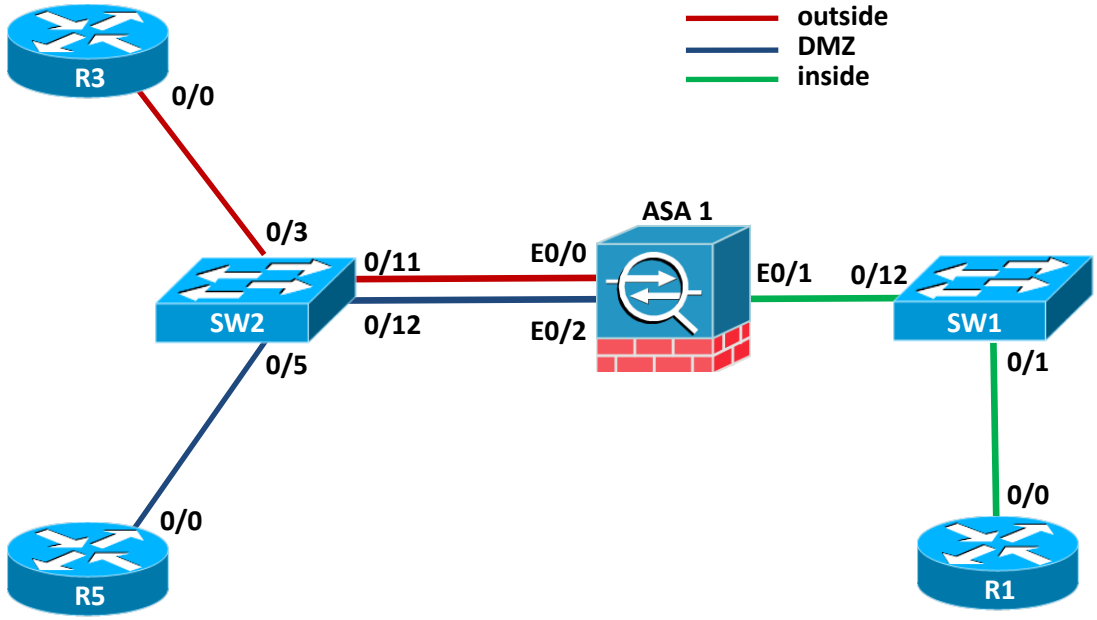
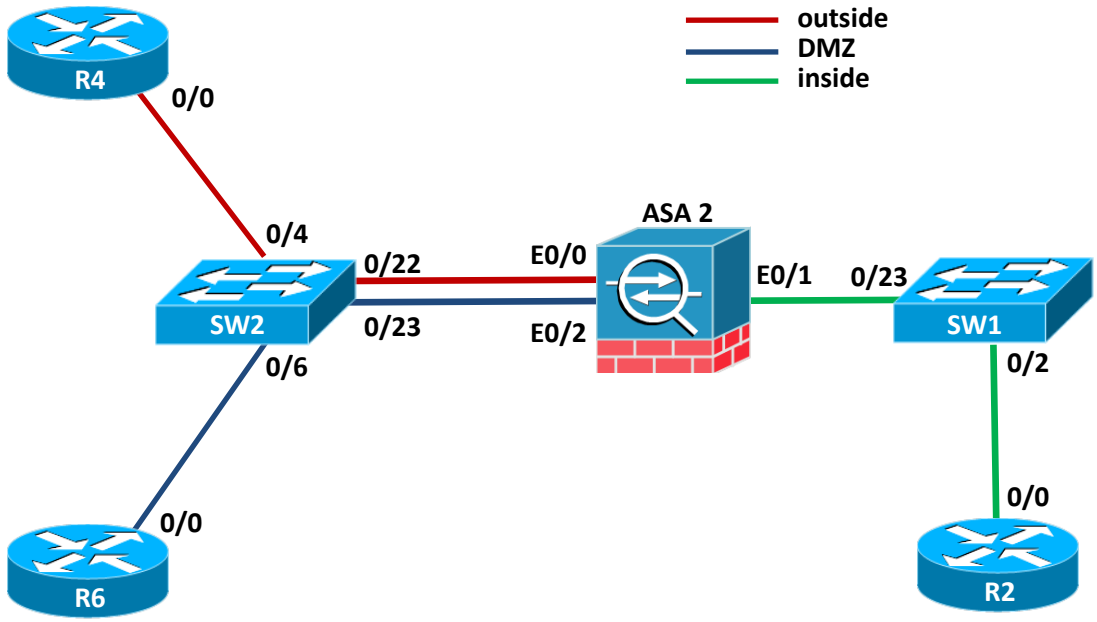
MSSR Cisco Lab 3 – NAT/ACL

1 Topologie





2 Obiective

În acest laborator studenții vor învăța să configureze scheme avansate de NAT pe ASA pentru a flexibiliza accesul la rețeaua DMZ și a ascunde IP-urile interne față de rețeaua externă. Se vor studia metode avansate de troubleshoot prin care se va simula flow-ul de pachete prin ASA pentru a determina problemele de conectivitate.

La finalul laboratorului, studenții vor avea următoarele competențe pe dispozitivele Cisco ASA:

- Configurarea Dynamic NAT pe ASA pentru a oferi acces la Internet rețelei DMZ
- Configurarea PAT pe ASA pentru a oferi acces la Internet rețelei interne
- Configurarea ASA pentru a filtra toate IP-urile private la ieșire în Internet
- Limitarea numărului de conexiuni TCP și UDP pentru translațiile configurate
- Eliminarea funcționalității de ISN randomization pentru translațiile configurate
- Configurarea Static PAT pentru a face posibilă contactarea serverele din DMZ
- Configurarea Outside NAT pentru a face conexiunile din Internet să apară cu IP-uri sursă din rețeaua locală
- Vizualizarea tabelelor de translații xlate
- Troubleshoot al proceselor NAT folosind packet tracer
- Configurarea ASA pentru a face posibilă comunicarea dintre DMZ și intern fără a trece prin NAT
- Configurarea ASA pentru a putea iniția conexiuni bidirecționale din DMZ către intern și din intern către DMZ

3 Taskuri

1. În cadrul acestui task studenții vor învăța cum să realizeze configurațiile de bază pe un echipament ASA

    a. Descărcați de pe cs.curs.pub.ro arhiva acces_echipamente_cisco.zip

    b. Dezarvați cele 3 fișiere .reg din interiorul arhivei și întrebați asistentul vostru cum să procedați în continuare

    c. Conectați-vă la echipamentele din topologia de mai sus funcție de distribuția realizată de asistent

2. În cadrul acestui task studenții vor realiza configurațiile necesare pentru a oferii acces la Internet rețelelor DMZ și LAN și a implementa în același timp scheme funcționale de NAT în rețea

    a. [2p]Configurați hostname-ul ASA-ului folosind prenumele vostru.

    b. [7p]Configurați rețeaua internă (interfața ASA și ruterul direct conectat) cu adrese din pool-ul de adrese private 192.168.1.0/24.

    c. [12p]Configurați rețeaua DMZ (interfața ASA și ruterul direct conectat) cu adrese din pool-ul de adrese private 10.10.10.0/24.

    d. [17p]Configurați rețeaua externă (interfața ASA și ruterul direct conectat) cu adrese din pool-ul de adrese publice 141.85.99.0/24

    e. [23p]Configurați dispozitivul ASA astfel încât următoarele tipuri de comunicații să fie posibile prin aceasta:

        i. Rețeaua internă să poată iniția conexiuni în DMZ și rețeaua externă

        ii. Rețeaua DMZ să poată iniția conexiuni în rețeaua externă, dar nu în rețeaua internă

        iii. Rețeaua externă să nu poată iniția conexiuni către DMZ sau către rețeaua internă

    f. [27p]Configurați ASA pentru ca firewall-ul să filtreze orice adrese private ce încearcă să părăsească rețeaua.

    g. [40p]Configurați rețeaua astfel încât rețeaua internă să poată accesa remote, prin telnet, ruterul din rețeaua externă. Toată rețeaua internă trebuie văzută în afară cu adresa publică alocată pe interfața outside a ASA și trebuie setați următorii parametrii la ieșirea din LAN:

        i. Conexiuni TCP: 1000

        ii. Conexiuni TCP embryonic: 100

        iii. Conexiuni UDP: 1000

    h. [45p]Testați configurația de la punctul g folosind telnet. Care este portul sursă folosit după translatare?

    i. [55p]Configurați rețeaua astfel încât rețeaua DMZ să poată da ping la ruterul din rețeaua externă. Toată rețeaua DMZ trebuie văzută în afară cu adrese din pool-ul public 99.85.77.0/24 și ISN-ul trebuie să nu fie randomizat de către ASA.

    j. [60p] Testați configurația (ping). Care este IP-ul global folosit de translația configurată?

3. În cadrul acestui task studenții vor realiza configurații avansate de NAT pentru a oferi acces la servicii în rețeaua DMZ.

    a. [65p]Rulați un server HTTP pe ruterul din DMZ. Se poate conecta ruterul din rețeaua internă la acest server?

    b. [70p]Identificați cauza lipsei de conectivitate folosind packet-tracer. Care este procesul care face DROP?

    c. [75p]Configurați rețeaua astfel încât să puteți accesa servicii HTTP din rețeaua internă în DMZ. Nu folosiți NAT-bypass. Testați rulând un server HTTP pe ruterul din DMZ (comanda **`ip http server`**).

    d. [80p]Configurați rețeaua astfel încât să puteți accesa servicii HTTP din rețeaua externă în DMZ.

    e. [85p]Configurați rețeaua astfel încât toate pachetele din Internet către serverul HTTP din DMZ să ajungă cu IP-uri sursă din rețeaua 10.10.10.0/24. Rulați comanda **`debug ip packet`** pe ruterul din DMZ pentru a verifica IP-ul sursă cu care vin pachetele.

4. În cadrul acestui task studenții vor realiza configurații avansate de NAT pentru a simplifica accesul din rețeaua internă în DMZ.

    a. Atenție: înainte de a configura taskurile de mai jos, chemați asistentul să vă corecteze deoarece veți invalida configurații anterioare.

    b. [90p]Configurați rețeaua astfel încât orice trafic între LAN și DMZ să nu fie trecut prin procesul de NAT. Folosiți Identity NAT (NAT Exemption are o problemă în versiunea de ASA OS instalată în laborator).

    c. [95p]Configurați rețeaua astfel încât să puteți inițiа conexiuni HTTP din DMZ în LAN fără a aplica un ACL nou pe o interfață. Consultați link-ul de mai jos pentru a realiza aceasta configurație

        - http://www.cisco.com/en/US/docs/security/asa/asa71/configuration/guide/intparam.html#wp1039276

    d. [100p]Folosiți comanda **`debug ip packet`** pentru a verifica adresa IP sursă care nu este translatată.