UNIUNEA EUROPEANĂ

GUVERNUL ROMÂNIEI

Instrumente Structurale
2007-2013

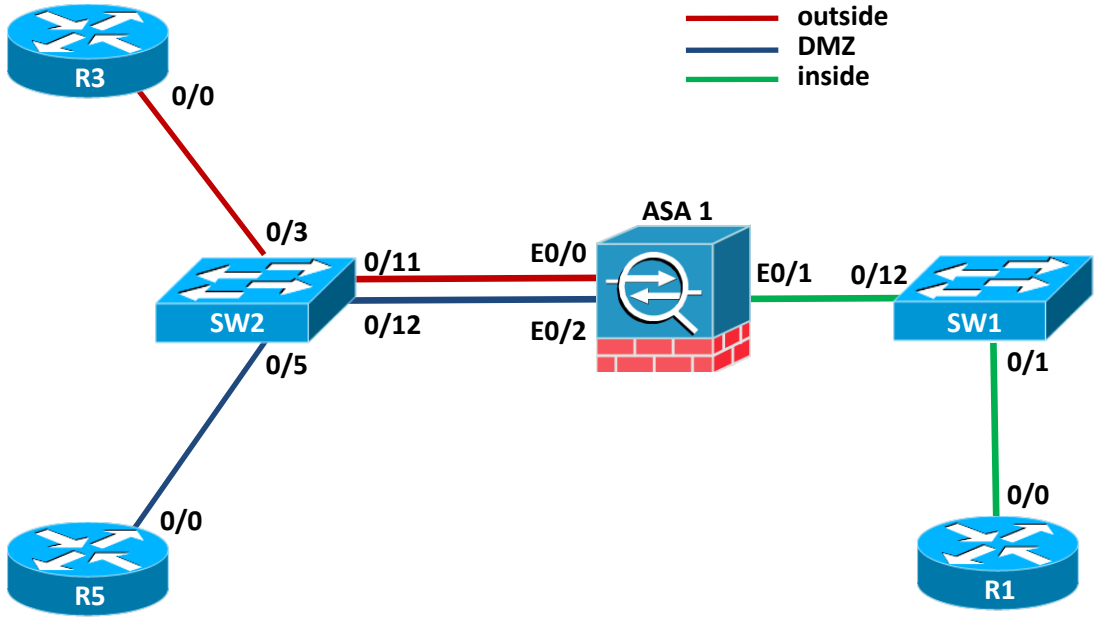
Platformă de e-learning și curriculă e-content pentru învățământul superior tehnic

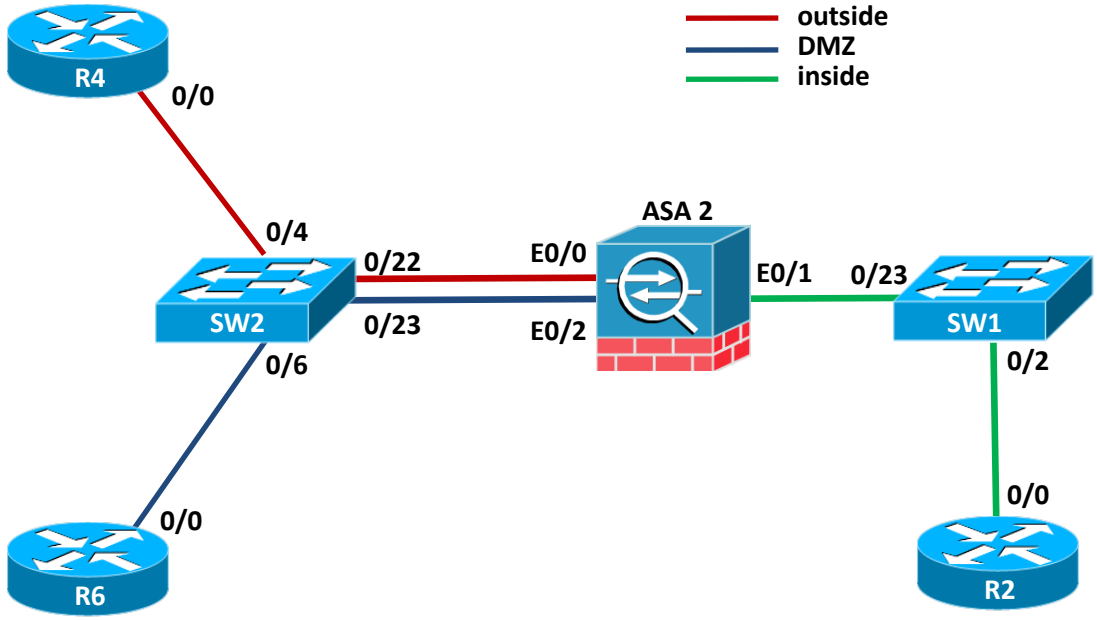
Securizarea rețelelor folosind sisteme dedicate

8. Definirea de ACL-uri și gruparea pe obiecte

SRSD 8 – Definirea de ACL-uri si gruparea pe obiecte

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

1. În cadrul acestui task studenții vor învăța cum să facă troubleshoot pentru conexiunile ce traversează dispozitivul ASA și să activeze inspecția pentru protocolul ICMP

   a. [40p]Creați rute default pe fiecare dintre cele 3 rutere definite **prin interfața de ieșire**

   b. [45p] Încercați să dați ping de la ruterul de pe interfața de inside către ruterul de pe interfața de outside. Funcționează?

   c. [50p]Pentru a depana problema, creați o listă de captură pe ASA pentru interfața de inside.

   d. [55p]Încercați să dați din nou ping. Vizualizați captura folosind comanda **show capture**. Ce concluzie trageți din captură? Apare vreun pachet ICMP? De ce nu?

   e. [60p] Modificați rutele default create pe rutere pentru a fi definite cu **IP-ul de next-hop**.

   f. [65p] Încercați din nou să dați ping de la ruterul de pe interfața de inside către ruterul de pe intrefața de outside. Funcționează? Verificați captura să vedeți dacă de data aceasta apar pachete ICMP.

g. [70p] Folosiți comanda **sh run** pentru a verifica protocoalele inspectate în mod implicit de ASA. ICMP se află printre ele?

h. [75p]Activați inspecția pentru protocolul ICMP prin editarea class_map-ului default.

*Hint: folosiți comenzile pe care le vedeți în running-config pentru a intra mai întâi în **policy-map**, apoi în clasa **inspection_default**, urmând ca apoi să activați inspecția pentru icmp folosind comanda **inspect**.*

i. [80p]Încercați încă o dată ping de la ruterul de pe interfața de inside către ruterul de pe intrefața de outside. Ar trebui să funcționeze.

2. În cadrul acestui task studenții vor învăța cum să definească liste de acces pe ASA și să le folosească pentru a permite trafic de la o zonă cu nivel de securitate mic la o zonă cu nivel de securitate mare.

   a. [85p]Activați un server HTTP pe ruterul conectat la interfața DMZ folosind comanda **ip http server**.

   b. [90p]Încercați să vă conectați la serverul HTTP folosind ruterul conectat la interfața inside folosind telnet pe portul 80. Ar trebui să funcționeze.

   c. [95p]Încercați să vă conectați la serverul HTTP folosind ruterul conectat la interfața outside folosind telnet pe portul 80. De ce nu funcționează?

   d. [100p]Configurați un ACL pe interfața de outside care să permită conexiuni HTTP de la ruterul din outside către serverul HTTP (ruterul din DMZ).