**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 №6**

**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 безпеки site-to-site IPsec VPN.

**Поставлене завдання:**

Перевірити з'єднання по всій мережі.

Налаштувати R1 для підтримки сайт-до-сайту IPsec VPN з R3.

**СЦЕНАРІЙ**

В топології мережі присутні три маршрутизатори. Необхідно налаштувати R1 і R3 для підтримки site-to-site IPsec VPN, коли трафік надсилається між їх відповідними LAN. Тунель IPsec VPN проходить від R1 до R3 через R2.

R2 виступає в ролі пропускного вузла і не містить інформації про VPN. IPsec забезпечує безпечну передачу конфіденційної інформації через незахищені мережі, такі як мережа Інтернет. IPsec працює на мережевому рівні і захищає та аутентифікує IP-пакети між вузлами-учасниками IPsec (однорангові пристрої), такими як маршрутизатори Cisco.

**Результат виконання роботи**

**ЧАСТИНА 1. НАЛАШТУВАННЯ ПАРАМЕТРІВ IPSEC НА R1.**

Крок 1. Перевірка з'єднання.

Виконаємо Ping з РС-А на РС-С. Як бачимо, з’єднання встановлено.

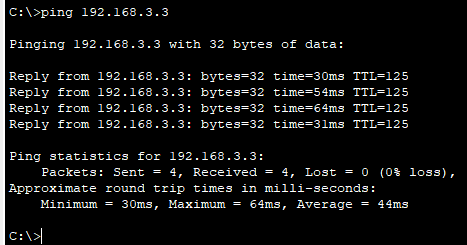


Рис.1. Ping з РС-А на РС-С

Крок 2. Увімкнення пакета технологій безпеки.

На R1 перевіримо чи увімкнена ліцензія пакету технологій безпеки.

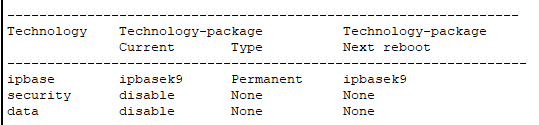


Рис.2. Перевірка увімкнення пакету технологій безпеки

Бачимо, що пакет не увімкнено. Переходимо до режиму глобальної нофігурації та скористаємось командою **R1(config)# license boot module c1900 technology-package securityk9.**

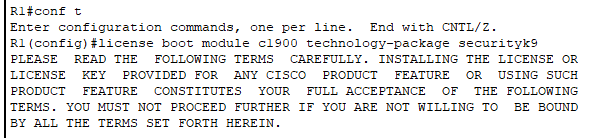
****

Рис.3. Увімкнення пакету технологій безпеки

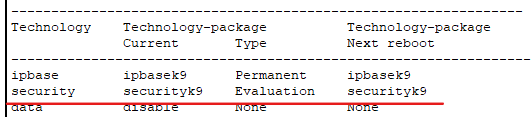
****

Рис.4. Перевірка увімкнення пакету технологій

Крок 3. Визначення цікавого трафіку на R1.

Налаштування ACL 110 для ідентифікації трафіку з LAN на R1 до LAN на R3 як цікавого. Цей цікавий трафік спричинить запуск IPsec VPN, коли є трафік між LAN R1 та R3. Весь інший трафік, що походить з LAN, не буде зашифрований. Через неявне заперечення всього, немає необхідності налаштовувати заперечення ip будь-якого будь-якого оператора.



Рис.5. Проведення визначення цікавого трафіку

Крок 4. Налаштування політики ISAKMP фази 1 IKE на R1.

Налаштуємо властивості політики crypto ISAKMP 10 на R1 разом з загальним криптографічним ключем vpnpa55. Для цього необхідно звернутися до таблиці ISAKMP фази 1 для конфігурації конкретних параметрів. Значення за замовчуванням налаштовувати не потрібно. Необхідно налаштувати тільки метод шифрування, метод обміну ключами та метод DH.

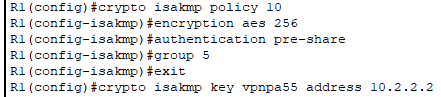


Рис.6. Налаштування політики ISAKMP

Крок 5. Налаштування політики IPsec фази 2 IKE на R1.

Створимо transform-set VPN-SET для використання esp-aes та esp-sha-hmac.



Рис.7. Створення transofm-set

А також створимо криптографічну мапу VPN-MAP, яка об'єднує всі параметри фази 2.

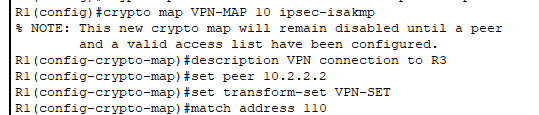


Рис.8. Створення криптографічної мапи VPN-MAP

Крок 6. Налаштування криптографічної мапи на вихідному інтерфейсі.

Прив'язуємо криптографічну мапу VPN-MAP до вихідного інтерфейсу Serial 0/0/0.



Рис.9. Налаштування криптографічної мапи на інтерфейсі

**ЧАСТИНА 2. НАЛАШТУВАННЯ ПАРАМЕТРІВ IPSEC НА R3.**

Крок 1. Увімкнути пакет технологій безпеки.

Аналогічно до R1, вмикаємо та перевіряємо увімкнення пакету технології безпеки **#license boot module c1900 technology-package securityk9**.

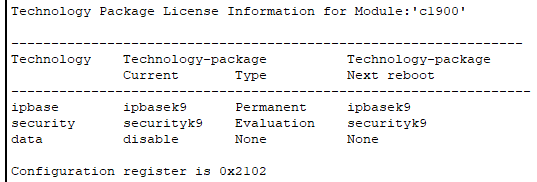


Рис.10. Увімкнення пакету технологій безпеки

Крок 2. Налаштувати маршрутизатор R3 для підтримки сайт-до-сайту VPN з R1.

Налаштуємо ACL 110, ідентифікуючи трафік з LAN на R3 до LAN на R1 як цікавий, аналогічно до R3.



Рис.11. Налаштування цікавого трафіку на R3

Крок 3. Налаштувати властивості ISAKMP фази 1 IKE на R3.

Налаштуємо властивості політики crypto ISAKMP 10 на R3 разом з загальним криптографічним ключем vpnpa55.

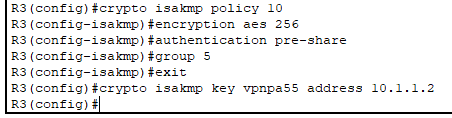


Рис.12. Налаштування властивості ISAKMP на R3

Крок 4. Налаштувати політику IPsec фази 2 IKE на R3.

Створимо transform-set VPN-SET для використання esp-aes та esp-sha-hmac.



Рис.13. Налаштування політики IPsec фази 2

А також створимо криптографічну мапу VPN-MAP, яка буде об'єднувати всі параметри фази 2. Використаємо номер послідовності 10 та ідентифікувати її як ipsec-isakmp мапу.

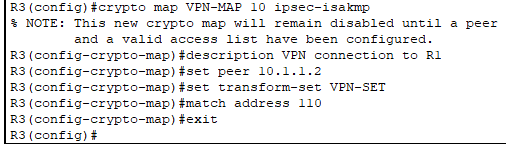


Рис.14. Створення криптографічної мапи VPN-MAP

Крок 5. Налаштувати криптографічну мапу на вихідному інтерфейсі.

Прив'язуємо криптографічну мапу VPN-MAP до вихідного інтерфейсу Serial 0/0/1.



Рис.15. Налаштування криптографічної мапи на інтерфейсі

**ЧАСТИНА 3. ПЕРЕВІРКА IPSEC VPN.**

Крок 1. Перевірити тунель перед цікавим трафіком.

Виконаємо команду **show crypto ipsec sa** на R1. Звернути увагу, що кількість пакетів, що обгортаються, шифруються, розшифровуються та розшифровуються, всі встановлені на 0.

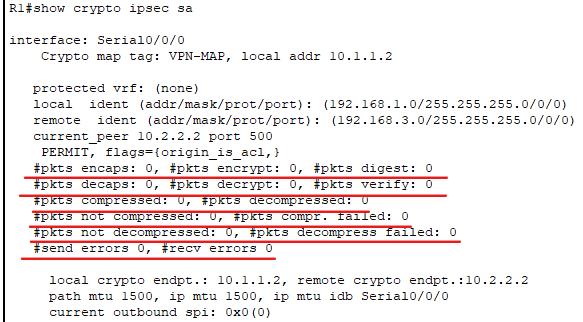


Рис.16. Перевірка тунелів перед цікавим трафіком

Крок 2. Створити цікавий трафік.

Для цього виконаємо Ping PC-C з PC-A.

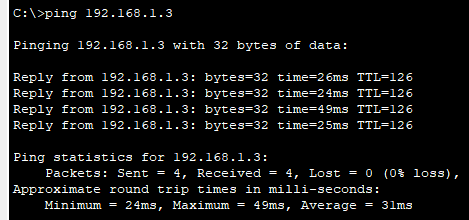


Рис.17. Ping PC-C з PC-A

Крок 3. Перевірити тунель після цікавого трафіку.

Повторно виконаємо команду show crypto ipsec sa. Звертаємо увагу, що кількість пакетів більше 0, що вказує на те, що тунель IPsec VPN працює.

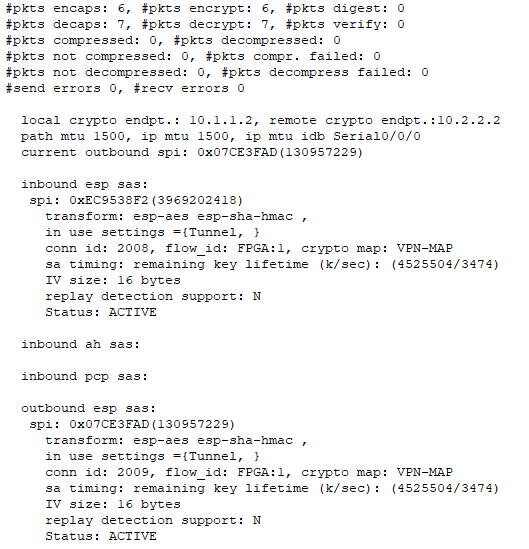


Рис.18. Перевірка тунелю після цікавого трафіку

Крок 4. Створити незацікавлений трафік.

Для цього виконаємо Ping PC-B з PC-A.

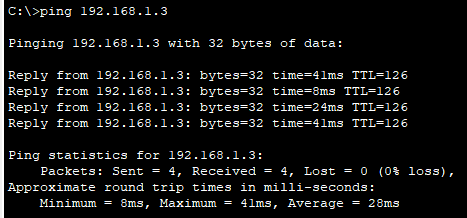


Рис.19. Ping PC-B з PC-A

Крок 5. Перевірити тунель.

Звертаємо увагу, що кількість пакетів не змінилася, що підтверджує, що незацікавлений трафік не зашифровано.

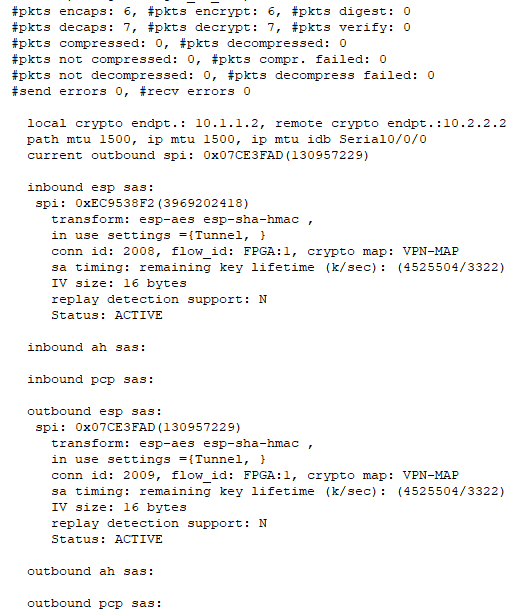


Рис.20. Повторна перевірка тунеля

Крок 6. Перевірка результатів.

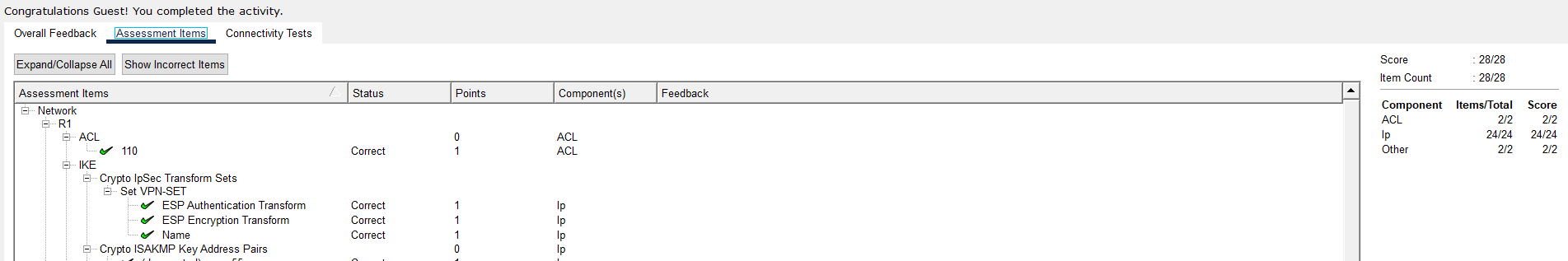


Рис.21. Перевірка результатів

**Висновок:**

У результаті виконання лабораторної роботи було досліджено особливості налаштування безпеки site-to-site IPsec VPN, а також було проведено налаштування параметрів IPSEC на R1 та R3 та виконано перевірку IPSEC VPN.