Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: "Використання гіпервізора XEN для створення захищеної IT-інфраструктури"

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Кащин Віталій Юрійович
підпис (прізвище та ініціали)

Керівник Тимощук Д. І.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Кащину Віталію Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Використання гіпервізора XEN для створення захищеної IT-інфраструктури

Керівник роботи Тимощук Дмитро Іванович, старший викладач кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «15» 04 2024 року № 4/7-350

2. Термін подання студентом завершеної роботи 12.06.2024

3. Вихідні дані до роботи Вимоги до безпеки IT-інфраструктури. Windows Server 2022 Гіпервізор XEN, брандмауер та маршрутизатор pfSense, NAS TrueNAS CORE

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1. Аналіз предметної області
2. Засоби створення лабораторного середовища віртуалізованої іт-інфраструктури
3. Встановлення, налаштування та тестування віртуалізованої іт-інфраструктури
4. Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Тема, мета, задачі. Огляд технології віртуалізації. Огляд архітектурних особливостей гіпервізора XEN. Типи віртуалізацій XEN. Схема лабораторного середовища. Платформа віртуалізації XCP-ng на основі гіпервізора XEN. Мережева архітектура XCP-ng. Консоль керування XCP-ng. XCP-ng Center. Вебінтерфейс керування Xen Orchestra. Налаштування брандмауера pfSense. Розгортання та налаштування NAS TrueNAS CORE. Розгортання та налаштування Windows Server 2022 RDS. Етапи тестування віртуалізованої IT-інфраструктури. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко С. Ю., к.т.н. доцент кафедри МТ		

7. Дата видачі завдання 29.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.01.2024	
2.	Опрацювання джерел в галузі дослідження	02.02 – 30.01	
3.	Оформлення розділу «Аналіз предметної області»	21.02 – 10.03	
4.	Оформлення розділу «Засоби створення лабораторного середовища віртуалізованої ІТ-інфраструктури»	11.03 – 25.03	
5.	Оформлення розділу «Встановлення, налаштування та тестування віртуалізованої ІТ-інфраструктури»	10.04 – 05.05	
6.	Оформлення розділу «Безпека життєдіяльності, основи охорони праці»	10.05 – 21.05	
7.	Оформлення кваліфікаційної роботи	23.05 – 06.06	
8.	Нормоконтроль	06.06 – 10.06	
9.	Перевірка на плагіат	11.06 – 12.06	
10.	Попередній захист кваліфікаційної роботи	14.06 – 15.06	
11.	Захист кваліфікаційної роботи	25.06.2024	

Студент _____ Кащин В. Ю.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Тимощук Д. І.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Використання гіпервізора XEN для створення захищеної IT-інфраструктури // Кваліфікаційна робота ОР «Бакалавр» // Кащин Віталій Юрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2024 // С. 73, рис. – 43, табл. – 0, кресл. – 14, додат. – 0.

Ключові слова: XEN, XCP-ng, pfSense, TrueNAS, NAT, гіпервізор, віртуалізація, Windows, брандмауер.

В бакалаврській кваліфікаційній роботі представлено розробку та налаштування безпечної IT-інфраструктури на основі гіпервізора типу 1 XEN, використовуючи платформу XCP-ng. Робота охоплює три основні розділи: огляд принципів віртуалізації і специфіки гіпервізора XEN, розробку тестового лабораторного середовища з використанням XCP-ng, та практичне впровадження маршрутизатора pfSense з функцією брандмауера та VPN концентратора, NAS сервера TrueNAS CORE, та Windows Server 2022 з роллю RDS для створення комплексної віртуалізованої IT-інфраструктури. В роботі детально проаналізовано архітектурні особливості та безпеку гіпервізора XEN, показано переваги комбінації паравіртуалізації та апаратної віртуалізації. В роботі демонструється налаштування та тестування ключових компонентів IT-інфраструктури, що підтверджує ефективність та безпеку створеної віртуальної інфраструктури. Результати дослідження мають практичне значення для розробки корпоративних IT-інфраструктур на основі віртуалізації.

ANNOTATION

Use of the XEN hypervisor to create a secure IT infrastructure. // Thesis of educational level "Bachelor"// Vitalii Kashchyn // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБ-41 // Ternopil, 2024 // P. 73, fig. - 43, tab. - 0, chair. - 14, added. - 0.

Keywords: XEN, XCP-ng, pfSense, TrueNAS, NAT, hypervisor, virtualization, Windows, firewall.

The bachelor's thesis presents the development and configuration of a secure IT infrastructure based on the XEN type 1 hypervisor using the XCP-ng platform. The work covers three main sections: an overview of the principles of virtualization and the specifics of the XEN hypervisor, the development of a test laboratory environment using XCP-ng, and the practical implementation of a pfSense router with the function of a firewall and a VPN hub, a TrueNAS CORE NAS server, and Windows Server 2022 with an RDS role to create complex virtualized IT infrastructure. The paper analyzes in detail the architectural features and security of the XEN hypervisor, and shows the advantages of a combination of paravirtualization and hardware virtualization. The work demonstrates the configuration and testing of key components of the IT infrastructure, which confirms the effectiveness and security of the created virtual infrastructure. The research results are of practical importance for the development of corporate IT infrastructures based on virtualization.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ВМ	—	Віртуальна машина
XS	—	XenStore/XenBus
TS	—	Toolstack
DE	—	Device Emulation
QEMU	—	Quick Emulator
PV	—	Paravirtualization
HVM	—	Hardware-assisted virtualization
LVM	—	Logical Volume Manager
iSCSI	—	Internet Small Computer System Interface
NFS	—	Network File System
NAS	—	Network Attached Storage
XCP-ng	—	Xen Cloud Platform - next generation
DMC	—	Dynamic Memory Control
xeCLI	—	Xen Command Line Interface
XO Lite	—	Xen Orchestra Lite
CLI	—	Command Line Interface
SR	—	Storage Repository
VDI	—	VirtualBox Disk Image
VHD	—	Virtual Hard Disk
PIF	—	Physical Interface
VIF	—	Virtual Interface
UUID	—	Universally Unique Identifier
VLAN	—	Virtual Local Area Network
PF	—	Packet Filter
IDS	—	Intrusion Detection System
IPS	—	Intrusion Prevention System
WAN	—	Wide Area Network

DHCP	—	Dynamic Host Configuration Protocol
NAT	—	Network Address Translation
L2TP	—	Layer 2 Tunneling Protocol
VPN	—	Virtual Private Network
LAN	—	Local Area Network
DH	—	Diffie-Hellman
SA	—	Security Association
ESP	—	Encapsulating Security Payload
UDP	—	User Datagram Protocol
ICMP	—	Internet Control Message Protocol
DNS	—	Domain Name System
DNSSEC	—	Domain Name System Security Extensions
TLS	—	Transport Layer Security
NAS	—	Network Attached Storage
ZFS	—	Zettabyte File System
SMB	—	Server Message Block
AES	—	Advanced Encryption Standard
GCM	—	Galois/Counter Mode
RDS	—	Remote Desktop Services
RDC	—	Remote Desktop Connection
CBC	—	Cipher Block Chaining

ВСТУП

У сучасному цифровому світі, де комп'ютерні технології є частиною нашого повсякденного життя та бізнес-процесів, питання безпеки та захисту інформаційних систем стає дедалі важливішим. Зростання кількості кіберзагроз та постійні спроби несанкціонованого доступу до конфіденційної інформації вимагають вдосконалення заходів захисту та надійності IT-інфраструктури. У цьому контексті актуальність дослідження використання гіпервізора XEN для створення захищеної IT-інфраструктури надає можливість вивчення та розробки ефективних заходів забезпечення безпеки в віртуальних середовищах.

Метою даного дослідження є розробка та практична реалізація захищеної IT-інфраструктури на основі гіпервізора XEN. Для досягнення цієї мети передбачено вирішення таких основних завдань:

- детальний аналіз архітектури гіпервізора XEN та можливості його використання для створення віртуалізованого середовища;

- розробка архітектури захищеної IT-інфраструктури з використанням віртуальних машин pfSense, TrueNAS CORE та Windows Server 2022;

- налаштування кожного компонента системи, зокрема VPN-сервера, брандмауера, NAS сервера та Windows RDS ;

- перевірка надійності та функціональності розробленої віртуалізованої IT-інфраструктури.

Об'єктом дослідження є гіпервізор XEN та віртуальні машини, що працюють під його управлінням, з фокусом на створенні безпечної та функціональної IT-інфраструктури.

Предметом дослідження є конфігурація та налаштування віртуальних машин pfSense, TrueNAS CORE та Windows Server 2022, а також їх взаємодія в рамках гіпервізора XEN. Основний акцент робиться на забезпеченні високого рівня безпеки та функціональності кожного компонента системи.

Одержані результати можуть знайти широке практичне застосування в області створення та управління захищеними IT-інфраструктурами. Використання гіпервізора XEN та відповідно налаштованих віртуальних машин

дозволить забезпечити надійний захист інформації, а також забезпечить стабільну та ефективну роботу системи в цілому.

РОЗДІЛ 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Огляд технології віртуалізації

Віртуалізація - це технологія, яка дозволяє одному фізичному серверу підтримувати роботу багатьох віртуальних серверів (операційних систем), які функціонують незалежно один від одного [1]. Технологія дає можливість створювати віртуальні екземпляри апаратного та/або програмного забезпечення, що забезпечує ізоляцію віртуальних серверів. Технологія віртуалізації відіграє ключову роль у створенні ефективних та гнучких IT-середовищ. Цей підхід дозволяє використовувати апаратне забезпечення більш ефективно, зменшуючи витрати та забезпечуючи легше управління інфраструктурою. Кожна ВМ має власне ізольоване середовище, що підвищує безпеку та стабільність.

Гіпервізори є ключовими компонентами віртуалізації та віртуальних середовищ [2]. Ці програмні рішення дозволяють запускати декілька віртуальних операційних систем на одному фізичному сервері. Існують два основних типи гіпервізорів: тип 1 та 2.

Гіпервізор типу 2 - це програмне забезпечення, яке встановлюється на операційну систему хоста і дозволяє створювати та керувати віртуальними машинами (див. рисунок 1.1).

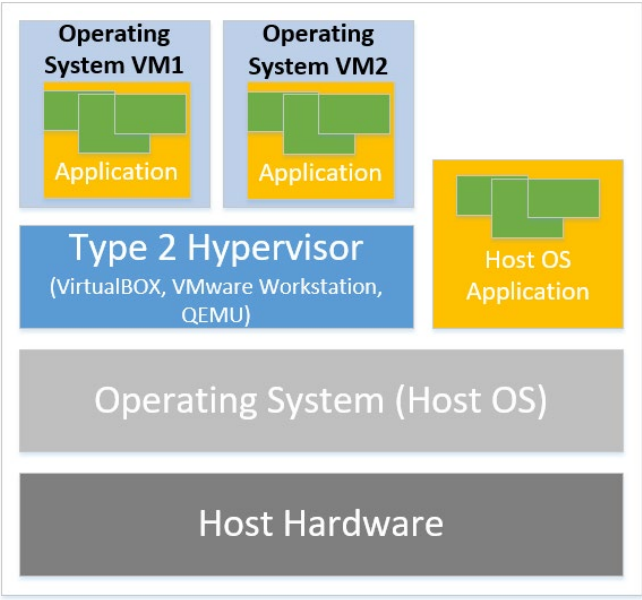

Рисунок 1.1 – Принципова схема гіпервізора типу 2

Відмінною особливістю гіпервізора типу 2 є те, що він не працює безпосередньо на апаратному забезпеченні, а використовує операційну систему хоста як проміжний шар для доступу до апаратних ресурсів. Це робить його більш гнучким у використанні, але впливає на продуктивність порівняно з гіпервізорами типу 1. Оскільки гіпервізор типу 2 встановлюється як додаткове програмне забезпечення на операційну систему хоста це дозволяє користувачам запускати ВМ у звичайному робочому середовищі, наприклад, на персональному комп'ютері або ноутбуці.

Даний тип гіпервізора зазвичай легший у встановленні та налаштуванні, що робить його популярним вибором для розробників, тестувальників та навчальних завдань, де потрібна швидка і проста віртуалізація. Користувачі можуть легко запускати декілька різних операційних систем на одному фізичному комп'ютері, що забезпечує велику гнучкість для тестування програмного забезпечення, емуляції середовищ або навчання. Через додатковий рівень абстракції, викликаний необхідністю проходження через операційну систему хоста для доступу до апаратного забезпечення, гіпервізори типу 2 мають нижчу продуктивність порівняно з гіпервізорами типу 1. Хоча гіпервізори типу 2 дозволяють ізоляцію ВМ одна від одної, вони залежать від безпеки та стабільності операційної системи хоста, що може створювати додаткові ризики.

Приклади гіпервізорів типу 2: VMware Workstation, Oracle VirtualBox, Parallels Desktop та QEMU.

Програмне забезпечення, яке працює прямо на апаратному забезпеченні хост-системи і відповідає за управління ВМ називається гіпервізором типу 1 (див. рисунок 1.2).

Він є основою для створення і керування віртуальними середовищами в центрах обробки даних і обчислювальних хмарах. При роботі безпосередньо на обладнанні гіпервізор тип 1 забезпечує високу ефективність та продуктивність в порівнянні з гіпервізорами типу 2.

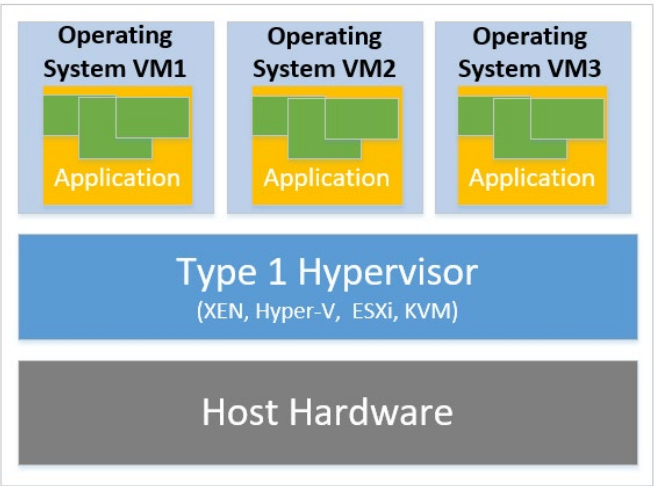

Рисунок 1.2 – Принципова схема гіпервізора типу 1

Кожна ВМ ізольована від інших, що забезпечує високий рівень безпеки. Якщо одна ВМ стає компрометованою або виходить з ладу, інші ВМ продовжують працювати без перебоїв.

Гіпервізори типу 1 супроводжуються інструментами керування, які дозволяють адміністраторам централізовано керувати віртуальними машинами, включаючи їх розгортання, моніторинг та резервне копіювання. Даний тип гіпервізора може підтримувати велику кількість ВМ на одному фізичному сервері, залежно від його апаратних ресурсів, таких як процесор, пам'ять, і мережеві можливості. Гіпервізори типу 1 проектуються сумісними з широким спектром апаратного забезпечення, але деякі з них можуть вимагати специфічне або сертифіковане апаратне забезпечення для оптимальної роботи. Він широко використовуються в корпоративних центрах обробки даних, хмарних обчисленнях, і для створення великих віртуальних IT-інфраструктур [3].

Приклади гіпервізорів типу 1: VMware ESXi, Microsoft Hyper-V, Xen та KVM.

Гіпервізор типу 1 є ключовим компонентом віртуальної IT-інфраструктури, що дозволяє підприємствам та хмарним провайдерам ефективно розподіляти ресурси, забезпечувати високу доступність та масштабувати свої IT-середовища [4]. Його використання забезпечує оптимальне використання апаратного забезпечення, підвищення безпеки та гнучкість у керуванні віртуальними машинами.

1.2 Загальний огляд гіпервізора XEN

XEN - це гіпервізор типу 1, призначений для одночасного запуску різних операційних систем на одному хості. Він використовується як основна технологічна основа для різноманітних комерційних і відкритих проектів, включаючи віртуалізацію серверів, віртуалізацію настільних комп'ютерів, інфраструктура як послуга (IaaS), програми безпеки, а також вбудовані та апаратні пристрої. Гіпервізор XEN знаходить широке застосування в найбільших хмарних обчисленнях на сьогоднішній день [5].

Оскільки XEN використовує структуру мікроядра з невеликим обсягом пам'яті та обмеженим інтерфейсом для гостьової системи, це надає йому переваги у надійності та безпеці порівняно з гіпервізорами іншої архітектури. Його стек керування (Domain0 або Dom0), зазвичай працює під управлінням операційної системи Linux, але може бути замінений іншими операційними системами, такими як NetBSD чи OpenSolaris.

Ця структура забезпечує невеликий обсяг пам'яті для мікроядра, що дозволяє гіпервізору працювати ефективно та мінімізувати вплив на продуктивність. Обмежений інтерфейс для гостьових систем покращує його безпеку, оскільки зменшує можливість атак та небезпечних вірусів.

У результаті такого підходу XEN стає надійним, ефективним та безпечним рішенням для віртуалізації, особливо для великих і складних обчислювальних середовищ.

Гіпервізор XEN володіє рядом особливостей, що роблять його потужним та гнучким інструментом для віртуалізації, включаючи здатність запускати основний драйвер пристрою всередині віртуальної машини. Цей підхід має свої переваг. Якщо основний драйвер пристрою віртуальної машини виходить з ладу, XEN дозволяє перезавантажити саму віртуальну машину, що містить драйвер, та перезапустити драйвер без впливу на решту системи. Це робить робочий процес більш гнучким і менше схильним до простоїв через неполадки в окремих компонентах.

XEN підтримує повністю паравіртуалізовані гостьові системи, що дозволяє їм працювати як віртуальні машини із максимальною ефективністю. Завдяки можливості паравіртуалізації, гостьові системи можуть працювати швидше, оскільки вони взаємодіють з гіпервізором безпосередньо, без необхідності використання апаратних розширень. Це особливо корисно в ситуаціях, де важлива висока продуктивність та низька затримка. Гіпервізор XEN може працювати на обладнанні, яке не підтримує апаратні розширення віртуалізації. Це робить його універсальним рішенням, що може бути використане на різноманітних серверах із різними характеристиками та підтримкою апаратури.

Гіпервізор мікроядра відрізняється від монолітного гіпервізора тим, що включає лише основні та незмінні функції, такі як керування фізичною пам'яттю та планування для процесора. Наприклад, драйвери пристроїв та інші змінні компоненти знаходяться поза мікроядерним гіпервізором. За своєю природою мікроядерний гіпервізор має менший розмір коду порівняно з монолітним гіпервізором. У контексті XEN, це означає, що гіпервізор надає лише основні можливості, не включаючи драйверів пристроїв. Він служить механізмом, що дозволяє гостьовим операційним системам мати прямий доступ до фізичних пристроїв, але не містить конкретні реалізації цих драйверів. Такий підхід забезпечує гнучкість та розширюваність системи віртуалізації.

Однією з вагомих переваг мікроядерного гіпервізора, зокрема XEN, є його малий розмір коду. Це робить систему менш вразливою до помилок та забезпечує високий рівень стабільності та безпеки. Гіпервізор XEN, власне кажучи, забезпечує віртуальне середовище, що розташоване між апаратурою та операційною системою, дозволяючи ефективно використовувати фізичні ресурси для віртуальних машин.

1.3 Архітектурні особливості XEN

Гіпервізор XEN працює безпосередньо на апаратному рівні та відповідає за критичні аспекти управління системою, такі як планування роботи процесора, управління пам'яттю, контроль таймерів і обробка переривань. Цей гіпервізор є

першою програмою, яка запускається після завантажувача, і вона забезпечує основні сервіси для всіх віртуальних машин в системі [6].

Над гіпервізором працює низка віртуальних машин, кожна з яких називається доменом або гостем (див.рисунок 1.3).

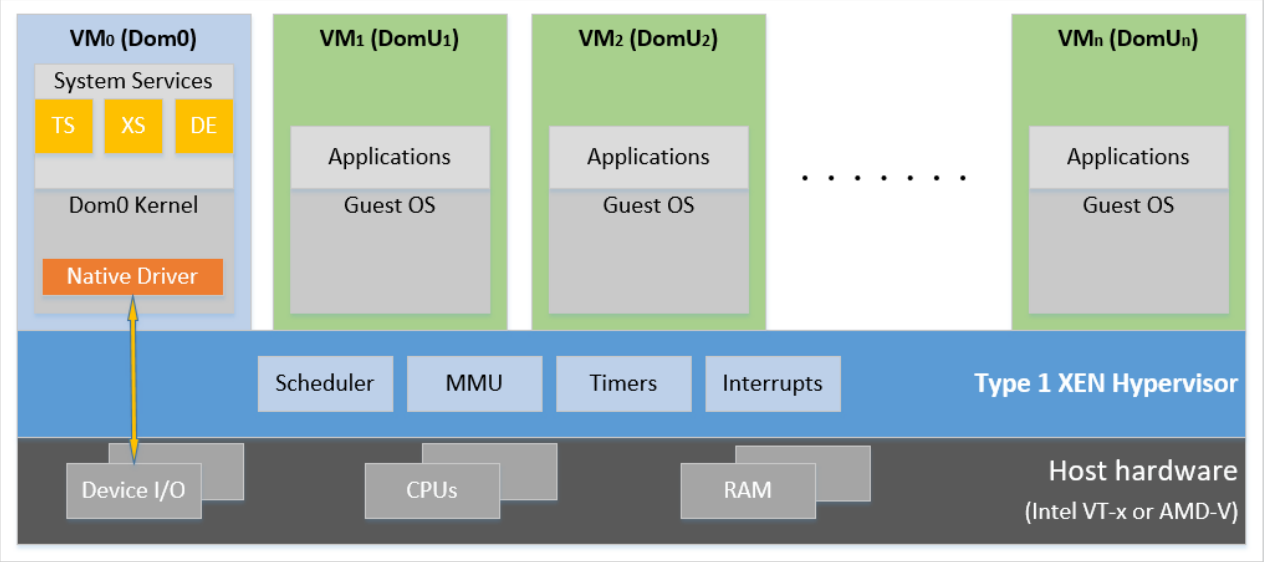

Рисунок 1.3 – Архітектура гіпервізора XEN

Dom0 – це домен для контролю. Dom0 містить драйвери для всіх пристроїв у системі, що робить його основним контрольним пунктом для обслуговування апаратного забезпечення.

Специфічні завдання Dom0 включають керування системними ресурсами, які надаються іншим віртуальним машинам, та надання сервісів для ефективного управління системою на основі XEN. До завдань Dom0 входить взаємодія з гіпервізором для запуску, зупинки та моніторингу віртуальних машин, а також розподілу ресурсів між ними. Таким чином, Dom0 виступає ключовою складовою для ефективного управління та функціонування системи віртуалізації на базі XEN.

Гіпервізор XEN - це винятково економний рівень програмного забезпечення. XEN на платформі Arm має менше ніж 65 тис. рядків коду, а на x86 - менше ніж 300 тис. рядків коду. Це свідчить про те, що гіпервізор XEN розроблений з використанням невеликої кількості коду, що є важливою рисою для забезпечення простоти, надійності та безпеки системи віртуалізації.

В системі віртуалізації XEN гостьові домени є базовою складовою. Кожен гостьовий домен створює власне віртуалізоване середовище, в якому працює власна операційна система та набір програм.

Одна з ключових характеристик XEN - це повна ізоляція гостьових віртуальних машин від апаратного забезпечення. Кожен гостьовий домен, також відомий як DomU (непривілейований домен), не має прямого доступу до апаратного забезпечення чи функцій введення-виведення. Це забезпечує високий рівень безпеки та ізоляції між віртуальними середовищами.

Контрольний домен (Dom0) у системі XEN є особливою та привілейованою віртуальною машиною, яка відіграє ключову роль у керуванні та обслуговуванні інших віртуальних машин. Dom0 має спеціальні привілеї, що надають йому можливість прямого доступу до апаратного забезпечення, управління функціями введення-виведення та взаємодії з іншими віртуальними машинами. Це дозволяє йому взаємодіяти з апаратурою, керувати ресурсами та координувати дії інших віртуальних машин. Dom0 відповідає за управління функціями введення-виведення системи. Це включає в себе роботу з пристроями введення-виведення та розподіл ресурсів між віртуальними машинами. Контрольний домен взаємодіє з іншими віртуальними машинами, надаючи їм можливість працювати, зупинятися та взаємодіяти одна з одною. Це забезпечує централізований підхід до управління системою віртуалізації. Dom0 відповідає за розподіл та управління ресурсами системи між різними віртуальними машинами. Це включає в себе призначення процесорного часу, пам'яті та інших апаратних ресурсів.

Гіпервізор XEN не може функціонувати без контрольного домену (Dom0), оскільки він виступає основним агентом для керування системою віртуалізації та забезпечення її ефективності та стабільності.

Контрольний домен (Dom0) у стандартній конфігурації гіпервізора XEN включає ключові компоненти для ефективного управління та функціонування системи віртуалізації. Він виступає важливою складовою системи, надаючи різноманітні служби та функції. XS - є системними службами, які входять до складу Dom0 і призначені для управління параметрами та обміну даними між

різними віртуальними машинами та гіпервізором. XS забезпечує централізований механізм зберігання конфігураційних даних.

Набір інструментів (TS) відкриває інтерфейс користувача для системи на основі XEN, дозволяючи адміністраторам ефективно керувати та моніторити віртуальні машини. TS включає різні інструменти для створення, запуску, зупинки та моніторингу віртуальних машин. Набір інструментів у гіпервізорі XEN відіграє важливу роль у спрощенні управління віртуальними машинами та надає різні зручні інтерфейси для користувачів та адміністраторів. TS надає користувачам можливість легко створювати, знищувати та конфігурувати віртуальні машини. Це включає в себе встановлення параметрів, таких як обсяги пам'яті, кількість процесорів, обрані образи операційних систем та інші налаштування. Він надає інтерфейси, які можуть працювати через командний рядок, графічний інтерфейс або інші методи. Це робить управління віртуальними машинами більш зручним та пристосованим до потреб користувачів.

Програмне забезпечення XEN використовує різноманітні набори інструментів, кожен з яких надає API для виклику інших інструментів або взаємодії з інтерфейсом користувача. XEN може бути інтегровано зі стандартним комплектом інструментів, Libvirt і XAPI. Спільне використання гіпервізора XEN та XAPI відоме як XCP і має свій розвиток як комерційний проект XenServer (Citrix Hypervisor) та в рамках відкритого проекту XCP-ng.

TS взаємодіє з хмарними оркестраторами, такими як OpenStack. Це дозволяє інтегрувати систему на основі XEN у великі хмарні інфраструктури та автоматизувати управління ресурсами.

Емуляція пристрою (DE) базується на QEMU та відповідає за емуляцію пристроїв в системах на основі XEN.

Dom0 включає драйвери для фізичних пристроїв, що надає підтримку для їх взаємодії з гіпервізором. Також містить драйвери для віртуальних пристроїв, що дозволяє взаємодіяти із засобами віртуалізації.

Для оптимального функціонування гіпервізора XEN і віртуальних машин у системі, різні компоненти вимагають специфічного програмного забезпечення та підтримки від операційної системи. Для Dom0 потрібне спеціальне ядро з

підтримкою XEN. Це ядро має деякі особливості, які дозволяють йому взаємодіяти з гіпервізором та ефективно керувати ресурсами.

Паравіртуалізовані гости в Dom0 вимагають гостьових систем з підтримкою PV. Це дозволяє оптимізувати взаємодію гіпервізора з гостьовими системами та підвищити продуктивність. Гостьова система повинна підтримувати PV. Це важливо для оптимізації взаємодії з гіпервізором та отримання максимальної продуктивності. Дистрибутиви Linux, які базуються на ядрах Linux, новіших за версію 3.0, зазвичай мають вбудовану підтримку для XEN. Ці дистрибутиви зазвичай включають гіпервізор та набір інструментів, що полегшує встановлення та конфігурацію. Усі ядра Linux, крім застарілих, старших за версію 2.6.24, повинні підтримувати XEN і здатні запускати гостьові системи з паравіртуалізацією.

1.4 Типи віртуалізацій XEN

Гіпервізор XEN підтримує паравіртуалізацію (PV) та повну віртуалізацію (HVM) та їх поєднання.

Паравіртуалізація представляє собою метод віртуалізації, який вперше з'явився у технології XEN та пізніше був використаний іншими віртуалізаційними платформами [7]. У порівнянні з іншими методами, PV не вимагає розширень віртуалізації від центрального процесора, що робить його ефективним для застосування на старішому обладнанні. Однак для оптимальної роботи паравіртуалізованих гостьових систем необхідно мати ядро з підтримкою PV та відповідні драйвери PV. Це дозволяє гостям взаємодіяти з гіпервізором без емуляції чи віртуального апаратного забезпечення, що сприяє їхній ефективності. Ядра з підтримкою PV доступні для операційних систем, таких як Linux, NetBSD і FreeBSD.

Система паравіртуалізації в XEN використовує два основних компонента для реалізації підтримки дисків та мережі: PV back-end та PV front-end драйвери [6]. Ця концепція сприяє високій продуктивності в порівнянні з повною віртуалізацією, оскільки гіпервізор та операційна система гостьової системи

співпрацюють більш ефективно, уникнувши накладних витрат, що виникають при емуляції ресурсів системи.

PV back-end компонент відповідає за забезпечення підтримки різних пристроїв, таких як диски, мережеві інтерфейси тощо. Він розташований на рівні Dom0 та надає інтерфейс для гостьових систем.

PV front-end компонент відповідає за надання підтримки пристроїв на рівні гостьової системи. Він взаємодіє з PV back-end та надає гостьовій системі зручний спосіб взаємодії з реальними або віртуальними пристроями.

Паравіртуалізація особливо корисна в області дисків та мережі, де використання мережі, драйверів шини та блокових пристроїв забезпечує близьку до реальної продуктивність. Це особливо стосується пристроїв, таких як блокові пристрої (диски), SCSI-пристрої та USB-пристрої. Паравіртуалізація дозволяє уникнути зайвих шарів емуляції та забезпечити ефективну роботу гостьових систем з реальним обладнанням.

Архітектурно паравіртуалізація функціонує, створюючи додаткові канали зв’язку між гіпервізором і гостьовими операційними системами за допомогою внутрішніх (back-end) та зовнішніх (front-end) драйверів PV (див. рисунок 1.4).

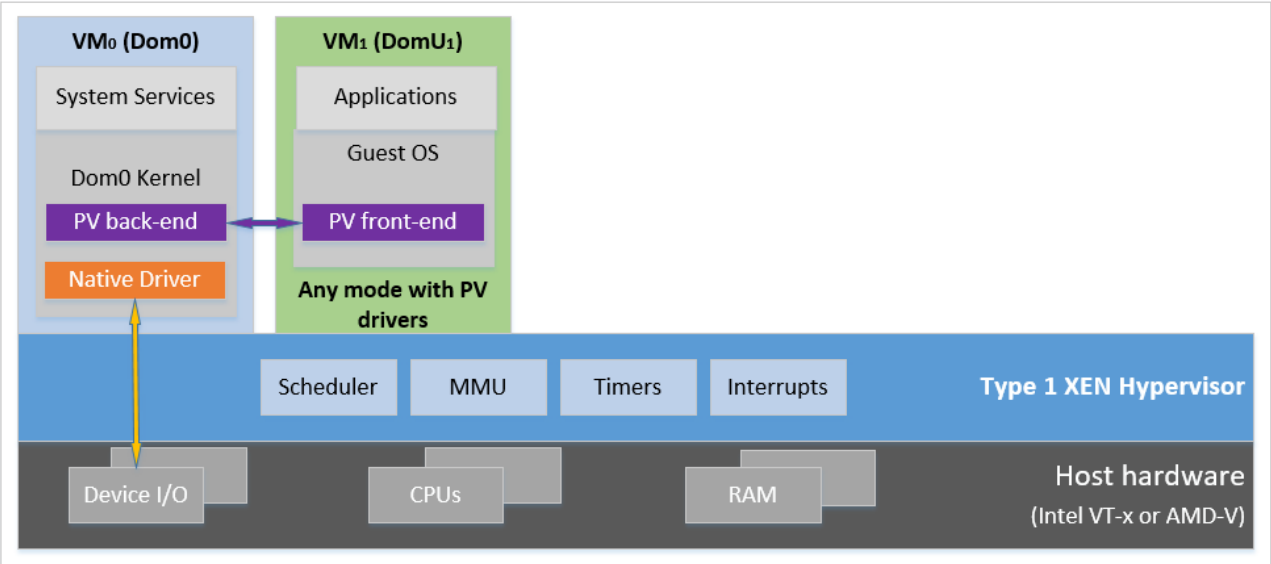

Рисунок 1.4 – Взаємодія драйверів апаратного забезпечення з системою PV та інтерфейсом PV

Паравіртуалізація представляє собою метод, що дозволяє продовжити використання застарілих та спеціалізованих програм, які підтримуються лише в старших операційних системах. Застосовуючи технологію віртуалізації XEN PV, можна запускати ці програми на новому, потужнішому та енергоефективному обладнанні.

Повна віртуалізація, також відома як апаратна віртуалізація (HVM), використовує розширення віртуалізації центрального процесора для створення віртуальних середовищ для гостьових систем. Для підтримки HVM необхідні апаратні розширення віртуалізації, такі як Intel VT або AMD-V.

Intel VT та AMD-V - це технології апаратної віртуалізації від Intel і AMD відповідно. Обидві ці технології розроблені для покращення ефективності та продуктивності віртуалізації на рівні апаратного забезпечення.

Програмне забезпечення XEN використовує QEMU для емуляції апаратного забезпечення ПК, включаючи BIOS, контролер диска IDE, графічний адаптер VGA, контролер USB, мережевий адаптер і т. д. Для підвищення продуктивності використовуються апаратні розширення віртуалізації.

У випадку повної віртуалізації, гостьові системи не вимагають модифікацій в їхньому ядрі, що дозволяє запускати операційні системи, такі як Windows, як гостьові системи XEN HVM. Цей підхід сприяє використанню різноманітних операційних систем у віртуальних середовищах.

У випадку старих операційних систем хоста, повністю віртуалізовані гостьові системи, зазвичай, працюють повільніше через необхідність емуляції. Для вирішення цього питання були розроблені драйвери PV та інтерфейси для операційних систем з відкритим кодом, таких як Linux. У системах з підтримкою XEN ці драйвери та програмні інтерфейси автоматично використовуються при виборі режиму віртуалізації HVM. Однак у Windows для використання цих переваг потрібно встановити відповідні драйвери PV.

Режим HVM, навіть з PV-драйверами, може бути неефективним у деяких аспектах. Наприклад, контролери переривань є однією з таких областей. У режимі HVM гостьовому ядру надаються емульовані контролери переривань (APIC та IOAPIC). Кожна інструкція, що взаємодіє з APIC, вимагає виклику XEN

і декодування програмної інструкції, і кожне доставлене переривання потребує кількох таких емуляцій.

Ідея створення режиму віртуалізації PVH (PVHVM) полягає в поєднанні переваг режимів PV і HVM та спрощенні інтерфейсу між операційними системами за допомогою гіпервізора XEN. Гості PVH представляють собою легкі гостьові системи HVM, які використовують підтримку апаратної віртуалізації для управління пам'яттю та привілейованими інструкціями, а також використовують драйвери PV для операцій введення-виведення та свої власні інтерфейси операційної системи для інших завдань. В PVH також відмовились від використання QEMU для емуляції пристроїв, хоча його можна використовувати для back-end модулів простору користувача.

Для використання режиму PVH необхідні гостьові системи з ядром Linux версії 4.11 або більш новою. Ця архітектура дозволяє отримати найкращі характеристики обох режимів віртуалізації, забезпечуючи високу продуктивність та ефективність використання ресурсів.

1.5 Віртуалізація процесів введення-виведення в XEN

Гіпервізор XEN підтримує три методи віртуалізації введення-виведення [6]. У PV split моделі, драйвер віртуального зовнішнього пристрою (front-end) взаємодіє з драйвером віртуального внутрішнього пристрою (back-end). Останній, у свою чергу, спілкується з фізичним пристроєм через власний (native) драйвер пристрою. Цей підхід дозволяє кільком віртуальним машинам використовувати один і той самий апаратний ресурс, використовуючи власну апаратну підтримку. У типовій конфігурації XEN, драйвери пристроїв та драйвери віртуальних внутрішніх пристроїв знаходяться в Dom0. Xen дозволяє запускати драйвери пристроїв у так званих доменах драйверів. Метод віртуалізації введення-виведення на основі PV є основним для дисків та мережі, але також існує безліч драйверів PV для сенсорного екрану, аудіо тощо, призначених для несерверного використання Xen. Ця модель не залежить від

режиму віртуалізації, який використовує Xen, і вимагає лише наявності відповідних драйверів. Драйвери постачаються разом з Linux і BSD за замовчуванням, а для Windows їх слід завантажити та встановити в гостьову операційну систему.

У Xen існують два варіанти моделі драйвера PV split. У першому варіанті зовнішній драйвер PV безпосередньо взаємодіє з внутрішнім драйвером PV в ядрі Dom0. Ця модель передбачає в основному використання для простої мережі та віртуалізації сховища за допомогою LVM, iSCSI та інших технологій (див.рисунок 1.4).

У другій моделі back-end простору користувача QEMU використовує інтерпретацію відформатованих даних файлу (наприклад, qcow2, vmdk, vdi) і надає необроблений дисковий інтерфейс для своєї власної back-end реалізації PV (див.рисунок 1.5).

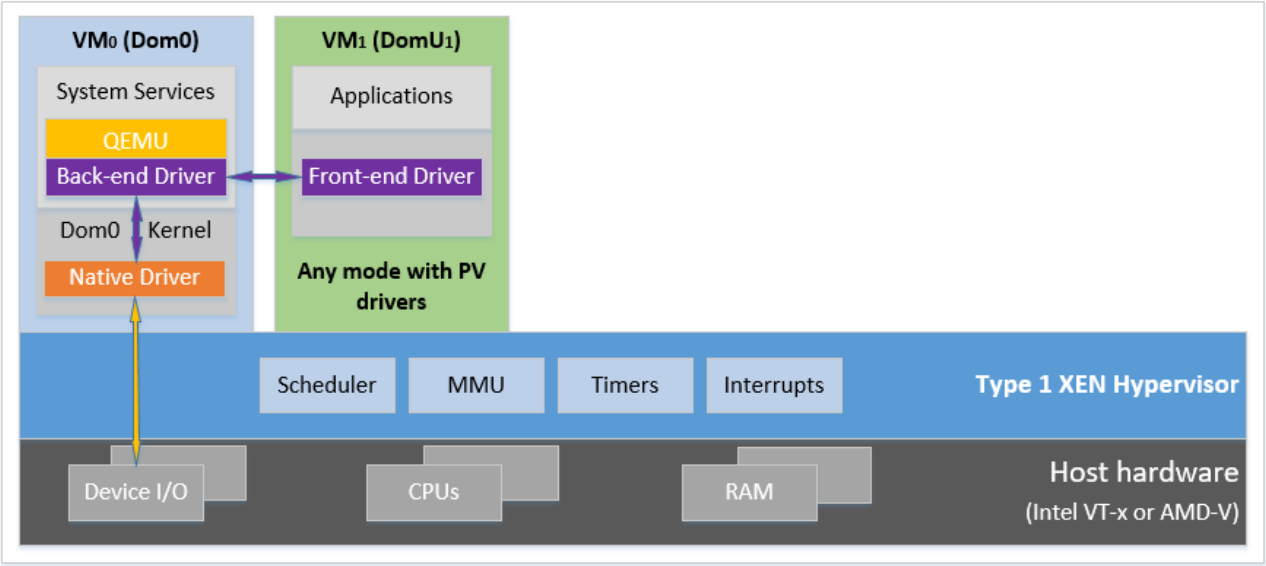

Рисунок 1.5 – Взаємодія драйверів апаратного забезпечення з системою PV та інтерфейсом PV через QEMU

З погляду користувача або гостя, відсутня видима різниця у тому, чи працює back-end драйвер у просторі користувача чи в ядрі. XEN автоматично обирає відповідну комбінацію front-end і back-end драйверів на основі параметрів конфігурації, які використовуються.

У реалізації введення-виведення на основі емуляції пристроїв гості HVM емулюють апаратні пристрої в програмному забезпеченні. У випадку XEN, для емуляції пристроїв використовується QEMU як емулятор пристрою. Завдяки високим накладним витратам на продуктивність, емуляція на основі пристрою зазвичай використовується лише під час завантаження системи, її інсталяції або для пристроїв із обмеженою пропускною здатністю.

На рисунку 1.6 демонструється використання емуляції пристрою як самостійного методу та його комбінація із підтримкою PV введення-виведення.

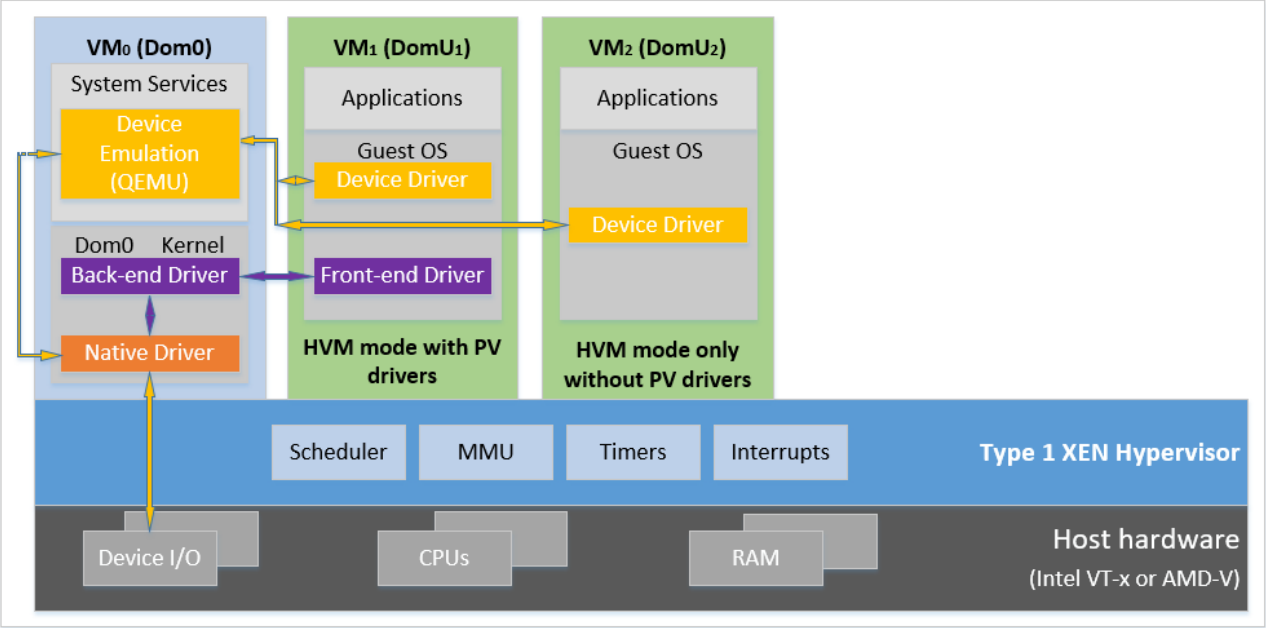

Рисунок 1.6 – Емуляція пристрою окремо та разом із підтримкою PV I/O

Ця можливість надається лише для віртуальних машин HVM та в основному використовується для емуляції застарілих пристроїв, необхідних під час завантаження гостьової системи. Також вона застосовується для пристроїв з низькою пропускною здатністю, наприклад, послідовної консолі для гостей HVM.

Наскрізний доступ (Passthrough) в XEN дозволяє передавати керування фізичними пристроями гостям. Це означає що можна використовувати PCI passthrough для призначення пристрою PCI (такого як мережева карта, контролер диска, USB-контролер, FireWire-контролер, аудіокарта тощо) гостьовій віртуальні машини, надаючи їй повний і безпосередній доступ до цього

пристрою PCI. XEN підтримує різні типи наскрізного доступу PCI, включаючи passthrough VT-d і SR-IOV. Важливо враховувати, що використання passthrough може мати негативний вплив на безпеку системи.

У гіпервізорі XEN система зберігання інформації, або storage, грає ключову роль у забезпеченні ефективності та надійності віртуалізованого середовища. XEN підтримує різні формати образів дисків, такі як raw, qcow2, vhd, і інші. Кожен з цих форматів має свої особливості і можливості. Гіпервізор підтримує концепцію сховища (storage repository), де можна зберігати образи віртуальних машин, що полегшує управління та резервне копіювання. XEN може використовувати LVM для зберігання віртуальних та динамічно розширюваних дисків віртуальних машин. Використання LVM дозволяє розділити фізичний диск на кілька логічних блоків, які можуть бути використані віртуальними машинами. Це дозволяє зберігати образи дисків гостей у файлах на локальній файловій системі. XEN також підтримує протоколи iSCSI та NFS для взаємодії зі зберіганням, що розташовано в мережі.

Гіпервізор XEN надає гнучкість та широкі можливості для конфігурації системи зберігання, дозволяючи адміністраторам оптимально використовувати ресурси та забезпечувати високий рівень доступності та надійності віртуалізованих середовищ.

1.6 Висновки до розділу

В першому розділі було проведено огляд принципів віртуалізації. Здійснено огляд гіпервізора типу 1 XEN. Описано переваги мікроядерної архітектури гіпервізора XEN в забезпечення високого рівня стабільності та безпеки віртуалізованого середовища. Також було описано архітектурні особливості гіпервізора XEN. Було показано, що простота та компактність коду гіпервізора XEN роблять його економічним та ефективним рішенням для забезпечення надійності та безпеки системи віртуалізації. Гіпервізор XEN демонструє високий рівень безпеки та ізоляції завдяки ізоляції гостьових віртуальних машин від апаратного забезпечення. Було проаналізовано типи віртуалізації і показано що

режим віртуалізації PHV, який полягає в поєднанні переваг паравіртуалізації і апаратної віртуалізація Intel VT або AMD-V є оптимальним рішенням в контексті забезпечення швидкодії, надійності та безпеки. Також було описано механізм віртуалізації процесів введення-виведення в гіпервізорі XEN.

РОЗДІЛ 2 ЗАСОБИ СТВОРЕННЯ ЛАБОРАТОРНОГО СЕРЕДОВИЩА ВІРТУАЛІЗОВАНОЇ ІТ-ІНФРАСТРУКТУРИ

2.1 Розробка схеми лабораторного середовища

На рисунку 2.1 представлено схему лабораторного середовища віртуалізованої інфраструктури на основі XCP-ng, що є варіантом гіпервізора XEN [8].

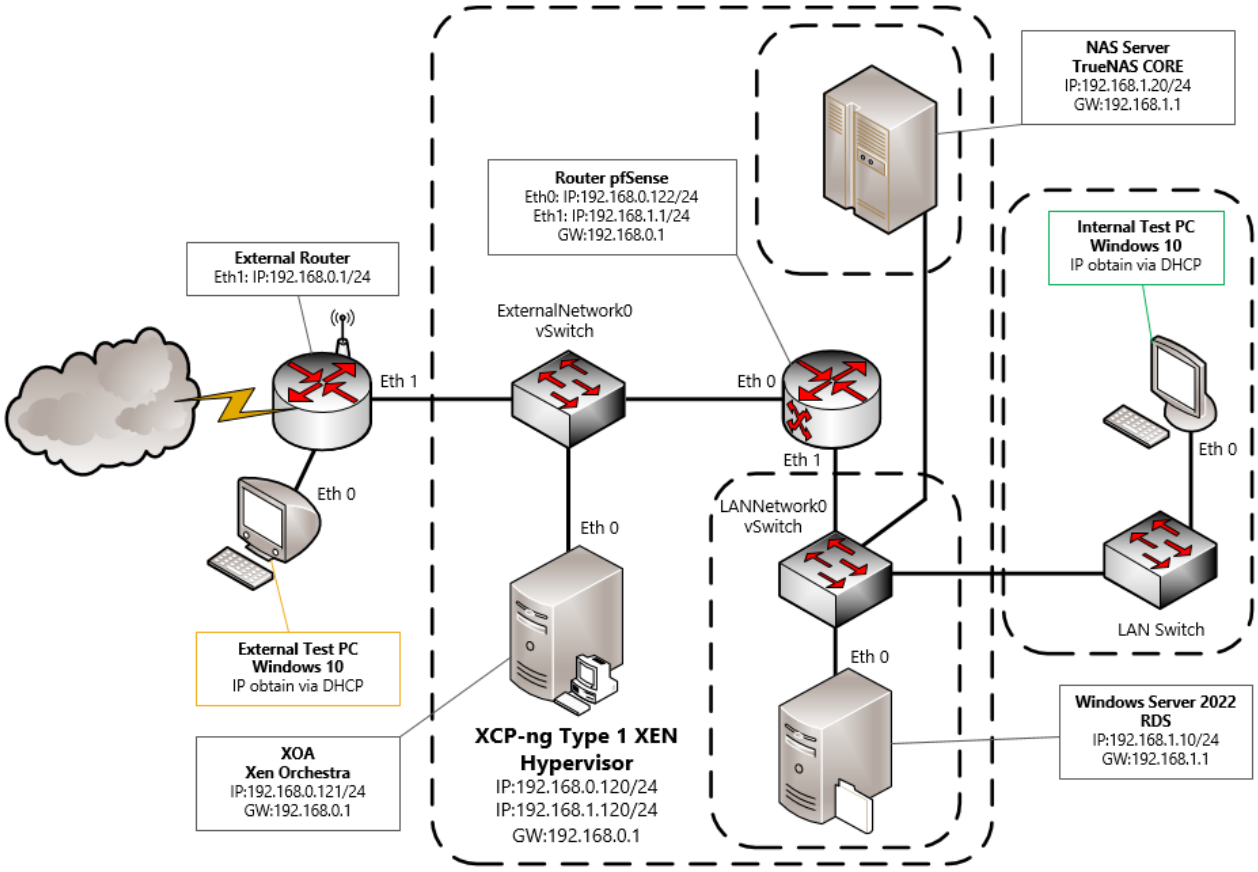

Рисунок 2.1 – Схема лабораторного середовища віртуалізованої інфраструктури

На схемі зображено різні компоненти мережі та їх взаємозв'язки. Основним елементом тестового середовища є гіпервізор типу 1 XEN XCP-ng. Інтерфейси для керування гіпервізором мають IP-адреси 192.168.0.120/24 та 192.168.1.120/24 для можливості управління гіпервізором через LANNetwork0 та ExternalNetwork0 віртуальні комутатори.

Xen Orchestra є вебінтерфейсом управління для XCP-ng та представляє собою окрему віртуальну операційну систему на базі Debian Linux з IP-адресою 192.168.0.121/24 та шлюзом за замовчуванням 192.168.0.1.

Віртуальний маршрутизатор pfSense виконує функції брандмауера та маршрутизатора між віртуальними мережами на основі ExternalNetwork0 та LANNetwork0 комутаторів. Також він має IP-адреси 192.168.0.122/24 та 192.168.1.1/24 відповідні до віртуальних мереж.

NAS Сервер (TrueNAS CORE) представляє собою сервер зберігання, який використовується для зберігання даних користувачі локальної мережі. Сервер під'єднаний до LANNetwork0 віртуального комутатора та має IP-адресу 192.168.1.20/24 з шлюзом за замовчуванням 192.168.1.1.

Windows Server 2022 з IP-адресою 192.168.1.10/24, шлюзом 192.168.1.1, також під'єднаний до LANNetwork0 віртуального комутатора та виконує функції RDS сервера в локальній мережі.

Тестові ПК InternalTestPC та ExternalTestPC з операційною системою Windows10 будуть використані для тестування віртуалізованої IT-інфраструктури з зовнішньої та внутрішньої мережі.

2.2 Платформа віртуалізації XCP-ng

XCP-ng є вільною та відкритою платформою віртуалізації, спроектованою на основі гіпервізора XEN [8]. Ця сучасна ітерація, яка є наступником XCP, розробляється спільнотою та підтримує відкриті технологічні стандарти. XCP-ng надає можливості для створення та управління віртуальними машинами, використовуючи гіпервізор XEN. Основні функціональності включають управління віртуальними дисками, міграцію віртуальних машин, а також контроль ресурсів, що дозволяє оптимально використовувати віртуалізоване середовище.

Однією з важливих переваг XCP-ng є її відкритість та доступність безкоштовно. Це робить платформу привабливою для користувачів, які шукають ефективне та масштабоване рішення в галузі віртуалізації. XCP-ng здатний

задовольнити потреби як великих обчислювальних центрів, так і хмарних сервісів, забезпечуючи широкі можливості управління віртуалізованим інфраструктурним середовищем.

2.2.1 Загальна архітектура

Архітектура XCP-ng включає компоненти та взаємодії між ними, що забезпечують функціональні можливості системи віртуалізації [8]. XCP-ng складається з декількох ключових компонентів, які доповнюють та розширюють функціонал гіпервізора XEN (див.рисунок 2.2).

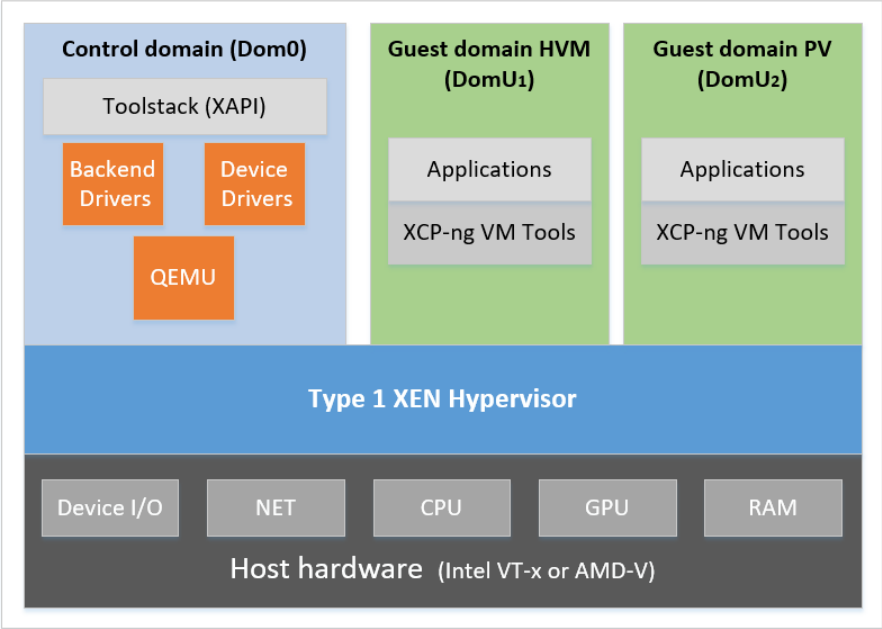

Рисунок 2.2 – Загальна архітектура XCP-ng

На апаратному рівні розташовані компоненти сервера, такі як процесор, оперативна пам'ять, мережеві інтерфейси та пристрої зберігання. Для ефективної роботи системи віртуалізації необхідне обладнання із підтримкою 64-розрядної архітектури та технологій Intel VT або AMD-V на базі x86 з одним чи кількома процесорами, щоб запустити різні операційні системи віртуальних машин.

Гіпервізор XCP-ng, який базується на гіпервізорі XEN, розширює його можливості та функціонал завдяки додатковим функціям і підтримці, що

надаються проектом XCP-ng. У версії XCP-ng 8.2 LTS використовується гіпервізор XEN версії 4.13.4.

Контрольний домен, також відомий як domain0 або dom0, представляє собою безпечну та привілейовану віртуальну машину на основі Linux, яка запускає набір інструментів управління XCP-ng, відомих як XAPI. Ця віртуальна машина побудована на базі дистрибутиву CentOS 7.5. Окрім своєї основної ролі управління XCP-ng, dom0 також відповідає за запуск драйверів фізичних пристроїв, які обслуговують мережу, зберігання та інші аспекти системи. Керуючий домен може взаємодіяти з гіпервізором, передаючи йому команди для запуску або зупинення гостьових віртуальних машин.

XAPI або TS - це програмний стек, який відповідає за управління операціями життєвого циклу віртуальної машини, мережі хоста та віртуальної машини, сховищем віртуальної машини та автентифікацією користувачів. Він також забезпечує можливість керування пулами ресурсів XCP-ng. XAPI надає документований API керування, який використовується різними інструментами для управління віртуальними машинами та пулами ресурсів.

Гостьові домени (domU) - це віртуальні машини, які створюються користувачами і запитують ресурси від контрольного домену (dom0).

Інструменти XCP-ng VM Tools надають високопродуктивні служби введення-виведення без накладних витрат, характерних для традиційної емуляції пристроїв. Ці інструменти складаються з драйверів введення-виведення (драйвери PV) і агента керування.

Драйвери введення-виведення включають інтерфейсне сховище та мережеві драйвери, а також низькорівневі інтерфейси керування. Ці драйвери замінюють емульовані пристрої, забезпечуючи швидкий транспорт між віртуальними машинами та програмним забезпеченням XCP-ng.

Агент керування (гостьовий агент) відповідає за функції високорівневого управління віртуальною машиною. Він надає повну функціональність XCP-ng Center для керування віртуальними машинами під управлінням операційної системи Windows.

Щоб забезпечити повністю підтримувану конфігурацію віртуальної машини під управлінням Windows, обов'язково потрібно встановити інструменти XCP-ng VM Tools. Вони повинні бути налаштовані на кожній віртуальній машині Windows. Хоча віртуальна машина може функціонувати і без XCP-ng VM Tools, проте без встановлених драйверів введення-виведення продуктивність значно знизиться.

Інструменти XCP-ng VM Tools для Linux включають гостьовий агент, який надає додаткову інформацію про віртуальну машину хосту. Також необхідно встановити гостьовий агент на кожній віртуальній машині Linux для активації динамічного управління пам'яттю (DMC).

2.2.2 Управління хостами

Управління хостами XCP-ng може здійснюватися різними методами, в залежності від потреб та вибору адміністратора.

Для одного хоста або невеликого пулу (кластера) XCP-ng, адміністратори можуть використовувати різні інструменти для управління та моніторингу.

Є можливість використовувати наступні інструменти:

- xeCLI є командним рядком інтерфейсу, який дозволяє адміністраторам виконувати команди для управління хостами та віртуальними машинами.

- XO Lite є легким веб-клієнтом для управління XCP-ng. Забезпечує базові функції моніторингу та управління через зручний веб-інтерфейс.

- Xen API надає програмний інтерфейс для взаємодії з гіпервізором XCP-ng через мережу. Дозволяє створювати власні програми або інтегрувати існуючі системи з XCP-ng.

- XCP-ng Center - це графічний клієнт для Windows, який дозволяє адміністраторам легко керувати пулами хостів та віртуальними машинами. Надає розширені функції моніторингу та управління.

Керувати декількома хостами або пулами зручніше через єдиний центральний оркестратор. Такі можливості надає Xen Orchestra [9].

Адміністратори можуть користуватися різними інтерфейсами для зручного та ефективного управління своєю інфраструктурою.

Є можливість використовувати наступні інструменти Xen Orchestra:

- Xen Orchestra Web Interface - це вебінтерфейс, який надає графічний спосіб управління та моніторингу інфраструктури XCP-ng. Має інтуїтивно зрозумілий інтерфейс для здійснення різних операцій, таких як створення та керування віртуальними машинами, налаштування резервних копій, моніторинг ресурсів і багато іншого.

- Xen Orchestra CLI - надає командний рядок для автоматизації завдань та взаємодії з Xen Orchestra через командний рядок.

- API Xen Orchestra API REST та JSON-RPC для взаємодії з інфраструктурою через програмний інтерфейс. Це дозволяє адміністраторам створювати власні скрипти, інтегрувати Xen Orchestra з іншими системами та автоматизувати багато задач.

Xen Orchestra робить управління та моніторинг XCP-ng більш доступним та зручним, забезпечуючи широкий спектр функціональностей через різні інтерфейси.

Вибір конкретного методу управління може залежати від індивідуальних вподобань, рівня зручності та завдань, які потрібно виконати.

2.2.3 Репозиторій зберігання

Зберігання в XCP-ng представлене як репозиторії зберігання (SR). Кожен SR містить образи віртуальних дисків (VDI), що включають в себе вміст віртуального диска. Ці репозиторії зберігання адаптивні та підтримують різні типи дисків, такі як SATA, SCSI, NVMe і SAS, які можуть бути локально підключені, а також віддалено через протоколи iSCSI, NFS, SAS, SMB і Fibre Channel. Концепція VDI служить абстракцією для зображення віртуального жорсткого диска (див.рисунок 2.3).

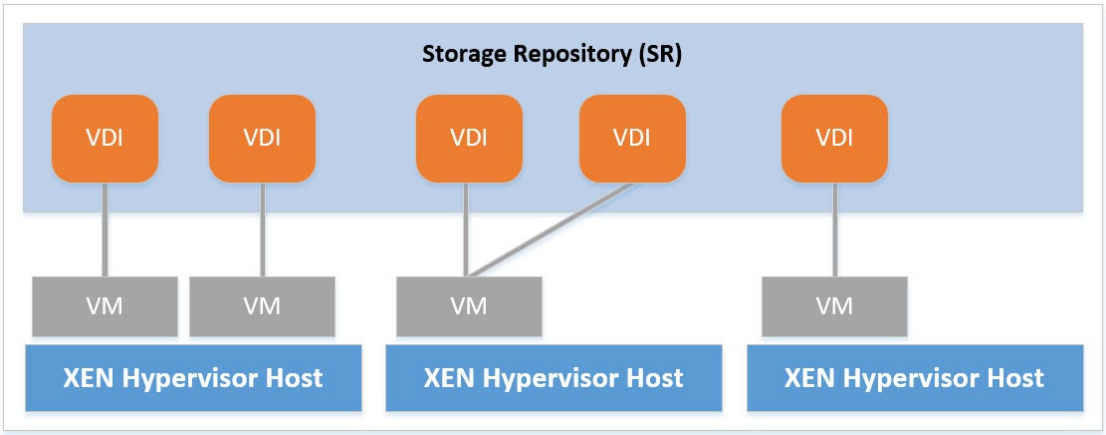

Рисунок 2.3 – Репозиторій для зберігання в XCP-ng

Абстракції SR та VDI дозволяють використовувати розширені можливості зберігання, такі як thin provisioning, створення знімків VDI та швидке клонування, які підтримуються цими абстракціями.

Thin provisioning (тонкий розподіл ресурсів) - це метод управління сховищем даних, що дозволяє оптимізувати та ефективно використовувати доступне дисковий простір у віртуалізованих середовищах або мережах зберігання даних. Використання тонкого розподілу ресурсів полягає в призначенні дискового простору для віртуальних машин на запит, замість фіксованого виділення повного обсягу дискового простору заздалегідь.

Традиційно, при створенні віртуального диска, потрібно було виділити фіксований обсяг дискового простору, який відразу ставав недоступним для інших задач, навіть якщо він фактично не використовувався. З використанням тонкого розподілу ресурсів система автоматично призначає дисковий простір в міру його використання. Це означає, що якщо ви створите віртуальний диск розміром 100 ГБ, але використовуєте лише 10 ГБ, то додаткові 90 ГБ залишатимуться доступними для інших процесів або віртуальних машин до тих пір, поки вони фактично не будуть використані. Тонке розподілення ресурсів дозволяє збільшити ефективність використання дискового простору.

Для підсистем зберігання даних, які не підтримують ці розширені операції безпосередньо в XCP-ng, надається програмний стек, що реалізує ці функції, і базується на специфікації Microsoft VHD.

Кожен хост XCP-ng може використовувати одночасно кілька SR різних типів. Ці SR можуть бути спільно використані між хостами або визначені для конкретних хостів. Спільне сховище об'єднує кілька хостів у визначений пул ресурсів. Щоб бути доступним кожному хосту в пулі, спільний SR повинен бути доступний через мережу. XCP-ng дозволяє управляти декількома серверами та їх підключеними спільними сховищами як єдиним цілим за допомогою пулів ресурсів. Пули ресурсів дозволяють переміщувати та запускати віртуальні машини на різних хостах XCP-ng. Також, вони дозволяють усім серверам використовувати загальну структуру для мережі та зберігання. Усі хости в одному пулі ресурсів повинні мати принаймні один спільний SR. Спільне сховище не можна спільно використовувати між декількома пулами.

2.2.4 Мережева архітектура

Мережева архітектура XCP-ng грає ключову роль у вирішенні питань комунікації між віртуальними машинами, хостами та іншими компонентами інфраструктури віртуалізації.

XCP-ng використовує Open vSwitch як основу для управління мережею та підтримує різні його функції [8]. Використання vSwitch спрощує завдання IT-адміністрування в віртуалізованих мережевих середовищах. Усі налаштування та статистика віртуальної машини залишаються зв'язаними з нею, навіть під час міграції віртуальної машини з одного фізичного хоста в пулі ресурсів на інший.

Під час установки XCP-ng автоматично створює окрему мережу для кожної фізичної мережевої карти. При додаванні сервера до пулу, ці мережі за замовчуванням об'єднуються. Це здійснюється для того, щоб всі фізичні мережеві карти з однаковою назвою пристрою мали доступ до однієї об'єднаної мережі.

В XCP-ng доступні три основні типи мереж: Зовнішні мережі (External networks), Об'єднані мережі (Bonded networks) та приватні мережі на одному сервером (Single-Server Private networks).

Зовнішні мережі забезпечують зв'язок між віртуальною машиною та фізичним мережевим інтерфейсом, який підключений до мережі. Дозволяють віртуальній машині з'єднуватися з ресурсами, доступними через фізичний мережевий адаптер сервера.

Об'єднані мережі створюють зв'язок між двома чи більше мережевими адаптерами для створення єдиного високопродуктивного каналу між віртуальною машиною та мережею. Забезпечують високу продуктивність та надійність, об'єднуючи ресурси кількох адаптерів.

Приватні мережі на одному сервером не пов'язані з фізичним мережевим інтерфейсом. Використовуються для забезпечення з'єднання між віртуальними машинами на конкретному хості, не маючи підключення до зовнішнього середовища.

Ці типи мереж дозволяють адміністраторам гнучко конфігурувати мережеві зв'язки віртуальних машин у XCP-ng залежно від конкретних потреб та вимог системи.

В архітектурі XCP-ng існують три типи програмних об'єктів для представлення мережевих структур на рівні сервера. Ці об'єкти включають PIF, VIF та Network (див.рисунок 2.4).

PIF представляє фізичну мережеву карту на хості та використовується в dom0. Має ім'я, опис, UUID, параметри фізичної мережевої карти та пов'язану мережу та сервер.

VIF представляє віртуальну мережеву карту на віртуальній машині та використовується в dom0. Має ім'я, опис, UUID та пов'язану мережу та віртуальну машину.

Network представляє віртуальний комутатор Ethernet на хості, який використовується для маршрутизації мережевого трафіку. Має ім'я, опис, UUID та пов'язаний набір VIF і PIF об'єктів.

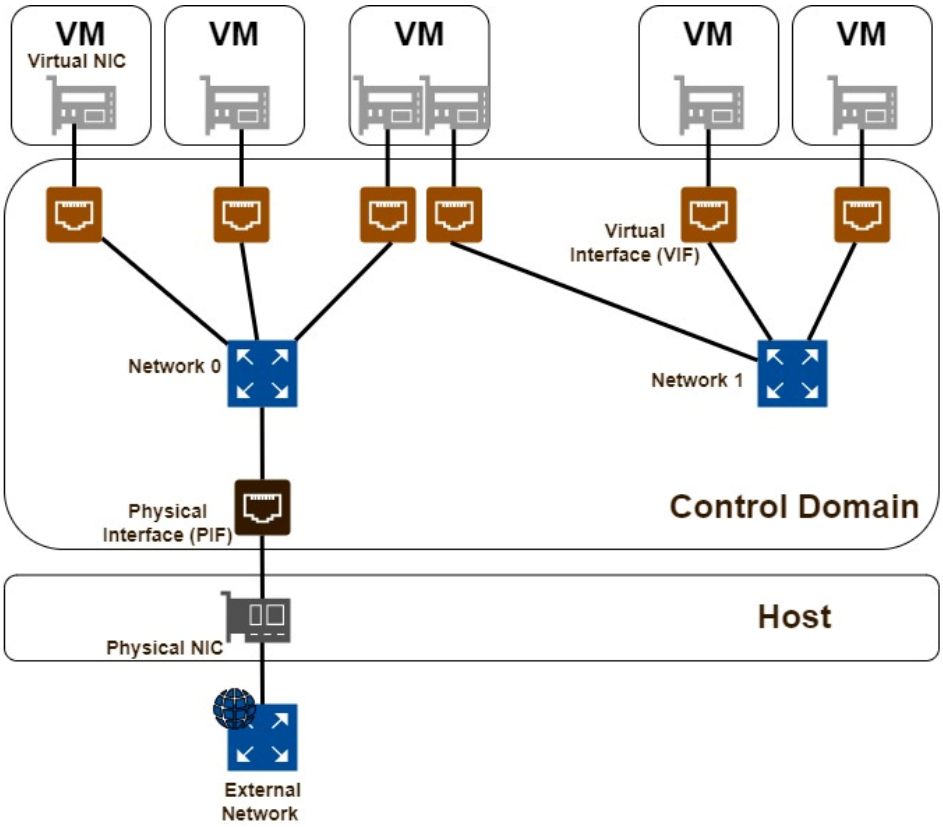

Рисунок 2.4 – Архітектура мережі в XCP-ng

Інструменти, такі як Xen Orchestra, xeCLI та XCP-ng Center, дозволяють налаштовувати параметри мережі. Можна встановлювати мережеві адаптери для операцій керування та створювати розширені мережеві функції, наприклад, VLAN.

2.3 Встановлення та налаштування XCP-ng

Встановлення та налаштування XCP-ng включає кілька етапів, від встановлення гіпервізора до конфігурації мережі та сховищ. Оскільки XCP-ng розроблено основі операційної системи Linux CentOS 7.5 етапи встановлення є простими та зрозумілими [8].

На рисунку 2.5 показано консоль керування XCP-ng, яка дає можливість налаштувати базові параметри гіпервізора одразу після встановлення.

Рисунок 2.5 – Консоль керування XCP-ng

Об’єкти сервера XCP-ng та список параметрів управління версіями і їх значення можна подивитись за допомогою стандартної команди (див.рисунок 2.6).

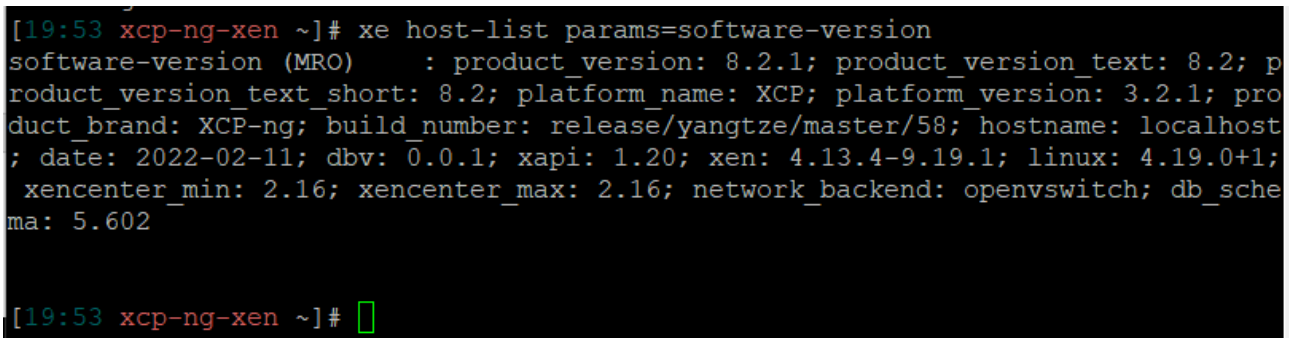

Рисунок 2.6 – Встановлені версії програмного забезпечення платформи XCP-ng

На першому етапі налаштування XCP-ng будемо здійснювати за допомогою XCP-ng Center. На рисунку 2.7 показано налаштування мережі в XCP-ng.

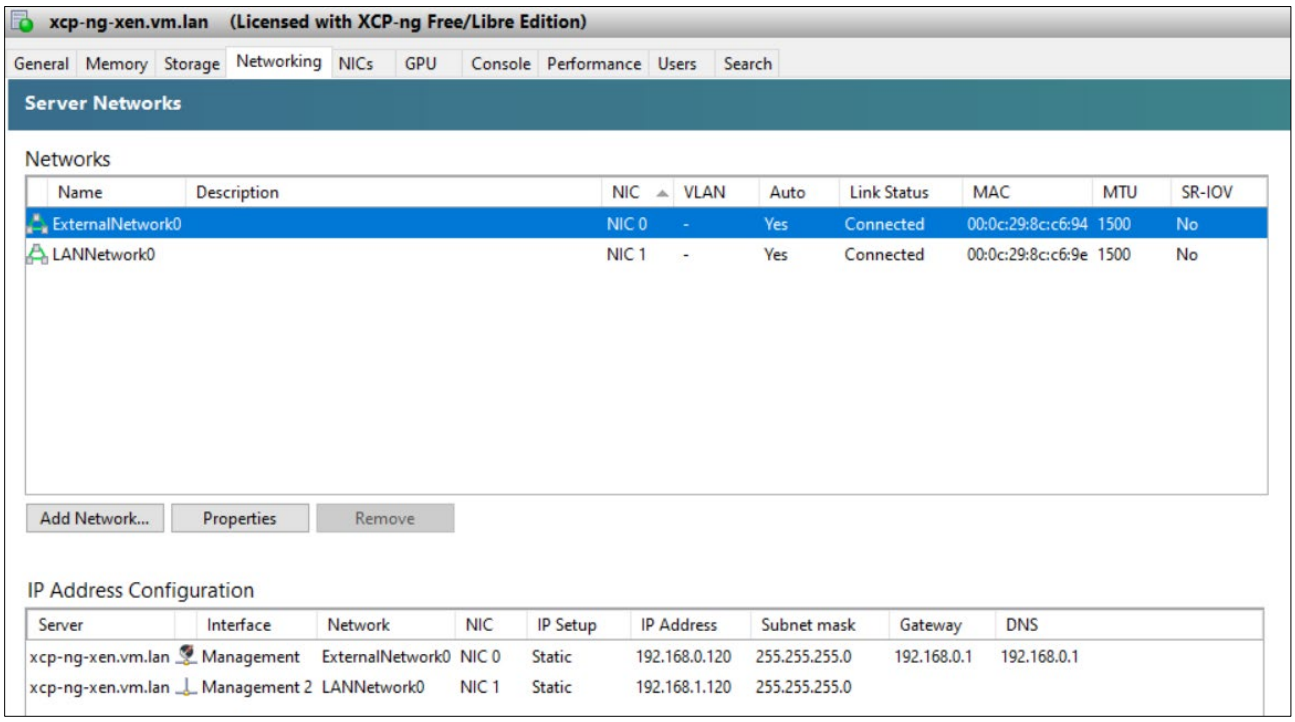

Рисунок 2.7 – Налаштування мережі в XCP-ng Center

Після попереднього налаштування XCP-ng встановимо Xen Orchestra. Xen Orchestra - це віртуальна машина, яка встановлюється в XCP-ng (див.рисунок 2.8).

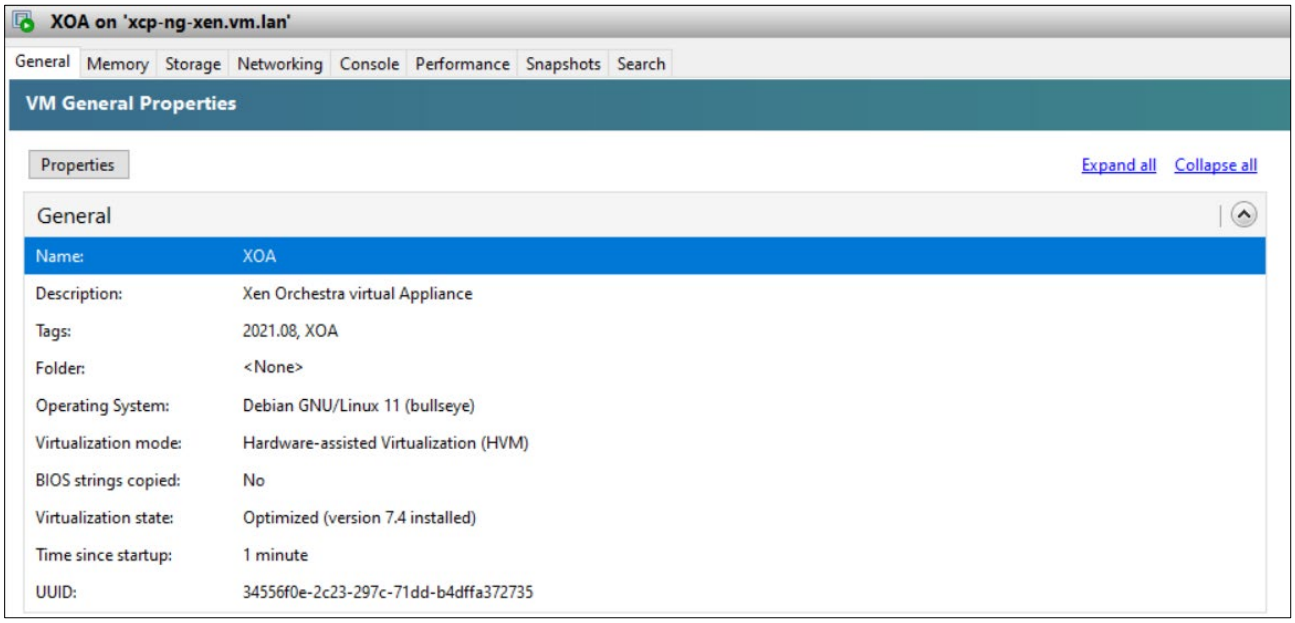

Рисунок 2.8 – Віртуальна машина Xen Orchestra в XCP-ng

Xen Orchestra надає користувачам зручний інтерфейс для віртуалізації та управління віртуальними машинами та ресурсами хоста. За допомогою Xen Orchestra можна створювати, редагувати, запускати та зупиняти віртуальні машини, а також переглядати статистику та проводити моніторинг ресурсів, таких як CPU, пам'ять, мережа.

На рисунку 2.9 показано вебінтерфейс керування Xen Orchestra.

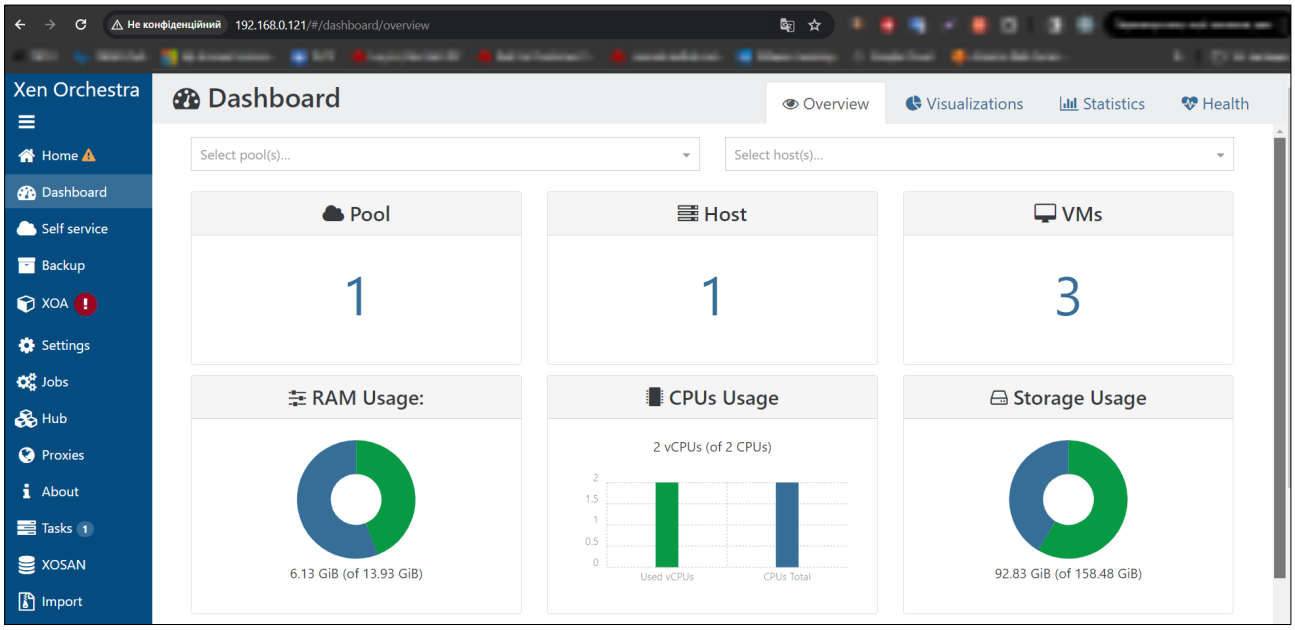

Рисунок 2.9 – Вебінтерфейс керування Xen Orchestra

Xen Orchestra використовує операційну систему Debian Linux для свого функціонування та надання віртуальних інфраструктурних можливостей. Xen Orchestra підтримує керування багатьма серверами XCP-ng одночасно.

2.4 Висновки до розділу

У другому розділі була розроблена структура лабораторного тестового середовища для створення віртуалізованої IT-інфраструктури, використовуючи віртуалізаційну платформу XCP-ng, яка є варіантом гіпервізора XEN.

Встановлено та налаштовано XCP-ng. Описано можливості та архітектуру XCP-ng з окремим акцентом на засобах зберігання та мережевих функціях.

Показано можливості управління хостами XCP-ng за допомогою XCP-ng Center, xeCLI та Xen Orchestra.

РОЗДІЛ 3 ВСТАНОВЛЕННЯ, НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ВІРТУАЛІЗОВАНОЇ ІТ-ІНФРАСТРУКТУРИ

Проведемо розгортання, налаштування та перевірку коректності роботи віртуалізованої ІТ-інфраструктури відповідно до схеми представленої на рисунку 2.1.

3.1 Розгортання та налаштування брандмауера pfSense

Проект pfSense - це безкоштовний дистрибутив, заснований на FreeBSD з відкритим вихідним кодом [10]. Він розроблений як брандмауер і маршрутизатор, та повністю керується через веб-інтерфейс. pfSense пропонує потужну та гнучку платформу для забезпечення безпеки мережі та маршрутизації. Зокрема, він включає різноманітні функції, а пакетна система дозволяє легко розширювати його можливості. pfSense використовується в різних середовищах, від домашніх мереж до корпоративних інфраструктур.

Програмне забезпечення pfSense з’явилось як відгалуження від проекту з відкритим вихідним кодом m0n0wall у 2004 році. Початково m0n0wall був спрямований на створення брандмауера та маршрутизатора для вбудованих пристроїв і був орієнтований на обмежені апаратні ресурси. У свою чергу, pfSense почав розвиватися як рішення для брандмауера та маршрутизатора з розширеним функціоналом на більших комп'ютерах і серверного обладнання. Протягом тривалого періоду часу pfSense надає широкий спектр можливостей, включаючи брандмауер, маршрутизатор, VPN, IDS/IPS та інші функції, і успішно використовується на різних рівнях апаратного забезпечення - від невеликих домашніх пристроїв до потужних серверів великих постачальників послуг.

Походження назви pfSense звязоно з початковим гаслом проекту "making sense of pf", що вказує на технологію фільтрації пакетів PF, яка є основою цього проекту. PF в FreeBSD здатний виконувати базові завдання фільтрації пакетів та впроваджувати брандмауер, QoS аналогічно до функціоналу, який надає pfSense. Проте pfSense робить керування, моніторинг і підтримку значно простішими. Це

досягається завдяки інтуїтивно зрозумілому графічному інтерфейсу користувача та налаштованим службам, які опосередковано взаємодіють з операційною системою та відповідними пакетами. Такий підхід формує повноцінне рішення для брандмауера, маршрутизатора та VPN, здатне виконувати набагато більше, ніж сума базових компонентів в FreeBSD.

pfSense забезпечує повнофункціональний брандмауер, який може контролювати рух даних на рівні мережі. Також він може використовуватися як маршрутизатор для ефективного направлення мережевого трафіку. Маршрутизатор pfSense підтримує різні протоколи VPN, включаючи IPsec, L2TP і OpenVPN. Це дозволяє створювати безпечні з'єднання між різними розташованими географічно мережами або забезпечувати безпечний доступ до мережі віддалених користувачів. pfSense має вбудовані засоби захисту від вторгнень (IDS/IPS), які виявляють та блокують потенційно шкідливий мережевий трафік.

Платформа підтримує балансування навантаження для різних WAN-з'єднань, щоб забезпечити ефективне використання доступних мережевих ресурсів. pfSense може використовуватися як прозорий проксі-сервер для фільтрації вебтрафіку і забезпечення безпеки під час використання Інтернету.

На рисунку 3.1 показано загальні налаштування віртуальної машини pfSense в Xen Orchestra.

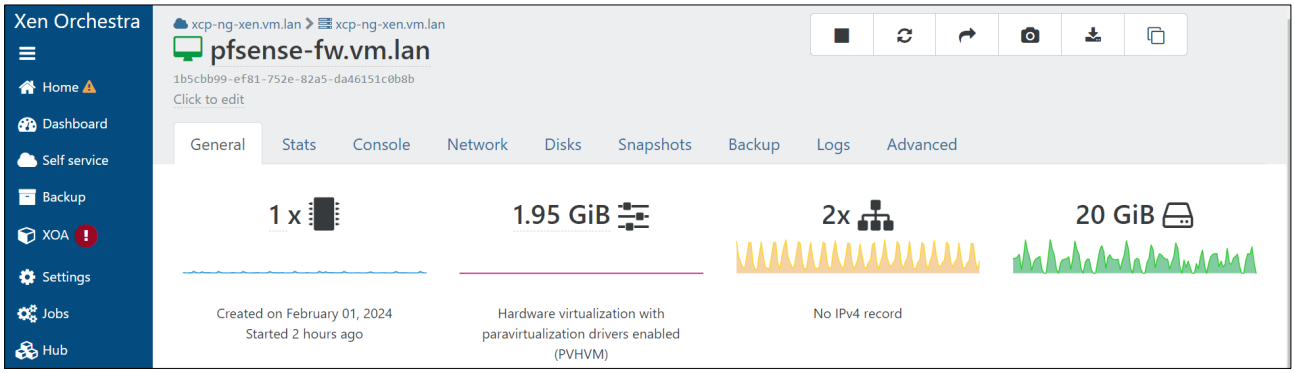

Рисунок 3.1 – Загальні налаштування віртуальної машини pfSense

На рисунку 3.2 показано налаштування мережі віртуальної машини pfSense.

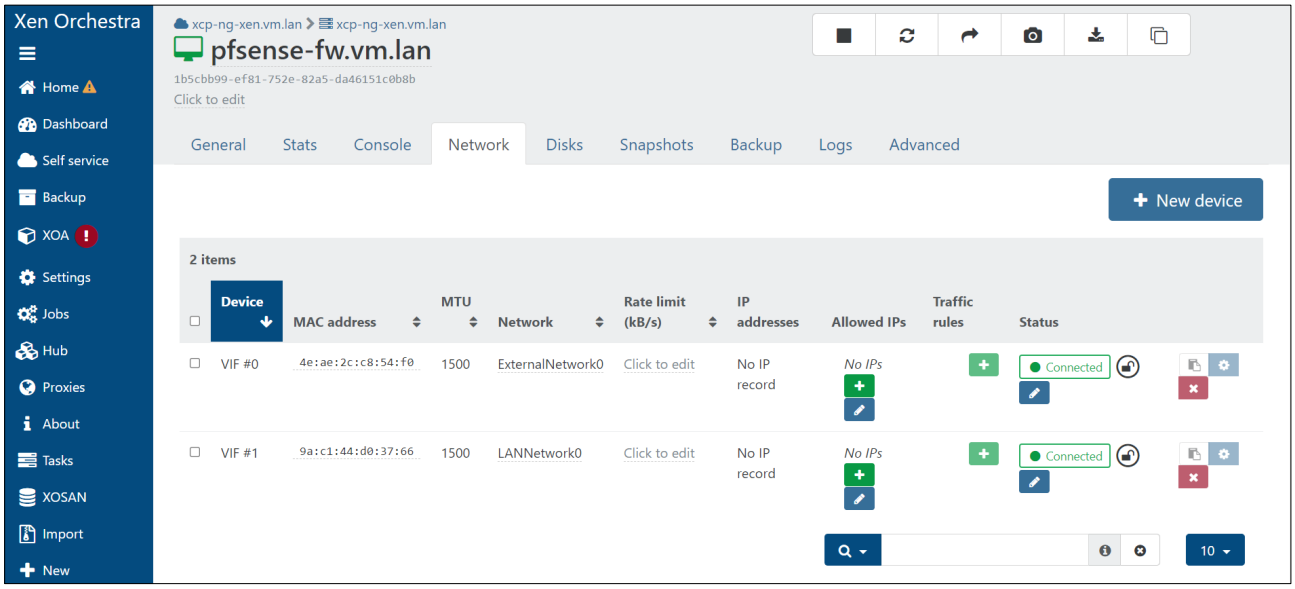

Рисунок 3.2 – Налаштування мережі віртуальної машини pfSense

Після встановлення віртуального маршрутизатора pfSense можна здійснити його початкові налаштування за допомогою інтерфейсу консолі (див. рисунок 3.3).

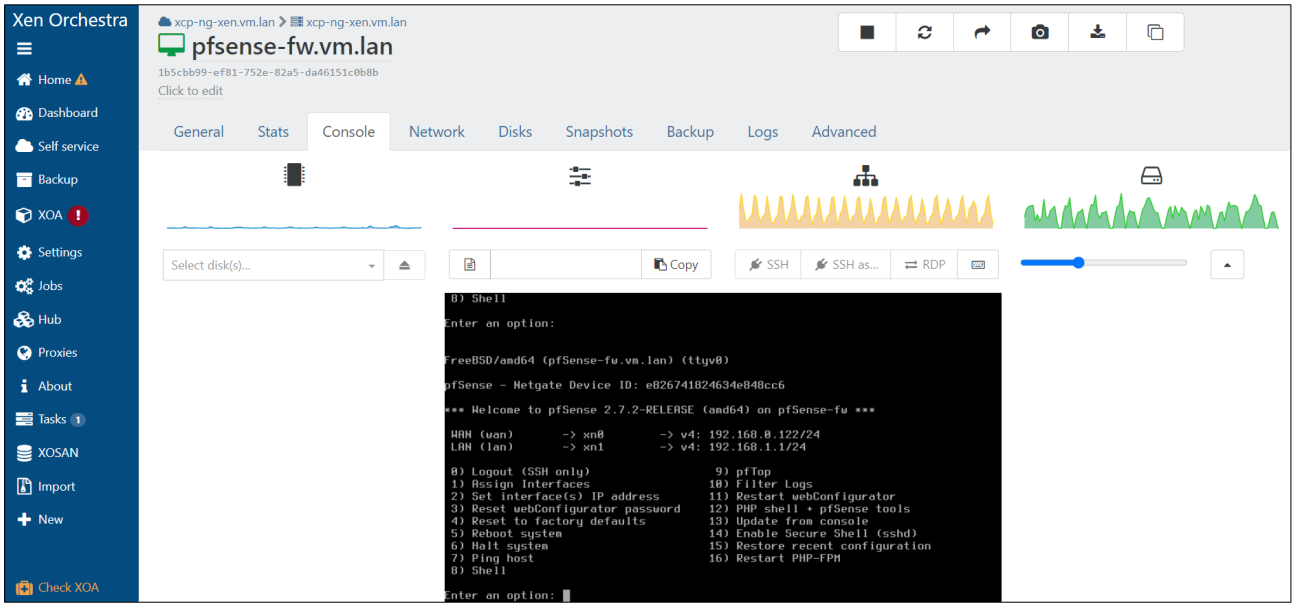

Рисунок 3.3 – Консоль віртуальної машини pfSense

Після встановлення та першого етапу налаштування мережі в pfSense потрібно виконати налаштувань DHCP сервера, брандмауера, NAT та L2TP/IPsec VPN сервера за допомогою вебінтерфейсу керування pfSense (див. рисунок 3.4).

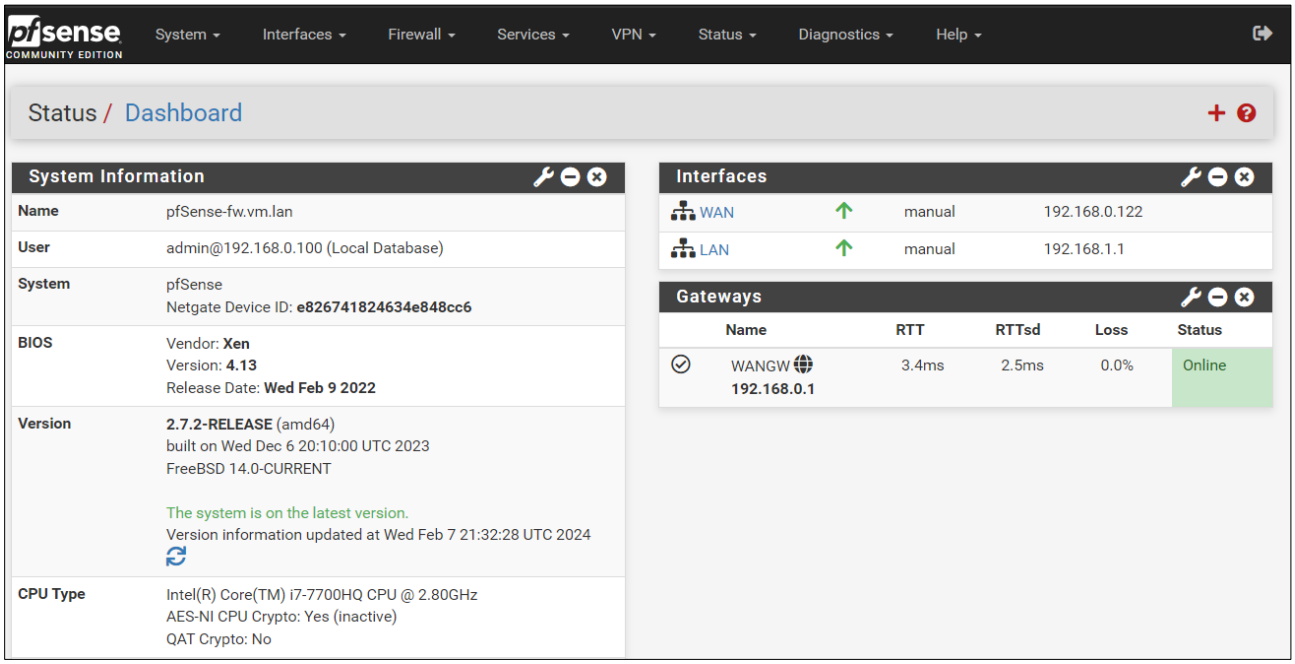

Рисунок 3.4 – Вебінтерфейс керування pfSense

На рисунку 3.5 показано інтерфейс налаштувань DHCP сервера в pfSense [11].

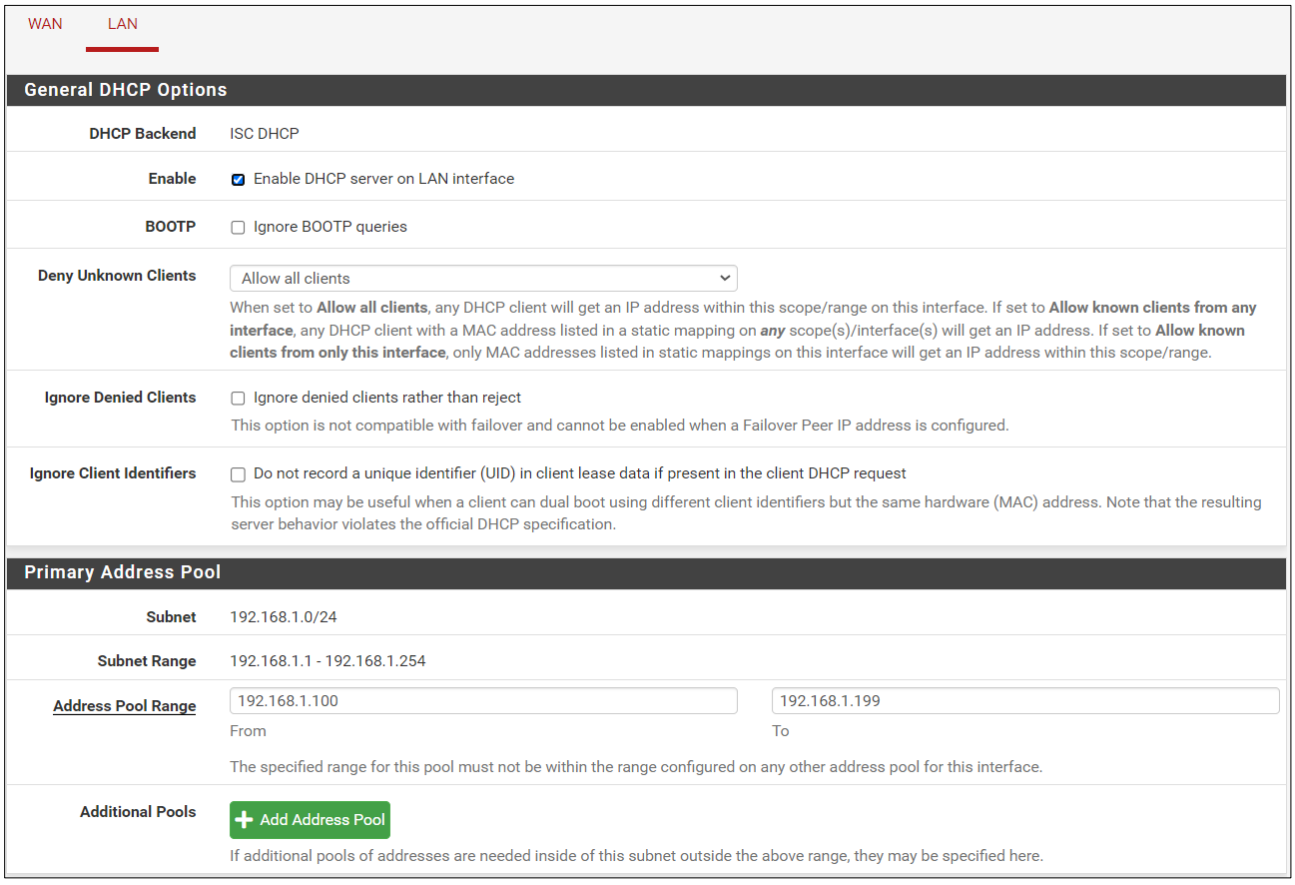

Рисунок 3.5 – Інтерфейс налаштувань DHCP сервера в pfSense

Вказано, що використовується ISC DHCP на LAN інтерфейсі. pfSense виконує роль DHCP сервера для локальної мережі, надаючи IP адреси від 192.168.1.100 до 192.168.1.199 для клієнтів, які підключаються до мережі зі шлюзом та DNS сервером з IP-адресою 192.168.1.1 за замовчуванням.

На рисунку 3.6 представлені налаштування VPN сервера для протоколу L2TP в pfSense [12].

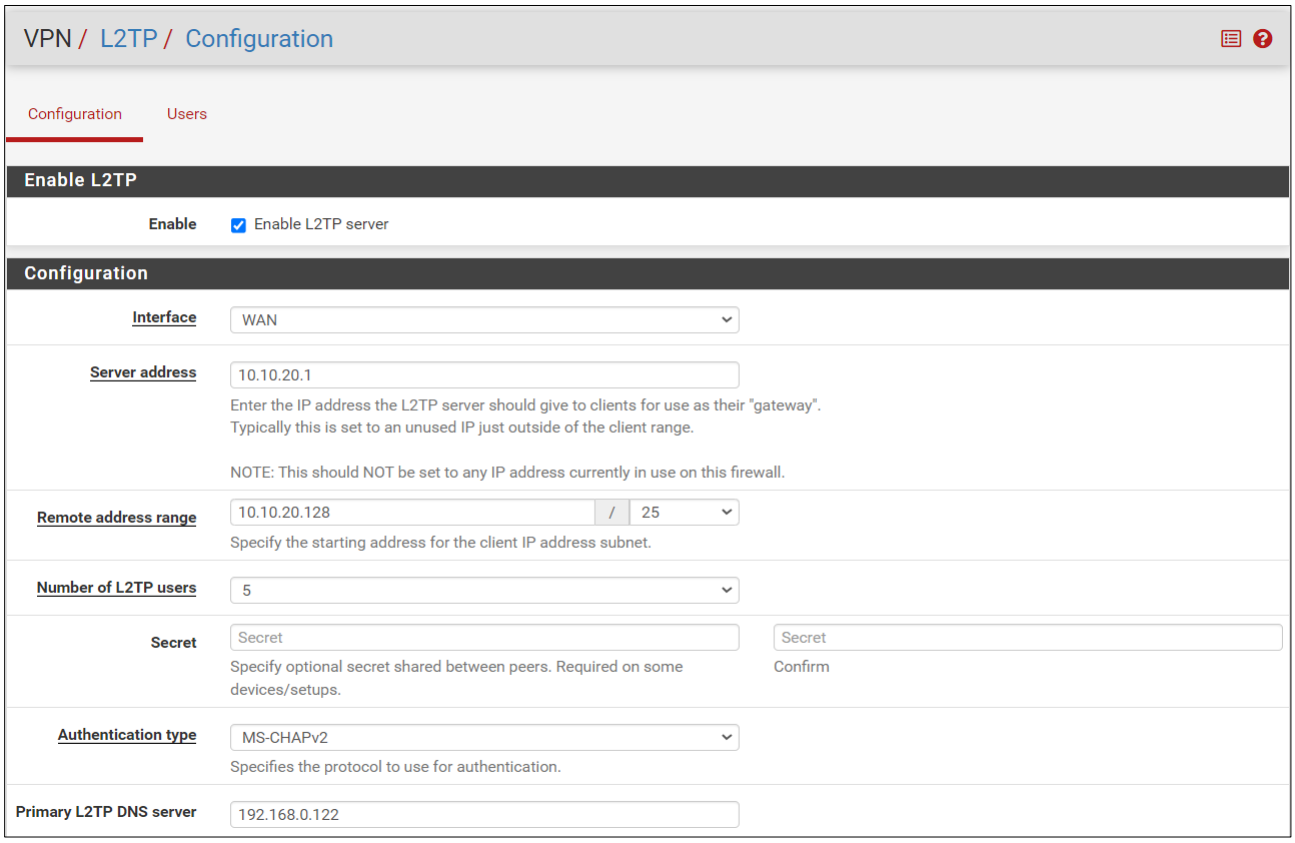

Рисунок 3.6 – Налаштування VPN сервера L2TP в pfSense

L2TP сервер буде прослуховувати з'єднання на інтерфейсі WAN. В Server address встановлено IP-адресу сервера 10.10.20.1, яка служитиме як шлюз для VPN клієнтів L2TP. Клієнтам будуть надаватися IP-адреси з діапазону 10.10.20.128/25. Дозволено одночасний доступ для 5 VPN користувачів.

Вибрано MS-CHAPv2, який є протоколом автентифікації. Та основний L2TP DNS сервер з IP-адресою 192.168.0.122.

На рисунку 3.7 показано параметри налаштувань для тунелів VPN з використанням протоколу IPsec в pfSense.

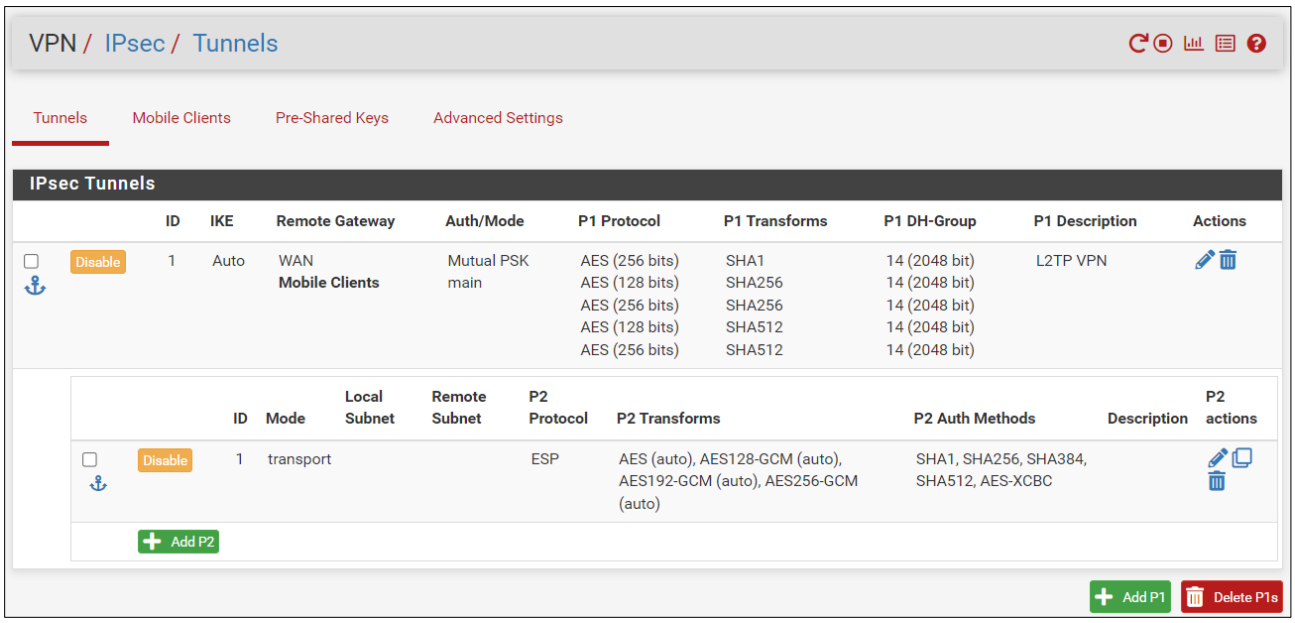

Рисунок 3.7 – Параметри налаштувань для тунелів VPN з використанням протоколу IPsec

В Remote Gateway вказано віддалений шлюз WAN інтерфейс, для якого налаштовується тунель. Режим автентифікації встановлено в Mutual PSK, що означає взаємний Pre-Shared Key. Pre-Shared Key - це рядок, відомий обом вузлам, який використовується як ключ для автентифікації тунелю, подібний до пароля. Цей ключ чутливий до регістру та має бути точно однаковим на обох кінцевих точках.

Можливі алгоритми шифрування для фази 1 AES-256 або AES-128 та хешування SHA1, SHA256, SHA512. Алгоритми хешування використовуються з IPsec для перевірки автентичності пакетних даних. Група Diffie-Hellman для фази 1 - 14 (2048 bit). IPsec використовує групу DH для першого дочірнього SA під час початкового будівництва тунелю.

Параметри фази 2 для тунелю IPsec визначають, як тунель обробляє трафік, а також шифрування цього трафіку. Режим transport вказує нате що шифрується весь трафік між кінцевими точками. Локальна мережа та віддалена мережа не встановлені для транспортного режиму, адреси базуються на налаштуваннях фази 1.

Протокол для фази 2 контролює, як IPsec захищає свій трафік. ESP шифрує трафік перед тим, як відправити його пристрою. Набір алгоритмів шифрування для фази 2 (AES (auto), AES128-GCM (auto), AES256-GCM (auto)) використовуються під час узгодження дочірніх записів SA фази 2 з пірами [13]. Методи автентифікації для фази 2 (SHA1, SHA256, SHA384, SHA512, AES-XCBC) контролює, які хеш-алгоритми використовуються під час узгодження дочірніх записів SA фази 2 з пірами.

Ці налаштування використовуються для створення захищеного з'єднання між клієнтом та корпоративною мережею.

На рисунку 3.8 відображено розділ правил мережевого екрана для LAN в інтерфейсі pfSense [14].

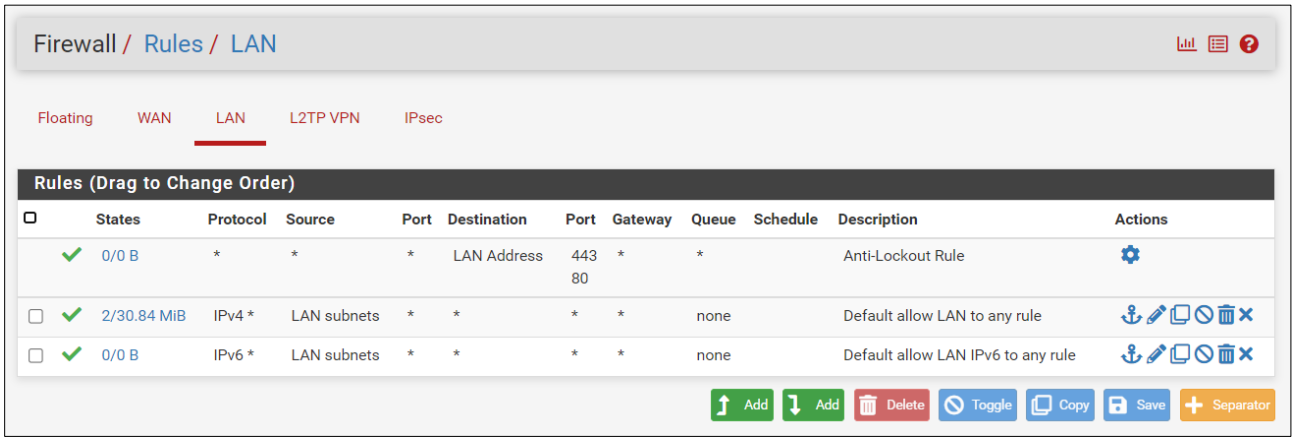

Рисунок 3.8 – Розділ правил мережевого екрана для локальної мережі

Ці правила визначають що мережевий трафік з LAN сегменту дозволено до будь-якого сегменту.

Для мережі WAN встановлено автоматичне правило заборони будь-яких з’єднань з зовні мережі. Правило заборонити все є правилом за замовчуванням для брандмауера pfSense. Це правило не відображається в наборі правил.

На рисунку 3.9 відображено правила для L2TP VPN маршрутизатора pfSense.

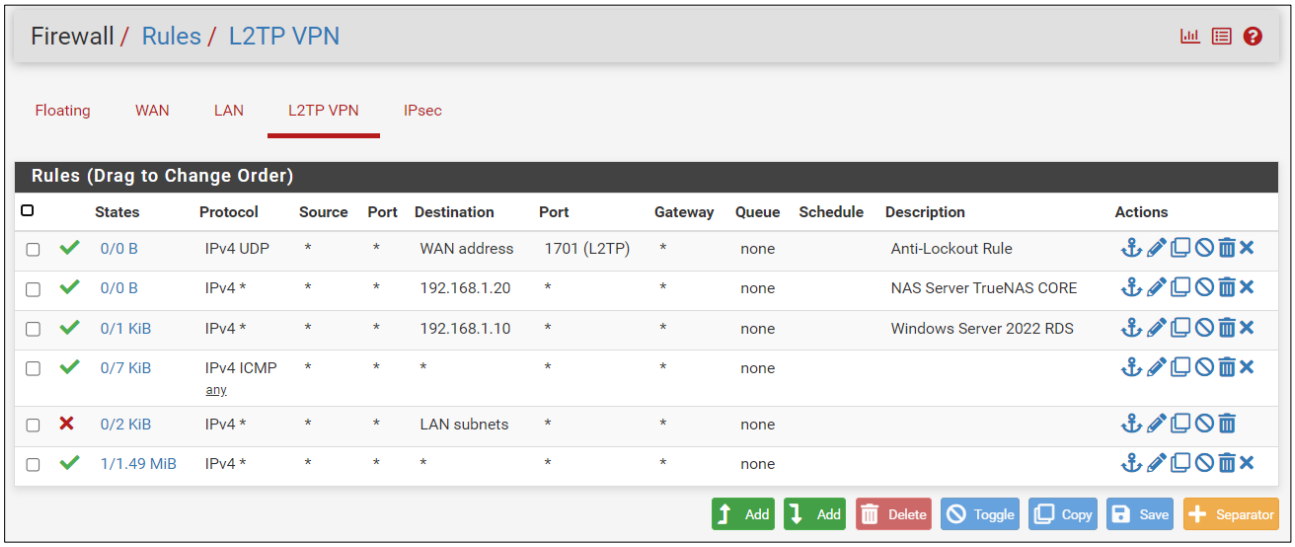

Рисунок 3.9 – Розділ правил брандмауера для L2TP VPN з’єднання

Правило проти блокування дозволяє IPv4 UDP трафік з будь-якої мережі до WAN адреси на порт 1701, який є стандартним портом для L2TP. Також дозволені з’єднання до двох локальних IP-адрес NAS Server TrueNAS CORE та Windows Server 2022 RDS. Дозволено протокол ICMP та заборонено доступ до решту LAN мережі. Останнє правило дозволяє клієнтам VPN доступ до будь-яких інших мереж включно з Інтернет.

На рисунку 3.10 зображено інтерфейс налаштувань брандмауера, конкретно вкладку NAT для вихідного трафіку [15].

Використовується автоматичне створення правил NAT в режимі Automatic outbound NAT rule generation (IPsec passthrough included). Автоматично генеровані правила включають NAT для локальної мережі 192.168.1.0/24 та для клієнтів L2TP/IPsec VPN.

DNS Resolver в програмному забезпеченні pfSense використовує unbound - рекурсивний, кешуючий DNS, який підтримує DNSSEC, DNS через TLS та має широкі можливості налаштувань. Resolver може функціонувати як DNS resolver або forwarder. У режимі resolver (за замовчуванням) DNS Resolver взаємодіє безпосередньо з кореневими DNS-серверами та іншими авторитетними серверами для пошуку відповідей на запити, відправлені клієнтами. Це усуває проблеми, пов'язані з неправильною локальною конфігурацією DNS.

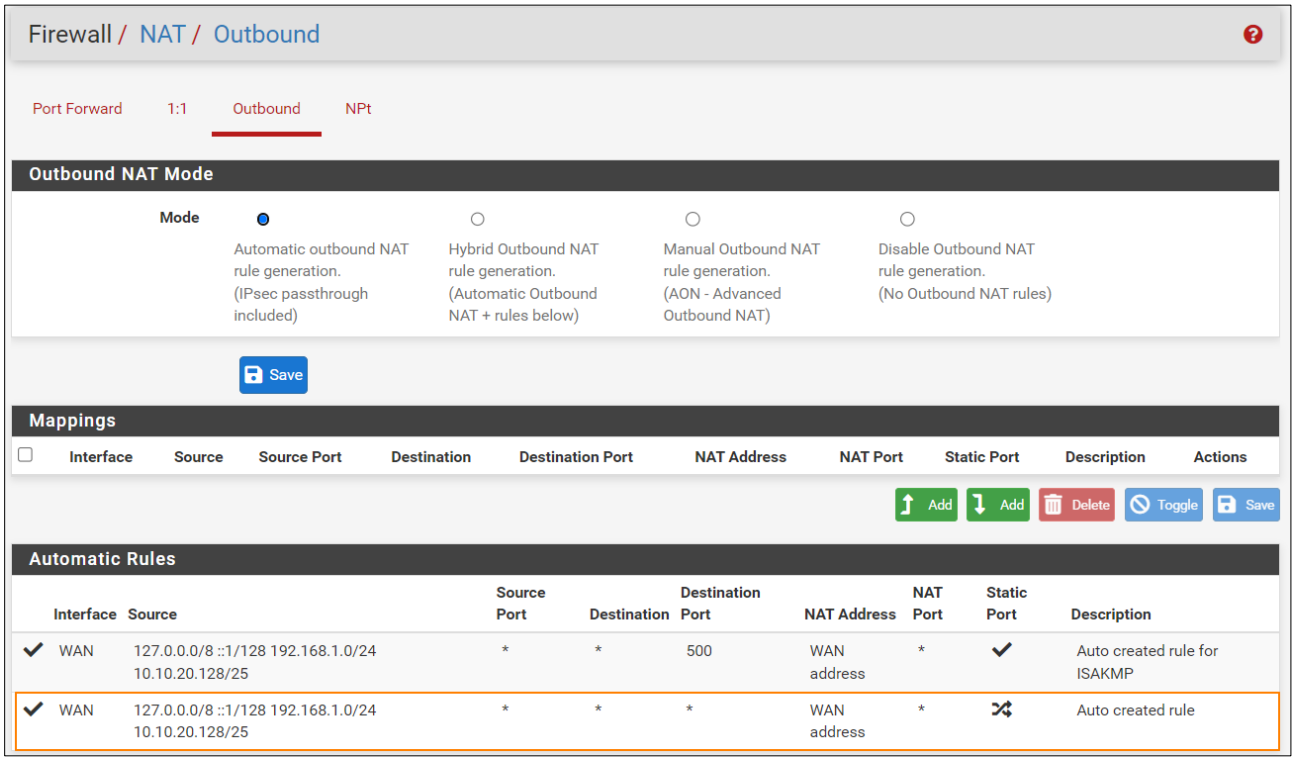

Рисунок 3.10 – Розділ правил NAT

Режим resolver також дозволяє використовувати розширення безпеки системи доменних імен (DNSSEC), що підвищує надійність та перевірку результатів DNS. Для розробленої схеми IT-інфраструктури було використано DNS в режимі роботи resolver з параметрами налаштування за замовчуванням.

3.2 Розгортання та налаштування NAS TrueNAS CORE

TrueNAS – це відкрита платформа для зберігання даних, яка базується на операційній системі FreeBSD [16]. Розроблена і підтримується компанією iXsystems. TrueNAS надає можливості мережевого зберігання (NAS) і є відомою своєю надійністю, продуктивністю та гнучкістю.

Однією з ключових особливостей TrueNAS є використання файлової системи ZFS, яка забезпечує високий рівень надійності, відновлення даних. TrueNAS підтримує різні протоколи доступу до даних, такі як SMB, NFS, AFP та iSCSI, і може використовуватися в різноманітних сценаріях, включаючи підприємства, освіту та домашній сектор.

Застосування шифрування для кореневого набору даних у новому пулі зберігання додає додатковий шар захисту для інформації. Всі набори даних, які додаються до цього зашифрованого пулу, автоматично успадковують його шифрування.

На рисунку 3.11 показано загальні налаштування віртуальної машини TrueNAS CORE в Xen Orchestra.

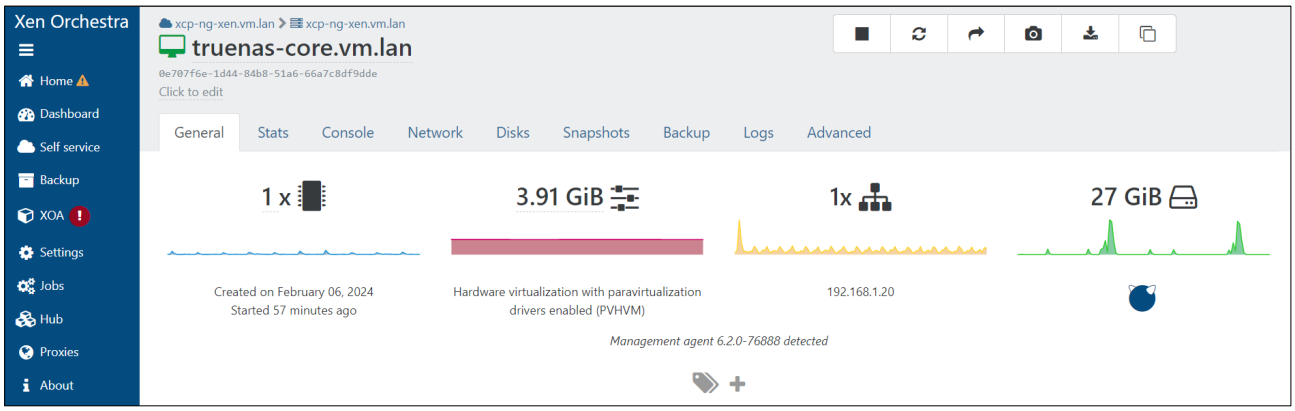

Рисунок 3.11 – Загальні налаштування віртуальної машини TrueNAS

На рисунку 3.12 показано налаштування мережі віртуальної машини TrueNAS.

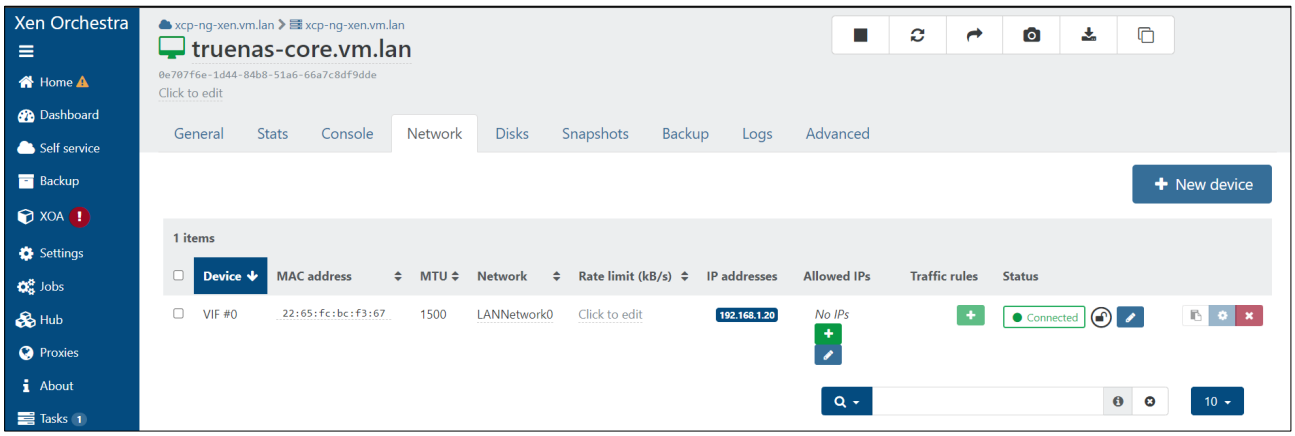

Рисунок 3.12 – Налаштування мережі віртуальної машини TrueNAS

Після встановлення TrueNAS потрібно здійснити його початкові налаштування за допомогою простого інтерфейсу консолі (див. рисунок 3.13).

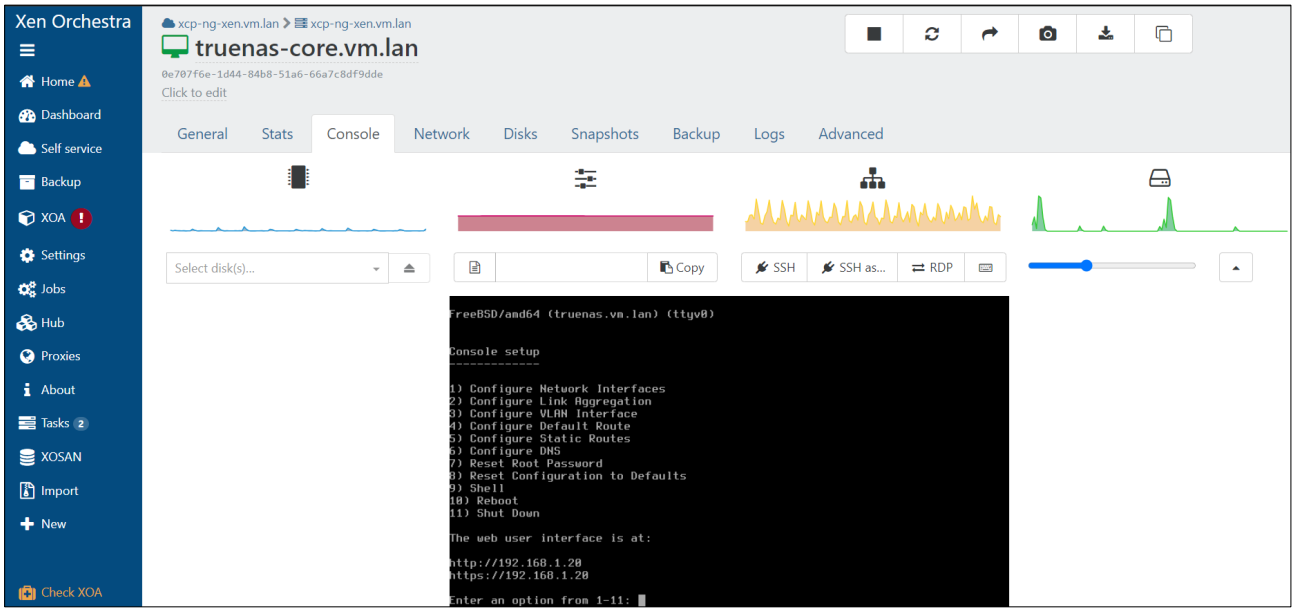

Рисунок 3.13 – Консоль віртуальної машини TrueNAS

На рисунку 3.14 показано вебінтерфейс TrueNAS CORE, який буде використано для налаштувань пулів зберігання та SMB.

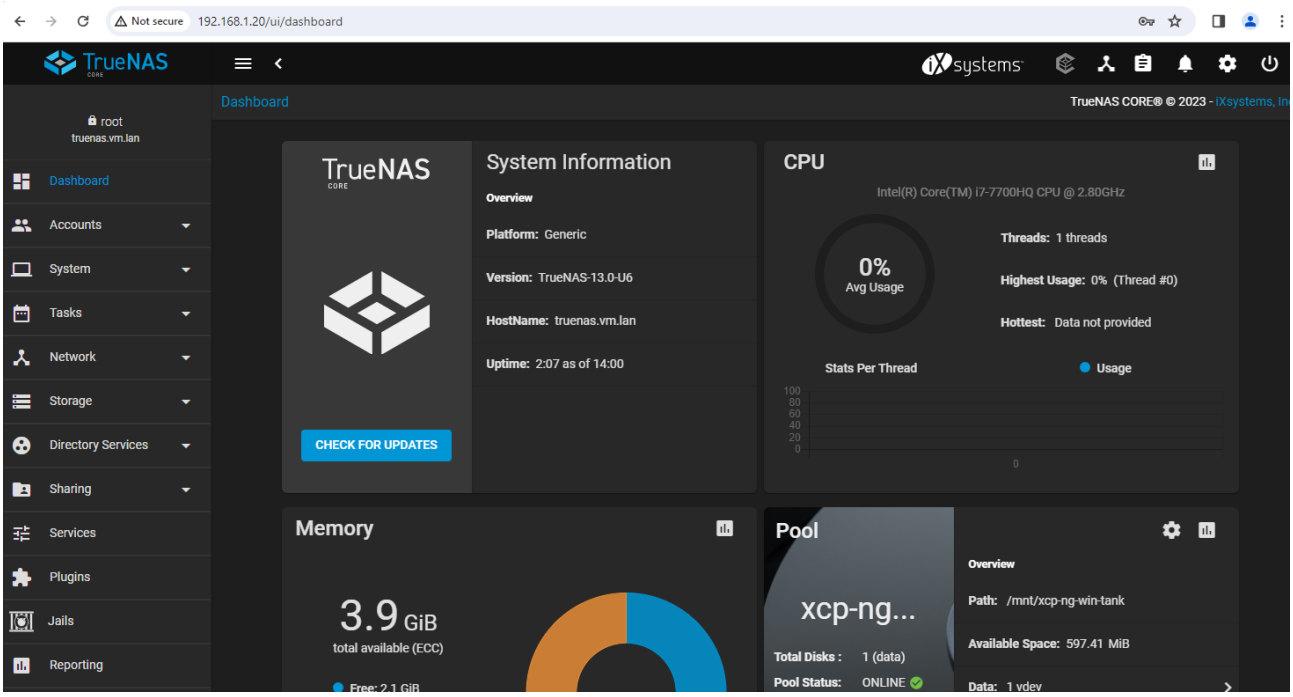

Рисунок 3.14 – Вебінтерфейс керування NAS сервером

На рисунку 3.15 показано налаштування шифрованого пулу зберігання в TrueNAS CORE [17].

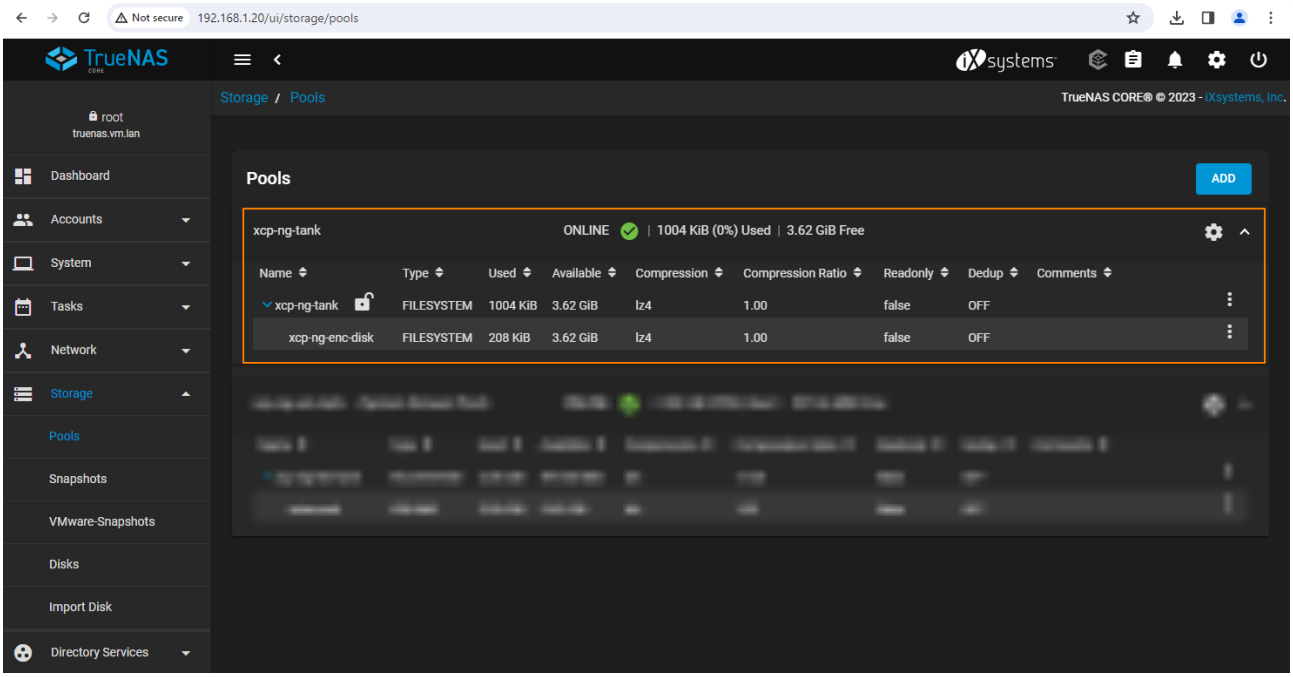

Рисунок 3.15 – Налаштування шифрованого пулу зберігання в TrueNAS CORE

Пул xcp-ng-tank буде використано для створення ресурсу зберігання даних користувачів Windows Server 2022.

На рисунку 3.16 представлено інформацію про алгоритм шифрування пулу зберігання.

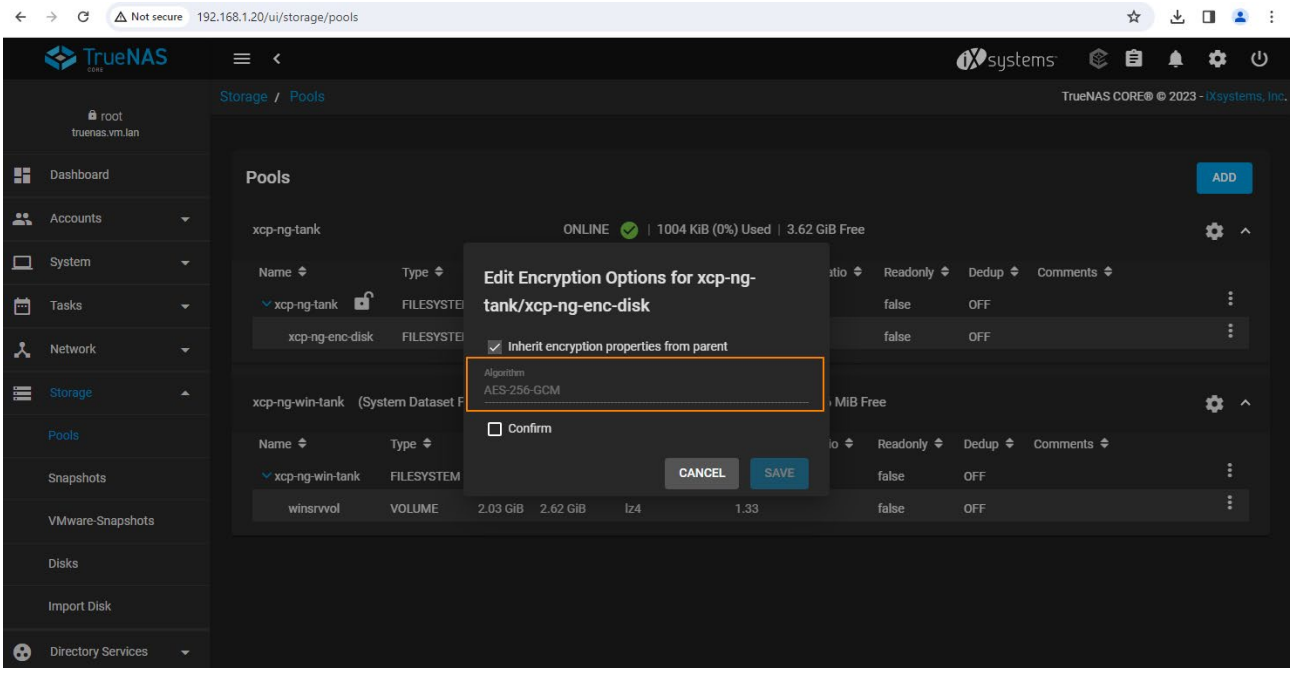

Рисунок 3.16 – Алгоритм шифрування пулу зберігання в TrueNAS CORE

При шифруванні пулу було використано алгоритм шифрування AES-256-GCM. AES-256-GCM - це сучасний стандарт шифрування, який використовує алгоритм AES і режим роботи GCM. Цей шифр використовує ключ завдовжки 256 біт для шифрування та автентифікації даних.

GCM - це режим блокового шифрування, який дозволяє шифрувати блоки даних і надає одночасну перевірку цілісності даних. Цей режим є ефективним і забезпечує високу швидкість шифрування та автентифікації, роблячи його популярним вибором для захисту даних.

На рисунку 3.17 показано налаштування SMB у системі TrueNAS CORE.

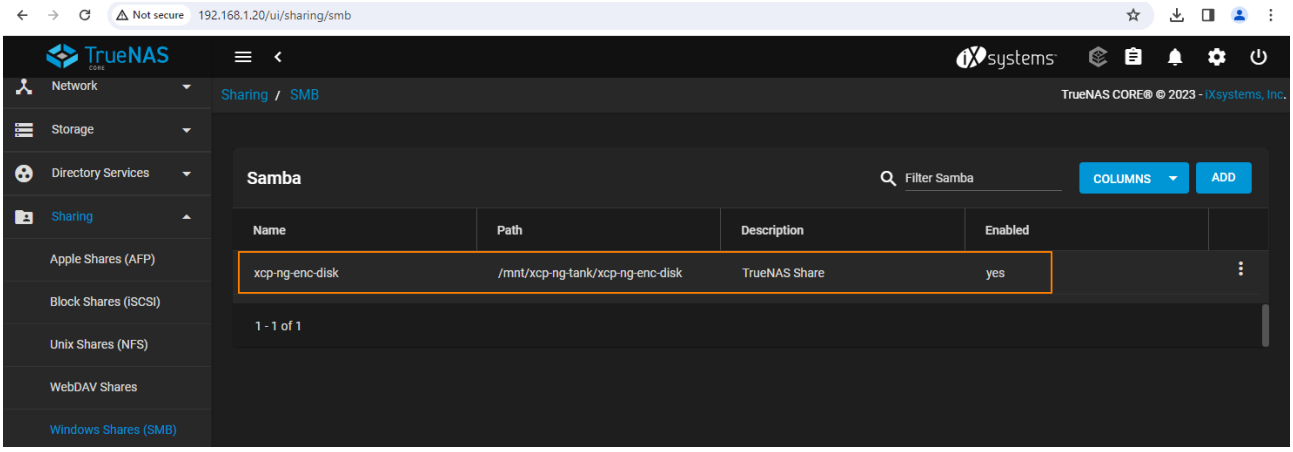

Рисунок 3.17 – Налаштування SMB в TrueNAS CORE

SMB - це стандартний протокол віддаленого доступу до файлів, який використовується переважно в Windows середовищі, але також підтримується багатьма іншими операційними системами.

Ресурс xcp-ng-enc-disk з описом TrueNAS Share активовано, що означає, що він доступний для користувачів, які використовують SMB протокол для доступу до файлів на сервері TrueNAS.

3.3 Розгортання та налаштування Windows Server 2022 RDS

Windows Server 2022 є новою версією серверної операційної системи від Microsoft, яка включає в себе безліч удосконалень та нововведень, спрямованих на підвищення безпеки, продуктивності та гнучкості розгортання

віртуалізованих інфраструктур [18]. Однією з ключових особливостей Windows Server 2022 є покращена безпека, що включає в себе захист від загроз на рівні ядра операційної системи, покращений захист від вірусів та кібератак, а також розширену підтримку зашифрованих з'єднань з використанням протоколу HTTPS та TLS 1.3 за замовчуванням.

У Windows Server 2022, служба віддаленого робочого столу (RDS) є важливим елементом, який забезпечує можливість користувачам отримувати віддалений доступ до програм та робочих столів, що розташовані на серверах. RDS в Windows Server 2022 пропонує поліпшену продуктивність та безпеку, дозволяючи організаціям забезпечити ефективний віддалений доступ для своїх співробітників [19].

Однією з основних удосконалень RDS у Windows Server 2022 є підвищення рівня безпеки. Це досягається за рахунок впровадження підтримки протоколу TLS 1.3 для забезпечення зашифрованого з'єднання між клієнтами та серверами RDS. Удосконалені можливості для захисту від вірусів через інтеграцію з Windows Defender та іншими інструментами безпеки. Можливість використання багатофакторної автентифікації для додаткового рівня верифікації користувачів при віддаленому доступі.

Покращення в Windows Admin Center забезпечують більш зручне та інтуїтивне управління RDS, включаючи налаштування сесій, додатків та безпеки.

RDS у Windows Server 2022 пропонує організаціям надійний, безпечний та ефективний спосіб надання віддаленого доступу до ресурсів сервера, підтримуючи при цьому високий рівень продуктивності та зручності для кінцевих користувачів.

На рисунку 3.18 показано загальні налаштування віртуальної машини Windows Server 2022 в Xen Orchestra.

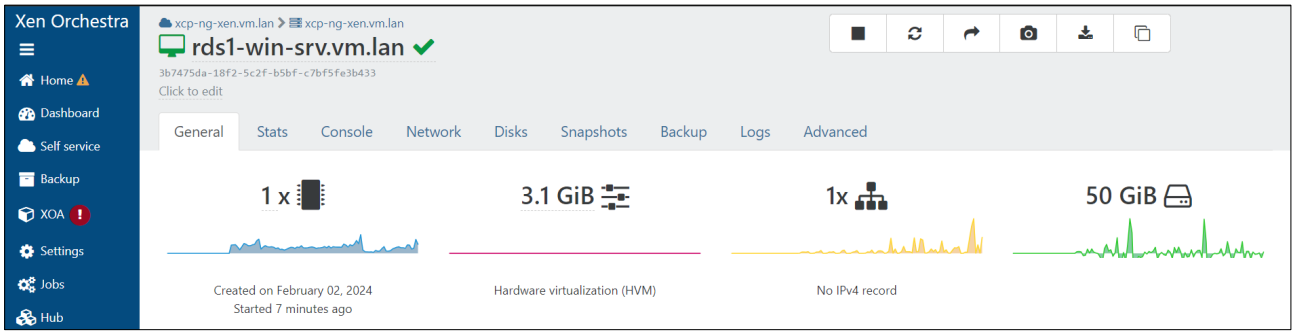

Рисунок 3.18 – Загальні налаштування віртуальної машини Windows Server 2022

Після встановлення Windows Server 2022 потрібно здійснити його початкові налаштування за допомогою графічного інтерфейсу (див. рисунок 3.19).

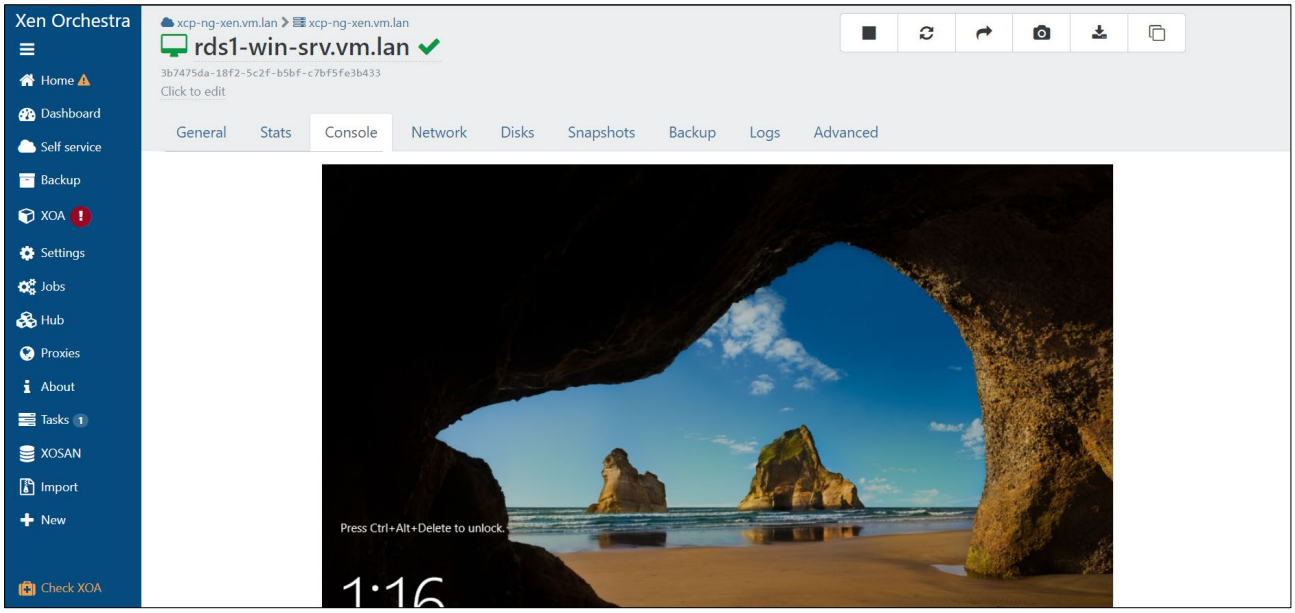

Рисунок 3.19 – Консоль віртуальної машини Windows Server 2022

На рисунку 3.20 показано встановлення RDS в Windows Server 2022 за допомогою PowerShell [20].

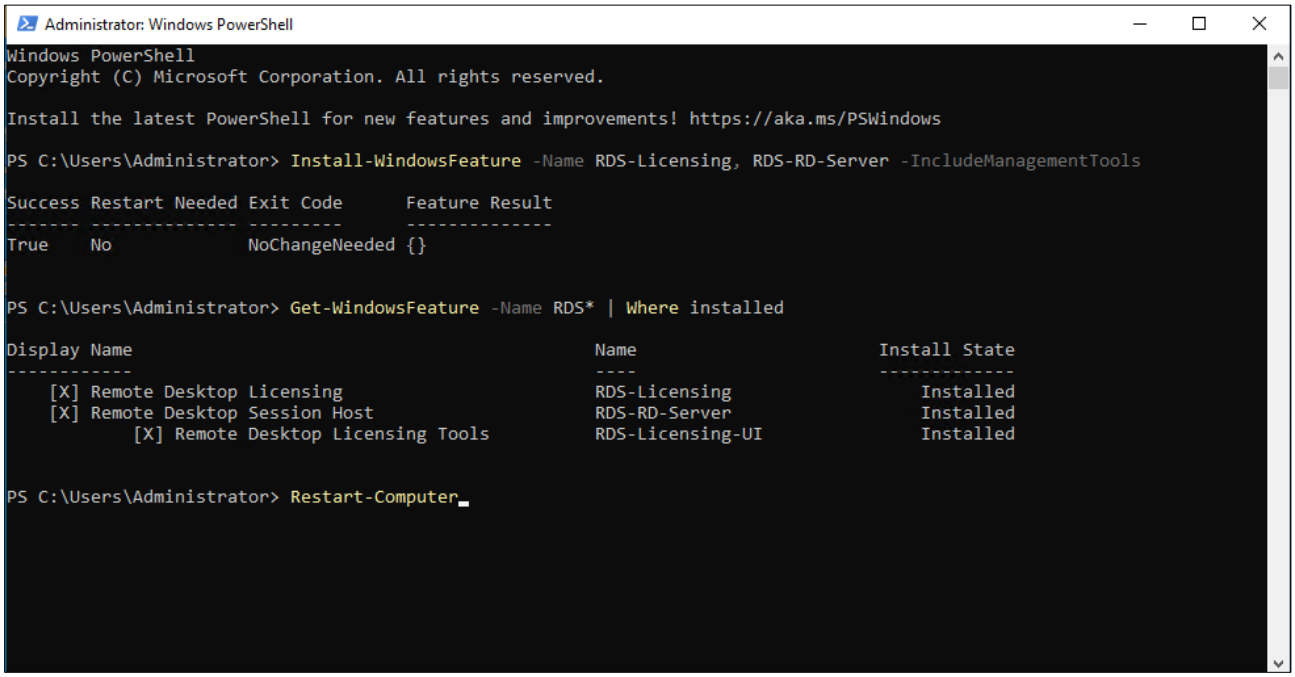

Рисунок 3.20 – Встановлення RDS в Windows Server 2022

Встановлення ролі RDS є завершальним етапом базового налаштування Windows Server 2022.

3.4 Проведення тестування віртуалізованої IT-інфраструктури

На першому етапі тестування перевіримо коректність отримання мережевих налаштувань за допомогою DHCP на тестовому комп'ютері InternalTestPC. У вікні командного рядка Windows 10 на комп'ютері InternalTestPC, зображеному на рисунку 3.21, використана команда `ipconfig /all` для отримання докладної інформації про конфігурацію мережевих інтерфейсів на даному комп'ютері.

Тестовий комп'ютер InternalTestPC отримав мережеві конфігураційні параметри від маршрутизатора pfSense за допомогою DHCP. Ці налаштування включають в себе IP-адресу, маску підмережі, шлюз, адресу DHCP та DNS серверів, які використовуються для з'єднання з мережею та отримання доступу до Інтернету.

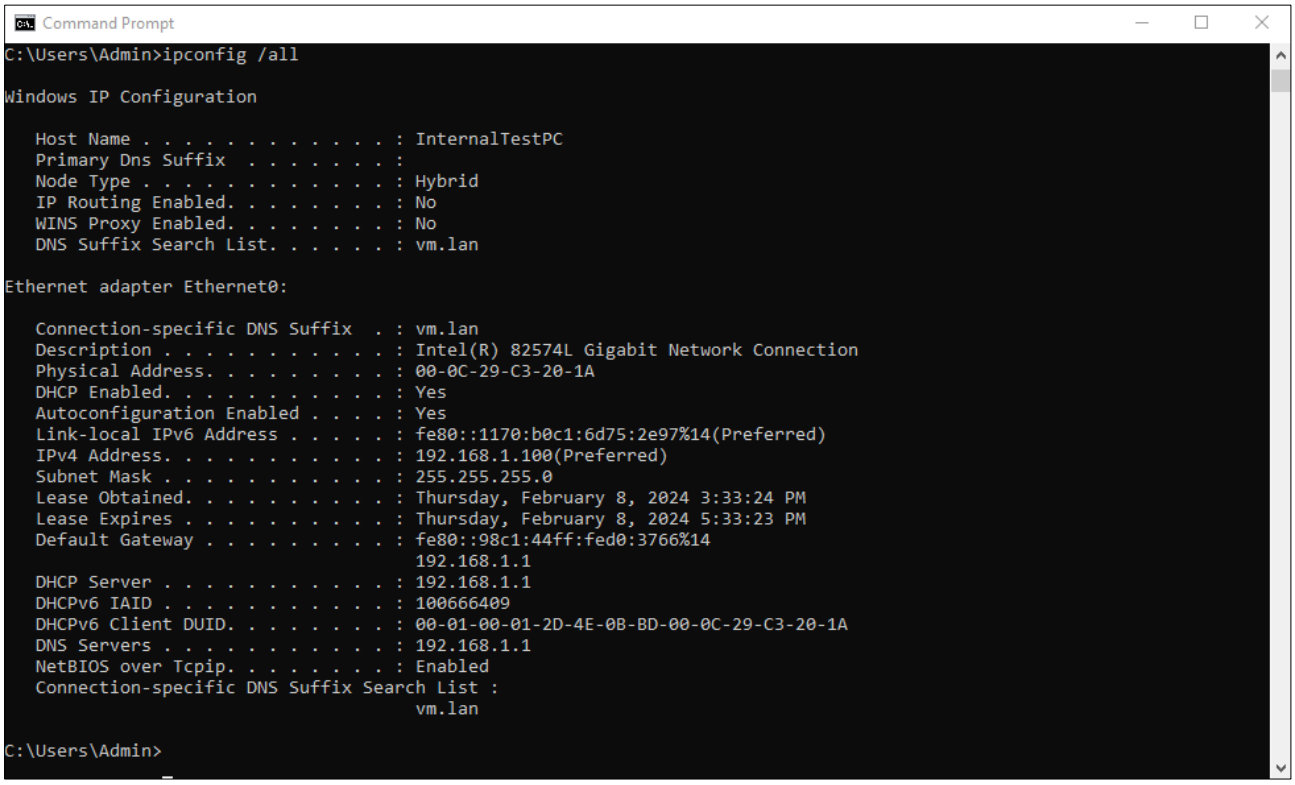

Рисунок 3.21 – Мережеві налаштування тестового комп'ютера InternalTestPC

Для проведення тестування віртуалізованого середовища створимо користувача з іменем `vitalii` на сервері Windows Server 2022. Після цього за допомогою протоколу SMB під’єднаємо каталог, який розташований на NAS-сервері, як домашній каталог, і визначимо його як диск W у налаштуваннях профілю цього користувача (див. рисунок 3.22).

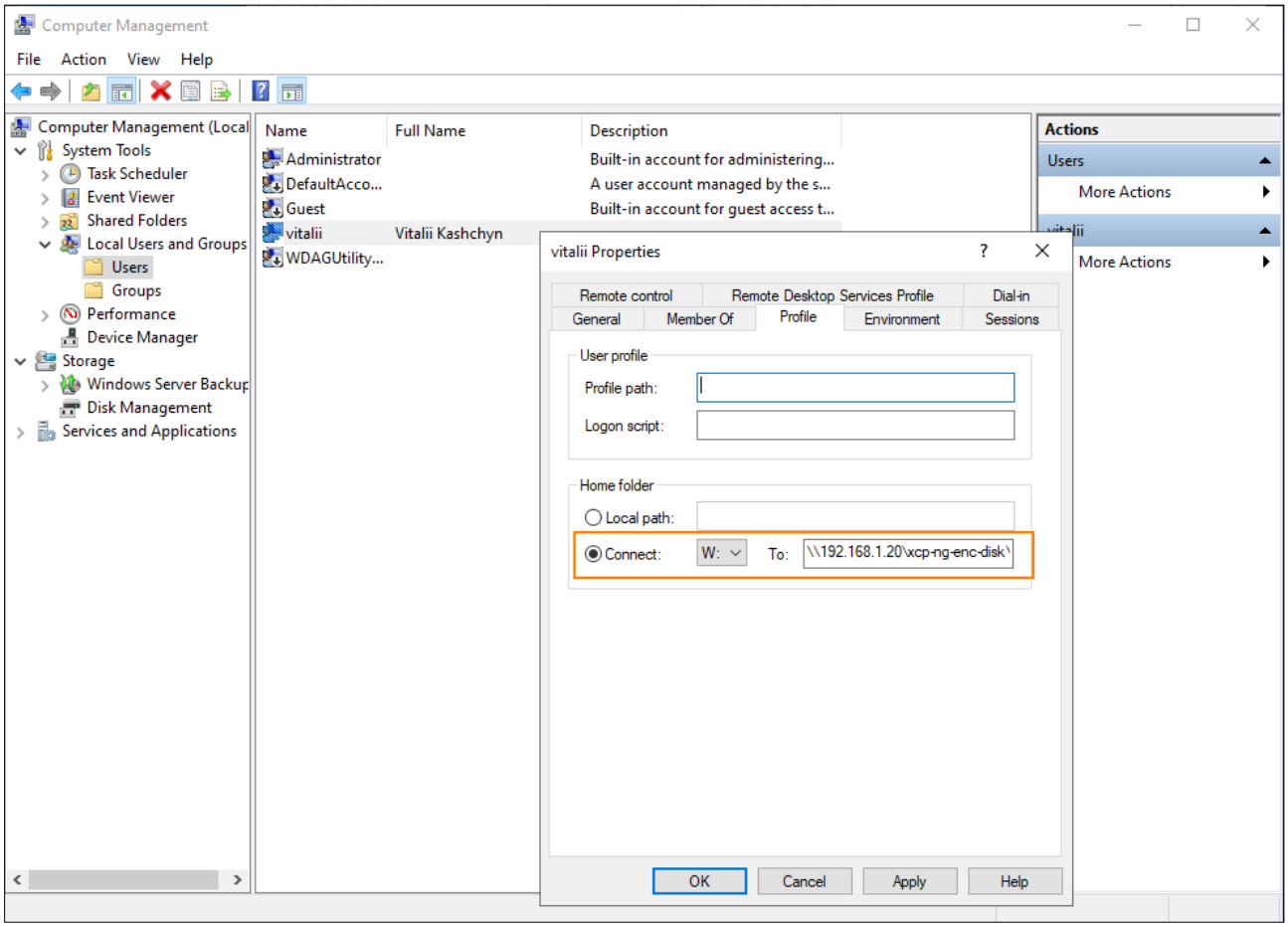

Рисунок 3.22 – Налаштування профілю користувача `vitalii`

Також для можливості віддаленого входу в Windows Server потрібно добавити користувача `vitalii` у відповідну групу доступу на сервері (див. рисунок 3.23).

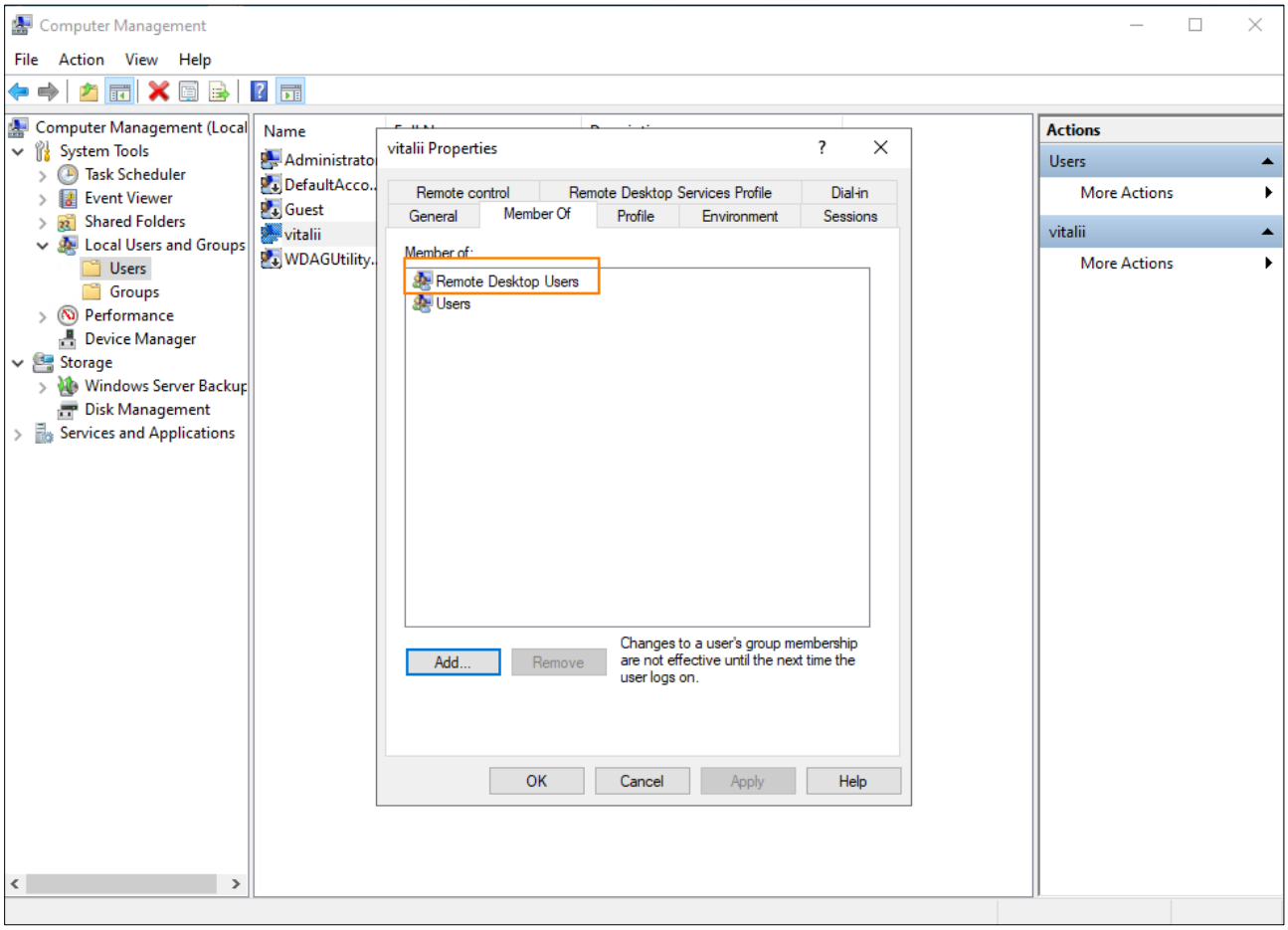

Рисунок 3.23 – Налаштування груп користувача `vitalii`

Під час віддаленого входу через RDC в операційну систему Windows Server 2022 з тестового комп'ютера Internal TestPC з логіном `vitalii`, домашній каталог користувача буде автоматично підключений як диск W (див. рисунок 3.24).

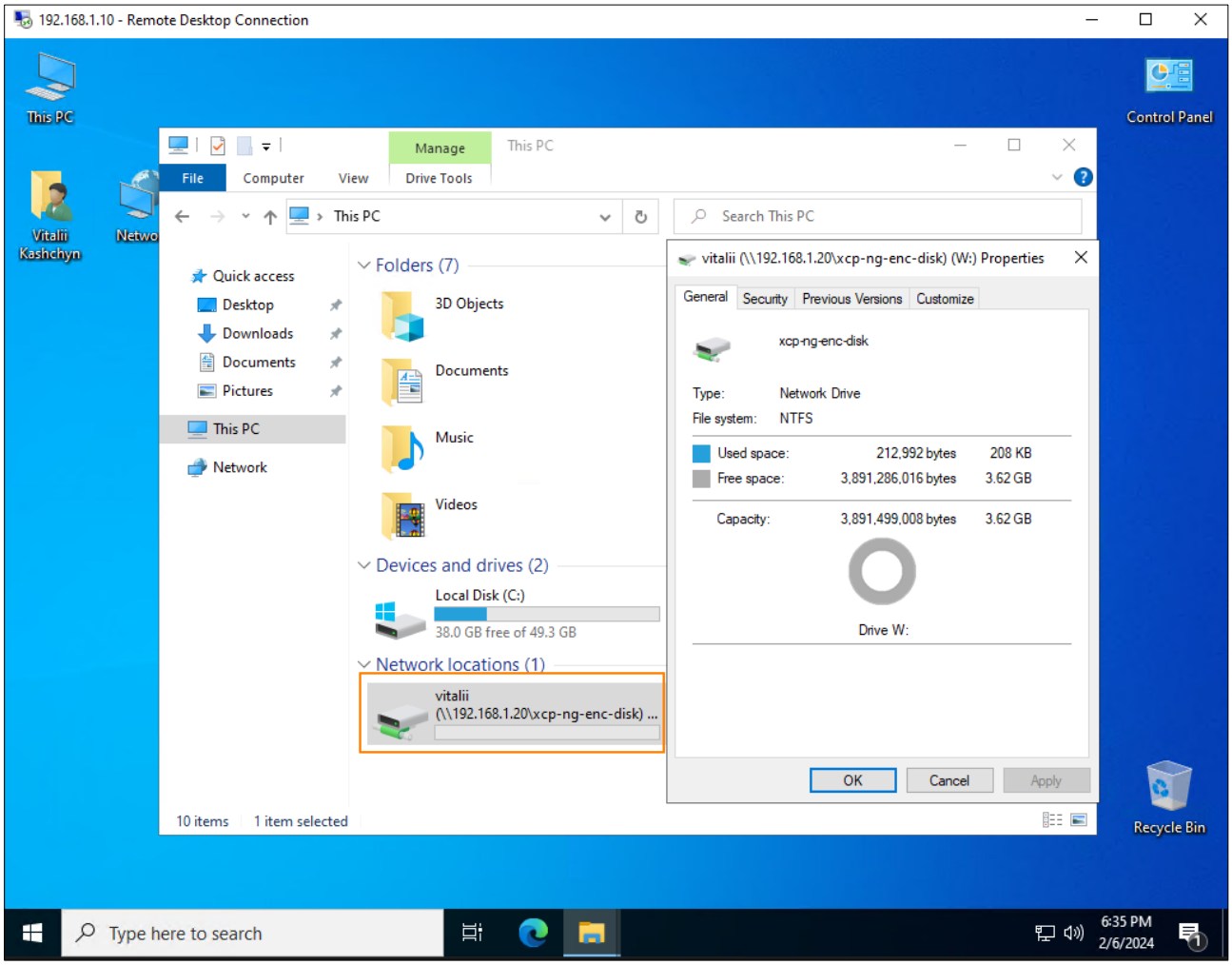

Рисунок 3.24 – Домашній каталог користувача `vitalii`

Для перевірки коректності роботи L2TP/IPsec VPN сервера створимо користувача `vitalii` в налаштуваннях VPN маршрутизатора pfSense (див. рисунок 3.25).

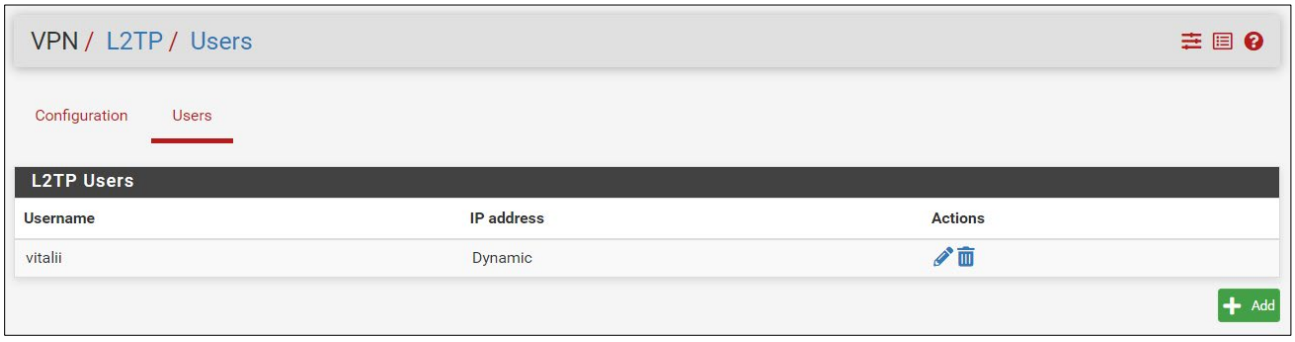

Рисунок 3.25 – Створення VPN користувача `vitalii` в pfSense

Налаштуємо VPN з’єднання на тестовому комп’ютері ExternalTestPC з Windows10 згідно параметрів описаних в пункті 3.1 (див. рисунок 3.26).

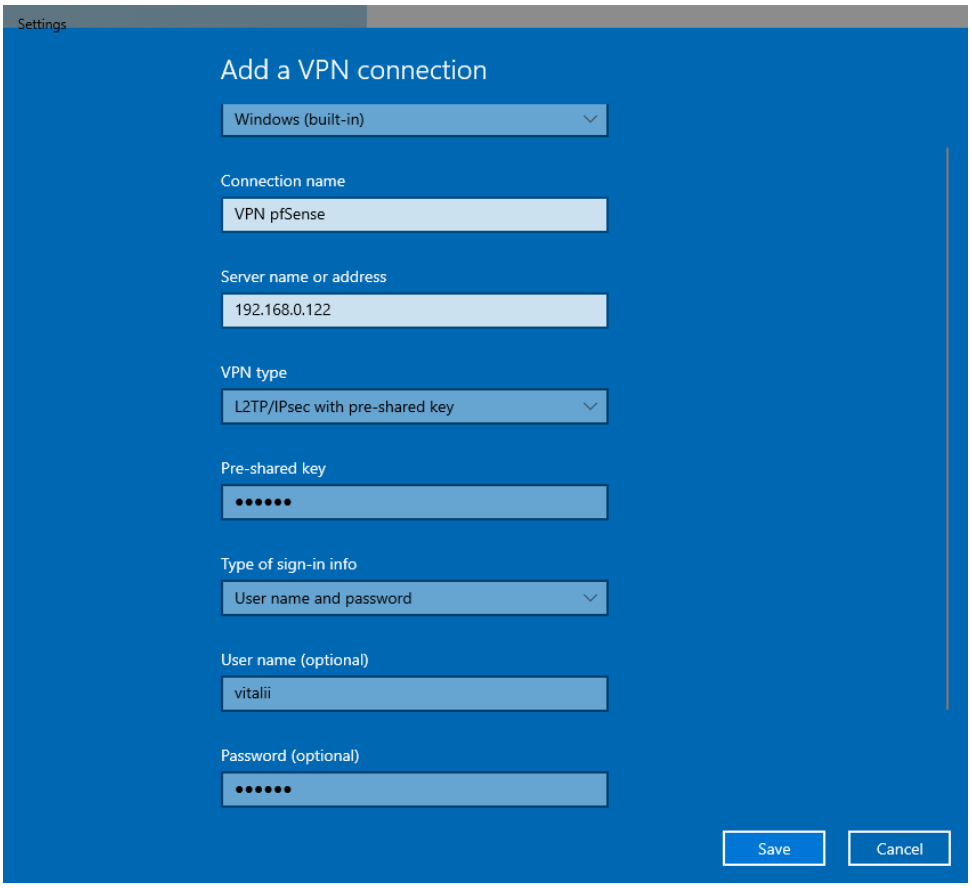

Рисунок 3.26 – Створення VPN з’єднання на тестовому комп’ютері ExternalTestPC

Використано стандартний VPN клієнт вбудований в Windows, який підтримує тип VPN L2TP/IPsec з додатковим загальним ключем. Він надає можливість користувачам здійснювати підключення до віддаленої корпоративної мережі через Інтернет з використанням безпечних технологій.

На рисунку 3.27 можна побачити що VPN працює коректно. Є доступ до мережі Інтернет та можливість віддаленого входу через RDC в операційну систему Windows Server 2022 з логіном `vitalii`

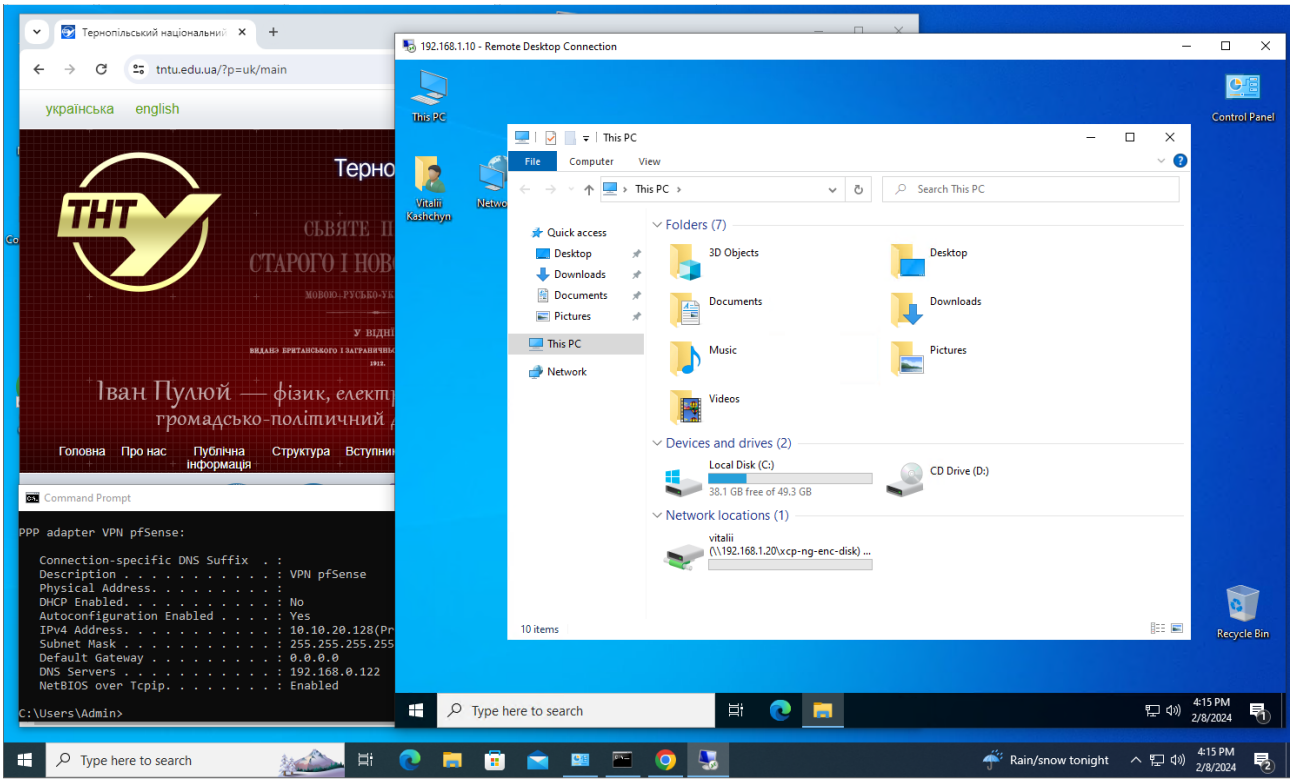

Рисунок 3.27 – Перевірка віддаленого входу через RDC при активному VPN з’єднанні

Також в статусі IPsec маршрутизатора pfSense можна побачити докладні параметри VPN з’єднання (див. рисунок 3.28).

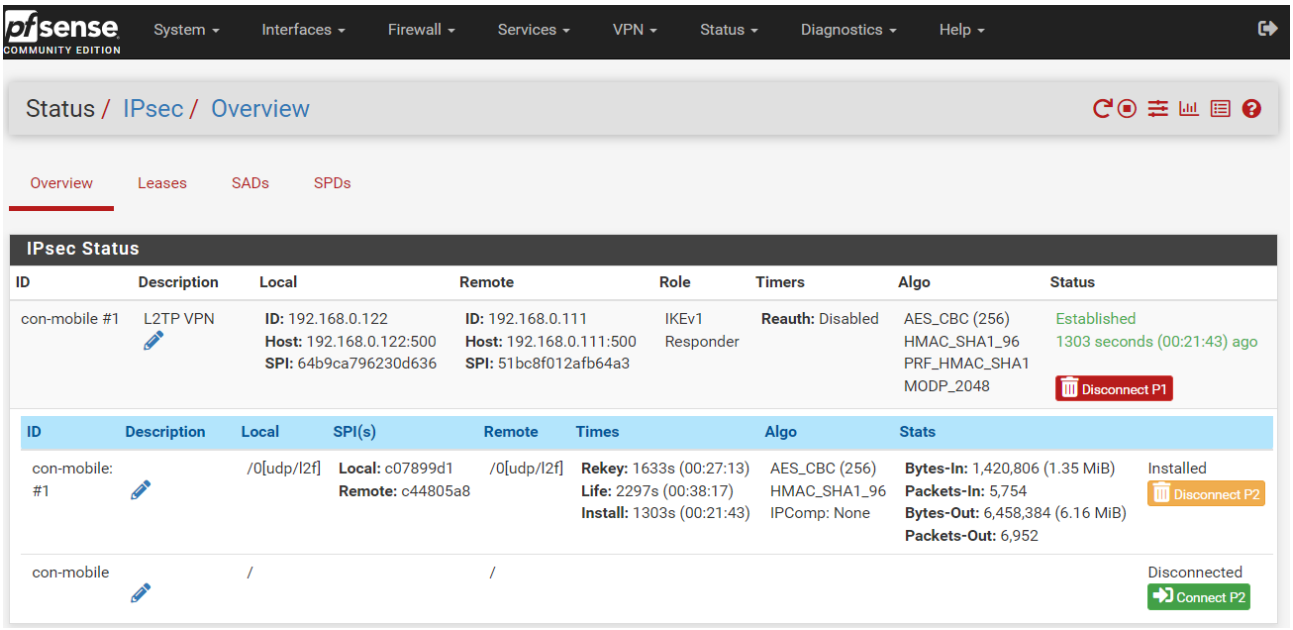

Рисунок 3.28 – Параметри активного L2TP/IPsec VPN з’єднанні в маршрутизаторі pfSense

В фазі P1 використовуються наступні алгоритми: AES_CBC (256), HMAC_SHA1_96, PRF_HMAC_SHA1, MODP_2048. В фазі P2: AES_CBC (256) та HMAC_SHA1_96.

AES_CBC (256) вказує на використання семеричного алгоритму шифрування AES у режимі CBC з ключем довжиною 256 біт [21]. В режимі CBC кожне шифрування одного й того ж відкритого тексту призводить до унікального зашифрованого тексту. Цей режим використовує вектор ініціалізації, який має такий самий розмір, як і зашифрований блок. Початково застосовується операція XOR між блоком відкритого тексту та вектором. Після цього блок шифрується за допомогою ключа шифрування. Результат кожного блоку після попередньої операції XOR стає вхідним для наступного блоку відкритого тексту під час процесу шифрування.

HMAC_SHA1_96 це Keyed-Hash Message Authentication Code, який використовує хеш-функцію SHA1 разом із секретним ключем для забезпечення автентифікації повідомлення та його цілісності. У випадку HMAC_SHA1_96, застосовується хеш-функція SHA1, але тільки перші 96 біт результату використовуються як код автентифікації. Це робиться для скорочення довжини коду автентифікації, зменшення обчислювального навантаження та економії пропускної здатності в мережевих з'єднаннях.

Алгоритм PRF_HMAC_SHA1 (Pseudo-Random Function based on HMAC-SHA1) використовує хеш-функцію HMAC-SHA1 для створення псевдовипадкової функції. HMAC-SHA1 використовується для обчислення значення, яке служить основою для генерації псевдовипадкових бітів для створення безпечних ключів.

MODP_2048 відноситься до однііє з груп Diffie-Hellman в контексті криптографічних протоколів, таких як IPsec. DH є методом безпечного обміну криптографічними ключами через незахищений канал зв'язку. MODP_2048 вказує на використання простого модуля з довжиною ключа 2048 біт, що використовується для обчислення спільного секретного ключа між двома сторонами в процесі обміну ключами Diffie-Hellman. Це забезпечує високий рівень безпеки для обміну ключами між хостами.

Ці параметри використовуються для визначення того, як дані будуть зашифровані та як буде перевірятися автентичність даних у VPN-тунелі. Вони допомагають забезпечити конфіденційність та цілісність даних, які передаються через L2TP\IPsec VPN.

Всі здійснені тести підтверджують ефективність віртуалізованої IT-інфраструктури на базі гіпервізора типу 1 XEN на платформі XCP-ng. Обрані операційні системи та налаштовані сервіси відповідають вимогам що до безпеки та надійності.

3.5 Висновки до розділу

В третьому розділі у віртуалізованому середовищі розгорнуто та налаштовано маршрутизатор з функцією брандмауера та VPN концентратора pfSense. За допомогою pfSense налаштовано маршрутизацію між віртуальними сегментами мережі ExternalNetwork0 та LANNetwork0 віртуальних комутаторів XCP-ng. В pfSense налаштовано DHCP сервера для локальної мережі, L2TP/IPsec VPN сервер для віддаленого доступу до серверів локальної мережі. Також pfSense налаштовано як брандмауер з функцією NAT для доступу клієнтів локальної мережі та VPN клієнтів до мережі Інтернет.

Встановлено та налаштовано NAS сервер TrueNAS CORE з шифрованим пулом зберігання, який використано для створення ресурсу зберігання даних (домашніх каталогів) користувачів Windows Server 2022. Встановлено та налаштовано Windows Server 2022 з роллю RDS, що дозволяє користувачам отримувати віддалений доступ до додатків та робочих столів, розміщених на Windows Server 2022.

Проведено тестування віртуалізованої IT-інфраструктури, а саме коректність роботи DHCP в pfSense, SMB в TrueNAS, RDS в Windows Server 2022 та L2TP/IPsec VPN в pfSense. Всі здійснені тести підтвердили ефективність та безпеку віртуалізованої IT-інфраструктури на базі гіпервізора типу 1 XEN на платформі XCP-ng.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при шоку

Долікарська допомога постраждалим при підозрі на шок є важливою процедурою, яку можуть виконувати особи без медичної освіти. Шок - це невідкладний стан, що виникає внаслідок порушення оксигенації тканин організму та може призвести до дисфункції важливих органів та систем.

Ознаки шоку включають бліду, холодну та вологу шкіру, загальну слабкість, неспокій, роздратованість, сухість в роті, спрагу, змінену частоту дихання та свідомість.

Причинами шоку можуть бути масивна зовнішня або внутрішня кровотеча, травми, анафілаксія або серцевий напад.

Наказ Міністерства охорони здоров'я України від 09.03.2022 р. № 441 " Про затвердження порядків надання домедичної допомоги особам при невідкладних станах" встановлює порядки надання домедичної допомоги постраждалим при підозрі на шок [22].

Надання домедичної допомоги постраждалим при підозрі на шок включає такі дії:

- переконатися у відсутності небезпеки та, якщо небезпеки немає, переходити до наступного кроку;
- заспокоїти постраждалого та пояснити свої дії;
- викликати швидку медичну допомогу та слідувати інструкціям диспетчера;
- виявити та усунути причину шоку, якщо це можливо;
- надати постраждалому протишокове положення:

а) перевести постраждалого в горизонтальне положення, якщо це не погіршує його дихання;

б) покласти під ноги валик з одягу тощо таким чином, щоб ступні ніг знаходились на рівні його підборіддя;

в) підкласти під голову постраждалого одяг/подушку, якщо це не погіршує його дихання;

г) вкрити постраждалого ковдрою або покривалом.

- забезпечити постійний нагляд за постраждалим до прибуття швидкої медичної допомоги;

- у разі погіршення стану постраждалого повторно викликати швидку медичну допомогу;

- зібрати максимально можливу інформацію про обставини травми та її механізм і передати цю інформацію працівникам швидкої медичної допомоги або диспетчеру.

Якщо постраждалий втратив свідомість до прибуття швидкої медичної допомоги, слід перейти до процедури надання долікарської допомоги дорослим або дітям при раптовій зупинці кровообігу, відповідно до встановленого Порядку.

Виконання цих кроків допоможе забезпечити постраждалому першу необхідну допомогу та зберегти його життя до прибуття медичних фахівців.

4.2 Естетичне оформлення робочого місця оператора ПК

В сучасному світі багато людей проводять значну частину свого часу за робочим столом оператора ПК. Робоче місце є місцем, де проходить багато годин концентрованої праці, комунікації і творчості. Тому важливо не лише забезпечити функціональність та зручність цього простору, але й звернути увагу на його естетичне оформлення.

Естетичне оформлення робочого місця оператора ПК не є просто прикрасою. Воно впливає на настрій, комфорт і продуктивність. Гармонійне та затишне оточення може стимулювати творчість, поліпшувати концентрацію і сприяти ефективній роботі. Крім того, персоналізація робочого простору дозволяє виразити свою індивідуальність та створити потрібну робочу атмосферу в довколишньому середовищі.

При організації естетичного оформлення робочого місця оператора ПК потрібно врахувати наступні моменти:

– Оптимальне розташування обладнання: розмістіть комп'ютер, монітор і периферійні пристрої (клавіатура, миша і т.д.) таким чином, щоб було зручно досягати до них і працювати. Уникайте перенавантаження робочої поверхні надмірною кількістю об'єктів.

– Організація кабелів: спробуйте зберегти порядок на робочому місці, організувавши кабелі. Використовуйте спеціальні тримачі або кабельні канали, щоб зібрати всі кабелі разом і уникнути безладу;

– Регульованість меблів: якщо це можливо, оберіть регульовані меблі, такі як стіл і стілець. Це дозволить вам налаштувати їх на оптимальну висоту і зручніше працювати. Також не забувайте про крісло, яке підтримує вашу спину та посадку, для забезпечення комфорту протягом тривалого робочого дня;

– Освітлення: забезпечте достатнє освітлення на робочому місці. Використовуйте природне освітлення, де це можливо, і додаткові лампи, якщо потрібно. Уникайте світлових джерел, які можуть втомлювати очі;

– Персоналізація: додайте особистого штриху до свого робочого простору, розташувавши на столі фотографії, рослини, мотиваційні цитати або речі, які надихають вас. Зробіть його комфортним і приємним для вас;

– Колірна гамма: використовуйте кольори, які вам подобаються і створюють приємну атмосферу. Наприклад, нейтральні або природні відтінки можуть сприяти спокою і концентрації;

– Мінімалізм: розгляньте можливість створення мінімалістичного дизайну. Уникайте зайвих предметів або безладу на робочому столі. Чистота та простота можуть сприяти зосередженості і ефективності;

– Правильне використання простору: максимізуйте використання доступного простору, особливо якщо у вас обмежений робочий простір. Використовуйте полички, ящики або стінні органайзери для зберігання речей і важливих документів;

– Зонування: якщо ви маєте можливість, створіть зони на робочому місці, наприклад, зона для роботи з комп'ютером або зона для письма. Це допоможе розподілити простір і зберегти організованість;

– Зображення та графіка: розгляньте можливість додавання художніх картин, плакатів або інших видів графіки на стіни робочого простору. Це може створити стимулююче середовище та надихати на творчість;

– Потрібні аксесуари: виберіть стильні й корисні аксесуари, які підходять до вашого стилю та потреб. Наприклад, стильна підставка для ноутбука, ергономічна підставка для рук або оригінальні канцелярські засоби;

– Правильна вентиляція та комфорт: переконайтеся, що у вас є належна вентиляція та забезпечена комфортна температура в приміщенні.

Загалом, естетичне оформлення робочого місця оператора ПК має бути практичним і зручним для роботи, одночасно створюючи приємну атмосферу, яка сприяє продуктивності і комфорту.

ВИСНОВКИ

В процесі виконання бакалаврської кваліфікаційної роботи було розроблено та налагоджено безпечна IT-інфраструктура, використовуючи гіпервізор типу 1 XEN на платформі XCP-ng.

У першому розділі кваліфікаційної роботи представлено детальний аналіз принципів віртуалізації, розглянуто особливості та переваги гіпервізора XEN, зокрема його мікроядерну архітектуру, що забезпечує високий рівень стабільності та безпеки віртуалізованих середовищ. Окрім того, акцентовано на архітектурних особливостях гіпервізора XEN, підкреслено, що його простота та мінімалізм коду сприяють економічності та ефективності, а високий рівень безпеки та ізоляції забезпечується завдяки відокремленню віртуальних машин від апаратної частини. Також описано режим віртуалізації PHV, що комбінує переваги паравіртуалізації та апаратної віртуалізації, та є ідеальним варіантом для досягнення високої продуктивності, надійності та безпеки. Висвітлено механізм віртуалізації процесів введення-виведення у гіпервізорі XEN.

У другому розділі описано процес створення лабораторного тестового середовища для віртуалізованої IT-інфраструктури на базі платформи XCP-ng, варіанту гіпервізора XEN. Детально розглянуто процес налаштування XCP-ng, його архітектурні особливості з фокусом на засоби зберігання даних та мережеві можливості. Представлено інструменти управління хостами XCP-ng: XCP-ng Center, xeCLI та Xen Orchestra.

У третьому розділі здійснено процес налаштування маршрутизатора з функціями брандмауера та VPN-концентратора pfSense у віртуалізованому середовищі. Описано налаштування маршрутизації між сегментами мережі за допомогою pfSense, конфігурацію DHCP сервера, L2TP/IPsec VPN для віддаленого доступу, а також налаштування брандмауера з NAT для забезпечення доступу до Інтернету. Додатково розглянуто встановлення та конфігурацію NAS сервера TrueNAS CORE з шифрованим зберіганням даних та Windows Server 2022 з роллю служби віддаленого робочого столу.

Проведено тестування віртуалізованої IT-інфраструктури, а саме коректність роботи DHCP в pfSense, SMB в TrueNAS, RDS в Windows Server 2022 та L2TP/IPsec VPN в pfSense. Результати тестів підтвердили ефективність та безпеку створеної системи на основі гіпервізора XEN на платформі XCP-ng. Отримані результати можуть мати практичне використання для створення безпечних та надійних корпоративних IT-інфраструктур на основі віртуалізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is Virtualization? URL: https://aws.amazon.com/what-is/virtualization/ (дата звернення: 09.02.2024).

2. What are hypervisors. URL: https://www.ibm.com/topics/hypervisors (дата звернення: 09.02.2024).

3. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ. Матеріали конференцій МЦНД, (24.05.2024; Запоріжжя, Україна), 145-146.

4. Тимощук, В., & Тимощук, Д. (2022). Віртуалізація в центрах обробки даних-аспекти відмовостійкості. Матеріали X науково-технічної конференції „Інформаційні моделі, системи та технології “Тернопільського національного технічного університету імені Івана Пулюя, 95-95.

5. Revniuk O.A., Zagorodna N.V., Kozak R.O., Karpinski M.P., Flud L.O. “The improvement of web-application SDL process to prevent Insecure Design vulnerabilities”. Applied Aspects of Information Technology. 2024; Vol. 7, No. 2: 162–174. DOI:https://doi.org/10.15276/aait.07.2024.12.

6. Xen Project Software Overview. URL: https://wiki.xenproject.org/wiki/Xen_Project_Software_Overview#PV_.28x86.29 (дата звернення: 09.02.2024).

7. Paravirtualization (PV). URL: https://wiki.xenproject.org/wiki/Paravirtualization_(PV) (дата звернення: 09.02.2024).

8. XCP-ng Introduction. URL: https://docs.xcp-ng.org/ (дата звернення: 09.02.2024).

9. Xen Orchestra Introduction. URL: https://xen-orchestra.com/docs/ (дата звернення: 09.02.2024).

10. pfSense Introduction. URL: https://docs.netgate.com/pfsense/en/latest/general/index.html (дата звернення: 09.02.2024).

11. Nataliya Zagorodna, Iryna Kramar (2020). Economics, Business and Security: Review of Relations. Business Risk in Changing Dynamics of Global Village BRCDGV-2020: Monograph / Edited by Pradeep Kumar, Mahammad Sharif. India, Patna: Novelty & Co., Ashok Rajpath,. 446 p., pp.25-39.

12. pfSense L2TP VPN. URL: https://docs.netgate.com/pfsense/en/latest/vpn/l2tp/index.html (дата звернення: 09.02.2024).

13. Karnaukhov, A., Tymoshchuk, V., Orlovska, A., & Tymoshchuk, D. (2024). USE OF AUTHENTICATED AES-GCM ENCRYPTION IN VPN. Матеріали конференцій МЦНД, (14.06. 2024; Суми Україна), 191-193.

14. pfSense Firewall. URL: https://docs.netgate.com/pfsense/en/latest/firewall/index.html (дата звернення: 09.02.2024).

15. pfSense Network Address Translation. URL: https://docs.netgate.com/pfsense/en/latest/nat/index.html (дата звернення: 09.02.2024).

16. TrueNAS Documentation Hub. URL: https://www.truenas.com/docs/ (дата звернення: 09.02.2024).

17. TrueNAS Storage Configuration. URL: https://www.truenas.com/docs/core/gettingstarted/storingdata/ (дата звернення: 09.02.2024).

18. Get started with Windows Server. URL: https://learn.microsoft.com/en-us/windows-server/get-started/get-started-with-windows-server (дата звернення: 09.02.2024).

19. Welcome to Remote Desktop Services. URL: https://learn.microsoft.com/uk-ua/windows-server/remote/remote-desktop-services/welcome-to-rds (дата звернення: 09.02.2024).

20. What is Windows PowerShell. URL: https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.4 (дата звернення: 09.02.2024).

21. Тимощук, В., & Стебельський, М. (2023). Шифрування даних в операційних системах. Матеріали VI Міжнародної студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання “, 183-184.

22. Про затвердження порядків надання домедичної допомоги особам при невідкладних станах. URL: https://zakon.rada.gov.ua/laws/show/z0356-22#n769(дата звернення: 09.02.2024).