ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИКОРИСТАННЯ OPENVPN ДЛЯ ЗАХИСТУ ПЕРЕДАЧІ ІНФОРМАЦІЇ В ЛОКАЛЬНІЙ МЕРЕЖІ»

Виконав студент 4 курсу, групи БСД-42
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»

(шифр і назва спеціальності)

Кліменченко В.С.

(прізвище та ініціали)

Керівник Довженко Н.М.

(прізвище та ініціали)

Рецензент

(прізвище та ініціали)

Нормоконтролер Чумак Н.С.

(прізвище та ініціали)

КИЇВ – 2023

ВСТУП

Актуальність дослідження. Маючи сьогодні понад мільярд користувачів, Інтернет став каналом, через який люди та компанії регулярно отримують доступ до корисної інформації, виконують такі завдання, як банківські операції та здійснюють покупки в різних торгових точках. Поява соціальних мереж також зробила Інтернет цінним майданчиком для бізнесу та інших організацій, де вони можуть здійснювати важливий брендинг та інші важливі взаємодії з клієнтами, часто приносячи при цьому значні прибутки. Однак, незважаючи на цю зручність, існує вразливість до збоїв.

Основним напрямком діяльності OpenVPN завжди був бізнес-бізнес (B2B), і перший продукт, який два засновники запустили разом, був розроблений як корпоративне рішення - Access Server. Цей інструмент дозволяє компаніям будь-якого розміру отримати доступ до безлічі функцій корпоративного рівня і є альтернативою складним апаратним системам, які є дорогими в обслуговуванні. OpenVPN Access Server - це високомасштабована і гнучка віртуальна приватна мережа (VPN), яка використовується для Сервер доступу OpenVPN - це високомасштабована і гнучка віртуальна приватна мережа (VPN), яка використовується для запуску передової платформи, що надає користувачам безпечні додатки. Інтуїтивно зрозуміла програмна платформа OpenVPN дозволяє співробітникам, філіям, постачальникам або клієнтам безпечно і легко отримувати віддалений доступ до спільних даних, таких як мережеві папки файлів і клієнт-серверні програми.

У 2020 році OpenVPN Inc. в черговий раз змінила ландшафт кібербезпеки, випустивши OpenVPN Cloud, перше рішення OpenVPN як послугу. Це рішення нового покоління для приватних мереж усуває необхідність встановлення VPN-сервера і дозволяє користувачам просто підключитися до хостингу, розташованого в будь-якій точці світу. Ця керована послуга забезпечує безпечну мережу між приватною мережею і віддаленими користувачами у вигляді «приватної мережі в

хмарі», що робить мережеву безпеку значно доступнішою, практичнішою і масштабованішою для підприємств будь-якого розміру. Не потребуючи капіталовкладень або робочого часу для управління, масштабування та розміщення VPN-серверів, а також завдяки набору функцій безпеки, доступних через онлайн-панель управління, компанії можуть легко контролювати свою мережу, дані та користувачів.

Ці інструменти стають все більш важливими, оскільки бізнес все більше покладається на цифрові дані; компанія Market Research Future повідомила у 2017 році, що світовий ринок VPN досягне 106 мільярдів доларів США до 2022 року. Висвітлення витоків даних у ЗМІ привернуло увагу до безпеки бізнесу та мереж, підвищивши обізнаність про необхідність кращого контролю доступу та захисту даних. Організації розуміють важливість використання VPN як частини загальної стратегії мережевої безпеки.

Організаціям необхідно впевнено використовувати онлайн-ресурси для підвищення ефективності та розвитку свого бізнесу. Свобода інформації, можливості для розвитку та безпечний, надійний доступ до Інтернету є важливими як для організацій, так і для приватних осіб. Ми завжди будемо рухатися вперед, намагаючись забезпечити цей вид безпеки за допомогою продуктів і послуг, які надають безпечний доступ до інформації: безпечне з'єднання з вашим світом.

Об’єкт дослідження – безпечне функціонування мережі з використанням технології тунелювання OpenVPN Server.

Предмет дослідження – методи захисту мережі пов’язані із використанням технології VPN для безпечного онлайн-зв’язку та передачі даних.

Мета роботи – розробка рекомендацій щодо підвищення захисту функціонування мережі з використанням технології OpenVPN.

Завдання бакалаврської роботи:

– проаналізувати структуру незахищених мереж та розробити вимоги до їх захисту;

– дослідити концепції та конфігурації для створення захищеної мережі VPN;

– розробити рекомендації щодо захисту локальної мережі з використанням технології OpenVPN.

Методи дослідження – опрацювання технічної літератури за даною темою, аналіз експлуатаційної документації інструментів, проведення тестування інструментів, аналіз сервісів.

Практичне значення одержаних результатів: рекомендації щодо застосування сервісів VPN можуть бути використані у сфері забезпечення кібербезпеки у персональних та корпоративних інформаційних системах.

1 АНАЛІЗ СТРУКТУРИ НЕЗАХИЩЕНИХ МЕРЕЖ ТА РОЗРОБКА ВИМОГ ДО ЗАХИСТУ

1.1 Визначення структури та основних характеристик незахищених мереж

Перш ніж будувати систему захисту , необхідно розробити та проаналізувати модель системи, яку потрібно захистити, щоб виділити її основні характеристики та загрози, які вона може реалізувати [1, 2].

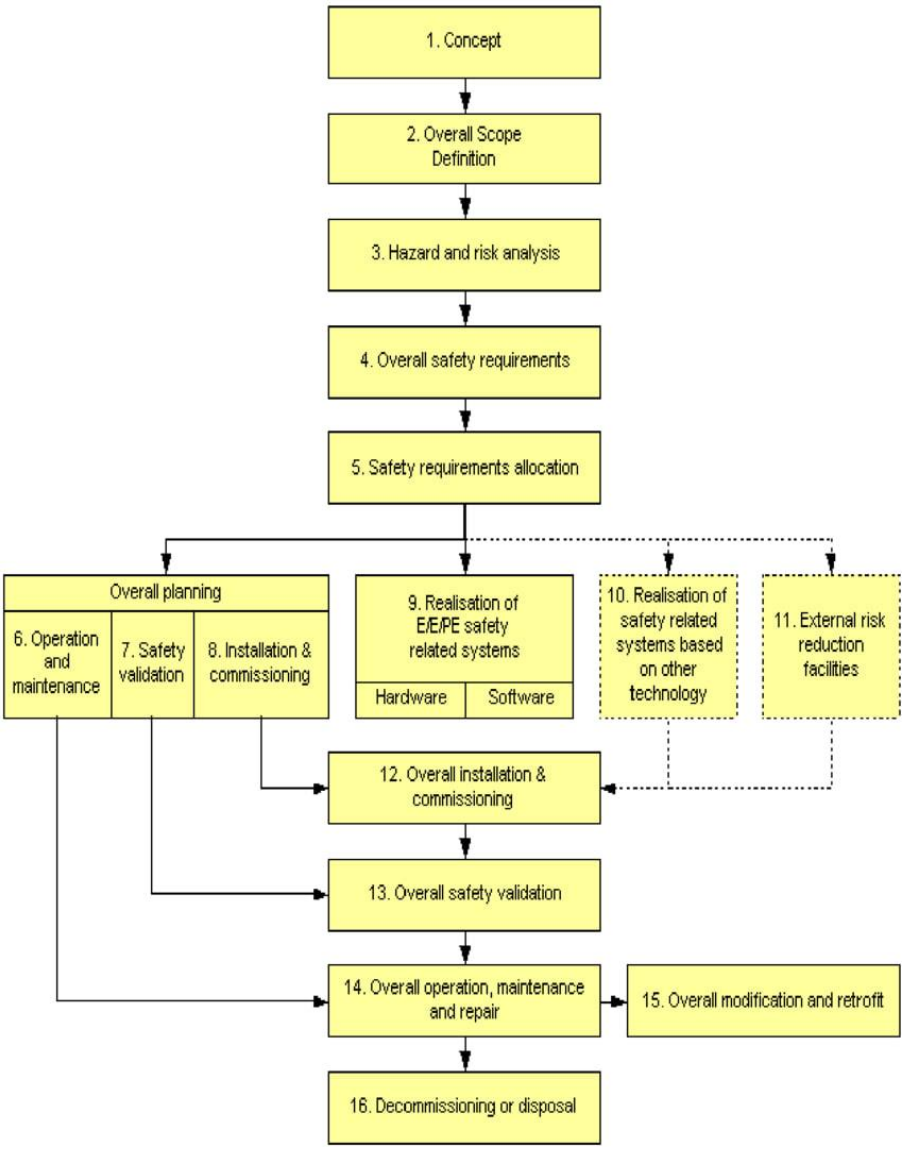

Рис. 1.1. Принципова схема незахищеної автоматизованої системи

Інформація про вихідну схему мережі [3]:

- адреси в локальній мережі є приватними;
- навході в локальну мережу знаходиться комп'ютер PROXY з реальною адресою;
- може існувати будь-яка кількість локальних мереж.

Може існувати будь-яка кількість мобільних користувачів, підключених до відкритого Інтернету.

До незахищених мереж належать комп'ютерні мережі, в яких відсутні достатні заходи безпеки для запобігання несанкціонованому доступу, крадіжці даних або іншим зловмисним діям. Ці мережі вразливі для різних типів кібератак, які можуть призвести до втрати даних, простою системи, фінансових втрат та репутаційної шкоди [2, 3, 5].

До основних характеристик незахищених мереж належать:

1. Відсутність автентифікації: у незахищених мережах часто відсутні належні механізми автентифікації, такі як надійні паролі або багатофакторна автентифікація, які можуть спростити зловмисникам доступ до конфіденційної інформації.

2. Слабке шифрування. Шифрування є важливим компонентом мережевої безпеки, оскільки воно захищає дані від перехоплення та читання неавторизованими сторонами. Незахищені мережі можуть використовувати слабкі методи шифрування або взагалі не використовувати шифрування, що робить дані вразливими для перехоплення та крадіжки.

3. Застаріле програмне забезпечення. У незахищених мережах може використовуватися застаріле програмне та апаратне забезпечення, яке може мати відомі вразливості в системі безпеки, які можуть використовувати хакери для отримання доступу до мережі.

4. Відсутність брандмауерів. Брандмауери — це пристрої, які відстежують та контролюють мережевий трафік, запобігаючи несанкціонованому доступу до мережі. У незахищених мережах можуть бути брандмауери, що полегшує зловмисникам проникнення в мережу.

5.Відсутність політик безпеки: у незахищених мережах може не бути чітко визначених політик або процедур безпеки, що ускладнює розуміння користувачами того, як належним чином захистити мережу та захистити конфіденційні дані [4].

В цілому, незахищені мережі вразливі для широкого спектру кіберзагроз, включаючи шкідливе програмне забезпечення, фішингові атаки, атаки типу «відмова в обслуговуванні» та багато інших. Для організацій дуже важливо робити кроки для захисту своїх мереж, впроваджуючи суворі заходи безпеки і регулярно відстежуючи та оновлюючи свої протоколи безпеки, щоб випереджати загрози, що виникають.

1.2 Ідентифікація та аналіз основних загроз безпеці системи

Існує безліч загроз безпеці системи, та їх ідентифікація має вирішальне значення для запобігання заподіянню ними шкоди. Ось деякі з основних загроз безпеки системи [5, 8]:

1. Шкідливе ПЗ: Шкідливе ПЗ — це скорочення від шкідливого програмного забезпечення, яке є програмним забезпеченням, призначеним для заподіяння шкоди комп'ютерній системі, мережі або користувачу. Це можуть бути віруси, черв'яки, трояни, шпигунське або рекламне програмне забезпечення. Шкідливе програмне забезпечення може потрапити в систему різними способами, включаючи вкладення електронної пошти, завантаження з ненадійних джерел або навіть фізичні носії, такі як USB-накопичувачі.

2. Соціальна інженерія. Соціальна інженерія — це тактика, яку використовують кіберзлочинці, щоб обманним шляхом змусити людей розголошувати конфіденційну інформацію, наприклад паролі або фінансову інформацію. Методи соціальної інженерії можуть набувати різних форм, включаючи фішинг, прийменник, приманку та послугу за послугу.

3. Атаки типу «відмова в обслуговуванні» (DoS): атаки типу «відмова в обслуговуванні» призначені для того, щоб зробити систему недоступною, перевантаживши її трафіком, що призведе до її збою або зависання. Ці атаки

можуть бути запущені з використанням різних методів, включаючи заповнення системи запитами або використання вразливостей програмного забезпечення системи.

4. Атаки «людина посередині» (MitM): атаки MitM включають перехоплення повідомлень між двома сторонами, що дозволяє зловмиснику підслуховувати, маніпулювати або навіть вставляти шкідливий код повідомлення.Ці атаки можуть бути особливо небезпечними у ситуаціях, коли передається конфіденційна інформація, така як фінансові транзакції або облікові дані для входу.

5. Атаки на паролі. Атаки на паролі включають спроби отримати доступ до системи шляхом підбору або злому паролів. Ці атаки можуть набувати різних форм, включаючи атаки методом повного перебору, атаки за словником та атаки по райдужних таблицях.

6. Внутрішні небезпеки. Внутрішні загрози – це ризики безпеки, які виходять із організації. Сюди можуть входити співробітники, які навмисно чи ненавмисно завдають шкоди системі, наприклад, шляхом крадіжки даних чи впровадження шкідливого ПЗ.

7. Загрози фізичної безпеки. До загроз фізичної безпеки належать будь-які загрози фізичного характеру, такі як крадіжка, вандалізм чи стихійні лиха. Ці загрози можуть призвести до втрати важливих даних, пошкодження обладнання або навіть загибелі людей.

Щоб зменшити ці загрози, важливо впровадити комплексний план забезпечення безпеки, що включає такі заходи, як надійні протоколи автентифікації, регулярні оновлення програмного забезпечення та навчання співробітників передовим методам безпеки. Також важливо регулярно відстежувати системи на наявність будь-яких ознак підозрілої активності та план швидкого реагування на будь-які інциденти безпеки [8, 9, 12].

Популярність IP-технології зумовлена її об'єктивними перевагами, серед яких не останнє місце посідає відносна простота базових принципів IP-технології. Одним з таких принципів є відкритість, що знаходить своє відображення у вільному обговоренні, дослідженні та тестуванні нових протоколів TCP/IP

світовою спільнотою, а також Робочою групою з розробки Інтернет-технологій (IETF).

Стандарти і специфікації, що розробляються і пропонуються, доступні практично всім користувачам Інтернету. Будучи відкритою технологією, вона дозволяє відносно легко інтегрувати інші технології в IP-мережі, що значно розширює спектр інтернет-додатків. Ще однією перевагою IP-технології є її масштабованість, яка вже була закладена при проектуванні Інтернету. Ієрархічно структурований стек TCP/IP дозволяє організаціям розширювати свої мережі до досить великих масштабів. Завдяки цим перевагам IP-технологія [12, 14] широко використовується і сьогодні.

Технологія, яка забезпечила успіх Інтернету, також виявилася дуже перспективною для інтрамереж, внутрішніх мереж організацій. Інтранет, або внутрішня мережа, - це мережа рівня підприємства, що використовує програмне забезпечення, засноване на стеку протоколів TCP/IP.

Екстранет - це інтрамережа, підключена до Інтернету, яка є мережею типу інтрамережі, але дозволяє доступ до ресурсів певним категоріям користувачів з відповідними дозволами. Для подальшого розгляду заходів захисту всі мережі представляються як локальні мережі, підключені до Інтернету [11].

У цьому випадку не має значення, чи використовуються в цій мережі веб-технології, тому такі мережі називаються тут корпоративними мережами.

Глобальність, масштабність і гетерогенність, які є основними характеристиками корпоративних мереж, також підвищують ризики для виконання їх функціональних завдань: сімейство протоколів TCP/IP розроблялося давно, коли питання безпеки не стояли так гостро, як зараз, і тому було, в першу чергу, функціональним і легко переносимим Вони розроблялися як функціональні та легко переносимі, що в першу чергу сприяло популяризації стеку TCP/IP на безлічі комп'ютерних платформ. Широке розповсюдження Інтернету також надало зловмисникам багато засобів і методів для проникнення в корпоративні мережі.

Оскільки кількість хостів, підключених до Інтернету, надзвичайно зросла, а кількість компаній, що ведуть бізнес з використанням Інтернет-технологій,

збільшилася, кількість інцидентів інформаційної безпеки (ІБ) також значно зросла Згідно з даними групи реагування на комп'ютерні надзвичайні ситуації (Computer Emergency Response Team, CERT), за останні два роки в світі було зафіксовано

Згідно з даними CERT (Computer Emergency Response Team), кількість виявлених вразливостей та повідомлень про інциденти невпинно зростає. Вразливості в інформаційних системах - це будь-яка характеристика, яка може бути використана зловмисником для здійснення загрози. Загроза інформаційній системі - це будь-яка подія, поведінка, процес або явище, що має потенціал завдати шкоди (матеріальної, психологічної або іншої) ресурсам системи. На сьогоднішній день відома велика кількість різноманітних загроз, що походять з різних джерел і несуть різну небезпеку для інформації [4, 7, 17]. Системна класифікація загроз наведена в таблиці 1.1.

Тип загрози є основоположним параметром, що визначає обсяг захисту інформації. Випадковість - це розуміння походження загроз, викликаних спонтанними ситуаціями, які не залежать від волі людини в процесі функціонування системи обробки даних. Найбільш відомими подіями є збої, несправності, помилки, стихійні лиха та побічні ефекти. - Відмова - це порушення працездатності елемента системи, що призводить до його нездатності виконувати свої основні функції.

Таблиця1.1.

Системна класифікація загрози

Параметри класифікації	Значення параметрів	Зміст значення
Види загрози	- Фізична цілісність - Логічна структура - Зміст - Конфіденційність - Право власності	1. Знищення (спотворення), 2. Спотворення структури, 3. Несанкціонована модифікація, 4. Несанкціоноване отримання, 5. Витік інформації, 6. Присвоєння чужої праці.
Походження загроз	- Випадковий - Навмисний	1. Відмови, 2. Збої, 3. Помилки, 4. Стихійні лиха, 5. Побічні впливи, 6. Зловмисні дії людей.
Передумови появи загрози	- Об'єктивне - Суб'єктивне	1. Кількісна та якісна недостатність елементів системи, 2. Промисловий шпигунство, 3. Недобросовісні співробітники, 4. Кримінальні та хуліганствуючі елементи, 5. Служби інших держав.
Джерела в небезпеці	- Люди - Технічні пристрої - Моделі - Алгоритми - Програми - Технічні схеми обробки - даних - Зовнішнє середовище	1. Користувачі, 2. Персонал, 3. Реєстрації, 4. Введення, 5. Обробки, 6. Зберігання, 7. Передачі та видачі 8. Загального призначення, 9. Прикладні, 10.Інтерактивні, 12. Внутрішньомашинні, 13. Мережеві.

- Відмова - тимчасова несправність елемента системи, яка може призвести до того, що його функція в цей час не виконується належним чином.

- Помилка - специфічний (постійний або тимчасовий) стан елемента, який не дозволяє йому правильно виконувати одну або декілька функцій (одинично або систематично).

- Ефект пульсації - негативний вплив на систему в цілому або її окремі елементи, спричинений якимось явищем, що відбувається всередині системи або в зовнішньому середовищі.

Навмисна генерація загроз - спричинена зловмисними діями людей з метою реалізації одного або декількох видів загроз. Передумови виникнення загроз бувають двох типів: об'єктивні (кількісний або якісний дефіцит елементів системи) і суб'єктивні (діяльність іноземних спецслужб, промислове шпигунство, діяльність кримінальних або хуліганських елементів, зловмисні дії корумпованих співробітників системи). Перераховані типи передумов інтерпретуються наступним чином

- Кількісні недоліки: фізичні дефекти одного або декількох елементів системи обробки даних, що призводять [14] до переривання обробки та/або перевантаження наявних елементів.

- Якісні недоліки - конструктивні (організаційні) недоліки елементів системи, які можуть мати ненавмисний або навмисний негативний вплив на інформацію, що обробляється або зберігається.

- Зовнішня розвідувальна діяльність - спеціально організована діяльність органів державної влади, професійно спрямована на отримання необхідної інформації всіма засобами і методами.

- Промислове шпигунство - негласна діяльність організацій (та їхніх представників), спрямована на отримання інформації, спеціально захищеної від несанкціонованого розголошення або розкрадання, та створення сприятливих для себе умов з метою отримання максимальної вигоди.

- Злочинна або хуліганська поведінка - крадіжка інформації або комп'ютерних програм з метою отримання прибутку або знищення їх на користь конкурентів.

- Зловмисні дії недобросовісних працівників - викрадення (копіювання) і знищення масивів даних і програм з егоїстичних або корисливих мотивів. Джерелами загроз є люди, технічні пристрої, програми, алгоритми, технічні схеми обробки даних і зовнішнє середовище [3, 19].

- Люди - співробітники, користувачі та сторонні особи, які можуть віддалено маніпулювати ресурсами та даними організації безпосередньо зі своїх робочих місць або через мережі.

- Технічні засоби - ті, що безпосередньо пов'язані з обробкою, зберіганням і передачею інформації (наприклад, реєстратори даних, засоби введення), а також ті, що їх підтримують (наприклад, електропостачання, кондиціонери).

- Моделі, алгоритми і програми - ця групаЗацікавленою стороною, яка здійснює несанкціонований доступ до інформації, може бути як держава, так і юридична особа, група осіб (у тому числі громадські організації) або окрема фізична особа.

Здобуття захищеної інформації розвідувальними органами може здійснюватися за допомогою технічних засобів (технічна розвідка) або негласно (агентурна розвідка).

Канал витоку інформації - це сукупність джерел інформації, матеріального носія або середовища поширення сигналів, що несуть інформацію, і засобів зняття інформації з сигналів або середовища [2, 3]. Однією з основних характеристик каналу є розташування засобів зняття інформації з сигналу або носія, які можуть знаходитися в межах або за межами зони контролю, що охоплює систему. Надалі будуть розглядатися тільки загрози, пов'язані зі з'єднанням.

Аналіз загроз і аналіз ризиків є важливими компонентами ефективної стратегії кібербезпеки. Як і аналіз загроз, аналіз ризиків спрямований на виявлення ризиків і проблем безпеки, з якими стикається організація.

Різниця полягає в тому, що аналіз ризиків заглиблюється в основні процеси і системи для виявлення проблем безпеки, тоді як аналіз загроз визначає загрози на основі проблем безпеки в міру їх виникнення в режимі реального часу. Оцінка ризиків, з іншого боку, забезпечує більш повне охоплення внутрішніх служб, додатків, політик і процедур, які впливають на вразливості організації. Наприклад, замість того, щоб чекати на оцінку організованих атак на інструменти безпеки, аналіз ризиків може зазирнути всередину інструментів безпеки, щоб переконатися, що вони працюють належним чином (більш проактивний підхід порівняно з аналізом загроз).

1.3 Виявлення та аналіз основних типів мережевих атак на систему

Мережеві атаки – це тип кібератаки, націленої на комп'ютерні мережі з метою отримання несанкціонованого доступу, порушення роботи мережі, крадіжки конфіденційної інформації або запуску інших шкідливих дій. Ці атаки можуть бути націлені на будь-яку мережу, включаючи корпоративні мережі, загальнодоступні мережі та навіть особисті мережі. У цій статті ми обговоримо основні типи мережевих атак та принципи їхньої роботи [14, 17, 19, 21].

1. Атаки типу «відмова в обслуговуванні» (DoS): Атака типу «відмова в обслуговуванні» - це тип атаки, націленої на мережу або систему з потоком трафіку або запитів, що робить її недоступною для законних користувачів. Зловмисники можуть використовувати різні методи запуску DoS-атаки, такі як повінь мережі трафіком, використання вразливостей у мережевих пристроях або переповнення мережевих ресурсів. DoS-атаки можуть виконуватись одним зловмисником або групою зловмисників з використанням ботнетів чи інших інструментів. DoS-атаки можуть завдати значних збитків підприємствам, особливо якщо вони покладаються на свою мережу у своїх операціях.

2. Розподілені атаки типу «відмова в обслуговуванні» (DDoS): Розподілені атаки типу «відмова в обслуговуванні» аналогічні атакам типу «відмова в обслуговуванні», але в них беруть участь кілька зловмисників, які використовують

кілька систем для запуску атаки. DDoS-атаки зазвичай більш потужні, і їх складніше виявити та пом'якшити, ніж DoS-атаки. Зловмисники можуть використовувати скомпрометовані пристрої або ботнети для запуску DDoS-атак, що ускладнює відстеження джерела атаки.DDoS-атаки можуть завдати значної шкоди бізнесу та призвести до втрати доходів, репутаційної шкоди та юридичної відповідальності.

3. Атаки «людина посередині» (MitM): В атаках «людина посередині» зловмисники перехоплюють та маніпулюють мережевим трафіком між двома сторонами. Зловмисники можуть прослуховувати мережевий трафік, красти конфіденційну інформацію або впроваджувати шкідливий код у мережевий трафік для виконання інших шкідливих дій. Атаки MitM можуть виконуватися в будь-якій мережі, включаючи загальнодоступні мережі Wi-Fi, і їх може бути складно виявити без належних заходів безпеки.

4. Фішингові атаки: Фішингові атаки - це атаки соціальної інженерії, які змушують користувачів розголошувати конфіденційну інформацію або завантажувати зловмисне програмне забезпечення. Зловмисники можуть використовувати різні тактики для проведення фішингових атак, наприклад відправляти шахрайські електронні листи або створювати підроблені веб-сайти, що імітують законні веб-сайти. Фішингові атаки широко поширені і можуть призвести до значних фінансових втрат та репутаційної шкоди.

5. Атаки SQL Injection: Атаки SQL Injection – це тип атак, націлених на серверну базу даних веб-програми. Зловмисники можуть впровадити шкідливий код SQL у поля введення веб-програми, щоб отримати конфіденційну інформацію або виконати довільний код. Атаки SQL Injection є серйозною загрозою для веб-додатків, і їх може бути складно виявити і пом'якшити без належних заходів безпеки.

6. Атаки з використанням міжсайтового скриптингу (XSS): В атаках з використанням міжсайтових сценаріїв зловмисники впроваджують шкідливі сценарії у веб-сторінки, які переглядають інші користувачі. Ці сценарії можуть викрадати конфіденційну інформацію або виконувати інші шкідливі дії. XSS-атаки

буває складно виявити, і вони широко поширені на веб-сайтах, які приймають дані, що вводяться користувачем.

7. Шкідливі атаки: Атаки шкідливих програм включають розгортання зловмисниками шкідливого програмного забезпечення в мережі або системі для крадіжки конфіденційної інформації, порушення роботи мережі або виконання інших зловмисних дій. Шкідливе програмне забезпечення може поширюватися по різних каналах, таких як вкладення електронної пошти, шкідливі посилання або завантаження зараженого програмного забезпечення. Атаки шкідливого ПЗ буває складно виявити та пом'якшити, і вони можуть призвести до значних фінансових втрат та репутаційної шкоди.

В заключення [20], мережеві атаки є серйозною загрозою як бізнесу, так окремих осіб, і дуже важливо розуміти різні типи мережевих атак і те, як вони працюють. Застосовуючи належні заходи безпеки, такі як брандмауери, системи виявлення вторгнень та програмне забезпечення для захисту від шкідливих програм, підприємства можуть знизити ризик атак на мережу та захистити свою конфіденційну інформацію та активи.

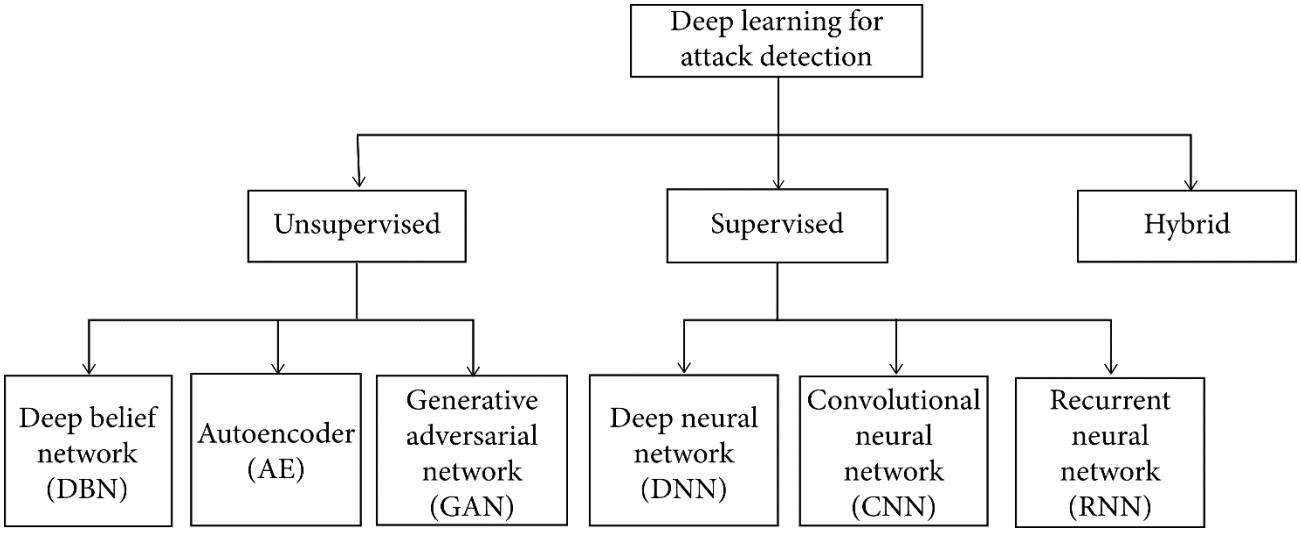

Рис. 1.2. Класифікація сучасних методів глибокого навчання для виявлення атак

Розглянемо загрози в мережах. Прийнято вважати, що можна виділити наступні основні загрози

- Загрози цілісності;

- Загрози конфіденційності;

- Загрози доступності.

Ці узагальнені типи загроз не охоплюють специфічні загрози. Тому, виходячи із загальних механізмів взаємозв'язку, можна виділити два основних типи загроз у випадку віддалених атак.

1. Загрози, що походять від учасників інформаційного обміну

- Відхилення даних після їх отримання

- Відмова від передачі даних після того, як вони були передані.

- Відмова від формування угоди.

2. Загрози з боку третіх осіб (зловмисників).

- Вставка даних в обмін.

- Відмова в обслуговуванні.

Загрози для мережі організації та її систем можна поділити на ***старі*** та ***нові***.

Старі загрози - це ті, що здійснюються за допомогою атак, які використовують добре відомі вразливості або сценарії атак (експлойти). Ці загрози походять від хакерів, які недостатньо компетентні (так звані «діти експлойтів») або взагалі не компетентні (так звані «новачки»). Ці типи зловмисників використовують готові сценарії атак і можуть не знати про реальні механізми експлойтів, що використовуються (або використовуються), або про їхні можливі побічні ефекти.

Однак це не робить їх менш небезпечними для організації. Це пов'язано з тим, що незахищені реалізації старих загроз можуть завдати значної шкоди, якщо організація не вживе заходів.

Нові загрози є більш серйозними і потенційно небезпечними для організації. Вони характеризуються прямими спробами завдати шкоди, отримати інформацію, порушити роботу тощо. Ці нові загрози зазвичай здійснюються кваліфікованими зловмисниками з детальним знанням мережевої механіки та логіки роботи додатків. Зловмисники використовують спеціальні інструменти та скрипти для отримання необхідної інформації (яка може бути використана слабшими

категоріями зловмисників для здійснення своїх атак) [8, 4, 10]. Нові загрози зазвичай використовують невідомі або нещодавно виявлені вразливості.

Весь спектр загроз можна розділити на зовнішні та внутрішні. Зовнішні загрози - це ті, що надходять ззовні. Внутрішні загрози - це загрози, ініційовані суб'єктами, які мають доступ до інфраструктури організації. Типовим прикладом внутрішньої загрози є обурення звільненого працівника, який спотворює інформацію організації.

Щороку виявляються нові вразливості, але знання, необхідні для здійснення атак, зменшуються, чому значною мірою сприяє широке використання Інтернету.

Нові та старі зовнішні загрози реалізуються через мережеві та віддалені мережеві атаки. Під віддаленими мережевими атаками ми розуміємо, що програмні засоби можуть впливати на програмні компоненти цільової системи. Таким чином, атака - це спроба отримати дані або здійснити вторгнення. Зазвичай виділяють три основні типи атак [1, 5, 16, 19].

1) Розвідувальні атаки (зондування, збір інформації).

2) Атаки на отримання доступу.

3) Атаки на відмову в обслуговуванні.

Ці атаки використовуються не завжди. Однією з головних проблем у сфері комп'ютерної безпеки є відсутність єдиної термінології. Ця проблема ще більше загострюється наступними обставинами.

- Різноманітність використовуваних термінів, які вже існують в тій мові, в якій вони вживаються.

- Поширеність перекладних книг, в яких перекладач використовує неоднозначні терміни (виключенням з цього правила є блискучий переклад книги «Новий словник хакера», який, на жаль, не включає в себе терміни, що увійшли в ужиток в комп'ютерній сфері в останні роки).

- Зловживання термінами постачальниками та виробниками засобів безпеки, які повинні переконувати клієнтів купувати їхні продукти.

- Відсутність стандартизованого переліку термінів або усталеної термінології.

Мережеві атаки націлені на програмні засоби хоста, що атакується. Програмне забезпечення, що атакується, може бути стеком мережевої операційної системи, іншим системним кодом або прикладними програмами, тобто елементами прикладного або системного програмного забезпечення. Як правило, атаки можливі через помилки або прорахунки в проектуванні, реалізації, конфігурації або використанні цих програмних засобів.

Розглянемо основні елементи термінології, що використовується стосовно мережевих атак. Помилки можуть бути ще неочевидними і не використовуватися зловмисником.

Несправність - недолік програмного інструменту, визначений його програмним кодом або недоліком у дизайні чи реалізації інструменту. Помилка - це вразливість.

Вразливість - це недолік програмного інструменту, який може бути використаний зловмисником.

Зловмисники розробляють шаблони атак для відомих вразливостей або опустити окремі кроки в сценарії.

Якщо зловмисник має легальний доступ до системи, він аналізуватиме файли, просто відкриваючи один за одним. При належному рівні контролю за дозволами доступ для нелегального користувача буде закрито, а спроби доступу зареєстровані в журналах.

Правильно налаштовані дозволи запобігають випадковому витоку інформації. Однак серйозний зловмисник намагатиметься обійти систему контролю та отримати доступ до потрібної інформації. Існує велика кількість вразливих місць, які допоможуть йому в цьому.

1.4. Різноманітність технології VPN

VPN (Virtual Private Network - віртуальна приватна мережа) - це технологія, яка дозволяє користувачам безпечно отримувати доступ і передавати дані через Інтернет, а також маскувати свою IP-адресу і шифрувати свою діяльність в Інтернеті Існує кілька типів технології VPN, кожен з яких має свої переваги і недоліки. Відповідь. Ця відповідь містить детальний огляд найпоширеніших технологій VPN .

Різні технології VPN пропонують різну «глибину» з'єднання. «Глибина» з'єднання з оператором може бути різною. Наприклад, з'єднання між віддаленими офісами в невеликих компаніях часто досягається за допомогою технології VPN Це часто досягається шляхом налаштування тунелю через Інтернет з використанням протоколу

У цьому випадку взаємодія з оператором дуже низька.

Підключення до Інтернету має бути забезпечено через канал з необхідною пропускною здатністю, а взаємодія з оператором дуже незначна.

Підключення до Інтернету має бути забезпечено через канал з необхідною пропускною здатністю, а завдання створення VPN вирішується фахівцями компанії або її експертами, або її партнерами з інтеграції.

Основною перевагою цього методу є його низька вартість.

Основними перевагами цього методу є його низька вартість і можливість швидко побудувати VPN в будь-якому місці.

Крім того, сьогодні доступ до інтернету є майже повсюдно доступним.

Закриті тунелі IPSec можна створювати як між офісами, так і між офісами та комп'ютерами.

Закриті тунелі IPSec також можна налаштувати між офісами та комп'ютерами, клієнтами та віддаленими співробітниками.

Домашні офіси співробітників.

Для цих цілей можна використовувати інші протоколи VPN.

Між користувачем і шлюзом працюють інші протоколи VPN: ssl/tls, pptp, l2tp.

Широке використання IPSec VPN сильно залежить від наявності відповідних пристроїв.

Широке використання IPSec VPN в значній мірі залежить від наявності відповідних пристроїв; при всіх своїх перевагах, IPSec

Технологія IPSec VPN має ряд недоліків. Криптографічні тунелі через Інтернет зазвичай використовуються для

Надання неслужбової інформації для налаштування резервного каналу зв'язку

Використовуються для організації резервного каналу зв'язку на випадок затримок або збоїв в основному каналі. Недоліками цього є те, що

IPSec VPN створює ілюзію незалежності від оператора зв'язку.

Тому що не підтримує параметри зв'язку між віддаленими підрозділами компанії.

Тому що не підтримує параметри зв'язку.

IPSec VPN є типовим прикладом віртуальних приватних мереж.

Це типовий приклад віртуальної приватної мережі, побудованої за так званою оверлейною моделлю.

У процесі маршрутизації клієнтського трафіку не використовується обладнання постачальника послуг.

Обладнання провайдера не використовується в процесі маршрутизації клієнтського трафіку, а мережа забезпечує лише «прозорі» з'єднання між сайтами компанії.

Інша модель конфігурації VPN, Peer to Peer.

Peer-to-peer передбачає взаємодію між обладнанням клієнта (маршрутизатором/комутатором) і клієнтським обладнанням.

Передбачає взаємодію між обладнанням постачальника послуг і обладнанням клієнта (маршрутизатором/комутатором), яке використовується для маршрутизації трафіку клієнта.

Використовується для маршрутизації трафіку клієнта.

Незалежний виділений маршрутизатор - зазвичай використовується сьогодні.

Віртуальний маршрутизатор з підтримкою IP/MPLS. Безпека мережі забезпечується додатковими адміністративними та технічними засобами захисту.

У цьому випадку мережева безпека забезпечується додатковими адміністративними та технічними методами, такими як пакетна та маршрутна

Мережева безпека забезпечується додатковими адміністративними та технічними заходами, такими як фільтрація пакетів та маршрутів.

1.5. Концепція віртуальної безпечної VPN

Віртуальні безпечні VPN працюють на мережі серверів, розташованих по всьому світу. Користувачі можуть отримати доступ до цих серверів за допомогою клієнтського програмного забезпечення VPN, встановленого на таких пристроях, як смартфони, планшети та комп'ютери. Коли користувач підключається до віртуальної захищеної мережі VPN, його інтернет-трафік шифрується і надсилається через захищений тунель на VPN-сервер, розташований в іншій точці світу. Цей процес гарантує, що діяльність користувача в Інтернеті прихована від сторонніх очей, включаючи хакерів і державні органи нагляду.

Віртуальна безпечна мережа VPN пропонує користувачам кілька переваг. По-перше, вони шифрують інтернет-трафік, що ускладнює перехоплення і крадіжку персональних даних користувачів хакерами і забезпечує додатковий рівень безпеки для користувачів. По-друге, віртуальні безпечні VPN допомагають користувачам обходити цензуру та географічні обмеження. Багато веб-сайтів та онлайн-сервісів не доступні в певних країнах або регіонах через державну цензуру або обмеження авторських прав. За допомогою віртуальної захищеної VPN користувачі можуть отримати доступ до цих сервісів, підключаючись до серверів, розташованих у країнах, де ці сервіси доступні. Нарешті, віртуальні безпечні VPN допомагають зберегти конфіденційність в Інтернеті, приховуючи IP-адресу та місцезнаходження користувача.

Таким чином, віртуальні безпечні VPN є ідеальним інструментом для тих, хто хоче підвищити свою безпеку і конфіденційність в Інтернеті. Шифруючи інтернет-

трафік і приховуючи свою поведінку в мережі, користувачі можуть захистити себе від хакерів, урядового нагляду та онлайн-відстеження. Крім того, віртуальні безпечні VPN дозволяють обійти цензуру та географічні обмеження і надають користувачам доступ до ширшого спектру онлайн-сервісів та інформації.

Зараз VPN конкурують з глобальними мережами (WAN).

VPN успішно інтегрують інфраструктури віддалених офісів в єдину корпоративну мережу, мінімізуючи витрати на корпоративну мережу.

VPN можуть успішно інтегрувати інфраструктури віддалених офісів в єдину корпоративну мережу в режимі онлайн, мінімізуючи витрати на корпоративну мережу.

Крім того, будь-який співробітник може легко підключатися до власної мережі під час доступу до Інтернету.

Вони можуть легко підключатися до корпоративної мережі з будь-якої точки світу.

Найбільш універсальним способом побудови VPN є технологія інкапсуляції або тунелювання.

Тунелювання використовується для пересилання пакетів з однієї мережі (первинної мережі) в іншу (вторинну мережу).

Використовується для пересилання пакетів з мережі (первинної мережі) через канал зв'язку іншої мережі (вторинної мережі) з несумісними протоколами.

(Вторинної мережі), де протоколи несумісні. З цієї причини пакети (дані та протоколи) з первинної мережі інкапсулюються в пакети вторинної мережі і стають видимими як дані. Таким чином.

Таким чином, пакети просуваються маршрутизатором основної мережі виключно на основі їхніх зовнішніх заголовків.

Таким чином, маршрутизатор основної мережі просуває пакети виключно на основі їхніх зовнішніх заголовків і не перевіряє вміст оригінального пакета. Це проілюстровано на рисунку 1.3, як дані передаються з точки A в точку B через тунель між точками X і Z.

На рисунку 1.3 показано, як дані передаються від A до B через тунель між X і Z. Проміжний вузол Y не знає адреси призначення B, але дані через тунель не знає адреси призначення B, але передає дані через тунель тільки до вузла Z. У цьому сценарії вузол X називається входом в тунель, вузол Z - виходом з тунелю називається входом тунелю, а вузол Z - виходом.

Рис. 1.3. Передача даних через тунель

Інкапсуляція зазвичай не включає кодування. Якщо потрібен вищий рівень безпеки потрібно підвищити рівень безпеки, це робиться через приватну мережу до того, як буде виконана інкапсуляція виконується через приватну мережу.

Функціонально тунель складається з початкової точки (точки входу, ініціатора) і одного або декількох ініціаторів тунелю і однієї або декількох кінцевих точок (виходів, термінаторів тунелю) можна розглядати як наскрізні віртуальні канали.

1.6. Різноманітність протоколів для побудови VPN

Відомо, що «слабкі місця» існують через структуру протоколу IP в мережах, що використовують протоколи IP.

Гнучкість протоколу дозволяє використовувати його в повній мірі для управління трафіком, контроль доступу та інші заходи безпеки можуть бути подолані.

Тому мережеві дані, що використовують протокол IP, можуть бути легко підроблені або перехоплені.

Легка підробка і перехоплення. Тунелі можуть бути вбудованими або інкапсульованими при передачі в пакетних мережах з використанням мережевих протоколів.

Тунелі вбудовуються або інкапсулюються в інші пакети мережевого протоколу при передачі в пакетних мережах з використанням мережевих протоколів.

PPTP. PPTP (Point-to-Point Tunneling Protocol) - це протокол тунелювання точка-точка.

Протокол тунелювання точка-точка, який дозволяє комп'ютерам встановлювати безпечні з'єднання.

Він дозволяє комп'ютеру встановити безпечне з'єднання з сервером шляхом тунелювання через стандартну незахищену мережу.

Створюючи тунель через стандартну незахищену мережу, комп'ютер може встановити безпечне з'єднання з сервером.PPTP може бути інкапсульованим (упакованим).

PPTP інкапсулює (упаковує або приховує від використання) PPP-пакети в пакети Інтернет-протоколу (IP).

(IP) пакети і можуть бути перетворені в (IP) пакети і передані через IP-мережі (включаючи Інтернет).

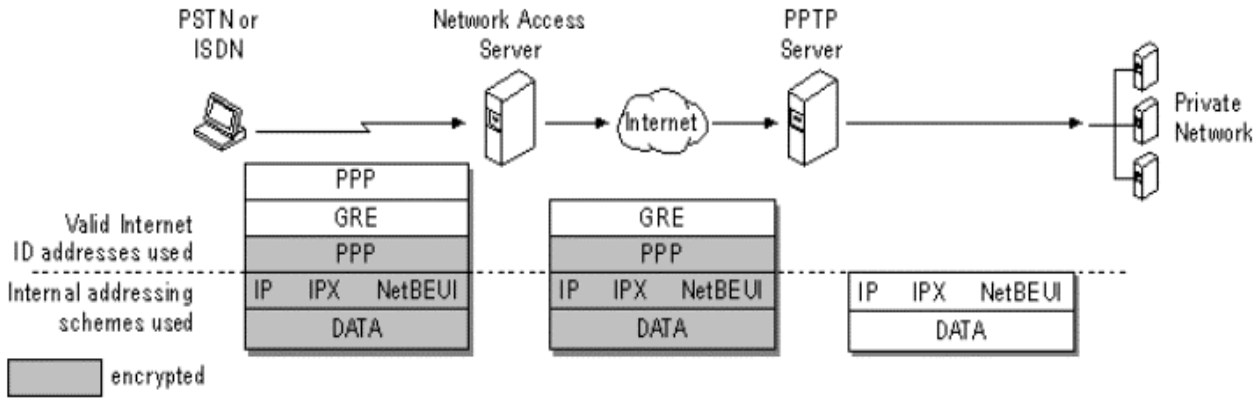

Рис. 1.4. Положення протоколу PPTP в моделі OSI

PTP забезпечує безпечну передачу даних на єдиний корпоративний сервер.

Він створює віртуальну мережу в мережі TCP/IP, яка є незалежною від віддаленого клієнта і дозволяє безпечно передавати дані на єдиний корпоративний сервер.

Створює віртуальну мережу в мережі TCP/IP, незалежну від клієнта PPTP також можна використовувати для створення тунелю між двома локальними мережами.

Його також можна використовувати для створення тунелю між локальними мережами; PPTP працює шляхом встановлення звичайного сеансу PPP з іншою стороною, використовуючи Generic Routing для встановлення звичайного сеансу PPP з іншою стороною.

Інкапсуляція (GRE), використовуючи друге з'єднання на TCP-порті 1723.

Друге з'єднання на TCP-порті 1723 використовується для ініціювання та контролю GRE-з'єднання. протокол MPPE

Дані трафіку PPTP можуть бути захищені. Для аутентифікації можуть використовуватися різні механізми.

Клієнти можуть бути авторизовані різними механізмами, найбезпечнішим з яких є MSCHAPv2.

MSCHAPv2 і EAP-TLS.

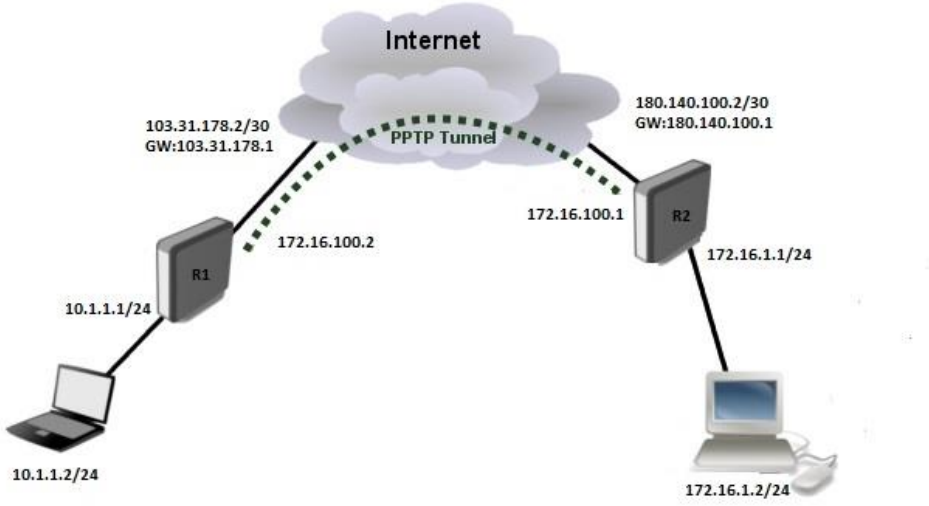

Рис. 1.5. Встановлення IP-з'єднання з сервером тунелю PPTP

Для використання клієнтського протоколу PPTP необхідно встановити сервер тунелювання PPTP (рис. 1.4).

Необхідно встановити IP-з'єднання з сервером тунелювання PPTP (рис. 1.5). Всі дані можна захистити і стиснути через це з'єднання. Тунель PPTP може передавати дані різних мережевих протоколів (TCP/IP, NetBEUI і IPX).

L2TP. L2TP (Layer 2 Tunneling Protocol) - це протокол тунелювання для рівня 2 (канального рівня).

Протокол тунелювання рівня 2 (канального рівня), об'єднаний з протоколом L2F (Layer 2 Forwarding).

Розроблений компанією Cisco, а протокол PPTP - компанією Microsoft.

VPN можна конфігурувати з попередньо встановленими пріоритетами доступу, але немає функцій захисту даних.

Пріоритети доступу до VPN можуть бути налаштовані, але не передбачено жодних заходів захисту даних або механізмів автентифікації.

Протокол L2TP використовує два типи повідомлень: керуючі повідомлення і повідомлення даних.

Це керуючі повідомлення і повідомлення даних (Малюнок 1.6). Керуючі повідомлення використовуються для встановлення, підтримки і видалення тунелів і викликів.

Ці повідомлення використовують довірений канал управління протоколу L2TP і для забезпечення їх доставки. Інформаційні повідомлення використовуються для інкапсуляції PPP-зображень, що надсилаються через тунель. Якщо пакет втрачено пакет не передається повторно.

L2TP також підтримує різні параметри аутентифікації, що здійснюються PPP.

Сюди входять: протокол автентифікації пароля, протокол автентифікації Microsoft Challenge-Handshake і CHAP. Додатковим способом аутентифікації кінцевих точок тунелю є використання L2TP для забезпечення додаткової безпеки, реалізованої за допомогою IP-безпеки (IPsec).

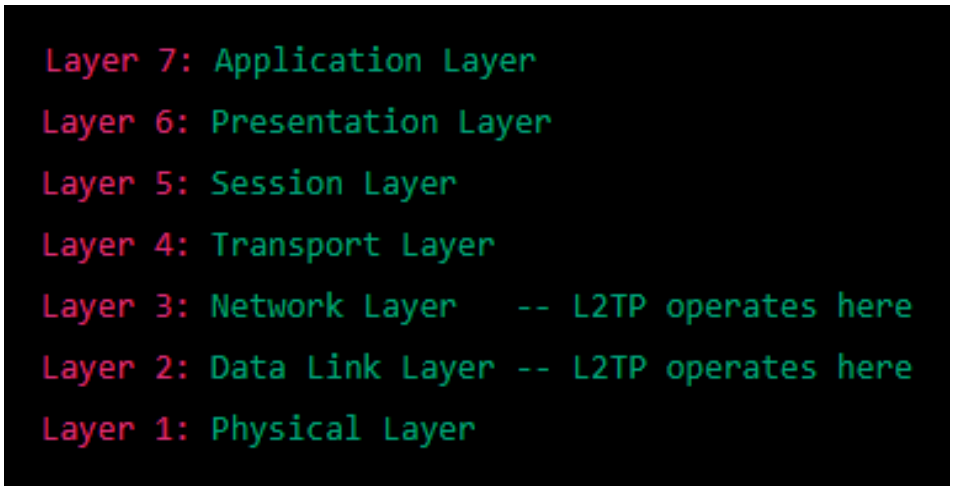

Рис. 1.6. Місце протокола L2TP у моделях OSI

Всі контрольні повідомлення повинні містити порядковий номер.

Це використовується для забезпечення надійної доставки по каналу управління.

IPSec. IPSec (IP Security) - це набір протоколів, які забезпечують безпеку при пересиланні IP-пакетів.

Набір протоколів, які займаються безпекою при пересиланні IP-пакетів IPSec також містить протоколи для безпечного обміну ключами через Інтернет.

Режим тунелю IPsec використовується між двома виділеними маршрутизаторами, при цьому кожен маршрутизатор діє як один кінець віртуального «тунелю» через публічну мережу. У режимі тунелю IPsec оригінальний IP-заголовок, що містить кінцевий пункт призначення пакета, шифрується, на додаток до корисного навантаження пакета. Щоб повідомити маршрутизаторам-посередникам, куди пересилати пакети, IPsec додає новий IP-заголовок. На кожному кінці тунелю маршрутизатори розшифровують IP-заголовки, щоб доставити пакети до місця призначення.

Протокол IPSec працює на рівні 3 мережевої моделі OSI (рис. 1.7).

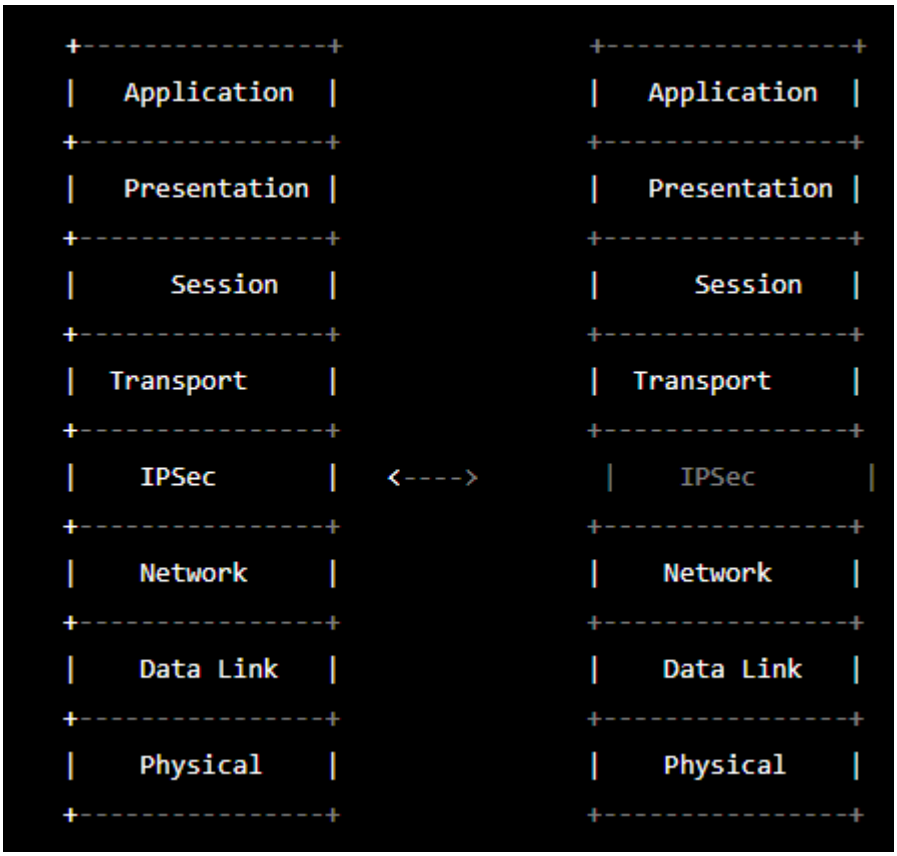

Рис. 1.7. Місце протоколу IPSec в моделі OSI

Інтернет-протокол (IP) не має засобів захисту даних, що передаються;

IP не може навіть гарантувати, що відправник є тим, за кого себе видає не може гарантувати, що це саме той, за кого себе видає. IPSec - це спроба виправити цю ситуацію При використанні IPSec за допомогою IPSec весь вихідний трафік захищається до того, як він буде відправлений в мережу.

За допомогою IPSec весь вихідний трафік захищається до того, як він буде відправлений в мережу (рис. 1.8).

Завдяки IPSec одержувач повідомлення може відстежити походження отриманих пакетів і перевірити цілісність даних.

Цілісність даних можна перевірити. Необхідно переконатися, що транзакція виконується тільки один раз, тобто тільки один раз (якщо тільки користувач не має права повторити її.)

Якщо користувач не має права повторити її). Іншими словами, не повинно бути можливості записувати транзакції і повторювати їх користувачеві.

У користувача створюється враження, що в цьому випадку відбулося більше однієї транзакції.

Деякі шахраї отримують інформацію про трафік і, перенаправляючи такий трафік

Перенаправляючи такий трафік, він/вона отримує певну вигоду для себе (наприклад в результаті на його рахунок надходять гроші тощо). Для цього передавати такий трафік багаторазово неможливо.

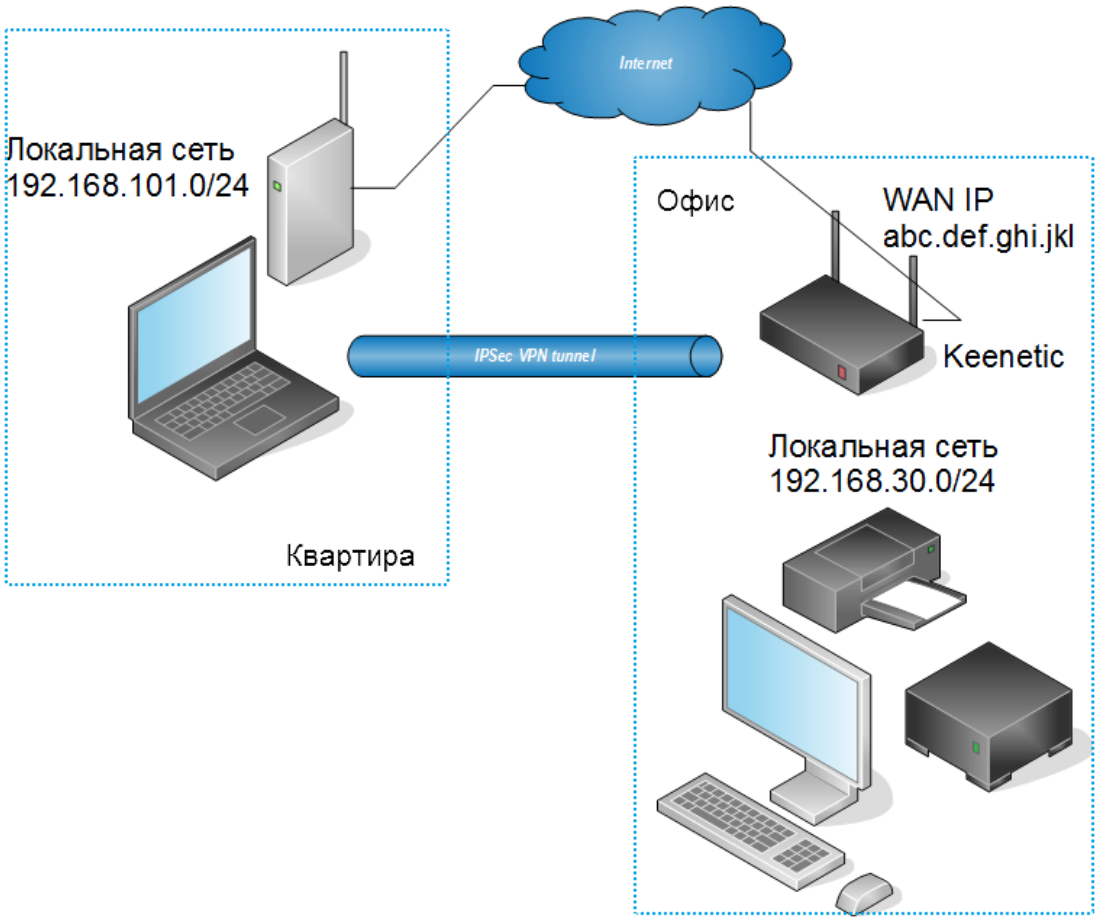

Рис. 1.8. IPSec-з'єднання в VPN-тунелях

IPSec VPN ідеально підходить для з'єднання мереж в різних офісах через Інтернет (рис. 1.9).

Вона ідеально підходить для (рис. 1.9).

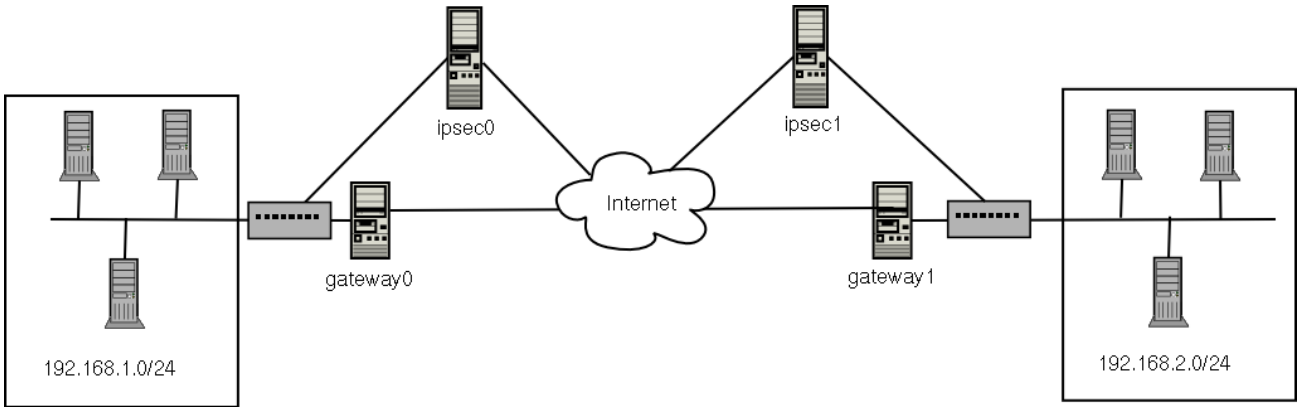

Рис. 1.9. VPN-з'єднання з використанням протоколу IPSec

IPSec VPN створюють певні переваги для користувачів.

SMB/SOHO (малий бізнес/малий офіс/домашній офіс).

- Економічна ефективність.

- Комплексне рішення, придатне для комерційного використання.

Для віддалених користувачів.

- Інтегроване та безпечне рішення.

- Не потребує додаткового програмного забезпечення.

- Простота в налаштуванні.

Для спільного використання.

- Економічно ефективне рішення для віддалених користувачів і філій та філій економічно ефективне рішення для віддалених користувачів і філій.

- Сумісне з рішеннями для віртуальних приватних мереж від більшості постачальників рішень.

Віртуальна приватна мережа. SSL (Secure Socket Layer) - протокол захищених сокетів.

Забезпечує безпечну передачу даних через Інтернет. Цей протокол створює захищене з'єднання між клієнтом і сервером.

SSL використовує захист даних відкритим ключем для автентифікації.

Захищає відправника та одержувача. Підтримує надійність передачі даних.

Дозволяє виправляти коди та хеші.

SSL використовує два ключі для захисту даних - відкритий ключ і приватний або секретний ключ, відомий одержувачу повідомлення.

Сьогодні SSL використовується на багатьох веб-сайтах.

Сьогодні існує багато веб-сайтів, які використовують SSL для захисту даних користувачів в Інтернеті (наприклад, комерційні та банківські послуги).

Усі поширені браузери, поштові клієнти та інтернет-додатки підтримують використання SSL.

Щоб отримати доступ до сторінки, захищеної SSL, зазвичай замість http для доступу до сторінок, захищених SSL, зазвичай замість префікса http використовується префікс https (порт 443), який вказує на те, що ви використовуєте SSL-з'єднання.

Це означає, що ви використовуєте SSL-з'єднання.

SSL також може захищати протоколи прикладного рівня.

(Він також може захищати протоколи прикладного рівня (рівень 7 моделі OSI), такі як POP3 і FTP. Щоб SSL працював сервер повинен мати сертифікат SSL.

Безпечний зв'язок між клієнтом і сервером за допомогою SSL забезпечує дві функції: автентифікацію та захист даних.

Він забезпечує виконання двох функцій: автентифікацію та захист даних.

SSL складається з двох рівнів Багаторівневий транспортний протокол

(TCP) використовується для шифрування протоколу та кодування протоколів нижчого рівня (4-5 рівень).

Він інкапсулює протоколи нижнього рівня (рівні 4-5) (наприклад, генерація пакетів).

Забезпечує умови для кожного інкапсульованого протоколу.

Забезпечує умови для автентифікації сервера і клієнта, захисту даних, що передаються, та обміну ключами.

Забезпечує умови для автентифікації сервера та клієнта, захисту даних, що передаються, та обміну ключами перед відправленням та отриманням даних.

Забезпечує захист даних, що передаються, та обмін ключами.

SSL VPN ідеально підходить для підключення віддалених користувачів до ресурсів локальної мережі офісу через Інтернет.

Ідеально підходить для підключення до (рис. 1.10).

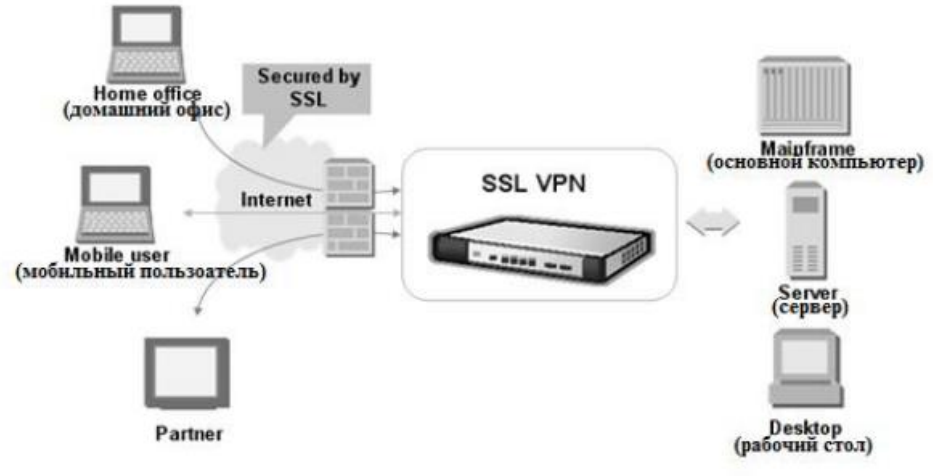

Рис. 1.10. Принцип підключення протоколу SSL VPN

SSTP (Secure Socket Tunneling Protocol) - протокол безпечного тунелювання сокетів [8, 13, 19].

Абревіатура для протоколу тунелювання сокетів, VPN-протоколу від Microsoft, заснованого на SSL, включеного в їхні операційні системи, починаючи з Windows 2008.

Включений в операційні системи компанії, починаючи з Windows 2008 і Windows Vista SP1.

З'єднання здійснюється за допомогою HTTPS через порт 44.3. SSL використовується для шифрування SSL використовується для шифрування, а SSL і PPP - для автентифікації.

Generic Routing Encapsulation (GRE) Загальна інкапсуляція маршрутизації.

Інкапсуляція - це протокол тунелювання мережевих пакетів, розроблений компанією Cisco Systems.

Cisco Systems GRE надає механізм для інкапсуляції пакетів інкапсулює будь-який пакет у будь-який транспортний протокол.

Висновки до першого розділу

Досліджено структури небезпечних мереж, проаналізовано слабкі місця, якими можуть скористатися зловмисники, щоб отримати несанкціонований доступ до конфіденційної інформації або завдати шкоди мережі.

Визначено дизайн і архітектуру мережі, типи використовуваних пристроїв і програмного забезпечення, а також вжиті заходи безпеки. Вибір відповідних інструментів безпеки та рішень повинен які ґрунтуються на конкретних потребах і вимогах мережі (OpenVPN Server).

Розглянуто концепцію та різноманітність протоколів віртуальної безпечної VPN.

2 ДОСЛІДЖЕННЯ КОНЦЕПЦІЙ ТА КОНФІГУРАЦІЙ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ МЕРЕЖІ VPN

2.1. Захист каналів в корпоративній мережі на основі VPN рішень

Корпоративна мережа — це тип комп’ютерної мережі, яка використовується підприємствами та організаціями для полегшення спілкування, співпраці та обміну інформацією між співробітниками, відділами та філіями. Корпоративна мережа може складатися з різних пристроїв і технологій, включаючи сервери, маршрутизатори, комутатори та інше мережеве обладнання.

Основна мета корпоративної мережі — дозволити співробітникам отримувати доступ до таких ресурсів, як дані, програми та принтери, і ділитися ними. Корпоративні мережі також можна використовувати для полегшення віддаленого доступу для співробітників, які працюють з дому або подорожують, дозволяючи їм безпечно підключатися до корпоративної мережі та отримувати доступ до тих самих ресурсів, що й в офісі.

Корпоративна мережа має [14, 15, 21]:

1. корпоративний сервер баз даних;
2. електронний документообіг
3. доступ до мережі Інтернет;
4. апаратно-програмний захист інформації;
5. відеоконференцзв'язок
6. корпоративна електронна пошта;
7. корпоративна IP-телефонія

КМ характеризується [15]:

1. Використання робочих інструментів для передачі даних публічного використання.

2. Доступ до інформації надається певному колу осіб.

3. Поширення інформації може бути трьох типів: офіційне, проектна група та неофіційне.

4. Наявність єдиної системи управління мережею підприємства.

КМ дає можливість ефективно інтегрувати території на окремі підрозділи [16, 17].

Одна мережа надає перелік можливостей [17]:

- Онлайн доступ до Workplace;
- Віддалений доступ до сервісів КМ;
- Доступ до Інтернету;
- Надсилання даних на основі адреси.

Таким чином, КМ надає можливість виходу в Інтернет з єдиної мережі і може зменшити вартість внутрішніх серверів і каналів розповсюдження для Інтернету [12].

КМ характеризуються функціональними елементами [16]:

Робочі місця користувачів розташовуються

- в одному приміщенні;
- в будь-якому місці.

Інформаційний сервер організації зберігає та обробляє дані, які можуть існувати як всередині, так і поза межами організації.

Телекомунікації - це взаємодія між робочими станціями та між робочими станціями та інформаційними серверами організації.

Телекомунікаційні засоби організації можуть бути [11, 17]:

- виділені;
- загальні.

Останній є найбільш поширеним [19].

В межах організації вплив на інформацію може здійснюватися за допомогою однієї або декількома послугами, що надаються за допомогою телекомунікацій [19].

1. Система управління ефективністю КМ. Залежно від набору послуг, що надаються, КМ повинна мати засоби управління мережею (засоби маршрутизації та засоби управління мережею (засоби маршрутизації та комутації, засоби управління). Серед елементів управління КМ розрізняють:

- керовані функціональні елементи в межах підприємства;
- некеровані функціональні елементи в межах корпорації, які належать до загальної підмережі, що використовується юридичною особою.

2. Функціонуюча система управління безпекою в КМ. В КМ реалізовані необхідні служби мережевої безпеки має використовуватися як належний захід безпеки.

3. Механізми забезпечення надійності КМ. Засоби забезпечення загальної працездатності мережі або її фрагментів у разі виходу з ладу елемента КМК.

4. Системи діагностики та контролю. У КМ повинні бути передбачені засоби контролю працездатності кожного елемента функціональних елементів (системи збору інформації про несправності, відмови та живучості, управління експлуатаційними характеристиками, управління безпекою) повинні бути передбачені в системі.

Для КМУ повинні бути створені такі функціональні елементи (системи збору інформації про несправності, відмови та живучість, управління експлуатаційними характеристиками, управління безпекою) засоби діагностики, які будуть впроваджуватися в процесі експлуатації мережі.

5. Операційні системи. ОСУ повинна бути визначена планом розвитку для забезпечення розвитку визначених у ньому функціональних функціональних можливостей, визначених у ньому.

Коли КМ узагальнюються, можна зробити класифікацію:

- за набором функціональних елементів;
- за ієрархією управління;
- за набором публічних підмереж, які об'єднані в рамках КМ:
- з набору публічних підмереж, об'єднаних в рамках КМ.

Безпека КМ має вирішальне значення для успіху будь-якої організації.

Великі організації покладаються на власний КМ для безпечного та постійного доступу до інформації, додатків та електронної пошти організації електронної пошти [18].

Комплексне рішення для забезпечення безпеки КМ дозволяє організаціям підтримувати операційну стабільність, стійкість до атак і захист конфіденційності даних та безперервний 24-годинний доступ [19].

Завдання КМ в межах одного офісу дуже просте можна вирішити досить легко. Однак сучасна інфраструктура компанії часто розташовані в декількох будівлях, наприклад, використовуються дата-центри, а оскільки ці будівлі можуть бути географічно віддалені від організації, то формування є дуже складним завданням [17].

З розвитком Інтернету та колективного доступу до інформації в режимі реального часу, що стало рушійною силою розвитку УЗ, користувачі недорогими і доступними інтернет-каналами. Організації отримали можливість використовувати захищені канали для доступу до критично важливої комерційної та та управлінської інформації [18].

В основі VPN лежать три методи реалізації [13]:

- **Тунелювання.** Забезпечує передачу даних між двома точками. У цьому випадку використовується транспорт У тунельному середовищі перехоплюються пакети обраних мережевих протоколів. Вони доставляються безпосередньо від входу до виходу тунелю. Створення тунелю достатньо з'єднати два вузли мережі, і з точки зору вузла мережі програмного забезпечення, що працює на ньому, здається, що він підключений до локальної мережі.

Варто пам'ятати, що дані, які проходять через проміжні вузли Маршрутизатори у відкритих загальнодоступних мережах У цій ситуації є дві суттєві проблеми. Перша проблема полягає в наступному. А саме, для автентифікації користувачів використовуються наступні протоколи. Для автентифікації користувачів використовуються протоколи MSCHAP версії 2 і EAP-TLS, що дозволяють взаємну автентифікацію, тобто VPN сервер і клієнт

ідентифікують один одного. В іншому випадку тільки сервер аутентифікує клієнта [16].

PPTP - забезпечує високий рівень безпеки і стоїть вище L2TP - IPSec Він більш надійний і забезпечує аутентифікацію на рівні «користувач» і «комп'ютер», а також «комп'ютера», а також аутентифікацію та шифрування даних.

- **Аутентифікація.** Може бути реалізована у вигляді відкритого тексту або методами запиту/відповіді. Відкрита автентифікація не є поширеною.

Схеми запиту/відповіді є дуже поширеними і виражаються наступним чином [17]:

- Клієнт надсилає серверу запит на автентифікацію;
- Сервер повертає випадкову відповідь;
- Клієнт вилучає хеш зі свого пароля, шифрує відповідь хешем і відправляє її на сервер на сервер;
- Робить те ж саме для сервера і порівнює результати з відповіддю клієнта;
- Якщо зашифрована відповідь збігається, вважається, що автентифікація пройдена успішно.

Спочатку клієнт і сервер VPN проходять автентифікацію, але L2TP через IPSec використовує локальний сертифікат, отриманий від служби автентифікації. Клієнт і сервер обмінюються сертифікатами і формують безпечне з'єднання ESP SA.

L2TP завершує процес автентифікації для комп'ютера, який виконується на рівні користувача. Можна використовувати будь-який протокол. Використовуючи MSCHAP для автентифікації користувача, можна використовувати Використовуючи різні ключі шифрування для автентифікації комп'ютера і користувача, можна автентифікації користувача, можна підвищити безпеку. шифрування.

- **Шифрування.** Відтворює дані недоступними. В даний час використовуються два методи шифрування шифрування:

Протоколи шифрування MPPE і TLS можуть бути обрані автоматично. Перший передбачає, що канали зв'язку точка-точка канал зв'язку «точка-точка», в якому пакети передаються послідовно, але з невеликою втратою даних. У цьому випадку значення ключа наступного пакета є результат декодування попереднього пакета. У віртуальній мережі, описаній вище мережі загального доступу, такі умови важко виконати, і пакети, що надходять можуть досягати одержувача в хаотичному порядку. Крім того, PPTP використовується для зміни ключа шифрування - порядкового номера пакетів, що підлягають розшифровці може використовуватися незалежно від раніше отриманих пакетів [11].

Таким чином, комплекс «Тунелювання + Аутентифікація + Шифрування» дозволяє передавати дані між двома точками в мережі загального користування, імітуючи роботу мережі загального користування, імітуючи роботу локальної мережі. Таким чином, можна можна побудувати 27 мережу. Ще однією перевагою VPN-з'єднання є те, що воно використовувати систему адрес, прийняту в локальній мережі. Віртуальну приватну мережу можна створити, встановивши VPN-сервер; віддалені користувачі за допомогою клієнтського програмного забезпечення VPN ініціює процедуру з'єднання з сервером [10]. Користувач проходить аутентифікацію, встановлюється VPN-з'єднання і, у разі успіху, клієнт і сервер клієнт і сервер узгоджують деталі безпеки з'єднання.

Після цього виконуються наступні кроки Встановлюється VPN-з'єднання для забезпечення обміну інформацією між клієнтом і сервером. У цьому випадку основна проблема полягає в тому, щоб забезпечити дотримання встановлених стандартів аутентифікації та обміну зашифрованою інформацією. Ці стандарти знаходяться в стадії розробки або плануються до розробки. Ця проблема може затримати впровадження VPN в організації, оскільки вони не є обов'язковими і не можуть бути нав'язані організації [10].

2.2. Налаштування VPN для безпечної передачі даних

В основі створення VPN лежить ідея обміну між двома вузлами. Крім того, для забезпечення конфіденційності побудовано віртуальний тунель. Забезпечити цілісність інформації, що передається через відкриту мережу. Доступ є складним для всіх учасників і третіх сторін, які не беруть участі [17].

Переваги для організацій, які використовують ці віртуальні тунелі Економічна економія, оскільки немає потреби будувати або здавати будівлю в оренду. Має виділений канал зв'язку та формує власну інтранет/екстранет мережу. Використовує недорогі інтернет-канали з відмінною надійністю та швидкістю. передача не втрачається; економічна ефективність інтеграції VPN технологія стимулює організації до її агресивного впровадження [19].

Для підключення локальної обчислювальної мережі підприємства до мережі відкритого типу існує декілька типів загроз безпеці [16]:

- НСД проти внутрішніх ресурсів локальної мережі підприємства, отримані шахраями в результаті вторгнення до входу в мережу;
- Вторгнення в корпоративні дані в процесі їх передачі у відкритих мережах. В процесі передачі у відкритих мережах. Безпечна інформаційна взаємодія між локальними мережами, а також та окремими комп'ютерами по відкритих каналах (включаючи Інтернет). вирішує наступні завдання [16]:
- Захист локальних мереж і окремих комп'ютерів, підключених до відкритих локальних мереж та окремих комп'ютерів, підключених до відкритих каналів зв'язку, від вторгнення;
- Захист інформації в процесі передачі відкритими каналами зв'язку. Захист каналів зв'язку.

Для захисту локальних мереж та окремих комп'ютерів від вторгнення з зовнішнього середовища; використання міжмережевих екранів для підтримання Безпека інформаційного обміну забезпечується шляхом фільтрації двостороннього

потоку двостороннього потоку обміну інформацією, опосередковуючи обмін повідомленнями.

Брандмауери знаходяться між локальними та відкритими мережами. Для захисту певних віддалених комп'ютерів, підключених до відкритої мережі, мережевої мережі, встановлюється програмне забезпечення брандмауера. Персональний [16].

Захист інформації в процесі передачі інформації відкритими каналами базується на використанні віртуальних приватних мереж (VPN), які являють собою об'єднання окремих комп'ютерів у локальну мережу з використанням відкритого зовнішнього середовища для поширення інформації в одній віртуальній корпоративної мережі, забезпечуючи при цьому безпеку даних, що циркулюють. будується на відкритих каналах зв'язку публічних мереж. До них відносяться. віртуальні, захищені канали зв'язку називаються VPN-тунелями: в мережі VPN можна VPN-тунелі з'єднують центральні офіси з іншими офісами та філіями, передавати інформацію через Інтернет з віддаленими користувачами (рис. 2.1). [16].

VPN-тунелі прокладаються у відкритій мережі для з'єднання через які проходять криптографічно захищені пакети даних. Захист інформації в процесі передачі через VPN-тунель відбувається наступним чином. [20]:

- Аутентифікація взаємодіючих сторін;

- Криптографічне закриття переданих даних;

- Перевірка автентичності та цілісності інформації, що передається доставляється.

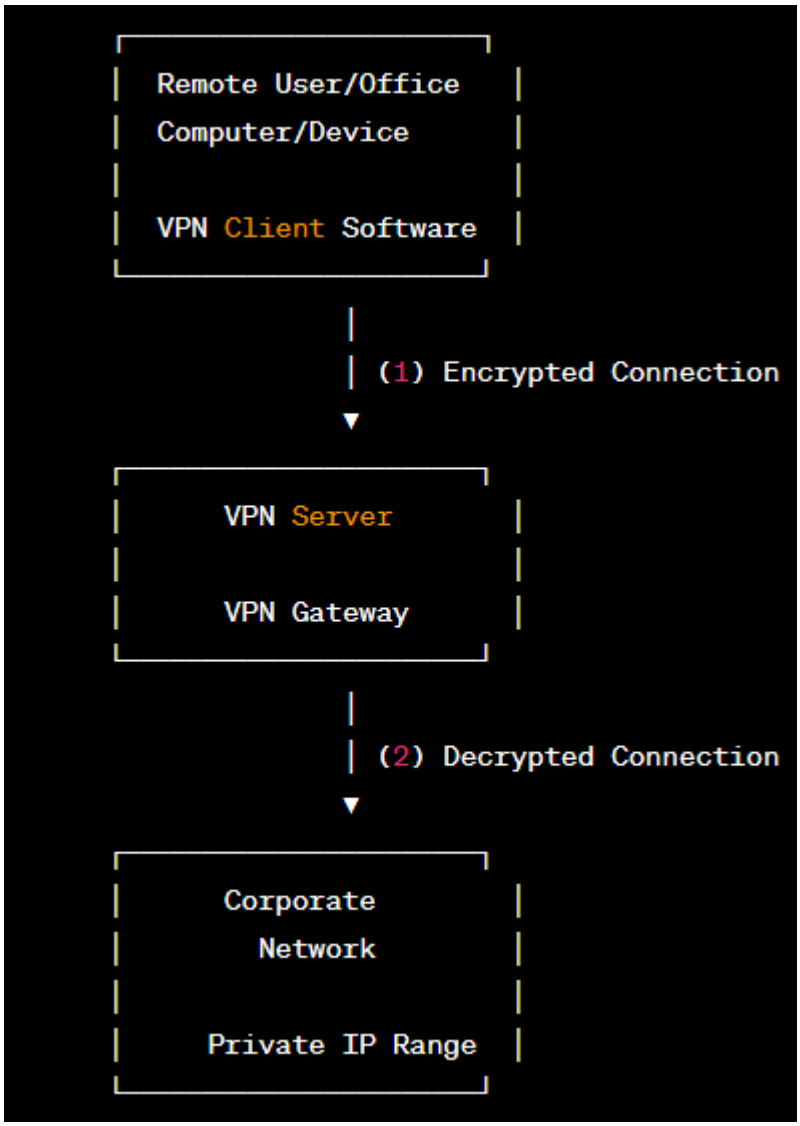

Рис. 2.1. Віртуальна захищена мережа VPN

Для цих функцій характерні відносини між сторонами. в реалізація та захист інформації за допомогою криптографічних методів. Захист ефективний завдяки використанню стику симетричні та асиметричні криптографічні схеми. Тунелі є створені за допомогою механізмів VPN і мають певні безпечні властивості. Це виділена лінія, розгорнута в рамках загальнодоступної мережі. Обладнання VPN має певні ролі: клієнт VPN, сервер VPN і шлюз безпеки VPN [21].

VPN-клієнт – це програмне забезпечення або комплекс програмно-апаратних засобів, які реалізовано на базі персонального комп'ютера. Модифікація програмного забезпечення мережі для шифрування та автентифікації трафіку, пристрій можна спільно використовувати з іншими клієнтами VPN, серверами VPN

або шлюзами безпеки VPN. Реалізація клієнта VPN — це програмне рішення, яке доповнює стандартну операційну систему - Windows 7/10 або Unix [13].

Сервер VPN у програмному чи апаратному вигляді є програмним забезпеченням безпеки, встановленої на комп'ютері, на якому запущена функція.

Сервер Сервер VPN захищає сервер від NDS і дозволяє організації Захищає підключення до окремих комп'ютерів і локальних сегментів Мережа, захищена відповідним продуктом VPN; Сервер VPN Функціональний аналог клієнтського продукту VPN для серверних платформ. Він має розширені ресурси для підтримки кількох підключень до Клієнт VPN. Він підтримує VPN-сервери з безпечними з'єднаннями з мобільні користувачі [20].

Шлюз безпеки VPN – це мережевий пристрій, який дві мережі, виконує функції шифрування та дозволити шлюзу безпеки VPN автентифікуватися на кількох хостах.Проходження Вкажіть адресу VPN Security Gateway як зовнішню адресу мережевого тунелю. Внутрішня адреса вхідних пакетів є специфічною хост за шлюзом. Шлюз безпеки VPN реалізований окремо програмне рішення та апаратний пристрій, наприклад маршрутизатор або мережеві екрани з можливостями VPN [20]. Відкрите зовнішнє середовище передачі інформації включає канали високошвидкісна передача даних з використанням Інтернету як використовується канал телефонної мережі. Визначення продуктивності VPN Ступінь безпеки інформації, що поширюється по відкритих каналах зв'язку.

Використовується для безпечної передачі даних по відкритих каналах зв'язку. інкапсуляція та тунелювання. За допомогою методів, які тунелюють пакети даних. для передачі по лініях загального користування. Між кожною парою «відправників» - одержувач», між «одержувачем» і «відправником» встановлюється логічний зв'язок, який може інкапсулювати дані з одного протоколу в пакети іншого протоколу. Тунелювання інкапсулює фрагмент даних, пакує його та надсилає. службові поля в новому конверті. Комплекти протоколів низького рівня Розміщується в полі пакетних даних протоколу верхнього рівня або еквівалентного протоколу Еквівалент Слід зазначити, що зробити тунелювання єдиним захистом найкраще як спосіб подолання ситуації, а не для захисту даних

від НСД і спотворень. Завдяки тунелюванню можна покращити KPI (початковий пакет). буде інкапсульований.Це необхідно для забезпечення конфіденційності переданих даних, відправник шифрує початковий пакет і пакує його у зовнішній пакет разом із новим пакетом IP-заголовок і відправляється через транзитну мережу (рис. 2.2) [8, 11].

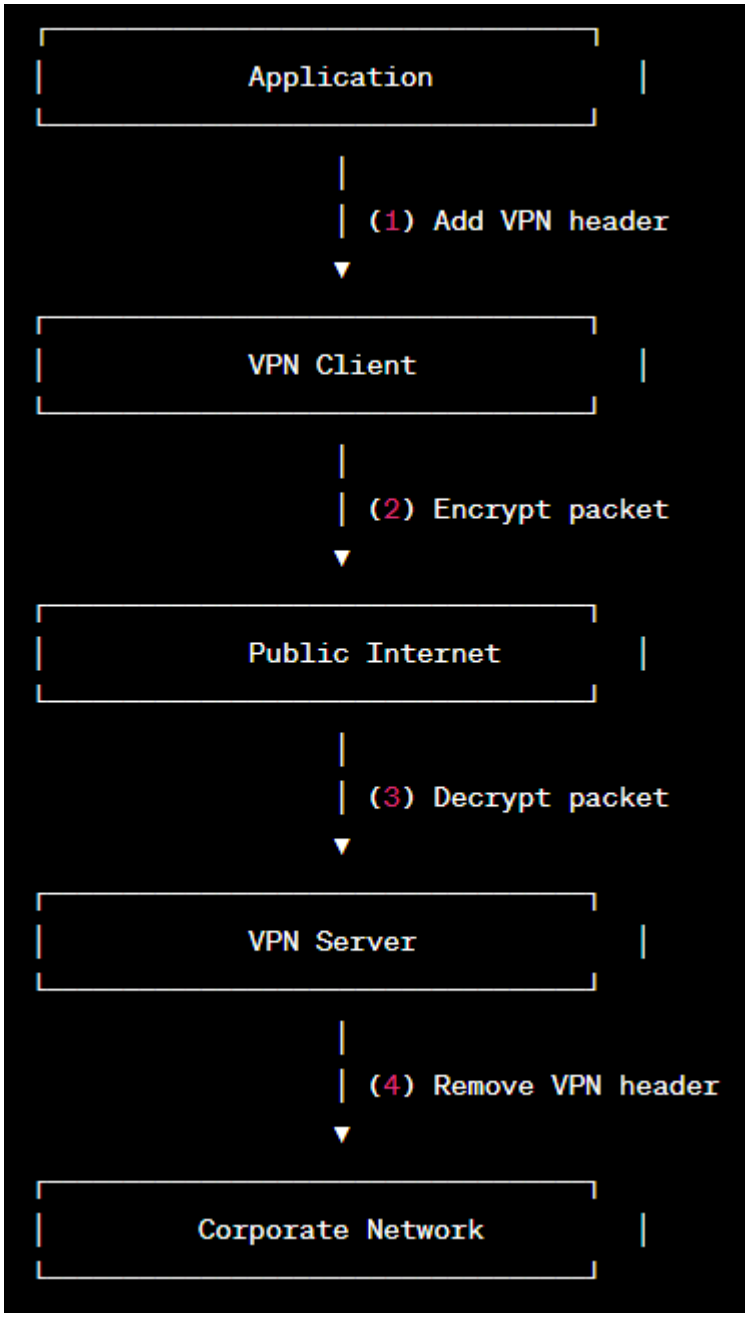

Рис. 2.2. Схема передачі пакету, підготовленого до тунелювання

Основна особливість технології тунелювання полягає у тому, що вона дозволяє захистити передачу даних від зовнішніх загроз, шляхом закладання

каналу зв'язку, що проходить через непевні мережі, наприклад, через Інтернет. Даний канал забезпечує конфіденційність, цілісність та автентичність передачі даних, що передаються. Також, технологія тунелювання може бути використана для підключення до мережі з віддаленої локації або віддаленого пристрою. Наприклад, якщо працівники компанії працюють з різних місць, вони можуть використовувати технологію VPN для забезпечення безпеки під час підключення до корпоративної мережі з будь-якого місця з Інтернетом.

Інкапсуляція використовується для захисту першого пакета і Тунелювання Перший пакет повністю зашифрований, а зашифрований пакет поміщається в інший зовнішній пакет, який відкривається. title Для подальшої передачі даних у відкритих мережах використовується відкрите поле заголовка у зовнішній упаковці [21].

Після того, як пакет буде доставлено, внутрішній насіннєвий пакет витягується і розшифровується та використовується для відновлення та подальшого передається у внутрішній мережі (рис. 2.3) [19].

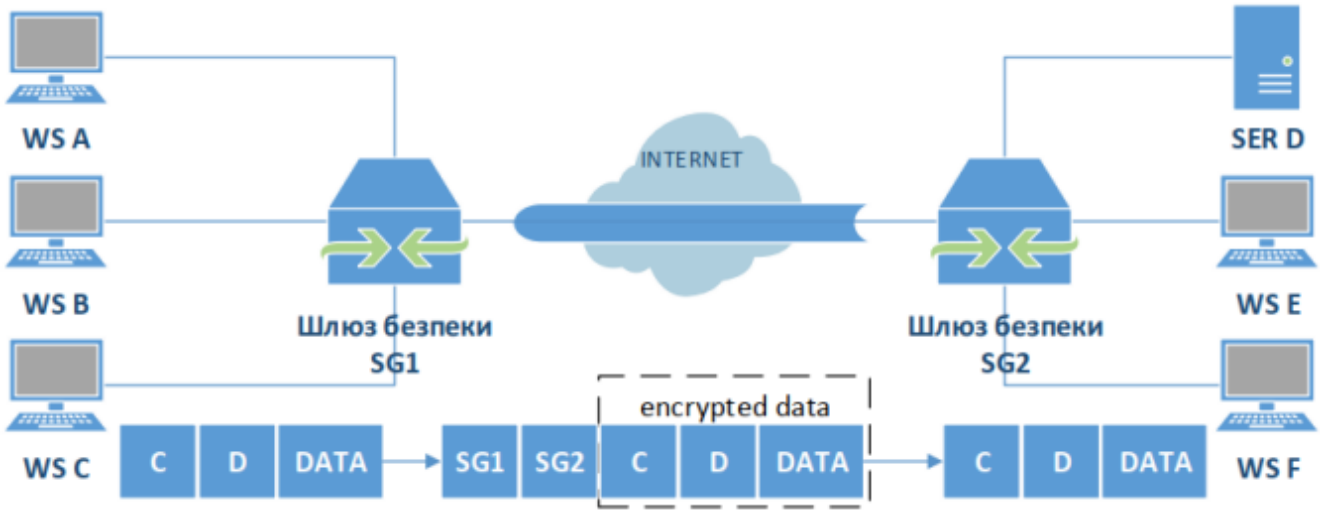

Рис. 2.3. Віртуальний захищений тунель

Тунелювання використовується для захисту конфіденційності та цілісності і автентичність даних пакета, тоді як КЕР поширюється на всі поля пакети Нарешті, щоб приховати структуру мережі між ними адреси, щоб запобігти можливим конфліктам. Локальна мережа При формуванні локальної мережі, яка не має

відношення до Інтернет, компанія використовує будь-яку IP-адресу для мережі пристроїв і комп'ютерів. Об’єднуючи раніше ізольовані мережі, ці адреси можуть конфліктувати між собою та з уже наявними адресами використовуються в Інтернеті [21].

Інкапсуляція пакетів вирішує цю проблему, оскільки вона може приховувати основна адреса плюс нова (унікальна) адреса. передача даних по віддалених мережах. Це також впливає на IP-адреси та інші налаштування мобільних користувачів, які підключаються до локальної мережі [20]. Механізми тунелювання використовуються в різноманітних протоколах Формування захисних водотоків Тунелі утворюються тільки на території Відкрита мережа, де конфіденційність і цілісність можуть бути порушені даних, між входом у відкритий Інтернет і входом у СМ. в з цієї причини граничні адреси використовуються для зовнішніх пакетів. Внутрішня адреса останнього з роутерів, встановлених на двох node зберігається в захищеному вигляді в початковому пакеті всередині. Зверніть увагу, що сам механізм тунелювання не залежить від методу Тунелювання використовується для Забезпечення конфіденційності та цілісності переданої частини даних, організація міграції між мережами з різними протоколами [4, 15].

VPN-тунелі формуються для різних типів кінцевих користувачів - це Локальні локальні мережі зі шлюзами безпеки або окремі віддалені комп’ютери або мобільних користувачів для створення віртуальної приватної мережі. Більшим організаціям може знадобитися використання шлюзу VPN, сервера VPN або VPN. VPN-шлюзи клієнтів використовуються для захисту локальної мережі організації, Сервер VPN і клієнт VPN використовуються для налаштування безпечної організації. З’єднання СМ з віддаленими та мобільними користувачами через Інтернет [16, 17].

Після розробки VPN можна розділити на дві схеми віртуальні канали захисту [4, 19] між:

1) Локальна мережа (канал LVSLVS);

2) Вузол і локальна мережа (рис. 2.4).

Схема 1 – дає можливість замінити дорогі виділені лінії між вузлами та локальними мережами. сформувати безпечний канал, доступний між ними окремими організаціями. У цьому випадку шлюз безпеки діє як інтерфейс між тунелем і користувачі локальної мережі використовують тунель. спілкуватися один з одним. Компанії можуть використовувати свого роду VPN як альтернативу або додавання глобальних мережевих підключень, таких як Frame Relay [20].

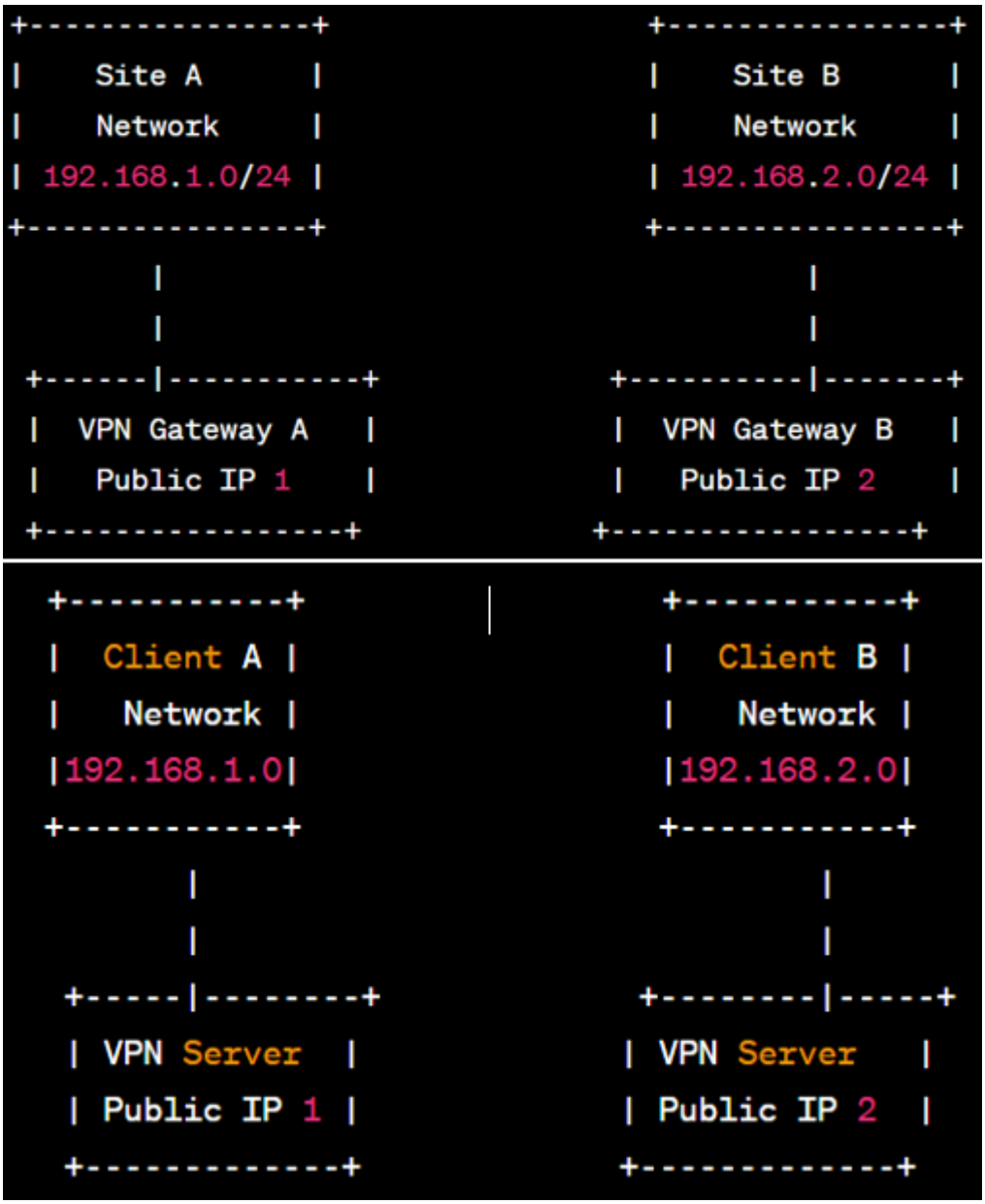

Рис. 2.4. Віртуальні захищені канали типу Мережа – Мережа, Клієнт – Клієнт

Схема 2 – Призначення та встановлення безпечного каналу VPN. Увімкніть підключення до віддалених і мобільних користувачів. Формування тунелю

ініціюється клієнтом. Під час спілкування зі шлюзом, який захищає віддалену мережу, і саме він запускає спеціальне програмне забезпечення для користувача на комп'ютері користувача. Цей тип VPN замінює комутоване підключення та може бути таким використовувати в поєднанні з традиційними методами віддаленого доступу [27, 19]. Як різновид методу віртуального захищеного каналу формується віртуальний захищений канал, що належить до кінцевої або проміжної точки. захищеного потоку повідомлень [18].

У обох випадках з'єднання між мережами або клієнтами здійснюється через Інтернет за допомогою віртуальної захищеної мережі (VPN). Це забезпечує безпеку передачі даних та дозволяє зберігати конфіденційну інформацію.

Захищені тунелі утворюються компонентами віртуальної мережі, які є функція, для якої формується тунель, і ці компоненти називаються ініціаторами і тунельні термінатори [12]. Ініціатор тунелю інкапсулює початковий пакет у новий пакет. містить заголовок з інформацією про відправника та одержувача. пакет, інкапсульований протокол може належати до будь-якого типу протоколу, містять пакети протоколу, які не підлягають маршрутизації. Всі пакети, які є надсилаються в тунель, і це IP-пакети. Маршрут до ініціатора є кінець тунелю визначає звичайну IP-мережу, яка маршрутизується відрізняється від Інтернету [12].

Різні мережеві пристрої мають право ініціювати та завершувати тунель, а також програмний ініціатор може бути наданий маршрутизаторам у локальній мережі. відповідну функцію. Закінчення тунелю. виконується мережевим комутатором або шлюзом постачальника послуг [12]. Термінатор тунелю виконує процес, зворотний інкапсуляції. Саме він видаляє новий заголовок і надсилає кожен пакет окремо одержувача в локальній мережі [12]. Конфіденційність пакета забезпечується шифруванням, цілісністю і надійності здійснюються в процесі формування КЕП.

Методів багато і KZI алгоритми, в яких ініціатор і термінатор тунелю погоджуються один з одним один і використовувати однакові методи й алгоритми захисту.

Висновки до другого розділу

Досліджено систему керування ІС мережі, яка забезпечує наскрізну безпеку VPN сервісів. Система також забезпечує високий рівень безпеки та управління VPN розповсюдження ключів шифрування та сертифікатів захищено. Централізована координація та управління захищеними КМ ІС.

Виокремлено IPSec як основний протокол для забезпечення безпеки передачі даних між двома пристроями та мережею. Застосування протоколу L2TP через IPSec до якого застосовується тип доступу користувача VPN завжди підключений до СМ і з високим рівнем безпеки, між користувачам і співробітникам надається повний доступ до мережі. Для швидкого розгортання мереж VPN і тимчасових підключень середня безпека даних із протоколом SSL підвищує рівень безпеки за рахунок поєднання SSL і IPSec.

3 РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ OPENVPN

3.1. Способи захисту мережі з використанням VPN

Від безпеки залежать і пріоритети захисту інформаційних ресурсів Дані, пов’язані з корпоративними користувачами та користувачами даних про продуктивність В результаті перехоплення інформації може постраждати організація отримання спаму або блокування серверів [14].

Багато програмних продуктів і інструментів пропонують можливість зберігання інформації в Інтернеті від віртуальних атак зловмисників у зручному та ефективний у захисті інформації. Необхідно використовувати VPN [14].

Із зростанням сучасних організацій зростають і їхні потреби в інформації. Кількість пристроїв обробки інформації зростає з кожним роком, тому важливо бути об'єднані в мережу разом. Розвиток комп'ютерних мереж супроводжується підвищений інформаційний ризик. Загрозою в цьому випадку є маніпуляція трафіку в процесі передачі в мережі. Тому є потреба розвиватися є способом протидії цій загрозі [18, 21].

Залежно від використання та призначення протоколу VPN пропонує три типи підключень [18, 21]:

- вузол-вузол
- вузол мережі;
- мережа.

VPN складається з таких частин [18, 21]:

- «внутрішня» мережа (може бути більше однієї);
- «зовнішня» мережа (унікальна інкапсуляція).

Окремі комп'ютери підключені до віртуальної мережі Підключення може здійснюватися як всередині, так і за межами компанії за допомогою сервера доступу. Мережа для підключення віддалених користувачів сервер доступу

вимагає процесу ідентифікації та автентифікації. Після того обидва процеси успішно завершені, віддалений користувач виконати процес авторизації для роботи в мережі [18, 21].

3.2. Встановлення та налаштування міжмережевого тунелю OpenVPN Server

OpenVPN — це рішення віртуальної приватної мережі (VPN), яке надається в репозиторіях Ubuntu. Він гнучкий, надійний і безпечний. Він належить до сімейства стеків SSL/TLS VPN (на відміну від IPSec VPN). У цьому розділі описано встановлення та налаштування OpenVPN для створення VPN.

Встановлення сервера

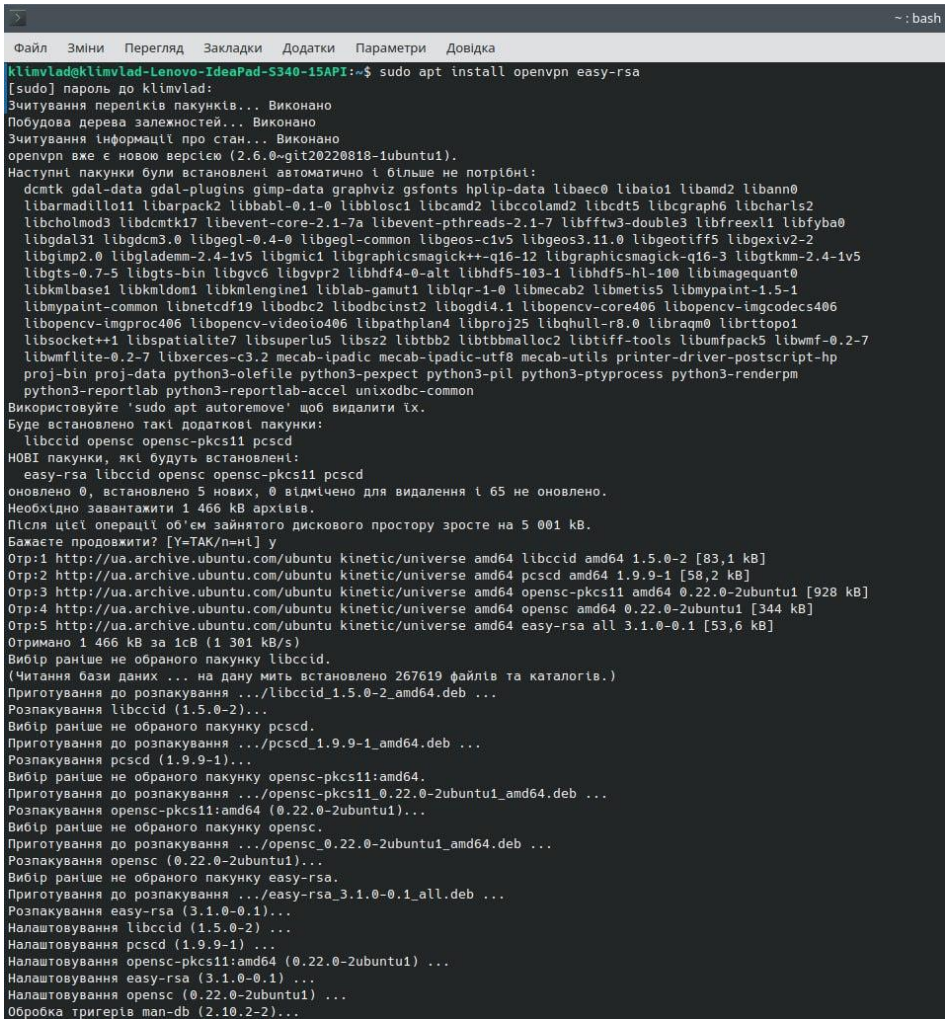

Рис. 3.1. Встановлення серверу OpenVPN

Першим кроком у налаштуванні конфігурації OpenVPN є створення PKI (інфраструктури відкритих ключів). CPI включають:

- Окремий сертифікат (також відомий як відкритий ключ) і закритий ключ для сервера та кожного клієнта.
- Кореневий сертифікат центру сертифікації (CA) і ключі, які використовуються для підпису сертифікатів сервера та клієнта.

OpenVPN підтримує взаємну автентифікацію на основі сертифікатів, тобто клієнт повинен автентифікувати сертифікат сервера, а сервер повинен автентифікувати сертифікат клієнта для встановлення взаємної довіри.

Сервер і клієнт роблять це, спочатку перевіряючи, що представлений сертифікат підписаний кореневим центром сертифікації (CA), а потім перевіряючи інформацію в заголовку автентифікованого сертифіката, наприклад загальну назву сертифіката або тип сертифіката (клієнт або сервер).) інша сторона).

Налаштування центру сертифікації

Щоб налаштувати власний центр сертифікації та створити сертифікати та ключі для сервера OpenVPN і кількох клієнтів, спочатку скопіюймо каталог ***easy-rsa*** до ***/etc/openvpn.conf***. Це гарантує, що нічого в сценарії не буде втрачено під час оновлення пакетів Change. З терміналу запускаємо:

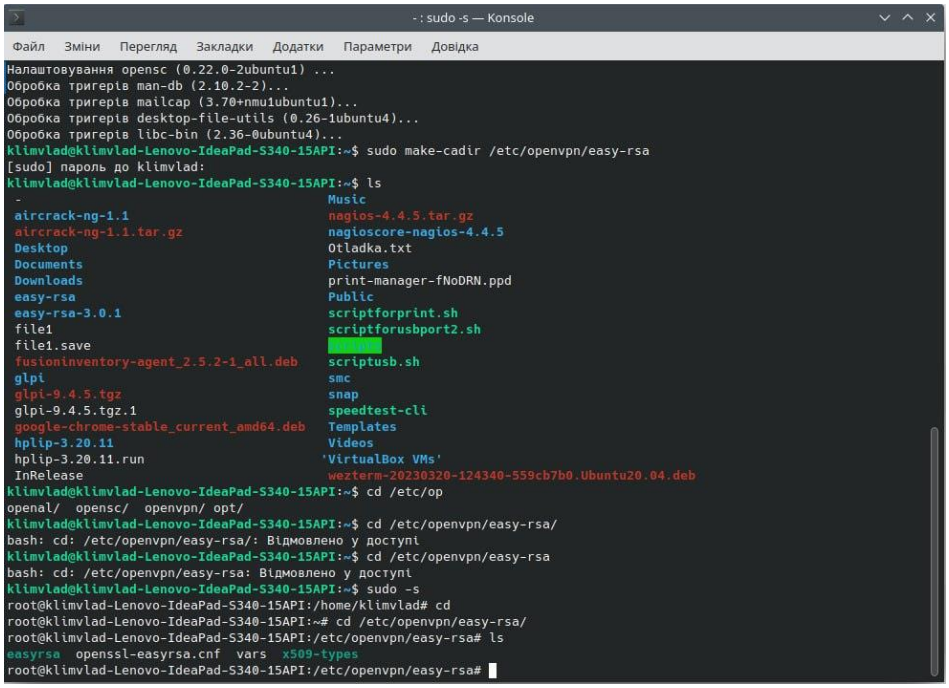

Рис. 3.2. Налаштування центру сертифікації

```
klimvlad@klimvlad-Lenovo-IdeaPad-S340-15API:~$ sudo ufw status
Стан: активний

До                         Дія         З
--                         ---         -
Apache                     ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere
993/tcp                    ALLOW       Anywhere
1194/tcp                   ALLOW       Anywhere
Apache (v6)                ALLOW       Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)
993/tcp (v6)               ALLOW       Anywhere (v6)
1194/tcp (v6)              ALLOW       Anywhere (v6)

klimvlad@klimvlad-Lenovo-IdeaPad-S340-15API:~$ sudo ufw enable
Брандмауер є активним і буде запускатися разом з системою
klimvlad@klimvlad-Lenovo-IdeaPad-S340-15API:~$ sudo ufw status
Стан: активний

До                         Дія         З
--                         ---         -
Apache                     ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere
993/tcp                    ALLOW       Anywhere
1194/tcp                   ALLOW       Anywhere
Apache (v6)                ALLOW       Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)
993/tcp (v6)               ALLOW       Anywhere (v6)
1194/tcp (v6)              ALLOW       Anywhere (v6)

klimvlad@klimvlad-Lenovo-IdeaPad-S340-15API:~$
```

Рис. 3.3. Налаштування правил фаєрволу

Другим кроком є створення інфраструктури відкритих ключів (Public Ключова інфраструктура, PKI) за допомогою команди «***./easyrsa init-pki***». тому Виконайте команду для створення каталогу ***/home/ershuev/easy-rsa/pki***, де Розташована інфраструктура відкритих ключів PKI (рис. 3.3).

Наступним кроком є створення концентратора за допомогою команди build-ca сертифікований. Завданням центру є видача підписаних сертифікатів і Клієнт OpenVPN.

Щоб отримати сертифікат, сервер або клієнт на своєму хості створює файл Запит на сертифікат. Цей файл запиту надсилається на хост CA, Він створює сертифікат і підписує його.

Потім підписаний сертифікат передається на хості. Закритий ключ генерується одночасно із запитом на сертифікат. приватний для всіх вузлів мережі OpenVPN, центрів сертифікації, сервер і всі клієнти OpenVPN. Щоб бути в безпеці, ключові файли ніколи не повинні Залиште вузли там, де вони були створені.

```
klimvlad@klimvlad-Lenovo-IdeaPad-S340-15API:~$ ln -s /usr/share/easy-rsa/* ~/easy-rsa/
ln: не вдалося створити символічне посилання '/home/klimvlad/easy-rsa/easyrsa': Файл вже існує
ln: не вдалося створити символічне посилання '/home/klimvlad/easy-rsa/openssl-easyrsa.cnf': Файл вже існує
ln: не вдалося створити символічне посилання '/home/klimvlad/easy-rsa/vars.example': Файл вже існує
ln: не вдалося створити символічне посилання '/home/klimvlad/easy-rsa/x509-types': Файл вже існує
klimvlad@klimvlad-Lenovo-IdeaPad-S340-15API:~$ cd /etc/openvpn/easy-rsa/
bash: cd: /etc/openvpn/easy-rsa/: Відмовлено у доступі
klimvlad@klimvlad-Lenovo-IdeaPad-S340-15API:~$ cd ./easy-rsa
klimvlad@klimvlad-Lenovo-IdeaPad-S340-15API:~/easy-rsa$ ls
ChangeLog   doc      gpl-2.0.txt  openssl-easyrsa.cnf  README.quickstart.md  x509-types
COPYING.md  easyrsa  mktemp.txt   README.md            vars.example
klimvlad@klimvlad-Lenovo-IdeaPad-S340-15API:~/easy-rsa$ ./easyrsa init-pki

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /home/klimvlad/easy-rsa/pki

klimvlad@klimvlad-Lenovo-IdeaPad-S340-15API:~/easy-rsa$
```

Рис. 3.4. Налаштування каталогу PKI

Щоб створити пару відкритих і закритих кореневих ключів для центру сертифікації, команду ***./easy-rsa*** потрібно запустити знову, але вже з опцією ***build-ca*****.** Використаємо пароль **- *Sqrt218ff*.**

Для ЦС команда build-ca створить два файли;

– ***/home/ca/easy-rsa-master/easyrsa3/pki/private/ca.key***;

– ***/home/ca/easy-rsa-master/easyrsa3/pki/ca.crt***.

Файл ca.key є закритим ключем центру сертифікації, він секретний і не можуть бути передані на інші вузли в поточній мережі. файл сертифіката ca.crt, інакше він відкритий і запитуватиметься на клієнтських і серверних вузлах OpenVPN.

```
klimvlad@klimvlad-Lenovo-IdeaPad-S340-15API:~/easy-rsa$ ./easyrsa build-ca

Using SSL: openssl OpenSSL 3.0.5 5 Jul 2022 (Library: OpenSSL 3.0.5 5 Jul 2022)

Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
Can't load /home/klimvlad/easy-rsa/pki/.rnd into RNG
4007769F317F0000:error:12000079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:106:F
ilename=/home/klimvlad/easy-rsa/pki/.rnd
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:Smart12

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

klimvlad@klimvlad-Lenovo-IdeaPad-S340-15API:~/easy-rsa$
```

Рис. 3.5. Конфігурація та налаштування ЦС

Далі нам потрібно створити запит на сертифікат сервера та ключ, опція ./easyrsa gen-req myservername згенерує цей запит. Потрібно переконатися, що ім’я сервера (загальне ім’я під час запуску сценарію) є унікальним. Можна використовувати параметр no pass, який означає відсутність небхідності імпортувати пароль, але в нашому випадку відтворимо запит на пароль,а також на ім’я сервера OpenVPN (рис. 3.5.). Буде створено два нові файли server.req та server.key.

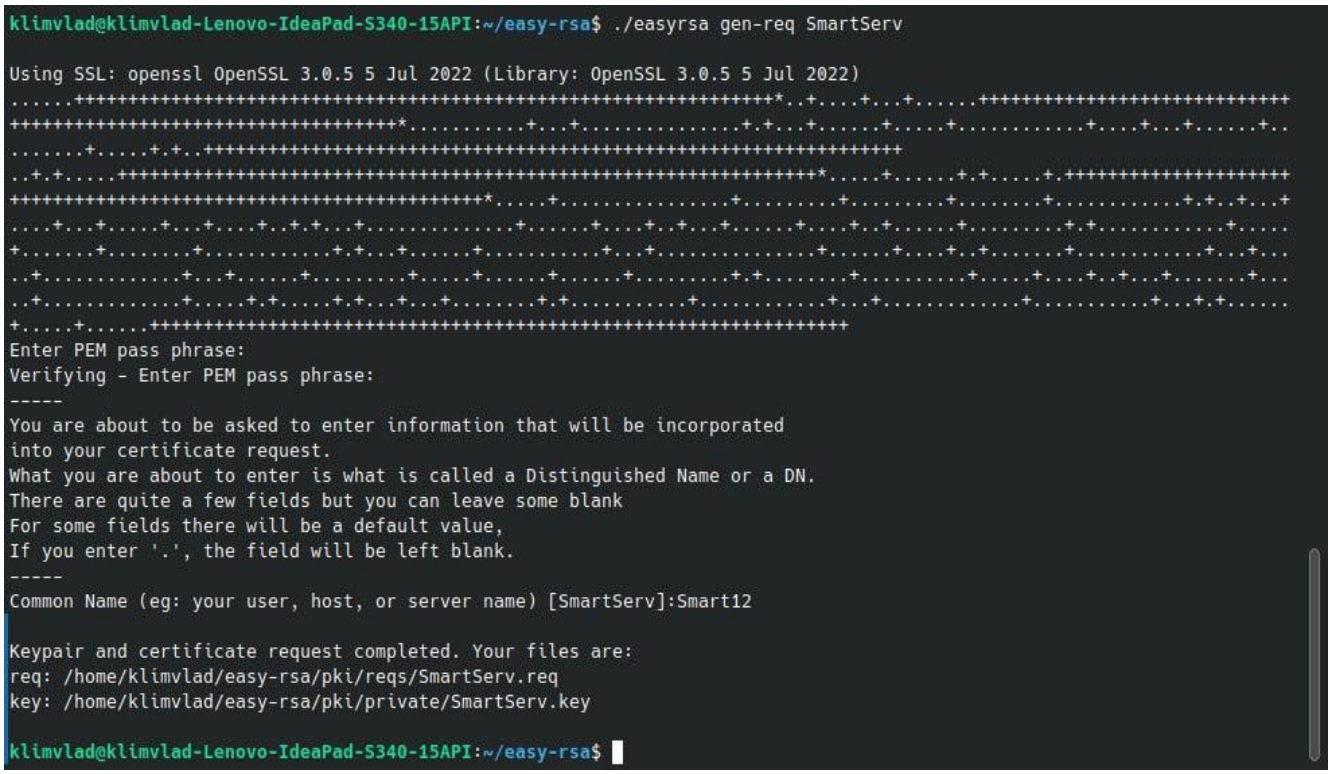

Рис. 3.6. Генерування запиту та приватного ключа серверу

Перший із цих файлів потрібно передати на сервер ЦС, а не секрет. Другий файл є конфіденційним і не повинен виходити за межі сервера Відкрити VPN. Створюємо запит на сертифікат для сервера та після генеруємо сам сертифікат.

** після введення команди підтверджуємо правильність даних, ввівши «**yes**» та вводимо пароль, який вказували при створенні кореневого сертифіката.*

** **nopass** можна упустити, якщо хочемо підвищити безпеку за допомогою пароля на сертифікат.*

```
klimvlad@klimvlad-Lenovo-IdeaPad-S340-15API:~/easy-rsa$ ./easyrsa sign-req server SmartServ

Using SSL: openssl OpenSSL 3.0.5 5 Jul 2022 (Library: OpenSSL 3.0.5 5 Jul 2022)


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 1080 days:

subject=
    commonName                = Smart12


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /home/klimvlad/easy-rsa/pki/safessl-easyrsa.cnf
Enter pass phrase for /home/klimvlad/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'Smart12'
Certificate is to be certified until Apr 22 19:28:26 2026 GMT (1080 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /home/klimvlad/easy-rsa/pki/issued/SmartServ.crt
```

Рис. 3.7. Створення запиту на отримання сертифікату ЦС

VPN-клієнту також знадобиться сертифікат для автентифікації на сервері. Як правило, для кожного клієнта створюється окремий сертифікат.

Це можна зробити на сервері (як ключ і сертифікат вище), а потім безпечно розповсюдити клієнту. Або навпаки: клієнт може зробити і надіслати запит, який відправляється і підписується сервером.

Потрібно підготувати сертифікат і ключ для клієнта OpenVPN. Сертифікат клієнта та запит на закритий ключ генеруються ***./easyrsa gen-req*** клієнта nopass, де використовується параметр «**nopass**», щоб уникнути необхідності вводити пароль.

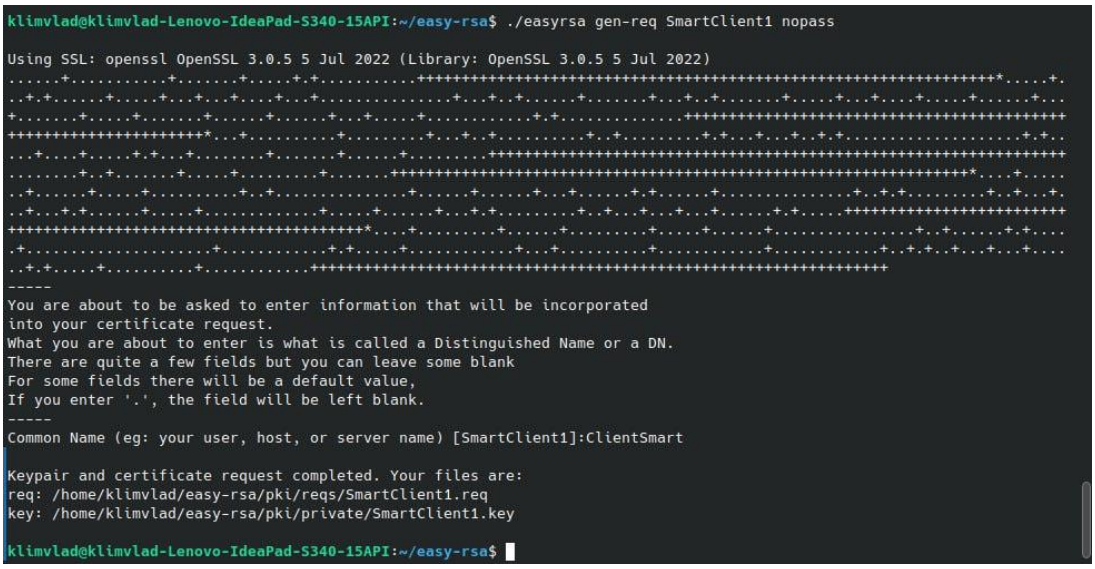

Рис. 3.8. Генерування клієнтського сертифікату без паролю

Тепер потрібно підписати запит на отримання сертифікату для нашого клієнта командою – ./easyrsa sign-req client SmartClient1

Після введення підтвердження та пароля буде згенеровано закритий ключ сертифікат. Ми маємо файл закритого ключа робочої станції client.key і Файл сертифіката Client.crt, підписаний ЦС.

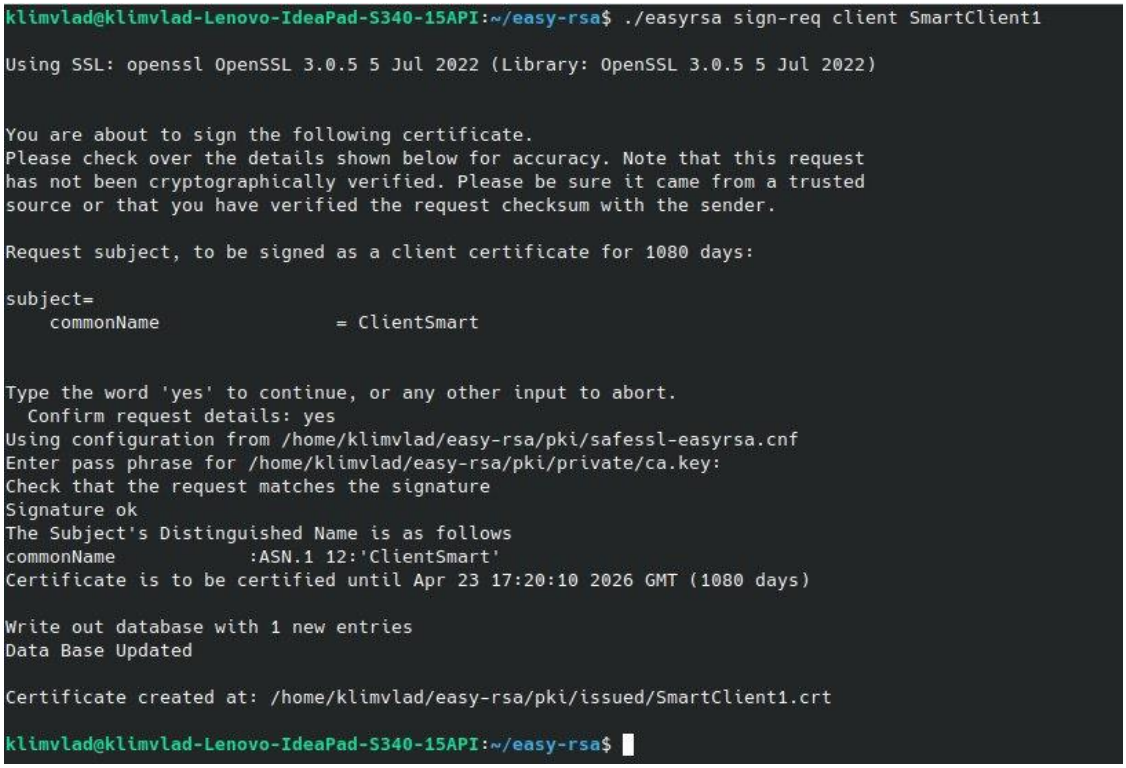

Рис. 3.9. Підписання клієнтського сертифікату без паролю

Далі потрібно згенерувати файл Діффі-Хелмана (Diffie-Hellman) необхідний реалізації однойменного протоколу, що дозволяє використовувати небезпечний канал для отримання загального секретного ключа. Цей ключ буде використовуватися для захищеного обміну даними за допомогою алгоритмів симетричного шифрування.

У застосуванні до OpenVPN файл Діффі-Хелмана потрібен для забезпечення захисту трафіку від розшифровки, якщо ключі були викрадені. Тут мається на увазі той трафік, записаний і збережений ще до викрадення ключів. Файл Діффі-Хелмана створюється на сервері OpenVPN.

Для того щоб створити ключ Діффі-Хелмана (Diffie-Hellman) потрібно використати команду ***./easyrsa gen-dh***. Після створення ключа, ми отпримаємо повідомлення – «Генерація параметрів DH, 2048-бітне безпечне просте число».

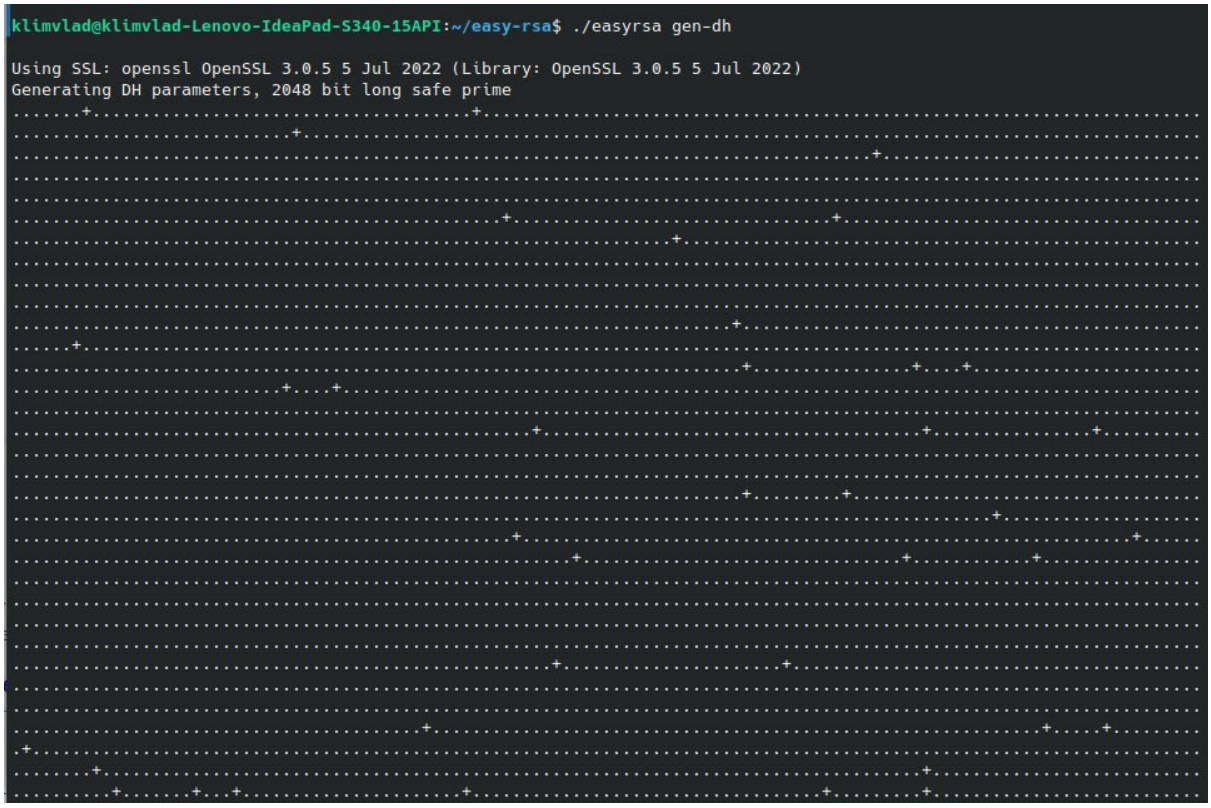

Рис. 3.10. Створення ключа Діффі-Хелмана (Diffie-Hellman)

Всі сертифікати і ключі були згенеровані в підкаталогах. Звичайною практикою є копіювання їх у ***/etc/openvpn/***:

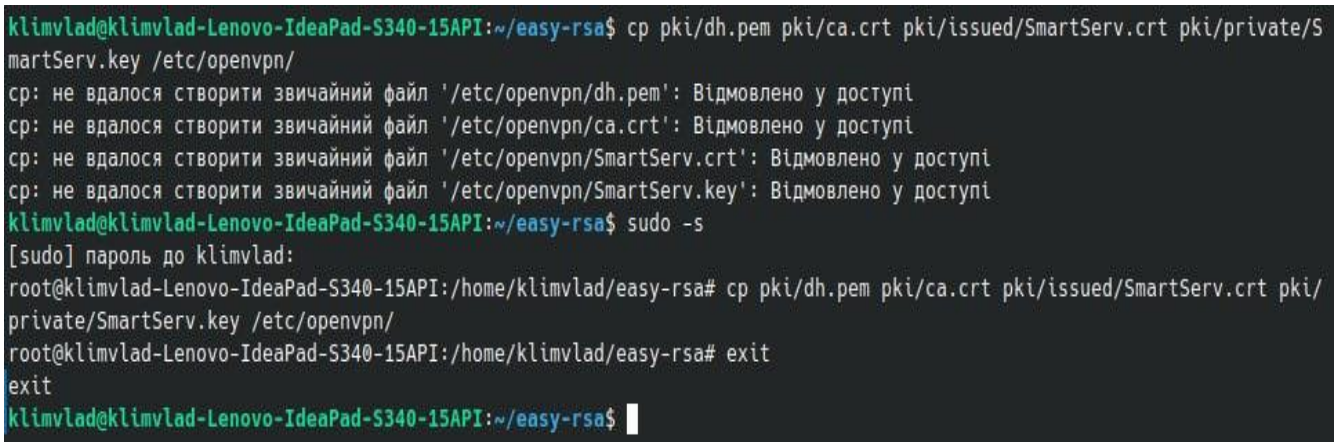

Рис. 3.11. Копіювання файлів в /etc/openvpn/

Тепер нам потрібно сконфігурувати наш сервер. Почнемо з копіювання та розпакування ***server.conf.gz*** до ***/etc/openvpn/server.conf***.

Необхідний файл конфігурації OpenVPN знаходиться в ***/usr/share/doc/openvpn/examples/sample-config-files/***. У ньому потрібно налаштувати деякі параметри. Найважливіше це порт і прото - порт і протокол, з якими буде працювати програма.

Цей файл потрібно редагувати щоб переконатися, що наведені нижче рядки вказують на сертифікати та ключі, які створені вище ***./etc/openvpn/myserver.conf.***

Наші ключі зберігаються на шляху ***/etc/openvpn***, тому до них можна не прописувати повний шлях:

- ca ca.crt
- cert SmartServ.crt
- key SmartServ.key
- dh dh2048.pem

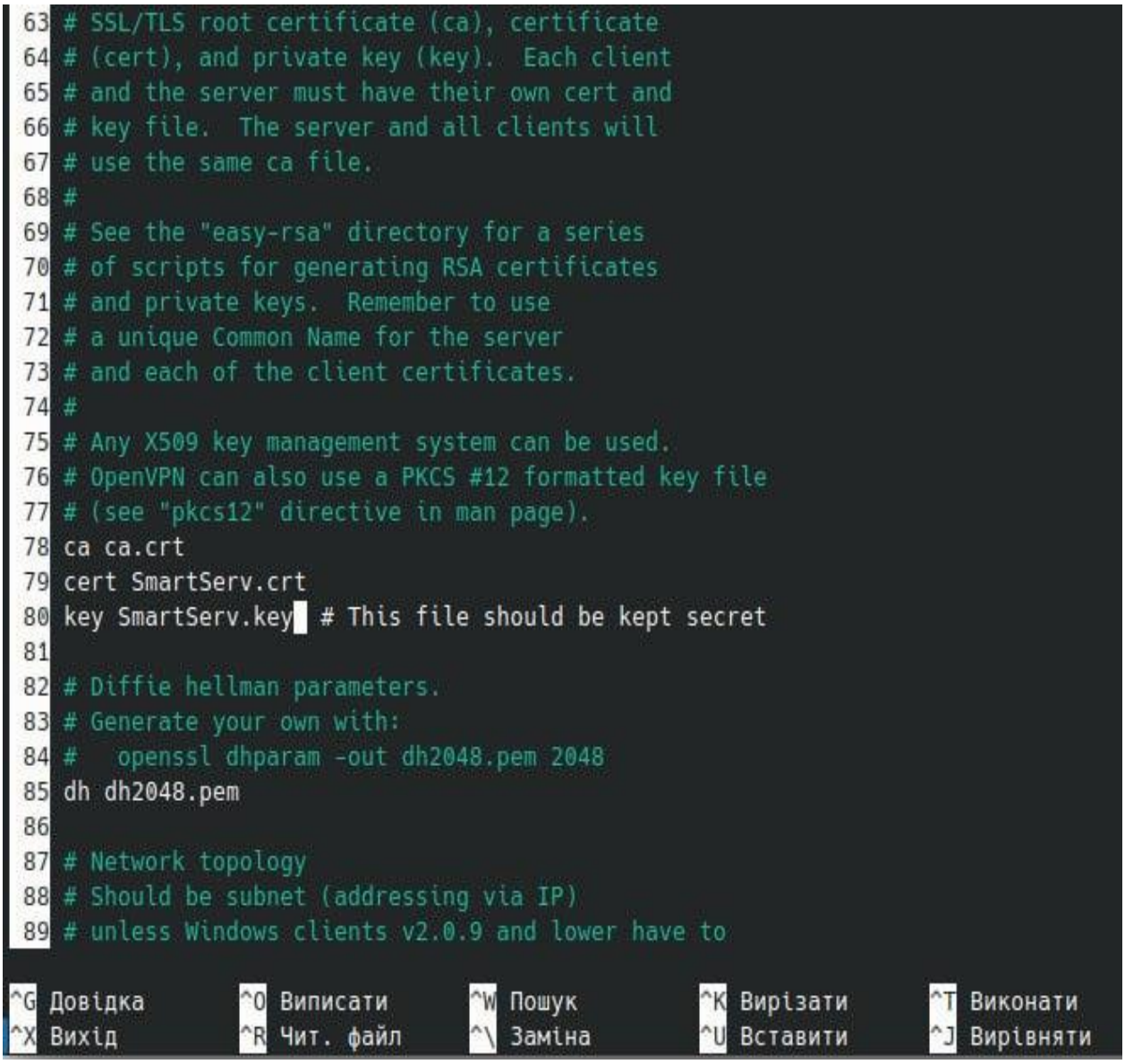

Рис. 3.12. Налаштування файлу конфіграції серверу

Налаштовуємо діапазон адрес для віртуальної мережі, наш сервер буде доступний по першому з них – 10.8.0.1. Після завершення налаштування потрібно зберегти зміни у файлі.

Налаштування сервера OpenVPN завершено. Далі потрібно запустити OpenVPN сервер. Це можна зробити прямо з командного рядка, просто вказати адресу конфігураційного файлу sudo openvpn /etc/openvpn/server.conf.

Повідомлення Initialization Sequence Completed на рисунку 3.11 значить, що все добре і сервер запустився

```
klimvlad@klimvlad-Lenovo-IdeaPad-S340-15API:/etc/openvpn$ sudo openvpn /etc/openvpn/server/server.conf
2023-05-09 00:31:14 WARNING: --topology net30 support for server configs with IPv4 pools will be removed in a future release. P
lease migrate to --topology subnet as soon as possible.
2023-05-09 00:31:14 Note: Kernel support for ovpn-dco missing, disabling data channel offload.
2023-05-09 00:31:14 OpenVPN 2.6_git x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2023-05-09 00:31:14 library versions: OpenSSL 3.0.5 5 Jul 2022, LZO 2.10
2023-05-09 00:31:14 net_route_v4_best_gw query: dst 0.0.0.0
2023-05-09 00:31:14 net_route_v4_best_gw result: via 192.168.0.1 dev wlp2s0
2023-05-09 00:31:14 NOTE: your local LAN uses the extremely common subnet address 192.168.0.x or 192.168.1.x.  Be aware that th
is might create routing conflicts if you connect to the VPN server from public locations such as internet cafes that use the sa
me subnet.
2023-05-09 00:31:14 Diffie-Hellman initialized with 2048 bit key
 Enter Private Key Password: *********
2023-05-09 00:31:20 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2023-05-09 00:31:20 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
2023-05-09 00:31:20 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
2023-05-09 00:31:20 net_route_v4_best_gw query: dst 0.0.0.0
2023-05-09 00:31:20 net_route_v4_best_gw result: via 192.168.0.1 dev wlp2s0
2023-05-09 00:31:20 ROUTE_GATEWAY 192.168.0.1/255.255.255.0 IFACE=wlp2s0 HWADDR=e8:d0:fc:ee:cd:b3
2023-05-09 00:31:20 TUN/TAP device tun0 opened
2023-05-09 00:31:20 net_iface_mtu_set: mtu 1500 for tun0
2023-05-09 00:31:20 net_iface_up: set tun0 up
2023-05-09 00:31:20 net_addr_ptp_v4_add: 10.8.0.1 peer 10.8.0.2 dev tun0
2023-05-09 00:31:20 net_route_v4_add: 10.8.0.0/24 via 10.8.0.2 dev [NULL] table 0 metric -1
2023-05-09 00:31:20 Could not determine IPv4/IPv6 protocol. Using AF_INET
2023-05-09 00:31:20 Socket Buffers: R=[212992->212992] S=[212992->212992]
2023-05-09 00:31:20 UDPv4 link local (bound): [AF_INET][undef]:1194
2023-05-09 00:31:20 UDPv4 link remote: [AF_UNSPEC]
2023-05-09 00:31:20 MULTI: multi_init called, r=256 v=256
2023-05-09 00:31:20 IFCONFIG POOL IPv4: base=10.8.0.4 size=62
2023-05-09 00:31:20 IFCONFIG POOL LIST
2023-05-09 00:31:20 Initialization Sequence Completed
```

Рис.3.13. Запуск серверу openVPN

Тепер підключимося до нашого серверу через протокол SFTP та викачаємо сертифікати, які необхідні для запуску клієнтського файлу конфігурацію.

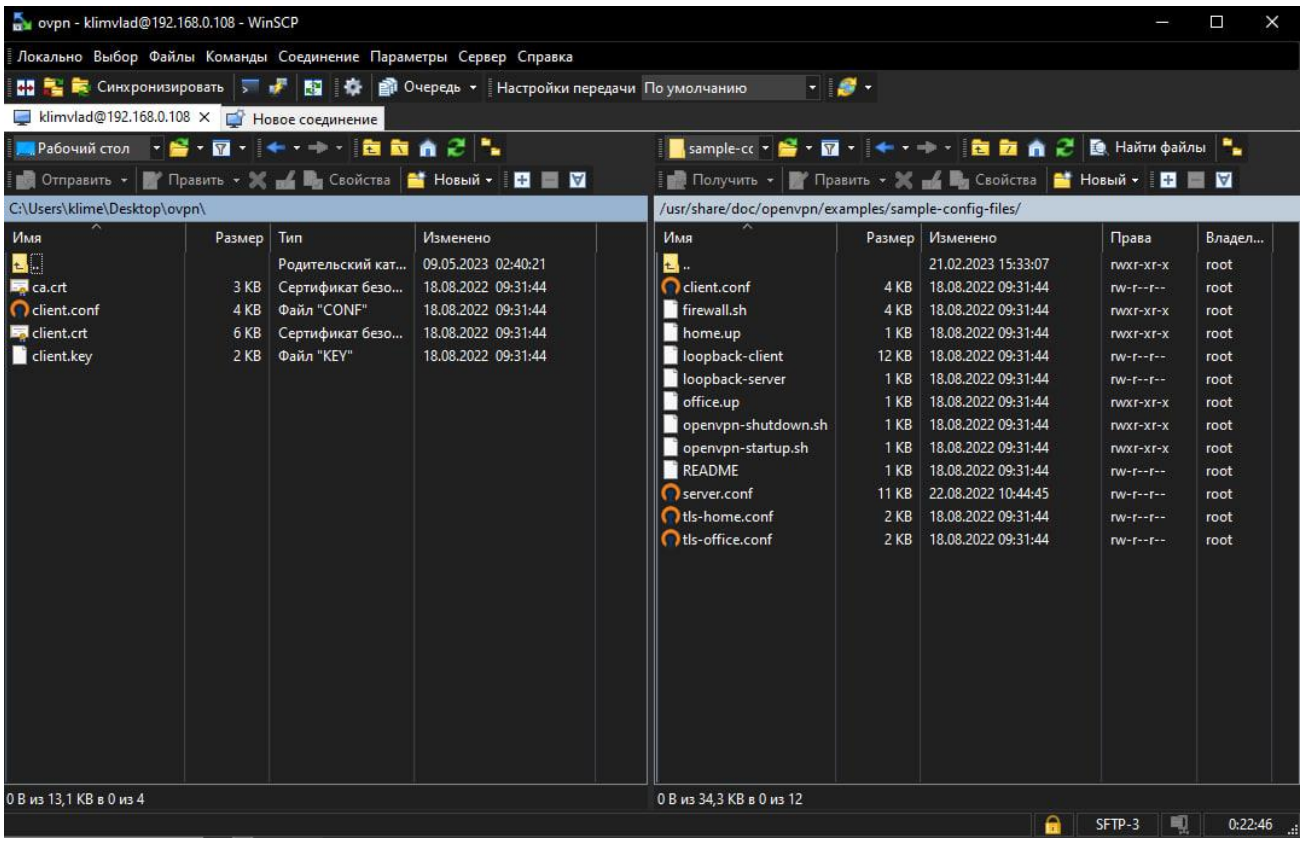

Рис.3.14. Пересилка клієнтських сертифікатів через WinSCP

Потрібно перевірити підключення, встановити клієнт OpenVPN на нашу клієнтську машину, та вибрати необхідний файл конфігурації.

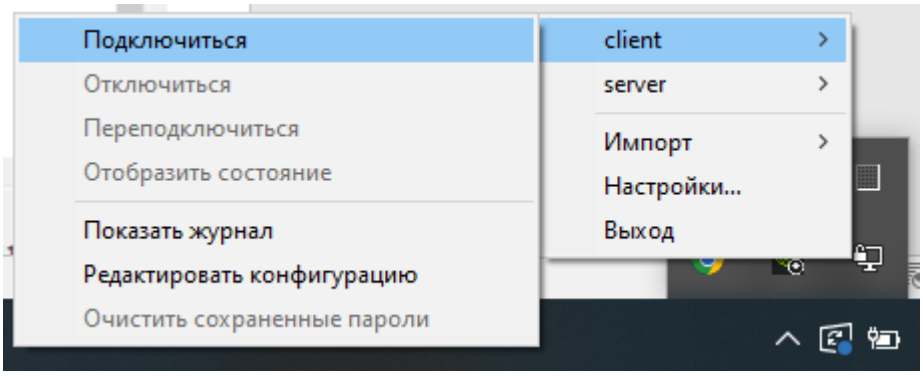

Рис.3.15. Імпортування фалу конфігурації в GUI

Як можемо побачити на рисунку 3.16, що наш клієнт підключений до нашого серверу та ініціалізація вдала.

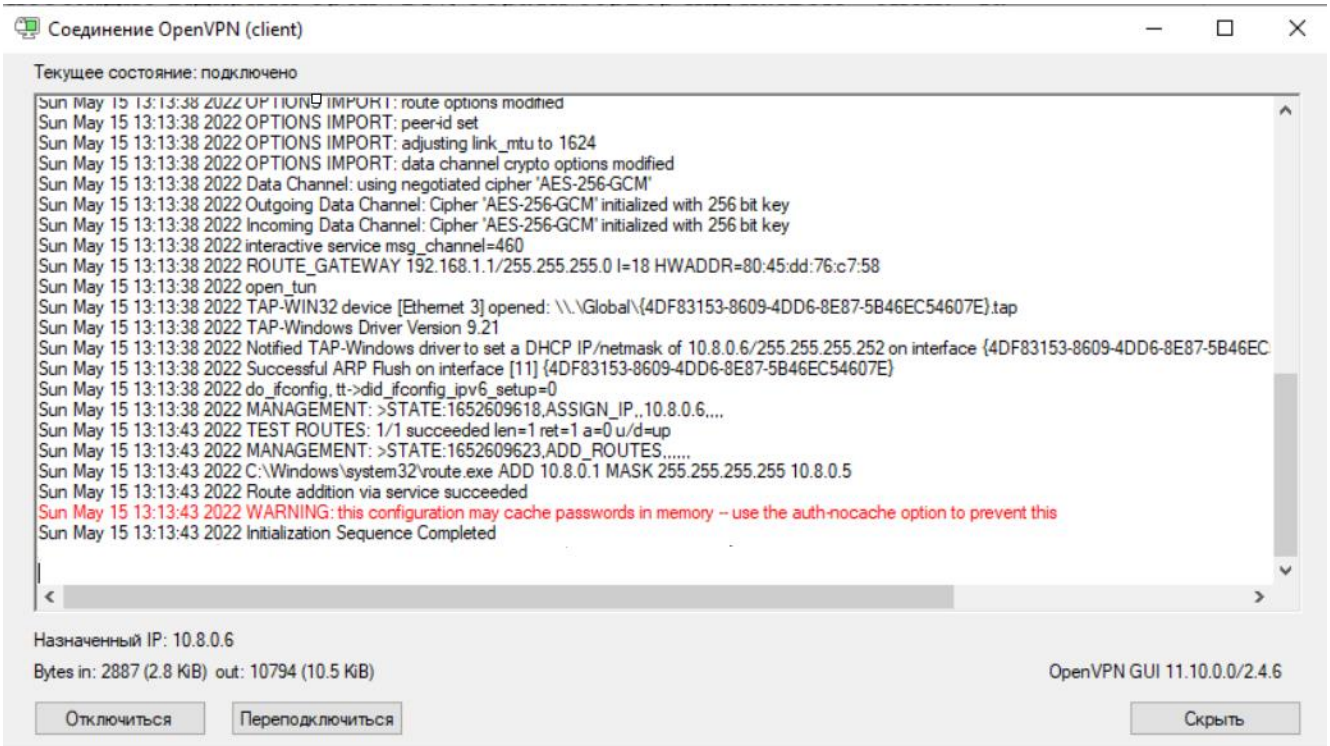

Рис.3.16. Підключення до нашого серверу OpenVPN

3.3 Рекомендації щодо підвищення безпеки сервера OpenVPN

1. Використовуйте надійну автентифікацію: OpenVPN підтримує кілька методів автентифікації, таких як ім’я користувача/пароль, автентифікація на основі

сертифіката та двофакторна автентифікація. Використання надійної автентифікації може допомогти запобігти несанкціонованому доступу до VPN.

2. Увімкнути шифрування: OpenVPN підтримує різні алгоритми шифрування. Рекомендується використовувати надійні алгоритми шифрування, такі як AES або Camellia, щоб захистити трафік VPN від перехоплення.

3. Використовуйте безпечний протокол: OpenVPN підтримує як протоколи UDP, так і TCP. UDP є швидшим, але TCP надійніший і може допомогти запобігти втраті пакетів.

4. Запровадити контроль доступу: запровадити механізми контролю доступу, щоб обмежити доступ до сервера VPN. Це можна зробити, налаштувавши правила брандмауера, обмеживши кількість одночасних підключень або налаштувавши сертифікати клієнта VPN.

5. Регулярно оновлюйте програмне забезпечення та застосовуйте виправлення: обов’язково оновлюйте OpenVPN та будь-яке інше програмне забезпечення, що використовується на сервері VPN, і застосовуйте виправлення безпеки, щойно вони стануть доступними.

6. Використовуйте брандмауер VPN: використовуйте брандмауер VPN, щоб захистити сервер VPN від зовнішніх атак і застосувати політики безпеки. Брандмауер VPN може бути окремим пристроєм або програмним брандмауером, що працює на тому самому сервері, що й VPN.

7. Увімкнути журналювання: увімкніть журналювання на сервері OpenVPN, щоб відстежувати та виявляти будь-яку підозрілу активність або спроби неавторизованого доступу.

8. Використовуйте виділений сервер для VPN: рекомендується використовувати виділений сервер для служби OpenVPN, щоб зменшити поверхню атаки та звести до мінімуму ризик компрометації через уразливості в інших службах, що працюють на тому ж сервері.

Висновки до третього розділу:

Досліджено способи захисту інформації в мережі з використанням VPN, як вони вкиористовуються в підключені до звонішніх та внутрішніх віртуальних мереж, що вони дозволяють отримувати доступ користувачам до внутрішніх ресурсів організаціїю.

Проаналізовано, що віртуальні приватні мережі використовують шифрування для створення безпечних з'єднань над незахищеною інфраструктурою Інтернету. Розглянуто один метод встановлення та налаштування віртуальної приватної мережі для захисту інформаційних систем, корпоративних даних і керування доступом користувачів до цих даних за допомогою VPN.

Визначено, які функції та можливості надає OpenVPN, забезпечуючи передачу даних використовуючи протокол SSL/TLS для шифрування, що забезпечує високий рівень безпеки передачі. Підтримується багатьма плтаформами та може приймати багатьох користувачів та клієнтів. Використовує гнучку маршрутизацію (політики маршрутизації), які дозволяють адміністраторам вибірково маршрутизувати трафік через VPN на основі фізичних критеріїв, таких як IP-адреса чи мережа джерела, IP-адреса чи мережа призначення або протокол.

ВИСНОВКИ

В бакалаврській роботі отримано наступні науково-теоретичні та науково-практична навички:

– Визначено дизайн і архітектуру мережі, типи використовуваних пристроїв і програмного забезпечення, а також вжиті заходи безпеки. Вибір відповідних інструментів безпеки та рішень повинен які ґрунтуються на конкретних потребах і вимогах мережі (OpenVPN Server).

– Розглянуто концепцію та різноманітність протоколів віртуальної безпечної VPN.

– Досліджено способи захисту інформації в мережі з використанням VPN, як вони вкиористовуються в підключені до звонішніх та внутрішніх віртуальних мереж

– Віртуальні приватні мережі використовують шифрування для створення безпечних з’єднань над незахищеною інфраструктурою Інтернету. Ми вивчаємо один метод встановлення та налаштування віртуальної приватної мережі для захисту інформаційних систем, корпоративних даних і керування доступом користувачів до цих даних за допомогою VPN.

– Виявлено та проаналізовано основні типи атака на мережеву систему.

– Визначено, які функції та можливості надає OpenVPN, забезпечуючи передачу даних використовуючи протокол SSL/TLS для шифрування, що забезпечує високий рівень безпеки передачі.

– Розроблено рекомендації, щодовстановлення та налаштування рішення від OpenVPN.

– Досліджено концепції та конфігурації для створення захищеної мережі VPN.