

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА
до випускної кваліфікаційної роботи бакалавра
на тему: «Проект захищеної інформаційно-
комунікаційної мережі з використанням технологій
VPN»

Виконав студент 4-го курсу групи КБ-19-1
спеціальності 125 «Кібербезпека»


Михайло ПЕКАРСВ

Керівник доцент кафедри КІ та КБ, к. пед.н


Олена ГОЛОВНЯ

Рецензент доцент кафедри КІ та КБ, к.т.н, доцент


Юрій РОССІНСЬКИЙ

м. Житомир – 2023 рік

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

Факультет інформаційно-комп'ютерних технологій

Кафедра комп'ютерної інженерії та кібербезпеки

Освітній рівень бакалавр

Спеціальність 125 «Кібербезпека»

ЗАТВЕРДЖУЮ

**Завідувач кафедри комп'ютерної інженерії
та кібербезпеки**



А.А. Єфіменко

“ 1 ” 03 20 23 року

ЗАВДАННЯ

НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Студент: Пекарєв Михайло Дмитрович

Тема роботи: «Проект захищеної інформаційно-комунікаційної мережі з використанням технологій VPN»

затверджена Наказом університету від 1 березня 2023 р. № 99/с

Термін здачі студентом закінченої роботи 10 червня 2023 р.

Вихідні дані до проекту (роботи):

- Топологія мережі.
- Налаштований GetVPN.
- Протоколи маршрутизації EIGRP, BGP.
- Протокол GDOI.

Обладнання та програмне забезпечення:

- 1. GNS3 – програмне забезпечення для моделювання та налаштування мереж.**
- 2. C7200 – образ використаних у мережі маршрутизаторів**

5. Консультанти розділів проєкту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ 1	Завідувач кафедри комп'ютерної інженерії та кібербезпеки, А. А. Єфіменко		

6. Дата видачі завдання 01 березня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	01.03.2023 р.	
2	Аналіз літературних джерел	05.03.2023 р.	
3	Аналіз об'єкта дослідження	16.03.2023 р.	
4	Постановка задачі дослідження	19.03.2023 р.	
5	Розробка структурної моделі	25.03.2023 р.	
6	Розрахунок параметрів адресації	05.04.2023 р.	
7	Вибір технології для реалізації	13.04.2023 р.	
8	Розробка захищеної КМ	23.05.2023 р.	
9	Налаштування мережі	27.05.2023 р.	
10	Налагодження GetVPN	03.05.2023 р.	
11	Оформлення пояснювальної записки	10.06.2023 р.	
12	Оформлення презентації	15.06.2023 р.	
	Захист	Згідно розкладу	

Студент

Керівник




М. Д. Пекарєв

О. С. Головня

АНОТАЦІЯ

Кваліфікаційну роботу присвячено створенню проєкту захищеної інформаційно-комунікаційної мережі з використанням технологій GetVPN. Пояснювальна записка до кваліфікаційної роботи складається з переліку умовних позначень, вступу, трьох розділів, висновків, списку використаної літератури та додатку.

Основний текст роботи викладено на 41 сторінках.

Пояснювальна записка має 13 сторінок додатків. Список використаних джерел містить 15 найменувань і займає 2 сторінки. В роботі наведено 20 рисунків.

В першому розділі коротко розглянуто теоретичні аспекти використання технологій VPN, аналоги технологій та обрано, яку буде використано.

У другому розділі проведено проєктування захищеної інформаційно-комунікаційної мережі з використанням обраної технології VPN. Були визначені моделі та схеми адресації, а також здійснено вибір обладнання та програмного забезпечення, необхідних для реалізації проєкту.

У третьому розділі проведено налаштування, аналіз, тестування проєкту. Було налаштовано обладнання та програмне забезпечення. Завдяки цьому етапу перевірено правильність налаштування та ефективність розробленої захищеної мережі.

Висновки містять результати виконаної роботи.

У додатку наведено лістинг налагодження пристроїв мережі.

Ключові слова: GetVPN, WireGuard, WebVPN, L2/L3 MPLS VPN, ISAKMP, GDOI.

КІК.КР.Б – 125 – 12 – ПЗ

Зм.	Арк.	№ докум.	Підпис	Дата	Проект захищеної інформаційно-комунікаційної мережі з використанням технологій VPN	Літ.	Арк.	Аркуші
Розроб.		Пекарев М. Д.		20.06.23				
Керівник		Головня О. С.		20.06.23			4	57
Реценз.		Росінський Ю. М.		20.06.23		ФІКТ, гр. КБ-19-1		
Н. Контр.								
Затверд.		Єфіменко А. А.		20.06.23				

ANNOTATION

The qualification work is devoted to the creation of a project of a secure information and communication network using GetVPN technologies. The explanatory note to the qualification project consists of a list of notations and abbreviations, an introduction, three sections, conclusions, a list of references and an appendix.

The main text is outlined on 41 pages of printed text.

The explanatory note has 13 pages of annexes. The list of used sources contains 15 names and occupies 2 pages. The work contains 20 images.

In the first section, the theoretical aspects of using VPN technologies, analogs of technologies and the choice of which one will be used were briefly considered.

In the second section, the design of a protected information and communication network using the selected VPN technology was carried out. Addressing models and schemes were determined, as well as the selection of equipment and software necessary for the implementation of the project.

In the third section, the setup and testing analysis of the project was carried out. Hardware and software have been configured. This stage intends to verify the correctness of the configuration and the effectiveness of the developed protected network.

The conclusions contain the results of the work performed.

The appendix provides a listing of debugging network devices.

Keywords: GetVPN, WireGuard, WebVPN, L2/L3 MPLS VPN, ISAKMP, GDOI.

		Пекарев М. Д.			КИК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	7
ВСТУП	8
РОЗДІЛ 1. Теоретичні аспекти створення захищеної інформаційно-комунікаційної мережі з використанням технологій VPN	9
1.1 Загальні відомості про VPN технології.....	9
1.2 Огляд різних варіантів побудови VPN	12
1.2.1 Web VPN.....	12
1.2.2 Get VPN.....	14
1.2.3 WireGuard	15
1.2.4 L2/L3 MPLS VPN.....	17
1.2.5 Порівняння технологій VPN.....	19
1.3 Вразливості та недоліки GetVPN.....	21
РОЗДІЛ 2. Проектування захищеної інформаційно-комунікаційної мережі з використанням GetVPN	24
2.1 Моделі та схеми адресації.....	24
2.2 Вибір серверної платформи та операційної системи.....	26
2.3. Топологія та схема мережі	29
Висновки до другого розділу	30
РОЗДІЛ 3. Налаштування та тестування проєкту	31
3.1 Налаштування обладнання та програмного забезпечення	31
3.2 Тестування та оцінювання результатів	34
Висновки до третього розділу.....	40
ВИСНОВКИ	41
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	42
ДОДАТКИ	44
Додаток А.....	45

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

GetVPN – Group Encrypted Transport VPN

MPLS – multiprotocol label switching

ISAKMP – Internet Security Association and Key Management Protocol

GDOI – Group Domain of Interpretation

VPN – virtual private network

SA – Security Association

GKM – Group Key Management

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

В сучасному світі не рідкістю є великі компанії, офіси яких знаходяться на значній відстані одне від одного. Компаніям необхідне швидке та захищене з'єднання до кожного з них.

Прокладати до всіх офісів свої власні дроти не є логічним та вигідним з економічної точки зору, набагато легше використати потужності, які вже існують, наприклад потужності провайдерів. Але як забезпечити захищене з'єднання для клієнта, щоб ніхто не мав доступу до його пакетів, і так само, як зробити це з'єднання безпечним для провайдера, щоб жоден клієнт не міг зайти в обладнання провайдера, щоб його присутність була взагалі непомітною?

Метою кваліфікаційної роботи є розробка проєкту захищеної інформаційно-комунікаційної мережі з використанням технології GetVPN.

Мета реалізується шляхом вирішення наступних **завдань**:

- Дослідження принципів, моделей та технологій побудови комп'ютерних мереж.
- Проєктування глобальної комп'ютерної мережі організації.
- Налагодження мережі та тестування її функціонування..

Об'єктом дослідження є методи та засоби з'єднання віддалених частин мережі на основі технологій VPN.

Предметом дослідження є процес розробки проєкту захищеної інформаційно-комунікаційної мережі з використанням технології GetVPN.

РОЗДІЛ 1. Теоретичні аспекти створення захищеної інформаційно-комунікаційної мережі з використанням технологій VPN

1.1 Загальні відомості про технології VPN

Віртуальна приватна мережа (VPN) - це технологія, яка дозволяє створювати безпечне з'єднання між двома або більше мережами через відкриту мережу, таку як Інтернет. Віртуальна приватна мережа забезпечує захист інформації, що передається по мережі, шляхом шифрування даних та застосування механізмів автентифікації та авторизації.

Технологія VPN дозволяє гарантувати безпеку під час передачі даних між віддаленими мережами, зокрема, віддаленими користувачами та офісами, які використовують Інтернет. За допомогою VPN, віддалений користувач може підключатися до мережі офісу через захищене з'єднання, що дозволяє йому отримувати доступ до ресурсів мережі офісу, якщо він має право на це.

Є два основні напрямки використання VPN: Site-to-site VPN та site-to-point VPN - це дві різні технології VPN, які використовуються для створення безпечних і захищених з'єднань між комп'ютерами або локальними мережами віддалених географічно.

Site-to-site VPN (також відомий як LAN-to-LAN VPN) - це технологія, яка дозволяє з'єднувати дві або більше локальних мереж, що розташовані в різних фізичних місцях, в єдину безпечну мережу. Це забезпечує спільний доступ до ресурсів та обмін даними між всіма віддаленими мережами. Ця технологія зазвичай використовується компаніями з кількома офісами або філіями, щоб гарантувати безпечний обмін даними між цими мережами.

Site-to-point VPN (також відомий як remote access VPN) - це технологія, яка дозволяє віддаленим користувачам підключатися до локальної мережі (точки), щоб отримати доступ до ресурсів, які зазвичай недоступні з публічного Інтернету. Це гарантує безпечний доступ до ресурсів компанії, що знаходяться в її локальній мережі,

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

з будь-якої точки світу. Ця технологія зазвичай використовується для підключення віддалених працівників, або для підключення мобільних пристроїв до локальної мережі. [1]

Основний принцип роботи обох технологій полягає в тому, що вони створюють безпечні тунелі через потенційно небезпечні зони, які забезпечують захист протоколів, які використовуються для передачі даних між віддаленими комп'ютерами або мережами. Тунель - це зашифрований канал, через який проходять дані між двома кінцевими точками мережі. Це забезпечує конфіденційність та захист даних, що передаються по мережі.

Site-to-site VPN і site-to-point VPN можуть використовувати різні протоколи, такі як IPsec, SSL / TLS, PPTP, L2TP та інші, для створення безпечного тунелю. Ці протоколи забезпечують аутентифікацію, шифрування та цілісність даних, що передаються через мережу VPN.

Site-to-site VPN має наступні переваги.

- Забезпечує спільний доступ до ресурсів між декількома локальними мережами.
- Забезпечує захист всієї мережі.
- Дозволяє економити кошти, оскільки не потрібно встановлювати окремі з'єднання з кожною локальною мережею.

Водночас, Site-to-site VPN, має й недоліки, зокрема наступні.

- Складність конфігурування.
- Вимагає високої пропускної здатності для передачі даних між віддаленими мережами.
- Вимагає спеціального обладнання та програмного забезпечення.

Тим часом, Site-to-point VPN має такі переваги.

- Дозволяє віддаленим користувачам зв'язуватися з локальною мережею з будь-якої точки світу.
- Гарантує безпеку та приватність з'єднання.
- Легко налаштовується та використовується.

Серед недоліків Site-to-point VPN зазначимо наступні.

- Обмежена пропускна здатність зв'язку, оскільки вся передача даних відбувається через одне з'єднання.
- Дорожче, коли потрібно підключити більше одного користувача.
- Залежить від швидкості та якості Інтернет-з'єднання користувача.

Загалом, якщо потрібно гарантувати безпечний доступ до ресурсів вашої компанії з будь-якої точки світу, site-to-point VPN може бути оптимальним варіантом. Якщо ж необхідно з'єднати кілька локальних мереж між собою, щоб обмінюватися ресурсами та даними між ними, то site-to-site VPN може бути кращим вибором. Проте, важливо врахувати, що для обох технологій потрібні відповідні налаштування та гарантування безпеки.

Шифрування даних є ключовим аспектом VPN технології. Коли дані передаються через відкриту мережу, таку як Інтернет, вони можуть бути перехоплені та прочитані зловмисниками. Шифрування даних в VPN дозволяє захистити дані від таких атак, оскільки вони будуть зашифровані та не зможуть бути прочитані без правильного ключа.



Рис. 1.1 – Принцип роботи VPN в мережі

Для того, щоб використовувати VPN, користувач повинен мати програмне забезпечення для підключення до віртуальної приватної мережі. Крім того, VPN може бути налаштована на різних рівнях, включаючи маршрутизатори, фаєрволи та інші мережеві пристрої.

Однією із головних переваг VPN є гарантування безпеки при передачі даних через відкриту мережу, що особливо важливо для підприємств та організацій, які передають чутливу інформацію по мережі Інтернет. Крім того, VPN може допомогти уникнути блокування контенту, яке здійснюють деякі країни або провайдери Інтернету, дозволяючи користувачам отримувати доступ до заблокованих ресурсів.

Однак, слід зазначити, що VPN не є повністю надійним та безпечним. Наприклад, якщо користувач використовує слабкий пароль для доступу до віртуальної приватної мережі, то його облікові дані можуть бути скомпроментовані. Крім того, деякі провайдери VPN можуть збирати та зберігати інформацію про активність користувачів, що може становити загрозу для приватності.

Також, слід зазначити, що використання VPN може сповільнити швидкість передачі даних через мережу, оскільки процес шифрування та дешифрування даних потребує додаткових ресурсів.

Загалом, VPN є потужним інструментом для гарантування безпеки та приватності при передачі даних через відкриту мережу, але використовувати його слід з обережністю та враховувати його обмеження та ризики.

1.2 Огляд різних варіантів побудови VPN

1.2.1 Web VPN

Web VPN - це технологія, що дозволяє користувачам підключатися до захищеної мережі через веб-браузер. Користувачі вводять адресу VPN-сервера у свій веб-браузер і вводять свої облікові дані. Захищене з'єднання налагоджується між клієнтом та VPN-сервером.

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

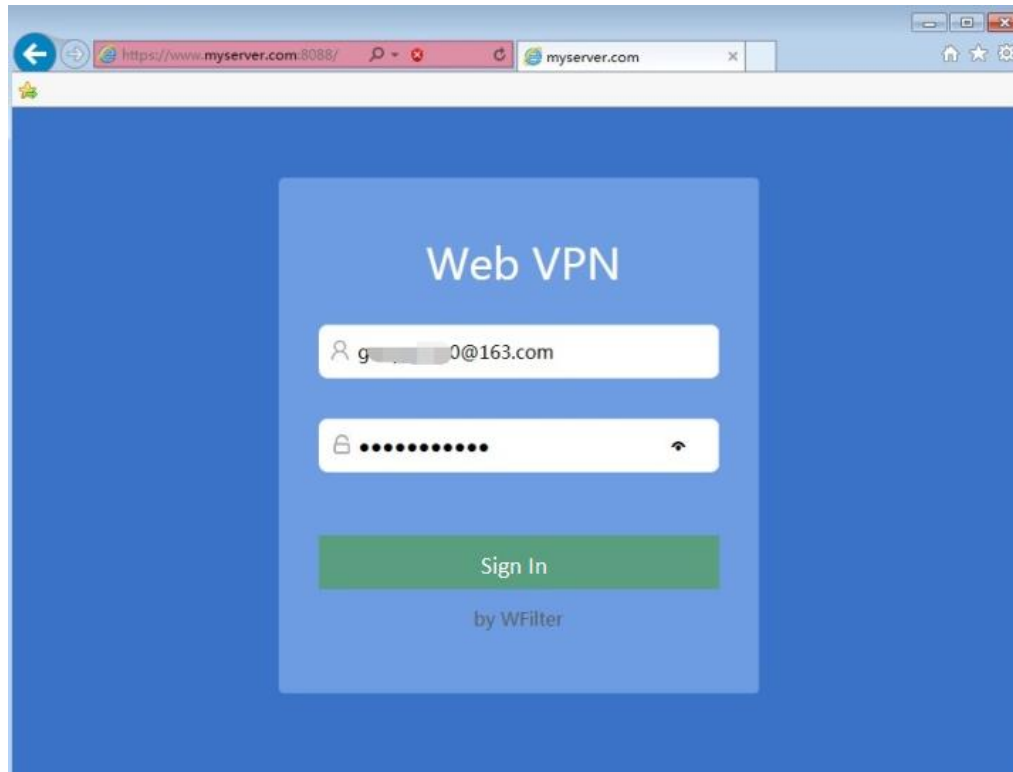


Рис.1.2 – Інтерфейс WebVPN

Однією з переваг Web VPN є простота його використання, оскільки він не вимагає встановлення спеціального програмного забезпечення на пристрої користувача. Іншою перевагою Web VPN є можливість віддаленого доступу до інформації з будь-якого місця, де є Інтернет. Крім того, використання Web VPN дозволяє уникнути необхідності встановлювати та налаштовувати VPN-клієнти на кожному пристрої користувача.

Однак, Web VPN має деякі недоліки. Одним з них є те, що обмеження більшості браузерів може призвести до того, що не всі типи додатків можна запускати через Web VPN. Крім того, веб-трафік може бути обмежений, якщо мережа забороняє використання певних портів.

Web VPN може бути менш надійним у порівнянні з іншими типами VPN, такими як IPsec або SSL VPN, оскільки він використовує браузер як місце підключення. Це може створити деякі вразливості, які можуть бути використані зловмисниками для проникнення в мережу. Крім того, Web VPN не гарантує

транспортну безпеку, тому він може бути менш ефективним для передачі конфіденційної інформації, такої як фінансові дані або медичні записи.

Також важливо зазначити, що використання Web VPN може знизити швидкість інтернет-з'єднання, оскільки весь трафік потрібно переслати через VPN-сервер. Це може бути особливо помітним для користувачів з повільним інтернет-з'єднанням або з великою кількістю трафіку.[2]

1.2.2 Get VPN

Group Encrypted Transport VPN (GetVPN) - це технологія VPN, яка дозволяє створювати захищені тунелі між вузлами мережі з використанням IPsec та протоколу тунелювання мережевих пакетів (GRE). Особливістю GetVPN є те, що вона дозволяє створювати глобальну політику безпеки для всіх тунелів у мережі, що значно спрощує керування ними та їх підтримку. GetVPN дозволяє гарантувати безпеку на рівні мережі та застосунків, шифруючи дані, які передаються через мережу.

Це дозволяє зменшити навантаження на мережевий протокол та збільшити продуктивність мережі.

Cisco GET VPN

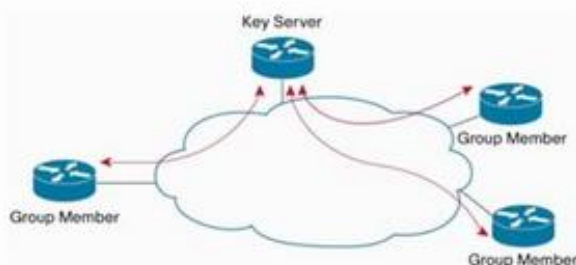


Рис. 1.3 – Принцип роботи GetVPN

GetVPN має кілька переваг порівняно з іншими технологіями VPN. По-перше, вона дозволяє гарантувати безпеку на рівні мережі та застосунків, що робить її особливо корисною для підприємств та організацій, які потребують максимального рівня безпеки своїх даних. По-друге, GetVPN дозволяє створювати глобальну політику безпеки для всіх тунелів у мережі, що спрощує керування та підтримку.

Крім цього, GetVPN забезпечує захист від різних видів атак, таких як атаки "Man-in-the-middle" та "Replay", що робить її однією з найбезпечніших технологій VPN. Крім того, GetVPN дозволяє підключати до мережі різні типи пристроїв, такі як роутери, комутатори, сервери та робочі станції, що робить її дуже гнучкою.

Недоліком GetVPN є те, що вона вимагає більш складного налаштування, ніж Web VPN. Крім того, для її використання необхідно мати певні знання з мережної безпеки та мережного дизайну.

Хоча GetVPN має свої недоліки, її переваги значно переважають над недоліками. За допомогою GetVPN підприємства та організації можуть забезпечити максимальний рівень безпеки своїх даних, збільшити продуктивність мережі та спростити керування тунелями у мережі.[3]

1.2.3 WireGuard

WireGuard є відносно новою технологією VPN, яка швидко набирає популярність в останні роки. Вона була розроблена з метою забезпечення швидкого та безпечного з'єднання між мережами, використовуючи сучасні шифрувальні алгоритми.



Рис. 1.4 – Логотип WireGuard

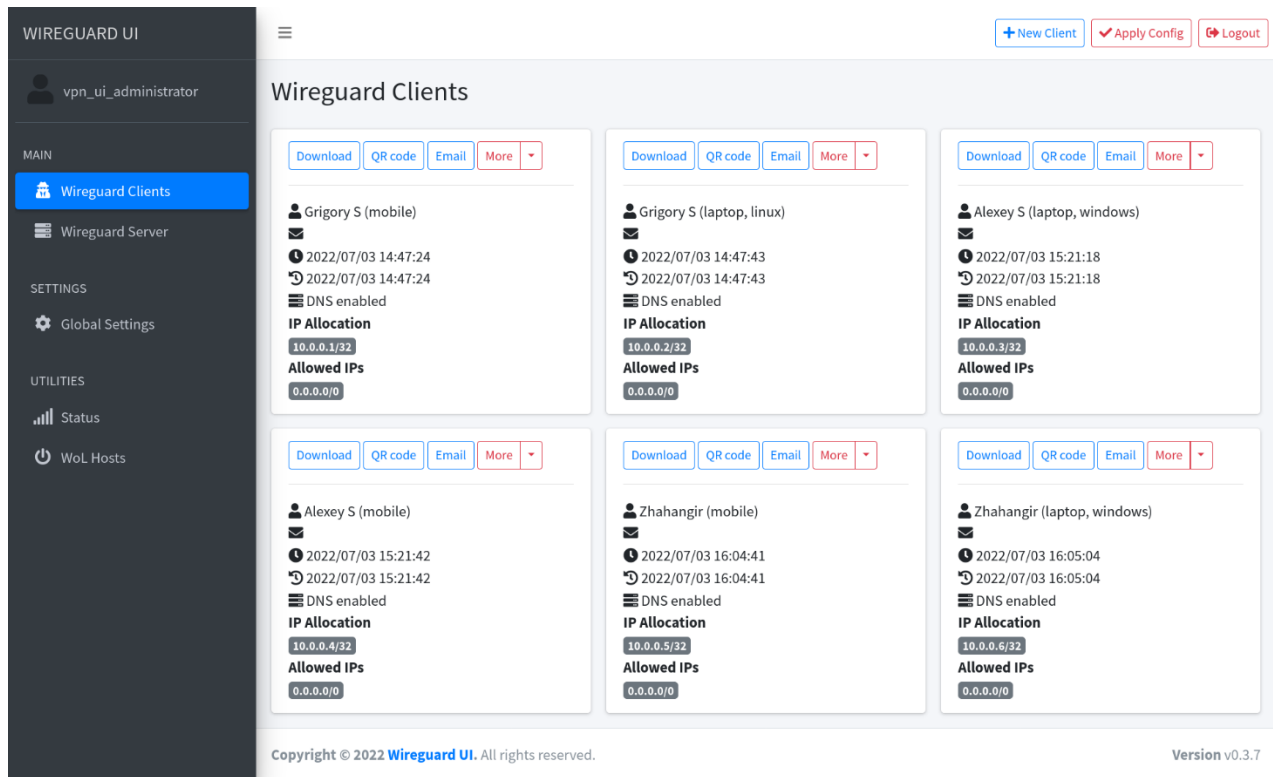


Рис. 1.5 – Інтерфейс WireGuard

WireGuard використовує публічний та приватний ключі для шифрування та розшифрування трафіку, що пересилається між мережами. Вона пропонує простий та легкий у використанні інтерфейс командного рядка, який дозволяє швидко налаштувати VPN-з'єднання.

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

Однією з переваг WireGuard є те, що вона пропонує більш простий та ефективний спосіб передачі даних, порівняно з традиційними технологіями VPN, такими як OpenVPN та IPSec. WireGuard також має відкритий вихідний код, що дозволяє розробникам детально аналізувати та вдосконалювати його безпеку. Недоліком WireGuard є те, що вона все ще розвивається та є відносно новою технологією, тому можуть бути проблеми з її сумісністю з іншими системами. Крім того, на даний момент WireGuard не підтримує деякі функції, такі як розширення маршрутизації, які доступні в інших технологіях VPN.

Отже, WireGuard є привабливою технологією VPN з високою швидкістю та ефективністю передачі даних, але може не підходити для всіх сценаріїв використання, особливо тих, які вимагають спеціальних функцій, які на даний момент ще не підтримуються WireGuard. Однак, з розвитком технології та підтримкою нових функцій, WireGuard може стати більш привабливою альтернативою для користувачів VPN.[4]

1.2.4 L2/L3 MPLS VPN

MPLS (англ. Multiprotocol Label Switching — багатопрокольна комутація за мітками) — механізм передачі даних, який емулює різні властивості мереж з комутацією каналів через мережі з комутацією пакетів.

MPLS працює на рівні, який можна було б розташувати між другим (канальним) і третім (мережевим) рівнями моделі OSI, і тому його зазвичай називають протоколом другого з половиною рівня (2,5-рівень). Його було розроблено з метою забезпечення універсальної служби передавання даних як для клієнтів мереж з комутацією каналів, так і мереж із комутацією пакетів. За допомогою MPLS можна передавати трафік найрізноманітнішої природи, як-от IP-пакети, ATM, Frame Relay, SONET і кадри Ethernet.

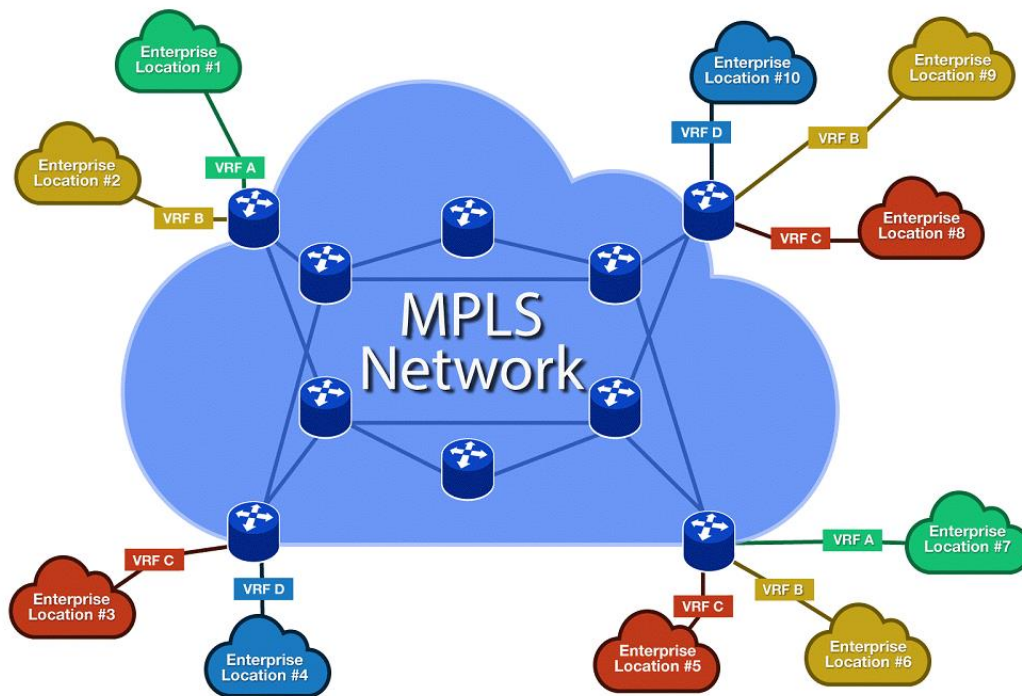


Рис. 1.6 – Схема побудови L2/L3 MPLS VPN

У традиційній IP-мережі пакети передаються від одного маршрутизатора до іншого, й кожний маршрутизатор, зчитуючи заголовок пакета, який є адресою, призначення приймає рішення про те, за яким маршрутом відправити пакет далі.

У протоколі MPLS жодного подальшого аналізу заголовків у маршрутизаторах на шляху проходження не проводиться, а керування переадресацією відбувається виключно на основі міток. Це має багато переваг над традиційною маршрутизацією на мережевому рівні.

Дана технологія має ряд недоліків, такі як: складність конфігурації, вартість, низька пропускна здатність та складність управління.

Налаштування та підтримка L2/L3 MPLS VPN можуть вимагати від інженера мережі значної експертизи та досвіду, оскільки ця технологія включає в себе різноманітні параметри та опції.

Якщо мережа використовується для передачі великих обсягів даних, може виникнути проблема недостатньої пропускної здатності мережі, оскільки L2/L3 MPLS VPN додає додатковий рівень обробки пакетів.[5]

1.2.5 Порівняння технологій VPN

Існує багато різних технологій VPN, кожна з яких має свої переваги та недоліки. У цьому розділі ми порівняємо Web VPN, GetVPN та WireGuard за кількома параметрами, щоб допомогти обрати технологію VPN, яка найбільше підходить для нашої мережі.

Безпека: Web VPN та GetVPN гарантують високий рівень безпеки, оскільки вони використовують шифрування для захисту даних, що передаються по мережі. У разі Web VPN це зазвичай SSL або TLS шифрування, тоді як у GetVPN використовується технологія IPsec. WireGuard також гарантує високий рівень безпеки за рахунок використання сучасних шифрувальних алгоритмів публічного та приватного ключів для шифрування та розшифрування трафіку.

Швидкість: WireGuard зазвичай забезпечує швидшу передачу даних порівняно з Web VPN та GetVPN. Це можливо завдяки його простоті та легкості в налаштуванні, а також використанню більш ефективних протоколів, таких як UDP. Водночас, Web VPN та GetVPN можуть мати більшу перевагу в обробці великої кількості одночасних підключень, особливо у мережах великих підприємств.

Надійність: GetVPN має високий рівень надійності, оскільки він використовує технологію мультикастингу, що дозволяє забезпечити відновлення підключень у разі збоїв мережі. У разі Web VPN та WireGuard можуть виникнути проблеми з надійністю, особливо при підключенні до нестабільної мережі.

Сумісність: Web VPN та GetVPN є сумісними з більшістю типами пристроїв та операційних систем, в той час як WireGuard підтримує лише деякі операційні системи, такі як Linux, Windows, macOS, Android та iOS. Однак, WireGuard може бути легко інтегровано з іншими технологіями VPN та мережевими пристроями.

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

Таблиця 1.1 – Порівняльна характеристика технологій VPN

Параметр	Web VPN	GetVPN	WireGuard
Безпека	Використовує SSL або TLS шифрування	Використовує технологію IPsec шифрування	Використовує сучасні шифрувальні алгоритми публічного та приватного ключів
Швидкість	Середня	Середня	Висока
Надійність	Можливі проблеми при підключенні до нестабільної мережі	Висока завдяки використанню технології мультикастингу	Можливі проблеми при підключенні до нестабільної мережі
Сумісність	Сумісний з більшістю типів пристроїв та операційних систем	Сумісний з більшістю типів пристроїв та операційних систем	Сумісний з Linux, Windows, macOS, Android та iOS
Інтеграція	Вимагає окремого сервера або апаратного забезпечення для налаштування	Інтегрований з мережевими пристроями безпосередньо	Легко інтегрується з іншими технологіями VPN та мережевими пристроями

Загалом, кожна з технологій VPN має свої переваги та недоліки, і вибір технології залежить від ваших потреб та умов використання. Web VPN та GetVPN гарантують високий рівень безпеки та надійності, тоді як WireGuard зазвичай забезпечує швидшу передачу даних. Крім того, Web VPN та GetVPN є більш сумісними з різними пристроями та операційними системами, в той час як WireGuard має підтримку лише обмеженої кількості операційних систем.

Для реалізації проєкту було обрано GetVPN через його високий рівень безпеки, особливо завдяки використанню технології IPsec для шифрування даних.

IPsec є надійним та широко використовуваним протоколом, який дозволяє захистити конфіденційні дані від несанкціонованого доступу. Крім того, GetVPN використовує технологію мультикастингу, що забезпечує стійкість та відновлення підключень навіть у випадку збоїв мережі. Це важливо для забезпечення надійного доступу до ресурсів у всіх умовах. Нарешті, GetVPN є сумісним з багатьма типами пристроїв та операційними системами, що дозволяє його легко інтегрувати у різні мережеві середовища.

1.3 Вразливості та недоліки GetVPN

Однією з вразливостей GetVPN є вразливість управління ключами. У протоколі GetVPN ключі шифрування передаються через контрольні пакети, які надсилаються між вузлами мережі. Це може створювати можливість для атаки великим потоком контрольних пакетів та викрадення ключів шифрування. Якщо зломисник здобуде доступ до ключів, він може отримати несанкціонований доступ до зашифрованих даних.

Потік трафіку Group Domain of Interpretation (GDOI) використовується в GetVPN для управління групами та розподілу ключів. Однак, існує певна вразливість пов'язана з використанням UDP-порту 848. Цей порт може бути використаний зломисниками для обходу політики шифрування. Зломисники можуть намагатися скористатися цим потоком трафіку та UDP-портом 848 для несанкціонованого доступу до мережі або перехоплення зашифрованої інформації. Це створює загрозу конфіденційності та безпеки передачі даних у GetVPN.

Крім того, була виявлена конкретна ідентифікована помилка в GetVPN, відома як помилка CSCui07698. Ця помилка виявляється в роботі протоколу та може створювати потенційну вразливість. Вона може дозволити зломисникам використовувати уразливість протоколу для отримання несанкціонованого доступу до зашифрованих даних або впливу на нормальну роботу мережі.[6]

Іншою вразливістю GetVPN є недостатня аутентифікація. Протокол GetVPN не надає повноцінної аутентифікації вузлів мережі. Це означає, що зломисники

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

можуть підробити ідентифікатори вузлів або скомпрометувати їх, отримуючи доступ до передачі даних. Відсутність надійної аутентифікації створює ризик підробки або спроби MITM-атак (Man-in-the-Middle).

Якщо один вузол GetVPN був скомпроментований, це може призвести до серйозних наслідків для безпеки мережі. Зловмисник може використовувати скомпроментований вузол для віддаленого доступу до всіх передач даних в мережі. Ця вразливість стає особливо небезпечною в ситуаціях, коли мережа містить вузли зі слабкою безпекою або незахищеними каналами зв'язку.

Злам GetVPN та потоку трафіку GDOI є викликом через високий рівень безпеки та криптографічних стандартів, на яких вони ґрунтуються. Проте, зловмисники можуть намагатися скористатися вразливостями, зокрема, вразливістю управління ключами та потоком трафіку GDOI через UDP-порт 848. Теоретичні методи злому можуть включати атаки на управління ключами та аутентифікацію, а також використання слабких вузлів у мережі.

Організації, які використовують GetVPN, повинні бути свідомі цих вразливостей та недоліків і приймати заходи для запобігання можливим атакам. Це включає регулярне оновлення протоколів та програмного забезпечення, впровадження надійних механізмів аутентифікації, контроль доступу та моніторингу мережі. Крім того, розробники GetVPN повинні постійно вдосконалювати протокол, виправляючи виявлені вразливості та недоліки.

Висновки до першого розділу

У цьому розділі було розглянуто різні технології VPN, які можуть бути використані для побудови захищеної мережі. Ми оглянули Web VPN, GetVPN та WireGuard, вивчивши їх принципи роботи, переваги та недоліки. Кожна з цих технологій має свої переваги та недоліки, і вибір технології залежить від конкретних потреб користувачів та вимог їх мережі.

Було розглянуто основні варіанти застосування VPN.

Site-to-site VPN використовуються для з'єднання декількох локальних мереж в одну велику мережу, щоб дозволити обмін даними та ресурсами між ними. Вона забезпечує захист всієї мережі, а не лише окремих пристроїв, і може економити кошти, оскільки не потрібно встановлювати окремі з'єднання з кожною локальною мережею. Проте, її налаштування може бути складним, вимагає високої пропускної здатності та спеціального обладнання та програмного забезпечення.

Site-to-point VPN використовується для з'єднання віддалених користувачів з локальною мережею. Вона дозволяє віддаленим користувачам зв'язуватися з локальною мережею з будь-якої точки світу, гарантує безпеку та приватність з'єднання, і легко налаштовується та використовується. Однак, пропускна здатність зв'язку може бути обмеженою, оскільки вся передача даних відбувається через одне з'єднання, і вона може бути дорогою, коли потрібно підключити більше одного користувача.

Для найкращого вибору технології VPN потрібно врахувати такі параметри, як безпека, швидкість, надійність та сумісність з іншими системами. Для реалізації в кваліфікаційній роботі було обрано GetVPN, оскільки він є надійним та стійким до атак, створює глобальну політику безпеки для всіх тунелів мережі та шифрує дані, що зменшує навантаження на мережевий протокол.

У наступному розділі ми розглянемо різні способи налаштування VPN, які допоможуть зробити мережу більш безпечною та зручною в користуванні.

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

РОЗДІЛ 2. Проєктування захищеної інформаційно-комунікаційної мережі з використанням GetVPN

2.1 Моделі та схеми адресації

GetVPN є однією з технологій VPN, яка гарантує безпеку та приватність комунікації, використовуючи симетричну криптографію. Для проєктування захищеної інформаційно-комунікаційної мережі з використанням GetVPN також потрібно розглянути структуру мережі та схему адресації.

Для гарантування безпеки та масштабованості мережі можна використовувати топологію "зірка". Кожен вузол мережі повинен підключатись до центрального маршрутизатора, який координує рух пакетів в мережі. Для гарантування безпеки комунікації, кожен вузол повинен мати свій власний ключ, який використовується для шифрування даних. Ключі можна генерувати за допомогою інструментів, які надає GetVPN.

GetVPN використовує різні технології для гарантування безпеки та приватності комунікації, включаючи шифрування даних, аутентифікацію та контроль цілісності даних. Ці технології дозволяють забезпечити надійний захист інформації під час її передачі по мережі.

Отже, якщо вам потрібно створити захищену мережу з використанням VPN технології, яка гарантує безпеку та приватність комунікації, то GetVPN може бути гарним варіантом. За допомогою правильної топології та ключів, які можна згенерувати за допомогою інструментів GetVPN, можна створити мережу з високим рівнем безпеки та масштабованості.

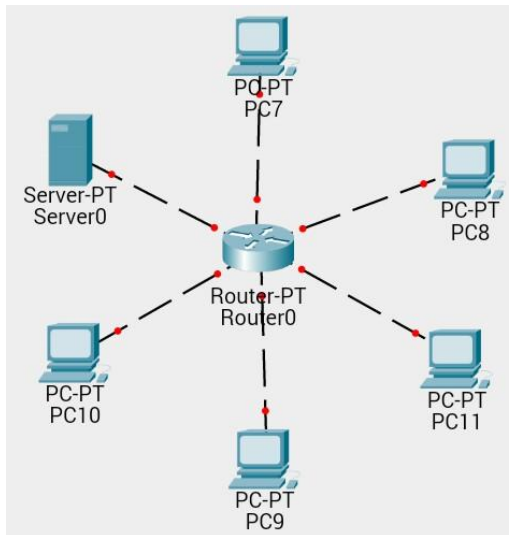


Рис. 2.1 – Схематичне подання топології «Зірка»

Топологія "зірка" є однією з найбільш поширених топологій для побудови VPN-мереж, оскільки вона дозволяє забезпечити високу масштабованість та простоту налаштування мережі. Кожен вузол в мережі має свій власний ключ, що гарантує безпеку комунікації між вузлами.

Для підключення до мережі з будь-якої точки, використовується віртуальна IP-адреса. Кожен вузол мережі повинен мати своє власне IP-адресування, яке використовується для ідентифікації вузла в мережі. Використання віртуального IP-адресування дозволяє гарантувати безпеку та приватність комунікації, оскільки кожен вузол має унікальну IP-адресу, яка не повторюється в мережі. Для гарантування безпеки комунікації, кожен вузол повинен мати унікальну IP-адресу, яка не повторюється в мережі. Для віртуального IP-адресування використовується підмережа з маскою /24.

Нижче наведено приклад схеми адресації мережі з використанням топології «зірка»:

- Центральний маршрутизатор (VPN-сервер): 10.0.0.1/24
- Вузол 1: 10.0.0.2/24
- Вузол 2: 10.0.0.3/24

- Вузол 3: 10.0.0.4/24
- ...

Кожен вузол мережі повинен мати свій власний ключ, який буде використовуватися для шифрування даних. Для генерації ключів можна використовувати інструменти, які надає GetVPN, або ж згенерувати їх самостійно.[7]

Загалом, GetVPN є простим та ефективним рішенням для гарантування безпеки та приватності комунікації в мережах, що дозволяє побудувати захищену VPN-мережу на основі топології "зірка" з використанням віртуального IP-адресування та індивідуальних ключів для кожного вузла мережі. GetVPN використовує протоколи транспортного рівня, такі як IPSec та SSL/TLS, для гарантування безпеки та інтегрованої аутентифікації та авторизації. Використання GetVPN дозволяє підвищити ефективність мережі та зменшити навантаження на мережеве обладнання. Крім того, GetVPN має підтримку різних типів мереж, включаючи MPLS та Ethernet, що дозволяє його використовувати в різних сценаріях.

2.2 Вибір серверної платформи та операційної системи

Для побудови захищеної мережі з використанням GetVPN необхідно обрати серверну платформу та операційну систему для VPN-сервера, які підтримують протокол GetVPN. До таких операційних систем належать зокрема, Cisco IOS та Cisco ASA. Залежно від обсягів обробки даних та кількості одночасних підключень до сервера, можна використовувати як фізичну, так і віртуальну серверну платформу. Рекомендується використовувати віртуальну серверну платформу для гарантування безпеки та масштабованості мережі, оскільки це дозволяє легко налаштувати віртуальні машини з різними операційними системами.

Для побудови захищеної мережі з використанням GetVPN також необхідно вибрати відповідне обладнання, таке як комутатори та маршрутизатори. Вибір такого обладнання залежить від обсягу та складності мережі.

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Один з прикладів комутаторів, який можна використовувати в системі, це Cisco Catalyst 2960. Цей комутатор має 24 порти із підтримкою Power over Ethernet (PoE), що дозволяє жити інші пристрої, такі як IP-телефони або відеокамери, без необхідності в окремому джерелі живлення. Крім того, Catalyst 2960 має підтримку технології Quality of Service (QoS), яка дозволяє регулювати пропускну здатність трафіку в мережі, забезпечуючи високу якість передачі даних. [8]



Рис. 2.2 – Cisco Catalyst 2960

Ще одним прикладом може бути комутатор HP J9773АНР. Цей комутатор також має 24 порти, але підтримує більш широкий діапазон протоколів, включаючи IPv6 та LLDP. Крім того, J9773АНР 2530 має інтегровані функції безпеки, такі як Access Control Lists (ACL) та Protected Ports, що дозволяє гарантувати безпеку мережі.[9]



Рис 2.3 – HP J9773АНР 2530-24G-PoE

Щодо маршрутизаторів, то можна використовувати, наприклад, Cisco 1941. Цей маршрутизатор має підтримку IPv6, Firewall, VPN та інших протоколів безпеки, що дозволяє гарантувати безпеку мережі. Крім того, 1941 має вбудовану підтримку Wi-Fi, що дозволяє підключати пристрої бездротово до мережі. [10]



Рис. 2.9 – Cisco 1941

Іншим прикладом маршрутизатора може бути Juniper SRX240. Цей маршрутизатор має вбудовані функції Firewall та VPN, що дозволяє гарантувати високий рівень безпеки мережі. Крім того, SRX240 підтримує технологію Quality of Service (QoS) та Network Address Translation (NAT), що дозволяє регулювати пропускну здатність трафіку та забезпечити надійну передачу даних в мережі.[11]



Рис. 2.10 Juniper SRX240

Вибір конкретного обладнання для захищеної мережі залежить від вимог до функціональності та безпеки мережі, а також від бюджету та наявної інфраструктури. Для найбільшої ефективності мережі, можна використовувати комутатори та маршрутизатори від одного виробника, що дозволяє забезпечити взаємодію між пристроями та спростити управління мережею.

2.3. Топологія та схема мережі

Для реалізації захищеної мережі з використанням GetVPN можна використовувати різні топології мережі, в залежності від потреб і вимог користувача. Однією з можливих топологій є топологія "зірка". У цій топології всі VPN-шлюзи підключені до центрального мережевого вузла, який виступає в ролі мережевого концентратора. Кожен VPN-шлюз підключений до центрального вузла за допомогою окремого тунелю GetVPN. Така топологія є простою в реалізації та керуванні, оскільки всі тунелі керуються централізовано, що дозволяє гарантувати високий рівень безпеки і стійкості мережі. Для налаштування топології "зірка" з використанням GetVPN необхідно налаштувати кожен VPN-шлюз з відповідними параметрами тунелю та підключити їх до центрального мережевого вузла.

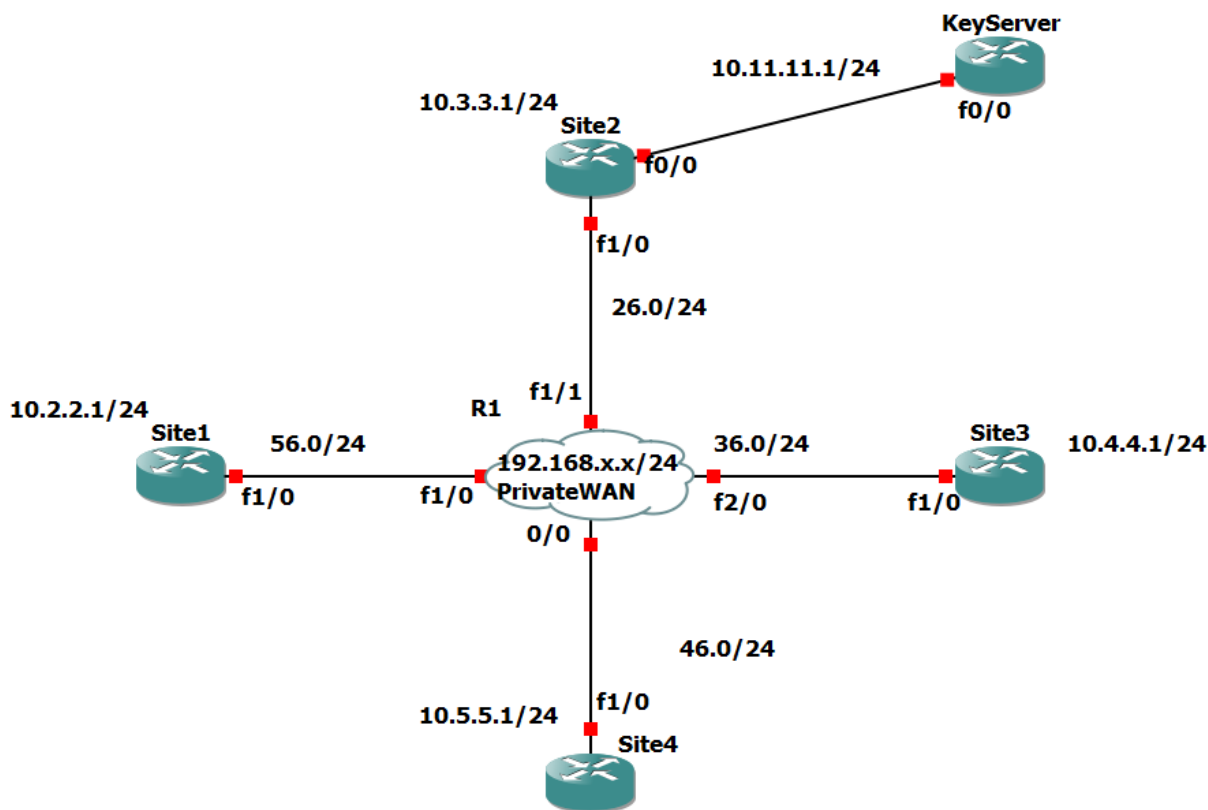


Рис. 2.11 – Топологія мережі

Висновки до другого розділу

У цьому розділі було розглянуто важливі аспекти побудови захищеної мережі з використанням протоколу GetVPN. Було надано загальний огляд протоколу, включаючи його переваги і недоліки, а також розглянуто основні етапи налаштування мережі з використанням GetVPN.

Також було розглянуто важливі аспекти вибору обладнання, таких як комутатори та маршрутизатори, для побудови захищеної мережі з використанням GetVPN. Було наведено приклади комутаторів та маршрутизаторів, що можуть бути використані в системі, з описом їх функціональних можливостей та важливих характеристик.

Складено топологію мережі, згідно з обраною топологією «зірка», яку в наступному розділі буде налаштовано.

Отже, для побудови захищеної мережі з використанням GetVPN потрібно ретельно вивчити можливості протоколу, а також правильно вибрати обладнання залежно від обсягу та складності мережі. Правильний вибір обладнання є ключовим етапом у побудові захищеної мережі з використанням GetVPN.

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

РОЗДІЛ 3. Налаштування та тестування проєкту

3.1 Налаштування обладнання та програмного забезпечення

GetVPN - це технологія, що гарантує безпеку даних в мережі, дозволяючи зашифровувати та автентифікувати трафік між вузлами мережі. GetVPN використовується для створення захищеної мережі з мінімальним впливом на роботу існуючої мережевої інфраструктури.

Загалом, цей розділ допоможе розібратися в технології GetVPN та надасть необхідну інформацію щодо її налаштування та використання в мережі.

Для налаштування GetVPN важливим є повне налаштування IP адресації та маршрутизації перед налаштуванням самого GetVPN.

Повне налаштування IP адресації та маршрутизації необхідне через декілька причин:

- GetVPN використовує тунелі між вузлами мережі для передачі зашифрованих даних. Налаштування маршрутизації допомагає ідентифікувати ці тунелі і визначити оптимальний шлях для передачі даних між ними.
- Віртуальна приватна мережа GetVPN передає трафік через наявну IP-мережу. Налаштування маршрутизації дозволяє визначити правила для маршрутизації трафіку між вузлами GetVPN і зовнішніми мережевими пристроями. Це забезпечує ефективну передачу даних та оптимізацію шляху доставки.
- GetVPN використовує механізм шифрування для захисту даних, які передаються. Правильне налаштування маршрутизації допомагає забезпечити, що дані, що проходять через мережу, будуть маршрутизуватись через тунелі GetVPN, які забезпечують шифрування та конфіденційність.

Переходимо до налаштувань GetVPN.

KeyServer:

crypto isakmp policy 10: Встановлює політику ISAKMP з пріоритетом 10. ISAKMP (Internet Security Association and Key Management Protocol) використовується для створення, управління та обміну ключами для безпеки IP-тунелів.

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

encr 3des: Встановлює алгоритм шифрування 3DES (Triple Data Encryption Standard) для ISAKMP. 3DES використовується для захисту конфіденційності даних.

hash md5: Встановлює алгоритм хешування MD5 для ISAKMP. MD5 використовується для перевірки цілісності даних.

authentication pre-share: Встановлює метод аутентифікації з попереднім обміном ключів для ISAKMP. У цьому випадку використовується попередньо встановлений ключ (pre-shared key).

group 2: Встановлює групу Діффі-Геллмана з номером 2 для обміну ключами в ISAKMP. Група Діффі-Геллмана визначає параметри обміну ключами.

crypto isakmp key cisco address 0.0.0.0 0.0.0.0: Налаштовує попередньо встановлений ключ "cisco" для всіх адрес (0.0.0.0/0) в управлінні ключами ISAKMP. Це означає, що ключ "cisco" буде використовуватись для аутентифікації з будь-якою адресою.

crypto ipsec transform-set T-SET esp-3des esp-sha-hmac: Визначає набір перетворень IPSec з назвою "T-SET", використовуючи шифрування 3DES і хешування SHA-НМАС. Набір перетворень встановлює правила шифрування, хешування та аутентифікації для IPSec трафіку.

crypto ipsec profile I-PROF: Створює профіль IPSec з назвою "I-PROF". Профіль IPSec містить налаштування для створення та обробки IPSec тунелів.

set transform-set T-SET: Асоціює набір перетворень "T-SET" з профілем IPSec "I-PROF". Це вказує, що профіль IPSec буде використовувати заданий набір перетворень для шифрування та аутентифікації.

crypto gdoi group IT-S: Розпочинає налаштування групи GDOI з назвою "IT-S". GDOI (Group Domain of Interpretation) використовується для керування груповими безпековими асоціаціями.

identity number 150: Призначає числовий ідентифікатор 150 для групи GDOI. Ідентифікатор використовується для ідентифікації групи в мережі.

server local: Вказує, що локальний пристрій є членом групи GDOI. Це вказує, що пристрій виконує роль сервера в групових асоціаціях.

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

rekey retransmit 10 number 2: Налаштовує групу GDOI на повторну передачу повідомлень про оновлення кожні 10 секунд з максимальною кількістю спроб 2. Це вказує, як часто оновлювати ключі та іншу інформацію в груповій асоціації.

sa ipsec 10: Вказує ідентифікатор SA (Security Association) 10 для групи GDOI. SA визначає параметри безпеки для IPSec тунелю.

profile I-PROF: Асоціює профіль IPSec "I-PROF" з SA 10 в групі GDOI. Це вказує, які налаштування IPSec використовувати для безпеки трафіку в груповій асоціації.

match address ipv4 101: Визначає ACL (Access Control List) з IPv4 адресою 101 для відповідності трафіку в групі GDOI. ACL використовується для фільтрації трафіку за певними правилами.

replay counter window-size 64: Встановлює розмір вікна перегляду лічильника повторів на 64 для групи GDOI. Це вказує, скільки повторних пакетів може бути оброблено перед відхиленням.

address ipv4 10.11.11.1: Призначає IPv4 адресу 10.11.11.1 для групи GDOI. Це вказує, яку IP-адресу використовувати для спілкування в груповій асоціації.

Site1:

crypto isakmp policy 10: Встановлює політику ISAKMP з пріоритетом 10. ISAKMP (Internet Security Association and Key Management Protocol) використовується для створення, управління та обміну ключами для безпеки IP-тунелей.

encr 3des: Встановлює алгоритм шифрування 3DES (Triple Data Encryption Standard) для ISAKMP. 3DES використовується для захисту конфіденційності даних.

hash md5: Встановлює алгоритм хешування MD5 для ISAKMP. MD5 використовується для перевірки цілісності даних.

authentication pre-share: Встановлює метод аутентифікації з попереднім обміном ключів для ISAKMP. У цьому випадку використовується попередньо встановлений ключ (pre-shared key).

group 2: Встановлює групу Діффі-Геллмана з номером 2 для обміну ключами в ISAKMP. Група Діффі-Геллмана визначає параметри обміну ключами.

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

crypto isakmp key cisco address 10.11.11.1: Налаштовує попередньо встановлений ключ "cisco" для адреси 10.11.11.1 в управлінні ключами ISAKMP. Це означає, що ключ "cisco" буде використовуватись для аутентифікації з даною адресою.

crypto gdoi group IT-GM: Розпочинає налаштування групи GDOI з назвою "IT-GM". GDOI (Group Domain of Interpretation) використовується для керування груповими безпековими асоціаціями.

identity number 150: Призначає числовий ідентифікатор 150 для групи GDOI. Ідентифікатор використовується для ідентифікації групи в мережі.

server address ipv4 10.11.11.1: Визначає IP-адресу 10.11.11.1 як адресу сервера для групи GDOI. Це вказує, який пристрій виконує роль сервера в групових асоціаціях.

crypto map IMAP 10 gdoi: Створює мапу IPsec з назвою "IMAP" та пріоритетом 10 для використання з протоколом GDOI. Мапа IPsec використовується для визначення налаштувань безпеки для тунелів IPsec.

set group IT-GM: Асоціює групу GDOI "IT-GM" з мапою IPsec "IMAP". Це вказує, що мапа IPsec використовує налаштування безпеки, визначені для групи GDOI "IT-GM".

crypto map IMAP: Активує мапу IPsec з назвою "IMAP". Це означає, що мапа IPsec застосовуватиметься до вхідного або вихідного трафіку на інтерфейсі.

Подібні налаштування проводяться на інших маршрутизаторах типу **site** (лістинг наведено в Додатку А).

3.2 Тестування та оцінювання результатів

Проведення тестування мережі з налаштованим GetVPN (Group Encrypted Transport VPN) вимагає використання певних команд для перевірки стану мережевих пристроїв та показників безпеки. У даному підрозділі розглянемо деякі з цих команд та їх вивід, який може бути корисним під час тестування мережі з використанням GetVPN.

1. ***show crypto isakmp sa*** - використовується для перевірки стану ISAKMP (Internet Security Association and Key Management Protocol) Security Associations

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

(SA). Вивід цієї команди має показувати інформацію про наявність активних SA, такі як ідентифікатори та статуси.

```
Site3#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
10.11.11.1    192.168.36.2  GDOI_IDLE      1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

Рис. 3.2 – Результат команди *show crypto isakmp sa* на пристрої Site3

Ця інформація показує, що для IPv4 існує активний тунель ISAKMP між IP-адресою 10.11.11.1 (призначення) та IP-адресою 192.168.36.2 (джерело) у стані очікування GDOI з ідентифікатором з'єднання 1001.

2. *show crypto gdoi ks member* - ця команда використовується для перевірки стану Key Server (KS) та членства в групі GetVPN. Вивід цієї команди повинен показувати інформацію про наявність та стан KS, а також перелік членів групи.

```
KeyServer#show crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group IT-S : 0

Group Member ID   : 192.168.26.2
Group ID           : 150
Group Name         : IT-S
Key Server ID     : 10.11.11.1

Group Member ID   : 192.168.36.2
Group ID           : 150
Group Name         : IT-S
Key Server ID     : 10.11.11.1

Group Member ID   : 192.168.46.2
Group ID           : 150
Group Name         : IT-S
Key Server ID     : 10.11.11.1
```

Рис. 3.3 – Результат команди *show crypto gdoi ks members* на пристрої KeyServer

Ця інформація показує, що в групі IT-S існують три члени групи з відповідними IP-адресами та ідентифікаторами, і всі вони використовують один і той же ключовий сервер з IP-адресою 10.11.11.1.

3. *show crypto gdoi gm* - ця команда використовується для перевірки стану Group Member (GM) у GetVPN. Вивід цієї команди має показувати інформацію про наявність та стан GM, включаючи їхній ідентифікатор та статус.

```
Site3#show crypto gdoi gm
Group Member Information For Group IT-GM:
  IPsec SA Direction      : Both
  ACL Received From KS    : gdoi_group_IT-GM_temp_acl
  Last rekey seq num      : 0
  Re-register
    Remaining time        : 3290 secs
  Retry Timer
    :NOT RUNNING
```

Рис. 3.4 – Результат команди *show crypto gdoi gm* на пристрої Site3

Ця інформація показує, що для групи IT-GM існує член групи, який має налаштовані IPsec безпеку для обох напрямків, отримав ACL від ключового сервера, має останній номер послідовності перезавантаження ключа 0 і наразі знаходиться в процесі повторної реєстрації. Таймер повторної спроби в даному випадку не активний.

4. *show crypto ipsec sa* - ця команда використовується для перевірки стану IPsec Security Associations (SA). Вивід цієї команди має показувати інформацію про активні IPsec SA, такі як ідентифікатори, статуси та статистику обміну даними.

```
Site3#show crypto ipsec sa

interface: FastEthernet1/0
  Crypto map tag: IMAP, local addr 192.168.36.2

protected vrf: (none)
local  ident (addr/mask/prot/port): (10.0.0.0/255.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.0.0.0/255.0.0.0/0/0)
current_peer 0.0.0.0 port 848
  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.: 192.168.36.2, remote crypto endpt.: 0.0.0.0
  path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
  current outbound spi: 0x7B5EAFB8 (2069802936)
  PFS (Y/N): N, DH group: none
```

```

inbound esp sas:
 spi: 0x7B5EAFB8 (2069802936)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 1, flow_id: SW:1, sibling_flags 80000040, crypto map: IMAP
  sa timing: remaining key lifetime (sec): (3418)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0x7B5EAFB8 (2069802936)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 2, flow_id: SW:2, sibling_flags 80000040, crypto map: IMAP
  sa timing: remaining key lifetime (sec): (3418)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

```

Рис. 3.5 – Результат команди *show crypto ipsec sa* на пристрої Site3

Цей вивід показує наявність вхідних і вихідних SA для ESP (Encapsulating Security Payload) на інтерфейсі FastEthernet1/0 з використанням трансформації esp-3des esp-sha-hmac. Всі SA мають статус ACTIVE, що свідчить про успішну налаштування та роботу IPsec з'єднання.

5. *show crypto engine connections active* - ця команда використовується для перевірки активних з'єднань криптографічного двигуна. Вивід цієї команди має показувати інформацію про активні з'єднання, включаючи типи шифрування та алгоритми, які використовуються.

```

KeyServer#show crypto engine connections active
Crypto Engine Connections

  ID   Type   Algorithm      Encrypt  Decrypt  IP-Address
  ----  ---  -
1001  IKE    MD5+3DES       0        0  10.11.11.1
1002  IKE    MD5+3DES       0        0  10.11.11.1
1003  IKE    MD5+3DES       0        0  10.11.11.1

```

Рис. 3.6 Результат команди *show crypto engine connections active* на пристрої KeyServer

У даному виводі наведено три активних з'єднання типу IKE з алгоритмом MD5+3DES, пов'язаних з IP-адресою 10.11.11.1.

```
Site3#show crypto engine connections active
Crypto Engine Connections

  ID  Type      Algorithm      Encrypt  Decrypt  IP-Address
  ---  ---      -
    1  IPsec     3DES+SHA       0        0    10.0.0.0
    2  IPsec     3DES+SHA       0        0    10.0.0.0
 1001  IKE       MD5+3DES       0        0   192.168.36.2
```

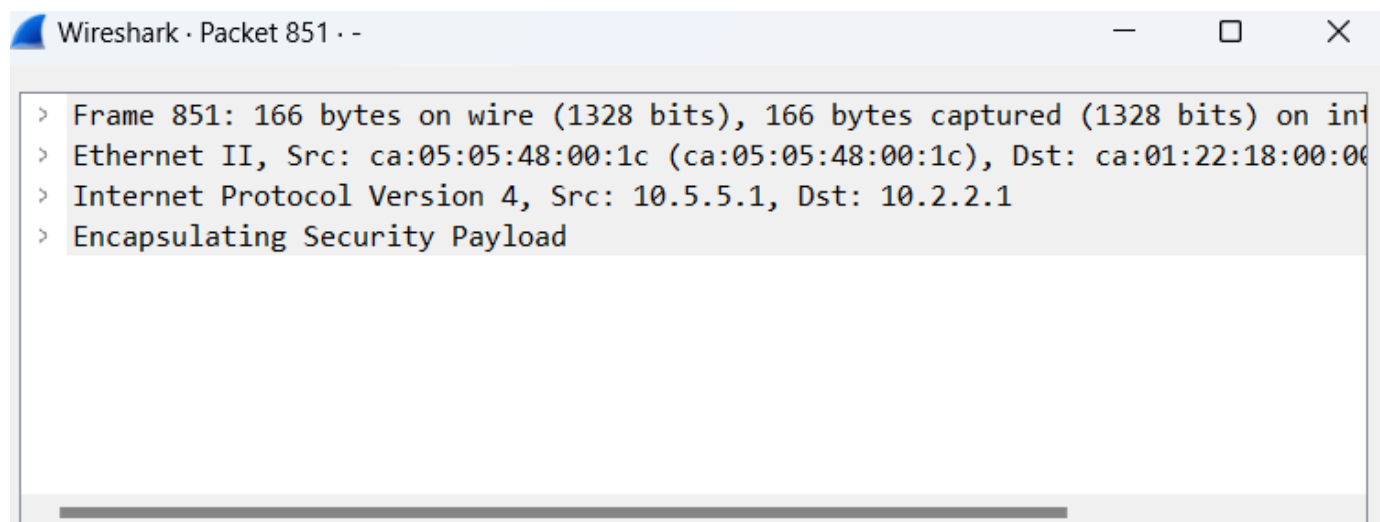
Рис. 3.7 Результат команди *show crypto engine connections active* на пристрої Site3

У даному виводі наведено три активних з'єднання: два з'єднання типу IPsec з алгоритмом 3DES+SHA, пов'язані з IP-адресою 10.0.0.0, та одне з'єднання типу IKE з алгоритмом MD5+3DES, пов'язане з IP-адресою 192.168.36.2.

Загальною метою тестування мережі з GetVPN є переконання, що мережа працює стабільно, безпечно та відповідає вимогам організації. Тестування допомагає виявити потенційні проблеми та вразливості, щоб їх вчасно виправити та покращити безпеку мережі.

Завдяки програмі Wireshark для моніторингу пакетів, можемо побачити наступні ESP пакети при пінгуванні.

No.	Time	Source	Destination	Protocol	Length	Info
844	1187.061275	10.5.5.1	10.2.2.1	ESP	166	ESP (SP
847	1189.055803	10.5.5.1	10.2.2.1	ESP	166	ESP (SP
850	1191.061980	10.5.5.1	10.2.2.1	ESP	166	ESP (SP
851	1193.071418	10.5.5.1	10.2.2.1	ESP	166	ESP (SP
856	1195.058743	10.5.5.1	10.2.2.1	ESP	166	ESP (SP



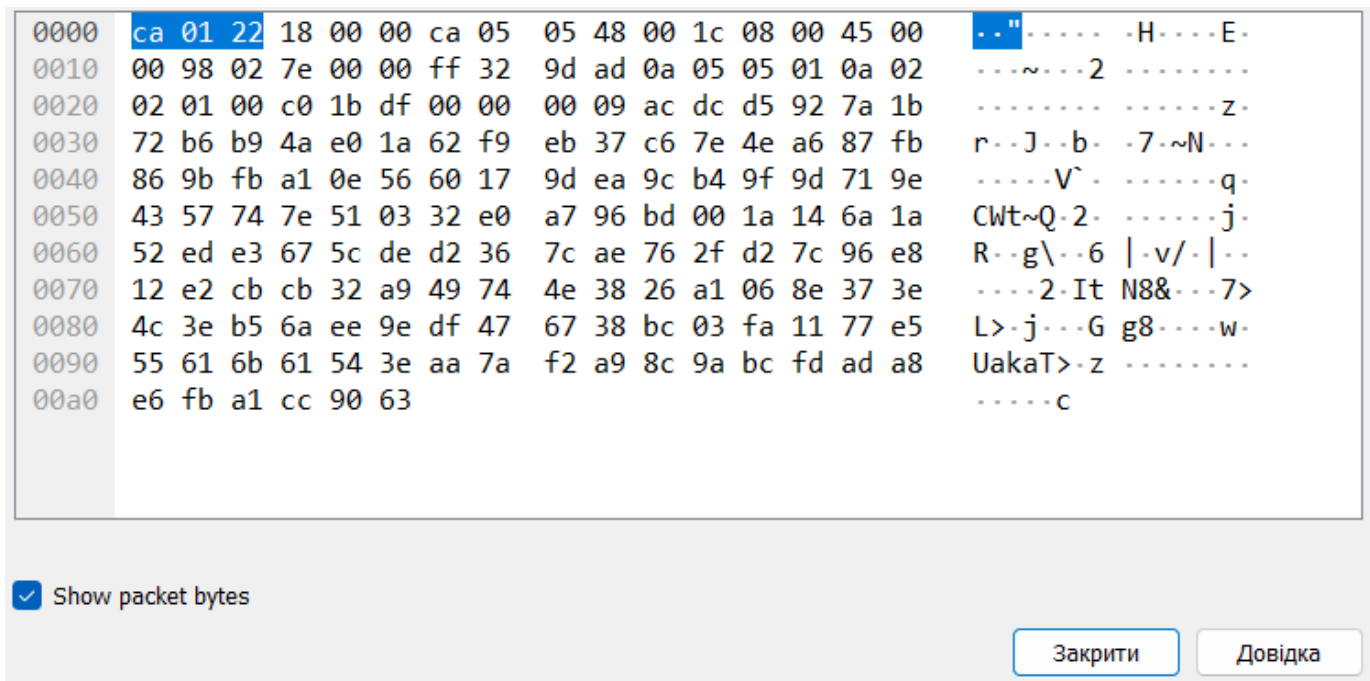


Рис. 3.8-3.9 – Перевірка пакетів у WireShark

ESP-пакети (Encapsulating Security Payload) є частиною протоколу IPsec, який забезпечує шифрування, аутентифікацію та захист цілісності даних, що передаються в мережі.

ESP пакети містять зашифровані дані, які включають оригінальні дані пакета IP, а також додаткові поля для гарантування безпеки. Вони застосовуються на рівні IP-пакетів, що дозволяє шифрувати та захищати дані, що пересилаються між вузлами в мережі.

ESP пакети, разом з іншими компонентами IPsec, створюють тунель для захищених комунікацій між вузлами в мережі. Це допомагає забезпечити приватність, цілісність та автентичність даних, що передаються в мережі.

Висновки до третього розділу

У цьому розділі було описано процес налаштування необхідного обладнання та програмного забезпечення для успішної реалізації проєкту. Були враховані вимоги та специфікації проєкту, і відповідно до них були здійснені необхідні налаштування. Цей етап включав встановлення та налаштування обладнання, налаштування програмного забезпечення, встановлення драйверів, вирішення конфліктів та забезпечення сумісності всіх компонентів системи.

Розглянуто можливі сценарії та проведено тестування проєкту для перевірки його працездатності та відповідності вимогам. Розглянуто команди для тестування та описано дані, отримані під час перевірки.

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У кваліфікаційній роботі було розроблено проєкт захищеної інформаційно-комунікаційної мережі з використанням технології GetVPN.

Розглянуто теоретичні аспекти створення захищеної інформаційно-комунікаційної мережі з використанням технологій VPN. У першому розділі було розглянуто загальні відомості про VPN технології, а також проведено огляд різних варіантів побудови VPN, зокрема Web VPN, GET VPN, WireGuard. Було здійснено порівняння цих технологій, що дало змогу визначити найбільш відповідну для створення захищеної мережі технологію GetVPN.

У другому розділі було проведено проєктування захищеної інформаційно-комунікаційної мережі з використанням обраної технології VPN. Були визначені моделі та схеми адресації, а також здійснено вибір обладнання та програмного забезпечення, необхідних для реалізації проєкту.

У третьому розділі було проведено налаштування та аналіз тестування проєкту. Було налаштовано обладнання та програмне забезпечення. Проведено тестування проєкту методом перевірки та аналізу виводу певних команд.

В результаті проведених досліджень та реалізації проєкту було встановлено, що технологія GetVPN є ефективним і надійним рішенням для створення захищеної інформаційно-комунікаційної мережі. Вона забезпечує конфіденційність, цілісність та доступність даних, а також ефективно працює в розподіленому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Порівняння, Site-to-site та Site-to-point VPN [Електронний ресурс] // businessyield.com – Режим доступу до ресурсу: <https://businessyield.com/technology/site-to-site-vpn-vs-point-to-site-vpn/>.
2. Web VPN [Електронний ресурс] // Cisco community – Режим доступу до ресурсу: <https://community.cisco.com/t5/security-knowledge-base/webvpn-ssl-vpn/tap/3112232>.
3. GetVPN [Електронний ресурс] // IPWITHEASE – Режим доступу до ресурсу: <https://ipwithease.com/introduction-to-getvpn/>.
4. WireGuard [Електронний ресурс] – Режим доступу до ресурсу: <https://www.wireguard.com/>.
5. L2/L3 MPLS VPN [Електронний ресурс] // Tech Library – Режим доступу до ресурсу: https://www.juniper.net/documentation/en_US/junos/topics/concept/mpls-ex-series-vpn-layer2-layer3.html.
6. Вразливість GetVPN через GDOI [Електронний ресурс] // CVE – Режим доступу до ресурсу: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3436>.
7. Топологія "Зірка" [Електронний ресурс] // Javatpoint – Режим доступу до ресурсу: <https://www.javatpoint.com/what-is-star-topology>.
8. Cisco Catalyst 2960 [Електронний ресурс] // Cisco – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/series.html>.
9. HP J9773AHP 2530-24G-PoE [Електронний ресурс] // Manualslib – Режим доступу до ресурсу: <https://www.manualslib.com/manual/831916/HP-2530-24.html#manual>.
10. Cisco 1941 [Електронний ресурс] // Cisco – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78_556319.html.
11. Juniper SRX240 [Електронний ресурс] // juniper-ua – Режим доступу до ресурсу: <https://juniper-ua.com/srx240>.

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

12. Налаштування мережі з GetVPN [Електронний ресурс] // GNS3 – Режим доступу до ресурсу: <https://www.gns3.com/marketplace/labs/get-vpn>.

13. Робота GetVPN [Електронний ресурс] // Cisco – Режим доступу до ресурсу: https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-3s/sec-get-vpn-xe-3s-book/sec-get-vpn-gikev2.html.xml.

14. Команди Show [Електронний ресурс] // Cisco – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/server_nw_virtual/2-5_release/command_reference/show.html.

15. IPSec VPN Design – 800 East 96th Street Indianapolis, IN 46240 USA: Cisco Press, 2006. – 352 с. – (Cisco) – Режим доступу до ресурсу: <https://ptgmedia.pearsoncmg.com/images/9781587051111/samplepages/9781587051111.pdf>.

ДОДАТКИ

		Пекарєв М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

Лістинг налагодження:

KeyServer:

```

crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto ipsec transform-set T-SET esp-3des esp-sha-hmac
crypto ipsec profile I-PROF
  set transform-set T-SET
crypto gdoi group IT-S
  identity number 150
  server local
  rekey retransmit 10 number 2
  sa ipsec 10
  profile I-PROF
  match address ipv4 101
  replay counter window-size 64
  address ipv4 10.11.11.1
ip tcp synwait-time 5
interface FastEthernet0/0
  ip address 10.11.11.1 255.255.255.0
  duplex half
interface FastEthernet1/0
  no ip address
  shutdown

```

		Пекарєв М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

```

duplex auto
speed auto
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
router eigrp 1
network 10.11.11.0 0.0.0.255
no auto-summary
ip forward-protocol nd
no ip http server
no ip http secure-server
access-list 101 permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0

```

		Пекарь М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

```

exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
end

```

R1

```

interface FastEthernet0/0
ip address 192.168.46.1 255.255.255.0
duplex half
interface FastEthernet1/0
ip address 192.168.56.1 255.255.255.0
duplex auto
speed auto
interface FastEthernet1/1
ip address 192.168.26.1 255.255.255.0
duplex auto
speed auto
interface FastEthernet2/0
ip address 192.168.36.1 255.255.255.0
duplex auto

```

		Пекарь М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

```

speed auto
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
router eigrp 1
network 192.168.0.0 0.0.255.255
auto-summary
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
end

```

		Пекарь М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

Site1

interface Loopback0

ip address 10.2.2.1 255.255.255.0

interface FastEthernet0/0

no ip address

shutdown

duplex half

interface FastEthernet1/0

ip address 192.168.56.2 255.255.255.0

duplex auto

speed auto

interface FastEthernet1/1

no ip address

shutdown

duplex auto

speed auto

interface FastEthernet2/0

no ip address

shutdown

duplex auto

speed auto

interface FastEthernet2/1

no ip address

shutdown

duplex auto

speed auto

router eigrp 1

network 10.2.2.0 0.0.0.255

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

```

network 192.168.56.0
no auto-summary
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 10.11.11.1
crypto gdoi group IT-GM
identity number 150

```

		Пекарь М. Д.			КИК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

server address ipv4 10.11.11.1

crypto map IMAP 10 gdoi

set group IT-GM

crypto map IMAP

end

Site2

crypto isakmp policy 10

encr 3des

hash md5

authentication pre-share

group 2

crypto isakmp key cisco address 10.11.11.1

crypto gdoi group IT-GM

identity number 150

server address ipv4 10.11.11.1

crypto map IMAP 10 gdoi

set group IT-GM

ip tcp synwait-time 5

interface Loopback0

ip address 10.3.3.1 255.255.255.0

interface FastEthernet0/0

ip address 10.11.11.2 255.255.255.0

duplex half

interface FastEthernet1/0

ip address 192.168.26.2 255.255.255.0

duplex auto

speed auto

		Пекарев М. Д.			КИК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

```

crypto map IMAP
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
router eigrp 1
network 10.0.0.0
network 192.168.26.0
no auto-summary
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0

```

		Пекарь М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

```

privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
end

```

Site3

```

crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 10.11.11.1
crypto gdoi group IT-GM
identity number 150
server address ipv4 10.11.11.1
crypto map IMAP 10 gdoi
set group IT-GM
ip tcp synwait-time 5
interface Loopback0
ip address 10.4.4.1 255.255.255.0
interface FastEthernet0/0

```

		Пекарев М. Д.			КИК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no ip address
shutdown
duplex half
interface FastEthernet1/0
ip address 192.168.36.2 255.255.255.0
duplex auto
speed auto
crypto map IMAP
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
router eigrp 1
network 10.4.4.0 0.0.0.255
network 192.168.36.0
no auto-summary
ip forward-protocol nd
no ip http server

```

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

```

no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
end

```

Site4

```

crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 10.11.11.1
crypto gdoi group IT-GM
identity number 150

```

		Пекарь М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

```

server address ipv4 10.11.11.1
crypto map IMAP 10 gdoi
set group IT-GM
ip tcp synwait-time 5
interface Loopback0
ip address 10.5.5.1 255.255.255.0
interface FastEthernet0/0
no ip address
shutdown
duplex half
interface FastEthernet1/0
ip address 192.168.46.2 255.255.255.0
duplex auto
speed auto
crypto map IMAP
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet2/1
no ip address
shutdown
duplex auto

```

		Пекарев М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

```

speed auto
router eigrp 1
network 10.5.5.0 0.0.0.255
network 192.168.46.0
no auto-summary
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
end

```

		Пекарєв М. Д.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
		Головня О. С.				57
Змн.	Арк.	№ докум.	Підпис	Дата		