**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 №7**

**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 міжмережного екрана Cisco ASA 5505.

**Поставлене завдання:**

1. Перевірити з'єднання ASA;
2. Налаштувати базові конфігурації ASA та рівні безпеки інтерфейсу за допомогою CLI;
3. Налаштувати маршрутизацію, переклад адрес та політику інспекції за допомогою CLI;
4. Налаштувати DHCP, AAA та SSH;
5. Налаштувати DMZ, Static NAT та ACLs.

**СЦЕНАРІЙ**

Компанія має одне місце підключення до провайдера Інтернет. R1 представляє пристрій CPE, яким керує провайдер Інтернет. R2 представляє проміжний маршрутизатор Інтернет. R3 представляє провайдера Інтернет, який з'єднує адміністратора з компанії з управління мережами, якого найняли для віддаленого керування мережею.

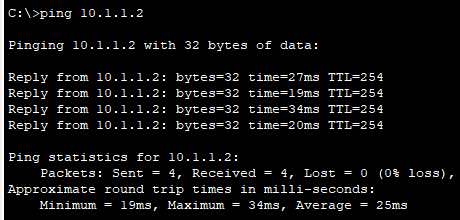
ASA є крайовим пристроєм безпеки CPE, який з'єднує внутрішню корпоративну мережу та DMZ з провайдером Інтернет, одночасно надаючи послуги NAT та DHCP внутрішнім хостам. ASA буде налаштовано для управління адміністратором внутрішньої мережі та віддаленим адміністратором. Провайдер Інтернет призначив публічний IP-діапазон 209.165.200.224/29, який буде використовуватися для перекладу адрес на ASA.

**Результат виконання роботи**

**ЧАСТИНА 1. ПЕРЕВІРКА З'ЄДНАННЯ ТА ДОСЛІДЖЕННЯ ASA**

**Крок 1. Перевірка з'єднання.**

Необхідно перевірити, чи PC-C може пінгувати будь-який інтерфейс маршрутизатора. PC-C не може пінгувати ASA, PC-B або сервер DMZ. Спробуємо пропінгувати R2 та сервер DMZ. Як бачимо, останній не виконується.



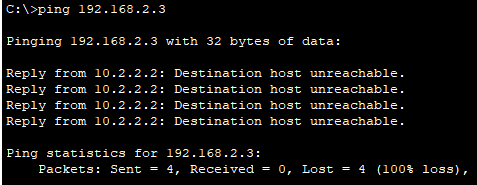


Рис.1. Перевірка з’єднання

**Крок 2. Визначити версію ASA, інтерфейси та ліцензію.**

Для цього використаємо команду show version.

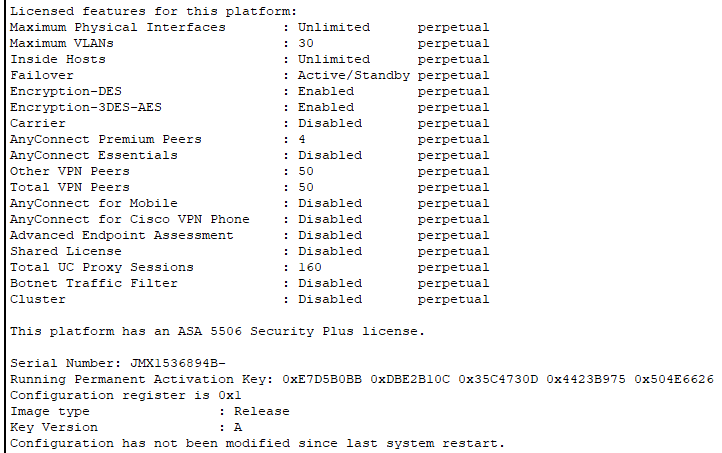


Рис.2. Визначення різних аспектів ASA

**Крок 3. Визначення файлової системи та вмісту флеш-пам'яті.**

У привілейованому режимі використаємо команди show file system та show flash для визначення файлової системи та вмісту флеш-пам’яті відповідно.

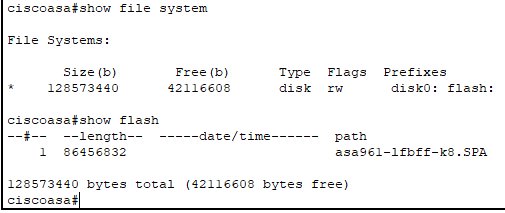


Рис.3. Визначення файлової системи та вмісту флеш-пам’яті

**ЧАСТИНА 2. НАЛАШТУВАННЯ НАЛАШТУВАНЬ ASA ТА БЕЗПЕКИ ІНТЕРФЕЙСУ ЗА ДОПОМОГОЮ CLI**

**Крок 1. Налаштувати імені хоста та доменного імені.**

Виконаємо команди hostname та domain-name у режимі глобальної конфігурації для застосування відповідних змін.



Рис.4. Налаштування імені хоста та домену

**Крок 2. Налаштувати пароль режиму enable.**

Щоб поставити пароль для режиму enable потрібно виконати #enable password ciscoenpa55.



Рис.5. Налаштування паролю для режиму enable

**Крок 3. Встановити дату та час.**



Рис.6. Установка дати та часу

**Крок 4. Налаштувати інтерфейси INSIDE та OUTSIDE.**

Створимо інтерфейс G1/1 для зовнішньої мережі (209.165.200.224/29), та встановимо найнижчий рівень безпеки 0 а також активуємо інтерфейс.

У іншому інтерфейсі G1/2 для внутрішньої мережі (192.168.1.0/24) робимо те саме, але вже встановлюємо найвищий рівень безпеки 100.

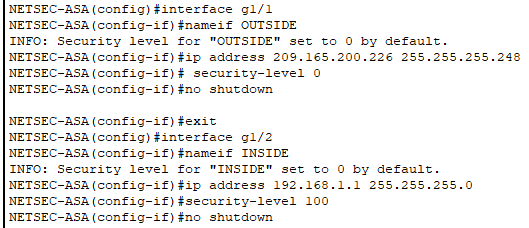
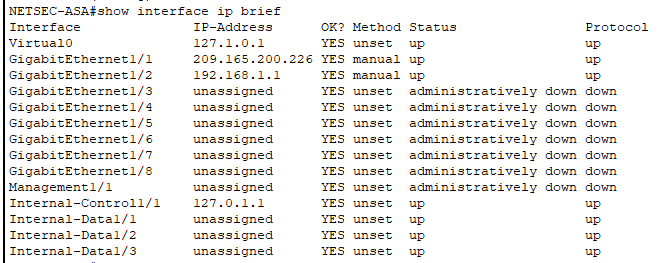


Рис.7. Налаштування інтерфейсів Inside та Outside

Після чого виконаємо перевірку конфігурації. Введемо спочатку команду **show interface ip brief**, щоб показати статус усіх інтерфейсів ASA. А потім **show ip address**, щоб показати інформацію про інтерфейс. Як бачимо – все налаштовано вірно.



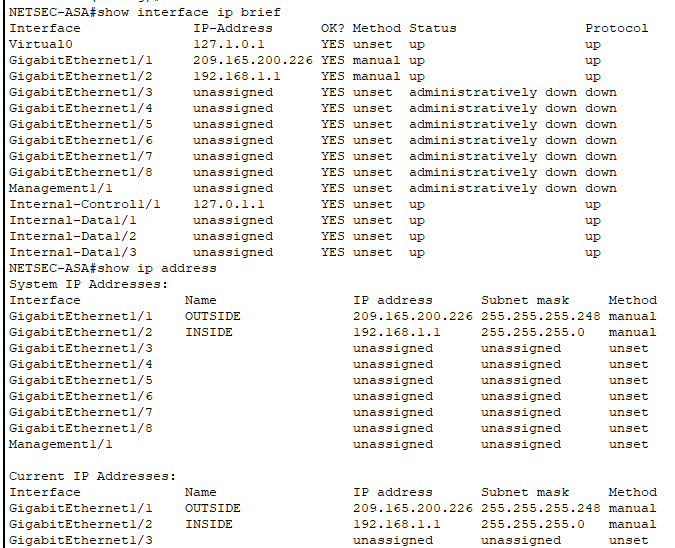
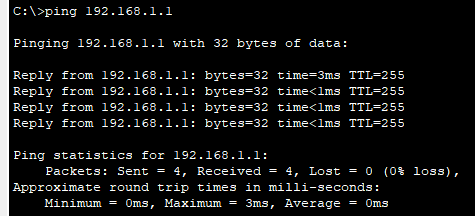


Рис.8. Перевірка конфігурації

**Крок 5. Перевірити з'єднання з ASA.**

Тут просто необхідно перевірити пінг з PC-B до внутрішньої адреси інтерфейсу ASA (192.168.1.1) (має бути успішно), а також здійснити пінг інтерфейс G1/1 (OUTSIDE) за IP-адресою 209.165.200.226 (спроба не повинна бути успішною).



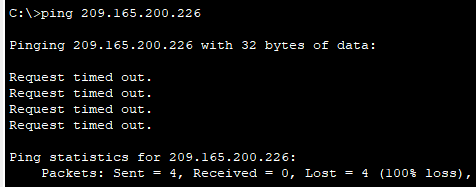


Рис.9. Перевірка з’єднання з ASA

**ЧАСТИНА 3. НАЛАШТУВАННЯ МАРШРУТИЗАЦІЇ, ПЕРЕКЛАДУ АДРЕС ТА ПОЛІТИКИ ПЕРЕВІРКИ ЗА ДОПОМОГОЮ CLI**

**Крок 1. Налаштувати статичний маршрут за замовчуванням для ASA.**

Створимо маршрут за замовчуванням «чотири нулі» за допомогою команди route, необхідно асоціювати його з інтерфейсом OUTSIDE ASA та вказати IP-адресу R1 G0/0 (209.165.200.225) як шлюз останнього вибору. А потім виконаємо перевірку статичного маршруту.

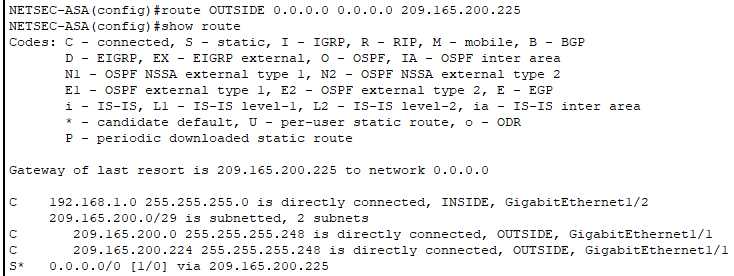


Рис.10. Створення статичного маршруту

Щоб впевнитись чи може ASA пінгувати IP-адресу R1 S0/0/0 10.1.1.1. виконаємо ping 10.1.1.1

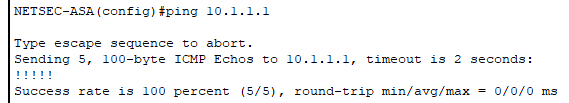


Рис.11. Перевірка ASA пінгуванням

**Крок 2. Налаштувати переклад адрес за допомогою PAT та мережевих об'єктів.**

Створимо мережевий об'єкт INSIDE-NET та призначимо йому атрибути, використовуючи команди subnet та nat.



Рис.12. Створеня мережевого об’єкту та призначення йому атрибутів

Показажемо конфігурацію NAT об'єкту за допомогою команди show run.

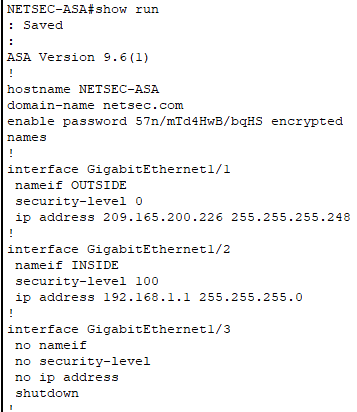


Рис.13. Конфігурація NAT-об’єкта

Тепер виконаємо пінг з PC-B інтерфейсу R1 G0/0 за IP-адресою 209.165.200.225. Пінги повинні бути невдалими.

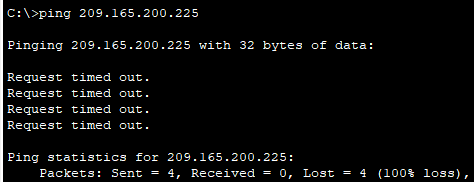


Рис.14. Пінг з PC-B інтрефейсу R1

Ввести команду show nat на ASA, щоб побачити перекладені та неперекладені складові.

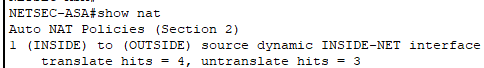


Рис.15. Показ перекладених та неперекладених складових

**ЧАСТИНА 4. НАЛАШТУВАННЯ DHCP, AAA ТА SSH**

**Крок 1. Налаштування ASA як сервера DHCP.**

Налаштуємо пул адрес DHCP та активувати його на інтерфейсі INSIDE ASA.



Рис.16. Налаштування пулу DHCP та його активація

Активувуємо службу DHCP у ASA для прослуховування запитів DHCP-клієнтів на активованому інтерфейсі (INSIDE).



Рис.17. Активація служби DHCP для прослуховування запитів

Увімкнемо DHCP на PC-B а після цього виконаємо ipconfig на PC-В для перевірки, чи отримує він інформацію про адресацію IP.

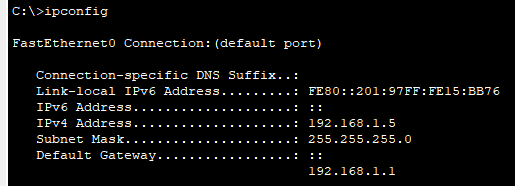


Рис.18. Перевірка інформації про адресацію на PC-B

**Крок 2. Налаштування AAA для використання локальної бази даних для аутентифікації.**

Визначимо локального користувача з ім'ям admin і налаштуємо AAA для використання локальної бази даних ASA для аутентифікації користувачів SSH.



Рис.19. Налаштування AAA для використання локальної БД

**Крок 3. Налаштування віддаленого доступу до ASA.**

Створимо пару ключів RSA, які потрібні для підтримки з'єднань SSH. Оскільки на пристрої ASA вже є ключі RSA, необхідно ввести no, коли запитують про їх заміну.

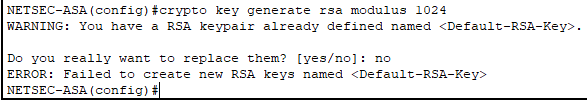


Рис.20. Створення ключів RSA

Налаштуємо ASA для дозволу з'єднань SSH від будь-якого хоста в мережі INSIDE (192.168.1.0/24) та від віддаленого хоста управління у філії (172.16.3.3) у мережі OUTSIDE. Встановити час очікування SSH на 10 хвилин (за замовчуванням 5 хвилин).



Рис.21. Налаштування дозволу з’єднань ssh в мережах INSIDE та OUTSIDE

Встановлюємо сеанс SSH з PC-C до ASA (209.165.200.226).

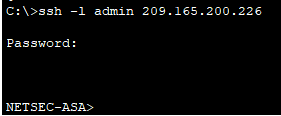


Рис.22. Встановлення сеансу з PC-C до ASA

Встановлюємо сеанс SSH з PC-B до ASA (192.168.1.1).

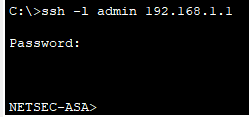


Рис.23. Встановлення сеансу з PC-B до ASA

**ЧАСТИНА 5. НАЛАШТУВАННЯ DMZ, СТАТИЧНОГО NAT ТА ACL**

**Крок 1. Налаштування інтерфейсу DMZ VLAN 3 на ASA.**

Налаштовуємо DMZ VLAN 3, де буде розташований веб-сервер з публічним доступом. Призначаємо йому IP-адресу 192.168.2.1/24, назвати його DMZ та призначити рівень безпеки 70. Оскільки серверу не потрібно ініціювати зв'язок з внутрішніми користувачами, вимкнути перенаправлення на інтерфейс VLAN 1.

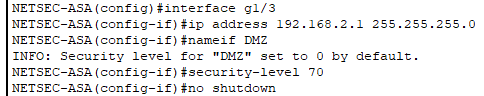


Рис.24. Налаштування DMZ VLAN 3

Для перевірки застосованих налаштувань виконуємо show interface ip brief та show ip address.

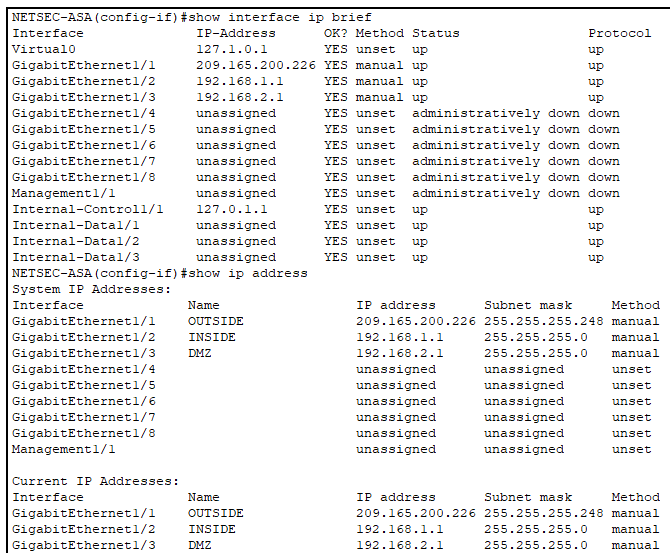


Рис.25. Перевірка налаштувань конфігурації

**Крок 2. Налаштування статичного NAT до сервера DMZ за допомогою мережевого об'єкта.**

Налаштовуємо мережевий об'єкт під назвою DMZ-SERVER та призначаємо йому статичну IP-адресу сервера DMZ (192.168.2.3). Також використаємо команду nat, щоб вказати, що цей об'єкт використовується для перекладу адреси DMZ на зовнішню адресу за допомогою статичного NAT, та вказати публічну перекладену адресу 209.165.200.227.



Рис.25. Налаштування статичного NAT до DMZ

**Крок 3. Налаштування ACL для дозволу доступу до сервера DMZ з Інтернет.**

Налаштовуємо названий список доступу OUTSIDE-DMZ, який дозволяє протокол TCP на порт 80 від будь-якого зовнішнього хоста до внутрішньої IP-адреси сервера DMZ. Застосовуємо список доступу до зовнішнього інтерфейсу ASA в напрямку «IN».





Рис.26. Налаштування ACL для дозволу доступу до сервера DMZ

**Крок 4. Перевірка доступу до сервера DMZ.**

З веб-браузера на PC-C переходимо до сервера DMZ (209.165.200.227).

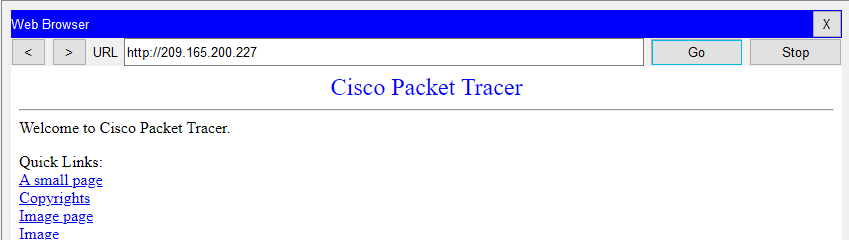


Рис.27. Перевірка доступу до сервера DMZ

**Висновок:**

У результаті виконання лабораторної роботи було набуто практичні навички в дослідженні особливостей налаштування міжмережевого екрана Cisco ASA 5505, а також було налаштовано базову конфігурацію ASA, рівні безпеки інтерфейсу; отримано навички роботи з DHCP, DMZ, Static NAT.