

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

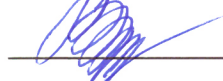
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захищеного обміну трафі-
ком на базі технологій VPN та обладнання компанії
Cisco»

Виконав: студент 4-го курсу групи КБп-20-1
спеціальності 125 «Кібербезпека»

 Марк БАЛАБОЛОВ

Керівник: професор кафедри КІ та КБ, д.т.н., доцент,

 Володимир ВОРОТНІКОВ

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

 Олексій ШЕЛУХА

Житомир – 2025

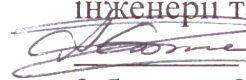
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко

3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Балаболов Марк Геннадійович

Тема роботи: «Проект підсистеми захищеного обміну трафіком на базі технологій VPN та обладнання компанії Cisco»

затверджена Наказом університету від 3 березня 2025 р. № 81/с

Термін здачі студентом закінченої роботи 27 березня 2025 р.

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

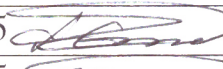
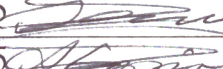
Об'єктом дослідження є процес побудови підсистеми захищеного обміну трафіком.

Предметом дослідження є технології VPN та засоби їх впровадження з використанням пристроїв Cisco ASA.

Обладнання та програмне забезпечення:

1. Мережевий симулятор Cisco Packet Tracer
2. Комутатори Cisco
3. Маршрутизатори Cisco
4. Міжмережевий екран Cisco ASA

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	07.01.2025 	07.01.2025 
2	Єфіменко А.А.	16.02.2025 	16.02.2025 
3	Єфіменко А.А.	06.03.2025 	06.03.2025 

Студент  Марк БАЛАБОЛОВ

Керівник  Володимир ВОРОТНІКОВ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	07.01.2025	Виконано
2	Аналіз отриманого завдання	08.01.2025	Виконано
3	Розробка плану роботи	14.01.2025	Виконано
4	Аналіз літературних джерел	20.01.2025	Виконано
5	Вибір обладнання та технологій	28.01.2025	Виконано
6	Розробка мережі	03.02.2025	Виконано
7	Налаштування пристроїв мережі	17.02.2025	Виконано
8	Тестування роботи мережі	02.03.2025	Виконано
9	Оформлення пояснювальної записки	04.03.2025	Виконано
10	Отримання відгуку та рецензії	27.03.2025	Виконано
11	Захист кваліфікаційної роботи	29.03.2025	

Студент  Марк БАЛАБОЛОВ

Керівник  Володимир ВОРОТНІКОВ

АНОТАЦІЯ

Кваліфікаційна робота на тему «Проект підсистеми захищеного обміну трафіком на базі технологій VPN та обладнання компанії Cisco» складається з переліку умовних скорочень, вступу, трьох розділів, висновків, списку використаних джерел і додатків.

Пояснювальна записка містить 112 сторінок, 2 таблиці та 76 рисунків. Список використаної літератури налічує 22 найменування та займає 2 сторінки.

Метою роботи є розробка підсистеми захищеного обміну трафіком для корпоративної мережі на основі технологій VPN та обладнання компанії Cisco, що забезпечує надійний захист даних та ефективну взаємодію між різними сегментами мережі.

У роботі було досліджено основні підходи до забезпечення захищеного обміну інформацією в корпоративних мережах. Обрано оптимальні технології для реалізації захисту трафіку, зокрема VPN-технології та міжмережеві екрани. Спроектовано структуру мережі, визначено компоненти, що забезпечують її надійність і безпеку. Налагоджено різноманітні мережеві пристрої, включаючи маршрутизатори, комутатори та брандмауери, а також забезпечено їх інтеграцію в єдину систему з використанням методів захисту, таких як сегментація мережі, контролю доступу та шифрування даних.

У додатку представлена схема спроектованої мережі, таблиця адресації та конфігурація пристроїв.

Ключові слова: ЗАХИСТ, КОРПОРАТИВНА МЕРЕЖА, ОБМІН ТРАФІКОМ, МІЖМЕРЕЖЕВИЙ ЕКРАН, VPN.

					ККІК<.КР.Б – 125 – 02 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захищеного об- міну трафіком на базі технологій VPN та обладнання компанії Cisco	Лім.	Арк.	Аркушів
Розроб.		Балаболов М. Г.		27.03				
Керівник		Воротніков В.В.		27.03			4	112
Реценз.		Шелуха О.О.		27.03		ФІКТ, Гр. КБп-20-1		
Н. контр.		Єфіменко А. А.		27.03				
Затверд.		Єфіменко А. А.		27.03				

ANNOTATION

The qualification work “Project of a subsystem of secure traffic exchange based on VPN technologies and Cisco company hardware” consists of a list of abbreviations, introduction, three chapters, conclusions, a list of used sources and attachments.

The explanatory note contains 112 pages and 76 pictures. The list of references includes 19 titles and takes up 2 pages.

The purpose of the work is to design a secure traffic exchange subsystem for a corporate network based on VPN technologies and Cisco company hardware, which provides reliable data protection and effective interaction between different network segments.

The main research approaches to ensuring secure information exchange in corporate networks were investigated. The optimal technologies for traffic protection, in particular VPN technologies and firewalls, are selected. The network structure is designed and the components that ensure its reliability and security are identified. Various network devices, including routers, switches, and firewalls, are configured and integrated into a single system using security methods such as network segmentation, access control, and data encryption.

The attachment presents a diagram of the designed network, addressing table, and device configuration.

Keywords: SECURITY, CORPORATE NETWORK, TRAFFIC EXCHANGE, FIREWALL, VPN.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ОБМІНУ ТРАФІКОМ В СУЧАСНИХ МЕРЕЖАХ	9
1.1 Основні аспекти забезпечення захищеного обміну трафіком	9
1.2 Базові технології та протоколи забезпечення захисту мережного обміну ...	14
1.3 Основні технічні рішення для забезпечення захищеного мережного обміну трафіком	19
1.4 Постановка технічного завдання	23
РОЗДІЛ 2 ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО ОБМІНУ ТРАФІКОМ.....	25
2.1 Аналіз мережевої інфраструктури підприємства та проблеми захисту	25
2.2 Розробка загальної структури підсистеми захищеного мережного обміну	30
2.3 Розробка компонентів підсистеми захисту.....	35
РОЗДІЛ 3 ВПРОВАДЖЕННЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО ОБМІНУ ТРАФІКОМ.....	38
3.1 Вибір обладнання компанії Cisco для побудови підсистеми захищеного обміну трафіком.....	38
3.2 Налагодження підсистеми захищеної мережі компанії	42
3.3 Тестування процесу захищеного обміну інформацією в корпоративній мережі	67
ВИСНОВКИ.....	83
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	84
ДОДАТКИ.....	86

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КМ – Комп’ютерна Мережа

ОС – Операційна Система

ПК – Персональний Комп’ютер

МЕ – Міжмережевий Екран

IP – Internet Protocol

VPN – Virtual Private Network

ASA – Adaptive Security Appliances

DMZ – Demilitarized Zone

VLAN – Virtual Local Area Network

SSH – Secure Shell

DHCP – Dynamic Host Configuration Protocol

TACACS+ – Terminal Access Controller Access Control System plus

SYSLOG – System Log

NTP – Network Time Protocol

ACL – Access Control List

EIGRP – Enhanced Interior Gateway Routing Protocol

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасному світі, де обмін інформацією через мережі стає основою для функціонування організацій, забезпечення захищеного передавання даних є надзвичайно важливим. Особливо це стосується компаній із розгалуженою структурою, де офіси та віддалені користувачі постійно обмінюються неофіційною інформацією через публічні мережі. Тому тема кваліфікаційної роботи покликана створити систему, що дозволить підвищити рівень безпеки даних та мінімізувати загрози несанкціонованого доступу.

Метою кваліфікаційної роботи є розробка ефективної та надійної підсистеми захищеного обміну трафіком між філіями та віддаленими користувачами компанії з використанням провідних технологій на базі обладнання Cisco.

Визначена мета обумовлює наступні завдання:

- Провести аналіз сучасних технологій захисту трафіку та VPN-рішень.
- Розробити модель мережної інфраструктури з урахуванням усіх вимог та потреб компанії.
- Обрати та налаштувати оптимальні протоколи та технології у мережі.
- Впровадити та протестувати підсистему з використанням обладнання Cisco.

Об'єктом дослідження є процес побудови захищеного обміну інформацією в корпоративних мережах.

Предметом дослідження є технології VPN та засоби їх впровадження з використанням пристроїв Cisco ASA.

У процесі виконання кваліфікаційної роботи було розроблено проект захищеної мережі для компанії з використанням технологій VPN та обладнання Cisco, який забезпечує безпечний обмін трафіком через публічні мережі.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ОБМІНУ ТРАФІКОМ В СУЧАСНИХ МЕРЕЖАХ

1.1 Основні аспекти забезпечення захищеного обміну трафіком

Протягом більш ніж десяти років різноманітні технологічні тенденції перепліталися, перетворюючи мережеву безпеку на складну задачу. Популярність веб-додатків і сервісів для завантаження файлів збільшила кількість атак, зростання кількості мобільних пристроїв створило новий масштаб мережевого трафіку, а широке розповсюдження віддаленої роботи ще більше ускладнило безпеку мережевого обміну даними. Ризики для кібербезпеки, спричинені цими тенденціями, настільки ж різноманітні, як і технології, що їх створюють. Шкідливе програмне забезпечення може проникати в мережі через завантаження файлів зі шкідливим кодом або URL-адреси, часто використовуючи вразливості «нульового дня», які ніколи не були виявлені, а отже, не мають відомих протитотрут. Несанкціонований доступ до мереж і додатків може призвести до підвищення доступу до ресурсів і встановлення стійкості, що є поширеною тактикою атак зловмисників-«вимагачів». Розподілені атаки на відмову в обслуговуванні (DDoS) порушують продуктивність і слугують стартовим майданчиком для подальших атак. Атаки типу «людина посередині» можуть захопити конфіденційну інформацію так само легко, як необережні помилки можуть призвести до витоку захищених даних, таких як персональна інформація (PII) або захищена інформація про стан здоров'я (PHI).

В результаті, на тлі цих викликів, пов'язаних зі зростанням кількості атак і складністю сучасного мережевого трафіку, організації все частіше звертаються до різноманітних пристроїв і рішень для забезпечення безпеки. Їх мета - захистити інфраструктуру від різноманітних мережевих загроз, таких як шкідливе програмне забезпечення, несанкціонований доступ і атаки типу «людина посередині».

Основні типи мережевих пристроїв і рішень для захисту:

- Мости (bridges) – колись використовувалися для з'єднання двох або більше хостів або сегментів мережі. Вони застаріли і більше не використовуються.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

- Концентратори – колись використовувалися для з'єднання пристроїв локальної мережі (LAN). Оскільки вони не мають вбудованого інтелекту, концентратори рідко використовуються в сучасних мережевих налаштуваннях.

- Мережевий комутатор – стандартний мережевий пристрій, що з'єднує комп'ютери, сервери, принтери та інші пристрої в локальній мережі. Він використовує MAC-адреси для керування та пересилання даних на певні пристрої. На відміну від концентратора, комутатор може розумно спрямовувати трафік, щоб зменшити перевантаження мережі та підвищити її продуктивність.

- Мережевий маршрутизатор – це пристрій, який спрямовує пакети даних між різними мережами, щоб полегшити підключення до Інтернету та внутрішню мережеву комунікацію. Маршрутизатори використовують IP-адреси для визначення найефективнішого шляху для передачі пакетів даних між мережами. Вони також можуть надавати функції безпеки, такі як списки контролю доступу, щоб обмежити доступ до мережі.

- Шлюз – це посередник між пристроями в різних мережах, який дозволяє їм спілкуватися, навіть якщо вони використовують різні протоколи зв'язку.

- Брандмауер (firewall) – відокремлює одну мережу від іншої. Брандмауери доступні в апаратній та програмній формі і можуть бути інтегровані в такі пристрої, як маршрутизатори або сервери. Класичним прикладом брандмауера є спеціальний пристрій, який слугує бар'єром між внутрішньою мережею та зовнішнім світом.

- Система контролю доступу до мережі (NAC) – оцінює, чи відповідають пристрої, які намагаються отримати доступ до мережі, визначеним стандартам безпеки (наприклад, сучасне антивірусне ПЗ, системні оновлення та певні налаштування конфігурації), а потім надає або забороняє доступ до мережі.

- Веб-фільтр – обмежує доступ до інтернет-контенту на основі заздалегідь визначених фільтрів. Наприклад, цей тип рішення для безпеки може блокувати доступ до шкідливих або неприйнятних веб-сайтів, як це визначено політикою організації.

- Проксі-сервер – це посередник між пристроєм користувача та інтернетом. Проксі-сервери можуть маскувати IP-адресу користувача, а також фільтрувати веб-запити, щоб заблокувати доступ до шкідливих сайтів або контенту.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

- Фільтр електронної пошти (спам-фільтр) – допомагає запобігти потрап-
лянню небажаних електронних листів до поштової скриньки користувача або доста-
вляє електронний лист, але видаляє потенційно шкідливі гіперпосилання та вкла-
дення. Прості фільтри використовують політики організації або шаблони, визначені
постачальником, для виявлення спаму; просунуті фільтри застосовують методи по-
шуку підозрілих шаблонів або частоти слів.

- Інструменти для боротьби з DDoS-атаками – призначені для виявлення роз-
поділених атак типу «відмова в обслуговуванні» (DDoS) на ранніх стадіях, погли-
нання пов'язаного з ними збільшення трафіку та визначення місця походження
атаки.

- Балансувальники навантаження – сприяють безпеці мережі, рівномірно ро-
зподіляючи мережевий трафік між кількома серверами. Наприклад, вони можуть до-
помогти запобігти перевантаженню будь-якого окремого сервера під час DDoS-
атаки.

Після визначення основних типів мережевих пристроїв, наступним кроком є розгляд найкращих практик, які організації повинні впроваджувати для підвищення рівня безпеки корпоративних мереж. Найкращі практики захисту корпоративних мереж допомагають створити багаторівневу систему безпеки, яка дозволяє вчасно виявляти загрози, мінімізувати вплив потенційних атак, забезпечувати конфіденційність і цілісність даних, а також підтримувати безперервний захист інфраструктури. Нижче наведені ключові практики [1], що є основою для забезпечення надійного захищеного обміну трафіком у корпоративних мережах, а також для зменшення ризиків виникнення інцидентів безпеки.

1. Сегментація мережі. Сегментація мережі передбачає розподіл її на логічні або функціональні зони з метою локалізації потенційних порушень безпеки в одній зоні та мінімізації збитків для всієї інфраструктури. Цього можна досягти за допомогою фізичних засобів, таких як маршрутизатори та комутатори, або віртуально, за допомогою VLAN. Сегментація також дозволяє ІТ-командам застосовувати різні заходи безпеки та моніторингу в кожній зоні. Особливо важливим є створення демілі-

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

таризованої зони (DMZ), яка виконує роль буфера між внутрішньою мережею та Інтернетом або іншими ненадійними мережами. У DMZ зазвичай розміщуються зовнішні сервіси, такі як веб-сервери додатків, щоб уникнути прямого доступу до внутрішньої мережі в разі їх компрометації.

2. Правильне розташування пристроїв безпеки. Ефективність роботи пристроїв безпеки значною мірою залежить від їх правильного розташування. Фаєрволи повинні бути встановлені на стиках між різними мережевими зонами, де вони виконують роль бар'єра між сегментами. Сучасні фаєрволи часто мають вбудовані функції, такі як системи виявлення та запобігання вторгнень (IDS/IPS), захист від DDoS-атак та веб-фільтрація, що робить їх важливими елементами захисту периметра мережі. Веб-фаєрволи (WAF) слід розміщувати в зонах, де розташовані додатки, зокрема у DMZ, щоб захистити веб-додатки від атак, таких як SQL-ін'єкції та міжсайтове виконання сценаріїв (XSS).

3. Фізична безпека мережевого обладнання. Доступ до мережевої інфраструктури повинен бути суворо контрольованим і надаватися лише авторизованому персоналу. Це стосується комутаційних шаф, основних і проміжних розподільчих кадрів (MDF, IDF), серверів і, особливо, дата-центрів. Для доступу до таких критичних зон обов'язково слід використовувати процедури аутентифікації. Крім того, рекомендується заборонити використання USB-накопичувачів та зовнішніх дисків, щоб запобігти несанкціонованому вивезенню конфіденційної інформації.

4. Використання трансляції мережевих адрес (NAT). Трансляція мережевих адрес (NAT) перетворює всі приватні IP-адреси організації на одну публічну IP-адресу для зовнішніх комунікацій, що дозволяє маскувати внутрішню структуру мережі від сторонніх осіб, додаючи додатковий рівень безпеки.

5. Використання персональних фаєрволів. Персональні фаєрволи є програмними засобами захисту, які встановлюються на кожен комп'ютер або сервер. Вони обмежують вхідний і вихідний трафік для захисту пристроїв від потенційних загроз. Хоча початкове налаштування персональних фаєрволів може бути трудомістким, це важливий крок для запобігання уразливостям пристроїв до атак або шкідливого ПЗ.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

6. Використання білого списку додатків. Білий список додатків передбачає створення списку дозволених програм та обмеження запуску інших додатків. Це суттєво знижує ризик зараження шкідливим ПЗ, яке може бути поширене через фішингові атаки або шкідливі веб-сайти. Однак цей підхід може бути не завжди практичним, оскільки список потрібно постійно оновлювати.

7. Використання проксі-серверів для управління доступом до Інтернету. Підключення через проксі-сервер дозволяє аутентифікувати користувачів та моніторити вихідні підключення, що допомагає запобігти встановленню з'єднань між шкідливими програмами та серверами зловмисників.

8. Принцип найменших привілеїв. Важливо обмежити права доступу користувачів до мінімуму, необхідного для виконання їхніх робочих обов'язків. Це знижує ризик випадкового або навмисного пошкодження даних, а також зменшує шкоду від потенційного компрометування облікових записів.

9. Вимога використання VPN для віддаленого доступу. Віртуальні приватні мережі (VPN) дозволяють створювати захищене з'єднання між віддаленими користувачами та корпоративною мережею через загальнодоступну мережеву інфраструктуру. VPN використовують шифрування для забезпечення конфіденційності даних та захисту від перехоплення, що особливо важливо для захисту трафіку віддалених користувачів.

У сучасному корпоративному середовищі дотримання вищезазначених практик є критично важливим елементом забезпечення мережевої безпеки та захисту трафіку. Використання цих методів може значно знизити ризик майбутніх загроз в роботі мережі.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2 Базові технології та протоколи забезпечення захисту мережного обміну

Неможливо побудувати надійну систему мережевої безпеки без використання найсучасніших технологій [2] і протоколів. Ці інструменти забезпечують конфіденційність, цілісність і доступність даних та захищають мережу від широкого спектру загроз.

Протоколи [3] мережевої безпеки складаються з правил і структур, призначених для захисту даних під час їх проходження через мережу. Вони також визначають, як дані передаються з точки А в точку Б, як кожен компонент отримує дані і як запобігти зловмиснику прочитати дані під час перехоплення повідомлення. Найперші протоколи мережевої безпеки були розроблені, щоб запобігти крадіжці або фальсифікації інформації хакерами з метою порушення зв'язку. Спочатку ці протоколи були ефективними, але з розвитком хакерських технологій протоколи довелося змінювати.

Існує три основні типи мережевих протоколів [4] - комунікаційні, керуючі та безпекові.

- Комунікаційні протоколи використовуються для того, щоб забезпечити передачу даних між двома кінцевими точками без пошкоджень або неповноти.
- Протоколи керування займаються адмініструванням і контролем різних ресурсів у мережі, які полегшують передачу даних. За допомогою протоколів керування можна контролювати кожен пристрій, щоб переконатися, що він передає інформацію так, як потрібно.
- Протоколи безпеки зосереджені на захисті даних і мережевих ресурсів від хакерів.

До комунікаційних протоколів належать: TCP, UDP, HTTP та FTP. Ці протоколи визначають, як дані передаються між пристроями в мережі.

- TCP (Transmission Control Protocol): Забезпечує надійну, орієнтовану на з'єднання передачу даних. Він розбиває дані на пакети, нумерує їх, підтверджує отримання кожного пакету і повторно передає втрачені пакети. Це гарантує, що дані будуть доставлені цілком і в правильному порядку.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

- UDP (User Datagram Protocol): Протокол ненадійної передачі даних, орієнтований на швидкість. Він не гарантує доставку пакетів і не забезпечує їх порядковість. UDP використовується для додатків, де втрата деяких пакетів допустима, наприклад, для потокового відео або голосової передачі.

- HTTP (Hypertext Transfer Protocol): Протокол для передачі гіпертекстових документів, основний протокол для веб-сервісів. Він використовується для отримання веб-сторінок, зображень, відео та інших ресурсів з веб-серверів.

- FTP (File Transfer Protocol): Протокол для передачі файлів між комп'ютерами. Він дозволяє завантажувати файли на сервери.

До керуючих протоколів належать: ICMP, SNMP та DNS. Ці протоколи керують мережевими пристроями та процесами.

- ICMP (Internet Control Message Protocol): Використовується для обміну діагностичними повідомленнями між пристроями в мережі. За допомогою ICMP реалізується функція "ping", яка дозволяє перевірити доступність іншого пристрою в мережі.

- SNMP (Simple Network Management Protocol): Протокол для віддаленого управління мережевими пристроями. Він дозволяє збирати інформацію про стан пристроїв, конфігурувати їх та діагностувати проблеми.

- DNS (Domain Name System): Система доменних імен, яка перетворює текстові доменні імена на числові IP-адреси, які комп'ютери використовують для взаємодії між собою.

До протоколів безпеки належать: SSH, TLS/SSL та IPsec. Ці протоколи захищають дані під час передачі по мережі.

- SSH (Secure Shell): Протокол для безпечного віддаленого доступу до комп'ютерів. Він забезпечує шифрування даних, аутентифікацію користувачів та авторизацію.

- TLS/SSL (Transport Layer Security/Secure Sockets Layer): Протокол для шифрування з'єднань між клієнтом і сервером. Він використовується для захисту передачі даних у веб-браузерах, електронній пошті та інших додатках.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

• IPsec: Набір протоколів, який забезпечує захист комунікацій в IP-мережах. Він включає в себе автентифікацію, шифрування та захист від підміни пакетів.

Для забезпечення комплексного захисту інформації недостатньо використовувати лише одні протоколи. Для ефективної боротьби з сучасними мережевими загрозами необхідно застосовувати різноманітні технології [5].

При роботі в Інтернеті брандмауери є найважливішим засобом захисту мережі організації для забезпечення інформаційної безпеки. Брандмауер захищає локальну мережу від зовнішніх загроз. Він контролює вхідний і вихідний трафік на комп'ютер або локальну мережу, зупиняючи майже всі типи мережових атак. Брандмауери на базі Windows ефективні, оскільки повністю замінюють стек протоколів TCP/IP, що унеможливорює втручання хакерів у їхню роботу шляхом спотворення зовнішніх мережових протоколів.

МЕ виконують такі функції:

- фізичне відділення робочих станцій і серверів внутрішнього сегмента мережі від зовнішніх каналів зв'язку;
- багатоетапну ідентифікацію запитів, що надходять в мережу;
- перевірку повноважень і прав доступу користувача до внутрішніх ресурсів мережі;
- реєстрацію всіх запитів до компонентів внутрішньої підмережі ззовні;
- контроль цілісності програмного забезпечення і даних;
- економію адресного простору мережі;
- приховування IP-адреси внутрішніх серверів з метою захисту від хакерів.

Розрізняють два типи МЕ: апаратний і програмний. Апаратний - це пристрій, який фізично підключений до мережі. Цей пристрій відстежує всі аспекти вхідного та вихідного обміну даними, а також перевіряє адреси джерела та призначення кожного оброблюваного повідомлення. Це забезпечує захист, допомагаючи запобігти небажаному проникненню в мережу або комп'ютер. Програмний тип виконує ті ж завдання, але використовує програмний продукт, який запуснений на кінцевому комп'ютері або шлюзі, а не зовнішній пристрій. Програмний тип реалізації МЕ має найбільшу поширеність.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

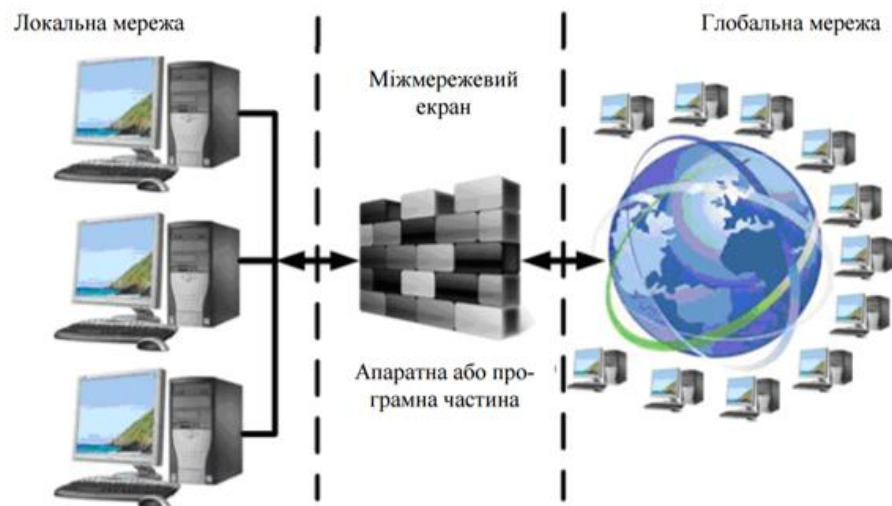


Рисунок 1.1 – Загальна схема роботи локальної мережі через МЕ

Брандмауери можуть захищати певні протоколи та програмні продукти. Однак брандмауери не є універсальним рішенням для всіх проблем безпеки в Інтернеті. Наприклад, брандмауери не сканують на віруси і не можуть забезпечити цілісність даних.

Хоча спілкування через Інтернет має свої недоліки, найголовнішим з яких є потенційна можливість порушення безпеки та конфіденційності, VPN гарантує, що повідомлення, надіслані через Інтернет, є такими ж безпечними, як і ті, що надсилаються через локальну мережу.



Рисунок 1.2 – Загальна схема роботи VPN

VPN - це логічна мережа, побудована на основі інших мереж (Інтернет) через публічний або віртуальний канал. Шифрування дозволяє пакетам передаватися через загальнодоступну мережу, створюючи таким чином канал для обміну інформацією, закритий для сторонніх. Наприклад, VPN з'єднує кілька географічно розподілених мереж організації в єдину мережу і використовує неконтрольовані канали зв'язку між ними. Технологія VPN створює віртуальні канали зв'язку, так звані «VPN-тунелі», через загальнодоступну мережу. Зв'язок з віддаленими філіями через тунель зашифрований. Зловмисники, які перехоплюють зашифровану інформацію, не зможуть її переглянути, оскільки не мають ключа розшифровки.

Спеціалізовані протоколи використовуються для передачі інформації з мережі VPN і включають в себе наступне:

- Layer 2 Forwarding Protocol - протокол переадресації 2-го рівня;
- Layer 2 Tunneling Protocol - протокол тунелювання на рівні з'єднання;
- PPTP (Point-to-Point Tunneling Protocol) - протокол тунелювання між вузлами.
- Протокол IPsec (IP-безпека);
- Протокол SKIP (Simple Key Management for Internet Protocol).

Згідно з цими протоколами, пакети мережевого рівня інкапсулюються в пакети PPP (Point-to-Point Protocol) і доставляються одержувачу.

Переваги VPN очевидні. Надаючи користувачам можливість підключатися до Інтернету, в першу чергу за рахунок збільшення пропускної здатності каналів зв'язку для масштабування при перевантаженні мережі, VPN може допомогти заощадити гроші на телефонних рахунках, усуваючи необхідність мати справу з модемами-пулами. Крім того, VPN дозволяють отримати доступ до мережевих ресурсів, які адміністратори зазвичай використовують через зовнішнє з'єднання.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

1.3 Основні технічні рішення для забезпечення захищеного мережного обміну трафіком

Оскільки вибір конкретного варіанту рішення безпосередньо впливає на рівень безпеки та продуктивність мережі, потрібно ретельно обирати технології для захисту мережного трафіку. В організаціях, що використовують обладнання Cisco, при виборі технології для забезпечення безпечного обміну мережевим трафіком необхідно враховувати наступні основні вимоги:

1. Сумісність з обладнанням Cisco: Обрані рішення повинні безпосередньо інтегруватися з наявною інфраструктурою на базі Cisco. Це дозволяє спростити адміністрування, знижуючи ризики конфліктів сумісності та забезпечуючи централізоване управління мережею.

2. Безпечне з'єднання з віддаленими офісами: Оскільки організація має кілька віддалених офісів, важливо забезпечити безпечне з'єднання між ними і головним офісом через інтернет. Необхідно використовувати надійні VPN-рішення для створення захищених тунелів між мережами.

3. Масштабованість та гнучкість: Технічні рішення повинні дозволяти легко розширювати мережу та підключати нові філії або користувачів, забезпечуючи гнучкість у впровадженні та налаштуванні нових сервісів.

4. Висока продуктивність: Забезпечення високої пропускну здатності та мінімальних затримок під час обміну трафіком між офісами та користувачами є критичним. Обладнання повинно забезпечувати оптимальну продуктивність навіть при інтенсивних навантаженнях.

5. Розширені функції захисту: Обране обладнання має підтримувати сучасні технології виявлення та запобігання вторгнень (IPS), управління політиками доступу, захист від шкідливого програмного забезпечення, а також можливості шифрування для VPN-з'єднань.

Для того, щоб обрати оптимальне рішення, яке буде підходити під описані вище критерії вибору, проведемо порівняння найвідоміших технологій для забезпечення VPN [6]. Найпоширенішими серед них є:

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

- IPsec VPN – стандартний протокол для забезпечення шифрування та безпеки на мережевому рівні. Він забезпечує захист IP-пакетів, використовуючи дві основні функції – AH (Authentication Header) і ESP (Encapsulating Security Payload).
- PPTP VPN – простий і швидкий протокол тунелювання, який забезпечує базову безпеку через MPPE (Microsoft Point-to-Point Encryption).
- PPPoE VPN – протокол, що поєднує PPP (Point-to-Point Protocol) з Ethernet, забезпечуючи автентифікацію користувачів при підключенні до мережі.
- L2TP VPN – протокол, що забезпечує тунелювання через два рівні, зазвичай використовується разом з IPsec для шифрування.
- OpenVPN SSL – VPN-протокол, що використовує SSL/TLS для захищеного тунелювання, забезпечуючи високий рівень безпеки та гнучкість налаштування. Популярний завдяки підтримці багатьох платформ.

Ці технології відрізняються між собою за рівнем захисту, масштабованістю, зручністю у впровадженні та продуктивністю [7]. У наведеній нижче таблиці порівняно основні особливості цих рішень.

Таблиця 1.1 – Порівняння провідних технологій VPN

Тип VPN	IPsec	PPTP	PPPoE	L2TP	OpenVPN
Призначення	Захист даних, передаваних через IP-мережі	Простий доступ до віддалених мереж	Підключення до Інтернет-провайдерів через Ethernet	З'єднання VPN через два рівні тунелювання	Віддалений доступ та створення захищених тунелів
Основні характеристики	Шифрує IP-пакети; підтримує AH та ESP	Швидкий і простий у налаштуванні; використовує MPPE	Поєднує PPP з Ethernet; забезпечує автентифікацію	Використовує UDP для обміну даними	Використовує SSL/TLS для шифрування
Переваги	Високий рівень безпеки, гнучкість у налаштуваннях	Легкість налаштування, підтримка широкого спектру платформ	Поширена технологія для ADSL-підключень	Краще шифрування, підтримка віртуальних приватних мереж	Високий рівень безпеки, гнучкість, підтримка багатьох платформ

Тип VPN	IPSec	PPTP	PPPoE	L2TP	OpenVPN
Недоліки	Складність налаштування, вимоги до ресурсів	Низький рівень безпеки, вразливий до атак	Не підходить для створення VPN; вразливий до атак	Не забезпечує шифрування самостійно, потребує IPSec	Може бути складним у налаштуванні для новачків
Безпека	Висока	Низька	Середня	Середня	Висока
Сумісність	Підтримується більшістю пристроїв	Підтримується більшістю пристроїв	Широка підтримка, особливо для ADSL	Підтримується більшістю пристроїв	Широка підтримка
Продуктові рішення	Cisco ASA, Juniper, Fortinet	Windows built-in, Cisco VPN Client	Cisco routers, Mikrotik, TP-Link routers	Windows built-in, Cisco routers, Fortinet	OpenVPN, Cisco AnyConnect, VyprVPN

Також для обладнання Cisco існують кілька варіантів використання міжмережових екранів, що дозволяють забезпечити захист на периметрі мережі. Серед найвідоміших рішень можна виділити:

- Firewall ZL1 – потужний міжмережовий екран, що забезпечує комплексний захист корпоративних мереж, включаючи функції контролю трафіку та виявлення загроз.
- Cisco ASA – багатофункціональний міжмережовий екран, що підтримує IPSec VPN, SSL VPN, а також функції виявлення та запобігання вторгнень (IPS).
- Checkpoint FireWall-1 – рішення для забезпечення безпеки мережі з потужними можливостями фільтрації, управління політиками доступу та виявлення загроз.
- Fortinet FortiGate – міжмережовий екран, що забезпечує інтеграцію функцій фаєрволу, VPN та захисту від шкідливого програмного забезпечення, а також аналітики загроз у реальному часі.
- WatchGuard Firebox – потужний пристрій для захисту мережі з функціями фільтрації контенту, управління пропускнуою здатністю та виявлення загроз.

Ці пристрої відрізняються між собою за рівнем захисту, масштабованістю, зручністю у впровадженні та продуктивністю. У наведеній нижче таблиці порівняно основні особливості цих рішень.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 1.2 – Порівняння популярних фаєрволів

Пристрій	Firewall ZL1	Cisco ASA	Checkpoint FireWall-1	Fortinet FortiGate	WatchGuard Firebox
Призначення	Захист мережі та контроль доступу	Багатофункціональний міжмережевий екран	Захист периметра мережі	Збалансування навантаження, захист від загроз	Захист мережі малого та середнього бізнесу
Основні характеристики	Основні функції фаєрволу, простота використання	Підтримка VPN, IPS, IDS, фільтрація трафіку, гнучкі політики безпеки	Гнучка система управління політиками безпеки, інтеграція з різними платформами	Інтеграція з функціями захисту, такими як IPS, захист від шкідливого програмного забезпечення, VPN	Простота налаштування, інтеграція з функціями захисту та моніторингу, хмарні функції
Переваги	Інтуїтивно зрозумілий інтерфейс	Висока продуктивність і надійність	Надійна безпека, потужні можливості звітності та аналітики	Висока продуктивність, багатофункціональність, доступність для малих і середніх підприємств	Простий інтерфейс управління, хороше співвідношення ціни і функціональності
Недоліки	Обмежена функціональність порівняно з конкурентами	Висока вартість та складність налаштування	Складна установка та управління	Може вимагати більшої настройки для оптимізації	Обмежені можливості для великих підприємств
Безпека	Висока	Висока	Висока	Висока	Висока
Сумісність	Сумісний з основними мережевими технологіями	Широка сумісність з різними мережевими пристроями	Сумісний з різними платформами і технологіями	Підтримує різні мережеві платформи	Сумісний з основними мережевими технологіями

За результатами порівняння Cisco ASA та IPsec Site-to-Site VPN були обрані як найкращі рішення для проекту. Це було зумовлено кількома факторами. По-перше, обидва рішення мають високу сумісність з обладнанням Cisco, що спрощує інтеграцію та управління в мережі. По-друге, Cisco ASA - це універсальний брандмауер, який не тільки захищає мережу, але й підтримує різні протоколи VPN, включаючи IPsec, що робить його універсальним інструментом безпеки. По-третє, Cisco ASA оснащений потужними функціями виявлення та запобігання вторгненням (IPS),

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

які забезпечують високий рівень безпеки конфіденційних даних організації. Крім того, IPsec Site-to-Site VPN забезпечує безпечне з'єднання між віддаленими мережами, що важливо для організацій з філіями або віддаленими працівниками, оскільки забезпечує надійне шифрування та автентифікацію даних.

1.4 Постановка технічного завдання

Метою проекту є забезпечення захищеного обміну трафіком через корпоративну мережу, і він має низку ключових цілей та завдань. Основна мета полягає у створенні надійної та безпечної інфраструктури для обробки даних, щоб зменшити ризики, пов'язані з несанкціонованим доступом та витоком інформації. Для досягнення цієї мети необхідно впровадити низку технічних рішень, включаючи належну сегментацію мережі, використання найсучасніших безпечних протоколів та інтеграцію надійних міжмережевих екранів.

Для досягнення цієї мети необхідно врахувати наступні основні вимоги:

1. Вимоги до безпеки: впровадження надійних методів шифрування та автентифікації для захисту даних, що передаються.
2. Сумісність: вибір рішень, які безперешкодно інтегруються з існуючим обладнанням Cisco в організації.
3. Продуктивність: забезпечення високої швидкості обробки даних і можливості масштабування системи в майбутньому.
4. Легкість управління: спрощення адміністративних завдань і моніторингу безпеки.
5. Масштабованість: система повинна бути здатною до подальшого розширення без суттєвих змін у базовій архітектурі.

В ході аналізу основних аспектів забезпечення захищеного обміну трафіком були розглянуті різні технології та рішення, що забезпечують необхідний рівень захисту. Виділено три основні типи мережеских протоколів: комунікаційні (TCP, UDP, HTTP, FTP), керування (ICMP, SNMP, DNS) та безпеки (SSH, TLS/SSL, IPsec), а також поняття міжмережеских екранів та віртуальних приватних мереж (VPN).

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Було проведено порівняння основних технологій VPN, включаючи IPSec, PPTP, PPPoE, L2TP та OpenVPN. Результати показали, що IPSec VPN пропонує найвищий рівень безпеки завдяки використанню складних методів шифрування та аутентифікації, що робить її ідеальним рішенням для безпечного обміну даними в корпоративних мережах. Аналогічним чином ми порівняли міжмережеві екрани, включаючи Firewall ZL1, Cisco ASA, Checkpoint FireWall-1, Fortinet FortiGate і WatchGuard Firebox, і виявили, що Cisco ASA є універсальним рішенням, яке підтримує IPSec VPN, SSL VPN та функції виявлення та запобігання вторгнень (IPS), що робить його найкращим вибором для цього проекту.

Згідно з проведеним аналізом, поєднання Cisco ASA та IPsec Site-to-Site VPN дозволить створити безпечну мережу, що відповідає всім вимогам проекту, забезпечуючи при цьому надійний захист від зовнішніх загроз і збереження конфіденційності даних.

Висновок до першого розділу:

У першому розділі були розглянуті основні аспекти забезпечення захищеного обміну трафіком, зокрема типи мережевих пристроїв та ключові практики безпеки. Описано основні технології та протоколи, важливі для ефективного захисту даних. Порівняння технологій VPN і міжмережевих екранів вказало на переваги Cisco ASA та IPsec Site-to-Site VPN, які виявилися найкращими рішеннями для реалізації проекту з використанням обладнання Cisco.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

РОЗДІЛ 2 ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО ОБМІНУ ТРАФІКОМ

2.1 Аналіз мережевої інфраструктури підприємства та проблеми захисту

На даному етапі розвитку майже кожен бізнес потребує ефективної комп'ютерної мережі для забезпечення зв'язку між співробітниками в межах одного офісу та між різними відділами, навіть якщо вони знаходяться в інших містах чи країнах. Комп'ютерна мережа [8] дозволяє швидко обмінюватися інформацією та координувати роботу всіх підрозділів компанії.

Корпоративна мережа - це внутрішня мережа компанії, доступ до якої мають лише працівники організації. Вона використовується для підтримки діяльності компанії і не надає доступу стороннім користувачам, наприклад, телекомунікаційним провайдерам. Залежно від розміру компанії та завдань, які вона вирішує, мережа може бути локальною мережею одного відділу, мережею, що охоплює кілька будівель (кампусів), або повноцінною корпоративною мережею, що з'єднує всі підрозділи.

Комп'ютерні мережі можна класифікувати за такими критеріями: кількість комп'ютерів, топологія, призначення, тип сервісу, методи управління та доступу, тип середовища передачі та швидкість передачі даних. Ефективність бізнесу значною мірою залежить від конфігурації та захисту мережі.

Також не менш важливою характеристикою корпоративної мережі є масштабованість, яка дозволяє мережі адаптуватися до зростання організації. Це означає, що мережа повинна мати можливість легко підтримувати збільшення кількості користувачів, пристроїв або офісів без необхідності радикально змінювати свою структуру. Наприклад, при відкритті нових філій або збільшенні кількості співробітників компанія може інтегрувати їх в існуючу мережу з мінімальними витратами часу і ресурсів.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

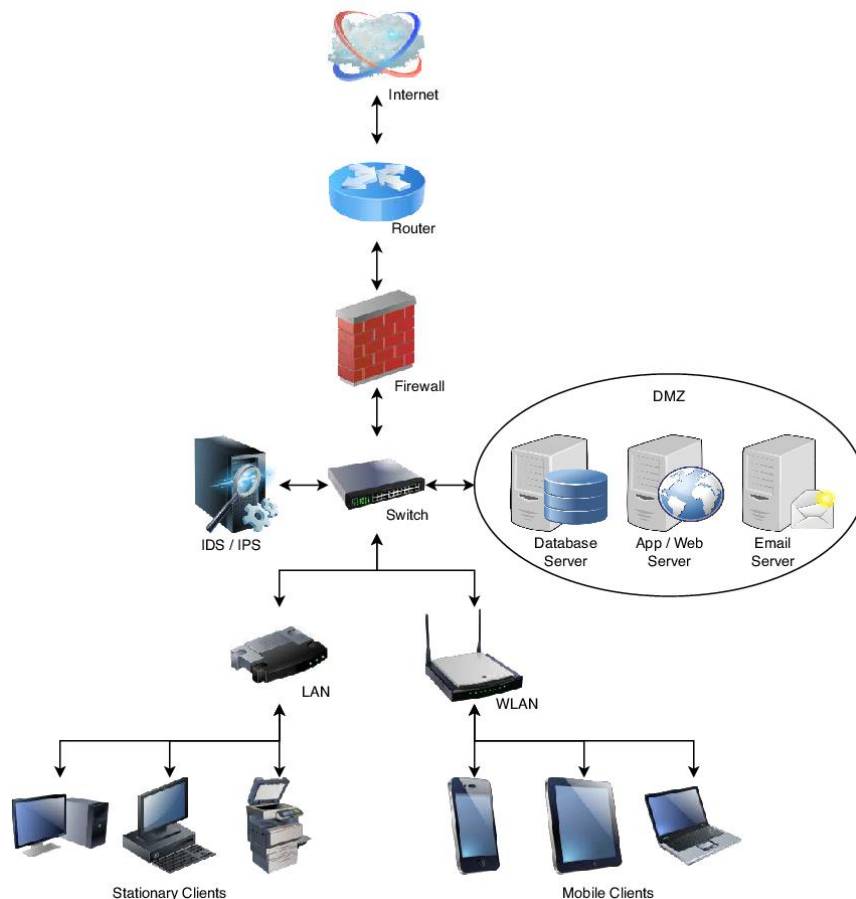


Рисунок 2.1 – Узагальнена схема корпоративної мережі

Сучасні мережі дуже складні через різноманітність конфігурацій, протоколів і технологій. Щоб упростити їхнє розуміння, можна використовувати ієрархічну модель. Ієрархії дозволяють структурувати всі компоненти мережі і полегшують їх аналіз. Компанія Cisco розробила ієрархічну модель [9], яка допомагає будувати, експлуатувати і підтримувати великі і надійні мережі. Ця модель має три рівні:

1. Базовий рівень (Core Layer): це ядро мережі, яке відповідає за швидкий та надійний обмін великими обсягами даних. Тут відбувається комутація трафіку для багатьох користувачів. Якщо на базовому рівні виникає помилка, це вплине на всіх користувачів, тому важливо забезпечити його високу надійність та швидкість передачі даних.

2. Рівень поширення (Distribution Layer): знаходиться між базовим рівнем і рівнем доступу. Цей рівень відповідає за маршрутизацію, фільтрацію трафіку та визначення правил доступу до базового рівня. Він також оптимізує обробку запитів

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

до служб і формує мережеву політику. Тут реалізуються такі функції, як перерозподіл маршрутів, налаштування системи безпеки (наприклад, брандмауерів) та VLAN-маршрутизація.

3. Рівень доступу (Access Layer): відповідає за управління доступом користувачів до мережевих ресурсів. На цьому рівні важливо, щоб більшість ресурсів була доступна локально для користувачів. Рівень доступу займається перенаправленням трафіку до віддалених служб і виконує такі задачі, як сегментація мережі та контроль доступу.

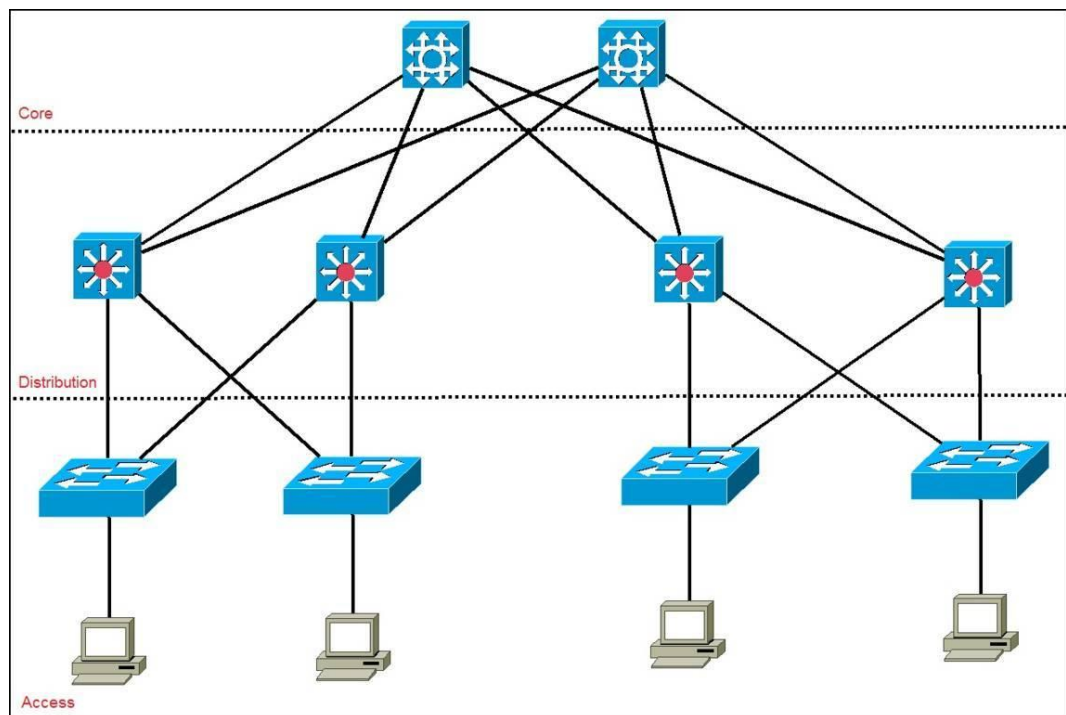


Рисунок 2.2 – Приклад ієрархічної моделі компанії Cisco

Розроблена корпоративна мережа нашої організації також базується на ієрархічній моделі трьохрівневої структури, що дозволяє ефективно організувати та управляти мережею. Організація складається з головного офісу та двох віддалених філій, що забезпечує нам можливість проводити комунікацію та обмін даними на великих відстанях. Одним із важливих елементів нашої мережі є демілітаризована зона (DMZ) [10], яка призначена для захисту критично важливих серверів від зовнішніх загроз. Ця зона забезпечує додатковий рівень безпеки, що є особливо важливим у разі кібератак.

У нашій корпоративній мережі також реалізовано віддалене підключення, що дозволяє працівникам працювати з дому чи з інших віддалених місць. Це рішення

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

стало особливо актуальним у сучасних умовах, коли гнучкий графік роботи і дистанційне виконання завдань набувають популярності. Віддалене підключення забезпечується через VPN, що дозволяє користувачам безпечно з'єднуватися з корпоративною мережею, забезпечуючи конфіденційність та захист даних.

Для з'єднання між головними пристроями в мережі використовуються Gigabit Ethernet, який є надійним і швидким рішенням для передачі даних. Це забезпечує високу продуктивність мережі, адже Gigabit Ethernet підтримує передачу даних на швидкостях до 1 Гбіт/с, що робить його ідеальним для нашої організації з великою кількістю працівників.

У проєкті ми використовуємо маршрутизатори моделей Cisco 2911 та 1841 а також фаєрвол Cisco ASA 5506-X, які розташовані у центрі мережі. Ці пристрої виконують роль бар'єра між нашою внутрішньою мережею та зовнішнім світом, відфільтровуючи весь вхідний та вихідний трафік. Це дозволяє нам забезпечити базовий захист від небажаних вторгнень і атак. На базовому рівні, таким чином, розташовані маршрутизатори та фаєрволи, які відповідають за первинну фільтрацію інформації та контроль доступу до мережі.

Окрім звичайних маршрутизаторів Cisco, в мережі також реалізовано бездротове підключення через Wi-Fi. Це дає можливість працівникам легко підключатися до мережі з мобільних пристроїв, ноутбуків або інших бездротових гаджетів. Безпроводні технології мають численні переваги, зокрема зручність використання, можливість підключення великої кількості пристроїв та гнучкість у виборі місця для роботи.

На розподільчому рівні ключову роль відіграють вже вказані вище маршрутизатори Cisco 2911 і комутатори серії Cisco 2960-24TT. Ці комутатори забезпечують швидку передачу даних між різними частинами мережі і мають вбудовані функції захисту, такі як контроль доступу та сегментація мережі. Це дозволяє нам оптимізувати роботу мережі і знижувати ризики потенційних загроз.

На рівні доступу розташовані кінцеві пристрої, такі як комп'ютери, ноутбуки та мобільні телефони, які використовують працівники для доступу до ресурсів мережі. Важливо, щоб ці пристрої були надійно захищені, оскільки вони є найбільш

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

вразливими до кібератак. З метою підвищення безпеки на цьому рівні, потрібно реалізувати політики контролю доступу та використання антивірусних рішень.

Щоб проілюструвати структуру нашої мережі, ми представимо короткий перелік основних компонентів. Хоча організація має велику кількість працівників, на схемі буде показано лише ключові елементи, що дозволить краще зрозуміти архітектуру нашої мережі. Це будуть маршрутизатори, комутатори, міжмережеві екрани, сервери, точки доступу Wi-Fi, а також кінцеві пристрої, які використовують працівники для роботи.

Звісно, часто у мережі ми стикаємося з певними проблемами, які потребують уваги. Наприклад, різноманітність апаратного і програмного забезпечення в різних підрозділах може ускладнювати інтеграцію та управління мережею. Також, при налаштуванні безпеки важливо враховувати ризики, пов'язані з віддаленим доступом, адже він може стати потенційним вектором атак. Наведемо короткий список основних проблем захисту мережі, описаної вище:

1. Безпека віддаленого підключення:

- Ризик несанкціонованого доступу через недостатньо захищені VPN-з'єднання.
- Можливість атак "людина посередині" (Man-in-the-Middle) під час передачі даних.

2. Вразливості бездротової мережі (Wi-Fi):

- Загроза доступу зловмисників до мережі через відкриті або недостатньо захищені Wi-Fi точки.
- Відсутність шифрування даних може призвести до перехоплення чутливої інформації.

3. Контроль доступу:

- Невірні налаштування системи контролю доступу можуть призвести до підключення неавторизованих пристроїв.
- Складність управління великим числом користувачів і пристроїв, що підключаються.

4. Захист даних:

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

- Небезпека витоку конфіденційної інформації через слабкі місця в захисті серверів.
- Відсутність регулярних резервних копій може призвести до втрати даних у разі атаки.

5. Системи моніторингу та управління:

- Відсутність або недостатня ефективність системи моніторингу для виявлення загроз у реальному часі.
- Недостатня увага до оновлень програмного забезпечення та патчів, що може призвести до вразливостей.

6. Фізичний доступ:

- Небезпечний фізичний доступ до критичних мережевих пристроїв, що може призвести до несанкціонованих змін або пошкоджень.

7. Неправильні конфігурації:

- Неправильна конфігурація мережевих пристроїв може створити вразливості та знизити рівень безпеки.

2.2 Розробка загальної структури підсистеми захищеного мережевого обміну

Після аналізу мережі можна приступити до розробки загальної структури і схеми мережі. Оскільки наша організація має головний офіс, дві віддалених філії та змогу підключення дистанційно, було б доречно побудувати її таким чином:

Основою всієї структури мережі є маршрутизатори Cisco 2911 і Cisco 1841, а також брандмауери Cisco ASA 5506-X, які забезпечують високий рівень безпеки та управління трафіком. Мережа розділена на кілька функціональних зон, кожна з яких виконує свої завдання та має свої особливості. Однією з таких зон є головний офіс, де розташовано велику кількість робочих місць і пристроїв, які потребують надійного захисту.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

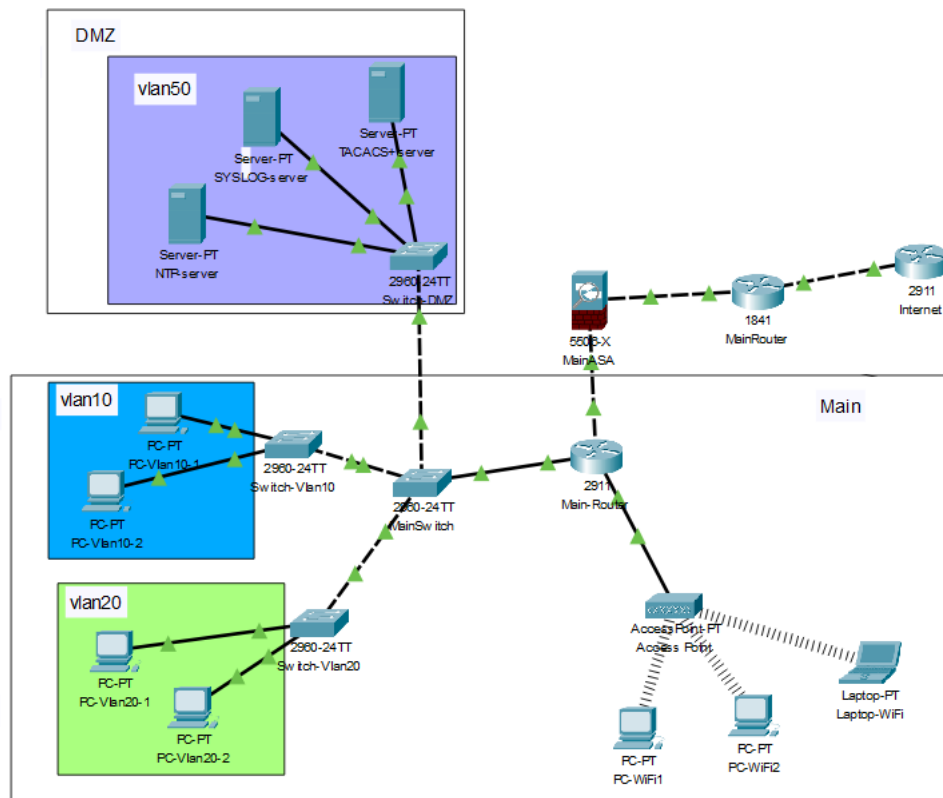


Рисунок 2.3 – Вигляд частини мережі головного офісу (DMZ і зона користувачів)

1. Головний офіс — це найважливіша частина мережі, де знаходиться найбільша кількість робочих станцій, серверів та інших пристроїв. Ця зона є критично важливою для функціонування організації, тому її захист є пріоритетним. На периметрі цієї зони встановлено брандмауер Cisco ASA 5506-X, який контролює весь трафік, що надходить та виходить з головного офісу. Це рішення забезпечує надійний захист від зовнішніх загроз, таких як атаки або несанкціонований доступ.

Брандмауер розділяє внутрішню мережу на дві ключові частини: демілітаризовану зону (DMZ) та зону користувачів.

DMZ (Demilitarized Zone) — це окрема мережа, яка призначена для зберігання та доступу до серверів, що використовуються для зовнішнього обміну даними. У нашій мережі в DMZ будуть розташовані основні сервери, такі як:

- Syslog-сервер (для зберігання журналів подій),
- TACACS+ (для автентифікації та управління доступом),
- NTP-сервер (для синхронізації часу).

DMZ дозволяє зовнішнім користувачам отримувати доступ до певних ресурсів (серверів) без ризику для основної внутрішньої мережі. Це є важливим аспектом безпеки, оскільки навіть якщо зовнішня атака буде спрямована на ці сервери, вона не зможе легко проникнути в головну мережу.

Зона користувачів — це зона, в якій знаходяться всі робочі станції співробітників, а також інші пристрої, такі як принтери, телефони та інші IoT-пристрої. Вона також поділена на декілька сегментів за допомогою VLAN, що дозволяє оптимізувати трафік і підвищити безпеку. Використання VLAN допомагає ізолювати різні групи користувачів (наприклад, адміністративний персонал, IT-відділ, відділ маркетингу тощо), що знижує ризики внутрішніх загроз та полегшує управління мережею.

Також в головному офісі передбачається використання точки доступу (Access Point) для бездротового з'єднання мобільних пристроїв та ноутбуків. Бездротова мережа повинна бути налаштована з використанням сучасних стандартів безпеки, таких як WPA2 або WPA3, щоб запобігти несанкціонованому доступу до внутрішніх ресурсів.

Таким чином, головний офіс має всі необхідні компоненти для стабільної та безпечної роботи організації. Завдяки розділенню на окремі зони (DMZ, зона користувачів) і використанню VLAN для сегментації мережі, досягається висока продуктивність і безпека. Брандмауер Cisco ASA 5506-X грає ключову роль у захисті від зовнішніх загроз і забезпечує безпечний доступ до зовнішніх ресурсів через DMZ.

Це рішення дозволяє організації не тільки захистити свої дані, але й забезпечити безперебійну роботу навіть у разі спроб атак або зовнішніх загроз.

2. Домашня мережа. Ця зона відповідає за підключення з домашнього комп'ютера або інших пристроїв, які знаходяться поза межами корпоративної мережі, але потребують доступу до її ресурсів. Важливим аспектом у цьому випадку є забезпечення надійного та захищеного каналу зв'язку між домом і головним офісом.

Між основним маршрутизатором головного офісу та домашнім маршрутизатором встановлюється VPN-з'єднання. Домашній маршрутизатор у цьому випадку виступає кінцевою точкою VPN-з'єднання. Він забезпечує маршрутизацію трафіку між домашніми пристроями (наприклад, комп'ютерами, ноутбуками, смартфонами) і

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

корпоративною мережею через захищений тунель. Це дозволяє працювати віддалено так, ніби користувач фізично знаходиться в офісі, що особливо важливо для віддалених працівників або для тих, хто працює з чутливою інформацією.

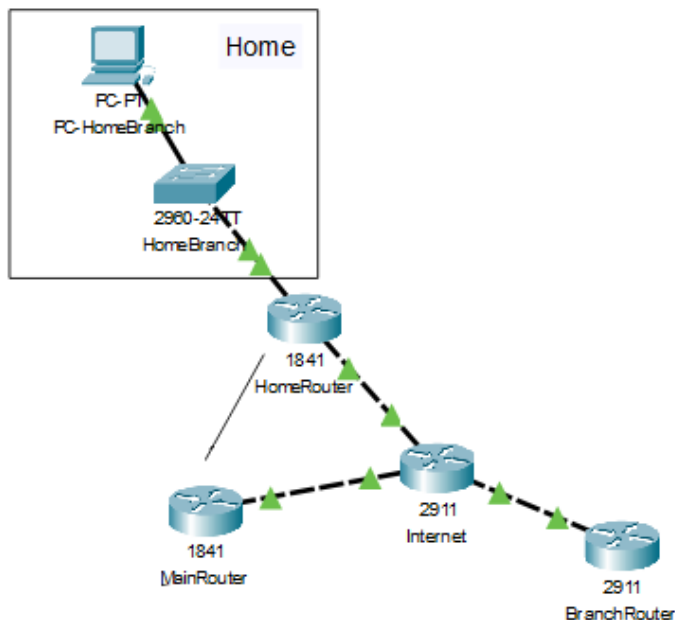


Рисунок 2.4 – Вигляд частини домашньої мережі разом з VPN-з'єднанням

Завдяки використанню VPN-з'єднання співробітники можуть працювати з будь-якого місця, не турбуючись про безпеку свого підключення. Це рішення ідеально підходить для підтримки віддаленої роботи або гнучкого графіка співробітників, які можуть виконувати свої обов'язки поза офісом, зберігаючи високий рівень захисту корпоративної мережі.

3. Гілка філій. Ця зона відповідає за організацію двох віддалених офісів, які повинні бути надійно інтегровані в корпоративну мережу головного офісу. Щоб забезпечити безпеку та надійність з'єднань між філіями і головним офісом, використовується спеціалізоване обладнання – брандмауери Cisco ASA 5506-X.

Філії підключені до одного маршрутизатора – BranchRouter який підключений напряду до Інтернету. Кожна філія має власний брандмауер, що працює на рівні мережевої безпеки. Усі брандмауери мережі мають VPN-з'єднання між собою для більшого захисту мережі. Це забезпечує захищений зв'язок між філіями і іншими мережами, дозволяючи безпечно передавати конфіденційні дані або забезпечувати доступ до центральних ресурсів компанії, таких як бази даних або файлові сервери.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

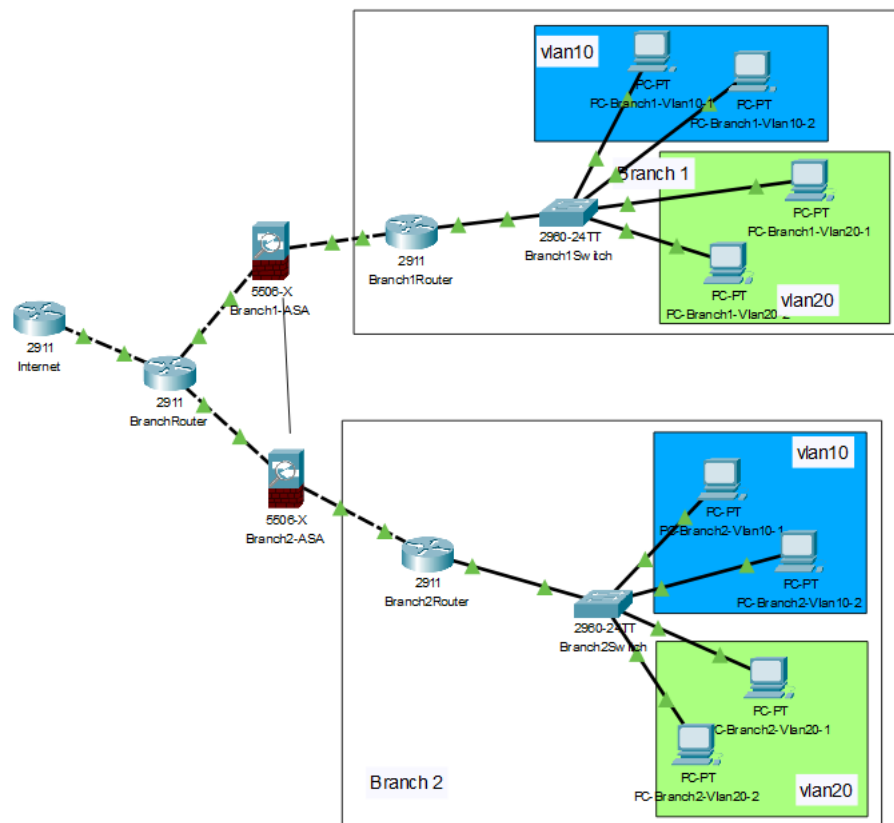


Рисунок 2.5 – Вигляд частини мережі з віддаленими філіями

Кожна філія також налаштована з використанням VLAN [11]. VLAN дозволяє розділити мережу на кілька віртуальних сегментів, що забезпечує більший рівень безпеки, підвищує ефективність адміністрування і керування мережею. Використання VLAN також спрощує адміністрування мережі, оскільки дозволяє легко налаштовувати і керувати окремими частинами мережі. Адміністратор може застосовувати різні політики безпеки для кожного VLAN, тим самим забезпечуючи контроль над тим, хто і що може робити в межах кожної філії.

Таким чином, віддалені офіси мають захищене підключення до головної мережі, а їхні внутрішні мережі ізольовані і добре структуровані за допомогою VLAN, що забезпечує безпеку і зручність в управлінні. Це рішення дозволяє філіям ефективно працювати, мати швидкий і захищений доступ до необхідних ресурсів, водночас забезпечуючи максимальний захист від можливих загроз, які можуть надходити як з Інтернету, так і зсередини мережі.

2.3 Розробка компонентів підсистеми захисту

Для забезпечення захисту мережевої інфраструктури було вирішено використовувати декілька ключових компонентів підсистеми безпеки. Кожен з них відіграє важливу роль у забезпеченні надійної роботи корпоративної мережі та захисту від зовнішніх і внутрішніх загроз.

1. Міжмережеві екрани Cisco ASA 5506-X. Важливою складовою підсистеми захисту є брандмауери Cisco ASA 5506-X, які забезпечують контроль трафіку та захист від несанкціонованого доступу. ASA використовується для розмежування зон мережі, таких як внутрішня корпоративна мережа, демілітаризована зона (DMZ), а також зовнішні підключення через Інтернет.

Основні функції міжмережевого екрану включають:

- Контроль доступу через списки контролю доступу (ACL).
- Натуралізація адрес (NAT) для маскуванню внутрішньої мережі.
- Інспекція трафіку та блокування підозрілих з'єднань.

2. Тунель IPSec Site-to-Site VPN. Для забезпечення безпечного обміну даними між головним офісом, віддаленими філіями та домашньою мережею буде налаштований тунель IPSec Site-to-Site VPN. У реальних умовах всі VPN-з'єднання мали б проходити через головний офіс, що дозволило б централізовано контролювати трафік та забезпечити безпечний доступ до корпоративних ресурсів. Однак, через обмеження Cisco Packet Tracer VPN буде налаштоване між міжмережевими екранами та деякими маршрутизаторами. Це забезпечить базову симуляцію шифрування трафіку, гарантуючи конфіденційність і цілісність даних.

3. SSHv2 (Secure Shell version 2). Для віддаленого адміністрування мережевих пристроїв буде використовуватися захищений протокол SSH 2 версії [12]. На відміну від незахищеного протоколу Telnet, SSH шифрує всі дані, що передаються між адміністратором та мережевим пристроєм, забезпечуючи захист від перехоплення паролів та іншої конфіденційної інформації.

4. VLAN (Virtual Local Area Network). Для сегментації мережі буде використовуватися технологія VLAN, яка дозволяє розділити фізичну мережу на логічні се-

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

гменти. Це забезпечить ізоляцію різних груп користувачів та підвищить безпеку мережі. Наприклад, у головному офісі планується створити окремі VLAN для адміністративного персоналу та інших користувачів. Це дозволить контролювати трафік і уникнути можливих конфліктів чи витоків інформації.

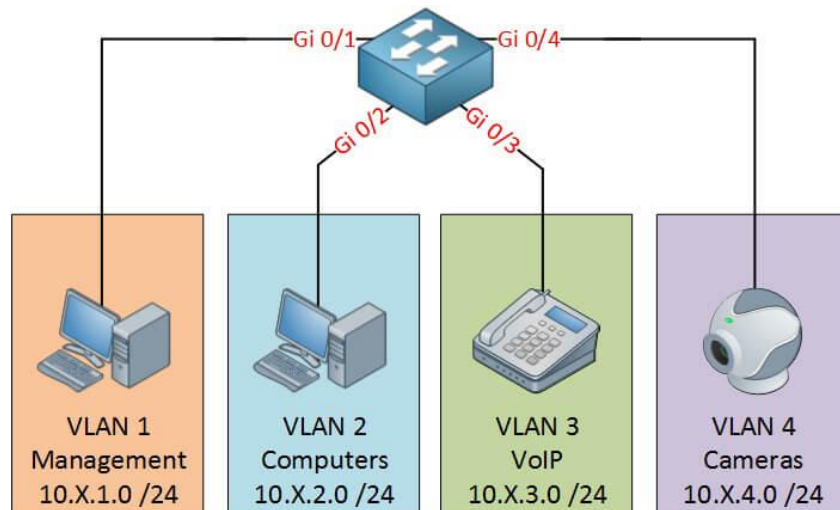


Рисунок 2.6 – Приклад розміщення пристроїв у різних VLAN

5. DHCP (Dynamic Host Configuration Protocol). Для автоматичного призначення IP-адрес всім підключеним пристроям у мережі головного офісу буде використовуватися сервер DHCP [13]. Це дозволить зменшити кількість ручних налаштувань та уникнути конфліктів адрес. Використання DHCP спрощує адміністрування мережі, особливо в великих організаціях, де кількість пристроїв може постійно змінюватися.

6. AAA (Authentication, Authorization, and Accounting). Для управління доступом до мережевих ресурсів буде налаштована система AAA [14]. В якості протоколу буде використано TACACS+ (Terminal Access Controller Access-Control System), що забезпечує централізовану автентифікацію, авторизацію та облік дій користувачів. Це дозволить контролювати, хто має доступ до мережевих пристроїв і які дії вони можуть виконувати. Також TACACS+ забезпечує можливість ведення логів для аудиту дій адміністраторів.

7. SYSLOG (System Logging Protocol). Для моніторингу та аудиту подій у мережі буде використано протокол SYSLOG [15]. Він дозволяє зберігати та аналізувати журнали подій з усіх мережевих пристроїв, таких як брандмауери,

маршрутизатори та комутатори. Це дозволить вчасно виявляти проблеми у мережі, аналізувати підозрілу активність та проводити розслідування інцидентів безпеки.

8. ACL (Access Control Lists). Списки контролю доступу (ACL) будуть налаштовані на брандмауерах Cisco ASA для визначення, який трафік дозволений або заборонений на кожному інтерфейсі. ACL дозволять налаштувати точковий контроль доступу до різних зон мережі, захистивши її від несанкціонованого доступу як ззовні, так і всередині. З їх допомогою можна налаштувати доступ лише для певних користувачів чи пристроїв, забезпечуючи гнучкий та ефективний захист.

9. Port Security. Ця функція дозволяє контролювати, які пристрої можуть підключатися до конкретного порту, базуючись на MAC-адресах. За її допомогою можна обмежити кількість дозволених пристроїв на одному порту, а також заблокувати неавторизовані підключення. Port Security буде налаштовано на комутаторах Cisco для обмеження доступу до мережі через порти.

Запропоновані компоненти підсистеми захисту працюють разом для створення надійної та захищеної мережі, що відповідає сучасним вимогам безпеки. Використання фаєрволів, VPN, VLAN та інших механізмів захисту дозволить мінімізувати ризики атак, забезпечити конфіденційність та цілісність даних, а також гарантувати надійну роботу мережевої інфраструктури.

Висновок до другого розділу:

У другому розділі було розглянуто структуру корпоративних мереж і проаналізовано мережу організації за трирівневою моделлю компанії Cisco. Також була розроблена загальна структура мережі, продемонстровано її схему та описано принципи роботи. Було визначено та розроблено компоненти захисту підсистеми, зокрема протоколи та технології, які будуть використовуватися при побудові мережі для забезпечення захищеного обміну трафіком.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

РОЗДІЛ 3 ВПРОВАДЖЕННЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО ОБМІНУ ТРАФІКОМ

3.1 Вибір обладнання компанії Cisco для побудови підсистеми захищеного обміну трафіком

Cisco Systems є світовим лідером у виробництві обладнання для комп'ютерних мереж та розробці рішень для мережної безпеки. Компанія здобула високу репутацію завдяки своїм надійним продуктам і технологіям, які дозволяють будувати масштабовані та безпечні мережі різної складності. Обладнання Cisco використовується в корпоративних мережах по всьому світу завдяки своїй ефективності, надійності, високому рівню безпеки та багатофункціональності. Використання рішень Cisco дозволяє компаніям будувати мережеві інфраструктури, що відповідають вимогам сучасного ринку, з акцентом на безпеку та оптимізацію трафіку.

Для побудови проекту для підсистеми захищеного обміну трафіком буде використано такі пристрої від Cisco:

- Маршрутизатор Cisco 2911
- Маршрутизатор Cisco 1841
- Міжмережевий екран Cisco ASA 5506-K9
- Комутатор Cisco WS-C2960-24TT-L

1. Маршрутизатор Cisco 2911 [16] – це потужний маршрутизатор серії Cisco ISR (Integrated Services Router), призначений для середніх і великих організацій. Він забезпечує високопродуктивну маршрутизацію, підтримує безпеку, а також можливість інтеграції різних сервісів, таких як голосові та відеопослуги через IP.

Основні характеристики Cisco 2911:

- 3 гігабітні Ethernet порти, що дозволяють обробляти великий обсяг трафіку.
- Підтримка до 50 тунелів VPN, що забезпечує захищене з'єднання між філіями або віддаленими користувачами.
- Інтегрована підтримка фаєрволів та IPS (систем запобігання вторгненням).
- Можливість розширення функціональності за рахунок додаткових модулів.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

- Підтримка голосових та відеопослуг через IP, що робить його універсальним для використання у великій корпоративній мережі.

Переваги маршрутизатора Cisco 2911 полягають у його високій пропускній здатності та надійності. Він здатний обробляти значні обсяги даних, забезпечуючи при цьому високий рівень безпеки. Гнучкість у налаштуванні та можливість додавання нових модулів робить цей маршрутизатор ідеальним для розширення мережевої інфраструктури.

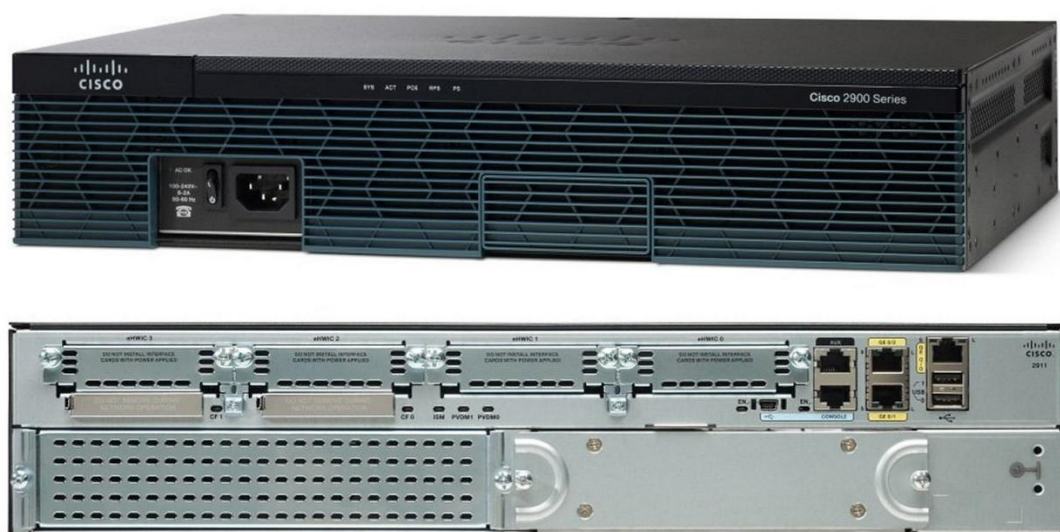


Рисунок 3.1 – Маршрутизатор Cisco 2911

2. Маршрутизатор Cisco 1841 [17] – це маршрутизатор серії ISR, який підходить для малого та середнього бізнесу, а також для віддалених офісів. Він дозволяє інтегрувати кілька мережевих сервісів на одному пристрої, що робить його універсальним інструментом для побудови надійної мережі.

Основні характеристики Cisco 1841:

- 2 порти Ethernet 10/100 Mbps для підключення до мережі.
- Підтримка VPN з пропускнуою здатністю до 800 Mbps для тунелів.
- Вбудована підтримка фаєрволів та IPS для запобігання атак.
- Можливість підтримки кількох VLAN, що дозволяє сегментувати мережу.
- Розширюваність за рахунок модулів, які додають підтримку додаткових функцій, таких як голосова передача.

		Балоболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

Переваги Cisco 1841 полягають у його компактності та простоті налаштування, що робить його ідеальним для віддалених філій. Підтримка VPN дозволяє забезпечити безпечний обмін даними між офісами, а сегментація мережі через VLAN допомагає зберігати дані в безпеці та забезпечує зручне адміністрування.



Рисунок 3.2 – Маршрутизатор Cisco 1841

3. Міжмережевий екран Cisco ASA 5506-K9 [18] – це потужний міжмережевий екран (фаєрвол), який забезпечує надійний захист мережі від зовнішніх загроз і атак. Він поєднує в собі функції фаєрволу, VPN-сервера та системи запобігання вторгненням (IPS).

Основні характеристики Cisco ASA 5506-K9:

- 8 гігабітних Ethernet портів для підключення до мережі.
- Підтримка VPN (IPSec, SSL), що дозволяє захистити з'єднання між віддаленими офісами або користувачами.
- Вбудований фаєрвол та IPS для виявлення та блокування атак на мережу.
- Підтримка VLAN через протокол 802.1Q для створення окремих сегментів мережі.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

- Можливість управління доступом за допомогою Access Control Lists (ACL), що підвищує безпеку мережі.

Переваги Cisco ASA 5506-K9 включають високу продуктивність та комплексний захист мережі. Інтеграція різних технологій безпеки в одному пристрої дозволяє забезпечити надійний захист від зовнішніх загроз. Підтримка VPN дозволяє створювати захищені з'єднання між різними частинами мережі, а сегментація трафіку за допомогою VLAN підвищує безпеку.

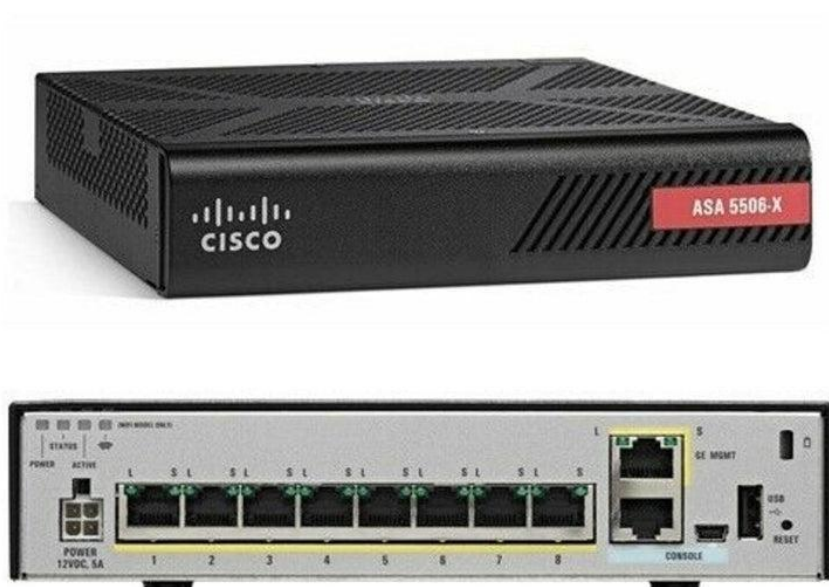


Рисунок 3.3 – Міжмережевий екран Cisco ASA5506-K9

4. Комутатор Cisco WS-C2960-24TT-L [19] – це комутатор рівня доступу, який призначений для побудови локальних мереж (LAN). Він забезпечує високошвидкісне комутування даних і підтримує різні функції для ефективного управління трафіком у мережі.

Основні характеристики Cisco WS-C2960-24TT-L:

- 24 порти Fast Ethernet (10/100 Mbps) та 2 гігабітних uplink порти для підключення до магістральної мережі.
- Підтримка VLAN для сегментації мережі.
- Підтримка функції QoS для управління пріоритетами трафіку та забезпечення якісного надання сервісів.
- Підтримка протоколу 802.1X для аутентифікації користувачів.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

Переваги Cisco WS-C2960-24TT-L полягають у його можливості забезпечувати ефективне управління локальною мережею. Він дозволяє створювати окремі сегменти мережі за допомогою VLAN, що покращує безпеку та полегшує адміністрування. Завдяки функціям QoS, комутатор може управляти трафіком, забезпечуючи пріоритетність критичних даних та сервісів у мережі.



Рисунок 3.4 – Комутатор Cisco WS-C2960-24TT-L

Обладнання Cisco, вибране для цього проекту, забезпечує високий рівень безпеки, масштабованість і продуктивність. Кожен пристрій має свої унікальні переваги, що дозволяє побудувати ефективну та захищену мережу для обміну трафіком між офісами та віддаленими користувачами.

3.2 Налаштування підсистеми захищеної мережі компанії

Першим етапом налагодження комп'ютерних мереж організації є виконання базових налаштувань. До цього етапу входить конфігурація інтерфейсів відповідно до визначених адрес, зазначених у таблиці 1 (див. Додаток Б). Спочатку буде виконано базове налаштування трьох ключових маршрутизаторів, які є центральними елементами мережі організації. Це – MainRouter (маршрутизатор головного офісу), HomeRouter (домашній маршрутизатор) і BranchRouter (маршрутизатор віддалених офісів). Саме ці пристрої забезпечують основний обмін даними між усіма сегментами мережі, а їх правильна конфігурація є критично важливою для стабільної та безпечної роботи всієї інфраструктури.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

Physical Config **CLI** Attributes

IOS Command Line Interface

```

Router>en
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MainRouter
MainRouter(config)#interface FastEthernet0/0
MainRouter(config-if)# ip address 20.10.1.2 255.255.255.252
MainRouter(config-if)#no shutdown

MainRouter(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

MainRouter(config-if)#exit
MainRouter(config)#interface FastEthernet0/1
MainRouter(config-if)# ip address 40.10.1.1 255.255.255.252
MainRouter(config-if)# no shutdown

MainRouter(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

MainRouter(config-if)#exit
MainRouter(config)#

```

Рисунок 3.5 – Базове налаштування маршрутизатора MainRouter

Physical Config **CLI** Attributes

IOS Command Line Interface

```

Router>en
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname HomeRouter
HomeRouter(config)#interface FastEthernet0/0
HomeRouter(config-if)#ip address 10.10.1.2 255.255.255.252
HomeRouter(config-if)#no shutdown

HomeRouter(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

HomeRouter(config-if)#exit
HomeRouter(config)#interface FastEthernet0/1
HomeRouter(config-if)# ip address 100.10.1.1 255.255.255.0
HomeRouter(config-if)# no shutdown

HomeRouter(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

HomeRouter(config-if)#exit
HomeRouter(config)#ip dhcp excluded-address 100.10.1.1 100.10.1.2
HomeRouter(config)#ip dhcp pool HomeBranch1
HomeRouter(dhcp-config)# network 100.10.1.0 255.255.255.0
HomeRouter(dhcp-config)# default-router 100.10.1.1
HomeRouter(dhcp-config)# domain-name my.net
HomeRouter(dhcp-config)#exit
HomeRouter(config)#

```

Рисунок 3.6 – Базове налаштування маршрутизатора HomeRouter

```

BranchRouter
Physical Config CLI Attributes
IOS Command Line Interface

Router>en
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BranchRouter
BranchRouter(config)#interface GigabitEthernet0/0
BranchRouter(config-if)# ip address 50.10.1.1 255.255.255.252
BranchRouter(config-if)#no shutdown

BranchRouter(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

BranchRouter(config-if)#exit
BranchRouter(config)#interface GigabitEthernet0/1
BranchRouter(config-if)# ip address 60.10.1.1 255.255.255.252
BranchRouter(config-if)# no shutdown

BranchRouter(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

BranchRouter(config-if)#exit
BranchRouter(config)#interface GigabitEthernet0/2
BranchRouter(config-if)# ip address 30.10.1.2 255.255.255.252
BranchRouter(config-if)#no shutdown

BranchRouter(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

BranchRouter(config-if)#exit
BranchRouter(config)#

```

Рисунок 3.7 – Базове налаштування маршрутизатора BranchRouter

Наступним кроком у процесі базового налаштування є конфігурація фаєрволів. Налагодження продемонстроване на фаєрволах MainASA та Branch1-ASA (оскільки налаштування фаєрволів віддалених філій здійснено аналогічно).

```

MainASA
Physical Config CLI Attributes
IOS Command Line Interface

ciscoasa>en
Password:
ciscoasa#conf t
ciscoasa(config)#hostname MainASA
MainASA(config)#interface GigabitEthernet1/1
MainASA(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
MainASA(config-if)#security-level 0
MainASA(config-if)# ip address 40.10.1.2 255.255.255.252
MainASA(config-if)#exit
MainASA(config)#interface GigabitEthernet1/2
MainASA(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
MainASA(config-if)# security-level 100
MainASA(config-if)# ip address 70.10.1.1 255.255.255.252
MainASA(config-if)#exit
MainASA(config)#

```

Рисунок 3.8 – Базове налаштування брандмауера MainASA

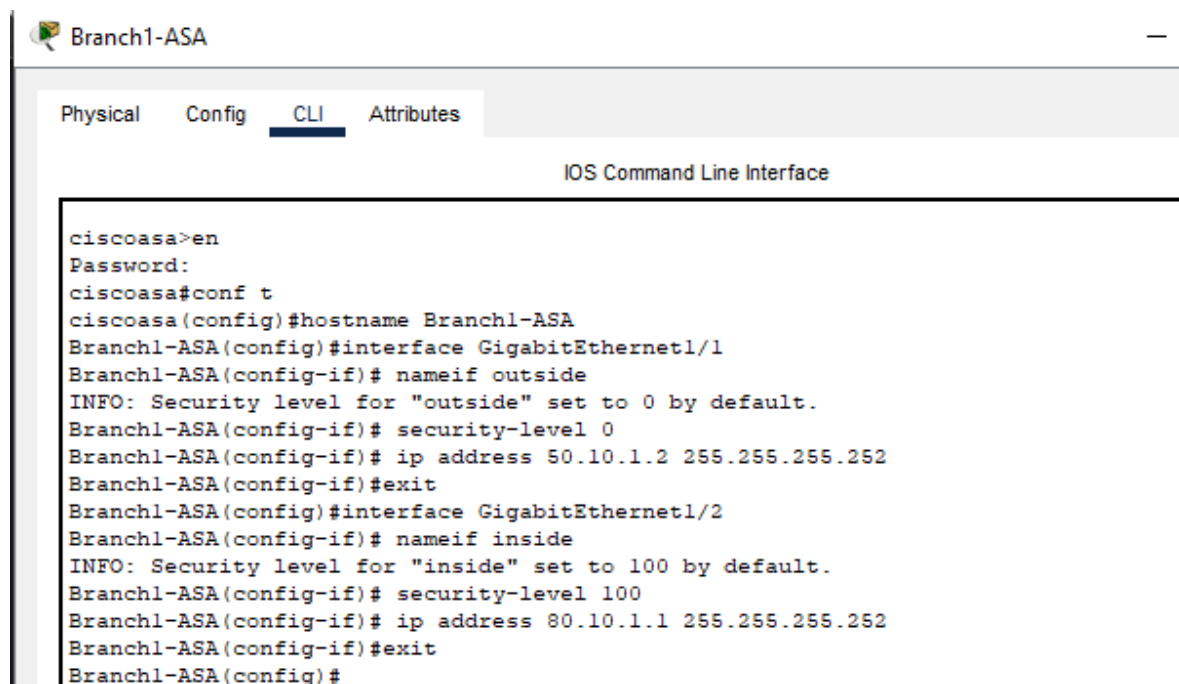


Рисунок 3.9 – Базове налаштування брандмауера Branch1-ASA

Після базового налаштування брандмауерів можна перейти до конфігурації маршрутизаторів внутрішньої зони, які відповідають за забезпечення зв'язку всередині корпоративної мережі. Вони мають підтримувати кілька VLAN для сегментації трафіку, зокрема VLAN 10, 20 і 50, які представляють окремі логічні сегменти мережі (наприклад, відділи або сервіси). На прикладі маршрутизаторів Main-Router і Branch1Router продемонстровано налаштування, яке включає: роздачу автоматичних IP-адрес через DHCP для кожного з VLAN, що дозволяє автоматизувати процес підключення клієнтів до мережі; конфігурацію фізичних інтерфейсів і підінтерфейсів [20] для забезпечення коректного функціонування VLAN і маршрутизації між ними.

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Main-Router
Main-Router(config)#interface GigabitEthernet0/0
Main-Router(config-if)# ip address 70.10.1.2 255.255.255.252
Main-Router(config-if)#no shut

Main-Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Main-Router(config-if)#exit
Main-Router(config)#interface GigabitEthernet0/1.10
Main-Router(config-subif)# encapsulation dot1Q 10
Main-Router(config-subif)# ip address 110.10.1.1 255.255.255.0
Main-Router(config-subif)#no shut
Main-Router(config-subif)#ex
Main-Router(config)#interface GigabitEthernet0/1.20
Main-Router(config-subif)# encapsulation dot1Q 20
Main-Router(config-subif)# ip address 120.10.1.1 255.255.255.0
Main-Router(config-subif)#no shut
Main-Router(config-subif)#ex
Main-Router(config)#interface GigabitEthernet0/1.50
Main-Router(config-subif)# encapsulation dot1Q 50
Main-Router(config-subif)# ip address 150.10.1.1 255.255.255.0
Main-Router(config-subif)#no shut
Main-Router(config-subif)#ex
Main-Router(config)#interface GigabitEthernet0/2
Main-Router(config-if)# ip address 130.10.1.1 255.255.255.0
Main-Router(config-if)#no shut

Main-Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

Main-Router(config-if)#ex
Main-Router(config)#ip dhcp excluded-address 110.10.1.1 110.10.1.4
Main-Router(config)#ip dhcp excluded-address 120.10.1.1 120.10.1.4
Main-Router(config)#ip dhcp excluded-address 130.10.1.1
Main-Router(config)#ip dhcp pool MainRouter1
Main-Router(dhcp-config)# network 110.10.1.0 255.255.255.0
Main-Router(dhcp-config)# default-router 110.10.1.1
Main-Router(dhcp-config)# domain-name my.net
Main-Router(dhcp-config)#ex
Main-Router(config)#ip dhcp pool MainRouter2
Main-Router(dhcp-config)# network 120.10.1.0 255.255.255.0
Main-Router(dhcp-config)# default-router 120.10.1.1
Main-Router(dhcp-config)# domain-name my.net
Main-Router(dhcp-config)#ex
Main-Router(config)#ip dhcp pool Main3
Main-Router(dhcp-config)# network 130.10.1.0 255.255.255.0
Main-Router(dhcp-config)# default-router 130.10.1.1
Main-Router(dhcp-config)# domain-name my.net
Main-Router(dhcp-config)#ex
Main-Router(config)#

```

Рисунок 3.10 – Базове налаштування маршрутизатора Main-Router

```

Branch1Router
Physical Config CLI Attributes
IOS Command Line Interface

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Branch1Router
Branch1Router(config)#interface GigabitEthernet0/0
Branch1Router(config-if)#ip address 80.10.1.2 255.255.255.252
Branch1Router(config-if)#no sh

Branch1Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Branch1Router(config-if)#ex
Branch1Router(config)#interface GigabitEthernet0/1.10
Branch1Router(config-subif)# encapsulation dot1Q 10
Branch1Router(config-subif)# ip address 110.10.2.1 255.255.255.0
Branch1Router(config-subif)#ex
Branch1Router(config)#interface GigabitEthernet0/1.20
Branch1Router(config-subif)# encapsulation dot1Q 20
Branch1Router(config-subif)# ip address 120.10.2.1 255.255.255.0
Branch1Router(config-subif)#ex
Branch1Router(config)#interface GigabitEthernet0/1
Branch1Router(config-if)#no sh

Branch1Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.10, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.20, changed state to up

Branch1Router(config-if)#ex
Branch1Router(config)#

```

Рисунок 3.11 – Базове налаштування маршрутизатора Branch1Router

Наступним етапом потрібно налаштувати комутатори мережі для забезпечення роботи VLAN. Спочатку буде показано конфігурацію магістрального комутатора, підключеного до внутрішнього маршрутизатора. Він передає трафік між VLAN через транкові канали та підтримує VLAN 10, 20 і 50. Налаштування включає створення транкових портів для зв'язку з іншими комутаторами. Далі налаштуємо комутатор рівня доступу, який підключається до кінцевих пристроїв і розподіляє порти між VLAN. Це забезпечить коректну сегментацію мережі для кінцевих станцій.

MainSwitch

Physical
Config
CLI
Attributes

IOS Command Line Interface

```

MainSwitch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MainSwitch(config)#int vlan 10
MainSwitch(config-if)#
*Mar 01, 00:00:58.000: %LINK-5-CHANGED: Interface Vlan10, changed state to up
*Mar 01, 00:00:58.000: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
MainSwitch(config-if)# ip address 110.10.1.2 255.255.255.0
MainSwitch(config-if)#no sh
MainSwitch(config-if)#ex
MainSwitch(config)#int vlan 20
MainSwitch(config-if)#
*Mar 01, 00:01:25.011: %LINK-5-CHANGED: Interface Vlan20, changed state to up
*Mar 01, 00:01:25.011: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
MainSwitch(config-if)# ip address 120.10.1.2 255.255.255.0
MainSwitch(config-if)#no sh
MainSwitch(config-if)#ex
MainSwitch(config)#int vlan 50
MainSwitch(config-if)#
*Mar 01, 00:01:35.011: %LINK-5-CHANGED: Interface Vlan50, changed state to up
*Mar 01, 00:01:35.011: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to up
MainSwitch(config-if)# ip address 150.10.1.2 255.255.255.0
MainSwitch(config-if)#no sh
MainSwitch(config-if)#ex
MainSwitch(config)#vlan 10
MainSwitch(config-vlan)#name Main1
MainSwitch(config-vlan)#ex
MainSwitch(config)#vlan 20
MainSwitch(config-vlan)#name Main 2
MainSwitch(config-vlan)#
% Invalid input detected at '^' marker.

MainSwitch(config-vlan)#name Main2
MainSwitch(config-vlan)#ex
MainSwitch(config)#vlan 50
MainSwitch(config-vlan)#name DMZ
MainSwitch(config-vlan)#ex
MainSwitch(config)#int range fa0/1-3
MainSwitch(config-if-range)#sw mode trunk

MainSwitch(config-if-range)#
*Mar 01, 00:03:40.033: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Mar 01, 00:03:40.033: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
*Mar 01, 00:03:40.033: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
*Mar 01, 00:03:40.033: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
MainSwitch(config-if-range)#ex
MainSwitch(config)#int gig0/1
MainSwitch(config-if)#sw mode trunk

MainSwitch(config-if)#
*Mar 01, 00:04:11.044: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
*Mar 01, 00:04:11.044: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
MainSwitch(config-if)#ex
MainSwitch(config)#

```

Рисунок 3.12 – Базове налаштування комутатора MainSwitch

```

Branch1Switch
Physical Config CLI Attributes
IOS Command Line Interface

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Branch1Switch
Branch1Switch(config)#vlan 10
Branch1Switch(config-vlan)#name Branch1-vlan10
Branch1Switch(config-vlan)#ex
Branch1Switch(config)#vlan 20
Branch1Switch(config-vlan)#name Branch1-vlan20
Branch1Switch(config-vlan)#ex
Branch1Switch(config)#int vlan 10
Branch1Switch(config-if)#
*Mar 01, 00:01:05.011: %LINK-5-CHANGED: Interface Vlan10, changed state to up
Branch1Switch(config-if)#ip address 110.10.2.2 255.255.255.0
Branch1Switch(config-if)#no sh
Branch1Switch(config-if)#ex
Branch1Switch(config)#int vlan 20
Branch1Switch(config-if)#
*Mar 01, 00:01:20.011: %LINK-5-CHANGED: Interface Vlan20, changed state to up
Branch1Switch(config-if)#ip address 120.10.2.2 255.255.255.0
Branch1Switch(config-if)#no sh
Branch1Switch(config-if)#ex
Branch1Switch(config)#int gig0/1
Branch1Switch(config-if)#sw mode trunk

Branch1Switch(config-if)#
*Mar 01, 00:01:53.011: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to down
*Mar 01, 00:01:53.011: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
*Mar 01, 00:01:53.011: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed
state to up
*Mar 01, 00:01:53.011: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed
state to up
Branch1Switch(config-if)#ex
Branch1Switch(config)#int range fa0/1, fa0/4
Branch1Switch(config-if-range)#switchport access vlan 10
Branch1Switch(config-if-range)#switchport mode access
Branch1Switch(config-if-range)#no sh
Branch1Switch(config-if-range)#ex
Branch1Switch(config)#int range fa0/2, fa0/5
Branch1Switch(config-if-range)#switchport access vlan 20
Branch1Switch(config-if-range)#switchport mode access
Branch1Switch(config-if-range)#no sh
Branch1Switch(config-if-range)#ex
Branch1Switch(config)#

```

Рисунок 3.13 – Базове налаштування комутатора Branch1Switch

Після налаштування комутаторів переходимо до конфігурації точки доступу, яка забезпечує бездротове з'єднання для клієнтів мережі. На цьому етапі присвоюємо SSID для ідентифікації мережі та налаштовуємо параметри безпеки, зокрема аутентифікацію з використанням WPA2-PSK для захисту переданих даних. У процесі налаштування задаємо пароль, який відповідатиме політиці безпеки мережі, забезпечуючи захист від несанкціонованого доступу.

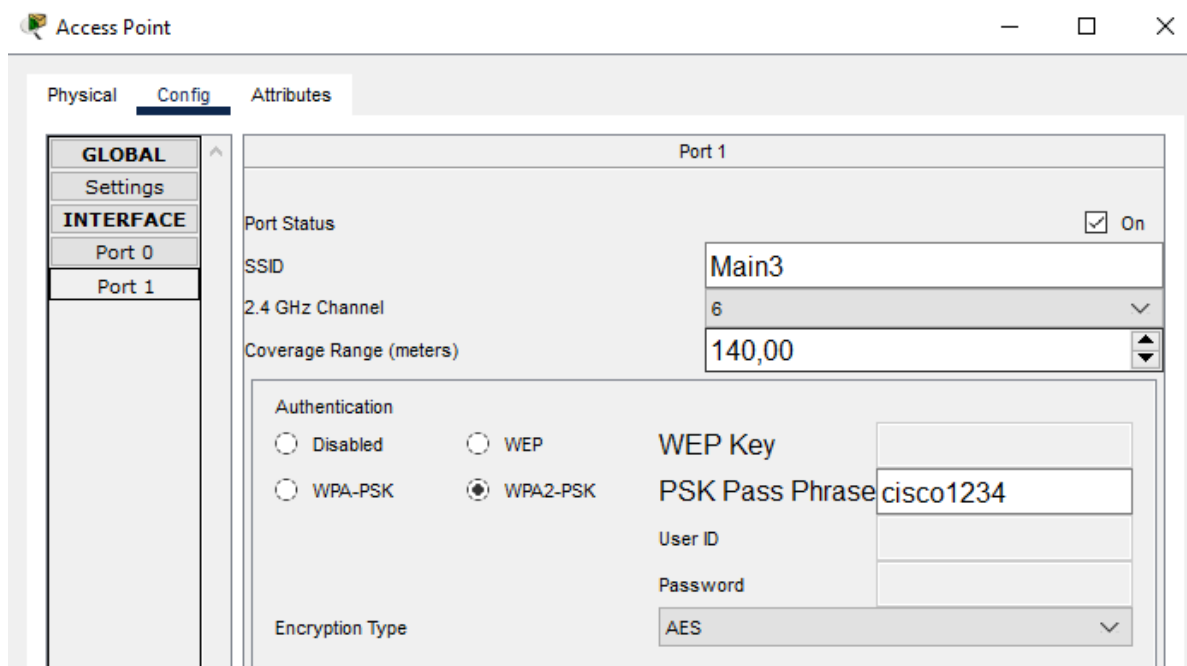


Рисунок 3.14 – Налаштування точки доступу Access Point

Встановлюємо потрібний адаптер на комп'ютері та вводимо пароль і SSID для отримання підключення до точки доступу:

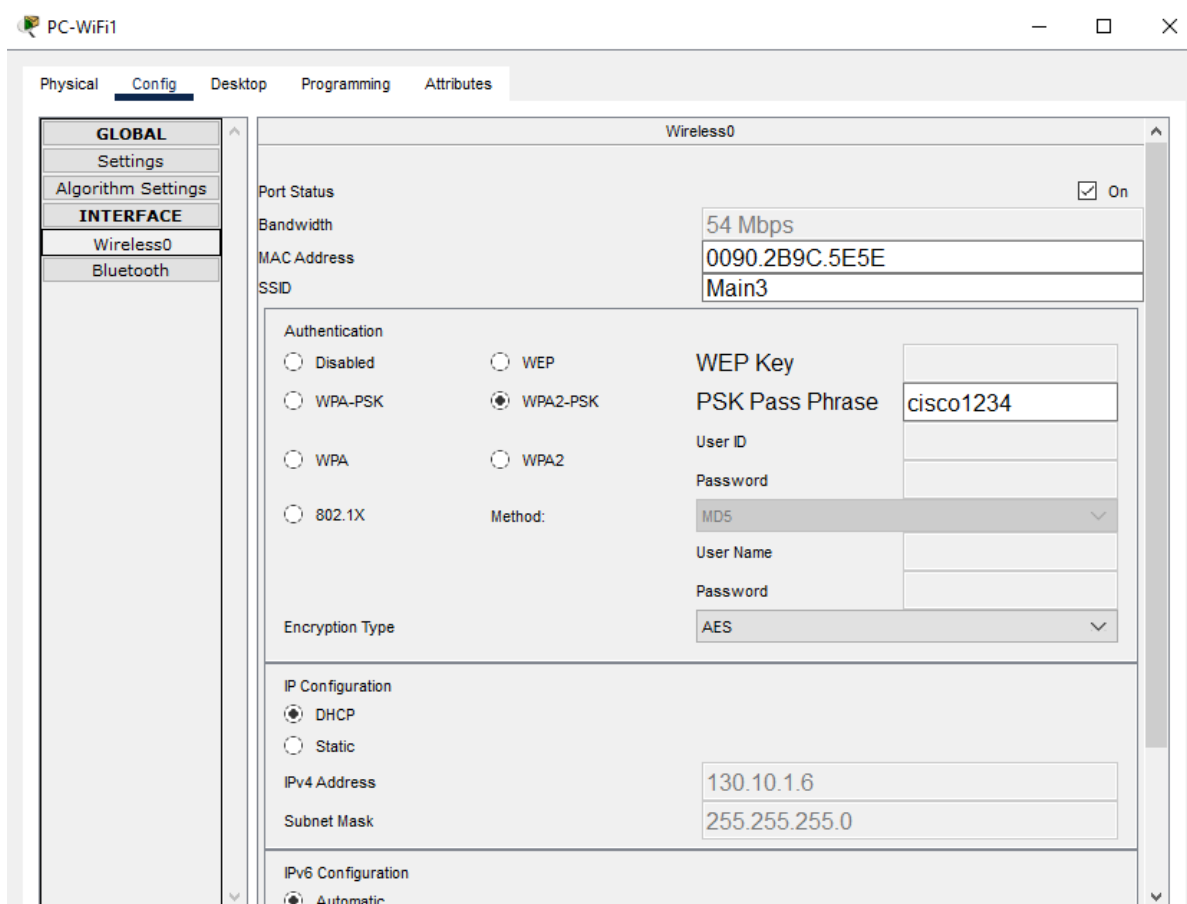


Рисунок 3.15 – Підключення комп'ютера мережі до точки доступу

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

Після завершення основних налаштувань перевіряємо, чи отримують станції свої IP-адреси автоматично через протокол DHCP як у головному офісі, так і в домашній мережі:

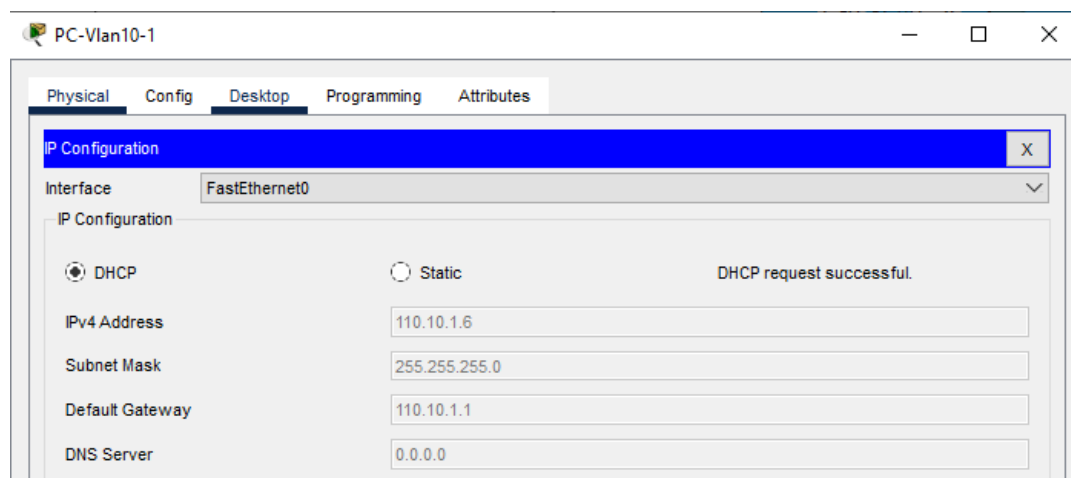


Рисунок 3.16 – Успішне отримання адреси на робочій станції PC-Vlan10-1

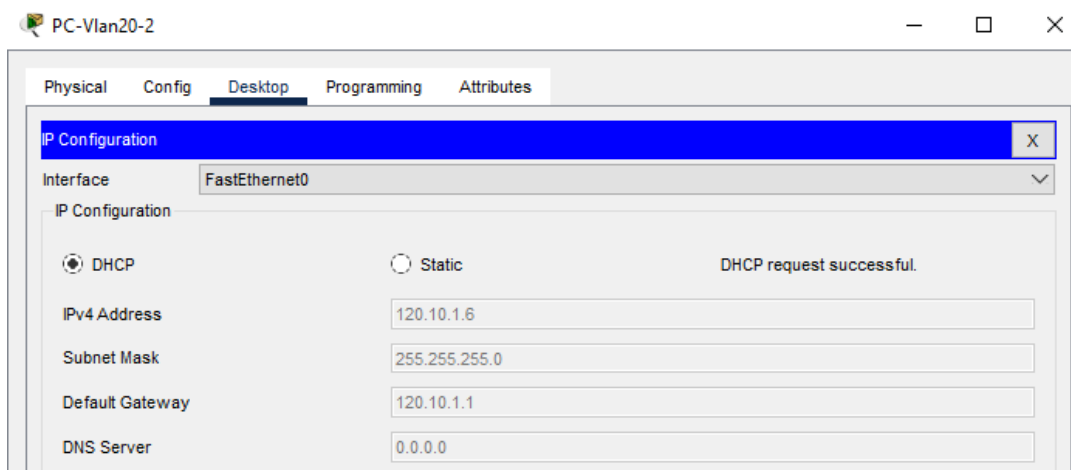


Рисунок 3.17 – Успішне отримання адреси на робочій станції PC-Vlan20-2

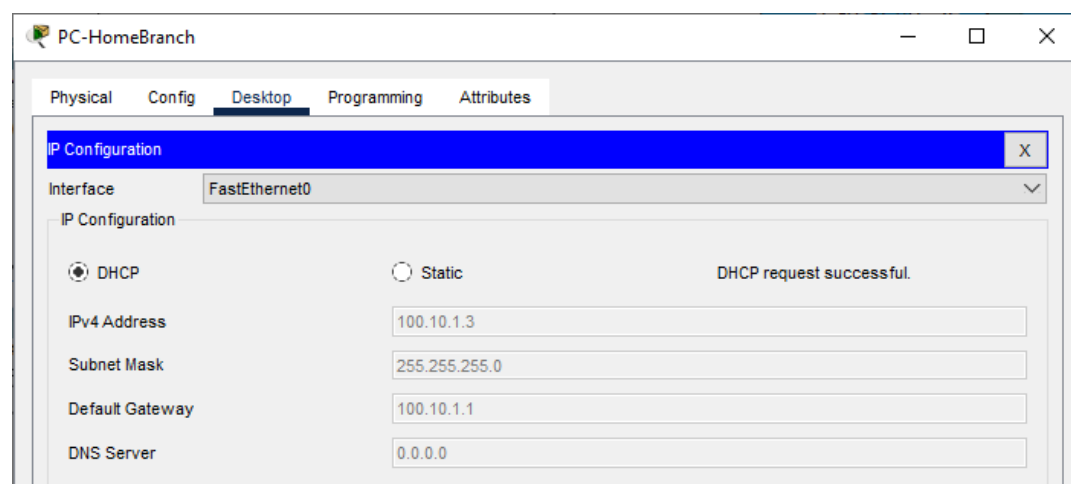


Рисунок 3.18 – Успішне отримання адреси на робочій станції PC-HomeBranch

Деякі станції отримали адреси автоматично, але сервери та комп'ютери віддалених філій потрібно налагодити вручну:

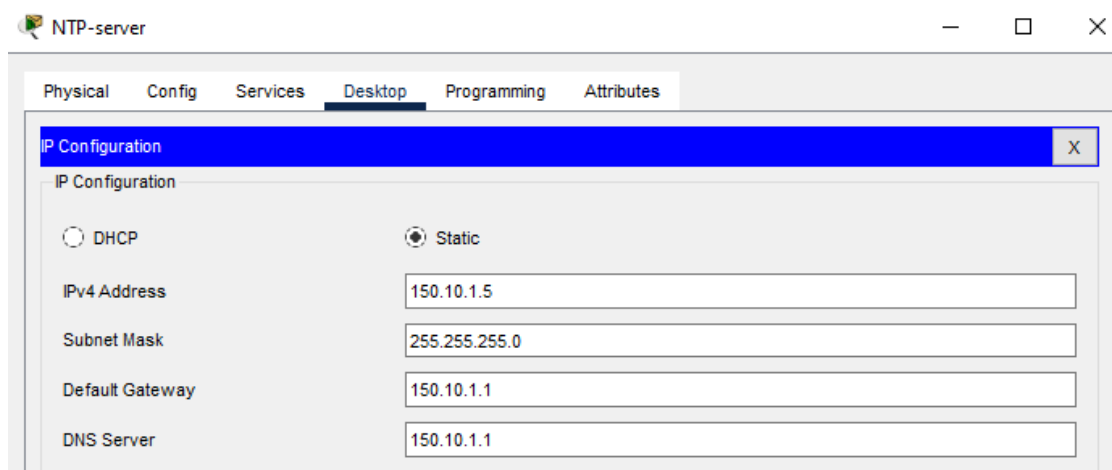


Рисунок 3.19 – Налаштування адресації на сервері NTP-server

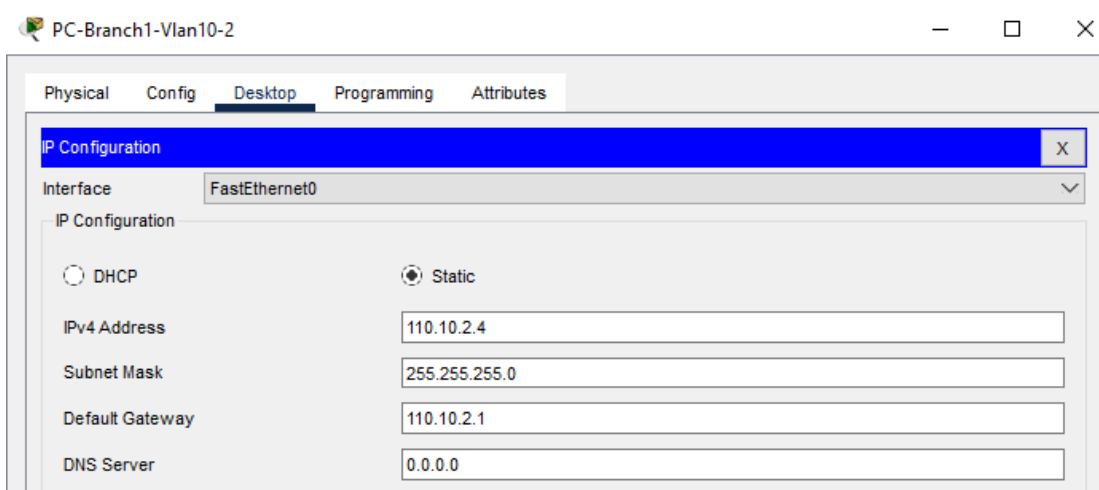


Рисунок 3.20 – Налаштування адресації на робочій станції PC-Branch1-Vlan10-2

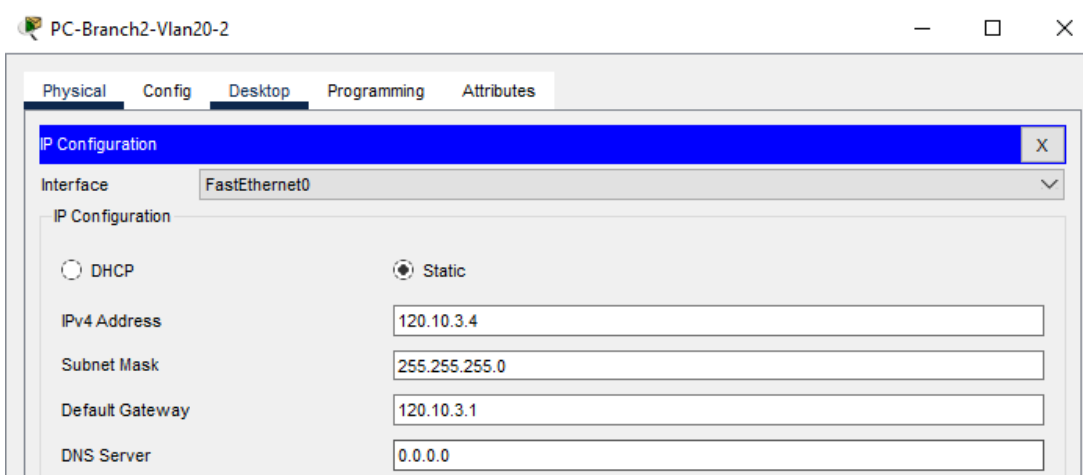


Рисунок 3.21 – Налаштування адресації на робочій станції PC-Branch2-Vlan20-2

Тепер переходимо до налаштування маршрутизації між пристроями мережі, що дозволить забезпечити передачу даних між різними підмережами та VLAN. Для цього буде використовуватися протокол маршрутизації EIGRP, який дозволяє ефективно обмінювати інформацію про маршрути між маршрутизаторами в мережі. Це налаштування є ключовим для створення взаємодії між внутрішніми сегментами мережі, а також для організації зв'язку з віддаленими офісами через захищені канали VPN. Використання EIGRP забезпечить швидке та надійне встановлення маршрутів, а також ефективне реагування на зміни в мережевій топології.

```

MainRouter
Physical Config CLI Attributes
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
MainRouter(config)#router eigrp 1
MainRouter(config-router)#network 20.10.1.0 0.0.0.3
MainRouter(config-router)# network 40.10.1.0 0.0.0.3
*Mar 01, 00:01:52.011: %DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 20.10.1.1
(FastEthernet0/0) is up: new adjacency
MainRouter(config-router)#
*Mar 01, 00:01:54.011: %DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 40.10.1.2
(FastEthernet0/1) is up: new adjacency
MainRouter(config-router)#ex
  
```

Рисунок 3.22 – Приклад налаштування маршрутизації на маршрутизаторі MainRouter

```

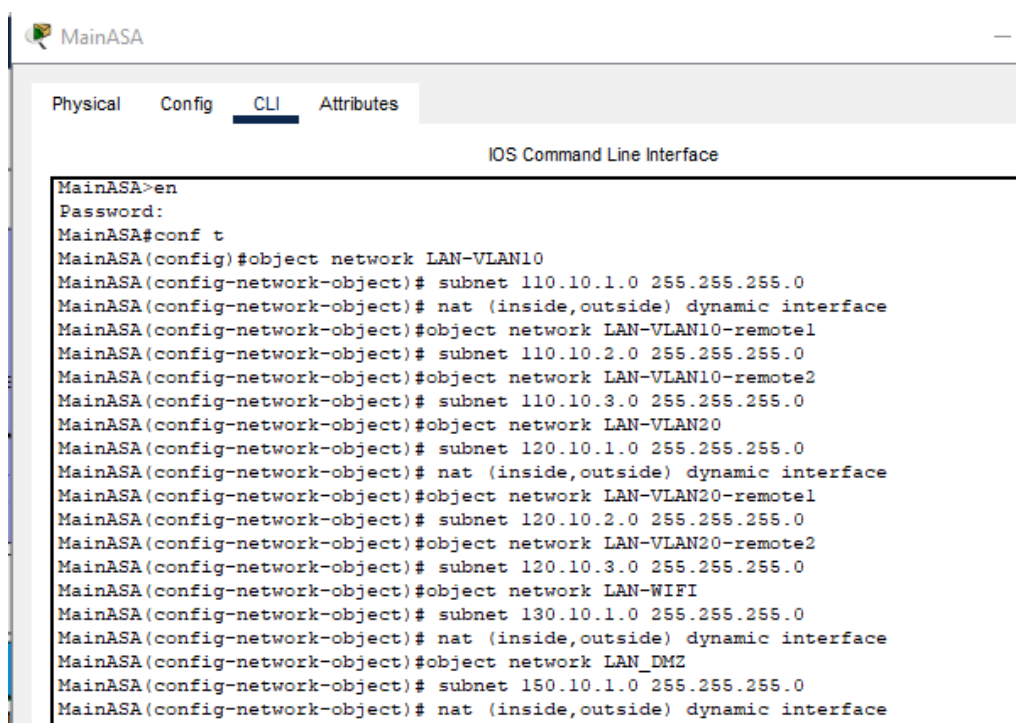
Branch2-ASA>
Branch2-ASA>en
Password:
Branch2-ASA#conf t
Branch2-ASA(config)#router eigrp 1
Branch2-ASA(config-router)# eigrp router-id 3.3.3.3
Branch2-ASA(config-router)# network 60.10.1.0 0.0.0.3
Branch2-ASA(config-router)# network 90.10.1.0 0.0.0.3
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 60.10.1.1 (GigabitEthernet1/1) is up: new
adjacency

Branch2-ASA(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 90.10.1.2 (GigabitEthernet1/2) is up: new
adjacency
Branch2-ASA(config-router)#
  
```

Рисунок 3.23 – Приклад налаштування маршрутизації на брандмауері Branch2-ASA

Після базових налагоджень ми можемо перейти вже до самого налаштування захищеного трафіку. Для цього прикладу будемо використовувати пару брандмауерів MainASA – Branch1-ASA та MainASA – Branch2-ASA . Налаштуємо списки доступу, тунель VPN та іншу конфігурацію для захисту мережі.

Першим кроком створимо об'єкт мережі [21] для зони inside, який буде використовуватись для подальшої конфігурації та налаштувань. Об'єкти мережі в Cisco ASA дозволяють групувати IP-адреси, що належать до однієї зони, в єдину структуру, спрощуючи управління та налаштування доступу до ресурсів. Це дає змогу легко створювати правила доступу (ACL), маршрути та інші конфігурації, де замість конкретних IP-адрес можна використовувати цей об'єкт.



```

MainASA
Physical Config CLI Attributes
IOS Command Line Interface
MainASA>en
Password:
MainASA#conf t
MainASA(config)#object network LAN-VLAN10
MainASA(config-network-object)# subnet 110.10.1.0 255.255.255.0
MainASA(config-network-object)# nat (inside,outside) dynamic interface
MainASA(config-network-object)#object network LAN-VLAN10-remotel
MainASA(config-network-object)# subnet 110.10.2.0 255.255.255.0
MainASA(config-network-object)#object network LAN-VLAN10-remote2
MainASA(config-network-object)# subnet 110.10.3.0 255.255.255.0
MainASA(config-network-object)#object network LAN-VLAN20
MainASA(config-network-object)# subnet 120.10.1.0 255.255.255.0
MainASA(config-network-object)# nat (inside,outside) dynamic interface
MainASA(config-network-object)#object network LAN-VLAN20-remotel
MainASA(config-network-object)# subnet 120.10.2.0 255.255.255.0
MainASA(config-network-object)#object network LAN-VLAN20-remote2
MainASA(config-network-object)# subnet 120.10.3.0 255.255.255.0
MainASA(config-network-object)#object network LAN-WIFI
MainASA(config-network-object)# subnet 130.10.1.0 255.255.255.0
MainASA(config-network-object)# nat (inside,outside) dynamic interface
MainASA(config-network-object)#object network LAN_DMZ
MainASA(config-network-object)# subnet 150.10.1.0 255.255.255.0
MainASA(config-network-object)# nat (inside,outside) dynamic interface

```

Рисунок 3.24 – Створення об'єктів мережі на брандмауері MainASA

```

Branch1-ASA>en
Password:
Branch1-ASA#conf t
Branch1-ASA(config)#object network LAN-VLAN10
Branch1-ASA(config-network-object)# subnet 110.10.2.0 255.255.255.0
Branch1-ASA(config-network-object)# nat (inside,outside) dynamic interface
Branch1-ASA(config-network-object)#object network LAN-VLAN10-remotel
Branch1-ASA(config-network-object)# subnet 110.10.1.0 255.255.255.0
Branch1-ASA(config-network-object)#object network LAN-VLAN10-remote2
Branch1-ASA(config-network-object)# subnet 110.10.3.0 255.255.255.0
Branch1-ASA(config-network-object)#object network LAN-VLAN20
Branch1-ASA(config-network-object)# subnet 120.10.2.0 255.255.255.0
Branch1-ASA(config-network-object)# nat (inside,outside) dynamic interface
Branch1-ASA(config-network-object)#object network LAN-VLAN20-remotel
Branch1-ASA(config-network-object)# subnet 120.10.1.0 255.255.255.0
Branch1-ASA(config-network-object)#object network LAN-VLAN20-remote2
Branch1-ASA(config-network-object)# subnet 120.10.3.0 255.255.255.0
Branch1-ASA(config-network-object)#object network LAN_DMZ
Branch1-ASA(config-network-object)# subnet 150.10.1.0 255.255.255.0

```

Рисунок 3.25 – Створення об’єктів мережі на брандмауері Branch1-ASA

Також налаштуємо маршрут за замовчуванням для вихідного інтерфейсу outside. Це забезпечить автоматичне перенаправлення всього неопізаного трафіку через вказаний шлюз за замовчуванням. Така конфігурація дозволяє маршрутизатору або брандмауеру передавати пакети, призначення яких не відповідає жодному з існуючих маршрутів у таблиці маршрутизації..

```

MainASA#conf t
MainASA(config)#route outside 0.0.0.0 0.0.0.0 40.10.1.1 1
MainASA(config)#

```

Рисунок 3.26 – Приклад налаштування маршруту за замовчуванням на брандмауері MainASA

Далі спробуємо налагодити списки контролю доступу з використанням вже створених об’єктів мережі.

```

MainASA
Physical Config CLI Attributes
IOS Command Line Interface
MainASA#conf t
MainASA(config)#access-list RES extended permit ip object LAN-VLAN10 any
MainASA(config)#access-list RES extended permit ip object LAN-VLAN20 any
MainASA(config)#access-list RES extended permit ip object LAN-WIFI any
MainASA(config)#access-list RES extended permit ip object LAN_DMZ any
MainASA(config)#access-list RES extended permit icmp object LAN-WIFI 100.10.1.0
255.255.255.0
MainASA(config)#access-list ENTRADA extended permit icmp object LAN-VLAN10-remote1 object
LAN-VLAN10
MainASA(config)#access-list ENTRADA extended permit icmp object LAN-VLAN10-remote2 object
LAN-VLAN10
MainASA(config)#access-list ENTRADA extended permit icmp object LAN-VLAN20-remote1 object
LAN-VLAN20
MainASA(config)#access-list ENTRADA extended permit icmp object LAN-VLAN20-remote2 object
LAN-VLAN20
MainASA(config)#access-list ENTRADA extended permit icmp 100.10.1.0 255.255.255.0 object
LAN-WIFI
MainASA(config)#access-list ENTRADA extended permit ip any object LAN_DMZ
MainASA(config)#access-list ENTRADA extended deny ip any any
MainASA(config)#access-group RES out interface inside
MainASA(config)#access-group ENTRADA in interface outside
MainASA(config)#

```

Рисунок 3.27 – Налаштування списків контролю доступу на брандмауері MainASA

```

Branch1-ASA
Physical Config CLI Attributes
IOS Command Line Interface
Branch1-ASA#conf t
Branch1-ASA(config)#access-list RES extended permit ip object LAN-VLAN10 any
Branch1-ASA(config)#access-list RES extended permit ip object LAN-VLAN20 any
Branch1-ASA(config)#access-list ENTRADA extended permit icmp object LAN-VLAN10-remote1
object LAN-VLAN10
Branch1-ASA(config)#access-list ENTRADA extended permit icmp object LAN-VLAN10-remote2
object LAN-VLAN10
Branch1-ASA(config)#access-list ENTRADA extended permit icmp object LAN-VLAN20-remote1
object LAN-VLAN20
Branch1-ASA(config)#access-list ENTRADA extended permit icmp object LAN-VLAN20-remote2
object LAN-VLAN20
Branch1-ASA(config)#access-list ENTRADA extended permit ip object LAN_DMZ any
Branch1-ASA(config)#access-list ENTRADA extended deny ip any any
Branch1-ASA(config)#access-group RES out interface inside
Branch1-ASA(config)#access-group ENTRADA in interface outside
Branch1-ASA(config)#

```

Рисунок 3.28 – Налаштування списків контролю доступу на брандмауері Branch1-ASA

Завершальним етапом налаштування фаєрвола є створення VPN-з'єднання. Першим кроком у налаштуванні тунелів VPN є створення списків контролю доступу, які будуть використовуватись для визначення дозволених або заборонених маршрутів трафіку через тунель.

```

MainASA
Physical Config CLI Attributes
IOS Command Line Interface
MainASA#conf t
MainASA(config)#access-list TRAFEGO-VPN1 extended permit ip 110.10.1.0 255.255.255.0
110.10.2.0 255.255.255.0
MainASA(config)#access-list TRAFEGO-VPN1 extended permit ip 120.10.1.0 255.255.255.0
120.10.2.0 255.255.255.0
MainASA(config)#access-list TRAFEGO-VPN1 extended permit ip 150.10.1.0 255.255.255.0
110.10.2.0 255.255.255.0
MainASA(config)#access-list TRAFEGO-VPN1 extended permit ip 150.10.1.0 255.255.255.0
120.10.2.0 255.255.255.0
MainASA(config)#access-list TRAFEGO-VPN2 extended permit ip 110.10.1.0 255.255.255.0
110.10.3.0 255.255.255.0
MainASA(config)#access-list TRAFEGO-VPN2 extended permit ip 120.10.1.0 255.255.255.0
120.10.3.0 255.255.255.0
MainASA(config)#access-list TRAFEGO-VPN2 extended permit ip 150.10.1.0 255.255.255.0
110.10.3.0 255.255.255.0
MainASA(config)#access-list TRAFEGO-VPN2 extended permit ip 150.10.1.0 255.255.255.0
120.10.3.0 255.255.255.0
MainASA(config)#

```

Рисунок 3.29 – Налаштування списків контролю доступу для VPN на бранд-мауері MainASA

```

Branch2-ASA
Physical Config CLI Attributes
IOS Command Line Interface
Branch2-ASA#conf t
Branch2-ASA(config)#access-list TRAFEGO-VPN1 extended permit ip 110.10.3.0 255.255.255.0
110.10.1.0 255.255.255.0
Branch2-ASA(config)#access-list TRAFEGO-VPN1 extended permit ip 120.10.3.0 255.255.255.0
120.10.1.0 255.255.255.0
Branch2-ASA(config)#access-list TRAFEGO-VPN1 extended permit ip 110.10.3.0 255.255.255.0
150.10.1.0 255.255.255.0
Branch2-ASA(config)#access-list TRAFEGO-VPN1 extended permit ip 120.10.3.0 255.255.255.0
150.10.1.0 255.255.255.0
Branch2-ASA(config)#access-list TRAFEGO-VPN2 extended permit ip 110.10.3.0 255.255.255.0
110.10.2.0 255.255.255.0
Branch2-ASA(config)#access-list TRAFEGO-VPN2 extended permit ip 120.10.3.0 255.255.255.0
120.10.2.0 255.255.255.0
Branch2-ASA(config)#

```

Рисунок 3.30 – Налаштування списків контролю доступу для VPN на бранд-мауері Branch2-ASA

Після створення ACL переходимо до налаштування VPN-з'єднання. Спочатку налаштовуємо трансформаційні набори, визначаючи алгоритми шифрування, такі як AES, і методи аутентифікації, наприклад, HMAC SHA. Це забезпечує шифрування та захист даних, що передаються через тунель. Далі створюємо крипто-мапи, які поєднують параметри шифрування з правилами для визначення трафіку, який проходить через VPN. Крипто-мапи зв'язуються з інтерфейсами маршрутизаторів або

брандмауерів для фільтрації та шифрування трафіку. Наступним кроком є налаштування параметрів безпеки для IKEv1 для безпечного обміну ключами і встановлення тунелю, вибираючи алгоритми шифрування та методи аутентифікації, наприклад, попередньо визначені ключі або сертифікати. Завершуємо налаштування створенням тунельної групи, де визначаємо методи автентифікації користувачів та IP-адреси для VPN-з'єднання.

```

MainASA
Physical Config CLI Attributes
IOS Command Line Interface
MainASA(config)#crypto ipsec ikev1 transform-set IPSEC esp-aes esp-sha-hmac
MainASA(config)#crypto map VPN 1 match address TRAFEGO-VPN1
MainASA(config)#crypto map VPN 1 set peer 50.10.1.2
MainASA(config)#crypto map VPN 1 set ikev1 transform-set IPSEC
MainASA(config)#crypto map VPN interface outside
WARNING: crypto map has incomplete entries
MainASA(config)#crypto map VPN 2 match address TRAFEGO-VPN2
MainASA(config)#crypto map VPN 2 set peer 60.10.1.2
MainASA(config)#crypto map VPN 2 set ikev1 transform-set IPSEC
MainASA(config)#crypto map VPN interface outside
WARNING: crypto map has incomplete entries
MainASA(config)#crypto ikev1 enable outside
MainASA(config)#crypto ikev1 policy 1
MainASA(config-ikev1-policy)#encr aes
MainASA(config-ikev1-policy)# authentication pre-share
MainASA(config-ikev1-policy)# group 5
MainASA(config-ikev1-policy)#ex
MainASA(config)#crypto ikev1 policy 2
MainASA(config-ikev1-policy)# encr aes
MainASA(config-ikev1-policy)# authentication pre-share
MainASA(config-ikev1-policy)# group 5
MainASA(config-ikev1-policy)#ex
MainASA(config)#tunnel-group 50.10.1.2 type ipsec-l2l
WARNING: L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode
MainASA(config)#tunnel-group 50.10.1.2 ipsec-attributes
MainASA(config-tunnel-ipsec)#ikev1 pre-shared-key SENHA
MainASA(config-tunnel-ipsec)#ex
MainASA(config)#tunnel-group 60.10.1.2 type ipsec-l2l
WARNING: L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode
MainASA(config)#tunnel-group 60.10.1.2 ipsec-attributes
MainASA(config-tunnel-ipsec)# ikev1 pre-shared-key SENHA
MainASA(config-tunnel-ipsec)#ex
MainASA(config)#

```

Рисунок 3.31 – Налаштування першої пари VPN-тунелів на брандмауері MainASA

```

Branch2-ASA#conf t
Branch2-ASA(config)#crypto ipsec ikev1 transform-set IPSEC esp-aes esp-sha-hmac
Branch2-ASA(config)#crypto map VPN 1 match address TRAFEGO-VPN1
Branch2-ASA(config)#crypto map VPN 1 set peer 40.10.1.2
Branch2-ASA(config)#crypto map VPN 1 set ikev1 transform-set IPSEC
Branch2-ASA(config)#crypto map VPN interface outside
WARNING: crypto map has incomplete entries
Branch2-ASA(config)#crypto map VPN 2 match address TRAFEGO-VPN2
Branch2-ASA(config)#crypto map VPN 2 set peer 50.10.1.2
Branch2-ASA(config)#crypto map VPN 2 set ikev1 transform-set IPSEC
Branch2-ASA(config)#crypto map VPN interface outside
WARNING: crypto map has incomplete entries
Branch2-ASA(config)#crypto ikev1 enable outside
Branch2-ASA(config)#crypto ikev1 policy 1
Branch2-ASA(config-ikev1-policy)# encr aes
Branch2-ASA(config-ikev1-policy)# authentication pre-share
Branch2-ASA(config-ikev1-policy)# group 5
Branch2-ASA(config-ikev1-policy)#ex
Branch2-ASA(config)#tunnel-group 40.10.1.2 type ipsec-l2l
WARNING: L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode
Branch2-ASA(config)#tunnel-group 40.10.1.2 ipsec-attributes
Branch2-ASA(config-tunnel-ipsec)# ikev1 pre-shared-key SENHA
Branch2-ASA(config-tunnel-ipsec)#tunnel-group 50.10.1.2 type ipsec-l2l
WARNING: L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode
Branch2-ASA(config)#tunnel-group 50.10.1.2 ipsec-attributes
Branch2-ASA(config-tunnel-ipsec)# ikev1 pre-shared-key SENHA
Branch2-ASA(config-tunnel-ipsec)#ex
Branch2-ASA(config)#

```

Рисунок 3.32 – Налаштування другої пари VPN-тунелів на брандмауері Branch2-ASA

Також доцільно налаштувати VPN-тунель [22] між домашнім роутером та головним маршрутизатором основного офісу для забезпечення захищеного з'єднання між робочими станціями. Це дозволить створити додатковий рівень безпеки для віддалених користувачів, які підключаються до корпоративної мережі через публічні мережі, такі як Інтернет. Налаштування VPN-тунелю гарантує, що дані будуть шифровані, а доступ до внутрішніх ресурсів компанії здійснюватиметься через надійний та захищений канал, що значно знижує ризики несанкціонованого доступу та витоку інформації.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

```

MainRouter
Physical Config CLI Attributes
IOS Command Line Interface
*Nov 20, 05:29:40.2929: SYS-5-CONFIG_I: Configured from console by console
MainRouter#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MainRouter(config)#access-list 100 permit ip 130.10.1.0 0.0.0.255 100.10.1.0 0.0.0.255
MainRouter(config)#crypto isakmp policy 10
MainRouter(config-isakmp)#encr aes 256
MainRouter(config-isakmp)#authentication pre-share
MainRouter(config-isakmp)#group 5
MainRouter(config-isakmp)#ex
MainRouter(config)#crypto isakmp key markkey address 10.10.1.2
MainRouter(config)#crypto ipsec transform-set main-home esp-aes 256 esp-sha-hmac
MainRouter(config)#crypto map VPN-MAP 10 ipsec-isakmp
MainRouter(config-crypto-map)#set peer 10.10.1.2
MainRouter(config-crypto-map)#set pfs group5
MainRouter(config-crypto-map)#set security-association lifetime seconds 86400
MainRouter(config-crypto-map)#set transform-set main-home
MainRouter(config-crypto-map)#match address 100
MainRouter(config-crypto-map)#ex
MainRouter(config)#interface FastEthernet0/0
MainRouter(config-if)#crypto map VPN-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
MainRouter(config-if)#
MainRouter(config-if)#ex

```

Рисунок 3.33 – Налаштування пари IPsec Site-to-Site VPN на першому маршрутизаторі MainRouter

```

HomeRouter
Physical Config CLI Attributes
IOS Command Line Interface
*Nov 20, 05:33:10.3333: SYS-5-CONFIG_I: Configured from console by console
HomeRouter#
HomeRouter#conf t
Enter configuration commands, one per line. End with CNTL/Z.
HomeRouter(config)#access-list 100 permit ip 100.10.1.0 0.0.0.255 130.10.1.0 0.0.0.255
HomeRouter(config)#crypto isakmp policy 10
HomeRouter(config-isakmp)#encr aes 256
HomeRouter(config-isakmp)#authentication pre-share
HomeRouter(config-isakmp)#group 5
HomeRouter(config-isakmp)#
HomeRouter(config-isakmp)#ex
HomeRouter(config)#crypto isakmp key markkey address 20.10.1.2
HomeRouter(config)#crypto ipsec transform-set home-main esp-aes 256 esp-sha-hmac
HomeRouter(config)#crypto map VPN-MAP 10 ipsec-isakmp
HomeRouter(config-crypto-map)#set peer 20.10.1.2
HomeRouter(config-crypto-map)#set pfs group5
HomeRouter(config-crypto-map)#set security-association lifetime seconds 86400
HomeRouter(config-crypto-map)#set transform-set home-main
HomeRouter(config-crypto-map)#match address 100
HomeRouter(config-crypto-map)#ex
HomeRouter(config)#interface FastEthernet0/0
HomeRouter(config-if)#crypto map VPN-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
HomeRouter(config-if)#ex
HomeRouter(config)#

```

Рисунок 3.34 – Налаштування пари IPsec Site-to-Site VPN на другому маршрутизаторі HomeRouter

Далі необхідно налаштувати роботу серверів між пристроями мережі. Першим кроком буде налаштування NTP-сервера для синхронізації часу на всіх пристроях

мережі. Це важливий етап, оскільки правильна синхронізація часу дозволяє зберігати узгодженість в реєстрації подій на всіх мережевих пристроях, включаючи маршрутизатори, брандмауери та сервери. Без налаштування NTP пристрої можуть працювати з різними часами, що ускладнює адміністрування, а також може призвести до помилок в логах, проблем з сертифікатами та іншими аспектами безпеки.

Для цього налаштовуємо NTP-сервер, визначаючи основний сервер часу, до якого всі пристрої в мережі будуть синхронізувати свої годинники. Після цього на кожному мережевому пристрої (маршрутизаторі, брандмауері тощо) налаштовуємо підключення до цього сервера для отримання точного часу.

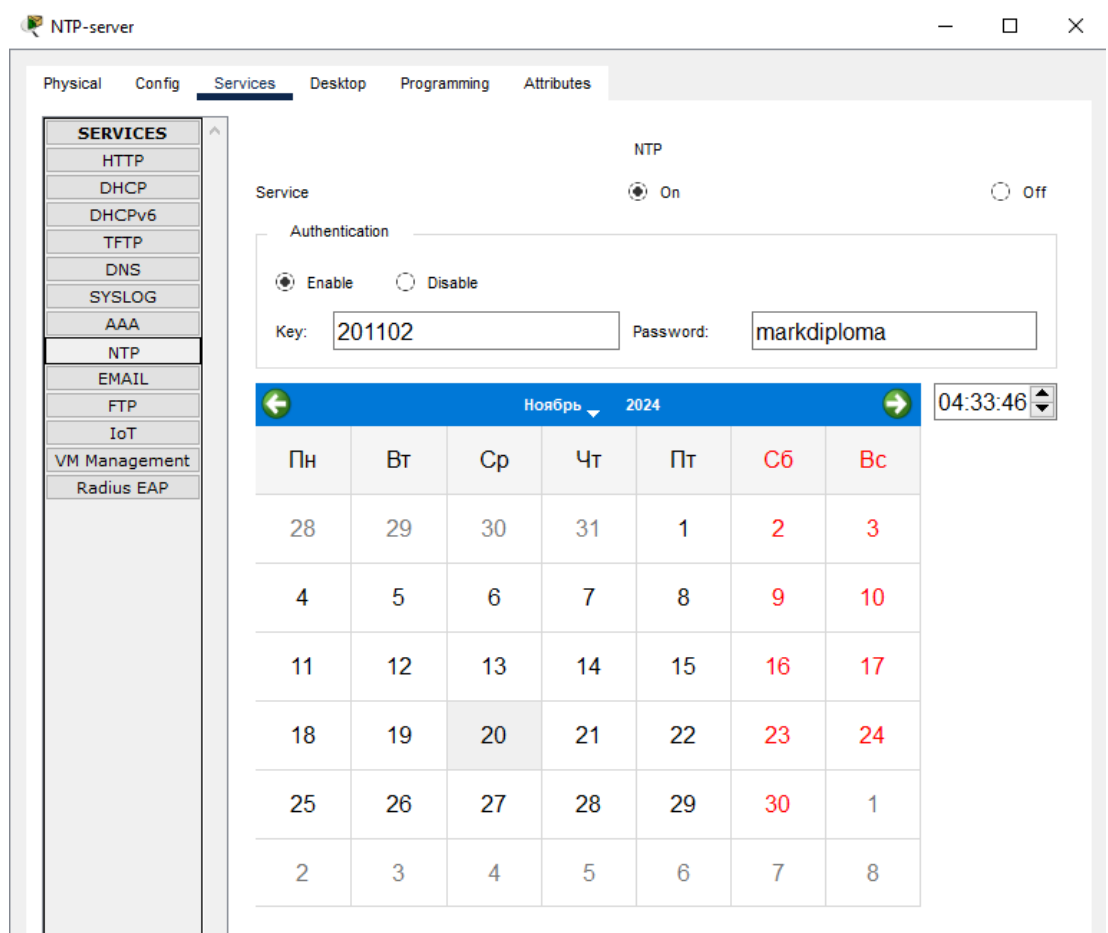


Рисунок 3.35 – Налаштування ключа та пароля на NTP-сервері

Включаємо сервіс NTP на сервері та налаштовуємо ключ і пароль. Далі за допомогою цих даних налаштовуємо синхронізацію на наших пристроях:

```

Branch2Router
Physical Config CLI Attributes
IOS Command Line Interface
Branch2Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Branch2Router(config)#service times log datetime msec
Branch2Router(config)#service times debug datetime msec
Branch2Router(config)#clock timezone GMT 2
Branch2Router(config)#ntp authentication-key 201102 md markdiploma
Branch2Router(config)#ntp trusted 201102
Branch2Router(config)#ntp server 150.10.1.5 key 201102
Branch2Router(config)#ex
Branch2Router#
*Nov 20, 04:33:58.3333: SYS-5-CONFIG_I: Configured from console by console
Branch2Router#

```

Рисунок 3.36 – Приклад налаштування синхронізації часу на маршрутизаторі Branch2Router

```

Branch1-ASA
Physical Config CLI Attributes
IOS Command Line Interface
Branch1-ASA#
Branch1-ASA#conf t
Branch1-ASA(config)#ntp authentication-key 201102 md markdiploma
Branch1-ASA(config)#ntp trusted 201102
Branch1-ASA(config)#ntp server 150.10.1.5 key 201102
Branch1-ASA(config)#ex
Branch1-ASA#

```

Рисунок 3.37 – Приклад налаштування синхронізації часу на брандмауері Branch1-ASA

```

HomeBranch
Physical Config CLI Attributes
IOS Command Line Interface
HomeBranch>en
HomeBranch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
HomeBranch(config)#service times log datetime msec
HomeBranch(config)#service times debug datetime msec
HomeBranch(config)#clock timezone GMT 2
HomeBranch(config)#ntp authentication-key 201102 md markdiploma
HomeBranch(config)#ntp trusted 201102
HomeBranch(config)#ntp server 150.10.1.5 key 201102
HomeBranch(config)#ex
HomeBranch#
*Mar 01, 01:19:24.1919: SYS-5-CONFIG_I: Configured from console by console
HomeBranch#

```

Рисунок 3.38 – Приклад налаштування синхронізації часу на маршрутизаторі HomeBranch

Наступним етапом буде налаштування SYSLOG-сервера для журналювання подій у нашій мережі. Першим кроком включаємо сам сервіс SYSLOG на сервері. Це забезпечить зберігання всіх журналів подій в одному місці для подальшого аналізу. Потім на кожному мережевому пристрої (маршрутизаторах, брандмауерах, комутаторах) налаштовуємо логування, вказуючи адресу SYSLOG-сервера для надсилання повідомлень про події:

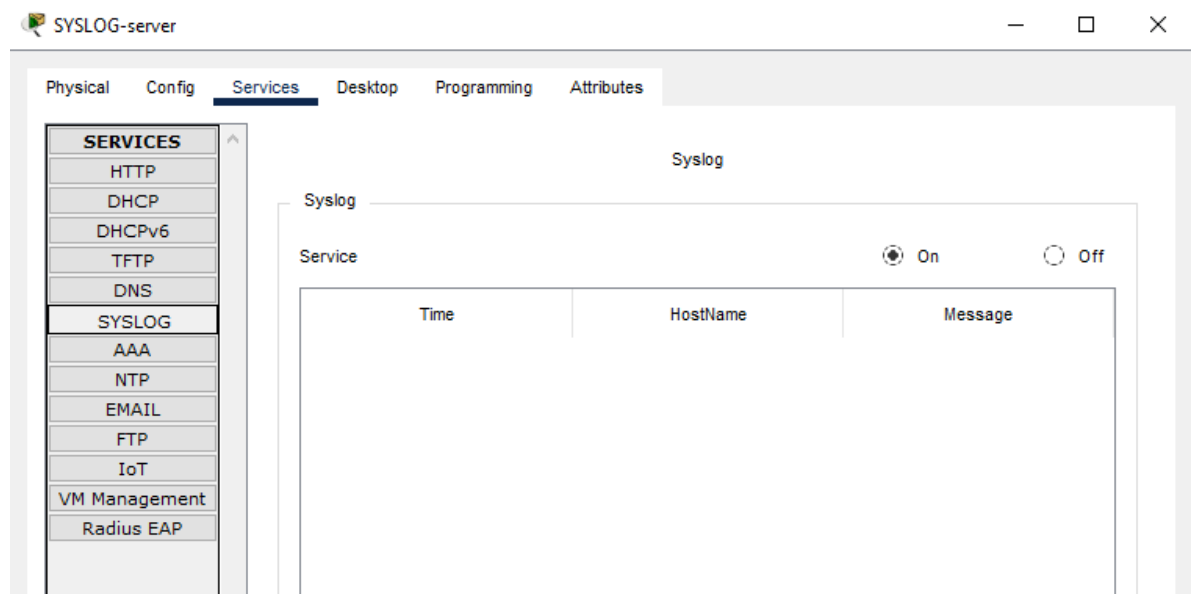


Рисунок 3.39 – Увімкнення сервісу SYSLOG на сервері

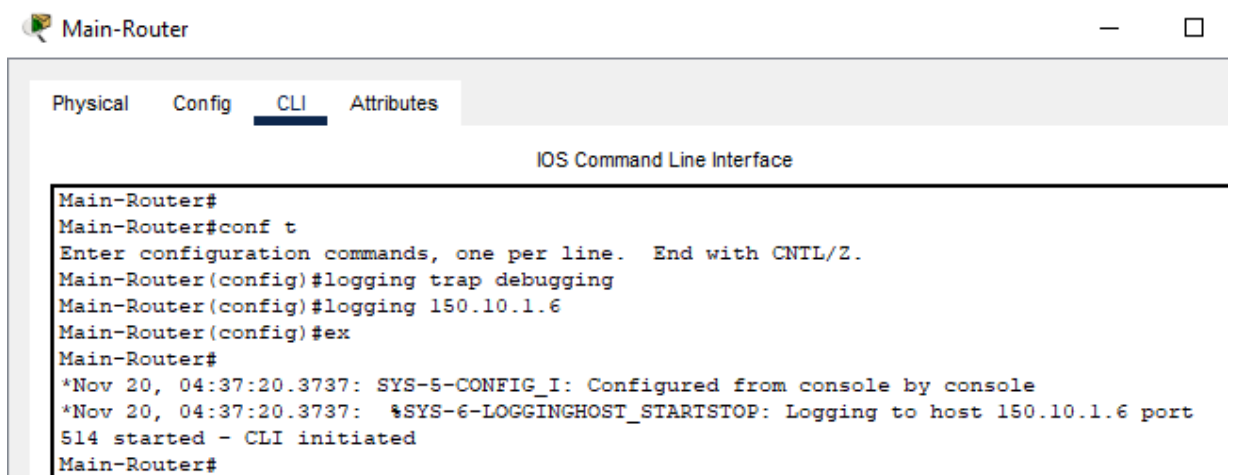


Рисунок 3.40 – Приклад налаштування журналювання подій на маршрутизаторі Main-Router

```

Branch2Switch
Physical Config CLI Attributes
IOS Command Line Interface

Branch2Switch>en
Branch2Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Branch2Switch(config)#logging trap debugging
Branch2Switch(config)#logging 150.10.1.6
Branch2Switch(config)#ex
Branch2Switch#
*Mar 01, 01:22:26.2222: SYS-5-CONFIG_I: Configured from console by console
*Mar 01, 01:22:26.2222: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 150.10.1.6 port
514 started - CLI initiated
Branch2Switch#

```

Рисунок 3.41 – Приклад налаштування журналювання подій на комутаторі Branch2Switch

Третім етапом налаштування мережі є інтеграція TACACS+ сервера для адміністрування за допомогою моделі AAA. Це дає змогу створити безпечне і контрольоване середовище для адміністраторів, де доступ до важливих мережевих пристроїв регулюється централізовано, а всі дії користувачів реєструються для подальшого аналізу.

Першим кроком є налаштування TACACS+ сервера, на якому потрібно створити користувачів з відповідними правами доступу. Кожен користувач отримає унікальний логін і пароль для входу на мережеві пристрої. Це забезпечує контроль за тим, хто має доступ до мережі, і дозволяє централізовано управляти обліковими записами.

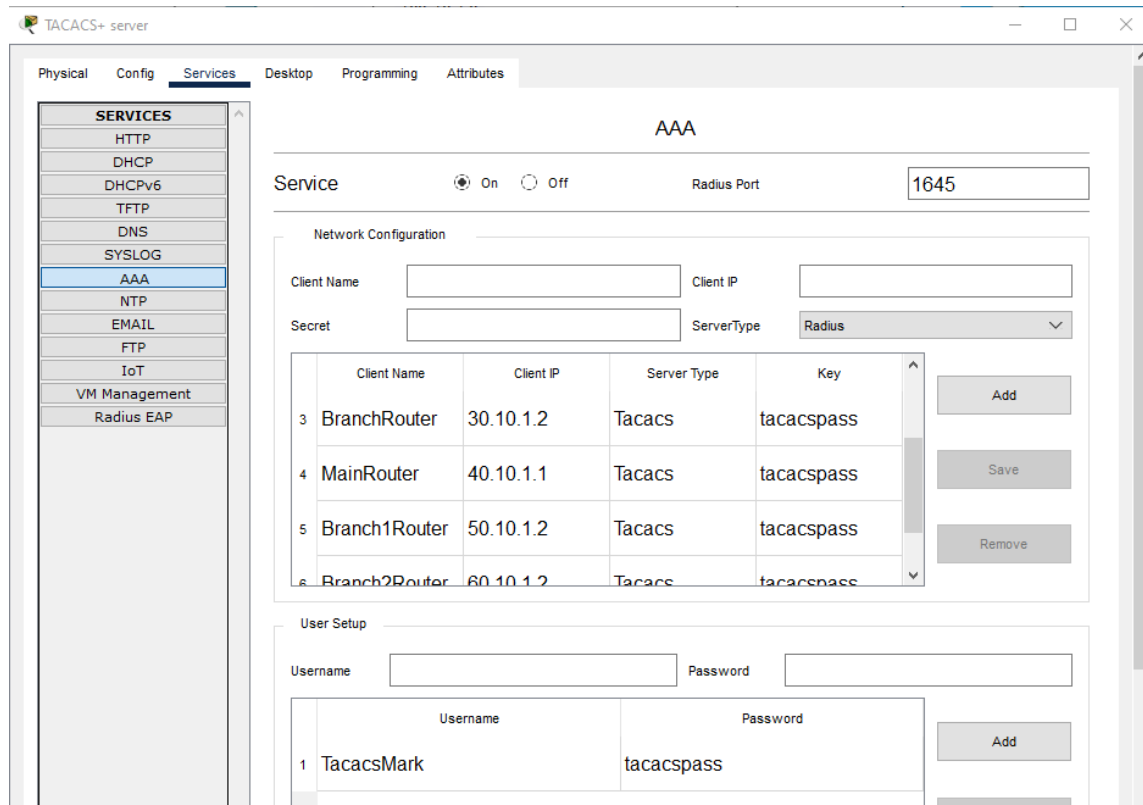


Рисунок 3.42 – Налаштування логіну і паролю, та додавання клієнтів на TACACS+ сервері

Далі потрібно налаштувати мережеві пристрої, такі як маршрутизатори та комутатори, для роботи з TACACS+. Для цього на кожному пристрої вказується адреса TACACS+ сервера та секретний ключ для захищеного з'єднання. Це дає змогу пристроям звертатися до TACACS+ сервера для аутентифікації користувачів перед наданням доступу до мережі.

Останнім кроком є налаштування моделі AAA на мережевих пристроях, що забезпечить використання TACACS+ для аутентифікації та авторизації доступу. Це дозволяє централізовано управляти правами доступу, обліковувати дії користувачів та створювати зручний механізм для адміністрування всієї мережі. Завдяки цим налаштуванням, зокрема у великих організаціях, забезпечується висока безпека і контроль за доступом до мережевих ресурсів.

Налаштовуємо протокол SSH з використанням TACACS+:

```

Branch1Router>en
Branch1Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch1Router(config)#aaa new-model
Branch1Router(config)#username TacacsMark privilege 15 secret tacacspass
Branch1Router(config)#enable secret tacacspass
Branch1Router(config)#tacacs-server host 150.10.1.7 key tacacspass
Branch1Router(config)#aaa authentication login default group tacacs+ local
Branch1Router(config)#line con 0
Branch1Router(config-line)#login authentication default
Branch1Router(config-line)#exit
Branch1Router(config)#ip domain-name my.net
Branch1Router(config)#crypto key generate rsa
The name for the keys will be: Branch1Router.my.net
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Branch1Router(config)#ip ssh version 2
*Mar 1 0:1:12.836: %SSH-5-ENABLED: SSH 1.99 has been enabled
Branch1Router(config)#ip ssh time-out 30
Branch1Router(config)#ip ssh authentication-retries 3
Branch1Router(config)#ex
Branch1Router#
  
```

Рисунок 3.43 – Приклад налаштування протоколу SSH + TACACS+ на маршрутизаторі Branch1Router

Завершальним кроком налаштування захисту мережі є впровадження протоколу Port Security на усіх кінцевих комутаторах. Використання цього протоколу допомагає запобігти підключенню небажаних або неавторизованих пристроїв, знижуючи ризик атак на мережу. Завдяки впровадженню Port Security, мережа буде більш захищеною, і зловмисникам буде набагато складніше здійснити несанкціонований доступ або атаки через фізичні порти.

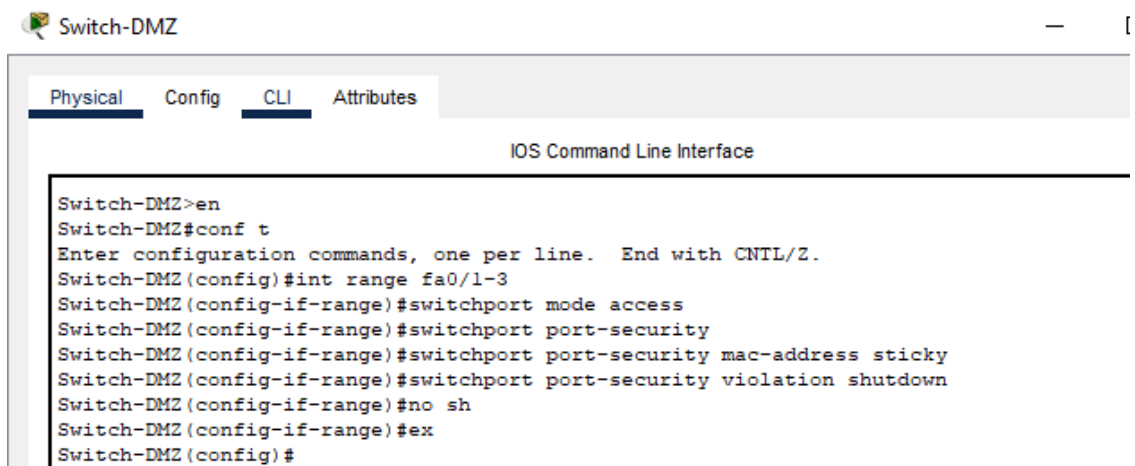


Рисунок 3.44 – Приклад налаштування протоколу Port Security на комутаторі Switch-DMZ

3.3 Тестування процесу захищеного обміну інформацією в корпоративній мережі

Після завершення налаштування мережі можемо перейти до безпосереднього тестування її роботи. Першим етапом буде перевірка зв'язку між робочими станціями головного офісу, що дозволить переконатися у коректності налаштувань локальної мережі та забезпеченні взаємодії між різними пристроями.

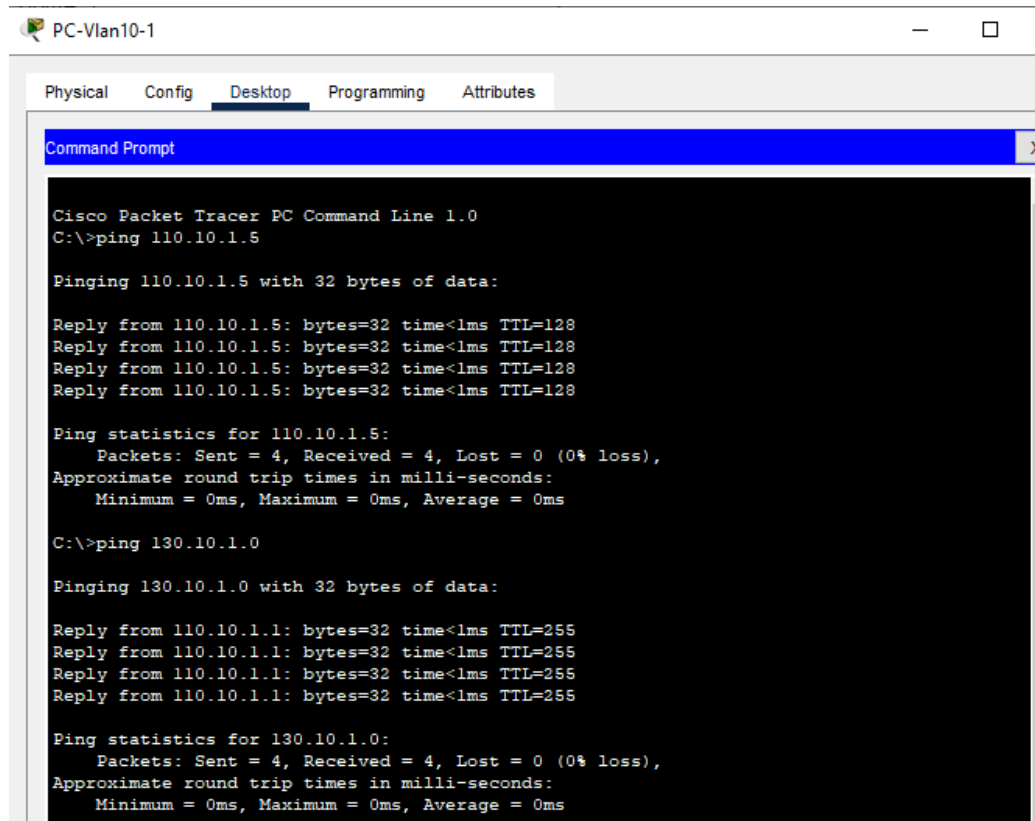


Рисунок 3.45 – Перевірка зв'язку між станціями в головному офісі

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

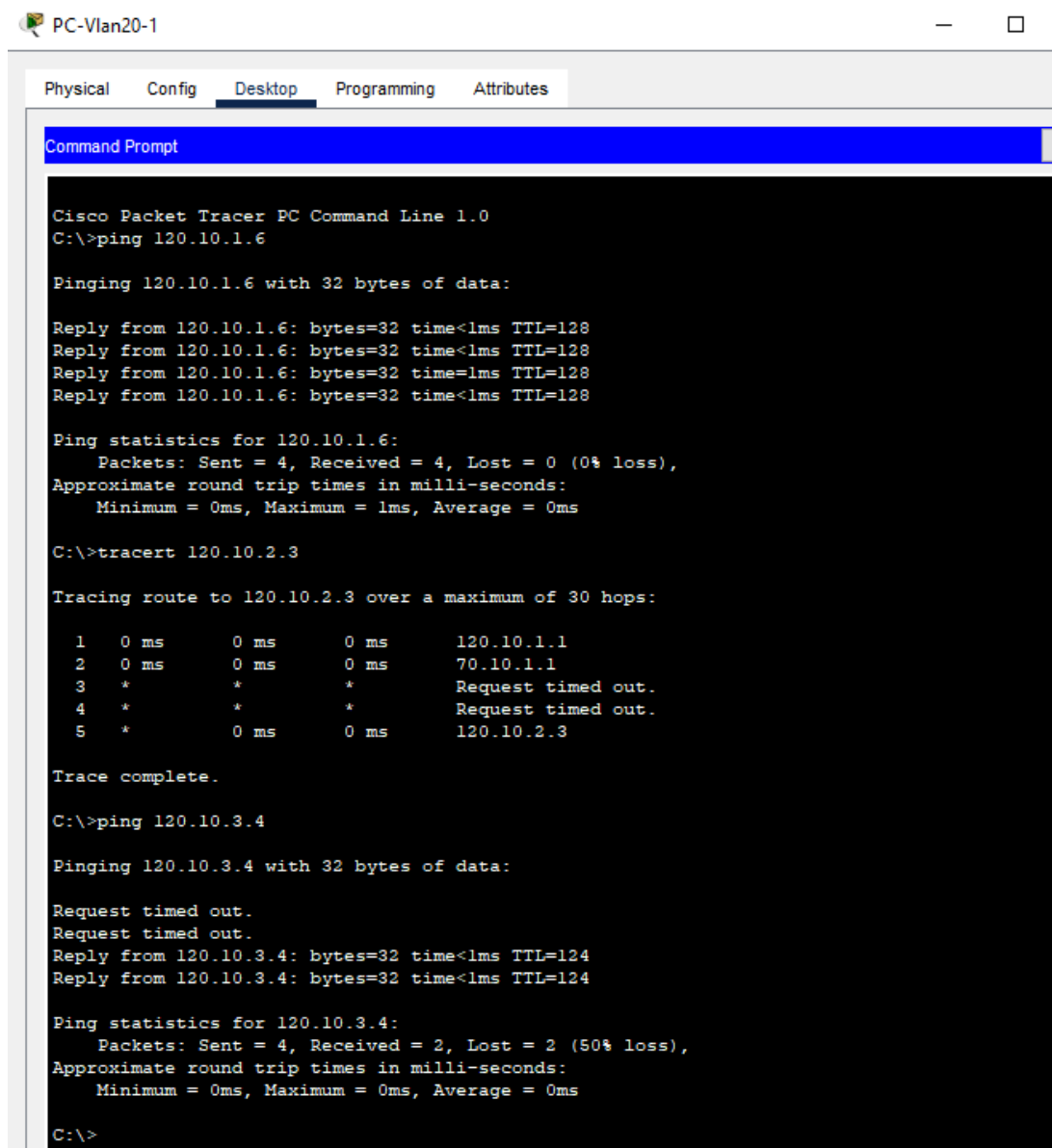


Рисунок 3.46 – Перевірка зв'язку між станціями одного VLAN з різних частин мережі

Оскільки VLAN з різних підмереж взаємодіють лише з відповідними VLAN, а бездротові пристрої мережі забезпечують зв'язок із домашнім комп'ютером, доцільно перевірити коректність цих налаштувань. Це включає тестування передачі даних між пристроями в межах однієї VLAN, а також перевірку стабільності зв'язку між бездротовими пристроями та домашньою мережею. Такий підхід дозволяє переконатися у правильному функціонуванні сегментації мережі, маршрутизації та відповідності всіх компонентів заданим вимогам.

PDU List Window										
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC-Vlan10-1	PC-Branch1-Vlan10-1	ICMP		0.000	N	0	(edit)	
	Successful	PC-Branch1-Vlan10-2	PC-Vlan10-2	ICMP		0.000	N	1	(edit)	
	Successful	PC-Vlan10-1	PC-Branch2-Vlan10-2	ICMP		0.000	N	2	(edit)	
	Successful	PC-Branch2-Vlan10-1	PC-Branch1-Vlan10-1	ICMP		0.000	N	3	(edit)	
	Successful	PC-Vlan20-1	PC-Branch1-Vlan20-1	ICMP		0.000	N	4	(edit)	
	Successful	PC-Vlan20-2	PC-Branch2-Vlan20-2	ICMP		0.000	N	5	(edit)	
	Successful	PC-Branch2-Vlan20-1	PC-Branch1-Vlan20-1	ICMP		0.000	N	6	(edit)	
	Failed	PC-Vlan10-1	PC-Branch1-Vlan20-1	ICMP		0.000	N	7	(edit)	
	Failed	PC-Branch2-Vlan20-1	PC-Branch1-Vlan10-1	ICMP		0.000	N	8	(edit)	
	Failed	PC-Branch2-Vlan10-2	PC-Vlan20-2	ICMP		0.000	N	9	(edit)	
	Failed	PC-Branch1-Vlan10-1	PC-Branch2-Vlan20-2	ICMP		0.000	N	10	(edit)	

Рисунок 3.47 – Перевірка зв'язку станцій в межах однієї VLAN та ні

PDU List Window										
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC-HomeBranch	PC-WiFi1	ICMP		0.000	N	0	(edit)	
	Successful	Laptop-WiFi	PC-HomeBranch	ICMP		0.000	N	1	(edit)	
	Failed	PC-HomeBranch	PC-Vlan10-1	ICMP		0.000	N	2	(edit)	
	Failed	PC-HomeBranch	PC-Vlan20-2	ICMP		0.000	N	3	(edit)	
	Failed	PC-HomeBranch	PC-Branch1-Vlan10-2	ICMP		0.000	N	4	(edit)	
	Failed	PC-WiFi2	PC-Branch2-Vlan10-1	ICMP		0.000	N	5	(edit)	
	Failed	Laptop-WiFi	PC-Branch1-Vlan20-1	ICMP		0.000	N	6	(edit)	

Рисунок 3.48 – Перевірка зв'язку домашньої та бездротових станцій і зв'язок з VLAN

Наступним етапом тестування коректності налаштувань корпоративної мережі є перевірка роботи серверів та ключових сервісів. Спочатку проводиться перевірка логування на сервері SYSLOG, щоб переконатися, що всі події мережі фіксуються коректно.

SYSLOG-server										
Physical Config Services Desktop Programming Attributes										
SERVICES										
HTTP										
DHCP										
DHCPv6										
TFTP										
DNS										
SYSLOG										
AAA										
NTP										
EMAIL										
FTP										
IoT										
VM Management										
Radius EAP										
Syslog										
Service										
On Off										
1	11.20.2024 05:32:49.128 AM	150.10.1.1	%SYS-5-CONFIG_I: Configured from console by console							
2	11.20.2024 05:32:29.823 AM	10.10.1.2	%SYS-5-CONFIG_I: Configured from console by console							
3	03.01.1993 12:02:19.657 AM	50.10.1.2	%SYS-5-CONFIG_I: Configured from console by console							
4	03.01.1993 12:02:19.657 AM	50.10.1.2	: %SYS-6-LOGGINGHOST_STARTSTOP...							
5	03.01.1993 12:02:50.277 AM	50.10.1.2	%SYS-5-CONFIG_I: Configured from console by console							

Рисунок 3.49 – Перевірка журналювання подій на сервері SYSLOG

Після цього здійснюється тестування доступу до мережевих пристроїв за допомогою протоколу SSH. Для цього використовується обліковий запис, створений на TACACS+ сервері. Така перевірка дозволяє підтвердити функціонування централізованого контролю доступу та відповідність налаштувань політикам безпеки мережі.

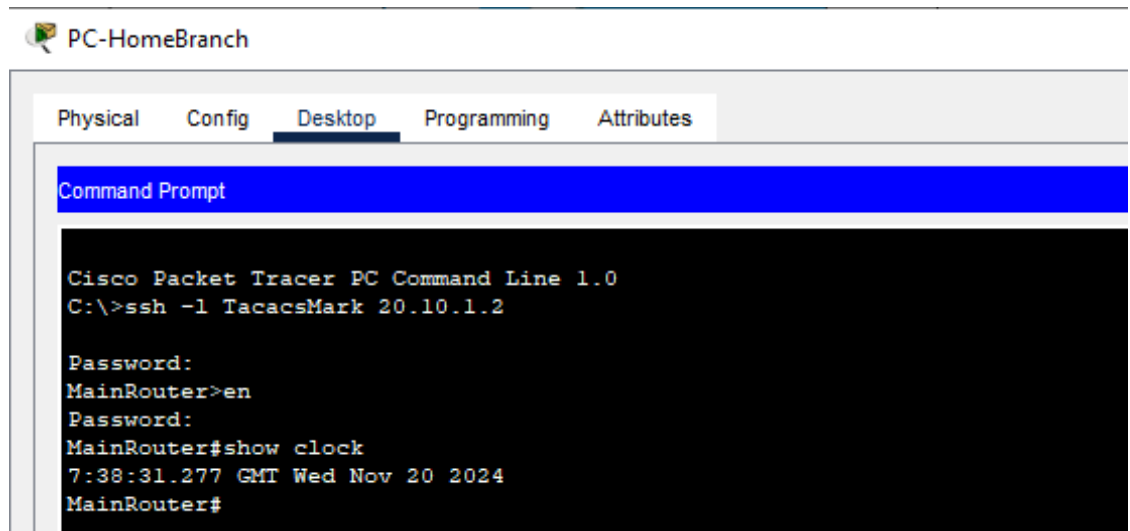


Рисунок 3.50 – Успішна спроба віддаленого підключення з робочої станції до маршрутизатора і вивід команди для перевірки часу

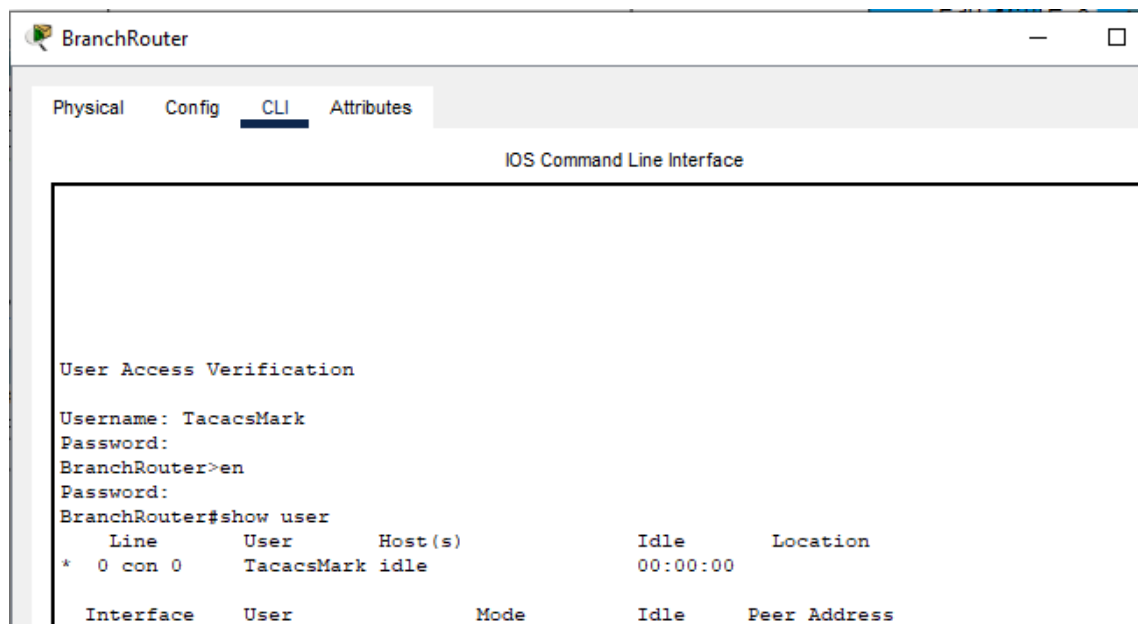


Рисунок 3.51 – Вхід під користувачем на маршрутизатор BranchRouter та вивід команди show user

Після перевірки зв'язку між пристроями та функціонування серверів можна переходити до виконання довідкових команд. Ці команди дозволяють переглянути поточну конфігурацію та статус роботи мережевих пристроїв. Цей етап тестування

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

є важливим для остаточної оцінки готовності мережі до експлуатації та забезпечення її відповідності заданим технічним вимогам.

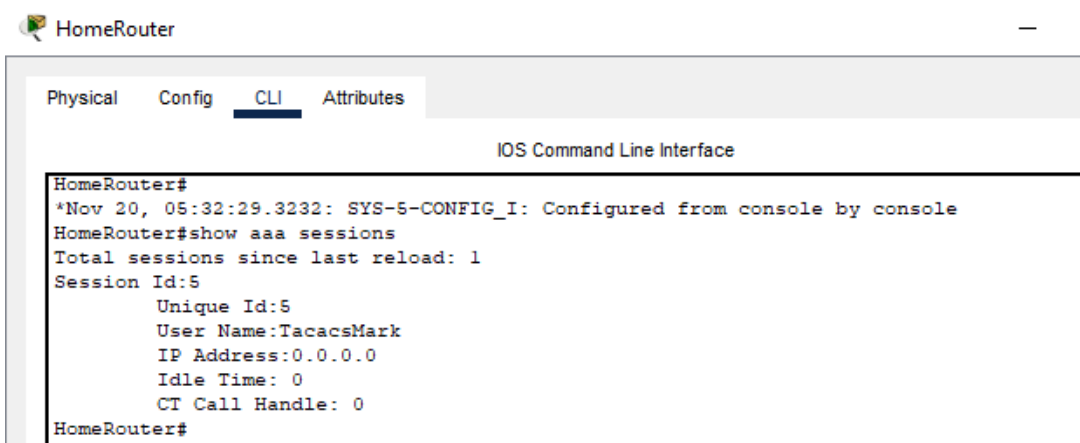


Рисунок 3.52 – Виконання команди show aaa sessions на маршрутизаторі HomeRouter

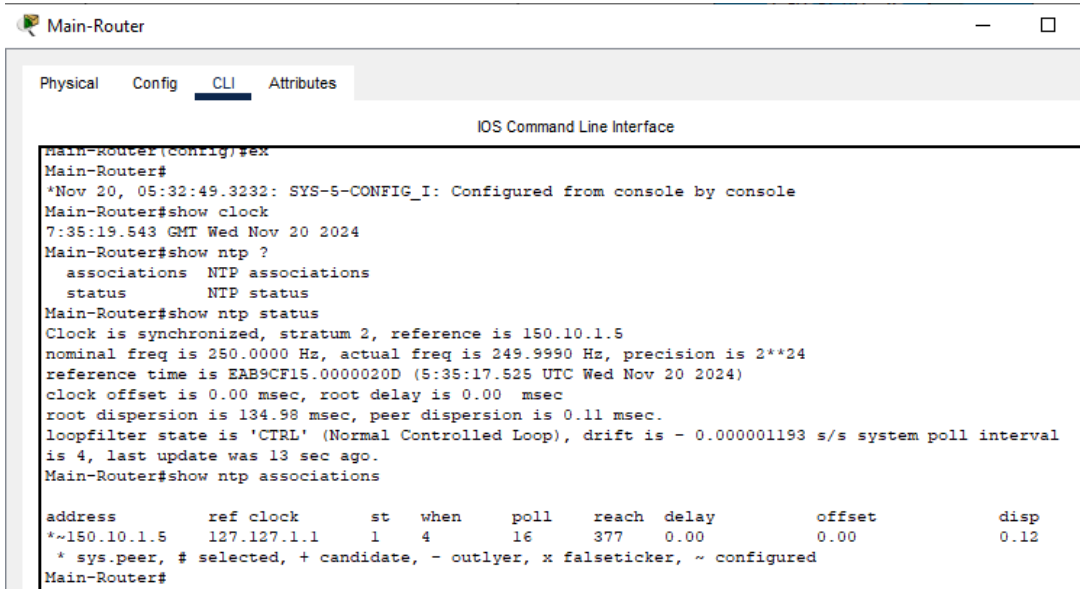


Рисунок 3.53 – Виконання команд show clock, show ntp status та show ntp associations на маршрутизаторі Main-Router

```

BranchRouter#sh logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
                    0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 7 messages logged, xml disabled,
filtering disabled
Monitor logging: level debugging, 7 messages logged, xml disabled,
filtering disabled
Buffer logging: disabled, xml disabled,
filtering disabled

Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
Trap logging: level debugging, 7 message lines logged
Logging to 150.10.1.6 (udp port 514, audit disabled,
authentication disabled, encryption disabled, link up),
7 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled
BranchRouter#
  
```

Рисунок 3.54 – Виконання команди show logging на маршрутизаторі BranchRouter

```

Branch2Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
  (Count)      (Count)      (Count)
-----
Fa0/1          1          1          0          Shutdown
Fa0/2          1          1          0          Shutdown
Fa0/4          1          1          0          Shutdown
Fa0/5          1          1          0          Shutdown
-----

Branch2Switch#show port-security int fa0/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
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 : 00D0.BA65.BA96:10
Security Violation Count : 0
Branch2Switch#
  
```

Рисунок 3.55 – Виконання команди show port-security на комутаторі Branch2Switch

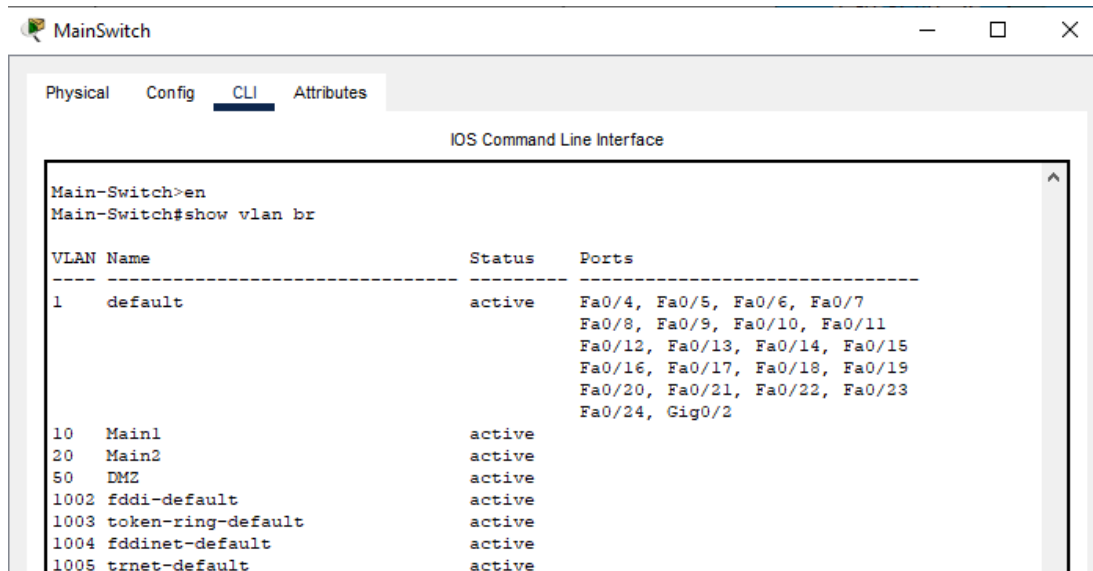


Рисунок 3.56 – Виконання команди show vlan brief на комутаторі MainSwitch

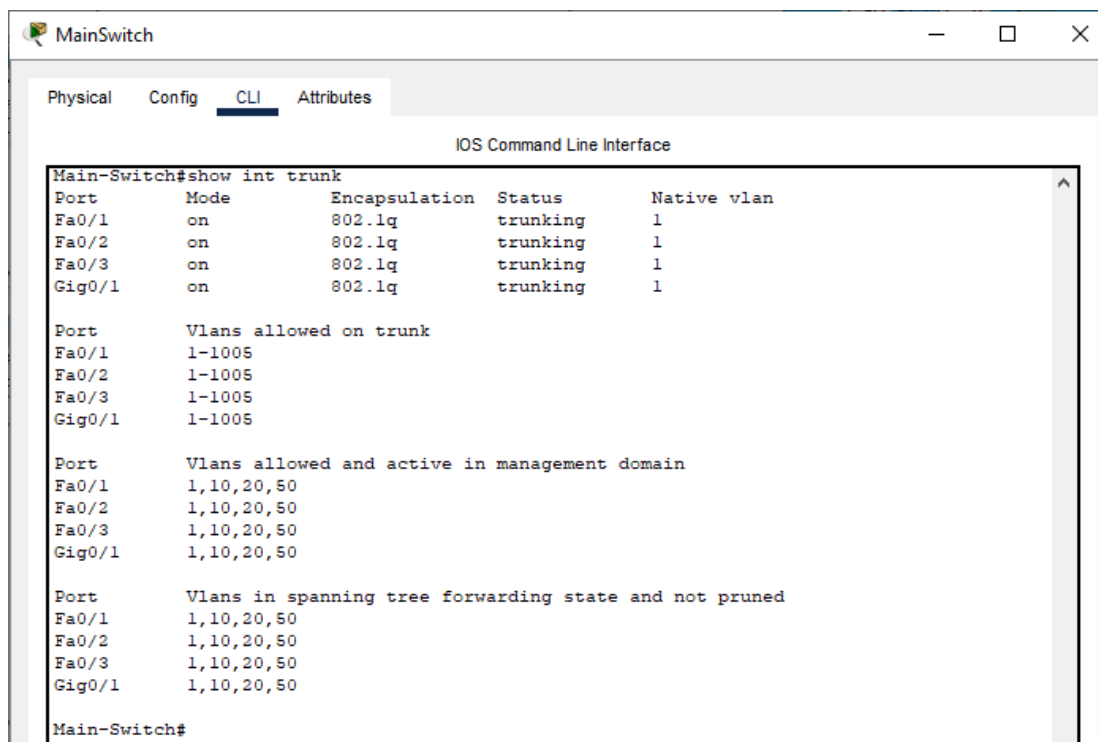


Рисунок 3.57 – Виконання команди show interface trunk на комутаторі MainSwitch

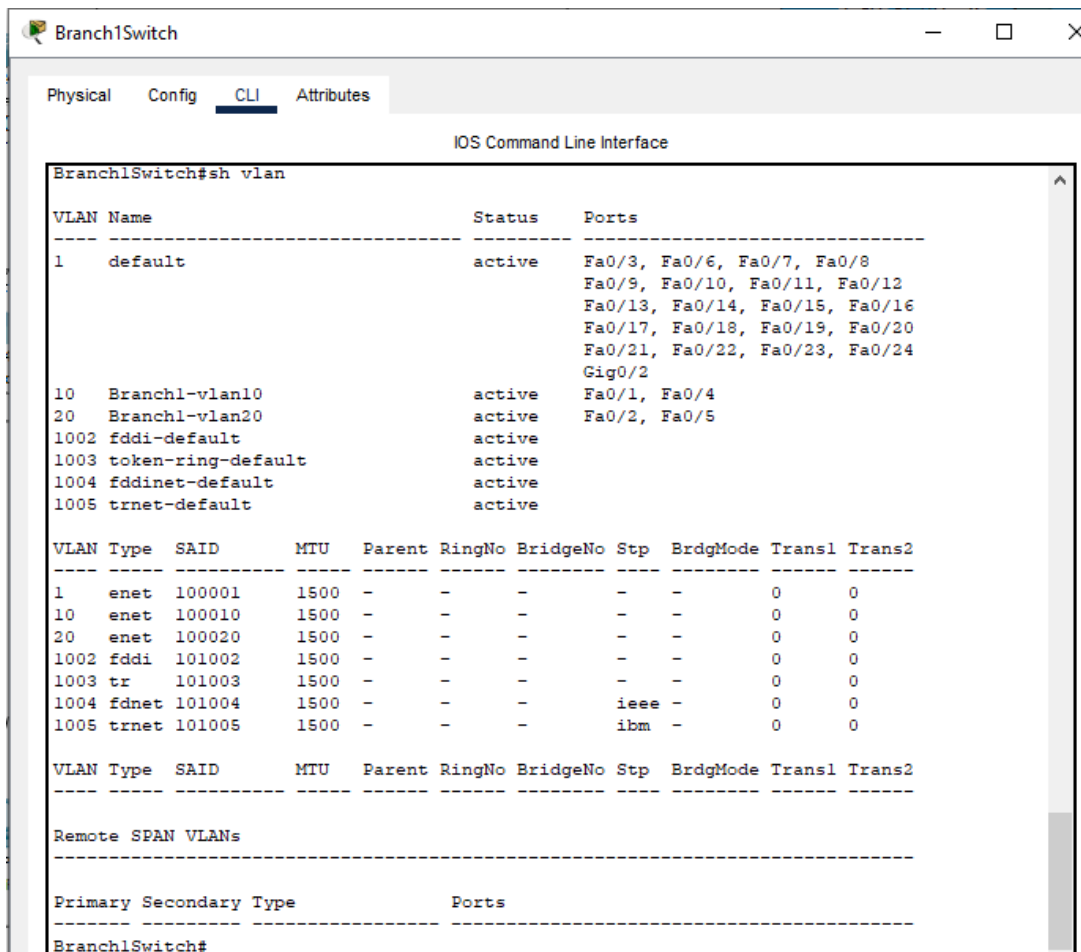


Рисунок 3.58 – Виконання команди show vlan на комутаторі Branch1Switch

Далі переходимо до виконання довідкових команд на міжмережевих екранах, що дозволить перевірити коректність налаштувань та функціонування ключових компонентів мережі.

Першим кроком є перевірка таблиці маршрутизації. Це дає змогу переконатися, що всі маршрути до внутрішніх підмереж та віддалених офісів правильно внесені і використовуються. Особливу увагу приділяємо маршрутам, які забезпечують передачу трафіку через тунелі VPN, щоб переконатися в їх коректній роботі.

Далі досліджуємо довідникові команди, пов'язані з VPN. Переглядаємо стан активних тунелів, параметри шифрування, а також статистику передачі даних через захищені канали. Це допомагає переконатися, що всі створені VPN-з'єднання стабільні, налаштовані відповідно до вимог безпеки та забезпечують належний рівень захищеності інформації.

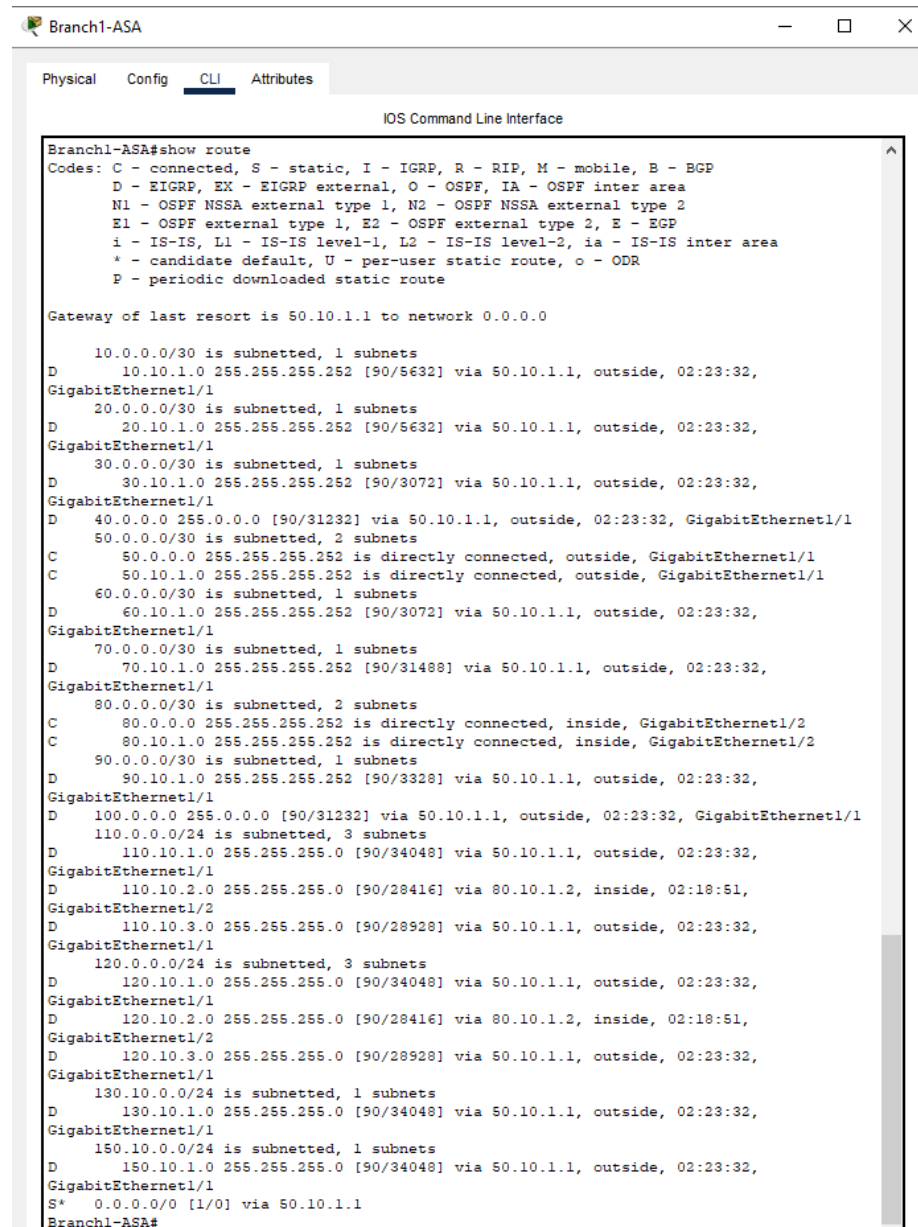


Рисунок 3.59 – Виконання команди show route на брандмауері Branch1-ASA

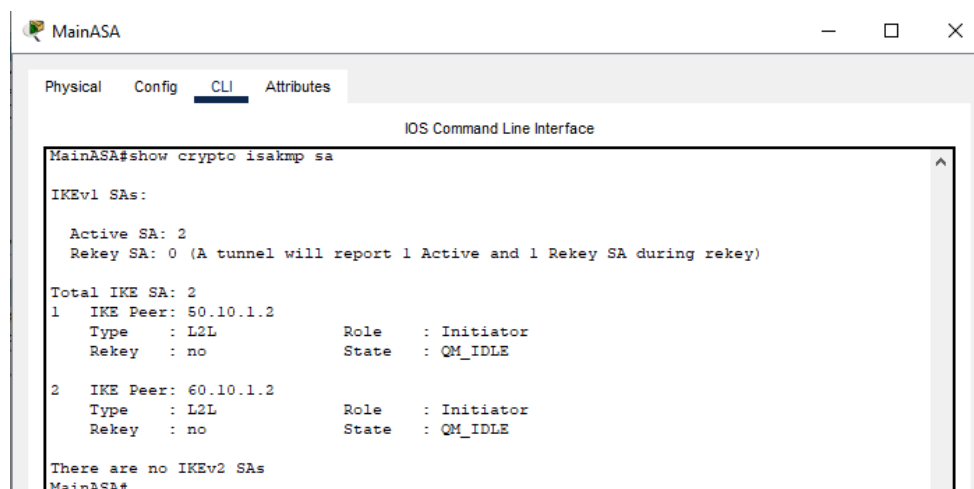


Рисунок 3.60 – Виконання команди show crypto isakmp sa на брандмауері MainASA

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Branch2-ASA#show crypto ipsec sa

interface: outside
  Crypto map tag: VPN, seq num: 1, local addr 60.10.1.2

    permit ip 110.10.3.0 255.255.255.0 110.10.1.0 255.255.255.0
    local ident (addr/mask/prot/port): (110.10.3.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (110.10.1.0/255.255.255.0/0/0)
    current_peer 40.10.1.2
      #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0
      #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors 0, #recv errors 2

    local crypto endpt.: 60.10.1.2/0, remote crypto endpt.:40.10.1.2/0
    path mtu 1500, ip mtu, ipsec overhead 78, media mtu 1500
    current outbound spi: 0x584CC9F6(1481427446)
    current inbound spi: 0x6C997E1F(1481427446)

  inbound esp sas:
    spi: 0x6C997E1F(1821998623)
      transform: esp-aes esp-sha-hmac no compression
      in use settings ={L2L, Tunnel, }
      slot: 0, conn id: 2003, crypto map: VPN
      sa timing: remaining key lifetime (k/sec): (4525504/1950)
      IV size: 16 bytes
      replay detection support: N
      Anti replay bitmap:
        0x00000000 0x0000001F
  outbound esp sas:
    spi: 0x584CC9F6(1481427446)
      transform: esp-aes esp-sha-hmac no compression
      in use settings ={L2L, Tunnel, }
      slot: 0, conn id: 2004, crypto map: VPN
      sa timing: remaining key lifetime (k/sec): (4525504/1950)
      IV size: 16 bytes
      replay detection support: N
      Anti replay bitmap:
        0x00000000 0x00000001

  Crypto map tag: VPN, seq num: 1, local addr 60.10.1.2

    permit ip 120.10.3.0 255.255.255.0 120.10.1.0 255.255.255.0
    local ident (addr/mask/prot/port): (120.10.3.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (120.10.1.0/255.255.255.0/0/0)
    current_peer 40.10.1.2
      #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors 0, #recv errors 2

    local crypto endpt.: 60.10.1.2/0, remote crypto endpt.:40.10.1.2/0
    path mtu 1500, ip mtu, ipsec overhead 78, media mtu 1500
    <--- More --->
  
```

Рисунок 3.61 – Виконання команди show crypto ipsec sa на брандмауері Branch2-ASA (частина 1)

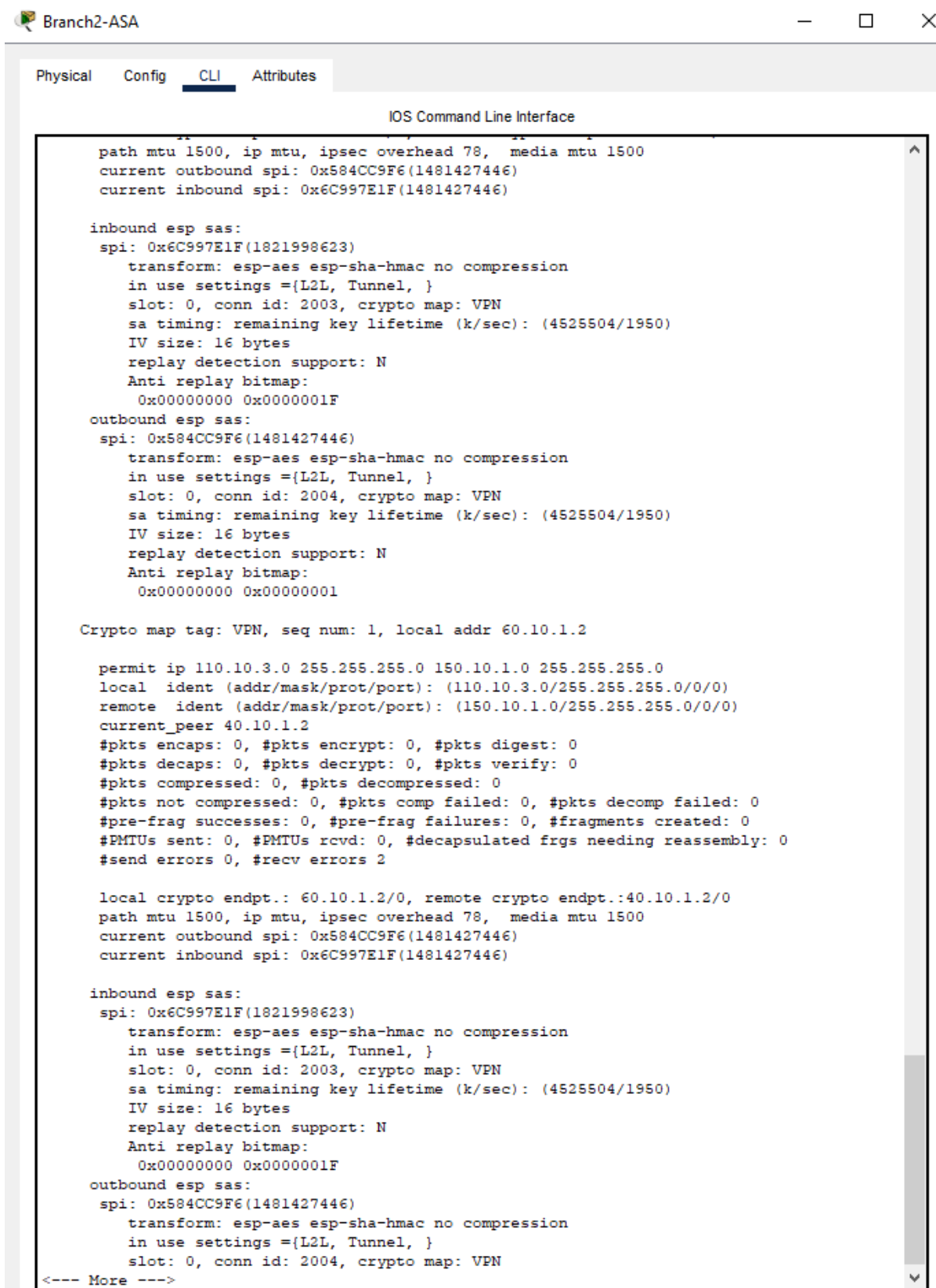


Рисунок 3.62 – Виконання команди show crypto ipsec sa на брандмауері Branch2-ASA (частина 2)

```

Branch2-ASA
Physical Config CLI Attributes
IOS Command Line Interface

sa timing: remaining key lifetime (k/sec): (4525504/1950)
IV size: 16 bytes
replay detection support: N
Anti replay bitmap:
0x00000000 0x00000001

Crypto map tag: VPN, seq num: 1, local addr 60.10.1.2

permit ip 120.10.3.0 255.255.255.0 150.10.1.0 255.255.255.0
local ident (addr/mask/prot/port): (120.10.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (150.10.1.0/255.255.255.0/0/0)
current_peer 40.10.1.2
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors 0, #recv errors 2

local crypto endpt.: 60.10.1.2/0, remote crypto endpt.: 40.10.1.2/0
path mtu 1500, ip mtu, ipsec overhead 78, media mtu 1500
current outbound spi: 0x584CC9F6(1481427446)
current inbound spi: 0x6C997E1F(1481427446)

inbound esp sas:
spi: 0x6C997E1F(1821998623)
transform: esp-aes esp-sha-hmac no compression
in use settings = {L2L, Tunnel, }
slot: 0, conn id: 2003, crypto map: VPN
sa timing: remaining key lifetime (k/sec): (4525504/1950)
IV size: 16 bytes
replay detection support: N
Anti replay bitmap:
0x00000000 0x0000001F

outbound esp sas:
spi: 0x584CC9F6(1481427446)
transform: esp-aes esp-sha-hmac no compression
in use settings = {L2L, Tunnel, }
slot: 0, conn id: 2004, crypto map: VPN
sa timing: remaining key lifetime (k/sec): (4525504/1950)
IV size: 16 bytes
replay detection support: N
Anti replay bitmap:
0x00000000 0x00000001

Crypto map tag: VPN, seq num: 2, local addr 60.10.1.2

permit ip 110.10.3.0 255.255.255.0 110.10.2.0 255.255.255.0
local ident (addr/mask/prot/port): (110.10.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (110.10.2.0/255.255.255.0/0/0)
current_peer 50.10.1.2
#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors 1, #recv errors 0

<--- More --->

```

Рисунок 3.63 – Виконання команди show crypto ipsec sa на брандмауері Branch2-ASA (частина 3)

```

Branch2-ASA

Physical Config CLI Attributes

IOS Command Line Interface

#send errors 1, #recv errors 0

local crypto endpt.: 60.10.1.2/0, remote crypto endpt.:50.10.1.2/0
path mtu 1500, ip mtu, ipsec overhead 78, media mtu 1500
current outbound spi: 0xDC36799C(3694557596)
current inbound spi: 0x445217CD(3694557596)

inbound esp sas:
spi: 0x445217CD(1146230733)
transform: esp-aes esp-sha-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn id: 2006, crypto map: VPN
sa timing: remaining key lifetime (k/sec): (4525504/2149)
IV size: 16 bytes
replay detection support: N
Anti replay bitmap:
0x00000000 0x0000001F
outbound esp sas:
spi: 0xDC36799C(3694557596)
transform: esp-aes esp-sha-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn id: 2007, crypto map: VPN
sa timing: remaining key lifetime (k/sec): (4525504/2149)
IV size: 16 bytes
replay detection support: N
Anti replay bitmap:
0x00000000 0x00000001

Crypto map tag: VPN, seq num: 2, local addr 60.10.1.2

permit ip 120.10.3.0 255.255.255.0 120.10.2.0 255.255.255.0
local ident (addr/mask/prot/port): (120.10.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (120.10.2.0/255.255.255.0/0/0)
current_peer 50.10.1.2
#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors 0, #recv errors 0

local crypto endpt.: 60.10.1.2/0, remote crypto endpt.:50.10.1.2/0
path mtu 1500, ip mtu, ipsec overhead 78, media mtu 1500
current outbound spi: 0xDC36799C(3694557596)
current inbound spi: 0x445217CD(3694557596)

inbound esp sas:
spi: 0x445217CD(1146230733)
transform: esp-aes esp-sha-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn id: 2006, crypto map: VPN
sa timing: remaining key lifetime (k/sec): (4525504/2149)
IV size: 16 bytes
replay detection support: N
Anti replay bitmap:
0x00000000 0x0000001F
outbound esp sas:
spi: 0xDC36799C(3694557596)
<--- More --->

```

Рисунок 3.64 – Виконання команди show crypto ipsec sa на брандмауері Branch2-ASA (частина 4)

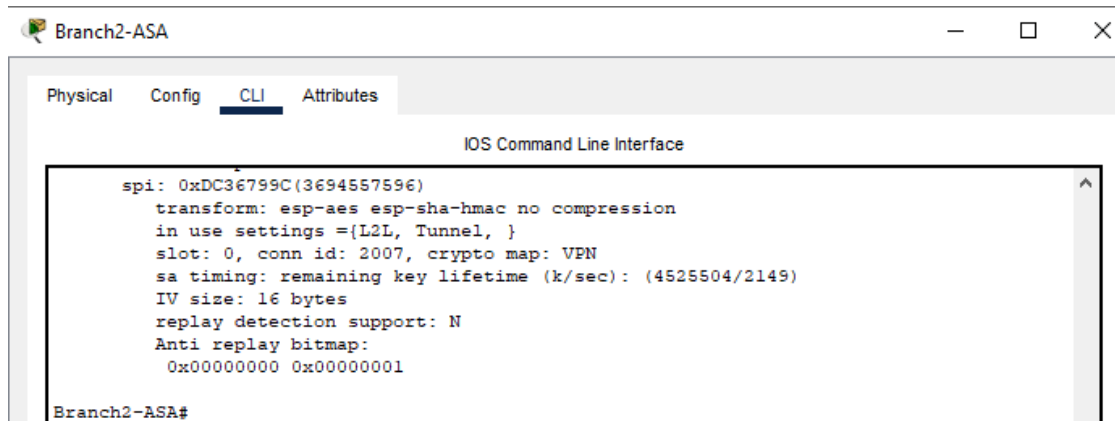


Рисунок 3.65 – Виконання команди show crypto ipsec sa на брандмауері Branch2-ASA (частина 5)

Також проведемо перевірку стану VPN-тунелю між маршрутизаторами HomeRouter та MainRouter:

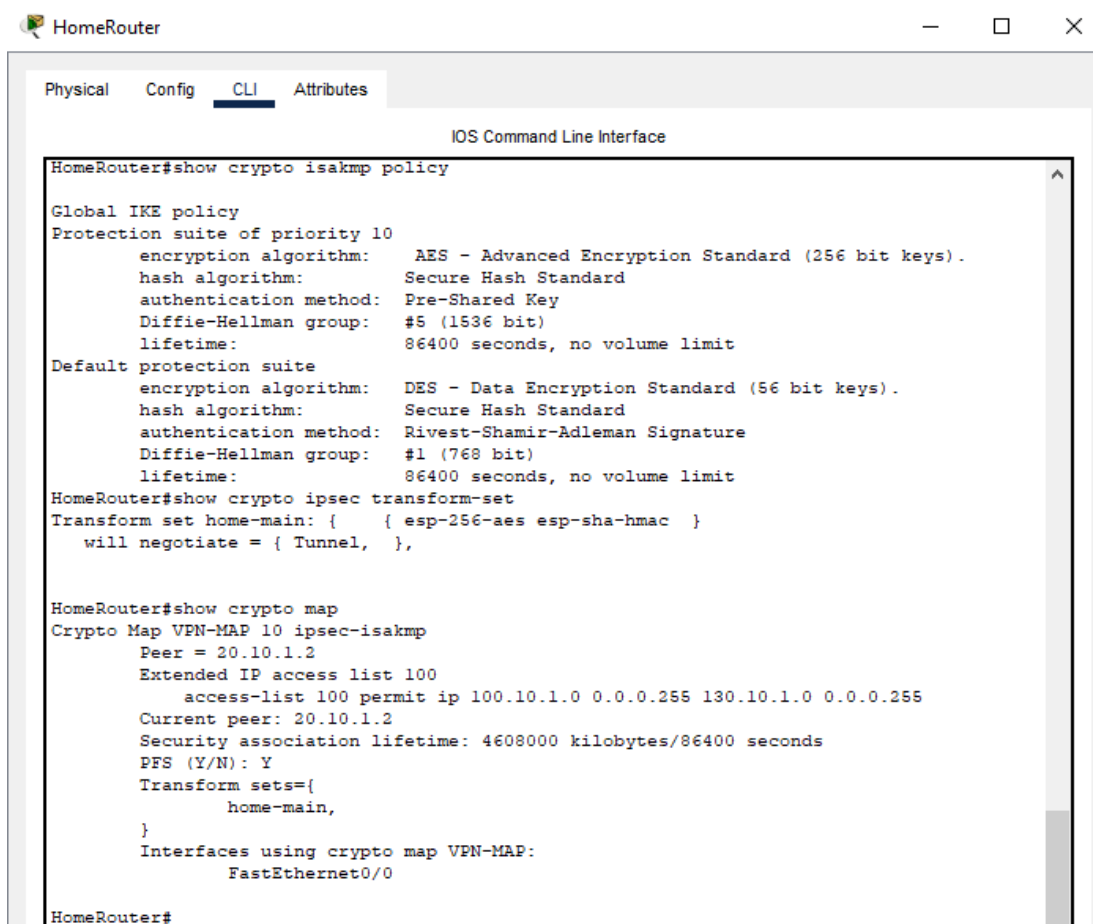


Рисунок 3.66 – Виконання команд show crypto isakmp policy та show crypto map на маршрутизаторі HomeRouter

```

MainRouter
Physical Config CLI Attributes
IOS Command Line Interface

Password: show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
10.10.1.2    20.10.1.2    QM_IDLE        1001      0  ACTIVE

IPv6 Crypto ISAKMP SA

MainRouter#show crypto ipsec sa

interface: FastEthernet0/0
  Crypto map tag: VPN-MAP, local addr 20.10.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (130.10.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (100.10.1.0/255.255.255.0/0/0)
current_peer 10.10.1.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 20.10.1.2, remote crypto endpt.:10.10.1.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x9D61E682(2640438914)

inbound esp sas:
  spi: 0x66E3BF6C(1726201708)
    transform: esp-aes 256 esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2008, flow_id: FPGA:1, crypto map: VPN-MAP
    sa timing: remaining key lifetime (k/sec): (4525504/84673)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x9D61E682(2640438914)
    transform: esp-aes 256 esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2009, flow_id: FPGA:1, crypto map: VPN-MAP
    sa timing: remaining key lifetime (k/sec): (4525504/84673)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:

MainRouter#

```

Рисунок 3.67 – Виконання команд show crypto isakmp sa та show crypto ipsec sa на маршрутизаторі MainRouter

```

MainASA#show clock
*8:5:8.423 UTC Wed Nov 20 2024
MainASA#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic LAN-VLAN10 interface
   translate_hits = 4, untranslate_hits = 0

4 (inside) to (outside) source dynamic LAN-VLAN20 interface
   translate_hits = 0, untranslate_hits = 0

7 (inside) to (outside) source dynamic LAN-WIFI interface
   translate_hits = 0, untranslate_hits = 0
8 (inside) to (outside) source dynamic LAN_DMZ interface
   translate_hits = 0, untranslate_hits = 0

MainASA#show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list TRAFEGO-VPN1; 4 elements; name hash: 0x16d56e0e
access-list TRAFEGO-VPN1 line 1 extended permit ip 110.10.1.0 255.255.255.0 110.10.2.0
255.255.255.0(hitcnt=0) 0xabd4388e
access-list TRAFEGO-VPN1 line 2 extended permit ip 120.10.1.0 255.255.255.0 120.10.2.0
255.255.255.0(hitcnt=1) 0xe23e3710
access-list TRAFEGO-VPN1 line 3 extended permit ip 150.10.1.0 255.255.255.0 110.10.2.0
255.255.255.0(hitcnt=1) 0x3d405445
access-list TRAFEGO-VPN1 line 4 extended permit ip 150.10.1.0 255.255.255.0 120.10.2.0
255.255.255.0(hitcnt=0) 0xa7779d04
access-list TRAFEGO-VPN2; 4 elements; name hash: 0xed241ded
access-list TRAFEGO-VPN2 line 1 extended permit ip 110.10.1.0 255.255.255.0 110.10.3.0
255.255.255.0(hitcnt=0) 0xa82a1a49
access-list TRAFEGO-VPN2 line 2 extended permit ip 120.10.1.0 255.255.255.0 120.10.3.0
255.255.255.0(hitcnt=1) 0x3821eb68
access-list TRAFEGO-VPN2 line 3 extended permit ip 150.10.1.0 255.255.255.0 110.10.3.0
255.255.255.0(hitcnt=0) 0xdc968048
access-list TRAFEGO-VPN2 line 4 extended permit ip 150.10.1.0 255.255.255.0 120.10.3.0

```

Рисунок 3.68 – Виконання команди show clock, show nat та show access-list на брандмауері MainASA

Після проведення перевірки роботи мережі можемо зробити висновок, що всі її компоненти налаштовані правильно, а сама мережа функціонує відповідно до заданих вимог.

Висновки до третього розділу:

У третьому розділі було детально розглянуто обладнання, що використовується в проєкті мережі, включаючи маршрутизатори, комутатори та брандмауери. Проведено базові налаштування мережевих пристроїв, які забезпечують стабільність і функціональність системи, а також впроваджено заходи для захисту мережі. Також було здійснено тестування основних функцій мережі, таких як взаємодія між VLAN, коректність роботи серверів та зв'язок через захищені канали. Результати підтвердили правильність налаштувань та відповідність мережі заданим вимогам.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		82

ВИСНОВКИ

У першому розділі було проведено аналіз основних аспектів забезпечення захищеного обміну трафіком, зокрема типів мережевих пристроїв та ключових практик безпеки. Розглянуто важливі технології та протоколи захисту даних, а також порівняно рішення для реалізації захищених мереж. Окремо було обґрунтовано вибір Cisco ASA та IPsec Site-to-Site VPN як оптимальних рішень для проекту.

У другому розділі було розроблено структуру корпоративної мережі, базуючись на трирівневій моделі Cisco, продемонстровано її схему та описано принципи роботи. Аналізовано потреби організації та визначено ключові компоненти мережі для забезпечення її надійності та безпеки.

У третьому розділі було реалізовано налаштування основного мережевого обладнання, зокрема маршрутизаторів, комутаторів та брандмауерів. Виконано базові налаштування, налаштовано безпеку через VPN, списки контролю доступу, Port Security та інші. Проведено тестування мережі, включаючи зв'язок між VLAN, роботу серверів та захищений обмін через VPN, що підтвердило стабільність і безпеку мережі.

Проведена кваліфікаційна робота успішно вирішила поставлені завдання. Було здійснено аналіз технологій і протоколів, які забезпечують захищений обмін інформацією, розроблено структуру корпоративної мережі з урахуванням її захищеності та функціональності, а також реалізовано налаштування основних компонентів мережі. Налаштована мережа забезпечує безпечний обмін даними між сегментами, стабільну взаємодію між робочими станціями та серверами, а також надійний зв'язок між віддаленими офісами через VPN. Проведене тестування підтвердило ефективність мережевої інфраструктури та її готовність до використання у корпоративному середовищі.

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				83
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Network security best practices.[Електронний ресурс] : Режим доступу: https://www.netwrix.com/network_security_best_practices.html
2. Коробейнікова Т. І., Захарченко С. М. Технології захисту локальних мереж на основі обладнання Cisco. – Львів: Видавництво Львівської політехніки, 2021. – 232 с.
3. Olifer N., Olifer V. Computer Networks: Principles, Technologies and Protocols for Network Design. – Wiley, 2005. – 1000 p.
4. 16 most common network protocols.[Електронний ресурс] : Режим доступу: <https://www.auvik.com/franklyit/blog/common-network-protocols/>
5. Види захисту. Захист комп'ютерних мереж.[Електронний ресурс] : Режим доступу: <https://magistrweb.wordpress.com/home-2/protection/>
6. The best VPN protocols and differences between VPN types.[Електронний ресурс] : Режим доступу: <https://nordvpn.com/uk/blog/protocols/>
7. Кулібачук І. П., Азарова А. О. Порівняння можливостей та продуктивності VPN-протоколів // Наукові праці Вінницького національного технічного університету, 2022.
8. Корпоративна мережа.[Електронний ресурс] : Режим доступу: <https://reporter.zp.ua/korporativna-merezha-l-uk.html>
9. Ієрархічна модель мережі від Cisco.[Електронний ресурс] : Режим доступу: <https://www.telesphera.net/blog/model-mereghi-vid-cisco.html>
10. What Is a DMZ Network and Why Would You Use It?[Електронний ресурс] : Режим доступу: <https://www.fortinet.com/resources/cyberglossary/what-is-dmz>
11. What is VLAN? How to Implement, Secure, and Manage.[Електронний ресурс] : Режим доступу: <https://www.zenarmor.com/docs/network-basics/what-is-vlan>
12. About SSH.[Електронний ресурс] : Режим доступу: <https://bitvise.com/ssh2>
13. Що таке DHCP? Простий посібник із розуміння призначення IP-адрес.[Електронний ресурс] : Режим доступу: <https://fiberroad.com/uk/resources/glossary/what-is-dhcp/>

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				84
Змн.	Арк.	№ докум.	Підпис	Дата		

14. What Is AAA Security?[Електронний ресурс] : Режим доступу: <https://www.fortinet.com/resources/cyberglossary/aaa-security>
15. What is a Syslog Server and How Does it Work?[Електронний ресурс] : Режим доступу: <https://www.whatsupgold.com/blog/what-is-a-syslog-server-and-how-does-it-work>
16. Cisco 2900 Series Integrated Services Routers Data Sheet.[Електронний ресурс] : Режим доступу: https://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data_sheet_c78_553896.html
17. Cisco 1800 Series Integrated Services Routers.[Електронний ресурс] : Режим доступу: <https://andovercg.com/datasheets/cisco-1841-router.pdf>
18. Мережевий екран Cisco ASA (ASA5506-K9).[Електронний ресурс] : Режим доступу: https://stack-systems.com.ua/mezhsetevoj-jekran-cisco-asa5506-k9?srsId=AfmBOoqj7TcYyKJD1B_dbTgNmjK-Wrd1mDjpZLMHAMmY0onehFDXbg1k
19. Комутатор Cisco Catalyst 2960 (WS-C2960-24TT-L). [Електронний ресурс] : Режим доступу: <https://stack-systems.com.ua/kommutator-cisco-ws-c2960-24tt-l?srsId=AfmBOooJ4otMSNYjFZZQZt7oeDOVhLCRHiT-lwHE6PQgPdU40cF5K3St2>
20. How to configure Router on a Stick. [Електронний ресурс] : Режим доступу: <https://networklessons.com/ip-routing/how-to-configure-router-on-a-stick>
21. Configure Network Address Translation and ACLs on an ASA Firewall. [Електронний ресурс] : Режим доступу: <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115904-asa-config-dmz-00.html>
22. Setting up Site-to-site IPSEC on Cisco Packet Tracer. [Електронний ресурс] : Режим доступу: <https://dingavinga.medium.com/setting-up-site-to-site-ipsec-on-cisco-packet-tracer-1349890ff3fb>

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				85
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				86
Змн.	Арк.	№ докум.	Підпис	Дата		

Схема розробленої корпоративної мережі

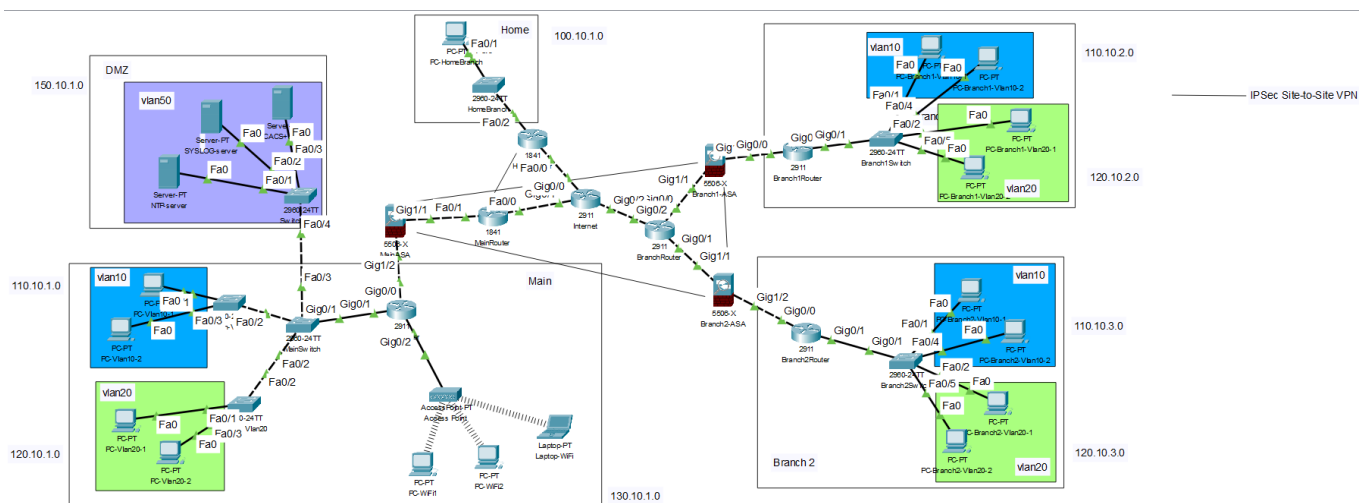


Рисунок А.1 – Схема розробленої корпоративної мережі

		Балаболов М. Г.		
		Воротніков В.В.		
Змн.	Арк.	№ докум.	Підпис	Дата

ККІКБ.КР.Б – 125 – 02 – ПЗ

Арк.

87

Адресація мережі

Таблиця Б. 1 –Адресація пристроїв мережі

Мережа/ Пристрій	Інтерфейс/Мереж- ний адаптер/Шлюз	ІР-адреса	Маска	Пре- фікс
Підмережа 1	-	10.10.1.0	255.255.255.252	/30
Підмережа 2	-	20.10.1.0	255.255.255.252	/30
Підмережа 3	-	30.10.1.0	255.255.255.252	/30
Підмережа 4	-	40.10.1.0	255.255.255.252	/30
Підмережа 5	-	50.10.1.0	255.255.255.252	/30
Підмережа 6	-	60.10.1.0	255.255.255.252	/30
Підмережа 7	-	70.10.1.0	255.255.255.252	/30
Підмережа 8	-	80.10.1.0	255.255.255.252	/30
Підмережа 9	-	90.10.1.0	255.255.255.252	/30
Підмережа 10	-	100.10.1.0	255.255.255.0	/24
Підмережа 11	-	110.10.1.0	255.255.255.0	/24
Підмережа 12	-	120.10.1.0	255.255.255.0	/24
Підмережа 13	-	130.10.1.0	255.255.255.0	/24
Підмережа 14	-	150.10.1.0	255.255.255.0	/24
Підмережа 15	-	110.10.2.0	255.255.255.0	/24
Підмережа 16	-	120.10.2.0	255.255.255.0	/24
Підмережа 17	-	110.10.3.0	255.255.255.0	/24
Підмережа 18	-	120.10.3.0	255.255.255.0	/24
Маршрутизатори				
Internet	Gig0/0	10.10.1.1	255.255.255.252	/30
	Gig0/1	20.10.1.1	255.255.255.252	/30
	Gig0/2	30.10.1.1	255.255.255.252	/30
HomeRouter	Fa0/0	10.10.1.2	255.255.255.252	/30
	Fa0/1	100.10.1.1	255.255.255.0	/24
MainRouter	Fa0/0	20.10.1.2	255.255.255.252	/30
	Fa0/1	40.10.1.1	255.255.255.252	/30

BranchRouter	Gig0/0	50.10.1.1	255.255.255.252	/30
	Gig0/1	60.10.1.1	255.255.255.252	/30
	Gig0/2	30.10.1.2	255.255.255.252	/30
Main-Router	Gig0/0	70.10.1.2	255.255.255.252	/30
	Gig0/1.10	110.10.1.1	255.255.255.0	/24
	Gig0/1.20	120.10.1.1	255.255.255.0	/24
	Gig0/1.50	150.10.1.1	255.255.255.0	/24
	Gig0/2	130.10.1.1	255.255.255.0	/24
Branch1Router	Gig0/0	80.10.1.2	255.255.255.252	/30
	Gig0/1.10	110.10.2.1	255.255.255.0	/24
	Gig0/1.20	120.10.2.1	255.255.255.0	/24
Branch2Router	Gig0/0	90.10.1.2	255.255.255.252	/30
	Gig0/1.10	110.10.3.1	255.255.255.0	/24
	Gig0/1.20	120.10.3.1	255.255.255.0	/24
Міжмережеві еркани				
MainASA	Gig1/1	40.10.1.2	255.255.255.252	/30
	Gig1/2	70.10.1.1	255.255.255.252	/30
Branch1-ASA	Gig1/1	50.10.1.2	255.255.255.252	/30
	Gig1/2	80.10.1.1	255.255.255.252	/30
Branch2-ASA	Gig1/1	60.10.1.2	255.255.255.252	/30
	Gig1/2	90.10.1.1	255.255.255.252	/30
Комутатори				
MainSwitch	Vlan10	110.10.1.2	255.255.255.0	/24
	Vlan20	120.10.1.2	255.255.255.0	/24
	Vlan50	150.10.1.2	255.255.255.0	/24
Switch-DMZ	Vlan50	150.10.1.3	255.255.255.0	/24
Switch-Vlan10	Vlan10	110.10.1.3	255.255.255.0	/24
Switch-Vlan20	Vlan20	120.10.1.3	255.255.255.0	/24
HomeBranch	Vlan1	100.10.1.2	255.255.255.0	/24
Branch1Switch	Vlan10	110.10.2.2	255.255.255.0	/24
	Vlan20	120.10.2.2	255.255.255.0	/24

Branch2Switch	Vlan10	110.10.3.2	255.255.255.0	/24
	Vlan20	120.10.3.2	255.255.255.0	/24
Сервери				
NTP-server	Мережний адаптер	150.10.1.5	255.255.255.0	/24
	Шлюз за замовч.	150.10.1.1	255.255.255.0	/24
SYSLOG-server	Мережний адаптер	150.10.1.6	255.255.255.0	/24
	Шлюз за замовч.	150.10.1.1	255.255.255.0	/24
TACACS+ server	Мережний адаптер	150.10.1.7	255.255.255.0	/24
	Шлюз за замовч.	150.10.1.1	255.255.255.0	/24
Робочі станції				
PC-Home-Branch	Мережний адаптер	DHCP		
	Шлюз за замовч.			
PC-Vlan10-1	Мережний адаптер	DHCP		
	Шлюз за замовч.			
PC-Vlan10-2	Мережний адаптер	DHCP		
	Шлюз за замовч.			
PC-Vlan20-1	Мережний адаптер	DHCP		
	Шлюз за замовч.			
PC-Vlan20-2	Мережний адаптер	DHCP		
	Шлюз за замовч.			
PC-WIFI1	Мережний адаптер	DHCP		
	Шлюз за замовч.			
PC-WIFI2	Мережний адаптер	DHCP		
	Шлюз за замовч.			
Laptop-WIFI	Мережний адаптер	DHCP		
	Шлюз за замовч.			
PC-Branch1-Vlan10-1	Мережний адаптер	DHCP		
	Шлюз за замовч.			
PC-Branch1-Vlan10-2	Мережний адаптер	DHCP		
	Шлюз за замовч.			
PC-Branch1-Vlan20-1	Мережний адаптер	DHCP		
	Шлюз за замовч.			

PC-Branch1- Vlan20-2	Мережний адаптер	DHCP
	Шлюз за замовч.	
PC-Branch2- Vlan10-1	Мережний адаптер	DHCP
	Шлюз за замовч.	
PC-Branch2- Vlan10-2	Мережний адаптер	DHCP
	Шлюз за замовч.	
PC-Branch2- Vlan20-1	Мережний адаптер	DHCP
	Шлюз за замовч.	
PC-Branch2- Vlan20-2	Мережний адаптер	DHCP
	Шлюз за замовч.	

Лістинг конфігурації пристроїв

```

Internet#sh r
Building configuration...

Current configuration : 944 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Internet
!
ip cef
no ipv6 cef
!
license udi pid CISCO2911/K9 sn FTX1524E6ZM-
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 10.10.1.1 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 20.10.1.1 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 30.10.1.1 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/2/0
no ip address
shutdown
!
interface GigabitEthernet0/3/0
no ip address
shutdown
!
interface Vlan1
no ip address

```

```

shutdown
!
router eigrp 1
network 10.10.1.0 0.0.0.3
network 20.10.1.0 0.0.0.3
network 30.10.1.0 0.0.0.3
!
ip classless
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
end

```

```

MainRouter#sh r
Building configuration...

Current configuration : 1619 bytes
!
version 12.4
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname MainRouter
!
enable secret 5 $1$mERr$6NDOFPHHdaxTFi0e5Smkj/
!
aaa new-model
!
aaa authentication login default group tacacs+ local
!
clock timezone GMT 2
!
ip cef
no ipv6 cef
!

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				92
Змн.	Арк.	№ докум.	Підпис	Дата		

```

username TacacsMark privilege 15 secret 5
$1$mERr$6NDOFPHHdaxTFi0e5Smkj/
!
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
!
crypto isakmp key markkey address 10.10.1.2
!
crypto ipsec transform-set main-home esp-aes 256 esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
set peer 10.10.1.2
set pfs group5
set security-association lifetime seconds 86400
set transform-set main-home
match address 100
!
ip ssh version 2
ip ssh time-out 30
ip domain-name my.net
!
!
spanning-tree mode pvst
!
interface FastEthernet0/0
ip address 20.10.1.2 255.255.255.252
duplex auto
speed auto
crypto map VPN-MAP
!
interface FastEthernet0/1
ip address 40.10.1.1 255.255.255.252
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router eigrp 1
network 20.10.1.0 0.0.0.3
network 40.10.1.0 0.0.0.3
auto-summary
!

```

```

ip classless
!
ip flow-export version 9
!
access-list 100 permit ip 130.10.1.0 0.0.0.255 100.10.1.0
0.0.0.255
!
tacacs-server host 150.10.1.7 key tacacspass
!
logging trap debugging
logging 150.10.1.6
line con 0
login authentication default
!
line aux 0
!
line vty 0 4
!
ntp authentication-key 201102 md5
082C4D5C021D0C071E040105 7
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
End

HomeRouter#sh r
Building configuration...

Current configuration : 1774 bytes
!
version 12.4
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname HomeRouter
!
enable secret 5 $1$mERr$6NDOFPHHdaxTFi0e5Smkj/
!
ip dhcp excluded-address 100.10.1.1 100.10.1.2
!
ip dhcp pool HomeBranch1
network 100.10.1.0 255.255.255.0
default-router 100.10.1.1
domain-name my.net
!

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

```

aaa new-model
!
aaa authentication login default group tacacs+ local
!
clock timezone GMT 2
!
ip cef
no ipv6 cef
!
username TacacsMark privilege 15 secret 5
$1$mERr$6NDOFPHHdaxTFi0e5Smkj/
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
!
crypto isakmp key markkey address 20.10.1.2
!
crypto ipsec transform-set home-main esp-aes 256 esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
set peer 20.10.1.2
set pfs group5
set security-association lifetime seconds 86400
set transform-set home-main
match address 100
!
ip ssh version 2
ip ssh time-out 30
ip domain-name my.net
!
spanning-tree mode pvst
!
interface FastEthernet0/0
ip address 10.10.1.2 255.255.255.252
duplex auto
speed auto
crypto map VPN-MAP
!
interface FastEthernet0/1
ip address 100.10.1.1 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address

```

```

shutdown
!
router eigrp 1
network 10.10.1.0 0.0.0.3
network 100.10.1.0 0.0.0.255
auto-summary
!
ip classless
!
ip flow-export version 9
!
access-list 100 permit ip 100.10.1.0 0.0.0.255 130.10.1.0
0.0.0.255
!
tacacs-server host 150.10.1.7 key tacacspass
!
logging trap debugging
logging 150.10.1.6
line con 0
login authentication default
!
line aux 0
!
line vty 0 4
!
ntp authentication-key 201102 md5
082C4D5C021D0C071E040105 7
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
End

BranchRouter#sh r
Building configuration...

Current configuration : 1456 bytes
!
version 15.1
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname BranchRouter
!
enable secret 5 $1$mERr$6NDOFPHHdaxTFi0e5Smkj/
!

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				92
Змн.	Арк.	№ докум.	Підпис	Дата		

```

aaa new-model
!
aaa authentication login default group tacacs+ local
!
clock timezone GMT 2
!
ip cef
no ipv6 cef
!
username TacacsMark privilege 15 secret 5
$1$mERr$6NDOFPHHdaxTFi0e5Smkj/
!
license udi pid CISCO2911/K9 sn FTX1524D42E-
!
ip ssh version 2
ip ssh time-out 30
ip domain-name my.net
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 50.10.1.1 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 60.10.1.1 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 30.10.1.2 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/2/0
no ip address
shutdown
!
interface GigabitEthernet0/3/0
no ip address
shutdown
!
interface Vlan1
no ip address
shutdown
!
!
router eigrp 1
network 30.10.1.0 0.0.0.3
network 50.10.1.0 0.0.0.3
network 60.10.1.0 0.0.0.3
!
ip classless
!
ip flow-export version 9
!
tacacs-server host 150.10.1.7 key tacacspass
!
logging trap debugging
logging 150.10.1.6
line con 0
login authentication default
!
line aux 0
!
line vty 0 4
!
ntp authentication-key 201102 md5
082C4D5C021D0C071E040105 7
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
End

MainASA#show run
: Saved
:
ASA Version 9.6(1)
!
hostname MainASA
names
!
interface GigabitEthernet1/1
nameif outside
security-level 0
ip address 40.10.1.2 255.255.255.252
!
interface GigabitEthernet1/2
nameif inside
security-level 100
ip address 70.10.1.1 255.255.255.252
!

```

		Балаболов М. Г.			ККИКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				93
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface GigabitEthernet1/3
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/4
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/5
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/6
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/7
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/8
no nameif
no security-level
no ip address
shutdown
!
interface Management1/1
management-only
no nameif
no security-level
no ip address
shutdown
!
object network LAN-VLAN10
subnet 110.10.1.0 255.255.255.0
nat (inside,outside) dynamic interface
object network LAN-VLAN10-remote1

```

```

subnet 110.10.2.0 255.255.255.0
object network LAN-VLAN10-remote2
subnet 110.10.3.0 255.255.255.0
object network LAN-VLAN20
subnet 120.10.1.0 255.255.255.0
nat (inside,outside) dynamic interface
object network LAN-VLAN20-remote1
subnet 120.10.2.0 255.255.255.0
object network LAN-VLAN20-remote2
subnet 120.10.3.0 255.255.255.0
object network LAN-WIFI
subnet 130.10.1.0 255.255.255.0
nat (inside,outside) dynamic interface
object network LAN_DMZ
subnet 150.10.1.0 255.255.255.0
nat (inside,outside) dynamic interface
!
route outside 0.0.0.0 0.0.0.0 40.10.1.1 1
!
access-list TRAFEGO-VPN1 extended permit ip 110.10.1.0
255.255.255.0 110.10.2.0 255.255.255.0
access-list TRAFEGO-VPN1 extended permit ip 120.10.1.0
255.255.255.0 120.10.2.0 255.255.255.0
access-list TRAFEGO-VPN1 extended permit ip 150.10.1.0
255.255.255.0 110.10.2.0 255.255.255.0
access-list TRAFEGO-VPN1 extended permit ip 150.10.1.0
255.255.255.0 120.10.2.0 255.255.255.0
access-list TRAFEGO-VPN2 extended permit ip 110.10.1.0
255.255.255.0 110.10.3.0 255.255.255.0
access-list TRAFEGO-VPN2 extended permit ip 120.10.1.0
255.255.255.0 120.10.3.0 255.255.255.0
access-list TRAFEGO-VPN2 extended permit ip 150.10.1.0
255.255.255.0 110.10.3.0 255.255.255.0
access-list TRAFEGO-VPN2 extended permit ip 150.10.1.0
255.255.255.0 120.10.3.0 255.255.255.0
access-list RES extended permit ip object LAN-VLAN10 any
access-list RES extended permit ip object LAN-VLAN20 any
access-list RES extended permit ip object LAN-WIFI any
access-list RES extended permit ip object LAN_DMZ any
access-list RES extended permit icmp object LAN-WIFI
100.10.1.0 255.255.255.0
access-list ENTRADA extended permit icmp object LAN-
VLAN10-remote1 object LAN-VLAN10
access-list ENTRADA extended permit icmp object LAN-
VLAN10-remote2 object LAN-VLAN10
access-list ENTRADA extended permit icmp object LAN-
VLAN20-remote1 object LAN-VLAN20

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				94
Змн.	Арк.	№ докум.	Підпис	Дата		

```

access-list ENTRADA extended permit icmp object LAN-
VLAN20-remote2 object LAN-VLAN20
access-list ENTRADA extended permit icmp 100.10.1.0
255.255.255.0 object LAN-WIFI
access-list ENTRADA extended permit ip any object
LAN_DMZ
access-list ENTRADA extended deny ip any any
!
access-group RES out interface inside
access-group ENTRADA in interface outside
!
ntp authentication-key 201102 md5 *****
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
class-map inspection_default
match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect tftp
!
telnet timeout 5
ssh timeout 5
!
crypto ipsec ikev1 transform-set IPSEC esp-aes esp-sha-hmac
!
crypto map VPN 1 match address TRAFEGO-VPN1
crypto map VPN 1 set peer 50.10.1.2
crypto map VPN 1 set ikev1 transform-set IPSEC
crypto map VPN interface outside
crypto map VPN 2 match address TRAFEGO-VPN2
crypto map VPN 2 set peer 60.10.1.2
crypto map VPN 2 set ikev1 transform-set IPSEC
crypto map VPN interface outside
crypto ikev1 enable outside
crypto ikev1 policy 1
encr aes
authentication pre-share
group 5
!
crypto ikev1 policy 2

```

```

encr aes
authentication pre-share
group 5
!
tunnel-group 50.10.1.2 type ipsec-l2l
tunnel-group 50.10.1.2 ipsec-attributes
ikev1 pre-shared-key SENHA
tunnel-group 60.10.1.2 type ipsec-l2l
tunnel-group 60.10.1.2 ipsec-attributes
ikev1 pre-shared-key SENHA
!
router eigrp 1
eigrp router-id 1.1.1.1
network 40.10.1.0 0.0.0.3
network 70.10.1.0 0.0.0.3
!
MainASA#

Branch1-ASA#show run
: Saved
:
ASA Version 9.6(1)
!
hostname Branch1-ASA
names
!
interface GigabitEthernet1/1
nameif outside
security-level 0
ip address 50.10.1.2 255.255.255.252
!
interface GigabitEthernet1/2
nameif inside
security-level 100
ip address 80.10.1.1 255.255.255.252
!
interface GigabitEthernet1/3
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/4
no nameif
no security-level
no ip address

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				95
Змн.	Арк.	№ докум.	Підпис	Дата		

```

shutdown
!
interface GigabitEthernet1/5
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/6
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/7
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/8
no nameif
no security-level
no ip address
shutdown
!
interface Management1/1
management-only
no nameif
no security-level
no ip address
shutdown
!
object network LAN-VLAN10
subnet 110.10.2.0 255.255.255.0
nat (inside,outside) dynamic interface
object network LAN-VLAN10-remote1
subnet 110.10.1.0 255.255.255.0
object network LAN-VLAN10-remote2
subnet 110.10.3.0 255.255.255.0
object network LAN-VLAN20
subnet 120.10.2.0 255.255.255.0
nat (inside,outside) dynamic interface
object network LAN-VLAN20-remote1
subnet 120.10.1.0 255.255.255.0
object network LAN-VLAN20-remote2
subnet 120.10.3.0 255.255.255.0

```

```

object network LAN_DMZ
subnet 150.10.1.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 50.10.1.1 1
!
access-list TRAFEGO-VPN1 extended permit ip 110.10.2.0
255.255.255.0 110.10.1.0 255.255.255.0
access-list TRAFEGO-VPN1 extended permit ip 120.10.2.0
255.255.255.0 120.10.1.0 255.255.255.0
access-list TRAFEGO-VPN1 extended permit ip 110.10.2.0
255.255.255.0 150.10.1.0 255.255.255.0
access-list TRAFEGO-VPN1 extended permit ip 120.10.2.0
255.255.255.0 150.10.1.0 255.255.255.0
access-list TRAFEGO-VPN2 extended permit ip 110.10.2.0
255.255.255.0 110.10.3.0 255.255.255.0
access-list TRAFEGO-VPN2 extended permit ip 120.10.2.0
255.255.255.0 120.10.3.0 255.255.255.0
access-list RES extended permit ip object LAN-VLAN10 any
access-list RES extended permit ip object LAN-VLAN20 any
access-list ENTRADA extended permit icmp object LAN-
VLAN10-remote1 object LAN-VLAN10
access-list ENTRADA extended permit icmp object LAN-
VLAN10-remote2 object LAN-VLAN10
access-list ENTRADA extended permit icmp object LAN-
VLAN20-remote1 object LAN-VLAN20
access-list ENTRADA extended permit icmp object LAN-
VLAN20-remote2 object LAN-VLAN20
access-list ENTRADA extended permit ip object LAN_DMZ
any
access-list ENTRADA extended deny ip any any
!
access-group RES out interface inside
access-group ENTRADA in interface outside
!
ntp authentication-key 201102 md5 *****
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
class-map inspection_default
match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				96
Змн.	Арк.	№ докум.	Підпис	Дата		

```

inspect ftp
inspect tftp
!
service-policy global_policy global
!
telnet timeout 5
ssh timeout 5
!
crypto ipsec ikev1 transform-set IPSEC esp-aes esp-sha-hmac
!
crypto map VPN 1 match address TRAFEGO-VPN1
crypto map VPN 1 set peer 40.10.1.2
crypto map VPN 1 set ikev1 transform-set IPSEC
crypto map VPN interface outside
crypto map VPN 2 match address TRAFEGO-VPN2
crypto map VPN 2 set peer 60.10.1.2
crypto map VPN 2 set ikev1 transform-set IPSEC
crypto map VPN interface outside
crypto ikev1 enable outside
crypto ikev1 policy 1
encr aes
authentication pre-share
group 5
!
tunnel-group 40.10.1.2 type ipsec-l2l
tunnel-group 40.10.1.2 ipsec-attributes
ikev1 pre-shared-key SENHA
tunnel-group 60.10.1.2 type ipsec-l2l
tunnel-group 60.10.1.2 ipsec-attributes
ikev1 pre-shared-key SENHA
!
router eigrp 1
eigrp router-id 2.2.2.2
network 50.10.1.0 0.0.0.3
network 80.10.1.0 0.0.0.3
!
Branch1-ASA#

Branch2-ASA#show run
: Saved
:
ASA Version 9.6(1)
!
hostname Branch2-ASA
domain-name my.net
names

```

```

!
interface GigabitEthernet1/1
nameif outside
security-level 0
ip address 60.10.1.2 255.255.255.252
!
interface GigabitEthernet1/2
nameif inside
security-level 100
ip address 90.10.1.1 255.255.255.252
!
interface GigabitEthernet1/3
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/4
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/5
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/6
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/7
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/8
no nameif
no security-level
no ip address
shutdown
!

```

		Балаболов М. Г.			ККИКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				97
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Management1/1
management-only
no nameif
no security-level
no ip address
shutdown
!
object network LAN-VLAN10
subnet 110.10.3.0 255.255.255.0
nat (inside,outside) dynamic interface
object network LAN-VLAN10-remote1
subnet 110.10.1.0 255.255.255.0
object network LAN-VLAN10-remote2
subnet 110.10.2.0 255.255.255.0
object network LAN-VLAN20
subnet 120.10.3.0 255.255.255.0
nat (inside,outside) dynamic interface
object network LAN-VLAN20-remote1
subnet 120.10.1.0 255.255.255.0
object network LAN-VLAN20-remote2
subnet 120.10.2.0 255.255.255.0
object network LAN_DMZ
subnet 150.10.1.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 60.10.1.1 1
!
access-list TRAFEGO-VPN1 extended permit ip 110.10.3.0
255.255.255.0 110.10.1.0 255.255.255.0
access-list TRAFEGO-VPN1 extended permit ip 120.10.3.0
255.255.255.0 120.10.1.0 255.255.255.0
access-list TRAFEGO-VPN1 extended permit ip 110.10.3.0
255.255.255.0 150.10.1.0 255.255.255.0
access-list TRAFEGO-VPN1 extended permit ip 120.10.3.0
255.255.255.0 150.10.1.0 255.255.255.0
access-list TRAFEGO-VPN2 extended permit ip 110.10.3.0
255.255.255.0 110.10.2.0 255.255.255.0
access-list TRAFEGO-VPN2 extended permit ip 120.10.3.0
255.255.255.0 120.10.2.0 255.255.255.0
access-list RES extended permit ip object LAN-VLAN10 any
access-list RES extended permit ip object LAN-VLAN20 any
access-list ENTRADA extended permit icmp object LAN-
VLAN10-remote1 object LAN-VLAN10
access-list ENTRADA extended permit icmp object LAN-
VLAN10-remote2 object LAN-VLAN10
access-list ENTRADA extended permit icmp object LAN-
VLAN20-remote1 object LAN-VLAN20

```

```

access-list ENTRADA extended permit icmp object LAN-
VLAN20-remote2 object LAN-VLAN20
access-list ENTRADA extended permit ip object LAN_DMZ
any
access-list ENTRADA extended deny ip any any
!
access-group RES out interface inside
access-group ENTRADA in interface outside
!
ntp authentication-key 201102 md5 *****
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
class-map inspection_default
match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect tftp
!
service-policy global_policy global
!
telnet timeout 5
ssh timeout 5
!
crypto ipsec ikev1 transform-set IPSEC esp-aes esp-sha-hmac
!
crypto map VPN 1 match address TRAFEGO-VPN1
crypto map VPN 1 set peer 40.10.1.2
crypto map VPN 1 set ikev1 transform-set IPSEC
crypto map VPN interface outside
crypto map VPN 2 match address TRAFEGO-VPN2
crypto map VPN 2 set peer 50.10.1.2
crypto map VPN 2 set ikev1 transform-set IPSEC
crypto map VPN interface outside
crypto ikev1 enable outside
crypto ikev1 policy 1
encr aes
authentication pre-share
group 5
!
tunnel-group 40.10.1.2 type ipsec-l2l

```

		Балаболов М. Г.			ККИКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				98
Змн.	Арк.	№ докум.	Підпис	Дата		

```

tunnel-group 40.10.1.2 ipsec-attributes
ikev1 pre-shared-key SENHA
tunnel-group 50.10.1.2 type ipsec-l2l
tunnel-group 50.10.1.2 ipsec-attributes
ikev1 pre-shared-key SENHA
!
router eigrp 1
eigrp router-id 3.3.3.3
network 60.10.1.0 0.0.0.3
network 90.10.1.0 0.0.0.3
!
Branch2-ASA#

Main-Router#sh r
Building configuration...

Current configuration : 2227 bytes
!
version 15.1
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname Main-Router
!
enable secret 5 $1$mERr$6NDOFPHHdaxTFi0e5Smkj/
!
ip dhcp excluded-address 110.10.1.1 110.10.1.4
ip dhcp excluded-address 120.10.1.1 120.10.1.4
ip dhcp excluded-address 130.10.1.1
!
ip dhcp pool MainRouter1
network 110.10.1.0 255.255.255.0
default-router 110.10.1.1
domain-name my.net
ip dhcp pool MainRouter2
network 120.10.1.0 255.255.255.0
default-router 120.10.1.1
domain-name my.net
ip dhcp pool Main3
network 130.10.1.0 255.255.255.0
default-router 130.10.1.1
domain-name my.net
!
!
aaa new-model

```

```

!
aaa authentication login default group tacacs+ local
!
clock timezone GMT 2
!
no ip cef
no ipv6 cef
!
username TacacsMark privilege 15 secret 5
$1$mERr$6NDOFPHHdaxTFi0e5Smkj/
!
license udi pid CISCO2911/K9 sn FTX1524BW6T-
!
ip ssh version 2
ip ssh time-out 30
ip domain-name my.net
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 70.10.1.2 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 110.10.1.1 255.255.255.0
!
interface GigabitEthernet0/1.20
encapsulation dot1Q 20
ip address 120.10.1.1 255.255.255.0
!
interface GigabitEthernet0/1.50
encapsulation dot1Q 50
ip address 150.10.1.1 255.255.255.0
!
interface GigabitEthernet0/2
ip address 130.10.1.1 255.255.255.0
duplex auto
speed auto
!

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				99
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface GigabitEthernet0/2/0
no ip address
shutdown
!
interface GigabitEthernet0/3/0
no ip address
shutdown
!
interface Vlan1
no ip address
shutdown
!
router eigrp 1
network 110.10.1.0 0.0.0.255
network 120.10.1.0 0.0.0.255
network 130.10.1.0 0.0.0.255
network 150.10.1.0 0.0.0.255
network 70.10.1.0 0.0.0.3
!
ip classless
!
ip flow-export version 9
!
tacacs-server host 150.10.1.7 key tacacspass
!
logging trap debugging
logging 150.10.1.6
line con 0
login authentication default
!
line aux 0
!
line vty 0 4
!
ntp authentication-key 201102 md5
082C4D5C021D0C071E040105 7
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
End

Branch1Router#sh r
Building configuration...

Current configuration : 1504 bytes
!

```

```

version 15.1
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname Branch1Router
!
enable secret 5 $1$mERr$6NDOFPHHdaxTFi0e5Smkj/
!
aaa new-model
!
aaa authentication login default group tacacs+ local
!
clock timezone GMT 2
!
no ip cef
no ipv6 cef
!
username TacacsMark privilege 15 secret 5
$1$mERr$6NDOFPHHdaxTFi0e5Smkj/
!
license udi pid CISCO2911/K9 sn FTX15242GEA-
!
ip ssh version 2
ip ssh time-out 30
ip domain-name my.net
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 80.10.1.2 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 110.10.2.1 255.255.255.0
!
interface GigabitEthernet0/1.20
encapsulation dot1Q 20
ip address 120.10.2.1 255.255.255.0
!

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				100
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
router eigrp 1
network 80.10.1.0 0.0.0.3
network 110.10.2.0 0.0.0.255
network 120.10.2.0 0.0.0.255
!
ip classless
!
ip flow-export version 9
!
tacacs-server host 150.10.1.7 key tacacspass
!
logging trap debugging
logging 150.10.1.6
line con 0
login authentication default
!
line aux 0
!
line vty 0 4
!
ntp authentication-key 201102 md5
082C4D5C021D0C071E040105 7
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
End

Branch2Router#sh r
Building configuration...

Current configuration : 1501 bytes
!
version 15.1
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption

!
hostname Branch2Router
!
enable secret 5 $1$mERr$6NDOFPHHdaxTFi0e5Smkj/
!
aaa new-model
!
aaa authentication login default group tacacs+ local
!
clock timezone GMT 2
!
ip cef
no ipv6 cef
!
username TacacsMark privilege 15 secret 5
$1$mERr$6NDOFPHHdaxTFi0e5Smkj/
!
license udi pid CISCO2911/K9 sn FTX15243E42-
!
ip ssh version 2
ip ssh time-out 30
ip domain-name my.net
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 90.10.1.2 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 110.10.3.1 255.255.255.0
!
interface GigabitEthernet0/1.20
encapsulation dot1Q 20
ip address 120.10.3.1 255.255.255.0
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				101
Змн.	Арк.	№ докум.	Підпис	Дата		

```

shutdown
!
interface Vlan1
no ip address
shutdown
!
router eigrp 1
network 90.10.1.0 0.0.0.3
network 110.10.3.0 0.0.0.255
network 120.10.3.0 0.0.0.255
!
ip classless
!
ip flow-export version 9
!
tacacs-server host 150.10.1.7 key tacacspass
!
logging trap debugging
logging 150.10.1.6
line con 0
login authentication default
!
line aux 0
!
line vty 0 4
!
ntp authentication-key 201102 md5
082C4D5C021D0C071E040105 7
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
End

HomeBranch#sh r
Building configuration...

Current configuration : 1367 bytes
!
version 15.0
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname HomeBranch
!
clock timezone GMT 2
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 000A.F3E2.C58E
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				102
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 100.10.1.2 255.255.255.0
!
logging trap debugging
logging 150.10.1.6
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
End

```

```

Main-Switch#sh r
Building configuration...

```

```

Current configuration : 1484 bytes
!
version 15.0
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname Main-Switch
!
clock timezone GMT 2
!
spanning-tree mode pvst

```

```

spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport mode trunk
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				103
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
switchport mode trunk
!
interface GigabitEthernet0/2
switchport mode access
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
ip address 110.10.1.2 255.255.255.0
!
interface Vlan20
ip address 120.10.1.2 255.255.255.0
!
interface Vlan50
ip address 150.10.1.2 255.255.255.0
!
logging trap debugging
logging 150.10.1.6
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
End

Switch-DMZ#sh r
Building configuration...

Current configuration : 1854 bytes
!
version 15.0

```

```

service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname Switch-DMZ
!
clock timezone GMT 2
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 50
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0060.5C36.AD7C
!
interface FastEthernet0/2
switchport access vlan 50
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0001.C97D.0615
!
interface FastEthernet0/3
switchport access vlan 50
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0002.1653.6B4C
!
interface FastEthernet0/4
switchport mode trunk
!
interface FastEthernet0/5
switchport access vlan 50
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				104
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan50
ip address 150.10.1.3 255.255.255.0
!
logging trap debugging
logging 150.10.1.6
!
line con 0
!
line vty 0 4
login

line vty 5 15
login
!
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
End

Switch-Vlan10#sh r
Building configuration...

Current configuration : 1624 bytes
!
version 15.0
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname Switch-Vlan10
!
clock timezone GMT 2
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 10
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0001.4262.A208
!
interface FastEthernet0/2
!
interface FastEthernet0/3
switchport access vlan 10
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0009.7CD1.DC15
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				105
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
ip address 110.10.1.3 255.255.255.0

```

```

!
logging trap debugging
logging 150.10.1.6
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
End

Switch-Vlan20#sh r
Building configuration...

Current configuration : 1624 bytes
!
version 15.0
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname Switch-Vlan20
!
clock timezone GMT 2
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 20
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0000.0CAC.D1D8
!
interface FastEthernet0/2
!
interface FastEthernet0/3
switchport access vlan 20
switchport mode access
switchport port-security

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				106
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport port-security mac-address sticky
switchport port-security mac-address sticky 0001.9780.7666
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!

```

```

interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan20
ip address 120.10.1.3 255.255.255.0
!
logging trap debugging
logging 150.10.1.6
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
End

Branch1Switch#sh r
Building configuration...

Current configuration : 2103 bytes
!
version 15.0
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname Branch1Switch
!
clock timezone GMT 2
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 10
switchport mode access
switchport port-security
switchport port-security mac-address sticky

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				107
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport port-security mac-address sticky 000A.F390.E4C1
!
interface FastEthernet0/2
switchport access vlan 20
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0060.3E3B.C5EC
!
interface FastEthernet0/3
switchport mode access
shutdown
!
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 00D0.BA00.5BBB
!
interface FastEthernet0/5
switchport access vlan 20
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0004.9AAC.0E89
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!

```

```

interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
ip address 110.10.2.2 255.255.255.0
!
interface Vlan20
ip address 120.10.2.2 255.255.255.0
!
logging trap debugging
logging 150.10.1.6
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
End

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				108
Змн.	Арк.	№ докум.	Підпис	Дата		

Branch2Switch#sh r
Building configuration...

Current configuration : 2103 bytes

!

version 15.0

service timestamps log datetime msec

service timestamps debug datetime msec

no service password-encryption

!

hostname Branch2Switch

!

clock timezone GMT 2

!

spanning-tree mode pvst

spanning-tree extend system-id

!

interface FastEthernet0/1

switchport access vlan 10

switchport mode access

switchport port-security

switchport port-security mac-address sticky

switchport port-security mac-address sticky 00D0.BA65.BA96

!

interface FastEthernet0/2

switchport access vlan 20

switchport mode access

switchport port-security

switchport port-security mac-address sticky

switchport port-security mac-address sticky 00D0.D34D.C36D

!

interface FastEthernet0/3

switchport mode access

shutdown

!

interface FastEthernet0/4

switchport access vlan 10

switchport mode access

switchport port-security

switchport port-security mac-address sticky

switchport port-security mac-address sticky 0001.C745.AB8E

!

interface FastEthernet0/5

switchport access vlan 20

switchport mode access

switchport port-security

switchport port-security mac-address sticky

switchport port-security mac-address sticky 0060.3E58.2299

!

interface FastEthernet0/6

!

interface FastEthernet0/7

!

interface FastEthernet0/8

!

interface FastEthernet0/9

!

interface FastEthernet0/10

!

interface FastEthernet0/11

!

interface FastEthernet0/12

!

interface FastEthernet0/13

!

interface FastEthernet0/14

!

interface FastEthernet0/15

!

interface FastEthernet0/16

!

interface FastEthernet0/17

!

interface FastEthernet0/18

!

interface FastEthernet0/19

!

interface FastEthernet0/20

!

interface FastEthernet0/21

!

interface FastEthernet0/22

!

interface FastEthernet0/23

!

interface FastEthernet0/24

!

interface GigabitEthernet0/1

switchport mode trunk

!

interface GigabitEthernet0/2

!

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				109
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Vlan1
no ip address
shutdown
!
interface Vlan10
ip address 110.10.3.2 255.255.255.0
!
interface Vlan20
ip address 120.10.3.2 255.255.255.0
!
logging trap debugging
logging 150.10.1.6
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
ntp trusted-key 201102
ntp server 150.10.1.5 key 201102
!
end

```

		Балаболов М. Г.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Воротніков В.В.				110
Змн.	Арк.	№ докум.	Підпис	Дата		