МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ВИПУСКНА РОБОТА

на тему:

«Надійні і високозахищені канали передачі даних в межах локальних мереж і мережі Інтернет»

Завідувач

випускаючої кафедри **Довбиш А.С.**

Керівник роботи **Ободяк В.К.**

Студента групи КБ – 61 **Сороки А.В.**

СУМИ 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерних наук

Затверджую_____

Зав. кафедрою Довбиш А.С.

"_____"_____2020 г.

ЗАВДАННЯ

до випускної роботи

Студента четвертого курсу, групи КБ-61 спеціальності "Кібербезпека" денної форми навчання Сороки Андрія Васильовича.

Тема: " Надійні і високозахищені канали передачі даних в межах локальних мереж і мережі Інтернет "

Затверджена наказом по СумДУ

№_____ от _____2020 г.

Зміст пояснювальної записки: 1) огляд існуючих методів реалізації для побудови мереж забезпечення комп'ютерного зв'язку; 2) опис основних положень, критеріїв захисту інформації, оцінка та порівняння актуальних загроз в сфері комп'ютерних мереж; 3) розробка та налаштування прототипу комп'ютерної мережі; 4) аналіз проведеної роботи.

Дата видачі завдання "_____"_____2020 г.

Керівник випускної роботи _____ Ободяк В.К.

Завдання прийняв до виконання _____ Сорока А.В.

РЕФЕРАТ

Записка: 50 стор., 16 рис., 2 табл., 14 джерел.

Об’єкт дослідження — процес створення і налагодження надійних і високозахищені канали передачі даних в межах локальних мереж і мережі Інтернет.

Мета роботи — створення прототипу локальної захищеної мережі з використанням безпечних протоколів передачі інформації, створення безпечного каналу зв’язку для передачі інформації між декількома локальними мережами.

Методи дослідження — використання протоколів передачі інформації для створення безпечного каналу зв’язку.

Результати — на практичному прикладі з використанням програмного забезпечення Cisco Packet Tracer 6.2 створено та налаштовано локальну мережу з використання технології VPN для об’єднання двох частин мережі. На прикладі окремо створеної мережі організовано DMZ-зону для зберігання даних, та розмежування прав доступу до неї.

КОМП’ЮТЕРНА МЕРЕЖА, ІНФОРМАЦІЙНА БЕЗПЕКА, МАРШРУТИЗАТОР, КОМП’ЮТЕР, ЛОКАЛЬНА МЕРЕЖА, ІНТЕРНЕТ-ЗАГРОЗА, VPN-ТУНЕЛЬ, VPN-МЕРЕЖА.

ЗМІСТ

ВСТУП

З стрімким розвитком комп’ютерної галузі виникає необхідність в захисті інформації, в її безпечному передаванні та поширенні. Захист інформації – є однією із основних постійних проблем в її досягненні та реалізації. Актуальним об'єктом дослідження науково-прикладного напрямку є саме проблеми інформаційної безпеки, її структуризація, а також джерела інформаційних загроз, показники, критерії та нормативи інформаційної безпеки. При створенні теорії інформаційної безпеки первинним завданням слід вважати формування системи понять, серед яких базовими є інформаційна небезпека, інформаційна загроза і інформаційна безпека. Інформаційною безпекою можна назвати заходи щодо захисту інформації від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок у доступі. Інформаційна безпека включає в себе заходи по захисту процесів створення даних, їх введення, обробки і виведення. Мета інформаційної безпеки - убезпечити цінності системи, захистити і гарантувати точність і цілісність інформації та мінімізувати руйнування, які можуть мати місце, якщо інформація буде модифікована або зруйнована.

1 ОГЛЯД ІСНУЮЧИХ РІШЕНЬ

Для забезпечення зв’язку між робочими станціями користувачів, швидкого обміну та передавання інформації створюються комп’ютерні мережі, які можуть мати різні розміри, мету створення, призначення, але поділяються в основному на декілька типів: локально обчислювальні мережі (LAN), регіонально обчислювальні мережі (WAN), глобальна обчислювальна мережа (Internet).

Не зважаючи на тип та архітектуру мережі вони мають основну мету – забезпечення зв’язку, тобто по суті використовується все існуючі рішення та методи для того, щоб цього досягти. Не менш важливим аспектом є впровадження засобів інформаційної безпеки, різних методів захисту мережі від стороннього втручання, забезпечення цілісності та конфіденційності особистих, корпоративних даних та даних подібного типу до котрих повинні мати доступ лише конкретні користувачі або групи осіб.

1.1 Локальна мережа – мета та ціль створення

Для здійснення безпечного документообміну, підвищення захищеності та зручності при передаванні інформації між робочими станціями, створюється локальна мережа, тобто LAN (Local area network) – вона являю собою комп’ютерну мережу яка покриває не велику територію, зазвичай розташовану в невеликій групі будівель.

Вона представляє собою набір комп’ютерного обладнання яке має можливість взаємодіяти з іншим обладнанням або ж подібними пристроями цієї ж мережі для обміну інформацією, та сполучене між собою за допомогою звитої пари, коаксіального, оптоволоконного кабелю, або ж іншого типу кабелів які можуть використовуватися при будівництві LAN мережі. До основних пристроїв комп’ютерної мережі окрім магістралей зв’язку можна віднести: персональні комп’ютери, принтери, факси, IP-телефони [1].

Метою створення LAN мережі є можливість використовувати загальних даних які можуть бути розташовані на локальному сервері, або ж на виділеному комп'ютері, використання загальних ресурсів, периферійних пристроїв (які знаходяться в одній мережі) також сумісною роботою с базою даних [10].

Мета створення комп'ютерної мережі:

- зв'язок;
- сумісне використання файлів;
- сумісна обробка інформації;
- централізоване курування комп'ютерами;
- резервне копіювання даних;
- доступ до мережі Інтернет;
- обмін документами, файлами.

Використання програмного–апаратних засобів дозволяє забезпечити захист даних на достатньому рівні. На робочих станціях при цьому потрібно використовувати певні методи захисту, такі як:

- стійкі паролі;
- антивірусне ПЗ;
- контроль та розмежування мережевих ресурсів;
- міжмережеві екрани для фільтрації трафіку між частинами локальних мереж або ж при його отриманні з глобальної мережі Інтернет [3].

1.2 Захист інформації в глобальній мережі Інтернет та складності його захисту

За своєю природою поняття "Internet" та "Інформаційна безпека" не сумісні між собою. Адже сама мережа Internet з'явилася як корпоративна мережа побудована на стеці протоколів TCP/IP. Яка об'єдную між собою не тільки корпоративні мережі, але й мережі які мають навчальне, комерційне, державне та військове значення.

Інтернет має низьку собівартість, тому як до нього має доступ майже кожна людина, адже за допомогою нього є можливість отримувати доступ до конкретних даних, ресурсів та будь якої інформації яка цікавить конкретного користувача та є йому необхідною, в робочих або особистих цілях.

Зазвичай за використання інформації в Інтернеті інколи потрібно заплатити велику вартість – це на сам перед безпека та конфіденційність інформації. Існує багато прикладів при яких треті особи отримавши певну інформацію використовують її для конкретної вигоди. Зазвичай доступ до сайту з поганим захистом простіше отримати, але при цьому особа яка має більш високі знання в сфері інформаційних технологій може отримати дані з пристрою за допомогою котрого користувач здійснив вхід, або ж взагалі видалити або змінити дані користувача [4].

Інтернет загроза – це сама розповсюджена проблема яка пов'язана з Інтернетом. В таких випадках краще використовувати брандмауери або ж інші програмні продукти для фільтрації мережевого трафіку, тому як це найпростіший, але ефективний спосіб захисту. При цьому суттєвим мінусом є те, що кожного дня з'являються нові комп'ютерні віруси, нова кіберзагроз, не кожний антивірус або інша програма захисту ще не навчилася її розпізнавати. В подібних випадках потрібні програми, які будуть аналізувати інтернет-ресурс та при знаходженні вірусу оновлювати свої дані. В таких випадках краще використовувати актуальне на сьогоднішній день антивірусне та захисне програмне забезпечення, яке має офіційну підтримку безпосередньо від розробників, та постійно оновлюється для забезпечення максимального рівня захисту.

1.3 Основні види Інтернет-загроз та способи захисту від них

Інтернет – є безмежним простором інформації, який може надавати широкі можливості для навчання, спілкування, роботи та інших особистих потреб, та який кожної секунди постійно доповнюється все новою та новою інформацією. При цьому він також зберігає велику кількість інформації про

його користувачів, яка при потраплянні до третіх осіб може використовуватися проти його власника. Існує багато типів Інтернет-загроз, яким можуть підвергнутися користувачі, до основних можна віднести: соціальну інженерію та технічні методи отримання інформації (різні програмні та апаратні засоби).

1.3.1 Шкідливі програми

Шкідливі програми – це різні форми шкідливого коду в незалежності від способу його розповсюдження та поведення, а також викликаної їм шкоди. До них можна віднести: віруси, програми-шпигуни, небажане рекламне забезпечення, різноманітні форми програмних кодів. Звичайному користувачу складно розпізнати файли які можуть нести шкідливий характер. Для таких випадків існує рішення для виявлення подібних загроз за допомогою бази даних вже відомих загроз з використанням технології захисту від нових, а також для видалення ПЗ яке може нести потенційну загрозу.

Як працює шкідливе ПЗ:

Кіберзлочинці постійно шукають нові способи зараження. При цьому сучасні загрози розповсюджуються через вразливості систем, уникаючи засобів безпеки. Найчастіше всього зараження пристроїв відбувається через людську неуважність, при спробі завантажити файли з підозрілого сайту, форум, відвідування веб-ресурсів які мають контент сумнівного характеру.

Як залишатися захищеним:

Щоб забезпечити захист від шкідливого програмного забезпечення, перш за все необхідно регулярно проводити оновлення програмного забезпечення, включаючи операційну систему та програм які забезпечують захист. Це допомогає виправити помилки та вразливості які можуть використовуватися більш сучасними загрозами, та розширити функціонал ПЗ.

1.3.2 Фішинг

Фішинг – форма атаки з використання соціальної інженерії, в ході якої зловмисник маскуючись під надійний об’єкт, виманює конфіденційну інформацію жертви.

Основною метою фітингу – є отримання даних користувачів, які можуть бути продані або використані для зловмисних цілей, таких як крадіжка коштів, особистих даних, вимагання.

Для запобігання подібних атак, перш за все потрібно більше звертати увагу на основні признаки: електронні повідомлення можуть містити в собі офіційні логотипи або ж інші признаки достовірності підприємства, звертати увагу на наявність орфографічних помилок та некоректну граматику, посилання на сумнівні веб-ресурси [2].

1.3.3 Спам

Спам – небажані повідомлення в будь якій формі, які зазвичай відправляються в великій кількості. Найчастіше за все спам відправляється в формі комерційних електронних листів, які розсилаються на велику кількість адрес.

Для запобігання та захисту від спаму, перш за все не потрібно публікувати свою особисту або ж робочу електронну адресу на публічних сайтах, форумах та різноманітних сервісах.

1.3.4 Троян

Троян – шкідливе програмне забезпечення, яке приховується під виглядом легітимного програмного продукту. При цьому на відміну від вірусу, він має змогу самостійно копіювати та заражати файли. На сьогоднішній момент троянські програми найбільш розповсюджена категорія загроз, яка може ви користуватися для відкриття бекдорів, видалення користувацьких даних або передавання їх зловмисникам, завантаження, запуск та встановлення інших шкідливих програм.

Захистити пристрої від подібного типу загроз є можливість завдяки дотриманню правил безпеки при роботі в мережі Інтернет, та використання надійних засобів захисту на робочій станції (брандмауер, антивірусні програмні продукти). Адже щоб проникнути за робочу станцію, трояни використовують вразливості в системах користувачів. Для запобігання подібних ситуації рекомендовано регулярно слідити за актуальністю версій ОС, та програмних продуктів, постійно їх оновлювати.

1.3.5 Крадіжка даних

Крадіжка даних – злочин при якому зловмисник використовує шахрайство або обман для отримання конфіденційної інформації жертви, з метою використати її в подальшому від імені жертви. Зловмисників зазвичай цікавить особиста інформація жертви: паролі, банківські дані, данні кредитних карт. В подальшому отримана інформація можу використовуватися для різних незаконних цілей.

Способи захисту від подібного шахрайства:

- Здійснювати підключення лише переконавшись, що воно є безпечним. При цьому бажано використовувати домашню, корпоративну мережу, або ж мобільний зв'язок. Дуже важливо уникати публічних точок доступу Wi-Fi з незахищеним паролем. Якщо інколи є необхідність підключитися з публічного Wi-Fi, в цьому випадку краще при підключенні використати VPN, щоб запобігти крадіжки особистих даних.
- Встановлювати лише надійні та складні паролі, які не повинні містити в собі дати народження, номерів телефону, по можливості чередувати великі на мала літери, спец-символи, ніколи не використовувати аналогічні паролі на декілька ресурсів. Якщо сервіс підтримує двухетапну аутентифікацію, краще використовувати її.
- Не відкривати підозрілі сайти та повідомлення.
- Не публікувати особисту інформацію в соціальних мережах.

1.3.6 Бекдор

Бекдор – програма або комплекс шкідливих програм для отримання доступу до робочої станції, серверу, іншого пристрою, або мережі шляхом обходу аутентифікації, а також інших методів та технологій безпеки. Частіше за все, це шкідливе програне забезпечення може проникати на пристрої жертви під час завантаження користувацьких файлів. Крім цього, під час здійснення атаки зловмисники часто використовують різні види атак та їх способів, тому бекдор може стати частиною троянської програми, програми-шпигуна.

Одним із відомих прикладів так званої бекдор атаки здійснила група кіберзлочинців TeleBots. Win32/Industroyer – одна із відомих загроз яку створила група. Основним компонентом цього програмного забезпечення був бекдор. Він використовувався кіберзлочинцями для керування атакою та міг встановлювати та контролювати інші компоненти. Також мав змогу підключатися до віддаленого серверу для отримання команд та надання інформації зловмисникам.

Для захисту рекомендовано, постійно оновлювати своє ПЗ, та програмні продукти на робочій станції які відповідають за її безпеку, крім цього рекомендовано завантажувати додатки, програмні продукти лише з офіційних магазинів та звертати увагу на відгуки, щодо ПЗ його рейтинг в порівнянні з іншими конкурентами.

1.3.7 Комп’ютерний вірус

Комп’ютерний вірус – шкідливий код який може нанести шкоди файлам, зміни, пошкодити або ж видалити їх. Це один із видів шкідливого програмного забезпечення, яке маж змогу розповсюджувати свої копії з метою зараження та пошкодження даних на пристрої жертви. Віруси на робочу станцію можуть попасти будь яким шляхом, через пристрої передавання інформації (CD, DVD диски, флеш-карти, різного виду накопичувачі), в тому числі через мережу Інтернет.

Основні види вірусних програм:

- Файлові – заражають файли з розширенням «.exe».
- Скриптові – набір файлових вірусів написаних на різних мовах скриптів (JavaScript, PHP і т.п.). Подібний спосіб здатний заражати файли з розширенням .html та інші подібні формати файлів.
- Завантажувальні – атакують завантажувальні сектори змінних носіїв (диски, флеш-накопичувачі), встановлюються при запуску пристрою.
- Мікровіруси – зазвичай влаштовані і програми для обробки текстової інформації або ж електронних таблиць. Прикладом можуть бути документи Microsoft Word (.doc), Excel (.xls), Блокнот (.txt), Portable Document Format (.pdf).

1.3.8 Експлойт

Експлойт – комп'ютерна програма, фрагмент комп'ютерного коду який використовує вразливості в системі безпеки програмного забезпечення для подальшого розповсюдження кіберзагроз.

В залежності від методу отримання доступу до вразливого програмного забезпечення експлойт можна розділити на два види:

- Віддалений експлойт – працює через мережу та використовує вразливості в захисті без якого-небудь доступу до вразливої системи.
- Локальний експлойт – запускається безпосередньо на вразливій системі, при цьому потребує постійного доступу до неї.

Атака експойта може бути пов'язана з різними компонентами обчислювальної системи - серверні додатки, клієнтські програми або модулі операційної системи. Для використання серверної уразливості потрібно сформувати і послати серверу запит, що містить шкідливий код. Уразливість клієнта трохи складніше - потрібно переконати користувача в необхідності підключення до підробленим сервера (перехід по посиланню в разі, якщо вразливий клієнт є браузером).

Останнім часом експлойт використовуються в багатьох кібератаках. Як приклад атака вірусу WannaCryptor, яка стала найбільшою цифровою загрозою в світі за останні декілька років.

1.3.9 Мережевий черв

Мережевий черв – вид шкідливого програмного забезпечення, яке здатне самостійно розповсюджуватися в локальній або Інтернет-мережі шляхом створення власник копій. Він являє собою програмну з шкідливим кодом, яка атакує комп'ютери в мережі та розповсюджується через них. Активний мережевий черв може знижувати продуктивність деяких програмних додатків, навіть самої операційної системи, видаляти та пошкоджувати деякі програми.

Основною різницею між вірусом та черв'яком є в тому, що черві здатні самостійно розповсюджуватися та копіювати самого себе. Вони не залежать від файлів на робочій станції [5].

1.4 Постановка задачі

Проведений літературний огляд показав, що для вирішення задачі по створенню прототипу локальної захищеної мережі з використанням безпечних протоколів передачі інформації, створення безпечного каналу зв'язку для передачі інформації між декількома локальними мережами. Необхідно вирішити такі задачі:

1. Вибрати необхідні засоби для створення захищеної мережі.
2. Побудувати захищену корпоративну мережу на основі технологій VPN.
3. Організувати захищену частину мережі за допомогою DMZ.
4. Протестувати розроблену мережу на ступінь захищеності.

2 ВИБІР ІНСТРУМЕНТІВ

2.1 Технологія VPN як спосіб організації зв'язку між локальними мережами

Будь яка організація, нехай це торгова, фінансова компанія або ж державна установа обов'язково стикаються з питанням передачі інформації між своїми філіалами, при цьому щоб дані які будуть передаватися не мали змоги отримати сторонні особи, окрім кінцевого отримувача. Не кожна фірма має можливість собі дозволити мати особистий виділений фізичний канал зв'язку, при цьому навіть якщо філіали знаходяться за сотні тисяч кілометрів один від одного.

В цьому випадку найдоречнішим варіантом буде використання віртуальних приватних мереж, або ж технології VPN, на основі якої можна з легкістю з'єднати декілька мереж в одну, навіть на різних точках земної кулі, при цьому забезпечити гнучкість та одночасно високу швидкість передачі даних, а головне безпеку при обміні інформацією [6].

Технологія VPN (Virtual Private Network) – загально прийнята назва технології яка дозволяє забезпечити одне або декілька мережевих з'єднань, поверх інших мереж. Існує багато тверджень стосовно технології VPN, при цьому однією з її головних рис є використання мережі Internet в якості магістралі для передавання IP-трафіку. Мережі VPN призначені для вирішення задачі підключення кінцевого користувача до виділеної мережі або до конкретного веб-ресурсу. Структура VPN мережі включає в себе канали глобальної мережі, захищені протоколи та маршрутизатори [11].

2.1.1 Принцип роботи VPN

Для об'єднання локальних мереж в одну віртуальну мережу використовуються спеціальні віртуальні виділені канали. Для створення подібних з'єднань використовується механізм тунелювання. Ініціатор тунелю інкапсулює пакети локальної мережі в нові IP-пакети, які містять в своєму заголовці адресу ініціатора тунелю та адресу термінатору тунелю. При

отриманні подібного пакету, кінцевий користувач (термінатор тунелювання) проводить зворотній процес розшифрування отриманого пакету.

При подібній передачі, перш за все потрібно враховувати питання конфіденційності та цілісності даних, які не моє можливості забезпечити шляхом тунелювання. Для того щоб досягти конфіденційності при передаванні інформації, потрібно використовувати певний алгоритм шифрування, при цьому він має буди аналогічний як для відправника, так і для отримувача, та лише вони повинні мати інформацію про те який саме використовуються алгоритм, також володіти ключем для шифрування та розшифрування трафіку. Протоколи шифрування можуть бути різними, все залежить від того який протокол тунелювання підтримується тим або ж іншим VPN-рішенням [12].

Однією з важливих характеристик VPN-рішень є: діапазон підтримуючих протоколів аутентифікації, саме більшість популярних продуктів працюють за стандартами з використанням відкритого ключа. Це означає, що є можливість підсилити захист віртуальної мережі відповідним протоколом аутентифікації, в такому випадку отримати доступ до захищених каналів можуть лише конкретні користувачі [7].

2.1.2 Класифікація VPN мереж

Класифікувати VPN-мережі можна по основним параметрам.

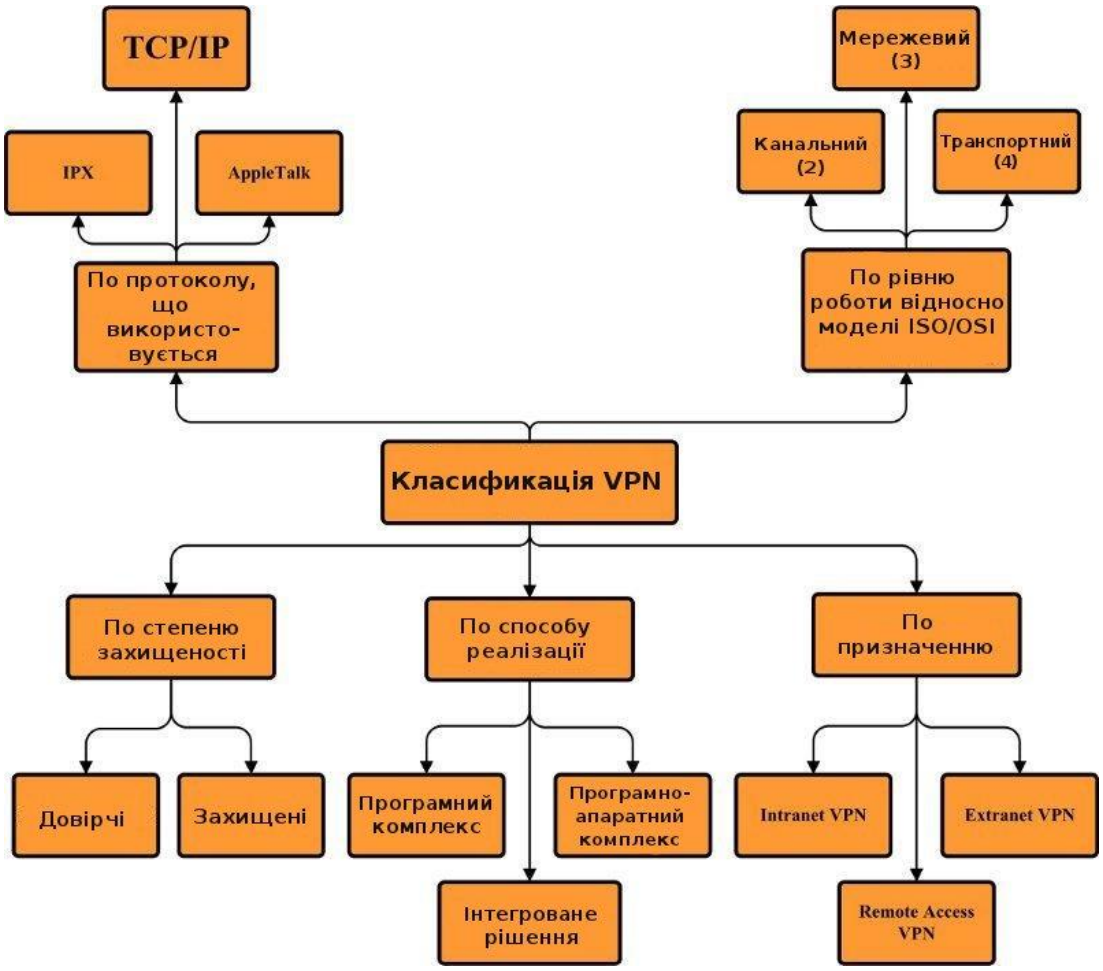

Рисунок 2.1 – Класифікація VPN-мереж

За типом середи використання:

- Захищені VPN-мережі, як найбільш розповсюджений тип мереж, за допомогою яких є можливість створювати захищені та одночасно надійні приватні мережі. Прикладом використання захищених мереж є: IPSec, SSL, PPTP.
- Довірчі VPN-мережі, використовуються у випадку, якщо середовище за допомогою котрого передають дані, можна вважати надійним та безпечним, та потрібно вирішити лише завдання створення віртуальної мережі, для подальшого об'єднання мереж іншого типу. Прикладом подібних VPN рішень можна вважати MPLS (Multi-protocol label switching) та L2TP (Layer 2 Tunnelling Protocol).

За способом реалізації:

- VPN-мережі в вигляді програмного рішення. Для реалізації потрібно мати персональний комп'ютер, та спеціальне налаштоване програмне забезпечення.
- VPN-мережі з комплексним рішенням. Основний критерій полягає в наявності спеціалізованого програмного забезпечення, яке має змогу не лише створювати захищені канали передачі даних, а також вирішувати задачі з фільтрації мережевого трафіку.

За призначенням:

- Intranet VPN – може використовуватися для об'єднання з захищену мережу декількох більш менших мереж для обміну та сумісного використання даних в середині організації.
- Remote Access VPN (шлюз захищеного віддаленого доступу) – являє собою програмно-апаратне рішення, яке забезпечує можливість створення та використання захищеного підключення користувачів до корпоративної мережі з використанням мережі Інтернет, або ж інших відкритих мереж. Використання подібного типу може бути доцільним в випадку коли є необхідність забезпечити конфіденційність та цілісність даних, які можуть передаватися по не захищеним каналам зв'язку.
- Extranet VPN – доцільне використання в мережах до котрих можуть підключатися сторонні користувачі (які можуть не бути співробітниками компанії, але їм необхідно мати доступ до конкретного переліку ресурсів, даних і т.п.). При подібному типі реалізації перш дуже важливі: аутентифікація користувача, перевірка наявності прав доступу і т.п.

2.2 Аналіз та порівняння протоколів реалізації VPN

Для того щоб була можливість створення VPN на обладнанні та програмному забезпеченні, необхідно використовувати певний стандартний механізм, так званий VPN-протокол.

Найбільш популярними протоколами для побудови VPN є: протоколи канального рівня PPTP та L2TP, протоколи мережевого рівня IPSec, а також OpenVPN, як комплексне рішення для побудови VPN-мережі.

Всі вище вказані протоколи достатньо широко використовуються, підтримуються та мають реалізацію в сучасних операційних системах: Microsoft Windows, Linux, Mac OS X, iOS та Android.

Кожний із протоколів має свої переваги та недоліки в порівнянні з іншими, та може використовуватися як для спеціалізованого направлення, так і для різних цілей.

Таблиця 2.1 Порівняльна характеристика проколів PPTP, L2TP/IPSec та OpenVPN

	PPTP	L2TP/IPSec	OpenVPN
Інформація	Тунельний протокол другого рівня типу з'єднання «точка-точка» (Point-to-Point Tunneling Protocol). Розроблений компанією Microsoft. Довгий час був стандартом для VPN-мереж. Володіє високою швидкістю та підтримується більшістю пристроїв які працюють з VPN.	Протокол тунелювання другого рівня (Layer 2 Tunneling Protocol) – VPN протокол який сам не забезпечує безпеку та цілісність даний, а лише дозволяє створювати тунель. Зазвичай використовується в сукупності з IPSec для забезпечення надійного шифрування трафіку. При налаштування L2TP/IPSec не виникає складності, також влаштований майже у всі ОС.	OpenVPN – рішення з відкритим кодом для побудови VPN мереж. Використовує бібліотеку OpenSSL. Гнучкий протокол, має можливість працювати на будь якому порту.

Алгоритм шифрування	MPPE-128.	AES-128 для даних, та SHA256 для повідомлень з контрольними сумами.	AES-256 для даних, SHA256 для повідомлень з контрольними сумами и 2048-бітне шифрування SSL/TLS.
Безпека	Має відомі проблеми з безпекою.	При правильну використанні не має значних вразливостей.	Надійний при використанні надійних ключів шифрування.
Переваги	- Просте налаштування - висока; швидкість роботи; - влаштований клієнт для більшості ОС.	- Просте налаштування та встановлення; - обходить мережеві заборони та блокування від провайдеру; - підтримується більшістю сучасних пристроїв та ОС.	- Гнучке налаштування; - швидкий та надійний; - обходить більшість мережевих екранів та блокувань від провайдерів.

Недоліки	- Низький рівень безпеки; - стабільність роботи залежить від якості з'єднання/зв'язку; - може бути заблокований.	- Повільніший в порівнянні з іншими протоколами; - може бути заблокований.	- Більш складне налаштування; - реалізований не для всіх мобільних пристроїв; - потребує встановлення додаткового програмного забезпечення.

Таким чином, із перерахованих VPN протоколів можна виділити PPTP як самий розповсюджений та легкий в налаштуванні, L2TP/IPSec протокол який забезпечує високу безпеку, OpenVPN як найбільш універсальне та гнучке рішення для побудови VPN-мереж.

2.2.1 Варіанти побудови VPN-мереж

Існують різні варіанти побудови VPN мереж, при виборі конкретного рішення, потрібно враховувати різні фактори. Перш за все фактори продуктивності при побудові з використанням конкретного типу мережі. Адже якщо маршрутизатор працює на межі своїх можливостей в звичайному режимі, то очевидно, що при додаткових функціях VPN-маршрутизування, відбудеться додаткове навантаження, це може вплинути на працездатність мережі, та вихід із строю проміжного обладнання, відповідно працездатність мережі також буде порушено. Зазвичай для побудови такого типу мереж використовують спеціалізоване обладнання, яке має змогу вирішити питання з продуктивністю, та мінімізувати шанс виходу із ладу. Використання подібного обладнання не аби як підіймає собівартість облаштування мережі, та тягне за собою певні фінансові затрати, але це ніщо в порівнянні з надійністю та продуктивністю.

Для побудови VPN-мереж, є можливість використовувати не лише апаратну частину (маршрутизатори, комутатори і т.п.), а також і програмну, до яких можна віднести: брандмауери, спеціалізоване програмне забезпечення та програмні реалізації VPN, та різних захищених середовищ для обміну інформацією.

2.2.2 VPN на базі маршрутизаторів

Більшість сучасних маршрутизаторів можуть брати участь у створенні захищеної VPN мережі. Так як вся інформація яка виходить з локальної мережі проходить через маршрутизатор, тому інколи є необхідність надати маршрутизатору задачу шифрування.

Рисунок 2.2 – Архітектура VPN на базі маршрутизаторів

Наглядним прикладом обладнання для побудови VPN на маршрутизаторі є обладнання компанії Cisco Systems. Маршрутизатори подібного типу підтримують протоколи L2TP та IPSec. Окрім просто шифрування інформації Cisco також підтримує інші функції VPN, такі як ідентифікація при встановленні тунельного з'єднання та обмін ключами.

Для побудови VPN, Cisco використовує тунелювання з шифруванням будь якого IP-потоку. Для підвищення продуктивності маршрутизатору можу ви користуватися додатковий модуль ESA (Encryption Service Adapter).

Переваги:

- Налаштування потрібно провести всього раз – в подальшому при підключенні клієнтів до маршрутизатору за замовчуванням вони зможуть використовувати налаштоване VPN-з'єднання.

- Захищеність від сторонніх осіб – якщо зловмисник збирає інформація про місцезнаходження, це дає можливість отримати доступ до реальної IP-адреси. Якщо на маршрутизаторі використувати VPN-з'єднання, це буде майже не можливим, так як реальна адреса буде змінена на іншу.

Недоліки:

- Зниження швидкості передачі даних – при використанні VPN на маршрутизаторі, значно знижається швидкість передачі даних, це відбувається майже з всіма повільними та слабкими CPU маршрутизатору. Одним із рішень – є придбання більш потужного маршрутизатору.
- Складності при доступі на конкретні ресурси – так як налаштування VPN на маршрутизаторі завжди будуть ввімкнені, IP-адреса буде належати країні, в якій розташований VPN-сервер, це робить недоступними конкретні ресурси.
- Налаштування VPN може бути складним – можуть виникнути складності в процесі налаштування, так як потрібно провести не мало маніпуляцій, для успішного налаштування. Отримати доступ до Default Gateway Address (шлюзу за замовчуванням), здійснити переналаштування мережевого з'єднання, завантажити та переналаштувати конфігураційні файли.
- Не всі маршрутизатори підтримують VPN-підключення – деякі роутери не підтримують технологію та функціонал VPN, як правило це пов'язано з прошивкою. Але навіть якщо маршрутизатор підтримує VPN, це не означає, що він буде підтримувати VPN-протоколи.
- VPN – шифрування на роутері не завжди ідеальне. Адже головною метою маршрутизатора є – маршрутизація та комутація трафіку, використання додаткового функціоналу на прикладі того ж самого VPN, є як додатковою функцією, яка може працювати, але не завжди як так як потрібно та коректно та якісно.

2.2.3 VPN на базі брандмауерів

Більшість брандмауерів підтримують тунелювання та шифрування даних. Зазвичай в програмне забезпечення брандмауера додається модуль шифрування. Якщо клієнти з'єднуються з VPN-сервером, вони поміщаються до так званого влаштованого мережевого об'єкту VPN Clients Network (мережа VPN-клієнтів).

Рисунок 2.3 - Архітектура VPN на базі брандмауерів

2.2.4 VPN на базі програмного забезпечення

До одного із методів реалізації VPN-мережі можна віднести лише самі програмні засоби які допомагають будувати мережу подібного типу. При реалізації цього підходу використовується спеціалізоване програмне забезпечення, яке працює на виділеному ПК (який може виступати в ролі серверу), або представляти собою роль proxy-серверу. При подібного роду реалізації сам сервер може знаходитися за мережевим екраном.

2.2.5 Переваги в використанні VPN

В порівнянні з звичайними локальними мережами, VPN-мережі мають ряд основних переваг, до яких можна віднести:

- Безпека – це один із головних факторів та аспектів роботи VPN-сервісів. Адже навіть якщо третя особа має змогу втрутитися в роботу VPN мережу та прослуховувати трафік, що передається по ній. Без змоги його розшифрувати вся отримана інформація буде набором незрозумілих даних. Без знання ключа, це зробити не має можливості, а на підбір ключа може піти не одна тисяча років, ці фактори можуть залежати від виду шифру, довжини ключа.

- Економність – при використанні VPN-мереж на підприємстві є можливість частково обмежити кількість проміжного обладнання (маршрутизаторів, свічів, серверів доступу, тощо), та розхідних матеріалів (кабелів, ліній зв'язку та інших технічних засобів), а головне суттєво зменшити витрати фізичне на обладнання та його обслуговування. Але при цьому не жертвуючи жодним із аспектів безпеки, навіть якщо користувач має змогу з'єднатися з мережею з будь якої точки земної кулі маючи лише дані для підключення та налаштований клієнт для встановлення зв'язку з мережею через приватний VPN-канал [8].

Компанія Forrester Research провела порівняльну характеристику в використанні VPN поверх Internet (з розрахунком 1000 користувачів), в порівнянні з центром видаленого доступу Remote Access Service.

Таблиця 2.2 – Порівняльна характеристика витрат на прикладі побудови мереж різного типу

Стаття витрат	Віддалений доступ (млн. дол.)	VPN (млн. дол.)
Оплата за послуги провайдеру зв'язку	1,08	0,54
Витрати на експлуатацію	0,3	0,3
Капіталовкладення	0,1	0,02
Інші витрати	0,02	0,09
Всього	1,5	0,89

Орієнтуючись на дані досліджень наглядно можна переконатися в порівняльній характеристиці собівартості, створення, реалізації, підтримці та обслуговування мережі.

Підхід використання саме VPN-мереж є доцільним в наш час, адже кожний вповноважений користувач моє змогу за допомогою мережі Інтернет отримати доступ до потрібних даних, мережевих ресурсів. Це робить

використання подібної технології конкурентно спроможним та актуальним в наш час. Тому як подібні властивості важко досягти при використанні звичайних, традиційних приватних мереж, тому як підприємства, які бажають та мають змогу використовувати мережеву ресурси, та мати до них доступ, інколи можуть мати не сумісні мережі, що суттєво ускладнює процес налаштування мережі такого типу. Особливо гостро це питання може виникати коли велика кількість організацій, бажають працювати разом через одну мережу.

3 СТВОРЕННЯ ТА НАЛАШТУВАННЯ ЗАХИЩЕНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

3.1 Побудова захищеної корпоративної мережі на основі технології VPN

Технологія VPN має багато переваг, однією з головних є – можливість побудови захищеної мережі використовуючи при цьому стандартні протоколи обміну інформації для побудови тунелю, обміну зашифрованою інформацією та забезпечення зв'язку для передавання зашифрованих даних.

В першу чергу для побудови мережі такого типу, потрібно визначити які її архітектуру, тобто кількість підмереж які будуть створені, кількість та тип проміжного обладнання (маршрутизатори, комутатори, тип транспортних магістралей і т.п.).

На практичному прикладі буде створена корпоративна мережі для підприємства ТОВ «Оберіг», підприємство є страховою компанією, головний офіс знаходиться в місті Харків, філіал в м. Суми.

Корпоративна мережа буде поділена на дві підмережі 192.168.1.0/24 та 192.168.2.0/24. Всі робочі пристрої кожної з мереж будуть з'єднані з проміжним маршрутизатором, тобто switch, який в свою чергу буде з'єднуватися з маршрутизатором котрий буде направляти або ж отримувати трафік з роутеру маршрутизатора провайдера для забезпечення функціонування мережі. В головному офісі в якості маршрутизатору буде Router1 який має дві ip-адреси на кожному інтерфейсі, перша належить до локальної мережі 192.168.1.1/24, інша адреса (180.180.1.2/30) відноситься до підмережі провайдера та була видана ним.

На маршрутизаторі Router2, який встановлений в мережі філіалу налаштування будуть аналогічні, але з урахуванням змін в ip-адресах. 192.168.2.1/24 – ip-адреса інтерфейсу зі сторони локальної мережі, 180.180.2.2 – ip-адреса інтерфейсу зі сторони провайдера зв'язку.

Головним пристроєм в створеній схемі виступає маршрутизатор провайдера, який виконує головну функцію – забезпечує зв'язок між під мережами. Він має назву Router0, має два інтерфейси в кожний з котрих направляється трафік FastEthernet 0/0 з адресою 180.180.1.1/30 та FastEthernet 0/1 з адресою 180.180.2.1/30 [13].

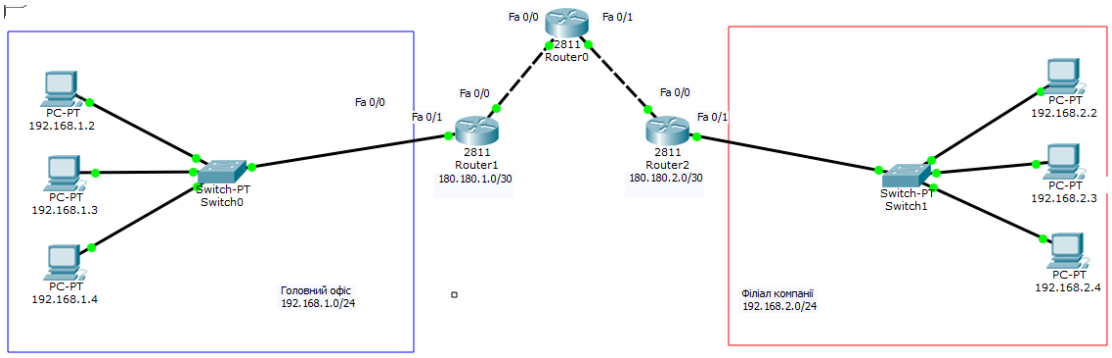

Рисунок 3.1 – Схема мережі компанії ТОВ «Оберіг»

3.1.1 Налаштування NAT

В першу чергу для забезпечення зв’язку між маршрутизаторами мережі та обладнанням провайдера слід налаштувати NAT, це потрібно зробити для того, щоб комп’ютери локальної мережі мали змогу відправляти запити до мережі Інтернет, так як локальні IP адреси в глобальній мережі з’являтися не можуть. Для цього потрібно відкрити налаштування одного з роутера який сполучає локальну мережу (Router1, Router2) та маршрутизатор провайдера (Router0), зайти в режим конфігурації, та в першу чергу налаштувати на кожний робочий інтерфейс тобто Ethernet на вхідний або ж вихідний трафік.

```
#conf t
#int fa0/0
#ip nat outside
#exit
#int fa0/1
#ip nat inside
#exit
```

Після визначення робочий інтерфейсів потрібно створити список доступу або ж access-list, та налаштувати його, для того щоб визначити який саме трафік потрібно відправляти в глобальну мережу.

```
#ip access-list standard THE-LOCAL-NAT
```

Наступний кроком потрібно вказати мережу (із зворотною маскою) з котрої буде надходити трафік, з локальної мережі на обладнання провайдера.

```
#permit 192.168.1.0 0.0.0.255
#exit
#ip nat inside source list THE-LOCAL-NAT interface fa0/0
overload
```

Після завершення налаштування потрібно вийти з режиму глобальної конфігурації використовуючи команду #end, та зберегти внесені зміни та налаштування до пам’яті роутеру за допомогою команди #wr mem.

Щоб переконатися, що налаштування пройшло успішно, потрібно виконати команду ping з будь якої робочої станції до маршрутизатору провайдера, вказавши його IP-адресу. При першій спробі виконання команди, перший ICMP пакет може не повернути жодного результату, при цьому видати повідомлення «request time out», в зв’язку з тим, що першочергово потрібно встановити зв'язок, та визначити маршрут. Наступні запити команди ping повинні повертати результат. Якщо все ж таки icmp пакети не будуть надходить, потрібно перевірити коректність налаштувань, та присвоєння пристроям мережі вірних ip-адрес з цієї ж мережі [14].

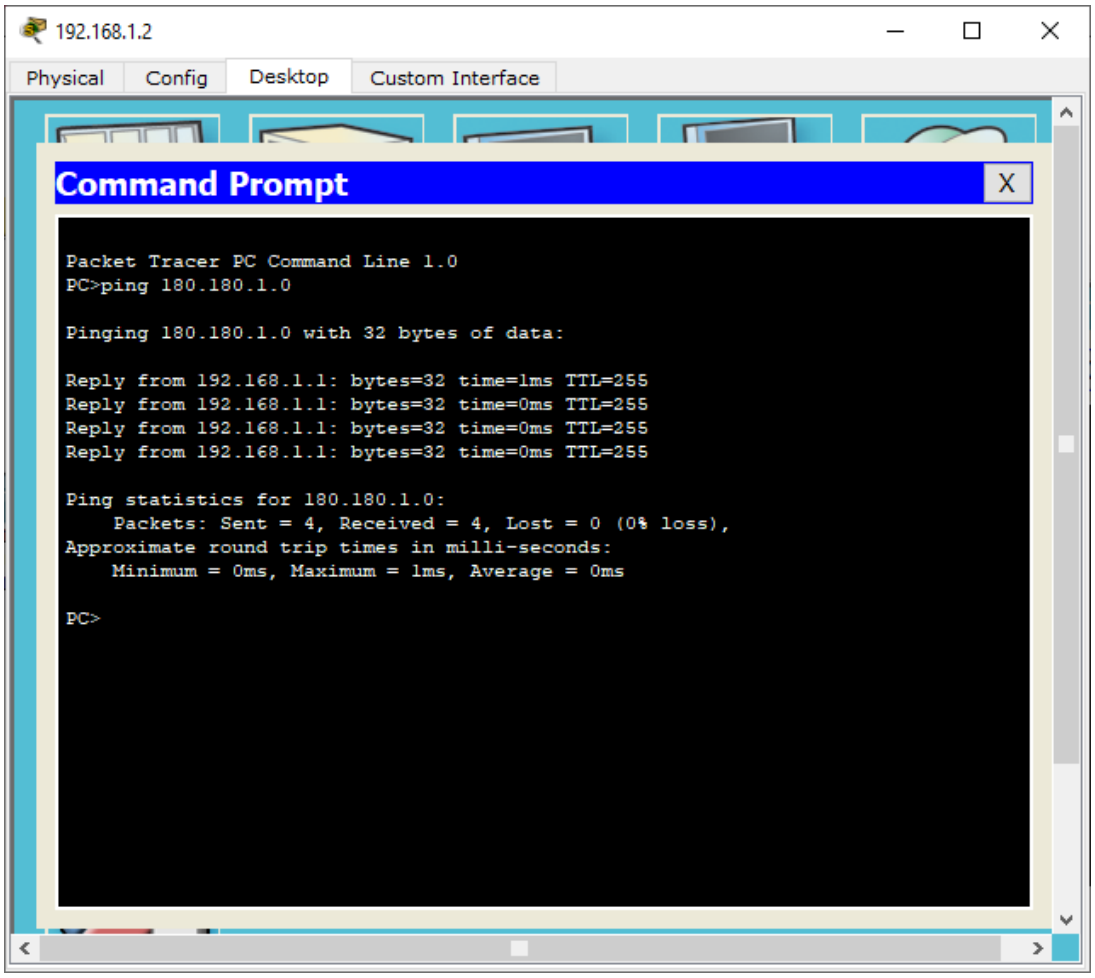

Рисунок 3.2 – Результат команди ping з Router1 до Router0

Після вдалого налаштування NAT на проміжному роутері який сполучає мережу 192.168.1.0/24 та маршрутизатор провайдера, потрібно провести аналогічні налаштування в філіалі з ip-адресою мережі 192.168.2.0/24. При налаштуванні потрібно використовувати аналогічні команди згідно першого випадку, але врахувавши зміни портів FastEthernet для вхідного та вихідного трафіку, та вказати ip-адресу поточної мережі.

```
#conf t
#int fa0/0
#ip nat outside
#exit
#int fa0/1
#ip nat inside
#exit
#ip access-list standard THE-LOCAL-NAT
#permit 192.168.2.0 0.0.0.255
#exit
```

```
#ip nat inside source list THE-LOCAL-NAT interface fa0/0 overload
```

Аналогічно першому випадку для збереження налаштувань потрібно завершити роботу за допомогою команди #end, та зберегти зміни з використанням команди #wr mem.

Для перевірки коректності встановлених налаштувань та працездатності мережі, потрібно виконати команду ping з локальної мережі до маршрутизатору провайдера.

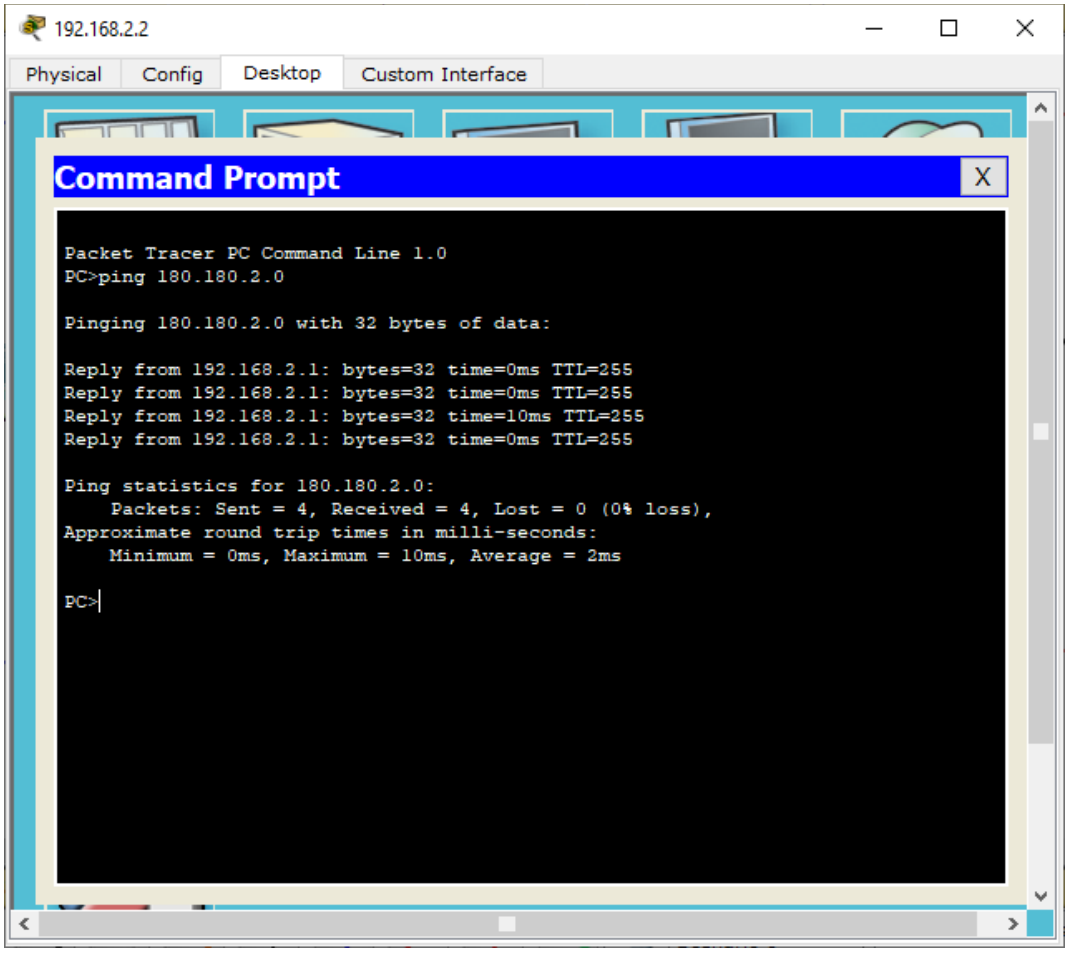

Рисунок 3.3 - Результат команди ping з Router2 до Router0

3.1.2 Налаштування VPN на маршрутизаторі

Налаштування VPN відбувається на маршрутизаторі який сполучає локальну та глобальну мережі. В першу чергу потрібно створити політику, тобто певні правила для налаштування VPN-з'єднань та побудови VPN-тунелю, в якій потрібно вказати алгоритми шифрування, хешування, тип аутентифікації, та відповідно обрати алгоритм Деффі-Хелмана, який слугує для обміну ключами шифрування.

```
#crypto isakmp policy 1
#encryption 3des
#hash md5
#authentication pre-share
#group 2
```

Наступним кроком потрібно налаштувати ключ аутентифікації та вказати IP адресу зовнішнього інтерфейсу маршрутизатору іншої локальної мережі до котрої в подальшому буде встановлений зв'язок для створення між ними VPN-каналу.

```
#crypto isakmp key ssu_soroka address 180.180.2.2
```

Основні параметри налаштовані, наступним етапом потрібно вказати параметри для побудови IPSec тунелю, з використанням команди transform-set, яка використовується для формування набору перетворень. Також потрібно вибрати тип перетворення, тобто алгоритм шифрування та хешування, для реалізації були взяті esp-3des – протокол ESP з 168-бітним алгоритмом 3DES, та esp-md5-hmac – протокол ESP з алгоритмом аутентифікації MD5.

```
#crypto ipsec transform-set TS esp-3des esp-md5-hmac
```

Наступним кроком потрібно створити список доступу, тобто access-list, для того щоб передавати трафік із мережі 192.168.1.0/24 в мережу 192.168.2.0/24. Необхідно створити розширений список доступу та присвоїти його унікальне ім'я, яке в подальшому буде використовуватися для VPN-тунелю. Відповідно в процесі створення та налаштування списку доступу потрібно вказати дії які необхідно проводити з трафіком (дозволи або ж

заборонити його), тобто в поточному випадку дозволити його проходження з використанням ключового слова permit, вказавши мережу відправника та отримувача з зворотною маскою.

```
#ip access-list extended THE-VPN-TEST
#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Далі потрібно створити криптографічну карту, вказати IPSec партнера для карти (зовнішній інтерфейс маршрутизатора який знаходиться в філіалі компаній), та прив'язати карту до щойно створеного access-list.

```
#crypto map CMAP 10 ipsec-isakmp
#set peer 180.180.2.2
#set transform-set TS
#match address THE-VPN-TEST
```

Одним із останніх параметрів налаштувань VPN-тунелю є – прив'язка криптокарти до зовнішнього інтерфейсу маршрутизатору, тобто Ethernet 0/0.

```
#interface FastEthernet 0/0
#crypto map CMAP
```

Відповідно після завершення налаштування, потрібно зберегти внесені зміни з використанням команди #wr mem, завчасно здійснивши вихід з режим глобальної конфігурації.

Подібним чином потрібно провести налаштування для маршрутизатора який знаходиться на межі глобальної та локальної мережі філіалу, при цьому з урахуванням змін в інтерфейсах пристроїв. На етапі налаштування ключа аутентифікації потрібно враховувати те, що ключ який був заданий першочергово ssu_soroka повинен співпадати на іншому маршрутизаторі.

```
#crypto isakmp policy 1
#encryption 3des
#hash md5
#authentication pre-share
#group 2
#exit
#crypto isakmp key ssu_soroka address 180.180.1.2
#crypto ipsec transform-set TS esp-3des esp-md5-hmac
#ip access-list extended THE-VPN-TEST
#permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
#exit
#crypto map CMAP 10 ipsec-isakmp
#set peer 180.180.1.2
```

```
#set transform-set TS
#match address THE-VPN-TEST
#exit
#interface FastEthernet 0/0
#crypto map CMAP
```

Більша частина налаштувань завершена, при цьому в поточному випадку при спробі відправити пакет з ПК однієї локальної мережі в іншу відбудеться помилка, з описом того що «Мережа не доступна».

Складність полягає в налаштованому NAT на роутері, тобто повністю весь трафік який проходить через роутера за налаштованим NAT, не направляється в створений VPN тунелю, та відповідно не находить кінцевому отримувачу. Для рішення подібної складності потрібно на маршрутизаторах Router1 та Router2 видалити створені access-list з поміткою standard, та створити розширені extended, явно вказавши при цьому який саме трафік потрібно ігнорувати для NAT, тобто направляти в VPN тунель, а який потрібно транслювати в NAT.

Для видалення access-list потрібно вказати параметри створено списку доступу, з ключовим словом no.

```
#no ip access-list standard THE-LOCAL-NAT
```

Наступною командою створити розширений список доступу з ключовим словом extended.

```
#ip access-list extended THE-LOCAL-NAT
```

З використанням ключового слова deny потрібно вказати трафік який не потрібно транслювати в NAT, тобто трафік який необхідно направляти лише в створений VPN-тунель, відповідно вказавши адреси мережі відправника та отримувача. Для того, щоб дозволити транслювати в NAT весь інший трафік, який не матиме відношення до іншої підмережі, а буде відправлятися лише на маршрутизатор Інтернет провайдера.

```
#deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
#permit ip 192.168.1.0 0.0.0.255 any
```

Після завершення налаштування одного з проміжних маршрутизаторів є можливість перевірити працездатність VPN-тунелю відправивши з однієї

мережі в іншу (використовуючи проміжний роутер на котрому був налаштований VPN на розширений список доступу) пакет ICMP при використанні команди ping.

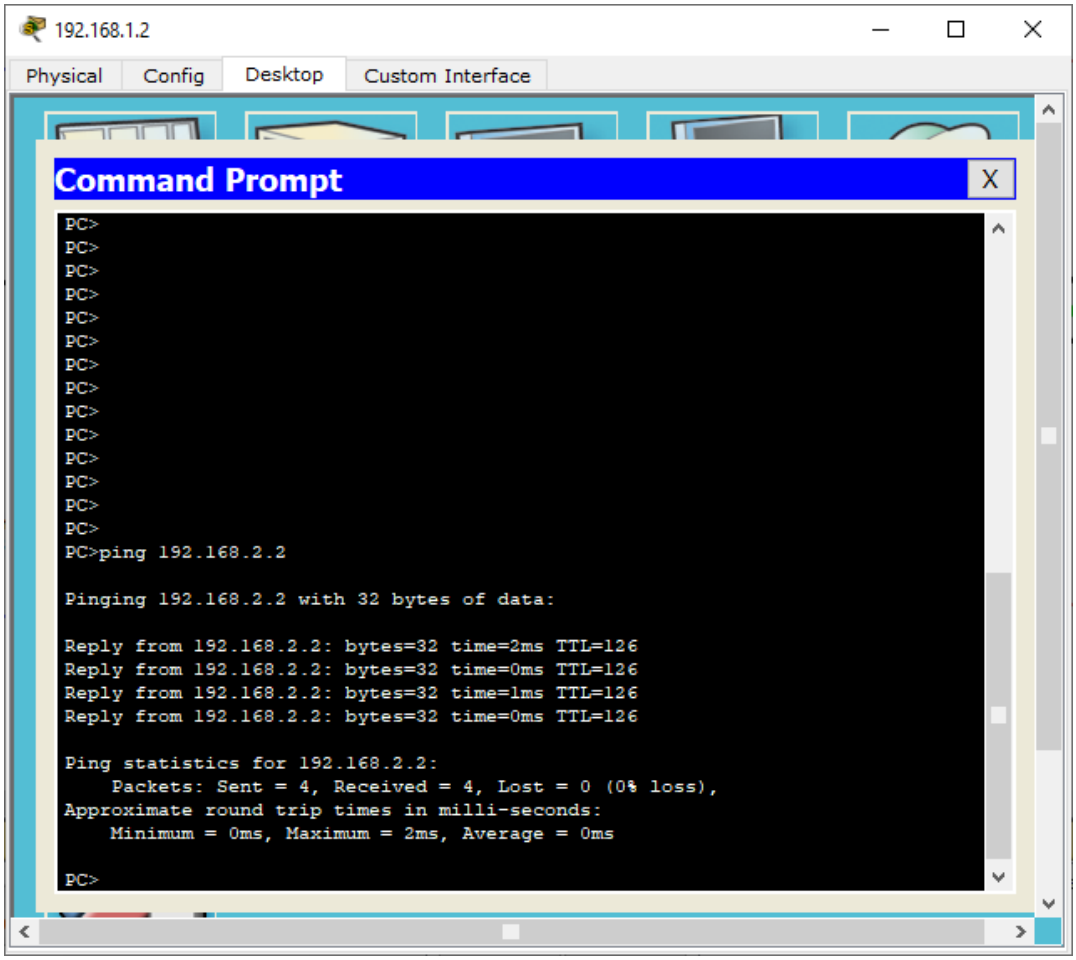

Рисунок 3.4 – Відправлення icmp-запиту з головного офісу в мережу філіалу

Аналогічним способом потрібно провести налаштування маршрутизатора в іншій мережі відповідно змінивши в процесі налаштування ip-адреси та інтерфейси.

```
#no ip access-list standard THE-LOCAL-NAT
#ip access-list extended THE-LOCAL-NAT
#deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
#permit ip 192.168.2.0 0.0.0.255 any
```

Для перевірки характеристики щодо створеного VPN-тунелю та вивести детальну інформацію про ISAKMP з’єднання, є можливість на

налаштованому маршрутизаторі набрати команду show crypto isakmp sa для перегляду детальної інформації.

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
180.180.2.2     180.180.1.2     QM_IDLE           1051    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

Рисунок 3.5 – Результат команди show crypto isakmp sa, перевірка характеристик VPN-тунелю

Також є можливість переглянути детальну інформації та характеристики IPSec тунелю з використанням команди show crypto ipsec sa.

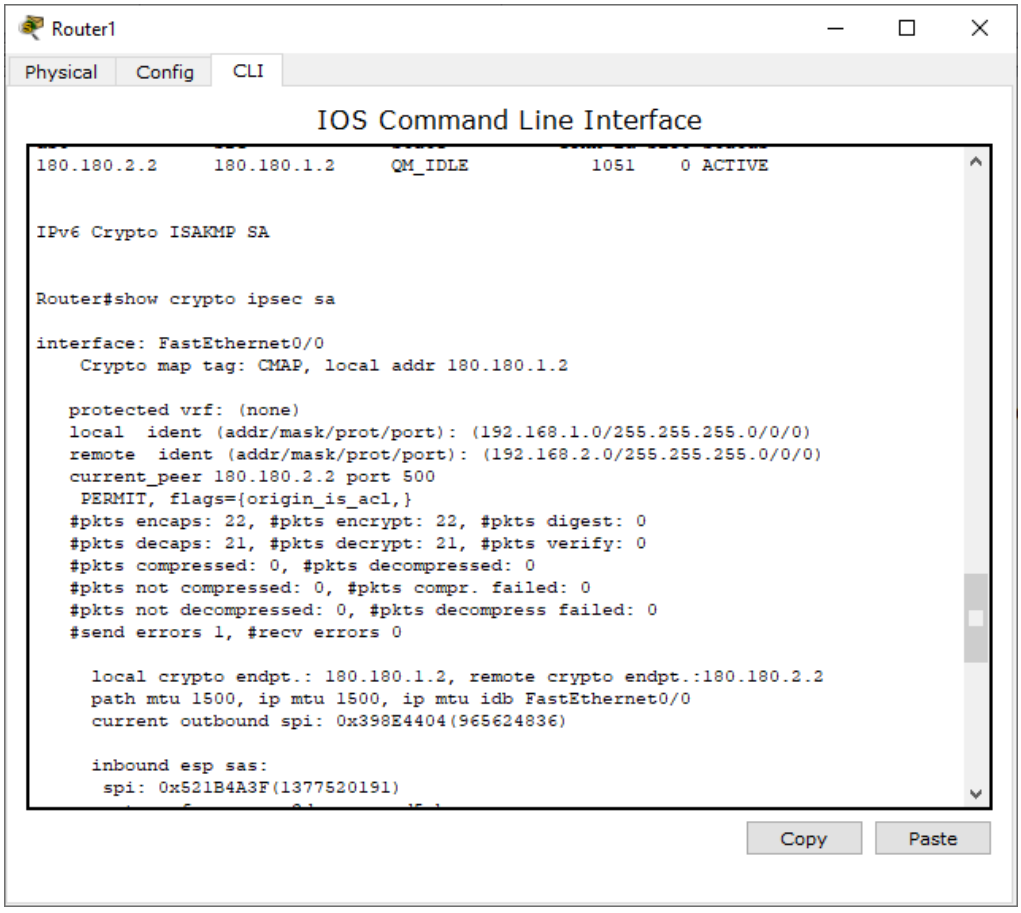

Рисунок 3.6 - Результат команди show crypto ipsec sa, детальна інформація про IPSec-тунель

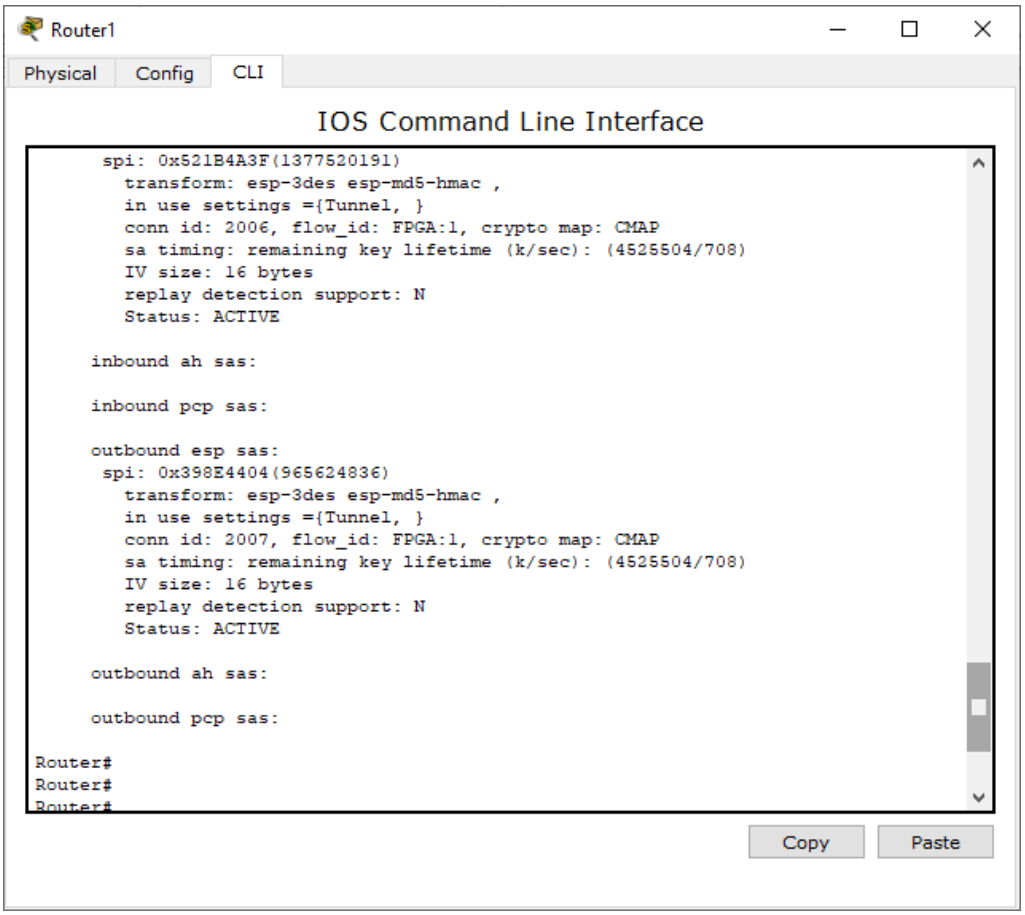

Рисунок 3.7 - Результат команди show crypto ipsec sa, детальна інформація про IPSec-тунель

3.2 DMZ – як спосіб організації захищеної частини мережі

DMZ (Demilitarized Zone) – частина корпоративної мережі яка містить загальнодоступні сервіси, такі як: web-сервер, email-сервер, ftp – сервер. При цьому отримати доступ до цих ресурсів є можливість як з корпоративної мережі, так із глобальної мережі Інтернет. Тому зазвичай подібні сервіси розміщують в окремому сегменті від корпоративних, так як вони є загальнодоступними, з можливістю отримати відкритий доступ з мережі Інтернет, тому суттєво зростає ризик злому, або несанкціонованого проникнення. При подібній структурі побудови (відокремлення DMZ в окрему частину мережі), навіть при проникненні зловмисника на подібний сервер, локальна мережа, котра з нею з'єднується, залишається захищеною. Таким чином мінімізуються збитки від можливого злому.

Для забезпечення повного захисту та підвищення рівня безпеки. Потрібно слідувати певним правилам та вимогам:

- Сервіси які знаходяться за межами DMZ повинні встановлювати з'єднання тільки до самої DMZ зони.
- Сервіси які розташовані всередині DMZ, повинні підключатися до глобальної мережі Інтернет лише з використанням проксі-сервера.
- Сервіси які є краще захищеними повинні взяти на себе роль бути клієнтами при здійсненні запиту із зон які є менш захищеними.
- За допомогою інспектування трафіку потрібно обмежити серверам DMZ ініціювати з'єднання з локальними мережами, які поключені до сервера, лише в зворотному порядку.

При побудові та налаштуванні дуже важливим аспектом є – використання міжмережевого екрану, тобто фаєрволу, зазвичай їх використовують два, для забезпечення більш надійного захисту від несанкціонованого доступу. Перший використовується на зовнішньому периметрі, та фільтрує трафік який надходить виключно на DMZ. Другий – є внутрішнім, який фільтрує трафік із DMZ до внутрішньої мережі [9].

3.2.1 Побудова мережі DMZ

На практичному прикладі буде створено та налаштовано частину корпоративної мережі для компанії ТОВ «Оберіг», підприємство є страховою компанією, головний офіс знаходиться в місті Харків, філіал в м. Суми. У компанії є необхідність використовувати зовнішній сервер з загальним доступом DMZ, при цьому, щоб доступ до нього мали як співробітники компанії з своїх робочих станції, які знаходяться в локальній мережі, так і клієнти компанії, отримуючи доступ до цифрових даних. При цьому забезпечивши безпеку від несанкціонованого проникнення в локальну мережу компанії.

За основу локальної мережі взято 3 робочі станції які сполучаються міжмережевим екраном, локальна мережа має адресу 192.168.1.0 за маскою 24. Наступним з'єднувальним елементом виступає маршрутизатор який з'єднує локальну мережу (через міжмережевий екран), та зовнішній сервер. За основу фаєрволу взято Cisco ASA 5505.

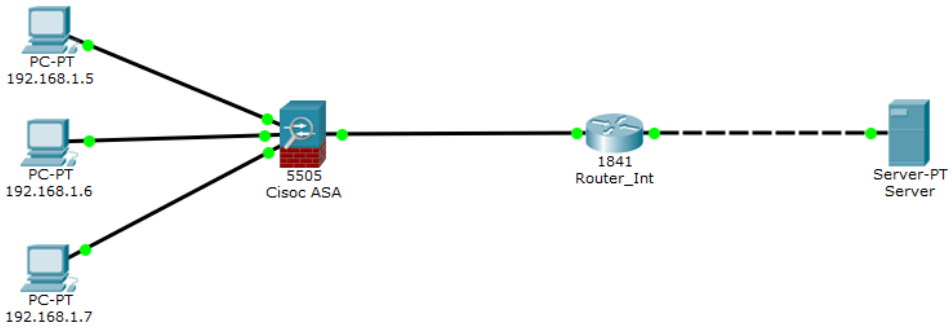

Рисунок 3.8 – Схема мережі для компанії ТОВ «Оберіг»

За умовчуванням Cisco ASA має влаштований DHCP сервер, тому для автоматичного отримання налаштувань для роботи мережі, на кожній із робочих станцій потрібно заздалегідь ввімкнути функцію DHCP.

В зв'язку з тим, що адміністратор не завжди є можливість фізично підключатися до Cisco ASA, для налаштувань, зміни параметрів і т.п. В

такому випадку є необхідність заздалегідь забезпечити можливість здійснювати віддалене підключення до Cisco ASA.

При подібних діях, в першу чергу потрібно встановити пароль, використовуючи наступну команду.

```
#enable password ssu_diplom_soroka
```

Далі потрібно створити користувача.

```
#username admin password ssu_diplom_soroka
```

Наступним кроком потрібно обрати протокол, по якому буде відбуватися підключення пристроїв локальної мережі до брандмауера, був обраний протокол SSH (Secure Shell) – який слугує для безпечного віддаленого підключення, після його вибору потрібно вказати інтерфейс через який буде здійснюватися доступ, тобто внутрішній інтерфейс inside.

```
#ssh 192.168.1.0 255.255.255.0 inside
```

Далі потрібно вказати параметри аутентифікації користувачів, з використанням локальної бази користувачів LOCAL.

```
#aaa authentication ssh console LOCAL
```

Для перевірки налаштувань достатньо з робочої станції виконати команду ssh, потім вказати параметри для підключення з ім’ям користувача та ip-адресою Cisco ASA.

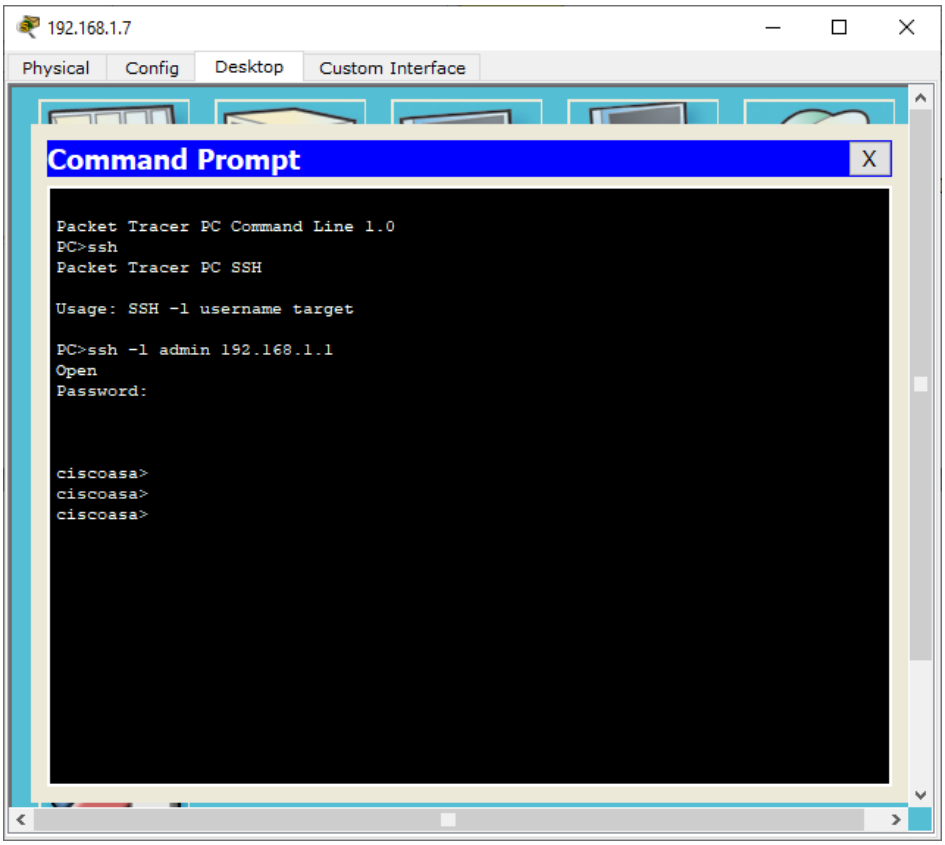

Рисунок 3.9 – Перевірка налаштувань віддаленого підключення з використанням SSH

Маршрутизатор Router_Int має на інтерфейсі Fa0/0 ip-адресу 180.180.1.0, при спробі виконати команду ping з робочої станції до маршрутизатору, спроба буде невдалою, в зв'язку з тим, що подібний трафік, тобто його передача можлива лише при використанні механізму Stateful Packet Inspection – інспектування трафіку з зберіганням стану. Подібний механізм дозволяє захиститися від атак, виконуючи перевірку вхідного трафіку на коректність. Міжмережевий екран перевіряє та запам'ятовує сесію та заносить її в свою динамічну пам'ять (в тому лише випадку, якщо відправка відбувається з інтерфейсу з більшим security level на менший). При зворотньому направленні пакету, бендмауер перевіряє його на відповідність з даними які занесені до його динамічної п'амяті, якщо відповідність була знайдена, тобто відправник, отримувач, порти відправника та отримувача, номер пакету, лише в цьому випадку пакет буде направлений отримувачу, в

іншому випадку пакет буде відкинуто. Подібний спосіб не аби як підвищує рівень захисту від стороннього втручання.

Тому для того, щоб була можливість відправити дані через Cisco ASA з локальної мережі на зовнішній роутер, в першу чергу потрібно налаштувати інспектування трафіку, потрібно визначити тип трафіку який потрібно пропускати, потім створити політику (дію яку потрібно виконувати над трафіком) в даному випадку інспектування, та визначити направлення в якому будуть діяти налаштовані правили (вхідний, вихідний трафік або ж в усіх направленнях).

```
#class-map inspection_default
#match default-inspection-traffic
#policy-map global-policy
#class inspection_default
#inspect icmp
#service-policy global-policy global
```

Після завершення налаштувань міжмережевого екрана, потрібно перевірити роботу використанням команди ping з комп’ютера локальної мережі до маршрутизатора та web-сервера через Cisco ASA.

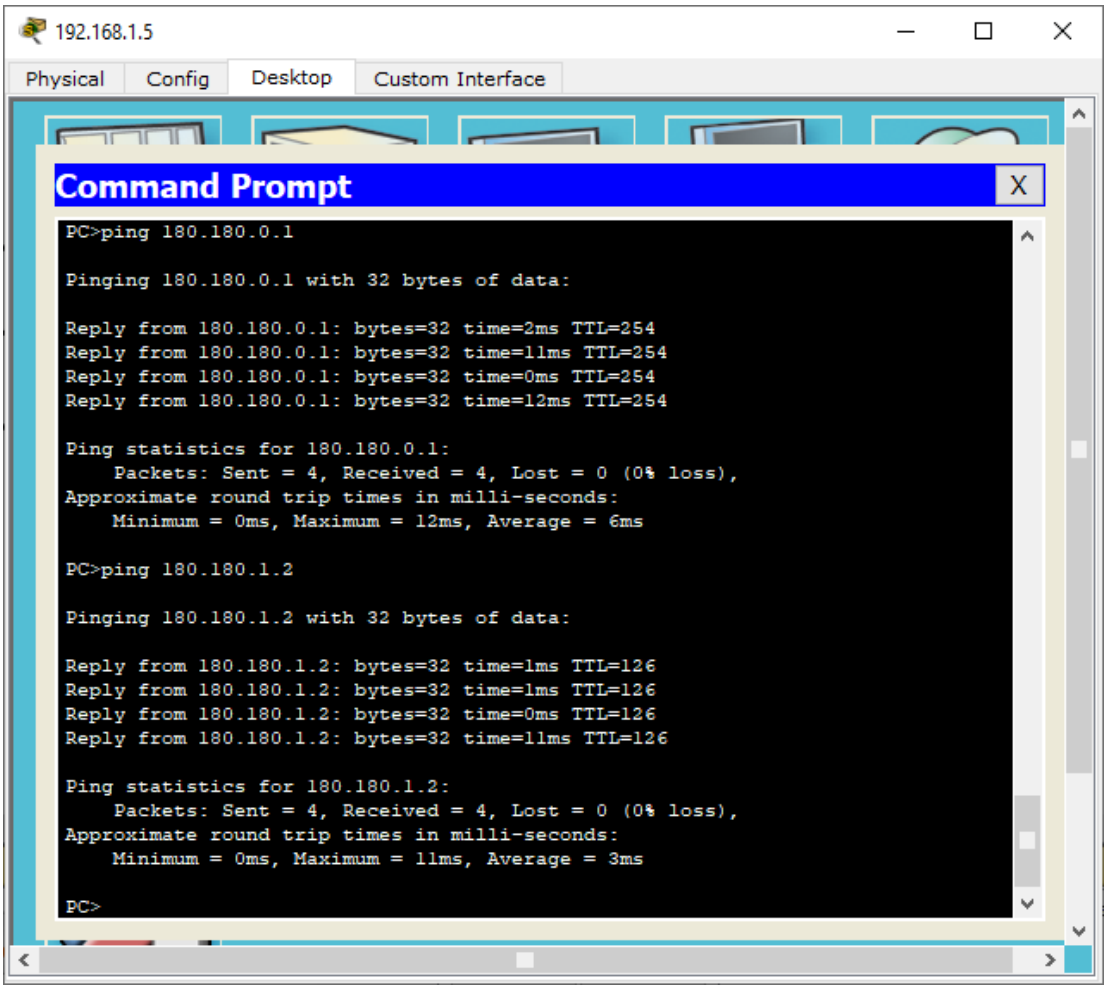

Рисунок 3.10 – Перевірка зв’язку з робочої станції до маршрутизатора провайдера на web-сервера

По результату виконання команди зв'язок встановлений успішно, але потрібно враховувати одну важливу деталь, що інспектування трафіку налаштоване лише для icmp пакетів, за допомогою команди inspect icmp, при відправленні трафіку іншого типу, спроба буде не успішною. Для того щоб дозволити пропускати трафік іншого типу на між мережевому екрані потрібно використати декілька команд, та вказати тип трафіку.

```
#policy-map global-inspect
#class inspection_default
#inspect http
```

Потрібно налаштувати NAT на маршрутизаторі.

```
#object network THE_NAT
#subnet 192.168.1.0 255.255.255.0
#nat (inside,outside) dynamic interface
```

До створеної схеми мережі потрібно додати окремий DMZ сервер, доступ до якого буде здійснюватися через Cisco ASA. Потрібно також дозволи трафік з локальної мережі до DMZ сервера, та з використанням списків доступу дозволити трафік з глобальної мережі до DMZ.

При додаванні нового сервера його потрібно з'єднати з Cisco ASA, при цьому дуже важливо щоб створений сервер мав статичну ip-адресу.

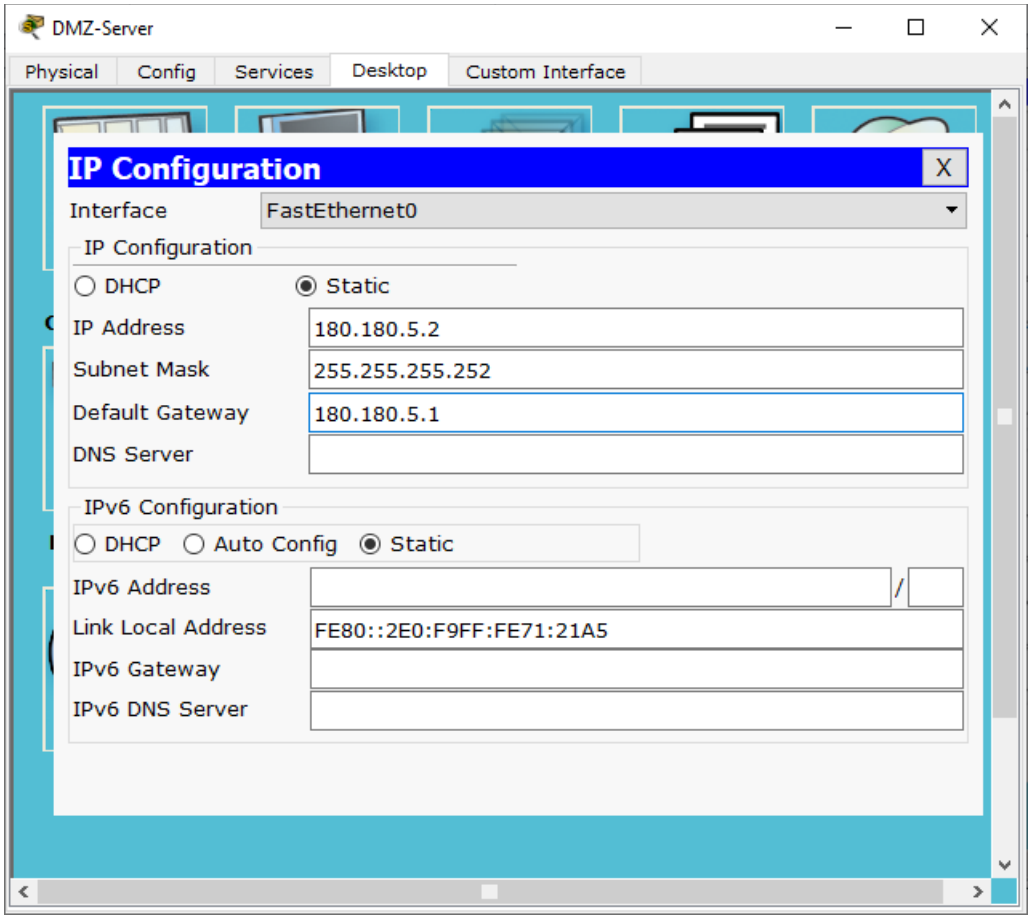

Рисунок 3.11 – Налаштування ip-адреси для DMZ сервера

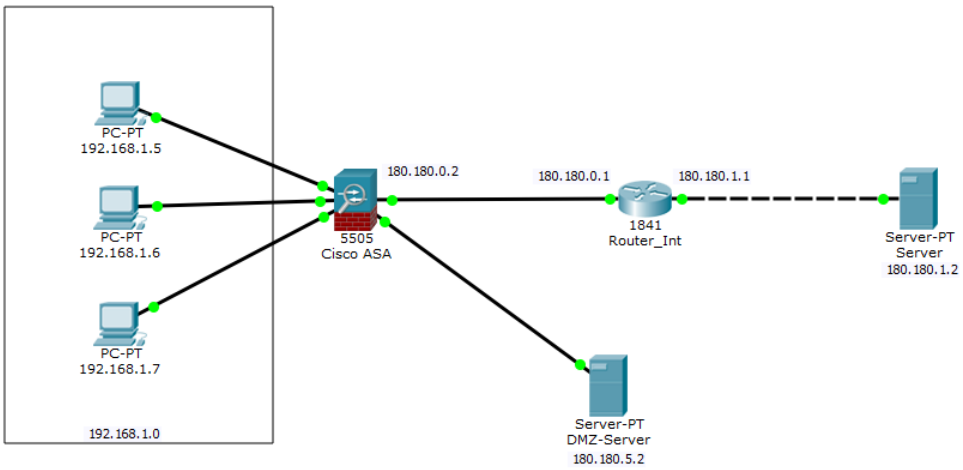

Рисунок 3.12 – Схема мережі з DMZ сервером

Для можливості підключення з зовнішньої мережі до DMZ, необхідно на роутері прописати маршрут з використанням зовнішнього інтерфейсу ASA.

```
#conf t
#ip route 180.180.5.0 255.255.255.252 180.180.0.0
```

З використанням вище вказаних команд маршрут прописаний, наступним кроком потрібно провести налаштування брандмауера.

```
#int vlan 3
#no forward interface vlan 1
#nameif dmz-server
INFO: Security level for "dmz-server" set to 0 by default.
#security-level 50
#ip address 180.180.5.2 255.255.255.252
#exit
#ping 180.180.5.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 180.180.5.2, timeout is 2
seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/6/9 ms
```

Наступним етапом необхідно провести налаштування доступу з публічного сервера до сервера DMZ з використанням списків доступу.

```
#access-list
#access-list THE-OUTSIDE-LIST extended permit icmp any host
180.180.5.2
#access-group THE-OUTSIDE-LIST in interface outside
```

Після виконання набору команд, зв'язок від публічного сервера до сервера DMZ дозволено, також дозволено доступ з локальної мережі до цього сервера, з урахуванням правил безпеки та запобігання несанкціонованого доступу з використанням таких механізмів як: брандмауер (на прикладі Cisco ASA 5505) та security-level.

При спробі відправити будь який запит з поза мережі через брандмауер, такий запит буде відхилено, так як першочергово від не був відправлений в цьому напрямку, та ASA не має про його жодного запису в своїй динамічній п'амяті.

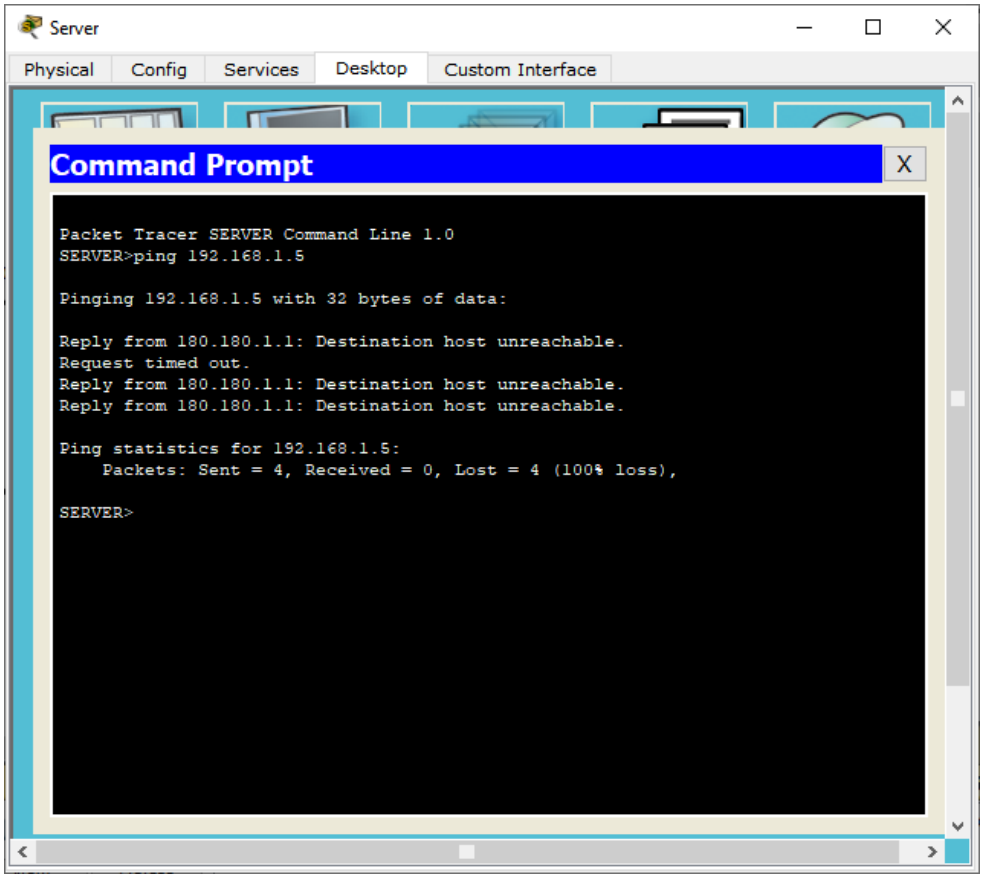

Рисунок 3.13 – Результат відправки запиту із зовнішньої мережі в локальну через брандмауер

Таким чином по результату тестування можна зробити висновок, що створений канал є захищеним.

ВИСНОВКИ

В ході виконання випускної роботи було:

Проведено огляд та аналіз існуючих засобів для забезпечення інформаційної безпеки локальних мереж.

Проаналізовано порівняльні характеристики протоколів передачі даних та організації зв’язку між віддаленими частинами мереж з використанням технології VPN. Описано основні ризики та загрози з якими можуть стикатися користувачі в мережі Інтернет, запобігання цьому за для забезпечення інформаційної безпеки. Розглянуто сучасні проблеми сьогодення в сфері інформаційної безпеки. Обрано актуальні засоби та способи захисту інформації для забезпечення цілісності та конфіденційності даних при обміні.

На практичному прикладі з використанням програмного продукту Cisco Packet Tracer 6.2 створено два прототипи локальних мереж з використанням VPN-з’єднання та налаштування віртуально каналу між ними, створення окремої мережі з застосуванням DMZ-сервера, як файлового сховища для даних до якого мають змогу отримати доступ як члени локальної мережі, так і інші користувачі сторонніх мереж в залежності від налаштованих рівнів доступу, з розмежуванням прав доступу та налаштування його як окремої виділеної частини мережі.

Тестування створеного продукту показало, що створений канал передачі даних є надійним і високозахищеним, відповідає критеріям інформаційної безпеки, представляє налаштовану структуру мережу з розмежуванням прав доступу, обмежує несанкціонований доступу сторонніх осіб в ієрархію комп’ютерної мережі.

СПИСОК ЛЕТЕРАТУРИ

1. В. Олифер, Н. Олифер «Компьютерные сети. Принципы, технологии, протоколы» (5-е издание) / В. Олифер, Н. Олифер, СПб.: “Питер”, 2016. – 992 с.

2. Що таке кібербезпека - https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html#~types-of-threats

3. Э. Таненбаум, Д. Уэзеролл "Компьютерные сети" 5-е изд. — СПб.: “Питер”, 2012. — 960 с.

4. Захист інформації в глобальній мережі -https://mirznanii.com/a/122769/zashchita-informatsii-v-globalnoy-seti/

5. Загрози в мережі Інтернет - https://safe-surf.ru/users-of/article/212/

6. Андрончик А. Н. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс : учеб. пособие / А. Н. Андрончик, А. С. Коллеров, Н. И. Синадский, М. Ю. Щербаков ; под общ. ред. Н. И. Синадского. – Екатеринбург: Изд-во Урал. ун-та, 2014.

7. Віртуальні приватні мережі VPN -https://www.ibm.com/support/knowledgecenter/ru/ssw_ibm_i_73/rzaja/rzajagetstart.htm

8. Переваги і недоліки використання VPN -https://uk.wizcase.com/blog/переваги-і-недоліки-використання-vpnзро/

9. Обзор вариантов организации доступа к сервисам корпоративной сети из Интернет - https://habr.com/ru/post/302068/

10. Поняття про комп’ютерні мережі, їх призначення. Типи комп’ютерних мереж і мережної взаємодії -https://edufuture.biz/index.php?title=Поняття_про_комп’ютерні_мережі,_їх_призначення._Типи_комп’ютерних_мереж_і_мережної_взаємодії.

11. Росляков, А.В. Виртуальные частные сети. Основы построения и применения / А.В. Росляков. - М.: Эко-Трендз, 2015. - 626 с.

12. Катаев, А. В. Информационные системы и модели оптимизации распределения заказов в партнерской сети виртуального предприятия: моногр. / А.В. Катаев. - М.: Синергия, 2019. - 599 с.

13. Gerardus Blokdyk, IPsec VPN A Complete Guide - 2019 Edition, 126 page.

14. Andrew S. Tanenbaum, David J. Wetherall Computer Networks (5th Edition)» / Prentice Hall, 2010. 960 page.