Національний університет «Полтавська політехніка імені Юрія Кондратюка»

Навчально-науковий інститут інформаційних технологій і роботехніки

Кафедра автоматики, електроніки та телекомунікацій

Пояснювальна записка

до кваліфікаційної роботи

магістр
(ступінь вищої освіти)

на тему **Розробка захищеної телекомунікаційної мережі організації**

Виконала: студентка 6 курсу, групи 601дТТ

спеціальності 172 «Телекомунікації та
(шифр і назва напряму підготовки, спеціальності)

радіотехніка»

Кравчина Т.В.
(прізвище та ініціали)

Керівник Штомпель М.А.
(прізвище та ініціали)

Рецензент Кислиця С.Г.
(прізвище та ініціали)

м. Полтава – 2024 рік

Національний університет «Полтавська політехніка імені Юрія Кондратюка»

Інститут Навчально-науковий інститут інформаційних технологій і роботехніки

Кафедра Автоматики, електроніки та телекомунікацій

Ступінь вищої освіти Магістр

Спеціальність 172 «Телекомунікації та радіотехніка»

ЗАТВЕРДЖУЮ

Завідувач кафедри автоматики,

електроніки та телекомунікацій

_____ О.В. Шефер

«_04_» _____09_____ 2023р.

ЗАВДАННЯ

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТЦІ

Кравчині Тетяні Вікторівні

1. Тема проекту (роботи): **«Розробка захищеної телекомунікаційної мережі організації»**

керівник роботи Штомпель Микола Анатолійович, д.т.н, професор, затверджена наказом вищого навчального закладу від «04» вересня 2023р. №986.

2. Строк подання студентом проекту (роботи): 09.12.2023р.

3. Вихідні дані до проекту (роботи) 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 розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Літературний огляд та аналіз предметної області. Обґрунтування вибору технології та мережевого обладнання для побудови VPN тунелю. Методи надійного шифрування мереж. Дослідження реалізації віддаленого підключення користувачів з використання технології SAML та порівняльний аналіз розроблених рішень з використанням цієї технології. Висновки.

5. Дата видачі завдання 02.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів магістерської роботи	Термін виконання етапів роботи			Примітка
1	Ознайомлення із завданням. Уточнення ТЗ.	10.09.23-02.10.23		15%	Пл.1
2	Пошук джерел за темою та виконання частини роботи	03.10.23-16.10.23	I	30%	Пл.2
3	Вступ. Літературний огляд та аналіз предметної області	17.10.23-21.10.23		45%	Пл.3
4	Обґрунтування вибору технології та мережевого обладнання для побудови VPN тунелю	03.10.23-17.10.23		60%	Пл.4
5	Методи надійного шифрування мереж	18.10.23-27.10.23	II	70%	Пл.5
6	Дослідження реалізації віддаленого підключення користувачів з використання технології SAML та порівняльний аналіз розроблених рішень з використанням цієї технології	28.10.23-15.11.23		80%	Пл.6
7	Висновки. Презентаційні матеріали за результатами виконання дипломної роботи	16.11.23-08.12.23		90%	Пл.7
8	Оформлення магістерської роботи	09.12.23	III	100%	Пл.8

Магістрант _____ Кравчина
(підпис) (прізвище та ін

Керівник роботи _____ Штомпель
(підпис) (прізвище та іні

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

SAML - Мови розмітки твердження безпеки

ASA -Адаптивний пристрій безпеки

Wi-Fi -Бездротова правдивість відтворення

IPsec -Захищений Інтернет-протокол

SSL -Рівень Захищених Сокетів

PPP -Протокол точка-точка

PPTP -Тунельний протокол типу точка-точка

L2TP -Протокол тунелювання другого рівня

TLS -Протокол захисту транспортного рівня

HTTPS -Захищений протокол передачі гіпертексту

GRE -Інкапсуляція маршрутів

IP -Інтернет Протокол

MFA -Багато факторна аутентифікація

L2TP -Протокол Тунелювання Рівня 2

LAN -Локальна Комп’ютерна Мережа

PPTP -Протокол Тунелювання точка-точку

TCP -Протокол Керування Передачею

TLS -Безпека Транспортного Рівня

VPN -Віртуальна Приватна Мережа

WAN -Глобальна Мережа

2FA -2 факторна аутентифікація

RDP -Протокол віддаленого підключення

DDoS -Відмова в обслуговуванні

DMVPN - VPN з можливістю динамічного тунелю

L3VPN -Протокол Тунелювання Рівня 3

MPLS -Багатопротокольна комутація за мітками

XML -Розширена мова розмітки

NAT -Трансляція мережевих адрес

AES -Розширений стандарт шифрування

DES -Стандарт шифрування даних

RSA -Рівест, Шамір, Адлеман

HMAC -Код автентифікації повідомлення на основі хешу

PFS -Ідеальна передня секретність

ЗМІСТ

ВСТУП

Актуальність теми

З кожним роком загрози кібербезпеці стають все більш високими та розповсюдженими. Організації стикаються зі зростаючими ризиками від кібератак, які можуть призвести до витоку конфіденційної інформації та великих фінансових втрат. Після появи пандемії COVID-19 багато організацій переходять до дистанційної роботи. Це створює потребу в надійних та безпечних телекомунікаційних мережах для забезпечення віддаленого доступу співробітників. Законодавство про захист даних стає все більш суворим, вимагаючи, щоб організації забезпечували адекватний рівень безпеки для особистих даних клієнтів та співробітників. Організації зберігають значну кількість конфіденційної інформації та інтелектуальної власності, яку потрібно захищати від несанкціонованого доступу. Розвиток технологій, таких як Інтернет речей і обчислення в хмарі, призводить до збільшеної складності мереж та більшої потреби в їх захисті. З урахуванням цих факторів, розробка захищеної телекомунікаційної мережі стає надзвичайно важливою для організацій у всіх сферах діяльності[1-4]. Така мережа може захищати від загроз, забезпечувати конфіденційність даних та забезпечувати надійний зв'язок, що є важливим для успішної діяльності та збереження репутації.

Актуальність теми полягає в тому, що останні роки відзначаються стрімким зростанням підприємств та їх розподіленістю. А так як пандемія та геополітичні події вимагають впровадження політики віддаленої роботи, то це створює необхідність забезпечити безпечний віддалений доступ до корпоративних систем і ресурсів через надійні мережі. Важливо не лише для корпоративних мереж з тисячами комп'ютерів, але і для домашніх мереж, де зберігаються особисті дані.

Проблема полягає в тому, що внутрішня мережа офісу доступна всім внутрішнім користувачам, забезпечуючи безпеку компанії. Віддалені працівники не можуть просто увійти в цю систему, тому потрібен віддалений доступ через VPN.

Використання віртуальних приватних мереж (VPN) є поширеним рішенням для задоволення цих потреб. Віддалений доступ за допомогою VPN створює зашифрований канал між користувачем та кінцевою точкою VPN. Це означає, що віддалені співробітники можуть з'єднуватися з офісною мережею з будь-якого місця, де є Інтернет, і отримувати доступ до ресурсів компанії, при цьому їх дані залишаються захищеними, навіть при використанні громадських Wi-Fi мереж [5-8].

Розвиток віддаленої роботи підштовхує до поширеного використання VPN і робить їх пріоритетною мішенню для кіберзлочинців. Атакування мереж, як домашніх, так і корпоративних, цілью якого є прибуток, стає все більшою загрозою. Ці зловмисні дії включають в себе крадіжку особистої інформації, такої як банківські рахунки, і шифрування файлів на комп'ютерах для вимагання викупу. Тому важлива безпека мережі для запобігання витоку конфіденційної інформації [9, 10]. Встановлення належних політик безпеки також захищає команду від потенційно небезпечних веб-сайтів.

Для відповіді на ці вимоги було вибрано незалежний сервер аутентифікації SAML, який може інтегруватися з доменними групами користувачів і відіграває ключову роль у забезпеченні мережевої безпеки. Ця роль полягає в можливості отримувати доступ до різних програм за допомогою одного набору облікових даних для авторизації. Він працює, обмінюючи аутентифікаційну інформацію у певному форматі між різними системами, включаючи систему управління доступом та веб-додаток. Саме через свої переваги, SAML є не так поширеним корпоративним рішенням в Україні[11]. Він спрощує життя користувачам, оскільки вони повинні авторизуватися лише один раз, щоб отримати доступ до різних додатків. Це не лише прискорює процес аутентифікації, але і вимагає запам'ятовування лише одного набору облікових даних для входу. Крім того, в корпоративному контексті SAML робить життя простішим, оскільки зменшує кількість звернень до служби підтримки щодо відновлення втрачених або забуті паролів.

Однією з переваг є те, що належно автоматизована система надання доступу забезпечує безпечну аутентифікацію. Це дозволяє компаніям вкладати ресурси та час у розробку та інтеграцію нових політик безпеки. Наприклад, система управління доступом може забезпечити комплексний захист особистих даних, включаючи функції, такі як багатофакторна аутентифікація, що захищає від найпоширеніших атак на конфіденційну інформацію.

У магістерській роботі проведено порівняльний аналіз двох протоколів безпеки. Досліджено умови налаштування SAML сервера та реалізацію двофакторної аутентифікації. Дослідження виконані на реальному обладнанні сімейства FortiNet з метою інтеграції у державній структурі.

Дипломна магістерська робота складається зі вступу, чотирьох розділів, висновків, списку використаних літературних джерел і додатків.

У першому розділі дипломної роботи здійснено опис віртуальних приватних мереж, розглянуто різновиди їх структури та архітектуру з'єднання обладнання. Детально описано протоколи безпеки та їх використання, і визначено необхідне обладнання.

У другому розділі магістерської роботи створено структурну схему проекту. Проведено докладний огляд технології SAML та особливостей її реалізації, особливо з огляду на використання тільки SSL VPN, що визначає спосіб налаштування мережі для віддаленого підключення. Важливість реалізації додаткових методів захисту VPN також розглядається.

У третьому розділі магістерської роботи детально розглянуто методи шифрування VPN. Вказано, що вся інформація, що проходить через VPN тунель, підлягає шифруванню. Крім того, VPN приховує фактичну IP-адресу та призначає приватну, яка генерується сервером VPN, до якого здійснюється підключення.

У четвертому розділі кваліфікаційної роботи надано порівняльний аналіз на основі двох реалізованих VPN та здійснено налаштування двоетапної аутентифікації з використанням мобільного токену від компанії FortiNet.

Висновки містять загальні результати на основі аналізу матеріалу розділів та виконання завдань, визначених у вступі.

Мета роботи полягає в створенні VPN тунелю для підключення віддалених користувачів до корпоративної мережі за допомогою технології SAML та налаштування доменної аутентифікації.

1. ЛІТЕРАТУРНИЙ ОГЛЯД ТА АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

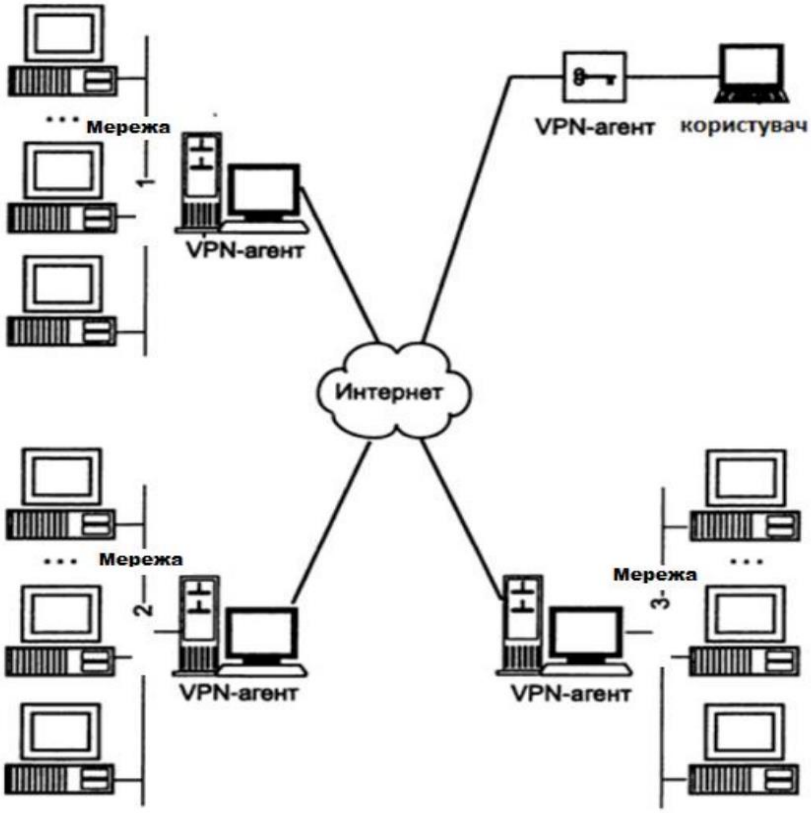
1.1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА VPN

Загалом, VPN - це потужний інструмент для створення безпечних і приватних мережових з'єднань через відкритий Інтернет і використовується як в корпоративних, так і в особистих цілях для забезпечення конфіденційності і захисту даних. VPN функціонує, маршрутизуючи з'єднання через обраний приватний сервер VPN, а не через постачальника Інтернету. Коли дані відправляються в Інтернет, вони проходять через VPN, а не безпосередньо з комп'ютера. VPN виступає посередником під час підключення до Інтернету, тим самим приховуючи IP-адресу, яку надає постачальник, і забезпечуючи анонімність користувача. Якщо дані будуть перехоплені, вони залишаються нечитабельними до тих пір, поки не досягнуть місця призначення. VPN створює приватний "тунель" від пристрою до Інтернету та захищає важливі дані за допомогою шифрування.

VPN використовує шифрування для захисту даних, які передаються через відкриті мережі. Це гарантує конфіденційність і захист інформації від несанкціонованого доступу. Шифрування - це процес, який використовується для захисту даних під час використання VPN. Воно перетворює інформацію у нечитабельний текст, який може бути розшифрований лише за наявності правильного ключа. Тільки сервер VPN та ваш комп'ютер знають цей ключ. Процес розшифрування даних відомий як дешифрування, і це відбувається шляхом використання ключа для перетворення закодованих даних назад у зрозумілу інформацію.

На прикладі введення даних кредитної картки на торговому веб-сайті можна пояснити, як працює шифрування. Під час здійснення будь-якої оплати в Інтернеті інформація шифрується, перетворюючись на нечитабельний код, доки не досягне місця призначення.

Різні послуги VPN використовують відповідні процеси шифрування. Під час підключення до VPN створюється захищений тунель, де дані кодуються, перетворюючись на нечитабельний код під час переміщення між комп'ютером та сервером VPN. Після підключення пристрій опиняється в тій же локальній мережі, що і використаний VPN. IP-адреса пристрою отримується від VPN-сервера провайдера. Ефективність шифрування залежить від обраних протоколів та механізму шифрування.



Малюнок 1.1 – Віртуальна приватна мережа

Більшість VPN-послуг безпосередньо інтегруються з операційною системою, такою як Windows, MacOS, iOS або Android. Це забезпечує захист особистих даних користувача, коли він користується браузером, вводячи, наприклад, дані банківської карти[12-14].

Автономні VPN-послуги часто використовуються в домогосподарствах та невеликих підприємствах. Вони використовують програмне забезпечення, що створює шифроване з'єднання до приватної мережі, яке обслуговує підключення до Інтернету в цілому.

Існують також VPN-розширення для браузерів, які встановлюються як додатки до браузерів, таких як Google Chrome або Firefox. Однак варто зауважити, що ці VPN-послуги захищають дані лише в межах веб-браузера, де вони встановлені. Також, VPN, налаштований в браузері, може бути менш надійним і призводити до можливого витоку IP-адреси[15-17].

Маршрутизатори з підтримкою VPN - ще один спосіб використання VPN. Це зручно для використання на кількох пристроях одночасно, оскільки захищає кожен пристрій, підключений до маршрутизатора, і забезпечує постійне підключення до VPN без необхідності налаштовувати VPN окремо для кожного пристрою. Важливо використовувати маршрутизатори, спеціально розроблені для роботи з VPN, щоб уникнути складних технічних налаштувань[18-20].

Корпоративні VPN часто використовуються організаціями для надання віддаленого доступу співробітникам, які працюють на відстані. Вони забезпечують безпечний доступ до внутрішньої мережі компанії за допомогою індивідуальних паролів та спеціалізованого програмного забезпечення. Реалізація такого рішення вимагає індивідуальної розробки та значних IT-ресурсів.

1.2 КЛАСИФІКАЦІЯ VPN

VPN поділяють на чотири основних типи:

1.Персональні VPN. Це VPN-з'єднання, призначені для індивідуальних користувачів. Вони створюють безпечні та приватні підключення до Інтернету, дозволяючи обходити брандмауери та географічні обмеження.

2.VPN віддаленого доступу. Цей тип VPN використовується підприємствами, де співробітники мають доступ до корпоративної мережі навіть поза офісом, під час подорожей або роботи з дому.

3.Мобільні VPN. Вони призначені для ситуацій, коли користувач не має постійного або стабільного з'єднання з Інтернетом і потребує доступу до VPN через мобільні пристрої.

4.VPN типу "мережа-мережа". Це тип віртуальної приватної мережі, який дозволяє з'єднувати дві або більше локальні мережі (зазвичай мережі на різних фізичних розташуваннях) через інтернет. Використовуються, коли декілька компаній прагнуть підключитися до однієї спільної приватної мережі, а не лише окремі співробітники.

VPN віддаленого доступу дозволяють використовувати Інтернет для підключення до приватних корпоративних мереж навіть за межами офісу.

Таблиця 1.1 – Порівняльна характеристика типів VPN

	VPN віддаленого доступу	Персональний VPN	Мобільний VPN	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 - це ненадійна ланка в спілкуванні. Шифрування VPN використовується для збереження конфіденційності та безпеки даних під час їх переміщення від і до приватної мережі.

Існує декілька методів використання VPN віддаленого доступу, наприклад:

1. Люди, які часто змінюють своє місце проживання, можуть використовувати VPN віддаленого доступу для з'єднання з мережею своєї компанії через Wi-Fi в готелі або в будь-якому громадському місці. Це дозволяє їм отримувати доступ до тих самих файлів і програмного забезпечення, які б мали у офісі. Крім того, VPN захищає їхні дані від будь-кого, хто може стежити за загальнодоступним Wi-Fi.

2. Особа, яка працює з дому, може використовувати VPN віддаленого доступу для підключення до корпоративної мережі зі свого дому. Комп'ютер працює так, ніби він підключений до мережі компанії в офісі, і дані залишаються захищеними під час їхнього переміщення через загальнодоступний Інтернет[21-24].

3. Для використання VPN віддаленого доступу на своєму пристрої, зазвичай потрібно встановити клієнтське програмне забезпечення або налаштувати операційну систему пристрою для підключення до VPN. У кінці мережі також повинен бути сервер VPN. Кілька клієнтських пристроїв може бути підключено, оскільки різні користувачі можуть здійснювати підключення до сервера.

4. Спочатку, сервер VPN перевіряє, чи має користувач доступ до мережі, вимагаючи введення пароля або використання біометричних даних, таких як відбиток пальця для ідентифікації. Деякі рішення дозволяють використовувати сертифікати безпеки для автоматичної автентифікації користувача в фоновому режимі, що сприяє швидкому підключенню. Це особливо корисно, коли користувачеві потрібно здійснювати підключення до декількох серверів VPN, наприклад, для доступу до різних мереж.

5. Після проходження процедури аутентифікації користувача, клієнт і сервер створюють між собою зашифрований тунель. Це захисний шар шифрування, який забезпечує безпеку трафіку під час його пересилання через Інтернет. Існує кілька різних протоколів VPN, які можуть використовуватися для налаштування шифрованого тунелю, включаючи IPsec і SSL.

Приклади VPN віддаленого доступу для бізнесу включають:

- Сервер доступу через OpenVPN, який надає можливість безкоштовного одночасного підключення до VPN для двох користувачів.

- Cisco AnyConnect, який інтегрується з корпоративними рішеннями безпеки Cisco.

Індивідуальні VPN-сервіси

Сервіс індивідуального VPN налаштовує з'єднання між вашим пристроєм та сервером VPN, який виступає посередником між вашим пристроєм і веб-службами, до яких вам потрібно отримати доступ.

Особисті VPN-послуги відрізняються від VPN віддаленого доступу, оскільки вони не надають доступу до приватних мереж. Замість цього, особистий VPN через зашифроване з'єднання надає можливість отримати доступ до загальнодоступної мережі Інтернет[25-29]. Існують численні мотиви використання особистого VPN, серед найпопулярніших:

1. Стрімінг фільмів і серіалів, або прослуховування музики, які недоступні у вашому географічному регіоні. Наприклад, ви можете підключитися до VPN-сервера у США, щоб отримати доступ до американського Netflix з його великим вибором контенту.

2. Оминання обмежень, накладених брандмауерами вашого інтернет-постачальника, і захист веб-трафіку від потенційного стеження державними структурами.

3. Приховання IP-адреси вашого 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.

4. Захист конфіденційності в інтернеті, оскільки інтернет-постачальники часом втручаються в підключення, сповільнюють швидкість чи обмежують доступ через виділення надмірного трафіку.

Особисті VPN-програми доступні на різних типах пристроїв, включаючи смартфони. Вони зазвичай пропонують велику кількість серверів для вибору. Якщо важлива конфіденційність, ви можете підключитися до локального сервера, щоб отримати найвищу швидкість.

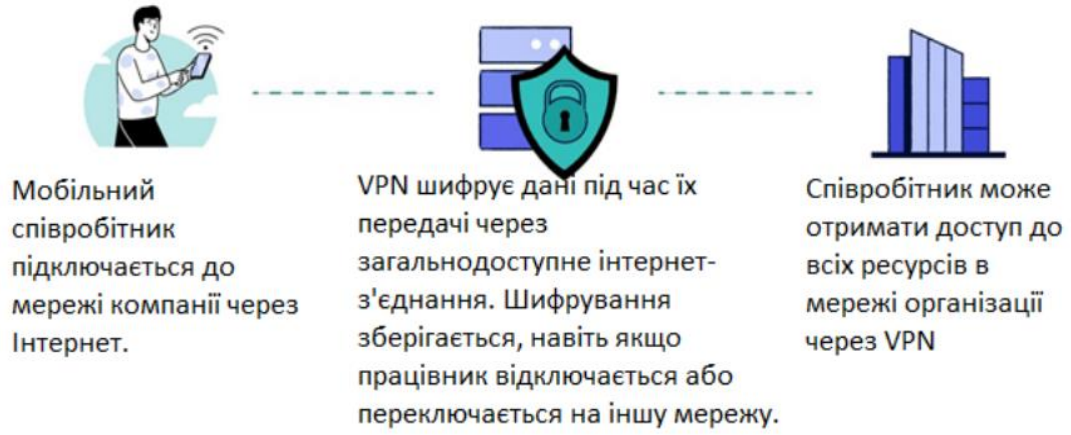
При підключенні до VPN весь ваш інтернет-трафік проходить через сервер постачальника VPN. Оскільки з'єднання шифроване, IP-адресу приховують, що дозволяє отримати доступ до географічно обмеженого вмісту з інших країн без особливих зусиль.

Декілька високорейтингових особистих VPN-послуг включають:

- ExpressVPN
- NordVPN
- Surfshark
- IPVanish

Мобільні VPN, як правило, використовуються для забезпечення надійності доступу для працівників, які використовують мобільні пристрої. Це особливо актуально в ситуаціях, коли стабільність з'єднання може бути недостатньою, але потрібно підтримувати доступ до різних ресурсів[30-32].

Для прикладу, військовослужбовці, що розташовані на блок-постах по всій Україні, використовують планшети та мобільні VPN для забезпечення доступу до різних баз даних та перевірки інформації щодо осіб чи транспортних засобів, що можуть становити загрозу.



Малюнок 1.2 – Приклад підключення за допомогою мобільного VPN

Мобільні VPN підтримують різні методи автентифікації, включаючи паролі, фізичні маркери, такі як смарт-карти, біометричні пристрої, сканери відбитків пальців та системи розпізнавання обличчя. У деяких випадках вони використовують сертифікати безпеки для автоматичної фонової автентифікації користувача.

Мобільний пристрій може перемикатися між мережами, такими як стільникова або Wi-Fi, і при цьому зберігається активне з'єднання. Це може призвести до зміни фізичної IP-адреси, але логічна IP-адреса, використовувана для VPN-тунелю, залишається постійною. Такий підхід забезпечує незмінність віртуального мережевого з'єднання, дозволяючи користувачеві працювати без перерв навіть під час перемикання мереж. Навіть якщо пристрій був вимкнений для економії заряду батареї, VPN-з'єднання залишається доступним після ввімкнення пристрою.

Тепер, щодо VPN типу "мережа-мережа":

Порівняно з VPN віддаленого доступу, який призначений для окремих користувачів, VPN типу "мережа-мережа" об'єднує дві окремі мережі. Наприклад, якщо компанія має два офіси на сході та заході, то VPN типу "мережа-мережа" дозволяє об'єднати їх в єдину мережу.

Існує кілька технологій, які можуть бути використані для реалізації VPN типу "мережа-мережа," серед них IPsec, DMVPN і L3VPN.

В цій категорії VPN існують два основних варіанти:

1. VPN на основі інтрамережі: коли об'єднання VPN створюється між мережами, які належать одній компанії. Це дозволяє компанії створити єдину глобальну мережу, що охоплює два чи більше офіси. Користувачі компанії отримують доступ до ресурсів із інших LAN, як якби вони були підключені фізично.

2. VPN на основі зовнішньої мережі: коли підключені мережі належать різним компаніям, таке об'єднання VPN називається VPN на основі екстрамережі. Цей вид VPN застосовується, наприклад, коли компанія бажає підключитися до мережі постачальника послуг[33, 34].

Існують три основні методи реалізації VPN типу "мережа-мережа":

1. Використання IPsec-тунелю.

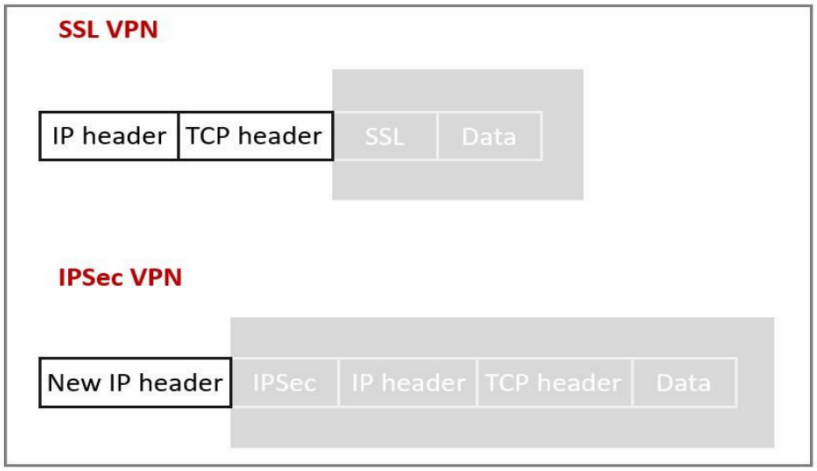
2. Використання динамічної багатоточкової VPN (DMVPN).

3. Використання VPN на третьому рівні (L3VPN).

Тунель IPsec використовується для об'єднання мереж, подібно до того, як він з'єднує окремі підключення з приватною мережею в рамках VPN віддаленого доступу. У випадку VPN типу "мережа-мережа" тунель IPsec шифрує трафік між підключеними мережами. Це може бути реалізовано двома способами:

- Тунель IPsec на основі маршруту, який передає весь трафік між мережами.

- Тунель IPsec на основі політики безпеки, який встановлює правила для контролю дозволеного трафіку та взаємодії між мережами. Такі тунелі IPsec можуть бути налаштовані за допомогою брандмауерів та мережевих маршрутизаторів.



Малюнок 1.3 – Склад пакетів протоколів SSL та Ipsec

Методика динамічного багатоточкового VPN (Dynamic MultiPoint VPN, DMVPN) запропонована як відповідь на обмеження тунелей IPsec, які об'єднують лише дві точки одна з одною. У відмінність від цього підходу, DMVPN дозволяє об'єднувати мережі за допомогою маршрутизатора-концентратора DMVPN та використовувати динамічні IP-адреси.

В той час як якість обслуговування у тунелях IPsec та DMVPN, які працюють поверх Інтернету, може бути непостійною, багатопротокольні мережі з комутацією міток MPLS на 3-му рівні можуть гарантувати надійність та стабільність зв'язку. MPLS є методом маршрутизації мережевих пакетів через різні транспортні середовища, такі як оптоволокно або супутник, за допомогою різних протоколів. Цей підхід дозволяє мережевим провайдерам створити VPN на 3-му рівні, що базується на мережевому рівні моделі OSI. Зазвичай ці MPLS VPN розгортаються провайдерами зв'язку.

Мережеві провайдери можуть створити окремі віртуальні мережі для кожного клієнта, які передаються через глобальну мережу. Ці віртуальні мережі забезпечують ізоляцію одна від одної, навіть якщо вони використовують спільні фізичні мережеві ресурси. За допомогою MPLS VPN можна встановлювати пріоритети для різних видів трафіку, таких як голосовий трафік, для забезпечення найкращої якості

обслуговування. Контроль над маршрутизацією мережевого трафіку є важливим для забезпечення стабільної та оптимізованої продуктивності.

Незважаючи на переваги приватних глобальних мереж, вони можуть бути високими за вартістю, тому багато компаній віддають перевагу дешевшим мережам VPN на базі Інтернету, за винятком ситуацій, де важлива критична затримка, наприклад, у програмах для моніторингу та обслуговування електричних мереж.

1.3 ОГЛЯД ІСНУЮЧИХ ПРОТОКОЛІВ БЕЗПЕКИ VPN ТА ТЕХНОЛОГІЇ НА ЯКИХ ҐРУНТУЄТЬСЯ ЇХ РОБОТА

В цьому розділі ми розглянемо різноманітні протоколи безпеки VPN та технології, що лежать в основі їхньої роботи. VPN (віртуальні приватні мережі) використовуються для забезпечення безпеки та приватності в мережах передачі даних, і існує кілька ключових протоколів та підходів, які допомагають досягти цих цілей. Значною мірою розглянемо також технології, на яких ґрунтується робота VPN. Це включає шифрування даних, аутентифікацію користувачів (часто з використанням паролів, фізичних маркерів або біометричних засобів), та управління ключами шифрування.

Для реалізації різних сценаріїв використання VPN існують різні види протоколів, які відповідають за забезпечення безпеки, шифрування трафіку та інші аспекти функціонування. Вибір конкретного протоколу VPN має велике значення при проектуванні рішень в цій області. Трьома найпоширенішими і важливими протоколами є OpenVPN, IPSec SSL і відносно новий WireGuard, який виник досить нещодавно і викликав обговорення серед спеціалістів. При цьому існують і інші протоколи, які, хоч і є застарілими, проте можуть використовуватися для конкретних завдань.

Вибір підходящого протоколу VPN обумовлюється декількома факторами та обставинами використання:

1. Пристрої. Різні пристрої підтримують різні протоколи, тому важливо враховувати сумісність.

2. Мережа. Наявність деяких послуг може бути обмежена у певних локаціях або країнах, тому вибір протоколу може залежати від цих обмежень. Наприклад, деякі VPN-постачальники працюють у Китаї, де більшість інших їхніх конкурентів заблоковані.

3. Продуктивність. Деякі протоколи можуть мати кращу продуктивність, особливо на мобільних пристроях, тоді як інші можуть бути більш практичними великих корпоративних мережах.

4. Модель загроз. Різні протоколи можуть виявляти себе в різних ситуаціях, і деякі можуть бути менш безпечними, що потребує відповідних заходів забезпечення безпеки.

Давайте розглянемо кілька найбільш поширених протоколів:

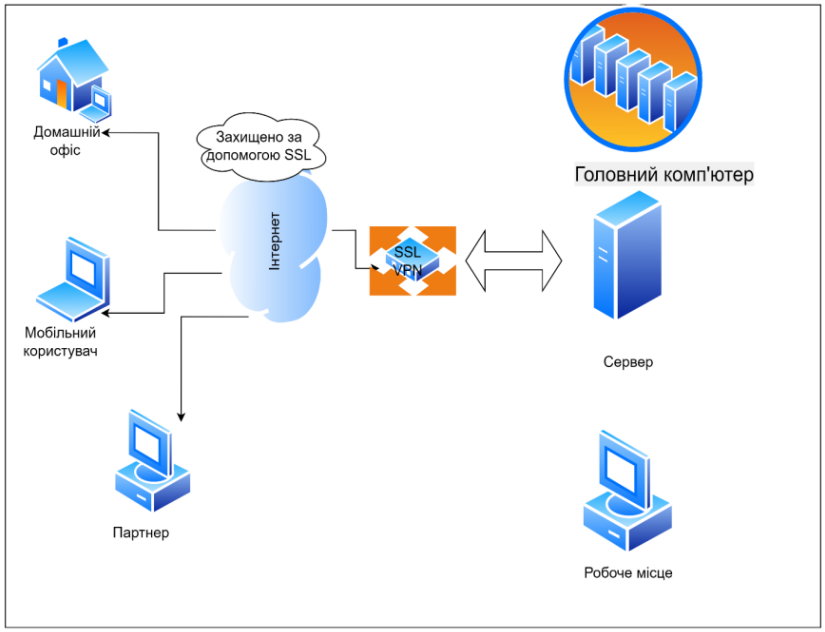
PPTP (Point-to-Point Tunneling Protocol):Однією з найдавніших VPN-технологій є PPTP, розроблена Microsoft. Вона використовує два канали для управління та передачі даних і має свої особливості.

PPTP доступний на всіх версіях Windows і широко підтримується багатьма операційними системами. Незважаючи на відносно високу швидкість, слід відзначити, що PPTP не є найбільш надійним протоколом, і він не відновлює підключення так швидко після переривань, як, наприклад, OpenVPN.

На цей момент PPTP є застарілим і Microsoft рекомендує використовувати інші VPN рішення, особливо з урахуванням важливості забезпечення безпеки та конфіденційності.

Звісно, якщо ваша основна мета використання VPN - розблокування контенту, PPTP може підійти, але варто розглянути більш безпечні альтернативи. SSTP (Secure Socket Tunneling Protocol) є пропрієтарним рішенням від Microsoft. Хоча SSTP не так

поширений серед VPN-протоколів, як PPTP, він має значно вищий рівень безпеки і не має серйозних проблем у цьому відношенні.



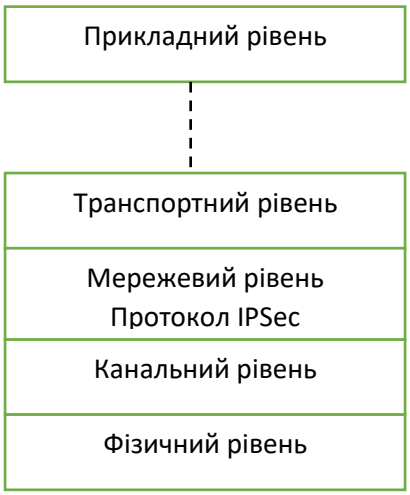
Малюнок 1.4 – Підключення з використанням SSL

SSTP використовує SSL для передачі трафіку через TCP-порт 443, що робить його вигідним в умовах обмежених мереж, наприклад, як в Китаї, де інші VPN можуть бути блоковані. Хоча SSTP теоретично може бути встановлений на Linux, цей протокол переважно використовується системами Windows. SSL може забезпечити захист протоколів прикладного рівня, таких як POP3 або FTP, і для його роботи потрібний SSL-сертифікат на сервері. Використовуючи SSL, безпечне з'єднання між клієнтом і сервером виконує дві основні функції: аутентифікацію та захист даних.

SSL має два рівні: нижні рівні у багаторівневому транспортному протоколі, такому як TCP, використовуються для інкапсуляції різних протоколів. Для кожного вкладеного протоколу, SSL забезпечує умови, в яких сервер і клієнт можуть підтверджувати свою автентичність, захищати передачу даних та обмінюватися ключами, перед тим як передача даних протоколу прикладного рівня розпочнеться.

SSL має численні переваги, включаючи простоту використання, відсутність необхідності в додатковому програмному забезпеченні та можливість безпечного віддаленого доступу. Щодо продуктивності, SSTP працює швидко, стабільно та надійно.

IPsec (Internet Protocol Security) - це набір протоколів для захисту даних, які передаються по IP-мережі. У відміну від SSL, який діє на рівні застосунків, IPsec працює на рівні мережі і може взаємодіяти з багатьма операційними системами без потреби в сторонніх програмах.

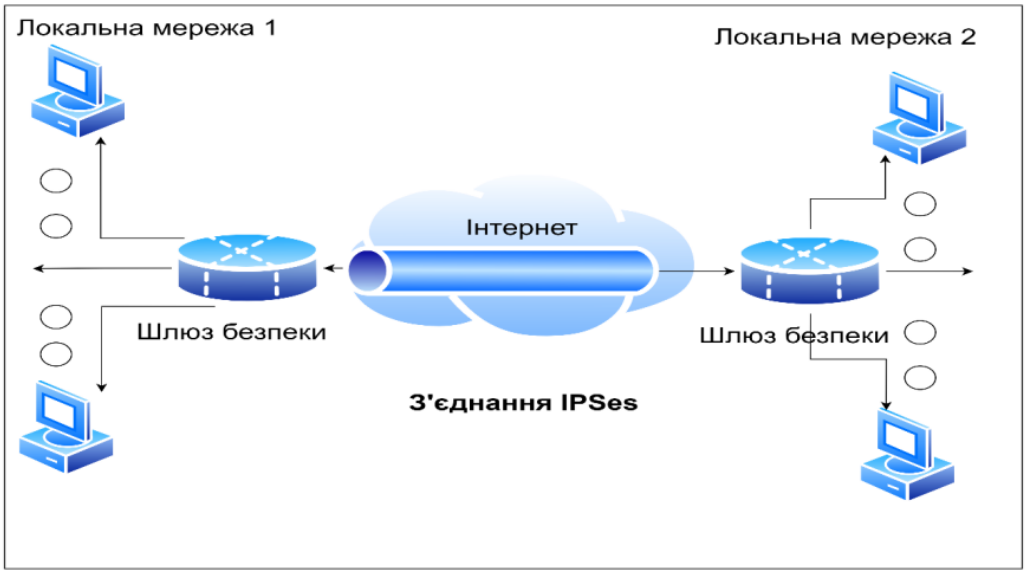


Малюнок 1.5 – Розміщення протоколу IPsec в модулі OSI

IPsec став дуже популярним для використання разом з протоколами L2TP або IKEv2. IPsec забезпечує шифрування всього IP-пакету, використовуючи два ключові компоненти:

- Authentication Header, що ставить цифровий підпис на кожному пакеті;

- Encapsulating Security Protocol, що гарантує конфіденційність, цілісність та аутентифікацію пакетів під час їх передачі.

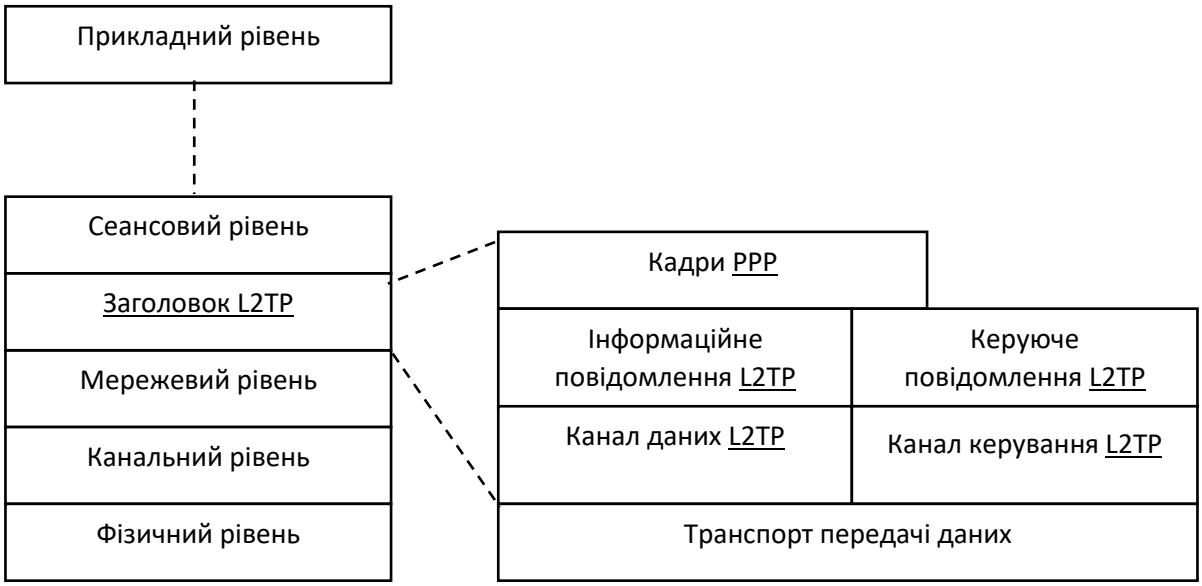


Малюнок 1.6 Приклад з’єднання на базі IPsec

Протокол L2TP/IPsec був вперше представлений у 1999 році як апгрейд протоколів L2F (Cisco) і PPTP (Microsoft). Оскільки L2TP сам по собі не надає шифрування чи аутентифікації, часто його використовують разом з IPsec. Підтримується багатьма операційними системами.

L2TP/IPsec вважається безпечним і не має серйозно виявлених проблем. В цьому протоколі може використовуватися шифрування 3DES або AES, проте зараз 3DES вважається вже застарілим і рідко використовується. В окремих випадках використання протоколу L2TP може стикається з проблемами через стандартне використання UDP-порту 500, який блокується деякими брандмауерами.

Протокол L2TP/IPsec надає високу надійність передачі даних, його налаштування просте і він підтримується всіма сучасними операційними системами. Однак L2TP/IPsec подвійно інкапсулює дані під час передачі, що робить його менш ефективним і повільнішим, ніж інші VPN-протоколи.



Малюнок 1.7 – Складові протоколу L2TP

IKEv2/IPsec (Internet Key Exchange version 2) - це протокол IPsec, призначений для взаємної аутентифікації, створення та управління захистом зв'язку. Його розроблено спільно Microsoft і Cisco, і існують відкриті реалізації, такі як OpenIKEv2, Openswan і strongSwan. Додатково, завдяки підтримці Mobility and Multi-homing Protocol, IKEv2 добре пристосований до змін мережевих умов. Це робить його ідеальним вибором для мобільних користувачів, які перемикаються між різними мережами або точками доступу. IKEv2/IPsec підтримує різні криптографічні алгоритми, включаючи AES, Blowfish та Camellia, включаючи 256-бітні ключі. І щодо продуктивності, у багатьох випадках IKEv2 працює швидше за OpenVPN, зокрема на мобільних пристроях. Цей протокол підтримується на різних операційних системах, включаючи Windows, Mac OS, iOS та певні пристрої Android.

OpenVPN - це популярний відкритий протокол VPN, розроблений OpenVPN Technologies. Він відзначається стабільністю та високою швидкістю передачі даних. OpenVPN використовує як TCP, так і UDP, і може бути альтернативою IPsec та SSL, особливо коли деякі протоколи VPN блокуються провайдером. Використання OpenVPN вимагає встановлення клієнтського програмного забезпечення, і багато VPN-постачальників розробляють власні програми для різних операційних систем і

пристроїв. Цей протокол може працювати на різних портах TCP та UDP і сумісний з багатьма платформами, включаючи Windows, Mac OS, Linux, Apple iOS і Android.

WireGuard - це новий протокол VPN, який розробники позиціонують як передову альтернативу для більшості випадків використання IPsec, OpenVPN та SSL. WireGuard відзначається високою безпекою, продуктивністю і простотою налаштування. Усі пакети IP, які надходять до інтерфейсу WireGuard, інкапсулюються через UDP. WireGuard використовує сучасні криптографічні засоби, включаючи Curve25519 для обміну ключами, ChaCha20 для шифрування, Poly1305 для аутентифікації даних, SipHash для хешування ключів та BLAKE2 для хешування. Порівняно з кодом OpenVPN, код WireGuard значно менший (4 тисячі рядків проти кількох сотень тисяч), що робить його більш доступним для дослідження на предмет вразливостей. Недавно було представлено WireGuard 1.0.0, який включає компоненти WireGuard в основний склад ядра Linux 5.6. Код, що включений до ядра Linux, пройшов додатковий аудит безпеки, проведений незалежною фірмою, і 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
Ліцензія	Proprietary	Proprietary	Proprietary	Власний, але існує протокол реалізації з відкритим вихідним кодом	GNU GPL	GNU GPL

Ознака	PPTP	SSTP	L2TP/IPsec	IKEv2/IPsec	OpenVPN	WireGuard
Розгортання	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+, Mac OS 10.11+ і більшість мобільних ОС мають вбудовану підтримку	Windows, Mac OS, GNU/Linux, Apple iOS, Android і маршрутиз атори. Необхідна установка спеціалізо ваного ПО, що підтримує роботу з даними протоколом	Windows, Mac OS, GNU/Linux , Apple iOS, Android. Встановити са WireGuard, а потім налаштувати і 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 криптографі чних алгоритмів, включаючи AES, Blowfish, Camellia	Використо вує бібліотеку OpenSSL (реалізує більшість популярних криптогра фічних стандартів)	Обмін ключами по 1-RTT, Curve2551 9 для ECDH, RFC7539 для ChaCha20 і Poly1305 для аутентифіка ційного шифрування і BLAKE2s для хешуван.
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
Недоліки безпеки	Має серйозні вразливості. MSCHAP-v2 уразливий для атаки, а алгоритм RC4 піддається атаці Bitflippin	Серйозних недоліків безпеки не було виявлено	3DES вразливий для Meet-inthe-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

1.4 ОГЛЯД СУЧАСНИХ ПІДХОДІВ ДО НАЛАШТУВАННЯ VPN ДЛЯ ВІДДАЛЕНОГО ПІДКЛЮЧЕННЯ ДО КОРПОРАТИВНОЇ МЕРЕЖІ

В сучасному світі віддалена робота стає все більш популярною, і вона вимагає надійного та безпечного способу доступу до корпоративних мереж. В цьому розділі ми розглянемо сучасні підходи до налаштування віртуальних приватних мереж (VPN) для забезпечення віддаленого підключення до корпоративних мереж.

1. Використання SSL VPN:

Серія технологій SSL VPN дозволяє користувачам безпечно підключатися до корпоративних ресурсів через веб-браузер, забезпечуючи високий рівень зручності та безпеки. Цей метод добре підходить для користувачів різних операційних систем і відрізняється простотою налаштування.

2. Використання IPsec VPN:

IPsec (Internet Protocol Security) є популярним методом створення безпечних VPN-з'єднань для віддалених користувачів. Він забезпечує високий рівень безпеки за допомогою шифрування та аутентифікації IP-пакетів.

3. Використання L2TP/IPsec та IKEv2:

Комбінація протоколів L2TP, IPsec і IKEv2 використовується для створення стійких і безпечних VPN-з'єднань, особливо для великих корпорацій з високими вимогами до безпеки.

4. Використання WireGuard:

Новітній протокол VPN, WireGuard, використовує сучасні криптографічні методи для створення швидких і безпечних VPN-з'єднань.
Ці різні підходи надають можливість вибору оптимального рішення для налаштування віддалених VPN-підключень в залежності від потреб у безпеці, зручності та продуктивності.

При використанні віддаленого доступу через браузер, користувач відвідує корпоративний портал, який налаштовується мережевим адміністратором на ASA. На цьому порталі користувач може знайти наступні основні розділи в залежності від типу доступних ресурсів:

- Веб-додатки (Web Applications);
- Перегляд мереж (Browse Networks);
- Доступ до програм (Application Access);
- Термінальні сервери (Terminal Servers).

Fortinet також має параметри налаштування для IPsec та SSL VPN. SSL VPN включає два режими: тунельний та веб-режим. Вибір режиму та рівня безпеки залежить від конкретних потреб та особливостей середовища. В тунельному режимі, клієнт SSL VPN шифрує весь трафік з віддаленого комп'ютера та надсилає його до FortiGate через тунель SSL VPN, використовуючи HTTPS-з'єднання.

Веб-режим надає можливість безклієнтського доступу до мережі через веб-браузер з вбудованим SSL-шифруванням. Він є простішим у налаштуванні, не вимагає встановлення окремого клієнта на кінцевій точці, але обмежений у підтримці деяких програм та вимагає більше ресурсів на FortiGate.

IPsec VPN, як було зазначено раніше, є стандартним протоколом, який дозволяє використовувати різні рішення для з'єднання кінцевих точок, включаючи FortiClient. Це стандартний протокол, який використовує певні порти і, іноді, може бути блокований провайдерами.

Висновки до розділу 1

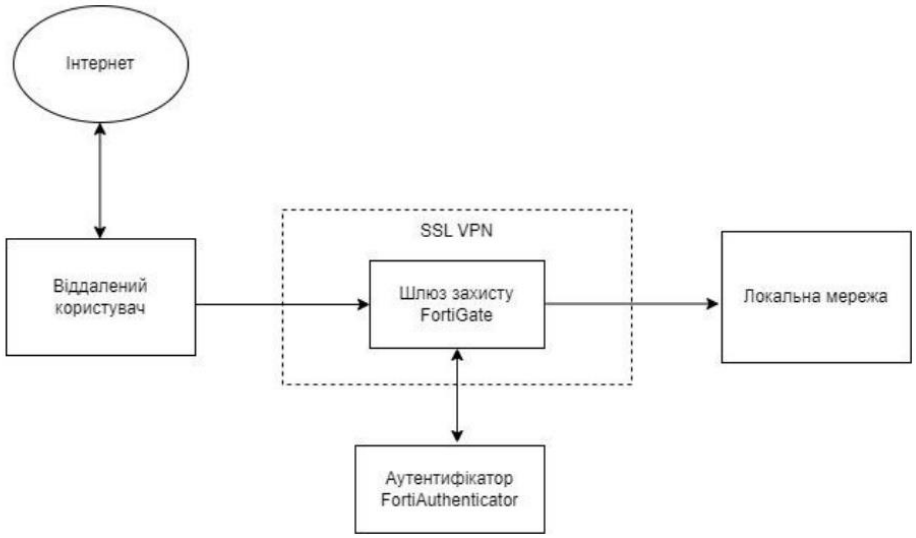
Підсумовуючи перший розділ дипломної роботи, ми визначили віртуальну приватну мережу, розглянули різні методи побудови та обговорили протоколи безпеки та обладнання, необхідне для її реалізації.

2. ОБРАННЯ ТЕХНОЛОГІЇ ТА МЕРЕЖЕВОГО ОБЛАДНАННЯ ДЛЯ СТВОРЕННЯ VPN

2.1 Схема VPN тунелю та вибір елементної бази

На сьогоднішній день у Інтернеті існує багато веб-сайтів, які використовують протокол SSL для захисту особистої інформації, зокрема ті, що надають комерційні та банківські послуги. Більшість популярних браузерів та інтернет-додатків підтримують протокол SSL, який можна розпізнати за префіксом https у URL.

SSL VPN є оптимальним рішенням для підключення віддалених користувачів до ресурсів локальної мережі офісу через Інтернет. У нашому випадку вибір SSL VPN обумовлений зручністю його використання, а також сумісністю з мережевим обладнанням FortiNet, яке вже використовується в організації. FortiGate обраний як шлюз захисту та аутентифікатор, забезпечуючи високий рівень сумісності та ефективну інтеграцію. Для забезпечення стабільної роботи і уникнення конфліктів вибрано FortiAuthenticator для інтеграції конфігурації користувача з існуючим сервером автентифікації. У зв'язку з великою кількістю користувачів в обраному середовищі, це рішення максимально спрощує процес автентифікації та забезпечує високий рівень безпеки. Структурна схема зображена на рисунку 2.1.



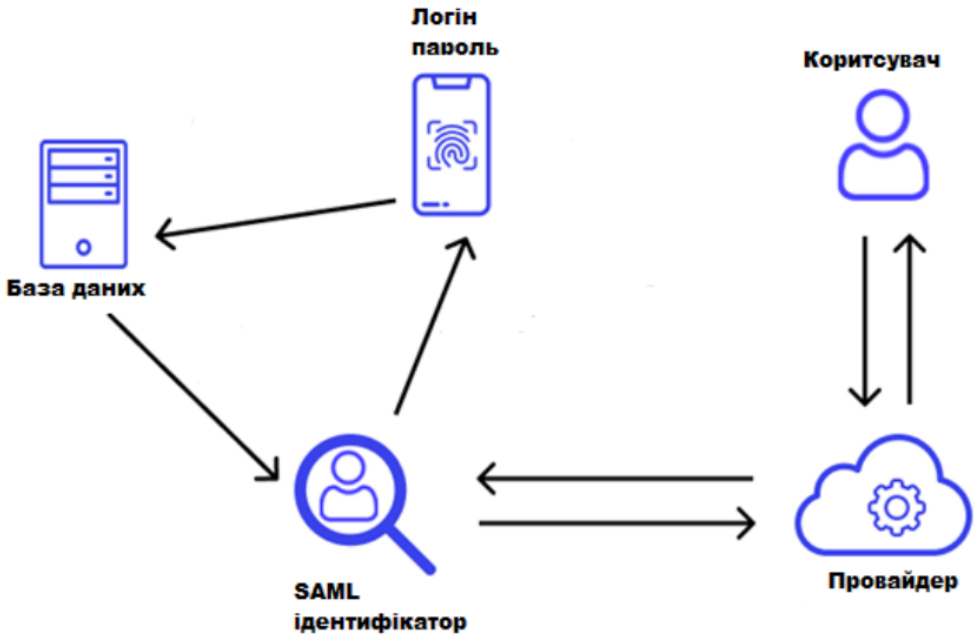
Малюнок 2.1 – Структурна схема VPN

Для непрямого входу встановлюється FortiClient, який підтримує різні методи підключення до VPN, включаючи SSL VPN та IPsec VPN. Роздільне тунелювання для віддалених користувачів дозволяє їм отримувати доступ до Інтернету, не пересилаючи весь трафік через сервер VPN, що полегшує передачу даних та покращує швидкість завантаження. FortiClient інтегрується з Microsoft Windows Active Directory, щоб синхронізувати структуру компанії та спростити управління. Централізована система управління FortiClient дозволяє адміністраторам віддалено налаштовувати та оновлювати клієнтів, спрощуючи процес запуску агентів.

FortiClient створює віртуальні групи, враховуючи стан безпеки кінцевих точок, що дозволяє реалізовувати динамічний контроль доступу залежно від їх стану. Роздільне тунелювання трафіку додатків гранулює передачу даних через шифрований тунель та Інтернет, покращуючи швидкість передачі. FortiClient автоматизує процеси підключення, вибору сервера VPN та використання багатофакторної автентифікації для забезпечення додаткового рівня безпеки VPN-з'єднання. Розділене тунелювання VPN може бути реалізоване за допомогою різних методів, таких як розділене тунелювання на основі URL-адрес, додатків чи зворотне розділене тунелювання.

2.2 ОСОБЛИВОСТІ НАЛАШТУВАННЯ SAML СЕРВЕРУ

SAML – це відкритий стандарт обміну автентифікаційними даними, побудований на мові XML. Веб-програми використовують SAML для передачі даних автентифікації між різними сторонами процесу, наприклад, між системою керування доступом та постачальником послуг. Розглянемо використання FortiClient як прикладу провайдера послуг у цьому контексті. SAML з'явився у високотехнологічній галузі для спрощення процесу автентифікації, особливо там, де користувачам необхідно мати доступ до різних веб-додатків у різних доменах. До введення SAML технологія єдиного входу була ефективною, але використовувала файли cookie, які обмежували свою дію лише в межах одного домену.



Малюнок 2.2 – Принцип роботи технології SAML

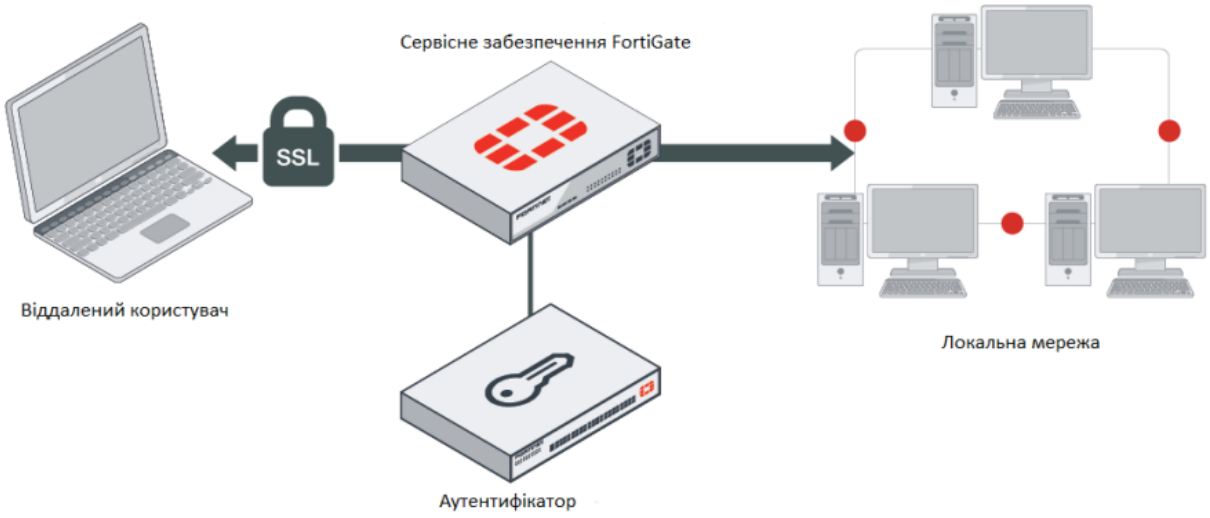
SAML впроваджується для спрощення процесу автентифікації, коли користувачам потрібен доступ до різних веб-додатків у різних областях. За допомогою SAML веб-програми взаємодіють із системою управління доступом, що дозволяє користувачам уникати запам'ятовування багатьох комбінацій логінів та паролів.

Суть концепції SAML полягає в обміні інформацією користувача, такої як логіни, стан автентифікації та ідентифікатори, між системою управління доступом та постачальником послуг. Це спрощує та забезпечує безпеку процесу автентифікації, дозволяючи користувачам увійти в систему лише один раз за допомогою одного набору даних для входу. Коли користувач подає запит на доступ до сайту, SAML передає аутентифікаційні дані постачальника послуг, що дозволяє користувачеві отримати доступ[20].

Процес двоетапної автентифікації розпочинається, коли користувач намагається увійти в додаток, службу чи систему, доки йому не нададуть доступ.

Алгоритм аутентифікації включає введення облікових даних, перевірку їх правильності, генерацію безпекового ключа, введення другого фактору автентифікації та завершення процесу для отримання доступу до системи.

Модель налаштування SAML для SSL VPN представлена на рисунку 2.2



Малюнок 2.3 – Модель мережевого підключення обладнання сімейства FortiGate

Розглянемо етапи мережевого підключення у такому порядку:

1. Адміністратор чи кінцевий користувач конфігурує SSL VPN, активуючи SAML.

2. FortiClient з'єднується із FortiGate.

3. FortiGate повертає посилання для перенаправлення на сторінку авторизації SAML IdP.

4. FortiClient відображає сторінку авторизації IdP у вбудованому вікні браузера.

5. Користувач вводить свої облікові дані у вікні для входу.

6. Після успішної аутентифікації FortiClient встановлює тунель до FortiGate. У такій конфігурації FortiGate діє як постачальник послуг (SP), а FortiAuthenticator — як постачальник ідентифікаційної інформації (IdP).

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

Принципи підвищення захищеності з’єднання є важливою складовою в забезпеченні безпеки мережевих з'єднань. Нижче розглянуті ключові принципи, що сприяють підвищенню рівня захисту з’єднань:

1. **Використання Криптографії:** Застосування сучасних криптографічних алгоритмів для шифрування даних у тунелях забезпечує конфіденційність та недоступність інформації для несанкціонованих осіб.

2. **Багатофакторна Аутентифікація:** Застосування систем аутентифікації, які використовують не лише паролі, але і додаткові елементи, такі як токени, біометричні дані чи смарт-карти, для підтвердження ідентичності користувача.

3. **Регулярні Оновлення та Патчі:** Постійне оновлення програмного та апаратного забезпечення забезпечує виправлення вразливостей, що допомагає у запобіганні атак та підвищенні стійкості системи.

4. **Логування та Моніторинг:** Ведення журналів подій та постійний моніторинг активності дозволяють вчасно виявляти та реагувати на потенційні загрози.

5. **Обмеження Прав Доступу:** Ретельне налаштування прав доступу для користувачів і системних ресурсів обмежує можливість несанкціонованого доступу.

6. **Захист від DDoS-Атак:** Застосування заходів для виявлення та запобігання атакам, які спрямовані на перенавантаження мережевого з'єднання (DDoS).

7. **Використання VPN та Тунелювання:** Встановлення віртуальних приватних мереж (VPN) та тунелювання для забезпечення безпеки під час передачі даних через неприватні мережі.

8. **Реєстрація та Аудит Безпеки:** Проведення регулярних аудитів безпеки для оцінки ефективності заходів безпеки та виявлення можливих слабких місць.

Захист з’єднань визначається комплексом цих принципів, що спільно допомагають у створенні надійної та стійкої мережевої інфраструктури.

У режимі тунелювання клієнт SSL VPN шифрує весь трафік з віддаленого комп'ютера та передає його на FortiGate через тунель SSL VPN за допомогою HTTPS-з'єднання. FortiGate налаштовує тунель, присвоюючи клієнту віртуальну IP-адресу з зарезервованого діапазону. Незважаючи на відмінності базових протоколів, це нагадує тунелі IPsec VPN, оскільки весь трафік користувача шифрується, що дозволяє обмінюватися різноманітним трафіком між користувачами та мережами.

Користувач, який має потребу у віддаленому підключенні до свого сервера через RDP, лише встановлює тунельне з'єднання, що дозволяє використовувати звичайну клієнтську програму RDP Windows для підключення. Звичайне тунелювання направляє весь трафік через FortiGate, тоді як розділене тунелювання направляє трафік тільки до певної мережі через FortiGate. Режим тунелю вимагає встановлення VPN-клієнта FortiClient на віддаленому кінці. Автономний VPN-клієнт FortiClient є безкоштовним та підтримує як тунелі SSL VPN, так і IPsec VPN.

Для мереж з численними користувачами рекомендується інтегрувати конфігурацію користувача з існуючими серверами автентифікації через LDAP, RADIUS або FortiAuthenticator. Інтеграція з серверами автентифікації, такими як Windows AD, спрощує налаштування користувачів та груп, а використання багатофакторної автентифікації забезпечує додатковий рівень безпеки, вимагаючи двох факторів для підтвердження ідентичності користувача.

Висновки до розділу 2

У другому розділі магістерської роботи була розроблена структурна схема проекту, де детально вивчено технологію SAML та її особливості в контексті реалізації SSL VPN. Це визначило спосіб конфігурації мережі для віддаленого підключення. Також розглянуто важливість використання додаткових заходів захисту VPN.

Рішення FortiGate SSL VPN включає в себе високопродуктивні криптографічні VPN для ефективного захисту користувачів від можливих загроз, що можуть призвести до витоку даних. Технологія Fortinet VPN створює безпечний канал зв'язку через Інтернет, незалежно від використовуваної мережі чи кінцевого пристрою.

Підбиваючи підсумок, легкість впровадження, розгортання та використання SSL VPN надають численні організаційні переваги в галузі безпеки. Цей вид VPN необхідний для підвищення рівня інформаційної безпеки та забезпечення надійної підтримки віддаленої роботи. У зв'язку зі зростанням кількості кіберзагроз, забезпечення безпеки конфіденційних даних стає важливим пріоритетом, і застосування захищеного VPN допомагає зменшити пов'язані з цим ризики.

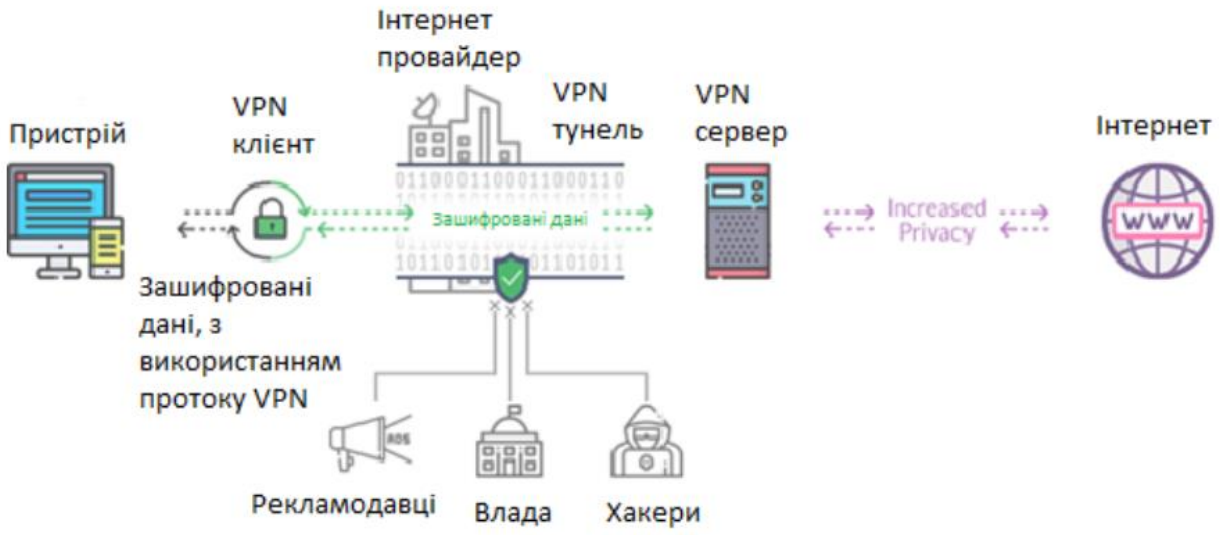
3. МЕТОДИ НАДІЙНОГО ШИФРУВАННЯ МЕРЕЖ

3.1 Алгоритми шифрування VPN

Шифрування представляє собою процес кодування частини інформації способом, який забезпечує доступ лише авторизованим сторонам та вимагає ключа для розшифрування. Сучасні технології шифрування майже невразливі до вторгнень. Навіть якщо доступ до інформації отримано, без належного ключа вона залишається нерозбірливою.

Для ефективної роботи шифрування відправник та отримувач повинні знати правила перетворення вихідного повідомлення в зашифровану форму. Ці правила базуються на алгоритмі та ключі. Алгоритм, як математична функція, об'єднує повідомлення з ключем, утворюючи нечитабельний шифрований рядок. Дешифрування без правильного ключа вкрай складне або навіть неможливе.

Використання криптографії у VPN означає застосування концепцій, таких як шифрування та дешифрування, для захисту інформації. Шифрування включає перетворення відкритого тексту в зашифрований за допомогою ключа, а дешифрування проводить зворотню операцію, перетворюючи зашифрований текст у відкритий за допомогою ключа.



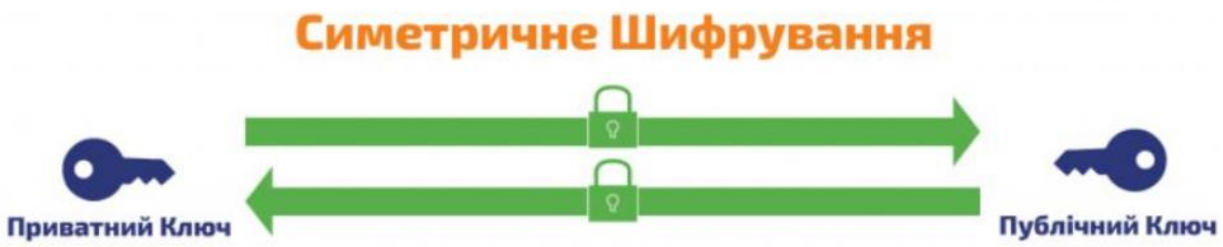
Малюнок 3.1 – Схема шифрування даних VPN

Ключ шифрування VPN, що є надійним паролем, використовується для кодування та розкодування даних, і відомий лише пристрою та серверу VPN. Довжина ключа вимірюється в бітах (послідовність двійкових одиниць і нулів) і може варіюватися.

Найпоширеніші методи шифрування для захисту онлайн-трафіку та з'єднання у VPN включають:

- Симетричне шифрування закритим ключем

Це шифрування передбачає, що обидві сторони, що обмінюються даними, використовують один і той самий ключ для шифрування та дешифрування відкритого тексту. Більшість VPN використовують цей метод шифрування.



Малюнок 3.2 – Використання ключу в симетричному шифруванні

Крім того, для симетричного шифрування використовуються алгоритми, такі як AES і Blowfish. Щодо асиметричного шифрування, воно базується на двох ключах: відкритому і закритому. Відкритий ключ використовується для шифрування вихідного тексту, тоді як лише закритий ключ може розшифрувати вхідний текст.

Малюнок 3.3 – Використання ключу в асиметричному шифруванні

Для асиметричного шифрування необхідно, щоб більшість користувачів володіли відкритим ключем, тоді як авторизована сторона має доступ лише до закритого ключа 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.

Високий стандарт шифрування демонструється через використання AES у симетричному шифруванні. Класифікація інформації розподіляється на три категорії: таємна, повністю таємна та інформація з обмеженим доступом. Для захисту повністю

таємного рівня та інформації з обмеженим доступом можна використовувати ключі різної довжини. Алгоритм AES включає різні перетворення для даних у масиві, такі як підстановка за таблицею, зсув рядків і змішування стовпців. Здійснюється останнє перетворення для кожного стовпця, використовуючи відповідний фрагмент ключа шифрування. Важливою є довжина ключа, оскільки більші ключі вимагають більше циклів перетворень.

Алгоритм шифрування Blowfish був впроваджений компаніями VPN як альтернатива AES. Його творець, Брюс Шнайер, спеціально не патентував алгоритм, щоб забезпечити вільне використання. Blowfish є блоковим шифром з 64-розрядним блоком, вдвічі меншим за AES, зробивши його менш стійким. Навіть як гідна альтернатива, його вразливість до атак обумовлена невеликим розміром блоку. Хоча він використовувався у деяких VPN, таких як Buffer і PrivateInternetAccess, більшість великих VPN-сервісів віддали перевагу AES, визнаючи його більшу безпеку.

Шифрування рукостискання

RSA – це узгоджений процес, який дозволяє сторонам при обміні даними визнавати одна одну та узгоджуватися щодо алгоритмів шифрування чи ключів використання.

У більшості випадків для шифрування RSA використовується алгоритм Рівест-Шаміра-Адлемана. Інші VPN також використовують обмін ключами за еліптичною кривою Діффі-Хеллмана. Відповідно до Діффі-Хеллмана, ключовий внесок сервера записується на сертифікаті, а клієнтський генерується випадковим чином.

Алгоритм безпечного хешування

SHA – це алгоритм хешування, призначений для перевірки автентичності даних SSL/TLS-з'єднань. Процес посилюється унікальним відбитком пальця, який створюється для перевірки дійсності сертифіката TLS. Це служить підтвердженням того, що підключення відбувається до правильного VPN-сервера. Зазначимо, що

відсутність SHA може спричинити перенаправлення інтернет-трафіку на сервер хакера замість цільових VPN-серверів.

Хеш-код автентифікації повідомлення

Система HMAC – це спосіб кодування повідомлень, який використовує криптографічну хеш-функцію та секретний криптографічний ключ. Цей метод призначений для перевірки цілісності та автентичності даних, забезпечуючи їхню безпеку. В багатьох високоякісних VPN застосовуються алгоритми хешування SHA разом із системою HMAC для максимального рівня безпеки.

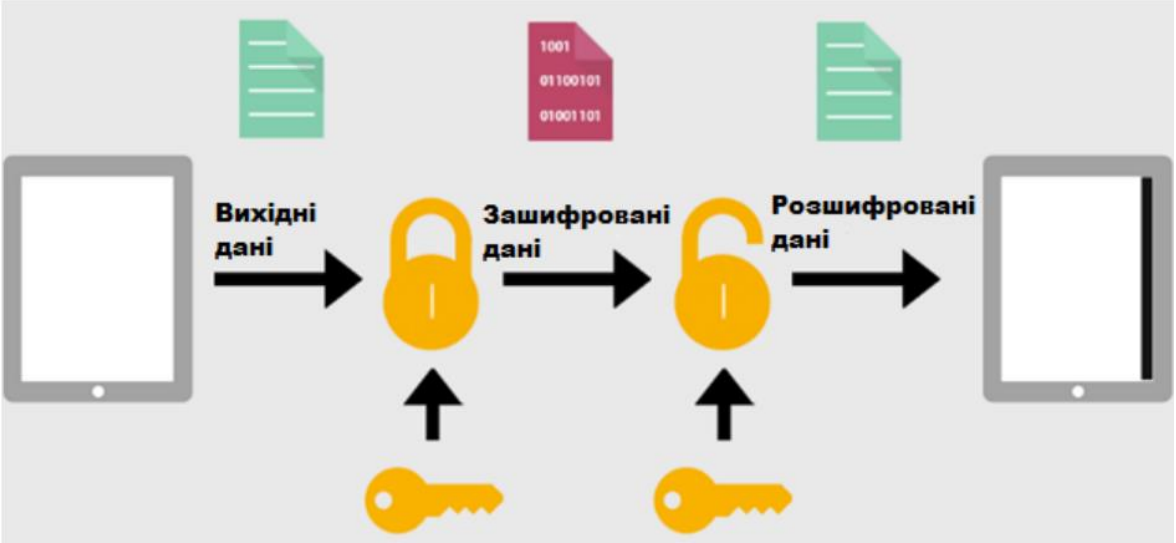
Ідеальна передня секретність

Perfect Forward Secrecy (PFS) – це метод шифрування, який використовує набір протоколів узгодження ключів, основними з яких є RSA та ECDH. Його мета - забезпечити, що сеансові ключі залишаються безпечними, навіть якщо конфіденційний ключ сервера буде порушено. PFS періодично генерує нові ключі для шифрування та дешифрування з метою підвищення безпеки.

Шифрування VPN військового класу

Шифрування VPN військового рівня представляє собою стандарт шифрування, який отримав визнання від військових установ. Воно використовує надійний протокол шифрування AES. Оскільки державні організації зазвичай працюють в умовах великої конфіденційності, вони вдаються до найкращих протоколів безпеки, щоб забезпечити захист та шифрування конфіденційної інформації.

Наскрізне шифрування дуже ефективно захищає інформацію, запобігаючи її незахищеному потраплянню на проміжний сервер. Без такого шифрування ваш інтернет-провайдер може отримати доступ до ваших повідомлень, якщо він моніторить вашу діяльність.

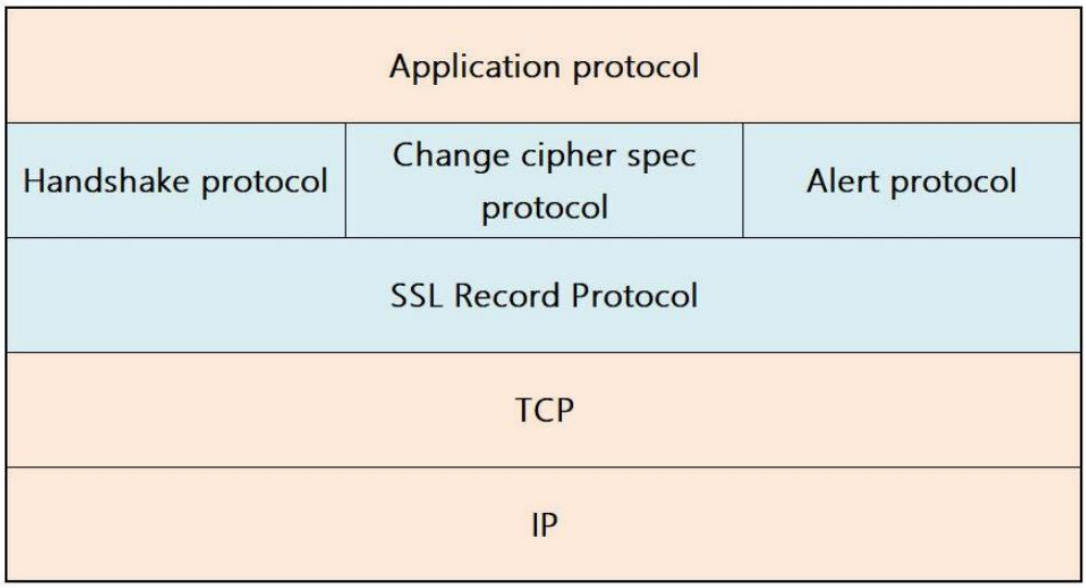


Малюнок 3.4 – Наскрізне шифрування

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

3.2 Шифрування VPN на основі SSL

SSL-протокол рукостискання включає такі протоколи рівня: протокол SSL-зміни для специфікації шифрування та протокол SSL-сповіщення. Вони використовуються для обміну інформацією про керування SSL, взаємної автентифікації між протоколами застосунків, передачі даних, узгодження алгоритмів шифрування та генерації ключів.



Малюнок 3.5 – Вміст протоколу рукостискання SSL

Серед всіх цих протоколів великої вагомості набувають протокол запису та протокол рукостискання.

Протокол запису SSL, який ґрунтується на надійному транспортному протоколі TCP, виконує основні функції, такі як інкапсуляція даних, стиснення та шифрування для протоколів вищого рівня.

Протокол рукостискання SSL, що базується на протоколі запису SSL, застосовується для аутентифікації двох сторін, узгодження алгоритмів шифрування та обміну ключами шифрування перед фактичною передачею даних.

Перевагою використання SSL є легкість обходження брандмауерів. Брандмауери NAT, як правило, налаштовані на маршрутизаторах, таких як Wi-Fi та інше мережеве обладнання, для відкидання нерозпізнаного інтернет-трафіку, який містить пакети даних без номерів портів. Оскільки зашифровані пакети IPSec не мають номерів портів за замовчуванням, вони можуть викликати проблеми з роботою IPSec VPN.

Трафік SSL прокладає шлях через порт 443, який більшість пристроїв розпізнає як безпечний порт для HTTPS. Більшість мереж допускає трафік HTTPS на порті 443.

В порівнянні з цим, OpenVPN зазвичай використовує порт 1194 для трафіку UDP, але може бути налаштований на використання портів UDP або TCP, включаючи порт TCP 443. Це робить SSL більш витонченим для обходження брандмауерів, які блокують трафік на основі портів.

Висновки до розділу 3

У висновках до третього розділу магістерської роботи розглянуті методи шифрування VPN. Пояснено, що вся інформація, яка проходить через VPN-тунель, шифрується. VPN також маскує фактичну IP-адресу, надаючи приватну, яка генерується з сервера VPN, до якого відбулося підключення. Процес шифрування включає в себе те, що VPN-клієнт шифрує запити на підключення, відправляє їх на VPN-сервер, який розшифровує та пересилає їх в Інтернет. Отримані дані знову шифруються VPN-сервером та відправляються VPN-клієнту, який розшифровує інформацію для користувача.

4. ДОСЛІДЖЕННЯ РЕАЛІЗАЦІЇ ВІДДАЛЕНОГО ПІДКЛЮЧЕННЯ КОРИСТУВАЧІВ

4.1 Формулювання проблеми та реалізація аутентифікації

Безпечний обмін даними представляє собою ключовий аспект у сучасних інформаційних технологіях при виконанні реальних завдань. Для аналізу потенційних загроз при передачі конфіденційної інформації через VPN тунель виникає необхідність дослідження безпечного з'єднання та авторизації користувачів у їх робочих областях.

Для досягнення цієї мети визначено наступні завдання:

- здійснити аналіз наявних протоколів VPN;

- аргументувати вибір технології та мережевого обладнання для створення VPN тунелю;

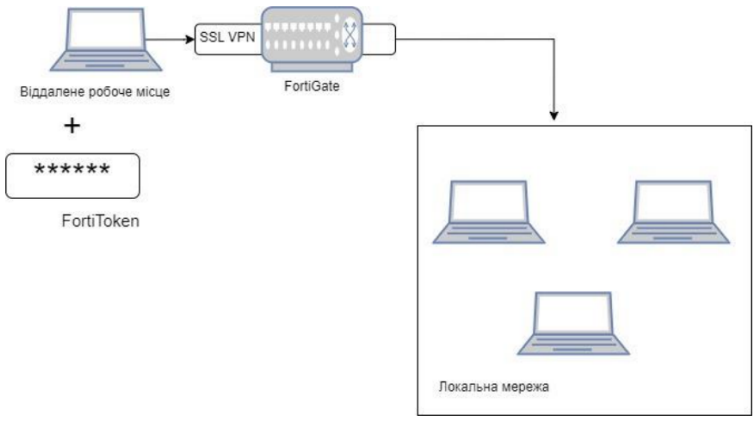
- вибрати середовище для реалізації обраної технології;

- реалізувати VPN із сервером авторизації;

- підвищити безпеку мережі VPN.

Організації все частіше використовують незалежні джерела аутентифікації для програм та веб-порталів. Дослідник SAML-аутентифікації, професор Луїсвільського університету Джеймс Левіс, визначив чимало її переваг, включаючи зменшення обтяження служби технічної підтримки, що залишається актуальним для багатьох організацій.

Застосування двофакторної автентифікації значно знижує ризик несанкціонованого доступу до онлайн-акаунтів, ефективно блокуючи 96% масових фішингових атак. Цей безпечний механізм автентифікації, що поєднує в собі цифрову ідентифікацію та двофакторну автентифікацію, розроблено для глобального застосування. Фактори автентифікації включають отримання одноразового пароля, надісланого на мобільний пристрій.



Малюнок 4.1 – Підключення з використанням мобільного токену

У цьому конфігураційному варіанті додається двофакторна автентифікація до розділеного тунелю, а саме налаштування SSL VPN для віддалених користувачів. Вона використовує один з двох доступних безкоштовних мобільних токенів FortiToken, які вже налаштовані на пристрої FortiGate.

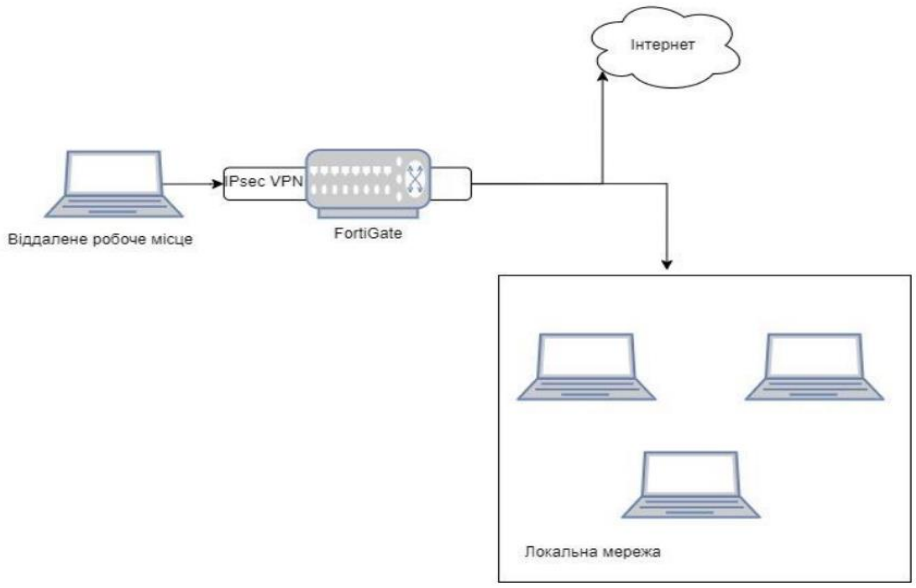
Коли FortiToken призначається користувачеві bbiliavets, система відправляє електронний лист на його електронну адресу. За допомогою інструкцій користувач повинен встановити мобільний додаток FortiToken на своєму пристрої, що призводить до активації токена.

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
```

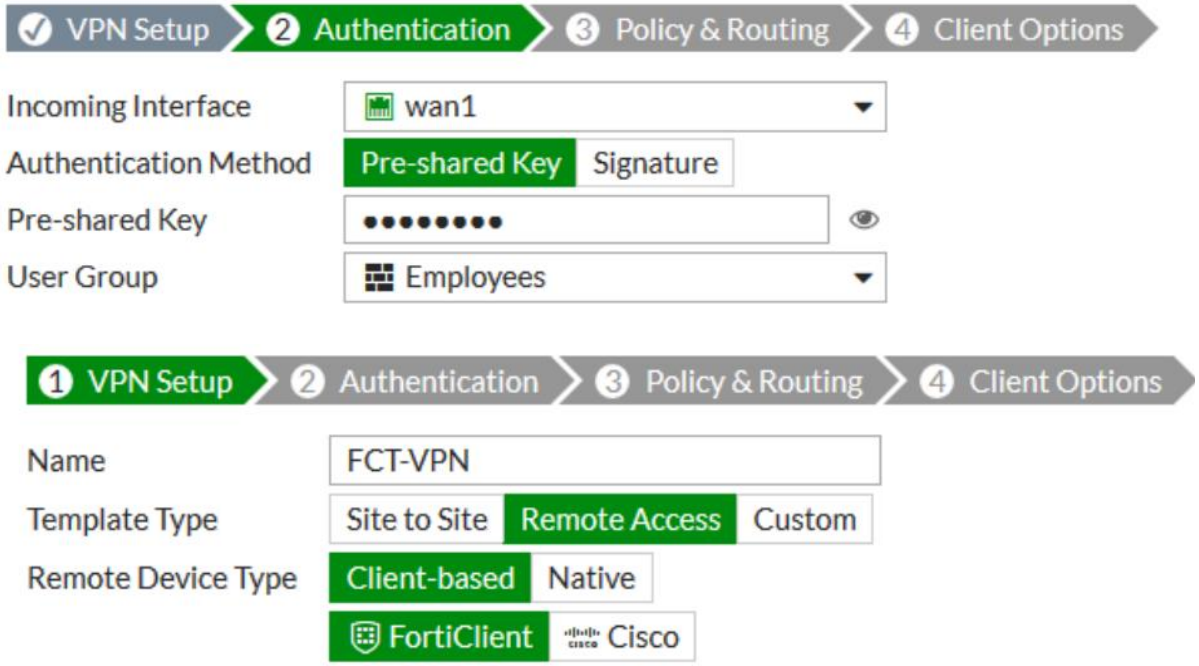
4.2 Налаштування VPN на базі IPSec

Під час дослідження було встановлено можливість дистанційного підключення користувача до корпоративної мережі через IPsec VPN, використовуючи FortiClient. Також було налаштовано направлення інтернет-трафіку віддаленого користувача через FortiGate. За необхідності можна створити користувача, який використовує двофакторну автентифікацію, або користувача LDAP. Всі ці налаштування можна виконати як у командному рядку, так і за допомогою графічного редактора, обраного для конфігурації IPsec VPN.



Малюнок 4.2 – Приклад підключення для IPsec VPN

Для створення VPN слід скористатися опцією VPN > IPsec Wizard та створити новий тунель, використовуючи відповідний шаблон. Важливо враховувати, що назва тунелю не повинна містити пробілів та обмежується 13 символами. Приклад обраних налаштувань подано на рисунку 4.3.



Малюнок 4.3 – Налаштування при створені Ipsec

Встановлюємо "Local Interface" на lan і "Local Address" на адресу локальної мережі. Задаємо діапазон IP-адрес для користувачів VPN. Важливо відзначити, що FortiOS може автоматично створити новий об'єкт брандмауера для VPN-тунелю, використовуючи назву тунелю з суфіксом "_range". Перевірте, що параметр "Увімкнути розділений тунель IPv4" не вибраний, щоб весь інтернет-трафік проходив через FortiGate.

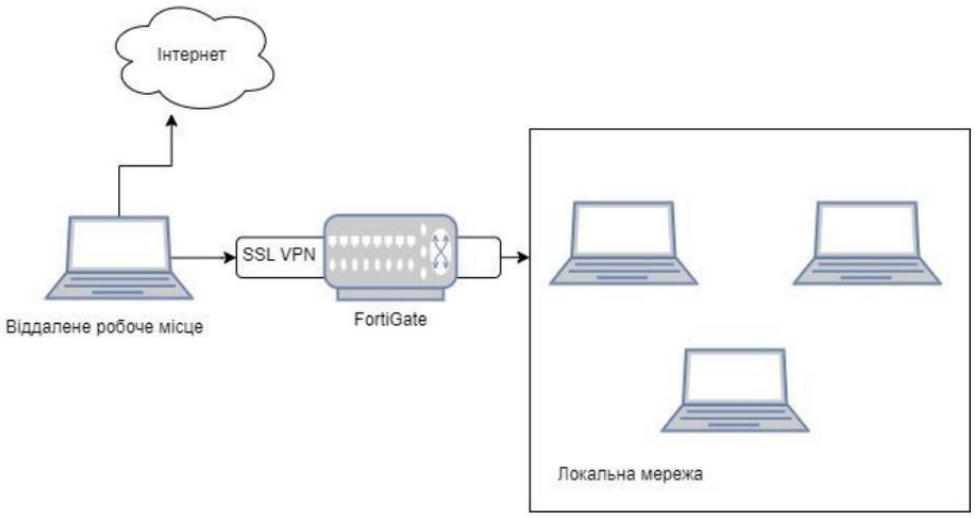
Якщо на одному інтерфейсі сервера віддаленого з’єднання існують декілька комутованих мереж IPsec VPN, кожна конфігурація фази 1 повинна мати унікальний ідентифікатор однорангового вузла, щоб відрізняти тунель, до якого підключений віддалений клієнт:

1. Перейдіть до VPN > Тунелі IPsec та відредагуйте новостворений тунель.
2. Оберіть «Перетворити на спеціальний тунель».
3. У розділі «Автентифікація» оберіть «Редагувати».
4. У розділі "Параметри однорангового вузла" встановіть для "Типів прийому" значення "Специфічний ідентифікатор однорангового вузла".

Для перегляду інтерфейсу VPN виберіть «Мережа», а потім «Інтерфейси».

4.3 Налаштування VPN на базі SSL

Це приклад конфігурації для віддалених користувачів, які забезпечують доступ до корпоративної мережі та Інтернету через режим тунелю SSL VPN за допомогою FortiClient, але мають прямий доступ до Інтернету, не пройшовши через тунель SSL VPN. (див. рисунок 3.6)



Малюнок 4.4 – Приклад підключення для SSL VPN

Інтерфейс WAN представляє собою з'єднання з постачальником послуг. Під час конфігурації вибрано статичний режим, а для подальшої експлуатації можна також використовувати режим DHCP або PPPoE. З'єднання SSL VPN встановлюється через інтерфейс WAN. Крім того, проводяться налаштування інтерфейсу та адрес 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
```

Створимо ще одне правило брандмауера SSL VPN для забезпечення доступу віддаленого користувача до внутрішньої мережі, дозволяючи переміщення трафіку від внутрішнього клієнта до віддаленого.

```
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
```

4.4 Порівняльний аналіз на базі двох протоколів безпеки

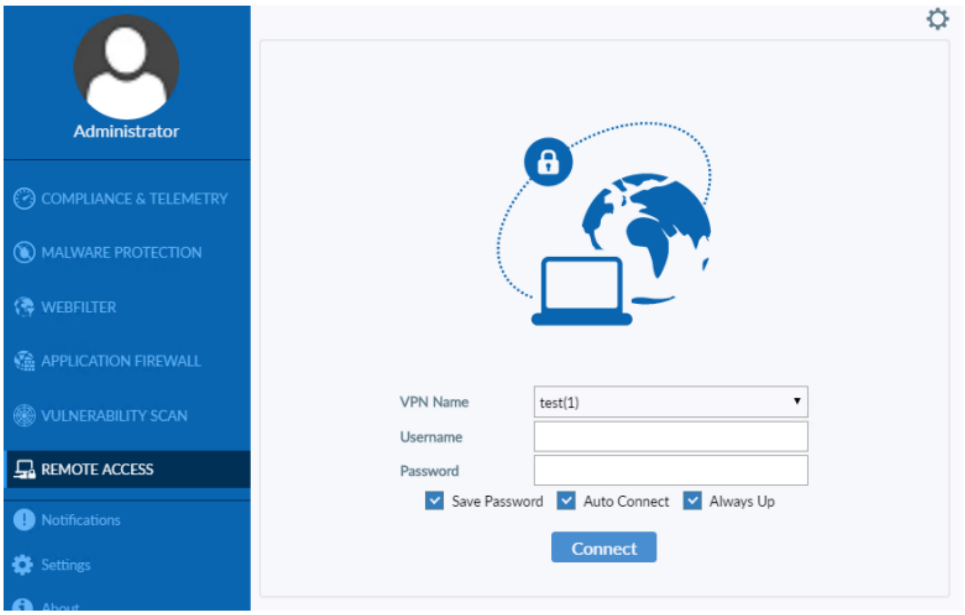
Головна відмінність між SSL VPN та IPSec VPN полягає в тому, що IPSec створює захищене з'єднання між віддаленою локальною мережею та клієнтським робочим місцем, надаючи повний доступ до ресурсів мережі. У випадку SSL VPN захищене з'єднання будується через браузер клієнтського робочого місця, надаючи доступ лише до веб-ресурсів віддаленої локальної мережі. Більшість систем в сучасному світі є веб-орієнтованими, тому використання SSL VPN у поєднанні з SAML авторизацією спрощує взаємодію користувача та не потребує додаткових облікових даних для віддалених ресурсів.

Для порівняння, використовуючи IPSec VPN, було налаштовано початкове підключення користувачів, і в результаті 10-денного моніторингу зафіксовано 53 заявки на відновлення паролів для віддалених робочих місць. Застосування технології SSL VPN та SAML авторизації значно знизило цю кількість, зафіксувавши лише 18 заявок, оскільки вона отримує дані про користувачів з Active Directory та авторизує їх через доменне ім'я без необхідності додаткових облікових записів.

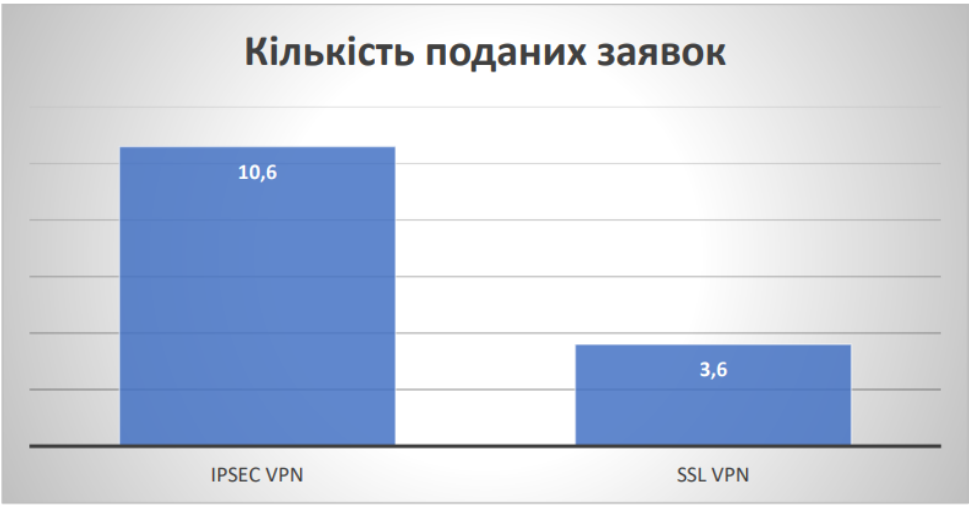
Таблиця 4.1 – Порівняння показники технологій IPSec VPN та SSL VPN

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.



Малюнок 4.5 – Віддалене підключення за допомогою FortiClent



Малюнок 4.6 – Діаграма відсоткового співвідношення

Висновки до розділу 4

Після проведеного порівняльного аналізу віддаленого підключення за допомогою технологій IPSec VPN та SSL VPN, зможливістю незалежного серверу авторизації, вказують на переваги використання протоколу SSL. Вивчення теми підтвердило, що налаштування SAML серверу можливе лише на основі SSL, згідно з

технічною документацією та доступними функціями. Практичні перевірки показали можливість реалізації єдиного входу за доменним обліковим записом, спрощуючи процес адміністрування та зберігання лог-файлів дій користувачів в одному місці.

Аналіз віддаленого підключення через обидва протоколи дав змогу визначити, що підключення через SSL VPN призводило до додаткового використання людських ресурсів. У підсумку варто відзначити, що вибір оптимального протоколу безпеки має бути індивідуальним, з урахуванням особливостей локальної мережі та завдань підприємства.

ВИСНОВКИ

У магістерській роботі успішно розв'язано наукову задачу, спрямовану на розробку методу безпечного віддаленого підключення користувачів до робочих місць. Проведений аналіз технологій забезпечення безпечного підключення та впроваджено двоетапну аутентифікацію осіб у внутрішню мережу. Це значно підвищило продуктивність працівників через доступ до файлів і системних ресурсів. Обрана технологія спрощує роботу інших працівників, які працюють в офісі або віддалено.

Проведено детальний аналіз принципів віддаленого доступу через VPN, що вказує на його розробку для безпечного забезпечення доступу персоналу до програм організації. З'ясовано, що VPN створено з метою забезпечення безпечного доступу до програм організації. Перенос даних відбувається у зашифрованому тунелі, що сприяє покращенню безпеки передачі даних, особливо важливо для віддалених працівників, які підключаються через незахищені мережі, такі як загальнодоступний Wi-Fi.

Метод віддаленої роботи, впроваджений організаціями, принесе істотні переваги, але вносить нові ризики. Описані умови для забезпечення захищеної корпоративної мережі при впровадженні системи віддаленої роботи, де використовуються протоколи віддаленого доступу. Реалізація дослідження проводилась на обладнанні сімейства FortiNet.

Отримані результати включають аналіз протоколів VPN, обгрунтування вибору технології та мережевого обладнання для створення VPN тунелю, реалізацію віддаленого підключення SSL VPN з сервером авторизації. Також розроблено методику для підвищення захисту каналу VPN, включаючи можливість багатофакторної аутентифікації та перенесення інфраструктури в хмарні середовища. Модель, розроблена в ході дослідження, успішно впроваджена 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-factorauthenticationimplementation-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_signon_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/administrationguide/989067/configuring-saml-sso-in-the-gui.

22. Бойко Ю.М. Концептуальні особливості реалізації безпровідних 79 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 інформаційнотелекомунікаційних 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) 80 [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/

ДОДАТКИ

ДОДАТОК А

1. LITERATURE REVIEW AND ANALYSIS OF THE SUBJECT FIELD

1.1 GENERAL CHARACTERISTICS OF VPN

In general, a VPN is a powerful tool for creating secure and private network connections over the open Internet and is used for both corporate and personal purposes to ensure privacy and data protection. A VPN works by routing your connection through your chosen private VPN server, not through your ISP. When data is sent to the Internet, it goes through the VPN, not directly from the computer. A VPN acts as an intermediary when connecting to the Internet, thereby hiding the IP address provided by the provider and ensuring the anonymity of the user. If data is intercepted, it remains unreadable until it reaches its destination. VPN creates a private "tunnel" from the device to the Internet and protects important data with encryption. A VPN uses encryption to protect data that is transmitted over open networks. This guarantees confidentiality and protection of information from unauthorized access. Encryption is a process used to protect data when using a VPN. It converts the information into unreadable text that can only be decrypted with the correct key. Only the VPN server and your computer know this key. The process of deciphering data is known as decryption, and it is done by using a key to convert the encoded data back into understandable information. The example of entering credit card information on a shopping website can explain how encryption works. When making any payment on the Internet, the information is encrypted, turning into an unreadable code, until it reaches its destination. Different VPN services use different encryption processes. When you connect to a VPN, a secure tunnel is created where data is encoded into an unreadable code as it travels between your computer and the VPN server. After connecting, the device is in the same local network as the VPN used. The IP address of the device is obtained from the provider's VPN server. The effectiveness of encryption depends on the selected protocols and encryption mechanism.

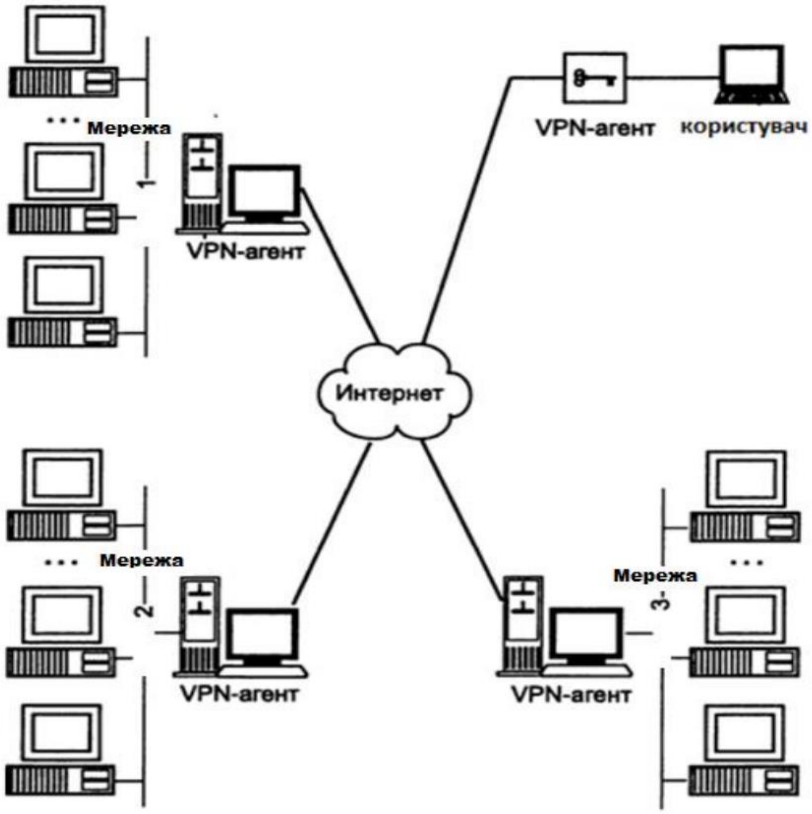


Figure 1.1 – Virtual private network

Most VPN services integrate directly with an operating system such as Windows, MacOS, iOS, or Android. This ensures the protection of the user's personal data when he uses the browser, entering, for example, bank card data [12-14]. Standalone VPN services are often used by households and small businesses. They use software that creates an encrypted connection to the private network that serves the Internet connection as a whole. There are also browser VPN extensions that are installed as browser add-ons, such as Google Chrome or Firefox. However, it is worth noting that these VPN services only protect data within the web browser where they are installed. Also, a VPN configured in a browser can be less reliable and lead to a possible leak of the IP address[15-17]. Routers with VPN support are another way to use VPN. This is convenient for use on multiple devices at the same time, as it protects each device connected to the router and ensures a constant connection to the VPN without having to configure the VPN separately for each device. It is

important to use routers specially designed to work with VPN to avoid complicated technical settings[18-20]. Corporate VPNs are often used by organizations to provide remote access to remote employees. They provide secure access to the company's internal network using individual passwords and specialized software. The implementation of such a solution requires individual development and significant IT resources.

1.2 VPN CLASSIFICATION

VPNs are divided into four main types:

1. Personal VPNs. These are VPN connections intended for individual users. They create secure and private Internet connections, bypassing firewalls and geographic restrictions.

2. VPN remote access. This type of VPN is used by businesses where employees have access to the corporate network even outside the office, while traveling or working from home.

3. Mobile VPNs. They are intended for situations where the user does not have a constant or stable connection to the Internet and needs to access the VPN through mobile devices.

4. VPN type "network-network".

This is a type of virtual private network that allows you to connect two or more local networks (usually networks in different physical locations) over the Internet. Used when multiple companies want to connect to a single shared private network, not just individual employees. Remote access VPNs allow you to use the Internet to connect to private corporate networks even outside the office.

Table 1.1 – Comparative characteristics of VPN types

	Remote access VPN	Personal VPN	Mobile VPN	VPN network
Connection	The user connects to a private network.	The user connects to the Internet through a third-party server.	The user connects to a private network.	The network is connecting to another network.
Software	Usually, users need to install software on their device or configure the operating system.	Users install the VPN service software on their device.	Usually, users need to install software on their device or configure the operating system.	Users do not need to run additional software.
It is best to use for:	Connecting to your company network or any other private network from home or another remote location.	Protecting your privacy and bypassing geographic restrictions on the Internet.	Achieving a permanent connection to a private network while using an unstable Internet connection.	Combining two or more networks to create one unified network.

The Internet is an unreliable link in communication. VPN encryption is used to keep data private and secure as it travels to and from the private network.

There are several methods of using a remote access VPN, such as:

1. People who often change their place of residence can use a remote access VPN to connect to their company's network via Wi-Fi in a hotel or any public place. This allows them to access the same files and software they would have in the office. Plus, a VPN protects their data from anyone who might be snooping on public Wi-Fi.

2. A person who works from home can use a remote access VPN to connect to the corporate network from their home. The computer works as if it is connected to the company's network in the office, and the data remains secure when it travels over the public Internet[21-24].

3. To use VPN remote access on your device, you usually need to install client software or configure your device's operating system to connect to the VPN. There must also be a VPN server at the end of the network. Multiple client devices can be connected because different users can connect to the server.

4. First, the VPN server verifies whether the user has access to the network by requiring a password or using biometrics such as a fingerprint for identification. Some solutions allow you to use security certificates for automatic user authentication in the background, which facilitates fast connection. This is especially useful when a user needs to connect to multiple VPN servers, for example to access different networks.

5. After passing the user authentication procedure, the client and the server create an encrypted tunnel between themselves. This is a protective layer of encryption that ensures the safety of traffic when it is forwarded over the Internet. There are several different VPN protocols that can be used to set up an encrypted tunnel, including IPsec and SSL.

Examples of business remote access VPNs include:

- Access server through OpenVPN, which provides the possibility of free simultaneous VPN connection for two users.

- Cisco AnyConnect, which integrates with Cisco enterprise security solutions.

Individual VPN services A private VPN service sets up a connection between your device and a VPN server that acts as an intermediary between your device and the web services you need to access. Personal VPN services differ from remote access VPNs in that they do not provide access to private networks. Instead, a personal VPN provides access to the public Internet through an encrypted connection [25-29]. There are many reasons for using a personal VPN, among the most popular are:

1. Streaming movies and series, or listening to music that is not available in your geographic region. For example, you can connect to a VPN server in the US to access American Netflix with its large selection of content.

2. Bypassing restrictions imposed by your ISP's firewalls and protecting your web traffic from potential government surveillance.

3. Hiding your device's IP address to protect yourself from targeted attacks. Gamers are increasingly using short but intense DDoS attacks to block competitors and ensure an unfair victory, which is impossible with VPNs.

4. Protection of privacy on the Internet, as Internet providers sometimes interfere with the connection, slow down the speed or limit access due to the allocation of excessive traffic.

Personal VPN programs are available on various types of devices, including smartphones. They usually offer a large number of servers to choose from. If privacy is important, you can connect to a local server to get the fastest speed. When you connect to a VPN, all your internet traffic goes through the VPN provider's server. Since the connection is encrypted, the IP address is hidden, which allows you to access geo-restricted content from other countries without much effort.

A few highly rated personal VPN services include:

- ExpressVPN

- NordVPN

- Surfshark

- IPVanish

Mobile VPN are typically used to provide reliable access for employees using mobile devices. This is especially relevant in situations where the stability of the connection may not be sufficient, but it is necessary to maintain access to various resources[30-32]. For example, military personnel stationed at checkpoints throughout Ukraine use tablets and mobile VPN to provide access to various databases and check information on persons or vehicles that may pose a threat.

Figure 1.2 – Example of connection using a mobile VPN

Mobile VPN support various authentication methods, including passwords, physical tokens such as smart cards, biometric devices, fingerprint scanners, and facial recognition systems. In some cases, they use security certificates for automatic background user authentication.

A mobile device can switch between networks, such as cellular or Wi-Fi, while maintaining an active connection. This may cause the physical IP address to change, but the

logical IP address used for the VPN tunnel remains constant. This approach ensures the immutability of the virtual network connection, allowing the user to work without interruption even when switching networks. Even if the device has been turned off to save battery power, the VPN connection remains available after the device is turned on. Now, regarding the network-to-network VPN:

Compared to a remote access VPN, which is designed for individual users, a network-to-network VPN connects two separate networks. For example, if a company has two offices in the east and west, then a "network-to-network" VPN allows you to combine them into a single network.

There are several technologies that can be used to implement a network-to-network VPN, including IPsec, DMVPN, and L3VPN.

There are two main options in this VPN category:

1. Intranet-based VPN: when a VPN connection is created between networks belonging to the same company. This allows the company to create a single global network covering two or more offices. Company users access resources from other LANs as if they were physically connected.

2. Extranet-based VPN: When the connected networks belong to different companies, such a VPN combination is called an extranet-based VPN. This type of VPN is used, for example, when a company wants to connect to the network of a service provider [33, 34].

There are three main methods of implementing a network-to-network VPN:

1. Using an IPsec tunnel.

2. Using Dynamic Multipoint VPN (DMVPN).

3. Using VPN at the third level (L3VPN).

An IPsec tunnel is used to bridge networks, just as it connects individual connections to a private network in a remote access VPN. In the case of a network-to-network VPN, an

IPsec tunnel encrypts traffic between connected networks. This can be implemented in two ways:

- A route-based IPsec tunnel that carries all traffic between networks. - A security policy-based IPsec tunnel that sets rules to control allowed traffic and interactions between networks. Such IPsec tunnels can be configured using firewalls and network routers.

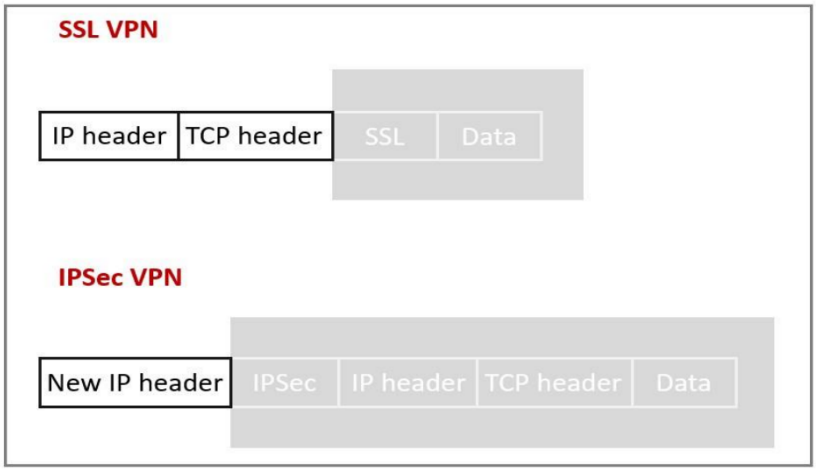


Figure 1.3 – Composition of SSL and Ipsec protocol packets

The Dynamic MultiPoint VPN (DMVPN) technique is proposed as a response to the limitations of IPsec tunnels, which connect only two points to each other. In contrast to this approach, DMVPN allows you to combine networks using a DMVPN hub router and use dynamic IP addresses.

While the quality of service in IPsec and DMVPN tunnels running on top of the Internet can be erratic, multiprotocol MPLS Layer 3 label-switched networks can guarantee reliable and stable communications. MPLS is a method of routing network packets over different transport media, such as fiber or satellite, using different protocols. This approach allows network providers to create a VPN at layer 3, which is based on the network layer of the OSI model. Typically, these MPLS VPNs are deployed by telecommunications providers.

Network providers can create separate virtual networks for each customer that are transmitted over the global network. These virtual networks provide isolation from each other, even if they share physical network resources. With MPLS VPN, you can prioritize different types of traffic, such as voice traffic, to ensure the best quality of service. Control over the routing of network traffic is essential to ensure stable and optimized performance.

Despite the advantages of private WANs, they can be expensive, so many companies prefer cheaper Internet-based VPNs, except in situations where critical latency is important, such as in power grid monitoring and maintenance applications.

1.3 OVERVIEW OF EXISTING VPN SECURITY PROTOCOLS AND THE TECHNOLOGIES ON WHICH THEIR WORK IS BASED

In this section, we will look at the various VPN security protocols and the technologies behind their operation. VPNs (Virtual Private Networks) are used to provide security and privacy on data networks, and there are several key protocols and approaches that help achieve these goals. To a large extent, we will also consider the technologies on which VPN work is based. This includes data encryption, user authentication (often using passwords, physical tokens, or biometrics), and encryption key management.

To implement different VPN usage scenarios, there are different types of protocols that are responsible for security, traffic encryption and other aspects of operation. Choosing a specific VPN protocol is of great importance when designing solutions in this area. Three of the most common and important protocols are OpenVPN, IPSec SSL, and the relatively new WireGuard, which appeared quite recently and caused discussion among specialists. At the same time, there are other protocols that, although they are outdated, can be used for specific tasks.

The choice of a suitable VPN protocol depends on several factors and circumstances of use:

1. Devices. Different devices support different protocols, so compatibility is important to consider.

2. Network. The availability of some services may be limited in certain locations or countries, so the choice of protocol may depend on these restrictions. For example, some VPN providers operate in China, where most of their other competitors are blocked.

3. Productivity. Some protocols may have better performance, especially on mobile devices, while others may be more practical in large corporate networks. 4. Threat model. Different protocols may manifest themselves in different situations, and some may be less secure, requiring appropriate security measures.

Let's consider some of the most common protocols: PPTP (Point-to-Point Tunneling Protocol): One of the oldest VPN technologies is PPTP, developed by Microsoft. It uses two channels for control and data transmission and has its own characteristics.

PPTP is available on all versions of Windows and is widely supported by many operating systems. Despite the relatively high speed, it should be noted that PPTP is not the most reliable protocol, and it does not restore the connection as quickly after interruptions as, for example, OpenVPN.

At this point, PPTP is deprecated and Microsoft recommends using other VPN solutions, especially given the importance of security and privacy.

Of course, if your main purpose of using a VPN is to unblock content, PPTP may be fine, but it's worth considering more secure alternatives. SSTP (Secure Socket Tunneling Protocol) is a proprietary solution from Microsoft. Although SSTP is not as common among VPN protocols as PPTP, it has a much higher level of security and does not have serious problems in this regard.

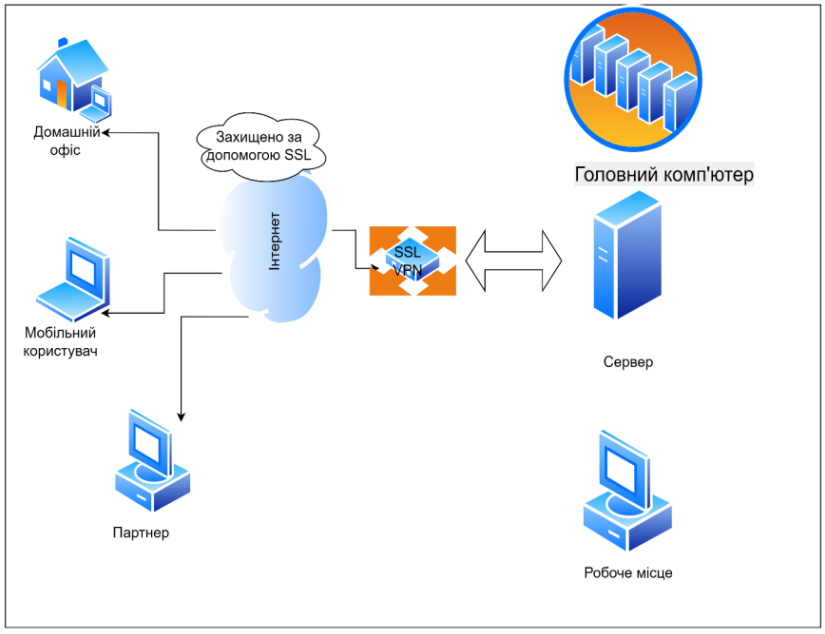


Figure 1.4 – Connection using SSL

SSTP uses SSL to transmit traffic over TCP port 443, making it useful in restricted networks such as China, where other VPNs may be blocked. Although SSTP can theoretically be installed on Linux, this protocol is mainly used by Windows systems. SSL can protect application layer protocols such as POP3 or FTP and requires an SSL certificate on the server to work. Using SSL, the secure connection between the client and the server performs two main functions: authentication and data protection.

SSL has two layers: the lower layers in a multi-layer transport protocol such as TCP are used to encapsulate different protocols. For each nested protocol, SSL provides conditions in which the server and client can authenticate themselves, secure data transmission, and exchange keys before application layer protocol data transmission begins.

SSL has numerous advantages, including ease of use, no need for additional software, and secure remote access. In terms of performance, SSTP is fast, stable and reliable.

IPsec (Internet Protocol Security) is a set of protocols for protecting data transmitted over the IP network. Unlike SSL, which operates at the application level, IPsec operates at

the network level and can interoperate with many operating systems without the need for third-party software.

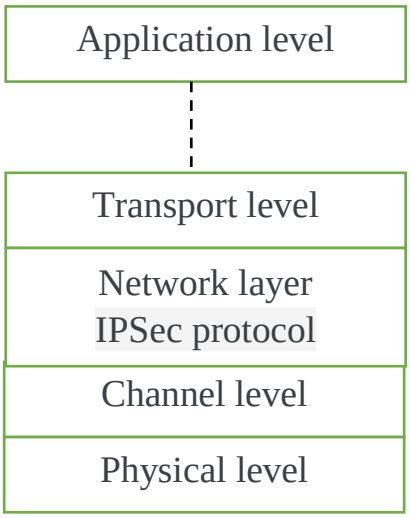


Figure 1.5 - Placement of the IPsec protocol in the OSI module

IPsec has become very popular for use with L2TP or IKEv2 protocols. IPsec provides encryption of the entire IP packet using two key components:

- Authentication Header, which places a digital signature on each packet;

- Encapsulating Security Protocol, which guarantees confidentiality, integrity and authentication of packets during their transmission.

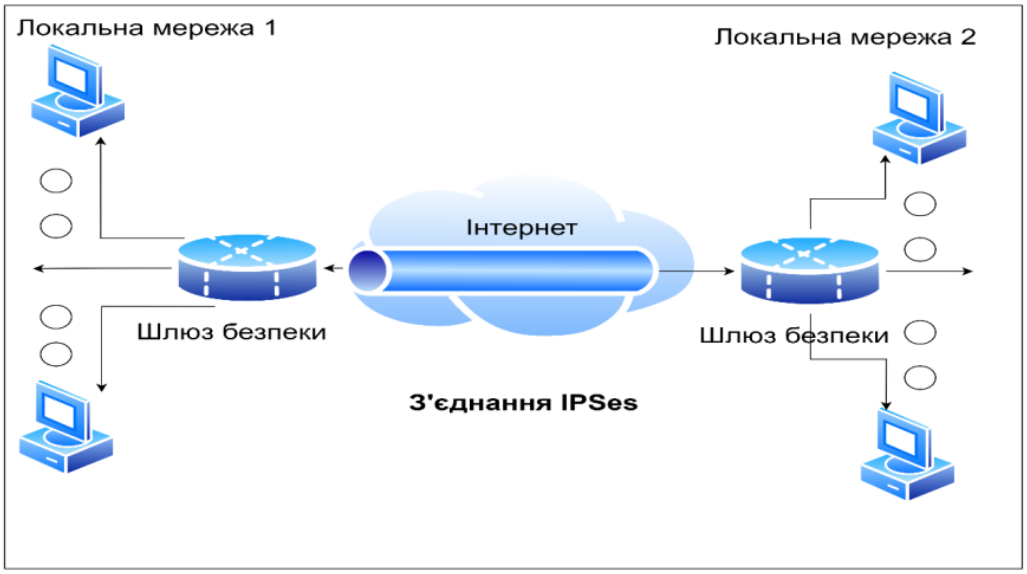


Figure 1.6 An example of an IPsec-based connection

The L2TP/IPsec protocol was first introduced in 1999 as an upgrade of the L2F (Cisco) and PPTP (Microsoft) protocols. Because L2TP does not provide encryption or authentication by itself, it is often used in conjunction with IPsec. It is supported by many operating systems.

L2TP/IPsec is considered secure and has no major identified issues. This protocol can use 3DES or AES encryption, but 3DES is now considered obsolete and rarely used. In some cases, the use of the L2TP protocol may face problems due to the standard use of UDP port 500, which is blocked by some firewalls. The L2TP/IPsec protocol provides high reliability of data transmission, its configuration is simple and it is supported by all modern operating systems. However, L2TP/IPsec double-encapsulates data in transit, making it less efficient and slower than other VPN protocols.

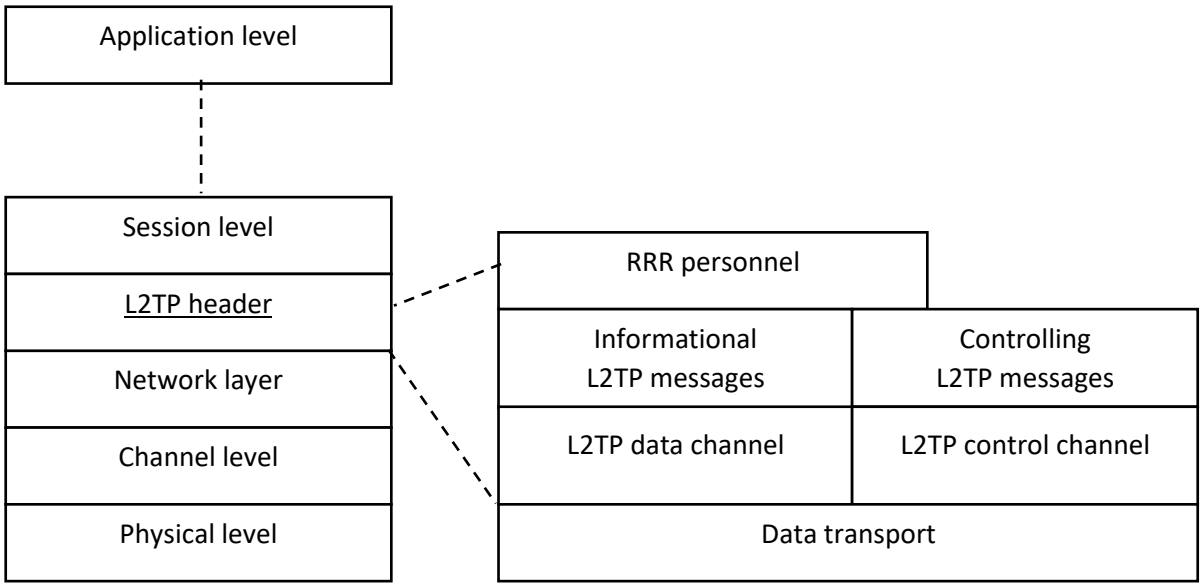


Figure 1.7 – Components of the L2TP protocol

IKEv2/IPsec (Internet Key Exchange version 2) is an IPsec protocol designed for mutual authentication, creation and management of communication security. It was jointly developed by Microsoft and Cisco, and there are open implementations such as OpenIKEv2, Openswan, and strongSwan. In addition, thanks to the support of the Mobility and Multi-homing Protocol, IKEv2 is well adapted to changes in network conditions. This makes it an ideal choice for mobile users who switch between different networks or access points.

IKEv2/IPsec supports various cryptographic algorithms, including AES, Blowfish, and Camellia, including 256-bit keys. And in terms of performance, IKEv2 is faster than OpenVPN in many cases, particularly on mobile devices. This protocol is supported on various operating systems, including Windows, Mac OS, iOS, and certain Android devices.

OpenVPN is a popular open source VPN protocol developed by OpenVPN Technologies. It is characterized by stability and high data transfer speed. OpenVPN uses both TCP and UDP and can be an alternative to IPsec and SSL, especially when some VPN protocols are blocked by the ISP. Using OpenVPN requires client software to be installed, and many VPN providers develop their own software for different operating systems and devices. This protocol can work on different TCP and UDP ports and is compatible with many platforms, including Windows, Mac OS, Linux, Apple iOS and Android.

WireGuard is a new VPN protocol that the developers position as an advanced alternative for most IPsec, OpenVPN and SSL use cases. WireGuard is characterized by high security, performance and ease of configuration. All IP packets arriving at the WireGuard interface are encapsulated via UDP. WireGuard uses modern cryptographic tools, including Curve25519 for key exchange, ChaCha20 for encryption, Poly1305 for data authentication, SipHash for key hashing, and BLAKE2 for hashing. Compared to the OpenVPN code, the WireGuard code is significantly smaller (4,000 lines versus several hundred thousand), making it more accessible for vulnerability research. WireGuard 1.0.0 was recently introduced, which includes WireGuard components in the core Linux 5.6 kernel. The code included in the Linux kernel underwent an additional security audit by an independent firm and found no issues.

Table 1.2 – Comparative characteristics of security ducts

Sign	PPTP	SSTP	L2TP/IPsec	IKEv2/IPsec	OpenVPN	WireGuard
Company the developer	Microsoft	Microsoft	L2TP — joint development of Cisco and Microsoft, IPsec — Internet Engineering Working Group	IKEv2 is a joint development of Cisco and Microsoft, IPsec is a working group for the development of the Internet	OpenVPN Technologies	Jason A. Donenfeld
License	Proprietary	Proprietary	Proprietary	Proprietary, but there is an open source implementation protocol	GNU GPL	GNU GPL
Deployment	Windows, MacOS, iOS, for a while GNU/Linux. Works from the device without requiring the installation of additional software	Windows. Works from the device without requiring the installation of additional software	Windows, Mac OS X, Linux, iOS, Android. Many OS (including Windows 2000/XP +, Mac OS 10.3+) have built-in support, no need to install additional software	Windows sh+, Mac OS 10.11+, and most mobile OS have built-in support	Windows, Mac OS, GNU/Linux, Apple iOS, Android and routers. It is necessary to install specialized software that supports work with this protocol	windows, Mac OS, GNU/Linux, Apple iOS, Android. Instal WireGuard itself, and then configure according to the manual
Encryption	Uses Microsoft Point-to-Point Encryption (MPPE), which implements RSA RC4 with a maximum of 128-bit session keys	SSL (all parts except TCP and SSL headers are encrypted)	3DES or AES	Implements a large number of cryptographic algorithms, including AES, Blowfish, Camellia	Uses the OpenSSL library (implements most of the popular cryptographic standards)	1-RTT key exchange, Curve2551 9 for ECDH, RFC7539 for ChaCha20 and Poly1305 for authentication encryption and BLAKE2s for hashing.
Ports	TCP port 1723	TCP port 443	UDP port 500 for initial key exchange and UDP port 1701 for initial L2TPconfiguration, UDP port 5500 for NAT bypass	UDP port 500 for initial key exchange and UDP port 4500 for NAT bypass	Any UDP or TCP port	Any UDP port

Sign	PPTP	SSTP	L2TP/IPsec	IKEv2/IPsec	OpenVPN	WireGuard
Security flaws	Has serious vulnerabilities. MSCHAP-v2 is vulnerable and the RC4 algorithm is vulnerable to the Bitflippin attack	No serious security flaws were found	3DES is vulnerable to Meet-inthe-middle and Sweet32, but AES has no known vulnerabilities. However, it is believed that the IPsec standard has been compromised.	Couldn't find any information on existing security flaws other than the IPsec report leak incident	No serious security flaws were found	No serious security flaws were found

1.4 OVERVIEW OF MODERN APPROACHES TO CONFIGURING VPN FOR REMOTE CONNECTION TO A CORPORATE NETWORK

In today's world, remote work is becoming more and more popular, and it requires a reliable and secure way to access corporate networks. In this section, we will look at modern approaches to configuring virtual private networks (VPNs) to provide remote connectivity to corporate networks.

1. Use of SSL VPN: A series of SSL VPN technologies allows users to securely connect to corporate resources through a web browser, providing a high level of convenience and security. This method is well suited for users of various operating systems and is easy to configure.

2. Using IPsec VPN: IPsec (Internet Protocol Security) is a popular method for creating secure VPN connections for remote users. It provides a high level of security by means of encryption and authentication of IP packets.

3. Using L2TP/IPsec and IKEv2: A combination of L2TP, IPsec and IKEv2 protocols is used to create stable and secure VPN connections, especially for large corporations with high security requirements.

4. Using WireGuard: The newest VPN protocol, WireGuard, uses modern cryptographic methods to create fast and secure VPN connections. These different

approaches make it possible to choose the optimal solution for configuring remote VPN connections depending on the needs of security, convenience and performance.

When using remote access through a browser, the user visits the corporate portal, which is configured by the network administrator on the ASA. On this portal, the user can find the following main sections depending on the type of available resources:

- Web applications (Web Applications);

- View networks (Browse Networks);

- Access to programs (Application Access);

- Terminal servers (Terminal Servers).

Fortinet also has configuration options for IPsec and SSL VPN. SSL VPN includes two modes: tunnel mode and web mode. The choice of mode and level of security depends on the specific needs and features of the environment. In tunnel mode, the SSL VPN client encrypts all traffic from the remote computer and sends it to the FortiGate over the SSL VPN tunnel using an HTTPS connection. Web mode provides clientless access to the network through a web browser with built-in SSL encryption. It is easier to configure, does not require a separate client to be installed on the endpoint, but is limited in supporting some applications and requires more resources on the FortiGate.

IPsec VPN, as mentioned earlier, is a standard protocol that allows the use of various endpoint connection solutions, including FortiClient. This is a standard protocol that uses certain ports and can sometimes be blocked by ISPs.

Conclusions to section 1

Summarizing the first chapter of the thesis, we defined a virtual private network, considered different construction methods, and discussed security protocols and equipment needed for its implementation.

ДОДАТОК Б

Кравчина Т.В., *магістрант, група 601-дТ*

Національний університет «Полтавська політехніка імені Юрія Кондратюка»

Керівник – проф. М.А. Штомпель

РОЗРОБКА ЗАХИЩЕНОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

Сучасні загрози телекомунікаційним мережам, такі як кібератаки, шпигунство та злами, ставлять під загрозу конфіденційність та цілісність інформації організацій. Важливо розробляти і впроваджувати захисні заходи для забезпечення безпеки та надійності телекомунікаційних мереж, оскільки втрата даних може призвести до серйозних фінансових та репутаційних втрат для організацій. Розробка захищеної телекомунікаційної мережі - ключовий аспект для збереження конфіденційності і цілісності даних в епоху загострених кіберзагроз. Головне - це аналіз та вибір технологій та рішень, які найкраще відповідають потребам організації з урахуванням загроз, бюджету та інфраструктури для ефективного захисту телекомунікаційних мереж.

Тому у роботі розглянуто тенденції у вдосконаленні захисту телекомунікаційних мереж, визначено віртуальну приватну мережу, розглянуто різні методи побудови та протоколи безпеки та обладнання, необхідне для її реалізації.

Міністерство освіти та науки України
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
КАФЕДРА АВТОМАТИКИ, ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ

Розробка захищеної телекомунікаційної мережі організації

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Виконала:
Студентка групи 601дТТ
КРАВЧИНА Т.В.

Керівник:
професор, д.т.н.
Штомпель М.А.

Полтава 2024

МЕТА, ПРЕДМЕТ, ОБ’ЄКТ ДОСЛІДЖЕННЯ

МЕТА

Створення VPN тунелю для з'єднання віддалених користувачів з корпоративною мережею за допомогою технології SAML та налаштування доменної аутентифікації – основна мета

ПРЕДМЕТ ДОСЛІДЖЕННЯ

Метод безпечного віддаленого підключення користувачів

ОБ’ЄКТ ДОСЛІДЖЕННЯ

Отримання доступу користувачів до мережі за допомогою сервера аутентифікації SAML – процес, що включає в себе використання незалежного серверу

ІННОВАЦІЙНІСТЬ НАУКОВОГО ВНЕСКУ ТА ПОДАЛЬШИЙ РОЗВИТОК ДОСЛІДЖЕННЯ

Інноваційність наукового внеску

Наведена методика створення VPN тунелю в державній організації з використанням технології SAML та двофакторної аутентифікації, яка включає в себе мобільний токен або брелок із періодичною генерацією унікального коду

Подальший розвиток

- Розробка методики для підвищення безпеки VPN-каналу, яка включає можливість багатофакторної аутентифікації, такої як сканування відбитків пальців або розпізнавання обличчя.
- - Розробка підходу для забезпечення оптимальних умов для міграції інфраструктури до хмарних середовищ, наприклад, Azure.

КЛАСИФІКАЦІЯ VPN

Основні види VPN

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

Основні протоколи VPN

- IPSec
- SSL
- OpenVPN

ПРОТОКОЛ IPSEC

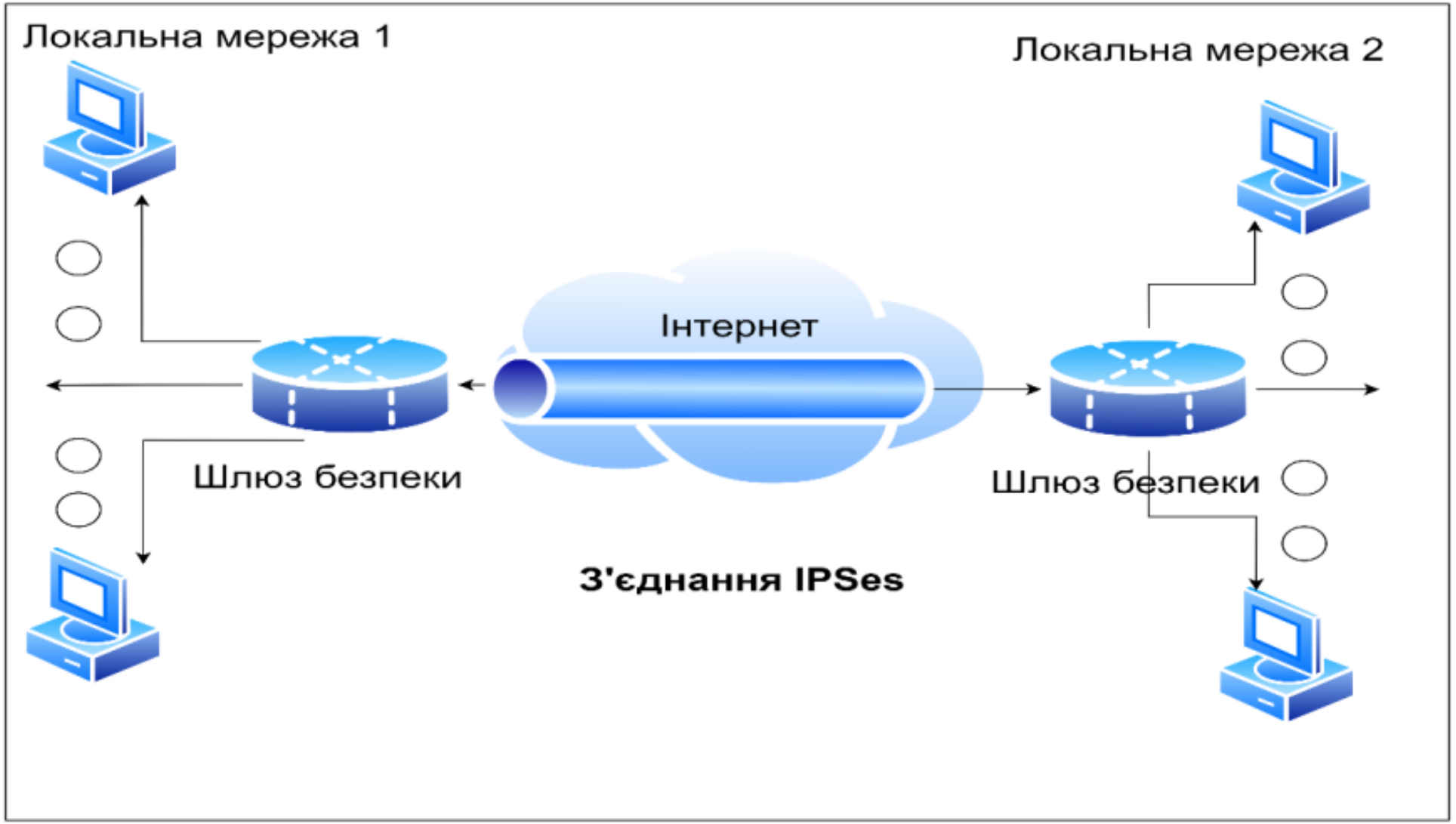


Рисунок 1 – Приклад з’єднання на базі IPsec

ПРОТОКОЛ SSL

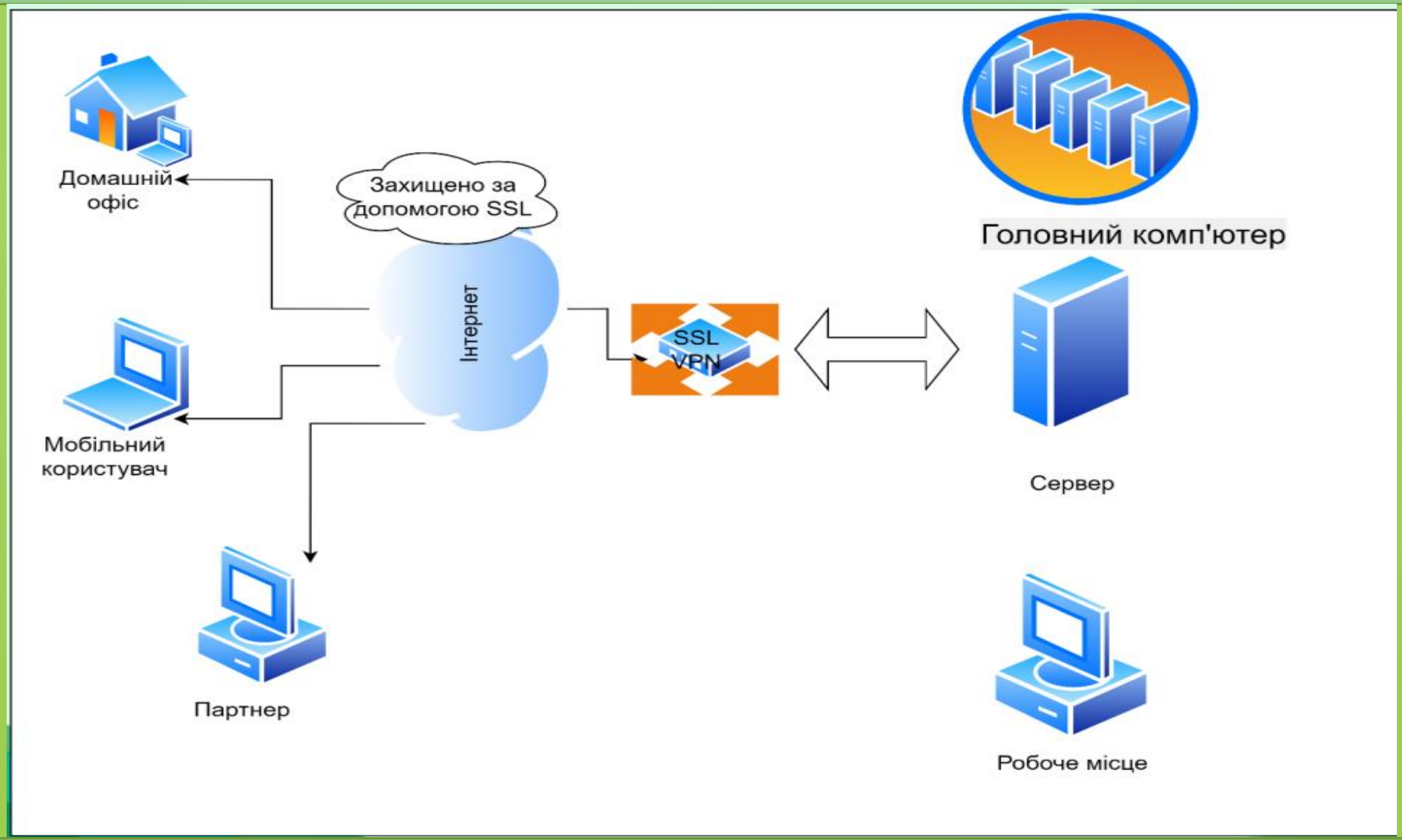


Рисунок 2 – Підключення з використанням SSL

СХЕМА СКЛАДОВИХ VPN

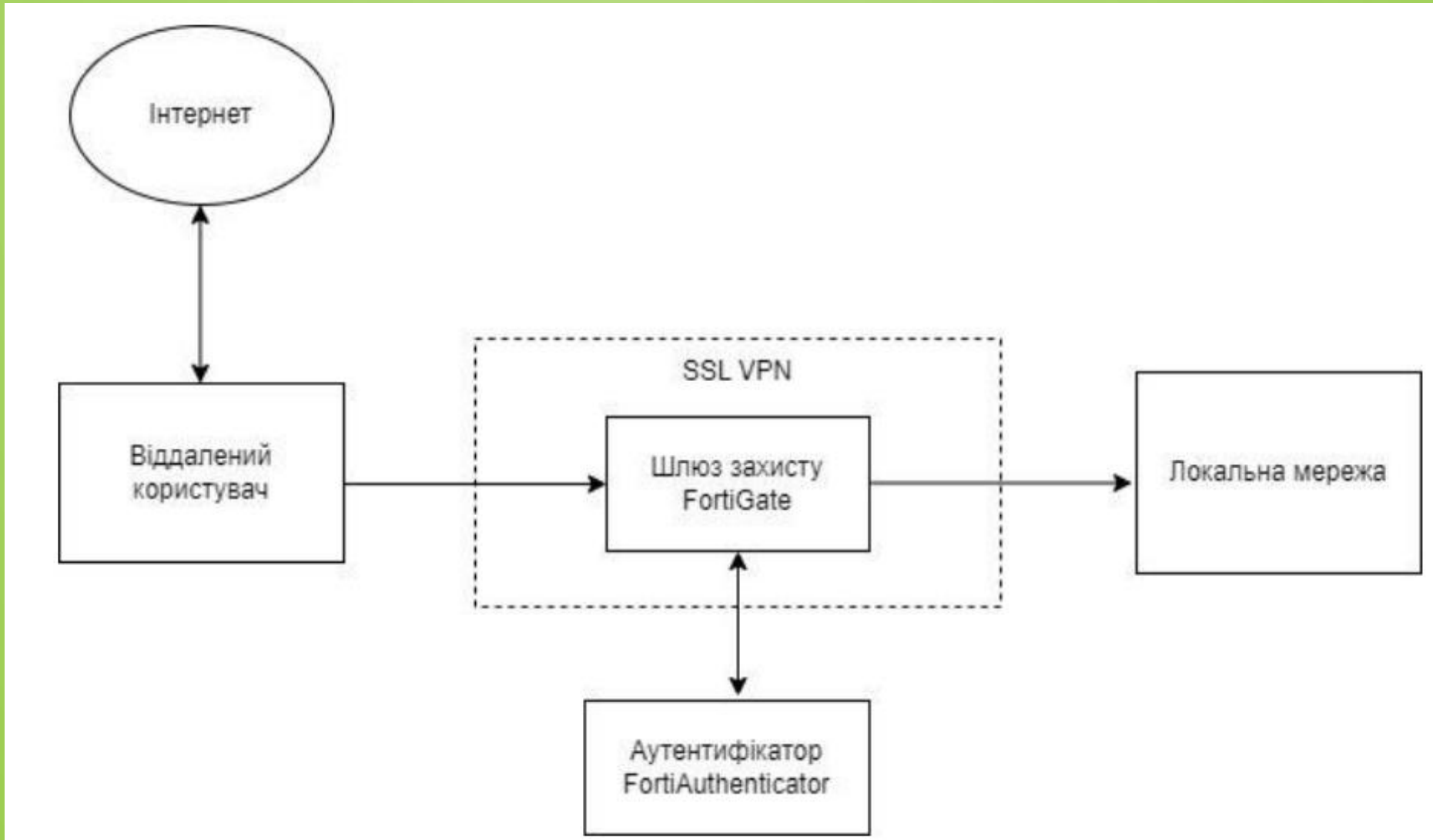


Рисунок 3 – структурна схема VPN

ШИФРУВАННЯ VPN

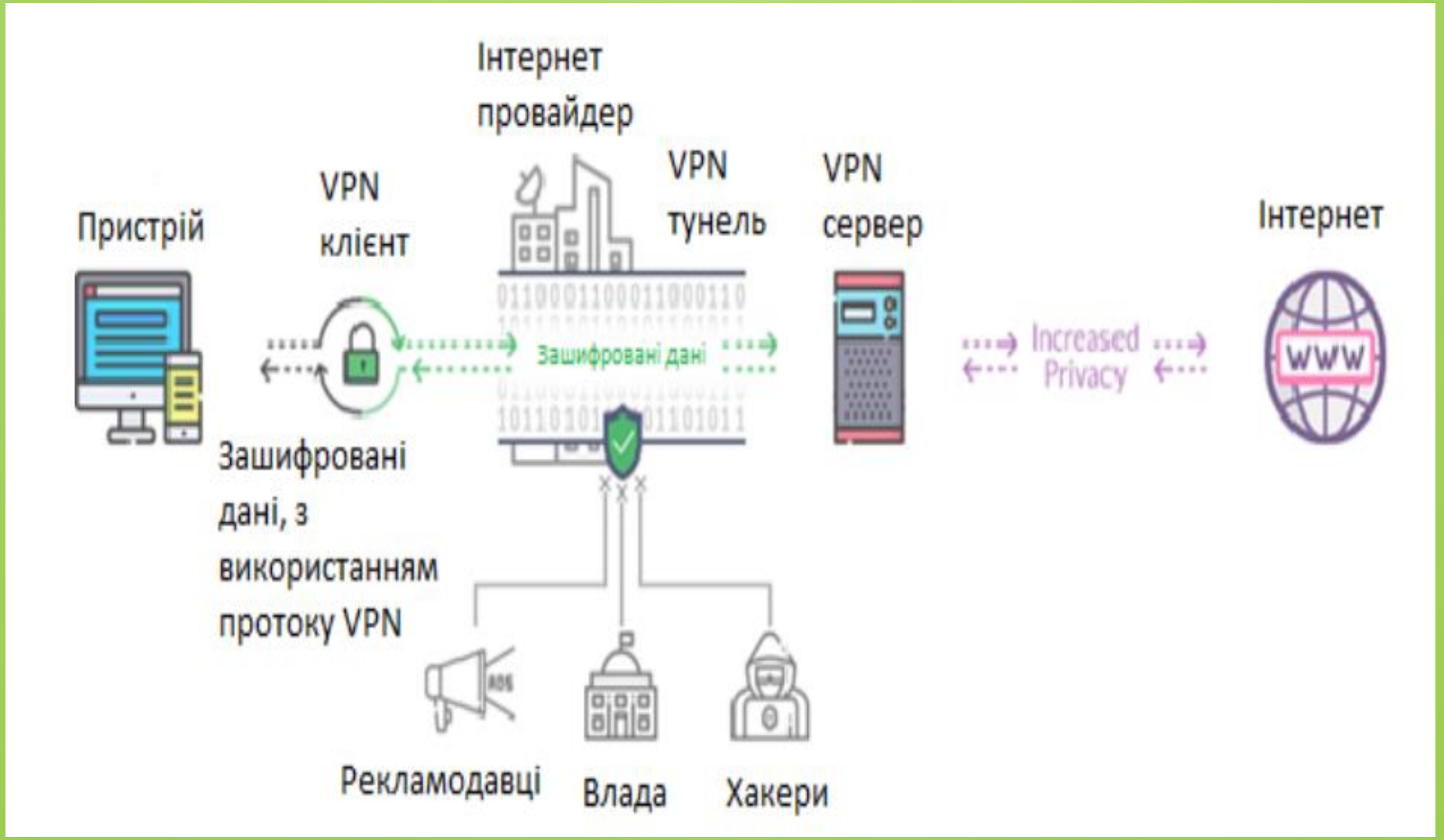


Рисунок 4 – Схема шифруванняVPN

ТЕХНОЛОГІЯ SAML

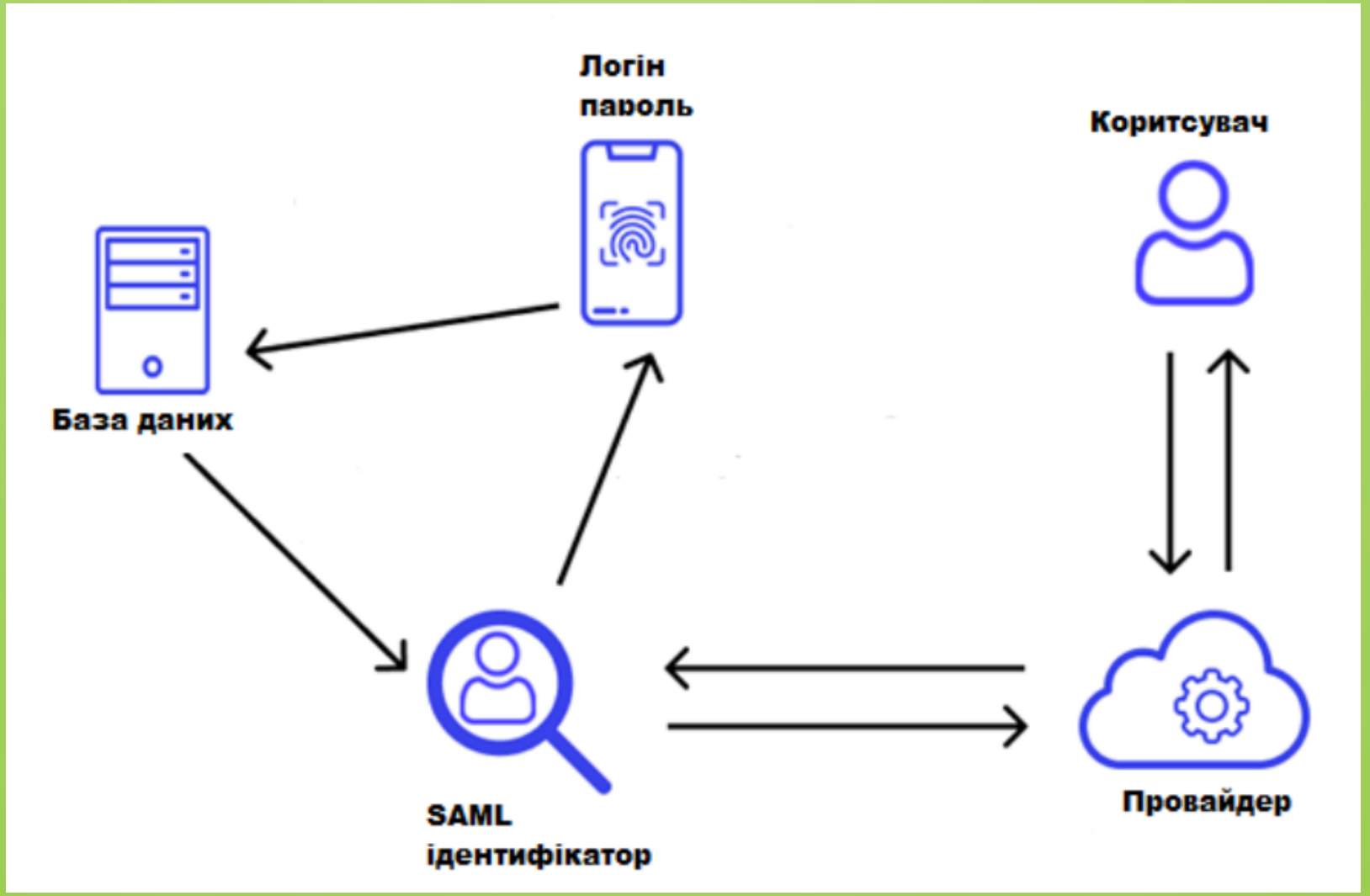


Рисунок 5 – Принцип роботи технології SAML

АНАЛІЗ ДОСЛІДЖЕННЯ

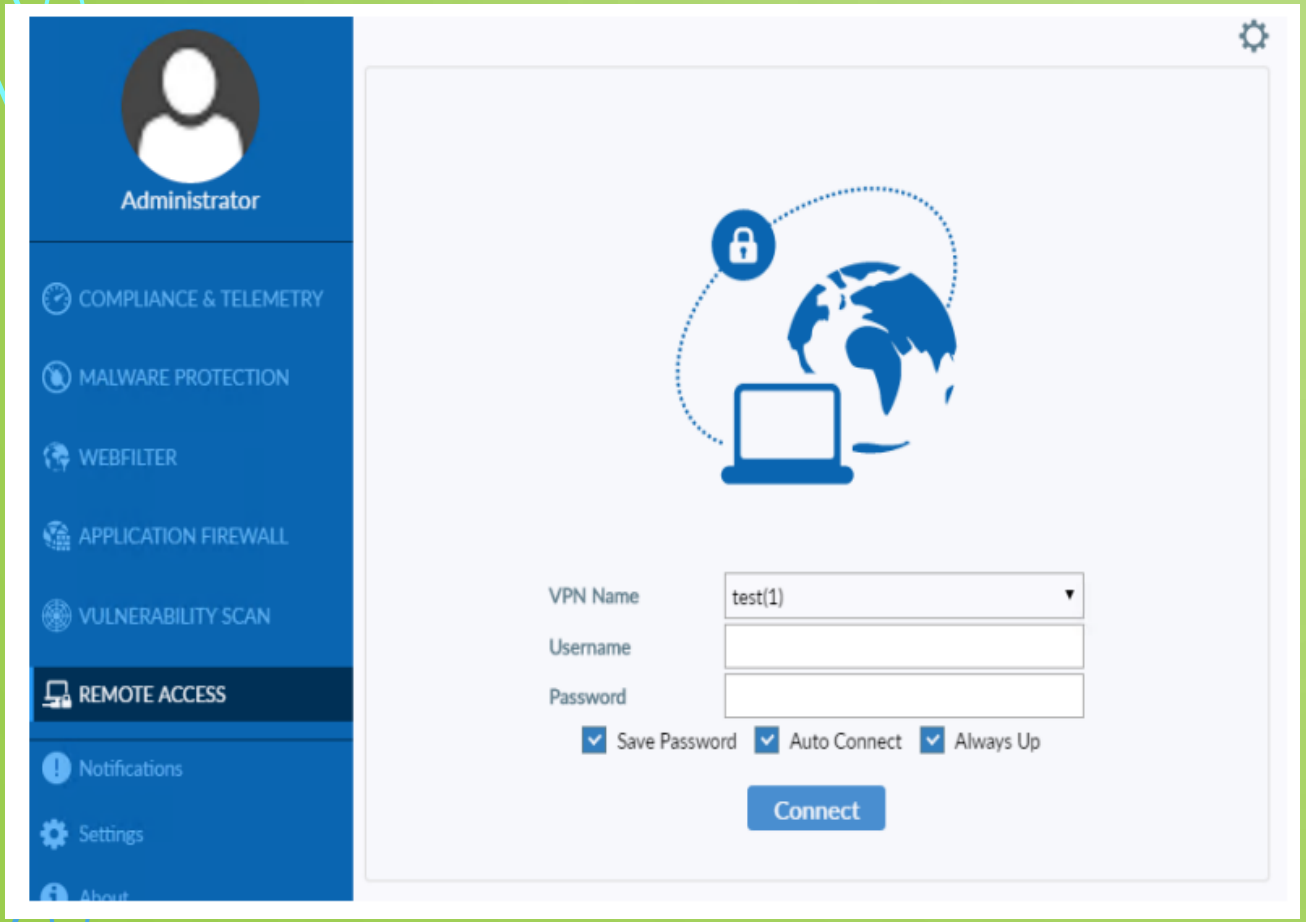


Рисунок 6 – Віддалене підключення за допомогою FortiClent

Рисунок 4.8 – Діаграма відсоткового співвідношення

ВИСНОВКИ

1. Проведено аналіз існуючих вразливостей VPN
2. Обгрунтовано вибір технології та мережевого обладнання для створення VPN тунелю
3. Реалізовано віддалене підключення через SSL VPN із сервером авторизації
4. Розширено методику підвищення безпеки VPN-каналу, включаючи можливість багатофакторної аутентифікації, такої як сканування відбитків пальців чи розпізнавання обличчя
5. Розвинуто методику забезпечення перенесення інфраструктури в хмарне середовище, наприклад, на платформу Azure
6. Налаштовано двофакторну аутентифікацію для підвищення безпеки каналу передачі даних
7. Розроблена модель успішно введена в експлуатацію підприємства після виходу з тестового режиму