



UNIUNEA EUROPEANĂ



GUVERNUL ROMÂNIEI



Instrumente Structurale  
2007-2013



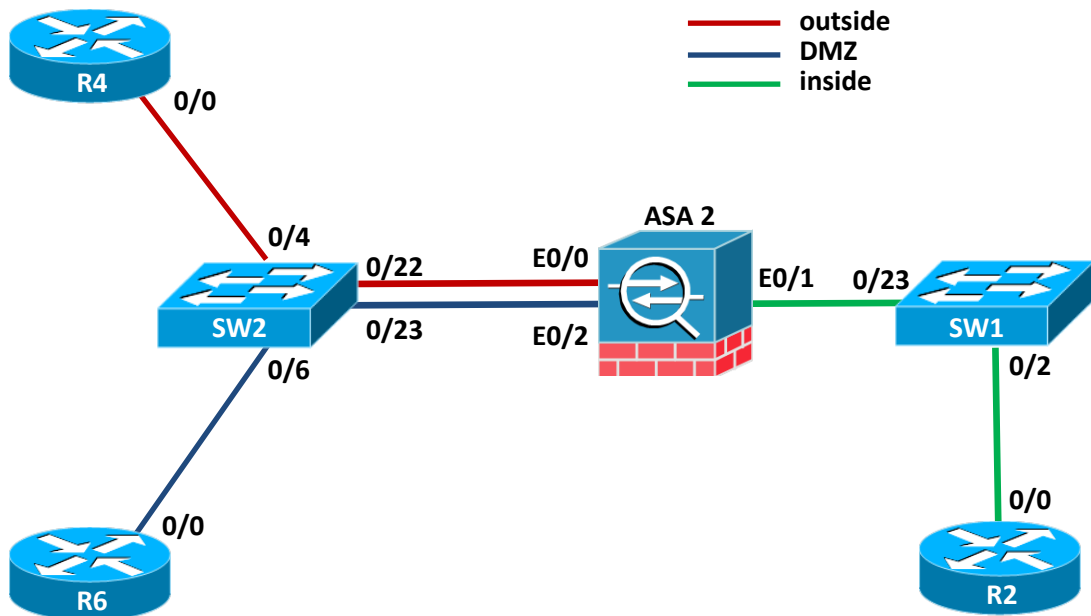
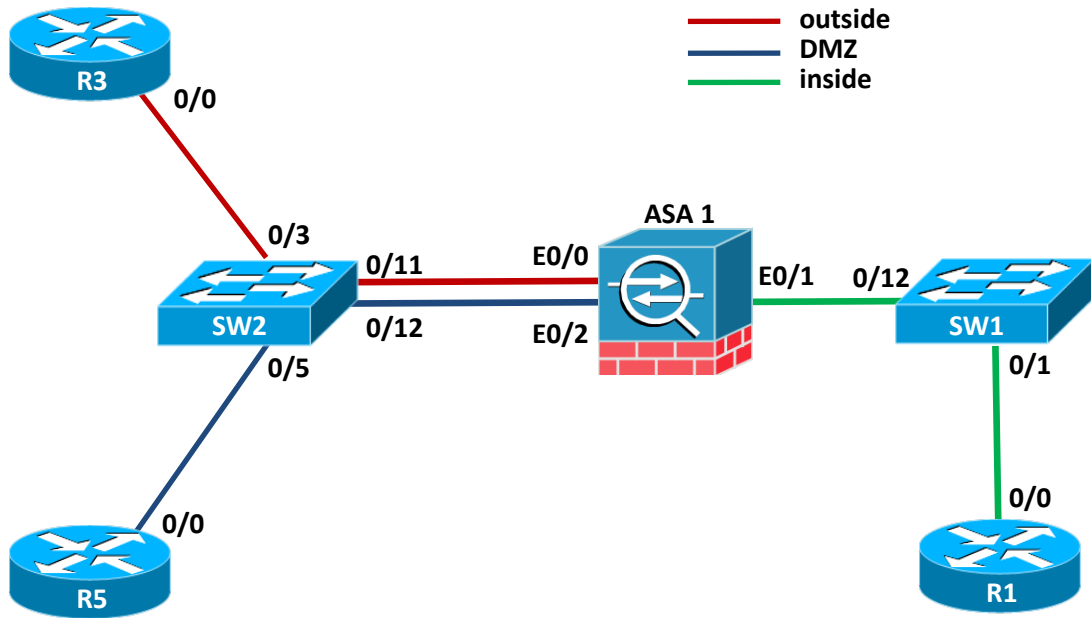
# Platformă de e-learning și curriculă e-content pentru învățământul superior tehnic

Securizarea rețelelor folosind sisteme dedicate

## 6. Implementarea serviciilor de bază de firewalling

# SRSD 6 – Implementarea serviciilor de bază de firewalling

## 1 Topologie



## 2 Obiective

În acest laborator studenții vor învăța să configureze firewall-ul dedicat ASA pentru a customiza inspecția protocoalelor implicite și a controla traficul icmp către interfețele firewall-ului. Se vor studia comenzi de troubleshoot care ajută în determinarea problemelor de traffic-flow la inspecția realizată de firewall.

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

- Configurarea nivelelor de securitate în ASA OS
- Testarea conectivității către ASA folosind ping
- Blocarea mesajelor specifice de ICMP către interfețele firewall-ului
- Configurarea de rute default cu next-hop și interfață de ieșire pe rutere Cisco
- Realizarea unei capturi de pachete pe interfețele dispozitivului ASA
- Analizarea funcționalității packet-tracer pe dispozitivul ASA
- Activarea inspecției pentru protocolul ICMP
- Activarea unui server HTTP pe un ruter Cisco
- Construirea și aplicarea ACL-urilor în ASA OS
- Afișarea conexiunilor create prin firewall-ul ASA

## 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 recapitula configurarea de nivele de securitate și adresare IP în ASA OS.
  - a. [2p]Configurați hostname-ul ASA-ului folosind prenumele vostru.

- b. [10p] Configurați adresarea IP de mai jos pe interfețele dispozitivului ASA.
  - o E0/0: 141.85.99.1/24
  - o E0/1: 192.168.1.1/24
  - o E0/2: 10.10.10.1/24
- c. [15p] Denumiți interfețele dispozitivului ASA precum în topologia de mai sus (inside, dmz, outside).
- d. [20p] Configurați nivelul de securitate al interfeței DMZ la valoarea 50. Verificați configurațiile realizate folosind comenzile:

```
ciscoasa# show nameif  
ciscoasa# show int ip brief
```

- 3. În cadrul acestui task studenții vor învăța cum să controleze mesajele ICMP destinate dispozitivului ASA.
  - a. [25p] Configurați adrese IP pe fiecare dintre cele 3 rutere folosind spațiul /24 adresat pe ASA și valoarea 100 în ultimul octet.
  - b. [30p] Testați folosind ping conectivitatea de la fiecare ruter la interfața ASA direct conectată. Funcționează ping pe toate interfețele?
  - c. [35p] Blocați mesajele de tip echo pe interfața outside, dar permiteți orice alt timp de ICMP. Verificați lipsa conectivității prin ping de pe ruterul conectat pe interfața outside.