**Національний технічний університет України**

**«Київський політехнчний інститут імені Ігоря Сікорського»**

**Навчально-науковий інститут атомної та теплової енергетики**

**Кафедра цифрових технологій в енергетиці**

**Звіт**

**з лабораторної роботи №3**

**з дисципліни «Безпека інформаційних систем»**

Виконав:

студент групи ТР-23

Ровний Г.О.

КИЇВ - 2024

**Мета роботи:** лабораторна робота спрямована на набуття практичних навичок роботи в емуляторі Cisco Packet Tracer та дослідженні особливостей налаштування автентифікації ААА на маршрутизаторах Cisco.

**Поставлене завдання:**

1. Налаштування, застосування та перевірка розширеного нумерованого ACL.
2. Налаштування, застосування та перевірка розширеного іменованого ACL.

**Результат виконання роботи**

**СЦЕНАРІЙ 1**

**Налаштування розширеного нумерованого ACL.**

Крок 1. Налаштування ACL, щоб дозволити FTP і ICMP.

На R1 переходимо до режиму глобальної конфігурації та вводимо команду для визначення першого дійсного номеру для розширеного списку доступу та за допомогою команди permit дозволяємо FTP-трафік.

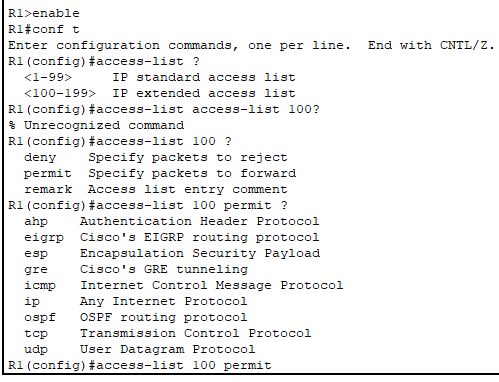


Рис.1. Дозвіл FTP-трафіку

Введемо додаткову команду # access-list 100 permit tcp ? яка дозволять уточнити довідку ACL.

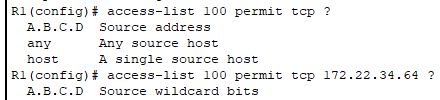


Рис.2. Дозвіл TCP для FTP

Обчислимо маску підстановки, яка буде визначати двійкову протилежність маски підмережі. Отриману маску підстановки додаємо до команди.

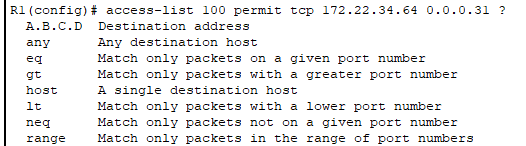


Рис.3. Додавання маски підстановки

Налаштовуємо адресу призначення. Додаємо ключове слово host та ip-адресу сервера.

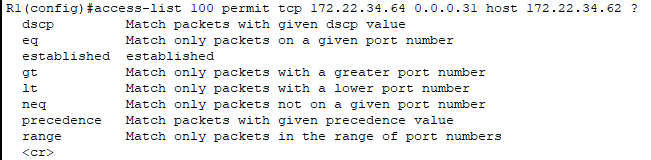


Рис.4. Налаштування адреси призначення сервера

Необхідно також додати ключове слово **eq та eq ftp ,** яке довзолить лише трафік FTP, обмеживши при цьому TCP.

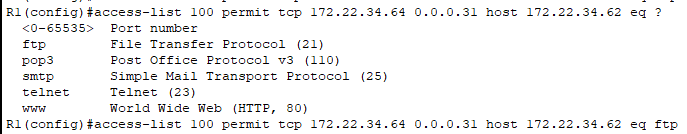


Рис.5. Обмеження TCP трафіку

Створимо другий оператор списку доступу, щоб дозволити трафік ICMP від PC1 до сервера.



Рис.6. Створення другого оператора списку доступу з ICMP трафіком

Крок 2. Застосування ACL до правильного інтерфейсу, щоб фільтрувати трафік.

Входимо у режим налаштування інтерфейсу за допомогою команди #interface gigabitEthernet 0/0 та застосовуємо ACL ( #ip access-group 100 in).



Рис.7. Застосування ACL для фільтрації трафіку

Крок 3: Перевірка реалізації ACL.

Проводимо пінгування з PC1 на сервер. Як бачимо все виконується.

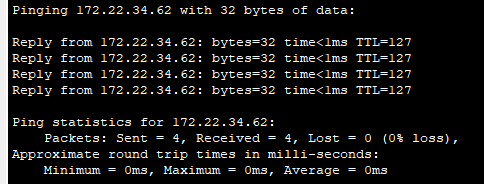


Рис.8. Пінгування з PC1 на Server

Проводимо FTP з PC1 на Server (пароль та username cisco).

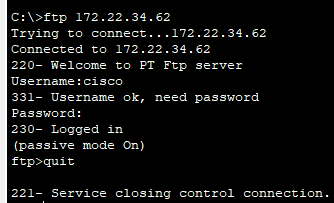


Рис.9. FTP з PC1 на Server

Проводимо пінгування з PC1 на PC2. Цільовий хост недоступний, оскільки трафік явно не дозволено.

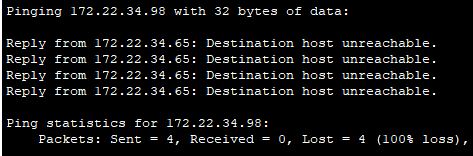


Рис.10. Пінгування з PC1 на PC2

**Налаштування, застосування, розширеного іменованого ACL.**

Крок 1. Налаштування ACL, щоб дозволити доступ HTTP та ICMP.

Входимо у режим глобальної конфігурації та налаштування іменованих ACL за допомогою команди #ip access-list ?



Рис.11. Режим налаштування іменованих ACl

Задаємо назву HTTP\_ONLY для cписку доступу іменованих ACL



Рис.12. Встановлюємо назву HTTP\_ONLY

У розширеному режимі налаштування ACL додаємо доступ TCP, додавши адресу мережі. Також обчислюємо маску підмережі яку потім необхідно ввести в команду.

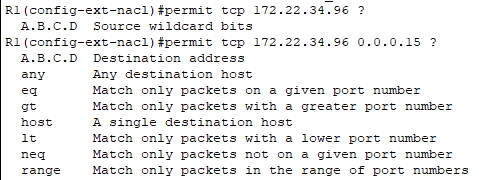


Рис.13. Додавання доступу TCP

Відфільтровуємо трафік www, ввівши адресу сервера. Після чого створюємо другий оператор списку, для того, щоб дозволити трафік ICMP від PC2 до сервера.



Рис.14. Фільтрування трафіку та встановлення дозволу на ICMP трафіку

Крок 2. Застосування ACL до правильного інтерфейсу, щоб фільтрувати трафік.

Входимо у режим налаштування інтерфейсу за допомогою команди #interface gigabitEthernet 0/1 та застосовуємо ACL ( #ip access-group HTTP\_ONLY in).



Рис.15. Застосування ACL для фільтрації трафіку

Крок 3. Перевірка реалізації ACL.

Проводимо пінгування з PC2 на сервер. Як бачимо, отримуємо всі відповіді.

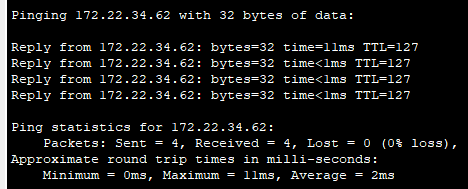


Рис.16. Пінгування з PC2 на Server

Проводимо FTP з PC2 на Server. З’єднання має бути невдалим.

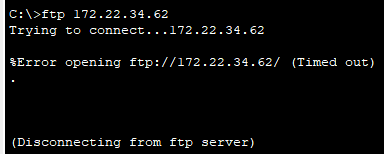


Рис.17. FTP з PC2 на Server

На PC2 відкриваємо веб браузер та вводимо IP-адресу як URL-адресу. Як результат – маємо успішне з’єднання.

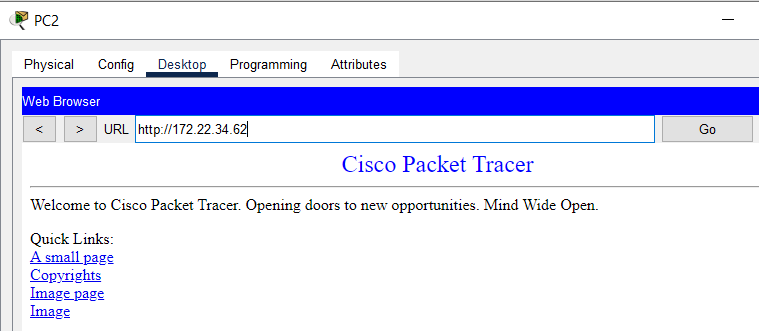


Рис.18. Встановлення з’єднання з IP-адресою у веб браузері PC2

**СЦЕНАРІЙ 2**

**Налаштування та перевірка розширеного нумерованого ACL.**

Крок 1. Налаштування розширеного ACL.

Перейдемо до режиму конфігурації на RTA (password: ciscoenpa55).



Рис.19. Режим налаштування розширеного ACl

У відповідному режимі конфігурації на RTA необхідно використовувати останній дійсний номер розширеного списку доступу, щоб налаштувати ACL. Для цього скористаємось командою **# access-list 199 permit tcp 10.101.117.32 0.0.0.15 10.101.117.0 0.0.0.31 eq 22**. Ця команда дозволяє TCP-з'єднання з вихідною мережею 10.101.117.32/28 до мережі призначення 10.101.117.0/27 на порті 22, який використовується для протоколу SSH.

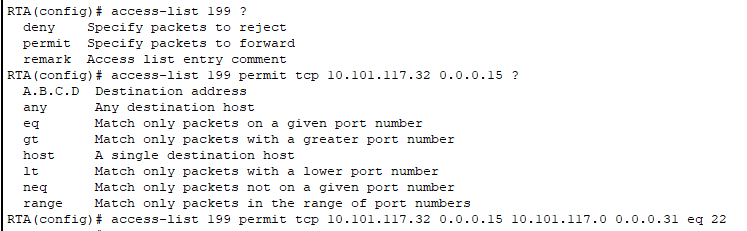


Рис.20. Налаштування першого оператора списку ACL

Другому оператору ACL надаємо дозвіл на весь ICMP-трафік не залежно від адреси відправника та призначення.



Рис.21. Дозвіл ICMP трафіку для другого оператора списку

Крок 2. Застосування розширеного ACL.

Входимо у режим налаштування інтерфейсу за допомогою команди #interface gigabitEthernet 0/2 та застосовуємо ACL (# ip access-group 199 out), який дозволить контролювати трафік від заданого інтерфейсу.

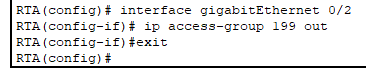


Рис.22. Застосування розширеного ACL для фільтрації трафіку

Крок 3. Перевірка реалізації розширеного ACL.

Пінг з PCB на всі інші IP-адреси в мережі.

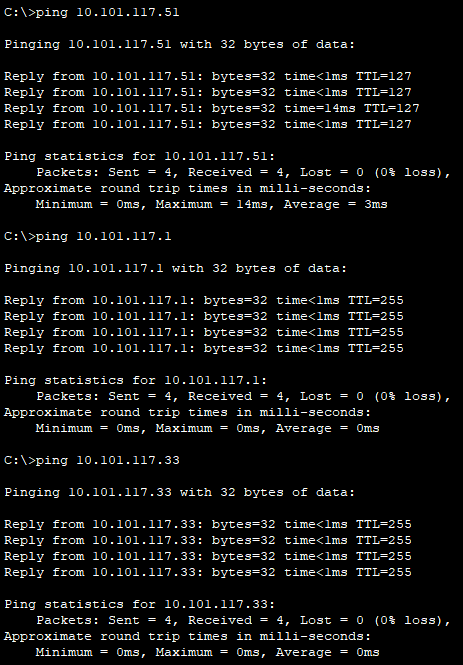


Рис.23. Пінг з PCB на всі інші IP-адреси мережі

SSH від PCB до SWC (password: Adminpa55).

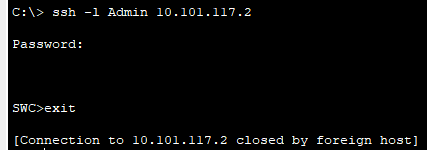


Рис.24. SSH від PCB до SWC

Пінг з PCA на всі інші IP-адреси в мережі.

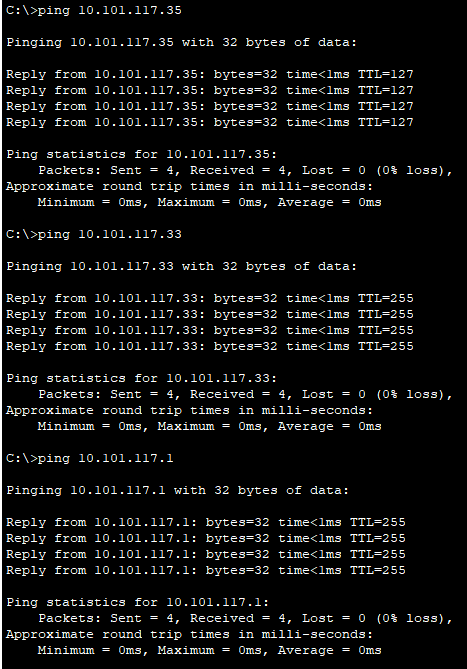


Рис.25. Пінг з PCA на всі інші IP-адреси мережі

SSH від PCA до SWC (маршутизатор відхиляє підключення).



Рис.26. SSH від PCA до SWC

SSH від PCA до SWB (password: Adminpa55).



Рис.27. SSH від PCA до SWB

SSH до SWC у привілейованому режимі EXEC.

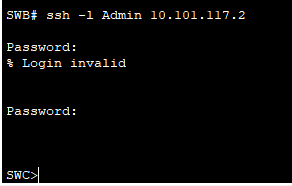


Рис.28. SSH до SWC у привілейованому режимі EXEC.

**Висновок:**

У результаті виконання лабораторної роботи було отримано практичні навички в емуляторі Cisco Packet Tracer з налаштування, застосування та перевірки роботи іменованого та розширеного Access Control List.