

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Інститут інформатики та радіоелектроніки
Факультет комп'ютерних наук і технологій
(повне найменування інституту, факультету)

Кафедра комп'ютерних систем і мереж
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
магістра
(ступінь вищої освіти)

на тему Дослідження та реалізація методів створення захищених
комп'ютерних мереж на базі CISCO

Виконав: студент(ка) 2 курсу, групи
КНТ₃-511м

Спеціальності _____
123 «Комп'ютерна інженерія»
(код і найменування спеціальності)

Освітня програма (спеціалізація) _____
«Комп'ютерні системи і мережі»

Костюк Валентина Григорівна
(прізвище та ініціали)

Керівник Киричек Г.Г.
(прізвище та ініціали)

Рецензент Самойлик С.С.
(прізвище та ініціали)

2022 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
 (повне найменування закладу вищої освіти)

Інститут, факультет ФКНТ
 Кафедра Комп'ютерних систем і мереж
 Ступінь вищої освіти Магістр
 Спеціальність 123 «Комп'ютерна інженерія»
 (код і найменування)
 Освітня програма (спеціалізація) «Комп'ютерні системи і мережі»
 (назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Завідувач кафедри KCM
 Кудерметов Р.К. *Руденко*
 «__» грудня 2022 року

ЗАВДАННЯ

НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

Костюк Валентини Григорівни

(прізвище, ім'я, по батькові)

- Тема проєкту (роботи) Дослідження та реалізація методів створення захищених комп'ютерних мереж на базі CISCO
 керівник проєкту (роботи) Киричек Галина Григорівна к.т.н. доцент,
 (прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
 затверджені наказом закладу вищої освіти від «07» листопада 2022 року № 367
- Строк подання студентом проєкту (роботи) 16 грудня 2022 року
- Вихідні дані до проєкту (роботи) наявні технології та методи застосування протоколів захисту мереж, Packet Tracer — симулятор мережі передачі даних, що випускається фірмою Cisco Systems.
- Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Аналіз проблеми та постановка завдань дослідження
2. Матеріали та методи
3. Застосування методів захисту мереж
4. Порівняння та дослідження методів захисту мереж
- Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Креслення 1 Функціональна схема корпоративної мережі
Креслення 2 Структурна схема корпоративної мережі
Плакат 1 Діаграми розширеного ping
Плакат 2 Архітектура та інкапсуляція протоколу IPSec

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-5	Киричек Г.Г., доцент		
нормо-			
контроль	Шербак Н.В.		

7. Дата видачі завдання « 03 » жовтня 2022 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Робота з літературою	10.10.2022 р.	
2	Розробка та затвердження завдання на випускную кваліфікаційную роботу	15.10.2022 р.	
3	Аналіз проблеми та постановка завдань дослідження	20.10.2022 р.	
4	Матеріали та методи	01.10.2022 р.	
5	Застосування методів захисту мереж	10.11.2022 р.	
6	Порівняння та дослідження методів захисту мереж.	25.11.2022 р.	
7	Оформлення графічного матеріалу	01.12.2022 р.	
8	Нормоконтроль та рецензування, перевірка на плагіат, оформлення дублінського ядра	10.12.2022 р.	

Студент(ка)

Керівник проєкту (роботи)

Костюк В.Г.
(підпис) (прізвище та ініціали)

Киричек Г.Г.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

ЗАХИЩЕНА МЕРЕЖА, VPN, IPSec, MTU, IP, AH GRE .

Пояснювальна записка до роботи магістра: 83 с., 31 рис., 4 табл
20 джерел, 4 графічних матеріалів.

Об'єкт дослідження – засоби побудови захищених комп'ютерних мереж.

Предмет дослідження – методи побудови захищених комп'ютерних мереж на основі мережевих технологій Cisco.

Мета роботи – моделювання та створення захищеної мережі комерційної організації.

Матеріали, методи та технічні засоби: методи розробки, дослідження та експерименту за допомогою симулятора Cisco Packet Tracer створений компанією Cisco. Програма дозволяє будувати і аналізувати мережі на різноманітному обладнанні в різних топологіях з підтримкою багатьох протоколів. на різних мережевих пристроїв.

Результати – змодельовано та створено захищену мережу на основі роутерів Cisco. Для захисту обрану технології VPN на основі протоколів IPSec та GRE. Для з'єднання обрано маршрутизатори Cisco 2811.

Галузь використання – малі підприємства та компанії.

ABSTRACT

SECURE NETWORK, VPN, IPSec, MTU, IP, AH GRE .

Explanatory note to the master's work: 83 p. , 32 figures, 4 tables., 20 sources, 4 graphic materials.

Object research - means of building secure computer networks.

The subject of research is methods of building secure computer networks based on cisco network technologies.

The purpose of the work is to model and create a secure network of a commercial organization.

Materials, Methods, and Techniques: Design, Research, and Experimentation Methods Using the Cisco Packet Tracer Simulator Created by Cisco. The program allows you to build and analyze networks on various equipment in various topologies with support for many protocols. on different network devices.

Results.– a secure network based on Cisco routers was modeled and created. VPN technology based on IPSec and GRE protocols is selected for protection. Cisco 2811 routers are selected for connection.

The field of use is small enterprises and companies.

ЗМІСТ

Перелік скорочень	8
Вступ.....	9
1 Аналіз проблеми та постановка завдань дослідження	10
1.1 Основні поняття комп'ютерних мереж.....	10
1.2 Класифікація, аналіз і порівняльна характеристика існуючих методів і засобів вирішення задачі	10
1.2.1 Міжнародні стандарти щодо побудови комп'ютерних мереж.....	10
1.2.2 Види протоколів для захисту мереж	11
1.2.3 Списки керування доступом для захисту мереж	15
1.2.4 Методи тунелювання та шифрування.....	16
1.2.5 Пристрої для налаштування безпеки мереж.....	21
1.3 Програмне забезпечення для моделювання мереж	23
1.4 Постановка завдання до роботи.....	24
1.5 Висновки за розділом 1	24
2 Матеріали та методи.....	24
2.1 Вибір засобів моделювання.....	24
2.2 Вибір методу технології організації захисту та побудови мереж.....	25
2.2.1 Вибір технологій захисту мереж	25
2.2.1 Вибір технологій організації vpn.....	30
2.2.2 Вибір параметрів шифрування та автентифікації.....	35
2.3 Вибір структурної схеми мережі.	38
2.4 Вибір мережевого обладнання.....	38
3. Застосування методів захисту мереж.....	46
3.1 Налаштування мережі, та створення протоколів захисту.....	46

3.2 Висновки за розділом 3	65
4 Порівняння та дослідження методів захисту мереж	66
4.1 Вплив VPN з'єднання на швидкість мережі.....	66
4.2 Перевірка захисту мережі.....	74
4.3 Вхідні та вихідні дані.....	79
4.5 Висновки за розділом 4	79
Висновки	81
Перелік посилань.....	82
Перелік графічних матеріалів:	
Креслення 1 Структурна схема мережі	
Креслення 2 Функціональна схема мережі	
Плакат 1 Діаграми розширеного ring	
Плакат 2 Архитектура та інкапсуляція IPSec	

ПЕРЕЛІК СКОРОЧЕНЬ

VPN – Virtual Private Network

IPSec – IP Security

MTU – Maximum Transmission Unit

IP – Internet Protocol

AH – Authentication Header

GRE – Generic Routing Encapsulation

ISAKMP – Internet Security and Key Management Protocol

DF – Don'tfragment

ACL – Access Control List

TCP – Transmission Control Protocol

UDP – User Data Protocol

ЛОМ – Локальна операційна модель

DH – Алгоритм Diffie-Hellman

DES – Data Encryption Standard

ВСТУП

Актуальність теми – Магістерська робота присвячена розв’язанню актуальної задачі методам створення захищених комп’ютерних мереж на базі CISCO. Необхідність цієї розробки виникає у зв’язку з тим, що ми живемо в інформаційному світі тому створення безпечних мереж є важливим. Користувачі хочуть мати одночасно швидкі та захищені мережі. Тому гостро стоїть питання створення якісних мереж на основі новітнього обладнання.

Предмет дослідження – методи створення захищених комп’ютерних мереж на базі CISCO.

Мета роботи –. дослідити та розробити методи захисту комп’ютерних мереж.

Завдання роботи:

- провести аналіз предметної області;
- визначити структуру мережі;
- спроектувати систему клієнт-серверної взаємодії;
- проаналізувати результати роботи мережі.

Практична значимість розробки: дозволяє робити мережі з зазначеними показниками.

1 АНАЛІЗ ПРОБЛЕМИ ТА ПОСТАНОВКА ЗАВДАНЬ ДОСЛІДЖЕННЯ

1.1 Основні поняття комп'ютерних мереж

Комп'ютерні мережі – зв'язку між двома чи більше комп'ютерами. У ширшому розумінні комп'ютерна мережа – це система зв'язку через кабельне чи бездротове середовище, самі комп'ютери різного функціонального призначення і мережеве обладнання. Для передачі інформації можуть бути використані різні фізичні явища, як правило – різні види електричних сигналів чи електромагнітного випромінювання. Середовищами передавання у комп'ютерних мережах можуть бути телефонні кабелі, та спеціальні мережеві кабелі: коаксіальні кабелі, виті пари, волоконно-оптичні кабелі, радіохвилі, світлові сигнали.

У сучасному світі багато організацій використовують велику кількість з'єднаних у мережу. Тому є питання про спільне використання ресурсів, надання доступу до баз даних, а також захисту від не санкціонованого доступу.

1.2 Класифікація, аналіз і порівняльна характеристика існуючих методів і засобів вирішення задач

1.2.1 Міжнародні стандарти щодо побудови комп'ютерних мереж

Міжнародний стандарт ISO/IEC 17799:2005 встановлює настанови та загальні принципи для ініціювання, впровадження, підтримки та покращення управління інформаційною безпекою в організації. Окреслені цілі надають загальні вказівки щодо загальновизнаних цілей управління інформаційною безпекою. ISO/IEC 17799:2005 містить передову практику цілей контролю та засобів контролю в таких сферах управління інформаційною безпекою:

- політика безпеки;
- організація інформаційної безпеки;
- управління активами;
- забезпечення людськими ресурсами;
- фізична та екологічна безпека;
- комунікації та управління операціями;
- управління доступом;
- придбання, розробка та супровід інформаційних систем;
- управління інцидентами інформаційної безпеки;
- управління безперервністю бізнесу;
- відповідність.

1.2.2 Види протоколів для захисту мереж

І хости, і шлюзи можуть використовувати методику динамічної маршрутизації (dynamic routing), яка дозволяє таблиці маршрутизації оновлюватись автоматично після зміни конфігурації мережі (наприклад, після виходу маршрутизатора з ладу). Функції маршрутизатора, що вийшов з ладу, можуть бути покладені на інший без втручання користувача, що робить всю мережу більш стійкою до відмов апаратного забезпечення.

Динамічна маршрутизація вимагає використання протоколу маршрутизації, який було б покладено завдання додавання і видалення записів з таблиці маршрутизації. Ця таблиця виконує самі функції, як і під час статичної маршрутизації, але її записи додаються і видаляються автоматично, а чи не вручну.

Розрізняють два типи протоколів маршрутизації: внутрішні та зовнішні. Внутрішні протоколи (interior protocols) використовують у межах (всередині) однієї автономної системи, тоді як зовнішні протоколи (exterior protocols) – між автономними системами. Під терміном "автономна система" мається на увазі мережа, що належить певній адміністративній одиниці (це може бути велика компанія або університет). Невеликі вузли, зазвичай, є частиною автономних систем провайдерів Internet.

Тут наведені назви основних VPN протоколів, які використовуються у тому числі також для захисту мереж:

- VPN (Virtual Private Network «Віртуальна приватна мережа») – узагальнена назва технологій, що дозволяють забезпечити одне або кілька мережевих з'єднань поверх іншої мережі, наприклад Інтернет. Незважаючи на те, що для комунікації використовуються мережі з меншим або невідомим рівнем довіри (наприклад, публічні мережі), рівень довіри до побудованої логічної мережі не залежить від рівня довіри до базових мереж завдяки використанню засобів криптографії (шифрування, аутентифікації, інфраструктури відкритих ключів, засобів захисту від повторів і змін повідомлень, що передаються по логічній мережі);

- IPSec (IP security) – Internet Protocol Security (IPsec) – це набір протоколів для забезпечення захисту даних, що передаються IP-мережею. IPsec працює на мережному рівні і може використовуватися з багатьма операційними системами, що дозволяє використовувати його без сторонніх додатків, часто використовується поверх IPv4. Також використовується в парі з L2TP або IKEv2. IPsec шифрує весь IP-пакет, використовуючи Authentication Header (AH), який на кожному пакеті ставить цифровий підпис. Encapsulating Security Protocol (ESP), який забезпечує під час передачі конфіденційність, цілісність та аутентифікацію пакета;

- PPTP та PPPoE (PPP (Point-to-Point Protocol) over Ethernet) – використовує два з'єднання, одне для управління з використанням TCP, у якому порт сервера 1723., інше для інкапсуляції даних, за допомогою протоколу GRE, який є транспортним протоколом. Встановлення зв'язку між двома маршрутизаторами протоколу PPP відбувається у такому порядку: LCP, NCP, корисні дані третього рівня. А розривається: кінець передачі корисних даних, NCP, LCP. Як видно, HDLC не встановлює і не розриває з'єднання, оскільки PPP використовуються HDLC кадри без підтвердження доставки;

- L2TP/IPsec – Оскільки L2TP сам по собі не забезпечує шифрування чи автентифікацію, часто з ним використовується IPsec. Може використовувати шифрування 3DES або AES;
- IKEv2/IPsec–Internet Key Exchange version 2 (IKEv2) є протоколом IPsec, що використовується для виконання взаємної автентифікації, створення та обслуговування Security Associations (SA), стандартизований в RFC 7296. Також захищений IPsec, як і L2TP, що може говорити про їхній однаковий рівень безпеки. Хоча IKEv2 був розроблений Microsoft спільно з Cisco, існують реалізації протоколу з відкритим вихідним кодом (наприклад, OpenIKEv2, Openswan та strongSwan). Може використовувати низку різних криптографічних алгоритмів, включаючи AES, Blowfish та Camellia, у тому числі з 256-бітними ключами;
- OpenVPN–Має високу швидкість передачі даних, використовує стандартні протоколи TCP та UDP, і це дозволяє йому стати альтернативою IPsec тоді, коли провайдер блокує деякі протоколи VPN. Може працювати на будь-якому з портів TCP та UDP і може використовуватись на всіх основних платформах через сторонні клієнти: Windows, Mac OS, Linux, Apple iOS, Android та вимагає спеціальне клієнтське програмне забезпечення;
- SSL – SSL VPN Технологія SSL VPN є доповненням технології IPsec VPN, застосування якої дозволяє використовувати практично будь-яку систему автентифікації, що існує в компанії, і гнучко здійснювати поділ доступу до ресурсів. VPN Підтримка PPP, bridge, point-to-point, multi-client server;
- GRE (англ. Generic Routing Encapsulation – загальна інкапсуляція маршрутів) – це протокол тунелювання, який використовується для передачі IP-пакетів по мережі. Розроблений Cisco Systems, який може інкапсулювати широкий спектр протоколів мережевого рівня всередині віртуальних двоточкових з'єднань по мережі IP. Він дозволяє маршрутизувати IP-пакети між приватними сетями IPv4/IPv6, які розділені через загальнодоступний

Інтернет. Також GRE підтримує інсталяцію широкого та багатоадресного трафіку IPv4/IPv6.

– IPsec (IPsecurityIP-безпека), описаного в RFC 2401, 2402, 2406 та інше. Не всім користувачам потрібне шифрування з'єднань (виконання відповідних процедур може займати значну частину обчислювальних ресурсів). Однак, замість того щоб робити шифрування необов'язковим, користувачеві пропонується у разі необхідності обрати порожній алгоритм. У RFC 2410 розписуються такі переваги, як простота, легкість реалізації та висока швидкість. IPsec є основою для безлічі послуг, алгоритмів та модулів. Основні послуги такі: секретність, цілісність даних, захист від злому методом повторення повідомлень (коли шахрай повторює підслухану розмову). Все це засноване на криптографії із симетричними ключами, оскільки тут критична висока продуктивність. Справа в тому, що вважається сьогоdnіадійним алгоритмом завтра може бути зламаний. Якщо зробити IPsec незалежним від конкретного алгоритму, стандарт виживе навіть у разі злому одного з алгоритмів. Модулі потрібні для того, щоб можна було захищати і одне TCP-з'єднання, і весь трафік між парою хостів, і весь трафік між парою захищених маршрутизаторів і т.д.

IPsec орієнтований на з'єднання, незважаючи на його присутність лише на рівні IP. Адже небезпеку можна забезпечити лише створенням ключа та використанням його протягом якогось часу. А це, по суті, різновид з'єднання. До того ж все з'єднання погашають витрати на їх встановлення за рахунок передачі великої кількості пакетів. "З'єднання" в контексті IPsec називається захищаючим зв'язком (Security Aconnection - SA). Захищаючий зв'язок - це симплексне з'єднання між двома кінцевими точками, з якими пов'язаний спеціальний ідентифікатор захисту. Якщо потрібна передача захищених даних в обох напрямках, знадобляться дві захищають зв'язки. Ідентифікатори захисту передаються в пакетах, наступних за цим надійним з'єднанням, і використовуються після прибуття захищених пакетів для пошуку ключів та іншої важливої інформації.

Технічно IPsec і двох основних частин. Перша описує два нових заголовка, які можна додавати до пакета для передачі ідентифікатора захисту, даних контролю цілісності та іншої інформації. Друга частина, ISAKMP (Internet Security and Key Management Protocol – інтернет-безпека та керування ключами), призначена для створення ключів. ISAKMP є середовищем. Основним протоколом до виконання роботи є IKE (Internet Key Exchange – обмін ключами в Інтернеті). Повинна використовуватись версія 2 IKE, так як раніше версія мала серйозні недоліки, як вказали Perlman і Kaufman, (2000).

IPsec може працювати у двох режимах. У транспортному режимі заголовок IPsec вставляється відразу за заголовком IP. Поле Protocol заголовка IP змінюється таким чином, щоб було зрозуміло, що далі слідує заголовок IPsec (перед заголовком TCP). У заголовку IPsec міститься інформація щодо безпеки, зокрема, ідентифікатор захисту, новий порядковий номер і, можливо, перевірка цілісності поля корисного навантаження.

У режимі тунелювання весь IP-пакет разом із заголовком вставляється всередину нового IP-пакету з новим заголовком. Цей режим хороший тоді, коли тунель закінчується десь поза кінцевим пунктом. У деяких випадках кінцем тунелю є шлюз, що забезпечує безпеку, наприклад, корпоративний міжмережевий екран. Він зазвичай використовується для VPN (Virtual Private Network віртуальна приватна мережа). У цьому режимі міжмережевий екран вставляє та виймає пакети, що проходять через нього у різні боки. За такої організації машини ЛОМ компанії гарантовано будуть обслужені за стандартом IPsec. Про це абсолютно не доводиться турбуватися: всі турботи бере на себе міжмережевий екран.

1.2.3 Списки керування доступом для захисту мереж

Access Control List (ACL) – лист, який визначає, хто або що може отримувати доступ до об'єкта (програми, процесу чи файлу), і які саме операції можна або заборонено виконувати суб'єкту (користувачу, групі користувачів).

Списки можуть бути стандартні та розширені.

Стандартні ACL, який можна налаштувати на маршрутизаторах Cisco. Трафік фільтрується на основі IP-адреси джерела та IP-пакетів. Номер списку доступу може бути будь-яким числом від 1 до 99. Його треба розміщувати поблизу місця призначення, щоб уникнути блокування законного трафіку з джерела.

Розширені списки керування доступом дозволяють фільтрувати IP-трафік на основі комбінації кількох критеріїв: IP-адреса джерела, IP-адреса призначення, порт TCP або UDP, протокол. В цих ACL, номер списку доступу може бути будь-яким числом від 100 до 199. Такі ACL також можна назвати списками доступу, у яких номер ACL замінено ключовим словом. Цей тип ACL слід розміщувати поблизу джерела, оскільки він дозволяє детально контролювати доступ до ресурсів, щоб змусити трафік проходити через мережу перед блокуванням.

Також цими списками можна створювати обмеження доступу до маршрутизатора:

R(config)#line vty 0 4 – переходимо в режим налаштувань віртуальних ліній.

R(config-line)#password <пароль>

R(конфігураційний рядок)#вхід

R(config-line)#access-class 231 in – налаштовуємо логін і пароль, а також зміцнюємо список доступу з дозволеними IP-адресами.

Існують також і іменовані списки доступу.

Router(config)#ip access-list {standard | extended} {<номер ACL> | <ім'я ACL>}

Router(config-ext-nacl)# {default | deny | exit | no | permit | remark}

1.2.4 Методи тунелювання та шифрування

Симетричне шифрування, або шифруванням із закритим ключем, засноване на секретному ключі, відомому обом взаємодіючим сторонам. Відправна сторона використовує цей ключ як аргумент математичного виразу, що перетворює нормальний текст на зашифрований. Сторона, що приймає,

використовує цей же ключ для розшифровки отриманого. Прикладом алгоритму симетричного шифрування є Data Encryption Standard (DES), що використовується в протоколі IPSec.

В асиметричному шифруванні, або шифруванні з відкритим ключем, використовуються два ключі. Один ключ є закритим і відомий тільки тій стороні, якій він належить. Інший ключ є загальнодоступним та відкритим. Закритий та відкритий ключі пов'язані математичним виразом. Один ключ використовується для шифрування, а інший – для розшифрування. При надсиланні зашифрованого повідомлення сторона, що відправляє, шифрує його за допомогою відкритого ключа сторони, що приймає. Сторона, що приймає, розшифровує це повідомлення за допомогою закритого ключа, який відомий тільки їй.

Технологія шифрування з відкритим ключем дає змогу реалізувати механізм цифрових підписів повідомлень. Для створення цифрового підпису відправник генерує хеш повідомлення. Хеш – це число, що представляє математичну суму повідомлення. Потім відправник шифрує хеш за допомогою закритого ключа. Шифр, що вийшов, є цифровим підписом повідомлення і посиляється разом з ним. Одержувач розшифровує хеш з допомогою відкритого ключа відправника і самостійно обчислює математичну суму, після чого порівнює результати. Збіг означає, що повідомлення не було модифіковано в процесі передачі, і що воно надіслано саме відправником.

У схемі симетричного шифрування відправник і одержувач знають секретний ключ. Передача цього ключа виконується (з відповідним захистом) до початку передачі даних. При асиметричному шифруванні відправник використовує для шифрування і підпису один ключ, а одержувач при розшифровці - інший. Відкритий ключ вільно поширюється і пересилається всім, кому може бути потрібна розшифровка повідомлень відправника. Однак закритий ключ повинен зберігатися в таємниці.

Основне правило криптографії полягає в припущенні, що криптоаналітику (зломщику шифру) відомий метод шифрування, що

використовується. Іншими словами, зловмисник точно знає, як працюють методи шифрування та дешифрації. Через величезні зусилля, необхідні розробки, тестування і впровадження нового методу, щоразу, коли старий метод виявлявся чи вважався скомпрометованим, зберігати алгоритм шифрування у секреті просто непрактично. Тут на допомогу приходить ключ шифрування. Ключ складається з відносно короткого рядка, що визначає один із величезної кількості варіантів результату шифрування. На відміну від методу шифрування, який може змінюватися лише раз на кілька років, ключ можна змінювати так часто, як це потрібно. Таким чином, наша базова модель являє собою постійний і відомий загальний метод, в якому як параметр використовується секретний ключ, що легко змінюється. Ідея, яка полягає в припущенні про те, що криптоаналітику відомий метод і наріжним каменем секретності є ексклюзивний ключ, називається принципом Керкгофа (Kerckhoff's principle). Алгоритми шифрування загальнодоступні; секретні лише ключі. Оскільки реально в таємниці зберігається лише ключ, основне питання полягає у його довжині. Ключ завдовжки дві цифри утворює 100 варіантів. Ключ завдовжки три цифри означає 1000 варіантів, а при довжині ключа в шість цифр число комбінацій досягає мільйона. Чим довше ключ, тим вище показник трудовитрат (workfactor) зломщика шифру. При збільшенні довжини ключа показник трудовитрат для злому системи шляхом перебору значень ключа зростає експоненційно. Секретність переданого повідомлення забезпечується потужним (але все ж таки відкритим) алгоритмом і довгим ключем.

Шифрування з відкритим ключем передбачає у кожного користувача наявність двох ключів - відкритого ключа (public), використовуваного всіма для шифрування повідомлень, надсланих цьому користувачеві, і закритого ключа (private), потрібного користувачеві для дешифрації повідомлень, що приходять до нього.

Використання послідовності шифрування, дешифрації та знову шифрування пояснюється зворотною сумісністю з існуючими DES-системами

з одним ключем. Обидві функції шифрування та дешифрації встановлюють відповідність між наборами 64-розрядних чисел. З погляду криптографії обидві функції однаково надійні. Однак використання EDE замість EEE дозволяє комп'ютеру, який застосовує потрібне шифрування, спілкуватися з комп'ютером, який застосовує звичайне одиночне шифрування, просто встановивши $K_1 = K_2$. Таким чином, потрібне шифрування можна легко включати у вигляді додаткового режиму роботи, що не є цікавим для вчених криптографів, але досить важливо для корпорації IBM та її клієнтів.

AES (Advanced Encryption Standard) –покращений стандарт шифрування). Вимоги до розробок були такі:

- Алгоритм має використовувати симетричний блоковий шифр;
- Усі деталі розробки мають бути загальнодоступними;
- Повинні підтримуватися довжини ключів 128, 192 та 256 біт;
- Має бути можлива як програмна, і апаратна реалізація;
- Алгоритм повинен бути загальнодоступним або базованим на поняттях, що не дискредитували себе.

Незважаючи на всю свою складність, AES (або DES, або будь-який інший блоковий код) є, по суті, моноалфавітним підстановним шифром з великими довжинами символів (в AES використовуються 128-бітові символи, в DES– 64-бітні). Для будь-якого уривка відкритого тексту шифр при прогоні через один і той же блок, що шифрує, буде виходити завжди однаковим. Скажімо, якщо ви 100 разів намагатиметеся зашифрувати текст abcdefgh, задаючи щоразу той самий ключ для алгоритму DES, ви отримаєте 100 однакових копій шифру. Зломщик може спробувати використати цей недолік під час спроби розшифрування тексту.

Найбільшого поширення набула функція SHA-1 (Secure Hash Algorithm 1 – надійний алгоритм хешування) (NIST, 1993). Як і всі профілі повідомлення, він перемішує вхідні біти досить складним чином, тому кожен вихідний біт залежить від кожного вхідного біта. Алгоритм SHA-1 також доповнює повідомлення одиничним бітом в кінці, за яким слідує така кількість нульових

біт (рівна як мінімум 64), щоб у результаті вийшло загальне число біт, кратне 512. Потім 64-розрядне число, що містить довжину повідомлення (до бітового доповнення), логічно складається (операція АБО) з 64 молодшими бітами.

Алгоритм MD5 (Message Digest 5 – профіль повідомлення 5) є п'ятою версією хеш-функцій, розроблених Рональдом Рівестом (Ronald Rivest). Спочатку повідомлення доповнюється до довжини 448 біт за модулем 512. Потім до нього додається вихідна довжина повідомлення, що розглядається як 64-розрядне число, в результаті чого отримується блок бітів довжиною кратної 512. Останній крок підготовки до обчислень ініціалізує 128-розрядний буфер, його вміст дорівнює якомусь фіксованому значенню. Потім починаються обчислення. На кожному етапі береться 512-розрядний блок вхідного тексту та ретельно перемішується зі 128-розрядним буфером. Для більшої наваристості в каструлю також кидається вміст таблиці синусів. Саме синуси використовуються не тому, що їх результат більш випадковий, ніж результат інших генераторів випадкових чисел (у яких часто також застосовуються тригонометричні функції), а щоб уникнути будь-яких підозр у створенні потайної лазівки, через яку потім розробник (або замовник) міг би увійти. Процес триває, доки не будуть оброблені всі вхідні блоки. Вміст 128-розрядного буфера та утворює профіль повідомлення.

Перелік методів, які застосовуються для методи хешування та шифрування:

- Encryption algorithms for confidentiality: DES, 3DES, AES;
- Hashing algorithms for integrity: MD5, SHA;.
- Authentication algorithms: Pre-shared keys (PSK), RSA digital signatures;
- Key management: An example would be Diffie-Hellman (DH), which can be used to;
- dynamically generate symmetrical keys to be used by symmetrical algorithms; PKI;

- which supports the function of digital certificates issued by trusted CAs; and Internet;
- Key Exchange (IKE), which does a lot of the negotiating and management for us for.

Тунелювання забезпечує спосіб інкапсуляції пакетів усередині транспортного протоколу та реалізовано як віртуальний інтерфейс та забезпечує засіб інкапсуляції пакетів усередині транспортного протоколу та реалізовано як віртуальний інтерфейс для забезпечення простого інтерфейсу. Інтерфейс тунелю не прив'язаний до конкретних «passenger» або «transport» протоколів, а скоріше це архітектура, яка розроблена надавати послуги, необхідні для реалізації будь-якої стандартної схеми інкапсуляції точка-точка. Оскільки тунелі є з'єднаннями «точка-точка», ви повинні налаштувати окремий тунель для кожного з'єднання. Тунелювання складається з таких головних компонентів:

- пасажирський протокол, який є протоколом, який ви інкапсулюється;
- операційний протокол загальної інкапсуляції маршрутизації (GRE) або протокол IPSec;
- транспортний протокол (IP або інший), який використовується для передачі інкапсульованого протоколу. або «транспортних» протоколів, а скоріше це архітектура, яка розроблена надавати послуги, необхідні для реалізації будь-якої стандартної схеми інкапсуляції точка-точка.

Побудова вихідного тунелю на роутері cisco робиться таким чином: “tunnel source {ip-address | interface-type}” і “тунель призначення {host-name | ip-address}” в режимі конфігурації інтерфейсу для тунелю.

1.2.5 Пристрої для налаштування безпеки мереж

Обладнання Cisco має такі пристрої для налаштування безпеки мереж:

- міжмережеві екрани;
- прокси –сервера;

- роутери.

Міжмережеві екранії ASA налаштовані під такі системи:

Application Visibility and Control (AVC)– контроль та блокування додатків за категоріями та протоколами, дозволяє, виділено заблокувати передачу файлів по Skype або використання BitTorrent клієнтів AVC використовує глибоку перевірку пакетів (DPI) для класифікації програм. Та може поєднувати DPI з такими методами, як статистична класифікація, кешування сокетів, виявлення служб, автоматичне навчання та DNS-AS. Спеціальні програми можуть виявляти рідні програми:

- Intrusion Prevention System (IPS)–система запобігання вторгненням. Дозволяє застосувати політики IPS, автоматично створені на основі використання трафіку в мережі;
- WEB-фільтр (URL)– контроль доступу до web-сайтів за категоріями сайтів та груп користувачів. Дозволяє автоматично обмежити доступ до заражених вірусами сайтів, а також інших сайтів неробочого призначення;
- Anti-MalwareProtection (AMP)– унікальна технологія шлюзового антивірусу із додатковою функцією ретроспективного захисту. Дозволяє простежити шлях поширення шкідливого файлу в мережі, виявити джерело та локалізувати всі заражені кінцеві точки.

Роутери, які мають такі конфігурації:

- SEC/K9– конфігурація з активованим модулем апаратного шифрування;
- HSEC/K9 –конфігурація з додатковим модулем крипто;
- CCME/K9 – конфігурація включає підтримку офісної телефонії за технологією CiscoCallManagerExpress;
- SRST/K9 – конфігурація аналогічна CCME/K9, Безперервність бізнесу та різноманітність WAN з надмірними каналами глобальної мережі.

1.3 Програмне забезпечення для моделювання мереж

Існує багато програм моделювання мереж (симулятори та емулятори), але не всі дають можливість створювати мережеві топології з широкого спектру маршрутизаторів та комутаторів. Різниця між симулятором та емулятором є в тому, що симулятор працює повністю з віртуальними об'єктами, у той час як емулятор дає змогу працювати з окремими реальними елементами. GNS3 є графічним емулятором мережі, який дозволяє змоделювати віртуальну мережу з маршрутизаторів та віртуальних машин.

Cisco Packet Tracer – це симулятор мережі, створений компанією Cisco. Програма дозволяє будувати і аналізувати мережі на різноманітному обладнанні в різних топологіях з підтримкою багатьох протоколів. на різних мережевих пристроїв: маршрутизаторів, комутаторів, персональних комп'ютерів, точок бездротового доступу. У симуляторі реалізовані серії маршрутизаторів Cisco 800, 1800, 1900, 2600, 2800, 2900 і комутаторів Cisco Catalyst 2950, 2960, 3560. Та серверів DHCP, HTTP, TFTP, FTP, DNS, AAA, SYSLOG, NTP і EMAIL. Також є робочі станції, різні модулі до маршрутизаторів і комп'ютерів, смартфони, хаби, а також хмари

GNS3 є графічним емулятором мережі, який дозволяє змоделювати віртуальну мережу з маршрутизаторів та віртуальних машин. За допомогою цієї програми можна створити модель комп'ютера та інших пристроїв і запустити програмне забезпечення. Всі основні компоненти пристрою емулюються в залежності від апаратної техніки, на якій буде використовуватися GNS3, можлива побудова комплексних проєктів, які складаються з маршрутизаторів Cisco та інших марок, серверів та свічів [6].

Інтерфейси цих програм є зрозумілими та пристосованими до реальних умов.

1.4 Постановка завдання до роботи

В роботі було поставлено задачу – дослідження та реалізація методів створення захищених комп'ютерних мереж на базі CISCO.

1.5 Висновки за розділом 1

Проведено детальний огляд методів створення захищених комп'ютерних мереж на базі CISCO

2 МАТЕРІАЛИ ТА МЕТОДИ

2.1 Вибір засобів моделювання

Cisco Packet Tracer – це багатофункціональна програма моделювання мереж, що дозволяє експериментувати з поведінкою мережі та оцінювати можливі сценарії. Вона здатна моделювати велике кількість пристроїв різного призначення, а також чимало різних типів зв'язків, що дозволяє проектувати мережі будь-якого розміру на високому рівні складності.

Програмний продукт Packet Tracer дає можливість створювати мережеві топології з широкого спектру маршрутизаторів та комутаторів компанії Cisco, робочих станцій та мережевих з'єднань типу Ethernet, Serial, ISDN, FrameRelay. Ця функція може бути виконана як для навчання, так роботи. Наприклад, щоб зробити налаштування мережі ще на етапі планування або створити копію робочої мережі з метою усунення несправності. Cisco

Packet Tracer виконує такі основні функції: що дозволяють досліджувати принципи побудови та функціонування комп'ютерних мереж.

Такі як наприклад:

- візуальна побудова мережі, що містить активне обладнання, кінцеві пристрої та лінії зв'язку;
- налаштування активного обладнання через інтерфейс командного рядка CLI-методом, що реально використовується в сучасному обладнанні;
- налаштування основних параметрів активного обладнання через графічний інтерфейс;
- додавання модулів активних пристроїв у середовищі емуляції, аналогічне підключенню додаткових модулів у реальному обладнанні;
- Спостереження за проходженням пакетів по мережі та підтримка кількох десятків різних протоколів у візуальному режимі.

GNS3 є графічним емулятором мережі, тому вона може робити і ті самі функції, що і програма Packet Tracer.

Отже, проведений аналіз аналогів визначив, що для розрахунку мережі на базі Cisco можна користуватись обома програмами. Для поставлених завдань вистачить програми Cisco Packet Tracer.

2.2 Вибір методу технології організації захисту та побудови мереж

2.2.1 Вибір технологій захисту мереж

Відомо, що завдання захисту даних можна розділити на дві підзавдання: захист даних усередині комп'ютера та захист даних у процесі передачі від одного комп'ютера до іншого. Для забезпечення безпеки даних при їх передачі WAN мережами використовуються різні технології захищеного каналу.

Технологія захищеного каналу забезпечує захист трафіку між двома точками у відкритій транспортній мережі Інтернет. Захищений захист виконує такі функції:

- взаємна автентифікація абонентів при встановленні з'єднання, шляхом обміну паролями;
- захист повідомлень, що передаються по каналу, від несанкціонованого шляхом шифрування;
- підтвердження цілісності повідомлень, що надходять по каналу.

Для початку визначемось для якої моделі OSI буде застосовано технології захисту. Для цього розглянемо модель OSI та TCP/IP.

Модель OSI – це концептуальна модель, розроблена ще у 1970-х роках, щоб описати архітектуру та принципи роботи мереж передачі даних. А також модель OSI характеризує та стандартизує те, як різні компоненти програмних забезпечення та апаратних засобів, що беруть участь у мережній комунікації, повинні розділяти працю та взаємодіяти один з одним. Це має сім рівнів.

Модель TCP/IP також є чотирирівнева мережева модель, але це модель. Модель TCP/IP визначає процес передачі цифрових даних. Він широко відомий як TCP/IP, оскільки основними протоколами є TCP та IP, але в цій моделі використовуються не тільки ці два протоколи. Ці моделі мають розподіл на рівні, всередині яких діють певні протоколи та виконуються власні функції.

Модель OSI та TCP/IP (рис. 2.1).

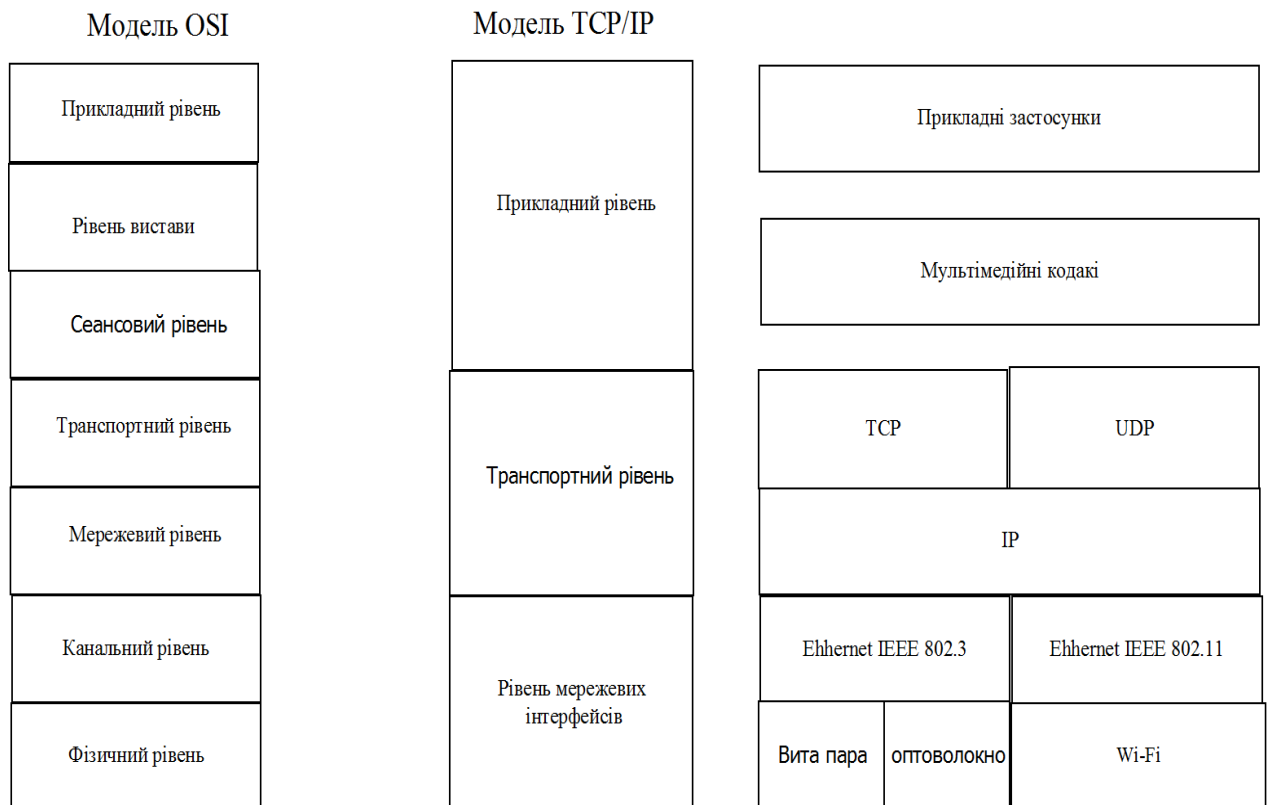


Рисунок 2.1 – Модель OSI та TCP/IP

Засоби безпеки технічного рівня можна розділити на програмні, апаратні та програмно-апаратні

Програмні засоби включають захисні інструменти операційних систем (підсистеми аутентифікації та авторизації користувачів, засоби управління доступом, аудит та ін.) та прикладні програми, призначені для вирішення завдань безпеки (системи виявлення та запобігання вторгненням, антивірусні засоби, проксі-сервери).

Прикладом апаратних засобів, що спеціалізуються на інформаційному захисті, є джерела безперебійного живлення, генератори напруги, засоби контролю доступу до приміщень та ін.

До апаратно-програмних засобів відносяться, аналізатори мережного трафіку та міжмережіві екрани. І хоча цей рівень засобів називається технічним, до нього також відносять математичні методи (методи криптографії), алгоритми (евристичний алгоритм розрахунку часу обороту в протоколі TCP), абстрактні моделі (моделі контролю доступу) тощо.

Коли безпека забезпечується на мережному та каналному рівнях, не захищеними стають додатки прикладних рівнів.

Якщо захист даних здійснюється засобами верхніх рівнів таких як прикладний або сеансовий, тому цей спосіб захисту не залежить від технологій транспортування даних (IP, Ethernet або MPLS), що можна вважати безперечною перевагою. У той самий час докладання у своїй стають залежними від конкретного протоколу захищеного каналу, оскільки у яких мають бути вбудовані явні виклики функцій цього протоколу.

Захищений канал, реалізований на найвищому (прикладному) рівні, захищає лише певну мережеву службу, наприклад файлову, гіпертекстову або поштову.

Робота протоколу захищеного каналу лише на рівні уявлення робить його універсальним засобом, ніж протокол безпеки прикладного рівня. Однак для того, щоб додаток зміг скористатися протоколом рівня подання, до нього доводиться вносити виправлення, хоча й не такі суттєві, як у випадку протоколу прикладного рівня. Модифікація програми у разі зводиться до вбудовування явних звернень до API відповідного протоколу безпеки.

На рівні представлення працює протокол безпеки транспортного рівня TLS (Transport Layer Security), який замінив протокол захищених сокетів SSL (Secure Socket Layer), який наразі визнаний уразливим та не рекомендується для використання. Протокол SSL був розроблений компанією Netscape Communications для захисту даних, що передаються між веб-сервером і веб-браузером, але він міг бути використаний будь-якими іншими програмами.

протокол IPSec працює на мережевому рівні, є компромісним варіантом. З одного боку, він прозорий для додатків та може працювати практично у всіх мережах, оскільки заснований на широко розповсюджені протоколі IP та використовує будь-яку технологію каналного рівня (PPP, Ethernet, MPLS та інші).

А також переглянемо перелік протоколів, які застосовуються у різних рівнях OSI (табл. 2.1.).

Таблиця 2.1. – Параметри інтерфейсів

Рівень протоколів	Види протоколів	Види захищених протоколів
Прикладний	HTTP, gopher, Telnet, DNS, DHCP, SMTP, SNMP, CMIP, FTP, TFTP, , IRC, AIM, NFS, NNTP, NTP, SNTP, XMPP, FTAM, APPC, X.400, X.500, AFP, LDAP, SIP, IETF, RTP, RTCP, ITMS, Modbus TCP, BACnet IP, IMAP, POP3, SMB, MFTP, BitTorrent, e2k, PROFIBUS	S/MIME, SSH
Представлення	ASN.1, XML, TDI, XDR, NCP, AFP, ASCII, Unicode	SSL, TLS
Сеансовий	ASP, ADSP, DLC, Named Pipes, NBT, NetBIOS, NWLink, Printer Access Protocol, Zone Information Protocol, SSL, TLS, SOCKS, PPTP	—
Транспортний	TCP, UDP, NetBEUI, AEP, ATP, IL, NBP, RTMP, SMB, SPX, SCTP, DCCP, STP, TFTP, RTP	—
Мережевий	IPv4, IPv6, ICMP, IGMP, IPX, NWLink, NetBEUI, DDP, IPSec, SKIP	IPSec, GRE
Канальний	ARCnet, ATM, DTM, SLIP, SMDS, Ethernet, ARP, FDDI, Frame Relay, LocalTalk, Token Ring, , StarLan, WiFi, PROFIBUS	PPL2F, L2TP, PPP, PPPoE

Продовження таблиці 2.1

Рівень протоколів	Види протоколів	Види захищених протоколів
Фізичний	RS-232, RS-422, RS-423, RS-449, RS-485, ITU-T, RJ-11, T-carrier (T1, E1), модифікації стандарту Ethernet: 10BASE-T, 10BASE2, 10BASE5, 100BASE-TX, 100BASE-FX, 100BASE-T, 1000BASE-T, 1000BASE-TX, 1000BASE-SX	—

Тому, щоб захистити мережу WAN обираємо технологію VPN.

2.2.1 Вибір технології організації VPN

VPN створює зашифрований тунель для захисту даних, що передаються між пристроєм і сервером. Ваша безпека повністю залежить від цього підключення, тому при позашляховому обриві підключень або зміні конфіденційності сервера ваша конфіденційність може виявитися під загрозою. Функція автоматичного відключення автоматично блокує доступ до Інтернету в разі виникнення проблеми з VPN, тому є останнім рубежем вашого захисту.

При класифікуванні VPN (рис 2. 2) звертають увагу на такі фактори:

- рівень захисту: приватна мережа або зашифровані дані;
- спосіб реалізації: інтегрований або програмний варіант;
- тип протоколу: TCP/IP, та інші;
- доступність: платно або безкоштовно.

Якщо треба з'єднати дві різні мережі використовується site-to-site.

Іноді додають ще третій тип Client/Server VPN. Цей тип використовується, коли створюється пара мереж. Користувачі підключаються до загального сервера, але передають інформацію по своїм внутрішнім мережам.

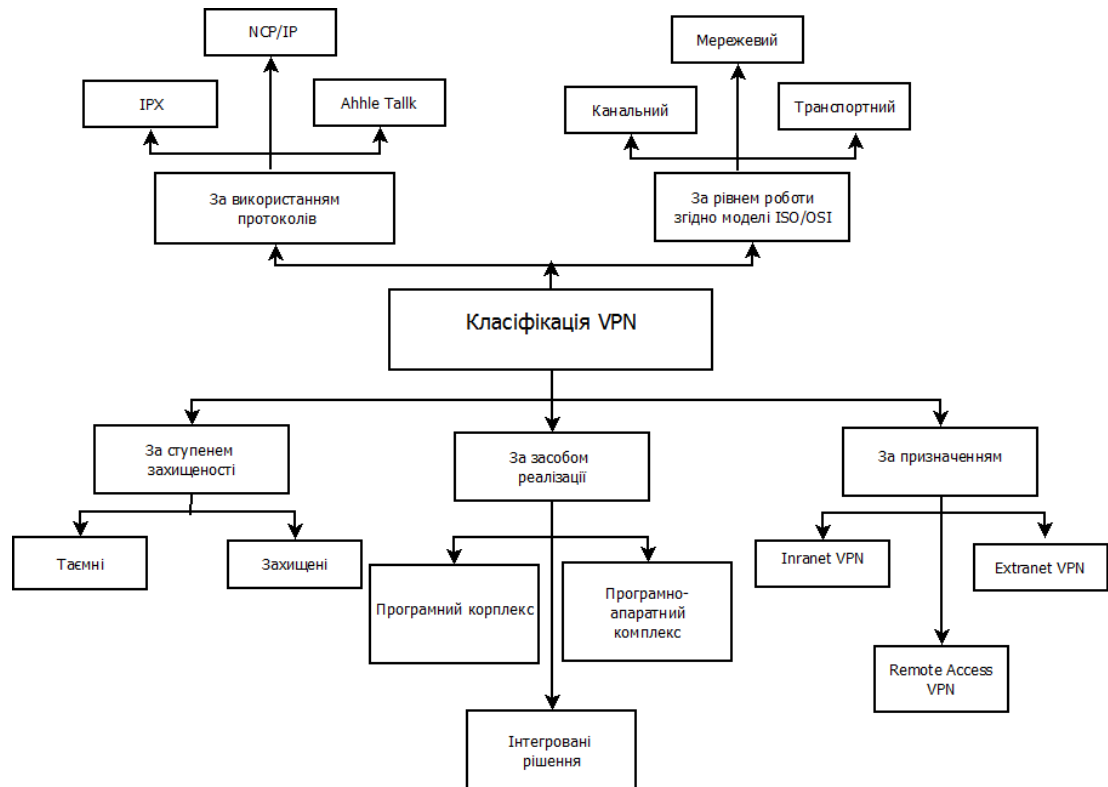


Рисунок 2.2 – Класифікація VPN

Мережі VPN на основі IPSec можуть бути побудовані за допомогою різних пристроїв таких як маршрутизатори Cisco, брандмауери Firewall, програмного забезпечення клієнта Cisco Secure VPN та концентраторів Cisco VPN. Маршрутизатори Cisco повинні мати вбудовану підтримку VPN з відповідними багатими можливостями програмного забезпечення Cisco IOS, що зменшує складність мережеских рішень та знижує загальну вартість VPN за можливості побудови багаторівневого захисту сервісів, що надаються. Брандмауер PIX Firewall є високопродуктивним мережеским пристроєм, який може обслуговувати кінцеві точки тунелів, забезпечуючи їм високу пропускну здатність та чудові функціональні можливості брандмауера, реалізацію стандартів IPSec (рис. 2.3) та забезпечуючи надійну взаємодію маршрутизаторів Cisco та брандмауерів PIX Firewall.

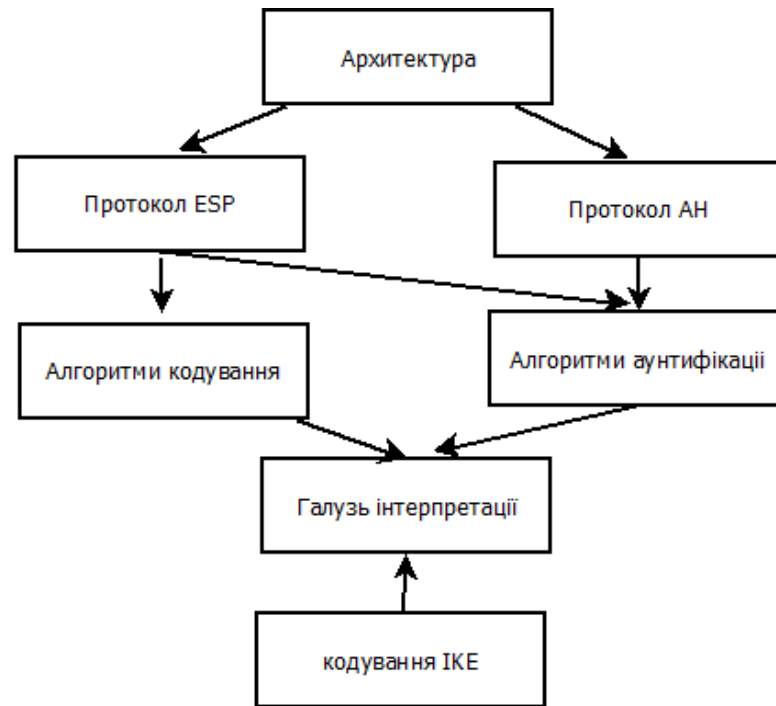


Рисунок 2 3 –Архітектура VPN

IPSec робить ряд технологічних рішень та методів шифрування.

Технічно IPSec і двох основних частин. Перша описує два нові заголовки, які можна додавати до пакета передачі ідентифікатора захисту, даних контролю цілісності та іншої інформації. Друга частина, ISAKMP (Internet Security and Key Management Protocol) – інтернет-безпека та протокол управління ключами), призначена для створення ключів. ISAKMP є середовищем. Основним протоколом для роботи є IKE (Internet Key Exchange – обмін ключами в Інтернеті). Повинна використовуватися версія 2 IKE, оскільки рання версія мала серйозні недоліки, як вказали Perlman і Kaufman, (2000).

Дію IPSec загалом можна як наступних основних кроків:

Крок 1. Початок процесу IPSec. Трафік, якому потрібно шифрування відповідно до політики захисту IPSec, узгодженої сторонами IPSec починає IKE-процес.

Крок 2. Перша фаза IKE. IKE-процес виконує аутентифікацію сторін IPSec та веде переговори про параметри асоціацій захисту IKE, внаслідок чого

створюється захищений канал для ведення переговорів про параметри асоціації захисту IPSec під час другої фази IKE.

Крок 3. Друга фаза IKE. IKE-процес веде переговори про параметри асоціації захисту IPSec та встановлює відповідні асоціації захисту IPSec для пристроїв сполучених сторін.

Крок 4. Передача даних. Відбувається обмін даними між сторонами IPSec, що базуються на параметрах IPSec та ключі, що зберігаються в базі даних асоціації захисту.

Крок 5. Завершення роботи тунелю IPSec. Асоціації захисту IPSec завершують свою роботу або в результаті їх видалення, або по причину перевищення граничного часу існування.

IPsec може працювати у двох режимах. У режимі транспортування заголовок IPsec вставляється відразу за заголовком IP. Поле Protocol заголовка IP змінюється таким чином, щоб було зрозуміло, що далі слідує заголовок IPsec (перед заголовком TCP). У заголовку IPsec міститься інформація щодо безпеки, зокрема, ідентифікатор захисту, новий порядковий номер і, можливо, перевірка цілісності поля корисного навантаження. У режимі тунелювання весь IP-пакет разом із заголовком вставляється всередину нового IP-пакету з новим заголовком. Цей режим хороший тоді, коли тунель закінчується десь поза кінцевим пунктом. У деяких випадках кінцем тунелю є шлюз, що забезпечує безпеку, наприклад корпоративний міжмережевий екран. Він зазвичай використовується для VPN (Virtual Private Network – віртуальна приватна мережа). У цьому режимі міжмережевий екран вставляє та виймає пакети, що проходять через нього у різні боки. За такої організації машини ЛОМ компанії гарантовано будуть обслужені за стандартом IPsec. Про це зовсім не доводиться турбуватися: всі турботи перебирає міжмережевий екран. Ще режим тунелювання корисний, коли кілька TCP-з'єднань об'єднуються разом і обробляються у вигляді єдиного шифрованого потоку, оскільки в цьому випадку зломщик не може дізнатися, хто і кому передає пакети, а також скільки.

Короткий опис VPN з огляду масштабованості:

- RegularIPSec/(cryptomap)/isakmp/ не масштабований;
- IPSec with dynamic IP (Dynamic VTI and Static VTI and IGP/Дуже масштабований. Всі spoke та hub знаходяться в одній мережі! Dynamic VTI (DVTIs) також point-to-point інтерфейс. У режимі point-to-multipoint сусідство OSPF не встановлюється. Використання Unnumbered IP як адреса DVTI обов'язково;
- EasyVPN/AAA – для авторизації / Масштабовантй.
- GRE / не масштабований. Утворює P2P лінк, кожен тунель – своя підмережа. Чудово підходить для тунелювання IGP протоколів.
- DMVPN / Найбільш масштабований протокол. GRE multipoint. Тунелі між віддаленими офісами створюються динамічно.
- PPTP / Масштабований з обмеженнями.
- Морально застарілий протокол, уразливість у криптографії в протоколі авторизації MSCHAPv2. Найчастіше використовується для створення віддаленого доступу. Підтримується безліччю популярних версій Windows. Використовується лише один протокол для шифрування -MPPE (RC4 зі 128-бітовим ключем). Підтримує мультикаст, т.к. PPP інкапсулюються у GRE.
- L2TPv2/v3 / Масштабований. Дас великі переваги, дозволяючи інкапсулювати не тільки PPP трафік, як L2TPv2, але й передавати мітку VLAN і, а також інкапсулювати HDLC, Frame Relay.
- OpenVPN / Масштабований. VPN-протокол та програмне забезпечення, яке використовує методи VPN для захисту з'єднань типу “точка-точка” та “сайт-сайт”.
- IGP over L2TPv2/v3 / Дуже масштабований. Дозволяє налаштовувати протоколи маршрутизації за замовчуванням, зв'язок віддалених офісів здійснюється через L2TPv2/v3 HUB (в центральному офісі).

Тому не для невеликих мереж, побудованих на роутерах, які не будуть швидко розширюватись можна обирати статичні протоколи VPN IPSec з

методами тунелювання, хешування та шифрування. Також оберемо метод site-to-site

2.2.2 Вибір параметрів шифрування та автентифікації

Автентифікація призначена для гарантії ідентичності користувачів і серверів. Користувачі надають пароль і сертифікат, сервери надають сертифікат.

Протоколи автентифікації:

PAP (відкритий текст);

– SPAP (повторно надсилає зашифрований пароль. Можливість повторного відтворення);

– CHAP (використовує MD5);

– MS-CHAP (односторонній, RSA MD4/DES);

– MS-CHAP v2 (кожен сеанс автентифікації використовує інший ключ);

– EAP (використовує MD5, подібний до CHAP, але у форматі EAP);

– EAP-TSL (використовується зі смарт-картами).

Шифрування робиться між кінцевими точками тунелювання. Пакети зашифровані та інкапсульовані у межах тунельного протоколу.

Перший тип коду, який ми введемо, називається симетричне шифрування ключа. Він передбачає: єдиний ключ для шифрування та розшифрування даних. Згаданий вище код був би дуже простою формою шифрування симетричного ключа, оскільки шифр ($a = z$, $b = y$, $c = x$ тощо) може використовуватися як для шифрування, так і для дешифрування інформації.

Зараз присутні такі версії як 3DES та AES є набагато складнішими. Вони передбачають додавання ключа до даних, а також багато раундів заміни та переміщення їх за допомогою складних математичних формул. Ці алгоритми роблять остаточний шифротекст абсолютно чужим від даних, які він повинен представляти.

Тому ми оберемо обидва методи, для побудови нашої мережі.

Команда `crypto isakmp policy` використовується для створення IKE політики, в якій вказуються бажані алгоритми та параметри захищеного каналу, що створюється.

Вказуються параметри ISAKMP SA за допомогою команд:

- authentication (IKE policy);
- encryption (IKE policy);
- hash (IKE policy);
- group (IKE policy);
- lifetime (IKE policy).

`priority` – унікальний ідентифікатор IKE політики. Як ідентифікатор слід використовувати ціле число від 1 до 10000. При цьому слід враховувати, що чим більше число, тим нижчим є пріоритет створюваної політики.

За замовчуванням в IKE політиці використовуються параметри для IKEv2 та IPsec.

- IKE policy encryption with Data Encryption Standard (DES) as the default,
 - IKE policy hash with Secure Hash Standard-1 (SHA-1) as the default,
 - IKE key exchange with Diffie-Hellman Group 1 (768-Bit) as the default,
 - IKE lifetime with a one-day (86,400 seconds) lifetime as the default,
- and

- IKE authentication with RSA public key as the default.
- Усі налаштування можна модифікувати, вимкнути та відновити:
- `default crypto ikev2 proposal`
- `default crypto ipsec transform-set`

Відновлення налаштувань:

- `crypto ikev2 proposal default;`
- `encryption aes-cbc-128;`
- `hash md5;`
- `crypto ipsec transform-set default aes-cbc 256 sha-hmac.`

Вимкнення налаштувань:

- no crypto ikev2 proposal default;
- no crypto ipsec transform-set default.

IKE SA lifetime 86400 сек. IPsec SA lifetime 3600 сек. Retransmission count 7 Retransmission interval 2, 4, 8, 16, 32, 64, 128 сек.

Кадр PPP шифрується за допомогою Microsoft Point-to-Point Encryption (MPPE) за допомогою ключів шифрування, згенерованих у процесі автентифікації MS-CHAP або EAP-TLS. Клієнти віртуальної приватної мережі повинні використовувати або протокол автентифікації MS-CHAP, або EAP-TLS, щоб корисне навантаження кадрів PPP було зашифровано. PPTP використовує переваги основного шифрування PPP та інкапсулює раніше зашифрований кадр PPP.

З доступних методів можливо обирати для crypto ikev2 одразу декілька методів, а для isakmp тільки по одному. Зазвичай обираються останні версії.

Приклад для обрання:

- encryption {des | 3des | aes | aes 192 | aes 256 };
- hash {sha | sha256 | sha384 | md5 };
- authentication {rsa-sig | rsa-encr | pre-share };
- group {1 | 2 | 5 | 14 | 15 | 16 | 19 | 20 | 24 };
- lifetime seconds.

Обираємо для порівняння hash {sha | md5 }; authentication pre-share; group { 2 | 5 } та застосуємо їх у нашій мережі.

2.3 Вибір структурної схеми мережі.

Оберемо найбільш часто випадок офісної мережі. З двома офісами та трьома роутерами, або двома офісами та можливістю з'єднання через Інтернет. На кожен роутер на внутрішню мережу додаємо по дві мережі.

Розробимо структурну схему мережі (рис.2.4).

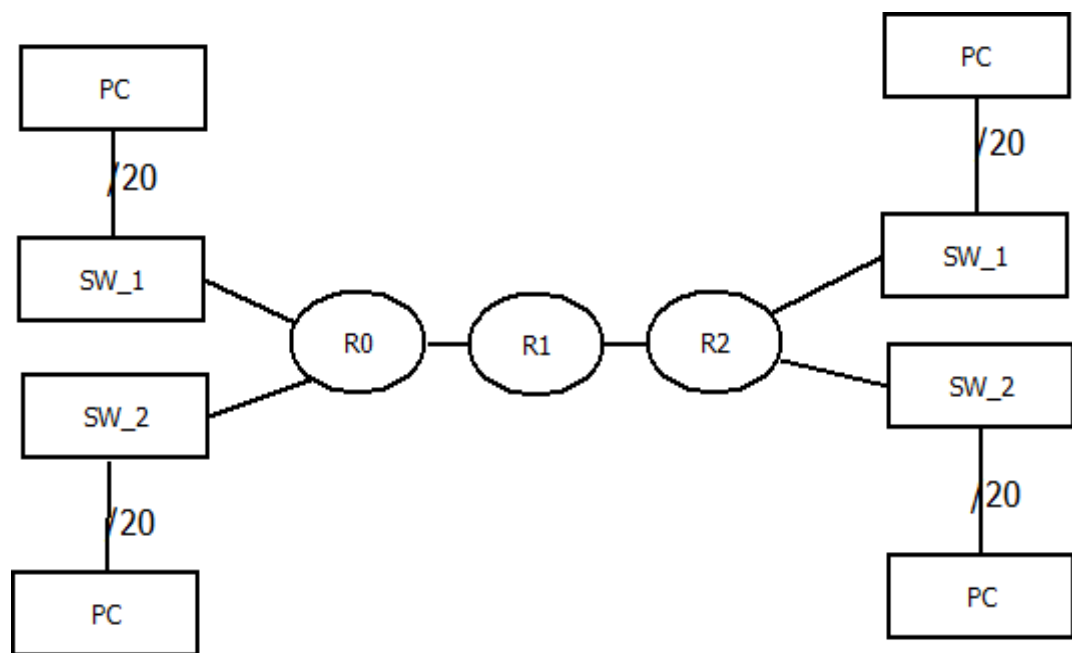


Рисунок 2.4 – Структурна схема корпоративної мережі

2.4 Вибір мережевого обладнання.

Активним мережним устаткуванням є маршрутизатор і комутатор. Повторювач (репітер) і концентратор (хаб) не є активним мережним устаткуванням, оскільки він тільки повторює сигнал для збільшення відстані з'єднання або топологічного розгалуження і нічого «інтелектуального» собою не являють. Але керовані комутатори відносяться до активного мережного

обладнання, так як можуть бути наділені певними «інтелектуальними властивостями».

Під пасивним мережним устаткуванням є обладнання, не наділене «інтелектуальними» особливостями. Наприклад – кабель, повторювач (репітер), патч-панель, концентратор (хаб), та інше. Працює на фізичному рівні мережевих протоколів – розмножує дані, що надходять на один порт з усіх інших.

Пристрої, що працюють на канальному рівні мережевих протоколів – записують MAC-адреси приєднаних комп'ютерів, деякі ідентифікатори мережевих карт і далі переправляють пакети тільки на той комп'ютер, чия MAC-адреса написана в пакеті. Перехід на свічі ліквідує проблему сніфінгу, крім того істотно знижує навантаження на лінії.

Свіч може мати виділений порт, так званий UpLink, призначений для відправки пакетів, що не знайшли адресата в локальній мережі. Найбільш поширені керовані світчі, що дозволяють до себе приєднатися – для початку через спеціальний порт (не мережевий) і налаштувати його з комп'ютера. Далі світча можна задати IP-адресу і надалі керувати ним по мережі. Незважаючи на наявність IP-адреси, світч залишається прозорим для мережевого рівня – наприклад, його неможливо виявити при трасуванні.

У локальній мережі основний роутер може роздавати IP-адреси по DHCP, контролювати допустимі IP-адреси. Роутери також виконують і функції більш високого рівня такі як мережевий екран. При цьому аналіз даних виконується на транспортному чи навіть прикладному рівні мережевих протоколів. Суть полягає в тому, що на роутері можна налаштувати, на які порти дозволити з'єднання, а на які – не потрібно, налаштувати переадресацію портів.

У сучасних мережах використовуються головним чином три типи середовищ, що зв'язують пристрої і забезпечують шлях, по якому передаються дані. До таких типів середовищ відносяться:

- металеві дроти усередині кабелю;

- скляні або пластикові волокна (оптоволоконний кабель);
- радіозв'язок.

Кодування сигналу, яке потрібне для передачі, здійснюється по-різному залежно від типу середовища. У металевих дротах дані кодуються у вигляді електричних імпульсів, що відповідають певним шаблонам. Передача в оптоволоконних мережах відбувається у вигляді імпульсів світла, в діапазоні інфрачервоного випромінювання або видимого світла. Для опису різних значень бітів При безпроводній передачі використовуються шаблони електромагнітного випромінювання. В мережевих технологіях існують три основні типи мідних кабелів:

- коаксіальний кабель;
- неекранована вита пара (UTP);
- екранована вита пара (STP).

Ці кабелі використовуються для з'єднання вузлів в локальній мережі і пристроїв мережевої інфраструктури, таких як комутатори, маршрутизатори і точки безпроводного доступу. Кожен тип з'єднання і відповідні пристрої мають певні вимоги до кабелів, передбачені стандартами фізичного рівня.

Коаксіальний кабель майже не використовують, тому швидкість передачі інформації від 1 до 10 Мбіт/с, в деяких випадках може досягати 50 і не має відповідної гнучкості для полегшення укладання.

Сучасні кабелі витой пари застосовуються в наступних стандартах технологій передачі пакетних даних: 100BASE-TX Ethernet; 1000BASE-T Ethernet; 10GBASE-T Ethernet; 40GbE, 100GbE.

Двожильне дротяне з'єднання "вита пара" є найбільш дешевим кабельним з'єднанням. Підтримує передачу даних на відстань до 100 метрів. На більших відстанях сигнал через загасання не розпізнається; якщо передача даних на більшу відстань все-таки необхідна, потрібно скористатися повторювачем, або задіяти інший кабель. Перевагами є низька ціна і легка установка. Неекранована вита пара складається з восьми дротів. Кожен дріт окремо ізольований; усі вісім дротів зібрано в чотири звиті пари. Скручення

дротів запобігає перехресним перешкодам, що наводяться сусідніми парами і зовнішніми джерелами. Усі чотири пари поміщені в загальну оболонку. Існують екранована вита пара (UTP) та екранована вита пара (STP) (рис 2.1).

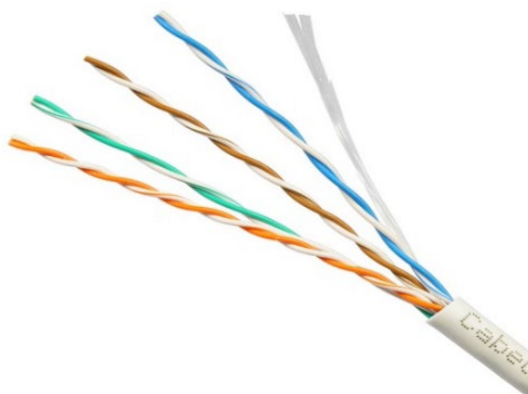


Рисунок 2.1 – Кабель вита пара

Для підвищення захищеності інформації часто використовують екрановану пару, поміщену в екрануючу оболонку, схожу до екрану коаксіального кабелю.

Оптоволоконний кабель – конструкція з одного або декількох ізолюваних один від одного оптичних волокон (оптоволокно), укладених в оболонку. Крім власне оптичних волокон і ізоляції може містити екран, силові елементи та інші конструктивні елементи. Також це фізичний медіум, що складається з певної кількості оптичних волокон, оточених спільною захисною оболонкою, та використовується для передачі світлового потоку.

Оптична кабельна лінія – лінія оптичних сигналів і складається з одного або декількох паралельних кабелів з з'єднувальними, стопорними та кінцевими муфтами (ущільненнями) та кріпильними деталями.

Оптичне волокно складається із:

- серцевини;
- оптичної оболонки
- захисного покриття

– буферного покриття (опціонально).

Одномодове волокно (SM) буває: 8/125 і 9/125 мкм (d серцевини – 8 мкм, діаметр волокна – 125 мкм тощо). Багатомодове (MM) буває: 50/125 і 62/125 мкм.(рис. 2.2). Одномодове волокно дешевше за багатомодове, дозволяє передавати оптичний імпульс на великі відстані, з меншим розходженням сигналу на виході, але в той же час прямо передавальне устаткування для нього значно дорожче. Є також багатомодове волокно з градієнтним профілем у якого ще менше недоліків.



Рисунок 2.2 – Кабель оптоволоконно

Тому для мереж WAN обираємо оптичне волокно, а для мереж LAN кабель віта пара.

За для безпеки мережі та налаштування IP-адрес комп'ютерів обираємо маршрутизатори(роутери). А за для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента комп'ютерів з роутерами обираємо мережевий комутатор (світ) з WS-C2950-24 комутатор такими параметрами:

- Кількість портів комутатора.....24 xEthernet 10/100 Мбіт/сек;
- Підтримка роботи у стеку.....є;
- Внутрішня пропускна здатність....13.6 Гбіт/сек;
- Розмір таблиці MAC адрес.....8192.

Серед маршрутизаторів обираємо обладнання компанії Cisco Systems, тому що вони реалізують широкий набір засобів і протоколів, використовуваних при взаємодії локальних мереж. Обладнання Cisco

підтримує різноманітні засоби підключення: Frame Relay X.25, та ISDN, дозволяє створювати доволі складні системи, має змогу додавати різні роземи, а так містять засоби розширеної аналітики, оптимізації роботи додатків, автоматичного виділення ресурсів та вбудованої безпеки. Тому ми обираємо роутер Cisco 2811 (рис.2.3).

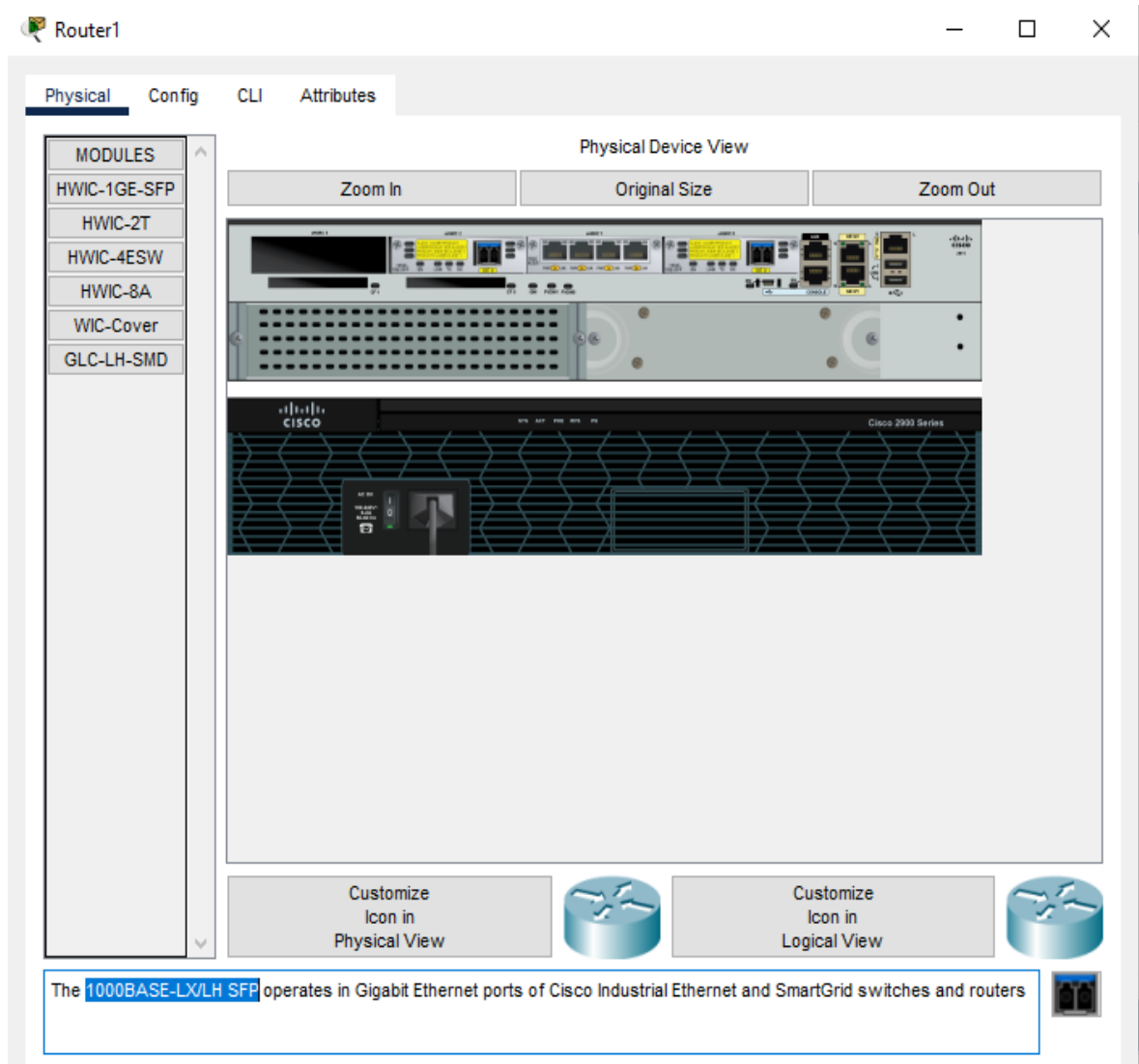


Рисунок 2.3 – Схема підключення роутера Cisco 2811

Технічні характеристики Маршрутизатора Cisco 2811-CCME/K9:

- Product Description: 2811 Voice Bundle w/ PVD2-16,FL-CCME-36,SP Serv,64F/256D;
- Network Technology: 10/100Base-TX;

– Certifications & Standards: IEEE 802.3: 10BASE-T/IEEE 802.3u: 100BASE-TX / USB 1.1.

Налаштуваннями безпеки:

- AIM-based security acceleration;
- SecureShell (SSH);
- Easy VPN Client and Server;
- VPN Hardware Acceleration (on motherboard);
- DES, 3DES, AES 128, AES 192, and AES 256;
- ThreatDefense;
- Cisco IOS Firewall;
- Transparent Firewall;
- Intrusion Detection;
- Intrusion Prevention;
- URL Filtering;
- Trust and Identity;
- Network Admission Control (NAC);
- Authentication, Authorization, and Accounting (AAA);
- 802.1x Support.

Опис Cisco GLC-LH-SM SFP Модуль Оптичний трансівер (рис 2.4)

Трансівери або SFP конвертори – це пристрої, які підключаються до гігабітного порту Ethernet і призначені для об'єднання цього порту з мережею. Трансівери взаємозамінні і можуть бути використані в змішаних комбінаціях 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, або 1000BASE-BX10-D/U. Стандартний Ethernet кабель (RJ45), ще називають кручений парою, здатний передавати сигнал на відстань 100 м, використовується для підключень в межах будівлі. Оптичне волокно може передавати сигнал на великі відстані та використовується для підключення віддалених пунктів до існуючої мережі. Модуль Cisco GLC-LH-SM є одним з найбільш широко використовуваних 1-гігабітних оптичних трансіверів; працює як зі стандартними сингломодовими

оптичними кабелями, довжиною до 10 км, так і з будь-якими мультимодовими волокнами, довжиною до 550 м.

Технічні характеристики Cisco GLC-LH-SM:

- вихідна потужність передавача: -9.5 ~ -3 dBm;
- чутливість приймача: -22 dBm;
- довжина хвилі передавача: 1270~1340 nm, (1310 nm);
- довжина хвилі приймача: 1100~1600 nm, (1310 nm);
- швидкість передачі даних: 100Mbps~ 1,25Gbps;
- максимальна довжина двоволоконного одномодового кабелю

оптичного 9/125 мкм: 10 km.



Рисунок 2.4 – GLC-LH-SM SFP Модуль Оптичний трансівер

2.4. Вибір списків керування доступом

Робимо розширені та іменовані списки керування доступом. Це ми робимо за для зручності та збільшення функціональності.

2.5 Висновки за розділом 2

У розділі було розглянуто та обрано зручні інструменти для розробки захищеної мережі на базі стимулятора CiscoPacketTracer, та протоколиVPN, GRE та IPsec, з використанням методів шифрування та автентифікації: Та обрані наступні методи шифрування та автентифікації:

- encryption { 3des | aes };
- hash { sha | md5 };
- authentication { pre-share };
- group { 2 | 5 }.

3. ЗАСТОСУВАННЯ МЕТОДІВ ЗАХИСТУ МЕРЕЖ

3.1 Налаштування мережі, та створення протоколів захисту

Налаштуємо звичайну мережу, яка створюється з двох офісів, які мають дві мережі з'єднані через роутер. Схема зібрана на стимуляторі Cisco Packet Tracer. (рис 3.1)

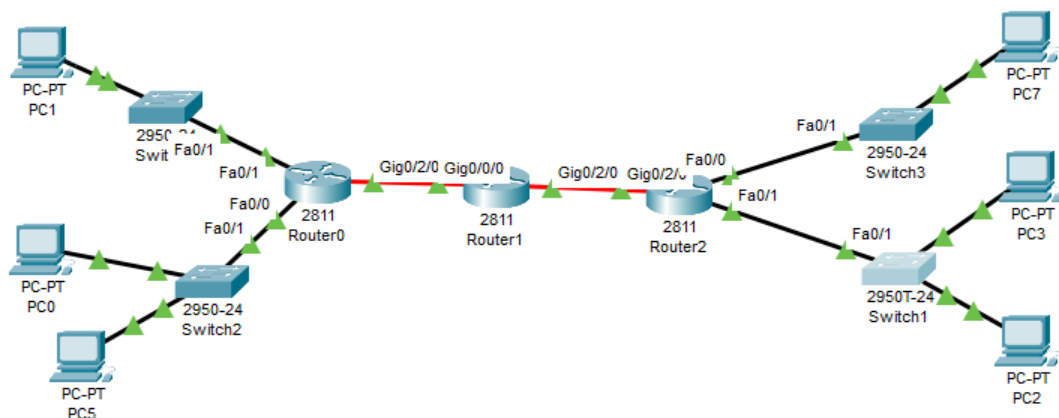


Рисунок 3.1 – Схема побудови мережі

Данні занесемо у таблицю 3.1

Таблиця 3.1 – Параметри інтерфейсів

Роутер	Інтерфейс	ІР-адреса	Маска
R0	Gi0/2/0	210.210.1.2	255.255.255.253
R0	Fa0/0	192.168.3.1	255.255.255.0
R0	Fa0/1	192.168.1.1	255.255.255.0
R0	Gi0/2/0	210.210.1.2	255.255.255.253
R1	Gi0/2/0	210.210.2.2	255.255.255.253
R1	Gi0/0/0	210.210.1.1	255.255.255.253
R2	Fa0/0	192.168.4.1	255.255.255.0
R2	Fa0/1	192.168.2.1	255.255.255.0
R2	Gi0/2/0	210.210.1.2	255.255.255.253

Спочатку налаштуємо мережу за допомогою протоколу Ospf.

Для роутера R0:

```
Router(config-if)#ex
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#network 210.210.1.0 0.0.0.3 area 0
Router(config-router)#
```

Для роутера R1:

```
Router(config-if)#ex
Router(config)#router ospf 1
Router(config-router)#network 210.210.2.0 0.0.0.3 area 0
Router(config-router)#network 210.210.1.0 0.0.0.3 area 0
Router(config-router)#
```

Для роутера R2:

```

Router(config)#router ospf 1
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#network 192.168.4.0 0.0.0.255 area 0
Router(config-router)#network 210.210.2.0 0.0.0.3 area 0

```

Зробимо команду ping PC1 на PC3 (рис.3.3), та PC1 на PC 7 (рис.3.2).

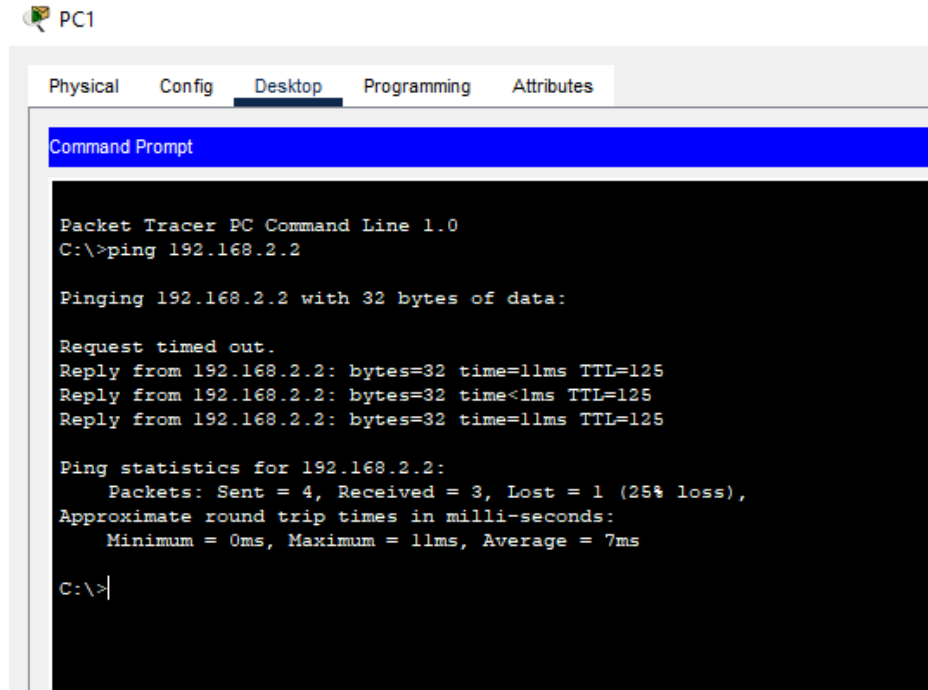


Рисунок 3.2 – Команда ping PC1 на PC3

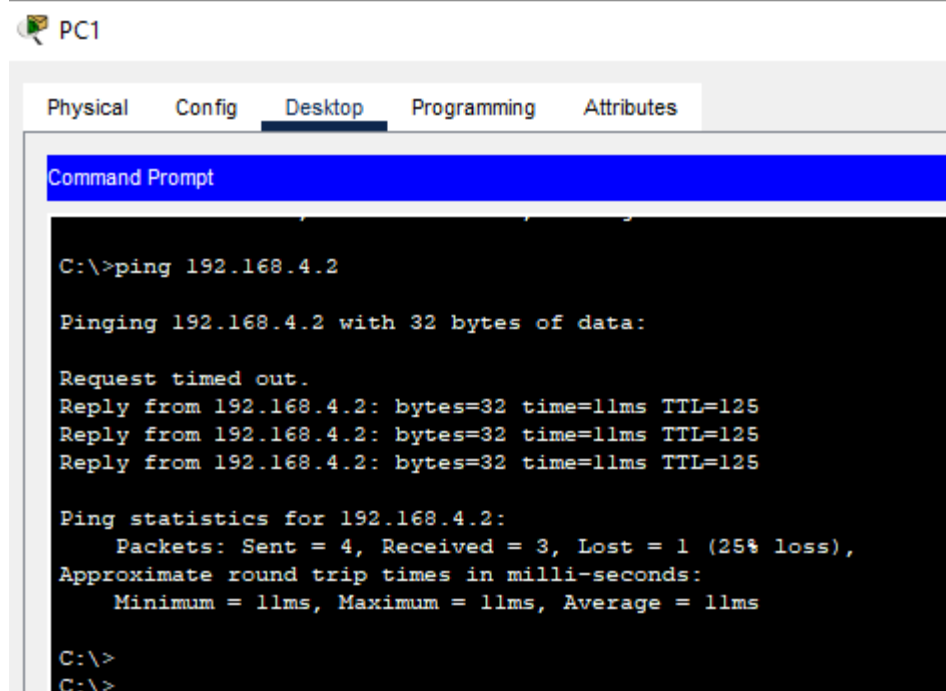


Рисунок 3.3– Команда ping PC1 PC7

Зробимо команду pingPC7 на PC (рис. 3.4), та PC7 на PC1 (рис. 3.5).

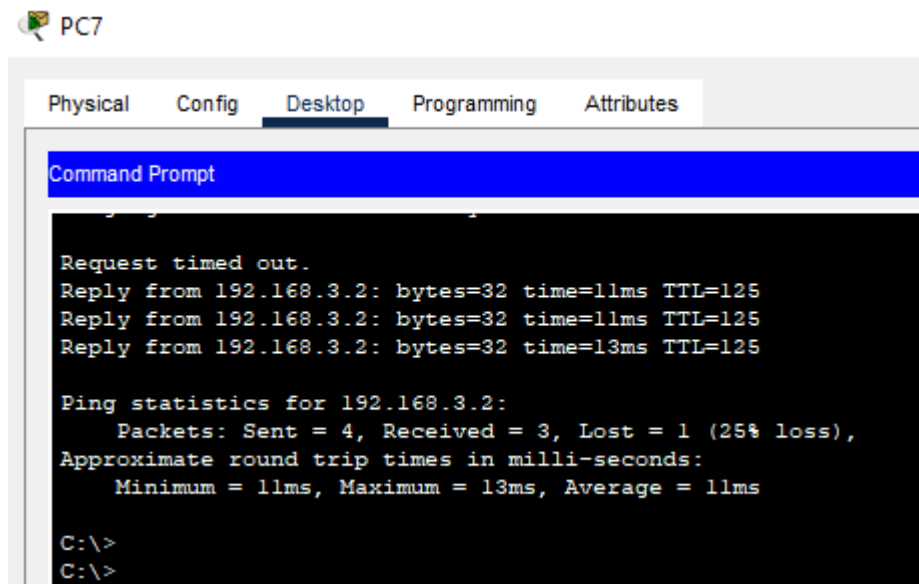


Рисунок 3. 4 – Команда pingPC7на PC5

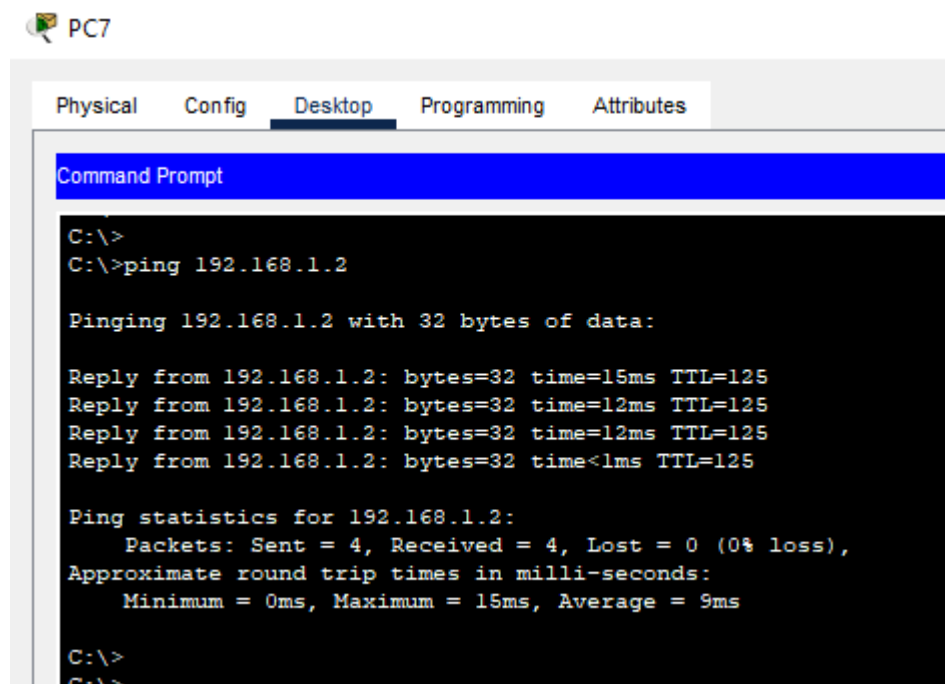


Рисунок 3.5 – Команда pingPC7на PC1

Мережа налаштована, та працює.

Пропишемо VPN першим способом. Налаштуємо для цієї мережі протокол IPSec (режим транспорт) over GRE для двох інтерфейсів на роутері R0:

```
Router(config)#access-list 160 permit ip 192.168.1.0
0.0.0.255 192.168.2.0 0.0.0.255
Router(config)#access-list 160 permit ip 192.168.3.0
0.0.0.255 192.168.4.0 0.0.0.255
Router(config)#crypto isakmp policy 160
Router(config-isakmp)#encryption aes
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#ex
Router(config)#crypto isakmp key cisco address 210.210.2.1
Router(config)#crypto ipsec transform-set RK_RZ_Setesp-
aesesp-sha-hmac
Router(config)#crypto map RK_RZ_Map 160 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
and a valid access list have been configured.
Router(config-crypto-map)#description VPN connection RK_RZ
Router(config-crypto-map)#set peer 210.210.2.1
Router(config-crypto-map)#set transform-set RK_RZ_Set
Router(config-crypto-map)#match address 160
Router(config-crypto-map)#ex
Router(config)#int gi0/2/0
Router(config-if)#crypto map RK_RZ_Map
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#ex
Router(config)#interface tunnel 0

Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

Router(config-if)#ip address 192.168.0.1 255.255.255.252
Router(config-if)#tunnel source gi0/2/0
Router(config-if)#tunnel destination 210.210.2.1
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to up
```

Аналогічно налаштовуємо роутер R2:

```
Router(config)#access-list 160 permit ip 192.168.2.0
0.0.0.255 192.168.1.0 0.0.0.255
Router(config)#access-list 160 permit ip 192.168.4.0
0.0.0.255 192.168.3.0 0.0.0.255
Router(config)#crypto isakmp policy 160
Router(config-isakmp)#encryption aes
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
```

```

Router(config-isakmp)#ex
Router(config)#crypto isakmp key cisco address 210.210.1.2
Router(config)#crypto ipsec transform-set RK_RZ_Setesp-
aesesp-sha-hmac
Router(config)#crypto map RK_RZ_Map 160 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
and a valid access list have been configured.
Router(config-crypto-map)#description VPN connection RK_RZ
Router(config-crypto-map)#set peer 210.210.1.2
Router(config-crypto-map)#set transform-set RK_RZ_Set
Router(config-crypto-map)#match address 160
Router(config-crypto-map)#ex
Router(config)#int gi0/2/0
Router(config-if)#crypto map RK_RZ_Map
*Jan 3 07:16:26.785: %CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
Router(config-if)#ex
Router(config)#interface tunnel 0

Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

Router(config-if)#ip address 192.168.0.2 255.255.255.252
Router(config-if)#tunnel source gi0/2/0
Router(config-if)#tunnel destination 210.210.1.2
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to up

```

Перевіряємо роутер R1:

```

Router(config-if)#tunnel mode greip
Router(config-if)#ex
Router>en
Router#sh crypto ipsectr
Transform set RK_RZ_Set: { {esp-aesesp-sha-hmac }
will negotiate = { Tunnel, },
Transform set #${default_transform_set_1: { esp-aesesp-sha-
hmac }
will negotiate = { Transport, },
Transform set #${default_transform_set_0: { esp-3des esp-
sha-hmac }
will negotiate = { Transport, },
Router#sh crypto isakmpsa
IPv4 Crypto ISAKMP SA
dstsrc state conn-id slot status
210.210.2.1 210.210.1.2 QM_IDLE 1064 0 ACTIVE
interface: GigabitEthernet0/2/0
Crypto map tag: RK_RZ_Map, local addr 210.210.1.2

protectedvrf: (none)

```

```

    local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port):
(192.168.2.0/255.255.255.0/0/0)
    current_peer 210.210.2.1 port 500
    PERMIT, flags={origin_is_acl,}
    #pktsencaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pktsdecaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pktscompressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pktscompr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
Router>en
Router#sh crypto ipsec sa

interface: GigabitEthernet0/2/0
Crypto map tag: RK_RZ_Map, local addr 210.210.1.2

protected vrf: (none)
    local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port):
(192.168.2.0/255.255.255.0/0/0)
    current_peer 210.210.2.1 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 210.210.1.2, remote crypto
endpt.:210.210.2.1
    path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/2/0
    current outbound spi: 0x0(0)

inbound esp sas:

--More--
00:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 210.210.2.2 on
GigabitEthernet0/2/0 from LOADING to FULL, Loading Done
inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

```

```

    local ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port):
(192.168.4.0/255.255.255.0/0/0)
    current_peer 210.210.2.1 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    --More--
    %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to up
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 210.210.1.2, remote crypto
endpt.:210.210.2.1
    path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/2/0
    current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:
Router>en
Router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id slot status
210.210.2.1 210.210.1.2 QM_IDLE 1082 0 ACTIVE

```

Аналогічно перевіряємо роутер R2:

```

localcryptoendpt.: 210.210.1.2,
remotecryptoendpt.:210.210.2.1
    pathmtu 1500, ipmtu 1500, ipmtuidb GigabitEthernet0/2/0
    current outbound spi: 0x0(0)

    local ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port):
(192.168.4.0/255.255.255.0/0/0)
    current_peer 210.210.2.1 port 500
    PERMIT, flags={origin_is_acl,}
    #pktsencaps: 0, #pkts encrypt: 0, #pkts digest: 0

```

```

#pktsdecaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pktscompressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pktscompr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 210.210.1.2, remote crypto
endpt.:210.210.2.1
pathmtu 1500, ipmtu 1500, ipmtuidb GigabitEthernet0/2/0
currentoutboundspi: 0x0(0)
Router#sh crypto ipsec sa

interface: GigabitEthernet0/2/0
Crypto map tag: RK_RZ_Map, local addr 210.210.2.1

protected vrf: (none)
local ident (addr/mask/prot/port):
(192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
current_peer 210.210.1.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 210.210.2.1, remote crypto
endpt.:210.210.1.2
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/2/0
current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcsp sas:

outbound esp sas:

outbound ah sas:

outbound pcsp sas:

local ident (addr/mask/prot/port):
(192.168.4.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
current_peer 210.210.1.2 port 500
PERMIT, flags={origin_is_acl,}

```

```

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 210.210.2.1, remote crypto
endpt.:210.210.1.2
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/2/0
current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcp sas:

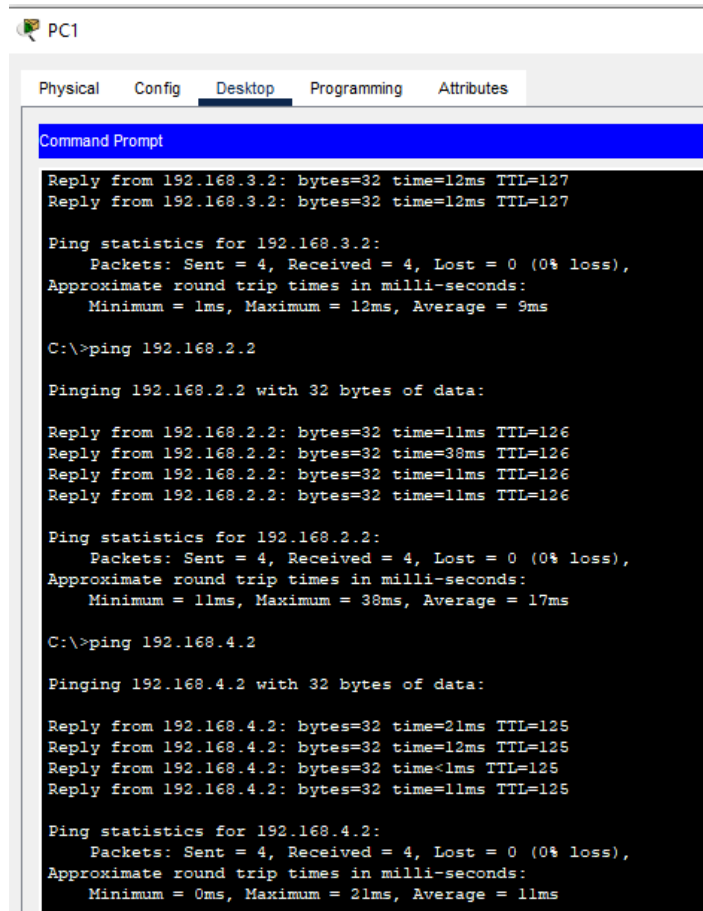
outbound esp sas:

outbound ah sas:

outbound pcp sas:
Router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id slot status
210.210.1.2 210.210.2.1 QM_IDLE 1057 0 ACTIVE

```

Перевіримо працездатність мережі за допомогою протоколу ICMP (Internet Control Messages Protocol) – протокол передачі керуючих повідомлень в Internet) за допомогою команди ping (рис. 3. 6), та зробимо pingз PC3 на PC1 та PC4 (рис. 3.7).



PC1

Physical Config Desktop Programming Attributes

Command Prompt

```

Reply from 192.168.3.2: bytes=32 time=12ms TTL=127
Reply from 192.168.3.2: bytes=32 time=12ms TTL=127

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 9ms

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=11ms TTL=126
Reply from 192.168.2.2: bytes=32 time=38ms TTL=126
Reply from 192.168.2.2: bytes=32 time=11ms TTL=126
Reply from 192.168.2.2: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 38ms, Average = 17ms

C:\>ping 192.168.4.2

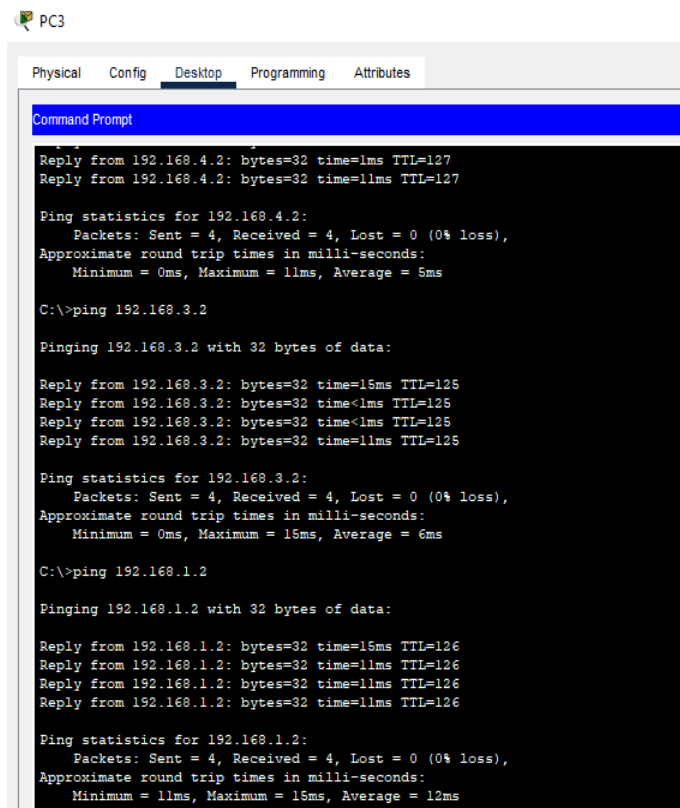
Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time=21ms TTL=125
Reply from 192.168.4.2: bytes=32 time=12ms TTL=125
Reply from 192.168.4.2: bytes=32 time<1ms TTL=125
Reply from 192.168.4.2: bytes=32 time=11ms TTL=125

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 21ms, Average = 11ms

```

Рисунок 3.6 – Команда pingPC1 на PC3 та PC7



PC3

Physical Config Desktop Programming Attributes

Command Prompt

```

Reply from 192.168.4.2: bytes=32 time=1ms TTL=127
Reply from 192.168.4.2: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 5ms

C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=15ms TTL=125
Reply from 192.168.3.2: bytes=32 time<1ms TTL=125
Reply from 192.168.3.2: bytes=32 time<1ms TTL=125
Reply from 192.168.3.2: bytes=32 time=11ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 15ms, Average = 6ms

C:\>ping 192.168.1.2

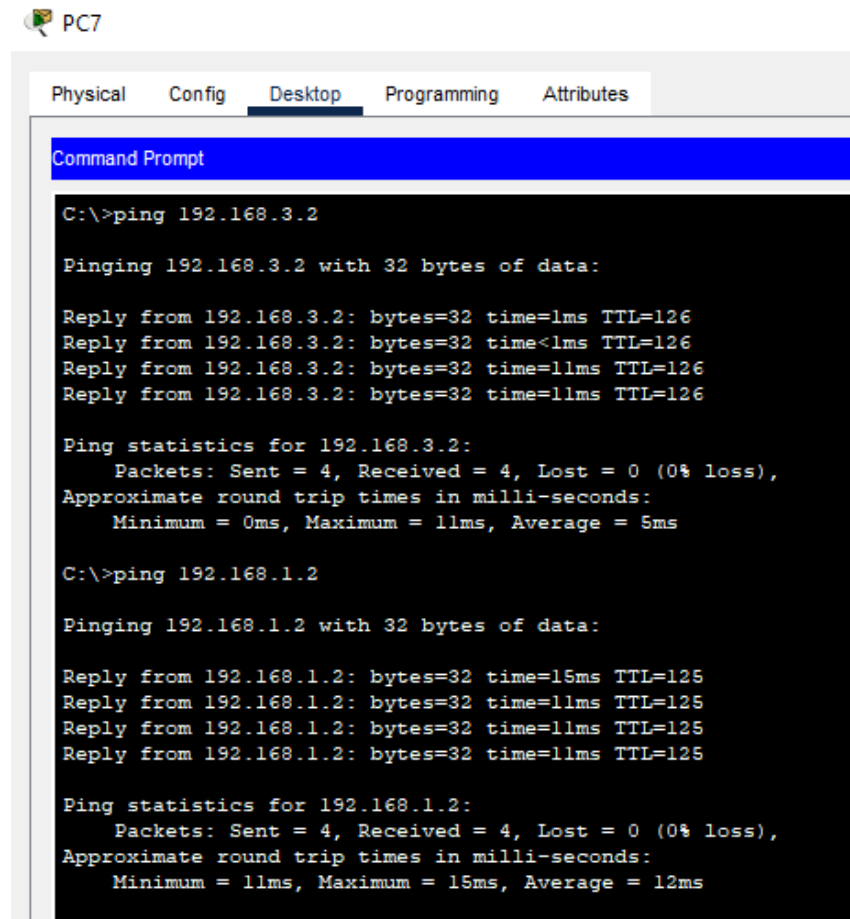
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=15ms TTL=126
Reply from 192.168.1.2: bytes=32 time=11ms TTL=126
Reply from 192.168.1.2: bytes=32 time=11ms TTL=126
Reply from 192.168.1.2: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 15ms, Average = 12ms

```

Рисунок 3.7 – Команда pingз PC3 на PC1 та PC5



The screenshot shows a PC7 desktop environment with a window titled 'PC7'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active, showing a 'Command Prompt' window. The Command Prompt displays the results of two ping commands: 'ping 192.168.3.2' and 'ping 192.168.1.2'. Both commands show successful results with 0% loss and round trip times in milliseconds.

```

C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Reply from 192.168.3.2: bytes=32 time<1ms TTL=126
Reply from 192.168.3.2: bytes=32 time=11ms TTL=126
Reply from 192.168.3.2: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 5ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=15ms TTL=125
Reply from 192.168.1.2: bytes=32 time=11ms TTL=125
Reply from 192.168.1.2: bytes=32 time=11ms TTL=125
Reply from 192.168.1.2: bytes=32 time=11ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 15ms, Average = 12ms
  
```

Рисунок 3.8– Команда ping з PC7 на PC1 та PC5

Всі роутери пінгуються один до одного.

Пропишемо VPN другим способом. Зробимо мережу, де комп'ютери з мережі 192.168.2.0 бачать тільки комп'ютери з мережі 192.168.1.0, а комп'ютери мережі 192.168.3.0 тільки комп'ютери 192.168.4.0. Для цього налаштуємо мережі 192.168.2.0 192.168.1.0 за допомогою IPSec, а мережі 192.168.3.0 192.168.4.0 за допомогою GRE:

На роутері R1:

```

Router(config-if)#ex
Router(config)#interface tunnel 0
Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up
Router(config-if)#ip address 192.168.0.1 255.255.255.252
Router(config-if)#tunnel source gi0/2/0
Router(config-if)#tunnel destination 210.210.2.1
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to up
Router(config-if)#tunnel mode greip
  
```

```
Router(config-if)#ex
```

На роутері R2:

```
Router(config-if)#ex
Router(config)#interface tunnel 0
Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up
Router(config-if)#ip address 192.168.0.2 255.255.255.252
Router(config-if)#tunnel source gi0/2/0
Router(config-if)#tunnel destination 210.210.1.2
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to up
Router(config-if)#tunnel mode greip
Router(config-if)#ex
```

На роутері R1:

```
Router(config)#router ospf 1
Router(config-router)#network 192.168.0.0 0.0.0.3 area 0
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#ex
```

На роутері R2:

```
Router(config)#router ospf 1
Router(config-router)#network 192.168.0.0 0.0.0.3 area 0
Router(config-router)#network 192.168.4.0 0.0.0.255 area 0
Router(config-router)#ex
```

Перевіримо формування тунелю (рис.3.9).

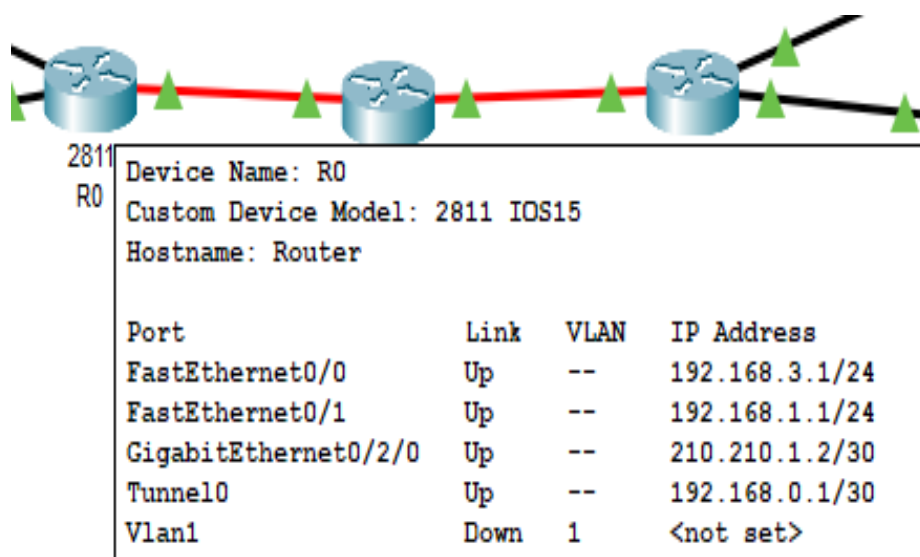


Рисунок 3.9– Формування тунелю

Для комп'ютерів мереж 192.168.1.0 та мереж 192.168.2.0 пропишемо IPSecsite-to-site:

На роутері R1:

```
Router#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encr 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#ex
Router(config)#crypto isakmp key cisco address 210.210.2.1
Router(config)#ip access-list extended VPN-TRAFFIC
Router(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255
Router(config-ext-nacl)#ex
Router(config)#crypto ipsec transform-set TS esp-3des esp-
md5-hmac
Router(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
and a valid access list have been configured.
Router(config-crypto-map)#set peer 210.210.2.1
Router(config-crypto-map)#set transform-set TS
Router(config-crypto-map)#match address VPN-TRAFFIC
Router(config-crypto-map)#ex
Router(config)#int gi0/2/0
Router(config-if)#crypto map CMAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#ex
```

Видаляємо старий access-list та створюємо новий.

```
Router(config)#no ip access-list standard FOR-NAT
Router(config)#ip access-list extended FOR-NAT
Router(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 any
Router(config-ext-nacl)#ex
Router(config)#
```

Аналогічно створюємо маршрутизацію на роутері R2:

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
```

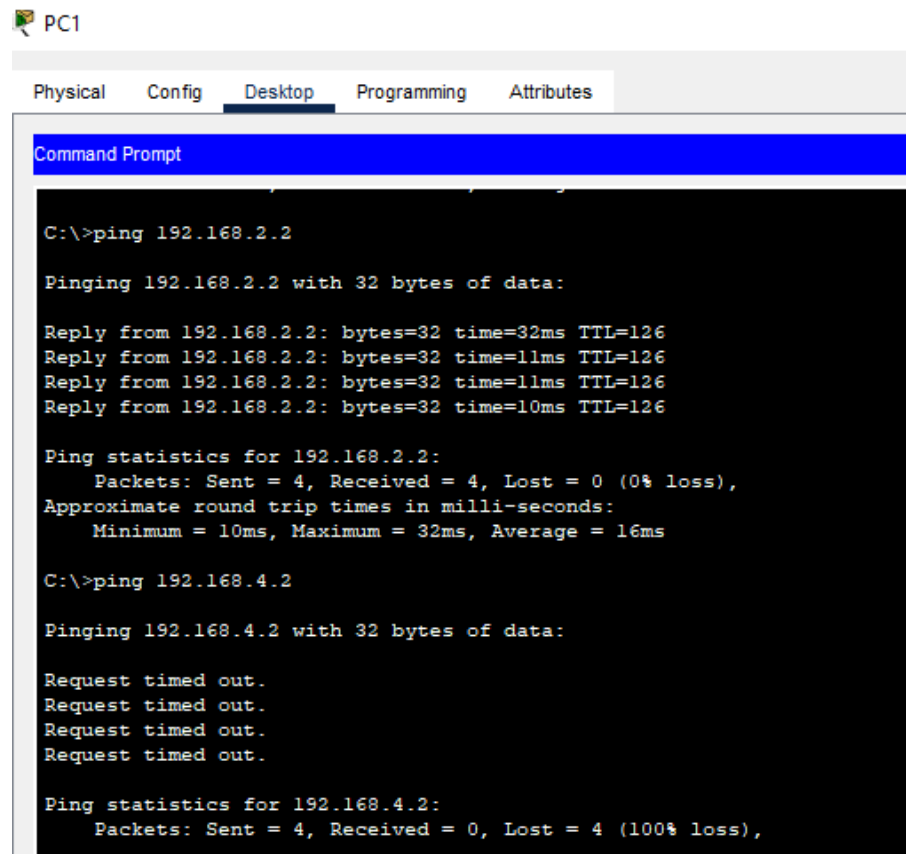
```

Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encr 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#ex
Router(config)#crypto isakmp key cisco address 210.210.1.2
Router(config)#ip access-list extended VPN-TRAFFIC
Router(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255
Router(config-ext-nacl)#ex
Router(config)#crypto ipsec transform-set TS esp-3des esp-
md5-hmac
Router(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
and a valid access list have been configured.
Router(config-crypto-map)#set peer 210.210.1.2
Router(config-crypto-map)#set transform-set TS
Router(config-crypto-map)#match address VPN-TRAFFIC
Router(config-crypto-map)#ex
Router(config)#int gi0/2/0
Router(config-if)#crypto map CMAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#ex
Router(config)#no ip access-list standard FOR-NAT
Router(config)#ip access-list extended FOR-NAT
Router(config-ext-nacl)#deny ip 192.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 any
Router(config-ext-nacl)#ex
Router(config)#

```

Як тільки ми застосуємо криптографічну карту до інтерфейсу, ми отримуємо повідомлення від маршрутизатора, що підтверджує, що isakmpувімкнено: “ISAKMP is ON”.

Перевіримо мережі за допомогою команди ping (рис 3.11 та рис 3.10).



PC1

Physical Config **Desktop** Programming Attributes

Command Prompt

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=32ms TTL=126
Reply from 192.168.2.2: bytes=32 time=11ms TTL=126
Reply from 192.168.2.2: bytes=32 time=11ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 32ms, Average = 16ms

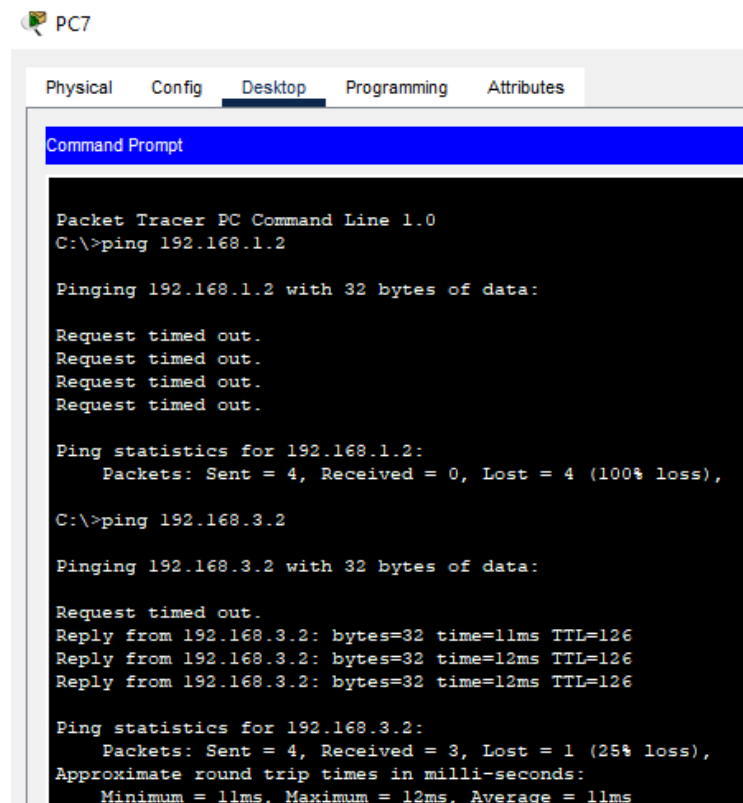
C:\>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рисунок 3.10 – Команда ping з PC1 на PC3 та PC7



PC7

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.3.2

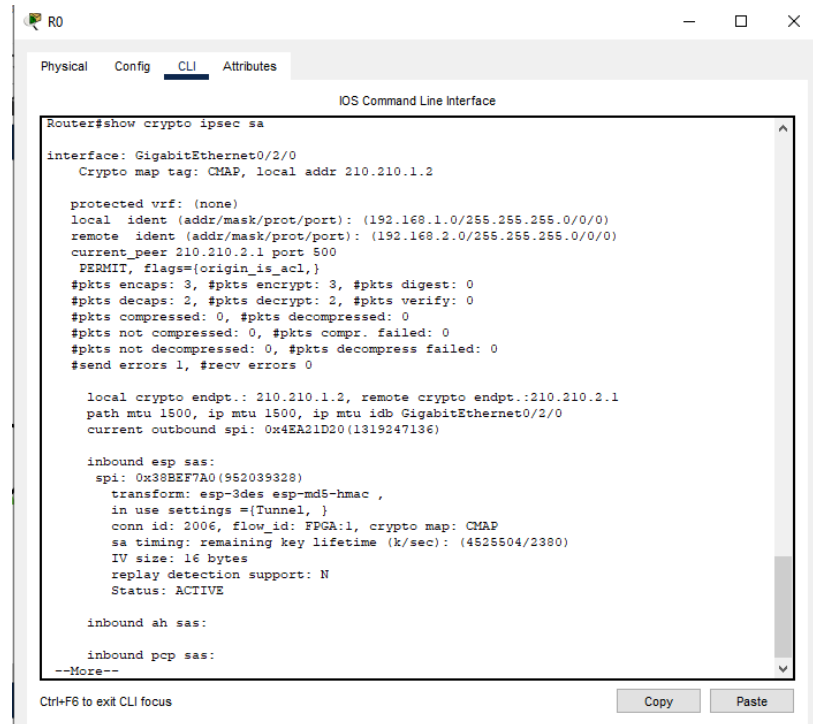
Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.2: bytes=32 time=11ms TTL=126
Reply from 192.168.3.2: bytes=32 time=12ms TTL=126
Reply from 192.168.3.2: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 12ms, Average = 11ms
```

Рисунок 3.11 – Команда ping з PC7 на PC1 та PC5

За допомогою команди `show crypto ipsec sa` са перевіriamo налаштування VPN (рис.3.12, рис.3.13).



```

Router#show crypto ipsec sa

interface: GigabitEthernet0/2/0
  Crypto map tag: CMAP, local addr 210.210.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer 210.210.2.1 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 210.210.1.2, remote crypto endpt.:210.210.2.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/2/0
current outbound spi: 0x4EA21D20(1319247136)

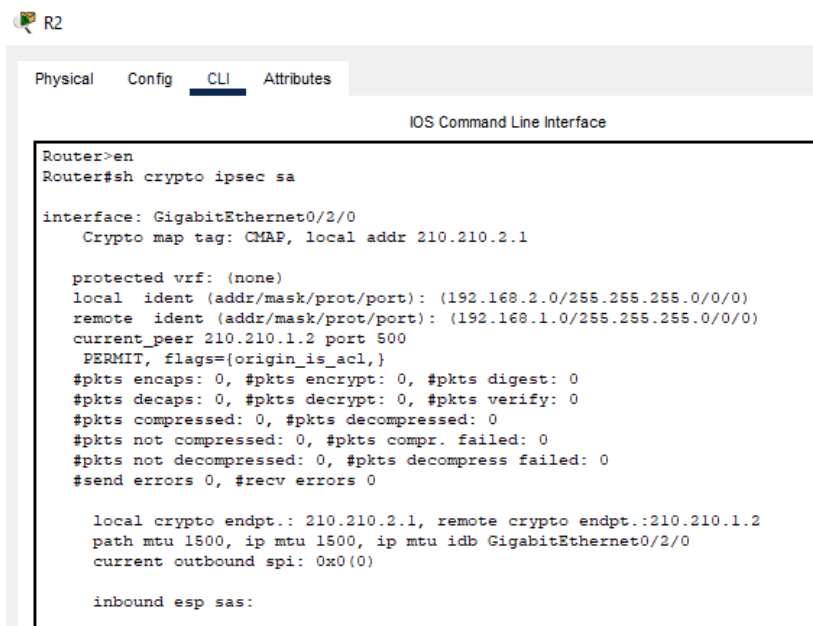
inbound esp sas:
  spi: 0x38BEF7A0(952039328)
    transform: esp-3des esp-md5-hmac ,
    in use settings = {Tunnel, }
    conn id: 2006, flow_id: FPGA:1, crypto map: CMAP
    sa timing: remaining key lifetime (k/sec): (4525504/2380)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

--More--
  
```

Рисунок 3.12 – Перевірка VPN на R0



```

Router>en
Router#sh crypto ipsec sa

interface: GigabitEthernet0/2/0
  Crypto map tag: CMAP, local addr 210.210.2.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 210.210.1.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 210.210.2.1, remote crypto endpt.:210.210.1.2
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/2/0
current outbound spi: 0x0(0)

inbound esp sas:
  
```

Рисунок 3.13 – Перевірка VPN на R2

Усі налаштування на роутері R0:

```

Router>en
Router#sh crypto ipsec sa

interface: GigabitEthernet0/2/0
Crypto map tag: CMAP, local addr 210.210.1.2

protected vrf: (none)
local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(192.168.2.0/255.255.255.0/0/0)
current_peer 210.210.2.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
#pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 210.210.1.2, remote crypto
endpt.:210.210.2.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/2/0
current outbound spi: 0x86E43B8B(2263104395)

inbound esp sas:
spi: 0x313B2B09(825961225)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2005, flow_id: FPGA:1, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4525504/2963)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x86E43B8B(2263104395)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2006, flow_id: FPGA:1, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4525504/2963)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

outbound ah sas:

```

```

outbound pcp sas:
Router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id slot status
210.210.2.1 210.210.1.2 QM_IDLE 1071 0 ACTIVE

```

Усі налаштування на роутері R2:

```

Router>en
Router#sh crypto ipsec sa

interface: GigabitEthernet0/2/0
Crypto map tag: CMAP, local addr 210.210.2.1

protected vrf: (none)
local ident (addr/mask/prot/port):
(192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
current_peer 210.210.1.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 210.210.2.1, remote crypto
endpt.:210.210.1.2
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/2/0
current outbound spi: 0x313B2B09(825961225)

inbound esp sas:
spi: 0x86E43B8B(2263104395)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2005, flow_id: FPGA:1, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4525504/587)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x313B2B09(825961225)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }

```

```

conn id: 2006, flow_id: FPGA:1, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4525504/587)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

```

```
outbound ah sas:
```

```

outbound pcp sas:
Router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id slot status
210.210.1.2 210.210.2.1 QM_IDLE 1024 0 ACTIVE

```

3.2 Висновки за розділом 3

Налаштували мережу, яка створюється з двох офісів, які мають по дві мережі з'єднані через роутер. Налаштування виконано двома способами за допомогою VPN.

Були обрані такі протоколи як Ospf, IPSec, GRE.

Обрані методи хешування та автетифікації.

У мережі 1 використовувались такі методи:

- encryption aes;
- authentication pre-share;
- group 5.

У мережі 2 використовувались такі методи:

- encr 3des;
- hash md5;
- authentication pre-share;
- group.

Схема була розроблена зібрана на симуляторі Cisco Packet Tracer на базі обладнання Cisco.

4 ПОРІВНЯННЯ ТА ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ МЕРЕЖ

4.1 Вплив VPN з'єднання на швидкість мережі

MTU (MaximumTransmissionUnit) – максимальний розмір блоку даних, який можна передати через інтерфейс.

Типовий розмір MTU для інтерфейсу 1500. IP-пакет розміром 1500 байт буде оброблено, а 1501 – відкинуто або фрагментовано.

Якщо фрагментацію пакетів заборонено, великі пакети відкидаються.

У прапорах IP-заголовка три біти використовуються під керуючі прапори. Тут слід зазначити, що прапор DF (don'tfragment –не фрагментувати) грає головну роль алгоритмі PMTUD: він повідомляє у тому, можна фрагментувати пакет чи ні. Біт 0 зарезервований. Його значення завжди дорівнює 0. Біт 1 це прапор DF (0 = дозволена фрагментація, 1 = заборонена фрагментація). Біт 2 – це прапор MF (0 = останній фрагмент, 1 = ще фрагменти). При використанні тунелювання стандартний розмір пакета збільшується за рахунок заголовків IPsec та GRE.

Тунель складається з чотирьох основних частин: мережевого заголовка для тунелю, заголовка тунелю, мережевого заголовка вихідного блоку протокольних даних (PDU) і данихкорисного навантаження вихідного PDU. PDU інкапсулюється з заголовками тунелю, після чого PDU входить у тунель, і так само заголовки тунелю видаляються, коли PDU залишає тунель (рис 4.1).

NEW IP header	Tunnel header	IP header	Date
------------------	------------------	--------------	------

Рисунок 4.1 – Фрейм тунелю

Тунельний мережевий заголовок – це вихідний PDU інкапсульовано в тунель, до якого додається новий мережевий заголовок. Цей заголовок містить

адреси джерела та призначення кінцевих точок тунелю. Заголовок тунельної мережі може складатися з заголовка одного рівня або кількох рівнів моделі OSI. Наприклад, мережевий заголовок тунелю для тунелю GRE (рис.4.2) це просто IP-заголовок, тоді як мережевий заголовок тунелю для тунелю L2TP – це одночасно IP-заголовок і UDP-заголовок.

Заголовок тунелю – це заголовок, специфічний для протоколу тунелювання, тому GRE, IPSec, L2TP і PPTP мають власний формат заголовка тунелю. Кінцеві точки тунелів можуть мати кілька тунелів між собою, і, серед іншого, заголовки тунелів дозволяють кінцевим точкам ідентифікувати трафік з того чи іншого тунелю.

NEW IP header	GRE	IP header	Date
------------------	-----	--------------	------

Рисунок 4.2 – Фрейм тунелю GRE

Де, IP header =20 байт, GRE=4 байт.

Тобто виходить $IP+IP+GRE=20+20+4=44$ байт.

$MTU=1500-44=1456$ байт.

В тунелі IPSec., вихідний пакет інкапсулюється в новий IP-пакет із заголовком тунелю IPSec. Тому що це тунель рівня 3, заголовок Ethernet рівня 2 не торкається, тому заголовок. Ethernet використовується як для вихідного, так і для нового IP-пакета тунелю (рис. 4.3).

IP header	AH header	ESP header	TCP header	Date	ESP Trail	ESP Auth data
--------------	--------------	---------------	---------------	------	--------------	------------------

Рисунок 4.3 – Фрейм IPSec

Де IPheader–20 байт.,

AHheader–8 байт,

ESPheader–8 байт,

TCPheader–20 байт,

ESPTrail–6 байт,

ESPAuthdata–4 байт.,

Отримаємо: $20+8+8+20+6+42+20=86$ байт

MTU=1500-86=1414 байт.

GRE + IPsec (транспортний режим) зображено на рисунку 4.4

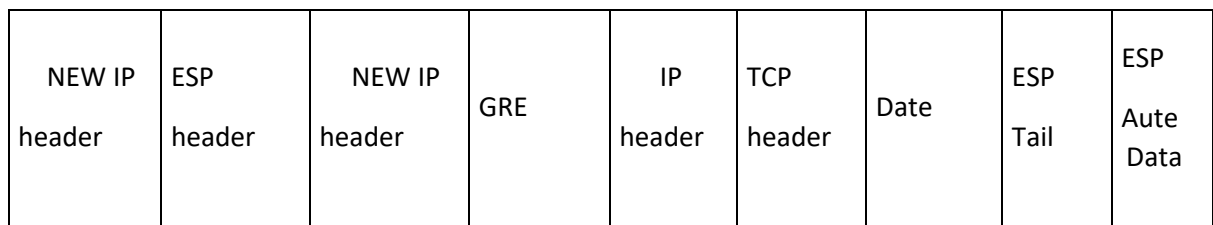


Рисунок 4.4 – Фрейм тунелюIPSec +GRE

Разом з GRE(4 байт)

$1500-86-4=1410$ байт.

GRE + IPsec (транспортний режим) 1440 байт 1400 байт GRE + IPsec
(тунельний режим) 1420 байт 1400 байт

Одночасне використання GRE та IPsec, треба встановити є встановити на GRE інтерфейсі оптимальне значення MTU та включається на тунельному інтерфейсі командою `tunnel path-mtu-discovery` та використовувати і команду `ipmtu 1400`. Щоб `ipmtu` забезпечуватиме простір для GRE + IPsec, у разі нижчих значень MTU по дорозі, IPMTU буде підкориговано динамічно. Значення 1400 рекомендовано, т.к. воно покриває більшість можливих комбінацій GRE+IPsec. Тому слід використовувати IP `tcp adjust-mss 1360` на тунельному інтерфейсі. Це дозволить маршрутизатору зменшити значення TCP MSS у TCP SYN Packet. Що дозволить двом кінцевим хостам генерувати досить малі пакети.

Тому перевіримо за допомогою протоколу ICMP за допомогою команди ping розроблені мережі.

Для першого випадку, коли в мережі був тільки протокол OSPFрозширений ping виглядав так (рис4.5).

```

Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router#ping
Protocol [ip]:
Target IP address: 192.168.2.2
Repeat count [5]:
Datagram size [100]: 2000
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 2000-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/9/19 ms

Router#ping
Protocol [ip]:
Target IP address: 192.168.2.2
Repeat count [5]:
Datagram size [100]: 1480
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1480-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/11 ms

```

Рисунок 4.5 –Розширений ping OSPF

Для другою випадку при протоколі IPSec+GRE (рис 4.6), та GRE (рис 4.7).

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```

Router#ping
Protocol [ip]:
Target IP address: 192.168.2.2
Repeat count [5]:
Datagram size [100]: 1450
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1450-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/9/19 ms

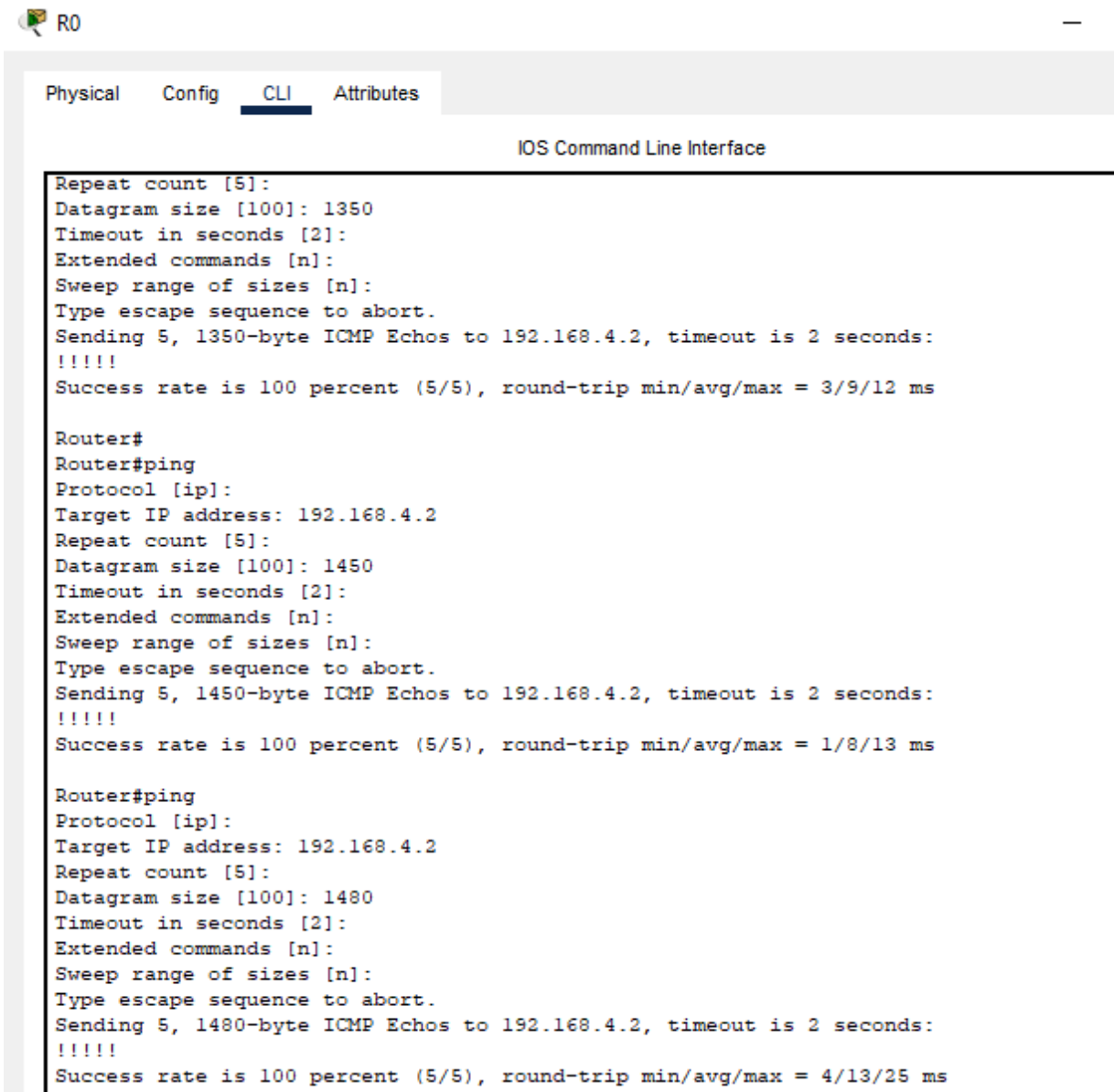
Router#
Router#ping
Protocol [ip]:
Target IP address: 192.168.2.2
Repeat count [5]:
Datagram size [100]: 1490
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1490-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/10/21 ms

Router#ping
Protocol [ip]:
Target IP address: 192.168.2.2
Repeat count [5]:
Datagram size [100]: 1400
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1400-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/9/12 ms

Router#

```

Рисунок 4.6 – Розширений ping IPSec+GRE



```

R0
Physical Config CLI Attributes
IOS Command Line Interface
Repeat count [5]:
Datagram size [100]: 1350
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1350-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/9/12 ms

Router#
Router#ping
Protocol [ip]:
Target IP address: 192.168.4.2
Repeat count [5]:
Datagram size [100]: 1450
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1450-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/13 ms

Router#ping
Protocol [ip]:
Target IP address: 192.168.4.2
Repeat count [5]:
Datagram size [100]: 1480
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1480-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/13/25 ms

```

Рисунок 4.7 – Розширений ping GRE

Тому, як можна побачити, при маленьких значеннях `Datagramsize` різниця між протоколами OSPF та GRE становить 01ms, також різниця IPsec + GRE ще на 0,01ms більша, це завдяки методам шифрування та тунелювання. При збільшенні `Datagramsize` вище 1450 швидкість падає в два рази, це виходить завдяки тому, що у фреймі не вистачає місця для протоколів VPN та його треба зменшувати. Наприклад `MTUdata` не повинна перевищувати 1400 згідно розрахунку. Ці дані було занесено у таблицю 4.1

Таблиця 4.1 –Розширений ping

Найменування протоколу	Datagram size	Час ms.
OSPF	100	7
OSPF	1300	9
OSPF	1400	9
OSPF	1500	10
OSPF	1510	12
OSPF	1550	11
OSPF	2000	14
GRE	100	8
GRE	1300	7
GRE	1400	7
GRE	1450	7
GRE	1500	7
GRE	1510	13
GRE	1550	12
GRE	2000	13
GRE+IPSec	100	9
GRE+IPSec	1300	9
GRE+IPSec	1400	9
GRE+IPSec	1450	9
GRE+IPSec	1500	10
GRE+IPSec	1510	11
GRE+IPSec	1550	11
GRE+IPSec	2000	16

Розробимо діаграми залежностей Datagram size / Час ms. (рис.4.8, рис.4.9, рис.4.10.).

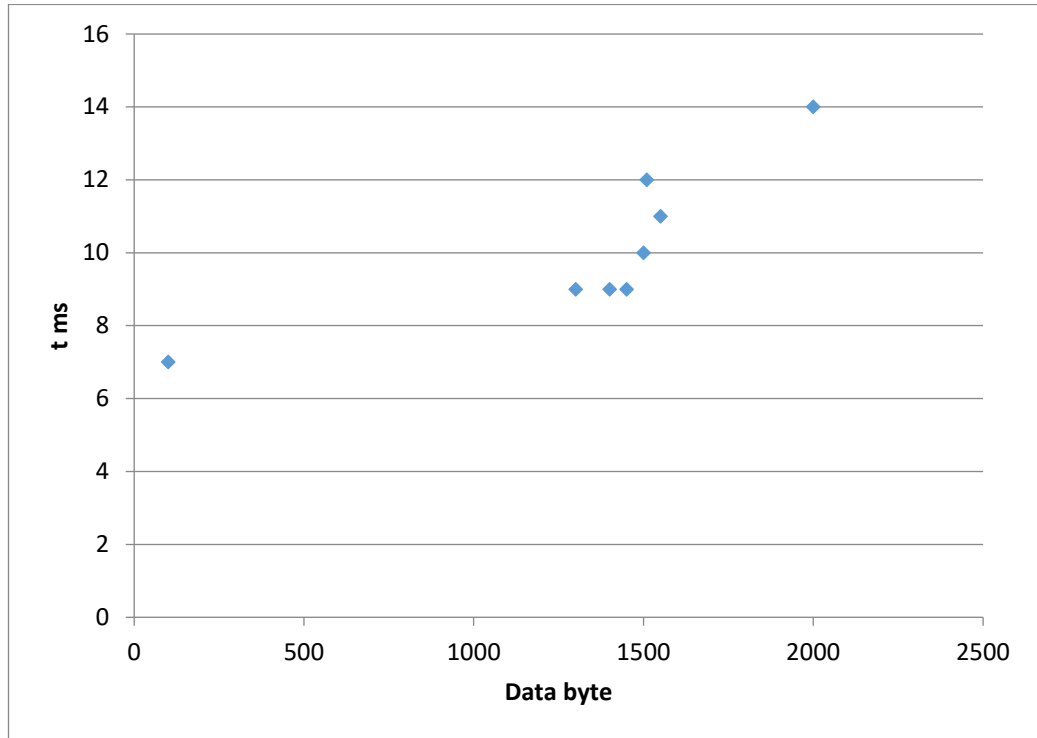


Рисунок 4.8–Діаграма OSPF

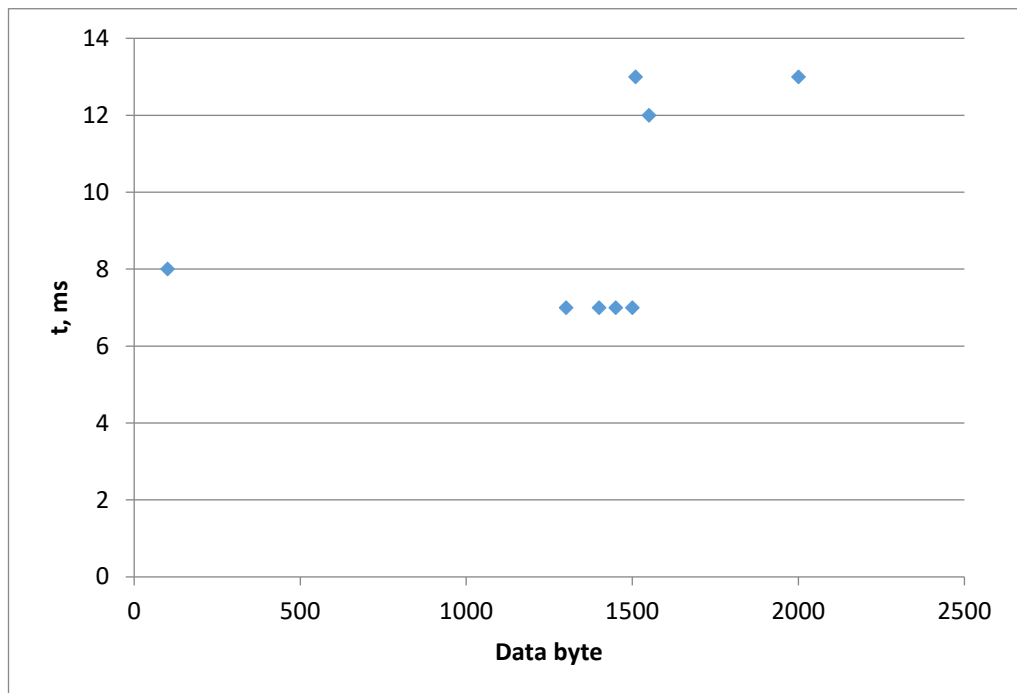


Рисунок 4.9 – Діаграма GRE

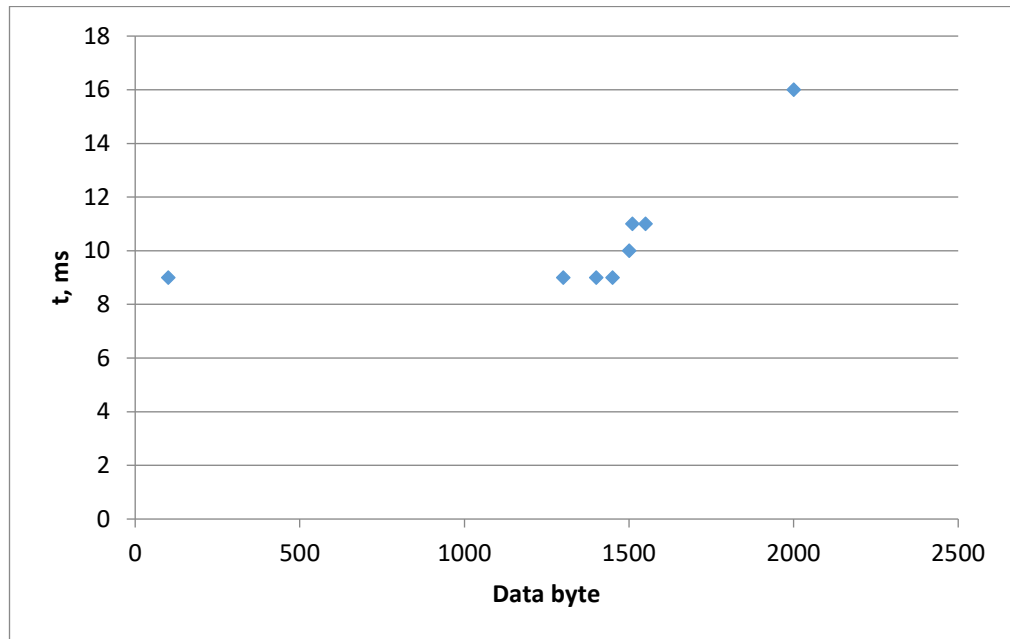


Рисунок 4.10 – Діаграма IPSec +GRE

4.2 Перевірка захисту мережі

Атаки, яких не буде при VPN, це такі атаки, як TCP-атаки. Протокол TCP використовується зловмисниками і як інструмент для організації атак (зазвичай - атак відмови в обслуговуванні), і як мета нападу - порушення TCP-сеансу програми

Атака підробкою TCP-сегменту полягає у генерації TCP-сегментів, всі атрибути яких мають значення, легітимні для деякого існуючого TCP-сеансу атакованого комп'ютера, тобто IP-адреси, номери TCP-портів джерела та приймача, а також порядкові номери із поточного діапазону вікна прийому. Приймаюча сторона не може відрізнити такі підроблені сегменти від справжніх і поміщає інформацію зловмисника в потік даних, а значить, зловмисник може досягти бажаного ефекту, наприклад, помістити неправдиву інформацію в базу даних, заразити вірус, що атакується, і т. п.

Атака скиданням TCP-з'єднання використовується для розриву TCP-з'єднань легальних користувачів. Для проведення атаки зловмисник повинен підробити заголовок TCP-сегменту. При надходженні TCP-сегмента зі встановленим прапором RST вузол повинен негайно завершити сеанс, до якого належить цей сегмент, і видалити всі дані, отримані під час сеансу. Розробники протоколу TCP ввели цей прапор обробки аварійних ситуацій. Наприклад, якщо в одному з вузлів під час TCP-сеансу відбувається збій, то після відновлення системи він може надіслати сегмент з цією ознакою, щоб повідомити вузол-співрозмовник про неможливість продовження сеансу. Скидання з'єднання використовується також деякими фаєрволами для припинення атаки.

Всі види атак на компоненти IPSec можна розділити на такі групи: атаки, що експлуатують кінцівку ресурсів системи (типовий приклад атаки "Відмова в обслуговуванні", Denial-of-service або DOS-атака), атаки, що використовують особливості та помилки конкретної реалізації IPSec та, нарешті, атаки, засновані на слабкості самих протоколів. AH та ESP.

Чисто криптографічні атаки можна не розглядати, тому що обидва протоколи визначають поняття, куди приховують всю криптографію. Якщо використовуваний криптоалгоритм стійок, а певний з ним трансформ не вносить додаткові слабкості (це не завжди так, тому правильніше розглядати стійкість усієї системи - Протокол-Трансформ-Алгоритм), то з цього боку все гаразд. Що лишається? Replay Attack -ssagenівелюється за рахунок використання Sequence Number (в одному єдиному випадку це не працює - при використанні ESP без аутентифікації та без AH). Далі порядок виконання дій (спочатку шифрування, потім аутентифікація) гарантує швидке відбраковування "поганих" пакетів (більше того, згідно з останніми дослідженнями у світі криптографії, саме такий порядок дій найбільш безпечний, зворотний порядок у деяких, правда дуже окремих випадках, може призвести до потенційних дірок у безпеці; на щастя, ні SSL, ні IKE, ні інші поширені протоколи з порядком дій "спочатку аутентифікувати, потім

зашифрувати", до цих окремих випадків неставляться, і, отже, цих дірок немає). Залишається Denial-Of-Service атака. Як відомо, це атака, від якої не існує повного захисту. Тим не менш, швидке відбраковування поганих пакетів і відсутність будь-якої зовнішньої реакції на них (згідно з RFC) дозволяють більш-менш добре справлятися із цією атакою. В принципі, більшості (якщо не всім) відомим мережевим атакам (sniffing, spoofing, hijacking і т.п.) AH і ESP при правильному їх застосуванні успішно протистоять. З IKE дещо складніше. Протокол дуже складний, важкий для аналізу. Крім того, через помилки (у формулі обчислення HASH_R) при його написанні і не зовсім вдалим рішенням (той самий HASH_R і HASH_I) він містить кілька потенційних "дір" (зокрема, в першій фазі не всі Payload у повідомленні аутентифікуються), втім, вони не дуже серйозні і ведуть, максимум, до відмови у встановленні з'єднання. Отата ктипа replay, spoofing, sniffing, hijacking IKE

Якоюсь мірою можна розглядати як слабкість IPsec те, що як єдине обов'язкового до реалізації криптоалгоритму у нинішніх специфікаціях

Отже, при правильній реалізації найбільш "небезпечною" атакою залишається Denial-Of-Service.

Потім перевіримо ці мережі згідно методів шифрування та автентифікації.

У мережі 1 використовувались такі методи:

- encryption aes;
- authentication pre-share;
- group 5.

У мережі 2 використовувались такі методи:

- encr 3des;
- hash md5;
- authentication pre-share;
- group.

Тобто виходить:

- encryption { 3des | aes };

- hash { | md5 | sha-1 };
- authentication { pre-share };
- group { 2 | 5 }.

3DES з трьома різними ключами має довжину ключа, що дорівнює 168 біт, але через атаки «зустріч посередині» ефективна криптостійкість становить лише 112 біт. У варіанті DES-EDE з $k_1 = k_3$ номінальний розмір ключа також становить 112 біт. Однак такий вибір ключів уразливий для певних атак на основі відкритих текстів, що зменшує ефективну довжину ключа до 80 біт. Для успішної атаки на 3DES потрібно близько $2^{32} \cdot 2^{32}$ біт відомого відкритого тексту, 2^{113} кроків, 2^{90} циклів DES-шифрування і 2^{88} біт пам'яті. На даний момент це непрактично, і, за оцінками НІСТ, алгоритм із вибором трьох різних ключів має залишитися надійним до 2030 років.

- розділіть дані на блоки;
- ключове розширення;
- додати круглий ключ;
- підміна/заміна байтів;
- посуне ряди;
- перемішайте стовпчики;
- знову додайте круглий ключ;
- повторює.

AES – цей алгоритм перетворює один 128-бітний блок в інший, використовуючи секретний ключ, який потрібен для такого перетворення. Для розшифровки отриманого 128-бітного блоку використовують друге перетворення з тим самим секретним ключем. AES – одна з найнадійніших систем у світі. Він набув широкого поширення у багатьох галузях, де потрібний надзвичайно високий рівень безпеки. Алгоритм шифрування AES

проходить через кілька раундів шифрування. Він може навіть пройти 9, 11 чи 13 раундів. Кожен раунд включає ті ж кроки, що і нижче:

Порівняння характеристик 3des та aes занесено у таблицю (табл. 4.2).

Таблиця 4.2 – Відмінності між шифруванням DES і AES

	DES	AES
Developed	1977	2000
Key Length	56 bits	128, 192, or 256 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block Size	64 bits	128 bits
Security	Proven inadequate	Considered secure

Алгоритм Diffie-Hellman Group може мати наступні значення:

- Diffie-Hellman Group 1 (768-bit);
- Diffie-Hellman Group 2 (1024-bit);
- Diffie-Hellman Group 5 (1536-bit);
- Diffie-Hellman Group 14 (2048-bit);
- Diffie-Hellman Group 15 (3072-bit).

Якщо швидкість для ініціалізації тунелю та повторного введення не викликає занепокоєння, ви можете використовувати вищу групу DH. Фактична швидкість ініціалізації та повторного введення залежить від низки факторів. Можливо, ви захочете спробувати одну з вищих груп DH і вирішити, чи є нижча продуктивність проблемою для вашої мережі. Якщо продуктивність є неприйнятною, перейдіть до нижчої групи. Тобто різниця

між Diffie-Hellman Group 2 (1024-bit) та Diffie-Hellman Group 5 (1536-bit) не дуже велика, але захист ефективніший на Group 5.

Md5 і sha-1 – це способи шифрування. Це способи обчислення хеш (хеш-функції). Вони використовуються не для того, щоб "зашифрувати" пароль. Вони використовуються для того, щоб не зберігати пароль взагалі.

Тому основна вимога до хеш-функції – мінімальна ймовірність колізій – знаходження іншого вхідного рядка, на якому хеш-функція видасть той самий результат. Ця ситуація мало ймовірна, проте - ймовірність колізій у sha-1 набагато менше, ніж у стародавньому md5. Тому використання sha-1 чи інших нових алгоритмів - кращий варіант.

Тому мережа 1 буде більш захищеною завдяки тому, що в ній використані більш нові алгоритми.

4.3 Вхідні та вихідні дані

Вхідними даними є кількість та тип комп'ютерів, роутерів, вимоги швидкості та захисту

Вихідними даними є конфігурація роутерів та іншого мережевого обладнання а також налаштування VPN.

4.5 Висновки за розділом 4

У цьому розділі було проведено аналіз впливу VPN з'єднання на швидкість та захист мережі. Виявилось, що для того, щоб підвищити швидкість з'єднання для протоколів трібно задавати MTU приблизно 1400 байт.

З точки зору безпеки, мережа VPN захищає від таких видів атак, як TCP-атаки. Методи безпеки, які були використані у першому способі налаштування VPN мережі були більш стійкі до мережевих атак, завдяки застосуванню більш нових засобів шифрування таких як aes , хешування sha- 1, та алгоритму group 5.

ВИСНОВКИ

В процесі виконання кваліфікаційної роботи магістра було розроблено та досліджено мережу на базі симулятора Cisco Packet Tracer.

З точки зору безпеки, мережа стала більш захищеною завдяки протоколам VPN та методам аунтифікації шифрування та хешування.

У першому розділі були розглянуті основні поняття. Проведено огляд методів та засобів які виконують функції побудливи та захисту мережі.

У другому розділі були обрано налаштування мережі, протоколів захисту за допомогою методів ACL, IPSec, GRE. Обрано технологію організації VPN, розробка структурної схеми.

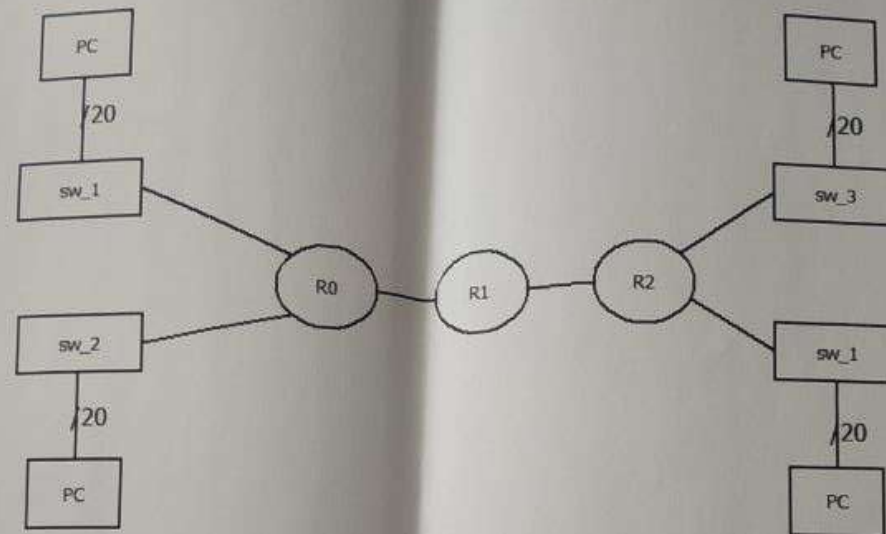
У третьому розділі було зроблено налаштування мережі, та створення протоколів захисту.

У четвертому розділі було приведено дослідження наступних мереж, та зроблені висновки щодо методів побудови захищених комп'ютерних мереж.

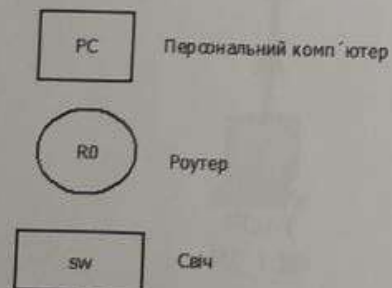
ПЕРЕЛІК ПОСИЛАНЬ

1. Marschall, M. Chef Infrastructure Automation Cookbook. Second Edition. Birmingham: Packt Publishing, 2015. 258 p.
2. Sebenik, C. Hatch, T. Salt Essentials: Getting Started with Automation at Scale. Sebastopol: O'Reilly Media Inc., 2015. 163 p.
3. Киричек Г.Г., Щетінін М.О. Конфігурація серверів з використанням Ansible. International scientific conference «Modern scientific research: achievements, innovations and development prospects», Riga, Latvia, October 1-2, 2021. P.15-17.
4. Rhett, J. Learning Puppet 4: A Guide to Configuration Management and Automation. Sebastopol: O'Reilly Media Inc., 2016. 550 p.
5. Tiahunova, M., Tronkina, O., Kirichek, G., Skrupsky, S. (2021). The neural network for emotions recognition under special conditions. In CEUR Workshop Proceedings 2864 (pp. 121-134).
6. Rudkovskyi O., Kirichek G. Interaction support system of network applications, Proceedings of the 3rd Workshop for Young Scientists in Computer Science & Software Engineering, CS&SE@SW 2020, Vol-2832, Kryvyi Rih, Ukraine, November 27, 2020. P.11-23.
7. Groeneveld, F., Mesbah, A., Van Deursen, A. (2010). Automatic invariant detection in dynamic web applications. Technical Report Series TUD-SERG-2010-037
8. Tiahunova, M., Kyrychek, H., Bohatyrova, T., Moshynets, D. (2021). System and method of automatic collection of objects in the room. In CEUR Workshop Proceedings 3077 (pp. 174-186).
9. Киричек Г.Г., Гаркуша В.Ю. Віртуалізація хостів на основі Proxmox VE в умовах надлишкового використання ресурсів. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки, 32 (71), №1, 2021, С.78-84.

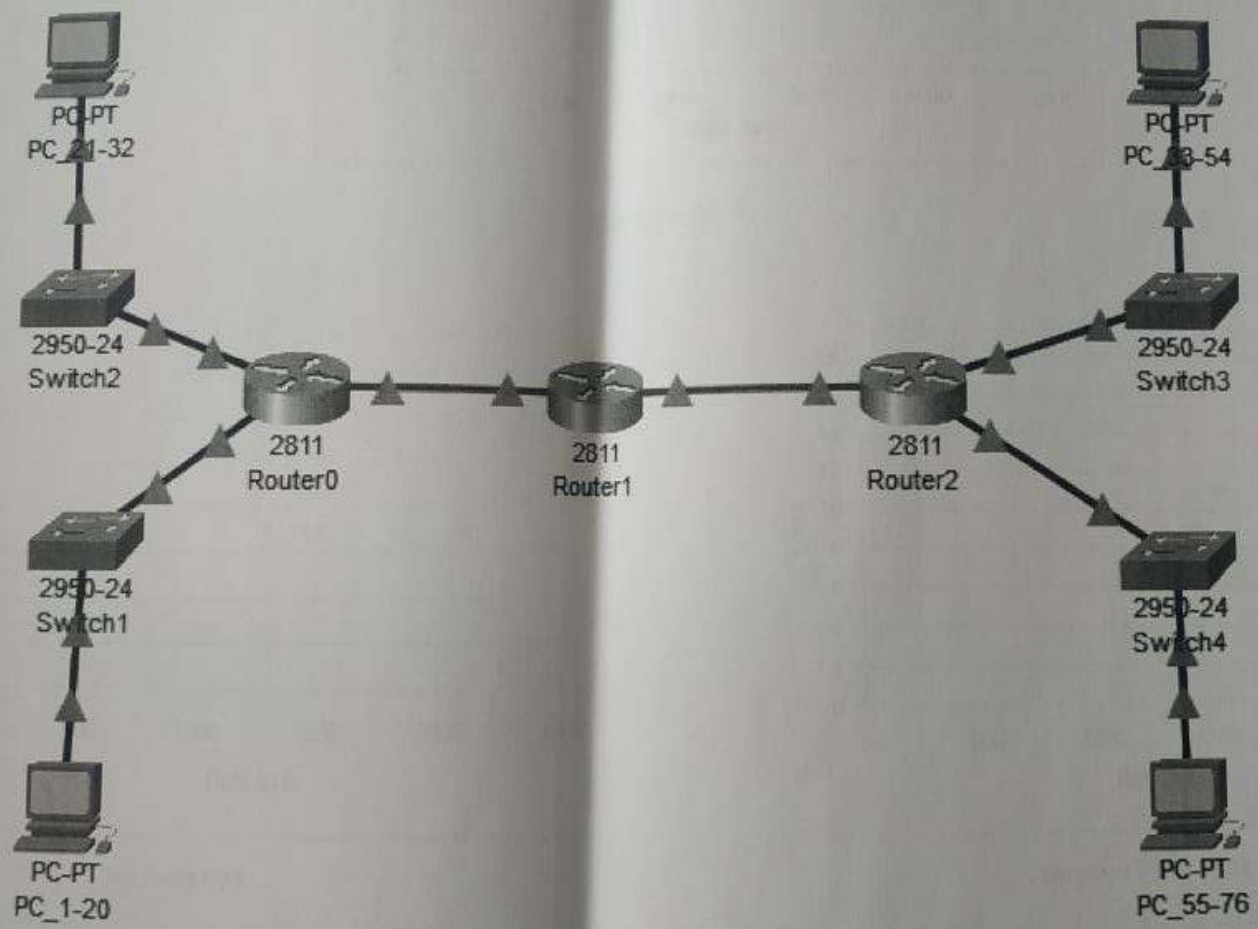
10. Виговський, О. С. Програмні продукти для моделювання мереж. Збірник матеріалів XIII Міжнародної науково-технічної конференції студентства та молоді, 2021. С. 23-25.
11. Романов, О. І., Нестеренко, М. М., Гордашник, Є. С. Аналіз функціональних особливостей побудови IP-мереж на базі Softswitch. Збірник наукових праць [Військового інституту телекомунікацій та інформатизації], 2015. Вип.1. С. 69-80.
12. Ozerchuk, I. Формування стійкого каналу передачі даних у мережі Інтернет. Computer-integrated technologies: education, science, production, 2021, Vol. 43. P. 212-217.
13. Галелюка І. Б. Моделювання бездротових сенсорних мереж. Комп'ютерні засоби, мережі та системи, 2015. Вип.14. С. 141-150.
14. Горященко, К. Л., Доротюк, М. Д. Огляд систем імітаційного моделювання телекомунікаційних мереж. Вісник Хмельницького національного університету. Технічні науки, 2014, Вип. 5. С. 115-118.
15. Шокотько, Л. М. Методи та засоби навчання проектування та обслуговування комп'ютерних мереж. Новітні комп'ютерні технології, 2016. Том XIV. С. 93.
16. Уривський, Л. О., Мошинська, А. В., Осипчук, С. О. Імітаційне моделювання систем і процесів у телекомунікаціях, Київ, 2022.
17. Website Wikipedia [Electronic resource]. – The Free Encyclopedia. – Access mode: https://uk.wikipedia.org/wiki/Комп%27ютерна_мережа#
18. ISO/IEC 17799:2005 / Information technology – Security techniques – Code of practice for information security management [Електронний ресурс] Режим доступу: <https://www.iso.org/ru/standard/39612.html>
19. WatchGuard [Електронний ресурс] Режим доступу: https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/bovpn/manual/diffie_hellman_c.html
20. Website Wikipedia [Electronic resource]. – Access mode: https://ru.wikipedia.org/wiki/Triple_DES



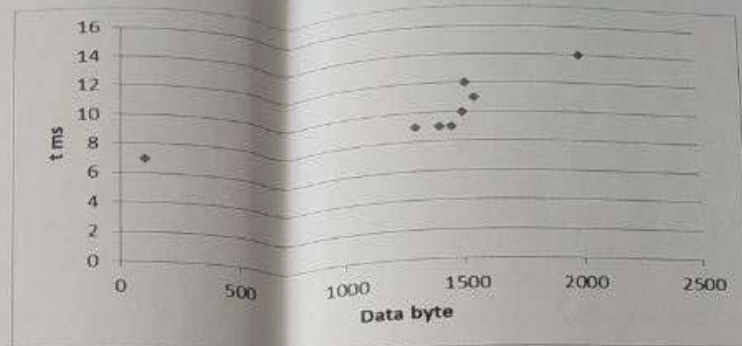
Условні позначки



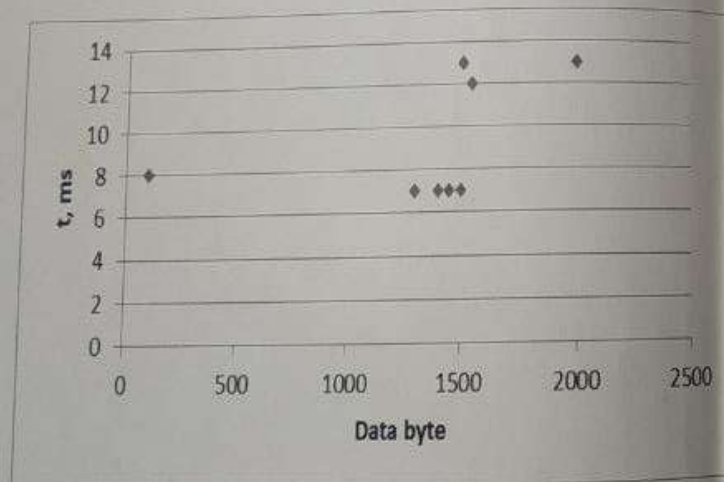
13. 02070849. 00019ПЛ1					
Зм.	Арх.	№ докум.	Підпис	Дата	
Розроб.	Костюк В.Г.				
Перевір.	Киричен Г.В.				
Реценз.	Семиніч С.С.				
Н. Контр.	Шебова Р.В.				
Затверд.					
Дослідження та реалізація методів створення захищених комп'ютерних мереж на базі CISCO					Лит.
					Арх.
					Актуальн.
					1
					№1
					НУ ЗП КНТ-5-511м



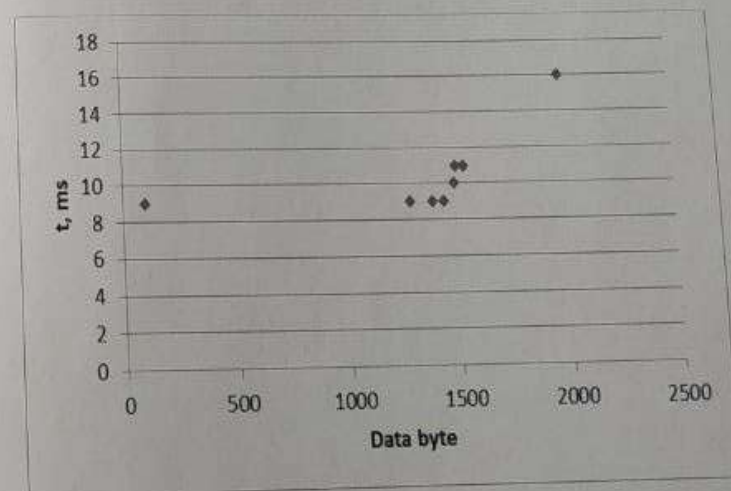
						13. 02070849: 00019ПЛТ2		
Змі.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Костюк В.Г.	Костюк В.Г.		Дослідження та реалізація методів створення захищених комп'ютерних мереж на базі CISCO	Літ.	Арк.	Акредит.
Перевір.		Коричук Г.В.	Коричук Г.В.				1	
Реценз.		Самодієв С.С.	Самодієв С.С.			НУ ЗП КНТЗ-511М		
Н. Компр.		Шевбак Р.В.	Шевбак Р.В.					
Затверд.		Губаренко Р.К.	Губаренко Р.К.					
					№2			



Діаграма OSPF



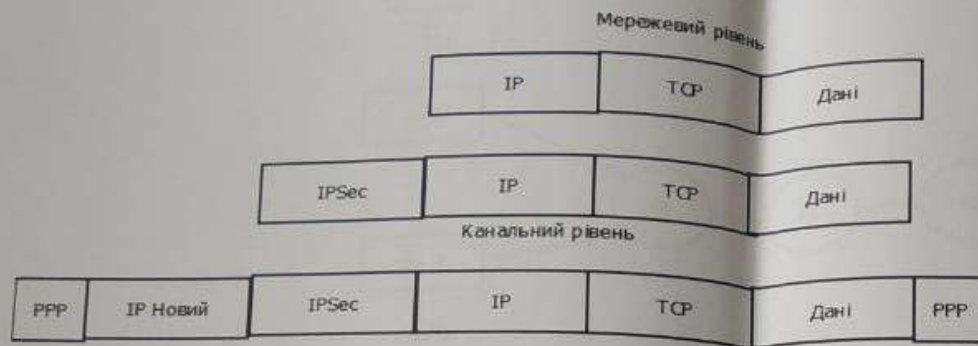
Діаграма GRE



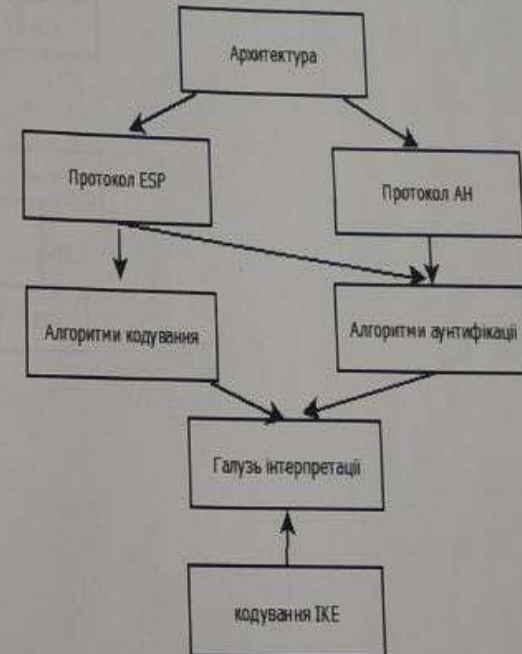
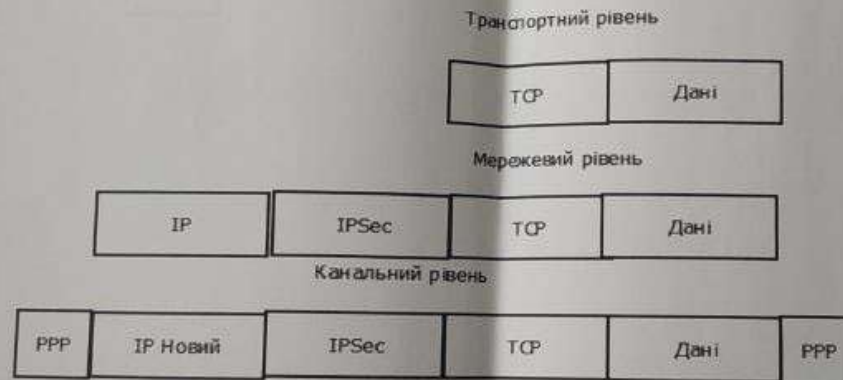
Діаграма IPSec + GRE

					13. 02070849 00019ПТЗ			
Зм.	Арх.	№ докум.	Підпис	Дата	Дослідження та реалізація методів створення захищених каналів ютерних мереж на базі CISCO	Лист	Арх.	Акц.
Розроб.		Костюк В.Г.	<i>[Signature]</i>			1		
Перевір.		Киричук Г.В.	<i>[Signature]</i>					
Реценз.		Самойлик С.С.	<i>[Signature]</i>					
Н. Конкр.		Шефак Р.В.	<i>[Signature]</i>					
Затверд.		Губаренко Г.П.	<i>[Signature]</i>		№3	НУ ЗП КНТЗ-511м		

Інкапсуляція IPSec для тунельного режиму



Інкапсуляція IPSec для транспортного режиму



					13. 02070849. 00019ПД4		
Зм.	Арх.	№ докум.	Підпис	Дата	Дослідження та реалізація методів створення захищених комп'ютерних мереж на базі CISCO		
Розроб.	Костик В.Г.						
Перевір.	Коричен Г.В.						
Реценз.	Самойлен С.С.						
Н. Кантр	Шевбак Р.В.						
Затверд.	Мухометов Г.К.				№4		
					Літ.	Арх.	Акція
					1		
					НУ ЗП КНТЗ-511м		