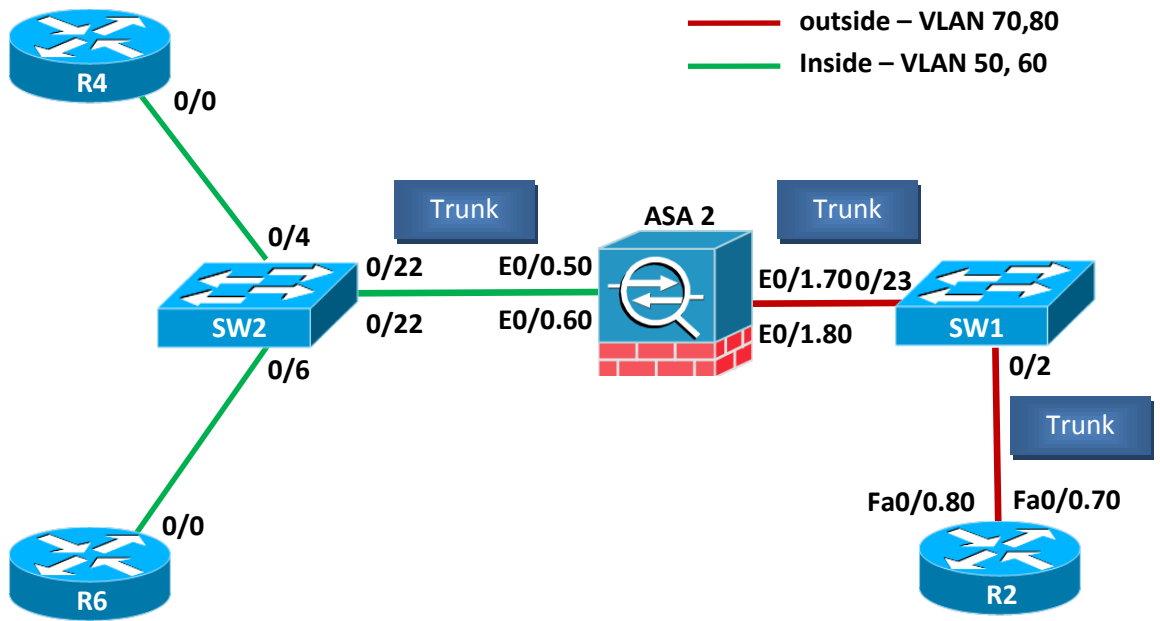
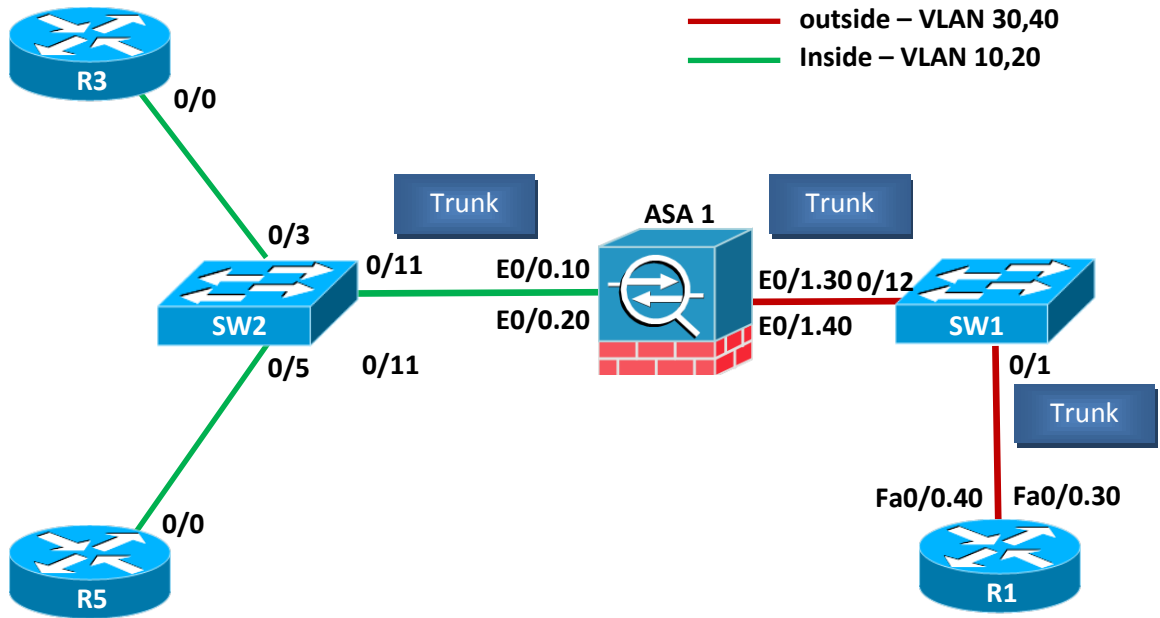


# MSSR Cisco Lab 6 – Contexte de securitate

## 1 Topologie



## 2 Obiective

În acest laborator studenții vor învăța să configureze ASA în modul „multiple”, activând contexte de securitate. În parcurgerea taskurilor se va urmări diferențierea clară între System Execution Space, Admin Context și customer context și se vor implementa topologii de comunicare între contexte de securitate.

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

- Configurarea ASA din single-mode în multiple-mode
- 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
- Implementarea politicilor de NAT pentru contexte diferite
- Implementarea politicilor de inspecție pentru contexte diferite

## 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](http://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 învăța 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 implicate, folosiți comanda **clear configure all** pentru a șterge memoria RAM a ASA.
  - b. [2p]Configurați hostname-ul ASA-ului folosind prenumele vostru.

- c. [7p]Configurați ASA în modul **multiple**. După ce ASA rebootează dați comanda **sh run** și analizați schimările.
- d. [15p]Configurați 2 subinterfețe pe interfața fizică 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
- e. [20p]Configurați 2 subinterfețe pe interfața fizică 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
- f. [30p]Configurați 2 contexte pe ASA după următoarea configurație:

**Topologia de sus**

- 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

**Topologia de jos**

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

g. [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 și adresa 192.168.10.1/24

2. E0/0.20 cu numele inside și adresa 192.168.20.1/24

3. E0/1.30 cu numele outside și adresa 141.85.30.1/24

4. E0/1.40 cu numele outside și adresa 141.85.40.1/24

**ii. Topologia de jos**

1. E0/0.50 cu numele inside și adresa 192.168.10.1/24

2. E0/0.60 cu numele inside și adresa 192.168.20.1/24

3. E0/1.70 cu numele outside și adresa 141.85.30.1/24

4. E0/1.80 cu numele outside și adresa 141.85.40.1/24

h. [50p]Configurați adrese IP și rute default pe ruterele Inside după schema de mai jos:

1. Ruterul R3/R4: 192.168.10.100/24 și rută default către 192.168.10.1

2. Ruterul R5/R6: 192.168.20.100/24 și rută default către 192.168.20.1

- i. [60p] Configurați ruterul din Outside cu următorii parametri:
- i. **Topologia de sus**
    1. Fa0/0.30 – VLAN = 30, IP = 141.85.30.100 și rută default către 141.85.30.1
    2. Fa0/0.40 – VLAN = 40, IP = 141.85.40.100 și rută default către 141.85.40.1
  - ii. **Topologia de jos**
    1. Fa0/0.70 – VLAN = 70, IP = 141.85.30.100 și rută default către 141.85.30.1
    2. Fa0/0.80 – VLAN = 80, IP = 141.85.40.100 și rută default către 141.85.40.1
- j. [65p] Testați comunicarea între ruterele din Inside și ruterul din Outside folosind telnet
3. În cadrul acestui task studenții vor implementa politici diferite de acces pentru fiecare context creat. În cele ce urmează vor trebui implementate următoarele politici pentru fiecare context:
- a. [75p] Toți utilizatorii din contextul Pitești ar trebui să poată realiza trafic ICMP către exterior. Configurați o politică pe interfața inside astfel încât să inspectați ICMP.
  - b. [80p] Toate adresele sursă din contextul Pitesti ar trebui să fie translatate la adresa de pe interfața outside folosind PAT.
  - c. [85p] Pe ruterul din contextul Pitesti (R3/R4) va rula un server HTTP. Configurați contextul astfel încât ruterul din Outside să se poată conecta la acest server. Porniți serverul HTTP folosind comanda **ip http server**.
  - d. [90p] Toți utilizatorii din contextul Galati nu trebuie să facă decât trafic HTTP către exterior.
  - e. [100p] Toate adresele sursa din contextul Galati ar trebui să fie translatate la adresa 141.85.40.101 folosind PAT.
  - f. Înainte să vă ridicați de la laborator, treceți ASA înapoi în modul single și ștergeți configurațiile de pe celelalte echipamente.