Міністерство освіти і науки України
Національний університет «Одеська політехніка»
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

Паталашко Павло Юрійович,
студент групи РЗ-181

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

Розробка програмного продукту для конфігурування безпечного під’єднання до корпоративних мереж

Спеціальність:
125 Кібербезпека

Спеціалізація, освітня програма:
Кібербезпека

Керівник:
Кушніренко Н.І.,
к.т.н., доцент

Одеса – 2022

Міністерство освіти і науки України
Національний університет «Одеська політехніка»
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення
Рівень вищої освіти перший (бакалаврський)
Спеціальність 125 – Кібербезпека
Освітня програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри КБПЗ

_____
д.т.н.,проф. А.А.Кобозєва
____ _____2022р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Паталашку Павлу Юрійовичу

1.Тема роботи: *Розробка програмного продукту для конфігурування безпечного під'єднання до корпоративних мереж*,
керівник роботи *Кушніренко Наталія Ігорівна, к. т. н., доцент*,
затверджені наказом ректора від 17.05. 2022р. №168-в .
2.Зміст роботи*: опис проблематики і технологій, огляд існуючих рішень і видів загроз при передачі даних, вибір протоколу для VPN, огляд AWS, розробка схеми мережі, розробка програмного забезпечення для створення і налаштування VPN-серверу, охорона праці*.
3.Перелік ілюстративного матеріалу: *глобальна структура AWS, топологія мережі, консоль AWS, розподіл ринку хмарних постачальників, робота програмного продукту.*

4. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
Охорона праці	Ярова І.А	Завдання видав	Завдання прийняв
		12.05.2022	09.06.2022

5. Дата видачі завдання "_____"_____2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання	Примітка
1	*Аналіз джерел з теми випускної кваліфікаційної роботи*	*15-11-2021*	*виконано*
2	*Обґрунтування вибору рішення. Збір даних*	*15-02-2022*	*виконано*
3	*Аналіз існуючих рішень, вибір протоколів для реалізації*	*03-03-2022*	*виконано*
4	*Аналіз структури мережі постачальника хмарних послуг AWS*	*20-03-2022*	*виконано*
5	*Розробка програмного продукту*	*24-04-2022*	*виконано*
6	*Підготовка тексту роботи*	*11-05-2022*	*виконано*
7	*Підготовка презентації та доповіді*	*27-05-2022*	*виконано*
8	*Попередній захист*	*02-06-2022*	*виконано*
9	*Нормоконтроль, рецензування*	*20-06-2022*	*виконано*

Здобувач вищої освіти _____ *Паталашко П.Ю.*

Керівник роботи _____ *Кушніренко Н.І.*

ЗАВДАННЯ

на розробку розділу «Охорона праці» у кваліфікаційній роботі бакалавра

студенту Паталашку Павлу Юрійовичу
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

Дата отримання завдання 12.05.2022
Консультації 19.05.2022, 26.05.2022
Дата закінчення розділу 09.06.2022

Тема роботи: *Розробка програмного продукту для конфігурування безпечного під'єднання до корпоративних мереж*

Зміст розділу

1. Аналіз умов праці і вибір основних заходів виробничої безпеки
2. Аналіз пожежної безпеки і вибір заходів і засобів пожежної безпеки

Керівник дипломної роботи

_____ Кушніренко Н. І.
(підпис)

« __ » _____ 2022 р.

Консультант з охорони праці

_____ Ярова І. А.
(підпис)

« __ » _____ 2022 р.

АНОТАЦІЯ

Кваліфікаційна робота на тему “Розробка програмного продукту для конфігурування безпечного під’єднання до корпоративних мереж” на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 - Кібербезпека, спеціалізація, освітня програма: кібербезпека, містить 23 рисунки, 1 таблицю, 2 діаграми, 17 літературних джерел за переліком посилань. Робота виконана на 50 сторінках загального тексту і 49 сторінках основного тексту.

Метою роботи є підвищення рівню безпеки і автоматизації створення під’єднання до внутрішніх корпоративних мереж шляхом розробки спеціалізованого програмного продукту.

У результаті виконання кваліфікаційної роботи розроблено програмний продукт, який зменшив витрати часу при створенні усіх необхідних компонентів для організації з’єднання, а також мінімізовано помилку людського фактору, за рахунок чого підвищено безпеку клієнту і серверу. Запропонований програмний продукт має зручний інтерфейс, за допомогою якого користувач може налаштувати VPN-сервер і створити конфігурації для клієнтів, які можуть одразу бути використані для безпечного під’єднання до приватної мережі.

ІНФОРМАЦІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, ПЕРЕДАЧА ДАНИХ, ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ, БЕЗПЕЧНЕ З’ЄДНАННЯ, ХМАРНІ ТЕХНОЛОГІЇ, AWS, АВТОМАТИЗАЦІЯ, КОНФІГУРАЦІЯ

SUMMARY

Qualification work "Development of software to configure safe connection to corporate networks" for the first (bachelor's) level of higher education in specialty 125 – Cybersecurity specialization, educational program: cybersecurity contains 23 figures, 1 table, 2 diagrams, 17 literature sources on the list of references. The work is performed on 50 pages of general text and 49 pages of main text.

The purpose of this work is to increase the level of security and automate the connection to internal corporate networks by developing a specialized software product.

As a result of the qualification work, a software product was developed that reduced the time spent creating all the necessary components to organize the connection, as well as minimizing human error, therefore increasing the security of the client and server. The proposed software has a user-friendly interface that allows the user to configure a VPN-server and create configurations for clients that can be used immediately to securely connect to a private network.

INFORMATION, INFORMATION SECURITY, DATA TRANSFER, VIRTUAL PRIVATE NETWORKS, SECURE CONNECTION, CLOUD TECHNOLOGIES, AWS, AUTOMATIZATION, CONFIGURATION

ЗМІСТ

ВСТУП

Зі стрімким розвитком сфери інформаційних технологій виникає потреба в захисті інформації та в безпечному передаванні її через глобальну мережу. Актуальним об'єктом дослідження є проблема інформаційної безпеки, її систематизація, виявлення джерел інформаційних загроз, показників, критеріїв та стандартів. Інформаційною безпекою можна назвати стан захищеності інформації від несанкціонованого отримання, модифікації, видалення, обмеження доступу до неї. Мета інформаційної безпеки - захистити дані і гарантувати точність, цілісність її на всіх стадіях існування та мінімізувати витрати, які можуть мати місце, якщо інформація буде модифікована або зруйнована. Проблема забезпечення безпеки інформації саме на стадії транспортування через мережу Інтернет має досить великий пріоритет для досліджень і створення різних рішень для її вирішення.

Технологія віртуальних приватних мереж (VPN) була створена через потребу в об’єднанні комп’ютерних мереж між собою використовуючи безпечний канал зв’язку через мережу з меншим показником довіри. З пункту №1 в пункт №2 необхідно передати дані таким чином, щоб до них неможливо було отримати доступ третім особам, і тільки адресат, якому вони передбачалась, мав змогу їх отримати та використати. Цілком реальна і практична проблема, актуальність якої зростає з кожним роком розвитку інформаційних технологій. В якості пунктів зв’язку можуть виступати окремі робочі станції, вузли, сегменти мереж або цілі мережі. У випадку з транспортуванням інформації між мережами, в якості безпечного рішення проблеми передачі може використовуватись виділений фізичний канал зв’язку. Але імплементація такого підходу не є тривіальною і потребує витрат на організацію та підтримку функціонування.

Більш простим і дешевим рішенням є використання вже існуючих фізичних каналів зв’язку, будь то створена попередньо корпоративна мережа або мережа Інтернет. Але у той же час інформація буде направлена по логічно відділеному від решти з’єднань «тунелю», який буде створюватись лише між відправником і

одержувачем. Уся інформація, що проходить через такий тунель, буде зашифрована, а відновлення до первозданного виду відбувається шляхом розшифрування на стороні отримувача. Така модель передачі даних може вирішити не тільки проблему передачі по мережі Інтернет. Така технологія може стати у нагоді в локальних мережах за потреби відділення одного типу трафіку від іншого.

Ще однією вагомою причиною для використання технології VPN є стрімкий розвиток і зростання популярності хмарних сервісів – відносно новий вид мережевих послуг, які надають можливість «орендувати» обчислювальні ресурси і пристрої зберігання інформації [1]. Також провайдери таких послуг можуть постачати вже готові рішення з вищим рівнем абстракції над інфраструктурою. На сьогодні усе більше компаній мігрують свої додатки з локальних дата-центрів до хмарних сервісів цілком, або створюючи гібридну архітектуру, об’єднуючи свою програмно-апаратну частину з хмарними рішеннями. В обох випадках необхідно вирішити проблему безпечного доступу працівників та з’єднання двох або більше мереж між собою через мережу Інтернет, не збільшуючи при цьому рівень загрози у зв’язку з пересіканням інформації через неї.

Метою даної роботи є автоматизація створення і налаштування серверу для безпечного під’єдання до приватних мереж, зокрема сфокусованого на хмарних технологіях, шляхом розробки спеціалізованого програмного продукту. За рахунок такого підходу підвищиться рівень безпеки і автоматизації організації з’єднання, та сильно знизяться ризики людського фактору і витрати часу при конфігуруванні власноруч. Альтернатив у відкритому Інтернеті не було знайдено, що підвищує цінність розробки. В процесі виконання даної роботи необхідно розв’язати наступні задачі:

- Дослідити предметну область, розібрати різні підходи до створення VPN;
- Навчитись налаштовувати VPN-сервер і клієнтів для нього власноруч;
- Створити програму для повної автоматизації конфігурації.

1 ОПИС ПРОБЛЕМАТИКИ І ТЕХНОЛОГІЙ

1.1 Огляд існуючих рішень

Коли виникає необхідність безпечного об’єднання двох пунктів для передачі інформації по мережі, в доступності є достатньо великий вибір засобів. Все залежить від можливостей, здібностей, фінансів та наявності обладнання у компанії.

Створення фізичного каналу зв’язку власноруч можливий використовуючи наступі способи:

- Ethernet - це скручена пара. До 100 метрів. Максимум у будівлі або між сусідніми будівлями. Швидкість з’єднання 1 Гбіт/с.
- Wi-fi. Відстань залежить від реалізації: можливо досягти продуктивності на 40 км, використовуючи потужні спрямовані антени. В середньому до 5 км з прямим видимістю. Швидкість залежить від стандарту та використаної відстані.
- Оптичне волокно. 1 Гб/с (рішення для 10 та 100 ГБ/с коштуватимуть забагато при критерії “ціна - якість”). Відстань залежить від багатьох факторів: від кількох кілометрів до сотень. Потрібні координації щодо прокладання кабелю, кваліфікованого персоналу для будівництва та обслуговування. Для невеликих компаній має сенс лише підключити будівлю недалеко від центрального вузла.

Загалом, кожен випадок є індивідуальним і вимагає свого підходу. При такому способі організації з’єднання для компанії усе прозоро – використання власної окремої фізичної лінії для передачі інформації без обмежень.

Іншим варіантом є оренда каналу зв’язку у постачальника. При необхідності стабільний канал до іншого міста є найпоширенішим і надійним варіантом. Провайдер може надати можливість доєднатися до своєї точки зв’язку. З боку провайдера трафік не контролюється жодним чином, не обмежуючись, він лише підтримує фізичний канал. Наприклад, у випадку аварії на лінії не доведеться наймати працівників для її налагодження, це зона відповідальності постачальника.

Тунель через публічну мережу – ще одне альтернативне рішення. Якщо обидві умовні вузли зв’язку мають доступ до Інтернету, найдешевший і найлегший у підтримці спосіб - побудувати тунель між цими двома точками. Для цього необхідномати публічні адреси на обладнанні, на якому він реалізується.

Звичайно, у кожного з вищенаведених способів об’єднання є свої недоліки. Завданням є не тільки створити зв’язок між клієнтами, сегментами мереж, або забезпечити віддаленого досупу. Не менш важливим фактором для урахування при налаштуванні середи для обміну інформацією є, власне, безпека цієї самої інформації. В цьому плані ідеального рішення немає і ніколи не буде. В будь-якому моменті існування інформації вона є вразливю до різного роду атак.

1.2 Основні види загроз при передачі даних

В Інтернет-просторі існує велика кількість різних загроз цілісності, доступності і конфіденційності інформації. Дослідження даної роботи розглядає конкретно проблему безпеки інформації в процесі передавання її по мережі.

1.2.1 Man-in-the-Middle

Типи кібератак «Людина посередині» (MITM) відносяться до порушень кібербезпеки, які дають можливість зловмиснику підслуховувати дані, що пересилаються між двома людьми, мережами або комп’ютерами. Це називається атакою «людина посередині», оскільки зловмисник розташовується «посередині» або між двома сторонами, які намагаються спілкуватися. Фактично, зловмисник стежить за взаємодією між двома сторонами. Під час атаки MITM обидві залучені сторони відчувають, що спілкуються, як зазвичай. Чого вони не знають, так це того, що особа, яка фактично надсилає повідомлення, має можливість незаконно модифікувати повідомлення або отримати доступ до нього, перш ніж воно досягне місця призначення.

1.2.2 Підслуховування

Найпростіший спосіб атаки – це просто «підслухати». Зловмисник може використати сегменти мережі, дані по якому проходить у відкритому вигляді. Термін підслуховування означає підслуховування без зайвих зусиль. Наприклад, ми можемо сказати, що зловмисник (або системний адміністратор) підслуховує, відстежуючи весь трафік, що проходить через певний вузол зв'язку. Підслуховування може бути активним і пасивним. При активному прослуховуванні зловмисник вставляє програмне забезпечення на шляху мережевого трафіку для збору інформації, яку аналізує на наявність корисних даних.

Адміністратор може мати законні цілі, наприклад, стежити за неналежним використанням ресурсів (наприклад, відвідувати веб-сайти, не пов'язані з роботою, із мережі компанії) або підозрілим спілкуванням (наприклад, передача чутливих до поширення файлів).

Більш «агресивним» терміном є «Wiretapping», при якому втручання в лінію зв'язку відбувається на фізичному рівні, тобто з підміною або додаванням під'єднання до кабелю [2]. В результаті зловмисник «копіює» трафік, що проходить крізь модифіковану лінію передачі. Також можливе встановлення «сніфферів» в сегменти телекомунікацій, які слугують для тієї ж самої цілі – прослуховування.

1.2.3 Перехоплення сесії

Зловмисник отримує контроль сеансу спілкування між клієнтом і сервером. Комп'ютер, який використовується для атаки, замінює свою адресу Інтернет-протоколу (IP) на адресу клієнтського комп'ютера, і сервер продовжує сеанс, не підозрюючи, що спілкується зі зловмисником, а не з клієнтом [3]. Цей вид атаки ефективний, оскільки сервер використовує IP-адресу клієнта для перевірки його особистості. Якщо IP-адреса зловмисника введена на початку сеансу, сервер може не підозрювати порушення, оскільки він уже задіяний у довіреному з'єднанні.

1.3 Технологія VPN

У минулому організації фізично встановлювали лінії на великі відстані, щоб забезпечити безпеку даних при передачі. Однак ця система не є достатньо практичною для кожного корпоративного підприємства та звичайних користувачів через вартість, місце та час, необхідний для таких налаштувань. В останні роки з експоненційним зростанням Інтернету, телекомунікаційні технології зазнають сильних змін і всесвітня мережа стала частиною майже усіх сфер діяльності людини, включаючи освіту, банківську справу, бізнес і медицину. Описані в попередньому розділі загрози конфіденційності і цілісності інформації мають прямий вплив на надійність, якість та коректне функціонування інфраструктури, що лежить в основі надання послуг через описані вище сфери. Будь яка компанія обов’язково стикається з питанням передачі інформації між своїми філіалами, офісами або організації доступу для співробітників віддалено. Фізично дані в такому випадку передаються через недостовірні канали зв'язку, тому потенційний зловмисник має можливість перехопити і використовувати інформацію.

1.3.1 Визначення VPN

При необхідності об’єднання декількох сегментів мереж найдоречнішим варіантом буде використання технології VPN (Virtual Private Network), на основі якої можна з’єднати декілька мереж в одну, навіть на різних точках земної кулі, при цьому забезпечити гнучкість та одночасно високу швидкість передачі даних, а головне - безпеку при обміні інформацією [4]. Віртуальну приватну мережу можна визначити як спосіб організації безпечного спілкування через використання телекомунікаційної інфраструктури загального користування, збереження конфіденційності за допомогою протоколу тунелювання і процедур безпеки.

Основна мета VPN – надати підприємствам ті ж можливості, або навіть краще, як у фізичних приватних мережах, але за набагато нижчою вартістю. Користь від VPN полягає у зниженні вартості, збільшення масштабованості та продуктивності без погіршення безпеки [5]. Технологія VPN дає змогу вирішити наступні завдання:

- конфіденційність – третя особа не повинна мати можливості скопіювати дані або ознайомитися з інформацією, що передається через спільну мережу;
- автентифікація – перевірка того, чи відправник пакетів є справжнім пристроєм, а не таким, що використовується зловмисником;
- цілісність даних – перевірка, при якій з'ясовується, чи не змінювався пакет при передачі;
- пересилання недостовірної інформації – третя особа не повинна мати можливості копіювати пакети даних, надіслані справжнім відправником, а потім пересилати ці пакети, видаючи себе за справжнього відправника.

В залежності від потреб, VPN може забезпечити наступні типи з’єднань:

- Site-to-Site: йдеться про з’єднання двох мереж у двох місцях, які є двостороннім або multi-to-multi. Це дозволяє будь-якому пристрою з першої підмережі зв’язуватися з іншим, і навпаки. Таке з’єдання налаштоване на рівні мережевих пристроїв для досягнення гнучкості, оскільки дозволяє будь-якій кількості пристроїв у мережі комунікувати безпосередньо з іншою мережею без додаткових кроків. Схему такого з’єднання зображено на рисунку 1.1.
- Віддалений доступ: він підключає окремих клієнтів до мереж VPN. Такий тип з’єдання слід налаштувати на кожному окремому пристрої клієнта. Наведений варіант найбільш підходить для умов постійної мобільності, тому немає необхідності налаштовувати підключення до мережі для проміжних пристроїв, щоб використовувати цей тип VPN. Схему такого з’єднання зображено на рисунку 1.2.

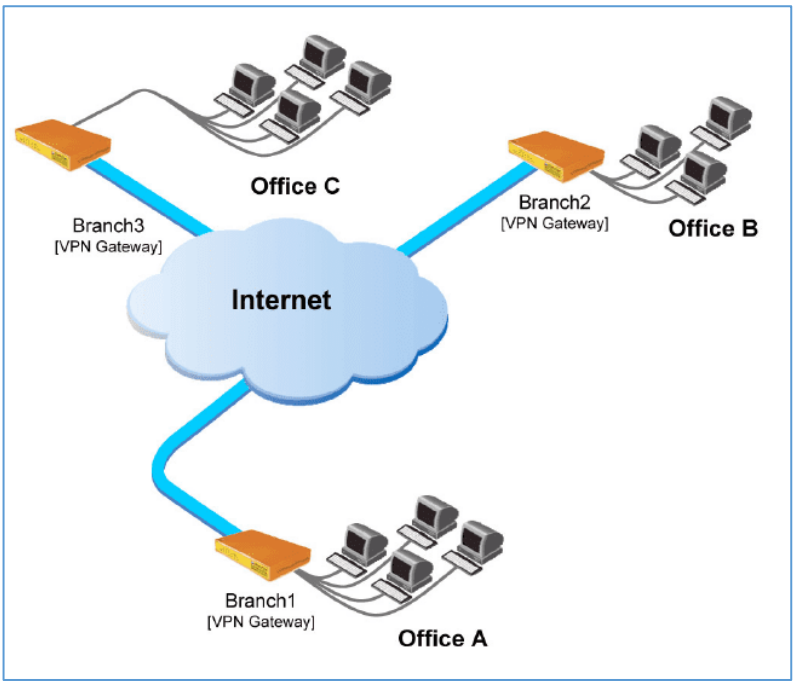


Рисунок 1.1 – Схема Site-to-Site VPN

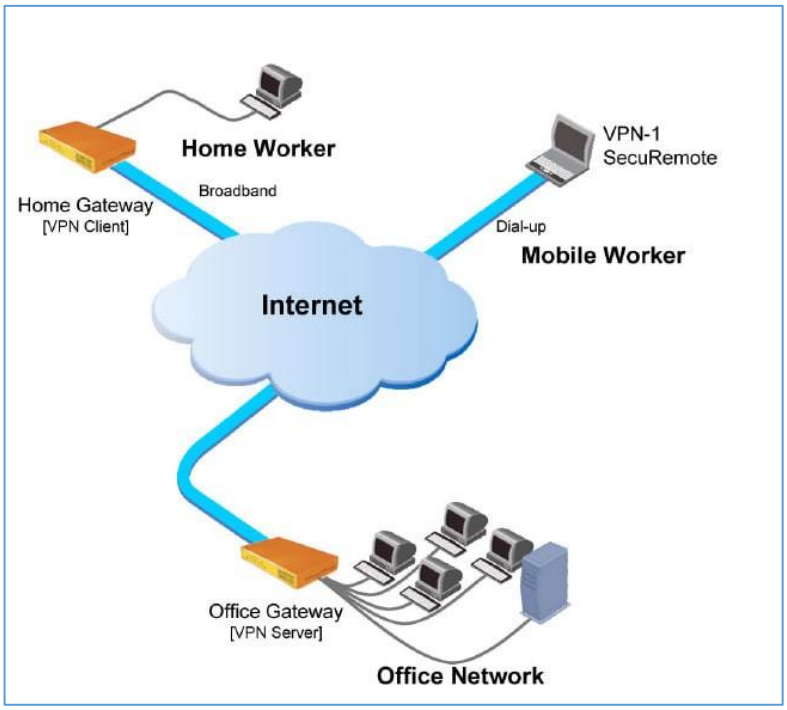


Рисунок 1.2 – Схема віддаленого доступу до мережі

1.3.2 Принципи роботи

Для об’єднання декількох мереж в одну віртуальну мережу використовуються спеціальні віртуальні виділені канали. Для створення подібних з’єднань використовується механізм тунелювання. Ініціатор тунелю інкапсулює

пакети локальної мережі в нові IP-пакети, які містять в своєму заголовку адресу ініціатора тунелю та адресу точки закінчення тунелю. При отриманні подібного пакету, кінцевий користувач проводить зворотній процес розшифрування отриманого пакету.

Для того щоб досягти конфіденційності при передаванні інформації, потрібно використовувати певний алгоритм шифрування, при цьому він має буди аналогічний як для відправника, так і для отримувача, та лише вони повинні мати інформацію про те який саме використовуються алгоритм, також володіти ключем для шифрування та розшифрування трафіку. Протоколи шифрування можуть бути різними, все залежить від того який протокол тунелювання використовується [6].

Існує багато характеристик VPN-протоколів. Вони різняться за кількістю підтриманих алгоритмів шифрування, швидкістю з'єднання, гнучкістю налаштувань і легкістю конфігурування.

1.4 Хмарні обчислення

Хмарні обчислення - концепт, в якому велика кількість інформаційних систем об'єднані в приватні або загальнодоступні мережі, з метою забезпечити динамічно масштабовану інфраструктуру для надання обчислювальної сили, зберігання даних і файлів. З появою цієї технології вартість розміщення додатків, веб-сторінок або обчислювальних навантажень, зберігання даних та доставки вмісту значно зменшилася [7].

Завдяки технології віртуалізації програмного та апаратного забезпечення досягається гнучке налаштування і виділення необхідної і достатньої кількості ком'ютерних ресурсів відповідно до вимог користувача. Визначення віртуалізації полягає у ізоляції ресурсів програмної або апаратної частини, що дозволяє розміщувати декілька різних обмежених від інших операційних систем, а також регулює виділення ресурсів для кожної індивідуально. Таким чином, потенціал кожної обчислювальної машини може бути використаний на повну, без простоїв її

ресурсів. Виділення ресурсів за потребою впливає на зниження витрат для клієнта.

Одною з основних переваг є зникання потреби встановлювати і налаштовувати апаратну частину інформаційної системи, що займає багато часу і витрат на компоненти, організацію і підтримку. Постачальники хмарних послуг використовують модель «розділеної відповідальності», яка відносить фізичну безпеку датацентрів, будівель і апаратної частини, її коректне налаштування, забезпечення стабільного підключення до інтернету, віртуалізаціїї апаратної частини до пунктів, за які відповідає провайдер послуг. У свою чергу, усе що стосується даних клієнта, їх шифрування, встановлення антивірусу, коректного налаштування програмної частини, створення і розмежування прав користувачів, перепадає на клієнта. Така модель вирішує велику кількість задач, що передстають перед створенням інформаційних систем: організація апаратної частини, витрати на підтримку та обслуговування, забезпечення безпеки.

Близько 90% комерційних компаній по всьому світу користуються тим чи іншим хмарним рішенням [8]. До них можуть входити віртуальні сервери, хостинг, бази даних, сервіси для зберігання даних.

У зв’язку з інтенсивним розвитком хмарних обчислень зростає і необхідність забезпечення доступу до них. Одним із таких постачальників хмарних послуг є AWS (Amazon Web Services) – найпопулярніший вибір серед корпоративних компаній. Безпечний доступ до ресурсів внутрішньої мережі AWS можливо створити саме за допомогою VPN-протоколів, що вирішить питання безпеки неминучого пересікання трафіку через незахищений Інтернет.

2 ВИБІР ОПЦІЙ ДЛЯ VPN І РОЗРОБКА СХЕМИ МЕРЕЖІ

2.1 Огляд різних VPN-протоколів

Згідно з дослідженням двома найпоширенішими протоколами для організації VPN являються IPsec (IP Security) та OpenVPN [9]. Відносно нове рішення під назвою Wireguard розробляється для заміни обох попередніх протоколів, при цьому претендуючи на кращу продуктивність [10]. Дані протоколи були взяті до огляду через відкритість їх коду. IPsec і OpenVPN на даний момент є відкритими стандартами для створення VPN-рішень.

2.1.1 OpenVPN

OpenVPN - протокол VPN на основі SSL, оскільки він використовує протоколи SSL і TLS для захищеного з'єднання. Однак OpenVPN також використовує HMAC у поєднанні алгоритму хешування для забезпечення цілісності пакетів. OpenVPN може бути налаштований для використання попередньо розділених ключів та сертифікатів. Ці функції, як правило, не доступні іншими VPN на основі SSL. Крім того, OpenVPN використовує віртуальний мережевий адаптер пристрій tun або tap як інтерфейс між програмним забезпеченням і операційною системою. На даний момент в список підтриманих систем входять Linux, Free/Open/NetBSD, Solaris, Windows та MacOS, а також пристрої iOS та Android. Для всіх цих платформ має бути встановлене клієнтське програмне забезпечення, що відрізняє OpenVPN від client-less або веб-VPN. Увесь трафік проходить через одне з'єднання UDP або TCP. Канал управління шифрується і захищається за допомогою SSL і TLS каналів, також дані шифруються за допомогою протоколу шифрування користувача. Стандартний протокол - UDP, порт - 1194.

Перевагами OpenVPN є простота установки конфігурації та можливість встановлення в обмежених мережах, включаючи мережі NAT. Крім того він включає в себе функції безпеки, які надають схожий рівень захищеності, як і у VPN на основі IPSec, включаючи підтримку для різних користувачів механіз

аутентифікації. Повний перелік налаштувань доступний через веб-інтерфейс серверу, де можна робити усі необхідні дії.

Недоліки OpenVPN полягають у відсутності його масштабованості та залежності від встановлення клієнтського програмного забезпечення. Зокрема, драйвер інтерфейсу tap для Microsoft Windows часто викликав проблеми розгортання, коли випускалася нова версія операційної системи.

2.1.2 IPSec

IPSec є офіційним стандартом IEEE/IETF для безпеки IP. Офіційно зареєстровано як RFC2411. Також вбудований у стандарт IPv6 [11]. IPSec функціонує на другому і третьому рівні моделі OSI мережної мережі. IPSec включає поняття політики безпеки, що робить даний протокол надзвичайно гнучким та потужним, але при цьому важко налаштовується та налагоджується. Безпека політики дозволяє адміністратору шифрувати трафік між двома кінцевими точками на основі параметрів, таких як IP-адреса джерела та IP-адреса призначення, а також між вихідним та кінцевим портами TCP або UDP. IPSec можна налаштувати на використання попередньо розділених ключів або сертифікатів для захисту підключення VPN. Крім того, він використовує сертифікати X.509, одноразові паролі, протоколи імен користувача або пароль для аутентифікації VPN-з'єднання.

Існує два режими роботи в IPSec: тунельний режим та транспортний режим. Транспортний режим найчастіше використовується в поєднанні з тунелюванням другого рівня (L2TP). L2TP протокол виконує автентифікацію користувача. Клієнти IPSec, вбудовані в операційні системи, зазвичай використовують IPSec з L2TP. У VPN-клієнту, вбудованого у Microsoft Windows, за замовчуванням використовується протокол IPSec з L2TP, але його можна змінити.

Стандарт IPSec включає три протоколи, кожен зі своїми функціями.

ESP (Encapsulating Security Payload – безпечна інкапсуляція корисного навантаження) займається безпосередньо шифруванням даних, а також може забезпечувати аутентифікацію джерела та перевірку цілісності даних.

AH (Authentication Header – заголовок аутентифікації) відповідає за аутентифікацію джерела та перевірку цілісності даних.

ISAKMP/IKE (Internet Key Exchange – обмін ключів в мережі) використовується для формування SA (Security Association – асоціація безпеки), узгодження інформації учасників захищеного з'єднання. Учасники домовляються, який алгоритм шифрування буде використовуватися, за яким алгоритмом проводитиметься перевірка цілісності, а також як автентифікувати один одного.

IPSec використовує два канали: канал керування для налаштування з'єднання та для передачі даних. Канал керування ініціюється через UDP. Канал передачі даних використовує протокол ESP. Цілісність пакетів забезпечується за допомогою автентифікації повідомлення (HMAC) - той же метод, який використовує OpenVPN.

Переваги стандарту IPSec - це його безпека, хороша підтримка з боку різних постачальників та платформ, включаючи маршрутизатори xDSL та Wi-Fi, гнучкість його налаштувань. Даний протокол став золотим стандартом для впровадження в корпоративні мережі. Програмне забезпечення IPSec входить до складу операційних систем, а також брандмауерів, маршрутизаторів.

Недоліками IPSec є складне налаштування, погана інтеграція з мережами NAT. Також багато організацій реалізували розширення до стандарту, які робить його більш складним для того, щоб з'єднати дві кінцеві точки IPSec від різних модифікованих версій протоколу.

2.1.3 Wireguard

Wireguard — відносно новий VPN-протокол, який має на меті створення простої та ефективної реалізації віртуальної приватної мережі. В основі створення даного протоколу лежить ідея увібрати в себе безпеку стандарту IPsec, і зробити процес налаштування легшим, ніж OpenVPN, в той же час не втрачати швидкість роботи з’єдання. Спочатку він був написаний для систем Linux, але тепер доступний на більшій кількості платформ. Мета дизайну — мати загальну пряму конфігурацію, схожу до SSH, тобто криптографію асиметричного ключа.

Wireguard використовує найсучасніші криптографічні алгоритми та протоколи, такі як:

– Curve25519 для обміну ключами;
– ChaCha20 і Poly1305 для симетричного шифрування;
– SipHash для ключів хеш-таблиць;
– BLAKE2s для функції криптографічного шифрування.

На даний момент протокол використовує лише UDP, порт за замовчуванням - 51280. WireGuard було надіслано в 2020 на перевірку для додавання в ядро Linux. Після успішного аудиту його було включено до ядра починаючи з версії 5.6 [12].

Переваги протоколу полягають у легкості налаштування як серверу, так і клієнтської частини. Він майже не має впливу на швидкість передачі інформації, при цьому використовує стійкі криптографічні алгоритми для шифрування [13]. На діаграмі 2.1 приведений тест швидкості протоколів з офіційної веб-сторінки.

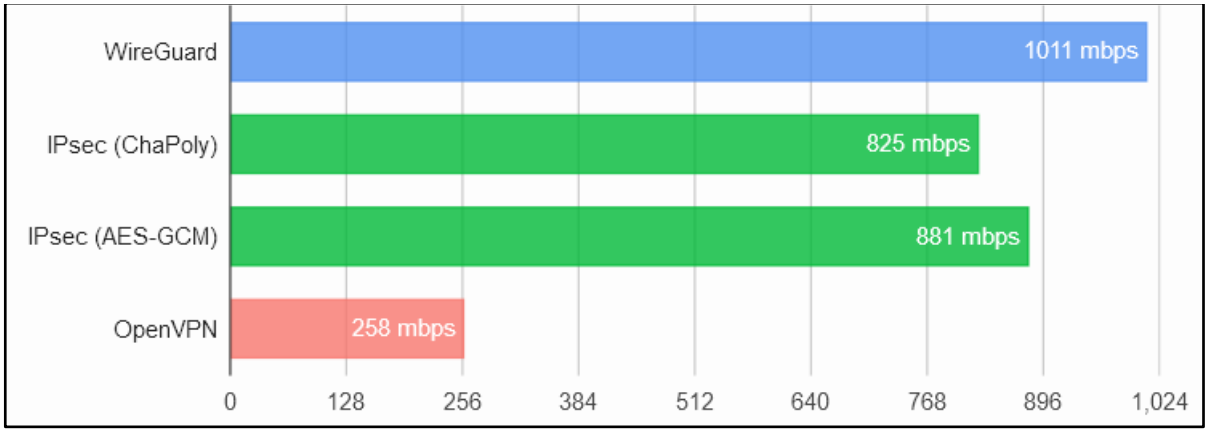


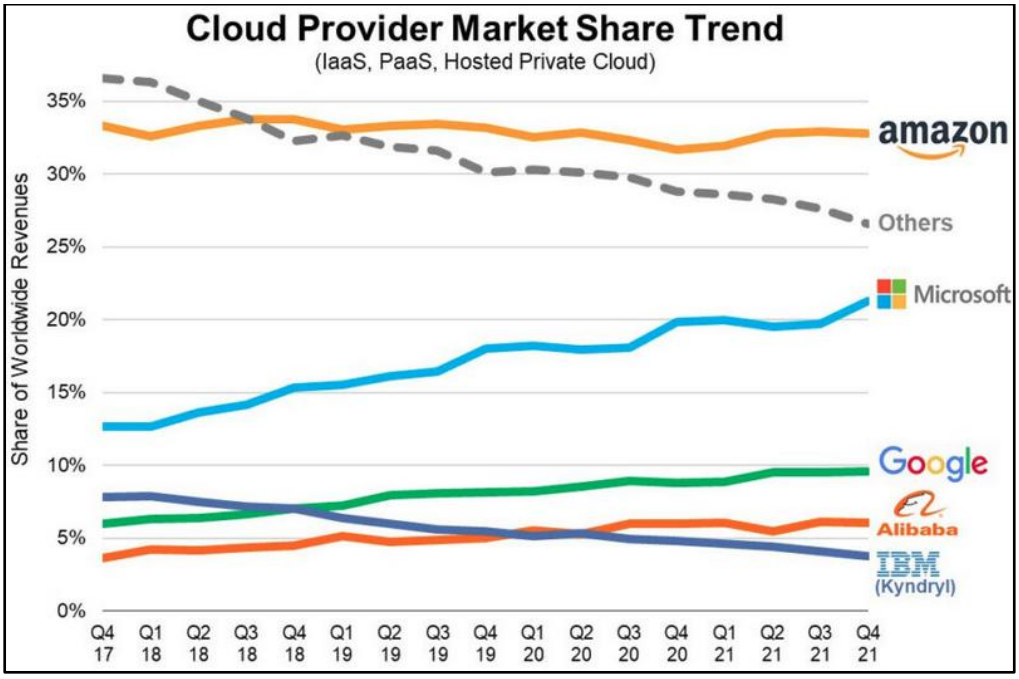
Рисунок 2.1 – Порівняння швидкості роботи VPN протоколів

Основа Wireguard вміщується в 7000 рядків коду, що у порівнянні з IPsec (400000 рядків) і OpenVPN (70000 рядків), що позитивно сприяє продуктивності роботи, аудитам безпеки і зниженню «засміченості» протоколу. В Wireguard передбачений механізм “kill-switch”, який полягає у припиненні пересилання трафіку через незахищену у разі переривання тунелю.

До недоліків можна віднести відсутність можливості вибору криптографічних алгоритмів, потребу встановлювати клієнтське програмне забезпечення. Також “зліпок” його заголовків легко ідентифікується, що може призвести до неможливості доступу до деяких сайтів, що блокують VPN-трафік.

2.2 Amazon Web Services

З кожним роком кількість постачальників хмарних послуг на ринку стрімко збільшується. На сьогоднішній день їх існує більше 800. Виходячи зі статистики на 1 квартал 2022 року, 62% світового ринку хмарних послуг займають AWS, Microsoft Azure і Google Cloud Platform [14]. З них, найпопулярнішим постачальником є Amazon Web Services, з 33% усієї долі.



Діаграма 2.2 – Світовий ринок постачальників хмарних послуг

AWS був запущений в 2006 році з внутрішньої інфраструктури, створеної Amazon.com для роботи з онлайн-роздрібними операціями. Amazon була однією з перших компаній, яка почала надавати послуги в моделі хмарних обчислень з оплатою по мірі використання, яка масштабується, щоб забезпечити користувачам обчислення, сховище або пропускну здатність за потреби.

Існує багато різних інструментів і рішень для підприємств і розробників програмного забезпечення, які можна використовувати в дата-центрах у 190 країнах світу. Державні установи, навчальні заклади, некомерційні та приватні організації, можуть з легкістю використовувати сервіси не залежно від місця розташування.

AWS поділяється на різні сервіси: кожен може бути налаштований різними способами залежно від потреб користувача. Наразі кількість сервісів перевищує 200 одиниць. З одного боку розмежування сервісів за призначенням є хорошою практикою, але у той же кожен з них має власний інтерфейс і спосіб налаштування, що може бути досить складно для використання. Зазвичай, можна виділити основні категорії сервісів, на яких все базується:

– Обчислення
– Віртуальна мережа
– Сховища даних
– Бази даних

Забезпечення високого рівню доступності і малої затримки зумовлені добре зпланованою схемою фізичної інфраструктури. Необхідно ввести поняття наступних ключових елементів.

Зона доступності - місце, яке містить кілька фізичних центрів обробки даних. В кожному регіоні повинно існувати щонайменше 2 зони доступності для надійності;

Регіон - сукупність зон доступності у географічній близькості, з’єднаних в одну мережу з низькою затримкою, розташовані по усьому світу.

Підприємство обирає одну або кілька зон доступності з різних причин, таких як відповідність вимогам і відносне розташування регіону до кінцевих клієнтів для зниження часу затримки. Схема фізичної інфраструктури зображена на рис. В межах предметної області для розробки програмного забезпечення будуть використані деякі сервіси із загальних категорій, а саме: VPC, EC2, IAM, SSM.

VPC (Virtual Private Cloud) – сервіс, в якому можливо створити ізольовану

віртуальну приватну мережу, підмережі, резервувати IP-адреси, створювати таблиці маршрутизації трафіку ззовні та з середини мережі. Підмережі бувають приватними і публічними. До приватних підмереж немає доступу з зовнішнього інтернету, до них можна отримати доступ лише з середини.

Для кожного ресурсу є опція вибору в якому регіоні його розташувати.

Рисунок 2.1 – Глобальна інфраструктура AWS

Ресурси в публічних мережах доступні з будь-яких джерел. Важливо зазначити, що за замовчуванням увесь трафік в межах однієї мережі повністю дозволений, тобто між двома приватними або між публічною і приватною підмережами завжди є зв’язок без потреби додавання правил.

EC2 (Elastic Cloud Compute) - середа для створення віртуальних серверів у хмарі. Вона надає можливість дуже гнучко налаштовувати і створювати обчислювальні машини. Користувач може обрати кількість процесорів, оперативну пам’ять, диск, різного роду адаптери, операційну систему і навіть задати перелік команд для виконання при створенні серверу. Опціонально можлива генерація SSH-ключа для подальшого отримання доступу до серверу для

конфігурації, а також вибір віртуальної мережі та підмережі. Безпека портів серверу контролюється групами безпеки (Security groups), де можна обрати протокол, порт, список адрес, з яких доступне з’єднання до обчислювальної машини. Можливе додавання до декількох груп безпеки одночасно.

IAM (Identity and Access Management) – потрібен для створення і керування користувачами, групами і ролями в межах одного облікового запису в AWS. Можна накладати обмеження на дії в акаунті для різних ресурсів, встановлювати правила. Наприклад, дозволити користувачу мати доступ лише на переглядання ресурсів, але без можливості змінювати їх. Також, при необхідності можливо згенерувати дані для програмного доступу для кожного користувача, за допомогою них відбувається “спілкування” з AWS через код або консоль. Концепт ролей в AWS полягає у тому, що вони призначені для надання можливості самим ресурсам робити деякі операції над іншими ресурсами. Дана функція є дуже корисною якщо необхідно, щоб сервер мав змогу наприклад, завантажити файли до сервісу сховища напряму.

SSM (Systems manager) – має низку корисних функцій для менеджменту існуючих ресурсів, редагування міток, виконання переліку команд на декількох серверах одночасно.

У кожного ресурсу, будь то сервер, диск, мережа або користувач, в AWS існує власний унікальний ідентифікатор, який однозначно вказує на ресурс. Саме за ним можливе звернення до об’єкту. Також на ресурси є можливість навішувати інформаційні мітки типу “ключ-значення”. Такий підхід спрощує управління, дозволяє згрупувати об’єкти за різними ознаками, а також розширити інформацію для користувача.

В основі спілкування AWS лежать API-виклики, за допомогою яких сервіси обмінюються інформацією один з одним. API можуть використовувати користувачі для створення і конфігурування ресурсів через командну строку, минуючи необхідність робити усе через графічний інтерфейс на веб-сторінці. Такий підхід допоможе автоматизувати і повторно використовувати створені команди, що зменшить рівень впливання людського фактору і час на операції.

Через те, що для доступу до ресурсів AWS трафік в будь-якому випадку потрібно передавати через відкриту мережу Інтернет, необхідно вирішити проблему безпечного під’єднання до VPC. Тому для цього вирішено створити з’єднання, використовуючи протоколи тунелювання, описані в розділі 2.1, і організувати автоматичне створення і налаштування VPN-серверу в публічній підмережі.

2.3 Створення схеми майбутньої мережі

Корпоративний працівник, якому потрібно отримати доступ до внутрішньої приватної підмережі, повинен мати змогу зробити це без зайвих зусиль. Трафік при цьому проходить шлях від роутера користувача до його Інтернет-провайдера, далі через Інтернет, в кінці потрапляючи до мережі AWS. Після входження до мережі, згідно з правилами таблиць маршрутизації може пройти далі до VPN-серверу в публічній підмережі, при цьому обов’язковими умовами для серверу є його розташування в саме публічній підмережі, а також присвоєна йому автоматично публічна IP-адреса. Перед входом на мережевий інтерфейс VPN-серверу, спрацьовують правила груп безпеки, які перевіряють чи дозволено даному клієнту мати доступ до порту. Налаштований VPN-сервер перебуває точкою для спілкування з внутрішньою підмережею, тунель закінчується на його стороні і далі трафік може бути проксований по мережі до адресату. В приватній підмережі можуть розташовуватись як і інші сервери, так і повноцінні сервіси, такі як внутрішні веб-сторінки і FTP-хости.

Таким чином, проаналізувавши хід трафіку від користувача до приватної мережі, можна побудувати схему з’єднання з усіма необхідними пунктами. Спираючись на модель мережі на рисунку 2.2, з’являється можливість для втілення плану такої схеми в реальних умовах.

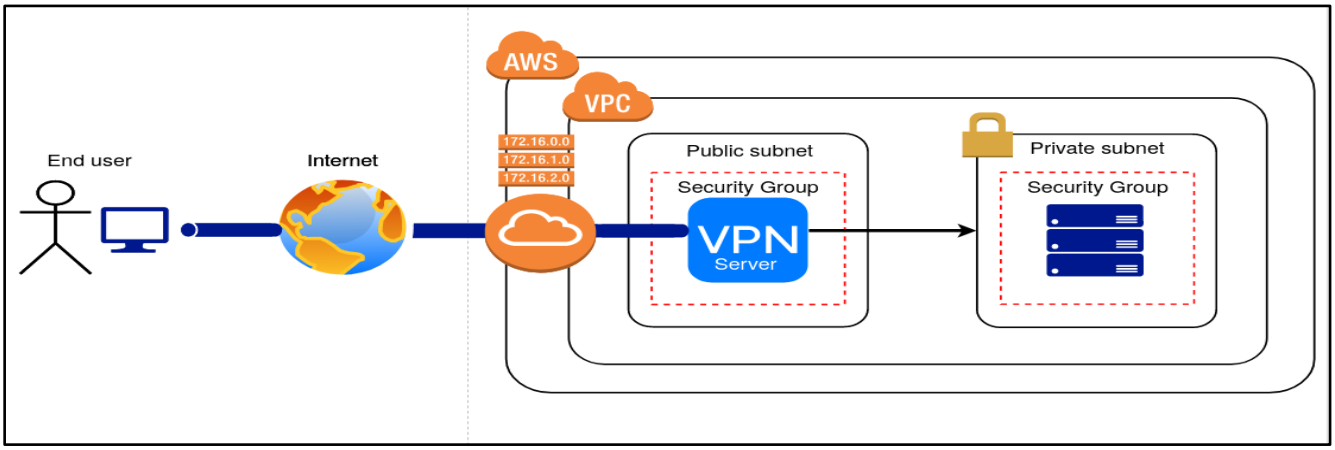


Рисунок 2.2 - Топологія мережі

Іншою проблемою в даному випадку являється складність і витрати часу для адміністратору мережі ручного створення серверу і усіх необхідних компонентів для його роботи, а також налаштування самих VPN-протоколів на ньому. Тому було вирішено створити програмний продукт з інтерфейсом, в якому можливо, використовуючи програмний доступ до акаунту, швидко і зручно повністю розгорнути готовий VPN-сервер з можливістю створення конфігурацій для клієнта у виді логіну і паролю, або файлу налаштувань. Завдяки тому, що в коді програми вже буде готовий шаблон для серверу, досягається безпомилкове створення. Необхідні змінні параметри будуть зв’язані з інтерфейсом програми, де їх можливо редагувати. Перелік команд для конфігурації клієнта і сервера будуть занесені до окремих файлів – скриптів, які викликаються за потребою. Також такий підхід дозволяє розбити програмний продукт на модулі, що сприяє тому, що ці скрипти можна власноруч запустити на будь-якому сервері не в мережі AWS. Тому результатом виконання даної роботи буде програмний продукт, що автоматизовано розгортає VPN-сервер в мережі AWS з ціллю підвищення безпеки, зниження витрат часу і запобігання людського фактору при створенні усього комплексу ресурсів.

3 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СТВОРЕННЯ І НАЛАШТУВАННЯ VPN-СЕРВЕРУ

3.1 Інструменти для розробки програмного продукту

Для реалізації програмного продукту була обрана мова програмування Python. Вона має низку переваг для досягнення цілей функції програмного забезпечення. Мова програмування Python була публічно випущена на початку 1990-х років для використання в системному адмініструванні. Вона набула великого успіху у даній галузі і зазнала широкого прийняття.

Python - це мова програмування загального призначення, яка використовується майже в кожній сфері інформаційних технологій. Зовсім недавно це стало фактичною мовою науки про дані (Big Data) та машинне навчання (Machine Learning). Мова використовувався в різних галузях, від авіації до біоінформатики. Python має великий арсенал інструментів для покриття широких потреб своїх користувачів.

До особливостей Python відноситься:

- Простота у підтримці: програмний код Python досить простий для розуміння іншими людьми;
- Широка стандартна бібліотека модулей: Основна частина бібліотеки Python досить об’ємна і включає в себе різноманіття включених пакетів;
- Інтерактивний режим: Python має підтримку інтерактивного режиму, який дозволяє інтерактивне тестування та налагодження фрагментів коду;
- Інтеграція: Сценарії Python можуть легко взаємодіяти з іншими частинами програми завдяки різним механізмам інтеграції;
- Портативність: Python може працювати на найрізноманітніших апаратних платформах і має однаковий інтерфейс на усіх платформах, сумісна з багатьма популярними архітектурами операційних систем, таких як UNIX, Windows та Mac;
- Розширюваність: Можливість додати модулі до інтерпретатора Python, написані спільнотою. Ці модулі дозволяють розробникам збагачувати вибір

своїх інструментів, щоб бути більш ефективними і не придумувати “велосипеди”;

– Програмування GUI: Python підтримує створення програм з графічним інтерфейсом, для полегшення взаємодії з програмними продуктами;
– Масштабованість: Python забезпечує кращу структуру та підтримку великих програм, протилежно до підходу створення окремих переліків команд (скриптів);

Python – інтерпретована мова програмування, це означає, що замість процесу компіляції (перекладу програмного коду до машинного, зрозумілий комп’ютеру) його код спочатку транслюється в байт-код. Байт-код являє собою перелік інструкцій, які можуть бути виконані інтерпретатором. Замість виконання процесором команд, інструкції з байт-коду виконуються на так званій віртуальній машині, за рахунок чого досягається однакова робота на усіх платформах.

Даній мові програмування часто приписують "повільність". Хоча термін є відносним і на рахунок цього існує багато суперечок, причина повільності полягає в тому, що інтерпретатор повинен виконати додаткову роботу, щоб інструкція з байт-коду була переведена у форму, яка може бути виконана процесором. На рисунку 3.1 зображена різниця в роботі інтерпретатора і компілятора.

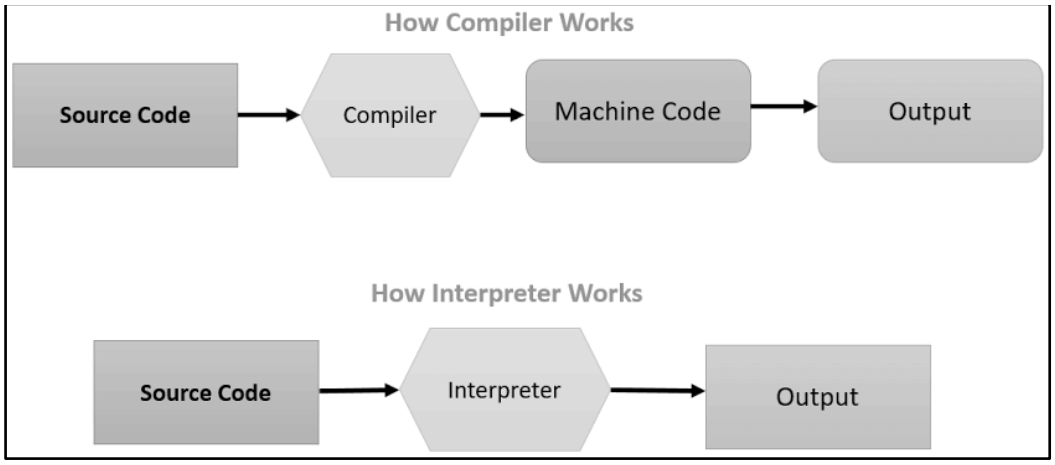


Рисунок 3.1 – Схема роботи інтерпретатора і компілятора

Як було описано вище, одною з основних переваг Python є велика кількість модулів. По суті кожен файл Python-файл, в якому реалізовані функції, являється

модулем. Це означає, що можливо імпортувати цей файл і користуватись вже готовими функціями з нього. Завдяки розробникам по усьому світі, було створено безліч таких модулів, як невеликих з декількома корисними функціями, так і абсолютно масивних, що самі по собі являються основою для програмних продуктів. В інших мовах програмування їх називають “Фреймворки”. Для встановлення модулів разом з Python в комплекті є вбудований менеджер пакетів “pip”.

В основі реалізації задуманого програмного продукту лежить модуль під назвою “boto3”. Даний модуль був створений розробниками AWS, він включає в себе набір інструментів для розробки програм, використовують і взаємодіють програмним інтерфейсом AWS. Завдяки ньому можливо робити виклики, постачаючи в них повну конфігурацію сервісу або об’єкту, або ж дізнаватися інформацію з вже існуючих компонентів. Майже усе, що користувач може зробити через інтерфейс на сайті, можливо описати за допомогою коду. Передумовами для користування ним є вилучені з акаунту користувача дані для програмного доступу з відповідними правами на маніпуляції з ресурсами, AWS_ACCESS_KEY_ID та AWS_SECRET_ACCESS_KEY.

Іншим важливим компонентом для створення графічного інтерфейсу послугував модуль “tkinter”, один із популярних, простих, але дуже потужних компонентів. Він дозволяє створювати віконні додатки з різними елементами, такими як кнопки, текстові поля, надписи, повзунки, списки тощо. Для зв’язання програмної логіки з інтерфейсом, в tkinter існує концепт подій – простіше кажучи, функції, які будуть викликатися при маніпуляціях з об’єктами. Такі події закріплюються за об’єктами, обираються умови спрацювання.

Boto3 і tkinter лежать в основі розробки програмного забезпечення даної роботи. Вони вирішать проблеми з взаємодією користувача з програмою, а програми з ресурсами AWS. Останнім компонентом являється налаштування самого серверу після його створення нашим додатком. Повністю реалізувати це на мові Python не має можливості – вона не передбачена для таких цілей. Оскільки ядром більшості операційних систем на серверах є Linux, для виконання

команд необхідно додатково створити файли з певними інструкціями для налаштування VPN і його користувачів мовою програмування Bash, що лежить в основі даних систем.

Завдяки тому, що при створенні серверу в AWS є можливість додати файл з командами для налаштування мовою Bash, досягається автоматична конфігурація VPN на сервері. За допомогою іншого сервісу AWS SSM, на вже створеному сервері можна викликати сценарії для створення записів клієнтів, з поточним поверненням виводу в якості зворотної відповіді від API-виклику.

3.2 Опис роботи розробленого програмного забезпечення

Після запуску програми перед користувачем з’явиться наступне вікно:

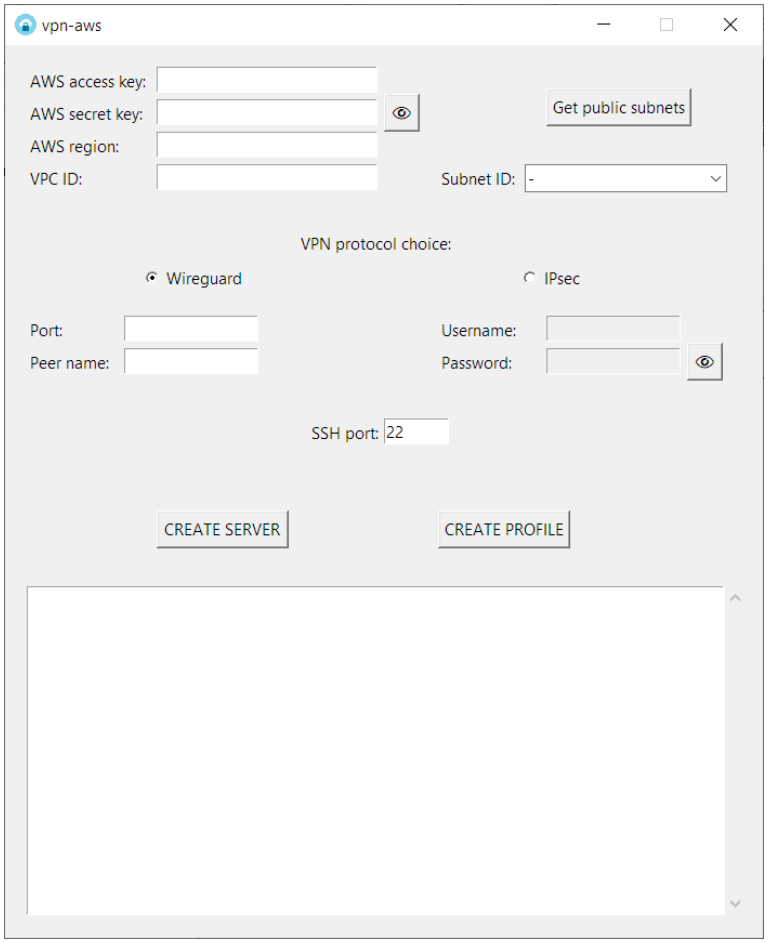


Рисунок 3.2 – Початкове вікно програми

Умовно інтерфейс можна поділити на три частини. Перша частина слугує для автентифікації та авторизації користувача за допомогою AWS_ACCESS_KEY_ID та AWS_SECRET_ACCESS_KEY. Також, необхідно ввести регіон і ідентифікатор мережі VPC. Дані поля є обов'язковими для заповнення і для подальшої роботи програми.

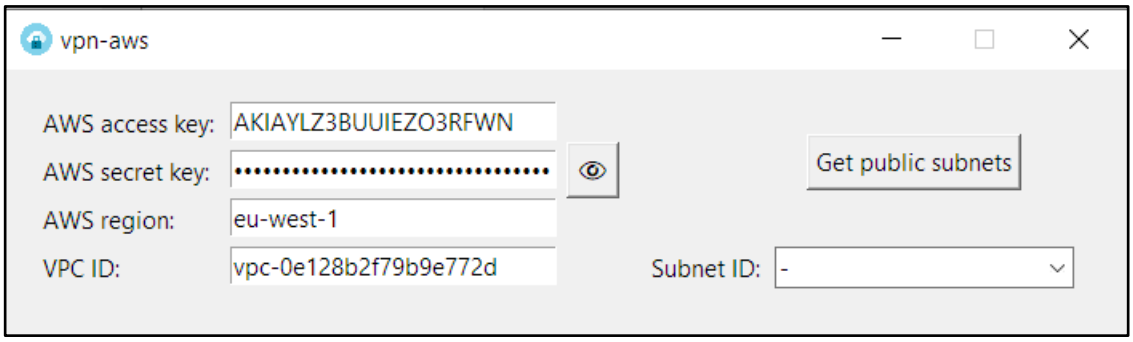


Рисунок 3.3 – Коректне заповнення необхідних полів

Після наповнення 4 полів, треба натиснути на кнопку «Get public subnets». Вона автоматично просканує обрану мережу на наявність в ній публічної підмережі. Це являється однією з умов для створення VPN, адже необхідно мати доступ з Інтернету до підмережі серверу. Якщо такі підмережі існують, їх унікальні ідентифікатори будуть додані до випадаючого списку нижче, де його можна розкрити і обрати підмережу за бажанням.

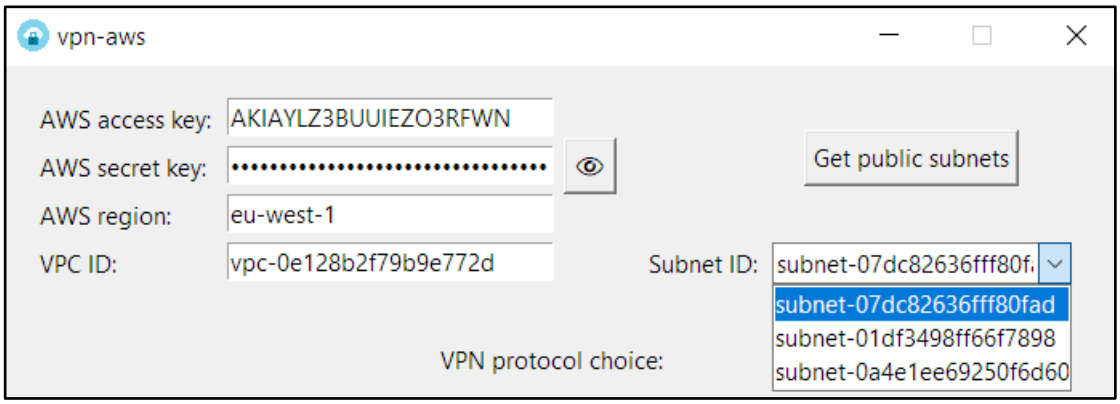


Рисунок 3.4 – Результат отримання публічних підмереж

У випадку не існування хоча б однієї потрібної підмережі, на екран буде виведене попередження про це.

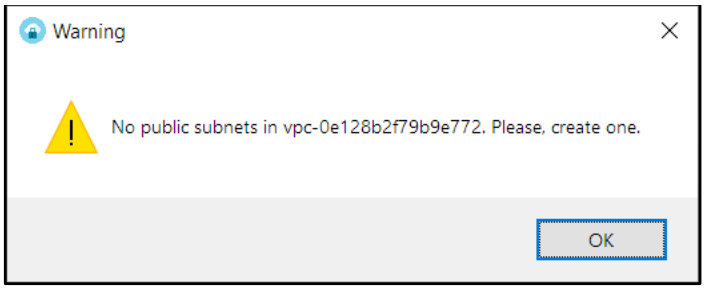


Рисунок 3.5 – Вікно попередження відсутності публічних підмереж

Другою частиною інтерфейсу є вибір протоколу тунелювання, реалізований за допомогою перемикачів. Вибір одного деактивує поля іншого. Користувачу надається можливість обрати між Wireguard та IPsec. В залежності від опції будуть виконані різні сценарії команд для відповідного налаштування. Також кожен протокол потребує свої дані, які заповнюються в текстові поля.

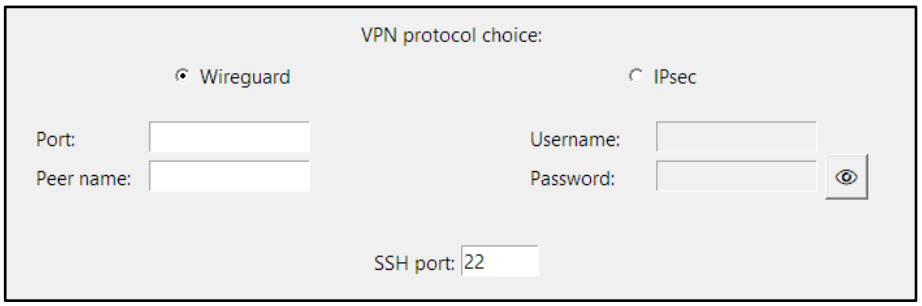


Рисунок 3.6 – Частина вибору протоколу тунелювання

Для демонстрації першого протоколу оберемо Wireguard. В поле «Port» можна ввести порт, на якому бажано щоб працював VPN-сервіс. «Peer name» – ім’я конфігурації майбутнього клієнту. Поле «SSH port» за замовчуванням має значення 22, але дозволяє обрати інший порт для SSH-під’єднання. Це є хорошою практикою для підвищення рівня безпеки самого серверу, оскільки порт під номером 22 найчастіше піддається атакам зловмисників.

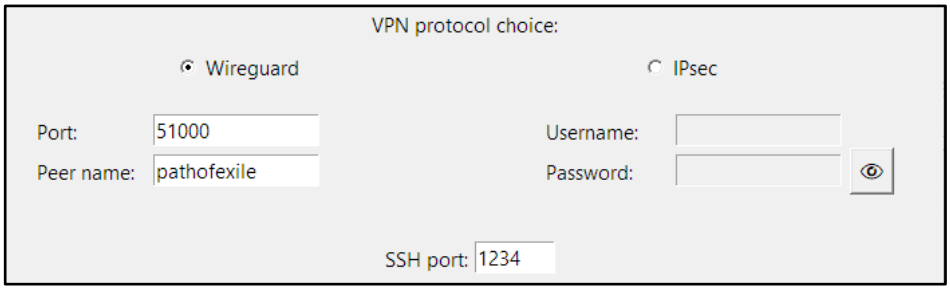


Рисунок 3.7 – Заповнення налаштувань протоколу Wireguard

На поля з обиранням портів накладені обмеження у виборі. Для Wireguard – з 49152 до 65530 (динамічні порти), для SSH – з 1024 до 32767 (вільні) + 22. При невірному вводі виникне помилка.

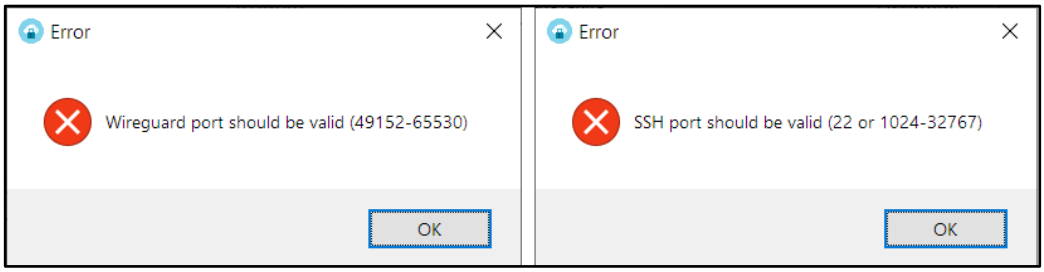


Рисунок 3.8 – Результат контролю невірних значень портів

Третя умовна частина програми – кнопки для створення серверу і конфігурації клієнтів, а також текстове вікно, в якому будуть виводитись інформаційні повідомлення, пов’язані з проходженням процесу створення. Також з даного вікна можливо вилучити готові дані для клієнтів, які можна одразу ж використовувати. Натиснемо на кнопку створення серверу.

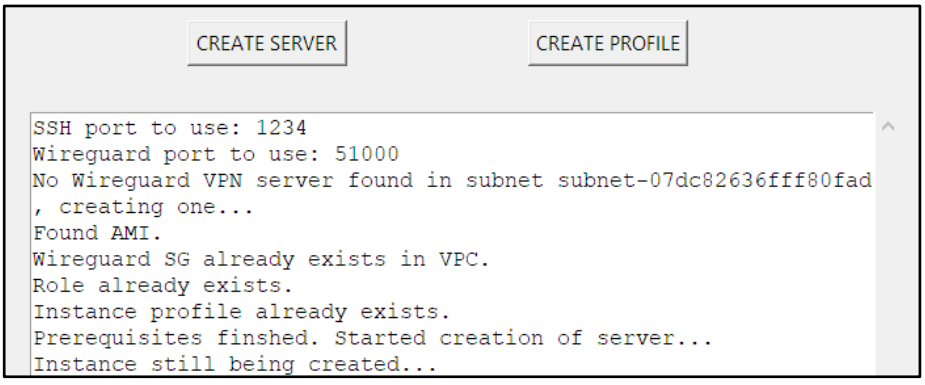


Рисунок 3.9 – Вивід подій при створенні серверу

З інтервалом в 10 секунд буде створюватись API-виклик, який перевіряє готовність VPN-серверу до роботи. Якщо сервер ще створюється, в текстове вікно буде записано відповідне повідомлення. Як тільки він отримає відповідь про успішне створення, наступне вікно буде виведене:

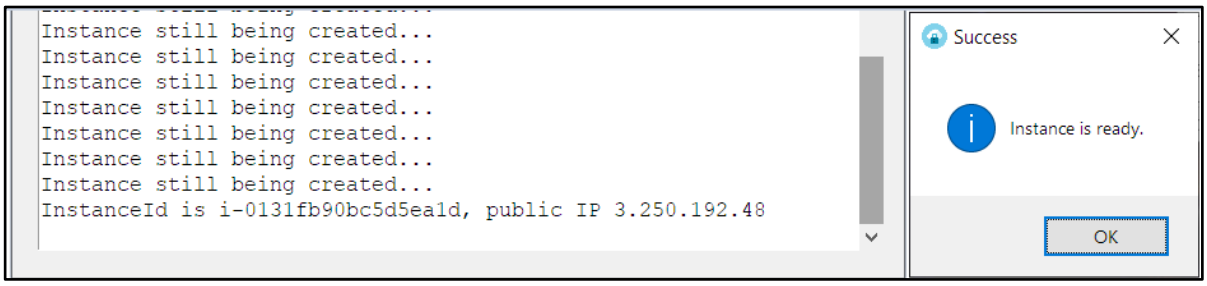


Рисунок 3.10 – Повідомлення про успішність створення VPN-серверу

Налаштування клієнта відбувається аналогічним чином при натисненні на відповідну кнопку. Уся необхідна інформація буде виведена у текстове вікно.

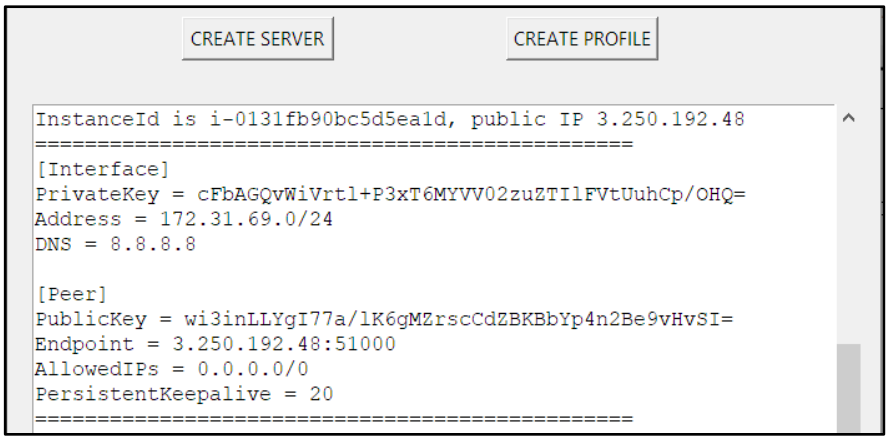


Рисунок 3.11 – Конфігурація клієнту Wireguard

Останнім кроком є запуск і додавання даної конфігурації в VPN-додаток. В додатку потрібно натиснути «Add tunnel» > «Add empty tunnel» > вставити вивід у вікно і зберегти.

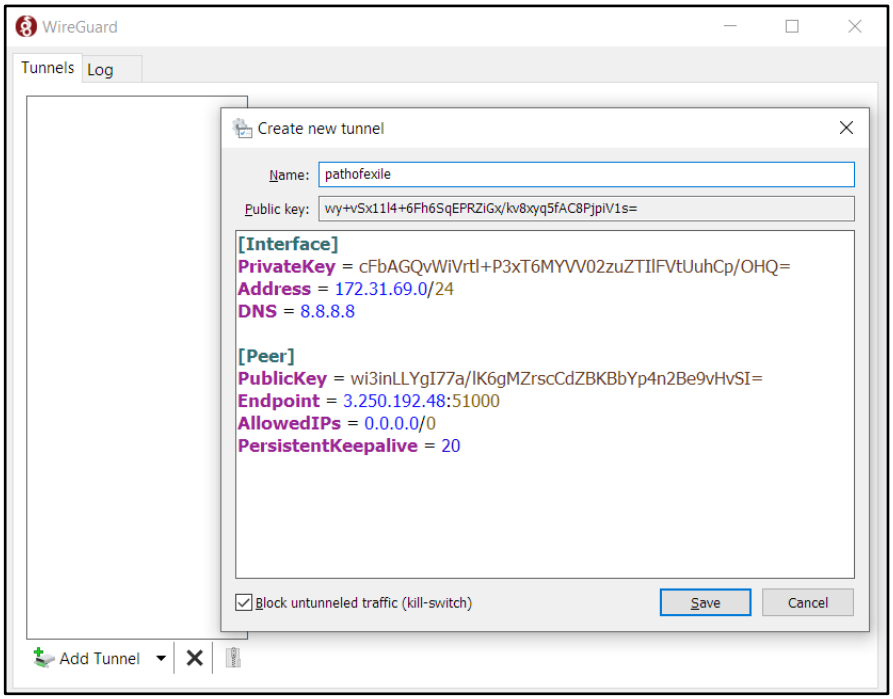


Рисунок 3.12 – Додавання нового тунелю в клієнті Wireguard

Для підключення до серверу потрібно обрати тунель і натиснути «Activate». Для перевірки роботи тунелю оберемо внутрішню адресу попередньо створеного тестового серверу, який розташований у приватній підмережі і спробуємо отримати від нього відповідь утилітою «Ping». В результаті не отримуємо відповіді.

```
C:\Users\foxth>ping 172.31.64.124

Pinging 172.31.64.124 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.31.64.124:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рисунок 3.13 – Тест під'єднання без активованого тунелю

Активуємо тунель і перевіримо з’єднання повторно. У цей раз ми отримуємо відповіді від серверу, розташованого у приватній підмережі. Це означає, що сервер налаштовано правильно, а створення клієнта відбувається коректно.

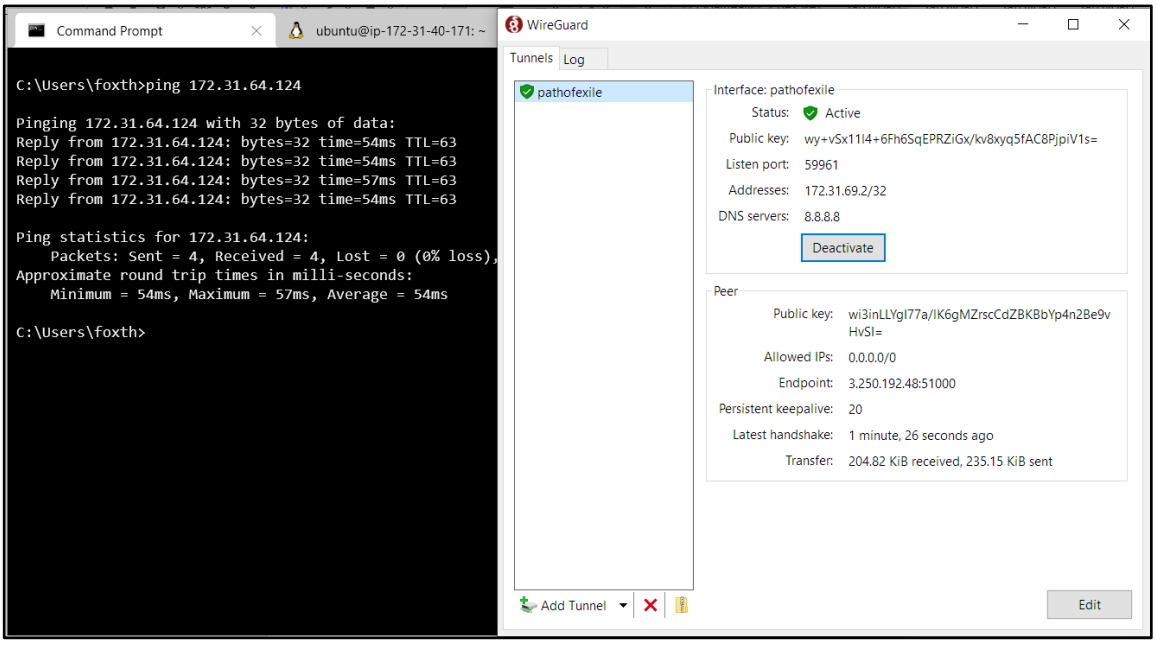


Рисунок 3.14 – Зв’язок з сервером через активований тунель Wireguard

Далі оберемо для демонстрації інший протокол – IPsec. Введемо дані для майбутнього клієнта. Для нього використовується інший сценарій налаштувань.

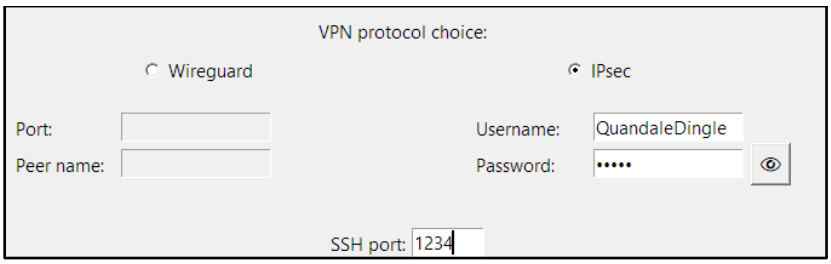


Рисунок 3.15 - Заповнення даних клієнта IPsec

В результаті буде створений сервер, а у текстове вікно виведеться необхідна інформація, якою можна користуватись клієнту.

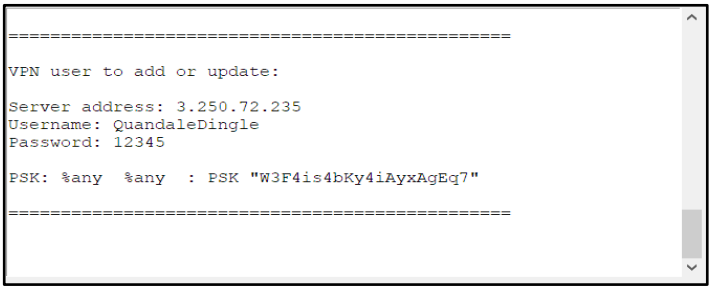


Рисунок 3.16 – Дані для створення тунелю

Для під’єднання до внутрішньої підмережі, в операційній системі Windows 10 є вбудований VPN-додаток. Його необхідно відкрити і заповнити відповідні поля, використовуючи дані з виводу програми.

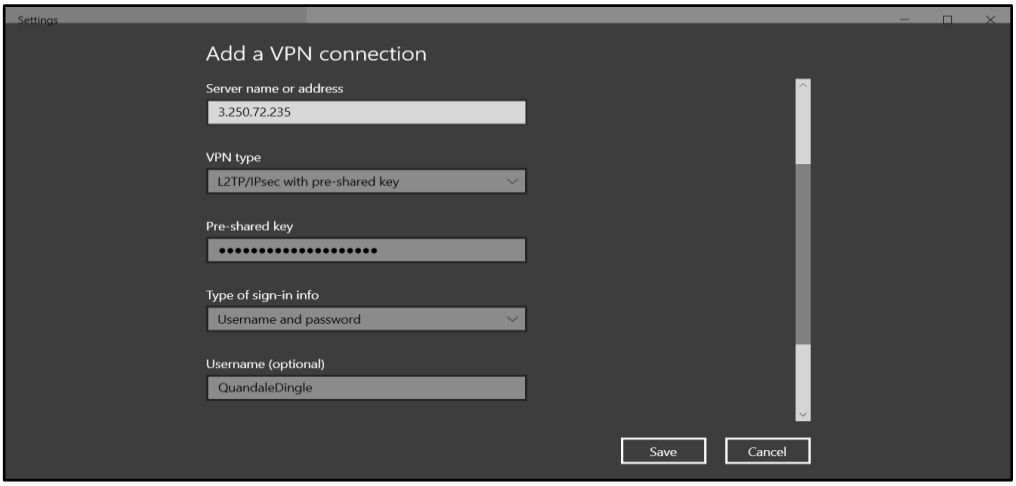


Рисунок 3.17 - Додавання нового VPN-з’єднання в клієнті Windows IPsec

Після додавання нового з’єднання активуємо його і спробуємо за допомогою утиліти «Ping», так само, як і з протоколом Wireguard, отримати відповідь від серверу, що знаходиться в приватній мережі.

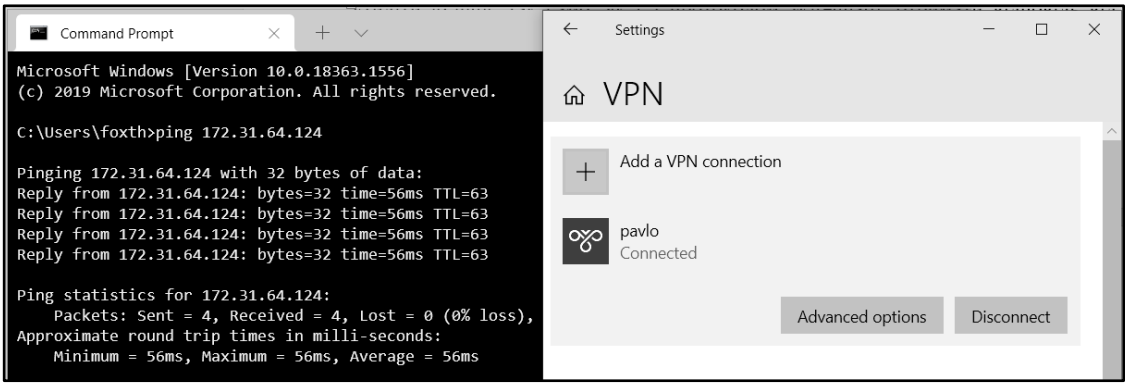


Рисунок 3.18 - Зв’язок з сервером через активований тунель IPsec

Як можна побачити, до серверу є доступ з мережі Інтернет, що свідчить про правильне налаштування як серверу так і клієнту. Консоль AWS, в інтерфейсі якого можливо побачити створений IPsec VPN-сервер, виглядає наступним чином:

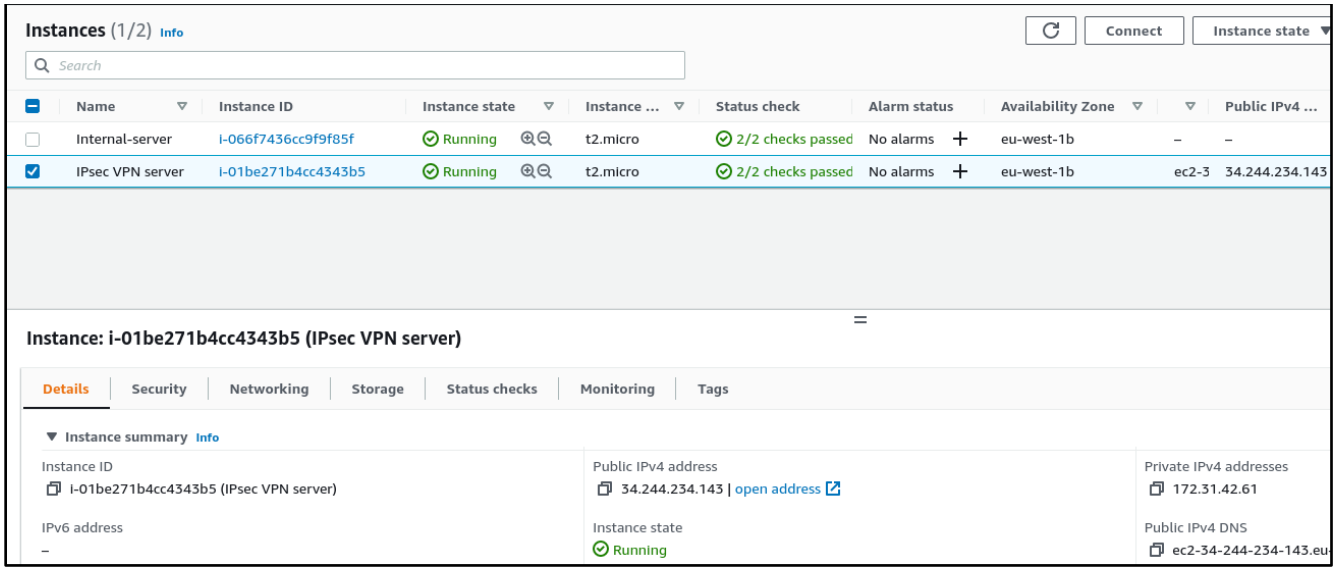


Рисунок 3.19 – Консоль сервісу EC2 зі списком серверів

В консолі при виділенні серверу можна дізнатись всю інформацію про нього, включаючи його публічну і приватну адресу, підмережу, групи безпеки, ролі, стан, можливість підключення і назву ключа, за допомогою якого можна під’єднатися адміністратору для конфігурування, якщо виникне така потреба.

4 ОХОРОНА ПРАЦІ

Охорона праці займається питаннями безпеки людини на виробництві. Виходячи з визначення науки «охорона праці», система охорони праці поєднує сукупність правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів і засобів, що спрямовані на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

Метою охорони праці є створення необхідних умов для безпечної життєдіяльності на робочому місці. Робочим місцем для спеціаліста з інформаційної безпеки для вирішення задачі розробки програмного продукту є стіл з розміщеним на ньому персональним комп’ютером і необхідної периферії (монітор, клавіатура, миша і т.д.). Також невід’ємним елементом роботи є робоче крісло. Джерело живлення для комп’ютера може потребувати від 100 до 600 Вт споживання, робоча напруга 5-12В для персональних комп’ютерів, 15-20В для ноутбуків.

Згідно з ГОСТ 12.0.003-74 умови праці визначаються сукупністю факторів виробничого середовища, які впливають на здоров’я і працездатність людини у процесі праці. Чинники поділяються на небезпечні і шкідливі. Виходячи з умов праці на описаному вище робочому місці були визначені шкідливі і небезпечні фактори:

- відсутність або нестача природного світла;
- недостатня освітленість робочої зони;
- підвищена яскравість світла;
- знижена контрастність;
- підвищений рівень шуму на робочому місці;
- підвищена чи знижена температура повітря робочої зони;
- підвищена чи знижена вологість повітря;
- підвищена запиленість повітря робочої зони;
- підвищена чи знижена рухливість повітря;

– підвищене значення напруги в електричному ланцюзі, замикання якого може статися через тіло людини;
– підвищений рівень статичної електрики.

При роботі за монітором в неоптимальних умовах можливо завдати шкоди органам зору. Раціональне виробниче освітлення повинне попереджати розвиток зорового і загального стомлення, забезпечувати психологічний комфорт при зорових навантаженнях, сприяти збереженню працездатності, а також підвищенню безпеки праці [15].

Залежно від природи джерела світлової енергії розрізняють три види освітлення: природне, штучне і суміщене. За будівельними нормами і правилами ДБН В.2.5-28-2006 необхідно, щоб усі виробничі, підсобні, складські та допоміжні приміщення були забезпечені денним світлом (для приміщень з постійним перебуванням людей) [16]. Для офісного приміщення ідеальним варіантом буде суміщене джерело освітлення, при якому недостатнє за нормами природне освітлення доповнюється штучним освітленням загального типу, регламентоване ДСанПін 3.3.2.007-98. Такий підхід зумовлений потребою напруження зору при роботі з дисплеєм. Це надає можливість регулювати рівень освітленості протягом дня в різні пори року. Таким чином, легко можна досягнути нормованого рівню освітленості на робочому столі – 300-500 лк.

Яскравість монітору необхідно корегувати відповідно до умов праці. Через поганий контраст дисплею з навколишнім фоном може виникнути додаткове навантаження на очі. Таким чином, при роботі в добре освітлювальному приміщені має сенс підвищити яскравість для кращого розрізнення елементів. Якщо є необхідність працювати в кімнаті з приглушеним світлом, потрібно зменшити яскравість. Але в ідеалі потрібно забезпечити рівномірність і постійність освітленості на комфортному і нормованому рівні.

Відомо, що так зване “синє випромінювання” від монітору може деяким чином відобразитись на нашому самопочутті. Наші очі здатні бачити в діапазоні від 380 до 780 нм. Синій колір має найкоротшу хвилю, порядку 400-450 нм,

коротше його вже невидимий нами ультрафіолет. Це значить, що у фотонів більше енергії, з чого можна зробити висновок, що вони більш руйнівні.

Синє світло від дисплею може вплинути на цикл сну. Датчики світла в очах можуть відрізнити денне світло від нічного. Яскраве денне світло має інтенсивні сині хвилі. Більш теплі червоні тони говорять про те, що день закінчується. Коли світло навколо вас переходить у теплі відтінки заходу сонця, датчики в ваших очах запускають ваше тіло, щоб вивільнити природні запаси мелатоніну - гормону, що викликає сон. Через свою довжину хвилі, синє світло порушує фізіологію здорового сну. Тому для вирішення даної проблеми можна встановити програму для зміни відтінку дисплею на більш теплий. Іншим варіантом виступають спеціальні окуляри, які фільтрують синє світло.

При роботі за комп’ютером люди часто протягом довгого часу фокусуються на екрані, що призводить до зменшення частоти кліпання очима. В середньому значення кількості блимань становить 12 разів на хвилину, а при фокусі уваги на чому небуть - 6 разів. В результаті око не отримує достатнього зволоження, сльози встигають випаровуватися з поверхні очей, що викликає їх сухість та запалення. Такі умови можуть стати причиною розвитку синдрому “сухого ока”. Тому потрібно впровадити перерви у роботі для відпочинку органів зору. Дотримання правила "20-20-20" - кожні 20 хвилин роботи за комп’ютером перерватися на 20 секунд, під час яких потрібно переглянути будь-який об'єкт 20 метрів від вас. Це дозволить очам почати блимати частіше і відпочивати.

Робота, пов’язана з розробкою програмного забезпечення, передбачає багато годин використання дисплею на день, тому в нагоду стають краплі для очей. Вони допоможуть краще змочити очне яблуко і принаймні частково запобігти від сухості та втоми очей.

Шум. Підвищений рівень шуму створює значне навантаження на нервову систему, причому шум, що створюється самою людиною, її не турбує. Шум з фізіологічної точки зору – це шкідливий дратівливий чинник, що впливає на органи слуху і весь організм людини.

Нормування шуму здійснюється згідно з ДСН 3.3.6.037–99 Санітарні норми виробничого шуму, ультра звуку та інфразвуку. Шум на робочих місцях не повинен перевищувати допустимих рівнів, значення яких наведені у ДСН 3.3.6.037–99 [17].

Джерелами шуму в офісному приміщенні можуть виступати: принтери, комп'ютери, клавіатури, кондиціонери, розмови інших людей. В ДСН 3.3.6.037–99 вказано, що гранично допустимий рівень звуку в офісі становить 50 дБА, який забезпечує відсутність ризику набуття вад слуху і майже не впливає на працездатність та стан здоров'я працівників.

Для зменшення рівню шуму на робочих місцях усі інші пристрої і елементи, які можуть призводити до виникнення зайвого звуку, по можливості слід розміщувати в інших приміщеннях. Зовнішні шуми знижують шляхом розміщення на стінах звукопоглинаючого покриття. До засобів звукоізоляції належать акустичні екрани, мінеральна вата, акустичний поролон, штучні поглиначі. Також гарним способом зниження фонового шуму є індивідуальна гарнітура, яка щільно прилягає до голови, тим самим перешкоджає потраплянню звукових хвиль до вуха.

Робота в положенні сидячи може завдати проблем здоров'ю людини. Таке положення тіла загалом не є природнім для нас, тим паче проводити в ньому щонайменше по 8 годин в день. Посилює рівень шкідливості неправильна поза при сидінні, яку займають більшість людей. Довге сидіння в неправильній позі може призвести до незворотних змін в організмі, що призводить до важких захворювань. Сам по собі малорухливий спосіб життя викликає дисфункцію хребта.

Тривала неправильна поза тягне за собою обмеження кровопостачання всієї опорно-рухової системи. Внаслідок цього починаються руйнівні процеси в дисках, суглобах, хребцях, що призводить до обмеження рухливості. Неправильна поза при сидінні збільшує навантаження на спину приблизно на 40%. Порушення нормального кровообігу органів тазу внаслідок сидячої пози і малорухомого способу життя може призвести до розвитку геморою.

Необхідно дотримуватись наступних правил:

- Використовувати зручний комп’ютерний стіл, висота якого повинна бути достатньою для того, щоб при сидінні його край опинявся на рівні сонячного сплетіння;
- Монітор потрібно розташувати і налаштувати так, щоб він стояв на рівні очей, і при роботі голова дивилася точно вперед, оптимальна відстань до екрану 40-75 см;
- Користуватись кріслом, що оснащене підлокітниками і можливістю регулювань необхідних параметрів для адаптації до індивідуальних особливостей людини;
- Необхідно сидіти прямо, спираючись на спинку крісла, що розвантажить хребет і допоможе зняти напруження м’язів спини;
- Ступні мають бути опущені на підлогу або стояти на спеціальній підставці для ніг;
- Руки повинні бути розслабленими, опиратись на підлокітники, лікті не мають висіти у повітрі, оптимальний кут 90-100 градусів.

Для подальшого зниження шкоди від сидячої пози рекомендується кожні 30 хвилин робити перерву на розминку. Розминка може являти собою п’ятихвилинну ходьбу, виконання фізичних вправ, або в крайньому випадку просто встати і потягнутися. Хорошою практикою є впровадження колективних занять з різними видами фізичної активності протягом робочого дня.

Вимоги до офісного приміщення та організації робочого місця. Площу приміщень, в яких розташовують персональні комп’ютери, визначають відповідно до нормативних документів. Виділення достатнього особистого простору для роботи дуже важливо і для нормального психічного стану людини. Відповідно до ДСанПіН 3.3.2.007-98 з розрахунку на одне робоче місце, обладнане ПК, встановлено такі норми:

- площа - не менше 6,0 кв. м.;
- об’єм - не менше 20,0 куб. м.;

– робочі місця повинні бути розташовані на відстані не менше ніж 1 м. від стіни з вікном, і 1,4 м. від звичайної стіни;
– відстань між бічними поверхнями комп‘ютерів має бути більше 1,2 м;

На робочому столі повинно бути достатньо простору. Ніщо не має заважати рухам під час роботи. Усі необхідні предмети мають бути в межах доступності. Безлад на робочому місці може призвести до травм або пошкодження працівником робочого обладнання.

Мікроклімат. До параметрів, які складають мікроклімат в приміщенні, входять: температура повітря, відносна вологість і швидкість руху повітря.

Для визначення оптимальних показників мікроклімату треба скористуватись стандартом ГОСТ 12.1.005-88, в якому зазначені критерії, від яких необхідно відштовхуватись. Робота в офісі передбачає категорію робіт “Легка-1а”, характер перебування – постійне робоче місце, оскільки людина проводить там більше 2 годин підряд. В таблиці 4.1 наведені оптимальні значення мікроклімату в теплий і холодний період року.

Таблиця 4.1 – Оптимальні значення мікроклімату в залежності від пори року

Період року	Холодний	Теплий
Температура повітря, градуси	22 - 24	23 - 25
Відносна вологість, %	40 - 60%	40 - 60%
Швидкість руху повітря, м/с	< 0,1 м/с	< 0,1 м/с

Для підтримки температури в офісному приміщені використовуються кондиціонери, вентилятори і обігрівачі, все залежить від пори року. Оптимальні значення вологості повітря досягаються розміщенням спеціальних зволожувачів повітря.

Офісні працівники часто нехтують якістю повітря, що звичайно ж негативно відображається на самопочутті і стані здоров’я при тривалому впливі на шкіру і органи дихання. В приміщенні накопичується бруд і пил, який застається в повітрі і може потрапити до організму, сприяти закупоренню пор в шкірі. Тому

необхідно організувати хорошу вентиляцію приміщення, регулярно провітрювати його, щоденно робити вологе прибирання та протирати робоче місце від пилу. До систем вентиляції існують наступні вимоги:

- без шуму і вібрацій;
- прилив повітря не має бути спрямований на робочі місця;
- вентиляція не має бути направлена на місця пилоутворення.

Електробезпека. Електробезпека - система організаційних і технічних заходів, засобів та способів, які забезпечують захист від шкідливої і небезпечної дії електричного струму. Причини ураження електричним струмом в умовах офісу:

- на підприємствах не розробляються організаційні заходи, що убезпечують працівників під час роботи;
- допуск до роботи ненавчених працівників та працівників, які не пройшли чергову перевірку знань з питань електробезпеки;
- недостатнє усвідомлення населенням небезпечності дотику до проводів, корпусів та інших відкритих провідних елементів електрообладнання;
- використання несправної техніки.

Частою проблемою в офісних приміщеннях є включення одночасно декількох дуже потужних приладів в один подовжувач, а також перевантажування мережі і створення схем типу «подовжувач в подовжувач». Такі дії можуть призвести до перегрівання проводів, знищення ізоляції з подальшим займанням або коротким замиканням. Необхідно регулярно перевіряти розетки, вилки, вимикачі, шнури - вони повинні мати корпус без пошкоджень та тріщин.

Статична електрика також має місце в офісі. В ролі “генераторів” статичного струму виступають різні електроприлади. При роботі вони створюють електростатичні поля. Тому заряджаються насамперед корпуси цих приладів та інші предмети неподалік, а також частинки пилу. Повітря з низькою вологістю, що додатково підсушується обігрівачами і кондиціонерами, ідеально сприяє утворенню статичних зарядів. Статична електрика може завдати як і злегка неприємні відчуття, наприклад при торканні корпусу може виникнути легкий

удар струмом. Але може статись стрибок напруги в техніці, що призведе до її виходу з ладу.

Щоб забезпечити безпечну роботу співробітників в офісі, приміщення має відповідати всім вимогам пожежної безпеки. Клас передбачуваної пожежі - “Е”, оскільки в приміщеннях встановлено системи, підключені до джерела електроенергії.

Об’єктами потенційної і підвищеної пожежної небезпеки в офісі є комп’ютер, розетки, технічне обладнання, розетки, проводка. Пожежа у приміщенні може виникнути у разі перевантаження блоку живлення, перегрівання, короткого замикання, перенавантаження мережі.

Для забезпечення пожежної сигналізації потрібно встановити спеціальні датчики, що реагують на появу диму або зміни температури в приміщенні. Така сигналізація може просто повідомити працівників про проблему, або ж активувати режим гасіння вогню.

Вогнегасники в офісних приміщеннях необхідно розташувати на видних місцях. Місце для зберігання балона слід вибирати темне, щоб не потрапляли промені сонця. Необхідно захистити балон від несприятливих факторів і механічних впливів, таких як вібрація, підвищена вологість. Кількість вогнегасників на в приміщенні або на поверсі треба розрахувати про принципу, що на кожні 25 м кв. площі має бути не менше 1 кг гасячої речовини, але, звичайно, не менше одного вогнегасника в цілому.

В офісах, де є електричне обладнання, використовують порошкові або ж вуглекислотні вогнегасники. Категорично забороняється використання води для ліквідації пожежі, а також вогнегасників, що утворюють піну. Згідно з правилами пожежної безпеки в Україні відстань між місцями для вогнегасників не повинна перевищувати 20 м, а дистанція до можливого осередку загоряння - 3 м. Балон необхідно оглядати регулярно, від дати останнього перезаряджання не повинно проходити більше року. Результати огляду фіксують в спеціально призначеному для цього журналі.

ВИСНОВКИ

В роботі було досліджено і описано технології і способи для створення з’єднанння за допомогою VPN, а також розроблено програмний продукт для автоматичного налаштування VPN-серверу для доступу до внутрішніх мереж хмарного постачальника Amazon Web Services.

Були проаналізовані різні способи об’єднання мереж між собою, наведені їх переваги та недоліки. Було виявлено найдоречніший і актуальний метод створення з’єднання через мережу Інтернет. Приведені основні загрози інформації при її передавані. Приведений опис технології VPN, що вирішує проблему із передаванням трафіку у відкритому виді, використовуючи шифрування і інкапсуляцію. Також була зазначена актуальність через зростаючу популярність хмарних обчислень.

Детально порівняно різні протоколи тунелювання для побудови VPN-з’єднання, їх сильні і слабкі сторони, при яких умовах доречніше використовувати. Було описано і охарактеризовано постачальника хмарних послуг AWS, розібрані основні концепти і сервіси, що послугували базою для розробки. Також побудована схема топології мережі, яка описує структуру з’єднання і потоку трафіку. Повною мірою викладена проблема, і які аспекти з неї вирішить програмний продукт.

Наведено і обґрунтовано перелік інструментів, що були використані при розробці програмного продукту. Пояснені складові програми, мови програмування, модулі для реалізації функціоналу. Робота програмного продукту була продемонстрована рисунками із текстовим супроводом.

Також були проаналізовані умови праці та визначено заходи і засоби захисту від небезпечних та шкідливих факторів на робочому місці. Наведені рекомендації і правила щодо дотримання пожежної безпеки в офісному приміщенні.

ПЕРЕЛІК ПОСИЛАНЬ

1. Визначення хмарних сервісів. URL:
https://www.redhat.com/en/topics/cloud-computing/what-are-cloud-services
2. Підслуховування в мережі. URL:
https://hackinglab.cz/en/blog/wiretapping/
3. R. Fisli, “Secure Corporate Communications over VPN-Based WANs,” Master’s Thesis in Computer Science at the School of Computer Science and engineering. Sweden: Royal Institute of Technology, 2005. P.61-83
4. Khan M., DeBlasio J., Voelker G.M., Snoeren A.C., Kanich C., Vallina-Rodriguez N. An Empirical Analysis of the Commercial VPN Ecosystem. *IMC.* 2018.P.170-186
5. Donenfeld J. WireGuard: Next Generation Kernel Network Tunnel. URL: http://www.wireguard.com/papers/wireguard.pdf
6. Криптографічні алгоритми в протоколах тунелювання, URL:
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.503.7298&type=pdf
7. Огляд концепції хмарних обчислень, URL:
https://www.torryharris.com/downloads/Cloud-Computing-Overview.pdf
8. Статистика використання хмарних обчислень, URL:
https://www.cloudwards.net/cloud-computing-statistics/
9. Огляд популярних протоколів тунелювання, URL:
https://www.netmotionsoftware.com/blog/connectivity/vpn-protocols
10. Опис протоколу Wireguard, URL:
https://www.wireguard.com/performance/eguard.pdf
11. IPsec, Матеріал з вікіпедії – вільної енциклопедії. URL:
https://ru.wikipedia.org/wiki/IPsec
12. Впровадження Wireguard до ядра Linux, URL:
https://lists.zx2c4.com/pipermail/wireguard/2020-March/005220.html
13. Оцінка і порівняння роботи основних VPN-протоколів, URL:
https://www.wireguard.com/performance/
14. Розподіл ринку в розрізі хмарних постачальників на 2022, URL:

https://www.channele2e.com/news/cloud-market-share-amazon-aws-microsoft-azure-google/

15. Березуцький В.В., Васьковец Л.А., Горбенко В.В., В.Ф. Райко В.Ф., Янчик О.Г. Основи професійної безпеки та здоров'я людини. Харків: НТУ ХПІ, 2018. 553с.

16. ДБН В.2.5-28-2006. Державні будівельні норми України. Інженерне обладнання будинків і споруд. Природне і штучне освітлення. [Чинний від 2006.05.15]. Київ, 2006. 22с.

17. ДСН 3.3.6.037–99. Державні санітарні норми. Санітарні норми виробничого шуму, ультразвуку та інфразвуку. [Чинний від 1999.12.01]. Київ, 1999. 15с.