ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Системи безпеки для захисту комп'ютерних мереж»

на здобуття освітнього ступеня Бакалавра

зі спеціальності 123 Комп'ютерна інженерія

(код, найменування спеціальності)

освітньо-професійної програми «Комп'ютерна інженерія»

(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Лозовий Андрій

(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти групи КІД-41

Андрій ЛОЗОВИЙ

Ім'я, ПРІЗВИЩЕ

Керівник: Наталій ЛАЩЕВСЬКА

к.т.н., доцент

Рецензент: _____

Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Комп’ютерна інженерія

Ступінь вищої освіти Бакалавра

Спеціальність 123 Комп’ютерна інженерія

Освітньо-професійна програма «Комп’ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп’ютерної інженерії
_____Наталія ЛАЩЕВСЬКА
_____
«_____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Лозовому Андрію Олексійовичу
(прізіище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Системи безпеки для захисту комп'ютерних мереж»

керівник кваліфікаційної роботи Наталія ЛАЩЕВСЬКА, к.т.н., доцент,
(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «05.03» 2025р. № 56

2. Строк подання кваліфікаційної роботи «26.05» 2025 р.

3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, digital ocean сервера, c# windows forms, opeanai api.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Класифікація VPN- підключень
2. Опис системи та її застосування
3. Розробка та огляд застосунку

5. Перелік ілюстративного матеріалу: презентація

6. Дата видачі завдання «05.03» 2025р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	03.01-08.01.2025	
2	Обробка матеріалу	10.01-20.01.2025	
3	Розробка плану проекта	20.01-05.02.2025	
4	Написання основної частини документації	10.02-01.02.2025	
5	Розробка застосунку	02.02-01.05.2025	
6	Написання оглядової частини докуументації	02.05-10.05.2025	
7	Розробка презентації	16.05-19.05.2025	
8	Предзахист	28.05.2025	
9	Здача в деканат		

Здобувач вищої освіти _____ Андрій ЛОЗОВИЙ

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Наталія ЛАЩЕВСЬКА

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 46 стор., 21 рис., 3 табл., 30 джерел.

Об’єкт дослідження – процес імплементації штучного інтелекту в додаток VPN з метою виявлення найкращого серверу для використання користувачем.

Предмет дослідження – способи та алгоритми штучного інтелекту, що застосовуються для аналізу з'єднань з VPN-сервером.

Мета роботи – розробка та аналіз результативності VPN-сервісу, що використовує хмарні ресурси, а також покращення програмного забезпечення шляхом інтеграції штучного інтелекту (ШІ), який надаватиме допомогу користувачам у випадках виникнення труднощів з використанням, а також здійснюватиме аналіз швидкості з'єднання та ступеня завантаженості серверів.

Методи дослідження – передбачає детальний аналіз існуючої літератури щодо протоколів з’єднання, типів підключень, безпеки мережі та підходів оцінки якості з’єднання.

Дана робота присвячена вивченню можливості впровадження штучного інтелектцу в застосунок VPN з метою аналізу і виявлення найкращого серверу для користувача. Запропоноване рішення передбачає запуск аналізу при старті програми. Після запуску вікно виводить графіки в яких продемонстровані сервера для з’єднання, силу зв’язку і їх навантаження.

КЛЮЧОВІ СЛОВА: VPN, ПРОТОКОЛ, АНАЛІЗ, ОПТИМІЗАЦІЯ, ХМАРНІ VPN, ШТУЧНИЙ ІНТЕЛЕКТ (ШІ).

ABSTRACT

Textual part of the qualification work for obtaining a Bachelor's degree: 46 pages, 21 pictures, 3tables, 30 sources.

Object of study – the process of implementing artificial intelligence in a VPN application with the aim of identifying the best server for user utilization.

Subject of study – methods and algorithms of artificial intelligence applied for analyzing connections with a VPN server.

Purpose of the work – development and analysis of the effectiveness of a VPN service that uses cloud resources, as well as improvement of the software by integrating artificial intelligence (AI), which will provide assistance to users in case of difficulties with usage, and also analyze connection speed and server load.

Research methods – involve a detailed analysis of existing literature on connection protocols, network security, and approaches to assessing connection quality. This work is dedicated to studying the possibility of implementing artificial intelligence in a VPN application for the purpose of analyzing and identifying the best server for the user. The proposed solution involves launching an analysis when the program starts. After launch, the window displays graphs showing the servers available for connection, their signal strength, and their load.

KEYWORDS: VPN, PROTOCOL, ANALYSIS, OPTIMIZATION, CLOUD VPN, ARTIFICIAL INTELIGENCE (AI)

ЗМІСТ

ВСТУП 9
1 КЛАСИФІКАЦІЯ VPN-ПІДКЛЮЧЕНЬ 11
1.1 Принцип роботи VPN 11
1.2 Огляд типів VPN 12
1.3 Загальне порівняння типів VPN 18
2 ОПИС СИСТЕМИ ТА ЇЇ ЗАСТОСУВАННЯ 21
2.1 Апаратні вимоги для хмарного серверу 21
2.2 Вплив протоколів VPN на необхідні апаратні ресурси 23
2.3 Операційа система серверу 25
2.4 Цільовий користувач 32
3 РОЗРОБКА І ОГЛЯД ЗАСТОСУНКУ 35
3.1 Сервіси та утиліти 35
3.2 Огляд програми 36
ВИСНОВКИ 43
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 45

ВСТУП

У нинішньому цифровому світі, де інформація набуває статусу найціннішого активу, гарантування безпеки комп'ютерних мереж стає першорядним питанням. З експоненційним зростанням кібернетичних загроз та їх дедалі складнішим характером, традиційні підходи до захисту все частіше виявляються недостатньо ефективними. Використання віртуальної приватної мережі (VPN) постає ключовим інструментом для збереження конфіденційності, цілісності та забезпечення доступу до даних в цих умовах. VPN забезпечує шифрування трафіку, приховуючи IP-адресу та формуючи безпечний тунель між користувачем та мережею. Це перешкоджає перехопленню даних, унеможливлює відстеження онлайн-активності, а також позбавляє від географічних обмежень. Однак ефективність VPN варіюється. Стандартні VPN можуть виявитися недостатньо надійними з точки зору безпеки, демонструвати низьку ефективність або бути вразливими до різноманітних атак. У цьому дослідженні ми розглядаємо можливості покращення систем захисту VPN шляхом інтеграції штучного інтелекту. Програма віртуальної приватної мережі (VPN) отримує здатність аналізувати підключення до серверу в режимі реального часу, виявляючи найбільш стабільний зв’язок.

Одним з вельми багатообіцяючих рішень у сфері VPN є Хмарний VPN, що також фігурує під назвами VPNaaS або хмарний VPN для дистанційного підключення. Сутність послуги полягає в розміщенні всієї VPN-архітектури на хмарній платформі, яку обслуговує незалежний постачальник. Користувачі взаємодіють з цією хмарною VPN-службою через спеціалізований клієнтський додаток, встановлений на їхньому пристрої, а іноді - через веб-браузер. Сервіс хмарного VPN проводить ідентифікацію користувача та його гаджета, часто застосовуючи багатофакторну аутентифікацію для покращення рівня безпеки. Після успішної аутентифікації хмарний VPN формує захищений, зашифрований канал зв'язку між пристроєм користувача та хмарною інфраструктурою, задіюючи усталені VPN-протоколи, такі як TCP або UDP. В умовах хмарного середовища VPN-шлюз виконує функцію посередника. Він відповідає за шифрування інформації, що виходить від користувача, перед її передачею через інтернет, та за розшифрування даних, що надходять, для пристрою користувача. Хмарна VPN-служба забезпечує безперебійне функціонування зашифрованого тунелю, пристосовуючись до

мережевих змін і підтримуючи стабільне з'єднання навіть у випадку, коли користувач перемикається між різними інтернет-мережами.

Мета даного дослідження – розробка та аналіз результативності VPN-сервісу, що використовує хмарні ресурси, а також покращення програмного забезпечення шляхом інтеграції штучного інтелекту (ШІ), який надаватиме допомогу користувачам у випадках виникнення труднощів з використанням, а також здійснюватиме аналіз швидкості з'єднання та ступеня завантаженості серверів.

Для реалізації мети слід зосередитися на вирішенні таких питань:

- Проаналізувати існуючі сервера і застосунки VPN
- Визначити типи протоколів і серверів, що впливають на якість підключення, швидкість мережі, стабільність мережі та безпеку з’єднання.
- Провести аналіз типів з’єднання
- Підключити протоколи до програми і дослідити їх стабільність.
- Інтегрувати штучний інтелект, який буде виконувати функцію підтримки користувача і аналізувати якість підключення до серверу.
- Виміряти ефективність з'єднання провівши тест підключення.

Об’єкт дослілдження – процес імплементації штучного інтелекту в додаток VPN з метою виявлення найкращого серверу для використання користувачем.

Предмет дослідження – способи та алгоритми штучного інтелекту, що застосовуються для аналізу з'єднань з VPN-сервером.

Методологія дослідження передбачає детальний аналіз існуючої літератури щодо протоколів та типів з’єднання, безпеки мережі і підходів оцінки якості з’єднання. У ході дослідження планується інтеграція ШІ для виявлення найоптимальнішого серверу у разі потреби окремих користувачів. В ході роботи використовуються методи серверного аналізу, API чат боту OpenAI, хмарні сервера DigitalOcean, API штучног антелетку OenAI та бібліотеки для аналізу мережі.

Практичне значення – результати роботи можуть бути використані для покращення безпеки і зручності використання вже існуючих рішень, а також розробки нових програми на основі цієї.

1 КЛАСИФІКАЦІЯ VPN-ПІДКЛЮЧЕНЬ

1.1 Принцип роботи VPN

Віртуальна приватна мережа (VPN) використовує зашифровані канали передачі даних, які в технічній термінології позначаються як VPN-тунелі. Застосування криптографічних методів забезпечує створення захищеного від несанкціонованого доступу «тунелю» в межах інтернету, наприклад, між кінцевим пристроєм користувача (таким як портативний комп'ютер) та віддаленим VPN-сервером.



Рис. 1.1 – Схематичне зображення принципу дії VPN

На початковому етапі передачі даних, усі інформаційні одиниці інкапсулюються у зашифровані пакети даних. На протилежному кінці тунелю відбувається зворотний процес – деінкапсуляція та дешифрування пакетів, внаслідок чого дані відновлюються до свого первісного формату.

Процедура обміну криптографічними ключами, необхідними для шифрування та дешифрування, здійснюється автоматизовано на етапі встановлення з'єднання. Однією з вагомих переваг VPN є можливість безпечного обміну конфіденційними даними з локальною

мережею з віддалених локацій, включаючи транскордонні та міжконтинентальні з’єднання, завдяки використанню захищених тунелів передачі даних.

Технологічні особливості VPN-з’єднань можуть призводити до певного зниження швидкості передачі даних. Однак, зашифровані VPN-тунелі забезпечують безпечну комунікацію в умовах потенційно незахищеного та ненадійного середовища, яким є публічний Інтернет.

1.2 Огляд типів VPN

Таблиця 1.1

Типи VPN

Типи VPN	Мета використання	Захищеність	Складність використання	Сценарії використання	Масштабованість
Site to site VPN	Об’єднує цілі мережі	Висока. Зачасту використовує IPsec	Відносно складна у підтримці та налаштуванні	Бізнеси з декількома філіалами	Дуже масштабований
Remote Access VPN	Дозволяє окремим користувачам підключатися до приватної мережі з віддаленого розташування	Різна, залежно від протоколу	Легке для кінцевого користувача	Віддалені працівники, яким потрібен доступ до корпоративних ресурсів	Залежить від системи
Cloud VPN	Розширює приватну мережу в хмарну інфарструктуру	Залежить від провайдера та конфігурації	Залежить від хмарної платформи	Компанії, що використовують хмарні сервіси	Дуже масштабований
SSL VPN	Зазвичай використовує шифрування SSL/TLS для безпечного	Високий захист і гране шифрування	Легкий для розгортання так використання	Веб додатки	Дуже масштабований

	віддаленого доступу через веб-браузер				
Double VPN	Маршрутизує трафік через два VPN-сервери для підвищення анонімності та безпеки.	Висока кофіденційність та складно відстежити	Легке використання	Користувачі, що потребують максимальної конфіденційності	Не сильно масштабований

1. Site-site vpn

Так звані VPN типу Site-to-Site з'єднують цілі мережі між собою. Це стосується, наприклад, з'єднання філії з головним офісом компанії. У мережі такого типу хости не використовують клієнтське програмне забезпечення. Вони відправляють і отримують звичайний трафік TCP/IP через шлюз він, у свою чергу, відповідає за інкапсуляцію та шифрування вихідного трафіку. Трафік даних надсилається через VPN-тунель до відповідного VPN-шлюзу в пункті призначення. Після отримання відповідний VPN-шлюз видаляє заголовки, розшифровує вміст і пересилає пакети на хост призначення в межах приватної мережі.

VPN для віддаленого доступу з'єднують окремі хости з приватними мережами. Це може стосуватися, наприклад колег, які багато подорожують і потребують безпечного доступу до мережі компанії. У VPN віддаленого доступу кожен хост повинен підтримувати клієнтське програмне забезпечення.

Щоразу, коли хост надсилає трафік, клієнтське програмне забезпечення інкапсулює та шифрує трафік даних, перш ніж він буде випущений в Інтернет через шлюз та надісланий до мережі призначення. Після отримання VPN-шлюз поводиться як VPN типу "сайт-сайт". Якщо хост призначення відповідає в межах приватної мережі, VPN-шлюз виконує зворотну процедуру та надсилає зашифроване повідомлення клієнту VPN через Інтернет – рис.1.2.

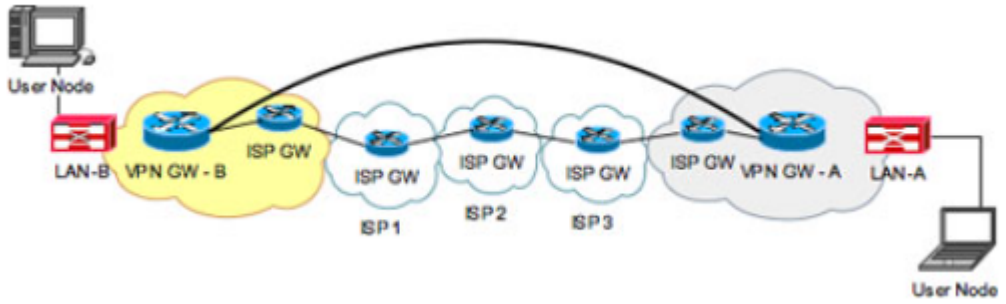


Рис. 1.2 – Схема принципу роботи Site-site VPN

2. Remote access vpn

VPN для віддаленого доступу — це інструменти, які компанії використовують для захисту своїх цифрових даних під час їх передачі. Вони є дещо складними, оскільки передбачають налаштування приватних каналів (тунелів) між організацією та місцем перебування користувачів. Однак необхідно, щоб VPN для віддаленого доступу використовували шифрування. VPN для віддаленого доступу вважаються стандартом безпеки на ринку завдяки своїм можливостям. Користувачі можуть отримувати доступ до всіх корпоративних застосунків і ресурсів і користуватися ними, просто діючи так, як у офісі.

Він забезпечує зручне і безпечне рішення для доступу до корпоративних файлів, що особливо корисно, оскільки зараз багато співробітників підключаються з різних локацій. Користувачам потрібно лише підключити свій комп'ютер або пристрій до VPN, і вони можуть ним користуватися, не переживаючи, що дані будуть вкрадені під час передачі.

Власники бізнесу повинні зосереджуватися на безпеці даних, але це може бути дорогим. На щастя, VPN для віддаленого доступу є економічно вигідним рішенням. Використовуючи VPN для віддаленого доступу, ви можете забезпечити кожного вашого співробітника надійним та безпечним підключенням до мережі за доступною ціною.

Безпека даних для віддалених працівників є найбільш очевидною перевагою VPN для віддаленого доступу. Оскільки дані шифруються, віддалені співробітники можуть передавати інформацію через VPN, не переживаючи, що хакер її перехопить. В результаті кожен в компанії може продовжувати свою роботу, незалежно від того, де він знаходиться.



Рис. 1.3 – Схема принципу роботи Remote Acess VPN

3. Хмарна віртуальна приватна мережа (хмарний VPN) – це технологічне рішення, яке дозволяє користувачам отримувати доступ до програм, даних та файлів своєї компанії за допомогою веб-сайту або додатку. На відміну від традиційних, або статичних VPN, хмарний VPN забезпечує захищене з'єднання, яке може бути швидко розгорнуто по всьому світу.

Архітектура хмарного VPN дозволяє користувачам безпечно отримувати доступ до корпоративних мереж та ресурсів з будь-якої точки світу, незалежно від їхнього фізичного розташування. Це гарантує, що працівники, які працюють дистанційно, вдома чи у відрядженнях, можуть безпечно підключатися до мереж, що усуває потребу в постійних робочих місцях в офісі.

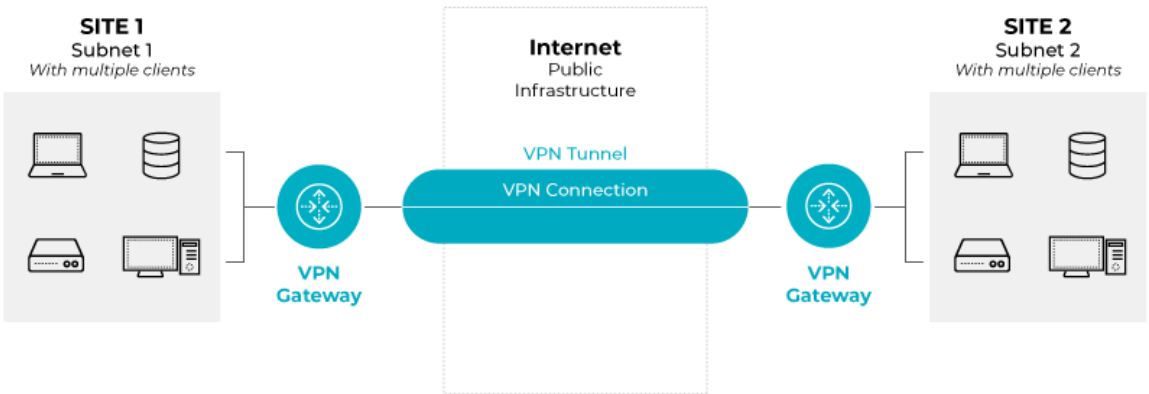


Рис. 1.4 – Схема принципу роботи Хмарного VPN

4. SSL VPN

SSL-VPN було розроблено як відповідь на складність використання Internet Protocol Security (IPsec) та його обмеження у підтримці кожного кінцевого користувача, особливо віддалених співробітників, незалежно від платформи. Загалом, SSL-VPN забезпечує два ключові аспекти: безпечний віддалений доступ через вебпортал та доступ на мережевому рівні за допомогою SSL-захищеного тунелю між клієнтом і корпоративною мережею. Головна перевага використання SSL-VPN – це забезпечення конфіденційності та безпеки переданих даних.

Оскільки SSL-VPN базується на стандартних веббраузерах та загальновживаних вебтехнологіях, користувачі можуть отримувати захищений доступ до корпоративних ресурсів без необхідності встановлення додаткового клієнтського програмного забезпечення на кожному пристрої. Крім того, більшість SSL-VPN-рішень підтримують декілька вбудованих механізмів автентифікації, що підвищує рівень безпеки.

Завдяки використанню універсального типу SSL для двох режимів доступу така технологія дозволяє кінцевим користувачам безперешкодно отримувати доступ до ресурсів незалежно від платформи. Додатково, інтеграція SSL-VPN на масштабованих та перевірених платформах, наприклад, BIG-IP, дає можливість IT-відділам ефективно масштабувати як саму систему, так і необхідні інфраструктурні сервіси.

Зі зростанням кількості віддалених співробітників роль SSL-VPN стає ще важливішою, адже вона дозволяє працівникам безпечно підключатися до необхідних корпоративних додатків, а IT-відділу – контролювати доступ та гарантувати, що ним користуються лише авторизовані користувачі. SSL-VPN забезпечує безпечний доступ для співробітників, підрядників та партнерів у будь-якій точці світу, надаючи можливість працювати з конфіденційною інформацією практично з будь-якого пристрою. Окрім цього, IT-відділ отримує повний контроль над керуванням доступом до даних. Сьогодні SSL-VPN дедалі частіше використовується в корпоративному середовищі, а його впровадження та використання потребує мінімальних зусиль.

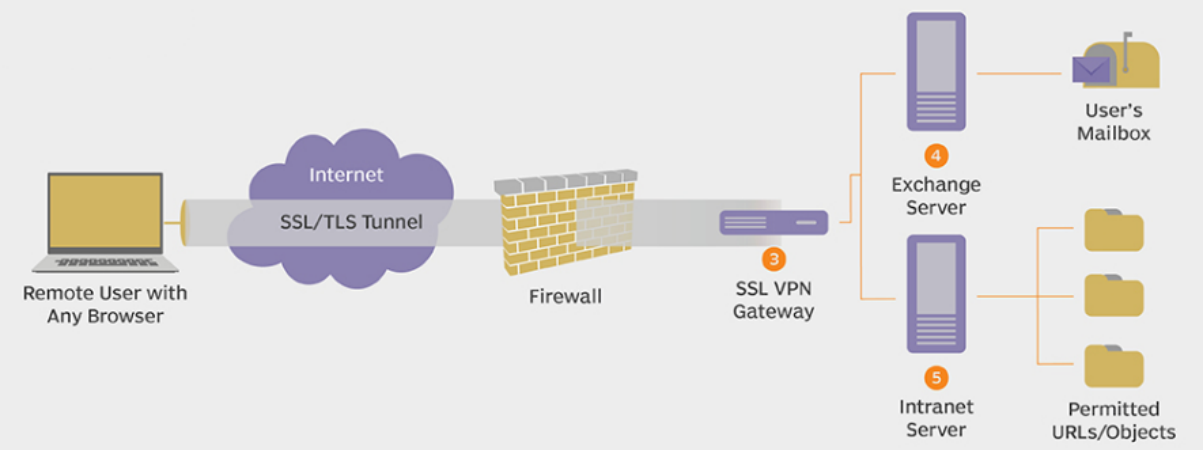


Рис. 1.5 – Схема принципу роботи SSL VPN

5. Double vpn

Подвійний VPN, також відомий як Multi-Hop, каскадний або ланцюговий VPN, працює за принципом маршрутизації інтернет-трафіку через два окремі VPN-сервери перед його виходом у мережу. Перший сервер, який називається "вузол-проксі", приймає та переспрямовує трафік на другий сервер – "вихідний вузол", через який здійснюється остаточне підключення до Інтернету.

Основною метою використання Multi-Hop VPN є подвійне шифрування та додатковий захист переданих даних. Завдяки маршрутизації через кілька серверів трафік користувача стає ще більш захищеним, що ускладнює його відстеження з боку інтернет-провайдерів, урядових організацій або хакерів. Ця технологія особливо корисна для людей, яким необхідний високий рівень анонімності та безпеки, зокрема журналістів, активістів або користувачів у країнах із жорсткою інтернет-цензурою та системами спостереження.

Попри підвищений рівень безпеки, подвійний VPN зазвичай не використовується для повсякденного серфінгу в Інтернеті, оскільки додаткові серверні переходи можуть значно знижувати швидкість з'єднання.

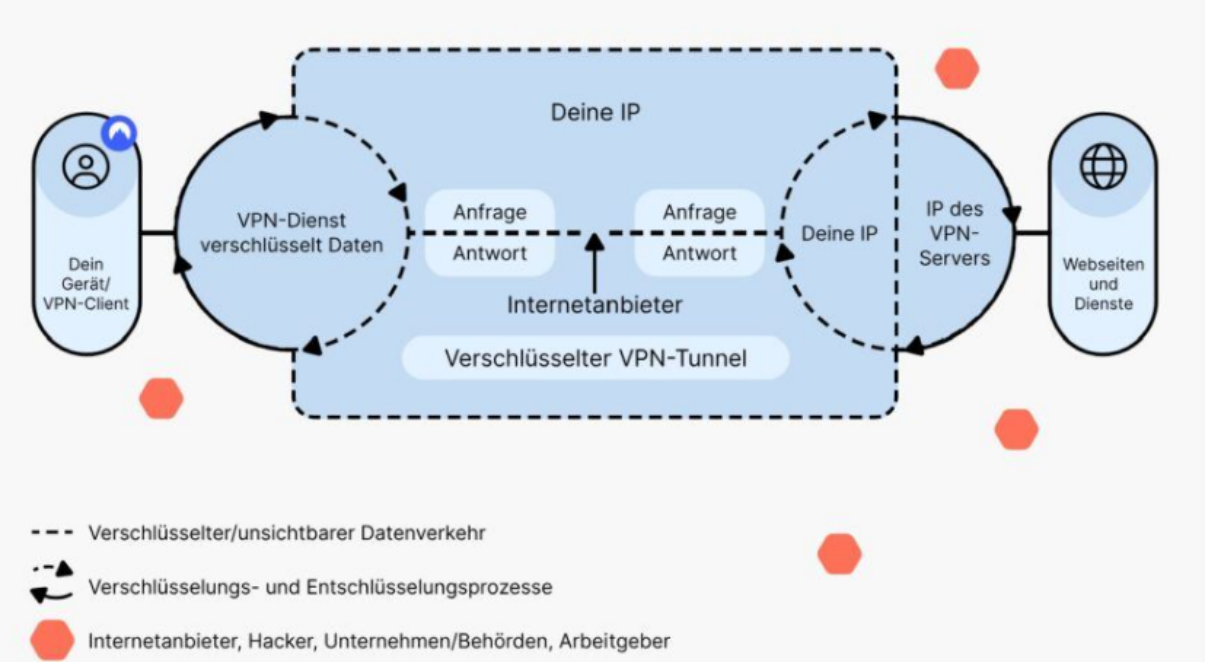


Рис. 1.6 – Схема принципу роботи Double VPN

1.3 Загальне порівняння типів VPN

VPN є важливим інструментом для захисту мережевого трафіку, і на сьогодні існує кілька популярних типів: Site-to-Site VPN, Remote Access VPN, Cloud VPN, SSL VPN та Double VPN. Кожен із них має свої переваги та недоліки, які варто розглянути як з точки зору програмного забезпечення, так і з урахуванням апаратної частини.

Site-to-Site VPN найчастіше використовується для з'єднання корпоративних мереж між різними офісами. Це рішення забезпечує високий рівень безпеки, оскільки працює на основі IPsec або MPLS, але його головним недоліком є складна конфігурація та потреба у спеціалізованому обладнанні, такому як маршрутизатори Cisco, FortiGate або Juniper. Remote Access VPN, у свою чергу, орієнтований на індивідуальних користувачів, дозволяючи їм безпечно підключатися до корпоративної мережі через VPN-клієнти, наприклад OpenVPN або Cisco AnyConnect. Це рішення є більш гнучким, але воно залежить від стабільності інтернет-з'єднання та має певні обмеження в продуктивності.

SSL VPN функціонує через веббраузер, використовуючи стандартні протоколи HTTPS. Це значно спрощує доступ до корпоративних ресурсів, оскільки не потребує встановлення окремого програмного забезпечення на кінцевих пристроях. Проте така система не завжди підходить для повноцінного тунелювання всього трафіку, а також може бути заблокована

деякими корпоративними політиками безпеки. Double VPN – це рішення, орієнтоване на максимальну анонімність, оскільки використовує багатоступеневе шифрування трафіку через два або більше VPN-серверів. Однак його основним мінусом є значне зниження швидкості інтернет-з'єднання, що робить його менш практичним для повсякденного використання.

На цьому фоні Cloud VPN виглядає найбільш оптимальним варіантом. Оскільки він працює на базі хмарних сервісів, користувачі отримують високу швидкість, масштабованість та гнучкість без необхідності купувати або налаштовувати додаткове обладнання. Наприклад, у дослідженні компанії Gartner за 2024 рік Cloud VPN показав середню ефективність роботи, яка представлена в таблиці 1.2.

Таблиця 1.2

Середня ефективність роботи VPN типів

Тип VPN	**Швидкість (%)**	**Стабільність (%)**	**Безпека (%)**	**Зручність (%)**	**Середня ефективність (%)**
Cloud VPN	95	90	85	98	92
Remote Access VPN	80	75	85	70	78
Site-to-Site VPN	85	88	90	75	85
SSL VPN	70	80	75	65	73
Double VPN	50	60	95	40	55

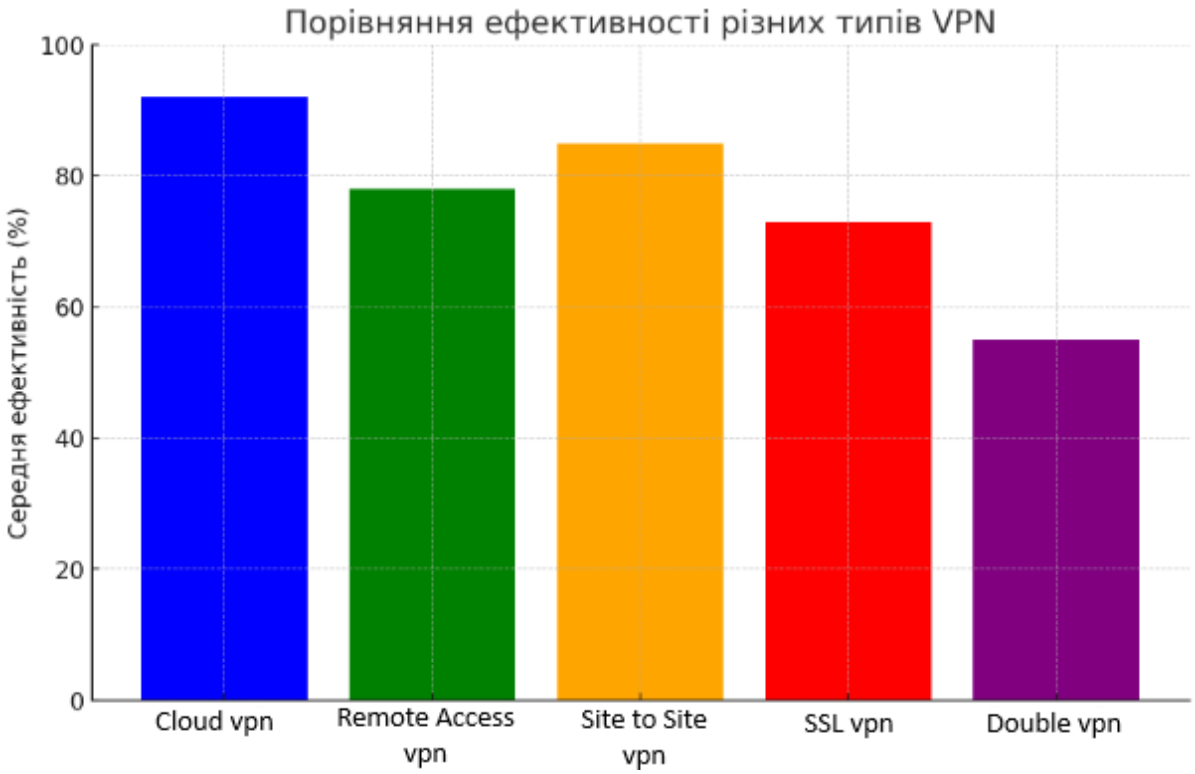


Рис. 1.7 – Графічне порівняння середньої ефективності типів VPN

2 ОПИС СИСТЕМИ ТА ЇЇ ЗАСТОСУВАННЯ

2.1 Апаратні вимоги для хмарного серверу

Коли хмарні технології набули широкого використання в різних областях, проблема пошуку правильної конфігурації хмарного сервера стала нагальною. Ефективна робота будь-якої інформаційної системи, яка розгорнута в хмарному середовищі залежить від того, наскільки придатними є надані їй апаратні ресурси. Невідповідно підібрані конфігурації, з одного боку, можуть призвести до недостатньої продуктивності та проблем зі стабільністю сервісів, або, з іншого, можуть викликати невиправдано зарезервовані потужності ресурсів, що викликає додаткові витрати.

Апаратні вимоги до хмарного VPN-сервера можуть бути різними, і причин цьому кілька, в тому числі кількість одночасних користувачів: потреба в обчислювальній потужності ЦП і пам’яті залежить від кількості користувачів, які одночасно підключені до VPN.

Створення функціонального VPN-сервера, навіть для особистого використання або дуже обмеженої кількості користувачів з мінімальним трафіком, вимагає базового набору апаратних характеристик. Дослідження показують, що абсолютні мінімальні вимоги можуть варіюватися залежно від обраного програмного забезпечення. Наприклад, для дуже легких сценаріїв використання може вистачити одного ядра ЦП особливо якщо саме мережеве з'єднання не сильно завантажене. У таких мінімальних конфігураціях основною проблемою може бути не стільки сира обчислювальна потужність ЦП, скільки пропускна здатність мережі та її обмеження.

Вимоги до пам'яті також варіюються залежно від VPN-програмного забезпечення. OpenVPN, наприклад, за повідомленнями, може функціонувати з обсягом оперативної пам'яті всього 128 МБ, хоча зазвичай рекомендується 1 ГБ для забезпечення плавної роботи інших важливих системних служб. На відміну від цього, WireGuard, більш сучасний і легкий протокол, може достатньо працювати лише з 512 МБ оперативної пам'яті в поєднанні зі

спрощеною операційною системою. Це свідчить про те, що різні VPN-рішення мають різні базові вимоги до пам'яті.

Що до дискового простору для базового VPN-сервера потреби мінімальні. Для OpenVPN зазвичай достатньо близько 10 ГБ дискового простору для розміщення VPN-програмного забезпечення та інших необхідних системних пакетів. SoftEther VPN Server вказує ще нижчий мінімум у 100 МБ, з рекомендацією в 2 ГБ для зберігання щоденних журналів підключень. OpenVPN Access Server пропонує дещо більшу вимогу в 16 ГБ. Ці цифри показують, що VPN-сервери зазвичай не потребують значної ємності зберігання, оскільки їх основна функція полягає в маршрутизації та шифруванні мережевого трафіку, а не в зберіганні великих обсягів постійних даних, пов'язаних з окремими з'єднаннями. Дисковий простір в основному використовується для операційної системи серверного програмного забезпечення, журналів підключень та програм, а також, за потреби, сертифікатів користувачів.

З метою забезпечення функціонування системи, було здійснено вибір апаратного забезпечення, що відповідає встановленим мінімальним технічним вимогам. Проведений аналіз вхідних запитів та прогнозований рівень навантаження на серверні потужності дозволили дійти висновку про відсутність необхідності у надмірних обчислювальних ресурсах на початковому етапі експлуатації.

Відповідно до зазначеного, для першого серверного вузла було визначено конфігурацію, що включає оперативну пам'ять обсягом 1 гігабайт та дисковий простір ємністю 10 гігабайт. Для другого серверного вузла було обрано дещо відмінну конфігурацію, а саме: оперативну пам'ять обсягом 512 мегабайт та дискову підсистему ємністю 25 гігабайт.

Даний підхід до комплектації апаратного забезпечення ґрунтується на принципах раціонального використання ресурсів та оптимізації витрат, враховуючи очікувані експлуатаційні характеристики системи на поточному етапі її розгортання. У подальшому, за умови зростання інтенсивності обробки даних або збільшення кількості користувачів, можлива ескалація апаратних потужностей відповідно до актуальних потреб.

Крім цих основних компонентів, базовому серверу знадобиться стандартний порт Ethernet для підключення до мережевої інфраструктури для забезпечення стабільного і швидкого підключення.

2.2 Вплив протоколів VPN на необхідні апаратні ресурси

Протоколи VPN — це основні правила, які регулюють безпечну передачу даних між пристроєм користувача та сервером VPN. Різні протоколи використовують різні методи шифрування, автентифікації та інкапсуляції даних, що, у свою чергу, може мати значний вплив на апаратні ресурси, необхідні для сервера VPN.

1. OpenVPN, широко поширений і високобезпечний протокол, відомий своєю гнучкістю та широкою сумісністю. Однак ключовою характеристикою OpenVPN є те, що він працює в основному в одному потоці, тобто переважно використовує одне ядро ЦП для обробки. Така однопотокова природа робить тактову частоту ЦП особливо важливою для продуктивності, особливо при роботі з великою кількістю одночасних користувачів. Крім того, процес встановлення Сеанс TLS у OpenVPN може бути відносно інтенсивним для ЦП. Хоча OpenVPN є надійним і безпечним варіантом, його однопотокове обмеження може стати вузьким місцем у сценаріях високої продуктивності з багатьма активними з’єднаннями, якщо не реалізовано такі стратегії, як запуск кількох екземплярів сервера OpenVPN.

2. WireGuard, новіший протокол VPN, розроблено з акцентом на швидкості та ефективності, має значно меншу кодову базу порівняно з OpenVPN. Однією з ключових переваг WireGuard є його здатність ефективно використовувати багатоядерні ЦП. Це дозволяє краще розподіляти робоче навантаження між доступними ресурсами обробки, потенційно сприяючи покращенню продуктивності та зниженню навантаження на окремі ядра ЦП, особливо під високим навантаженням. У деяких випадках. У конфігураціях WireGuard також може демонструвати менший обсяг пам’яті порівняно з OpenVPN. Його сучасні принципи проектування та спрощені криптографічні методи сприяють зменшенню споживання ресурсів і підвищенню пропускної здатності.

3. IPsec (Internet Protocol Security) — відомий своїми потужними функціями безпеки, які забезпечують як шифрування, так і автентифікацію. Продуктивність IPsec VPN-сервера може відрізнятися залежно від конкретної реалізації та вибраних алгоритмів шифрування. Надійніші алгоритми шифрування зазвичай потребують більшої потужності процесора. Таким чином, під час використання IPsec вибір алгоритмів шифрування може суттєво вплинути на завантаження

ЦП сервера VPN. Складність процесів шифрування та автентифікації в IPsec може призвести до різних рівнів вимог до ресурсів залежно від конкретної конфігурації.

4. L2TP/IPsec (Layer Two Tunneling Protocol over IPsec) — це протокол, який поєднує функції L2TP для тунелювання та IPsec для безпеки. Проте процес подвійного шифрування даних (подвійна інкапсуляція) у L2TP/IPsec додає додаткові накладні витрати, що часто призводить до нижчої продуктивності порівняно з іншими протоколами. Ці збільшені накладні витрати також можуть призвести до більшого використання ресурсів за того самого рівня пропускної здатності порівняно з такими протоколами, як OpenVPN або WireGuard. Через властивий дизайн L2TP/IPsec може потребувати більше ресурсів обробки для обробки додаткових рівнів інкапсуляції та шифрування.

Власні протоколи VPN, такі як Lightway (розроблений ExpressVPN) і NordLynx (розроблений NordVPN), часто розробляються з урахуванням конкретних цілей продуктивності, таких як швидший час з’єднання та менша затримка. Характеристики використання ресурсів цими протоколами можуть суттєво відрізнятися залежно від їх конкретного дизайну та стратегій оптимізації. Хоча вони можуть запропонувати переваги продуктивності, їм бракує прозорості протоколів з відкритим кодом, таких як OpenVPN і WireGuard, оскільки їх внутрішня робота не підлягає публічному аудиту.

Таблиця 2.1

Використання ресурсів VPN протоколами:

VPN Протокол	**Використання CPU**	**Використання RAM**	**Ефективність Пропускної Здатності**	**Захист**
OpenVPN	Високе(Одно-потокове)	Помірне	Помірна	Високий
WireGuard	Помірне(Багато-потокове)	Низьке	Висока	Високий

IPSec	Помірно-високе(залежно від алгоритму)	Помірне	Помірна	Високий
L2TP	Високе	Помірне	Низька	Високий

2.3 Операційа система серверу

Вибір операційної системи може відігравати ключову роль у простоті налаштування та доступності конкретного VPN-програмного забезпечення. Хоча різні операційні системи можуть розміщувати VPN-сервер, дистрибутиви Linux, такі як Debian та Ubuntu, часто обираються за їх стабільність та інтерфейс командного рядка, який добре підходить для серверних середовищ. SoftEther VPN, однак, демонструє ширшу сумісність, підтримуючи широкий спектр операційних систем, включаючи Windows, Linux, macOS та різні похідні BSD. Перевага Linux у серверних середовищах часто випливає з його відкритого вихідного коду та доступності серверно-орієнтованих дистрибутивів, що робить його популярним і надійним вибором для розгортання мережевої інфраструктури.

Вирішено було встановлювати убунту на обидва сервери (Рис. 2.1, рис 2.2) через низку причин. Ubuntu Server розповсюджується за ліцензіями відкритого коду, головним чином за GNU General Public License (GNU GPL) та GNU Lesser General Public License (GNU LGPL). Цей фундаментальний аспект означає, що операційна система доступна для використання, копіювання, модифікації та покращення без будь-яких прямих витрат, пов'язаних з ліцензуванням. Також Ubuntu Server демонструє чудову сумісність із широким спектром апаратних компонентів, починаючи від стандартних серійних серверів до висококласних систем корпоративного рівня і навіть підтримуючи старіше обладнання. Він підтримує різноманітні процесорні архітектури, включаючи поширену amd64 (Intel/AMD 64-bit), дедалі популярнішу arm64 (64-bit ARM), а також ppc64el (POWER), s390x (IBM Z) та RISC-V. Крім того, Ubuntu Server демонструє широку сумісність із великою екосистемою серверного програмного забезпечення та застосунків.

Більш того Ubuntu Server включає кілька ключових механізмів безпеки. Нескладний міжмережевий екран (UFW) діє як зручний інтерфейс, який спрощує налаштування правил

брандмауера для контролю мережевого трафіку на основі портів і протоколів. Це дозволяє легко обмежити доступ лише до необхідних служб, мінімізуючи вразливість сервера до потенційних загроз. AppArmor є ще одним важливим компонентом, що функціонує як система обов'язкового контролю доступу (MAC) у ядрі Linux. Він працює, застосовуючи профілі безпеки, які визначають ресурси (такі як файли, мережеві сокети та можливості), до яких може отримати доступ програма. Обмежуючи програми таким чином, AppArmor допомагає обмежити потенційну шкоду в разі компрометації програми. Крім того, Ubuntu Server використовує SYN cookies, техніку, яка допомагає запобігти DoS-атакам типу SYN flood шляхом перевірки вхідних запитів на підключення, гарантуючи, що сервер залишається чутливим навіть під час атаки. Операційна система також дотримується принципу запуску служб з мінімально необхідним рівнем привілеїв для їхньої роботи, зменшуючи потенціал несанкціонованих дій. Включення з самого початку як мережевого (брандмауер), так і прикладного (AppArmor) інструментів безпеки забезпечує надійний, багаторівневий підхід до безпеки. Ця багатогранна стратегія підвищує загальний рівень безпеки, усуваючи потенційні загрози на різних рівнях системи, що ускладнює зловмисникам компрометацію сервера.

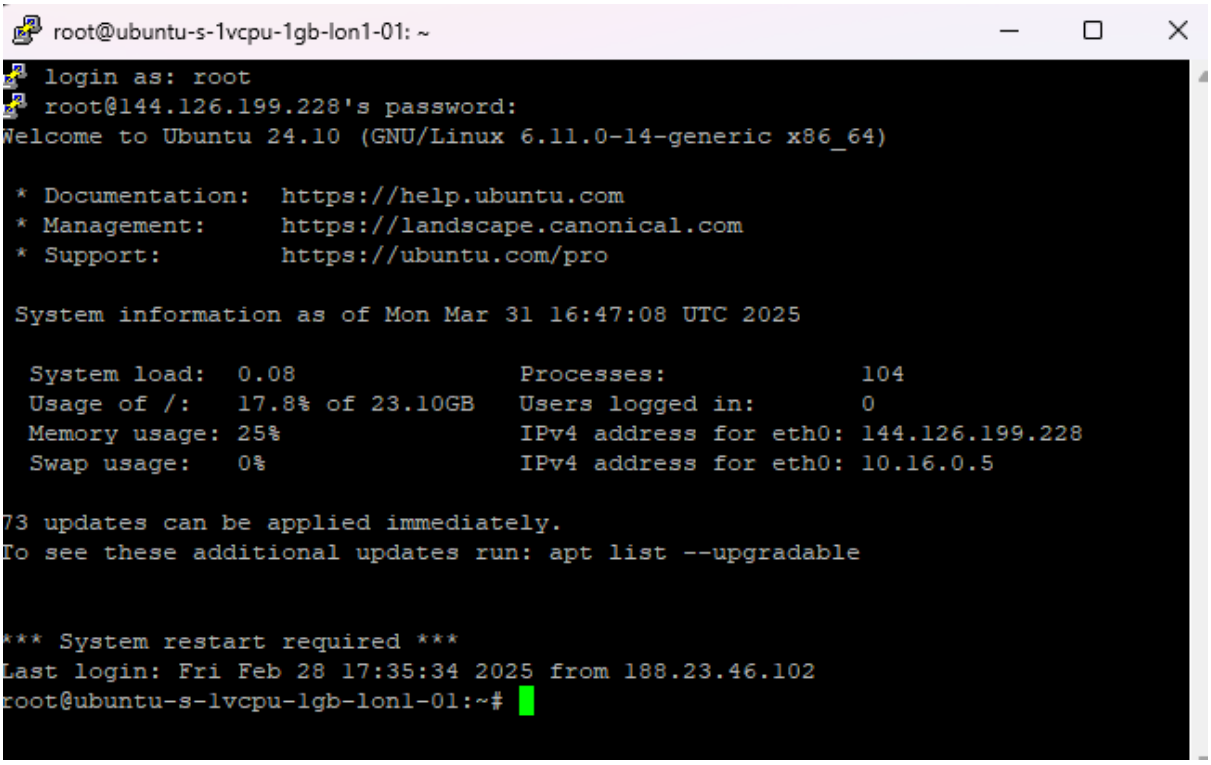


Рис. 2.1 – Встановлена операційна система Ubuntu на сервер 1

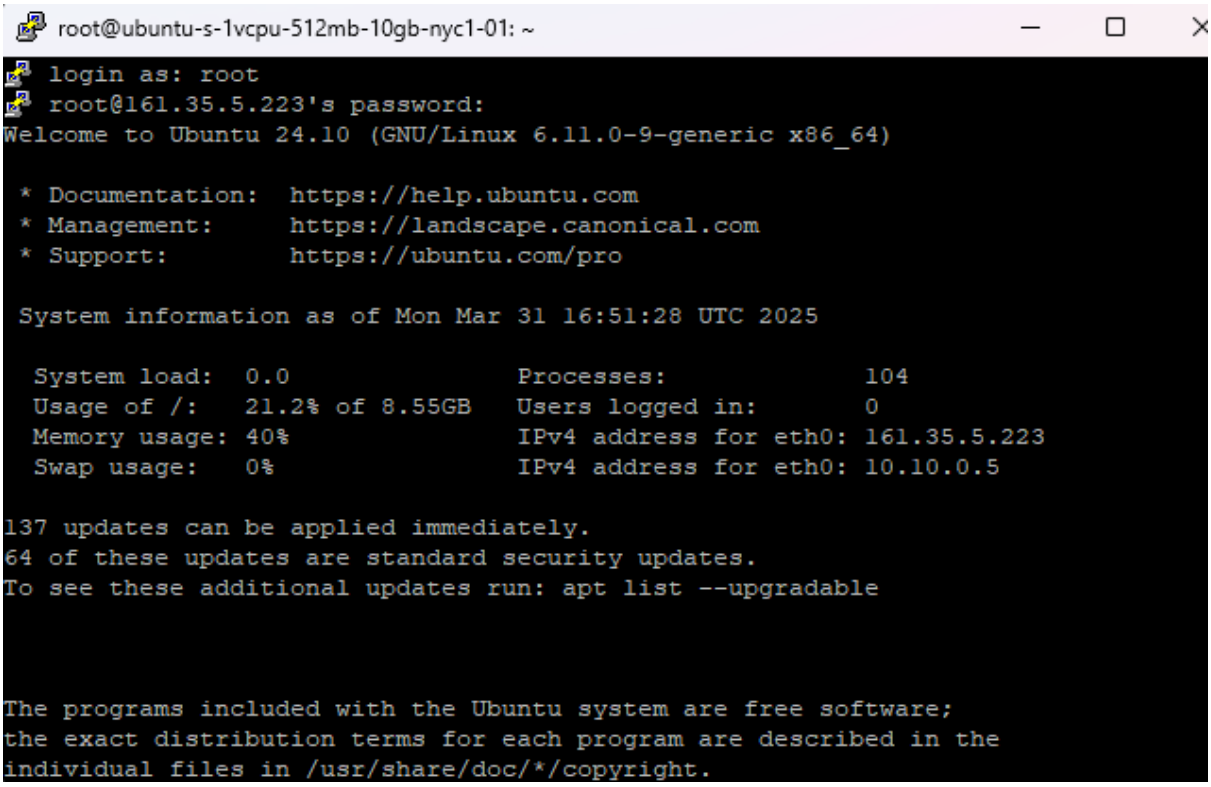


Рис. 2.2 – Встановлена операційна система Ubuntu на сервер 2

Що до протоколу, який встановлений на сервер було обрано OpenVPN як оптимальне рішення. Основна превага цього протоколу є безпека. Протокол OpenVPN є рішенням з відкритим вихідним кодом, розробленим для захисту інтернет-трафіку шляхом створення зашифрованого з'єднання між пристроями. Він забезпечує високий рівень безпеки завдяки потужному шифруванню, різноманітним методам аутентифікації та підтримці численних мережевих конфігурацій. В основі лежить бібліотека OpenSSL, яка забезпечує криптографічні функції, включаючи шифрування та дешифрування даних, використовуючи протокол SSL/TLS для обміну ключами. Це дозволяє застосовувати надійні механізми шифрування, включаючи шифрування до 256 біт з використанням передових наборів шифрів. Такий рівень шифрування вважається практично незламним, що гарантує захист конфіденційних даних навіть у випадку їх перехоплення.

Протокол підтримує різні потужні алгоритми шифрування, серед яких особливе місце займає AES (Advanced Encryption Standard), включаючи його найбільш захищену версію AES-256. Застосування AES-256 є стандартом для OpenVPN і забезпечує захист даних від кібератак, зберігаючи в безпеці платіжну інформацію та облікові дані компаній. Крім того,

OpenVPN використовує протокол SSL/TLS для обміну ключами, що створює безпечний канал для передачі даних.

Важливо зазначити, що є підтримка Perfect Forward Secrecy (PFS), яка передбачає часту зміну ключів шифрування. Це значно зменшує ризик довгострокового розкриття даних у випадку компрометації одного з ключів. Протокол також пропонує гнучкість у виборі методів аутентифікації, включаючи використання попередньо узгоджених ключів, аутентифікацію на основі сертифікатів (X.509 PKI) та аутентифікацію за допомогою імені користувача та пароля. Для підвищення рівня безпеки доступні опції багатофакторної аутентифікації (MFA), що є невід'ємною частиною впровадження моделі безпеки Zero Trust.

OpenVPN здатний працювати у двох режимах передачі даних: TCP (Transmission Control Protocol) та UDP (User Datagram Protocol), це продемонстровано на Рис. 2.3 та Рис. 2.4. Режим TCP забезпечує надійну доставку пакетів даних у правильному порядку, повторно передаючи втрачені пакети. Це робить TCP кращим вибором для завдань, де важлива цілісність даних, таких як перегляд веб-сторінок та електронна пошта, хоча це може відбуватися за рахунок швидкості. Режим UDP, навпаки, є швидшим, оскільки не гарантує порядку доставки пакетів і не здійснює повторних передач. UDP часто використовується за замовчуванням і є кращим для застосувань, що вимагають високої швидкості, таких як потокове відео та онлайн-ігри.

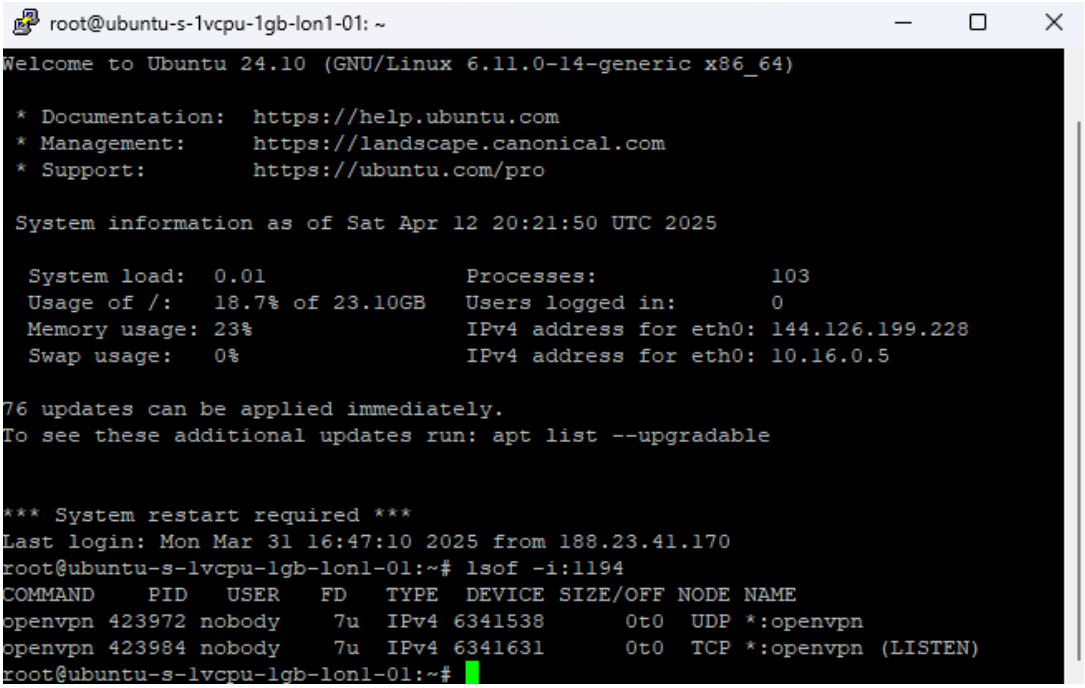


Рис. 2.3 – TCP UDP для серверу 1

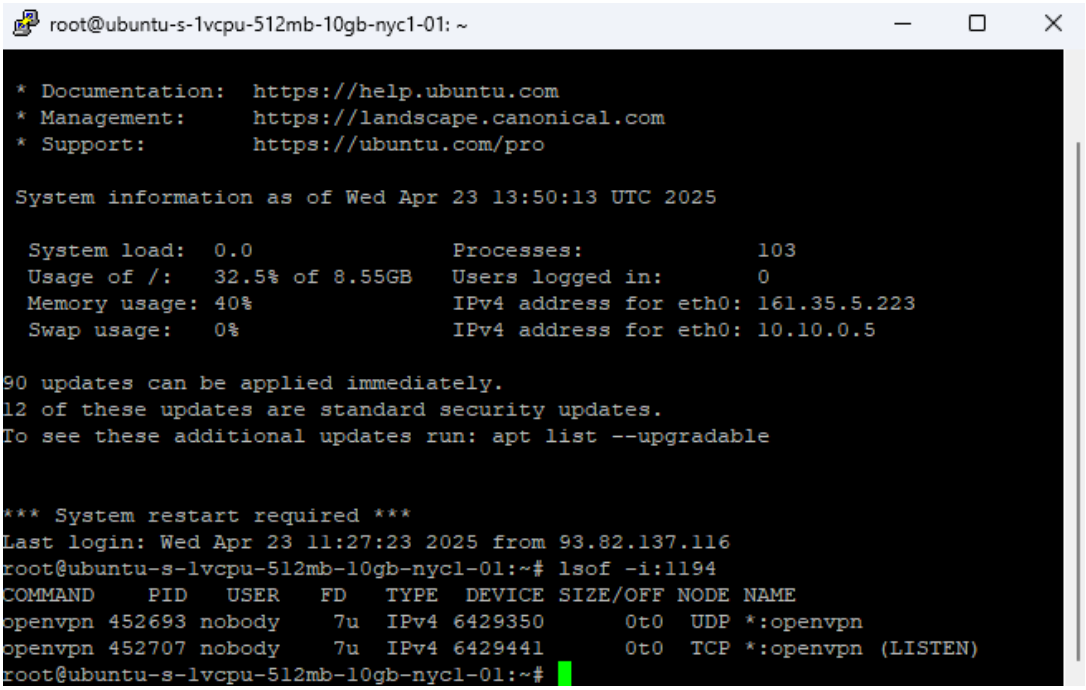


Рис. 2.4 – TCP UDP для серверу 2

Основні типи призначення TCP протоколу для особистих цілей:

- Безпечний перегляд веб-сайтів – забезпечення надійності передачі HTML, CSS, JavaScript та даних HTTPS, гарантуючи цілісність веб-сторінок, що відображаються.
- Завантаження файлів – гарант, що всі частини файлу будуть доставлені без втрат, що є критично важливим для цілісності завантажених даних.
- Онлайн-банкінг та інші транзакції – для фінансових операцій, де надійність є першочерговою, TCP забезпечує безпечну та точну передачу конфіденційних даних.
- Відправка та отримання електронної пошти – протоколи SMTP, IMAP та POP, які використовуються для електронної пошти, працюють на основі TCP, забезпечуючи надійну доставку повідомлень.
- Віддалене адміністрування – протоколи SSH та Telnet, які використовуються для віддаленого доступу до серверів, також використовують TCP для забезпечення надійного з'єднання.

Слід зазначити, що використання TCP через VPN може призвести до деякого збільшення затримки через додаткові заголовки та механізми контролю надійності як на рівні VPN, так і на рівні самого протоколу TCP. Однак для завдань, де цілісність даних є критично важливою, надійність TCP є більш пріоритетною, ніж максимально можлива швидкість.

Основні типи прихначення UDP протоколу для особистих цілей:

- Онлайн-ігри – UDP забезпечує швидку передачу інформації про дії гравців, що є критично важливим для ігрового процесу в реальному часі. Незначна втрата пакетів може бути менш помітною, ніж затримка, спричинена повторною передачею в TCP.
- Потокове відео – UDP використовується для передачі відео- та аудіоданих у реальному часі. Хоча деякі пакети можуть бути втрачені, що може призвести до незначних артефактів, загальний досвід потокового перегляду часто є більш плавним завдяки нижчій затримці.
- Голосовий зв'язок (VoIP) – протокол є кращим вибором для голосових дзвінків через Інтернет, оскільки він забезпечує швидку передачу голосових пакетів, мінімізуючи затримку та забезпечуючи більш природну розмову.
- Перегляд потокових трансляцій (Live Broadcasting) – забезпечує швидку доставку даних у реальному часі, що є важливим для прямих трансляцій спортивних подій, новин або онлайн-концертів.

Що до самого серверу, було використано Cloud Server від компанії DigitalOcean. Поєднання надійної безпеки та гнучкості OpenVPN зі зручною платформою та економічно вигідною інфраструктурою Digital Ocean створює лаконічне поєднання підтримки інфраструктури серверу і захисту для користувачів з високим ступенем контролю та можливостей налаштування:

Розгортання власного VPN-сервера стає надзвичайно простим завдяки доступності 1-Click App у Digital Ocean Marketplace, що дозволяє користувачам миттєво налаштувати повністю функціональне середовище OpenVPN без необхідності складних ручних конфігурацій. OpenVPN вирізняється своєю гнучкістю, підтримуючи різноманітні мережеві топології, включаючи безпечний віддалений доступ до окремих пристроїв, надійні з'єднання "сайт-сайт" між різними мережами, а також створення масштабованих топологій "зірка" для

об'єднання численних віддалених локацій з центральною мережею. Протокол OpenVPN славиться своїм високим рівнем безпеки, використовуючи перевірені часом та надійні алгоритми шифрування, такі як AES-256, та ефективні методи аутентифікації, що гарантує конфіденційність та цілісність переданих даних.

Інфраструктура Digital Ocean забезпечує стабільну та продуктивну основу для роботи VPN-сервера, пропонуючи широку мережу центрів обробки даних по всьому світу, що сприяє високій доступності сервісу та потенційному зниженню затримки в залежності від обраного географічного розташування. Економічна ефективність є ще однією важливою перевагою, оскільки Digital Ocean пропонує різноманітні тарифні плани для своїх Droplets, включаючи бюджетні варіанти, що робить розміщення персонального або невеликого VPN-сервера фінансово доступним, при цьому забезпечуючи прозоре ціноутворення та можливість масштабування ресурсів відповідно до потреб.

Запуск власного VPN-сервера на платформі Digital Ocean надає користувачам повний контроль над їхніми даними та журналами активності, забезпечуючи високий рівень приватності, оскільки виключається доступ будь-яких сторонніх VPN-провайдерів до мережевого трафіку. Крім того, функція приватних мереж Digital Ocean може бути ефективно використана в поєднанні з OpenVPN для створення захищених каналів зв'язку між різними Droplets, розташованими в одному центрі обробки даних, без необхідності передачі трафіку через публічний Інтернет, що значно підвищує рівень безпеки для багаторівневих застосунків. Нарешті, кросплатформна сумісність клієнтів OpenVPN охоплює широкий спектр операційних систем та пристроїв, включаючи настільні комп'ютери, ноутбуки, смартфони та планшети, забезпечуючи можливість підключення практично для будь-якого користувача незалежно від використовуваної платформи.

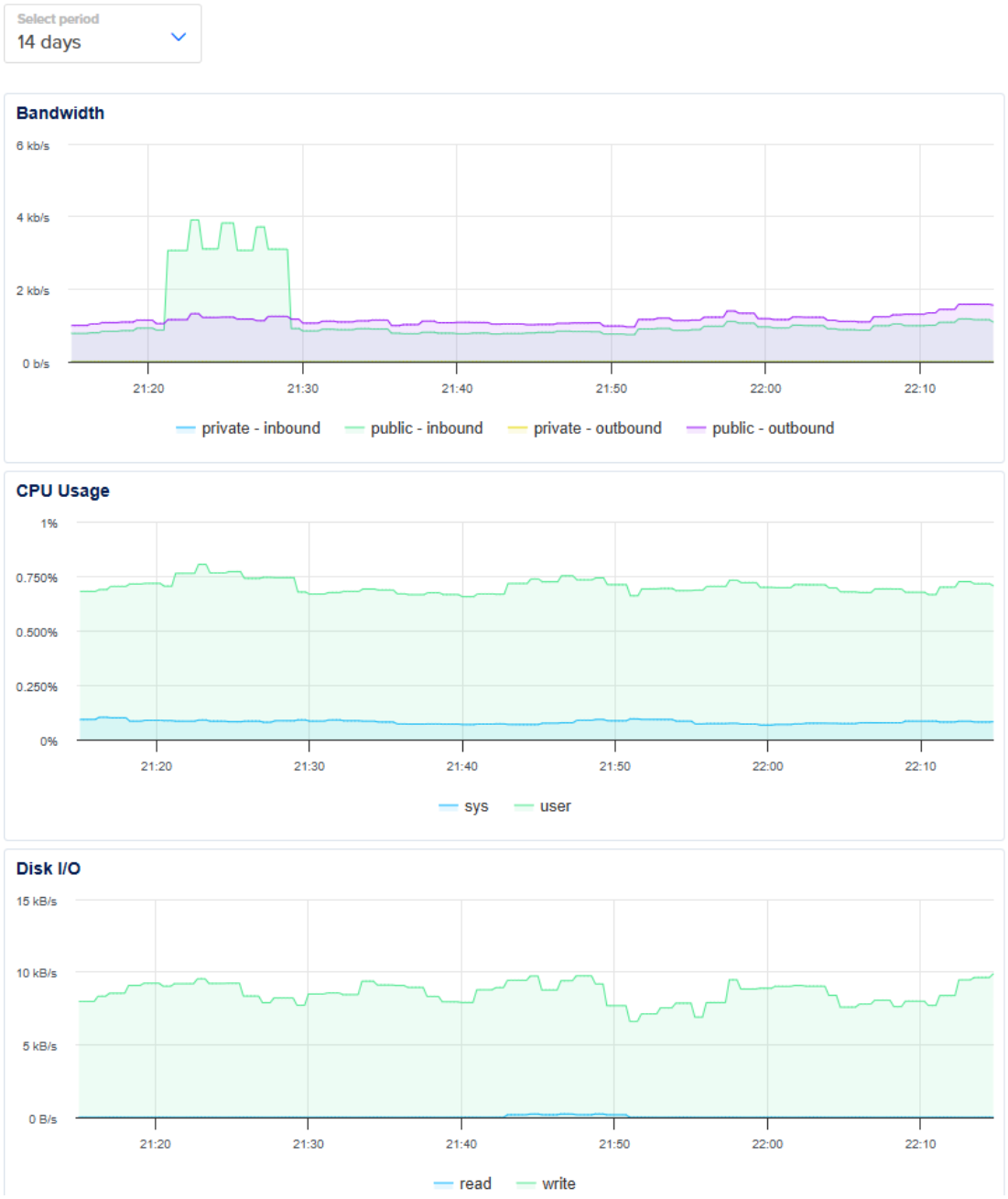


Рис. 2.4 – Графік використання серверу DigitalOcean

2.4 Цільовий користувач

Оскільки в програму інтегрований штучний інтелект, який аналізує трафік і чатбот за для допомоги у разі потреби, то застосунком може користуватись будь-хто почнаючи від дитини, якій потрібно подивитись відео улюбленого блогера з іншої країни і до висококваліфікованих розробників. Зазвичай цільовою аудиторією для VPN є технічно обізнані користувачі, які прагнуть мати більший контроль над своїм VPN-з'єднанням та

даними. Це можуть бути особи, які цінують конфіденційність та безпеку в інтернеті та хочуть мінімізувати ризики, пов'язані з використанням сторонніх VPN-сервісів. Користувачі, які потребують обходу географічних обмежень для доступу до певного контенту, також входять до цієї аудиторії. Зазвичай сервісом користуються розробники або IT-фахівці, які використовують VPN для тестування або безпечного доступу до віддалених ресурсів, а також студенти або дослідники, яким може знадобитися доступ до академічних ресурсів з географічними обмеженнями. Статистичні дані свідчать, що часто це молоді чоловіки з вищою освітою, які є ранніми адептами технологій.

Можливі сценарії використання VPN-застосунку:

- Захист конфіденційності в публічних мережах Wi-Fi: Користувачі можуть використовувати VPN для шифрування свого інтернет-трафіку при підключенні до публічних мереж Wi-Fi в кафе, аеропортах або готелях, захищаючи свої дані від потенційних перехоплень.
- Обхід географічних обмежень: VPN дозволяє користувачам отримати доступ до потокових сервісів, спортивних трансляцій або новинних веб-сайтів, які можуть бути заблоковані в їхньому регіоні, шляхом підключення до сервера в іншій країні.
- Забезпечення безпечного доступу до контенту: Користувачі можуть використовувати VPN для безпечного доступу до корпоративних ресурсів при віддаленій роботі, хоча цей звіт орієнтований на особисте використання.
- Анонімне завантаження файлів: VPN може забезпечити анонімність при завантаженні файлів через торренти та обміні файлами за технологією P2P.
- Обхід інтернет-цензури: У країнах з обмеженим доступом до Інтернету VPN може бути використаний для обходу цензури та доступу до заблокованих веб-сайтів.
- Покращення конфіденційності при пошуку в Інтернеті: VPN може запобігти відстеженню з боку рекламодавців та покращити конфіденційність при пошуку в Інтернеті.

Відкритий вихідний код застосунку має значний позитивний вплив на користувача. Цінувачі безпеки та надійності отримають можливість самостійно впевнитись у відсутності шкідливих елементів або прихованих бекдорів, що значно підвищує довіру. Це також

дозволить експертам безпеки перевіряти код на наявність вразливостей, а технічно підкованим юзерам модифікувати його під себе або інтегрувати у свої системи за потреби.

3 РОЗРОБКА І ОГЛЯД ЗАСТОСУНКУ

3.1 Сервіси та утиліти

Для розробки клієнтської частини застосунку було обрано мову програмування C# у поєднанні з фреймворком Windows Forms. Вибір C# зумовлений його потужними можливостями в розробці застосунків під операційну систему Windows, високою продуктивністю та розвиненою екосистемою. Windows Forms, у свою чергу, надає інструменти для швидкого створення графічного інтерфейсу користувача, що є оптимальним рішенням для десктопних застосунків, орієнтованих на зручність та інтеграцію з операційною системою.

В якості серверної інфраструктури було використано віртуальні сервери (droplets), орендовані у DigitalOcean. DigitalOcean вирізняється своєю надійністю, масштабованістю та зручним інтерфейсом для керування серверами. Орендовані droplets були індивідуально налаштовані для забезпечення оптимальної продуктивності та безпеки. На серверах було встановлено операційну систему Ubuntu, яка є стабільним, безпечним та широко підтримуваним дистрибутивом Linux, що робить її привабливим вибором для серверних застосунків.

Для забезпечення безпечного та стабільного з'єднання між клієнтською частиною застосунку та серверами було розгорнуто OpenVPN. OpenVPN є надійним рішенням для створення віртуальних приватних мереж (VPN), що дозволяє шифрувати трафік та забезпечувати конфіденційність переданих даних. Це рішення було обрано для гарантування захищеного обміну інформацією між застосунком та сервером, мінімізуючи ризики несанкціонованого доступу.

Функціональність штучного інтелекту в застосунку реалізовано шляхом інтеграції з OpenAI API. Використання OpenAI API надає доступ до передових моделей обробки природної мови, що дозволяє реалізувати функцію чат-бота. Застосунок може надсилати запити до API та отримувати інтелектуальні відповіді, що розширює можливості взаємодії з

користувачем та надання інформаційної підтримки безпосередньо в інтерфейсі застосунку. Вибір OpenAI API обумовлений високою якістю та різноманітністю пропонованих моделей, а також зручністю інтеграції через програмний інтерфейс.

3.2 Огляд програми

Головне меню застосунку, розташоване у лівій частині інтерфейсу, надає користувачеві доступ до основних функціональних блоків. У верхній частині відображається індикатор, що візуалізує обсяг трафіку. Нижче розміщена інтерактивна кнопка для керування з'єднанням. Основна навігація здійснюється через вертикально орієнтоване меню, що включає розділи "Головна", "Налаштування" та "Довідка.

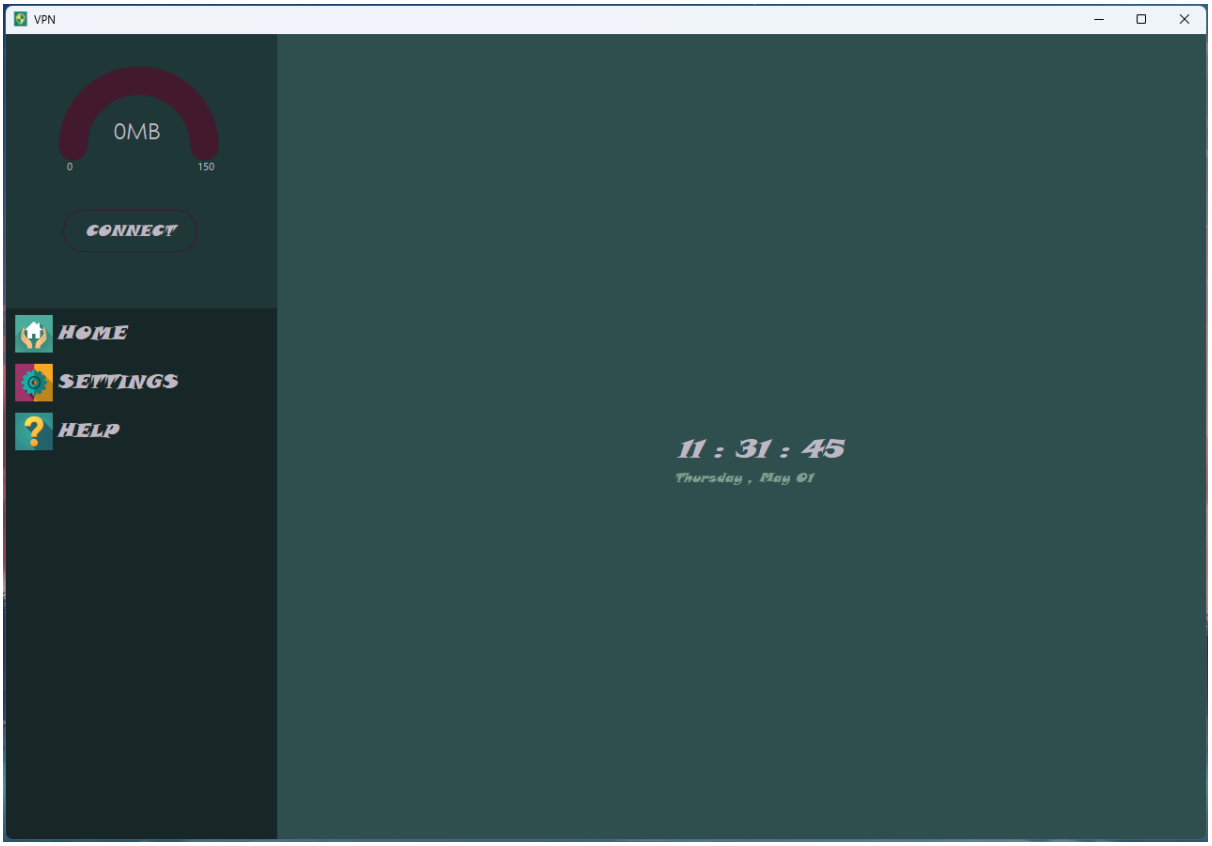


Рис. 3.1 – Головна сторінка застосунку

Після ініціації з'єднання за допомогою відповідної кнопки у лівій частині головного меню, користувачеві надається можливість вибору серверу, що визначається географічним розташуванням, та протоколу з'єднання. Перелік доступних країн-серверів відображається у правій частині вікна застосунку. Нижче розташований блок для вибору бажаного протоколу передачі даних.

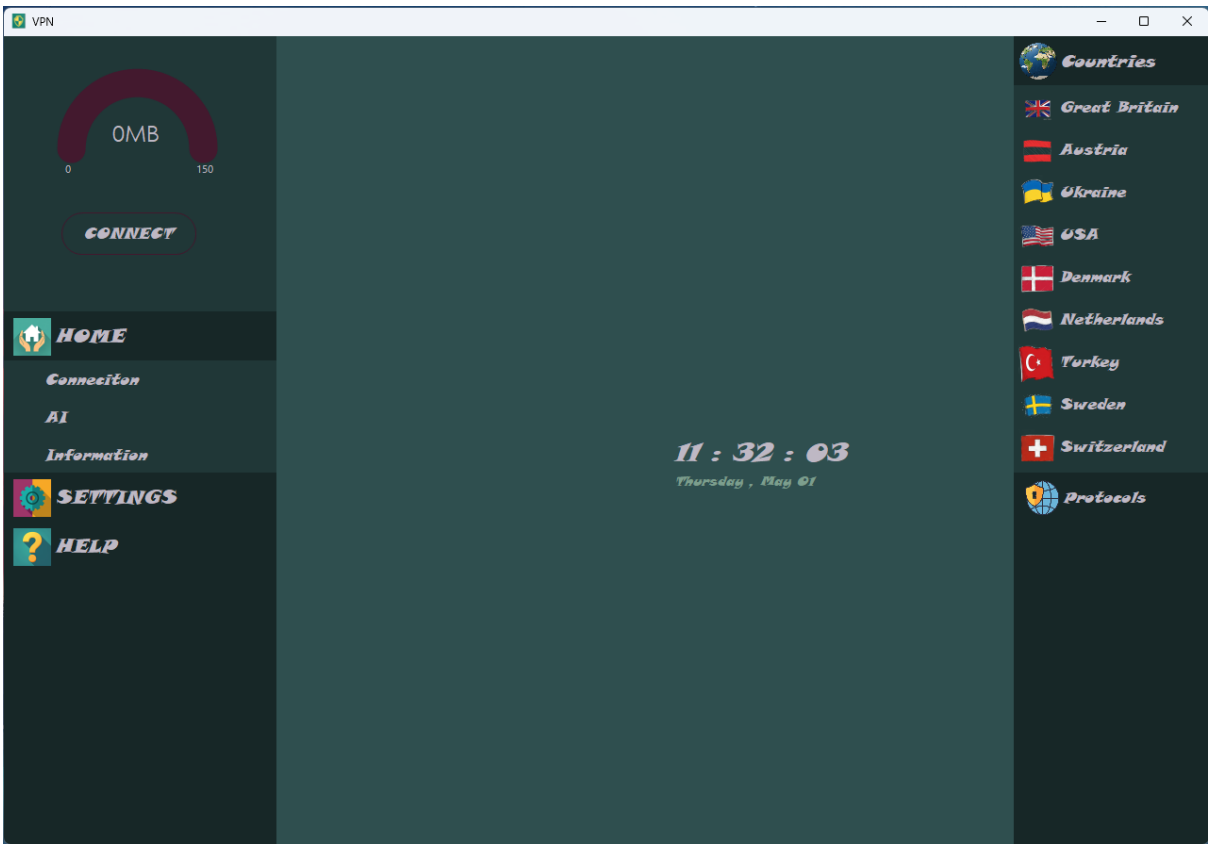


Рис. 3.2 – Країни серверів для підключення

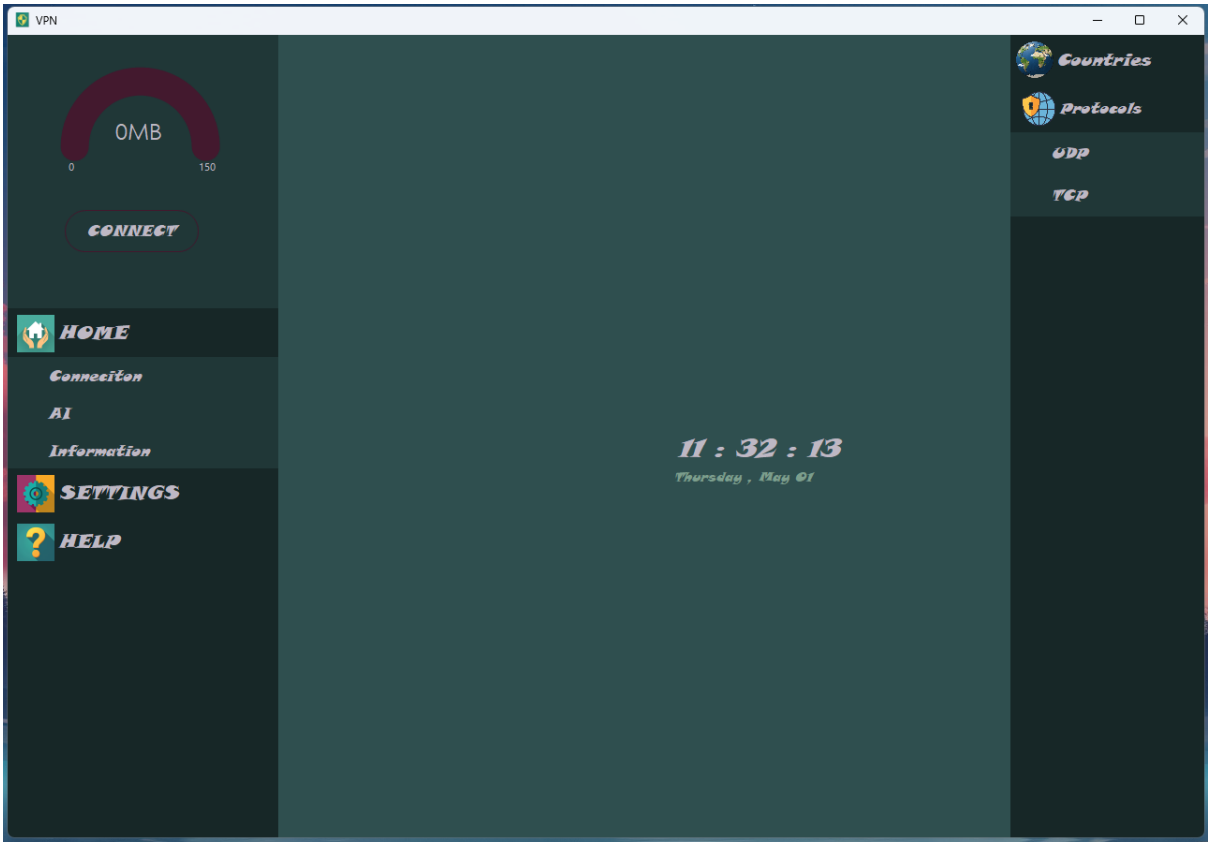


Рис. 3.3 – Протоколи серверів для підключення

Надана демонстрація на Рис. 3.4 ілюструє функціонування застосунку, зокрема процес встановлення VPN-з'єднання. Згідно з відображеною інформацією, було здійснено підключення до серверу, розташованого у Великій Британії. Факт успішної зміни IP-адреси та віртуального географічного розташування підтверджується даними, отриманими з вебсайту whatismyipaddress.com.

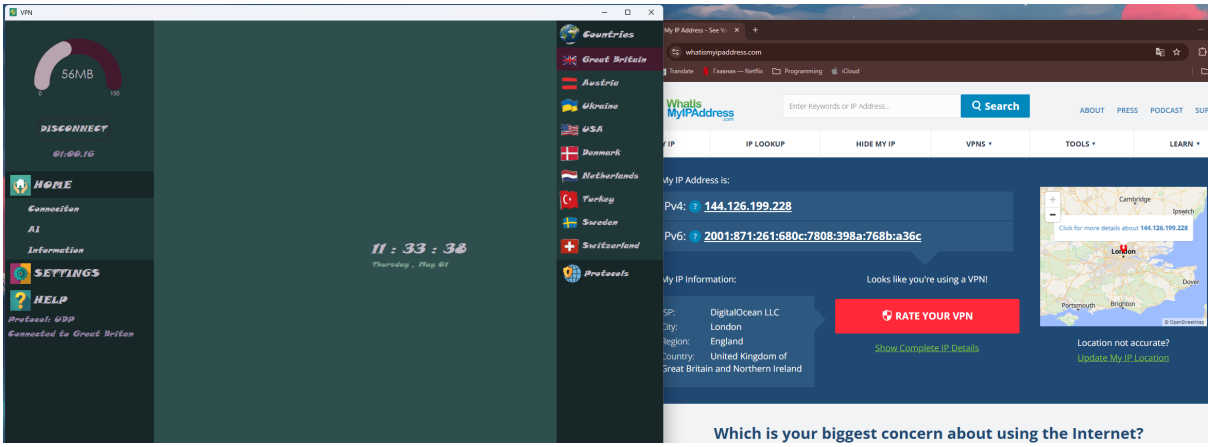


Рис. 3.4 – Демонстрація роботи застосунку

Додано функціональну можливість керування комбінаціями клавіш, що сприяє оптимізації та підвищенню зручності керування застосунком для користувача.

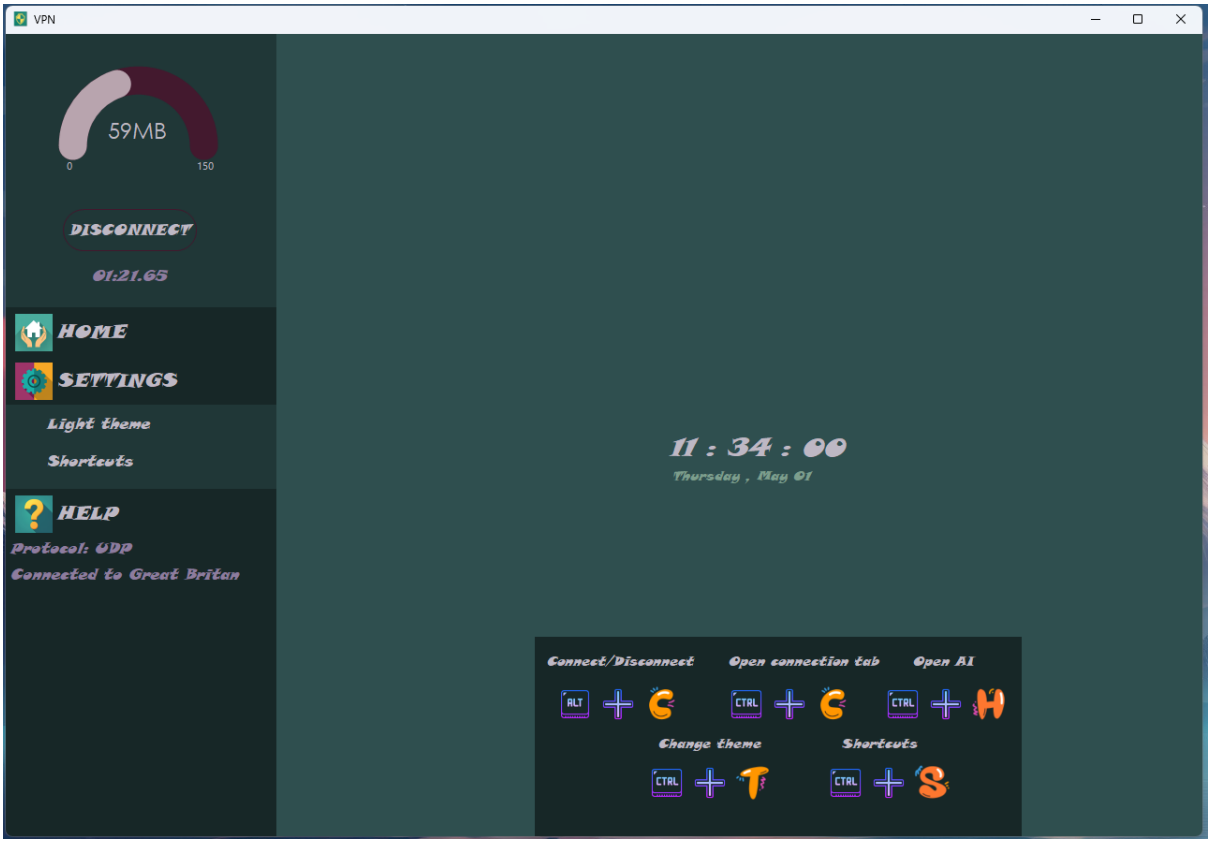


Рис. 3.5 – Комбінації клавіш

Розділ "Help" надає користувачеві можливість звернутися за підтримкою до розробника, а також ознайомитися з основною інформацією щодо застосунку.

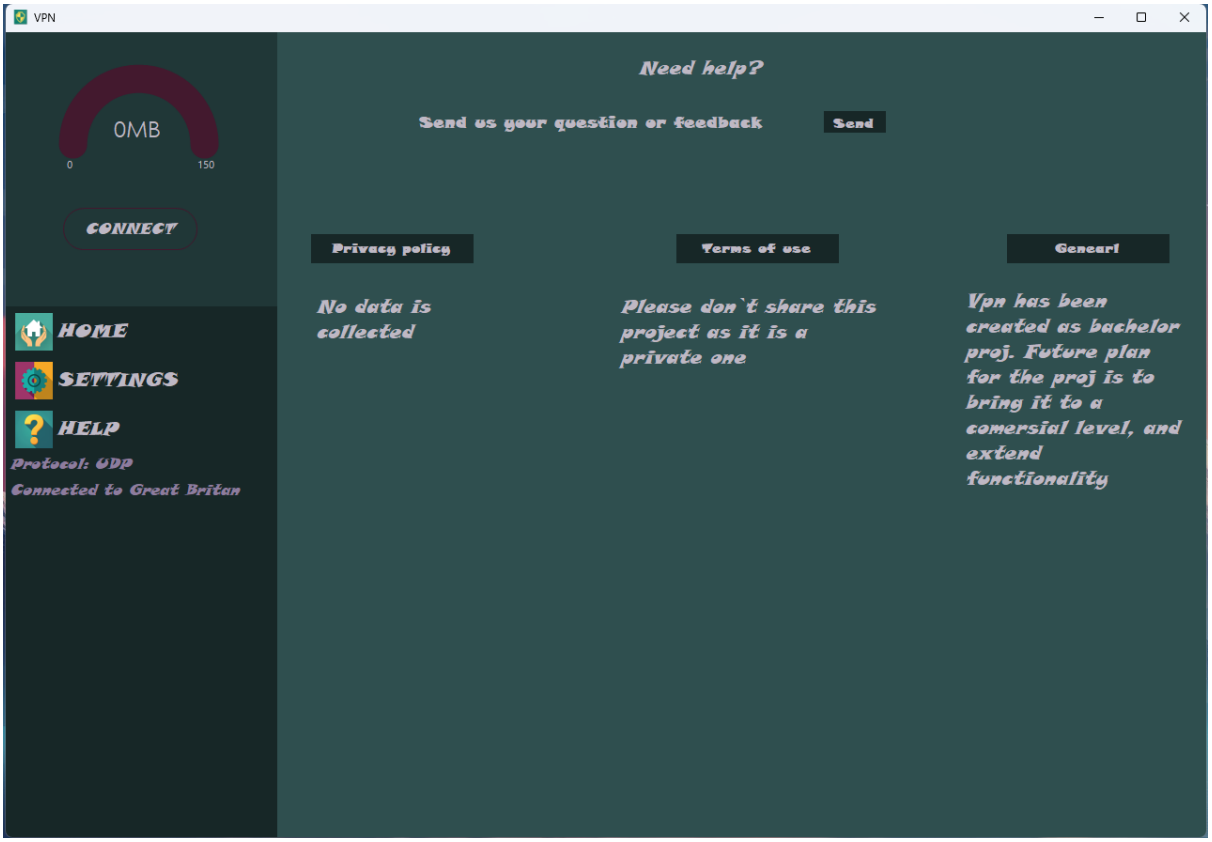


Рис. 3.6 – Розділ “Help”

Розділ "AI" надає користувачеві функціональність взаємодії з чат-ботом шляхом надсилання запитів. Крім того, у даному розділі передбачено дві інтерактивні опції: "Connection Analysis" та "Load Analysis". При активації функції "Connection Analysis" у лівій нижній частині інтерфейсу відображається графік, що візуалізує середню швидкість підключення до серверів з використанням різних протоколів. Функція "Load Analysis", у свою чергу, забезпечує отримання та відображення інформації щодо поточного навантаження оперативної пам'яті та центрального процесора системи.

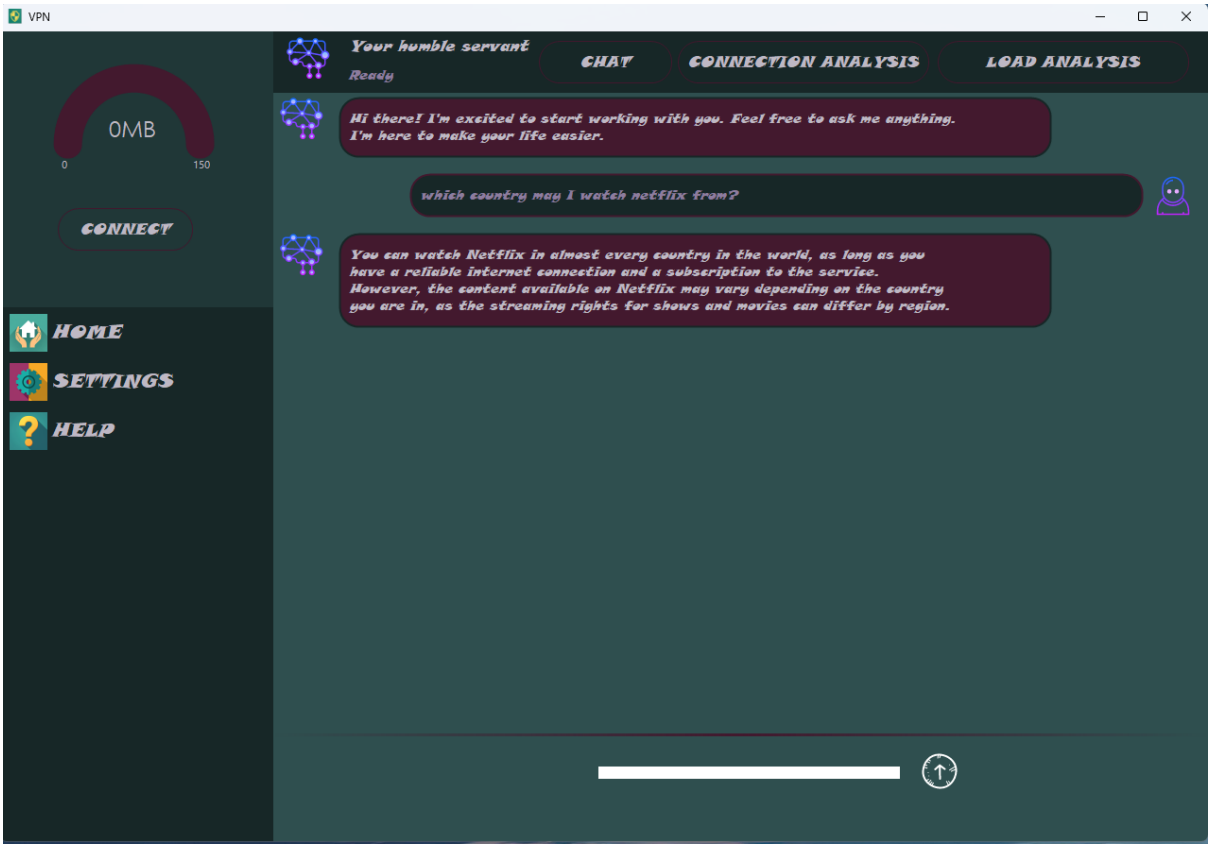


Рис. 3.7 – Робота штучного інтелекту

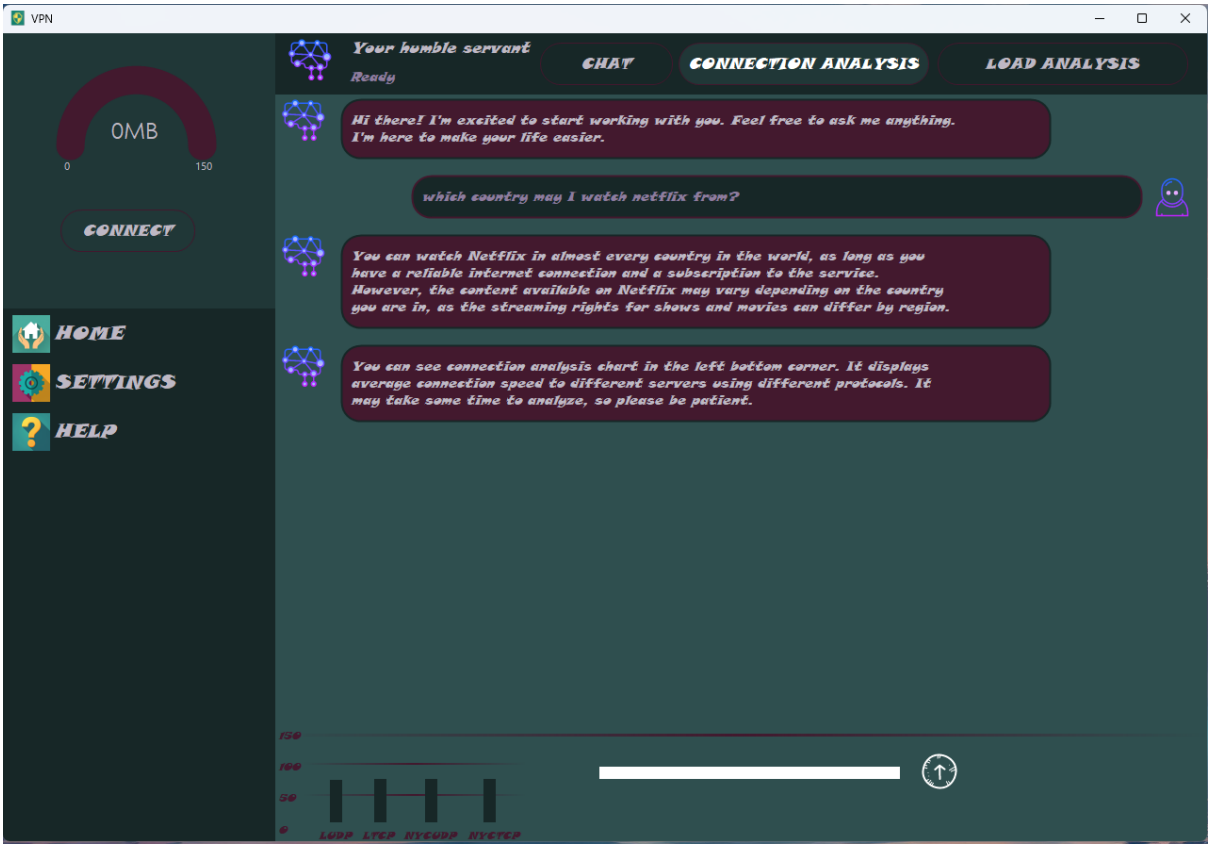


Рис. 3.7 – Аналіз підключення

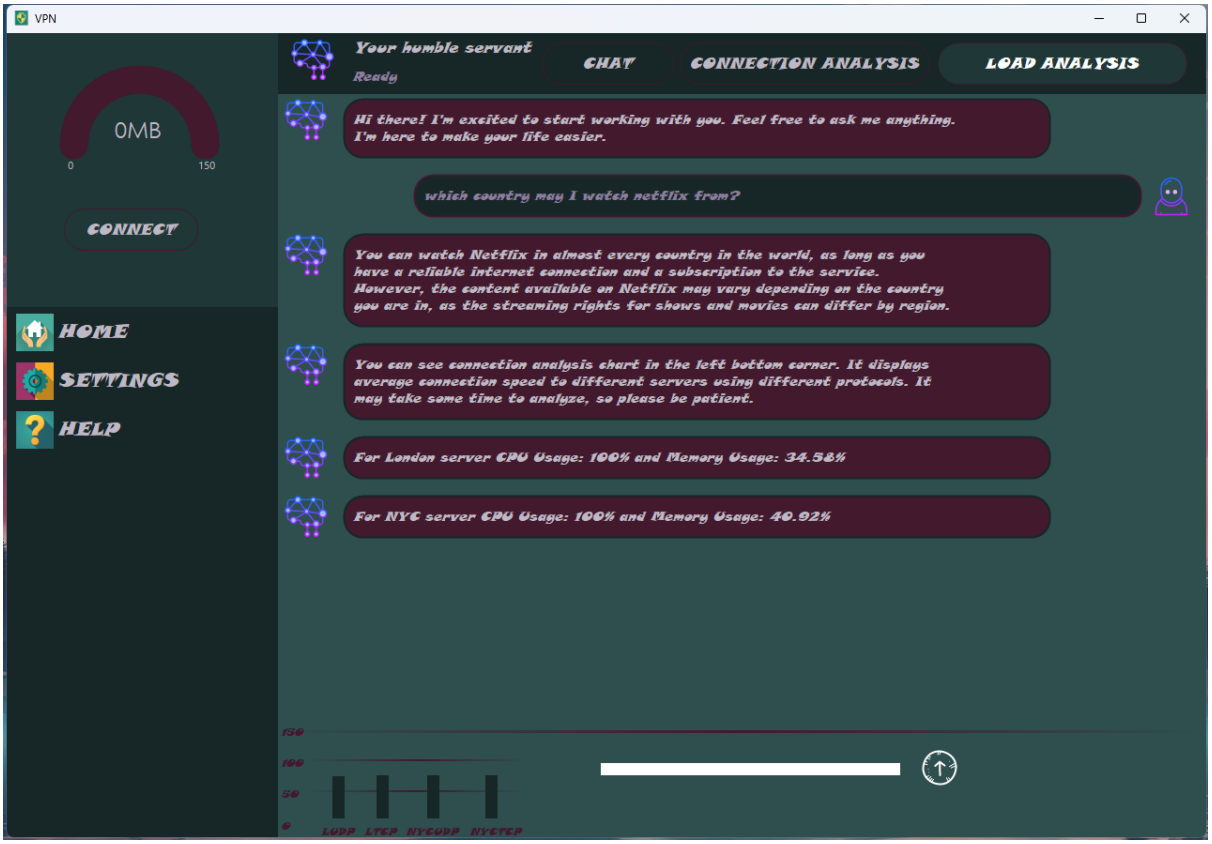


Рис. 3.8 – Аналіз навантаження

ВИСНОВКИ

У процесі виконання дослідження було здійснено ґрунтовний аналіз існуючих типів VPN-підключень, а саме: Site-to-Site VPN, Remote Access VPN, Cloud VPN, SSL VPN та Double VPN. Детально розглянуто їхні функціональні особливості, переваги, недоліки та специфічні сценарії застосування. Це дало змогу сформувати чітке розуміння сильних і слабких сторін кожного типу VPN, що стало основою для обґрунтованого вибору оптимального рішення для подальшої розробки.

Зокрема, Cloud VPN було визначено як найбільш перспективний тип для реалізації поставлених завдань, зважаючи на його високу масштабованість, гнучкість, швидкість розгортання та ефективність використання хмарних ресурсів.

Крім того, було проведено ретельний аналіз апаратних вимог до хмарного VPN-серверу. Це включало в себе дослідження необхідних обчислювальних потужностей центрального процесора, обсягу оперативної пам'яті та дискового простору для забезпечення належної продуктивності та стабільності серверної інфраструктури.

На основі отриманих даних було здійснено обґрунтований вибір апаратного забезпечення для серверної частини розробленого VPN-сервісу. При цьому враховувалися як мінімальні вимоги для функціонування системи, так і прогнозовані рівні навантаження, що дозволило оптимізувати витрати та забезпечити необхідну продуктивність.

Ключовим результатом даної роботи є розробка функціонального VPN-сервісу з інтегрованою системою штучного інтелекту. Зазначена система здатна здійснювати аналіз параметрів підключення в режимі реального часу, надавати користувачам рекомендації щодо вибору оптимальних серверів та протоколів, а також забезпечувати підтримку у вирішенні можливих проблем.

Актуальність даної роботи важко переоцінити у сучасному цифровому світі, де інформаційна безпека стає критично важливою. Зростання кількості кіберзагроз, потреба в захисті конфіденційних даних та забезпечення безпечного доступу до інформації з будь-якої точки світу роблять VPN-технології незамінним інструментом.

Вклад даної роботи у сучасний світ полягає у розробці інтелектуальної VPN-системи, яка не лише забезпечує безпечне з'єднання, але й активно допомагає користувачеві у його налаштуванні та використанні. Інтеграція штучного інтелекту дозволяє автоматизувати процеси аналізу та оптимізації з'єднання, що значно підвищує зручність використання та ефективність VPN-сервісу.

Проведене дослідження підтвердило високу актуальність та значний практичний потенціал обраної теми. Розроблені в рамках роботи рішення можуть бути використані для модернізації існуючих VPN-сервісів, підвищення рівня їхньої безпеки та зручності використання, а також для створення принципово нових програмних продуктів у даній сфері.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Computer Networking: A Top-Down Approach (Kurose & Ross)
2. VPNs and Tunneling Technologies (Gray)
3. The Role of Artificial Intelligence in Cybersecurity. URL: https://www.cisco.com/c/en/us/products/security/state-of-ai-security.html?utm_medium=search-paid&utm_source=g+google&utm_campaign=AID_EMEA_EU_EN_GS_Nonbrand_Network_Security_T1&utm_content=state-of-ai-securityc&_bt=747798652264&_bk=ai%20information%20security&_bm=e&_bn=g&_bg=177750258683&gad_source=1&gad_campaignid=22443417303&gbraid=0AAAAA_G3KuDmxX2_gr9xY298aUw6YNvEp&gclid=Cj0KCQjw5ubABhDIARIsAHMighY0OgoLkjDdNEVC-S-sK4vY75lbEGvwq0zrL_YeoWNTS3mi0h3XMJYaAi13EALw_wcB
4. What is VPN. URL: https://www.avast.com/c-what-is-a-vpn
5. Types of VPNs and protocols. URL: https://nordlayer.com/learn/vpn/types-and-protocols/
6. AI-Powered Network Security. URL: https://www.google.com/search?q=https://nilesecure.com/ai-networking/ai-network-security%23:~:text%3DAI%252Dpowered%2520network%2520security%2520systems,actions%2520to%2520neutralize%2520the%2520threat.
7. Cloud network security. URL: https://aviatrix.com/learn-center/cloud-network-security/site-to-cloud-vpn/
8. Підвищення якості надання композитних сервісів у мережах із сервісно-орієнтованою архітектурою. URL: https://lpnu.ua/sites/default/files/2020/dissertation/1552/disshpurprint.pdf
9. Cloud VPN. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-a-cloud-vpn
10. Impact of cloud infrastructure on VPN performance. URL: https://www.diva-portal.org/smash/get/diva2:1867383/FULLTEXT01.pdf
11. Огляд VPN протоколів. URL: https://wiki.securepoint.de/UTM/VPN/%C3%9Cbersicht
12. Типи впн. URL: https://www.paloaltonetworks.com/cyberpedia/types-of-vpn

13. Digitalocean droplets. URL: https://cyberpanel.net/blog/digitalocean-droplets
14. Open VPN system requirements. URL: https://openvpn.net/as-docs/system-requirements.html#cpu-requirements
15. Ubuntu. URL: https://de.wikipedia.org/wiki/Ubuntu_(Betriebssystem)
16. Ubuntu Server Operating System: Setup and Benefits. URL: https://contabo.com/blog/ubuntu-server-operating-system-setup-and-benefits/
17. Installation of Open VPN on ubuntu. URL: https://documentation.ubuntu.com/server/how-to/security/install-openvpn/index.html
18. Selfhosted server. URL: https://cybernews.com/what-is-vpn/how-to-make-your-own-vpn-server/
19. VPN protocols. URL: https://surfshark.com/blog/vpn-protocols
20. Open VPN vulnerabilities. URL: https://cyberpress.org/attackers-to-execute-arbitrary-code/
21. Cloud VPN. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-a-cloud-vpn
22. Benefits of cloud VPN. URL: https://www.goodaccess.com/blog/what-is-cloud-vpn
23. Cloud based access. URL: https://blog.repairdesk.co/2023/04/13/cloud-based-access-vs-vpn-the-better-solution-for-your-business/
24. Disadvantages of VPN. URL: https://www.theknowledgeacademy.com/blog/disadvantages-of-vpn/
25. Performance testing. URL: https://community.openvpn.net/openvpn/wiki/PerformanceTestingOpenVPN
26. C# network library. URL: https://github.com/Toemsel/Network
27. Windows forms guide. URL: https://learn.microsoft.com/en-us/dotnet/desktop/winforms/overview/?view=netdesktop-9.0
28. OpenAI API. URL: https://openai.com/index/openai-api/
29. Differences between UDP and TCP. URL: https://www.spiceworks.com/tech/networking/articles/tcp-vs-udp/
30. OpenAI usage. URL: https://www.newhorizons.com/resources/blog/the-complete-guide-for-using-the-openai-python-api