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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра на тему: «Методи та технології побудови та адміністрування сегментованих мереж на базі відкритих рішень»

Виконав студент 2-го курсу групи КІм-23-1
спеціальності 123 «Комп’ютерна інженерія»
_____ Володимир ІВАНЕНКО

Керівник старший викладач кафедри КІ та КБ
_____ Ігор ФАЛЬКОВСЬКИЙ

Рецензент доцент кафедри КІ та КБ, к.т.н.
_____ Олексій ШЕЛУХА

Житомир – 2024

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
Андрій Єфіменко
17 09 2024 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу магістра

Студент: Іваненко Володимир Вадимович

Тема роботи: «Методи та технології побудови та адміністрування сегментованих мереж на базі відкритих рішень»

затверджена Наказом університету від 17 вересня 2024 р. № 478/с

Термін здачі студентом закінченої роботи 16 грудня 2024 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
1. Сегментована мережа
2. Технологія QEMU, VLAN, DNS

Обладнання та програмне забезпечення:

1. ПЗ Proxmox, Opnsense, Suricata
2. Операційна Debian Linux, FreeBSD, Windows Server
3. Ethernet USB-пристрій
4. ESP32 Cam
5. Платформа AMD Ryzen

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Фальковський І. Г	17.09.2024	17.09.2024
2	Фальковський І. Г	17.09.2024	17.09.2024
3	Фальковський І. Г	17.09.2024	17.09.2024

Студент _____ Іваненко В.В

Керівник _____ Фальковський І. Г

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	17.09.2024	Виконано
2	Пошук інформації стосовно сегментації	01.10.2024 - 15.10.2024	Виконано
3	Аналіз інструментів для маршрутизації та віртуалізації	16.10.2024	Виконано
4	Порівняння засобів маршрутизації та віртуалізації	17.10.2024 -20.10.2024	Виконано
5	Ознайомлення з особливостями архітектури	21.10.2024 -22.10.2024	Виконано
6	Ознайомлення з технологією Proxmox	23.10.2024-30.10.2024	Виконано
7	Вибір інструментів для маршрутизації	2.11.2024-5.11.2024	Виконано
8	Проєктування фізичної топології	12.11.2024	Виконано
9	Вибір технологій для побудови мережі	13.11.2024 - 15.11.2024	Виконано
10	Ознайомлення з технологією OPNSense	15.11.2024	Виконано
11	Вивчення інформації стосовно налаштувань OPNSense, ProxMox та RouterOS	16.11.2024 -25.11.2024	Виконано
12	Налаштування та тестування мережі	26.11.2024-8.12.2024	Виконано
13	Написання пояснювальної записки	8.12.2024-16.12.2024	Виконано
14	Отримання відгуку та рецензій	16.12.2024-26.12.2024	Виконано
15	Захист	27.12.2024	Виконано

Студент _____ Іваненко В.В

Керівник _____Фальковський І. Г

АНОТАЦІЯ

Кваліфікаційна робота складається з реалізації побудови сегментованої мережі на основі відкритих рішень та пояснювальної записки до неї. Пояснювальна записка містить 59 сторінок, 78 ілюстрацій, 2 таблиці та 2 додатки. Список використаних джерел містить 25 найменувань і займає 3 сторінки

Метою роботи є побудова сегментованої мережі на основі відкритих технологій і створення захищеного середовища.

В роботі проведена побудова сегментованої мережі на основі відкритих технологій та проведені налаштування технологій які забезпечують безпеку мережі.

Описані технології що використовуються для реалізації програмного рішення.

Ключові слова: СЕГМЕНТАЦІЯ, VLAN, DMZ, DNS, Proxmox, OPNsense, БЕЗПЕКА, IPS/IDS, ВІРТУАЛІЗАЦІЯ, МЕРЕЖА

ANNOTATION

The qualification work consists of the implementation of building a segmented network based on open solutions and an explanatory note to it. The explanatory note contains 59 pages, 78 illustrations, 2 tables and 2 appendices. The list of used sources contains 25 names and occupies 3 pages.

The purpose of the work is to build a segmented network based on open technologies and create a secure environment.

The work includes the construction of a segmented network based on open technologies and the configuration of technologies that ensure network security.

The technologies used to implement the software solution are described.

Keywords: SEGMENTATION, VLAN, DMZ, DNS, Proxmox, OPNsense, SECURITY, IPS/IDS, VIRTUALIZATION, NETWORK

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 6

ВСТУП 8

РОЗДІЛ 1 ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ 9

1.1 Основні принципи та методи сегментації мережі 9
1.2 Теоретичні відомості VLAN 10
1.3 Теоретичні відомості DMZ 14
1.4 Теоретичні відомості DNS 15
1.5 Переваги сегментації для продуктивності та безпеки. 16
Висновки до розділу 1 17

РОЗДІЛ 2. ВИБІР ТЕХНОЛОГІЙ ТА ІНСТРУМЕНТІВ 18

2.1 Визначення технічних вимог 18
2.2 Вибір гіпервізора та порівняння 18
2.3 Вибір засобу для маршрутизації 22
2.4 Інтеграція рішень між собою у рамках однієї мережі 23
Висновки до розділу 2 24

РОЗДІЛ 3.МЕТОДОЛОГІЯ ТА РЕАЛІЗАЦІЇ СЕГМЕНТОВАНОЇ МЕРЕЖІ 25

3.1 Проектування структури мережі і побудова фізичної інфраструктури 25
3.2 Встановлення та налаштування Proxmox 25
3.3 Початкові налаштування OPNsense 28
3.4 Налаштування маршрутизації 29
3.5 Налаштування комутатора 33
3.6 Налаштування безпеки 36
3.7 Налаштуваня безпеки DNS 39
3.8 Створення та налаштування правил фаєрволу 41
Висновки до розділу 3 48

РОЗДІЛ 4. ТЕСТУВАННЯ СЕРВІСІВ ТА ПЕРЕВІРКА БЕЗПЕКИ 49

4.1 Перевірка роботи 49
4.2 Перевірка безпеки 54
Висновки до розділу 4 56

ВИСНОВКИ 58

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 60

ДОДАТКИ 63

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – Операційна система

VLAN – Virtual Local Area Network

DMZ – Demilitarized Zone

DNS – Domain Name System

IPS/IDS – Intrusion Prevention/Detection System

NAT – Network Address Translation

USB – Universal Serial Bus

VPN – Virtual Private Network

KVM – Kernel-based Virtual Machine

QEMU – Quick Emulator

LXC – Linux Containers

RDP – Remote Desktop Protocol

WAN – Wide Area Network

LAN – Local Area Network

IoT – Internet of Things

DNSSEC – Domain Name System Security Extensions

DHCP – Dynamic Host Configuration Protocol

ВСТУП

Сучасні комп'ютерні мережі є основою функціонування інформаційних систем, що використовуються у різних галузях. В умовах стрімкого зростання обсягів даних, кількості пристроїв і вимог до безпеки, питання побудови ефективної мережевої інфраструктури стає все більш актуальним. У цьому контексті сегментація мережі є одним із ключових підходів для оптимізації використання ресурсів, забезпечення продуктивності та підвищення рівня безпеки.

Актуальність теми. Використання відкритих програмних рішень для побудови сегментованих мереж дозволяє знизити витрати, забезпечуючи при цьому високу функціональність і гнучкість у налаштуванні. Технології, такі як VLAN, DMZ, DNS, та інструменти, Proxmox і OPNsense, є хорошим рішенням для створення сучасних мережевих архітектур, які відповідають вимогам безпеки та продуктивності.

Мета роботи. Побудова сегментованої мережі на основі відкритих рішень, яка має ефективні засоби для адміністрування та забезпечення безпеки пристроїв.

Об'єкт дослідження. Сегментовані мережі, що забезпечують ізоляцію трафіку, підвищення безпеки та оптимізацію ресурсів.

Предмет дослідження. Методи та технології побудови і адміністрування сегментованих мереж із використанням відкритих рішень.

РОЗДІЛ 1 ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1 Основні принципи та методи сегментації мережі

Сегментація мережі є важливим аспектом проектування та управління комп'ютерними мережами, що сприяє підвищенню продуктивності, безпеки та ефективності використання ресурсів. Основні підходи до сегментації можна розділити на фізичну та логічну.

Фізична сегментація передбачає розділення мережі на окремі сегменти за допомогою фізичних пристроїв і каналів. Для кожного сегмента використовується власне обладнання, що дозволяє ізолювати пристрої різних сегментів, підключаючи їх до окремих мережевих елементів. Цей підхід мінімізує взаємний вплив трафіку та підвищує безпеку. Проте, його недоліками є висока вартість через необхідність у додатковому обладнанні та складність масштабування мережі.

Логічна сегментація здійснюється шляхом поділу мережі на віртуальні сегменти без модифікацій фізичної структури. Вона базується на принципах, таких як віртуальні локальні мережі VLAN, логічне розділення за портами, протоколами або групами користувачів. Також можуть використовуватися мітки для визначення належності пристроїв до певних сегментів. Перевагами цього підходу є гнучкість у налаштуванні, економія коштів, оскільки не потрібне нове обладнання, а також легкість інтеграції з сучасними протоколами. Однак це вимагає високої кваліфікації адміністраторів і може призводити до проблем з безпекою через можливі помилки в конфігурації.

Таким чином, обидва підходи мають свої сильні та слабкі сторони, і вибір між ними залежить від специфічних вимог мережі .

Таблиця 1.1

Порівняння підходів сегментації

Критерій	Фізична сегментація	Логічна сегментація
Вартість	Висока	Нижча
Гнучкість	Низька	Висока
Безпека	Висока	Залежить від налаштувань
Складність	Низька	Висока
Масштабованість	Складна	Легка

Фізична сегментація підходить для невеликих мереж або там, де критично важлива фізична ізоляція (наприклад, для конфіденційних даних). Логічну сегментація потрібно використовувати в корпоративних мережах, де важливі гнучкість, масштабованість та інтеграція з іншими технологіями.

У реальних умовах часто застосовується комбінація фізичної та логічної сегментації для досягнення балансу між безпекою та ефективністю

1.2 Теоретичні відомості VLAN

Віртуальною локальною мережею VLAN називається логічна група вузлів мережі, трафік якої, в тому числі і широкомовний, на канальному рівні повністю ізольований від інших вузлів мережі. Це означає, що передача кадрів між різними віртуальними мережами на підставі MAC-адреси неможлива незалежно від типу адреси - унікального, групового або широкомовного. У той же час всередині віртуальної мережі кадри передаються по технології комутації, тобто лише на той порт, який пов’язаний з адресом призначення кадру. Таким чином за допомогою віртуальних мереж вирішується проблема поширення широкомовних кадрів спричинених ними наслідків, які можуть розвинутися в широкомовні шторми істотно знизити продуктивність мережі.

На комутаторах можуть бути реалізовані наступні типи VLAN:

– На основі портів;

При такому типі кожен порт комутатора статично прив'язується до певної VLAN. Будь-який пристрій, підключений до цього порту, автоматично стає членом відповідної VLAN.

– На основі стандарту IEEE 802.1Q;

Цей тип використовує тегування кадрів Ethernet, додаючи ідентифікатор VLAN ID до кожного кадру. Це дозволяє передавати кілька VLAN через один фізичний порт (trunk port).(рис 1.2.1)

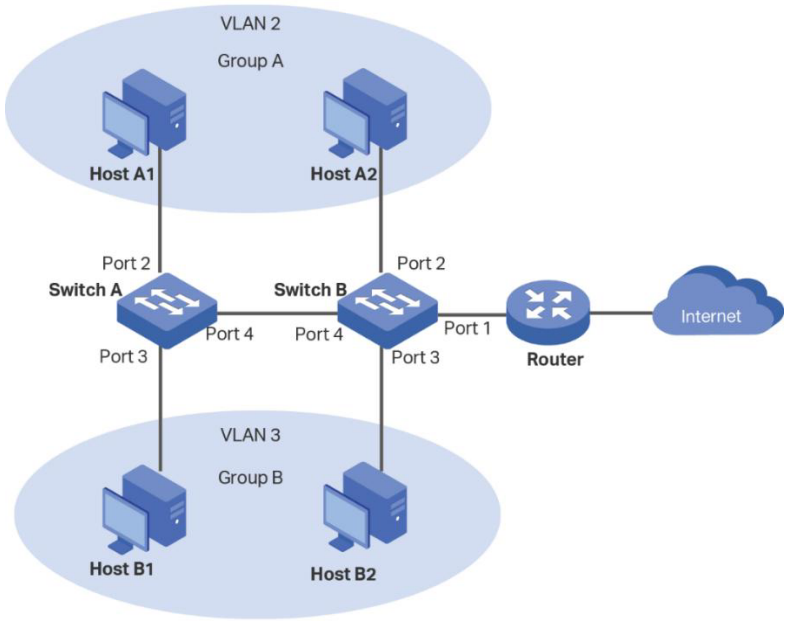


Рисунок 1.2.1 – VLAN на основі стандарту IEEE 802.1Q

– На основі стандарту IEEE 802.1ad (Q-in-Q VLAN);

Дозволяє вкладати одну VLAN у іншу (тегування в тегах)(рис 1.2.2)

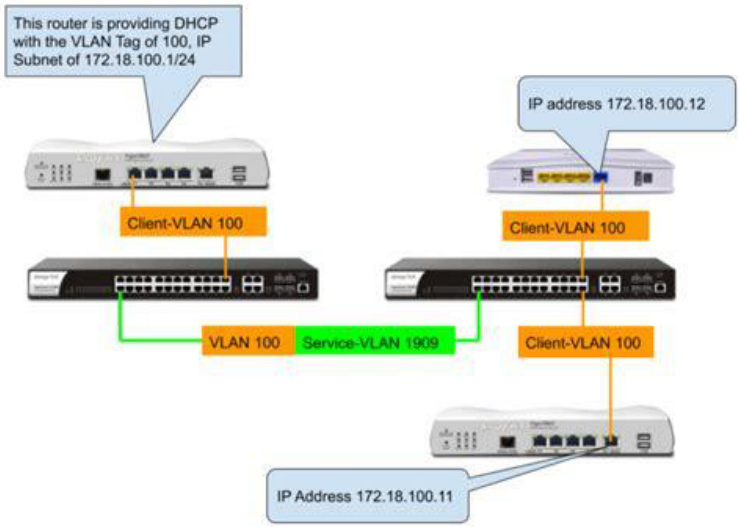


Рисунок 1.2.2 – VLAN на основі стандарту IEEE 802.1ad

– На основі портів і протоколів IEEE 802.1v;

VLAN створюються на основі мережевих протоколів (наприклад, IPv4, IPv6, ARP)

– На основі MAC-адрес;

У цьому випадку пристрої автоматично призначаються до VLAN на основі їхніх MAC-адрес.(рис 1.2.3)

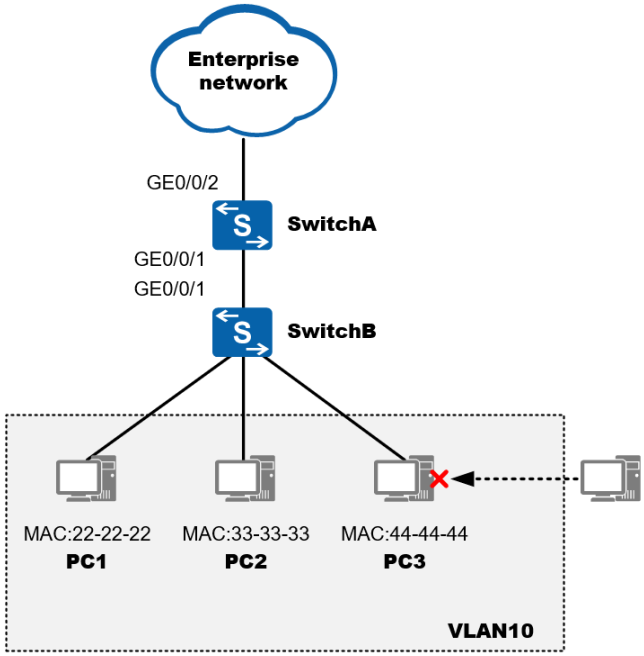


Рисунок 1.2.3 – VLAN на основі MAC адрес

– Асиметричні.

Дозволяють різним VLAN використовувати спільні порти для передачі даних.(рис.1.2.4)

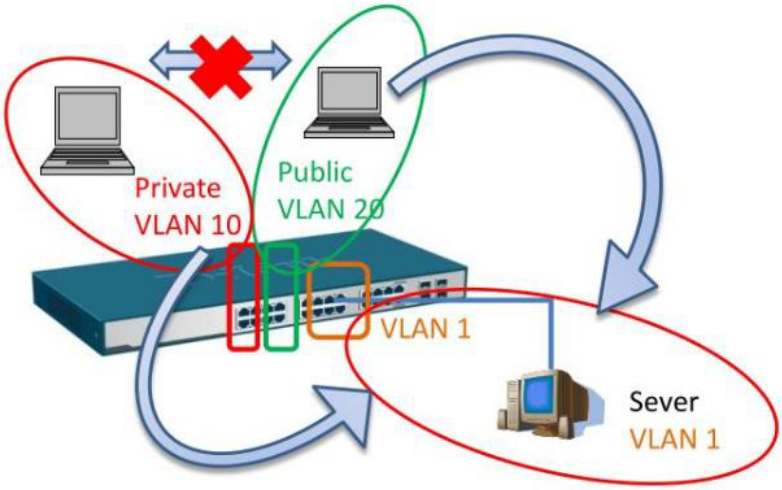


Рисунок 1.2.4 – Асиметричні VLAN

Також для сегментування мережі на канальному рівні моделі OSI в комутаторах можуть використовуватися інші функції, наприклад функція Traffic Segmentation. При правильному налаштуванні віртуальні локальні мережі покращують продуктивність зайнятих мереж. VLAN групують клієнтські пристрої, які часто спілкуються між собою. Трафік між пристроями, розділеними на дві або більше фізичних мереж, зазвичай обробляють основні маршрутизатори мережі. За допомогою VLAN цей трафік обробляється більш ефективно мережевими комутаторами.

Також це приносить переваги безпеці у великих мережах, дозволяючи краще контролювати, які пристрої мають доступ один до одного Адміністратори мережі часто посилаються на статичні VLAN як VLA на портах. У статичній VLAN адміністратор призначає окремі порти мереж перемикатися у віртуальну мережу. Незалежно від того, який пристрій підключається до цього порту, він стає членом цієї попередньо призначеної віртуальної мережі.

У динамічній конфігурації VLAN адміністратор визначає приналежність до мережі відповідно до характеристик пристроїв, а не розташування порту комутатора. Наприклад, динамічну VLAN можна визначити зі списком фізичних адрес (MAC-адреси) або іменами мережевих облікових записів.

Стандарти VLAN для мереж Ethernet відповідають галузевому стандарту IEEE 802.1Q. Стандарт 802.1Q складається з 32 бітів (4 байти) даних, вставлених у заголовок кадру Ethernet. Перші 16 біт цього поля містять жорстко закодований номер 0x8100, який запускає пристрої Ethernet розпізнавати кадр як належний 802.1Q VLAN. Останні 12 біт цього поля містять номер VLAN, число від 1 до 4094.

Класична мережа Ethernet це фізичне середовище спільної комунікації. При цьому за допомогою спеціального ПЗ можна перехопити конфіденційні повідомлення, паролі, тощо. Часто сегментувати таку мережу фізично немає змоги через географічні та інші обмеження. За допомогою віртуальних локальних мереж можна об’єднати всіх користувачів за рівнем доступу, правами, обов’язками, належністю до певного відділу й тощо. незалежно від місця їх знаходження. VLAN утворюють додатковий рівень безпеки, передаючи трафік в межах однієї

віртуальної мережі. Якщо фрейми є одно адресними, вони будуть відправлятися тільки на один заданий порт призначення, а не всім користувачам, тобто комутатор з налаштуваннями VLAN фільтрує трафік.

1.3 Теоретичні відомості DMZ

Демілітаризована зона (DMZ) — це архітектура мережевої безпеки, яка забезпечує ізоляцію внутрішньої мережі від зовнішніх загроз через створення проміжного сегмента. DMZ розташовується між внутрішньою мережею (LAN) та недовіреною мережею, як-от інтернет. Цей сегмент використовується для розміщення ресурсів, доступних ззовні, таких як веб-сервери, поштові сервери або DNS.

Головна мета DMZ це додати рівень безпеки, що ускладнює доступ до внутрішньої мережі навіть у разі атаки на публічні сервіси. Архітектура DMZ базується на принципі «захисту в глибину», де кожен рівень мережі має свої протоколи та політики безпеки. Ресурси в DMZ ізольовані, що зменшує ризик поширення атаки на конфіденційні дані.

Для налаштування DMZ часто використовуються брандмауери з різними наборами правил, що забезпечує контроль трафіку між сегментами. Наприклад, атакуючий може отримати доступ лише до серверів DMZ, не маючи прямого доступу до внутрішньої мережі. Впровадження DMZ передбачає використання маршрутизаторів, брандмауерів і політик доступу.

Ефективність архітектури перевіряється через аналіз трафіку. Інструменти на кшталт Wireshark дозволяють ідентифікувати пакети, які можуть спробувати проникнути в DMZ. Якщо конфіденційні сервери не відповідають на запити з інтернету, то архітектура працює правильно.

DMZ може бути реалізована у дротових і бездротових середовищах. Зараз актуальною є задача створення Wireless DMZ (WDMZ), яка враховує специфіку бездротових мереж і їхні загрози, такі як перехоплення даних і несанкціонований доступ.

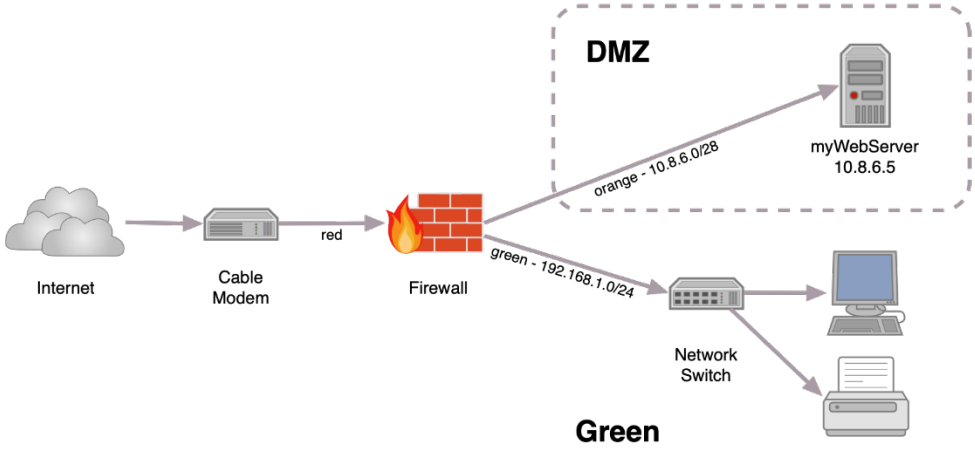


Рисунок 1.3.1 – Принцип побудови DMZ

1.4 Теоретичні відомості DNS

Система доменних імен (DNS) — це основа сучасної мережевої архітектури, що забезпечує перетворення доменних імен на IP-адреси, необхідні для взаємодії пристроїв у мережі. Ця система функціонує як «телефонна книга» Інтернету, дозволяючи користувачам працювати з доменами, а не складними числовими адресами.

DNS працює за допомогою багаторівневої ієрархії серверів. Запити проходять кілька етапів (рис 1.4.1):

1. Клієнт звертається до локального резолвера, який шукає інформацію в кеші.
2. У разі відсутності відповіді резолвер звертається до кореневих серверів, далі — до серверів домену верхнього рівня (наприклад, .com), і завершує пошук на сервері авторизації для конкретного домену.
3. Після отримання IP-адреси клієнт встановлює з'єднання з потрібним ресурсом.

Локальні DNS-рішення, дозволяють створювати записи для внутрішніх серверів чи пристроїв. Це спрощує управління мережею та зменшує навантаження на зовнішні DNS-сервери. Для налаштування DNS необхідно правильно визначити ієрархію серверів і політики. Наприклад, у OPNsense можна інтегрувати UnboundDNS із фільтрацією та захистом від атак. Перевірка ефективності

конфігурації здійснюється за допомогою аналізу DNS-трафіку через такі інструменти, як Wireshark.

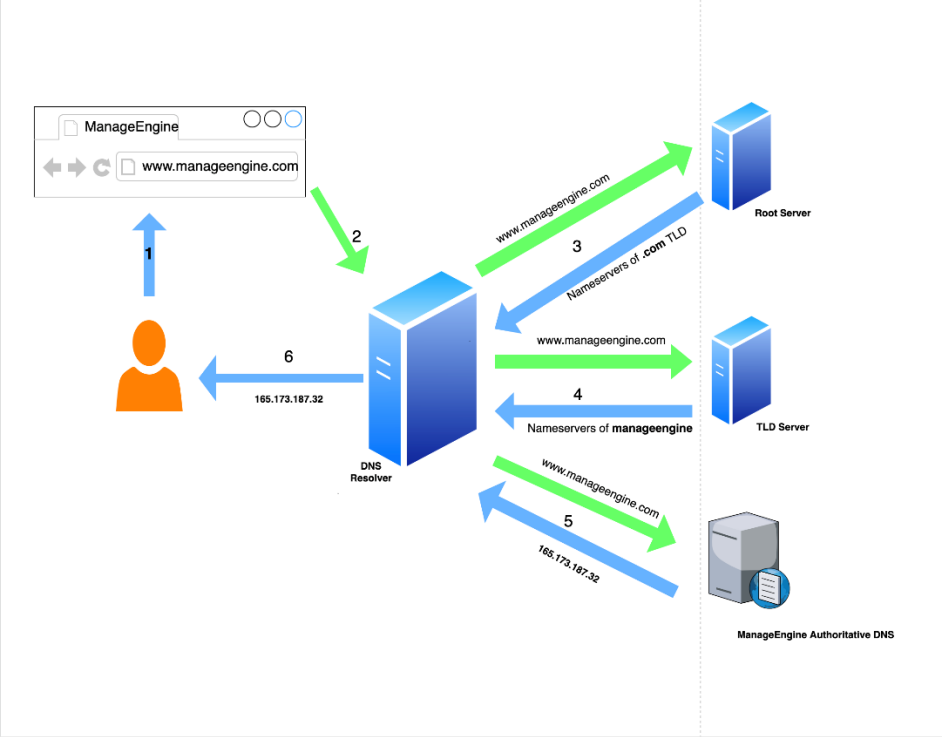


Рисунок 1.4.1 – Принцип роботи DNS

1.5 Переваги сегментації для продуктивності та безпеки.

Сегментація мережі є ефективним підходом для зменшення мережевого трафіку, оскільки широкомовні запити обмежуються рамками кожного сегмента. Це сприяє зниженню навантаження на всю мережу, що особливо важливо для великих підприємств. Менша кількість трафіку в межах сегментів також прискорює передачу даних між пристроями, що позитивно впливає на загальну продуктивність.

Крім того, сегментація дозволяє оптимізувати використання ресурсів. Ви можете виділяти окремі сегменти для критичних додатків і завдань, гарантуючи надійний доступ до необхідної смуги пропускання. Нові сегменти можна легко інтегрувати, не порушуючи стабільності роботи інших частин мережі.

У контексті безпеки сегментація забезпечує ефективний контроль доступу до конфіденційних даних, розділяючи інформацію на спеціалізовані сегменти. Це суттєво підвищує захист від несанкціонованого доступу та дозволяє

впроваджувати різноманітні політики безпеки для кожного сегмента. Наприклад, ви можете налаштувати специфічні фільтри та політики контролю доступу, що покращують загальний рівень захисту мережі. Розподіл на сегменти також знижує ризик поширення атак: якщо один сегмент зазнає компрометації, загроза не поширюється на інші частини мережі.

Висновки до розділу 1

У першому розділі розглянуто основні теоретичні відомості, що є основою для побудови сегментованих мереж: визначено основні підходи до сегментації мережі, включаючи фізичну сегментацію (засновану на розділенні фізичних компонентів) та логічну сегментацію (на основі програмних рішень). Описано принципи роботи віртуальних локальних мереж (VLAN), які забезпечують логічну ізоляцію трафіку в межах однієї фізичної інфраструктури. VLAN сприяють ефективному використанню мережевих ресурсів і підвищенню безпеки завдяки можливості поділу мережі на ізольовані сегменти. Розглянуто поняття демілітаризованої зони (DMZ) як методу підвищення захищеності критичних сервісів шляхом їх ізоляції від внутрішньої мережі та прямого доступу ззовні.

Наведено основи роботи системи доменних імен (DNS), яка забезпечує зручний доступ до мережевих ресурсів через імена замість IP-адрес. Вказано на її роль у забезпеченні продуктивності та зручності в роботі мережі. Проаналізовано ключові переваги сегментації, серед яких підвищення продуктивності мережі через зменшення конфліктів трафіку та підвищення безпеки шляхом ізоляції підмереж і обмеження впливу потенційних загроз. Таким чином, розглянуті у розділі теоретичні аспекти забезпечують базис для подальшого вибору технологій та інструментів, необхідних для проектування та впровадження сегментованих мереж.

РОЗДІЛ 2. ВИБІР ТЕХНОЛОГІЙ ТА ІНСТРУМЕНТІВ

2.1 Визначення технічних вимог

Програмне забезпечення має бути безкоштовним. Гіпервізор повинен мати підтримку KVM для повної віртуалізації, тим самим працювати на високій швидкості обробки мережевих запитів без значного навантаження на ресурси. Фаєрвол повинен мати функціональність для створення, керування та управління трафіком між VLAN і підтримку IPS/IDS. Загальними вимогами є підтримка сучасних стандартів шифрування та автентифікації, можливість розширення конфігурації мережі без значних змін, інтеграція всіх компонентів у єдину екосистему та реалізація інструментів для спостереження за станом мережі та виявлення проблем. Також плюсом буде наявність веб-інтерфейсу для адміністрування.

2.2 Вибір гіпервізора та порівняння

Proxmox — це платформа віртуалізації з відкритим кодом, основана на модифікованому ядрі Debian GNU/Linux, яка поєднує технології KVM та LXC в одному інтерфейсі. Вона надає прості механізми управління віртуальними машинами та контейнерами через веб-інтерфейс (рис.2.2.1), CLI або REST API, а також дозволяє керувати системою за допомогою скриптів. Як і LXC, система може запускати кілька ізольованих Linux-систем на одному хості, що робить її чудовим рішенням для контейнеризованих застосунків. KVM суттєво пришвидшує створення віртуальних машин, запускаючи кілька операційних систем майже на рівні нативної продуктивності. Кожна віртуальна машина має свої ресурси, такі як мережа, диск, графічні адаптери тощо, таким чином вдається зекономити на витратах на апаратні ресурси. Proxmox підтримує кластеризацію, що дозволяє кільком вузлам працювати разом як одна віртуальна інфраструктура. Файлова система pmxcfs дозволяє платформі синхронізувати свої конфігурації в режимі реального часу для досягнення прийнятного рівня доступності та стабільності. Ця функція міграції поза каналом дозволяє живу міграцію віртуальних машин між

вузлами. Вбудовані брандмауери, підтримка IPv4 та IPv6, а також контрольований доступ через налаштування ACL забезпечують потужну безпеку. Proxmox також пропонує вбудовані можливості для резервного копіювання та відновлення даних, включаючи варіанти швидкого відновлення віртуальних машин і контейнерів. Крім того, інструмент високої доступності High Aavailability робить можливим створення надійних кластерів, які самовідновлюються при виході з ладу одного з вузлів

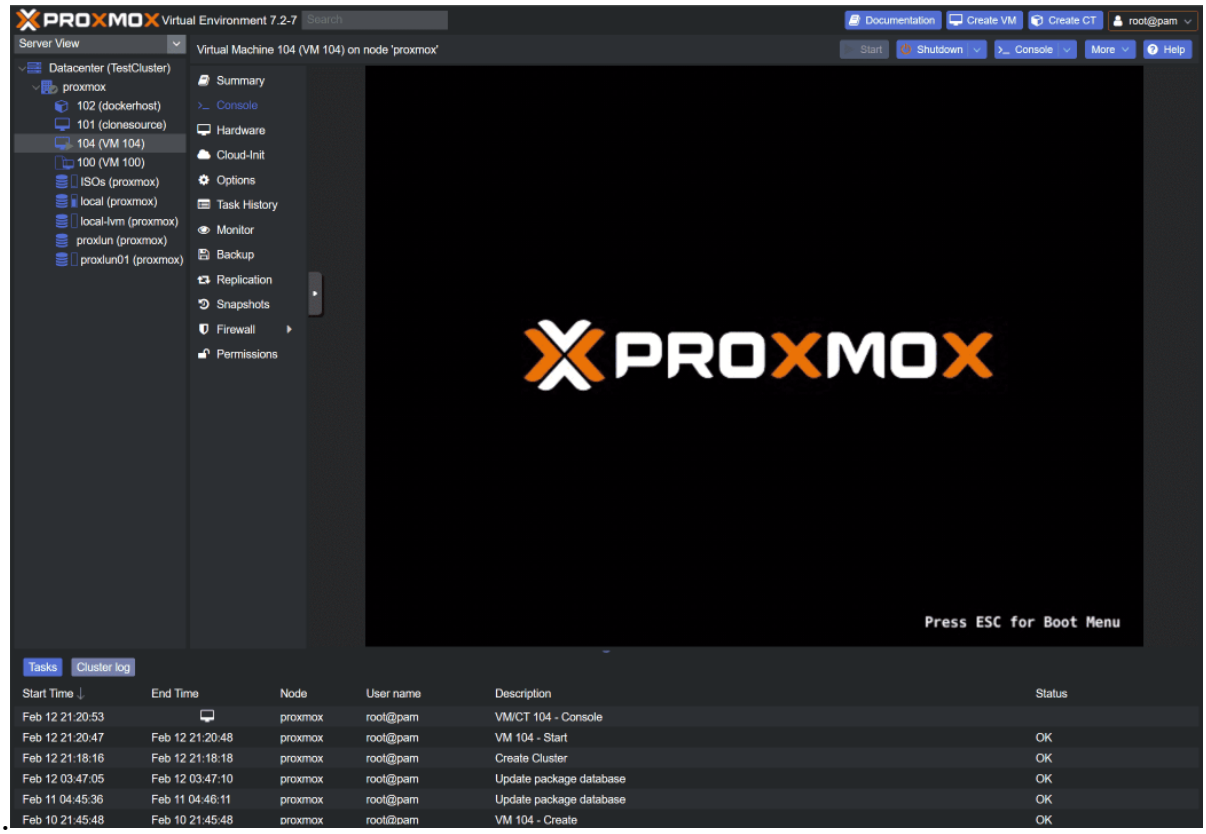


Рисунок 2.2.1 – Веб-інтерфейс панелі керування Proxmox

VMware vSphere - це термін, що позначає рішення віртуалізації, які допомагають керувати, відстежувати і налаштовувати віртуальний центр обробки даних VMware. Центральним ядром vSphere є сам гіпервізор VMware ESXi який встановлюється безпосередньо на пристрій та працює як мініатюрна ОС. Інші компоненти Vsphere це сервер VCENTER, клієнт VSPHERE та Vspere Web (рис 2.2.2). Вони використовуються для управління одним або декількома машинами.

Коли машини об'єднуються у кластер, він керується сервером VCENTER, який контролює всіма ресурсами віртуальних машин. Сервер VCENTER може бути

запущений зовні або як частина кластера. При адміністративному кластері адміністратори підключаються до сервера VCENTER, використовуючи Vsphere Клієнт або веб-клієнт. VMware Vsphere має високу функцію доступності, яка забезпечує доступність віртуальних машин в разі відмови.

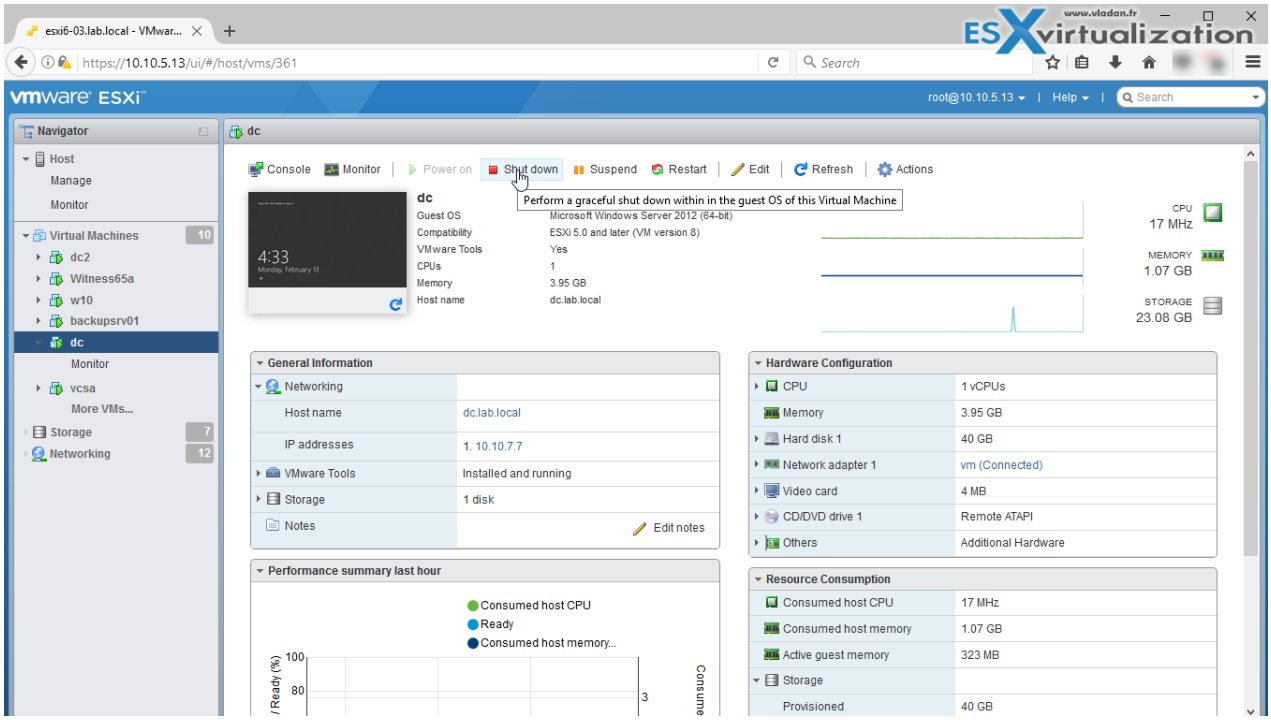


Рисунок 2.2.2 - Веб-інтерфейс панелі керування VMware vSphere

Citrix XenServer — це платформа для віртуалізації, що забезпечує широкий набір функцій для управління віртуальними середовищами. Вона як Proxmox і VMware vSphere, пропонує єдину точку управління віртуальними машинами, але заснована на абсолютно іншій архітектурі.

XenServer використовує гіпервізор Xen, який відзначається технологією паравіртуалізації. Цей підхід дозволяє отримати велику потужність і доступність завдяки оптимізації віртуальних машин до апаратної частини. З метою підвищення ефективності роботи з різними типами навантажень, однією з важливих можливостей XenServer є підтримка паравіртуалізованих і повністю віртуальних машин.

Кожна система здатна масштабуватися, тому ключовою функцією XenServer є Citrix Cloud, який дозволяє використовувати хмарні ресурси. Адміністрування системи легке за рахунок XenCenter — графічний інтерфейс (рис 2.2.3), який

дозволяє адміністратору контролювати віртуальні машини. Забезпечення високої доступності реалізовано шляхом автоматичного перезапуску віртуальних машин на інших хостах у разі виникнення апаратних збоїв. Це мінімізує час простою та гарантує безперервність процесів.

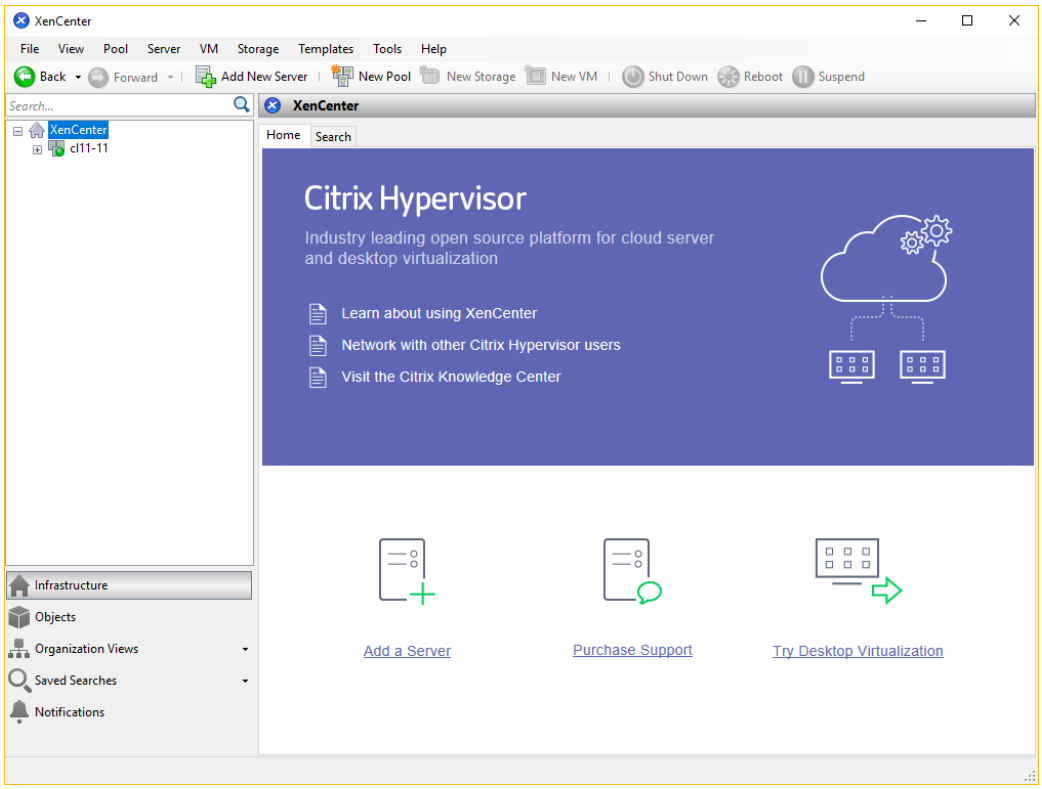


Рисунок 2.2.3 - Інтерфейс панелі керування Citrix XenServer

Вибір Proxmox є обґрунтованим рішенням завдяки його відкритій архітектурі, безкоштовному доступі та простоті налаштування. Він дозволяє легко створювати та управляти віртуальними машинами та контейнерами, що робить його ідеальним для розгортання різних сервісів у домашньому середовищі.

Веб-інтерфейс є інтуїтивно зрозумілим, що дозволяє навіть новачкам швидко освоїтися. У порівнянні з конкурентами, vSphere від VMware, Proxmox не вимагає високих витрат на ліцензування, хоча існує безкоштовна версія VMware ESXi Free Edition яка надає певний функціонал але обмежена в розширених можливостях, таких як резервне копіювання та кластеризація, також він може бути складним у налаштуванні та вимагати значних технічних знань, що може бути перешкодою для користувачів, які не мають досвіду в цій галузі. Citrix Hypervisor, хоча і пропонує деякі корисні функції, може бути менш гнучким в домашніх

умовах, оскільки його основна орієнтація на віртуалізацію робочих столів може не відповідати потребам користувачів, які хочуть розгортати різноманітні серверні додатки. Крім того, Citrix має обмежену підтримку спільнотою, що ускладнює адміністрування та вирішення проблем. Отже, Proxmox є оптимальним вибором для домашньої мережі завдяки своїй доступності, простоті використання та гнучкості, в той час як конкуренти мають недоліки, які роблять їх менш оптимальними для домашніх мереж.

2.3 Вибір засобу для маршрутизації

PfSense та OPNsense це платформи мережевої безпеки, які, попри схожість, мають свої унікальні риси. PfSense, розроблений компанією Netgate, є класичним вибором із багаторічною історією, що пропонує перевірену стабільність і підтримку корпоративного рівня. OPNsense, у свою чергу, виріс із бажання створити відкриту і сучасну альтернативу яка відзначається інтуїтивно зрозумілим інтерфейсом, регулярними оновленнями, гнучкістю та прозорістю, пропонуючи новітні API, детальну звітність і привабливий дизайн. PfSense зберігає свою силу у традиціях і функціональності, забезпечуючи стабільність для тих, хто цінує перевірені рішення.(рис 2.3.2)

OPNsense розроблений на базі FreeBSD, призначена для забезпечення мережевої безпеки та управління. Вона виконує функції брандмауера, маршрутизатора, VPN-сервера, системи фільтрації контенту і захисту від загроз. Завдяки фільтрації пакетів (PF), OPNsense надає гнучкі налаштування брандмауера та NAT. Підтримка OpenVPN, IPSec, WireGuard і PPTP дозволяє створювати захищені VPN-з’єднання. Функціонал IDS/IPS на базі Suricata допомагає виявляти та нейтралізувати загрози. Платформа оснащена зручним веб-інтерфейсом (рис 2.3.1) для моніторингу трафіку, аналітики та управління журналами. Можливості системи можна розширити плагінами, зокрема для двофакторної автентифікації чи антивірусу. Підтримка VLAN, балансування навантаження та резервування забезпечує високу стабільність мережі, а регулярні оновлення підтримують актуальний рівень безпеки.

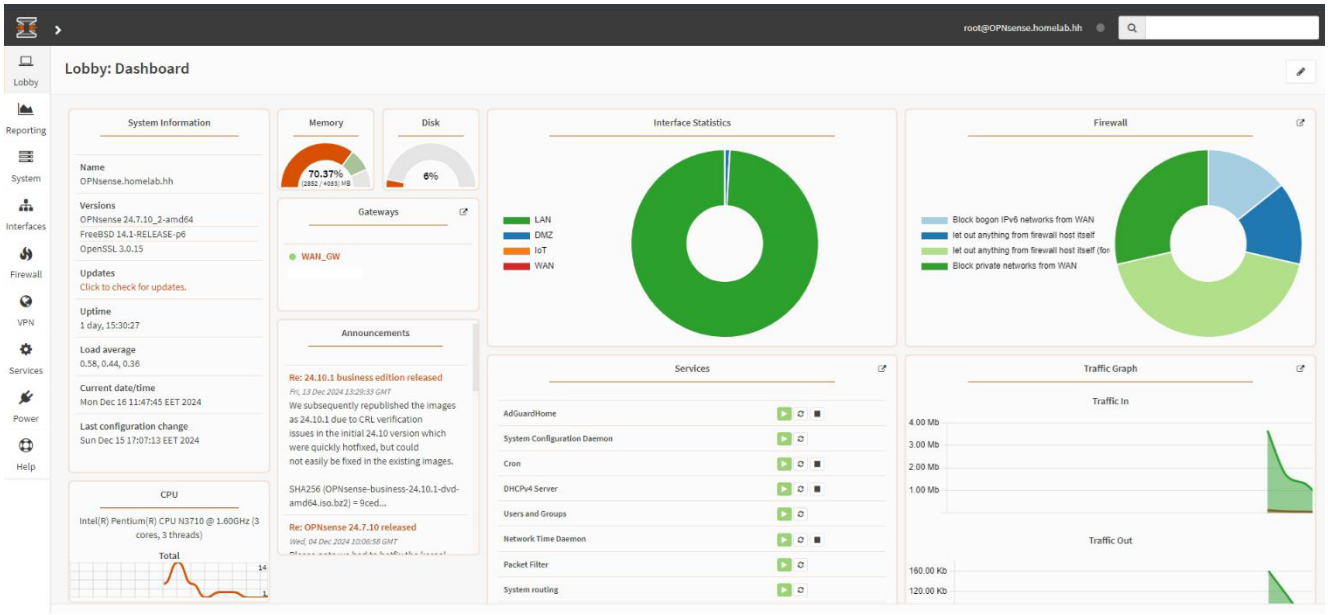


Рисунок 2.3.1 – Веб-інтерфейс панелі показників Opnsense

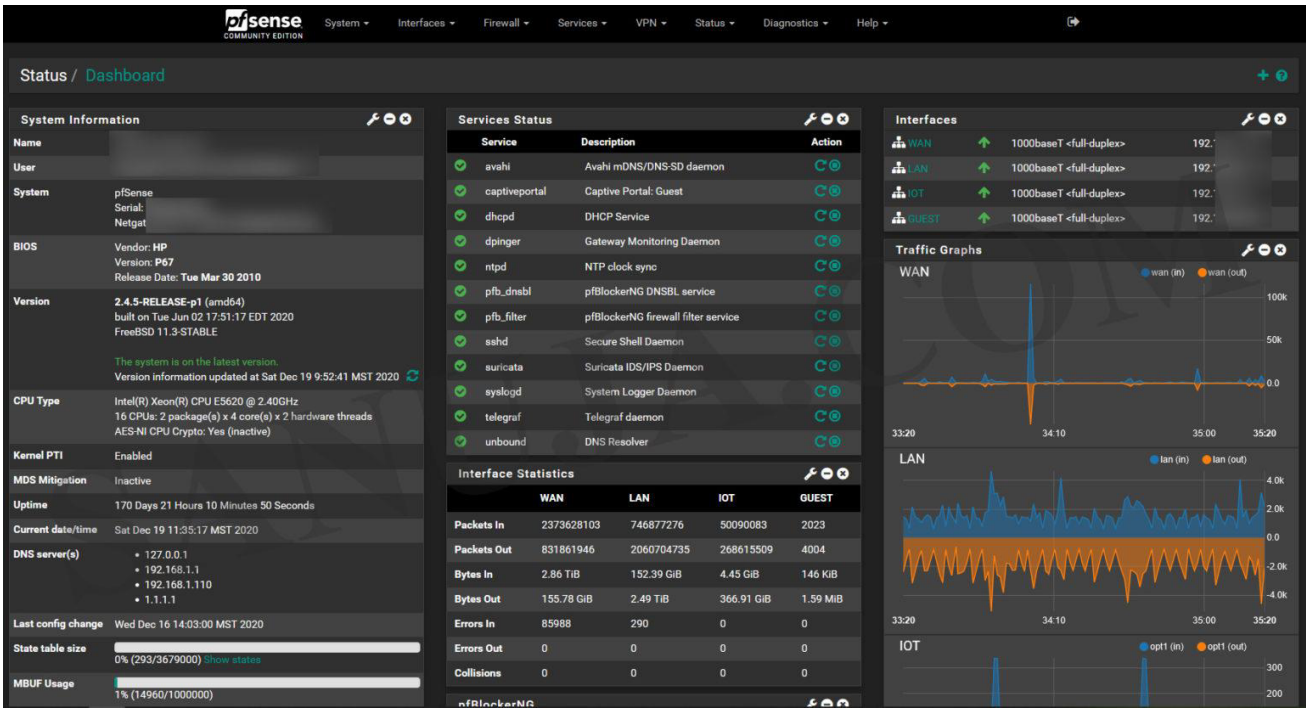


Рисунок 2.3.2 – Веб-інтерфейс панелі показників pfSense

2.4 Інтеграція рішень між собою у рамках однієї мережі

Інтеграція відкритих програмних рішень у локальній мережі дозволяє ефективно організувати сегментацію та ізоляцію трафіку. Proxmox використовується для розгортання OPNsense який забезпечує управління VLAN і виконує між мережеву маршрутизацію та впроваджує IDS/IPS для покращення

безпеки. Mikrotik виконує функції керованого комутатора з підтримкою VLAN і створює Wi-Fi точки доступу для різних груп користувачів. Така структура сприяє побудові гнучкої та захищеної мережевої архітектури, оптимізуючи ресурси і спрощуючи адміністрування.

Висновки до розділу 2

У цьому розділі було встановлено ключові технічні вимоги до побудови сегментованої мережі, серед яких забезпечення масштабованості, продуктивності, безпеки, обґрунтовано вибір відкритого програмного забезпечення та інструментів Proxmox і OPNsense. Рішення базуються на їх функціональності, простоті налаштування та доступності.

Проведено порівняння доступних гіпервізорів (OPNSense, CitrixXen, VMware ESXi) за критеріями продуктивності, сумісності, гнучкості в налаштуванні та використання відкритого програмного забезпечення. У результаті обрано Proxmox як найбільш відповідний варіант для реалізації поставлених завдань.

Також, у розділі обгрунтовано методи інтеграції обраних технологій для забезпечення узгодженої роботи компонентів та визначено ключові аспекти взаємодії гіпервізора, засобів маршрутизації і інших компонентів, що гарантують стабільну та ефективну роботу сегментованої мережі.

РОЗДІЛ 3.МЕТОДОЛОГІЯ ТА РЕАЛІЗАЦІЇ СЕГМЕНТОВАНОЇ МЕРЕЖІ

3.1 Проектування структури мережі і побудова фізичної інфраструктури

Проектування структури мережі складається з кількох ключових етапів, а саме визначення вимог до мережі, потреб користувачів, пристроїв та служб, і вимог до пропускної здатності, надійності та безпеки.

Мережа повинна бути гнучкою, безкоштовною в плані програмного забезпечення та дешевою у фізичній реалізації. Обране раніше ПЗ, добре підходить для цієї задачі. Proxmox буде розміщений на пристрої з достатньою потужністю центрального процесора та великим обсягом оперативної пам’яті і дискового простору, єдина проблема яка виникає у такому випадку, це недостатня кількість портів Ethernet, але вирішення цього це додаткові USB адаптери, які мають підтримку Proxmox. Сегментація засобами OPNsense, буде поділена на мережу LAN для основних робочих станцій, мережу VLAN для IoT пристроїв та DMZ для Windows Server. В якості комутатора пристроїв та точки доступу використаний Mikrotik hAP lite, який має хороший функціонал та невелику ціну, що робить його гарним вибором для домашніх мереж.

Для забезпечення безпеки мережі розробляються політики доступу та фільтрації трафіку для кожного VLAN, а також використовуються система для виявлення загроз (IDS/IPS) Suricata та брандмауери. Фізична топологія зірка.

3.2 Встановлення та налаштування Proxmox

В якості середовища для розгортання Proxmox, було обрано ноутбук на основі процесора Intel, який має 4 ядра та 4 потоки, 8 гігабайт оперативної пам’яті та внутрішнє сховище SSD обсягом у 120 гб.

Завантаживши ISO файл з офіційного сайту, була проведена інсталяція.(рис 3.2.1)

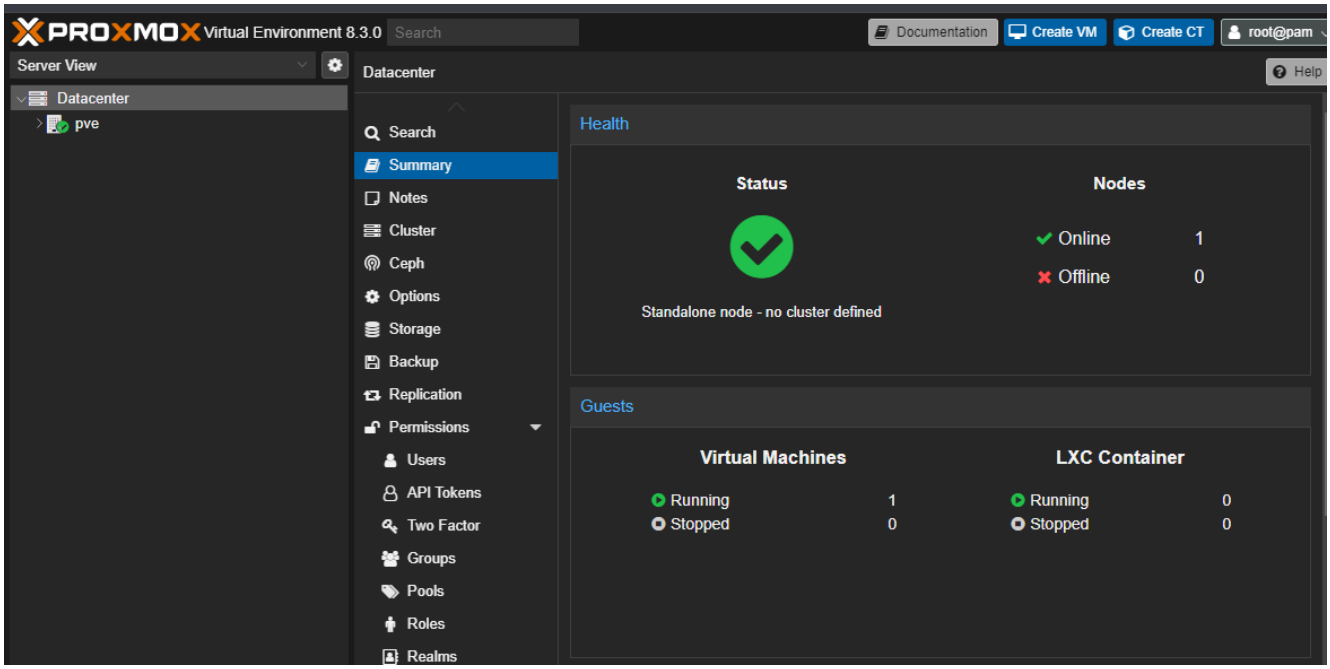


Рисунок 3.2.1 – Огляд середовища Proxmox

Наступним етапом буде налаштування мережевих інтерфейсів, додавання USB адаптерів та створення віртуальних мостів (рис 3.2.2).

Name	Type	Active	Autostart	VLAN a...	Ports/Slaves	Comment
eno1	Network Device	Yes	No	No		Фізичний Ethernet порт
enx00e04c680060	Network Device	No	No	No		USB адаптер для DMZ
enxc84d4429cc54	Network Device	Yes	No	No		USB адаптер для WAN
vmbr0	Linux Bridge	Yes	Yes	No	eno1	main bridge
vmbr1	Linux Bridge	Yes	Yes	No	enxc84d4429cc54	wan
vmbr2	Linux Bridge	Yes	Yes	No	enx00e04c680060	DMZ

Рисунок 3.2.2 – Огляд мережевих адаптерів

В системі присутні фізичні порти, eno1, основний порт вбудований в материнську плату та USB адаптери. До них було налаштовано 3 віртуальні мости vmbr для коректної роботи з віртуальними машинами, і позначені як WAN, LAN і DMZ. Тобто, через порт WAN весь трафік заходить в пристрій та через порт LAN та DMZ виходить.

Далі створюється віртуальна машини OPNsense (рис 3.2.3).

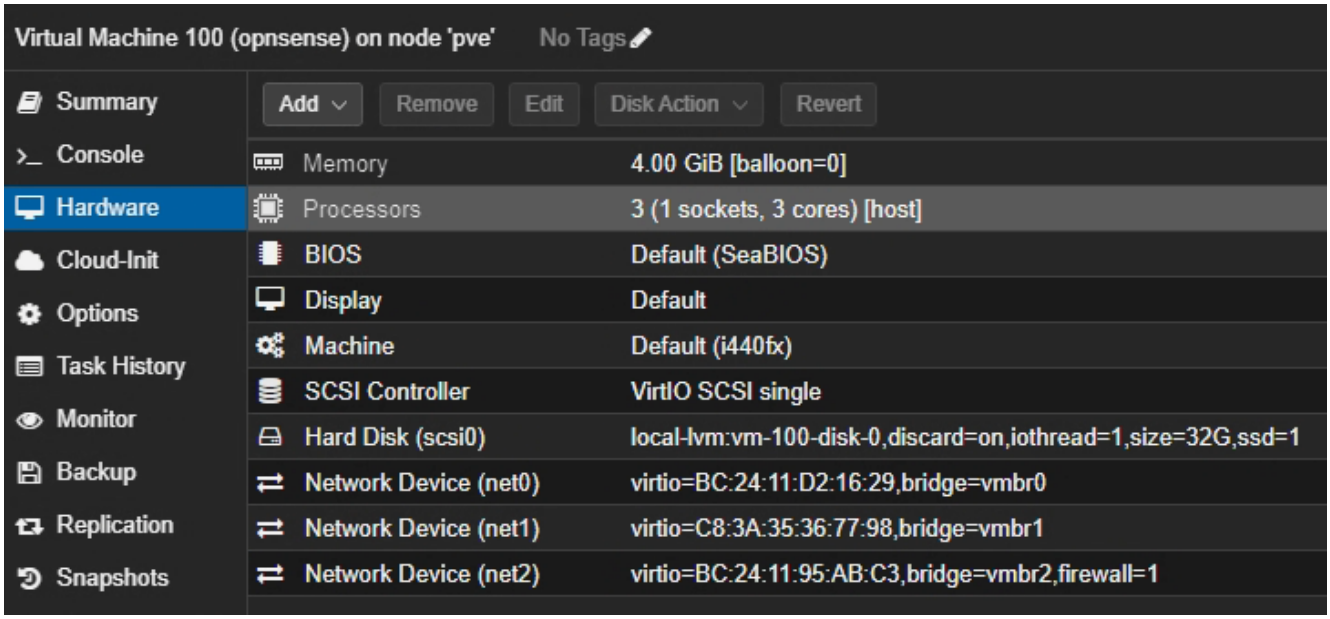


Рисунок 3.2.3 – Створення віртуальної машини Opnsense

Мережеві адаптери додаємо окремо, та прописуємо MAC-адресу для коректної роботи інтернет провайдера.

Для забезпечення безперервної роботи, потрібно увімкнути резервне копіювання, яке буде виконуватись кожної неділі о 1 годині ночі і зберігатись на локальному сховищі (рис 3.2.4).

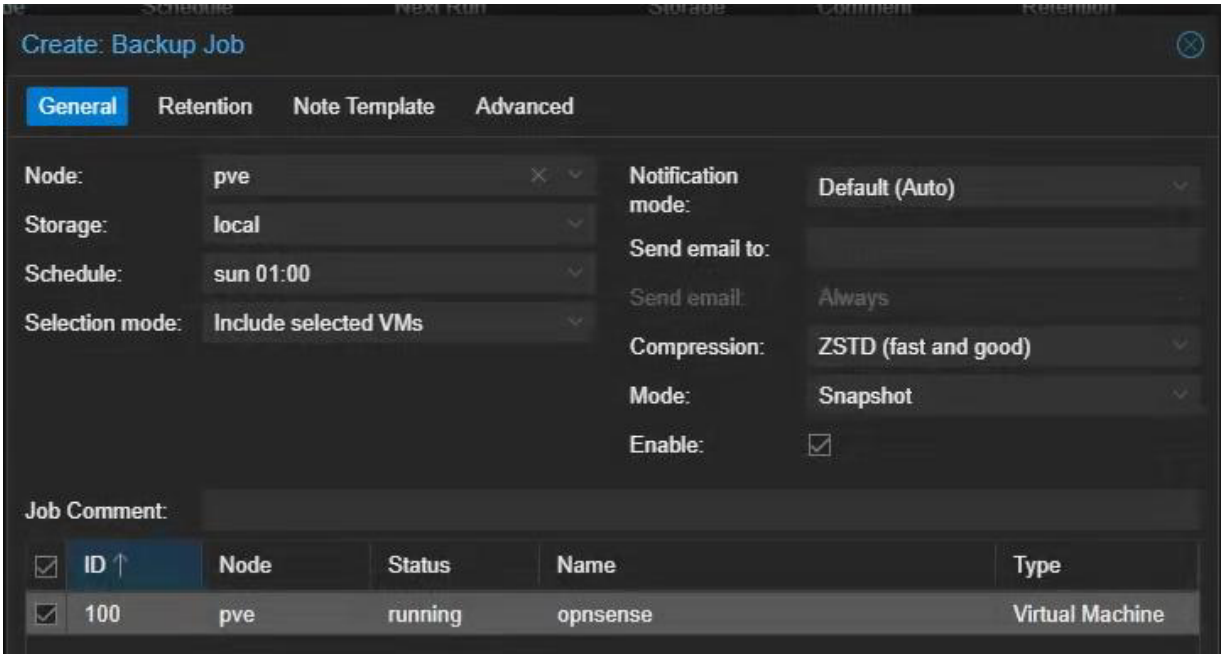


Рисунок 3.2.4 – Налаштування резервного копіювання

3.3 Початкові налаштування OPNsense

Щоб провести початкові налаштування, потрібно перейти до System > Wizard та слідувати покроковій інструкції. На цьому етапі важливим моментом є не вмикати параметр “Allow DNS servers to be overridden by DHCP/PPP on WAN”, який запобігає використанню DNS від провайдера що забезпечує справну роботу власного DNS серверу (рис 3.3.1). Наступні кроки це налаштування часового поясу (рис 3.3.2), адреси порту WAN, даними інтернет провайдера (рис 3.3.3) та налаштування порту LAN (рис 3.3.4).

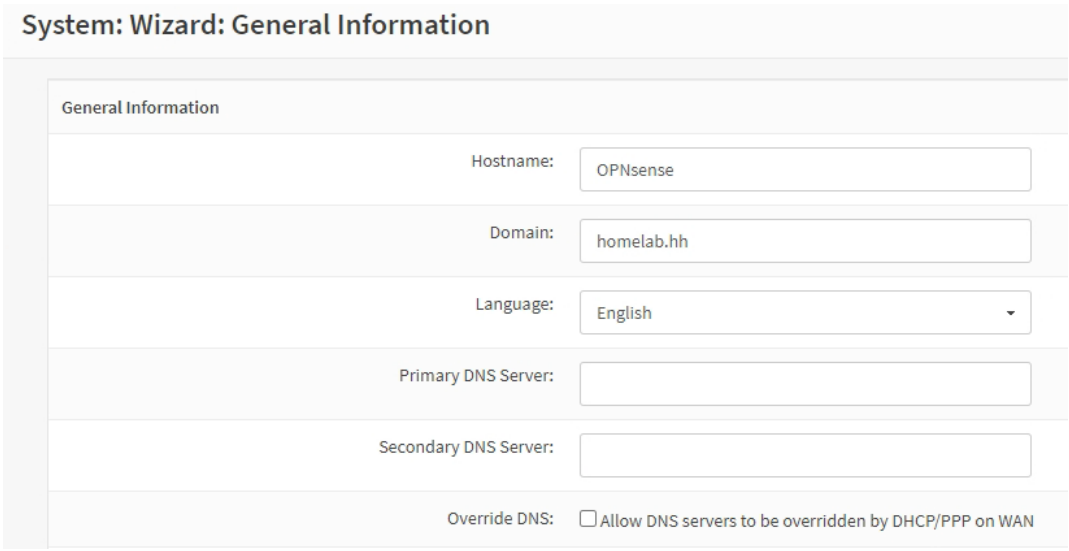


Рисунок 3.3.1 – Налаштування імен домену та DNS

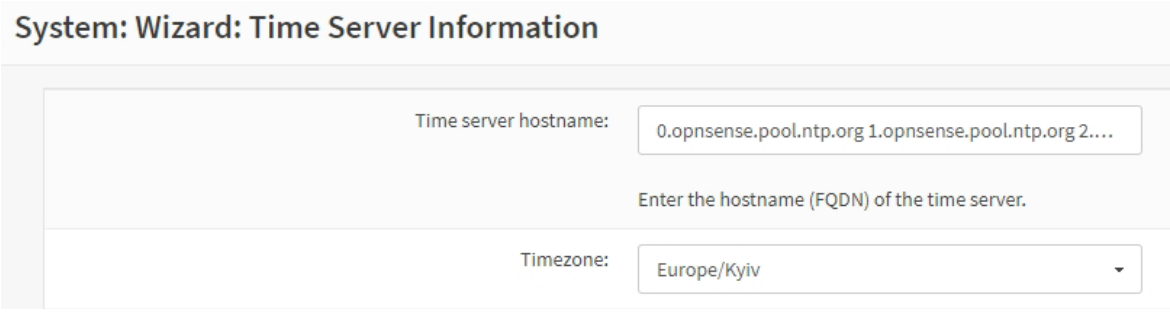


Рисунок 3.3.2 – Налаштування часового поясу системи

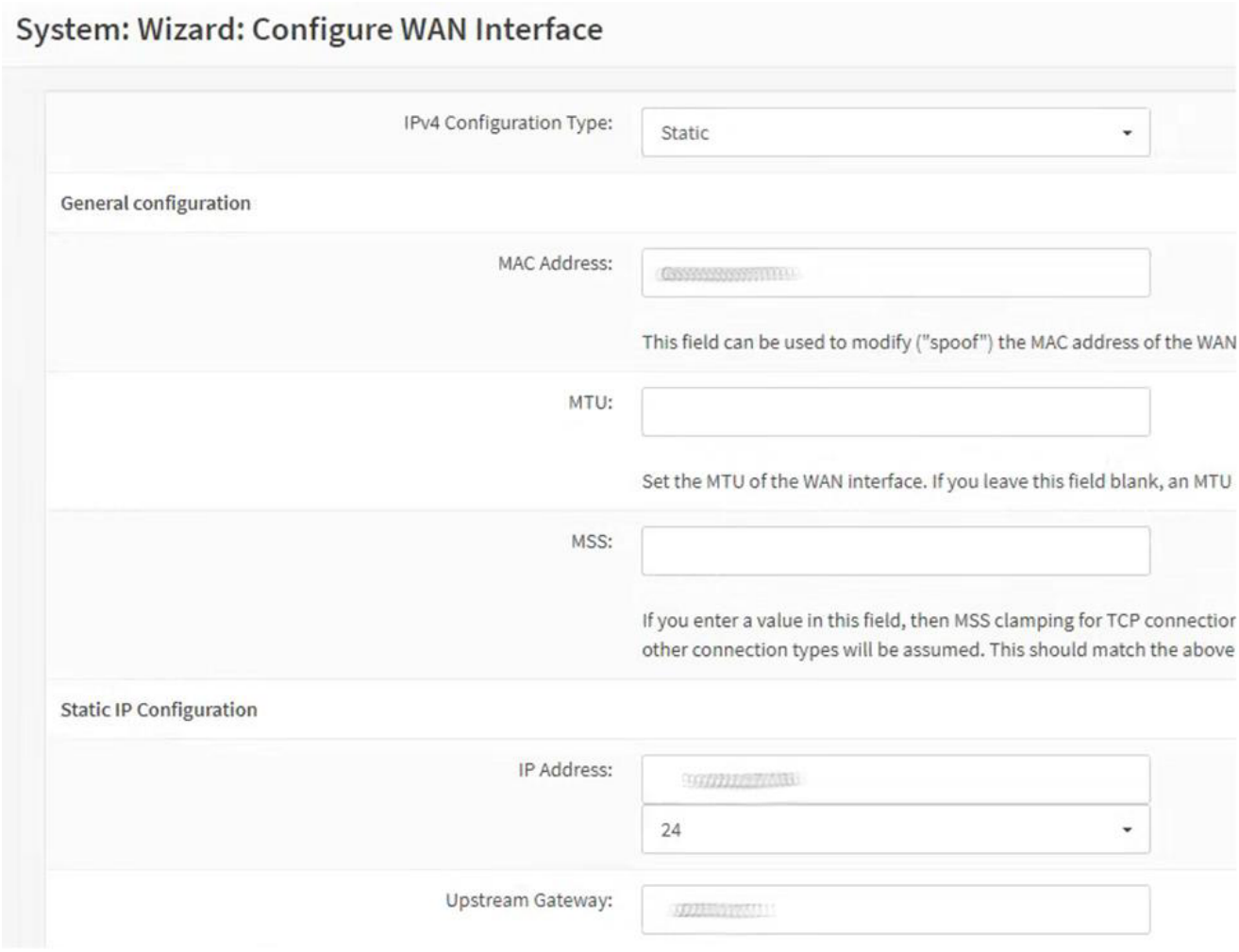


Рисунок 3.3.3 – Налаштування WAN інтерфейсу.



Рисунок 3.3.4 – Налаштування LAN інтерфейсу.

3.4 Налаштування маршрутизації

Першим етапом налаштування мережі буде створення VLAN. Для цього скористаємось веб-інтерфейсом OPNSense.

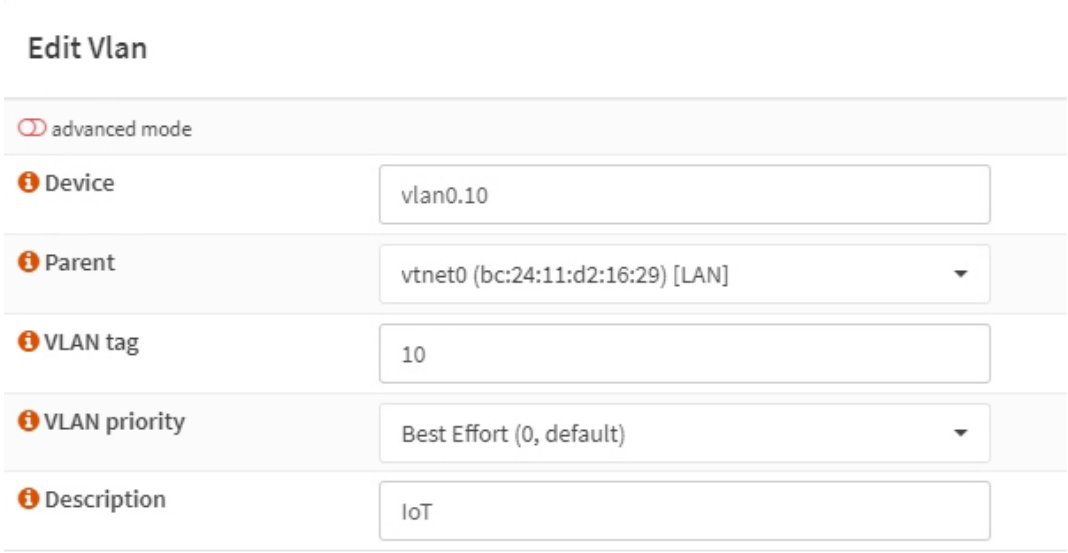


Рисунок 3.4.1 – Створення VLAN для IoT пристроїв

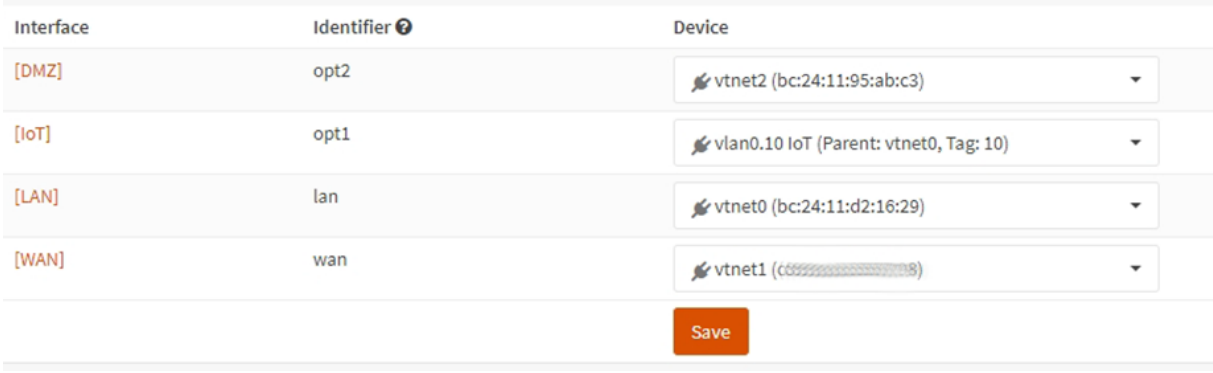


Рисунок 3.4.2 – Розподілення інтерфейсів за портами

Створивши VLAN і розподіливши їх за портами, далі потрібно задати адреси цим мережам.

Таблиця 3.4.1

Параметри адресації мереж

Мережа	Адреса	Маска
LAN	192.168.0.1	255.255.255.0
DMZ	172.16.0.1	255.255.255.0
VLAN 10	192.168.10.1	255.255.255.0

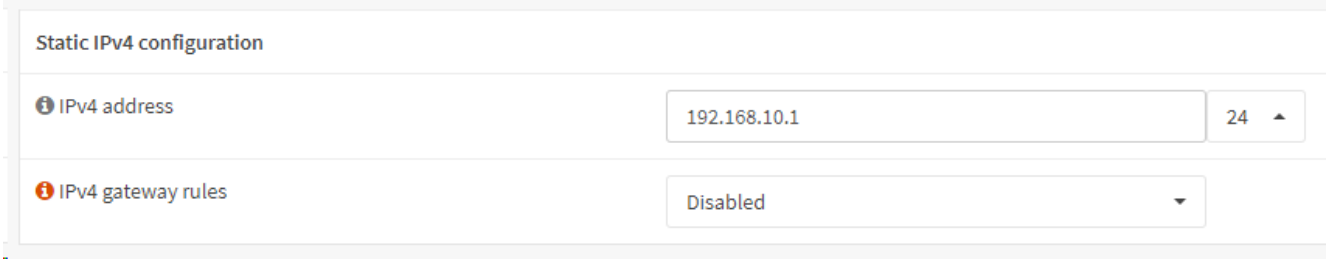


Рисунок 3.4.3 – Налаштування VLAN 10

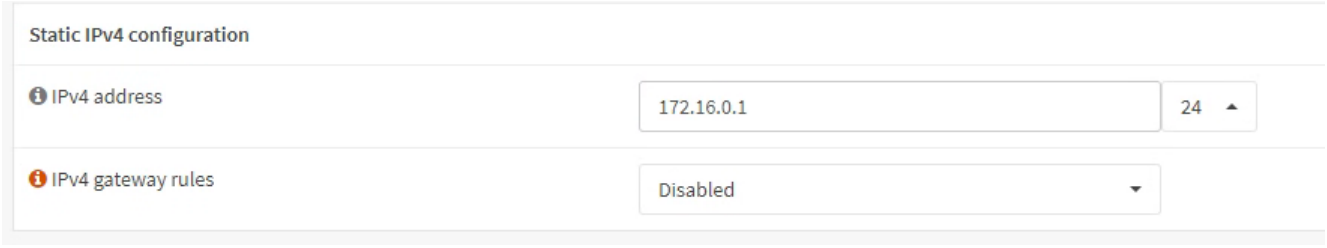


Рисунок 3.4.4 – Налаштування DMZ

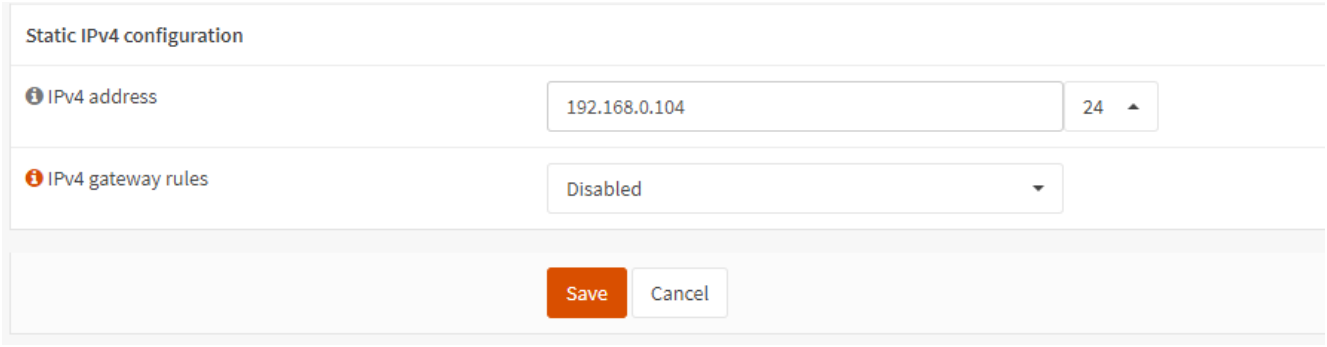


Рисунок 3.4.5 – Налаштування LAN

Налаштуємо DHCPv4 сервери для інтерфейсів (рис 3.4.5).

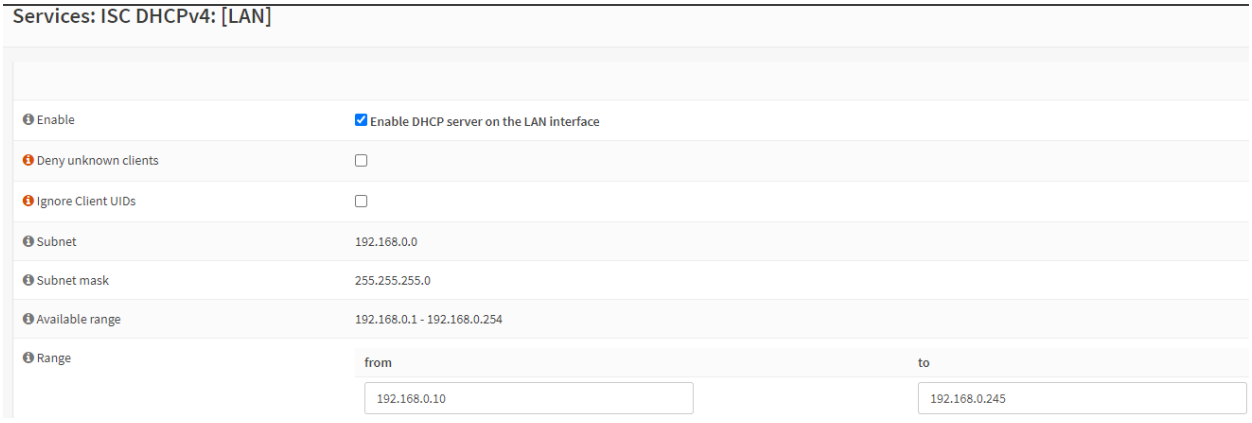


Рисунок 3.4.6 – Налаштування DHCP LAN

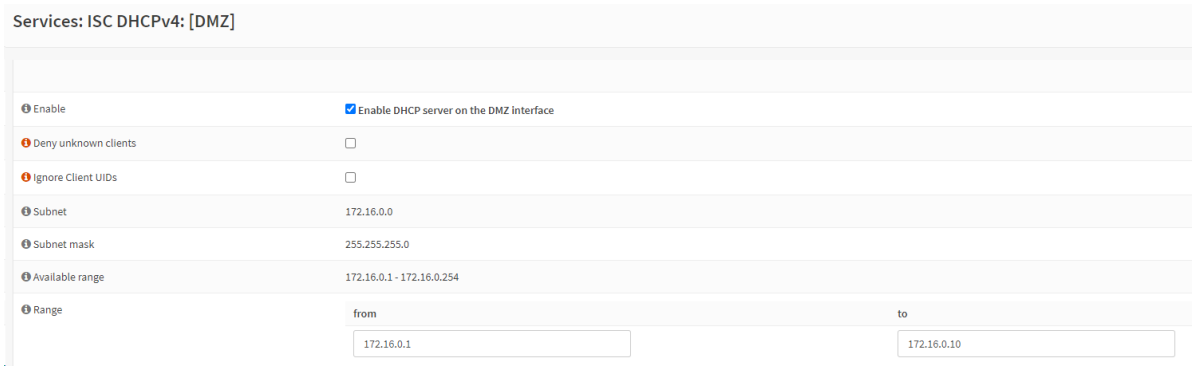


Рисунок 3.4.7 – Налаштування DHCP DMZ

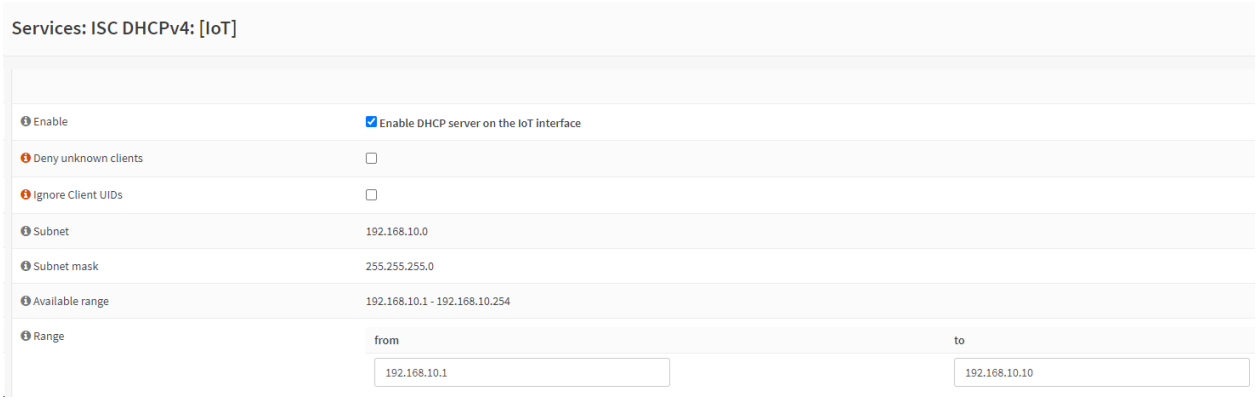


Рисунок 3.4.8 – Налаштування DHCP IoT VLAN 10

Перевіримо роботу DHCP (рис 3.4.8).

Interface	IP Address	MAC Address	Hostname
DMZ	172.16.0.2	00:e0:21:57:f2:1e *FREEGATE CORP.*	dayzsever
LAN	192.168.0.11	9a:73:d1:ce:3b:0f	
LAN	192.168.0.100	00:d8:61:55:2f:32 *Micro-Star INTL CO., LTD.*	DESKTOP-2H0JV5L
LAN	192.168.0.111	cc:2d:e0:df:64:c0 *Routerboard.com*	MikroTik
IoT	192.168.10.1		esp32-264D24
IoT	192.168.10.2	c8:2e:18:26:4d:24 *Espressif Inc.*	esp32-264D24

Рисунок 3.4.9 – Робота DHCP

Пристрої отримують адреси, означає що DHCP працює належним чином.

Останнім налаштуємо WAN, для доступу в інтернет (рис 3.4.9).

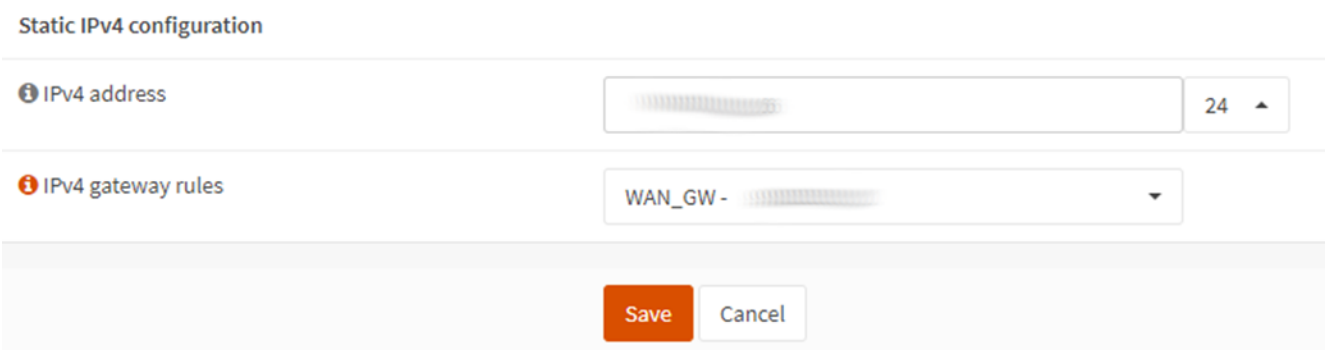


Рисунок 3.4.10 – Налаштування WAN

Перевіримо роботу на робочій станції (рис 3.4.10).

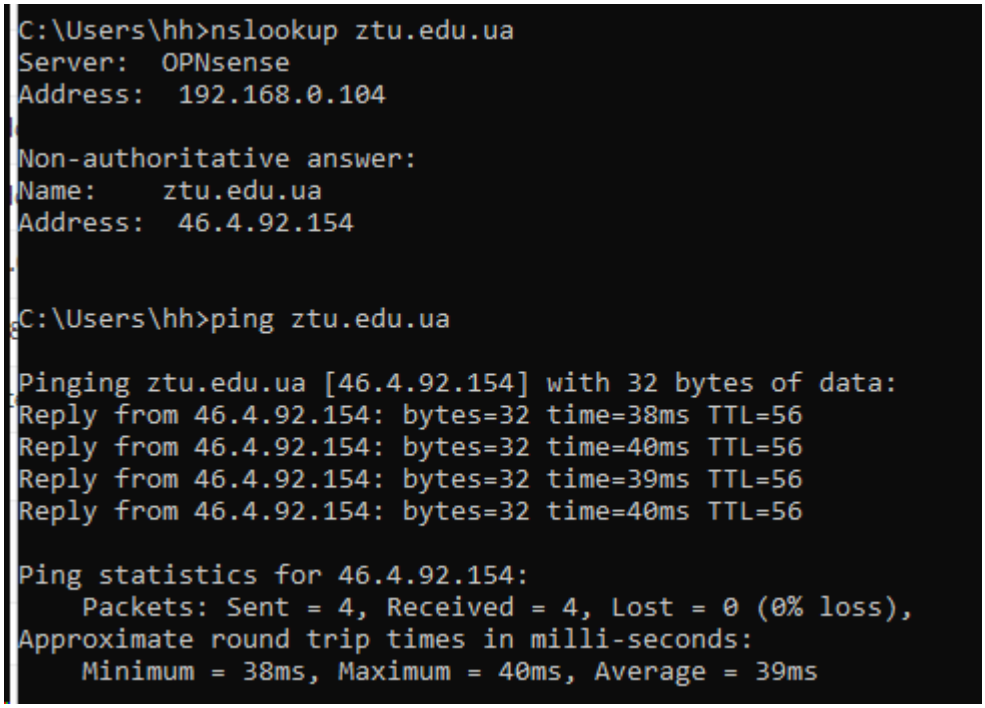


Рисунок 3.4.11 – Перевірка роботи

Комп’ютер отримав адресу через DHCP та має доступ до інтернету.

3.5 Налаштування комутатора

В якості комутатора виступає MikroTik, на основі RouterOS, який завдяки своїй гнучкості та широким можливостям, дозволяє побудувати ефективну і безпечну мережеву інфраструктуру

Після налаштувань VLAN на OPNsense, необхідно направити трафік на потрібний порт, в моєму випадку це Wi-Fi мережа

Перший крок це додавання мережі VLAN, та призначення її на необхідний інтерфейс (рис 3.5.1).

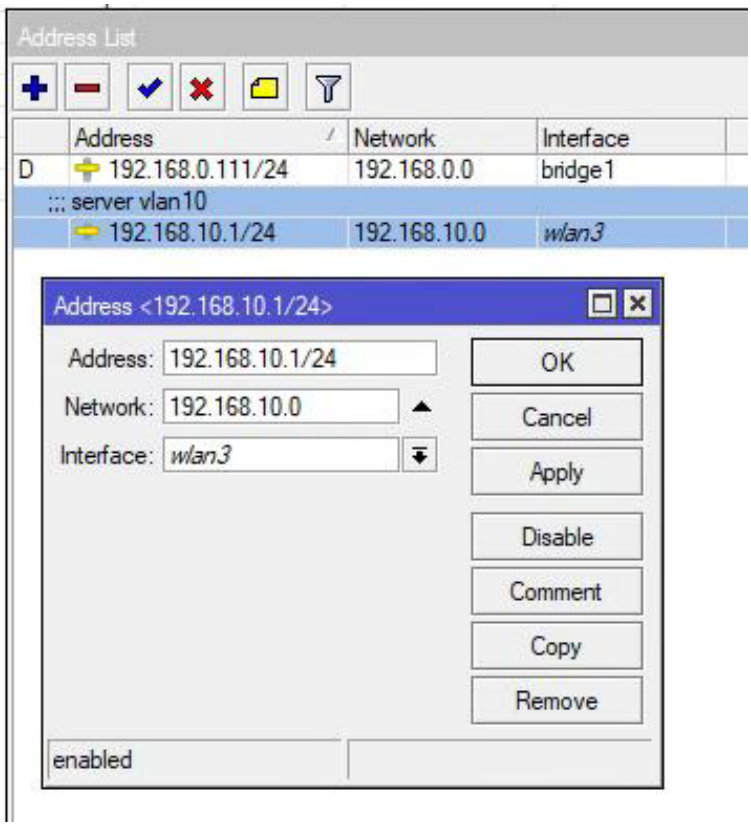


Рисунок 3.5.1 – Створення адреси VLAN

Далі потрібно налаштувати VLAN на мережевому інтерфейсі bridge1 (рис 3.5.2).

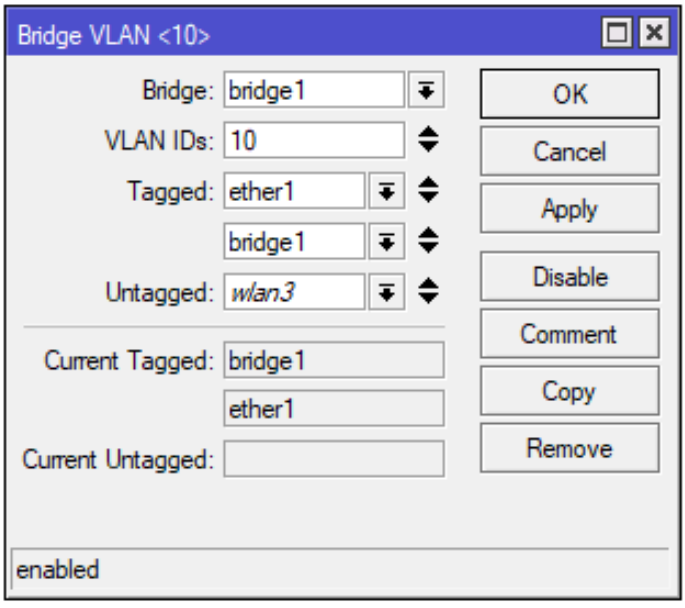


Рисунок 3.5.2 – Налаштування VLAN

І призначимо цей VLAN до інтерфейсу wlan3 (рис 3.5.3).

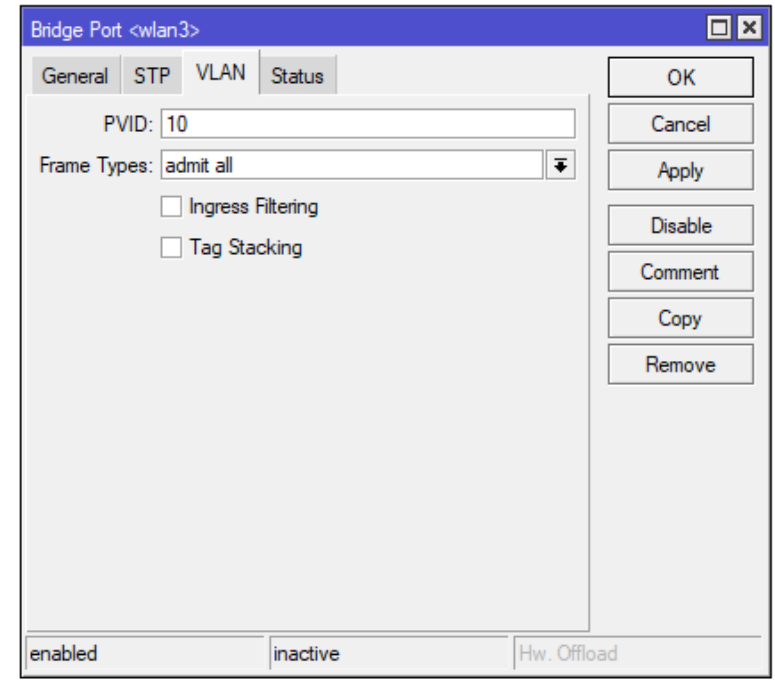


Рисунок 3.5.3 – Налаштування VLAN

Останній крок налаштування RouterOS, це створення WiFi точки доступу з відповідним VLAN ID (3.5.4).

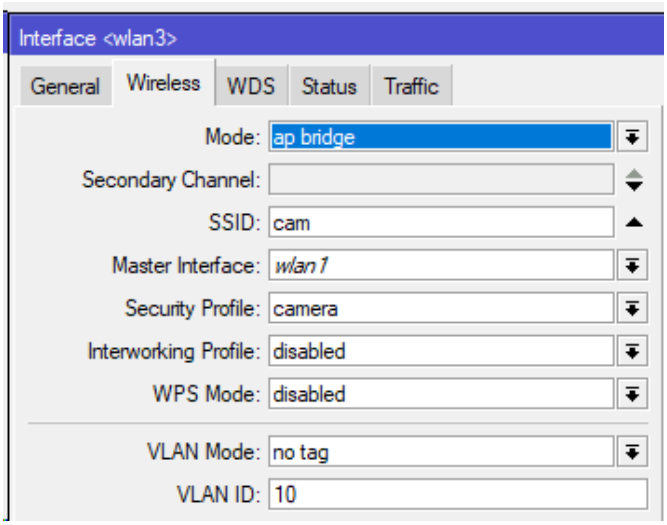


Рисунок 3.5.4 – Налаштування інтерфейсу Wlan3

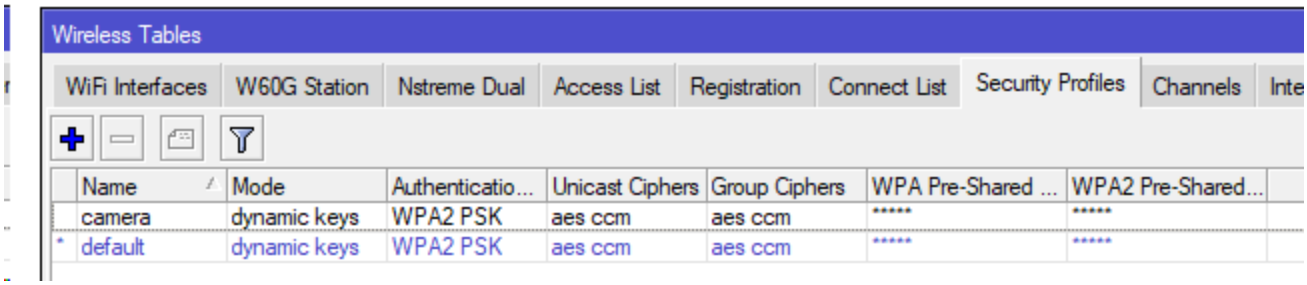


Рисунок 3.5.5 – Налаштування профілю безпеки для wlan 3

3.6 Налаштування безпеки

Першим кроком налаштування безпеки буде перевірка оновлень та встановлення актуальний пакетів для OPNSense (рис. 3.6.1).

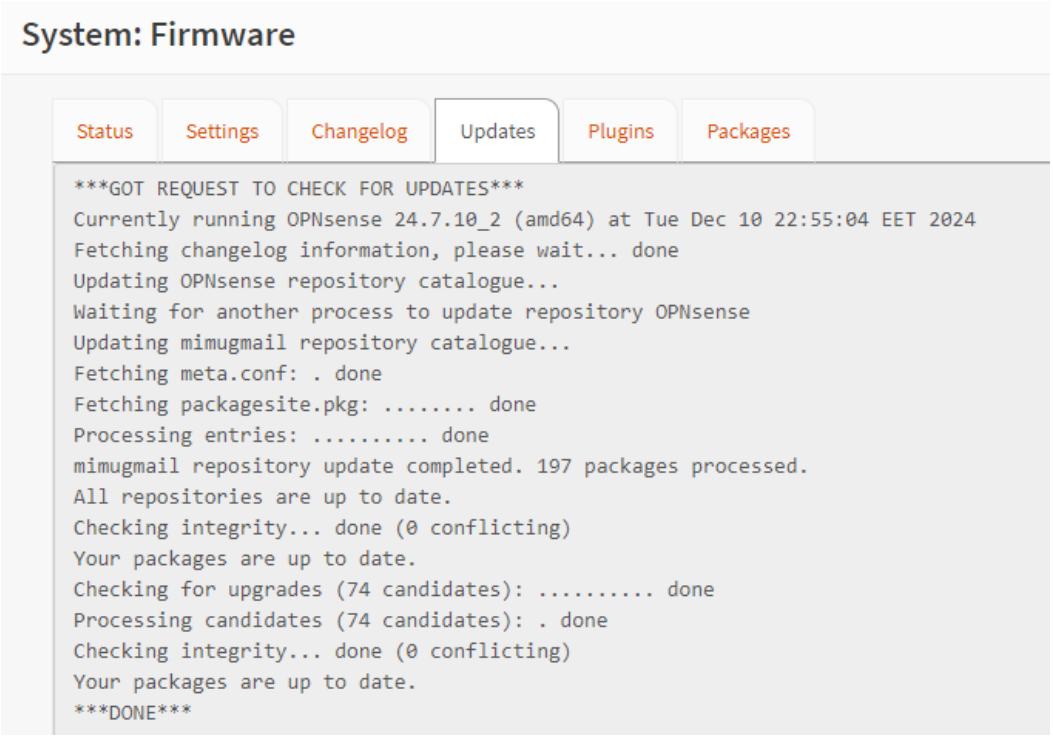


Рисунок 3.6.1 – Оновлення пакетів

Далі потрібно змінити стандартний пароль адміністратора на більш надійний (рис.3.6.2).

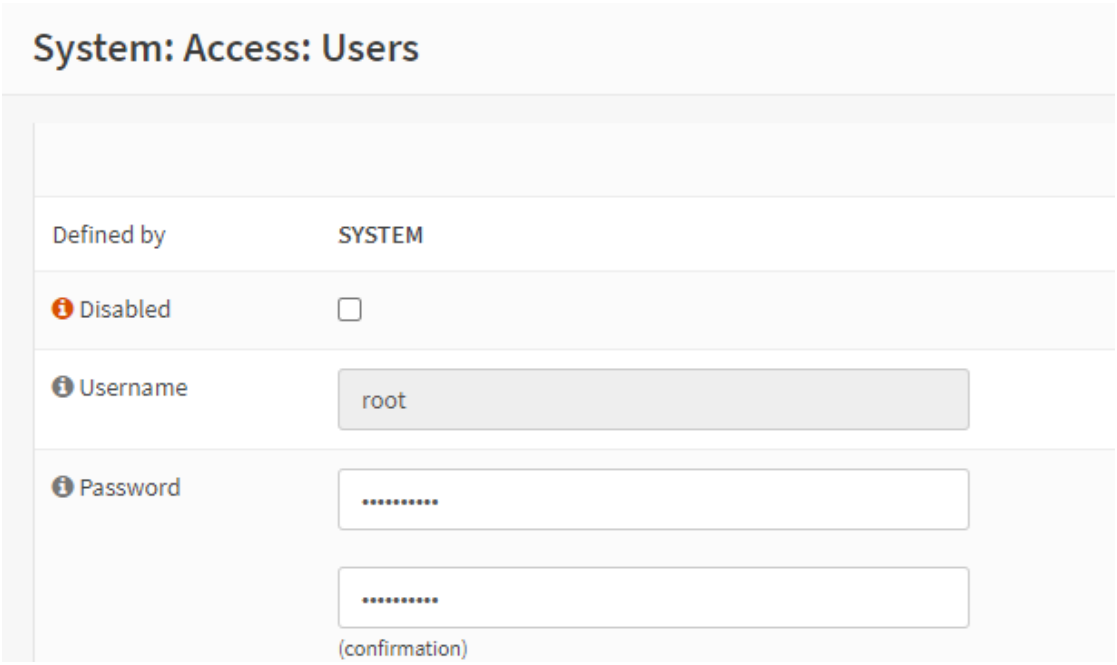


Рисунок 3.6.2 – Налаштування паролю до користувача root

Для додаткової безпеки акаунта адміністратора, потрібно увімкнути двох факторну автентифікацію використовуючи застосунок Google Authenticator. Спочатку для цього треба створити запис у параметрі Servers (рис. 3.6.3).

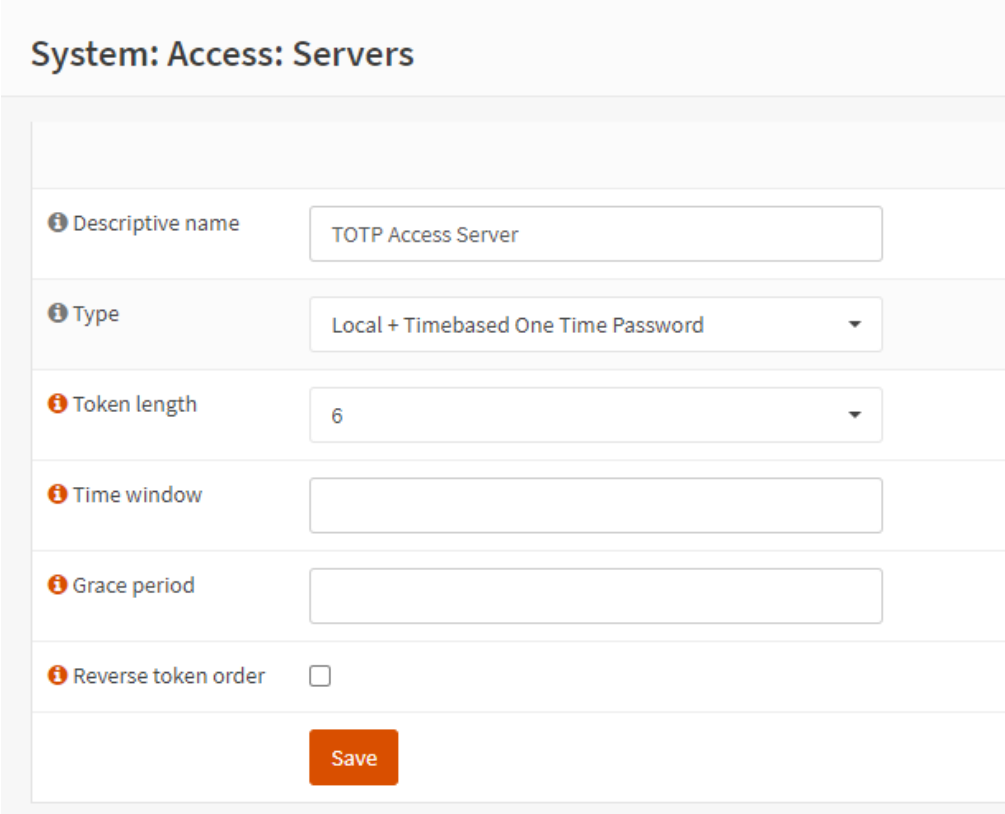


Рисунок 3.6.3 – Налаштування серверу автентифікації

Та налаштувати додаток на смартфоні (рис. 3.6.4).

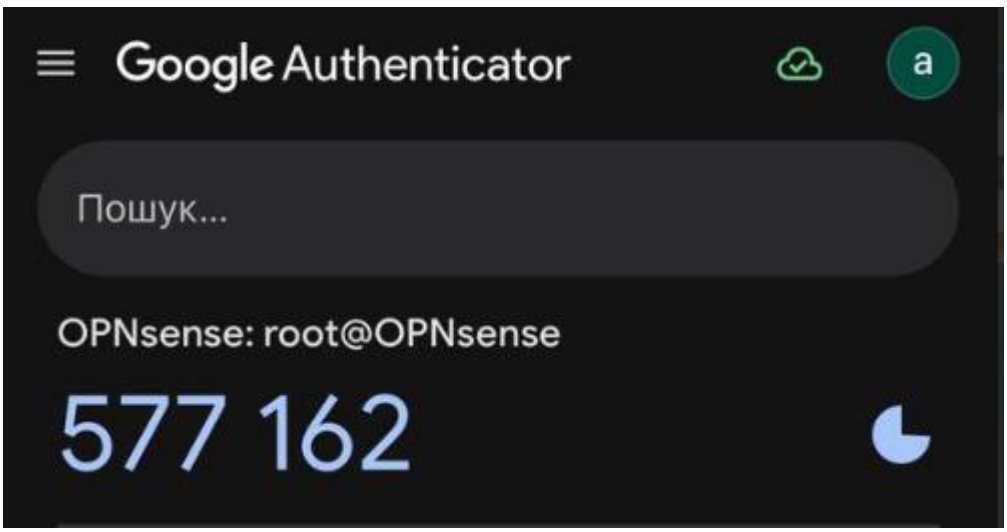


Рисунок 3.6.4 – Отримання коду доступу на смартфоні

Цей метод вимагає введення кодів з автентифікатора перед основним паролем у вікні входу.

Закриття порту SSH допомагає мінімізувати ризик атак, таких як brute force або сканування портів.

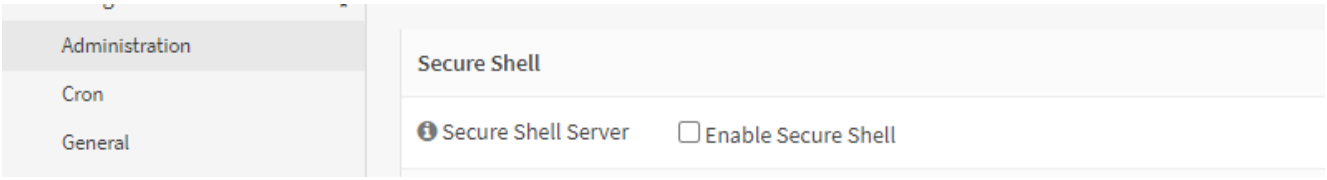


Рисунок 3.6.5 – Налаштування SSH

Увімкнення системи виявлення та запобігання вторгнень (IPS/IDS) Suricata в OPNsense додає додатковий рівень захисту мережі (рис 3.6.6). Suricata дозволяє виявляти та блокувати загрози в реальному часі за допомогою методів, таких як визначення за сигнатурами, аналіз аномалій та репутаційний підхід. Це знижує ризик витоків даних та підвищує безпеку системи (рис 3.6.7).

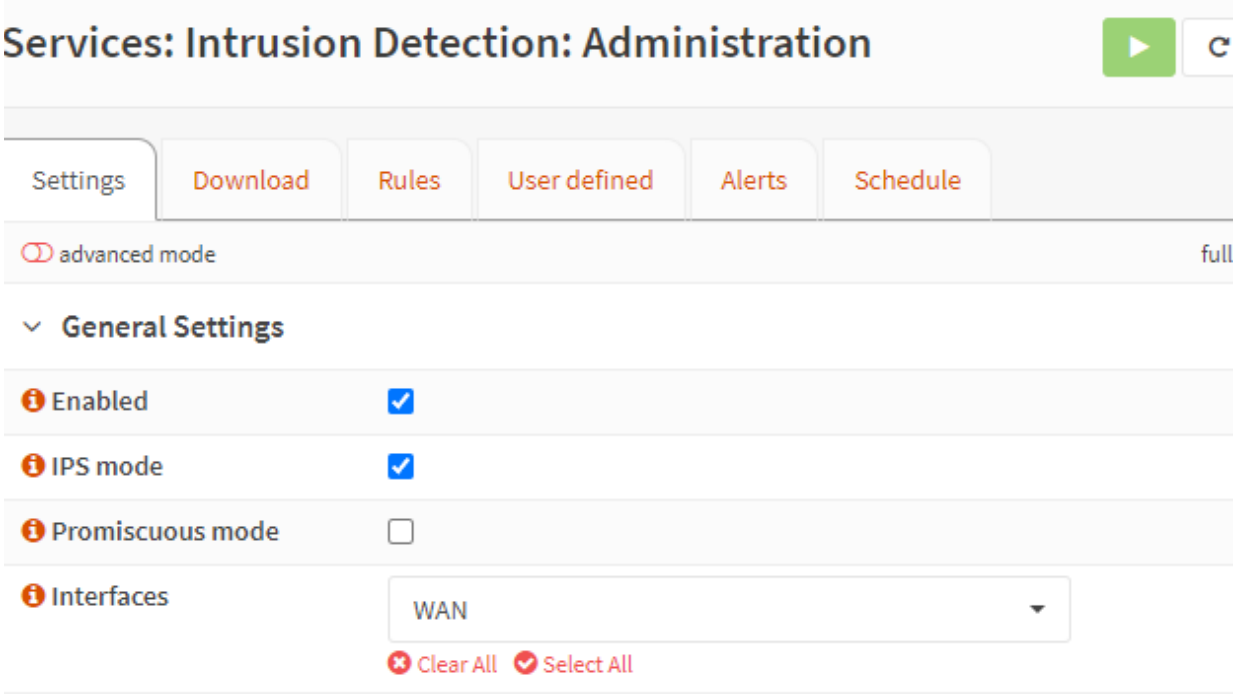


Рисунок 3.6.6 – Налаштування Suricata на інтерфейсі WAN

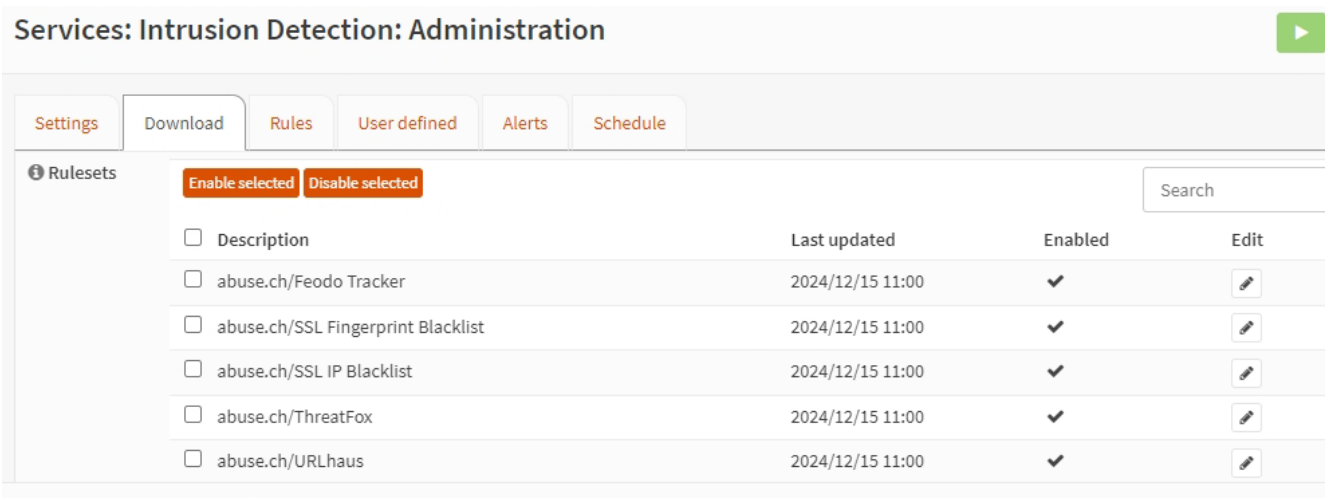


Рисунок 3.6.7 – Застосування правил безпеки

3.7 Налаштуваня безпеки DNS

Для забезпечення безпеки DNS, скористаюсь вбудованим резолвером UnboundDNS (рис 3.7.1). Він підтримує функції кешування, блокування реклами, захисту від підробки DNS-запитів (DNSSEC) і дозволяє конфігурувати локальні записи DNS.

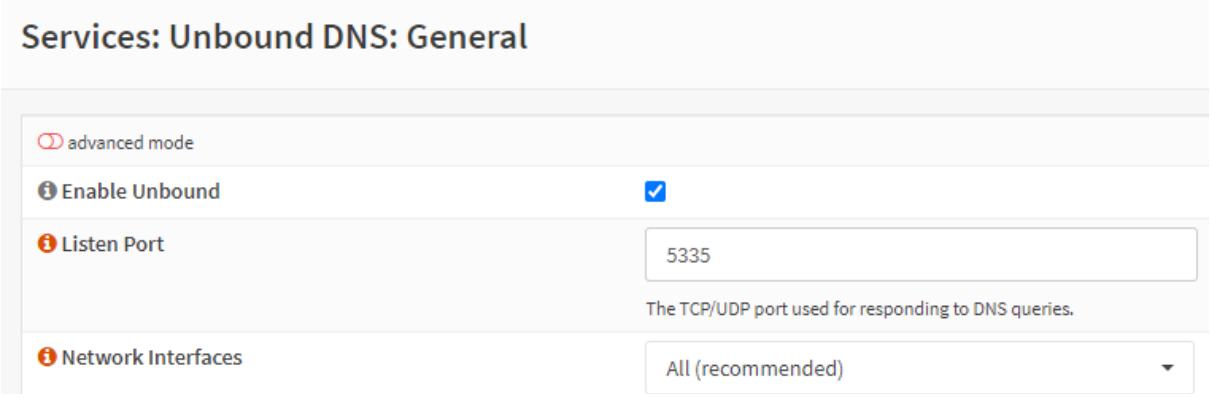


Рисунок 3.7.1 – Налаштування Unbound DNS на порт 5353

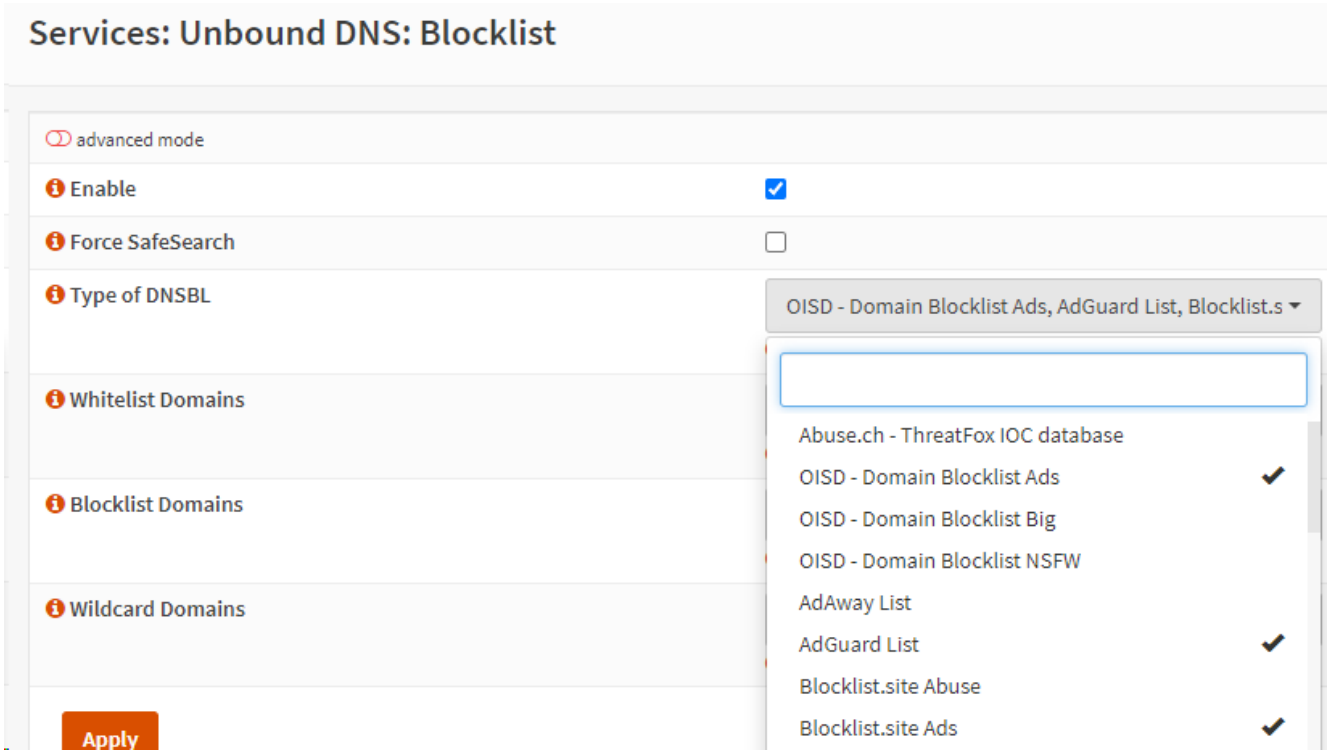


Рисунок 3.7.2 – Налаштування блоклистів Unbound DNS

Та додатково налаштуємо Adguard плагін для порту 53 (рис. 3.7.3).

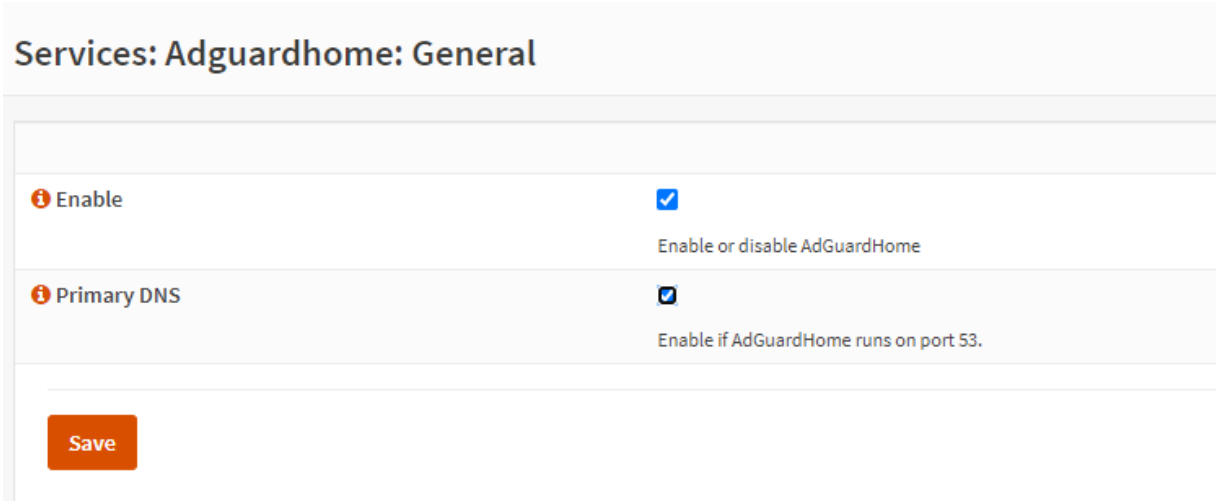


Рисунок 3.7.3 – Налаштування Adguard DNS на порт 53

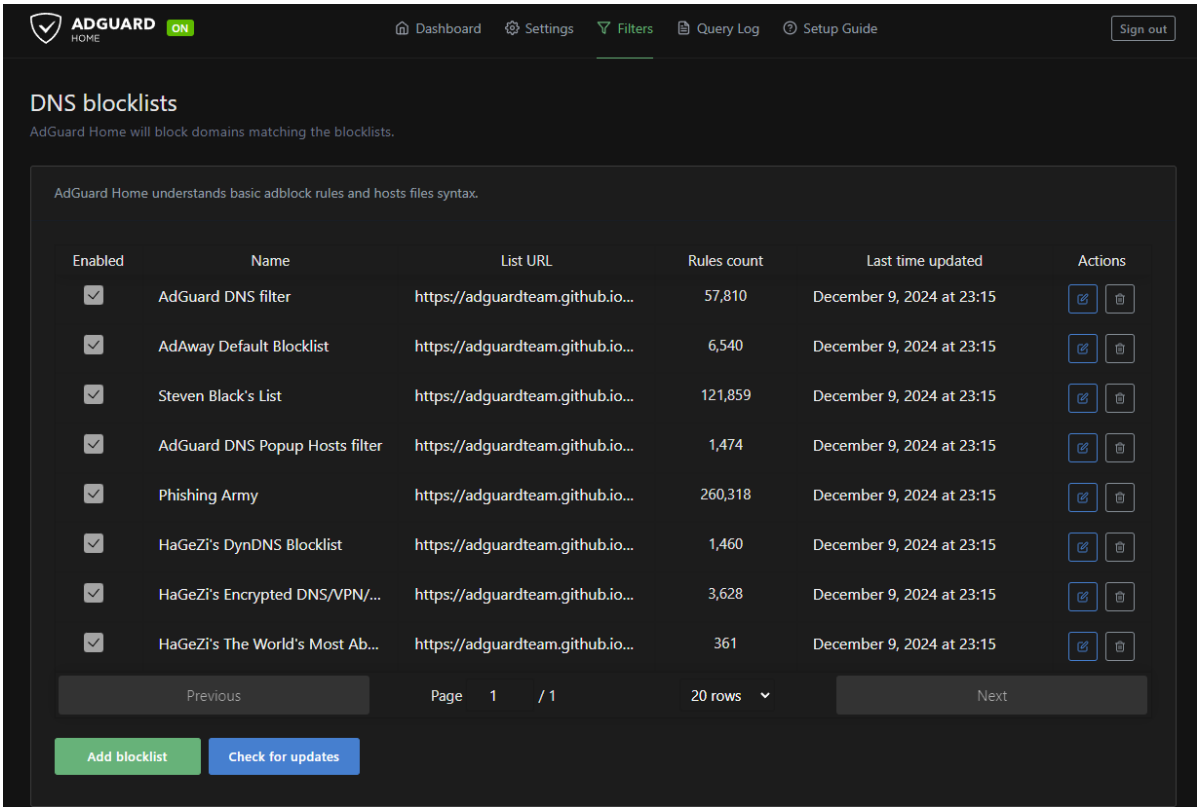


Рисунок 3.7.4 – Налаштування блоклистів Adguard DNS

3.8 Створення та налаштування правил фаєрволу

Використання геоблокування є важливим заходом безпеки, який дозволяє обмежити доступ до серверу і мережі на основі географічного розташування користувачів. Це буде корисно для запобігання несанкціонованому доступу з країн, з яких не бажаний трафік (рис 3.8.1).

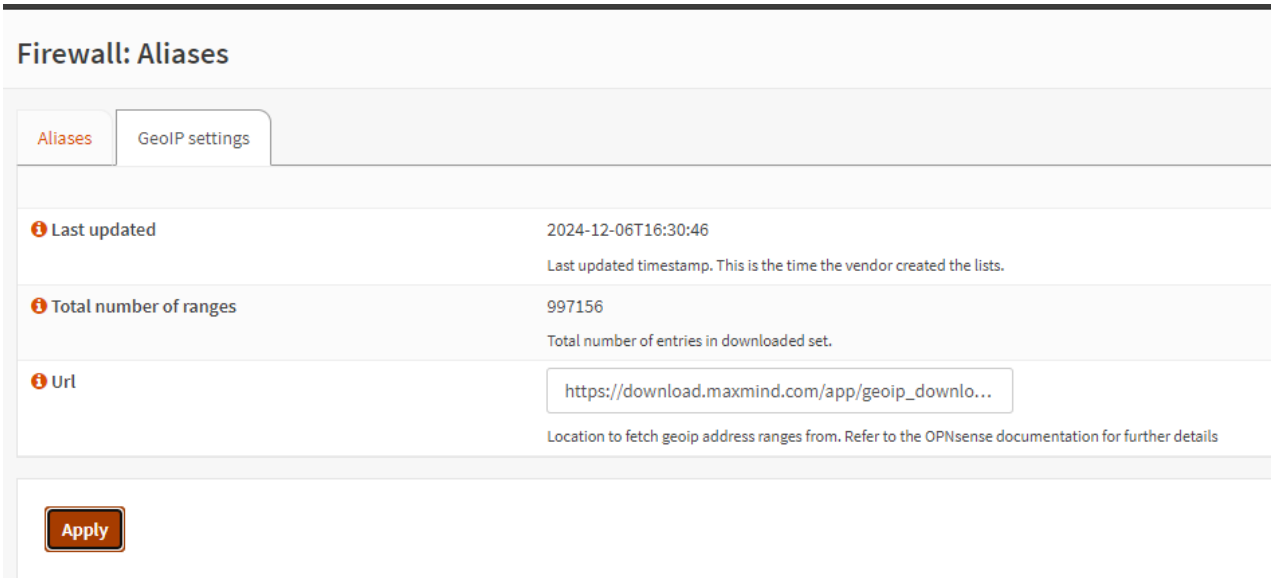


Рисунок 3.8.1 – Створення псевдоніму та налаштування списку геоблокування

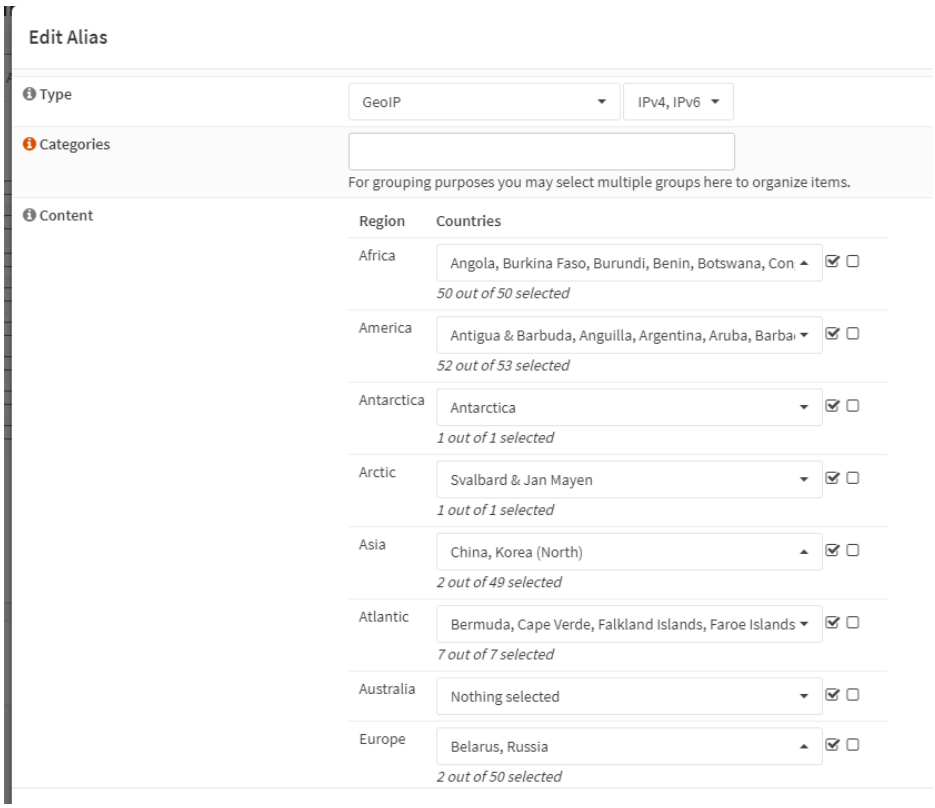


Рисунок 3.8.2 – Вибір країн, трафік з яких буде заблоковано

IP-блок листи це інструмент для підвищення безпеки мережі, який блокує доступ до небажаних або потенційно шкідливих IP-адрес (рис. 3.8.3).

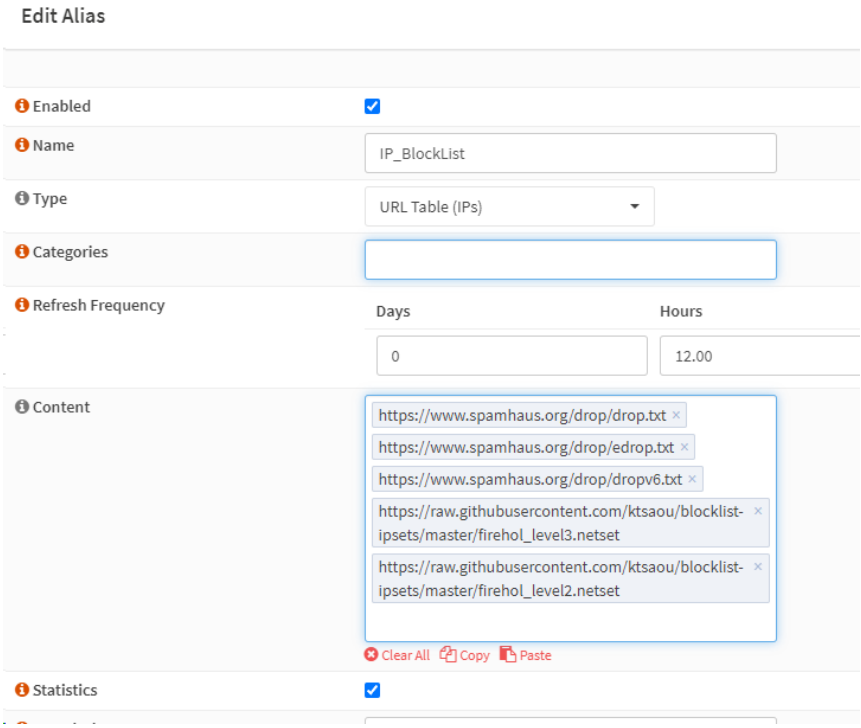


Рисунок 3.8.3 – Створення псевдоніму та налаштування списку IP блокування

Далі налаштуємо базові правила для DMZ зони, які забороняють доступ до локальної мережі, але дозволяють доступ в інтернет (рис 3.8.4).

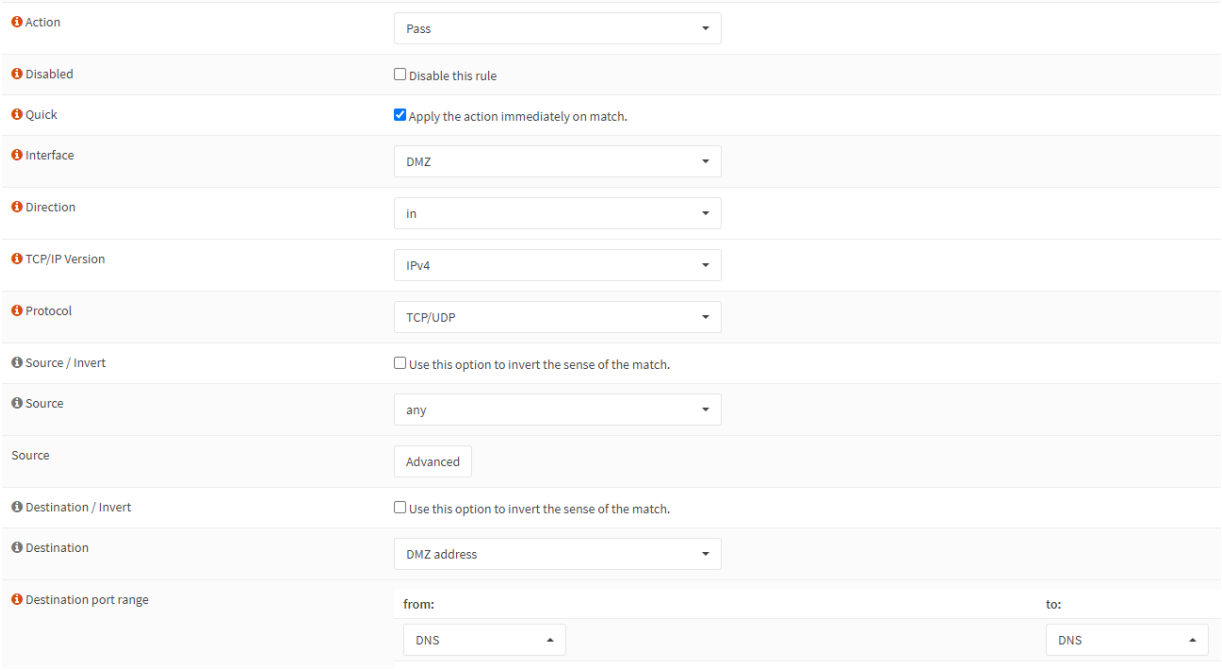


Рисунок 3.8.4 – Правило дозволу DNS.

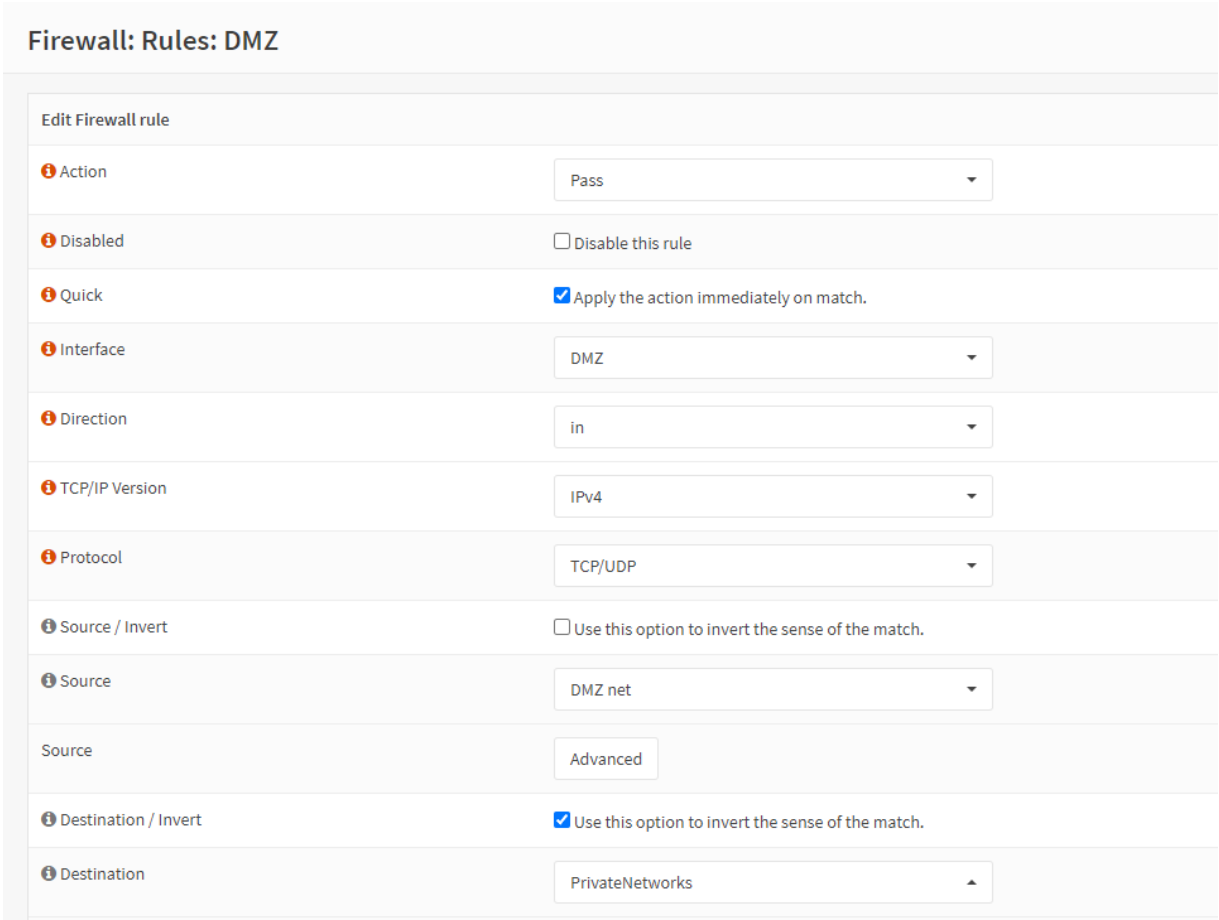


Рисунок 3.8.5 – Правило блокування доступу до локальних мереж.

Для роботи Windows Server, на якому розміщений сервер онлайн відеогри, потрібно відкрити потрібні порти використовуючи NAT Port Forwarding (рис 3.8.6).

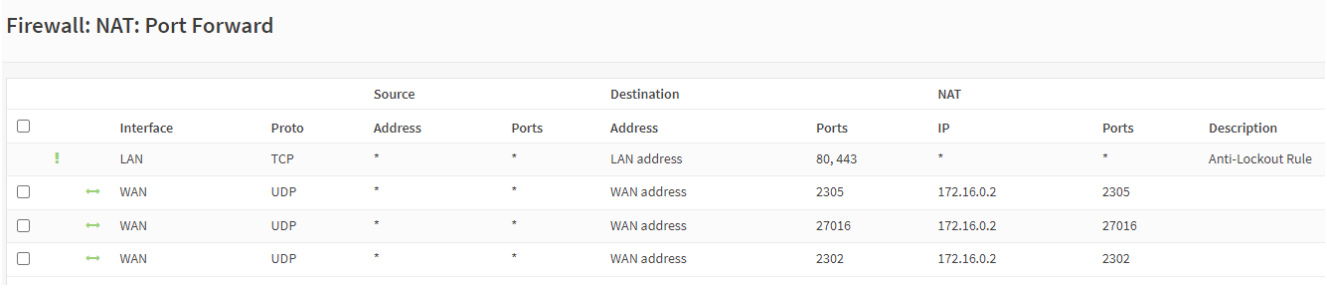


Рисунок 3.8.6 – Список правил NAT

При створенні правил NAT Port Forwarding, вони автоматично застосовуються на WAN інтерфейс (рис 3.8.7).

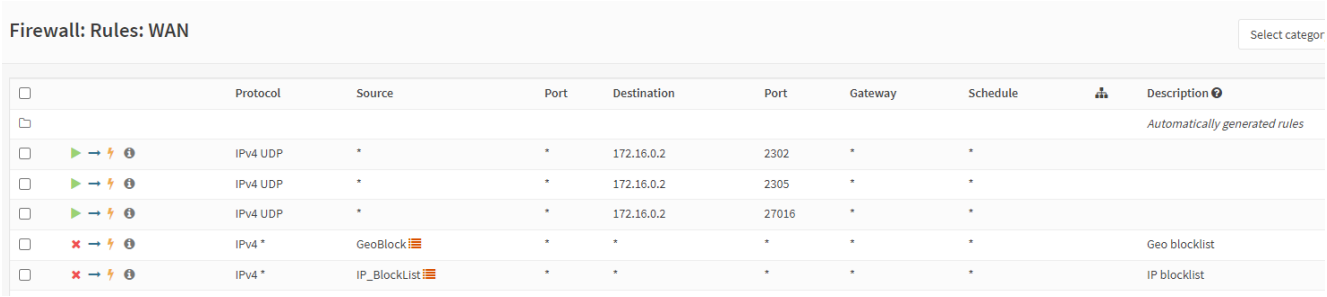


Рис 3.8.7 – Список правил WAN інтерфейсу

Для мережі LAN застосовані правила доступу до DNS (рис.3.8.8), для коректного функціонування інтернет запитів, для сервісу Adguard, доступ до потрібного порту (рис 3.8.9), Що б мати змогу підключитись до серверу в DMZ, необхідно відкрити порт, по якому працює MS RDP (рис 3.8.10), та доступ до веб інтерфейсу IP камери, через порт HTTP (рис 3.8.11).

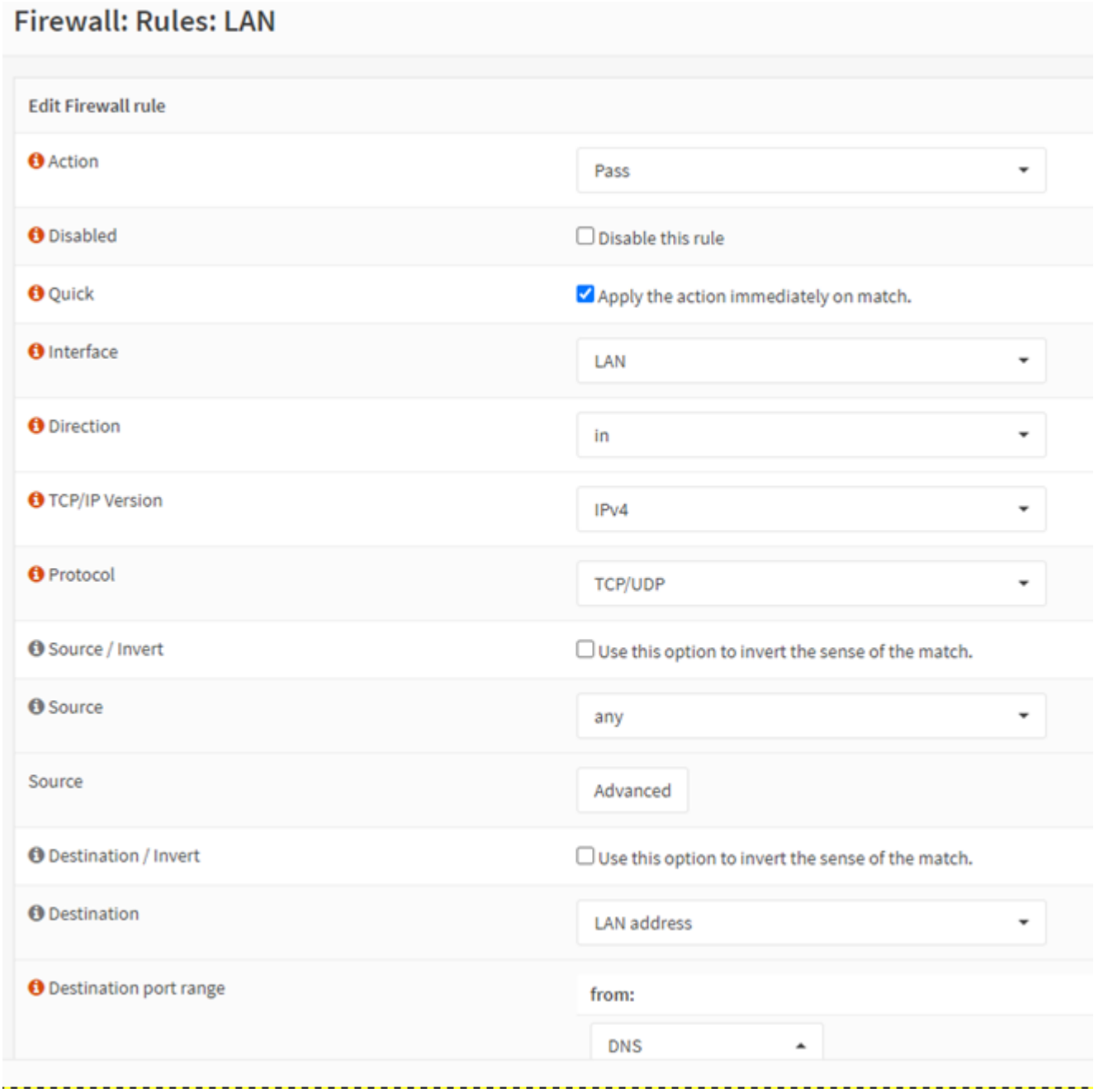


Рисунок 3.8.8 – Доступ до DNS

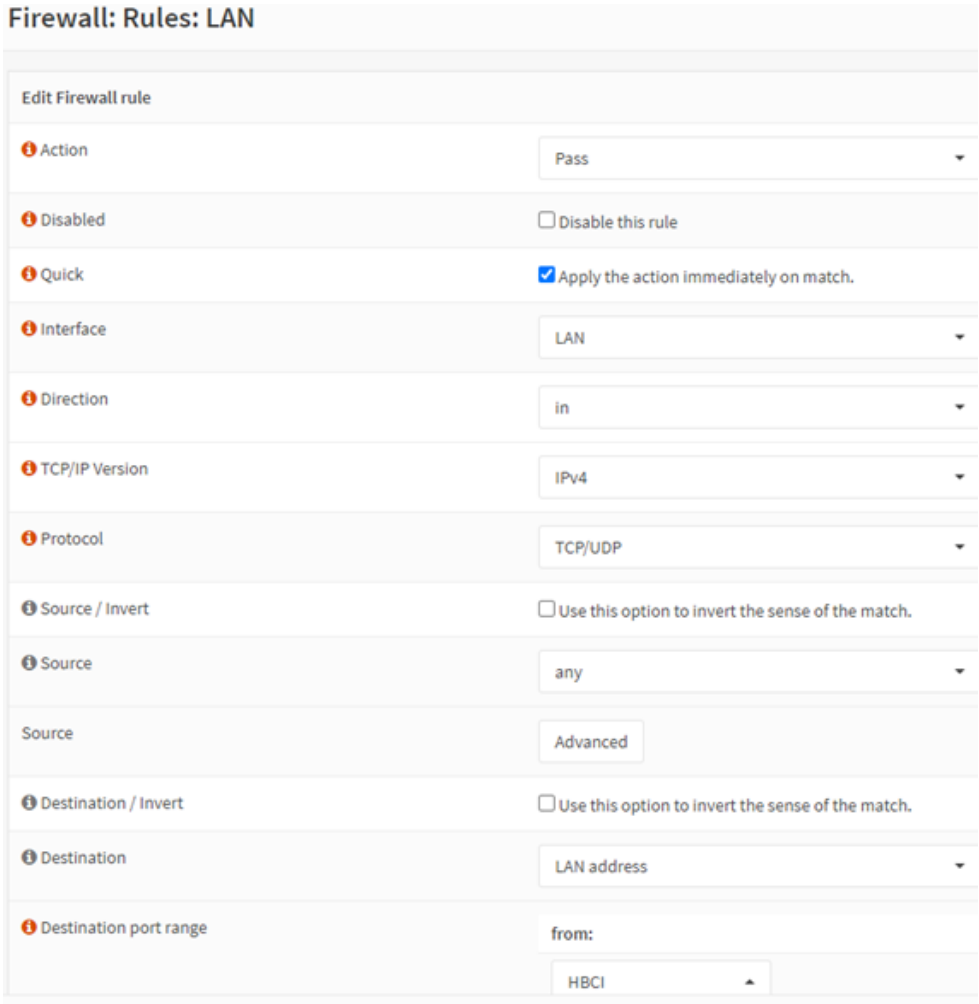


Рисунок 3.8.9 – Доступ до порту 3000, для роботи adguard home

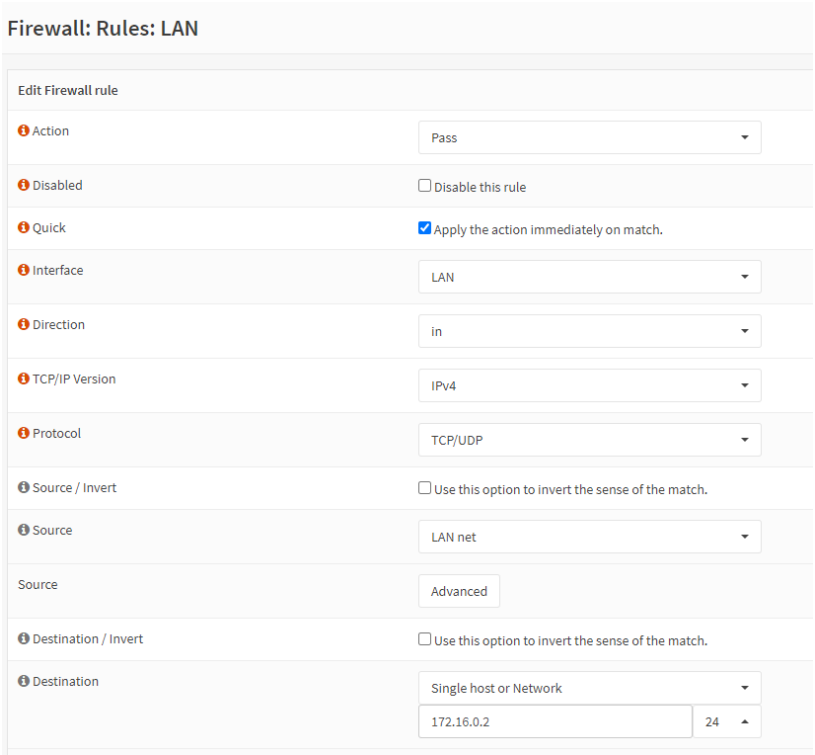


Рисунок 3.8.10 – Доступ до серверу використовуючи RDP.

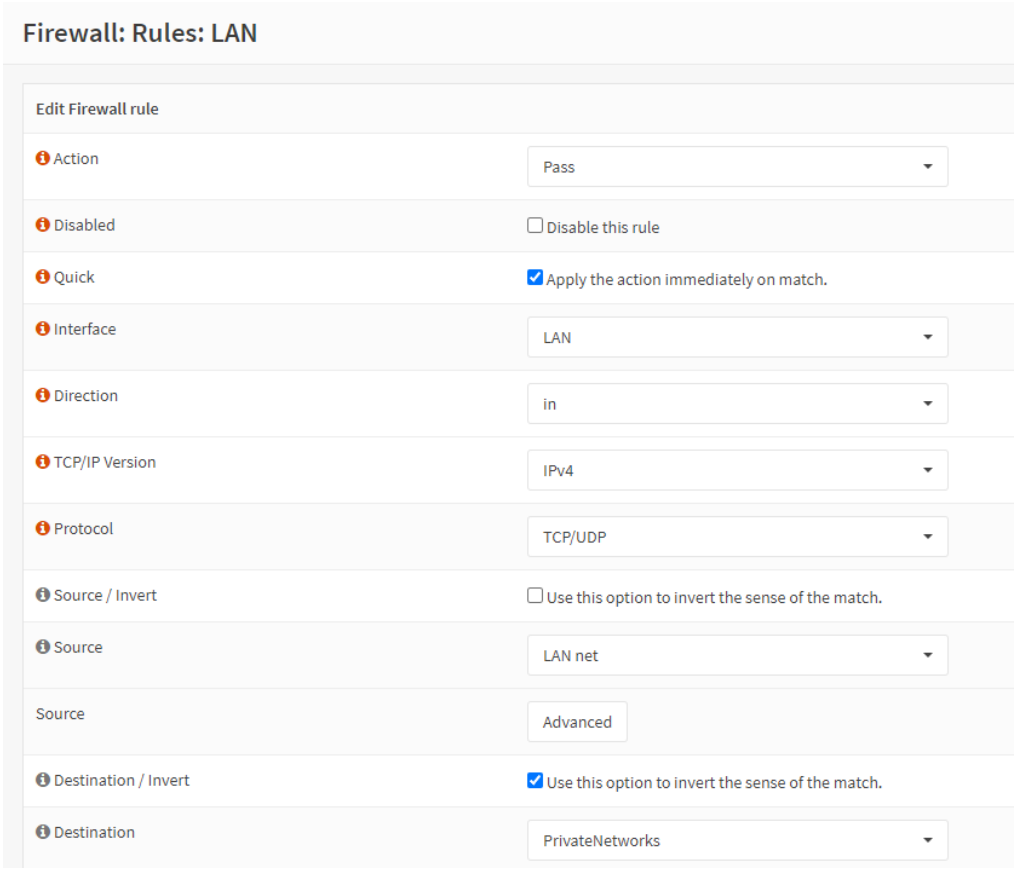


Рисунок 3.8.11 – Блокування доступу до локальних мереж.

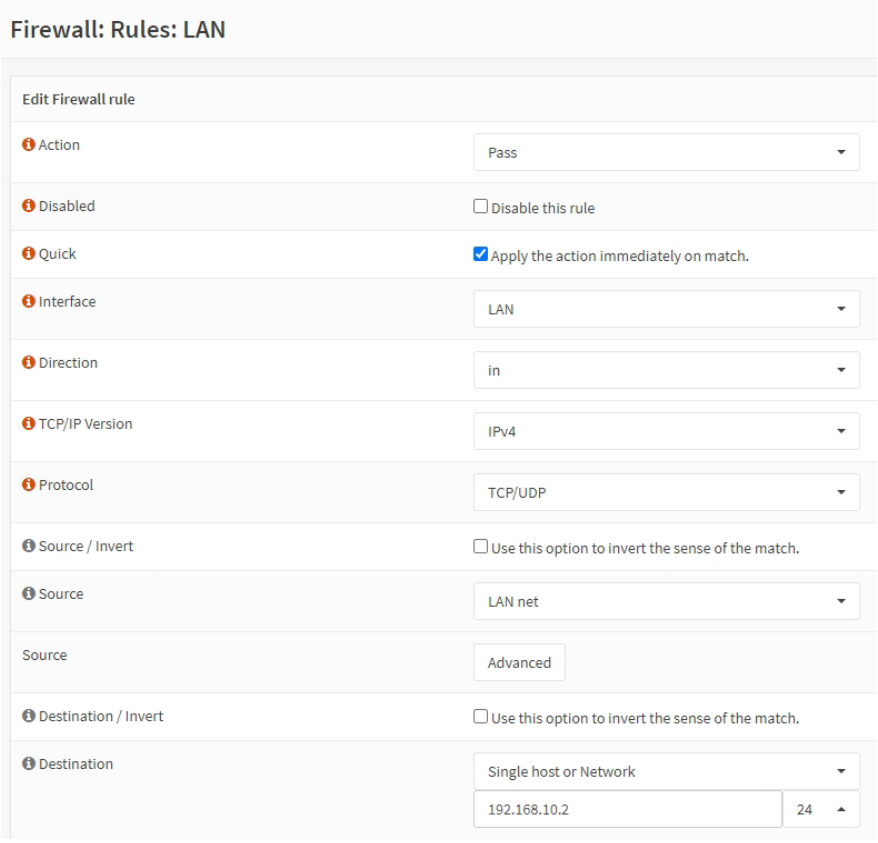


Рисунок 3.8.12 – Доступ до IP камери в мережі VLAN 10.

Мережі VLAN 10, яка використовується для IoT пристроїв, інтернет не потрібен, тому налаштуємо тільки правило яке забороняє доступ до локальних мереж.

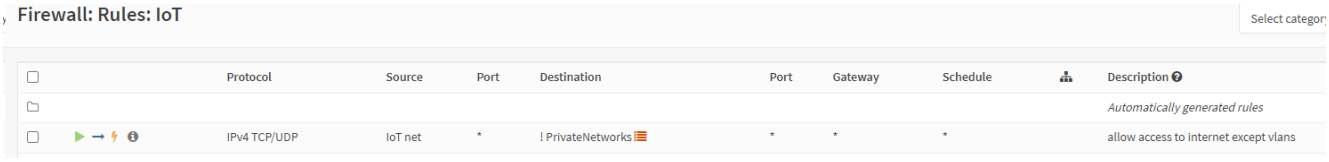


Рисунок 3.8.13. – Блокування доступу до локальних мереж.

Висновки до розділу 3

Третій розділ присвячено детальному опису методології проектування та впровадження сегментованої мережі та спроектована її логічна та фізична структура з урахуванням вимог масштабованості, продуктивності та безпеки. Фізична інфраструктура створена на основі сучасних відкритих рішень: розгорнутого та налаштованого Proxmox як платформи для віртуалізації, що забезпечує ефективне використання серверних ресурсів. Налаштування включали створення віртуальних машин для основних мережевих компонентів.

OPNsense налаштовано як основний маршрутизатор і між мережевий екран а також реалізовано базові функції маршрутизації, VPN і механізми контролю доступу. Забезпечено логічну сегментацію мережі через використання VLAN та виконано маршрутизацію між сегментами з використанням OPNsense та комутатора, що підтримує VLAN. Реалізовано багаторівневий підхід до захисту мережі. Встановлено та налаштовано IPS/IDS для виявлення та запобігання загрозам, створено правила фаєрволу та впроваджено механізми геоблокування.

Налаштовано безпечну роботу DNS, включаючи використання захищених серверів для запобігання DNS-спуфінгу та інших атак.

Забезпечено узгоджену роботу всіх компонентів мережі, що гарантує стабільність, високу продуктивність та відповідність вимогам безпеки.

Таким чином, виконано практичну реалізацію сегментованої мережевої інфраструктури з використанням відкритих рішень, що демонструє можливість створення захищеної та функціональної мережі із дотриманням сучасних стандартів.

РОЗДІЛ 4. ТЕСТУВАННЯ СЕРВІСІВ ТА ПЕРЕВІРКА БЕЗПЕКИ

4.1 Перевірка роботи

Для початку перевіримо швидкість інтернет з’єднання (рис. 4.1.1).

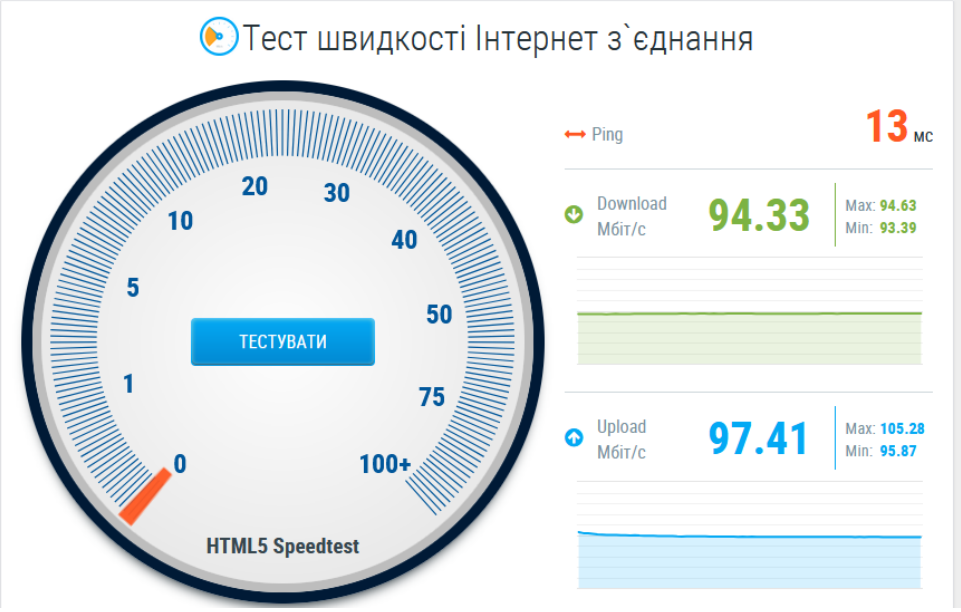


Рисунок 4.1.1 – Перевірка швидкості інтернет з’єднання

Швидкість інтернету на максимально заявленому провайдером рівні.

Далі перевіримо доступність пристроїв в мережі.

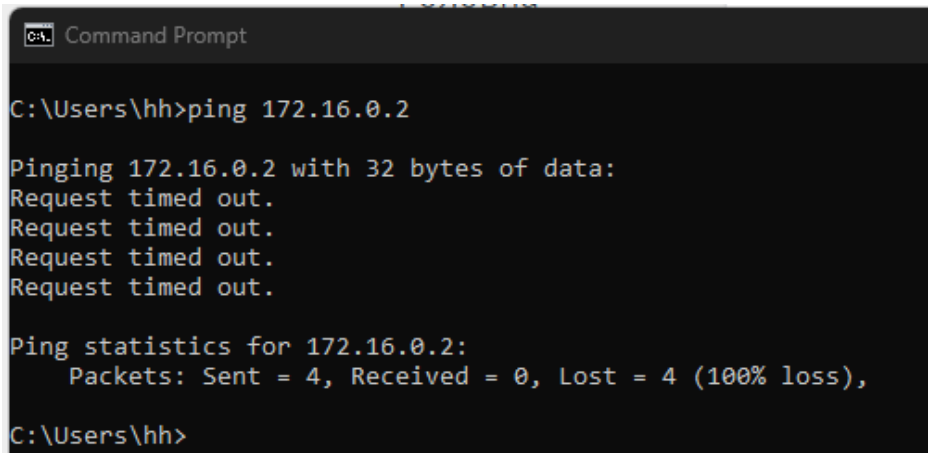


Рисунок 4.1.2 – Ping до серверу в DMZ зоні.

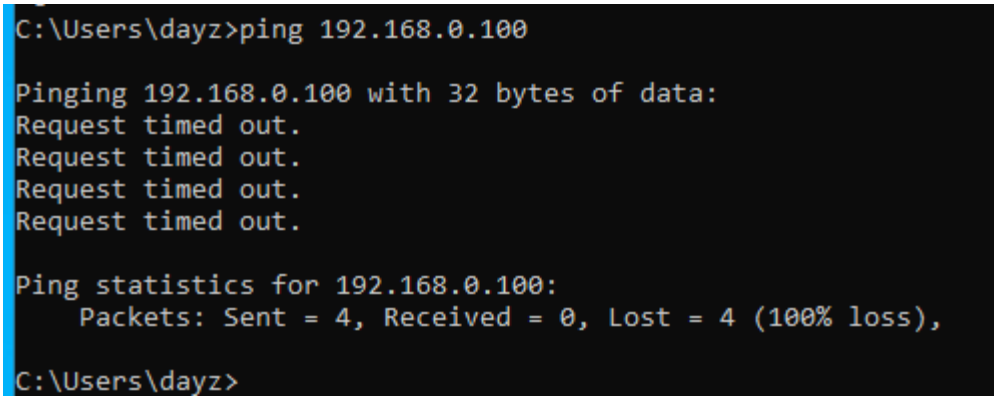


Рисунок 4.1.3. – Ping з серверу в DMZ зоні до мережі LAN.

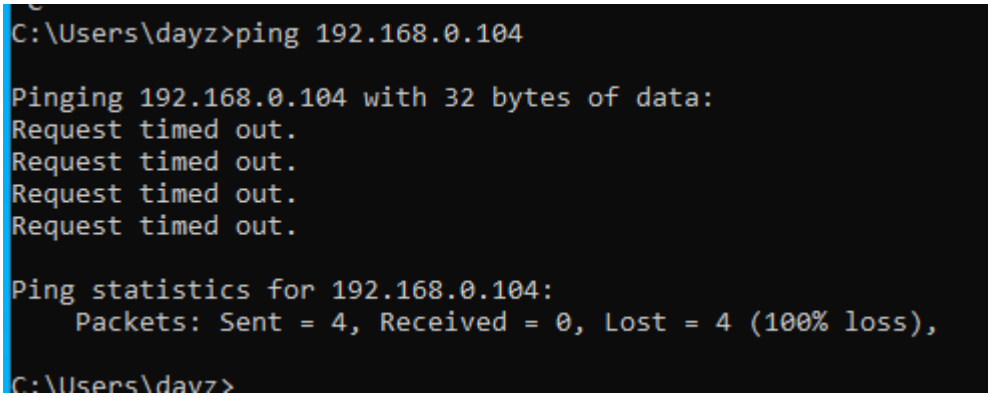


Рисунок 4.1.4 – Ping з серверу в DMZ зоні до OPNsense.

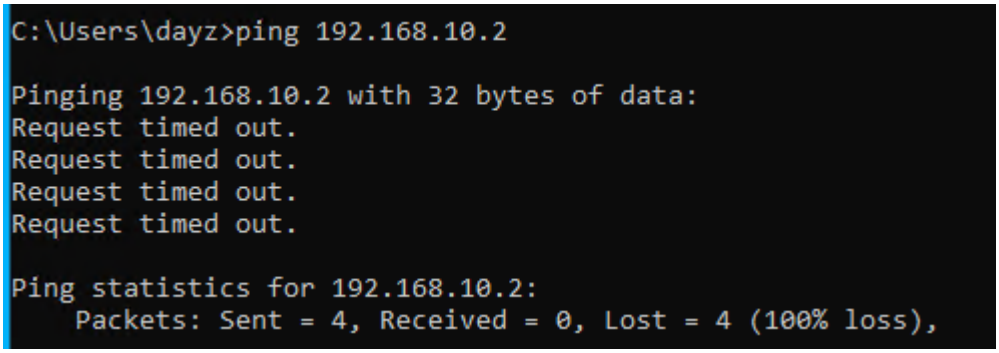


Рисунок 4.1.5 – Ping з серверу в DMZ зоні до VLAN.

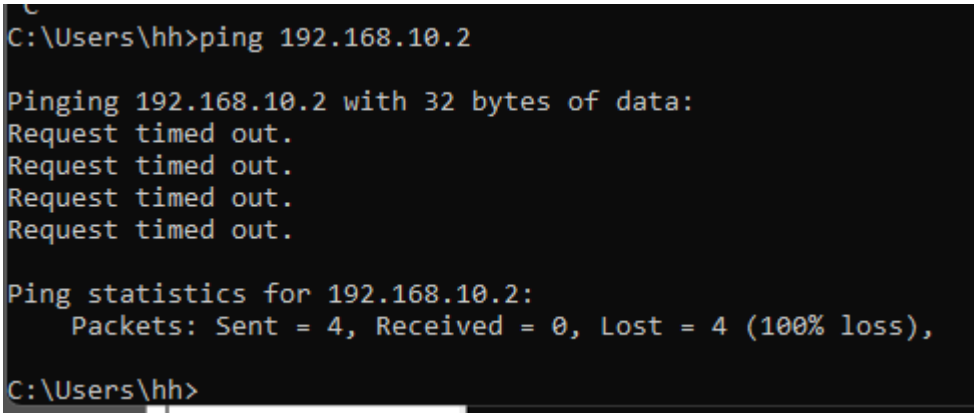


Рисунок 4.1.6 – Ping з хосту до IP камери у Vlan.

Хоч і засобом ping, до IP камери у мережі VLAN з’єднання не отримати, налаштоване правило фаєрволлу яке дозволяє доступ з хосту до камери портом 80, з’єднання і зображення ми отримати можемо (рис. 4.1.7).

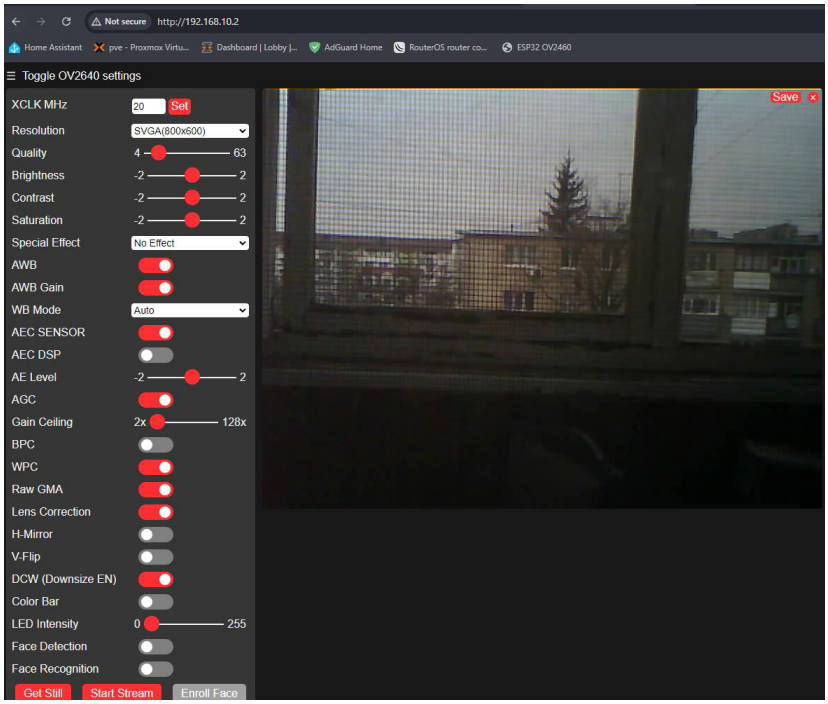


Рисунок 4.1.7 – Web інтерфейс IP камери

Налаштовані правила забезпечують ізольованість серверу від пристроїв мережі, доступ до нього тільки через технологію RDP з визначеного хоста (рис 4.1.8).

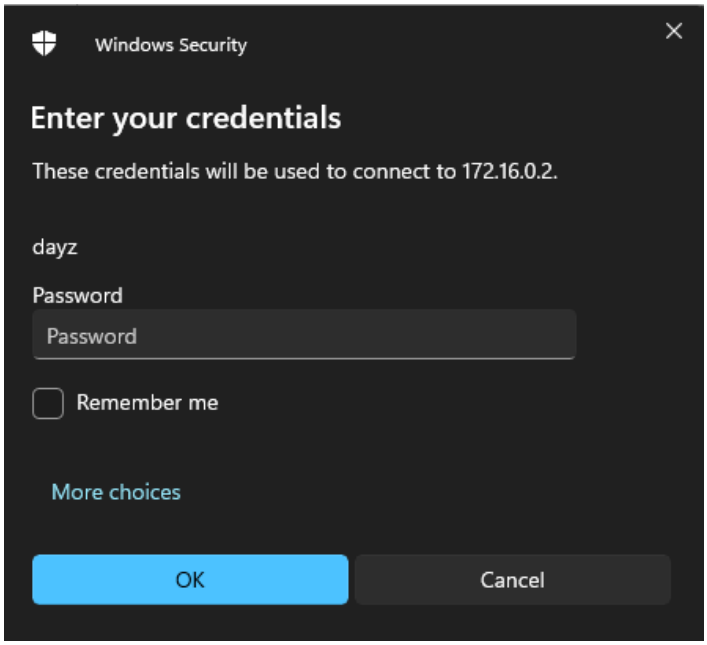


Рисунок 4.1.8 – Доступ до серверу через RDP

В DMZ зоні, розміщується Windows Server, на якому запущено локальний сервер онлайн відеогри (рис 4.1.9). Після налаштувань фаєрволу, потрібно перевірити його доступність з інтернету та наявність у списку лаунчера гри (рис 4.1.10).

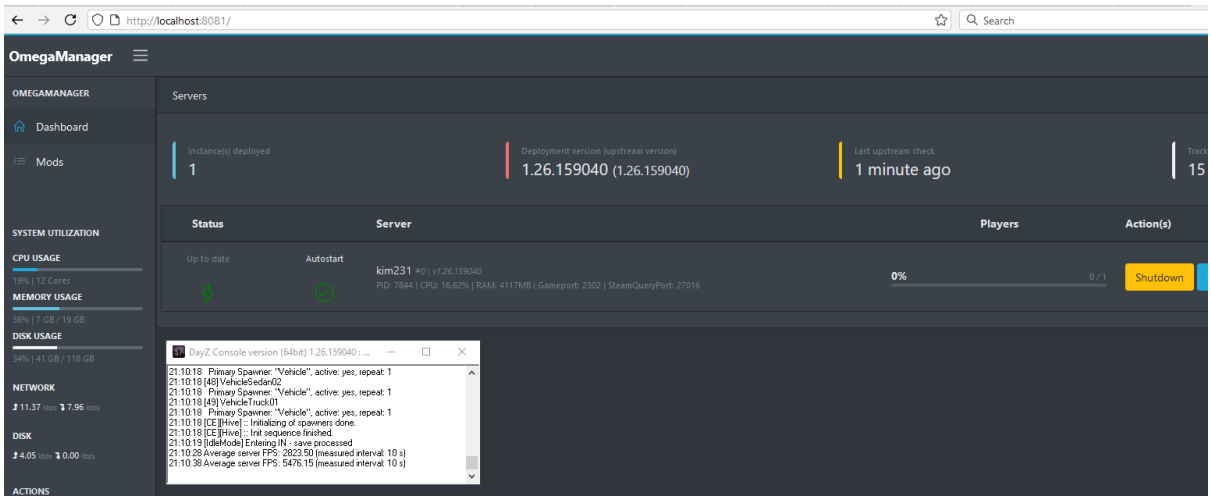


Рисунок 4.1.9 – Web інтерфейс системи управління сервером

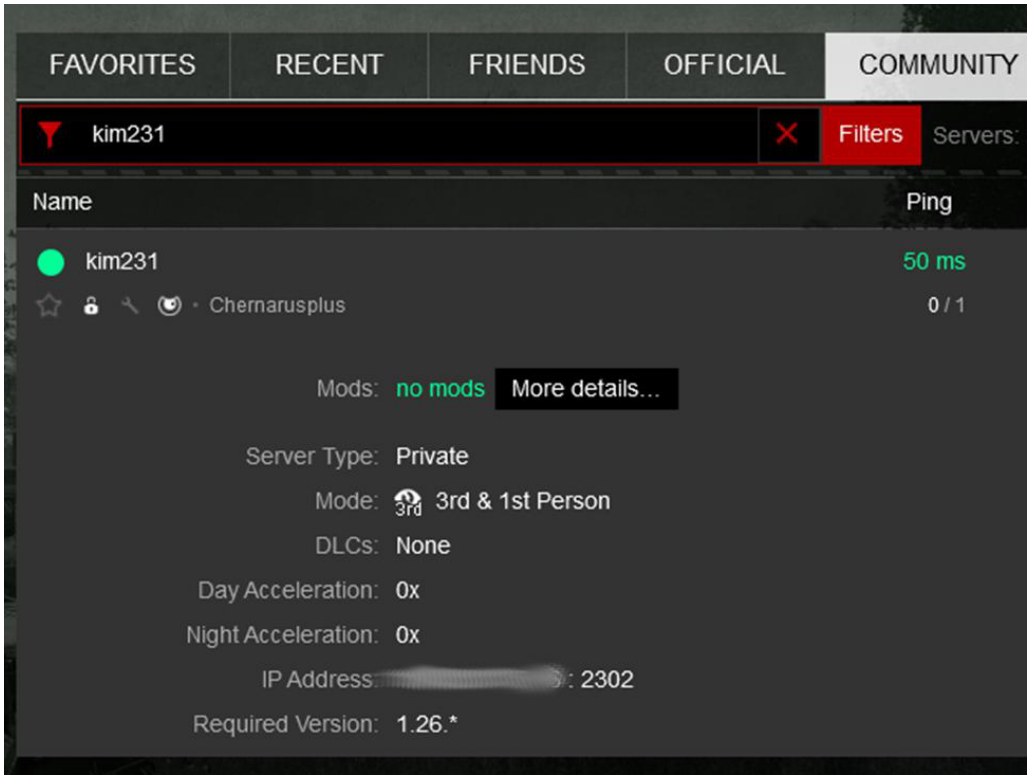


Рисунок 4.1.10 – Доступність з лаунчера гри



Рисунок 4.1.11 – Підключення до серверу

Сервер функціонує, відображається у списку серверів у лаунчері гри та забезпечує стабільне з’єднання.

Перевіримо роботу налаштованих Unboud DNS (рис. 4.1.13) та Adguard DNS (рис 4.1.12) сервісів.

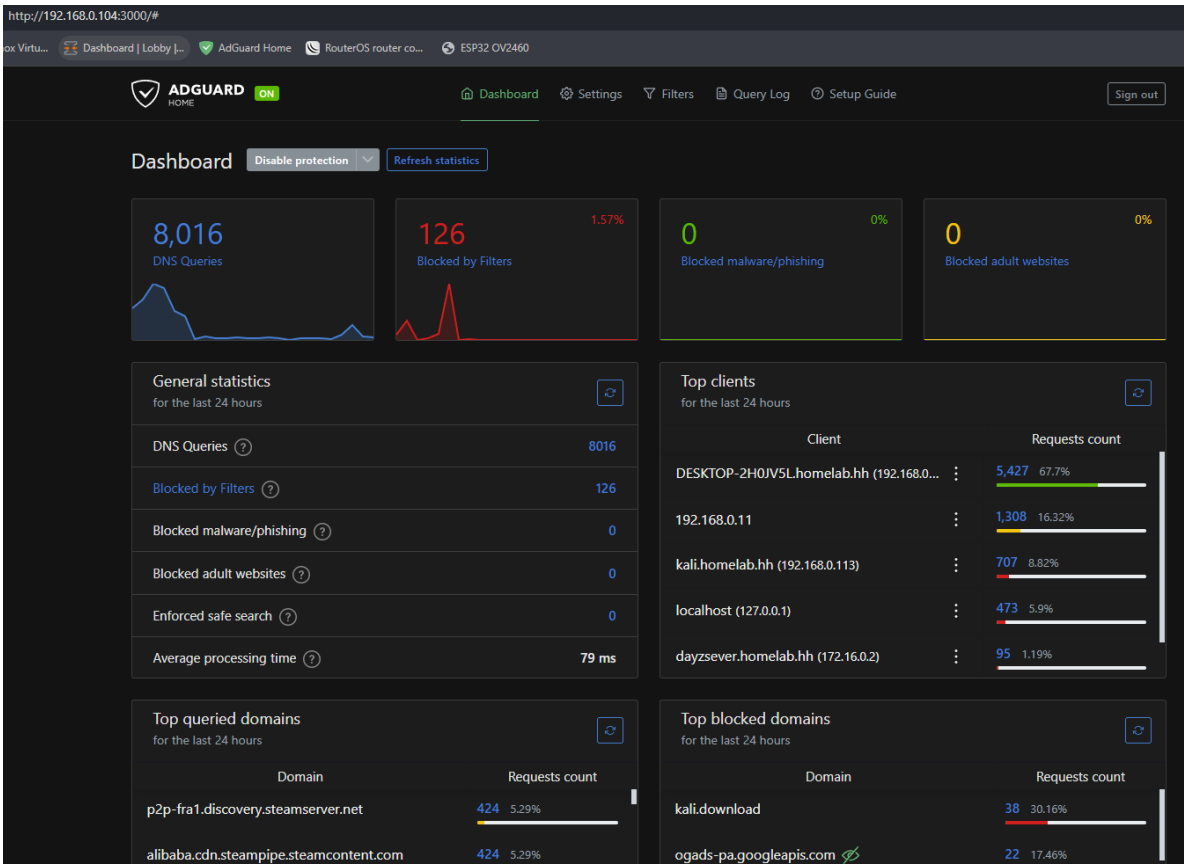


Рисунок 4.1.12 – Adguard DNS

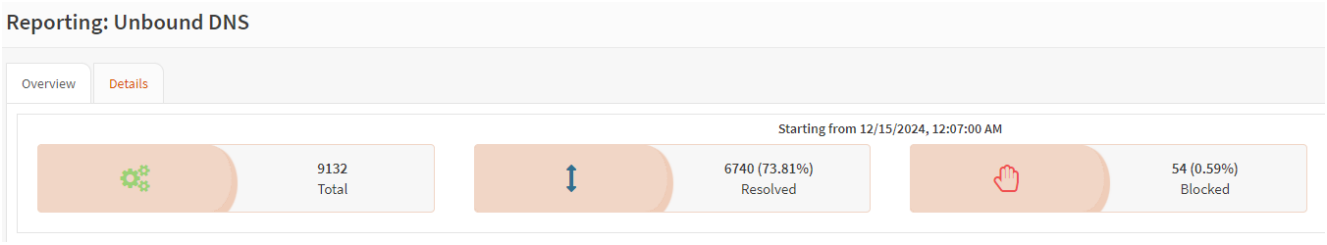


Рисунок 4.1.13 – Unbound DNS

Сервіси DNS працюють добре, блок-листи забезпечують блокування небажаних запитів.

4.2 Перевірка безпеки

Для перевірки безпеки налаштованої мережевої інфраструктури було використано кілька методів тестування, зокрема аналіз вразливостей, перевірка доступності мережевих ресурсів та тестування захисту від зовнішніх атак.

Основним інструментом для активного тестування безпеки став фреймворк Metasploit, який дозволяє моделювати реальні атаки та перевіряти ефективність впроваджених заходів безпеки.

Виконавши базове сканування портів, інформації про відкриті порти не було отримано (рис. 4.2.1), тому що весь трафік заблокував фаєрвол (рис 4.2.2).

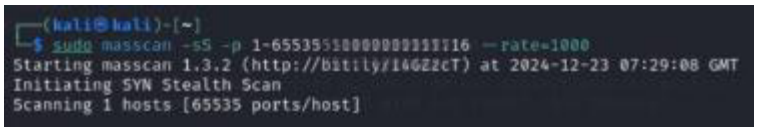


Рисунок 4.2.1– Проведення сканування портів

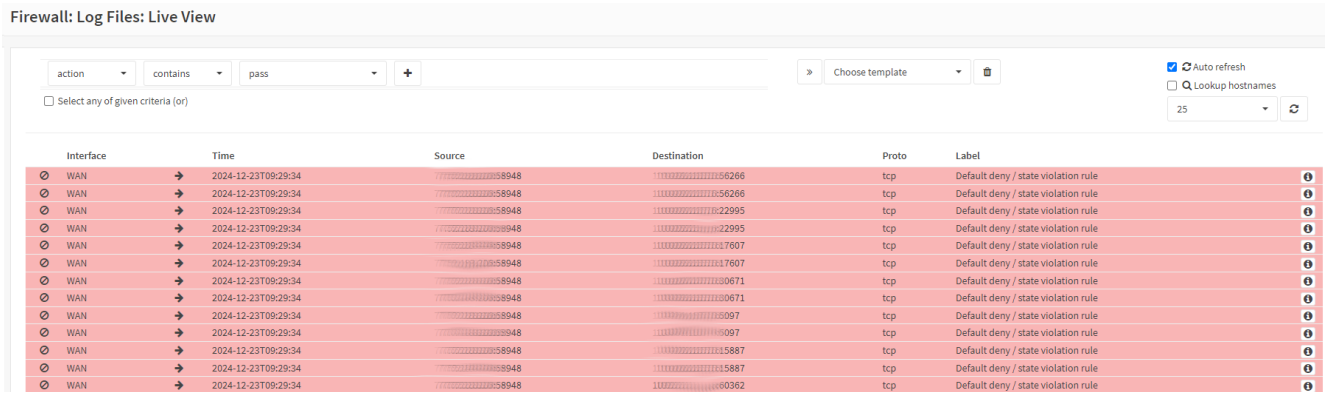


Рисунок 4.2.2 – Робота фаєрволу

Провівши сканування на доступність HTTP з’єднання з фаєрволом (рис 4.2.3), результату не отримали, це означає що дістатись по цьому протоколу до веб інтерфейсу неможливо (рис 4.2.4).

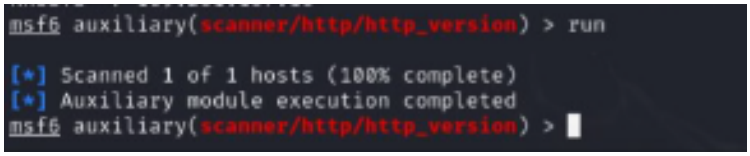


Рисунок 4.2.3– Проведення сканування HTTP

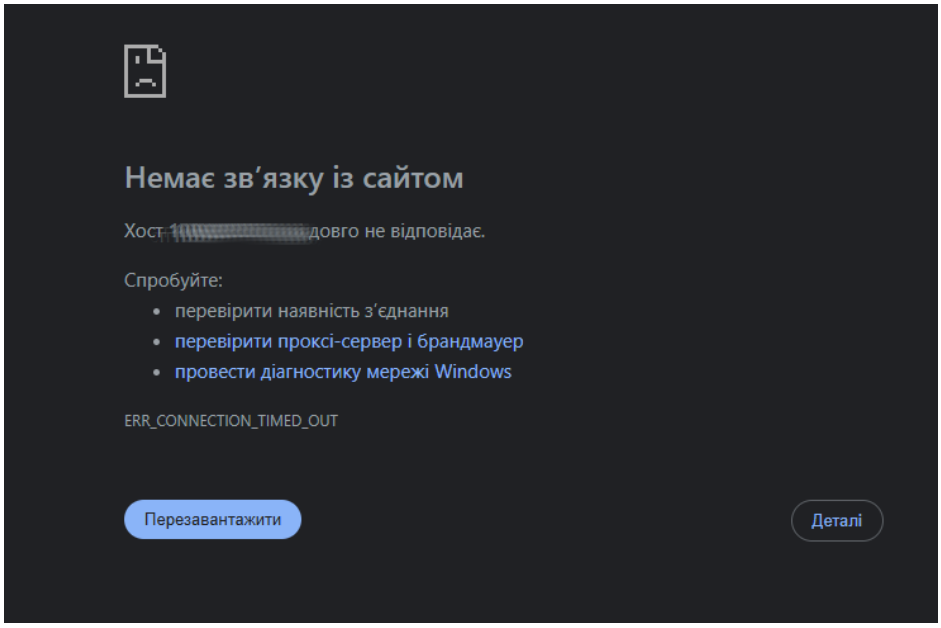


Рисунок 4.2.4– Перевірка доступу по протоколу HTTP

Перевірка налаштування DNS показала, що вони працюють справно (рис 4.2.5) та мають високу оцінку безпеки (рис 4.2.6).

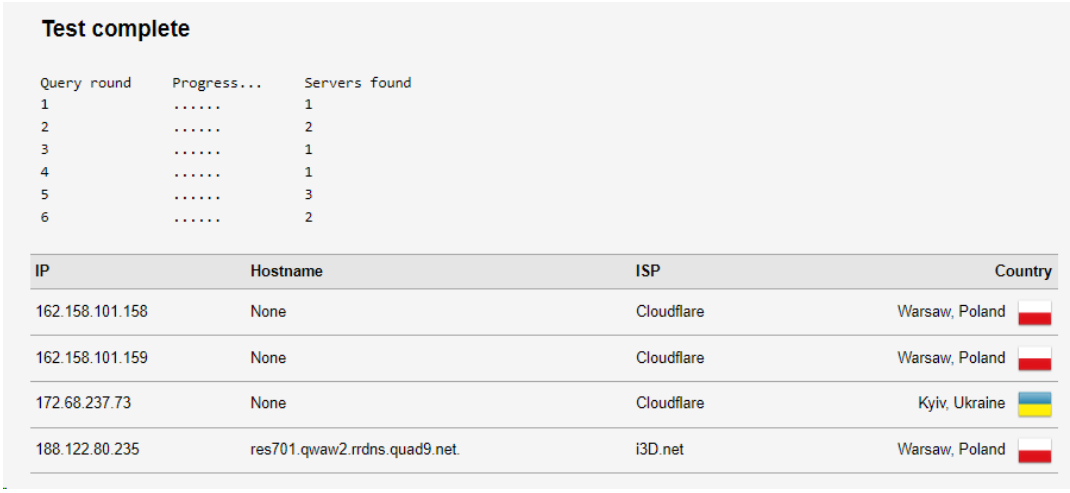


Рисунок 4.2.5 – Перевірка DNS на витік IP адреси

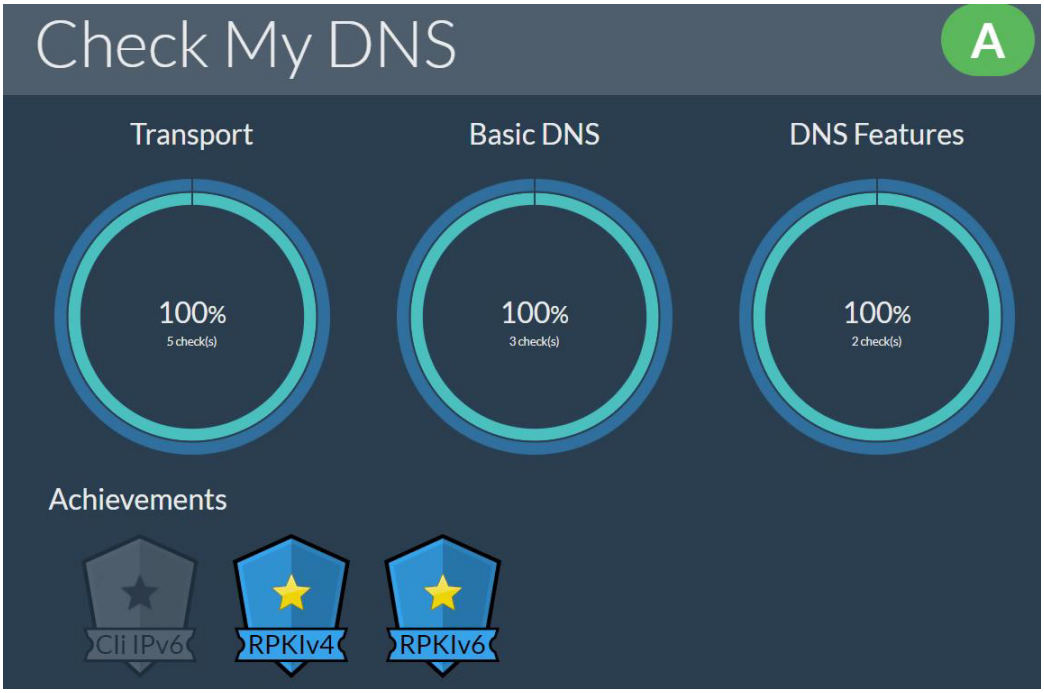


Рисунок 4.2.6 – Перевірка DNS на рівень захищеності

Також перевірка роботи IDS/IPS показала, що правила і сам сервіс працюють добре (рис 4.2.7).

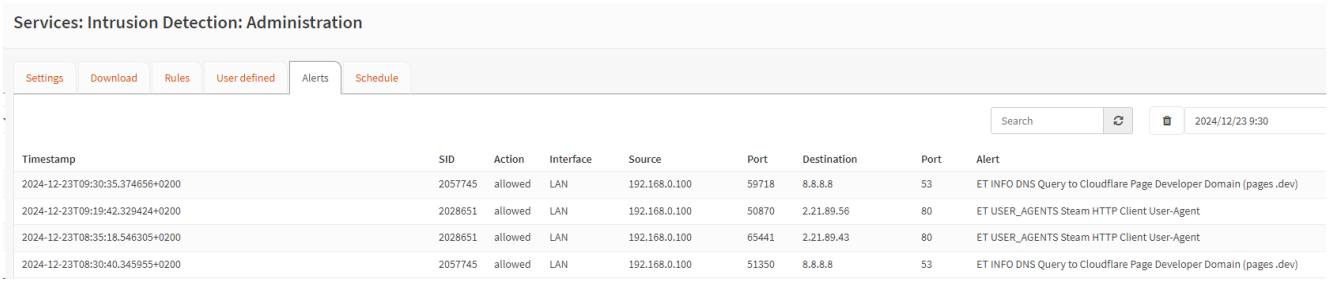


Рисунок 4.2.7 – Перевірка Suricata

Висновки до розділу 4

У четвертому розділі роботи проведено тестування створеної мережевої інфраструктури для оцінки її працездатності та рівня безпеки. Виконано тестування основних функцій мережевої інфраструктури, включаючи маршрутизацію, сегментацію трафіку, доступ до сервісів через VLAN та роботу DNS. Результати перевірки підтвердили стабільність роботи мережі, коректність налаштувань і відповідність функціональним вимогам.

Проведено оцінку ефективності впроваджених заходів безпеки, включаючи IPS/IDS, правила фаєрволу, геоблокування та захист DNS. Перевірка виявила стійкість мережі до базових атак. Виявлені незначні недоліки було оперативно усунуто.

Таким чином, результати тестування підтвердили ефективність запропонованих рішень, їх відповідність вимогам продуктивності та безпеки. Реалізована мережа готова до експлуатації в реальних умовах.

ВИСНОВКИ

У першому розділі розглянуто основні теоретичні відомості, що є основою для побудови сегментованих мереж: визначено основні підходи до сегментації мережі, включаючи фізичну сегментацію (засновану на розділенні фізичних компонентів) та логічну сегментацію (на основі програмних рішень). Описано принципи роботи віртуальних локальних мереж (VLAN), які забезпечують логічну ізоляцію трафіку в межах однієї фізичної інфраструктури. Розглянуто поняття демілітаризованої зони (DMZ) як методу підвищення захищеності критичних сервісів шляхом їх ізоляції від внутрішньої мережі та прямого доступу ззовні.

Наведено основи роботи системи доменних імен DNS. Вказано на її роль у забезпеченні продуктивності та зручності в роботі мережі. Проаналізовано ключові переваги сегментації. Таким чином, розглянуті у розділі теоретичні аспекти забезпечують базис для подальшого вибору технологій та інструментів, необхідних для проектування та впровадження сегментованих мереж.

У другому розділі було встановлено ключові технічні вимоги до побудови сегментованої мережі, обґрунтовано вибір відкритого програмного забезпечення та інструментів Proxmox і OPNsense. Рішення базуються на їх функціональності, простоті налаштування та доступності.

Проведено порівняння доступних гіпервізорів (OPNSense, CitrixXen, VMware ESXi) за критеріями продуктивності, сумісності, гнучкості в налаштуванні та використання відкритого програмного забезпечення. У результаті обрано Proxmox як найбільш відповідний варіант для реалізації поставлених завдань.

Також, у другому розділі обґрунтовано методи інтеграції обраних технологій для забезпечення узгодженої роботи компонентів та визначено ключові аспекти взаємодії гіпервізора, засобів маршрутизації і інших компонентів, що гарантують стабільну та ефективну роботу сегментованої мережі.

Третій розділ присвячено детальному опису методології проектування та впровадження сегментованої мережі та спроектована її логічна та фізична структура з урахуванням вимог масштабованості, продуктивності та безпеки. Фізична інфраструктура створена на основі сучасних відкритих рішень:

розгортутого та налаштованого Proxmox як платформи для віртуалізації, що забезпечує ефективне використання серверних ресурсів. Налаштування включали створення віртуальних машин для основних мережевих компонентів.

OPNsense налаштовано як основний маршрутизатор і міжмережевий екран а також реалізовано базові функції маршрутизації, VPN і механізми контролю доступу. Забезпечено логічну сегментацію мережі через використання VLAN та виконано маршрутизацію між сегментами з використанням OPNsense та комутатора, що підтримує VLAN. Реалізовано багаторівневий підхід до захисту мережі. Встановлено та налаштовано IPS/IDS для виявлення та запобігання загрозам, створено правила фаєрволу та впроваджено механізми геоблокування.

Налаштовано безпечну роботу DNS, включаючи використання захищених серверів для запобігання DNS-спуфінгу та інших атак.
Забезпечено узгоджену роботу всіх компонентів мережі, що гарантує стабільність, високу продуктивність та відповідність вимогам безпеки.

У четвертому розділі роботи проведено тестування створеної мережевої інфраструктури для оцінки її працездатності та рівня безпеки. Виконано тестування основних функцій мережевої інфраструктури, включаючи маршрутизацію, сегментацію трафіку, доступ до сервісів через VLAN та роботу DNS. Результати перевірки підтвердили стабільність роботи мережі, коректність налаштувань і відповідність функціональним вимогам.

Проведено оцінку ефективності впроваджених заходів безпеки, включаючи IPS/IDS, правила фаєрволу, геоблокування та захист DNS. Перевірка виявила стійкість мережі до базових атак. Виявлені незначні недоліки було оперативно усунуто.

Розроблене рішення має практичну значущість, оскільки може бути використане як у домашніх, так і у корпоративних умовах, забезпечуючи економію витрат на апаратне забезпечення та ліцензії. Висока гнучкість, простота адміністрування та можливість масштабування роблять запропоновану мережеву архітектуру ефективним інструментом для створення безпечного та продуктивного середовища для роботи з мережевими пристроями і сервісами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) Introduction to VLAN [Електронний ресурс]. – Режим доступу: https://www.amgsystems.com/news-and-media/technical-bulletins/introduction-to-vlan

2) VLANS - IEEE 802.1Q TRUNK LINK PROTOCOL ANALYSIS [Електронний ресурс]. – Режим доступу: http://www.firewall.cx/networking-topics/vlan-networks/221-vlan-8021q-analysis.html

3) INTERVLAN ROUTING - ROUTING BETWEEN VLAN NETWORKS [Електронний ресурс]. – Режим доступу: http://www.firewall.cx/networking-topics/vlan-networks/220-vlan-isl-analysis.html

4) Cisco: What is a DMZ? [Електронний ресурс]. – Режим доступу: https://community.cisco.com/t5/switching/what-is-the-use-dmz/td-p/2313763

5) How to set up a DMZ OPNsense [Електронний ресурс]. – Режим доступу: https://getlabsdone.com/how-to-configure-opnsense-dmz-step-by-step/

6) Cloudflare Learning Center: What is DNS? [Електронний ресурс]. – Режим доступу: https://www.cloudflare.com/learning/dns/what-is-dns/

7) IETF RFC 1035: Domain Names - Implementation and Specification [Електронний ресурс]. – Режим доступу: https://www.ietf.org/rfc/rfc1035.txt

8) OPNsense Documentation: Configuring UnboundDNS [Електронний ресурс]. – Режим доступу: https://docs.opnsense.org/manual/unbound.html

9) ICANN: DNS Security (DNSSEC) [Електронний ресурс]. – Режим доступу: https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

10) OPNsense Documentation [Електронний ресурс]. – Режим доступу https://docs.opnsense.org/

11) OPNsense Setup Guide [Електронний ресурс]. – Режим доступу: https://protectli.com/blog/opnsense-setup-guide/

12) OPNsense vs. pfSense Comparison [Електронний ресурс]. – Режим доступу: https://www.netgate.com/blog/opnsense-vs-pfsense.html

13) VE Documentation [Електронний ресурс]. – Режим доступу: https://pve.proxmox.com/wiki/Main_Page

14) Proxmox 101 [Електронний ресурс] – Режим доступу: https://medium.com/devopsdudes/proxmox-101-8204eb154cd5

15) Backup and Restore [Електронний ресурс] – Режим доступу: https://pve.proxmox.com/wiki/Backup_and_Restore

16) High Availability [Електронний ресурс] – Режим доступу: https://pve.proxmox.com/wiki/High_Availability

17) How to Create a VM in Proxmox VE [Електронний ресурс] – Режим доступу: https://support.us.ovhcloud.com/hc/en-us/articles/360010916620-How-to-Create-a-VM-in-Proxmox-VE

18) Qemu/KVM Virtual Machines [Електронний ресурс] – Режим доступу: https://pve.proxmox.com/wiki/Qemu/KVM_Virtual_Machines

19) Proxmox VE Administration Guide [Електронний ресурс] – Режим доступу: https://pve.proxmox.com/pve-docs/pve-admin-guide.html

20) How Server Virtualization Works [Електронний ресурс] – Режим доступу: https://computer.howstuffworks.com/server-virtualization.htm

21) What is Virtual Firewall? [Електронний ресурс] – Режим доступу: https://www.zenarmor.com/docs/network-security-tutorials/what-is-virtual-firewall

22) Details About Hardware Virtualization. [Електронний ресурс] – Режим доступу: https://docs.oracle.com/en/virtualization/virtualbox/6.0/admin/hwvirt-details.html

23) Adguard Home DNS [Електронний ресурс] – Режим доступу: https://github.com/AdguardTeam/AdGuardHome

24) Suricata User Guide [Електронний ресурс] – Режим доступу: https://docs.suricata.io/_/downloads/en/suricata-6.0.16/pdf/

25) Examine alerts, logs, and rules with Suricata Activity overview [Електронний ресурс] – Режим доступу: https://michaelwconrad.com/wp-content/uploads/2024/07/Suricata_Examine-alerts-logs-rules.pdf

ДОДАТКИ

Модель мережі

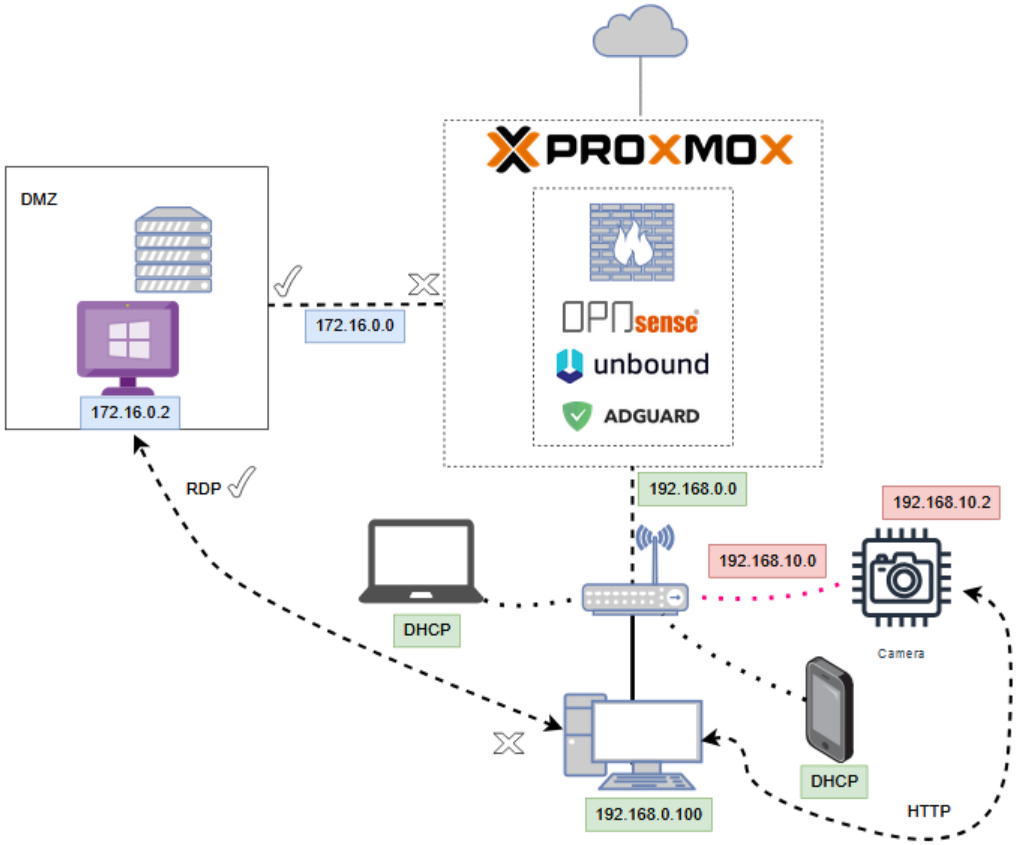


Рисунок 1 - Графічне відображення логічної схеми мережі

Мережа/Пристрій	Шлюз	IP-адреса	Маска	Префікс
Мережа LAN	-	192.168.0.0	255.255.255.0	/24
Робоча станція	192.168.0.104	192.168.0.100	255.255.255.0	/24
Ноутбук	192.168.0.104	DHCP	255.255.255.0	/24
Коммутатор	192.168.0.104	192.168.0.111	255.255.255.0	/24
Мережа VLAN	-	192.168.10.0	255.255.255.0	/24
IP Камера	192.168.10.1	192.168.10.2	255.255.255.0	/24
Мережа DMZ	-	172.16.0.0	255.255.255.0	/24
Сервер	172.16.0.1	172.16.0.2	255.255.255.0	/24

Рисунок 2 - Таблиця адресації мережі

Додаток Б

Макет системи

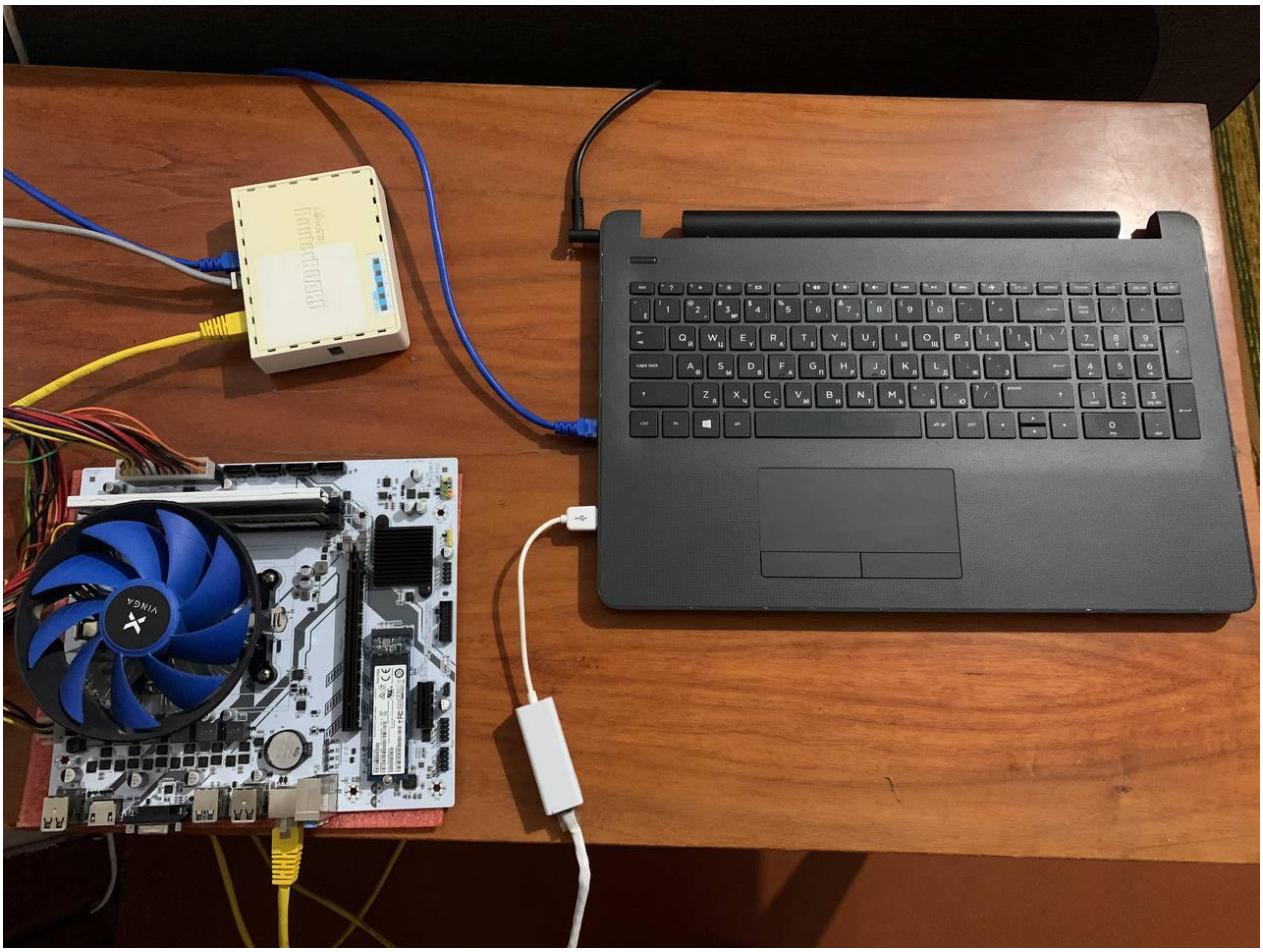


Рисунок 3 - Фізична реалізація мережі



Рисунок 4 - Комутатор та точка доступу MikroTik Router Board hAP lite



Рисунок 5 – IP Камера ESP32 Cam



Рисунок 6 – Серверне обладнання на основі AMD Ryzen