МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра електроніки і комп’ютерної техніки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи
на тему:
«Проєктування корпоративної мережі на базі технологій VPN»

Завідуючий кафедрою А. С. Опанасюк

Керівник
кваліфікаційної роботи О.В. Д’яченко

Розробив студент
групи ТК-71 М.О. Третяк

Суми 2021

Сумський державний університет

Факультет денний **Кафедра** електроніки і комп'ютерної техніки

Спеціальність телекомунікації та радіотехніка

ЗАТВЕРДЖУЮ**:**
Зав. кафедри ЕКТ
Опанасюк А. С.
«___» _____ 2021 р.

Завдання

на дипломний проект студенту

Третяк Марині Олександрівні
(прізвище,ім'я,по батькові)

1. Тема проекту: «Проєктування корпоративної мережі на базі технологій VPN»
затверджено наказом університету від «05» квітня 2021 р. № 0154- VI
v

2. Термін здачі студентом закінченого проекту 30 травня 2021 р.

3. Вихідні дані до проекту: розробити захищену корпоративну мережу на базі протокол IPSec, використати мережеве обладнання cisco, зробити можливим підключення та використання ресурсів мережі за допомогою віддаленого доступу, провести налаштування такої мережі.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які підлягають розробці)

Огляд літератури по тематиці проекту. Розробка схем функціонування пристрою (схема алгоритм, структурна схема, топологія мережі).

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) схема алгоритму протоколу IPsec; схема архітектури протоколу IPsec; топологія проєктованої мережі.

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів дипломного проекту	Термін виконання етапів проекту	Примітка
1.	Огляд літератури по тематиці проекту	23.04.2021	
2.	Розробка схеми алгоритму	27.04.2021	
3.	Розробка структурної схеми	02.05.2021	
4.	Розробка топології	06.05.2021	
6.	Оформлення графічної частини	13.05.2021	
7.	Оформлення пояснювальної записки	20.05.2021	
8.	Рецензування роботи та підготовка до захисту	31.05.2021	

Студент-дипломник _____

Керівник проекту _____

РЕФЕРАТ

Кваліфікаційна робота бакалавра складається зі вступу, трьох розділів, висновку та списку використаних джерел, що включає(цифра) найменувань. Загальний обсяг бакалаврської роботи складає сторінки, в тому числі таблиці та рисунки.

У дипломній роботі було розроблено та спроектовано корпоративну мережу на базі технологій VPN.Описана актуальність розробки, проблеми які вирішено, викладена загальна інформація про методи розробки VPN та протоколи. Розглянута архітектура протоколу Ipsec та схема алгоритму.

Розроблена топологія мережі віддаленого доступу на основі протоколу Ipsec.

Зроблено висновки щодо актуальності VPN та застосування Ipsec для корпоративної мережі.

КЛЮЧОВІ СЛОВА :VPN, Ipsec, протокол, мережа, віддалений доступ, шифрування даних, канал, налаштування, роутер.

KEYWORDS:VPN, Ipsec, protocol, network, remote network, data encryption,channel, settings, router.

ЗМІСТ

ВСТУП 4

1.ТЕОРЕТИЧНИЙ ОГЛЯД 5

1.1 Історія VPN 5

2. ПОБУДОВА VPN мережі. 7

2.1 VPN на базі брандмауера. 7
2.2VPN на базі маршрутизаторів. 8
2.3 VPN на основі Програмного забезпечення 8
2.4 VPN на основі мережевій ОС 9
2.5 VPN на базі апаратного засобів 10
2.6 Таблиця переваги та недоліки побудови VPN 10

2.3 Основні складові та протоколи VPN мереж 12

2.3.1VPN канального рівня 15
2.3.2 VPN мережевого рівня 16
2.3.3Транспортний рівень 17
2.4 Протоколи VPN 18

2.4.1 PPTP 19
2.4.2 L2TP і L2TP / IPsec 20
2.4.3OpenVPN 21
2.4.4 SSTP 23
2.4.5 IKEv2 24
3. РЕАЛІЗАЦІЯ ВИБРАНОГО ПРОТОКОЛУ VPN 27

3.1Схема алгоритму IPsec 29

3.2 Етапи створення корпоративної мережі на базі VPN 33

ВИСНОВКИ 49

СПИСОК ДЖЕРЕЛ ПОСИЛАНЬ 50

ВСТУП

В даний час послуги віртуальної приватної мережі (VPN) є досить гарячою темою, оскільки конфіденційність в Інтернеті піддається критиці з багатьох сторін. Так як, великі компанії Facebook, Google, Microsoft і багато інших намагаються зібрати більше даних про користувачів, яку вони можуть використовувати в комерційних цілях. Так само є ще проблема на сьогоднішній день це віддалена робота. На початку 2020 року більшість людей, які працювали оффлайн перейшли на онлайн.

І є спосіб вирішити ці завдання захистом інформації в сучасному мережевому середовищі за рахунок використання технології захищених віртуальних мереж (Virtual Privat Network-VPN), надійно шифруючих інформацію, передану по відкритих мережах Internet.

Віртуальна приватна мережа (VPN) може приховувати адреса внутрішнього протоколу користувача (IP-адреса) і блокувати його місце розташування і історію браузера, дозволяючи їм ділитися і отримувати інформацію в загальнодоступних інтернет-мережах більш конфіденційно.

Чи шукаєте ви щось в Інтернеті або спілкуєтеся через соціальні мережі, ви залишаєте цифрові сліди у вигляді історії переглядів, файлів cookie та кешованих даних.

Ваш інтернет-провайдер (ISP), уряд та інші треті сторони можуть відстежувати, що ви шукаєте, відвідуєте і завантажуєте.

Навіть якщо ви використовуєте режим приватного перегляду, ваш IP-адреса все одно може бути отриманий.

Коли ви завантажуєте і активуєте VPN перед переглядом веб-сторінок, VPN може забезпечити конфіденційність в мережі і підвищити безпеку, допомагаючи приховати вашу особистість в мережі і зашифрувати ваш трафік. Хакери і треті особи зможуть бачити тільки IP-адреса віддаленої VPN. Це не дозволяє їм отримати доступ до вашого розташування, історії браузера або

особистої інформації, яку ви могли відправити або отримати під час цього сеансу перегляду.

1.ТЕОРЕТИЧНИЙ ОГЛЯД

1.1 Історія VPN.

Міністерство оборони США почали дослідження і впровадження електронних методів зв'язку між віддаленими місцями в 1960 році.

Основним результатом їх зусиль стала мережа ARPANET (Advanced Research Projects Agency Network), що представляє собою мережу з комутацією пакетів. Крім того, вони розробили протокол управління передачею / Інтернет-протокол (TCP / IP).[1]

Ця система TCP / IP була початком всесвітньої павутини, якою ми її знаємо сьогодні. Пакет Internet Protocol Suite з'явився в 1982 році в результаті цього дослідження і пізніше був прийнятий комерційної комп'ютерної індустрією в 1985 році.

TCP / IP працює на чотирьох рівнях: канал, Інтернет, транспорт і додаток. Логічно, що Інтернет - це рівень, на якому локальні мережі та пристрої підключаються до універсальної мережі і де існує найбільший ризик зовнішнього моніторингу, цензури, вторгнення і перехоплення даних.[3.]

Коли потреба в мережевий і інтернет-безпеки стала більш ніж очевидною, Джон Іоаннідіс і його команда почали дослідження технологій інтернет-безпеки в Колумбійському університеті і в AT & T Bell Labs в 1993 році. Їх зусилля увінчалися створенням програмного протоколу IP-шифрування, який був першою формою VPN.

У 1994 році Вей Сюй розробив мережу Ipsec, протокол інтернет-безпеки, який аутентифікує і шифрує інформаційні пакети, що передаються в Інтернеті. У той же час був створений протокол безпеки інкапсуляції, який ознаменував ще один крок до технології VPN.

Оскільки ці протоколи ставали все швидшими і просунутими, VPN був в межах досяжності, і його винахід було лише питанням часу.

Нарешті, в 1996 році Гурдип Сингх-Палл, співробітник Microsoft, почав розробку протоколу тунелювання точка-точка (PPTP), щоб користувачі могли мати безпечне підключення до Інтернету, працюючи вдома. Більшість експертів вважають цю подію початком VPN.

Переваги і недоліки VPN мережі

Таблиця 1.2-Переваги та недоліки мережі VPN[2].

Переваги	Недоліки
1.Можливість підключитися до заблокованого контенту.	1. Якісний VPN коштує дорого.
2.Захист даних в Інтернеті.	2. Іноді повільна швидкість інтернету.
3.Безпечне онлайн-з'єднання.	3. Існує технологія блокування VPN.
4. Обхід геоблокувань.	4. VPN не для всіх пристроїв.
5. Обхід брандмауерів.	
6. Анонімність.	
7.Захищений обмін файлами.	

2. ПОБУДОВА VPN мережі.

Існує багато варіантів створення VPN. Вибираючи рішення, вам слід враховувати коефіцієнти продуктивності вашого конструктора VPN. Наприклад, якщо ваш маршрутизатор вже працює з обмеженням потужності процесора, додавання тунелю VPN та забезпечення шифрування / дешифрування даних може вимкнути всю мережу, оскільки вона не може працювати з цим маршрутизатором. Не кажучи вже про VPN - це звичайний трафік. Досвід показує, що для створення VPN найкраще використовувати спеціальне обладнання, але якщо ваші кошти обмежені, ви можете зосередитись лише на програмних рішеннях. Давайте розглянемо деякі варіанти побудови VPN.

2.1 VPN на базі брандмауера.

Між мережеві екрани більшості виробників підтримують тунелювання і шифрування даних. Всі подібні продукти засновані на тому, що трафік, що проходить через між мережевий екран, зашифрований. До фактичного програмного забезпечення брандмауера доданий модуль шифрування. Недоліком цього методу є те, що продуктивність залежить від обладнання, на якому запущений брандмауер. При використанні між мережевих екранів на базі ПК майте на увазі, що це рішення можна використовувати тільки для невеликих мереж з невеликим трафіком.

Прикладом брандмауера VPN є Firewall-1 від Check Point Software Technologies. FairWall-1 використовує стандартний підхід, заснований на IPSec, для побудови VPN. Трафік, що надходить на між мережевий екран, розшифровується, а потім до нього застосовуються стандартні правила контролю доступу. FireWall-1 працює в операційних системах Solaris і Windows NT 4.0.

2.2VPN на базі маршрутизаторів.

Побудова VPN-каналів на базі маршрутизаторів компанії Cisco здійснюється засобами самої операційної системи, починаючи з версії Cisco IOS 12.x. Якщо на прикордонні маршрутизатори Cisco інших відділень компанії встановлена дана операційна система, то є можливість сформувати корпоративну VPN, що складається із сукупності віртуальних захищених тунелів типу «точка-точка» від одного маршрутизатора до іншого (малюнок 1.3). Як правило, для шифрування даних в каналі за замовчуванням застосовується криптоалгоритм DES з довжиною ключа 56 біт.

Інший спосіб побудувати VPN - використовувати маршрутизатори для створення захищених каналів. Оскільки вся інформація, яка виходить із локальної мережі, проходить через маршрутизатор, рекомендується призначити йому завдання шифрування.

Прикладом обладнання для побудови VPN на маршрутизаторах є обладнання від Cisco Systems. Починаючи з версії ПЗ IOS 11.3, маршрутизатори Cisco підтримують L2TP і IPSec. На додаток до простого шифрування переданої інформації Cisco також підтримує інші функції VPN, такі як аутентифікація при установці тунельного з'єднання і обмін ключами.

Додатковий модуль шифрування ESA може використовуватися для підвищення продуктивності маршрутизатора. Крім того, Cisco System випустила спеціальний пристрій VPN під назвою Cisco 1720 VPN Access Router для малих і середніх підприємств і великих філій.

2.3 VPN на основі Програмного забезпечення

Наступний підхід до побудови VPN - чисто програмні рішення. При реалізації такого рішення використовується спеціалізоване програмне забезпечення, яке працює на виділеному комп'ютері і в більшості випадків

виступає в ролі проксі-сервера. Комп'ютер з таким програмним забезпеченням може бути розташований за брандмауером.

Програмне забезпечення Digital AltaVista Tunnel 97 є прикладом такого рішення. Використовуючи це програмне забезпечення, клієнт підключається до сервера Tunnel 97, аутентифицирующей з ним і обмінюється ключами. Шифрування виконується на основі 56- або 128-бітних ключів, отриманих в процесі встановлення з'єднання. Потім зашифровані пакети інкапсулюються в інші IP-пакети, які, в свою чергу, відправляються на сервер. Крім того, це програмне забезпечення кожні 30 хвилин генерує нові ключі, що значно підвищує безпеку з'єднання.

Позитивні якості AltaVista Tunnel 97 - простота установки і зручність управління. До недоліків даної системи можна віднести нестандартну архітектуру (власний алгоритм обміну ключами) і низьку продуктивність.

2.4 VPN на основі мережевій ОС

Рішення для мережевих ОС розглянемо приклади системи Microsoft Windows NT. Для створення VPN Microsoft використовує PPTP, інтегрований в Windows NT. Це рішення дуже привабливо для організацій, що використовують Windows в якості корпоративної операційної системи. Слід зазначити, що вартість такого рішення значно нижче вартості інших рішень. VPN на базі Windows NT використовують базу користувачів NT, що зберігається на основному контролері домену (PDC). При підключенні до сервера PPTP користувач аутентифікується за допомогою PAP, CHAP або MS-CHAP. Передані пакети інкапсулюються в пакети GRE / PPTP. Для шифрування пакетів використовується нестандартний протокол Microsoft Point-to-Point Encryption з 40- або 128-бітовим ключем, отриманим під час встановлення з'єднання. До недоліків цієї системи можна віднести перевірку відсутності цілісності даних і неможливість зміни ключів при з'єднанні. Позитивні сторони - простота інтеграції з Windows і невисока вартість.

2.5 VPN на базі апаратного засобів

Можливість побудови VPN на спеціальних пристроях може використовуватися в мережах, що вимагають високої продуктивності. Прикладом такого рішення є продукт Radguard IPro-VPN. У цьому продукті використовується апаратне шифрування переданої інформації, що дозволяє передавати потік зі швидкістю 100 Мбіт / с. IPro-VPN підтримує протокол IPSec і механізм управління ключами ISAKMP / Oakley. Крім іншого, даний пристрій підтримує трансляцію мережевих адрес і може бути доповнено спеціальною картою, яка додає функції брандмауера.[3]

2.6 Переваги та недоліки побудови VPN

Таблиця 2.1-Поріняння VPN

	Переваги	**Недоліки**
VPN на базі маршрутизатора	Функції підтримки мереж VPN можуть бути вбудовані маршрутизующій пристрій, які не потребують додаткових витрат на придбання засобів, що реалізують ці функції. Спрощується адміністрування VPN.	Функціонування VPN може негативно вплинуть на інший трафік. Канал між одержувачем інформації в середині ЛВС і маршрутизатором може стати вразливою ланкою в системі захисту.
VPN на базі брандмауера	Можливий контроль тунельованого трафіку. Досягається висока ефективність адміністрування	Операції, зв’язані з шифруванням даних, можуть надмірно завантажувати процесор і знижувати

	захищених віртуальних мереж. Забезпечується комплексний захист інформаційного обміну. Відсутнє надмірність апаратних платформ для засобів мережевого захисту.	продуктивність мережевого екрану. Якщо захищений тунель завершуєтеся на мережевому екрані, то канал між одержувачем інформації всередині ЛВС і мережовим екраном може стати вразливою ланкою в системі захисту. При підвищенні продуктивності серверних продуктів апаратне забезпечення буде потрібно модернізувати
VPN на базі мережевої ОС	Можливість модернізації і оновлення версій. Оперативність вирішення проблем. Не потрібні спеціальні апаратні засоби.	Адміністрування VPN може потребувати окремого додатку, можливо навіть виділеного каталогу. При підвищені продуктивності сервісних продуктів апаратне забезпечення може потребувати модернізації.
VPN на базі апаратного забезпечення	Забезпечуються біль висока продуктивність. Багатофункціональні схеми апаратні пристрої полегшують конфігурацію і	В багатофункціональних блоках продуктивність однієї програми підвищується часто на шкоду іншому. Одно функціональні пристрої можуть вимагати окремих

	обслуговування. Одно функціональні апаратні пристрої допускають тонке налаштування для найвищої продуктивності.	інструментів адміністрування і каталогів. Модернізація для підвищення продуктивності нерідко виявляється занадто дорогим або неможливо. Канал між одержувачем інформації всередині ЛВС і апаратним пристроєм шифрування трафіку може стати вразливою [4]

2.3 Основні складові та протоколи VPN мереж

Віртуальна приватна мережа базується на реалізації трьох складових:

· Тунелювання;

· Шифрування;

· Аутентифікація

Тунелювання забезпечує передачу даних між двома точками - закінченнями тунелю - таким чином, що для джерела і приймача даних виявляється прихованою вся мережева інфраструктура, що лежить між ними.

Транспортне середовище тунелю, як паром, підхоплює пакети використовуваного мережевого протоколу біля входу в тунель і без змін доставляє їх до виходу. Побудови тунелю досить для того, щоб з'єднати два мережевих вузла так, що з точки зору працюючого на них програмного забезпечення вони виглядають підключеними до однієї (локальної) мережі. Однак не можна забувати, що насправді «парою» з даними проходить через безліч проміжних вузлів (маршрутизаторів) відкритої публічної мережі.

Такий стан справ таїть в собі дві проблеми. Перша полягає в тому, що передається через тунель інформація може бути перехоплена зловмисниками.

Якщо вона конфіденційна (номери банківських карток, фінансові звіти, відомості особистого характеру), то цілком реальна загроза її компрометації, що вже само по собі неприємно. Гірше того, зловмисники мають можливість модифікувати передані через тунель дані так, що одержувач не зможе перевірити їх достовірність. Наслідки можуть бути жахливими. З огляду на сказане, ми приходимо до висновку, що тунель в чистому вигляді придатний хіба що для деяких типів мережевих комп'ютерних ігор і не може претендувати на більш серйозне застосування. Обидві проблеми вирішуються сучасними засобами криптографічного захисту інформації, зокрема застосовуються різні методи аутентифікації і шифрування.

Щоб перешкодити внесенню несанкціонованих змін в пакет з даними на шляху його проходження по тунелю, використовується метод електронного цифрового підпису. Суть методу полягає в тому, що кожен переданий пакет забезпечується додатковим блоком інформації, який виробляється у відповідності з асиметричним криптографічним алгоритмом і унікальний для вмісту пакета і секретного ключа ЕЦП відправника. Цей блок інформації є ЕЦП пакету і дозволяє виконати аутентифікацію даних одержувачем, якому відомий відкритий ключ ЕЦП відправника. Захист переданих через тунель даних від несанкціонованого перегляду досягається шляхом використання сильних алгоритмів шифрування.

За допомогою тунелювання пакети даних транслюються через загальнодоступну мережу як за звичайним Двоточковий з'єднанню. Між кожною парою «відправник-одержувач даних» встановлюється своєрідний тунель - безпечне логічне з'єднання, що дозволяє інкапсулювати дані одного протоколу в пакети іншого. Основними компонентами тунелю є:

- ініціатор;
- маршрутизацій мережу;
- тунельний комутатор;
- один або кілька тунельних термінаторів.

Сам по собі принцип роботи VPN який суперечить основним мережним технологіям і протоколам. Наприклад, при встановленні з'єднання віддаленого доступу клієнт посилає серверу потік пакетів стандартного протоколу PPP. У разі організації віртуальних виділених ліній між локальними мережами їх маршрутизатори також обмінюються пакетами PPP. Проте, принципово новим моментом є пересилання пакетів через безпечний тунель, організований в межах загальнодоступної мережі.[5]

Тунелювання дозволяє організувати передачу пакетів одного протоколу в логічній середовищі, що використовує інший протокол. В результаті з'являється можливість вирішити проблеми взаємодії кількох різнотипних мереж, починаючи з необхідності забезпечення цілісності та конфіденційності даних і закінчуючи подоланням невідповідностей зовнішніх протоколів або схем адресації.

Існуюча мережева інфраструктура корпорації може бути підготовлена до використання VPN як за допомогою програмного, так і за допомогою апаратного забезпечення. Організацію віртуальної приватної мережі можна порівняти з прокладанням кабелю через глобальну мережу. Як правило, безпосереднє з'єднання між віддаленим користувачем і кінцевим пристроєм тунелю встановлюється по протоколу PPP.

Найбільш поширений метод створення тунелів VPN - інкапсуляція мережевих протоколів (IP, IPX, AppleTalk і т.д.) в PPP і подальша інкапсуляція освічених пакетів в

протокол тунелювання. Зазвичай в якості останнього виступає IP або (набагато рідше) ATM і Frame Relay. Такий підхід називається тунелювання другого рівня, оскільки «пасажиром» тут є протокол саме другого рівня.

Альтернативний підхід - інкапсуляція пакетів мережевого протоколу безпосередньо в протокол тунелювання (наприклад, VTP) називається тунелюванням третього рівня.

Незалежно від того, які протоколи використовуються або які цілі переслідуються при організації тунелю, основна методика залишається практично незмінною. Зазвичай один протокол використовується для встановлення з'єднання з віддаленим вузлом, а інший - для інкапсуляції даних і службової інформації з метою передачі через тунель.

Мережі VPN будуються з використанням протоколів тунелювання даних через мережу зв'язку загального користування Інтернет, причому протоколи тунелювання забезпечують шифрування даних і здійснюють їх наскрізну передачу між користувачами. Як правило, на сьогоднішній день для побудови мереж VPN використовуються протоколи наступних рівнів:

- Канальний рівень
- Мережевий рівень
- Транспортний рівень.

2.3.1VPN канального рівня

Засоби VPN, які використовуються на канальному рівні моделі OSI, дозволяють забезпечити інкапсуляцію різних видів трафіку третього рівня (і більш високих рівнів) і побудова віртуальних тунелів типу точка-точка (від маршрутизатора до маршрутизатора або від персонального комп'ютера до шлюзу ЛВС). До цієї групи належать VPN-продукти, які використовують протоколи L2F (Layer 2 Forwarding) і PPTP (Point-to-Point Tunneling Protocol), а також порівняно недавно затверджений стандарт L2TP (Layer 2 Tunneling Protocol), розроблений спільно фірмами Cisco Systems і Microsoft .

Протокол захищеного каналу PPTP заснований на протоколі PPP, який широко використовується в з'єднаннях «точка-точка», наприклад при роботі по виділеним лініям. Протокол PPTP забезпечує прозорість засобів захисту для додатків і служб прикладного рівня і не залежить від застосовуваного протоколу мережевого рівня. Зокрема, протокол PPTP може переносити пакети як в мережах IP, так і в мережах, що працюють на основі протоколів

IPX, DECnet або NetBEUI. Однак, оскільки протокол PPP використовується далеко не в усіх мережах (в більшості локальних мереж на канальному рівні працює протокол Ethernet, а в глобальних - протоколи ATM, frame relay), то PPTP не можна вважати універсальним засобом. Дійсно, в різних частинах великої складовою мережі, взагалі кажучи, використовуються різні канальні протоколи, тому прокласти захищений канал через цю гетерогенну середу за допомогою єдиного протоколу канального рівня неможливо.

Протокол L2TP, стане, ймовірно, домінуючим рішенням для організації віддаленого доступу до ЛВС (оскільки базується в основному на ОС Windows). Тим часом рішення другого рівня не придбають, ймовірно, таке ж значення для взаємодії ЛВС, через недостатню масштабованості при необхідності мати кілька тунелів з загальними кінцевими точками.

2.3.2 VPN мережевого рівня

VPN-продукти мережевого рівня виконують инкапсуляцию IP в IP. Одним з широко відомих протоколів на цьому рівні є протокол SKIP, який поступово витісняється новим протоколом IPSec (IP Security), призначеним для аутентифікації, тунелювання і шифрування IP-пакетів. Стандартизований консорціумом Internet Engineering Task Force (IETF) протокол IPSec увібрав в себе всі кращі рішення щодо шифрування пакетів і повинен увійти в якості обов'язкового компонента в протокол IPv6.

Працюючий на мережевому рівні протокол IPSec є компромісним варіантом. З одного боку, він прозорий для додатків, а з іншого - він може працювати практично у всіх мережах, так як заснований на широко поширеному протоколі IP. В даний час в світі тільки 1% комп'ютерів не підтримує IP взагалі, інші 99% використовують його або як єдиний протокол, або в якості одного з декількох протоколів.[6]

Протокол IPSec передбачає стандартні методи ідентифікації користувачів або комп'ютерів при ініціації тунелю, стандартні способи

використання шифрування кінцевими точками тунелю, а також стандартні методи обміну і управління ключами шифрування між кінцевими точками.

Протокол IPSec стрімко завойовує популярність і стане, ймовірно, домінуючим методом VPN для взаємодії ЛВС. Тим часом не слід забувати, що специфікація IPSec орієнтована на IP і, таким чином, не підходить для трафіку будь-яких інших протоколів мережевого рівня. Протокол IPSec може працювати спільно з протоколом L2TP, в результаті ці два протоколи забезпечують більш надійну ідентифікацію, стандартизоване шифрування і цілісність даних. Тунель IPSec між двома локальними мережами може підтримувати безліч індивідуальних каналів передачі даних, в результаті чого додатки даного типу отримують переваги з точки зору масштабування в порівнянні з технологією другого рівня.

Говорячи про IPSec, необхідно згадати протокол IKE (Internet Key Exchange), що дозволяє захистити передану інформацію від стороннього втручання. Він вирішує завдання безпечного управління та обміну криптографічними ключами між віддаленими пристроями. Протокол IKE, заснований на алгоритмі шифрування відкритим ключем, автоматизує обмін ключами і встановлює захищене з'єднання, тоді як IPSec кодує і «підписує» пакети. Крім того, IKE дозволяє змінювати ключ для вже встановленого з'єднання, що підвищує конфіденційність переданої інформації.

2.3.3Транспортний рівень

призначений для доставки даних. При цьому неважливо, які дані передаються, звідки і куди, тобто, він надає сам механізм передачі. Блоки даних він розділяє на фрагменти, розміри яких залежать від протоколу: короткі об'єднує в один, а довгі розбиває. Протоколи цього рівня призначені для взаємодії типу точка-точка. Приклад: TCP, UDP, SCTP.

Існує безліч класів протоколів транспортного рівня, починаючи від протоколів, які надають тільки основні транспортні функції, наприклад,

функції передачі даних без підтвердження прийому, і закінчуючи протоколами, які гарантують доставку в пункт призначення кількох пакетів даних в належній послідовності, мультиплексує кілька потоків даних, забезпечують механізм управління потоками даних і гарантують достовірність отриманих даних.[10]

Деякі протоколи транспортного рівня, звані протоколами без установки з'єднання, не гарантують, що дані доставляються за призначенням в тому порядку, в якому вони були послані пристроєм-джерелом. Деякі транспортні рівні справляються з цим, збираючи дані в потрібній послідовності до передачі їх на сеансовий рівень. Мультиплексування (multiplexing) даних означає, що транспортний рівень здатний одночасно обробляти кілька потоків даних (потоки можуть чинити і від різних додатків) між двома системами. Механізм управління потоком даних - це механізм, що дозволяє регулювати кількість даних, переданих від однієї системи до іншої. Протоколи транспортного рівня часто мають функцію контролю доставки даних, змушуючи приймаючу дані систему відправляти підтвердження передавальній стороні про прийом даних.

2.4 Протоколи VPN

Якщо пояснювати просто, то VPN-протокол - це сама суть будь-якого VPN-сервісу. Протокол в даному випадку є фундаментом, на якому збудований сервіс, адже в ньому містяться протоколи передачі даних і стандарти шифрування, які дозволяють вам швидко і захищено обмінювати даними з VPN-серверами. Є п'ять основних VPN-протоколів: OpenVPN, PPTP, L2TP / IPSec, IKEv2 і SSTP. З плином часу стало зрозуміло, яким з цих протоколів не варто довіряти, а якими користуватися не тільки можна, а й навіть потрібно.

2.4.1 PPTP

Цей протокол розроблений асоціацією, очолюваної Microsoft, і являє собою тунелювання «точка-точка», тобто створюється віртуальна приватна мережа всередині загальної мережі, цей протокол був, є і залишається стандартом VPN з моменту створення. Це перший VPN-протокол, підтримуваний Windows, безпека забезпечується різними методами аутентифікації, наприклад, найпоширеніший з них MS_CHAP v2.

Кожен пристрій, що працює з VPN, підтримує PPTP за замовчуванням, і, оскільки його дуже просто налаштувати, цей протокол продовжує залишатися найпопулярнішим серед власників компаній і VPN-провайдерів. Це також найшвидший протокол, так як для його реалізації потрібно найменше обчислень.

Однак, хоча за замовчуванням використовується 128-бітове шифрування, присутні певні уразливості безпеки, одна з найсерйозніших – не інкапсульована аутентифікація MS-CHAP v2. Через це PPTP можна зламати протягом двох днів. І хоча ця проблема була виправлена Microsoft, все ж рекомендується використовувати протоколи SSTP або L2TP для підвищеної безпеки.

І, звичайно ж, настільки низька захист PPTP обумовлює те, що розшифровка цього протоколу - стандартна процедура на сьогодні. Що ще більше турбує, так це те, що Агентство національної безпеки США розшифровує не тільки справжній трафік, але і дані, які були зашифровані ще в той час, коли протокол PPTP вважався безпечним.

Таблиця 2.2 Переваги та недоліки PPTP протоколу.

Переваги	Недоліки
Висока швидкість	Протокол зламаний Агентством національної безпеки США.
Вбудований клієнт практично на всіх платформах.	Чи не гарантує повну безпеку.
Просте налаштування.	

2.4.2 L2TP і L2TP / IPsec

Протокол тунелювання, на відміну від інших протоколів VPN, які не шифрує і не захищає дані. Через це часто використовуються додаткові протоколи, зокрема IPSec, за допомогою якого дані шифруються ще до передачі. Всі сучасні пристрої та системи, сумісні з VPN, мають вбудований протокол L2TP / IPSec. Установка і налаштування відбуваються легко і не займають багато часу, проте може виникнути проблема з використанням порту UDP 500, який блокується файрвол NAT. Так що, якщо протокол використовується з брандмауером, може знадобитися переадресація портів.

Чи не відомо про будь-яких великих вразливості IPSec, і при правильному застосуванні, цей протокол забезпечує повний захист конфіденційних даних. Проте, Едвард Сноуден також зазначає, що і цей протокол не так безпечний. Джон Гілмор, засновник і фахівець з безпеки Electric Frontier Roundation, заявляє, що Агентство національної безпеки США навмисно послаблює протокол. Більш того, дворазове капсулирование даних робить протокол не настільки ефективним, як, наприклад, рішення на основі SSL, але при цьому він працює повільніше інших протоколів.[7]

Таблиця 2.3- Переваги та недоліки L2TP і L2TP / IPsec протоколу.

Плюси	Мінуси
Чи вважаються відносно безпечними.	Повільніше ніж OpenVPN.
Доступні в більшості систем і майже на всіх пристроях.	Захист протоколу порушена Агенцією національної безпеки США. Найімовірніше, національна безпека США послаблює навмисно протокол.
Просте налаштування.	Складно використовувати при наявності блокування з боку брандмауера.

2.4.3OpenVPN

Відносно нова технологія з відкритим вихідним кодом, OpenVPN використовує протоколи SSLv3 / TLSv1 і бібліотеку OpenSSL, а також деякі інші технології, що в цілому забезпечує надійне і потужне VPN-рішення для користувачів. Протокол гнучкий в налаштуванні і найкраще працює через UDP-порт, однак його можна налаштувати для роботи з будь-яким іншим портом, так що сервісів типу Google буде важко їх заблокувати.

Інша значуща перевага полягає в тому, що бібліотека OpenSSL підтримує різні алгоритми шифрування, в тому числі 3DES, AES, Camellia, Blowfish, CAST-128, хоча провайдери VPN використовують практично виключно тільки Blowfish або AES / За замовчуванням надається 128-бітове шифрування Blowfish. Зазвичай воно вважається безпечним, проте були відзначені деякі уразливості.

Якщо говорити про шифрування, AES - це найновіша технологія і вона вважається «золотим стандартом». На даний момент не відомо про уразливість

цієї системи, так що вона навіть використовується урядом і секретними службами США для захисту даних. AES краще справляється з об'ємними файлами, ніж, наприклад, Blowfish, так як розмір блоку становить 128 біт, тоді як у Blowfish - 64 біта. Проте, обидва механізми шифрування сертифіковані NIST, а значить, існують певні проблеми, про які ми поговоримо далі.

Перш за все, швидкість OpenVPN залежить від рівня шифрування, хоча зазвичай вона вища, ніж у IPSec. І хоча OpenVPN - це підключення, використовується за умовчанням більшістю VPN-провайдерів, воно не підтримується на будь-яких платформах. Однак активно розробляються додатки від сторонніх виробників, зокрема для Android і iOS.

Установка трохи складніше, ніж для L2TP / IPSec і PPTP, зокрема коли використовується загальне додаток для OpenVPN. Вам буде потрібно не просто завантажити і встановити клієнт, але ще і витратити час на зміну файлів настройки. Деякі VPN-провайдери пропонують попередньо налаштовані клієнти.

Однак, з урахуванням всіх факторів та інформації, представленої Едвардом Сноуденом, здається, що протокол OpenVPN є найбезпечнішим на даний момент. Також передбачається, що він захищений від втручання Агентства національної безпеки США, так як протокол використовує експериментальні методи шифрування. Без сумніву, ніхто не знає всіх можливостей Агентства національної безпеки, однак, швидше за все це єдиний по-справжньому безпечний протокол на сьогодні.

Таблиця 2.4- Переваги та недоліки протоколу OpenVPN.

Плюси	**Мінуси**
Дозволяє обходити більшість файрволов.	Складно налаштовувати.
Гнучке налаштування	Потрібно стороннє ПО.
Відкритий вихідний код- може швидко адаптуватися до нових небезпек.	Підтримка комп'ютерів не погана, але на мобільних пристроях протокол працює не кращим чином.
Сумісний з різними алгоритмами шифрування.	
Високий ступінь безпеки.	

2.4.4 SSTP

Вперше цей протокол був представлений компанією Microsoft в SP1 для Windows Vista, на сьогодні цей протокол доступний для SEIL, Linux, RouterOS, але переважно він розрахований для роботи в Windows. У ньому використовується SSL v3, так що вас чекають практично ті ж переваги, що й у OpenVPN, зокрема, можливість обходити файрволи NAT. SSTP - це стабільний і простий у використанні протокол, інтегрований в Windows.

Однак, усі права на нього володіє Microsoft. Відомо, що гігант індустрії активно працює зі спецслужбами, крім того, ходять чутки про те, що в систему Windows спочатку вбудовані механізми стеження.

Таблиця 2.5-Переваги та недоліки SST.

Плюси	Мінуси
Дозволяє обходити більшість файрволов.	Оскільки протоколом володіє компанія Microsoft, перевірити чи поліпшити його неможливо.
Рівень безпеки залежить від обраного шифру, зазвичай він досить високий.	Працює тільки на платформі Windows
Гарна взаємодія з ОС Windows.	
Підтримка Microsoft.	

2.4.5 IKEv2

Це протокол тунелювання (протокол обміну ключами, версія 2), розроблений Cisco і Microsoft, він вбудований в Windows 7 і наступні версії. Протокол допускає модифікації з відкритим вихідним кодом, зокрема для Linux та інших платформ, також підтримуються пристрої Blackberry.

Він добре підходить для установки автоматичного VPN-підключення, якщо інтернет-з'єднання періодично розривається. Користувачі мобільних пристроїв можуть скористатися ним як протоколом для бездротових мереж за замовчуванням - він дуже гнучкий і дозволяє без праці переключатися між мережами. Крім того, він прекрасно підійде для користувачів Blackberry - це один з небагатьох протоколів, з підтримкою подібних пристроїв. Хоча IKEv2 доступний на меншій кількості платформ в порівнянні з, наприклад, IPSec, він вважається досить хорошим протоколом з точки зору стабільності, безпеки і швидкості роботи.

Таблиця 2.4.5- Переваги та недоліки IKEv2.

Плюси	**Мінуси**
Високий ступінь безпеки - підтримка різних шифрів, зокрема 3DES, AES, AES 256.	Підтримує мала кількість платформ.
Також підтримує пристрої Blackberry.	Порт UDP 500 блокується простіше, ніж рішення на основі SSL, як, наприклад, SSTP або OpenVPN
Стабільно підключається знову після розриву з'єднання або зміни мереж.	Вихідний код не відкритий
Просто встановити і налаштувати.	Установка на сервер досить важка, це може викликати потенційні проблеми.
Швидше, ніж L2TP, PPTP і SSTP.	

Звичайно, вибір оптимальної реалізації VPN залежить від конкретних завдань. Однак загальні висновки такі:

PPTP - стабільний і простий у використанні, проте досить уразливий з погляду безпеки. Непоганий вибір при мінімальних вимогах до конфіденційності тунелю, альтернатива IPsec або L2TP + IPsec (які в тих же умовах надають більше можливостей: кроссплатформеність, поріг входження в конфігурацію для адміністратора, більш високий рівень безпеки).

IPsec своєму розпорядженні велику кількість алгоритмів шифрування і аутентифікації для VPN, незважаючи на те що є стеком протоколів для захисту IP-пакетів при їх передачі. IPsec ідеальний для розгортання VPN, безпеку яких особливо актуальна. Для таких завдань IPsec краще використовувати в зв'язці з L2TP. У плані можливостей IPsec - один з кращих варіантів для VPN.[11]

L2TP в зв'язці з IPsec також оптимальний і в плані безпеки, і в плані сумісності з популярними ОС. Недоліки: можлива необхідність додаткового налаштування роутера / firewall на дозвіл використовуваних LT2P / IPsec портів (UDP 1 701, UDP 4500, UDP 500), а також подвійна інкапсуляція, уповільнює роботу тунелю.

Протокол SSTP відрізняється зручністю конфігурації, стабільністю та безпекою, але прив'язаний тільки до систем Microsoft. На інших ОС SSTP на порядок менш функціональний.

OpenVPN за багатьма параметрами збалансований ідеально.

Швидкість: за рахунок стиснення LZO і опції роботи по протоколу UDP

Стабільність: особливо при роботі через TCP

Гнучкість конфігурації: доступні додаткові опції, наприклад, балансування навантаження, різні типи аутентифікації

Кросплатформеність: наявність клієнтських додатків для більшості сучасних ОС, в т.ч. мобільних

Безпека: завдяки роботі з усіма інструментами бібліотеки openssl

Однак навіть первинна конфігурація OpenVPN може виявитися складніше, в порівнянні іншими реалізаціями.[9]

3. РЕАЛІЗАЦІЯ ВИБРАНОГО ПРОТОКОЛУ VPN

Для реалізації було розглянуто всі протоколи. Але найбільш раціональним для створення мережі на базі VPN це – IPces протокол.

Архітектура вибраного протоколу показана на рисунку 3.1.

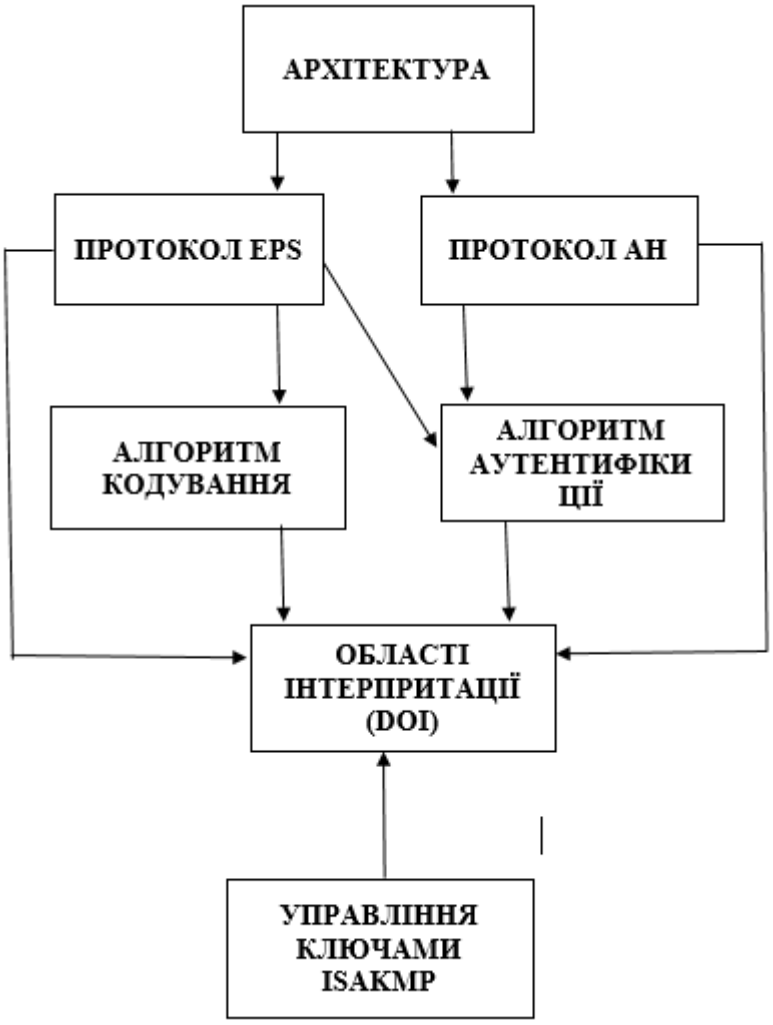


Рис 3.1- Архітектура протоколу VPN

AH (Authentication Header)- управління цілісністю переданих даних і аутентифікацію. призначений для забезпечення аутентифікації відправника, контролю цілісності даних та додатково для запобігання повторному відтворенню пакета - за умови, що приймаюча сторона налаштована на перевірку серійного номера пакета. Поля пакетів IP, які

змінюються з часом, не підлягають перевірці цілісності. АН захищає дані протоколу вищого рівня та ті поля заголовків IP, які не змінюються по маршруту доставки або змінюються передбачувано - кількість "непередбачуваних" полів невелика - це прийом (клас трафіку), мітка потоку та обмеження стрибків. присутній необов’язковий заголовок вихідної маршрутизації.).

ESP (Encapsulating Security Payload)- шифрування даних.

Надає три види охоронних послуг:

- Забезпечення конфіденційності (шифрування вмісту пакетів IP, а також частковий захист від аналізу трафіку через тунельний режим);

- Цілісність IP-пакетів, аутентифікація джерела даних.

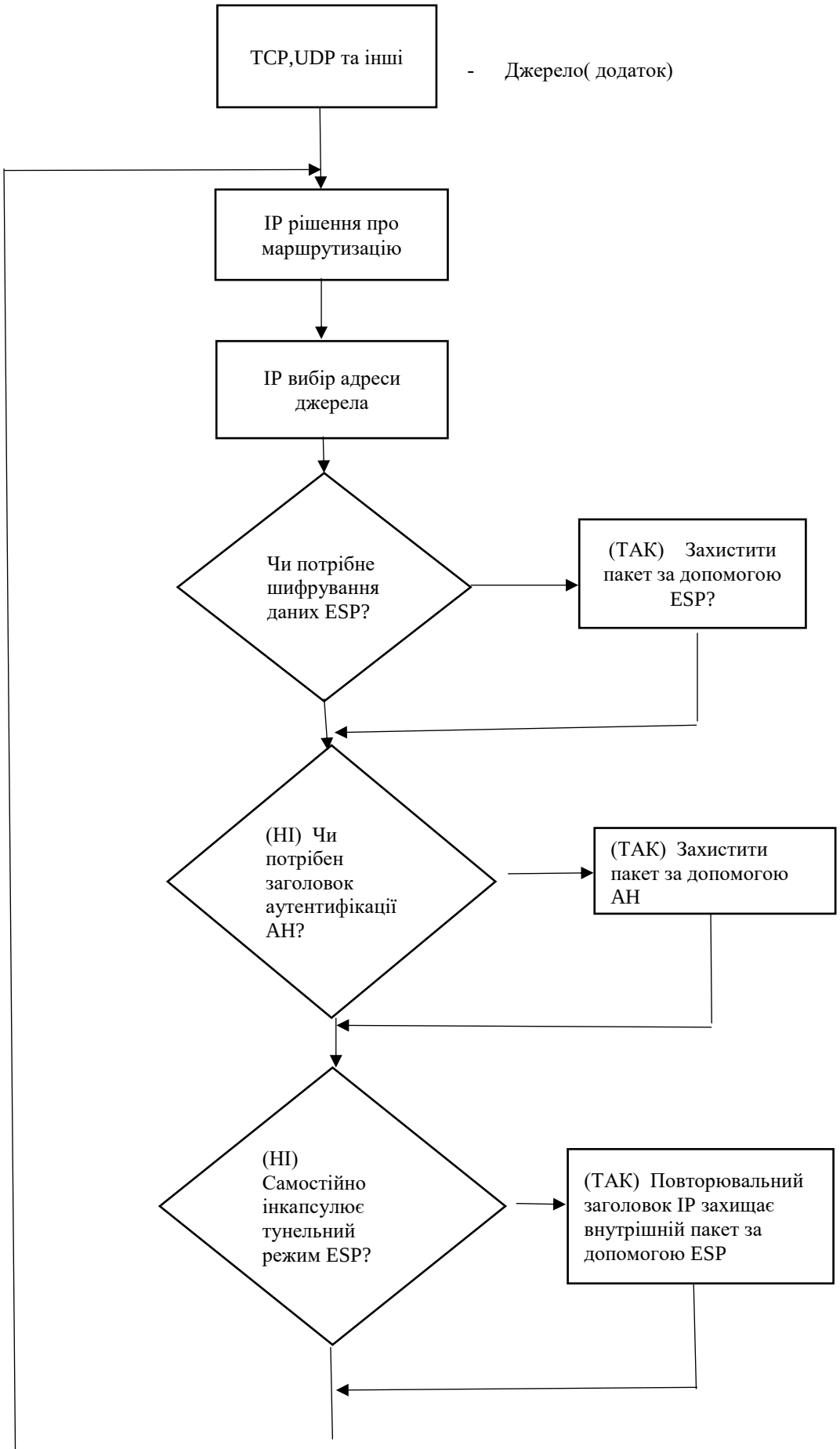
- Забезпечення захисту від відтворення IP-пакетів.

Функціональність ESP ширша, ніж АН (додано шифрування); ESP не повинен надавати всі послуги, але повинен включати або конфіденційність, або автентифікацію. Розмір заголовка - це не стільки заголовок, скільки код (накладення) кодованого вмісту. Наприклад, наступне заголовкове посилання не можна розмістити на початку відписаної частини, оскільки воно втратить конфіденційність.

ISAKMP (Internet Security Association and Key Management Protocol)- управління установкою з'єднання, взаємну аутентифікації кінцевими вузлами один одного і обмін секретними ключами.

SA (Security Association) - це набір параметрів про те як сторони будуть надалі використовувати ті чи інші властивості протоколів зі складу IPsec.[8]

3.1Схема алгоритму IPsec



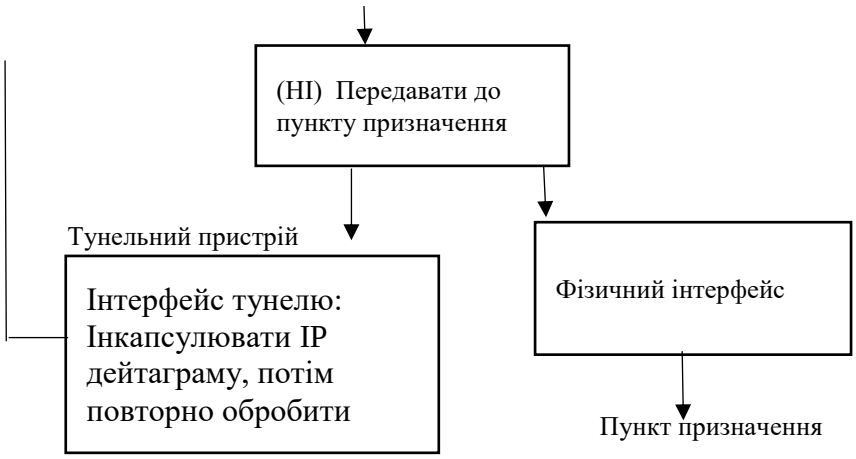
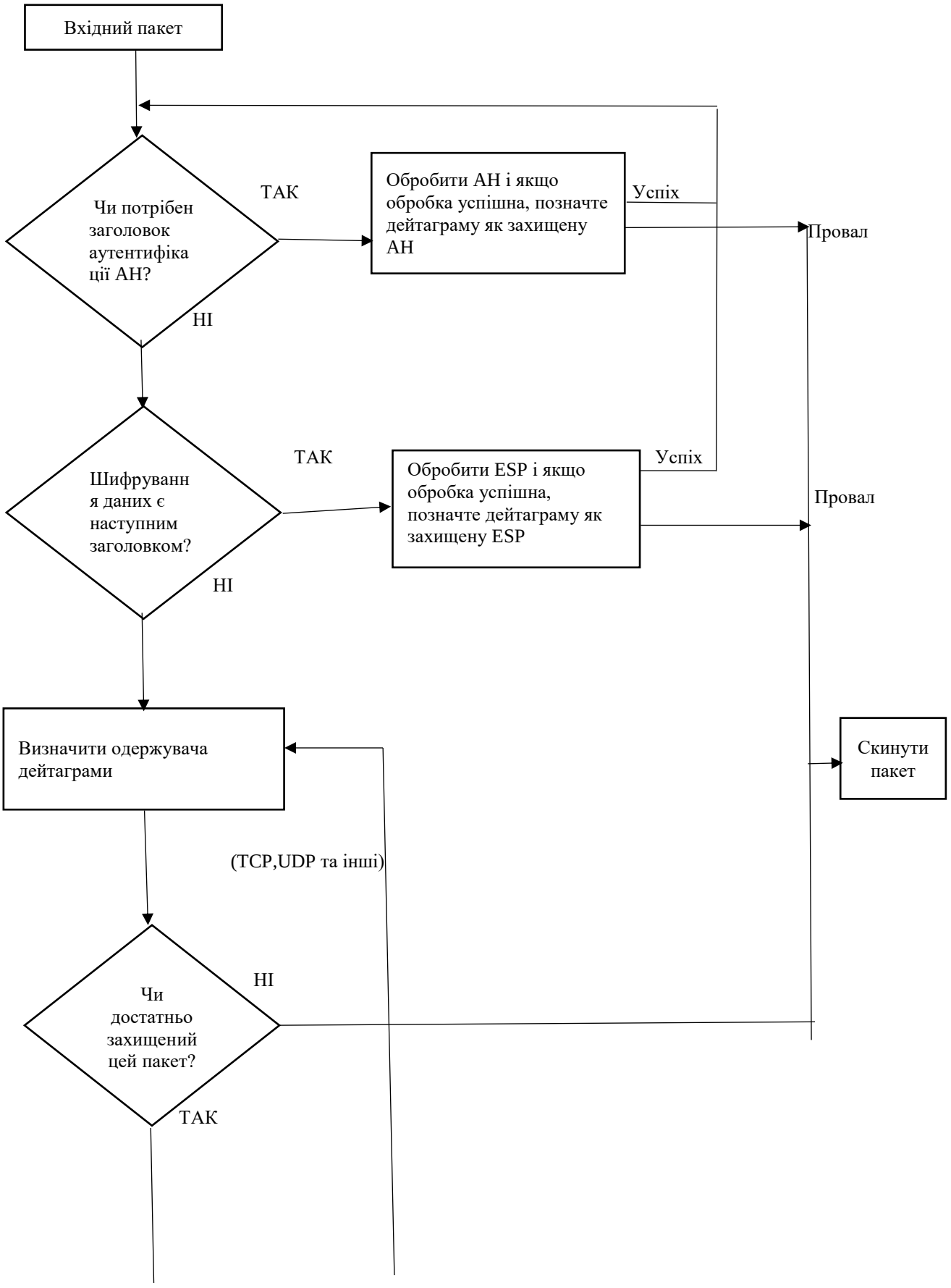


Рисунок 3.2-Схема алгоритму IPsec, застосований до процесу вихідних пакетів


Вхідний пакет
Чи потрібен заголовок аутентифіка ції АН?
ТАК
Обробити АН і якщо обробка успішна, позначте дейтаграму як захищену АН
Успіх
Провал
НІ
Шифруванн я даних є наступним заголовком?
ТАК
Обробити ESP і якщо обробка успішна, позначте дейтаграму як захищену ESP
Успіх
Провал
НІ
Визначити одержувача дейтаграми
Скинути пакет
(TCP,UDP та інші)
Чи достатньо захищений цей пакет?
НІ
ТАК

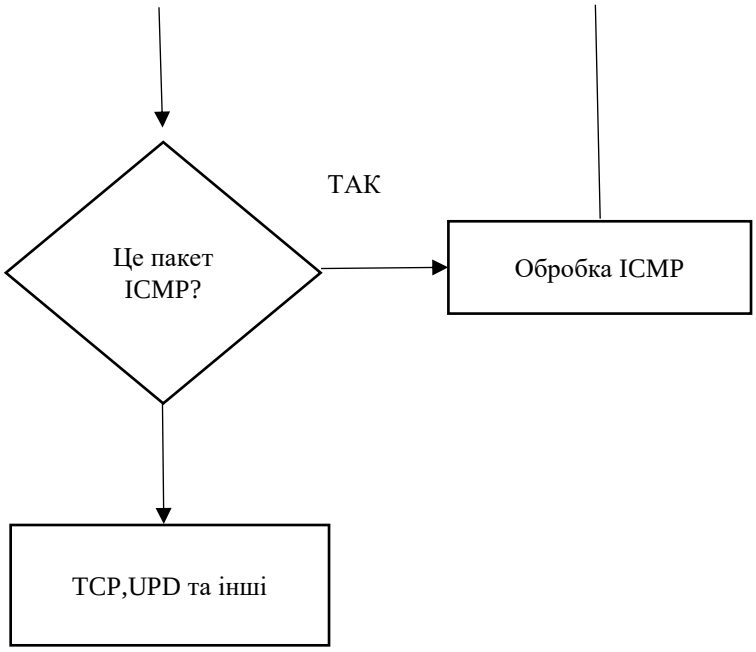


Рисунок 3.3 -Схема алгоритму IPsec застосований до процесу вхідних даних

3.2 Етапи створення корпоративної мережі на базі VPN

Етап 1: 1) Створюємо топологію Cisco Packet Tracer.

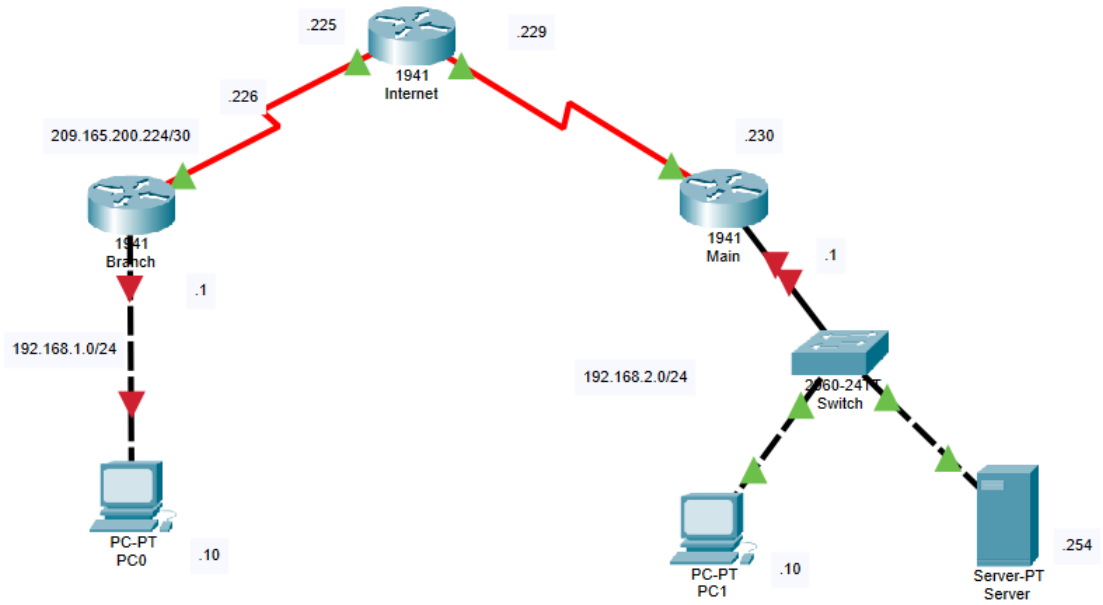


Рисунок 3.1– Топологія проєктованої мережі.

Таблиця 3.2-пристрої топології

Пристрій	Інтерфейс	IP-адрес	Маска підмережі	Шлюз за умовчуванням
Branch	g0/0	192.168.1.1	255.255.255.0	-
	S0/0/0	209.165.200.226	255.255.255.252	-
Main	G0/0	192.168.2.1	255.255.255.0	-
	S0/0/1	209.165.200.230	255.255.255.252	-
Switch	VLAN1	192.168.2.2	255.255.255.0	192.168.2.1
Server	VLAN1	192.168.2.254	255.255.255.0	192.168.2.1
PC0	NIC	192.168.1.10	255.255.255.0	192.168.1.1
PC1	NIC	192.168.2.10	255.255.255.0	192.168.2.1

2) Синім-визначено головний офіс Main, рожевим- віддалений працівник Branch.

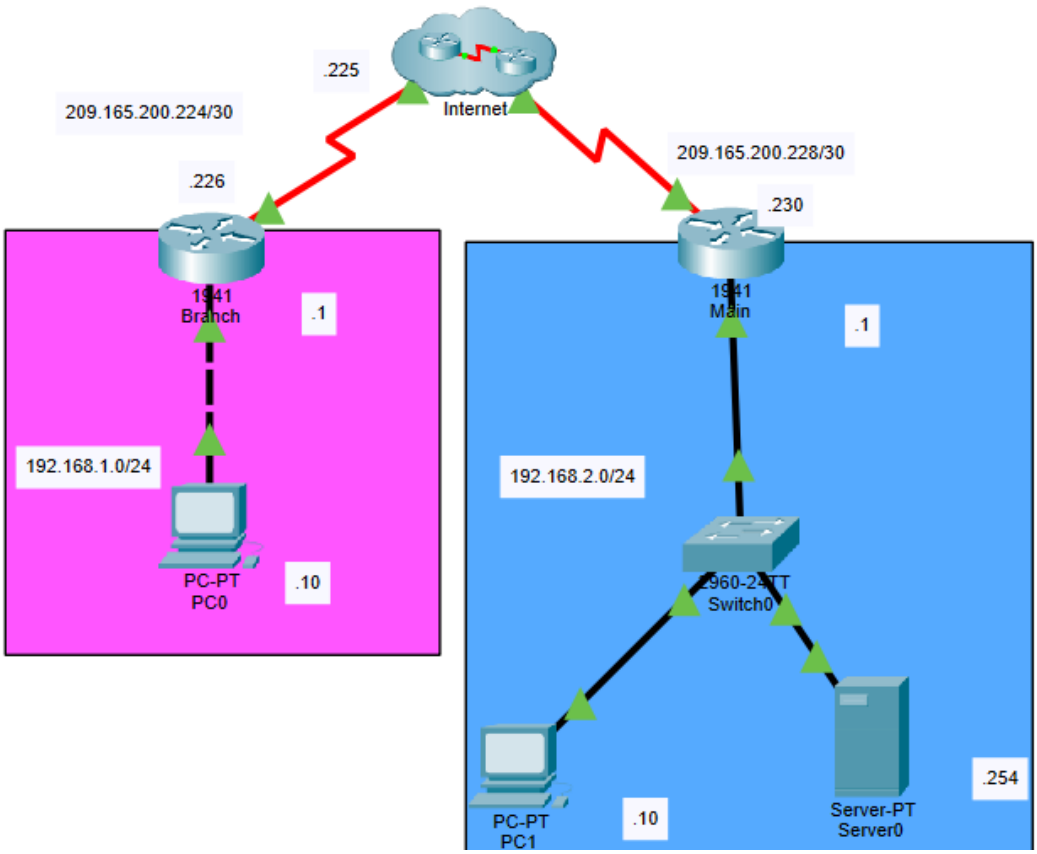


Рисунок 3.2- Топологія проєктованої мережі.

3) Налаштування IP-адреси Branch:

Router>en

Router#conf term

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

Router(config)#hostname Branch

Branch(config)#int g0/0 [визначили интерфейс]

Branch(config-if)#ip address 192.168.1.1 255.255.255.0

Branch(config-if)# no shutdown

Branch(config-if)#

%LINK-5-CHANGED: Interface /……

Branch(config-if)# int s0/0/0

Branch(config-if)#ip address 209.165.200.226 255.255.255.252

Branch(config-if)# no shutdown

…

4) Налаштування маршрутизатора Internet

Router>en

Router#conf term

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

Router(config)#hostname Internet

Internet (config)#int s0/0/0 [визначили интерфейс]

Internet (config-if)#ip address 209.165.200.225 255.255.255.252

Internet (config-if)# clock rate 4000000[швидкість каналу в бітах]

Internet (config-if)# no shutdown

%LINK-5-CHANGED: Interface /……..

Internet (config-if)# int s0/0/1

Internet (config-if)# ip address 209.165.200.229 255.255.255.252

Тепер налаштовуємо ті самі частоти маски підмережі

Internet(config-if)# no shutdown

%LINK-5-CHANGED: Interface /……..

Internet (config-if)# clock rate 4000000

Internet (config-if)# no shutdown

%LINK-5-CHANGED: Interface /……..

5) Налаштування основного маршрутизатора Main:

Router>en

Router#conf term

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

Router(config)#hostname Main

Main(config)#int g0/0 [визначили интерфейс]

Main(config-if)#ip address 192.168.2.1 255.255.255.0

Main(config-if)# no shutdown

%LINK-5-CHANGED: Interface /……

Main(config)#int s0/0/1

Main(config-if)#ip address 209.165.200.230 255.255.255.252

Main(config-if)# no shutdown

%LINK-5-CHANGED: Interface /……

Етап 2: Налаштовуємо IP адреси всіх ПК та сервера.

1) Налаштування IP адреси ПК PC0

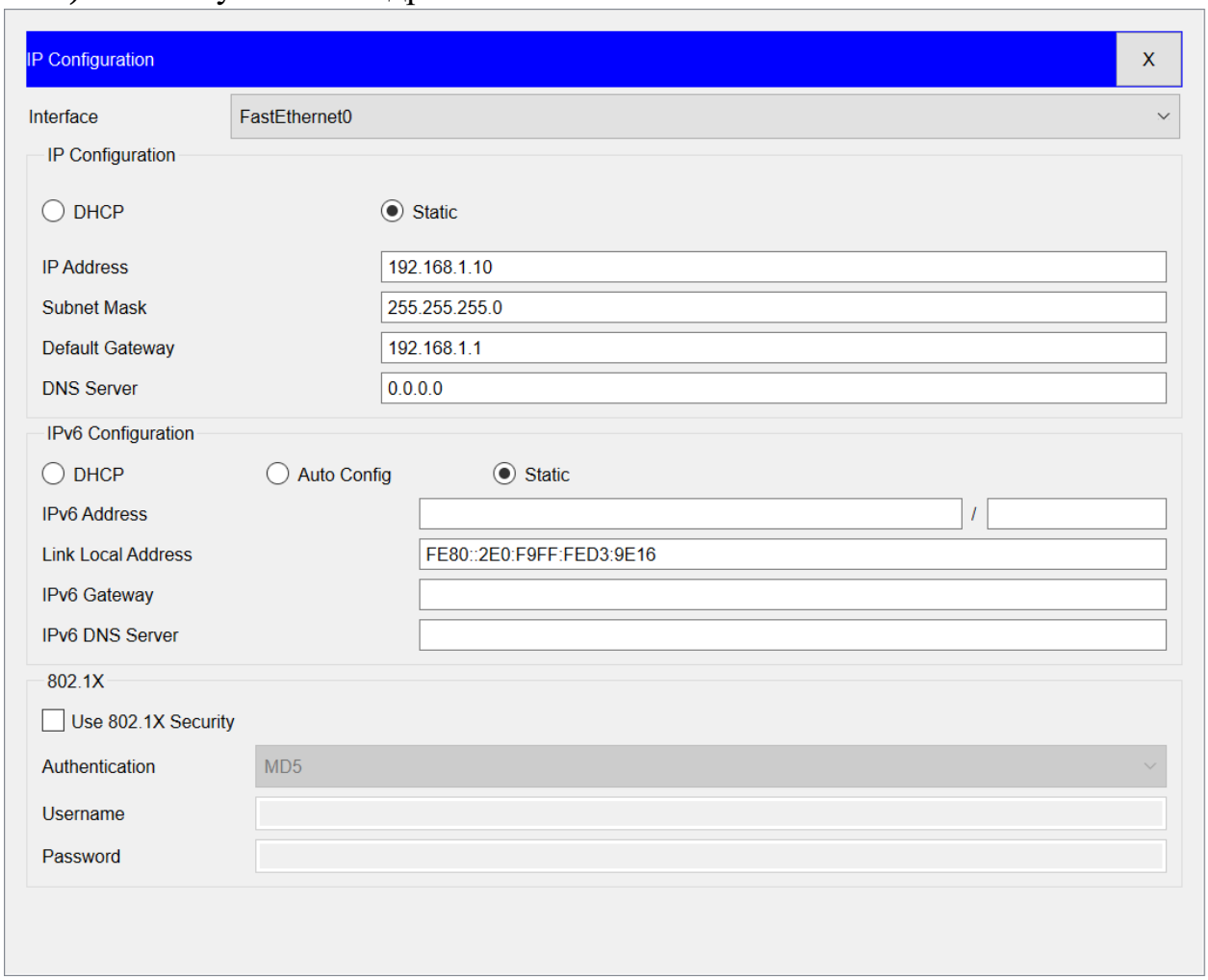


Рисунок 3.3-Налаштування IP адреси PC0

2) Налаштування IP адреси ПК PC1

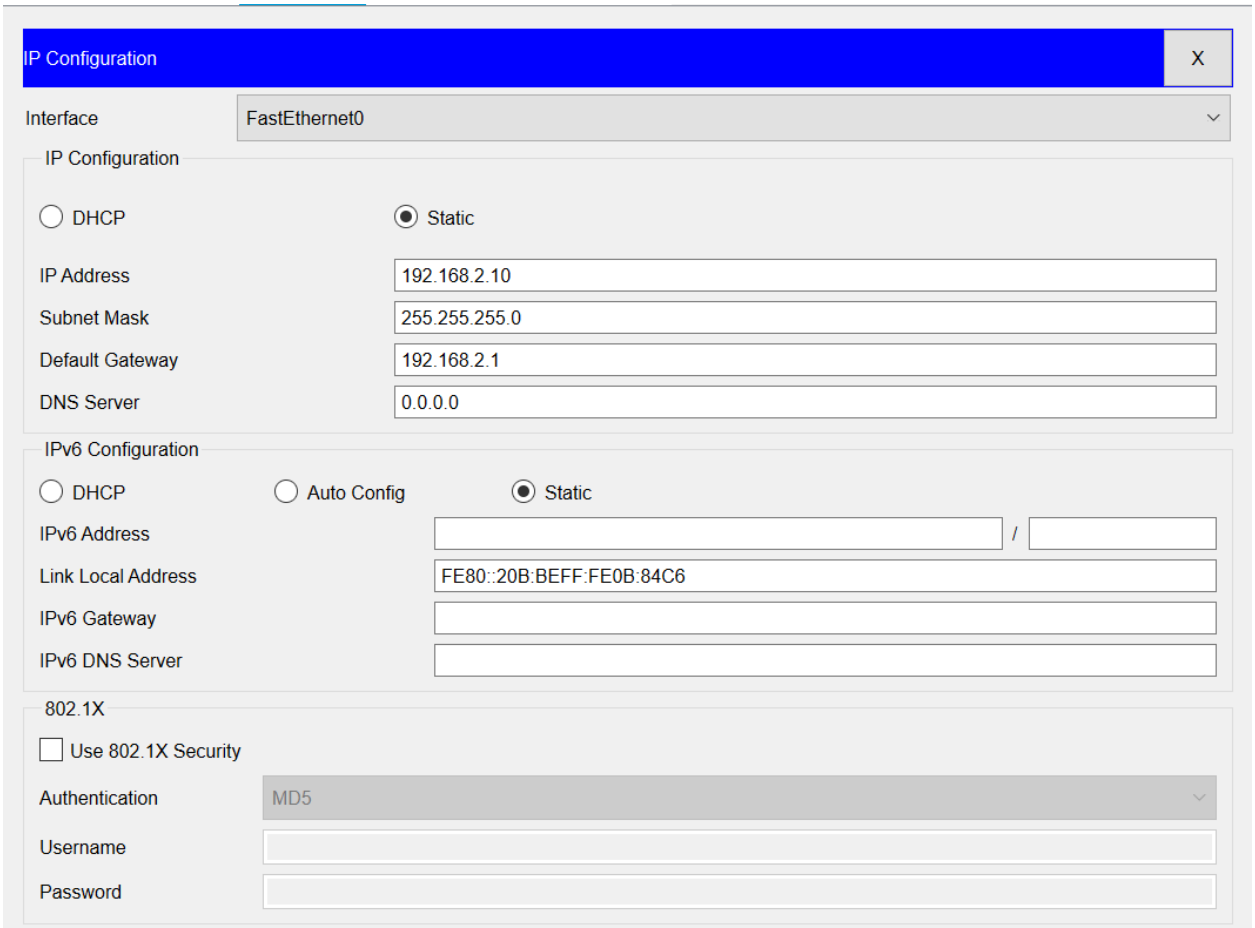


Рисунок 3.4 - Налаштування IP адреси PC1

3)Налаштування IP адреси сервера:

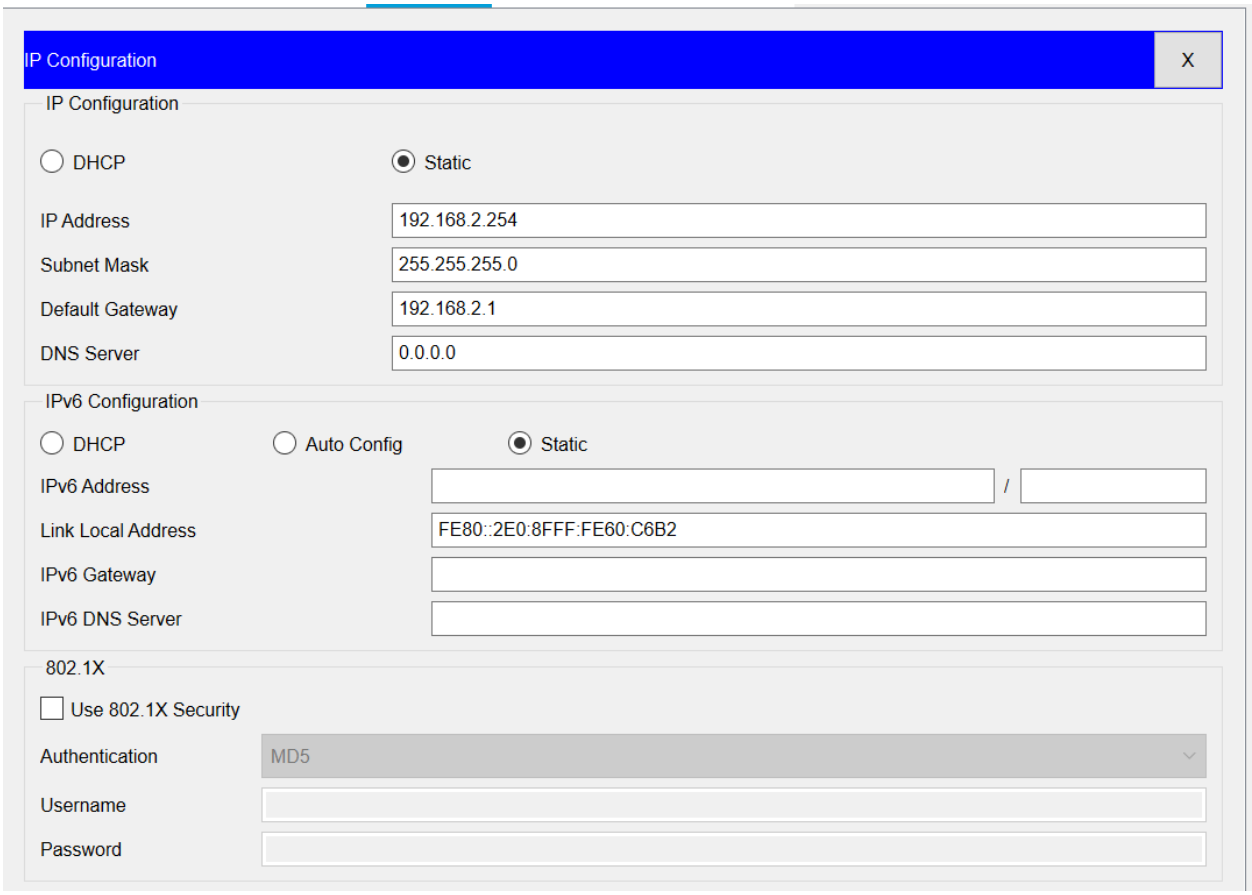


Рисунок 3.5 - Налаштування IP адреси сервера

Етап 3:Налаштовуємо маршрутизацію на маршрутизаторах Branch та Main:

Branch(config-if)#exit

Branch(config) ip route 0.0.0.0 0.0.0.0 s0/0/0

%Default route without gateway, if not a point-to-point interface, may impact performance

Main(config-if)#exit

Main(config) ip route 0.0.0.0 0.0.0.0 s0/0/1

%Default route without gateway, if not a point-to-point interface, may impact performance

Етап 4: Перевіримо працездатність з'єднання:

Packet Tracer PC Command Line 1.0

C:\>ipconfig

FastEthernet0 Connection:(default port)

Link-local IPv6 Address.....: FE80::2E0:F9FF:FED3:9E16

IP Address.....: 192.168.1.10

Subnet Mask.....: 255.255.255.0

Default Gateway.....: 192.168.1.1

Bluetooth Connection:

Link-local IPv6 Address.....: ::

IP Address.....: 0.0.0.0

Subnet Mask.....: 0.0.0.0

Default Gateway.....: 0.0.0.0

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=15ms TTL=255

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 15ms, Average = 3ms

Перший ping працює з ПК на найближчий роутер.

:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 209.165.200.225:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Другій ping не працює на роутері Internet тому що, на цьому роутері не налаштована маршрутизація.

C:\>ping 209.165.200.230

Pinging 209.165.200.230 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 209.165.200.230:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Етап 5: Створюємо стандартний список контроля доступу ALC_NAT

Branch(config-if)#exit

Branch(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0

%Default route without gateway, if not a point-to-point interface, may impact performance

Branch(config)# ip access-list standard ACL_NAT

Branch(config-std-nacl)#permit 192.168.1.0 0.0.0.255

Branch(config-std-nacl)#exit

Branch(config)#ip nat inside source list ACL_NAT interface s0/0/0

Branch(config)#int s0/0/0

Branch(config-if)# ip nat outside

Branch(config-if)#int g0/0

Branch(config-if)#ip nat inside

Етап 6: Налаштувати адресний пул

ASA вимагає метод призначення IP-адрес користувачам. В цьому розділі як приклад використовуються пули адрес.

Main(config)#ip local pool PoolVPN 192.168.2.100 192.168.2.115

Main(config)#aaa new-model

Main(config)#aaa authentication login UserVPN local

Main(config)#aaa authorization network GroupVPN local

Main(config)#username uservpn secret ciscovpn

Етап 7:Створіть набір перетворень IKEv1 або пропозицію IKEv2

У цьому розділі показано, як налаштувати набір перетворень (IKEv1) або пропозицію (IKEv2), які об'єднують метод шифрування і метод аутентифікації.

Наступні кроки показують, як створити пропозицію IKEv1 і IKEv2.

Main(config)#crypto isakmp policy 100

Main(config-isakmp)#encryption aes 256

Main(config-isakmp)#hash sha

Main(config-isakmp)#authentication pre-share

Main(config-isakmp)#group 5

Main(config-isakmp)#lifetime 3600

Main(config-isakmp)#exit

Main(config-)# crypto isakmp client configuration

% Incomplete command

Main(config)# crypto isakmp client configuration group GroupVPN

Main(config-isakmp-group)#key ciscogroupvpn

Main(config-isakmp-group)#pool PoolVPN

Налаштуйте набір перетворень IKEv1, який визначає шифрування IPsec IKEv1 і алгоритми хешування, які будуть використовуватися для забезпечення цілісності даних.

Main(config)#crypto ipsec transform-set SetVPN esp-aes esp-sha-hmac

Main(config)#crypto dynamic-map DynamicVPN 100

Main(config-crypto-map)#set transform-set SerVPN

Main(config-crypto-map)#reverse-route

Після всіх операцій, заходимо в VPN configuration та вводимо дані.

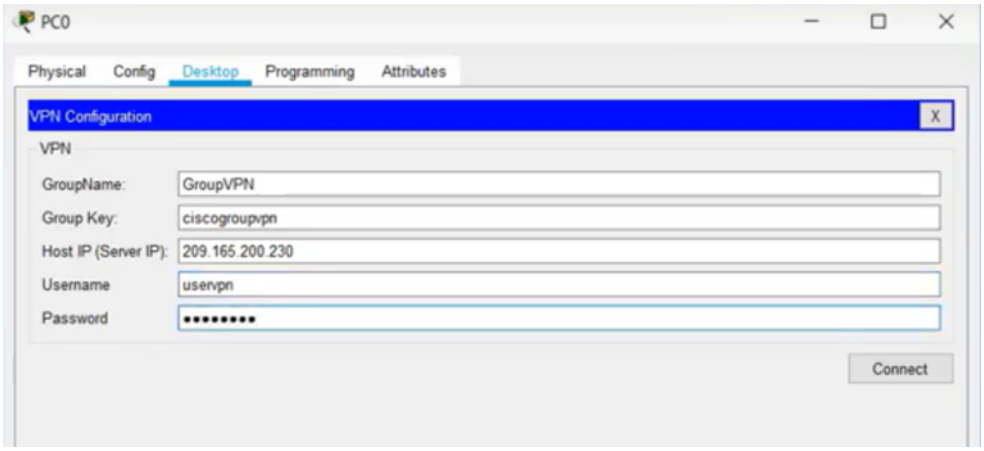


Рисунок 3.6- Під’єднання користувача VPN

Отримали результат роботи: Проведено налаштування мережевих пристроїв. Реалізована можливість підключення до корпоративної мережі віддаленого доступу використовуючи протокол IPsec.

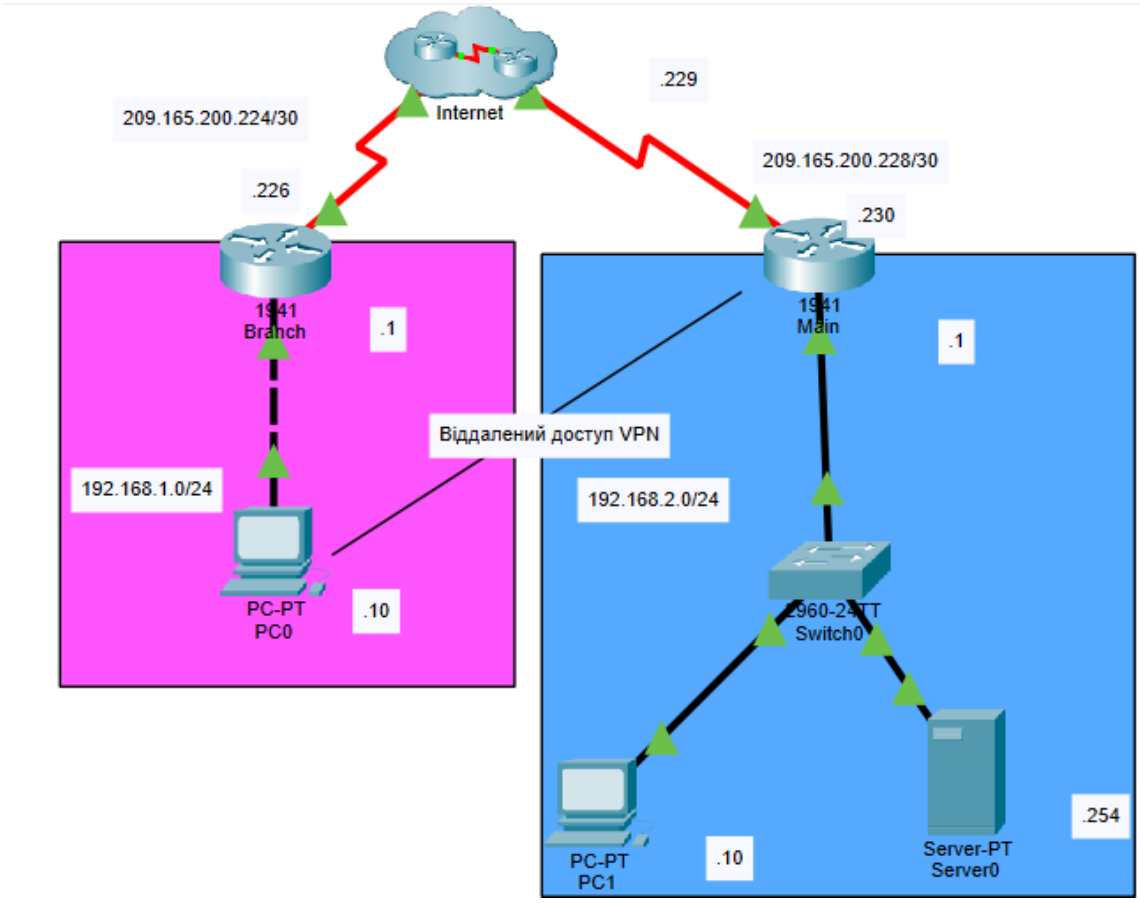


Рисунок 3.7- Спрощена топологія проєктованої мережі

- Налаштування маршрутизатора Main корпоративної мережі:

Main#SHOW RUN
Building configuration...

Current configuration : 1627 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Main
!
!
aaa new-model
!
aaa authentication login UserVPN local
!
!
aaa authorization network GroupVPN local
!
no ip cef
no ipv6 cef

```
!
!
!
username uservpn secret 5 $1$mERr$Hz.95IyOHimhrSwO9HzIo/
!
!
license udi pid CISCO1941/K9 sn FTX1524E6Z8-
license boot module c1900 technology-package securityk9
!
!
!
crypto isakmp policy 100
encr aes 256
authentication pre-share
group 5
lifetime 3600
!
!
!
crypto isakmp client configuration group GroupVPN
key ciscogroupvpn
pool PoolVPN
!
!
crypto ipsec transform-set SetVPN esp-aes esp-sha-hmac
!
crypto dynamic-map DynamicVPN 100
set transform-set SetVPN
reverse-route
!
crypto map StaticMap client authentication list UserVPN
crypto map StaticMap isakmp authorization list GroupVPN
crypto map StaticMap client configuration address respond
crypto map StaticMap 20 ipsec-isakmp dynamic DynamicVPN
!
!
!
!
spanning-tree mode pvst
!

!
!
interface GigabitEthernet0/0
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
```

```
speed auto
shutdown
!
interface Serial0/0/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/0/1
ip address 209.165.200.230 255.255.255.252
crypto map StaticMap
!
interface Vlan1
no ip address
shutdown
!
ip local pool PoolVPN 192.168.2.100 192.168.2.115
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
ip flow-export version 9
!
!

!
!
line con 0
!
line aux 0
!
line vty 0 4
!
!
!
    end
```

- Налаштування маршрутизатора Branch мережі віддаленого доступу:

```
Branch>EN
Branch#SH RUN
Building configuration...

Current configuration : 959 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Branch
!
```

```
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX15242VBR-
!
!
spanning-tree mode pvst
!
!
!
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 209.165.200.226 255.255.255.252
ip nat outside
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip nat inside source list ACL_NAT interface Serial0/0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip flow-export version 9
!
!
ip access-list standard ACL_NAT
permit 192.168.1.0 0.0.0.255
!
!
!
!
```

```
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

- Налаштування маршрутизатора Internet:

```
Internet#SHOW RUN
Building configuration...

Current configuration : 791 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Internet
!
!
no ip cef
no ipv6 cef
!
!
license udi pid CISCO1941/K9 sn FTX1524VY5P-
!
!
spanning-tree mode pvst
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 209.165.200.225 255.255.255.252
clock rate 4000000
```

```
!
interface Serial0/0/1
ip address 209.165.200.229 255.255.255.252
clock rate 4000000
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
    End
```

ВИСНОВКИ

VPN на сьогоднішній день дуже актуальна тема. Аби приховати дані та забезпечити безпеку в мережі Internet. Звісно, у VPN є свої недоліки: якісний VPN коштує дорого, буває повільна швидкість Інтернету, в 2021 році є можливість обходу VPN сервісу. Але є також і переваги це- анонімність, захищений обмін даними, обхід геоблакувань та інші переваги.

В даному проєкті розроблялась корпоративна мережа віддаленого доступу VPN. Були розглянуті протоколи та методи реалізації віртуальних мереж. Проаналізувавши всі доступні протоколи, та порівнявши переваги та недоліки кожного з них. І таким чином за основу був взятий протокол IPSec.

Використали програму Cisco Packet Tracer в якій спроєктували топологію майбутньої мережі. Для підключення віддалених працівників.

Можна заробити висновок, що VPN дає можливість віддаленим працівникам безпечно підключатися до сервера компанії та обмінюватися файлами.

СПИСОК ДЖЕРЕЛ ПОСИЛАНЬ

1. Igor Zagradanin History of VPN URL-https://www.geosurf.com/blog/history-of-vpn-the-quest-for-a-better-internet/04.04.2021: Текст – електронний.
2. Vinay Prajapati /URL-https://www.techprevue.com/pros-and-cons-of-vpn/ 24.01.2021:Текст -електронний.
3. URL-https://studfile.net/preview/5337444/page:4/#
4. URL-https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html 13.10.2008 Текст-електронний/14106.
5. Virtual Private network/ experpted from: Broadband Tlecommunication Handbooks//Regis J. Bates
6. URL-https://www.cisco.com/c/ru_ru/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html#vpn_tech/ 1.01.1970/14106.
7. Основы локальных компьютерных сетей А.Сергеев /издательство-Лань2016-32с
8. С.В.Запечников, Н.Г. Милославская, Л.И.Толстой Основы построения виртуальных частных сетей: учебное пособие для вузов М.: Горячая линия- Телеком,2003-249с.
9. Третяк М.О. Пристрій кодування на основі матричного коду з перевіркою на парність / М.О. Третяк, О. В. Д’яченко, Т. О. Протасова // ФЕЕ–2021 : матеріали та програма міжнародної науково-технічної конференції студентів та молодих вчених, Суми, 19–23 квітня 2021. – С. 101.
10. У.Одом /Официальное руководство Cisco по подготовке к сертифицированным экзаменам CCNA ICND2 200-10. Маршрутизация и коммутация./2016.

11. Сравнение протоколов URL-https://ru.vpnmentor.com/blog.b2-vpn-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/ 27.042021.