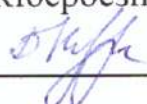


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект захищеної мережевої інформації на
основі сучасних VPN рішень»

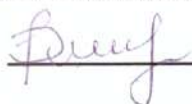
Виконав студент 4-го курсу групи КБ-21-2
спеціальності 125 «Кібербезпека»

 Богдан КАРНАУХ

Керівник: старший викладач кафедри КІ та КБ

 Олександра ПОКОТИЛО

Рецензент: старший викладач кафедри КІ та КБ

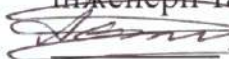
 Єлизавета ТРОКОЗ

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

3 березня 2025 р.

ЗАВДАННЯ

на випускн у кваліфікаційну роботу бакалавра

Студент: Карнаух Богдан Олексійович

Тема роботи: «Проект захищеної мережевої інформації на основі сучасних VPN рішень»

затверджена Наказом університету від 3 березня 2025 р. № 80/с

Термін здачі студентом закінченої роботи 27 червня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Об'єктом дослідження є процес забезпечення захищеного віддаленого доступу в корпоративних мережах за допомогою VPN-рішень.

Предметом дослідження є методи та засоби реалізації VPN-з'єднань на основі протоколу IPsec для забезпечення конфіденційності та цілісності даних у корпоративному середовищі.

Обладнання та програмне забезпечення:

1. Маршрутизатор Cisco 7200 Series
2. Комутатор Cisco Catalyst WS-C2960-24TT-L
3. ОС Windows 10
4. TACACSGUI
5. GNS3

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Дячук О.Ю.	3.03.2025	03.03.2025
2	Дячук О.Ю.	3.03.2025	03.03.2025
3	Дячук О.Ю.	3.03.2025	03.03.2025

Студент Богдан КАРНАУХ

Керівник Олександра ПОКОТИЛО

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	17.03.2025	Виконано
2	Аналіз літературних джерел	25.03.2025	Виконано
3	Розробка структурної моделі	04.04.2025	Виконано
4	Розрахунок параметрів адресації	06.04.2025	Виконано
5	Вибір технологій для реалізації	08.04.2025	Виконано
6	Проектування КМ	25.04.2025	Виконано
7	Підготовка компонентів для мережі	05.05.2025	Виконано
8	Налаштування мережі	13.05.2025	Виконано
9	Налагодження захисту мережі	19.05.2025	Виконано
10	Тестування роботи КМ	26.05.2025	Виконано
11	Оформлення пояснювальної записки	30.05.2025	Виконано
12	Оформлення презентації	09.06.2025	Виконано
13	Захист	27.06.2025	Виконано

Студент Богдан КАРНАУХ

Керівник Олександра ПОКОТИЛО

АНОТАЦІЯ

Кваліфікаційна робота бакалавра присвячена розробці проєкту захищеної корпоративної мережі на основі сучасних VPN-рішень.

Обсяг пояснювальної записки становить 55 сторінок, містить 32 рисунки та 4 таблиці. Список використаних джерел налічує 20 найменувань.

Метою випускної кваліфікаційної роботи є розробка та реалізація проєкту захищеної корпоративної мережі, зокрема, впровадження Site-to-Site тунелів за допомогою фреймворку IPsec на обладнанні Cisco.

В результаті виконання роботи було спроектовано та впроваджено комплексну підсистему захисту. Проведено налаштування мережевих протоколів EIGRP, SSHv2, DHCP, а також реалізовано захищені IPsec VPN-тунелі. Для централізованого управління доступом та моніторингу впроваджено сервери TACACS+ та Syslog.

Отримані результати включають створення надійної та захищеної інфраструктури, де конфіденційність та цілісність даних при передачі між офісами забезпечується за допомогою шифрування IPsec. Впровадження TACACS+ забезпечило гранулярний контроль доступу адміністраторів до мережевого обладнання.

Результати роботи можуть бути використані як практичний посібник для побудови безпечних корпоративних мереж малого та середнього бізнесу.

Ключові слова: IPSEC, VPN, CISCO, TACACS+, SYSLOG, EIGRP, DHCP, SSHV2, КОРПОРАТИВНА МЕРЕЖА, ЗАХИСТ МЕРЕЖІ, ТРИРІВНЕВА ТОПОЛОГІЯ.

					ККІК<.КР.Б – 125 – 1 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект захищеної мережевої інформації на основі сучасних VPN рішень	Літ.	Арк.	Аркушів
Розроб.		Карнаух Б.О.		26.06.25				
Керівник		Покотило О.А.		26.06.25			4	87
Реценз.		Трокоз Є.М.		26.06.25		ФІКТ, Гр. КБ-21-2		
Н. контр.		Покотило О.А.		26.06.25				
Затверд.		Єфіменко А.А.		26.06.25				

ANNOTATION

The bachelor's thesis is dedicated to the project of a secure corporate network based on modern VPN solutions.

The explanatory note consists of 55 pages, including 32 figures and 4 tables. The list of references contains 20 sources.

The purpose of the qualification thesis is the design and implementation of a secure corporate network project, specifically, the deployment of Site-to-Site tunnels using the IPsec framework on Cisco equipment.

As a result of this work, a comprehensive security subsystem was designed and implemented. Network protocols such as EIGRP, SSHv2, and DHCP were configured, and secure IPsec VPN tunnels were implemented. For centralized access management and monitoring, TACACS+ and Syslog servers were deployed.

The obtained results include the creation of a reliable and secure infrastructure where the confidentiality and integrity of data transmitted between offices are ensured through IPsec encryption. The implementation of TACACS+ has provided granular access control for administrators to the network equipment.

The results of this work can be used as a practical guide for building secure corporate networks for small and medium-sized businesses.

Keywords: IPSEC, VPN, CISCO, TACACS+, SYSLOG, EIGRP, DHCP, SSHV2, CORPORATE NETWORK, NETWORK SECURITY, THREE-TIER TOPOLOGY.

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 АНАЛІЗ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ З ВИКОРИСТАННЯМ VPN-ТЕХНОЛОГІЙ	9
1.1 Загальні принципи функціонування віртуальних приватних мереж (VPN)	9
1.2 Класифікація VPN за архітектурою та призначенням (Remote Access, Site-to-Site).....	11
1.3 Огляд та порівняльний аналіз сучасних VPN-протоколів	13
1.4 Обґрунтування вибору технології IPsec для корпоративної мережі.....	17
РОЗДІЛ 2 ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ	21
2.1 Розробка трирівневої топології мережі.....	21
2.2 Вибір мережевого обладнання та програмних засобів.....	23
2.3 Розробка схеми адресації мережі.....	25
2.4 Аналіз потенційних загроз та вразливостей підсистеми.....	27
РОЗДІЛ 3 ВПРОВАДЖЕННЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ ...	30
3.1 Реалізація підсистеми захисту	30
3.2 Реалізація захищеного тунелю за допомогою IPsec VPN	33
3.3 Налаштування допоміжних систем захисту (TACACS+, Port Security, DHCP Snooping)...	36
3.4 Тестування працездатності та ефективності підсистеми захисту	39
ВИСНОВКИ.....	51
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	52
ДОДАТКИ.....	55

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AAA – Authentication, Authorization, and Accounting (Автентифікація, авторизація та облік)

ACL – Access Control List (Список контролю доступу)

AH – Authentication Header (Заголовок автентифікації в IPsec)

CLI – Command-Line Interface (Інтерфейс командного рядка)

DHCP – Dynamic Host Configuration Protocol (Протокол динамічної конфігурації хоста)

DNS – Domain Name System (Система доменних імен)

EIGRP – Enhanced Interior Gateway Routing Protocol (Пропрієтарний протокол динамічної маршрутизації Cisco)

ESP – Encapsulating Security Payload (Протокол інкапсуляції зашифрованих даних в IPsec)

IKE – Internet Key Exchange (Протокол обміну ключами в Інтернеті)

IPsec – Internet Protocol Security (Набір протоколів для забезпечення захисту даних на мережевому рівні)

LAN – Local Area Network (Локальна обчислювальна мережа)

OSI – Open Systems Interconnection (Модель взаємодії відкритих систем)

PSK – Pre-Shared Key (Попередньо узгоджений ключ)

RFC – Request for Comments (Документ, що описує технічні специфікації та стандарти Інтернету)

SSH – Secure Shell (Протокол безпечного віддаленого доступу)

Syslog – System Logging Protocol (Протокол для централізованого збору системних повідомлень)

TACACS+ – Terminal Access Controller Access-Control System Plus (Протокол централізованого управління доступом до мережевих пристроїв)

VLAN – Virtual Local Area Network (Віртуальна локальна мережа)

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. В умовах сучасних кіберзагроз та поширення географічно розподілених офісів, надійний захист каналів передачі корпоративних даних є критично важливим завданням. Ефективним рішенням цієї проблеми є використання віртуальних приватних мереж (VPN). Дана робота присвячена проектуванню та реалізації комплексної системи захисту на основі перевіреної часом технології IPsec та допоміжних механізмів безпеки.

Метою кваліфікаційної роботи є розробка та реалізація проекту захищеної корпоративної мережі на основі IPsec VPN, що забезпечить високий рівень конфіденційності, цілісності та доступності даних.

Для досягнення мети було поставлено завдання: проаналізувати сучасні VPN-технології для обґрунтування вибору IPsec, розробити архітектуру та схему адресації мережі, впровадити захищені тунелі, налаштувати допоміжні системи (TACACS+, Syslog, SSH, Port Security) та провести комплексне тестування розробленого рішення.

Об'єктом дослідження є процес забезпечення безпеки корпоративної мережі, а предметом — методи та засоби його реалізації, зокрема, технологія IPsec VPN та інтегровані з нею системи безпеки.

Методи дослідження включають аналіз технічної літератури, системне моделювання та комп'ютерну емуляцію в середовищі GNS3.

Практичне значення роботи полягає в тому, що її результати є готовим проектним рішенням, яке може слугувати шаблоном для побудови захищених мереж малих та середніх підприємств.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків та додатків, у яких послідовно розкрито етапи аналізу, проектування, впровадження та тестування розробленої системи.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 АНАЛІЗ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ З ВИКОРИСТАННЯМ VPN-ТЕХНОЛОГІЙ

1.1 Загальні принципи функціонування віртуальних приватних мереж (VPN)

Віртуальна приватна мережа (VPN, Virtual Private Network) — це технологія, яка забезпечує захищене з'єднання між двома або більше пристроями через незахищену мережу, таку як Інтернет [1]. Основна мета VPN — захистити дані, що передаються, шляхом створення зашифрованого тунелю між користувачем і VPN-сервером, що унеможливорює перехоплення чи модифікацію інформації сторонніми особами [2]. Завдяки VPN користувачі можуть працювати так, ніби вони знаходяться в одній приватній мережі, навіть якщо фізично розташовані в різних місцях, з'єднаних через публічний Інтернет [3]. Це особливо актуально для корпоративних мереж, де потрібен безпечний віддалений доступ до ресурсів компанії.

Ключові технології та компоненти VPN

Тунелювання

Основний принцип роботи VPN полягає у створенні захищеного тунелю — процесу інкапсуляції (обгортання) одного мережевого протоколу в інший [4]. Це дозволяє приховати реальний зміст даних від сторонніх осіб під час їх передачі через Інтернет. Поширені протоколи тунелювання включають:

- PPTP (Point-to-Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)
- IPsec (Internet Protocol Security)
- OpenVPN
- SSTP, WireGuard, IKEv2/IPsec [5]

Кожен із цих протоколів має свої особливості щодо рівня захисту, швидкості та сумісності з різними платформами.

- Шифрування

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

Для забезпечення конфіденційності VPN використовує сучасні алгоритми шифрування, такі як AES (Advanced Encryption Standard), який є галузевим стандартом для захисту даних у цифровому середовищі [6]. Шифрування гарантує, що навіть у разі перехоплення трафіку зломисник не зможе прочитати зміст переданої інформації без відповідного ключа.

- Автентифікація

Механізми автентифікації дозволяють переконатися, що до VPN підключаються лише авторизовані користувачі. Для цього застосовуються паролі, цифрові сертифікати, двофакторна автентифікація (2FA), а також біометричні дані (відбитки пальців, розпізнавання обличчя) [3]. Надійна автентифікація є критично важливою для запобігання несанкціонованому доступу до корпоративних ресурсів.

- Цілісність даних

Для гарантування того, що дані не були змінені під час передачі, використовуються криптографічні хеш-функції, зокрема HMAC (Hashed Message Authentication Code) на основі алгоритмів MD5, SHA-1, SHA-2 [3]. Якщо хеш-код отриманих даних не збігається з очікуваним, це свідчить про спробу їх модифікації, і такі дані відхиляються.

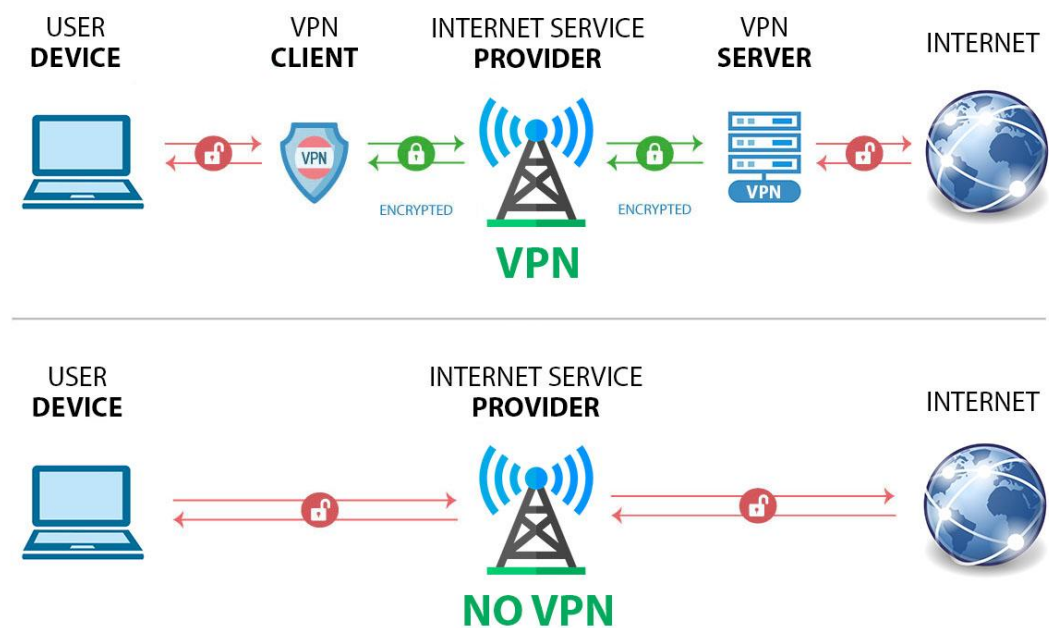


Рисунок 1.1 – Схема роботи VPN

Роботу VPN доцільно проілюструвати схемою, яка відображає основні етапи захищеного з'єднання (див. рис. 1.1).

Переваги використання VPN у корпоративному середовищі

Безпечний віддалений доступ. VPN дозволяє співробітникам безпечно підключатися до корпоративної мережі з будь-якої точки світу, забезпечуючи захист даних навіть у публічних Wi-Fi мережах.

Захист конфіденційних даних. Шифрування трафіку зменшує ризик витоку чутливої інформації компанії, навіть якщо передача відбувається через незахищені канали.

Подолання географічних обмежень. VPN надає можливість отримувати доступ до корпоративних ресурсів, які можуть бути заблоковані або обмежені в окремих регіонах.

У сучасних умовах активного зростання кіберзагроз та масового переходу до віддаленої роботи VPN залишається одним із ключових засобів захисту корпоративних даних. Постійний розвиток технологій VPN, впровадження нових протоколів і вдосконалення стандартів шифрування забезпечують високий рівень безпеки та адаптацію до нових викликів у сфері кібербезпеки.

1.2 Класифікація VPN за архітектурою та призначенням (Remote Access, Site-to-Site)

У сучасних корпоративних мережах VPN-технології поділяються на два основних типи відповідно до архітектури та призначення: VPN з віддаленим доступом (Remote Access VPN) та VPN типу "сайт-до-сайту" (Site-to-Site VPN). Кожен із цих типів вирішує специфічні задачі інформаційної безпеки та організації доступу до корпоративних ресурсів [7].

VPN з віддаленим доступом (Remote Access VPN)

Remote Access VPN орієнтований на забезпечення захищеного підключення окремих користувачів (співробітників, підрядників) до внутрішньої корпоративної

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

мережі. Найбільш поширений сценарій — співробітник працює з дому, у відрядженні чи з публічного Wi-Fi і потребує безпечного доступу до корпоративних ресурсів.

Користувач встановлює на свій пристрій VPN-клієнт, який ініціює зашифрований тунель до VPN-сервера, розташованого у корпоративній мережі. Весь трафік між пристроєм користувача та сервером шифрується, що гарантує конфіденційність і цілісність даних [8].



Рисунок 1.2 – Remote Access VPN

VPN "сайт-до-сайту" (Site-to-Site VPN)

Site-to-Site VPN призначений для об'єднання двох або більше локальних мереж (наприклад, центрального офісу та філій) в єдину захищену корпоративну інфраструктуру. Це особливо актуально для організацій із географічно розподіленою структурою [7].

На кожній стороні встановлюється VPN-шлюз (зазвичай це маршрутизатор або спеціалізований пристрій з підтримкою VPN), які автоматично встановлюють і підтримують постійний зашифрований тунель між собою. Користувачі всередині кожної локальної мережі працюють із ресурсами іншої мережі так, ніби вони знаходяться в одній фізичній мережі, без необхідності додаткового програмного забезпечення чи ручного підключення.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

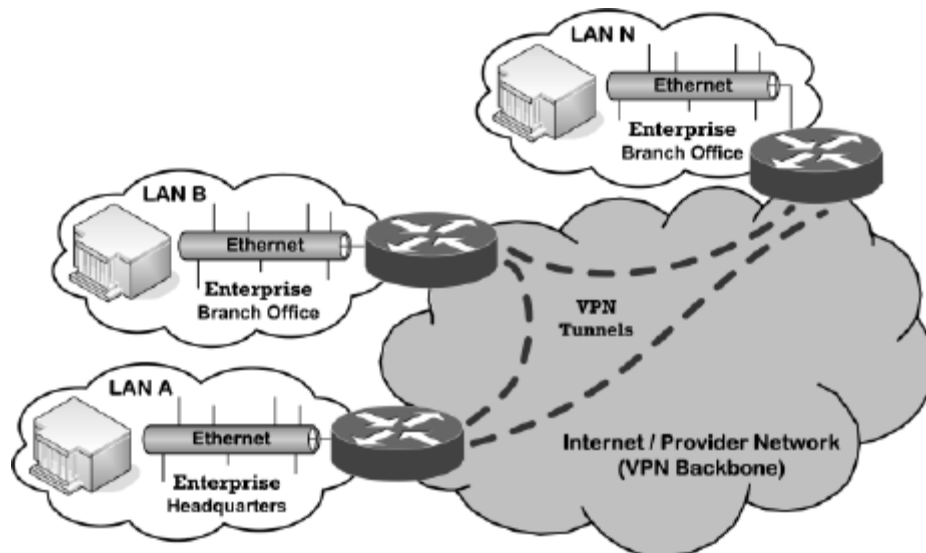


Рисунок 1.3 – Архітектура Site-to-Site VPN

У межах цієї кваліфікаційної роботи буде реалізовано саме VPN типу "сайт-до-сайту", оскільки це оптимальне рішення для об'єднання кількох офісів компанії в єдину захищену мережу.

Чітке розмежування між Remote Access VPN та Site-to-Site VPN дозволяє обрати оптимальну архітектуру відповідно до потреб організації. Вибір Site-to-Site VPN у цьому проєкті зумовлений необхідністю інтеграції віддалених офісів у єдину захищену інфраструктуру з мінімальними зусиллями для кінцевих користувачів.

1.3 Огляд та порівняльний аналіз сучасних VPN-протоколів

Вибір технології VPN є критично важливим етапом для побудови захищеної корпоративної мережі, оскільки саме від нього залежить баланс між рівнем безпеки, продуктивністю та складністю експлуатації інфраструктури. Сьогодні ринок VPN-рішень пропонує низку протоколів, однак у корпоративному сегменті найбільшого поширення набули три:

- IPsec — галузевий стандарт із широкою підтримкою мережевого обладнання;
- OpenVPN — універсальне програмне рішення з відкритим кодом;
- WireGuard — сучасний високопродуктивний протокол із мінімалістичною архітектурою.

IPsec (Internet Protocol Security) — це не окремий протокол, а цілий фреймворк, який працює на мережевому рівні моделі OSI (Layer 3) і забезпечує захист IP-пакетів шляхом шифрування, автентифікації та контролю цілісності [10].

Основні компоненти IPsec:

- IKE (Internet Key Exchange): протокол, який відповідає за автоматизований обмін ключами, автентифікацію сторін та узгодження параметрів захисту. Сучасна версія IKEv2 відзначається підвищеною стійкістю до атак та кращою продуктивністю.
- ESP (Encapsulating Security Payload): забезпечує шифрування та цілісність даних, що передаються, захищаючи їх від несанкціонованого доступу та модифікації.
- AH (Authentication Header): використовується для контролю цілісності та автентифікації IP-пакетів, але не забезпечує шифрування (зараз використовується рідко, оскільки ESP підтримує обидві функції).

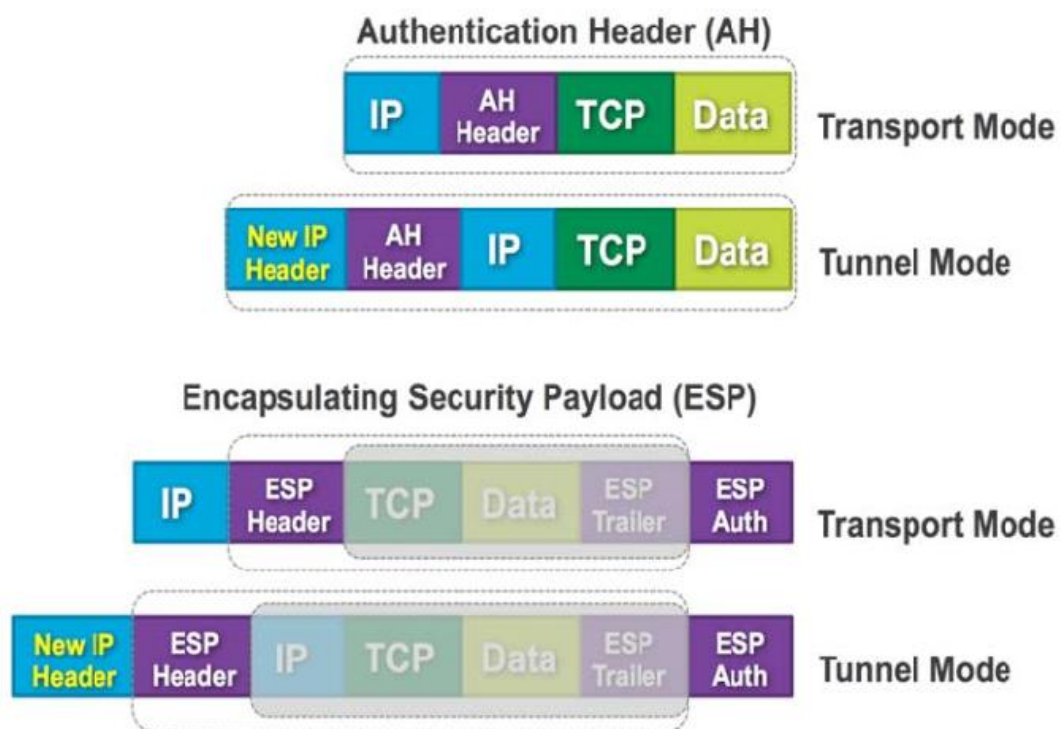


Рисунок 1.4 – Методи реалізації інкапсуляції IPsec-заголовка

Режими роботи:

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

Тунельний режим (Tunnel Mode): використовується для побудови Site-to-Site VPN, коли весь IP-пакет інкапсулюється та шифрується для передачі між VPN-шлюзами.

Транспортний режим (Transport Mode): застосовується для захисту трафіку між окремими пристроями, коли шифрується лише корисне навантаження IP-пакета.

IPsec підтримується більшістю професійного мережевого обладнання (Cisco, Juniper, Huawei та ін.), що дозволяє досягати високої продуктивності завдяки апаратному прискоренню шифрування. Це робить IPsec оптимальним вибором для корпоративних Site-to-Site VPN [9].

OpenVPN — це програмний VPN-протокол із відкритим кодом, який використовує бібліотеку OpenSSL та протоколи SSL/TLS для створення захищених тунелів [11].

OpenVPN працює на транспортному (Layer 4) та сеансовому (Layer 5) рівнях моделі OSI, що дозволяє йому використовувати стандартні порти (наприклад, TCP/UDP 443) і легко проходити крізь NAT та фаєрволи. Протокол підтримує широкий спектр алгоритмів шифрування (AES-256, Blowfish тощо) та аутентифікації (сертифікати, ключі, паролі) [12].

Сильні сторони:

- Висока гнучкість налаштувань — можливість тонкого налаштування політик доступу, маршрутів, параметрів шифрування.
- Кросплатформеність — підтримка Windows, Linux, macOS, iOS, Android.
- Потужна спільнота розробників і користувачів, активна підтримка та регулярні оновлення.

Вимагає встановлення клієнтського програмного забезпечення, не завжди підтримується апаратно на мережевих пристроях, що може обмежувати продуктивність у великих корпоративних мережах.

WireGuard — це сучасний VPN-протокол, який вирізняється мінімалістичною архітектурою та високою продуктивністю [14].

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

- Мала кодова база (близько 4000 рядків коду) — спрощує аудит безпеки, знижує ризик вразливостей.
- Сучасні криптографічні алгоритми — ChaCha20 для шифрування, Poly1305 для автентифікації, Curve25519 для обміну ключами, BLAKE2s для хешування [13].
- Інтеграція на рівні ядра ОС — забезпечує максимальну швидкість обробки трафіку та низькі затримки.
- Простота налаштування — конфігурація займає лічені хвилини, що особливо цінується адміністраторами.

WireGuard ще не став повноцінним галузевим стандартом, його підтримка на професійному мережевому обладнанні (особливо Cisco) лише набирає обертів. Також відсутня нативна підтримка динамічних IP-адрес та деяких корпоративних функцій.

Таблиця 1.1

Порівняльна таблиця сучасних VPN-протоколів

Критерій	IPsec	OpenVPN	WireGuard
Безпека	Висока (AES, SHA, IKEv2)	Висока (SSL/TLS, AES-256, сертифікати)	Висока (ChaCha20, Curve25519)
Продуктивність	Висока (апаратне прискорення)	Середня/Висока	Дуже висока (ядро ОС, мінімалізм)
Складність налаштування	Висока (особливо для Site-to-Site)	Середня	Низька
Сумісність	Дуже висока (стандарт для роутерів, Cisco)	Середня (потрібен клієнт)	Зростає (ще не стандарт для Cisco)
Гнучкість	Висока (гранулярні політики)	Дуже висока (гнучке ПЗ)	Середня (мінімалізм, простота)
Підтримка NAT	Обмежена (NAT Traversal)	Відмінна	Хороша (простий UDP)

Проведений аналіз демонструє, що кожен із розглянутих VPN-протоколів має свої переваги та обмеження. WireGuard — ідеальний для сучасних, простих і високопродуктивних рішень, але ще не має повної підтримки на професійному обладнанні. OpenVPN — універсальний і гнучкий, але поступається IPsec у продуктивності та сумісності з мережевим залізом. IPsec — галузевий стандарт із нативною підтримкою на більшості корпоративних маршрутизаторів (зокрема Cisco), що забезпечує максимальну продуктивність, масштабованість і безпеку для Site-to-Site VPN.

Проведений аналіз закладає підґрунтя для наступного підрозділу, де буде детально обґрунтовано вибір саме IPsec для побудови захищеної корпоративної мережі на базі обладнання Cisco.

1.4 Обґрунтування вибору технології IPsec для корпоративної мережі

Вибір технологічної платформи для реалізації віртуальної приватної мережі є фундаментальним архітектурним рішенням, що безпосередньо впливає на безпеку, продуктивність, масштабованість та керованість усієї корпоративної інфраструктури. На основі проведеного в попередньому підрозділі аналізу, для реалізації поставлених у даній кваліфікаційній роботі завдань — побудови захищеного, стабільного та продуктивного Site-to-Site з'єднання на базі обладнання Cisco — було обрано фреймворк IPsec (Internet Protocol Security). Це рішення ґрунтується на низці прагматичних інженерних аргументів.

У корпоративному середовищі, де безперервність бізнес-процесів є найвищим пріоритетом, надійність технології має першочергове значення. IPsec є зрілим, перевіреним десятиліттями фреймворком, стандартизованим IETF (Internet Engineering Task Force) [15]. Його специфікації детально описані в численних документах RFC, що гарантує передбачувану поведінку та високий рівень сумісності між обладнанням різних виробників. Для інженера це означає мінімізацію ризиків, пов'язаних із впровадженням, та прогнозовану експлуатацію. На відміну від новітніх протоколів, як-от WireGuard, IPsec має величезну історію розгортань у найвищих інфраструктурах світу, що підтверджує його промислову надійність.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

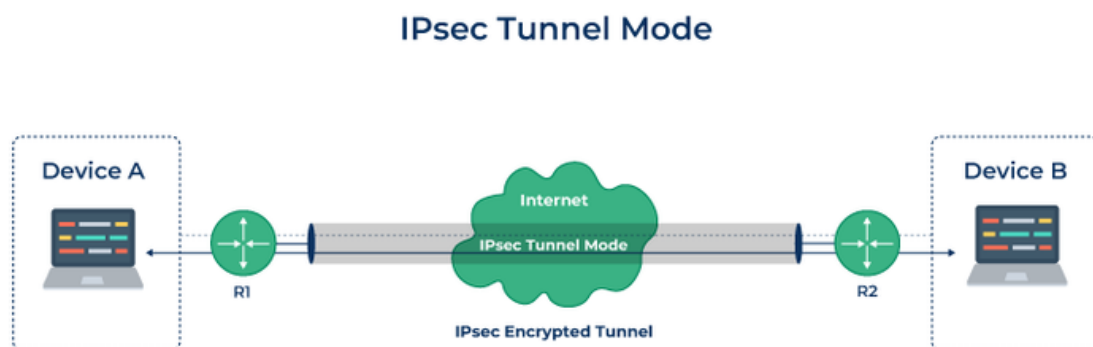


Рисунок 1.5 – Модель інтеграції IPsec

Ключовою перевагою IPsec у рамках даного проєкту є його глибока, нативна інтеграція в операційну систему Cisco IOS [16]. Це не сторонній програмний модуль, а невіддільна частина функціоналу, що забезпечує низку переваг:

Маршрутизатори корпоративного класу, такі як обраний у проєкті Cisco 7200 Series, оснащуються спеціалізованими криптографічними модулями [16]. Ці модулі беруть на себе виконання ресурсомістких операцій шифрування (AES) та хешування (SHA), розвантажуючи центральний процесор (CPU) маршрутизатора. Це дозволяє досягти гігабітних швидкостей обробки VPN-трафіку без деградації продуктивності інших сервісів. Програмні рішення, зокрема OpenVPN, виконують криптографічні операції на CPU, що при високих навантаженнях неминуче призводить до зростання затримок та падіння пропускної здатності [17].

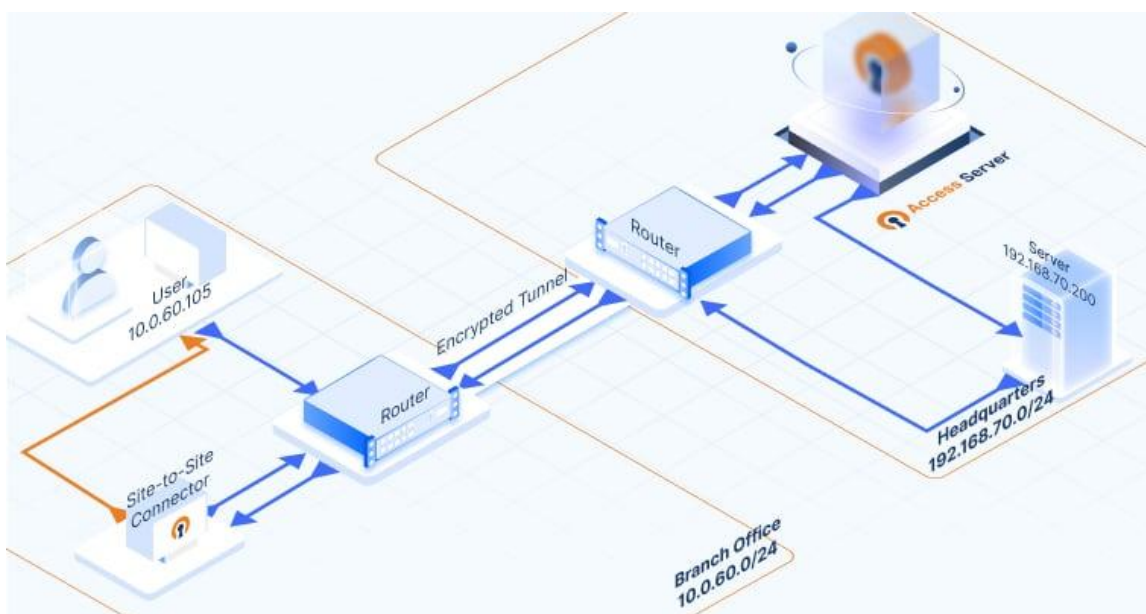


Рисунок 1.6 – Модель інтеграції OpenVPN

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

Функціонал IPsec безшовно взаємодіє з іншими технологіями Cisco IOS, такими як динамічна маршрутизація (EIGRP, OSPF), якість обслуговування (QoS) та механізми безпеки (Zone-Based Firewall, ACL) [16]. Це дозволяє будувати комплексні, керовані та гнучкі політики безпеки.

Вибір IPsec також обґрунтований обмеженнями альтернативних протоколів для вирішення поставленої задачі:

Попри свою надзвичайну гнучкість та здатність легко долати NAT, його головним недоліком у сценарії Site-to-Site є відсутність можливості використання апаратного прискорення на маршрутизаторах Cisco. Для каналу зв'язку між офісами, де очікується значний трафік, це стало б критичним «вузьким місцем», що обмежує потенціал мережевої інфраструктури [17].

Це технологічно прогресивний протокол, що демонструє видатну продуктивність та простоту. Проте його основна проблема — недостатня зрілість екосистеми в корпоративному сегменті. На момент виконання проєкту його нативна підтримка на багатьох платформах Cisco IOS є обмеженою або експериментальною [17]. Робити ставку на таку технологію для побудови основи корпоративної безпеки є невиправданим інженерним ризиком.

Таким чином, вибір IPsec є виваженим та технічно обґрунтованим рішенням. Він продиктований не простотою, а вимогами до стабільності, максимальної продуктивності на обраному обладнанні та можливостями глибокої інтеграції в корпоративну інфраструктуру. Для побудови надійного Site-to-Site VPN-тунелю на платформі Cisco фреймворк IPsec залишається оптимальним та найбільш професійним вибором.

Висновок до першого розділу

У першому розділі було проведено комплексний теоретичний аналіз сучасних технологій побудови віртуальних приватних мереж (VPN), що є фундаментом для подальшого проєктування захищеної корпоративної інфраструктури.

Було розглянуто ключові принципи функціонування VPN, зокрема механізми тунелювання, шифрування, автентифікації та забезпечення цілісності даних, які є

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

основою для створення безпечних каналів зв'язку. Проведено класифікацію VPN-рішень, де виділено та описано дві основні архітектури: VPN з віддаленим доступом (Remote Access) для окремих користувачів та VPN типу «сайт-до-сайту» (Site-to-Site) для об'єднання локальних мереж. Встановлено, що для завдань даної роботи найбільш відповідною є архітектура Site-to-Site.

Виконано порівняльний аналіз трьох провідних VPN-протоколів: IPsec, OpenVPN та WireGuard. Аналіз показав, що кожен із них має свої сильні сторони: IPsec вирізняється статусом надійного галузевого стандарту з широкою підтримкою обладнання, OpenVPN — високою гнучкістю та кросплатформеністю, а WireGuard — максимальною продуктивністю та простотою.

На основі проведеного аналізу було детально обґрунтовано вибір фреймворку IPsec як оптимального технологічного рішення для даного проєкту. Ключовими факторами, що зумовили цей вибір, стали його нативна інтеграція з обладнанням Cisco, можливість використання апаратного прискорення для досягнення високої пропускної здатності та доведена роками стабільність у корпоративних середовищах. Таким чином, теоретичне підґрунтя, закладене в цьому розділі, дозволяє перейти до наступного етапу — практичного проєктування захищеної корпоративної мережі на основі обраної технології.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Розробка трирівневої топології мережі

Основою для проєктування будь-якої надійної, масштабованої та безпечної корпоративної мережі є вибір правильної топології. Для даної кваліфікаційної роботи за основу було взято класичну трирівневу ієрархічну модель Cisco, яка є галузевим стандартом і складається з рівнів доступу, розподілу та ядра. Ця архітектура забезпечує високий рівень гнучкості, відмовостійкості та керованості.

З огляду на розмір та потреби симульованої організації, в проєкті застосовано варіацію цієї моделі — архітектуру зі схлопнутим ядром та розподілом (Collapsed Core/Distribution Model). Такий підхід дозволяє зменшити кількість необхідного обладнання та спростити управління, зберігаючи при цьому ключові переваги ієрархічного дизайну.

Загальну топологію спроектованої корпоративної мережі, що складається з центрального офісу та філій, наведено на рис. 2.1.

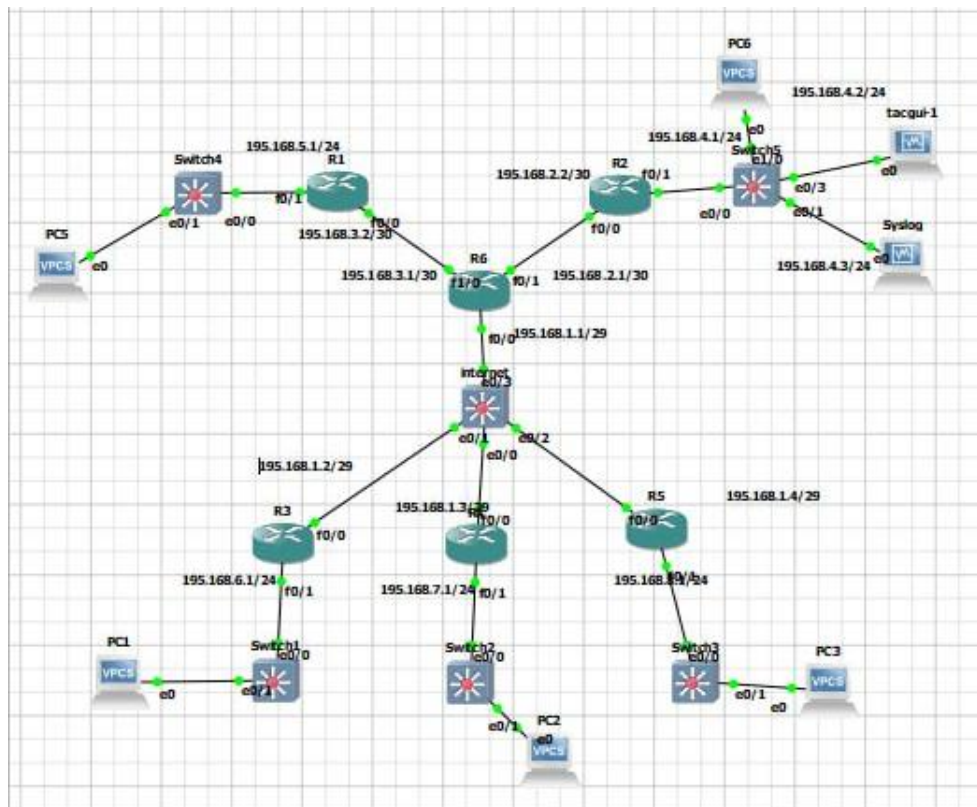


Рисунок 2.1 – Загальна топологія спроектованої корпоративної мережі

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

Рівень ядра (Core Layer)

Ядро мережі, що відповідає за високошвидкісну та надійну комутацію трафіку, формується групою взаємопов'язаних маршрутизаторів: R3, R4, R5, R6 та центрального маршрутизатора Internet. Вони створюють відмовостійку магістраль, що забезпечує зв'язок між центральним офісом (верхня частина схеми) та віддаленими філіями (нижня частина).

Рівень розподілу (Distribution Layer)

Функції цього рівня реалізовані по-різному для окремих сегментів мережі у центральному офісі, маршрутизатори R1 та R2 виконують класичну роль рівня розподілу, агрегуючи трафік від комутаторів доступу та підключаючись до ядра через маршрутизатор R6.

У філіях рівні ядра та розподілу є схлопнутими. Маршрутизатори R3, R4 та R5 виконують подвійну функцію, вони є частиною магістралі (ядра) і водночас безпосередньо служать точкою агрегації для своїх комутаторів доступу.

Рівень доступу (Access Layer)

Цей рівень представлений комутаторами Switch1, Switch2, Switch3, Switch4 та Switch5. Вони забезпечують підключення до мережі кінцевих пристроїв, таких як робочі станції (PC1, PC2, PC3), а також серверної інфраструктури в центральному офісі:

Сервер Tacs+ (195.168.4.2/24): Використовується для централізованої автентифікації, авторизації та обліку (AAA) адміністраторів.

Сервер Syslog (195.168.4.3/24): Призначений для централізованого збору та зберігання журналів подій з усіх мережевих пристроїв.

Таким чином, розроблена ієрархічна архітектура зі схлопнутим ядром є реалістичним та економічно ефективним рішенням, яке створює логічно структуровану, керовану та захищену інфраструктуру. Вона слугує міцним фундаментом для подальшого впровадження політик безпеки та налаштування захищених VPN-тунелів на основі технології IPsec.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

2.2 Вибір мережевого обладнання та програмних засобів

Для побудови надійної, продуктивної та безпечної корпоративної мережі критично важливим є правильний вибір апаратного та програмного забезпечення. У рамках даного проєкту було обрано обладнання фірми Cisco, яка є світовим лідером у галузі мережевих технологій, а також спеціалізовані програмні засоби для реалізації функцій управління та моніторингу.

Для виконання функцій на рівні ядра та розподілу, а також у ролі VPN-шлюзів, було обрано маршрутизатор Cisco 7200 Series [18]. Цей вибір обґрунтований наступними характеристиками:

Висока продуктивність, маршрутизатор забезпечує високу пропускну здатність, необхідну для швидкої комутації трафіку між центральним офісом та філіями.

Розширений функціонал, підтримує широкий спектр протоколів маршрутизації, зокрема EIGRP, який використовується в проєкті для обміну маршрутною інформацією.

Підтримка IPsec, найважливішою перевагою є його потужна підтримка фреймворку IPsec. Cisco 7200 дозволяє створювати складні та безпечні Site-to-Site VPN-тунелі, а також підтримує апаратне прискорення криптографічних операцій, що є критичним для забезпечення високої продуктивності зашифрованого трафіку.



Рисунок 2.2 – Маршрутизатор Cisco 7200 Series

На рівні доступу для підключення кінцевих пристроїв та серверів використовується комутатор Cisco Catalyst WS-C2960-24TT-L [19].

Надійність та поширеність, це надійний комутатор корпоративного класу, який є стандартом для побудови мереж доступу.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

Щільність портів, наявність 24 портів Fast Ethernet забезпечує достатню кількість підключень для потреб спроектованої мережі.

Функції безпеки на рівні 2, комутатор підтримує ключові технології безпеки, які будуть налаштовані в рамках роботи: Port Security (для захисту від несанкціонованого підключення), VLAN (для сегментації трафіку) та DHCP Snooping (для протидії атакам на DHCP-сервер).



Рисунок 2.3 – Комутатор Cisco Catalyst WS-C2960-24TT-L

Для реалізації функцій централізованого управління, моніторингу та автентифікації було розгорнуто два віртуальні сервери.

Сервер TACACS+. Для централізованої автентифікації, авторизації та обліку (AAA) адміністративного доступу до мережевих пристроїв використовується програмний комплекс TacsacsGUI [20]. Він надає зручний веб-інтерфейс для керування обліковими записами адміністраторів, групами пристроїв та політиками доступу, що значно підвищує рівень безпеки та керованості інфраструктури.

Сервер Syslog. Збір та аналіз журналів подій з маршрутизаторів та комутаторів є критично важливим для моніторингу стану мережі та розслідування інцидентів. Для цього в проєкті розгорнуто Syslog-сервер на базі операційної системи Windows 10.

Таким чином, обрана комбінація мережевого обладнання Cisco та спеціалізованих серверних рішень створює потужну, гнучку та безпечну платформу, що повністю відповідає цілям та завданням даної кваліфікаційної роботи

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

2.3 Розробка схеми адресації мережі

Правильно спланована схема IP-адресації є критично важливим елементом для забезпечення керованості, безпеки та масштабованості корпоративної мережі. Логічна та ієрархічна структура адресації спрощує налаштування протоколів маршрутизації, реалізацію політик безпеки за допомогою списків контролю доступу (ACL) та подальше розширення інфраструктури.

Для даного проєкту було розроблено структуровану схему на основі IPv4. Хоча в проєкті використовуються адреси з діапазону 195.168.0.0, який формально належить до публічних, у лабораторних умовах він використовується як приватний. У реальному корпоративному середовищі для внутрішніх мереж слід використовувати діапазони, визначені в RFC 1918 (наприклад, 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).

Основні принципи розробленої схеми:

Використання VLSM (Variable Length Subnet Masking): Для ефективного використання адресного простору застосовано маски змінної довжини.

Адресація локальних мереж (LAN): Сегменти мережі, де знаходяться кінцеві користувачі та сервери, отримали маску /24 (255.255.255.0). Це забезпечує до 254 унікальних IP-адрес у кожному сегменті, що дає значний запас для майбутнього зростання.

Адресація глобальних з'єднань (WAN): Для з'єднань типу «точка-точка» (Point-to-Point) між маршрутизаторами використано маску /30 (255.255.255.252). Це є найкращою практикою, оскільки такі з'єднання потребують лише дві IP-адреси, що дозволяє суттєво економити адресний простір.

Детальний план розподілу адресного простору наведено в таблицях нижче.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 2.1

Адресація локальних мереж (LAN)

Назва сегмента	Адреса мережі	Маска підмережі	Опис
Central Office - Servers	195.168.4.0	255.255.255.0 (/24)	Мережа з серверами Tacacs+ та Syslog
Central Office - Users	195.168.5.0	255.255.255.0 (/24)	Мережа для робочих станцій центрального офісу
Branch 1 (PC1)	195.168.6.0	255.255.255.0 (/24)	Мережа для робочих станцій першої філії
Branch 2 (PC2)	195.168.7.0	255.255.255.0 (/24)	Мережа для робочих станцій другої філії
Branch 3 (PC3)	195.168.8.0	255.255.255.0 (/24)	Мережа для робочих станцій третьої філії

Таблиця 2.2

Адресація з'єднань «точка-точка» (Point-to-Point)

З'єднання	Адреса мережі	Маска підмережі	IP-адреса (При-стрій 1)	IP-адреса (При-стрій 2)
R6 ↔ Internet	195.168.1.0	255.255.255.248 (/29)	195.168.1.1 (R6)	-
R2 ↔ R6	195.168.2.0	255.255.255.252 (/30)	195.168.2.1 (R2)	195.168.2.2 (R6)
R1 ↔ R6	195.168.3.0	255.255.255.252 (/30)	195.168.3.1 (R1)	195.168.3.2 (R6)
R3 ↔ Internet	195.168.1.0	255.255.255.248 (/29)	195.168.1.2 (R3)	-
R3 ↔ Internet	195.168.1.0	255.255.255.248 (/29)	195.168.1.3 (R3)	-
R5 ↔ Internet	195.168.1.0	255.255.255.248 (/29)	195.168.1.4 (R5)	-

Для прикладу, параметри адресації для серверної мережі центрального офісу представлено в таблиці 2.3.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

Детальні параметри адресації мережі Central Office – Servers

Параметр	Значення
Адреса мережі	195.168.4.0
Маска підмережі	255.255.255.0 (/24)
Широкомовна адреса	195.168.4.255
Адреса шлюзу	195.168.4.1 (інтерфейс на R2)
Діапазон доступних адрес	195.168.4.1 - 195.168.4.254
Статичні адреси серверів	195.168.4.2 (Tacacs+), 195.168.4.3 (Syslog)

Розроблена схема є логічною, ієрархічною та ефективною з точки зору використання адресного простору. Вона створює прозору та керовану структуру, яка є необхідною умовою для успішної реалізації протоколів маршрутизації та політик безпеки на наступних етапах роботи.

2.4 Аналіз потенційних загроз та вразливостей підсистеми

Проектування надійної мережевої інфраструктури вимагає не тільки правильного вибору топології та обладнання, але й глибокого розуміння потенційних загроз та вразливостей. Навіть найсучасніші технології можуть бути скомпрометовані, якщо не враховувати вектори атак, притаманні їм. Мета цього підрозділу — ідентифікувати потенційні загрози для ключових протоколів та технологій, що використовуються в проєкті, та визначити превентивні заходи для їх нейтралізації. У спроектованій мережі використовуються наступні технології, що потребують аналізу безпеки: EIGRP, SSH, DHCP, Port Security, TACACS+ та ключова технологія для захисту каналів — IPsec.

Протокол динамічної маршрутизації EIGRP, що є основою для обміну маршрутною інформацією, вразливий до фальсифікації маршрутів та пасивного прослуховування. Успішна атака може призвести до порушення зв'язності, перенаправлення трафіку через пристрій зловмисника для реалізації атаки «людина посередині» (Man-in-the-Middle), або створення «чорних дір» (black-holing) для відмови в обслуговуванні. Для протидії цим загрозам у проєкті буде реалізовано механізм автентифікації EIGRP, що гарантує прийняття оновлень лише від довірених сусідів.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Протокол SSH, що використовується для безпечного віддаленого адміністрування, є частою ціллю для атак перебору пароля (brute-force) та атак «людина посередині». Успіх таких атак рівнозначний повному компрометуванню мережі. Для захисту буде примусово використовуватись SSH версії 2, складні паролі, а також буде налаштовано обмеження кількості спроб входу та списки доступу (ACL), що дозволяють підключення лише з довірених IP-адрес.

Автоматизація видачі IP-адрес за допомогою DHCP створює ризики атак типу DHCP Spoofing та DHCP Starvation. Ці атаки можуть призвести до перехоплення трафіку клієнтів або відмови в обслуговуванні для нових пристроїв. Для захисту на комутаторах рівня доступу буде налаштовано DHCP Snooping, що дозволить фільтрувати шкідливі DHCP-повідомлення з неавторизованих портів.

На фізичному рівні загрози включають несанкціоноване підключення до мережі та атаки на переповнення таблиці MAC-адрес. Наслідком може стати надання доступу до мережі стороннім особам або можливість прослуховування трафіку. Прямим заходом протидії є технологія Port Security, яка буде налаштована для обмеження кількості MAC-адрес на кожному порту з автоматичним блокуванням у разі порушення.

Централізована система автентифікації TACACS+ також може стати ціллю, зокрема DoS-атак або атак на компрометацію спільного секретного ключа. Це може призвести до неможливості керування пристроями або компрометації облікових даних. Для мінімізації цих ризиків сервер TACACS+ буде розміщено у захищеному сегменті мережі, а для зв'язку з пристроями використовуватиметься довгий та складний спільний секретний ключ.

Ключова технологія захисту каналів, IPsec, також має свої вразливості. Основні загрози включають атаки перебору на слабкі попередньо узгоджені ключі (PSK) в IKE Phase 1, використання застарілих криптографічних алгоритмів та DoS-атаки на VPN-шлюз. Успішна експлуатація цих вразливостей може призвести до розшифрування конфіденційного трафіку та несанкціонованого доступу до внутрішніх мереж. Тому в проєкті буде реалізовано надійну політику IPsec: використання дов-

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

гих, випадково згенерованих ключів PSK; застосування сильних сучасних алгоритмів (AES-256 для шифрування, SHA-256 для цілісності, DH Group 14); налаштування ACL для дозволу IKE (UDP 500) та ESP трафіку тільки між довіреними IP-адресами шлюзів (R6, R3, R4, R5).

Висновок до другого розділу

У другому розділі було виконано комплексне проєктування захищеної корпоративної мережі, що заклало архітектурний та логічний фундамент для її подальшої реалізації.

На першому етапі було розроблено мережеву топологію на основі ієрархічної моделі Cisco зі схлопнутим ядром та розподілом, що є оптимальним рішенням для мережі такого масштабу. Далі було обґрунтовано вибір мережевого обладнання: маршрутизаторів **Cisco 7200**, що забезпечують високу продуктивність та підтримку IPsec, і комутаторів **Cisco Catalyst 2960**, які надають необхідні функції безпеки на рівні доступу. Для централізованого управління та моніторингу було обрано сервери **Tacacs+** та **Syslog**.

На основі обраної топології було розроблено детальну та ефективну схему IP-адресації з використанням VLSM, яка передбачає поділ на підмережі для LAN-сегментів та Point-to-Point з'єднань. На завершення було проведено ретельний аналіз потенційних загроз та вразливостей для всіх ключових технологій проєкту (EIGRP, IPsec, SSH, DHCP, TACACS+, Port Security) та визначено конкретні заходи протидії, які будуть реалізовані на етапі впровадження.

Таким чином, у даному розділі було створено повний технічний проєкт мережі, що включає логічну і фізичну структуру, специфікацію обладнання, план адресації та стратегію безпеки. Це дозволяє перейти до наступного етапу — практичної реалізації та тестування спроектованої підсистеми захисту.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 ВПРОВАДЖЕННЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ

3.1 Реалізація підсистеми захисту

Цей розділ присвячений практичній реалізації спроектованої в попередньому розділі архітектури. Першим і найважливішим етапом є налаштування базової конфігурації мережевого обладнання та серверів, що є фундаментом для всіх подальших політик безпеки. Цей процес включає призначення статичних IP-адрес ключовим серверам, конфігурацію інтерфейсів маршрутизаторів, запуск протоколу динамічної маршрутизації для забезпечення зв'язності та налаштування служби DHCP для автоматизації видачі адрес кінцевим пристроям.

Для стабільної роботи централізованих сервісів, таких як TACACS+ та Syslog, їм необхідно призначити статичні IP-адреси. Це гарантує, що мережеві пристрої завжди зможуть до них звернутися. Для прикладу, на віртуальній машині з ОС Windows 10, де розгорнуто сервер Syslog, були виконані стандартні налаштування мережевого адаптера, як показано на рис. 3.1.

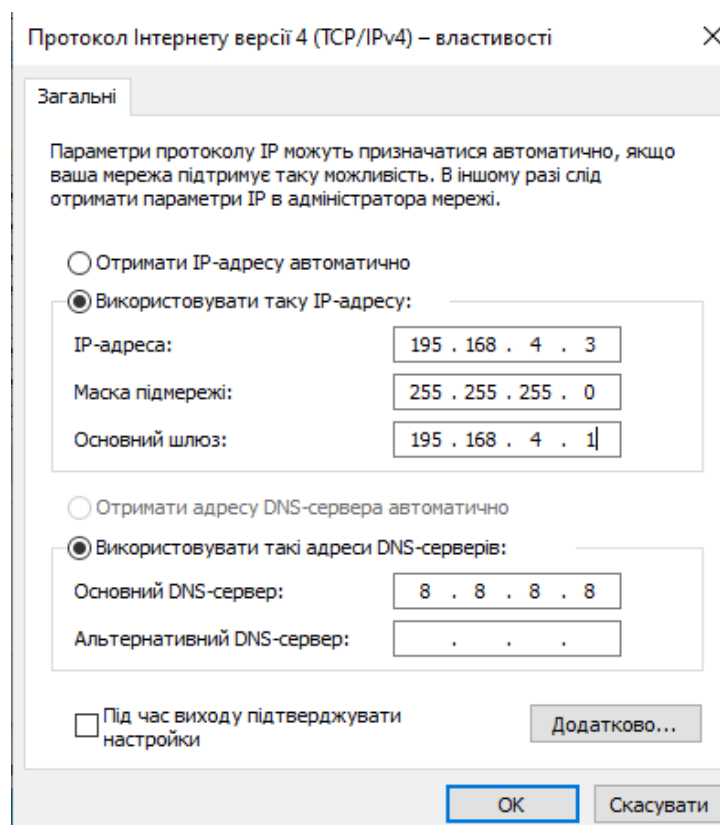


Рисунок 3.1 – Призначення статичної IP-адреси серверу Syslog

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

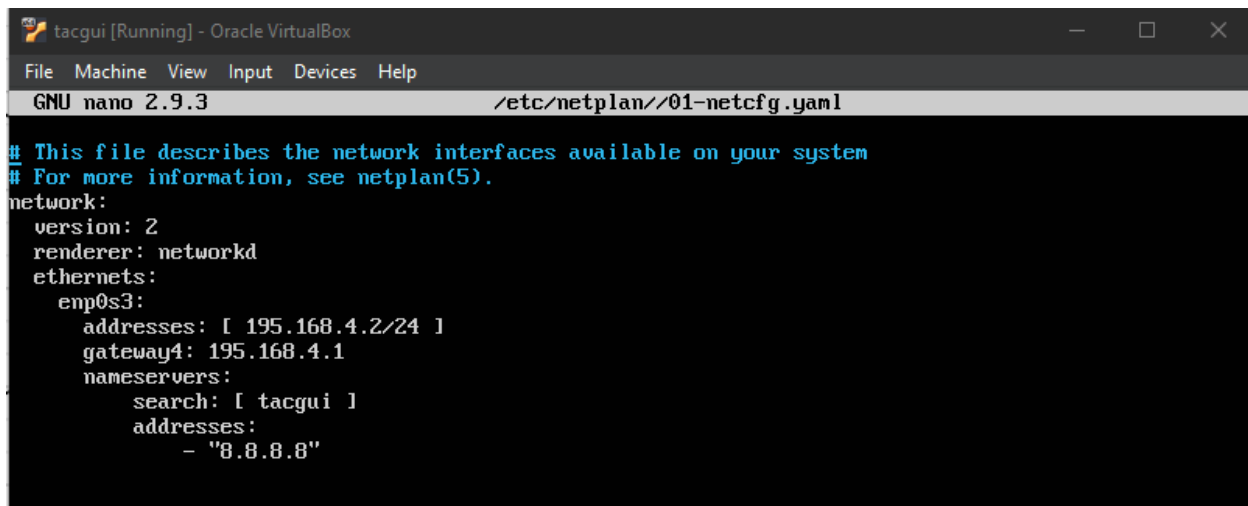


Рисунок 3.2 – Призначення статичної IP-адреси серверу Тасас

Наступним кроком є конфігурація маршрутизаторів. Цей процес включає призначення IP-адрес на їхні інтерфейси згідно з розробленою схемою адресації (підрозділ 2.3) та налаштування протоколу динамічної маршрутизації. У якості такого протоколу було обрано EIGRP з номером автономної системи 100 за його швидку збіжність та ефективність у мережах Cisco.

Нижче наведено приклад базової конфігурації для одного з маршрутизаторів ядра, що демонструє процес налаштування IP-адрес на інтерфейсах та активацію EIGRP для анонсування підключених до нього мереж.

R6# conf t

Enter configuration commands, one per line. End with CNTL/Z.

! Налаштування IP-адрес на інтерфейсах

R6(config)# interface f0/0

R6(config-if)# ip address 195.168.1.1 255.255.255.252

R6(config-if)# no shut

R6(config-if)# exit

R6(config)# interface f0/1

R6(config-if)# ip address 195.168.2.2 255.255.255.252

R6(config-if)# no shut

R6(config-if)# exit

R6(config)# interface f1/0

R6(config-if)# ip address 195.168.3.2 255.255.255.252

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R6(config-if)# no shut
R6(config-if)# exit
! Запуск процесу EIGRP та анонсування мереж
R6(config)# router eigrp 100
R6(config-router)# network 195.168.1.0 0.0.0.3
R6(config-router)# network 195.168.2.0 0.0.0.3
R6(config-router)# network 195.168.3.0 0.0.0.3
R6(config-router)# no auto-summary
R6(config-router)# exit

```

Для автоматизації процесу отримання IP-адрес кінцевими пристроями у філіях налаштовується служба DHCP. Це дозволяє уникнути ручної конфігурації кожної робочої станції та спрощує адміністрування мережі. Приклад налаштування DHCP-пулу для мережі першої філії (195.168.6.0/24) на маршрутизаторі R3:

```

R3# conf t
Enter configuration commands, one per line. End with CNTL/Z.
! Налаштування DHCP-пулу для локальної мережі філії
R3(config)# ip dhcp pool POOL_R3
R3(dhcp-config)# network 195.168.6.0 255.255.255.0
R3(dhcp-config)# default-router 195.168.6.1
R3(dhcp-config)# dns-server 8.8.8.8
R3(dhcp-config)# lease 1 0 0
R3(dhcp-config)# exit

```

Після виконання цих базових налаштувань у мережі встановлюється повна IP-зв'язність. Маршрутизатори обмінюються маршрутною інформацією, а кінцеві пристрої можуть успішно отримувати мережеві налаштування. Це створює необхідний фундамент для впровадження комплексних механізмів безпеки, які будуть розглянуті в наступних підрозділах.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2 Реалізація захищеного тунелю за допомогою IPsec VPN

Центральним елементом підсистеми захисту спроектованої мережі є створення зашифрованих каналів зв'язку між центральним офісом та віддаленими філіями. Для цього було обрано технологію Site-to-Site IPsec VPN, яка забезпечує конфіденційність, цілісність та автентичність даних, що передаються через публічну мережу Internet.

Процес налаштування IPsec тунелю є комплексним і складається з п'яти основних етапів:

1. Налаштування політики IKE Phase 1 (ISAKMP Policy): Визначення параметрів для захисту самого процесу обміну ключами.
2. Конфігурація ключів автентифікації (Pre-Shared Keys): Встановлення "паролів" для взаємної автентифікації VPN-шлюзів.
3. Налаштування політики IKE Phase 2 (Transform Set): Визначення алгоритмів для захисту безпосередньо даних користувачів.
4. Створення списків доступу (ACL): Ідентифікація трафіку, який потрібно шифрувати (так званий "цікавий трафік").
5. Створення та застосування криптографічної карти (Crypto Map): Поєднання всіх елементів в єдину політику та її активація на зовнішньому інтерфейсі.

Маршрутизатор R6 виступає в ролі центрального вузла (Hub), до якого підключатимуться всі філії.

1. Налаштування IKE Phase 1. Створюється політика ISAKMP, що визначає використання шифрування AES, хешування SHA, автентифікацію на основі попередньо узгоджених ключів та групу Діффі-Геллмана 2.

```
R6(config)# crypto isakmp policy 10
```

```
R6(config-isakmp)# encr aes
```

```
R6(config-isakmp)# hash sha
```

```
R6(config-isakmp)# authentication pre-share
```

```
R6(config-isakmp)# group 2
```

2. Конфігурація Pre-Shared Keys. Для кожної філії (R3, R4, R5) задається свій унікальний секретний ключ для автентифікації.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

```
R6(config)# crypto isakmp key MySecretKey123 address 195.168.1.5
```

```
R6(config)# crypto isakmp key MySecretKey456 address 195.168.1.9
```

```
R6(config)# crypto isakmp key MySecretKey789 address <IP-адреса R4>
```

3. Налаштування IKE Phase 2 (Transform Set). Створюється набір перетворень, що вказує на використання протоколу ESP з шифруванням AES та автентифікацією HMAC-SHA для захисту даних.

```
R6(config)# crypto ipsec transform-set IPSEC_SET esp-aes esp-sha-hmac
```

```
R6(cfg-crypto-trans)# mode tunnel
```

4. Створення ACL. Для кожної філії створюється окремий список доступу, який визначає, який трафік (від серверної та користувацької мереж центрального офісу) має бути зашифрований та відправлений у відповідний тунель.

! ACL для трафіку до філії 1 (за R3)

```
R6(config)# ip access-list extended ACL_TO_BRANCH1
```

```
R6(config-ext-nacl)# permit ip 195.168.4.0 0.0.0.255 195.168.6.0 0.0.0.255
```

```
R6(config-ext-nacl)# permit ip 195.168.5.0 0.0.0.255 195.168.6.0 0.0.0.255
```

! Аналогічні ACL створюються для філій 2 (195.168.7.0/24) та 3 (195.168.8.0/24)

5. Створення та застосування Crypto Map. Створюється криптографічна карта з різними послідовними номерами (10, 20, 30), кожен з яких відповідає за тунель до окремої філії, поєднуючи IP-адресу піра, набір перетворень та відповідний ACL. Після цього карта активується на зовнішньому інтерфейсі.

```
R6(config)# crypto map IPSEC_CRYPTO_MAP 10 ipsec-isakmp
```

```
R6(config-crypto-map)# set peer 195.168.1.5
```

```
R6(config-crypto-map)# set transform-set IPSEC_SET
```

```
R6(config-crypto-map)# match address ACL_TO_BRANCH1
```

! Аналогічні секції 20 та 30 створюються для інших філій

! Застосування карти до зовнішнього інтерфейсу

```
R6(config)# interface f0/0
```

```
R6(config-if)# crypto map IPSEC_CRYPTO_MAP
```

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Конфігурація на маршрутизаторах філій є дзеркальною до налаштувань центрального шлюзу.

! Кроки 1-3: Налаштування політик IKE та PSK (аналогічно до R6)

```
R3(config)# crypto isakmp policy 10
```

```
R3(config-isakmp)# encr aes
```

```
R3(config-isakmp)# hash sha
```

```
R3(config-isakmp)# authentication pre-share
```

```
R3(config-isakmp)# group 2
```

```
R3(config)# crypto isakmp key MySecretKey123 address 195.168.1.1
```

```
R3(config)# crypto ipsec transform-set IPSEC_SET esp-aes esp-sha-hmac
```

```
R3(cfg-crypto-trans)# mode tunnel
```

! Крок 4: Створення ACL для трафіку, що прямує до центрального офісу

```
R3(config)# ip access-list extended ACL_TO_HQ
```

```
R3(config-ext-nacl)# permit ip 195.168.6.0 0.0.0.255 195.168.4.0 0.0.0.255
```

```
R3(config-ext-nacl)# permit ip 195.168.6.0 0.0.0.255 195.168.5.0 0.0.0.255
```

! Крок 5: Створення та застосування Crypto Map

```
R3(config)# crypto map IPSEC_CRYPTOMAP 10 ipsec-isakmp
```

```
R3(config-crypto-map)# set peer 195.168.1.1
```

```
R3(config-crypto-map)# set transform-set IPSEC_SET
```

```
R3(config-crypto-map)# match address ACL_TO_HQ
```

```
R3(config)# interface f0/0
```

```
R3(config-if)# crypto map IPSEC_CRYPTOMAP
```

Аналогічні налаштування виконуються на маршрутизаторах R4 та R5 з відповідними IP-адресами та ключами. Після виконання цих конфігурацій між центральним офісом та кожною філією встановлюється захищений IPsec-тунель, що забезпечує конфіденційну передачу даних.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

3.3 Налаштування допоміжних систем захисту (TACACS+, Port Security, DHCP Snooping)

Окрім захисту даних у дорозі за допомогою IPsec VPN, для побудови комплексної та ешелонованої системи безпеки необхідно впровадити допоміжні механізми захисту. Вони спрямовані на контроль доступу до управління мережею, захист від загроз на рівні доступу та забезпечення централізованого моніторингу. У цьому підрозділі детально розглянуто налаштування TACACS+, SSH, Syslog та Port Security.

Для підвищення безпеки та спрощення адміністрування було налаштовано централізовану систему автентифікації, авторизації та обліку (AAA) за допомогою протоколу TACACS+. Це дозволяє керувати доступом адміністраторів до всіх мережевих пристроїв з єдиної точки. Для безпечного віддаленого підключення використовується протокол SSH, а для збору подій — централізований сервер Syslog.

Нижче наведено приклад конфігурації маршрутизатора R2, що демонструє комплексне налаштування цих служб:

! Налаштування сервера для збору логів

```
R2(config)# logging host 195.168.4.3
```

! Створення локального користувача як резервного методу входу

```
R2(config)# username test priv 15 secret testtest
```

```
R2(config)# enable secret adminpass
```

! Увімкнення фреймворку AAA та налаштування сервера TACACS+

```
R2(config)# aaa new-model
```

```
R2(config)# tacacs-server host 195.168.4.2
```

```
R2(config)# tacacs-server key tacacskey
```

! Налаштування методу автентифікації: спочатку TACACS+, потім локальна база

```
R2(config)# aaa authentication login default group tacacs+ local
```

```
R2(config)# line con 0
```

```
R2(config-line)# login authentication default
```

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

! Генерація ключів для запуску SSH

```
R2(config)# ip domain-name my.net
```

```
R2(config)# crypto key generate rsa
```

How many bits in the modulus [512]: 2048

% Generating 2048 bit RSA keys... [OK]

! Увімкнення SSH версії 2

```
R2(config)# ip ssh version 2
```

```
R2(config)# ip ssh time-out 30
```

Ключова команда `aaa authentication login default group tacacs+ local` створює надійний механізм входу: пристрій спочатку намагається зв'язатися з сервером TACACS+; якщо сервер недоступний, використовується локальна база даних користувачів (username test...).

На стороні сервера, через веб-інтерфейс **TacacsGUI**, створюються облікові записи для адміністраторів та групи пристроїв, що дозволяє гнучко керувати правами доступу (рис. 3.3 - 3.7).

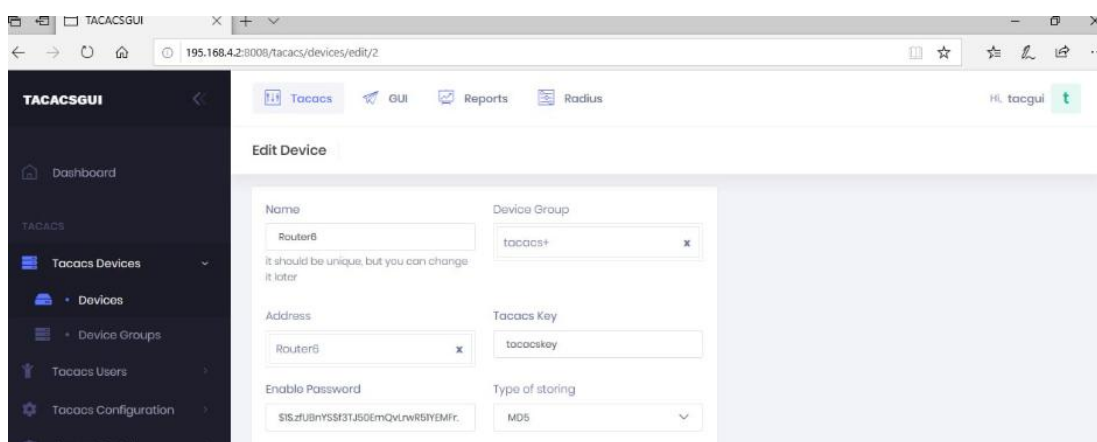


Рисунок 3.3 – Створення користувача в TACACS

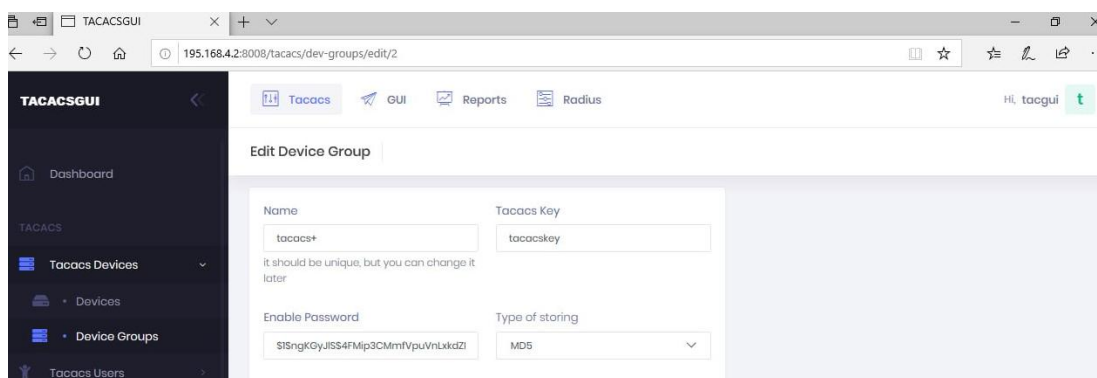


Рисунок 3.4 – Створення групи

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

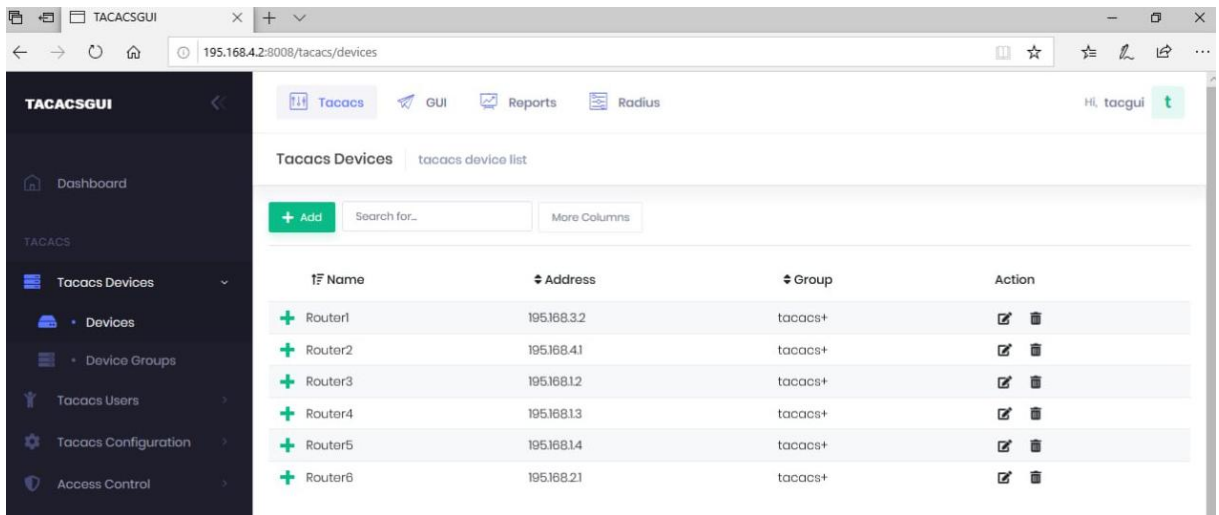


Рисунок 3.5 – Результат створення всіх користувачів

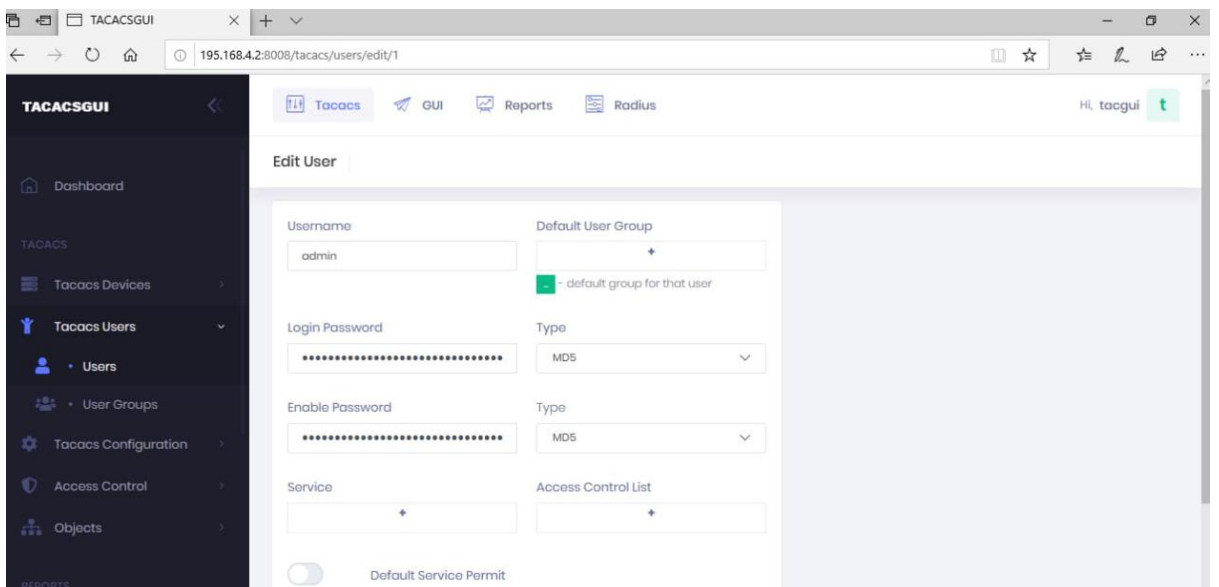


Рисунок 3.6 – Створення юзера admin

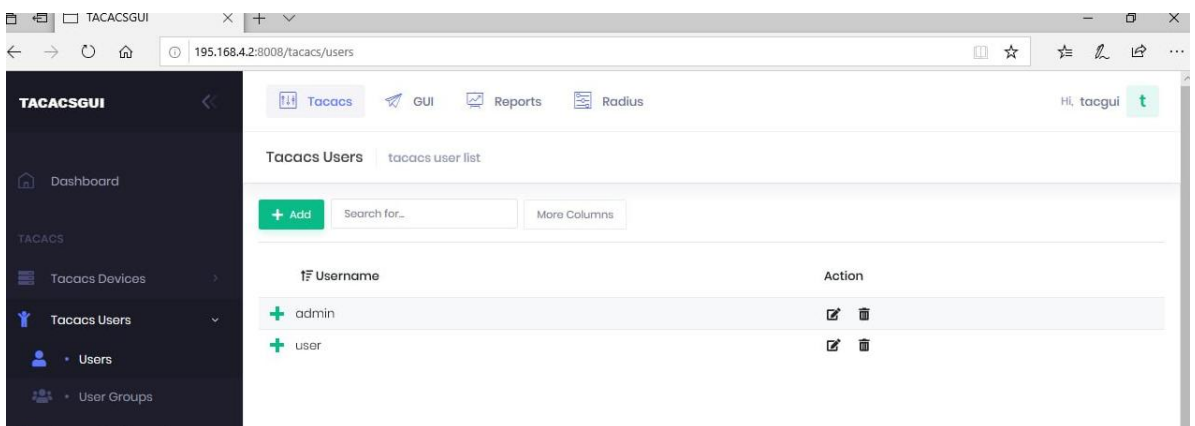


Рисунок 3.7 – Результат створення всіх юзерів

Для запобігання несанкціонованому фізичному підключенню до мережі на портах комутаторів рівня доступу налаштовується функція Port Security. Вона дозволяє обмежити кількість пристроїв, що можуть підключатися до одного порту, та визначає дії у разі порушення.

Приклад налаштування на комутаторі Switch4:

```
Switch4(config)# interface e0/1
```

```
Switch4(config-if)# switchport mode access
```

```
Switch4(config-if)# switchport port-security
```

! Дозволити лише 1 MAC-адресу на порту

```
Switch4(config-if)# switchport port-security maximum 1
```

! У разі порушення - блокувати трафік зловмисника, але не вимикати порт

```
Switch4(config-if)# switchport port-security violation restrict
```

! Автоматично вивчити та "запам'ятати" MAC-адресу першого пристрою

```
Switch4(config-if)# switchport port-security mac-address sticky
```

Така конфігурація забезпечує надійний контроль доступу на фізичному рівні.

Як було зазначено в аналізі загроз, для протидії атакам типу DHCP Spoofing та DHCP Starvation використовується технологія DHCP Snooping. Її налаштування, хоч і не показане тут детально, виконується на комутаторах рівня доступу та передбачає визначення довірених портів, через які дозволено надсилати DHCP-пропозиції.

Впровадження цих допоміжних систем захисту створює багатoshарову оборону, яка суттєво підвищує загальну безпеку корпоративної мережі, доповнюючи захист каналів зв'язку, реалізований за допомогою IPsec VPN.

3.4 Тестування працездатності та ефективності підсистеми захисту

Фінальним етапом впровадження є комплексне тестування, мета якого — перевірити коректність роботи всіх налаштованих сервісів та механізмів безпеки. Тестування дозволяє переконатися, що мережа не тільки функціонує згідно з проектом, але й ефективно протистоїть потенційним загрозам, які були ідентифіковані в

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

розділі 2.4. Перевірці підлягають як основний функціонал (IPsec VPN), так і допоміжні системи захисту.

Основне завдання — переконатися, що IPsec-тунель між центральним офісом (шлюз R6) та філіями (шлюз R3) встановлено і він коректно шифрує трафік. Для перевірки статусу тунелю використовуються спеціалізовані команди show.

Спочатку перевіряється статус асоціації безпеки IKE Phase 1 (ISAKMP SA). Успішне завершення цієї фази є необхідною умовою для побудови тунелю. Статус QM_IDLE у виводі команди show crypto isakmp sa на обох маршрутизаторах свідчить про те, що перша фаза пройшла успішно і шлюзи готові до встановлення каналу для передачі даних.

```

R6#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
195.168.1.1  195.168.1.3  QM_IDLE       1003 ACTIVE
195.168.1.1  195.168.1.4  QM_IDLE       1002 ACTIVE
195.168.1.1  195.168.1.2  QM_IDLE       1001 ACTIVE
IPv6 Crypto ISAKMP SA

```

Рисунок 3.7 – Результат виконання команди show crypto isakmp sa на маршрутизаторі R6

```

R3#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
195.168.1.1  195.168.1.2  QM_IDLE       1001 ACTIVE

```

Рисунок 3.8 – Результат виконання команди show crypto isakmp sa на маршрутизаторі R3

Далі виконується перевірка IKE Phase 2, тобто безпосередньо тунелю, через який передаються дані. Команда show crypto ipsec sa показує статистику роботи IPsec-тунелю. Ключовими показниками є лічильники #pkts encrypt та #pkts decrypt. Після надсилання тестового трафіку (наприклад, ping з однієї філії в іншу) ці лічильники мають збільшуватися, що є прямим доказом того, що тунель активний і трафік успішно шифрується та розшифровується.

```

R6#show crypto ipsec sa

interface: FastEthernet0/0
  Crypto map tag: IPSEC_MAP, local addr 195.168.1.1

protected vrf: (none)
local ident (addr/mask/prot/port): (195.168.5.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (195.168.7.0/255.255.255.0/0/0)
current_peer 195.168.1.3 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
  #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
  #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.: 195.168.1.1, remote crypto endpt.: 195.168.1.3
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x4E814B5B(1317096283)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x911BFBAD(2434530221)
    transform: esp-aes esp-sha-hmac ,
    in use settings ~(Tunnel, )
    conn id: 5, flow_id: 5, sibling_flags 80000040, crypto map: IPSEC_MAP
    sa timing: remaining key lifetime (k/sec): (4312097/3349)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x4E814B5B(1317096283)
    transform: esp-aes esp-sha-hmac ,
    in use settings ~(Tunnel, )
    conn id: 6, flow_id: 6, sibling_flags 80000040, crypto map: IPSEC_MAP
    sa timing: remaining key lifetime (k/sec): (4312097/3349)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (195.168.4.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (195.168.6.0/255.255.255.0/0/0)
current_peer 195.168.1.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
  #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
  #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

--More--

```

Рисунок 3.9 – Результат виконання команди show crypto ipsec sa на маршрутизаторі R6 (частина 1)

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

```

local crypto endpt.: 195.168.1.1, remote crypto endpt.: 195.168.1.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x98C097DE(2562758622)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xB944CE28(3108294184)
transform: esp-aes esp-sha-hmac ,
in use settings =(Tunnel, )
conn id: 11, flow_id: 11, sibling_flags 80000040, crypto map: IPSEC_MAP
sa timing: remaining key lifetime (k/sec): (4247391/3572)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x98C097DE(2562758622)
transform: esp-aes esp-sha-hmac ,
in use settings =(Tunnel, )
conn id: 12, flow_id: 12, sibling_flags 80000040, crypto map: IPSEC_MAP
sa timing: remaining key lifetime (k/sec): (4247391/3572)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (195.168.4.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (195.168.7.0/255.255.255.0/0/0)
current_peer 195.168.1.3 port 500
PERMIT, flags=(origin_is_acl,)
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#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.: 195.168.1.1, remote crypto endpt.: 195.168.1.3
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x87EEB830(2280568880)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x604F6328(1615815464)
transform: esp-aes esp-sha-hmac ,
in use settings =(Tunnel, )
conn id: 9, flow_id: 9, sibling_flags 80000040, crypto map: IPSEC_MAP
sa timing: remaining key lifetime (k/sec): (4180638/3558)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

```

Рисунок 3.10 – Результат виконання команди show crypto ipsec sa на маршрутизаторі R6 (частина 2)

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

```

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x87EEB830(2280568880)
transform: esp-aes esp-sha-hmac ,
in use settings =(Tunnel, )
conn id: 10, flow_id: 10, sibling_flags 80000040, crypto map: IPSEC_MAP
sa timing: remaining key lifetime (k/sec): (4180638/3558)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (195.168.5.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (195.168.6.0/255.255.255.0/0/0)
current peer 195.168.1.2 port 500
PERMIT, flags=(origin_is_acl,)
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
#pkts decaps: 13, #pkts decrypt: 13, #pkts verify: 13
#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.: 195.168.1.1, remote crypto endpt.: 195.168.1.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xF8009477(4160787575)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xFF6D27F6(4285343734)
transform: esp-aes esp-sha-hmac ,
in use settings =(Tunnel, )
conn id: 1, flow_id: 1, sibling_flags 80000040, crypto map: IPSEC_MAP
sa timing: remaining key lifetime (k/sec): (4362414/2998)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xF8009477(4160787575)
transform: esp-aes esp-sha-hmac ,
in use settings =(Tunnel, )
conn id: 2, flow_id: 2, sibling_flags 80000040, crypto map: IPSEC_MAP
sa timing: remaining key lifetime (k/sec): (4362415/2998)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

```

Рисунок 3.11 – Результат виконання команди show crypto ipsec sa на маршрутизаторі R6 (частина 3)

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

```

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (195.168.4.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (195.168.8.0/255.255.255.0/0/0)
current_peer 195.168.1.4 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
#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.: 195.168.1.1, remote crypto endpt.: 195.168.1.4
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x6D15F0E4(1830154468)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x50FE05AB(1358824875)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 7, flow_id: 7, sibling_flags 80000040, crypto map: IPSEC_MAP
    sa timing: remaining key lifetime (k/sec): (4214536/3469)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x6D15F0E4(1830154468)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 8, flow_id: 8, sibling_flags 80000040, crypto map: IPSEC_MAP
    sa timing: remaining key lifetime (k/sec): (4214536/3469)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (195.168.5.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (195.168.8.0/255.255.255.0/0/0)
current_peer 195.168.1.4 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#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.: 195.168.1.1, remote crypto endpt.: 195.168.1.4
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

```

Рисунок 3.12 – Результат виконання команди show crypto ipsec sa на маршрутизаторі R6 (частина 4)

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

```

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x5F4CD68F(1598871183)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x46C67978(1187412344)
transform: esp-aes esp-sha-hmac ,
in use settings =(Tunnel, )
conn id: 3, flow_id: 3, sibling_flags 80000040, crypto map: IPSEC_MAP
sa timing: remaining key lifetime (k/sec): (4351302/3339)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x5F4CD68F(1598871183)
transform: esp-aes esp-sha-hmac ,
in use settings =(Tunnel, )
conn id: 4, flow_id: 4, sibling_flags 80000040, crypto map: IPSEC_MAP
sa timing: remaining key lifetime (k/sec): (4351302/3339)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

```

Рисунок 3.13 – Результат виконання команди show crypto ipsec sa на маршрутизаторі R6 (частина 5)

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

```

R3#show crypto ipsec sa

interface: FastEthernet0/0
  Crypto map tag: IPSEC_MAP, local addr 195.168.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (195.168.6.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (195.168.4.0/255.255.255.0/0/0)
current_peer 195.168.1.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
  #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
  #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.: 195.168.1.2, remote crypto endpt.: 195.168.1.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xB944CE28(3108294184)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x98C097DE(2562758622)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 3, flow_id: 3, sibling_flags 80004040, crypto map: IPSEC_MAP
    sa timing: remaining key lifetime (k/sec): (4161637/3403)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xB944CE28(3108294184)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 4, flow_id: 4, sibling_flags 80004040, crypto map: IPSEC_MAP
    sa timing: remaining key lifetime (k/sec): (4161637/3403)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (195.168.6.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (195.168.5.0/255.255.255.0/0/0)
current_peer 195.168.1.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 13, #pkts encrypt: 13, #pkts digest: 13
  #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
  #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.: 195.168.1.2, remote crypto endpt.: 195.168.1.1

```

Рисунок 3.14 – Результат виконання команди show crypto ipsec sa на маршрутизаторі R3

Після підтвердження роботи VPN-тунелю проводиться тестування допоміжних систем.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

SSH та TACACS+: Виконується спроба підключення до маршрутизатора по протоколу SSH. Успішна автентифікація підтверджує працездатність SSH. Для перевірки інтеграції з TACACS+ аналізуються логи на сервері TacacsGUI, які мають фіксувати кожну спробу входу — як успішну, так і невдалу. Це підтверджує, що централізована система AAA працює коректно. Команда `debug tacacs` на маршрутизаторі дозволяє в реальному часі побачити обмін пакетами з сервером.

```

R6#ssh -l admin 195.168.2.2

Password:

R2>en
Password:
R2#

```

Рисунок 3.15 – Успішна перевірка працездатності SSH

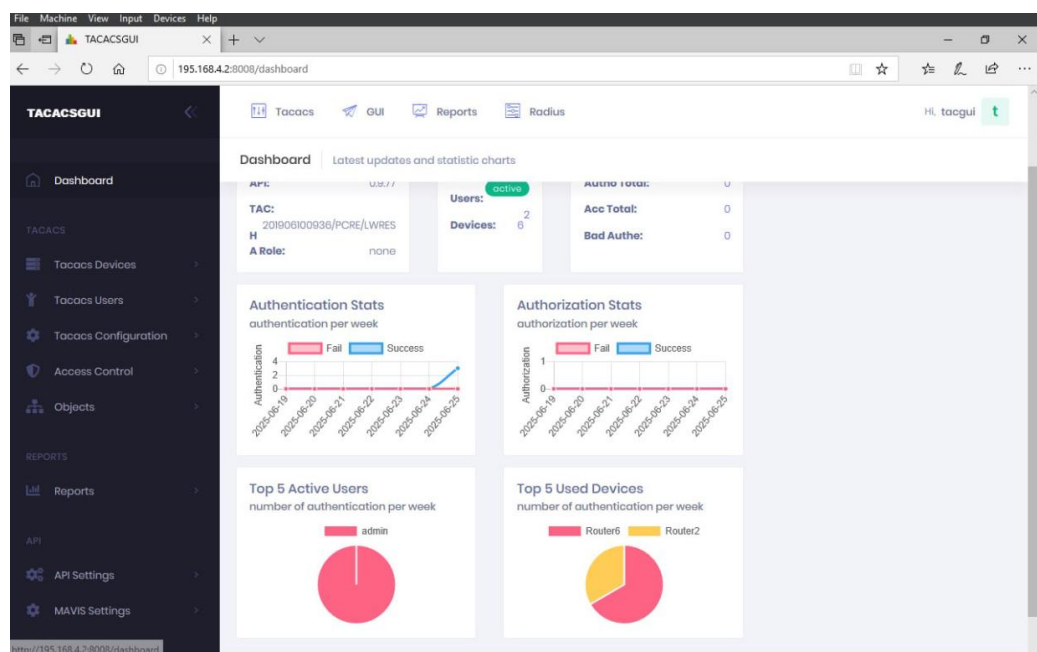


Рисунок 3.16 – Інформація в TACACSGUI в Dashbroad

```

User Access Verification
Username:
*Jun 25 05:10:39.047 UTC: AAA/BIND(0000000D): Bind i/f
*Jun 25 05:10:39.051 UTC: AAA/AUTHEN/LOGIN (0000000D): Pick method list 'default
*Jun 25 05:10:39.055 UTC: TPLUS: Queuing AAA Authentication request 13 for proce
ssing
*Jun 25 05:10:39.059 UTC: TPLUS(0000000D) login timer started 1020 sec timeout
*Jun 25 05:10:39.063 UTC: TPLUS: processing authentication start request id 13
*Jun 25 05:10:39.063 UTC: TPLUS: Authentication start packet created for 13()
*Jun 25 05:10:39.063 UTC: TPLUS: Using server 195.168.4.2
*Jun 25 05:10:39.071 UTC: TPLUS(0000000D)/O/NB_WAIT/6758D820: Started 5 sec time
out
*Jun 25 05:10:39.111 UTC: TPLUS(0000000D)/O/NB_WAIT: socket event 2
*Jun 25 05:10:39.111 UTC: TPLUS(0000000D)/O/NB_WAIT: wrote entire 29 bytes reques
t
*Jun 25 05:10:39.111 UTC: TPLUS(0000000D)/O/READ: socket event 1
*Jun 25 05:10:39.111 UTC: TPLUS(0000000D)/O/READ: Would block while reading
*Jun 25 05:10:39.139 UTC: TPLUS(0000000D)/O/READ: socket event 1
*Jun 25 05:10:39.139 UT

User Access Verification
Username: C: TPLUS(0000000D)/O/READ: read entire 12 header bytes (expect 43 byte
s data)
*Jun 25 05:10:39.139 UTC: TPLUS(0000000D)/O/READ: socket event 1
*Jun 25 05:10:39.139 UTC: TPLUS(0000000D)/O/READ: read entire 55 bytes response
*Jun 25 05:10:39.143 UTC: TPLUS(0000000D)/O/6758D820: Processing the reply packe
t
*Jun 25 05:10:39.143 UTC: TPLUS: Received authen response status GET_USER (7)

User Access Verification

```

Рисунок 3.17 – Перевірка за допомогою команди debug tacacs (частина 1)

```

Username: admin
Password:
*Jun 25 05:12:17.171 UTC: TPLUS: Queuing AAA Authentication request 14 for processing
*Jun 25 05:12:17.175 UTC: TPLUS(0000000E) login timer started 1020 sec timeout
*Jun 25 05:12:17.175 UTC: TPLUS: processing authentication continue request id 14
*Jun 25 05:12:17.179 UTC: TPLUS: Authentication continue packet generated for 14
*Jun 25 05:12:17.179 UTC: TPLUS(0000000E)/O/WRITE/6758D4AC: Started 5 sec timeout
*Jun 25 05:12:17.179 UTC: TPLUS(0000000E)/O/WRITE: wrote entire 22 bytes request
*Jun 25 05:12:17.203 UTC: TPLUS(0000000E)/O/READ: socket event 1
*Jun 25 05:12:17.203 UTC: TPLUS(0000000E)/O/READ: read entire 12 header bytes (expect 16 bytes data)
*Jun 25 05:12:17.207 UTC: TPLUS(0000000E)/O/READ: socket event 1
*Jun 25 05:12:17.207 UTC: TPLUS(0000000E)/O/READ: read entire 28 bytes response
*Jun 25 05:12:17.207 UTC: TPLUS(0000000E)/O/6758D4AC: Processing the reply packet
*Jun 25 05:12:17.211 UTC: TPLUS: Received authen response status GET_PASSWORD (8)

R6#
*Jun 25 05:12:19.979 UTC: TPLUS: Queuing AAA Authentication request 14 for processing
*Jun 25 05:12:19.983 UTC: TPLUS(0000000E) login timer started 1020 sec timeout
*Jun 25 05:12:19.987 UTC: TPLUS: processing authentication continue request id 14
*Jun 25 05:12:19.991 UTC: TPLUS: Authentication continue packet generated for 14
*Jun 25 05:12:19.991 UTC: TPLUS(0000000E)/O/WRITE/679CD4FC: Started 5 sec timeout
*Jun 25 05:12:19.995 UTC: TPLUS(0000000E)/O/WRITE: wrote entire 26 bytes request
*Jun 25 05:12:20.023 UTC: TPLUS(0000000E)/O/READ: socket event 1
*Jun 25 05:12:20.023 UTC: TPLUS(0000000E)/O/READ: read entire 12 header bytes (expect 6 bytes data)
*Jun 25 05:12:20.023 UTC: TPLUS(0000000E)/O/READ: socket event 1
*Jun 25 05:12:20.023 UTC: TPLUS(0000000E)/O/READ: read entire 18 bytes response
*Jun 25 05:12:20.027 UTC: TPLUS(0000000E)/O/679CD4FC: Processing the reply packet
*Jun 25 05:12:20.027 UTC: TPLUS: Received authen response status PASS (2)

R6#

```

Рисунок 3.18 – Перевірка за допомогою команди debug tacacs (частина 2)

Syslog: Для перевірки централізованого збору логів на одному з пристроїв виконуються дії, що генерують системні повідомлення (наприклад, зміна конфігурації). Після цього перевіряється інтерфейс Syslog-сервера, де мають з'явитися відповідні записи з вказанням часу, IP-адреси пристрою та тексту повідомлення.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

Setup Font Processing Highlighting Goto new More View prev View next View file Clear About Terminate Display View file syslog Message filtering All messages match						
Displaying 30 messages						
Time	IP	Host	Facility	Priority	Tag	Message
Jun 25 08:05:19	195.168.4.1		local7	info	48	*Jun 25 05:05:17.011 UTC: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 195.168.4.3 port 514 started - CLI ini
Jun 25 08:05:34	195.168.2.1		local7	info	23	*Jun 25 05:05:32.923 UTC: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 195.168.4.3 port 514 started - CLI ini
Jun 25 08:05:57	195.168.4.1		local7	warning	49	*Jun 25 05:05:55.571 UTC: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/1 (not half dupl
Jun 25 08:06:07	195.168.4.1		local7	notice	50	*Jun 25 05:06:05.371 UTC: %SSH-5-ENABLED: SSH 1.99 has been enabled
Jun 25 08:06:08	195.168.4.1		local7	notice	51	*Jun 25 05:06:06.523 UTC: %SYS-5-CONFIG_1: Configured from console by console
Jun 25 08:06:22	195.168.2.1		local7	notice	24	*Jun 25 05:06:20.075 UTC: %SSH-5-ENABLED: SSH 1.99 has been enabled
Jun 25 08:06:23	195.168.2.1		local7	notice	25	*Jun 25 05:06:21.291 UTC: %SYS-5-CONFIG_1: Configured from console by console
Jun 25 08:06:58	195.168.4.1		local7	warning	52	*Jun 25 05:06:55.591 UTC: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/1 (not half dupl
Jun 25 08:07:57	195.168.4.1		local7	warning	53	*Jun 25 05:07:55.591 UTC: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/1 (not half dupl
Jun 25 08:08:57	195.168.4.1		local7	warning	54	*Jun 25 05:08:55.595 UTC: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/1 (not half dupl
Jun 25 08:09:57	195.168.4.1		local7	warning	55	*Jun 25 05:09:55.599 UTC: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/1 (not half dupl
Jun 25 08:10:57	195.168.4.1		local7	warning	56	*Jun 25 05:10:55.599 UTC: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/1 (not half dupl
Jun 25 08:11:57	195.168.4.1		local7	warning	57	*Jun 25 05:11:55.599 UTC: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/1 (not half dupl
Jun 25 08:12:58	195.168.4.1		local7	warning	58	*Jun 25 05:12:55.603 UTC: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/1 (not half dupl
Jun 25 08:13:58	195.168.4.1		local7	warning	59	*Jun 25 05:13:55.611 UTC: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/1 (not half dupl
Jun 25 08:13:59	195.168.2.1		local7	info	13	*Jun 25 05:13:57.763 UTC: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 195.168.4.3 port 514 started - CLI ini

Рисунок 3.19 – Успішна перевірка працездатності Syslog

Port Security: Для тестування цього механізму до порту, де налаштовано port-security, підключається неавторизований пристрій. Реакція комутатора (повідомлення про порушення безпеки в консолі) та вивід команди show port-security interface підтверджують, що захист спрацював.

```

Jun 25 05:36:45.837: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occ
rrred, caused by MAC address 0800.27f9.201d on port Ethernet0/2.
witch5#
Jun 25 05:36:51.859: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occ
rrred, caused by MAC address 0800.27f9.201d on port Ethernet0/2.
witch5#

```

Рисунок 3.20 – Результат перевірки працездатності Port-Security

```

switch5#show port-security interface eth0/2
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Restrict
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 0
Sticky MAC Addresses   : 1
Last Source Address:Vlan : 0800.27f9.201d:1
Security Violation Count : 354

```

Рисунок 3.21 – Результат виконання команди show port-security int eth0/2

DHCP: Працездатність DHCP перевіряється з кінцевого пристрою (VPCS) шляхом надсилення запиту на отримання IP-адреси. Успішне отримання адреси з правильного пулу, а також адреси шлюзу та DNS-сервера, свідчить про коректну роботу служби.

```

PC5> ip dhcp
ODORA IP 195.168.5.2/24 GW 195.168.5.1
PC5>

```

Рисунок 3.22 – Успішна перевірка працездатності DHCP

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

Результати проведеного тестування підтверджують, що всі компоненти спроектованої підсистеми захисту функціонують коректно та взаємодіють між собою, забезпечуючи надійний та багатошаровий захист корпоративної мережі.

Висновок до третього розділу

У третьому розділі було послідовно виконано практичну реалізацію та комплексне тестування спроектованої підсистеми захисту корпоративної мережі. Даний розділ продемонстрував перехід від теоретичного проектування до створення повноцінно функціонуючої та захищеної інфраструктури.

На етапі впровадження було виконано всі необхідні налаштування:

- Створено базову конфігурацію мережевого обладнання, що включає налаштування IP-адресації, запуск протоколу динамічної маршрутизації EIGRP для забезпечення зв'язності та розгортання служби DHCP для автоматизації роботи клієнтських пристроїв.
- Реалізовано ключовий елемент безпеки — Site-to-Site IPsec VPN тунелі між центральним офісом та філіями, що забезпечує конфіденційність та цілісність даних, які передаються через публічну мережу.
- Впроваджено багатошарову систему захисту, що включає налаштування TACACS+ для централізованої автентифікації, SSH для безпечного адміністрування, Syslog для моніторингу подій та Port Security для захисту на фізичному рівні.

На етапі тестування було проведено ретельну перевірку всіх реалізованих механізмів. Результати підтвердили, що IPsec-тунелі успішно встановлені та коректно шифрують трафік, а допоміжні системи, такі як TACACS+, Syslog, SSH та Port Security, функціонують згідно з очікуваннями.

Таким чином, практична частина роботи продемонструвала, що розроблений проєкт є життєздатним, а впроваджені заходи безпеки ефективно виконують свої функції, що підтверджує досягнення поставлених на початку роботи цілей.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було успішно досягнуто поставленої мети — розроблено та реалізовано комплексний проєкт захищеної корпоративної мережі на основі сучасних VPN-рішень.

Робота над проєктом розпочалася з глибокого теоретичного аналізу сучасних VPN-технологій, за результатами якого було обґрунтовано вибір фреймворку IPsec як найнадійнішого та найпродуктивнішого рішення для корпоративної мережі на базі обладнання Cisco. На основі цього вибору було розроблено детальний проєкт мережі, що включає ієрархічну топологію зі схлопнутим ядром, ефективну схему IP-адресації та аналіз потенційних векторів атак. Практична частина роботи полягала в повній реалізації спроектованої архітектури: було налаштовано базову мережеву зв'язність за допомогою EIGRP, впроваджено захищені Site-to-Site IPsec-тунелі між офісами, а також реалізовано багатопарову систему захисту, що включає TACACS+, SSH, Syslog та Port Security.

Проведене комплексне тестування підтвердило повну працездатність та ефективність всіх впроваджених компонентів. Тести показали, що IPsec-тунель успішно шифрує трафік, а допоміжні системи безпеки коректно виконують свої функції, забезпечуючи надійний та ешелонований захист інфраструктури.

Таким чином, розроблений проєкт є комплексним, готовим до впровадження рішенням, яке може слугувати практичним посібником для створення безпечних мережевих інфраструктур для підприємств малого та середнього бізнесу. Напрямами подальшого вдосконалення даного проєкту може бути перехід від автентифікації на основі Pre-Shared Keys до більш масштабованої інфраструктури публічних ключів (PKI) з використанням цифрових сертифікатів, а також інтеграція систем виявлення та запобігання вторгненням (IDS/IPS) для проактивного захисту від загроз.

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What Is A VPN? A Best (Yet Thorough) Explanation Of 2025 // VPN.com : [Електронний ресурс]. – Режим доступу: <https://vpn.com/faq/what-is-a-vpn/> (дата звернення: 25.06.2025).
2. What is a VPN? How It Works, Types, and Benefits // Kaspersky : [Електронний ресурс]. – Режим доступу: <https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn> (дата звернення: 25.06.2025).
3. Virtual private network // Wikipedia : [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Virtual_private_network (дата звернення: 25.06.2025).
4. What is a VPN Tunnel? // Palo Alto Networks : [Електронний ресурс]. – Режим доступу: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-vpn-tunnel> (дата звернення: 25.06.2025).
5. How Does a VPN Work? // Fortinet : [Електронний ресурс]. – Режим доступу: <https://www.fortinet.com/resources/cyberglossary/how-does-vpn-work> (дата звернення: 25.06.2025).
6. AES Encryption: What Is It & How Does It Work? // SafeShellVPN : [Електронний ресурс]. – Режим доступу: <https://www.safeshellvpn.com/blog/aes-encryption.html> (дата звернення: 25.06.2025).
7. Site-to-site VPN: що це таке і як працює // NordVPN : [Електронний ресурс]. – Режим доступу: <https://nordvpn.com/uk/blog/site-to-site-vpn/> (дата звернення: 25.06.2025).
8. Francis-Press. A Comparative Study of VPN Protocols // Francis Press : [Електронний ресурс]. – Режим доступу: <https://francispress.com/uploads/papers/VydclV52hOq5Qta6hQOQozgqGL1aIyHXdzzoDFvD.pdf> (дата звернення: 25.06.2025).
9. RFC 4301: Security Architecture for the Internet Protocol // IETF : [Електронний ресурс]. – Режим доступу: <https://datatracker.ietf.org/doc/html/rfc4301> (дата звернення: 25.06.2025).

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

10. Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.6 // Cisco : [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect46/administration/guide/b_AnyConnect_Administrator_Guide_4-6/configure-vpn.html (дата звернення: 25.06.2025).
11. Reference Manual for OpenVPN 2.4 // OpenVPN : [Електронний ресурс]. – Режим доступу: <https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/> (дата звернення: 25.06.2025).
12. Security Overview // OpenVPN Community : [Електронний ресурс]. – Режим доступу: <https://community.openvpn.net/Archived/SecurityOverview> (дата звернення: 25.06.2025).
13. WireGuard: Technical Whitepaper // WireGuard : [Електронний ресурс]. – Режим доступу: <https://www.wireguard.com/papers/wireguard.pdf> (дата звернення: 25.06.2025).
14. WireGuard: Fast, Modern, Secure VPN Tunnel // WireGuard : [Електронний ресурс]. – Режим доступу: <https://www.wireguard.com/> (дата звернення: 25.06.2025).
15. RFC 4301: Security Architecture for the Internet Protocol // IETF : [Електронний ресурс]. – Режим доступу: <https://datatracker.ietf.org/doc/html/rfc4301> (дата звернення: 25.06.2025).
16. Configuring Security for VPNs with IPsec // Cisco : [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpns/configuration/12-4/sec-sec-for-vpns-w-ipsec-12-4-book.pdf (дата звернення: 25.06.2025).
17. IPsec vs WireGuard: Which VPN Protocol is Better? // Netmaker : [Електронний ресурс]. – Режим доступу: <https://www.netmaker.io/resources/ipsec-vs-wireguard> (дата звернення: 25.06.2025).
18. Color-Cisco 7200 Hardware // ICANN Archive : [Електронний ресурс]. – Режим доступу: https://archive.icann.org/en/tlds/org/applications/dotorgfoundation/Tech_Attac

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

hments/Hardware/Network/Color-Cisco_7200.pdf (дата звернення: 25.06.2025).

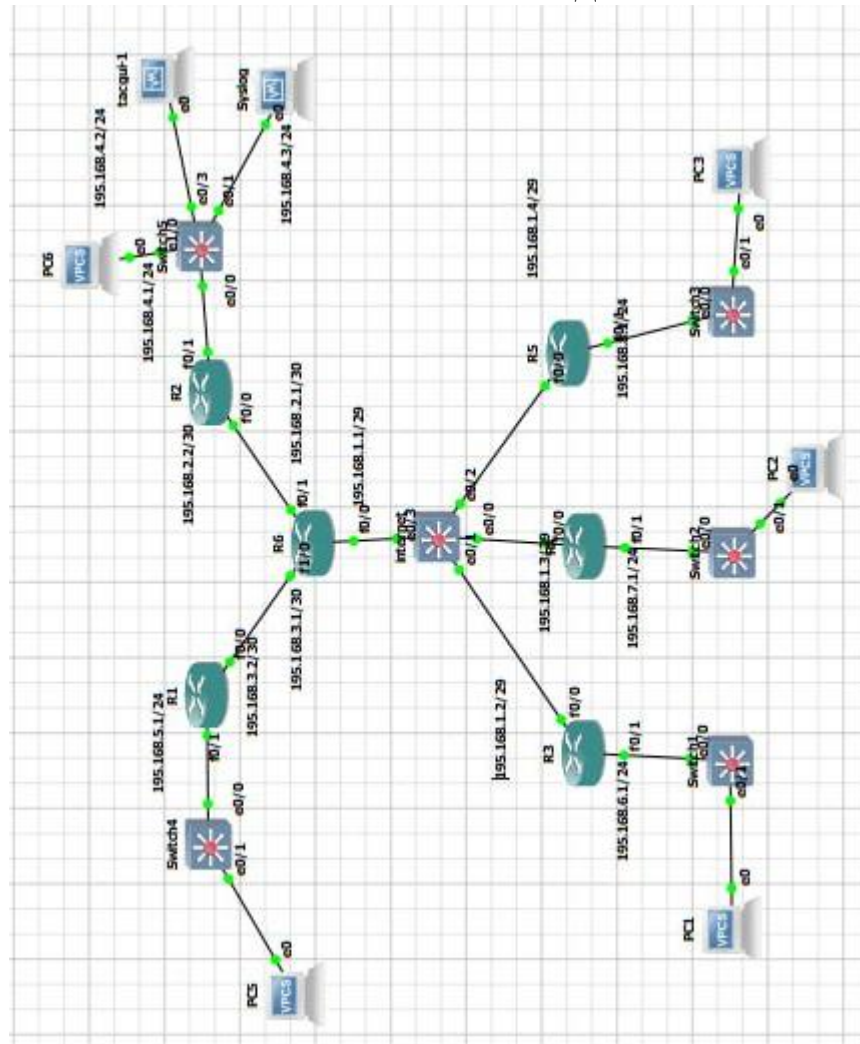
19. Cisco Catalyst WS-C2960-24TT-L Datasheet // MrShabake : [Електронний ресурс]. – Режим доступу: <https://mrshabake.com/wp-content/uploads/2023/05/cisco-catalyst-WS-C2960-24TT-L-datasheet.pdf> (дата звернення: 25.06.2025).

20. TACACS+ GUI Support // TACACSGUI : [Електронний ресурс]. – Режим доступу: <https://tacacsgui.com/support/> (дата звернення: 25.06.2025).

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				55
Змн.	Арк.	№ докум.	Підпис	Дата		



		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

```
R1#show run
Building configuration...

Current configuration : 1609 bytes
!
! Last configuration change at 06:17:59 UTC Wed Jun 25 2025
!
version 15.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$szS8$9TI9RxD/pPsNSj1g6nVAV1
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
!
!
!
!
!
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
ip dhcp pool POOL_R3
network 195.168.5.0 255.255.255.0
default-router 195.168.5.1
dns-server 8.8.8.8
!
!
!
no ip domain lookup
ip domain name my.net
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
username test privilege 15 secret 5 $1$/QwM$XjwrvSml0IicWUmoZWTKv0
!
!
ip tcp synwait-time 5
ip ssh time-out 30
ip ssh version 2
!
```

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 195.168.3.2 255.255.255.252
speed auto
duplex auto
!
interface FastEthernet0/1
ip address 195.168.5.1 255.255.255.0
speed auto
duplex auto
!
interface FastEthernet1/0
no ip address
shutdown
speed auto
duplex auto
!
interface FastEthernet1/1
no ip address
shutdown
speed auto
duplex auto
!
!
router eigrp 100
network 195.168.3.0 0.0.0.3
network 195.168.5.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
logging host 195.168.4.3
!
!
tacacs-server host 195.168.4.2
tacacs-server key tacacskey
!
!
control-plane
!
!
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

```

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

stopbits 1
line vty 0 4
!
!
end
Switch4#show run
Building configuration...

Current configuration : 1527 bytes
!
! Last configuration change at 05:35:31 UTC Wed Jun 25 2025
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Switch4
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ip icmp rate-limit unreachable
!
no ip cef
!
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
interface Ethernet0/0

```

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Ethernet0/1
 duplex auto
!
interface Ethernet0/2
 duplex auto
!
interface Ethernet0/3
 duplex auto
!
interface Ethernet1/0
 duplex auto
!
interface Ethernet1/1
 duplex auto
!
interface Ethernet1/2
 duplex auto
!
interface Ethernet1/3
 duplex auto
!
interface Ethernet2/0
 duplex auto
!
interface Ethernet2/1
 duplex auto
!
interface Ethernet2/2
 duplex auto
!
interface Ethernet2/3
 duplex auto
!
interface Ethernet3/0
 duplex auto
!
interface Ethernet3/1
 duplex auto
!
interface Ethernet3/2
 duplex auto
!
interface Ethernet3/3
 duplex auto
!
interface Vlan1
 no ip address
 shutdown
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15

```

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

```

logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end
R6#show run
Building configuration...

Current configuration : 2716 bytes
!
! Last configuration change at 06:17:34 UTC Wed Jun 25 2025
!
version 15.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
hostname R6
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$Gl83$SfQy17IVjb7OoVfGRuDHO/
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
!
!
!
!
!
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
!
no ip domain lookup
ip domain name my.net
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
username test privilege 15 secret 5 $1$nQdo$LmCLd.XnxYiHCHEySJxRS0
!
!
ip tcp synwait-time 5

```

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip ssh time-out 30
ip ssh version 2
!
!
!
!
!
crypto isakmp policy 10
  encr aes
  authentication pre-share
  group 2
crypto isakmp key MySecretKey123 address 195.168.1.2
crypto isakmp key MySecretKey456 address 195.168.1.3
crypto isakmp key MySecretKey789 address 195.168.1.4
!
!
crypto ipsec transform-set IPSEC_SET esp-aes esp-sha-hmac
mode tunnel
!
!
!
crypto map IPSEC_MAP 10 ipsec-isakmp
  set peer 195.168.1.2
  set transform-set IPSEC_SET
  match address ACL_TO_BRANCH_R3
crypto map IPSEC_MAP 20 ipsec-isakmp
  set peer 195.168.1.3
  set transform-set IPSEC_SET
  match address ACL_TO_BRANCH_R4
crypto map IPSEC_MAP 30 ipsec-isakmp
  set peer 195.168.1.4
  set transform-set IPSEC_SET
  match address ACL_TO_BRANCH_R5
!
!
!
!
!
interface FastEthernet0/0
  ip address 195.168.1.1 255.255.255.248
  speed auto
  duplex auto
  crypto map IPSEC_MAP
!
interface FastEthernet0/1
  ip address 195.168.2.1 255.255.255.252
  speed auto
  duplex auto
!
interface FastEthernet1/0
  ip address 195.168.3.1 255.255.255.252
  speed auto
  duplex auto
!
interface FastEthernet1/1
  no ip address
  shutdown
  speed auto
  duplex auto
!
!
router eigrp 100
  network 195.168.1.0 0.0.0.7

```

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

```

network 195.168.2.0 0.0.0.3
network 195.168.3.0 0.0.0.3
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ip access-list extended ACL_TO_BRANCH_R3
permit ip 195.168.4.0 0.0.0.255 195.168.6.0 0.0.0.255
permit ip 195.168.5.0 0.0.0.255 195.168.6.0 0.0.0.255
ip access-list extended ACL_TO_BRANCH_R4
permit ip 195.168.4.0 0.0.0.255 195.168.7.0 0.0.0.255
permit ip 195.168.5.0 0.0.0.255 195.168.7.0 0.0.0.255
ip access-list extended ACL_TO_BRANCH_R5
permit ip 195.168.4.0 0.0.0.255 195.168.8.0 0.0.0.255
permit ip 195.168.5.0 0.0.0.255 195.168.8.0 0.0.0.255
!
logging host 195.168.4.3
!
!
tacacs-server host 195.168.4.2
tacacs-server key tacacskey
!
!
control-plane
!
!
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
!
!
end

R2#show run
Building configuration...

Current configuration : 1522 bytes
!
! Last configuration change at 06:17:59 UTC Wed Jun 25 2025
!
version 15.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$zNvN$.uufEv5Yrx9XFxb6YuQua.
!

```

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

```

aaa new-model
!
!
aaa authentication login default group tacacs+ local
!
!
!
!
!
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
!
!
no ip domain lookup
ip domain name my.net
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
username test privilege 15 secret 5 $1$Xsox$XDpbzJdNY6wJIFD8fyU0F/
!
!
ip tcp synwait-time 5
ip ssh time-out 30
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 195.168.2.2 255.255.255.252
speed auto
duplex auto
!
interface FastEthernet0/1
ip address 195.168.4.1 255.255.255.0
speed auto
duplex auto
!
interface FastEthernet1/0
no ip address
shutdown
speed auto

```

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

```

duplex auto
!
interface FastEthernet1/1
no ip address
shutdown
speed auto
duplex auto
!
!
router eigrp 100
network 195.168.2.0
network 195.168.2.0 0.0.0.3
network 195.168.4.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
logging host 195.168.4.3
!
!
tacacs-server host 195.168.4.2
tacacs-server key tacacskey
!
!
control-plane
!
!
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
!
!
end

Switch5#show run
Building configuration...

Current configuration : 1878 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Switch5
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

```

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

```

logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ip icmp rate-limit unreachable
!
no ip cef
!
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
duplex auto
!
interface Ethernet0/1
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0800.27ef.f2e9
duplex auto
!
interface Ethernet0/2
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0800.2779.d97f
duplex auto
!
interface Ethernet0/3
duplex auto
!
interface Ethernet1/0
duplex auto
!
interface Ethernet1/1

```

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

```

duplex auto
!
interface Ethernet1/2
duplex auto
!
interface Ethernet1/3
duplex auto
!
interface Ethernet2/0
duplex auto
!
interface Ethernet2/1
duplex auto
!
interface Ethernet2/2
duplex auto
!
interface Ethernet2/3
duplex auto
!
interface Ethernet3/0
duplex auto
!
interface Ethernet3/1
duplex auto
!
interface Ethernet3/2
duplex auto
!
interface Ethernet3/3
duplex auto
!
interface Vlan1
no ip address
shutdown
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

```

```

R3#show run
Building configuration...

```

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Current configuration : 2096 bytes
!
! Last configuration change at 06:18:24 UTC Wed Jun 25 2025
!
version 15.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$t57b$h3xv43q.53ETfBYa8IVdi/
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
!
!
!
!
!
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
ip dhcp pool POOL_R3
network 195.168.6.0 255.255.255.0
default-router 195.168.6.1
dns-server 8.8.8.8
!
!
!
no ip domain lookup
ip domain name my.net
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
username test privilege 15 secret 5 $1$4dE7$WZaBJOPoyd3VwLnnHZXWh1
!
!
ip tcp synwait-time 5
ip ssh time-out 30
ip ssh version 2
!
!
!
!
!

```

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
crypto isakmp policy 10
  encr aes
  authentication pre-share
  group 2
crypto isakmp key MySecretKey123 address 195.168.1.1
!
!
crypto ipsec transform-set IPSEC_SET esp-aes esp-sha-hmac
  mode tunnel
!
!
!
crypto map IPSEC_MAP 10 ipsec-isakmp
  set peer 195.168.1.1
  set transform-set IPSEC_SET
  match address ACL_TO_HQ
!
!
!
!
interface FastEthernet0/0
  ip address 195.168.1.2 255.255.255.248
  speed auto
  duplex auto
  crypto map IPSEC_MAP
!
interface FastEthernet0/1
  ip address 195.168.6.1 255.255.255.0
  speed auto
  duplex auto
!
interface FastEthernet1/0
  no ip address
  shutdown
  speed auto
  duplex auto
!
interface FastEthernet1/1
  no ip address
  shutdown
  speed auto
  duplex auto
!
!
router eigrp 100
  network 195.168.1.0 0.0.0.7
  network 195.168.6.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ip access-list extended ACL_TO_HQ
  permit ip 195.168.6.0 0.0.0.255 195.168.4.0 0.0.0.255
  permit ip 195.168.6.0 0.0.0.255 195.168.5.0 0.0.0.255
!
logging host 195.168.4.3
!
!

```

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

tacacs-server host 195.168.4.2

tacacs-server key tacacskey

!

!

control-plane

!

!

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

!

!

end

Switch1#show run

Building configuration...

Current configuration : 1727 bytes

!

! Last configuration change at 06:19:03 UTC Wed Jun 25 2025

!

version 15.1

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service compress-config

!

hostname Switch1

!

boot-start-marker

boot-end-marker

!

!

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

!

no aaa new-model

no ip icmp rate-limit unreachable

*Jun 25 06:19:03.990: %SYS-5-CONFIG_I: Configured from console by console

--More--

!

no ip cef

!

!

no ip domain-lookup

no ipv6 cef

ipv6 multicast rpf use-bgp

!

!

!

!

!

!

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
interface Ethernet0/0
!
interface Ethernet0/1
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0050.7966.6800
duplex auto
!
interface Ethernet0/2
duplex auto
!
interface Ethernet0/3
duplex auto
!
interface Ethernet1/0
duplex auto
!
interface Ethernet1/1
duplex auto
!
interface Ethernet1/2
duplex auto
!
interface Ethernet1/3
duplex auto
!
interface Ethernet2/0
duplex auto
!
interface Ethernet2/1
duplex auto
!
interface Ethernet2/2
duplex auto
!
interface Ethernet2/3
duplex auto
!
interface Ethernet3/0
duplex auto
!
interface Ethernet3/1

```

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

```

duplex auto
!
interface Ethernet3/2
duplex auto
!
interface Ethernet3/3
duplex auto
!
interface Vlan1
no ip address
shutdown
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

R4#show run
Building configuration...

Current configuration : 2096 bytes
!
! Last configuration change at 06:22:54 UTC Wed Jun 25 2025
!
version 15.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
hostname R4
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$VT8/$Ys2nDi/DQZSjmPP9W31D5.
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
!
!
!
!
!
!

```

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

```

aaa session-id common
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
ip dhcp pool POOL_R4
network 195.168.7.0 255.255.255.0
default-router 195.168.7.1
dns-server 8.8.8.8
!
!
!
no ip domain lookup
ip domain name my.net
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
username test privilege 15 secret 5 $1$dAYO$TCVHern6iqWImC52yk.Cb0
!
!
ip tcp synwait-time 5
ip ssh time-out 30
ip ssh version 2
!
!
!
!
!
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
crypto isakmp key MySecretKey456 address 195.168.1.1
!
!
crypto ipsec transform-set IPSEC_SET esp-aes esp-sha-hmac
mode tunnel
!
!
!
crypto map IPSEC_MAP 10 ipsec-isakmp
set peer 195.168.1.1
set transform-set IPSEC_SET
match address ACL_TO_HQ
!
!
!
!
!
interface FastEthernet0/0
ip address 195.168.1.3 255.255.255.248
speed auto
duplex auto

```

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

```

crypto map IPSEC_MAP
!
interface FastEthernet0/1
ip address 195.168.7.1 255.255.255.0
speed auto
duplex auto
!
interface FastEthernet1/0
no ip address
shutdown
speed auto
duplex auto
!
interface FastEthernet1/1
no ip address
shutdown
speed auto
duplex auto
!
!
router eigrp 100
network 195.168.1.0 0.0.0.7
network 195.168.7.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ip access-list extended ACL_TO_HQ
permit ip 195.168.7.0 0.0.0.255 195.168.4.0 0.0.0.255
permit ip 195.168.7.0 0.0.0.255 195.168.5.0 0.0.0.255
!
logging host 195.168.4.3
!
!
tacacs-server host 195.168.4.2
tacacs-server key tacacskey
!
!
control-plane
!
!
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
!
!
end

```

Switch2#show run
Building configuration...

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

```

*Jun 25 06:23:20.717: %SYS-5-CONFIG_I: Configured from console by console
Current configuration : 1727 bytes
!
! Last configuration change at 06:23:20 UTC Wed Jun 25 2025
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Switch2
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ip icmp rate-limit unreachable
!
no ip cef
!
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
!
interface Ethernet0/1
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0050.7966.6801

```

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

```

duplex auto
!
interface Ethernet0/2
duplex auto
!
interface Ethernet0/3
duplex auto
!
interface Ethernet1/0
duplex auto
!
interface Ethernet1/1
duplex auto
!
interface Ethernet1/2
duplex auto
!
interface Ethernet1/3
duplex auto
!
interface Ethernet2/0
duplex auto
!
interface Ethernet2/1
duplex auto
!
interface Ethernet2/2
duplex auto
!
interface Ethernet2/3
duplex auto
!
interface Ethernet3/0
duplex auto
!
interface Ethernet3/1
duplex auto
!
interface Ethernet3/2
duplex auto
!
interface Ethernet3/3
duplex auto
!
interface Vlan1
no ip address
shutdown
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0

```

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

```

exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

```

```

R5#show run
Building configuration...

```

```

Current configuration : 2096 bytes
!
! Last configuration change at 06:18:22 UTC Wed Jun 25 2025
!
version 15.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
hostname R5
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$uAJ0$thSK6zo/IpmFWDbHKURC0/
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
!
!
!
!
!
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
ip dhcp pool POOL_R5
network 195.168.8.0 255.255.255.0
default-router 195.168.8.1
dns-server 8.8.8.8
!
!
!
no ip domain lookup
ip domain name my.net
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!

```

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
username test privilege 15 secret 5 $1$.CWD$H.zMbU7Uwvmwt3Am4uYbL.
!
!
ip tcp synwait-time 5
ip ssh time-out 30
ip ssh version 2
!
!
!
!
!
crypto isakmp policy 10
  encr aes
  authentication pre-share
  group 2
crypto isakmp key MySecretKey789 address 195.168.1.1
!
!
crypto ipsec transform-set IPSEC_SET esp-aes esp-sha-hmac
  mode tunnel
!
!
!
crypto map IPSEC_MAP 10 ipsec-isakmp
  set peer 195.168.1.1
  set transform-set IPSEC_SET
  match address ACL_TO_HQ
!
!
!
!
!
interface FastEthernet0/0
  ip address 195.168.1.4 255.255.255.248
  speed auto
  duplex auto
  crypto map IPSEC_MAP
!
interface FastEthernet0/1
  ip address 195.168.8.1 255.255.255.0
  speed auto
  duplex auto
!
interface FastEthernet1/0
  no ip address
  shutdown
  speed auto
  duplex auto
!
interface FastEthernet1/1
  no ip address
  shutdown
  speed auto
  duplex auto
!
!
router eigrp 100
  network 195.168.1.0 0.0.0.7
  network 195.168.8.0
!
ip forward-protocol nd
!

```

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
no ip http server
no ip http secure-server
!
ip access-list extended ACL_TO_HQ
 permit ip 195.168.8.0 0.0.0.255 195.168.4.0 0.0.0.255
 permit ip 195.168.8.0 0.0.0.255 195.168.5.0 0.0.0.255
!
logging host 195.168.4.3
!
!
tacacs-server host 195.168.4.2
tacacs-server key tacacskey
!
!
control-plane
!
!
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
!
!
end

Switch3#show run
Building configuration...

Current configuration : 1727 bytes
!
! Last configuration change at 06:24:25 UTC Wed Jun 25 2025
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Switch3
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ip icmp rate-limit unreachable
--More--
*Jun 25 06:24:25.325: %SYS-5-CONFIG_I: Configured from console by console
!
no ip cef

```

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
interface Ethernet0/0
!
interface Ethernet0/1
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0050.7966.6802
duplex auto
!
interface Ethernet0/2
duplex auto
!
interface Ethernet0/3
duplex auto
!
interface Ethernet1/0
duplex auto
!
interface Ethernet1/1
duplex auto
!
interface Ethernet1/2
duplex auto
!
interface Ethernet1/3
duplex auto
!
interface Ethernet2/0
duplex auto
!
interface Ethernet2/1
duplex auto

```

		Карнаух Б.О.			ККИКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Ethernet2/2
 duplex auto
!
interface Ethernet2/3
 duplex auto
!
interface Ethernet3/0
 duplex auto
!
interface Ethernet3/1
 duplex auto
!
interface Ethernet3/2
 duplex auto
!
interface Ethernet3/3
 duplex auto
!
interface Vlan1
 no ip address
 shutdown
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end

```

!

		Карнаух Б.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Покотило О.А.				28
Змн.	Арк.	№ докум.	Підпис	Дата		