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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему:: «Проект підсистеми захисту мережі з використанням технології OpenVPN»

Виконав студент 4-го курсу групи КБ-19-2
спеціальності 125 «Кібербезпека»
_____ Владислав Вовк
Керівник, старший викладач кафедри КІ та КБ
_____ Єлизавета Байлюк
Рецензент, старший викладач кафедри КІ та КБ
_____ Олександра Покотило

Житомир – 2023

Державний університет «Житомирська політехніка»

Факультет інформаційно-комп'ютерних технологій

Кафедра комп'ютерної інженерії та кібербезпеки

Спеціальність 125 «Кібербезпека»

Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

Андрій Єфіменко

1 березня 2023 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу бакалавра

Студент: Вовк Владислав Олександрович

Тема роботи: «Проєкт підсистеми захисту мережі з використанням технології OpenVPN»

затверджена Наказом університету від 1 березня 2023 р. № 99/с

Термін здачі студентом закінченої роботи 26 червня 2023 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження): Об'єктом дослідження є процес проектування підсистеми захисту мережі з використанням технології OpenVPN. Предметом дослідження є технологія проектування підсистеми захисту мережі з використанням технології протоколу OpenVPN

Обладнання та програмне забезпечення:

1. Мережевий емулятор EVE NG
2. маршрутизатор Cisco 800 Integrated Services Routers
3. комутатор Cisco 2960

4. операційна система Sierra macOS
5. операційна система Windows 10
6. операційна система Kali Linux
7. OpenVPN connect v.2.5.6

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Байлюк Є.М.	25.03.2023	25.03.2023
2	Єфіменко А.А	17.04.2023	17.04.2023
3	Байлюк Є.М	9.05.2023	9.05.2023

Студент _____ Владислав Вовк

Керівник _____ Єлизавета Байлюк

АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра являє собою проект підсистеми захисту мережі з використанням технології OpenVPN.

Мета і завдання роботи. Метою роботи є проектування підсистеми захисту мережі з використанням технології OpenVPN.

Досягнення поставленої мети передбачає розв'язання наступних завдань:

1. Проведення аналізу поняття VPN, його архітектури та принципів роботи.

2. Аналіз наявних технологій VPN, зокрема аналіз OpenVPN як провідного протоколу.

3. Розробка корпоративної мережі інфраструктури на базі технологій OpenVPN.

4. Проведення тестування на проникнення та розробка правил безпеки на основі результатів цього тестування.

5. Перевірка ефективності створених правил шляхом повторного тестування, та створення рекомендацій для покращення підсистеми захисту.

Об'єктом дослідження є процес проектування підсистеми захисту мережі з використанням технології OpenVPN.

Предметом дослідження є технологія проектування підсистеми захисту мережі з використанням технології OpenVPN.

Пояснювальна записка до випускної кваліфікаційної роботи містить в собі 96 сторінок, 7 таблиць та 147 рисунків. Список використаних джерел містить 22 найменування і займає 3 сторінки.

Ключові слова: АУТЕНТИФІКАЦІЯ, ІНТЕГРАЦІЯ, КЛЮЧ, ТУНЕЛЮВАННЯ, ШИФРУВАННЯ.

					Державний університет "Житомирська політехніка" КБ.КР.Б – 125 – 03 – ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Вовк В.О		20.06.23	Проєкт підсистеми захисту мережі з використанням технології OpenVPN	Літ.	Арк. 5 / Аркушів 97
Керівник		Байлюк Е.М.		20.06			
Реценз.		Покотило О.А		20.06		ФІКТ, Гр. КБ-19-2	
Н. контр.		Колощук М.С		20.06			
Затверд.		Ефіменко А.А		20.06.23			

`

ANNOTATION

The bachelor's thesis is a project of a network security subsystem using OpenVPN technology.

The purpose and objectives of the work. The aim of the work is to design a network security subsystem using OpenVPN technology.

Achieving this goal involves solving the following tasks:

1. Analyzing the concept of VPN, its architecture and principles of operation.

2. Analysis of existing VPN technologies, including analysis of OpenVPN as a leading protocol.

3. Development of a corporate network infrastructure based on OpenVPN technologies.

4. Conducting penetration testing and developing security rules based on the results of this testing.

5. Verification of the effectiveness of the created rules through repeated testing, and creation of recommendations for improving the security subsystem.

The object of research is the process of designing a network security subsystem using OpenVPN technology.

The subject of research is the technology of designing a network security subsystem using OpenVPN technology.

Explanatory note to the final qualification work contains 96 pages, 7 tables and 147 figures. The list of references includes 22 items and occupies 3 pages.

Keywords: AUTHENTICATION, ENCRYPTION, INTEGRATION, KEY, TUNNELING.

`

ЗМІСТ

ВСТУП 9
РОЗДІЛ 1 ОГЛЯД ОСНОВНИХ ПРИНЦИПІВ РОБОТИ ТЕХНОЛОГІЇ VPN .. 11
1.1 Загальний огляд технології VPN: принципи роботи, архітектура, переваги та недоліки. 11
1.2 Алгоритми шифрування та хешування технологій VPN 13
1.3 Дослідження відомих протоколів VPN 19
1.4 Обгрунтування вибору протоколу OpenVPN 29
1.5 Висновки до першого розділу 30
РОЗДІЛ 2 ПРОЕКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ МЕРЕЖІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ OPENVPN 31
2.1 Алгоритми роботи, архітектура та загальна структура системи 31
2.2 Вибір мережевого обладнання, побудова та налаштування мережі 38
2.3 Розгортання VPNaaS на базі OpenVPN Conneхa та Google Cloud 50
2.4 Моделювання загроз мережі на базі протоколу OpenVPN 57
Висновки до другого розділу 64
РОЗДІЛ 3 НАЛАШТУВАННЯ, ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ ТА ЗАХИЩЕНОСТІ МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЇ OPENVPN 65
3.1 Налаштування OpenVPN сервера на операційній системі Windows 65
3.2 Перевірка працездатності мережі та роботи OpenVPN сервера 73
3.3Тестування мережі на проникнення 84
Висновки до третього розділу 91
ВИСНОВКИ 92
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 93
ДОДАТКИ 96

`

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

1. VPN - Virtual Private Network
2. IP - Internet Protocol
3. TCP - Transmission Control Protocol
4. UDP - User Datagram Protocol
5. SSL - Secure Sockets Layer
6. TLS - Transport Layer Security
7. PPTP - Point-to-Point Tunneling Protocol
8. L2TP - Layer 2 Tunneling Protocol
9. IKE - Internet Key Exchange
10. IPSec - Internet Protocol Security
11. SSTP - Secure Socket Tunneling Protocol
12. DNS - Domain Name System
13. NAT - Network Address Translation
14. VPNaaS - VPN as a Service
15. MPLS - Multiprotocol Label Switching
16. CPE - Customer Premises Equipment
17. VPN Client - Virtual Private Network Client
18. VPN Server - Virtual Private Network Server
19. VPN Gateway - Virtual Private Network Gateway
20. VPN Concentrator - Virtual Private Network Concentrator

`

ВСТУП

Актуальність теми. В сучасному світі актуальність сервісів VPN стає все більше необхідною, через зростання кількості атак на мережеві системи, та звичайних користувачів. Порушення конфіденційності в кіберпросторі завдає колосальних збитків не тільки серед пересічних користувачів, але і мережевих гігантів.

Використовуючи технологію VPN можна захистити себе та свої конфіденційні дані від несанкціонованого втручання, вона дозволяє забезпечити безпеку транзакцій, обійти блокування ресурсів та створити захищений канал для користування у громадських мережах Wi-Fi.

Для корпоративного сегмента технологія VPN є головною для передачі важливої інформації, розголошення якої може нанести збитки та репутаційну шкоду. Для забезпечення захисту віддалених користувачів використання VPN з'єднання є обов'язковою складовою захисту від перехоплення даних, а також для забезпечення доступу до локальних даних компанії з меншим ризиком зловживання правами доступу. Використання технологій шифрування збільшують криптостійкість системи, та даних які передають захищеним каналом від перехоплення.

В період пандемії та постійних кібератак з боку злочинців, використання технології VPN є актуальним, воно забезпечує захист даних, між різними відділами, працівником та роботодавцем, і може застосовувати й для забезпечення конфіденційності персональних даних як звичайних громадян, так і корпорацій.

Метою кваліфікаційної роботи є реалізація комплексної системи захисту мережі з використанням технології OpenVPN.

Визначена мета обумовлює наступні завдання:

1. Створення надійного та безпечного доступу локальних ресурсів користувачів.

2. Забезпечення захисту персональних даних, та конфіденційної інформації.

`

3. Забезпечення цілісності та доступності й шифруванню даних, які передаються мережею.

Об’єктом дослідження є проект підсистеми захисту мережі з використанням технології OpenVPN. В ході виконаної роботи було розглянуто широкий спектр застосування технології OpenVPN, встановлення та налаштування фаєрвола, розробка контролю доступу, та вибір налаштувань сервера, розробка стратегії захисту мережі організації від несанкціонованого доступу.

Предметом дослідження є проект підсистеми захисту мережі з використанням технології OpenVPN, який є головним функціональним компонентом. Створення та реалізація стабільно та захищеної мережевої інфраструктури, їх налаштування та управління OpenVPN. Аналіз ефективності та їх надійності для реалізації й застосування OpenVPN для кращої кібербезпеки в інформаційному просторі.

У процесі виконання кваліфікаційної роботи було розроблено проект підсистеми захисту мережі з використанням технології OpenVPN, яка забезпечує шифрування та передавання даних по захищених каналах між користувачами, їх авторизацію в мережі. Розроблено політики безпеки фаєрволу для збільшення надійності та захищеності системи, від несанкціонованого доступу із зовнішньої мережі інтернет.

`

РОЗДІЛ 1 ОГЛЯД ОСНОВНИХ ПРИНЦИПІВ РОБОТИ ТЕХНОЛОГІЇ VPN

1.1 Загальний огляд технології VPN: принципи роботи, архітектура, переваги та недоліки.

VPN це віртуальна приватна мережа, технологія якої забезпечує конфіденційність та безпеку при користуванні інтернетом, та передачі даних в ньому[1].

VPN шифрує ваші дані за певним протоколом, та передають вже зашифровану інформацію на сервер через тунель. Ці дії забезпечують захищений канал, який оберігає дані від кібератак. VPN використовують для захисту персональних даних та конфіденційної інформації від несанкціонованого доступу.

VPN дозволяє отримувати доступ до заблокованих сайтів в інтернеті, обходячи блокування у чинній країні, та забезпечити анонімність дій користувача.

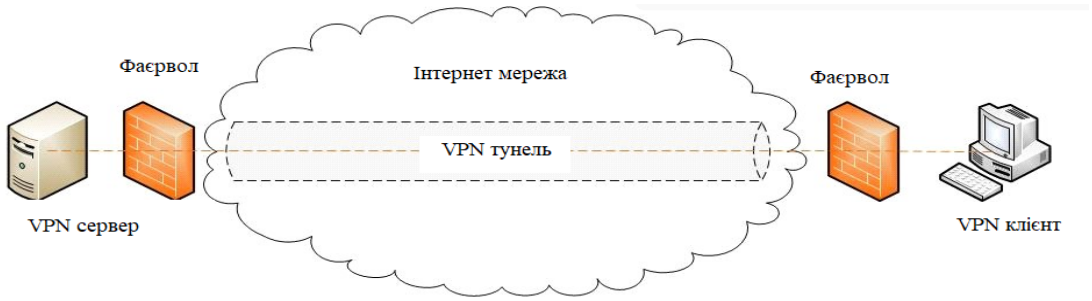


Рисунок 1.1 - Схема роботи технології VPN

За ідею роботи взято створення тунелю між двома станціями. Тунель - це захищене з’єднання зашифрованих даних, яке захищає потік даних від перехоплення, та від потрапляння до третіх осіб[2].

Тунелювання відбувається шляхом створення захищеного каналу, який прокладається між двома вузлами зв’язку за допомогою технологій шифрування, автентифікації, та іншого криптологічного захисту для надійного захисту інформації у мережі. Користувач шифрує дані, та відправляє їх по захищеному тунелю на сервер, який має відповідні ключі та розшифровує, і вже відправляє кінцевому користувачу.

`

Створення захищеного тунелю дозволяє користувачу отримати доступ до ресурсів зі всього світу, та обійти обмеження які чинні у даній країні. Для цього достатньо приєднатися до VPN сервера в іншій країні, та користуватися його IP адресою і ви вже автоматично будете користувачем іншого сегменту інтернету.

Використання тунелів має і ряд обмежень, які можуть викликати певні труднощі при використанні, та зменшити ваші можливості. Зменшення пропускної здатності каналу, може впливати на швидкість передачі даних, через обмеження сервера, та постійне шифрування даних, яке буде давати навантаження на мережу. Створення тунелю процес не з важких, але відсутність досвіду у користувачів може відштовхнути їх від роботи з VPN. Через велику кількість стандартів та протоколів VPN, не завжди можна розраховувати на кросплатформеність вашого сервера, і VPN з'єднання між вашим комп'ютером та телефоном може не відбутися[3].

Режими роботи VPN:

Режим маршрутизації - в цьому режимі дані користувача маршрутизуються в захищеному з'єднанні між сервером та клієнтом. Під'єднані користувачі отримують доступ до локальних ресурсів мережі, які знаходячись за межами локальної мережі.

У даному режимі клієнт використовує таблицю маршрутизації для побудови шляху передачі даних через тунель. В цьому режимі можна більш гнучко налаштувати мережу, та підключатися до мереж з різними адресами IP та отримувати доступ до підмереж, що розташовані за його межами, і з'єднання між різними клієнтами. Використання протоколу маршрутизації дає можливість вибрати кращий маршрут для передачі даних між різними підмережами.

Режим мосту - об'єднання двох локальних мереж в одну і створення одного сегменту мережі. В режимі мосту трафік передається на канальному рівні, а не на мережевому. Використання мосту потрібне для пристроїв зі статичним IP де не можливо, або проблематично змінити адрес.

Повне тунелювання - режим роботи в якому повний обсяг трафіку проходить від клієнта до сервера через тунель. В цьому режимі всі ваші дані, які

`

ви відправляєте будуть відправлені спочатку на VPN сервер, а він вже відправить його за адресою. В цьому режимі забезпечено найбільший рівень безпеки для користувачів, які користуються публічними мережами, і хочуть отримати захист від крадіжки даних. Повне тунелювання дозволяє контролювати та обмежувати за потреби весь трафік в мережі, і розмежовувати права доступу до певних серверів та сайтів.

Роздільне тунелювання - метод маршрутизації трафіку в мережі VPN, при якому вибирається який трафік буде проходити через VPN сервер, а який буде на пряму виходити в мережу інтернет.

1.2 Алгоритми шифрування та хешування технологій VPN

Для забезпечення захисту даних при передачі тунелем технології VPN використовують різні алгоритми шифрування. Основними алгоритмами шифрування є: Симетричне шифрування, асиметричне, та хешування.

Симетричне шифрування - використовує один ключ як для шифрування даних, та і дешифрування даних. Алгоритм роботи даного шифрування виконується в декілька етапів, які пов’язані між собою. Першим кроком є генерація ключа шифрування, який буде відомий тільки серверу та клієнту, ним буде зашифровано повідомлення відправником, а вже отримувач знаючи ключ розшифрує отримане повідомлення. Всі дані перед відправленням розбиваються на блоки та шифруються в залежності від алгоритму шифрування. Потім ці дані відправляються в зашифрованому вигляді по захищеному каналу, де в автоматичному режимі отримує розшифровану інформацію[4].

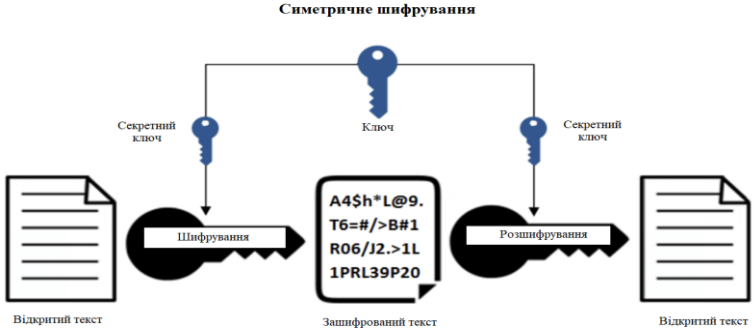


Рисунок 1.2 - алгоритм роботи симетричного шифрування

`

AES - симетричний алгоритм шифрування який використовують для захисту інформацію, включаючи у VPN. AES є потужним та надійним алгоритмом захисту, що використовується і на даний час[5].

Даний алгоритм має велику кількість режимів які можна використовувати для шифрування даних. В режимі блокового шифрування дані розбивають на блоки певної довжини у бітах, і кожен блок шифрують використовуючи спеціальний ключ до кожного блоку окремо, що дозволяє шифрувати дані в режимі реального часу.

Алгоритм застосовує ключі шифрування для створення таблиці змінної, яка перетворює значення в байтах та інші значення, для підвищення надійності. Далі використовується зсув рядка, і змішування колонок, для підвищення стійкості, а також перестановка і змішування бітів блоку.

Перевагою даного алгоритму є його швидкодія та простота, швидкодія шифрування у реальному часі дає змогу передавати інформацію без затримок, що є важливою у даному часі, а простота реалізації та надійності робить його привабливим для підтримки, і забезпечує його кросплатформеність.[22]

Перевагами симетричного шифрування є його швидкодія в порівнянні з асиметричним. Використання меншої кількості ресурсів які залучені для шифрування робить його зручним для роботи з великими об’ємами даних, оскільки споживає менше ресурсів. Простота шифрування шляхом в декілька етапів робить його простим в реалізації та використанні. Широкий спектр застосування та підтримки робить симетричне шифрування зручним та надійним у використанні для широкого загалу не досвідчених користувачів[6].

Симетричний ключ є як і головною перевагою даного алгоритму, так і головною проблемою. Забезпечення захищеної передачі ключа є головною задачею даного шифрування через те, що перехоплений ключ відкриває доступ до всіх зашифрованих даних. Керування великою кількістю користувачів створює велику кількість ключів які потрібно зберігати, та керувати ними, що робить захист їх ще важчими. Використання коротких ключів дозволяє зловмисникам отримати доступ до даних шляхом брутфорсу паролів. Чим

`

довший ключ, тим більше потрібно часу та ресурсів для підбору паролів, тому потрібно вибирати шифрування з високою бітністю.

Асиметричне шифрування - шифрування даних з використанням метода відкритих ключів. Для роботи потрібно мати відкритий та закритий ключі які між собою пов’язані, і потрібні для шифрування та дешифрування даних.

Використання публічного ключа в асиметричному шифруванні відбувається відкрито, і доступ до нього може отримувати будь-хто, а приватний ключ є секретним і має бути не наголошеним. Дані зашифровані відкритим ключем можуть бути розшифровані тільки приватним ключем, і тому тільки власник публічного ключа може їх отримати.

Асиметричне шифрування можна використовувати як цифровий підпис, і вже отримувач може за допомогою свого ключа перевірити автентичність повідомлення.

Використання публічного ключа є доволі простим, і його можна розповсюджувати у відкритому доступі, і не мати для себе ніяких наслідків. Приватний ключ має зберігатися в надійному місці й не розголошуватися так, які він є головним для розшифрування даних, так перевірки їх автентичності.

Після шифрування даних їх можна передавати навіть по не захищеному каналу без страху перехоплення даних чи відкритого ключа. Для перевірки автентичності даних можна використати його і для цифрового підпису і перевіряти достовірність зашифрованого повідомлення.

Здатність до обчислення асиметрично шифрування є складнішою, і більш витратно чим симетричне через використання математичних операцій з бітовою послідовністю і це створює велике навантаження на обчислювальні ресурси системи.

Для злому даного шифру потрібно використовувати великі обчислювальні потужності, які є тільки у квантових комп'ютерів які можуть здійснювати колосальні обчислення та шляхом підбору можуть знайти ключ від зашифрованого повідомлення.

`

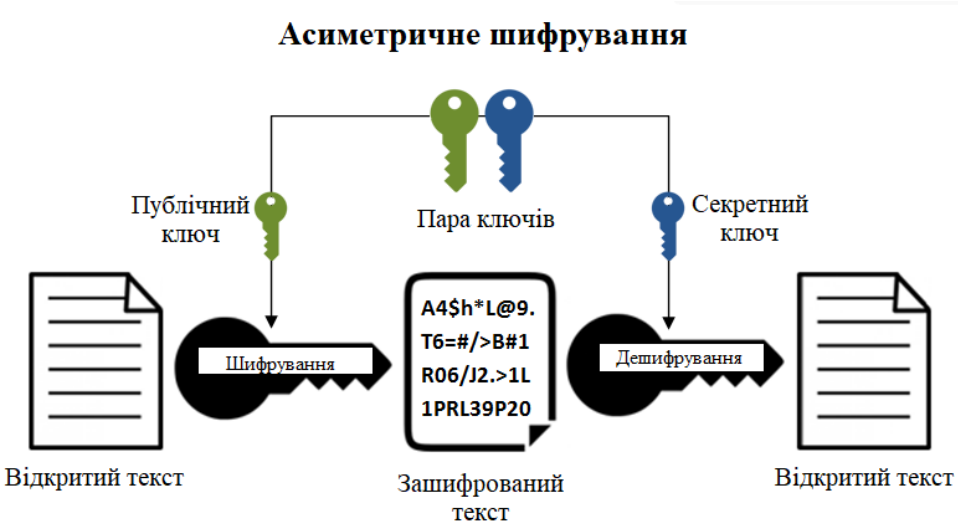


Рисунок 1.3 - Алгоритм асиметричного шифрування

Типи симетричного шифрування:

RSA - алгоритм асиметричного шифрування, в основі якого лежать математичні принципи факторизації великих простих чисел.

Алгоритм генерує пару ключів. Публічний ключ відповідає за шифрування, а приватний за розшифрування. Ключі пов'язані між собою і тому зашифровані дані публічним ключем, можуть бути розшифровані тільки відповідним приватним ключем, і навпаки, дані які були підписані приватним ключем, перевіряються приватним ключем[7].

Стійкість даного алгоритму підтримується шляхом факторизації великих простих чисел і захищає від злому. Система асиметричних ключів захищає від перехоплення секретного ключа, оскільки для розшифрування потрібен приватний ключ, який не передається в мережі, а зберігається в адресата. Використання RSA для цифрового підпису є надійним та захищеним методом для підтвердження автентичності даних після надсилання в мережі.

За роки свого існування RSA завоював велику базу прихильників та підтримки на різних платформах та областях застосування від захищених повідомлень, до VPN сервісів. Обчислювальна ефективність даного шифрування чудово підходять для передачі коротких повідомлень, але він не обмежений у розмірах повідомлень, і може використовуватися і для великих об'ємів даних. Використання апаратного прискорення допоможе здійснити швидку обробку

`

даних на пристроях де є інтегрована система RSA, оскільки даний алгоритм широко використовується він є один зі стандартів криптографічного захисту.

Через складність шифрування та роботу з великим об’ємом даних RSA є вимогливим до ресурсів системи. Великий розмір ключів вимагає більший об’єм пам'яті, та генерує великий об’єм інформації та витрат на обчислення. Через великий розмір ключа швидкість підписання та перевірки дійсності збільшує навантаження на систему і викликає проблеми при підписі великої кількості повідомлень. Відсутність прямого обміну ключів вимушує сторони обмінюватися відкритими ключами між собою, а свої приватні ключі зберігати, бо його втрата загрожує всім даним.

Перевагами асиметричного шифрування є його безпека, та легкість в передаванні ключів. Ключ в симетричному шифруванні потрібно передавати по захищеному каналу, і в разі втрати його всі дані будуть скомпрометовано, а в асиметричному алгоритмі публічний ключ може бути розповсюджений в будь-який спосіб, і без секретного не несе ніякої загрози.

Більше надійності створює більший об’єм даних, який створює велике навантаження на систему, і потребує більше ресурсів для обчислення. Великий обсяг даних робиться ще більшим, а при роботі з обмеженими ресурсами це неможливо. Використання публічних ключів це добре, але при роботі з великою кількістю користувачів постає питання про менеджмент ключів та їх обліку й управлінню. Поява квантових комп'ютерів ставить під загрозу надійність асиметричного шифрування, та підштовхує до створення більш надійного захисту інформації, та надійних алгоритмів.

В технологіях VPN перевірку цілісності даних виконує хеш-функція та контрольна сума. Дані які передають в пакетах отримують певні заголовки, які потім звіряються, та робляться висновки до їх автентичності.

Дані розбиваються на блоки чи пакети, і їх обробляють хеш-функцією SHA-256 чи MD5, після цього перетворюються в хешоване повідомлення унікальної побітової послідовності. Хеш-функція обчислює вихідні хешовані дані за допомогою внутрішніх алгоритмів і генерує хеш-код фіксованої довжини.

`

Побітова послідовність даних є унікальною, і при зміні навіть одного елемента змінює її зміст, і створює новий унікальний хеш, який не відповідає першому.



Рисунок 1.4 - алгоритм роботи хеш-функції

SHA-2 – хеш-функція яка генерує хеш фіксованої довжини 224, 256, 384, 512 біт. При використанні фіксованого хешу, довжина вихідних даних завжди буде однакова. Дана хеш-функція є криптографічно стійкою до колізій і не піддається математичним обчисленням. Незворотний механізм хешування забезпечує надійний захист від зміни даних, і при спробі здійснити несанкціоновані дії процес буде не зворотній. Протокол має блискавичну швидкодію, і має широке застосування. Простота та надійність робить дане хешування розповсюдженим та використовується з такими протоколами як SSL/TLS, IPSec, PGP[8].

Хешування даних є надійним, але використання великих обчислювальних потужностей можуть методом колізій хеш-функцій підібрати правильну послідовність даних, та зменшити вашу криптостійкість. Широке використання функцій дає і ширший потенціал і для злочинців які постійно шукають вразливі місця у вашій системі. Використання довіреності сторони постійно потребує підтвердження надійності обох сторін, і перевірку автентичності.

Після генерації блоків інформації до кожного з них додається заголовок який містить контрольну хеш-суму, яка звіряється хешуванням для перевірки автентичності даних.

MD5 - популярний алгоритм хешування для роботи зі 128 бітної хеш-суми для безпеки мережі та цифрового підпису.

`

На даний час алгоритм не вважається надійним та не створює надійні умови захисту інформації. Хешування вразливе до колізій, що робить його вразливим до обробки інформації, використання атак на розширення та побічних каналів, що робить його непридатним для захисту інформації.

1.3 Дослідження відомих протоколів VPN

PPTP - протокол для створення віртуальної приватної мережі, який дозволяє об’єднувати декілька локальних мереж в інтернеті. Протокол створює тунель між двома станціями, та зашифровує дані для передачі. Забезпечення конфіденційності відбувається криптологічними методами шляхом шифрування даних у захищеному тунелі, в протоколі присутні механізми автентифікації для підтвердження автентичності користувачів мережі.

Налаштування PPTP простий в налаштуванні, який дозволяє з легкістю налаштувати тунелі між користувачами, та гнучко їх налаштувати. Для налаштування достатньо зробити записи в конфігураційних файлах і менеджерах налаштувань на клієнті та сервері. Багато операційних систем мають підтримку протоколу, що полегшує нам роботу.

Поширеність даного протоколу та підтримка зробила його привабливим для користувачів. Підтримка на різних операційних системах дозволяє створювати кросплатформені з’єднання що було зручно для використання. Підтримка поширених стандартів дозволяло комбінувати його зі стандартним мережевим обладнанням, та без особливих часових та матеріальних затрат зробити свій VPN сервер

IPSec - група протоколів та набір функцій, що забезпечує захист мережевих комунікацій на протокольному рівні IP. Протокол забезпечує конфіденційність, цілісність та аутентифікацію даних при передачі в мережі.

Протокол працює на рівні мережевого стека з використанням IPv4 та IPv6, що дозволяє захищати мережеві комунікації на рівні IP[9].

Основними компонентами IPSec є AH протокол який використовується для автентифікації та цілісності даних, при передачі даних через протокол всі

`

пакети отримують заголовки з певною інформацією для перевірки на автентичність.

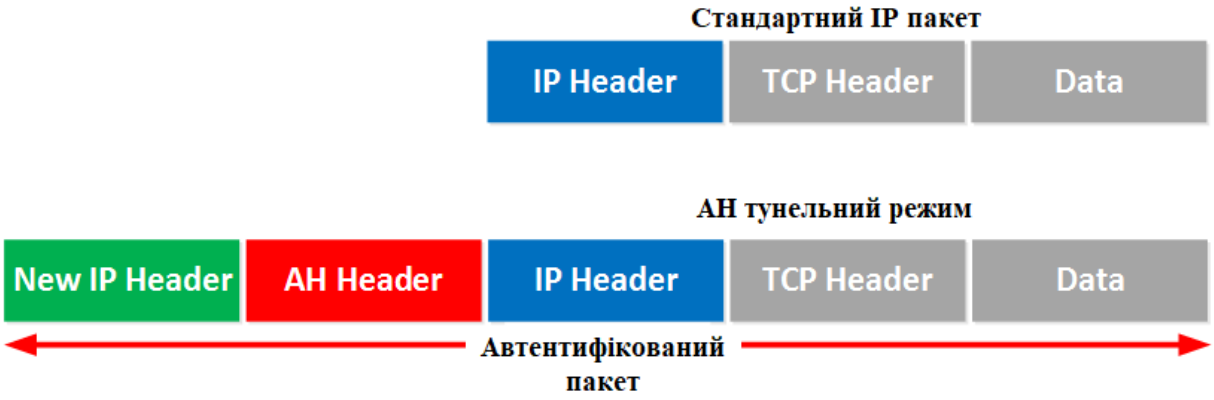


Рисунок 1.5 - Вигляд пакету IPSec

Надійні механізми захисту та аутентифікації забезпечують цілісність та автентичність, і робить його ефективним для захисту конфіденційної інформації. Налаштування IPSec досить гнучке, та може бути налаштоване в залежності від рівня захисту який вимагається, і від рівня інфраструктури. Шифрування всього трафіку мережі та створення захищеного з'єднання гарантують конфіденційність та безпеку. Кросплатформеність та стандартизація протоколу дозволяє працювати в різних мережах та операційних системах без ризику створення конфліктних. Гнучкість та надійність забезпечили протоколу широку популярність, та підтримку користувачів на великій кількості платформ, що робить його незамінним у корпоративній інфраструктурі, хмарному середовищі, та у технологіях VPN.

L2TP/IPSec - протокол тунелювання, який шифрує дані між двома вузлами робочих станцій та створює захищений зв’язок. L2TP еволюціонував від PPTP і L2F протоколів. Для маршрутизації протокол використовує UPD та IP протоколи для передачі даних.

Протокол L2TP використовується для створення безпечного підключення до мережі й підтримання належного рівня конфіденційності та захищеності при передачі даних у відкритій мережі. Захищає від перехоплення даних, та створює безпечне та захищене віддалене з’єднання.

`

За допомогою протоколу шифрування IPSec забезпечується надійний та стабільний рівень захисту. L2TP забезпечує стабільний тунель на рівні каналу, з підтримкою автентифікації з допомогою паролю, сертифікату та токену для входу.

Великою перевагою протоколу є його можливість працювати з мережевим екраном, для роботи з сервером по порту 1701 UPD. Кросплатформеність даного протоколу дозволяє з’єднувати велику кількість пристроїв та мережевого обладнання, і працювати з ними.

SSTP - протокол VPN, який створює захищене з’єднання між двома станціями з використанням протоколу шифрування SSL/TLS, який є розробкою Microsoft. В більшості випадків використовується на операційній системі Windows з використання порту 443, що дає йому доступ до мережевих екранів та брандмауерів. Автентифікація користувачів відбувається з використанням сертифікатів для підтвердження достовірності особи.

Після встановлення з'єднання між клієнтом і сервером створюється захищений канал, який відправляє захищені HTTPS пакети, які зашифровані стандартом SSL/TLS.

Великою перевагою SSTP є його алгоритм роботи, який дозволяє йому пройти через фаєрволи та NAT, бо використовує стандартні порти Windows, і забезпечує надійний рівень захисту. Через відмову використання UPD пакетів, і використання протоколу TCP що дозволяє швидше, та ефективніше передавати дані у порівнянні з іншими протоколами. Простота налаштування дозволяє користувачу без особливих проблем налаштувати тому, що протокол є стандартним.

SSL/TLS - протокол безпеки який займається шифруванням та захистом і передачею даних в мережі. SSL розробила компанія Netscape, а згодом версія SSL була обновлена до TLS.

SSL протокол забезпечує захищену передачу даних у мережі, і розроблений для конфіденційної передачі інформації, перевірки її цілісності та автентичності між клієнтом та сервером. Використання криптографічних

`

сертифікатів, які видає довірена сторона, базується на роботі з відкритим ключем для шифрування даних, та його цифрового підпису для перевірки особи, та автентичності даних[10].

TLS є модифікованою версією SSL і у своїй роботі використовує алгоритми шифрування та криптографічного захисту інформації, автентифікації користувачів та ідентифікації сторін, і працює з великою кількістю протоколів, таких як HTTP, SMTP, FTP.

Протокол використовує симетричне, та асиметричне шифрування, що дозволяє обмінюватися ключами в активній сесії, і вибрати криптографічні параметри захисту в мережі. Підтвердження автентичності даних та користувачів відбувається перед початком обміну ключами, і збільшує рівень довіри до сторін та захищає від перехоплення даних. Використання хешування дозволяє перевірити цілісність даних, і виявити чи були дані перехоплені та скомпрометовані. Стандарт SSL/TLS використовується великою кількістю браузерів та програм, і дозволяє користуватися з вебресурсами по безпечному з’єднанні.

IKEv2/IPSec - протокол обміну ключами для безпечного з’єднання в VPN, який є частиною IPSec, і забезпечує автоматичну настройку з'єднання між двома станціями.

Протокол працює в два етапи, які забезпечують створення тунелю, та надійного з'єднання, та аутентифікації користувачів. В першій фазі - IKE_SA_INIT відбувається обмін ключами та їх параметрами хешування для створення тунелю. Після створення тунелю відбувається обмін ключів захисту для наступного етапу протоколу. В другому етапі - IKE_AUTH відбувається автентифікація двох станцій, перевірка цілісності та достовірності повідомлення, обмін ключами шифрування та підтвердження автентичності. Після цих двох етапів відбувається тунельна асоціація, і дані можуть передаватися по каналу.

Перевагами даного протоколу є його швидкість роботи в порівнянні з іншими протоколами. Використання алгоритмів шифрування AES та SHA-2 створюють надійний захист. Автоматичне відновлення з'єднання після розриву

`

підвищує його ефективність на фоні інших, що робить його незамінним для мобільних пристроїв які постійно пересуваються з однієї мережі в іншу, і часто втрачають з'єднання. Використання мультикасту дозволяє створювати захищені сесії для великої кількості користувачів одночасно, що робить його привабливим для корпоративних мереж, і дозволяє ефективніше працювати колективу в локальній мережі.

WireGuard - протокол VPN з відкритим кодом, який створений для забезпечення швидкого та надійного з'єднання. Протокол є відносно новим, але вже зарекомендував себе як надійний та стабільний інструмент для роботи в кіберпросторі.

Новизна протоколу полягає в сучасній криптографічній системі, та спрощення в архітектурі, що виділяє його поміж інших. Алгоритм роботи містить створення захищеного каналу, і видання IP адресу від віртуального адаптера інтерфейсу, що дає змогу станціям обмінюватися інформацією між собою.

Спрощеність архітектури робить його одним із найстійкіших VPN протоколів. Менша кількість коду полегшує його інтеграцію в інші системи, дає змогу провести аудит захисту системи, та провести тестування на проникнення, та виявити всі сильні та слабкі сторони.

Через свою новизну протокол WireGuard не такий популярний та перевірений і його потенціал та рівень безпеки не такий досліджений спеціалістами як інші. Рівень підтримки та сервісу не такий універсальний як у своїх конкурентів і не підтримується на всіх платформах, що робить його не таким універсальним. Підтримка різних версій може не працювати на тих чи інших пристроях і застаріле обладнання не підтримує протокол WireGuard.

OpenVPN - відкритий протокол VPN, який використовує технології SSL/TLS шифрування і створення з’єднань, має підтримку кросплатформеності та гнучкість в налаштуванні.

Архітектура протоколу складається з клієнта та сервера які обмінюються інформацією між собою. Клієнт встановлюється на пристрою користувача, а

`

VPN сервер керує з'єднаннями між клієнтами, та займається маршрутизацією. Створення конфігураційних файлів дозволяє налаштувати як сервер та клієнт, в залежності від поставлених потреб. На сервері створюються ключі які використовуються для шифрування даних та автентифікації на сервері. Клієнтська база даних створюється для полегшення роботи з користувачами та створення таблиці для аутентифікації користувачів. Мережевий стек полегшує та пришвидшує роботу з мережевим трафіком та координує сервер для роботи з клієнтами. Створення тунелів потрібне для передачі зашифрованого трафіку в мережі.

Протокол в основі криптографічного захисту використовує відкриту бібліотеку OpenSSL яка дає змогу застосувати широкий спектр алгоритмів шифрування, протоколів та функцій.

Використання алгоритмів шифрування AES, Blowfish, 3DES забезпечує надійну криптостійкість, а методи автентифікації SHA-1, SHA-256, HMAC, RSA допомагають в ідентифікації користувачів та перевірки їх достовірності.

Для симетричного шифрування протокол використовує алгоритм AES, Blowfish та CAST-128. В процесі з'єднання та роботи, сервер і клієнт обмінюються ключами шифрування та встановлюють з'єднання по TLS протоколу. В залежності від задачі ми самі вибираємо рівень симетричного шифрування даних.

Асиметричне шифрування відбувається з допомогою сертифікатів інфраструктури відкритих ключів. В ході створення з'єднання створюється взаємодія автентифікації між сервером та клієнтом. Протокол обміну ключами DeffieHellman створює спільний секретний ключ між клієнтом та сервером для шифрування мережевого трафіку. Використання цифрових сертифікатів для перевірки автентичності користувачів. Інструмент EasyRSA дозволяє створити центр сертифікації для перевірки сервера та клієнта.

EasyRSA - інструмент для роботи з ключами та сертифікатами доступу в протоколі OpenVPN. Він створює умови для генерації, налаштуванні та управління сертифікатами, що базується на відкритій бібліотеці OpenSSL. Має

`

простий та логічний інтерфейс для створення центру сертифікації та їх генерації. З цим інструментом можна самостійно генерувати само підписані сертифікати для інфраструктури ключів та з їх допомогою виконувати автентифікацію на сервері. EasyRSA генерує сертифікати на основі RSA ключів, дозволяє їх налаштувати та займатися адмініструванням в базі даних PKI. Використання даного набору скриптів та інструментів полегшує роботу з керуванням та адмініструванням ключами та сертифікатами в протоколів OpenVPN

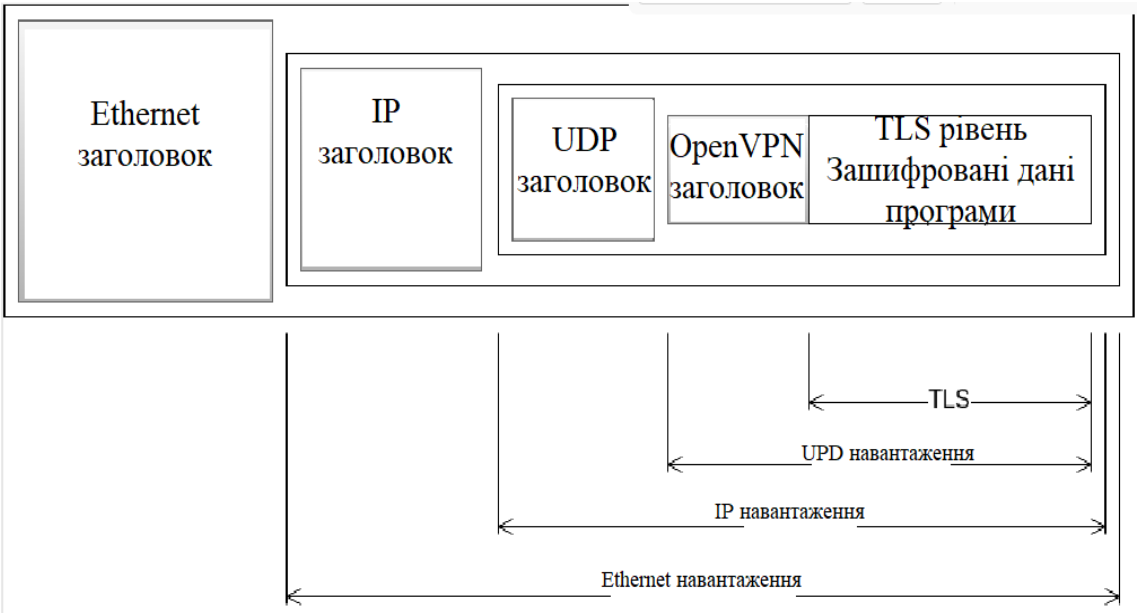


Рисунок 1.6 - Вигляд пакету протоколу OpenVPN

Додаткові технології захисту та безпеки з'єднання для автентифікації клієнта та сервера роблять OpenVPN незамінним для роботи з важливою інформацією. Використання HMAC для перевірки та забезпечення цілісності даних за допомогою хеш-функції з використанням секретного ключа. При отриманні даних отримана інформація перевіряється за допомогою ключа, і при будь-якій зміні ключ буде не відповідним і інформація буде скомпрометована. Ця технологія допомагає захиститися від атак людина посередині[11].

OpenVPN використовує двофакторну аутентифікацію, яка створює додатковий рівень захисту. Для використання доступні різні методи, і їх можна комбінувати для більшого захисту. Використання логіна та пароля дає не достатній рівень захисту, а в комбінації зі смс-кодом для автентифікації

`

надійність зростає в рази. Використання спеціального сертифіката й цифрового підпису захищена від підміни сертифіката.

Використання токенів ще один рівень захисту облікових записів, що унеможливлює несанкціонований доступ до ваших даних. Токени можуть бути відправлені вам на номер телефону, або на пошту і використані як додатковий захист разом з логіном і паролем. Створення одноразових паролів на основі алгоритму псевдовипадкових на певний період часу дають високий рівень стійкості та захисту. Ще є апаратні види токенів на USB-порти або на дистанційне під'єднання, що дозволяє використовувати біометрику та інші форми автентифікації.

TLS-аутентифікація забезпечує обміну даних між клієнтом і сервером. TLS створює двосторонню автентифікацію для підтвердження автентичності як і сервера, так і клієнта. Клієнт та сервер обмінюються сертифікатами з публічними ключами й перевіряють достовірність цифрових підписів та перевіряє його ідентичність. Використання TLS сертифікатів піднімає рівень надійності та захищає від заміни і підробки, та перехоплення даних у мережі.

Режими роботи протоколу:

1. Режим віддаленого доступу: використовується для створення безпечного доступу користувачів до локальних ресурсів системи.

2. Міжсайтовий режим: використовується для з'єднання декількох локальних мереж між собою для створення віртуальної приватної мережі, що дозволяє обмінюватися даними та ресурсами між мережами.

3. Режим точка-точка: створення з'єднання двох користувачів між собою.

4. Режим мосту: об'єднання віртуальної приватної мережі з локальною та створення з'єднання між ними.

OpenVpn може працювати з двома транспортними протоколами: UDP та TCP.

1. UDP режим: протокол не перевіряє наявність пакетів після доставки, та не відновлює їх в разі втрат, що дозволяє збільшити швидкість передачі даних, та передати частину інформації в разі поганого з'єднання. Використання

`

коротших заголовків пакетів в порівнянні з TCP, що зменшує об’єм переданої інформації та ефективніше використовувати ресурси системи. Відсутність перевірки перевантаження мережі дозволяє швидко передати дані. Але через відсутність перевірки цілісності доставки пакетів існує загроза втратити дані через нестабільну роботу мережі. Пакети UPD можуть піддаватися перешкодам, що може вплинути на якість та швидкість передачі даних.

2. TCP режим: гарантує безпечну доставку пакетів з перевіркою цілісності та автоматичне відновлення в разі втрати пакета для забезпечення надійності передачі даних. Контроль навантаження мережі дозволяє уникнути перевантаження мережі та забезпечити стабільність системи. Використання протоколу TCP робить його сумісним з великою кількістю пристроїв та систем. Протокол має додаткові витрати в порівнянні з UPD, що збільшує обсяг переданої інформації, а використання механізмів контролю навантаження та доставки створюють додаткове навантаження.



Рисунок 1.7 - Режими роботи

Головними перевагами OpenVPN є його відкритість та підтримка на різних платформах. Кросплатформеність OpenVPN дозволяє створювати з'єднання між різними операційними системами та не відчувати дискомфорт. Гнучкість у налаштуванні дозволяє створити надійну та захищену криптосистему та створити всі умови для стабільної роботи. Високий рівень безпеки протоколу полягає в різних методах криптологічного захисту інформації, підтримки різних методів ідентифікації та перевірки автентичності користувачів так і даних у мережі шляхом використання хешування та сертифікатів з цифровими підписами. Швидкодія протоколу з низькою затримкою роблять його стабільним

`

та надійним сервісом у роботі. Простота використання приваблює велику кількість користувачів, що дозволяє проекту постійно розвиватися та покращуватися. OpenVPN перевірений часом та демонструє свою стабільність та надійність і дозволяє користувачам у будь-який час та з будь-якого місця отримувати захищене з'єднання та доступ до даних. В таблиці 1.1 буде здійснено порівняння наявних алгоритмів VPN[12].

Таблиця 1.1 Порівняння алгоритмів VPN

Протокол VPN	PPTP	SSTP	L2TP/IPsec	IKEv2/IPsec	OpenVPN	WireGuard
Розробник	Microsoft	Microsoft	L2TP — Cisco Microsoft, IPsec — The Internet Engineering Task Force	IKEv2 — Cisco Microsoft, IPsec — The Internet Engineering Task Force	OpenVPN Technologies	Jason A. Donenfeld
Платформа	Windows, macOS, iOS,	Windows	Windows,Mac OS X, Linux, iOS, Android.	Windows 7+, macOS 10.11+	Windows, Mac OS, GNU/Linux, Apple iOS, Android , маршрутизатори	Windows, Mac OS, GNU/Linux, Apple iOS, Android.
Шифрування	MPPE, RSA RC4 128-біит	SSL	3DES или AES	AES, Blowfish, Camellia	OpenSSL	1-RTT, Curve25519 для ECDH, RFC7539 для ChaCha20 Poly1305 BLAKE2
Порт	TCP-порт 1723	TCP-порт 443	UDP-порт 500 для обміну ключів і UDP-порт 1701	UDP-порт 500 для обміну ключів і UDP-порт 4500	Будь-який UDP-TCP-порт	Будь-який UDP-порт

`

Продовження табл 1.1 Порівняння алгоритмів VPN

Протокол VPN	PPTP	SSTP	L2TP/IPsec	IKEv2/IPsec	OpenVPN	WireGuard
Недолік безпеки	MSCHAP-v2 - атаки по словнику, RC4 атака Bit-flipping	Серйозні вразливості відсутні	3DES вразливий Meet-in-the-middle и Sweet32, IPsec скомпрометований	IPsec скомпрометований	Серйозних недоліків не виявлено	Серйозних недоліків не виявлено

1.4 Обгрунтування вибору протоколу OpenVPN

В сучасному кіберпросторі неможливо обійтися без технологій VPN. Широкий вибір VPN сервісів ставить користувача перед важким вибором - який протокол краще виконує всі поставлені задачі та цілі. Дослідивши сучасні протоколи можна зробити висновки, що найкраще використовувати надійні та перевірені протоколи.

OpenVPN є одним із найзахищеніших протоколів на даний час та використовує широкий арсенал криптологічних можливостей. Сильне шифрування з використанням протоколу TLS/SSL, використання симетричного протоколу шифрування AES, асиметричного RSA, які є визнаними стандартами безпеки.

Надійність в роботі та його стабільність завоювали йому широку популярність. Робота в режимі UPD та TCP дозволяє контролювати мережевий потік, та здійснювати контроль пакетів, а за необхідності відправляти пакети та без перевірки для розвантаження системи. Незалежне використання портів дозволяє обходити блокування чи обмежень з боку мережевих адміністраторів, що робить його незамінним при роботі з проксі-серверами.

`

Широка підтримка спільноти користувачів збільшує його рівень підтримки на різних платформах. Підтримка на всіх популярних операційних системах дозволяють з'єднувати різні пристрої без проблем сумісності, що забезпечує універсальність використання.

Гнучкість в налаштуваннях та режимах роботи дозволяють налаштувати мережу під будь-які задачі. Робота в режимі сайт-сайт, клієнт-сайт, клієнт-клієнт створює умови для роботи з різними конфігураціями системи, та роботи як з окремими користувачами, так із локальними серверами.

Відкритий програмний код створює багато перспектив в його розвитку та інтеграції з різними системами та додатками. Відкритий програмне забезпечення може бути повністю протестовано та проведено аудит на вразливості, що збільшує його стійкість від атак, і дозволяє відразу ліквідовувати знайдені вразливості.

Легкість в налаштуванні приваблює не досвідчених користувачів, та дає можливість створити безпечний канал в короткі терміни без значних витрат. Для роботи з даним протоколом існує велика кількість технічних та наукових статей, де розписано весь алгоритм налаштування. Наявність графічного інтерфейсу полегшує навігацію та налаштування сервера.

1.5 Висновки до першого розділу

У розділі було представлено детальний опис технології VPN та її основних алгоритмів, зокрема OpenVPN. Було описано основні алгоритми шифрування та хешування, їх переваги та недоліки.

Наведено важливість та актуальність теми, оскільки вона створює умови для безпеки та конфіденційності передачі даних в мережі. Дозволяє з'єднувати віддалені мережі та надавати локальний доступ віддаленим користувачам по зашифрованому тунелю.

В ході роботи було проведено порівняння наявних технологій VPN, наведено їх переваги та недоліки, та обгрунтування вибору алгоритму OpenVPN. Наведена інформація підкреслила актуальність вибору теми для створення проекту мережі.

`

РОЗДІЛ 2 ПРОЕКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ МЕРЕЖІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ OPENVPN

2.1 Алгоритми роботи, архітектура та загальна структура системи

Проектування мережі залежить від поставлених задач та цілий, і має відповідати вимогам та стандартам для належного захисту від кібератак та витоку інформації. Архітектура створеної топології повинна забезпечити стабільну та надійну роботу в середині мережі та створити комфортні умови для роботи користувачів.

Одна з головних задач технології VPN це створення захищеного каналу для віддалених користувачів, чи цілих відділів для роботи з головним офісом, де вся інформація яка передається є дуже важливою та секретною. Для звичайних користувачів VPN використовується для конфіденційності та обходу блокувань контенту в мережі.

Для реалізації даної мережі було використано мережевий віртуальний емулятор EVE-NG, який є першим емулятором мережі на без клієнтській системі. Вся робота відбувається в ізольованому середовищі на стороні сервера, а користувач вже сам вносить зміни у свій проект.

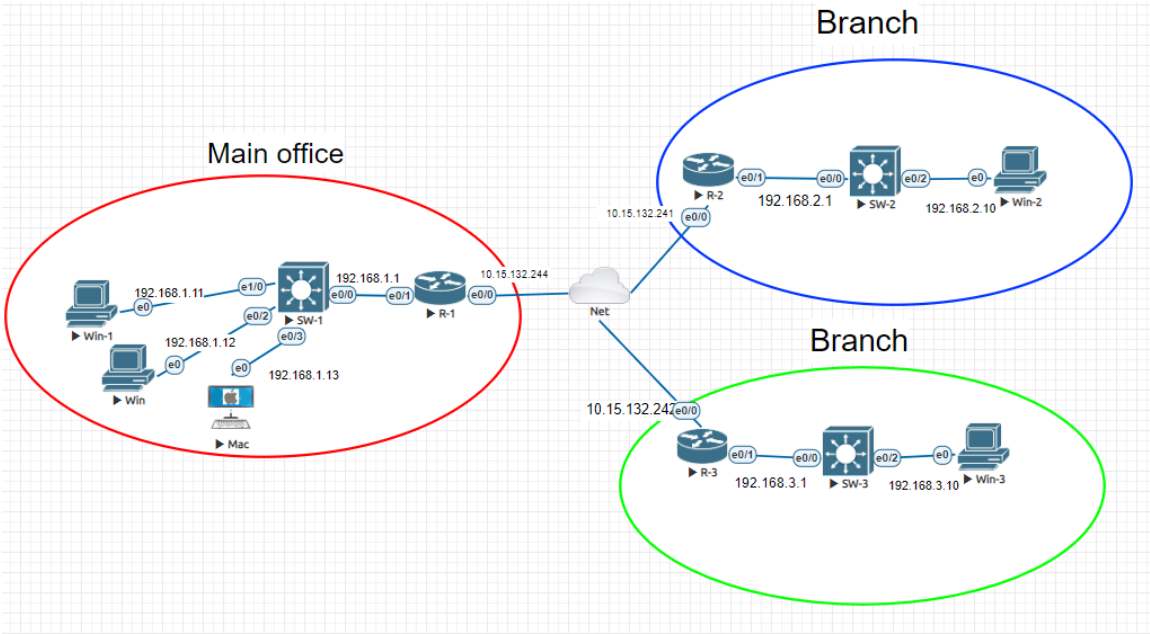


Рисунок 2.1 - топологія мережі

`

Для забезпечення роботи мережі VPN потрібно мати VPN сервер та клієнт, які налаштовані на прийом та відправку пакетів по тунелю.

Клієнт може бути як додаток для операційної системи, так і стандартний та інтегрований в систему. Клієнт потрібен для аутентифікації користувачів у мережі, перевіряючи їх дані для підтвердження їх автентичності. Забезпечує процес шифрування даних та всього трафіку який приймає та відправляє клієнт, щоб його не можна було перехопити. В клієнті можна налаштувати який тип з'єднання нам потрібен, який протокол використовувати, та який алгоритм шифрування. Ці параметри дозволяють клієнту гнучко налаштувати сервіс, та в залежності від поставлених потреб вибрати ту чи іншу конфігурацію.

Сервер це головна складова системи, яке займається маршрутизацією, та розподілом ресурсів клієнтів у мережі. Головне завдання сервера є створення безпечного з'єднання використовуючи доступні протоколи VPN та зашифрувати цей трафік відповідно до обраного алгоритму шифрування. Виконання аутентифікації та авторизації для обліку користувачів з метою перевірки їх достовірності. Сервер може виконувати ролі як для забезпечення доступу віддалених користувачів, так і для об'єднання декількох підрозділів в одну мережу, що полегшує роботу компаній, та забезпечує надійний захист при передачі файлів і даних[13].

Транспортування та логістика передачі пакетів в мережі залежить від мережевого обладнання, яке маршрутизує та комутує потік зашифрованих даних, та допомагає пакетам знайти свого адресата, та пройти весь шлях за короткий термін та без затримок і втрат.

Для забезпечення повноцінного функціонування роботи VPN потрібно правильність в алгоритмі налаштування, та дотримання всіх правил та стандартів роботи з серверами VPN.

Клієнт та сервер взаємодіють між собою та мають надійне та захищене з'єднання. Клієнт є програмним компонентом, або додатком, який простий в налаштуванні, та дає змогу користувачу отримати з'єднання з сервером.

`

Серверна частина знаходиться на фізичних, так і на хмарних та віртуальних серверах.

Клієнтське програмне забезпечення створює безпечний тунель між вашим пристроєм, та сервером. Створений канал є зашифрований, та захищений від перехоплення, та несанкціонованого втручання. Клієнт дозволяє користувачу пройти авторизацію, та обмінятися з сервером ключами, для підтвердження вашого статусу.

Серверна частина відповідає за збереження даних користувачів, їх автентифікацію, та якісне обслуговування, та створення комфортних умов для використання. Сервер маршрутизує трафік мережі, та створює відповідні тунелі й виконує роль розподільчої станції між кінцевими користувачами.

В парі з протоколами VPN використовують і алгоритми шифрування які відіграють ключову роль в забезпеченні надійності та конфіденційності даних мережі, і вберігають від несанкціонованого доступу[14].

Для стабільної роботи в парі з VPN сервером ще налаштовується мережевий екран, який відповідає за безпеку в мережі, та захищає від злому та від DDoS атак. Створює захист від зовнішніх ризиків та факторів, фільтруючи трафік мережі, і блокуючи весь заборонений, або підозрілий.

Мережевий екран використовується для безпеки мережі та створення розмежування прав та доступу в мережі. Фаєрвол може бути як фізичним, так і програмним застосунком, який фільтрує весь трафік в мережі. Використання фаєрволу дозволяє розподілити права та ресурси в залежності від рівня доступу. Мережевий екран виконує і функції аутентифікації та підтвердження достовірності користувачів, які приєднуються до сервера та перевіряє їх логін та пароль, сертифікати та токени. Виконання шифрування як IPSec та SSL/TLS підсилює криптостійкість системи, та захищає дані при їх передачі.

Цифровий підпис перевіряє не тільки цілісність даних, але й автентичність відправника. В роботі цифрового підпису відбувається обмін публічними ключами, і користувачі перевіряють автентичність один одного і створюють між собою зв’язок. Цифровий підпис потрібен для забезпечення високого рівня

`

захисту та довіреності між сторонами. Використання асиметрично шифрування зменшує ризик підробки даних та підпису, і захищає отримувача від отримання скомпрометованої інформації.

Використання цифрового підпису надійний інструмент для технологій VPN, щоб перевірити достовірність та надійність даних які були отримані у мережі.

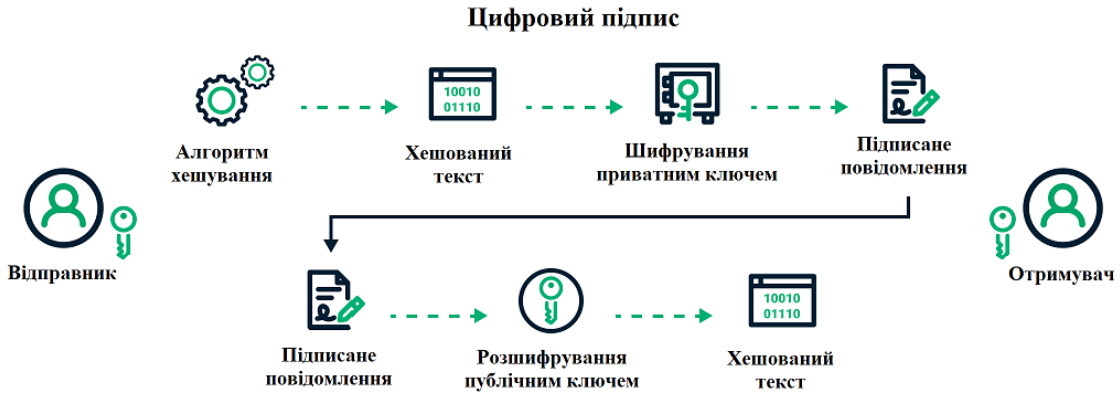


Рисунок 2.2 - Алгоритм роботи цифрового підпису

HMAC - алгоритм хеш-функції для перевірки даних на цілісність та автентичність, базується на MD5, SHA-1, SHA-2.

Використовує у своїй роботі спільний ключ який обчислює хеш повідомлення та додає хеш-код до нього. Після отримання користувач звіряє отриманий код з відкритим ключем та отримує дані про його автентичність.

Використання перевірки на автентичність дозволяє перевірити чи були зміни в тексті шляхом перевірки контрольної суми, та за допомогою відкритого ключа перевірити автентичність відправника. Хешування використовує незначний обсяг ресурсів, що дозволяє використовувати його з великим об'ємом даних. Використовувати хешування можна як вже на зашифрований потік даних, так і на звичайні, і з урахуванням цього можна створювати гнучкі сценарії налаштування.

Правильне налаштування та дотримання політик безпеки допоможуть зберегти стійкість системи. Використання одного ключа довгий час піддає ризику вашу криптостійкість, і може призвести до його втрати чи перехоплення, що скомпрометує ваші дані[15].

`

DSA - асиметричний алгоритм цифрового підпису для забезпечення автентичності та і перевірки цілісності даних.

При генерації ключів вибирається величина розміру ключа, та генерується секретний ключ, а публічний ключ генерується на основі приватного. Цифровий підпис відбувається шляхом вибору випадкового ключа та отриманні хеш-функції. Після отримання публічного ключа та обчислення хешування повідомлення й оберненого елемента, відбувається зіставлення отриманим та заявленим даних у хеш-функції і її валідація.

Даний алгоритм дає змогу зробити та перевірити автентичність підписів, що робить наші дані безпечними та автентичними. Алгоритм грунтується на роботі великих та простих чисел з дискретним логарифмуванням. Розмір даного алгоритму менший за аналогів, що робить його ефективним для мобільних пристроїв. Широка відомість даного цифрового підпису робить його ефективним у використанні, підтримка на великій кількості платформ та сумісності з різними протоколами забезпечує його довіреність і визнання.

DSA працює з обмеженим розміром ключа 1024 та 2048 біт, який є відносно великий та потребує більше ресурсів при використанні великих простих чисел. Велика довжина ключа створює великий об’єм даних, які пов’язані з факторизацією та дискретним логарифмуванням вразливий до атак квантових комп’ютерів. На даний час квантові комп'ютери це велика рідкість і ймовірність кібератак з їх використанням малоймовірна. Вузька спеціалізація даного алгоритму полягає в цифровому підписі, і його в основному використовують в парі з іншими алгоритмами. Новизна алгоритму робить його не таким популярним як RSA та ECC, і має меншу підтримку користувачів та протоколів[16].

Алгоритми автентифікації застосовують для перевірки сторін комунікації, та автентичності сторін для запобігання несанкціонованого доступу до системи, щоб довірені сторони могли працювати один з одним.

`

Зазвичай для перевірки автентичності використовується зв'язка логіна та пароля. Облікові дані користувачів дозволяють ідентифікувати користувачів, та авторизувати їх у системі, і валідувати для доступу.

Сертифікати доступу взаємної автентифікації дозволяють користувачам обмінюватися публічними ключами, та перевірити автентичність клієнтів, і створити довірені сторони.

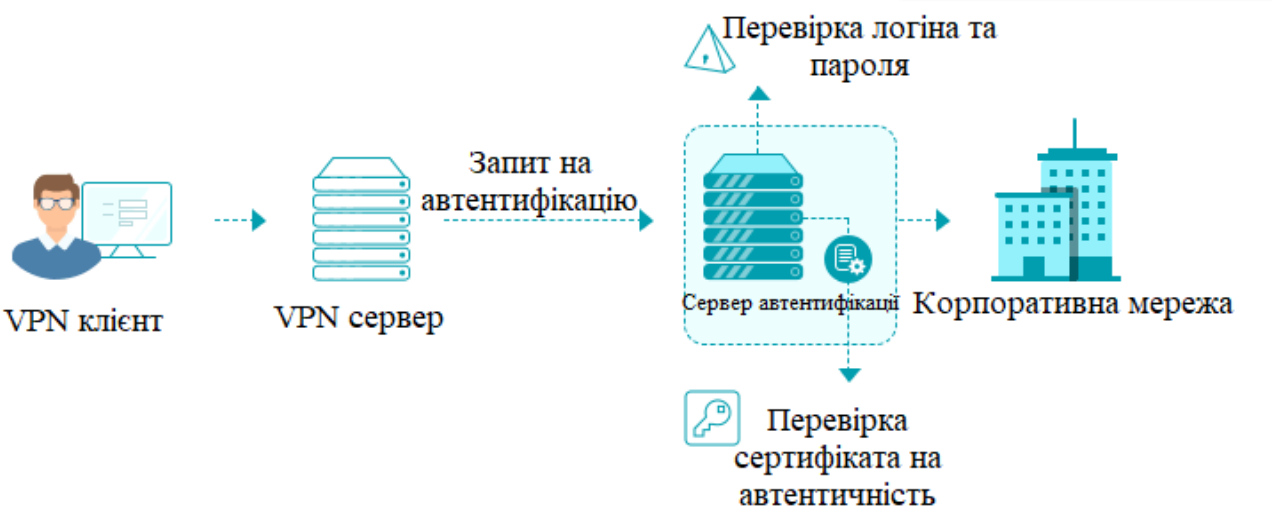


Рисунок 2.3 - Алгоритм роботи сервера автентифікації

CHAP - протокол автентифікації який використовується в технологіях VPN для перевірки користувачів на автентичність. Сервер посилає користувачу повідомлення-виклик, користувач обчислює хеш-функцію і відповідає назад на сервер. Сервер звіряє отриману хеш-функцію зі своєю базою даних, та верифікує користувача в системі.

Використання випадкових викликів та хешування даних, забезпечують протоколу надійність та захищають від підробки, що збільшує стійкість до атак перехоплення, та відтворення[17].

Аутентифікація відбувається без пароля, а за допомогою хеш-функції, що дозволяє зберігати пароль в секретному місці, і не передавати його в мережі. Простота в налаштуванні зробила його популярним серед користувачів, та допомогла завоювати широку підтримку на різних платформах.

Одностороння автентифікація сервера робить його не таким надійним в експлуатації, та може піддаватися атаці в разі підміни сервера. Використання

`

хеш-пароля може призвести до витоку даних в мережі, та бути перехоплені та використанні для атак відбирання та повторення даних. Відсутнє шифрування даних створює загрозу конфіденційності, і тому даний алгоритм аутентифікації не рекомендується для використання.

Для покращення показників захисту автентифікації компанія Microsoft модифікувала даний протокол та використовує його у своїй операційній системі. MS-CHAPv2 - протокол автентифікації який базується на основі CHAP та EAP, і поєднання цих протоколів доповнює один одного, і перекриває всі слабкі сторони.

EAP - протокол автентифікації який використовує різні методи аутентифікації в мережі. Може використовувати як логін та пароль, так і сім-карти, біометрику та інші. EAP може бути в різних варіаціях EAP-TLS, EAP-MD5, EAP-PEAP, EAP-TTLS.

1. EAP - MD5: використовує хеш-функцію для перевірки аутентифікації з використанням пароля.

2. EAP-TLS: використання сертифіката X509 створює канал зв'язку, який є безпечний, а сертифікат виконує основну роботу для аутентифікації користувачів.

3. EAP-PEAP: створює захищений тунель для роботи та обміну даних по ньому.

4. EAP-TTLS: створення тунелю з автентифікацією через EAP, та використання TLS для цифрових сертифікатів.

5. PEAPv0/EAP-MSCHAPv2 - комбінація PEAP з протоколом Microsoft для роботи з їх операційною системою.

Використання різних методів та протоколів дозволяє підлаштувати авторизацію під різні задачі, та гнучко налаштувати сценарій роботи. Використання криптографічного захисту даних робить використання даного протоколу безпечним в мережі[18].

Алгоритм визначає структурну роботу протоколу, та дозволяє нам самим вибрати в якому режимі працювати.

`

2.2 Вибір мережевого обладнання, побудова та налаштування мережі

У проекті було побудовано мережу в якій є головний офіс, та два відділення. Обладнання яке було використано в головному офісі: маршрутизатор Cisco 800 Series Integrated Services Routers, мережевий комутатор Cisco 2960, робоча станція Windows 10 з налаштованим OpenVPN клієнтом, робоча станція Sierra macOS з налаштованим OpenVPN клієнтом, робоча станція Windows 10 з налаштуванням OpenVPN сервером. Дослідження та перехоплення трафіку в мережі буде здійснюватися за допомогою WireShark. У відділенні 1 та 2 було використано аналогічні маршрутизатор, комутатор та робочі станції.

Основою мережі слугує мережеве обладнання від світового бренду CISCO, яке зарекомендувало себе як одне з найкращих у своїй категорії. Надійність пристроїв перевірена роками та роботою в реальних мережевих середовищах. При виборі обладнання від CISCO ми можемо підібрати як і для малих підприємств, так і для мережевих гігантів. Широкий спектр послуг для обладнання дозволяє постійно оновлювати пристрої, та модифікувати новими модулями вже наявну техніку.

Компанія також відома інноваціями у сфері захисту мережевої інфраструктури. В асортименті послуг по кіберзахисту присутні вбудовані функції шифрування, аутентифікації та авторизації, VPN, міжмережеві екрани, та інше.

Компанія має велику кількість партнерів, що дозволяє інтегрувати обладнання в різні системи, і створювати цілі мережні системи. Велика підтримка серед користувачів та уніфікована система команд дозволяють підтримувати попит на дані пристрої, та розширювати аудиторію. Наявність школи CISCO та різних курсів допомагає навчати велику кількість спеціалістів, та підіймати рівень знань всіх охочих.

Cisco 800 Series Integrated Services Routers - лінійка маршрутизаторів які були розроблені для малого бізнесу та віддалених філій. Мають високу продуктивність що забезпечує достатній рівень пропускної здатності та обробки даних. Можуть працювати в режимах 10/100/1000 Mbps.

`

Інтеграція різних технологій дозволяє гнучко налаштувати маршрутизацію та комутацію в мережі. Широкосмуговий доступ та керування VLAN можуть розмежувати доступ в мережі. Використання фаєрволу та VPN допомагають захистити мережу від атак та втрати конфіденційних даних. Деякі версії підтримують технології бездротового зв'язку.

Управління відбувається через спеціальні інструменти моніторингу та управління мережі, та логування подій.



Рисунок 2.4 – Маршрутизатори Cisco 800 Series ISR

Cisco Catalyst 2960 - це лінійка комутаторів, які були створені для розгалужених мереж малих та середніх підприємств. Даний маршрутизатор доступний в різних конфігураціях і може бути налаштований в залежності від потреб організації

Комутатор може працювати в різних швидкісних режимах 10/100/1000 Mbps, в комплектації може налічуватися від 8 до 48 портів Fast Ethernet, або Gigabit Ethernet, так можуть бути підключені SFP модулі для більшої гнучкості та стекування декількох фізичних комутаторів в один логічний.

Наявність живлення по Power over Ethernet дозволяє реалізувати на їх базі системи відеонагляду, wi-fi системи та IP-телефонію.

Управління може здійснюватися як по командному рядку, так і в графічному інтерфейсі. Є підтримка роботи протоколів віддаленого доступу SSH та Telnet.

Різні механізми захисту роблять його складною ціллю для атаки. Використання контролю доступу до портів - Port-based Access Control, протоколи безпеки - Security Protocol, фільтрацію MAC адрес - MAC Address Filtering, та інших[18].

`

Використання протоколів STP та RSTP дозволяють створювати резервні шляхи та агреговані канали без ризику створення мережевих петель.



Рисунок 2.5 – Комутатори cisco 2960 x series

На маршрутизаторах було налаштовано static NAT для маршрутизації трафіку в інтернет, налаштовано маршрутизації в середині мережі та прописані маршрути до відділень 1 та 2. Налаштовано віддалене підключення по протоколу SSH для віддаленого налаштування мережевого обладнання, заблоковано непотрібні та небезпечні протоколи такі як telnet та http які не мають шифрування. Вхід до мережевого обладнання відбувається під паролем, для захисту від несанкціонованого доступу, застосовано логування успішних та помилкових входів в пам’яті, обмежено час сесії SHH та час між спробами автентифікації. Для більшого захисту було створені ACL правила для доступу по SSH тільки користувачам в локальній мережі.

В налаштуваннях комутатора було застосовано switch security configuration та BPDU guard. Всі не залучені порти було вимкнено, вхід до комутатора за паролем. На інтерфейсах робочих станцій було налаштовано port security в режимі access з доступом тільки по mac адресу який закріплений за даним портом, а в разі вторгнення та невідповідності mac адресу порт буде вимкнений.

На робочій станції Windows 10 було налаштовано OpenVPN сервер, та налаштовано підключення клієнтів з віддалених відділів. Трафік який проходить по VPN тунелю маршрутизується на сервері, наданий віддалений доступ до локальних даних в офісі. Всі під'єднанні клієнти можуть бачити один одного в мережі. Налаштуваннях Firewall було створено правила для дозволу ICMP пакетів з дозволених підмереж. Дозволено UDP пакети по 1194 порті для роботи OpenVPN, 22 порт для роботи SSH, 443 для роботи https, 445 для роботи SMB в

`

межах тунелю VPN. Порти які непотрібні і є потенційно небезпечними заблоковано. В таблицях 2.1 – 2.3 показано параметри з’єднання, а у таблицях 2.4-2.6 параметри маршрутизації.

Таблиця 2.1 Інформація інтерфейсів пристроїв Офісу

Пристрій	Інтерфейс	Підключення	Інтерфейс підключення
R-1	eth0/0	Net	
	eth0/1	SW-1	eth0/0
SW-1	eth0/0	SW-1	eth0/1
	eth0/1	Win	eth0/0
	eth0/2	Win-1	eth0/0
	eth0/3	Mac	eth0/0
Win	eth0/0	SW-1	eth0/1
	wintun	Win-1	wintun
Win-1	eth0/0	SW-1	eth0/2
	wintun	Win-1	wintun
Mac	eth0/0	SW-1	eth0/3
	wintun	Win-1	wintun

Таблиця 2.2 Інформація інтерфейсів пристроїв відділення 1

Пристрій	Інтерфейс	Підключення	Інтерфейс підключення
R-2	eth0/0	Net	•
	eth0/1	SW-2	eth0/0
SW-2	eth0/0	SW-2	eth0/1
	eth0/1	Win-2	eth0/0
Win-2	eth0/0	SW-2	eth0/1
	wintun	Win-1	wintun

`

Таблиця 2.3 Інформація інтерфейсів пристроїв відділення 2

Пристрій	Інтерфейс	Підключення	Інтерфейс підключення
R-3	eth0/0	Net	•
	eth0/1	SW-3	eth0/0
SW-3	eth0/0	SW-3	eth0/1
	eth0/1	Win-3	eth0/0
Win-3	eth0/0	SW-3	eth0/1
	wintun	Win-1	wintun

Таблиця 2.4 - Таблиця маршрутизації IP-адрес Офісу

Обладнання	Інтерфейс/ шлюз	IP адреса	Маска	номер маски
R-1	eth0/0	10.15.132.244	255.240.0.0	12
	eth0/1	192.168.1.1	255.255.255.0	24
	шлюз	10.0.0.1	255.240.0.0	12
SW-1	Vlna 1	192.168.1.2	255.255.255.0	24
	шлюз	192.168.1.1	255.255.255.0	24
Win	eth0/1	192.168.1.11	255.255.255.0	24
	wintun	192.168.10.2	255.255.255.0	24
	шлюз	192.168.1.1	255.255.255.0	24
Win-1	eth0/2	192.168.1.12	255.255.255.0	24
	wintun	192.168.10.1	255.255.255.0	24
	шлюз	192.168.1.1	255.255.255.0	24
Mac	eth0/3	192.168.1.13	255.255.255.0	24
	wintun	192.168.10.4	255.255.255.0	24

`

Таблиця 2.5 - Таблиця маршрутизації IP-адрес відділення 1

Обладнання	Інтерфейс/ шлюз	IP адреса	Маска	номер маски
R-2	eth0/0	10.15.132.241	255.240.0.0	12
	eth0/1	192.168.2.1	255.255.255.0	24
	шлюз	10.0.0.1	255.240.0.0	12
SW-2	Vlna 1	192.168.2.2	255.255.255.0	24
	шлюз	192.168.2.1	255.255.255.0	24
Win-2	eth0/1	192.168.2.11	255.255.255.0	24
	шлюз	192.168.2.1	255.255.255.0	24
	wintun	192.168.10.3	255.255.255.0	24

Таблиця 2.6 - Таблиця маршрутизації IP-адрес відділення 2

Обладнання	Інтерфейс/ шлюз	IP адреса	Маска	номер маски
R-3	eth0/0	10.15.132.242	255.240.0.0	12
	eth0/1	192.168.3.1	255.255.255.0	24
	шлюз	10.0.0.1	255.240.0.0	12
SW-3	Vlna 1	192.168.3.2	255.255.255.0	24
	шлюз	192.168.3.1	255.255.255.0	24
Win-3	eth0/1	192.168.3.11	255.255.255.0	24
	шлюз	192.168.3.1	255.255.255.0	24
	wintun	192.168.10.4	255.255.255.0	24

Налаштування параметрів маршрутизатора R-1: SSH, NTP, маршрутизація та встановлення параметрів входу. Налаштування R-2, R-3 аналогічні.

```
Router>en
Router#conf t
Router(config)#hostname R-1
R-1(config)#username admin privilege 15 secret admin
R-1(config)#int e0/0
R-1(config-if)#ip address dhcp
```

`

```
R-1(config-if)#ip nat outside
R-1(config-if)#no shut
R-1(config-if)#int e0/1
R-1(config-if)#ip address 192.168.1.1 255.255.255.0
R-1(config-if)#ip nat inside
R-1(config-if)#exit
R-1(config)#ip nat inside source static 192.168.1 0 10.15.132.244
R-1(config)#ip route 192.168.2.0 255.255.255.0 10.15.132.241
R-1(config)#ip route 192.168.3.0 255.255.255.0 10.15.132.242
R-1(config)#ntp server 216.238.35.0
R-1(config)#ip default-gateway 10.0.0.1
R-1(config)#ip domain-name vovkvpn.com
R-1(config)#access-list 11 permit 192.168.1.0 0.0.0.255
R-1 (config)#crypto key generate rsa general modul 1024
R-1(config)#line vty 0 4
R-1(config-line)#access-class 11 in
R-1(config-line)#transport input ssh
R-1(config-line)#password admin
R-1(config-line)#login
R-1(config)#line console 0
R-1(config-line)#login
R-1 (config-line)#password admin
R-1 (config)#username admin priv 15 secret admin
R-1 (config)#ip ssh version 2
R-1 (config)#ip ssh time-out 60
R-1 (config)#ip ssh logging events
R-1 (config)#ip ssh authentication-retries 3
R-1 (config)#login on-failure log every 3
R-1 (config)#login on-success log every 3
R-1 (config-line)# session-timeout 60
R-1 (config-line)# exec-timeout 9
R-1 (config)# login delay  9
R-1 (config)# no service telnet
R-1 (config)# no snmp-server
R-1 (config)# no http servert
```

Налаштування мережевого комутатора SW-1: VLAN, SSH, Port-security, BPDU Guadr, налаштування параметрів входу. На SW-2 та SW-3 аналогічні налаштування.

```
switch>en
switch#conf t
switch(config)#hostname SW-1
SW-1(config)#int vlan 1
SW-1(config-if)#ip add 192.168.2.1 255.255.255.0
```

`

```
SW-1(config)#enable secret admin
SW-1(config)#line console 0
SW-1(config-line)#password admin
SW-1(config-line)#login
SW-1(config-line)#line vty 0 4
SW-1(config-line)#password admin
SW-1(config-line)#login
SW-1(config-line)#exit
SW-1(config-if)#range interface eth0/1-3
SW-1(config-if-range)#switchport port-security
SW-1(config-if-range)#switchport port-security maximum 1
SW-1(config-if-range)#switchport port-security mac-address sticky
SW-1(config-if-range)#switchport port-security violation shutdown
SW-1(config-if-range)#spanning-tree portfast
SW-1(config-if-range)#spanning-tree bpduguard enable
SW-1(config-line)#exit
SW-1(config)#access-list 11 permit 192.168.1.0 0.0.0.255
SW1(config-if)#range interface eth1/0-3
SW-1(config-if-range)#shutdown
SW-1(config)# ip dhcp snooping
SW-1(config)# ip dhcp snooping vlan 1
SW-1(config)#crypto key generate rsa general modul 1024
SW-1(config)#line vty 0 4
SW-1(config-line)#access-class 11 in
SW-1(config-line)#transport input ssh
SW-1(config-line)#password admin
SW-1(config-line)#login
SW-1(config)#line console 0
SW-1(config-line)#login
SW-1(config-line)#password admin
SW-1(config)#username admin priv 15 secret admin
SW-1(config)#ip ssh version 2
SW-1(config)#ip ssh time-out 60
SW-1(config)#ip ssh logging events
SW-1(config)#ip ssh authentication-retries 3
SW-1(config)#login on-failure log every 3
SW-1(config)#login on-success log every 3
SW-1(config-line)# session-timeout 60
SW-1(config-line)# exec-timeout 9
SW-1(config)# login delay  9
```

Після налаштування мережевого обладнання потрібно перевірити працездатність мережі виконавши команди для тестування.

`

```
R-1#sh ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                10.15.132.244   YES DHCP   up                    up
Ethernet0/1                192.168.1.1     YES manual up                    up
Ethernet0/2                unassigned      YES unset  administratively down down
Ethernet0/3                unassigned      YES unset  administratively down down
NVI0                       10.15.132.244   YES unset  up                    up
```

Рисунок 2.6 – Команда show ip interface brief на маршрутизаторі R-1

```
R-1#sh ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
 ~216.239.35.0    .INIT.          16      -   1024     0  0.000   0.000 15937.
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

Рисунок 2.7 – Команда show ntp association на маршрутизаторі SW-1

```
R-1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static rout
e
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.0.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [254/0] via 10.0.0.1
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.0.0/12 is directly connected, Ethernet0/0
L        10.15.132.244/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Ethernet0/1
L        192.168.1.1/32 is directly connected, Ethernet0/1
S     192.168.2.0/24 [1/0] via 10.15.132.241
S     192.168.3.0/24 [1/0] via 10.15.132.242
R-1#
```

Рисунок 2.8 - Команда show ip route на маршрутизаторі R-1

```
R-1#sh ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDOKE7LkZzQGZzqFKG3ZNKQoUGis9DVTHOFh2bvEWF5
ZlZkXsCV9VfqUTIcJ71nVyovoJndkzpSlKA7baBF1WlpRQan2Be0k/BRmodK6DPyyQv/Hu2/bF3lsmMf
Xc7gZOTKm+fikFM3+NO5SvP5spxfJ/VI2PXusay0cYREPfDN/Q==
R-1#
```

Рисунок 2.9 – Команда show ip ssh на маршрутизаторі R-1

```
SW-1#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
Ethernet1/0            unassigned      YES unset  up                    up
Ethernet1/1            unassigned      YES unset  administratively down down
Ethernet1/2            unassigned      YES unset  administratively down down
Ethernet1/3            unassigned      YES unset  administratively down down
Vlan1                  192.168.1.2     YES NVRAM  up                    up
```

Рисунок 2.10 – Команда show ip interface brief на комутаторі SW-1

`

```
SW-1#sh ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 60 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): SW-1.vovkvpn.com
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDJrebWzKCodBrLA0Xs+dovdJ5dgnCdsSo6clOFZH4p
KwpmgxIsuQDSMggsEYCoZWbAbcpr4kF7cssdR03rQIlbCCQxkedI6eHbDodTvp4AchfkOBFyWtIpiUJr
2d5qz34FrPMI1gbTHH2fnhlxHBAst9YxKTdK1SR2hVO64tIqmQ==
```

Рисунок 2.11 – Команда show ip ssh на комутаторі SW-1

```
SW-1#show port-security int eth0/1
Port Security               : Enabled
Port Status                 : Secure-up
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses       : 1
Total MAC Addresses         : 0
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 0
Last Source Address:Vlan    : 0000.0000.0000:0
Security Violation Count    : 0
```

Рисунок 2.12 – Команда show port-security int eth0/1 на комутаторі SW-1

```
SW-1#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001
Extended system ID                      is enabled
Portfast Default                        is disabled
Portfast Edge BPDU Guard Default        is disabled
Portfast Edge BPDU Filter Default       is disabled
Loopguard Default                       is disabled
PVST Simulation Default                 is enabled but inactive in rapid-pvst
 mode
Bridge Assurance                        is enabled
EtherChannel misconfig guard            is enabled
Configured Pathcost method used is short
UplinkFast                              is disabled
BackboneFast                            is disabled

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
VLAN0001                    0         0        0          5          5
-------------------- -------- --------- -------- ---------- ----------
1 vlan                      0         0        0          5          5
SW-1#
```

Рисунок 2.13 – Команда show spanning-tree summary на комутаторі SW-1

```
R-1#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/5 ms
R-1#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R-1#ping 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R-1#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R-1#
```

Рисунок 2.14 – Команда ping на комутаторі R-1

Спробуємо зайти на SW-1 і перевірити чи працюють налаштування авторизації.

`

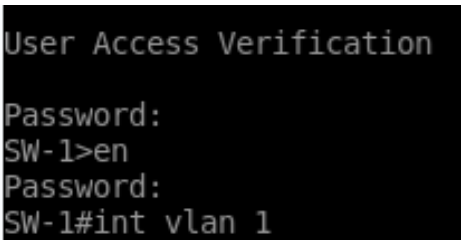


Рисунок 2.15 – Успішна авторизація на обладнанні

Наступним кроком перевіримо налаштування SSH при невдалих спробах, і перевищенні ліміту який ми задали.

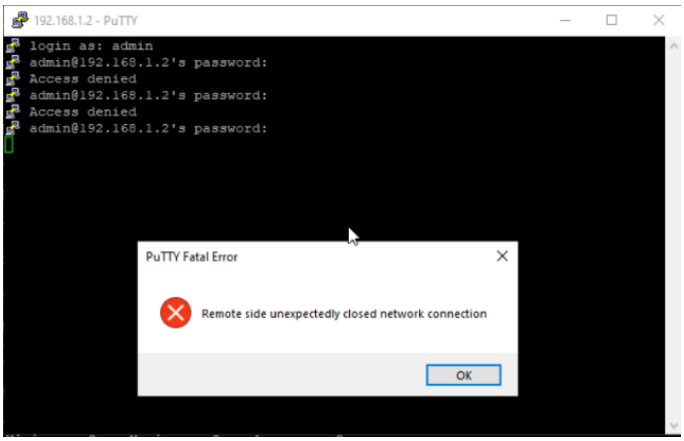


Рисунок 2.16 – Перевищення спроб підключення по SSH на комутаторі SW-1

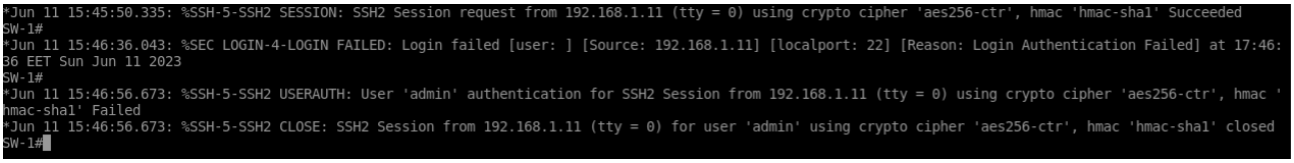


Рисунок 2.17 – Вміст логу SW-1

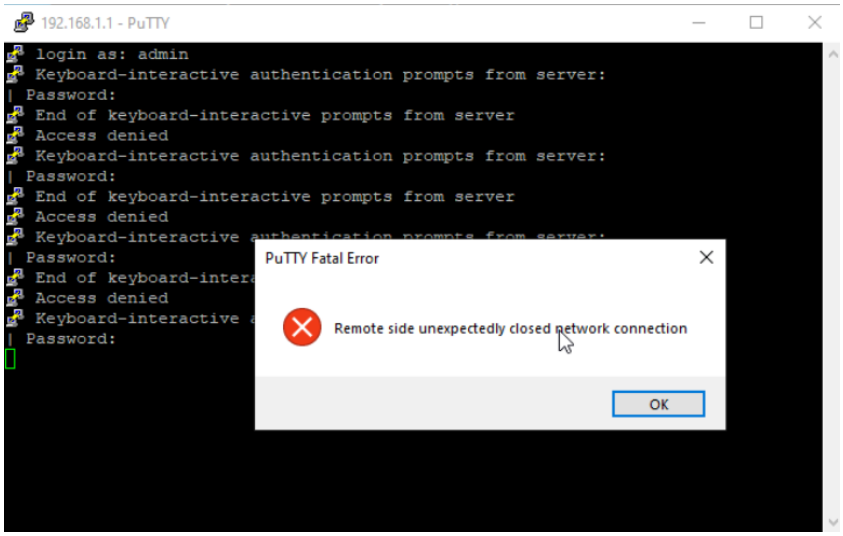


Рисунок 2.18 – Перевищення спроб підключення по SSH на комутаторі R-1

`

```
*Jun 11 15:48:42.238: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: 192.168.1.11] [localport: 22] [Reason: Login Authentication Failed] at 1
7:48:42 EET Sun Jun 11 2023
R-1#
*Jun 11 15:49:29.591: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/0 (not full duplex), with Router FastEthernet0/0 (full duplex).
R-1#
*Jun 11 15:49:43.918: %SSH-5-SSH2_USERAUTH: User 'admin' authentication for SSH2 Session from 192.168.1.11 (tty = 0) using crypto cipher 'aes256-cbc', hmac '
hmac-sha1' Failed
*Jun 11 15:49:43.918: %SSH-5-SSH2_CLOSE: SSH2 Session from 192.168.1.11 (tty = 0) for user 'admin' using crypto cipher 'aes256-cbc', hmac 'hmac-sha1' closed
R-1#
```

Рисунок 2.19 – Вміст логу R-1

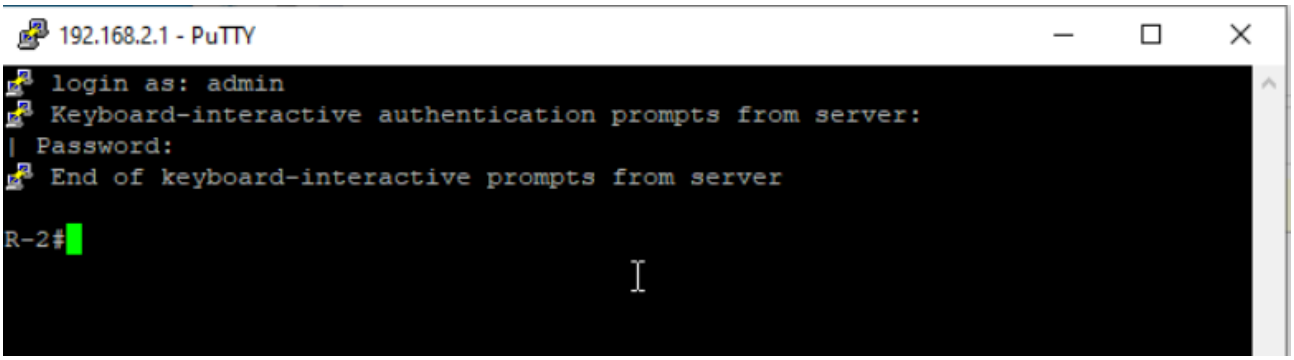


Рисунок 2.20 – Результат успішного підключення

Протокол SHH зашифровує вміст своїх повідомлень, і без ключа ми не зможемо розшифрувати зміст.

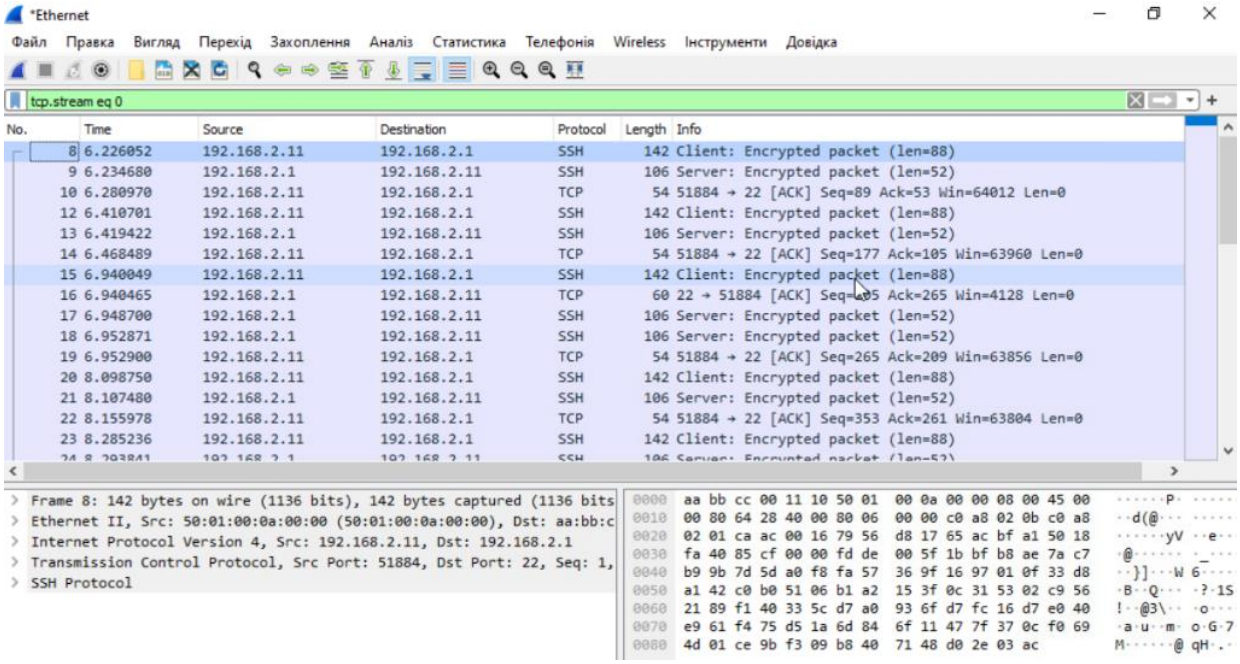


Рисунок 2.21 – Вміст перехопленого пакета SSH

`

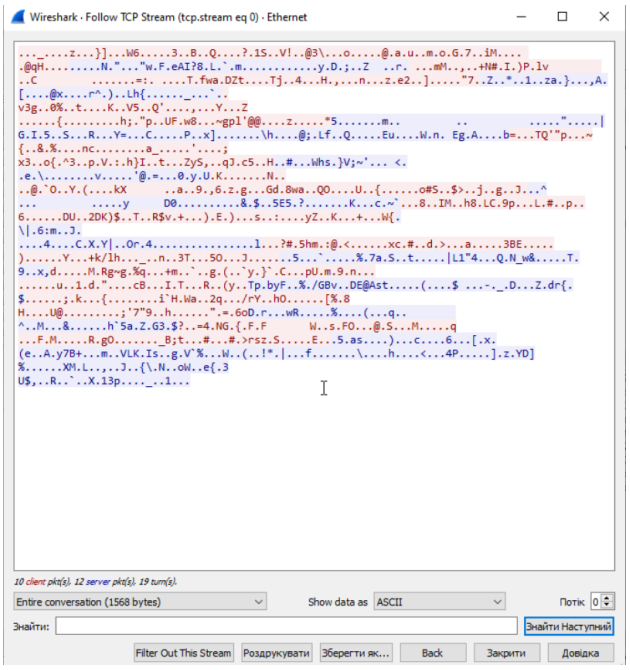


Рисунок 2.22 – Зашифрований вміст TCP пакета SSH

На фото можемо бачити результат перевірки налаштувань, та впевнитися в працездатності мережі. Перевірено роботу маршрутизації, NAT, ввімкнення захисту маршрутизатора та комутатор, показано спроби невдалого підключення до R-1 та SW-1 по SSH з робочої станції Win-1. Перехоплено пакет SHH та перевірено що вміст пакета зашифровано і його не прочитає зловмисник.

2.3 Розгортання VPNaaS на базі OpenVPN Connexa та Google Cloud

OpenVPN Connexa хмарний сервіс який використовує технології віртуальної приватної мережі OpenVPN. Використання віртуальних серверів дозволяє розгорнути сервер у будь-якому місці, та під'єднатися до нього віддалено, що спрощує процес створення VPN сервера. Простий та інтуїтивний інтерфейс допомагає легко орієнтуватися в налаштуваннях людям які не мають достатнього рівня навичок[19].

Хмарні сервіси OpenVPN мають високий рівень захищеності шляхом шифрування трафіку та аутентифікації користувачів. Гнучкість налаштування дозволяє вибрати тип підключення та параметри згідно з поставленою задачею. Ми самі вибираємо масштаб та обсяг використання потужностей сервера, і можемо застосувати його від малих офісних систем, до хмарних середовищ.

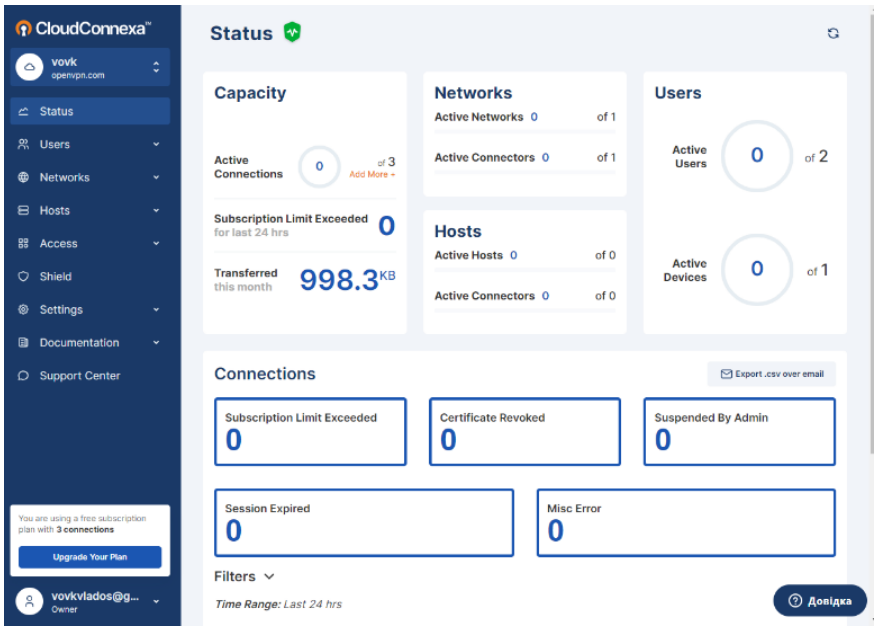


Рисунок 2.23 – Веб-інтерфейс CloudConnexa

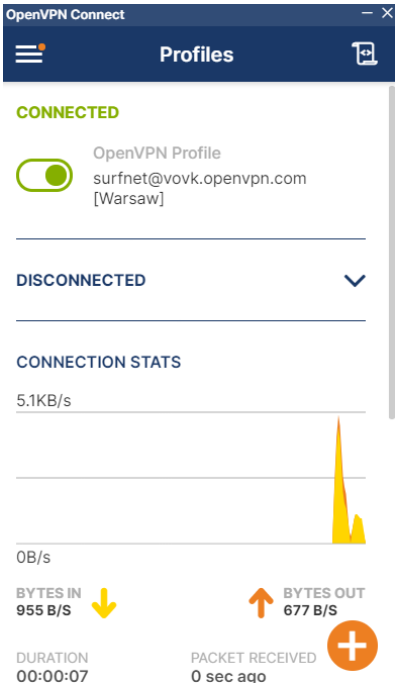


Рисунок 2.24 – Під'єднання до сервера користувачем vovk

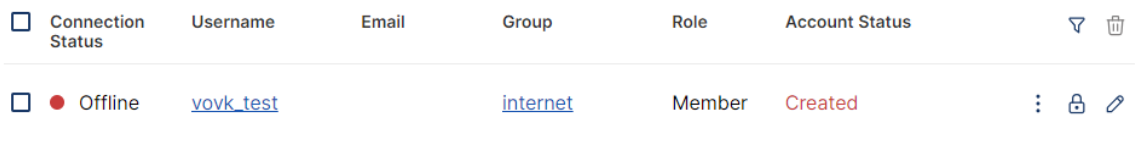


Рисунок 2.25 – Створення користувача vovk_test

`

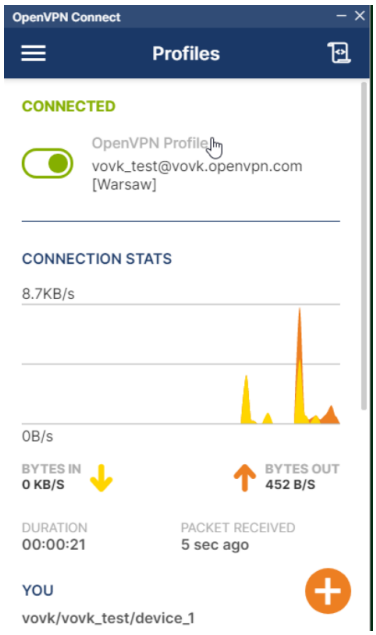


Рисунок 2.26 – Під’єднання до сервера користувачем vovk_test

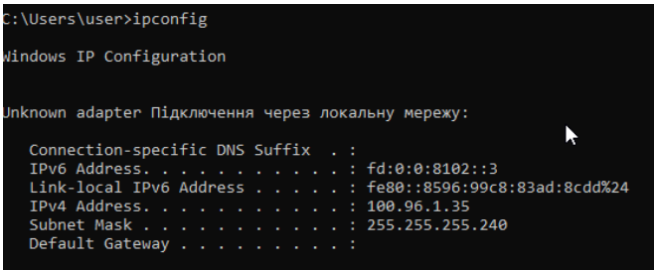


Рисунок 2.27 – Відображення віртуального VPN адаптера

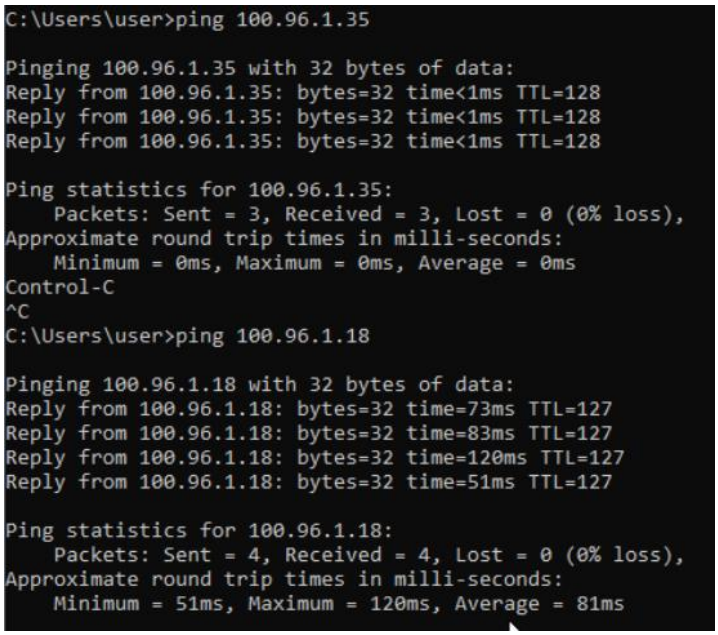


Рисунок 2.28 – Перевірка зв'язку між користувачами Vovk та test_vovk

`

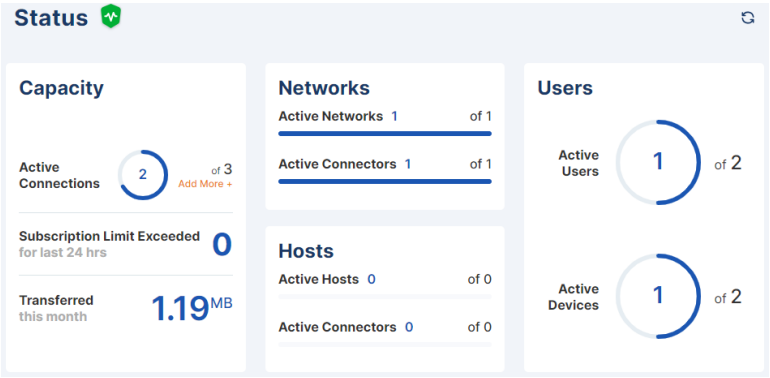


Рисунок 2.29 – Відображення статусу після під'єднання нового користувача

Налаштувавши зв'язок між клієнтами та сервером ми можемо спробувати перевірити ефективність роботи протоколу. Створимо теку зі спільним доступом, та передамо файли по SMB протоколу.

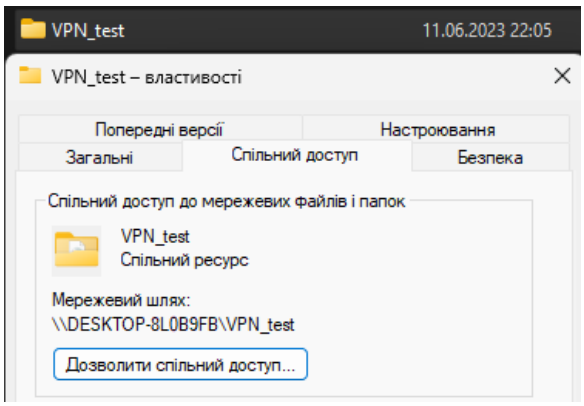


Рисунок 2.30 – Створення спільної мережевої теки на Vovk

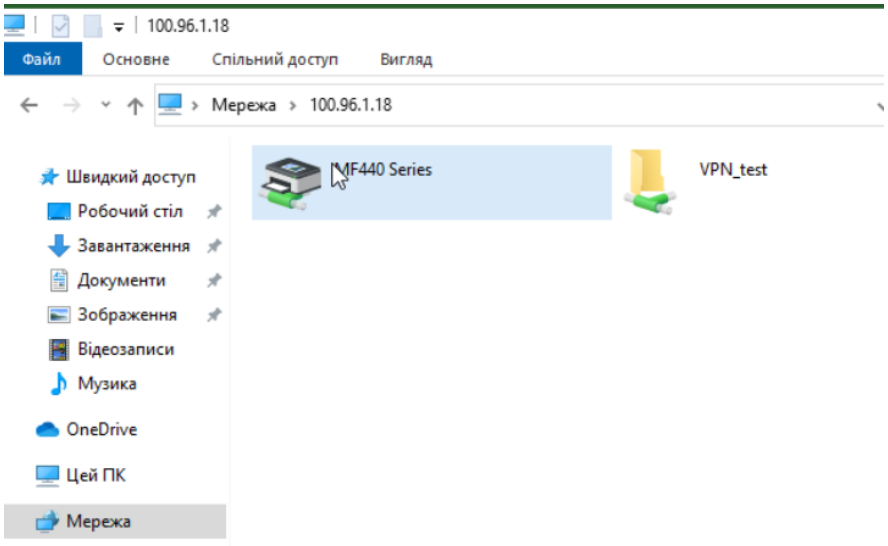


Рисунок 2.31 – Доступ до спільної мережевої теки vovk_test

```
TCP    100.96.1.18:139        0.0.0.0:0              LISTENING
TCP    100.96.1.18:445        100.96.1.35:34017      ESTABLISHED
```

Рисунок 2.32 – Виконання команди netstat –a

`

Перевіривши працездатність сервера можна зробити висновок, що CloudConnexa є досить зручним та ефективним VPN сервером. Швидкість розгортання та відсутність необхідності у втручання роботи віртуального сервера робить його зручним та компактним вибором для роботи.

OpenVPN Access Server може бути встановлений як на серверах OpenVPN, так і на інших доступних хмарних сервісах. Для розгортання сервера було обрано Google Cloud Platform де надалі буде встановлено VPN server.

Google Cloud Platform - це платформа хмарних серверів від компанії Google, яка дає широкий спектр послуг для роботи з хмарними середовищами. На даній платформі можна розгорнути велику кількість різних готових модулів і вибрати потрібну конфігурацію обладнання. Платформа є масштабною системою яка інтегрована зі всіма сервісами Google, що дозволяє ефективно використовувати всі її потужності. Доступність сервера та можливість реплікації надійно захищає ваші дані від втрати, а використання передових технологій шифрування робить ваші дані конфіденційними.

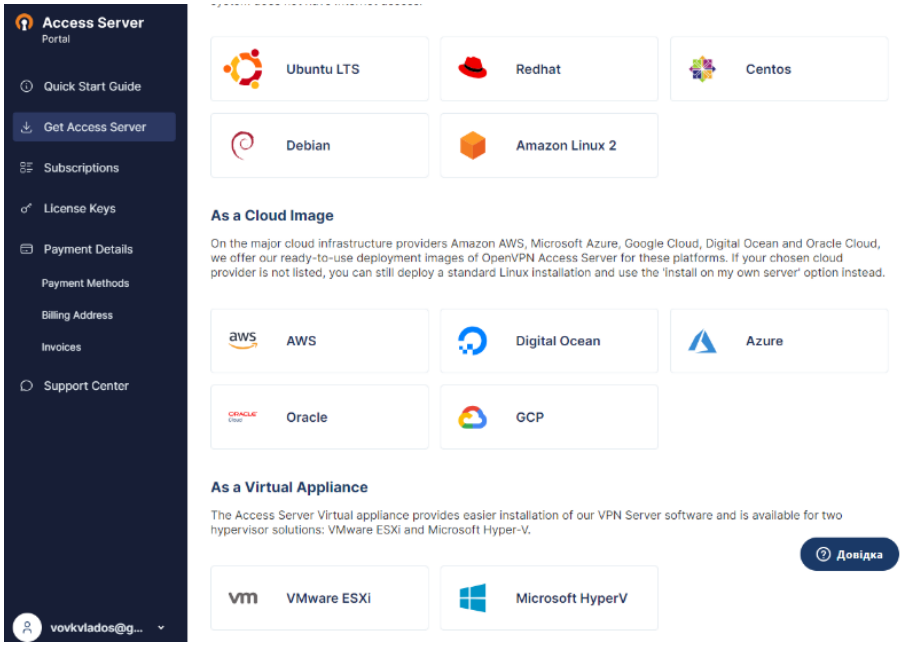


Рисунок 2.33 – Розгортання сервісу на хмарних серверах GCP

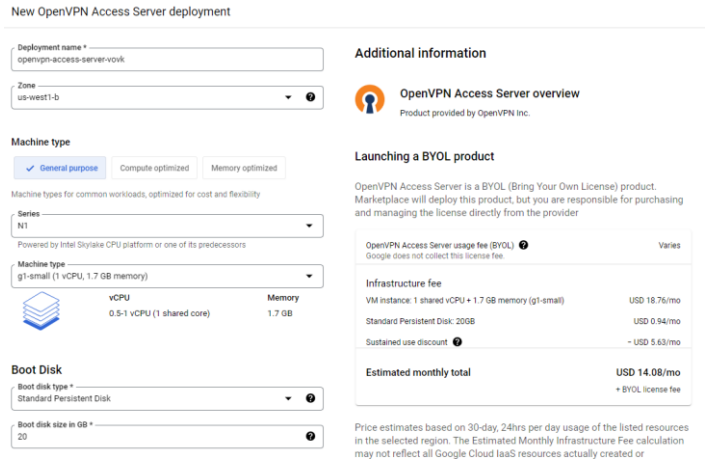


Рисунок 2.34 – Вибір налаштувань сервера

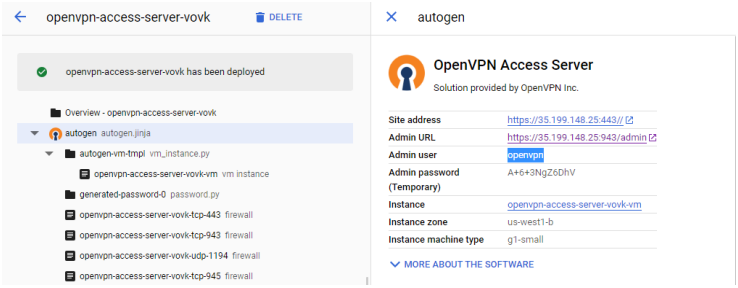


Рисунок 2.35 – Розгорнутий сервер OpenVPN

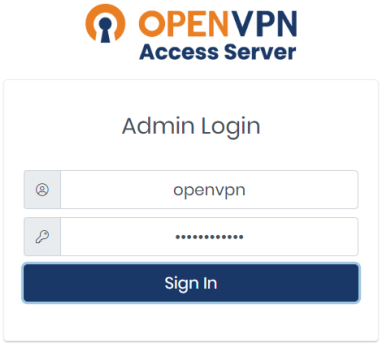


Рисунок 2.36 – Вхід в адмін панель OpenVPN

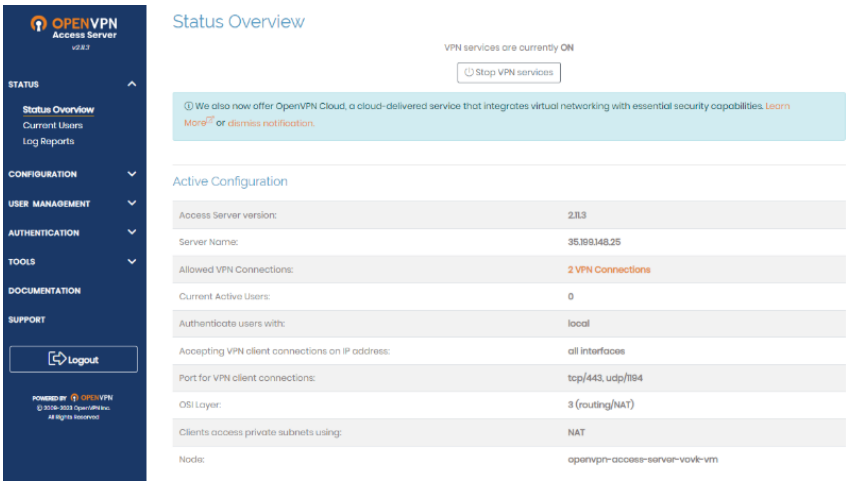


Рисунок 2.37 – Головна панель OpenVPN

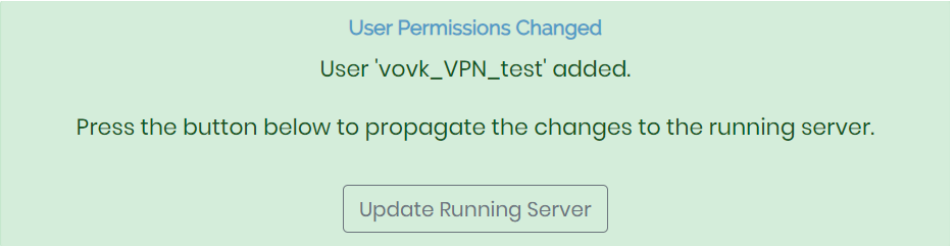


Рисунок 2.38 – Створення нового користувача vovk_VPN_test

SN #	Autologin	tls-crypt v2	Created	Expires	Signing CA	Comment	Last Used	Delete
3	N	N	2023-06-10	2033-06-08	OpenVPN CA			

Рисунок 2.39 – Створений користувач vovk_VPN_test

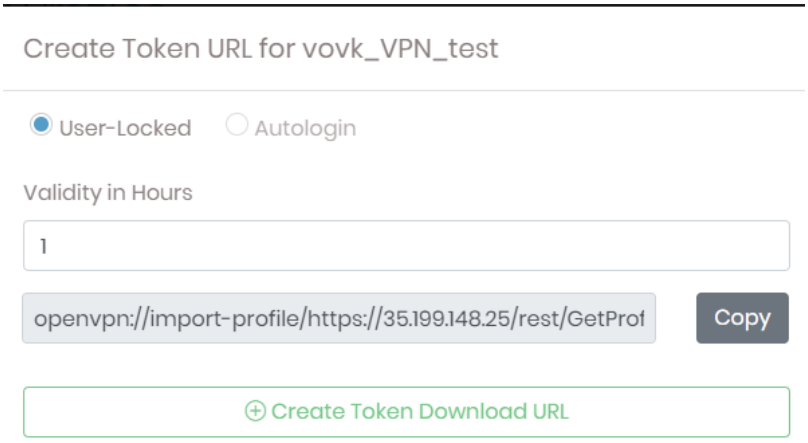


Рисунок 2.40 – Створення токену авторизації vovk_VPN_test

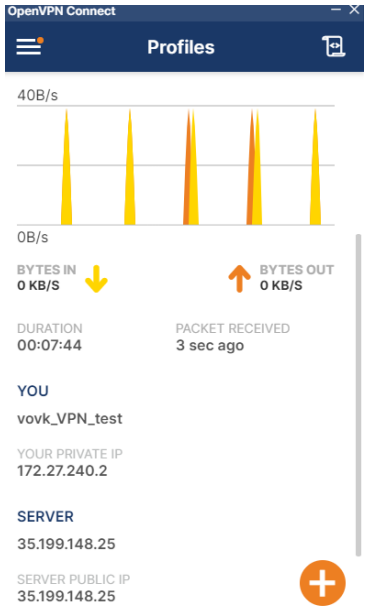


Рисунок 2.41 – Авторизація користувача vovk_VPN_test

`

```
Unknown adapter Підключення через локальну мережу:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2fb3:8d11:3fb:cd33%16
   IPv4 Address. . . . . . . . . . . : 172.27.240.2
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
```

Рисунок 2.42 – VPN інтерфейс

Active Configuration

Access Server version:	2.11.3
Server Name:	35.199.148.25
Allowed VPN Connections:	2 VPN Connections
Current Active Users:	2
Authenticate users with:	local
Accepting VPN client connections on IP address:	all interfaces
Port for VPN client connections:	tcp/443, udp/1194
OSI Layer:	3 (routing/NAT)
Clients access private subnets using:	Routing
Node:	openvpn-access-server-vovk-vm

Рисунок 2.43 – Стан VPN сервера

Common Name	Real Address	VPN Address	Bytes Sent Received	Connection Duration	Block
openvpn	188.163.18.85:62067	172.27.224.130	16.01KB 4.12KB	0:03:15	-
vovk_VPN_test	195.69.223.142:50055	172.27.240.5	20.41KB 5.30KB	0:02:51	⊘

Рисунок 2.44 – Користувачі VPN сервера

2.4 Моделювання загроз мережі на базі протоколу OpenVPN

Комп'ютерна мережа постійно піддається впливу різних факторів які частіше можуть як нашкодити системі. Для підвищення рівня захисту мережі потрібно перевіряти її на міцність та проводити аудит безпеки. Система має бути захищена як з середини, так і ззовні. Зазвичай слабкою ланкою в будь-якій системі є людський фактор який важко передбачити, а захистися від цього вкрай важко[20].

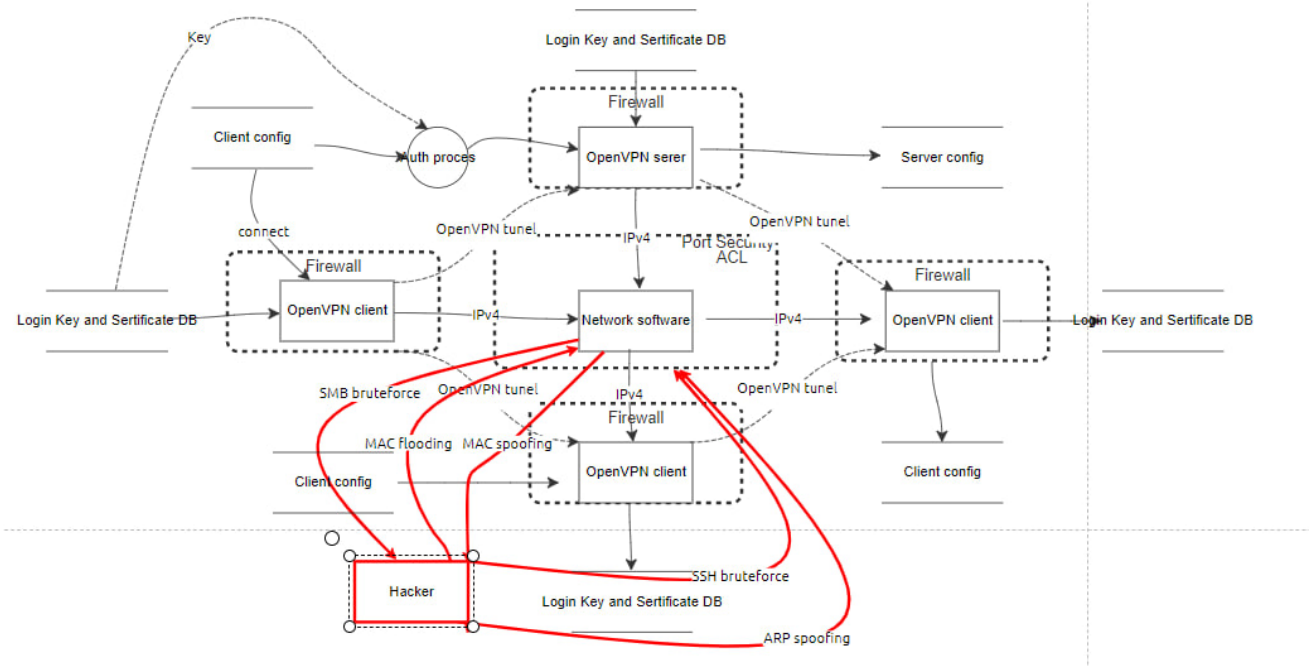


Рисунок 2.45 – Діаграма моделі загроз мережі на базі протоколу OpenVPN

В роботі мережі виступає модель сервер-клієнт:

1. Клієнтський комп'ютер: використовується для під'єднання до сервера та передачі даних по тунелю. Виконує функції шифрування та дешифрування даних.

2. Сервер OpenVPN: головний вузол обміну інформації по зашифрованому тунелю, який маршрутизує потік даних. Виконує функції шифрування, дешифрування, автентифікації та перевірки достовірності.

3. Конфігураційні файли: використовують для функціонування клієнт-серверної системи. В середині записано параметри маршрутизації та функцій які мають виконуватися.

4. Сертифікати та ключі: використовуються для створення каналу зв'язку та перевірки автентичності користувачів. Шифрування даних відбувається з використанням даних ключів та сертифікатів.

5. Зашифрований тунель: виконує функції захищеного з'єднання між клієнтами та сервером. Забезпечує конфіденційність та цілісність даних при передачі.

6. Протоколи та алгоритми шифрування: шифрують дані від несанкціонованого доступу та перевіряють цілісність після доставки.

Інформація в середині мережі поділяється на потоки:

`

1. Сервер-Клієнт: обмін даних по захищеному тунелю.

2. Дані маршрутизації мережі: весь мережевий трафік який проходить по мережевому обладнанню.

3. Дані автентифікації: дані які використовують між сервером та клієнтом для авторизації.

4. Дані керування: використання додаткових потоків для керування параметрами підключення та керування сеансами.

Соціальна інженерія постійно рухається в перед та створює нові методи роботи які націлені як на групи людей, так і на вас персональна. Фішингові атаки, вішинг, втирання в довіру та виманювання інформації виходить на новий рівень. Кожного дня знаходяться люди які попадають на гачок до аферистів і віддають добровільно свої персональні дані. Захистом для цього є навчання в кібергігієні та підвищення рівня власної обізнаності.

Атаки з використанням вразливостей можуть викликати збій в роботі системи, що зупинить роботу сервера та принесе шкоду компанії. Відмова сервера в обслуговувані викликана великою кількістю запитів на сервер спровокує переповнення буфера даних.

Якщо зловмисник зможе попасти в мережу та під’єднатися до локальної мережі він зможе моніторити трафік та спробувати його перехопити. Використання VPN тунелю захистить від таких загроз і ваші дані будуть захищені від модифікування, або крадіжки.

Щоб попасти у тунель злочинець має викрасти ключ та сертифікат відповідного сервера, й мати відповідні логін та пароль. Крадіжка сертифікатів може відбутися шляхом втручання в комп’ютер жертви. Відсутність модуль шифрування, та вимкнений BitLocker розв’яжуть руки для використання WinPE. Наявність відкритих USB портів, відсутність пароля для BIOS дасть повний доступ до ваших даних на комп’ютері.

Після отримання ключів та сертифікатів потрібно підібрати логін та пароль до сервера. Використання слабких даних для авторизації робить атаку грубої сили ефективною та в лічені хвилини дасть успішний результат

`

Поширеними атаками на мережеве обладнання є атаки грубої сили на протокол SSH. Атака містить спробу незаконної авторизації до системи шляхом підбору логіну та парою, що дасть доступ до мережевого обладнання. Зловмисник може спробувати перехопити дані автентифікації та спробувати розшифрувати вміст повідомлення якщо налаштовано слабке шифрування.

Тип загрози: атака мережевого рівня.

Рівень загрози: високий.

Для захисту від таких атак потрібно:

1. Використання надійних паролів.
2. Обмеження кількості спроб.
3. Обмеження часу очікування між спробами.
4. Оновлення протоколу та алгоритмів шифрування.
5. Використання IDS/IPS систем моніторингу підозрілого трафіку.
6. Використання ACL та налаштувань фаєрвола.

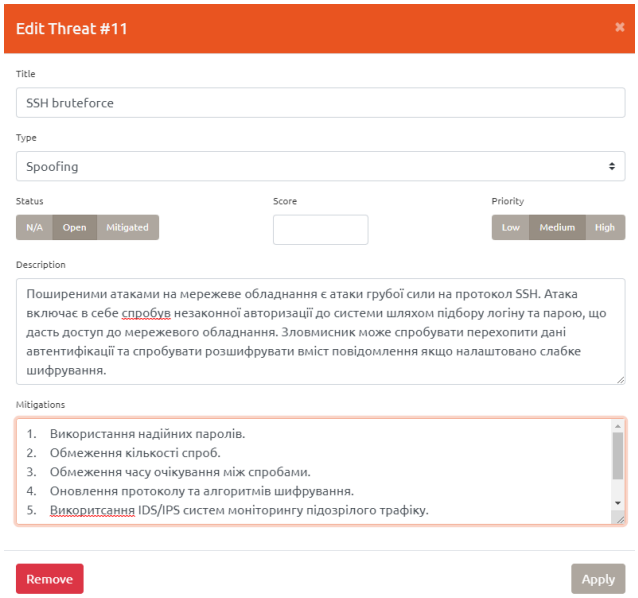


Рисунок 2.46 – Опис загрози SSH bruteforce

Атака Mac spoofing полягає в можливості змінити реальний MAC адрес зловмисника на MAC жертви, та отримати доступ до мережевих ресурсів системи. Після заміни фізичного адресу зловмисник може перехоплювати пакети в мережі, переглядати незашифрований трафік.

Тип загрози: атака мережевого рівня.

`

Рівень загрози: високий.

Для захисту від таких атак потрібно:

1. Налаштування захисту Port Security на мережевому обладнанні.
2. Автентифікація користувачів на мережевому рівні
3. Шифрування трафіку в мережі
4. Моніторинг мережевого трафіку

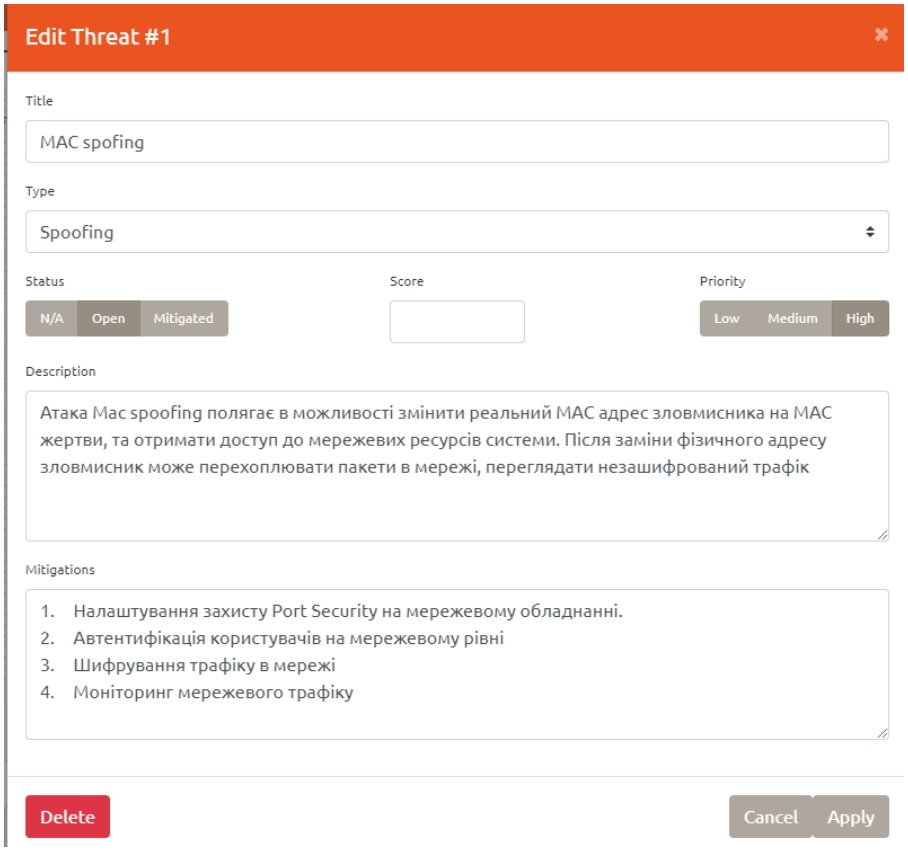


Рисунок 2.47 – Опис загрози Mac spoofing

Атака Mac flooding використовується для переповнення таблиці MAC адрес на мережевому обладнанні шляхом генерації випадкових адрес і пристрої, що перевантажує потік даних у мережі.

Тип загрози: атака мережевого рівня.

Рівень загрози: високий.

Для захисту від таких атак потрібно:

1. Встановлення обмеження пропускної здатності.
2. Використання механізмів захисту Port Security
3. Використання статичних адрес

`

4. Використання систем моніторингу мережевого трафіку.

5. Оновлення програмного забезпечення.

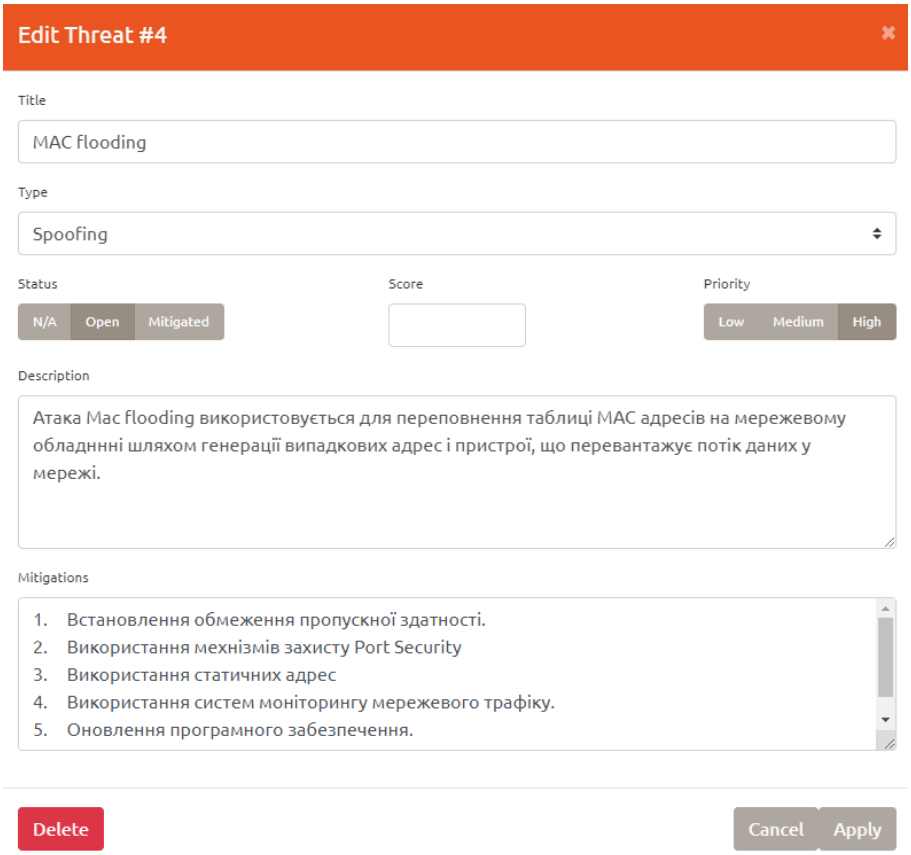


Рисунок 2.48 – Опис загрози Mac flooding

ARP Spoofing атака спрямована на підробку ARP запитів та генерації великої кількості фальшивих запитів які завантажують мережу.

Тип загрози: атака мережевого рівня.

Рівень загрози: високий.

Для захисту від таких атак потрібно:

1. Використання захисту Port Security

2. Встановлення статичних ARP запитів

3. Використання механізмів автентифікації

4. Використання систем IDS/IPS для моніторингу системи.

5. Налаштування фаєрвола системи

`

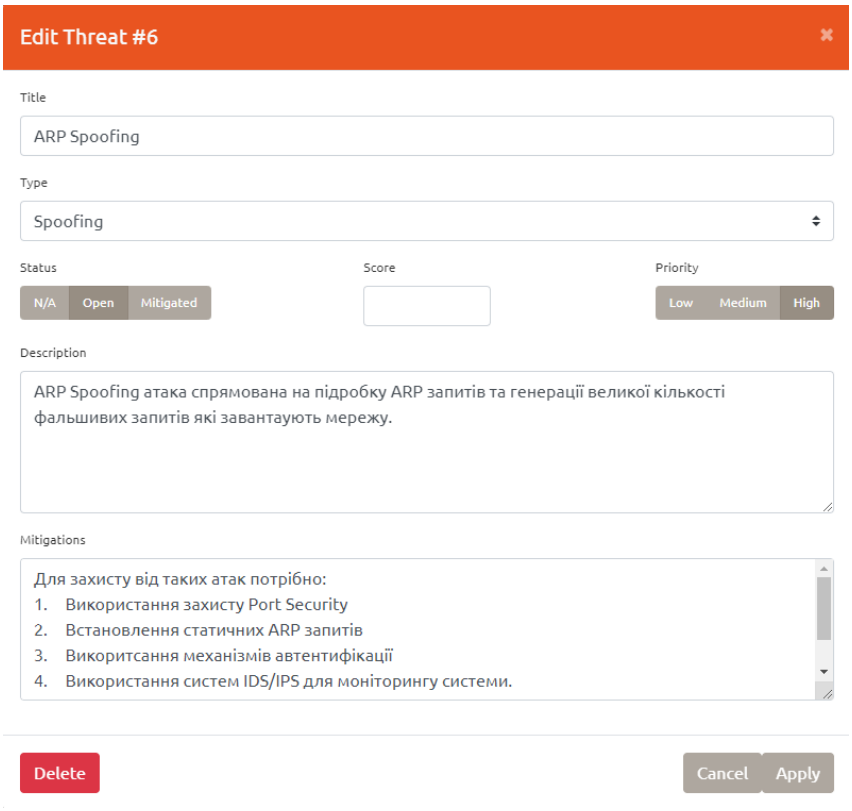


Рисунок 2.49 – Опис загрози ARP spoofing

Сканування відкритих портів комп'ютера дозволяє виявити вразливі місця системи які можна атакувати та отримати доступ до файлів системи. Атака на відкритий 445 порт SMB дозволить зловмиснику отримати доступ до спільних файлів системи.

Тип загрози: атака мережевого рівня.

Рівень загрози: високий.

Для захисту від таких атак потрібно:

1. Заборона доступу до портів ззовні в параметрах фаєрвола, або ACL
2. Використання останньої версії протоколу
3. Генерація сильних паролів та імен користувачів
4. Розмежування прав доступу користувачів
5. Встановлення систем IDS/IPS моніторингу мережі

`

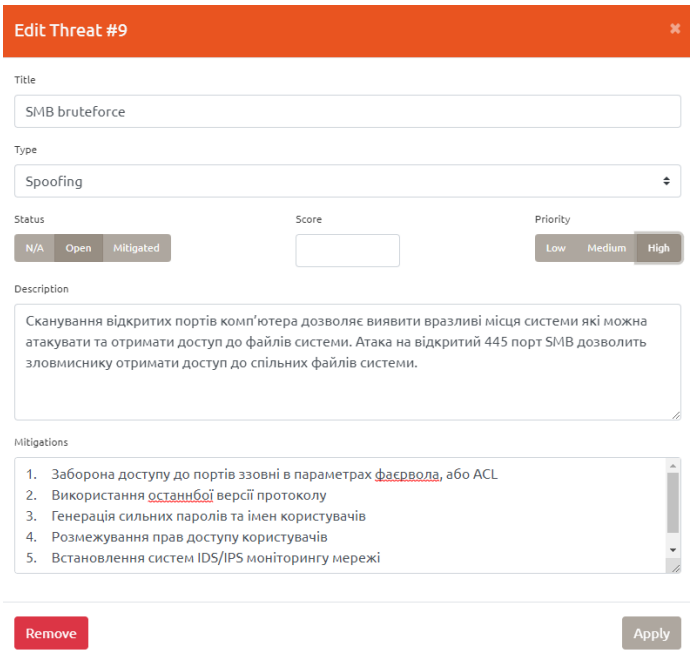


Рисунок 2.50 – Опис загрози SMB bruteforce

Висновки до другого розділу

В даному розділу було описано структуру та алгоритм роботи мережі на основі технології VPN, описано механізм перевірки цілісності даних та аутентифікації користувачів.

Показано розроблену топологію мережі, використане обладнання та його характеристика. Наведено лістинг налаштувань маршрутизатора та комутатора, на яких було зроблено вхід за паролем, створено авторизованих користувачів, віддалений зв'язок по SSH та базові налаштування захисту від несанкціонованого вторгнення.

Продемонстровано розгортання OpenVPN сервера на базі хмарних серверів Connexa та Google Cloud. Налаштовано роботу сервера, та створено захищений тунель між робочими станціями. Продемонстровано віддалений доступ до локальних ресурсів мережі, та підключення звичайних користувачів до сервера.

Наведено модель діаграми загроз мережі на базі протоколу OpenVPN та описано атаки на мережу, й заходи боротьби та зменшення наслідків атак.

`

РОЗДІЛ 3 НАЛАШТУВАННЯ, ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ ТА ЗАХИЩЕНОСТІ МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЇ OPENVPN

3.1 Налаштування OpenVPN сервера на операційній системі Windows

OpenVPN є кросплатформеним та може бути налаштованим як на різних операційних системах:Windows, Linux, Mac. Більшість користувачів використовують Windows, тому налаштування буде саме на ньому.

Наступним кроком буде налаштування роботи сервера, створення всіх необідних ключів та сертифікатів. Створення конфігураційного файлу та налаштування коректної роботи[21].

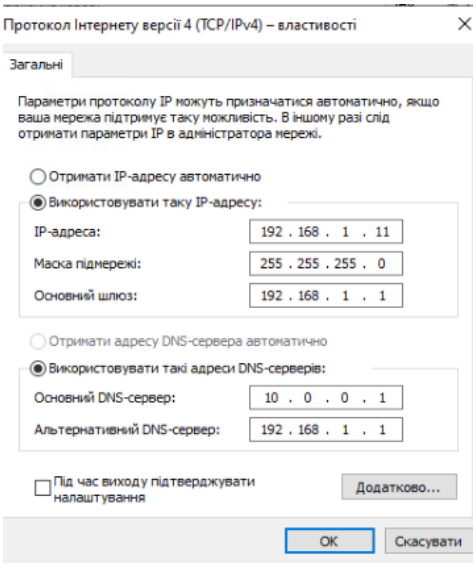


Рисунок 3.1 – Налаштування маршрутизації на сервері

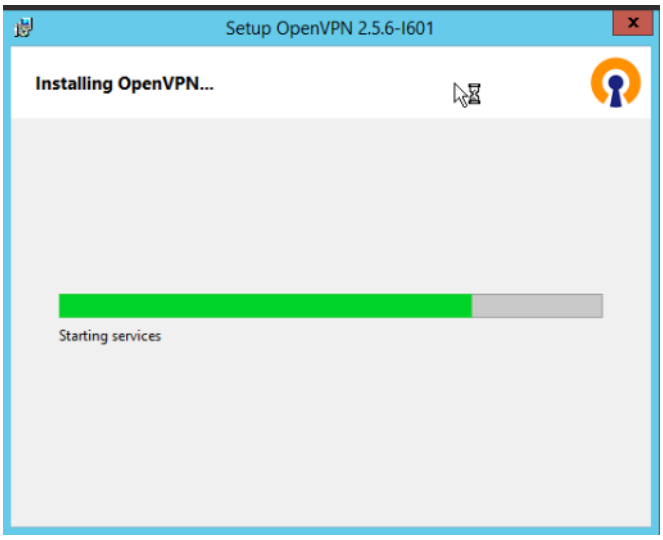


Рисунок 3.2 – Встановлення OpenVPN server на Windows 10

```
set_var EASYRSA_REQ_COUNTRY "UA"
set_var EASYRSA_REQ_PROVINCE    "Kiev"
set_var EASYRSA_REQ_CITY    "Kiev"
set_var EASYRSA_REQ_ORG "Vovk VPN"
set_var EASYRSA_REQ_EMAIL   "kb192_vvo@student.ztu.edu.ua"
set_var EASYRSA_REQ_OU      "VPN_serv"
```

Рисунок 3.3 - Внесення правок в налаштування центра сертифікації

```
EasyRSA Shell
# ./easyrsa init-pki

Note: using Easy-RSA configuration from: ./vars
path = /temp/easy-rsa-7692.a04532/tmp.XXXXXX
lpPathBuffer = C:\Users\ADMINI~1\AppData\Local\Temp\
szTempName = C:\Users\ADMINI~1\AppData\Local\Temp\tmp6716.tmp
path = C:\Users\ADMINI~1\AppData\Local\Temp\tmp6716.tmp
fd = 3

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: C:/Program Files/OpenVPN/easy-rsa/pki
```

Рисунок 3.4 - Запуск BAT файлу EasyRSA та створення директорії pki

```
C:\Windows\system32\cmd.exe
# ./easyrsa build-ca

Note: using Easy-RSA configuration from: ./vars
Using SSL: C:/Program Files/OpenVPN/bin/openssl.exe OpenSSL 1.1.1n  15 Mar 2022
path = /temp/easy-rsa-8716.a07652/tmp.XXXXXX
lpPathBuffer = C:\Users\ADMINI~1\AppData\Local\Temp\
szTempName = C:\Users\ADMINI~1\AppData\Local\Temp\tmp4AAB.tmp
path = C:\Users\ADMINI~1\AppData\Local\Temp\tmp4AAB.tmp
fd = 3
path = /temp/easy-rsa-8716.a07652/tmp.XXXXXX
lpPathBuffer = C:\Users\ADMINI~1\AppData\Local\Temp\
szTempName = C:\Users\ADMINI~1\AppData\Local\Temp\tmp4BA5.tmp
path = C:\Users\ADMINI~1\AppData\Local\Temp\tmp4BA5.tmp
fd = 3
path = /temp/easy-rsa-8716.a07652/tmp.XXXXXX
lpPathBuffer = C:\Users\ADMINI~1\AppData\Local\Temp\
szTempName = C:\Users\ADMINI~1\AppData\Local\Temp\tmp4CCE.tmp
path = C:\Users\ADMINI~1\AppData\Local\Temp\tmp4CCE.tmp
fd = 3

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)
path = /temp/easy-rsa-8716.a07652/tmp.XXXXXX
lpPathBuffer = C:\Users\ADMINI~1\AppData\Local\Temp\
szTempName = C:\Users\ADMINI~1\AppData\Local\Temp\tmp1E5.tmp
path = C:\Users\ADMINI~1\AppData\Local\Temp\tmp1E5.tmp
fd = 3
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]:

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
C:/Program Files/OpenVPN/easy-rsa/pki/ca.crt
```

Рисунок 3.5 - Створення корінного сертифіката ca.crt

`

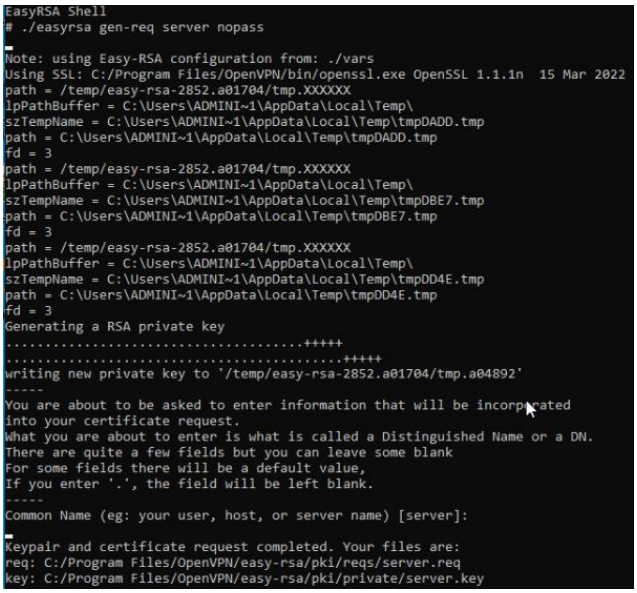


Рисунок 3.6 - Створення сертифіката та ключа сервера

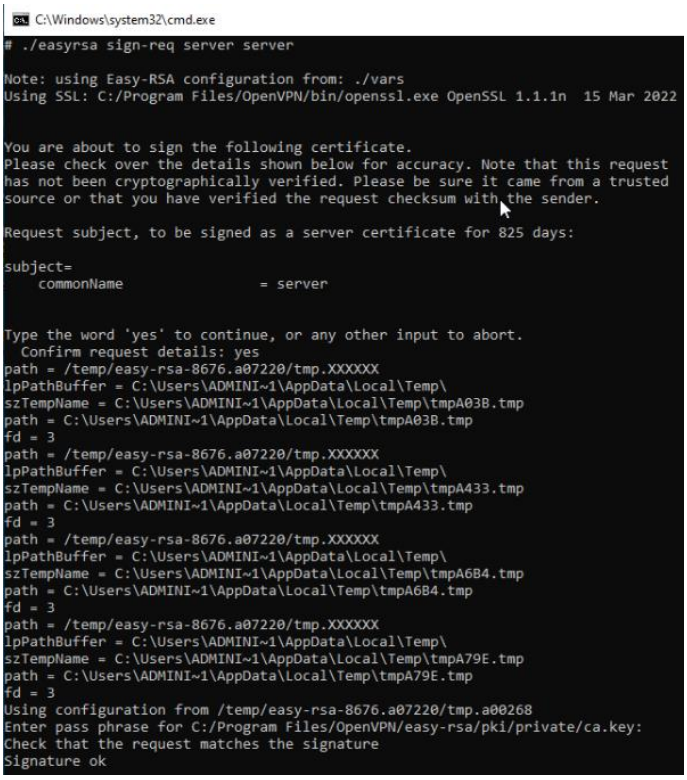


Рисунок 3.7 - Підпис сертифіката створеним ключем

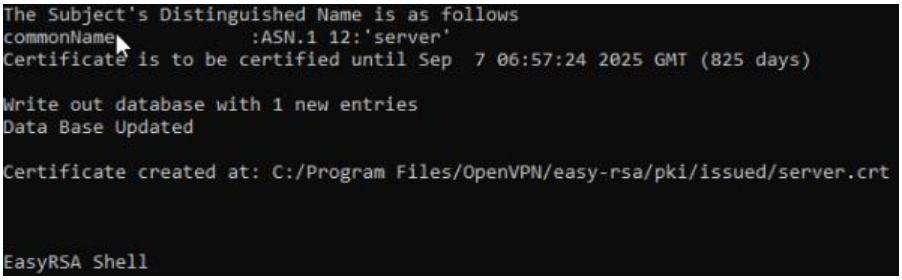


Рисунок 3.8 - Підписаний сертифікат server.crt

`

```
EasyRSA Shell
# ./easyrsa gen-dh

Note: using Easy-RSA configuration from: ./vars
Using SSL: C:/Program Files/OpenVPN/bin/openssl.exe OpenSSL 1.1.1n  15 Mar 2022
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.+..+........+.......................+.....................................
.....................................................................................
```

Рисунок 3.9 - Створення ключа Деффі-Хелмена

```
.....................................................................................
....+.........................+.....................................++*++*++*++*

DH parameters of size 2048 created at C:/Program Files/OpenVPN/easy-rsa/pki/dh.pem
```

Рисунок 3.10 - Згенерований ключ Деффі-Хелмена

```
C:\Program Files\OpenVPN\bin>openvpn --genkey secret ta.key
```

Рисунок 3.11 - Налаштування автентифікації TLS auth

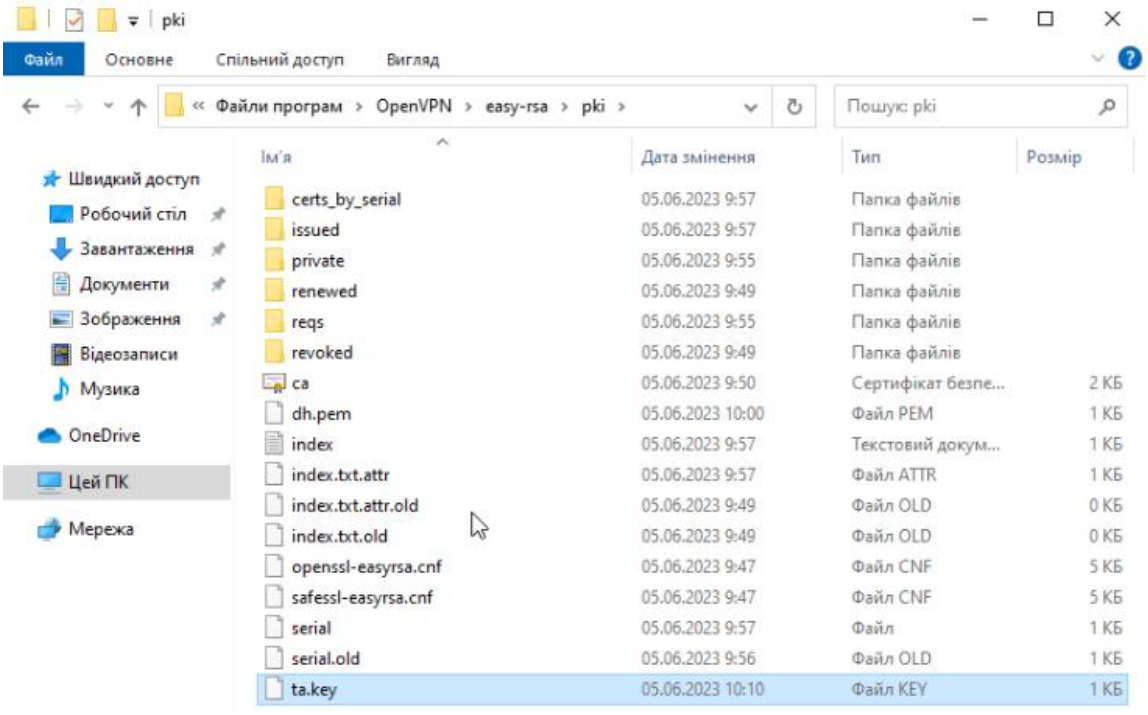


Рисунок 3.12 - Директорія з ключами

Далі налаштуємо конфігураційного файлу сервера. Налаштуємо маршрутизацію трафіка в мережі VPN через сервер, доступ користувачів один до одного, та логування всіх користувачів в окремий файл. Решта налаштувань слугують для захисту мережі, та пришвидшення роботи протоколу.

`

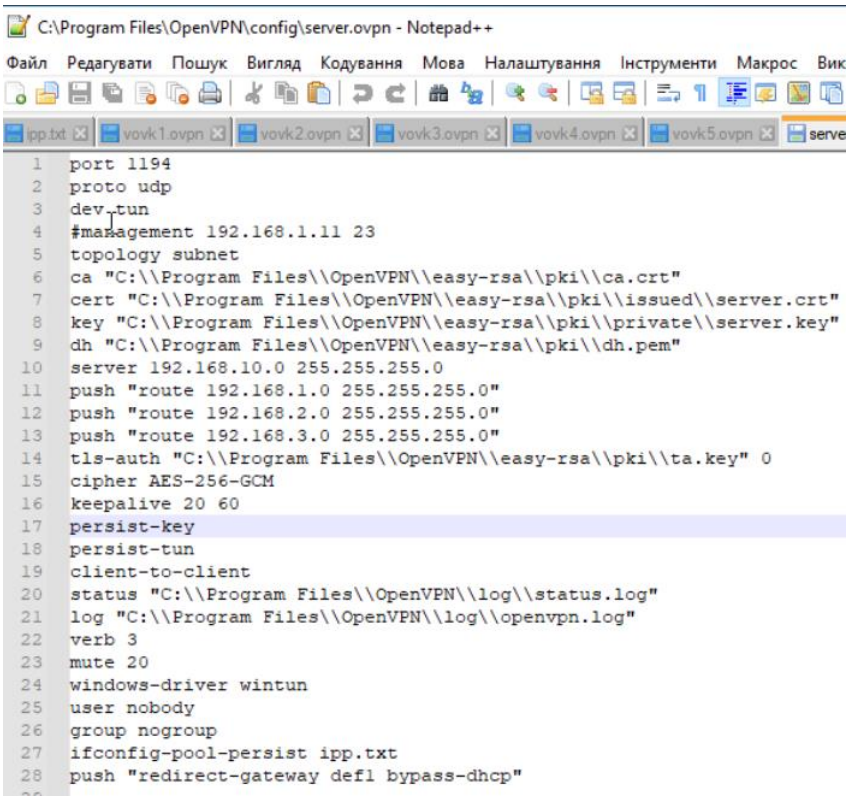


Рисунок 3.13 - Створення конфігураційного файла сервера

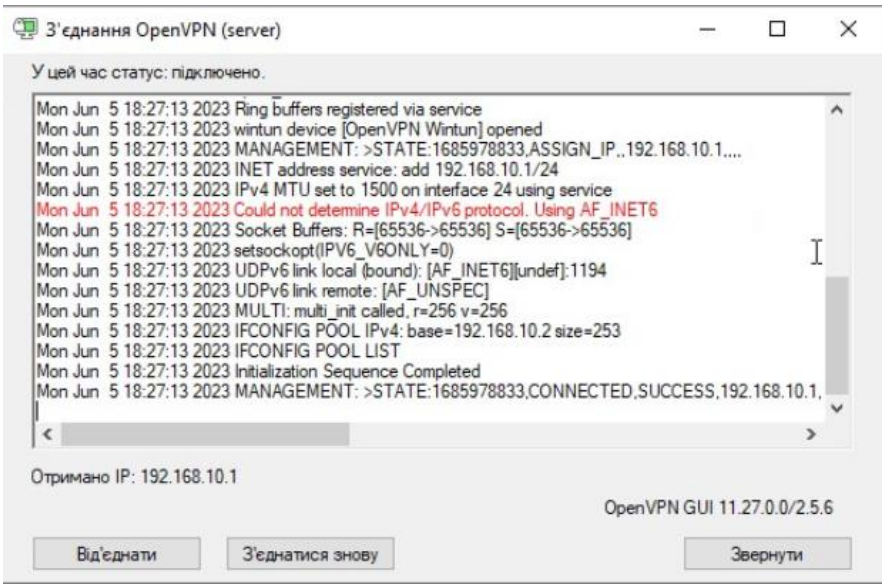


Рисунок 3.14 - Статус сервера

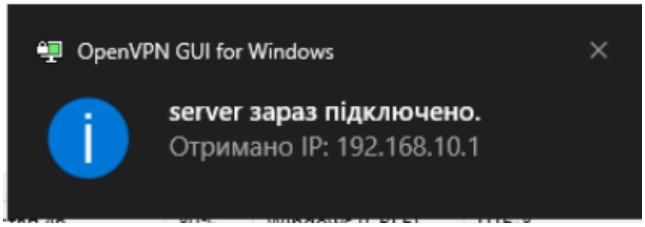


Рисунок 3.15 - Результат успішного з'єднання

`

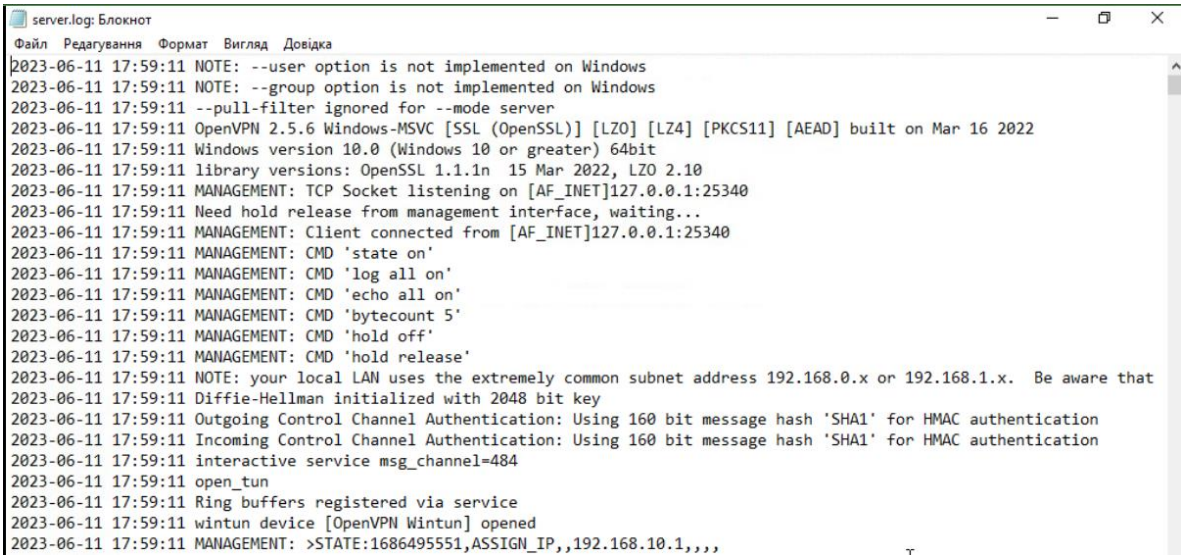


Рисунок 3.16 - Відображення логу сервера

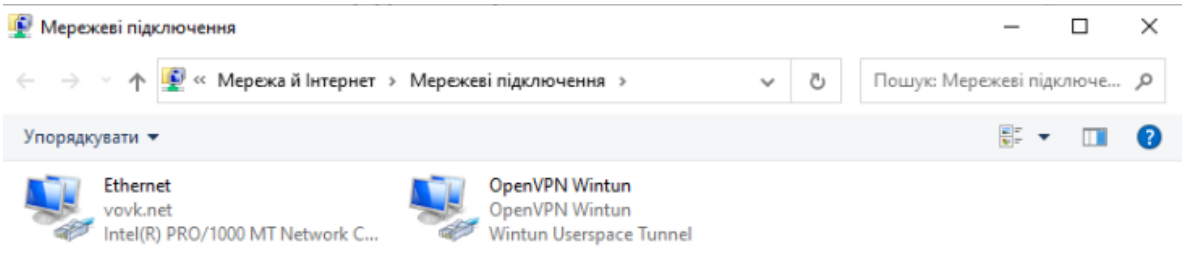


Рисунок 3.17 - Інтерфейс OpenVPN Wintun

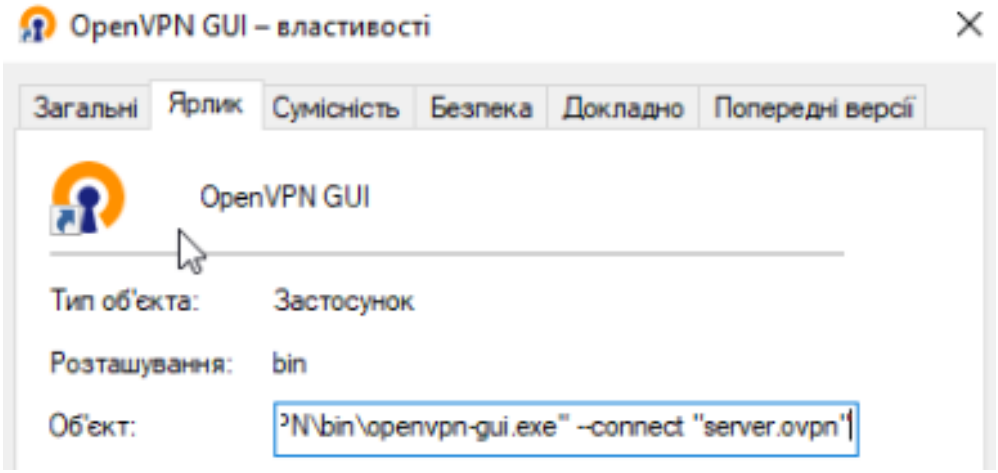


Рисунок 3.18 - Налаштування автозапуску сервера

Переконавшись в працездатності сервера потрібно згенерувати дані для входу користувачів, та створити відповідний конфігураційний файл. Вміст файлу має відповідати параметрам які ми задали в конфігураційному файлі сервера, а інакше клієнт не зможе приєднатися до сервера.

`

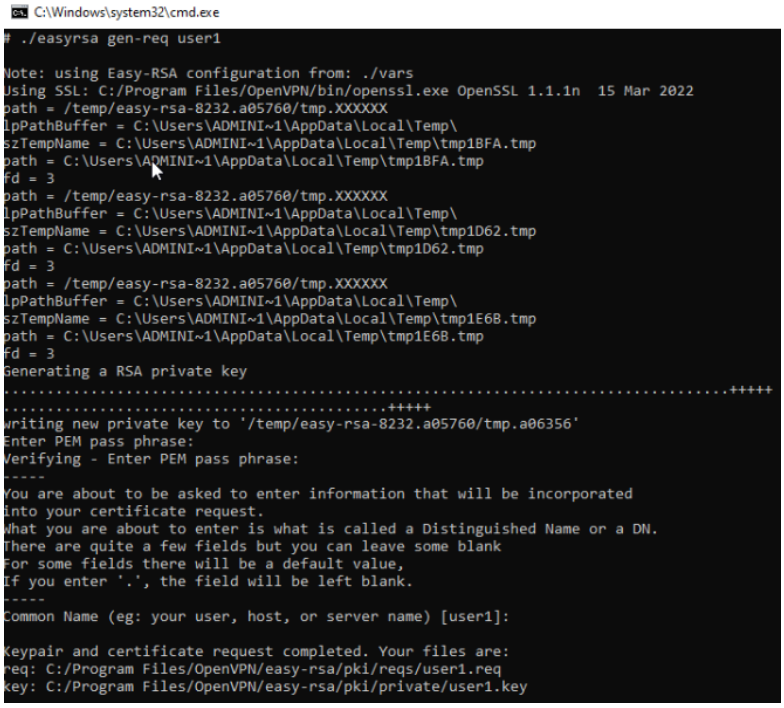


Рисунок 3.19 - Створення ключів для користувача user1

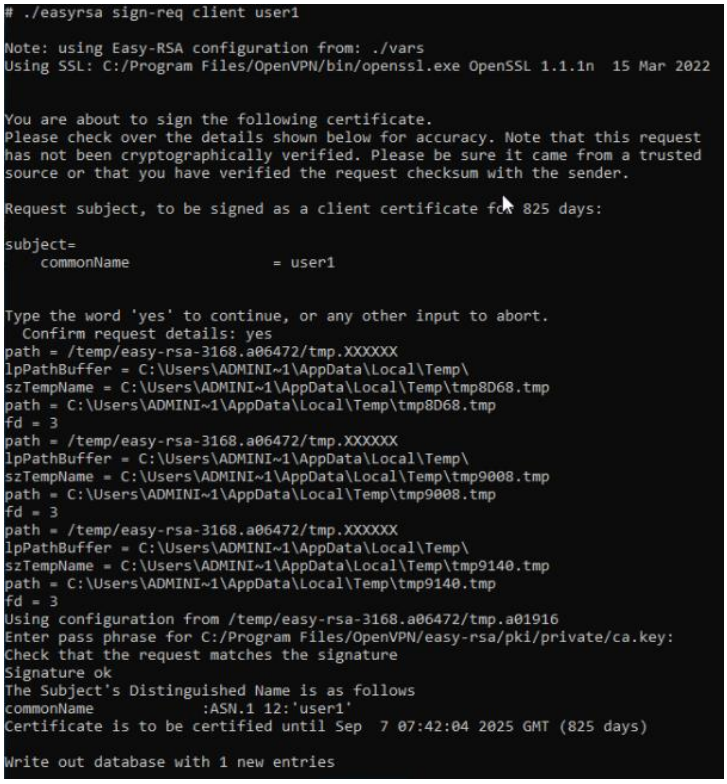


Рисунок 3.20 - Підпис сертифіката user1



Рисунок 3.21 - Створений сертифікат

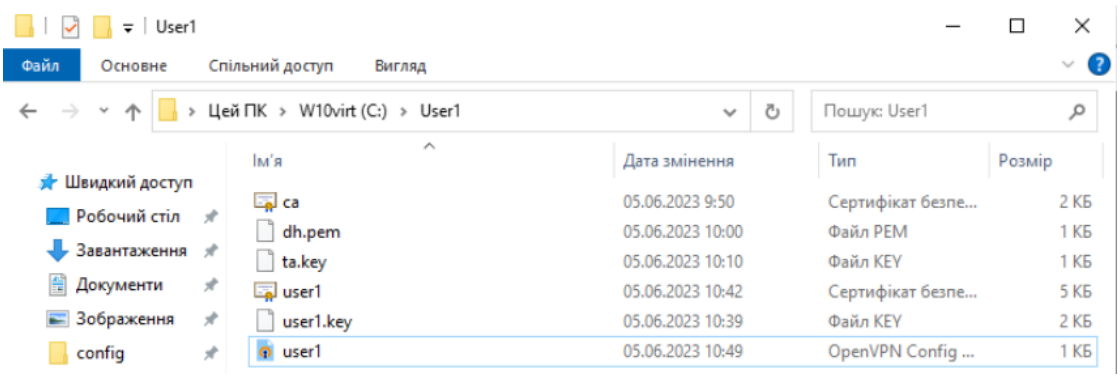


Рисунок 3.22 - Перелік необхідних файлів для користувача

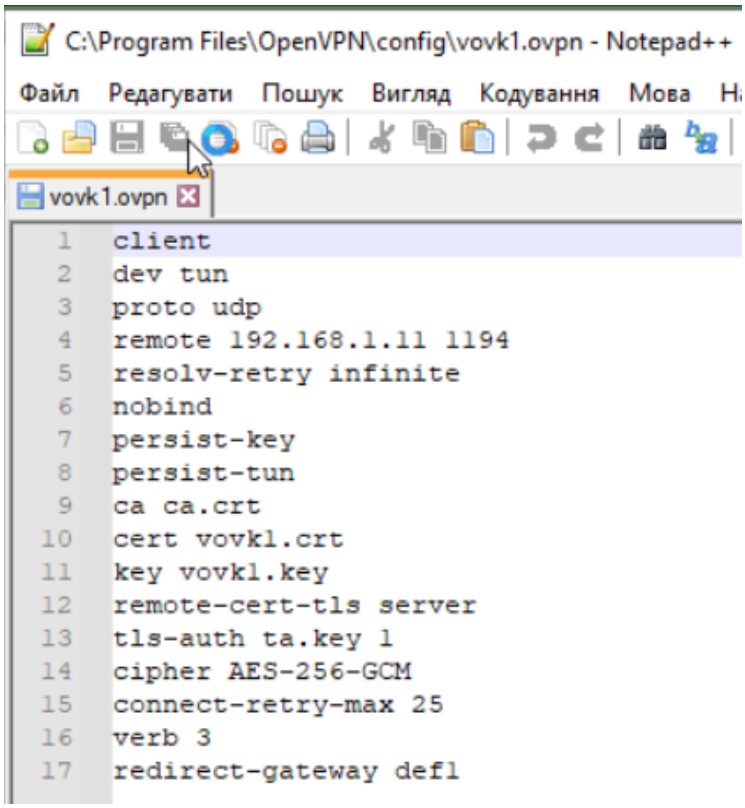


Рисунок 3.23 - Конфігураційний файл користувача

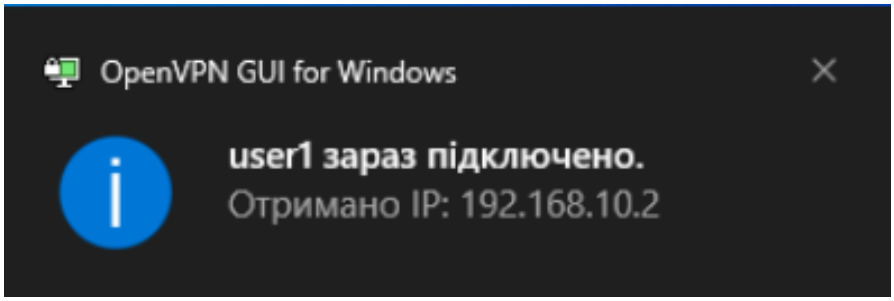


Рисунок 3.24 - Підключення клієнта

`

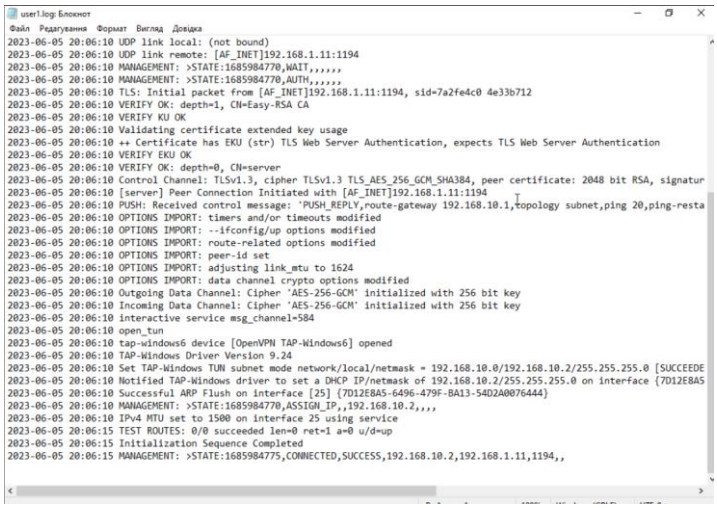


Рисунок 3.25 - Лог сервера після під’єднання користувача user1

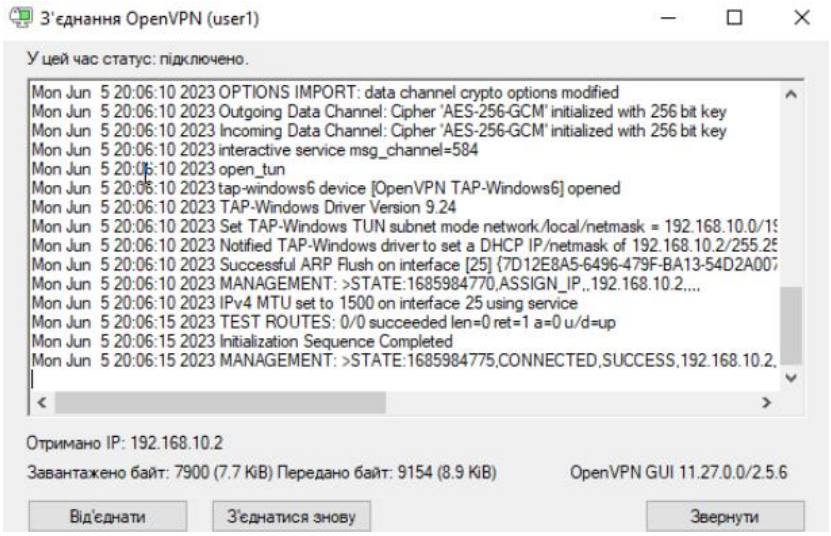


Рисунок 3.26 - Статус з’єднання

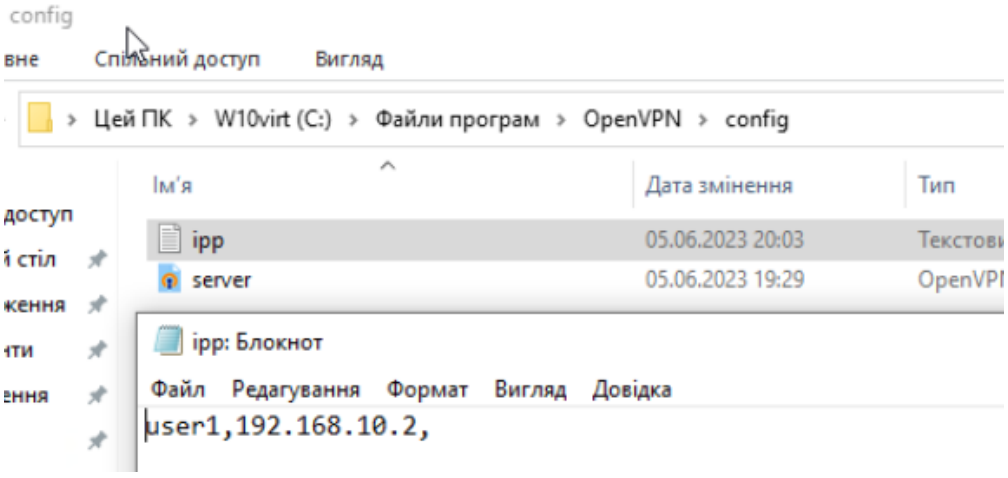


Рисунок 3.27 - Добавлення в таблицю користувачів

3.2 Перевірка працездатності мережі та роботи OpenVPN сервера

Далі потрібно перевірити можливість одночасного під’єднання декількох користувачів. Для цього буде створено користувачів vovk1, vovk2, vovk3.

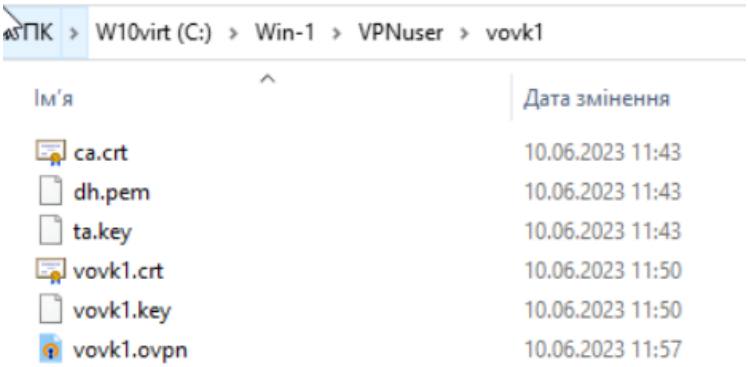


Рисунок 3.28 - Створений користувач vovk1

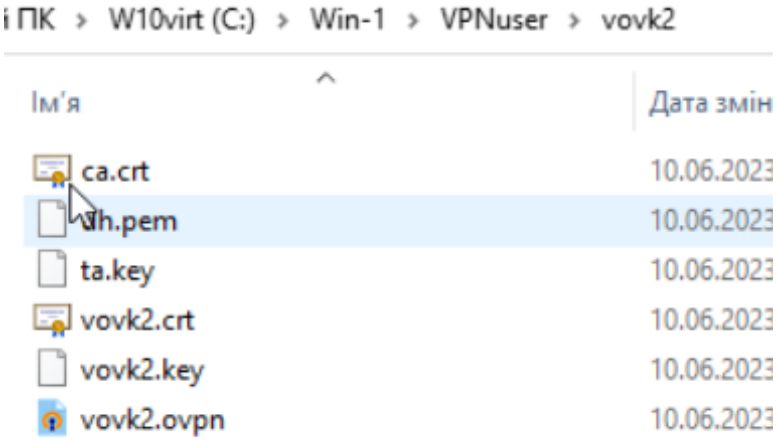


Рисунок 3.29 - Створений користувач vovk2

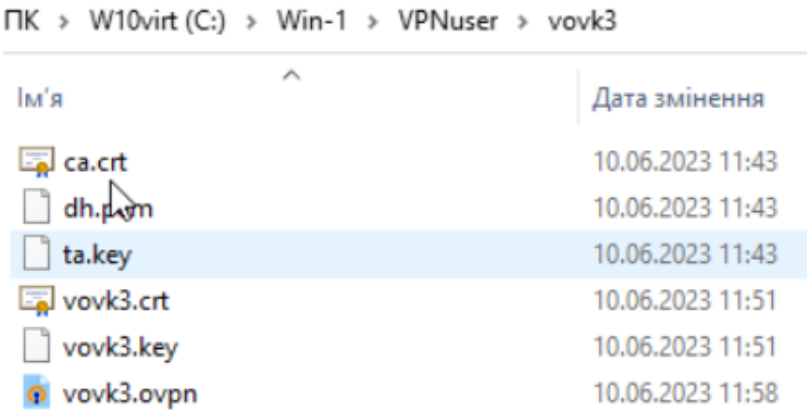


Рисунок 3.30 - Створений користувач vovk3

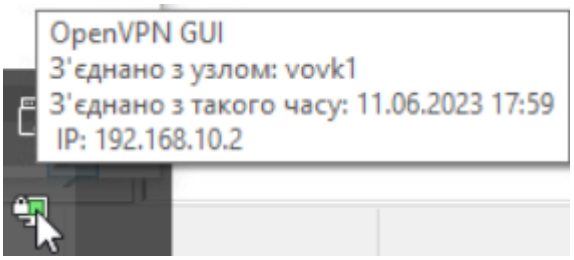


Рисунок 3.31 - Результат з'єднання з сервером користувача vovk1

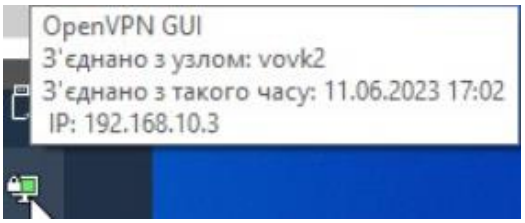


Рисунок 3.32 - Результат з’єднання з сервером користувача vovk2

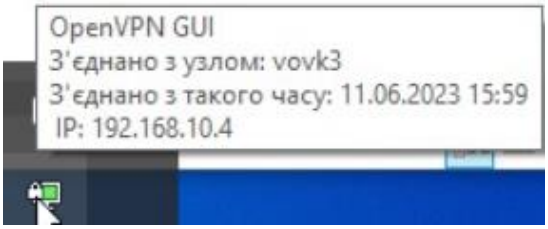


Рисунок 3.33 - Результат з’єднання з сервером користувача vovk3

```
2023-06-12 22:00:14 MULTI: new connection by client 'vovk1' will cause previous active sessions by this client to be dropped.
2023-06-12 22:00:14 MULTI_sva: pool returned IPv4=192.168.10.2, IPv6=(Not enabled)
2023-06-12 22:00:14 MULTI: Learn: 192.168.10.2 -> vovk1/192.168.1.12:58699
2023-06-12 22:00:14 MULTI: primary virtual IP for vovk1/192.168.1.12:58699: 192.168.10.2
2023-06-12 22:00:14 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2023-06-12 22:00:14 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2023-06-12 22:00:14 SENT CONTROL [vovk1]: 'PUSH_REPLY,route 192.168.1.0 255.255.255.0,route 192.168.2.0 255.255.255.0,route 1
```

Рисунок 3.34 - Лог сервера після під’єднання користувача vovk1

```
2023-06-12 22:00:18 MULTI: Learn: 192.168.10.3 -> vovk2/192.168.2.11:50715
2023-06-12 22:00:18 MULTI: primary virtual IP for vovk2/192.168.2.11:50715: 192.168.10.3
2023-06-12 22:00:18 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2023-06-12 22:00:18 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2023-06-12 22:00:18 SENT CONTROL [vovk2]: 'PUSH_REPLY,route 192.168.1.0 255.255.255.0,route 192.168.2.0 255.255.255.0,route 1
```

Рисунок 3.35 - Лог сервера після під’єднання користувача vovk2

```
2023-06-12 22:00:24 MULTI_sva: pool returned IPv4=192.168.10.4, IPv6=(Not enabled)
2023-06-12 22:00:24 MULTI: Learn: 192.168.10.4 -> vovk3/192.168.3.11:63132
2023-06-12 22:00:24 MULTI: primary virtual IP for vovk3/192.168.3.11:63132: 192.168.10.4
2023-06-12 22:00:24 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2023-06-12 22:00:24 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2023-06-12 22:00:24 SENT CONTROL [vovk3]: 'PUSH_REPLY,route 192.168.1.0 255.255.255.0,route 192.168.2.0 255.255.255.0,route 1
```

Рисунок 3.36 - Лог сервера після під’єднання користувача vovk3

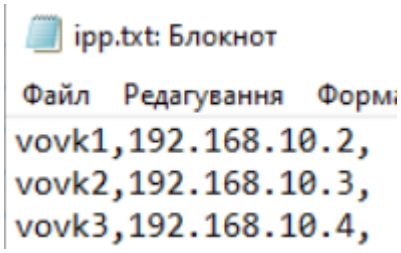


Рисунок 3.37 - Добавлення в таблицю користувачів

`

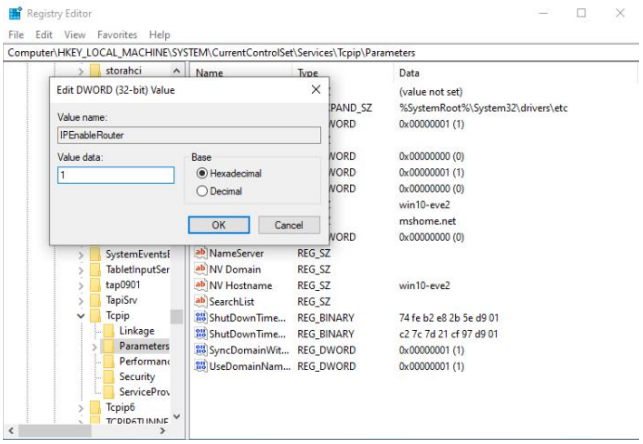


Рисунок 3.38 - Налаштовуємо можливість маршрутизації трафіку в мережі

Для підтвердження кросплатформеної роботи сервера створимо користувача для Mac Sierra. Виконаємо налаштування маршрутизації, на сервері згенеруємо відповідні ключі, та встановимо Tunnelblick без якого ми не під'єднаємося до сервера.

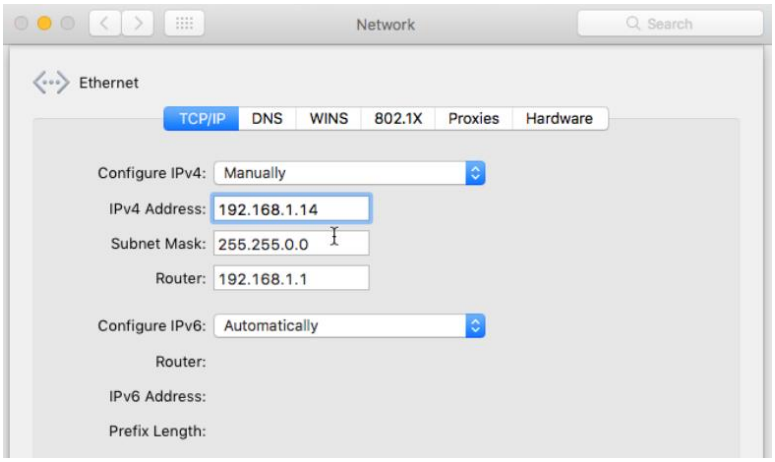


Рисунок 3.39 – налаштування маршрутизації Mac Sierra

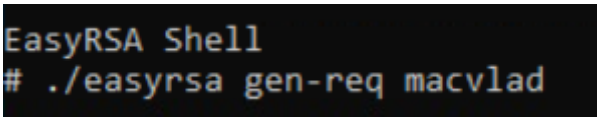


Рисунок 3.40 – створення ключа для macvlad



Рисунок 3.41 - створення сертифіката для macvlad

`



Рисунок 3.42 – встановлення Tunnelblick для налаштування тунелю



Рисунок 3.43 – відкриття конфігураційного файлу

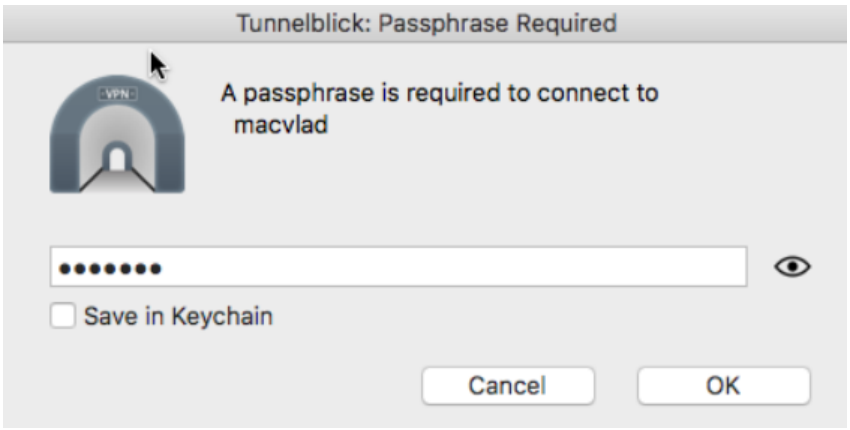


Рисунок 3.44 – авторизація користувача macvlad

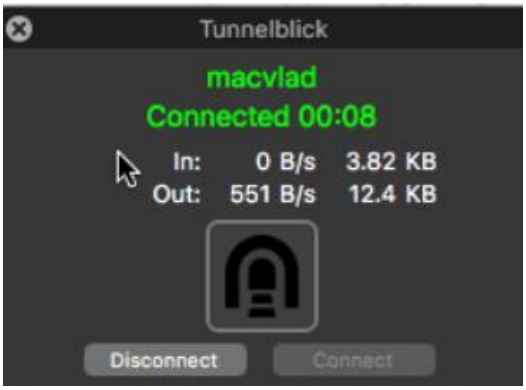


Рисунок 3.45 – Результат успішного з’єднання

`

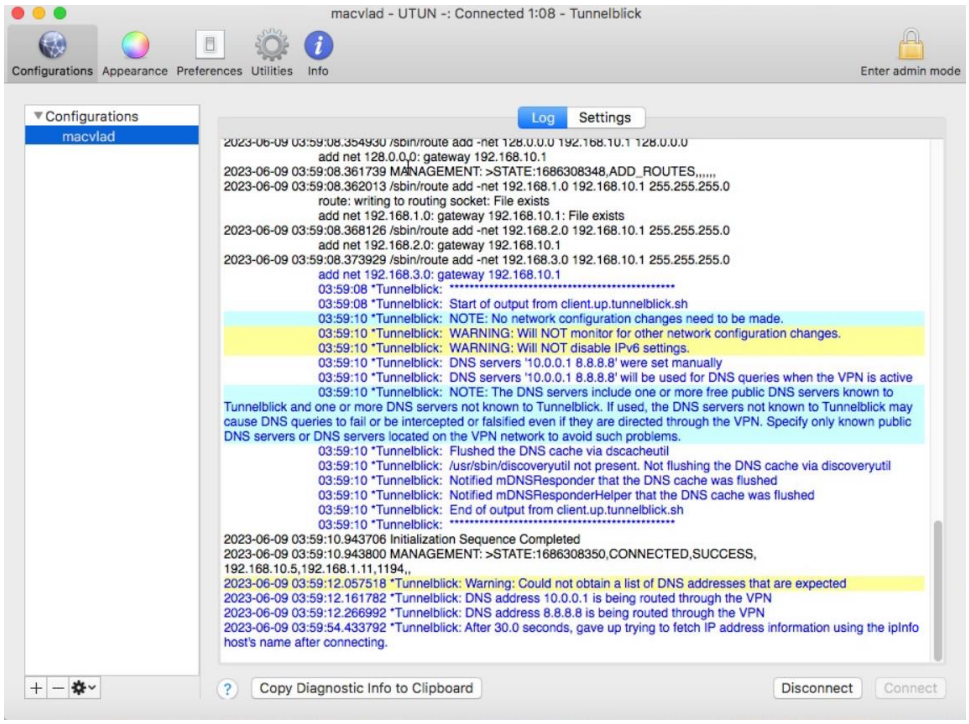


Рисунок 3.46 – Статус з’єдання

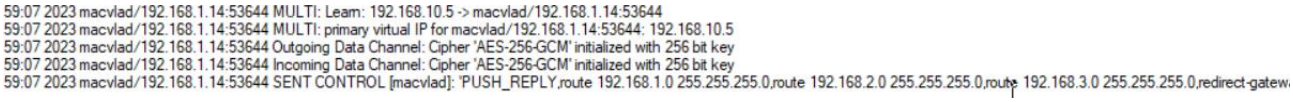


Рисунок 3.47 – Лог сервера після підключення користувача macvlad

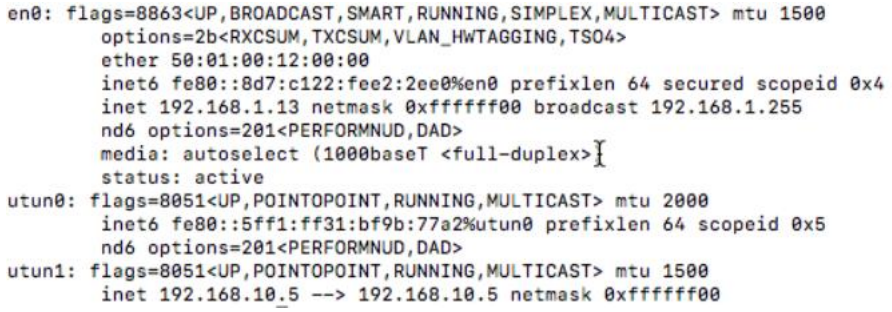


Рисунок 3.48 – створений інтерфейс на Mac Sierra

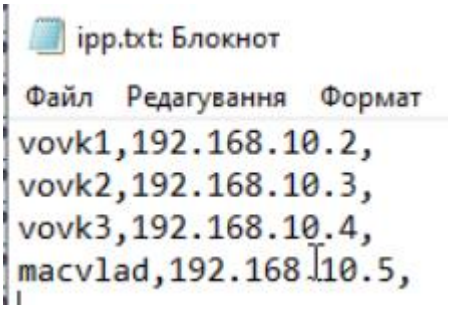


Рисунок 3.49 – підключений користувач macvlad

Для повноцінного функціонування сервера потрібно налаштувати права доступу та фаєрвола. Будуть створені правила та винятки які допоможуть системі повноцінно функціонувати.

`

OpenVPN працює з 1194 UDP та TCP портом, тому їх потрібно додати у винятки. В налаштуваннях фаєрвола додамо OpenVPN у винятки, щоб випадково його не заблокувати. Дозволимо exo-пакети ICPM, щоб бачити сусідні машини. SMB протокол дозволимо тільки для мережі 192.168.10.0/24, а порти 22, 80, 443, 445, 1194 додамо у виняток. Решта портів заблокується для захисту мережі від вторгнення.

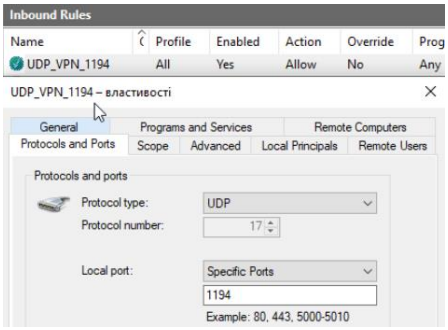


Рисунок 3.50 – UDP 1194



Рисунок 3.51 – TCP 1194



Рисунок 3.52 – винятки

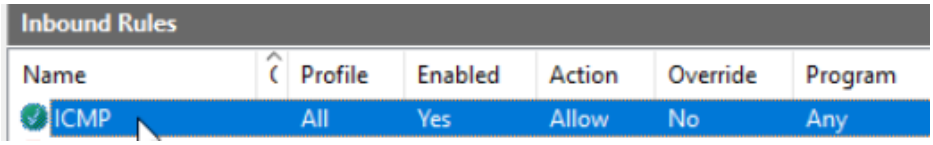


Рисунок 3.53 – exoICMP для пінгування машин



Рисунок 3.54 – 445 SMB OpenVPN

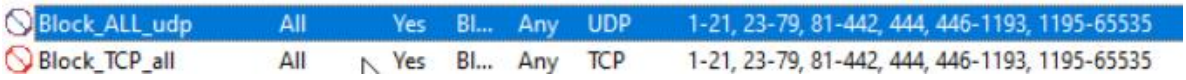


Рисунок 3.55 – UDP TCP блокування

3.2 Перевірка працездатності мережі та тестування правил безпеки

Потрібно здійснити діагностичні команди та перевірити працездатність налаштувань.

`

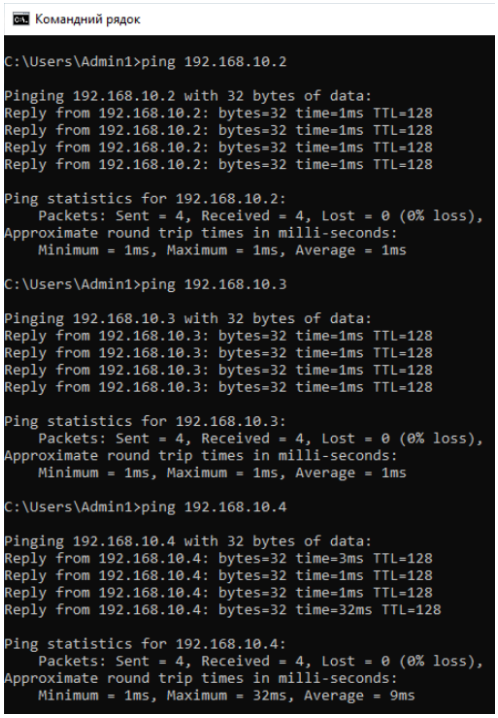


Рисунок 3.56 – перевірка зв’язку з користувачами по тунелю

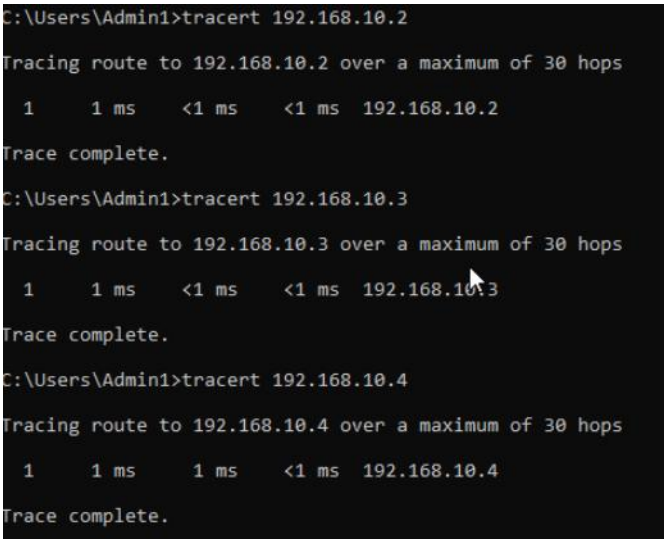


Рисунок 3.57 – Перевірка пройденого шляху користувачів

Створимо мережеву теку та звичайного користувача для перевірки роботи зі спільними теками.

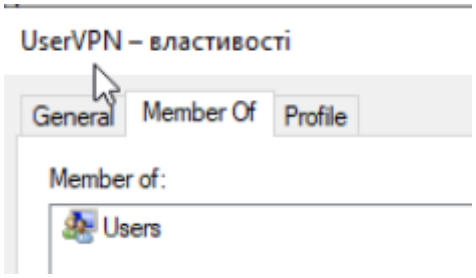


Рисунок 3.58 - UserVPN

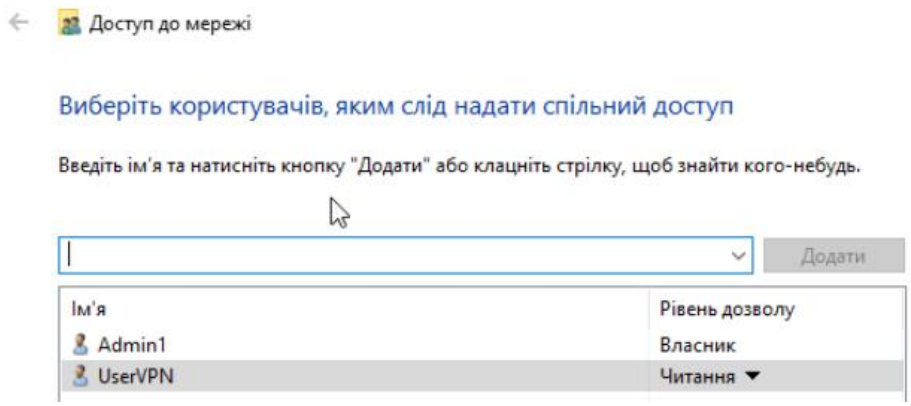


Рисунок 3.59 - Спільний доступ до теки VPN_test для UserVPN з правами читання

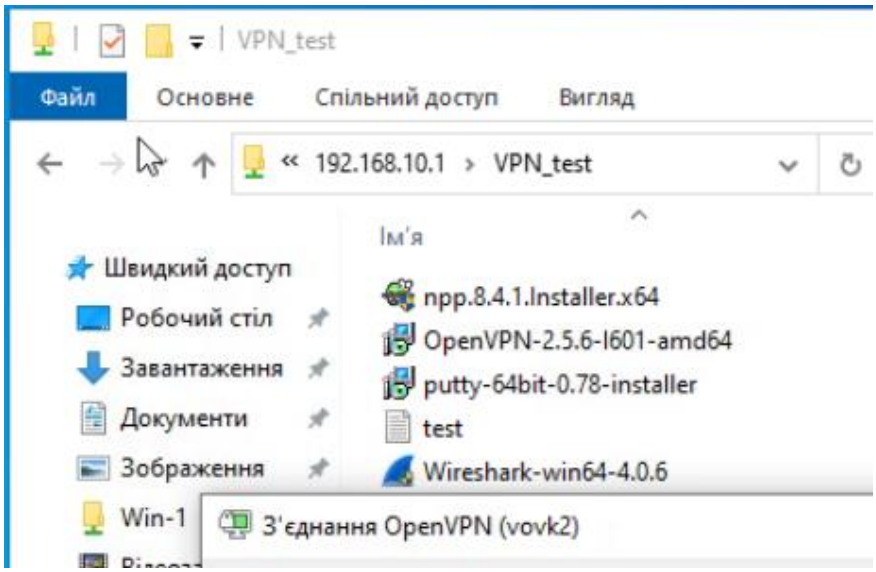


Рисунок 3.60 – Вхід під користувачем UserVPN

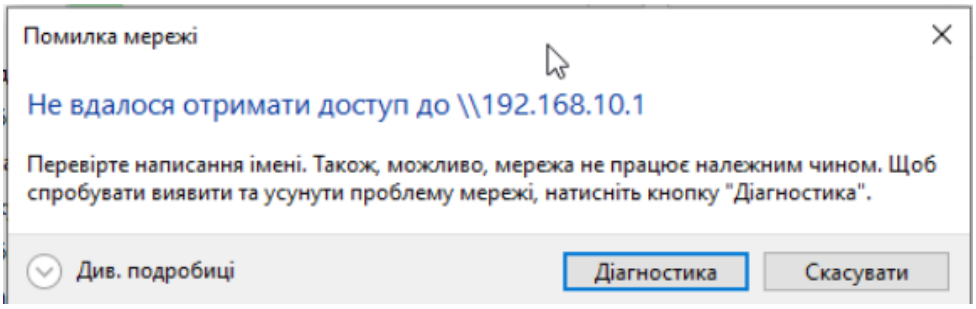


Рисунок 3.61 – Спроба зайти без VPN з’єднання

`

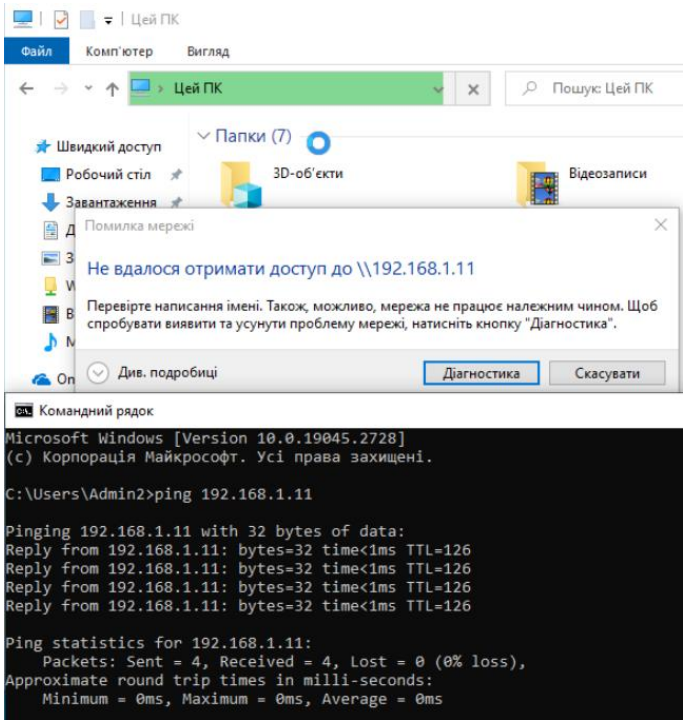


Рисунок 3.62 – Спроба зайти до серверу по локальному IP.

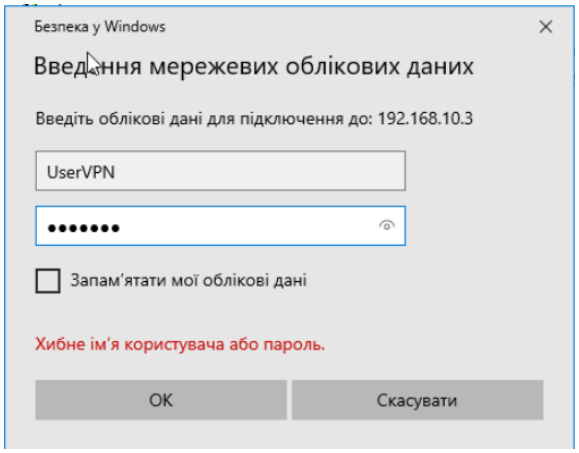


Рисунок 3.63 – Вхід під створеним користувачем UserVPN з правами читання

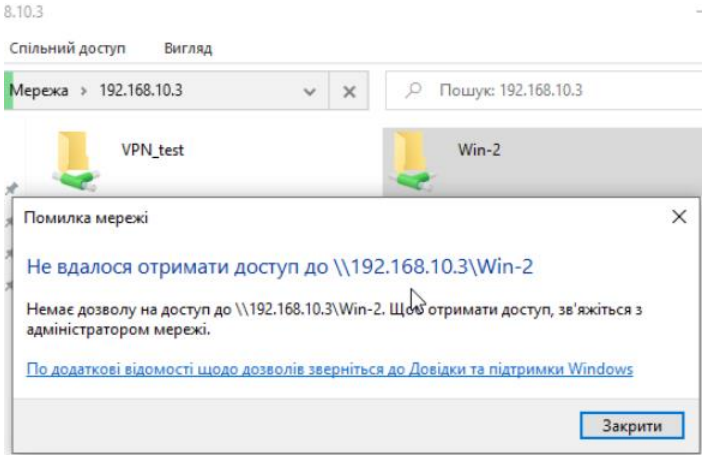


Рисунок 3.64 – Відмова у доступі

`

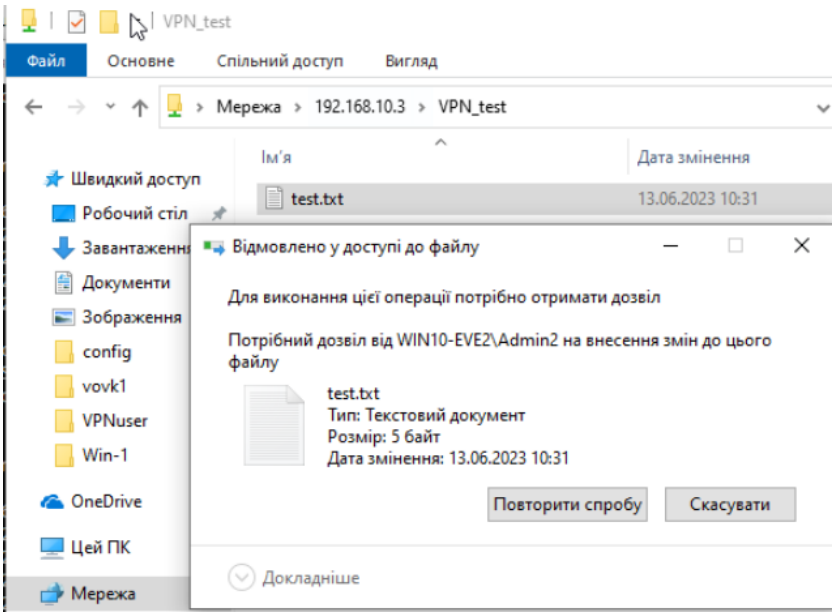


Рисунок 3.65 – Спроба видалення файлу test.txt

OpenVPN використовує захищений тунель, а дані в середині зашифровані, тому при спробі перехопити пакети ми бачимо набір знаків і цифр.

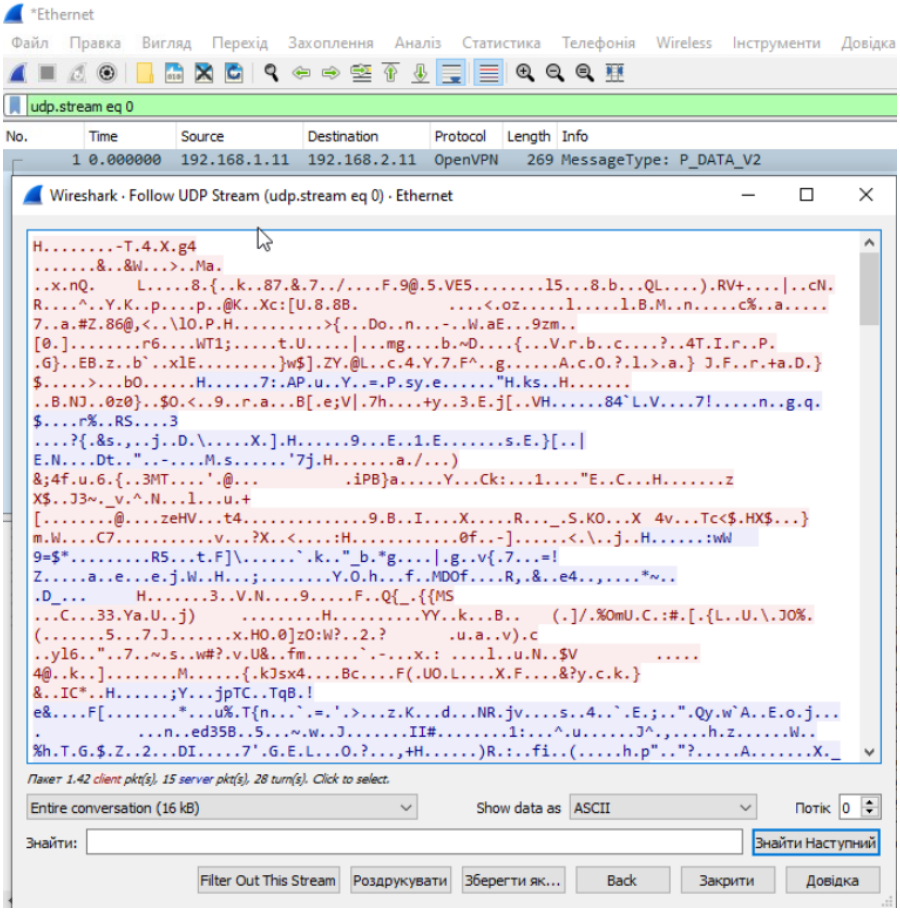


Рисунок 3.66 – Спроба перехопити пакет OpenVPN

`

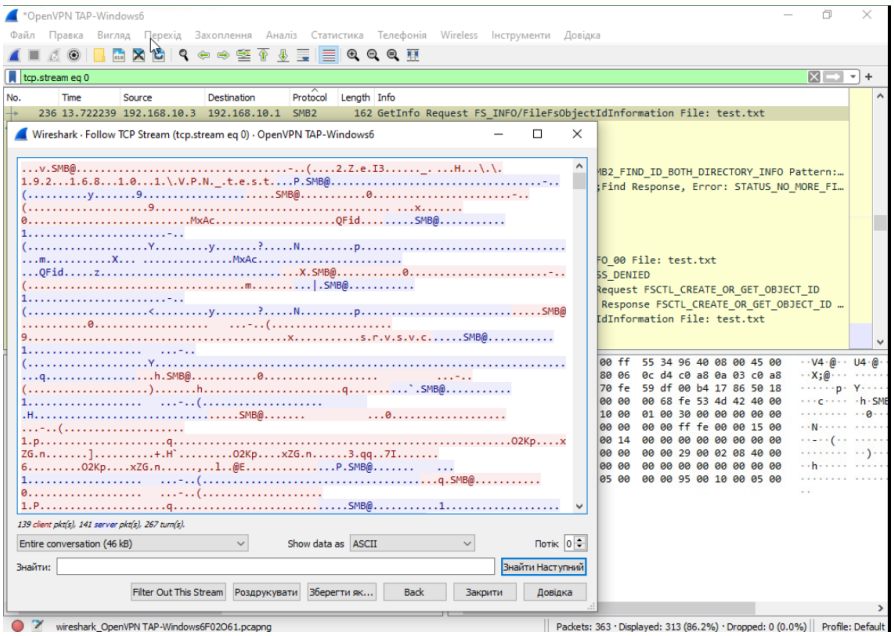


Рисунок 3.67 – Спроба перехоплення файлу test.txt

3.3Тестування мережі на проникнення

Для перевірки захищеності системи ми використаємо Kali Linux, який має широкий набір програм та інструментів для аудиту.

Виконаємо bruteforce атаку на протокол SHH, та спробуємо під’єднатися до R-1.

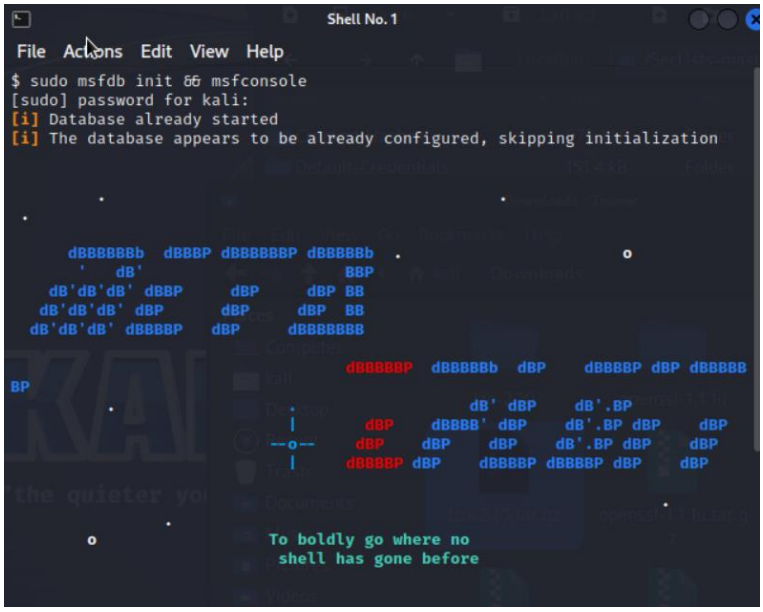


Рисунок 3.68 – Використання набору скриптів metaspolit

`

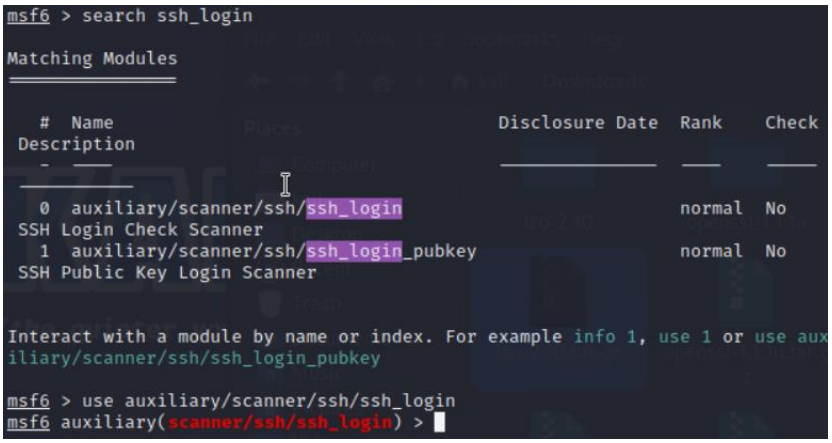


Рисунок 3.69 – Вибираємо скрипт атаки на SSH

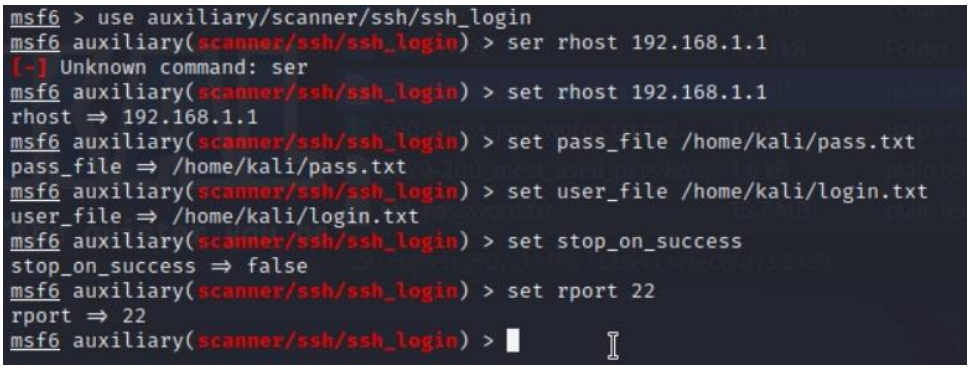


Рисунок 3.70 – Задаємо параметри атаки на R-1

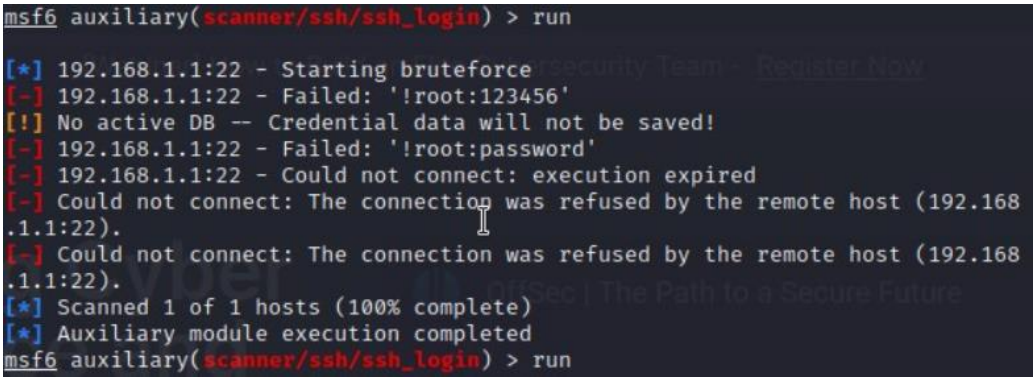


Рисунок 3.71 – Блокування спроби після перевищення ліміту під’єднання

Використання Mac spoofing змінює mac адрес вашого пристрою, що допомагає обійти різні мережеві захисти, й отримати доступ до мереж.

Використаємо інструмент Macchanger та замінимо mac адрес Kali linux на Sierra та обійдемо switchport security.

`

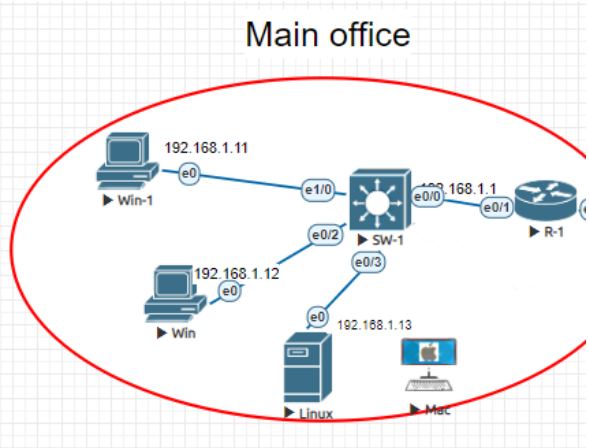


Рисунок 3.72 встановлення Kali linux на місце Mac Sierra

```
*Jun 14 13:19:26.045: %PM-4-ERR DISABLE: psecure-violation error detected on Et0/3, putting Et0/3 in err-disable state
SW-1#
*Jun 14 13:19:26.045: %PORT SECURITY-2-PSECURE VIOLATION: Security violation occurred, caused by MAC address 0050.0100.0c00 on port Ethernet0/3.
*Jun 14 13:19:27.047: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down
SW-1#
*Jun 14 13:19:28.051: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to down
```

Рисунок 3.73 Спрацювання port security на невідомий mac адрес

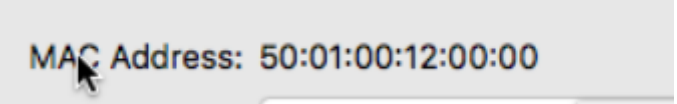


Рисунок 3.74 Дізнаємося мак адрес Sierra

```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.6  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::ebd6:1c54:61f4:5ade  prefixlen 64  scopeid 0x20<link>
        ether 00:50:01:00:0c:00  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 855 (855.0 B)
        RX errors 0  dropped 7  overruns 0  frame 0
        TX packets 69  bytes 10138 (9.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1344 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1344 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali]
└─# ifconfig eth0 down

┌──(root㉿kali)-[/home/kali]
└─# macchanger -m 50:01:00:12:00:00
GNU MAC Changer
Usage: macchanger [options] device

Try `macchanger --help' for more options.

┌──(root㉿kali)-[/home/kali]
└─# macchanger -m 50:01:00:12:00:00 eth0
Current MAC:   00:50:01:00:0c:00 (YAMASHITA SYSTEMS CORP.)
Permanent MAC: 00:50:01:00:0c:00 (YAMASHITA SYSTEMS CORP.)
New MAC:       50:01:00:12:00:00 (unknown)

┌──(root㉿kali)-[/home/kali]
```

Рисунок 3.75 Замінюємо mac адрес на вже відомий нам

`

```
SW-1#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
Ethernet1/0            unassigned      YES unset  up                    up
Ethernet1/1            unassigned      YES unset  administratively down down
Ethernet1/2            unassigned      YES unset  administratively down down
Ethernet1/3            unassigned      YES unset  administratively down down
Vlan1                  192.168.1.2     YES NVRAM  up                    up
SW-1#
```

Рисунок 3.76 Перезавантажимо SW-1, і бачимо що інтерфейс не відключився

```
┌──(root㉿kali)-[/home/kali]
└─# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=10.6 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.389 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.464 ms
^C
── 192.168.1.1 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2032ms
rtt min/avg/max/mdev = 0.389/3.822/10.614/4.802 ms

┌──(root㉿kali)-[/home/kali]
└─#
```

Рисунок 3.77 – Зв’язок з роутером

Здійснимо атаку Mac flooding створює потік з фальшивих mac адрес та завантажує трафік хибними повідомленнями, що навантажує систему.

```
kali@kali: ~
File  Actions  Edit  View  Help
Currently scanning: 192.168.109.0/16   |   Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 246

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname

192.168.1.1     aa:bb:cc:00:61:10      1      60  Unknown vendor
192.168.1.2     aa:bb:cc:80:31:00      1      60  Unknown vendor
192.168.1.6     50:01:00:12:00:00      1      42  Unknown vendor
192.168.1.11    50:01:00:0b:00:00      1      42  Unknown vendor
192.168.1.12    50:01:00:09:00:00      1      42  Unknown vendor
```

Рисунок 3.78 Перевіряємо пристрої мережі

`

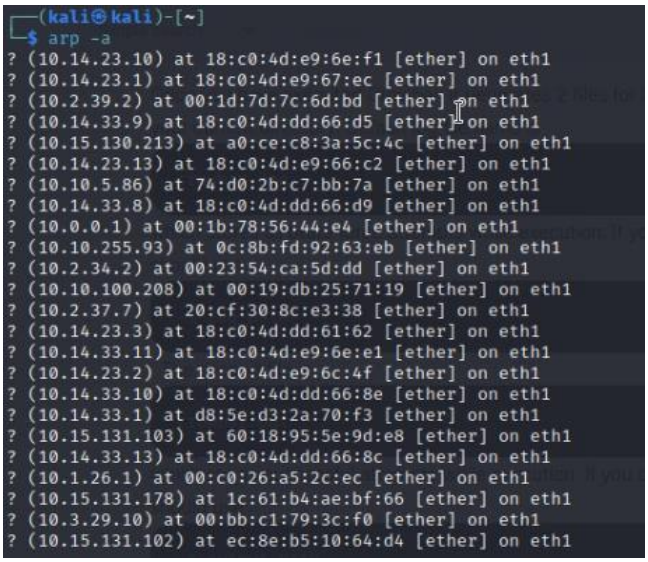


Рисунок 3.79 Вмикаємо мак спуфінг

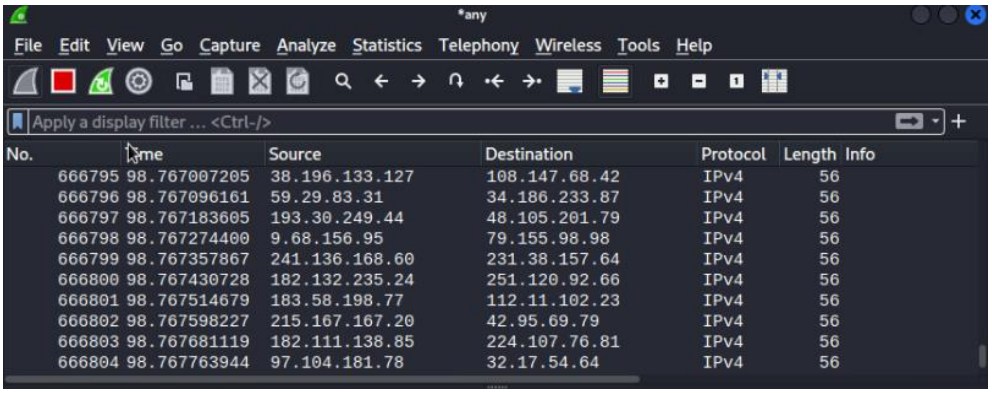


Рисунок 3.80 – Сканування мережі на наявність спуфінгу

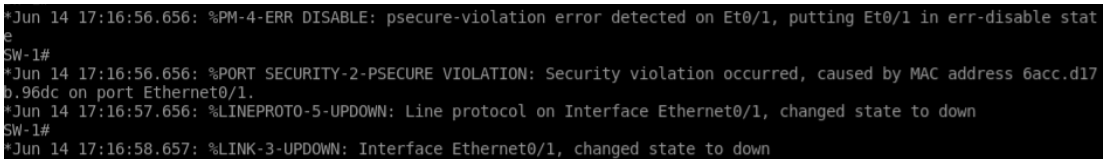


Рисунок 3.81 – Спрацювання Port Security

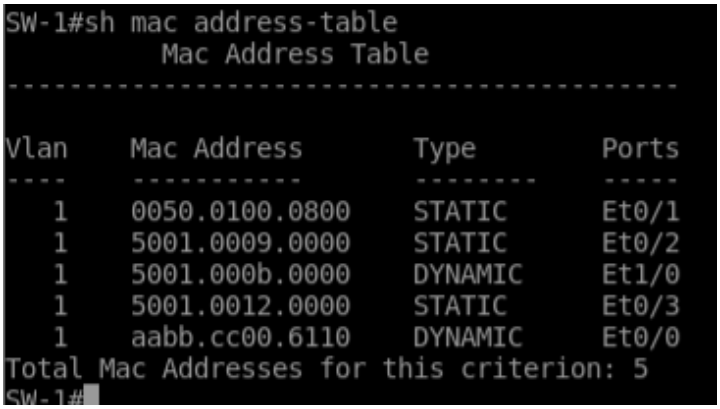


Рисунок 3.82 – Перевірка таблиці mac-адрес

`

ARP spoofing генерує постійний потік ARP запитів та перевантажує мережеву, що призводить до її відмови.

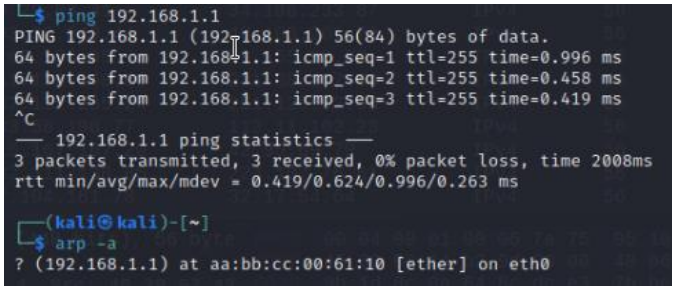


Рисунок 3.83 – Перевірка таблиці ARP

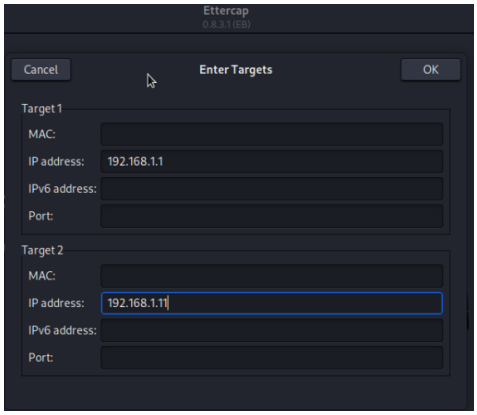


Рисунок 3.84 – Визначаємо цілі в інструменті Ettercap

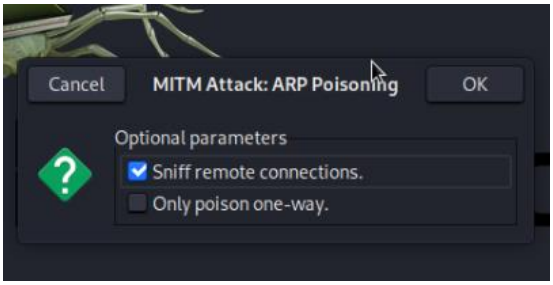


Рисунок 3.85 – Вмикаємо режим ARP Poisoning

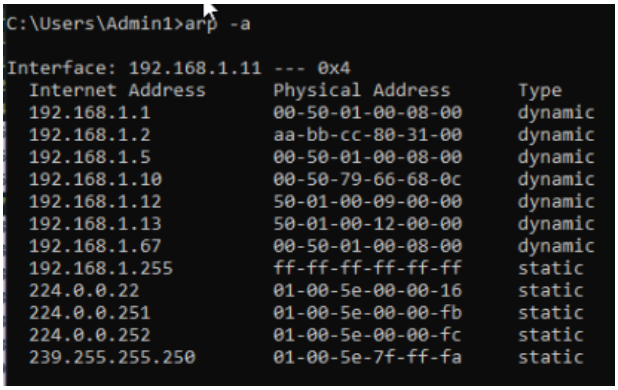


Рисунок 3.86 – Перевірка таблиці ARP запитів

`



Рисунок 3.87 – Спрацювання switchport security

Відкриті порти створюють велику загрозу, тому потрібно блокувати вхідні порти які не залучені, й не впливають на роботу системи.

Використаємо програму nmap та проскануємо порти SW-1 і зможемо побачити відкритий 445 порт, який використовується для SMB протоколу. Зламавши цей порт ми зможемо отримати доступ до всіх спільних файлів в мережі.



Рисунок 3.88 – Сканування WS-1 з допомогою nmap

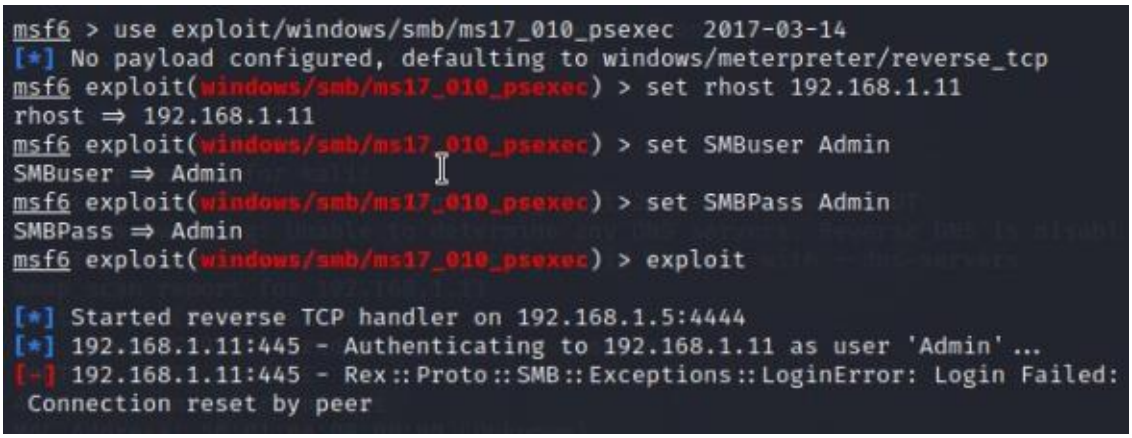


Рисунок 3.89 – Спроба зайти в локальні файли на Win-1 з випадковими даними

`



Рисунок 3.90 – Спроба зайти в локальні файли на Win-1 з даними адміністратора мережі

Для доступу по 445 порту SW-1 використовує пул адрес VPN, тому атака була невдалою.

Висновки до третього розділу

В розділі було детально показано встановлення та налаштування OpenVPN сервера. Створено конфігураційні файли для сервера та клієнта, що дозволяють клієнтам бачити один одного в мережі, а весь трафік маршрутизується через сервер. Згенеровано унікальних користувачів, та створено багатокористувацьке підключення до тунелю відразу 4 користувачами. Під’єднано користувача на Mac OS, що демонструє кросплатформеність даного протоколу.

Реалізували перехоплення пакета OpenVPN, та перевірено наявність шифрування тунелю. Здійснено перехоплення пакета протоколу SMB2 в середині самого тунелю по якому було передано файлу test.txt який теж був зашифрований. Налаштували властивості фаєрвола для роботи з OpenVPN, додали винятки для OpenVPN server, та відповідних портів. Решту не залучених портів заблоковано. Створено користувачів для доступу по SMB протоколу за логіном та паролем.

Перевірено вразливість мережі атаками на протокол SHH та SMB, реалізовано атаки Mac spoofing, Mac flooding та перевірено відкриті порти на наявні вразливості. Проведені атаки показали захищеність системи та її стійкість.

`

ВИСНОВКИ

В даній кваліфікаційній роботі було спроектовано та показано роботу підсистеми захисту мережі з використанням технології OpenVPN

В першому розділі детально розглянули технологію VPN та алгоритми роботи. Здійснили розгляд алгоритмів симетричного та асиметричного шифрування які залучені в роботі VPN. Провели порівняння та аналіз чинних алгоритмів VPN. Зробили висновки та обгрунтування вибору протоколу OpenVPN, навели його переваги та недоліки.

В другому розділі описали структуру та алгоритм роботи створеної мережі на основі технології OpenVPN, розглянули механізми перевірки цілісності та автентифікації даних. Показано алгоритм розробки топології мережі, використане обладнання і його характеристики. Наведено параметри налаштування маршрутизатора та комутатора для коректної роботи системи. Наведено приклад реалізації VPNaaS на базі хмарних сервісів OpenVPN Connexa та Google Cloud. Реалізовано з’єднання віддаленого користувача до хмарного сервера. Побудовано діаграму загроз мережі та описано атаки на мережу,й засоби захисту від атак.

В третьому розділі показано алгоритм встановлення та налаштування OpenVPN сервера та клієнта. Створено сертифікати та ключі для криптографічного захисту з’єднання. Згенеровано конфігураційний файл сервера та клієнтів, що дозволяє обмін даними між з’єднаними клієнтами. Створено користувача для Mac Sierra і здійснено підключення, що демонструє кросплатформеність алгоритму. Здійснили перехоплення пакетів OpenVPN з допомогою додатку WireShark та пакету SMB протоколу в середині тунелю. Обидва файли були зашифровані та не придатними для вільного читання, що показує захищеність даних в мережі. Налаштували правила для фаєрвола, щоб захистити мережу від атак ззовні. Було здійснено атаки на мережевому рівні для перевірки міцності системи та налаштувань захисту. Атаки не змогли досягти всіх своїх цілей та були заблоковані системами захисту, що демонструє стійкість системи.

`

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. "Asymmetric Encryption" [Електронний ресурс] - Режим доступу до ресурсу: https://www.cloudflare.com/learning/ssl/what-is-asymmetric-encryption/
2. "Block Cipher" [Електронний ресурс] - Режим доступу до ресурсу: https://www.tutorialspoint.com/cryptography/block_cipher.htm
3. "Introduction to VPN" [Електронний ресурс] - Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html
4. "Choosing the Right VPN Protocol" [Електронний ресурс] - Режим доступу до ресурсу: https://www.cloudwards.net/vpn-protocol/
5. "OpenVPN vs PPTP vs L2TP/IPSec vs SSTP vs IKEv2" [Електронний ресурс] - Режим доступу до ресурсу: https://www.vpnuniversity.com/learn/vpn-protocols-compared
6. "OpenVPN Security Best Practices" [Електронний ресурс] - Режим доступу до ресурсу: https://community.openvpn.net/openvpn/wiki/Hardening
7. “Шифрування VPN | Що потрібно знати, щоб бути в безпеці” [Електронний ресурс] - Режим доступу до ресурсу: https://blog.hidemyass.com/uk/guide-to-encryption
8. “Шифрування: типи і алгоритми. Що це, чим відрізняються“ [Електронний ресурс] - Режим доступу до ресурсу: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms
9. “The best VPN services of 2023 | TechRadar [Електронний ресурс] - Режим доступу до ресурсу: https://www.techradar.com/vpn/best-vpn
10. “The ultimate guide to VPN encryption, protocols, and ciphers” [Електронний ресурс] - Режим доступу до ресурсу: https://cybersecurity.att.com/blogs/security-essentials/the-ultimate-guide-to-vpn-encryption-protocols-and-ciphers

`

11. “Everything to Know About VPN Encryption“ [Електронний ресурс] - Режим доступу до ресурсу: https://allaboutcookies.org/everything-to-know-about-vpn-encryption
12. “What Is IPSec? Encryption” [Електронний ресурс] - Режим доступу до ресурсу: https://aws.amazon.com/what-is/ipsec/
13. “Authentication and Encryption Algorithms” [Електронний ресурс] - Режим доступу до ресурсу: https://docs.oracle.com/cd/E19683-01/816-7264/ipsec-ov-11/index.html
14. “Cryptographic Settings” [Електронний ресурс] - Режим доступу до ресурсу: https://docs.netgate.com/pfsense/en/latest/vpn/openvpn/configure-server-crypto.html
15. “What are the Benefits of Using VPN Encryption?” [Електронний ресурс] - Режим доступу до ресурсу: https://linfordco.com/blog/vpn-encryption/
16. “OpenVPN Vs IKEV2 Vs L2TP- VPN Protocols Compared” [Електронний ресурс] - Режим доступу до ресурсу: https://www.utunnel.io/blog/vpn-technology/openvpn-vs-ikev2-vs-l2tp-vpn-protocols-compared
17. “OpenVPN Cipher Negotiation (Quick reference)” ¶[Електронний ресурс] - Режим доступу до ресурсу: https://community.openvpn.net/openvpn/wiki/CipherNegotiation
18. “Symmetric Key Encryption - why, where and how it’s used” [Електронний ресурс] - Режим доступу до ресурсу: https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking
19. “AES vs. RSA Encryption: What Are the Differences?” [Електронний ресурс] - Режим доступу до ресурсу: https://www.precisely.com/blog/data-security/aes-vs-rsa-encryption-differences
20. “Using RSA public keys to protect keys sent between systems [Електронний ресурс]”- Режим доступу до ресурсу:

https://www.ibm.com/docs/en/zos/2.3.0?topic=pdk-using-rsa-public-keys-protect-keys-sent-between-systems

21. “How do you use AES and RSA together for hybrid encryption schemes? Systems” [Електронний ресурс] - Режим доступу до ресурсу: https://www.linkedin.com/advice/0/how-do-you-use-aes-rsa-together-hybrid-encryption-schemes
22. “AES vs RSA Encryption” [Електронний ресурс] - Режим доступу до ресурсу: https://www.phalanx.io/blog/aes-vs-rsa-encryption

`

ДОДАТКИ

`

Додаток А – Виконання Show Run на SW-1

```
SW-1#sh run
Building configuration...


Current configuration : 2085 bytes
!
! Last configuration change at 19:32:05 EET Wed Jun 14 2023
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname SW-1
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$Cum8$7apJU7OjeBv1TOscueySu0
!
username admin privilege 15 secret 5 $1$nfGB$wQPBbcR9/1VUnhaFbPUfW.
no aaa new-model
clock timezone EET 2 0
!
!
!
!
!
!
!
!
ip dhcp snooping vlan 1
ip dhcp snooping
ip domain-name vovkvpn.com
ip cef
login delay 9
login on-failure log every 3
login on-success log every 3
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
```

Рис. А.1 – Виконання команди Show Run на SW-1

`

```
interface Ethernet0/1
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0050.0100.0800
 switchport port-security
 spanning-tree portfast edge
 spanning-tree bpduguard enable
!
interface Ethernet0/2
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 5001.0009.0000
 switchport port-security
 spanning-tree portfast edge
 spanning-tree bpduguard enable
!
interface Ethernet0/3
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 5001.0012.0000
 switchport port-security
 spanning-tree portfast edge
 spanning-tree bpduguard enable
!
interface Ethernet1/0
 spanning-tree portfast edge
 spanning-tree bpduguard enable
!
interface Ethernet1/1
 shutdown
!
interface Ethernet1/2
 shutdown
!
interface Ethernet1/3
 shutdown
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip ssh time-out 60
ip ssh logging events
ip ssh version 2
```

Рис. А.2 – Виконання команди Show Run на SW-1

```
control-plane
!
!
line con 0
 password 7 1304131F0202
 logging synchronous
 login
line aux 0
line vty 0 4
 session-timeout 60
 access-class 11 in
 exec-timeout 9 0
 password 7 11081D081E1C
 login
 transport input ssh
!
!
end
```

Рис. А.3 – Виконання команди Show Run на SW-1

`

Додаток Б – Виконання Show Run на R-1

```
R-1#sh run
Building configuration...

Current configuration : 1531 bytes
!
! Last configuration change at 18:09:29 EET Sun Jun 11 2023
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R-1
!
boot-start-marker
boot-end-marker
!
!
!
aaa new-model
!
!
!
!
!
!
!
aaa session-id common
!
clock timezone EET 2 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
!
!
!
!
!
ip domain name vovkvpn.com
ip cef
login delay 9
login on-failure log every 3
login on-success log every 3
no ipv6 cef
!
multilink bundle-name authenticated
```

Рис. Б.1 – Виконання команди Show Run на R-1

`



Рис. Б.2 – Виконання команди Show Run на R-1

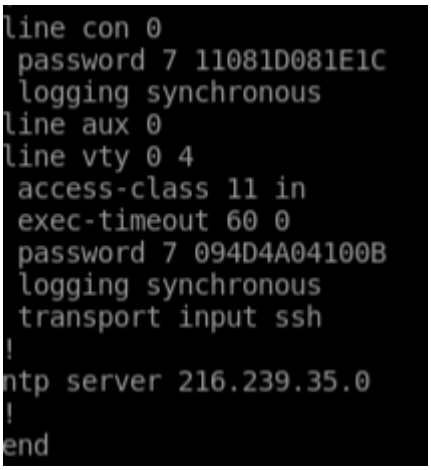


Рис. Б.3 – Виконання команди Show Run на R-1

`

Додаток В – Конфігураційний файл OpenVPN сервер

```
port 1194
proto udp
dev tun
#management 192.168.1.11 23
topology subnet
ca "C:\\Program Files\\OpenVPN\\easy-rsa\\pki\\ca.crt"
cert "C:\\Program Files\\OpenVPN\\easy-rsa\\pki\\issued\\server.crt"
key "C:\\Program Files\\OpenVPN\\easy-rsa\\pki\\private\\server.key"
dh "C:\\Program Files\\OpenVPN\\easy-rsa\\pki\\dh.pem"
server 192.168.10.0 255.255.255.0
push "route 192.168.1.0 255.255.255.0"
push "route 192.168.2.0 255.255.255.0"
push "route 192.168.3.0 255.255.255.0"
tls-auth "C:\\Program Files\\OpenVPN\\easy-rsa\\pki\\ta.key" 0
cipher AES-256-GCM
keepalive 20 60
persist-key
persist-tun
client-to-client
status "C:\\Program Files\\OpenVPN\\log\\status.log"
log "C:\\Program Files\\OpenVPN\\log\\openvpn.log"
verb 3
mute 20
windows-driver wintun
user nobody
group nogroup
ifconfig-pool-persist ipp.txt
push "redirect-gateway def1 bypass-dhcp"
```

`

Додаток Г – Конфігураційний файл OpenVPN клієнт

```
client
dev tun
proto udp
remote 192.168.1.11 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert vovk1.crt
key vovk1.key
remote-cert-tls server
tls-auth ta.key 1
cipher AES-256-GCM
connect-retry-max 25
verb 3
redirect-gateway def1
```