МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри

_____ Ігор ЖУКОВ
(підпис)

« ___ » _____ 2023 р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»
СПЕЦІАЛЬНІСТЬ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

Тема: «Захищена мережа ІТ-компанії з використанням технології *VPN*»

Виконавець: студент групи КС-231М Пістюльга Сергій Миколайович

Керівник: доктор технічних наук, професор Гільгурт Сергій Яковлевич

Нормоконтролер: _____ Василь МАЛЯРЧУК
(підпис)

Засвідчую, що у магістерській роботі немає запозичень праць інших авторів без відповідних посилань

Студент Пістюльга С.М.

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних наук та технологій

Кафедра комп'ютерних систем та мереж

Спеціальність 123 «Комп'ютерна інженерія»

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Ігор ЖУКОВ
(підпис)

« ____ » _____ 2023 р.

З А В Д А Н Н Я
на виконання дипломної роботи

Пістюльги Сергія Миколайовича
(прізвище, ім'я, по батькові)

1. Тема роботи: «Захищена мережа ІТ-компанії з використанням технології *VPN*»

затверджена наказом ректора від " 29 " серпня 2023 №1521/ст

2. Термін виконання роботи: з 02.10.2023 до 31.12.2023

3. Вихідні дані до роботи: створення захищеної мережі ІТ-компанії з використанням технології *VPN*.

4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):

1) аналітичний огляд літературних джерел з тематики диплому;

2) аналіз потреб ІТ-компаній у сфері захисту даних;

3) проблеми захисту даних в комп'ютерних мережах;

4) дослідження технології віртуальних приватних мереж;

5) проектування моделі корпоративної *VPN*-мережі для ІТ-компаніїї.

5. Перелік обов’язкового графічного матеріалу: презентація *Power Point*

6. Календарний план-графік.

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1	Ознайомлення з завданнями на виконання дипломної роботи.	02.10.2023 – 07.10.2023	
2	Огляд літературних джерел за тематикою дослідження.	08.10.2023 – 17.10.2023	
3	Опрацювання та аналіз отриманої інформації, підготовка матеріалів для оформелння пояснювальної записки.	18.10.2023 – 27.10.2023	
4	Опис об’єкта та предмета дослідженнь.	28.10.2023 – 31.10.2023	
5	Вивчення окремих аспектів розглянутої проблеми. Огляд засобів захисту інформації.	01.11.2023 – 10.11.2023	
6	Дослідження технології *VPN* як способу посилення безпеки мережі.	11.11.2023 – 22.11.2023	
7	Практична (програмна) реалізація захищеної мережі ІТ-компанії з використанням технології *VPN*.	23.11.2023 – 03.12.2023	
8	Підведення підсумків проведеної роботи.	04.12.2023 – 10.12.2023	
9	Оформлення пояснювальної записки.	11.12.2023 – 12.12.2023	
10	Проходження нормоконтролю.	13.12.2023 – 22.12.2023	
11	Підготовка презентації та захист роботи.	23.12.2023- 31.12.2023	

7. Дата видачі завдання « 02 » жовтня 2023р.

Керівник дипломної роботи _____ Гільгурт С.Я.
(підпис керівника)

Завдання прийняв до виконання _____ Пістюльга С.М.
(підпис випускника)

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Захищена мережа IT-компанії з використанням технології *VPN*»: 96 с., 35 рис., 32 літературних джерела.

ЗАХИСТ ІНФОРМАЦІЇ, *VPN, CISCO PACKET TRACER.*

Мета дипломної роботи: вдосконалення наявних рішень у сфері безпеки комп'ютерних мереж (КМ); підвищення рівня захисту КМ для IT-компанії; проектування надійного і безпечного *VPN*-рішення для корпоративної мережі IT-компанії, яке забезпечить безпечну передачу даних та захистить мережеві ресурси компанії від небажаних вторгнень.

Об'єкт дослідження: процеси захисту інформації в комп'ютерних мережах.

Предмет дослідженння: технологія віртуальних приватних мереж.

Методи дослідження: порівняльний аналіз, обробка літературних джерел, моделювання та налаштування мережі в емуляторі *Cisco Packet Tracer*.

Результати магістерської роботи рекомендується використовувати під час проведення наукових досліджень та в практичній діяльності фахівців із комп'ютерних мереж. Розроблені в рамках роботи рішення можуть бути впроваджені в реальному середовищі IT-компанії і допоможуть вирішити ряд конкретних проблем та викликів, серед яких: забезпечення безпеки; підтримка мобільності працівників; масштабованість.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

VPN – *Virtual Private Network* (технологія віртуальних приватних мереж)

DDoS – *Distributed Denial-of-Service Attack* (атаки розподіленої відмови в обслуговуванні)

VoIP – *Voice over IP* (технологія передачі медіа-даних у реальному часі за допомогою сімейства протоколів *TCP/IP*)

TCP/IP – *Transmission Control Protocol/Internet Protocol* (протокол управління передачею/міжмережевий протокол)

IDS/IPS – *Intrusion Detection System /Intrusion Prevention System* (системи виявлення та запобігання вторгненням)

OSI – *Open Systems Interconnection Basic Reference Model* (базова еталонна модель взаємодії відкритих систем)

API – *Application Programming Interface* (прикладний програмний інтерфейс)

APT – *Advanced Persistent Threat* (розвинена стала загроза, постійна загроза підвищеної складності)

SFA – *Single-Factor Authentication* (однофакторна аутентифікація)

2FA – *Two-Factor Authentication* (двофакторна аутентифікація)

MFA – *Multi-factor authentication* (багатофакторна аутентифікація)

AES – *Advanced Encryption Standard*

3DES – *Triple Data Encryption Standard*

PPTP – *Point-to-Point Tunneling Protocol* (тунельний протокол

типу точка-точка)

L2TP – *Layer 2 Tunneling Protocol* (протокол тунелювання другого рівня)

SSTP – *Secure Socket Tunneling Protocol* (протокол безпечного тунелювання сокетів)

IKEv2 – *Internet Key Exchange version 2* (протокол обміну ключами Інтернет)

IPsec – *IP Security* – набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу *IP*

LAN – *Local area network* (локальна комп'ютерна мережа)

WAN – *Wide area network* (глобальна комп'ютерна мережа)

SD-WAN – *Software-defined networking in a wide area network* (програмно-визначена глобальна комп’ютерна мережа)

ACL – *Access Control List* (список контролю доступу)

GRE – *Generic Routing Encapsulation* (протокол тунелювання мережевих пакетів, основне призначення — інкапсуляція пакетів мережевого рівня мережевої моделі OSI в IP пакети)

PPP – *Point-to-Point Protocol* (протокол точка-точка)

VPDN – *Virtual Private Dial-up Network* (віртуальна приватна мережа з доступом через комутовані канали)

DHCP – *Dynamic Host Configuration Protocol* (протокол динамічної конфігурації вузла)

TFTP – *Trivial File Transfer Protocol* (тривіальний протокол передачі файлів)

NAT – *Network Address Translation* (перетворення мережевих адрес)

IPV4 – *Internet Protocol version 4* (четверта версія мережевого протоколу IP)

DWDM – *Dense Wavelength Division Multiplexing* (технологія

щільного спектрального мультиплексування)

RAID – *Redundant Array of Independent Disks* (технологія віртуалізації даних, яка об'єднує кілька дисків в логічний елемент для надійності збереження інформації та підвищення продуктивності накопичувачів)

ILO – *Integrated Lights-Out* (механізм керування серверами в умовах відсутності фізичного доступу до них)

AC – *Alternating current* (змінний струм)

DC – *Direct current* (постійний струм)

SFP – *Small Form-factor Pluggable* (промисловий стандарт модульних компактних приймачів)

GE – *Gigabit Ethernet* (набір технологій для передачі пакетів Ethernet зі швидкістю 1 Гбіт/с)

ISR – *Interrupt Service Routine* (опрацьовувач переривань)

PoE – *Power over Ethernet* (технологія передачі електроенергії та даних за допомогою «звитої пари»)

PTZ – *Pan–tilt–zoom* (технологія панорамуванням і масштабуванням)

HTTP/ DNS – *HyperText Transfer Protocol/ Domain Name System* (протокол для розв'язання *DNS* за протоколом *HTTP*)

КМ – Комп’ютерна мережа

ЛОМ – Локальна обчислювальна мережа

БД – База даних

ВСТУП

Початок третього тисячоліття ознаменувався революцією у сфері інформаційних технологій. Комп'ютерні системи та мережі набули величезного значення в економіці, науці, освіті, медицині, культурі та інших галузях суспільного життя. Протягом короткого періоду часу, особливо інтенсивного розвитку зазнали IT-компанії, які допомагають людству використовувати всі переваги технологічного прогресу та надають широкий спектр послуг, від програмування та розробки веб-сайтів до обслуговування корпоративних мереж та систем безпеки.

Однак, з появою нових можливостей та розвитком мережевих технологій виникли й нові проблеми. Одна з них – це безпека даних. Зі збільшенням обсягів обміну інформацією та її значенням в сучасному світі, питання захисту даних набуло особливої актуальності. Інформація стає цінним активом, який потрібно надійно захищати.

Традиційні мережеві рішення для захисту даних, такі як файрволи, антивіруси, системи виявлення вторгнень є потужними засобами, які допомагають вирішувати безпекові проблеми. Однак, ступінь захисту інформації в цілому тим вищий, чим більше задіяно різних засобів і технологій протидії загрозам. У цьому контексті технологію віртуальних приватних мереж (*VPN*) можна вважати додатковим рівнем для захисту даних в мережі.

VPN – це технологія, що дозволяє створювати безпечні з'єднання між мережами через небезпечні канали зв'язку, такі як Інтернет. Вона дозволяє забезпечити конфіденційність передачі даних за допомогою шифрування, цілісність даних за допомогою алгоритмів хешування, а також аутентифікацію користувачів і пристроїв.

Проектування мереж з використанням технології *VPN* вимагає глибокого розуміння не тільки принципів роботи цієї технології, але й вміння

вибрати правильні рішення з погляду топології мережі, вибору обладнання та налаштування *VPN*-каналів.

Корпоративна віртуальна приватна мережа для IT-компанії – це комплексне рішення, що забезпечує захищений доступ до корпоративних ресурсів для працівників компанії, незалежно від їх географічного розташування, а також надійний захист передачі даних в мережі Інтернет.

Ця мережа базується на використанні сучасних стандартів *VPN*, включаючи протоколи тунелювання та шифрування. Основними компонентами цього рішення є *VPN*-сервери, розташовані в дата-центрах компанії, *VPN*-клієнти, встановлені на пристроях користувачів, та спеціалізоване програмне забезпечення для управління та моніторингу *VPN*-мережі.

Впровадження *VPN* включає проектування та реалізацію архітектури мережі, вибір і налаштування обладнання, налаштування *VPN*-тунелів та механізмів шифрування, а також тестування та аудит безпеки *VPN*-мережі.

Актуальність теми дипломного проекту виходить зі зростаючих потреб сучасних IT-компаній у надійних та безпечних способах передачі даних. У світі, де кіберзлочинність постійно зростає, захист мережевих ресурсів стає вирішальним фактором для будь-якої компанії.

Потреба виконання даної роботи назріла саме тепер, оскільки в сучасних умовах рівень кіберзагроз лише зростає, а технологія *VPN* може стати надійним рішенням для їх протидії. Враховуючи нинішній стан існуючих розробок у цій області, можна констатувати, що багато з них мають свої обмеження або не надають достатнього рівня захисту. Отже, є потреба в розробці більш надійних та ефективних рішень, які б могли забезпечити захист даних на високому рівні.

Дана робота спрямована на реалізацію найновіших технологій і стандартів у сфері безпеки IT, що відповідає стратегічним цілям і планам більшості IT-компаній. Крім того, вона є актуальною у контексті виконання

державних та галузевих програм з підвищення рівня надійності та захищеності комп’ютерних мереж.

Метою дипломної роботи є вдосконалення наявних рішень у сфері безпеки комп’ютерних мереж; підвищення рівня захисту КМ для ІТ-компанії; проектування надійного і безпечного *VPN*-рішення для корпоративної мережі ІТ-компанії, яке забезпечить безпечну передачу даних та захистить мережеві ресурси компанії від небажаних вторгнень.

Для досягнення цієї мети, необхідно вирішити наступні завдання:

− проведення аналізу поточного стану технології *VPN*, включаючи основні принципи роботи, архітектуру, протоколи та механізми захисту;

− вивчення основних проблем та викликів в сфері комп’ютерних мереж, з якими стикаються ІТ-компанії, а також дослідження можливості їх розв'язання за допомогою технології *VPN*;

− проектування моделі корпоративної *VPN*-мережі для ІТ-компанії, включаючи вибір необхідного обладнання та програмного забезпечення, розробку архітектури мережі та плану налаштування *VPN*;

− реалізація запропонованого *VPN*-рішення, включаючи налаштування обладнання та програмного забезпечення, налаштування *VPN*-тунелів та шифрування, тестування та оптимізація роботи мережі;

− аудит безпеки та тестування ефективності реалізованого *VPN*-рішення, включаючи виявлення та усунення можливих недоліків, перевірку стійкості до різних типів атак, оцінку ефективності захисту даних та ресурсів мережі.

Об'єктом дослідження дипломної роботи є процеси захисту інформації в комп’ютерних мережах.

Предмет дослідження – технологія віртуальних приватних мереж.

Практична значимість дипломної роботи полягає в можливості забезпечити надійний та безпечний обмін інформацією в мережі Інтернет. Це особливо актуально в умовах сучасного ІТ-світу, де питання захисту даних стоїть дуже гостро.

Впровадження *VPN* в корпоративну мережу дозволяє забезпечити конфіденційність передачі даних, що неможливо переоцінити в умовах постійної загрози кібератак. Це дозволить IT-компанії забезпечити захист комерційної, персональної та іншої конфіденційної інформації.

Використання *VPN* дозволить підвищити продуктивність роботи працівників, що знаходяться за межами офісу, надаючи їм безпечний доступ до корпоративних ресурсів. Впровадження *VPN* забезпечує можливість швидкої адаптації до змін у бізнес-процесах, що дозволяє знизити витрати на IT-інфраструктуру, забезпечуючи високу гнучкість корпоративної мережі.

Основні технології та інструменти, що використані в роботі, були визнані найбільш ефективними та надійними відносно інших доступних аналогів. До даних засобів належать:

− емулятор *Cisco Packet Tracer* був обраний через його надійність та гнучкість у моделюванні та тестуванні різних мережевих сценаріїв. Альтернативи, такі як *GNS3* та *NetSim*, були також розглянуті, але *Packet Tracer* виявився більш відповідним для потреб даної роботи;

− обладнання *Cisco* було обрано з огляду на його високу якість, надійність та сумісність з іншими технологіями та інструментами, що використовуються в роботі;

− технологія *DWDM* була обрана через її здатність забезпечити високу пропускну спроможність та масштабованість для оптичних мереж;

− протокол *IPv4* був обраний через його широку підтримку та сумісність. У роботі було розглянуто можливість використання *IPv6*, але з огляду на поточну інфраструктуру та потреби, *IPv4* було визнано більш підходящим.

Таким чином, аналіз аналогів та вибір технологій та інструментів був важливою частиною виконання роботи, що дозволило досягти мети роботи і забезпечити надійність та безпеку створеної мережі.

Результати розробленого в рамках дипломної роботи продукту можуть бути впроваджені в реальному середовищі IT-компанії і допоможуть вирішити ряд конкретних проблем та викликів, серед яких:

− забезпечення безпеки. Захищена *VPN*-мережа може значно покращити безпеку передачі даних між різними відділеннями компанії та працівниками, які працюють на відстані;

− підтримка мобільності працівників. Використання *VPN* дозволяє працівникам безпечно підключатися до корпоративної мережі з будь-якого місця, що підтримує продуктивність та гнучкість роботи;

− масштабованість. Завдяки використанню оптичної *DWDM*-мережі, мережа може легко масштабуватися для підтримки зростання компанії.

РОЗДІЛ 1
АНАЛІЗ ІТ-КОМПАНІЙ ТА ПРОБЛЕМ ЗАХИСТУ ДАНИХ В ЇХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

1.1. Характеристика сучасних ІТ-компаній

Сучасні ІТ-компанії характеризуються високим рівнем цифровізації, інноваційністю та гнучкістю у використанні нових технологій. У контексті мережевих структур, основні характеристики таких компаній можна виділити наступним чином:

Висока залежність від мережі. Сучасні ІТ-компанії в силу специфіки своєї діяльності в більшості випадків мають високу залежність від мережі. Це зумовлено тим, що основна діяльність таких компаній пов'язана з обробкою, зберіганням та передачею даних, які нерозривно пов'язані з мережевою інфраструктурою. Основні напрями діяльності, які залежать від стабільності та надійності мережі, включають:

- обмін даними. Усі види комунікацій, включаючи електронну пошту, обмін файлами, конференції, обмін даними між різними відділами або працівниками – все це потребує стабільного мережевого з'єднання;
- співпраця. У багатьох ІТ-компаніях команди розподілені географічно або працюють віддалено. Це означає, що для забезпечення ефективної співпраці необхідно безперебійне і швидке мережеве з'єднання;
- взаємодія з клієнтами. Будь-яка інтеракція з клієнтами, від веб-сайтів і онлайн-сервісів до підтримки клієнтів, потребує стабільної і надійної мережі;
- внутрішні операції. Операції, такі як управління проектами, управління ресурсами, аналітика, використання бізнес-додатків, вимагають безперебійної роботи мережі.

Саме через ці причини, відсутність доступу до мережі або недостатня якість мережевого з'єднання може призвести до втрати продуктивності або навіть втрати даних. Це може вплинути на фінансовий результат і репутацію компанії. Отже, для IT-компаній критично важливо мати надійну і стабільну мережеву інфраструктуру [1].

Мобільність та гнучкість роботи в IT-компаніях. Однією з ключових особливостей сучасних IT-компаній є їхня гнучкість та мобільність в організації роботи. Завдяки технологічним засобам та інноваціям, працівники мають змогу працювати в режимі реального часу з будь-якої точки світу, якщо тільки є доступ до інтернету. Це дає можливість реалізувати такі моделі роботи, як:

− віддалена робота. Дана модель передбачає можливість працівників виконувати свої обов'язки поза традиційним офісом. Це може бути дім, кафе, співробітничий простір або будь-яке інше місце. Головне – наявність стабільного інтернет-з'єднання;

− робота в рухомому стані (*mobile work*). Ця модель дозволяє працівникам працювати під час подорожей, на зустрічах з клієнтами, конференціях або у відрядженнях. Все, що для цього потрібно – портативні пристрої (наприклад, ноутбук, планшет або смартфон) та доступ до мережі;

− робота в розподіленій команді. Цей підхід передбачає, що команда, яка працює над одним проектом, може бути географічно розсіяна. Члени команди можуть працювати в різних часових поясах та країнах, але завдяки мережевим технологіям, вони можуть спілкуватися і співпрацювати ефективно.

Ці моделі роботи дають IT-компаніям ряд переваг, включаючи доступ до глобального таланту, підвищену продуктивність, зниження витрат на оренду офісного простору та поліпшення балансу між роботою та особистим життям працівників. Проте, вони також вимагають наявності стабільного та надійного мережевого з'єднання, як ніколи важливого для підтримки безперебійного робочого процесу [2].

Безпека даних в сучасних ІТ-компаніях. У сучасному цифровому світі, безпека даних стала важливим аспектом для будь-якої ІТ-компанії. Оскільки велика кількість конфіденційних даних обробляється та зберігається в цифровій формі, захист цієї інформації від несанкціонованого доступу, витоку, втрати або пошкодження стає пріоритетом.

До ключових аспектів, що стосуються безпеки даних в ІТ-компаніях відносять:

− конфіденційні дані. ІТ-компанії зазвичай обробляють велику кількість конфіденційних даних, включаючи персональні дані співробітників та клієнтів, фінансову інформацію, дані про продукцію і сервіси, інформацію про внутрішні процеси та стратегії. Ця інформація є цільовим об'єктом для хакерів, які можуть використовувати її для злочинних цілей;

− ризики безпеці. Ризики безпеці можуть виникнути з багатьох джерел, включаючи внутрішні (наприклад, співробітники, які випадково або навмисно викликають витік даних) та зовнішні (наприклад, кібератаки, шкідливе ПЗ). ІТ-компанії мають розробляти та впроваджувати різноманітні заходи безпеки, щоб захистити свої дані від цих ризиків;

− заходи безпеки. Основні заходи безпеки включають використання міцного шифрування для захисту даних під час передачі та зберігання; використання двофакторної або багатофакторної автентифікації для обмеження доступу до систем та даних; регулярні аудити та моніторинг систем, щоб виявити будь-які аномалії або підозрілі дії; та проведення регулярних тренінгів для співробітників щодо безпеки інформації;

− комплексний підхід до безпеки даних. Ефективний захист даних вимагає комплексного підходу, який об'єднує технології, процеси та людей. ІТ-компанії мають розуміти, що безпека – це неодноразове завдання, а постійний процес, який вимагає неперервного моніторингу, оновлення та всебічного удосконалення [3].

Високі вимоги до швидкості та якості передачі даних. ІТ-компанії часто працюють з великими обсягами даних і потребують високої швидкості обробки

та передачі даних. Вони створюють, обробляють та аналізують гігабайти і терабайти інформації щодня. Це може включати все, від транзакцій клієнтів та даних про користувачів до бізнес-аналітики і машинного навчання.

Висока швидкість обробки і передачі даних стає критичною для ефективного функціонування. Затримки в мережі або низька швидкість передачі даних можуть призвести до втрати продуктивності, погіршення досвіду користувача, а в деяких випадках навіть до фінансових втрат.

Залежність IT-компаній від мережевої інфраструктури для забезпечення щоденної діяльності IT-компаній та їх вимог до високого рівня мережевих сервісів включають:

− обробка та зберігання великих обсягів даних. IT-компанії активно зберігають та обробляють значні обсяги даних, що ставить перед ними вимогу до високої надійності мережевих систем для ефективної обробки та передачі цих даних;

− потреба у високій швидкості обробки та передачі даних. Велика швидкість є фундаментальним вимогам в IT-компаніях, оскільки вони потребують мереж, які здатні передавати дані з високою швидкістю та мінімізованою затримкою;

− вимоги до якості передачі даних. Для IT-компаній надзвичайно важливо забезпечити передачу даних без помилок або втрат, що гарантує високу точність та цілісність оброблених даних;

− використання передових технологій. Для підтримки надійності, швидкості та якості мережевого обслуговування, IT-компанії активно застосовують найновіші технології, які можуть задовольнити широкий спектр мережевих і технічних вимог компанії.

Беручи до уваги розглянуті вище характеристики, можемо зазначити, що технологія *VPN* може значно покращити ефективність та безпеку роботи IT-компаній. *VPN* дозволяє компаніям створювати безпечні приватні мережі через публічні мережі, які забезпечують безпечну віддалену роботу, надійну передачу даних та захист від кіберзагроз [4].

1.2. Огляд типових проблем з обміном та захистом даних в комп’ютерних мережах IT-компаній

Захист та обмін даних у мережах IT-компаній є актуальними та надзвичайно важливими питаннями. Несприятливі наслідки проблем, пов'язаних із цими питаннями, можуть включати витоки конфіденційної інформації, порушення роботи систем, зниження продуктивності та навіть юридичні проблеми. Найбільш поширені проблеми, з якими можуть зіткнутися IT-компанії включають:

Кібератаки. Кібератаки – це один з найважливіших викликів, з якими стикаються IT-компанії у своїй щоденній діяльності. Їх негативні наслідки можуть варіюватися від втрати конфіденційної інформації до зупинення роботи інфраструктури компанії, що призводить до значних фінансових втрат і шкоди репутації. До найбільш поширених кібератак на IT-компанії належать:

− атаки *DDoS*. Зловмисники можуть проводити так звані атаки розподіленої відмови в обслуговуванні (*DDoS*), засипаючи мережеві ресурси великою кількістю запитів, що призводить до відмови в обслуговуванні легітимних користувачів;

− *ransomware*. Цей тип шкідливого програмного забезпечення зашифровує файли на зараженому комп'ютері, після чого зловмисники вимагають від жертви відшкодування (зазвичай в криптовалюті) за розшифровку даних;

− віруси та шкідливі програми. Вони можуть вкрасти конфіденційну інформацію, знищити дані або зламати системи. Такі атаки можуть включати встановлення кейлоггерів для викрадення облікових даних, троянських коней для отримання віддаленого контролю над системами, або використання вірусів для поширення шкідливого коду по мережі.

Ці атаки вимагають від IT-компаній застосування різноманітних механізмів захисту, як-от міцних систем антивірусного захисту, мережевих

фаєрволів, системи захисту від *DDoS*-атак, системи резервного копіювання даних, та освіченого персоналу, що знає про можливі загрози і як їх треба уникати [5,6].

Ненадійність мережі. Ненадійність мережі може бути серйозною проблемою для IT-компаній, які великою мірою залежать від стабільних і надійних мережевих з'єднань для своєї повсякденної роботи. Ключові аспекти цієї проблеми включають:

− проблеми з підключенням до мережі. Іноді мережеві з'єднання можуть бути нестабільними або відсутніми через різні причини, включаючи проблеми з обладнанням, помилки в конфігурації або зовнішні фактори, такі як перебої з живленням. Це може зробити неможливим доступ до важливих даних або служб, що може призвести до втрати продуктивності;

− мережеві затримки. Мережеві затримки впливають на час, який потрібен пакету даних для проходження від одного місця до іншого в мережі. Високі мережеві затримки можуть спричинити відчутні затримки в роботі додатків та служб, особливо тих, які залежать від швидкого обміну даними, таких як *VoIP*, відеоконференції, стрімінгове відео та інтерактивні онлайн-ігри;

− проблеми з пропускною здатністю. Пропускна здатність визначає, скільки даних може бути передано через мережеве з'єднання за певний проміжок часу. Якщо пропускна здатність не є достатньою, це може призвести до повільного завантаження веб-сторінок, затримок у стрімінговому відео або зниження якості в *VoIP*-дзвінках.

Всі ці проблеми можуть призвести до втрати даних під час передачі, а також низької продуктивності та задоволеності користувачів. Їх можна вирішити за допомогою різних методів, включаючи використання високоякісного обладнання, оптимізацію конфігурації мережі, регулярне обслуговування та моніторинг мережі [7].

Несанкціонований доступ. Несанкціонований доступ до мережі чи до окремих систем - це одна з найбільш серйозних проблем з безпекою, які можуть виникнути в IT-компаніях. Це може стати причиною значних втрат

даних або викликати непоправні пошкодження. В цьому контексті є декілька ключових питань, які варто розглянути:

− витік даних. Якщо зловмисник отримує несанкціонований доступ до мережі або системи, він може викрасти цінні дані, такі як персональні дані клієнтів, комерційні секрети, фінансову інформацію та інше. Це може призвести до значних фінансових збитків та до руйнування репутації компанії;

− зміни в даних. Несанкціонований користувач може внести зміни в дані, які зберігаються в мережі або системі. Він може змінити або маніпулювати даними таким чином, щоб приховати свої дії, у підсумку інформація стає недостовірною та може нашкодити компанії;

− видалення або пошкодження даних. У найгіршому випадку, зловмисник може видалити або пошкодити дані, що може призвести до втрати важливої інформації та вимагати значних зусиль для відновлення.

Для запобігання цим проблемам, ІТ-компанії повинні впроваджувати різноманітні міри безпеки, включаючи сильні політики паролів, двофакторну аутентифікацію, шифрування даних, системи виявлення та запобігання вторгненням, регулярні аудити безпеки та навчання співробітників [8].

Втрати даних. Втрата даних – одна з найбільш серйозних проблем, з якими можуть зіткнутися ІТ-компанії. Вона може бути спричинена різними факторами, серед яких можна виділити:

− технічні збої. Технічні проблеми, такі як пошкодження апаратного забезпечення, відмова серверів, відмова жорсткого диска, або проблеми з програмним забезпеченням можуть призвести до втрати даних. Це може означати, що важливі документи, бази даних, фінансова інформація або інша ключова інформація можуть бути незворотно втрачені, якщо не існує резервних копій або систем відновлення;

− помилки користувачів. Людські помилки також можуть призвести до втрати даних. Наприклад, співробітник може випадково видалити файл або базу даних, не розуміючи наслідків своїх дій. Крім того, співробітники можуть

ненавмисно встановлювати шкідливе програмне забезпечення або відкривати шкідливі посилання, які можуть призвести до втрати або пошкодження даних.

Для запобігання втраті даних, ІТ-компанії повинні впроваджувати комплексні стратегії захисту даних. Це може включати в себе регулярне створення резервних копій, використання відмовостійкого апаратного забезпечення, забезпечення надійного живлення та охолодження для серверів, використання антивірусного програмного забезпечення та файрволів, а також навчання співробітників правилам безпечного використання ІТ-ресурсів.

Вразливості в програмному забезпеченні. Вразливості в програмному забезпеченні представляють собою одну з найсерйозніших загроз для цифрової безпеки ІТ-компаній. Ці вразливості – це дефекти або слабкі місця в коді програмного забезпечення, які можуть бути використані зловмисниками для вторгнення в систему, викрадення, зміни або видалення даних, або навіть взяття системи під свій контроль. Серед вразливостей програмного забезпечення виділяють:

− експлуатація вразливостей. Зловмисники намагаються знайти і експлуатувати вразливості в програмному забезпеченні для отримання несанкціонованого доступу до систем. Це може включати використання спеціалізованих інструментів або скриптів для автоматизації процесу пошуку вразливостей;

− вразливості нульового дня (*Zero-day*). Це вразливості, які відомі зловмисникам, але ще не виявлені або не виправлені виробником програмного забезпечення. Такі вразливості є особливо небезпечними, оскільки для них ще не існує патчів або виправлень;

− застаріле програмне забезпечення. Часто виявляється, що старі версії програмного забезпечення містять вразливості, які були виправлені в більш нових версіях. Проте, якщо оновлення не встановлено, старі версії програмного забезпечення можуть стати входом для зловмисників.

Для запобігання цим загрозам, ІТ-компанії повинні вживати заходів для регулярного оновлення та патчування всього програмного забезпечення,

використовувати програми для виявлення вразливостей, а також забезпечити відповідні процедури відновлення в разі успішної атаки [9].

Несумісність систем. Несумісність систем є важливою проблемою в IT-секторі, яка може призвести до комплексу проблем, зокрема втрати або пошкодження даних. Несумісність систем може включати в себе:

− проблеми з обміном даними. Коли дві системи не можуть ефективно обмінюватися даними через несумісність, інформація може бути втрачена або пошкоджена під час передачі. Це може включати неповне або неправильне відображення даних, втрату даних або навіть системні збої;

− помилки відтворення даних. Дані, що надходять з несумісної системи, можуть бути відтворені неправильно, що призводить до невірних результатів або помилок;

− неефективність процесів. Несумісність систем може також призвести до неефективності в роботі. Це може включати потребу в ручній обробці даних, зайвих кроків або додаткового програмного забезпечення для забезпечення сумісності.

Для вирішення цієї проблеми, компанії можуть використовувати стандартизовані формати обміну даними, адаптоване програмне забезпечення, а також розробляти і впроваджувати політики сумісності систем. Додатково, технології, такі як *API*, можуть бути використані для підтримки ефективного обміну даними між різними системами.

1.3. Основні методи вирішення мережевих проблем

Традиційні мережеві рішення для захисту даних в IT-компаніях є системами, які використовуються для виявлення, запобігання і реагування на загрози безпеці. Задля вирішення проблем мережевої безпеки в IT-компаніях, необхідно розробити і застосувати багаторівневий підхід, що передбачає використання комплексу технічних засобів, корпоративних політик та стратегій. Цей підхід наголошує на важливості балансу між запобіжними,

відновлювальними та адаптивними заходами безпеки. Серед основних методів вирішення проблем захисту даних ІТ-компаній можна виділити:

Фаєрволи (Брандмауери). Брандмауери, відомі також як фаєрволи, представляють собою основний компонент будь-якої системи захисту мережі. Вони створюють віртуальну «стіну», що регулює вхідний та вихідний трафік в мережі, блокуючи небезпечний та несанкціонований доступ. Це може включати блокування ненадійних веб-сайтів, заборону певних типів додатків або блокування спроб несанкціонованого доступу до внутрішніх ресурсів.

Брандмауери можуть бути апаратними або програмними. Апаратні фаєрволи – це фізичні пристрої, які підключаються до мережі, тоді як програмні фаєрволи встановлюються на комп'ютери або сервери. Кожен тип має свої переваги: апаратні фаєрволи зазвичай надають більш сильний рівень захисту і менш схильні до вразливостей, але програмні фаєрволи часто надають більш гнучкі та кастомізовані налаштування.

Усе вказане робить фаєрволи незамінним компонентом в захисті мережевих ресурсів компанії від зовнішніх та внутрішніх загроз [10].

Антивірусне програмне забезпечення. Антивірусне програмне забезпечення є фундаментальною частиною стратегії захисту ІТ-компаній. Це програми, які сканують комп'ютери та мережі на наявність шкідливого програмного забезпечення, включаючи віруси, троянські коні, шпигунське ПЗ, ransomware та інші потенційні загрози. Після виявлення шкідливого ПЗ, антивірусне програмне забезпечення намагається його нейтралізувати, видалити або перенести в карантин.

Антивіруси використовують різні методи виявлення, включаючи сигнатурне сканування, яке знаходить відомі віруси на основі їх «сигнатур» або унікальних ідентифікаторів, та евристичне сканування, яке виявляє нові або невідомі загрози, аналізуючи підозрілу поведінку або код.

Більш передові антивірусні рішення також використовують технології, такі як аналіз поведінки, машинне навчання та штучний інтелект, для прогнозування і виявлення нових загроз, що постійно еволюціонують. Це все

допомагає компаніям виявляти і блокувати шкідливе програмне забезпечення, перш ніж воно зможе пошкодити системи або викрасти дані [11].

Системи виявлення та запобігання вторгненням (IDS/IPS). Системи виявлення та запобігання вторгненням є важливими інструментами в боротьбі проти кіберзлочинності, які забезпечують активний моніторинг мережі та захист від шкідливого або підозрілого трафіку. Ці системи функціонують, аналізуючи мережевий трафік і порівнюючи його з відомими шаблонами атаки або аномальною поведінкою.

Такі системи сканують мережевий трафік для виявлення потенційних загроз, включаючи спроби несанкціонованого доступу, *DDoS*-атаки, сканування портів та інші підозрілі активності. Вони можуть генерувати сповіщення при виявленні таких активностей, щоб адміністратори могли вжити відповідних дій.

Системи запобігання вторгненням, з іншого боку, не просто виявляють потенційні загрози, але й здатні активно блокувати або втручатися в них, незалежно від того, чи це блокування шкідливого трафіку, закриття підозрілих портів або ізоляція інфікованих систем.

Разом, *IDS/IPS* надають потужні засоби для раннього виявлення та реагування на кібератаки, допомагаючи захистити IT-ресурси компанії [12].

Резервне копіювання та відновлення даних. Резервне копіювання та відновлення даних є критично важливими аспектами стратегії захисту даних для будь-якої IT-компанії. Вони забезпечують захист від можливих втрат даних, що можуть виникнути в результаті технічних збоїв, помилок користувачів, вірусних атак або інших небезпечних ситуацій.

Стратегія резервного копіювання включає в себе створення копій даних на випадок їх втрати або пошкодження. Зазвичай резервні копії зберігаються відокремлено від первинних даних – це може бути інший сервер, хмарна платформа або зовнішній жорсткий диск. Важливо проводити резервне копіювання регулярно, щоб мінімізувати втрату даних у випадку збою.

Системи відновлення даних, з іншого боку, допомагають відновити інформацію з резервних копій. Вони можуть використовуватися для відновлення втрачених або видалених файлів, відновлення системи після технічного збою або відновлення даних після кібератаки.

Разом, резервне копіювання та відновлення даних створюють захисну мережу для IT-компаній, яка зменшує ризик втрати важливої інформації і допомагає впевнено відновлювати роботу після непередбачуваних подій [13].

Покращення системи управління доступом. Політики доступу є важливим компонентом мережевої безпеки. Вони допомагають контролювати, хто може отримати доступ до мережевих ресурсів, та як ці ресурси можуть бути використані. Політики доступу визначають дозволені дії користувачів, що сприяє запобіганню ненавмисних або навмисних дій, що можуть призвести до втрати або пошкодження даних.

Підвищення ефективності системи управління доступом є важливою частиною стратегії безпеки IT-компанії. У цьому контексті, політика доступу, яка включає принцип найменшого привілею (*Principle of Least Privilege - PoLP*), відіграє ключову роль.

Принцип найменшого привілею полягає в наданні користувачам, системам або процесам лише мінімального обсягу привілеїв, які є необхідними для виконання їх обов'язків. Це означає, що користувачі мають доступ лише до інформації та ресурсів, необхідних для виконання їх конкретних завдань, а весь інший доступ обмежений.

Цей принцип допомагає знизити ризик несанкціонованого доступу до конфіденційних даних або систем. За умови, що зловмисник здатен скомпрометувати обліковий запис користувача, він зможе отримати доступ лише до тих ресурсів, до яких у цього користувача був доступ, що обмежує потенційні збитки.

Оптимізація системи управління доступом вимагає впровадження різних політик та процедур. Важливим аспектом є створення чіткої ролевої моделі, яка визначає, до якої інформації мають доступ різні користувачі або групи

користувачів. Також необхідно регулярно проводити аудит системи доступу, переглядати та оновлювати політики доступу відповідно до змін у бізнес-потребах або структурі компанії [14].

Політики доступу можуть включати в себе також різні рівні авторизації для різних користувачів, двофакторну аутентифікацію, обмеження доступу до важливих систем із використанням списків контролю доступу (*ACLs*) та інше. Виконання політик доступу необхідно регулярно перевіряти та оновлювати, щоб впевнитися, що вони залишаються ефективними в міру розвитку технологій та зміни загроз.

Отже, вдосконалення системи управління доступом, яка базується на принципі найменшого привілею, може забезпечити значне покращення безпеки ІТ-компанії.

Створення ефективного плану відгуку на інциденти безпеки. Ефективний план відгуку на інциденти безпеки має бути гнучким і здатним адаптуватися до змінюваного кіберпростору, але водночас має включати чіткі, стандартизовані процедури для різних типів інцидентів безпеки.

Перш за все, такий план відгуку на інциденти безпеки має містити процедури для виявлення та ідентифікації інцидентів. Це може включати в себе моніторинг систем, аналіз логів та алгоритми для виявлення аномального поведінки, які допомагають виявити можливі порушення безпеки.

Наступний крок — аналіз інциденту. Це включає в себе визначення типу атаки, визначення обсягу порушення, ідентифікацію потенційно заражених систем і даних. Важливо швидко і точно оцінити масштаб інциденту, щоб прийняти виважене рішення щодо подальших дій.

Третій крок полягає у відповіді на інцидент. Це може включати в себе ізоляцію заражених систем, видалення шкідливого ПЗ, відновлення втрачених або пошкоджених даних та, при необхідності, введення змін в інфраструктуру для виправлення слабких місць, які були використані для атаки.

Останній крок включає відновлення системи після інциденту. Це може передбачати відновлення з резервних копій, оновлення систем та ПЗ, а також

проведення розгляду інциденту для виявлення слабких місць та вдосконалення процедур відгуку на інциденти.

Підготовка персоналу є критичною частиною ефективного плану відгуку на інциденти безпеки. Якщо співробітники не знають, як реагувати на інциденти безпеки, можливо, вони не в змозі вчасно ідентифікувати або реагувати на порушення, що може призвести до більшого збитку.

Регулярне навчання і тестування співробітників щодо процедур відгуку на інциденти безпеки важливе для забезпечення того, що вони знають свої обов'язки та розуміють, як діяти в критичний момент. Це навчання має включати не тільки теоретичну інформацію, але й практичні вправи, такі як тренування на вирішення реальних ситуацій, включаючи симуляцію атак.

Також критично важливо, щоб ці процедури були добре документовані. У випадку інциденту безпеки, співробітники мають можливість швидко звернутися до цих документів для отримання вказівок. Документи мають бути легкими для читання та використання, містити конкретні кроки та бути регулярно оновлюваними, щоб відображати будь-які зміни в інфраструктурі або стратегії безпеки компанії.

Для впровадження плану відгуку на інциденти безпеки, керівництво компанії має продемонструвати свою підтримку та включеність. Це означає забезпечення необхідних ресурсів для підготовки персоналу та забезпечення того, що відповідь на інциденти безпеки стане пріоритетом на всіх рівнях організації.

Освіта та тренінги для співробітників. Освіта та тренінги для працівників в контексті кібербезпеки включають в себе інформування та підвищення обізнаності персоналу щодо кіберзагроз, їх можливого впливу та стратегій мінімізації ризиків. Така освіта забезпечує зменшення ризику кібератак, оскільки багато із них базуються на використанні людського фактору, в основному незнанні або недбалості співробітників.

Персонал організації може стати найслабкішим ланцюгом в системі захисту, якщо не буде належно освіченим щодо потенційних кіберзагроз та

важливості дотримання протоколів безпеки. Навчання та тренування можуть забезпечити працівників відповідними знаннями та навичками, які необхідні для розуміння та реагування на потенційні загрози.

Освіта персоналу може охоплювати різноманітні теми, починаючи від основних принципів кібербезпеки, таких як важливість міцних паролів і обережне поводження з електронною поштою, до більш складних питань, таких як розуміння конкретних кіберзагроз та протоколів реагування на інциденти безпеки. До цього можуть належати і практичні аспекти, такі як вміння виявляти фішингові спроби, використовувати двофакторну аутентифікацію та інші заходи захисту даних.

Навчання співробітників має бути не одноразовим процесом, а стати неперервною діяльністю, що включає регулярні оновлення та тренінги для адаптації до змінюваних умов та нових загроз. Впровадження такої політики є важливим кроком до створення організаційної культури, що орієнтована на безпеку, де кожен співробітник відчуває свою відповідальність за захист організації від кіберзагроз.

Хоча ці традиційні мережеві рішення можуть надати певний рівень захисту, вони мають свої обмеження. Наприклад, вони можуть бути неефективними проти деяких сучасних кібератак, таких як розширені персистентні загрози (*APT*). Крім того, вони можуть не забезпечувати достатній захист для віддалених працівників або для даних, що передаються по незахищених мережах. Існують більш сучасні рішення, такі як віртуальні приватні мережі, які можуть допомогти вирішити деякі з цих проблем.

Усі згадані методи захисту є взаємопов'язаними, і найкращий результат можна досягти шляхом їх комплексного застосування. Важливо постійно моніторити, оцінювати та оновлювати свої стратегії впровадження безпеки, щоб вони відповідали сучасним загрозам та викликам [15,16].

1.4. Визначення проблем та задач, які можуть бути вирішені застосуванням VPN

Віртуальні приватні мережі відіграють ключову роль в галузі мережевої безпеки, надаючи ефективний засіб для захисту даних та приватності користувача. Ця технологія працює за принципом створення безпечного тунелю для передачі даних через публічні мережі, як-от Інтернет, використовуючи процеси шифрування для забезпечення конфіденційності та цілісності цих даних.

Основна відмінність *VPN* від традиційних мережевих рішень полягає у тому, що *VPN* створює зашифроване з'єднання, яке забезпечує безпечний транзит інформації між користувачем і цільовою мережею. Це означає, що навіть якщо дані перехоплені під час передачі, зловмисники не зможуть їх розшифрувати без відповідного ключа шифрування.

Використання *VPN* також важливе для захисту ідентичності користувача. Воно маскує *IP*-адресу користувача, що дозволяє обмежити його слід в мережі Інтернет і зменшити ризик стеження або зловмисного використання особистої інформації.

Подолання цензури або блокування ресурсів – інша важлива властивість *VPN*. В деяких регіонах або корпоративних мережах можуть існувати обмеження на доступ до певних веб-ресурсів. *VPN* дозволяє користувачам обходити такі обмеження, забезпечуючи свободу доступу до інформації.

Основні проблеми, які можна вирішити за допомогою використання VPN включають:

Небезпечні публічні Wi-Fi мережі. Публічні *Wi-Fi* мережі стають все більш поширеними в сучасному світі, але вони часто не надають достатнього захисту для даних користувачів. Коли співробітники IT-компаній використовують ці мережі для доступу до корпоративних ресурсів, вони

можуть ненавмисно відкрити ворота до конфіденційної інформації для потенційних зловмисників.

Хоча публічні *Wi-Fi* мережі зручні, вони часто відкриті для всіх користувачів, що створює можливість для несанкціонованого доступу. Кіберзловмисники можуть використовувати різні техніки, включаючи «*man-in-the-middle*» атаки, для перехоплення незашифрованих комунікацій або навіть спроби злому паролів (рис. 1.1).

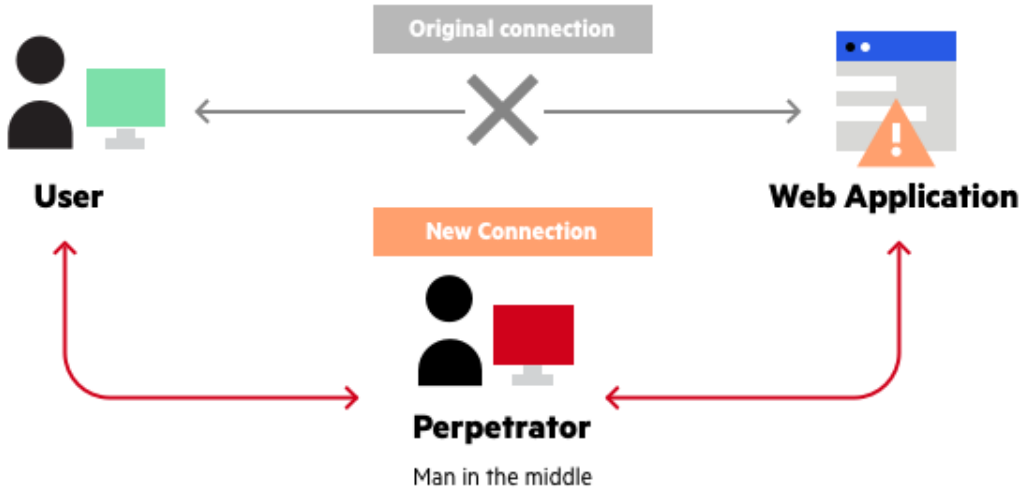


Рис. 1.1. Загальна схема атаки *Man-in-the-Middle*

Вирішенням цієї проблеми може стати використання віртуальної приватної мережі. *VPN* створює зашифрований «тунель» між пристроєм користувача та сервером *VPN*, через який проходять всі дані (рис. 1.2). Це означає, що навіть якщо зловмисник намагається перехопити дані, він не зможе їх прочитати через шифрування.

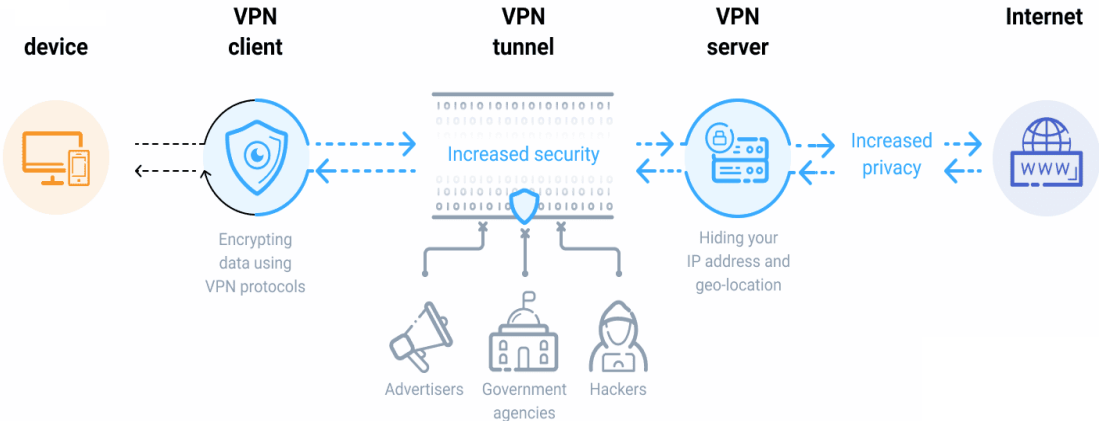


Рис. 1.2. Схема *VPN* з'єднання між пристроєм та *Internet*

Завдяки використанню *VPN*, співробітники можуть безпечно працювати з корпоративними ресурсами, навіть користуючись публічними *Wi-Fi* мережами.

Втім, варто пам'ятати, що *VPN* забезпечує лише один рівень захисту, і його необхідно використовувати у поєднанні з іншими мережевими заходами інформаційної безпеки [17].

Захист від витоку даних. Витік даних є одним з найбільших ризиків, з якими стикаються IT-компанії в сучасному цифровому середовищі. Витік даних може виникнути в результаті ряду причин, включаючи несанкціонований доступ, кібератаки, або навіть ненавмисне розголошення інформації співробітниками. Без належного захисту, конфіденційні ділові дані, особиста інформація співробітників, інформація про клієнтів, і навіть пропрієтарні технології компанії можуть стати доступними третім сторонам, що може призвести до серйозних наслідків, включаючи фінансові втрати, втрату репутації, і юридичні проблеми.

Вирішенням цієї проблеми може бути використання віртуальної приватної мережі. *VPN* пропонує додатковий рівень захисту від витоку даних, шифруючи всі дані, які передаються між пристроями користувачів і мережею компанії. Завдяки цьому, навіть якщо дані перехоплені під час передачі, вони залишаються недоступними для зловмисників через шифрування. Це означає, що навіть у випадку компрометації мережі, конфіденційні дані компанії залишаються в безпеці.

Втім, важливо зазначити, що, хоча *VPN* пропонує значний рівень захисту, він повинен бути використаний як частина більш широкої стратегії безпеки, яка також може включати антивірусне програмне забезпечення, фаєрволи, системи виявлення та запобігання вторгненням, а також строгі політики доступу.

Доступ до ресурсів з будь-якої точки світу. Віддалена робота та глобальна присутність компаній стали значними аспектами сучасного бізнес-пейзажу. Однак, вони також вимагають надійного та безпечного доступу до корпоративних ресурсів з різних місць світу. Саме тут важливу роль відіграє *VPN*.

Ця технологія дозволяє співробітникам підключатися до корпоративних мереж через зашифрований канал, незалежно від їхнього фізичного місцезнаходження. Це означає, що вони можуть безпечно доступатися до внутрішніх систем та ресурсів компанії, таких як електронна пошта, файли, бази даних або спеціалізовані застосунки, навіть якщо вони знаходяться в іншій країні або працюють вдома.

Цей аспект особливо важливий для організацій з глобальною присутністю, які мають офіси, партнерів або співробітників у різних країнах. Завдяки *VPN* їхні співробітники можуть спілкуватися та співпрацювати ефективно, незалежно від часових поясів або географічних обмежень.

Також, у контексті віддаленої роботи, *VPN* є важливим інструментом, який забезпечує безпечний доступ до ресурсів компанії. Співробітники можуть продовжувати свою роботу з комфортом своїх осель, мати повний доступ до необхідних даних і систем, при цьому забезпечуючи безпеку та конфіденційність корпоративної інформації.

Проте, важливо зрозуміти, що для забезпечення оптимальної ефективності та безпеки, слід правильно налаштувати *VPN*, а також поєднати його з іншими методами захисту, такими як брандмауери, антивіруси, системи виявлення та запобігання вторгненням та строгі політики доступу.

Захист ідентичності користувача. Технологія *VPN* відіграє ключову роль у захисті ідентичності користувачів в онлайн-просторі. Один з основних принципів безпеки, які вона застосовує, це приховування реальних *IP*-адрес користувачів. Інформація про *IP*-адресу може використовуватися зловмисниками для визначення географічного місцезнаходження користувача, його провайдера інтернету і інших технічних подробиць. У руках недобросовісних осіб ця інформація може бути використана для кіберзлочинів, таких як крадіжка даних, шахрайство або навіть атаки *DDoS*.

Коли користувач підключається до *VPN*, його реальна *IP*-адреса замінюється на *IP*-адресу *VPN*-сервера, до якого він підключається. Це означає, що будь-яка активність, яка відслідковується або записується в Інтернеті, буде

пов'язана з *IP*-адресою *VPN*-сервера, а не з *IP*-адресою користувача. Це ефективно приховує ідентичність користувача і робить його більш анонімним в онлайн-просторі.

Використання *VPN* для захисту ідентичності користувача може зменшити ризик витоку даних і зловмисних атак. Втім, важливо зауважити, що хоча *VPN* забезпечує високий рівень конфіденційності, він не повністю гарантує анонімність. Для повноцінного захисту рекомендується використовувати *VPN* у поєднанні з іншими заходами безпеки, такими як антивірусне програмне забезпечення, фаєрволи, двофакторна аутентифікація та освіченість користувачів з питань кібербезпеки.

Уникнення цензури або блокування. У глобальному інтернет-просторі існує широкий спектр політик цензури та блокування веб-ресурсів, що варіюються від країни до країни. В деяких регіонах обмеження можуть бути настільки серйозними, що вони ускладнюють або повністю перешкоджають доступ до певних сайтів, сервісів або інформації.

Віртуальні приватні мережі надають користувачам можливість обходити таку цензуру або блокування. Коли користувач підключається до *VPN*, його мережевий трафік перенаправляється через сервер *VPN*, який може знаходитися в будь-якому місці світу. Таким чином, користувач може здаватися особою, яка перебуває в іншому географічному регіоні, де веб-ресурси не заблоковані.

Використання *VPN* для обходу цензури та блокування дає користувачам можливість забезпечити більш вільний та незалежний доступ до інформації. Це особливо важливо для журналістів, активістів, науковців та бізнесменів, яким потрібен доступ до незаконодавчо обмежених ресурсів. Однак варто зауважити, що використання *VPN* для обходу цензури може бути протиправним в деяких країнах, тому користувачам слід бути свідомими місцевого законодавства та розуміти потенційні ризики.

Отже, віртуальні приватні мережі надають комплексне рішення для забезпечення безпеки даних та приватності в Інтернеті. Важливо зазначити, що

VPN не є універсальним рішенням для всіх проблем безпеки. Наприклад, він не захистить від внутрішніх загроз, таких як ненавмисні помилки співробітників або зловмисний інсайдер. Крім того, якщо кінцевий пристрій вже інфікований шкідливим програмним забезпеченням, *VPN* не зможе захистити передані з нього дані. Тому *VPN* має використовуватися в комбінації з іншими інструментами і стратегіями безпеки [18].

Висновки за розділом

У межах першого розділу було проведено детальний аналіз сучасних IT-компаній та проблем, пов'язаних із захистом та обміном даними, з якими стикаються дані установи. Основними характеристиками типових IT-компаній є висока залежність від мережі, мобільність та гнучкість роботи, високі вимоги до швидкості та якості передачі даних, а також необхідність забезпечити безпеку даних.

Проблеми, з якими стикаються IT-компанії, охоплюють широкий спектр питань, включаючи кібератаки, ненадійність мережі, несанкціонований доступ, втрату даних, вразливості в програмному забезпеченні та несумісність систем. Для вирішення цих проблем були розглянуті традиційні мережеві рішення для захисту даних, такі як фаєрволи, антивірусне програмне забезпечення, системи виявлення та запобігання вторгненням, резервне копіювання та відновлення даних, а також політики доступу. Також були визначені конкретні проблеми, для вирішення яких є доцільним використання мереж *VPN*.

Було розглянуто основні методи вирішення мережевих проблем та з’ясовано, що використання *VPN*, систематичне резервне копіювання та відновлення даних, покращення системи управління доступом, а також створення ефективного плану відгуку на інциденти безпеки є важливими етапами організації захищеної системи.

Таким чином, проведене дослідження та аналіз стану справ допомагає визначити ключові проблеми та відповідні рішення, які допоможуть

наблизитися до досягнення мети відповідно до теми роботи – забезпечення безпеки даних в комп'ютерних мережах IT-компаній. У наступних розділах будуть розглянуті способи практичного впровадження цих рішень.

РОЗДІЛ 2
ТЕХНОЛОГІЯ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

2.1. Концепція технології *VPN*

Технологія віртуальних приватних мереж забезпечує захищене з'єднання між віддаленими користувачами та центральними мережевими ресурсами компанії через публічний інтернет. *VPN* є технологією, яка створює безпечний тунель через публічний Інтернет, забезпечуючи приватність та анонімність користувача. На рис. 2.1 представлено основні компоненти та процеси, що відбуваються під час використання *VPN*.

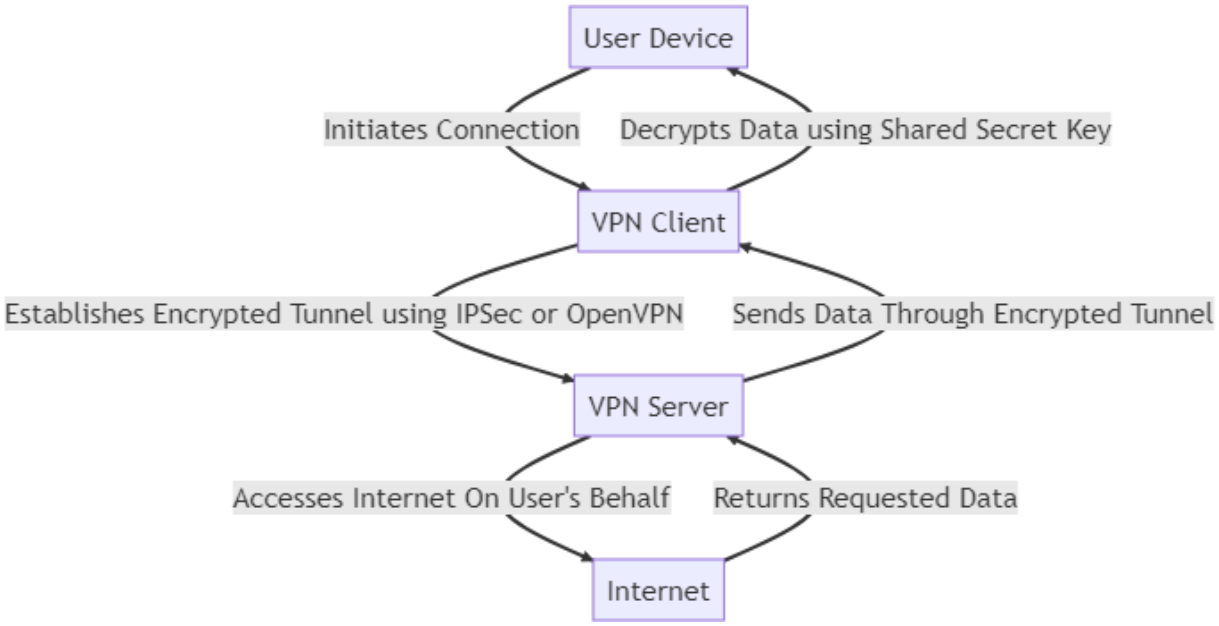


Рис. 2.1. Концепція роботи *VPN*

Отже, основні компоненти з якими взаємодіє *VPN*:

− користувацький пристрій (*User Device*). Це може бути будь-який пристрій, який має доступ до Інтернету, наприклад, комп'ютер, смартфон або планшет. Користувач ініціює з'єднання з *VPN*, відправляючи запит на підключення до *VPN*-клієнта;

–

− *VPN*-клієнт (*VPN Client*). Це програмне забезпечення, встановлене на пристрої користувача, яке відповідає за встановлення та управління *VPN*-з'єднанням. Після отримання запиту від користувача, *VPN*-клієнт встановлює зашифрований тунель до *VPN*-сервера, використовуючи протоколи, такі як *IPSec* або *OpenVPN*. Ці протоколи забезпечують безпеку та приватність даних, які передаються через *VPN*;

− *VPN*-сервер (*VPN Server*). Це сервер, який приймає вхідні *VPN*-з'єднання. Після встановлення зашифрованого тунелю, *VPN*-сервер здійснює доступ до Інтернету від імені користувача. Це означає, що всі запити до Інтернету виглядають так, ніби вони відправлені з *VPN*-сервера, а не від пристрою користувача, що забезпечує анонімність користувача;

− Інтернет (*Internet*). Це глобальна система з'єднаних комп'ютерних мереж, яка передає дані між пристроями. Після отримання запиту від *VPN*-сервера, Інтернет повертає запитані дані назад до *VPN*-сервера.

Після отримання даних від Інтернету, *VPN*-сервер надсилає ці дані назад через зашифрований тунель до *VPN*-клієнта на пристрої користувача. *VPN*-клієнт потім розшифровує ці дані за допомогою спільного секретного ключа і доставляє їх до користувацького пристрою. Завдяки цьому процесу дані залишаються приватними і безпечними від початку до кінця передачі.

Важливо зазначити, що різні рішення *VPN* використовують різні протоколи для шифрування та аутентифікації. Деякі з них, як-от *OpenVPN* та *L2TP/IPsec*, надають сильне шифрування та високу надійність, тоді як інші, наприклад *PPTP*, є швидшими, але менш безпечними [19].

VPN технології також можуть забезпечувати анонімність користувачів шляхом зміни їх *IP*-адреси та маршрутизації всього їх трафіку через *VPN*-сервер. Це означає, що дії користувача в мережі стають менш прозорими для сторонніх спостерігачів, включаючи інтернет-провайдерів, що може бути корисним для захисту приватності та обходу географічних обмежень.

Останнім часом *VPN* стає все більш важливим елементом в системі інформаційної безпеки IT-компаній. Зокрема, з поширенням роботи на віддаленому доступі та збільшенням кількості мобільних пристроїв в корпоративному використанні.

2.2. Принципи роботи технології *VPN*

Віртуальна приватна мережа є технологією, яка використовується для створення безпечного та приватного з'єднання між пристроями через відкриті мережі, такі як Інтернет. *VPN* побудована на трьох основних принципах: шифрування, тунелювання та аутентифікація.

2.2.1. Шифрування

Шифрування в мережах *VPN* забезпечує конфіденційність даних, перетворюючи читабельну інформацію (відому як текст відкритого доступу) в нечитабельний формат (відомий як шифротекст) за допомогою алгоритму шифрування. Шифровані дані можуть бути розшифровані або повернуті до їхнього оригінального формату лише за допомогою відповідного ключа шифрування. На рис. 2.2 зображено загальну схему шифрування даних у *VPN* мережі.

Процес шифрування даних у віртуальній приватній мережі є важливим елементом забезпечення конфіденційності та безпеки інформації. Послідовність дій, які відбуваються під час шифрування та передачі даних через *VPN*:

− користувацький пристрій (*User Device*). Користувацький пристрій відправляє дані до *VPN*-клієнта для подальшого шифрування та передачі;

− *VPN*-клієнт (*VPN Client*). *VPN*-клієнт шифрує дані, які він отримав від користувацького пристрою, за допомогою спільного секретного ключа. Цей ключ є унікальним для кожного *VPN*-з'єднання і використовується для шифрування та розшифрування даних;

– *VPN*-сервер (*VPN Server*). Це сервер, який приймає вхідні *VPN*-з'єднання. Після отримання зашифрованих даних від *VPN*-клієнта, *VPN*-сервер розшифровує ці дані за допомогою того ж спільного секретного ключа. Після розшифрування, *VPN*-сервер відправляє дані до Інтернету;

– Інтернет (*Internet*). Після отримання даних від *VPN*-сервера, Інтернет обробляє запит і повертає дані запиту назад до *VPN*-сервера.

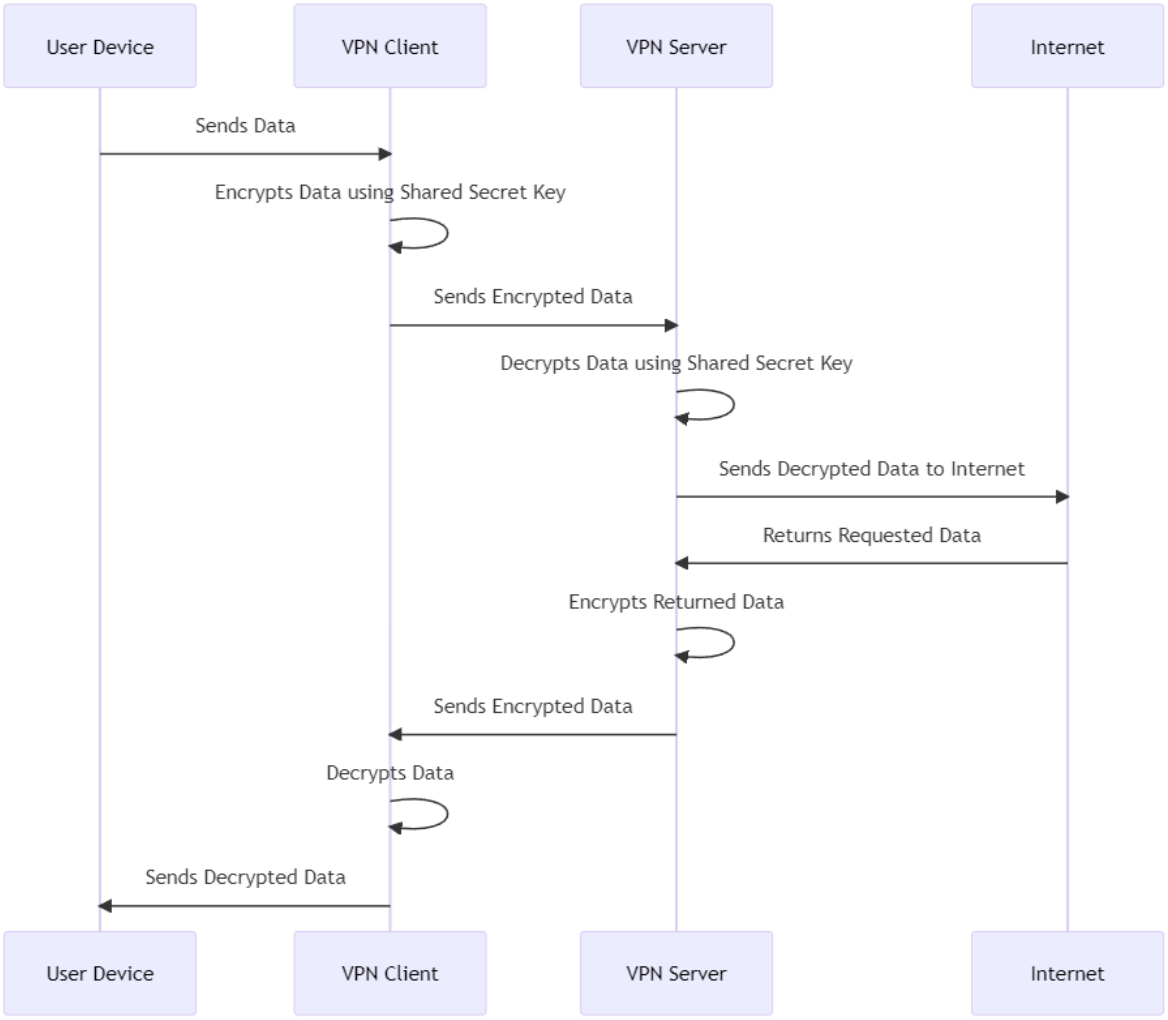


Рис. 2.2. Схема шифрування даних *VPN*-мереж

Після отримання даних від Інтернету, *VPN*-сервер знову шифрує ці дані перед тим, як відправити їх назад до *VPN*-клієнта. *VPN*-клієнт потім розшифровує ці дані за допомогою спільного секретного ключа і відправляє розшифровані дані назад до користувацького пристрою.

Завдяки вищеописаному процесу, дані залишаються конфіденційними і безпечними від початку до кінця передачі, незалежно від того, чи є підключення до Інтернету захищеним.

2.2.2. Тунелювання

Тунелювання *VPN* є процесом, за допомогою якого дані передаються приватно через публічний Інтернет. Узагальнену схему *VPN* тунелю зображено на рис. 2.3. Рис. 2.4 відображає основні компоненти та процеси, що відбуваються під час тунелювання *VPN*.

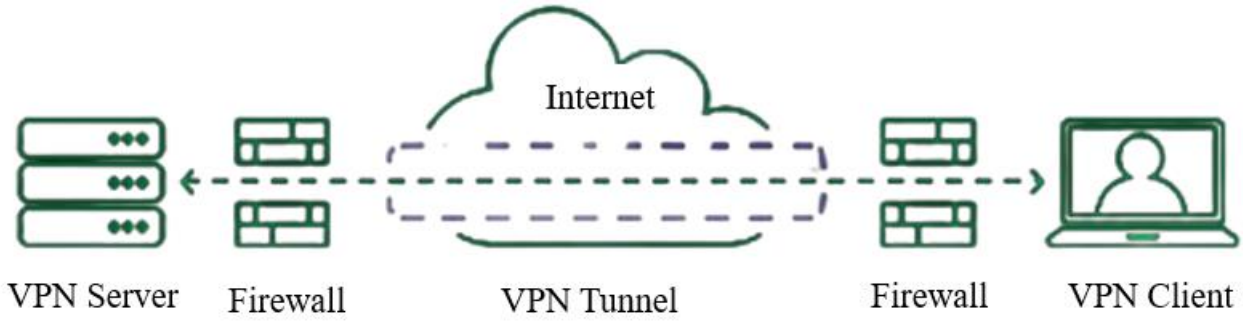


Рис. 2.3. Схема *VPN* тунелю

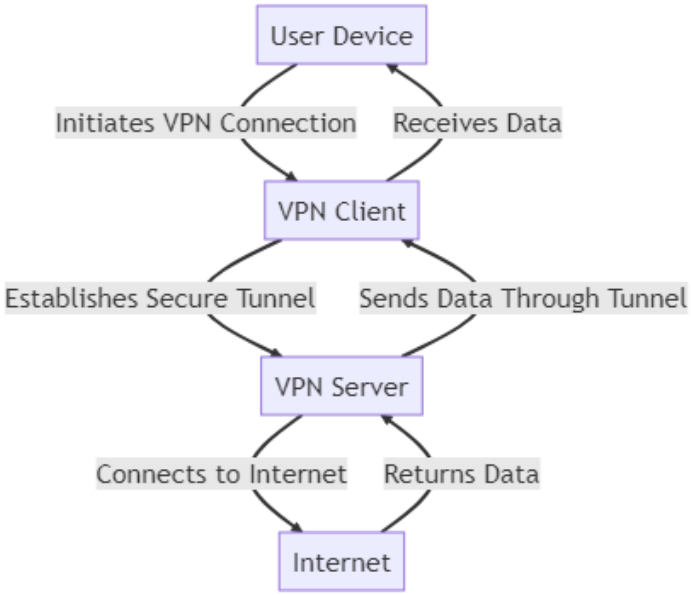


Рис. 2.4. Процес шифрування даних під час тунелювання *VPN*

Взаємодія компонентів діаграми відбувається наступним чином:

– користувацький пристрій (*User Device*). Користувач ініціює з'єднання з *VPN*, відправляючи запит на підключення до *VPN*-клієнта;

– *VPN*-клієнт (*VPN Client*). Після отримання запиту від користувача, *VPN*-клієнт встановлює безпечний тунель до *VPN*-сервера. Цей тунель є віртуальним "коридором", через який передаються дані, і він забезпечує їх безпеку від зовнішніх втручань;

− *VPN*-сервер (*VPN Server*). Після встановлення безпечного тунелю, *VPN*-сервер здійснює доступ до Інтернету від імені користувача. Це означає, що всі запити до Інтернету виглядають так, ніби вони відправлені з *VPN*-сервера, а не від пристрою користувача, що забезпечує анонімність користувача;

− Інтернет (*Internet*). Після отримання запиту від *VPN*-сервера, Інтернет повертає запитані дані назад до *VPN*-сервера.

Після отримання даних від Інтернету, *VPN*-сервер надсилає ці дані назад через безпечний тунель до *VPN*-клієнта на пристрої користувача. *VPN*-клієнт потім передає ці дані до користувацького пристрою.

2.2.3. Аутентифікація

Автентифікація — це процес перевірки та визначення того, чи хтось (щось) є тим, за кого себе видає. Дана технологія передбачає перевірку відповідності облікових даних, які вводить користувач, даним, які зберігаються в аутеризованій базі динних користувачів або на виділеному сервері аутентифікації [20].

Існує декілька видів аутентифікації.Однофакторна аутентифікація (*SFA*) – зазвичай використовує ідентифікатор користувача та відповідний йому пароль. У цьому випадку, з метою ідентифікації, користувач надає свій унікальний номер (код) *id*, а процес аутентифікації відбувається пізніше, коли користувач вводить пароль, або інші облікові дані, які мають відповідати номеру *id*. Часто, однофакторна аутентифікація є недостатнім захистом, тому, на сьогоднішній день, широко використовується двофакторна аутентифікація (*2FA*). Даний процес може включати в себе відправку *SMS* повідомлення на мобільний телефон, а також використання біометричних даних користувача, таких як відбиток пальця, сканування обличчя тощо. Багатофакторна аутентифікація(*MFA*) – використовує три та більше позицій перевірки автентичності особи та забезпечує найвищий рівень захисту, може вимагати від користувача номер *id*, пароль, біометричні дані, а також відповіді на заздалегіть підготоване питання.

Процес аутентифікації *VPN* є важливим етапом встановлення безпечного *VPN*-з'єднання. На рис. 2.5 представлено послідовність дій, які відбуваються під час аутентифікації *VPN*.

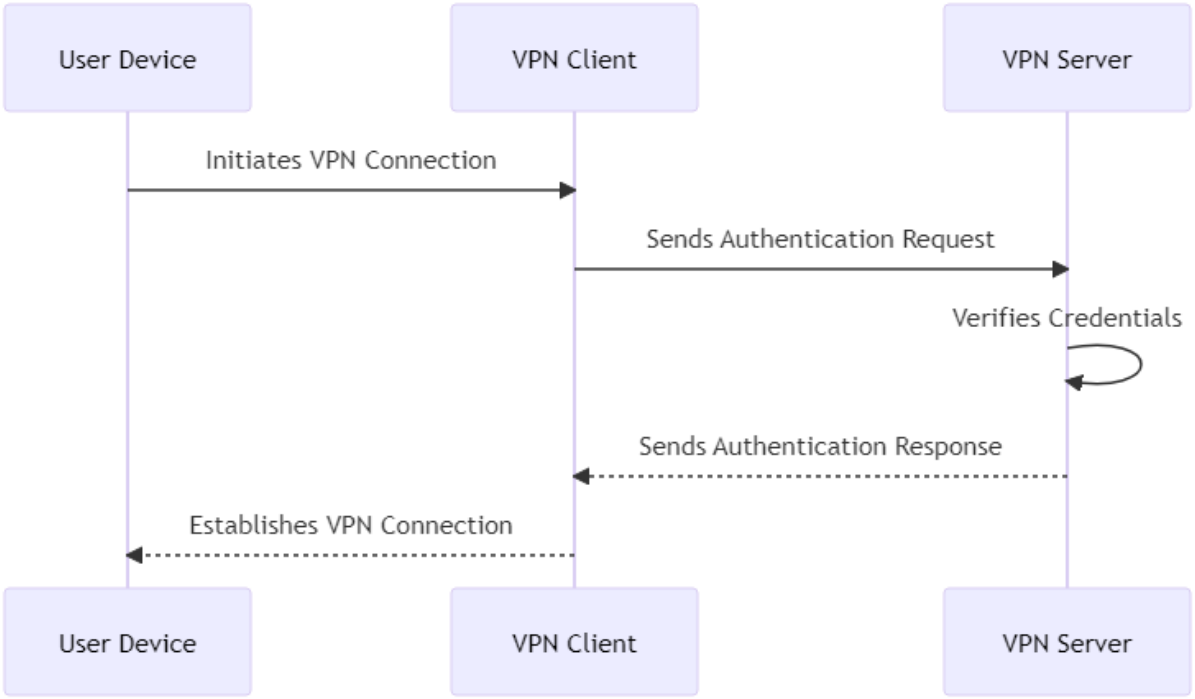


Рис. 2.5. Процес аутентифікації *VPN*

Процес аутентифікації користувача у мережі *VPN* включає в себе:

– користувацький пристрій (*User Device*). Користувацький пристрій відправляє запит на встановлення *VPN*-з'єднання до *VPN*-клієнта;

– *VPN*-клієнт (*VPN Client*). Після отримання запиту від користувача, *VPN*-клієнт відправляє запит на аутентифікацію до *VPN*-сервера. Запит на аутентифікацію зазвичай включає в себе облікові дані користувача, такі як ім'я користувача та пароль;

– *VPN*-сервер (*VPN Server*). Після отримання запиту на аутентифікацію від *VPN*-клієнта, *VPN*-сервер перевіряє облікові дані користувача. Якщо облікові дані вірні, *VPN*-сервер відправляє відповідь про аутентифікацію до *VPN*-клієнта.

Після отримання відповіді про аутентифікацію від *VPN*-сервера, *VPN*-клієнт встановлює *VPN*-з'єднання і повідомляє користувацький пристрій про успішне встановлення з'єднання.

Завдяки цьому процесу, тільки авторизовані користувачі можуть встановити *VPN*-з'єднання, що допомагає забезпечити безпеку та конфіденційність даних.

2.3. Алгоритми шифрування

Сучасні *VPN* мережі різноманітні та надзвичайно гнучкі щодо використання різних алгоритмів шифрування. Декілька найпоширеніших алгоритмів включають *AES*, *Blowfish*, *3DES* та *Camellia*.

Advanced Encryption Standard (AES). Це один з найпоширеніших алгоритмів, який використовується у *VPN*. Це симетричний алгоритм шифрування, який використовує блоки даних розміром 128 біт та ключі довжиною 128, 192 або 256 біт. *AES-256* вважається досить безпечним для усіх комерційних застосувань і є стандартом для урядових органів США [21, 22].

Схему роботи алгоритму *AES* зображено на рис. 2.6.

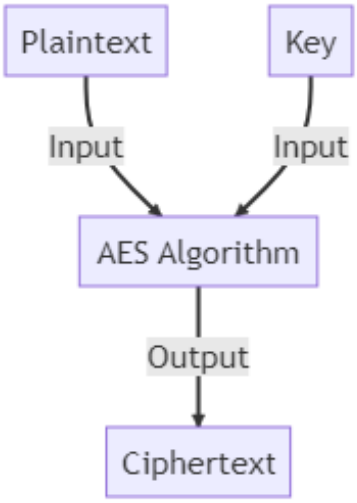


Рис. 2.6. Схема роботи алгоритму *AES*

AES є симетричним алгоритмом шифрування, який використовує один і той же ключ для шифрування та розшифрування даних. Основні компоненти та процеси, що відбуваються під час шифрування *AES*:

− відкритий текст (*Plaintext*). Це вихідні дані, які потрібно зашифрувати. Відкритий текст може бути будь-якими даними, наприклад,

текстовим повідомленням, файлом або пакетом даних. Відкритий текст вводиться в алгоритм *AES* як вхідні дані;

− ключ (*Key*). Це секретний ключ, який використовується для шифрування відкритого тексту. Ключ також вводиться в алгоритм *AES* як вхідні дані. Важливо, що цей ключ повинен бути відомий тільки відправнику та отримувачу даних, оскільки він використовується для шифрування та розшифрування даних;

− алгоритм *AES* (*AES Algorithm*). Це серцевина процесу шифрування. Алгоритм *AES* приймає відкритий текст та ключ як вхідні дані, а потім використовує ряд математичних операцій для перетворення відкритого тексту в зашифрований текст. Ці операції включають в себе ряд раундів субституції, перестановки, змішування та додавання раундового ключа;

− зашифрований текст (*Ciphertext*). Це зашифровані дані, які виводяться з алгоритму *AES*. Зашифрований текст має вигляд нерозбірливого набору даних, який може бути розшифрований тільки за допомогою того ж ключа, який був використаний для шифрування.

Цей процес забезпечує, що дані можуть бути безпечно передані через небезпечні мережі, такі як Інтернет, без ризику їх перехоплення та розшифрування несанкціонованими особами.

Triple Data Encryption Standard (3DES). Це покращена версія оригінального *DES*, який був одним з перших алгоритмів шифрування. *3DES* виконує шифрування *DES* тричі для кожного блоку даних, що забезпечує більший рівень безпеки, але він вважається повільнішим, ніж більш сучасні алгоритми, такі як *AES*. Його детальну схему зображено на рис. 2.7.

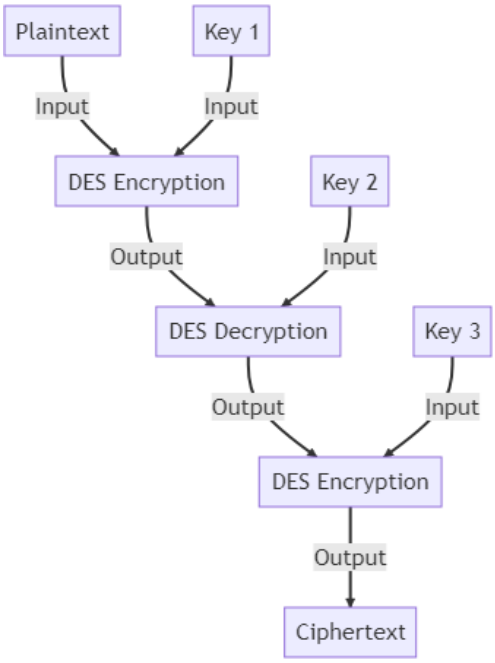


Рис. 2.7. Схема роботи алгоритму *3DES*

3DES є симетричним алгоритмом шифрування, який використовує один або три окремі 64-бітні ключі для шифрування та розшифрування даних. На рисунку 2.7 представлено основні компоненти та процеси, що відбуваються під час шифрування *3DES*, а саме:

– відкритий текст (*Plaintext*). Відкритий текст вводиться в перший етап шифрування DES як вхідні дані;

– ключі (*Key* 1, *Key* 2, *Key* 3). Секретні ключі, які використовуються для шифрування відкритого тексту. Кожен ключ вводиться в свій відповідний етап шифрування *DES* як вхідні дані;

– етапи шифрування *DES* (*DES Encryption, DES Decryption*). Це серцевина процесу шифрування. Кожен етап *DES* приймає вихідні дані попереднього етапу та відповідний ключ як вхідні дані, а потім використовує ряд математичних операцій для перетворення вхідних даних. Перший та третій етапи виконують шифрування, а другий етап виконує розшифрування;

– зашифрований текст (*Ciphertext*). Це зашифровані дані, які виводяться з останнього етапу шифрування *DES*. Зашифрований текст має вигляд нерозбірливого набору даних, який може бути розшифрований тільки за допомогою тих же ключів, які були використані для шифрування.

3DES використовується в ситуаціях, коли потрібна вища ступінь безпеки, ніж та, що надається оригінальним алгоритмом *DES* [23].

Camellia. Це алгоритм шифрування, який вважається еквівалентом *AES* і також використовує блоки даних розміром 128 біт та ключі довжиною 128, 192 або 256 біт. Він не є таким поширеним, як *AES*, але все ж використовується в деяких *VPN*. Детальну схему роботи алгоритму *Camellia* зображено на рис. 2.8.

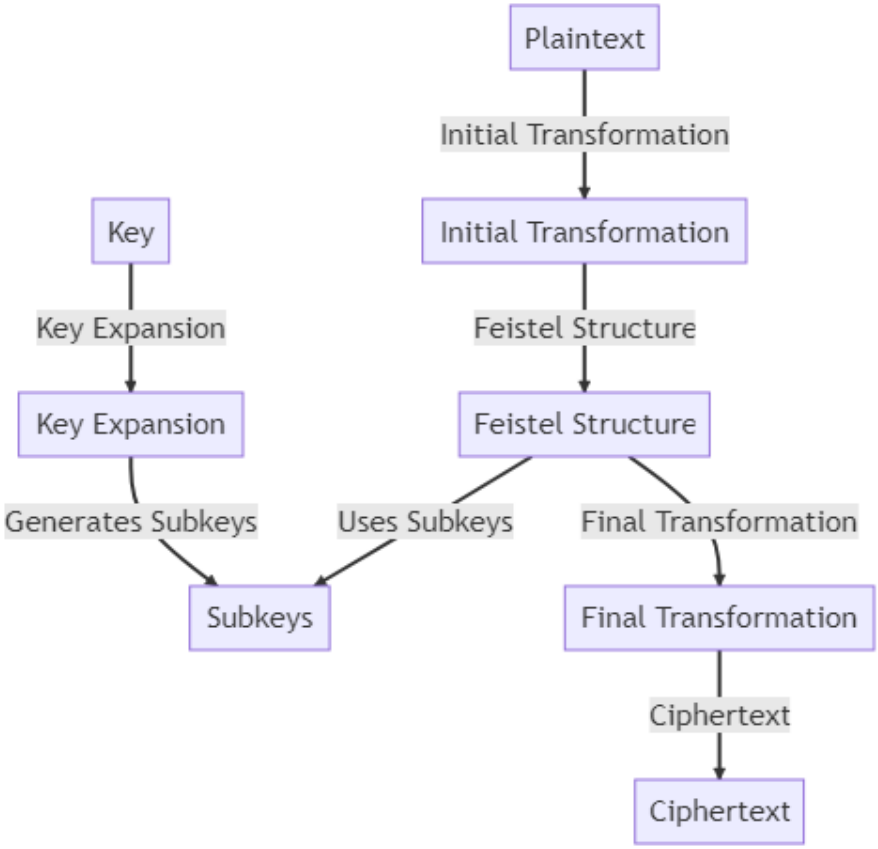


Рис. 2.8. Схема роботи алгоритму *Camellia*

Алгоритм *Camellia* є симетричним алгоритмом блочного шифрування, розробленим в Японії. Він використовує однаковий ключ для шифрування та дешифрування даних.

Принцип роботи алгоритму та основні складові:

– ключ (*Key*). Це секретний ключ, який використовується для шифрування та дешифрування даних. Він передається до процесу розширення ключа;

– розширення ключа (*Key Expansion*). В цьому процесі ключ розширюється та генерує набір підключів;

− підключі (*Subkeys*). Це ключі, які генеруються під час розширення ключа. Вони використовуються в структурі *Feistel* для шифрування даних;

− відкритий текст (*Plaintext*). Це вхідні дані, які потрібно зашифрувати. Вони проходять через початкову трансформацію перед тим, як ввійти в структуру *Feistel*;

− початкова трансформація (*Initial Transformation*). Це перший крок в процесі шифрування, де відкритий текст трансформується перед входом в структуру *Feistel;*

− структура *Feistel* (*Feistel Structure*). Це серце алгоритму *Camellia*, де відбувається більшість шифрування. Вона використовує підключі для шифрування даних;

− кінцева трансформація (*Final Transformation*). Після того, як дані проходять через структуру *Feistel*, вони проходять через кінцеву трансформацію, щоб отримати кінцевий зашифрований текст;

− зашифрований текст (*Ciphertext*). Це кінцевий результат шифрування, який отримується після кінцевої трансформації.

Варто зазначити, що, хоча сильніші алгоритми шифрування забезпечують вищий рівень безпеки, вони також суттєво знижують продуктивність через великі вимоги до обчислювальних потужностей.

Асиметричне шифрування використовує пару ключів: приватний ключ, який зберігається в таємниці, та публічний ключ, який може бути вільно розповсюджений. Дані, зашифровані публічним ключем, можна розшифрувати лише приватним ключем, і навпаки.

Асиметричне шифрування є більш складним і працює повільніше, ніж симетричні канали, але воно дозволяє вирішити проблему пересилання секретного ключа відкритими каналами, притаманну симетричним алгоритмам. На практиці ж, можливе використання поєднання цих технологій, при якому самі дані шифруються більш швидким симетричним методом, а асиметричний алгоритм використовується для пересилання секретного ключа симетричного алгоритму [24].

2.4. Протоколи *VPN*

Протоколи *VPN* – це набори інструкцій, які визначають, як передаються дані в мережі *VPN*. Існує декілька протоколів *VPN*, кожен з яких має свої особливості, переваги та недоліки. Найбільш поширеними протоколами є:

PPTP (Point-to-Point Tunneling Protocol). Це один з найдавніших протоколів *VPN*, що походить від 1990-х років. Він пропонує найвищі швидкості та найменше використання обчислювальних ресурсів. Однак його рівень безпеки вважається слабким і він не рекомендований для сучасних застосувань. Схема роботи протоколу *PPTP*, що зображена на рис.2.9 показує, як *PPTP* використовує тунелювання для передачі даних між клієнтом та сервером.

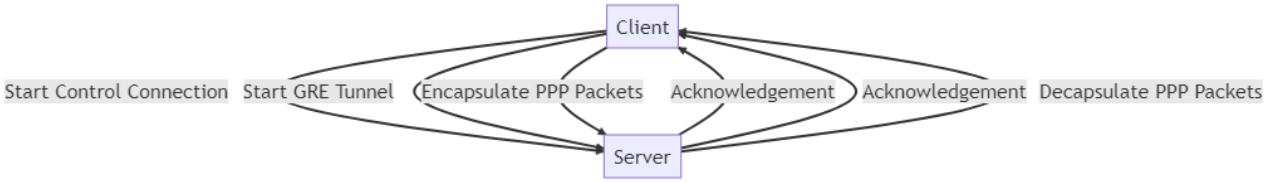


Рис. 2.9. Схема роботи протоколу *PPTP*

Протокол тунелювання точка-до-точки є методом створення віртуальної приватної мережі. Він використовує протокол керування тунелями для створення, управління та видалення сесій тунелювання між точками доступу. Ось детальний опис процесу, зображеного на схемі (див. рис. 2.9):

− клієнт (*Client*). Це пристрій, який ініціює з'єднання з сервером. Клієнт починає процес, відправляючи запит на встановлення керування з'єднанням до сервера;

− сервер (*Server*). Це пристрій, який отримує запит від клієнта. Після отримання запиту на встановлення керування з'єднанням від клієнта, сервер відправляє підтвердження назад до клієнта;

− початок *GRE*-тунелю (*Start GRE Tunnel*). Після встановлення керування з'єднанням, клієнт починає процес створення *GRE*-тунелю. *GRE*

(*Generic Routing Encapsulation*) – це протокол, який дозволяє інкапсуляцію різних типів пакетів мережі в пакети іншої мережі;

− інкапсуляція *PPP*-пакетів (*Encapsulate PPP Packets*). Після створення *GRE*-тунелю, клієнт починає інкапсуляцію *PPP* (*Point-to-Point Protocol*) пакетів. Це означає, що дані, які потрібно передати, упаковуються в *PPP*-пакети, а потім відправляються через *GRE*-тунель;

− декапсуляція *PPP*-пакетів (*Decapsulate PPP Packets*). Коли *PPP*-пакети досягають сервера, вони декапсулюються, що означає, що дані витягуються з *PPP*-пакетів. Після декапсуляції дані можуть бути оброблені сервером [25].

L2TP/IPsec (Layer 2 Tunneling Protocol with IP Security). L2TP створює тунель між двома точками з'єднання, а *IPsec* забезпечує шифрування даних, що проходять через цей тунель. Він пропонує солідний рівень безпеки, але може бути повільнішим через двійкову обробку даних [26].

Схема роботи протоколу *L2TP/IPsec* зображено на рис. 2.10. Протокол тунелювання другого рівня (*L2TP*) з *IP*-безпекою (*IPsec*) є методом створення віртуальної приватної мережі. Він використовує *L2TP* для створення тунелю та *IPsec* для шифрування даних, що проходять через тунель. Процес, що зображено на схемі (рис. 2.10) виглядає наступним чином:

− *VPN*-клієнт (*VPN Client*). Це пристрій, який ініціює з'єднання з *VPN*-сервером. Він відправляє пакет *L2TP* до сервера *L2TP/IPsec*;

− сервер *L2TP/IPsec* (*L2TP/IPsec Server*). Це сервер, який отримує пакет *L2TP* від *VPN*-клієнта. Він шифрує пакет *L2TP* за допомогою *IPsec* і відправляє зашифрований пакет через Інтернет;

− *IPsec*. Це протокол безпеки, який використовується для шифрування пакетів *L2TP*. Він шифрує дані перед їх відправкою через Інтернет;

− Інтернет (*Internet*). Це мережа, через яку передаються зашифровані дані;

− *IPsec* на місці призначення (*IPsec at Destination*). Це *IPsec* на сервері призначення. Він розшифровує дані, отримані через Інтернет;

– сервер *L2TP/IPsec* на місці призначення (*L2TP/IPsec Server at Destination*). Це сервер на місці призначення, який отримує розшифрований пакет *L2TP* від *IPsec*.

– місце призначення (*Destination*). Це кінцеве місце, куди дані потрібно доставити дані. Він отримує розшифровані дані від сервера *L2TP/IPsec*.

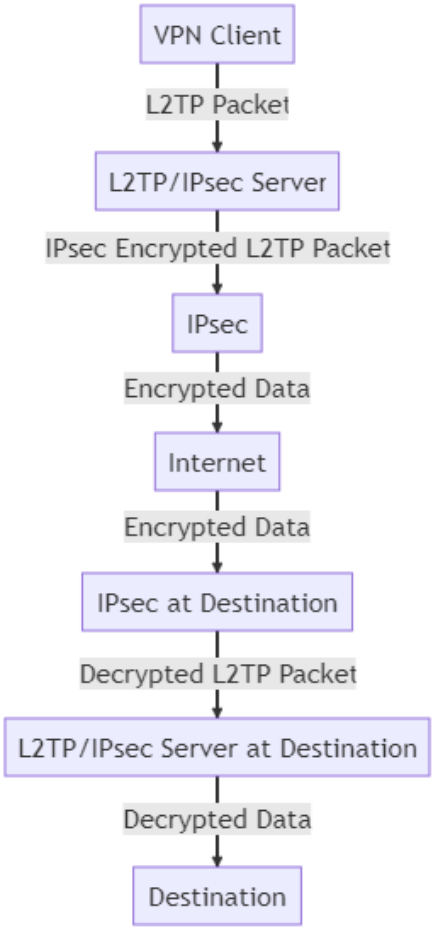


Рис. 2.10. Схема роботи протоколу *L2TP/IPsec*

Також, можна виділити й такі протоколи як:

– *SSTP* (*Secure Socket Tunneling Protocol*). Цей протокол надає захищене з'єднання через зашифровані *SSL*/*TLS* канали. *SSTP* відомий тим, що може обходити більшість блокувань брандмауера, але він переважно обмежений *Windows*;

– *IKEv2* (*Internet Key Exchange version 2*). Цей протокол ідеально підходить для мобільних пристроїв через його здатність швидко перез'єднуватись при втраті з'єднання. *IKEv2* може бути використаний самостійно або в поєднанні з *IPsec* для збільшення безпеки;

− *OpenVPN*. Підтримує багато методів шифрування, добре працює через брандмауери, пропонує високий рівень безпеки та може бути використаний на багатьох платформах.

Протоколи *VPN*, такі як *PPTP*, *L2TP/IPsec*, *SSTP*, *IKEv2* та *OpenVPN*, відіграють критичну роль у забезпеченні безпечного і приватного з'єднання в мережі. Вони мають різні характеристики, включаючи швидкість, рівень безпеки, сумісність з різними операційними системами, а також здатність працювати в різних мережевих умовах.

PPTP, який є одним з найдавніших протоколів *VPN*, може забезпечити швидке з'єднання, але має низький рівень безпеки. *L2TP/IPsec* та *SSTP* надають більш високий рівень безпеки, але можуть бути повільнішими за швидкістю. *IKEv2* ідеально підходить для мобільних пристроїв завдяки своїй здатності швидко відновлювати з'єднання. *OpenVPN* має високу ступінь безпеки, гнучкість та сумісність.

Таким чином, при виборі протоколу *VPN* для IT-компанії необхідно враховувати ці різні аспекти, щоб забезпечити оптимальний баланс між безпекою, швидкістю, сумісністю та функціональністю.

2.5. Типи мереж *VPN* та їх характеристики

Віртуальні приватні мережі були розроблені з метою установлення безпечного, приватного з'єднання між різними точками в мережі через використання зашифрованих каналів передачі даних. Вони допомагають гарантувати приватність та анонімність при онлайн-спілкуванні та можуть бути розглянуті як мости, що з'єднують різні локальні мережі (*LAN*) в одну широку мережу.

Серед основних типів організації мереж *VPN* можна виділити два: мережі *VPN* типу "віддалений доступ" (*Remote Access VPN;* з’єднання типу клієнт-мережа) та мережі *VPN* типу "сайт-до-сайту" (*Site-to-Site VPN* або мережа-мережа). Структури цих типів мереж зображено на рис. 2.11.

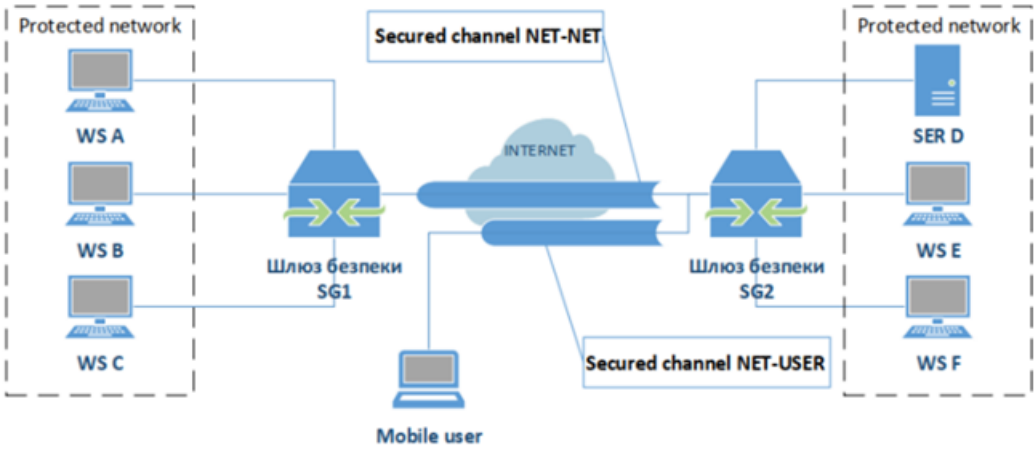


Рис. 2.11. Канали *VPN* типу мережа-мережа, клієнт-мережа.

Віддалений доступ VPN. Віддалений доступ *VPN*, також відомий як *Virtual Private Dial-up Network* (*VPDN*), це тип *VPN*, який дає користувачам можливість встановлювати безпечне з'єднання з корпоративною мережею віддалено. Цей тип мережі зазвичай використовується співробітниками компаній, які працюють поза офісом та потребують доступу до корпоративних ресурсів. Він використовує тунельний протокол, щоб забезпечити безпечність даних, і потребує від користувача аутентифікації для доступу до мережі [27].

Сайт-до-сайту VPN. Мережі *VPN* типу "сайт-до-сайту", також відомі як *Router-to-Router VPN*, з'єднують дві або більше мереж в одну. Цей тип *VPN* використовується, коли декілька відділень однієї компанії потребують постійного з'єднання між собою для обміну інформацією. У цьому випадку, *VPN* забезпечує з'єднання між двома маршрутизаторами, і всі дані, що проходять через це з'єднання, автоматично зашифровуються.

VPN типу "сайт-до-сайту" на основі інтрамережі об'єднує більше однієї локальної мережі у глобальну мережу (*WAN*). Компанія також може використовувати цей тип налаштування для об’єднання програмно визначеної глобальної мережі (*SD-WAN*). Межвузлові *VPN* на основі інтрамережі є корисними інструментами для безпечного об’єднання ресурсів, розміщених у різних офісах, ніби всі вони знаходяться в одному фізичному місці.

VPN типу "сайт-до-сайту" на основі інтрамережі особливо корисний, якщо кожен відділ або розробляє власні ресурси, або розміщує унікальні

процеси, доступ до яких даватиме користь усій компанії. Наприклад, якби кожен офіс розробляв продукт, що постійно оновлюється та підлаштовується до клієнтів, *VPN* типу "сайт-до-сайту" давала б особам, які приймають рішення, безпечний доступ до всього, що виробляється, незалежно від їх фізичного розташування.

Межвузлові *VPN* на основі екстрамережі часто використовуються двома або більше різними компаніями, які хочуть спільно використовувати певні ресурси, але залишати інші приватними. Завдяки мережі *VPN* типу "сайт-до-сайту" кожна організація підключається до мережі *VPN* і вибирає, що вона хоче зробити доступною для інших компаній. Таким чином вони можуть співпрацювати та ділитися без розголошення конфіденційних даних [28].

Кожен з цих типів *VPN* використовує різні методи шифрування та протоколи для забезпечення безпечного з'єднання і захисту даних. Вибір типу *VPN* залежить від конкретних потреб IT-компанії, зокрема, від кількості мереж, які потребують з'єднання, та вимог до доступу до мережі.

2.6. Процес проходження *IP*-пакету мережею з налаштованим *VPN*

Технологія *VPN* надає захист інформації, створюючи безпечне "тунельне" з'єднання через небезпечну публічну мережу. Однак, щоб глибше зрозуміти, як *VPN* забезпечує цей рівень захисту, потрібно детально розглянути процес, за допомогою якого *IP*-пакети проходять через мережу з налаштованим *VPN*. Схему процесу проходження *IP*-пакету мережею з налаштованим *VPN* представлена на рис. 2.12.

Наведена схема (рис. 2.12) показує, як *VPN* забезпечує безпечну передачу *IP*-пакетів через небезпечні мережі, такі як Інтернет, шляхом інкапсуляції *IP*-пакетів у *VPN*-пакети.

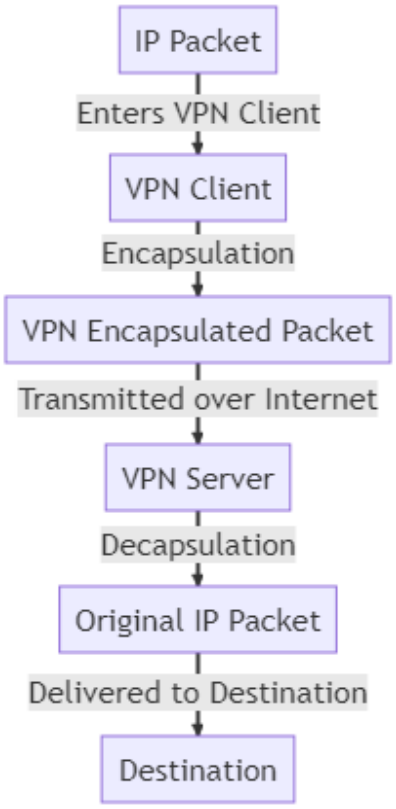


Рис. 2.12. Процес проходження *IP*-пакету мережею з налаштованим *VPN*

Схема проходження *IP*-пакету мережею з налаштованим *VPN* включає в себе наступні етапи:

– *IP*-пакет (*IP Packet*). Це основна одиниця передачі даних в мережах *IP*. Кожен *IP*-пакет містить в собі дані (вміст), які потрібно передати, а також метадані, такі як *IP*-адреса відправника та отримувача;

– клієнт *VPN* (*VPN Client*). Це програмне забезпечення або пристрій, який встановлює *VPN*-з'єднання. Коли *IP*-пакет входить в *VPN*-клієнт, він інкапсулюється в *VPN*-пакет;

– інкапсуляція (*Encapsulation*). Це процес, під час якого *IP*-пакет вкладається в *VPN*-пакет. Це забезпечує безпеку даних, оскільки вміст *IP*-пакету стає невидимим для будь-кого, хто спостерігає за передачею даних;

– *VPN*-пакет (*VPN Encapsulated Packet*). Це пакет даних, який містить в собі оригінальний IP-пакет. Він передається через Інтернет до *VPN*-севера;

– *VPN*-сервер (*VPN Server*). Це сервер, який приймає *VPN*-пакети від *VPN*-клієнта. Він декапсулює *VPN*-пакет, витягуючи оригінальний IP-пакет;

− декапсуляція (*Decapsulation*). Це процес, під час якого *VPN*-пакет відкривається, і оригінальний *IP*-пакет витягується. Після цього *IP*-пакет може бути доставлений до свого призначення;

− оригінальний *IP*-пакет (*Original IP Packet*). Це *IP*-пакет, який був вкладений в *VPN*-пакет. Після декапсуляції він доставляється до свого призначення;

− призначення (*Destination*). Це кінцеве місце, куди доставляється *IP*-пакет. Це може бути сервер, комп'ютер або будь-який інший пристрій, що під’єднано до мережі.

2.7. Поняття та типи реплікації даних в контексті використання *VPN*

Реплікація даних є критичною компонентою більшості сучасних систем обробки даних, що забезпечує високу доступність, продуктивність та надійність. У своїй основі реплікація даних полягає у створенні та управлінні копіями даних в різних місцях з метою підвищення доступності даних та зменшення ризику втрати даних.

В контексті використання *VPN*, реплікація даних може бути особливо корисною для організацій з розгалуженою структурою, які потребують обміну даними між різними локаціями. Використання *VPN* дозволяє безпечно та ефективно передавати дані для реплікації через публічні мережі.

Способи реплікації даних варіюються, і вибір залежить від конкретних вимог до доступності, продуктивності, співвідношення вартості та складності системи. Серед найпоширеніших типів реплікації даних варто відзначити:

− майстер-слейв реплікація. В цьому типі реплікації одна база даних (майстер) служить як основне джерело даних, і всі зміни відбуваються на ньому. Зміни потім передаються до одного або більше слейвів;

− мульти-майстер реплікація. У цьому випадку декілька баз даних можуть приймати зміни, і ці зміни потім реплікуються між всіма базами даних у системі;

− асинхронна та синхронна реплікація. У асинхронній реплікації зміни записуються в основну копію даних, а потім розповсюджуються на репліки з певною затримкою. У синхронній реплікації зміни одночасно записуються на всі репліки;

− віддалена та локальна реплікація. Віддалена реплікація передбачає розташування реплік у різних географічних локаціях для підвищення надійності та доступності. Локальна реплікація, в свою чергу, створює додаткові копії даних у тому ж місці.

Отже, використання *VPN* в комбінації з реплікацією даних може забезпечити високу надійність, доступність та безпеку даних в сучасних IT-організаціях.

Висновки за розділом

В даному розділі досліджено технологію *VPN*, що є ключовим інструментом для створення захищеної мережі в сучасних IT-компаніях. Визначено основні принципи роботи технології *VPN*, зокрема тунелювання, аутентифікацію та шифрування, що забезпечують безпеку передачі даних через публічні мережі.

Проаналізовано сучасні алгоритми шифрування, такі як *AES, 3DES* та *Camellia*, що використовуються в *VPN* для забезпечення конфіденційності даних.

Розглянуто основні протоколи *VPN*: *PPTP* та *L2TP/IPsec*, що використовуються для створення безпечного тунелю між вузлами мережі.

Визначено основні типи мереж *VPN*: віддалений доступ *VPN* та сайт-до-сайту *VPN*, які можуть бути використані в залежності від специфіки IT-структури компанії.

Описано процес проходження *IP*-пакету мережею з налаштованим *VPN*, що допомагає краще зрозуміти механізми захисту даних, які використовуються в *VPN*.

Останньою темою дослідження в розділі стала реплікація даних в контексті використання *VPN*. Визначено основні типи реплікації та їх вплив на доступність, надійність та ефективність обробки даних.

На основі отриманих результатів зроблено важливий крок до реалізації головної мети дослідження – створення захищеної мережі для ІТ-компанії з використанням технології *VPN*. У наступному розділі увага буде зосереджена на практичному впровадженні цих знань для вирішення конкретних задач в контексті розглянутої ІТ-структури.

РОЗДІЛ 3
МОДЕЛЮВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ ІТ-КОМПАНІЇ

3.1. Постановка завдання

У межах даного дослідження передбачається створення моделі інтегрованої мережевої структури, яка включає в себе центральний офіс компанії (у подальшому тексті - "*Office*") та підрозділи (віддалені майданчики "*Dep1*", "*Dep2*"), які будуть підключені через мережу інтернет.

Кожен з цих майданчиків, включаючи центральний офіс, повинен мати встановлену локальну мережу з адресацією *IPV4*, що включає в себе два окремих сегмента мережі – серверну мережу та мережу розробників/управління.

Основні бази даних (БД) компанії мають бути розміщені на двох серверах-видавцях (*Publishers*), які знаходяться в офісі компанії. Водночас, на віддалених майданчиках "*Dep1*" і "*Dep2*" мають бути встановлені реплікації (*Distributors*) основних БД компаній, з якими будуть працювати розробники цих підрозділів.

Важливою умовою є те, що доступ до основних БД компанії повинен бути обмежений лише розробниками з центрального офісу. У той же час, розробники з майданчиків "*Dep1*" та "*Dep2*" повинні мати можливість працювати тільки з реплікаціями БД, забезпечуючи розподіл завантаження між цими підрозділами.

Майданчики "*Office*", "*Dep1*" та "*Dep2*" повинні бути з’єднані між собою через *IPV4*-тунелі за допомогою процедур криптозахисту *IPSEC*, з використанням оптичного *Ethernet* середовища, організованого через *DWDM*-мережу.

Необхідно реалізувати функції *IP*-телефонії на кожному з майданчиків з можливістю наскрізної маршрутизації викликів між ними. Також слід

забезпечити доступ до мережі інтернет для всіх користувачів через центральний офіс. Завдання представляє собою складну проблему, що вимагає детального розуміння принципів роботи мережевих технологій та інтеграції різних компонентів системи.

3.2. Вимоги до обладнання мережі

З метою підключення до мережі *DWDM* необхідно застосувати обладнання, що підтримує промисловий стандарт *SFP+* (рис. 3.1).

Рис. 3.1. Маркування обладнання промислового стандарту *SFP+*

Планується використовувати маршрутизатори на майданчиках, які повинні бути обладнані мережевими інтерфейсами, сумісними з цими модулями.

Відповідно до вимог, маршрутизатори мають підтримувати наступні функції:

- диспонувати достатню кількістю мережевих інтерфейсів;
- створювати *ACL* (списки розмежування доступу) для *IPV4*;
- реалізовувати роль *DHCP*-сервера для *IPV4*;
- здійснювати процедури тунелювання трафіку;
- підтримувати функції криптозахисту *IPSEC*.

Мережеві комутатори мають включати достатню кількість портів і підтримувати технологію *VLAN*.

Сервери, призначені для основних БД та реплікацій, слід вибирати з урахуванням потреби в достатньому об’ємі внутрішнього сховища на базі накопичувачів, що підтримують *RAID*-технологію. Також сервери повинні підтримувати технологію *ILO* для діагностування стану компонентів сервера.

3.3. Вибір комутаційного та мережевого обладнання

Вибір маршрутизаторів було здійснено на користь моделі *Cisco 4461 ISR*, загальний вигляд якої зображено на рис.3.2.

Рис. 3.2. Маршрутизатор *Cisco 4461 ISR*

Цей тип маршрутизаторів відповідає вимогам щодо продуктивності та щільності портів, забезпечуючи маршрутизацію 10Гбіт/с каналів. Особливістю цього класу маршрутизаторів є можливість установки до двох вводів енергоживлення *AC* або *DC* типу.

Модулі *Cisco Gigabit Ethernet WAN* представляють собою високощільні варіанти підключення з підтримкою малого форм-фактора *Pluggable* (*SFP*) та мідних (*RJ-45*) 1 *Gigabit* і 10 *Gigabit Ethernet* (*GE*) інтерфейсів. Ці модулі призначені для використання з маршрутизаторами серії *Cisco 4000* з інтегрованими послугами (*ISR*). Максимізуючи гнучкість, модулі сприяють прискоренню таких додатків, як доступ до *Ethernet WAN*, маршрутизація між *VLAN* і високошвидкісне підключення до комутаторів і серверів локальної мережі.

Порти на цих модулях працюють як маршрутуючі порти рівня 3. Варто зазначити, що перемикання рівня 2 між локальними портами на модулі або між портами на модулі та іншими портами в системі маршрутизатора не підтримується. Порт ізолює канали рівня 2 від зовнішніх підключених комутаторів, і інформація про канали рівня 2 і *VLAN* не перемикається на інші порти в системі. Хост-маршрутизатор направляє весь трафік, що надходить до цих модулів. Модулі *Cisco Gigabit Ethernet WAN* не підтримують живлення через *Ethernet* (*PoE*) [29].

Cisco пропонує чотири типи модулів *Ethernet WAN*:

− 1-портовий модуль мережевого інтерфейсу *Cisco Gigabit Ethernet WAN* (*NIM-1GE-CU-SFP*) (рис. 3.3);

− 2-портовий модуль мережевого інтерфейсу *Cisco Gigabit Ethernet WAN* (*NIM-2GE-CU-SFP*) (рис. 3.3);

− службовий модуль *Cisco High-Density Gigabit Ethernet WAN* (*SM-X-6X1G*) (рис. 3.4);

− 4-портовий гігабітний або 1-портовий 10-гігабітний модуль *Ethernet WAN Cisco* (*SM-X-4X1G-1X10G*) (рис. 3.5).

Рис. 3.3. 1-портовий та 2-портовий модуль мережевого інтерфейсу *Cisco*

Рис. 3.4. Службовий модуль *Cisco*

Рис. 3.5. Модуль *Cisco* з підтримкою *SFP+*

Службовий модуль *Cisco* 4-портовий гігабітний або 1-портовий 10-гігабітний *Ethernet WAN* може працювати в двох взаємовиключних режимах:

− 4-портовий режим *Gigabit Ethernet*;

− 1-портовий режим 10 *Gigabit Ethernet*. При використанні порту 10 *Gigabit Ethernet*, інші порти вимикаються [30, 31].

Використовуватимуться мережеві комутатори *CBS250-24T-4X*, оснащені 24-ма 1Гбіт/с мідними портами *Ethernet* та 4-ма портами 10 біт/с з підтримкою *SFP+* (рис. 3.6).

Рис. 3.6. *CBS250-24T-4X*

Серія комутаторів *Cisco Business* 250 представляє наступне покоління економічних розумних комутаторів, що об'єднують високу продуктивність, надійність та повний набір необхідних для стабільної бізнес-мережі функцій. Відзначаючись гнучкими параметрами керування, докладними можливостями захисту та функціями статичної маршрутизації рівня 3, ці комутатори суттєво відрізняються від некерованих комутаторів або комутаторів споживчого класу, пропонуючи при цьому більш демократичну цінову політику порівняно з повністю керованими комутаторами.

Основні характеристики серії комутаторів включають:

− надійність і продуктивність. Комутатори серії *Cisco Business 250* підтримують висхідні канали зв’язку 10 *Gigabit Ethernet*, що дозволяє побудувати високопродуктивну мережу;

− статична маршрутизація рівня 3. Ця функція дозволяє сегментувати мережу на окремі робочі групи і обмінюватися даними через *VLAN* без зниження продуктивності програми. В результаті, управління внутрішньою маршрутизацією можливе за допомогою комутаторів, а маршрутизатор може бути присвячений зовнішньому трафіку та безпеці, що сприяє ефективності роботи мережі;

− живлення через *Ethernet* (*PoE*). Комутатори *Cisco Business* серії 250 доступні з *PoE+* на моделях *Gigabit Ethernet*. Ця можливість дозволяє розгортати *IP*-телефонію, бездротовий зв’язок, відеоспостереження та інші

рішення за допомогою одного мережевого кабелю, що усуває потребу в окремих джерелах живлення чи кабелях. *PoE+* забезпечує до 30 Вт потужності на порт, що ідеально підходить для розгортання точок бездротового доступу *802.11ac, IP*-камер з панорамуванням і масштабуванням (*PTZ*), відеотелефонів і тонких клієнтів, забезпечуючи більшу гнучкість та захист інвестицій;

− гарантія безпеки мережі. Комутатори з серії *Cisco Business* 250 впроваджують набір функцій безпеки та керування мережею, що сприяють підтриманню високого рівня безпеки бізнесу, відвертають несанкціонований доступ до мережі та захищають корпоративні дані. У них вбудовано системи мережевої безпеки, спрямовані на мінімізацію ризиків порушень безпеки, включають захист портів за стандартом *IEEE 802.1X* для контролю доступу до мережі, протидію атакам, що призводять до відмови в обслуговуванні, з метою підтримання безперебійної роботи мережі під час атак, а також розширений контроль доступу за допомогою списків доступу для захисту конфіденційних областей мережі від несанкціонованого доступу та захисту від мережевих атак;

− гнучкість та компактність конструкції. Детально продумана та компактна конструкція комутаторів надає додаткову гнучкість щодо їх розміщення, дозволяючи встановлювати їх в зовнішніх шафах з прокладанням проводки, таких як магазини роздрібної торгівлі, відкриті офіси або класні кімнати, без негативного впливу на навколишнє середовище;

− енергоефективність. Комутатори серії *Cisco Business 250* розроблені з урахуванням принципів енергоефективності та екологічності, не жертвуючи продуктивністю. Вони сприяють економії енергії шляхом оптимізації її використання, тим самим захищаючи навколишнє середовище та зменшуючи витрати на електроенергію [32].

3.4. Розробка схеми мережі на базі емулятора *Cisco Packet Tracer*

На загальному зображенні мережі (рис. 3.7) можна виявити три кластери, названі як "*Office*", "*Dep1*" та "*Dep2*". Всі ці кластери між собою з'єднані

оптичними каналами через емулятор *DWDM*-маршрутизатора, що на схемі позначено як "*DWDM*". Кластер "*Office*" є під'єднаним за допомогою оптичного каналу до емулятору доступу до мережі Інтернет, що на схемі відзначено як "*Internet*". У додатках А та Б, представлені в робочій області *Cisco Packet Tracer*, наведено загальну схему мережі та схему мережі кластеру "*Office*".

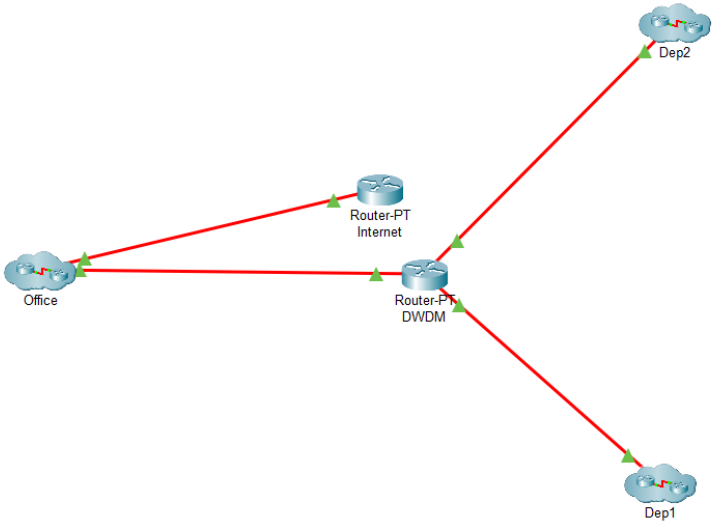


Рис. 3.7. Загальна схема мережі

На кожному з вказаних майданчиків представлено центральний маршрутизатор, створений на основі моделі маршрутизатора *Cisco 2811*, оснащений достатньою кількістю оптичних інтерфейсів (рис. 3.8).

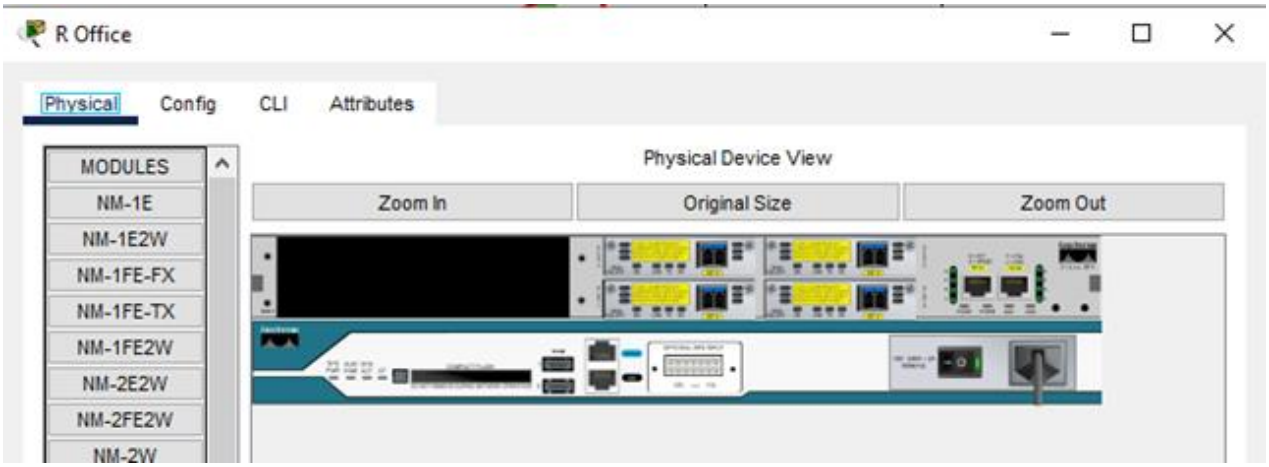


Рис. 3.8. Оптичні інтерфейси маршрутизатора *R Office*

Нульовий оптичний інтерфейс під'єднаний до *DWDM*-маршрутизатора, перший — до мережевого комутатора серверного фрагменту, другий — до мережевого комутатора розробників/управління, а третій (виключно для майданчика *Office*) — до мережі Інтернет (рис 3.9). Оскільки *IOS* емулятору *2811* не дозволяє налаштування вхідного *NAT* для *Tunnel*-інтерфейсів, на схемі

майданчика Office додатково включено вузол *R Office NAT*, що організовує доступ до мережі Інтернет для всіх клієнтів мережі. На реальному обладнанні *R Office* та *R Office NAT* буде представлено одним фізичним вузлом.

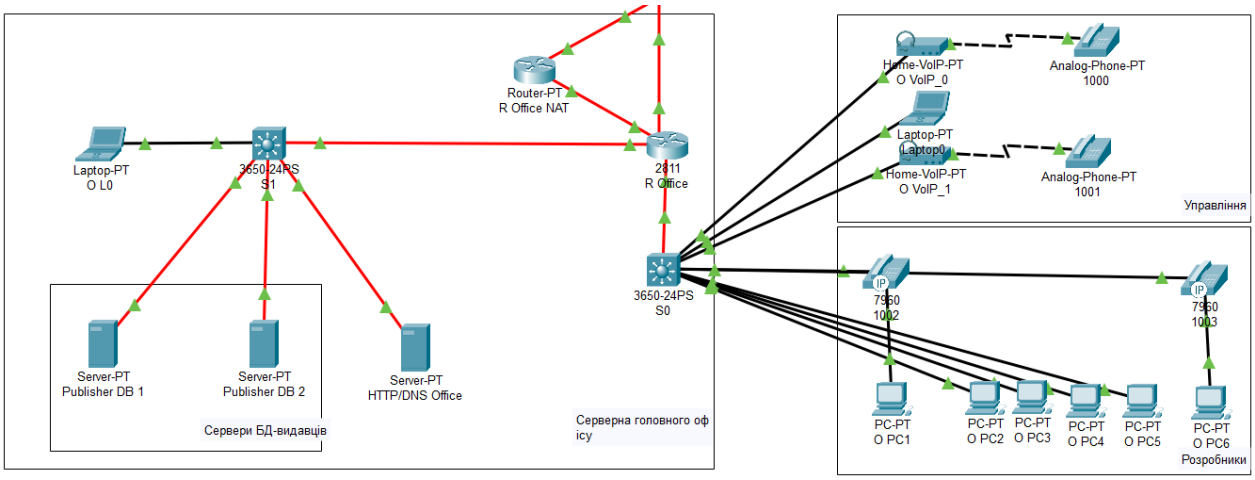


Рис. 3.9. Схема мережі майданчику *Office*

За допомогою схеми, що зображена на рис. 3.9 можна побачити відокремлене приміщення серверної, у якому розташований центральний маршрутизатор, два мережевих комутатори, які підключені до різних інтерфейсів маршрутизатора (один для підключення серверів БД, другий — для підключення мережі розробників та управління). Центральний маршрутизатор також виконує роль *DHCP*-сервера та сервера *IP*-телефонії. У серверному фрагменті на кожному з майданчиків додатково розташовано *HTTP/DNS* сервер, що обслуговує клієнтів відповідного майданчика.

3.5. З’єднання компонентів мережі за допомогою *VPN*-каналів

3.5.1. Вибір топології

Конструкцію *VPN* між вказаними майданчиками буде реалізовано використовуючи *IPV4*-тунелі. Створення цих тунелів базується на принципі "кожен-з-кожним", що означає, що кожен майданчик буде мати безпосереднє тунельне з'єднання з кожним іншим майданчиком.

Ці тунелі надають додатковий рівень захисту, оскільки вони включають функцію криптозахисту трафіку на рівні тунелю. Ця функція забезпечує

шифрування даних перед їх передачею через тунель, що забезпечує конфіденційність та цілісність даних під час передачі між майданчиками.

У результаті, *VPN*-тунелі, створені між майданчиками, забезпечують безпечне та ефективне з'єднання, що дозволяє передавати дані між різними майданчиками в безпечний і контрольований спосіб.

3.5.2. Розробка схеми адресації для *DWDM*-маршрутизатора

Потрібно розробити детальну схему адресації для «спілкування» між маршрутизатором *DWDM* і маршрутизатором кожного з окремих майданчиків. Цей процес передбачає визначення унікальних *IP*-адрес для кожного інтерфейсу, що забезпечує зв'язок між маршрутизаторами.

Схема адресації є критичним компонентом будь-якої мережі, оскільки вона визначає, як інформація буде маршрутизована між різними вузлами. Правильно сконструйована схема адресації забезпечує ефективність, швидкість і надійність передачі даних у мережі.

При розробці схеми адресації, важливо врахувати планування мережі, потреби у швидкості передачі даних та можливості масштабування мережі в майбутньому. Детальна схема адресації для цієї конфігурації представлена в табл. 3.1.

Таблиця 3.1

Схеми адресації для *DWDM*-маршрутизатора

Ділянка	Мережа	*DWDM*	Майданчик
DWDM-Office	10.0.0.0/30	10.0.0.1	10.0.0.2
DWDM-Dep1	10.0.0.4/30	10.0.0.5	10.0.0.6
DWDM-Dep2	10.0.0.8/30	10.0.0.9	10.0.0.10

3.5.3. Розробка схеми адресації для ЛОМ кожного з майданчиків

У межах даного проекту здійснюється створення систематизованого розподілу адресації локальних обчислювальних мереж (ЛОМ) для кожного майданчика. Цей процес передбачає виділення окремих діапазонів *IP*-адрес для кожного майданчика, що сприяє ефективному управлінню мережею та

спрощує процес ідентифікації вузлів. Створення забезпечує узгодженість, логічність та прозорість у мережевому проектуванні. Це, в свою чергу, полегшує подальше масштабування мережі, поліпшує мережеву безпеку і сприяє ефективному вирішенню проблем мережі. Докладний розподіл адресації локальних мереж для кожного майданчика подається в таблиці 3.2.

Таблиця 3.2

Розподіл адресації ЛОМ

Майданчик	Ділянка	Мережа	Тип	Адреса на маршрутизаторі
Office	Розр./управл.	192.168.0.0/24	Динамічна	192.168.0.1
Office	Серверна	192.168.1.0/24	Статична	192.168.1.1
Dep1	Розр./управл.	192.168.2.0/24	Динамічна	192.168.2.1
Dep1	Серверна	192.168.3.0/24	Статична	192.168.3.1
Dep2	Розр./управл.	192.168.4.0/24	Динамічна	192.168.4.1
Dep2	Серверна	192.168.5.0/24	Статична	192.168.5.1
Office	*Internet/NAT*	192.168.6.0/30	Статична	192.168.6.1

Після цього необхідно створити розподіл статичної адресації кожного з майданчиків (табл. 3.3).

Таблиця 3.3

Розподіл статичної адресації кожного з майданчиків

Майданчик	Ресурс	Адреса
Office	*БД Publisher 1*	192.168.1.2
Office	*БД Publisher 2*	192.168.1.3
Office	*DNS*	192.168.1.5
Dep1	*БД Distributor 1 1*	192.168.3.2
Dep1	*БД Distributor 1 2*	192.168.3.3
Dep1	*DNS*	192.168.3.5
Dep2	*БД Distributor 2 1*	192.168.3.2
Dep2	*БД Distributor 2 2*	192.168.3.3
Dep2	*DNS*	192.168.3.5

3.5.4. Розробка схеми адресації для *IPV4*-тунелів

У рамках цієї роботи впроваджується створення систематичного розподілу для *IPv4*-тунелів. Цей процес об'єднує всі тунелі в логічну, консистентну структуру, що забезпечує зрозумілість, управління та моніторинг тунельних з'єднань.

Такий розподіл дозволяє визначати та трекати індивідуальні тунелі, що сприяє ефективному управлінню мережею, зокрема, при виявленні і усуненні проблем, пов'язаних із з'єднаннями.

Створення розподілу для *IPv4*-тунелів є важливим кроком в побудові *VPN*-інфраструктури, оскільки воно забезпечує координованість, прозорість і логічність в управлінні тунелями. Деталізований розподіл для *IPv4*-тунелів представлено в таблиці 3.4.

Таблиця 3.4

Розподіл адресації тунелів

Тунель	Адресація	Примітка
Office-Dep1	10.0.1.0/30	*Office* – 10.0.1.1
Office-Dep2	10.0.1.4/30	*Office* – 10.0.1.5
Dep1-Dep2	10.0.1.8/30	*Dep1* – 10.0.1.9

3.6. Організація оптичної *DWDM*-мережі між майданчиками

3.6.1. Конфігурація емулятора мережі інтернет

У ході виконання проекту, специфічні налаштування будуть застосовані до емулятора маршрутизатора *DWDM*, зокрема з урахуванням встановлення адрес згідно вимог, висунутих у табл. 3.1.

Цей процес конфігурації передбачає детальне і ретельне налаштування параметрів емулятора, зокрема, налаштування *IP*-адрес, що відповідають вимогам, вказаним у таблиці 3.1.

Зазначені налаштування важливі для ефективного функціонування *DWDM* маршрутизатора в мережевому середовищі, вони впливають на маршрутизацію та обробку трафіку між різними вузлами мережі.

Повна конфігурація емулятора *DWDM* маршрутизатора, яка була виконана з урахуванням вище зазначених вимог, представлена в лістингу 3.1. Ця таблиця містить детальний список всіх налаштувань, що були застосовані до емулятора.

Лістинг 3.1

Конфігурація маршрутизатора *DWDM*

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
no ip cef
no ipv6 cef
interface GigabitEthernet0/0
ip address 10.0.0.1 255.255.255.252
interface GigabitEthernet1/0
ip address 10.0.0.5 255.255.255.252
interface GigabitEthernet2/0
ip address 10.0.0.9 255.255.255.252
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
login
end
```

3.6.2. Конфігурація інтерфейсів маршрутизаторів майданчиків

Згідно табл. 3.1 та 3.2 виконано налаштування інтерфейсів маршрутизаторів майданчиків на прикладі вузлу *R Office* (лістинг 3.2).

Лістинг 3.2

Конфігурації інтерфейсів на *R Office*

```
interface GigabitEthernet0/0/0
ip address 10.0.0.2 255.255.255.252
interface GigabitEthernet0/1/0
ip address 192.168.0.1 255.255.255.0
interface GigabitEthernet0/2/0
ip address 192.168.1.1 255.255.255.0
interface GigabitEthernet0/3/0
```

```
ip address 192.168.6.1 255.255.255.252
```

Реалізація налаштування маршрутизації відбувається з урахуванням специфікацій, вказаних у табл. 3.1. Статичний маршрут на підмережі *DWDM*-мережі виглядає наступним чином:

ip route 10.0.0.0 255.255.255.0 10.0.0.1

Цей процес орієнтований на забезпечення коректної роботи мережі за рахунок встановлення адекватних маршрутів до відповідних підмереж.

Із метою полегшення процесу додавання нових майданчиків до мережі, рекомендовано встановити маршрут до всієї мережі 10.0.0.0. Такий підхід спрощує подальше масштабування мережі та забезпечує її гнучкість.

Аналогічний процес буде виконано для конфігурації інтерфейсів маршрутизаторів *Dep1* та *Dep2*, що здійснюється відповідно до вимог, вказаних у табл. 3.1 та 3.2. Цей процес включає конфігурацію параметрів кожного з інтерфейсів з метою забезпечення їх коректної роботи в мережевому середовищі.

3.6.3. Тестування маршрутизації у створеному фрагменті мережі

У лістингу 3.3 наведено поточну таблицю маршрутизації *DWDM*-маршрутизатора.

Лістинг 3.3

Поточна маршрутизація маршрутизатору *DWDM*

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/30 is subnetted, 3 subnets
C 10.0.0.0 is directly connected, GigabitEthernet0/0 …
```

Після цього необхідно виконати перевірку доступності майданчиків *Dep1* та *Dep2* з майданчику *Office* (рис. 3.10).

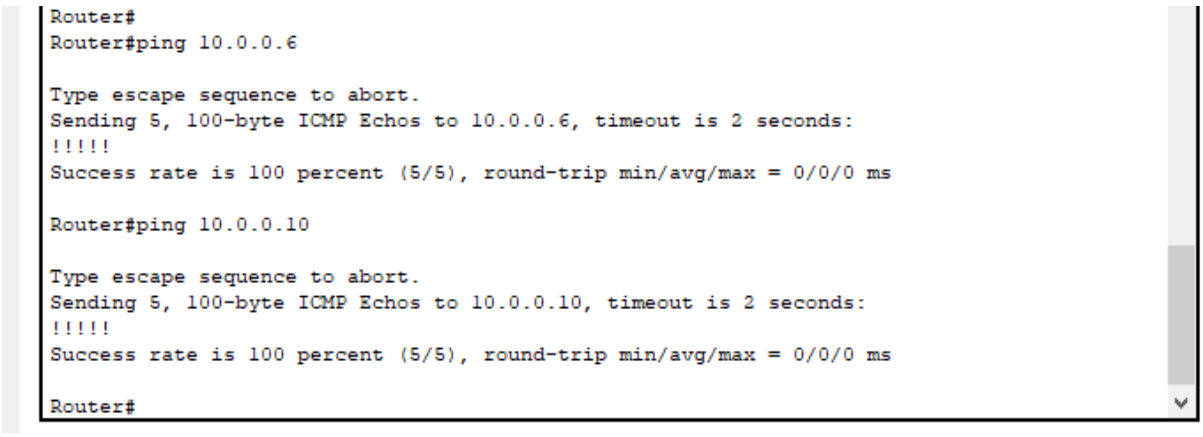


Рис. 3.10. Перевірка доступності майданчиків

3.7. Конфігурація *IPV4*-тунелів між кожним з майданчиків

3.7.1. Конфігурація тунелів

Настроювання тунелів передбачає певний комплекс дій. В якості прикладу розглянемо процес налаштування на маршрутизаторі *R Office*. Для цього маршрутизатора створюються два тунелі, що ведуть до кожного з майданчиків. Детальні параметри цих налаштувань наведені у лістингу 3.4.

Лістинг 3.4

Конфігурація тунелів на *R Office*

```
!
interface Tunnel0
ip address 10.0.1.1 255.255.255.252
mtu 1476
tunnel source GigabitEthernet0/0/0
tunnel destination 10.0.0.6
!
interface Tunnel1
ip address 10.0.1.5 255.255.255.252
mtu 1476
tunnel source GigabitEthernet0/0/0
tunnel destination 10.0.0.10
!
```

Важливим елементом цього процесу є визначення адреси джерела для тунелів. У цьому контексті в якості такої адреси буде встановлено адресу нульового оптичного інтерфейсу маршрутизатора *R Office*. Це дозволяє

забезпечити належну роботу тунелів, а також уніфікованість процесу налаштування тунельних з'єднань між маршрутизаторами.

3.7.2. Створення маршрутів через *IPV4*-тунелі

Згідно таблиці 3.3 додано статичні маршрути на мережі майданчиків *Dep1*, *Dep2* (лістинг 3.5).

Лістинг 3.5

Статичні маршрути з *R Office*

```
ip route 192.168.2.0 255.255.255.0 10.0.1.2
ip route 192.168.3.0 255.255.255.0 10.0.1.2
ip route 192.168.4.0 255.255.255.0 10.0.1.6
ip route 192.168.5.0 255.255.255.0 10.0.1.6
```

3.7.3. Тестування створеного фрагменту мережі

Наступним кроком у процесі налаштування є перевірка стану вже створених тунелів на маршрутизаторі *R Office*. Ця процедура необхідна для впевненості у правильності виконаних конфігурацій та відповідного функціонування тунелів, як це відображено на рис. 3.11.

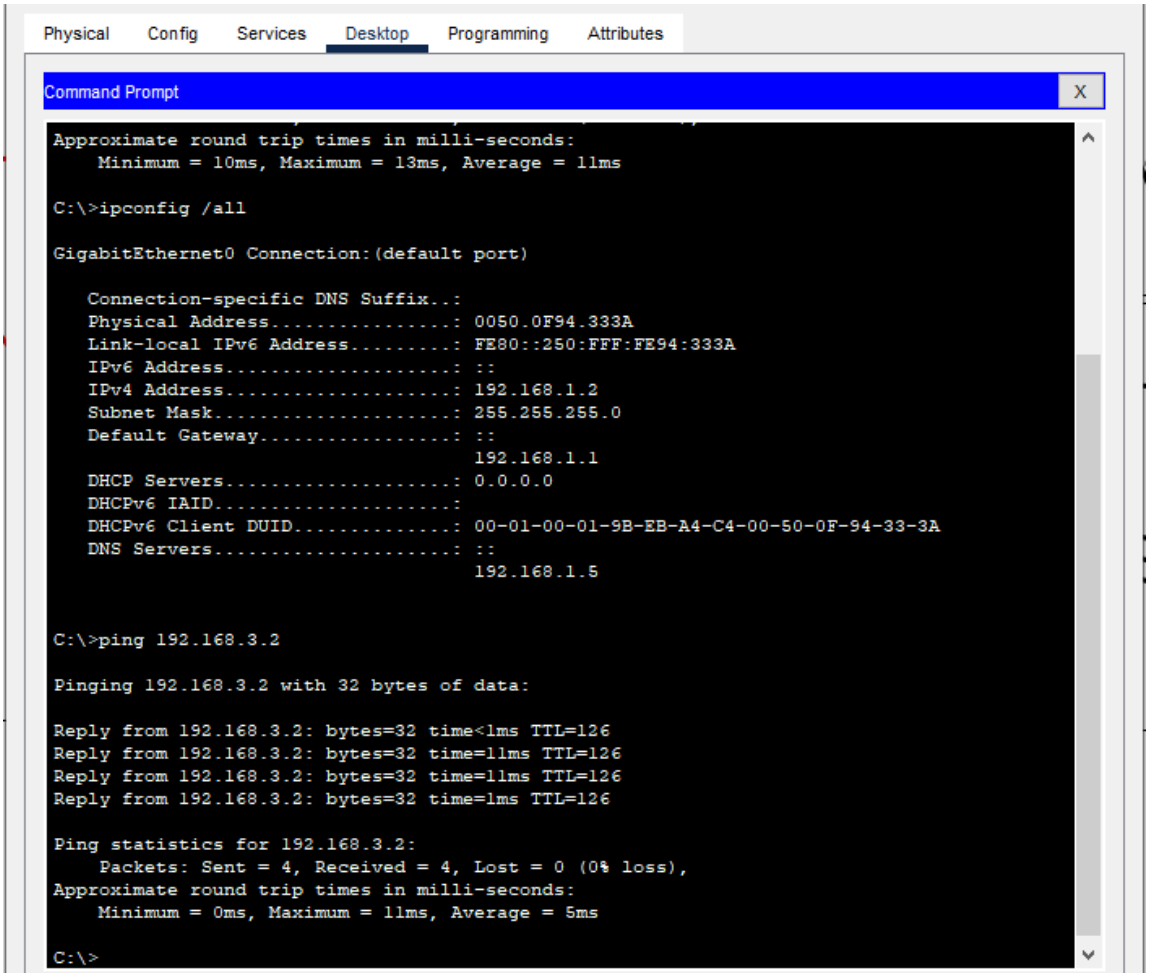


Рис. 3.11. Тестування доступу між мережами майданчиків через тунелі

3.7.4. Конфігурація *IPSec*

Здійснимо процес конфігурації *IPSec*, використовуючи як приклад тунелі майданчика Office. Спочатку ініціюємо налаштування криптозахисту на інтерфейсі *GigabitEthernet 0/0/0* для обміну тунельованими даними між майданчиками. Першим етапом цього процесу є налаштування автентифікації за допомогою *Internet Key Exchange* (*IKE*), що становить першу фазу встановлення захищеного з'єднання. Деталі цієї процедури представлено в лістингу 3.6.

Лістинг 3.6

Налаштування автентифікації *IKE*

```
!
crypto isakmp policy 10
encr aes
authentication pre-share
group 5
crypto isakmp key vpnuser address 10.0.0.6
crypto isakmp key vpnuser address 10.0.0.10
```

Було створено політику безпеки з пріоритетом 10 для управління трафіком, що прямує через тунель до *Dep1*, та з пріоритетом 11 для трафіку, що прямує до *Dep2*. Для цих політик було обрано алгоритм криптування *AES*, метод автентифікації – за ключем, а група *Diffie-Hellman* була встановлена як 5. На наступному етапі, здійснюється налаштування *transform-set* (набір комбінацій протоколів захисту та алгоритмів криптування). Це налаштування здійснюється наступною командою:

crypto ipsec transform-set myset esp-aes esp-sha-hmac

Подальшим кроком стає налаштування списків контролю доступу, які визначають адреси, під які буде застосовуватися криптування:

access-list 100 permit ip host 10.0.0.2 host 10.0.0.6

access-list 101 permit ip host 10.0.0.2 host 10.0.0.10

У даному контексті, *ACL* застосовуються для управління трафіком, що прямує через тунелі між окремими майданчиками.

Наступним етапом є створення об'єкта "*crypto map*", в якому буде зібрано всі раніше створені об'єкти криптозахисту, а також будуть вказані кінцеві

хости *IPSec* (лістинг 3.7). Після створення цього об'єкта, його конфігурація буде застосована до налаштувань інтерфейсу *GigabitEthernet 0/0/0*.

Лістинг 3.7

Налаштування *crypto map*

```
!
crypto map mymap 10 ipsec-isakmp
set peer 10.0.0.6
set transform-set myset
match address 100
!
crypto map mymap 11 ipsec-isakmp
set peer 10.0.0.10
set transform-set myset
match address 101
!
interface GigabitEthernet0/0/0
ip address 10.0.0.2 255.255.255.252

crypto map mymap
```

3.7.5. Перевірка стану криптозахисту створеної мережі

Наступним кроком є перевірка статусів пар *SA* на маршрутизаторі *R Office*, результати якої можна побачити на рис. 3.12.

```
Router#sh cr ?
  ipsec   Show IPSEC policy
  isakmp  Show ISAKMP
  key     Show long term public keys
  map     Crypto maps
Router#sh cr isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.0.0.6        10.0.0.2        QM_IDLE           1058    0 ACTIVE

10.0.0.10       10.0.0.2        QM_IDLE           1066    0 ACTIVE


IPv6 Crypto ISAKMP SA


Router#
```

Рис. 3.12. Стан пар *SA*

Далі буде здійснено процедуру перевірки статусу об'єкта криптозахисту, який був названий "*mymap*" та прив'язаний до нульового оптичного інтерфейсу. Візуальне зображення цієї перевірки представлене на рис. 3.13. Цей етап необхідний для підтвердження коректності налаштувань та функціональності об'єкту криптозахисту.

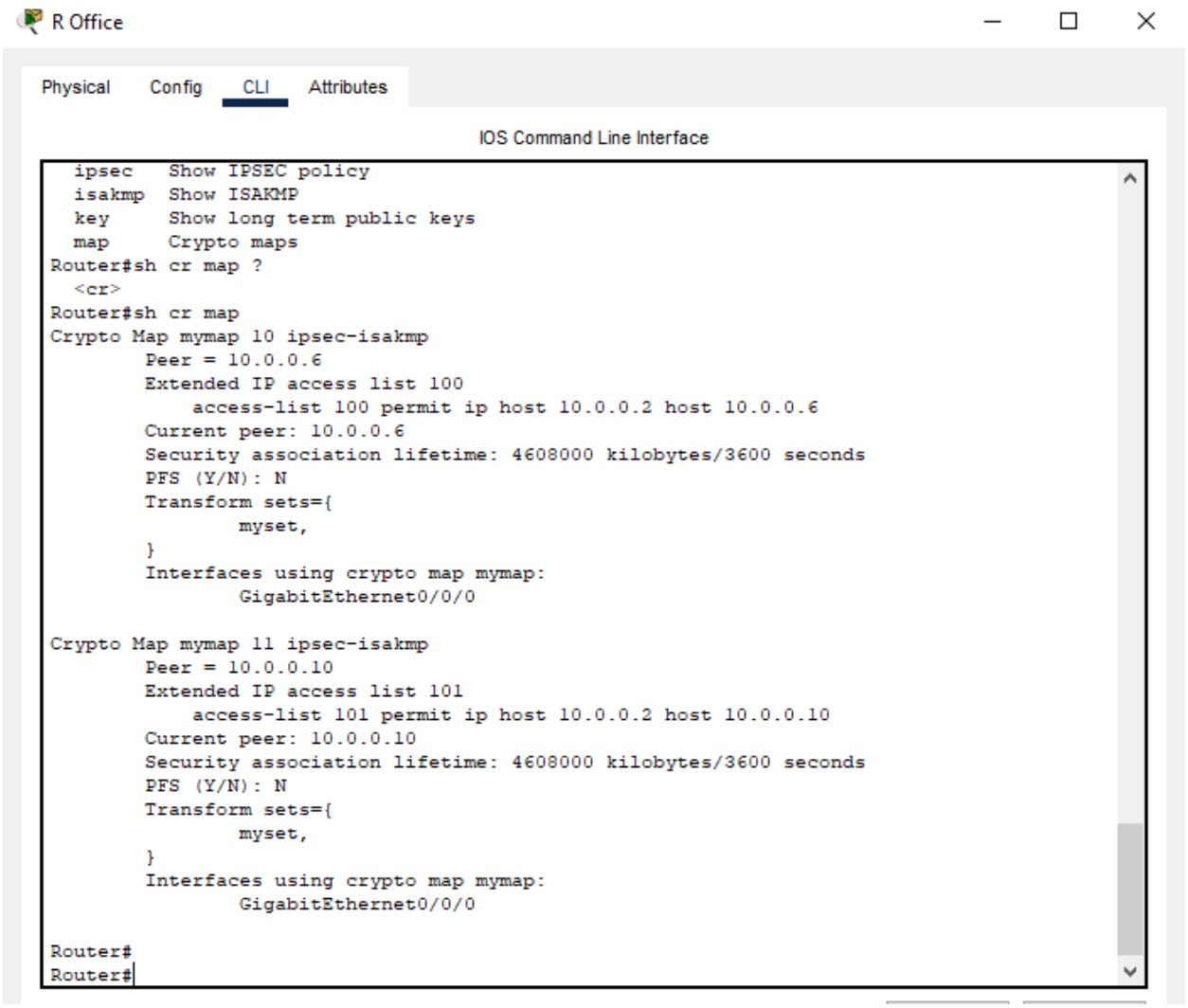


Рис. 3.13. Стан об’єкту *mymap*

Отже, ввесь тунельований трафік між майданчиками є криптований.

3.8. Налаштування ЛОМ майданчиків

3.8.1. Налаштування *DHCP*-серверів маршрутизаторів майданчиків

Після перевірки статусу пар Безпеки Інтернету (*SA*) на маршрутизаторі *R Office* (рис. 3.12) можна переходити до виконання налаштування серверів динамічної конфігурації хостів (*DHCP*) на маршрутизаторах згідно з інформацією, представленою в табл. 3.2. Важливим етапом є додавання опції 150, яка визначає адресу сервера *Trivial File Transfer Protocol* (*TFTP*) для забезпечення правильної роботи телефонів *Cisco IP Phone*.

Далі, виконаємо налаштування *DHCP*-сервера для вузла *R Office*, процедура якого представлена в лістингу 3.8. Зазначимо, що адреса *DNS*-

сервера буде взята з глобальних налаштувань маршрутизатора для забезпечення коректної роботи всієї системи.

Лістинг 3.8

Налаштування *DHCP*-серверу *R Office*

```
ip dhcp excluded-address 192.168.0.1 192.168.0.5
ip dhcp excluded-address 192.168.0.254
ip dhcp pool net0
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1
option 150 ip 192.168.0.1
ip name-server 192.168.1.5
```

3.8.2. Налаштування мереж зі статичною адресацією

Наступним кроком є виконання налаштування хостів серверної мережі статичними *IPV4*-адресами згідно табл. 3.2 на прикладі хосту *Publisher DB 1* майданчику *Office* (рис. 3.14 та 3.15).

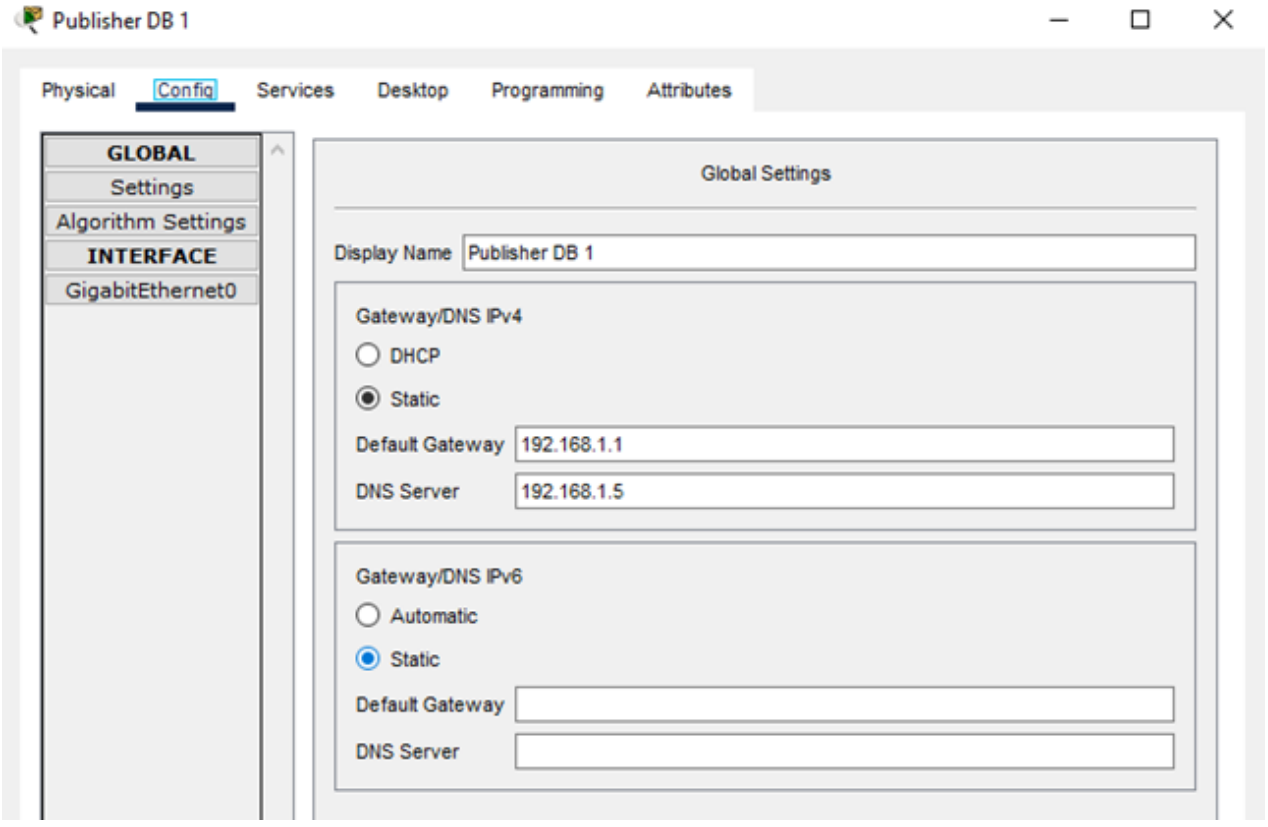


Рис. 3.14. Шлюз за замовчуванням та *DNS*

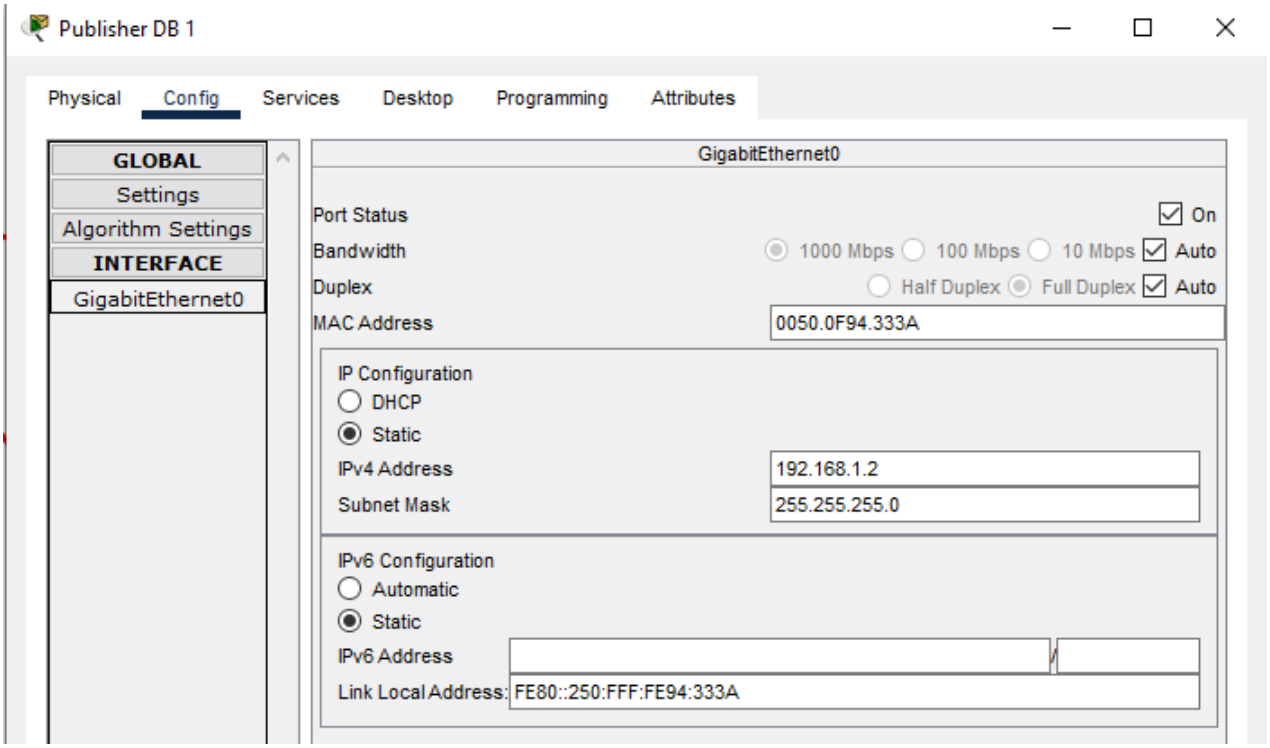


Рис. 3.15. *IPV4*-адреса

3.8.3. Налаштування мереж із динамічною адресацією

Для мереж управління та розробників необхідно виконати налаштування хостів за допомогою *DHCP*-серверу (рис. 3.16 та 3.17).

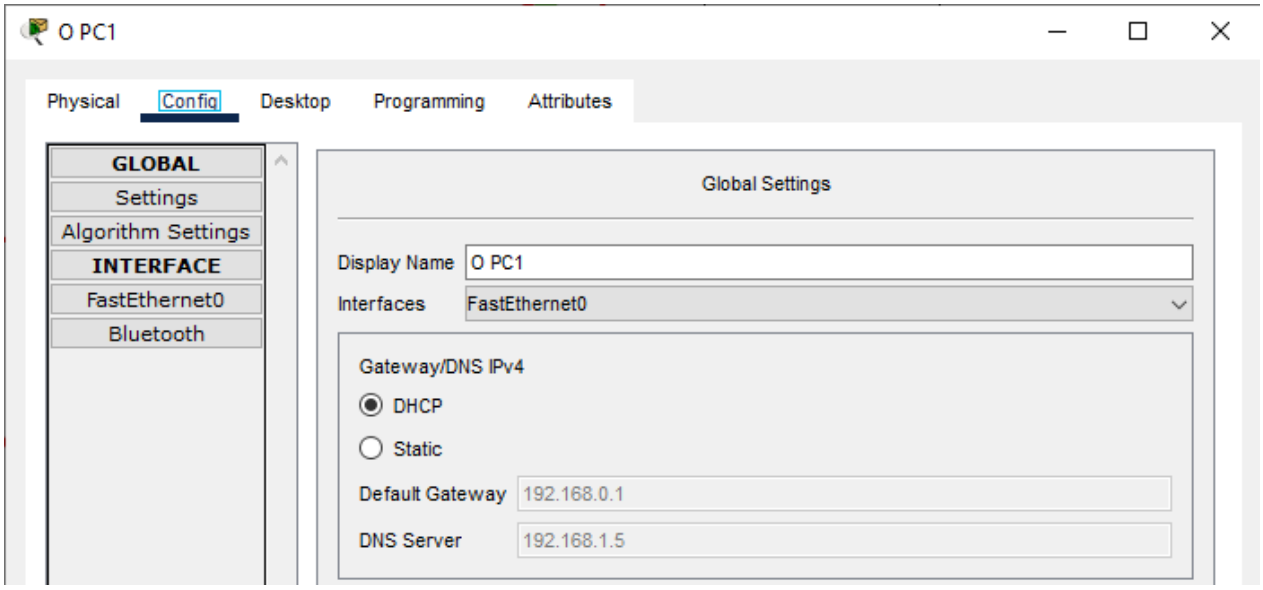


Рис. 3.16. Шлюз за замовчуванням та *DNS*

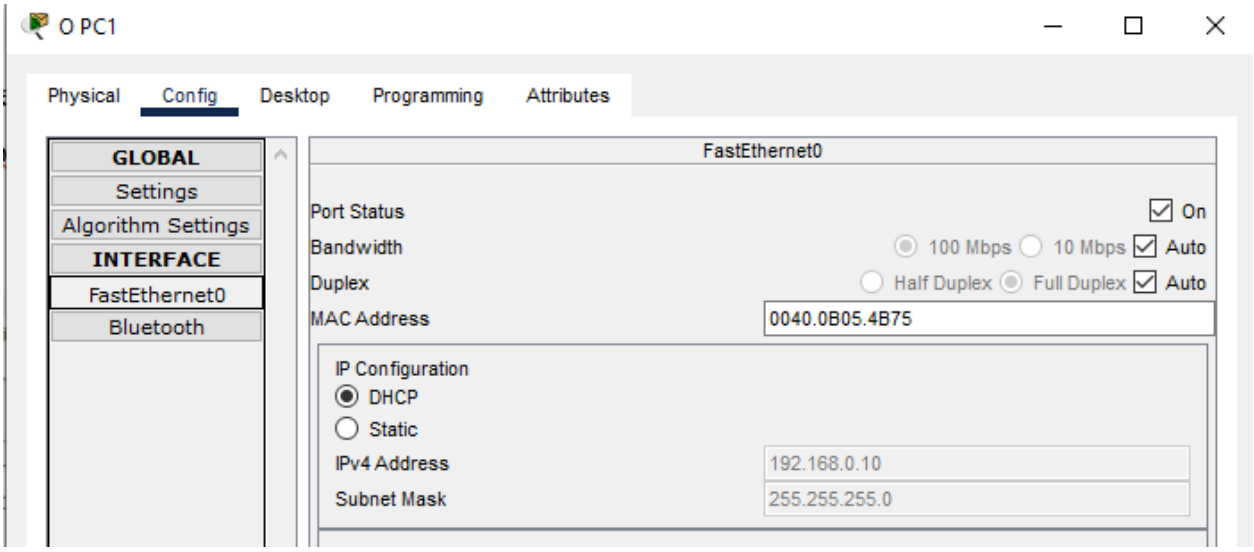


Рис. 3.17. *IPV4*-адреса

3.8.4. Тестування стану *DHCP*-серверів

Ретельний аналіз всіх присвоєних *IP*-адрес, що здійснюється на маршрутизаторі *R Office*, дозволяє отримати об'єктивну картину розподілу цих адрес. Результати цього аналізу подаються в лістингу 3.9.

Лістинг 3.9

Видані *IP*-адреси на *R Office*

```
Router#sh ip dhcp bind
IP address Client-ID/ Lease expiration Type
Hardware address
192.168.0.8 0001.63E7.931D -- Automatic
192.168.0.9 0001.9705.1131 -- Automatic
192.168.0.7 0060.7068.697B -- Automatic
192.168.0.10 0040.0B05.4B75 – Automatic
192.168.0.6 000A.F37A.07ED -- Automatic
192.168.0.15 0001.96B1.865B -- Automatic
192.168.0.14 0060.47E7.57CC -- Automatic
192.168.0.11 0090.2B50.7C84 -- Automatic
192.168.0.16 0090.2BB6.B6BC -- Automatic
192.168.0.13 0001.9701.9412 -- Automatic
192.168.0.12 00D0.9731.E3A4 -- Automatic
Router#
```

3.8.5. Налаштування *DNS*-серверів майданчиків

Приклад налаштування *DNS*-записів для серверів реплікацій буде продемонстрований на *DNS*-сервері майданчика *Dep1*. Детальна візуалізація цього процесу представлена на рис. 3.18.

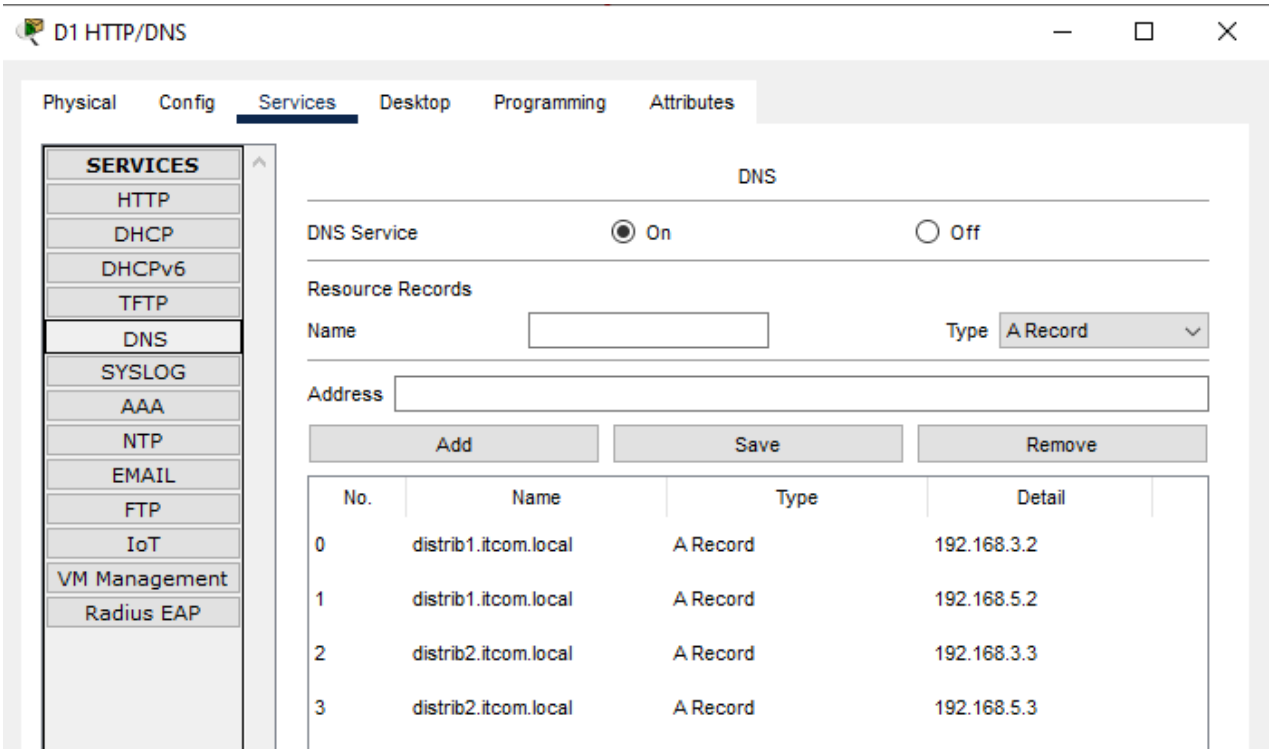


Рис. 3.18. Налаштування *DNS*-записів

3.8.6. Налаштування менеджерів викликів

Одним із завдань є розробка плану нумерації для телефонної мережі. Даний план викладено в табл. 3.5.

Таблиця 3.5

План нумерації телефонної мережі

Майданчик	Нумерація
Office	1xxx
Dep1	2xxx
Dep2	3xxx

Наступним етапом є конфігурація менеджерів викликів на маршрутизаторах окремих майданчиків. Необхідно здійснити налаштування параметрів "*telephony-service*", вказавши при цьому адресу і порт сервісу, кількість терміналів та номерів (лістинг 3.10), з автоматичним наданням конфігурації.

Лістинг 3.10

Налаштування *telephony-service* маршрутизатора *R Dep1*

```
telephony-service
max-ephones 4
max-dn 4
ip source-address 192.168.0.1 port 2000
auto assign 1 to 4
```

Продовжуючи цей процес, номери від 1000 до 1003 будуть встановлені відповідно до лістингу 3.11. Далі слід провести моніторинг автоматичного надання конфігурацій терміналів, який представлено в лістингу 3.12.

Лістинг 3.11

Налаштування номерів *ephone-dn* маршрутизатора *R Dep1*

```
ephone-dn 1
number 1000
!
ephone-dn 2
number 1001
ephone-dn 3
number 1002
!
ephone-dn 4
number 1003
```

Лістинг 3.12

Автоматична конфігурація *ephone* маршрутизатора *R Dep1*

```
ephone 1
device-security-mode none
mac-address 0040.0BC5.3A80
type 7960
button 1:1
!
ephone 2
device-security-mode none
mac-address 0004.9AA3.00A3
type 7960
button 1:2
ephone 3
device-security-mode none
mac-address 0003.E4E5.65D1
type ata
button 1:3
!
ephone 4
device-security-mode none
mac-address 000B.BE6A.D11E
type ata
```

```
button 1:4
```

3.8.7. Налаштування *VoIP*-терміналів

Наступним етапом є маршрутизація викликів до нумерації, яка розташована на інших площадках мережі. Для цього ми створимо об'єкти типу "*dial-peer*", в яких буде вказано план нумерації та адресу, куди будуть направлятися виклики з цього плану, відповідно до табл. 3.5, як показано в лістингу 3.13. Варто відзначити, що трафік, генерований цими викликами, буде прямувати через захищені тунелі, створені на попередніх стадіях.

Лістинг 3.13

Автоматична конфігурація *ephone* маршрутизатора *R Dep1*

```
dial-peer voice 1000 voip
destination-pattern 1...
session target ipv4:192.168.0.1
dial-peer voice 3000 voip
destination-pattern 3...
session target ipv4:192.168.4.1
```

Щодо терміналів *Cisco IP Phone 7960*, подальша конфігурація виявилася незайвою, оскільки все необхідне було вже виконано за допомогою налаштувань *DHCP*-сервера. Однак, щодо терміналів *VoIP*, з'явилася необхідність вказувати *IPV4*-адресу сервісу *telephony*, процес якого можна бачити на рис. 3.19.

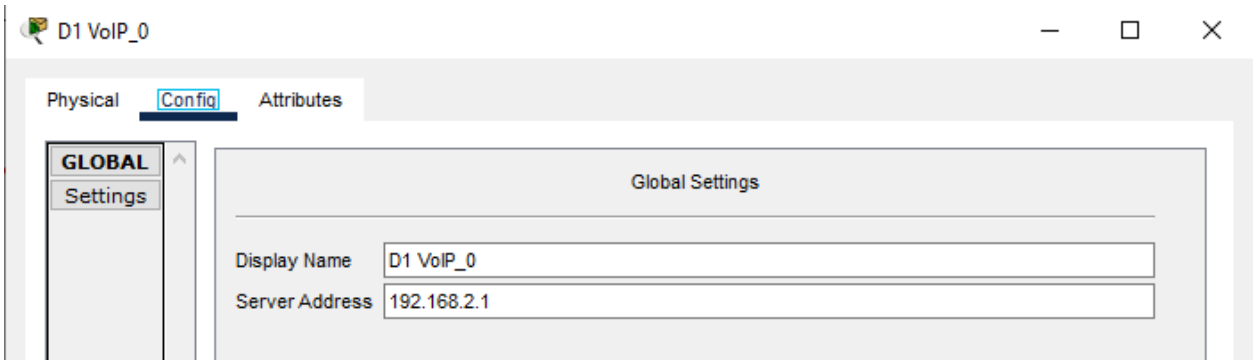


Рис. 3.19. Налаштування *VoIP*-терміналу

3.8.8. Здійснення викликів між майданчиками

Після завершення всіх налаштувань, буде проведено тестування функціональності побудованої мережі *IP*-телефонії. Спочатку необхідно впевнитися у коректності реєстрації *VoIP*-терміналів на майданчику *Dep1*, що демонструється у лістингу 3.14.

Лістинг 3.14

Стан зареєстрованих *VoIP*-терміналів *Dep1*

```
Router#sh eph
ephone-1 Mac:0040.0BC5.3A80 TCP socket:[1] activeLine:0 REGISTERED
in SCCP ver 12 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0
debug:0 caps:8
IP:192.168.2.7 1025 7960 keepalive 43 max_line 2
button 1: dn 1 number 2000 CH1 IDLE

ephone-2 Mac:0004.9AA3.00A3 TCP socket:[1] activeLine:0 REGISTERED
in SCCP ver 12 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0
debug:0 caps:8
IP:192.168.2.8 1025 7960 keepalive 43 max_line 2
button 1: dn 2 number 2001 CH1 IDLE

ephone-3 Mac:0003.E4E5.65D1 TCP socket:[1] activeLine:0 REGISTERED
in SCCP ver 12 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0
debug:0 caps:8
IP:192.168.2.10 1028 ata keepalive 43 max_line 2
button 1: dn 3 number 2002 CH1 IDLE

ephone-4 Mac:000B.BE6A.D11E TCP socket:[1] activeLine:0 REGISTERED
in SCCP ver 12 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0
debug:0 caps:8
IP:192.168.2.12 1028 ata keepalive 43 max_line 2
button 1: dn 4 number 2003 CH1 IDLE
Router#
```

Для додаткової перевірки взаємодії між різними майданчиками, будуть виконані виклики за допомогою графічного інтерфейсу користувача, як це видно на рис. 3.20.

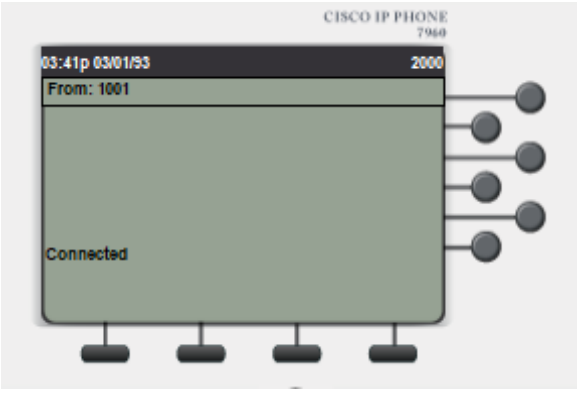


Рис. 3.20. Виклик з 1001 на 2000 (комутація)

3.9. Налаштування виходу до мережі Інтернет

На наступному етапі необхідно додати маршрут за замовчуванням на кожному з маршрутизаторів майданчиків. Визначено, що для підрозділів шлюзом буде кінцева адреса тунелю, що веде до головного офісу. У випадку з маршрутизатором *R Office*, шлюзом буде інтерфейс віртуального маршрутизатора *R Office NAT*, як зазначено в табл. 3.6.

Таблиця 3.6

Маршрути за замовчуванням

Маршрутизатор	Конфігурація
R Office	*ip route 0.0.0.0 0.0.0.0 192.168.6.2*
R Dep1	*ip route 0.0.0.0 0.0.0.0 10.0.1.1*
R Dep2	*ip route 0.0.0.0 0.0.0.0 10.0.1.5*

Після цього буде виконано налаштування *Network Address Translation* (*NAT*) на маршрутизаторі *R Office NAT*. Згідно з вихідними даними, мережа для підключення до провайдера інтернет-послуг визначена як 5.5.5.0/30. Конфігурація налаштувань для вихідного *NAT* представлена в лістингу 3.15.

Лістинг 3.15

Налаштування вихідного *NAT*

```
interface GigabitEthernet0/0
ip address 5.5.5.2 255.255.255.252
ip nat outside
interface GigabitEthernet1/0
ip address 192.168.6.2 255.255.255.252
ip nat inside
ip nat inside source list internet interface GigabitEthernet0/0
overload
ip classless
ip route 192.168.0.0 255.255.0.0 192.168.6.1
ip route 10.0.0.0 255.255.0.0 192.168.6.1
ip flow-export version 9
!
ip access-list extended internet
permit ip 192.168.0.0 0.0.255.255 any
permit ip 10.0.0.0 0.0.255.255 any!
```

3.10. Реалізація і дослідження реплікації даних

Оскільки архітектура компанії передбачає наявність в системі центрального офісу та декількох підрозділів, то доцільним є організація майстер-слейв реплікації. У цьому випадку, сервер центрального офісу слугуватиме майстром – основним джерелом даних. Майстер надсилатиме дані слейвам – серверам підрозділів. Розробники з підлеглих департаментів працюють зі слейвами та після завершення роботи, надсилають дані на слейв свого департаменту. Далі, з серверів підрозділів дані передаються майстру, якщо розробники центрального офісу погоджують зміни, то вони вносяться до центрального серверу. Також варто зазначити, що реалізована реплікація даних є асинхронною, адже, зміни спочатку записуються в основну копію даних, а потім розповсюджуються на репліки з певною затримкою.

З метою зменшення навантаження під час реплікації даних, буде виконано ряд заходів, що відповідають вимогам, зазначеним в пункті 3.1, щодо обмеження доступу розробників з підрозділів до баз даних видавців. Ця мета буде досягнута шляхом блокування доступу до серверів БД з *IP*-адресами 192.168.1.2 та 192.168.1.3 з мереж, що мають адреси 192.168.2.0/24 та 192.168.4.0/24 відповідно. Для реалізації цієї задачі на маршрутизаторі *R Office* буде створено відповідний список доступу (*access-list*), як визначено в лістингу 3.16.

Лістинг 3.16

Access-list для блокування доступу

```
ip access-list extended topublish
deny ip 192.168.2.0 0.0.0.255 host 192.168.1.2
deny ip 192.168.2.0 0.0.0.255 host 192.168.1.3
deny ip 192.168.4.0 0.0.0.255 host 192.168.1.2
deny ip 192.168.4.0 0.0.0.255 host 192.168.1.3
permit ip any any
```

Далі буде виконане налаштування вихідного списку контролю доступу (*access-group*) на другому оптичному інтерфейсі маршрутизатора *R Office*, згідно інформації, представленої в лістингу 3.17.

Лістинг 3.17

Вихідний *access-group*

```
interface GigabitEthernet0/2/0
ip address 192.168.1.1 255.255.255.0
ip access-group topublish out
```

Після завершення цього етапу налаштування, наступним кроком буде проведення тестування. Мета тестування – перевірити можливість доступу розробників з підрозділу *Dep1* до баз даних видавців. Візуалізація процесу тестування зображена на рис. 3.21.

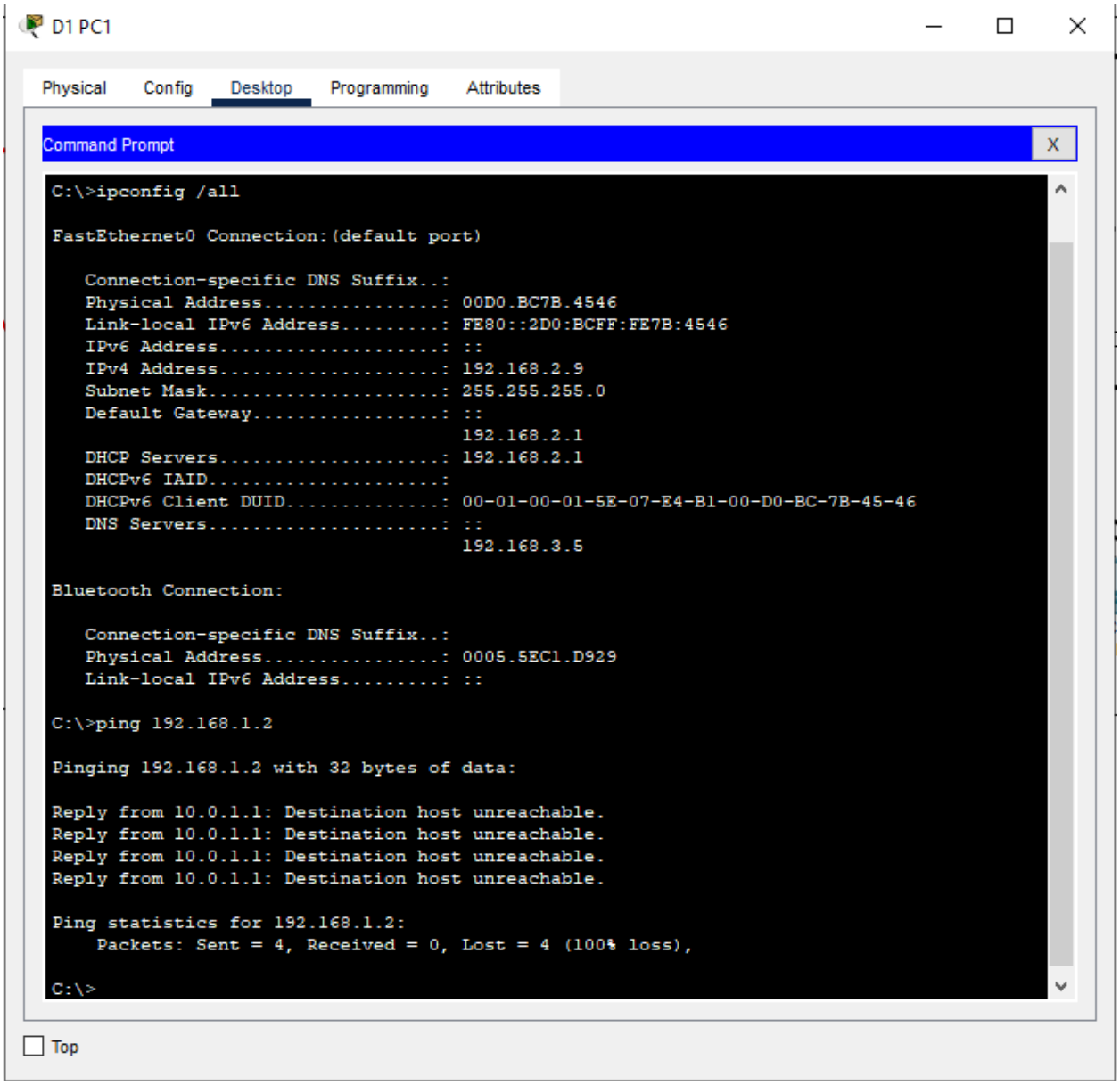


Рис. 3.21. Тестування списків доступу

3.11. Аналіз переваг та недоліків створеної системи

Однією з ключових переваг розробленої мережевої системи є її масштабованість. Цей аспект відображається у здатності системи адаптуватися до додавання нових підрозділів без зайвих труднощів. Для цього достатньо додати необхідні нові тунелі до нового майданчика, внести до системи маршрути до нових мереж через ці створені тунелі, а також додати відповідні правила криптування каналу.

Конструкцію *VPN* між вказаними майданчиками реалізовано використовуючи *IPV4*-тунелі. Створення цих тунелів базується на принципі "кожен-з-кожним", тобто кожен майданчик має тунельне з'єднання з кожним іншим майданчиком.

Система працює на основі протоколів сімейсва *L2TP/IPsec*, що забезпечує високий рівень захисту. У якості алгоритму шифрування було обрано *Advanced Encryption Standard*, симетричний алгоритм, який дозволяє надійно криптувати дані.

Однак, система не позбавлена недоліків. Основним з них є ситуація, коли може виникнути втрата зв'язку між підлеглими майданчиками. У такому випадку, *DNS*-резолвера при одному виклику може надавати недоступний для підключення сервер реплікації, що створює проблеми у координації та взаємодії між різними частинами мережі.

Висновки за розділом

У даному розділі було розроблено структуру мережі IT-компанії, що охоплює центральний офіс та географічно роззосереджені підрозділи. З використанням тунелів, оснащених функціоналом криптозахисту, ці сегменти були інтегровані у єдину мережу з централізованою маршрутизацією. На головному майданчику були розташовані сервери-видавці баз даних,

розроблених цією IT-компанією, тоді як на територіальних підрозділах були встановлені сервери-дистриб’ютори цих баз даних. Схема мережі була розроблена за допомогою інструментарію *Cisco Packet Tracer*.

У рамках проекту були визначені: структура мережі, схема адресації, політика криптозахисту для тунелів між майданчиками, а також здійснений вибір та описано використовуване обладнання для створення мережі. Відповідно до технічного завдання були виконані операції щодо оптимізації реплікації баз даних з серверів-видавців до серверів-дистриб’юторів.

Під час тестування мережі було доведено її працездатність, забезпеченість високими показниками експлуатації та можливість масштабування в разі необхідності. Таким чином, спроектована модель мережі може служити основою для створення реальної мережі IT-компанії.

ВИСНОВКИ

У ході виконання дипломної роботи було досліджено технологію *VPN* та її роль при створенні захищених комп’ютерних мереж.

У першому розділі було проведено комплексний аналіз сучасного стану IT-компаній. Важливим моментом цього аналізу є визначення відповідності сучасних IT-компаній до високих вимог сучасності, зокрема, невід'ємної ролі комп'ютерних мереж у їх функціонуванні. Сучасні IT-компанії значною мірою залежать від ефективності роботи своїх комп'ютерних мереж, що забезпечують високий рівень мобільності та гнучкості виконання завдань.

Водночас, у ході аналізу, було виявлено, що одним з ключових аспектів діяльності IT-компаній є захист даних. Відповідність до високих стандартів безпеки інформації стає першочерговою проблемою, враховуючи постійне зростання вимог в цій сфері.

Попри це, проведене дослідження виявило ряд типових проблем, що мають місце в процесі обміну та захисту даних в комп'ютерних мережах IT-компаній. До них належать: виникнення кібератак, ненадійність мережі, ризик несанкціонованого доступу, можливість втрати даних, вразливості в програмному забезпеченні, а також проблеми несумісності систем.

Другий розділ даної роботи повністю присвячений детальному розгляду технології *VPN*, яка є одним із потужних інструментів забезпечення захисту даних в IT-компаніях.

У рамках цього розділу було проведено глибокий аналіз концепції технології *VPN*. Ключові принципи роботи *VPN* були розглянуті у відповідності до основних компонентів, які вони включають: процеси тунелювання, аутентифікації та шифрування даних.

Було здійснено огляд процесів шифрування даних, що відбуваються під час тунелювання *VPN*, а також процесу аутентифікації в рамках *VPN*. У

контексті шифрування даних було розглянуто найбільш поширені алгоритми шифрування, що застосовуються в технології *VPN*. До них відносяться *Advanced Encryption Standard, Triple Data Encryption Standard, Camellia*.

Аналізу також було піддано основні протоколи, які використовуються в *VPN*. Зокрема, було досліджено протоколи *PPTP* та *L2TP/IPsec*.

Цей розділ також включав в себе огляд основних типів мереж *VPN*, їх основних характеристик, різних варіантів реалізації *VPN*. Було описано процес проходження *IP*-пакету мережею, налаштованою на використання *VPN*, що допомогло краще зрозуміти роботу цієї технології.

Третій розділ даної роботи присвячений практичній реалізації захищеної мережі IT-компанії з використанням технології *VPN*. Цей етап роботи передбачав комплекс заходів, починаючи від постановки завдання і визначення переліку та характеристик необхідного обладнання для нормального функціонування мережі, закінчуючи реалізацією практичних заходів з впровадження технології *VPN*.

Спочатку було визначено цілі та завдання, що ставилися перед реалізацією проекту. Вони включали в себе вибір обладнання, розробку мережі, її налаштування та тестування. Далі було здійснено вибір комутаційного та мережевого обладнання, що відповідає вимогам сучасних стандартів безпеки та надійності.

У рамках розробки мережі було використано емулятор *Cisco Packet Tracer*, на основі якого було створено схему мережі. Після цього було визначено топологію зв'язку між головним офісом та підрозділами компанії, а також було розроблено схеми *VPN*-каналів.

У процесі реалізації проекту було здійснено конфігурацію *VPN*-каналів та проведено їх тестування. Кожний етап впровадження проекту був супроводжений ретельною діагностикою роботи системи, що дозволило забезпечити високий рівень надійності та безпеки реалізованої мережі.

У результаті проведеного комплексного дослідження та практичної реалізації проекту було підтверджено важливість використання технології *VPN* для забезпечення захисту даних в комп'ютерних мережах IT-компаній.

Враховуючи актуальність та значущість проблеми захисту даних у сучасному IT-світі, можна стверджувати, що подальше розповсюдження та удосконалення технологій, що базуються на *VPN*, представляють собою перспективний напрямок розвитку в IT-галузі. Отже, результати даного дослідження підкреслюють важливість продовження наукових розробок та практичних застосувань в області *VPN* технологій.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Голидьбіна А.В. Особливості сучасного ринку ІТ-послуг та специфіка просування на ньому / А.В. Голидьбіна, Н.В. Язвінська // Економічний вісник НТУУ «КПІ». – 2017. – № 14. – С. 1-13.

2. Німуха Ю.К. Особливості управління персоналом в ІТ-компаніях. Сучасні підходи до управління підприємством: зб. тез доп. VIII Всеукраїнської наук.-практ. конф., 6 квіт. 2017 р. – Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2017. – С. 81

3. Кирій В.В. Формування інформаційної складової забезпечення безпеки підприємств / В. В. Кирій; Харків: ХНУРЕ, 2014.– 58с.

4. Войтко С.В. Ринок інформаційно-комунікаційних технологій: структура та аналіз [Електронний ресурс] / *Web*-сайт*: vlp.com.ua* – Режим доступу: *http://vlp.com.ua/files/58.pdf*

5. *DDoS*-атака. [Електронний ресурс] / *Web*-сайт*: eset.com.ua* – Режим доступу: *https://www.eset.com/ua/support/ information/entsiklopediya-ugroz/distributed-denial-of-service/.*

6. Рибальченко Л. В. Основи управління інформаційною безпекою / Л. В. Рибальченко, А. М. Гребенюк; навч. посібник 2020, 144 с.

7. *Concerning the legal capacity of cyberspace safe operation. Cybersecurity in Ukraine: legal and organizational issues: materials of the III AllUkrainian scientific-practical conference, november 30, 2018. Odessa. pp. 5–7*

8. *Outstanding innovation, superior protection for your devices* / *BullGuard Internet Security 2021 Edition.* – 2021. [Електронний ресурс] / *Web*-сайт*: bullguard.com* – Режим доступу: *https://www.bullguard.com/products/bullguardinternet-security.aspx.*

9. *Computer Hardware Global Market Report / The business research company.* – 2020. [Електронний ресурс]. – Режим доступу:

https://www.thebusinessresearchcompany. com/report/computer-hardware-globalmarket-report-2020-30-covid-19-impact-and-recovery.

10. *About Firewalls*. [Електронний ресурс] / *Web*-сайт*: checkpoint.com* – Режим доступу: *https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/.*

11. Якубенко С.С. Аналіз ринку антивірусних програм / С. С. Якубенко / Наукова конференція *intkonf*. – 2010.

12. *IDS/IPS*. [Електронний ресурс] / *Web*-сайт*: techukraine.net* – Режим доступу: *https://techukraine.net/8-інструментів-ids-та-ips-для-кращого-аналізу.*

13. *Digital service act package.* [Електорнний ресурс] / *Web*-сайт*: digitalstrategy.ec.europa.eu* – Режим доступу: *https://digitalstrategy.ec.europa.eu/en/policies/digital-services-act-package.*

14. *Principle of Least Privilege*. [Електронний ресурс] / *Web*-сайт*: paloaltonetworks.com* – Режим доступу: *https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege.*

15. 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.

16. *Merkow M. S. The Complete Guide to Internet Security / M. S. Merkow, J. Breithaupt. – AMACOM,* 2018. – *pp*. 34-52

17. *Virtual Private Network*. [Електронний ресурс] / *Web*-сайт*: cisco.com* – Режим доступу: *https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html.*

18. *Gilman E. Zero Trust Networks. Building Secure Systems in Untrusted Networks / E Gilman, D Barth*. – 2017. – 424с.

19. *Openvpn vs l2tp/ipsec*. [Електронний ресурс] / *Web*-сайт*: howtogeek.com* – Режим доступу: *https://www.howtogeek.com/211329/which-is-the-best-vpn-protocol-pptp-vs.-openvpn-vs.-l2tpipsec-vs.-sstp/.*

20. *Authentication.* [Електронний ресурс] / *Web*-сайт*: techtarget.com* – Режим доступу: *https://searchsecurity.techtarget.com/definition/authentication*.

21. *Advanced Encryption Standard (AES)*. [Електронний ресурс] / *Web*-сайт: *usnews.com* – Режим доступу: *https://www.usnews.com/360-reviews/privacy/what-is-advanced-encryption-standard.*

22. *Is AES 128 or 256*? [Електронний ресурс] / *Web*-сайт*: ubiqsecurity.com* – Режим доступу: *https://www.ubiqsecurity.com/128bit-or-256bit-encryption-which-to-use/.*

23. *Triple Data Encryption Standard*. [Електронний ресурс] / *Web*-сайт: *csrc.nist.gov* – Режим доступу: *https://csrc.nist.gov/glossary/term/triple_data_encryption_standard*.

24. *Camellia algorithm*. [Електронний ресурс] / *Web*-сайт: *crypto-it.net* – Режим доступу: *http://www.crypto-it.net/eng/symmetric/camellia.html.*

25. *Point-to-Point Tunneling Protocol.* [Електронний ресурс] / *Web*-сайт*: expressvpn.com* – Режим доступу: *https://www.expressvpn.com/what-is-vpn/protocols/pptp.*

26. *Layer 2 Tunneling Protocol with IP Security*. [Електронний ресурс] / *Web*-сайт*: techtarget.com* – Режим доступу: *https://www.techtarget.com/searchnetworking/definition/Layer-Two-Tunneling-Protocol-L2TP*.

27. *Virtual Private Dial-up Network.* [Електронний ресурс] / *Web*-сайт*: techopedia.com* – Режим доступу: *https://www.techopedia.com/definition/9971/virtual-private-dial-up-network-vpdn.*

28. *What Is A Site-to-Site VPN?* [Електронний ресурс] / *Web*-сайт*: fortinet.com* – Режим доступу: *https://www.fortinet.com/resources/cyberglossary/what-is-site-to-site-vpn.*

29. *Cisco 4461 ISR.* [Електронний ресурс] / *Web*-сайт*: cisco.com* – Режим доступу: *https://www.cisco.com/c/en/us/support/routers/4461-integrated-services-router/model.html.*

30. *Cisco Gigabit Ethernet WAN (NIM-1GE-CU-SFP).* [Електронний ресурс] / *Web*-сайт*: stack-systems.com* – Режим доступу: *https://stack-systems.com.ua/interfejsnyj-modul-cisco-nim-1ge-cu-sfp*.

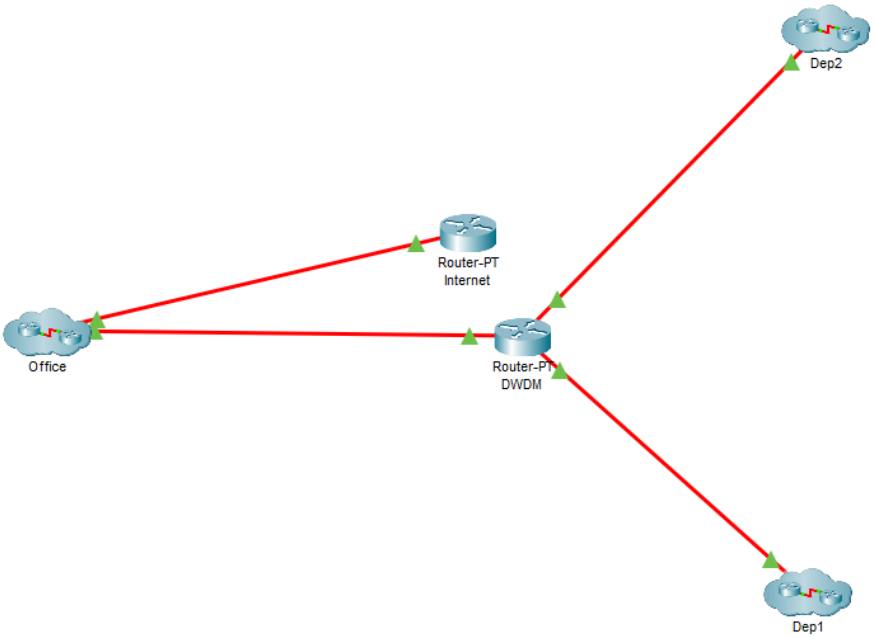
31. *Cisco High-Density Gigabit Ethernet WAN (SM-X-6X1G).* [Електронний ресурс] / *Web*-сайт *router-switch.com* – Режим доступу: *https://www.router-switch.com/sm-x-6x1g-p-24048.html*.

32. Комутатор *Cisco CBS250-24T-4X*. [Електронний ресурс] / *Web*-сайт *cisco.com.ua* – Режим доступу*: https://cisco.com.ua/cbs250-24t-4x-eu*.

ДОДАТКИ

Додаток А

Загальна схема мережі



Додаток Б

Схема мережі майданчику *Office*