МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

ІМ. І. СІКОРСЬКОГО”

ФАКУЛЬТЕТ ІНФОРМАТИКИ ТА ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

КАФЕДРА ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

ЛАБОРАТОРНА РОБОТА №6

З курсу

«Мобільні комп’ютерні мережі»

Виконав:

Терешкович Максим ІТ-02

Київ — 2023 р.

Мета роботи

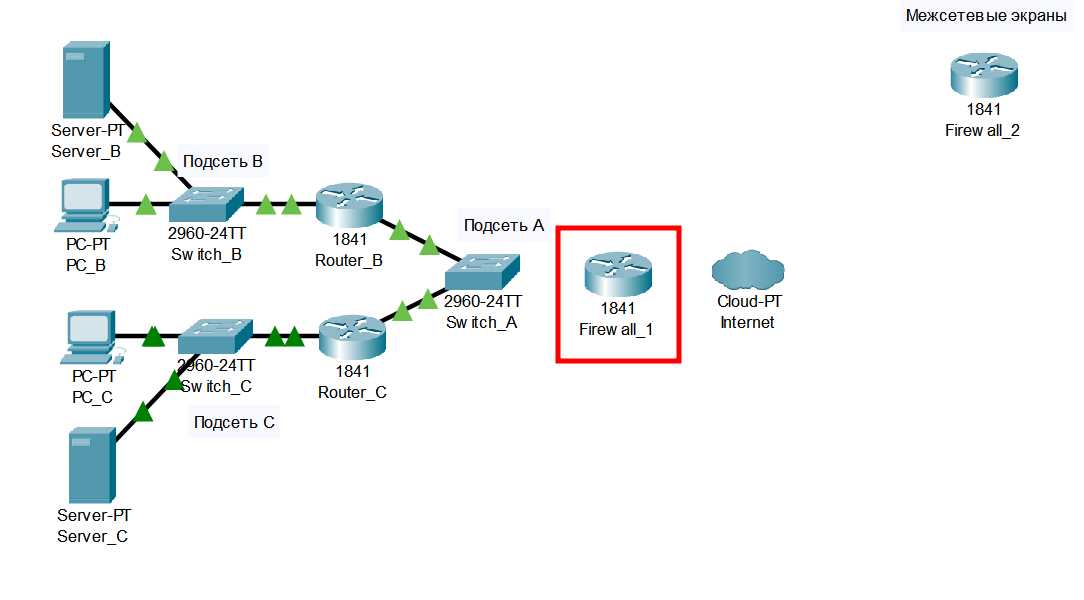
- Розміщення брандмауерів у відповідних місцях, що задовольняють вимогам безпеки.Вы являетесь техником, осуществляющим поддержку работы сети среднего предприятия.

У процесі зростання підприємства відкрито науково-дослідний відділ, який працює над новим, вельми секретним проектом. Існування проекту залежить від захисту даних, які використовує науково-дослідна група.

Ваше завдання - встановити міжмережеві екрани, щоб захистити мережу відповідно до конкретних вимог. Топологія службової програми Packet Tracer, яку потрібно використовувати, містить два попередньо налаштовані міжмережеві екрани. У двох запропонованих сценаріях ви замінюєте наявні маршрутизатори міжмережевими екранами. Міжмережеві екрани необхідно налаштувати, задавши відповідну конфігурацію IP-адрес, і протестувати, щоб переконатися, що вони правильно встановлені та налаштовані.

Сценарій 1. Захист мережі від хакерів.

#### 1) Крок 1. Заміна маршрутизатора Router\_A брандмауером Firewall\_1.

Демонтуйте маршрутизатор Router\_A і замініть його брандмауером Firewall\_1

Підключіть інтерфейс технології Fast Ethernet 0/0 брандмауера Firewall\_1 до інтерфейсу Fast Ethernet 0/1 комутатора Switch\_A. Підключіть інтерфейс Fast Ethernet 0/1 брандмауера Firewall\_1 до інтерфейсу Ethernet 6 хмари мережі ISP. (Використовуйте прямий кабель для обох з'єднань.)A diagram of a computer network

Description automatically generated

Підтвердіть ім'я мережевого вузла для Firewall\_1 - "Firewall\_1".A screenshot of a computer

Description automatically generated

На Firewall\_1 налаштуйте IP-адресу глобальної мережі та маску підмережі для інтерфейсу Fast Ethernet 0/1: 209.165.200.225 і 255.255.255.224, відповідно.

На брандмауері Firewall\_1 виберіть IP-адресу глобальної мережі та маску підмережі для інтерфейсу Fast Ethernet 0/1: 192.168.1.1 і 255.255.255.0.A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

#### 2) Крок 2. Перевірка конфігурації брандмауера Firewall\_1.

Для перевірки налаштування використовуйте команду show run. Нижче наводиться частина приблизного лістингу:A screenshot of a computer

Description automatically generated

З комп'ютера ПК\_B надішліть ехо-запит 209.165.200.225, щоб переконатися, що у внутрішнього комп'ютера є доступ до Інтернету.A screenshot of a computer program

Description automatically generated

У привілейованому режимі EXEC брандмауера Firewall\_1 збережіть поточну конфігурацію в початкову за допомогою команди copy run start.

A screenshot of a computer

Description automatically generated

Сценарій 2. Захист мережі відділу досліджень і розробок.

#### 1) Крок 1. Заміна маршрутизатора Router\_С брандмауером Firewall\_2.

Видаліть маршрутизатор Router\_C і замініть його брандмауером Firewall\_2.

Підключіть інтерфейс Fast Ethernet 0/1 брандмауера Firewall\_2 до інтерфейсу Fast Ethernet 0/3 комутатора Switch\_A. Підключіть інтерфейс Fast Ethernet 0/0 брандмауера Firewall\_2 до інтерфейсу Fast Ethernet 0/1 комутатора Switch\_C. (Використовуйте прямий кабель для обох з'єднань.)A diagram of a diagram

Description automatically generated

Підтвердіть ім'я мережевого вузла для Firewall\_2 - "Firewall\_2"A screenshot of a computer

Description automatically generated

На Firewall\_2 налаштуйте IP-адресу глобальної мережі та маску підмережі для інтерфейсу Fast Ethernet 0/1: 192.168.1.3 і 255.255.255.0, відповідно.

На брандмауері Firewall\_1 виберіть IP-адресу локальної мережі та маску підмережі для інтерфейсу FastEthernet 0/0: 192.168.3.1 і 255.255.255.0.A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

#### 2) Крок 2. Перевірка конфігурації брандмауера Firewall\_2.

Для перевірки налаштування використовуйте команду "show run". Далі представлено частину вихідних даних.A screenshot of a computer

Description automatically generated

За запитом команди на ПК\_B використовуйте команду ping, щоб переконатися, що комп'ютери в підмережі Subnet B не можуть отримати доступ до комп'ютерів у підмережі Subnet C.A screenshot of a computer program

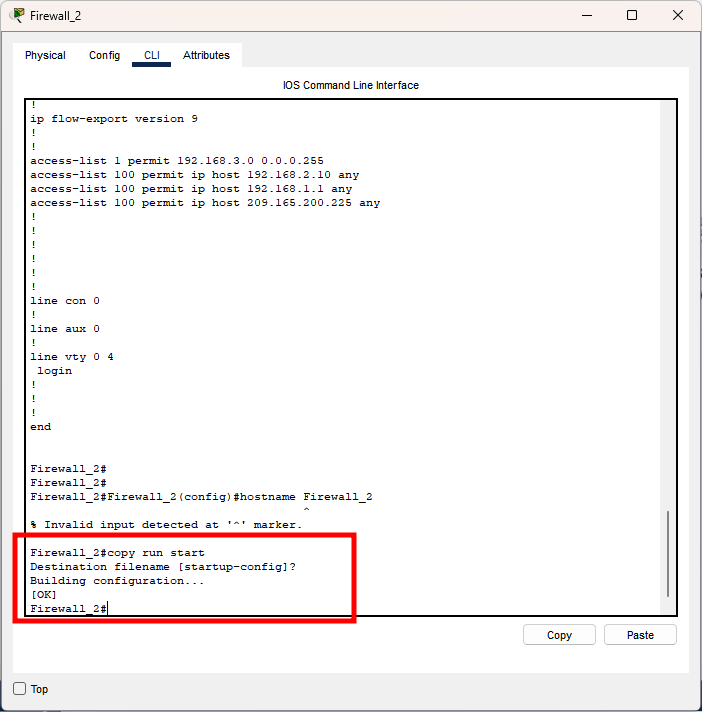
Description automatically generated

За запитом команди на ПК\_С використовуйте команду ping, щоб переконатися, що комп'ютери в підмережі Subnet С мають доступ до сервера в підмережі Subnet B.A computer screen shot of a black screen

Description automatically generated

За запитом команди на ПК\_С використовуйте команду ping, щоб переконатися, що комп'ютери в підмережі Subnet С мають доступ до Інтернету.A screenshot of a computer program

Description automatically generated

В привилегированном режиме EXEC брандмауэра Firewall\_2 сохраните текущую конфигурацию в начальную с помощью команды copy run start.

**Питання для роздумів:**

1. Навіщо потрібно встановлювати брандмауер у внутрішній мережі?

Встановлення брандмауера у внутрішній мережі забезпечує додатковий рівень безпеки за межами межі мережі, зокрема, в межах самої мережі. Це дає змогу контролювати та фільтрувати трафік між різними підмережами всередині організації. Брандмауер всередині мережі може запобігати небажаному доступу до певних ресурсів, контролювати обмін даними між підрозділами, фільтрувати шкідливий трафік і забезпечувати додатковий захист від внутрішніх загроз.

1. Яким чином маршрутизатор, налаштований для використання довідки NAT, дає змогу захистити комп'ютерні системи, розташовані всередині маршрутизатора NAT?

Маршрутизатор із налаштованим Network Address Translation (NAT) виконує перетворення IP-адрес і портів внутрішніх пристроїв перед надсиланням пакетів у зовнішню мережу. Це створює додатковий рівень анонімності для внутрішніх комп'ютерів, приховуючи їхні реальні IP-адреси від зовнішнього світу. Водночас, якщо зовнішній трафік спрямований на внутрішні пристрої, NAT переводить зовнішню адресу і порт назад у відповідну внутрішню адресу і порт.

Цей процес допомагає захистити комп'ютерні системи, оскільки зовнішній світ бачить тільки публічну IP-адресу маршрутизатора NAT, і не має прямого доступу до конкретних пристроїв усередині мережі. Це ускладнює завдання зловмисникам, які могли б спробувати проникнути в мережу через внутрішні пристрої.

1. Вивчіть розташування брандмауерів Firewall\_1 і Firewall\_2 у завершеній топології мережі. Які мережі можна вважати надійними та ненадійними для брандмауера Firewall\_1? Які мережі вважаються надійними та ненадійними для брандмауера Firewall\_2?Firewall\_1:

Надійні мережі: У даному контексті, можна вважати надійними мережі, підключені до інтерфейсу Fast Ethernet 0/0, оскільки цей інтерфейс має конфігурацію ip nat inside. Це найчастіше означає внутрішні мережі, захищені брандмауером.

Ненадійні мережі: Інтерфейс Fast Ethernet 0/1 налаштований як ip nat outside, що робить мережу, підключену до цього інтерфейсу, ненадійною. У цьому випадку, це з'єднання з провайдером Інтернету (ISP).

Firewall\_2:

Надійні мережі: Інтерфейс Fast Ethernet 0/0 налаштований як ip nat inside, що робить мережу, підключену до цього інтерфейсу, надійною. У цьому разі, це підмережа Subnet C.

Ненадійні мережі: Інтерфейс Fast Ethernet 0/1 налаштований як ip nat outside, що робить мережу, підключену до цього інтерфейсу, ненадійною. У цьому випадку, це підключення до підмережі Subnet B і далі до зовнішньої мережі.

Загалом, брандмауер Firewall\_1 захищає внутрішні мережі від ненадійної зовнішньої мережі, тоді як брандмауер Firewall\_2 захищає підмережу Subnet C від доступу з підмережі Subnet B і зовнішньої мережі.