DOI 10.15276/imms.v12.no1-2.73
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 73-83

АВТОМАТИЗАЦІЯ КОНФІГУРУВАННЯ БЕЗПЕЧНОГО ПІД'ЄДНАННЯ ДО КОРПОРАТИВНИХ МЕРЕЖ

П.Ю. Паталашко, Н.І. Кушніренко

Національний університет «Одеська Політехніка», просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: infsec2011@gmail.com

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. Проблема забезпечення безпеки інформації саме на стадії транспортування через мережу Інтернет має досить великий пріоритет для досліджень і створення різних підходів 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, на яку націлена технологія віртуальних приватних мереж. Ще однією вагомою причиною для використання технології VPN є стрімкий розвиток і зростання популярності хмарних сервісів. 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 неминучим проходженням інформації через неї. Розроблений програмний продукт може бути рекомендований для використання на практиці при реальних потребах компаній, які використовують постачальника хмарних послуг Amazon Web Services для автоматизованої організації безпечного з'єднання з внутрішніми мережами. Також дана розробка може виступати основою для втілення аналогічних рішень, які задовольняють умови кожного користувача індивідуально, оскільки кодова база буде спільною для будь-якого постачальника.
Ключові слова: віртуальні приватні мережі, передача даних, організація безпечного з'єднання, протоколи тунелювання, хмарні сервіси, AWS.

Вступ

Зараз технологія VPN є стандартом в сфері інформаційних технологій для об'єднання декількох пунктів зв'язку між собою. 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.

Основними проблемами підходу зі створенням VPN-тунелю є досить важке налаштування серверу і створення та менеджмент конфігурацій клієнтів. Для коректної роботи не достатньо лише згенерувати дані для входу клієнта, але й занести відповідні записи до певних файлів серверу, перезавантажити програмну частину. Зі збільшенням клієнтів, значно збільшується і складність підтримки серверу. Враховуючи, що системному адміністратору доводиться робити усі дії вручну, це може погіршити загальну безпеку через можливість впливу людського фактору. Тому актуальним завданням є повна автоматизація усіх мануальних кроків, від створення і налаштування серверу до додавання конфігурацій клієнтів, які можуть бути використані для безпечного під'єднання по шифрованому тунелю одразу після отримання.

Мета і задачі дослідження

Метою роботи є підвищення рівню безпеки і автоматизації створення під'єднання до внутрішніх корпоративних мереж шляхом розробки спеціалізованого програмного продукту, зокрема сфокусованого на хмарних технологіях. За рахунок такого підходу підвищиться рівень безпеки і автоматизації організації з'єднання, та сильно знизяться ризики людського фактору і витрати часу при конфігуруванні власноруч. В процесі виконання даної роботи необхідно розв'язати наступні задачі:

– розглянути і проаналізувати різні підходи до організації зв'язку між сегментами мереж, визначити загрози інформації при передачі;

– провести аналіз та порівняння сучасних протоколів тунелювання;

– обрати необхідні компоненти AWS для створення серверу;

– створити схему топології мережі;

– розробити програмний продукт для повної автоматизації конфігурації VPN-серверу і клієнту.

Основна частина

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. Наприклад, 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 [1].

– 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 [1].

– 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 [1].

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.

Тунель через публічну мережу – ще одне альтернативне рішення. Якщо обидва умовні вузли зв'язку мають доступ до Інтернету, найдешевший і найлегший у підтримці спосіб - побудувати тунель між цими двома точками. Для цього необхідно мати 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.

В Інтернет-просторі існує велика кількість різних загроз цілісності, доступності і конфіденційності інформації. В розрізі дослідження розглядаються загрози даним в процесі передачі. Типи кібератак «Людина посередині» (MITM) відносяться до порушень кібербезпеки, які дають можливість зловмиснику підслуховувати дані, що пересилаються між двома людьми, мережами або комп’ютерами [2]. Це називається атакою «людина посередині», оскільки зловмисник розташовується «посередині» або між двома сторонами, які намагаються спілкуватися. Під час атаки MITM обидві залучені сторони відчувають, що спілкуються, як зазвичай. Але особа, яка фактично надсилає повідомлення, має можливість незаконно модифікувати повідомлення або отримати доступ до нього, перш ніж воно досягне місця призначення.

Перехоплення сесії є також поширеним способом отримання несанкціонованого доступу. 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.

Описані загрози конфіденційності і цілісності інформації мають прямий вплив на надійність, якість та коректне функціонування інфраструктури, що лежить в основі майже усіх сфер діяльності, включаючи освіту, банківську справу, бізнес і медицину. 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.

Технологія VPN (Virtual Private Network), на основі якої можливо з’єднати декілька мереж в одну, при цьому забезпечити гнучкість та одночасно високу швидкість передачі даних, а головне - безпеку при обміні інформацією [4]. 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.

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.

Існує багато характеристик VPN-протоколів. Вони різняться за кількістю підтриманих алгоритмів шифрування, швидкістю з'єднання, гнучкістю налаштувань і складністю конфігурування. Згідно з дослідженням двома найпоширенішими протоколами для організації VPN являються IPsec (IP Security) та OpenVPN. Відносно нове рішення під назвою Wireguard розробляється для заміни обох попередніх протоколів, при цьому претендуючи на кращу продуктивність [6]. Дані протоколи були взяті до огляду через відкритість їх коду. IPsec і OpenVPN на даний момент є відкритими стандартами для створення VPN-рішень.

OpenVPN - протокол VPN на основі SSL, оскільки він використовує протоколи SSL і TLS для захищеного з'єднання. 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. 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.

Офіційним стандартом IEEE/IETF для безпеки IP є IPSec. Офіційно зареєстровано як RFC2411. Також вбудований у стандарт IPv6. 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.

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.

Відносно новим VPN-протоколом, який має на меті створення простої та ефективної реалізації віртуальної приватної мережі, є Wireguard. 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. Мета дизайну - мати загальну пряму конфігурацію, схожу до SSH, тобто криптографію асиметричного ключа. Wireguard використовує найсучасніші криптографічні алгоритми, 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 [7].

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 [8]. На рис.1 приведений тест швидкості протоколів з офіційної веб-сторінки.

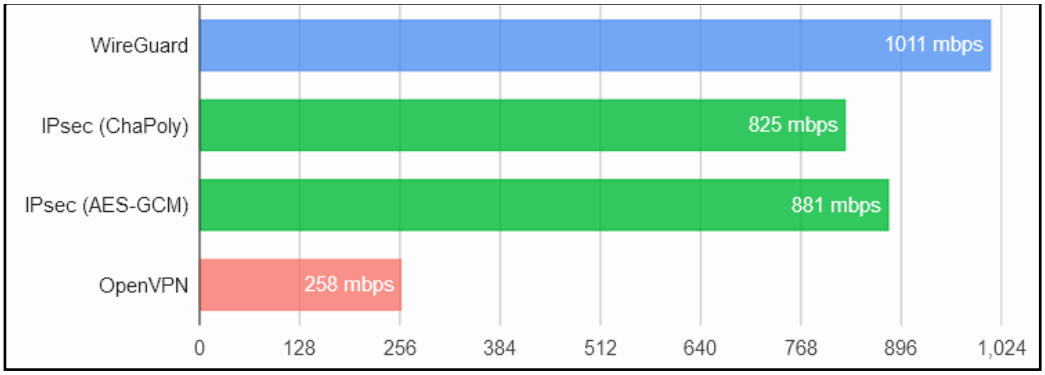

Рис.1. Порівняння швидкості роботи VPN протоколів

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.

У якості постачальника хмарних послуг було обрано Amazon Web Services. Виходячи зі статистики на 1 квартал 2022 року, 62% світового ринку хмарних послуг займають AWS, Microsoft Azure і Google Cloud Platform [9]. AWS в свою чергу має 33% усієї долі ринку. Тому даний провайдер є більш пріоритетною ціллю для організування до нього безпечного з'єднання.

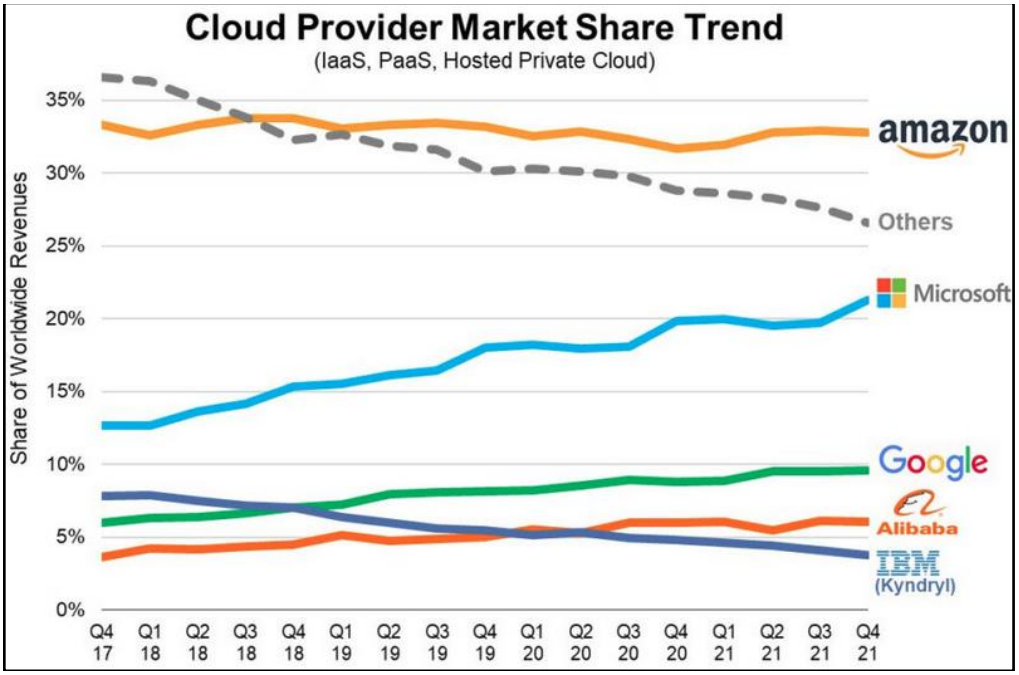

Рис.2. Світовий ринок постачальників хмарних послуг

AWS поділяється на різні сервіси: кожен може бути налаштований різними способами залежно від потреб користувача. Наразі кількість сервісів перевищує 200 одиниць. 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 [10]. Підмережі бувають приватними і публічними. До приватних підмереж немає доступу з зовнішнього інтернету, до них можна отримати доступ лише з середини. 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 [10]. 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.

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, і організувати автоматичне створення і налаштування VPN-серверу в публічній підмережі.

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 рис.3, з'являється можливість для втілення плану такої схеми в реальних умовах.

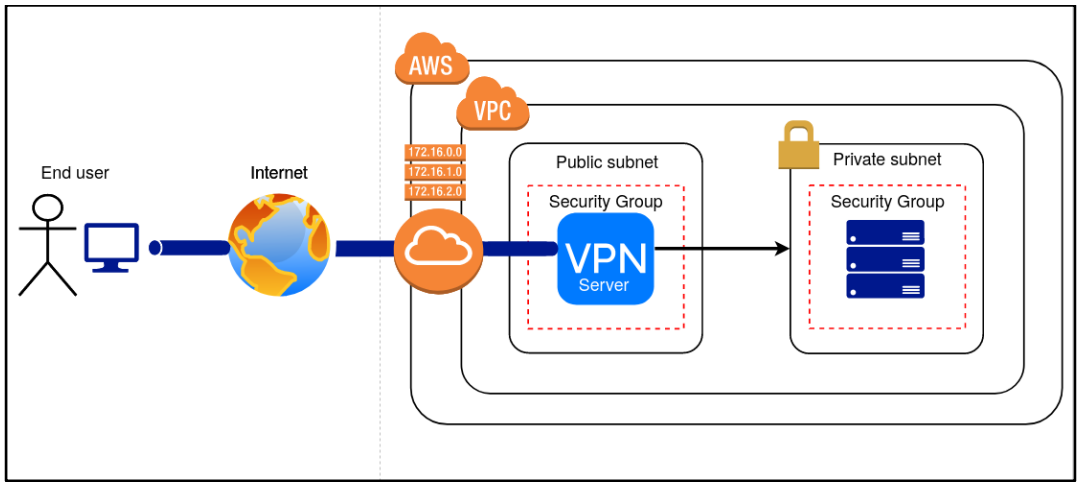

Рис.3. Схема топології мережі та з'єднання

Основною 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.

Для реалізації програмного продукту була обрана мова програмування Python через її потужність і модульність. В основі задуманого програмного продукту лежить модуль під назвою “boto3”. Даний модуль був створений розробниками AWS, він включає в себе набір інструментів для розробки програм, які використовують і взаємодіють з 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.

В результаті роботи була створена програма, що працює за наступною логікою:

– Введення та валідація даних для доступу в AWS і їх мережу;
– Перевірка на наявність та отримання ідентифікаторів публічних підмереж;
– Вибір протоколу тунелювання через елемент RadioButton, зміна портів за необхідністю;
– Створення серверу із заданою конфігурацією;
– Після попереднього кроку, уведення та перевірка даних для користувача, з подальшим створенням конфігурації клієнту;
– Отримання виводу програми з готовими налаштуваннями для клієнту.

Інтерфейс готового програмного продукту зображений на рис.4., а результат її відпрацювання (вивід готових даних для створення тунелю) – на рис.5.

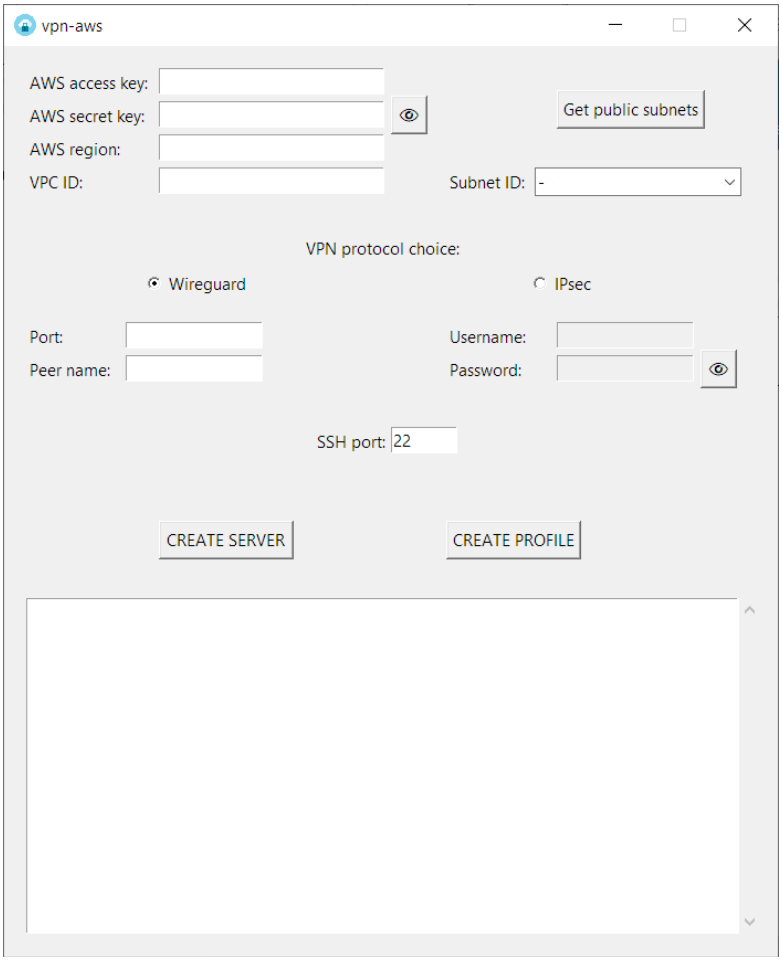

Рис.4. Інтерфейс програми

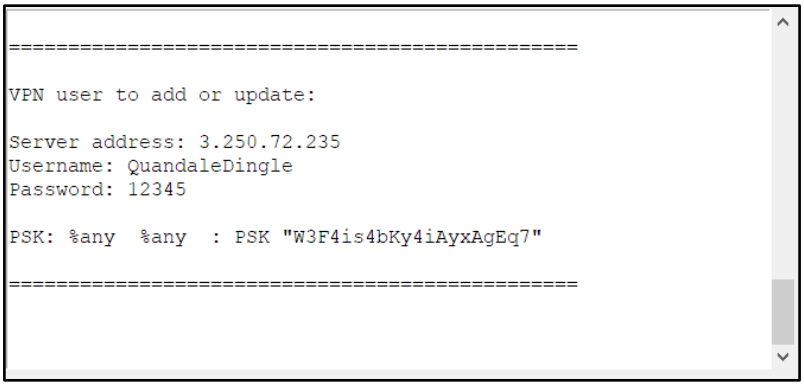

Рис.5 Приклад готової конфігурації для клієнта

Висновки

В роботі було розглянуто сучасні підходи до об’єднання сегментів мереж, їх сильні і слабкі сторони. Було виявлено найдоречніший і актуальний метод створення з’єднання через мережу Інтернет. Приведені основні загрози інформації при її передаванні. Приведений опис технології VPN, що вирішує проблему із передаванням трафіку у відкритому виді, використовуючи шифрування і інкапсуляцію.

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.

Розроблене програмне рішення, яке зменшило витрати часу при створенні усіх необхідних компонентів для організації з'єднання, а також мінімізувало 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.

Для подальшого покращення програми рекомендується додати підтримку для більшої кількості хмарних постачальників і VPN-протоколів.

Список літератури

1. Організація комп'ютерних мереж. URL: https://ela.kpi.ua/bitstream/123456789/22890/1/Organizacia_komputernyh_merezh_Konspekt_lekciy.pdf

2. Тип атаки «Людина по середині». URL: https://csrc.nist.gov/glossary/term/man_in_the_middle_attack

3. OWASP Session hijacking threat. URL: https://owasp.org/www-community/attacks/Session_hijacking_attack

4. Fisli R. Secure Corporate Communications over VPN-Based WANs. Master's Thesis in Computer Science at the School of Computer Science and engineering, Royal Institute of Technology, Sweden. 2005. P.61-83

5. Khan M.T., 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

6. Donenfeld J. Next Generation Kernel Network Tunnel. WireGuard, 2018. URL: http://www.wireguard.com/papers/wireguard.pdf

7. Впровадження Wireguard до ядра Linux. URL: https://lists.zx2c4.com/pipermail/wireguard/2020-March/005220.html

8. Оцінка і порівняння роботи основних VPN-протоколів. URL: https://www.wireguard.com/performance/

9. Розподіл ринку в розрізі хмарних постачальників на 2022. URL: https://www.channele2e.com/news/cloud-market-share-amazon-aws-microsoft-azure-google/

10. Огляд найпопулярніших сервісів Amazon Web Services. URL: https://www.clickittech.com/aws/aws-services-list/

AUTOMATION OF CONFIGURATING SECURE CONNECTION TO CORPORATE NETWORKS

P. Patalashko, N. Kushnirenko

National Odesa Polytechnic University,
1, Shevchenko Ave., Odesa, 65044, Ukraine; e-mail: infsec2011@gmail.com

With the rapid development of information technology, there is a increasing need to protect information and securely transmit it over the global network. The purpose of work is the problem of information security, its systematization, identification of sources of information threats, indicators, criteria and standards. The problem of information security at the stage of transportation via the Internet has a high priority for research and the development of various solutions. Virtual private network (VPN) technology was created because of the need to connect computer networks or their segments to each other using a secure communication channel over a network with less trust. From point №1 to point №2, the data must be transmitted in such a way that it cannot be accessed by third parties and only the intended reciever has the ability to obtain and use it. Quite a real and practical problem, the relevance of which grows with each year of development of information technology, which is aimed at the technology of virtual private networks. Another important reason for using VPN technology is the rapid growth of cloud services. The problem of secure access of employees and connection of two or more networks to each other via the Internet must be solved, without increasing the level of threat due to the inevitable intersection of information through open network. The proposed software product can be recommended for use in practice with the real needs of companies that use Amazon Web Services, for automated organization of secure connection to internal networks. Also, this development can serve as a basis for the implementation of similar solutions that will satisfy the conditions of each user individually, as the code base will be same for any provider.
Keywords: virtual private networks, data transmission, organization of secure connection, tunneling protocols, cloud services, AWS.