

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 захищеного безпроводного сегменту
мережної інфраструктури комерційного підприємства»

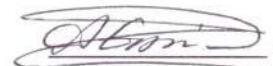
Виконав студент 4-го курсу групи КІ-4
спеціальності 123 «Комп'ютерна інженерія»

 Федір Рачкінда

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

 Юрій Россінський

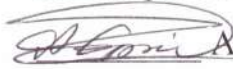
Рецензент завідувач кафедри КІ та КБ, к.т.н., доцент

 Андрій Єфіменко

Житомир – 2022

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
 Андрій Єфіменко

1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Рачкинда Федір Федорович

Тема роботи: «Проект захищеного безпроводного сегменту мережної інфраструктури комерційного підприємства»

затверджена Наказом університету від 1 березня 2022 р. № 127/с

Термін здачі студентом закінченої роботи 10 червня 2022 р.

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

Об'єктом дослідження є захищеність даних в мережі підприємства та визначення доступності даних для користувачів вільного простору.

Обладнання та програмне забезпечення:

1. Cisco Packet Tracer
2. Cisco ASA 5505, Маршрутизатори 1841, точка доступу, сервери.

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Морозов Д.С.	02.03.22	 02.03.22
2	Морозов Д.С.	14.04.22	 14.04.22
3	Морозов Д.С.	08.05.22	 08.05.22

Студент  Федір Рачкинда

Керівник  Юрій Россінський

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	02.03.22 - 11.03.22	Виконано
2	Аналіз літературних джерел	12.03.22 – 01.04.22	Виконано
3	Розробка структурної моделі	02.04.22 – 13.04.22	Виконано
4	Розрахунок параметрів адресації	14.04.22 – 26.04.22	Виконано
5	Вибір технології для реалізації	27.04.22 – 07.05.22	Виконано
6	Налаштування захищеної мережі	08.05.22 – 25.05.22	Виконано
7	Перевірка працездатності	26.05.22 – 02.06.22	Виконано
8	Оформлення записки	02.06.22 – 20.06.22	Виконано
9	Оформлення презентації	21.06.22 – 26.06.22	Виконано
10	Захист		

Студент  Федір Рачкінда

Керівник  Юрій Россінський

АНОТАЦІЯ

Кваліфікаційна робота у вигляді проекту мережі з використанням бездротових технологій, DMZ, VPN виконана та містить 44 сторінки, 24 рисунки, одну таблицю та 22 найменування у списках використаних джерел що розміщені на двох сторінках.

Метою випускної кваліфікаційної роботи є розробка проекту мережі з використанням захищеного бездротового сегменту.

Було визначено завдання для побудови захищеного сегменту використовувати VPN, теоретичні відомості DMZ було проаналізовано та розглянуто особливості використання бездротових пристроїв. Також було проведено результати тестування цих пристроїв.

Ключові слова: DMZ, NAT, OSPF, VPN, ASA.

					КІК.КР.Б - 123 - 18 - ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект захищеного безпроводного сегменту мережної інфраструктури комерційного підприємства	Літ.	Арк.	Аркушів
Розроб.		Рачкінда Ф.Ф.		10.06				
Керівник		Росієвський Ю.М.		20.06				
Реценз.		Сфіменко А.А.		20.06		ФІКТ, Гр. КІ-4		
Н. контр.		Росієвський Ю.М.		20.06				
Затверд.		Сфіменко А.А.		20.06				

ANNOTATION

Qualification work in the form of a network project using wireless technologies, DMZ, VPN is performed and contains 44 pages, 24 figures, one table and 22 names in the lists of used sources located on two pages.

The purpose of the final qualification work is to develop a network project using a secure wireless segment.

The task for building a secure segment using VPN was defined, DMZ theoretical information was analyzed and the peculiarities of using wireless devices were considered. The test results of these devices were also performed.

Keywords: DMZ, NAT, OSPF, VPN, ASA.

		Рачкинда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росієнський Ю.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ МЕРЕЖІ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ БЕЗДРОТОВОГО З'ЄДНАННЯ ТА ТЕХНОГОЛІЯМИ DMZ, VPN	9
1.1 Теоретичні відомості функціонування технологій FastEthernet та коротні відомості про бездротовий маршрутизатор.....	9
1.2 Теоретичні відомості про демілітаризовану зону.....	11
1.3 Загальні відомості VPN	13
1.4 Теоретична інформація про wi-fi в соho офісах та способи організації бездротової мережі.....	15
РОЗДІЛ 2 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ.....	19
2.1 Розробка комп'ютерної мережі.....	19
2.2 Розробка схеми адресації мережі.....	21
2.3 Функціонал та налаштування міжмережного екрану.....	22
2.4 Вибір обладнання для організації роботи мережі.....	24
РОЗДІЛ 3 НАЛАГОДЖЕННЯ ОБЛАДНАННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ ПІДПРИЄМСТВА	28
3.1 Налагодження обладнання мережі	28
3.2 Перевірка працездатності мережі	33
ВИСНОВКИ.....	36
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	37
ДОДАТКИ.....	39

		Рачкінда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – Програмне Забезпечення

DMZ - Demilitarized Zone

VPN - Virtual Private Network

IPsec – IP Security

FTP - File Transfer Protocol

		Рачкинда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росієнський Ю.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Важливу роль в нашому житті відіграє комунікабельність. Підтримувати зв'язок з оточуючими нам допомагає Інтернет. Нікому не секрет що глобальна мережа розвивається досить швидко тому найближчим часом вона стане головною серед комунікаційних мереж. Для того щоб втілювати нові ідеї в життя компанії все частіше використовують мережі а для швидкого підключення використовують бездротові з'єднання.

Метою кваліфікаційної роботи є розробка корпоративної мережі підприємства використовуючи безпроводне з'єднання.

Визначена мета обумовлює наступні завдання:

- Теоретичний аналіз для будування мережі
- Створення топології мережі
- Вибір та налаштування певного обладнання
- Перевірка на пропускатність мережі

Об'єктом дослідження є продемонструвати переваги бездротового з'єднання та захищеності такої мережі.

Предметом дослідження є створення офісного мережі яка буде містити гостьову підмережу та філіал та для захисту даних використовуватиметься VPN.

У процесі виконання кваліфікаційної роботи було розроблено проект мережі комерційного підприємства яка містить бездротовий сегмент, DMZ та VPN для захисту та цілісності інформації.

		Рачкинда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росієвський Ю.М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ МЕРЕЖІ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ БЕЗДРОТОВОГО З'ЄДНАННЯ ТА ТЕХНОГОЛІЯМИ DMZ, VPN

1.1 Теоретичні відомості функціонування технологій FastEthernet та коротні відомості про бездротовий маршрутизатор

FastEthernet відноситься до набору мережевих стандартів для швидкостей передачі даних, які перевищують початкову швидкість Ethernet 10 мегабіт на секунду (Мбіт/с). Програмне та апаратне забезпечення, які підтримують FastEthernet, можуть забезпечити швидкість до 100 Мбіт/с. Оригінальний Ethernet (іноді називають 10Base-T) для передачі даних в базовій смузі 10 Мбіт/с по витковій парі. «Вита пара» — це один із типів мідних кабелів Ethernet, що використовуються в мережах. FastEthernet також відомий як 100Base-T, хоча є й інші позначення для інших типів кабелів.

FastEthernet хоч і покращив швидкість мережі в десять разів, наразі це лише архітектура Ethernet середнього рівня. Gigabit Ethernet (GbE) працює в десять разів швидше, ніж FastEthernet, зі швидкістю 1 гігабіт на секунду (gbps) або 1000Base-T і швидше. Публікація 802x Інституту інженерів з електротехніки та електроніки (IEEE) визначає технічні стандарти для локальних мереж, щоб сумісним було мережеве обладнання або сумісним у своєму класі. Існує декілька різних стандартів для кожного класу локальної мережі Ethernet.



Рисунок 1.1 – Існує кілька різних стандартів для кожного класу локальної мережі Інтернет

		Рачкінда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росінський Ю.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

Устаткування для швидшої локальної мережі зазвичай вимагає більше початкових інвестицій, ніж повільніше. Однак, якщо потрібна швидкість, вона з часом окупається продуктивністю. З іншого боку, офіс малого бізнесу може побажати сенс у зменшенні прибутку, якщо розглянути надшвидкий GbE над менш дорогою, але все ще дуже ефективною локальною мережею FastEthernet.

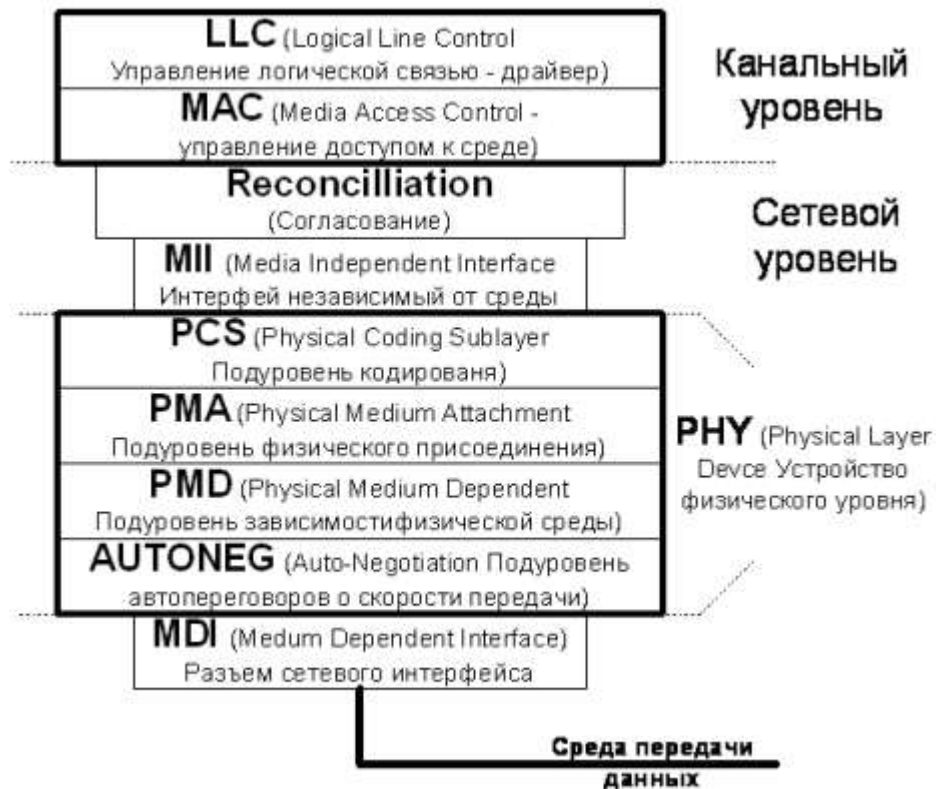


Рисунок 1.2 – Технологія FastEthernet

Бездротові маршрутизатори зазвичай зустрічаються вдома або в офісі - це апаратні пристрої, які постачальники послуг Інтернету використовують для підключення вас до своєї інтернет-мережі xDSL. Бездротовий маршрутизатор (його також називають маршрутизатором Wi-Fi) поєднує в собі функції мережі бездротової точки доступу та маршрутизатора. Він підключається до вашої широкомугової лінії та надсилає інтернет-сигнал з вашого домашнього (офісного) з'єднання на ваші пристрої, підключені до Інтернету.

Маршрутизатор поєднує локальні мережі з Інтернетом або іншими локальними мережами. Точка доступу (бездротова) підключає пристрої до мережі бездротовим способом, використовуючи радіочастоти в діапазонах 900 МГц і 2,4, 3,6, 5 і 60 ГГц. Останні бездротові маршрутизатори базуються на стандарті IEEE 802.11ac Wave 2, який часто скорочується до Wave 2. Коли ви вперше під'єднаєтеся до свого маршрутизатора Wi-Fi, вам буде запропоновано ввести пароль, який зазвичай надається вашим провайдером і буде надрукований на нижній частині маршрутизатора. Зазвичай це довгий і заплутаний ряд великих і малих літер і цифр, що ускладнює запам'ятовування, але також практично неможливо для інших здогадатися. Це робиться для того, щоб забезпечити підвищену безпеку та захистити вашу мережу від незаконного використання іншими. Кожен постачальник широкосмугового доступу надсилатиме маршрутизатор Wi-Fi всім своїм новим клієнтам. Якщо ви отримаєте базовий пакет ADSL, ви можете розраховувати на простий маршрутизатор, який виконує роботу з підключення до Інтернету та дуже мало іншого. Однак, якщо ви зареєструєтеся для широкосмугового волоконно-оптичного зв'язку, ви можете очікувати кращої моделі з більшими функціями.

1.2 Теоретичні відомості про демілітаризовану зону

DMZ — це фізична або логічна підмережа, яка ізолює локальну мережу від ненадійних мереж, таких як публічний Інтернет. Будь-яка послуга, яка пропонується користувачам у загальнодоступному Інтернеті, повинна бути налаштована в мережі DMZ. Зовнішні сервери, служби та ресурси зазвичай розміщуються там. Послуги включають Інтернет, систему доменних імен (DNS), електронну пошту, проксі-сервери та протокол передачі файлів (FTP), протокол передачі голосу через Інтернет (VoIP).

Мережа DMZ з єдиним брандмауером- ця конфігурація складається з трьох ключових елементів.

		Рачкинда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росієнський Ю.М.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

- Брандмауер: будь-який зовнішній трафік повинен спочатку вразити брандмауер.
- Перемикачі: комутатор DMZ перенаправляє трафік на загальнодоступний сервер. Внутрішній комутатор перенаправляє трафік на внутрішній сервер.
- Сервери: потрібна публічна та приватна версія.

Налаштуйте свою мережу таким чином, і ваш брандмауер буде єдиним елементом, який захищає вашу мережу. Перемикачі забезпечують переміщення трафіку в потрібний простір.

Для створення цієї форми DMZ достатньо одного брандмауера з трьома доступними мережевими інтерфейсами. Але вам потрібно буде створити кілька наборів правил, щоб ви могли контролювати та спрямовувати трафік всередині та навколо мережі.

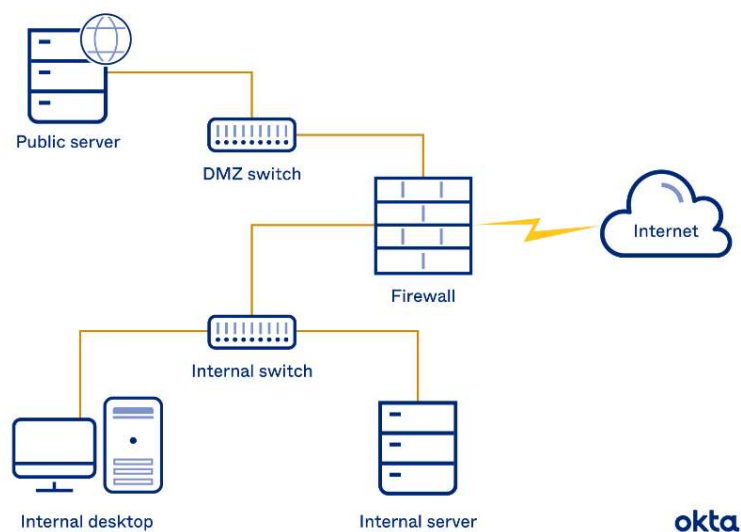


Рисунок 1.3 – Приклад роботи DMZ

Брандмауер не забезпечує ідеального захисту. Хакери часто обговорюють, скільки часу їм потрібно, щоб пройти повз системи безпеки компанії, і часто їхні відповіді бентежать. Але DMZ забезпечує рівень захисту, який може захистити цінні ресурси.

Компанії часто розміщують ці послуги в межах DMZ:

		Рачкінда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росінський Ю.М.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

- Веб-сервери: очевидно, вам потрібно дозволити трафіку в вашу компанію та з неї отримати доступ до Інтернету. Тримайте сервер в межах DMZ, але захищайте базу даних за брандмауером для додаткового захисту. Порушення вашого веб-сайту може бути надзвичайно важко виявити.
- FTP-сервери. Переміщення та розміщення вмісту на вашому веб-сайті простіше за допомогою FTP. Але ця функція супроводжується надзвичайними ризиками для безпеки. Дозволяйте доступ і використання в межах DMZ, але тримайте свої сервери за брандмауером.

Загалом, будь-яка компанія, яка має конфіденційну інформацію на сервері компанії, і якій потрібно надати публічний доступ до Інтернету, може використовувати DMZ.

1.3 Загальні відомості VPN

Віртуальна приватна мережа, більш відома як VPN, забезпечує конфіденційність та анонімність в Інтернеті, створюючи приватну мережу з загальнодоступного інтернет-з'єднання. VPN маскують вашу адресу Інтернет-протоколу (IP), тому ваші дії в Інтернеті практично не відстежуються. Найважливіше, послуги VPN встановлюють безпечні та зашифровані з'єднання, щоб забезпечити більшу конфіденційність, ніж навіть захищена точка доступу Wi-Fi.

Віртуальна приватна мережа є ключовим інструментом конфіденційності, який ви повинні використовувати, коли ви входите в Інтернет із загальнодоступного місця, такого як кав'ярня, фойє готелю чи будь-якого іншого місця, яке пропонує доступ до безкоштовного загальнодоступного Wi-Fi.

VPN створює тип тунелю, який приховує вашу онлайн-активність, включаючи посилання, які ви натискаєте, або файли, які ви завантажуєте, так що кіберзлочинці, підприємства, державні установи чи інші шпигуни не можуть його побачити.

		Рачкінда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росієнський Ю.М.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Перегляд в Інтернеті або транзакції в незахищеній мережі Wi-Fi означають, що ви можете розкрити свою особисту інформацію та звички перегляду. Ось чому VPN має бути обов'язковою для всіх, хто турбується про свою безпеку та конфіденційність в Інтернеті.

Якщо ви не ввійшли в приватну мережу Wi-Fi, для якої потрібен пароль, будь-які дані, передані під час ваших онлайн-сеансів, можуть бути вразливими для підслуховування незнайомцями, які використовують ту саму мережу.

VPN також може приховати вашу IP-адресу, щоб шпигуни не знали, що це ви переглядаєте мережу, завантажуйте файли. VPN шифрує дані, які ви надсилаєте та отримуєте на будь-якому пристрої, яким ви користуєтесь, включаючи телефон, ноутбук або планшет. Він надсилає ваші дані через захищений тунель на сервери постачальника послуг VPN. Ваші дані шифруються і перенаправляються на будь-який сайт, на який ви намагаєтесь перейти.

IPSEC дозволяє мережевим адміністраторам використовувати Інтернет для створення безпечних з'єднань між мережами (дистанційні працівники, віддалені сайти, ...). Маршрутизатори Cisco 2811 використовують стандарти тунелювання ISAKMP і IPsec для створення тунелів і керування ними. IPsec надає послуги аутентифікації (AH) і шифрування (ESP), щоб запобігти несанкціонованому доступу до даних або їх модифікації. ISAKMP — це протокол переговорів, який змушує колеги домовлятися про те, як створити асоціацію безпеки IPsec.

Основна мета IPsec - забезпечити безпеку зв'язку під час проходження ваших даних через загальнодоступну мережу, наприклад Інтернет. Щоб встановити з'єднання IPsec, вам потрібно мати IPsec-сумісні пристрої, такі як маршрутизатори на базі Cisco IOS. З IPsec використовується наступна криптографічна технологія

- Обмін ключами Діффі-Хеллмана
- Криптографія з відкритим ключем

		Рачкінда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росієнський Ю.М.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

- Алгоритм шифрування даних - він допомагає перевірити особу відправника і
- Алгоритм хешування – він перевіряє справжність і цілісність даних. Використовуються алгоритми хешування HMAC, SHA-1, MD5
- Цифровий сертифікат – спосіб підтвердити особу відправника. Цифровий сертифікат містить ідентифікаційні дані власника відкритого ключа і видається ЦС.

Щоб забезпечити швидкий, надійний і безпечний спосіб передачі даних через двох користувачів або мережі, використовуються VPN. Оскільки безпека є основною проблемою, VPN забезпечує економічне рішення для безпечної передачі даних і захищає цілісність ресурсів і конфіденційних даних компаній.

1.4 Теоретична інформація про wi-fi в soho офісах та способи організації бездротової мережі

Загалом розділяють 3 способи організації бездротової мережі :

- Wi-fi міст.
- Wi-fi роутер.
- Wi-fi точка доступу.

У мостовому режимі точки доступу використовуються для з'єднання двох мереж. У режимі Bridge є два підрежими. Існує:

- Від точки до точки.
- Точка-багатоточка.

За допомогою режиму мосту «точка-точка» ми можемо підключити локальну мережу маршрутизатора до віддаленої точки доступу.

Завдяки режиму мосту «точка-багато точок» ми можемо з'єднати дві локальні мережі за допомогою одного бездротового з'єднання.

Режим точки доступу або іншими словами локальний режим є основним режимом, який використовується для підключення бездротових клієнтів, таких

		Рачкинда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росінський Ю.М.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

як ноутбуки, смартфони, планшети тощо. У цьому режимі клієнти можуть спілкуватися з точкою доступу. Режим точки доступу (локальний режим) є режимом за замовчуванням, і тут точка доступу підтримує тунель до свого бездротового контролера.

Wi-fi маршрутизатор – самий найпоширеніший варіант бездротового з'єднання. Ми маємо роутер з підключеним кабелем від інтернет-провайдера. І уже цей маршрутизатор розподіляє інтернет по Wi-fi. Зручний спосіб для використання.

Вайфай роутер зазвичай має:

- Дротовий інтерфейс WAN порт Ethernet для підключення до зовнішнього каналу від Інтернет-провайдера.

- 5 портовий Ethernet комутатор (switch) та wireless інтерфейси 2.4 та 5 ГГц, а також 6 ГГц для підключення по кабелю та Wi-Fi клієнтських пристроїв домашньої мережі LAN та Wireless LAN.

Комутатор Wi-Fi роутера зазвичай підтримує типові для свіча функції – сегментація VLAN, Port Forwarding та ін.

У більшості випадків вайфай роутери оснащені зовнішніми всеспрямованими штиревидними антенами з посиленням 2-5 дБі та призначені для використання всередині приміщень.

Ми матимемо в головному офісі гостьову мережу. До одного маршрутизатора підключатись будь яким користувачам заборонено тому що це небезпечно для всієї структури організації. Тому для відвідувачів відведена окрема точка доступу. А для того що б вони не мали змоги звертатись до головного офісу, організовано access lists.

Також для безпеки налаштовано на Wi-Fi пристроях режими автентифікації. Усього передбачено чотири режими автентифікації користувачів.

		Рачкинда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росіньський Ю.М.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

1. Disabled – режим у якому автентифікація вимкнена, тобто. кожен може використовувати бездротову точку для доступу до мережі. Шифрування у цьому режимі не використовується.

2. WEP (Wired Equivalent Privacy – провідний монтажний еквівалент захисту інформації від несанкціонованого доступу) – режим з використанням статичного ключа автентифікації. Даний тип автентифікації підтримує два типи шифрування: 40/64-bits (тобто 64 бітний ключ складається з 40 бітного фактичного ключа та 24 бітного вектора ініціалізації) та 104/128-bits (тобто використовується 128 бітний ключ, який складається з 104 біт фактичного ключа та 24 бітного вектора ініціалізації). Цей тип автентифікації вважається ненадійним через недосконалі методи шифрування, які він використовує. Саме тому його рекомендується використовувати лише тоді, коли режими WPA/WPA2 недоступні.

3. WPA-PSK (Wi-Fi Protected Access Pre-Shared Key – захищений доступ до бездротової мережі з використанням заздалегідь заданого ключа) – є режимом автентифікації з використанням заздалегідь заданого ключа. Тобто. у налаштуваннях у полі Pass Phase необхідно вказати ключ і він повинен абсолютно збігатися на кожному пристрої підключеного до цієї точки доступу. Цей режим має два типи шифрування: найсучасніший AES (Advanced Encryption Standard – симетричний алгоритм блокового шифрування) та TKIP (Temporal Key Integrity Protocol – протокол цілісності тимчасового ключа).

4. WPA 2-PSK - по відношенню до WPA є більш сучасним і містить нові більш стійкі до атак алгоритми автентифікації. Також має два типи шифрування: AES та TKIP.

Таким чином, найсучаснішим і найнадійнішим методом автентифікації є режим WPA 2-PSK з типом шифрування AES. При виборі пароля потрібно користуватися правилами «сильного пароля», також обраний пароль має бути довшим за 8 символів.

		Рачкінда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росієнський Ю.М.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Завершивши перший розділ ми маямо розуміння з приводу демілітаризованої зони, як вона функціонує, її переваги та недоліки, віртуальної приватної мережі та їхнього з'єднання завдяки FastEthernet, ми визначили плюси використання wi-fi модулів та безпековий аспект а саме режим автентифікації. Також IPsec site-to-site дозволяє захистити та зберегти цілими данні які передаються з однієї мережі в іншу.

		Рачкінда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росієнський Ю.М.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ

2.1 Розробка комп'ютерної мережі

Загальна спроектована мережа зображена на рис. 2.1

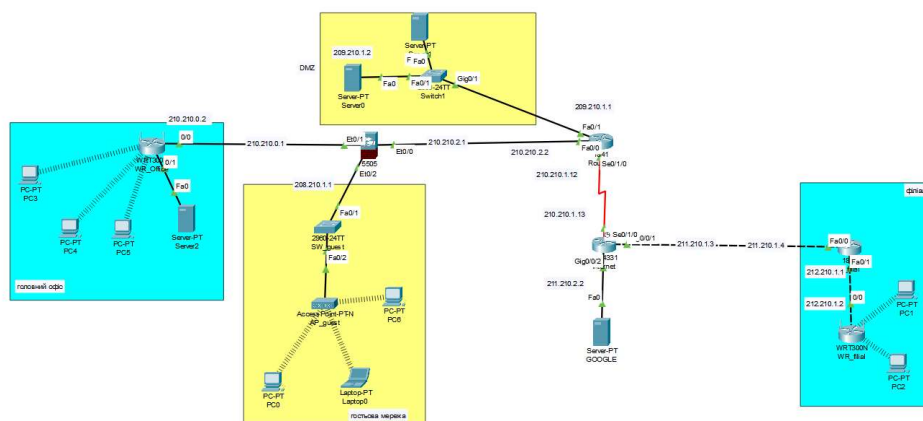


Рисунок 2.1 – Загально спроектована мережа

Розглянемо по частинам спроектовану мережу.

Мережу було поділено на відділи а саме: головний офіс, гостьову мережу, філіал та зону DMZ. Загальна структура мережі наведена в додатку А. Схема складається з двох комутаторів, трьох роутерів, двох бездротових роутерів, між-мережевого екрана, точки доступу та чотирьох серверів.

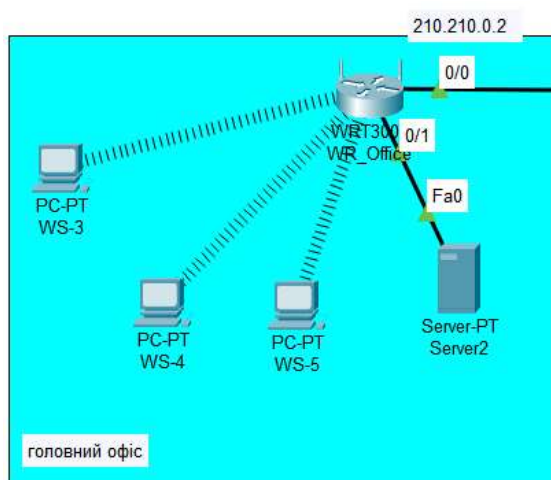


Рисунок 2.2 – Wi-Fi router та підключені чотири кінцевих вузли які знаходяться в головному офісі

Також головний офіс має гостьову мережу. Гостьова мережа зображена на рис.2.3. Вона містить комутатор, точку доступу та кінцеві вузли (клієнти які звертаються до компанії).

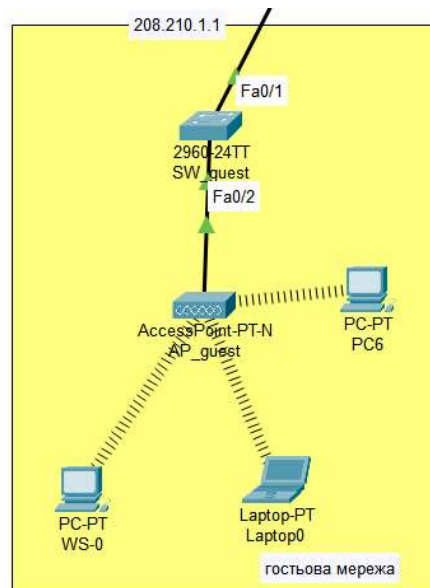


Рисунок 2.3 – Гостьова мережа та її кінцеві вузли

Також в головному офісі схематично зображено DMZ зону. DMZ містить комутатор та два сервери. Зображено DMZ на рис. 2.4.

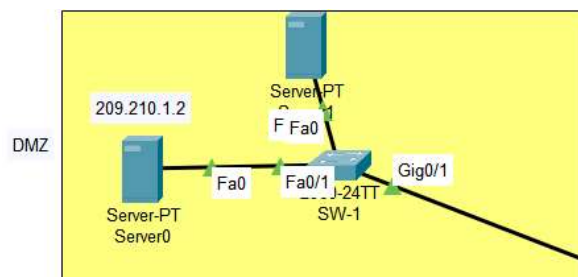


Рисунок 2.4 – Зображена на схемі DMZ

Також компанія розвивається. І тому вона створює свій філіал (рис. 2.5). Філіал містить маршрутизатор, Wi-fi роутер та кінцеві вузли.

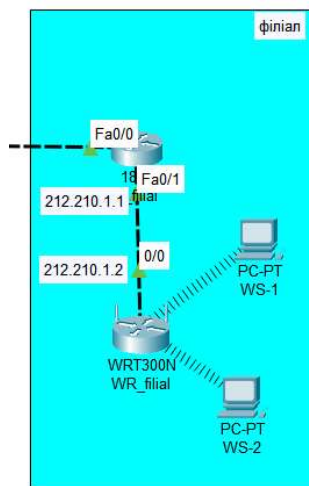


Рисунок 2.5 – Філіал зображений на схемі мережі

2.2 Розробка схеми адресації мережі

Таблиця 1.1 – Адресація мережі

Назва пристрою	Шлях	Адреса	Маска (префікс)
WR_Office	-	210.210.0.2	/24
Router	Internet	210.210.1.12	/24
	ASA	210.210.2.2	/24
	SW-1	209.210.1.1	/24
Internet	Router	210.210.1.13	/24
	R_filial	211.210.1.3	/24
	GOOGLE	211.210.2.2	/24
R_filial	Internet	211.210.1.4	/24
	WR_filial	212.210.1.1	/24
WR_filial	R_filial	212.210.1.2	/24
Server_DMZ	Asa	209.210.1.2	/24
ASA	Router	210.210.2.1	/24
	WR_office	210.210.0.1	/24
	SW_guest	208.210.1.1	/24

Перевіримо налаштування в головному офісі на Wi-fi роутері (рис. 2.6)

Рисунок 2.6 – Перевірка налаштування IP WR_Office

2.3 Функціонал та налаштування міжмережного екрану

Cisco Adaptive Security Appliance (ASA) — це досить універсальний пристрій, який інтегрує брандмауер, що підтримує програми, SSL і IPsec VPN, систему запобігання вторгненням (IPS), антивірус, антиспам, антифішинг і служби веб-фільтрації. Cisco ASA також підтримує протоколи маршрутизації, такі як протокол інформації про маршрутизацію (RIP), розширений протокол внутрішньої маршрутизації шлюзу (EIGRP) і останнє, але не менш важливе, Open Shortest Path First (OSPF).

Загальний список функції ASA:

- Packet filtering - іншими словами це звичайний ACL. Різниця з ACL маршрутизатора на ASA нужно вводить реальну маску.
- Stateful filtering - за умовчанням будь-який розділений трафік включається в BD Stateful filtering. На практиці це означає, що достатньо дозволити трафік у напрямку його ініціалізації, а відповідний трафік буде автоматично пропущено.

- Application inspection/awareness - ASA вміє прослуховувати і розуміти трафік на рівні доданого. Як результат ASA здатна динамічно дозволити, необхідні для правильної роботи додаткових портів. Наприклад, це дозволяє дозволити FTP і SIP трафік, які можуть динамічно використовувати додаткові порти.
- Network Address Translation - Трансляція мережевих адрес (NAT)
- DHCP.
- Routing - доступна підтримка RIP, EIGRP, OSPF, Static Routing
- Layer 3 or Layer 2 implementation - ASA може бути розвинена на традиційному 3-м рівні (виступаючий шлюз), так і на 2-му рівні (як міст L2).
- VPN support - ASA підтримує VPN віддаленого доступу IPsec і VPN-тунелі "сайт-сайт". Також є повна підтримка VPN з віддаленим доступом на рівні Secure Sockets Layer (SSL).
- Object groups - конфігураційна одиниця, яка дозволяє групувати об'єкти, облегчає адміністрування.
- Botnet traffic filtering - ботнет - це викликані машини спеціальним вірусом, і в результаті відбувається під контролем 3-х сторін. Часто використовуються для координуваних атак. ASA може працювати з базою даних фільтрів трафіку ботнетів Cisco і відсеивати трафік від таких адрес.
- Advanced malware protection (AMP) - це частина брандмауера нового покоління (NGFW). AMP дозволяє адміністратору захищати мережу від відомих і розширених загроз, включаючи розширені постійні загрози (APT) і цільові атаки.
- Підтримка AAA - ASA уміє використовувати сервіси AAA + ACS

		Рачкинда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росінський Ю.М.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ASA(config)#enable password cisco
ASA(config)#username admin password cisco
ASA(config)#show run
: Saved
:
ASA Version 8.4(2)
!
hostname ASA
domain-name fedir.net
enable password 4IncP7vTjpaba2aF encrypted
names

```

Рисунок 2.7 – Створення користувача та паролю



Рисунок 2.8 – Вигляд ASA та наведена таблиця ASA моделей

2.4 Вибір обладнання для організації роботи мережі

При виборі моделі комутатора основними критеріями виступають:

- кількість портів;
- швидкість передачі портів;
- керований/не керований комутатор.

У даній мережі використовуються дві моделі комутатора, а саме:

- Найбільш оптимальним є комутатор фірми Cisco, а саме Cisco Systems WS-C2960-24TC-S, рисунок 3.1.
- Модель керованого комутатора PT-Empty на десять портів. Дана модель використовується на рівні доступу, так як гарантує підключення десяти кінцевих вузлів, та забезпечує високу швидкість передачі трафіку на рівень розподілу.



Рисунок 2.9 - Cisco Systems WS-C2960-24TC-S

Cisco Systems WS - C2960 - 24TC -S - керований комутатор з 24 портами Fast Ethernet портів і 2 комбо Gigabit SFP. Перемикачі Cisco Catalyst 2960, 2960 -C і 2960- S підтримують передачу голосу, відео і даних з високими стандартами безпеки доступу. Крім того, вони забезпечують масштабоване управління відповідно до потреб бізнесу.

Особливості комутатору Cisco Catalyst 2960 , 2960 -C і 2960- S:

- Універсальність: підтримка передачі даних , бездротового і голосового зв'язку.
- Інтелектуальне управління: призначення пріоритетів голосовим трафікам або передачі даних з метою домовленості про доставку інформації від організацій.
- Підвищена безпека: захист важливої інформації, попередження про неавторизований доступ користувачів, і забезпечення безпечної роботи.
- Надійність: використання переваг стандартних методів і модулі FlexStack для підвищення надійності та швидкого знищення помилок.
- Зручність налаштування конфігурації: використання набору функцій Cisco Catalyst Kit Smart Operations і Cisco Network Assistant для спрощення налаштування, оновлення та виправлення всіх помилок.
- Запорука спокою: всі комутатори серії Catalyst 2960, 2960 -C і 2960- S захищені гарантією, діючою протягом усього терміну служби устаткування, і відсутність обмежень на оновлення.

		Рачкинда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Маршрутизатор Cisco 1841 розроблено для безпечного підключення даних і забезпечує значну додаткову цінність порівняно з попередніми поколіннями маршрутизаторів Cisco серії 1700, пропонуючи більш ніж п'ятикратне збільшення продуктивності, інтегроване апаратне шифрування, що забезпечується додатковим образом безпеки програмного забезпечення Cisco IOS, і різке збільшення продуктивності та щільності гнізда інтерфейсної карти при збереженні підтримки більш ніж 30 існуючих інтерфейсних карт WAN (WIC) і карт мультифлекса магістральних (голосові/WICs [VWICs] - лише для даних на маршрутизаторі Cisco 1841) серії Cisco 1700.



Рисунок 2.10 – Маршрутизатор Cisco 1841

Маршрутизатор Cisco 1841 забезпечує таку підтримку:

- Швидкість дроту для одночасних послуг зі швидкістю WAN T1/E1.
- Покращений захист інвестицій завдяки підвищеній продуктивності та модульності.
- Покращений захист інвестицій завдяки підвищеній модульності.
- Підвищена щільність завдяки високошвидкісним слотам інтерфейсу WAN (два).
- Підтримка понад 90 існуючих і нових модулів.
- Підтримка більшості існуючих WIC, VWIC і VIC (лише в режимі даних).
- Два вбудованих порти 10/100 Fast Ethernet.
- Внутрішнє шифрування.

		Рачкинда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

- Підтримка до 800 VPN-тунелів за допомогою модуля AIM-EPI-PLUS.
- Підтримка антивірусного захисту через мережевий контроль доступу (NAC).
- Запобігання вторгненням, а також підтримка брандмауера Cisco IOS з контролем стану та багато інших основних функцій безпеки

Як висновок, можна зазначити що нам вдалося спроектувати та виконати початкові налаштування на мережі підприємства, котра матиме головний офіс, гостьову мережу, філіал та DMZ. Також в таблиці ми навели схеми адресації мережі і визначились з обладнанням яке буде використовуватись в нашій мережі.

		Рачкінда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

РОЗДІЛ 3 НАЛАГОДЖЕННЯ ОБЛАДНАННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ ПІДПРИЄМСТВА

3.1 Налаштування обладнання мережі

Розглянемо лістинг налаштування на прикладі міжмережного екрана ASA5505:

```
conf t
host ASA
domain-name fedir.net
no dhcpd enable inside
no dhcpd auto_config outside
no dhcpd address 192.168.1.5-192.168.1.35 inside
int vlan 1
ip add 210.210.0.1 255.255.255.0
ex
int vlan 2
ip add 210.210.2.1 255.255.255.0
no shut
ex
int vlan 3
ip add 208.210.1.1 255.255.255.0
no shut
no forward interface vlan 1
nameif guest
ex
int e0/2
switchport mode access
switchport access vlan 3
ex
route outside 0.0.0.0 0.0.0.0 210.210.2.2 1
class-map MY_MAP
match default-inspection-traffic
ex
policy-map MY_POLICY
```

		Рачкінда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росінський Ю.М.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

```

class MY_MAP
inspect icmp
inspect http
inspect ftp
inspect dns
ex
policy-map GUEST_POLICY
class MY_MAP
inspect icmp
inspect http
inspect dns
ex
service-policy GUEST_POLICY interface guest
service-policy MY_POLICY interface inside
object network inside-subnet
subnet 210.210.0.0 255.255.255.0
nat (inside,outside) dynamic interface
exit
conf t
object network guest-subnet
subnet 208.210.1.0 255.255.255.0
nat (guest,outside) dynamic interface
ex
enable password cisco
username admin password cisco

```

Для присвоєння IP використовується технологія NAT.

Також завдяки Access List ми маємо змогу контролювати трафік і визначати куди він має право рухатись.

		Рачкинда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

Налаштування R_filial:

```
en
conf t
host R_Filial
int fa0/0
ip add 211.210.1.4 255.255.255.0
no shut
ex
int fa0/1
ip add 212.210.1.1 255.255.255.0
no shut
ex
router ospf 1
network 211.210.1.0 0.0.0.255 area 0
network 212.210.1.0 0.0.0.255 area 0
```

Налаштування на Internet:

```
en
conf t
host Internet
int s0/1/0
ip add 210.210.1.13 255.255.255.0
no shut
int g0/0/1
ip add 211.210.1.3 255.255.255.0
no shut
ex
int g0/0/2
ip add 10.10.10.1 255.255.255.0
no shut
ex
router ospf 1
network 210.210.1.0 0.0.0.255 area 0
network 211.210.1.0 0.0.0.255 area 0
network 10.10.10.0 0.0.0.255 area 0
```

		Рачкинда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Россінський Ю.М.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

Налаштування Router:

```
int fa0/0
ip add 210.210.2.2 255.255.255.0
no shut
ex
int fa0/1
ip add 209.210.1.1 255.255.255.0
no shut
ex
int s0/1/0
ip add 210.210.1.12 255.255.255.0
no shut
ex
router ospf 1
network 210.210.2.0 0.0.0.255 area 0
network 210.210.1.0 0.0.0.255 area 0
network 209.210.1.0 0.0.0.255 area 0
exit
ip domain-name fedir.net
ip dhcp pool ASA-POOL-1
network 210.210.2.0 255.255.255.0
default-router 210.210.2.2
exit
ip dhcp excluded-address 210.210.2.2
ip access-list extended FROM_DMZ_ACL
permit ip 209.210.1.0 0.0.0.255 any
exit
ip access-list extended TO_DMZ_ACL
permit tcp 210.210.0.0 0.0.0.255 209.210.1.0 0.0.0.255 eq www
permit tcp 210.210.0.0 0.0.0.255 209.210.1.0 0.0.0.255 eq domain
permit tcp 210.210.2.0 0.0.0.255 209.210.1.0 0.0.0.255 eq www
permit tcp 210.210.2.0 0.0.0.255 209.210.1.0 0.0.0.255 eq domain
permit tcp 212.210.1.0 0.0.0.255 209.210.1.0 0.0.0.255 eq domain
permit tcp 212.210.1.0 0.0.0.255 209.210.1.0 0.0.0.255 eq www
```

		Рачкинда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росінський Ю.М.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

```

exit
int fa0/1

ip access-group TO_DMZ_ACL out

ip access-group FROM_DMZ_ACL in

exit

```

Налаштування VPN на ASA:

```

ASA(config)#show run | sec crypto
crypto ipsec ikev1 transform-set TS esp-aes esp-sha-hmac
crypto map To-Site2 1 match address FOR-VPN
crypto map To-Site2 1 set peer 211.210.1.4
crypto map To-Site2 1 set security-association lifetime seconds 86400
crypto map To-Site2 1 set ikev1 transform-set TS
crypto map To-Site2 interface outside
crypto ikev1 enable outside
crypto ikev1 policy 1
  encr aes
  authentication pre-share
  group 2
  lifetime 36000

```

Рисунок 3.1 – Виведення команди show run | sec crypto

```

ASA(config)#show run | sec tunnel
tunnel-group 211.210.1.4 type ipsec-l2l
tunnel-group 211.210.1.4 ipsec-attributes
  ikev1 pre-shared-key cisco
ASA(config)#

```

Рисунок 3.2 – Виведення команди show run | sec tunnel

Призначення IP для користувачів гостьової мережі :

```

ASA(config)#dhcp address 208.210.5.2-208.210.5.20 guest
Address range subnet 208.210.5.2 or 208.210.5.20 is not the same as inside interface
subnet 208.210.1.1
ASA(config)#dhcp address 208.210.1.3-208.210.1.20 guest
ASA(config)#dhcp dns 11.11.11.11
ASA(config)#dhcp enable ?

```

configure mode commands/options:
 inside Name of interface Vlan1
 outside Name of interface Vlan2
 guest Name of interface Vlan3
 ASA(config)#dhcp enable guest

3.2 Перевірка працездатності мережі

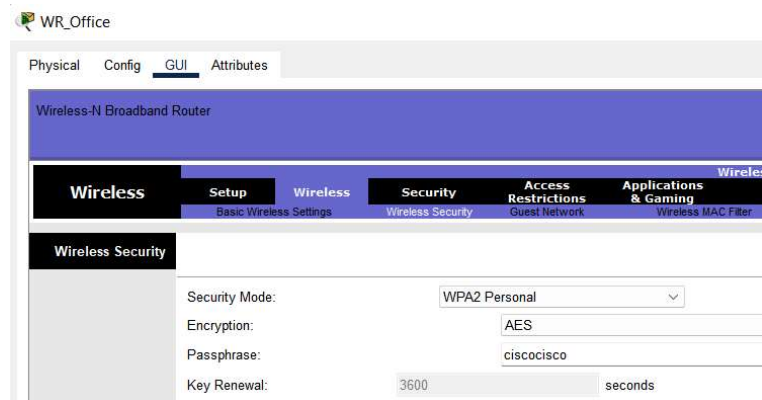


Рисунок 3.3 – Роздача мережі з паролем ciscocisco який шифрується за допомогою AES

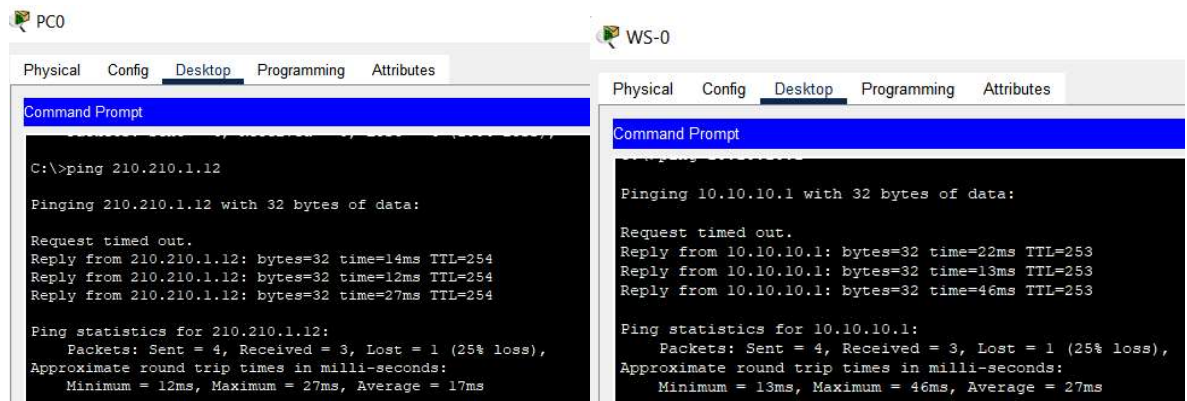


Рисунок 3.4 – Перевірка з'єднання гостьової мережі до інтернету та GOOGLE

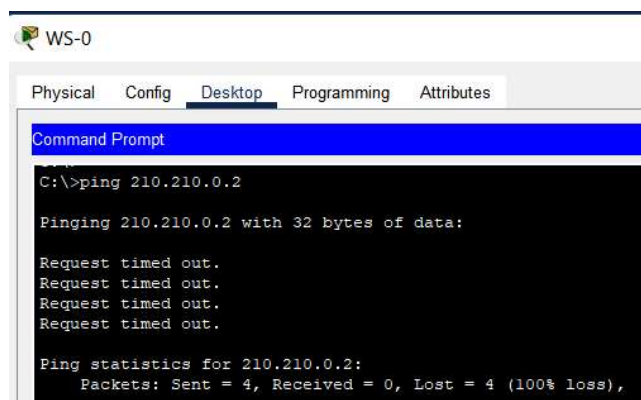


Рисунок 3.5 – Перевірка дії Access list (ping гостьової мережі до головного офісу)

		Рачкінда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

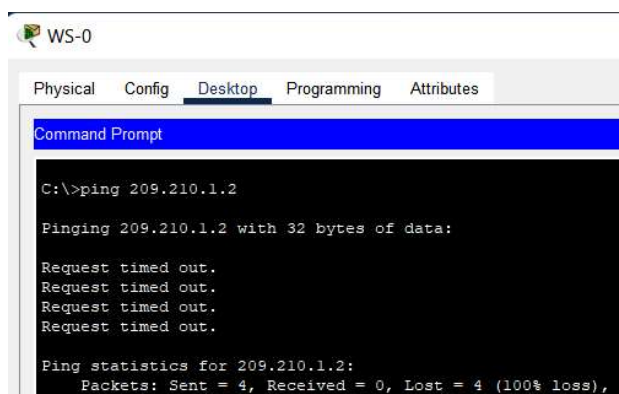


Рисунок 3.6 – Заборона відвідувачам підключатись до DMZ

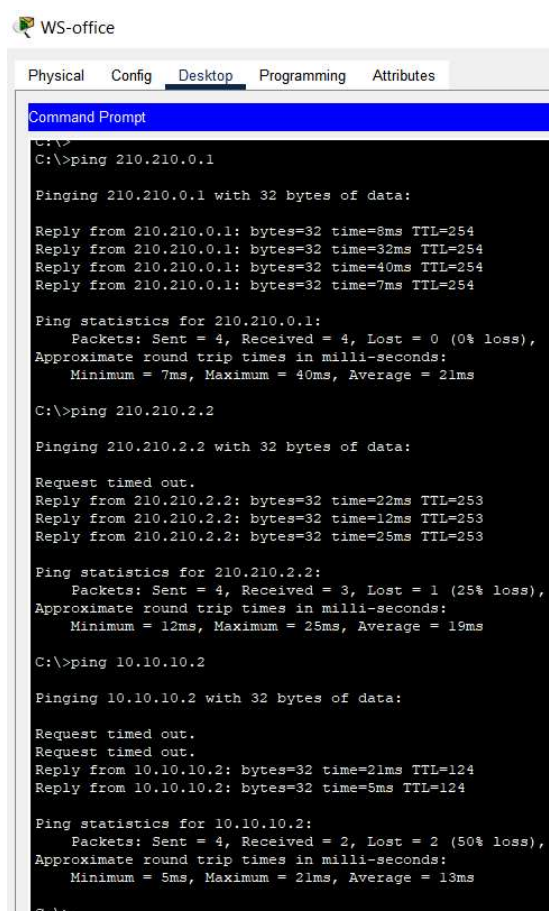


Рисунок 3.7 – Пінгування офісного працівника до ASA та інтернету,
GOOGLE

		Рачкинда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

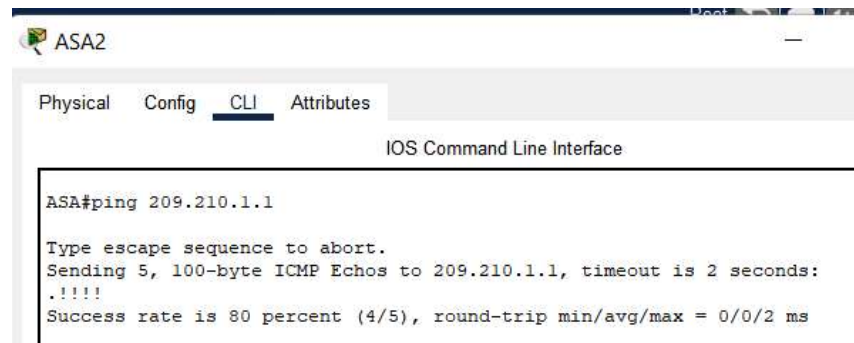


Рисунок 3.8 – Перевірка зв'язку між Asa і DMZ

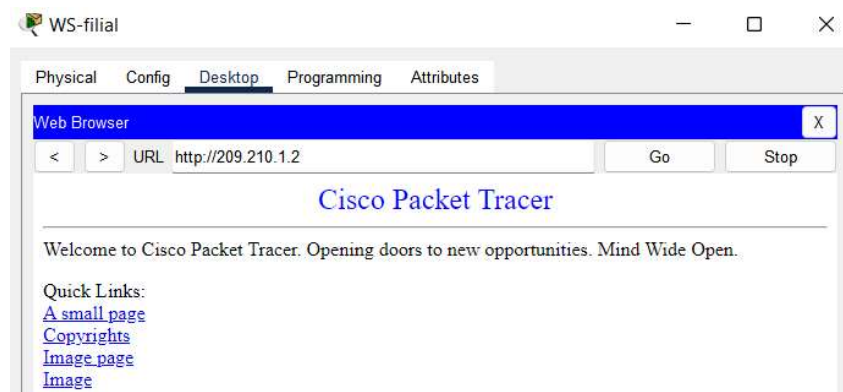


Рисунок 3.9 – Зв'язок з філіала до DMZ лише веб

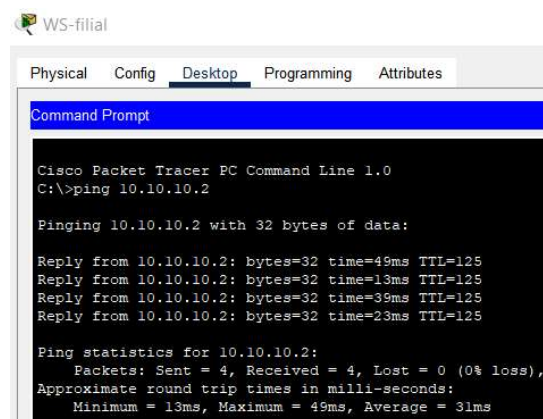


Рисунок 3.10 – З'єднання з філіалу до GOOGLE

Виконавши налаштування та аналіз працездатності пристроїв можна зробити висновок що все налаштовано вірно та ми маємо результат який бажали отримати з початку.

		Рачкінда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росінський Ю.М.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

При виконанні кваліфікаційної роботи в першому розділі було проаналізовано особливості функціонування мережевих технологій FastEthernet. Проаналізували переваги та недоліки технологій VPN та DMZ та знайшли варіанти виконання поставленого завдання.

В другому розділі розробили проект мережі підприємства, наведено обґрунтування вибору маршрутизаторів та їх переваги. Наведено кількість необхідного обладнання. Для мережі розроблено схему адресації. Проаналізувавши особливості побудови мережі вибрали обладнання для організації роботи.

В третьому розділі виконавши поставлене перед нами завдання, можемо зробити висновок що ми налаштували захищену мережу підприємства з використанням безпроводного сегменту в симуляторі Cisco Packet Tracer.

		Рачкінда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Abelar G. Securing your business with CISCO ASA and PIX firewalls. Indianapolis, Ind : Cisco, 2005. 266 p.
2. Academy C. N. C. N. CCNA Cybersecurity Operations Lab Manual. Cisco Press, 2018. 400 p.
3. Academy C. N. C. N. IT Essentials. Pearson Education, Limited, 2014. 432 p.
4. Academy C. N. C. N. Switching, Routing, and Wireless Essentials V7. 0 (SRWE) Companion Guide. Pearson Education, Limited, 2020. 750 p.
5. Black U. D. IP Routing Protocols. Prentice Hall, 2001. 271 p.
6. Hylton B. Router Magic. Rodale Pr, 1999.
7. Layer 2 VPN Architectures /D.Bokotey et al. Brand: CiscoPress, 2005. 648 p
8. Misra S., Goswami S. Network Routing. Chichester, UK : John Wiley & Sons, Ltd, 2017. URL: <https://doi.org/10.1002/9781119114864>.
9. Moy J. T. OSPF Complete Implementation. Pearson Education, Limited, 2008. 400 p.
10. Press C. CCNA Self-Study: CCNA Basics (CCNAB). Cisco Press, 2002. 592 p.
11. VPN: Virtual Private Network. Novatec, 2002.
12. Zinin A. Cisco IP Routing: Packet Forwarding & Intra-domain Routing Protocol.
13. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2001. – 672 с.
14. Амато, Вито. Основы организации сетей Cisco, том 2. - Издательский дом "Вильямс", 2004. – 464 с.
15. Дж.Бони. Руководство по CiscoIOS. – Издательство "Русская редакция", 2008. – 784 с.
16. Кулаков Ю.О., Луцкий Г.М. Комп'ютерні мережі. Підручник / За ред. Ю.С. Ковтанюка. – К.: Юніор, 2003. – 400 с.
17. Олифер В.Г., Олифер Н.А. Сетевые операционные системы: Учебник для вузов. 2-е изд. – СПб.: Питер, 2007. – 672 с.

		Рачкинда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росінський Ю.М.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

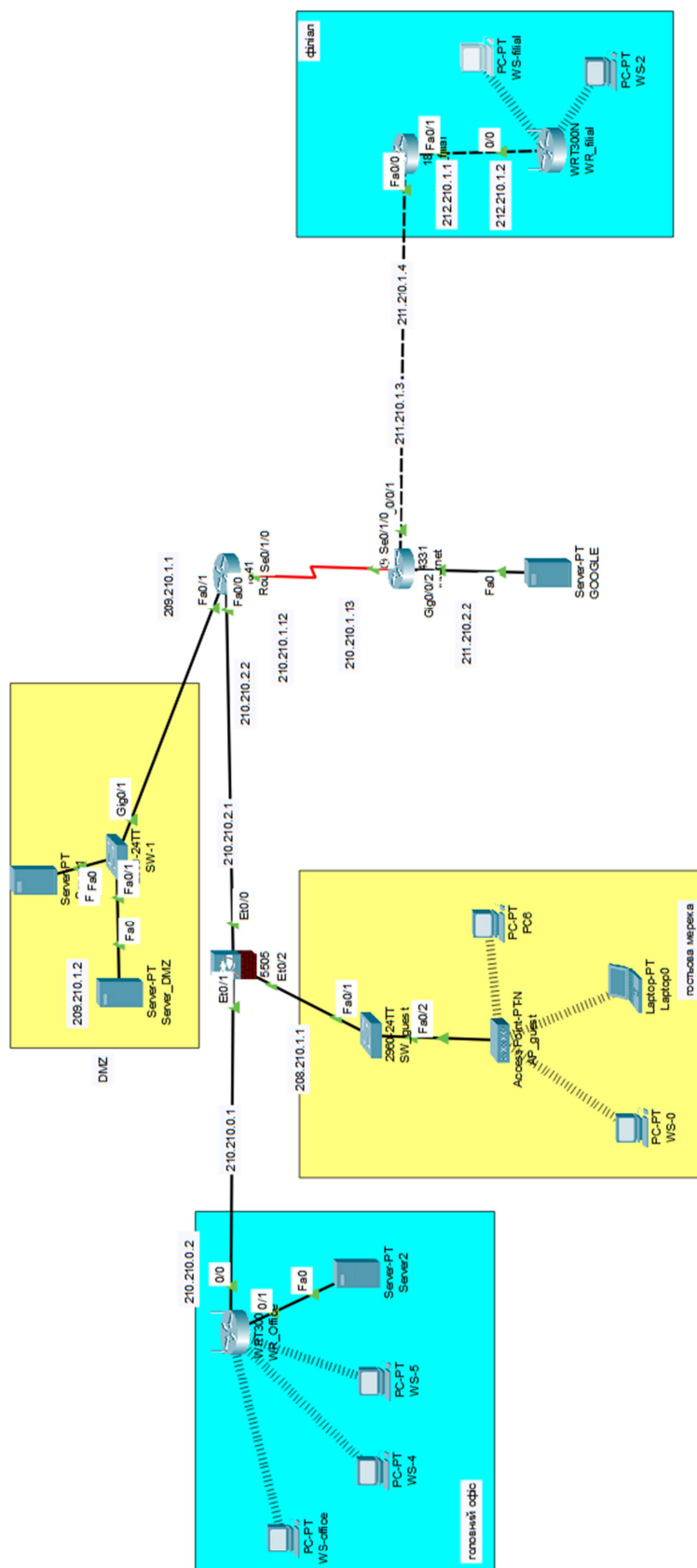
18. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – СПб.: Питер, 2005. – 958 с.
19. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. – СПб.: Питер, 2002. – 544 с.
20. Хендерсон Л., Дженкинс Т. Frame Relay. Межсетевое взаимодействие. - ЭНТРОП. 2000. - 320 с.
21. Хилл Брайан. Полный справочник по Cisco. - Издательский дом "Вильямс", 2004. - 1053 с.
22. Мережева академія Dark Maycal [Електронний ресурс] – Режим доступу до ресурсу: <https://darkmaycal-it.ru/.ls>. Addison-Wesley Professional, 2001. 512 p.

		Рачкинда Ф.Ф.			КІК.КР.Б – 123 – 18 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

ДОДАТКИ

		Рачкинда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росі́нський Ю.М.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток А – Схема мережі



		Рачкінда Ф.Ф.		
		Росінський Ю.М.		
Змн.	Арк.	№ докум.	Підпис	Дата

КІК.КР.Б - 123 - 18 - ПЗ

Арк.

40


```

!
access-list FOR-VPN extended permit ip
210.210.0.0 255.255.255.0 212.210.1.0
255.255.255.0
!
!
!
username admin password 4IncP7vTjpaba2aF
encrypted
!
class-map MY_MAP
match default-inspection-traffic
!
policy-map MY_POLICY
class MY_MAP
inspect dns
inspect ftp
inspect http
inspect icmp
policy-map GUEST_POLICY
class MY_MAP
inspect dns
inspect http
inspect icmp
!
service-policy MY_POLICY global
!
telnet timeout 5
ssh timeout 5
!
dhcpd dns 11.11.11.11
dhcpd auto_config outside
!
!
!
dhcpd address 208.210.1.3-208.210.1.20 guest
dhcpd enable guest
!
!
crypto ipsec ikev1 transform-set TS esp-aes
esp-sha-hmac
!
crypto map To-Site2 1 match address FOR-
VPN
crypto map To-Site2 1 set peer 211.210.1.4
crypto map To-Site2 1 set security-association
lifetime seconds 86400
crypto map To-Site2 1 set ikev1 transform-set
TS
crypto map To-Site2 interface outside
crypto ikev1 enable outside
crypto ikev1 policy 1

```

```

ip access-group FROM_DMZ_ACL in
ip access-group TO_DMZ_ACL out
duplex auto
speed auto
!
interface Serial0/1/0
ip address 210.210.1.12 255.255.255.0
!
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 210.210.2.0 0.0.0.255 area 0
network 210.210.1.0 0.0.0.255 area 0
network 209.210.1.0 0.0.0.255 area 0
!
router rip
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended FROM_DMZ_ACL
permit ip 209.210.1.0 0.0.0.255 any
ip access-list extended TO_DMZ_ACL
permit tcp 210.210.0.0 0.0.0.255 209.210.1.0
0.0.0.255 eq www
permit tcp 210.210.0.0 0.0.0.255 209.210.1.0
0.0.0.255 eq domain
permit tcp 210.210.2.0 0.0.0.255 209.210.1.0
0.0.0.255 eq www
permit tcp 210.210.2.0 0.0.0.255 209.210.1.0
0.0.0.255 eq domain
permit tcp 212.210.1.0 0.0.0.255 209.210.1.0
0.0.0.255 eq domain
permit tcp 212.210.1.0 0.0.0.255 209.210.1.0
0.0.0.255 eq www
!
!
!
!
!
!
line con 0

```

		Рачкінда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

```

encr aes
authentication pre-share
group 2
lifetime 36000
!
tunnel-group 211.210.1.4 type ipsec-l2l
tunnel-group 211.210.1.4 ipsec-attributes
ikev1 pre-shared-key cisco
!

```

Internet :

```

spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/0/1
ip address 211.210.1.3 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/0/2
media-type sfp
ip address 10.10.10.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/1/0
ip address 210.210.1.13 255.255.255.0
clock rate 2000000
!
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 210.210.1.0 0.0.0.255 area 0

```

```

!
line aux 0
!
line vty 0 4
login
!
!
!
!
End

```

R_filial:

```

crypto isakmp policy 1
encr aes
group 2
!
crypto isakmp key cisco address 210.210.2.1
!
!
!
crypto ipsec transform-set TS esp-aes esp-sha-
hmac
!
crypto map CMAP 10 ipsec-isakmp
set peer 210.210.2.1
set transform-set TS
match address FOR-VPN
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
ip address 211.210.1.4 255.255.255.0
duplex auto
speed auto
crypto map CMAP
!
interface FastEthernet0/1
ip address 212.210.1.1 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address

```

		Рачкінда Ф.Ф.			КІК.КР.Б - 123 - 18 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

```

network 211.210.1.0 0.0.0.255 area 0
network 10.10.10.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end

```

```

shutdown
!
router ospf 1
log-adjacency-changes
network 211.210.1.0 0.0.0.255 area 0
network 212.210.1.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended FOR-VPN
permit ip 210.210.1.0 0.0.0.255 210.210.0.0
0.0.0.255
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end

```