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: "Забезпечення конфіденційності даних з використанням OpenVPN в контейнеризованому середовищі"

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)

Букатка С. Р.
підпис (прізвище та ініціали)

Керівник Загородна Н. В.
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 Букатці Соломії Романівні
(прізвище, ім'я, по батькові)

1. Тема роботи Забезпечення конфіденційності даних за допомогою OpenVPN в контейнеризованому середовищі

Керівник роботи Загородна Наталія Володимирівна, к.т.н., доцент, завідувач 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 17.06.2023

3. Вихідні дані до роботи Вимоги до забезпечення конфіденційності в мережевій безпеці (інформаційно-комунікаційних системах)

4. Зміст роботи (перелік питань, які потрібно розробити)
Проаналізувати загрози безпеки даних.
Визначити методи протидії загрозам безпеки даних.
Дослідити особливості роботи OpenVPN та контейнеризації.
Дослідити особливості інтеграції OpenVPN та контейнеризації.
Здійснити практичну реалізацію та тестування впровадженої системи захисту даних.
Безпека життєдіяльності, основи охорони праці.
Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Тема. Мета роботи. Основні завдання безпеки. Найпоширеніші загрози безпеки даних. Найпоширеніші методи протидії загрозам безпеки даних. Аналіз OpenVPN. Аналіз контейнеризації. Інтеграція OpenVPN та контейнеризації. Порівняння Docker-образів. Етапи практичної реалізації. Тестування роботи для різних ОС. Перевірка шифрування даних. Перевірка швидкості зв'язку. Перевірка стабільності роботи. Переваги та недоліки інтеграції. 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 – 02.02	Виконано
2.	Підбір джерел для аналізу основних аспектів конфіденційності даних	02.01 – 05.02	Виконано
3.	Теоретичний аналіз літератури та наукових статей з питань інформаційної безпеки та контейнеризації	07.02 – 18.02	Виконано
4.	Проведення аналізу методів протидії загрозам безпеки даних	20.02 – 29.02	Виконано
5.	Вивчення особливостей роботи OpenVPN та технологій контейнеризації	01.03 – 10.03	Виконано
6.	Реалізація та налаштування OpenVPN сервера у контейнері Docker	12.03 – 25.03	Виконано
7.	Проведення тестування ефективності та безпеки впровадженого рішення	28.03 – 07.04	Виконано
8.	Оформлення розділу «Основні аспекти конфіденційності даних»	08.04 – 15.04	Виконано
9.	Оформлення розділу «Теоретичні аспекти використання OpenVPN та контейнеризації»	18.04 – 25.04	Виконано
10.	Оформлення розділу «Практична реалізація захисту даних за допомогою OpenVPN в контенері»	26.04 – 01.05	Виконано
11.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	02.05 – 15.05	Виконано
12.	Оформлення кваліфікаційної роботи	15.05 – 27.05	Виконано
13.	Нормоконтроль	03.06 – 05.06	Виконано
14.	Перевірка на плагіат	06.06 – 07.06	Виконано
15.	Попередній захист кваліфікаційної роботи	18.06.2024	Виконано
16.	Захист кваліфікаційної роботи	27.06.2024	

Студент _____ Букатка С. Р.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Загородна Н. В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Забезпечення конфіденційності даних з використанням OpenVPN в контейнеризованому середовищі // Кваліфікаційна робота ОР «Бакалавр» // Букатка Соломія Романівна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-42 // Тернопіль, 2024 // С. 56, рис. – 10, табл. – 7 , кресл. – -, додат. – -.

КЛЮЧОВІ СЛОВА: VPN, OpenVPN, контейнеризоване середовище, конфіденційність, інформація, сервер.

Кваліфікаційна робота присвячена дослідженню аспектів забезпечення конфіденційності даних у сучасних інформаційних системах. У роботі розглянуті основні аспекти конфіденційності даних, включаючи поняття та роль конфіденційності в інформаційних системах, аналіз загроз безпеці даних та методи їх протидії. Також розглянуто теоретичні аспекти та запропоновано використання OpenVPN для забезпечення мережевої безпеки та контейнеризації для ізоляції даних.

Особлива увага приділяється практичній реалізації захисту даних з використанням OpenVPN у контейнеризованому середовищі. Робота включає огляд процесу встановлення та налаштування OpenVPN сервера у Docker, а також інструкції щодо встановлення клієнтського програмного забезпечення та тестування роботи сервера. Окремий розділ присвячено безпеці життєдіяльності та основам охорони праці для працівників, що працюють з інформаційними технологіями.

Отримані результати можуть бути використані для подальших досліджень і розробок у сфері кібербезпеки, а також для впровадження в корпоративних мережах для захисту конфіденційних даних.

ABSTRACT

Ensuring Data Confidentiality Using OpenVPN in a Containerized Environment // Thesis of educational level "Bachelor"// Bukatka Solomia Romanivna // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБс-42 // Ternopil, 2024 // P. 56 fig. - 10, tab. – 7, chair. – -, added. – -.

KEYWORDS: VPN, OpenVPN, containerized environment, confidentiality, information, server.

The qualification paper is devoted to the study of aspects of data privacy in modern information systems. The paper considers the main aspects of data privacy, including the concept and role of privacy in information systems, analysis of data security threats and methods of counteracting them. The theoretical aspects of using OpenVPN to ensure network security and containerization for data isolation are also considered.

Particular attention is paid to the practical implementation of data protection using OpenVPN in a containerized environment. The paper includes an overview of the process of installing and configuring an OpenVPN server in Docker, as well as instructions for installing client software and testing the server. A separate section is devoted to life safety and the basics of labor protection for employees working with information technology.

The results obtained can be used for further research and development in the field of cybersecurity, as well as for implementation in corporate networks to protect confidential data.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

VPN	—	Virtual Private Network
GDPR	—	General Data Protection Regulation
ПЗ	—	Програмне забезпечення
TCP	—	Transmission Control Protocol
UDP	—	User Datagram Protocol
IP	—	Internet Protocol
PKI	—	Public Key Infrastructure
CA	—	Certificate Authority

ВСТУП

Сьогодні важко уявити повсякденне життя без мобільних пристроїв та Інтернету, проблеми забезпечення безпеки в мережі стали надзвичайно актуальними. Завдяки неймовірному зростанню обсягу цифрових даних та транзакцій, з'явилася необхідність вдосконалення технологій та інфраструктури для захисту особистої інформації, корпоративних даних і конфіденційних комунікацій. З огляду на це, особлива увага приділяється розробці ефективних засобів, спрямованих на забезпечення конфіденційності даних під час їх передачі та зберігання. У цьому контексті віртуальні приватні мережі (VPN) виявилися потужним інструментом для забезпечення кібербезпеки та конфіденційності в мережі.

Віртуальні приватні мережі є важливою складовою сучасних операційних систем і мережевої безпеки. VPN дозволяють користувачам створювати безпечне з'єднання з мережами чи інтернет-ресурсами через публічну мережу, таку як Інтернет. Головною метою VPN є шифрування даних під час їхньої передачі, щоб забезпечити конфіденційність та безпеку інформації.

Окрім того, із розвитком технологій з'являється все більше вимог до гнучкості та масштабованості програмних рішень. Контейнеризація, дає можливість покращувати безпеку інформаційно-комунікаційної системи завдяки можливості ізолювати додатки та їх залежності. Контейнери забезпечують високу портативність та ефективне використання ресурсів, що робить їх ідеальним рішенням для розгортання та масштабування сучасних додатків.

Мета роботи полягає в дослідженні та практичній реалізації методів застосування OpenVPN для забезпечення конфіденційності в контейнеризованому середовищі.

Основні завдання включають в себе:

– аналіз сучасних викликів у галузі забезпечення конфіденційності даних;

– огляд особливостей OpenVPN та контейнеризації: огляд OpenVPN, огляд контейнеризованого середовища, вибір найкращого Docker-образу;

– практичну реалізацію: розгортання OpenVPN сервера в контейнеризованому середовищі, налаштування Docker-образу та методу шифрування для OpenVPN, тестування роботи OpenVPN сервера в контейнері для виявлення та усунення можливих вразливостей.

Актуальність теми дослідження обумовлена необхідністю удосконалення методів захисту в умовах швидкого розвитку технологій та поширення віртуалізації та контейнеризації. Застосування OpenVPN у поєднанні з контейнеризацією визначає новий рівень безпеки для передачі даних та обробки інформації.

Сучасні розробки в галузі кібербезпеки свідчать про постійний пошук нових шляхів захисту конфіденційності даних. Використання технологій контейнеризації разом з OpenVPN визначається як перспективний напрямок, що дозволяє забезпечити ефективний та надійний захист інформації.

1 ОСНОВНІ АСПЕКТИ КОНФІДЕНЦІЙНОСТІ ДАНИХ

Модель CIA є основною концепцією в інформаційній безпеці, яка визначає три найважливіші аспекти захисту інформації:

– Confidentiality (конфіденційність). Забезпечення того, щоб інформація була доступна тільки тим особам, які мають на це дозвіл. Конфіденційність передбачає захист даних від несанкціонованого доступу, щоб зберегти приватність та запобігти витоку інформації.

– Integrity (цілісність). Забезпечення того, щоб дані залишалися точними та не були змінені або знищені несанкціонованим чином. Цілісність гарантує, що інформація, яка зберігається або передається, не була змінена або втрачена внаслідок зловмисних дій або технічних збоїв.

– Availability (доступність). Забезпечення того, щоб інформація та ресурси були доступні уповноваженим користувачам у будь-який час, коли вони потрібні. Доступність гарантує, що інформаційні системи працюють належним чином і користувачі можуть отримати доступ до необхідних даних без перерв.

Забезпечення кожного з цих аспектів є критично важливим для ефективного захисту даних і безперебійної роботи інформаційних систем. Конфіденційність відіграє вирішальну роль у захисті від несанкціонованого доступу та збереженні приватності інформації. Тому необхідно детальніше розглянути поняття конфіденційності та її роль в інформаційних системах.

1.1 Поняття конфіденційності та її роль в інформаційних системах

Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом [1].

Такий захист є не лише важливим для військових та урядових організацій, які повинні зберігати свої плани та можливості в таємниці від ворогів. Але він також корисний для компаній та користувачів, які хочуть захистити свої комерційні таємниці або запобігти доступу сторонніх осіб до конфіденційної

інформації (наприклад, юридичної, особистої або медичної інформації). В останні кілька років питанням конфіденційності приділяється все більше уваги, і стало важливо захищати особисту інформацію, що зберігається в автоматизованих системах як у державному, так і в приватному секторах. Конфіденційність повинна бути чітко визначена, а процедури для її захисту повинні бути ретельно впроваджені.

В інформаційній безпеці існує кілька видів конфіденційності, нижче наведено основні їх види.

– Конфіденційність даних – стосується захисту даних, що зберігаються в комп'ютерних системах і мережах, від несанкціонованого доступу, використання, розкриття або модифікації. Це досягається за допомогою різних методів, таких як шифрування та контроль доступу.

– Мережева конфіденційність – стосується захисту інформації, що передається через комп'ютерні мережі, від несанкціонованого доступу, перехоплення або підробки. Це досягається за допомогою шифрування та захищених протоколів, таких як SSL/TLS.

– Наскрізна конфіденційність – стосується захисту інформації, що передається між двома кінцевими точками, наприклад, між клієнтом і сервером, від несанкціонованого доступу або підробки. Це досягається за допомогою шифрування та захищених протоколів.

– Конфіденційність додатків – стосується захисту конфіденційної інформації, що обробляється та зберігається програмними додатками, від несанкціонованого доступу, використання або модифікації. Це досягається за допомогою автентифікації користувача, контролю доступу та шифрування даних, що зберігаються в додатку.

У сфері інформаційної безпеки конфіденційність використовується для захисту даних та інформації від несанкціонованого доступу та розголошення. Конфіденційність ґрунтується на кількох ключових принципах [2]:

– Шифрування. Виступає як ефективний метод захисту конфіденційної інформації від несанкціонованого доступу під час її передачі та зберігання.

Застосування сучасних криптографічних алгоритмів гарантує, що навіть у випадку проникнення зловмисника дані залишаються незрозумілими та невикористовуваними.

– Контроль доступу. Це базовий принцип конфіденційності, який визначає, що лише ті користувачі, які мають відповідні повноваження, можуть отримати доступ до конфіденційної інформації. Це досягається через впровадження системи авторизації та управління правами доступу.

– Маскування даних. Це метод, який використовується для приховування конфіденційної інформації, наприклад, номерів кредитних карток або номерів соціального страхування, щоб запобігти несанкціонованому доступу.

– Віртуальні приватні мережі. VPN дозволяють користувачам безпечно підключатися до мережі через Інтернет і захищають конфіденційність їхніх даних під час передачі.

– Безпечні протоколи передачі файлів (SFTP). SFTP використовуються для безпечної передачі конфіденційних даних через Інтернет, захищаючи їхню конфіденційність під час передачі.

– Двофакторна автентифікація. Двофакторна автентифікація допомагає гарантувати, що тільки авторизовані користувачі мають доступ до конфіденційної інформації, вимагаючи другої форми автентифікації, наприклад, відбитка пальця або одноразового коду.

– Запобігання втраті даних (DLP). Це захід безпеки, який використовується для запобігання витоку або втрати конфіденційних даних. Він відстежує і контролює потік даних, захищаючи їхню конфіденційність.

Роль конфіденційності в інформаційних системах наступна:

– Захист від несанкціонованого доступу. Конфіденційність гарантує, що лише авторизовані користувачі мають доступ до конфіденційної інформації. Це важливо для запобігання несанкціонованому використанню та несанкціонованому використанню даних.

– Захист критичної інформації. В інформаційних системах конфіденційність забезпечує збереження критичної інформації, такої як комерційні та технічні дані, бізнес-плани і дані про клієнтів.

– Відповідність правовим нормам і стандартам безпеки. У багатьох галузях існують обов'язкові вимоги до конфіденційності інформації, як-от галузеві стандарти та європейський GDPR. Забезпечення конфіденційності – важливий аспект дотримання правових норм і стандартів безпеки.

– Безпека торгівельних і комерційних відносин. Конфіденційність відіграє важливу роль у бізнесі під час збереження конкурентних переваг, комерційної таємниці та інших конфіденційних даних, які є частиною корпоративної стратегії.

– Запобігання витоку інформації. Захист конфіденційної інформації від несанкціонованого доступу може допомогти запобігти витоку даних, який може мати серйозні фінансові, репутаційні та юридичні наслідки для організації.

Загалом, конфіденційність інформації в інформаційних системах є критичним аспектом, спрямованим на обмеження доступу до важливих даних та їх збереження від несанкціонованого використання чи розголошення. Забезпечення конфіденційності визначається як ключовий елемент безпеки інформації, гарантуючи дотримання вимог законодавства, захист торговельних та комерційних інтересів, а також запобігаючи витокам даних. Управління конфіденційністю є невід'ємною частиною стратегії інформаційної безпеки, сприяючи надійності та стійкості інформаційних систем.

1.2 Аналіз загроз безпеки даних

Визначення потенційних загроз для безпеки даних є одним із найважливіших кроків у розробці стратегії безпеки даних, яка має слугувати основою для всіх інших дій, пов'язаних із захистом даних. Хоча перелік усіх потенційних загроз для безпеки даних є довгим і складним, не кожна компанія чи користувач може зіткнутися з усіма з них, залежно від типу конфіденційних

даних, що обробляються, і способу їх обробки. Нижче наведено деякі з найпоширеніших загроз безпеки даних, які слід враховувати під час аналізу загроз:

1. Шкідливе програмне забезпечення.

– Короткий опис: зловмисне ПЗ, що включає віруси, трояни, черви, програми-вимагачі та шпигунські програми.

– Потенційні наслідки: втрата даних, порушення роботи систем, викрадення конфіденційної інформації.

– Цільова аудиторія: усі користувачі мережі.

– Методи протидії: використання антивірусного ПЗ, регулярне оновлення ПЗ, встановлення програмного забезпечення лише з надійних джерел, ізоляція середовища за допомогою контейнеризації для обмеження поширення шкідливого ПЗ.

– Приклад реального інциденту: атака WannaCry в 2017 році [3], яка паралізувала тисячі систем по всьому світу.

2. Атаки на відмову в обслуговуванні.

– Короткий опис: атаки, що перевантажують ресурси мережі, роблячи сервіси недоступними для користувачів.

– Потенційні наслідки: недоступність сервісів, фінансові втрати, зниження репутації.

– Цільова аудиторія: власники веб-сайтів, онлайн-сервісів.

– Методи протидії: використання захисних сервісів, налаштування брандмауерів для обмеження трафіку, мережевий моніторинг для виявлення атак.

– Приклад реального інциденту: атака на Dyn в 2016 році [4], що вивела з ладу багато популярних веб-сайтів.

3. Фішинг.

– Короткий опис: обман користувачів з метою отримання конфіденційної інформації через підроблені повідомлення або сайти.

– Потенційні наслідки: викрадення конфіденційної інформації, фінансові втрати, підміна облікових записів.

– Цільова аудиторія: усі користувачі електронної пошти та онлайн-сервісів.

– Методи протидії: навчання користувачів розпізнавати фішингові атаки, використання фільтрів для електронної пошти, впровадження багатофакторної аутентифікації (MFA), використання VPN для безпечного підключення до мережі.

– Приклад реального інциденту: фішингова атака на користувачів Gmail у 2017 році, яка маскувалася під документи Google Docs [5].

4. Перехоплення даних.

– Короткий опис: несанкціоноване перехоплення мережевого трафіку для викрадення інформації.

– Потенційні наслідки: викрадення конфіденційних даних, компрометація облікових записів.

– Цільова аудиторія: усі користувачі мережі, особливо ті, що використовують незахищені мережі.

– Методи протидії: використання шифрування даних (SSL/TLS), встановлення систем виявлення вторгнень (IDS), використання захищених протоколів передачі даних, використання VPN.

– Приклад реального інциденту: інцидент з перехопленням даних через уразливість у Wi-Fi протоколі WPA2 (атака KRACK) у 2017 році [6].

5. Внутрішні загрози.

– Короткий опис: загрози від співробітників або інших осіб з доступом до мережі.

– Потенційні наслідки: викрадення або втрата даних, порушення роботи систем.

– Цільова аудиторія: співробітники, внутрішні користувачі мережі.

– Методи протидії: впровадження політик безпеки та контролю доступу, моніторинг активності користувачів, навчання співробітників принципам

безпеки, використання VPN для захисту віддаленого доступу, ізоляція середовища за допомогою контейнеризації.

– Приклад реального інциденту: інцидент з витоком даних у компанії Tesla в 2018 році через дії незадоволеного співробітника [7].

Загалом, захист мережевих інфраструктур є критично важливим для забезпечення конфіденційності, цілісності та доступності даних. Аналіз потенційних загроз для безпеки даних є критичним етапом для розробки ефективної стратегії захисту. Розглянуті найпоширеніші загрози безпеки даних вимагають комплексного підходу до захисту, що включає в себе застосування різноманітних методів їх протидії.

1.3 Методи протидії загрозам безпеки даних

Методи протидії загрозам безпеки даних включають в себе використання широкого спектру технологій та стратегій, спрямованих на запобігання несанкціонованому доступу, злому та крадіжці інформації. Серед них можна виокремити: використання VPN технологій, встановлення ефективних систем захисту, шифрування конфіденційних даних, використання ізольованого середовища, регулярне оновлення програмного забезпечення, навчання персоналу. Крім того, важливим аспектом є вчасна виявлення і реагування на інциденти безпеки, в тому числі за допомогою моніторингу та аналізу активності в мережі. Нижче наведено детальний огляд кожного методу протидії загрозам.

1. Використання VPN технологій. VPN дозволяє створити захищене з'єднання через незахищені мережі, такі як Інтернет. VPN шифрує інтернет-трафік користувача, приховує його IP-адресу, забезпечує конфіденційність і захищає від перехоплення даних.

До основних переваг відносяться:

– Захист від перехоплення. VPN шифрує трафік і маскує IP-адресу, захищаючи дані від прослуховування.

– Доступ до обмеженого контенту. Дозволяє обійти географічні блокування і отримати доступ до ресурсів, недоступних у вашому регіоні.

– Безпека на громадських Wi-Fi. Забезпечує безпеку даних на відкритих мережах Wi-Fi, шифруючи трафік.

До основних недоліків відносяться:

– Зменшення швидкості. Може призвести до зменшення швидкості з'єднання через шифрування.

– Вартість. Деякі сервіси є платними, що може вимагати додаткових витрат.

– Надійність сервісу. Не всі VPN-сервіси однаково надійні, що може стати проблемою для конфіденційних даних.

Загрози, яким протидіє:

– Перехоплення даних. Без VPN дані користувачів можуть бути відомі зловмисникам, які перехоплюють трафік на небезпечних мережах або через методи "людина посередині". Використання VPN шифрує трафік, ускладнюючи перехоплення та розшифрування даних.

– Відстеження онлайн-активності. Без VPN провайдер Інтернету та інші сторонні особи можуть відстежувати онлайн-активність за IP-адресою. Використання VPN маскує IP-адресу, роблячи користувача анонімним в Інтернеті та ускладнюючи відстеження інтернет-перегляду.

– Обмеження доступу до контенту. Деякі веб-сайти та сервіси обмежують доступ до контенту залежно від місця знаходження. VPN дозволяє обійти ці географічні обмеження, дозволяючи отримувати доступ до заблокованого контенту.

– Блокування шкідливих сайтів. Деякі VPN-провайдери мають функціонал, що блокує доступ до шкідливих або небажаних веб-сайтів, допомагаючи запобігти потенційним загрозам безпеки.

2. Встановлення систем захисту. Це включає впровадження антивірусного програмного забезпечення, файрволів, систем виявлення вторгнень (IDS) та

систем запобігання вторгнень (IPS). Вони допомагають виявляти, запобігати та реагувати на кіберзагрози.

До основних переваг відносяться:

– Захист від різноманітних загроз. Забезпечує захист системи від вірусів, шкідливих програм і вторгнень.

– Моніторинг та виявлення інцидентів. Допомагає вчасно виявляти потенційні загрози і реагувати на них.

– Забезпечення відповідності. Допомагає відповідати стандартам безпеки та регулятивним вимогам.

До основних недоліків відносяться:

– Постійне оновлення. Вимагає постійного оновлення програмного забезпечення та виявлення нових загроз.

– Складність налаштування. Налаштування може бути складним, особливо для складних систем.

Загрози, яким протидіє:

– Віруси і шкідливі програми. Захищає систему від інфікування та розповсюдження вірусів.

– Вторгнення. Захищає систему від несанкціонованого доступу та вторгнень.

– Витік конфіденційної інформації. Захищає конфіденційну інформацію від неавторизованих користувачів.

3. Шифрування конфіденційних даних. Шифрування перетворює дані у форму, яку можуть прочитати лише ті, хто має відповідний ключ дешифрування. Це забезпечує захист інформації від несанкціонованого доступу, зберігаючи її конфіденційність як під час передачі, так і в стані спокою.

До основних переваг відносяться:

– Захист від несанкціонованого доступу. Шифрування даних зробить їх непридатними для перегляду без відповідного ключа шифрування.

– Забезпечення конфіденційності. Допомагає уникнути витоку конфіденційної інформації, навіть якщо дані стануть доступними зловмисникам.

– Вимоги до відповідності. Виконання регулятивних вимог і стандартів щодо захисту даних.

До основних недоліків відносяться:

– Управління ключами. Необхідно правильно керувати ключами шифрування для забезпечення безпеки даних.

– Додаткові витрати. Деякі методи шифрування можуть потребувати додаткових витрат на обладнання та програмне забезпечення.

Загрози, яким протидіє:

– Перехоплення даних. Шифрування захищає дані від перехоплення сторонніми особами під час передачі по мережі.

– Витік конфіденційної інформації. Шифрування робить дані непридатними для використання навіть у випадку їхнього несанкціонованого доступу.

4. Використання ізольованого середовища. Ізольоване середовище дозволяє запускати програми в окремому, безпечному середовищі. Це обмежує можливість шкідливого програмного забезпечення впливати на основну систему і дозволяє безпечно тестувати підозрілі програми.

До основних переваг відносяться:

– Відокремлення ризиків. Допомагає уникнути поширення інфекцій та загроз між різними середовищами.

– Забезпечення безпеки. Захищає систему від потенційних загроз, які можуть виникнути у інших середовищах.

– Тестування безпеки. Надає можливість випробувати нові програми та веб-сайти в безпечному середовищі.

До основних недоліків відносяться:

– Витрати ресурсів. Використання ізольованого середовища може вимагати додаткових ресурсів комп'ютера.

– Складність конфігурації. Налаштування і підтримка ізольованого середовища може бути складними завданнями.

Загрози, яким протидіє:

– Вторгнення. Ізольоване середовище допомагає уникнути вторгнень у головну систему з небезпечних джерел.

– Розповсюдження інфекцій. Захищає від поширення інфекцій та шкідливих програм між різними середовищами.

5. Регулярне оновлення програмного забезпечення. Регулярні оновлення для операційних систем, програмного забезпечення та додатків усувають вразливості та баги. Це знижує ризик експлуатації цих вразливостей кіберзлочинцями для проведення атак.

До основних переваг відносяться:

– Усунення вразливостей. Оновлення допомагають усувати вразливості, які можуть бути використані для атак.

– Покращення функціональності. Нові версії програмного забезпечення часто містять покращення та нові функції.

– Відповідність стандартам. Допомагає відповідати стандартам безпеки та вимогам, що може бути критично важливим для підтримки діяльності

До основних недоліків відносяться:

– Час та зусилля. Оновлення програмного забезпечення може вимагати значного часу та зусиль для виконання.

– Сумісність. Нові версії програм можуть бути несумісними з існуючими системами або додатками.

– Можливість збоїв. Оновлення може призвести до несправностей або втрати функціональності в програмному забезпеченні.

Загрози, яким протидіє:

– Вразливості. Регулярні оновлення допомагають уникнути використання вразливостей для атак.

– Кібератаки. Оновлене програмне забезпечення може мати покращені захисні функції, які допомагають уникнути кібератак.

– Втрата даних. Зменшує ризик втрати даних через атаки або небажані програмні помилки.

Хоч кожен із цих методів має свої недоліки, їх комбінація може створити надійний комплексний захист. Наприклад, поєднання використання VPN з ізоляцією середовища за допомогою контейнеризації може забезпечити не лише шифрування трафіку, але й відокремлення додатків, зменшуючи ризик передачі шкідливих програм. Тому в подальшому для дослідження та аналізу буде використана інтеграція OpenVPN та контейнеризації, що відкриває нові можливості у цій області, дозволяючи постійно вдосконалювати методи захисту даних.

2 ТЕОРЕТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ OPENVPN ТА КОНТЕЙНЕРИЗАЦІЇ

2.1 Огляд OpenVPN для безпеки мережі та конфіденційності даних

OpenVPN – це система віртуальної приватної мережі (VPN), яка реалізує методи створення безпечних з'єднань «point-to-point» або «site-to-site» у маршрутизованих або мостових конфігураціях, а також засобів віддаленого доступу [8]. Вона реалізує як клієнтські, так і серверні додатки. OpenVPN є одним з найбільш популярних VPN-рішень завдяки своїй відкритій архітектурі, широким можливостям налаштування та надійному захисту.

OpenVPN працює, створюючи безпечне з'єднання між пристроєм користувача та інтернетом через віртуальну приватну мережу. Спочатку користувач встановлює OpenVPN-клієнт на своєму пристрої, який підключається до OpenVPN сервера через інтернет. Вони перевіряють один одного за допомогою сертифікатів або імені користувача і пароля. Після успішної аутентифікації всі дані, які передаються між пристроєм і сервером, шифруються, забезпечуючи захист від перехоплення. Це дозволяє безпечно передавати дані через інтернет, захищаючи приватність та конфіденційність.

До особливостей та переваг OpenVPN відносяться:

– Протоколи шифрування та безпеки [9]. OpenVPN використовує надійні стандарти шифрування, включаючи AES-256, що забезпечує високий рівень захисту даних [10]. Він підтримує протоколи TCP і UDP, дозволяючи користувачам вибирати, виходячи з власних потреб у швидкості та надійності.

– Прозорість відкритого коду [9]. Оскільки OpenVPN має відкритий вихідний код, що дає швидко виявляти і виправляти вразливості, підтримуючи високий стандарт безпеки.

– Налаштування та контроль. OpenVPN пропонує широкі можливості налаштування, включаючи конфігурації повного тунелю і розділеного тунелю,

що дозволяє користувачам направляти певний трафік через VPN, в той час як інший трафік обходить його.

– Багатофакторна автентифікація (MFA). Для подальшого підвищення безпеки OpenVPN підтримує MFA, додаючи додатковий рівень захисту, окрім паролів.

– Багатоплатформна сумісність [9]. OpenVPN можна використовувати на широкому спектрі операційних систем, включаючи Windows, macOS, Linux та Android. Це робить її доступною для широкого кола користувачів.

– Продуктивність. Хоча OpenVPN є дуже безпечним, такий рівень шифрування може іноді призводити до зниження продуктивності порівняно з іншими протоколами, такими як WireGuard. Цей компроміс часто вважається прийнятним з огляду на високий рівень безпеки, який він забезпечує.

– Підтримка [9]. OpenVPN забезпечує потужну підтримку за допомогою спільноти користувачів та розробників, а також детальної документації. Характер проекту, керованого спільнотою, також означає, що існує безліч ресурсів і форумів, де користувачі можуть звернутися за допомогою і поділитися конфігураціями.

Загалом, OpenVPN є потужним інструментом для тих, хто прагне надійної безпеки та конфіденційності. Його надійне шифрування, широкі можливості налаштування та відкритий вихідний код роблять його надійним вибором, хоча для налаштування та оптимізації може знадобитися певний технічний досвід. Для тих, кому потрібне захищене і налаштовуване VPN-рішення, OpenVPN є чудовим варіантом, який підтримується як спеціальною спільнотою, так і регулярними аудитами безпеки.

2.2 Роль контейнеризації у безпеці та ізоляції даних

Контейнеризація – це метод віртуалізації, який використовує легкі, автономні пакети програмного забезпечення, які називаються контейнерами. Кожен контейнер включає в себе код програми, його залежності та бібліотеки, а

також конфігурацію, необхідну для його запуску. Це робить контейнери ідеальними для розгортання програм у середовищах з високим рівнем безпеки.

Контейнеризація працює шляхом упаковки застосунку разом з усіма його залежностями в окремий контейнер. Спочатку користувач створює Docker-образ, який містить код застосунку, необхідні бібліотеки та налаштування. Цей образ запускається в ізольованому середовищі – контейнері, який використовує ресурси операційної системи (хоста). Завдяки цьому контейнери швидко запускаються, працюють ефективно та можуть легко переноситися між різними середовищами, такими як локальні машини, тестові сервери та хмарні платформи.

До особливостей та переваг контейнеризації відносяться:

– Ізоляція [11]. Кожен контейнер ізольований від інших контейнерів, а також від базової системи. Це означає, що зловмисний код або шкідливі програми, які можуть заразити один контейнер, не зможуть вплинути на інші контейнери або систему. Ця ізоляція робить контейнери стійкішими до кібератак, адже зловмисникам буде складніше отримати доступ до критичних даних або систем.

– Контроль доступу. Доступ до контейнерів та їх ресурсів можна чітко контролювати. Це дозволяє адміністраторам обмежувати доступ до певних контейнерів лише авторизованим користувачам або процесам. Це допомагає захистити конфіденційні дані та запобігти несанкціонованому доступу.

– Незмінність. Контейнери можна створити та розгорнути з гарантією їх незмінності. Це означає, що код та конфігурація контейнера не можуть бути змінені після його створення. Це робить контейнери стійкими до маніпуляцій та гарантує, що програми завжди запускатимуться очікуваним чином.

– Легкість розгортання. Контейнери можна легко розгорнути та масштабувати. Це робить їх ідеальними для розгортання програм у хмарних середовищах або для швидкого створення нових середовищ розробки та тестування.

– Ефективність [11]. Контейнери використовують менше ресурсів, ніж традиційні віртуальні машини. Це робить їх більш економічно вигідними для розгортання та експлуатації.

Контейнеризація також може допомогти забезпечити ізоляцію даних. Оскільки кожен контейнер має власну ізольовану файлову систему, дані одного контейнера недоступні для інших контейнерів або для базової системи. Це може допомогти захистити конфіденційні дані та запобігти витоку даних. Крім того, контейнери можна використовувати для шифрування даних, що робить їх ще більш стійкими до несанкціонованого доступу.

2.3 Інтеграція OpenVPN і контейнеризованого середовища

Інтеграція OpenVPN у контейнеризовані середовища, такі як Docker, забезпечує високий рівень захисту конфіденційності та безпеки даних. Ця комбінація об'єднує переваги обох технологій для створення надійного та безпечного середовища.

Інтеграція OpenVPN і контейнеризованого середовища полягає у встановленні та запуску OpenVPN сервера всередині контейнера. Для цього використовується відповідний образ, який містить необхідне програмне забезпечення та налаштування для роботи з OpenVPN. Після запуску контейнера користувач може виконати необхідну конфігурацію OpenVPN, таку як налаштування мережних параметрів, ключі шифрування та аутентифікації, після чого сервер буде готовий приймати з'єднання від клієнтів.

Інтеграція OpenVPN і контейнеризації може дати ряд переваг, таких як підвищена безпека, ізоляція мережі, доступність з будь-якого місця, масштабованість і гнучкість.

Однак важливо врахувати потенційні недоліки цієї інтеграції, такі як збільшення навантаження на систему, складність налаштування, можливість витоку IP-адреси, можливість атак типу "людина посередині" та можливість відстеження трафіку. Ці недоліки можна частково або повністю усунути за допомогою таких методів, як використання більш потужного обладнання,

використання інструментів автоматизації, використання VPN-шлюзу, використання сертифіката підпису та використання шифрування.

2.4 Аналіз Docker-образів з OpenVPN сервером: огляд, порівняння

OpenVPN, як відкрита і надійна реалізація VPN, забезпечує зашифровану та безпечну передачу даних між користувачами та серверами. Проте для успішного використання OpenVPN необхідно ефективно розгорнути його сервер.

Однією з передових технологій для розгортання серверних програм у сучасних системах є контейнеризація. Контейнери, зокрема Docker, надають зручний та ізольований спосіб розгортання, управління та масштабування додатків. Інтеграція OpenVPN з контейнеризованим середовищем, таким як Docker, відкриває нові можливості для швидкого та зручного розгортання VPN-серверів з мінімальними зусиллями.

У даному контексті важливо ретельно дослідити різні Docker-образи, які включають в себе OpenVPN сервер, з метою порівняння їхніх можливостей, безпеки та продуктивності. Це допоможе зробити обґрунтований вибір підходящого образу для конкретних потреб користувача.

Існує багато Docker-образів, які пропонують OpenVPN сервер. Ці образи дозволяють легко налаштувати та запустити VPN-сервер у вашому контейнері Docker.

Деякі з найпопулярніших Docker-образів OpenVPN включають:

– linuxserver/openvpn [12]. Цей образ базується на відкритому програмному забезпеченні та надає можливість швидко налаштувати OpenVPN сервер у контейнері Docker. Він містить всі необхідні компоненти для роботи з VPN, включаючи сервер, клієнтів та інструменти керування.

– kyleman/docker-openvpn [13]. Цей образ є простим у використанні OpenVPN-образом Docker. Він відрізняється простотою використання та налаштування, має активну спільноту користувачів, яка забезпечує підтримку, та

зручний інтерфейс з детальною документацією. Цей образ користується популярністю серед користувачів Docker завдяки своїм функціональностям та надійності.

– openvpn/openvpn-as [14]. Цей образ від компанії OpenVPN містить Access Server (AS), який є комерційним рішенням для створення VPN мережі. Він надає розширений набір функцій, таких як графічний інтерфейс користувача, інструменти адміністрування та можливості інтеграції з іншими системами.

В таблиці 2.1 наведено порівняльний аналіз цих трьох найпопулярніших Docker-образів.

Таблиця 2.1 – Порівняння найпопулярніших Docker-образів

Функціональність	linuxserver/openvpn	kyleman/docker-openvpn	openvpn/openvpn-as
Тип образу	Сервер OpenVPN	Сервер OpenVPN	Менеджер OpenVPN з сервером
Підтримка Docker Compose	Так	Так	Так
Відкритий код	Так	Так	Ні
Версія OpenVPN	2.4.5	2.5.4	2.5.4
Підтримка протоколів	UDP, TCP	UDP, TCP	UDP, TCP
Методи шифрування	AES-128-CBC, AES-256-CBC, Blowfish-CBC	AES-128-CBC, AES-256-CBC, Blowfish-CBC	AES-128-CBC, AES-256-CBC, Blowfish-CBC
Аутентифікація	Пароль, сертифікат, PAM	Пароль, сертифікат	Пароль, сертифікат, LDAP
Підтримка IPv6	Так	Так	Так
Підтримка Docker Swarm	Так	Так	Так

Продовження таблиці 2.1

Моніторинг	Prometheus, Grafana	Prometheus, Grafana	Prometheus, Grafana
Оновлення	Автоматичне	Автоматичне	Автоматичне
Підтримка спільноти	Форум, GitHub	Форум, GitHub	GitHub
Ліцензія	GNU GPL v2.0	GNU GPL v3.0	GNU GPL v2.0

На основі наведеного порівняння, kyleman/docker-openvpn є чудовим вибором для багатьох користувачів завдяки своїй простоті використання, набору функцій та розміру образу. До ключових причин належать:

– Простота використання. Цей образ простий у налаштуванні та запуску, що робить його чудовим вибором для початківців.

– Функціональність. Він пропонує всі основні функції OpenVPN, а також деякі додаткові функції, такі як підтримка Tunnelblick.

– Розмір образу. Він має порівняно невеликий розмір образу, що робить його зручним для використання на пристроях з обмеженими ресурсами.

– Автоматичні оновлення. Образ автоматично оновлюється, що гарантує використання вами найновішої версії OpenVPN.

– Підтримка спільноти. Він має активну спільноту користувачів на GitHub та форумах, які можуть допомогти вам у разі виникнення проблем.

Отже, на основі цих факторів образ Docker kylemanna/docker-openvpn є найкращим варіантом для реалізації віртуальної приватної мережі OpenVPN з точки зору спрощення налаштування, зручності управління та розширюваності.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХИСТУ ДАНИХ ЗА ДОПОМОГОЮ OPENVPN В КОНТЕЙНЕРІ

У цьому розділі буде детально розглянуто процес практичної реалізації захисту даних за допомогою OpenVPN у контейнеризованому середовищі. Спочатку буде описано встановлення Docker, що є необхідним для створення ізольованого середовища для OpenVPN. Далі буде налаштовано самий OpenVPN-сервер у Docker-контейнері, включаючи генерацію сертифікатів і ключів для забезпечення безпечного з'єднання. На завершення буде розглянуто встановлення клієнтського програмного забезпечення OpenVPN на різних пристроях та тестування з'єднання для перевірки його працездатності.

3.1 Встановлення Docker

Цей пункт кваліфікаційної роботи детально описує процес встановлення Docker на пристрої з операційною системою Linux. Docker є платформою для розробки, доставки та запуску додатків у контейнерах. Контейнери дозволяють ізолювати додатки від системного середовища, забезпечуючи їх незалежну та стабільну роботу.

Для початку встановлення Docker необхідно увійти на пристрій з операційною системою Linux під обліковим записом з адміністративними правами. Це дозволить виконувати необхідні команди для встановлення та налаштування Docker.

Перед встановленням Docker, необхідно встановити деякі пакети, що є передумовою для його коректної роботи. Для цього необхідно виконати наступну команду в терміналі:

```
$ sudo apt install apt-transport-https ca-certificates curl software-properties-common gnupg-agent -y
```

Ця команда встановлює пакети для транспортування через HTTPS, сертифікати, утиліту curl для завантаження файлів з інтернету, утиліти для управління репозиторіями та агент GPG для управління ключами. Наступний крок – додавання GPG ключа Docker, який забезпечує автентичність завантажених пакетів Docker. Для цього необхідно виконати наступну команду:

```
$ curl -fsSL https://download.docker.com/linux/$(awk -F'=' '/^ID=/{
print $NF }' /etc/os-release)/gpg | sudo apt-key add -
```

Ця команда завантажує GPG ключ Docker та додає його до системи ключів Linux дистрибутиву. Далі необхідно додати офіційний репозиторій Docker до системних джерел. Для цього потрібно виконати наступну команду:

```
$ sudo add-apt-repository "deb [arch=$(dpkg --print-architecture)]
https://download.docker.com/linux/$(awk -F'=' '/^ID=/{ print $NF }'
/etc/os-release) $(lsb_release -cs) stable"
```

Ця команда додає репозиторій Docker, який містить стабільні версії Docker для дистрибутиву Linux. Після додавання репозиторію можна встановити Docker та Docker Compose, виконавши наступну команду:

```
$ sudo apt install docker-ce docker-compose containerd.io -y
```

Ця команда встановлює Docker Engine, Docker Compose для управління багатоконтейнерними додатками та containerd.io – інфраструктуру контейнерів, яку використовує Docker. Після встановлення Docker необхідно активувати та запустити його службу, виконавши наступні команди:

```
$ sudo systemctl enable docker
$ sudo systemctl start docker
```

Перша команда дозволяє автоматичний запуск служби Docker при завантаженні системи, а друга запускає службу Docker. Для зручності та безпеки

можна додати поточного користувача до групи Docker, щоб мати можливість виконувати Docker команди без sudo, виконавши команду:

```
$ sudo usermod -aG docker $USER
```

Ця команда додає поточного користувача до групи Docker. Щоб зміни набули чинності, необхідно виконати ре-аутентифікацію користувача, виконавши команду:

```
$ su - $USER
```

Ця команда завершить поточний сеанс і розпочне новий з оновленими груповими налаштуваннями.

Після виконання всіх вищезазначених кроків Docker буде встановлений і готовий до використання на Linux пристрої. Це дозволить користувачу створювати та керувати контейнерами, які ізолюють додатки від системного середовища, забезпечуючи їх стабільну та незалежну роботу.

3.2 Налаштування сервера OpenVPN у Docker

У цьому пункті буде детально розглянуто процес налаштування сервера OpenVPN у Docker-контейнері. OpenVPN у контейнеризованому середовищі забезпечує ізоляцію та незалежність від основної системи, що підвищує безпеку та спрощує керування.

Першим кроком є створення робочої директорії для зберігання конфігураційних файлів та інших даних OpenVPN. Для цього необхідно виконати наступну команду в терміналі:

```
$ mkdir ~/docker/openvpn-server -p
```

Ця команда створює директорію openvpn-server у домашній директорії під директорією docker. Далі необхідно встановити кілька змінних оточення, які

будуть використовуватися під час налаштування OpenVPN, виконавши команди, що наведені в лістингу 3.1.

Лістинг 3.1 – Код для встановлення змінного оточення

```
$ OVPN_DATA="ovpn-data-dockerserver"
$ OVPN_HOST="udp://5.58.107.210"
$ OVPN_CLIENT="windows-client"
```

Змінна OVPN_DATA визначає ім'я контейнера з даними, OVPN_HOST встановлює адресу сервера OpenVPN, а OVPN_CLIENT задає ім'я клієнта. Після встановлення змінних оточення необхідно завантажити Docker-образ OpenVPN, виконавши наступну команду:

```
$ docker pull kylemanna/openvpn
```

Результат виконання команди наведено на рисунку 3.1.

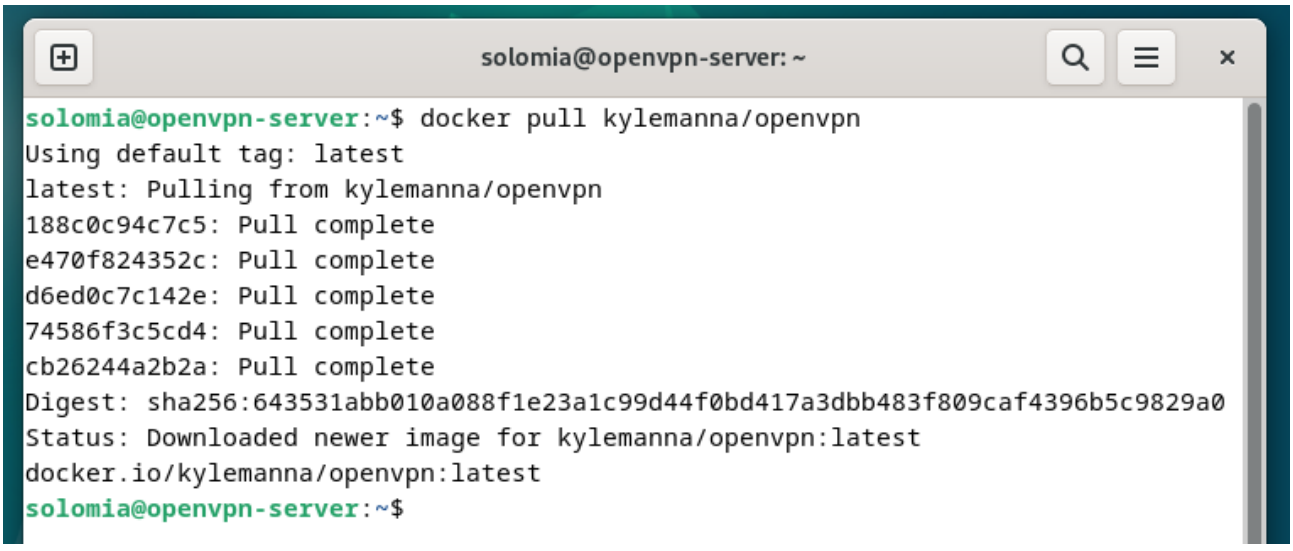

Рисунок 3.1 – Завантаження Docker-образу

Ця команда завантажує офіційний Docker-образ OpenVPN від користувача kylemanna з Docker Hub. Наступним кроком є генерація конфігураційних файлів OpenVPN. Для цього необхідно виконати наступну команду:

```
$ docker run -v ~/docker/openvpn-server:/etc/openvpn --rm kylemanna/openvpn ovpn_genconfig -u ${OVPN_HOST}
```

Результат виконання команди наведено на рисунку 3.2.

Рисунок 3.2 – Процес генерації конфігураційних файлів

Ця команда створює необхідні конфігураційні файли та зберігає їх у робочій директорії ~/docker/openvpn-server. Далі необхідно ініціалізувати інфраструктуру публічних ключів (PKI) для OpenVPN, виконавши наступну команду:

```
$ docker run -v ~/docker/openvpn-server:/etc/openvpn --rm -it kylemanna/openvpn ovpn_initpki
```

При виконанні цієї команди користувач повинен ввести наступну інформацію:

– Пароль для захисту PKI. Користувач буде запитаний ввести та підтвердити пароль для захисту інфраструктури публічних ключів (PKI). Цей пароль захищає ключі і сертифікати, які будуть створені.

– Загальне ім'я для сертифікату сертифікаційного центру (CA). Користувач буде запитаний ввести загальне ім'я для сертифікату CA. Це ім'я ідентифікує сертифікаційний центр і використовується для підписування інших сертифікатів.

– Пароль для захисту приватного ключа CA. Користувач буде запитаний ввести та підтвердити пароль для захисту приватного ключа сертифікаційного центру (CA). Цей пароль потрібен для додаткового захисту ключа CA, який використовується для підписування сертифікатів.

На рисунку 3.3 та 3.4 наведено процес ініціалізації інфраструктуру публічних ключів.

```
solomia@openvpn-server:~$ docker run -v ~/docker/openvpn-server:/etc/openvpn --r
m -it kylemanna/openvpn ovpn_initpki

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /etc/openvpn/pki


Using SSL: openssl OpenSSL 1.1.1g  21 Apr 2020

Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
Generating RSA private key, 2048 bit long modulus (2 primes)
...+++++
.....................................................................+++++
e is 65537 (0x010001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:openvpn-server
```

Рисунок 3.3 – Процес ініціалізації інфраструктури публічних ключів

```
.....................................................................
.....................................................+++++
writing new private key to '/etc/openvpn/pki/easy-rsa-73.OpMFfc/tmp.LcdBEF'
-----
Using configuration from /etc/openvpn/pki/easy-rsa-73.OpMFfc/tmp.IkdmKH
Enter pass phrase for /etc/openvpn/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'192.168.28.158'
Certificate is to be certified until Apr 20 17:01:56 2026 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Using SSL: openssl OpenSSL 1.1.1g  21 Apr 2020
Using configuration from /etc/openvpn/pki/easy-rsa-148.iHpkHN/tmp.kpnlfC
Enter pass phrase for /etc/openvpn/pki/private/ca.key:

An updated CRL has been created.
CRL file: /etc/openvpn/pki/crl.pem
```

Рисунок 3.4 – Процес ініціалізації інфраструктури публічних ключів

Після завершення ініціалізації PKI можна запустити контейнер OpenVPN-сервера, виконавши наступну команду:

```
$ docker run -v ~/docker/openvpn-server:/etc/openvpn --rm -it kylemanna/openvpn ovpn_initpki
```

Ця команда запускає контейнер у фоновому режимі, мапує порт 1194 для UDP-з'єднань і надає контейнеру необхідні привілеї мережевого адміністрування. Контейнер буде автоматично перезапущено у разі збою або перезавантаження системи. Результат виконання команди наведено на рисунку 3.5.

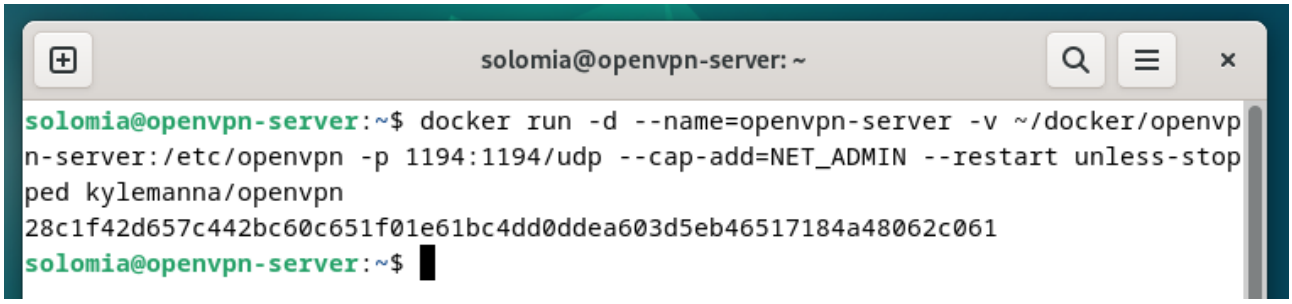

Рисунок 3.5 – Процес запуску контейнера OpenVPN-сервера

Далі необхідно створити сертифікат для клієнта. Для цього користувачу необхідно виконати наступну команду:

```
$ docker run -v ~/docker/openvpn-server:/etc/openvpn --rm -it kylemanna/openvpn easyrsa build-client-full ${OVPN_CLIENT}:1194 nopass
```

Результат виконання цієї команди наведено на рисунку 3.6. Ця команда генерує клієнтський сертифікат без пароля для вказаного імені клієнта. Під час виконання команди буде запитано пароль для захисту приватного ключа сертифікаційного центру. При виконанні цієї команди користувач повинен ввести наступну інформацію:

– Пароль для захисту PKI. Перший запит буде на введення пароля для захисту інфраструктури публічних ключів.

– Підтвердження пароля для захисту PKI. Після введення пароля, потрібно його підтвердити, ввівши той самий пароль ще раз.

– Загальне ім'я для сертифікату сертифікаційного центру. Після введення і підтвердження пароля користувач буде запитаний ввести загальне ім'я для сертифікату CA. Це ім'я ідентифікує сертифікаційний центр і буде використовуватися для підписування інших сертифікатів.

– Пароль для захисту приватного ключа CA. Останній запит буде на введення пароля для захисту приватного ключа сертифікаційного центру. Цей пароль потрібен для додаткового захисту ключа CA, який використовується для підписування сертифікатів.

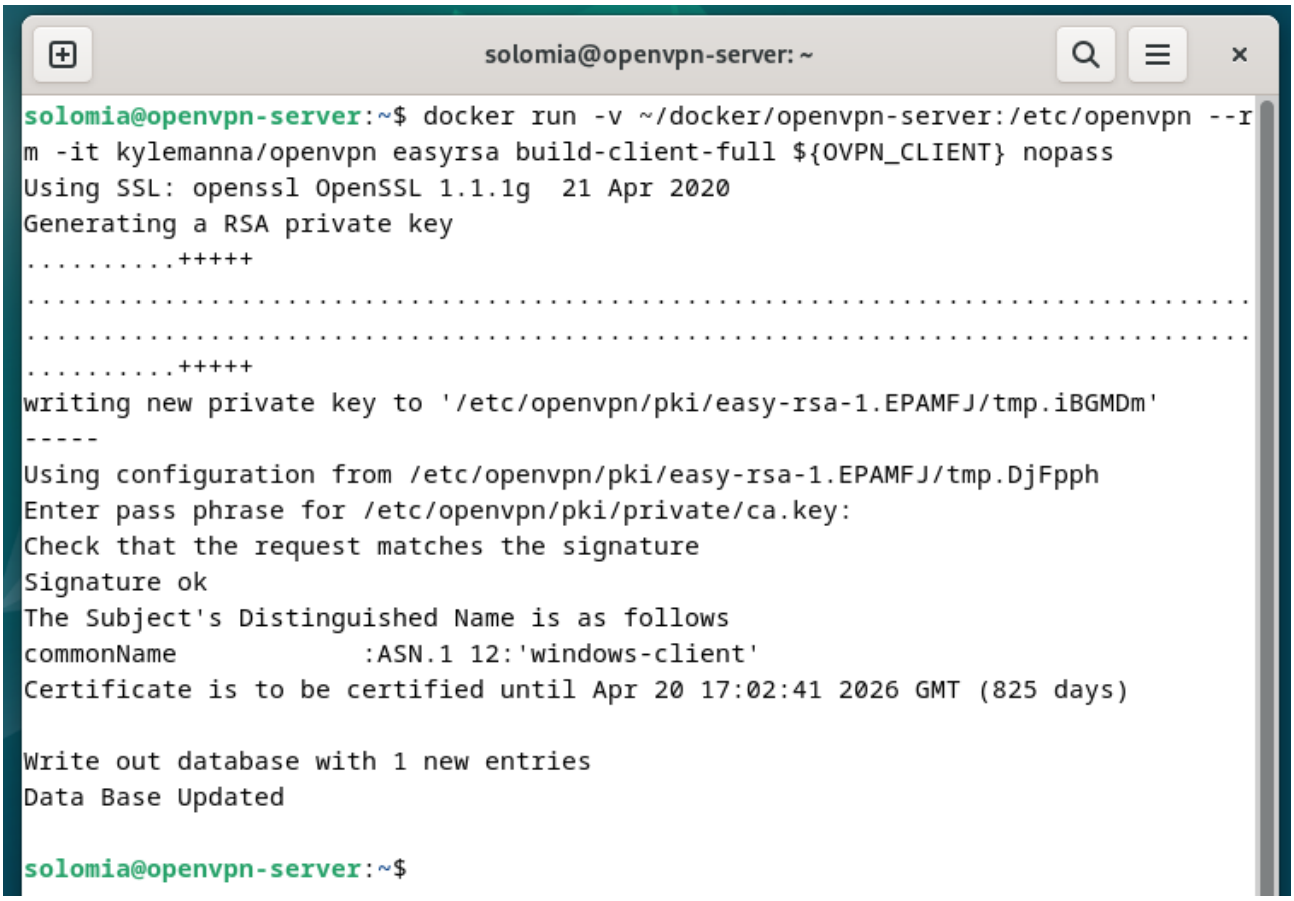

Рисунок 3.6 – Процес створення сертифікатів клієнта

На завершення необхідно створити конфігураційний файл для клієнта, виконавши наступну команду:

```
$ docker run -v ~/docker/openvpn-server:/etc/openvpn --rm kylemanna/openvpn ovpn_getclient ${OVPN_CLIENT} > ${OVPN_CLIENT}.ovpn
```

Ця команда генерує конфігураційний файл OpenVPN для клієнта і зберігає його у файлі ${OVPN_CLIENT}.ovpn.

Ці кроки забезпечують повну налаштування OpenVPN-сервера у Docker-контейнері, створення необхідних сертифікатів і ключів, а також генерацію конфігураційного файлу для клієнтських пристроїв.

3.3 Встановлення OpenVPN клієнтського програмного забезпечення та тестування

У цьому розділі проводиться встановлення та налаштування клієнтського програмного забезпечення для OpenVPN на різних платформах, таких як Windows, iOS та Android. Тестування здійснюється з метою перевірки коректності налаштувань, стабільності з'єднання та забезпечення конфіденційності даних під час використання віртуальної приватної мережі.

3.3.1 Процес підключення до OpenVPN сервера на клієнтських пристроях

Для того, щоб підключитися до OpenVPN сервера на пристрої Windows, необхідно виконати кілька простих кроків:

1. Завантажити OpenVPN клієнта із офіційного сайту OpenVPN та інсталювати його на пристрій.

2. Перемістити конфігураційного файл (.ovpn) до директорії C:\Program Files\OpenVPN\config.

3. Запустити OpenVPN GUI від імені адміністратора.

4. Знайти конфігураційний файл у списку та натиснути кнопку "Підключити".

Після успішного підключення іконка OpenVPN у системному треї змінить колір на зелений.

На рисунку 3.7 наведено результат під’єднання до OpenVPN сервера клієнтським пристроєм Windows.

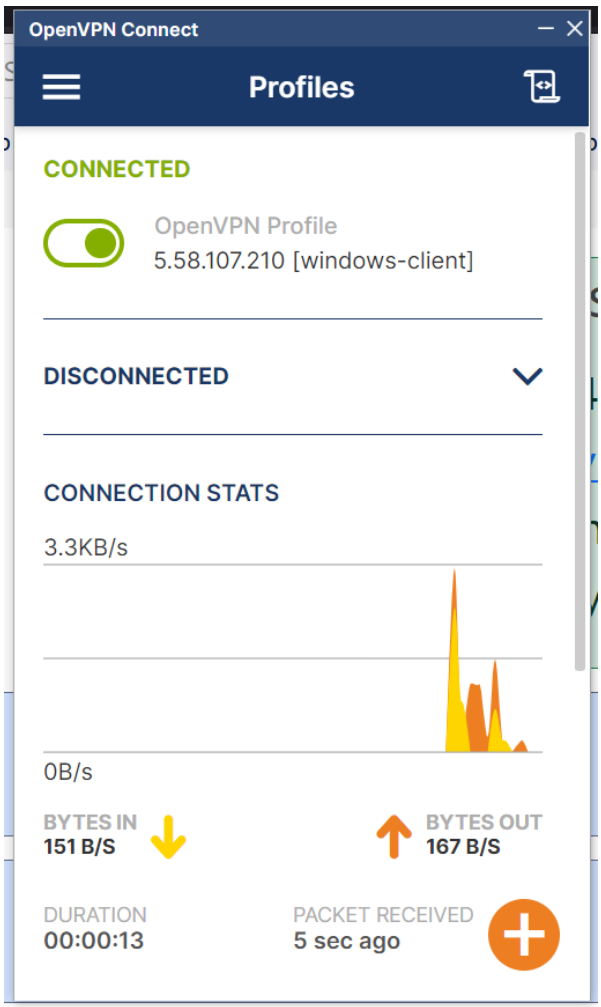

Рисунок 3.7 – Успішне під’єднання до OpenVPN сервера з Windows

Для того, щоб підключитися до OpenVPN сервера на пристрої IOS, необхідно виконати кілька кроків:

1. Завантажити OpenVPN Connect з App Store.
2. Отримати конфігураційний файл (.ovpn).
3. Відкрити файл за допомогою OpenVPN Connect.
4. Запустити додаток OpenVPN Connect, здійснити імпорт конфігураційного файлу та натиснути кнопку підключення.

Після успішного підключення статус зміниться на "Connected" і з’явиться іконка VPN у верхньому рядку пристрою.

На рисунку 3.8 наведено результат під’єднання до OpenVPN сервера клієнтським пристроєм IOS.

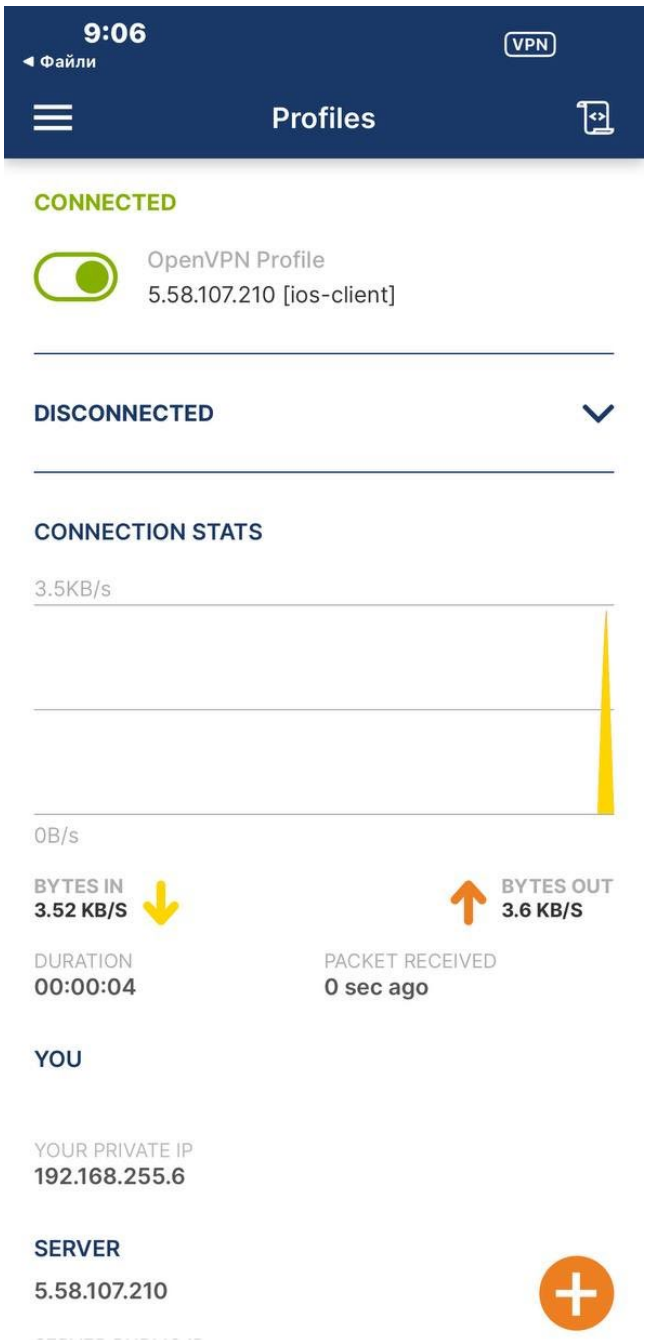

Рисунок 3.8 – Успішне під’єднання до OpenVPN сервера з IOS

Для того, щоб підключитися до OpenVPN сервера на пристрої Android, необхідно виконати аналогічні кроки, що і на пристрої IOS, лише різниця полягає у тому, що додаток OpenVPN Connect необхідно завантажити із Play Market, а не App Store.

На рисунку 3.9 наведено результат під’єднання до OpenVPN сервера клієнтським пристроєм Android.

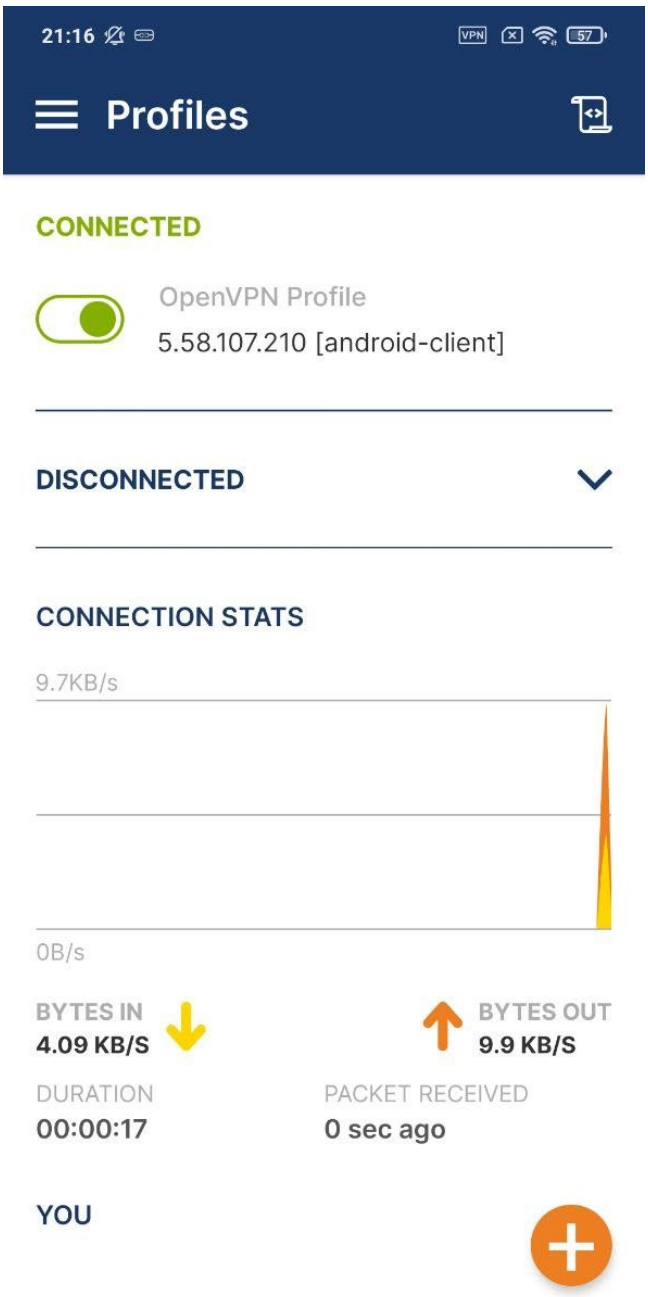

Рисунок 3.9 – Успішне під’єднання до OpenVPN сервера з Android

Процес підключення до OpenVPN сервера на клієнтських пристроях різних платформ є інтуїтивно зрозумілим та простим. Незалежно від того, чи користувач використовує Windows, iOS або Android, він може швидко налаштувати та підключитися до VPN, забезпечивши захищене та конфіденційне з'єднання для своїх даних.

3.3.2 Тестування роботи OpenVPN сервера в контейнеризованому середовищі

Тестування роботи OpenVPN сервера є важливим етапом для забезпечення його належного функціонування та перевірки захищеності даних. Цей процес включає кілька кроків, які допоможуть визначити стабільність з'єднання, ефективність шифрування та загальну продуктивність VPN.

Wireshark – це інструмент для аналізу мережевого трафіку, який дозволяє детально вивчити, що відбувається на мережевому рівні. За його допомогою можна переконатися, що трафік через OpenVPN сервер шифрується і передається належним чином. Нижче наведена детальна інструкція щодо перевірки роботи OpenVPN за допомогою Wireshark.

1. Запуск Wireshark та початок захоплення трафіку.

– Відкрити Wireshark.

– У списку інтерфейсів обрати той, через який проходить інтернет-трафік (зазвичай це Ethernet або Wi-Fi).

– Натиснути кнопку "Start capturing packets" для початку захоплення трафіку.

2. Підключення до OpenVPN сервера.

– Під’єднати клієнтський пристрій до OpenVPN сервера (Windows, iOS або Android), як описано у попередніх інструкціях.

3. Фільтрація трафіку в Wireshark.

– Щоб зосередитися на OpenVPN трафіку, необхідно ввести у поле фільтра в верхній частині вікна Wireshark наступний фільтр: udp.port == 1194.

4. Аналіз трафіку.

– У фільтрованих пакетах користувач може побачити трафік, пов'язаний з OpenVPN.

– Обрати один з пакетів і натиснути на нього, щоб переглянути детальну інформацію в нижній частині вікна Wireshark. Користувач побачить, що пакет містить дані, зашифровані OpenVPN.

5. Перевірка наявності шифрування.

– Окрім того, що дані в пакетах виглядають зашифрованими, можна переконатися в наявності шифрування, переглянувши метадані пакету. Вони повинні включати інформацію про використання OpenVPN та метод шифрування.

– Необхідно обрати пакет OpenVPN і переглянути поле "Data" в нижній частині Wireshark. Користувач побачить, що дані зашифровані (рис. 3.10).

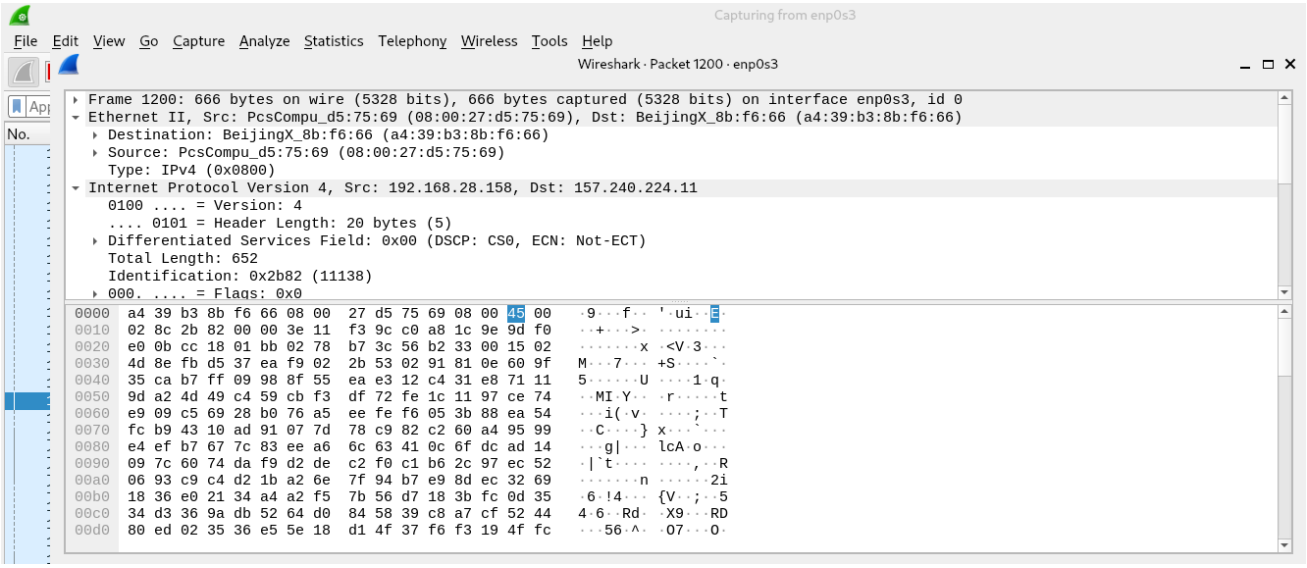

Рисунок 3.10 – Дані, що передаються – зашифровані

Отже, Wireshark є хорошим інструментом, який дозволяє детально аналізувати мережевий трафік та перевірити роботу OpenVPN. З його допомогою можна переконатися, що дані, передані через OpenVPN, надійно зашифровані та захищені від несанкціонованого доступу. Це важливий крок для забезпечення безпеки та конфіденційності даних в мережі.

Перевірка продуктивності OpenVPN, зокрема швидкості передачі даних, є важливою для оцінки ефективності інфраструктури VPN.

Для оцінки продуктивності OpenVPN з точки зору швидкості передачі даних було проведено серію тестів з використанням популярних онлайн-сервісів для вимірювання швидкості Інтернет-з'єднання. Тестування здійснювалося за допомогою наступних сайтів:

– Speedtest.net.ua [15].

– 2ip.ua [16].

Процедура тестування швидкості передбачала наступне:

– Перед підключенням до OpenVPN були виконані тести швидкості на обох сайтах для отримання базових показників швидкості Інтернет-з'єднання без використання VPN. Це включало вимірювання як вхідної (download), так і вихідної (upload) швидкості.

– Після отримання базових показників було здійснено підключення до сервера OpenVPN. Параметри підключення включали стандартне налаштування OpenVPN з використанням протоколу UDP для зниження затримок і максимізації пропускної здатності.

– Здійснювалися повторні тести швидкості на обох сервісах з активним з'єднанням через OpenVPN. Це дозволило оцінити вплив VPN на швидкість передачі даних та виявити можливі втрати в продуктивності.

– Порівнювалися результати тестів без VPN і з VPN для визначення змін у швидкості.

Результати вимірювання швидкості наведено в таблиці 3.1.

Таблиця 3.1 – Порівняння швидкості Інтернет-з'єднання без VPN і з VPN

Тестовий сервіс	Швидкість без VPN (Download/Upload, Mbps)	Швидкість з VPN (Download/Upload, Mbps)	Зниження швидкості (%)
Speedtest.net.ua	30.2 / 25.3	20.3 / 24.3	32 / 3
2ip.ua	30.29 / 30.29	22.13 / 25.37	26 / 16

Тестування швидкості OpenVPN за допомогою сервісів показало, що використання VPN з'єднання може призводити до певного зниження швидкості Інтернет-з'єднання. Це зниження пов'язане з додатковими витратами на шифрування і маршрутизацію трафіку через VPN сервери. Проте, навіть з

урахуванням цього, з'єднання залишалося стабільним і забезпечувало прийнятні швидкості для більшості завдань, що підтверджує ефективність і надійність використання OpenVPN у контейнеризованому середовищі.

Для забезпечення стабільності і надійності роботи VPN сервера важливо оцінити його час автономної роботи, тобто період, протягом якого сервер працює без перебоїв. Це тестування дозволяє визначити, наскільки стійким є сервер до тривалого навантаження та чи здатний він підтримувати постійне з'єднання з клієнтами. Процедура тестування стабільності роботи передбачала наступне:

– Сервер OpenVPN був налаштований у контейнеризованому середовищі на виділеному сервері.

– До VPN сервера підключилися клієнти з різних пристроїв (Windows, iOS, Android), щоб перевірити взаємодію з різними операційними системами та забезпечити навантаження на сервер.

– Використовувалися інструменти моніторингу для спостереження за роботою VPN сервера.

– Сервер OpenVPN працював протягом тривалого часу (кілька діб) без перезавантажень і втручань. Під час цього періоду клієнти регулярно підключалися та відключалися, а також передавали дані через VPN.

– Після завершення тестування були проаналізовані логи сервера для виявлення будь-яких перерв у роботі, помилок або зниження продуктивності.

Результати тестування наведено в таблиці 3.2.

Таблиця 3.2 – Результати тестування стабільності роботи

Параметр	Значення
Тривалість тестування	3 дні
Час автономної роботи	72 години (без перерв)

Продовження таблиці 3.2

Кількість відключень	0
Середній час відгуку (ping)	40 мс
Максимальний час відгуку (ping)	55 мс
Мінімальний час відгуку (ping)	35 мс

Тестування часу автономної роботи VPN сервера показало, що сервер OpenVPN у контейнеризованому середовищі є надійним і стабільним рішенням для забезпечення безперервного з'єднання. Сервер здатний працювати протягом тривалого часу без перерв, забезпечуючи високу якість з'єднання та захист даних. Це робить його ефективним інструментом для захисту конфіденційності даних і підтримки стабільного доступу до мережевих ресурсів.

Таким чином, інтеграція OpenVPN з контейнеризацією демонструє значні переваги та певні недоліки, які наведені в таблиці 3.3.

Таблиця 3.3 – Переваги та недоліки інтеграції OpenVPN і контейнеризації

Переваги	Недоліки	Вирішення недоліків
Ізоляція	Контейнери можуть споживати додаткові ресурси на сервері.	Оптимізація контейнерів та налаштування ресурсних обмежень.
Портативність	Налаштування мережевих політик та маршрутизації може бути складним.	Використання Docker Network Policies.
Масштабованість	Використання неконтрольованих Docker-образів може бути небезпечним.	Використання офіційних або перевірених Docker-образів, регулярні оновлення.

Продовження таблиці 3.3

Легка конфігурація та оновлення	Недостатній моніторинг може призвести до пропуску загроз.	Впровадження інструментів моніторингу та логування.
Швидкий запуск та ефективність	Контейнери можуть мати уразливості, які впливають на безпеку.	Регулярний аудит та оновлення контейнерів.
Доступність з будь-якого місця	Якщо OpenVPN налаштовано неправильно, IP-адреса клієнта може бути виявлена.	Використання VPN-шлюзу може допомогти приховати IP-адресу клієнта.

Інтеграція OpenVPN з контейнеризацією надає значні переваги в безпеці, портативності та масштабованості, роблячи це рішення ідеальним для сучасних динамічних мережевих середовищ. Попри деякі недоліки, такі як ресурсомісткість та складність налаштування, переваги значно переважають, роблячи контейнеризоване VPN рішення ефективним та надійним інструментом для захисту конфіденційних даних та забезпечення стабільного з'єднання.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Психофізіологічне розвантаження для працівників

У сучасному світі, де темп життя постійно зростає, а вимоги до працівників стають все вищими, питання збереження здоров'я та працездатності персоналу набуває особливої актуальності. Одним із ефективних методів вирішення цієї проблеми є психофізіологічне розвантаження.

Психофізіологічне розвантаження – це комплекс заходів, спрямованих на відновлення психофізіологічного стану працівників, зниження рівня їх втоми, підвищення працездатності та профілактику професійних захворювань. Це особливо актуально в умовах інтенсивної роботи, де високі навантаження можуть призводити до виснаження і професійного вигорання.

Психофізіологічне розвантаження допомагає працівникам впоратися зі стресом, підтримувати концентрацію та ефективність на роботі, а також покращують їх взаємовідносини з колегами. Ці методи включають фізичні активності, релаксаційні активності, психологічну методики. Нижче наведено кожен із цих методів детально.

Фізичні методи мають значний позитивний вплив на психофізіологічний стан працівників. Основні аспекти цих методик наведені в таблиці 4.1.

Таблиця 4.1 – Основні аспекти фізичної методики

Вид фізичної активності	Вплив на організм працівника
Біг, плавання, велосипедний спорт	Ці види активності сприяють вивільненню ендорфінів, які покращують настрій і знижують рівень стресу.
Танці та групові заняття	Залучають соціальну взаємодію, що також знижує рівень стресу та покращує психологічний стан.

Продовження таблиці 4.1

Важка атлетика, фітнес	Покращують фізичну силу та витривалість, підвищують самооцінку та загальне самопочуття.
Йога	Включає розтяжку та контроль дихання, що допомагає розслабити м'язи та знизити рівень кортизолу [17].

Релаксаційні методи є також важливим компонентом психофізіологічного розвантаження, допомагаючи зменшити стрес, покращити загальне самопочуття та відновити психофізіологічний баланс. Основні аспекти релаксаційних методів наведені в таблиці 4.2.

Таблиця 4.2 – Основні аспекти релаксаційної методики

Вид релаксаційної активності	Вплив на організм працівника
Медитація	Включає зосередження на диханні, мантрах або спокійних образах, що допомагає знизити тривожність і стрес [18].
Прогресивна м'язова релаксація (ПМР)	Практикується шляхом напруження та подальшого розслаблення різних груп м'язів, що допомагає зменшити фізичну напругу і зняти стрес [19].
Дихальні техніки	Зосереджені повільні, глибокі вдихи і видихи сприяють зниженню частоти серцевих скорочень і заспокоєнню нервової системи.

Психологічні методи є не менш важливими компонентами в управлінні стресом та забезпеченні психофізіологічного розвантаження для працівників. Основні аспекти цієї методики наведені в таблиці 4.3.

Таблиця 4.3 – Основні аспекти психологічних методів

Вид психологічної активності	Вплив на організм працівника
Індивідуальна та групова терапія	Надає можливість виразити свої почуття та отримати підтримку від професіонала або співрозмовників, сприяє розумінню власних емоцій.
Менторство та коучинг	Забезпечує особисту підтримку та розвиток навичок управління стресом та використання позитивних стратегій адаптації до навантажень.
Корпоративні програми підтримки	Сприяють створенню позитивної психологічної атмосфери в організації, підвищують свідомість працівників щодо їхнього психологічного здоров'я та навчають ефективним стратегіям управління стресом.

Психофізіологічне розвантаження для працівників відіграє ключову роль у забезпеченні їхнього психічного та фізичного благополуччя, а також підтримує продуктивність та ефективність на робочому місці. Застосування різноманітних методів, таких як фізичні вправи, релаксаційні техніки, психологічна підтримка та використання технічних засобів, сприяє зниженню рівня стресу, покращенню загального самопочуття та здоров'я працівників. Використання різноманітних підходів до психофізіологічного розвантаження створює можливості для працівників знайти та використовувати оптимальні стратегії для саморегуляції і

релаксації у різних ситуаціях. Це не лише сприяє покращенню їхнього психічного стану, але й підвищує загальний рівень задоволення від роботи та стимулює досягнення більш високих результатів у професійній діяльності.

4.2 Роль центральної нервової системи в трудовій діяльності людини

Центральна нервова система (ЦНС) — система органів людей та тварин, побудована з нервових клітин, яка координує функціонування та взаємозв'язок усіх інших органів та систем органів організму [20]. Вона має найголовніше значення в організмі людини, координуючи, регулюючи роботу всіх внутрішніх органів і здійснюючи зв'язок організму із зовнішнім середовищем [21]. Функції центральної нервової системи можна узагальнити наступним чином:

1. Регуляція та координація рухів. ЦНС контролює всі рухи тіла, необхідні для виконання роботи, від дрібної моторики пальців до складних координаційних рухів. Вона регулює м'язовий тонус, силу та швидкість м'язових скорочень, а також плавність та точність рухів. Завдяки ЦНС людина може адаптувати свої рухи до мінливих умов праці та виконувати складні завдання з високою точністю.

2. Сприйняття інформації. ЦНС отримує інформацію з органів чуття (зір, слух, дотик, нюх, смак), обробляє її та формує уявлення про навколишнє середовище. Ця інформація використовується для прийняття рішень, контролю за виконанням роботи та попередження помилок. Чим краще розвинені органи чуття та увага людини, тим швидше та точніше вона може реагувати на зміни в робочому середовищі.

3. Пам'ять та мислення. ЦНС зберігає інформацію про попередній досвід роботи, навички та знання, які необхідні для виконання трудових завдань. Вона використовує цю інформацію для прийняття рішень, планування дій та вирішення проблем. Здатність до навчання та запам'ятовування нової інформації є важливим фактором успішної трудової діяльності.

4. Емоції та мотивація. ЦНС регулює емоційний стан людини, який може впливати на її працездатність та продуктивність. Позитивні емоції, такі як

задоволення від роботи та почуття власної значущості, можуть стимулювати людину до більш активної та результативної роботи. Негативні емоції, такі як стрес, тривога та втома, можуть призводити до зниження працездатності та погіршення якості роботи.

5. Адаптація до мінливих умов. ЦНС допомагає людині адаптуватися до мінливих умов праці, таких як фізичне навантаження, шум, вібрація та інші фактори. Вона регулює роботу серцево-судинної, дихальної та інших систем організму, забезпечуючи їх оптимальне функціонування в умовах праці.

6. Формування трудових навичок. ЦНС відіграє важливу роль у формуванні трудових навичок, таких як координація рухів, увага, пам'ять, мислення та інші. Ці навички розвиваються в процесі навчання та роботи, і їх рівень визначає успішність людини в трудовій діяльності.

7. Захист від шкідливих факторів. ЦНС активує захисні механізми організму у відповідь на шкідливі фактори виробничого середовища, такі як токсичні речовини, пил, шум та інші. Це допомагає запобігти розвитку професійних захворювань та травм.

Під час тривалої або інтенсивної роботи ЦНС може втомлюватися. Це може призводити до зниження концентрації уваги, погіршення пам'яті, уповільнення реакції та інших проблем, які негативно впливають на результати роботи. Для того, щоб запобігти перевтомі центральної нервової системи, рекомендується: робити регулярні перерви в роботі, дотримуватися режиму дня та сну, правильно харчуватися, займатися спортом та уникати стресових ситуацій.

Центральна нервова система (ЦНС) є фундаментальною для функціонування організму людини, відіграючи низку важливих ролей у трудовій діяльності. Вона координує рухи тіла, сприймає та обробляє інформацію, керує пам'яттю та мисленням, регулює емоційний стан та мотивацію, а також допомагає адаптуватися до змін у робочому середовищі. Таким чином, ЦНС є невід'ємною частиною успішної трудової діяльності та загального благополуччя людини.

ВИСНОВКИ

У результаті проведеного дослідження та практичної реалізації досягнуто мету кваліфікаційної роботи – впровадження OpenVPN для забезпечення конфіденційності даних у контейнеризованому середовищі. У процесі роботи було виконано наступні ключові завдання:

1. Аналіз сучасних викликів у галузі забезпечення конфіденційності даних:

– Визначено основні загрози безпеці даних у сучасному інформаційному суспільстві.

– Розглянуто роль конфіденційності у функціонуванні інформаційних систем та важливість її забезпечення.

2. Огляд особливостей OpenVPN та контейнеризації:

– Проведено детальний аналіз можливостей OpenVPN як засобу забезпечення безпеки мережевих з'єднань.

– Оцінено переваги контейнеризації для ізоляції додатків та забезпечення безпеки даних.

– Проведено порівняння різних Docker-образів з OpenVPN сервером та вибрано оптимальний варіант для впровадження.

3. Практична реалізація:

– Встановлено та налаштовано Docker.

– Розгорнуто OpenVPN сервер у контейнеризованому середовищі та налаштовано відповідний Docker-образ.

– Проведено тестування роботи OpenVPN сервера, включаючи встановлення клієнтських програм на Windows, iOS та Android, і перевірку безпеки даних під час передачі.

Завдяки впровадженню OpenVPN у контейнеризованому середовищі було досягнуто високого рівня конфіденційності та безпеки даних. Тестування показало, що трафік успішно шифрується, а з'єднання забезпечує належний захист від потенційних загроз. Це підтверджує доцільність використання

OpenVPN разом із контейнеризацією як ефективного рішення для забезпечення кібербезпеки в сучасних інформаційних системах.

Актуальність даної роботи підкреслюється постійним розвитком технологій та необхідністю захисту інформації в умовах збільшення обсягів цифрових даних та транзакцій. Використання OpenVPN у поєднанні з контейнеризацією не тільки забезпечує надійний захист даних, але й підвищує гнучкість та масштабованість інформаційних систем.

Отримані результати можуть бути використані для подальших досліджень і розробок у сфері кібербезпеки, а також для впровадження в корпоративних мережах для захисту конфіденційних даних. Застосування розглянутих методів і технологій дозволяє створювати більш безпечні та стійкі до атак інформаційні системи, що є важливим кроком у напрямку підвищення загальної безпеки в цифровому світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Учасники проектів Вікімедіа. Конфіденційність – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Конфіденційність (Дата доступу: 23.02.2024).

2. Information Security | Confidentiality - GeeksforGeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/information-security-confidentiality/ (Дата доступу: 23.02.2024).

3. Учасники проектів Вікімедіа. WannaCry – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/WannaCry (Дата доступу: 24.02.2024).

4. Учасники проектів Вікімедіа. Кібератака на Dyn – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Кібератака_на_Dyn (Дата доступу: 24.02.2024).

5. MediaSapiens. Gmail повідомив про фішингову розсилку, замасковану під Google Docs. ms.detector.media. URL: https://ms.detector.media/it-kompanii/post/18852/2017-05-04-gmail-povidomyv-pro-fishyngovu-rozsylku-zamaskovanu-pid-google-docs/ (Дата доступу: 24.02.2024).

6. Учасники проектів Вікімедіа. KRACK – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/KRACK (Дата доступу: 26.02.2024).

7. 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

8. Contributors to Wikimedia projects. OpenVPN - Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/OpenVPN (Дата доступу: 05.03.2024).

9. OpenVPN Access Server Advantages | OpenVPN. OpenVPN. URL: https://openvpn.net/advantages/ (Дата доступу: 06.03.2024).

10. 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 URL: https://doi.org/10.62731/mcnd-14.06.2024.004 (Дата доступу: 15.06.2024).

11. Adetunji D. How Docker Containers Work – Explained for Beginners. freeCodeCamp.org. URL: https://www.freecodecamp.org/news/how-docker-containers-work/ (Дата доступу: 06.03.2024).

12. linuxserver/openvpn-as. Docker Hub. URL: https://hub.docker.com/r/linuxserver/openvpn-as (Дата доступу: 09.03.2024).

13. kylemanna/openvpn. Docker Hub. URL: https://hub.docker.com/r/kylemanna/openvpn (Дата доступу: 09.03.2024).

14. openvpn/openvpn-as. Docker Hub. URL: https://hub.docker.com/r/openvpn/openvpn-as (Дата доступу: 09.03.2024).

15. Український SPEEDTEST - Тест швидкості Інтернет з'єднання. URL: SPEEDTEST. https://speedtest.net.ua/ua (Дата доступу: 04.04.2024).

16. Тест швидкості Інтернет з`єднання | 2IP.ua. 2IP.ua. URL: https://2ip.ua/ua/services/ip-service/speedtest (Дата доступу: 04.04.2024).

17. 6 фактів про користь йоги для здоров'я. Міністерство охорони здоров'я України. URL: https://moz.gov.ua/article/health/6-faktiv-pro-korist-jogi-dlja-zdorovja (Дата доступу: 04.05.2024).

18. Медитація корисна для вашого здоров'я. Медична та наукова платформа. Лекції, статті, зустрічі з успішними особистостями. | INgenius. URL: https://ingeniusua.org/articles/medytatsiya-korysna-dlya-vashoho-zdorovya (Дата доступу: 04.05.2024).

19. Прогресивна м’язова релаксація за Джейкобсоном: проста методика проти стресу та тривожності – Be calm. URL: https://becalm.com.ua/body/progresyvna-m-yazova-relaksatsiya-za-dzhejkobsonom-prosta-metodyka-proty-stresu-ta-tryvozhnosti/ (Дата доступу: 07.05.2024).

20. Учасники проектів Вікімедіа. Центральна нервова система – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Центральна_нервова_система (Дата доступу: 07.05.2024).

21. Роль центральної нервової системи в трудовій діяльності людини. Бібліотека економіста. URL: https://library.if.ua/book/9/920.html (Дата доступу: 10.05.2024).