fail2ban-cheat-sheet/ (дата звернення: 12.03.2026).

48. OpenSSH. *OpenSSH*. URL: https://www.openssh.org/ (дата звернення: 12.03.2026).

49. UFW - community help wiki. *Official Ubuntu Documentation*. URL: https://help.ubuntu.com/community/UFW (дата звернення: 12.03.2026).

50. Anicas M., Heidi E., Kurup M. UFW essentials: common firewall rules and commands for linux security. *AI-Native Cloud | DigitalOcean*. URL: https://www.digitalocean.com/community/tutorials/ufw-essentials-common-firewall-rules-and-commands (дата звернення: 12.03.2026).

51. Nginx documentation. *nginx*. URL: https://nginx.org/en/docs/ (дата звернення: 12.03.2026).

52. Tenzin C. A beginners guide to openSSH. *Medium*. URL: https://medium.com/@tenze_21/a-beginners-guide-to-openssh-6485d56d041d (дата звернення: 12.03.2026).

53. Kali docs | kali linux documentation. *Kali Linux*. URL: https://www.kali.org/docs/ (дата звернення: 26.03.2026).

54. GeeksforGeeks. Installing kali linux on virtualbox. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/linux-unix/how-to-install-kali-linux-in-virtualbox/ (дата звернення: 26.03.2026).

55. Introduction to VPNs. *Networklessons*. URL: https://networklessons.com/vpn/introduction-to-vpns (дата звернення: 20.05.2026).

56. What is IPsec? | How IPsec VPNs work. *Cloudflare*. URL: https://www.cloudflare.com/learning/network-layer/what-is-ipsec/ (дата звернення: 14.04.2026).

57. Secure VPN solutions for business & remote access | openvpn. *OpenVPN*. URL: https://openvpn.net/ (дата звернення: 20.05.2026).

58. WireGuard: fast, modern, secure VPN tunnel. *WireGuard: fast, modern, secure VPN tunnel*. URL: https://www.wireguard.com/ (дата звернення: 15.04.2026).

59. Hayden J. WireGuard VPN on Linux: Complete Setup Guide | LinuxBlog.io. *LinuxBlog.io*. URL: https://linuxblog.io/wireguard-vpn-linux-setup-guide (дата звернення: 15.04.2026).

60. What is SIEM? How security information & event management works. *Fortinet*. URL: https://www.fortinet.com/resources/cyberglossary/what-is-siem (дата звернення: 29.04.2026).

61. Wazuh documentation. *Wazuh documentation*. URL: https://documentation.wazuh.com/current/index.html (дата звернення: 29.04.2026).

62. How to install wazuh SIEM step by step. *Quape*. URL: https://www.quape.com/how-to-install-wazuh-on-vps-or-cloud/ (дата звернення: 29.04.2026).

63. TecnoDigital. Що таке Wazuh: Все про платформи SIEM та XDR з відкритим кодом. *Informática y Tecnología Digital*. URL: https://informatecdigital.com/uk/що-таке-вазух/ (дата звернення: 29.04.2026).

ДОДАТОК А
ТАБЛИЦЯ IP-АДРЕСАЦІЇ ТА МАРШРУТИЗАЦІЇ ІНЖЕНЕРНОГО СТЕНДА

Таблиця А.1 – Схема розподілу адресного простору комплексної системи захисту

№	Назва вузла / пристрою	Мережевий інтерфейс	Тип IP-адреси	IP-адреса / маска	Функціональне призначення інтерфейсу
1	Основний шлюз pfSense Master	em0 WAN	DHCP	192.168.1.111/24	Зовнішній транзитний канал, термінація IPS Suricata
2	Основний шлюз pfSense Master	em1 ADMIN	Статична IPv4	192.168.10.1/24	Шлюз технологічної мережі управління
3	Основний шлюз pfSense Master	em2 DMZ	Статична IPv4	10.0.3.1/24	Шлюз демілітаризованої серверної зони захисту
4	Резервний шлюз pfSense Backup	em0 WAN	DHCP	192.168.1.112/24	Резервний зовнішній транзитний канал зв'язку
5	Резервний шлюз pfSense Backup	em1 ADMIN	Статична IPv4	192.168.10.2/24	Резервний шлюз мережі адміністрування

6	Резервний шлюз pfSense Backup	em2 DMZ	Статична IPv4	10.0.3.1/24	Резервний шлюз демілітаризованої серверної зони
7	pfSense Master / Backup	em4 SYNC	Статична IPv4	192.168.254.1/24 192.168.254.2/24	Ізольований лінк міжкластерної синхронізації pfsync
8	Віртуальні IP-адреси CARP VIP	em1 ADMIN	Віртуальна	192.168.10.254/24	Спільна зовнішня адреса для публікації сервісів
9	Абонентський сегмент 1 VLAN 10	em3.10	Статична IPv4	172.16.10.1/24	Шлюз замовчуванням абонентської групи №1 (PoE/Static ARP
10	CPE / Клієнт VLAN 10	Клієнтський	DHCP	172.16.10.10/24	Клієнтська робоча станція
11	Абонентський сегмент 2 VLAN 20	em3.20	Статична IPv4	172.16.20.1/24	Шлюз замовчуванням абонентської групи №2 IPoE/Static ARP
12	CPE / Клієнт VLAN 20	Клієнтський	DHCP	172.16.20.10/24	Клієнтська робоча станція

13	Сервер віддаленого доступу VPN	tun_wg0	VPN тунель	10.0.5.1/24	Захищений криптографічний інтерфейс віддаленого адміністрування

ДОДАТОК Б
ІНСТРУКЦІЯ З НАЛАШТУВАННЯ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ

1. Загальні положення та призначення

1.1. Цей регламент визначає порядок організації захищеного доступу інженерного персоналу до ізольованої технологічної мережі управління з недовірених зовнішніх мереж.

1.2. В основі механізму віддаленого доступу лежить протокол WireGuard, який використовує асиметричну криптографію Curve25519 для обміну ключами та шифрування трафіку ChaCha20-Poly1305.

1.3. Будь-який прямий доступ до портів управління мережевим обладнанням чи серверами з глобальної мережі суворо заборонений. Усі адміністративні сесії мають проходити виключно через VPN-тунель.

2. Вимоги до безпеки клієнтських пристроїв

2.1. Конфігураційний файл клієнта .conf, який містить закритий приватний ключ, є критичним активом. Його передача стороннім особам або пересилання відкритими каналами зв'язку суворо заборонена.

2.2. Робоча станція інженера, з якої здійснюється підключення, повинна мати активований локальний міжмережевий екран, оновлене антивірусне ПЗ та увімкнене повнодискове шифрування.

3. Порядок ініціалізації клієнтського підключення

3.1. Завантажити та встановити офіційний клієнт WireGuard для відповідної операційної системи з ресурсу wireguard.com/install/.

3.2. Отримати від головного адміністратора згенерований конфігураційний файл, який містить такі обов'язкові параметри:

— PrivateKey – унікальний закритий ключ клієнта;

— Address – статична IP-адреса клієнта у транзитній VPN-підмережі;

— PublicKey – відкритий ключ магістрального шлюзу pfSense;

— Endpoint – публічна IP-адреса та UDP-порт маршрутизатора;

— AllowedIPs – перелік підмереж, трафік до яких буде маршрутизуватися через зашифрований тунель.

3.3. У графічному інтерфейсі клієнта натиснути «Додати тунель» (Add Tunnel) та імпортувати отриманий файл.

3.4. Натиснути кнопку «Активувати» (Activate). Успішне встановлення криптографічної сесії підтверджується зміною статусу на «Active» та появою лічильника отриманих даних (Received bytes) у розділі «Latest handshake».

4. Діагностика та усунення типових несправностей

4.1. **Проблема:** Тунель переходить у статус «Active», відправляються байти, але кількість отриманих байтів (Received) дорівнює нулю. Відсутній Handshake.

Рішення: Це свідчить про те, що клієнтські пакети не досягають шлюзу або відкидаються. Перевірити доступність нестандартного UDP-порту шлюзу. Переконатися, що публічний ключ клієнта коректно внесений до налаштувань Peer на стороні pfSense.

4.2. **Проблема:** Handshake відбувається успішно, але відсутній доступ до внутрішніх ресурсів.

Рішення: Перевірити параметр AllowedIPs у клієнтському конфігу чи включена туди цільова підмережа. Перевірити правила міжмережевого екрана на вкладці WireGuard у вебконсолі pfSense – чи дозволено трафік від IP-адреси VPN-клієнта до цільової зони.