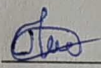


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

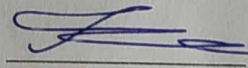
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захищеного віддаленого
доступу користувачів до ресурсів мережі
організації на базі технологій Remote Access VPN»

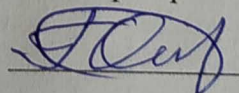
Виконав студент 4-го курсу, групи КІ-3
спеціальності 123 «Комп'ютерна інженерія»

 Д.І. Гнатюк

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

 Ю.М. Росінський

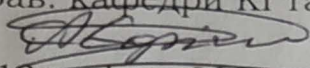
Рецензент к.пед.н., доцент кафедри КІ та КБ

 О.С. Головня

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри КІ та КБ



Єфіменко А. А.

«12» квітня 2021р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента: Гнатюка Дениса Ігоровича

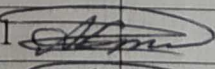
Тема роботи: «Проект підсистеми захищеного віддаленого доступу користувачів до ресурсів мережі організації на базі технологій Remote Access VPN»

Затверджена Наказом університету від «12» квітня 2021 р. № 133\С

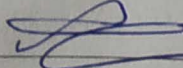
Термін здачі студентом закінченої роботи 24.06.2021

Вихідні дані роботи (зазначається предмет і об'єкт дослідження): процес проектування та побудови підсистеми захищеного віддаленого доступу до ресурсів мережі організації на базі технологій Remote Access VPN; технології та пристрої віддаленого доступу до ресурсів мережі організації на базі технологій Remote Access VPN.

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	12.04.2021 	12.04.20.21 
2	Єфіменко А.А.	13.05.2021 	13.05.2021 
3	Єфіменко А.А.	15.06.2021 	15.06.2021 

Керівник



Росіїнський Ю. М.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Видача завдання	12.04.2021	
2	Розробка плану роботи	14.04.2021 – 18.04.2021	
3	Розробка розгорнутого плану	19.04.2021 – 20.04.2021	
4	Подача чернетки керівнику для перевірки	24.04.2021	
5	Доопрацювання роботи та перевірка керівником	27.04.2021 – 29.05.2021	
6	Затвердження графічних матеріалів у керівника	01.06.2021 – 04.06.2021	
7	Проведення попереднього захисту	05.06.2021	
8	Отримання відгуку керівника	15.06.2021	
9	Допуск завідувача кафедри	16.06.2021	
10	Подання роботи на рецензування	22.06.2021	
11	Захист		

Студент  Гнатюк Д. І.

Керівник  Россінський Ю. М.

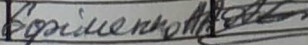
АНОТАЦІЯ

Випускна дипломна кваліфікаційна робота представляє з себе проект підсистеми захисту корпоративної комп'ютерної мережі. Пояснювальна записка до випускної дипломної кваліфікаційної роботи містить в собі 53 сторінки, 26 рисунків та 7 таблиць. Список використаних джерел містить 20 найменувань і займає 2 сторінки.

Метою випускної кваліфікаційної роботи є розробка підсистеми захищеного віддаленого доступу користувачів до мережевих ресурсів організації на базі технологій Remote Access VPN та забезпечення функціонування даної системи.

В роботі визначено основні завдання для побудови локальної мережі організації, та підсистеми віддаленого доступу користувачів, проаналізовано базові підходи, методи та технології побудови локальних мереж та підсистем віддаленого доступу користувачів. Наведено розробку, налагодження функціонування підсистеми захищеного віддаленого доступу користувачів до мережевих ресурсів організації та тестування її працездатності й виконання поставлених задач.

Ключові слова: ЗАХИСТ, ВІДДАЛЕНИЙ ДОСТУП, ВІДДАЛЕНИЙ КОРИСТУВАЧ, ЛОКАЛЬНА МЕРЕЖА, МЕРЕЖЕВІ РЕСУРСИ, VPN, CISCO.

					КІК.КР.Б – 123 – 04 – ПЗ				
Зм.	Арк.	№ докум.	Підпис	Дата					
Розроб.		Гнатюк Д.І.		25.06.21	Проект підсистеми захищеного віддаленого доступу до ресурсів мережі організації на базі технологій Remote Access VPN	Літ.	Арк.	Аркушів	
Керівник		Росієнський Ю.		25.06.21				4	54
Реценз.		Головня О. С.		25.06.21		ФІКТ, Гр. КІ-3			
Н. контр.									
Затверд.				25.06.21					

ANNOTATION

The final dissertation is a project of the subsystem of corporate computer network protection. The explanatory note to the final diploma qualification work contains 54 pages, 26 figures and 7 tables. The list of used sources contains 20 names and occupies 2 pages.

The purpose of the final qualification work is to develop a subsystem of secure remote access of users to network resources of the organization based on Remote Access VPN technologies and ensure the functioning of this system.

The main tasks for building the local network of the organization and the subsystem of remote access for defined users, the basic approaches, methods and technologies of construction of local networks and subsystems of remote access of users are analyzed. Showed development and adjustment of functioning of a protected remote connect subsystem of users to network resources of the organization and testing of its working capacity and performance of the set tasks are planned.

Keywords: PROTECTION, REMOTE ACCESS, REMOTE USER, LOCAL AREA NETWORK, NETWORK RESOURCES, VPN, CISCO.

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росієнський Ю. М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	7
РОЗДІЛ 1 ТЕОРЕТИЧНІ ВІДОМОСТІ ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ	9
1.1 Загальна інформація про віртуальні приватні мережі	9
1.2 Методи реалізації Remote Access VPN	10
1.3 Протоколи для реалізації Remote Access VPN	12
1.4 Постановка технічного завдання	18
РОЗДІЛ 2 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ ТА ПІДСИСТЕМИ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ КОРИСТУВАЧІВ НА БАЗІ ТЕХНОЛОГІЙ REMOTE ACCESS VPN	20
2.1 Розробка фізичної топології мережі	20
2.2 Розробка логічної топології мережі.....	21
2.3 Вибір обладнання для реалізації проекту комп'ютерної мережі та підсистеми захищеного віддаленого доступу користувачів	23
2.4 Вибір програмного забезпечення для реалізації проекту комп'ютерної мережі та підсистеми захищеного віддаленого доступу користувачів	25
2.5 Проектування системи віддаленого доступу.....	27
РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ РОБОТИ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ПІДСИСТЕМИ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ КОРИСТУВАЧІВ	29
3.1 Налаштування мережевих пристроїв та домену Windows.....	29
3.2 Налаштування підсистеми віддаленого доступу	34
3.3 Тестування роботи мережі та підсистеми захищеного віддаленого доступу	37
ВИСНОВКИ.....	42
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	44
ДОДАТКИ.....	46

ВСТУП

На сьогоднішній день неможливо уявити роботу організації без обчислювальної та комп'ютерної техніки, за допомогою якої обробляється величезна кількість інформації. В межах організації забезпечити безпеку інформації доволі просто навіть без використання технічних методів. Проте з приходом пандемії COVID-19 з'явилась нагальна потреба відправлення працівників на віддалений режим роботи. В зв'язку з цим постає питання забезпечення захищеного доступу працівників до мережевих ресурсів організації. Передача важливих корпоративних даних по недостатньо захищеним підключенням, може призвести від фінансових втрат та зменшення репутації до повного руйнування установи, оскільки зловмисники можуть не тільки перехопити дані, але й отримати доступ до внутрішньої мережі організації. Тому питання побудови підсистем захищеного віддаленого доступу до мережевих ресурсів на сьогодні є надзвичайно важливим.

Актуальність теми дослідження обумовлена необхідністю створення захищених каналів зв'язку між віддаленими користувачами та корпоративними мережами, для запобігання витоків інформації, та втручання сторонніх осіб в роботу організації.

Об'єктом дослідження є процес проектування та побудови підсистеми захищеного віддаленого доступу до ресурсів мережі організації на базі технологій Remote Access VPN.

Предметом дослідження є технології та пристрої віддаленого доступу до ресурсів мережі організації на базі технологій Remote Access VPN.

Метою кваліфікаційної роботи є розробка проекту підсистеми захищеного віддаленого доступу до мережевих ресурсів організації за допомогою технології Remote Access VPN.

Досягнення даної мети включає в себе рішення наступних задач:

- аналіз існуючих методів організації підсистем захищеного віддаленого доступу;

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росієнський Ю. М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

- аналіз мережевих технологій та пристроїв за допомогою яких здійснюється побудова підсистем захищеного віддаленого доступу;
- розробка загального проекту мережі;
- розробка фізичної та логічної топологій;
- вибір обладнання та сімейства операційних систем;
- розробка підсистеми віддаленого доступу на базі обраного обладнання;
- налагодження мережевого обладнання, підсистеми віддаленого доступу та робочих станцій;
- тестування працездатності та коректності налаштованої системи;

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Россінський Ю. М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ ВІДОМОСТІ ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО ВІДДА- ЛЕНОГО ДОСТУПУ

1.1 Загальна інформація про віртуальні приватні мережі

VPN – віртуальна приватна мережа, узагальнена назва технології, що дозволяє створювати віртуальні мережі через існуюче, реальне з'єднання. Найпершими мережами VPN були звичайні IP-тунелі, в яких не здійснювалися операції аутентифікації чи шифрування даних. Одним з прикладів таких тунелів є GRE, розроблений компанією Cisco, він може інкапсулювати пакети різноманітних протоколів мережевого рівня всередині IP-тунелів. Нині в мережах VPN застосовуються сучасні криптографічні методи, котрі дозволяють встановлювати надійне та захищене з'єднання між пристроями.

За типом використання середовища VPN-мережі класифікуються на захищені і довірчі. Захищені використовуються тоді, коли потрібно створити надійну і захищену підмережу на основі ненадійної, зазвичай, інтернету. Такі підмережі хоч і мають високу безпеку, проте через наявність багатьох криптографічних методів мають низьку швидкість обмінну даними. Довірчі мережі зазвичай реалізують через середовище, котре можна вважати умовно надійним, та для забезпечення більшої швидкості передачі даних. Прикладом таких мереж є особисті, чи орендовані лінії передачі даних.

Сценарії використання VPN можуть бути різноманітними, проте найбільшої популярності здобули Site-to-Site VPN та Remote Access VPN.

Site-to-Site VPN – найбільш розповсюджений тип VPN в бізнес середовищі. Дозволяє з'єднувати дві чи більше мережі між собою через мережу Інтернет. На границях мереж знаходяться пристрої, котрі відповідають за інкапсуляцію та шифрування вихідного трафіку. Такі пристрої налаштовані статично, тунель існує майже постійно, а внутрішні хости не знають про існування VPN. Використовується даний метод зазвичай для з'єднання географічно віддалених сегментів корпоративної мережі.

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Россінський Ю. М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

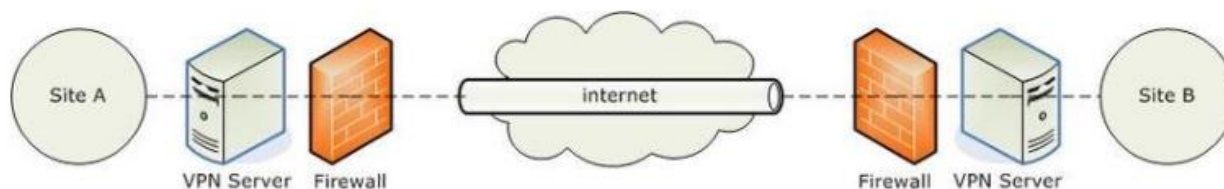


Рисунок 1.1 – Приклад Site-to-Site VPN

Remote Access VPN – метод підключення віддалених користувачів до мережі організації. Цей метод майже завжди передбачає використання загальних незахищених каналів зв'язку. Зазвичай використовується, коли організації необхідно забезпечити захищений доступ користувачам до внутрішньої мережі.

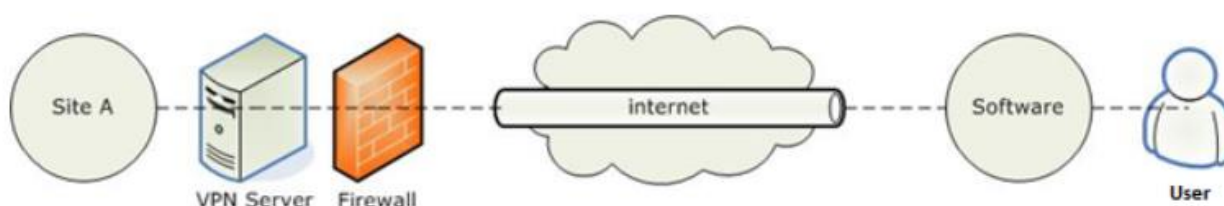


Рисунок 1.2 – Приклад Remote Access VPN

Також варто зазначити про такий спосіб використання VPN як анонімізація кінцевого користувача та шифруванням трафіку на шляху від VPN-сервера до цього користувача. В сьогоденні він представлений безліччю умовно-безкоштовних програм, проте відомі випадки коли надавачі таких послуг здійснювали накопичення та продаж даних користувачів третім особам.

1.2 Методи реалізації Remote Access VPN

Remote Access VPN базуються на реалізації трьох складових:

- тунелювання;
- шифрування;
- аутентифікація.

Тунелювання забезпечує передачу даних між двома точками – кінцями тунелю, таким чином, що для джерела та приймача даних вся система яка розташована між ними є прихованою. З точки зору роботи програмного забезпечення кінцеві пристрої тунелю будуть знаходитися в одній локальній мережі.

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росієвський Ю. М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Шифрування забезпечує конфіденційність даних, котрі передаються через мережу, щоб навіть у випадку перехоплення трафіку сторонніми особами, його вміст залишився невідомим для злоумисників.

Аутентифікація дозволяє впевнитись в тому, що підключення здійснюється легітимним користувачем чи пристроєм.

Існують різні варіанти побудови таких VPN з'єднань, тому при виборі рішення потрібно враховувати фактори продуктивності засобів побудови.

Найбільш поширеними є:

- VPN на базі мережевих екранів.
- VPN на базі маршрутизаторів.
- VPN на базі програмного забезпечення.
- VPN на базі мережевої ОС.

Мережеві екрани більшості виробників підтримують тунелювання і шифрування даних. Оскільки ці пристрої призначені для захисту інформаційної взаємодії з відкритими мережами, то при створення на їх базі VPN з'єднання забезпечується комплексний захист інформаційного обміну. Недоліком такої системи можна назвати залежність продуктивності від апаратного забезпечення, на котрому працює мережевий екран.

Реалізовувати VPN на базі маршрутизатора, доцільно в тому випадку, коли локальна мережа організації є доволі невеликою, та в цілях економії фінансових витрат. Прикладом такого обладнання є маршрутизатори Cisco, котрі починаючи з версії IOS 11.3 підтримують L2TP та IPSec. Про варто зазначити, що під час криптографічного опрацювання пакетів задіюється більше ресурсів пристроїв. Для підвищення продуктивності маршрутизатора можна додатково використати модуль шифрування ESA.

Програмне рішення для VPN це, як правило, готовий застосунок, котрий встановлюється на підключеному до мережі ПК. Із міркувань безпеки та продуктивності, для встановлення таких програм найкраще виділяти окремий ПК, котрий буде виступа в ролі сервера; для клієнтського пристрою такі дії вико-

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росінський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

нувати не потрібно. Загалом такі рішення складніше для розгортання та обслуговування ніж ті, котрі базуються на апаратних засобах, а також, в своїй більшості, не є безкоштовними продуктами, що тягне за собою додаткові витрати.

В якості мережевої ОС, як приклад, можна використовувати Windows Server з виділеною IP адресою. Це дозволяє застосовувати базу користувачів котра вже існує в організації, легко конфігурувати параметри з'єднання, та не залучати додаткових коштів. Проте в ході незалежних тестувань було з'ясовано що існують помилки та слабкі місця в самій ОС, що ставить під загрозу данні, котрі будуть передаватися таким з'єднанням.

1.3 Протоколи для реалізації Remote Access VPN

Протокол VPN визначає, яким чином система VPN взаємодіє з іншими системами в інтернеті, а також рівень захищеності трафіку. Протокол VPN впливає на загальний рівень безпеки системи, оскільки протокол VPN використовується для обміну ключами шифрування між двома кінцевими вузлами. Якщо цей обмін не захищений, зловмисник може перехопити ключі і потім розшифрувати трафік, звівши нанівець всі переваги VPN. Як правило, на сьогоднішній день для побудови мереж VPN використовуються протоколи наступних рівнів:

- каналний рівень (PPTP, L2TP);
- мережевий рівень (IPSec);
- транспортний рівень (TLS);

PPTP – тунельний протокол типу «точка-точка», котрий дозволяє віддаленому вузлу встановлювати захищене з'єднання з сервером за рахунок створення тунелю в звичайній незахищеній мережі. Він був розроблений компаніями Microsoft та 3Com з метою надання безпечного віддаленого доступу до корпоративних мереж через мережу Інтернет. Даний протокол підтримує шифрування та інкапсуляцію мультпротокольного трафіку з використанням IP-заголовку для відправки по IP-мережам.

Протокол PPTP інкапсулює PPP-кадри в IP-датаграми для передачі даних по мережі. Для керування тунелем використовується TCP-з'єднання на 1723

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росієнський Ю. М.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

порті, а також модифікована версія протокола GRE для інкапсуляції PPP-кадрів. Корисні дані інкапсульованих PPP-кадрів можуть бути шифрованими та/чи стиснутими.

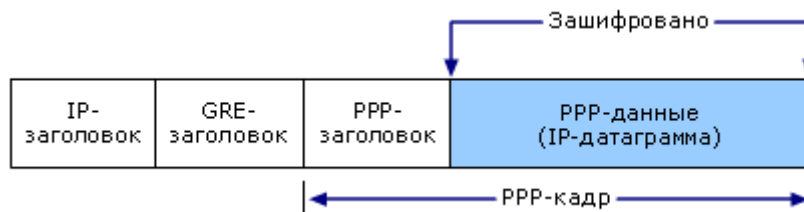


Рисунок 1.3 – Кадр PPTP

Кадр PPP поміщується в оболонку з заголовком GRE і заголовком IP. В заголовку IP-адреса джерела та приймача відповідають VPN-клієнту та VPN-серверу. Заголовок GRE складається з двох частин по два байти де перші два байти містять в собі поля контрольних сум, ключа, порядковий номер та версію GRE, а третій та четвертий містять в собі тип протоколу інкапсульованого пакету.

Як правило в PPTP для аутентифікації використовується MS-CHAP v.2, проте можуть бути використані і інші методи, такі EAP, CHAP, MS-CHAP v.1, SPAP та PAP. Через свою простоту він присутній, на сьогоднішній день, майже у всіх операційних системах. Головною його перевагою є незначне використання обчислювальних ресурсів і з цього випливає його висока швидкість роботи. Проте його базові протоколи аутентифікації мають проблеми з вразливістю, і як наслідок Microsoft рекомендувала для використання інші VPN-протоколи.

З'єднання L2TP, котрі іноді називають віртуальними лініями, – спосіб підключення віддалених користувачів, де їх IP адресами керує корпоративна система під'єднана до мережі. Даний протокол є розширенням протоколу PPP і об'єднує в собі функції PPTP і L2F.

L2TP підтримує тунелі двох типів: обов'язкові та необов'язкові. Головна відмінність між ними складається в тому, яка система бере на себе роль кінцевої точки тунелю: кінцевою точкою необов'язкового тунеля є віддалений клієнт, а обов'язкового – ISP.

У випадку обов'язкового тунелю L2TP, віддалений вузол встановлює з'єднання зі своїм провайдером. Після цього ISP встановлює з'єднання L2TP між віддаленим користувачем і корпоративною мережею. При цьому користувач може самостійно обрати необхідні засоби захисту даних, котрі надаються VPN. Для застосування обов'язкового тунелю, ISP повинен підтримувати протокол L2TP.

У випадку необов'язкового тунелю, L2TP з'єднання встановлюється віддаленим користувачем. Зазвичай для цього застосовується клієнт тунелів L2TP. Віддалений користувач надсилає пакети L2TP своєму ISP, котрий пересилає їх в корпоративну мережу. Для функціонування необов'язкового тунелю, не потребується підтримка провайдером L2TP.

L2TP використовує два види пакетів: інформаційні та керуючі. Керуючі пакети встановлюють та підтримують тунельне з'єднання. Вони надсилаються через надійний керуючий канал, котрий передає пакети в межах того ж пакетного транспортування. Інформаційні пакети інкапсулюють PPP-кадри, що надсилаються через тунель, та у випадку їх втрати повторно не надсилаються.

Хоч протокол і використовується для створення VPN-з'єднань, сам по собі він не може забезпечити конфіденційність чи аутентифікацію, котрі є важливими параметрами VPN-з'єднань, тому найчастіше він застосовується в парі з IPsec, котрий забезпечує безпеку з'єднання.

IPsec – структура відкритих стандартів для забезпечення конфіденційних, безпечних з'єднань через IP-мережі. Цей метод підтримує аутентифікацію сторін на мережевому рівні, перевірку достовірності джерела даних, їх цілісність і конфіденційність, а також захист від повторного відтворення. Специфіка IPsec, складається в тому, що він реалізується на мережевому рівні, доповнюючи його таким чином, щоб для наступних рівнів мережі все відбувалось непомітно. IPsec складається з трьох основних частин: AH, ESP, IKE.

Протокол AH додає в пакет спеціальний заголовок з контрольним значенням. Він забезпечує ідентифікацію відправника, цілісність даних і їх захист від відтворення. На практиці він використовується рідко, оскільки він не забезпечує конфіденційності. Проте його часто використовують в парі з OSPFv3, оскільки

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росієнський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

дана версія протоколу, на відміну від попередника, не пропонує ніякого функціоналу для захисту від підробних анонсів.

Протокол ESP забезпечує конфіденційність, ідентифікацію, перевірку цілісності даних та захист від їх відтворення. Для шифрування даних обидві кінцеві системи використовують спільний ключ. Якщо одночасно застосовуються засоби шифрування і ідентифікації, то віддалена система спочатку ідентифікує пакет, і якщо вона успішна, то розшифровує пакет. Такий спосіб обробки пакетів зменшує навантаження на систему і зменшує ризики втручання в систему через її відмову. Для даного протоколу також визначений перелік обов'язкових алгоритмів – DES, MD5, SHA-1.

Ці протоколи можуть використовуватися одночасно, що дає змогу захистити всю датаграму IP. Це забезпечує більш високий рівень захисту, але і потребує значно більше ресурсів системи. Функціонувати ці протоколи можуть в двох режимах: транспортному і тунельному.

В транспортному режимі шифруються та/чи підписуються тільки данні IP-пакету, а заголовок зберігається. Цей режим використовується для встановлення з'єднання між кінцевими вузлами. Також він може бути використаний між шлюзами для захисту тунелів, котрі організовані іншим протоколом (L2TP).

В тунельному режимі відбувається інкапсуляція IP-пакету. Він використовується для підключення віддалених комп'ютерів до віртуальних приватних мереж, чи передачі даних через відкриті канали зв'язку між шлюзами для з'єднання різних частин віртуальної мережі.

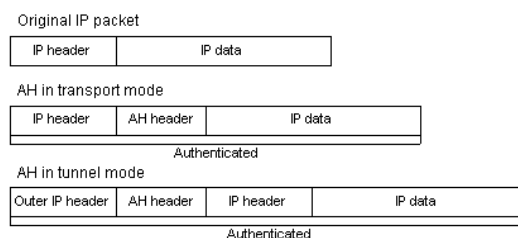


Рисунок 1.4 – AH в транспортному та тунельному режимах

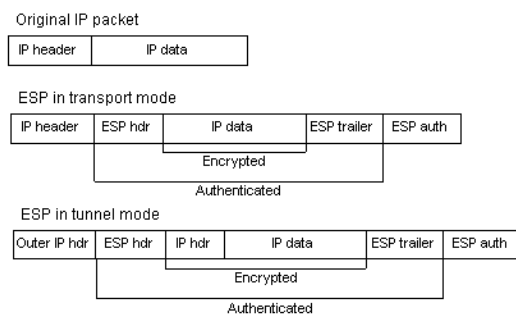


Рисунок 1.5 – ESP в транспортному та тунельному режимах

Протокол обміну ключами IKE призначений для початкового етапу встановлення з'єднання та визначає спосіб ініціалізації захищеного каналу, а також процедури обміну і керування секретними ключами у рамках захищеного з'єднання, методи шифрування і т.д.

Сам по собі IKE є комбінацією трьох протоколів – ISAKMP, Oakley і SKEME. Загальні правила керування безпечним з'єднанням (SA) в IP-мережах визначає протокол ISAKMP. Проте він задає тільки послідовність етапів встановлення безпечного з'єднання, формати пакетів для встановлення і розриву з'єднання, вимоги до процедур аутентифікації сторін і обмін секретними ключами, проте самі протоколи аутентифікації сторін в ньому не визначені. Тому розробники протоколу IKE доповнили загальні правила та процедури протоколу ISAKMP процедурами аутентифікації та обміну ключами з протоколів Oakley та SKEME. Оскільки IKE використовує для керування SA алгоритми та формати протоколу ISAKMP, то ці назви іноді використовуються як синоніми.

Аутентифікація сторін в IKE відбувається двома способами. Перший спосіб здійснює аутентифікацію типу «запит-відповідь» з використанням хеш-функції та спільним секретним ключем. В другому використовуються сертифікати відкритих ключів стандарту X.509. Кожна із сторін підписує свій сертифікат своїм секретним ключем і передає ці данні протилежній стороні.

Після встановлення аутентичності сторін, протокол IKE використовує алгоритм Діффі-Хеллмана, за допомогою якого сторони визначають спільний секретний ключ, котрий буде використовуватися в SA протоколами AH і ESP. Якщо тривалість життя ключа закінчується SA розривається і встановлюється нова для якої генерується новий ключ.

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росінський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

Взаємодія протоколів IKE, AH і ESP відбувається наступним чином:

1. За допомогою IKE між двома точками встановлюється SA, та відбувається аутентифікація кінцевих точок, обираються параметри захисту даних.
2. В рамках встановленого SA починають працювати протоколи AH або ESP. Якщо для VPN з'єднання задіяно обидва ці протоколи, то для кожного з них створюється окреме SA.

Базові протоколи IPsec визначені суворо, проте ця система дозволяє забезпечити високу гнучкість за рахунок використання різноматніх алгоритмів аутентифікації та шифрування. Наприклад, вибір в якості алгоритму шифрування DES, ніяк не впливає на вибір функції для вирахування хеш-коду, що використовується для аутентифікації даних.

Хоч IPsec найбільш популярне, та одне з найкращих рішень для створення віртуальних приватних мереж, все ж він має декілька недоліків. При застосуванні його в транспортному режимі не виключається можливість атак зі сторони, що викликано певними обмеженнями ISAKMP. Якщо не використовується заголовок аутентифікації AH, данні зломисника можуть бути поміщені в потік інформації, або у випадку використання Unix-систем, як приклад, при додавання до потоку команду `rm -R`, кінцевий пристрій може залишитися взагалі без файлів.

SSL – криптографічний протокол, розроблений компанією NetScape в 1996 році. На сьогодні він інтегрований в більшість браузерів і веб-серверів, оскільки забезпечує захищеним обміном даними через мережу Інтернет.

Серед методів аутентифікації в даному протоколі може використовуватися як передача паролів у вигляді звичайного тексту так і до використання спеціальних захищених фізичних носіїв з окремими сертифікатами аутентифікації та авторизації. SSL підтримує три типи аутентифікації:

- аутентифікація обох сторін (клієнт-сервер);
- аутентифікація сервера з неаутентифікованим клієнтом;
- повна анонімність;

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Россінський Ю. М.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Зазвичай для аутентифікації використовуються алгоритми RSA, DSA, EC-DSA. Якщо сервер аутентифікований, то його повідомлення про сертифікацію повинно забезпечити правильну сертифікаційну послідовність, котра спрямовує до центру сертифікації. Кожна сторона відповідає за перевірку того, що сертифікат іншої сторони не був скасований чи його термін дії не закінчився.

Для шифрування застосовуються RC4, MD5, RSA та інші алгоритми захисту даних. SSL використовує два ключі – відкритий та приватний, котрий відомий тільки отримувачу повідомлення.

1.4 Постановка технічного завдання

Метою кваліфікаційної роботи є проектування та побудова підсистеми захищеного вітдаленого доступу користувачів до ресурсів мережі організації на базі технологій Remote Access VPN, що передбачає виконання наступних завдань:

1. Розробка фізичної топології мережі;
2. Розробка логічної топології мережі;
3. Проектування системи вітдаленого доступу;
4. Вибір мережевого обладнання;
5. Вибір операційних систем для робочих станцій та серверів;
6. Налаштування необхідних функцій на мережевому обладнанні;
7. Налаштування Windows мережі;
8. Тестування працездатності налагодженої мережі.

При розробці фізичної та логічної топології мережі потрібно врахувати особливості розташування пристроїв комп'ютерної мережі та розробити схему їх підключень. Потрібно розробити логіку взаємодії пристроїв мережі. При аналізі та розробці структури мережі необхідно обрати операційні системи для робочих станцій та врахувати особливості роботи серверів.

Після проектування усіх вищевказаних пунктів потрібно перейти до налаштування функцій вітдаленого доступу до мережі організації за допомогою

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Россінський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

функцій Remote Access VPN. Також необхідно налаштувати сервери та усі кінцеві вузли.

Після налагодження усього необхідного обладнання необхідно провести тестування працездатності підсистеми та перевірити правильність виконання усіх поставлених задач.

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Россінський Ю. М.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ ТА ПІДСИСТЕМИ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ КОРИСТУВАЧІВ НА БАЗІ ТЕХНОЛОГІЙ REMOTE ACCESS VPN

2.1 Розробка фізичної топології мережі

Проект загальної мережі (додаток А) складається з чотирьох складових: локальної мережі організації, двох проміжних мереж (інтернет-провайдерів), та домашньої мережі віддаленого користувача.

Локальна мережа організації побудована за ієрархічним принципом, така мережа ще називається розширеною зіркою. Вона складається з трьох рівнів: базовий, поширення, доступу. Кожен з цих рівнів відповідає за реалізацію певних функцій, проте вони є логічними і не завжди погоджені з фізичними пристроями.

Базовий рівень формує ядро мережі, він відповідає за швидку та надійну пересилку великих об'ємів трафіку.

Рівень поширення відповідає за маршрутизацію, фільтрацію і доступ.

Рівень доступу реалізовується управління користувачами і робочими групами. Найбільша частина необхідних користувачам мережевих ресурсів має знаходитися саме на цьому рівні.

В даній мережі рівень ядра складається з одного пристрою – міжмережного екрану ASA1-ORG. Рівень поширення складається з двох комутаторів: SW_ORG_1 та SW_ORG_2. Рівень доступу представлений трьома комутаторами та під'єднаних до них кінцевих пристроїв.

Даний тип топології був обраний, тому що він зможе забезпечити розширення мережі без внесення змін у конфігурацію мережевих пристроїв.

Мережі інтернет провайдерів складаються з одного маршрутизатора та одного комутатора. Мережі провайдерів з'єднані між собою за допомогою комутатора. До комутаторів будуть під'єднані мережі організації та віддаленого користувача.

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Россінський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

Домашня мережа віддаленого користувача складається з маршрутизатора, комутатора та одного ПК.

2.2 Розробка логічної топології мережі

Адресація усіх пристроїв мережі буде здійснюватися на базі протоколу IPv4.

В домашній мережі віддаленого користувача маршрутизатор буде мати фіксовану IP-адресу, а внутрішнім пристроям видавати адреси за допомогою DHCP з діапазону. На цьому ж маршрутизаторі буде реалізовано NAT, тому внутрішні пристрої не будуть доступними ззовні. Комутатор буде працювати на каналному рівні та матиме фіксовану конфігурацію. Таблиця адресації пристроїв домашньої мережі віддаленого користувача наведена в таблиці 2.4

Таблиця 2.1 – Адресація локальної мережі віддаленого користувача

Пристрій	Інтер-фейс	IP-Адреса	Маска мережі	Префікс
Маршрутизатор Home_Gateway	Fa0/0	10.1.1.2	255.255.255.0	/24
	Fa0/1	192.168.0.1	255.255.255.0	/24
ПК Remote_User	Eth0	DHCP		

Мережі інтернет провайдерів будуть складатися з двох підмереж. Одна з них призначена для адресації пристроїв внутрішньої мережі, інша для зв'язку з провайдерів один з одним. Міжмережний зв'язок буде здійснюватися за допомогою OSPF. Комутатори даних мереж будуть некерованими, тому не матимуть IP-адреси. Адресацію мереж провайдерів наведено в таблиці 2.5

Таблиця 2.2 – Адресація проміжних мереж

Пристрій	Інтер-фейс	IP-Адреса	Маска мережі	Префікс
Маршрутизатор ISP1	Fa0/0	34.135.3.10	255.255.255.248	/29
	Fa0/1	34.135.3.1	255.255.255.248	/29
Маршрутизатор ISP2	Fa0/0	34.135.3.9	255.255.255.248	/29
	Fa0/1	34.135.3.17	255.255.255.248	/29

В локальній мережі організації міжмережний екран матиме виділену IP-адресу, що зробить його доступним із зовнішніх мереж. На мережевому екрані буде налаштовано NAT для внутрішньої мережі. Сервер в матиме статичну IP-адресу. Адресація робочих станцій буде здійснюватися за допомогою DHCP з певного діапазону. Також слід врахувати зовнішню підключення пристрої шляхом віддаленого доступу, вони також потребуватимуть IP-адреси для успішного зв'язку з іншими пристроями в мережі. Хоч і в економії адресного простору немає потреби, проте слід враховувати можливе розширення мережі, та її подальшу сегментацію тому для мережі обрано маску /27. Адресація пристроїв локальної мережі організації наведена в таблиці 2.6.

Таблиця 2.3 – Адресація пристроїв мережі організації

Пристрій	Інтер-фейс	IP-Адреса	Маска мережі	Префікс
Міжмережний екран ASA1-ORG	Gig0/0	34.135.3.18	255.255.255.248	/29
	Gig0/1	192.168.100.1	255.255.255.224	/27
Сервер Main_Server	Eth0	192.168.100.9	255.255.255.224	/27
Робочі станції	Eth0	DHCP		

2.3 Вибір обладнання для реалізації проекту комп'ютерної мережі та підсистеми захищеного віддаленого доступу користувачів

Одним з важливих етапів проектування мережі є вибір обладнання. При виборі слід враховувати сумісність пристроїв, відповідність запланованим технологіям та протоколам, ціну, а також можливі майбутні розширення мережі.

Лідером світового ринку є компанія Cisco Systems. Цей виробник відомий своїми надійними та багатofункціональними пристроями, серед яких присутні рішення як для домашнього користування так і для корпоративних мереж. Тому вибір мережевих пристроїв буде здійснюватися серед продуктів даного виробника.

Міжмережні екрани для малих та середніх підприємств представлені серією ASA 5500-X. В якості мережевого екрану було обрано Cisco ASA 5506-X (рисунок 2.1). Цей пристрій гарантує надійний захист пристроїв на всіх етапах атак та мережевих загроз. Його функції з міжмережного екранування з підтримкою стану з'єднань наступного покоління – Next-Generation Firewall забезпечують гнучкість, прозорість та контроль. Він дозволяє створювати шифровані VPN-з'єднання між філіалами компаній, а також для підключення віддалених користувачів до внутрішньої мережі чи її окремих ресурсів. Технічні характеристики пристрою наведені в таблиці Б.1.

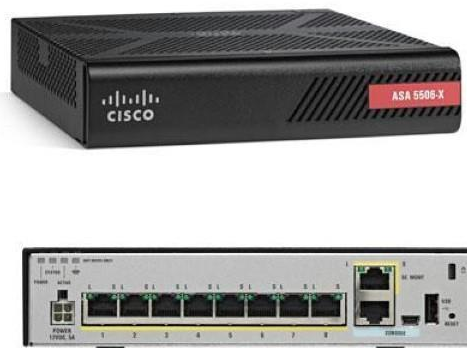


Рисунок 2.1 – Cisco ASA 5506-X

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росінський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

При виборі некерованого комутатора найголовнішим критерієм є кількість та швидкість портів, оскільки вони мають забезпечувати якісний зв'язок, та мати резерв портів при підключенні нових пристроїв.

В якості некерованого комутатора було обрано Cisco CBS110-16T-EU (рисунок 2.2). Це економічний комутатор бізнес серії з підтримкою гігабітних підключень для невеликих мереж. Перевагами даного комутатора є його енергоефективність, виявлення петель, діагностика підключень. Детальні характеристики пристрою наведені в таблиці Б.2



Рисунок 2.2 – Cisco – CBS110-16T-EU

Хоч в спроектованій мережі маршрутизатор не відіграє провідну роль, проте підтримка визначених технологій та параметрів необхідні для повноцінного функціонування проект. При виборі моделі маршрутизатора потрібно враховувати як він маршрутизує пакети в складній мережі з різними видами топологій. Маршрутизатор має містити достатню кількість портів, забезпечувати необхідну швидкість передачі та обробки даних.

В якості маршрутизатора було обрано Cisco 3745 (рисунок 2.3). Це компактний пристрій котрий є хорошим рішенням для організації локальних мереж малих та середніх підприємств. Хоча він і має 2 порти 10/100Base-TX, проте є можливості для додаткового розширення: три слоти для WAN інтерфейсних модулів (WIC), чотири слоти для мережевих модулів (NM), та два внутрішніх слоти для встановлення сервісних модулів (AIM). Оснащений даний маршрутизатор 128 Мб оперативної пам'яті, та 32 Мб флеш-пам'яті.

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росінський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24



Рисунок 2.3 – Cisco 3745

2.4 Вибір програмного забезпечення для реалізації проекту комп'ютерної мережі та підсистеми захищеного віддаленого доступу користувачів

При виборі сімейства операційних систем потрібно враховувати наступні фактори:

- підтримка великого спектру периферійного обладнання;
- наявність необхідного програмного забезпечення для забезпечення виробничих потреб організації;
- стійкість проти вірусів;
- захист системних файлів та файлів користувачів від навмисного чи наневмисного внесення змін чи видалення;
- технічна підтримка та документація;
- вимоги до апаратного забезпечення;
- ліцензійність ОС та програмного забезпечення;

На даний момент двома найбільш популярними сімействами операційних систем є сімейства Windows та Linux.

Операційні системи сімейства Windows розповсюджуються на комерційній основі, мають зручний графічний інтерфейс, та постійні оновлення актуальних версій, що усувають наявні недоліки та вразливості системи. На сьогодні вони підтримують більшість наявних периферійних пристроїв, а більшість програм, що розробляються орієнтуються на дану платформу. Хоч самі ОС даного сімейства мають закритий вихідний код, вони мають багато вразливостей, на основі яких створюються вірусне ПЗ. Також дане сімейство

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росініський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

операційних систем характерне своєю надлишковістю, при встановленні системи в ній одразу буде безліч служб та функцій, які можуть ніколи і не використовуватися, проте будуть здійснювати навантаження на ресурси пристрою.

Лінійка операційних систем представлена двома типами рішень: для персональних комп'ютерів та серверів. Останньою версією для персональних комп'ютерів є Windows 10, а її серверного аналога Windows Server 2019. Microsoft перейшла на модель оновлення «Windows як послуга», і замість випуску нової Windows, компанія двічі на рік випускає нові RTM збірки. Вимоги даних операційних систем до апаратного забезпечення наведені в таблиці 2.4.

Таблиця 2.4 – Мінімальні вимоги операційних систем Windows

Параметри	Windows 10	Windows Server 2019
Процесор	1 ГГц+	1.4 ГГц, 64-бітний
Оперативна пам'ять	1 Гб для 32-розрядної версії та 2 Гб для 64	512 Мб, для консольної версії та 2 Гб для графічного інтерфейсу
Місце на жорсткому диску	16 Гб для 32-розрядної та 32 Гб для 64	34 Гб
Відеоадаптер	З підтримкою DirectX 9 або новішої версії з драйвером WDDM 1.0	Для графічного інтерфейсу підтримка DirectX 9 або новішої версії з драйвером WDDM 1.0
Монітор	800x600	

Хоча і офіційно заявлені компанією Microsoft необхідні характеристики невеликі, як показує практика, для стабільної роботи пристрою вони повинні бути вдвічі вищими.

Сімейство операційних систем Linux представлене різноманітними рішеннями як для персональних комп'ютерів так і для серверів. Більшість дистрибутивів є безкоштовними чи умовно-безкоштовними, проте незважаючи на це, порівняно з ОС Windows, дистрибутиви на ядрі Linux мають менше вразливостей. Більшість операційних систем даного сімейства не вимогливі до апаратного забезпечення, проте при встановленні драйверів до них можуть виникати труднощі. Спектр програмного забезпечення, котре могло б використовуватися для корпоративних потреб, менший чим у того ж сімейства Windows.

Серед рішень для корпоративних мереж можна виділити такі як Ubuntu Desktop та Ubuntu Server. Хоча обидві редакції і використовують одні і ті ж репозиторії, що дозволяє легко встановлювати серверні додатки як на Desktop Edition так і на Server Edition, головною різницею між ними є відсутність у Server Edition віконного інтерфейсу на етапі процесу встановлення системи та в опціях ядра.

Вимоги актуальних версій операційних систем Ubuntu Desktop та Ubuntu Server наведені у таблиці 2.5

Таблиця 2.5 – Мінімальні вимоги систем Ubuntu

Параметри	Desktop	Server
Процесор	Двоядерний, 2 ГГц	Одноядерний, 2 ГГц
Оперативна пам'ять	4 Гб	2 Гб
Місце на жорсткому диску	25 Гб	10 Гб
Відеоадаптер / Монітор	VGA з розширенням 1024x768	Будь-яка графічна карта та монітор розширення 640x480

Хоча і операційні системи сімейства Linux мають значно більше переваг, такі як продуктивність, надійність, краща безпека, проте вони є досить складними для пересічного користувача, тому в якості операційних систем було обрано для робочих станцій було обрано Windows 10 Pro та для серверів Windows Server 2019.

2.5 Проектування системи віддаленого доступу

Систему віддаленого доступу буде реалізована на базі міжмережного екрану Cisco ASA 5506-X. Хоча компанія Cisco рекомендує виділяти окремий пристрій для встановлення VPN-з'єднань, дана реалізація в поточному проекті була б надлишковою.

Формування VPN-з'єднання буде здійснюватися за допомогою SSL/IKEv2. Параметри шифрування та хешування будуть обрані відповідно до можливо-

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росієнський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

стей міжмережного екрану. Хоча базова ліцензія дозволяє одночасне підключення двох користувачів, проте додатковими ліцензіями можна збільшити число одночасно підключених користувачів, так і розширити функціонал та можливості самого міжмережного екрану.

Аутентифікація користувачів буде здійснюватися шляхом перевірки логіну та паролю, її можна здійснювати як і за допомогою локальної бази даних міжмережного екрану, так і за допомогою серверів Radius та Tacs+. Оскільки в якості серверної операційної системи було обрано Windows Server 2016, цілком доцільно реалізувати на базі головного серверу Radius-сервер, котрий буде аутентифікувати користувачів на основі визначеної групової політики.

Вибір методів аутентифікації між Radius-сервером та міжмережним екраном не є принциповим, оскільки передача даних буде здійснюватися у внутрішній частині мережі, тому шанси витоку даних мінімальні.

Здійснювати підключення зі сторони клієнта можна за допомогою функціоналу вбудованого у ОС Windows, за допомогою браузера, чи клієнта Cisco Anyconnect. Також серед клієнтів був актуальним Cisco VPN client, він хоч і передбачав найбільш детальний спосіб налаштування клієнтської сторони, проте, на сьогодні, він не підтримується та не може бути встановленим на робочі станції під керівництвом ОС Windows 64-бітної версії. VPN клієнти сторонніх виробників не розглядаються з міркувань безпеки. Оскільки підключення здійснюватиметься за допомогою SSL/IKEv2 в якості клієнту було обрано сучасний Cisco Anyconnect, щоб користувач був логічно підключеним до внутрішньої мережі.

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росініський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ РОБОТИ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ПІДСИСТЕМИ ЗАХИЩЕНОГО ВІДДАЛЕ- НОГО ДОСТУПУ КОРИСТУВАЧІВ

3.1 Налаштування мережевих пристроїв та домену Windows

Налагодження модельного прикладу мережі буді здійснюватися за допомогою програми GNS3 з симуляцією мережі, та емулюванням операційних систем мережевих пристроїв, емуляція операційних систем робочих станцій буде здійснюватися за допомогою VirtualBox.

Спочатку налагодимо локальну мережу віддаленого користувача. Задамо IP-адреси інтерфейсам, визначимо пул адрес для DHCP, виключимо з пулу для видачі адресу, котра призначена внутрішньому інтерфейсу маршрутизатора, а також пропишемо маршрут для пристроїв, та налаштуємо трансляцію адрес:

```
...
Home_Gateway(config)#int fa0/1
Home_Gateway(config-if)#ip add 192.168.0.1 255.255.255.0
Home_Gateway(config-if)#no sh
Home_Gateway(config-if)#exit
Home_Gateway(config)#ip dhcp excluded-address 192.168.0.1
Home_Gateway(config)#ip dhcp pool HOME
Home_Gateway(dhcp-config)#network 192.168.0.0 255.255.255.0
Home_Gateway(dhcp-config)#default-router 192.168.0.1
Home_Gateway(dhcp-config)#exit
Home_Gateway(config)#int fa0/0
Home_Gateway(config-if)#ip add 34.135.3.2 255.255.255.248
Home_Gateway(config-if)#no sh
Home_Gateway(config-if)#exit
Home_Gateway(config)#ip route 0.0.0.0 0.0.0.0 fa0/0
Home_Gateway(config)#ip access-list standard ACL_NAT
Home_Gateway(config-std-nacl)#permit 192.168.0.0 0.0.0.255
Home_Gateway(config-std-nacl)#int fa0/1
Home_Gateway(config-if)#ip nat inside
Home_Gateway(config-if)#exit
Home_Gateway(config)#int fa0/0
Home_Gateway(config-if)#ip nat outside
Home_Gateway(config-if)#ip nat inside source list ACL_NAT interface fa0/0
Home_Gateway(config)#exit
Home_Gateway#copy ru st
...
```

		Гнатюк Д.І.		
		Росієнський Ю. М.		
Змн.	Арк.	№ докум.	Підпис	Дата

Наступним кроком налаштуємо проміжні мережі інтернет провайдерів. Для цього потрібно задати IP-адреси інтерфейсам та налаштувати OSPF. Конфігурації пристроїв будуть здійснюватися аналогічним чином.

Конфігурація R_ISP1_1:

```
...
R_ISP1_1#conf t
R_ISP1_1(config)#int fa0/1
R_ISP1_1(config-if)#ip add 34.135.3.1 255.255.255.248
R_ISP1_1(config-if)#no sh
R_ISP1_1(config-if)#exit
R_ISP1_1(config)#int fa0/0
R_ISP1_1(config-if)#ip add 34.135.3.10 255.255.255.248
R_ISP1_1(config-if)#no sh
R_ISP1_1(config-if)#exit
R_ISP1_1(config)#router ospf 1
R_ISP1_1(config-router)#network 34.135.3.0 0.0.0.7 area 1
R_ISP1_1(config-router)#network 34.135.3.8 0.0.0.7 area 1
R_ISP1_1(config-router)#exit
...
```

Конфігурація R_ISP2_1:

```
...
R_ISP2_1(config)#int fa0/0
R_ISP2_1(config-if)#ip add 34.135.3.9 255.255.255.248
R_ISP2_1(config-if)#no sh
R_ISP2_1(config-if)#exit
R_ISP2_1(config)#int fa0/1
R_ISP2_1(config-if)#ip add 34.135.3.17 255.255.255.248
R_ISP2_1(config-if)#no sh
R_ISP2_1(config-if)#exit
R_ISP2_1(config)#router ospf 1
R_ISP2_1(config-router)#network 34.135.3.8 0.0.0.7 area 1
R_ISP2_1(config-router)#network 34.135.3.16 0.0.0.7 area 1
...
```

Наступним кроком налаштуємо міжмережний екран ASA. Для початку задамо IP-адреси, імена та опис для мережевих інтерфейсів і визначимо для них рівні безпеки. Хоч і рівень безпеки за замовчування для outside становить 0, а для inside – 100, на всяк випадок введемо відповідні команди.

```
...
ciscoasa(config)# interface gig0/0
ciscoasa(config-if)# nameif outside
```

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росієнський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

```

ciscoasa(config-if)# description Provider
ciscoasa(config-if)# ip address 34.135.3.18 255.255.255.248
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# no sh
ciscoasa(config-if)# exit
ciscoasa(config)# int gig0/1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# description Organization
ciscoasa(config-if)# ip add 192.168.100.1 255.255.255.224
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no sh
ciscoasa(config-if)# exit
...

```

Налаштуємо роботу OSPF для всіх визначених на міжмережному екрані мереж:

```

...
ciscoasa(config)# router ospf 1
ciscoasa(config-router)# network 34.135.3.16 255.255.255.248 area 1
ciscoasa(config-router)# network 192.168.100.0 255.255.255.224 area 2
...

```

Для інтерфейсів, що знаходяться в зоні inside, налаштуємо DHCP з розрахунком на 11 пристроїв, час дії виданої адреси встановимо на 2 години, а шлюзом визначимо даний інтерфейс з іменем inside.

```

...
ciscoasa(config)# dhcpd address 192.168.100.10-192.168.100.20 inside
ciscoasa(config)# dhcpd lease 7200
ciscoasa(config)# dhcpd option 3 ip 192.168.100.1
ciscoasa(config)# dhcpd enable inside
ciscoasa(config)#
...

```

Створимо об'єкт на основі внутрішньої мережі, та застосуємо до нього динамічний NAT:

```

...
ciscoasa(config-router)# object network inside-subnet
ciscoasa(config-network-object)# subnet 192.168.100.0 255.255.255.224
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
ciscoasa(config-network-object)# exit
ciscoasa(config)#
...

```

Налаштуємо SSH для конфігурування пристрою з внутрішньої мережі. Для цього створимо локального користувача, визначимо інтерфейс, з підмережі якого

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росієнський Ю. М.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

можна здійснювати підключення, а також створимо новий пароль для увімкнення режиму конфігурування. Також потрібно буде регенерувати новий ключ RSA. Оскільки налаштування імені було пропущеним, здійснимо ще налаштування імені пристрою

```
...
ciscoasa(config-pmap)# enable password koloraten
ciscoasa(config)# username sysadmin password 4f6pkoloraten privilege 15
ciscoasa(config)# crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.
Do you really want to replace them? [yes/no]: y
Keypair generation process begin. Please wait...
ciscoasa(config)# aaa authentication ssh console LOCAL
ciscoasa(config)# ssh 192.168.100.0 255.255.255.0 inside
ciscoasa(config)# hostname ASA1-ORG
ASA1-ORG(config)#
...
```

Налагодження мережевого домену розпочнемо зі створення віртуальної машини в середовищі емулятора VirtualBox. Фізичні параметри створюваної машини наведені на рисунку 3.1.

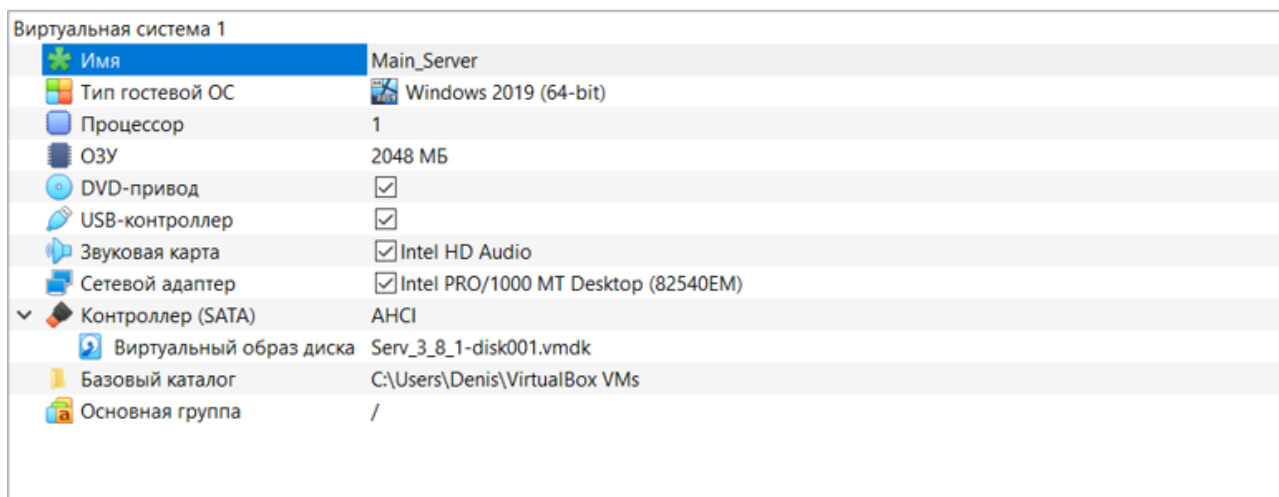


Рисунок 3.1 – Параметри емульованого пристрою

Після встановлення операційної системи Windows Server 2019 необхідно встановити на ньому необхідні ролі та компоненти для функціонування Active Directory. Також серед обраних ролей серверу присутня “Служба полики сети и доступа” за допомогою якої вподальшому буде налаштовано Radius-сервер. Обрані параметри відображені на рисунку 3.2

		Гнатюк Д.І.			KIK.KP.B – 123 – 04 – ПЗ	Арк.
		Росси́нский Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

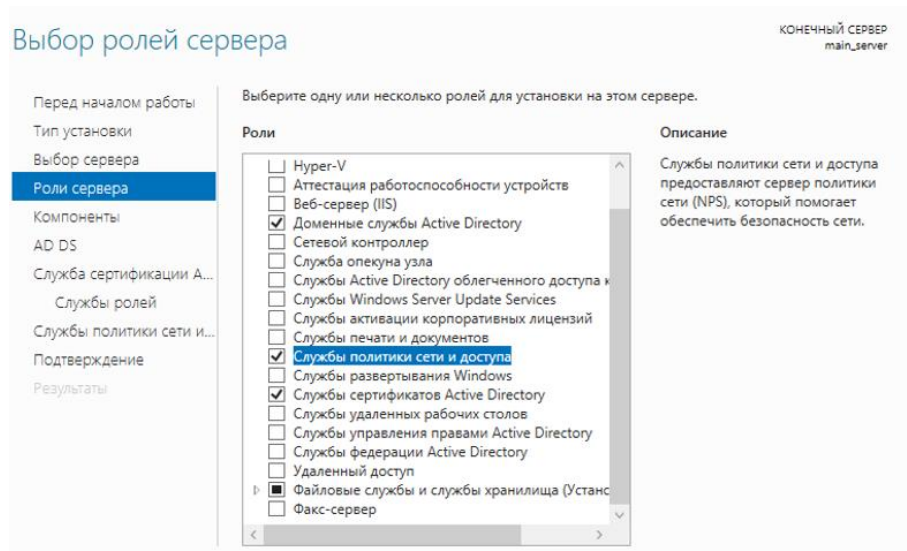


Рисунок 3.2 – Обрані до встановлення ролі

Коли встановлення компонентів завершиться, необхідно перезавантажити машину, щоб зміни прийшли в дії. Після цієї операції можна приступити до налаштування нового лісу. Ім'я встановимо gnatyuk.com, режим роботи лісу та домену – Windows Server 2016. Також необхідно задати пароль для режиму відновлення служб каталогів. Після встановлення цих параметрів почнеться процес інсталяції, і по її завершенню необхідно буде перезавантажити пристрій.

Наступним кроком для головного серверу задамо IP-адресу в параметрах мережевого адаптеру (рисунок 3.3).

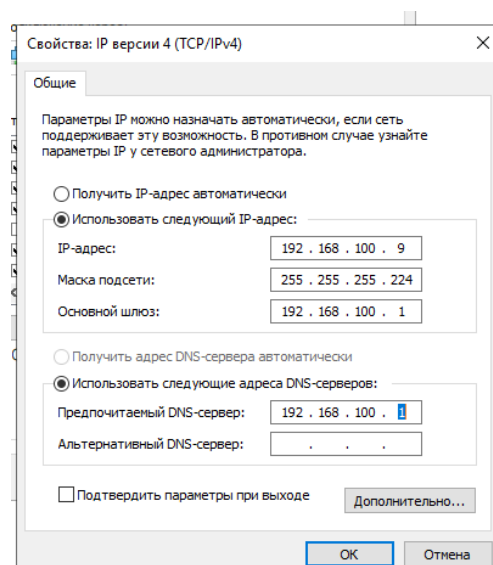


Рисунок 3.3 – Налаштування параметрів IP адаптеру

Інші пристрої будуть отримувати IP-адреси за допомогою DHCP.

		Гнатюк Д.І.			KIK.KP.B – 123 – 04 – ПЗ	Арк.
		Росінський Ю. М.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2 Налаштування підсистеми віддаленого доступу

Першим етапом налаштування підсистеми захищеного віддаленого доступу буде налаштування Radius-сервера на базі Windows Server. Спочатку на контролері домену створимо групу RemoteAccess (рисунок 3.4), в котру будуть включатися користувачі, котрим буде дозволено здійснювати віддалене підключення.

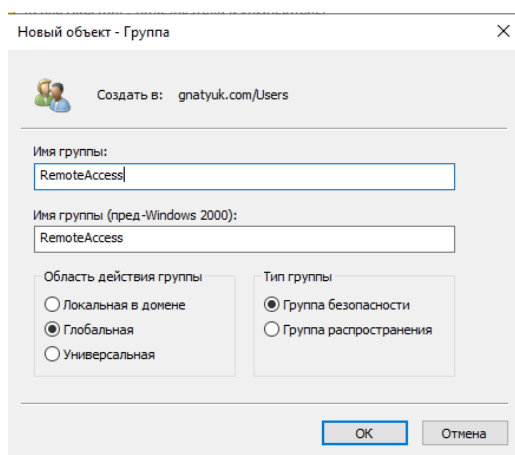


Рисунок 3.4 – Створення групи

Надалі на NPS додати новий Radius-клієнт, котрий буде відповідати нашому міжмережному екрану, задати його ім'я та IP-адресу, а також пароль для встановлення зв'язку.

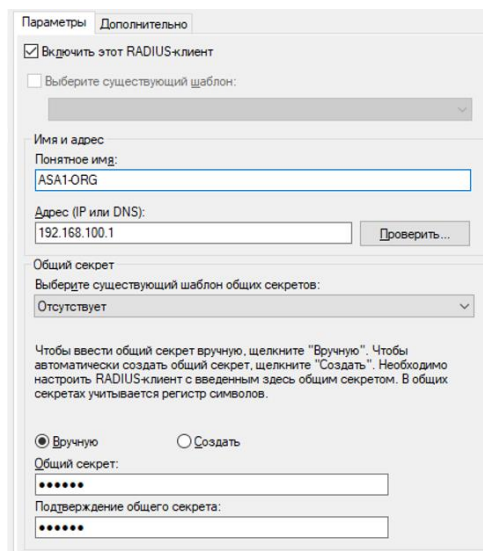


Рисунок 3.5 – Налаштування Radius-клієнта

Після цього потрібно створити дві мережеві політики, одна для підключення пристрою, інша для визначення групи користувачів, котрим дозволено аутентифікуватися даним методом. В нашому випадку це група RemoteAccess.

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росінський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

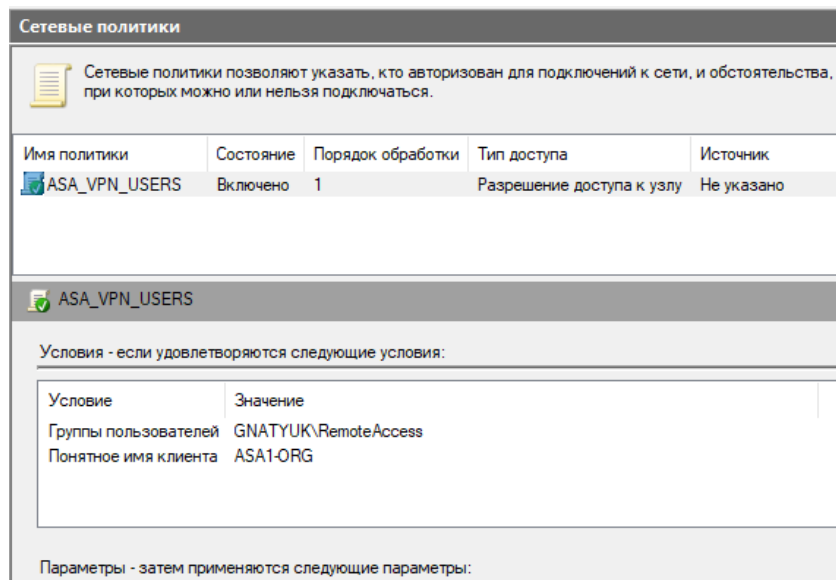


Рисунок 3.6 – Налаштовані мережеві політики

Другим етапом буде налаштування міжмережного екрану ASA1-ORG. Спочатку здійснимо налаштування aaa-серверу. Для цього потрібно задати ім'я групі серверів, визначити протокол та мережу в якій він розташований, задати його IP-адресу, а також пароль, котрий був раніше сконфігурований на Radius-сервері.

```
...
ASA1-ORG(config)# aaa-server win-serv protocol radius
ASA1-ORG(config-aaa-server-group)# exit
ASA1-ORG(config)# aaa-server win-serv (inside) host 192.168.100.9
ASA1-ORG(config-aaa-server-host)# key radeon
ASA1-ORG(config-aaa-server-host)# exit
ASA1-ORG(config)#
...
```

Наступним кроком налаштуємо діапазон адрес, котрі будуть видаватися віддаленим користувачам:

```
...
ASA1-ORG(config)# ip local pool VPN-POOL-1 192.168.100.21-192.168.100.25 mask
255.255.255.224
...
```

Сформуємо список криптографічних перетворень котрі будуть надсила-
тися клієнту. В якості протоколу оберемо ESP, шифрування встановимо aes-
256, хешування sha-1 та md5.

```
...
ASA1-ORG(config)# crypto ipsec ikev2 ipsec-proposal AES256
```

```
ASA1-ORG(config-ipsec-proposal)# protocol esp encryption aes-256
ASA1-ORG(config-ipsec-proposal)# protocol esp integrity sha-1 md5
ASA1-ORG(config-ipsec-proposal)# crypto ipsec security-association pmtu-aging $
...
```

Створимо нову динамічну криптографічну мапу, та застосуємо до неї визначений раніше список криптографічних перетворень. Варто зауважити, що списків криптографічних перетворень можна призначати декілька, і вони будуть перебиратися по порядку визначеності.

```
...
ASA1-ORG(config)# crypto dynamic-map VPN-MAP 65535 set ikev2 ipsec-proposal
AES256
ASA1-ORG(config)# crypto map outside_map 65535 ipsec-isakmp dynamic VPN-MAP
ASA1-ORG(config)# crypto map outside_map interface outside
...
```

Наступним кроком створимо новий RSA-ключ з міткою sslvpnkey, та за допомогою нього підпишемо новостворений сертифікат.

```
...
ASA1-ORG(config)# crypto key generate rsa label sslvpnkey
INFO: The name for the keys will be: sslvpnkey
Keypair generation process begin. Please wait...
ASA1-ORG(config)# crypto ca trustpoint localtrust
ASA1-ORG(config-ca-trustpoint)# enrollment self
ASA1-ORG(config-ca-trustpoint)# fqdn none
ASA1-ORG(config-ca-trustpoint)# subject-name cn=192.168.100.1, CN=ASA1-ORG
ASA1-ORG(config-ca-trustpoint)# keypair sslvpnkey
ASA1-ORG(config-ca-trustpoint)# crl configure
ASA1-ORG(config-ca-crl)# crypto ca trustpool policy
ASA1-ORG(config-ca-trustpool)# auto-import
...
```

Далі оберемо клієнт Anyconnect, увімнемо webvpn, створимо групову політику, в якій вкажемо протокол ikev2 та підключення за допомогою клієнту. Також необхідно задати розділення тунелів, щоб криптографічно оброблявся трафік, котрий проходить тільки у внутрішню мережу. Також додамо ще один NAT, щоб не відбувалась трансляція адрес на захищений канал.

```
...
ASA1-ORG(config)# access-list SPLIT-ACL standard permit 192.168.100.0
255.255.255.224
```

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росінський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

```

ASA1-ORG(config)# nat (inside,outside) source static any any destination stati$
ASA1-ORG(config-webvpn)# group-policy VPN-GROUP-POLICY internal
ASA1-ORG(config)# group-policy VPN-GROUP-POLICY attributes
ASA1-ORG(config-group-policy)# vpn-tunnel-protocol ikev2 ssl-client
ASA1-ORG(config-group-policy)# split-tunnel-policy tunnelspecified
ASA1-ORG(config-group-policy)# split-tunnel-network-list value SPLIT-ACL
ASA1-ORG(config-group-policy)#

```

...

Створимо тунелюну групу та визначимо її тип як remote-access. В її атрибути вкажемо раніше створений діапазон адрес для віддалених користувачів, групу серверів для аутентифікації, групову політику VPN-GROUP-POLICY. Також вкажемо alias для створеної групи.

...

```

ASA1-ORG(config)# crypto ikev2 enable outside client-services port 443
ASA1-ORG(config-group-policy)# tunnel-group RA-VPN type remote-access
ASA1-ORG(config)# tunnel-group RA-VPN general-attributes
ASA1-ORG(config-tunnel-general)# authentication-server-group win-serv
ASA1-ORG(config-tunnel-general)# default-group-policy VPN-GROUP-POLICY
ASA1-ORG(config-tunnel-general)#
ASA1-ORG(config-tunnel-general)# tunnel-group RA-VPN webvpn-attributes
ASA1-ORG(config-tunnel-webvpn)# group-alias RA-VPN enable
ASA1-ORG(config-tunnel-webvpn)# tunnel-group RA-VPN general-attributes
ASA1-ORG(config-tunnel-general)# address-pool VPN-POOL-1
ASA1-ORG(config-tunnel-general)#

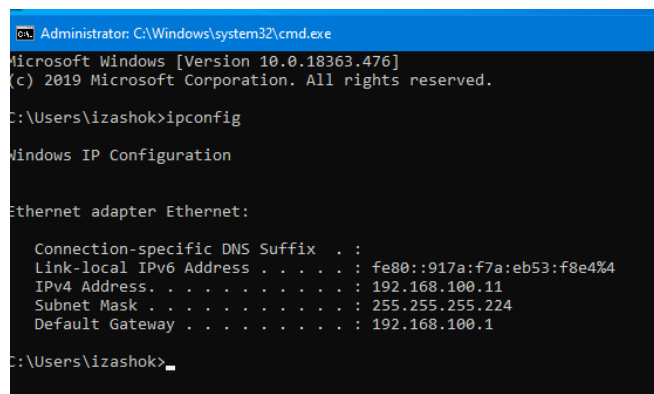
```

...

На цьому налаштування підсистеми віддаленого доступу завершено.

3.3 Тестування роботи мережі та підсистеми захищеного віддаленого доступу

Для початку перевіримо отримання IP-адреси комп'ютерами мережі.



```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.18363.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\izashok>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::917a:f7a:eb53:f8e4%4
    IPv4 Address. . . . . : 192.168.100.11
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : 192.168.100.1

C:\Users\izashok>

```

Рисунок 3.7 – Отримання адреси WS_ORG_1

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росінський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Як видно на рисунку 3.7, пристрій успішно отримав адресу із визначеного раніше діапазону.

Також відобразимо список клієнтів на ASA1_ORG

IP address	Client Identifier	Lease expiration	Type
192.168.100.11	0108.0027.8af8.6c	5995 seconds	Automatic

Рисунок 3.8 – Список клієнтів ASA1_ORG

Наступним кроком перевіримо зв'язок між пристроями. Для цього надішлемо спочатку ICMP запит з роботи станції віддаленого користувача, а після цього скористаємося утилітою tracert.

```
C:\Users\izashok>ping 34.135.3.18

Pinging 34.135.3.18 with 32 bytes of data:
Reply from 34.135.3.18: bytes=32 time=56ms TTL=252
Reply from 34.135.3.18: bytes=32 time=64ms TTL=252
Reply from 34.135.3.18: bytes=32 time=47ms TTL=252
Reply from 34.135.3.18: bytes=32 time=58ms TTL=252

Ping statistics for 34.135.3.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 47ms, Maximum = 64ms, Average = 56ms

C:\Users\izashok>tracert 34.135.3.18

Tracing route to 34.135.3.18 over a maximum of 30 hops:
  0  6 ms   9 ms   9 ms  192.168.0.1
  1  63 ms  30 ms  31 ms  34.135.3.1
  2  57 ms  84 ms  42 ms  34.135.3.9
  3  71 ms  95 ms  52 ms  34.135.3.18

Trace complete.
```

Рисунок 3.9 – Відправка запитів з Remote_User

Як можемо побачити, два віддалені елементи мережі мають зв'язок один з одним.

Виведемо базу даних OSPF на ASA1-ORG за допомогою команди sh ospf database.

```
ASA1-ORG# sh ospf database

OSPF Router with ID (192.168.100.1) (Process ID 1)

Router Link States (Area 1)

Link ID      ADV Router   Age         Seq#         Checksum Link count
34.135.3.10  34.135.3.10  99          0x80000003  0x98f5  2
34.135.3.17  34.135.3.17  1803        0x80000004  0x3774  2
192.168.100.1 192.168.100.1 1802        0x80000002  0x9678  1

Net Link States (Area 1)

Link ID      ADV Router   Age         Seq#         Checksum
34.135.3.9   34.135.3.17  159         0x80000002  0x6dea
34.135.3.17  34.135.3.17  1803         0x80000001  0xf048

Router Link States (Area 2)

Link ID      ADV Router   Age         Seq#         Checksum Link count
192.168.100.1 192.168.100.1 1810        0x80000001  0x1fbd  1
ASA1-ORG#
```

Рисунок 3.10 – База даних OSPF на ASA1-ORG

Наступним кроком спробуємо підключитися до внутрішньої локальної мережі організації по налаштованому захищеному з'єднанню. Для цього запустимо на робочій станції віддаленого користувача програму Anyconnect, введемо адресу сервера VPN. Програма видасть попередження про сертифікат серверу, натискаємо “Connect Anyway”.

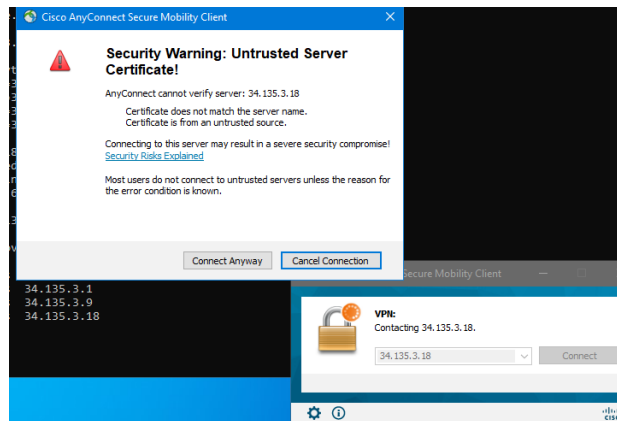


Рисунок 3.11 – Попередження про недовірений сертифікат

Після цього програма виведе діалогове вікно, в якому потрібно ввести корпоративний логін та пароль.

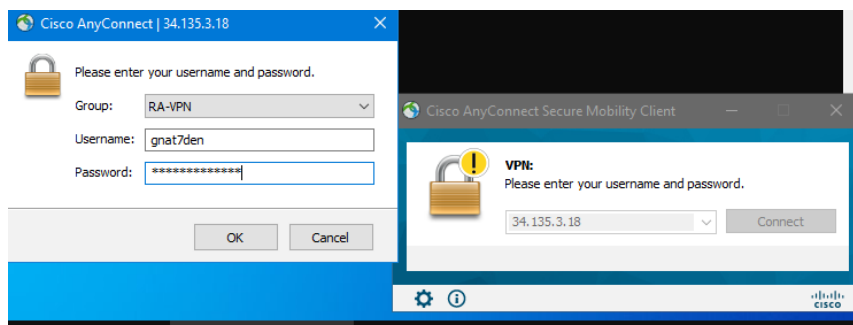


Рисунок 3.11 – Вікно аутентифікації

Після проходження аутентифікації, віртуальний інтерфейс створений програмою Anyconnect має отримати мережеві налаштування від ASA1-ORG.

```
Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::3dcf:70c5:993:2dd5%10
    Link-local IPv6 Address . . . . . : fe80::bae4:5a31:4c2c:5e3d%10
    IPv4 Address. . . . . : 192.168.100.21
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : ::

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::f063:9c47:926e:73d5%4
    IPv4 Address. . . . . : 192.168.0.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

C:\Users\izashok>
```

Рисунок 3.12 – IP-конфігурація мережевих інтерфейсів

		Гнатюк Д.І.			KIK.KP.B – 123 – 04 – ПЗ	Арк.
		Росінський Ю. М.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

Як бачимо, пристрій отримав IP-адресу від ASA1-ORG, тому наступним кроком перевіримо зв'язок між пристроями через захищений канал зв'язку. Надішлемо ICMP запити до пристроїв WS_ORG_1 та Main_Server.

```
C:\Users\izashok>ping 192.168.100.9
Pinging 192.168.100.9 with 32 bytes of data:
Request timed out.
Reply from 192.168.100.9: bytes=32 time=63ms TTL=128
Reply from 192.168.100.9: bytes=32 time=44ms TTL=128
Reply from 192.168.100.9: bytes=32 time=39ms TTL=128

Ping statistics for 192.168.100.9:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 39ms, Maximum = 63ms, Average = 48ms

C:\Users\izashok>ping 192.168.100.11
Pinging 192.168.100.11 with 32 bytes of data:
Request timed out.
Reply from 192.168.100.11: bytes=32 time=77ms TTL=128
Reply from 192.168.100.11: bytes=32 time=64ms TTL=128
Reply from 192.168.100.11: bytes=32 time=62ms TTL=128

Ping statistics for 192.168.100.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 62ms, Maximum = 77ms, Average = 67ms

C:\Users\izashok>
```

Рисунок 3.13 – Результат виконання команди ping

Також перевіримо роботу розділеного тунелювання, для цього скористаємося утилітою tracert, один запит надішлемо у внутрішню мережу організації, інший до зовнішнього інтерфейсу ASA1-ORG.

```
Tracing route to MAIN_SERVER [192.168.100.9]
over a maximum of 30 hops:

  1    61 ms    63 ms    63 ms  MAIN_SERVER [192.168.100.9]

Trace complete.

C:\Users\izashok>tracert 34.135.3.18

Tracing route to 34.135.3.18 over a maximum of 30 hops

  1    11 ms     9 ms    10 ms  192.168.0.1
  2    15 ms    20 ms    20 ms  34.135.3.1
  3    27 ms    31 ms    29 ms  34.135.3.9
  4    37 ms    52 ms    41 ms  34.135.3.18

Trace complete.
```

Рисунок 3.14 – Результат роботи tracert

При виконанні запиту до пристрою Main_Server пакет був спрямований через тунель, та не був розпізнаний проміжними пристроями. При направленні до зовнішнього інтерфейсу ASA1-ORG, пакет був спрямований звичайним шляхом.

На пристрої ASA1-ORG виведемо підключених користувачів за допомогою клієнта Anyconnect.

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росінський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

```

ASA1-ORG# sh vpn-sessiondb anyconnect

Session Type: AnyConnect

Username      : gnat7den           Index      : 1
Assigned IP   : 192.168.100.21     Public IP   : 34.135.3.2
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 4518               Bytes Rx    : 11563
Group Policy  : VPN-GROUP-POLICY   Tunnel Group : RA-VPN
Login Time    : 08:45:56 UTC Thu Jun 24 2021
Duration      : 0h:11m:04s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                VLAN         : none
Audt Sess ID  : c0a864010000100060d44644
Security Grp  : none
ASA1-ORG#

```

Рисунок 3.15 – Підключені користувачі

Як можемо побачити, параметри захищеного зв'язку застосовуються такі ж які були визначені у налаштуваннях.

Спробуємо з комп'ютера віддаленого користувача, отримати доступ до мережевих ресурсів організації. Відкриємо спільний каталог, котрий розміщений на WS_ORG_1 з робочої станції Remote_User.

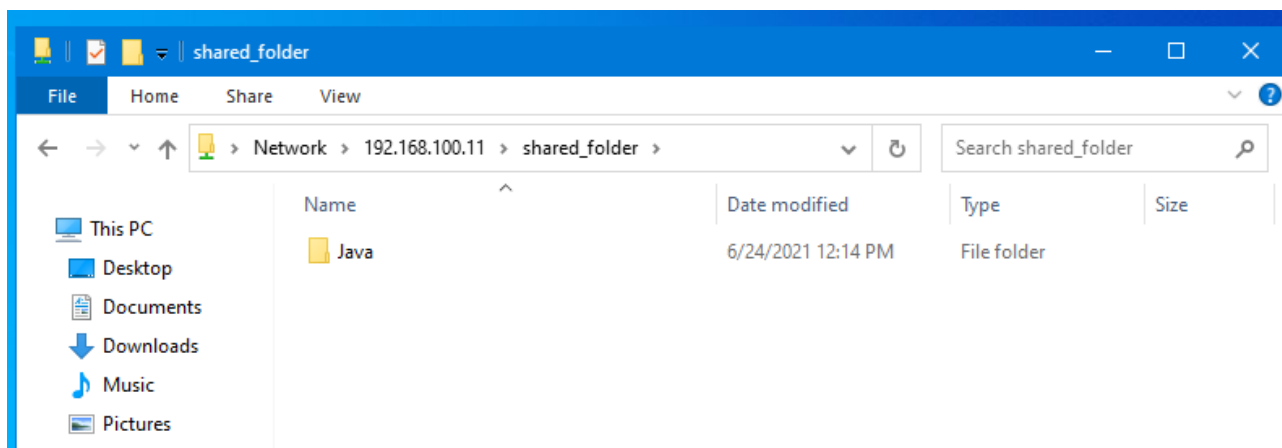


Рисунок 3.16 – Відображений спільний каталог

Усі тести були успішно пройдені, мережеві пристрої мають зв'язок один з одним, як це було визначено у налаштуваннях, підсистема захищеного віддаленого доступу функціонує повноцінно.

ВИСНОВКИ

У даній кваліфікаційній роботі було досягнути поставлені задачі через дослідження та аналіз, проектування та розробку проекту підсистеми захищеного віддаленого доступу користувачів до ресурсів мережі організації на базі технологій Remote Access VPN.

В першому розділі було визначено основні поняття віртуальних приватних мереж (VPN). Було проведено дослідження та аналіз найбільш поширених методів та засобів побудови захищених з'єднань за допомогою різноманітних протоколів. Дослідженню найбільш поширені протоколи котрі застосовуються у створенні VPN-мереж.

В другому розділі було спроектовано загальний проект мережі, котрий включає в себе мережу віддаленого користувача, локальну мережу організації та проміжні пристрої. Було визначено основні типи фізичних взаємодій між мережами. Також було здійснено розробку логічного проекту мережі, визначено основні технології маршрутизації та адресації пристроїв. Важливим етапом став вибір апаратного забезпечення, оскільки від нього залежав подальше проектування підсистеми захищеного віддаленого доступу. Було проаналізовано можливості апаратних засобів компанії Cisco та обрано до подальшого втілення проекту. При виборі програмного забезпечення, було проаналізовано найбільш популярних виробників, визначено їх переваги та недоліки, а також вимоги до апаратного забезпечення.

Проектування підсистеми захищеного віддаленого доступу було здійснено на основі обраних пристроїв та сімейства операційних систем. Для забезпечення більш зручного та надійного методу аутентифікації, було вирішено використувати для цього Radius-сервер на основі Windows Server 2019. Враховуючи апаратні та програмні можливості обраного міжмережного екрану було обрано протокол для побудови VPN-мережі. При виборі клієнта були проаналізовані найбільш безпечні для ініціації підключення рекомендовані компанією Cisco.

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Россінський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

У третьому розділі було здійснено відповідно до проекту було здійснено налагодження мережевих пристроїв та підсистеми захищеного віддаленого доступу до ресурсів мережі організації.

Налагодження мережі та підсистеми здійснювалось за допомогою програми симулятора GNS3 та програми-емулятора Virtualbox. Відповідні сценарії налаштування можна застосовувати на реальному обладнанні.

Спочатку було здійснено налаштування проміжних мережевих пристроїв та кінцевих пристроїв локальних мереж віддаленого користувача та організації. Було задано базові мережеві налаштування на міжмережному екрані.

Після цього, було здійснено налагодження підсистеми захищеного віддаленого доступу до ресурсів мережі. Ядром даної підсистеми став міжмережний екран, а його допоміжним засобом Radius-сервер реалізований на базі Windows Server 2019. Відповідно до проекту було здійснено налаштування взаємодії між цими двома пристроями, а також налаштування протоколів, політик, та списків доступу на мережевому екрані для функціонування сервера віддаленого доступу.

Після завершення налаштування всієї системи, було перевірено налаштовані параметри зв'язку, а також перевірено працездатність та коректність налаштувань підсистеми захищеного віддаленого доступу відповідно до всіх поставлених задач на дану кваліфікаційну роботу.

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росієнський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кульгин М. Технологии корпоративных сетей / Максим Кульгин. – Санкт-Петербург: Питер, 2000. – 704 с. – (Питер).
2. Туннельный протокол второго уровня (L2TP) [Электронный ресурс] – Режим доступа до ресурсу: <https://www.ibm.com/docs/ru/i/7.1?topic=concepts-layer-2-tunnel-protocol>.
3. Запечников С. В. Основы построения виртуальных частных сетей / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, 2003. – 249 с.
4. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – Москва: "Кудиц - Образ", 2001. – 368 с.
5. Организация защищенного удаленного доступа [Электронный ресурс] – Режим доступа до ресурсу: <http://ypn.ru/414/securing-remote-access/>.
6. IPsec (IP Security) [Электронный ресурс] – Режим доступа до ресурсу: [https://ru.bmstu.wiki/IPsec_\(IP_Security\)](https://ru.bmstu.wiki/IPsec_(IP_Security)).
7. Suite B Cryptographic Suites for IPsec [Электронный ресурс] – Режим доступа до ресурсу: <https://datatracker.ietf.org/doc/html/rfc4869>.
8. Ієрархічна модель мережі від Cisco [Электронный ресурс] – Режим доступа до ресурсу: <http://www.telesphera.net/blog/model-mereghi-vid-cisco.html>.
9. Overview of IKEv2 – IETF [Электронный ресурс] – Режим доступа до ресурсу: <https://www.ietf.org/proceedings/52/slides/ipsec-10.pdf>.
10. IPSec and SSL Virtual Private Networks [Электронный ресурс] – Режим доступа до ресурсу: <https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/s14-ipv6-ipsecandssl.pdf>.
11. ASA 5506-X with FirePOWER Services [Электронный ресурс] – Режим доступа до ресурсу: <https://www.cisco.com/c/en/us/support/security/asa-5506-x-firepower-services/model.html#~tab-specs>.

		Гнатюк Д.І.			<i>KIK.KP.B – 123 – 04 – ПЗ</i>	Арк.
		Росінський Ю. М.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

12. Протокол туннелей на сетевом уровне L2 (L2TP) [Электронный ресурс]
– Режим доступа до ресурсу:
https://www.opennet.ru/docs/RUS/inet_book/4/44/l2pr.html.
13. IPSec — протокол защиты сетевого трафика на IP-уровне [Электронный ресурс]
– Режим доступа до ресурсу:
<https://www.ixbt.com/comm/ipsecure.shtml>
14. SHA-1 (Secure Hash Algorithm 1) [Электронный ресурс] – Режим доступа до ресурсу: [https://ru.bmstu.wiki/SHA-1_\(Secure_Hash_Algorithm_1\)](https://ru.bmstu.wiki/SHA-1_(Secure_Hash_Algorithm_1))
15. AES (Advanced Encryption Standard) [Электронный ресурс] – Режим доступа до ресурсу: [https://ru.bmstu.wiki/AES_\(Advanced_Encryption_Standard\)](https://ru.bmstu.wiki/AES_(Advanced_Encryption_Standard))
16. Протокол ESP [Электронный ресурс] – Режим доступа до ресурсу:
<https://www.ibm.com/docs/ru/i/7.3?topic=protocols-encapsulating-security-payload>
17. Маршрутизаторы [Электронный ресурс]. Режим доступа:
https://www.cisco.com/c/ru_ru/products/routers/index.html
18. CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.6 [Электронный ресурс]. Режим доступа:
<https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/vpn/asa-96-vpn-config/vpn-remote-access.html>
19. Cisco ASA Anyconnect Remote Access VPN [Электронный ресурс]. Режим доступа: <https://networklessons.com/cisco/asa-firewall/cisco-asa-anyconnect-remote-access-vpn>
20. The Protocols Behind IPSec [Электронный ресурс]. Режим доступа:
http://www.watchguard.com/training/vvpn/VPN_Policies/vpnpoli4.htm

ДОДАТКИ

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росі́нський Ю. М.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

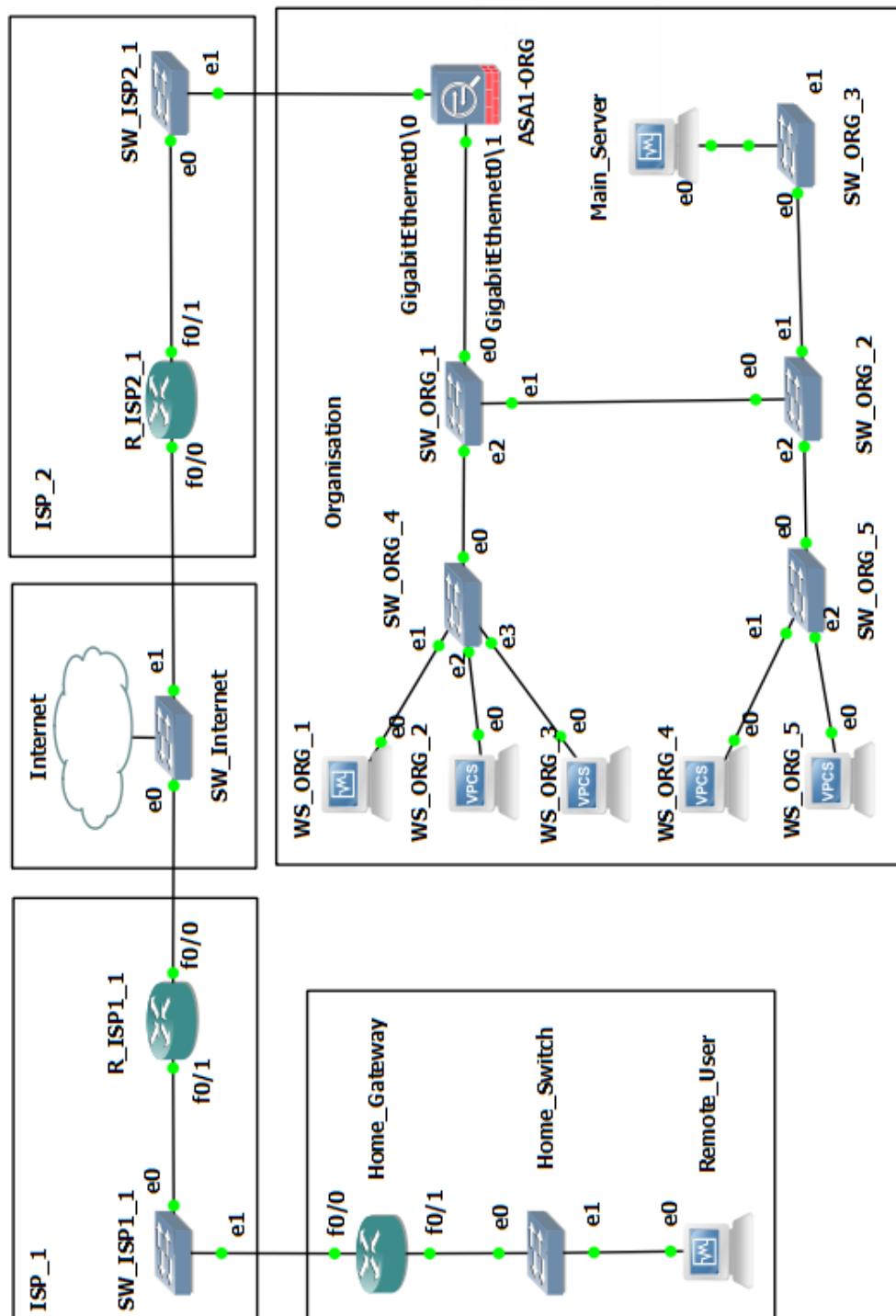


Рисунок А.1 – Частина загальної топології комп'ютерної мережі організації

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росінський Ю. М.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток Б – Характеристики пристроїв Cisco ASA

Таблиця Б.1 – Характеристики Cisco ASA 5506-X

Параметр	Значення
Розміри	4.36 x 19.99 x 23.44 см.
Вага	1.82 кг.
Лінійні порти	1 RJ-45 та Mini USB
Порти	8 Gigabit Ethernet
Оперативна пам'ять	4 Гб
Постійна пам'ять	50 Гб
Флеш-пам'ять	8Гб +
Пропускна здатність з контролем стану підключень при використанні кількох протоколів	300 Мбіт/с
Пропускна здатність з контролем стану підключень	750 Мбіт/с
Максимальна пропускна здатність з AVC (ідентифікація, моніторинг, контроль)	250 Мбіт/с
Максимальна пропускна здатність для VPN з'єднання на алгоритмах 3DES/AES	100 Мбіт/с
Кількість Vlan	5/30
Кількість віддалених підключень IP-sec IKEv1	10/50
Кількість віддалених підключень за допомогою AnyConnect (IKEv2) чи без застосування клієнту	2/50
Максимальна кількість одночасних підключень	3000+
Кількість одночасних сесій	20 000 / 50 000

Таблиця Б.2 – Характеристики Cisco CBS110-16T-EU

Параметр	Значення
Розміри	27.9 x 17 x 4.4 см
Вага	0.97 кг
Охолодження	Пасивне
Кількість портів	16 Gigabit Ethernet
Комутаційна здатність	32 Гбіт/с
Розмір таблиці MAC-адрес	8000 Кб
Буфер пакетів	2 Мб
Флеш-пам'ять	16 Мб
Процесор	ARM 400 МГц
Стандарти	IEEE 802.3 (10BASE-T Ethernet), IEEE 802.3u (100BASE-TX Fast Ethernet), IEEE 802.3ab (1000BASE-T Gigabit Ethernet), IEEE 802.3z (Gigabit Ethernet), IEEE 802.3x (контроль потоків), пріоритет 802.1p, Energy Efficient Ethernet, 802.3af

Конфігураційний файл ASA1-ORG

```

:
: Serial Number: 9ASXC6K12A7
: Hardware:  ASAv, 2048 MB RAM, CPU Pentium II 2000 MHz
:
ASA Version 9.7(1)
!
hostname ASA1-ORG
enable password $sha512$5000$0b0Iz+ocTDoWvfuLKLpbqw==$dZQhaIyK8j+xlusdl8s4pg== pbkdf2
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names
ip local pool VPN-POOL-1 192.168.100.21-192.168.100.25 mask 255.255.255.224

!
interface GigabitEthernet0/0
description Provider
nameif outside
security-level 0
ip address 34.135.3.18 255.255.255.248
!
interface GigabitEthernet0/1
description Organization
nameif inside
security-level 100
ip address 192.168.100.1 255.255.255.224
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/4
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/5
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/6
shutdown
no nameif

```

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росінський Ю. М.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
ftp mode passive
object network inside-subnet
subnet 192.168.100.0 255.255.255.224
access-list SPLIT-ACL standard permit 192.168.100.0 255.255.255.224
pager lines 23
mtu outside 1500
mtu inside 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
nat (inside,outside) source static any any destination static inside-subnet inside-subnet no-proxy-arp route-lookup
!
object network inside-subnet
nat (inside,outside) dynamic interface
router ospf 1
network 34.135.3.16 255.255.255.248 area 1
network 192.168.100.0 255.255.255.224 area 2
log-adj-changes
!
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
aaa-server win-serv protocol radius
aaa-server win-serv (inside) host 192.168.100.9
key *****
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 192.168.100.0 255.255.255.224 inside
no snmp-server location
no snmp-server contact
crypto ipsec ikev2 ipsec-proposal AES256
protocol esp encryption aes-256
protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map VPN-MAP 65535 set ikev2 ipsec-proposal AES256
crypto map outside_map 65535 ipsec-isakmp dynamic VPN-MAP
crypto map outside_map interface outside
crypto ca trustpoint _SmartCallHome_ServerCA
no validation-usage
crl configure
crypto ca trustpoint localtrust
enrollment self

```

		Гнатюк Д.І.			KIK.KP.Б – 123 – 04 – ПЗ	Арк.
		Росінський Ю. М.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

```

fqdn none
subject-name cn=192.168.100.1, CN=ASA1-ORG
keypair sslvpnkey
crl configure
crypto ca trustpool policy
auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
certificate ca 18dad19e267de8bb4a2158cdcc6b3b4a
308204d3 308203bb a0030201 02021018 dad19e26 7de8bb4a 2158cdcc 6b3b4a30
0d06092a 864886f7 0d010105 05003081 ca310b30 09060355 04061302 55533117
30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 1f301d06 0355040b
13165665 72695369 676e2054 72757374 204e6574 776f726b 313a3038 06035504
0b133128 63292032 30303620 56657269 5369676e 2c20496e 632e202d 20466f72
20617574 686f7269 7a656420 75736520 6f6e6c79 31453043 06035504 03133c56
65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61 72792043
65727469 66696361 74696f6e 20417574 686f7269 7479202d 20473530 1e170d30
36313130 38303030 3030305a 170d3336 30373136 32333539 35395a30 81ca310b
30090603 55040613 02555331 17301506 0355040a 130e5665 72695369 676e2c20
496e632e 311f301d 06035504 0b131656 65726953 69676e20 54727573 74204e65
74776f72 6b313a30 38060355 040b1331 28632920 32303036 20566572 69536967
6e2c2049 6e632e20 2d20466f 72206175 74686f72 697a6564 20757365 206f6e6c
79314530 43060355 0403133c 56657269 5369676e 20436c61 73732033 20507562
6c696320 5072696d 61727920 43657274 69666963 6174696f 6e204175 74686f72
69747920 2d204735 30820122 300d0609 2a864886 f70d0101 01050003 82010f00
3082010a 02820101 00af2408 08297a35 9e600caa e74b3b4e dc7cbc3c 451cbb2b
e0fe2902 f95708a3 64851527 f5f1adc8 31895d22 e82aaaa6 42b38ff8 b955b7b1
b74bb3fe 8f7e0757 ecef43db 66621561 cf600da4 d8def8e0 c362083d 5413eb49
ca595485 26e52b8f 1b9feb5f a191c233 49d84363 6a524bd2 8fe87051 4dd18969
7bc770f6 b3dc1274 db7b5d4b 56d396bf 1577a1b0 f4a225f2 af1c9267 18e5f406
04ef90b9 e400e4dd 3ab519ff 02baf43c eee08beb 378becf4 d7acf2f6 f03dafdd
75913319 1d1c40cb 74241921 93d914fe ac2a52c7 8fd50449 e48d6347 883c6983
cbfe47bd 2b7e4fc5 95ae0e9d d4d143c0 6773e314 087ee53f 9f73b833 0acf5d3f
3487968a ee53e825 15020301 0001a381 b23081af 300f0603 551d1301 01ff0405
30030101 ff300e06 03551d0f 0101ff04 04030201 06306d06 082b0601 05050701
0c046130 5fa15da0 5b305930 57305516 09696d61 67652f67 69663021 301f3007
06052b0e 03021a04 148fe5d3 1a86ac8d 8e6bc3cf 806ad448 182c7b19 2e302516
23687474 703a2f2f 6c6f676f 2e766572 69736967 6e2e636f 6d2f7673 6c6f676f
2e676966 301d0603 551d0e04 1604147f d365a7c2 ddecbbf0 3009f343 39fa02af
33313330 0d06092a 864886f7 0d010105 05000382 01010093 244a305f 62cfd81a
982f3dea dc992dbd 77f6a579 2238ecc4 a7a07812 ad620e45 7064c5e7 97662d98
097e5faf d6cc2865 f201aa08 1a47def9 f97c925a 0869200d d93e6d6e 3c0d6ed8
e6069140 18b9f8c1 eddfdb41 aae09620 c9cd6415 3881c994 eea28429 0b136f8e
db0cdd25 02dba48b 1944d241 7a05694a 584f60ca 7e826a0b 02aa2517 39b5db7f
e784652a 958abd86 de5e8116 832d10cc defda882 2a6d281f 0d0bc4e5 e71a2619
e1f4116f 10b595fc e7420532 dbce9d51 5e28b69e 85d35bef a57d4540 728eb70e
6b0e06fb 33354871 b89d278b c4655f0d 86769c44 7af6955c f65d3208 33a454b6
183f685c f2424a85 3854835f d1e82cf2 ac11d6a8 ed636a
quit
crypto ikev2 policy 1
encryption aes-256
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 enable outside client-services port 443
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.100.0 255.255.255.0 inside
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
<--- More --->
Warning: ASA's platform license state is Unlicensed.

```

		Гнатюк Д.І.			KIK.KP.B – 123 – 04 – ПЗ	Арк.
		Росінський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

```

Install ASAv platform license for full functionality.
dhcpd lease 7200
dhcpd option 3 ip 192.168.100.1
!
dhcpd address 192.168.100.10-192.168.100.20 inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
enable outside
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable
group-policy VPN-GROUP-POLICY internal
group-policy VPN-GROUP-POLICY attributes
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value SPLIT-ACL
dynamic-access-policy-record DfltAccessPolicy
username sysadmin password $sha512$5000$REkzChbqML0XCy6MaFuvuQ==$I7gkmtgC+3YOxJRzzrmGCQ==
pbkdf2 privilege 15
tunnel-group RA-VPN type remote-access
tunnel-group RA-VPN general-attributes
address-pool VPN-POOL-1
authentication-server-group win-serv
default-group-policy VPN-GROUP-POLICY
tunnel-group RA-VPN webvpn-attributes
group-alias RA-VPN enable
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
policy-map global_policy
class inspection_default
inspect dns migrated_dns_map_1
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
policy-map type inspect dns migrated_dns_map_2
parameters
message-length maximum client auto

```

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Россінський Ю. М.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

```

message-length maximum 512
no tcp-inspection
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1
no active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
profile License
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http
Cryptochecksum:b5ed437aeb2b2839318b6c95203cd10f
: end

```

		Гнатюк Д.І.			КІК.КР.Б – 123 – 04 – ПЗ	Арк.
		Росініський Ю. М.				
Змн.	Арк.	№ докум.	Підпис	Дата		54