МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний технічний університет

«Харківський політехнічний інститут»

Навчально-науковий інститут комп’ютерного моделювання, прикладної фізики та математики

Кафедра динаміки та міцності машин

Звіт

про виконання

лабораторної роботи № 7

по курсу «Комп’ютерні мережі та розподілені обчислювання»

з теми "Списки доступу ACL"

                                                    Виконав:

студент групи ІКМ-220Б

Пономаренко О.В.

Викладач:

доцент кафедри ДММ

Трубаєв О.І.

Харків 2022

**Завдання лабораторної роботи**

**Завдання №1.** Створення стандартного списку доступу

**Завдання №2.** Розширені списки доступу ACL

**Теоретичні відомості**

Списки доступу (access-lists) використовуються в цілому ряді випадків і є механізмом задання умов, які роутер перевіряє перед виконанням будь-яких дій. Маршрутизатор перевіряє кожен пакет і на підставі перерахованих вище критеріїв, зазначених в ACL, визначає, що потрібно зробити з пакетом, пропустити або відкинути. Типовими критеріями є адреси відправника і одержувача пакету, тип протоколу. Кожен критерій в списку доступу записується окремим рядком. Список доступу в цілому являє собою набір рядків з критеріями, що мають один і той же номер (або ім'я). Порядок завдання критеріїв в списку істотний. Перевірка пакету на відповідність списку проводиться послідовним застосуванням критеріїв з даного списку (у тому порядку, у якому вони були введені). Пакет, який не відповідає жодному з введених критеріїв буде відкинутий. Для кожного протоколу на інтерфейс може бути призначений тільки один список доступу. Як приклад нижче наведена таблиця списку управління досту-пом за замовчуванням:

**Без ACL** - за замовчуванням при створенні кінцевої точки їй все дозволено.

**Дозволити** - при додаванні одного або декількох діапазонів "дозволу" всі інші діапазони за замовчуванням забороняються. Тільки пакети з дозволеного діапазону IP-адрес зможуть досягти кінцевої точки віртуальної машини.

**Заборонити** - при додаванні одного або декількох діапазонів "заборонити" всі інші діапазони трафіку за замовчуванням дозволяються.

**Поєднання дозволу і заборони** - можна використовувати поєднання правил

"дозволити" і "заборонити", щоб вказати вкладений дозволений або заборонений діа-пазон IP-адрес. [1]

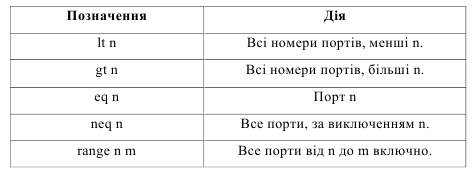
**Види ACL**

**Динамічний (Dynamic ACL)**

Дозволяє зробити наступне, наприклад, у вас є маршрутизатор, який підключений до якогось сервера і нам потрібно закрити доступ до нього із зовнішнього світу, але в той же час є кілька людей, які можуть підключатися до сервера.

Ми налаштовуємо динамічний список доступу, прикріплюємо його на вхідному напрямку, а далі людям, яким потрібно підключитися, підключатися через Telnet до цього пристрою, в результаті динамічний ACL відкриває прохід до сервера, і людина може зайти скажемо через HTTP потрапити на сервер. За промовчанням через 10 хвилин цей прохід закривається і користувач повинен ще раз виконати Telnet щоб підключитися до пристрою.

**Позначення портів у ACL:**



**Рефлексивний (Reflexive ACL)**

Тут ситуація трохи відрізняється, коли вузол у локальній мережі відправляє TCP запит в Інтернет, у нас повинен бути відкритий прохід, щоб прийшла TCP відповідь для встановлення з'єднання. Якщо проходу не буде — ми не зможемо встановити з'єднання, і цим проходом можуть скористатися зловмисники, наприклад проникнути в мережу. Рефлексивні ACL працюють таким чином, блокується повністю доступ (deny any) але формується ще один спеціальний ACL, який може читати параметри сесій, які згенеровані з локальної мережі і для них відкривати прохід в deny any, в результаті виходить що з Інтернету не зможуть встановити з'єднання. А на сесії згенеровані з локальної мережі надходитимуть відповіді.

**Обмеження часу (Time-based ACL)**

Звичайний ACL, але з обмеженням часу, ви можете ввести спеціальний розклад, який активує той чи інший запис списку доступу. І зробити такий фокус, наприклад пишемо список доступу, в якому забороняємо HTTP-доступ протягом робочого дня і вішаємо його на інтерфейс маршрутизатора, тобто, співробітники підприємства прийшли на роботу, їм закривається HTTP-доступ, робочий день закінчився, HTTP-доступ відкривається ,

будь ласка, якщо хочете – сидіть в Інтернеті. [2]

**Хід роботи**

**Завдання №1.**

Потрібно дозволити доступ на сервер PC1 з адресою 192.168.0.12, а PC0 з адре-

сою 192.168.0.11 - заборонити (рис. 1).

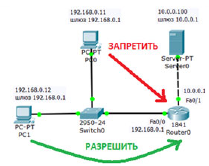


Рисунок 1 - Постановка задачі

Зберемо дану схему і налаштуємо її.

Інтерфейс 0/0 маршрутизатора 1841 налаштуємо на адресу 192.168.0.1 і включимо наступними командами (рис. 2):

*Router>en*

*Router#conf t*

*Router (config)#int fa0/0*

*Router (config-if)#ip addr 192.168.0.1 255.255.255.0*

*Router (config-if)#no shut*

*Router (config-if)#exit*

Другий інтерфейс маршрутизатора (порт 0/1) налаштуємо на адресу 10.0.0.1 і

так само включимо:

*Router (config)#intfa0/1*

*Router (config-if)#ip addr 10.0.0.1 255.255.255.0*

*Router (config-if)#no shut*



Рисунок 2 - налаштування роутера

Далі встановимо для сервера ip – 10.0.0.100, маску підмережі – 255.255.255.0 та шлюз – 10.0.0.1 (рис. 3)

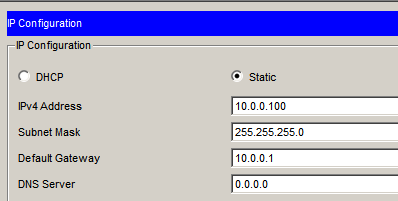


Рисунок 3 - налаштування сервера

Пробує пінганути наш сервер з комп’ютера (рис. 4)

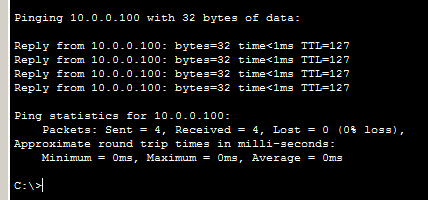


Рисунок 4 - пінг сервера

Можна побачити, що сервер повертає нам відповідь на наші запити, тож можна приступати до виконання самого завдання.

Відкриємо консоль роутера там встановимо доступ тільки для певного комп’ютера (192.168.0.12) (рис. 5)

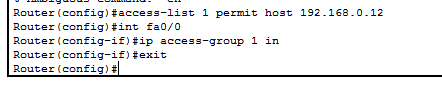


Рисунок 5 - обмеження доступу для певних комп'ютерів

Тепер спробуємо пінганути наш сервер знову, з обох комп’ютерів (рис. 6)

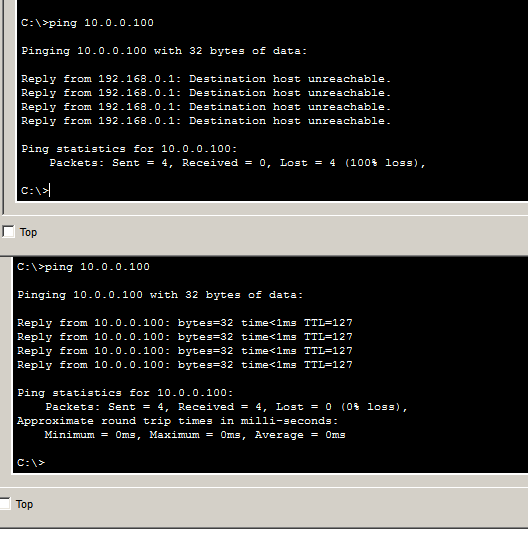


Рисунок 6 - фінальний пінг сервера

Як ми бачимо сервер повертає відповідь одному комп’ютеру, а заблокованому, роутер повертає такий результат, що досягнути сервера не можна.

**Завдання №2.**

Для другого завдання створимо таку мережу (рис. 7)

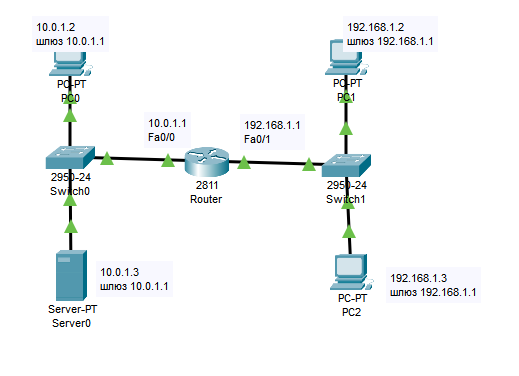


Рисунок 7 - схема мережі

Тут нам потрібно дозволити доступ до FTP сервера 10.0.1.3 для вузла 192.168.1.2 і заборонити для вузла 192.168.1.3.

Спочатку ми зробимо налаштування роутера для двох підмереж по типу, як ми це робили в 5 лабороторній роботі. (рис. 8)

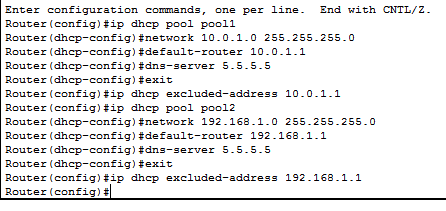


Рисунок 8 - конфігурація роутера

Далі нам потрібно додати дозволені та заборонені ip-адреси та порти до сервера через командну строку в роутері. (рис. 9)

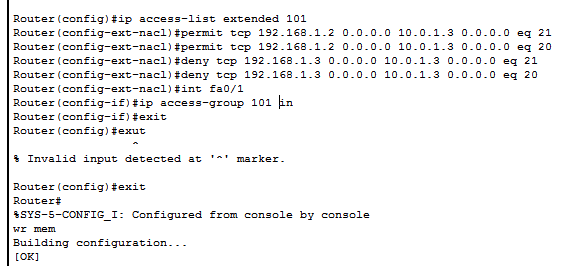


Рисунок 9 - налаштування списки дозволених портів

Тепер ми заблокували комп’ютер 192.168.1.3 на портах 20 та 21 (ftp), та дозволили доступ комп'ютеру 192.168.1.2 на тих самих портах. Спробуємо під'єднатися до сервера через ftp (рис. 10)

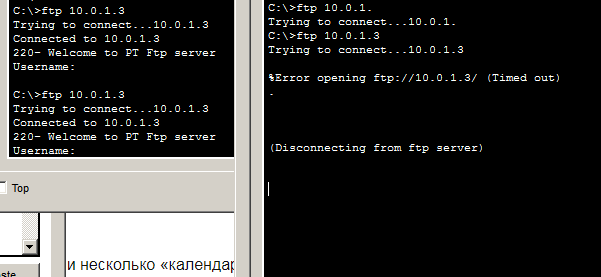


Рисунок 10 - під'єднання до сервера через ftp, з двох комп'ютерів

**Висновки**

Отже, виконуючи дану лабораторну роботу я навчився фільтрувати трафік у мережі за допомогою списків контролю доступу.

**Список джерел**

1. Комп’ютерний практикум № 7.
2. https://habr.com/ru/post/121806/