МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ВИПУСКНА РОБОТА

на тему:

«Графічний інтерфейс налаштування розподіленої обчислювальної мережі компанії з використанням IPSec VPN»

Завідувач
випускаючої кафедри **Довбиш А.С.**

Керівник роботи **Великодний Д.В.**

Студент гр. ІН-61 **Білоцерковець С.А.**

СУМИ 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК
СЕКЦІЯ ІКТ

Затверджую_____

Зав. кафедрою Довбиш А.С.

“_____” _____2020 р.

ЗАВДАННЯ

до випускної роботи

Студента четвертого курсу, групи ІН-61 спеціальності “Інформатика” денної форми навчання Білоцерковця Сергія Андрійовича.

Тема: “**Графічний інтерфейс налаштування розподіленої обчислювальної мережі компанії з використанням IPSec VPN**”

Затверджена наказом по СумДУ

№_____ від _____2020 р.

Зміст пояснювальної записки:1)огляд існуючих рішень; 2)постановка завдання й формування завдань дослідження; 3)Налаштування технології IPSec VPN; 4) програмна реалізація та її опис; 5)висновки.

Дата видачі завдання “_____”_____2020 р.

Керівник випускної роботи_____ Великодний Д.В.

Завдання прийняв до виконання _____ Білоцерковець С.А.

РЕФЕРАТ

Записка: 51 стор., 18 рис., 4 додатки, 10 джерел

Об’єкт дослідження — Технологія IPSec VPN

Мета роботи — Розроблення графічного інтерфейсу налаштування мережі

Методи дослідження — Моделювання схеми з налаштуванням IPSec VPN у симуляторі Cisco Packet Tracer на основі Cisco ASA-5506. Застосування мов розмітки HTML та CSS та мови програмування JavaScript для розробки веб-додатку

Результати — Розроблено веб-додаток для налаштування мережі. Користувач додатку вводить всі необхідні данні (ip-адреси, маски) та обирає додаткові налаштування трафіку. Додаток конфігурує данні введені користувачем ти виводить їх. Через буфер обміну данні можна скопіювати та використовувати для налаштування схеми.

IPSEC, VPN, CISCO, PACKET TRACER, HTML, CSS, JavaScript

ЗМІСТ

ВСТУП

На сьогоднішній день проблема мережевої безпеки стала на одне із перших місць. Корпоративні мережі та їх ресурси постійно перебувають від загрозою мережевої атаки або зараження шкідливим програмним забезпеченням. Цілі й завдання зловмисників можуть бути різними, а способи вторгнень можуть варіюватися від вірусів, надісланих електронною поштою, до повноцінної атаки ботнет-мереж. Джерелом небезпеки можуть бути не тільки хакери, а навіть власні співробітники.

Щоб нейтралізувати ці загрози, уникнути або мінімізувати можливі збитки, необхідно застосовувати відповідні механізми захисту.

Для вирішення цих проблем часто використовують міжмережеві екрани, так звані “Firewall”. Міжмережевий екран – це апаратно – програмний комплекс, який розділяє мережу на зони безпеки та здійснює ревізію трафіку, який проходить через нього, відповідно до заданих правил. Також часто на допомогу приходять програмні технології забезпечення безпеки – IPSec, VPN, Web Proxy, Antivirus та ін.

Великий попит на послуги на забезпечення мережевої безпеки обіцяє великі прибутки тим, хто їх надає. Оскільки процес налаштування міжмережевого екрану доволі ресурсозатратний процес, а системному адміністратору початківцю це зробити буде важко, було вирішено розробити графічний інтерфейс, який би спрощував налаштування мережевої безпеки для користувацьких даних.

Сьогодні важко уявити своє життя без інтернету. Доступ до нього мають майже всі жителі розвинутих країн. Тому було вирішено створити веб-додаток з використанням однієї з найпопулярніших у світі технології – IPSec на основі міжмережевого екрану Cisco ASA. За допомогою цього додатку користувачі зможуть полегшити собі налаштування безпеки у своїх мережах.

1 ОГЛЯД ІСНУЮЧИХ РІШЕНЬ

1.1 Апаратне забезпечення

Існує багато апаратних засобів мережевої безпеки, але в основному в саме для цих цілей використовуються роутери та міжмережеві екрани. Якщо подивитися на функції, які часто використовуються на практиці, то вони присутні як і в роутерах так і в міжмережевих екранах (Access-list, VPN та ін.) [1].

Роутер, або маршрутизатор (також часто “шлюз”) – електронний пристрій, що використовується для поєднання двох, або більше мереж між собою використовуючи принцип маршрутизації. Його робота полягає в тому, щоб передивлятися кожний пакет даних, що він отримує, зчитувати IP-адресу його джерела, знаходити його в своїй таблиці маршрутизації та відправляти за назначенням [2].

Рисунок 1.1 — Маршрутизатор Cisco 2911 [2]

Оскільки роутери допускають більше одного комп’ютера до мережі, вони також відкривають можливості для більшої кількості подій безпеки. Часто маршрутизатори знаходяться прямо у шлюза зовнішньої (мережа Інтернет) та внутрішньої мереж, що робить їх “першою лінією оборони”, але

тільки за умови, що вони захищені належним чином. Незахищені роутери відкривають надають зловмисникам великі можливості.

Але оскільки мережева безпека не основне призначення маршрутизатора, а лише додаткова функція, то для вирішення саме проблем безпеки потрібно використовувати міжмережевий екран.

Міжмережевий екран (фаєрволл або брандмауер) – це електронний пристрій або набір пристроїв, призначенням якого є допуск, відхилення, шифрування, пропуск через проксі весь трафік між областями різної згідно з набором правил чи інших критеріїв [3].

Рисунок 1.2 — Міжмережевий екран Cisco5500-X [4]

Найчастіше міжмережевий екран – це окремий прилад. Також міжмережевим екраном називають спеціальне програмне забезпечення. Дешеві та прості фаєрволли можуть не мати обширної та гнучкої системи налаштувань.

В залежності від активних з’єднань міжмережеві екрани розділяють :

- Stateless (Проста фільтрація) – поточні з’єднання не відслідковуються, потік даних фільтрується на основі статичних правил.

- Stateful (Фільтрація з урахуванням контексту) – поточні з’єднання відслідковуються, пропускаються лише ті пакети, які відповідають логіці й алгоритмам роботи відповідних протоколів та програм.

Також для того щоб відповідати вимогам широкого кола користувачів, існує три типи мережевих екранів:

- **Мережевого рівня** – представлений екрануючим маршрутизатором. Він контролює лише дані службової інформації пакетів мережевого і транспортного рівнів моделі OSI. Мінусом таких фаєрволлів є те, що п’ять рівнів залишаються неконтрольованими.
- **Прикладного рівня –** також відомий як проксі сервер. Мережеві екрани цього рівня встановлюють поділ між внутрішньою та зовнішньою мережами. Але вони неминуче зменшують продуктивність мережі.
- **Рівня з’єднання –** схожі на фаєрволли прикладного рівня, але різниця полягає в тому, що мережеві екрани рівня з’єднання вимагають спеціального забезпечення для кожної окремої служби (наприклад FTP, HTTP). Натомість вони обслуговують велику кількість протоколів.

Очевидно, що міжмережеві екрани відіграють величезну роль у мережевій безпеці. Зокрема фаєрволли фільтрації пакетів перевіряють заголовки всіх пакетів даних, що надходять у мережу та виходять з неї. Вони переглядають адресу джерела, інформацію про призначення та порт кожного пакету, щоб визначити його легітимність, а потім вирішують чи надсилати данні далі, чи блокувати їх, ґрунтуючись на наборі заздалегідь визначених правил, створених адміністратором мережі.

Незалежно від того, який міжмережевий екран використовується, його основна функція – це виявлення та блокування загроз, роблячи це ключовою частиною функцій безпеки вашої мережі.

Якщо порівнювати функціонал маршрутизатора та міжмережевого екрана саме з точки зору мережевого екрану, то найкращим вибором буде міжмережевий екран. Маршрутизатор також може бути налаштований так, щоб запобігти несанкціонованому доступу до мережі, але кібербезпека не його основне призначення. Основне ж призначення фаєрволла є запровадження мережевої безпеки.

Опираючись на все вище сказане для розроблення прототипу мережі для додатку за основу буде взятий міжмережевий екран, а саме один з найпопулярніших у світі – Cisco ASA5560 [4].

1.2 Технологія IPSec VPN

Технологія IPSec VPN – це набір протоколів для забезпечення захисту даних, які передаються по міжмережевому протоколу IP. Ця технологія дозволяє здійснювати аунтефікацію, перевірку цілісності та шифрування IP пакетів. IPSec також включає в себе протоколи для захищеного обміну ключами в мережі. В основному використовується для організації VPN – з’єднань [5].

Побудова захищеного каналу зв’язку може бути реалізована на різних рівнях моделі OSI. Так, наприклад, SSL-протокол працює на рівні представлення, а PPTP – на сеансовому. Компромісом у виборі рівня є IPSec: він розташовується на мережевому рівні, використовуючи найпоширеніший протокол цього рівня – IP. Це робить IPSec гнучкішим, так що він може використовуватися для захисту будь-яких протоколів, що базуються на TCP і UDP (наприклад DNS та HTTP).

Ця технологія є набором стандартів Інтернету. Її ядро складають три протоколи:

- Authentication Header (AH) – забезпечує цілісність даних, які передаються та аунтефікацію джерела.
- Encapsulating Security Payload (ESP) – забезпечує шифрування даних, обмежує потік конфіденціального трафіка.
- Internet Security Association and Key Management Protocol (ISAKMP) – використовується для первинного налаштування з'єднання, взаємної аунтефікації кінцевими вузлами один-одного та обміну секретними ключами.

IPSec може функціонувати в двох режимах: транспортному та тунельному. В транспортному режимі шифруються тільки дані пакету, а заголовок зберігається. Його як правило використовують для встановлення з'єднання між хостами. В тунельному режимі шифрується весь IP пакет і вставляється

В поле даних нового пакета. Цей режим використовується для підключення віддалених приладів до приватних мереж або для організації безпечної передачі даних через відкритий канал зв'язку для об'єднання різних частин приватних мереж. Ці два режими не є взаємовиключними.

Перед початком обміну даними необхідно встановити з'єднання, яке називається SA (Security Association). Концепція SA є головним принципом IPSec. Вона описує, як сторони будуть використовувати сервіси для безпечного обміну даними. Встановлення з' єднання починається зі взаємної аунтефікації сторін, далі відбувається вибір параметрів (шифрування, аунтефікації, перевірка цілісності даних) і необхідного протоколу (AH, ESP). Після цього обираються конкретні алгоритми шифрування (DES, MD5, SHA-1 та ін.).

IKE – протокол, який з'єднує всі компоненти IPSec в працеспроможне ціле. Так цей протокол забезпечує початкову аунтефікацію сторін, а також їх обмін секретними ключами.

Принцип роботи IKE можна розбити на дві фази:

- Перша фаза – встановлюється безпечний канал між двома вузлами. Також в цій фазі 2 вузли обговорюють сесійних ключ по алгоритму Диффи-Хеллмана.
- Друга фаза – встановлюється загальна політика IPSec, отримуються загальні секретні ключі, встановлюється IPSec SA.

В роботі протоколу IPSec можна виділити 5 основних етапів:

1. На першому етапі на кожному із вузлів створюється політика безпеки, яка підтримує стандарти IPSec.
2. Другий етап по суті є першою фазою IKE – організація безпечного каналу.
3. Третій етап є другою фазою IKE. На цьому етапі створюється IPSec-тунель.
4. Робочій етап – починається обмін інформацією через IPSec-тунель.
5. Кінець життєвого циклу IPSec SA. Якщо передача даних не завершилась, створюється нове з’єднання IPSec SA.

Протокол IPSec використовується, в основному, для організації VPN-тунелів. У цьому випадку протоколи ESP та AH працюють в режимі тунелювання [6].

Site-to-site VPN – спосіб реалізації технології VPN, призначений для створення захищеного віртуального тунелю. Основна його відмінність від традиційного режиму використання VPN (Point-to-point) – це відсутність необхідності налаштування параметрів підключення для кожного пристрою, досить лише конфігурувати по одному шлюзу з кожної з сторін. Також саме Site-to-Site VPN часто використовують для безпечного з’єднання філіалів компаній.

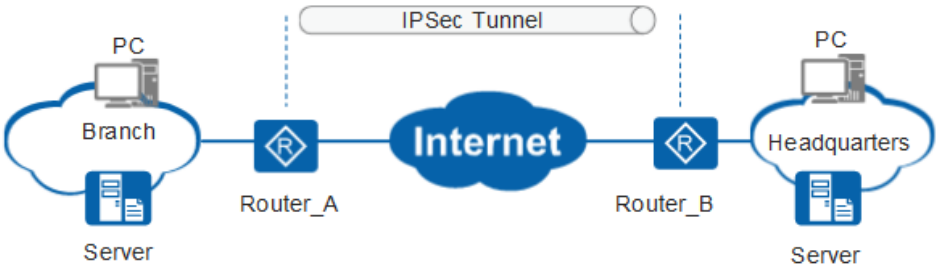

Рисунок 1.3 — Приклад IPSec VPN тунелю через мережу Internet [5]

Спираючись на вищесказане для забезпечення безпеки у мережі, а саме у прототипі мережі для додатку, буде використовуватися технологія IPSec VPN.

1.3 Постановка задачі

Провівши аналіз літератури можна виділити такі висновки. IPSec – одна із найпопулярніших технологій для забезпечення мережевої безпеки в сучасному світі, але для її налаштування необхідно виконати деякі дії.

Постановку задачі можна сформувати наступним чином:

1. Налаштувати прототипу мережі на основі міжмережевого екрану Cisco ASA у програмі Cisco Packet Tracer.
2. Проаналізувати схему, та визначити які дії можна спростити та автоматизувати за допомогою додатку.
3. Створити веб-додаток використовуючи HTML, CSS та JavaScript.

2 НАЛАШТУВАННЯ ТЕХНОЛОГІЇ IPSec

2.1 Налаштування схеми з технологією IPSec VPN

У симуляторі Cisco Packet Tracer створимо таку мережу:

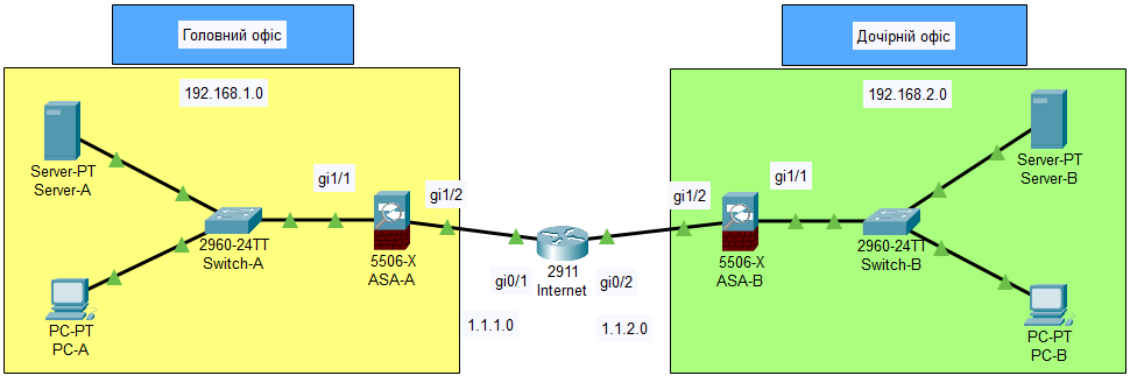

Рисунок 2.1 – Топологія мережі

На схемі мережі показано 2 офісі компанії, між ними роутер, який симулює провайдера та мережу Internet. Для демонстрації всіх можливостей IPSec VPN

Налаштуємо сервер B під DNS-сервер в дочірньому офісі.

Для налаштування даної схеми необхідно виконати наступні команди:

На роутері Internet вмикаємо та задаємо ip-адреси на інтерфейсах:

```
enable
conf t
int gi0/1
ip address 1.1.1.2 255.255.255.252
no sh
int gi0/2
```

ip address 1.1.2.2 255.255.255.252

no sh

На ASA-A:

Вмикаємо інтерфейси та задаємо ip-адреси на них:

enable

conf t

int gi1/2

nameif outside

ip address 1.1.1.1 255.255.255.252

no sh

exit

int gi1/1

nameif inside

ip address 192.168.1.1 255.255.255.0

no sh

Встановлюємо маршрут з мережі через інтерфейс outside через IP провайдера:

route outside 0.0.0.0 0.0.0.0 1.1.1.2

Далі налаштовуємо інспектування трафіку.

Визначення class-map:

class-map inspection_default

match default-inspection-trafic

Визначаємо policy-map:

policy-map global_policy

class inspection_default

Додаємо інспектування icmp трафіку:

inspect icmp

Робимо політику глобальною:

service-policy global_policy global

Налаштовуємо VPN першої фази:

crypto ikev1 enable outside

crypto ikev1 policy 1

encryption 3des

hash md5

authentication pre-share

group 2

lifetime 43200

Налаштування ключа аунтефікації та піра:

tunnel-group 1.1.2.1 type ipsec-l2l

tunnel-group 1.1.2.1 ipsec-attributes

ikev1 pre-shared-key cisco

Налаштування VPN другої фази:

crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac

Визначаємо, який трафік шифрувати:

access-list FOR-VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0

Створюємо криптkарту:

crypto map To-Site2 1 match address FOR-VPN

crypto map To-Site2 1 set peer 1.1.2.1

crypto map To-Site2 1 set security-association lifetime seconds 86400

crypto map To-Site2 1 set ikev1 transform-set TS

Прив’язуємо криптокарту до інтерфейсу:

crypto map To-Site2 interface outside

Дозволяємо вхідний трафік:

access-list FROM-VPN extended permit icmp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0

access-group FROM-VPN out interface inside

На міжмережевому екрані ASA-B налаштування майже нічим не відрізняються див. Додаток Д.

Для перевірки правильності налаштувань на міжмережевих екранах необхідно ввести команду “show crypto ipsec sa”

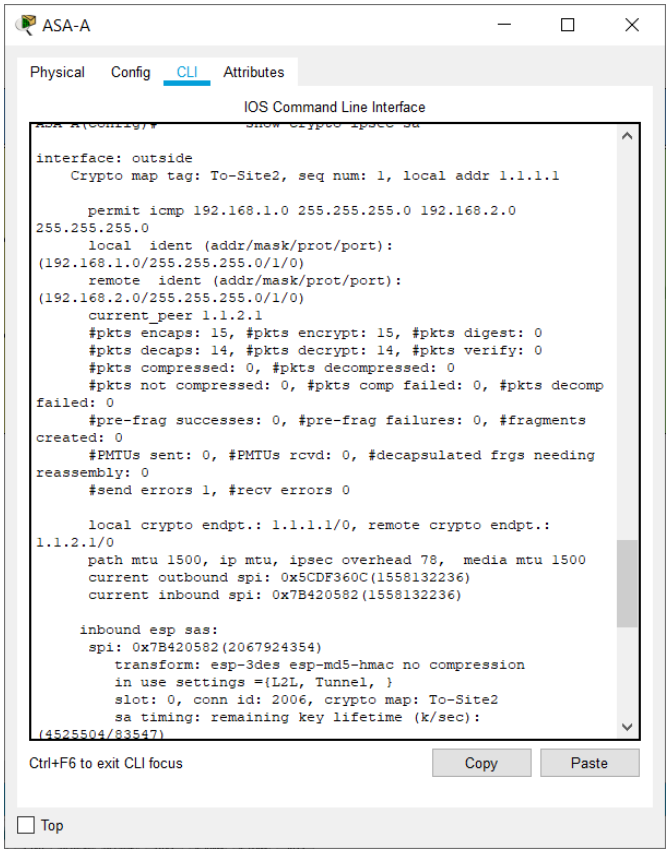

Рисунок 2.2 – Результат команди “show crypto ipsec sa”

Після цих налаштувань необхідно також конфігурувати комп’ютери та сервери у двох мережах. Для зручності у додатку Packet Tracer можна використати екранні форми. Також на всіх пристроях необхідно вказати DNS-server 192.168.2.2 , а на сервері Server-B налаштувати цей сервер. Після налаштувань необхідно перевірити мережу.

На рис. 2.2 видно всі задані налаштування, тепер необхідно перевірити їх. Для цього скористаємося командою “ping” на одному з комп’ютерів для перевірки з’єднання з іншим офісом. Ця команда є прикладом icmp трафіку.

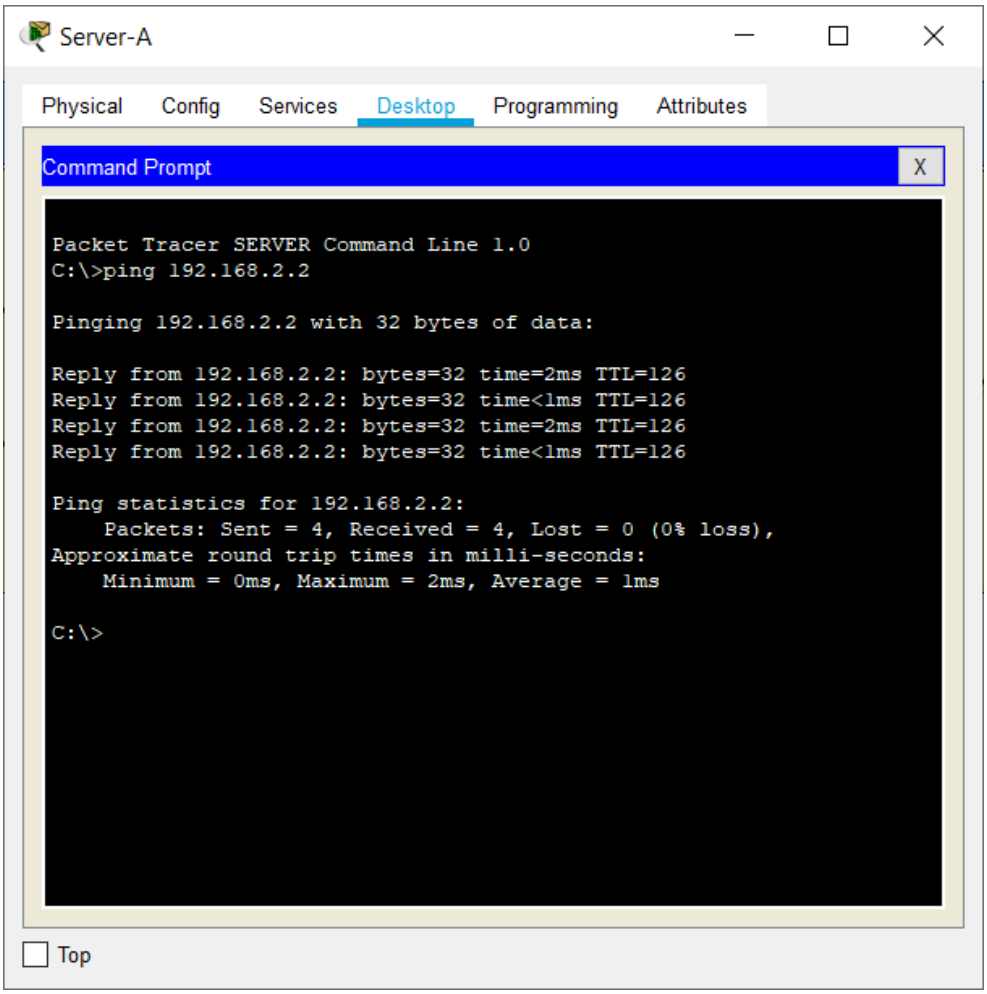

Рисунок 2.3 – Результат команди “ping”

На рис. 2.3 видно «Sent = 4, Received = 4, Lost = 0», це означає що було послано 4 пакети і кожен дійшов до адресата 192.168.2.2. Тому

можемо зробити висновок, що мережа та технологія IPSec налаштовані вірно.

Також можна зконфігурувати додаткові налаштування, а саме можливість переглядати внутрішній корпоративний сайт з будь-якого пристрою. Для цього потрібно дозволити пропуск DNS та HTTP трафіку на міжмережевих екранах. Розглянемо на прикладі налаштування ASA-A(для ASA-B див. Додаток Д):

Налаштовуємо інспектування цих типів трафіку:

```
policy-map global_policy
class inspection_default
inspect dns
inspect http
exit
```

Визначаємо, який трафік потрібно шифрувати. Для передачі трафік типу dns та http використовуються протоколи вищого рівня, такі як UDP(dns) та TCP(http:)

```
access-list FOR-VPN extended permit udp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
access-list FOR-VPN extended permit tcp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0

access-list FROM-VPN extended permit udp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list FROM-VPN extended permit tcp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
```

Ці команди розширюють налаштування міжмережевих екранів і дозволяють шифрувати та пропускати відповідний трафік між двома мережами.

Тепер можна перевірити налаштування. Для цього необхідно відкрити веб-браузер на комп’ютері А та вписати в адресну строку доменне ім’я сайту filial.com.

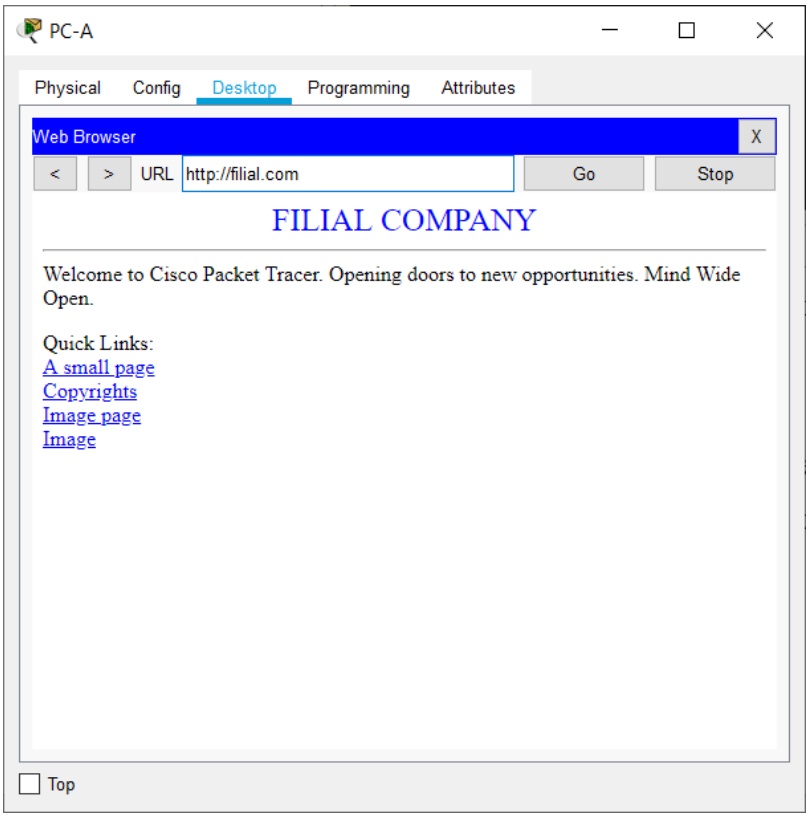

Рисунок 2.4 – Результат налаштувань веб-трафіку

Результат додаткових налаштувань можна побачити на рис. 2.4. Веб-сторінка відкрилась, отже можна впевнитися, що VPN-тунель шифрує та передає дані відповідних типів між мережами.

2.2 Засоби створення веб-додатків

Існує багато способів створення веб-додатків, але найпопулярніший із них – це використання мов розмітки HTML та CSS, та мови програмування JavaScript.

HTML (від англ. HyperText Markup Language – “Мова розмітки гіпертексту”) – це загальноприйнята мова розмітки документів у мережі Інтернет. Більшість веб-сторінок створюються за допомогою цієї мови. Мова HTML інтерпріюється браузерами у вигляді документа в зручній для користувача формі.

CSS (від англ. Cascading Style Sheets – “Каскадні таблиці стилів”) – формальна мова опису зовнішнього вигляду документа, написаного за допомогою мови розмітки. Використовується, як засіб опису зовнішнього вигляду веб-сторінок.

CSS є зручним, практичним та ефективним інструментом оформлення зовнішнього вигляду веб-сторінок. Однією з переваг використання саме CSS є розмежування коду і оформлення. Принцип полягає в тому, щоб HTML був звільнений від елементів оформлення. Також перевагою є можливість створення динамічних сторінок та різне оформлення для різних пристроїв. За допомогою CSS можна визначити вид веб-сторінки в залежності від пристрою виводу. Також стилі, як правило, зберігаються в одному або в декількох спеціальних файлах, посилання на які вказуються в усіх документах сайту. Завдяки цьому зручно правити стиль в одному місці, при цьому оформлення елементів автоматично змінюється на всіх сторінках, які пов’язані із зазначеним файлом.

JavaScript – одна із найпопулярніших мов програмування для створення веб-додатків. Вона підтримує як об’єктно-орієнтований так і імперативний та функціональний стилі. Основною особливістю цієї мови програмування є те, що вона виконується на стороні користувача, а не на сервері.

В основному JavaScript використовується для FrontEnd - розробки, а саме в управлінням властивостями веб-сторінки та вікном браузера. Ця мова програмування дає можливість змінювати сторінки веб-браузерів, додавати чи видаляти HTML-теги, змінювати стилі сторінок і також робота з cookie-файлами.

В порівнянні з іншими мовами програмування JavaScript має такі переваги:

- Підтримується всіма сучасними веб-браузерами.
- Простий синтаксис
- Корисні функціональні налаштування
- Взаємодія з додатками може відбуватися навіть через текстові редактори

Також JS має декілька недоліків:

- Знижений рівень безпеки. Це спричинено тим, що вихідні коди популярних скриптів знаходяться у відкритому доступі.
- Вважається менш професіональним в порівнянні з іншими.

Спираючись на всі вищеперечислені факти можна з впевненістю сказати, що графічний інтерфейс веб-додатку краще розробляти за допомогою HTML та CSS, а функціонал за допомогою JavaScript.

3 РОЗРОБКА ВЕБ-ДОДАТКУ

3.1 Розробка інтерфейсу додатка

На основі розробленого прототипу мережі, де були дві мережі, VPN-тунель між ними та технологія IPSec для безпечної передачі даних між ними. У ході налаштування прототипу мережі були виявлені процеси налаштування які можна спростити та автоматизувати за допомогою додатку. На основі цього був розроблений інтерфейс додатку.

Відкривши додаток, користувач побачить схему налаштування мережі.

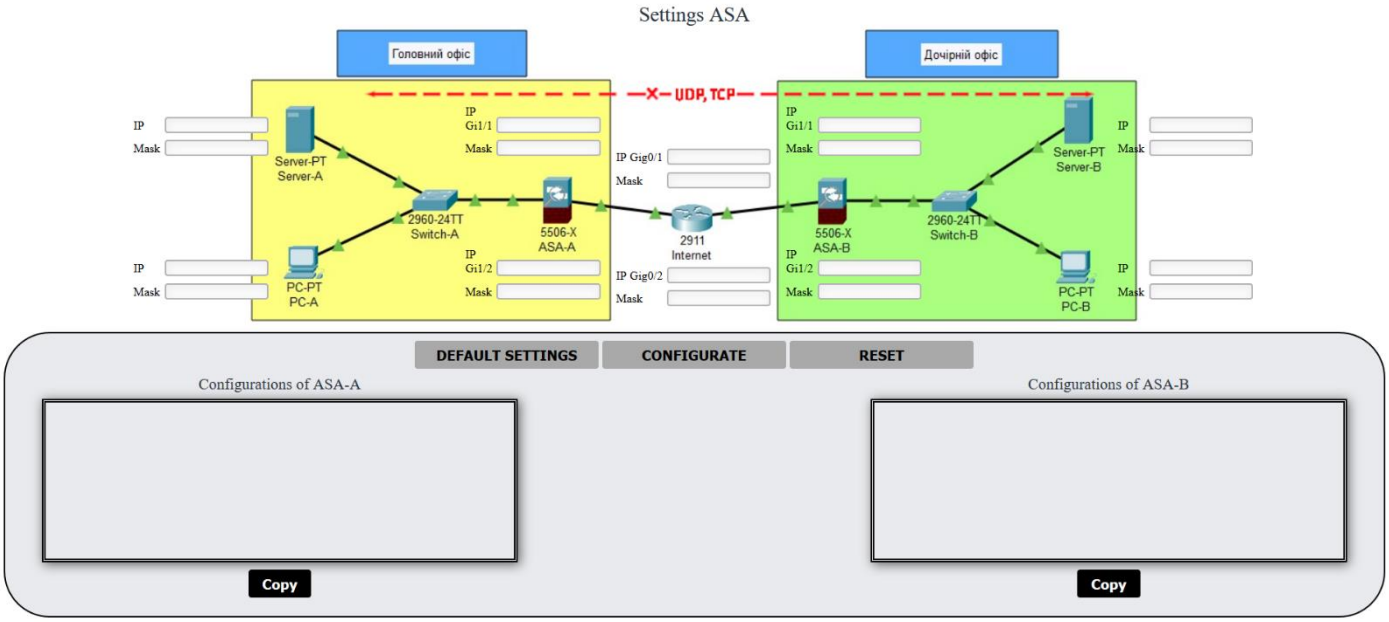

Рисунок 3.1 – Зовнішній вигляд додатку

На рис. 3.1 можна побачити зовнішній вигляд додатку. Текстові поля для вводу ip-адрес, та масок для кожного пристрою в мережі. Під схемою мережі можна побачити основне меню додатку: кнопки конфігурації та місця виводу команд.

3.2 Опис функціоналу додатка

Користувач має можливість самому вводити данні для кожного пристрою, або ж скористатися функцією стандартних налаштувань. Для цього користувачу необхідно натиснути на кнопку “Default Settings”.

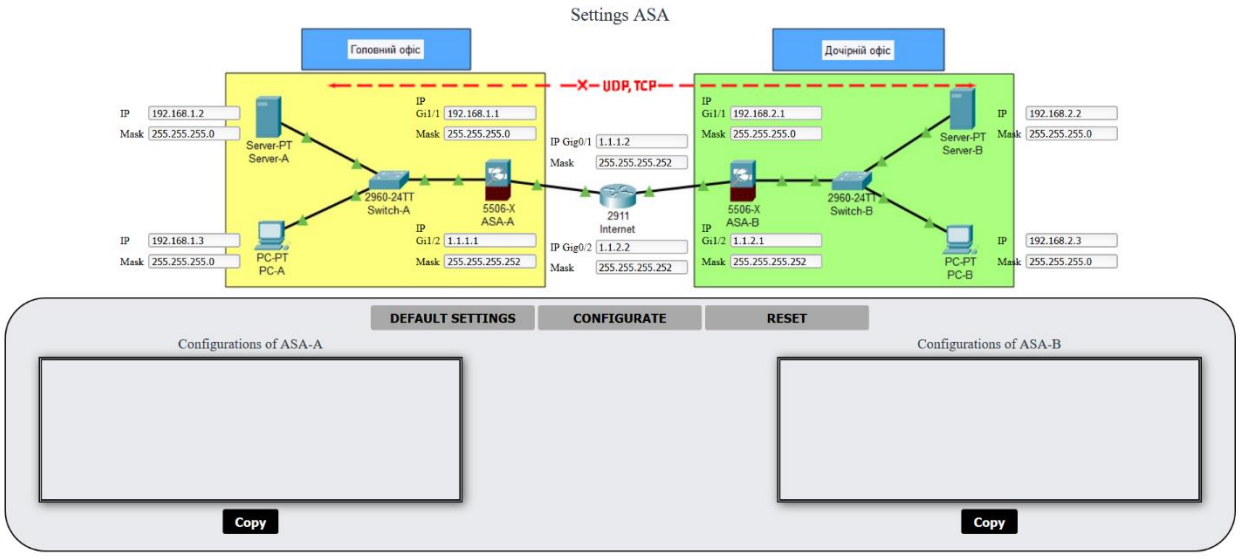

Рисунок 3.2 – Приклад роботи кнопки “Default Settings”

Рисунок 3.3 – Приклад роботи додатку при неправильному заповненні полів

Після цього користувач має змогу отримати команди для налаштування міжмережевих екранів. Для цього він має натиснути на кнопку “Configurate”.

Якщо одне з полів вводу залишилось не заповненим, то користувач отримає відповідне повідомлення як показано на рис. 3.3.

При правильному заповненні полів додаток автоматично зконфігурує налаштування двох міжмережевих екранів та виведе їх у відповідні поля виводу.

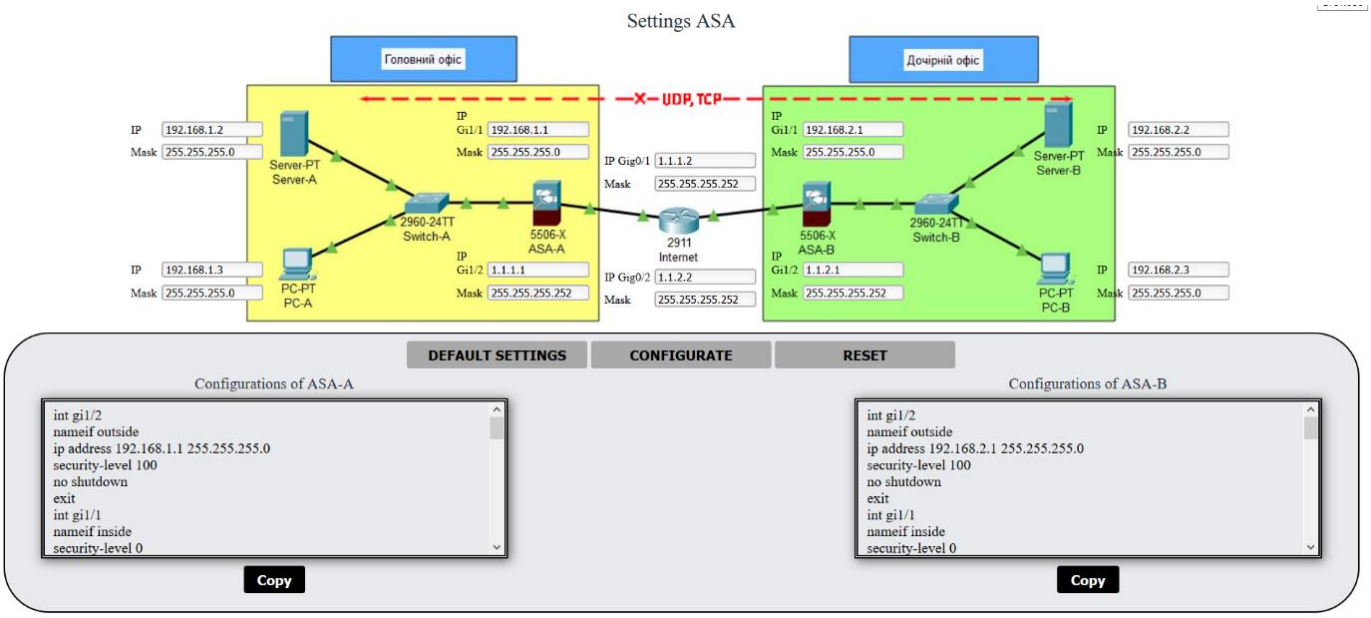

Рисунок 3.4 – Приклад конфігурації додатку

Також для зручності на головну меню є кнопка “Reset”, яка при натиску на неї очищую всі поля.

За замовчуванням між двома офісами можна передавати icmp трафік. На схемі мережі для додаткових налаштувань (DNS, HTTP – трафіку) знаходиться чутлива до натиску червона стрілка. При натиску на неї колір стрілочки змінюється на зелений, а до налаштувань міжмережевих екранів додаються команди дозволу для цих видів трафіку. При повторному натиску на неї, стрілка знову стає червоною, а відповідний тип трафіку забороняється.

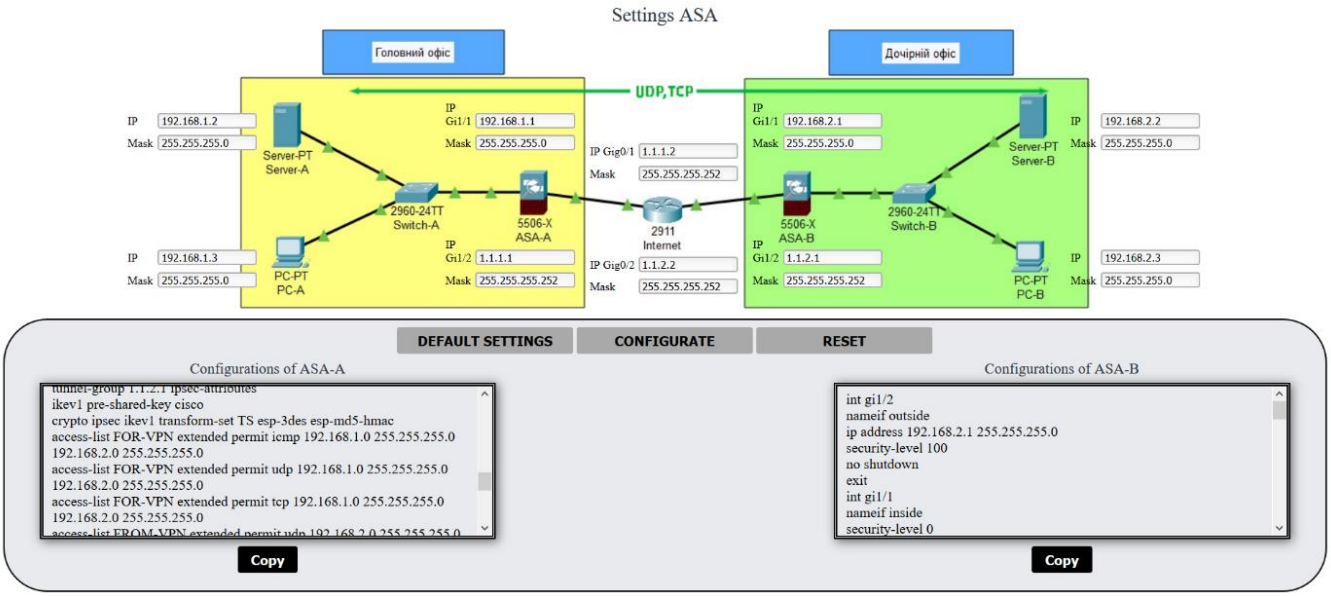

Рисунок 3.4 – Приклад використання додаткових параметрів

Також користувач має змогу скопіювати налаштування для відповідного фаєрволлу до буферу обміну кнопкою “Copy”.

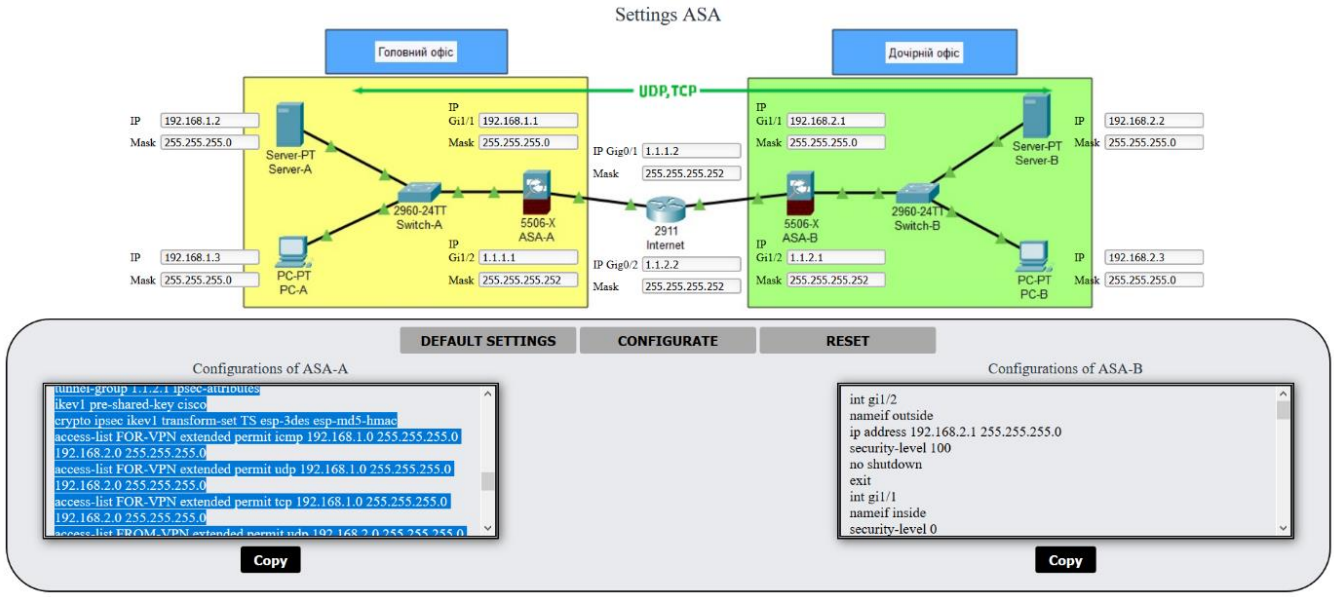

Рисунок 3.5 – Приклад роботи кнопки “Copy”

3.3 Тестування додатку

Відкриємо додаток, натискаємо кнопку “Default settings” та натискаємо на червону стрілку. Додаток автоматично заповнить всі поля див. рис 3.9.

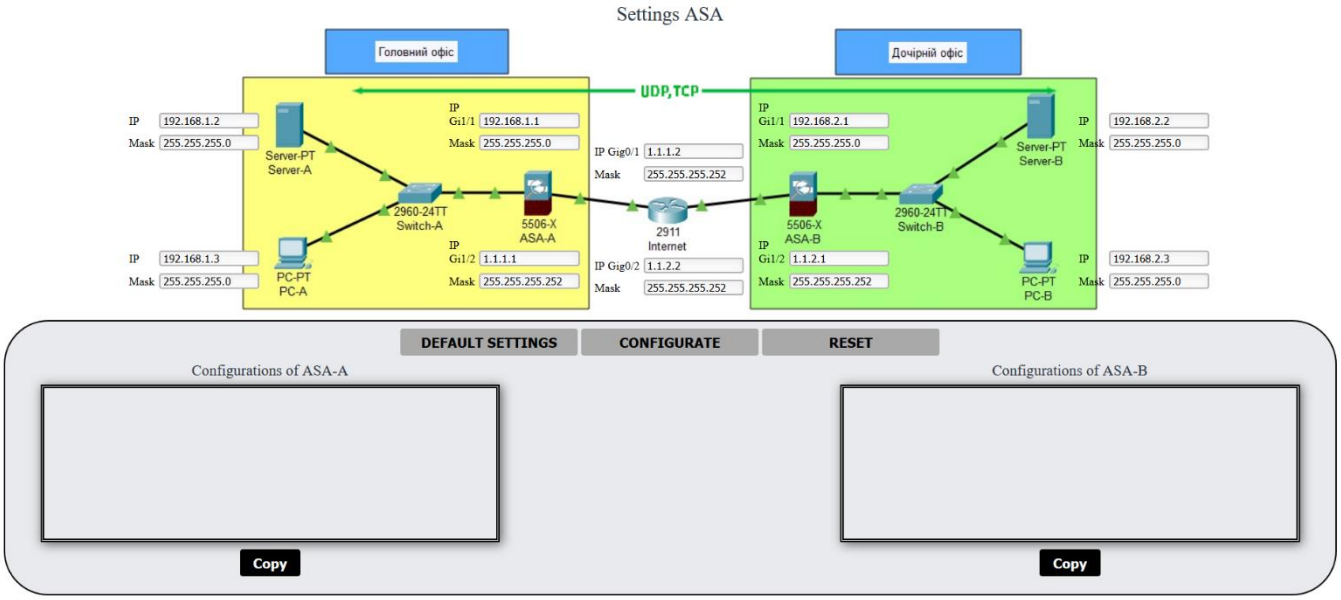

Рисунок 3.9 – Заповнення полів

Після цього натискаємо кнопку «Configurate». Додаток зконфігурує налаштування для міжмережевих екранів див. рис. 3.10.

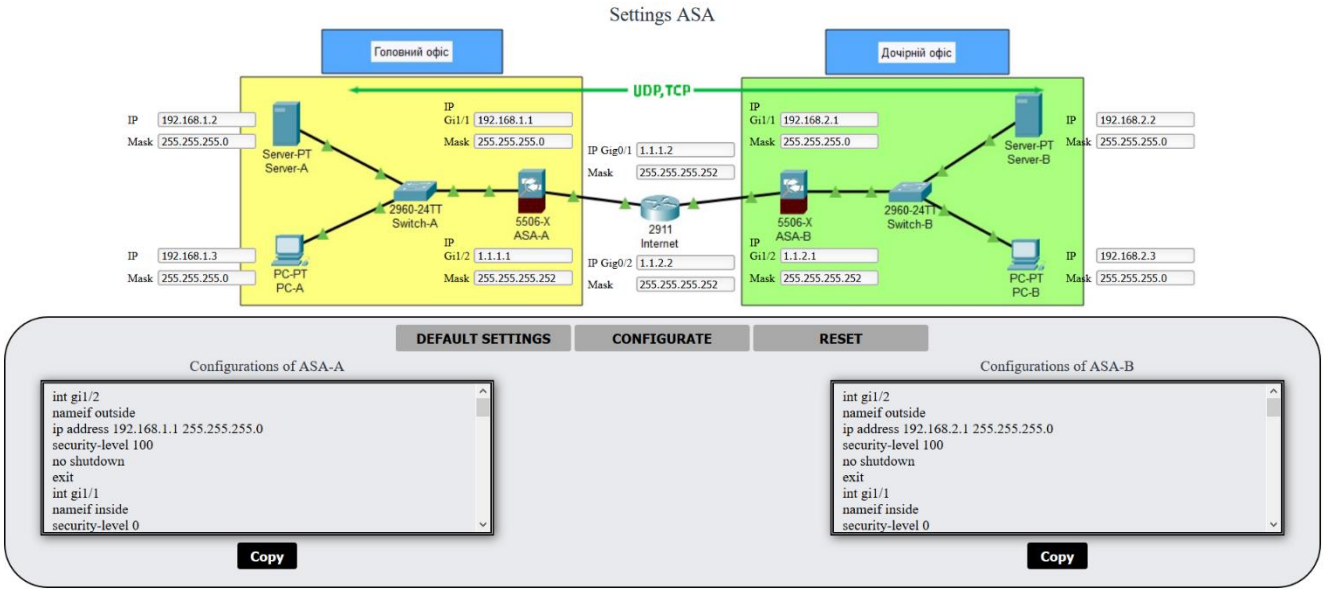

Рисунок 3.10 – Команди конфігурації

Далі копіюємо команди відповідного міжмережевого екрану та налаштовуємо схему у програмі Cisco Packet Tracer.

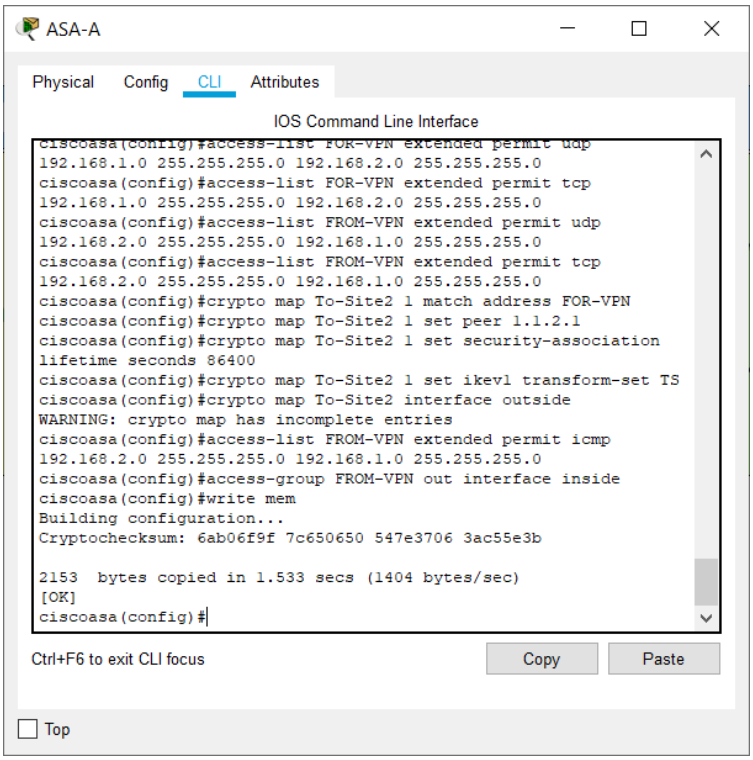

Рисунок 3.11 – Налаштування фаєрволлу за допомогою скопійованих команд

Тепер налаштовуємо всі інші прилади в мережі. Після завершення налаштувань необхідно перевірити їх правильність за допомогою команді “show crypto ipsec sa”. На рис. 3.12 показано результат виконання цієї команди.

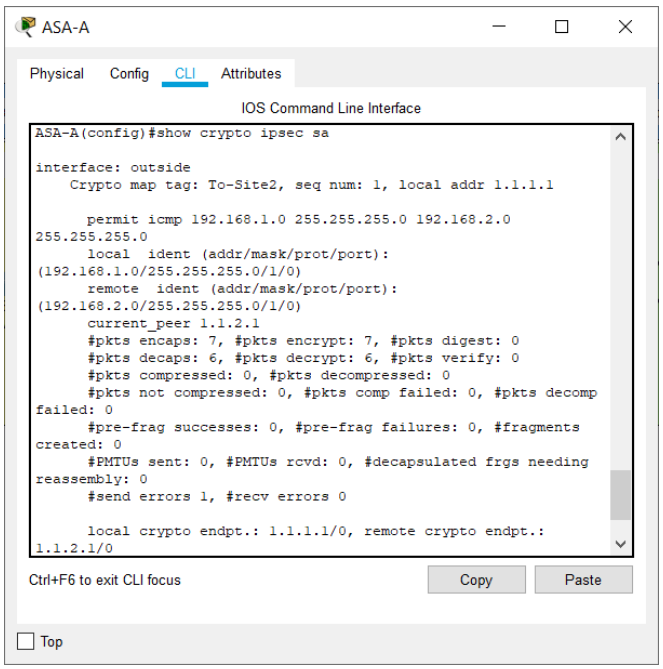

Рисунок 3.12 – Результат налаштування

Щоб повністю впевнитись у роботоспроможності додатку скористаємося командою “ping” та пропінгуємо комп’ютери з різних мереж. Між комп’ютерами встановлене надійне з’єднання див. рис. 3.13.

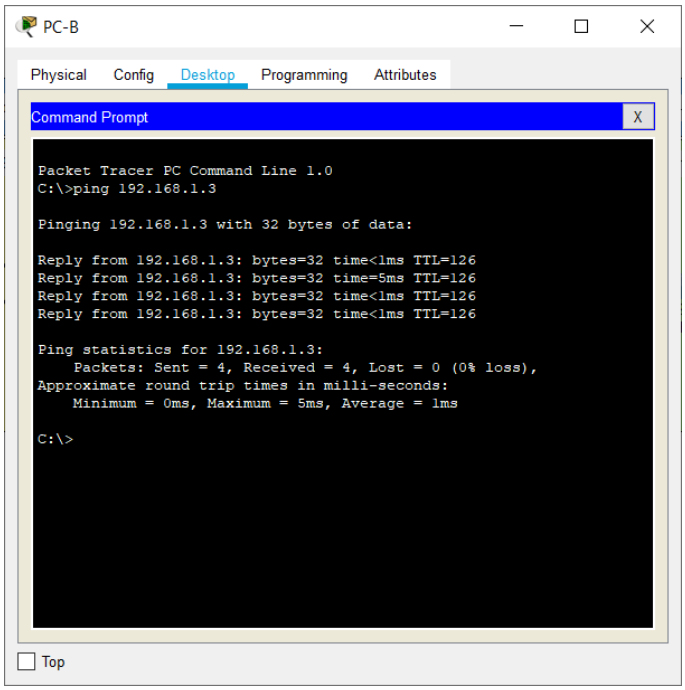

Рисунок 3.13 – Результат використання команди “ping”

Як можна побачити на рис. 3.12 та на рис. 3.13 схема налаштована правильно, а отже можна зробити висновок, що додаток повністю працеспроможний.

ВИСНОВКИ

У ході виконання роботи було розібрано необхідність мережевої безпеки, а також розібрано засоби її запровадження як апаратні (міжмережевий екран) так і програмні (IPSec). Технологія IPSec допомагає запроваджувати основні способи захисту даних.

IPsec розташовується на мережевому рівні моделі OSI, використовуючи найпоширеніший протокол цього рівня – IP. Це робить IPSec гнучкішим, так що він може використовуватися для захисту будь-яких протоколів, що базуються на TCP і UDP (наприклад DNS та HTTP).

Технологія IPSec є також багатопротокольною, що дозволяє використовувати її для широкого спектру задач.

Був створений прототип мережі в програмі Cisco Packet Tracer, на якому зручно продемонструвати основні можливості IPSec та міжмережевих екранів.

Проаналізувавши схему та її принципові налаштування був розроблений веб-додаток, за допомогою якого зручно і швидко налаштовувати мережу з використанням міжмережевих екранів та технології IPSec. У ході роботи додаток був протестований, а саме, була налаштована схема з використанням додатку. В майбутньому додаток може бути покращений – додавання розгалужень до мережі та більш обширні налаштування трафіку.

Додаток зручний і простий у використанні навіть адміністраторами початківцями. Використання додатку значно полегшує налаштування мережі.

СПИСОК ЛІТЕРАТУРИ

1. Безпека Мережі
   [Електронний ресурс] - http://www.zirozebar.com/pedia-uk/wiki/Безпека_мережі
2. Routers, Switches and Firewalls: What are the difference?
   [Електронний ресурс] - https://developcents.com/2013/08/12/routers-switches-firewalls-differences/
3. Міжмережевий екран
   [Електронний ресурс] -https://uk.wikipedia.org/wiki/Мережевий_екран
4. Прилади захисту Cisco ASA
   [Електронний ресурс] - https://www.bytemag.ru/articles/detail.php?ID=8789
5. Технологія IPSec VPN
   [Електронний ресурс] - https://ru.wikipedia.org/wiki/IPsec#Стандарти
6. Site-to-Site VPN Routing Explained In Details
   [Електронний ресурс] - https://openvpn.net/vpn-server-resources/site-to-site-routing-explained-in-detail/
7. Д. Н. Роббінс "HTML5, CSS3, JavaScript. Исчерпывающее руководство. 4-е издание" 2014 - 516
8. В. Олифер, Н. Олифер "Компьютерные сети. Принципы, технологии, протоколы. Учебник" 2016. – 233 с.
9. Э. Таненбаум, Д. Уэзеролл "Компьютерные сети" 5-е изд. 2016. – 95 с.
10. Грайворонський М. В. Безпека інформаційно-комунікаційнихсистем : підручник для ВНЗ / М. В. Грайворонський, О. М. Новіков // М-во праці та соц. політики України. Держнагляд охорон праці України. - К. : ВНV, 2009. - 607 с.

ДОДАТКИ

Додаток А

Графічний інтерфейс додатку

```
<html>
<head>

<script src="js/clipboard.js"></script>
<script src="js/jquery.min.js"></script>
<script src="js/script.js"></script>
<link rel="stylesheet" href="css/style.css">
<title>Settings ASA</title>

</head>
<body>
<div class="title_prog">Settings ASA</div>
<div class="map">
<div class="arrow"></div>
<div class="router_internet">
<div class="router_internet_gi_0_1">
<div class="label">IP Gig0/1</div><input id="router_ip_gi_0_1" type="text" name="" > <br>  <div
class="label">Mask</div><input id="router_mask_gi_0_1" type="text" name="" > <br>
</div>
<br>
<div class="router_internet_gi_0_2">
<div class="label">IP Gig0/2</div><input id="router_ip_gi_0_2" type="text" name="" > <br>
<div class="label">Mask</div><input id="router_mask_gi_0_2" type="text" name="" > <br>
</div>
</div>
<div class="main_office">
<div class="server_A">
<div class="label">IP </div><input id="ip_server_a" type="text" name="" > <br>
<div class="label">Mask </div><input id="mask_server_a" type="text" name="" >
</div>
<div class="asa_A_gi_1_1">
<div class="label">IP Gi1/1</div><input id="ip_asa_A_gi_1_1" type="text" name="" > <br>
<div class="label">Mask </div><input id="mask_asa_A_gi_1_1" type="text" name="" >
</div>
<br>
```

```
<div class="pc_A">
<div class="label">IP </div><input id="ip_pc_a" type="text" name="" > <br>
<div class="label">Mask </div><input id="mask_pc_a" type="text" name="" >
</div>
<div class="asa_A_gi_1_2">
<div class="label">IP Gi1/2</div><input id="ip_asa_A_gi_1_2" type="text" name="" > <br>
<div class="label">Mask </div><input id="mask_asa_A_gi_1_2" type="text" name="" >
</div>
</div>
<div class="fillial_office">
<div class="asa_B_gi_1_1">
<div class="label">IP Gi1/1</div><input id="ip_asa_B_gi_1_1" type="text" name="" > <br>
<div class="label">Mask </div><input id="mask_asa1_asa_A_gi_1_1" type="text" name="" >
</div>
<div class="server_B">
<div class="label">IP </div><input id="ip_server_b" type="text" name="" > <br>
<div class="label">Mask </div><input id="mask_server_b" type="text" name="" >
</div>
<br>
<div class="asa_B_gi_1_2">
<div class="label">IP Gi1/2</div><input id="ip_asa_B_gi_1_2" type="text" name="" > <br>
<div class="label">Mask </div><input id="mask_asa_B_gi_1_2" type="text" name="" >
</div>
<div class="pc_B">
<div class="label">IP </div><input id="ip_pc_b" type="text" name="" > <br>
<div class="label">Mask </div><input id="mask_pc_b" type="text" name="" >
</div>
</div>
</div>
<div class="asa_config_bg">
<div class="block_kontr">
<div class="buttons">
<div class="buttons_conf"><input class="button_default" type="button" value="Default settings" ></div>
<div class="buttons_conf"><input class="button_conf" type="button" value="Configurate" ></div>
<div class="buttons_conf"><input class="button_reset" type="button" value="Reset" ></div>
</div>
<div class="asa_a_config">
<div class="title_config_A">Configurations of ASA-A</div>
<div id="output_config_A" class="output_config_A"></div>
<input id="copy_A" class="copy_A" data-clipboard-target="#output_config_A" type="button" value="Copy" >
</div>
```

```
<div class="asa_b_config">
<div class="title_config_B">Configurations of ASA-B</div>
<div id="output_config_B" class="output_config_B"></div>
<input id="copy_B" class="copy_B" data-clipboard-target="#output_config_B" type="button" value="Copy" >
</div>
</div>
</div>
</body>
</html>
```

Додаток Б

Оформлення графічного інтерфейсу додатку

```
.title_prog {
    text-align: center;
    font-size: 22px;
    color: #2A3541;
}
.output_config_A {
    width: 500px;
    height: 160px;
    overflow: auto;
    padding: 5px 0 5px 10px;
    box-shadow: 2px 2px 12px 0px rgba(50, 50, 50, 0.75);
    border: 4px double black;
}
.output_config_B {
    width: 500px;
    height: 160px;
    overflow: auto;
    padding: 5px 0 5px 10px;
    box-shadow: 2px 2px 12px 0px rgba(50, 50, 50, 0.75);
    border: 4px double black;
}
.label{
        width: 34px;
        margin: 5px 0;
        display: inline-block;
    font-size: 13px;
}

.router_internet input,
.main_office input,
.fillial_office input{
        width: 113px;
    padding: 0 3px;
    background-color: #fcfcfc;
    border: 2px solid #b3b2b2;
    color: #000;
    font-size: 12px;
    border-radius: 3px;
```

```
    box-shadow: inset 1px 3px 10px 0 #eeeeef;
}


.main_office input{
        margin: 3px 0;
}
.map{
    background: url(../image/bg_map.jpg) no-repeat center;
        width: 1080px;
        height: 332px;
        position: relative;
        margin: 0 auto;
}
.main_office {
    position: absolute;
    top: 70;
    left: -70;
        z-index: 10;
}
.fillial_office {
    position: absolute;
    top: 70;
    left: 640;
        z-index: 10;
        width: 1000px;
}
.buttons_conf{
        margin: 0 auto;
        position: relative;
        display: inline-block;
}


.asa_b_config {
    display: inline-block;
    float: right;
    margin: -20px 40px 0 0 ;
}
.asa_a_config {
    display: inline-block;
```

```
    margin: -20px 0 0 40px;
}


.main_office .asa_A_gi_1_1 {
    display: inline-block;
    margin: 10px 0 0 160px;
}
.main_office .server_A {
    display: inline-block;
    margin: 20px 50px 0 0 ;
}
.main_office .pc_A{
            display: inline-block;
            margin: 0px 0 0 0px;
}
.main_office .asa_A_gi_1_2 {
            display: inline-block;
    margin: 90px 0 0 210px;
}


.fillial_office .asa_B_gi_1_1 {
    display: inline-block;
    margin: 10px 0 0 0;
}
.fillial_office .asa_B_gi_1_2 {
            display: inline-block;
            margin: 90px 0 0 0 ;
}
.fillial_office .server_B {
    display: inline-block;
    margin: 0 0px 0 210px;
}
.fillial_office .pc_B{
            display: inline-block;
            margin: 0 0 0 210px;
}

.asa_config_bg {
    background: #E9EAED;
```

```
    padding: 0 0 20px 0;
}
input.copy_B {
    margin: 10px 0 0 0;
    float: center;
}
input.copy_A {
    margin: 10px 0 0 0;
}
input.button_reset,
input.button_default,
input.button_conf {
    padding: 6px 15px;
    background-color: #A9A9A9;
    border: 0;
    border-radius: 3px;
    color: #000;
    font-size: 15.4px;
    text-transform: uppercase;
    font-weight: 600;
    margin: 8px 0 0 0;
    cursor: pointer;
    width: 200px;
}
input.button_reset:hover,
input.button_default:hover,
input.button_conf:hover,
input.button_enter_default:hover {
    background: #708090;
    color: #fff;
}

.title_config_A,
.title_config_B {
    text-align: center;
    font-size: 17px;
    margin: 0 0 6px 0;
    color: #2A3541;
}
input#copy_A,
input#copy_B {
```

```
    background: #000;
    padding: 6px 15px;
    border: 0;
    border-radius: 3px;
    color: #fff;
    font-size: 15.4px;
    font-weight: 600;
    margin: 8px 0 0 225px;
    cursor: pointer;
}
input#copy_A:hover,
input#copy_B:hover {
    background: #047390;
}

.main_office input:focus,
.fillial_office input:focus,
.router_internet input:focus {
    border-color: #74d36b;
}


.router_internet {
    position: absolute;
    top: 240;
    left: 455;
            z-index: 10;
}

.router_internet_gi_0_1{
            position: absolute;
            margin: -110px 0 0 0;
}


.router_internet .label{
    width: 55px;
}
.asa_config_bg {
    width: 1500px;
    margin: 0 auto;
```

```
    background: #E9EAED;
    border: 2px solid #000;
    border-radius: 50px;
}


.arrow {
    width: 800px;
    height: 16px;
    position: absolute;
    bottom: 250px;
    left: 180px;
    cursor: pointer;
    background: url(../image/arrow_red.png) no-repeat;
}

.buttons {
    text-align: center;
    height: 65px;
}
```

Додаток В

Функціонал графічного інтерфейсу

```
$(document).ready(function(){

new Clipboard('.copy_A');
new Clipboard('.copy_B');



$(".button_conf").click(function(){

var router_ip_gi_0_1 = document.getElementById("router_ip_gi_0_1").value;
var router_mask_gi_0_1 = document.getElementById("router_mask_gi_0_1").value;
var router_ip_gi_0_2 = document.getElementById("router_ip_gi_0_2").value;
var router_mask_gi_0_2 = document.getElementById("router_mask_gi_0_2").value;

var ip_server_a = document.getElementById("ip_server_a").value
var mask_server_a = document.getElementById("mask_server_a").value
var ip_asa_A_gi_1_1 = document.getElementById("ip_asa_A_gi_1_1").value
var mask_asa_A_gi_1_1 = document.getElementById("mask_asa_A_gi_1_1").value
var ip_pc_a = document.getElementById("ip_pc_a").value
var mask_pc_a = document.getElementById("mask_pc_a").value
var ip_asa_A_gi_1_2 = document.getElementById("ip_asa_A_gi_1_2").value
var mask_asa_A_gi_1_2 = document.getElementById("mask_asa_A_gi_1_2").value



var ip_asa_B_gi_1_1 = document.getElementById("ip_asa_B_gi_1_1").value
var mask_asa_B_gi_1_1 = document.getElementById("mask_asa1_asa_A_gi_1_1").value
var ip_server_b = document.getElementById("ip_server_b").value
var mask_server_B = document.getElementById("mask_server_b").value
var ip_asa_B_gi_1_2 = document.getElementById("ip_asa_B_gi_1_2").value
var mask_asa_B_gi_1_2 = document.getElementById("mask_asa_B_gi_1_2").value
var ip_pc_b = document.getElementById("ip_pc_b").value
var mask_pc_b = document.getElementById("mask_pc_b").value




if(router_ip_gi_0_1 == "" ||
        router_mask_gi_0_1 == "" ||
```

```
        router_ip_gi_0_2 == "" ||
        router_mask_gi_0_2 == "" ||

        ip_server_a == "" ||
        mask_server_a == "" ||
        ip_asa_A_gi_1_1 == "" ||
        mask_asa_A_gi_1_1 == "" ||
        ip_pc_a == "" ||
        mask_pc_a == "" ||
        ip_asa_A_gi_1_2 == "" ||
        mask_asa_A_gi_1_2 == "" ||

        ip_asa_B_gi_1_1 == "" ||
        mask_asa1_asa_A_gi_1_1 == "" ||
        ip_server_b == "" ||
        mask_server_b == "" ||
        ip_asa_B_gi_1_2 == "" ||
        mask_asa_B_gi_1_2 == "" ||
        ip_pc_b == "" ||
        mask_pc_b == ""){
alert("Ви заповнили не всі поля");
}else{


if(mask_asa_A_gi_1_1 == "255.0.0.0"){
        var netwrok = ip_asa_A_gi_1_1.split('.');
        var network_number_A = netwrok[0] + ".0.0.0";
}
if(mask_asa_A_gi_1_1 == "255.255.0.0"){
        var netwrok = ip_asa_A_gi_1_1.split('.');
        var network_number_A = netwrok[0] + "." + netwrok[1] + ".0.0";
}
if(mask_asa_A_gi_1_1 == "255.255.255.0"){
        var netwrok = ip_asa_A_gi_1_1.split('.');
        var network_number_A = netwrok[0] + "." + netwrok[1] + "." + netwrok[2] +".0";
}


if(mask_asa_B_gi_1_1 == "255.0.0.0"){
        var netwrok = ip_asa_B_gi_1_1.split('.');
        var network_number_B = netwrok[0] + ".0.0.0";
```

```
}
if(mask_asa_B_gi_1_1 == "255.255.0.0"){
        var netwrok = ip_asa_B_gi_1_1.split('.');
        var network_number_B = netwrok[0] + "." + netwrok[1] + ".0.0";
}
if(mask_asa_B_gi_1_1 == "255.255.255.0"){
        var netwrok = ip_asa_B_gi_1_1.split('.');
        var network_number_B = netwrok[0] + "." + netwrok[1] + "." + netwrok[2] +".0";
}




if (arrow==1){
        var access_list_FOR_A =
        "<br>access-list FOR-VPN extended permit udp " + network_number_A + " " + mask_asa_A_gi_1_1 +
" " + network_number_B + " " + mask_asa_B_gi_1_1 +
        "<br>access-list FOR-VPN extended permit tcp " + network_number_A + " " + mask_asa_A_gi_1_1 +
" " + network_number_B + " " + mask_asa_B_gi_1_1 +
        "<br>access-list FROM-VPN extended permit udp " + network_number_B + " " + mask_asa_B_gi_1_1
+ " " + network_number_A + " " + mask_asa_A_gi_1_1 +
        "<br>access-list FROM-VPN extended permit tcp " + network_number_B + " " + mask_asa_B_gi_1_1
+ " " + network_number_A + " " + mask_asa_A_gi_1_1;

        var access_list_FOR_B =
        "<br>access-list FOR-VPN extended permit udp " + network_number_B + " " + mask_asa_B_gi_1_1 +
" " + network_number_A + " " + mask_asa_A_gi_1_1 +
        "<br>access-list FOR-VPN extended permit tcp " + network_number_B + " " + mask_asa_B_gi_1_1 +
" " + network_number_A + " " + mask_asa_A_gi_1_1 +
        "<br>access-list FROM-VPN extended permit udp " + network_number_A + " " + mask_asa_A_gi_1_1
+ " " + network_number_B + " " + mask_asa_B_gi_1_1 +
        "<br>access-list FROM-VPN extended permit tcp " + network_number_A + " " + mask_asa_A_gi_1_1
+ " " + network_number_B + " " + mask_asa_B_gi_1_1;
}
else{
        var access_list_FOR_A=""
        var access_list_FOR_B=""
}
```

```
var Config_A = document.getElementById('output_config_A');
Config_A.innerHTML = "int gi1/2" +
"<br>nameif outside" +
"<br>ip address " + ip_asa_A_gi_1_1 +  " " + mask_asa_A_gi_1_1 +
"<br>security-level 100" +
"<br>no shutdown" +
"<br>exit" +
"<br>int gi1/1" +
"<br>nameif inside" +
"<br>security-level 0" +
"<br>ip address " + ip_asa_A_gi_1_2 + " " + mask_asa_A_gi_1_2 +
"<br>no shutdown" +
"<br>exit" +
"<br>route outside 0.0.0.0 0.0.0.0 " +  router_ip_gi_0_1 +
"<br>class-map inspection_default" +
"<br>match default-inspection-traffic" +
"<br>policy-map global_policy" +
"<br>class inspection_default" +
"<br>inspect icmp" +
"<br>ex" +
"<br>service-policy global_policy global" +
"<br>crypto ikev1 enable outside" +
"<br>crypto ikev1 policy 1" +
"<br>encryption 3des" +
"<br>hash md5" +
"<br>authentication pre-share" +
"<br>group 2" +
"<br>lifetime 43200" +
"<br>tunnel-group " + ip_asa_B_gi_1_2 + " type ipsec-l2l" +
"<br>tunnel-group " + ip_asa_B_gi_1_2 + " ipsec-attributes" +
"<br>ikev1 pre-shared-key cisco" +
"<br>crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac" +
"<br>access-list FOR-VPN extended permit icmp " + network_number_A + " " + mask_asa_A_gi_1_1 + " " +
network_number_B + " " + mask_asa_B_gi_1_1 +
access_list_FOR_A +
"<br>crypto map To-Site2 1 match address FOR-VPN"+
"<br>crypto map To-Site2 1 set peer " + ip_asa_B_gi_1_2 +
"<br>crypto map To-Site2 1 set security-association lifetime seconds 86400" +
"<br>crypto map To-Site2 1 set ikev1 transform-set TS" +
"<br>crypto map To-Site2 interface outside" +
```

```
"<br>access-list FROM-VPN extended permit icmp " + network_number_B + " " + mask_asa_B_gi_1_1 + " " +
network_number_A + " " + mask_asa_A_gi_1_1 +
"<br>access-group FROM-VPN out interface inside" +
"<br>write mem"



var Config_B = document.getElementById('output_config_B');
Config_B.innerHTML = "int gi1/2" +
"<br>nameif outside" +
"<br>ip address " + ip_asa_B_gi_1_1 +  " " + mask_asa_B_gi_1_1 +
"<br>security-level 100" +
"<br>no shutdown" +
"<br>exit" +
"<br>int gi1/1" +
"<br>nameif inside" +
"<br>security-level 0" +
"<br>ip address " + ip_asa_B_gi_1_2 + " " + mask_asa_B_gi_1_2 +
"<br>no shutdown" +
"<br>exit" +
"<br>route outside 0.0.0.0 0.0.0.0 " +  router_ip_gi_0_2 +
"<br>class-map inspection_default" +
"<br>match default-inspection-traffic" +
"<br>policy-map global_policy" +
"<br>class inspection_default" +
"<br>inspect icmp" +
"<br>ex" +
"<br>service-policy global_policy global" +
"<br>crypto ikev1 enable outside" +
"<br>crypto ikev1 policy 1" +
"<br>encryption 3des" +
"<br>hash md5" +
"<br>authentication pre-share" +
"<br>group 2" +
"<br>lifetime 43200" +
"<br>tunnel-group " + ip_asa_A_gi_1_2 + " type ipsec-l2l" +
"<br>tunnel-group " + ip_asa_A_gi_1_2 + " ipsec-attributes" +
"<br>ikev1 pre-shared-key cisco" +
"<br>crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac" +
"<br>access-list FOR-VPN extended permit icmp " + network_number_B + " " + mask_asa_B_gi_1_1 + " " +
network_number_A + " " + mask_asa_A_gi_1_1 +
```

```
access_list_FOR_B +
"<br>crypto map To-Site2 1 match address FOR-VPN"+
"<br>crypto map To-Site2 1 set peer " + ip_asa_A_gi_1_2 +
"<br>crypto map To-Site2 1 set security-association lifetime seconds 86400" +
"<br>crypto map To-Site2 1 set ikev1 transform-set TS" +
"<br>crypto map To-Site2 interface outside" +
"<br>access-list FROM-VPN extended permit icmp " + network_number_A + " " + mask_asa_A_gi_1_1 + " " +
network_number_B + " " + mask_asa_B_gi_1_1 +
"<br>access-group FROM-VPN out interface inside" +
"<br>write mem"

}

});


var arrow = 0

$(".arrow").click(function(){
        if(arrow == 1){
                $(".arrow").css("background","url(../Web/image/arrow_red.png)");
                arrow = 0;
        }else{
                $(".arrow").css("background","url(../Web/image/arrow_green.png)");
                arrow = 1;
        }

});



$(".button_default").click(function(){
        document.getElementById("router_ip_gi_0_1").value = "1.1.1.2";
        document.getElementById("router_mask_gi_0_1").value = "255.255.255.252";
        document.getElementById("router_ip_gi_0_2").value = "1.1.2.2";
        document.getElementById("router_mask_gi_0_2").value = "255.255.255.252";

        document.getElementById("ip_server_a").value = "192.168.1.2";
        document.getElementById("mask_server_a").value = "255.255.255.0";
        document.getElementById("ip_asa_A_gi_1_1").value = "192.168.1.1";
        document.getElementById("mask_asa_A_gi_1_1").value = "255.255.255.0";
```

```
        document.getElementById("ip_pc_a").value = "192.168.1.3";
        document.getElementById("mask_pc_a").value = "255.255.255.0";
        document.getElementById("ip_asa_A_gi_1_2").value = "1.1.1.1";
        document.getElementById("mask_asa_A_gi_1_2").value = "255.255.255.252";

        document.getElementById("ip_asa_B_gi_1_1").value = "192.168.2.1";
        document.getElementById("mask_asa1_asa_A_gi_1_1").value = "255.255.255.0";
        document.getElementById("ip_server_b").value = "192.168.2.2";
        document.getElementById("mask_server_b").value = "255.255.255.0";
        document.getElementById("ip_asa_B_gi_1_2").value = "1.1.2.1";
        document.getElementById("mask_asa_B_gi_1_2").value = "255.255.255.252";
        document.getElementById("ip_pc_b").value = "192.168.2.3";
        document.getElementById("mask_pc_b").value = "255.255.255.0";
});



$(".button_reset").click(function(){
        $(".arrow").css("background","url(../Web/image/arrow_red.png)");
        arrow=0


        document.getElementById("router_ip_gi_0_1").value = "";
        document.getElementById("router_mask_gi_0_1").value = "";
        document.getElementById("router_ip_gi_0_2").value = "";
        document.getElementById("router_mask_gi_0_2").value = "";

        document.getElementById("ip_server_a").value = "";
        document.getElementById("mask_server_a").value = "";
        document.getElementById("ip_asa_A_gi_1_1").value = "";
        document.getElementById("mask_asa_A_gi_1_1").value = "";
        document.getElementById("ip_pc_a").value = "";
        document.getElementById("mask_pc_a").value = "";
        document.getElementById("ip_asa_A_gi_1_2").value = "";
        document.getElementById("mask_asa_A_gi_1_2").value = "";

        document.getElementById("ip_asa_B_gi_1_1").value = "";
        document.getElementById("mask_asa1_asa_A_gi_1_1").value = "";
        document.getElementById("ip_server_b").value = "";
        document.getElementById("mask_server_b").value = "";
        document.getElementById("ip_asa_B_gi_1_2").value = "";
```

```
        document.getElementById("mask_asa_B_gi_1_2").value = "";
        document.getElementById("ip_pc_b").value = "";
        document.getElementById("mask_pc_b").value = "";

        var Config_A = document.getElementById('output_config_A');
        Config_A.innerHTML = "";
        var Config_B = document.getElementById('output_config_B');
        Config_B.innerHTML = "";
});
});
```

Додаток Д

Налаштування для ASA-A

```
enable
configure terminal
interface gigabitEthernet0/0
nameif outside
ip address 1.1.1.2 255.255.255.252
no shutdown
exit
interface gigabitEthernet0/1
nameif inside
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
route outside 0.0.0.0 0.0.0.0 1.1.1.1
class-map inspection_default
match default-inspection-traffic
exit
policy-map global_policy
class inspection_default
inspect icmp
service-policy global_policy global
crypto ikev1 enable outside
crypto ikev1 policy 1
encryption 3des
hash md5
authentication pre-share
group 2
lifetime 43200
tunnel-group 1.1.2.2 type ipsec-l2l
tunnel-group 1.1.2.2 ipsec-attributes
ikev1 pre-shared-key cisco
crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac
access-list FOR-VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
crypto map To-Site2 1 match address FOR-VPN
crypto map To-Site2 1 set peer 1.1.2.2
crypto map To-Site2 1 set security-association lifetime seconds 86400
crypto map To-Site2 1 set ikev1 transform-set TS
crypto map To-Site2 interface outside
access-list FROM-VPN extended permit icmp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
```

access-group FROM-VPN out interface inside

write mem

Налаштування для ASA-B

enable

configure terminal

interface gigabitEthernet0/0

nameif outside

ip address 1.1.2.2 255.255.255.252

no shutdown

exit

interface gigabitEthernet0/1

nameif inside

ip address 192.168.2.1 255.255.255.0

no shutdown

exit

route outside 0.0.0.0 0.0.0.0 1.1.2.1

class-map inspection_default

match default-inspection-traffic

exit

policy-map global_policy

class inspection_default

inspect icmp

service-policy global_policy global

crypto ikev1 enable outside

crypto ikev1 policy 1

encryption 3des

hash md5

authentication pre-share

group 2

lifetime 43200

tunnel-group 1.1.1.2 type ipsec-l2l

tunnel-group 1.1.1.2 ipsec-attributes

ikev1 pre-shared-key cisco

crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac

access-list FOR-VPN extended permit icmp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0

crypto map To-Site1 1 match address FOR-VPN

crypto map To-Site1 1 set peer 1.1.1.2

crypto map To-Site1 1 set security-association lifetime seconds 86400

crypto map To-Site1 1 set ikev1 transform-set TS

crypto map To-Site1 interface outside

```
access-list FROM-VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
access-group FROM-VPN out interface inside
write mem
```