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

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

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Дослідження відмовостійкості з'єднання OpenVPN для забезпечення неперервності бізнес-процесів

Виконав: студент 6 курсу, групи СБмз-61
спеціальності 125 «Кібербезпека»
(шифр і назва спеціальності)

(підпис) Космина А.С. (прізвище та ініціали)

Керівник (підпис) (прізвище та ініціали)

Нормоконтроль (підпис) (прізвище та ініціали)

Завідувач кафедри (підпис) (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль
2021

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

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

Кафедра Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Заморська Н.В.
(підпис) (прізвище та ініціали)
«21» грудня 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 125 «Кібербезпека»
(шифр і назва спеціальності)

студенту Космині Андрію Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження відмовостійкості з'єднання OpenVPN для забезпечення неперервності бізнес-процесів

Керівник роботи Муж Валерій Вікторович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «____» _____ 20___ року № _____

2. Термін подання студентом завершеної роботи 16 грудня 2021 року

3. Вихідні дані до роботи

4. Зміст роботи (перелік питань, які потрібно розробити)

1. Проведення аналізу видів VPN та їх використання для бізнесу
2. Здійснення загального аналізу OpenVPN технології та порівняння продуктивності алгоритмів шифрування
3. Практична реалізація відмовостійкого з'єднання OpenVPN з функцією автоматичної зміни сервера.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

1. Титульний аркуш презентації
2. Мета та актуальність роботи, завдання роботи
3. Класифікація VPN
4. Порівняння криптографічних протоколів
5. Порівняння головних рішень VPN для бізнесу
6. Функції безпеки, що забезпечує Open VPN
7. Алгоритми, що підтримує OpenVPN
8. Порівняння алгоритмів шифрування
9. Схема відмовостійкої мережі
10. Етапи налаштування мережі 11. Результати виконаної роботи

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці безпека в надзвичайних ситуаціях	Осухівська Т.М. Кандак В.П. ст. викладач		2.12 17.12.21

7. Дата видачі завдання 18 листопада 2021 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Окреслювання завдання	04.10.21	виконано
2	Аналіз літературних джерел	05.10.21	виконано
3	Написання 1-го розділу	20.10.21	виконано
4	Розробка та аналіз задачі	10.11.21	виконано
5	Написання 2-го розділу	16.11.21	виконано
6	Написання 3-го розділу	20.11.21	виконано
7	Опрацювання питань розділу 4	01.12.21	виконано
8	Оформлення роботи	04.12.21	виконано
9	Перевірка на плагіат	09.12.21	виконано
10	Попередній захист	17.12.21	виконано
11	Захист	23.12.21	

Студент _____ (підпис) Косміна А.С. (прізвище та ініціали)

Керівник роботи _____ (підпис) Мупс В.В. (прізвище та ініціали)

АНОТАЦІЯ

Дослідження відмовостійкості з'єднання OpenVPN для забезпечення неперервності бізнес-процесів// Дипломна робота ОР «Магістр» // Космина Андрій Сергійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБмз-61 // Тернопіль, 2021 // С. 75 , рис. – 14 , табл. – 3 , додат. – 5 .

Ключові слова: ВІРТУАЛЬНА ПРИВАТНА МЕРЕЖА, VPN, OPENVPN, ШИФРУВАННЯ, АЛГОРИТМИ ШИФРУВАННЯ, ТУНЕЛЮВАННЯ, ІНКАПСУЛЯЦІЯ.

.

Дана магістерська кваліфікаційна робота присвячена дослідженню відмовостійкості з'єднання OpenVPN для забезпечення неперервності бізнес-процесів. Проведено аналіз видів VPN та їх використання для бізнесу, аналіз OpenVPN технології та порівняння продуктивності алгоритмів шифрування. Організовано мережу відмовостійкого з'єднання OpenVpn з функцією автоматичної зміни сервера.

У першій главі розглянуто основні характеристики віртуальних приватних мереж та проведено аналіз видів VPN та способи їх використання для потреб бізнесу.

У другій главі проведено загальний аналіз технології OpenVPN та проведено порівняння продуктивності основних алгоритмів шифрування

У третій главі проведено практичну побудову відмовостійкого з'єднання OpenVpn з функцією автоматичної зміни сервера з використанням найоптимальніших налаштувань та продуктивних алгоритмів вибраних на основі порівняння в попередньому розділі.

У підрозділі "Охорона праці" розглянуто загальні правила охорони праці та питання забезпечення електробезпеки користувачів ПК.

ANNOTATION

Research of fault tolerance of OpenVPN connection for ensuring continuity of business processes // Thesis of OR "Master" // Kosmyna Andriy Sergiyovich // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group SBmz-61 // Ternopil, 2021 // P- 75 , fig. - 14 , table. - 3 , add. - 5.

Keywords: VIRTUAL PRIVATE NETWORK (VPN), OPENVPN, ENCRYPTION, ENCRYPTION ALGORITHMS, TUNNELING, ENCAPSULATION.

This master's thesis is devoted to the study of fault tolerance of OpenVPN connections to ensure business continuity. The analysis of VPN types and their use for business, the analysis of OpenVPN technology and the comparison of productivity of encryption algorithms are carried out. Organize a failover OpenVpn connection with automatic server change.

The first chapter discusses the main characteristics of virtual private networks and analyzes the types of VPN and ways to use them for business purposes.

The second chapter provides a general analysis of OpenVPN technology and compares the performance of basic encryption algorithms

The third chapter provides a practical way to build a failover OpenVpn connection with an automatic server change function using the most optimal settings and productive algorithms selected based on the comparison in the previous section.

In the subsection "Labor protection" the general rules of labor protection and questions of ensuring electrical safety of PC users are considered.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ОС - операційна система

ПЗ - програмне забезпечення

CA - Certificate authority (центр сертифікації)

DHCP - Dynamic Host Configuration Protocol

IP - Internet Protocol (протокол інтернету)

OSI - Open System Interconnection (модель взаємодії відкритих систем)

IPSec - Internet protocol security (інтернет протокол безпеки)

NAT - Network address translation (трансляція мережевих адрес)

PKI - Public key infrastructure (інфраструктура відкритих ключів)

PPP - Point to Point Protocol

PPTP - Point-to-point tunneling protocol (протокол тунелювання двоточкового з'єднання)

HMAC - Hash-based message authentication code (хеш-код автентифікації повідомлень)

SSL - Secure sockets layer (рівень захищених гнізд)

TCP - Transmission control protocol (протокол управління передачею)

TLS - Transport layer security (безпека транспортного рівня)

UDP - User datagram protocol (протокол дейтаграми користувача)

VPN - Virtual private network (віртуальна приватна мережа)

ЗМІСТ

ВСТУП

Кожного дня в світі телекомунікаційних технологій спостерігається підвищення інтересу до віртуальних приватних мереж (Virtual Private Network - VPN). Цей інтерес обумовлено необхідністю створення захищеного підключення для користувачів за допомогою незахищеної мережі Internet до віддалених офісів.

Проте необхідно розуміти, що у разі об'єднання підключення через мережу Internet, одразу ж виникає питання про безпечну передачу даних, саме тому виникає необхідність для створення механізмів, які дозволять забезпечити доступність, цілісність та конфіденційність інформації, яка передається.

Одним із елементів побудови такої системи є віртуальні приватні мережі. Тому постає *актуальна задача* створення та дослідження ефективних механізмів забезпечення конфіденційності, цілісності та відмовостійкості з’єднання за технологією віртуальних приватних мереж.

Метою даної роботи є реалізація та аналіз захищеної відмовостійкої мережі з використанням технології OpenVPN.

Для досягнення мети в роботі поставлені наступні ***завдання****:*

1. Провести аналіз видів VPN та їх використання для бізнесу. (РОЗДІЛ 1).
2. Здійснити загальний аналіз OpenVPN технології та порівняння продуктивності алгоритмів шифрування. (РОЗДІЛ 2).
3. Організація відмовостійкого з’єднання OpenVpn з функцією автоматичної зміни сервера. (РОЗДІЛ 3).

Головним *теоретичним результатом* є вивчення та побудова відмовостійких та продуктивних рішень технології OpenVPN.

Практичним результатом нашої роботи є реалізація відмовостійкого з’єднання з використанням технології OpenVPN на базі операційних систем Ubuntu 16.05.7 x64 та Microsoft Windows 10.

Об’єкт дослідження – процес побудови VPN-мережі для підприємства.

Предмет дослідження – моделі побудови та алгоритми шифрування при створенні VPN-мережі.

Методами дослідження є загальнонаукові методи пізнання: порівняння та системний аналіз.

Наукова новизна: запропонована в роботі модель простої VPN-мережі для бізнесу, що забезпечує конфіденційність даних, високу продуктивність передачі захищеної інформації та легку можливість масштабування.

Практичне значення роботи полягає в тому, що запропонована модель VPN-мережі є універсальною, доступною, відносно не складною в налаштуванні і може бути використаним для широкого кола організацій.

Апробація результатів роботи. Окремі результати роботи доповідались на IX науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 8 – 9 грудня 2021 р.

РОЗДІЛ 1 ЗАГАЛЬНИЙ АНАЛІЗ ТЕХНОЛОГІЇ ВІРТУАЛЬНИХ МЕРЕЖ

1.1 Загальні положення технології VPN

VPN (англ. *Virtual Private Network* - віртуальна приватна мережа) - це створена поверх будь-якої іншої мережі не фізична мережа. Комунікація відбувається через загальнодоступні мережі та використовує небезпечні відкриті протоколи, за допомогою шифрування можна створити канали обміну інформацією, що будуть закриті та недоступні для сторонніх осіб.[1]

VPN допомагає об'єднувати, наприклад, офіси певної організації, що розташовуються далеко один від одного в одну мережу без прокладання окремо виділеної лінії зв’язку. Для цього можна використовувати будь-які відкриті та непідконтрольні канали для обміну інформацією такі як Internet.

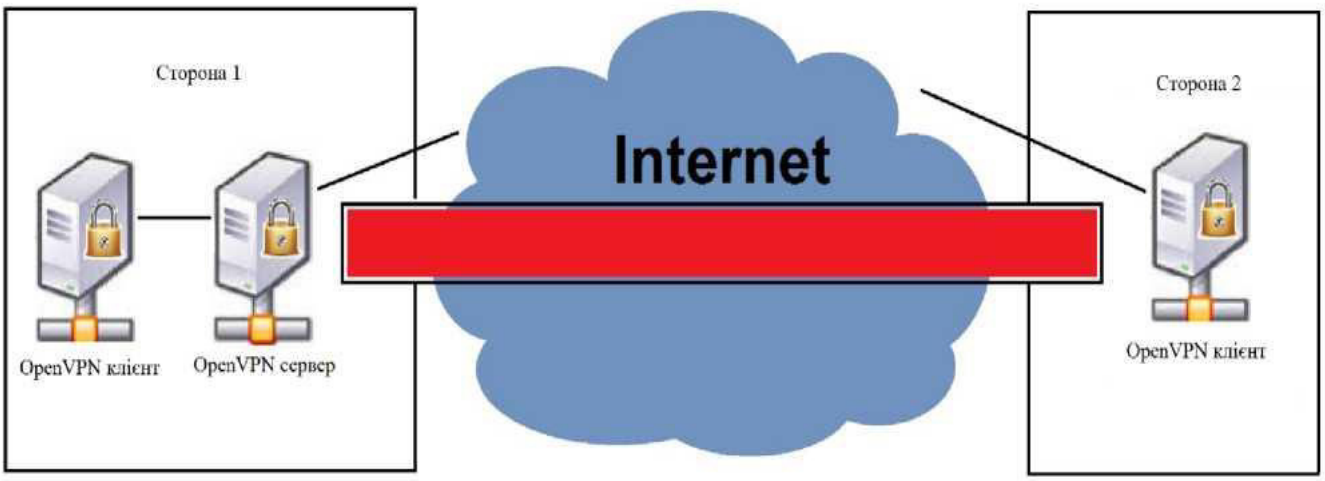

Рисунок 1.1 - Загальна схема VPN - з’єднання.

Virtual Private Network, за принципом дії, володіє такими ж властивостями як виділена лінія, однак його можна розгорнути в загальнодоступному та незахищеному Інтернеті.[2]

Пакети з даними передаються через Інтернет як по звичайному з'єднанню Точка-Точка, використовуючи метод тунелювання.

Між відправникои та одержувачем створюється віртуальний тунель. З його допомогою можна інкапсулювати дані з одного протоколу в пакети іншого протоколу мережі.

Головні компоненти такого тунелю :

- ініціатор
- маршрутизатор мережі;
- тунельний комутатор;
- тунельні термінали.

VPN не конфліктує з основними мережевими технологіями чи протоколами. Наприклад, для встановлення комутованого з'єднання клієнт повинен відправити стандартні пакети PPP на сервер. Коли віртуальна виділена лінія організована між локальними мережами, їх маршрутизатори виконують обмін пакетами PPP. Однак абсолютно новий підхід полягає в тому, щоб пересилати пакети через захищений тунель, створений через загальнодоступний Інтернет.[6]

Тунелювання дозволяє організувати передачу пакетів, що містять дані з одного протоколу в логічне середовище іншого протоколу. У цьому випадку можна вирішити проблему взаємодії кількох мереж різного типу, починаючи від вирішення конфліктів, які можуть виникнути при використанні інших протоколів або конкретних схем адресації в мережі, аж до необхідності підтримки цілісності. та гарантія конфіденційності переданих даних. Існуючу структуру корпоративної мережі організації можна підготувати до використання технології VPN за допомогою програмного, апаратного або комбінованого апаратно-програмного забезпечення. Організація віртуальної приватної мережі схожа на прокладку кабелів через глобальну мережу. За допомогою протоколу PPP встановлюється пряме з'єднання між кінцевими пристроями тунелю.

Найбільш поширений метод створення VPN-тунелів - це інкапсуляція мережевих протоколів (IPX, IP , Apple Talk і т.д.) в PPP і подальша їх інкапсуляція в протоколи тунелювання. Останнім зазвичай є протокол IP. Цей підхід називається тунелюванням рівня 2, оскільки тут використовується протокол рівня 2.

Використання інкапсуляції пакетів мережевих протоколів у протоколи тунелювання це ще один підхід до вирішення цієї задачі. Метод, який використовує

інкапсуляцію мережевих протоколів у транспортних протоколах, відомий як тунелювання рівня 3.[8]

Незалежно від протоколів, які використовуються або яка головна мета організації такого тунелю, основна методика залишається практично незмінною. Схема побудови тунелю використовує один протокол щоб встановити з'єднання, а інший протокол використовується щоб інкапсулювати дані і службову інформацію.

1.2 Класифікація VPN

VPN прийнято класифікувати за такими основними параметрами.

Призначення мережі:

• Внутрішньо корпоративна мережа (Intranet VPN).

Використовується для з'єднання кількох розподілених мереж LAN до захищеної мережі.. Обмін даними відбувається відкритими каналами передачі інформації.

• Мережа віддаленого доступу (Remote Access VPN).

Він використовується щоб створити безпечний канал зв'язку між віддаленим користувачем та корпоративною мережею (штаб-квартирою) завдяки можливості підключатися до корпоративних ресурсів з домашнього АРМ або інших портативних пристроїв таких як ноутбук або планшет.

• Extranet VPN.

Використовується за необхідності підключення до корпоративної мережі компанії інших користувачів (наприклад клієнти компанії, замовники, постачальники послуг та інші). Степінь довіри до такої категорії користувачів корпоративної мережі значно нижчий ніж у працівників компанії, саме тому необхідно забезпечити спеціальні засоби захисту які обмежують доступність таким особам конфіденційно важливої інформації.[20]

1.3 Функції безпеки, які забезпечються технологією VPN

Основна функція VPN – це забезпечення безпеки передачі даних. Надійний

захист повинен бути гарантований на шляху проходження з клієнтських комп'ютерів на сервер VPN через Інтернет. Оскільки відстань між клієнтським комп’ютером та сервером зазвичай дуже велика , дані можуть проходити через різні пристрої багатьох виробників та провайдерів на шляху до корпоративної мережі.. Можна використовувати різні методи аутентифікації та шифрування, щоб гарантувати, що дані не перезаписуються чи не зчитуються під час передачі.

Аутентифікація

Використовуючи протокол PPTP для аутентифікації можна залучити будь-який протокол при змінюваних для PPP

- AEP;
- MS CHAP;
- CHAP;
- SPAP;
- PAP.

Прийнято вважати протоколи MS CHAP_v2 і TLS більш надійними. Таким чином сервер та клієнт можуть ідентифікувати один одного. При використанні усіх інших протоколів тільки сервер має можливість проводити аутентифікацію підключених клієнтів.

PPTP забезпечує достатню захищеність, проте, використання L2TP налаштованого поверх IPSec буде надійнішим. Використання L2TP налаштованого поверху IPSec забезпечить аутентифікацію на рівнях користувач і комп'ютер, окрім того воно виконуватиме шифрування та аутентифікацію.

Аутентифікація користувачів відбувається або з використанням відритого тексту, або за схемою запит/відгук. Метод відкритого тексту зрозумілий. Сервер отримує пароль від користувача незашифрованим. Проводиться перевірка правильність паролю та у разі успіху Сервер дозволяє доступ. Використання відкритої аутентифікації рідко використовується, оскільки перехопити пароль у

відкритому вигляді дуже просто.

Схема з використанням запиту / відгуку має набагато більше можливостей.:

- клієнт надсилає request-запит для аутентифікація серверу;
- сервер у відповідь надсилає challenge-відгук з довільним текстом ;
- клієнт шифрує утвореним з пароля хешем отриманий відгук та відправляє назад серверу;
- таку ж процедуру проробляє сервер, результати отримані сервером та клієнтом порівнюються;
- вважається, що аутентифікація пройшла успішно, якщо зашифрований клієнтом відгук збігається з тим, що зашифрував сервер.

Конфіденційність

Конфіденційність інформації - суб'єктивно визначена характеристика, яка вказує на необхідність введення обмежень на суб'єкти, що мають доступ до даної інформації, і забезпечувана здатністю системи зберігати вказану інформацію в таємниці від суб'єктів, що не мають повноважень доступу до неї. Об'єктивні передумови подібного обмеження доступності інформації для одних суб'єктів полягають в необхідності захисту їх законних інтересів від інших суб'єктів інформаційних стосунків.

Ризик порушення конфіденційності полягає в тому, що інформація стає відомою стороннім людям.

Абонентське шифрування дозволяє забезпечити конфіденційність даних, які передаються між двома прикладними об'єктами (абонентами). Абонентське шифрування можна реалізувати за допомогою протоколу прикладного або рівня представлення еталонної моделі OSI. В такому випадку захищеною залишається тільки повідомлення, а вся службова інформація залишається відкритою.

Для забезпечення безпеки керуючого каналу і потоку даних OpenVPN

використовує бібліотеку OpenSSL. Завдяки цьому залучено весь набір алгоритмів шифрування, доступних у цій бібліотеці. Також може використовуватися апаратне прискорення щоб поліпшити продуктивність шифрування.

OpenSSL — відкритий програмний продукт, розроблений як універсальна бібліотека для криптографії, що використовує протоколи Secure Sockets Layer та Transport Layer Security. Його використовуються щоб реалізувати роботу з протоколом https. Доступна для більшості UNIX-подібних операційних систем і Microsoft Windows.[18]

OpenVpn Реалізує наступні алгоритми шифрування:

Таблиця 1.1 - Алгоритми шифрування, які реалізує OpenVPN

Шифри	AES, Blowfish, Camellia, SEED, CAST-128, DES, IDEA, RC2, RC4, RC5, Triple DES, GOST 28147-89
Криптографічні хеш-функції	MD5, MD2, SHA-1, SHA-2, RIPEMD-160, MDC-2, GOST R 34.1194
Асиметричні алгоритми шифрування	RSA, DSA, Протокол Діффі- Г еллмана, Еліптична криптографія, GOST R 34.10-2001

Цілісність

Цілісність інформації - існування інформації в неспотвореному вигляді (незмінному по відношенню до деякого фіксованого її стану). Точніше кажучи, суб'єктів цікавить забезпечення ширшої властивості - достовірності інформації, яке складається з повноти і точності відображення стану області і безпосередньо цілісності інформації, тобто її не спотворення.

Загроза порушення цілісності включає будь-яку навмисну зміну інформації, що зберігається в обчислювальній системі або передається з однієї системи в іншу.

Коли зловмисники навмисно змінюють інформацію, йде мова про порушення цілісності інформації. Цілісність також буде порушена, якщо випадкова помилка програмного або апаратного забезпечення приводить до несанкціонованої зміни інформації. Санкціонованими змінами є ті зміни, які зроблені уповноваженими особами з обґрунтованою метою (наприклад, санкціонованою зміною є періодична запланована корекція деякої бази даних). Інформація зберігає цілісність, якщо дотримуються установлених правил її модифікації (видалення).

Для забезпечення вищого рівня безпеки можна використовувати пакетну авторизацію HMAC.

HMAC (англ. Hash-based message authentication code , код аутентифікації (перевірки справжності) повідомлень, що використовує хеш - функції) - це популярний механізм перевірки цілісності інформації. Цей механізм забезпечує те, що дані, не були змінені іншими особами методом атаки «Людина посередині» при передачі або зберіганні в ненадійному середовищі. Механізм HMAC застосовує імітовставку (MAC). MAC — стандарт, який описує спосіб обміну даними та спосіб перевірки цілісності даних, переданих з використанням таємного ключа. Два клієнти, які використовують MAC, здебільшого використовують спільний секретний ключ. HMAC - надбудова над MAC; механізм обміну даними з використанням секретного ключа (як у MAC) та хеш-функцій .

Тунелювання

Тунелювання (англ. tunnelling - «Прокладка тунелю») - процес, в ході якого створюється логічне з'єднання між двома точками за допомогою інкапсуляції даних різних протоколів. Тунелювання це метод побудови мереж, при якому дані одного мережевого протоколу разом зі службовими полями інкапсулюються в область корисного навантаження пакета несучого протоколу. Від звичайних мережевих моделей з розподіленням на рівні тунелювання відрізняється тим, що протокол, який інкапсулюється, відноситься до того ж або нижчого рівня, ніж використовується в якості тунелю.

Комбінація шифрування разом з тунелюванням позволяє реалізацію закритих віртуальних приватних мереж (VPN). При використанні методу тунелювання зазвичай застосовується погоджування транспортних протоколів чи створення захищеного з'єднання між вузлами такої мережі .

Тунелювання забезпечує передачу захищених даних таким чином, що вся мережева інфраструктура яка розвертається між джерелом і приймачем даних виявляється прихованою від зовнішнього аналізу.

Транспортне середовище тунелю, отримує пакети мережевого протоколу який використовується на вході в тунель та без змін транспортує їх до виходуз тунелю. Для з'єднання двох мережевих вузлів так, що вони виглядатимуть як підключені до однієї (локальної) мережі, буде достатньо побудови тунелю. Проте слід пам’ятати, що насамперед данні проходять через безліч сторонніх проміжних маршрутизаторів відкритої публічної мережі.

З цього виникають дві основні проблеми. Перша полягає в тому, що інформацію що передається через тунель можуть перехопити зловмисники. Якщо інформація конфіденційна, то цілком реальною стає загроза компрометації цієї інформації. Більше того, зловмисники будуть мати можливість змінити дані що передані через тунель так, що адресат не матиме можливості перевірити їх на достовірність. Це може призвести до небажаних та непрогнозованих проблем.

Опираючись на вище сказане, ми розуміємо, що тунель в чистому вигляді підходящий хіба що для онлайн комп'ютерних ігор або інших задач, в яких цілісність даних не відіграє важливої ролі і не може використовуватись у більш серйозних завданнях. Кожну з цих проблем можна вирішити використанням сучасних методів криптографічного захисту інформації. Щоб запобігти внесенню несанкціонованих змін до пакету з даними на шляху його проходження по тунелю, доцільно використовувати метод електронного цифрового підпису (ЕЦП).

Суть цього методу полягає в наступному: кожен із переданих пакетів забезпечується додатковим блоком інформації, який утворюється у відповідності з

асиметричним криптографічним алгоритмом і унікальний для вмісту пакета і секретного ключа ЕЦП адресанта. Цей додатковий блок інформації це ЕЦП пакету. Він дозволяє виконати перевірку отриманих даних одержувачем, за умови що отримувачу відомий відкритий ключ ЕЦП відправника. Для забезпечення захисту даних переданих через тунель від несанкціонованого перегляду використовуються сильні крипостійкі алгоритми шифрування.

1.4 Порівняння найпоширеніших протоколів (PPTP,L2TP,IPSec)

PPTP

Протокол тунелювання точка-точка (Point-to-Point Tunneling Protocol) - це протокол, винайдений компанією Microsoft для організації VPN-з'єднання через мережі комутованого доступу. PPTP або протокол тунелювання "точка-точка" створює тунель і обмежує пакет даних. Протокол «точка-точка» (PPP) використовується для шифрування даних між з'єднаннями. PPTP є одним з найбільш широко використовуваних протоколів VPN. PPTP також використовується на Mac і Linux. Доступність його, як стандартного протоколу майже у всіх операційних системах та на більшості пристроїв, що підтримують VPN, - дозволяє використовувати його без необхідності встановлення додаткового програмного забезпечення. PPTP залишається популярним вибором як підприємств, так і VPN-провайдерів. Його перевага також у тому, що він використовує менше обчислювальних ресурсів, отже має високу швидкість роботи.

Хоча PPTP зазвичай і використовується з 128-бітовим шифруванням, після включення цього протоколу до складу Windows 95 OSR2 ще в 1999 році , протягом кількох років, булу знайдено ряд критичних вразливостей. Найбільш серйозною з яких стала вразливість протоколу аутентифікації MS-CHAP_v.2. Використовуючи цю вразливість, PPTP був зламаний протягом 2 днів. І хоча компанією Microsoft помилка була виправлена (на зміну протоколу
MS-CHAP_v.2 почали використовувати новий протокол аутентифікації PEAP), вона сама рекомендувала до використання в якості VPN проколів L2TP або SSTP.

плюси:

- клієнт PPTP вбудований майже в усі операційні системи
- легкість налаштування
- працює достатньо швидко

мінуси:

- небезпечний (вразливий протокол аутентифікації MS-CHAP v.2)

L2TP і L2TP / IPsec

L2TP або Layer 2 Tunneling Protocol — це протокол тунелювання, який часто поєднується з іншим протоколом безпеки VPN, таким як IPSec, для встановлення високобезпечного VPN-з'єднання. L2TP створює тунель між двома точками підключення L2TP, а протокол IPSec шифрує дані та підтримує безпечний зв'язок між тунелем.

L2TP / IPsec вмонтований в усі сучасні операційні системи та VPN-сумісні пристрої, і так само легко може бути налаштований як і PPTP (зазвичай використовується той же клієнт). Проблеми можуть виникнути в тому, що L2TP використовує UDP-порт 500, який може бути заблокований мережевим екраном, якщо клієнт перебуває за NATом. Тому можуть знадобитися додаткові налаштування роутера для переадресації портів. До речі, протокол SSL, наприклад, використовує TCP-порт 443, щоб не відрізнятись від звичайного HTTPS-трафіку.

Протокол IPsec на даний момент не має ніяких серйозних вразливостей і вважається дуже безпечним при використанні таких алгоритмів шифрування, як AES. Однак, оскільки він інкапсулює дані двічі, це не так ефективно, як SSL-рішення (наприклад, OpenVPN або SSTP), і тому працює трохи повільніше.

плюси:

- висока степінь безпечності

- легкість налаштування
- доступність в усіх сучасних операційних системах

мінуси:

- працює повільніше, ніж OpenVPN
- потрібне додаткове налаштування роутера

OpenVPN

OpenVPN є відносно новою технологією з відкритим кодом, яка для своєї роботи використовує бібліотеку OpenSSL та протоколи SSL_v3 / TLS_v1, разом з безліччю схожих технологій для забезпечення надійного VPN-рішення. Одним з головних переваг OpenVPN є те, що він відносно простий для встановлення та гнучкий в налаштуваннях. Цей протокол може бути налаштований для роботи з використанням будь-якого порту, в тому числі на TCP-порті 443. Це дозволить замаскувати трафік усередині OpenVPN під виглядом звичайного HTTPS (який використовує, наприклад, Facebook або Gmail), а оскільки він зашифрований, то його важко розпізнати та заблокувати.

Ще однією перевагою OpenVPN є те, що використовуються для шифрування бібліотеки OpenSSL, які підтримують безліч криптографічних алгоритмів (наприклад, AES, 3DES, Blowfish, CAST-128, Camelia і інші). Найбільш поширені алгоритми, які використовують VPN-провайдери - AES і Blowfish. AES не є новою технологією, і хоча обидва вважаються безпечними, той факт, що він має 128-бітний розмір блоку, а не 64-бітний як у Blowfish, означає, що він може працювати з великими (більше 1Гб) файлами краще. Проте, відмінності досить незначні. Те, як швидко працює OpenVPN, залежить від обраного алгоритму шифрування, але, як правило, працює швидше, ніж IPsec.

OpenVPN став технологією №1 при використанні VPN, і хоча він спочатку не підтримується операційними системами, цей протокол широко підтримується через

стороннє програмне забезпечення. Зовсім недавно неможливо було використовувати OpenVPN на iOS і Android без jailbreak і правд доступу рута, згодом з'являлися сторонні додатки, які частково вирішили цю проблему. Зараз існують офіційні клієнти OpenVpn для таких мобільних платформ як iOS та Android.

З цим пов'язана інша проблема OpenVPN - гнучкість може зробити його незручним в налаштуванні. Зокрема, при використанні типової програмної реалізації OpenVPN (наприклад, стандартний відкритий клієнт OpenVPN під Windows) необхідно не тільки завантажити і встановити клієнт, але і завантажити (або створити) і встановити додаткові конфігураційні файли. Багато VPN-провайдерів вирішують цю проблему шляхом використання пре налаштованих VPN-клієнтів.

плюси:

- гнучко настроюється
- дуже безпечний (залежить від обраного алгоритму шифрування, але всі вони безпечні)
- може працювати без проблем з мережевими екранами
- може використовувати широкий спектр алгоритмів шифрування

мінуси:

- необхідно додаткове програмне забезпечення
- може бути незручний в налаштуванні

1.5 Порівняння готових рішень VPN для бізнесу

Для реалізації віддаленого захищеного підключення користувачів до корпоративної мережі доцільно використовувати технологію VPN. Для визначення кращого варіанту реалізації поставленої задачі додатково до вище перелічених протоколів розглянемо готові рішення від сторонніх компаній.

Основними вимогами до побудови відмовостійкої мережі є:

1. Конфіденційність, що забезпечується використанням надійного алгоритму шифрування трафіку та захистом даних користувачів.
2. Безперебійний доступ до інформації в корпоративній мережі шляхом автоматичного переключення на резервний канал зв'язку.
3. Наявність виділених серверів із статичними IP адресами, для налаштування прав доступу та мережевого екрану корпоративної мережі.
4. Вартість готового рішення та складність його реалізації.

Для реалізації поставленої задачі проаналізуємо доступні варіанти та складемо порівняльну таблицю. В межах поставленої задачі проаналізовано кілька популярних варіантів, що надають можливість «remote access vpn» для бізнесу.

Для порівняння використовувались такі параметри:

1. Доступні алгоритми шифрування- забезпечення надійного шифрування.
2. Реальна перевірена пропускна здатність серверів в МБ/с.
3. Конфіденційність
4. Наявність статичних IP адрес для налаштування доступу до корпоративної мережі.
5. Кількість серверів для резервування.
6. Наявність функції автоматичної зміни сервера
7. Можливість адміністрування користувачів
8. Складність реалізації
9. Ціна готового рішення.

Створено порівняльну таблицю можливостей цих компаній яка представлена в додатку Б.

Усі з представлених компаній пропонують реалізацію поставленої задачі за ціною від 13$ за 5 користувачів.

NordVPN та Torguard пропонують сервери зі статичним IP. І лише Torguard пропонує виділені сервери які будуть використовуватись лише для нашої організації. В NordVPN та Hotspot Shield на офіційному сайті не вказані алгоритми

що використовуються для шифрування. ExpressVPN та Torguard заявляють на офіційних сайтах, що не зберігають історію переглядів і підключень. Проте, існують підтверджені випадки неодноразового порушення цих правил іншими компаніями.

На основі цього ми розуміємо, що жоден із запропонованих на ринку продуктів не може в повній мірі відповідати поставленим задачам у сфері конфіденційності. Саме тому постає необхідність створення власної реалізації за допомогою програмного забезпечення з відкритим кодом та власними серверами.

В такому випадку компанія може повною мірою бути впевнена у конфіденційності даних, адже доступ до серверу та його даних буде лише у працівників цієї компанії.[21]

Також ціна такої реалізації буде значно нижчою ніж купівля готового рішення.

Висновки до розділу 1

У даному розділі було розглянуто поняття віртуальної приватної мережі, а також її класифікація та принципи роботи. Здійснено порівняння VPN-сервісів для бізнесу. VPN являє собою мережу, що створюється поверх іншої реальної мережі. Функціонування VPN відбувається відповідно до основних мережевих вимог та протоколів, але є певні характерні відмінності, наприклад, посилання пакетів через безпечний тунель. Класифікуються VPN за чотирма основними ознаками, а саме: за типом використовуваного середовища, за способом реалізації, за призначенням та за типом використовуваного протоколу.

Основним завданням розділу був загальний огляд технології та визначення факторів, що забезпечують безпечну передачу інформації в умовах використання небезпечних протоколів та публічних мереж. Проведено аналіз доступних готових VPN-рішень та порівняння їх з самостійною реалізацією на базі OpenVPN. Безпека передачі даних є основним завданням технології та забезпечується шляхом використання автентифікації та шифрування. Технологія використовує більш просунуту схему запит/відгук, що складається з чотирьох послідових кроків.

Водночас абонентське шифрування відбувається завдяки використанню бібліотеки OpenSSL, яка реалізовує понад десять різних алгоритмів шифрування.[19]

Окремо було розглянуто тунелювання, яке забезпечує передачу даних таким чином, що для джерела повідомлення та його приймача уся мережева інфраструктура залишається прихованою. Отож з точки зору працюючого програмного забезпечення, користувачі знаходяться в межах однієї локальної мережі, хоча насправді дані проходять через велику кількість проміжних вузлів відкритої мережі. Водночас для унеможливлення перехоплення інформації та внесення несанкціонованих змін в пакет використовується метод електронного цифрового підпису.

РОЗДІЛ 2 АНАЛІЗ ТЕХНОЛОГІЇ OPENVPN

Даний розділ присвячено ознайомленню з технологією OpenVPN, видами та схемами мережі. Розглянуто також реалізації відмовостійкого VPN- з'єднання на базі технології OpenVPN, зокрема будуть розглянуті загальні відомості про технологію OpenVPN, переваги та недоліки технології OpenVPN.

2.1 OpenVPN, призначення, мережі та схема використання

OpenVPN - це інструмент із відкритим вихідним кодом, який використовується для побудови «site-to-site» VPN мереж з використанням протоколу SSL/TLS або з розділеними ключами. Він виконує роль тунелю для передачі даних через TCP/UDP порт в небезпечній мережі, такій як Інтернет.

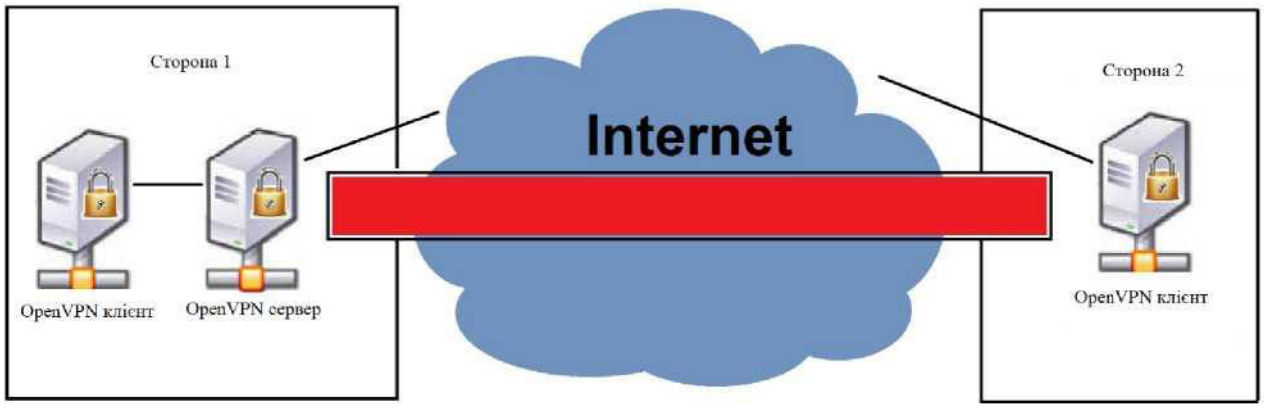

Рисунок 2.1 - Приклад OpenVPN мережі

Можливості які надає OpenVPN:

- Офіційно OpenVPN успішно працює під керуванням наступних ОС: Linux, Solaris, FreeBSD, MacOS, Android, iOS, Windows. Це дозволяє створювати складні крос платформні тунелі. Втім, не складе ніяких труднощів перенести OpenVPN на будь-яку іншу систему, для якої існує драйвер TUN/TUP-пристроїв. До того ж дана розробка незалежна від розміру й старшинства байтів у машинному слові, що полегшує перенос на нові ОС.

- Відмінно працює в мережах, де адреси розподіляються за допомогою Dynamic Host Configuration Protocol.

- Дає можливість працювати з будь-якими механізмами шифрування, вбудованими в OpenSSL для захисту переданого трафіку. А це, у свою чергу дозволяє кожному клієнтові вибрати тип, режим роботи й розмір ключа шифру відповідно до індивідуальних переваг.
- Для автентифікації дейтаграми, що пересилають по тунелю, можна використати Hash-based Message Authentication code - дайджест.
- Кожна дейтаграма позначається за допомогою спеціальних Identifier (далі ID), створюваних на основі часу відправлення й номеру послідовності. Таким чином, запобігає можливості повторного програвання зловмисником послідовності записаних пакетів. В якості додаткової міри безпеки використаний протокол TLS, що дозволяє автентифікувати сесію за допомогою динамічного обміну сертифікатами. Таким чином, навіть частий обмін між сервером і клієнтом ключами розміром не більш ніж 2048 байт практично не впливає на швидкість передачі тунельованих даних.
- Ще одною корисною з погляду безпеки властивістю є наявність ключа mlock. Він дозволяє заборонити OpenVPN записувати в процесі роботи на жорсткий диск будь-яку інформацію, пов’язану із секретними ключами й даними, переданими по тунелі. Це забезпечує додатковий захист трафіку, який проходить через VPN-сервер.
- У зв’язку з тим, що дана програма є всього лише звичайним користувальницьким додатком, а не частиною ядра, вона може цілком мирно співіснувати з іншими додатками, що використовують TUN/TAP-тунелі.
- Дозволяє зручно працювати через міжмережеві екрани з контролем стану з’єднання. У випадку якщо по тунелю не передаються дані, OpenVPN дозволяє через певні проміжки часу посилати ping, для того щоб не дати міжмережевим екранам розірвати з’єднання через неактивність.

TUN/TAP драйвер забезпечується з відкритим вихідним кодом проекту, що входить до складу всіх сучасних Linux/UNIX дистрибутивів, а також до Windows і Mac OS X. Як і SSL/TLS, він використовується в багатьох проектах, тому він постійно вдосконалюється. Використання TUN/TAP пристроїв надає багато

можливостей OpenVPN. Проста структура OpenVPN приносить більшу безпеку в порівнянні з іншими рішеннями VPN. Наприклад, IPSec має складну структуру зі складними змінами в ядрі, тим самим створюючи безліч можливих лазівок в безпеці.

- Універсальний TUN/TAP драйвер був розроблений для забезпечення підтримки Linux ядра для IP тунелювання трафіка. Це віртуальний мережевий інтерфейс, що позиціонується як універсальний для всіх додатків, і тільки ім'я TUNx або TAPx відрізняє його від інших пристроїв. Кожен додаток, що здатний використати мережевий інтерфейс, зможе використати інтерфейс тунелю. Кожна технологія, що буде використовувати мережеву карту, може бути запущена на інтерфейсі TUN або TAP. Устаткування TAP може бути використане як віртуальний Ethernet адаптер (рис. 2.2).

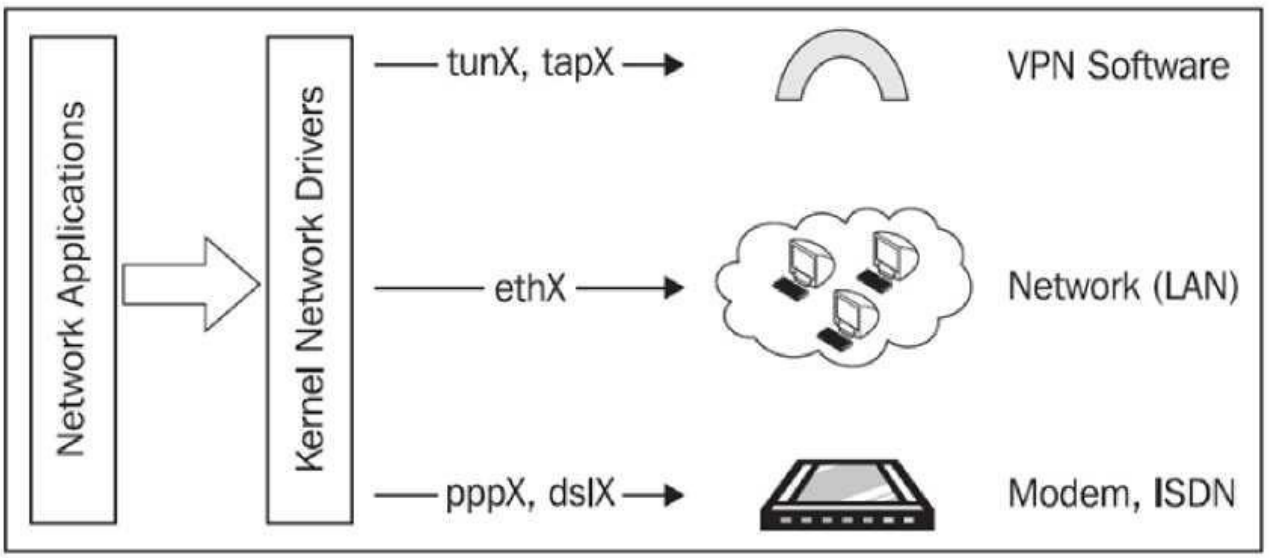

Рисунок 2.2 - OpenVPN з використанням стандартних інтерфейсів

Додатки можуть виконувати зчитування/запис за допомогою цього інтерфейсу, програмне забезпечення (драйвери тунелю) буде приймати всі дані і використовувати криптографічні бібліотеки SSL/TLS для їх шифрування. Пакетні дані відправляються на інший кінець тунелю.

OpenVPN взаємодіє з TUN/TAP устаткуванням, приймає трафік, зашифровує його та відправляє до іншого користувача OpenVPN, де він, у свою чергу одержує дані, розшифровує їх і передає на віртуальне мережеве устаткування, в якому додаток може уже приймати дані.

А оскільки OpenVPN використовує стандартні мережеві пакети, він легко взаємодіє з NAT. Хост у локальній мережі в точці «А» з місцевими IP може почати створювати тунель на інший комп’ютер у локальній мережі в точці «Б», що також оснащений локальним IP.

Оскільки мережевий інтерфейс є стандартним інтерфейсом мережі Linux (TUN або TAP), все що можливо на мережевому Ethernet, може бути зроблене в VPN-тунелі:

- Між мережеві екрани можуть обмежувати й контролювати весь трафік, що проходить в мережі.
- Формування трафіка є винятковою особливістю OpenVPN .

OpenVPN швидше, ніж яке-небудь інше програмне рішення VPN.

OpenVPN прекрасно працює із брандмауерами. Є кілька рішень VPN, які можуть претендувати на аналогічну підтримку мережевого екрану, але ніхто не може запропонувати такий же рівень безпеки.

Правила між мережевого екрану визначають, як поводитися з конкретними даними і трафіком.

Між мережевий екран може бути встановлений на сервері програмного забезпечення, або на інших пристроях. Брандмауер обробляє дані VPN тунелю й може їх вільно пропускати. Залежно від рівня OSI між мережевий екран може приймати рішення на основі даних, знайдених в заголовках пакетів чи даних додатка. Фільтрація пакетів брандмауером працює по принципу фільтрації заголовків IP-даних.

В OpenVPN використовується порт 1194 для підключення до VPN-сервера організацій. Після підключення, весь Інтернет-трафік від цього комп’ютера направляється через мережу організацій за допомогою VPN-з’єднання.

Модульна структура OpenVPN може мати місце не тільки в моделі забезпечення її безпеки, але також і в мережевій схемі. Джеймс Йонен вибрав універсальний драйвер TUN/TAP для мережевого рівня OpenVPN.

В наш час багато компаній вважають своїм обов’язком організовувати VPN

канали для своїх співробітників, що працюють віддалено (рис. 2.3).

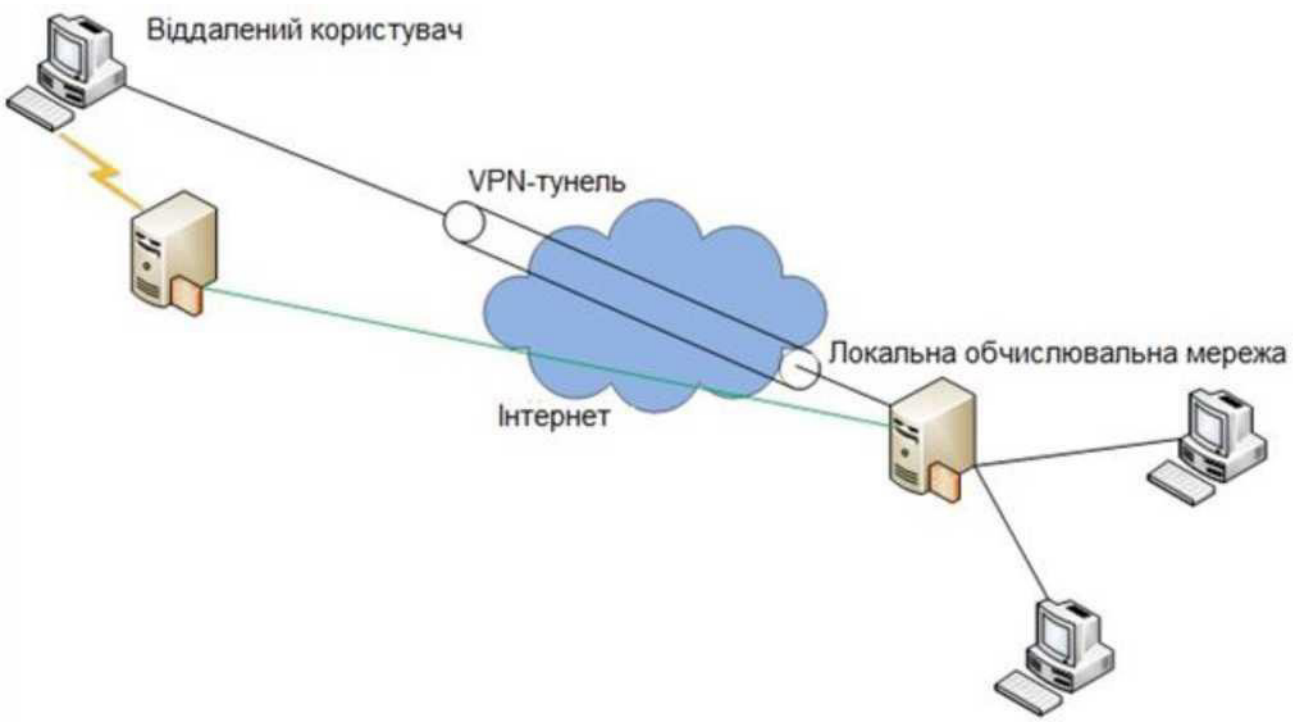

Рисунок 2.3 - VPN для віддалених користувачів.

VPN модель, яка зображена на рис. 2.4 представляє концепцію об'єднання окремих АРМ або цілих локальних мереж у віртуальну мережу, яка забезпечує цілісність та безпеку даних що передаються в цій мережі. Вона має властивості виділеної приватної мережі і дозволяє передавати дані між двома комп'ютерами через проміжну мережу, наприклад Інтернет.

OpenVPN відрізняється низкою економічних переваг порівняно з іншими методами віддаленого доступу.

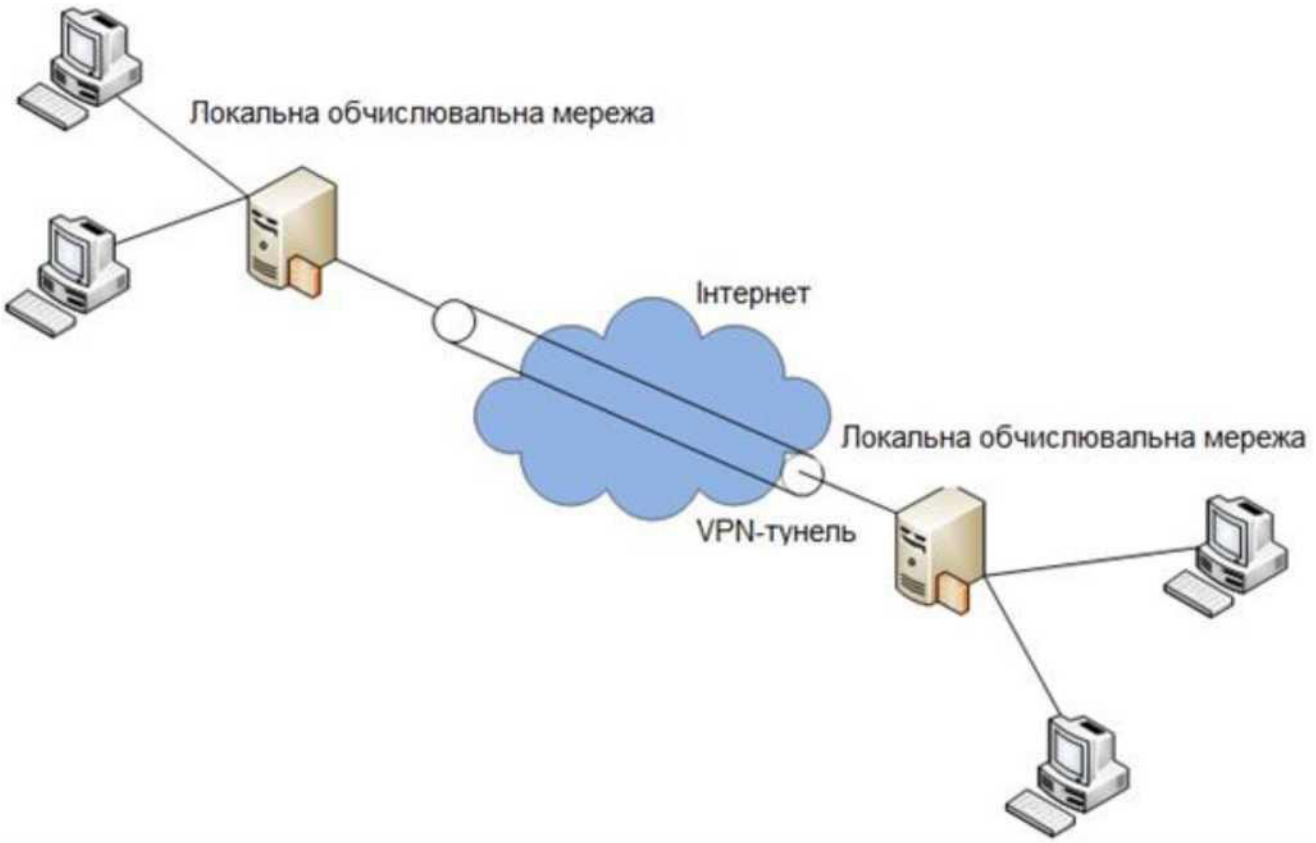

Рисунок 2.4 - VPN для двох локальних мереж

Маючи доступ до Інтернету, будь-який користувач може з легкістю підключитися до внутрішньої мережі фірми. Слід зауважити, що загальнодоступність цих даних аж ніяк не означає їх незахищеність. Система безпеки OpenVPN - це броня, яка захищає всю інформацію що циркулює в корпоративній мережі від несанкціонованого доступу сторонніх осіб. Насамперед, інформацію яка передається в зашифрованому вигляді. Прочитати отримані дані може тільки власник ключа до шифру. [16]

2.2 Переваги та недоліки протоколу OpenVpn.

З OpenVPN, вийшла на сцену як VPN нового покоління. У той час коли інші вирішення для VPN часто використовують власні або нестандартні механізми, у OpenVPN є модульне поняття, як для основної безпеки так і для мережі. OpenVPN використовує безпечні, стабільні, і популярні механізми SSL/TLS для автентифікації і шифрування, користувач не страждає від складності, що характеризує інші реалізації VPN, такі як лідер ринку - IPsec. Одночасно, це пропонує можливості, що йдуть поза будь-яким обсягом реалізації VPN:

- VPN Рівня 2 і Рівня 3: OpenVPN пропонує два основні режими, які

працюють або як VPN Рівня 2 або як VPN Рівня 3. Таким чином тунелі OpenVPN можуть транспортувати Ethernet фрейми, пакети IPX і мережу перегляду пакетів у Windows (NetBIOS), всі перераховані є проблемами в більшості інших вирішень для VPN.

- Захист віддалених робочих з внутрішнім брандмауером: віддалений робочий, з'єднаний з центральним відгалуженням його компанії тунелем VPN, може змінити мережеві налаштування на його комп'ютері, так, щоб весь його мережевий трафік був відправлений через тунель. Як тільки OpenVPN встановив тунель, брандмауер в центральному відгалуженні компанії може захистити ноутбук, навіть при тому, що це не локальна машина. Віддаленим робочим повинен бути відкритий тільки один мережевий порт для локальної мереж. Співробітник захищений центральним брандмауером кожен раз, коли він з'єднаний з VPN.
- З'єднання OpenVPN можуть бути тунельовані майже через кожен брандмауер: Якщо є доступ до Інтернету і якщо ми можемо отримувати доступ до веб-сайтів HTTPS, тунелі OpenVPN повинні працювати без додаткових налаштувань.
- Підтримка за дорученням і конфігурації: OpenVPN має підтримку за дорученням і може бути налаштований, щоб працювати як служба TCP або UDP, і як сервер або клієнт. Як сервер, OpenVPN просто очікує, поки клієнт не запитує з'єднання, тоді працюючи як клієнт, він намагається встановити з'єднання згідно своєї конфігурації.
- Достатньо, щоб хоча б один порт в брандмауері був відкритий, щоб дозволити вхідні з'єднання:
- Починаючи з OpenVPN 2.0 спеціальний режим сервера дозволяє багаторазові вхідні з'єднання на тому ж порту TCP або UDP, використовуючи різні конфігурації для кожного з'єднання.
- Віртуальні Інтерфейси дозволяють дуже конкретні мережі і правила брандмауера: Всі правила, обмеження, передаючи механізми і поняття як NAT можуть використовуватися з тунелями OpenVPN.
- Висока гнучкість з великими можливостями сценаріїв: OpenVPN

пропонує численні точки під час з'єднання, встановленого, щоб запустити окремі сценарії. Ці сценарії можуть використовуватися для великої різноманітності цілей від автентифікації до відмовостійкості і більше.

- Прозора, високоефективна підтримка динамічних IPs: За допомогою OpenVPN більше немає ніякої потреби, щоб використовувати статичні IPs по обидві сторони від тунелю. У обох тунельних кінцевих точках може бути доступ DSL з динамічним IPs, і користувачі досить рідко будуть помічати зміну IP з обох сторін. Буде тільки здаватися що сеанси термінального сервера Windows і сеанси безпечної оболонки (SSH) зависнуть, протягом декількох секунд, але не закінчяться і продовжать ті дії, які вимагаються після короткої паузи.
- Ніяких проблеми з NAT: І сервер OpenVPN і клієнти можуть бути в мережі, використовуючи тільки приватні IP-адреси. Кожен брандмауер може використовуватися, щоб відправити тунельний трафік в іншу тунельну кінцеву точку.
- Проста установка на будь-якій платформі: І установка і використання неймовірно прості. Особливо, якщо спробувати встановити з'єднання IPsec з різними реалізаціями, ми звернемо увагу на OpenVPN.
- Модульна конструкція: Модульна конструкція з високим ступенем простоти, прославлена і в безпеці і в мережах. Ніяке інше вирішення для VPN не може запропонувати такий же діапазон можливостей на цьому рівні безпеки.
- Відсутність апаратної реалізації компенсується високою пропускною спроможністю до 20Мб/с навіть на сервері з 1ГГц процесором.
- Проте у OpenVPN є декілька слабких місць:
- Він не сумісний з IPsec, а IPsec - це стандартне рішення для VPN. Багато пристроїв, як маршрутизатори Cisco або Bintec, використовують IPsec і можуть з'єднуватися з додатками інших виробників або клієнтів програмного забезпечення IPsec.
- Немає простого та інтуїтивно зрозумілого робочого GUI для адміністрування (але є деякі перспективні проекти).
- Отже, основні слабкі місця OpenVPN - це несумісність з IPSec і

відсутність загальновідомого факту про його функції і виробників устаткування.

- Сумісності OpenVPN і IPSec ніколи не буде, ймовірно, тому що їхні архітектури занадто відрізняються.[7,10]

2.3 Реалізація відмовостійкого з'єднання на базі програмного забезпечення OpenVpn.

У час розвитку інформоційно-коммунікаційних систем одне з важливіших місць займає доступність та безпека інформації Головним чинником у цій справі є використання безпечних потоків для її передачі а також забезпечення доступності та цілісності. Використання віртуальних приватних мереж є стандартом для безпечного віддаленого доступу та об'єднання мереж через незахищений простір наприклад Інтернет та надання віддаленого доступу до приватної мережі організації.

Щоб організувати віддалений доступ користувачів до ресурсів корпоративної мережі може використовуватись VPN.

Для максимального захисту корпоративної мережі, доступ до неї, віддалені користувачі можуть получити лише через VPN-з'єднання з сервером організації.

Таке рішення мінімізує втручання в корпоративну мережу, оскільки підключення з зовнішньої мережі можливе лише через VPN-сервер організації. Всі інші з'єднання буде автоматично відхиляти Firewall.

Таким чином у нас існує лише одна підконтрольна нами точка доступу в корпоративну мережу. Разом з цим постає проблема забезпечення постійної доступності цього входу. Подібно з будь якою будівлею необхідно створити «запасний вхід» на випадок атаки, відмови, або його фізичне пошкодження. Це забезпечить більш надійний доступ для доступу та користування корпоративною мережею.

Саме так постає завдання створення відмовостійкого з'єднання методом створення резервного каналу зв'язку з корпоративною мережею. Простими словами

нам необхідно налаштувати два фізично рознесені VPN-сервери, які слугуватимуть нам входом в корпоративну мережу. У разі втрати з'єднання з першим, клієнт матиме можливість відновити з'єднання через резервний канал.

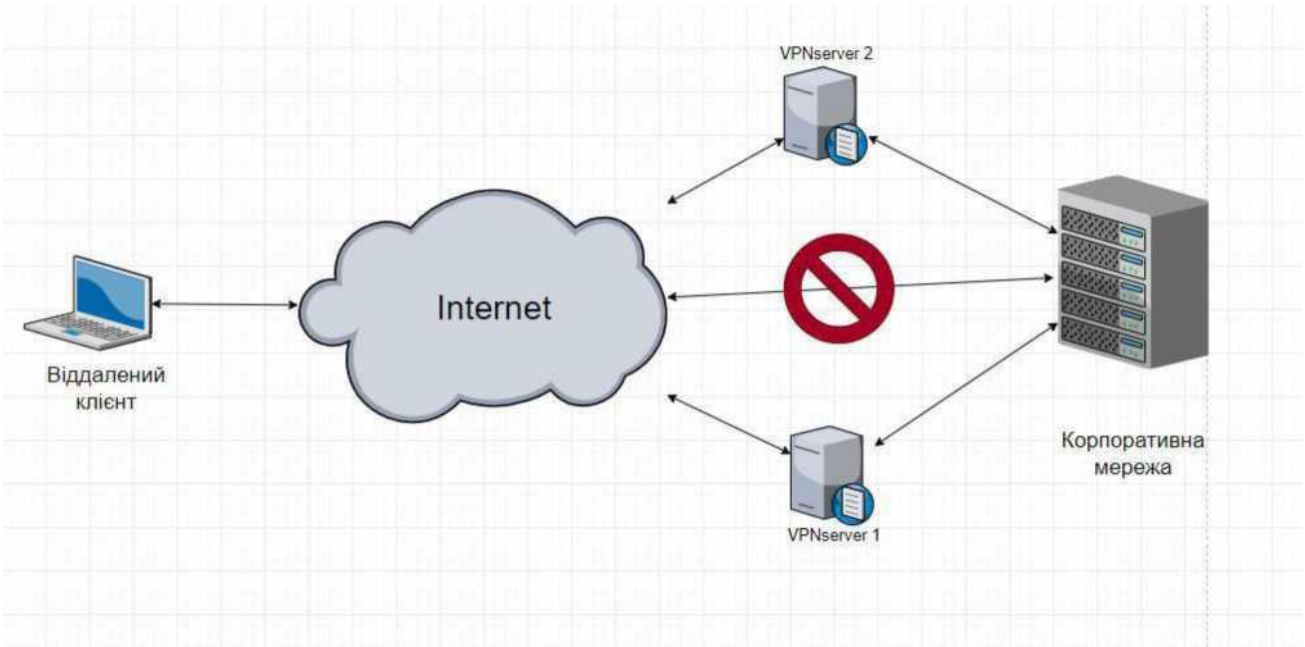

Рисунок 2.5 - Загальний вигляд відмовостійкого з'єднання.

Для реалізації даної задачі буде використано три віртуальні виділені сервери на базі операційної системи: Ubuntu 16.04.06. На основі серверів 1 та 2 буде розгорнуто VPN-сервери шляхом використання програмного забезпечення OpenVpn. Сервер 3 моделюватиме корпоративну мережу з Firewall, який дозволяє зовнішні підключення лише з IP-адресів серверів 1 та 2.

2.4 Порівняння продуктивності алгоритмів шифрування які підтримує OpenVPN.

Окрім надійності алгоритму однією з важливих задач шифрування є продуктивність. Проведемо дослідження швидкості роботи програмної реалізації різних алгоритмів шифрування та виберемо оптимальний який підтримує OpenVPN.

OpenVPN підтримує такі види шифрування:

- DES-CBC
- DES-EDE-CBC
- DES-EDE3-CBC
- DESX-CBC
- BF-CBC
- RC2-40-CBC
- CAST5-CBC
- RC2-64-CBC
- AES-128-CBC
- AES-192-CBC
- AES-256-CBC

Для дослідження використаємо бібліотеку Crypto++ Library 8.6 яка працює з компілятором Visual Studio 2003 – 2019. Для тестування було використано ЕОМ з процесором Intel Core 2 1.83 GHz. Тестування проводилось в режимі роботи одного ядра.

Таблиця 2.1 – Порівняння продуктивності алгоритмів шифрування

	Розмір ключа	MiB/S	Циклів на байт	Мікросекунди до налаштування ключа
DES- CBC	56	32	54.8	8.322
DES-EDE3	56	13	134.6	27.417
DESX-CBC	566	29	60.7	8.509
BF-CBC	32-448	58	30.0	62.783
AES/CBC (128-bit key)	128	109	16.0	0.549
AES/CBC (192-bit key)	192	92	18.9	0.582
AES/CBC (256-bit key)	256	81	22.7	0.629

За результатами тестування вияснили максимальну швидкість обчислення алгоритмами невеликих блоків випадково згенерованих даних.

Алгоритм DES з розміром ключа 56-біт не забезпечує необхідного рівня стійкості шифрування.

Алгоритм BlowFish навіть при використанні короткого ключа 32-біт є помітно повільнішим ніж алгоритм AES з довжиною ключа 256-біт.

Алгоритм AES з будь-якою довжиною ключа забезпечує високу швидкість обчислення. Тому жертвуючи 20% продуктивності можна використовувати максимально можливу довжину ключа 256-біт

Для реалізації поставленої задачі, доцільно вважати алгоритм AES-256-CBC найбільш оптимальним в плані швидкості передачі даних та достатньо стійким для забезпечення конфіденційності.[22]

Висновки до розділу 2

В розділі продемонстровано, що одним з провідних VPN рішень є безкоштовна технологія OpenVPN - VPN з відкритим вихідним кодом, з побудовою з'єднань типу "точка-точка". З появою технології OpenVPN, послуги якісного VPN стали доступні для всіх охочих. Нами також було розглянуто призначення та можливості OpenVPN, а саме можливість його роботи на таких ОС як: Linux, Solaris, FreeBSD, NetBSD, MacOS, Windows, iOS, Android, можливість роботи з будь-якими механізмами шифрування, які вбудовані в OpenSSL, для захисту переданого трафіку, використання механізму HMAC та співіснування з іншими мережевими додатками.

Окрім цього, ми дослідили основні типи мереж, де використовується технологія OpenVPN та протоколи зв'язку, що дозволяють вирішити ряд задач, які постійно виникають перед адміністраторами комп'ютерних мереж: керування OpenVPN, адже OpenVPN досить гнучка в налаштуванні та розгортанні.

Разом з цим, в даному розділі було висвітлено методи забезпечення безпеки, що використовуються в OpenVPN. Досліджено продуктивність різних алгоритмів шифрування, що підтримує OpenVPN. На основі отриманих даних проведено

порівняння продуктивності роботи даних алгоритмів шляхом обчислення невеликих блоків випадково згенерованих даних.

Сьогодні, лише OpenVPN може безкоштовно забезпечити припустимий рівень безпеки інформації, використовуючи досить прості протоколи та механізми захисту. Він не поступається іншим готовим VPN рішенням, за встановлення і користування якими доводиться платити доволі значні суми коштів. Також були розглянуті різні види реалізації технології OpenVPN, вказані переваги і недоліки кожного способу та ознайомлено з принципами тунелюванням мереж.

Детальний практичний аналіз, використання технології OpenVPN та практична організація відмовостійкого з’єднання будуть продемонстровані у наступному розділі.

РОЗДІЛ 3 ОРГАНІЗАЦІЯ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ПІДКЛЮЧЕННЯ ДО РЕСУРСІВ КОРПОРАТИВНИХ МЕРЕЖ ВИКОРИСТОВУЮЧИ ТЕХНОЛОГІЮ OPENVPN

3.1 Описання проблеми та моделювання мережі.

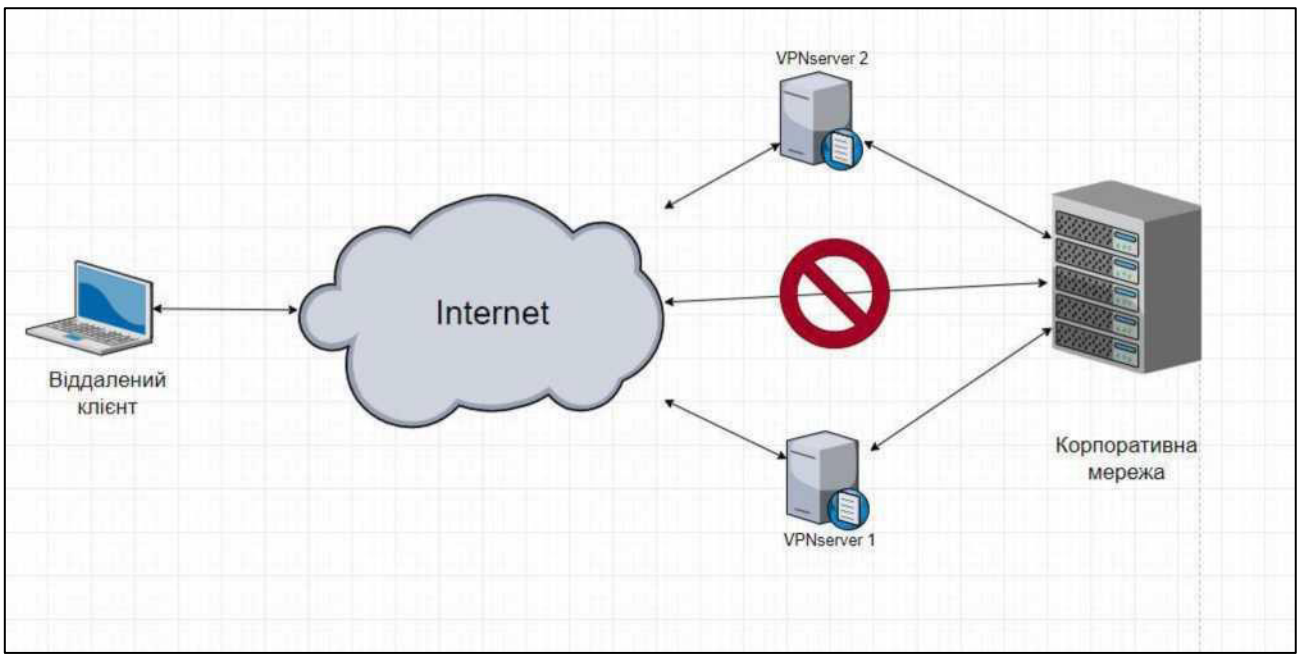

Рисунок 3.1 - Загальна схема реалізації відмовостійкого з’єднання

На рисунку показано, що сервер 3 моделює корпоративну мережу з Firewall, який дозволяє зовнішні підключення лише з IP-адресів серверів 1 та 2.

Апаратним забезпеченням для організації мережі та VPN-серверів слугують віртуальні виділені сервери компанії Digital Ocean. Використання віддалених виділених віртуальних серверів, на протиставлення з використанням технології віртуалізації VMware створює підключення через реальну мережу Internet, створює умови максимально наближені до реальної мережі.

Компанія Digital Ocean спеціалізується на хмарних технологіях.. Вони надають майданчик не тільки для розробників, але і звичайних користувачів, а настройка віртуальної машини проводиться порівняно швидко та просто.

Основні характеристики серверів:

Сервер 1:

- IP: 134.209.83.196

- Операційна система: Ubuntu 16.05.7 x64

Сервер 2:

- IP: 134.209.91.71
- Операційна система: Ubuntu 16.05.7 x64

Сервер 3:

- IP: 206.189.12.64
- Операційна система: Ubuntu 16.05.7 x64

3.2 Створення реальної моделі відмовостійкої мережі.

В даній роботі було налаштовано OpenVPN з технологією обміну сертифікатів.

Для налаштування будь-яких технологій та мережевих протоколів, що використовуються в мережі, обов'язково повинна бути налаштована правильна мережева взаємодія.

Налаштування мережі виконується на Ubuntu 16.05.7 x64.[11]

3.2.1 Встановлення OpenVPN

Спочатку встановимо OpenVPN на наш сервер. OpenVPN доступний в стандартних репозиторіях Ubuntu. Також ми встановимо пакет easy-rsa. Він дозволяє налаштувати наш власний внутрішній центр сертифікації (certificate authority, CA) для використання з нашим VPN.

Оновимо список пакетів сервера і встановимо необхідні пакети наступними командами:

```
#sudo apt-get update
#sudo apt-get install openvpn easy-rsa
```

Необхідне програмне забезпечення встановлено і готове до налаштування.[15]

3.2.2 Створення директорії центру сертифікації

OpenVPN використовує сертифікати для шифрування трафіку між сервером і клієнтами. Для випуску довірених сертифікатів (trusted certificates) нам буде потрібно створити наш власний центр сертифікації.

Для початку скопіюємо шаблонну директорію easy-rsa в нашу домашню директорію за допомогою команди make-cadir та зайдемо в цю директорію для початку налаштування ЦС:

```
#make-cadir ~/openvpn-ca

#cd ~/openvpn-ca
```

3.2.3 Налаштування центру сертифікації

Для настройки змінних нашого центру сертифікації нам необхідно відредагувати файл vars. Відкрийтємо цей файл у текстовому редакторі NANO:

Всередині файлу знаходяться змінні, які можна відредагувати, і які задають параметри сертифікатів при їх створенні. Нам потрібно змінити лише кілька змінних.

Потрібно перейти ближче до кінця файлу і знайти налаштування полів, які використовуються за замовчуванням при створенні сертифікатів. Вони повинні виглядати приблизно так:

```
export KEY_COUNTRY="US"
export KEY_PROVINCE="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@myhost.mydomain"
export KEY_OU="MyOrganizationalUnit"
```

Лістинг 3.1. - файл конфігурації OpenVPN.

Потрібно замінити стандартні значення, на що-небудь інше, не залишаючи їх не заповненими:

```
export KEY_COUNTRY="UA"
export KEY_PROVINCE=TE"
export KEY_CITY="TERNOPIL"
export KEY_ORG="TNTU"
export KEY_EMAIL="kosmyna@example.com"
export KEY_OU="CorpVPN"
```

Лістинг 3.2. - необхідний вигляд файлу конфігурації OpenVPN .

Потрібно також для простоти відредагувати значення KEY_NAME, яке заповнює поле суб'єкта сертифікатів. Для простоти можна задати йому назву server:

```
export KEY_NAME="server"
```

Лістинг 3.3. - необхідний параметр значення KEY_NAME конфігурації OpenVPN

3.2.4 Створення центру сертифікації

Тепер можна використовувати задані змінні і утиліти easy-rsa для створення центру сертифікації. Потрібно перейти в директорію центру сертифікації і використати команду source до файлу vars:

```
#cd ~/openvpn-ca

#source vars
```

Повинен появитись наступний висновок:

```
NOTE: If you run ./clean-all, I will be doing a rm -rf on /home/sammy/openvpn-ca/keys
```

Лістинг 3.4. - попередження про очищення середовища.

Потрібно працювати в "чистому середовищі", а після цього можна створити кореневої центр сертифікації командою:

```
#./clean-all
#./build-ca
```

Ця команда запустить процес створення ключа і сертифіката кореневого центру сертифікації. Оскільки ми відредагували файл vars та внесли у нього всі змінні, всі потрібні значення будуть введені автоматично:

Перевіряємо коректність усіх данних а отримуємо наступне:

```
Generating a 2048 bit RSA private key +++ .... +++
writing new private key to 'ca.key'
---- 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.
Country Name (2 letter code) [UA]:
State or Province Name (full name) [TE]:
Locality Name (eg, city) [TERNOPIL]:
Organization Name (eg, company) [TNTU]:
Organizational Unit Name (eg, section) [CorpVPN]:
Common Name (eg, your name or your server's hostname) [Vpn server]:
Name [server]:
Email Address [kosmyna@example.com]:
```

Лістинг 3.5. - Створення ключа та сертифіката кореневого центру сертифікації.

Тепер є центр сертифікації, який можна використовувати для створення всіх інших необхідних файлів.

3.2.5 Створення сертифіката, ключа і файлів шифрування для сервера

Далі створюється сертифікат, пара ключів і деякі додаткові файли, які використовуються для здійснення шифрування, для заданого сервера. Потрібно розпочати зі створення сертифіката OpenVPN і ключів для сервера. Це можна зробити за допомогою такої команди:

```
#./build-key-server server
```

Усі необхідні для створення данні знову будуть міститись значення за замовчуванням, передані цій команді , а також значення з файлу vars. Потрібно погодитись з усіма значеннями за замовчуванням, натискаючи ENTER. Challenge password встановлювати не потрібно. В кінці процесу потрібне підтвердження створення сертифіката:

```
Certificate is to be certified until
May 1 17:51:16 2026 GMT (3650 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified,
commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Лістинг 3.6. - кінцеве підтвердження створення сертифікату.

Далі необхідно генерувати стійкі ключі, які будуть використовуватись при обміні ключами. Для прикладу використовується ключі на основі протоколу Діффі-Хеллмана.

Виконуємо команду:

```
#./build-dh
```

Для завершення цієї команди, в залежності від продуктивності сервера, може знадобитися кілька хвилин.

3.2.6 Створення сертифіката і пари ключів для клієнта

Далі необхідно згенерувати сертифікат і пару ключів для клієнта. Взагалі це можна зробити і на клієнтській машині і потім підписати отриманий ключ центром сертифікації сервера, проте, в даній роботі використовується лише один клієнт доцільніше згенерувати підписаний ключ на сервері. Після цього передати його для клієнта.

Оскільки нам необхідні ключ і сертифікат тільки для одного клієнта повторимо команду source для файлу vars, а для простоти розуміння використовується параметр client для створення сертифікату та ключа.

Потрібно створити файли без пароля для полегшення автоматичних з'єднань. Використовується команда build-key:

```
#cd ~/openvpn-ca
#source vars
#./build-key client
```

В ході процесу створення файлів всі значення за замовчуванням будуть введені, оскільки всі значення будуть отримані з файлу vars. Challenge password не встановлюється і підтверджуються всі запити про підписи і підтвердження створення сертифіката.

3.2.7 Налаштування сервісу OpenVPN

Далі потрібно налаштувати сервіс OpenVPN з використанням створених раніше файлів. Копіювання раніше створених файлів в директорію OpenVPN.

Створені раніше файли знаходяться в директорії ~/openvpn-ca/keys, в якій вони і були створені. Необхідно скопіювати їх в директорію /etc/openvpn.

Потрібно створити сертифікат і ключ центру сертифікації, сертифікат і ключ сервера, а також файл Diffie-Hellman:

```
#cd ~/openvpn-ca/keys
#sudo cp ca.crt ca.key server.crt server.key ta.key
dh2048.pem /etc/openvpn
```

Далі потрібно створити файл конфігурації сервера OpenVPN в конфігураційній директорії. Повний опис файлу конфігурації для сервера описано в Додатку Д.

3.2.8 Налаштування мережевої конфігурації сервера

Далі необхідно налаштувати мережеву конфігурацію сервера, щоб OpenVPN міг коректно перенаправляти трафік. Проводиться налаштування перенаправлення IP-адрес. Це налаштування необхідне для коректної роботи сервісу та перенаправлення трафіку через сервер. Спочатку потрібно дозволити серверу перенаправляти трафік. Це ключова функціональність VPN сервера.

Налаштовується це за допомогою наступної команди в файлі

/etc/sysctl.conf:

```
#sudo nano /etc/sysctl.conf
```

На завершення потрібно дозволити маршрутизацію в ядрі. Щоб це зробити

потрібно знайти рядок налаштування *net.ipv4.ipforward* та змінити 0 на1. Видалити "#" з початку рядка, щоб розкоментувати його у файлі /etc/sysctl.conf:

Для застосування налаштувань до поточної сесії потрібно ввести команду:

```
#sudo sysctl -p
```

Щоб OpenVPN працював тільки через потрібний інтерфейс потрібно додати три нові правила в iptables, для цього від імені адміністратора відкривається файл /etc/sysconfig/iptables та записуєтсья в нього таке правило:

```
iptables -t nat -A POSTROUTING -s 192.168.101.0/24 -o ethO -j MASQUERADE
```

Після додання нового правила в iptables, нам потрібно перезавантажити цю службу за допомогою команди:

```
# service iptables restart
```

3.2.9 Відкриття порту OpenVPN і застосування змін

Далі налаштовується сам Firewall для дозволу трафіку в OpenVPN.

Порт і протокол в файлі /etc/openvpn/server.conf не змінювались та залишились стандартними, тоді необхідно дозволити трафік UDP для порту 1194.

```
#sudo ufw allow 1194/udp
```

Тепер потрібно перезавантажити процес UFW для застосування внесених змін:

```
#sudo ufw disable
#sudo ufw enable
```

3.2.10 Включення сервісу OpenVPN

Необхідно запустити сервер OpenVPN. Вказувати ім'я створеного файлу конфігурації не потрібно, оскільки він один та вибирається автоматично.

```
#/etc/init.d/openvpn start
```

Переконаємося, що сервіс успішно запущений командою:

```
#servise openvpn status
```

Якщо все вийшло, вивід команди повинен виглядати приблизно так:

```
openvpn.service - OpenVPN service
Loaded: loaded (/lib/systemd/system/openvpn.service; enabled;
vendor preset: enabled)
Active: active (exited) since Thu 2021-10-06 07:58:10 UTC; 3 days ago
Main PID: 18821 (code=exited, status=0/SUCCESS)
Tasks: 0
Memory: 0B
CPU: 0
CGroup: /system.slice/openvpn. service
Oct 10 06:47:43 server-kos-1 systemd: Starting OpenVPN service...
Oct 10 06:47:43 server-kos-1 systemd: Started OpenVPN service
```

Лістинг 3.7. - статус роботи сервісу OpenVpn.

Після запуску служби OpenVPN, перевіряємо чи піднявся тунель за допомогою команди *# ifixmfig* та отримаємо наступний вивід:

```
tun0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr: 192.168.101.1 P-t-P:192.168.101.2 Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric: 1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:18 errors:0 dropped:0
overruns:0 carrier:0 collisions:0 txqueuelen:100
RX bytes:0 (0.0 B) TX bytes:720 (720.0 B)
```

Лістинг 3.8. - відображення створеного нового мережевого інтерфейсу.

З виводу команди можна побачити, що створений новий мережевий інтерфейс tun0. Отже налаштування відбулось успішно.

3.2.11 Налаштування серверу 2.

Налаштування серверу 2 ідентичне налаштуванню сервера 1 (кроки 1-2,810), окрім кроків де необхідно створювати сертифікати. Для автоматичного переключення серверу необхідно, щоб на усіх серверах були одинакові сертифікати та ключі. Тому необхідно не створювати нові, а копіювати з сервера 1 на сервер 2 такі фали:

ca.crt
server.crt
server.key
ta.key
dh2048.pem

3.2.12 Налаштування серверу 3

Цей сервер буде налаштовано таким чином, щоб дозволяти підключення лише від IP-адрес сервера 1 та 2. Таким чином виконавши команду ping зі сторони клієнта можна перевірити реалізацію VPN-з’єднання та перевірити автоматичну зміну сервера з відновленням з’єднання. На нього не потрібно встановлювати будь-яке додаткове ПО.

В налаштуваннях серверу налаштовується Firewall, та створються такі правила:

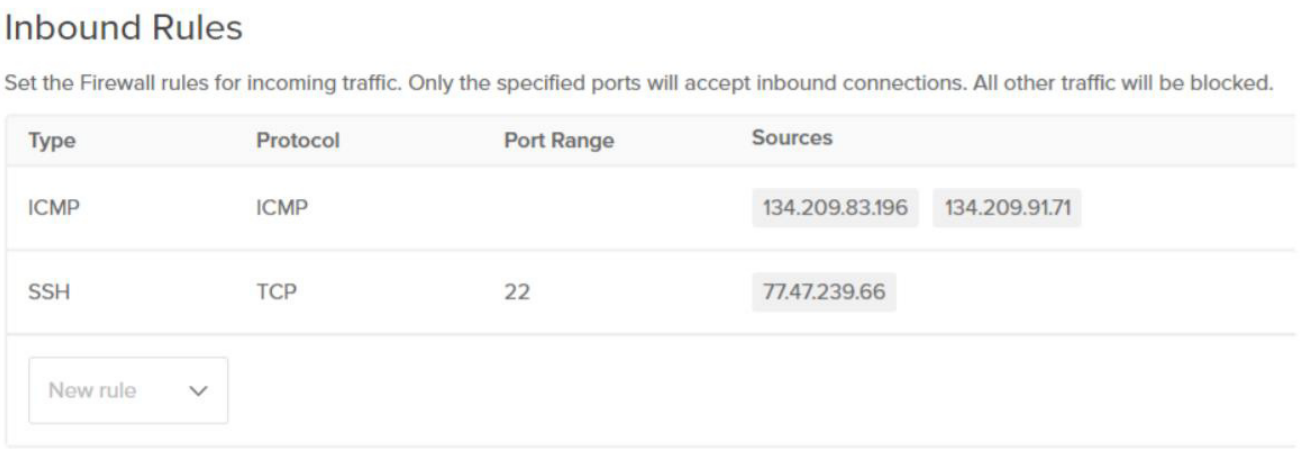

Рисунок 3.1 - Правила для Firewall на сервері 3.

Ці правила створюються лише для сервера 3. Будь-який ICMP-трафік (В цьому випадку запит Ping) буде дозволений лише з IP-адресів VPN-серверів компанії.[12]

Також, дозволений SSH доступ для налаштування серверу з робочої машини. Цей сервер виступає моделлю корпоративної мережі, доступ до якої можливий лише через захищене з'єднання через один з VPN-серверів.

3.3 Порядок дій для налаштування клієнта

У цій роботі представлено налаштування клієнтської сторони для OS Windows.

3.3.1 Завантаження необхідного ПЗ

Завантажити клієнт для роботи з OpenVPN для Windows можна на офіційному сайті зі сторінки завантажень OpenVPN . Використовується найактуальніша версія на даний час - 2.4.7.

3.3.2 Створення файлу конфігурації

Після установки OpenVPN необхідно створити файл конфігурації .ovpn та помістити його в директорію:

C:\Program Files\OpenVPN\config

Для створення з’єднання, яке здатне автоматично змінити підключення постійного сервер на резервний сервер необхідно відредагувати конфігураційний файл та добавити кілька нових змінних:

Опція	Опис
float	Віддалений хост може змінювати IP-адресу в процесі з'єднання, при цьому останнє не буде розірвано.
remote 134.209.83.196	IP-адрес основного сервера до якого підключається клієнт
remote 134.209.91.71	IP-адрес резервного сервера, до якого буде підключатись сервер у разі розірвання з’єднання з першим
connect-retry 2	Перепідключитися до сервера через вказану кількість секунд, якщо з'єднання було розірвано.
connect-retry-max	Скільки разів повторювати з'єднання, якщо воно було розірвано.
keepalive 2 4	Пінгувати кожні 2 секунди сервер і якщо протягом 4 секунд не будуть отримані відповідні пакети, перезапустити підключення. Основна опція, що контролює підключення до серверу

Таблиця 3.1 - Опис основних змінних конфігураційного файлу для клієнта.

Повний опис файлу конфігурації описано в додатку В.

3.4 Практичне виконання відмовостійкого з’єднання

Перед підключенням до VPN-серверу зі сторони клієнта відправляємо ping запит на IP-адрес сервера 3 (рис 3.2). Після запиту можна побачити, що Firewall на сервері 3 налаштований коректно, та відхилив ping запит.

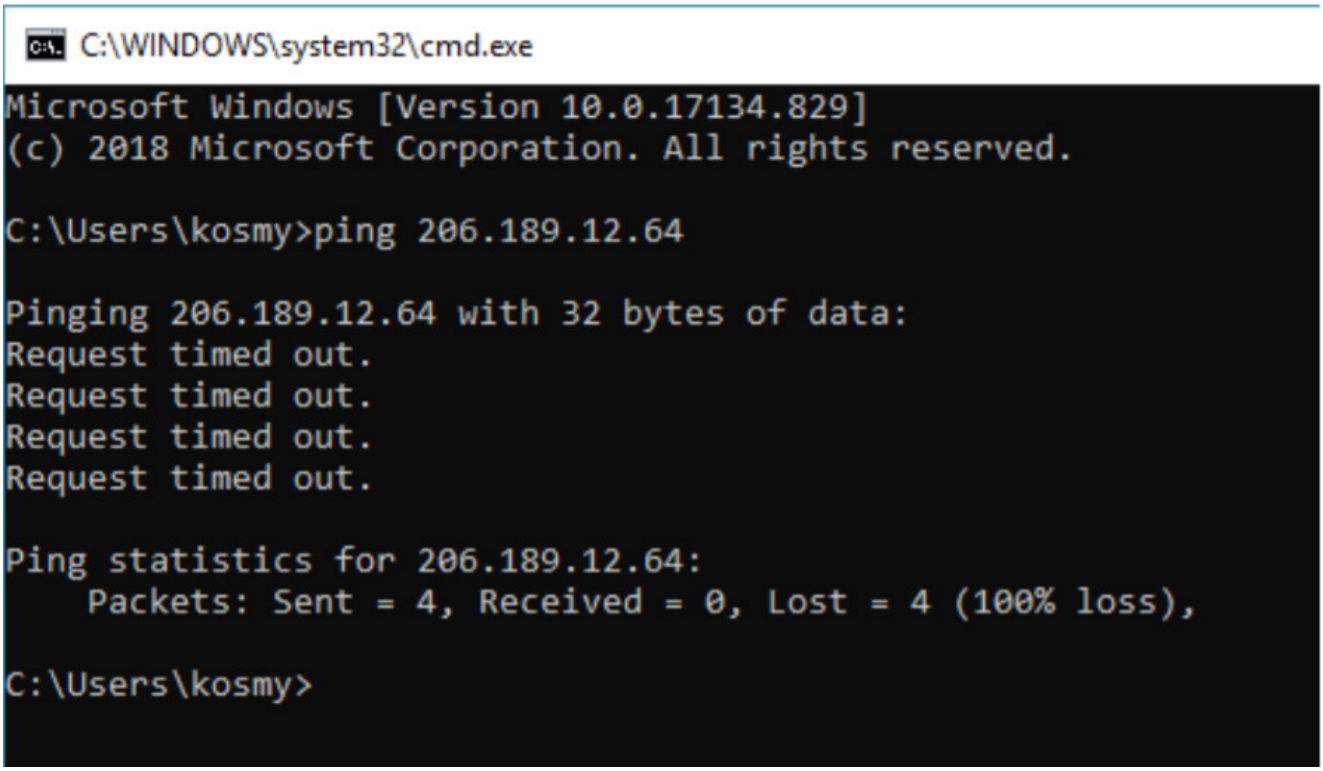

Рисунок 3.2 - Перший Ping запит від клієнта до сервера

Можна впевнитись в тому, що доступу до сервера 3 немає. Виконуєтсья підключення до VPN-серверу через OpenVPN. Клієнт OpenVPN вимагає запуску з правами адміністратора навіть для акаунтів адміністратора (окрім Windows 10).

При включенні OpenVPN, клієнт повинен автоматично побачити налаштований профіль. Для встановлення з'єднання зробіть клацання правою кнопкою миші на іконці OpenVPN в системному треї. У контекстному меню натисніть З’єднати (Connect).

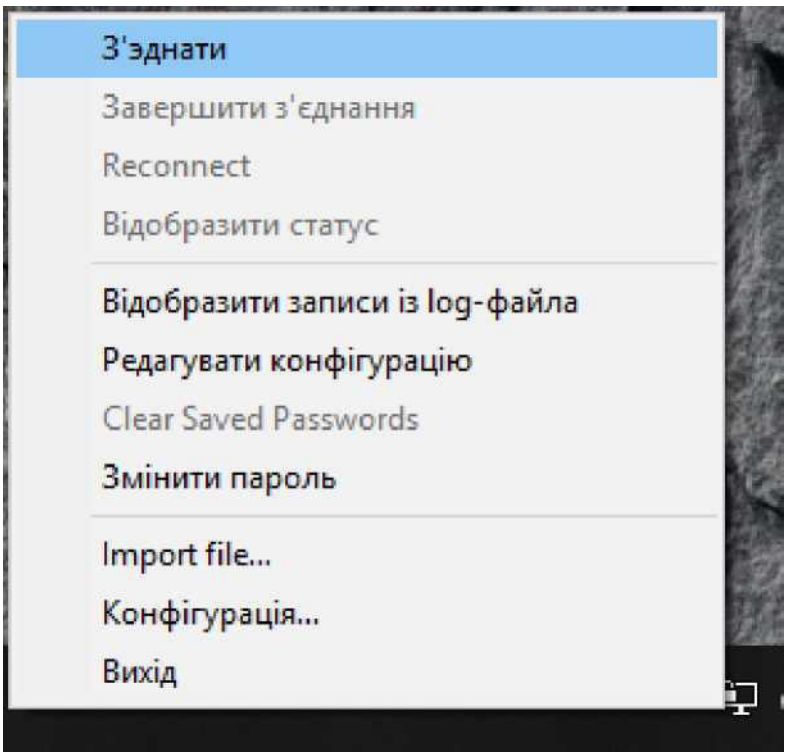

Рисунок 3.3 - Контекстне меню OpenVpn

Відкриється вікно статусу, яке буде відображати лог з'єднання.

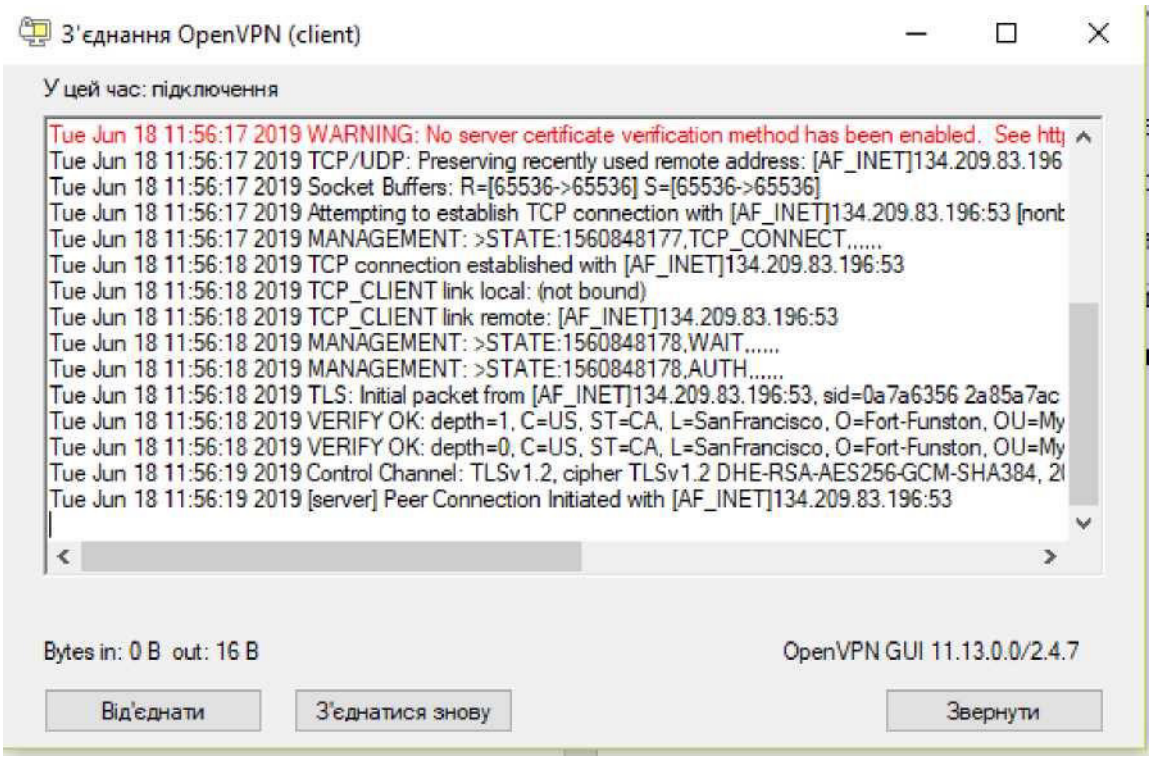

Рисунок 3.4 - Відображення Log-файлу під час підключення

З лог файлу після підключення можна побачити, що тепер ми отримали зовнішню IP-адресу 134.209.83.196.

Після вдалого створення з’єднання можна побачити системне сповіщення про підключення та отримання нової (внутрішньої) IP-адреси.

Рисунок 3.5 - Системне сповіщення, про успішне підключення

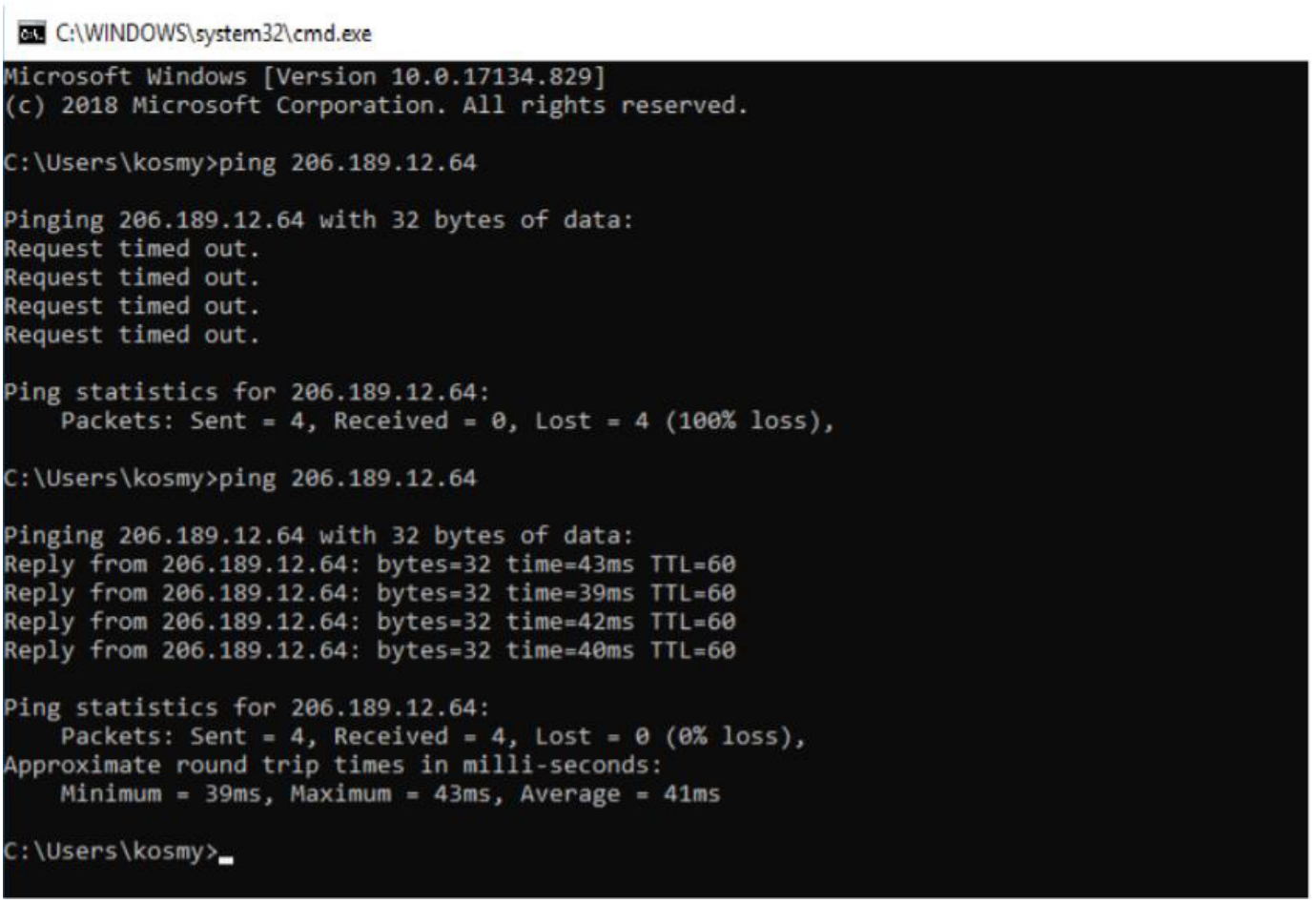

Рисунок 3.6 - Другий Ping запит від клієнта до сервера

Тепер, коли отримано IP-адрес VPN-сервера 1, запит ping дозволений. Тепер, необхідно відключити сервер 1, щоб побачити чи буде переключення автоматичним.

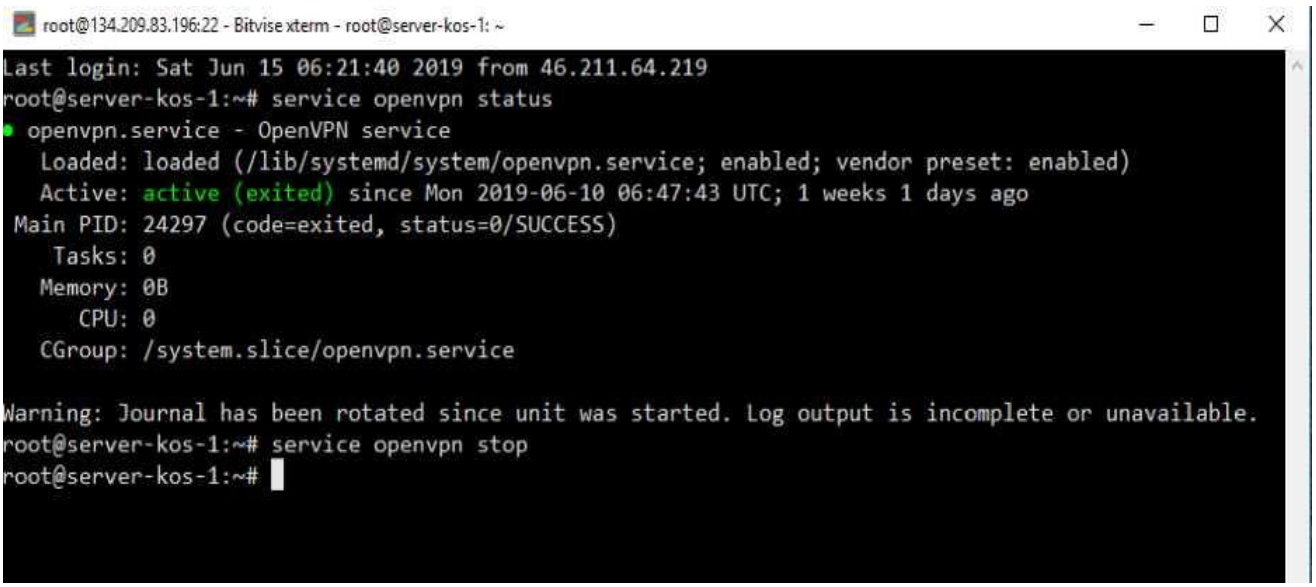

Рисунок 3.7 - Емуляція відмови серверу 1.

Після відключення серверу 1 потрібно переглянути лог файл OpenVpn на клієнті. В лог файлі можна побачити логування всього процесу перепідключення та перевірити чи дійсно пройшла автоматична зміна сервера.

З лог файлу (Лістинг 3.9) після перепідключення можна побачити, що тепер ми отримали зовнішню IP-адресу 134.209.91.71. Перепідключення пройшло вдало, отримана нова IP-адреса .

```
Tue Jun 18 20:56:06 2019 C:\WINDOWS\system32\route.exe ADD
134.209.91.71 MASK 255.255.255.255 192.168.1.1
Tue Jun 18 20:56:06 2019 Route addition via service succeeded
Tue Jun 18 20:56:06 2019 C:\WINDOWS\system32\route.exe ADD 0.0.0.0
MASK 128.0.0.0 192.168.101.5
Tue Jun 18 20:56:06 2019 Route addition via service succeeded
```

Лістинг 3.9 - Лог-запис, який вказує на присвоєння нової IP-адреси.

Повний лог файл після перепідключення показано у додатку Е.

Коли переключення пройшло успішно, після цього повторюємо запит ping. На Рисунку 3.8 можна побачити, що при використанні IP-адреси VPN- сервера 2 ping-запит також проходить успішно.

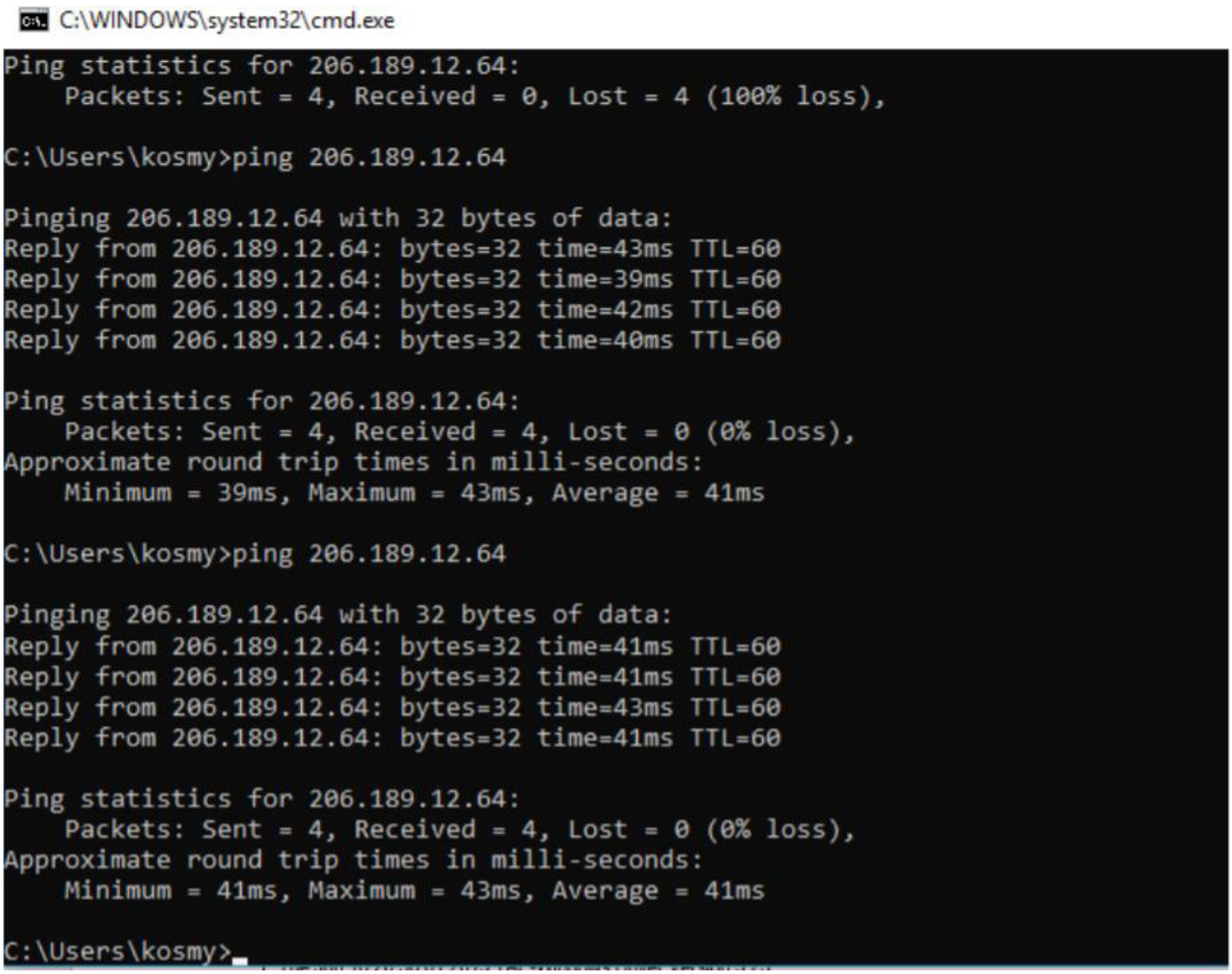

Рисунок 3.8 - Третій Ping запит від клієнта до сервера

Таким чином ми переконались що змодельована нами мережа та основний сервер виконують необхідні функції. Переключення відбувається успішно, про що свідчать ping запити.

Висновки до розділу 3

Під час виконання третього розділу було створено та налаштовано реальну модель VPN-з’єднання, що має достатній рівень захищеності конфіденційної інформації, здатне автоматично змінити підключення постійного сервера на резервний сервер, змодельовано корпоративну мережу, а також, продемонстровано та проаналізовано роботу технології OpenVPN на побудованій відмовостійкій мережі з автоматичною зміною сервера.

Для практичного аналізу було використано спеціальне хмарне середовище DigitalOcean з відповідним програмним забезпеченням, на якому встановлено три операційні системи Ubuntu 16.05.7 x64. Дві з них були налаштовані як VPN-сервери на базі програмного забезпечення OpenVPN. Сервер 3 моделює корпоративну мережу з Firewall, який дозволяє зовнішні підключення лише з IP-адресів серверів 1 та 2.

Для налаштування технології OpenVPN було завантажено бібліотеку easy-RSA а також ПЗ для налаштування самого OpenVPN.

Для роботи з технологією OpenVPN, було створено та налаштовано конфігураційні файли серверів server.conf. Для створення з’єднання, яке здатне автоматично змінити підключення постійного сервера на резервний сервер було створено відредаговано згідно з поставленою задачею конфігураційний файл client.ovpn. Згенеровано усі необхідні ключі та сертифікати для серверів та клієнта.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людини в процесі праці. Головний об'єкт охорони праці - це людина в процесі праці, виробниче середовище, організація праці на виробництві. Основна мета охорони праці - це створення здорових і безпечних умов праці.

Законодавство про охорону праці складається з закону України „Про охорону праці" та інших нормативних актів. Закон України „Про охорону праці" був прийнятий Верховною Радою України 14 жовтня 1992 року і введений в дію з 24 жовтня 1992 року. Він визначає основні положення щодо реалізації конституційного права громадян на охорону, їх життя і здоров'я в процесі трудової діяльності, регулює за участю відповідних державних органів відносини між власником підприємства, установи і організації або уповноваженим їм органом і працівником з питань безпеки, гігієни праці та виробничого середовища і установлює єдиний порядок організації охорони праці в Україні.

Відповідно до Закону «Про охорону праці» роботодавець зобов'язаний створити умови праці в кожному структурному підрозділі та на робочому місці відповідно до вимог нормативних актів та забезпечити дотримання прав працівників, гарантованих положеннями про охорону праці. Очевидно, що відношення керівника до створення служби охорони праці відображає його ставлення до створення безпечних і здорових умов праці, а власне, охорони життя і здоров'я його підлеглих. Робота служби охорони праці спрямована на створення здорових і безпечних умов праці та збереження життя і здоров'я працівників при виконанні трудових обов'язків.

Перш за все, слід розуміти, що відділ охорони праці підприємства повинен забезпечити дотримання чинного законодавства України з питань охорони праці, а також повинен надавати посібники та навчальні матеріали з цих тем, організовувати

роботу у сфері охорони праці, проводити наради, семінари та інші заходи з цих питань.

Одним із найважливіших завдань служби охорони праці є участь у розслідуванні нещасних випадків, професійних захворювань та аварій на виробництві. Фахівці з охорони праці також залучаються до розробки санітарно-гігієнічних норм робочих місць, проводити внутрішні аудити з охорони праці та атестації робочих місць щодо дотримання правил охорони праці, складати професійні та трудові реєстри, згідно з якими працівники підлягають обов'язковим первинним та черговим медичним оглядам; організовувати навчальні курси в галузі охорони праці та роботу комісії з перевірки знань з цих предметів.

Відділ охорони праці підприємства також відповідає за контроль за дотриманням роботодавцем законодавства з охорони праці, тому має право видавати керівникам структурних підрозділів на робочих місцях обов'язкові для виконання інструкції з метою усунення наявних недоліків та отримувати від них інформацію, документацію та пояснення.

4.2 Забезпечення електробезпеки користувачів ПК

Сучасні офісні приміщення, де знаходяться робочі місця з електронно-обчислювальними машинами і персональними комп'ютерами (далі — ЕОМ), за рівнем електробезпеки здебільшого належать до приміщень без підвищеної небезпеки. За способом захисту людини від ураження електричним струмом ПК і мають відповідати I класу захисту. Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями, затверджені наказом Міністерства соціальної політики України від 14 лютого 2018 р. № 207 (далі — НПАОП 0.00-7.15-18).

Сучасний комп'ютер не є електроустановкою, то ж вимоги ПУЕ та ПТЕЕС можуть бути правомірні тільки для мережі його електроживлення, тобто на саму комп'ютерну техніку не поширюються. Вимоги безпеки електрообладнання комп'ютерної техніки регламентують державні стандарти, зокрема, серії ДСТУ EN 60335 та ДСТУ EN 60950.

Під час монтажу та експлуатації ліній електромережі до яких підключені ЕОМ необхідно повністю унеможливити виникнення електричного джерела загоряння внаслідок короткого замикання та перевантаження проводів, обмежувати застосування проводів з легкозаймистою ізоляцією і, за можливості, застосовувати негорючу ізоляцію. Доцільно також використовувати гофровані труби з негорючого матеріалу.

Лінія електромережі для живлення ЕОМ виконується як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення ЕОМ.

Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від групового розподільного щита, розподільного пункту до розеток електроживлення.

У приміщенні, де одночасно експлуатуються понад п'ять ЕОМ, на помітному та доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення.

За способом захисту людини від ураження електричним струмом ЕОМ з ВДТ і ПП мають відповідати I класу захисту згідно з ГОСТ 12.2.007.0-75 "ССБТ. Изделия электротехнические. Общие требования безопасности" та ГОСТ 25861-83 "Машины вычислительные и системы обработки данных. Требования по электрической и механической безопасности и методы испытаний" або мають бути заземлені відповідно до вимог НПАОП 40.1-1.32-01.

Технічні засоби загального (побутового) призначення не повинні використовуватися в умовах підвищеної небезпеки, тож експлуатація сучасної комп’ютерної техніки не належить до робіт підвищеної небезпеки.

Порядок використання комп’ютерної техніки на виробництві визначається настановою з експлуатування її заводу-виробника.

Допуск працівників до роботи з комп’ютерною технікою повинен здійснюватися шляхом проведення навчання, до програми якого мають бути включені питання безпеки під час експлуатації комп’ютерної техніки як

електротехнічного пристрою.

Державні стандарти (ДСТУ EN) для користувачів не вимагають наявності інструкції з охорони праці під час роботи з комп’ютерною технікою, а передбачають правила користування (настанову з експлуатування) від заводу-виробника. Саме тому розробляти окрему інструкцію з охорони праці під час використання на виробництві комп’ютерної техніки недоцільно, достатньо розробити загальну інструкцію з електробезпеки, яка враховує специфіку експлуатації цього обладнання.

Основні вимоги безпеки під час роботи на ПК:

- Не залишати працюючі ПК і їхні пристрої без нагляду.
- Підключати і відключати роз'єм кабелів пристроїв ПК тільки при відключеній напрузі.
- Подавати напругу на пристрої і окремі блоки ПК тільки після ретельної перевірки надійності кріплення провідників заземлення, справності кабелів і роз'ємів мережі електроживлення.
- При виявленні запаху горілого в пристроях ПК необхідно вимкнути апаратуру, повторно не включати і звернутися до спеціаліста з технічного обслуговування ПК.

ВИСНОВКИ

В даній дипломній роботі було розглянуто поняття віртуальної приватної мережі, а також принципи роботи технології та класифікація, зокрема технологія OpenVPN. Основним завданням роботи був загальний огляд технології та визначення факторів, що забезпечують безпечну передачу інформації в умовах використання небезпечних протоколів та публічних мереж, аналіз та порівняння доступних реалізації створення VPN-мережі для бізнесу, аналіз продуктивності алгоритмів шифрування, що підтримуються програмним забезпеченням OpenVPN.

У роботі було розглянуто популярні доступні на ринку реалізації віддаленого захищеного підключення користувачів до корпоративної мережі з використанням технології VPN. Проведеної їх порівняння з самостійною реалізацією з використанням технології OpenVPN

З появою технології OpenVPN, послуги якісного VPN стали доступні для всіх бажаючих. Також розглянуто призначення та можливості OpenVPN, можливість роботи з будь-якими механізмами шифрування, які вбудовані в OpenSSL, використання механізму HMAC та співіснування з іншими мережевими додатками. Окрім цього були розглянуті основні типи мереж, де використовується технологія OpenVPN та протоколи зв’язку.

Було проведено аналіз продуктивності алгоритмів шифрування та за результатом аналізу складено порівняльну таблицю. На основі порівняння було вирішено використовувати алгоритм AES-256-CBC, оскільки він найбільш оптимальний в плані швидкості передачі даних та достатньо стійкий для забезпечення конфіденційності.

Для роботи з технологією OpenVPN, було створено та налаштовано конфігураційні файли серверів server.conf. Для створення з’єднання, яке здатне автоматично змінити підключення постійного сервера на резервний сервер було створено та відредаговано, згідно з поставленою задачею, конфігураційний файл client.ovpn. Згенеровано усі необхідні ключі та сертифікати для серверів та клієнта.

В результаті виконання роботи було розглянуто популярні доступні на ринку реалізації віддаленого захищеного підключення користувачів до корпоративної

мережі та їх порівняння з самостійною реалізацією з використанням технології OpenVPN створено та налаштовано реальну модель VPN-з’єднання, яка здатна автоматично змінити підключення постійного сервера на резервний сервер, у разі втрати з’єднання з першим. Змодельована корпоративна мережа, а також продемонстровано та проаналізовано роботу технології OpenVPN на побудованій відмовостійкій мережі з автоматичною зміною сервера.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Курс «Безопасность Информационных Технологий» [електронний ресурс]. - Режим доступу: http://asher.ru/security/book/its. - назва з екрану.

2. Петренко С. Захищена віртуальна приватна мережа: сучасний погляд на захист конфіденційних даних/Світ Internet. - М.: № 2, 2001;

3. OpenVPN 2 Cookbook 2nd Edition «100 simple and incredibly effective recipes for harnessing the power of the OpenVPN 2 network», Jan Just Keijser, Packt Publishing- 2017.-400c.

4. Mastering OpenVPN, Eric F. Crist and Jan Just Keijser, Packt Publishing- 2015.- 364c.

5. Стаття «VPN и IPSec на пальцах» // URL: https://nestor.minsk.by/sr/2005/03/050315.html, 09.10.2021.

6. Лапонина О. Р. Основи сетевой безопасности. Часть 2. Технологии туннелирования / О. Р. Лапонина. - Москва: Національний Відкритий Университет «ИНТУИТ», 2014. - 249 с. - (474). - (Основи информационньїх технологий).

7. Настройка OpenVPN клиента. // URL: https://www.dmosk.ru/miniinstruktions.php?mini=openvpn- client, 21.09.2021.

8. Національна бібліотека ім. Н. Е. Баумана // VPN URL: https://ru.bmstu.wiki/VPN_(Virtual_Private_Network)/, 09.10.2021.

9. Additional Documentation // openvpn.net URL: https://openvpn.net/community-resources/how-to/, 15.09.2021.

10. OpenVpn community and Wiki // URL: https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage, 15.09.2021.

11. How to Create a Droplet from the DigitalOcean Control Panel // DigitalOcean Docs URL: https://docs.digitalocean.com/products/droplets/how-to/create/, 20.09.2021.

12. Cloud Firewalls // DigitalOcean Docs URL: https://docs.digitalocean.com/products/networking/firewalls/, 20.09.2021.

13. How to Connect to Droplets with SSH // DigitalOcean Docs URL: https://docs.digitalocean.com/products/droplets/how-to/create/, 20.09.2021.

14. Change encryption cipher in Access Server // OpenVpn URL:

https://openvpn.net/vpn-server-resources/change-encryption-cipher-in-access-server/, 21.09.2021.

15. Jan Just Keijser OpenVPN Cookbook - 2nd Edition. Packt Publishing, 2017. 400 c.

16. How a VPN Helps with Network Security // OpenVpn URL: https://openvpn.net/blog/vpns-and-network-security/, 14.09.2021.

17. Adnan Abdulazeez Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol: Iraq, 2021. // URL: https://www.learntechlib.org/p/218341 13.09.2021.

18. SSL Remote Access VPNs (Network Security). Qiang Huang, Jazib Frahim,. Cisco Press, 2008.

19. Sawalmeh, Hanan, et al. "VPN Remote Access OSPF-based VPN Security Vulnerabilities and Counter Measurements." 2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT). IEEE, 2021..

20. Гостеева, А. И., and ЕЕ ИСТРАТОВА. "Сравнительный анализ технологий организации VPN-соединений." Программно-техническое обеспечение автоматизированных систем. 2021.

21. NordVPN URL: https://nordvpn.com/ , 01.11.2021.

22. VPN Comparative Test URL: https://www.av-test.org/fileadmin/pdf/reports/AV-TEST_NordVPN_Comparative_Test_Report_September_2020.pdf, 01.11.2021.

ДОДАТКИ

Додаток А

Тези конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

IX НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

8–9 грудня 2021 року

ТЕРНОПІЛЬ
2021

УДК 004.056
А.С. Космина
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВІДМОВОСТІЙКЕ З'ЄДНАННЯ OPENVPN

UDC 004.89
A.S. Kosmyna

FAULT-TOLERANT CONNECTION OPENVPN

Мережа Інтернет не є тим середовищем передачі інформації, де забезпечується достатній рівень захищеності даних, що передаються. Тому виникає потреба у використанні засобів, що роблять з'єднання безпечним для циркуляції конфіденційної інформації. Одним з таких засобів є організація віртуальних приватних мереж (VPN), які являють собою відокремлену підмножину реальної мережі, що моделюється реальними каналами. Популяризація технології призводить до напливу великої кількості користувачів, які намагаються підключитися до сервера VPN, але внаслідок технічної обмеженості бувають випадки, коли не вдається встановити з'єднання чи постійно виникають обриви з'єднання, що змушує користувача проводити повторне підключення чи обирати інший сервер.

З метою забезпечення неперервності бізнес-процесів та сталого з'єднання або розподілу навантаження між серверами здійснюється організація VPN на основі OpenVPN з функцією автоматичної зміни сервера. Існує декілька варіантів реалізації VPN в залежності від рівня моделі OSI. Технологія OpenVPN має переваги, що виявляються у гнучкому налаштуванні сервера, завдяки чому він підлаштовується під конкретні завдання та вимоги.[1]

Гнучкі налаштування OpenVPN пропонують на вибір достатню кількість алгоритмів шифрування. В сучасних бізнес процесах циркулює великий обсяг інформації, саме тому окрім надійності алгоритму важливу роль відіграє швидкість шифрування та передачі такої інформації. При виборі алгоритму шифрування для реалізації VPN-з'єднання, окрім ступеню захищеності, потрібно звертати увагу на його продуктивність та пропускну здатність. [2]

Саме тому було проведено дослідження продуктивності основних алгоритмів шифрування, що підтримуються OpenVPN. На основі програмної реалізації алгоритмів з використанням бібліотеки Crypto++ Library 8.6 виявлено максимальну швидкість обчислення невеликих блоків випадково згенерованих даних для кожного з алгоритмів.

Реалізація відбувається на основі декількох серверів та кліситів з відповідними налаштуваннями для автоматизації процесу перепідключення та перенаправлення користувачів у разі втрати з'єднання з одним із серверів.

Основним результатом є розгляд організації та переваг VPN на основі OpenVPN з налаштуванням автоматичної зміни сервера, вибір найбільш оптимального алгоритму шифрування на основі захищеності та продуктивності.

Реалізація VPN на основі OpenVPN з автоматичною зміною сервера дозволяє впроваджувати гнучкі налаштування відповідно до поставлених задач та забезпечувати усім користувачам стале й якісне швидкісне з'єднання шляхом унеможливлення обриву з'єднання окрім випадків, коли усі сервери будуть недоступні, а також достатню захищеність мережі передачі інформації.

Література.

1. 1. Електронний ресурс https://sites.google.com/site/ponatievpn/home/klassifikacia-vpn. Last accessed: 27.11.2021
2. OpenVPN 2 Cookbook 2nd Edition «100 simple and incredibly effective recipes for harnessing the power of the OpenVPN 2 network», Jan Just Keijser, Packt Publishing-2017.-400 c.

Додаток Б

Файл конфігурації клієнта

Назва	шифрування	Пропускна здатність	Конфіденційність	Наявність статичного IP	Кількість серверів	Функція автоматичної зміни	Адмін панель користувачів	Складність реалізації	Ціна
NordVPN	Алгоритми невідомі	20-50Мб/с	Не вказано	+40$/міс	33шт	+	+	3/10	Від 9$/М
ExpressVPN	256-bit AES, DNS/IPv6	10-90Мб/с	Заявлено відсутність логування на серверах	-	160шт	-	-	2/10	13$ /М До 5 користувачів
TorGuard	AES-256 encryption with SHA-512--alongside	5-40МБ/с	Заявлено відсутність логування на серверах	10 виділених серверів зі статичним IP	3000 серверів 50 країн	-	-	4/10	169$/М 20 користувачів
Hotspot Shield	Military-grade encryption	20-91Мб/с	Не вказано	-	115шт	+	-	3/10	13$/М До 5 користувачів
Реалізація на базі OpenVPN	DES-CBC DES-EDE-CBC DES-EDE3-CBC DESX-CBC BF-CBC RC2-40-CBC CAST5-CBC RC2-64-CBC AES-128-CBC AES-192-CBC AES-256-CBC	В залежності від алгоритму 30-109Мб/с	Є можливість керувати логуванням	Залежить від провайдера інтернету	Не обмежено	+	Налаштування користувачів в ручному режимі	9/10	

Додаток В

Файл конфігурації клієнта

Опція	Опис
float	Віддалений хост може змінювати IP-адресу в процесі з'єднання, при цьому останнє не буде розірвано.
remote 134.209.83.196	IP-адрес основного сервера до якого підключається клієнт
remote 134.209.91.71	IP-адрес резервного сервера, до якого буде підключатись сервер у разі розірвання з'єднання з першим
connect-retry 2	Перепідключитися до сервера через вказану кількість секунд, якщо з'єднання було розірвано.
connect-retry-max	Скільки разів повторювати з'єднання, якщо воно було розірвано.
keepalive 2 4	Пінгувати кожні 2 секунди сервер і якщо протягом 4 секунд не будуть отримані відповідні пакети, перезапустити підключення. Основна опція, що контролює підключення до серверу
port 53	Вказує на якому порту буде працювати OpenVPN (локально і віддалено)
proto tcp	який протокол буде використовуватися. Можливі значення: udp, tcp, tcp-client, tcp-server. З використанням протоколу udp VPN буде працювати трохи швидше, ніж tcp. Але в плані стабільності роботи краще вибирати tcp .
dev tun	Визначає який використовувати тип пристрою tun або TAP.

persist-key	Вказує не зчитувати файли ключів при перезапуску тунелю.
persist-tun	Ця опція залишає без зміни пристрій tun / TAP при перезапуску OpenVPN.
ca ca.crt	Вказує на файл сертифіката для CA
cert client.crt	Вказує на файл сертифікат локальної машини (клієнта)
key client.key	Вказує на локальний файл ключа машини
cipher AES-256-CBC	Вказує алгоритм шифрування
verb 3	Встановлює рівень інформативності налагоджувальних повідомлень в лог файлі. Може приймати параметр від 0 до 11.
mute 10	якщо значення встановлено в 10, то в лог буде записуватися тільки по 10 повідомлень з однієї категорії.
nobind	використовувати динамічний порт для підключення (тільки для клієнта)
redirect-gateway	Встановлює шлюзом за замовчуванням віддалений сервер. Тобто коли віддалений користувач підключається до нашого сервера, то йому буде поставлено шлюз на наш сервер.

Додаток Д.

Файл конфігурації серверу

port 53	Вказує на якому порту буде працювати OpenVPN (локально і віддалено)
proto tcp	Вказує який протокол буде використовуватися. Можливі значення: udp, tcp, tcp-client, tcp- server. з використанням протоколу udp VPN буде працювати трохи швидше, ніж tcp. Але в плані стабільності роботи краще вибирати tcp .
dev tun	Визначає який використовувати тип пристрою tun або TAP.
tls-server	Явно вказує, що даний хост є tls-server
cipher AES-256-CBC	Вказує алгоритм шифрування
server 192.168.101.0 255.255.255.0	Автоматично привласнює адреси всім клієнтам в зазначеному діапазоні з маскою мережі.
keepalive 10 120	Пінгувати кожні 10 секунди клієнтів і якщо протягом 120 секунд не будуть отримані відповідні пакети,
persist-key	Вказує не зчитувати файли ключів при перезапуску тунелю.
persist-tun	Ця опція залишає без зміни пристрій tun / TAP при перезапуску OpenVPN.

push redirect-gateway	Встановити шлюзом за замовчуванням віддалений сервер. Тобто коли віддалений користувач підключається до нашого сервера, то йому буде поставлено шлюз на наш сервер.
push route 192.168.101.0 255.255.155.0	Передача клієнту конфігураційних параметрів.
ca /etc/openvpn/ca.crt	Вказує на файл сертифіката для CA
cert /etc/openvpn/server.crt	Вказує на локальний файл сертифікат ключа серверу
key /etc/openvpn/server.key	Вказує на локальний файл ключа серверу
dh /etc/openvpn/dh2048.pem	Вказує на локальний файл DH серверу

Додаток Е.

Лог файл клієнта OpenVpn, під час перепідключення.

Tue Jun 18 20:53:56 2019 Connection reset, restarting

Tue Jun 18 20:53:56 2019 C:\WINDOWS\system32\route.exe DELETE 192.168.101.1 MASK 255.255.255.255 192.168.101.5

Tue Jun 18 20:53:56 2019 Route deletion via service succeeded

Tue Jun 18 20:53:57 2019 Closing TUN/TAP interface

Tue Jun 18 20:53:57 2019 TAP: DHCP address released

Tue Jun 18 20:53:57 2019 SIGUSR1[soft,connection-reset] received, process restarting

Tue Jun 18 20:53:57 2019 MANAGEMENT: >STATE: 1560880437,RECONNECTING,connection-reset,,,,,

Tue Jun 18 20:53:57 2019 Restart pause, 1 second(s)

Tue Jun 18 20:53:58 2019 WARNING: No server certificate verification method has been enabled. See http://openvpn.net/howto.html#mitm for more info.

Tue Jun 18 20:53:58 2019 TCP/UDP: Preserving recently used remote address: [AF_INET]134.209.83.196:53

Tue Jun 18 20:53:58 2019 Socket Buffers: R=[65536->65536] S=[65536->65536]

Tue Jun 18 20:53:58 2019 Attempting to establish TCP connection with [AF_INET]134.209.83.196:53 [nonblock]

Tue Jun 18 20:53:58 2019 MANAGEMENT: >STATE:1560880438,TCP_CONNECT,,,,,,

Tue Jun 18 20:55:58 2019 TCP: connect to [AF_INET]134.209.83.196:53 failed: Unknown error

Tue Jun 18 20:55:58 2019 SIGUSR1[connection failed(soft),init_instance] received, process restarting

Tue Jun 18 20:55:58 2019 MANAGEMENT: >STATE: 1560880558,RECONNECTING,init_instance,,,,,

Tue Jun 18 20:55:58 2019 Restart pause, 1 second(s)

Tue Jun 18 20:55:59 2019 WARNING: No server certificate verification method has been enabled. See http://openvpn.net/howto.html#mitm for more info.

Tue Jun 18 20:55:59 2019 TCP/UDP: Preserving recently used remote address:

[AF_INET]134.209.91.71:53
Tue Jun 18 20:55:59 2019 Socket Buffers: R=[65536->65536] S=[65536->65536]
Tue Jun 18 20:55:59 2019 Attempting to establish TCP connection with [AF_INET]134.209.91.71:53 [nonblock]
Tue Jun 18 20:55:59 2019 MANAGEMENT: >STATE:1560880559,TCP_CONNECT,,,,,,
Tue Jun 18 20:56:00 2019 TCP connection established with [AF_INET]134.209.91.71:53
Tue Jun 18 20:56:00 2019 TCP_CLIENT link local: (not bound)
Tue Jun 18 20:56:00 2019 TCP_CLIENT link remote: [AF_INET]134.209.91.71:53
Tue Jun 18 20:56:00 2019 MANAGEMENT: >STATE:1560880560,WAIT,,,,,,
Tue Jun 18 20:56:00 2019 MANAGEMENT: >STATE:1560880560,AUTH,,,,,,
Tue Jun 18 20:56:00 2019 TLS: Initial packet from [AF_INET]134.209.91.71:53, sid=2604e2fd 657bb6c6
Tue Jun 18 20:56:00 2019 VERIFY OK: depth=1, C=US, ST=CA, L=SanFrancisco, O=Fort-Funston, OU=MyOrganizationalUnit, CN=Fort-Funston CA, name=EasyRSA, emailAddress=me@myhost.mydomain
Tue Jun 18 20:56:00 2019 VERIFY OK: depth=0, C=US, ST=CA, L=SanFrancisco, O=Fort-Funston, OU=MyOrganizationalUnit, CN=server, name=EasyRSA, emailAddress=me@myhost.mydomain
Tue Jun 18 20:56:00 2019 Control Channel: TLSv1.2, cipher TLSv1.2 DHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
Tue Jun 18 20:56:00 2019 [server] Peer Connection Initiated with [AF_INET]134.209.91.71:53
Tue Jun 18 20:56:01 2019 MANAGEMENT: >STATE: 1560880561 ,GET_CONFIG,,,,,,
Tue Jun 18 20:56:01 2019 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
Tue Jun 18 20:56:01 2019 PUSH: Received control message: 'PUSH_REPLY,redirect-gateway,route 192.168.101.0 255.255.155.0,route 192.168.101.1,topology net30,ping 10,ping-restart 120,ifconfig 192.168.101.6 192.168.101.5'

Tue Jun 18 20:56:01 2019 Flag 'def1' added to --redirect-gateway (iservice is in use)
Tue Jun 18 20:56:01 2019 OPTIONS IMPORT: timers and/or timeouts modified
Tue Jun 18 20:56:01 2019 OPTIONS IMPORT: --ifconfig/up options modified
Tue Jun 18 20:56:01 2019 OPTIONS IMPORT: route options modified
Tue Jun 18 20:56:01 2019 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
Tue Jun 18 20:56:01 2019 Outgoing Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentication
Tue Jun 18 20:56:01 2019 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
Tue Jun 18 20:56:01 2019 Incoming Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentication
Tue Jun 18 20:56:01 2019 interactive service msg_channel=716
Tue Jun 18 20:56:01 2019 ROUTE_GATEWAY 192.168.1.1/255.255.255.0 I=18 HWADDR=b8:86:87:4a:b9:2b
Tue Jun 18 20:56:01 2019 open_tun
Tue Jun 18 20:56:01 2019 TAP-WIN32 device [Ethernet 2] opened: \\.\Global\{E297E3DC-3B46-46E4-BC67-7B42DBABE895}.TAP Tue Jun 18 20:56:01 2019 TAP-Windows Driver Version 9.23
Tue Jun 18 20:56:01 2019 Notified TAP-Windows driver to set a DHCP IP/netmask of 192.168.101.6/255.255.255.252 on interface {E297E3DC-3B46-46E4-BC67-7B42DBABE895} [DHCP-serv: 192.168.101.5, lease-time: 31536000]
Tue Jun 18 20:56:01 2019 Successful ARP Flush on interface {E297E3DC- 3B46-46E4-BC67-7B42DBABE895 }
Tue Jun 18 20:56:01 2019 MANAGEMENT: >STATE:1560880561,ASSIGN_IP,,192.168.101.6,,,,
Tue Jun 18 20:56:06 2019 TEST ROUTES: 3/3 succeeded len=2 ret=1 a=0 u/d=up
Tue Jun 18 20:56:06 2019 C:\WINDOWS\system32\route.exe ADD 134.209.91.71 MASK 255.255.255.255 192.168.1.1
Tue Jun 18 20:56:06 2019 Route addition via service succeeded

Tue Jun 18 20:56:06 2019 C:\WINDOWS\system32\route.exe ADD 0.0.0.0 MASK 128.0.0.0 192.168.101.5

Tue Jun 18 20:56:06 2019 Route addition via service succeeded

Tue Jun 18 20:56:06 2019 C:\WINDOWS\system32\route.exe ADD 128.0.0.0 MASK 128.0.0.0 192.168.101.5

Tue Jun 18 20:56:06 2019 Route addition via service succeeded

Tue Jun 18 20:56:06 2019 MANAGEMENT: >STATE:1560880566,ADD_ROUTES,,,,,,

Tue Jun 18 20:56:06 2019 C:\WINDOWS\system32\route.exe ADD 192.168.101.0 MASK 255.255.155.0 192.168.101.5

Tue Jun 18 20:56:06 2019 ROUTE: route addition failed using service: The parameter is incorrect. [status=87 if_index=22]

Tue Jun 18 20:56:06 2019 Route addition via service failed

Tue Jun 18 20:56:06 2019 C:\WINDOWS\system32\route.exe ADD 192.168.101.1 MASK 255.255.255.255 192.168.101.5

Tue Jun 18 20:56:06 2019 Route addition via service succeeded

Tue Jun 18 20:56:06 2019 Initialization Sequence Completed

Tue Jun 18 20:56:06 2019 MANAGEMENT: >STATE:1560880566,CONNECTED,SUCCESS,192.168.101.6,134.209.91.71,53,