ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розроблення рекомендацій щодо використання віртуальних приватних мереж для забезпечення віддаленого доступу до корпоративних даних на базі рішення OpenVPN»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Кирило БРОДА
(підпис)

Виконав: здобувач вищої освіти групи БСД-43
БРОДА Кирило
(прізвище, ім'я)

Керівник ГАНЧЕНКО Марія
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ ГАЙДУР Галина
"___" _____ 2024
року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Броді Кирилу Олександровичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розроблення рекомендацій щодо використання віртуальних приватних мереж для забезпечення віддаленого доступу до корпоративних даних на базі рішення OpenVPN»

керівник кваліфікаційної роботи ГАНЧЕНКО Марія
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» лютого 2024 року № 36.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 31.06.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення OpenVPN;
наукова та технічна література, експлуатаційна документація.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Теоретичні аспекти віртуальних приватних мереж.
2. Дослідження можливостей OpenVPN у забезпеченні віддаленого доступу до корпоративних даних.
3. Розробка рекомендацій щодо оптимізації використання OpenVPN для підвищення рівня безпеки корпоративних даних.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 15.04.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту віддаленого доступу.	15.04.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	20.04.2024 р.	
3.	Дослідження можливостей OpenVPN у забезпеченні віддаленого доступу до корпоративних даних	10.05.2024 р.	
4.	Розробка рекомендацій щодо оптимізації використання OpenVPN для підвищення рівня безпеки корпоративних даних.	20.05.2024 р.	
6.	Оформлення результатів дослідження.	23.05.2024 р.	
7.	Підготовка доповіді до захисту.	31.05.2024 р.	

Здобувач вищої освіти _____ Кирило БРОДА
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Марія ГАНЧЕНКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача БРОДИ Кирила

на тему: «Дослідження шляхів та розроблення рекомендацій щодо використання віртуальних приватних мереж для забезпечення віддаленого доступу до корпоративних даних на базі рішення OpenVPN»

Актуальність: Віртуальні приватні мережі (VPN), такі як OpenVPN, забезпечують шифрування трафіку та захист корпоративних даних від несанкціонованого доступу, що є важливим через зростання спектру кіберзагроз. OpenVPN використовує сильні шифрувальні алгоритми, що значно знижує ризик перехоплення конфіденційної інформації при її передачі каналами зв'язку. Зростання тенденції використання організаціями хмарних технологій підвищує потребу в захищених каналах зв'язку, які забезпечує OpenVPN. Гнучкість і масштабованість рішення дозволяє працювати з будь-якої локації (локальна та віддалена робота) та з використанням різних платформ, забезпечуючи стабільний доступ навіть в умовах нестабільного з'єднання. Таким чином використання OpenVPN для здійснення віддаленого доступу до корпоративної мережі та її ресурсів є ефективним та сучасним рішенням для забезпечення безпеки конфіденційних даних будь-якої організації

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми забезпечення віддаленого доступу до корпоративних даних організації, визначено мету та завдання для підвищення безпеки.
2. Досліджено більшість аспектів налаштування протоколу OpenVPN.
3. Запропоновано варіант підвищення захисту в корпоративних мережах за допомогою протоколу OpenVPN, надано інструкції з його розгортання.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. Запропонований варіант підвищення безпеки віддаленого доступу до корпоративних даних за допомогою OpenVPN було б доцільно протестувати у реальному середовищі організації.

Відзначене зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **"добре"**, а здобувач(ка) **БРОДА Кирило** – присвоєння кваліфікації бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім'я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач БРОДА Кирило до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації

освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Дослідження шляхів та розроблення рекомендацій щодо використання віртуальних приватних мереж для забезпечення віддаленого доступу до корпоративних даних на базі рішення OpenVPN».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***БРОДА Кирило*** обрав тему роботи, метою якої було дослідити шляхи використання віртуальних приватних мереж для забезпечення віддаленого доступу до корпоративних даних, а також розробка рекомендації щодо підвищення безпеки кінцевих точок організації на базі рішення OpenVPN. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***БРОДА Кирило*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***БРОДИ Кирила*** на оцінку **"добре"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Марія ГАНЧЕНКО
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **БРОДА Кирило** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 69 сторінок, 33 рисунки, 9 джерел.

Об'єкт дослідження – процес забезпечення безпеки віддаленого доступу до корпоративних даних за допомогою віртуальних приватних мереж.

Предмет дослідження – рішення OpenVPN для забезпечення захищеного віддаленого доступу до корпоративних даних.

Мета роботи дослідження шляхів впровадження та розробка рекомендацій щодо ефективного використання OpenVPN для забезпечення захищеного віддаленого доступу до корпоративних даних. Дослідження включає аналіз технічного застосування та визначення оптимальних налаштувань рішення OpenVPN.

Методи дослідження – опрацювання літератури за даною темою та аналіз експлуатаційної документації.

Системи віртуальних приватних мереж (VPN) відіграють важливу роль у забезпеченні безпеки віддаленого доступу до корпоративних даних. VPN-системи призначені для створення захищеного з'єднання між віддаленим користувачем та корпоративною мережею, що дозволяє зберегти конфіденційність та цілісність переданих даних. Використання VPN забезпечує безпечний доступ до ресурсів організації незалежно від місця знаходження користувача.

У роботі досліджено проблему забезпечення безпечного віддаленого доступу до корпоративних даних, визначено його мету та завдання. Досліджено методи та засоби організації віддаленого доступу на базі рішення OpenVPN. Визначено основні функціональні можливості та компоненти рішення OpenVPN.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ВІРТУАЛЬНА ПРИВАТНА МЕРЕЖА, VPN, OPENVPN, ВІДДАЛЕНИЙ ДОСТУП, ЗАБЕЗПЕЧЕННІ ВІДДАЛЕНОГО ДОСТУПУ ДО КОРПОРАТИВНИХ ДАНИХ, ЗАХОДИ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AES – Advanced Encryption Standard

CRL – Certificate Revocation List (список відкликаних сертифікатів)

ECDHE – Elliptic Curve Diffie-Hellman Ephemeral

HMAC – Hash-based Message Authentication Code

IAM – Identity and Access Management

IP – Internet Protocol

ISP – Internet Service Provider

L2TP – Layer 2 Tunneling Protocol

LDAP – Lightweight Directory Access Protocol

LZO – Lempel-Ziv-Oberhumer

MFA – Multi-Factor Authentication

MTU – Maximum Transmission Unit

NAT – Network Address Translation

OTP – One-Time Password

PKI – Public Key Infrastructure

PPTP – Point-to-Point Tunneling Protocol

QoS – Quality of Service

RADIUS – Remote Authentication Dial-In User Service

RSA – Rivest–Shamir–Adleman (encryption algorithm)

SSH – Secure Shell

SSL – Secure Sockets Layer

TCP – Transmission Control Protocol

TLS – Transport Layer Security

UDP – User Datagram Protocol

VPN – Virtual Private Network

ЦС – Центр Сертифікації

ВСТУП

Актуальність дослідження. У сучасному світі, де все більше організацій переходять до моделі віддаленої роботи, питання безпечного доступу до корпоративних даних набуває критичного значення. Використання віртуальних приватних мереж (VPN) стало одним із ключових методів забезпечення цього доступу. Проте, зростання кіберзагроз та вимоги до безпеки конфіденційних даних ставлять нові виклики перед існуючими рішеннями.

Організації використовують VPN-технології, які не завжди забезпечують належний рівень безпеки або мають проблеми з продуктивністю. Особливо актуальним це питання є для України. Держава постійно стикається з високим рівнем кіберзагроз. Захищений VPN, як OpenVPN, допомагає мінімізувати ризики перехоплення даних та кібератак на підприємства та державних установ. В умовах війни багато українських компаній перейшли на віддалену роботу. OpenVPN забезпечує надійний та безпечний доступ до корпоративних ресурсів для співробітників, що працюють з дому або в інших безпечних місцях. OpenVPN дозволяє безпечно співпрацювати з міжнародними партнерами та клієнтами, забезпечуючи захист даних під час їх передачі.

Розробка рекомендацій щодо використання OpenVPN як рішення для забезпечення безпечного віддаленого доступу є важливим кроком для підвищення рівня кібербезпеки вітчизняних компаній.

Актуальність даної роботи полягає у вирішенні проблеми забезпечення безпечного віддаленого доступу до корпоративних даних, що є невід'ємною частиною загальної системи кібербезпеки будь-якої організації. Тому, у рамках кваліфікаційної роботи, дослідження спрямоване на розробку рекомендацій для впровадження найкращих практик, щодо налаштування та використання OpenVPN. Досліджуване рішення дозволить підвищити захищеність інформації, а надані рекомендації сприятимуть досягненню відповідності стандартам безпеки.

Об'єкт дослідження – процес забезпечення безпеки віддаленого доступу до корпоративних даних за допомогою віртуальних приватних мереж.

Предмет дослідження – рішення OpenVPN для забезпечення захищеного віддаленого доступу до корпоративних даних.

Мета роботи дослідити шляхи впровадження та розробити рекомендації для ефективного використання OpenVPN та забезпечення захищеного віддаленого доступу до корпоративних даних.

Основні задачі роботи:

1. Визначити та класифікувати типи віртуальних приватних мереж, їх ключові особливості.
2. Визначити принцип роботи та архітектуру VPN на базі OpenVPN.
3. Класифікувати загрози та виклики безпеки при використанні VPN.
4. Визначити конфігурацію та налаштування серверу та клієнтів OpenVPN.
5. Визначити налаштування клієнтів для підключення до VPN та розробити інструкції для різних операційних систем.
6. Визначити практичні аспекти використання OpenVPN в корпоративному середовищі.
7. Визначити рекомендації з конфігурації рішення з точки зору підвищення безпеки.
8. Визначити стратегії масштабування та адаптації VPN-інфраструктури під зростаючі потреби бізнесу.

Методи дослідження – опрацювання літератури за даною темою та аналіз експлуатаційної документації.

Практичне значення одержаних результатів полягає у розробці конкретних рекомендацій для фахівців з кібербезпеки щодо впровадження OpenVPN як надійного засобу для забезпечення безпечного віддаленого доступу до корпоративних даних. Запропоновані рекомендації дозволять організаціям підвищити рівень захисту своїх даних, що є критично важливим у сучасних умовах та зростаючому спектрі кіберзагроз.

РОЗДІЛ 1 ТЕОРИТИЧНІ АСПЕКТИ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

1.1 Визначення та класифікація віртуальних приватних мереж

Віртуальна приватна мережа (VPN) - це технологія, яка дозволяє створити захищене з'єднання поверх незахищеної мережі, такої як Інтернет. VPN використовує методи шифрування і аутентифікації для забезпечення конфіденційності, цілісності та автентичності передаваних даних. Основною метою VPN є створення безпечного каналу для передачі даних між віддаленими користувачами та корпоративними мережами або між різними мережами компанії.

Віртуальні приватні мережі (VPN) є важливим елементом сучасної IT-інфраструктури, особливо в корпоративному середовищі. Їх застосування дозволяє забезпечити безпечний доступ до ресурсів компанії з будь-якої точки світу та захист даних при передачі від несанкціонованого доступу. У цьому розділі розглядаються визначення, основні функції та класифікація VPN, зокрема типи з'єднань, включаючи OpenVPN, а також теоретичні аспекти їх використання в корпоративних мережах.

З метою забезпечення конфіденційності та безпеки користувачів в Інтернеті, VPN дозволяє шифрувати трафік, що передається між пристроєм користувача і веб-сайтами чи сервісами, з якими він взаємодіє.

На рисунку 1.1.1 представлено, роботу VPN, а саме:

1. Пристрій користувача, наприклад, комп'ютер або смартфон, який підключається до Інтернету через VPN.
2. VPN-клієнт на пристрої користувача шифрує дані перед їх передачею через Інтернет. Це забезпечує захист даних від перехоплення.
3. Після шифрування дані проходять через Інтернет-провайдерів (ISP). Завдяки шифруванню, провайдери не можуть бачити зміст трафіку користувача.
4. Зашифрований VPN-тунель, через який передаються дані від пристрою користувача до VPN-сервера. Такий тунель забезпечує конфіденційність даних під час їх передачі через мережу.

5. Після того, як дані досягають VPN-сервера, вони декодуються і передаються в Інтернет. Вебсайти та сервіси бачать IP-адресу VPN-сервера замість справжньої IP-адреси користувача.
6. Веб-сервіси отримують запити від IP-адреси VPN-сервера, що приховує справжню IP-адресу користувача.

Завдяки VPN, користувач може захистити свої дані від різних загроз, таких як хакери, несанкціоноване спостереження з боку Інтернет-провайдерів, компаній, агентств чи роботодавців. На рисунку 1.1.1 червоними шестикутниками позначено загрози для яких вміст зашифрованих даних є недоступним [1].

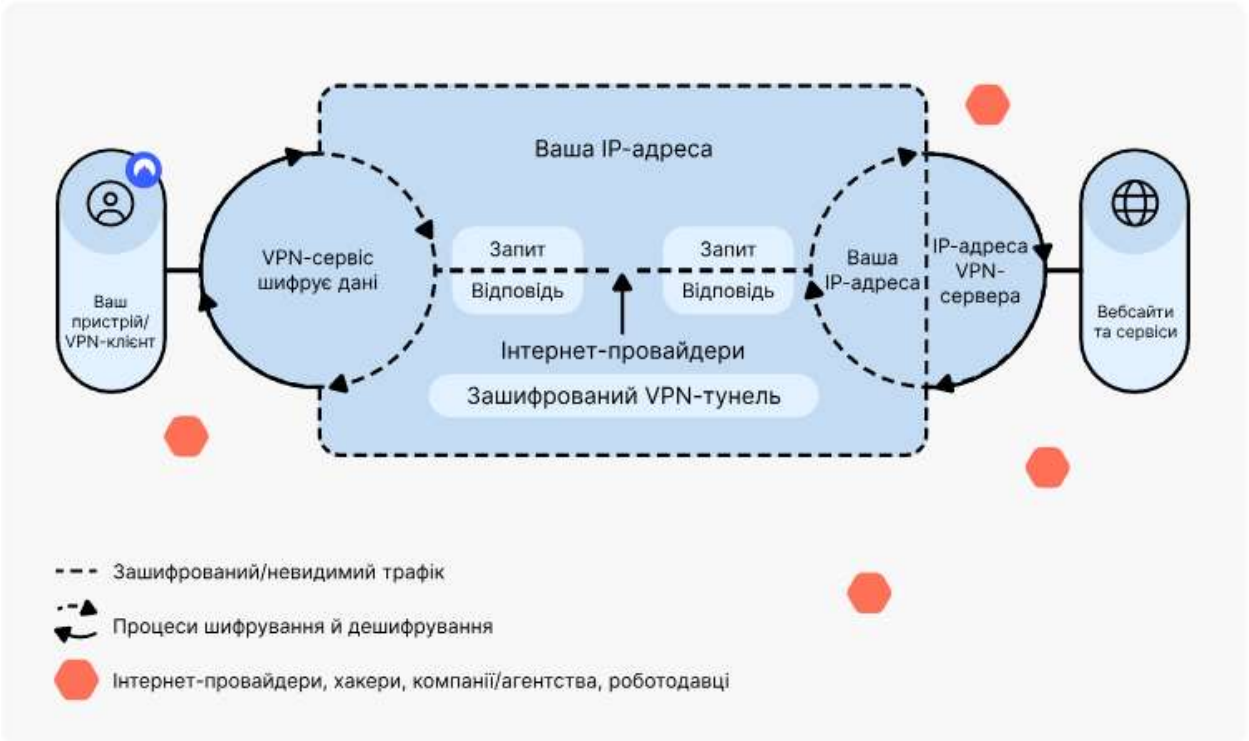

Рис. 1.1.1 – Схема роботи VPN [1]

У сучасних корпоративних мережах використання VPN (віртуальної приватної мережі) є критично важливим для забезпечення безпеки та конфіденційності передачі даних. Основні функції VPN включають шифрування даних, аутентифікацію користувачів, забезпечення цілісності даних та конфіденційність. Розглянемо детальніше кожну з цих функцій у контексті корпоративних мереж.

Шифрування даних є ключовою функцією VPN, що забезпечує захист інформації під час її передачі через Інтернет. У корпоративних мережах це особливо важливо, оскільки компанії часто обробляють конфіденційну

інформацію, таку як фінансові дані, комерційна таємниця та персональні дані. Використання сильних алгоритмів шифрування, таких як AES (Advanced Encryption Standard), гарантує, що навіть у випадку перехоплення даних зловмисниками, вони не зможуть розшифрувати інформацію. Шифрування дозволяє співробітникам безпечно підключатися до корпоративної мережі з будь-якої точки світу, використовуючи публічні мережі Wi-Fi без ризику витоку даних.

Аутентифікація користувачів є важливою для запобігання несанкціонованому доступу до корпоративної мережі. В корпоративному середовищі це допомагає забезпечити, що лише авторизовані співробітники можуть отримати доступ до внутрішніх ресурсів компанії. Використання багатофакторної аутентифікації (MFA), яка поєднує паролі, біометричні дані та одноразові коди, значно підвищує рівень безпеки. Адміністратори мережі можуть централізовано керувати правами доступу користувачів, забезпечуючи гнучкість і контроль над тим, хто має доступ та до яких ресурсів.

Цілісність даних гарантує, що дані залишаються незмінними під час передачі, запобігаючи їх модифікації зловмисниками. У корпоративних мережах це особливо важливо для підтримання точності та достовірності переданої інформації. Використання криптографічних хеш-функцій для перевірки цілісності даних. Використання криптографічних хеш-функцій дозволяє перевіряти цілісність даних, наприклад алгоритмів SHA-256 для створення унікальних контрольних сум з метою перевірки автентичності даних під час їх передачі каналами зв'язку; цифрових підписів для підтвердження справжності документів і повідомлень, що надсилаються через корпоративну мережу.

Конфіденційність забезпечує приватність даних та їх доступність лише авторизованим користувачам. У корпоративному контексті це допомагає захистити комерційну таємницю, службову інформацію та персональні дані, що можуть зберігатись та оброблятись в інформаційних системах організацій. VPN приховує реальні IP-адреси користувачів, що ускладнює відстеження їхньої діяльності в Інтернеті з боку конкурентів чи зловмисників. Використання VPN дозволяє розділяти корпоративну мережу на сегменти з різними рівнями доступу,

забезпечуючи конфіденційність чутливих даних та обмежуючи доступ до них тільки тим співробітникам, яким це потрібно для виконання їхніх службових обов'язків.

Окрім основних функцій, VPN в корпоративних мережах має кілька додаткових переваг:

- VPN-системи можуть надавати докладні звіти про використання мережі, дозволяючи адміністраторам відстежувати підключення та активність користувачів.
- Сучасні VPN-рішення оптимізовані для забезпечення високої швидкості передачі даних без втрати безпеки, що є важливим для ефективної роботи будь-якої організації.

У корпоративних мережах використовуються різні типи VPN, кожен з яких має свої особливості і застосування. Розуміння різниці між цими типами і знання їх особливостей допоможе ефективно використовувати VPN для різних потреб компанії. Розглянемо чотири основні типи VPN, які використовуються в корпоративних мережах:

VPN типу **Віддалений доступ (Remote Access VPN)** являє собою технологію, яка дозволяє користувачам з віддалених локацій безпечно підключатися до корпоративної мережі через Інтернет. Це досягається шляхом створення захищеного тунелю між користувачем і корпоративною мережею, що забезпечує конфіденційність та цілісність переданих даних. Основною метою використання Remote Access VPN в корпоративних мережах є надання працівникам можливості працювати з корпоративними ресурсами з будь-якої точки світу, забезпечуючи при цьому високий рівень безпеки. Це особливо важливо в умовах зростаючої тенденції до дистанційної роботи та необхідності доступу до корпоративної інформації в будь-який час.

Процес використання Remote Access VPN включає декілька ключових етапів. Спочатку користувач проходить процедуру аутентифікації, яка може включати використання паролів, сертифікатів або двофакторної аутентифікації. Після успішної аутентифікації створюється захищений тунель між пристроєм

користувача та корпоративною мережею, який шифрує всі передані дані. Далі користувач отримує доступ до внутрішніх ресурсів компанії, таких як файлові сервери, бази даних, внутрішні веб-додатки та інші сервіси, що дозволяє їм ефективно виконувати свої обов'язки незалежно від їх фізичної локації.

Remote Access VPN надає ряд суттєвих переваг для корпоративних мереж. Перш за все, він забезпечує високий рівень безпеки, оскільки всі дані, що передаються через VPN, шифруються, що захищає їх від перехоплення та несанкціонованого доступу. По-друге, Remote Access VPN пропонує гнучкість та мобільність, дозволяючи працівникам виконувати свої обов'язки з будь-якого місця, маючи доступ до необхідних ресурсів без фізичної присутності в офісі. Третя перевага полягає у зниженні витрат, оскільки відсутність необхідності у фізичній інфраструктурі для віддалених офісів знижує витрати на оренду та обслуговування. Крім того, можливість працювати віддалено сприяє підвищенню продуктивності працівників, дозволяючи їм виконувати завдання в зручний для них час. Таким чином, Remote Access VPN стає важливим інструментом для сучасних компаній, що прагнуть забезпечити безпечний та ефективний доступ до своїх ресурсів у будь-яких умовах [2].

Site-to-Site VPN – це тип віртуальної приватної мережі, яка дозволяє об'єднати декілька локальних мереж (сайтів) у єдину захищену мережу через Інтернет. На відміну від Remote Access VPN, де користувачі підключаються до корпоративної мережі з віддалених місць, Site-to-Site VPN забезпечує постійний зв'язок між різними офісами або підрозділами компанії.

Основне призначення Site-to-Site VPN полягає у забезпеченні безпечного та стабільного зв'язку між географічно розподіленими офісами або відділеннями організації. Це дозволяє:

- Забезпечити централізований доступ до корпоративних ресурсів.
- Підвищити рівень безпеки даних, переданих між офісами.
- Знизити витрати на оренду виділених ліній зв'язку.
- Забезпечити ефективну взаємодію між співробітниками, що знаходяться в різних місцях.

Site-to-Site VPN створюється шляхом налаштування спеціального мережевого обладнання, такого як маршрутизатори або міжмережеві екрани, на кожному кінці з'єднання. Ці пристрої встановлюють захищений тунель через Інтернет, шифруючи весь трафік, що проходить через нього.

Використання Site-to-Site VPN у корпоративних мережах надає ряд важливих переваг. По-перше, цей тип VPN забезпечує високий рівень безпеки, оскільки весь трафік, що передається між офісами, шифрується. Це значно знижує ризик несанкціонованого доступу до конфіденційної інформації. По-друге, Site-to-Site VPN підвищує ефективність роботи IT-відділу, дозволяючи централізовано керувати мережею та спрощуючи адміністрування і моніторинг мережевої інфраструктури. Завдяки постійному з'єднанню між офісами забезпечується стабільний доступ до корпоративних ресурсів, що позитивно впливає на продуктивність співробітників. Крім того, використання Site-to-Site VPN є економічно вигідним рішенням, оскільки знижуються витрати на створення та обслуговування виділених ліній зв'язку. Також важливою перевагою є гнучкість цієї технології, яка дозволяє легко масштабувати мережу при розширенні компанії. Site-to-Site VPN може бути інтегрований з іншими технологіями безпеки, такими як брандмауери та системи виявлення вторгнень, що забезпечує додатковий рівень захисту. Підтримка різних мережевих пристроїв і операційних систем робить цей тип VPN універсальним рішенням для багатьох організацій [2].

Intranet VPN, або внутрішній VPN, призначений для захисту передачі даних між різними офісами або філіями однієї компанії. Відмінною особливістю Intranet VPN є те, що він використовується виключно для внутрішніх потреб організації, на відміну від Extranet VPN, який забезпечує безпечний доступ зовнішніх користувачів до внутрішніх ресурсів компанії.

Intranet VPN використовує шифрування та інші механізми безпеки для забезпечення конфіденційності та цілісності даних, що передаються між офісами через Інтернет або інші публічні мережі. Це дозволяє організаціям створювати єдину корпоративну мережу, де всі ресурси доступні незалежно від географічного розташування.

Intranet VPN використовується для забезпечення безпечного з'єднання між різними офісами компанії. Основні цілі використання Intranet VPN включають:

- Забезпечення безпечної передачі конфіденційних даних між офісами.
- Створення єдиної корпоративної мережі для зручного доступу до ресурсів незалежно від місця розташування.
- Централізоване управління IT-інфраструктурою та ресурсами компанії.
- Забезпечення безперервного доступу до корпоративних систем і додатків для всіх співробітників.

Intranet VPN пропонує численні переваги для корпоративних мереж. Однією з основних переваг є підвищена безпека, яку забезпечують захищені з'єднання з використанням шифрування та аутентифікації. Це значно знижує ризик перехоплення або втрати конфіденційної інформації. Використання Інтернету як транспортної мережі дозволяє значно знизити витрати на оренду виділених ліній, що робить Intranet VPN економічно вигідним рішенням. Гнучкість і масштабованість цієї технології дає можливість легко додавати нові офіси або користувачів до мережі, що є важливим для зростаючих компаній. Крім того, централізоване управління IT-інфраструктурою спрощує адміністрування та підтримку, що сприяє підвищенню ефективності роботи [2].

Extranet VPN є важливим інструментом для корпоративних мереж, який забезпечує захищене з'єднання між внутрішніми мережами компаній та зовнішніми партнерами, клієнтами чи постачальниками.

Extranet VPN використовується для ряду цілей, включаючи:

- Забезпечує захищений доступ до внутрішніх ресурсів компанії для зовнішніх партнерів.
- Дозволяє клієнтам безпечно підключатися до специфічних ресурсів, таких як портали підтримки або системи відстеження замовлень.
- Постачальники можуть отримати доступ до інформації про замовлення або інші корпоративні дані, необхідні для ефективної співпраці.

Extranet VPN надає компаніям значні переваги, включаючи підвищену безпеку, зменшення витрат і високу гнучкість та масштабованість. Завдяки захищеним з'єднанням і шифруванню даних, ризик несанкціонованого доступу значно знижується, що є критично важливим для захисту конфіденційної інформації. Використання Extranet VPN також дозволяє уникнути витрат на фізичну інфраструктуру, що зазвичай необхідна для традиційних мережевих рішень, що, в свою чергу, сприяє зниженню загальних витрат на управління та підтримку мережі. Крім того, Extranet VPN забезпечує високу гнучкість і масштабованість, дозволяючи легко додавати нових користувачів або розширювати мережу відповідно до потреб компанії. Це робить Extranet VPN ідеальним рішенням для динамічно змінюваних бізнес-середовищ, де важливо швидко адаптуватися до нових вимог та викликів [2].

Типи з’єднання. Корпоративні мережі використовують VPN-з'єднання для забезпечення безпечного доступу до внутрішніх ресурсів компанії з будь-якої точки світу. Основні типи VPN-з'єднань, які застосовуються в корпоративних мережах, включають PPTP, L2TP/IPsec, OpenVPN, SSTP та IKEv2/IPsec.

1. PPTP є одним з найстаріших і найпростіших у налаштуванні протоколів VPN. У корпоративних мережах він використовується рідше через низький рівень безпеки, але все ще може бути корисним для менш критичних задач. Використання PPTP підходить для підключення до менш критичних ресурсів та може застосовуватися для швидкого налаштування тимчасових з'єднань. Простота налаштування дозволяє швидко встановлювати з'єднання на різних пристроях, що робить його зручним у певних ситуаціях.
2. L2TP/IPsec поєднує в собі переваги L2TP та IPsec, що забезпечує високий рівень безпеки і конфіденційності. Цей протокол широко використовується в корпоративних мережах для захисту чутливих даних. Він забезпечує захист конфіденційних корпоративних даних та віддалений доступ до внутрішніх ресурсів компанії. IPsec забезпечує шифрування і аутентифікацію, гарантує цілісність даних, що робить цей протокол надійним вибором для

корпоративних середовищ. L2TP/IPsec часто використовується для створення тунелів між філіями компанії та головним офісом.

3. OpenVPN є відкритим і дуже гнучким протоколом, який забезпечує високий рівень безпеки. Він часто використовується в корпоративних мережах завдяки своїй надійності та можливості налаштування під конкретні потреби компанії. OpenVPN забезпечує безпечний віддалений доступ співробітників до корпоративних ресурсів та з'єднання між різними офісами компанії. Використовуючи SSL/TLS для шифрування, цей протокол дозволяє уникати блокувань з боку мережевих файрволів. Крім того, OpenVPN підтримує різні алгоритми шифрування та аутентифікації, що робить його дуже гнучким у використанні.
4. SSTP використовує SSL/TLS для забезпечення захисту даних і переважно підтримується Windows. Це робить його зручним для компаній, які використовують Windows у своїй інфраструктурі. SSTP забезпечує високий рівень безпеки та сумісність з різними типами мережевих середовищ, що дозволяє використовувати його для забезпечення безпечного доступу до внутрішніх мережевих ресурсів. Інтеграція з Windows спрощує налаштування та управління цим протоколом. Використання стандартного HTTPS порту дозволяє SSTP обходити блокування, що робить його корисним в умовах жорстких мережевих обмежень.
5. IKEv2/IPsec забезпечує швидке і стабільне з'єднання, що робить його популярним вибором для мобільних пристроїв та корпоративних мереж, де важливі швидкість і надійність. Цей протокол широко використовується для захисту мобільних пристроїв, таких як смартфони і планшети, та підключення до корпоративної мережі з мобільних пристроїв. IKEv2/IPsec забезпечує швидке відновлення з'єднання після втрати сигналу, що є важливою перевагою для мобільних користувачів. Використання IPsec забезпечує високий рівень безпеки і шифрування даних, що робить цей протокол надійним і безпечним рішенням для корпоративних мереж [3].

Таким чином, вибір VPN-протоколу для корпоративної мережі залежить від конкретних вимог компанії щодо безпеки, швидкості, сумісності та легкості налаштування. Найпопулярнішими в корпоративних середовищах є L2TP/IPsec, OpenVPN та IKEv2/IPsec завдяки їх високому рівню безпеки і надійності [2].

OpenVPN є популярним інструментом для створення віртуальних приватних мереж (VPN), який забезпечує високий рівень безпеки та гнучкість у налаштуваннях. Використання OpenVPN в корпоративних мережах має ряд переваг, які роблять його ідеальним вибором для багатьох підприємств. Однією з головних особливостей OpenVPN є його відкритий вихідний код, що дозволяє розробникам та системним адміністраторам модифікувати його відповідно до специфічних потреб організації. Відкритий код також сприяє прозорості та безпеці, оскільки будь-які уразливості можуть бути виявлені та усунені спільнотою розробників.

Однією з найважливіших переваг OpenVPN є високий рівень безпеки. Використання протоколів SSL/TLS для захисту даних гарантує, що всі передані через VPN дані залишаються конфіденційними та недоступними для сторонніх осіб. Крім того, OpenVPN підтримує широкий спектр криптографічних алгоритмів, що дозволяє вибрати оптимальний баланс між безпекою та продуктивністю. Це особливо важливо для корпоративних мереж, де захист чутливої інформації є пріоритетом.

Гнучкість налаштувань є ще однією ключовою перевагою OpenVPN. Він підтримує роботу через різні порти та протоколи, що дозволяє обходити мережеві фільтри та брандмауери. Це робить OpenVPN універсальним рішенням для забезпечення віддаленого доступу до корпоративної мережі з будь-якої точки світу. Крім того, OpenVPN може працювати як у режимі клієнт-сервер, так і в режимі site-to-site, що дозволяє підключати віддалені офіси та філії до центральної мережі компанії.

Економічна ефективність є ще одним важливим аспектом, який робить OpenVPN привабливим для бізнесу. Використання відкритого програмного забезпечення дозволяє уникнути значних витрат на ліцензії та обслуговування.

Крім того, завдяки широкій спільноті користувачів та розробників, можна легко знайти підтримку та ресурси для вирішення будь-яких технічних питань.

OpenVPN також відзначається високою стабільністю та надійністю. Він підтримує різні операційні системи, включаючи Windows, macOS, Linux, iOS та Android, що забезпечує широкі можливості для інтеграції в існуючу IT-інфраструктуру компанії. Постійні оновлення та вдосконалення програмного забезпечення гарантують, що OpenVPN залишається актуальним та відповідає сучасним вимогам безпеки.

1.2 Принципи роботи та архітектура VPN на базі OpenVPN

Протокол OpenVPN складається з кількох основних компонентів, які разом забезпечують надійну віртуальну приватну мережу. Розуміння цих компонентів має важливе значення для правильного налаштування та керування розгортанням OpenVPN.

Компоненти OpenVPN:

- Центр сертифікації ЦС. Сертифікати видаються за запитом вузлів мережі VPN, підписаний сертифікатом ЦС. Надайте вузлу VPN власний сертифікат для перевірки ЦС. Керуйте списком аудиту сертифікатів CRL.
- Сервер OpenVPN. Серверне програмне забезпечення OpenVPN створює тунелі в незахищеній мережі, наприклад Інтернеті. Цей тунель забезпечує безпечний зашифрований трафік між вузлами, що беруть участь у мережі OpenVPN.
- Клієнт OpenVPN. Клієнтське програмне забезпечення OpenVPN встановлюється на всіх вузлах, яким необхідно встановити безпечні канали передачі даних із сервером OpenVPN. При правильній конфігурації сервера OpenVPN дані можна безпечно передавати між клієнтами OpenVPN, а не лише між клієнтом і сервером OpenVPN.
- Сертифікат X.509 (відкритий ключ). Сертифікат X.509 — це відкритий ключ, сертифікований ЦС. Вони використовуються для шифрування даних. Сертифікат сертифікований центром сертифікації ЦС і може ідентифікувати сторону, яка передає зашифровані дані.
- Приватний ключ. Приватний ключ є секретним. Вони повинні створюватися та зберігатися на кожному вузлі мережі OpenVPN, використовуватися для розшифровки даних і ніколи не повинні передаватись через мережу.
- Список відкликаних сертифікатів CRL. Містить список сертифікатів, які втратили довіру. Він створюється та редагується на вузлі ЦС. Щоб від’єднати вузол від мережі, просто введіть його сертифікат у список CRL.

Приклад OpenVPN рішення представлений на рис. 1.2.1

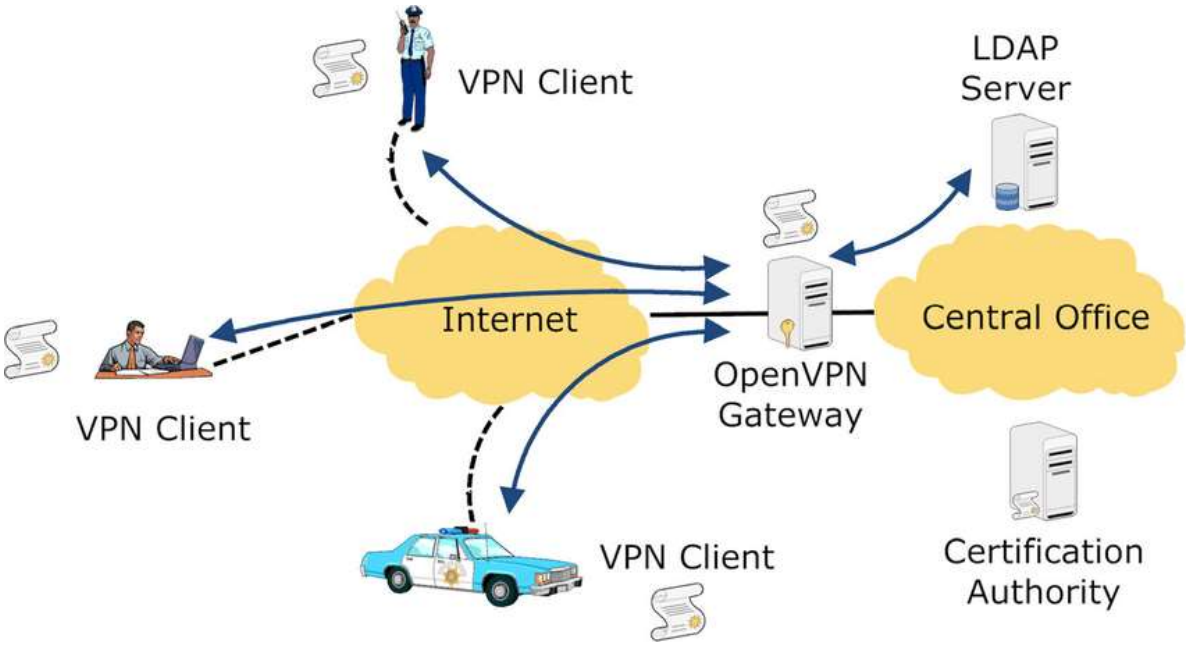

Рис. 1.2.1 – Приклад мережі OpenVPN

Принципи роботи складових OpenVPN:

Сервер OpenVPN є основним елементом налаштування VPN, відповідальним за автентифікацію OpenVPN клієнтів, встановлення зашифрованих тунелів і керування безпечною передачею даних між OpenVPN клієнтами та безпечною мережею. Сервер забезпечує безпечний зв'язок і захищає від несанкціонованого доступу.

Сервер OpenVPN працює як демон (англ. daemon), постійно працює у фоновому режимі. Він прослуховує вхідні запити на підключення від клієнтів, шифрує та розшифровує дані та гарантує, що всі дані, що передаються через VPN, є безпечними. Файли конфігурації сервера містять параметри, які визначають поведінку сервера. Це включає параметри мережі, параметри безпеки та інструкції щодо керування з’єднаннями OpenVPN клієнтів. Важливі параметри включають IP-адресу та порт, який прослуховує сервер, використовуваний протокол (TCP або UDP) і використовуваний метод шифрування.

OpenVPN покладається на шифрування SSL/TLS для безпеки. Серверу потрібен набір криптографічних сертифікатів і ключів для автентифікації OpenVPN клієнтів і встановлення безпечного з’єднання. Зазвичай вони включають сертифікати сервера, закриті ключі та сертифікати центру сертифікації (ЦС).

Сервер інтегрується з мережевим стеком системи для керування інтерфейсами VPN і маршрутизації трафіку. Це включає створення віртуальних мережевих інтерфейсів (наприклад, налаштування або вимкнення пристроїв) і налаштування IP-переадресації та маршрутизації для забезпечення безпечного потоку трафіку між OpenVPN клієнтами та захищеною мережею.

Клієнт OpenVPN відповідає за ініціювання підключення до сервера OpenVPN, встановлення захищеного тунелю зв'язку та забезпечення шифрування даних, які надсилаються на клієнтський пристрій і з нього. OpenVPN клієнт забезпечує безпечний віддалений доступ до мережевих ресурсів сервера.

Кросплатформений OpenVPN клієнт надає інтерфейс користувача та основні функції для підключення до серверів OpenVPN. Він ініціює процес підключення, виконує автентифікацію та керує VPN-тунелем.

Подібно до сервера, файл конфігурації OpenVPN клієнта містить параметри, необхідні для підключення до сервера. Цей файл містить адресу, порт і параметри шифрування сервера, а також шляхи до сертифікатів і ключів, необхідних для автентифікації.

Для встановлення безпечного з'єднання OpenVPN клієнту потрібен власний набір сертифікатів і ключів, включаючи сертифікат клієнта, закритий ключ і сертифікат ЦС. Ці облікові дані підтверджують автентичність OpenVPN клієнта на сервері та забезпечують зашифрований зв'язок.

OpenVPN клієнт також взаємодіє з мережевим стеком системи для створення віртуальних мережевих інтерфейсів і керування маршрутизацією. Це гарантує, що всі дані, які надсилаються до VPN, шифруються та надсилаються через безпечний тунель.

Клієнтські програми зазвичай включають інтерфейс користувача, який дозволяє користувачам керувати підключеннями, налаштовувати параметри та переглядати стан підключення. Інтерфейс дозволяє користувачам легко підключатися до VPN і контролювати свої підключення.

Автентифікація є дуже важливою частиною OpenVPN, і для автентифікації користувачів використовуються різні методи автентифікації, які забезпечують

високий рівень безпеки, який забезпечує OpenVPN. Таким чином, він гарантує, що лише ті, хто має повноваження, можуть підключитися до VPN. Сертифікати, ключі, логіни та паролі є основними методами автентифікації, які використовуються в OpenVPN.

Центр сертифікації (ЦС). ЦС є довіреним центром, який підписує сертифікати сервера та OpenVPN клієнта; він відповідає за видачу дійсних сертифікатів.

Щоб гарантувати безпеку системи OpenVPN, центр сертифікації (ЦС) займає ключову позицію. ЦС — це організація, якій доручено видавати, керувати та відкликати цифрові сертифікати, які відіграють роль у автентифікації та шифруванні інформації в мережі. У наступних розділах ми глибше розглянемо ролі, які виконує ЦС, особливо зосередившись на їх актуальності в сферах OpenVPN.

Основними обов'язками центру сертифікації (ЦС) є видача сертифікатів. Цифрові сертифікати як для серверів, так і для OpenVPN клієнтів надаються ЦС, забезпечуючи особу власника та полегшуючи автентифікацію між об'єктами мережі. Щоб підтвердити автентичність і дійсність сертифіката, ЦС підписує його своїм закритим ключем після перевірки особи запитувача сертифіката.

Функції та важливість сертифікаційних центрів в інфраструктурі OpenVPN:

- *Автентифікація сертифікатів*

  Підпис ЦС на сертифікаті засвідчує його надійність для інших користувачів мережі, що змушує їх довіряти будь-яким сертифікатам, підписаним цим ЦС. Відкритий ключ власника підписується у сертифікаті, що може слугувати основою для шифрування та автентифікації.

- *Керування сертифікатами*

  ЦС відповідає за зберігання та підтримку виданих ним сертифікатів, включаючи відстеження термінів їхньої дії та актуальності.

- *Анулювання сертифікатів*

  У разі зламу або компрометації закритого ключа, або якщо власник сертифіката поводиться недобросовісно, ЦС може відкликати сертифікат.

Списки відкликаних сертифікатів (CRL) публікуються ЦС для перевірки статусу сертифікатів іншими учасниками мережі.

- *Довіра та безпека*

Центр сертифікації є джерелом довіри в інфраструктурі OpenVPN, де всі учасники мережі покладаються на нього для перевірки автентичності сертифікатів. Використання сертифікатів, підписаних ЦС, забезпечує надійну безпеку, дозволяючи створювати з'єднання лише довіреним учасникам.

- *Захист від зловмисників.*

Вимога автентифікації на основі сертифікатів у OpenVPN ефективно запобігає несанкціонованому доступу до мережі. Тільки законні клієнти OpenVPN з дійсними сертифікатами можуть підключатися, що підвищує загальний рівень безпеки.

- *Екранування даних.*

Канали передачі даних VPN захищені сертифікатами, створеними центром сертифікації, що забезпечує цілісність і конфіденційність переданої інформації. Навіть у разі перехоплення, дані залишаються зашифрованими та недоступними для зловмисників.

Сертифікати X.509 є найпоширенішим методом автентифікації в OpenVPN. Вони забезпечують двосторонню автентифікацію, що означає, що сервер і клієнт OpenVPN повинні бути автентифіковані один одним.

Сертифікат сервера: сертифікат, який використовує сервер, щоб підтвердити свою ідентичність OpenVPN клієнту, підписаний закритим ключем ЦС.

Сертифікат клієнта. Кожен OpenVPN клієнт також має власний сертифікат, підписаний ЦС. Це засвідчує особу OpenVPN клієнта на сервері.

Сертифікаційний центр (ЦС): ЦС є довіреним органом, який підписує сертифікати як сервера, так і клієнтів OpenVPN. ЦС видає сертифікати, гарантуючи, що вони дійсні.

Приватні ключі: як сервер, так і клієнт OpenVPN мають приватні ключі, які використовуються разом з відповідними сертифікатами для шифрування та підпису даних.

Сильні сторони: Безпека на піку: шифрування SSL/TLS гарантує першокласний захист завдяки використанню сертифікатів. Взаємна автентифікація між сервером і клієнтом можлива за допомогою сертифікатів. Сертифікати ускладнюють підробку, що підвищує рівень захисту.

Слабкі сторони: Плутаність у складності: тонкощі керування сертифікатами можуть перетворитися на заплутаний процес, особливо у великих організаціях. Виникає необхідність у надійному ЦС, який би підписував сертифікати.

Ключі. OpenVPN може використовувати спільні секретні ключі (pre-shared keys) для аутентифікації та шифрування даних. Цей метод менш поширений, але може бути корисним у простих або тимчасових налаштуваннях.

Спільний секретний ключ – ключ, яким обмінюються заздалегідь між сервером та клієнтом OpenVPN, він використовується для шифрування та дешифрування даних.

Переваги: з точки зору простоти, спільні секретні ключи легко впровадити та керувати ними без необхідності центру сертифікації. Крім того, такі ключі пропонують швидкість, оскільки встановлення з’єднання відбувається швидше через відсутність необхідності взаємної автентифікації за допомогою сертифікатів.

Однак є і недоліки: якщо приватний ключ буде зламано, усі з’єднання, які використовують цей ключ, стануть уразливими. Крім того, таким ключам бракує масштабованості, що робить їх непридатним для великих організацій з великою кількістю користувачів.

Автентифікації користувачів через OpenVPN за допомогою логінів і паролів:

- Вхід користувача: складається з унікального імені користувача, введеного для автентифікації на сервері.
- Пароль: секретний код, який використовується разом із логіном для підтвердження особи користувача.

Метод має певні переваги, він простий у використанні, оскільки користувачі вже знайомі з ним і можуть легко отримати доступ. Автентифікація за допомогою

логінів і паролів може використовуватися в поєднанні з іншими методами автентифікації для підвищення безпеки.

Недоліки: логіни та паролі можуть бути скомпрометовані через фішинг або брутфорс-атаки. Вимагає належного управління паролями та політик безпеки.

Двофакторна автентифікація (2FA)

Двофакторна автентифікація (2FA) додає додатковий рівень безпеки, поєднуючи те, що користувач знає (наприклад, пароль), з тим, що він має (наприклад, мобільний пристрій для отримання коду).

Компоненти двофакторної аутентифікації:

Основний фактор: дані для входу користувача.

Додатковий фактор: тимчасовий одноразовий пароль, згенерований на окремому пристрої або отриманий через SMS.

Переваги: навіть якщо один фактор скомпрометований, неавторизований доступ стає майже неможливим завдяки дворівневій безпеці. Підтримується багатьма сучасними додатками та системами безпеки.

Недоліки: складність налаштування вимагає впровадження додаткового обладнання або програмного забезпечення, яке може надати користувачам одноразові паролі, що є суттєвим обмеженням. Взаємодія з користувачем пов’язана з ускладненням процесу входу для користувачів.

Протоколи шифрування в OpenVPN

OpenVPN реалізує низку протоколів шифрування, щоб переконатися, що дані, які надсилаються через VPN, є конфіденційними, цілісними та автентичними. AES, RSA та HMAC є одними з основних протоколів шифрування, які використовуються в OpenVPN.

AES — це симетричний блоковий шифр — який передбачає захист даних шляхом шифрування та дешифрування за допомогою одного ключа. Уряд США прийняв цей стандарт шифрування, отже, отримав всесвітнє визнання.

Ключ: AES приймає ключі довжиною 128, 192 або 256 біт. Більша кількість бітів у ключі означає підвищений рівень безпеки.

Блоки: розширений стандарт шифрування, або AES, працює, обробляючи 128-бітні блоки даних.

Режими шифрування: AES має різні режими, такі як CBC (Cipher Block Chaining) і GCM (Galois/Counter Mode) з унікальними аспектами безпеки та продуктивності.

RSA (Рівест–Шамір–Адлеман)

RSA виступає як асиметричний криптографічний алгоритм, який використовує два ключі для різних цілей. Один ключ є відкритим і призначений для шифрування, а інший є закритим і використовується для дешифрування; він знаходить широке застосування, коли є потреба як у захисті даних, так і в автентифікації.

Відкритий ключ: його основне призначення полягає в тому, щоб переконатися, що дані, які пересилаються між відправником і одержувачем, жодним чином не змінюються під час передачі. Це досягається шляхом шифрування даних на стороні відправника та створення цифрових підписів, які можна розшифрувати лише за допомогою відповідного закритого ключа.

Приватний ключ: використовується разом із відкритим ключем як частина асиметричної схеми шифрування, де для шифрування та дешифрування використовуються різні ключі.

Модулі та експоненти: це важливі компоненти ключів RSA. Показник степеня, як правило, невеликий і вибирається через його простоту обчислення, тоді як модуль є дуже великим числом, що робить обчислювально неможливим визначення закритого ключа від відкритого.

HMAC (код автентифікації повідомлення на основі хешу)

HMAC — це криптографічна функція, яка використовується для забезпечення цілісності та автентичності даних. Він передбачає використання хеш-функції разом із секретним ключем.

Компоненти, які складають HMAC:

- Хеш-функція: можна використовувати будь-яку хеш-функцію, наприклад SHA-256, MD5 тощо.

- Секретний ключ: використовується в поєднанні з хеш-функцією для створення MAC.
- MAC: вихідні дані операції HMAC, яка вказує на те, що повідомлення не змінено та відправник авторизований.

Протоколи тунелювання в OpenVPN

OpenVPN підтримує два основні протоколи тунелювання: UDP (протокол дейтаграм користувача) і TCP (протокол керування передачею). Вони мають свої особливості, плюси і мінуси, які роблять їх придатними для різних ситуацій. Ось детальний опис обох протоколів:

UDP (протокол дейтаграм користувача) — це метод передачі даних без підключення. Він працює як протокол транспортного рівня, який не створює жодного фіксованого з’єднання між відправником і одержувачем даних; отже, він швидкий і забезпечує низьку затримку. З іншого боку, це не гарантує доставку пакетів і не гарантує, що вони будуть узгодженими або непошкодженими. UDP не потребує з’єднання, що означає, що не вимагає встановлення з’єднання перед передачею даних, що призводить до зниження витрат на обробку даних. Крім того, швидкість є перевагою UDP, оскільки вона не забезпечує доставку пакетів, як TCP, отже, швидше, ніж TCP. Завдяки низькій затримці та відсутності перевірки помилок, що призводить до відсутності контролю над доставкою чи замовленням (хоча створює такі ризики, як втрата чи дублювання даних), UDP підходить для програм, чутливих до затримки.

Переваги включають високу швидкість передачі даних завдяки зниженню часу на їх обробку та простоту завдяки необхідним мінімальним вимогам. Основним недоліком є відсутність гарантій щодо доставлених пакетів: дані можуть бути втрачені або зіпсовані після надходження.

TCP (протокол керування передачею)

TCP є протоколом з'єднання транспортного рівня, який забезпечує надійну передачу даних між відправником та отримувачем. Він гарантує доставку всіх пакетів у правильному порядку та забезпечує контроль помилок. TCP встановлює з'єднання між відправником та одержувачем перед передачею даних, що додає

додаткові витрати часи. TCP забезпечує контроль помилок, перевіряючи цільність кожного пакета. У разі втрати пакета TCP автоматично повторно передає його.

Переваги: гарантована доставка даних у правильному порядку. Забезпечує цільність та правильність даних. Стабільність є ключовою характеристикою цієї технології, що робить її ідеальною для додатків, які вимагають надійної передачі, наприклад, при перегляді веб-сторінок, спілкуванні електронною поштою, передачі файлів тощо.

Недоліки:

1) перевірка помилок та встановлення з'єднання можуть призводити до значних затримок передачі даних.
2) реалізація TCP складніша порівняно з UDP.

Вибір протоколу для OpenVPN

Вибір між UDP і TCP залежить від конкретних вимог та умов використання.

UDP є відповідним у випадку, коли перевагу надають швидкості і мінімальній підтримці, навіть якщо це може призвести до втрати деяких даних. Це ідеальний вибір для задач, що працюють в режимі реального часу, таких як голосові дзвінки, відеоконференції та онлайн-геймінг.

TCP протокол підходить для завдань, які вимагають бездоганної передачі даних, таких як перегляд веб-сторінок, завантаження файлів та використання електронної пошти.

Забезпечення конфіденційності та цілісності даних OpenVPN

OpenVPN використовує кілька методів для захисту конфіденційності та цілісності даних, якими обмінюються через VPN, причому шифрування є основним методом.

OpenVPN застосовує потужні алгоритми шифрування, такі як AES (Advanced Encryption Standard), для захисту даних під час передачі. Це гарантує, що навіть якщо зловмисник перехопить трафік, він не зможе прочитати або змінити дані. Відповідно до вимог, щодо безпеки, шифрування можна налаштувати з використанням ключів довжиною 128, 192 або 256 біт.

Аутентифікація

OpenVPN використовує сертифікати X.509 для аутентифікації серверів і клієнтів. Такий підхід забезпечує перевірку ідентичності обох сторін перед встановленням з'єднання. З метою забезпечення додаткового рівня безпеки використовується асиметричне шифрування RSA для захисту сеансових ключів.

Цілісність даних

OpenVPN використовує HMAC (код аутентифікації повідомлення на основі хешу) для забезпечення цільності даних, який гарантує, що дані не були змінені під час передачі. HMAC генерується за допомогою хеш-функцій, таких як SHA-256, які мають високий рівень захисту.

1.3 Аналіз загроз та викликів безпеки при використанні VPN

У сучасну епоху цифрових технологій важливо мати можливість захистити інформацію. Серед найбільш популярних технологій для створення VPN є OpenVPN, яка забезпечує безпечну передачу даних у незахищеній мережі. Однак навіть під час використання OpenVPN існують серйозні загрози для її використання, які зрештою можуть мати катастрофічні наслідки для організації та її користувачів.

Загрози компрометації облікових даних:

1) Фішинг і соціальна інженерія.

   Одним із найпоширеніших методів викрадення облікових даних користувача є фішинг. У більшості випадків створюється підроблена веб-сторінка або надсилається електронний лист, який виглядає як справжнє повідомлення, з метою отримання пароля користувача та інших важливих даних. Наприклад, користувачу може бути надіслано спеціально створений електронний лист, що виглядає як повідомлення від IT-відділу, з проханням оновити свій пароль за наданим посиланням. Після введення облікових даних на підробленому сайті зловмисники отримують доступ до VPN.

2) Використання слабких паролів або повторне використання одного пароля.

   Ненадійні паролі або повторне використання одного пароля для різних облікових записів значно підвищують ризик компрометації. Зловмисникам легко зламати слабкі паролі, використовуючи методи грубої сили або атаки за словником. Наприклад, паролі на кшталт «password123» або «admin2021» можна зламати за секунди.

3) Недостатній захист облікових даних під час зберігання та передачі.

   Зберігання облікових даних у відкритому та незашифрованому вигляді або їх передача через відкриті канали зв’язку може загрожувати безпеці. Зловмисники можуть перехопити або викрасти такі дані. Наприклад, зберігання конфігураційних файлів OpenVPN з відкритими паролями на неконтрольованих пристроях або передача паролів електронною поштою у відкритому вигляді.

4) Відсутність багатофакторної аутентифікації (MFA).

Використання лише пароля для аутентифікації користувача не забезпечує достатнього захисту. MFA значно підвищує рівень безпеки, оскільки вимагає додаткового підтвердження особистості користувача. Наприклад, поєднання одноразового пароля (OTP) або біометричних даних з основним паролем ускладнює злом.

5) Внутрішні загрози.

Співробітники організації можуть скомпрометувати облікові дані випадково або навмисно. Недостатня обізнаність щодо безпеки або зловмисний намір можуть призвести до серйозних витоків інформації. Наприклад, працівник, який залишив свій ноутбук підключеним до VPN у громадському місці, може втратити його разом із обліковими даними.

Методи захисту компрометації облікових даних:

1) Освіта та підвищення обізнаності користувачів

Навчання користувачів основам кібербезпеки та проведення семінарів допоможуть запобігти фішинговим атакам та небезпечним діям. Наприклад, регулярні тренінги з розпізнавання фішингових електронних листів підвищать рівень обізнаності користувачів.

2) Політика надійних паролів

Організація повинна запровадити політику, що вимагає використання складних паролів і їх зміни через певні проміжки часу. Наприклад, паролі повинні містити принаймні 12 символів, великі та малі літери, цифри та спеціальні символи.

3) Багатофакторна аутентифікація (MFA)

Використання MFA мінімізує можливість компрометації даних, навіть якщо пароль було вкрадено. Наприклад, генерація OTP за допомогою мобільних додатків або SMS значно підвищує безпеку.

4) Зберігання та захист під час передавання даних

Захист облікових даних під час зберігання та їх безпечна передача є критичними для безпеки. Наприклад, конфігурації OpenVPN повинні

зберігатися у зашифрованому вигляді, а паролі передаватися через безпечні канали.

5) Моніторинг і виявлення аномалій

Системи моніторингу, здатні виявляти аномальну поведінку чи іншу підозрілу активність, є ефективним захистом від компрометації облікових даних. Наприклад, використання систем виявлення вторгнень для моніторингу мережевої активності дозволяє виявляти несанкціоновану або підозрілу поведінку.

OpenVPN є одним з найпоширеніших методів створення VPN. Крім основних можливостей і переваг OpenVPN все ще може стати об’єктом кількох атак, серед них MITM-атаки.

Атака MITM – це будь-яка атака, за якою зловмисник може перехоплювати, слухати і навіть змінювати повідомлення між двома сторонами, які вірять ситуації у прямому зв’язку одна з одною. В результаті таємного аспекту ситуації зловмисник отримає доступ до конфіденційних даних, зможе вкрасти обліковий запис або сконструювати дані.

Типи атак MITM:

- ARP-протокол: фальсифікація ARP-запитів, щоб перехопити трафік, який проходить від клієнтів до OpenVPN.
- Підробка DNS-протоколів: це механізм фальсифікації DNS, для того щоб перенаправляти OpenVPN клієнтів на інші.
- Видалення SSL-протоколу: це проведення маркера веб-сайту до рівня HTTP і перехоплення незашифрованої інформації.
- Перехоплення сеансу: це викрадення активного клієнтського сеансу для доступу до їхніх облікових записів або сервісів [9].

Реалізація атаки MITM на OpenVPN:

1) Зловмиснику потрібно чітко визначити свою позицію в мережі так, щоб трафік був дійсно перехоплений. Це може бути досягнуто через компрометацію мережі або шахрайством ARP/DNS.

2) Зловмисник використовує фальшиві SSL-сертифікати для того, аби ввести в оману OpenVPN клієнта, щодо легітимності сервера.

Вразливості OpenVPN до MITM-атак:

Основні вразливості OpenVPN, які надають зловмиснику можливість виконання MITM-атак з використанням цього протоколу, описані нижче:

- Використовуються надто прості методи аутентифікації або сертифікати, які не є надійними.
- Відсутній ефективний спосіб перевірки дійсності отриманого сертифіката, що дозволяє використовувати підробки.
- Відсутність можливості захисту від підробки DNS-записів призводить до перенаправлення трафіку на шкідливі ресурси.

Методи захисту реалізації OpenVPN від MITM-атак:

Для забезпечення безпеки реалізації OpenVPN від MITM-атак, можна застосувати такі заходи:

- Використання двофакторної аутентифікації або надійних сертифікатів.
- Налаштування OpenVPN на примусову перевірку дійсності сертифікатів та перевірку їх відповідності довіреними центрами сертифікації.
- Використання DNSSEC або приватних DNS-серверів, щоб знизити ризики, пов'язані з підміною DNS-записів.
- Аналіз даних про трафік для виявлення всіх підозрілих транзакцій.

Вразливості протоколів шифрування OpenVPN

Вразливості в протоколах шифрування OpenVPN можуть призвести до серйозних проблем безпеки. Конфіденційна інформація може бути перехоплена та прочитана неавторизованими особами. Зловмисники можуть отримати контроль над активними сесіями, отримавши доступ до захищених ресурсів. Перехоплення та модифікація комунікацій можуть відбутися через використання недоліків шифрування, а порушення служби VPN можуть виникати через використання вразливості протоколу.

Вразливості SSL/TLS:

- Атака BEAST: Експлойт браузера проти SSL/TLS, що порушує конфіденційність даних, переданих через з’єднання SSL 3.0 і TLS 1.0.
- Атака POODLE: Експлойт, який використовує слабкі сторони SSL 3.0 у зв’язку з пониженими застарілими з’єднаннями, створеними з ним.
- Heartbleed: Слабкість бібліотеки OpenSSL, що дозволяє зловмисникам зчитувати пам’ять із систем, які містять конфіденційні дані.
- Атаки на пониження версії TLS: Змушують підключення використовувати старішу та менш безпечну версію TLS.

AES також має свої вразливості. Атаки побічного каналу отримують інформацію про роботу алгоритму шифрування на основі фізичної реалізації, наприклад, атаки за часом. Крім того, атаки зі слабким ключем використовують неправильно підібрані ключі для легшого зламу шифрування.

Алгоритм RSA не є винятком і має власні вразливості. Атаки факторизації можуть зламати шифр, розбираючи велике ціле число, що використовується в RSA. Часові атаки аналізують час, необхідний для криптографічних операцій, щоб отримати інформацію про закритий ключ.

Вразливості HMAC включають атаки розширення довжини, використовують спосіб, яким певні хеш-функції керують вхідними даними, щоб додати додаткову інформацію, зберігаючи при цьому цілісність повідомлення.

РОЗДІЛ 2 ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ OPENVPN У ЗАБЕЗПЕЧЕННІ ВІДДАЛЕНОГО ДОСТУПУ ДО КОРПОРАТИВНИХ ДАНИХ

2.1 Конфігурація та налаштування сервера OpenVPN

Для прикладу розгортання та налаштування серверу OpenVPN обрано операційну систему Linux, дистрибутив Ubuntu. Процес розгортання та налаштування буде покроково описаний нижче.

Крок 1 - Встановлення OpenVPN та Easy-RSA.

Перший крок використовує інсталяцію OpenVPN та Easy-RSA. Easy-RSA – це інструмент управління інфраструктурою відкритих ключів (PKI), який буде використаний на сервері OpenVPN, щоб згенерувати запит на отримання сертифіката, який потім буде перевірятися та підписуватися на сервері ЦС.

Створюється новий каталог на сервері OpenVPN, від імені non-root користувача з назвою *~/easy-rsa*:

mkdir ~/easy-rsa

Далі створюється символьне посилання із скрипту easyrsa, встановленого пакетом у директорії ~/easy-rsa, щойностореного:

ln -s /usr/share/easy-rsa/ ~/easy-rsa/*

Власником директорії має бути користувач non-root user з привілеями sudo, обмежуємо доступ за допомогою команди chmod:

sudo chown sammy ~/easy-rsa

chmod 700 ~/easy-rsa

Після встановлення цих програм та їх переміщення у потрібні локації у системі, наступним кроком буде створення інфраструктури відкритих ключів (PKI) на сервері OpenVPN, щоб можна було б запитувати та керувати сертифікатами TLS для OpenVPN клієнтів та інших серверів, які підключатимуться до VPN.

Крок 2 - Створення PKI для OpenVPN.

Перш ніж можна буде створювати закритий ключ і сертифікат сервера OpenVPN, потрібно створити локальну директорію інфраструктури відкритих ключів на сервері OpenVPN. Директорія буде для керування запитами сертифіката сервера та клієнтів замість того, щоб отримувати їх прямо на сервері ЦС.

cd ~/easy-rsa

nano vars

Після відкриття файлу вставляємо наступні два рядки:

set_var EASYRSA_ALGO "ec"

set_var EASYRSA_DIGEST "sha512"

Ці два рядки будуть потрібні у файлі *vars* на сервері OpenVPN, оскільки він не використовуватиметься як ЦС. Вони будуть гарантувати, що закриті ключі та запити сертифіката будуть налаштовані для використання сучасної криптографії на еліптичних кривих (Elliptic Curve Cryptography, ECC) під час генерації ключів та захищених підписів для клієнтів та сервера OpenVPN. Під налаштуванням використання ECC для серверів OpenVPN і ЦС мається на увазі, що коли OpenVPN клієнт і сервер намагатимуться встановити загальний симетричний ключ, вони будуть використовувати алгоритми еліптичної кривої для обміну. Використання ECC для обміну ключами значно швидше, ніж використання простого алгоритму Діффі-Хеллмана з класичним алгоритмом RSA, оскільки числа набагато менші, а обчислення виконуються швидше.

Після додавання даних до файлу *vars* можна перейти до створення директорії PKI. Для цього скористайтесь скриптом *easyrsa* з опцією *init-pki*.

./easyrsa init-pki

На сервері OpenVPN не потрібно створювати центр сертифікації. Сервер ЦС відповідає за валідацію та підпис сертифікатів. PKI на сервері VPN використовується лише як зручне та централізоване місце зберігання запитів сертифіката та публічних сертифікатів. Після ініціалізації PKI на сервері OpenVPN, переходимо до наступного кроку та створюємо запит сертифікату та закритого ключа серверу OpenVPN.

Крок 3 — Створення запиту сертифіката та закритого ключа сервера OpenVPN.

Згенеруємо закритий ключ і запит підпису сертифіката на сервері OpenVPN. Після цього передаємо запит до центру сертифікації для підпису, створивши необхідний сертифікат. Після підпису сертифіката передаємо його назад на сервер

OpenVPN та налаштовуємо для використання на сервері. Перейдіть до директорії *~/easy-rsa* на сервері OpenVPN, використовуючи користувача non-root user:

cd ~/easy-rsa

Тепер можна викликати *easyrsa* з опцією *gen-req*, до якої необхідно вказати стандартне ім'я для комп'ютера. Можна використовувати будь-яке стандартне ім'я, але найкраще вибрати варіант, що запам'ятовується. У прикладі буде використовуватися стандартне ім'я *server*. Додаємо опцію *nopass*. Без цього файл запиту буде захищений паролем, що згодом може призвести до проблем із дозволами. Результат зазначено нижче, на рис. 2.1.1.

./easyrsa gen-req server nopass

```
Output
Common Name (eg: your user, host, or server name) [server]:

Keypair and certificate request completed. Your files are:
req: /home/sammy/easy-rsa/pki/reqs/server.req
key: /home/sammy/easy-rsa/pki/private/server.key
```

Рис. 2.1.1 – Створення закритого ключа для сервера та файл запиту сертифіката

В результаті буде створено закритий ключ для сервера та файл запиту сертифіката з ім'ям *server.req*. Скопіюємо ключ сервера в каталог */etc/openvpn/server:*

sudo cp /home/sammy/easy-rsa/pki/private/server.key /etc/openvpn/server/

В результаті виконання цих кроків успішно створено закритий ключ та запит на підпис сертифіката для сервера OpenVPN. Запит на підпис сертифіката тепер готовий до підпису у центрі сертифікації.

Крок 4 — Підпис запиту сертифіката сервера OpenVPN

У попередньому кроці створено запит на підпис сертифіката (CSR) та закритий ключ для сервера OpenVPN. Тепер сервер ЦС повинен дізнатися про сертифікат *server* та виконати його валідацію. Після підтвердження сертифіката сервером ЦС та його відправлення назад на сервер OpenVPN клієнти, які довіряють вашому ЦС, зможуть довіряти серверу OpenVPN.

На сервері OpenVPN від імені користувача *non-root user* скористаємось запитом на передачу сертифіката *server.req* на сервер ЦС для підпису:

*scp /home/sammy/easy-rsa/pki/reqs/server.req **sammy**@**your_ca_server_ip**:/tmp*

Наступним кроком буде увійти на сервер ЦС як користувач без привілеїв *root*, якого створили для керування ЦС. Використовуючи команду *cd* для переходу в каталог *~/easy-rsa*, імпортуємо запит сертифіката за допомогою скрипта *easyrsa*:

cd ~/easy-rsa

./easyrsa import-req /tmp/server.req server

Підписуємо запит, запустивши скрипт *easyrsa* з опцією *sign-req* та вказівкою типу запиту та стандартного імені. Як тип запиту може використовуватися *client* або *server*. Оскільки працюємо із запитом сертифіката сервера OpenVPN, необхідно використовувати тип запиту *server*:

./easyrsa sign-req server server

У вводі, як зазначено на рис. 2.1.2 потрібно буде підтвердити, що запит надійшов із надійного джерела. Вводимо *yes*, натискаємо *ENTER*, щоб підтвердити:

```
Output
You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 3650 days:

subject=
commonName = server


Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
. . .
Certificate created at: /home/sammy/easy-rsa/pki/issued/server.crt
```

Рис. 2.1.2 – Підпис сертифікату серверу

Якщо закритий ключ ЦС зашифрований, буде запропоновано ввести пароль в даний момент.

Після виконання цих кроків запит сертифіката сервера OpenVPN за допомогою закритого ключа сервера ЦС успішно підписано. Отриманий файл *server.crt* містить відкритий ключ шифрування сервера OpenVPN, а також новий підпис від сервера ЦС. Зміст підпису полягає в тому, щоб повідомити всіх, хто довіряє серверу ЦС,

що вони також можуть довіряти серверу OpenVPN при підключенні до нього. Для завершення налаштування сертифікатів скопіюємо файли *server.crt* та *ca.crt* із сервера ЦС на сервер OpenVPN:

scp pki/issued/server.crt sammy@your_vpn_server_ip:/tmp

scp pki/ca.crt sammy@your_vpn_server_ip:/tmp

Повернемось на сервер OpenVPN, скопіюємо файли з /tmp в /etc/openvpn/server:

sudo cp /tmp/{server.crt,ca.crt} /etc/openvpn/server

Крок 5 - Налаштування криптографічних матеріалів OpenVPN

Як додатковий рівень безпеки додаємо загальний секретний ключ, який використовують сервер і всі клієнти OpenVPN, за допомогою директиви OpenVPN *tls-crypt*. Ця опція допомагає зашифрувати сертифікат TLS, що використовується при першому підключенні сервера та клієнта OpenVPN один до одного. Крім того, сервер OpenVPN використовує її для швидкої перевірки вхідних пакетів: якщо пакет підписаний за допомогою попередньо наданого ключа, сервер обробляє його; якщо підпису немає, сервер розпізнає пакет як отриманий з неперевіреного джерела та може відхилити його без додаткового розшифрування.

Для отримання попередньо наданого ключа tls-crypt запустіть наступну команду на сервері OpenVPN в директорії ~/easy-rsa:

cd ~/easy-rsa

openvpn --genkey --secret ta.key

В результаті отримаємо файл з назвою *ta.key*. Скопіюємо його в директорію */etc/openvpn/server/:*

sudo cp ta.key /etc/openvpn/server

Після отримання цих файлів на сервері OpenVPN переходимо до створення клієнтських сертифікатів та файлів ключів для користувачів, які будуть підключатися до VPN.

Крок 6 - Створення сертифіката клієнта та пари ключів

Розглядається процес генерування запиту сертифіката на сервері OpenVPN. Перевага цього підходу полягає в тому, що можна створити скрипт, який автоматично генеруватиме файли конфігурації OpenVPN клієнтів, що містять усі

необхідні ключі та сертифікати. Завдяки цьому не потрібно буде передавати ключі, сертифікати та файли конфігурації на клієнтські системи, а процес підключення до VPN прискорюється. Створюємо одну пару з ключа і сертифіката для клієнтської системи. Якщо є кілька клієнтських систем, можна повторити цей процес для кожної такої системи. Для кожного OpenVPN клієнта в скрипті потрібно вказати унікальне ім'я. Генеруємо першу пару сертифікат/ключ під іменем *client1*.

Спочатку створюється у домашній директорії структуру директорій, де зберігатимуться файли сертифікатів та ключів клієнтської системи:

mkdir -p ~/client-configs/keys

Оскільки в цій директорії зберігатимуться пари сертифікат/ключ клієнтів та файли конфігурації, для неї слід закрити всі дозволи:

chmod -R 700 ~/client-configs

Повертаємось в директорію EasyRSA і запускаємо скрипт *easyrsa* з опціями *gen-req* і *nopass*, вказавши ім'я OpenVPN клієнта:

cd ~/easy-rsa

./easyrsa gen-req client1 nopass

Натискаємо ENTER, щоб підтвердити ім'я. Копіюємо файл *client1.key* у раніше створену директорію ~/client-configs/keys/ :

cp pki/private/client1.key ~/client-configs/keys/

Передаємо файл *client1.req* на сервер ЦС, використовуючи безпечний метод:

scp pki/reqs/client1.req ***sammy@your_ca_server_ip****:/tmp*

Виконуємо вхід на сервер ЦС. Переходимо до директорії EasyRSA та імпортуємо запит сертифіката:

cd ~/easy-rsa

./easyrsa import-req /tmp/client1.req client1

Підписуємо запит, як це було для сервера на попередньому етапі. Однак цього разу обов'язково вказується тип запиту *client*:

./easyrsa sign-req client client1

При запиті вводимо *yes*, як зазначено на рис. 2.1.3 для підтвердження, що плануємо підписати запит сертифіката та що він надійшов із довіреного джерела:

```
Output
Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
```

Рис. 2.1.3 – Підтвердження підпису сертифікату

Якщо ключ ЦС зашифровано, буде запропоновано ввести пароль.

В результаті буде створено файл сертифікат OpenVPN клієнта з ім'ям *client1.crt*. Перемістимо файл назад на сервер.

scp pki/issued/client1.crt ***sammy@your_server_ip****:/tmp*

Повертаємось на сервер OpenVPN, копіюємо клієнтський сертифікат у директорію *~/client-configs/keys/ :*

cp /tmp/client1.crt ~/client-configs/keys/

Копіюємо файли *ca.crt* та *ta.key* у директорію *~/client-configs/keys/* і надаємо відповідні дозволи для користувача sudo:

cp ~/easy-rsa/ta.key ~/client-configs/keys/

sudo cp /etc/openvpn/server/ca.crt ~/client-configs/keys/

*sudo chown sammy.sammy ~/client-configs/keys/**

В результаті згенеровано ключі та сертифікати для сервера та клієнта, їх збережено у відповідних директоріях на сервері OpenVPN.

Крок 7 - Налаштування OpenVPN

Буде надано інструкції з налаштування конфігурації сервера OpenVPN на основі одного з прикладів конфігураційних файлів, який включено в документацію для цього програмного забезпечення.

Спочатку скопіюємо файл *server.conf* як відправну точку для власного файлу конфігурації:

sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz/etc/openvpn/server/

sudo gunzip /etc/openvpn/server/server.conf.gz

Відкриваємо новий файл для редагування в текстовому редакторі nano.

sudo nano /etc/openvpn/server/server.conf

Потрібно змінити кілька рядків у цьому файлі. Спочатку необхідно знайти розділ HMAC у конфігурації, виконавши пошук директиви *tls-auth*. Цей рядок має бути розкоментований. Закоментуйте її, додавши; на початок рядка. Потім додаємо після неї новий рядок, що містить лише значення *tls-crypt ta.key*, як зазначено на рис. 2.1.4.

/etc/openvpn/server/server.conf

```
; tls-auth ta.key 0 # This file is secret
tls-crypt ta.key
```

Рис. 2.1.4 – Конфігурація файлу server.conf

Знаходимо розділ криптографічних шифрів, виконавши пошук рядків із текстом *cipher*. За замовчуванням встановлено значення AES-256-CBC, проте шифр AES-256-GCM забезпечує вищий рівень шифрування, продуктивності та краще підтримується сучасними клієнтами OpenVPN. Закоментуємо значення за замовчуванням, додавши *;* на початок цього рядка, а потім додамо інший рядок після неї, як показано на рис. 2.1.5, що містить оновлене значення AES-256-GCM:

/etc/openvpn/server/server.conf

```
; cipher AES-256-CBC
cipher AES-256-GCM
```

Рис. 2.1.5 – Зміна криптографічного шифру

Відразу після цього рядка додаємо директиву *auth*, зазначено на рис. 2.1.6, для вибору алгоритму вибірки повідомлень HMAC. Для цього підійде SHA256:

/etc/openvpn/server/server.conf

```
auth SHA256
```

Рис. 2.1.6 – Додавання директиви auth до server.conf

Знаходимо рядок з директивою *dh*, який визначає параметри алгоритму Діффі - Хеллмана. Оскільки налаштовано всі сертифікати для використання криптографії на еліптичних кривих, немає необхідності використовувати файл прототипу Діффі

— Хеллмана. Рис. 2.1.7 показано, закоментуємо існуючий рядок *dh dh2048.pem* або *dh dh.pem*. Ім'я файлу для ключа Діффі-Хеллмана може відрізнятися від того, що перераховано в прикладі конфігураційного файлу сервера. Додаємо рядок після неї із вмістом *dh none*:

/etc/openvpn/server/server.conf

```
; dh dh2048.pem
dh none
```

Рис. 2.1.7 – Відключення протоколу Діффі — Хеллмана

Далі потрібно запустити OpenVPN без привілеїв, з якими він запущений, тому потрібно зазначити необхідність запуску з користувачем *nobody* та групою *nogroup*. Щоб активувати цю можливість, знайдемо та розкоментуємо рядки *user nobody* та *group nogroup*, вилучивши *;* на початку кожного рядка, продеменстровано на рис. 2.1.8:

/etc/openvpn/server/server.conf

```
user nobody
group nogroup
```

Рис. 2.1.8 – Зміна користувача та групи за замовчуванням

(Необов'язково) Зміна порту та протоколу.

За замовчуванням сервер OpenVPN використовує для підключення клієнтів порт 1194 та протокол UDP. Якщо потрібно використовувати інший порт через обмеження мережі OpenVPN клієнта, можна змінити номер порту. Якщо не зберігається веб-контент на сервері OpenVPN, підійде порт 443, оскільки зазвичай його не забороняють правила брандмауера. Щоб змусити OpenVPN прослуховувати порт 443, відкриваємо файл *server.conf* і знайдемо рядок, як зазначено на рис. 2.1.9.

/etc/openvpn/server/server.conf

```
port 1194
```

Рис. 2.1.9 – Зміна порту протоколу за замовчуванням

Вказуємо порт 443.

Досить часто цей порт також обмежує протокол. У цьому випадку знайдемо рядок *proto* під рядком *port* і змінимо протокол з *udp* на *tcp*, представлено на рис. 2.1.10:

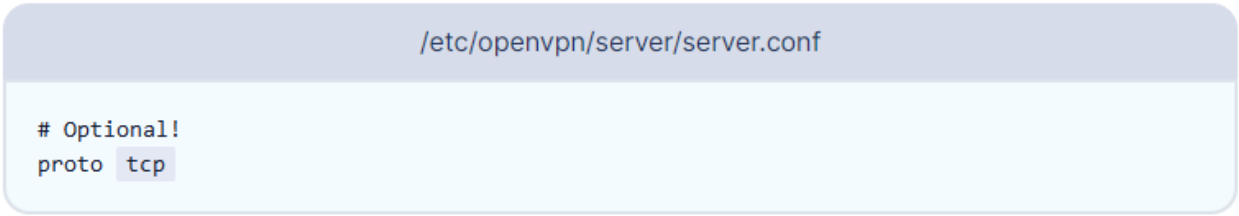

Рис. 2.1.10 – Зміна протоколу за замовчуванням

Якщо змінили протокол на TCP, потрібно буде змінити значення директиви *explicit-exit-notify* з *1* на *0*, оскільки ця директива використовується лише протоколом UDP. В іншому випадку при запуску служби OpenVPN можливі помилки протоколу TCP.

Як показано на рис. 2.1.11, знаходимо рядок *explicit-exit-notify* в кінці файлу та змінимо значення на 0:

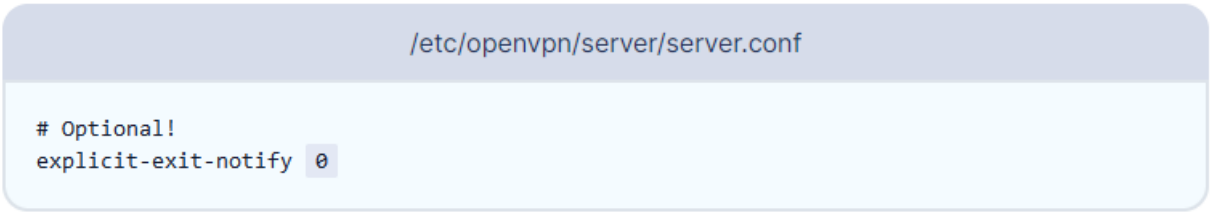

Рис. 2.1.11 – Зміна директиви за замовчуванням

Якщо не потрібно використовувати інші порт і протокол, краще залишити ці налаштування без змін.

Крок 8 — Налаштування конфігурації мережі сервера OpenVPN

Щоб OpenVPN міг правильно перенаправляти трафік через мережу VPN, необхідно змінити деякі параметри конфігурації мережі сервера. Насамперед потрібно змінити параметр *IP forwarding*, який визначає необхідність перенаправлення IP-трафіку. Це необхідно для реалізації функцій VPN, які надаються сервером.

Для зміни налаштування IP-передачі сервера OpenVPN, що використовуються за замовчуванням, відкриваємо файл /etc/sysctl.conf за допомогою nano або бажаного редактора:

sudo nano /etc/sysctl.conf

Як показано на рис. 2.1.12, додаємо наступний рядок до кінця файлу:

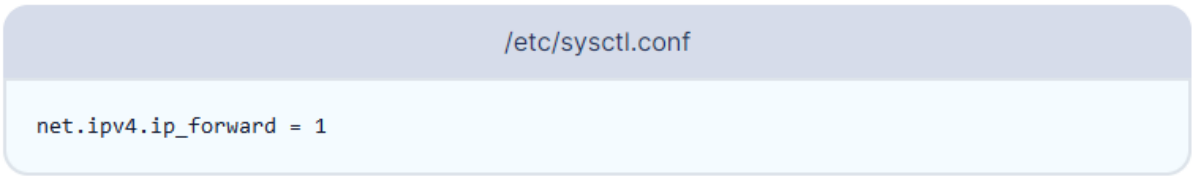

Рис. 2.1.12 – Зміна налаштування IP-передачі сервера

Зберігаємо файл та закриваємо його.

Щоб прочитати файл та завантажити значення для поточної сесії, вводимо:

sudo sysctl -p

Тепер сервер OpenVPN зможе перенаправляти вхідний трафік з одного мережного пристрою на інший. Ця команда гарантує, що сервер зможе спрямовувати трафік від клієнтів, підключених до віртуального інтерфейсу VPN, на інші фізичні мережеві пристрої. Конфігурація буде передавати весь веб-трафік від клієнта через IP-адресу вашого сервера, а відкрита IP-адреса OpenVPN клієнта буде фактично прихована.

Крок 9 - Налаштування брандмауера

На даний момент встановлено OpenVPN на сервер, налаштувано його та створено ключі та сертифікати, необхідні OpenVPN клієнту для доступу до VPN. Однак ще не надали OpenVPN жодних інструкцій про те, куди потрібно відправляти вхідний веб-трафік від його клієнтів. Вказуємо, як сервер повинен обробляти трафік клієнта, додавши ряд правил брандмауера і налаштувавши конфігурацію маршрутизації.

Щоб дозволити OpenVPN через брандмауер, потрібно буде увімкнути маскування. Маскування – це концепція таблиць *iptables*, на основі якої виконується автоматична трансляція мережевих адрес (NAT) для правильної маршрутизації клієнтських з'єднань.

Перш ніж відкрити конфігураційний файл брандмауера для додавання правил, потрібно попередньо знайти публічний мережевий інтерфейс комп'ютера.

Для цього вводимо:

ip route list default

Рядок після слова *"dev"* у цій команді - це публічний інтерфейс.

Наприклад, на рис. 2.1.13 продемонстровано інтерфейс з ім'ям *eth0*:

```
Output
default via 159.65.160.1 dev eth0 proto static
```

Рис. 2.1.13 – Визначення публічного мережевого інтерфейсу

Відкриваємо файл */etc/ufw/before.rules*, щоб додати відповідну конфігурацію:

sudo nano /etc/ufw/before.rules

Правила UFW зазвичай додаються за допомогою команди *ufw*. Правила, перелічені у файлі before.rules, зчитуються та активуються до завантаження звичайних правил UFW. Додаємо у верхню частину файлу виділені на рис. 2.1.14 рядки. Після цього буде задана політика за замовчанням для ланцюжка *POSTROUTING* у таблиці *nat*, і будь-який трафік VPN маскуватиметься.

/etc/ufw/before.rules

```
#
# rules.before
#
# Rules that should be run before the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   ufw-before-input
#   ufw-before-output
#   ufw-before-forward
#

# START OPENVPN RULES
# NAT table rules
*nat
:POSTROUTING ACCEPT [0:0]
# Allow traffic from OpenVPN client to eth0 (change to the interface you discovered!)
-A POSTROUTING -s 10.8.0.0/8 -o eth0 -j MASQUERADE
COMMIT
# END OPENVPN RULES

# Don't delete these required lines, otherwise there will be errors
*filter
. . .
```

Рис. 2.1.14 – Зміна правил UFW

Зберігаємо файл та закриваєм.

Вказуємо UFW дозволяти перенаправлення пакетів за замовчуванням. Для цього відкриваємо файл */etc/default/ufw*:

sudo nano /etc/default/ufw

Знайдемо у файлі директиву *DEFAULT_FORWARD_POLICY* і змініть значення з *DROP* на *ACCEPT*, як показано на рис. 2.1.15:

Рис. 2.1.15 – Зміна правил UFW

Зберігаємо файл та закриваємо.

Потім змінюємо налаштування брандмауера, щоб дозволити трафік OpenVPN. Якщо не змінювали порт і протокол у файлі */etc/openvpn/server.conf*, потрібно буде відкрити трафік UDP на порті 1194. Якщо змінювали порт або протокол, замінюємо вибрані значення. Також додаємо порт SSH:

sudo ufw allow 1194/udp

sudo ufw allow OpenSSH

Після додавання цих правил вимкнемо і заново увімкнемо UFW, щоб завантажити зміни зі всіх змінених файлів:

sudo ufw disable

sudo ufw enable

Після створення правил брандмауера можна запустити службу OpenVPN на сервері.

Крок 10 - Запуск OpenVPN

OpenVPN працює як служба *systemd*, тому можна використовувати *systemctl* для керування. Налаштуємо для OpenVPN запуск під час завантаження, щоб можна було підключатися до VPN у будь-який час, поки сервер працює. Для цього активуємо службу OpenVPN, додавши її до *systemctl*:

sudo systemctl -f enable openvpn-server@server.service

Запускаємо службу OpenVPN:

sudo systemctl start openvpn-server@server.service

Первіряємо, що служба OpenVPN активна, скориставшись наступною командою. Ви повинні побачити у виводі *active* (*running*), як на рис. 2.1.16:

sudo systemctl status openvpn-server@server.service

```
Output
● openvpn-server@server.service - OpenVPN service for server
     Loaded: loaded (/lib/systemd/system/openvpn-server@.service; enabled; vendor preset: e
     Active: active (running) since Wed 2020-04-29 15:39:59 UTC; 6s ago
       Docs: man:openvpn(8)
             https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
             https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 16872 (openvpn)
     Status: "Initialization Sequence Completed"
      Tasks: 1 (limit: 1137)
     Memory: 1.0M
     CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server.service
             └─16872 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log --sta
. . .
. . .
Apr 29 15:39:59 ubuntu-20 openvpn[16872]: Initialization Sequence Completed
```

Рис. 2.1.16 – Перевірка запуску служби OpenVPN

Успішно завершено конфігурацію OpenVPN на стороні сервера. Далі налаштування клієнтського комп'ютер і підключення до сервера OpenVPN.

2.2 Налаштування клієнтів для підключення до VPN

Крок 1 - Створення інфраструктури конфігурації клієнтських систем

Замість створення єдиного конфігураційного файлу, який можна використовувати лише для одного OpenVPN клієнта, на цьому кроці зазначено процес створення інфраструктури клієнтської конфігурації, який використовується для швидкого генерування файлів конфігурації. Спочатку створюємо базовий файл конфігурації, а потім сценарій, який дозволить при необхідності генерувати унікальні файли конфігурації OpenVPN клієнтів, сертифікати та ключі.

Створюємо нову директорію для зберігання файлів конфігурації клієнтів у раніше створеній директорії *client-configs*:

mkdir -p ~/client-configs/files

Потім скопіюємо файл зі зразком конфігурації клієнта в каталог *client-configs*, щоб використовувати його як базову конфігурацію:

cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client-configs/base.conf

Відкриємо новий файл у nano або іншому текстовому редакторі:

nano ~/client-configs/base.conf

Знайдемо у файлі директиву *remote*. Вона вказує OpenVPN клієнту адресу сервера OpenVPN, тобто публічну IP-адресу вашого сервера OpenVPN. Якщо змінено порт, який прослуховуватиме сервер OpenVPN, потрібно буде замінити 1194 на вибраний порт, як зазначено на рис. 2.2.1 нижче:

~/client-configs/base.conf

```
. . .
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote your_server_ip 1194
. . .
```

Рис. 2.2.1 – Конфігурація IP-адреси та порту серверу OpenVPN для клієнту

На рис. 2.2.2 продемонстровано, протокол повинен відповідати значенням, які використовуються в конфігурації сервера,:

~/client-configs/base.conf

```
proto udp
```

Рис. 2.2.2 – Конфігурація протоколу серверу OpenVPN для клієнту

Розкоментуємо директиви *user* та *group*, вилучивши символ *;* на початку кожного рядка, рис. 2.2.3:

~/client-configs/base.conf

```
# Downgrade privileges after initialization (non-Windows only)
user nobody
group nogroup
```

Рис. 2.2.3 – Конфігурація привілеї OpenVPN клієнта

Знайдемо директиви, які задають *ca, cert* та *key*. Як показано на рис. 2.2.4, поставимо знак коментаря перед рядками цих директив, оскільки додамо сертифікати та ключі до самого файлу:

~/client-configs/base.conf

```
# SSL/TLS parms.
# See the server config file for more
# description. It's best to use
# a separate .crt/.key file pair
# for each client. A single ca
# file can be used for all clients.
; ca ca.crt
; cert client.crt
; key client.key
```

Рис. 2.2.4 – Відключення директив сертифікатів для OpenVPN клієнту

Потім закоментуємо директиву *tls-auth*, представлено на рисунку 2.2.5, оскільки додаємо *ta.key* прямо до файлу конфігурації клієнта (а сервер налаштований на використання *tls-crypt*):

~/client-configs/base.conf

```
# If a tls-auth key is used on the server
# then every client must also have the key.
; tls-auth ta.key 1
```

Рис. 2.2.5 – Відключення директиви *tls-auth*

Створюємо дзеркало налаштувань *cipher* та *auth*, як показано на рис. 2.2.6, заданих у файлі */etc/openvpn/server/server.conf:*

~/client-configs/base.conf

```
cipher AES-256-GCM
auth SHA256
```

Рис. 2.2.6 – Створення дзеркала налаштувань *cipher* та *auth*

Додаємо у файл директиву *key-direction*. Потрібно встановити значення *«1»,* щоб VPN правильно працював на клієнтському комп'ютері:

~/client-configs/base.conf

```
key-direction 1
```

Рис. 2.2.7 – Додавання директиви *key-direction*

Насамкінець, як зазначено на рис. 2.2.8, додаємо кілька закоментованих рядків для обробки різних методів, які клієнти VPN на базі Linux будуть використовувати для дозволу DNS. Також додамо два схожі, але окремі набори закоментованих рядків. Перший набір призначений для клієнтів, які не використовують *systemd-resolved* для керування DNS. Ці клієнти використовують утиліту *resolvconf* для оновлення інформації DNS для клієнтів Linux.

~/client-configs/base.conf

```
; script-security 2
; up /etc/openvpn/update-resolv-conf
; down /etc/openvpn/update-resolv-conf
```

Рис. 2.2.8 – Додаткова конфігурація для керування DNS

Тепер додаємо інший набір рядків для клієнтів, які використовують *systemd-resolved* для дозволу DNS, зображено на рис. 2.2.9:

~/client-configs/base.conf

```
; script-security 2
; up /etc/openvpn/update-systemd-resolved
; down /etc/openvpn/update-systemd-resolved
; down-pre
; dhcp-option DOMAIN-ROUTE .
```

Рис. 2.2.9 – Дозвіл DNS для OpenVPN клієнтів *systemd-resolved*

Зберігаємо файл та закриваємо.

Створюємо простий скрипт, який скомпілює базову конфігурацію з відповідним сертифікатом, ключем та файлами шифрування, переносимо згенеровану конфігурацію в директорію *~/client-configs/files*. Відкриємо новий файл з ім'ям *make_config.sh* у директорії *~/client-configs:*

nano ~/client-configs/make_config.sh

Як представлено на рис. 2.2.10, додаємо до файлу наступне:

~/client-configs/make_config.sh

```
#!/bin/bash

# First argument: Client identifier

KEY_DIR=~/client-configs/keys
OUTPUT_DIR=~/client-configs/files
BASE_CONFIG=~/client-configs/base.conf

cat ${BASE_CONFIG} \
    <(echo -e '<ca>') \
    ${KEY_DIR}/ca.crt \
    <(echo -e '</ca>\n<cert>') \
    ${KEY_DIR}/${1}.crt \
    <(echo -e '</cert>\n<key>') \
    ${KEY_DIR}/${1}.key \
    <(echo -e '</key>\n<tls-crypt>') \
    ${KEY_DIR}/ta.key \
    <(echo -e '</tls-crypt>') \
    > ${OUTPUT_DIR}/${1}.ovpn
```

Рис. 2.2.10 – Скрипт для компіляції базової кофігурації

Зберігаємо файл та закриваємо.

Позначаємо цей файл як виконуваний, ввівши таку команду:

chmod 700 ~/client-configs/make_config.sh

Цей скрипт створює копію створеного файлу *base.conf*, збирає всі створені для OpenVPN клієнта файли сертифікатів та ключів, витягує їх вміст, додає їх у копію базового файлу конфігурації та експортує все це у новий файл конфігурації клієнта. Це означає, що вся необхідна інформація зберігається в одному місці, і не потрібно керувати файлами конфігурації клієнта, сертифікатами і ключами окремо. Перевага такого методу полягає в тому, що якщо в майбутньому потрібно додати OpenVPN клієнта, можна просто запустити цей скрипт, щоб швидко створити файл конфігурації, а вся важлива інформація зберігатиметься в одному зручному для доступу місці.

При додаванні кожного нового OpenVPN клієнта потрібно буде згенерувати для нього нові ключі та сертифікати, перш ніж запускати цей скрипт і генерувати файл конфігурації.

Крок 2 - Створення конфігурацій клієнтів

Створили клієнтський сертифікат та ключ з іменами client1.crt та client1.key відповідно. Тепер створюємо файл конфігурації для цих облікових даних, перейшовши в директорію *~/client-configs* і запускаємо скрипт, створений наприкінці попереднього кроку:

cd ~/client-configs

./make_config.sh client1

При цьому файл *client1.ovpn* буде створений у директорії *~/client-configs/files* Цей файл потрібно буде перемістити на пристрій, який планується використовувати як клієнт. Наприклад, це може бути локальний комп'ютер або мобільний пристрій.

Хоча конкретні програми передачі залежать від операційної системи пристрою, один з найбільш надійних та безпечних способів – використовувати SFTP (протокол передачі файлів SSH) або SCP (захищене копіювання) на стороні сервера. При цьому файли автентифікації VPN клієнта передаватимуться через шифроване з'єднання.

Наведено приклад команди SFTP, яку можна запустити з локального комп'ютера (під керуванням macOS або Linux). Вона копіюватиме файл client1.ovpn, який створено, у домашню директорію:

*sftp **sammy@openvpn_server_ip**:client-configs/files/client1.ovpn ~/*

Крок 3 - Встановлення клієнтської конфігурації

Показано, як встановити клієнтський профіль VPN у Windows, macOS, Linux.

Підключення OpenVPN матиме ім'я, що збігається з ім'ям .ovpn. Це означає, що з'єднання матиме ім'я *client1.ovpn*, що відповідає першому згенерованому клієнтському файлу.

Windows. Встановлення

Завантажуємо клієнтську програму OpenVPN для Windows з офіційного сайту OpenVPN. Вибираємо відповідну версію інсталяції програми для версії Windows.

Після встановлення OpenVPN копіюємо файл *.ovpn* у:

C:\Program Files\OpenVPN\config

При запуску OpenVPN профіль буде автоматично виявлено та стане доступним. Потрібно запускати OpenVPN від імені адміністратора щоразу, навіть якщо використовується обліковий запис адміністратора. Щоб не потрібно було при кожному запуску VPN натискати праву кнопку миші та вибирати «Запуск від імені адміністратора», такий запуск слід налаштувати в обліковому записі адміністратора. Це також означає, що звичайним користувачам потрібно буде ввести пароль адміністратора для використання OpenVPN. Звичайні користувачі не зможуть правильно підключитися до сервера, якщо програма OpenVPN на клієнтській системі не має прав адміністратора, тому необхідний підвищений рівень привілеїв.

Щоб налаштувати OpenVPN для запуску від імені адміністратора при кожному запуску, натискаємо правою кнопкою миші на його ярлик і обираємо «Властивості». У нижній частині вкладки «Сумісність» натискаємо кнопку «Змінити параметри для всіх користувачів». У новому вікні встановлюємо позначку «Запускати цю програму від імені адміністратора».

При запуску клієнтської програми OpenVPN в області завдань з'являється значок програми, за допомогою якого можна підключати та вимикати з'єднання VPN; з'єднання VPN не встановлюється автоматично.

Після запуску OpenVPN натискаємо правою кнопкою на піктограму OpenVPN в області завдань, щоб створити з'єднання. Відкриється контекстне меню. Обираємо *client1* у верхній частині меню (це профіль client1.ovpn) і тиснемо «Підключитися».

Відкриється вікно стану, де будуть виведені дані журналу під час встановлення з'єднання, і після підключення OpenVPN клієнта буде виведено повідомлення.

Відключення від VPN виконується аналогічно: переходимо в область завдань, натисніть піктограму OpenVPN правою кнопкою миші, вибираємо профіль клієнта і тиснемо «Відключитись».

macOS. Встановлення

Tunnelblick — безкоштовний клієнт OpenVPN з відкритим кодом для macOS. Завантажуємо останній образ цієї клієнтської програми зі сторінки завантаження Tunnelblick. Двічі натискаємо завантажений файл .dmg і дотримуйтесь інструкцій з інсталяції. Наприкінці процесу встановлення Tunnelblick запитає, чи є конфігураційні файли. Вказуємо – «У мене є конфігураційні файли» і даємо Tunnelblick завершити роботу. Відкриваємо вікно «Finder» та двічі натискаємо *client1.ovpn*. Tunnelblick встановить профіль клієнта. Для цього потрібні привілеї адміністратора.

Запускаємо Tunnelblick, двічі клацнувши піктограму Tunnelblick у папці «Програми». Після запуску Tunnelblick у верхньому правому куті екрана з'явиться значок Tunnelblick для керування з'єднаннями. Натискаємо значок, а потім натискаємо меню «Підключити client1», щоб створити з'єднання VPN.

Linux. Встановлення

Якщо використовується Linux, існують різні інструменти, залежно від дистрибутива. Однак найпростіше використовувати для цього програмне забезпечення OpenVPN.

У Ubuntu або Debian можна встановити його так само, як і сервер, ввівши команду:

sudo apt install openvpn

У CentOS можна активувати репозиторії EPEL і виконати інсталяцію, ввівши команди:

sudo dnf install epel-release

sudo dnf install openvpn

Налаштування клієнтів, що використовують *systemd-resolved*

Спочатку визначаємо, чи використовує система *systemd-resolved* для дозволу DNS, перевіривши файл /etc/resolv.conf:

cat /etc/resolv.conf

Якщо система налаштована для використання systemd-resolved для дозволу DNS, як зазначено на рис. 2.2.11, IP-адреса після опції nameserver буде мати значення 127.0.0.53. Також у файлі повинні бути коментарі, зокрема інформація про те, як *systemd-resolved* управляє файлом. Якщо відображається не 127.0.0.53, а інша IP-адреса, то є ймовірність, що ваша система не використовує *systemd-resolved*. У цьому випадку можна перейти до наступного розділу, призначеного для налаштування OpenVPN клієнтів Linux, які використовують скрипт *update-resolv-conf*.

```
Output
# This file is managed by man:systemd-resolved(8). Do not edit.
. . .

nameserver 127.0.0.53
options edns0
```

Рис. 2.2.11 – Визначення *systemd-resolved* системи.

Для підтримки OpenVPN клієнтів *systemd-resolved* необхідно попередньо встановити пакет *openvpn-systemd-resolved*. Він містить скрипти, що примусово запускають використання *systemd-resolved* для дозволу DNS сервером VPN.

sudo apt install openvpn-systemd-resolved

Після встановлення пакета налаштовуємо OpenVPN клієнт для його використання та надсилання всіх запитів DNS через інтерфейс VPN. Відкриваємо файл VPN клієнта:

nano client1.ovpn

Розкоментовуємо наступні рядки, додані раніше, як показано на рис. 2.2.12:

client1.ovpn

```
script-security 2
up /etc/openvpn/update-systemd-resolved
down /etc/openvpn/update-systemd-resolved
down-pre
dhcp-option DOMAIN-ROUTE .
```

Рис. 2.2.12 – Конфігурація OpenVPN клієнту під *systemd-resolved*.

Налаштування клієнтів, які використовують *update-resolv-conf*

Якщо система не використовує *systemd-resolved* для керування DNS, перевіряємо наявність у дистрибутиві скрипту */etc/openvpn/update-resolv-conf:*

ls /etc/openvpn

```
Output
update-resolv-conf
```

Рис. 2.2.13 – Перевірка update-resolv-conf у системі.

Якщо OpenVPN клієнт має файл *update-resolv-conf,* як представлено на рис. 2.2.13, змінимо раніше переданий файл конфігурації клієнта OpenVPN:

nano client1.ovpn

Розкоментуємо три додані рядки, щоб змінити налаштування DNS, показано на рис. 2.2.14:

client1.ovpn

```
script-security 2
up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf
```

Рис. 2.2.14 – Зміна налаштування DNS

Якщо використовується CentOS, змінимо директиву *group* з *nogroup* на *nobody* для відповідності доступним групам дистрибутива, як зображено на рис. 2.2.15:

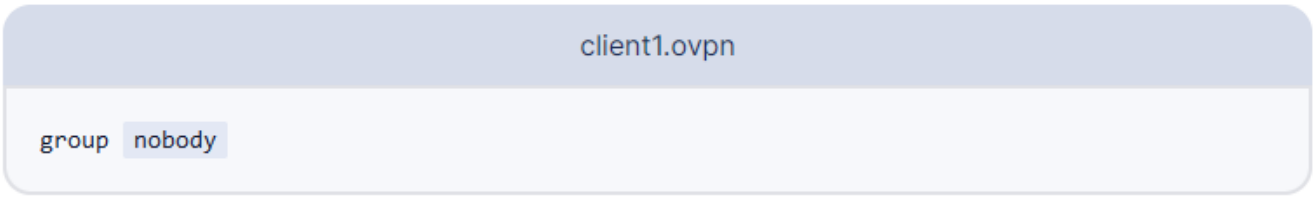

Рис. 2.2.15 – Зміна директиви *group*

Зберігаємо та закриваємо файл.

Підключення. Тепер для підключення до VPN можна просто вказати команді *openvpn* файл конфігурації клієнта:

sudo openvpn --config client1.ovpn

Ця команда встановлює підключення до VPN [7].

2.3 Практичні аспекти використання OpenVPN в корпоративному середовищі

Використання OpenVPN для персоналу віддаленого офісу

OpenVPN — це інструмент, відомий своєю потужністю та гнучкістю у створенні віртуальних приватних мереж (VPN), тому широко використовується в корпоративному світі як популярне рішення. Це забезпечує безпечне підключення до внутрішніх ресурсів компанії з будь-якої точки земної кулі, таким чином забезпечуючи доступ до активів компанії незалежно від місця розташування.

Однією з головних причин використання OpenVPN є захист даних. В Україні, як і в усьому світі, кіберзагрози стають все більш серйозними. Використання OpenVPN допомагає шифрувати всі дані, що передаються між віддаленими пристроями працівників та корпоративною мережею. Це знижує ризик перехоплення конфіденційної інформації, забезпечуючи її захист від несанкціонованого доступу. Для компаній, що працюють з чутливою інформацією, такою як фінансові дані або особисті дані клієнтів, ця функція є критично важливою.

OpenVPN забезпечує віддаленим працівникам зручний доступ до корпоративних ресурсів з будь-якого місця і в будь-який час. Це дозволяє співробітникам бути більш гнучкими та продуктивними, оскільки вони можуть виконувати свої обов'язки незалежно від свого місцезнаходження.

Використання OpenVPN дозволяє компаніям знизити витрати на забезпечення безпеки даних. Традиційні методи, такі як оренда виділених ліній зв'язку, можуть бути дорогими та складними в управлінні. OpenVPN використовує існуючу інфраструктуру Інтернету для створення захищених з'єднань, що значно знижує витрати на обладнання та обслуговування.

Використання OpenVPN забезпечує надійний контроль доступу до корпоративних ресурсів. Кожен користувач отримує унікальні ключі та сертифікати для аутентифікації, що унеможливлює доступ несанкціонованих осіб. Такий підхід є важливим для компаній, які прагнуть зберегти високу конфіденційність та безпеку своїх даних [5].

Переваги для українських комерційних та державних організацій

Для України важливість використання OpenVPN ще більш підкреслюється в контексті політичних та економічних викликів, які можуть впливати на стабільність діяльності. Захист даних стає критичним фактором для забезпечення безперебійної роботи організацій та збереження їхньої конкурентоспроможності на міжнародному ринку. Використання OpenVPN дозволяє українським організаціям оперативно адаптуватись до змін, забезпечуючи безпеку своїх інформаційних систем та підвищуючи ефективність роботи.

Українські урядові організації стикаються з численними кіберзагрозами, які можуть поставити під загрозу безпеку державних даних. Використання OpenVPN дозволяє шифрувати весь трафік між державними службовцями та центральними серверами, що значно ускладнює можливість перехоплення або зламу даних. Це особливо важливо для захисту конфіденційної інформації, такої як особисті дані громадян, фінансові документи та інші важливі державні інформаційні ресурси.

OpenVPN дозволяє державним службовцям безпечно працювати з будь-якого місця, забезпечуючи доступ до необхідних ресурсів та інформації. Це особливо важливо для працівників, які часто подорожують або працюють у віддалених регіонах України. Використання OpenVPN забезпечує надійний зв'язок між центральними урядовими офісами та віддаленими робочими місцями, підвищуючи ефективність та продуктивність роботи.

OpenVPN також може бути використаний для забезпечення безпечного обміну інформацією між українськими державними установами та міжнародними партнерами. Це дозволяє здійснювати ефективну співпрацю з іншими країнами, міжнародними організаціями та інститутами, забезпечуючи захист переданих даних. У контексті зростаючої ролі України на міжнародній арені, це є важливим аспектом забезпечення безпеки та довіри у відносинах з іншими державами.

Використання OpenVPN допомагає знизити ризик внутрішніх загроз, таких як витік інформації або несанкціонований доступ до державних ресурсів. Кожен користувач отримує унікальні ключі та сертифікати для аутентифікації, що дозволяє точно контролювати доступ до конфіденційної інформації. Це забезпечує

високий рівень безпеки та зменшує можливість зловживання доступом до інформації для службового використання даних.

Україна має велику кількість критичної інфраструктури, включаючи енергетичні, транспортні та комунікаційні мережі. Захист цієї інфраструктури є пріоритетним завданням для національної безпеки. Використання OpenVPN для захищеного доступу до систем управління та моніторингу цієї інфраструктури допомагає зменшити ризик кібератак і забезпечити стабільну роботу важливих об'єктів. Шифрування даних і надійна аутентифікація знижують вразливість до атак, які можуть порушити функціонування інфраструктурних об'єктів.

Уряд і бізнеси в Україні активно впроваджують цифрові послуги, такі як електронне урядування, онлайн-банкінг, та інші сервіси. Використання OpenVPN для захисту цих послуг допомагає підвищити рівень довіри серед громадян і клієнтів, оскільки вони будуть впевнені в безпеці своїх даних під час користування цифровими платформами. Це сприяє більш широкому прийняттю та використанню електронних послуг, що в свою чергу стимулює економічний розвиток.

В умовах зростаючої цифрової цензури та спостереження у світі, забезпечення приватності та свободи слова стає критично важливим. Використання OpenVPN дозволяє українським громадянам захищати свою приватність в Інтернеті, обходити обмеження доступу до інформації та зберігати свободу слова. Це є важливим аспектом для забезпечення демократичних цінностей та прав людини в країні.

Україна відома своїм активним стартап-середовищем і високим рівнем інновацій у сфері IT. Використання OpenVPN забезпечує безпеку даних для стартапів, дозволяючи їм зосередитися на розвитку своїх продуктів та послуг, не турбуючись про кіберзагрози. Це також дозволяє залучати інвестиції, оскільки інвестори цінують високий рівень безпеки даних.

Успішні кейси з використанням OpenVPN великими компаніями

GlobalTech, гігант із розробки програмного забезпечення, успішно інтегрував OpenVPN у свою систему, щоб гарантувати безпеку та підвищити продуктивність своїх розгалужених команд. Завдяки використанню OpenVPN компанії вдалося

запропонувати надійний і безпечний канал для співробітників, які перебувають у різних країнах, щоб легко отримати доступ до внутрішніх ресурсів — крок, який сприяв високому рівню продуктивності та захистив конфіденційні дані від потрапляння в чужі руки.

Softech — це глобальна технологічна компанія, яка надає різноманітні програмні рішення для аеропортів, метеорологічних, екологічних і транспортних організацій. Вперше заснована в 1991 році, компанія фактично контролює та вимірює все, що рухається, а також результує наслідки, включаючи шум, забруднення, трафік і багато іншого. Група Softech має сильну міжнародну присутність, провадячи діяльність від Мілана до Бангкока та від Джидди до Ріо-де-Жанейро.

Зважаючи на характер своєї роботи, співробітникам Softech потрібно було дистанційно підключатися до клієнтів через Інтернет — з упевненістю, що не буде проблем із підключенням або розриву з'єднання. Але, як пояснив власник: «Раніше, ми використовували модемне з'єднання, але воно було дуже повільним і мало багато проблем із безпекою та з'єднанням. Нам потрібен був кращий і міцніший зв'язок, щоб дозволити компанії розвиватися». Компанія не могла розвиватися так, як їм потрібно, доки дистанційне рішення залишало їх (та їхніх клієнтів) у безвихідному стані.

Компанії було потрібне нове рішення, яке дозволило б надавати оперативну підтримку своїм клієнтам — і їм потрібно було, щоб воно було надійним, доступним і простим у використанні.

Після пошуку рішення, яке могло б задовольнити їхні потреби як компанії, що розвивається, Softech знайшла OpenVPN, і їй сподобалося, що його так легко встановити та використовувати. За словами власника, OpenVPN вирішив багато проблем компаній, оскільки це рішення забезпечує швидке та надійне з'єднання та дозволило їм вирішити всі проблеми, з якими стикалися їхні клієнти, не змушуючи компанію витрачати багато грошей. Сервер доступу OpenVPN вирішив проблеми з підключенням і безпекою, дотримуючись бачення компанії про створення нових рішень і одночасно інтегруючи інноваційні сценарії в існуючі середовища [4].

OpenVPN є універсальним інструментом, який може бути використаний у різних сферах для забезпечення безпеки даних та ефективного управління віддаленими працівниками. В умовах сучасних викликів, таких як військовий стан, кіберзагрози, економічна нестабільність та необхідність адаптації до нових умов, використання OpenVPN стає критично важливим для захисту національної безпеки, підтримки інновацій та розвитку цифрової економіки в Україні.

РОЗДІЛ 3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ОПТИМІЗАЦІЇ ВИКОРИСТАННЯ OPENVPN ДЛЯ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ КОРПОРАТИВНИХ ДАНИХ

3.1 Найкращі практики безпеки та рекомендації щодо конфігурації OpenVPN

Конфігурація протоколів шифрування є одним із найважливіших аспектів забезпечення безпеки OpenVPN. Використання сучасних, надійних алгоритмів шифрування є ключовим для захисту даних, що передаються через VPN. Одним з найкращих варіантів є AES. AES-256, зокрема, є широко визнаним стандартом для сильного шифрування даних, що забезпечує високу стійкість до атак. Завдяки своїй надійності та швидкості, AES-256 широко використовується у багатьох безпекових додатках, включаючи VPN-сервіси.

Для захисту каналу керування варто використовувати TLS версії 1.2 або новішу. TLS забезпечує надійну аутентифікацію та захист даних під час встановлення з'єднання між OpenVPN клієнтом і сервером. Необхідно налаштувати OpenVPN для використання сильних шифрів та протоколів обміну ключами. Зокрема, ECDHE забезпечує надійний обмін ключами, дозволяючи створювати нові ключі для кожної сесії, що значно підвищує безпеку. Для хешування варто використовувати SHA-256 або новіші алгоритми, що гарантують високий рівень захисту від хеш-колізій.

HMAC є ще одним критично важливим компонентом безпеки. Використання HMAC з алгоритмом SHA-256 для аутентифікації повідомлень допомагає запобігти спробам модифікації даних під час передачі. HMAC забезпечує цілісність та автентичність повідомлень, що передаються через VPN, знижуючи ризики атак MITM.

Налаштування OpenVPN з використанням AES-256 для шифрування даних, TLS 1.2 або новішої версії для захисту каналу керування та HMAC з SHA-256 для аутентифікації повідомлень є оптимальним підходом для забезпечення високого рівня безпеки VPN-з'єднання.

Протоколи аутентифікації

В корпоративних мережах аутентифікація є одним із ключових аспектів забезпечення безпеки OpenVPN. Використання TLS для аутентифікації є стандартом, оскільки забезпечує надійний захист даних і підтвердження ідентичності як клієнтів, так і серверів. Взаємна аутентифікація TLS вимагає наявності сертифікатів у обох сторін з'єднання, що гарантує, що сервер аутентифікує клієнта, а клієнт - сервер. Це значно підвищує рівень безпеки, адже навіть якщо хтось зуміє викрасти сертифікат сервера, без клієнтського сертифіката він не зможе встановити з'єднання.

Використання сертифікатів X.509. Сертифікати X.509 видаються довіреним ЦС і містять унікальні криптографічні ключі, які підтверджують ідентичність користувачів. В корпоративних мережах можна налаштувати власний ЦС для видачі сертифікатів співробітникам і пристроям. Це дозволяє централізовано управляти сертифікатами, відкликати їх у разі компрометації та забезпечувати дотримання внутрішніх політик безпеки.

Примусова перевірка сертифікатів є ще одним важливим аспектом аутентифікації. В OpenVPN можна налаштувати параметри перевірки сертифікатів, такий як *«remote-cert-tls»*, що дозволяє примусово перевіряти тип сертифіката сервера. Це запобігає атакам з використанням неправдивих сертифікатів та гарантує, що з'єднання встановлюється тільки з довіреним сервером. Така перевірка допомагає уникнути підробок і забезпечує цілісність з'єднання.

Регулярне оновлення сертифікатів та ключів є необхідними діями для підтримання високого рівня безпеки. Сертифікати мають обмежений термін дії, і своєчасне їх оновлення запобігає використанню застарілих або скомпрометованих ключів. Постійне оновлення дозволяє також інтегрувати новітні алгоритми та технології безпеки, що підвищують загальний рівень захисту корпоративної мережі.

Багатофакторна автентифікація є ключовим елементом забезпечення безпеки в корпоративних мережах, які використовують OpenVPN. MFA додає додатковий рівень захисту, що значно ускладнює несанкціонований доступ до мережі. Основна ідея багатофакторної автентифікації полягає в тому, що для підтвердження особи

користувача необхідно надати два або більше незалежних фактори. Ці фактори можуть включати щось, що користувач знає (наприклад, пароль), щось, що він має (наприклад, мобільний пристрій для отримання одноразового коду) та біометричні дані (наприклад, відбиток пальця).

В корпоративних середовищах однією з найпоширеніших реалізацій MFA є комбінація паролю та одноразового коду (OTP), згенерованого спеціальним додатком, таким як Google Authenticator або отриманого через SMS. Ця комбінація значно підвищує рівень безпеки, оскільки навіть у разі викрадення пароля, зловмисник не зможе отримати доступ до системи без одноразового коду, який зазвичай має короткий термін дії і генерується динамічно.

Інтеграція багатофакторної автентифікації з OpenVPN вимагає налаштування спеціальних серверів аутентифікації, таких як RADIUS або використання протоколу LDAP. Ці сервери можуть бути налаштовані для роботи з різними методами MFA, забезпечуючи централізоване управління доступом та автентифікацією. Використання RADIUS-сервера дозволяє легко інтегрувати MFA з існуючою інфраструктурою безпеки підприємства, забезпечуючи гнучке управління політиками доступу. Ще одним ефективним методом є використання апаратних токенів або смарт-карт для аутентифікації. Ці пристрої генерують одноразові коди або містять цифрові сертифікати, які можуть бути використані для підтвердження особи користувача. Апаратні токени та смарт-карти надають додатковий рівень фізичної безпеки, оскільки їх важко підробити або викрасти в цифровому вигляді. Це робить їх особливо корисними для захисту критичних систем та даних в корпоративних мережах.

Для максимальної ефективності багатофакторної автентифікації важливо проводити регулярні навчання співробітників щодо використання MFA та загальних практик кібербезпеки. Користувачі повинні розуміти важливість збереження конфіденційності своїх облікових даних та дотримання встановлених політик безпеки. Регулярні навчання допомагають мінімізувати ризик людських помилок, які можуть призвести до компрометації мережі.

Обмеження доступу залежно від IP-адреси та часу

Одним з найбільш ефективних методів знизити ризики несанкціонованого доступу та забезпечити кращий контроль є налаштування доступу на основі IP-адреси. Це можна зробити за допомогою списків дозволених (whitelisting) та заборонених (blacklisting) IP-адрес. Списки дозволених IP-адрес обмежують доступ до VPN лише з визначених діапазонів IP, які належать, наприклад, до офісних приміщень компанії або певних регіонів. Це дозволяє значно знизити ймовірність несанкціонованого доступу з невідомих або потенційно небезпечних IP-адрес. Відповідно, списки заборонених IP-адрес можуть блокувати доступ з відомих джерел атак або небажаних регіонів.

Налаштування доступу на основі часу також є ефективним способом забезпечення безпеки. Це передбачає обмеження доступу до VPN лише в певні години або дні. Наприклад, можна дозволити доступ лише в робочі години, коли користувачі повинні бути підключені до корпоративної мережі. Це допомагає запобігти можливим атакам, які можуть бути здійснені поза робочим часом, коли спостереження за діяльністю користувачів є менш активним. Такий підхід також може бути корисним для обмеження доступу під час святкових днів або періодів, коли компанія не працює.

Для реалізації обмежень по IP-адресам та часу можна використовувати різні інструменти та технології. Наприклад, брандмауери можуть бути налаштовані для фільтрації трафіку на основі IP-адрес та часу. Використання правил *iptables* в Linux дозволяє детально налаштувати політики доступу, визначаючи дозволені або заборонені IP-адреси та часові інтервали. Крім того, OpenVPN підтримує використання скриптів і конфігураційних файлів для автоматизації цих налаштувань.

Логування та моніторинг підключень

Налаштування детального логування в OpenVPN є необхідним для забезпечення прозорості та можливості проведення аналізу подій. Логи повинні містити інформацію про кожне підключення, включаючи дату та час, IP-адресу користувача, який підключається, тривалість сесії та обсяг переданих даних. Така інформація дозволяє відстежувати активність користувачів, виявляти

невідповідності та аномалії, що можуть свідчити про спроби несанкціонованого доступу або інші загрози.

Для ефективного управління логами рекомендується використовувати централізовані системи збору та аналізу журналів, такі як Syslog або спеціалізовані рішення для управління журналами та подіями безпеки (SIEM). Ці системи дозволяють агрегувати логи з різних серверів OpenVPN, зберігати їх у безпечному місці та забезпечувати зручний доступ для аналізу. Централізоване управління логами також спрощує процеси відповідності вимогам регуляторних органів та внутрішніх політик безпеки.

Моніторинг підключень в режимі реального часу є ще одним важливим аспектом забезпечення безпеки. Використання інструментів для моніторингу мережевої активності дозволяє оперативно виявляти та реагувати на підозрілі дії. Наприклад, інтеграція моніторингу з системами виявлення вторгнень (IDS) або системами запобігання вторгнень (IPS) може забезпечити автоматичне виявлення аномалій та блокування підозрілих підключень. Це допомагає знизити ризик компрометації мережі та забезпечити її безперервну роботу.

Важливою складовою моніторингу є також регулярний аналіз зібраних логів. Адміністратори мережі повинні періодично переглядати журнали підключень, шукаючи ознаки підозрілої активності, такі як повторні невдалі спроби входу, підключення з невідомих IP-адрес або підозріло велика кількість даних, що передаються. Аналіз логів дозволяє виявляти потенційні загрози на ранніх стадіях та вживати відповідних заходів для їх своєчасної нейтралізації.

Крім того, варто налаштувати систему оповіщення про критичні події. Це можуть бути автоматичні сповіщення адміністраторам мережі про підозрілу активність або аномалії, що вимагають уваги та реакції. Оповіщення можуть надсилатися електронною поштою, через SMS або інші канали комунікації, що дозволяє швидко реагувати на загрози.

3.2 Рекомендовані стратегії щодо масштабування та адаптації VPN-інфраструктури під зростаючі потреби бізнесу

З розвитком бізнесу зростає його потреба у відповідному масштабуванні та адаптації інфраструктури віртуальної приватної мережі (VPN). VPN (віртуальна приватна мережа) є ключовим елементом для забезпечення безпечного доступу до корпоративних ресурсів через Інтернет. Зі зростанням кількості віддалених співробітників, підключених пристроїв та обсягів даних, компанії стають викликаними масштабуванням їх VPN-мереж.

Масштабування інфраструктури VPN включає в себе впровадження ряду стратегій, які забезпечують ефективну роботу мережі, підтримку високої продуктивності та забезпечення безпеки даних. Серед основних напрямків масштабування можна виділити горизонтальне та вертикальне масштабування, оптимізацію пропускної здатності мережі, інтеграцію з хмарними сервісами та впровадження нових технологій для підвищення продуктивності.

Масштабування в горизонтальному та вертикальному напрямках.

Розширення кількості серверів та підключень є основною стратегією масштабування інфраструктури OpenVPN. Додавання нових серверів і збільшення кількості можливих з'єднань допоможе задовольнити зростаючі бізнес-потреби. Це дозволить розподілити навантаження в мережі та забезпечити постійний доступ до корпоративних ресурсів для всіх користувачів.

Горизонтальне масштабування передбачає додавання нових серверів або пристроїв до існуючої інфраструктури. Це дозволить розподілити навантаження та підвищити загальну пропускну здатність мережі. Використання цієї стратегії допоможе уникнути перевантаження окремих мережевих вузлів та забезпечить стійкість до відмов.

Вертикальне масштабування полягає у підвищенні продуктивності існуючих серверів за допомогою додавання потужнішого обладнання або збільшення обсягу пам'яті. Це може бути доцільним у випадках, коли збільшення кількості серверів є економічно недоцільним або технічно складним. Вертикальне масштабування

дозволить збільшити продуктивність без значного розширення фізичної інфраструктури.

Переваги розширення серверів:

Додавання нових серверів OpenVPN дозволяє рівномірно розподілити завантаження між усіма наявними серверами. Це зменшує ризик перевантаження окремих вузлів і підвищить загальну продуктивність мережі. Більша кількість серверів підвищить стійкість до помилок у мережі: у разі відмови одного сервера, навантаження може бути автоматично перенаправлене на інші.

Можливість додавання нових серверів забезпечить гнучкість у реагуванні на зростаючі потреби бізнесу. Це дозволить швидко масштабувати мережі відповідно до збільшення кількості користувачів або обсягу трафіку. Завдяки цьому ви зможете підтримувати високий рівень обслуговування та забезпечувати безперебійний доступ до необхідних ресурсів [8].

Технічні аспекти

При розширенні інфраструктури сервера, обирайте обладнання, яке відповідає вимогам до продуктивності та надійності. Важливо використовувати сервери з достатньою обчислювальною потужністю, пам'яттю та дисковим простором, щоб забезпечити стабільну роботу мережі.

Інтегруйте нові сервери OpenVPN з існуючою інфраструктурою. Налаштування мережевих конфігурацій та встановлення необхідного програмного забезпечення забезпечить сумісність з існуючими протоколами безпеки. Це допоможе уникнути конфліктів і забезпечить безперебійну роботу всієї системи.

Впроваджуйте механізми балансування навантаження для автоматичного розподілу трафіку між усіма доступними серверами. Використовуйте спеціалізоване програмне забезпечення, таке як HAProxy або NGINX, для реалізації цієї функції. Це дозволить ефективно розподілити навантаження, покращити продуктивність мережі та забезпечити надійність доступу до ресурсів [8].

Використання балансування навантаження

Балансування навантаження є критично важливим елементом масштабування інфраструктури VPN, особливо на основі OpenVPN. Це дозволяє розподіляти

трафік між ключовими серверами, забезпечуючи високу продуктивність, стабільність і стійкість мережі до відмов.

Для забезпечення ефективного використання ресурсів та покращення якості обслуговування користувачів, особливо в умовах збільшення навантаження в мережі, використовуйте балансування навантаження. Розподіл трафіку між кількома серверами зменшить ризик перенавантаження окремих вузлів, що забезпечить стабільну та високу продуктивність мережі. У разі відмови одного з серверів, механізм балансування автоматично перенаправить трафік на інші доступні сервери, забезпечуючи безперебійну роботу мережі.

Рекомендовані рішення для балансування навантаження:

- HAProxy: Надійний та високопродуктивний балансувальник завантажень, який забезпечує розподіл трафіку на рівнях HTTP та TCP. Використовуйте HAProxy для балансування навантаження в інфраструктурі OpenVPN.
- NGINX: Потужний веб-сервер, який також може виступати як балансувальник навантаження. NGINX підтримує різні алгоритми балансування та надає гнучкі налаштування.

Методи балансування навантажень:

- Round Robin: Розподіл трафіку між усіма доступними серверами по черзі.
- Least Connections: Трафік направляється на сервер з найменшою кількістю активних підключень.
- IP Hash: Забезпечення стабільності з'єднання з конкретним сервером шляхом розподілу трафіку на основі хешування IP-адреси клієнта.

Використовуйте системи моніторингу, такі як Zabbix або Prometheus, для відстеження стану серверів та швидкої реакції на зміни навантаження. Це гарантує високу доступність і продуктивність мережі. Важливо також забезпечити сумісність балансувальників завантаження з існуючою інфраструктурою OpenVPN та протестувати налаштування перед розгортанням у виробничому середовищі.

Впровадження балансування навантаження може бути технічно складним процесом, який вимагає ретельного планування та конфігурації мережевої інфраструктури. Використовуйте звітну документацію та залучайте досвідчених

спеціалістів для вирішення цього питання. Балансування навантаження повинно відповідати вимогам мережевої безпеки, включаючи захист від DDoS-атак, налаштування шифрування трафіку та використання багатофакторної аутентифікації [8].

Оптимізація пропускної здатності мережі.

Для забезпечення зручного використання мережевих ресурсів віддаленими співробітниками, зосередьтеся на зниженні затримок і підвищенні швидкості підключення. Оптимізований VPN дозволить співробітникам виконувати завдання більш ефективно без затримок або перебоїв. Ефективна оптимізація також допоможе зменшити навантаження на сервери, підвищуючи надійність і стійкість мережі.

Оптимізація пропускної здатності мережі

- Застосовуйте QoS для пріоритезації трафіку, що дозволить важливим даним передаватися швидше.
- Використовуйте стиснення даних для зменшення обсягу переданих даних, що підвищить швидкість підключення.
- Переглядайте та оптимізуйте маршрути передачі даних для мінімізації затримок.

Замість TCP, обирайте UDP у файлах конфігурації OpenVPN. UDP швидший за TCP, оскільки не потребує підтвердження отримання кожного пакета, що зменшує затримку і покращує швидкість підключення.

Використовуйте компресію трафіку для зменшення обсягу переданих даних. OpenVPN підтримує компресію LZO, що може підвищити швидкість підключення. Проте врахуйте, що компресія може збільшити навантаження на процесор.

Використання менш ресурсоємних алгоритмів шифрування: Обирайте сучасні алгоритми, такі як AES-256-GCM, для підвищення продуктивності без значних втрат у безпеці.

Процесори з підтримкою апаратного прискорення шифрування: Використовуйте процесори, що підтримують апаратне прискорення шифрування (наприклад, Intel AES-NI), щоб зменшити навантаження на сервери.

Виберіть оптимальний розмір MTU для підключення OpenVPN. Це допоможе зменшити кількість фрагментованих пакетів, підвищуючи ефективність передачі даних.

Впровадження цих рекомендацій забезпечить стабільну роботу інфраструктури VPN, покращить продуктивність мережі та задовольнить потреби віддалених співробітників у швидкому та надійному доступі до корпоративних ресурсів..

Інтеграція з хмарними сервісами.

Використання хмарних технологій надає додаткові можливості для масштабування інфраструктури VPN. Інтеграція інфраструктури OpenVPN з хмарними сервісами дозволяє динамічно збільшувати мережеві ресурси відповідно до потреб бізнесу, забезпечуючи гнучкість і зменшуючи витрати на обслуговування власного обладнання.

Переваги інтеграції інфраструктури OpenVPN з хмарними сервісами:

- Використовуйте хмарні технології для динамічного масштабування мережевих ресурсів відповідно до змін у навантаженні. Це дозволить швидко адаптувати інфраструктуру до зростаючих потреб бізнесу.
- Використання хмарних ресурсів зменшує витрати на обслуговування та оновлення власного обладнання, оскільки ви оплачуєте тільки за використані ресурси.
- Хмарні сервіси дозволяють швидко регулювати зміни навантаження, забезпечуючи надійний доступ до корпоративних ресурсів для всіх користувачів.

Використання хмарних технологій допоможе вашому бізнесу ефективно реагувати на зміни у навантаженні та забезпечити стабільну та безперебійну роботу інфраструктури VPN. Інтеграція хмарних рішень з інфраструктурою OpenVPN також сприяє підвищенню загальної продуктивності та надійності мережі, дозволяючи зосередитися на основних бізнес-завданнях без зайвих турбот про технічну інфраструктуру.

ВИСНОВОК

В роботі було подано результати дослідження та розроблено рекомендації щодо використання віртуальних приватних мереж для забезпечення віддаленого доступу до корпоративних даних на базі рішення OpenVPN.

У результаті було здійснено:

1. Аналіз теоретичних аспектів віртуальних приватних мереж (VPN). Визначено та класифіковано віртуальні приватні мережі, які поділяються на кілька основних типів: віддалений доступ, сайт-до-сайт та інші. Розглянуто їхні особливості та застосування в різних корпоративних середовищах.
2. Вивчено принципи роботи та архітектуру VPN на базі OpenVPN. Показано, що OpenVPN забезпечує високий рівень безпеки завдяки використанню шифрування SSL/TLS, підтримці різних методів аутентифікації та можливості налаштування для різних сценаріїв використання.
3. Проаналізовано загрози та виклики безпеки при використанні VPN, такі як потенційні вразливості до атак типу MITM, злом криптографічних ключів та інші. Виявлено, що належна конфігурація та регулярне оновлення програмного забезпечення є критичними для підтримання високого рівня безпеки.
4. Досліджено можливості OpenVPN у забезпеченні віддаленого доступу до корпоративних даних. Розглянуто конфігурацію та налаштування серверу OpenVPN. Показано, що налаштування сервера включає створення сертифікатів, налаштування параметрів шифрування, а також конфігурацію мережевих інтерфейсів та правил доступу.
5. Вивчено налаштування OpenVPN клієнтів для підключення до VPN. Розроблено інструкції для різних операційних систем, включаючи Windows, macOS, Linux та мобільні платформи, що забезпечує гнучкість та універсальність рішення.

6. Проаналізовано практичні аспекти використання OpenVPN в корпоративному середовищі. Виявлено, що OpenVPN забезпечує надійне та захищене з'єднання навіть у складних мережевих умовах, а також легко інтегрується з існуючими мережевими інфраструктурами.
7. Розроблено рекомендації щодо оптимізації використання OpenVPN для підвищення рівня безпеки корпоративних даних. Виокремлено найкращі практики конфігурації та безпеки OpenVPN. Рекомендовано використовувати сильні методи шифрування, такі як AES-256, налаштовувати багатофакторну аутентифікацію, а також забезпечувати регулярне оновлення програмного забезпечення для захисту від нових загроз.
8. Розглянуто стратегії масштабування та адаптації VPN-інфраструктури під зростаючі потреби бізнесу. Запропоновано методи оптимізації продуктивності VPN-серверів, забезпечення високої доступності та відмовостійкості системи, а також інтеграції з іншими мережевими службами для забезпечення безперебійної роботи.

OpenVPN доцільно використовувати як основний засіб для забезпечення віддаленого доступу до корпоративних даних завдяки його гнучкості, надійності та можливості адаптації до специфічних потреб організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Що таке VPN? URL: https://nordvpn.com/uk/what-is-a-vpn/ (дата звернення: 10.05.2024)

2. Найкращі протоколи VPN та відмінності між типами VPN. URL: https://nordvpn.com/uk/blog/protokoly/
(дата звернення: 10.05.2024).

3. Типи VPN-з'єднань в Keenetic. URL: https://keenetic.biz/tipi-vpn-ziednan-v-keenetic/
(дата звернення: 10.05.2024).

4. OpenVPN. Case Study: Softech URL: https://openvpn.net/case-study/softech/
(дата звернення: 18.05.2024).

5. Securing Remote Access Using VPN URL: https://openvpn.net/whitepaper/
(дата звернення: 18.05.2024)

6. Use-cases for the OpenVPN Access Server product URL: https://openvpn.net/vpn-server-resources/use-cases-for-the-openvpn-access-server-product/
(дата звернення: 18.05.2024).

7. Установка и настройка сервера OpenVPN в Ubuntu 20.04 URL: https://www.digitalocean.com/community/tutorials/how-to-set-up-and-configure-an-openvpn-server-on-ubuntu-20-04-ru#13
(дата звернення: 20.05.2024).

8. Масштабованість хмари: горизонтальне та вертикальне масштабування IT-інфраструктур URL: https://cases.media/en/article/masshtabovanist-khmari-gorizontalne-ta-vertikalne-masshtabuvannya-it-infrastruktur
(дата звернення: 20.05.2024).

9. What Is a Man-in-the-Middle Attack? Definition, Detection, and Prevention Best Practices for 2022 URL: https://www.spiceworks.com/it-security/data-security/articles/man-in-the-middle-attack/ (дата звернення: 20.05.2024).

ДЕМОНСТРАЦІЙНИЙ МАТЕРІАЛ (Презентація)