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: " Створення захищеної корпоративної інфраструктури на основі гіпервізора VMware ESXi"

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Горішний Остап Юрійович
підпис (прізвище та ініціали)

Керівник Кульчицький Т. Р.
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 Горішному Остапу Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Створення захищеної корпоративної інфраструктури на основі гіпервізора VMware ESXi

Керівник роботи Кульчицький Тарас Русланович, доктор філософії, 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 захисту копоративної інфраструктури. Гіпервізор VMware ESXi, брандмауер та маршрутизатор OPNsense.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1. Огляд технологій
2. Засоби створення корпоративної інфраструктури на основі гіпервізора
3. Налаштування та тестування віртуалізованої корпоративної 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. Інтеграція брандмауерів в віртуалізовані середовища. Архітектура та особливості роботи гіпервізора VMware ESXi. Вебінтерфейс управління гіпервізором ESXi. Інтерфейс користувача прямої консолі (DCUI). Апаратна віртуалізація Intel та AMD. Огляд маршрутизатора та брандмауера OPNsense. Схема лабораторного тестового середовища. Інтерфейс управління VMware ESXi. Налаштування маршрутизатора OPNsense. Налаштування OpenVPN сервера. Статус та параметри підключення Viscosity OpenVPN клієнта. Перевірка маршрутизації за допомогою WinMTR. Підключення по RDP протоколу до Windows Server 2022.
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 «Огляд технологій»	21.02 – 10.03	
4.	Оформлення розділу «Засоби створення корпоративної інфраструктури на основі гіпервізора»	11.03 – 25.03	
5.	Оформлення розділу «Налаштування та тестування віртуалізованої корпоративної 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	27.06.2024	

Студент _____ Горішний О.Ю.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Кульчицький Т. Р.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Створення захищеної корпоративної інфраструктури на основі гіпервізора VMware ESXi // Кваліфікаційна робота ОР «Бакалавр» // Горішний Остап Юрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-43 // Тернопіль, 2024 // С. 67, рис. – 34, табл. – - 0 , кресл. – 14, додат. – 0.

Ключові слова: VMware, ESXi, OPNsense, OpenVPN, NAT, гіпервізор, віртуалізація, Windows, брандмауер.

Кваліфікаційна робота бакалавра присвячена дослідженню технології віртуалізації та реалізації захищеної корпоративної інфраструктури на основі гіпервізора VMware ESXi. Проведено детальний огляд різних технологій віртуалізації та їхніх можливостей для створення безпечних корпоративних середовищ. Виконано встановлення та конфігурацію гіпервізора VMware ESXi, що служить основою створення віртуальних інфраструктур. Встановлено та налаштовано віртуальну машину OPNsense як маршрутизатора з підтримкою OpenVPN, NAT, DNS, DHCP сервера та брандмауера. Здійснено процес встановлення та конфігурації операційної системи Windows Server 2022 як корпоративного сервера з підтримкою RDP. Розроблено механізми створення та налаштування шифрованого VPN-з'єднань між корпоративною інфраструктурою та клієнтськими пристроями.

Виконано серію тестів для перевірки ефективності та надійності створеної системи, що підтвердило її високий рівень функціональності. Результати даного дослідження сприятимуть створенню безпечних корпоративних мереж, забезпечуючи високий рівень захисту VPN-з'єднань.

ANNOTATION

Creation of a secure corporate infrastructure based on the VMware ESXi hypervisor. // Thesis of educational level "Bachelor"// Ostap Horishnyi // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБс-43 // Ternopil, 2024 // P. 67, fig. - 34, tab. - 0, chair. - 14, added. – 0.

Keywords: VMware, ESXi, OPNsense, OpenVPN, NAT, Hypervisor, Virtualization, Windows, Firewall.

The bachelor's thesis is devoted to the study of virtualization technology and the implementation of a protected corporate infrastructure based on the VMware ESXi hypervisor. A detailed review of various virtualization technologies and their capabilities for creating secure corporate environments has been conducted. VMware ESXi hypervisor has been installed and configured, which serves as the basis for creating virtual infrastructures. Installed and configured the OPNsense VM as a router with OpenVPN, NAT, DNS, DHCP server and firewall. The process of installing and configuring the Windows Server 2022 operating system as an enterprise server with RDP support is done. Mechanisms for creating and configuring encrypted VPN connections between corporate infrastructure and client devices have been developed.

A series of tests was performed to check the efficiency and reliability of the created system, which confirmed its high level of functionality. The results of this study will contribute to the creation of secure corporate networks, providing a high level of protection for VPN connections.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ОС	—	Операційна система
GUI	—	Graphical User Interface
SI	—	Stateful Inspection
NAT	—	Network Address Translation
DCUI	—	Direct Console User Interface
UDP	—	User Datagram Protocol
DoS	—	Denial of Service
DDoS	—	Distributed Denial of Service
LAN	—	Local Area Network
WAN	—	Wide Area Network
VMM	—	Virtual Machine Monitor
TCP	—	Transmission Control Protocol
VMX	—	Virtual Machine Extensions
CIM	—	Common Information Model
DHCP	—	Dynamic Host Configuration Protocol
NTP	—	Network Time Protocol
SNMP	—	Simple Network Management Protocol
EPT	—	Extended Page Tables
SVM	—	Secure Virtual Machine
NPT	—	Nested Page Tables
VM	—	Virtual Machine
VPN	—	Virtual Private Network
DNS	—	Domain Name System
CA	—	Certificate Authority
SSL	—	Secure Sockets Layer
TLS	—	Transport Layer Security
AES	—	Advanced Encryption Standard
GCM	—	Galois/Counter Mode

AEAD	—	Authenticated Encryption with Associated Data
SHA	—	Secure Hash Algorithms
RDP	—	Remote Desktop Protoco
EMI	—	Електромагнітний імпульс
ЕМП	—	Електромагнітне поле

ВСТУП

Стрімкий розвиток інформаційних технологій загострив питання забезпечення безпеки корпоративних мереж та IT-інфраструктури в цілому. Зловмисники постійно вдосконалюють свої методи атак, і тому створення ефективної та захищеної корпоративної IT-інфраструктури є актуальним завданням для багатьох підприємств та організацій.

Метою даного дослідження є розробка та реалізація заходів щодо створення захищеної корпоративної інфраструктури на основі гіпервізора VMware ESXi. Для досягнення цієї мети потрібно вирішити наступні завдання:

- огляд та аналіз існуючих технологій віртуалізації та їхніх можливостей для створення безпечних корпоративних середовищ;
- встановлення та конфігурація гіпервізора VMware ESXi;
- встановлення та конфігурація віртуальних машин OPNsense для використання як маршрутизатора з підтримкою OpenVPN, NAT та брандмауера;
- встановлення та налаштування Windows Server 2022 як корпоративного сервера з підтримкою RDP;
- створення та налаштування VPN-з'єднань між корпоративною інфраструктурою та клієнтськими пристроями;
- проведення тестів для перевірки ефективності та надійності створеної системи.

Об’єктом дослідження є процес створення та налаштування захищеної корпоративної інфраструктури на основі гіпервізора.

Предметом дослідження є методи та засоби створення та налаштування захищеної корпоративної інфраструктури на основі гіпервізора VMware ESXi з використанням віртуальних машин OPNsense та Windows Server 2022.

Результати даного дослідження матимуть велике практичне значення для організацій та підприємств, які прагнуть забезпечити високий рівень безпеки своїх корпоративних мереж. Оптимізація та захист інфраструктури від сучасних загроз дозволить забезпечити надійну роботу та конфіденційність інформації.

РОЗДІЛ 1 ОГЛЯД ТЕХНОЛОГІЙ

1.1 Огляд технології віртуалізації

Віртуалізація — це ключова технологія, яка змінила спосіб, яким ми підходимо до розгортання та управління обчислювальними ресурсами. Вона є визначальною технологією в інформаційних середовищах, яка дозволяє ефективно використовувати ресурси та спрощує управління обчислювальною інфраструктурою. Головною складовою віртуалізації є гіпервізори, які поділяються на два основні типи: тип 1 (native) та тип 2 (hosted) [1].

Гіпервізор типу 2, відомий як гіпервізор, що працює поверх операційної системи, це програмне забезпечення, яке встановлюється на операційну систему хоста та дозволяє віртуалізувати операційні системи в межах цієї ОС (див.рисунок1.1).

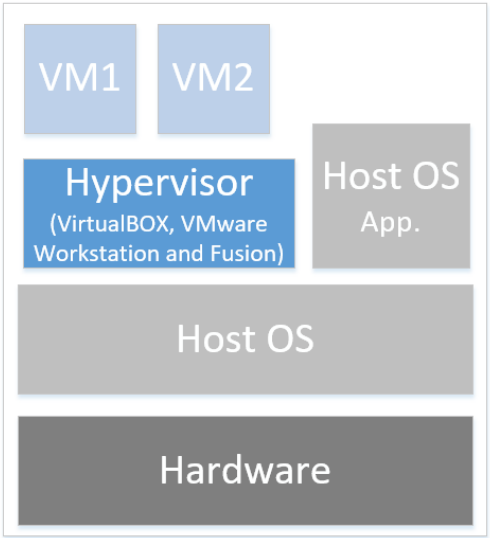

Рисунок 1.1 - Гіпервізор тип 2

Гіпервізор типу 2 використовується переважно для розробки, тестування та експериментів на локальних робочих станціях. Він потребує операційної системи хоста для своєї роботи. Він взаємодіє з ОС для взаємодії з апаратним забезпеченням. Оскільки гіпервізор працює поверх операційної системи, це

може призвести до певного надмірного навантаження (overhead) та впливу на продуктивність порівняно з гіпервізором типу 1.

Даний тип гіпервізору надає інтерфейс користувача для управління віртуальними машинами. Це може бути графічний інтерфейс або командний рядок. Рівень ізоляції та безпеки залежить від безпеки операційної системи хоста. Якщо ОС хоста скомпрометована, це може вплинути на безпеку віртуальних машин. Гіпервізор типу 2 часто використовується розробниками та тестувальниками для швидкої і легкої роботи з віртуальними середовищами без необхідності установки гіпервізора типу 1. Масштабованість гіпервізора типу 2 обмежена ресурсами ОС хоста та не досягає такого рівня, як у випадку гіпервізора типу 1.

Існує багато виробників гіпервізорів типу 2, які призначені для використання на робочих станціях та локальних системах для віртуалізації операційних систем. Найбільш розповсюджені це Oracle VirtualBox, VMware Workstation Pro, VMware Workstation Player, VMware Fusion for MacOS, Parallels Desktop for MacOS.

Oracle VirtualBox є безкоштовним гіпервізором типу 2, розробленим компанією Oracle [2]. Він надає можливість віртуалізації різних операційних систем на одному фізичному комп'ютері. VirtualBox підтримує широкий спектр гостьових операційних систем, включаючи Windows, Linux, macOS, BSD, Solaris та інші. VirtualBox доступний для Windows, Linux, macOS та Solaris. Має графічний інтерфейс користувача (GUI) та можливість управління через командний рядок. Встановлення VirtualBox досить просте та інтуїтивно зрозуміле. Він надає графічний інтерфейс для конфігурації віртуальних машин.

VirtualBox надає розширені можливості конфігурації, включаючи віртуальні процесори, обсяги пам'яті, мережеві параметри та інші налаштування. Механізм снапшотів дозволяє створювати та відновлювати точки віртуальної машини на різних етапах. Гіпервізор дозволяє легко створювати копії віртуальних машин (клони) для різних використань. VirtualBox підтримує віртуалізацію 3D графіки для покращення продуктивності та сприяння графічним застосункам. VirtualBox підтримує різні режими роботи мережі,

включаючи NAT, Host-Only та Bridged Networking, що дозволяє гнучко налаштовувати з'єднання між віртуальними та реальними мережами.

Також гіпервізор дозволяє обмінюватися файлами та текстом між гостьовою та хост-операційною системами. VirtualBox має активну спільноту користувачів, а також офіційну документацію та форуми підтримки.

Oracle VirtualBox є добре відомим та популярним гіпервізором, особливо серед індивідуальних користувачів, розробників та тестувальників. Завдяки своїм розширеним можливостям та відкритій природі, він широко використовується для різних цілей віртуалізації.

VMware Workstation Pro є комерційним гіпервізором типу 2, розробленим компанією VMware [3]. Гіпервізор підтримує велику кількість гостьових операційних систем, включаючи різні версії Windows, Linux, macOS, та інші. Надає розширені параметри для конфігурації віртуальних машин, включаючи встановлення кількості процесорів, обсягу пам'яті, та інші характеристики.

Підтримка технологій віртуалізації графіки, таких як DirectX та OpenGL для оптимізованої роботи графічних застосунків віртуальних машин. Надає можливість обмінюватися файлами між гостьовою та хост-операційною системами, а також копіювати-вставляти текст. Запуск віртуальних машин в окремому вікні або в повноекранному режимі, забезпечуючи гнучку інтеграцію з робочим столом.

VMware Workstation Player, також відомий як VMware Player, є безкоштовною версією гіпервізора від VMware [4]. Він призначенмй для індивідуальних користувачів. Гіпервізор має простий та зрозумілий інтерфейс, що робить його ідеальним для неспеціалізованого користувача. Має підтримку різних гостьових операційних систем, включаючи різні версії Windows, Linux та інші. Подібно до версії Pro, VMware Workstation Player дозволяє створювати копії та снапшоти для зручного управління віртуальними машинами.

VMware Fusion - це гіпервізор для операційної системи macOS, який дозволяє віртуалізувати інші операційні системи, такі як Windows чи Linux, на комп'ютерах Mac [5]. Гіпервізор підтримує різні гостьові операційні системи, зокрема різні версії Windows, Linux, BSD та інші.

Є зручна інтеграція з операційною системою macOS та можливість використовувати графічні прискорювачі для оптимізації віртуалізації графічних застосунків. Гіпервізор підтримує функції для обміну інформацією між віртуальною та хостовою системами, включаючи копіювання-вставлання тексту та файлів.

Всі ці гіпервізори від VMware надають різні рівні функціональності та призначені для різних користувацьких потреб. VMware Workstation Pro та VMware Fusion дозволяють професіоналам віртуалізації широко використовувати функції віртуалізації, тоді як VMware Workstation Player надає безкоштовний варіант для індивідуальних користувачів.

Parallels Desktop - це гіпервізор тип 2 для операційної системи macOS, призначений для віртуалізації інших операційних систем, зокрема Windows та різних дистрибутивів Linux, на комп'ютерах Mac [6].

Гіпервізор підтримує широкий спектр операційних систем, включаючи різні версії Windows, Linux, macOS та інші. Забезпечує ефективну інтеграцію з операційною системою macOS, включаючи обмін файлами.

Надає можливість використовувати графічні прискорювачі для оптимізації віртуалізації графічних застосунків, включаючи 3D-графіку.

Надає ідеальне середовище для тестування програмного забезпечення на різних операційних системах без необхідності фізичних пристроїв.

Забезпечує безпечного та ізольованого середовища для віртуальних машин, що допомагає захистити основну операційну систему.

Parallels Desktop є однією з популярних опцій для користувачів Mac, які потребують віртуалізації для запуску Windows чи інших операційних систем на своєму комп'ютері Mac. Він надає широкий функціонал та покращену інтеграцію з операційною системою macOS.

Гіпервізор типу 1 є спеціальною платформою для віртуалізації, яка працює безпосередньо на апаратному рівні фізичного сервера. Цей тип гіпервізора забезпечує найвищу продуктивність та ефективність, оскільки він не використовує операційну систему хоста і взаємодіє прямо з апаратним забезпеченням [7]. Гіпервізор отримує прямий доступ до апаратного

забезпечення сервера, що дозволяє ефективно розподіляти та керувати ресурсами між віртуальними машинами (див.рисунок1.2).

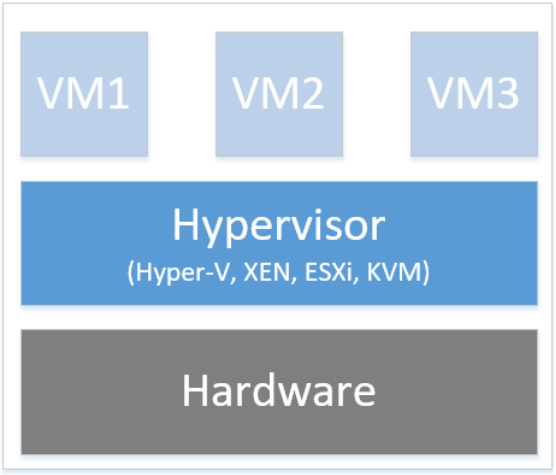

Рисунок 1.2 - Гіпервізор тип 1

Оскільки гіпервізор працює безпосередньо на апаратному рівні, він не має додаткових накладних витрат (overhead), що забезпечує високий рівень продуктивності віртуальних машин.

Гіпервізор тип 1 зазвичай надає централізований інтерфейс для управління віртуальними машинами та ресурсами, що полегшує адміністрування. Він широко використовується в корпоративних-середовищах, де вимагається висока продуктивність та безпека. Великі дата-центри та корпорації використовують даний тип гіпервізорів для роботи віртуальних машин [8].

Найбільш розповсюджені гіпервізори типу 1 це VMware ESXi, Microsoft Hyper-V, XEN та KVM [8].

Гіпервізор типу 1 забезпечує гнучкість у масштабування віртуальних середовищ відповідно до потреб організації. Він є основою для побудови великих та високоефективних інфраструктур віртуалізації, надаючи стабільність, безпеку та продуктивність в обробці віртуальних машин на різних рівнях складності та масштабів.

1.2 Огляд принципів роботи брандмауера

Брандмауер - це програмне або апаратне забезпечення, призначене для захисту комп'ютерної мережі від несанкціонованого доступу, контролю руху даних та запобігання атакам [9].

Фільтрація трафіку є одним з основних принципів роботи брандмауера, спрямованим на контроль і обмеження потоку даних, що переходить через мережевий вузол. Цей процес дозволяє брандмауеру визначати, який мережевий трафік дозволено або заблоковано на основі певних правил. Базовий рівень фільтрації полягає в аналізі мережевих пакетів даних. Пакети - це невеликі блоки інформації, які передаються через мережу. Брандмауер аналізує заголовки та дані кожного пакета і приймає рішення щодо того, чи дозволити, чи заборонити його передачу в мережі. Брандмауер може фільтрувати трафік в залежності від його джерела та призначення. Наприклад, можливо встановити правило, що блокує певні IP-адреси або дозволяє тільки зазначені адреси. Адміністратор встановлює правила для фільтрації трафіку. Ці правила вказують, як брандмауер повинен обробляти різні види трафіку. Правила можуть враховувати різні параметри, такі як порти, протоколи, IP-адреси тощо. Брандмауер може блокувати або дозволяти трафік на основі номерів портів, які використовуються для ідентифікації конкретних служб. Фільтрація може бути здійснена на рівні мережевих протоколів. Брандмауер може дозволяти або блокувати певні мережеві протоколи, такі як TCP, UDP, ICMP тощо.

Stateful Inspection, або динамічна фільтрація, є продвинутою технікою фільтрації трафіку в брандмауерах. Цей метод аналізує не лише окремі пакети даних, але і визначає контекст та стан з'єднання. SI відстежує стан з'єднань, що проходять через брандмауер. Кожен мережевий пакет аналізується не лише ізольовано, але й в контексті його відношення до існуючих з'єднань. Для ведення відстеження використовується таблиця стану (State Table), де зберігається інформація про активні з'єднання, включаючи IP-адреси, порти, стани та інші характеристики. SI проводить двосторонній аналіз пакетів, що включає

врахування як вхідного, так і вихідного трафіку. Це дозволяє брандмауеру визначати стан кожного з'єднання.

Якщо в процесі передачі даних стан з'єднання змінюється (наприклад, відбувається встановлення нового з'єднання або завершення існуючого), брандмауер аналізує ці зміни та приймає відповідні рішення щодо дозволу або блокування трафіку. SI може використовуватися для аналізу та відстеження стану з'єднань на рівні протоколів вищих рівнів, таких як TCP, UDP або додаткові протоколи, що використовуються в додатках.

Брандмауер, що використовує SI, забезпечує, що тільки трафік, який відповідає легітимним з'єднанням і не порушує правила безпеки, проходить через фільтрацію.

NAT - це техніка, що використовується в брандмауерах та маршрутизаторах для перетворення IP-адрес, що використовуються в одній мережі, в інші IP-адреси при передачі трафіку через мережевий пристрій. Багато компаній використовують приватні IP-адреси у своїх внутрішніх мережах. NAT дозволяє приховати ці приватні адреси за публічними IP-адресами, що дозволяє пристроям у внутрішній мережі взаємодіяти з інтернетом чи іншими мережами. NAT надає певний рівень захисту внутрішньої мережі, оскільки приховує приватні адреси та ускладнює прямий доступ зовнішнім пристроям. Використання NAT дозволяє економити публічні IP-адреси, оскільки внутрішні пристрої можуть використовувати одну або кілька публічних IP-адрес.

Технологія NAT у брандмауері грає ключову роль у забезпеченні ефективного використання IP-адрес та захисту внутрішньої мережі від прямого доступу зовнішніх пристроїв.

Журналювання і моніторинг в брандмауері є одним з компонентів для ефективного виявлення та вирішення проблем безпеки мережі. Ці функції дозволяють адміністраторам вести журнали подій, аналізувати трафік та виявляти потенційні загрози.

Брандмауер зазвичай веде журнали подій, де фіксується важлива інформація про трафік, правила фільтрації, атаки, використання ресурсів та інші події. Ці журнали можуть бути використані для аналізу та виявлення аномалій. Також

брандмауер може надавати інтерфейс для моніторингу мережевого трафіку в режимі реального часу. Це дозволяє адміністраторам бачити, який трафік проходить через мережу, і вчасно реагувати на небезпечні ситуації.

Адміністратори можуть аналізувати журнали подій для виявлення патернів, атак чи непередбачуваних подій. Це дозволяє вчасно виявляти загрози безпеки та вживати відповідні заходи. Брандмауер може підтримувати системи сповіщень, які повідомляють адміністраторів про події, що вимагають їхньої уваги. Це важливо для оперативного реагування на проблеми безпеки.

Журнали подій та моніторинг трафіку використовуються для виявлення інцидентів безпеки, таких як атаки, витоки даних або інші небезпечні події. Журнали можуть включати інформацію про те, які правила фільтрації були застосовані до конкретного трафіку. Це допомагає адміністраторам перевіряти та налаштовувати правила для оптимального захисту мережі. Аналіз журналів та моніторинг трафіку дозволяють брандмауеру виявляти та запобігати різним видам мережевих нападів, таких як злам, витік інформації, DoS або DDoS атаки. Журнали подій зазвичай зберігаються протягом певного періоду часу. Це може бути важливим для аналізу історії подій та відстеження тривалості відмов чи атак.

Журналювання і моніторинг в брандмауері є необхідною складовою для забезпечення ефективної безпеки мережі та вчасного реагування на потенційні загрози.

1.3 Інтеграція брандмауерів в віртуалізовані середовища

Інтеграція брандмауерів в віртуальні середовища стає ключовим аспектом для забезпечення безпеки віртуалізованого інфраструктурного середовища.

Основний момент це вибір гіпервізора типу 1, який може ефективно працювати з віртуальними брандмауерами. Популярні гіпервізори, такі як VMware ESXi, Microsoft Hyper-V чи KVM, мають розширений функціонал для роботи з віртуальними мережами та брандмауерами.

Створення віртуальних машин для брандмауерів у гіпервізорі з необхідними ресурсами та налаштуваннями розпочинається з визначення параметрів, таких як обсяги пам'яті, кількість ядер процесора, та мережеві налаштування [10]. Налаштування мережевої інтеграції для взаємодії віртуальної машини брандмауера та інших віртуальних об'єктів у інфраструктурі потребує визначення мережевих інтерфейсів, налаштування VLAN та інших параметрів.

Розробка стратегії регулярного резервного копіювання конфігурацій та стану віртуальних брандмауерів, а також процедур відновлення у випадку виникнення непередбачуваних ситуацій чи втрати конфігурацій є важливим моментом інтеграції.

Інтеграція брандмауерів як віртуальних машин в віртуальні середовища дозволяє ефективно захищати та управляти віртуальною інфраструктурою, забезпечуючи безпеку та контроль над мережевим трафіком.

1.4 Висновки до розділу

В першому розділі було проведено огляд технології віртуалізації. Було досліджено гіпервізори типу 1 та 2 та їх можливості що до запуску та управління віртуальними машинами. Показано що технології віртуалізації дозволяють ефективно використовувати апаратне забезпечення, полегшують масштабування та забезпечують зручне тестування та розгортання програмного забезпечення.

Проаналізовано роль брандмауера, як важливого компонента мережевої безпеки, який використовується для фільтрації трафіку між мережами та захисту від потенційних загроз. Досліджено принципи роботи брандмауера включають фільтрацію трафіку, виявлення та блокування небезпечних з'єднань, використання правил та політик безпеки. Досліджено використання функцій, таких як NAT, проксі-сервер, фільтрація трафіку та журналювання подій для створення ефективного захисного шару для мережі та забезпечення контролю над мережевими з'єднаннями.

Проаналізовано можливість інтеграції брандмауерів в віртуальні середовища для забезпечення безпеку корпоративній інфраструктурі.

РОЗДІЛ 2 ЗАСОБИ СТВОРЕННЯ КОРПОРАТИВНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ГІПЕРВІЗОРА

2.1 Архітектура та особливості роботи гіпервізора VMware ESXi

2.1.1 Огляд гіпервізора VMware ESXi

VMware ESXi є високоефективним гіпервізором, розробленим компанією VMware для віртуалізації обчислювальних ресурсів [11]. VMware ESXi відноситься до гіпервізорів типу 1, що означає, що він працює безпосередньо на апаратному забезпеченні сервера без необхідності встановлення операційної системи хоста. Це забезпечує оптимальну продуктивність та ефективне використання ресурсів [12].

Гіпервізор надає інтерфейс для створення нових віртуальних машин. Адміністратор може визначити параметри, такі як обсяги пам'яті, обчислювальна потужність, кількість процесорів та обсяги зберігання для кожної віртуальної машини. Кожна віртуальна машина використовує власне віртуальне середовище, що забезпечує ізоляцію між віртуальними машинами. Крім того, VMware ESXi підтримує механізми для розподілу та призначення обчислювальних та мережевих ресурсів. VMware ESXi підтримує широкий спектр операційних систем, включаючи різні версії Windows, Linux, Unix та інші. Це дозволяє використовувати різноманітні ОС в межах віртуального середовища.

Адміністратори можуть створювати шаблони віртуальних машин, які визначають конфігурацію та параметри. Це дозволяє швидко розгортати нові віртуальні машини з попередньо визначеними налаштуваннями. Гіпервізор також підтримує збереження стану віртуальних машин, що дозволяє швидко відновити їх стан після відключення або аварії.

Гіпервізор VMware ESXi забезпечує безпечну взаємодію віртуальних машин між собою та з мережею. Для цього використовуються віртуальні комутатори та ізольовані мережеві сегменти.

Установка та використання VMware Tools відкриває доступ до додаткових функцій та драйверів, що поліпшують взаємодію між гостьовою операційною системою та гіпервізором.

Підтримка віртуальних машин у VMware ESXi робить його потужним інструментом для віртуалізації, забезпечуючи адміністраторам гнучкість, масштабованість та надійність у керуванні віртуальною інфраструктурою.

Масштабованість в VMware ESXi визначає його здатність ефективно вирішувати завдання віртуалізації при зростанні об'єму ресурсів та завдань. Велика масштабованість дозволяє платформі працювати інтенсивно в умовах великої кількості віртуальних машин, серверів та обчислювальних завдань.

VMware ESXi підтримує велику кількість віртуальних машин на одному сервері. Це дозволяє адміністраторам гнучко розгортати та керувати сотнями, а навіть тисячами віртуальних машин на кластерах серверів.

Для масштабованості використовується концепція кластерів, яка дозволяє об'єднувати фізичні сервери в єдиний кластер. VMware ESXi використовує розподіл ресурсів та систему кластерів, таку як Distributed Resource Scheduler (DRS), для оптимізації розміщення віртуальних машин та забезпечення рівномірного розподілу навантаження. VMware ESXi використовує технології, такі як vSphere High Availability (HA) та vSphere Fault Tolerance (FT), для забезпечення надійності та високої доступності віртуальних машин в умовах масштабування кластера.

Для ефективного використання обчислювальних ресурсів VMware ESXi використовує технології, такі як vMotion та DRS. Міграція та динамічне управління ресурсами - це концепції, які забезпечують ефективне використання обчислювальних ресурсів та оптимізацію віртуального середовища у VMware ESXi.

Технологія vMotion дозволяє живу міграцію віртуальних машин між фізичними серверами без припинення їх роботи. Забезпечує надійність та високу доступність, дозволяючи переміщати віртуальні машини для уникнення відмови обладнання. Дозволяє оптимізувати розподіл ресурсів та навантаження в кластері серверів. Забезпечує виконання ряду адміністративних завдань, таких

як резервне копіювання та обслуговування серверів без припинення роботи віртуальних машин.

Технологія Storage vMotion використовується для переміщення віртуальних машин між сховищами даних без відключення. Дозволяє оптимізувати використання зберігання, переміщуючи дані віртуальних машин між різними сховищами. Забезпечує гнучкість управління даними та зменшує необхідність відключення віртуальних машин під час переміщення.

Distributed Resource Scheduler (DRS) використовується для автоматичного розподілу та балансування ресурсів віртуальних машин в межах кластера серверів. Технологія дозволяє автоматично визначати і оптимізувати розташування віртуальних машин відносно ресурсів та завдань. Забезпечує підтримку та виконання політик віртуального середовища. Призначає та перерозподіляє віртуальні машини для забезпечення рівномірного розподілу навантаження.

Resource Pools дозволяють групувати та управляти ресурсами віртуальних машин відповідно до конкретних вимог або пріоритетів. Дозволяє визначати обмеження та пріоритети для груп віртуальних машин. Допомагає управляти та контролювати виділення ресурсів для різних додатків.

Ці функції роблять VMware ESXi дуже ефективним інструментом для управління ресурсами та забезпечення високої доступності віртуального середовища. Вони дозволяють адміністраторам автоматизувати та оптимізувати роботу великих кластерів серверів, забезпечуючи високий рівень продуктивності та доступності віртуальних машин.

VMware ESXi також масштабується в сфері зберігання за допомогою технологій, таких як VMware vSAN. Вони дозволяють підключати та масштабувати сховища даних для задоволення вимог обсягу і доступності.

VMware ESXi також інтегрується з хмарними рішеннями, такими як VMware Cloud on AWS, що дозволяє масштабувати інфраструктуру в хмарі та легко переміщати віртуальні машини між локальними серверами та хмарними ресурсами.

Масштабованість в VMware ESXi визначається не лише здатністю підтримувати велику кількість віртуальних машин, але й забезпечити ефективне використання та управління ресурсами в умовах зростання обчислювальних завдань.

2.1.2 Архітектура VMware ESXi

Архітектура VMware ESXi визначає структуру та взаємодію компонентів для забезпечення віртуалізації [11]. Архітектура є основою оптимізації продуктивності та безпеки віртуальних машин та включає оперційну систему, що називається VMKernel, та процеси. VMKernel надає засоби для запуску всіх процесів у системі, включаючи програми управління та агенти, а також віртуальні машини. Вона має контроль над усіма апаратними пристроями на сервері та керує ресурсами для додатків.

Основними процесами, що працюють поверх VMKernel є:

- Інтерфейс користувача прямої консолі (DCUI) - інтерфейс конфігурації та управління низьким рівнем, доступний через консоль сервера, що використовується насамперед для початкової базової конфігурації.

- Монітор віртуальної машини (VMM), який є процесом, який забезпечує середовище виконання для віртуальної машини, а також процес-помічник, відомий як VMX. Кожна запущена віртуальна машина має власний процес VMM та VMX.

- Різні агенти, які використовуються для забезпечення високого рівня управління інфраструктурою VMware з віддалених додатків.

- Загальна інформаційна модель (CIM) - це інтерфейс, який дозволяє керувати рівнем апаратного забезпечення з віддалених програм за допомогою набору стандартних API.

На рисунку 2.1 показана схема загальної архітектури ESXi.

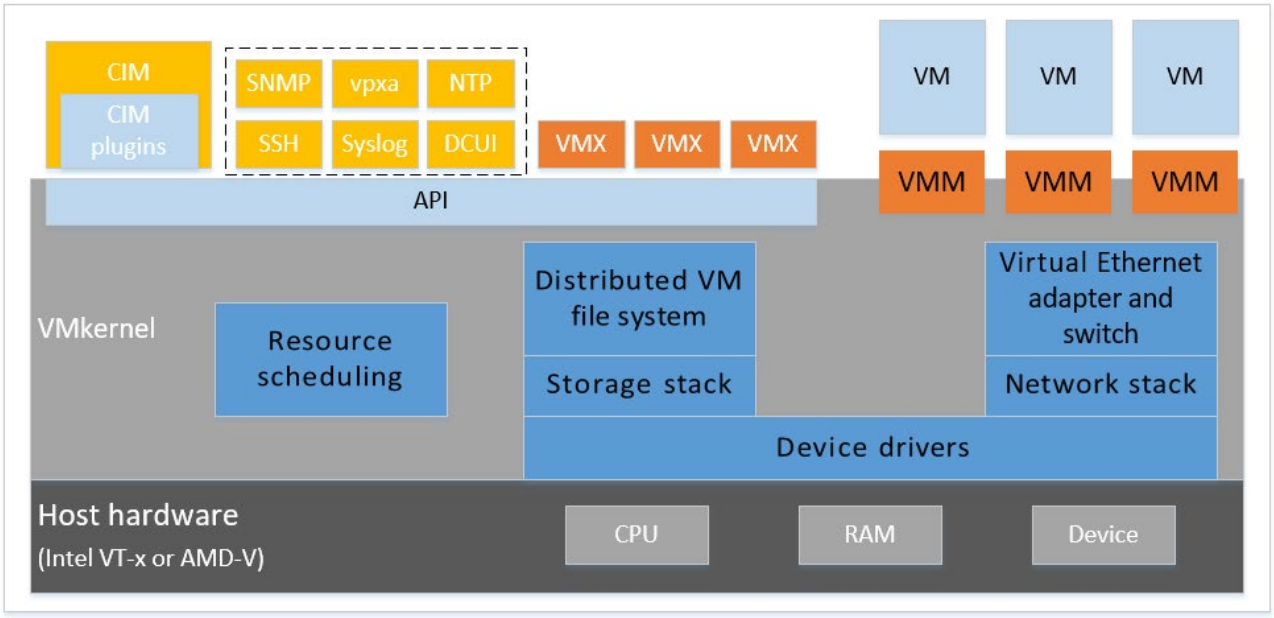

Рисунок 2.1 – Загальна архітектура гіпервізора ESXi

VMKernel - це операційна система, схожа на POSIX, розроблена VMware, і забезпечує певну функціональність, подібну до того, що в інших операційних системах, таку як створення та управління процесами, сигнали, файлова система та потоки процесів. Вона розроблений спеціально для підтримки запуску багатьох віртуальних машин та забезпечує таку основну функціональність, як:

- планування ресурсів;
- стек вводу/виводу (I/O);
- драйвери пристрою.

VMKernel використовує просту файлову систему в пам'яті для зберігання файлів конфігурації ESXi, файлів журналів та поетапних патчів. Конфігурації ESXi знаходяться у /etc/vmware, а файли журналу знаходяться в/var/log/vmware. Поетапні патчі завантажуються на /tmp (див. рисунок 2.2).

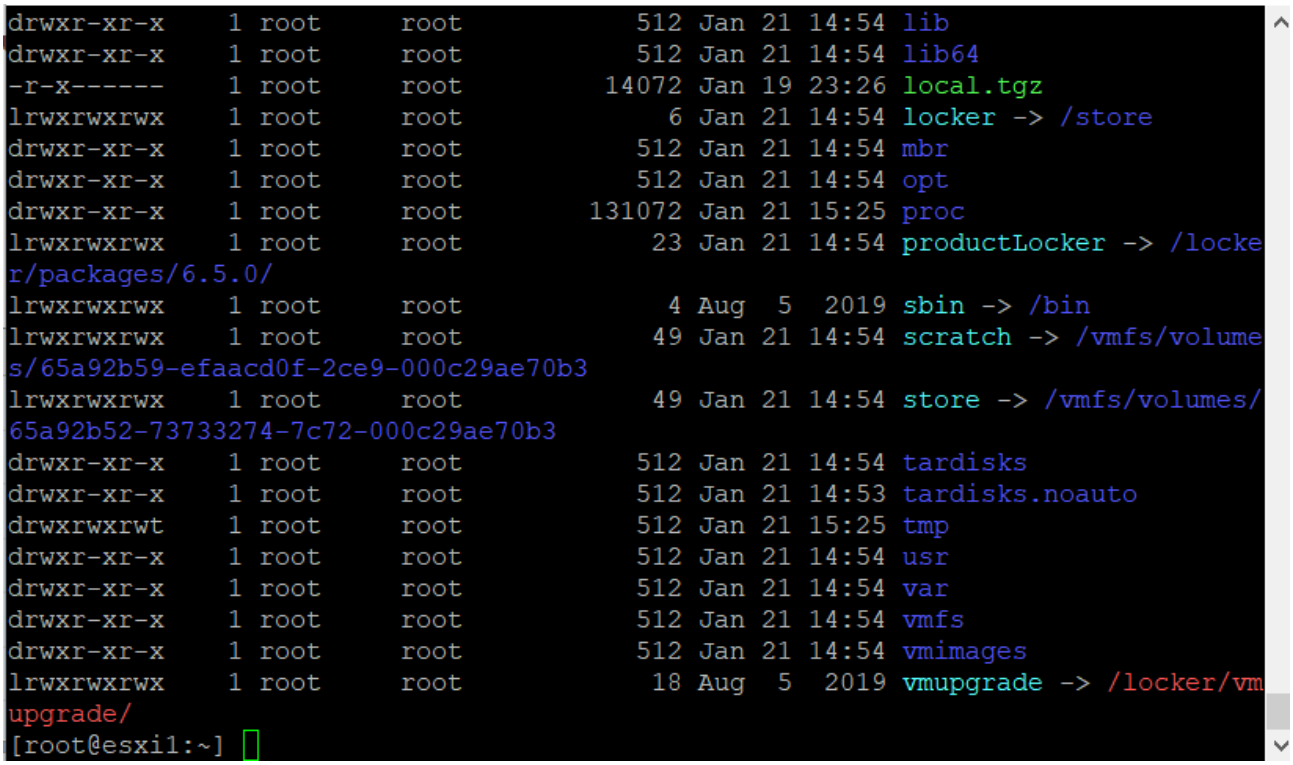

Рисунок 2.2 – Файлова система гіпервізора ESXi

Ця файлова система не залежить від файлової системи VMware VMFS, яка використовується для зберігання віртуальних машин. VMware VMFS datastore може бути створений на локальному диску в хост системі або на спільному сховищі. Якщо єдині дані VMFS, які використовуються хостом, знаходяться на зовнішньому спільному сховищі, система ESXi насправді не потребує локального жорсткого диска. Запускаючи бездискові установки, ви можете підвищити надійність, уникаючи збоїв на жорсткому диску та зменшуючи потужність та споживання охолодження.

Інтерфейси віддаленого командного рядка надають можливості управління файлами як для файлової системи в пам'яті, так і для даних VMware VMFS. Доступ до файлової системи реалізується за допомогою HTTPS (див. рисунок 2.3) та автентифікації через користувачів та групи, налаштовані локально на сервері.

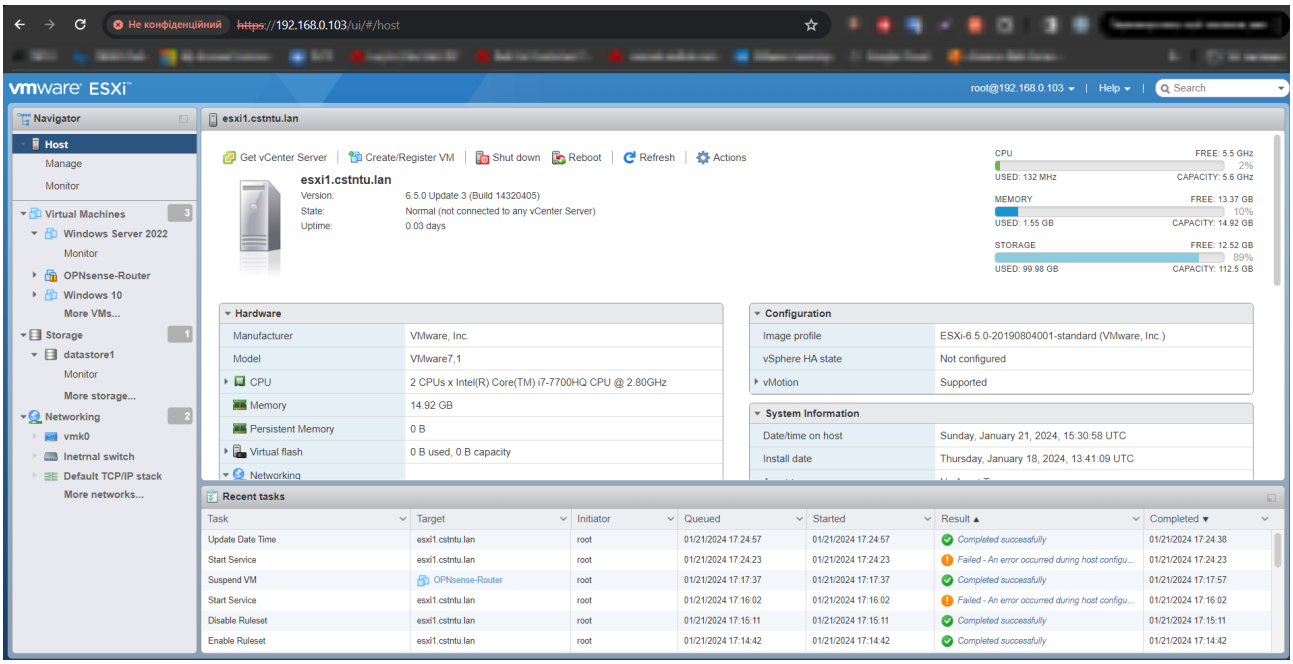

Рисунок 2.3 – Вебінтерфейс управління гіпервізором ESXi

ESXi має можливість налаштувати віддалений сервер Syslog, що дозволяє зберігати всю інформацію про журнал у зовнішній системі.

Користувачі та групи можна визначити локально в системі ESXi. Вони надають спосіб розрізнити користувачів, які отримують доступ до системи через клієнтів віртуальної інфраструктури, інтерфейси віддаленого командного рядка або API.

Групи можуть використовуватися для комбінування декількох користувачів, як і в інших операційних системах. Групи можна використовувати, наприклад, для встановлення привілеїв для багатьох користувачів одночасно. Існує кілька користувачів та груп системи, які заздалегідь визначені для визначення певних процесів, що працюють у VMKernel.

Адміністративні привілеї можна встановити індивідуально для кожного користувача або групи. Визначення користувача та групи зберігаються у файловій системі у файлах /etc/passwd, /etc/shadow, та /etc/group (див. рисунок 2.4). Паролі генеруються за допомогою стандартних криптографічних функцій.

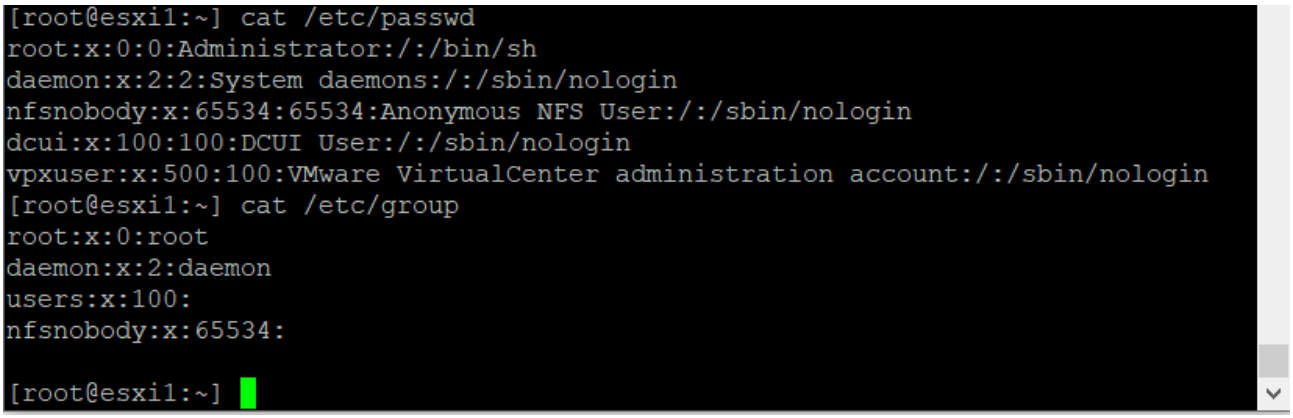

Рисунок 2.4 – Користувачі та групи в ОС VMkernel

Процеси, що виконується в операційній системі VMkernel обмежені порівняно з тим, що є в універсальній POSIX-сумісній операційній системі, такій як Linux. Набір доступних сигналів обмежений, API системи - це підмножина POSIX, файлова система /proc дуже обмежена. Один файл підкачки (swap) доступний для всіх процесів користувачів. Якщо існує локальний диск, файл swap створюється автоматично в невеликому розділі VFAT. В іншому випадку користувач може розмістити файл підкачки на одному з VMFS datastores.

Операційна система VMkernel не призначена для запуску довільних програм, а забезпечує лише достатню структуру для процесів, які повинні виконуватися в середовищі гіпервізора.

Кілька важливих процесів виконуються в користувацькому режимі. Їх можна розглядати як рідні програми VMkernel.

DCUI - це локальний інтерфейс користувача, який відображається лише на консолі системи ESXi (див. рисунок 2.5).

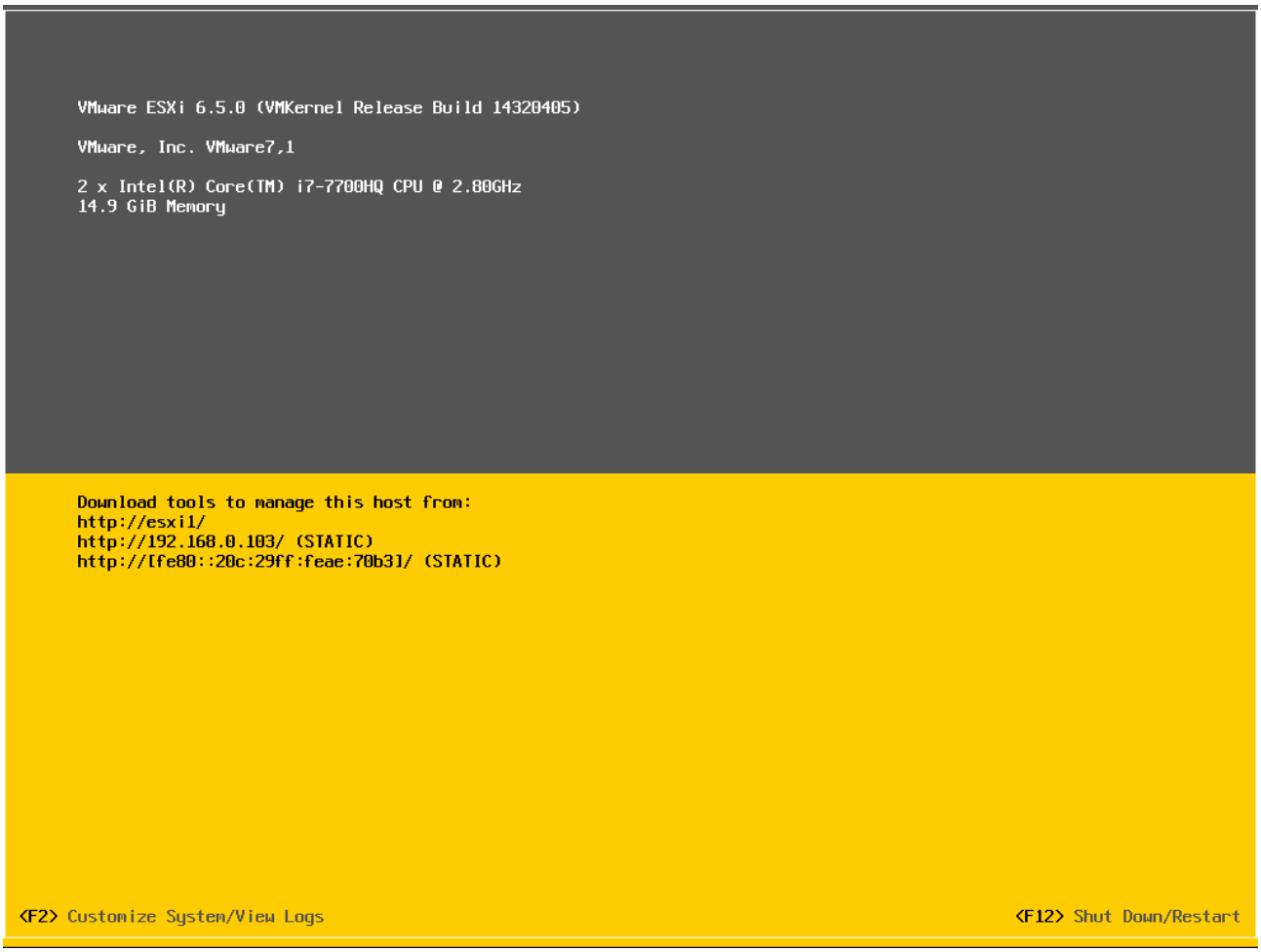

Рисунок 2.5 – Інтерфейс користувача прямої консолі (DCUI)

Він забезпечує інтерфейс, керований меню, для взаємодії з системою. Основна його призначення - початкова конфігурація та усунення несправностей. Одним із користувачів системи, визначеним у VMKernel, є dcui, який використовується процесом DCUI для ідентифікації себе під час спілкування з іншими компонентами в системі.

Завдання конфігурації DCUI включають:

- встановлення адміністративного паролю;

- налаштування мереж, якщо це не робиться автоматично за допомогою DHCP;

- завдань усунення несправностей.

Користувач здійснює мінімальну конфігурацію з DCUI, а потім використовує інструмент віддаленого управління, наприклад, вебінтерфейс або інтерфейси віддаленого командного рядка, щоб виконати всі інші завдання конфігурації та постійні завдання управління.

Кожен, хто використовує DCUI, повинен ввести пароль адміністративного рівня, наприклад, root пароль.

На рисунку 2.6 показано сервіси, які є стандартними в гіпервізорі ESXi.

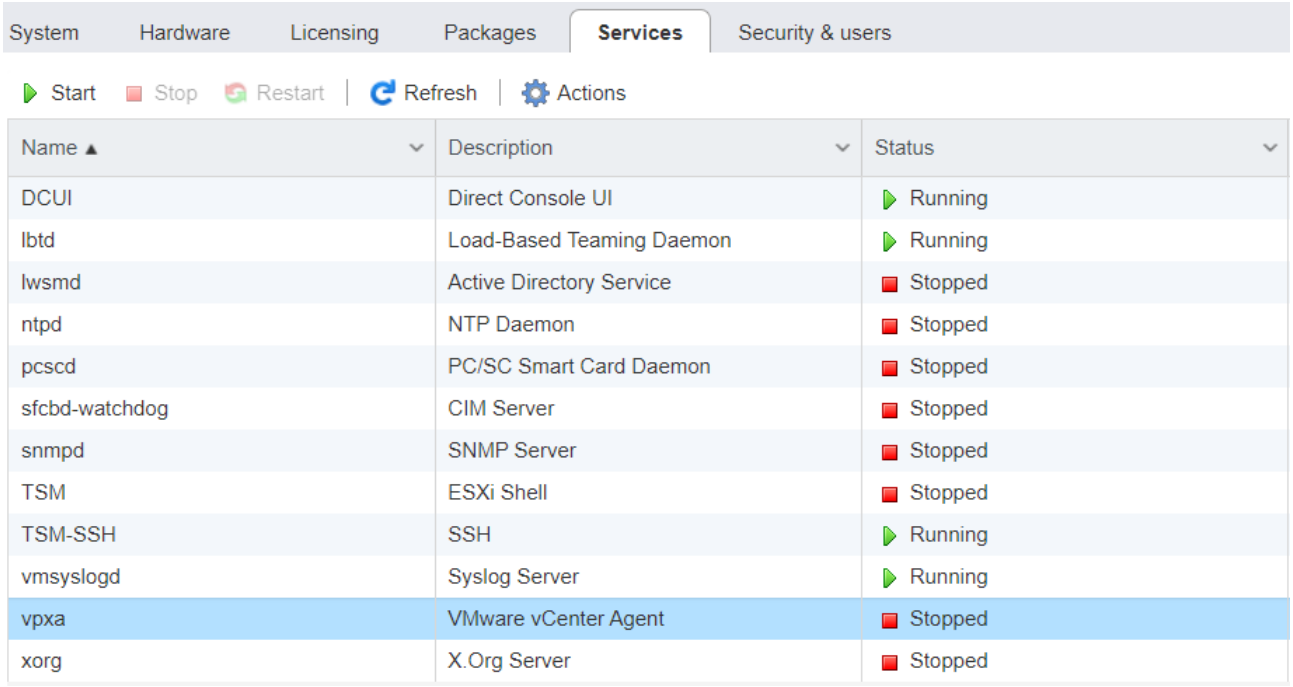

Рисунок 2.6 – Сервіси в гіпервізорі ESXi

Процес hostd забезпечує програмний інтерфейс VMKernel. Процес автентифікує користувачів і відстежує, які користувачі та групи мають привілеї. Це також дозволяє створювати та керувати місцевими користувачами. Процес vpxa - це VMware vCenter Agent, який використовується для підключення до vCenter. Він працює як спеціальний користувач системи під назвою vpxuser. Він виступає посередником між агентом хлста hostd та vCenter.

Демон Syslog передає всі журнали до віддаленої цілі на додаток до розміщення їх у локальних файлах.

Крім того, ESXi має процеси, які дозволяють синхронізацію часу на основі NTP та моніторинг SNMP. Також гіпервізор має обмежену кількість відкритих мережевих портів.

CIM - це відкритий стандарт, який визначає, як можна представити обчислювальні ресурси та керувати ними. Це забезпечує основу для моніторингу

апаратних ресурсів на основі стандартів. Цей framework складається з менеджера об'єктів CIM, який часто називають брокером CIM та набору провайдерів CIM.

Провайдери CIM використовуються як механізм для забезпечення доступу до драйверів пристроїв та основного обладнання. Постачальники апаратних засобів, до яких належать як виробники серверів, так і конкретні постачальники апаратних пристроїв, можуть створювати CIM провайдери для забезпечення моніторингу та управління їх конкретними пристроями. VMware також розробляє CIM провайдерів, які реалізують моніторинг апаратного забезпечення сервера, інфраструктуру зберігання ESXi та ресурси, що стосуються віртуалізації. Ці провайдери працюють всередині системи ESXi, а отже, розроблені як надзвичайно легкі та зосереджені на конкретних завданнях управління. Брокер CIM бере інформацію від усіх провайдерів CIM та представляє її за допомогою стандартних API.

2.1.3 Апаратна віртуалізація Intel та AMD

Апаратна віртуалізація - це технологія, яка дозволяє використовувати апаратне забезпечення комп'ютера для створення та управління віртуальними машинами [13].

Intel Virtualization Technology (VT-x) - це технологія віртуалізації, яку надає компанія Intel. Завдяки VT-x, віртуальна машина може отримувати прямий доступ до апаратних ресурсів процесора, що покращує продуктивність віртуалізованих систем.

Технологія віртуалізації Intel VT-x представляє собою комплекс апаратних інновацій, спрямованих на полегшення створення та управління віртуальними машинами. Цей набір вдосконалень включає в себе VMX та EPT, які спроектовані для максимальної оптимізації продуктивності в області віртуалізованих обчислювальних завдань.

VMX відображає схему взаємодії між гіпервізором та віртуальною машиною, створюючи ефективне віртуальне середовище. Це розширення

архітектури процесора дозволяє оптимально використовувати його ресурси та сприяє безперебійній взаємодії гіпервізора з віртуальними машинами.

EPT, з іншого боку, розширює можливості процесора щодо взаємодії з віртуальною пам'яттю. Ця технологія дозволяє більш ефективно керувати віртуальною пам'яттю та ресурсами, що призводить до підвищення продуктивності віртуалізованих обчислювальних завдань.

Технологія Intel VT-x не лише спрощує створення та керування віртуальними машинами, але й надає надійну базу для оптимізованої та продуктивної роботи віртуалізованих обчислювальних середовищ.

AMD Virtualization (AMD-V) представляє собою аналогічну технологію віртуалізації від компанії AMD, яка спрямована на створення та ефективне управління віртуальними машинами на процесорах від AMD.

В рамках AMD-V важливою особливістю є технологія SVM, яка відповідає за забезпечення безпеки віртуальних машин. SVM дозволяє створювати ізольовані та безпечні віртуальні середовища, зменшуючи ризик витоку інформації між віртуальними машинами та гіпервізором.

Крім того, AMD-V підтримує технологію NPT, яка подібна до EPT в Intel VT-x. NPT сприяє оптимізації взаємодії процесора з віртуальною пам'яттю, полегшуючи керування та доступ до ресурсів віртуальних машин.

AMD Virtualization забезпечує не лише можливість створення та управління віртуальними середовищами на процесорах AMD, але і враховує аспекти безпеки та оптимізації роботи з віртуальною пам'яттю.

Технології VT-x та AMD-V дозволяють працювати віртуальним машинам з більш високою ефективністю, так як вони надають можливість напряму взаємодіяти з апаратним обладнанням. Вони дозволяють віртуальним машинам взаємодіяти з процесором, кешем, пам'яттю та іншими апаратними ресурсами безпосередньо.

Ці технології користуються популярністю в сферах віртуалізації серверів, розробки програмного забезпечення та тестування, де використання віртуальних машин є розповсюдженим підходом для оптимізації ресурсів та забезпечення ізоляції середовищ.

На рисунку 2.7 показано процес перевірити підтримки VT-x або AMD-V на хості ESXi.

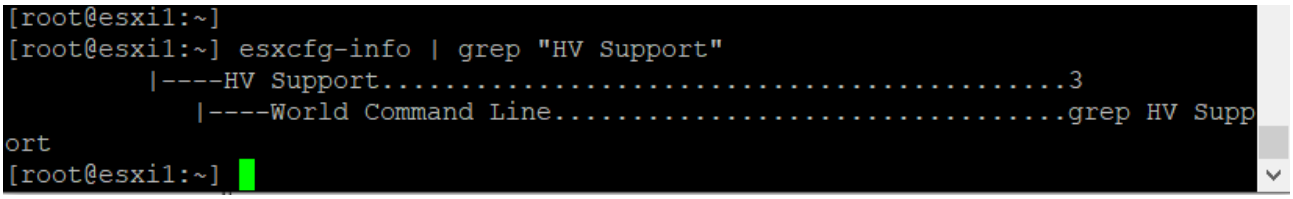

Рисунок 2.7 – Перевірка підтримки апаратної віртуалізації в гіпервізорі ESXi

За результатами виводу команди, можна визначити, що технологія апаратної віртуалізації підтримується на хості ESXi. Рядок "HV Support" із значенням "3" свідчить про те, що апаратна віртуалізація увімкнена.

2.2 Огляд маршрутизатора та брандмауера OPNsense

OPNsense - це високофункціональний маршрутизатор та брандмауер з відкритим кодом, що базується на операційній системі FreeBSD [14]. Він надає багатофункціональність та різноманітні інструменти для керування мережею, забезпечуючи безпеку, оптимізацію трафіку та розширені можливості [15].

На рисунку 2.8 показана інформаційна панель OPNsense.

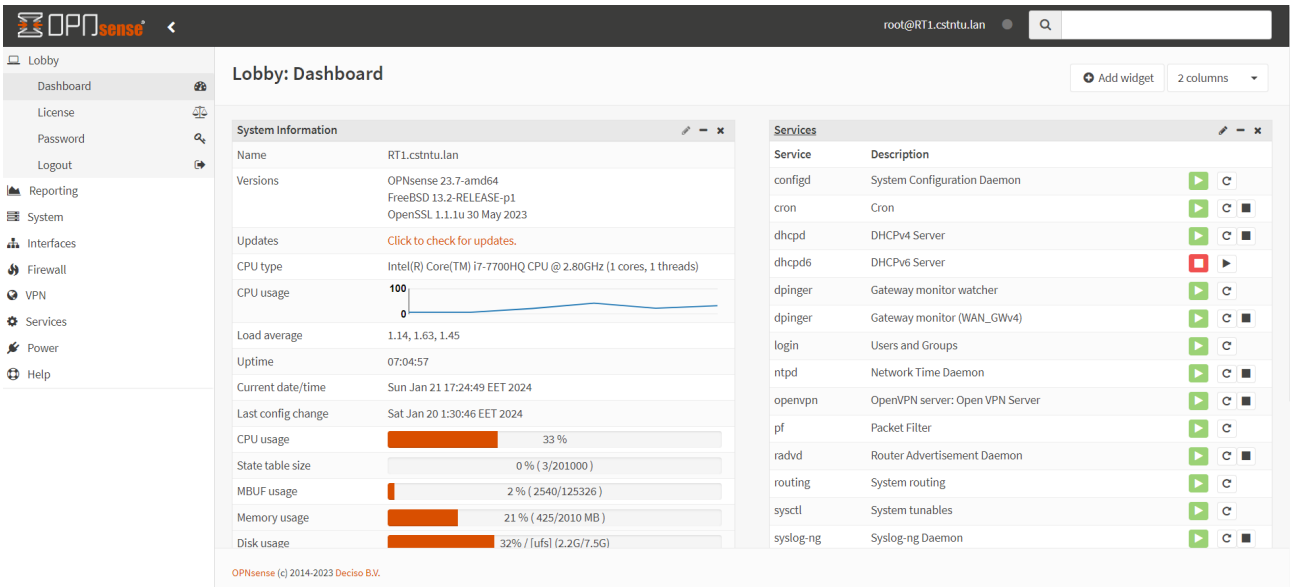

Рисунок 2.8 – Інформаційна панель OPNsense

OPNsense включає в себе stateful inspection firewall, який надає високий рівень безпеки та контролю над мережевим трафіком.

Stateful inspection firewall - це форма брандмауера, яка використовує метод аналізу та відстеження стану мережевого з'єднання для прийняття рішення щодо передачі або блокування трафіку. Цей тип брандмауера відрізняється своєю здатністю розуміти стан кожного мережевого з'єднання та відповідно налаштовувати правила фільтрації трафіку.

Брандмауер має внутрішню таблицю стану для кожного мережевого з'єднання. Це включає інформацію про стани з'єднань, такі як відкриті порти, стан сеансу, та інше. Кожен мережевий пакет, який проходить через брандмауер, аналізується з урахуванням інформації в таблиці стану. Якщо пакет відповідає існуючому стану, він допускається. В іншому випадку, він перевіряється за визначеними правилами. Stateful inspection firewall використовує правила фільтрації, які можуть бути налаштовані адміністратором. Ці правила визначають, які типи трафіку дозволені або заборонені. Stateful Inspection дозволяє брандмауеру приймати рішення про допущення чи блокування трафіку швидше та ефективніше, порівняно з іншими методами фільтрації.

Брандмауер має можливості ведення журналів та моніторингу для відстеження подій та стану брандмауера. Взаємодія з іншими складовими OPNsense, такими як VPN, IDS/IPS, дозволяє створювати комплексні заходи забезпечення безпека мережі.

Traffic shaper в OPNsense є функцією, яка дозволяє контролювати та оптимізовувати мережевий трафік. Основна мета цього інструменту - забезпечити ефективну роботу мережі, надаючи адміністраторам можливість встановлювати пріоритети, обмеження та керувати розподілом пропускної здатності для різних видів даних. Це важливо для забезпечення необхідного рівня обслуговування для різних додатків чи служб.

Можливість встановлювати ліміти для вхідного та вихідного трафіку по види трафіку чи користувачах дозволяє керувати використанням мережевих ресурсів. Вбудовані графіки відображають обсяги трафіку для різних категорій. Це полегшує моніторинг та аналіз використання мережевого трафіку. Traffic

Shaper підтримує можливість планування обмежень пропускної здатності за графіком, а також резервування пропускної здатності для конкретних потреб.

Traffic Shaper в OPNsense є потужним інструментом для управління трафіком, особливо в ситуаціях, де важлива ефективність та пріоритетність використання мережевих ресурсів. Ця функція дозволяє адміністраторам мережі точно налаштовувати та контролювати роботу мережі відповідно до конкретних вимог та завдань.

OPNsense надає розширені можливості для налаштування та управління віртуальними приватними мережами. VPN використовується для створення зашифрованих тунелів через відкриті мережі, щоб забезпечити безпеку та конфіденційність обміну даними між вузлами мережі. OPNsense підтримує різні протоколи VPN, такі як IPsec (включаючи тунельний та транспортний режими), OpenVPN, L2TP/IPsec, та інші.

В маршрутизаторі є можливість налаштовувати site-to-site VPN для безпечного з'єднання між різними мережами організації. Вбудована підтримка віддаленого доступу (remote access VPN) для динамічно змінюючихся вузлів, таких як віддалені працівники. Для забезпечення безпеки обміну даними є можливість вибору різних алгоритмів шифрування та методів аутентифікації та використання сертифікатів або заздалегідь визначених ключів. Маршрутизатор підтримує функціональність розділення тунелю (split tunneling) для регулювання того, який трафік проходить через VPN, а який - напряму через Інтернет.

VPN в OPNsense дозволяє створювати безпечні та ефективні з'єднання між різними вузлами мережі, надаючи адміністраторам повний контроль над параметрами та безпекою VPN-з'єднань.

OPNsense має вбудовані інструменти для обробки запитів DNS, забезпечуючи функції DNS Server та DNS Forwarder. Ці інструменти дозволяють забезпечити ефективну роботу DNS в мережі та швидкість вирішення імен. Маршрутизатор може діяти як локальний DNS-сервер для мережі, надаючи можливість реєстрації та вирішення імен для вузлів у локальній мережі.

Підтримка динамічного оновлення DNS-записів, особливо корисна для динамічних IP-адрес вузлів. Є можливості налаштування захисту від DNS-

спуфінгу та інших атак, пов'язаних із DNS та ведення журналів дій та помилок для аналізу роботи DNS-сервера.

DNS Server та DNS Forwarder в OPNsense надають широкі можливості налаштування та контролю над DNS в мережі, забезпечуючи швидке та надійне вирішення імен та захист від різних загроз.

OPNsense має вбудовані засоби для обробки запитів DHCP, які дозволяють автоматично надавати конфігурацію мережевим пристроям. Це включає в себе DHCP Server для локальних мережевих сегментів та DHCP Relay для пересилання запитів на інший DHCP-сервер.

DHCP Server здійснює автоматичне присвоєння IP-адрес, підмереж, шлюзу, DNS-сервера та інших параметрів мережевої конфігурації пристроям в локальній мережі. Має можливість налаштовувати резервування конкретних IP-адрес для певних пристроїв за їх MAC-адресами. Підтримує контроль часових інтервалів оренди IP-адрес, щоб уникнути конфліктів та забезпечити ефективне використання адрес. Включає в себе можливість налаштовувати DHCP для пристроїв, які підтримують IPv6.

DHCP Relay дозволяє пересилати DHCP-запити від клієнтів до визначеного DHCP-сервера в іншій частині мережі. Є підтримка пересилання DHCPv6-запитів для надання конфігурації IPv6 в мережі. Вбудована можливість визначення конкретних зон для пересилання, щоб керувати тим, які запити пересилаються до DHCP-серверів.

DHCP Server та Relay в OPNsense дозволяють ефективно управляти розподілом IP-адрес та іншою конфігурацією в мережі, спрощуючи процес налаштування та забезпечуючи автоматичну конфігурацію пристроїв.

OPNsense надає вбудовані інструменти для ведення журналів, аналізу та моніторингу мережевої активності. Ці засоби допомагають адміністраторам отримувати інформацію про стан системи, мережі та безпекових подій [13].

Маршрутизатор веде журнали подій (Event Logs), в яких реєструються різноманітні події, такі як блокування трафіку, VPN-з'єднання, зміни конфігурації та інші. Вбудована система RRD Graphs надає графіки та статистику

для різних параметрів, таких як використання пропускної здатності, завантаження системи, робота VPN тунелів та інші (див. рисунок 2.9).

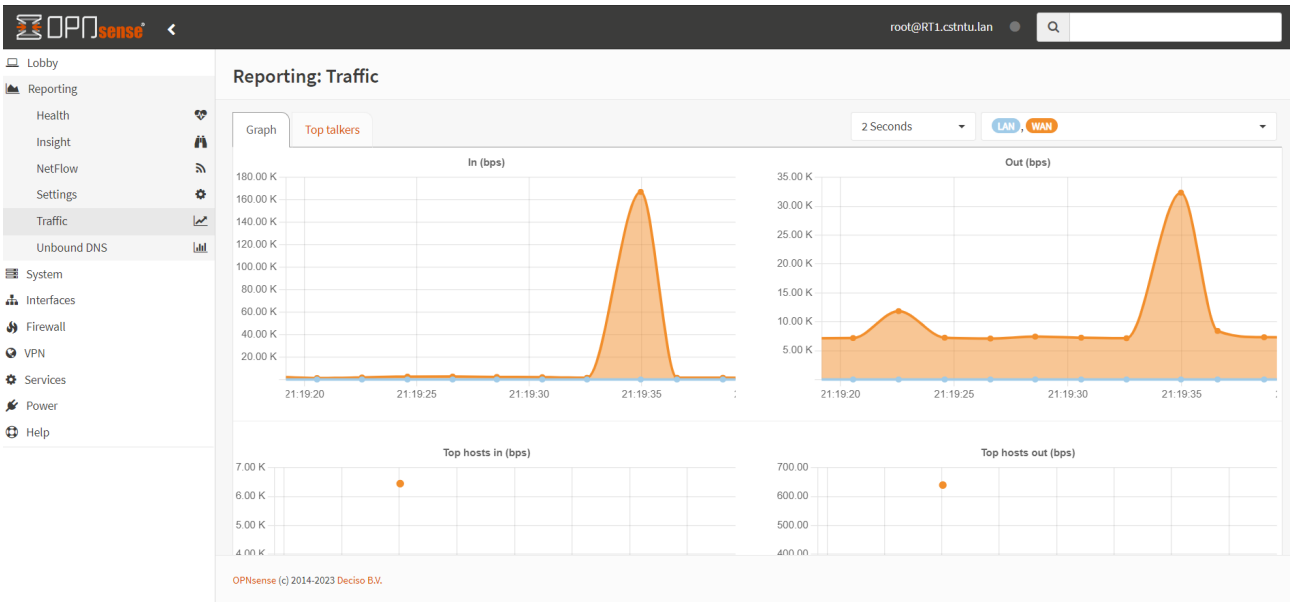

Рисунок 2.9 – Вбудована система відображення статистики в OPNsense

Підтримка Netflow для аналізу та моніторингу мережевого трафіку, включаючи інформацію про вузли та протоколи. Маршрутизатор має інструменти, які надають огляд стану системи, включаючи використання ресурсів, температуру, обсяг вільної пам'яті та інші параметри. Підтримується можливість захоплення пакетів для аналізу мережевого трафіку в реальному часі. Також є можливість налаштування автоматичних сповіщень по електронній пошті чи іншим каналам для важливих подій.

Built-in Reporting and Monitoring Tools в OPNsense дозволяють адміністраторам отримувати комплексну інформацію щодо стану системи та мережі, сприяючи вчасному виявленню проблем та реагуванню на них.

2.3 Висновки до розділу

У другому розділі було висвітлено ключові моменти архітектури та гіпервізора VMware ESXi та його функціональних можливостей. Проведено огляд впливу апаратної віртуалізації Intel VT-x та AMD-V на продуктивність та безпеку віртуалізованого середовища. Intel VT-x та AMD-V виконують ключову

роль у створенні ізольованих віртуальних областей, що дозволяє забезпечити безпеку та ефективність роботи віртуальних машин.

Також був проведений докладний огляд можливостей маршрутизатора та брандмауера OPNsense. OPNsense є потужним інструментом для створення безпечних мережевих інфраструктур, забезпечуючи різноманітні функції, такі як Traffic Shaper, Stateful Inspection Firewall, VPN, DHCP Server та інші.

Комбінація гіпервізора VMware ESXi та брандмауера OPNsense створює дієву та надійну платформу для віртуалізованого корпоративного середовища, яка поєднує в собі ефективність, безпеку та зручність управління.

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ВІРТУАЛІЗОВАНОЇ КОРПОРАТИВНОЇ ІНФРАСТРУКТУРИ

3.1 Схема тестового середовища

На рисунку 3.1 представлена схема лабораторного тестового середовища, яка використана для створення віртуалізованої корпоративної інфраструктури та тестування працездатності.

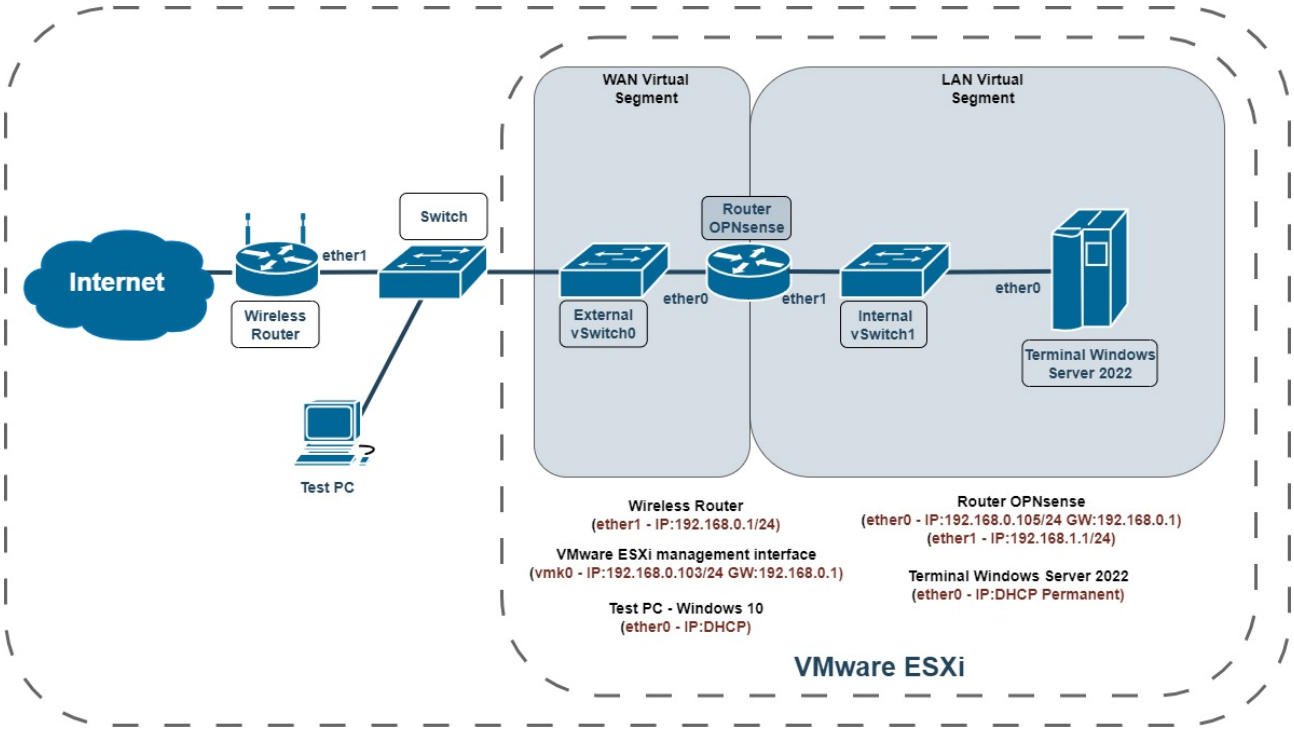

Рисунок 3.1 – Схема лабораторного тестового середовища

Схема включає бездротовий маршрутизатор, який підключений до мережі Інтернет, тестовий ПК, комутатор, а також гіпервізор VMware ESXi з віртуалізованими LAN та WAN сегментами.

WAN віртуалізований сегмент містить маршрутизатор OPNsense з одним зовнішнім мережевим інтерфейсом (ether0), підключеним до зовнішнього віртуального комутатора (External vSwitch0). LAN віртуалізований сегмент включає в себе внітрішній мережевим інтерфейсом (ether1) маршрутизатор OPNsense та сервер Windows Server 2022, які підключені до внутрішнього віртуального комутатора (Internal vSwitch1).

Маршрутизатор Wireless Router має IP-адресу 192.168.0.1/24 та є шлюзом за замовчуванням. VMware ESXi management interface має IP адресу 192.168.0.103/24 (vmk0), і шлюз за замовчуванням 192.168.0.1.

Сервер Windows Server 2022 отримує постійну IP-адресу через DHCP. Тестовий ПК з Windows 10 також отримує IP-адресу через DHCP.

Маршрутизатор OPNsense має дві IP-адреси. Для зовнішнього інтерфейсу (ether0) - 192.168.0.105/24, для внутрішнього інтерфейсу (ether1) - 192.168.1.1/24. OPNsense виконує функції брандмауера, маршрутизатора та VPN концентратора. Управляє трафіком між WAN та LAN віртуалізованими сегментами та забезпечує захисту віртуалізованих серверів.

3.2 Налаштування гіпервізора VMware ESXi

Налаштування гіпервізора VMware ESXi включає кілька етапів, починаючи від установки та завершуючи налаштуванням мережі, вбудованого брандмауера та віртуальних машин [11].

На рисунку 3.2 представлено інтерфейс управління VMware ESXi.

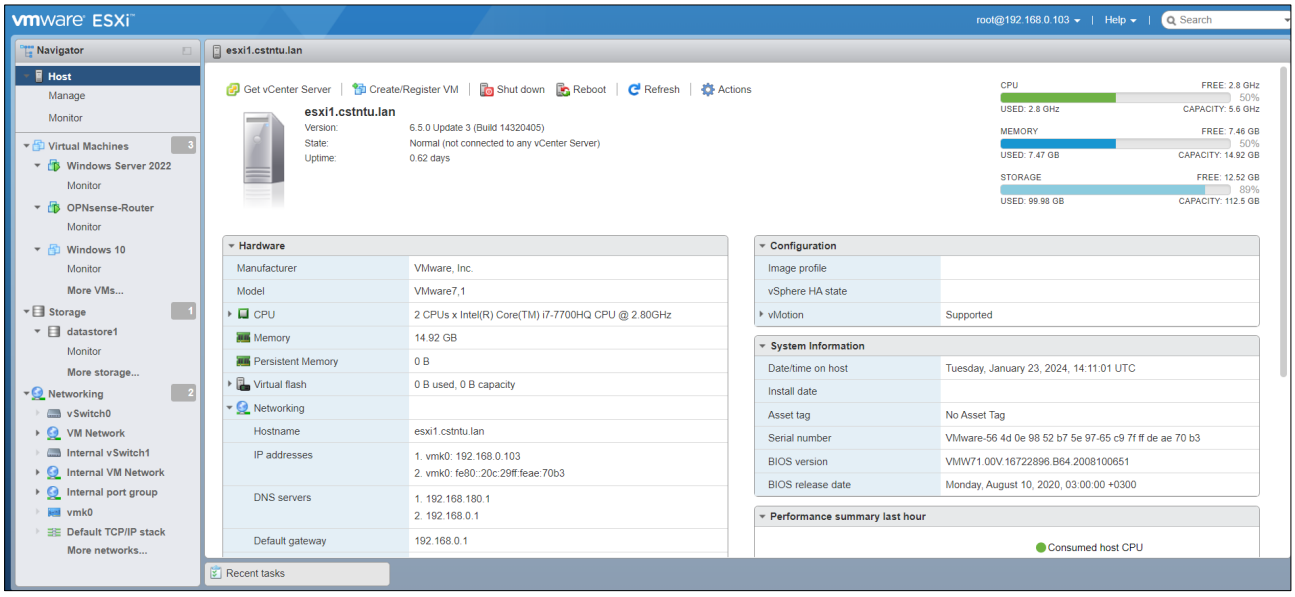

Рисунок 3.2 – Інтерфейс управління VMware ESXi

Ім’я хоста ESXi - esxi1.csnttu.lan. IP адреси для інтерфейсу керування (vmk0) 192.168.0.103, DNS сервери - 192.168.180.1 і 192.168.0.1, шлюз за замовчуванням - 192.168.0.1.

Цей інтерфейс використовується системними адміністраторами для управління віртуальними машинами, їхніми ресурсами та мережевими налаштуваннями на фізичному сервері.

На рисунку 3.3 показано інтерфейс управління внутрішнім віртуальним комутатором (Internal vSwitch1) в VMware ESXi.

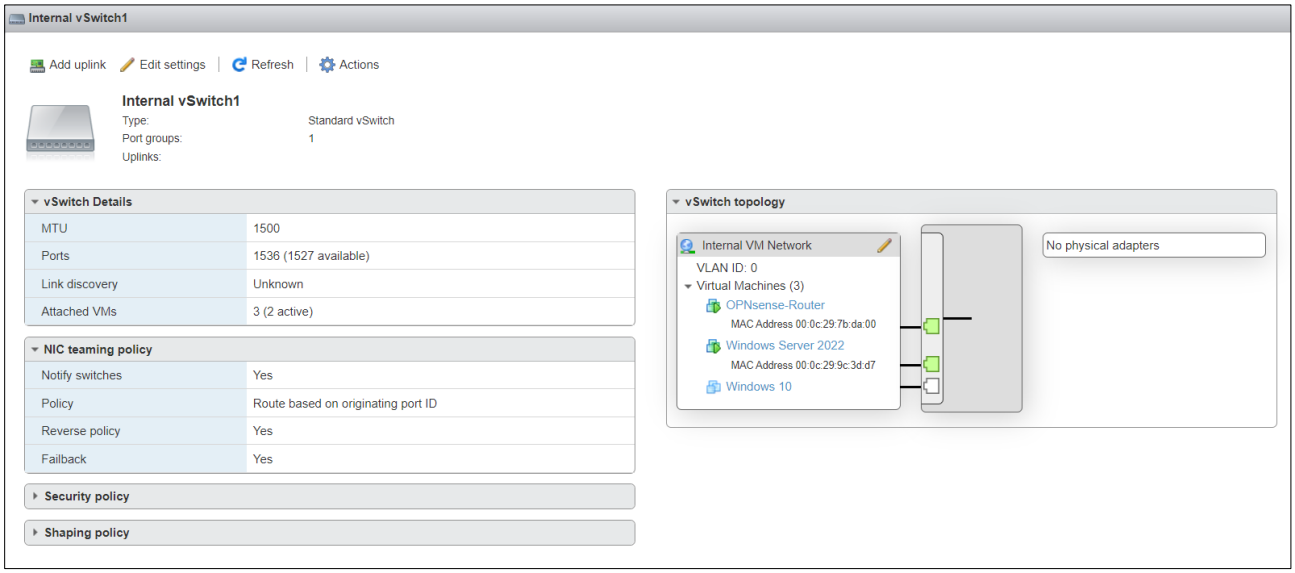

Рисунок 3.3 – Інтерфейс управління внутрішнім віртуальним комутатором

Internal vSwitch1 містить одну групою портів Internal VM Network та без фізичних адаптерів. До комутатора прикріплено три віртуальні машини OPNsense-Router, Windows Server 2022 та Windows 10.

Ця сторінка є частиною інтерфейсу управління ESXi і використовується для налаштування мережевих параметрів віртуальних машин і віртуальних комутаторів, що є важливою частиною управління віртуалізованою інфраструктурою.

На рисунку 3.4 показано інтерфейс управління зовнішнім віртуальним комутатором (vSwitch0) в VMware ESXi.

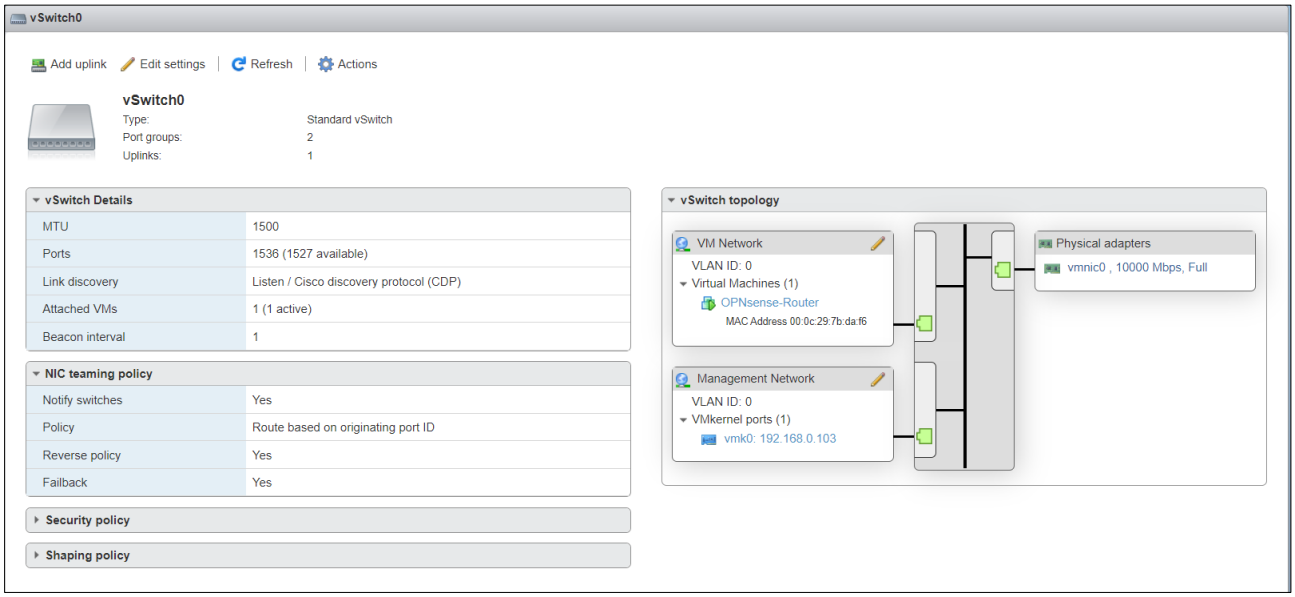

Рисунок 3.4 – Інтерфейс управління зовнішнім віртуальним комутатором

vSwitch0 - це стандартний віртуальний комутатор із двома групами портів та одним фізичним адаптером. Налаштовано дві групи мереж. VM Network з VLAN ID 0, до якої приєднано віртуальну машину OPNsense-Router та Management Network також з VLAN ID 0, до якої приєднано VMkernel port vmk0 з IP адресою 192.168.0.103. Зовнішній віртуальний комутатор спілкується з зовнішньою мережею через фізичний адаптер vmnic0.

На рисунку 3.5 відображено інтерфейс управління сховищем даних (datastore1) в VMware ESXi.

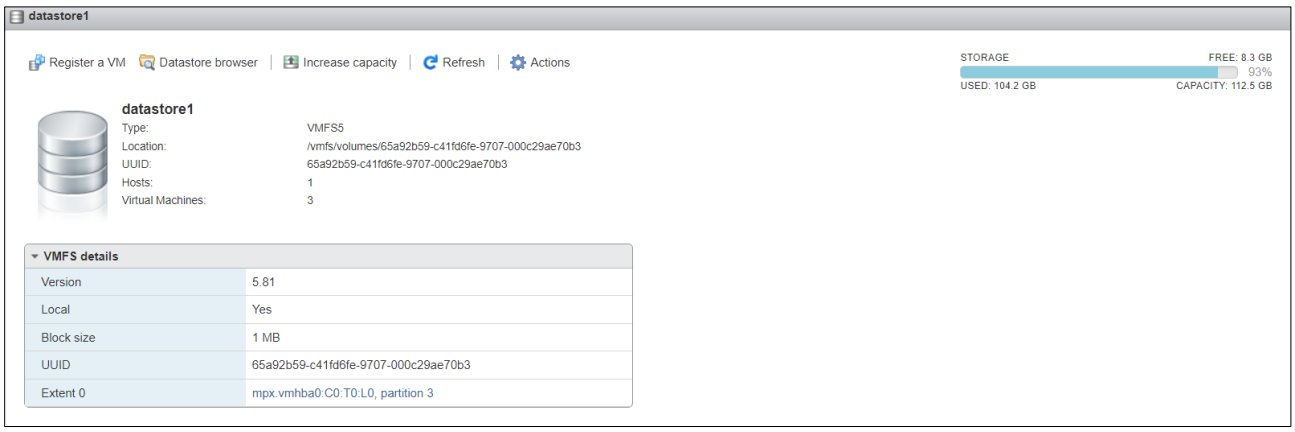

Рисунок 3.5 – Інтерфейс управління сховищем даних

Сховище datastore1 використовує файлову систему VMFS5. Сховище даних змонтовано в ОС VMkernel як /vmfs/volumes/65a92b59-c41fd6fe-9707-000c29ae70b3. Де 65a92b59-c41fd6fe-9707-000c29ae70b3 є унікальним ідентифікатором (UUID)для цього сховища даних.

3.3 Налаштування маршрутизатора OPNsense

Налаштування брандмауера OPNsense включає ряд кроків для забезпечення ефективної захисту мережі та належного функціонування всіх його функціональних можливостей [15].

3.3.1 Налаштування мережі та NAT

На рисунку 3.6 показано інтерфейс керування мережевими інтерфейсами в OPNsense та налаштування інтерфейсу WAN.

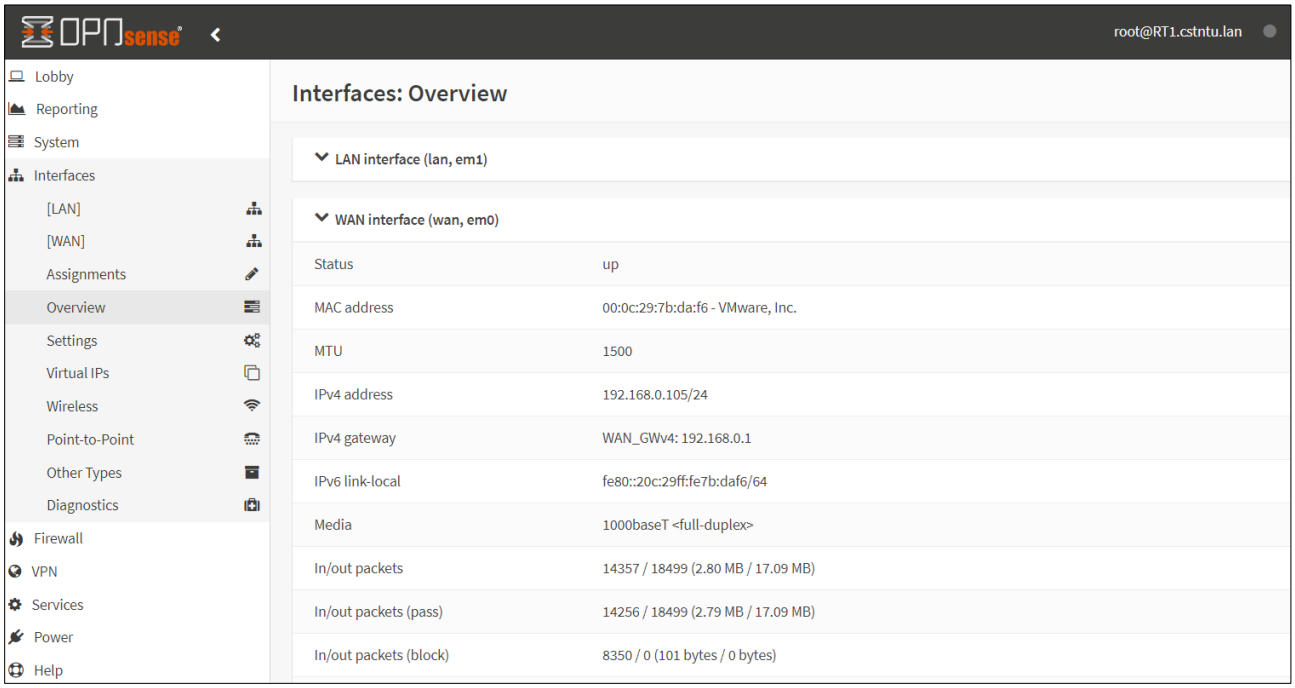

Рисунок 3.6 – Налаштування інтерфейсу WAN

На рисунку 3.7 показано інтерфейс налаштування DHCP сервера в OPNsense для LAN.

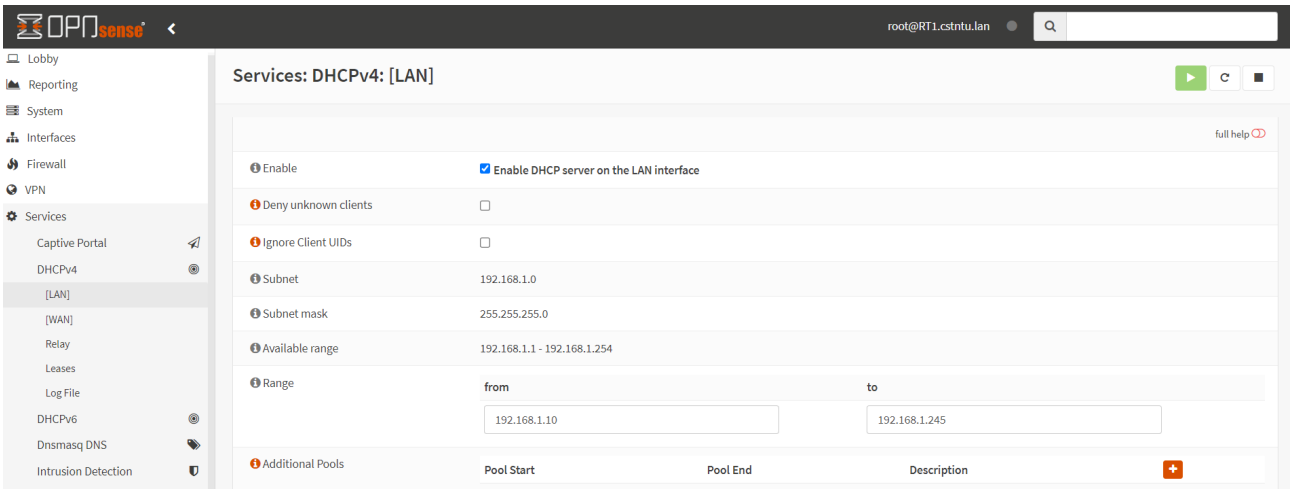

Рисунок 3.7 – Інтерфейс налаштування DHCP сервера в OPNsense

Опція Deny unknown clients не відмічена, тобто DHCP сервер буде видає IP адреси всім клієнтам, навіть якщо їх MAC адреси не зазначені в списку дозволених. Ignore Client UIDs також не відмічена, що означає, що сервер DHCP враховує унікальні ідентифікатори (UID) клієнтів при видачі IP адрес.

Підмережа 192.168.1.0/255.255.255.0 є базовою мережею для DHCP. Доступний діапазон для видачі IP адрес від 192.168.1.1 до 192.168.1.254. Специфічний діапазон, який DHCP сервер буде використовувати для розподілу IP адрес, від 192.168.1.10 до 192.168.1.245.

Ця сторінка дозволяє адміністраторам мережі налаштовувати параметри DHCP сервера для автоматичного призначення IP адрес у мережі без необхідності ручного конфігурування кожного пристрою.

На рисунку 3.8 показано налаштування NAT для вихідного (outbound) трафіку в OPNsense.

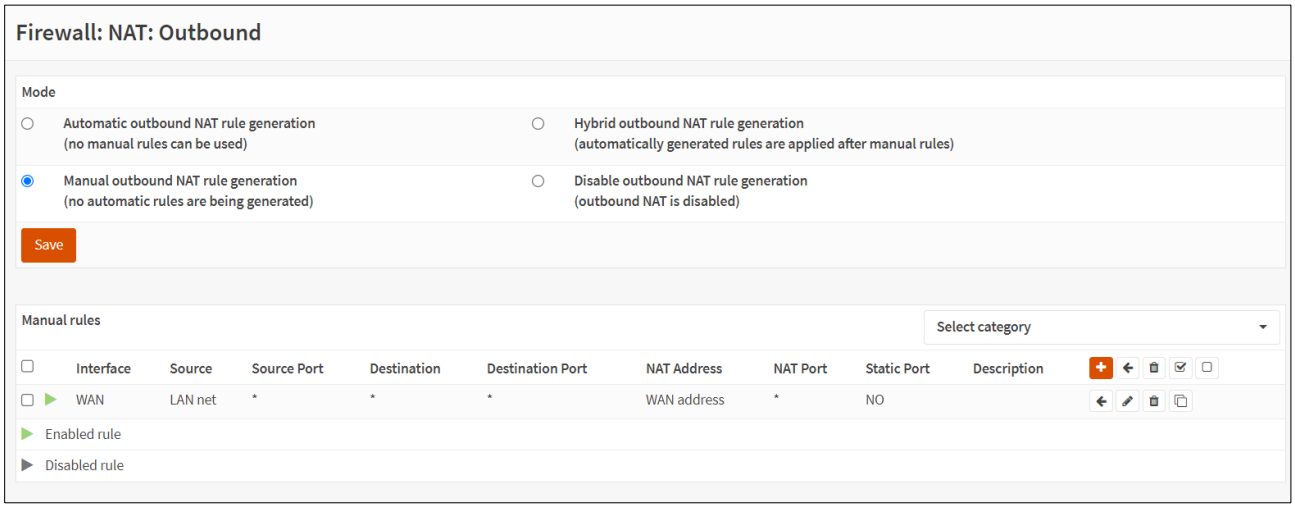

Рисунок 3.8 – Налаштування NAT в OPNsense

Вибрано режими Manual outbound NAT rule generation, що означає, що правила NAT для вихідного трафіку створюються в ручному режимі без автоматичного генерування.

Правило вказує, що трафік з локальної мережі LAN, який проходить через інтерфейс WAN буде перетворений за допомогою NAT.

Ці налаштування важливі для забезпечення правильного перекладу приватних IP адрес мережі на зовнішню IP адресу, що дозволяє внутрішнім користувачам підключатися до інтернету.

3.3.2 Налаштування OpenVPN сервера та брандмауера

Мобільним користувачам потрібен безпечний доступ до інфраструктури організації. OPNsense використовує OpenVPN для конфігурації SSL VPN OpenVPN — це протокол VPN з відкритим кодом, який створює безпечні з'єднання за допомогою методів VPN.

Протокол OpenVPN має високий рівень безпеки. Він поставляється з 256-бітним шифруванням через OpenSSL. OpenVPN може використовувати два різні протоколи для передачі даних: TCP і UDP. Більш широко використовуваним і рекомендованим протоколом є UDP. OpenVPN підтримує попередні спільні ключі, автентифікацію на основі сертифіката, автентифікацію за іменем користувача та паролем.

OpenVPN вимагає сертифікатів для захисту служби VPN за допомогою шифрування та автентифікації. Першим кроком у налаштуванні OPNsense є створення центру сертифікації (CA).

На рисунку 3.9 показано створений центри сертифікації в OPNsense.

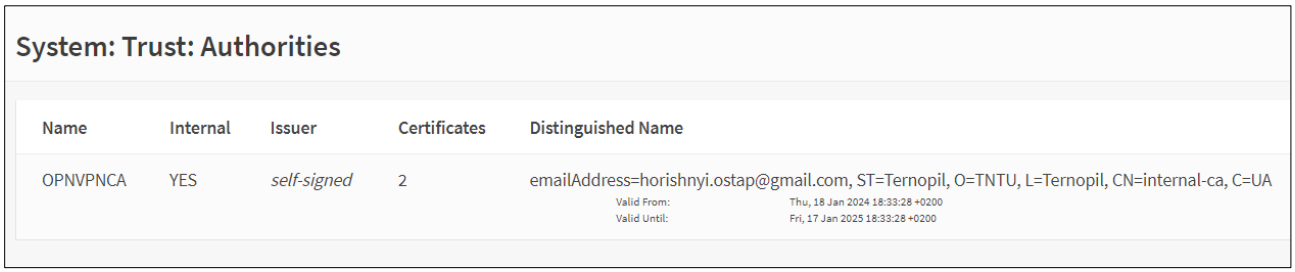

Рисунок 3.9 – Центри сертифікації в OPNsense

Назва довіреної організації сертифікації (CA) вказана як "OPNVPNCA". Internal = "YES" означає, що це внутрішня CA в системі. Видавець сертифіката позначений як "self-signed", що означає, що сертифікат був виданий самою системою, а не зовнішньою CA.

На рисунку 3.10 показано створений сертифікат сервера, який клієнти використовуватимуть для перевірки ідентичності сервера під час підключення до нього та сертифікат користувача.

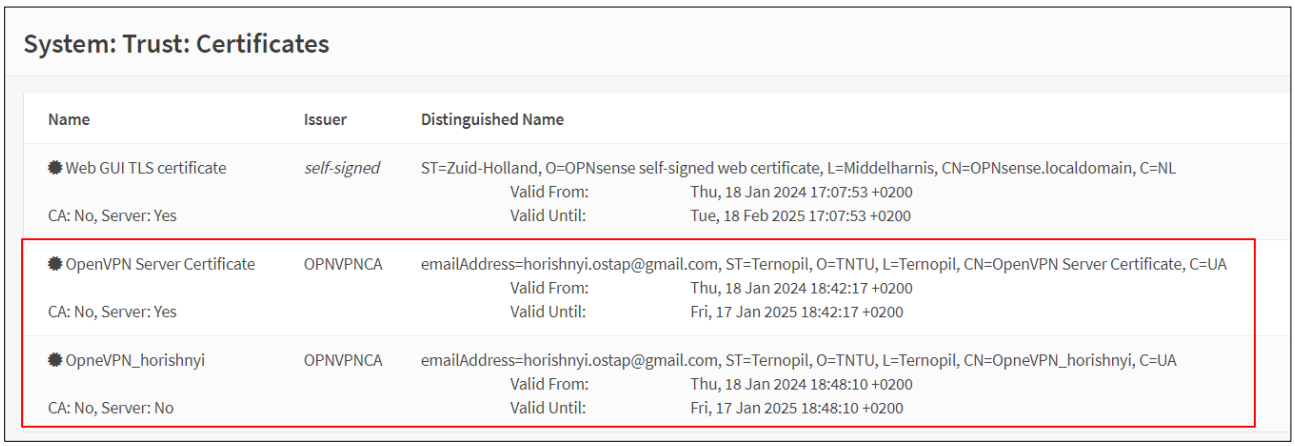

Рисунок 3.10 – Сертифікат сервера та користувача

Сертифікат Web GUI TLS certificate використовується для адміністрування OPNsense через вебпортал адміністратора. Оскільки HTTPS увімкнено за

замовчуванням сертифікат генерується автоматично під час встановлення OPNsense.

Для автентифікації користувачів VPN було використано Local User Access (див.рисунок 3.11).

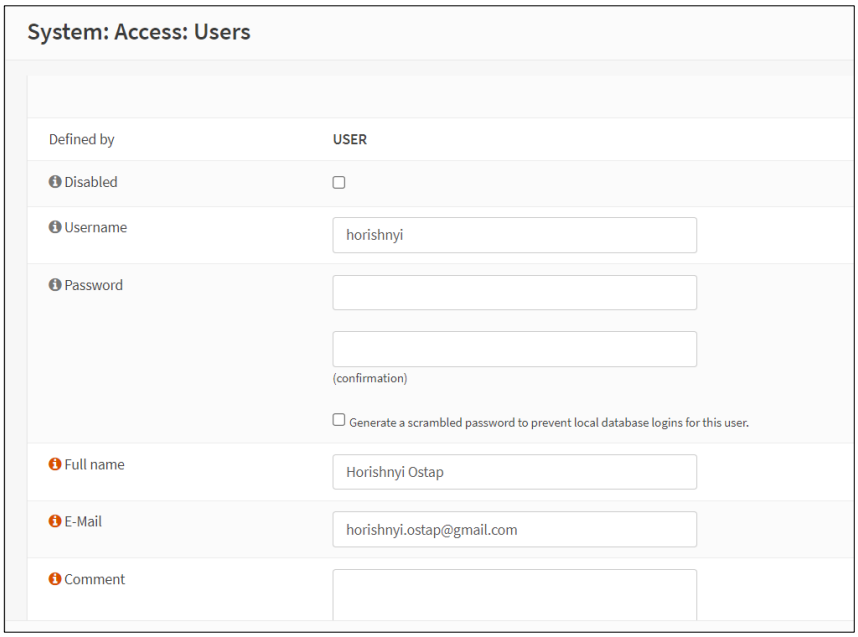

Рисунок 3.11 – Локальний користувач VPN `horishnyi`

Під час використання локальних користувачів сертифікати кожного користувача можна легко використовувати та керувати ними в графічному інтерфейсі OPNsense (див.рисунок 3.12).

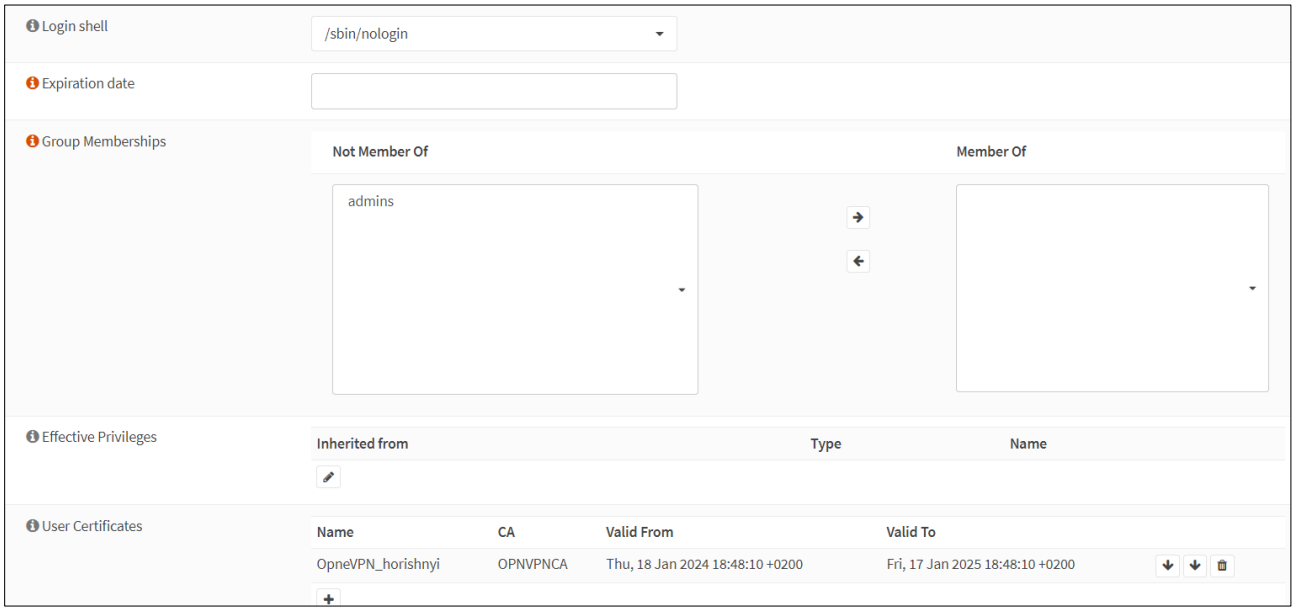

Рисунок 3.12 – Підключення сертифікату користувача до логіну `horishnyi`

Це набагато безпечніше, але залежно від кількості людей, які матимуть доступ до служби, це може бути менш зручним, ніж використання центральної системи автентифікації.

Після створення користувачів і сертифікатів VPN можна почати налаштовувати сервер OpenVPN у брандмауері OPNsense.

На рисунку 3.13 показано налаштування загальних параметрів сервера OpenVPN в OPNsense.

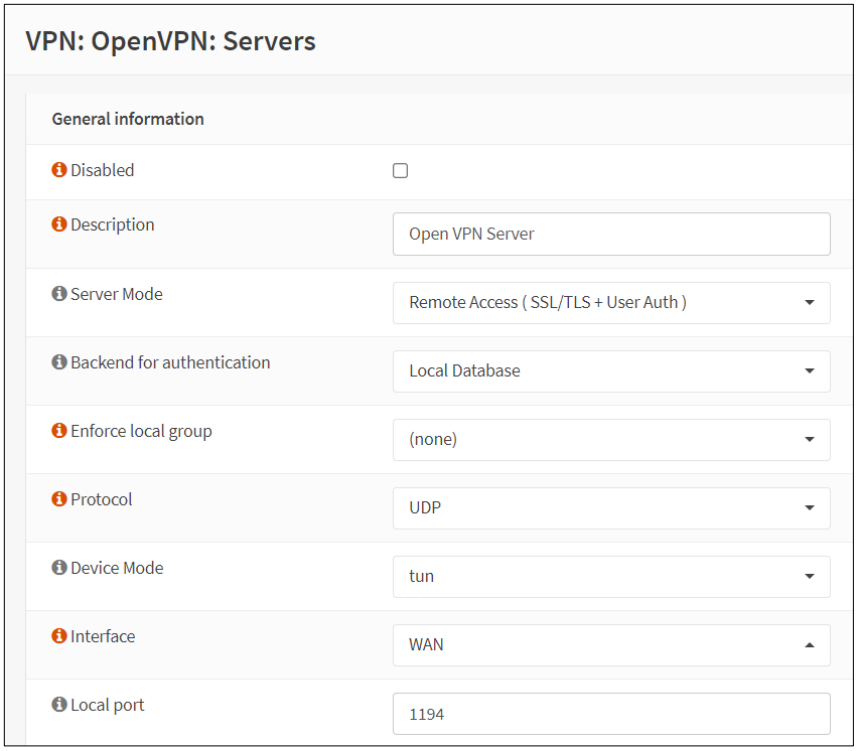

Рисунок 3.13 – Налаштування загальних параметрів сервера OpenVPN

В конфігурації Server Mode встановлено в режим "Remote Access (SSL/TLS + User Auth)", що вказує на віддалений доступ з використанням SSL/TLS для шифрування і аутентифікації користувача. Для аутентифікації використовується локальна база даних користувачів. Протокол з'єднання встановлено як UDP, що є стандартним вибором для OpenVPN з'єднань. Device Mode використовує "tun" режим, що створює точка-точка IP тунель. Сервер працює на WAN інтерфейсі.

Локальний порт для VPN сервера встановлено як 1194, що є стандартним портом для OpenVPN.

На рисунку 3.14 показано криптографічні налаштування сервера OpenVPN в OPNsense.

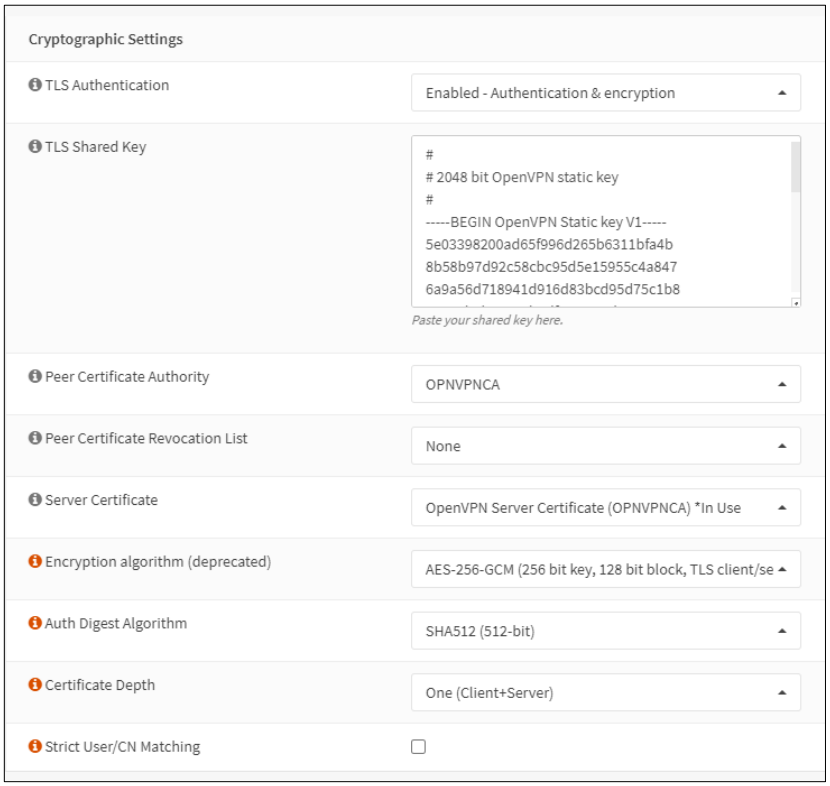

Рисунок 3.14 – Налаштування криптографічних параметрів сервера OpenVPN

В налаштування TLS Authentication вказано, що використання як аутентифікації, так і шифрування. В TLS Shared Key встановлено спільний ключа TLS, який використовується для додаткового шару безпеки у VPN з'єднаннях. Peer Certificate Authority вибрано "OPNVPNCA" як довірену організацію сертифікації для перевірки сертифікатів пар. В Server Certificate вказано "OpenVPN Server Certificate (OPNVPNCA)" як сертифікат, який використовується сервером [22].

Обрано AES-256-GCM як сучасний і безпечний алгоритм шифрування. AES-256-GCM є режимом блочного шифрування, який поєднує AES з довжиною ключа 256 біт і режимом GCM [16]. AES - це симетричний блочний шифр, що використовується для шифрування і дешифрування даних. Симетричний

означає, що для шифрування і дешифрування використовується один і той же ключ. AES є широко визнаним і використовуваним стандартом шифрування. Ключ з довжиною 256 біт забезпечує високий рівень безпеки. GCM є режимом шифрування, який не тільки шифрує дані, але й надає механізм аутентифікації повідомлень, відомий як аутентифіковане шифрування з пов'язаними даними (AEAD). Це означає, що крім шифрування, GCM також перевіряє цілісність і автентичність даних [21].

GCM дозволяє швидке шифрування та дешифрування даних, що робить його практичним для використання в реальному часі. Інтегрований механізм аутентифікації дозволяє перевіряти, чи не були дані змінені після шифрування.

AES-256-GCM часто використовується в сучасних протоколах безпеки, таких як TLS і VPN, а також у рішеннях для шифрування на дисках та в хмарних сервісах [20].

Параметр Auth Digest Algorithm встановлено в значення SHA512. SHA-512 є частиною сімейства криптографічних хеш-функцій SHA. SHA-512 генерує 512-бітний (64-байтовий) хеш-відбиток.

Параметр Certificate Depth встановлено One (Client+Server), що вказує на обмеження перевірки ланцюжка сертифікатів до одного рівня.

На рисунку 3.15 показано налаштування параметрів тунелю в сервері OpenVPN.

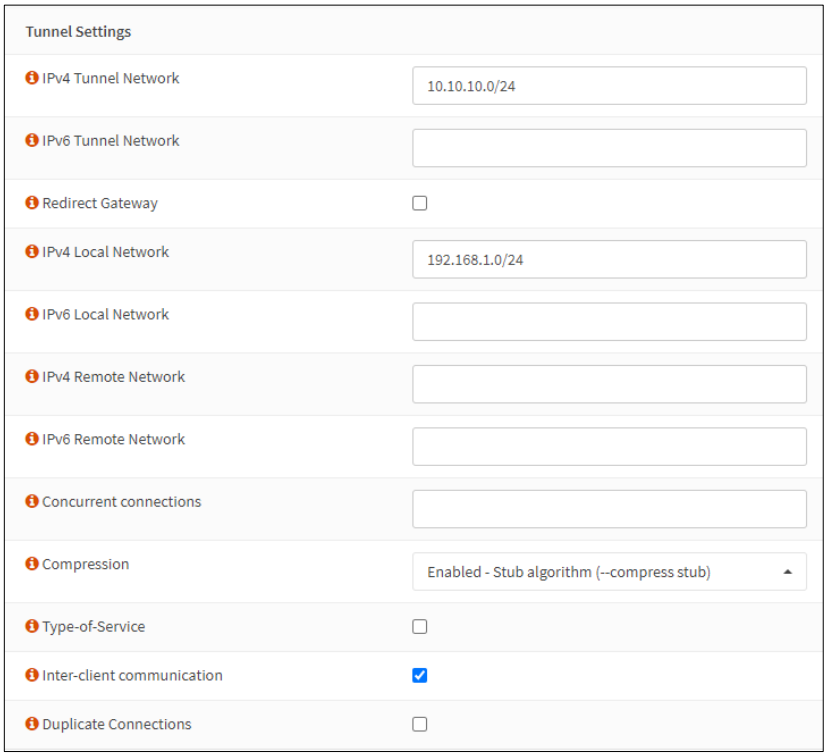

Рисунок 3.15 – Налаштування параметрів тунелю в сервері OpenVPN

В параметрі IPv4 Tunnel Network вказано мережу 10.10.10.0/24, яка є віртуальною мережею для приватного зв'язку між сервером і клієнтами VPN. Опція Redirect Gateway не включена, що означає, що весь клієнтський трафік не буде примусово направлятися через VPN. Параметр IPv4 Local Network заданий як 192.168.1.0/24, це мережа, до якої можна буде отримати доступ з віддаленої точки підключення. Параметри Compression включено. Алгоритм стиснення може поліпшити продуктивність мережі за рахунок зменшення кількості даних, які передаються через тунель.

На рисунку 3.16 показано налаштування додаткових клієнтських параметрів.

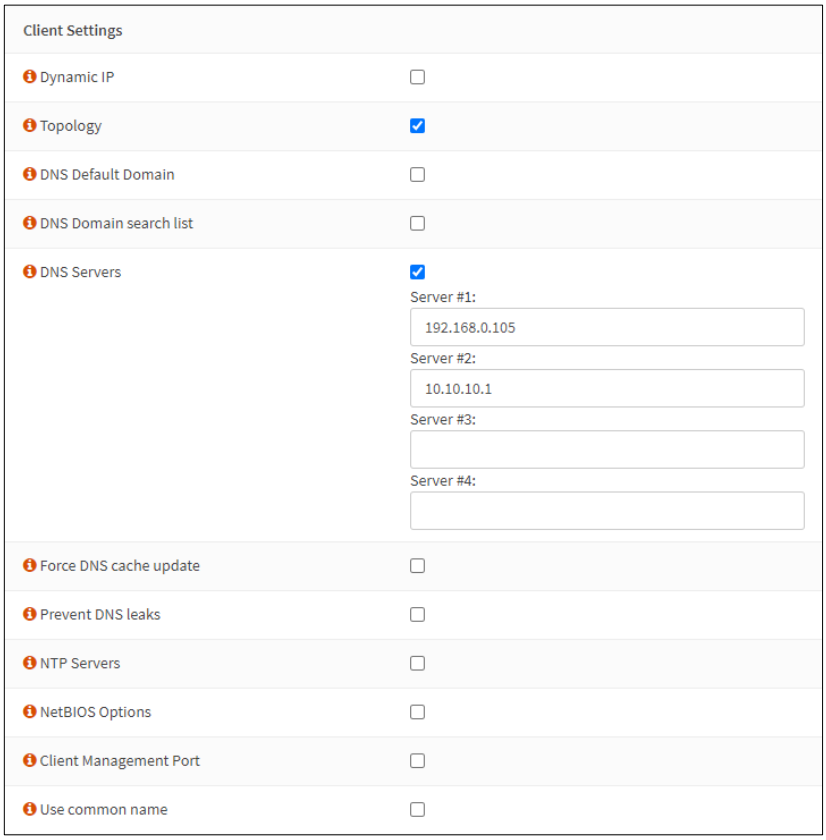

Рисунок 3.16 – Налаштування додаткових клієнтських параметрів в сервері OpenVPN

Параметр Topology включено, це встановлює використання спільної підмережі для всіх клієнтів (topology subnet), замість виділення окремої підмережі для кожного клієнта (topology net30). Це важливо при використанні режиму tun на IPv4. Опція DNS Servers відмічена, і встановлено два DNS сервери з IP-адресами 192.168.0.105 та 10.10.10.1.

За замовчуванням увесь трафік, що надходить до сервера OpenVPN або проходить через тунелі VPN, заборонено. На рисунку 3.17 показано правила брандмауера OPNsense, які дозволяють підключатись клієнтам VPN.

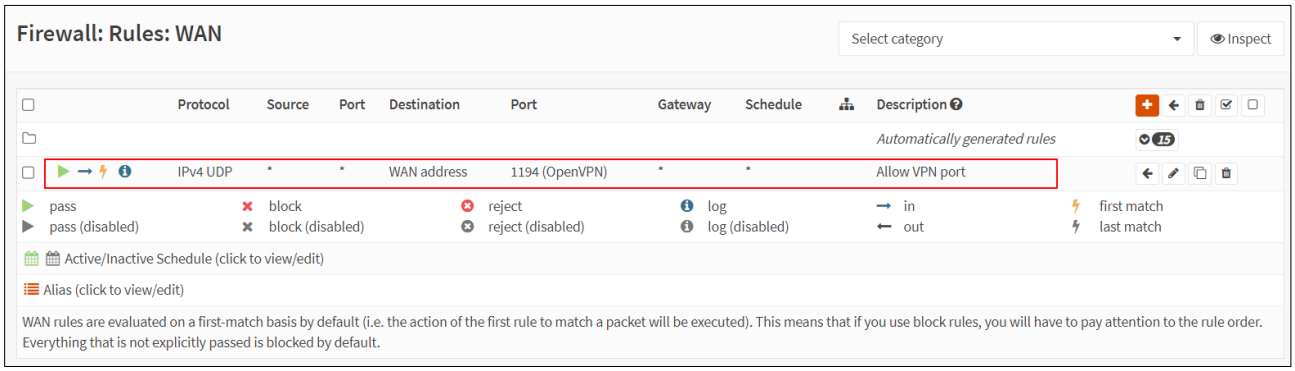

Рисунок 3.17 – Правила брандмауера OPNsense, які дозволяють підключатись клієнтам VPN

Дозвіл доступу до порту сервера OpenVPN, за замовчуванням UDP/1194, на інтерфейсі WAN потрібен для підключення клієнтів SSL VPN.

Щоб дозволити VPN-клієнтам підключатися до серверів локальної мережі через VPN-тунель потрібно встановити відповідні правила в брандмауері (див.рисунок 3.18).

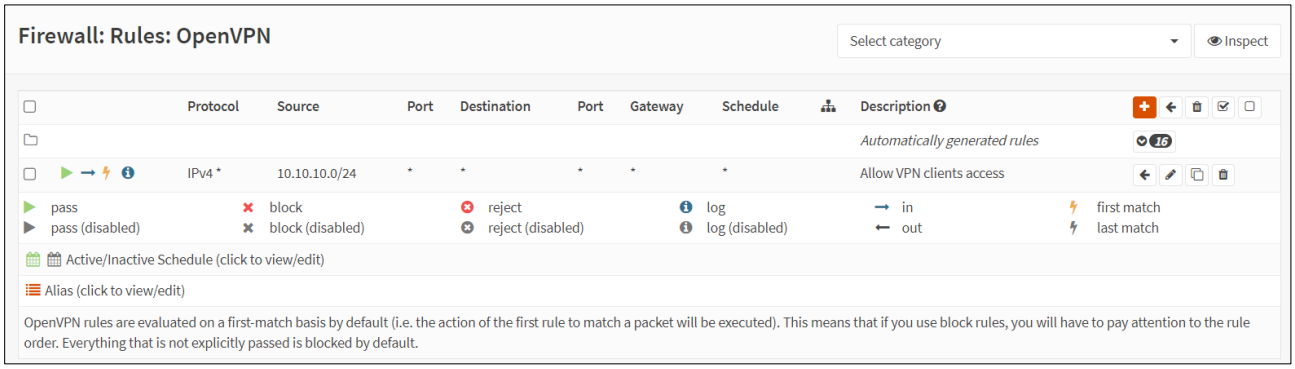

Рисунок 3.18 – Правила брандмауера OPNsense для VPN клієнтів

Дане правило дозволяє доступ VPN клієнтам до локальної мережі в які знаходиться Windows Server 2022.

3.4 Перевірка працездатності реалізованої схеми

Для підключення до OpenVPN сервера використаємо Viscosity OpenVPN клієнт в операційній системі Windows 10 [15]. Viscosity дуже простий у налаштуванні та використанні та добре працює в операційній системі Windows.

На рисунку 3.19 показано експорт налаштувань для Viscosity OpenVPN клієнта.

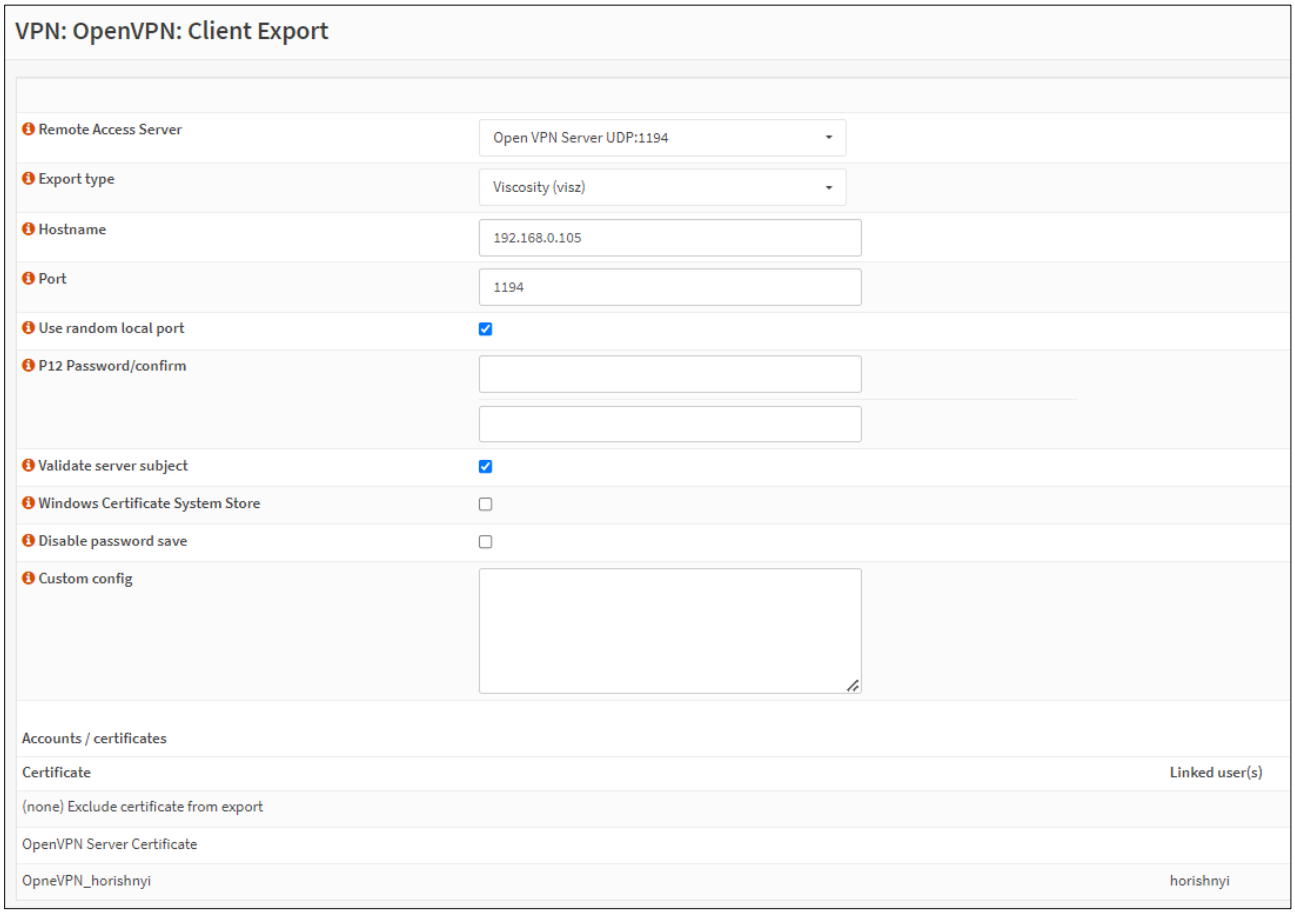

Рисунок 3.19 – Панель експорту налаштувань для Viscosity OpenVPN клієнта

Цей інтерфейс дозволяє адміністраторам легко експортувати налаштування клієнта VPN для різних користувачів, що спрощує процес розгортання клієнтських VPN з'єднань.

Тепер на комп’ютері Windows 10 потрібно розпакувати пакет і імпортувати файл Open_VPN_Server_OpneVPN_horishnyi.visz в Viscosity OpenVPN клієнт.

На рисунку 3.20 можна побачити що підключення до OpenVPN сервера в активному стані.

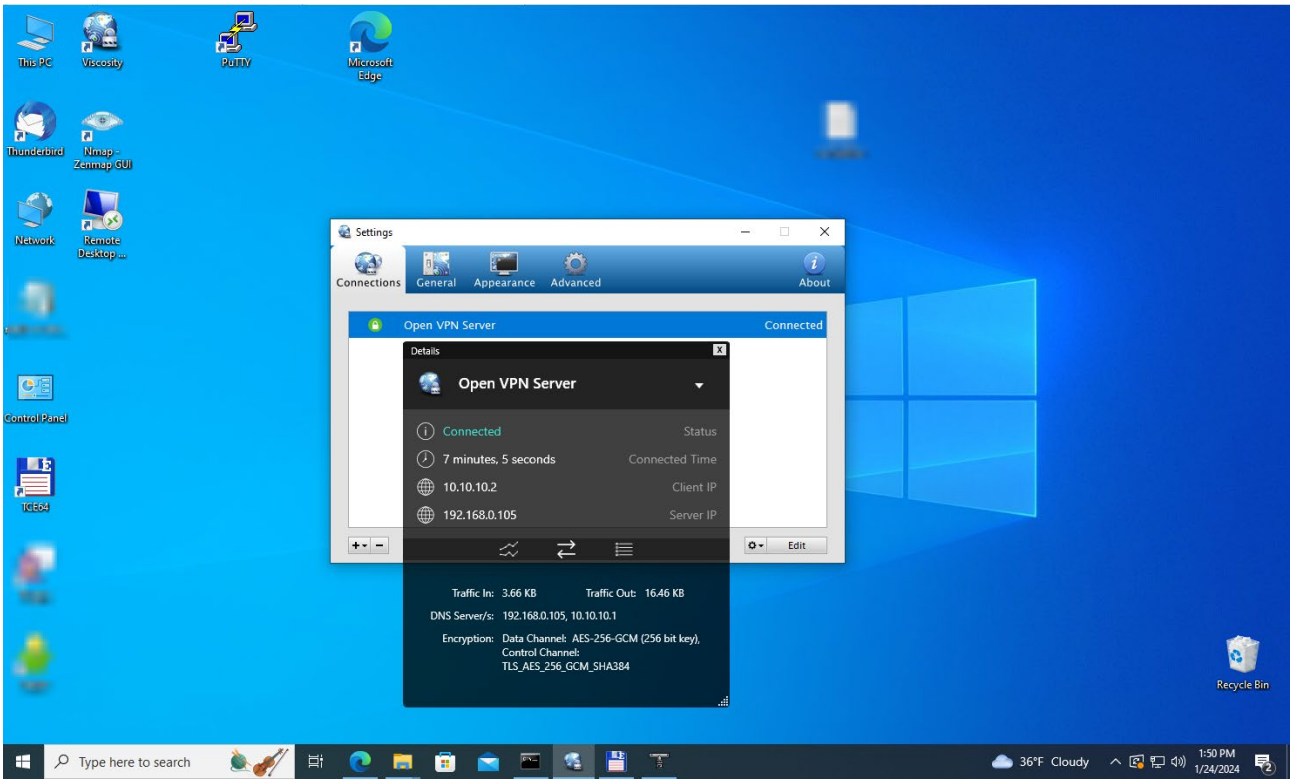

Рисунок 3.20 – Статус та параметри підключення Viscosity OpenVPN клієнта

Клієнтська IP-адреса в мережі VPN - 10.10.10.2. IP-адреси DNS сервери 10.10.10.1 та 192.168.0.105. Використовується алгоритму шифрування AES-256-GCM в Data Channel та TLS_AES_256_GCM_SHA384 набір шифрів для Control Channel.

Data Channel та Control Channel є двома ключовими компонентами протоколу OpenVPN, які використовуються для забезпечення безпеки VPN-з'єднання.

Data Channel - це канал, через який проходить фактичний користувацький трафік, такий як веб-сторінки, файли, аудіо та відео дані. Data Channel забезпечує шифрування користувацьких даних, що передаються між клієнтом і сервером Використання AES-256-GCM на Data Channel означає, що весь трафік, який проходить через VPN, зашифрований з високим рівнем безпеки.

Control Channel - це канал, який використовується для безпечного обміну ключами, аутентифікації та управління сеансом між клієнтом і сервером. Control Channel забезпечує захищене підключення до VPN перед тим, як будь-які користувацькі дані почнуть передаватися. Набір шифрів TLS_AES_256_GCM_SHA384 використовує TLS для захисту Control Channel

[17]. AES-256-GCM забезпечує шифрування, а SHA384 використовується для створення хешу в Control Channel, який забезпечує цілісність даних та захист від змін. SHA384 створює хеш-відбиток довжиною 384 біти, що забезпечує додатковий рівень безпеки [18].

Використання цих сильних криптографічних алгоритмів у Data Channel та Control Channel забезпечує високий рівень безпеки для VPN-з'єднань, роблячи їх стійкими до спроб перехоплення та розшифрування [19].

Також статус підключення можна побачити на інформаційній панелі в OPNsense (див. рисунок 3.21).

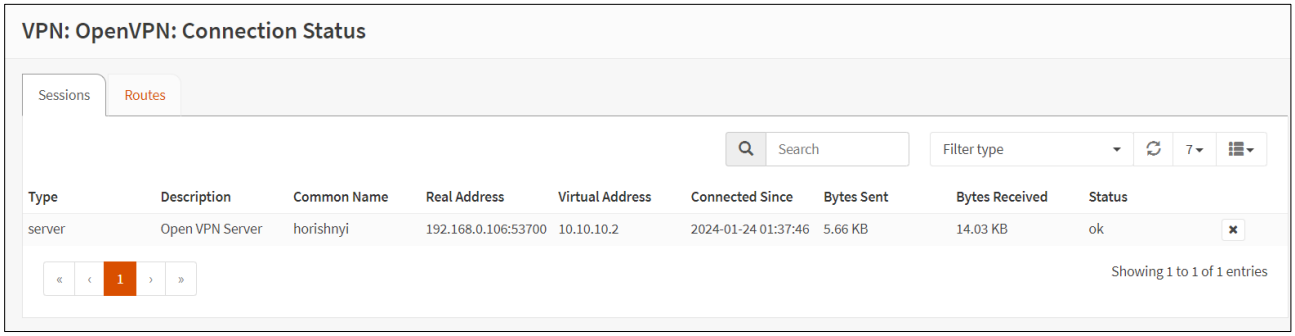

Рисунок 3.21 – Статус підключення VPN клієнтів в OPNsense

За допомогою утиліти WinMTR можна переконатись що лише трафік до локальної корпоративної мережі проходить через VPN з’єднання арешту інтернет трафіку проходить загальним каналом підключення (див.рисунки 3.22-3.23).

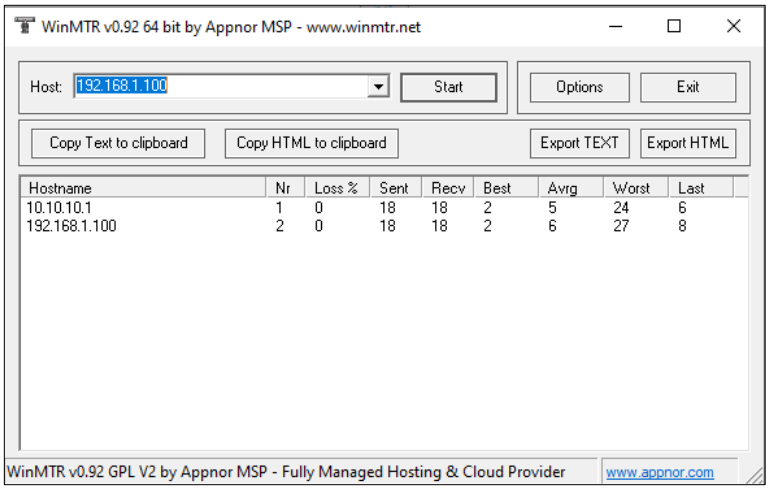

Рисунок 3.22 – Маршрут до локальної корпоративної мережі

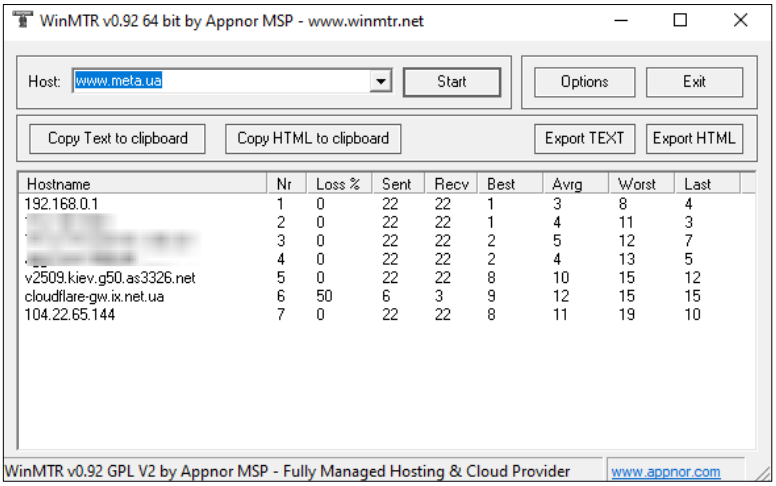

Рисунок 3.22 – Маршрут до хостів в мережі Інтернет

На завершальному етапі перевірки здійснимо підключення до Windows Server 2022 за допомогою протоколу RDP (порт 3389 TCP) з використанням термінал клієнта (див. рисунок 3.23).

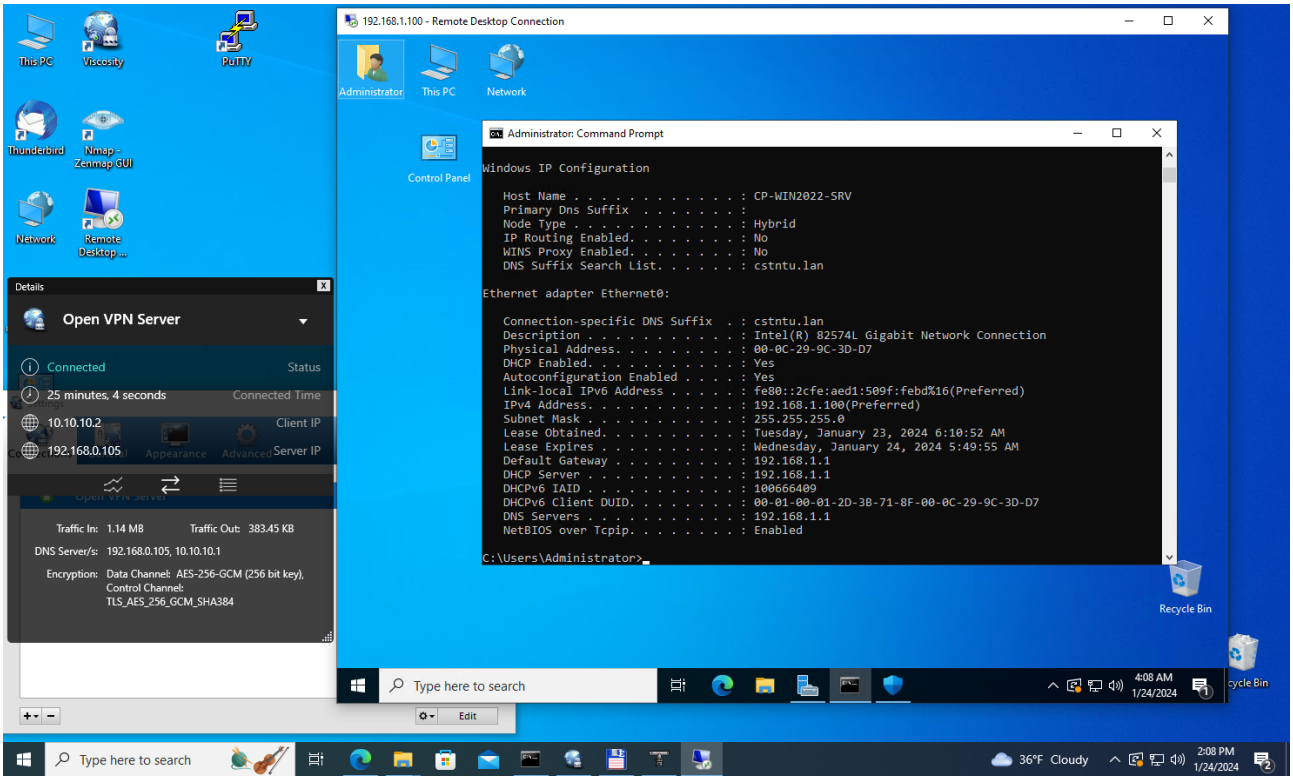

Рисунок 3.23 – Підключення по RDP протоколу до Windows Server 2022

Протокол RDP є протоколом віддаленого доступу, розробленим компанією Microsoft, і використовується для забезпечення можливості віддаленого

управління комп'ютерами або серверами через мережу. В основному, він використовується для віддаленої роботи з серверами чи комп'ютерами, які працюють під управлінням операційних систем Windows.

Після успішного підключення можна управляти Windows Server 2022 та використовувати локальні ресурси корпоративного сервера.

3.5 Висновки до розділу

В третьому розділі було розроблено схему лабораторного тестового середовища, яка була використана для створення віртуалізованої корпоративної інфраструктури. Проведе встановлення та налаштування гіпервізора VMware ESXi. У віртуалізованому середовищі встановлено маршрутизатор OPNsense Здійснено налаштування мережевих параметрів, NAT, брандмауера, DNS, DHCP сервера та OpenVPN сервера з підтримкою шифрування в маршрутизатор OPNsense. Також в віртуалізованому середовищі встановлено та налаштовано Windows Server 2022, як термінал сервер. З тестової операційної системи Windows 10 перевірено працездатність реалізованого рішення. Підтверджено що в даній конфігурації OpenVPN сервер стабільно підтримує шифровані VPN тунелі та надає безпечний доступ до віртуалізованої корпоративної інфраструктури.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при масивній зовнішній кровотечі

Масивна зовнішня кровотеча є надзвичайно небезпечним станом, який може призвести до серйозної загрози життю постраждалої особи. Невідкладна надання домедичної допомоги може врятувати життя і запобігти подальшій крововтраті.

Долікарська допомога постраждалим при кровотечі є важливою процедурою, яку можуть виконувати особи без медичної освіти.

Ознаками масивної зовнішньої кровотечі є будь-що з нижченаведеного:

- швидке, інтенсивне витікання крові з рани;
- пульсуючий характер кровотечі (кров б’є фонтаном);
- пляма крові біля постраждалого, яка швидко збільшується;
- значне просякнення одягу постраждалого кров’ю;
- порушення або втрата свідомості у постраждалого без ознак черепно-мозкової травми, при наявності зовнішньої кровотечі;
- бліда шкіра, холодні кінцівки тощо, при наявності зовнішньої кровотечі.

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 при масивній зовнішній кровотечі. У цьому порядку термін “тепловий удар” вживаються у такому значенні - невідкладний стан, викликаний дією високої температури навколишнього середовища, що спричиняє системні розлади у постраждалого [23].

Надання домедичної допомоги постраждалим при масивній зовнішній кровотечі передбачає такі кроки:

1) Переконайтесь що небезпеки для вас немає.

2) Закличте оточуючих на допомогу. Якщо є кілька свідків, зверніться до конкретної особи, щоб вона надала допомогу.

3) Перед початком надання допомоги, за можливості, захистіть себе за допомогою індивідуальних засобів захисту, таких як рукавички, маска і захист для очей.

4) Якщо є кровотеча з рани на кінцівці, і вона видно:

а) Здійсніть максимальний тиск на рану руками;

б) Накладіть пов'язку, що чинитиме тиск на рану, і оцініть її ефективність;

в) Якщо кровотеча зупинилась, заспокойте постраждалого, викличте екстрену медичну допомогу та слідуйте вказівкам диспетчера;

г) Якщо кровотеча не зупинилась, накладіть кровоспинний джгут на відстані 5-7 см вище рани. Уникайте накладання джгута безпосередньо на суглоби ліктя або коліна.

ґ) Перевірте ефективність накладеного кровоспинного джгута. Якщо кровотеча зупинилась, зафіксуйте час накладання на джгуті або запишіть його на видимому місці. Якщо неможливо записати час, повідомте медичному персоналу. Якщо вмієте, перевірте пульс нижче джгута. Якщо пульс є, здійсніть додатковий тиск кровоспинним джгутом або накладіть ще один джгут вище. Якщо кровотеча не зупинилась, продовжуйте надавати прямий тиск на рану до прибуття медичної бригади або тампонуйте рану.

5) При кровотечі з рани кінцівки без можливості її чіткої візуалізації:

а) Накладіть кровоспинний джгут якомога вище на кінцівку;

б) Заспокойте постраждалого та поясніть подальші кроки;

в) Якщо можливо, розріжте одяг на кінцівці;

г) Оцініть ефективність накладання кровоспинного джгута:

Якщо кровотеча зупинилась, зафіксуйте точний час накладання джгута на самому джгуті або видимому місці. Якщо неможливо зафіксувати час, повідомте медичному персоналу та переконайтеся, що ця інформація буде внесена до медичних записів.

Якщо у вас є навик перевірки пульсу на кінцівці нижче джгута, перевірте його. Якщо пульс присутній, збільште тиск кровоспинного джгута або накладіть додатковий джгут.

Якщо кровотеча не зупинилась, збільште тиск на кровоспинному джгуті або накладіть ще один джгут в залежності від місця рани. Якщо другий джгут не є ефективним або неможливо його накласти, продовжуйте чинити прямий тиск на рану руками до прибуття медичної бригади або тампонуйте рану.

Не знімайте або не послабляйте кровоспинний джгут до прибуття медичної бригади.

6) При кровотечі з рани, розташованої в пахвових ділянках, сідницях або основі шиї:

а) Застосуйте максимальний тиск на рану;

б) Заспокойте постраждалого та поясніть подальші дії;

в) Тампонуйте рану тугим гемостатичним засобом або марлевим бинтом. Після тампонування продовжуйте здійсніть прямий тиск на рану протягом 3 хвилин (з гемостатиком) або 10 хвилин (з марлевим бинтом);

г) Оцініть ефективність тампонування рани.

Якщо кровотеча зупинилась, продовжуйте надавати іншу домедичну допомогу, передбачену процедурою.

Якщо кровотеча не зупинилась, спробуйте повторно тампонувати рану. Якщо це неможливо, продовжуйте чинити максимальний тиск на рану руками до прибуття швидкої медичної допомоги.

Це загальна послідовність дій, яку слід виконати, але завжди важливо дотримуватись інструкцій медичних фахівців та адаптувати допомогу до конкретної ситуації. Виконання цих кроків допоможе забезпечити постраждалому першу необхідну допомогу та зберегти його життя до прибуття медичних фахівців.

4.2 Підвищення стійкості роботи комп’ютеризованих систем в умовах дії ЕМІ ядерних вибухів

Інтенсивний сучасний технічний розвиток несе комфорт і процвітання в усі сфери людської діяльності, проте поряд з цим зростає ймовірність техногенної небезпеки. Техногенні небезпеки можуть носити механічний, енергетичний та

хімічний характер. Однією з найпотужніших енергетичних небезпек є ядерний вибух. Ядерний вибух – це вибух, який утворюється при виділенні внутрішньої енергії при розпаді важких ядер урану-235, 233, 238, плутонію-239 та ін.

Внаслідок дії своїх вражаючих факторів ядерні вибухи призводять до масштабних небезпек та таких негативних наслідків як загибель людей, тварин і рослин, потрапляння радіоактивних речовин в навколишнє середовище, руйнування будівель, затоплення територій, пожеж.

Електромагнітне поле – це особлива форма матерії, яка виникає в результаті виробничої діяльності людей. Електромагнітні хвилі можуть існувати у вигляді випромінювань, що переміщуються в просторі зі швидкістю світла (с).

Вплив ЕМП на здоровий організм людини досліджений ще в наш час недостатньо. Існує ймовірність, що ЕМП призводить до розщеплення атомів і молекул організму на іони, а це може бути причиною утворення іонних струмів, які в результаті сприяють підвищенню температури тіла людини. Дослідження показали, що ЕМП може призводити до гальмування рефлексів, гіпотонії, збільшення лейкоцитів в крові людини, погіршення зору та ін. Певну небезпеку представляють для людини лінії електропередачі, поблизу яких визначається дуже значна напруженість електричного поля (до 15 КВ/м) [24].

При ядерному вибуху утворюється сильне електромагнітне випромінювання в широкому діапазоні хвиль з максимумом спектральної щільності в області 15-30 кГц. Це випромінювання триває кілька мікросекунд, тому його прийнято називати електромагнітним імпульсом.

ЕМІ характеризується великою напруженістю електричного та магнітного полів. Ці параметри є основним вражаючим фактором для струмопровідних елементів, хоча значного впливу на людину не мають. Імпульс струму, що з’являється на момент вибуху і високий потенціал можуть вивести з ладу трансформатор, пошкодити напівпровідникові елементи в приладах, розплавити ізоляційний матеріал на кабелях, спричинити вигорання запобіжників та розрядників. Особливу увагу слід приділити пунктам управління, де працюють люди, оскільки існує загроза ураження персоналу внаслідок виведення з ладу техніки та розгортання аварійної ситуації.

Для захисту необхідно здійснити екранування ліній зв'язку, пунктів управління, окремих вузлів та блоків, електро та радіоапаратури, використовувати спеціальні захисні пристрої [25].

Поряд з цим слід зазначити, оскільки час EMI в кілька мільярдних часток секунд настільки мізерний, що його зовсім недостатньо, щоб спрацювали більшість електронних систем захисту. Тому чутливе комп'ютерне обладнання не завжди зможе уникнути потужного перенавантаження. Комп'ютерні системи містять багато напівпровідникових елементів (цифрові процесори, діоди, транзистори, випрямлячі та ін.), які є дуже вразливими до дії EMI.

У випадку, коли ядерний вибух відбувся неподалік лінії електропостачання, то наведені в них напруги можуть проходити через провідники впродовж багатьох кілометрів, а також псувати апаратуру та становити загрозу людям, які перебувають на безпечній відстані від вибуху.

Отже, основні критерії, які слід враховувати під час підвищення стійкості роботи електричних та комп'ютеризованих систем при дії EMI - це максимальна напруга та максимальна енергія. Зокрема напруга, що наводиться у струмопровідних елементах та кабельних лініях передач, при якій ще не виходять з ладу системи.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було проведено дослідження технологій віртуалізації, розроблено та налаштовано захищену корпоративну інфраструктуру на базі гіпервізора VMware ESXi.

У першому розділі виконано огляд технологій віртуалізації, де досліджено типи гіпервізорів 1 та 2 та їхні можливості в управлінні та ефективному використанні апаратних ресурсів. Відзначено, що використання технологій віртуалізації дозволяє ефективно використовувати апаратне забезпечення, спрощує масштабування та надає зручність у тестуванні та розгортанні програмного забезпечення.

Досліджено роль брандмауера як ключового компонента мережевої безпеки, який застосовується для фільтрації трафіку між мережами та захисту від потенційних загроз. Розглянуті принципи функціонування брандмауера, включаючи фільтрацію трафіку, виявлення та блокування небезпечних з'єднань, а також використання правил та політик безпеки. Проведено дослідження можливостей функцій, таких як NAT, фільтрація трафіку та журналювання подій, з метою створення ефективного захисного шару для мережі та забезпечення контролю над мережевими з'єднаннями. Також розглянуто можливості інтеграції брандмауерів у віртуальні середовища для підвищення безпеки корпоративних інфраструктур.

У другому розділі висвітлено ключові моменти архітектури та функціональних можливостей гіпервізора VMware ESXi. Проведено аналіз впливу апаратної віртуалізації Intel VT-x та AMD-V на продуктивність та безпеку віртуалізованого середовища та визначено ключову роль Intel VT-x та AMD-V у створенні ізольованих віртуальних областей, що сприяє забезпеченню безпеки та ефективності роботи віртуальних машин.

Також надано докладний огляд можливостей маршрутизатора та брандмауера OPNsense, який є потужним інструментом для створення безпечних мережевих інфраструктур, що забезпечує різноманітні функції, такі як Traffic Shaper, Stateful Inspection Firewall, VPN, DHCP Server та інші.

Поєднання гіпервізора VMware ESXi та брандмауера OPNsense формує ефективну та надійну платформу для віртуалізованого корпоративного середовища, яка об'єднує в собі ефективність, безпеку та зручність управління.

У третьому розділі було розроблено схему лабораторного тестового середовища, яка була використана для створення віртуалізованої корпоративної інфраструктури. Здійснено встановлення та налаштування гіпервізора VMware ESXi, а також встановлено маршрутизатор OPNsense в віртуалізованому середовищі. Проведено налаштування мережевих параметрів, NAT, брандмауера, DNS, DHCP сервера та OpenVPN сервера з підтримкою шифрування в маршрутизаторі OPNsense.

Також було встановлено та налаштовано Windows Server 2022 як термінал сервер. Здійснено перевірку працездатності реалізованого рішення з тестової операційної системи Windows 10. Виконано серію тестів для оцінки ефективності та надійності створеної системи.

Підтверджено, що в даній конфігурації OpenVPN сервер стабільно підтримує шифровані VPN тунелі та забезпечує безпечний доступ до віртуалізованої корпоративної інфраструктури. Отримані результати дослідження сприятимуть створенню безпечних корпоративних мереж, забезпечуючи високий рівень захисту VPN-з'єднань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What are hypervisors. URL: https://www.ibm.com/topics/hypervisors (дата звернення: 24.01.2024).

2. Oracle VM VirtualBox User Manual. URL: https://www.virtualbox.org/manual/ (дата звернення: 24.01.2024).

3. VMware Workstation Pro Documentation. URL: https://docs.vmware.com/en/VMware-Workstation-Pro/index.html (дата звернення: 24.01.2024).

4. VMware Workstation Player Documentation. URL: https://docs.vmware.com/en/VMware-Workstation-Player/index.html (дата звернення: 24.01.2024).

5. VMware Fusion Documentation. URL: https://docs.vmware.com/en/VMware-Fusion/index.html (дата звернення: 24.01.2024).

6. Getting Started with Parallels Desktop 10: Docs & Videos. URL: https://kb.parallels.com/en/122673 (дата звернення: 24.01.2024).

7. 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. https://doi.org/10.62731/mcnd-24.05.2024.001

8. 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.

9. What is a firewall? How network firewalls work. URL: https://www.cloudflare.com/learning/security/what-is-a-firewall/ (дата звернення: 24.01.2024).

10. What is Virtual Firewall? URL: https://www.zenarmor.com/docs/network-security-tutorials/what-is-virtual-firewall (дата звернення: 24.01.2024).

11. VMware vSphere Documentation URL: https://docs.vmware.com/en/VMware-vSphere/index.html (дата звернення: 24.01.2024).

12. 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.

13. Details About Hardware Virtualization. URL: https://docs.oracle.com/en/virtualization/virtualbox/6.0/admin/hwvirt-details.html (дата звернення: 24.01.2024).

14. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ВИКОРИСТАННЯ ТЕХНІКИ ДИНАМІЧНОГО ВІДКРИВАННЯ МЕРЕЖЕВИХ ПОРТІВ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ СЕРВЕРІВ. Collection of scientific papers «ΛΌГОΣ», (May 24, 2024; Zurich, Switzerland), 233-234. https://doi.org/10.36074/logos-24.05.2024.051

15. OPNsense documentation. URL: https://docs.opnsense.org/intro.html (дата звернення: 24.01.2024).

16. 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. https://doi.org/10.62731/mcnd-14.06.2024.004

17. Viscosity OpenVPN. URL: https://www.sparklabs.com/viscosity/ (дата звернення: 24.01.2024).

18. Kuznetsov, A., Karpinski, M., Ziubina, R., Kandiy, S., Frontoni, E., Peliukh, O., ... & Kozak, R. (2023). Generation of nonlinear substitutions by simulated annealing algorithm. Information, 14(5), 259.

19. Tymoshchuk, V., Karnaukhov, A., & Tymoshchuk, D. (2024). USING VPN TECHNOLOGY TO CREATE SECURE CORPORATE NETWORKS. Collection of scientific papers «ΛΌГОΣ», (June 21, 2024; Seoul, South Korea), 166-170. https://doi.org/10.36074/logos-21.06.2024.034

20. Cipher Suite Knowledge Base. URL: https://scanigma.com/knowledge-base/tls/ciphersuite/tls-aes-256-gcm-sha384 (дата звернення: 24.01.2024).

21. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). СИСТЕМА ЗМЕНШЕННЯ ВПЛИВУ DOS-АТАК НА ОСНОВІ MIKROTIK. Матеріали конференцій МЦНД, (17.05. 2024; Ужгород, Україна), 198-200. https://doi.org/10.62731/mcnd-17.05.2024.008

22. Lechachenko, T., Kozak, R., Skorenkyy, Y., Kramar, O., & Karelina, O. (2023). Cybersecurity Aspects of Smart Manufacturing Transition to Industry 5.0 Model. In ITTAP (pp. 416-424).

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

24. Зацарний В.В, Праховнік Н.А., Землянська О.В. Безпека життєдіяльності: Конспект лекцій для студентів усіх спеціальностей за освітньо кваліфікаційним рівнем «бакалавр». Київ: НТУУ КПІ, 2016. 92 с.

25. Стручок В.С. Техноекологія та цивільна безпека. Частина «Цивільна безпека». Навчальний посібник. Тернопіль: ТНТУ, 2022. 150 с.