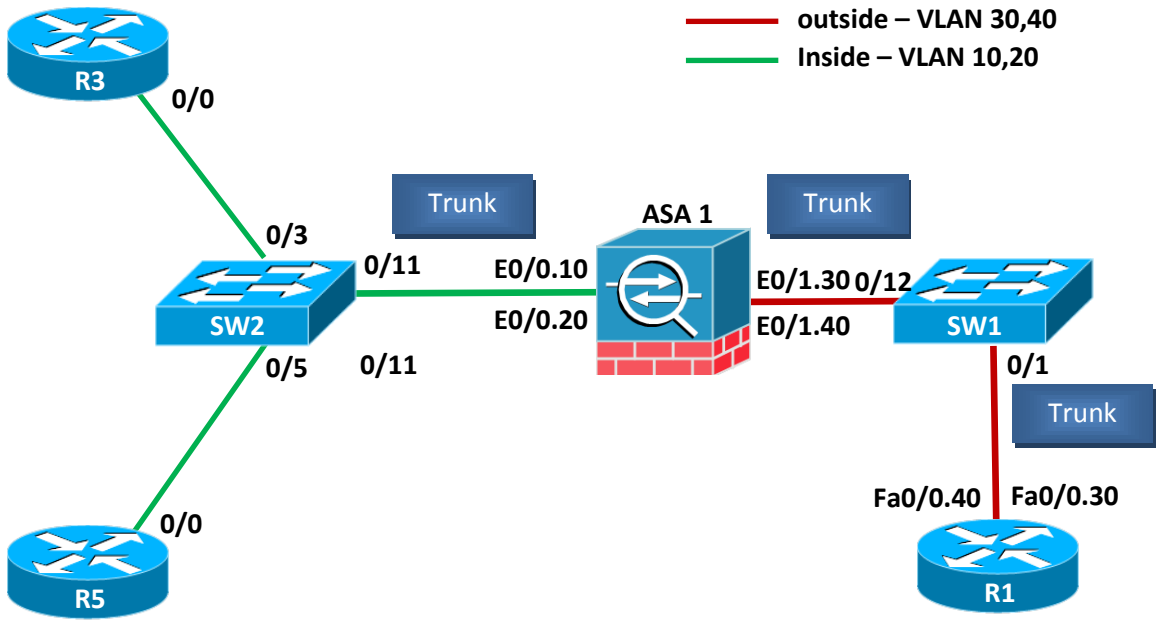
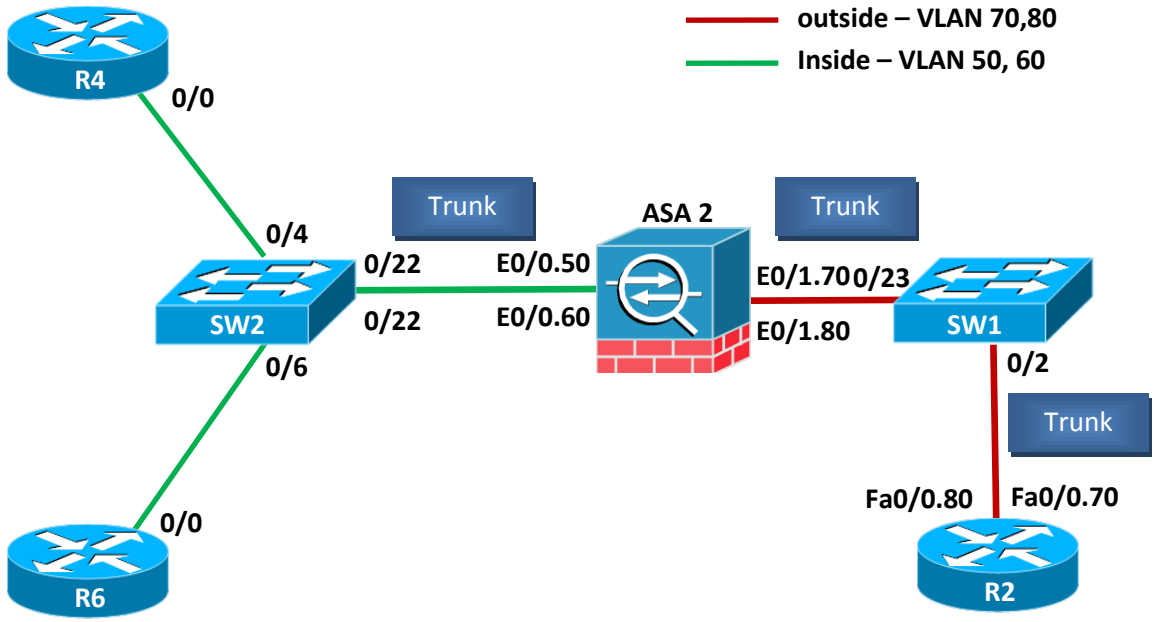
MSSR Cisco Lab 9 – Transparent firewalling și contexte de securitate

1 Topologie





2 Obiective

În acest laborator studenții vor învăța să configureze ASA în modul transparent în cadrul unei implementări de ASA multiple-context.

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

- Configurarea ASA din single-mode în multiple-mode
- Configurarea ASA în modul transparent
- Crearea contextelor de securitate din System Execution Space
- Asocierea interfețelor cu contextele de securitate create
- Specificarea fișierelor de configurare pentru fiecare context
- Implementarea unei topologii cu acces la Internet pentru două context diferite folosind subinterfețe mapate pe VLAN-uri
- Configurarea parametrilor de L2 din modul transparent

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 învăță să configureze ASA activând mai multe contexte și realizând comunicarea între acestea folosind subinterfețe de tip VLAN și un ruter extern ce realizează Inter-VLAN Routing.

    a. Dacă ASA are configurații ce nu sunt implicite, folosiți comanda **clear configure all** pentru a șterge memoria RAM a ASA.

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

    c. [5p]Configurați ASA în modul **transparent**. Folosiți comanda **sh firewall** pentru a verifica modul de funcționare.

d. [7p]Configurați ASA în modul **multiple.** După ce ASA rebootează dați comanda **sh run** și analizați schimările**.**

e. [15p]Configurați 2 subinterfețe pe interfața fizica E0/0 a ASA pe care configurați următoarele VLAN-uri

    i. Dacă sunteți pe **topologia de sus:**

        1. E0/0.10 – VLAN 10
        2. E0/0.20 – VLAN 20

    ii. Dacă sunteți pe **topologia de jos**:

        1. E0/0.50 – VLAN 50
        2. E0/0.60 – VLAN 60

f. [20p]Configurați 2 subinterfețe pe interfața fizica E0/1 a ASA pe care configurați următoarele VLAN-uri

    i. Dacă sunteți pe **topologia de sus**

        1. E0/1.30 – VLAN 30
        2. E0/1.40 – VLAN 40

    ii. Dacă sunteți pe **topologia de jos**

        1. E0/1.70 – VLAN 70
        2. E0/1.80 – VLAN 80

g. [30p]Configurați 2 contexte pe ASA după următoarea configurație:

<u>Topologia de sus</u>

    i. Contextul Pitesti

        1. Nume: Pitesti
        2. Interfețe alocate: E0/0.10, E0/1.30
        3. Config-url: disk0:/Pitesti.cfg

    ii. Contextul Galati

        1. Nume: Galati
        2. Interfețe alocate: E0/0.20, E0/1.40

3. Config-url: disk0:/Galati.cfg

<u>Topologia de jos</u>

i. Contextul Pitesti

4. Nume: Pitesti
5. Interfețe alocate: E0/0.50, E0/1.70
6. Config-url: disk0:/Pitesti.cfg

ii. Contextul Galati

7. Nume: Galati
8. Interfețe alocate: E0/0.60, E0/1.80
9. Config-url: disk0:/Galati.cfg

h. [40p]Intrați în fiecare context și configurați adrese IP și nume pe subinterfețele configurate urmărind schema de mai jos

i. Topologia de sus

1. E0/0.10 cu numele inside
2. E0/0.20 cu numele inside
3. E0/1.30 cu numele outside
4. E0/1.40 cu numele outside

ii. Topologia de jos

1. E0/0.50 cu numele inside
2. E0/0.60 cu numele inside
3. E0/1.70 cu numele outside
4. E0/1.80 cu numele outside

i. [50p]Configurați adrese pe ruterele Inside după schema de mai jos:

1. Ruterul R3/R4: 192.168.10.100/24

   Ruterul R5/R6: 192.168.20.100/24

j. [60p]Configurați ruterul din Outside cu următorii parametrii:

i. **Topologia de sus**

1. Fa0/0.30 – VLAN = 30, IP = 192.168.10.1/24

   Fa0/0.40 – VLAN = 40, IP = 192.168.20.1/24

ii. **Topologia de jos**

1. Fa0/0.70 – VLAN = 70, IP = 192.168.10.1/24
2. Fa0/0.80 – VLAN = 80, IP = 192.168.20.1/24

k. [65p]Testați comunicarea între ruterele din Inside și ruterul din Outside folosind telnet

3. În cadrul acestui task studenții vor modifica parametrii de L2 din configurația de transparent firewall și vor testa capabilitățile de filtrare a ASA în acest mod.

   a. [70p]Vizualizați tabela CAM a ASA folosind comanda **sh mac-address-table.**

   b. [73p]Configurați aging-time-ul tabelei CAM la 20 de minute.

   c. [75p]Configurați intrări statice în tabela CAM a ASA pentru ruterele din inside. Folosiți comanda **mac-address-table static**.

   d. [80p]Dezactivați învățarea de adrese MAC pe interfețele inside din fiecare context folosind comanda **mac-learn.**

   e. [83p]Acum că firewall-ul este în modul Layer 2, puteți folosi CDP pentru a vedea un ruter vecin de pe un altul? Încercați comanda **sh cdp neighbors** pentru a verifica acest lucru.

   f. [90p]Implicit ASA blochează CDP-ul în modul transparent. Încercați să configurați o listă de acces de tip ethertype care să permită CDP și să o aplicați pe interfața de outside și inside dintr-un context. A avut vreun efect?

   g. [95p]Se poate configura un ACL în modul transparent care să blocheze ARP? Încercați.

   h. [100p]Se poate configura un ACL care să blocheze trafic TCP? Încercați.

   i. Înainte să vă ridicați de la laborator, treceți ASA înapoi în modul single și ștergeți configurațiile de pe celelalte echipamente.