ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій

Кафедра телекомунікацій, медійних та інтелектуальних технологій

ДИПЛОМНА РОБОТА

Другий (Магістерський)
Освітній рівень

Галузь знань 17 Електроніка та телекомунікації
Шифр і назва спеціальності

Спеціальність 172 Телекомунікації та радіотехніка
Шифр і назва спеціальності

на тему Метод налаштування конфігурації VPN з віддаленим доступом

ДРТР.2021057.01.02.ПЗ

Виконала: студент 2 курсу, група ТРм-21-1 _____ Б.С. Білявець
підпис Ініціали, прізвище

Керівник: д-р техн. наук, проф. _____ Ю.М. Бойко
підпис Ініціали, прізвище

До захисту допускаю:

Зав. кафедри: д-р техн. наук, проф. _____ С.К. Підченко
підпис Ініціали, прізвище

05 _____12_____ 2022 р.

Хмельницький, 2022

Хмельницький національний університет

Факультет *інформаційних технологій*
Кафедра *телекомунікації, медійних та інтелектуальних технологій*
Освітній рівень *другий (магістерський)*
Галузь знань *17 _ Електроніка та телекомунікації*
Спеціальність *172 – Телекомунікації та радіотехніка*
Освітня-професійна програма *Телекомунікації та радіотехніка*

ЗАТВЕРДЖУЮ
Зав. кафедрою__
_____
«_05_»_____09_____ 2022р.

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Білявець Богдані Сергіївні

1 Тема роботи: *Метод налаштування конфігурації VPN з віддаленим доступом*
керівник роботи Бойко Юлій Миколайович, д.т.н, професор.
Затверджено наказом по університету від «01» липня 2022р. № 83.
2 Строк подання студентом роботи на кафедру: 23.11.2022р.
3 Вихідні дані (характеристика об'єкта, умов дослідження та ін.)
Мета роботи полягає у створені VPN тунелю для підключення віддалених користувачів до корпоративної мережі з використанням технології SAML для налаштування доменної аутентифікації.
Предметом дослідження є методи безпечного віддаленого підключення користувачів.
Об'єктом дослідження є процес отримання доступу користувачам до мережі з використанням незалежного серверу аутентифікації SAML.
4 Зміст пояснювальної записки (перелік питань, що їх належить розробити):
1 Літературний огляд та аналіз предметної області. 2 Обґрунтування вибору технології та мережевого обладнання для побудови VPN тунелю. 3 Методи надійного шифрування мереж. 4 Дослідження реалізації віддаленого підключення користувачів з використання технології SAML та порівняльний аналіз розроблених рішень з використанням цієї технології.
Висновки.

Завдання отримала _____
Науковий керівник_____

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів (розділів) дипломної роботи	Строк виконання етапів дипломної роботи	Примітка
1	Вступ. Літературний огляд та аналіз предметної області.	30.09.2022	Вик.
2	Обґрунтування вибору технології та мережевого обладнання для побудови VPN тунелю	15.10.2022	Вик.
3	Методи надійного шифрування мереж	28.10.2022	Вик.
4	Дослідження реалізації віддаленого підключення користувачів з використання технології SAML та порівняльний аналіз розроблених рішень з використанням цієї технології	17.11.2022	Вик.
5	Висновки. Презентаційні матеріали за результатами виконання дипломної роботи.	23.11.2022	Вик.

Студент _____ Б.С. Білявець
підпис Ініціали, прізвище

Керівник роботи _____ Ю.М. Бойко
підпис Ініціали, прізвище

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

SAML	Security Assertion Markup Language	Мови розмітки твердження безпеки
ASA	Adaptive Security Appliance	Адаптивний пристрій безпеки
Wi-Fi	Wireless Fidelity	бездротова правдивість відтворення
IPsec	Internet Protocol Security	Захищений Інтернет-протокол
SSL	Secure Sockets Layer	Рівень Зхищених Сокетів
PPP	Point-to-Point Protocol	Протокол точка-точка
PPTP	Point-to-Point Tunneling Protocol	Тунельний протокол типу точка-точка
L2TP	Layer 2 Tunneling Protocol	Протокол тунелювання другого рівня
TLS	Transport Layer Security	Протокол захисту транспортного рівня
HTTPS	HyperText Transfer Protocol Secure	Захищений протокол передачі гіпертексту
GRE	Generic Routing Encapsulation	Інкапсуляція маршрутів
IP	Internet Protocol	Інтернет Протокол
MFA	Multi-Factor Authentication	Багато факторна аутентифікація
L2TP	Layer 2 Tunneling Protocol	Протокол Тунелювання Рівня 2
LAN	Local Area Network	Локальна Комп’ютерна Мережа
PPTP	Point-to-Point Tunneling Protocol	Протокол Тунелювання точка-точку

TCP	Transmission Control Protocol	Протокол Керування Передачею
TLS	Transport Layer Security	Безпека Транспортного Рівня
VPN	Virtual Private Network	Віртуальна Приватна Мережа
WAN	Wide Area Network	Глобальна Мережа
2FA	2 factor-auth	2 факторна аутентифікація
RDP	Remote Desktop Protocol	Протокол віддаленого підключення
DDoS	Denial of Service	Відмова в обслуговуванні
DMVPN	Dynamic MultiPoint VPN	VPN з можливістю динамічного тунелю
L3VPN	Layer 3 Tunneling Protocol	Протокол Тунелювання Рівня 3
MPLS	Multiprotocol label switching	Багатопротокольна комутація за мітками
XML	Extensible Markup Language	Розширена мова розмітки
NAT	Network Address Translation	Трансляція мережевих адрес
AES	Advanced Encryption Standard	Розширений стандарт шифрування
DES	Data Encryption Standard	Стандарт шифрування даних
RSA	Rivest, Shamir, Adleman	Рівест, Шамір, Адлеман
HMAC	Hash-based message authentication code	Код автентифікації повідомлення на основі хешу
PFS	Perfect forward secrecy	Ідеальна передня секретність

ЗМІСТ

Вступ…….. 8

1 Літературний огляд та аналіз предметної області…… 13

1.1 Загальна характеристика VPN……. 13

1.1.1 Класифікація VPN……. 16

1.2 Огляд існуючих протоколів безпеки VPN та технології, на яких ґрунтується їх робота…… 25

1.3 Огляд сучасних підходів до налаштування VPN для віддаленого підключення до корпоративної мережі……. 35

Висновки до розділу 1…….. 37

2 Обґрунтування вибору технології та мережевого обладнання для побудови VPN тунелю……. 38

2.1 Синтез структурної схеми VPN тунелю та вибір елементної бази…… 38

2.2 Особливості налаштування SAML серверу ……. 40

2.3 Принципи підвищення захищеності з’єднання…… 45

Висновки до розділу 2…….. 50

3 Методи надійного шифрування мереж ……. 52

3.1 Алгоритми шифрування VPN……. 52

3.2 Шифрування VPN на основі SSL……. 61

Висновки до розділу 3…….. 63

4 Дослідження реалізації віддаленого підключення користувачів з використання технології SAML……... 64

4.1 Формулювання проблеми та постановка завдання на дослідження…….. 64

4.2 Реалізація двоетапної аутентифікації з використанням токену…….. 64

4.3 Налаштування VPN на базі IPSec…….. 66

4.4 Налаштування VPN на базі SSL……. 69

4.5 Порівняльний аналіз на базі двох протоколів безпеки…….. 72

Висновки до розділу 4…… 74

Висновки…… 75

Перелік джерел посилання……. 77

Додаток А Елементи програмного коду, налаштування обладнання…….. 81

Додаток Б Матеріали апробації наукових результатів отриманих у магістерській роботі…….. 85

Додаток В Презентаційні матеріали за результатами виконання дипломної роботи……... 93

ВСТУП

Актуальність теми

Впродовж останніх років підприємства стрімко зростають та стають все більш розподіленими. Пандемія стала основною рушійною силою, після чого додалось повномасштабне вторгнення країни-агресора, надихнувши багато організацій прийняти політику віддаленої роботи, яка може зберігатися й надалі. Тому працівникам потрібен безпечний віддалений доступ до систем і ресурсів компанії через надійні мережі. Компанії також зазвичай мають супутникові офіси та хмарну інфраструктуру, в результаті чого виникає потреба в безпечному з'єднанні цих територіально розподілених мереж [1-4].

Безпека мережі асоціюється з великою корпоративною мережею, до якої належать тисячі комп'ютерів. Однак навіть кілька комп'ютерів, підключених до домашнього роутера, також вважаються мережею. Створення безпечного домашнього середовища не менш важливе, оскільки це доступ до особистих даних.

Проблема в тому, що всі члени команди в офісі використовують внутрішню мережу. Це забезпечує їх ресурсами, а компанію – безпекою. Віддалені працівники не можуть увійти в систему, тому й виникає потреба у віддаленому доступі з використанням VPN.

Віртуальні приватні мережі є поширеним вибором для задоволення цих потреб. VPN із віддаленим доступом створює зашифрований тунель між комп'ютером користувача та кінцевою точкою VPN, тоді як VPN типу «мережа-мережа» створює зашифрований тунель між двома кінцевими точками VPN.

VPN віддаленого доступу означає, що віддалені співробітники можуть увійти в мережу офісу з будь-якого місця: з дому, у дорозі чи в закладі харчування, тобто де є доступ до Інтернету [5-8]. Тоді вони отримають доступ до всіх ресурсів компанії, але дані однаково залишаються захищені, навіть якщо використовує публічний Wi-Fi.

Розвиток віддаленої роботи спонукає до використання VPN, зробивши цю технологію головною мішенню для кіберзлочинців. Зловмисники вміло інфікують домашні та корпоративні мережі з метою отримання прибутку. Дані маніпуляції включають крадіжки особистих даних, наприклад, номера банківських рахунків та шифрування файлів комп'ютера з метою викупу. Тому безпека мережі так важлива для унеможливлення витоку конфіденційної інформації [9, 10]. Правильне налаштування політик безпеки захищає команду від неоднозначних веб-сайтів.

Для виконання всіх вимог було обрано незалежний сервер аутентифікації SAML з можливістю інтегрування доменних груп користувачів, ключова роль якого є забезпечення мережевої безпеки. Вона полягає в тому, що він дозволяє отримати доступ до декількох програм, використовуючи один набір облікових даних для авторизації. Він працює за допомогою обміну аутентифікаційною інформацією у певному форматі між учасниками, зокрема між системою управління доступами та веб-додатком.

Завдяки своїм численним перевагам SAML [11] є не досить широко використовуваним корпоративним рішенням в Україні. Він спрощує дії користувача, адже тепер потрібно лише один раз авторизуватися, щоб отримати доступ до кількох додатків. Це не тільки прискорює процес аутентифікації, але також означає, що потрібно пам'ятати лише один набір облікових даних для входу. У корпоративному плані SAML також значно полегшує роботу, оскільки кількість звернень до служби технічної підтримки, пов'язаних з відновленням втрачених і забутих паролів буде значно нижчою.

Крім того, SAML не тільки покращує роботу користувачам, але й забезпечує підвищений рівень безпеки. Оскільки система керування доступом зберігає всю інформацію для входу, тому на окремих серверах більше немає необхідності зберігати будь-які облікові дані у своїй базі.

Однією з переваг є, те що правильно автоматизована система надання доступу здійснює безпечну автентифікацію. В компаній з'являється можливість інвестувати час і ресурси в розробку та інтеграцію нових політик безпеки.

Наприклад, система керування доступами забезпечує комплексний захист особистих даних, що включає такі функції, як багатофакторна автентифікація, яка захищає від найбільш поширених атак на конфіденційну інформацію.

У магістерській атестаційній роботі проводиться порівняльний аналіз двох протоколів безпеки. Досліджено умови налаштування SAML серверу та реалізація додатково двофакторної аутентифікації. Дослідження проводились на реальному обладнанні сімейства FortiNet з ціллю інтеграції у державній структурі.

Дипломна магістерська робота складається з вступу, чотирьох розділів, висновків, списку використаних літературних джерел та додатків.

В **першому** розділі дипломної роботи здійснено опис віртуальної приватної мережі, розглянуто типи побудови та деяку архітектуру з'єднання обладнання. Описано протоколи безпеки та їх використання, визначено з необхідним обладнання.

В **другому** розділі магістерської роботи створено структурну схему проекту. Розглянуто технологію SAML та особливість реалізації лише з SSL VPN, що визначило спосіб налаштування мережі для віддаленого підключення. Важливість реалізації використання додаткових способів захисту VPN.

В **третьому** розділі магістерської роботи з'ясовано методи шифрування VPN. Роз'яснено що вся інформація, яка проходить через VPN тунель шифрується. Також VPN приховує фактичну IP-адресу та призначає приватну, яка генерується з сервера VPN, до якого відбулося підключення.

В **четвертому** розділі кваліфікаційної роботи представлено порівняльний аналіз на базі двох реалізованих VPN, та проведено налаштування двоетапної автентифікації з використанням мобільного токену від компанії FortiNet

Висновки містять загальні результати відповідно до проаналізованого матеріалу розділів та результати виконання завдань наведених у вступі.

Мета роботи: полягає у створені VPN тунелю для підключення віддалених користувачів до корпоративної мережі використовуючи технологію SAML з налаштування доменної аутентифікації.

Для досягнення цієї мети необхідно вирішити наступні завдання:

- провести аналіз наявних проколів VPN;
- обґрунтувати вибір технології та мережевого обладнання для побудови VPN тунелю;
- обрати середовище реалізації обраної технології;
- реалізувати VPN з сервером авторизації;
- підвищити захищеність мережі VPN.

Об’єктом дослідження: процес отримання доступу користувачам до мережі з використанням незалежного серверу аутентифікації SAML.

Предметом дослідження: метод безпечного віддаленого підключення користувачів.

Наукова новизна отриманих результатів. В роботі отримано такі наукові результати:

Вперше:

- запропонована методика побудови VPN тунелю з використанням технології SAML в державній організації з використанням двофакторної аутентифікації, яка передбачає використання мобільного токену чи брелка з періодичною генерацією унікального коду.

Дістали подальшого розвитку:

- методика підвищення захисту каналу VPN з можливістю реалізації багатофакторної аутентифікації по типу сканування відбитків пальців чи розпізнавання обличчя;
- методика забезпечення сприятливих умов перенесення інфраструктури в хмарні середовища по типу Azure.

Практична цінність отриманих результатів.

Досліджено аспекти практичного вибору обладнання та конструкцію мережі VPN. З’ясовані практичні особливості налаштування протоколів безпеки та їх вразливості чи несумісності з різними провайдерами.

Розглянуто налаштування способів підсилення захисту мережевого з’єднання для унеможливлення стороннього входу в LAN.

Публікації. Основні положення та основні результати магістерської дипломної роботи апробовано та відображено у статті в фаховому журналі «Вимірювальна та обчислювальна техніка в технологічних процесах» №4, 2022 рік.

1 ЛІТЕРАТУРНИЙ ОГЛЯД ТА АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Загальна характеристика VPN

VPN працює шляхом маршрутизації підключення до Інтернету пристрою через вибраний приватний сервер VPN, а не через провайдера Інтернету так, що коли дані передаються в Інтернет, вони надходять з VPN, а не з комп'ютера. VPN діє як посередник, коли відбувається підключення до Інтернету, тим самим приховуючи IP-адресу – рядок номерів, які провайдер призначає підключеному пристрою, таким чином захищаючи особу. Крім того, якщо дані якимось чином буде перехоплено, вони будуть нечитабельними, доки не досягнуть місця призначення.

VPN створює приватний «тунель» від пристрою до Інтернету та приховує важливі дані за допомогою так званого шифрування. Шифрування – це термін, який використовується для опису того, як дані зберігаються конфіденційними під час використання VPN.

Шифрування приховує інформацію таким чином, що її неможливо прочитати без надійного пароля, відомого як ключ. Цей ключ по суті спотворює код, у який перетворились дані. Тільки комп'ютер і сервер VPN знають цей ключ. Процес декодування даних відомий як дешифрування, тобто процес повторного читання зашифрованої інформації за допомогою застосування ключа.

Як повсякденний приклад є введення даних кредитної картки на торгівельному веб-сайті, при здійсненні будь-якої оплати в Інтернеті, в результаті ця інформація шифрується та стає нечитабельною, доки не досягне кінцевого пункту призначення.

Різні служби VPN використовують відповідні процеси шифрування, послідовність процесу шифрування VPN виглядає наступним чином:

При підключенні до VPN будується захищений тунель, де дані кодуються. Це означає, що під час переміщення даних між комп'ютером і сервером VPN інформація перетворюються на нечитабельний код.

В результаті чого пристрій перебуває в тій самій локальній мережі, що й використаний VPN. Таким чином IP-адреса пристрою який підключається, отримає адресу з пулу налаштованого на VPN сервері провайдера. (рисунок 1.1)

Ефективність шифрування даних залежить від протоколів та механізму шифрування обраного провайдера VPN. Ступінь впливу на VPN залежатиме від програмного забезпечення.

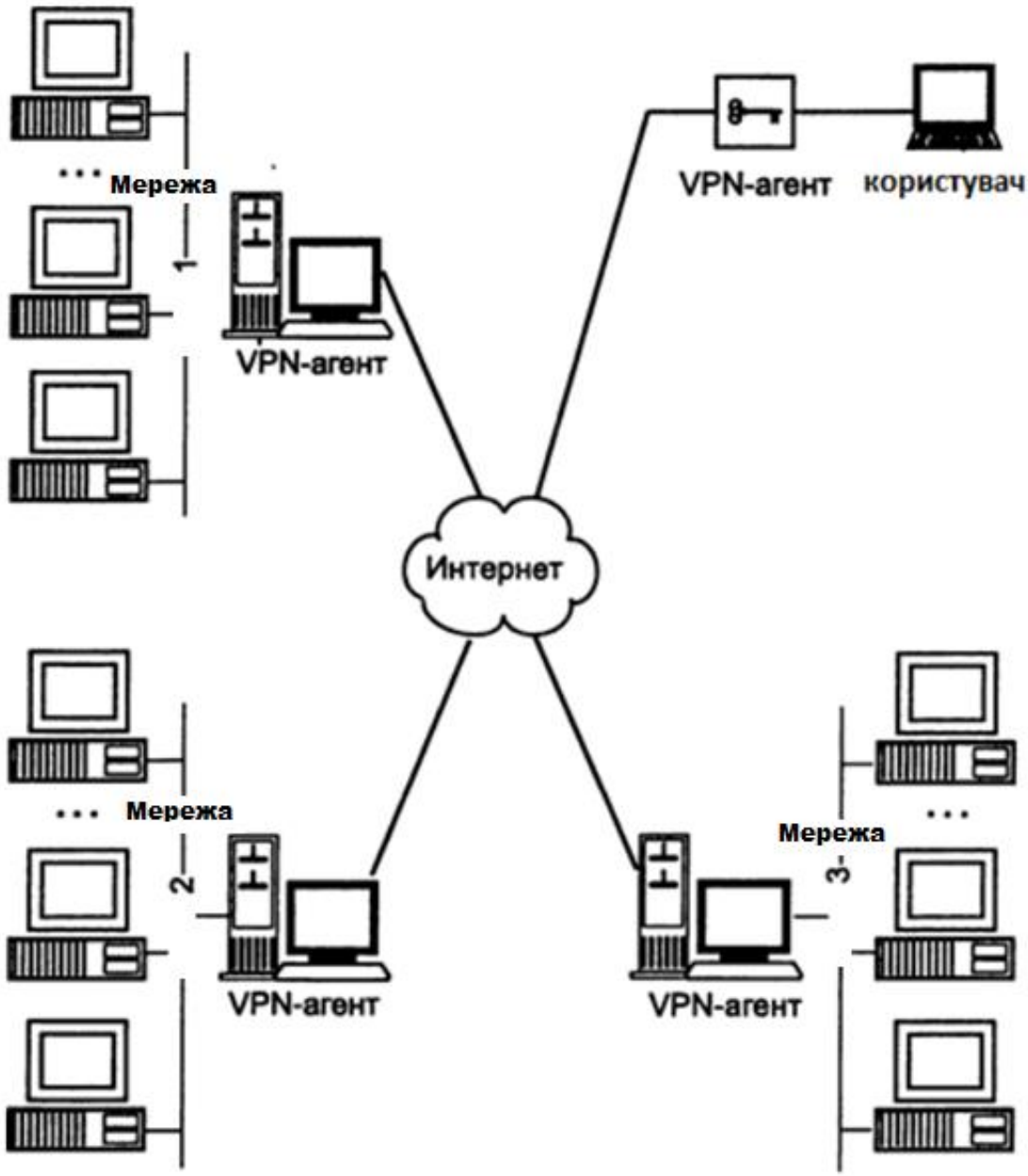


Рисунок 1.1 – Віртуальна приватна мережа

Більшість VPN працюють безпосередньо з налаштуваннями операційної системи, до прикладу Windows, MacOS, iOS або Android, щоб при використанні браузера для введення банківської карти чи інших особистих даних інформація була захищена [12-14].

Автономні служби VPN

Це мережа VPN, яка найчастіше використовується будинками та малими підприємствами. Такий вид використовує програму, яка створює зашифроване підключення до приватної мережі, яке слугує для підключення до Інтернету в цілому.

Розширення браузера

Деякі VPN працюють як розширення у браузері. Існує безліч додатків, які можна встановити в такі браузери, як Google Chrome або Firefox тощо. Недоліком цього є те, що дані будуть захищені лише тоді, коли використовується саме браузер з встановленим розширенням. Крім того, VPN налаштований у браузері, як правило, більш вразливий, в результаті чого може статися витік IP-адреси [15-17].

Маршрутизатор VPN

Ще один спосіб реалізації VPN – через маршрутизатор із підтримкою VPN. Досить зручно при використанні кількох пристроїв одразу, для яких є потреба в захищеному з'єднанні, оскільки це захистить кожен пристрій, підключений до маршрутизатора, заощаджуючи час та необхідність у встановлені VPN окремо. Крім того, потрібно буде лише один раз здійснити підключення до маршрутизатора, натомість він завжди буде підключений до VPN.

Варто використовувати маршрутизатор, який розроблено одразу підтримкою VPN, без необхідності виконувати будь-які додаткові технічні дії, окрім введення даних про VPN. Такі маршрутизатори зазвичай дорожчі за звичайні [18-20].

Корпоративний VPN

Організації часто використовують VPN віддаленого доступу для співробітників, які працюють віддалено. Завдяки такому налаштуванню співробітники можуть безпечно отримати доступ до приватної внутрішньої мережі компанії, часто за допомогою пароля та програми. Це індивідуальне рішення, яке потребує персоналізованої розробки та великих IT-ресурсів.

1.1.1 Класифікація VPN

Служби віртуальної приватної мережі поділяються на чотири основні типи:

- персональні VPN;
- VPN віддаленого доступу;
- мобільні VPN;
- VPN типу "мережа-мережа".

Персональні VPN використовуються для створення безпечних і приватних підключень до мережі Інтернет, а також для обходу брандмауерів і географічних обмежень Інтернету.

Для порівняння, підприємства використовують VPN віддаленого доступу , який дозволяє співробітникам отримувати доступ до приватної мережі компанії під час подорожей або роботи з дому. Якщо у працівника немає постійного або стабільного підключення до Інтернету, замість нього можна використовувати мобільну VPN .

Коли є кілька компаній, які намагаються підключитися до однієї приватної мережі (а не лише один співробітник), тоді компаніям потрібно буде використовувати мережу VPN типу «мережа-мережа».

VPN віддаленого доступу дозволяє використовувати Інтернет для підключення до приватної мережі, наприклад офісної мережі компанії.

Таблиця 1.1 – Характеристика видів VPN

	VPN віддаленого доступу	Персональний VPN	Мобільний VPN	Мережа-Мережа VPN
Підключення	Користувач підключається до приватної мережі.	Користувач підключається до Інтернету через сторонній сервер.	Користувач підключається до приватної мережі.	Мережа підключається до іншої мережі.
Програмне забезпечення	Зазвичай користувачам потрібно встановити програмне забезпечення на свій пристрій або налаштувати операційну систему.	Користувачі встановлюють програмне забезпечення служби VPN на свій пристрій.	Зазвичай користувачам потрібно встановити програмне забезпечення на свій пристрій або налаштувати операційну систему.	Користувачам не потрібно запускати додаткове програмне забезпечення.
Найкраще використовувати для:	Підключення до мережі вашої компанії або будь-якої іншої приватної мережі з дому чи іншого віддаленого місця.	Захисту вашої конфіденційності та обхід географічних обмежень в Інтернеті.	Досягнення постійного підключення до приватної мережі під час використання нестабільного підключення до Інтернету.	Об’єднання двох або більше мереж для створення однієї об’єднаної мережі.

Інтернет є ненадійною ланкою в спілкуванні. Шифрування VPN використовується для збереження конфіденційності та безпеки даних під час їх переміщення до приватної мережі та з неї.

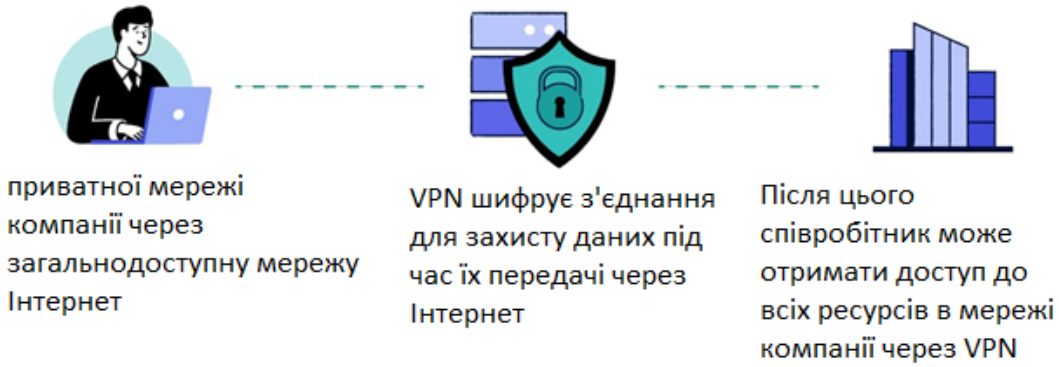


Рисунок 1.2 – Приклад підключення за допомогою віддаленого доступу

Існують різні способи використання VPN віддаленого доступу, наприклад:

Люди, котрі часто змінюють своє місце проживання, можуть використовувати VPN віддаленого доступу для підключення до мережі своєї компанії через Wi-Fi у готелі чи будь-якому громадському місці. Вони можуть отримати доступ до тих самих файлів і програмного забезпечення, які мали б в офісі. VPN також захищає дані від будь-кого, хто стежить за загальнодоступним Wi-Fi.

Хтось, хто працює з дому, може використовувати VPN віддаленого доступу для підключення до мережі компанії з дому. Комп’ютер працює так, ніби він підключений до мережі компанії в офісі, а дані захищені, коли вони проходять через загальнодоступний Інтернет [21-24].

Щоб використовувати VPN віддаленого доступу на своєму пристрої, зазвичай потрібно встановити клієнтське програмне забезпечення або налаштувати операційну систему пристрою для підключення до VPN. На кінці мережі також має бути сервер VPN. Клієнтських пристроїв може бути багато, оскільки багато різних користувачів можуть підключатися до сервера.

Спочатку сервер VPN перевіряє, чи дозволено користувачеві доступ до мережі при введенні пароля або використанні біометричних даних, таких як відбиток пальця для ідентифікації. У деяких рішеннях сертифікати безпеки можна використовувати для автоматичної автентифікації користувача у фоновому режимі, що забезпечує швидше з’єднання. Це особливо корисно, коли

користувачеві потрібно підключитися до кількох серверів VPN – наприклад, для доступу до різних мереж.

Після аутентифікації користувача клієнт і сервер встановлюють між собою зашифрований тунель. Це оболонка шифрування, яка захищає трафік через Інтернет. Існує багато різних протоколів VPN, які можна використовувати для налаштування тунелю шифрування: IPsec і SSL.

Приклади VPN віддаленого доступу для бізнесу включають:

- Сервер доступу через OpenVPN , який є безкоштовним для двох одночасних підключень VPN.
- Cisco AnyConnect , який інтегрується з корпоративними рішеннями безпеки Cisco.

Персональні послуги VPN

Персональна служба VPN з’єднує пристрій із сервером VPN, який потім діє як посередник між девайсом і онлайн-службами, до яких потрібно отримати доступ.

Персональний VPN, який іноді також називають «споживчим» або «комерційним» VPN, шифрує з’єднання, приховує особу в Інтернеті та дозволяє підробити географічне розташування.

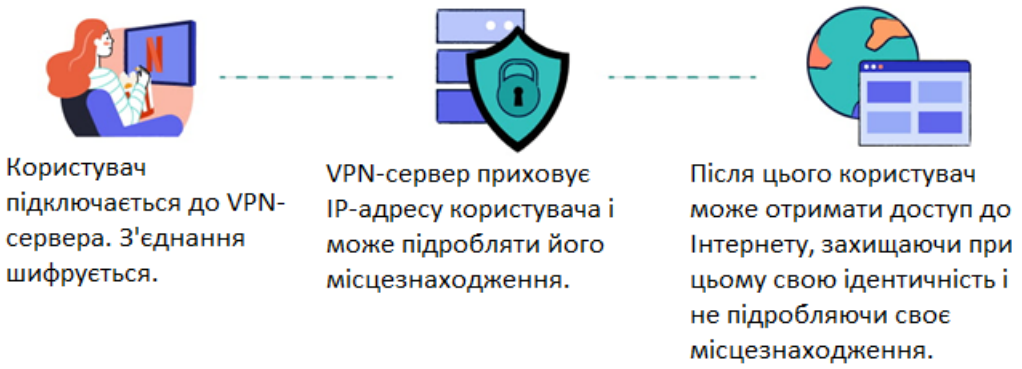


Рисунок 1.3 – Приклад підключення за допомогою персонального VPN

Персональна служба VPN відрізняється від VPN віддаленого доступу тим, що вона не дає доступу до приватної мережі.

Натомість персональний VPN за допомогою зашифрованого з'єднання надає доступ до загальнодоступної мережі Інтернет.

Є багато причин використовувати особисту VPN. Деякі з найпопулярніших:

Потокова трансляція фільмів і серіалів чи прослуховування аудіотреків недоступна у вашому географічному розташуванні. Наприклад, ви можете підключитися до сервера VPN у США та отримати доступ до американської Netflix, яка є однією з найбільших бібліотек контенту Netflix, якщо є така потреба.

VPN надає доступ до вмісту, заблокованого брандмауерами провайдера, і приховує веб-трафік від державних систем спостереження [25-29].

Приховування IP-адреси пристрою, щоб захистити себе від цілеспрямованих атак. Геймери все частіше використовують короткі, але інтенсивні DDoS-атаки, щоб заблокувати конкурентів і забезпечити нечесну перемогу, що унеможливлюється з використанням VPN.

Захист конфіденційності в Інтернеті, оскільки провайдери іноді переривають або сповільнюють з'єднання, помічаючи, що використовується понаднормовий трафік. Персональні програми VPN доступні на всіх типах пристроїв, включаючи смартфони.

Персональні VPN зазвичай мають великі серверні мережі на вибір. Якщо є потреба захисту конфіденційності, потрібно підключитися до локального сервера для отримання найбільшої швидкості.

Під час підключення до VPN весь інтернет-трафік проходить через сервер провайдера. Безпосередньо з'єднання зашифровано, тому IP-адреса прихована, в результаті чого отримати доступ до географічно обмеженого вмісту іншої країни не складе клопоту.

Перелік персональних VPN з найвищим рейтингом:

- ExpressVPN
- NordVPN
- Surfshark

- IPVanish

Мобільні VPN

При використанні VPN з віддаленим доступом передбачається, що користувач матиме стабільне підключення до Інтернет мережі, тому в разі розірванні з'єднання побудований тунель втрачається.

Мобільний VPN доцільніше використовувати ніж VPN віддаленого доступу, якщо є прогнозованість нестабільного з'єднання в мережі протягом усього сеансу [30-32].

З мобільним VPN з'єднанням зберігається, навіть якщо користувач перемикає Wi-Fi або стільникову мережу, втрачає з'єднання або вимикає свій пристрій на деякий час.

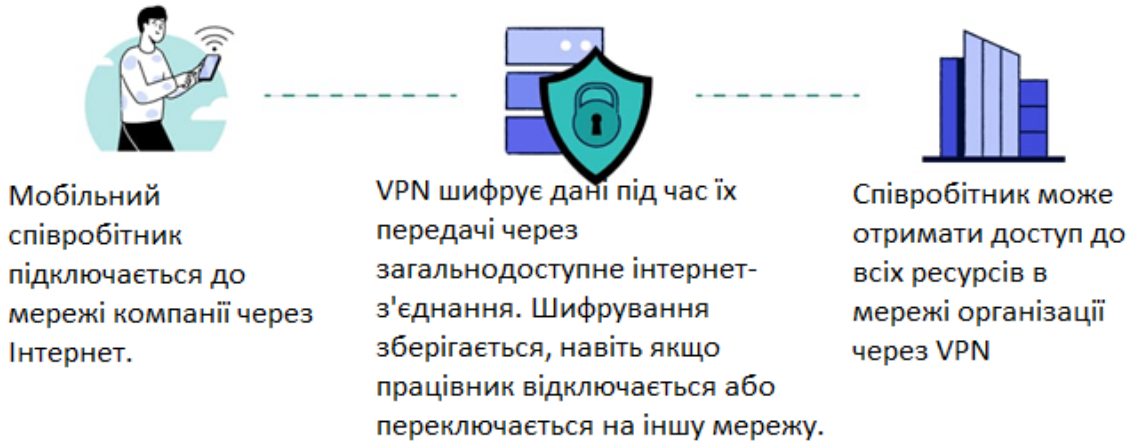


Рисунок 1.4 – Приклад підключення за допомогою мобільного VPN

Мобільні VPN, як правило, використовуються для забезпечення стабільної доступності для працівників, які виконують роботу за допомогою мобільних пристроїв, Тому є необхідність у VPN, який допускає зміну підключення.

До прикладу, військовослужбовці, котрі несуть службу на блок-постах, встановлених по Україні, використовують планшети та мобільний VPN, щоб мати доступ до різних баз даних, для перевірки осіб чи транспортних засобів, які викликають підозру.

Спеціалісти, які працюють вдома з поганим покриттям, що в теперішній час досить поширено, можуть використовувати мобільний VPN, щоб підтримувати доступ до офісу впродовж дня, навіть якщо з'єднання перериватиметься.

Параметри автентифікації можуть включати паролі, фізичні маркери, такі як смарт-карти, біометричні пристрої, сканери відбитків пальців, а також системи розпізнавання обличчя. У деяких випадках використовуються сертифікати, щоб автентифікація відбувалася автоматично у фоновому режимі.

Мобільний термінал має можливість перемикатися між мережами, такими як стільникова або Wi-Fi. Така переміна може змінити фізичну IP-адресу, але логічна IP-адреса, яку використовує VPN-тунель, залишається незмінною. Віртуальне мережеве з'єднання стійке до змін, тому користувач може безперебійно працювати, доки у нього є з'єднання.

Якщо пристрій вимкнено для збереження заряду батареї, VPN-з'єднання буде все ще доступне при ввімкненні пристрою знову.

Приклади мобільних VPN включають:

- Bittium SafeMove Mobile VPN: автоматично підключає користувачів і забезпечує роумінг.
- Програмне забезпечення Radio IP: дозволяє використовувати мобільні VPN для всіх технологій бездротової мережі.

VPN типу "мережа-мережа".

У той час як VPN віддаленого доступу розроблено, щоб дозволити окремим користувачам підключатися до мережі та використовувати її ресурси, VPN типу «мережа-мережа» об'єднує дві мережі.

Наприклад, якби компанія мала два офіси на східному та західному напрямках, для об'єднання їх у єдину мережу доцільно було б використовувати такий вид VPN.

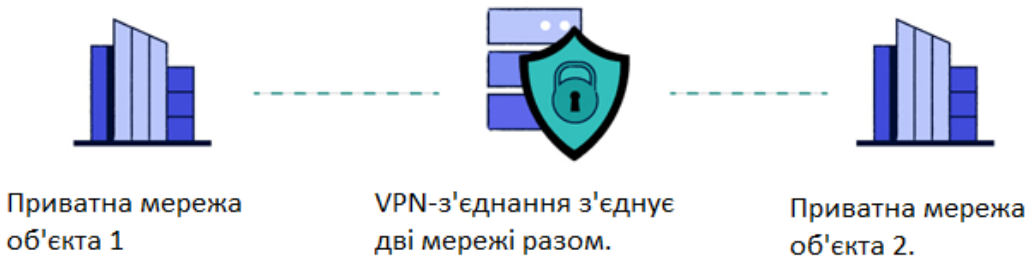


Рисунок 1.5 – Приклад з’єднання по типу «мережа-мережа»

Різні технології можуть бути використані для реалізації VPN типу «мережа-мережа». До них належать IPsec, DMVPN і L3VPN.

Існують дві різні форми VPN типу «мережа-мережа»:

VPN на основі інтрамережі: за умови якщо підключені мережі належать одній компанії, таке об’єднання VPN визначено вважати на основі інтрамережі. Це дозволяє компанії створити єдину глобальну мережу, яка охоплює два чи більше офісів. Користувачі компанії можуть отримати доступ до ресурсів з іншої LAN так, ніби вони підключені фізично.

VPN на основі зовнішньої мережі: якщо підключені мережі належать різним компаніям, об’єднана VPN називається VPN на основі екстрамережі. Такий вид VPN використовується, наприклад, коли компанія хоче підключитися до мережі провайдера [33, 34].

Є три основні способи реалізації VPN типу "мережа-мережа":

- Використання тунелю IPsec;
- Використання динамічної багатоточкової VPN;
- Використання VPN 3-го рівня.

Тунель IPsec можна використовувати для об’єднання мереж, приблизно так само, як він з’єднує окремі підключення з приватною мережею в межах VPN віддаленого доступу.

Однак у цьому випадку VPN реалізується маршрутизаторами на двох або більше мережах, які підключаються один до одного. З цієї причини його іноді також називають VPN маршрутизатор-маршрутизатор .

У той час як VPN віддаленого доступу створює тунель для підключення одного пристрою до приватної мережі, у випадку VPN типу "мережа-мережа" тунель IPsec шифрує трафік між підключеними мережами. Це може мати дві форми:

- Тунель IPsec на основі маршруту пропускає будь-який трафік між мережами.
- Тунель IPsec на основі політики безпеки встановлює правила, які визначають дозволений трафік для проходження, та мережі можуть спілкуватися з будь-якими іншими. Тунелі IPsec можна побудувати за допомогою брандмауерів і мережевих маршрутизаторів.

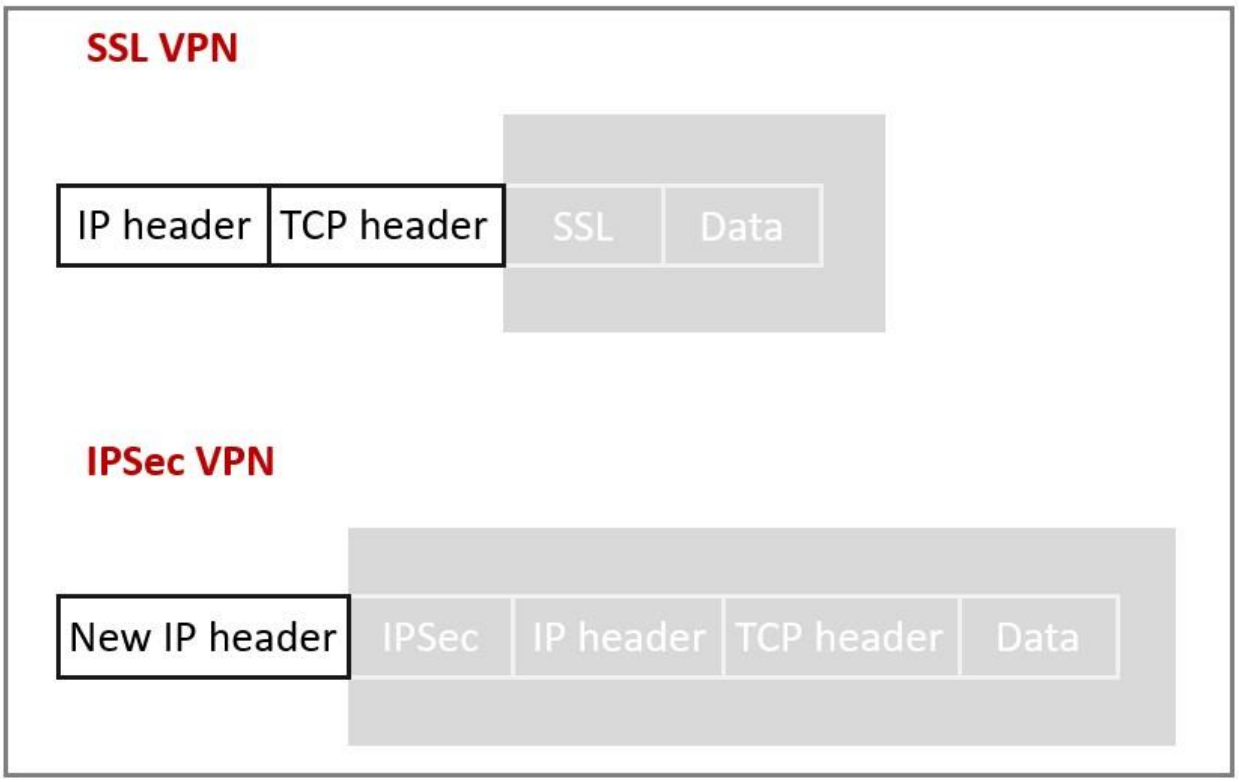


Рисунок 1.6 – Склад пакетів протоколів SSL та IPsec

Dynamic MultiPoint VPN

Проблема з тунелями IPsec полягає в тому, що IPsec з’єднує дві точки одна з одною. Замість цього рішення пропонується технологія Cisco Dynamic MultiPoint VPN (DMVPN). Вона дозволяє об’єднувати мережі з використанням маршрутизатора-концентратора DMVPN за допомогою динамічних IP-адрес.

VPN 3 рівня на основі MPLS

Обидва підходи IPsec і DMVPN працюють поверх Інтернету, що дає малу гарантію продуктивності.

Навпаки, багатопротокольні мережі з комутацією міток MPLS 3-го рівня можуть забезпечити гарантовану якість обслуговування з глобальним підключенням. Це пояснюється тим, що MPLS — це спосіб маршрутизації мережевих пакетів через будь-яке транспортне середовище (наприклад, оптоволоконне або супутник) з використанням будь-якого протоколу.

Тому провайдери можуть використовувати MPLS для створення VPN 3-го рівня. Відповідно до моделі OSI такий VPN створюється на мережевому рівні. Хоча деякі великі компанії можуть створювати власні MPLS VPN, зазвичай їх створюють провайдери зв’язку.

Мережеві провайдери можуть створити окрему віртуальну мережу для кожного клієнта, яку передає у користування вже в результаті глобальної мережі. Віртуальні мережі ізольовані одна від одної, навіть якщо вони можуть спільно використовувати деякі фізичні мережеві ресурси.

За допомогою MPLS VPN можна визначити пріоритетність певних типів трафіку, наприклад, голосового трафіку, щоб забезпечити кращу якість обслуговування. Маршрут проходження мережевого трафіку важливо контролювати, щоб забезпечити послідовну та добре оптимізовану продуктивність.

Послуги приватної глобальної мережі є економічно не вигідними , тому компанії мають тенденцію відмовлятися від MPLS на користь дешевших мереж VPN на базі Інтернету. Основні винятки становлять ситуації, коли будь-яка затримка критична, наприклад, у програмах, які виявляють несправності та збої в електромережі.

1.2 Огляд існуючих протоколів безпеки VPN та технології на яких ґрунтується їх робота

Для реалізації цих сценаріїв існують різні види протоколів VPN — для зв'язку, для шифрування трафіку та інші. І вже на підставі відповідного

протоколу можливо проектувати своє рішення. Три найвідоміші протоколи, що широко використовуються — OpenVPN, IPSec SSL, а порівняно недавно з'явився WireGuard, що викликав деякі розбіжності. Також є інші альтернативи, які вже застарілі, але цілком здатні вирішувати певні завдання.

Перевага того чи іншого протоколу VPN залежить від низки факторів та умов використання:

Пристрої – різні пристрої підтримують різні протоколи.

Мережа — якщо певні послуги не доступні у вашій локації, деякі протоколи можуть не підійти. Наприклад, є VPN Providers, які працюють у Китаї, тоді як більшість існуючих провайдерів заблоковано.

Продуктивність — деякі протоколи мають більшу продуктивність, особливо на мобільних пристроях. Інші — зручніші для використання у великих мережах.

Модель загроз — деякі протоколи менш безпечні за інші, тому й зловмисники можуть впливати на них по-різному.

PPTP

Point-to-Point Tunneling Protocol - один із найстаріших VPN протоколів, що використовуються досі, спочатку був розроблений компанією Microsoft.

PPTP використовує два з'єднання – одне для управління, інше для інкапсуляції даних. Перше працює з використанням TCP, у якому порт сервера 1723. Друге працює з допомогою протоколу GRE, який є транспортним протоколом (тобто заміною TCP/UDP). Заголовок GRE пакету виглядає наступним чином:

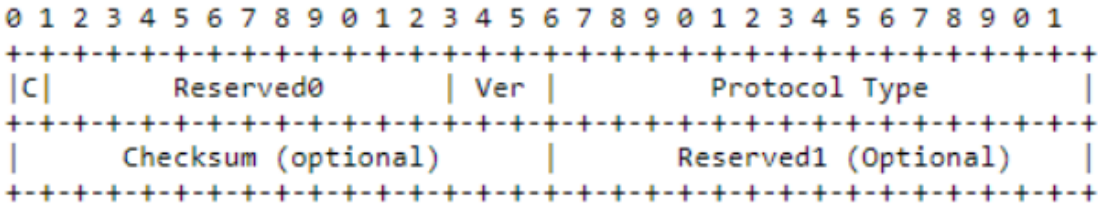


Рисунок 1.7 – Заголовок пакету GRE

Цей факт заважає клієнтам, що перебувають за NAT, встановити підключення з сервером, оскільки для них встановити підключення точка-точка неможливо по замовчуванню. Однак, в протоколі GRE, що використовує PPTP (а саме enhanced GRE), є заголовок Call ID, маршрутизатори можуть ідентифікувати та зіставити GRE трафік, що йде від клієнта локальної мережі до зовнішнього сервера і навпаки. Це дозволяє клієнтам за NAT встановити підключення точка-точка і користуватися протоколом GRE. Ця технологія називається VPN PassTrough. Вона підтримується великою кількістю сучасного клієнтського мережного обладнання.

PPTP підтримується на всіх версіях Windows, та у більшості існуючих операційних систем. Незважаючи на відносно високу швидкість, PPTP не надто надійний: після обриву з'єднання він не відновлюється так само швидко, як, наприклад, OpenVPN.

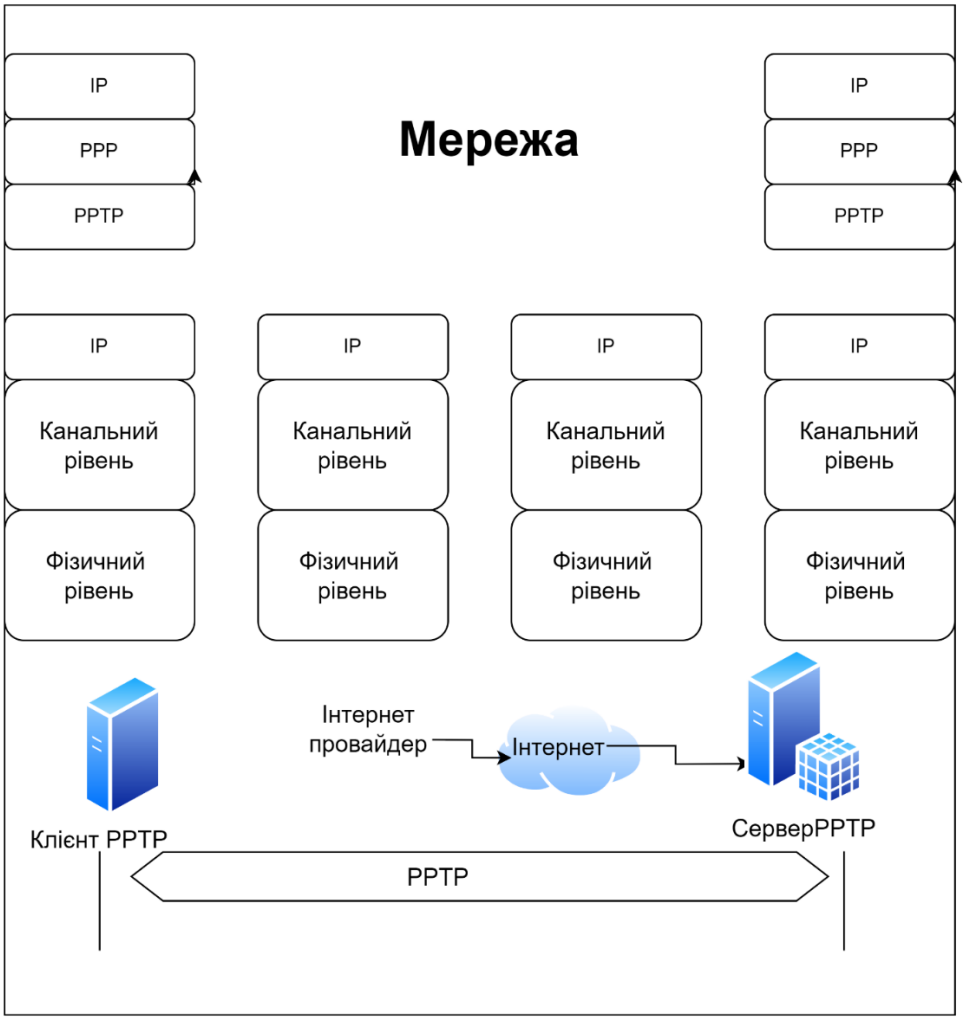


Рисунок 1.8 – Клієнт-серверна архітектура PPTP

В даний час PPTP суттєво застарів і Microsoft радить користуватися іншими VPN рішеннями, з урахуванням того, що важлива безпека та конфіденційність.

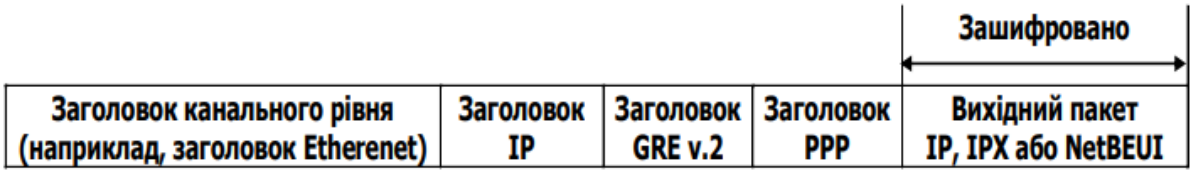


Рисунок 1.9 – Структура пакета PPTP

Звичайно, якщо просто використовувати VPN для розблокування контенту, PPTP вистачить, однак, варто обирати більш безпечні варіанти.

SSTP

Secure Socket Tunneling Protocol – пропрієтарний продукт від Microsoft. Як і PPTP, SSTP не дуже широко використовується в індустрії VPN, але, на відміну від PPTP, він не діагностує серйозні проблеми з безпекою.

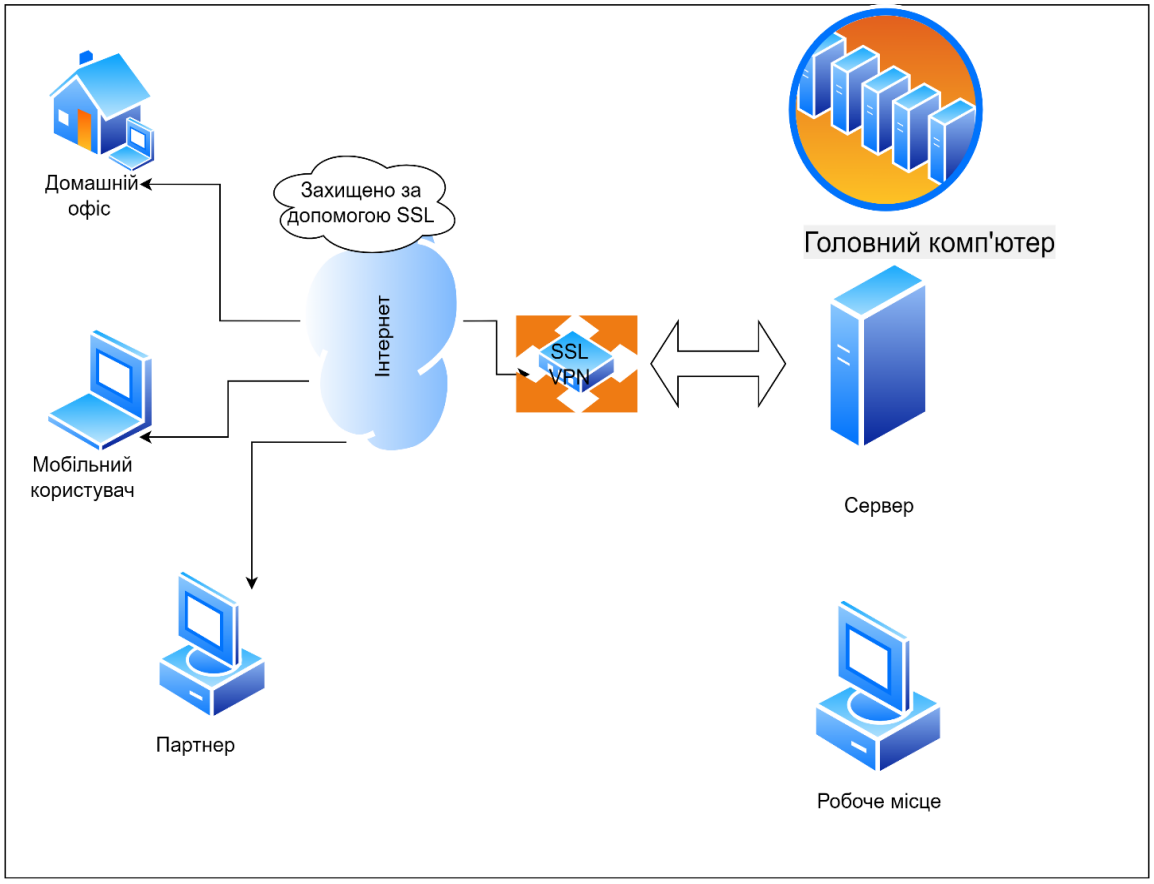


Рисунок 1.10 – Підключення з використанням SSL

SSTP відправляє трафік SSL через TCP-порт 443. Це надає переваги для використання в обмежених мережевих ситуаціях, наприклад, якщо потрібен VPN для Китаю. Незважаючи на те, що SSTP також доступний і на Linux, переважно він все одно використовується Windows-системами.

SSL може забезпечити захист протоколів прикладного рівня, наприклад, таких як POP3 або FTP. Для роботи SSL потрібно, щоб на сервері був SSL-сертифікат.

Безпечне з'єднання між клієнтом і сервером під час використання SSL виконує дві функції - аутентифікацію і захист даних.

SSL складається з двох рівнів. На нижніх рівнях (4-5) багаторівневого транспортного протоколу (наприклад, TCP) він є протоколом запису і використовується для інкапсуляції (тобто формування пакета) різних протоколів. Для кожного інкапсульованого протоколу він забезпечує умови, за яких сервер і клієнт можуть підтверджувати один одному свою автентичність, виконувати захист переданих даних і обмінюватися ключами, перш ніж протокол прикладної програми почне передавати й отримувати дані.

Переваги протоколу SSL:

- Простота використання;
- Немає необхідності в додатковому програмному забезпеченні;
- Безпечний віддалений доступ.

З точки зору продуктивності SSTP працює швидко, стабільно та безпечно.

IPsec

Internet Protocol Security – це набір протоколів для забезпечення захисту даних, що передаються IP-мережею. На відміну від SSL, який працює на прикладному рівні, IPsec працює на мережному рівні і може поєднуватись з багатьма операційними системами, що дозволяє використовувати його без сторонніх програм.

Рисунок 1.11 – Розміщення протоколу IPsec в модулі OSI

IPsec став дуже популярним протоколом для використання в парі з L2TP або IKEv2.

IPsec шифрує весь IP-пакет, використовуючи:

- Authentication Header, який ставить цифровий підпис на кожному пакеті;
- Encapsulating Security Protocol, який забезпечує конфіденційність, цілісність та аутентифікацію пакета під час передачі.

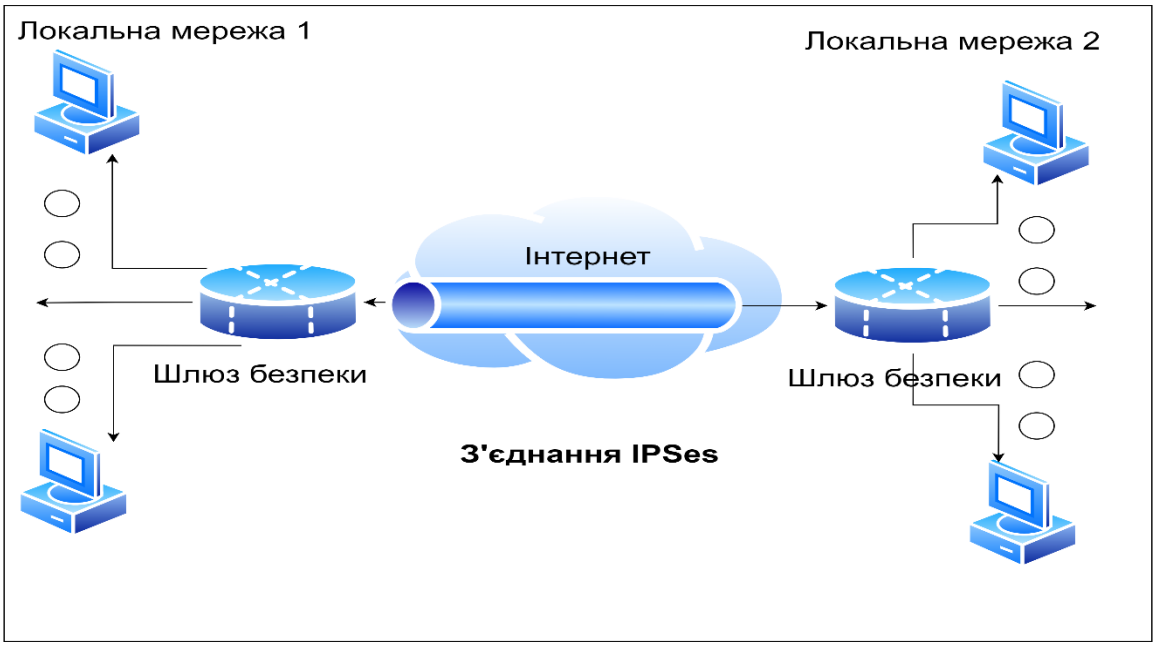


Рисунок 1.12 – Приклад з’єднання на базі IPsec

L2TP/IPsec

Layer 2 Tunneling Protocol був вперше запропонований в 1999 році як оновлення протоколів L2F (Cisco) і PPTP (Microsoft). Оскільки L2TP сам по собі не забезпечує шифрування чи автентифікацію, часто з ним використовується IPsec. L2TP у парі з IPsec підтримується багатьма операційними системами.

L2TP/IPsec вважається безпечним і не має серйозних виявлених проблем. L2TP/IPsec може використовувати шифрування 3DES або AES, хоча з огляду на те, що 3DES в даний час вважається слабким шифром, він використовується рідко. У протоколі L2TP іноді виникають проблеми через стандартне використання UDP-порту 500, який, як відомо, блокується деякими брандмауерами.

Протокол L2TP/IPsec дозволяє забезпечити високу надійність передачі даних, простий у налаштуванні та підтримується всіма сучасними операційними системами. Однак L2TP/IPsec інкапсулює дані при передачі двічі, що робить його менш ефективним і повільнішим, ніж інші VPN-протоколи.

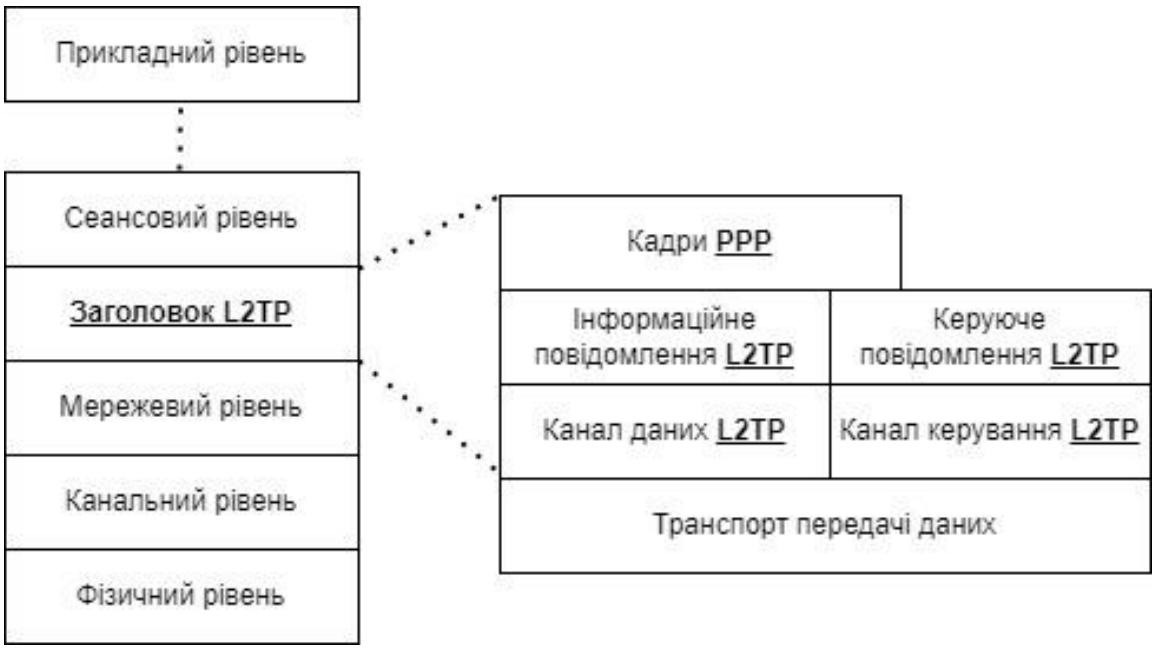


Рисунок 1.13 – Складові протоколу L2TP

IKEv2/IPsec

Internet Key Exchange version 2 є протоколом IPsec, що використовується для виконання взаємної аутентифікації, створення та обслуговування Security

Associations. IKEv2 був розроблений Microsoft спільно з Cisco, існують реалізації протоколу з відкритим вихідним кодом (наприклад, OpenIKEv2, Openswan та strongSwan).

Завдяки підтримці Mobility and Multi-homing Protocol IKEv2 є дуже стійкий до зміни мереж. Це робить IKEv2 відмінним вибором для користувачів смартфонів, які регулярно перемикаються між домашнім Wi-Fi та мобільним з'єднанням або переміщуються між точками доступу.

IKEv2/IPsec може використовувати низку різних криптографічних алгоритмів, включаючи AES, Blowfish та Camellia, у тому числі з 256-бітними ключами.

У багатьох випадках IKEv2 швидше за OpenVPN, оскільки він менш ресурсномісткий. З точки зору продуктивності IKEv2 може бути найкращим варіантом для мобільних користувачів, оскільки він добре встановлює з'єднання. IKEv2 нативно підтримується на Windows, Mac OS, iOS, а також на деяких Android-пристроях.

OpenVPN

OpenVPN – це універсальний протокол VPN з відкритим вихідним кодом, розроблений компанією OpenVPN Technologies. На сьогоднішній день це, мабуть, найпопулярніший протокол VPN. Будучи відкритим стандартом, він пройшов не одну незалежну безпекову експертизу.

У більшості ситуацій, коли потрібне підключення через VPN, швидше за все підійде OpenVPN. Він стабільний та пропонує хорошу швидкість передачі даних. OpenVPN використовує стандартні протоколи TCP та UDP, і це дозволяє йому стати альтернативою IPsec та SSL тоді, коли провайдер блокує деякі протоколи VPN.

Для роботи OpenVPN потрібне спеціальне клієнтське програмне забезпечення. Більшість VPN-сервісів створюють свої програми для роботи з OpenVPN, які можна використовувати в різних операційних системах та пристроях. Протокол може працювати на будь-якому з портів TCP та UPD і може

використовуватись на всіх основних платформах через сторонні клієнти: Windows, Mac OS, Linux, Apple iOS, Android.

WireGuard

Найновіший і незвіданий протокол VPN - WireGuard. Позиціонується розробниками як заміна IPsec, OpenVPN та SSL для більшості випадків їх використання, будучи більш безпечним, продуктивним і простим у використанні.

Всі IP-пакети, що приходять на WireGuard інтерфейс, інкапсулюються в UDP. WireGuard використовує сучасну криптографію:

- Curve25519 для обміну ключами;
- ChaCha20 для шифрування;
- Poly1305 для аутентифікації даних;
- SipHash для ключів хеш-таблиці;
- BLAKE2 для хешування.

Код WireGuard виглядає набагато простіше, ніж код OpenVPN, внаслідок чого його простіше досліджувати на вразливості (4 тисяч рядків коду проти кількох сотень тисяч).

Нещодавно був представлений WireGuard 1.0.0, який відзначив собою постачання компонентів WireGuard в основному складі ядра Linux 5.6. Включений до складу ядра Linux код пройшов додатковий аудит безпеки, виконаний незалежною фірмою, який не виявив жодних проблем.

Таблиця 1.2 – Порівняльна характеристика протоків безпеки

Ознака	**PPTP**	**SSTP**	**L2TP/IPsec**	**IKEv2/IPsec**	**OpenVPN**	**WireGuard**
Компанія-розробник	Microsoft	Microsoft	L2TP — спільна розробка Cisco і Microsoft, IPsec — Інженерна робоча група Інтернету	IKEv2 — спільна розробка Cisco і Microsoft, IPsec — робоча група з розробки Інтернету	OpenVPN Technologies	Jason A. Donenfeld

Ознака	PPTP	SSTP	L2TP/IPsec	IKEv2/IPsec	OpenVPN	WireGuard
Ліцензія	Proprietary	Proprietary	Proprietary	Власний, але існує протокол реалізації з відкритим вихідним кодом	GNU GPL	GNU GPL
Розгорта-ння	Windows, MacOS, iOS, деякий час GNU/Linux. Працює з пристрою, не вимагаючи установки додаткового ПЗ	Windows. Працює з пристрою, не вимагаючи установки додаткового ПЗ	Windows, Mac OS X, Linux, iOS, Android. Багато ОС (включаючи Windows 2000/XP +, Mac OS 10.3+) мають вбудовану підтримку, немає необхідності встановлювати додаткові ПО	Windows 7+, macOS 10.11+ і більшість мобільних ОС мають вбудовану підтримку	Windows, Mac OS, GNU/Linux, Apple iOS, Android і маршрутизатори. Необхідна установка спеціалізованого ПО, що підтримує роботу з даними протоколом	Windows, Mac OS, GNU/Linux, Apple iOS, Android. Встановити сам WireGuard, а потім налаштувати по руководству
Шифрування	Використовує Microsoft Point-to-Point Encryption (MPPE), який реалізує RSA RC4 з максимум 128-розрядними сеансовими ключами	SSL (шифруються всі частини, крім TCP- та SSL-заголовків)	3DES або AES	Реалізує велику кількість криптографічних алгоритмів, включаючи AES, Blowfish, Camellia	Використовує бібліотеку OpenSSL (реалізує більшість популярних криптографічних стандартів)	Обмін ключами по 1-RTT, Curve25519 для ECDH, RFC7539 для ChaCha20 і Poly1305 для аутентифікаційного шифрування, і BLAKE2s для хешування
Порти	TCP-порт 1723	TCP-порт 443	UDP-порт 500 для первонач. обміну ключами та UDP-порт 1701 для початкової конфігурації L2TP, UDP-порт 5500 для обходу NAT	UDP-порт 500 для початкового обміну ключами, а UDP-порт 4500 для обходу NAT	Будь-який UDP- або TCP-порт	Будь-який UDP-порт

Ознака	PPTP	SSTP	L2TP/IPsec	IKEv2/IPsec	OpenVPN	WireGuard
Недоліки безпеки	Має серйозні вразливості. MSCHAP-v2 уразливий для атаки, а алгоритм RC4 піддається атаці Bit-flipping	Серйозних недоліків безпеки не було виявлено	3DES вразливий для Meet-in-the-middle та Sweet32, але AES не має відомих уразливостей. Однак є думка, що стандарт IPsec скомпрометовано.	Не вдалося знайти інформації про наявні недоліки безпеки, крім інциденту з витоком доповідей щодо IPsec	Серйозних недоліків безпеки не було виявлено	Серйозних недоліків безпеки не було виявлено

1.3 Огляд сучасних підходів до налаштування VPN для віддаленого підключення до корпоративної мережі

VPN із віддаленим доступом дозволяє пристрою безпечно з’єднуватися з приватною чи локальною мережею компанії незалежно від того, де знаходиться пристрій або локальна мережа, щоб реалізувати безпечний доступ співробітників до ресурсів усієї мережі.

Безумовно, VPN типу «мережа-мережа» забезпечує багато переваг для відносно великої компанії, однак це коштуватиме значних витрат і людських ресурсів.

MCE ASA є одним з найбільш високотехнологічним з погляду функціоналу VPN-з'єднань.

Класифікація користувацького VPN за типом тунельного методу, що надається Cisco:

- IPsec - застарілий спосіб (не потребує додаткових ліцензій);
- SSL/TLS - сучасний спосіб (потребує додаткових ліцензій).

Для з'єднання за першим способом - IPsec - використовується клієнтський додаток Cisco VPN Client. Для підключення користувач має встановити та налаштувати клієнтський застосунок самостійно.

Спосіб другий – SSL/TLS з використанням клієнтського додатка - є аналогом першому способу. У випадку для підключення використовується клієнтський додаток Anyconnect. Головна перевага використання цього способу

полягає в тому, що додаток Anyconnect може бути завантажений користувачем самостійно безпосередньо з MCE ASA. При цьому встановлення цього додатка буде виконано в автоматичному режимі. Таке рішення багато в чому спрощує адміністрування сервісу Remote Access. Мережевим інженерам досить роздати користувачам посилання, за яким можна завантажити і встановити клієнт Anyconnect і логін/пароль. Крім того, разом із клієнтом Anyconnect на користувацький пристрій завантажується профіль підключення, що описує всі необхідні налаштування. Користувачеві не потрібно налаштовувати під'єднання, як це було в разі використання Cisco VPN Client. Якщо на пристрої користувача вже встановлений клієнт Anyconnect, для підключення досить увімкнути клієнт, натиснути "Connect" і ввести логін/пароль.

При використанні підключення за допомогою браузера, користувач заходить на корпоративний портал. Даний портал налаштовується на ASA мережевим адміністратором. Залежно від типу ресурсів, що надаються для віддаленого доступу, на порталі користувач зможе знайти такі основні вкладки:

- Web Applications;
- Browse Networks;
- Application Access;
- Terminal Servers.

Fortinet так само має параметри налаштування IPsec і SSL VPN. В свою чергу SSL VPN має два режими: тунель і веб.

Вибір режиму роботи та застосування відповідних рівнів безпеки залежить від конкретного середовища та вимог.

У режимі тунелю клієнт SSL VPN шифрує весь трафік від віддаленого клієнтського комп’ютера та надсилає його на FortiGate через тунель SSL VPN через з’єднання HTTPS між користувачем і FortiGate.

Веб-режим забезпечує налаштування безклієнтського доступу до мережі за допомогою веб-браузера з вбудованим шифруванням SSL. Його легше налаштувати, ніж режим тунелю, і не вимагає встановлення

програми на кінцевій точці, але він має обмежену підтримку програм і потребує більше ресурсів на FortiGate.

IPsec VPN, як і зазначалось раніше, це стандартний протокол, який дозволяє використовувати різноманітні рішення для підключення кінцевих точок, включаючи FortiClient. Це чітко визначений протокол, який використовує певні порти, і провайдери досить часто блокують їх.

Висновки до розділу 1

В **першому** розділі дипломної роботи здійснено опис віртуальної приватної мережі, розглянуто типи побудови та деяку архітектуру з’єднання обладнання. Описано протоколи безпеки та їх використання, визначено з необхідним обладнання.

2 ОБҐРУНТУВАННЯ ВИБОРУ ТЕХНОЛОГІЇ ТА МЕРЕЖЕВОГО ОБЛАДНАННЯ ДЛЯ ПОБУДОВИ VPN ТУНЕЛЮ

2.1 Синтез структурної схеми VPN тунелю та вибір елементної бази

На сьогоднішній день, в мережі Інтернет можна зустріти безліч сайтів, на яких використовується протокол SSL для забезпечення безпеки персональних даних (наприклад, веб-сайти, що надають комерційні та банківські сервіси). Практично всі найпопулярніші браузери, поштові клієнти та інтернет-додатки підтримують роботу з протоколом SSL. Для доступу до сторінок, захищеним протоколом SSL, в URL замість звичайного префікса http, як правило, застосовується префікс https (порт 443), який вказує на те, що буде використовуватися SSL-з'єднання.

SSL VPN оптимальний для підключення віддалених користувачів до ресурсів локальної мережі офісу через Інтернет. Його зручність і є однією з причин вибору саме SSL VPN для реалізації проекту. Оскільки в організації, де розгортається проект дослідження, використовується мережеве обладнання сімейства FortiNet, тому обрано саме такий шлюз захисту та аутентифікатор.

З врахування того, що це обладнання розроблене однією компанію, передбачається високий рівень сумісності, відсутність конфліктуючих факторів та мінімальна кількість додаткових надбудов у вигляді окремих програм. FortiGate встановлює тунель із клієнтом і призначає віртуальну IP-адресу клієнту з діапазону зарезервованих адрес.

Обране середовище дослідження містить велику кількість користувачів, тому визначено інтегрувати конфігурацію користувача з наявним серверам автентифікації через FortiAuthenticator. Структурна схема зображена на рисунку 2.1.

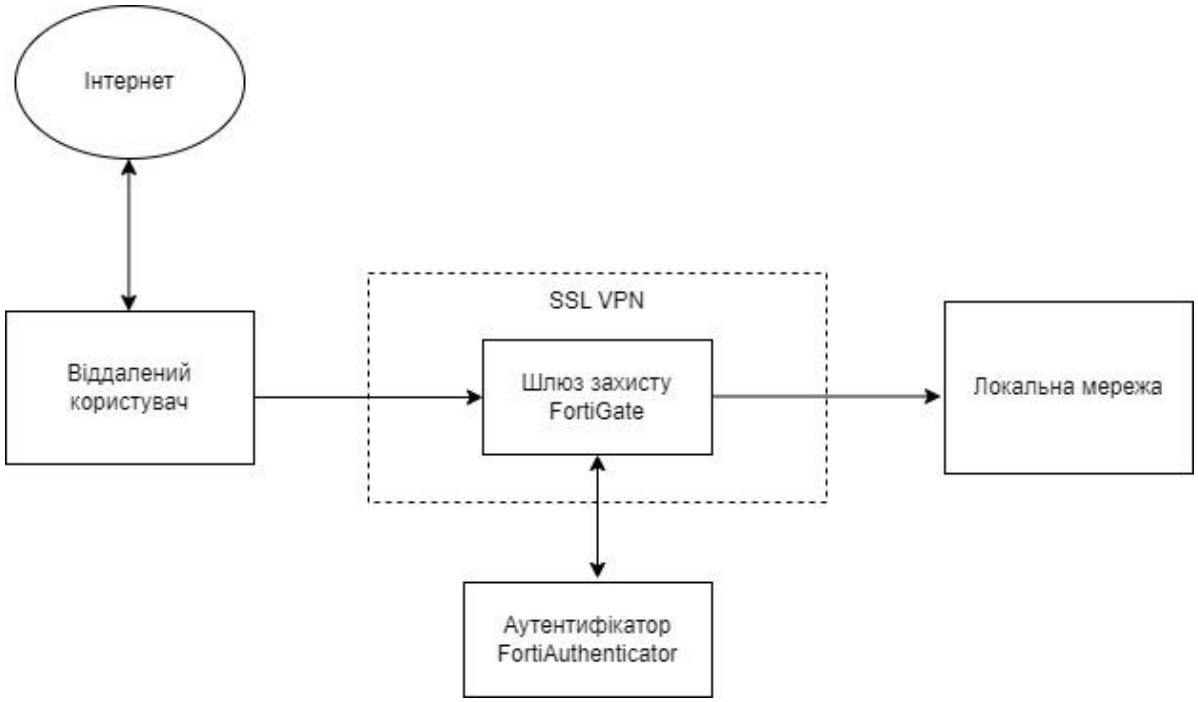


Рисунок 2.1 – Структурна схема VPN

Для безпосереднього входу додатково встановлюється лише FortiClient Він надає різноманітні можливості підключення до VPN, підтримується як технологія SSL VPN і класичний IPsec VPN. Можливість роздільного тунелювання для віддалених користувачів дозволяє отримати доступ до Інтернету без необхідності перенаправляти весь трафік через корпоративний сервер VPN. Ця функція зменшує тимчасову затримку при передачі даних через мережу, що позитивно позначається на швидкості завантаження даних для користувачів. У той же час, FortiClient включає засоби захисту, які гарантують, що дані з Інтернету не зможуть потрапити назад у VPN з'єднання та поставити під загрозу корпоративну мережу.

Інтеграція зі службою каталогів Microsoft Windows Active Directory дозволяє синхронізувати використовувану організаційну структуру компанії в консоль керування. Це дозволить спростити управління та можливість використовувати ідентичні групи до тих, що вже існують в службах каталогів Windows.

Централізована система управління агентами FortiClient дозволяє адміністраторам віддалено встановлювати, оновлювати та конфігурувати клієнтів системи, що значно спрощує початковий етап запуску агентів.

FortiClient створює віртуальні групи на основі стану безпеки кінцевих точок. Ці віртуальні групи використовується у FortiGate при застосуванні політик. Це дозволяє реалізувати динамічний контроль доступу клієнтів залежно від їх поточного стану. Використання динамічних груп допомагає автоматизувати та значно спростити дотримання різних вимог безпеки.

Роздільне тунелювання трафіку додатків дозволяє гранульовано визначити, які дані повинні бути передані через шифрований тунель, а які безпосередньо через Інтернет. Це позитивно позначиться на швидкості передачі. Підсумовуючи, FortiClient спрощує процеси автоматичного підключення та динамічного вибору сервера VPN, також використання багатофакторної автентифікації для забезпечення додаткового рівня безпеки VPN-з'єднання.

Існує кілька різних способів реалізації розділеного тунелювання VPN:

- Розділене тунелювання на основі URL-адрес дає змогу вибрати, які саме URL-адреси потрібно зашифрувати через VPN. Зазвичай це робиться за допомогою розширення браузера VPN.
- Розділене тунелювання на основі додатків працює подібним чином, оскільки воно дає вам змогу вибирати, які програми потрібно направляти через VPN, тоді як решта трафіку йде через звичайну мережу.
- Зворотне розділене тунелювання працює навпаки. Хоча перші два приклади направляють усе через відкриту мережу за замовчуванням, можливий вибір програми та URL-адреси, яку потрібно направляти через VPN, із зворотним розділеним тунелюванням увесь трафік автоматично надсилається через VPN, якщо не вказати інше. За допомогою інверсного розділеного тунелювання потрібно вибрати, які URL-адреси та програми не бажано перевіряти через VPN.

2.2 Особливості налаштування SAML серверу

SAML представляє собою відкритий стандарт обміну даними автентифікації, що базується на мові XML. Веб-програми використовують SAML, щоб передавати автентифікаційні дані між сторонами процесу: а саме між

системою керування доступом та провайдером. Для прикладу розглянемо використання в якості провайдера послуг FortiClient.

SAML з'явився в індустрії високих технологій для спрощення процесу автентифікації, коли користувачам потрібно було отримати доступ до кількох незалежних веб-додатків у різних доменах. До появи SAML, технологія єдиного входу цілком виконувала поставлені задачі, проте базувалася на файлах cookies, які були актуальними лише в межах одного домену.

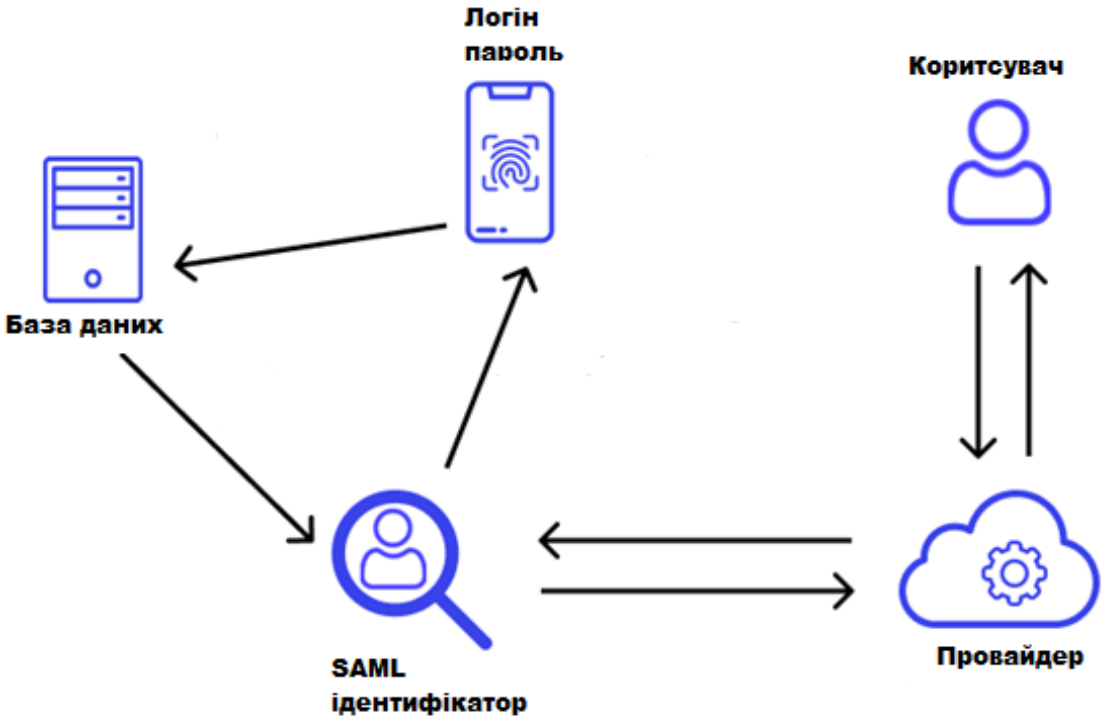


Рисунок 2.2 – Принцип роботи технології SAML

При використанні SAML технологія входу досягається за рахунок узгодження процесу автентифікації із системою управління доступом. Веб-програми можуть використовувати SAML, через систему керування доступом. Такий метод автентифікації означає, що користувачам більше не потрібно запам'ятовувати численні комбінації логінів та паролів. Більш того, він має безперечну перевагу для провайдера, у вигляді підвищення рівня безпеки платформи, переважно завдяки тому, що усунуто необхідність зберігання паролів та процесів їх відновлення.

Концепція SAML працює шляхом обміну інформацією користувача (логіни, стан автентифікації, ідентифікатори та інші дані) між системою управління доступом та провайдером послуг. В результаті, це спрощує і забезпечує безпеку процесу автентифікації, так як в такому випадку користувачеві необхідно увійти в систему тільки один раз з використанням одного набору даних для входу. Таким чином, коли користувач надає запит для отримання доступу до сайту, SAML передає аутентифікаційні дані постачальника послуг, які в результаті дозволяють доступ користувачеві [20].

Процес двоетапної автентифікації починається в той момент, коли користувач намагається увійти в додаток, службу або систему, доки йому не буде надано доступ для використання. Алгоритм аутентифікації виглядає наступним чином:

Крок 1. Користувач відкриває програму або веб-сайт, до якої він хоче отримати доступ. Здійснює введення облікових даних для входу.

Крок 2. Далі він зазначає свої дані, якими звичайно є ім’я користувача та пароль. Додаток або веб-сайт підтверджує деталі та розпізнає, що було введено правильні дані початкової автентифікації на сервері авторизації в нашому випадку за протоколом SAML.

Крок 3. Якщо програма або веб-сайт не використовує облікові дані для входу з паролем, буде згенеровано ключ безпеки для користувача. Ключ буде оброблено інструментом автентифікації, а сервер перевірить початковий запит.

Крок 4: Користувачеві пропонується надіслати другий фактор автентифікації. Очевидно, що таким фактором буде підтвердження прав власності. Наприклад, додаток або веб-сайт надішле унікальний код на мобільний пристрій користувача.

Крок 5: Користувач вводить код у програму або на веб-сайт, і якщо код буде схвалено, відбудеться автентифікація і доступ до системи.

Модель налаштування SAML для SSL VPN представлена на рисунку 2.2

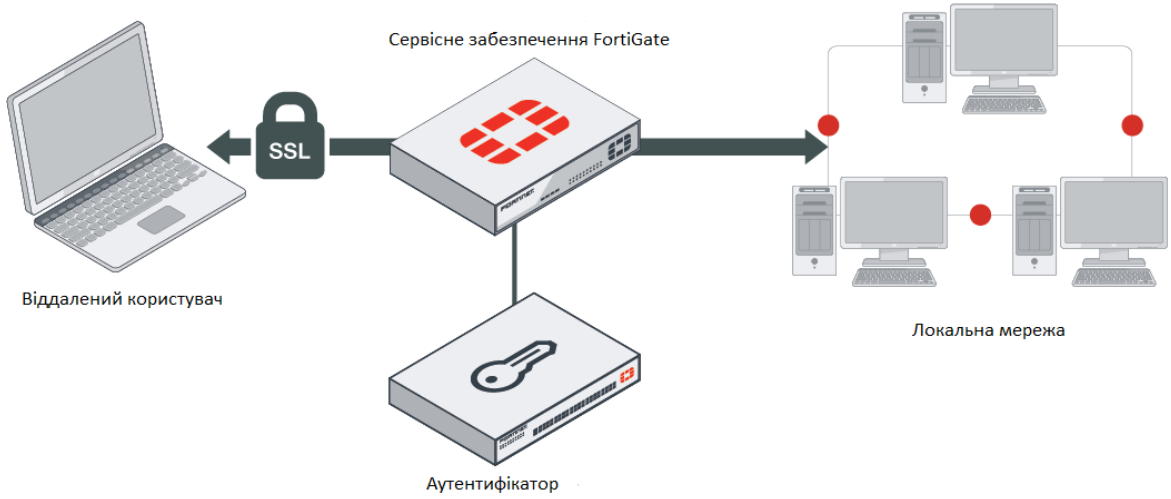


Рисунок 2.3 – Модель мережевого підключення обладнання сімейства FortiGate

Розглянемо процес мережевого підключення в наступній послідовності:

Адміністратор або кінцевий користувач налаштовує з’єднання SSL VPN із увімкненим SAML.

FortiClient підключається до FortiGate.

FortiGate повертає посилання перенаправлення на сторінку авторизації SAML IdP.

FortiClient відображає сторінку авторизації IdP у вбудованому вікні браузера.

Кінцевий користувач вводить свої облікові дані у вікні для входу.

Після успішної спроби входу FortiClient встановлює тунель до FortiGate.

У такій схемі FortiGate налаштовується як SP (постачальник послуг), а FortiAuthenticator — як IdP (постачальник ідентифікаційної інформації).

Загалом, безпечне віддалене підключення можна реалізувати великим набором способів, використовуючи протоколи, а також групові чи індивідуальні політики безпеки [16, 21]. Потрібно наголосити, що особливість несанкціонованого входу зумовлюється і тим, що внаслідок витоку інформації можливий вільний доступ до облікових даних, і в цьому випадку такі дані

можуть бути використані без відома особи власника та зокрема в злочинних цілях.

Налаштуємо FortiGate SP як користувача SAML. Ми повинні налаштувати віддалений сертифікат IdP від FortiAuthenticator на FortiGate [21]:

```
config user saml
edit "bbiliavets"
set cert "Fortinet_Factory"
set entity-id "http://172.17.61.59:11443/remote/saml/metadata/"
set single-sign-on-url "https://172.17.61.59:11443/remote/saml/login/"
set single-logout-url "https://172.17.61.59:11443/remote/saml/logout/"
set idp-entity-id "http://172.17.61.118:443/saml-idp/101087/metadata/"
set idp-single-sign-on-url "https://172.17.61.118:443/saml-idp/101087/login/"
set idp-single-logout-url "https://172.17.61.118:443/saml-idp/101087/logout/"
set idp-cert "REMOTE_Cert_4"
next
end
```

Додаємо користувача SAML до групи користувачів:

```
config user group
edit "ra-admin"
set member "bbiliavets"
next
end
```

Встановлюємо групу SAML у налаштуваннях SSL VPN:

```
config vpn ssl settings
config authentication-rule
edit 1
set groups "ra-admin"
set portal "full-access"
```

next

next

end.

2.3 Принципи підвищення захищеності з’єднання

Безпека віддаленого доступу до мережевих ресурсів є важливою частиною безпеки. SSL VPN дозволяє адміністраторам налаштовувати, адмініструвати та розгортати стратегію віддаленого доступу для своїх віддалених працівників.

Вибір правильного режиму роботи та застосування належних рівнів безпеки є невід’ємною частиною забезпечення оптимальної продуктивності та взаємодії з користувачем, а також збереження даних у безпеці.

У режимі тунелю клієнт SSL VPN шифрується весь трафік від віддаленого клієнтського комп’ютера та надсилається на FortiGate через тунель SSL VPN з використанням HTTPS-з’єднання між користувачем і FortiGate.

FortiGate встановлює тунель із клієнтом і призначає віртуальну IP-адресу клієнту з діапазону зарезервованих адрес. Хоча базові протоколи відрізняються, результат дуже схожий на тунель IPsec VPN. Весь клієнтський трафік зашифровано, що дозволяє користувачам і мережам обмінюватися широким діапазоном трафіку, незалежно від програм чи протоколів.

Реалізація такого налаштування передбачає наступні результати:

- Широкий спектр програм і протоколів, до яких має доступ віддалений клієнт;
- FortiGate не виконує роль проксі-сервера;
- Просте налаштування та адміністрування, оскільки трафік контролюється політиками брандмауера;
- Прозорий досвід для кінцевого користувача.

Наприклад, користувачеві, який потребує RDP до свого сервера, потрібне лише тунельне підключення, в результаті чого використовуючи звичайну клієнтську програму RDP Windows відбувається з’єднання.

Звичайне тунелювання весь трафік пропускає через FortiGate. Розділене тунелювання лише направляє трафік до визначеної мережі через FortiGate.

Режим тунелю вимагає, щоб клієнт FortiClient VPN був встановлений на віддаленому кінці. Автономний VPN-клієнт FortiClient є безкоштовним для використання та може підтримувати тунелі SSL VPN та IPsec VPN.

Лише режим веб забезпечує безклієнтський доступ до мережі за допомогою браузера з вбудованим шифруванням SSL. Користувачі проходять автентифікацію на веб-порталі FortiGate SSL VPN, який забезпечує доступ до мережевих служб і ресурсів, включаючи HTTP/HTTPS, Telnet, FTP, SMB/CIFS, VNC, RDP і SSH. Коли користувач починає підключення до сервера з веб-порталу, FortiOS проксі-сервер будує з'єднання з сервером. Весь зв’язок між FortiGate і користувачем продовжує здійснюватися через HTTPS, незалежно від служби, до якої здійснюється доступ.

Реалізація такого налаштування передбачає наступні результати:

- Рішення, у якому доступ до всіх віддалених служб здійснюється через веб-портал;
- Жорсткий контроль за вмістом веб-порталу.

Інтеграція з серверами автентифікації

Для мереж із багатьма користувачами доцільно інтегрувати конфігурацію користувача з наявними серверами автентифікації через LDAP, RADIUS або FortiAuthenticator.

Завдяки інтеграції з існуючими серверами автентифікації, такими як Windows AD, кількість помилок під час налаштування локальних користувачів і груп користувачів зменшується, відповідно зусилля з адміністрування також зменшуються. Для підвищення захищеного з’єднання варто використовувати наступне:

Багатофакторну автентифікацію

Багатофакторна автентифікація гарантує, що кінцевий користувач є тим, ким він себе видає, вимагаючи принаймні двох факторів – частини інформації, яку користувач знає тобто пароль, і ресурсу, який користувач має тобто

токен. Третій фактор, який також є підтвердженням користувача може використовуватися відбиток пальця чи розпізнавання обличчя. FortiToken Mobile зазвичай використовується для MFA. FortiGate постачається з двома безкоштовними токенами FortiToken, а інші можна встановити в додатку FortiToken Mobile iOS або через партнерів Fortinet. 2FA є підмножиною MFA, також можна налаштувати за допомогою маркерів електронної пошти.

Розгортання сертифікатів користувачів для віддалених користувачів SSL VPN

Цей метод 2FA використовує сертифікат користувача як другий фактор автентифікації. Це безпечно, оскільки ідентифікує кінцевого користувача за допомогою сертифіката. Конфігурація та адміністрування цього рішення є значно складнішими та потребують адміністраторів із глибокими знаннями про FortiGate та розгортання сертифікатів.

Рисунок 2.4 – Двофакторна аутентифікація

Належним чином керувати політиками та профілями брандмауера лише для рівня доступу, необхідного для віддаленого користувача

Користувачам не потрібен однаковий доступ. Доступ слід надавати лише після ретельного розгляду. Як правило, користувачі розміщуються в групи, і кожній групі надається доступ до обмежених ресурсів. Використання сфер SSL VPN спрощує визначення структури керування для зіставлення користувачів і груп із відповідними ресурсами.

Довірені центри сертифікації

Сертифікат має ідентифікувати домен, щоб віддалений користувач міг розпізнати сервер або портал, до якого налаштований доступ через довірений центр сертифікації.

Стандартні самопідписані сертифікати Fortinet надаються для спрощення початкової інсталяції та тестування. Якщо використовувати ці сертифікати, є вразливість до атак типу «людина посередині», коли зловмисник підробляє сертифікат, компрометує з'єднання та викрадає особисту інформацію. Варто придбати сертифікат сервера в надійного центру сертифікації, що здійснюються в межах організації оскільки присутній зареєстрований такий центр, щоб віддалені користувачі могли впевнено підключатися до SSL VPN.

Важливим є увімкнення параметра «Не попереджати про недійсний сертифікат сервера» на клієнті. Він вимикає попереджувальне повідомлення про сертифікат, потенційно дозволяючи користувачам випадково підключатися до ненадійних серверів. Не рекомендується вимикати попередження про недійсний сертифікат сервера.

Все це застосовується для обмеження несанкціонованого доступу особам, які потрапляють в канал зв'язку між адресатами з метою заволодіння інформацією або з метою її змінити, рисунок 2.5.

Рисунок 2.5 – Схема асиметричного шифрування документу при передачі файлів

У випадку асиметричного шифрування використовуються два різні ключі: один для шифрування (відкритий), інший для розшифровування (закритий).

Аутентифікація є невід'ємною частиною кожного з'єднання TLS. Розглянемо найпростіший процес аутентифікації між двома користувачами, рисунок 2.6.

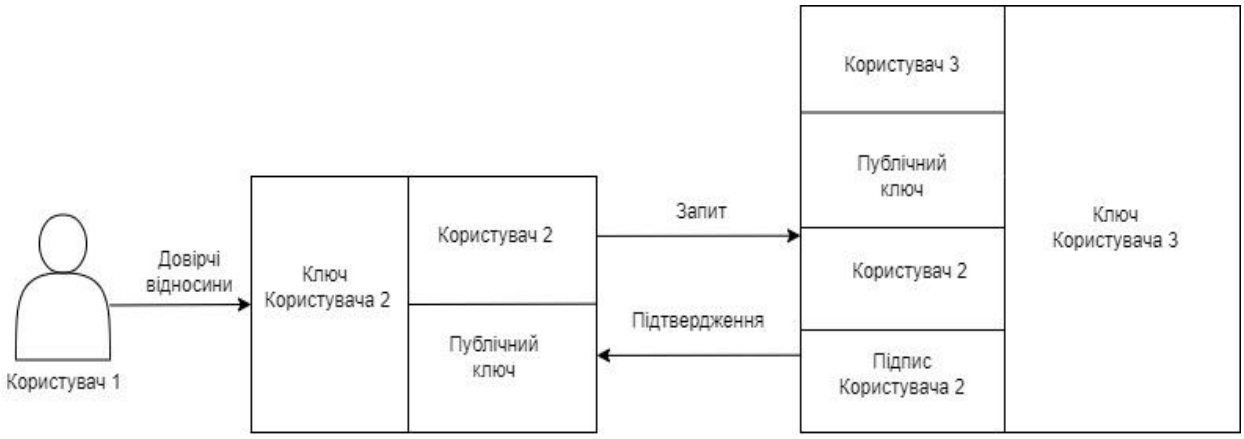


Рисунок 2. 6 –Побудова довірчих відносин між користувачами

Обидва користувачі системи генерують власні відкриті та закриті ключі. Вони обмінюються відкритими ключами. Один з них генерує повідомлення, шифрує його своїм закритим ключем та відправляє іншому. Користувач 2 використовує отриманий від Користувача 1 ключ для розшифрування повідомлення і таким чином перевіряє справжність отриманого повідомлення.

Очевидно, що ця схема побудована на довірі між користувачами мережі. Передбачається, що обмін відкритими ключами відбувся, наприклад, під час особистої зустрічі. Таким чином, перший користувач впевнений, що отримав ключ саме від другого, тобто між ними побудовані довірчі відносини.

Нехай тепер Користувач 1 отримує повідомлення від Користувача 3, з яким він не знайомий, але який стверджує, що має довірчі відносини із Користувачем 2. Щоб це довести, Користувач 3 заздалегідь попросив підписати власний відкритий ключ закритим ключем Користувача 2 і прикріпив цей підпис до повідомлення Користувачу 1. У цьому разі Користувач 1 спочатку повинен перевірити підпис Користувача 2 на ключі Користувача 3, та переконатись у дійсності налагоджених довірчих відносин.

Описана вище схема є технологію створення «ланцюжка довіри».

У протоколі TLS дані ланцюга довіри засновані на сертифікаті автентичності, який надається спеціальними органами які називаються центрами сертифікації (CA). Центри сертифікації проводять перевірку та у випадку, якщо виданий сертифікат скомпрометований, виконується процедура відкликання сертифікату [15-17]. З виданих сертифікатів складається вже розглянутий ланцюжок довіри. Ключовим елементом підтвердження ступеня довіри є сертифікат Root CA certificate (головний центр сертифікації), який підписаний авторизованим центром сертифікації, довіра до якого незаперечна. В загальному вигляді організація ланцюжка довіри виглядає так, як представлено на рисунку 2.7.

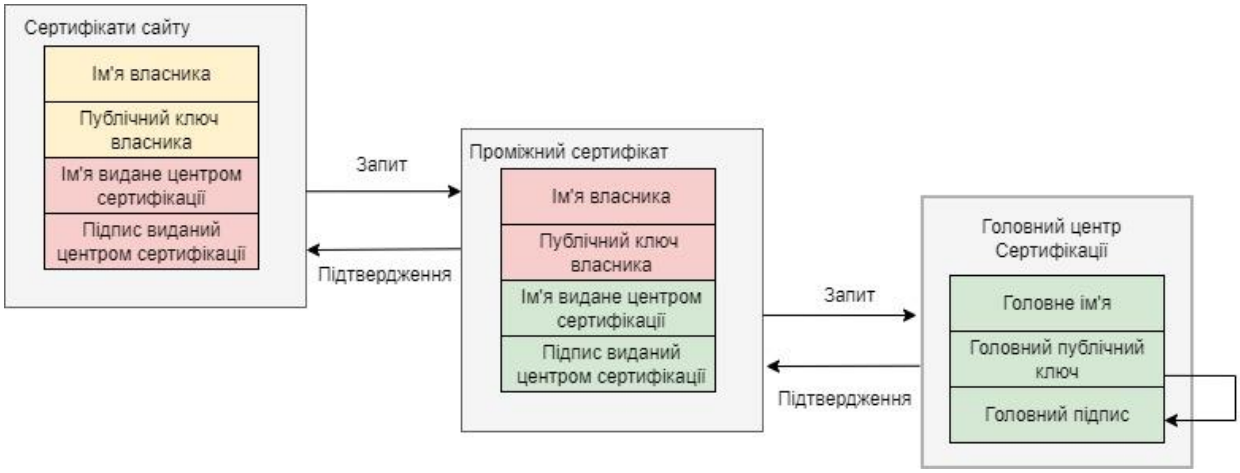


Рисунок 2.7 – Схема обміну сертифікатами для налаштування довірчих відносин

Висновки до розділу 2

В **другому** розділі магістерської роботи створено структурну схему проекту. Розглянуто технологію SAML та особливість їїау реалізації саме з SSL VPN, що визначило спосіб налаштування мережі для віддаленого підключення. Важливість реалізації використання додаткових способів захисту VPN.

Рішення FortiGate SSL VPN включають високопродуктивні криптографічні VPN для захисту користувачів від загроз, які можуть призвести до витоку даних. Технологія Fortinet VPN створює безпечний зв’язок через Інтернет незалежно від використовуваної мережі чи кінцевого пристрою.

Підводячи підсумок, SSL VPN легко впроваджувати, розгортати та використовувати. Це надає кілька організаційних переваг безпеки . Цей VPN також необхідний для підвищення інформаційної безпеки, що реалізує надійну підтримку віддаленої роботи. Зважаючи на зростання кількості кіберзагроз, безпека конфіденційних даних стала головним пріоритетом. Захищене рішення VPN допомагає зменшити ці ризики .

3 МЕТОДИ ЗАБЕЗПЕЧЕННЯ ШИФРУВАННЯ МЕРЕЖІ

3.1 Алгоритми шифрування VPN

Шифрування — це процес кодування частини інформації певним чином, щоб лише авторизовані сторони могли отримати до неї доступ і розшифрувати її. Сучасні технології шифрування практично неможливо зламати. Крім того, навіть якщо комусь вдасться отримати доступ до інформації, вони не зможуть прочитати її, якщо відсутній ключ.

Щоб шифрування працювало у відправника та одержувача необхідно знати правила, які використовуються для перетворення вихідного повідомлення в кодовану форму. Правила засновані на алгоритмі і ключі. Алгоритм — це математична функція, яка поєднує повідомлення, текст, символи або всі три способи, які називають ключем. Результатом є нечитабельний рядок шифру. Розшифровка надзвичайно складна або неможлива без правильного ключа.

VPN реалізує використання криптографії, яка охоплює захист інформації за допомогою таких концепцій, як шифрування та дешифрування.

Шифрування передбачає перетворення відкритого тексту у зашифрований за допомогою ключа. Дешифрування відбувається навпаки, зашифрований текст перетворюється у відкритий за допомогою ключа.

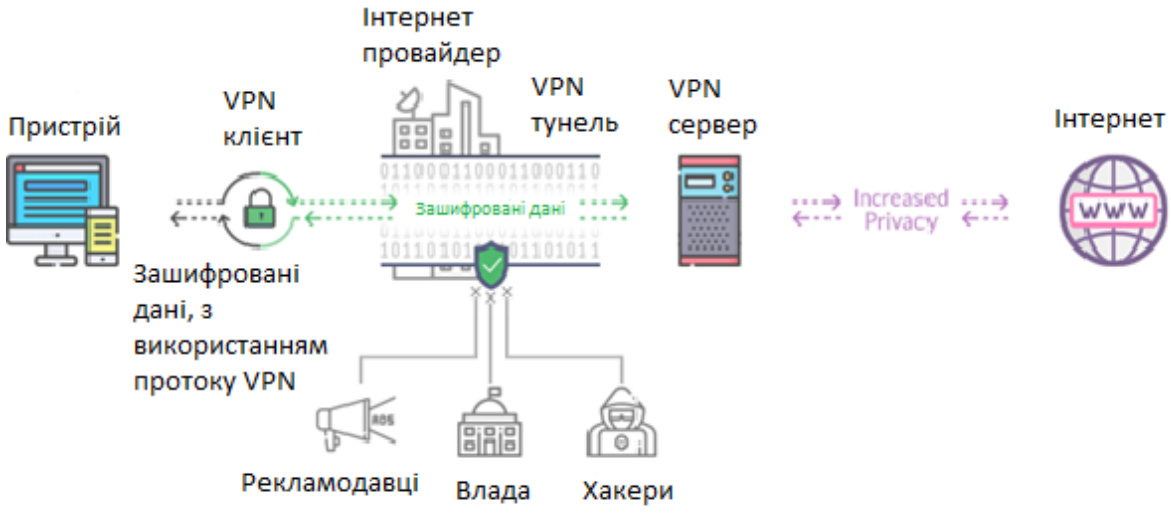


Рисунок 3.1 – Схема шифрування даних VPN

Ключ шифрування VPN — це надійний пароль, який використовується для шифрування й розшифрування даних і відомий лише ПК або пристрою і серверу VPN. Довжина ключа вимірюється в бітах (двійковий код з одиниць і нулів) і може бути різною.

Найпоширеніші методи шифрування, які VPN використовують для захисту онлайн-трафіку та з'єднання:

- Шифрування закритим ключем (симетричне)

Симетричне шифрування передбачає, що обидві сторони, при обміні даними, мають однаковий ключ для шифрування відкритого тексту та його дешифрування. Більшість VPN використовують цей алгоритм шифрування.

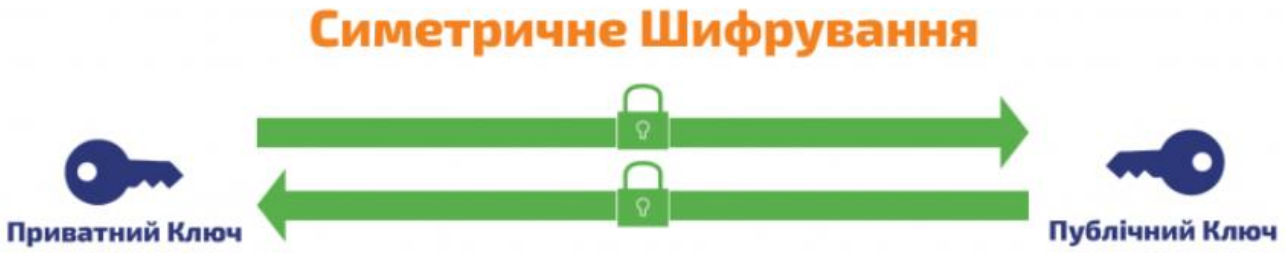


Рисунок 3.2 – Використання ключу в симетричному шифруванні

Крім того, симетричне шифрування використовується такими шифрами, як AES і Blowfish.

- Шифрування відкритим ключем (асиметричне)

Асиметричне шифрування використовує два ключі: відкритий і закритий. Відкритий ключ шифрує вихідний текст та лише закритий ключ може розшифрувати вхідний текст.

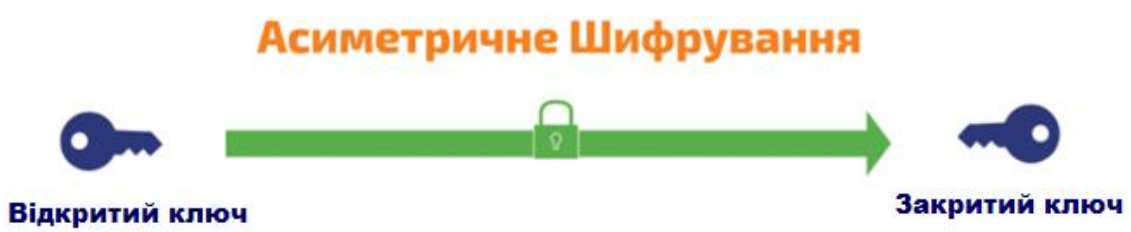


Рисунок 3.3 – Використання ключу в асиметричному шифруванні

Асиметричне шифрування вимагає, щоб більшість користувачів мали відкритий ключ, а авторизована сторона мала ще закритий ключ для дешифрування.

Таблиця 3.1 – Узагальнення переваг

Симетричне шифрування	Асиметричне шифрування
Один ключ використовується для шифрування і дешифрування даних.	Пара ключів використовується для шифрування і дешифрування. Ці ключі відомі як “відкритий ключ” і “закритий ключ”.
Простий метод шифрування, так як використовується тільки один ключ.	У зв’язку з тим, що використовується пара ключів – складний процес.
Використовується для шифрування великих об’ємів даних.	Забезпечує аутентифікацію.
Забезпечує високу продуктивність і вимагає менше обчислювальної потужності.	Складні процеси протікають повільніше і вимагають більшої обчислювальної потужності.
Для шифрування даних використовується менша довжина ключа (128-256 біт).	Використовуються довші ключі шифрування (1024-4096 біт).
Ідеально підходить для шифрування великої кількості даних.	Використовується при шифруванні невеликого об’єму даних.
Стандартні алгоритми: RC4, AES, DES, 3DES.	Стандартні алгоритми: RSA, Diffie-Hellman, El Gamal і DSA.

Розширений стандарт шифрування

Найкращим прикладом симетричного шифрування є AES. Інформація класифікується за трьома категоріями: таємна, цілком таємна або з обмеженим

доступом. Усі ключі довжини можна використовувати для захисту цілком таємного рівня та інформації з обмеженим доступом.

Алгоритм шифрування AES визначає численні перетворення, які відбуваються з даними, що зберігаються в масиві. Перше – це перетворення в шифруванні AES. Відбувається підстановка даних за допомогою таблиці підстановки; друге – перетворення зсуває рядки даних, а третє – змішує стовпці. Останнє перетворення виконується для кожного стовпця з використанням іншої частини ключа шифрування. Довжина ключа важлива, оскільки довші ключі потребують більшої кількості циклів перетворень.

AES включає три блокові шифри :

AES-128 використовує 128-бітний ключ для шифрування та дешифрування блоку повідомлень.

AES-192 використовує 192-бітний ключ для шифрування та дешифрування блоку повідомлень.

AES-256 використовує 256-бітний ключ для шифрування та дешифрування блоку повідомлень

Кожен метод шифрує та розшифровує дані блоками по 128 біт за допомогою криптографічних ключів 128, 192 та 256 біт відповідно.

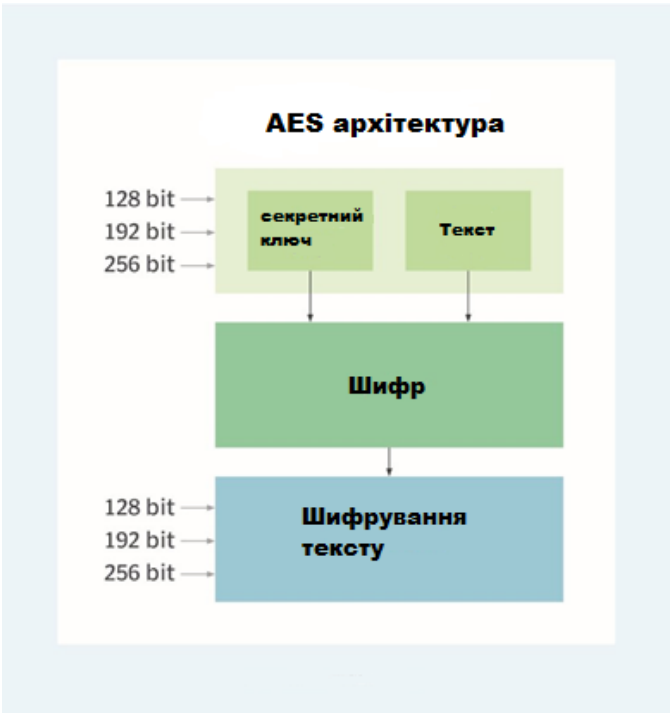


Рисунок 3.4 – Архітектура шифрування AES

Blowfish

Blowfish був реалізований компаніями VPN, які хотіли надати альтернативу AES. Творець шифру Брюс Шнайер навмисне не патентував алгоритм, щоб ним міг вільно користуватися кожен. Це одна з причин, чому його включили до безкоштовної системи OpenVPN із відкритим кодом.

Це блоковий шифр, який використовує менший масив, ніж AES. Він має 64-розрядний блок, який вдвічі менший за розмір сітки AES. Це робить систему набагато слабшою за AES. Хоча шифр Blowfish займав нішу як гідна альтернатива AES. Однак невеликий розмір блоку робить його вразливим до атак. Жоден великий VPN-сервіс не пропонує Blowfish. Він був доступний у Buffer і PrivateInternetAccess, але обидві мережі VPN тепер відмовилися від Blowfish на користь AES.

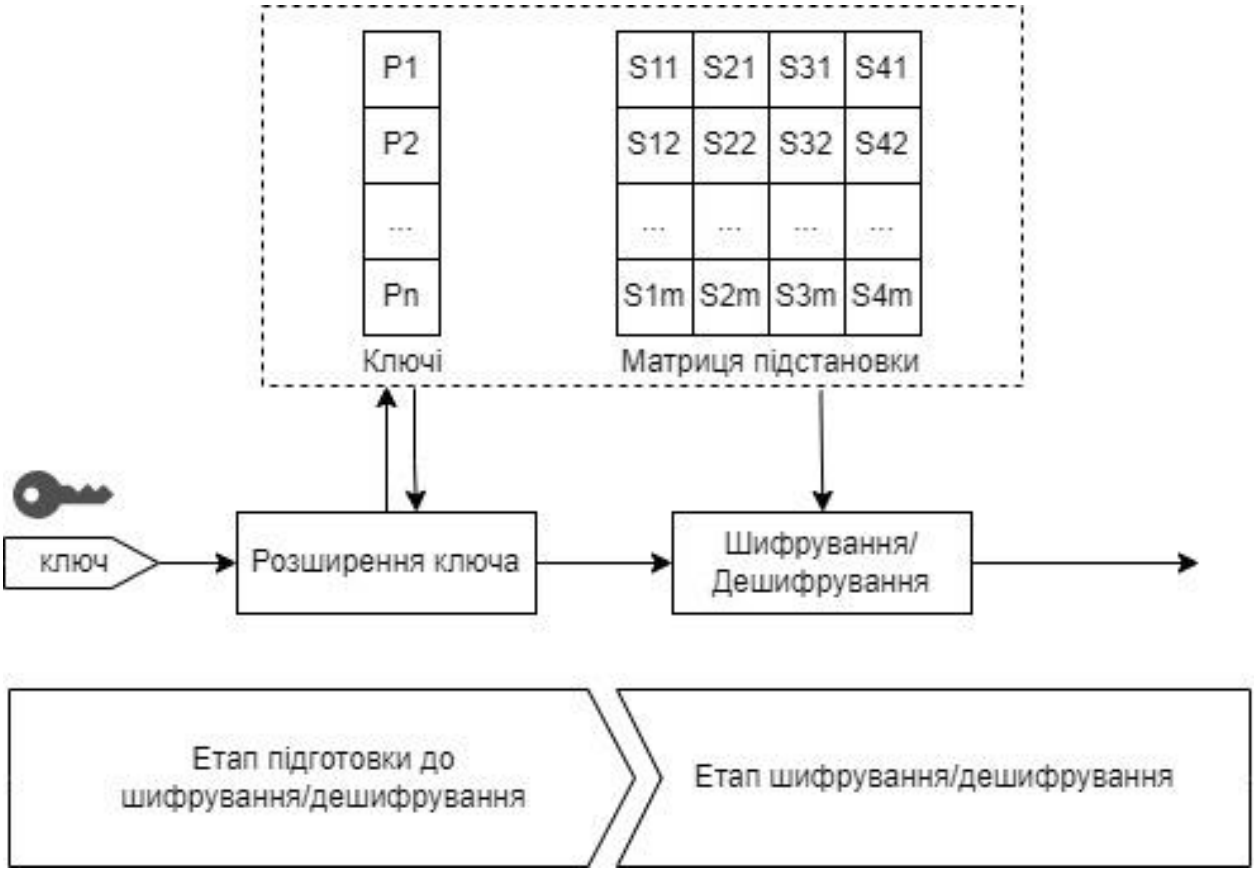


Рисунок 3.5 – Принцип шифрування Blowfish

Шифрування рукостискання

RSA – це процес узгодження, який дозволяє сторонам, при обміні даними, визнати одна одну та домовитися про алгоритми шифрування чи ключі використання.

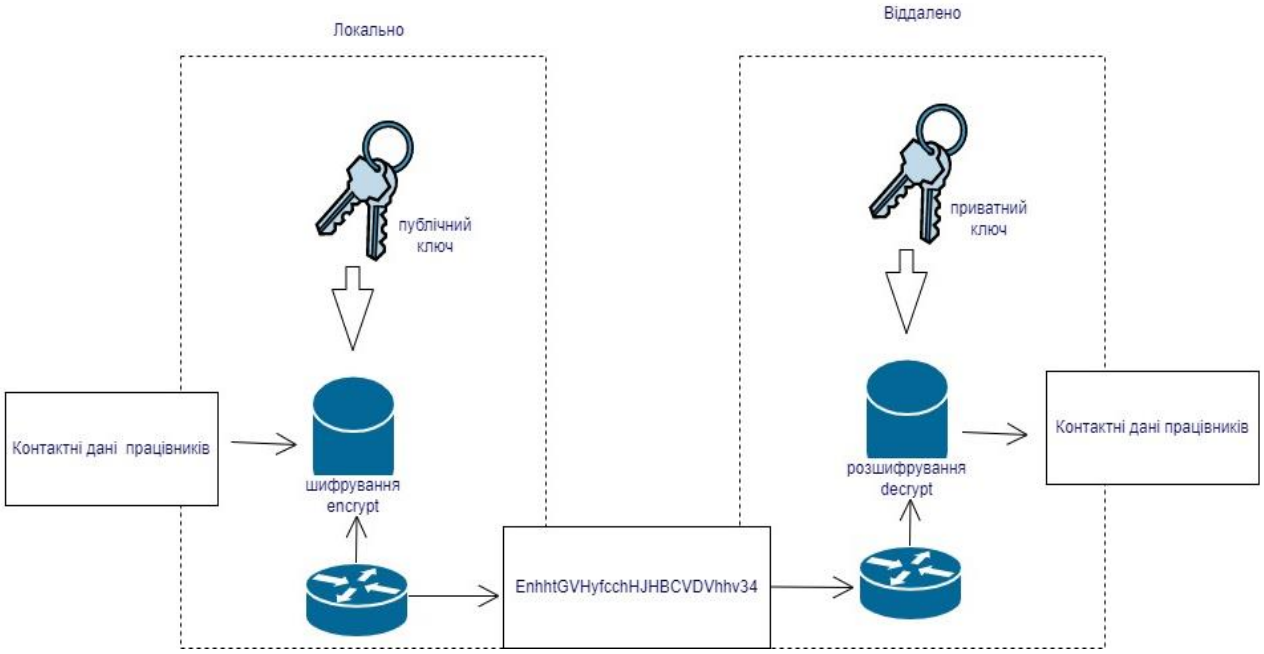


Рисунок 3.6 – Принцип шифрування RSA

У більшості випадків для шифрування RSA використовується алгоритм Рівест-Шаміра-Адлемана. Інші VPN також використовують обмін ключами за еліптичною кривою Діффі-Хеллмана.

Діффі-Хеллман

Згідно з цією формулою, кожна сторона підключення має приватний ключ, а переговори між двома сторонами генерують відкритий ключ і спільний приватний ключ, який відомий як «спільний секрет».

Відповідно до Діффі-Хеллмана, ключовий внесок сервера записується на сертифікаті, а клієнтський генерується випадковим чином. Цей стан називається «статично-ефемерним», де значення сертифіката сервера є статичним, а випадковий внесок від клієнта називається «ефемерним». Ключ-значення наданий сервером, також є випадковим числом, тому цю систему називають «ефемерно-ефемерною» або ефемерною Діффі-Хеллмана.

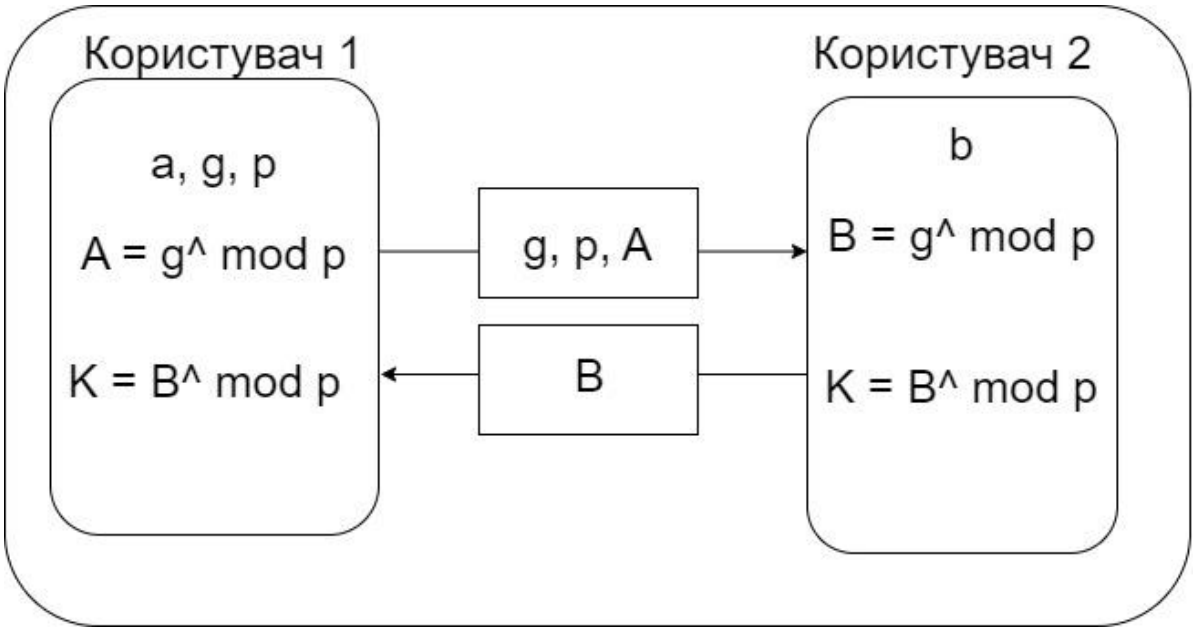


Рисунок 3.7 – Принцип кодування Діффі-Хеллмана

Алгоритм безпечного хешування

SHA – це алгоритм хешування для перевірки автентичності даних SSL/TLS-з'єднань.

Процес посилюється унікальним відбитком пальця, який він створює для перевірки дійсності сертифіката TLS як підтвердження того, що відбувається підключення до правильного VPN-сервера.

Важливо зазначити, що без SHA цифровий хакер може легко перенаправити ваш інтернет-трафік на свій сервер замість цільових VPN-серверів.

Хеш-код автентифікації повідомлення

Код HMAC - це тип коду автентифікації повідомлень, який поєднує в собі криптографічну хеш-функцію та секретний криптографічний ключ.

Цей метод перевіряє цілісність і автентичність даних, щоб гарантувати, що вони залишаться недоторканими. Більшість якісних VPN часто використовують алгоритми хешування SHA разом з автентифікацією HMAC для максимальної безпеки.

Ідеальна передня секретність

Perfect Forward Secrecy – це метод шифрування, який використовується набором протоколів узгодження ключів (в першу чергу RSA та ECDH), щоб гарантувати, що сеансові ключі залишаються непорушними, навіть якщо приватний ключ сервера буде скомпрометований.

PFS генерує нові ключі, що використовуються для шифрування та дешифрування, кожні кілька секунд.

Рисунок 3.8 – Кодування PFS

Шифрування VPN військового класу

Шифрування VPN військового рівня є стандартним шифруванням, яке використовується військовими установами. Це надійне та доступне шифрування AES. Оскільки державні організації часто працюють поза увагою, вони зазвичай використовують найкращі доступні протоколи безпеки, щоб гарантувати, що кожна інформація залишається прихованою та зашифрованою.

Через те, що це передова та складна технологія шифрування, не багато служб VPN можуть собі це дозволити. Ось чому більшість служб VPN використовують звичайне або, в деяких випадках, розширене шифрування. Це все ще досить безпечно та надійно, але набагато слабкіше, ніж шифрування VPN військового рівня. В ідеалі, обираючи службу VPN, користувачі підбирати функції, яка пропонує найвищі можливі стандарти шифрування.

Наскрізне шифрування

Наскрізне шифрування надзвичайно ефективно захищає інформацію. Без нього вона та дані були б не зашифровані, коли вони потрапляють на проміжний сервер. Це означає, що ваш інтернет-провайдер може бачити ваші повідомлення, якщо він стежить за вашою діяльністю.

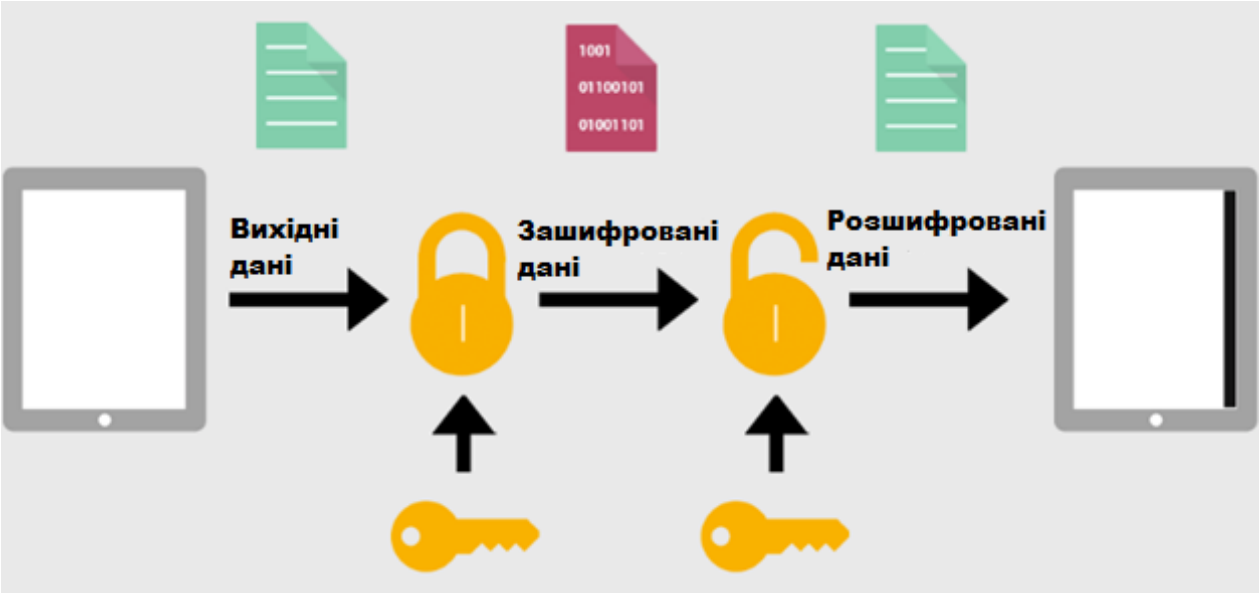


Рисунок 3.9 – Наскрізне шифрування

Зважаючи на це, наскрізне шифрування є важливим для збереження вашої особистої та фінансової інформації.

Недоліки наскрізного шифрування

Незважаючи на те, що це один із найнадійніших інструментів, який можна використовувати для забезпечення конфіденційності та безпеки, наскрізне шифрування має слабкі місця, як і будь-який інший інструмент. Хоча їх небагато, деякі з найбільш значних загроз включають:

- Наскрізне шифрування не захищає кінцеві точки, тому в разі успішного злому з одного боку ключ може бути скомпрометований;
- Не всі програми та браузери використовують наскрізне шифрування. Одним із прикладів цього є додаток WhatsApp. Хоча він шифрує свої повідомлення, він не шифрує резервні копії повідомлень, які зберігає на серверах Google. Це означає, що Google може отримати доступ до журналів резервного копіювання своїх користувачів;

- Хакери можуть перехопити ваші дані, використовуючи троянські віруси або зловмисне програмне забезпечення. Це дозволяє їм обійти шифрування та отримати доступ до вашої особистої інформації.

3.2 Шифрування VPN на основі SSL

Рівень протоколу рукостискання SSL включає наступні протоколи:

- протокол рукостискання SSL;
- протокол специфікації шифрування SSL Change;
- протокол оповіщення SSL.

Ці протоколи використовуються для обміну інформацією про керування SSL, забезпечення взаємної автентифікації між протоколами застосунків, що передають дані, узгодження алгоритмів шифрування і генерації ключів.

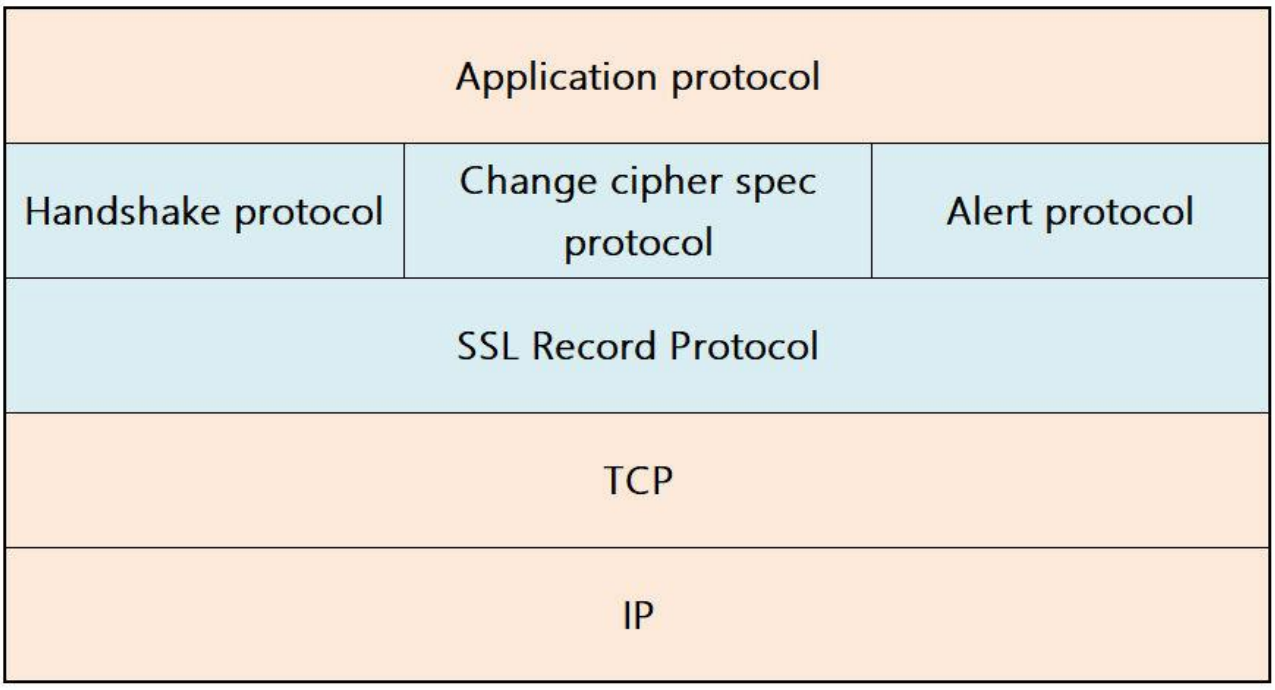


Рисунок 3.10 – Вміст протоколу рукостискання SSL

З усіх цих протоколів найбільш важливими є протокол запису та рукостискання.

Протокол запису SSL: Він заснований на надійному транспортному протоколі TCP і забезпечує базові функції, такі як інкапсуляція даних, стиснення та шифрування для протоколів вищого рівня.

Протокол рукостискання SSL: Він заснований на протоколі запису SSL і використовується для аутентифікації двох сторін, узгодження алгоритмів шифрування, обміну ключами шифрування і т.д. На початок фактичної передачі даних.

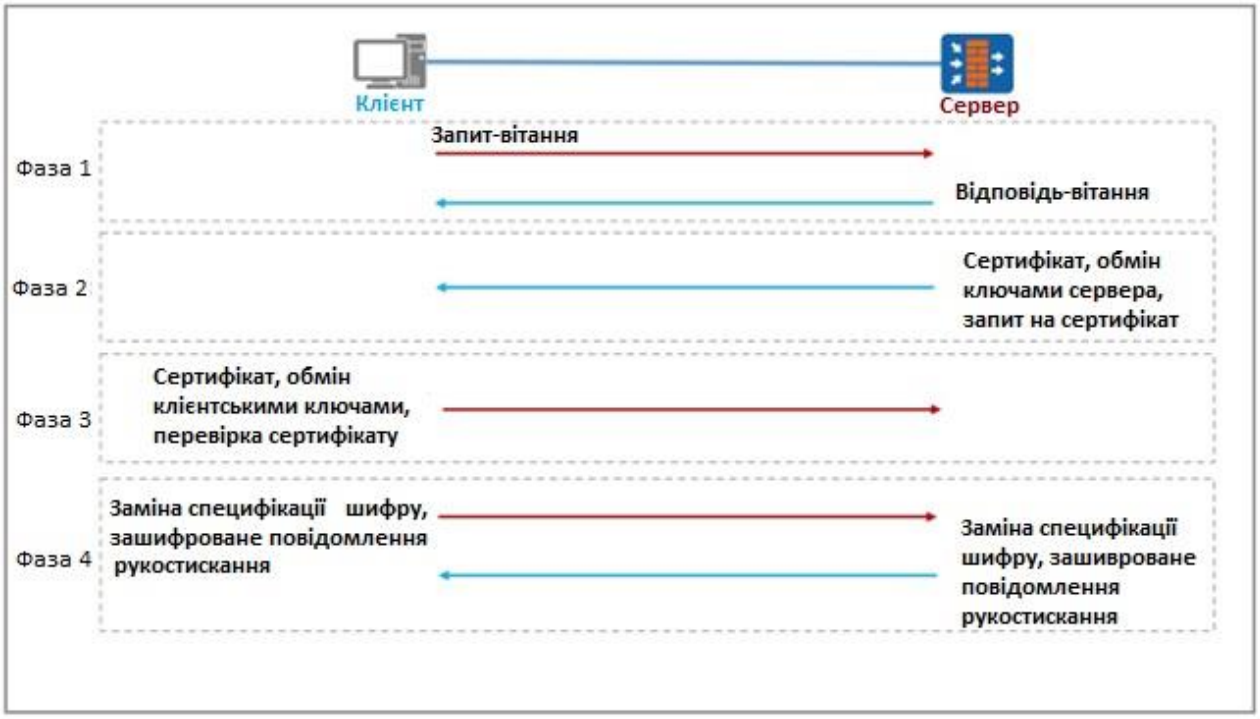


Рисунок 3. 11 – Процесу протоколу рукостискання SSL

Однією з переваг використання SSL є зручність обходу брандмауерів. Брандмауери NAT часто налаштовані на маршрутизаторах по типу Wi-Fi та іншому мережевому обладнанні. Для захисту від загроз вони відкидають будь-який нерозпізнаний інтернет-трафік, який включає пакети даних без номерів портів. Зашифровані пакети IPSec не мають номерів портів, призначених за замовчуванням, це означає, що вони можуть потрапити в брандмауери NAT. Це може перешкоджати роботі IPSec VPN.

Трафік SSL проходить через 443 порт, який більшість пристроїв розпізнає як порт для безпечного трафіку HTTPS. Майже всі мережі дозволяють трафік HTTPS на порт 443. OpenVPN за замовчуванням використовує порт 1194 для трафіку UDP, але його можна пересилати через порти UDP або TCP, включаючи порт TCP 443. Це робить SSL більш корисним для обходу брандмауерів, які блокують трафік на основі портів.

Висновки до розділу 3

В **третьому** розділі магістерської роботи з’ясовано методи шифрування VPN. Роз’яснено що вся інформація, яка проходить через VPN тунель шифрується. Також VPN приховує фактичну IP-адресу та призначає приватну, яка генерується з сервера VPN, до якого відбулося підключення.

Отже, шифрування відбувається наступним чином: VPN-клієнт спочатку шифрує запити на підключення і відправляє їх на VPN-сервер, який розшифровує їх та пересилає в Інтернеті. Потім отримані дані шифруються VPN-сервером і відправляються VPN-клієнту, який розшифровує отриману інформацію для вас.

4 ДОСЛІДЖЕННЯ РЕАЛІЗАЦІЇ ВІДДАЛЕНОГО ПІДКЛЮЧЕННЯ КОРИСТУВАЧІВ З ВИКОРИСТАННЯ ТЕХНОЛОГІЇ SAML

4.1 Формулювання проблеми та постановка завдання на дослідження

Безпечний обмін даними є важливим з використанням сучасних інформаційних технологій, в ході виконання реальних завдань. Аналізуючи наявність прогнозованих загроз при проходженні конфіденційної інформації у VPN тунелі, виникає необхідність дослідження безпечного підключення та авторизації користувачів до своїх робочих місць.

Для досягнення поставленої цілі:

- провести аналіз наявних проколів VPN;
- обґрунтувати вибір технології та мережевого обладнання для побудови VPN тунелю;
- обрати середовище реалізації обраної технології;
- реалізувати VPN з сервером авторизації;
- підвищити захищеність мережі VPN.

Організації все частіше починають використовувати незалежні джерела аутентифікації для програм та веб-порталів. Одним з дослідників SAML аутентифікації є викладач Луїсвільського університету Джеймс Левіс, який дослідив та підтвердив чимало її переваг, однією з яких є зменшення кількості звернень до служби технічної підтримки, що й досі актуально для функціонування багатьох організацій.

4.2 Реалізація двоетапної аутентифікації з використанням токену

Двофакторна автентифікація значно знижує ризик доступу хакерів до онлайн-акаунтів, блокуючи 96% масових фішингових атак. Поєднуючи цифрову ідентифікацію та 2FA, ви отримуєте безпечний продукт автентифікації, створений для глобального масштабування. Фактори автентифікації включають одноразовий пароль, надісланий на мобільний пристрій.

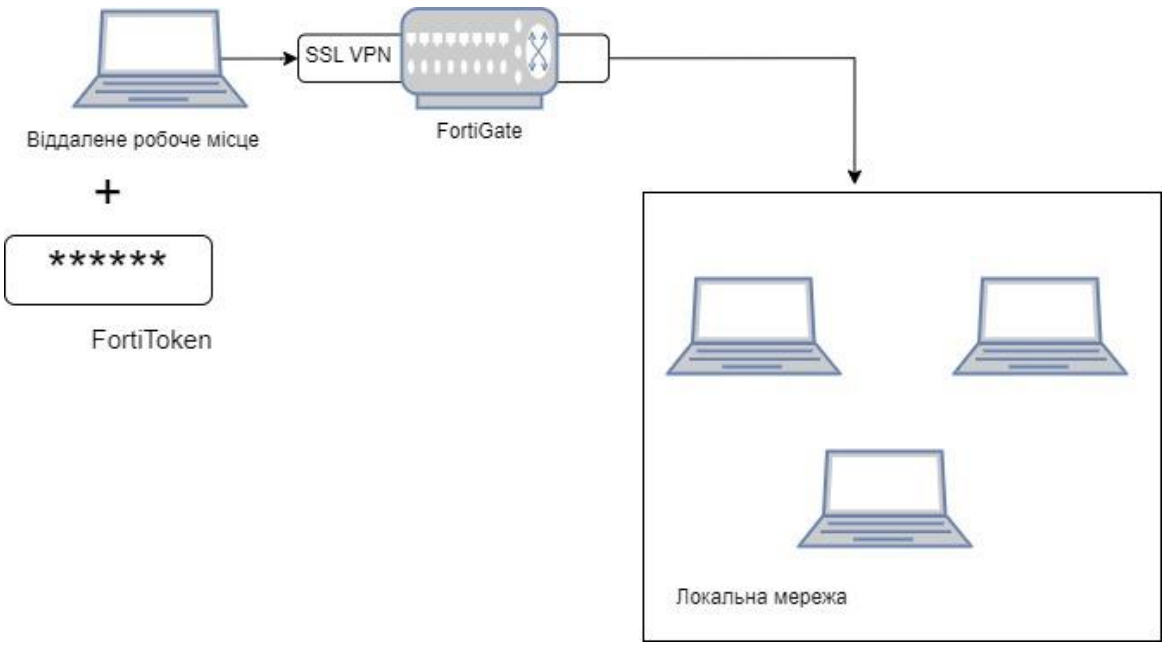


Рисунок 4.1 – Підключення з використанням мобільного токену

Ця конфігурація додає двофакторну автентифікацію до конфігурації розділеного тунелю тобто налаштування SSL VPN для віддаленого користувача. Він використовує один із двох безкоштовних мобільних токенів FortiToken, які вже встановлені на FortiGate.

Приклад програмного коду для налаштування користувача та групи користувачів:

```
config user local
    edit "bbiliavets"
        set type password
        set two-factor fortitoken
        set fortitoken <select mobile token for the option
list>
        set email-to <bbilivets@adps.dpsu>
        set passwd <**********>
    next
end
config user group
    edit "ra-admin"
        set member "bbiliavets"
    next
end
```

Коли FortiToken додається до користувача *bbiliavets* , на електронну адресу надсилається електронний лист. При дотриманні інструкцій, потрібно встановити мобільний додаток FortiToken на своєму пристрої, в наслідок чого активується маркер.

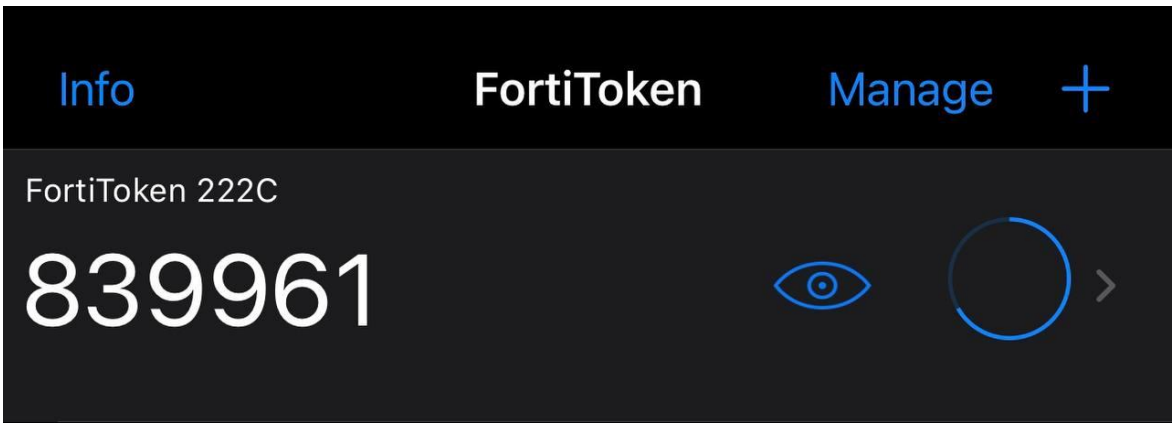


Рисунок 4.2 – Персональний токен для входу в мережу

4.3 Налаштування VPN на базі IP Sec

В ході дослідження було налаштовано віддалене підключення користувача до корпоративної мережі за допомогою IPsec VPN, до якої вони підключаються за допомогою FortiClient. Інтернет-трафік віддаленого користувача також направляється через FortiGate.

За бажанням можна створити користувача, який використовує двофакторну автентифікацію, і користувача LDAP. Здійснення налаштування можливе як за допомогою командного рядку, та і у графічному редакторі, який було обрано для налаштування IPsec VPN.

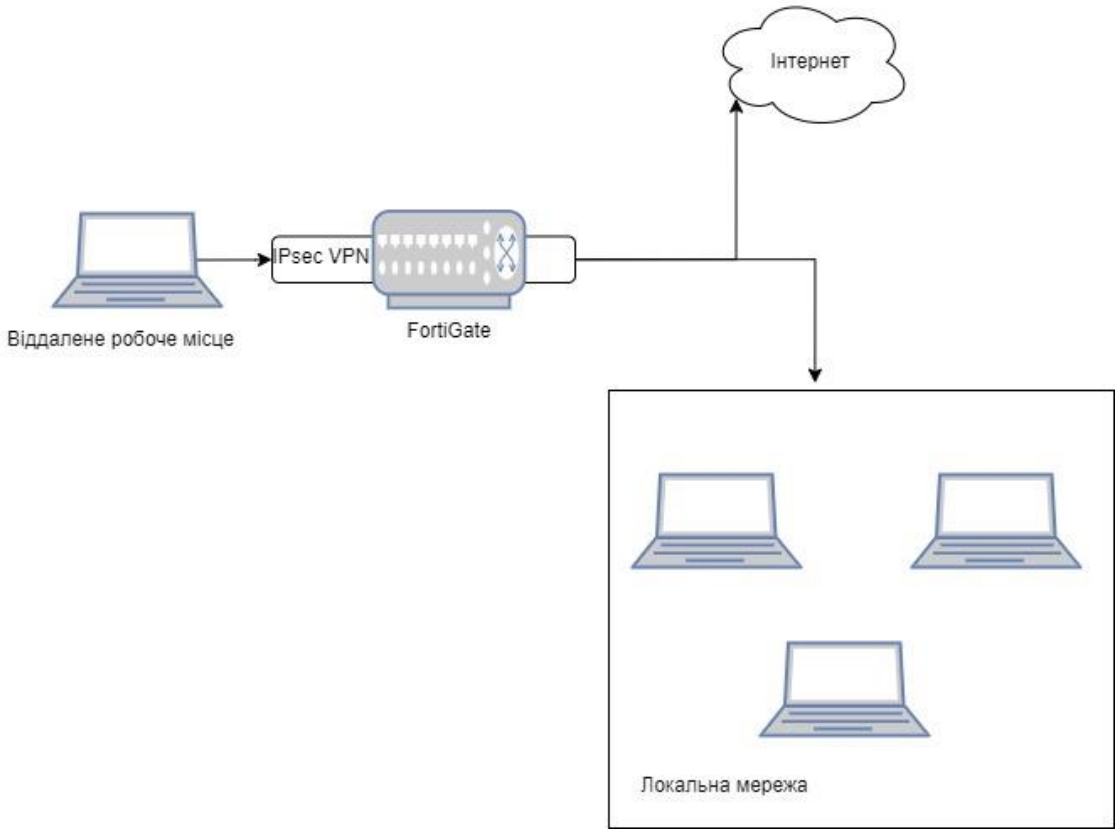
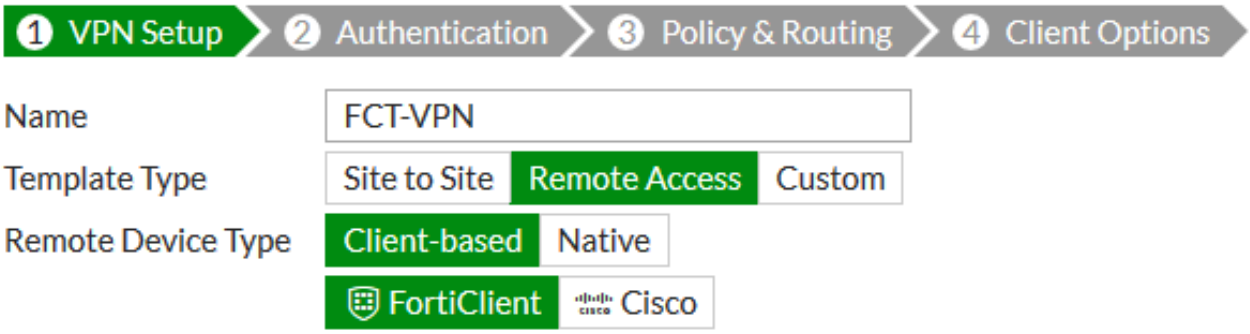


Рисунок 4.3 – Приклад підключення для IPsec VPN

Для створення VPN, додаємо до VPN > IPsec Wizard і створюємо новий тунель за допомогою шаблону. Варто знати, що назва тунелю не може містити пробілів або перевищувати 13 символів. Приклад обраних налаштувань зображено на рисунку 4.4.



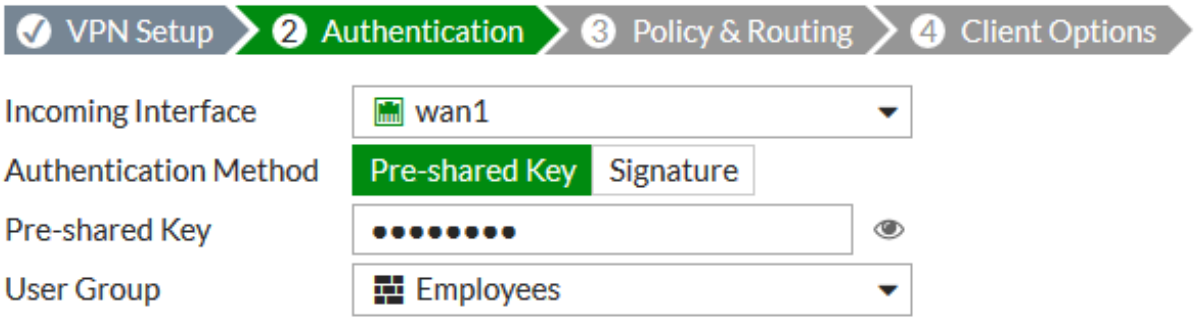


Рисунок 4.4 – Налаштування при створені IPsec

Встановлюємо Local Interface на lan і Local Address на адресу локальної мережі.

Вводимо діапазон адрес користувачів VPN. Діапазон IP-адрес, який ми вводимо, спонукає FortiOS створити новий об'єкт брандмауера для VPN-тунелю, використовуючи назву тунелю з суфіксом _range. Переконуємось, що не обрано параметр «Увімкнути розділений тунель IPv4» , щоб увесь Інтернет-трафік проходив через FortiGate.

10. Якщо для одного інтерфейсу сервера віддаленого з'єднання визначено декілька комутованих мереж VPN IPsec, кожна конфігурація фази 1 має визначати унікальний ідентифікатор однорангового вузла, щоб розрізнити тунель, до якого під'єднується віддалений клієнт:

1. Переходимо до VPN > Тунелі IPsec і редагуємо щойно створений тунель.

2. Обираємо «Перетворити на спеціальний тунель» .

3. У розділі «Автентифікація» обираємо «Редагувати» .

4. У розділі Параметри однорангового вузла встановлюємо для «Типів прийому значення Специфічний ідентифікатор однорангового вузла» .

Для перегляду інтерфейсу VPN, обираємо «Мережа», а далі «Інтерфейси» .

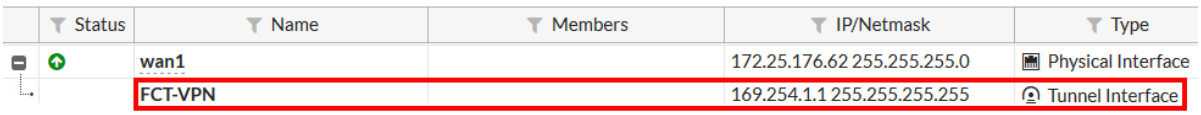


Рисунок 4.5 – Інтерфейс мережевого налаштування VPN

4.4 Налаштування VPN на базі SSL

Це зразок конфігурації віддалених користувачів, які отримують доступ до корпоративної мережі та Інтернету через SSL VPN у режимі тунелю за допомогою FortiClient, але отримують доступ до Інтернету без проходу через тунель SSL VPN. (рисунок 3.6)

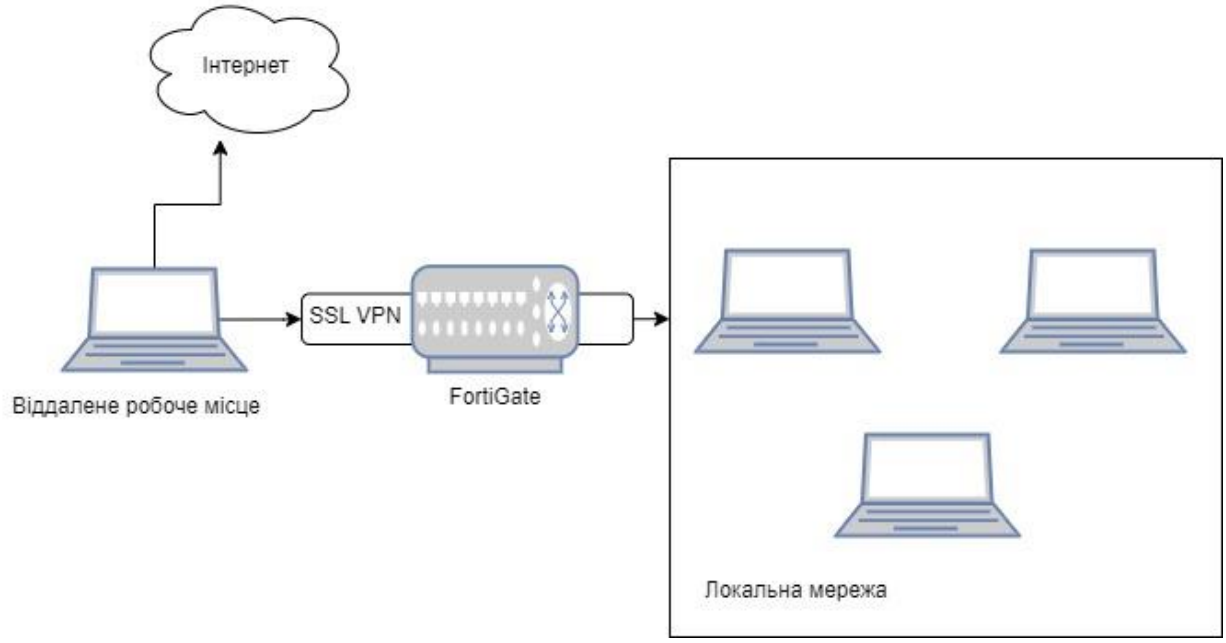


Рисунок 4.6 – Приклад підключення для SSL VPN

Інтерфейс WAN – це інтерфейс, підключений до провайдера. В ході налаштування обрано статичний режим. В подальшій експлуатації також можливо використовувати режим DHCP або PPPoE. Підключення SSL VPN встановлюється через інтерфейс WAN.

Налаштування інтерфейсу і адреси брандмауера.

```
config system interface
    edit "wan1"
        set vdom "root"
        set ip 172.20.120.123 255.255.255.0
    next
end
```

Налаштування внутрішнього інтерфейсу і захищеної підмережі, а потім підключення інтерфейсу port1 до внутрішньої мережі.

```
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.1.99 255.255.255.0
    next
end
config firewall address
    edit "192.168.1.0"
        set subnet 192.168.1.0 255.255.255.0
    next
end
```

Налаштування користувача та групи користувачів.

```
config user local
    edit "bbiliavets"
        set type password
        set passwd your-password
    next
end
config user group
    edit "ra-admin"
        set member "bbiliavets"
    next
end
```

Налаштування веб-порталу SSL VPN.

```
config vpn ssl web portal
    edit "my-split-tunnel-portal"
        set tunnel-mode enable
        set split-tunneling  enable
        set split-tunneling-routing-address "192.168.1.0"
        set ip-pools "SSLVPN_TUNNEL"
    next
end
```

Налаштування параметрів SSL VPN.

```
config vpn ssl settings
    set servercert "Fortinet_Factory"
    set tunnel-ip-pools "SSLVPN_TUNNEL"
    set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6"
    set source-interface "wan1"
    set source-address "all"
    set source-address6 "all"
    set default-portal "full-access"
    config authentication-rule
        edit 1
            set groups "ra-admin"
            set portal "my-split-tunnel-portal"
        next
    next
end
```

Налаштуємо ще одну політику брандмауера SSL VPN, щоб дозволити віддаленому користувачеві отримати доступ до внутрішньої мережі. Трафік перекидається від внутрішнього до віддаленого клієнта.

```
config firewall policy
    edit 1
        set name "sslvpn split tunnel access"
        set srcintf "ssl.root"
        set dstintf "port1"
        set srcaddr "SSLVPN_TUNNEL"
        set dstaddr "192.168.1.0"
        set groups "ra-admin"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

4.5 Порівняльний аналіз на базі двох протоколів безпеки

Головною відмінністю між SSL VPN та IPSec VPN є те, що IPSec будує захищене з'єднання між віддаленою локальною мережею та клієнтським робочим місцем дозволяючи отримати повний доступ до віддаленої мережі так, наче клієнтське робоче місце безпосередньо підключене до неї та надає всі доступні ресурси мережі. SSL VPN же для побудови захищеного з'єднання використовує браузер клієнтського робочого місця, завдяки чому надається доступ тільки до веб-ресурсів віддаленої локальної мережі [22, 23]. Враховуючи сучасні тенденції, більшість систем є веб-орієнтованими та надають доступ до своїх ресурсів за допомогою браузера, що полегшує взаємодію користувача з системою та не вимагає додаткових зусиль з боку користувача. У випадку поєднання SSL VPN з SAML авторизацією, зникає необхідність запам'ятовування безлічі облікових даних віддалених ресурсів, до яких надається доступ шляхом використання параметрів єдиного входу. Також, на відміну від IPSec, SSL VPN здійснює безпечне підключення тільки до веб додатків, що забезпечує додатковий рівень захисту віддаленої мережі та не дозволяє отримувати доступ до інших ресурсів, які не є веб орієнтованими та не потрібні користувачу.

Для проведення практичного порівняння початкове підключення користувачів було налаштовано за допомогою технології IPSec VPN. Впродовж 10 днів було зафіксовано подані заявки для відновлення паролів до віддалених робочих місць, які може змінювати лише адміністратор безпеки компанії, на відміну від доменного паролю, який користувач має можливість змінювати самостійно (рисунок 4.7).

Кількість заявок про втрату паролю становила 53 з 500 підключених користувачів. В результаті реалізації SS VPN технології SAML, яка отримує дані про користувачів з Active Directory, тобто авторизація користувачів відбувається через доменне ім’я без використання додаткових облікових записів, зафіксована кількість заявок – 18. Отримані дані зведено до таблиці 4.1.

Таблиця 4.1 – Порівняння показники технологій IPSec VPN та SSL VPN

Технологія	Кількість заявок	Відсоткове відношення %
IPSec VPN	53	10,6
SSL VPN	18	3,6

Проаналізувавши отримані дані, отримаємо результат у вигляді економії часу адміністратора на виконання заявок майже у 3 рази, рисунок 4.7.

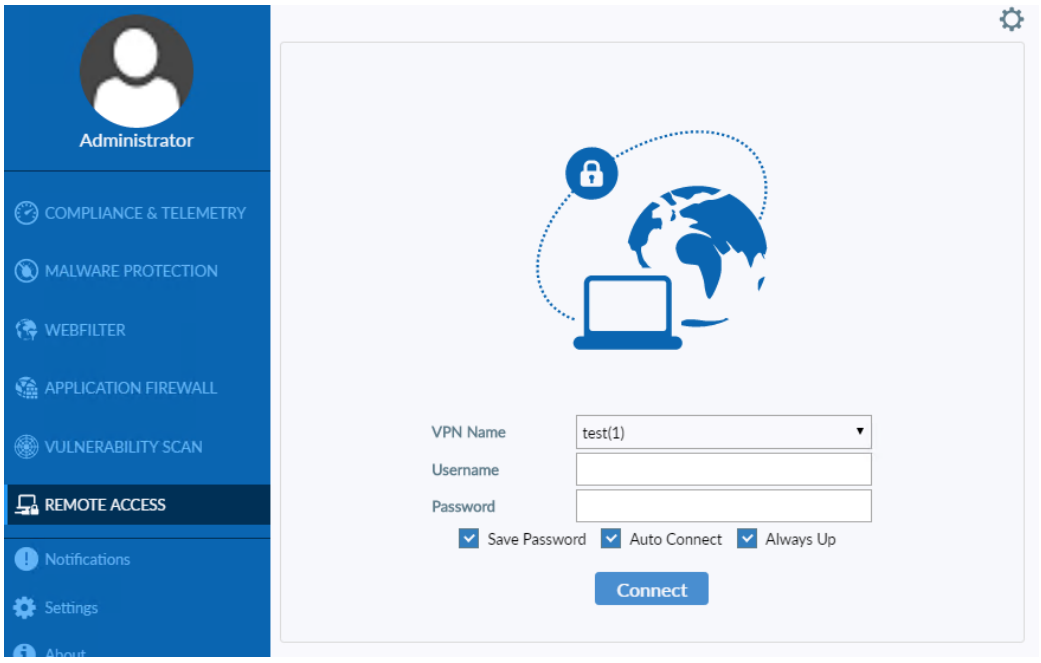


Рисунок 4.7 – Віддалене підключення за допомогою FortiClent

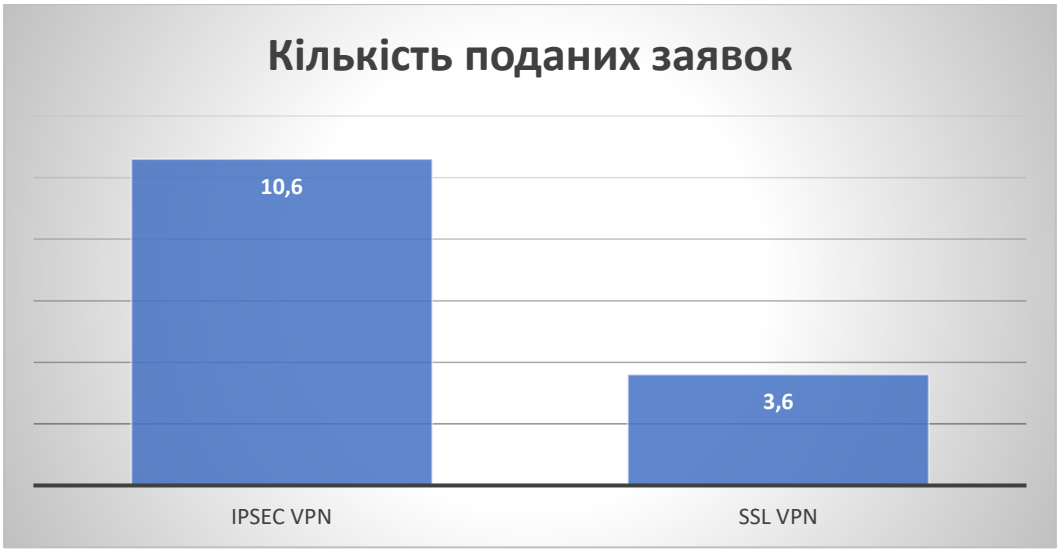


Рисунок 4.8 – Діаграма відсоткового співвідношення

Висновки до розділу 4

Проведено порівняльний аналіз віддаленого підключення з використанням технології IPSec VPN та SSL VPN, з можливістю реалізації незалежного серверу авторизації. В ході вивчення питання, було виявлено, що налаштування SAML серверу можливе лише на базі протоколу SSL, відповідно до технічної документації та доступних функцій. Під час перевірки було виявлено можливість реалізації єдиного входу за доменним обліковим записом, що економить час для додаткового адміністрування, а також зберігання лог-файлів з діями користувачів в одному місці. Перевіривши на практиці віддалене підключення, за двома протоколами, отримано аналітику з якої встановлено, що підключення через SSL VPN створювало додаткове використання людського ресурсу.

Отже, підсумовуючи вище зазначене, потрібно наголосити на наявності значної кількості протоколів безпеки. У зв’язку з цим до вибору необхідного протоколу безпеки потрібно підходити індивідуально, тобто обирати найбільш зручний спосіб для кожного конкретного підприємства, врахувавши особливості побудови локальної мережі та задачі, які покладаються на неї.

ВИСНОВКИ

В магістерській роботі вирішено наукову задачу розробки методу безпечного віддаленого підключення користувачів до робочих місць. Проаналізовано технології досягнення безпечного підключення та реалізація двоетапної аутентифікації осіб до внутрішньої мережі. Дана реалізація дає можливість підвищити продуктивність працівників завдяки доступу до файлів і системних ресурсів. Зазначена технологія значно полегшує роботу для інших працівників компанії, які працюють в межах офісу або віддалено.

Проведено аналіз принципів надання віддаленого доступу за допомогою VPN. Показано, що VPN було розроблено щоб дозволити персоналу безпечно отримувати доступ до програм організації.

Визначено, що безпека передачі даних покращується завдяки інкапсуляції даних у зашифрованому тунелі, який захищає їх від перехоплення. Це особливо важливо для віддалених працівників, які часто підключаються через незахищену інфраструктуру, наприклад використовуючи загальнодоступний Wi-Fi.

Метод віддаленої роботи, запроваджений багатьма організаціями, має суттєві переваги, але супроводжується виникненням нових ризиків які можуть зруйнувати всю компанію. Описано умови для забезпечення захищеної корпоративної мережі під час впровадження системи віддаленої роботи, керуючись протоколами підключення віддаленого доступу.

Реалізація дослідження була виконана на обладнанні сімейства FortiNet.

В ході виконання роботи отримано наступні результати:

1 Здійснено аналіз наявних проколів VPN;
2 Обґрунтувати вибір технології та мережевого обладнання для побудови VPN тунелю;
3 Реалізовано віддалене підключення SSL VPN з сервером авторизації;
4 Дістали подальшого розвитку методика підвищення захисту каналу VPN з можливістю реалізації багатофакторної аутентифікації по типу сканування відбитків пальців чи розпізнавання обличчя;

5 Дістали подальшого розвитку методика забезпечення сприятливих умов перенесення інфраструктури в хмарні середовища по типу Azure.

6 Налаштовано двофакторну аутентифікацію для підвищення захисту каналу передачі даних.

7 Розроблена модель перейшла з тестового режиму в постійну експлуатацію підприємства.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1 Горбатий І. В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи / І. В. Горбатий, А. П. Бондарєв. – Львів : Львівська політехніка, 2016. - 336 с.

2 Черевко О. В. Джерела виникнення загроз інформаційній безпеці банківських установ / О. В. Черевко, В. М. Андрієнко, І. Ю. Напора // Вісник Черкаського університету. Серія: Економічні науки. – 2016. – № 3. – С. 120- 127.

3 Запечніков С.В. Основи побудови віртуальних приватних мереж: Навчальний посібник для вузів / С.В. Запечніков, Н.Г. Мілославская, А.Н. Толстой: 2003. 249 с.

4 Бобало Ю.Я. Інформаційна безпека: навчальний посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарєв, С.С. Войтусік, А.Я. Горпенюк, О.А. Нємкова, І.М. Журавель, Б.М. Березюк, Є.І. Яковенко, В.І. Отенко, І.Я. Тишик. Львів: Видавництво Львівської політехніки, 2019. – 580 с.

5 Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. К.: КУБГ, 2019. 218 с

6 Захист інформації в комп'ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". Харків : НТУ "ХПІ", 2014. 251 с.

7 SSL VPN vs IPSec VPN – Pros & Cons Of Both VPNs [Електронний ресурс] – https://www.limevpn.com/ssl-vpn-vs-ipsec-vpn-pros-cons-of-both-vpns/

8 Technologies for Optimized Remote Access [Електронний ресурс] – https://www.remoteaccessworks.com/Remote-Access-Technologies.asp

9 Two Factor Authentication Implementation Methods and Bypasses [Електронний ресурс] – https://www.geeksforgeeks.org/two-factor-authenticationimplementation-methods-and-bypasses/

10 Cisco Networking Academy Connecting Networks v6 Companion Guide. US, 2017. 512.

11 Дослідження аутентифікації SAML [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/45872317_Web_single_sign-on_authentication_using_SAML.

12 Оліфер В.Г. Комп'ютерні мережі. Принципи, технології, протоколи / В.Г. Оліфер, Н.А. Оліфер. — 4-е изд. — СПб.:Питер, 2010 - 668 с.

13 Смірнов О.А. Інформаційна безпека в комп’ютерних мережах: навчальний посібник /О.А. Смірнов, С.А. Конопліцька-Слободенюк, К.О. Смірнов, Т.В. Буравченко, Л.І. Смірнова [та інш.]. – Кропивницький : Центральноукраїнський національний університет, 2020. - 295 с.

14 Ільченко М.Ю. Телекомунікаційні системи /М.Ю. Ільченко, С.О. Кравчук. – Київ: Наукова думка, 2017. - 305 с.

15 Мирошниченко В. Використання сучасних інформаційних технологій. Формування мультимедійної компетентності / В. Мирошниченко. - Центр навчальної літератури, 2017. - 296 с.

16 Аудит інформаційної безпеки інформаційних систем та інформаційно-телекомунікаційних систем [Електронний ресурс]. – Режим доступу: http://www.uss.gov.ua/audit-of-information-security.

17 iWar: A new threat, its convenience and our increasing vulnerability [Електронний ресурс]. – Режим доступу: http://www.nato.int/docu/review/2007/issue4/english/analysis2.html .

18 SAML 2.0: A Clear and Concise Reference Paperback – 2021. – 187 p.

19 Open Source Security Testing Methodology Manual (OSSTMM) [Електронний ресурс]. – Режим доступу: https://www.isecom.org/OSSTMM.3.pdf.

20 A Framework for IP Based Virtual Private Networks / B. Gleeson, A. Lin, J. Heinanen. [Електронний ресурс]. — http://www.ietf.org/rfc/rfc2764.txt

21 Настанова з налаштування обладнання сімейства FortiNet [Електронний ресурс]. – Режим доступу: https://docs.fortinet.com/document/fortigate/7.0.2/administration-guide/989067/configuring-saml-sso-in-the-gui.

22 Бойко Ю.М. Концептуальні особливості реалізації безпровідних

сенсорних мереж / Ю.М. Бойко, В.М. Локазюк, В.В. Мішан // Вісник Хмельницького національного університету. – 2010. – № 2. – С. 94–97.

23 Boiko J.M. Solutions improve signal processing in digital satellite communication channels /J. M. Boiko, A. I. Eromenko //20th International Conference on Microwaves, Radar and Wireless Communications. MIKON 2014. June, Gdansk – Poland. - 2014. – PP. 126-129.

24 А.В. Соколов, В.Ф.Шаньгін. Захист інформації в розподілених корпоративних мережах і системах. -М.: ДМК Пресс, 2002. -656с. 11.

25 Інформаційні системи в економіці: навч. посібник / під ред.Г.А.Тіторенко-2-е ізд., перераб. і доп. -М .: Юніті-Дана, 2008

26 Платонов В.В. Програмно-апаратні засоби забезпечення інформаційної безпеки обчислювальних мереж: навч. посібник для студ. вищ. навч. закладів / В.В. Платонов. -М. : Видавничий центр «Академія», 2006. -240 с.

27 Фортенбері Т. Проектування віртуальних приватних мереж в середовищі Windows2000: пер.с англ. / Т. Фортенбері. М.: Іздательскійдом "Вільямс", 2002. 320 с.23.Зіма В.М. Безпека глобальних мережевих технологій /

28 Запечніков С.В. Основи побудови віртуальних приватних мереж: Навчальний посібник для вузів / С.В.Запечніков, Н.Г.Мілославская, А.Н.Толстой. М.: Гаряча лінія-Телеком, 2003. 249 с

29 Порівняння технологій IPsec та SSL в технології VPN [Електронний ресурс] Режим доступу: http://www.sovit.net/articles/technologies/ipsec_vs_ssl/

30 . SSL VPN -крок вперед в технології VPN мереж [Електронний ресурс] Режим доступу: https://www.anti-malware.ru/node/449

31 Аудит інформаційної безпеки інформаційних систем та інформаційно-телекомунікаційних систем [Електронний ресурс]. – Режим доступу: http://www.uss.gov.ua/audit-of-information-security

32 iWar: A new threat, its convenience and our increasing vulnerability [Електронний ресурс]. – Режим доступу: http://www.nato.int/docu/review/2007/issue4/english/analysis2.html

33 Open Source Security Testing Methodology Manual (OSSTMM)

[Електронний ресурс]. – Режим доступу: http://www.isecom.org/research/osstmm.html.

34 Мережі VPN та проблеми їх захисту [Електронний ресурс] – Режим доступу до ресурсу: https://studfile.net/preview/8099727/.

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій

Метод налаштування конфігурації VPN з віддаленим доступом

Спеціальність 172 «Телекомунікації та радіотехніка»

Богдана БІЛЯВЕЦЬ
Студент групи ТРм-21-1

Керівник:
професор кафедри телекомунікаційних та інформаційних систем
доктор технічних наук, професор
Юлій БОЙКО

МЕТА, ПРЕДМЕТ, ОБ'ЄКТ ДОСЛІДЖЕННЯ

МЕТА

полягає у створені VPN тунелю для підключення віддалених користувачів до корпоративної мережі використовуючи технологію SAML з налаштування доменної аутентифікації.

ПРЕДМЕТ ДОСЛІДЖЕННЯ

метод безпечного віддаленого підключення користувачів.

ОБ'ЄКТ ДОСЛІДЖЕННЯ

процес отримання доступу користувачам до мережі з використанням незалежного серверу аутентифікації SAML.

НАУКОВА НОВИЗНА, ПОДАЛЬШИЙ РОЗВИТОК ДОСЛІДЖЕННЯ

Факультет інформаційних технологій

Наукова новизна Вперше:

- запропонована методика побудови VPN тунелю з використанням технології SAML в державній організації з використанням двофакторної аутентифікації, яка передбачає використання мобільного токену чи брелка з періодичною генерацією унікального коду.

Дістали подальшого розвитку:

- методика підвищення захисту каналу VPN з можливістю реалізації багатофакторної аутентифікації по типу сканування відбитків пальців чи розпізнавання обличчя;
- методика забезпечення сприятливих умов перенесення інфраструктури в хмарні середовища по типу Azure.

Основні види VPN

- **Персональні VPN;**
- **VPN із віддаленим доступом;**
- **Мобільні VPN;**
- **VPN типу «мережа-мережа»**

Основні протоколи VPN

- **IPSec**
- **-SSL**
- **OpenVPN**

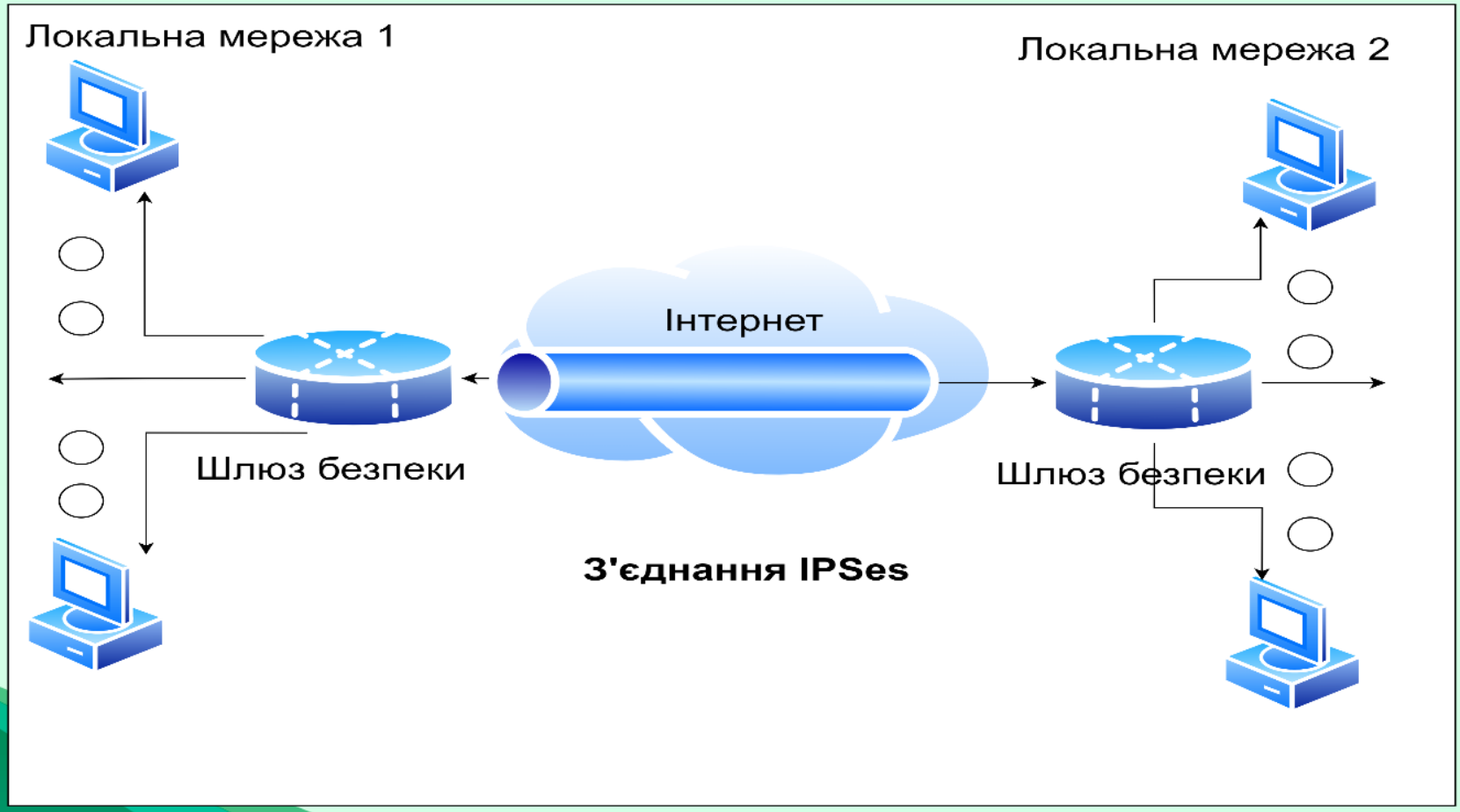


Рисунок 1 – Приклад з’єднання на базі IPsec

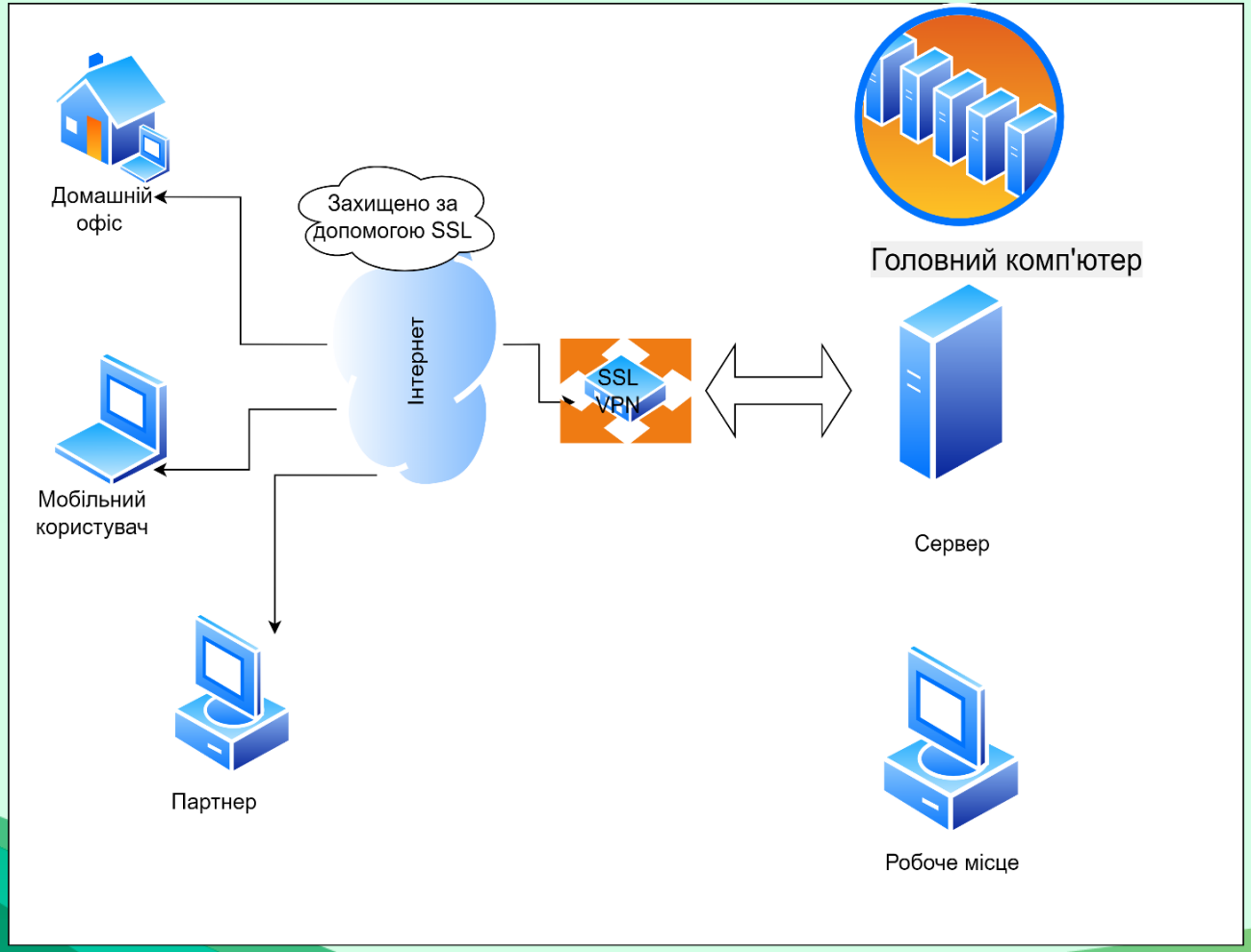


Рисунок 2 – Підключення з використанням SSL

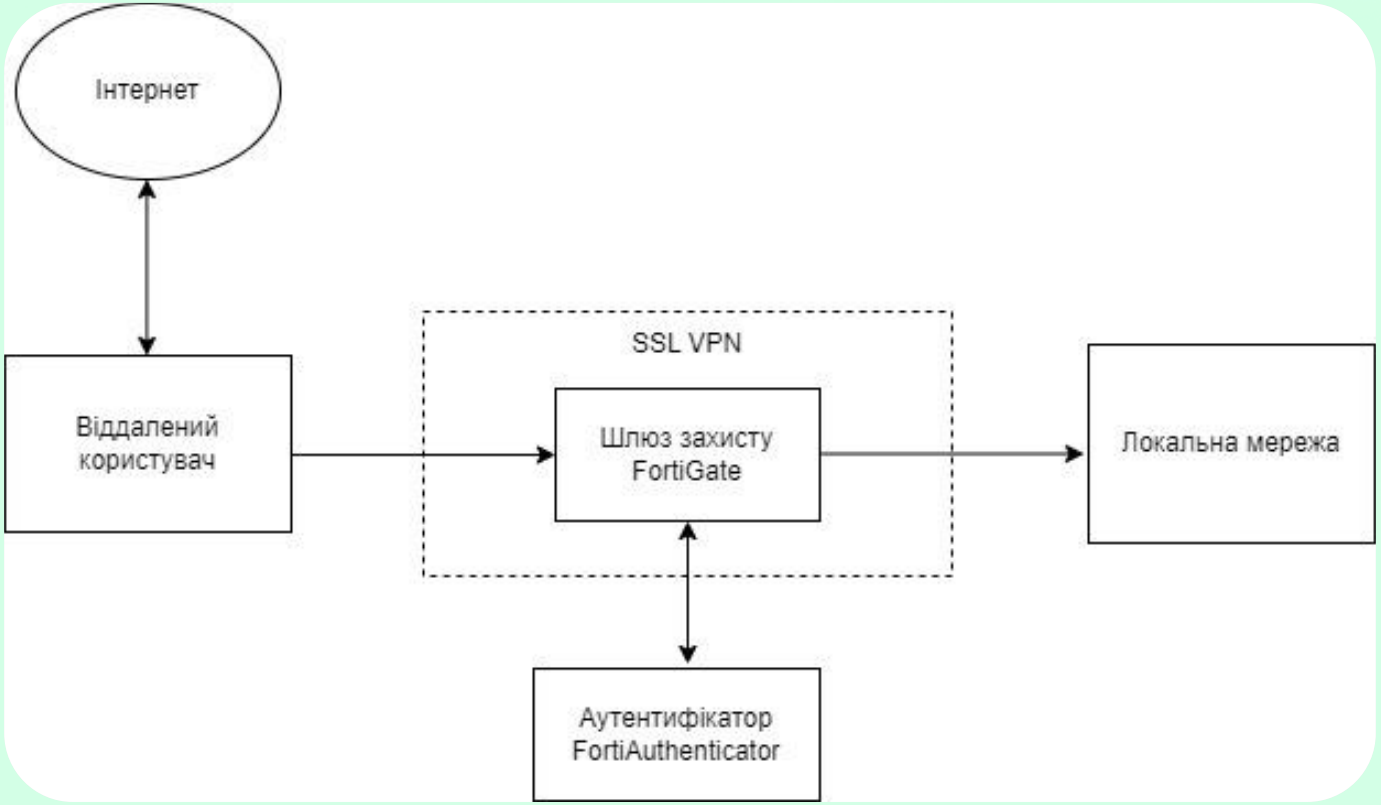


Рисунок 3 – Структурна схема VPN

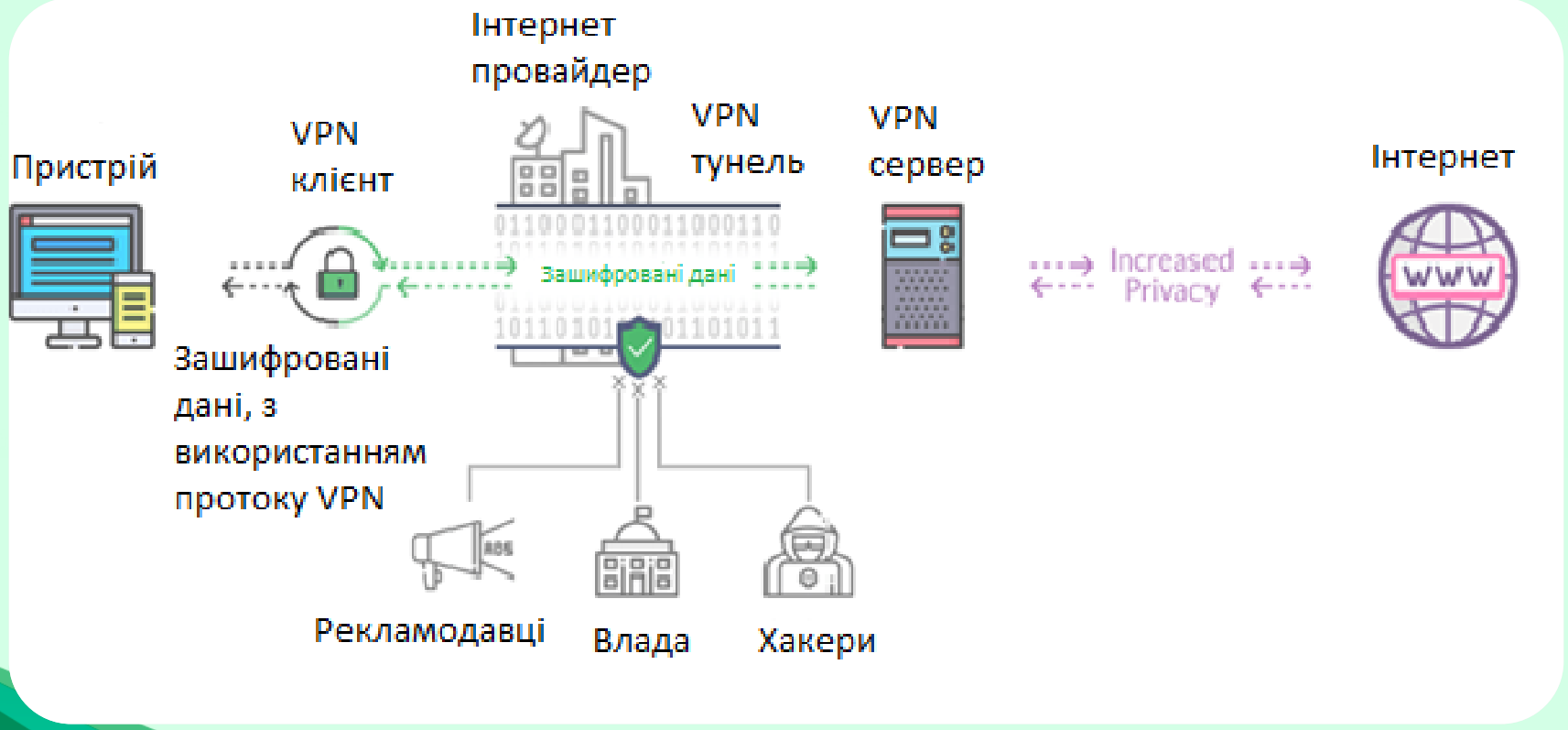


Рисунок 4 – Схема шифруванняVPN

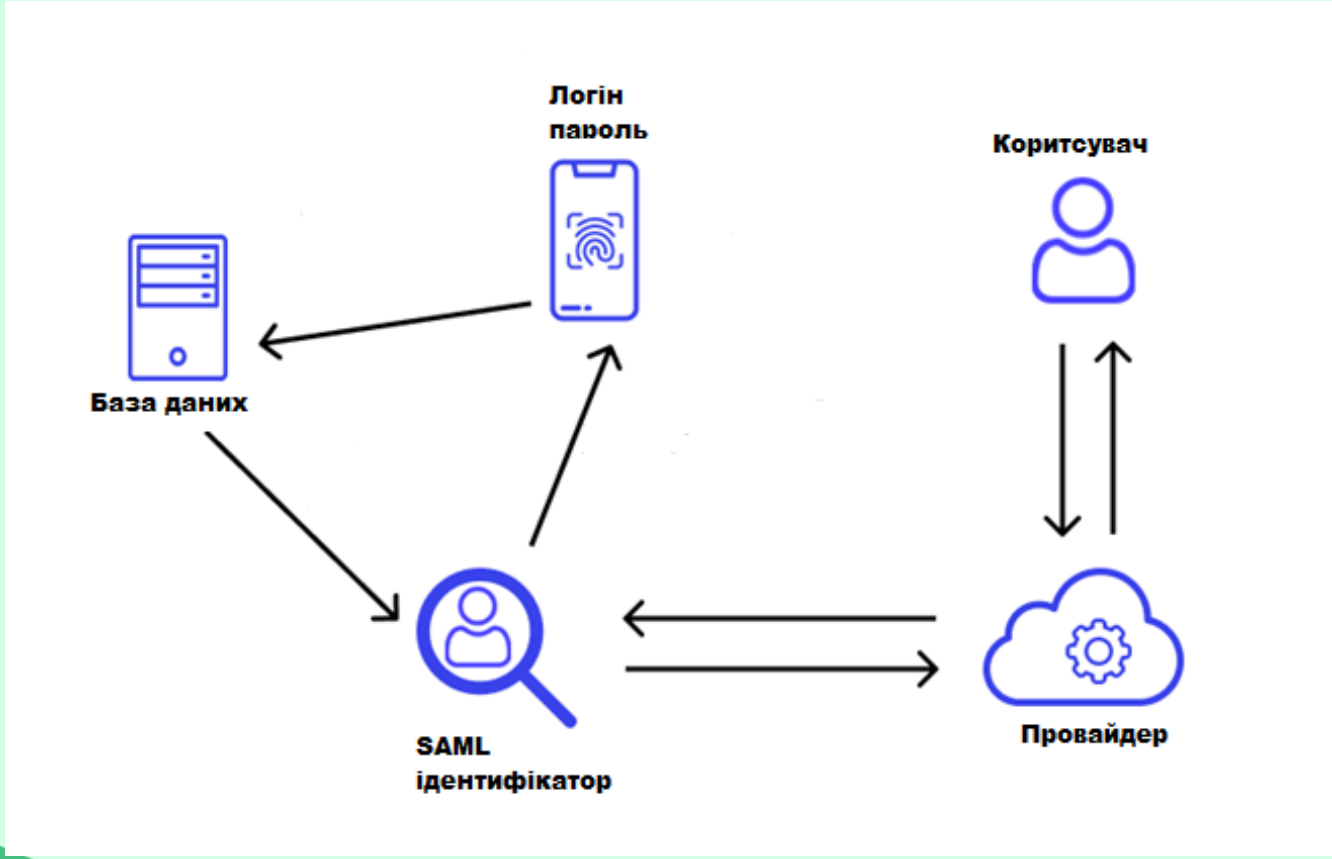


Рисунок 5 – Принцип роботи технології SAML

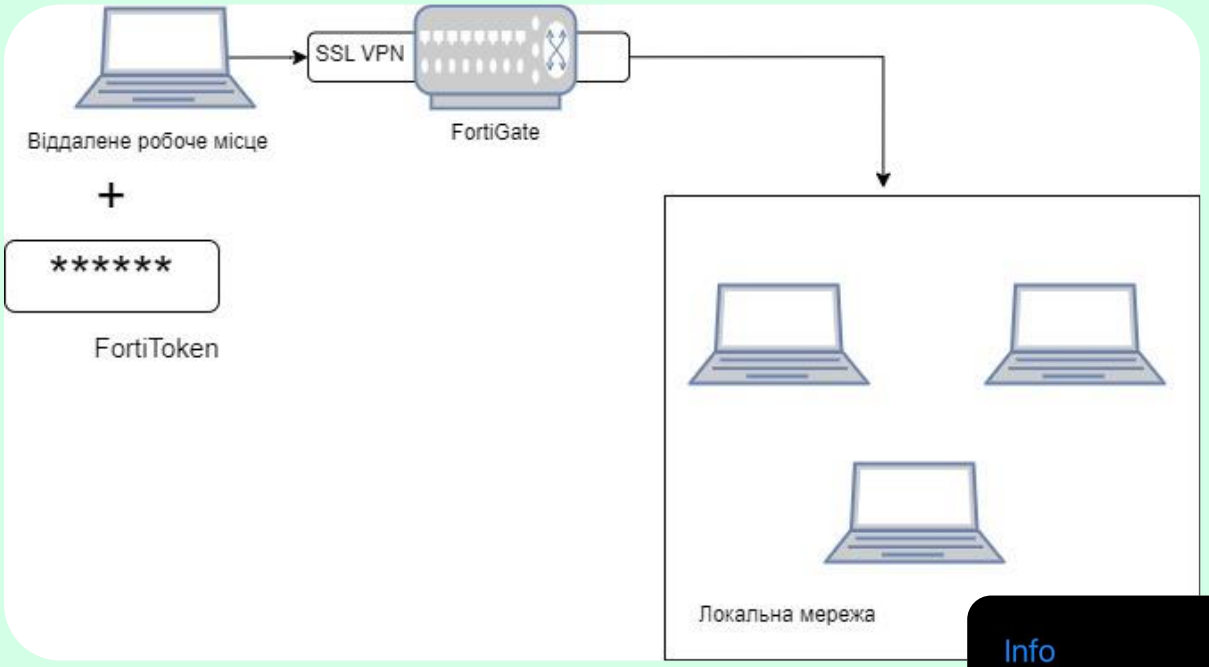


Рисунок 6 – Підключення з використанням мобільного токену

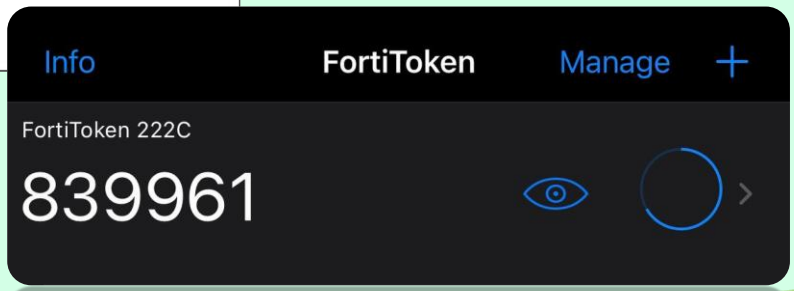


Рисунок 7 – Персональний токен для входу в мережу

АНАЛІЗ ДОСЛІДЖЕННЯ

Факультет інформаційних технологій

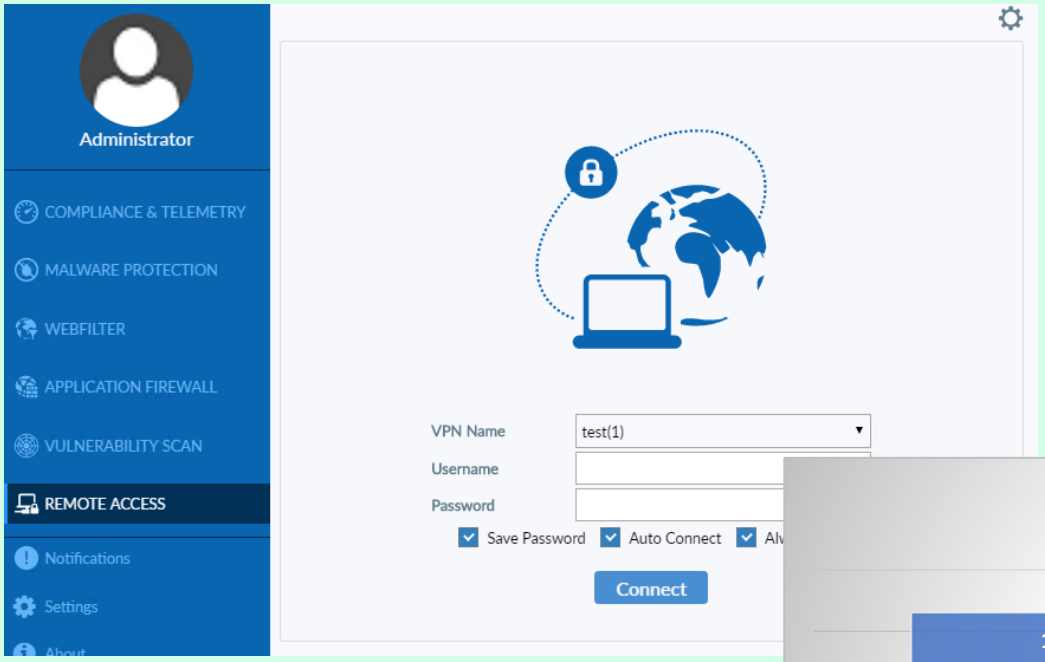


Рисунок 8 – Віддалене підключення за допомогою FortiClient

Рисунок 9 – Діаграма відсоткового співвідношення

ВИСНОВКИ

1 Здійснено аналіз наявних проколів VPN;

2 Обґрунтувати вибір технології та мережевого обладнання для побудови VPN тунелю;

3 Реалізовано віддалене підключення SSL VPN з сервером авторизації;

4 Дістали подальшого розвитку методика підвищення захисту каналу VPN з можливістю реалізації багатофакторної аутентифікації по типу сканування відбитків пальців чи розпізнавання обличчя;

5 Дістали подальшого розвитку методика забезпечення сприятливих умов перенесення інфраструктури в хмарні середовища по типу Azure.

6 Налаштовано двофакторну аутентифікацію для підвищення захисту каналу передачі даних.

7 Розроблена модель перейшла з тестового режиму в постійну експлуатацію підприємства.

Довідка: ВОТТП 1/11/22

Видання: Вимірювальна та обчислювальна техніка у технологічних процесах

Категорія фаховості видання: фахове видання України, у якому можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора наук, кандидата наук та ступеня доктора філософії, категорії «Б» (наказ МОН №1643 від 28.12.2019). Напрям – технічні науки за спеціальностями – 121, 122, 123, 125, 126, 151, 152, 172.

Назва статті: SAML: ДЕФІНІЦІЯ ТА ПРИНЦИП РОБОТИ ЧЕРЕЗ VPN ТУНЕЛЬ У ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ МЕРЕЖАХ

Автори: ЮЛІЙ БОЙКО (Хмельницький національний університет), БОГДАНА БІЛЯВЕЦЬ (Хмельницький національний університет)
Номер, у який прийнято статтю: №4, до друку рекомендовано буде до 30 грудня 2022 року.

01.12.2022

https://doi.org/
УДК 621.396.969.1

ЮЛІЙ БОЙКО
Хмельницький національний університет
https://orcid.org/0000-0003-0603-7827
e-mail: boiko_julius@ukr.net
БОГДАНА БІЛЯВЕЦЬ
Хмельницький національний університет
https://orcid.org/0000-0002-4330-3605
e-mail: dana.bilyavets@gmail.com

SAML: ДЕФІНІЦІЯ ТА ПРИНЦИП РОБОТИ ЧЕРЕЗ VPN ТУНЕЛЬ У ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ МЕРЕЖАХ

У статті піднімаються питання віддаленого підключення користувачів до робочих місць. Аналізуються технології досягнення безпечного підключення та реалізація двоетапної аутентифікації зареєстрованих осіб внутрішньої мережі, що дає можливість підвищити продуктивність працівників завдяки доступу до файлів і системних ресурсів. Розглянута технологія полегшує роботу з іншими колегами, які працюють в межах офісу або в інших місцях. Організації мають можливість найняти найкращих спеціалістів із будь-якої частини світу, що забезпечує покращену якість продукції без додаткових накладних витрат. Проведено аналіз принципів надання віддаленого доступу за допомогою VPN. Показано, що VPN було розроблено щоб дозволити філіям безпечно отримувати доступ до програм організації. Таким чином, він забезпечує зашифроване та безпечне підключення до мережі. Визначено особливості налаштування віддаленого доступу, що має важливе значення для віддалених працівників, оскільки воно дає їм прямий доступ до ресурсів організації, не перебуваючи в офісі. Користувачі можуть підключатися до мережі з різних областей у всьому світі за допомогою своїх пристроїв. Встановлено, що за наявності віддаленого доступу персонал може отримати доступ до віддаленого пристрою без фізичної присутності. Визначено, що безпека покращується завдяки інкапсуляції даних у зашифрованому тунелі, який захищає їх від перехоплення. Це особливо важливо для віддалених працівників, які часто підключаються через незахищену інфраструктуру, наприклад публічного Wi-Fi у готелі, аеропорту чи вдома. Доведено, що метод віддаленої роботи, запроваджений багатьма організаціями, має важливі переваги але супроводжується виникненням нових ризиків які можуть зруйнувати всю компанію. Описано вимоги до забезпечення належної корпоративної безпеки під час впровадження системи віддаленої роботи, керуючись протоколами підключення віддаленого доступу. З метою підтвердження припущення було проведено статистичний аналіз і порівняння показників обслуговування користувачів при використанні технологій IPSec VPN та SSL VPN.

Ключові слова: система VPN, SAML, двофакторна аутентифікація, віддалені робочі місця

JULIY BOIKO, BOHDANA BILIAVETS
Khmelnytskyi National University

SAML: DEFINITION AND PRINCIPLES OF OPERATION THROUGH A VPN TUNNEL IN SECURE INFORMATION NETWORKS

The article raises issues of remote connection users to workplaces. The technologies for achieving a secure connection and the implementation of two-step authentication of registered persons of the internal network are analyzed, which allows increasing the productivity of workers through access to files and system resources. The considered technology makes it easier to work with other colleagues working in the office or in other places. Organizations can hire the best talent from anywhere in the world, delivering improved product quality without additional overhead. An analysis of the principles providing remote access using VPN has been carried out. VPN is shown to have been designed to allow branch offices to securely access an organization's programs. Thus, it provides an encrypted and secure connection to the network. The features of setting up remote access are determined, which is important for remote workers, since it gives them direct access to the organization's resources without being in the office. Users can connect to the network from different areas around the world using their devices. It has been determined that when setting up remote access, IT staff can access a remote device without being physically present. It is determined that security is improved by encapsulating the data in an encrypted tunnel that protects it from interception. This is especially important for remote workers, who often connect through insecure infrastructure, such as public Wi-Fi at a hotel, airport, or home. The method of remote work adopted by several organizations has been proven to have important benefits, but comes with new risks that can destroy the entire company. The requirements for ensuring proper corporate security when implementing a remote work system are described, guided by remote access connection protocols. It has been proven that secure data exchange is important in the conditions of modern information technologies, when real tasks are performed with the requirement of high efficiency. It is shown that due to the emergence of predictable threats to stay at the enterprise, it becomes necessary to study the secure connection and authorization of users to their workplaces.

Keywords: VPN system, SAML, two-factor authentication, remote workplaces

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Зловмисники вправно проникають у корпоративні та домашні інформаційні мережі з метою викрадення конфіденційної інформації. Метою є крадіжка особистих персональних та корпоративних даних,

таких як облікові дані з відповідним доступом, номера банківських карт, вилучення цінних документів з можливістю шантажування та викупу. Тому налаштування безпечної інформаційної мережі потребує відповідального ставлення до захисту особистих даних від кіберзлочинців.

Захищеність мережі асоціюється з розгортанням великої корпоративної мережі, до якої належать тисячі робочих місць. Однак, навіть кілька пристроїв підключених до домашнього роутера також вважаються мережею. Забезпечення їх безпеки не менш важливе, оскільки вони також містять конфіденційні файли.

Безпечний обмін даними є важливим з використанням сучасних інформаційних технологій, в ході виконання реальних завдань, коли вони потребують вирішення на високому рівні, що є можливе лише із врахуванням вимог до захисту інформації і даних. Аналізуючи наявність прогнозованих загроз захисту конфіденційної інформації, виникає необхідність дослідження безпечного підключення та авторизації користувачів до своїх робочих місць.

Метою статті є порівняльний аналіз і експериментальна перевірка віддаленого керування сервером авторизації на основі мови розмітки декларації безпеки SAML (Мови розмітки твердження безпеки).

Аналіз досліджень та публікацій

Організації все частіше починають використовувати незалежні джерела аутентифікації для програм та веб-порталів. Одним з дослідників SAML аутентифікації є викладач Луїсвільського університету Джеймс Левіс, який дослідив та підтвердив чимало її переваг, однією з яких є зменшення кількості звернень до служби технічної підтримки, що й досі актуально для функціонування багатьох організацій [1].

Виклад основного матеріалу

Структура інформаційних мереж в офісах приватних і державних компаній дозволяє працівникам отримати доступ до принтерів, підключитися до IT-ресурсів, передавати дані тощо. Загалом такий доступ є безпечним та захищає фірми і компанії від неоднозначних веб-сайтів. Організація корпоративної офісної мережі ґрунтується на принципі, коли всі працівники в офісі використовують локальну мережу. Це забезпечує їх ресурсами, а компанію – безпекою. Віддалені працівники не можуть увійти в систему, так як для цього потрібен віддалений доступ до робочого місця, що підводить до реалізації такого порталу.

Концепція VPN (віртуальної приватної мережі) віддаленого доступу означає, що віддалені співробітники можуть увійти в мережу конкретного офісу з будь-якого місця — з дому, у дорозі чи в будь-якому громадському місці, де є доступ до Інтернету. За таких умов вони отримають доступ до всіх ресурсів необхідної компанії, а корпоративні дані компанії, як і раніше, будуть захищені, навіть у випадку використання публічного Wi-Fi [2].

VPN використовують різні протоколи. Старіші протоколи, такі як PPP (протокол точка-точка) і PPTP(тунельний протокол типу точка-точка), вважаються менш безпечними. Розглянемо деякі типи протоколів безпеки.

PPTP був найпершим із протоколів безпеки та вперше випущений у Windows 95. Він вважається швидкісний, проте характеризується низьким рівнем шифрування.

IP Sec (безпека Інтернет-протоколу) — це популярний протокол, який захищає дані в транспортному або тунельному режимі.

Протокол тунелювання рівня 2 (L2TP)/IPSec. L2TP — це протокол VPN, який сам по собі не шифрує дані. У зв'язку з цим, він поєднується з шифруванням IPSec. Однією з його головних переваг є доступність для більшості пристроїв і операційних систем, які реалізовують високий рівень безпеки, але це може призвести до уповільнення з'єднань. В цьому випадку використовується процес подвійної інкапсуляції.

Secure Sockets Layer (SSL) і Transport Layer Security (TLS). SSL (рівень захищених сокетів) був протоколом шифрування VPN, який найчастіше використовувався до 2015 року. Подальшим його розвитком став протокол TLS(протокол захисту транспортного рівня) для шифрування даних, котрі передаються на сервер SSL VPN.

SSL — криптографічний протокол, який передбачає забезпечення більш безпечного зв'язку. По суті, це спосіб передачі інформації в Інтернеті, який характеризується прозорим шифрування даних. Протокол широко використовувався для обміну миттєвими повідомленнями та передачі голосу через IP (VoIP) у таких додатках, як електронна пошта, Інтернет-факс та інші. Згодом на підставі протоколу SSL 3.0 було розроблено та прийнято стандарт RFC (запити коментарів), який отримав назву TLS [3, 4].

TLS – протокол захисту транспортного рівня, який як і його попередник SSL – криптографічний протокол, що забезпечує захищену передачу даних між вузлами в мережі Інтернет. SSL і TLS використовують для шифрування трафік в роботі з сайтами. Коли дані передаються за протоколом HTTPS (захищений протокол передачі гіпертексту), трафік шифрується сертифікатом який використовує той чи інший ресурс.

SSL-сертифікат — містить інформацію про власника, а також відкритий ключ, який використовується для створення захищеного каналу зв'язку. Організації та фізичні особи отримують підтвердження того, що сайт чи інший ресурс дійсно підтримують такий сертифікат і не відносяться до підробленого ресурсу. Сертифікати отримують або купують у авторизованих довірених центрах сертифікації.

Все це застосовується для обмеження несанкціонованого доступу особам, які потрапляють в канал зв'язку між адресатами з метою заволодіння інформацією або з метою її змінити, рис. 1.

Рис. 1. Схема асиметричного шифрування документу при передачі файлів

У випадку асиметричного шифрування використовуються два різні ключі: один для шифрування (відкритий), інший для розшифровування (закритий).

Аутентифікація є невід'ємною частиною кожного з'єднання TLS. Розглянемо найпростіший процес аутентифікації між двома користувачами, рис. 2.

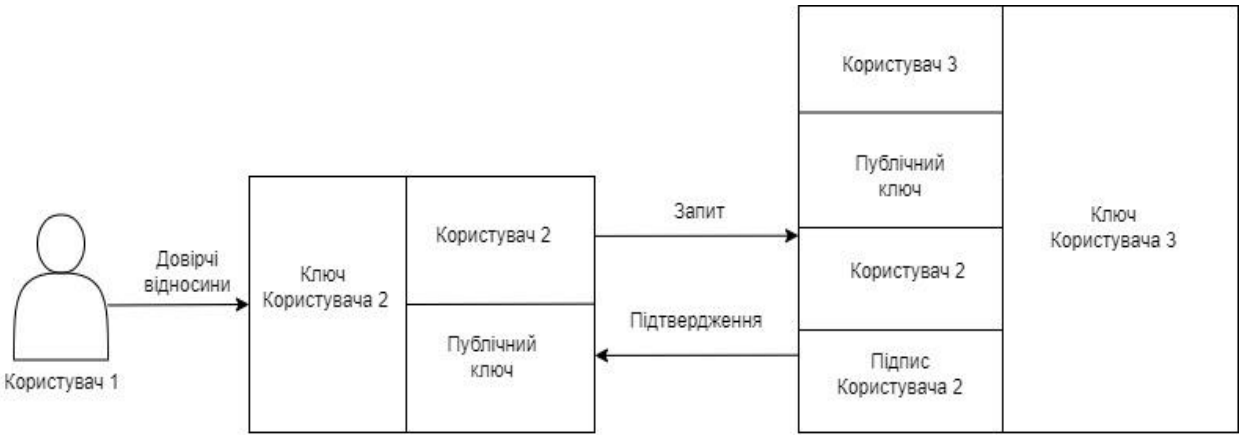


Рис. 2. Схема побудови довірчих відносин між користувачами

Обидва користувачі системи генерують власні відкриті та закриті ключі. Вони обмінюються відкритими ключами. Один з них генерує повідомлення, шифрує його своїм закритим ключем та відправляє іншому. Користувач 2 використовує отриманий від Користувача 1 ключ для розшифрування повідомлення і таким чином перевіряє справжність отриманого повідомлення.

Очевидно, що ця схема побудована на довірі між користувачами мережі. Передбачається, що обмін відкритими ключами відбувся, наприклад, під час особистої зустрічі. Таким чином, перший користувач впевнений, що отримав ключ саме від другого, тобто між ними побудовані довірчі відносини.

Нехай тепер Користувач 1 отримує повідомлення від Користувача 3, з яким він не знайомий, але який стверджує, що має довірчі відносини із Користувачем 2. Щоб це довести, Користувач 3 заздалегідь попросив підписати власний відкритий ключ закритим ключем Користувача 2 і прикріпив цей підпис до повідомлення Користувачу 1. У цьому разі Користувач 1 спочатку повинен перевірити підпис Користувача 2 на ключі Користувача 3, та переконатись у дійсності налагоджених довірчих відносин.

Описана вище схема є технологію створення «ланцюжка довіри».

У протоколі TLS дані ланцюга довіри засновані на сертифікаті автентичності, який надається спеціальними органами які називаються центрами сертифікації (CA). Центри сертифікації проводять

ISSN 2219-9365

перевірку та у випадку, якщо виданий сертифікат скомпрометований, виконується процедура відкликання сертифікату [5-7]. З виданих сертифікатів складається вже розглянутий ланцюжок довіри. Ключовим елементом підтвердження ступеня довіри є сертифікат Root CA certificate (головний центр сертифікації), який підписаний авторизованим центром сертифікації, довіра до якого незаперечна. В загальному вигляді організація ланцюжка довіри виглядає так, як представлено на рис. 3.

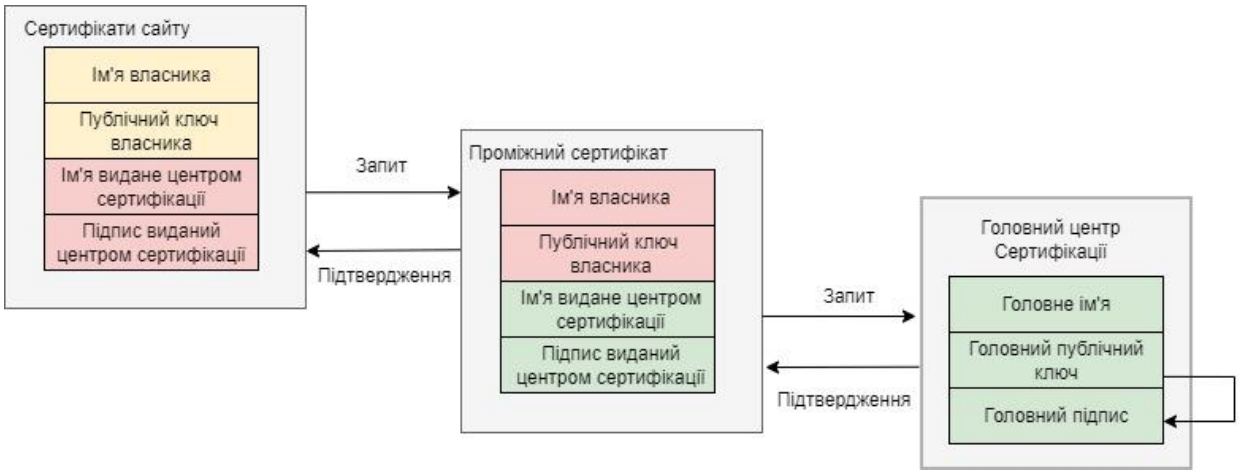


Рис. 3. Схема обміну сертифікатами для налаштування довірчих відносин

Розглянемо віддалений доступ VPN в умовах вже наявного підключення. Найбільш логічним і популярним способом передачі інформації є загальнодоступний Інтернет, тому VPN передає інформацію використовуючи його ресурси. Однак в цьому випадку, доступ до всієї інформації, яка передається через Інтернет і не є захищеною може отримати зловмисник. Наприклад, будь-хто у локальній мережі Wi-Fi може організувати підслуховування або доступ до інформації. Дієвим способом запобігання таких протиправних дій є застосування ефективних методів шифрування [7-9].

Процедура шифрування використовується на сервері доступу. Таким чином, будь-який контент, який передається через корпоративну мережу Wi-Fi піддається шифруванню. Така особливість забезпечує захист інформації та дозволяє доступ до читання даних лише в межах корпорації, окреслених мережевих меж офісу. Для інших осіб, непов'язаних з структурою офісних мереж доступ до інформації буде закрито.

Доступ до інформації можна отримати на основі серверу доступу. Сервер доступу володіє ключем для розшифрування зашифрованої інформацій [8]. В цьому випадку, будь-яка інформація, яка далі надсилається назад на певний пристрій із сервера доступу, також піддається шифруванню, а отже, все, що надходить через таке з'єднання в будь-якому напрямку неможливо прочитати іншим стороннім особам.

Завдяки параметрам на сервері персонал може використовувати доступе їм програмне забезпечення. Сервер доступу можна налаштувати для роботи в режимі первинного-вторинного відновлення після відмови для розгортання локальної мережі, щоб підтримувати високу доступність яка необхідна для цілодобової роботи без вихідних.

SAML, як вже будо зазначено вище, скорочення від Security Assertion Markup Language (Мова розмітки декларації безпеки). ЇЇ ключова роль у забезпеченні мережевої безпеки полягає в тому, що її застосування дозволяє отримати доступ до декількох додатків на основі використання одного набору облікових даних для авторизації. Така схема працює за допомогою обміну автентифікаційною інформацією у певному форматі між учасниками, зокрема між системою управління доступом та веб-додатком.

SAML представляє собою відкритий стандарт обміну даними автентифікації, що базується на мові XML (розширювана мова розмітки). Веб-програми використовують SAML, щоб передавати автентифікаційні дані між сторонами процесу: а саме між системою керування доступом та провайдером послуг. Для прикладу розглянемо використання в якості провайдера послуг FortiClient.

SAML з'явився в індустрії високих технологій для спрощення процесу автентифікації, коли користувачам потрібно було отримати доступ до кількох незалежних веб-додатків у різних доменах. До появи SAML, технологія єдиного входу цілком виконувала поставлені задачі, проте базувалася на файлах cookies, які були актуальними лише в межах одного домену.

При використанні SAML технологія входу досягається за рахунок узгодження процесу автентифікації із системою управління доступом. Веб-програми можуть використовувати SAML, через систему керування доступом. Такий метод автентифікації означає, що користувачам більше не потрібно запам'ятовувати численні комбінації логінів та паролів. Більш того, він має безперечну перевагу для

провайдера, у вигляді підвищення рівня безпеки платформи, переважно завдяки тому, що усунуто необхідність зберігання паролів та процесів їх відновлення.

Концепція SAML працює шляхом обміну інформацією користувача (логіни, стан автентифікації, ідентифікатори та інші дані) між системою управління доступом та постачальником послуг. В результаті, це спрощує і забезпечує безпеку процесу автентифікації, так як в такому випадку користувачеві необхідно увійти в систему тільки один раз з використанням одного набору даних для входу. Таким чином, коли користувач надає запит для отримання доступу до сайту, SAML передає аутентифікаційні дані постачальника послуг, які в результаті дозволяють доступ користувачеві [10].

Процес двоетапної автентифікації починається в той момент, коли користувач намагається увійти в додаток, службу або систему, доки йому не буде надано доступ для використання. Алгоритм аутентифікації виглядає наступним чином:

- Крок 1. Користувач відкриває програму або веб-сайт, до якої він хоче отримати доступ. Здійснює введення облікових даних для входу.
- Крок 2. Далі він зазначає свої дані, якими звичайно є ім'я користувача та пароль. Додаток або веб-сайт підтверджує деталі та розпізнає, що було введено правильні дані початкової автентифікації на сервері авторизації в нашому випадку за протоколом SAML.
- Крок 3. Якщо програма або веб-сайт не використовує облікові дані для входу з паролем, буде згенеровано ключ безпеки для користувача. Ключ буде оброблено інструментом автентифікації, а сервер перевірить початковий запит.
- Крок 4: Користувачеві пропонується надіслати другий фактор аутентифікації. Очевидно, що таким фактором буде підтвердження прав власності. Наприклад, додаток або веб-сайт надішле унікальний код на мобільний пристрій користувача.
- Крок 5: Користувач вводить код у програму або на веб-сайт, і якщо код буде схвалено, він буде автентифікований і отримає доступ до системи.

Модель налаштування SAML для SSL VPN представлена на рис. 4.

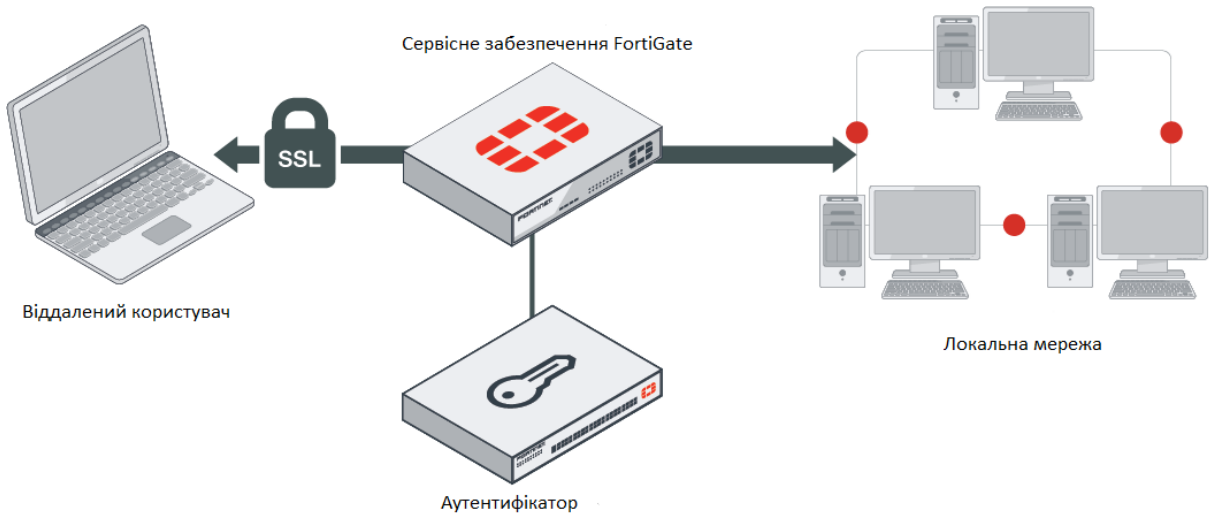


Рис. 4. Модель мережевого підключення обладнання сімейства FortiGate

Розглянемо процес мережевого підключення в наступній послідовності:

1. Адміністратор або кінцевий користувач налаштовує з'єднання SSL VPN із увімкненим SAML SSO.
2. FortiClient підключається до FortiGate.
3. FortiGate повертає посилання перенаправлення на сторінку авторизації SAML IdP.
4. FortiClient відображає сторінку авторизації IdP у вбудованому вікні браузера.
5. Кінцевий користувач вводить свої облікові дані у вікні для входу.
6. Після успішної спроби входу FortiClient встановлює тунель до FortiGate.

У такій схемі FortiGate налаштовується як SP (постачальник послуг), а FortiAuthenticator — як IdP (постачальник ідентифікаційної інформації).

Загалом, безпечне віддалене підключення можна реалізувати великим набором способів, використовуючи протоколи, а також групові чи індивідуальні політики безпеки [6, 11]. Потрібно наголосити, що особливість несанкціонованого входу зумовлюється і тим, що внаслідок витоку інформації

можливий вільний доступ до облікових даних, і в цьому випадку такі дані можуть бути використані без відома особи власника та зокрема в злочинних цілях.

Головною відмінністю між SSL VPN та IPSec VPN є те, що IPSec будує захищене з'єднання між віддаленою локальною мережею та клієнтським робочим місцем дозволяючи отримати повний доступ до віддаленої мережі так, наче клієнтське робоче місце безпосередньо підключене до неї та надає всі доступні ресурси мережі. SSL VPN же для побудови захищеного з'єднання використовує браузер клієнтського робочого місця, завдяки чому надається доступ тільки до веб-ресурсів віддаленої локальної мережі [12, 13]. Враховуючи сучасні тенденції, більшість систем є веб-орієнтованими та надають доступ до своїх ресурсів за допомогою браузера, що полегшує взаємодію користувача з системою та не вимагає додаткових зусиль з боку користувача. У випадку поєднання SSL VPN з SAML авторизацією, зникає необхідність запам'ятовування безлічі облікових даних віддалених ресурсів, до яких надається доступ шляхом використання параметрів єдиного входу. Також, на відміну від IPSec, SSL VPN здійснює безпечне підключення тільки до веб додатків, що забезпечує додатковий рівень захисту віддаленої мережі та не дозволяє отримувати доступ до інших ресурсів, які не є веб орієнтованими та не потрібні користувачу.

Налаштуємо FortiGate SP як користувача SAML. Ми повинні налаштувати віддалений сертифікат IdP від FortiAuthenticator на FortiGate [11]:

```
config user saml
edit "saml-user"
set cert "Fortinet_Factory"
set entity-id "http://172.17.61.59:11443/remote/saml/metadata/"
set single-sign-on-url "https://172.17.61.59:11443/remote/saml/login/"
set single-logout-url "https://172.17.61.59:11443/remote/saml/logout/"
set idp-entity-id "http://172.17.61.118:443/saml-idp/101087/metadata/"
set idp-single-sign-on-url "https://172.17.61.118:443/saml-idp/101087/login/"
set idp-single-logout-url "https://172.17.61.118:443/saml-idp/101087/logout/"
set idp-cert "REMOTE_Cert_4"
next
end
```

Додаємо користувача SAML до групи користувачів:

```
config user group
edit "saml_grp"
set member "saml-user"
next
end
```

Встановлюємо групу SAML у налаштуваннях SSL VPN:

```
config vpn ssl settings
config authentication-rule
edit 1
set groups "saml-group"
set portal "full-access"
next
next
end.
```

Для проведення практичного порівняння початкове підключення користувачів було налаштовано за допомогою технології IPSec VPN. Впродовж 10 днів було зафіксовано подані заявки для відновлення паролів до віддалених робочих місць, які може змінювати лише адміністратор безпеки компанії, на відміну від доменного паролю, який користувач має можливість змінювати самостійно (рис. 5).

Кількість заявок про втрату паролю становила 53 з 500 підключених користувачів. В результаті реалізації SS VPN технології SAML, яка отримує дані про користувачів з Active Directory, тобто авторизація користувачів відбувається через доменне ім’я без використання додаткових облікових записів, зафіксована кількість заявок – 18. Отримані дані зведено до табл. 1

Таблиця 1

Порівняння показники технологій IPSec VPN та SSL VPN

Технологія	Кількість заявок	Відсоткове відношення %
IPSec VPN	53	10,6
SSL VPN	18	3,6

Проаналізувавши отримані дані, отримаємо результат у вигляді економії часу адміністратора на виконання заявок майже у 3 рази, рис. 6.

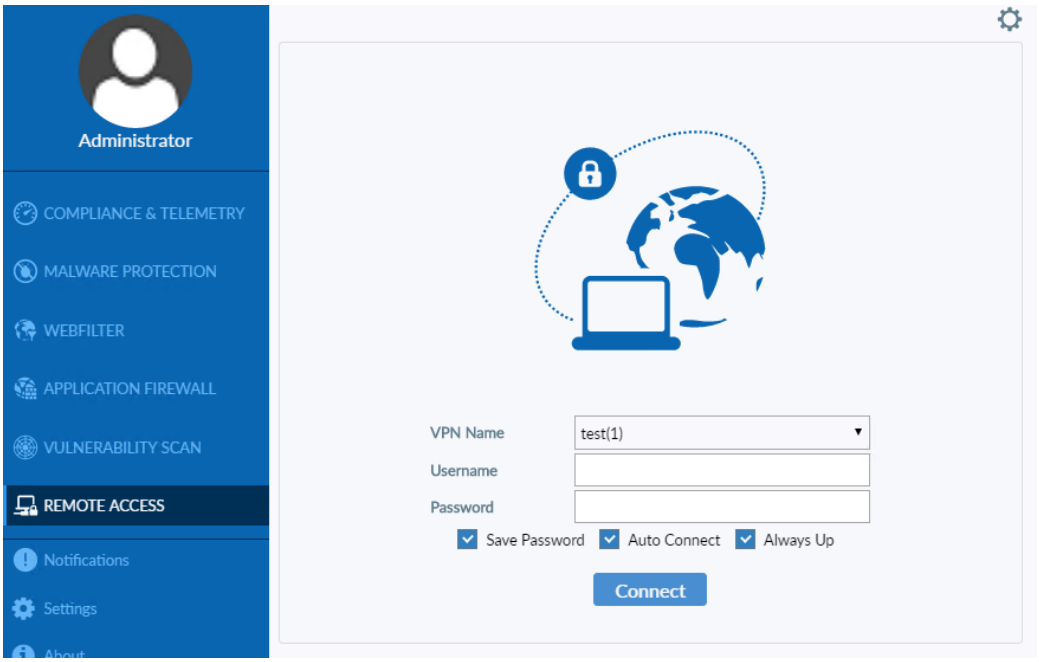


Рис. 5. Віддалене підключення за допомогою FortiClent

Рис. 6. Діаграма відсоткового співвідношення

Висновки з даного дослідження і перспективи подальшого розвитку у даному напрямі

Проведено порівняльний аналіз віддаленого підключення з використанням технології IPSec VPN та SSL VPN, з можливістю реалізації незалежного серверу авторизації. В ході вивчення питання, було виявлено, що налаштування SAML серверу можливе лише на базі протоколу SSL, відповідно до технічної документації та доступних функцій. Під час перевірки було виявлено можливість реалізації єдиного входу за доменним обліковим записом, що економить час для додаткового адміністрування, а також зберігання лог-файлів з діями користувачів в одному місці. Перевіривши на практиці віддалене підключення, за двома протоколами, отримано аналітику з якої встановлено, що підключення через SSL VPN створювало додаткове використання людського ресурсу.

Отже, підсумовуючи, потрібно наголосити на наявності існуючої значної кількості протоколів безпеки. У зв'язку з цим до вибору необхідного протоколу безпеки потрібно підходити індивідуально, тобто обирати найбільш зручний спосіб для кожного конкретного підприємства, врахувавши особливості

побудови локальної мережі та задачі, які покладаються на неї. Перспективами подальших досліджень вважаємо використання хмарних рішень з можливістю розташування незалежних серверів авторизації, VPN-тунелю та зберігання домен-контролерів з даними про користувачів мережі.

Література

1. Дослідження аутентифікації SAML [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/45872317_Web_single_sign-on_authentication_using_SAML (date of appeal: 5.11.2022).

2. Горбатий І. В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи / І. В. Горбатий, А. П. Бондарєв. – Львів : Львівська політехніка, 2016. - 336 с.

3. Смірнов О.А. Інформаційна безпека в комп'ютерних мережах: навчальний посібник /О.А. Смірнов, С.А. Конопліцька-Слободенюк, К.О. Смірнов, Т.В. Буравченко, Л.І. Смірнова [та інш.]. – Кропивницький : Центральноукраїнський національний університет, 2020. - 295 с.

4. Ільченко М.Ю. Телекомунікаційні системи /М.Ю. Ільченко, С.О. Кравчук. – Київ: Наукова думка, 2017. - 305 с.

5. Мирошниченко В. Використання сучасних інформаційних технологій. Формування мультимедійної компетентності / В. Мирошниченко. - Центр навчальної літератури, 2017. - 296 с.

6. Аудит інформаційної безпеки інформаційних систем та інформаційно-телекомунікаційних систем [Електронний ресурс]. – Режим доступу: http://www.uss.gov.ua/audit-of-information-security (date of appeal: 5.11.2022).

7. iWar: A new threat, its convenience and our increasing vulnerability [Електронний ресурс]. – Режим доступу: http://www.nato.int/docu/review/2007/issue4/english/analysis2.html (date of appeal: 5.11.2022).

8. SAML 2.0: A Clear and Concise Reference Paperback – 2021. – 187 p.

9. Open Source Security Testing Methodology Manual (OSSTMM) [Електронний ресурс]. – Режим доступу: https://www.isecom.org/OSSTMM.3.pdf (date of appeal: 5.11.2022).

10. A Framework for IP Based Virtual Private Networks / B. Gleeson, A. Lin, J. Heinanen. [Електронний ресурс]. — http://www.ietf.org/rfc/rfc2764.txt (date of appeal: 5.11.2022)

11. Настанова з налаштування обладнання сімейства FortiNet [Електронний ресурс]. – Режим доступу: https://docs.fortinet.com/document/fortigate/7.0.2/administration-guide/989067/configuring-saml-sso-in-the-gui (date of appeal: 5.11.2022).

12. Бойко Ю.М. Концептуальні особливості реалізації безпровідних сенсорних мереж / Ю.М. Бойко, В.М. Локазюк, В.В. Мішан // Вісник Хмельницького національного університету. – 2010. – № 2. – С. 94–97.

13. Boiko J.M. Solutions improve signal processing in digital satellite communication channels /J. M. Boiko, A. I. Eromenko //20th International Conference on Microwaves, Radar and Wireless Communications. MIKON 2014. June, Gdansk – Poland. - 2014. – PP. 126-129.

References

1. Research on SAML authentication [Electronic resource]. – Access mode: https://www.researchgate.net/publication/45872317_Web_single_sign-on_authentication_using_SAML (date of appeal: 5.11.2022).

2. Horbatyi I. V. Telekomunikatsiini systemy ta merezhi. Pryntsypy funktsionuvannia, tekhnolohii ta protokoly / I. V. Horbatyi, A. P. Bondariev. – Lviv : Lvivska politekhnika, 2016. - 336 s.

3. Smirnov O.A. Informatsiina bezpeka v kompiuternykh merezhakh: navchalnyi posibnyk /O.A. Smirnov, S.A. Konoplitska-Slobodeniuk, K.O. Smirnov, T.V. Buravchenko, L.I. Smirnova [ta insh.]. – Kropyvnytskyi : Tsentralnoukrainskyi natsionalnyi universytet, 2020. - 295 s.

4. Ilchenko M.Iu. Telekomunikatsiini systemy /M.Iu. Ilchenko, S.O. Kravchuk. – Kyiv: Naukova dumka, 2017. - 305 s.

5. Myroshnychenko V. Vykorystannia suchasnykh informatsiinykh tekhnolohii. Formuvannia multymediinoi kompetentnosti / V. Myroshnychenko. - Tsentr navchalnoi literatury, 2017. - 296 s.

6. Audyt informatsiinoi bezpeky informatsiinykh system ta informatsiino-telekomunikatsiinykh system [Electronic resource]. – Access mode: http://www.uss.gov.ua/audit-of-information-security (date of appeal: 5.11.2022).

7. iWar: A new threat, its convenience and our increasing vulnerability [Electronic resource]. – Access mode: http://www.nato.int/docu/review/2007/issue4/english/analysis2.html (date of appeal: 5.11.2022).

8. SAML 2.0: A Clear and Concise Reference Paperback - 2021. - 187 p.

9. Open-Source Security Testing Methodology Manual (OSSTMM) [Electronic resource]. – Access mode: https://www.isecom.org/OSSTMM.3.pdf (date of appeal: 5.11.2022).

10. A Framework for IP Based Virtual Private Networks / B. Gleeson, A. Lin, J. Heinanen. [Electronic resource]. — http://www.ietf.org/rfc/rfc2764.txt (date of appeal: 5.11.2022)

11. Fortinet family equipment configuration manual [Electronic resource]. – Access mode: https://docs.fortinet.com/document/fortigate/7.0.2/administration-guide/989067/configuring-saml-sso-in-the-gui (date of appeal: 5.11.2022).

12. Boiko J. M. Kontseptualni osoblyvosti realizatsii bezprovidnykh sensornykh merezh /J.M. Boiko, V.M. Lokaziuk,

V.V. Mishan // Herald of Khmelnytskyi national university. – 2010. – № 2. – S. 94–97.

13. Boiko J.M. Solutions improve signal processing in digital satellite communication channels /J. M. Boiko, A. I. Eromenko //20th International Conference on Microwaves, Radar and Wireless Communications. MIKON 2014. June, Gdansk – Poland. - 2014. – PP. 126-129.

Рецензія/Peer review : _.__.2022 Надрукована/Printed :__._.2022

Завідувачу кафедри телекомунікацій,
медійних і інтелектуальних технологій_ХНУ
Підченку Сергію Костянтиновичу
здобувача вищої освіти, студента Білявець
Богдани Сергіївни, факультету інформаційних
технологій, 2-го курсу, група ТРм-20-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї магістерської дипломної роботи виконаної за темою «Метод налаштування конфігурації VPN з віддаленим доступом» для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

28.11.2022 _____

дата підпис

Fri Dec 02 16:55:30 EET 2022, Стецюк Віктор Іванович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 2.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 13%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 108894 Название: Метод налаштування конфігурації VPN з віддаленим доступом Добавлено в БД: 2022-12-02 Авторы: Білявець Богдана Сергіївна Руководители: Бойко Юлій Миколайович Консультанты: Опоненты: Мартинюк Валерій Володимирович	Символы	Лексемы	Символы	Лексемы
	74780	1137	2360 (3%)	33 (3%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

Ім'я користувача:
Kafedra TMIT KhNU

ID перевірки:
1013152285

Дата перевірки:
02.12.2022 12:47:02 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
02.12.2022 12:48:38 EET

ID користувача:
100005657

Назва документа: Білявець_ТРм-21

Кількість сторінок: 82 Кількість слів: 12661 Кількість символів: 96371 Розмір файлу: 1.86 MB ID файлу: 1012908912

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

5.7%
Схожість

Найбільша схожість: 2.06% з джерелом з Бібліотеки (ID файлу: 1009458598)

3.27% Джерела з Інтернету 94 ..... Сторінка 84

2.74% Джерела з Бібліотеки 120 ..... Сторінка 85

0% Цитат

Не знайдено жодних цитат

Посилання 1 ..... Сторінка 85

0%
Вилучень

Немає вилучених джерел

Рецензія

опонента на дипломну роботу виконану за темою «Метод налаштування конфігурації VPN з віддаленим доступом»

студента групи ТР$_м$-21-1 Богдани БІЛЯВЕЦЬ

Спеціальність: 172 «Телекомунікації та радіотехніка».

Освітньо-професійна програма: 172 «Телекомунікації та радіотехніка».

Актуальність теми.

Магістерська робота студента Богдани Білявець присвячена дослідженню реалізації методів безпечних віддалених підключень з використанням VPN тунелю з двофакторною автентифікацією. Розвиток інтернет індустрії відкриває великі можливості і збільшує ступінь практичного використання питань, які виконані у магістерській роботі, тому тема роботи є актуальною.

Відповідність виконаної роботи виданому завданню.

Тема роботи відповідає наказу ректора Хмельницького національного університету від 01 липня 2022 р. № 83 та виконана у відповідності до календарного плану та виданого завдання.

Найважливіші теоретичні та практичні результати роботи.

Метою кваліфікаційної роботи є створення VPN тунелю для підключення віддалених користувачів до корпоративної мережі використовуючи технологію SAML з налаштування доменної аутентифікації.

Позитивні сторони.

1. Зміст магістерської роботи відповідає завданню. Під час виконання роботи Богдана Білявець, показала гарний рівень знань і ступінь підготовленості спеціаліста до майбутньої роботи з фаху.

2. Поставлені в магістерській роботі задачі з реалізації віддаленого підключення користувачів з використанням технології VPN на базі SAML аутентифікації, виконані в повному обсязі.

3. Технічні питання викладені успішно і якісно.

4. Текст викладений грамотно, ясно, послідовно. Широкий обсяг використання науково-технічної літератури.

Недоліки

1. В роботі доцільно було б розглянути більш детально способи проходження трафіку, та впливу на нього технології SAML.

Відзначене зауваження не впливає на загальну позитивну оцінку магістерської роботи.

Загальний висновок.

Робота є завершеною, самостійно виконаною, має наукову складову та може бути допущеною до захисту на засіданні екзаменаційної комісії. Магістерська робота заслуговує на оцінку «*відмінно*».

Опонент: к.т.н., доцент кафедри фізики та електротехніки  **Олександр ЄРЬОМЕНКО**

Відгук на дипломну кваліфікаційну магістерську роботу виконану за темою
«Метод налаштування конфігурації VPN з віддаленим доступом»
ст. гр. ТР$_м$-21-1 Білявець Б.С.

В дипломній роботі ст. Білявець Б.С. вирішено наукову задачу розробки методики віддаленого підключення користувачів до робочих місць.

Стрімкий розвиток як корпоративних так і приватних інформаційних мереж на сучасному етапі розвитку телекомунікацій, пов'язаний із поширеними викликами щодо несанкціонованого викрадення конфіденційної інформації користувачів. Ризику піддають як особисті дані користувачів, карткові рахунки, облікові дані так і конфіденційні документи установ, цінні папери тощо. В багатьох випадках мета таких дій зловмисників спрямована на неприпустимі дії у вигляді шантажу і викупу. В цих умовах розробка методик захисту інформації, побудова безпечних (захищених) телекомунікаційних мереж є як ніколи актуальною і всеосяжною для функціонування всієї інформаційної спільноти.

В роботі ст. Білявець Б.С. проаналізовано технології досягнення безпечного підключення та реалізація двоетапної аутентифікації осіб до внутрішньої мережі. Запропонована реалізація дає можливість підвищити продуктивність працівників завдяки доступу до файлів і системних ресурсів.

Пояснювальна записка містить огляд сучасних підходів до налаштування VPN для віддаленого підключення до корпоративної мереж. Звертає на себе увагу здійснений в магістерський роботі синтез структурної схеми VPN тунелю та вибір елементної бази, описані концепції налаштування SAML серверу та з’ясовані принципи підвищення захищеності з’єднання. Автор роботи приділив окрему увагу методам надійного шифрування мереж. Зокрема, розроблені питання пов’язані із формуванням алгоритмів шифрування VPN на основі SSL. Дослідницький розділ охопив питання реалізації віддаленого підключення користувачів з використання технології SAML. В роботі представлена технологія двоетапної аутентифікації з використанням токену, налаштування VPN на базі IPSec і SSL. Ефективність запропонованих рішень перевірена проведеним порівняльним аналізом на базі двох протоколів безпеки.

Безпечний обмін даними є важливим з використанням сучасних інформаційних технологій, в ході виконання реальних завдань, коли вони потребують вирішення на високому рівні, що є можливе лише із врахуванням вимог до захисту інформації і даних. Аналізуючи наявність прогнозованих загроз захисту конфіденційної інформації, виникає необхідність дослідження безпечного підключення та авторизації користувачів до своїх робочих місць. Саме ці актуальні завдання захисту конфіденційної інформації вирішені в магістерський роботі ст. Білявець Б.С.

Результати отримані в дипломній роботі апробовано статтею у фаховому рецензованому журналі «Вимірювальна та обчислювальна техніка в технологічних процесах».

В цілому магістерська кваліфікаційна робота виконана на високому науково-технічному рівні, має безперечну актуальність в області сучасних телекомунікацій, інформаційних технологій, технологій захисту інформації, а студентка Білявець Б.С. заслуговує оцінки «***відмінно***».

Професор кафедри ТМІТ  **Юлій БОЙКО**

РІШЕННЯ **КАФЕДРИ ТЕЛЕКОМУНІКАЦІЙ, МЕДІЙНИХ ТА ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ**

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: **Метод налаштування конфігурації VPN з віддаленим доступом**

Автор: **Білявець Б.С.**

Спеціальність:**172 Телекомунікації та радіотехніка**

Науковий керівник: **д.т.н., професор Бойко Ю.М.**

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	**відповідає**
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	-
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	-
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	-
5	Інше:	-

Підтвердження: Виявленні запозичення не є плагіатом так як розміщенні в розділах, які не описують безпосередньо авторське дослідження (є власні терміни, визначення тощо), складають 5,7% та мають посилання на приведений список літературних джерел

02.12.2022
Дата

Підпис керівника

Підпис завідувача кафедри