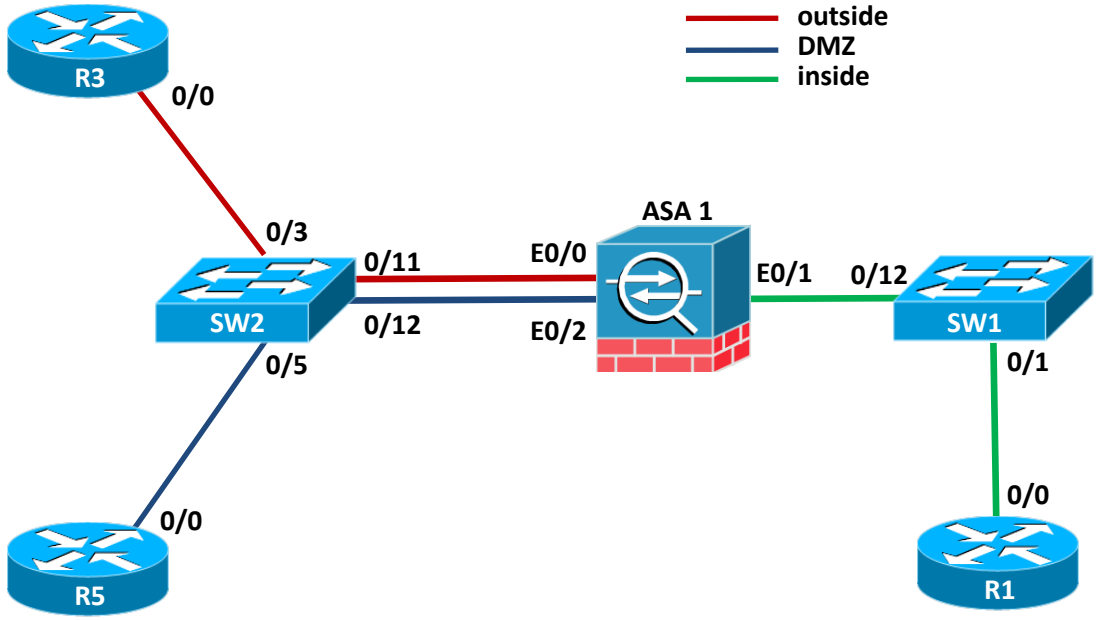
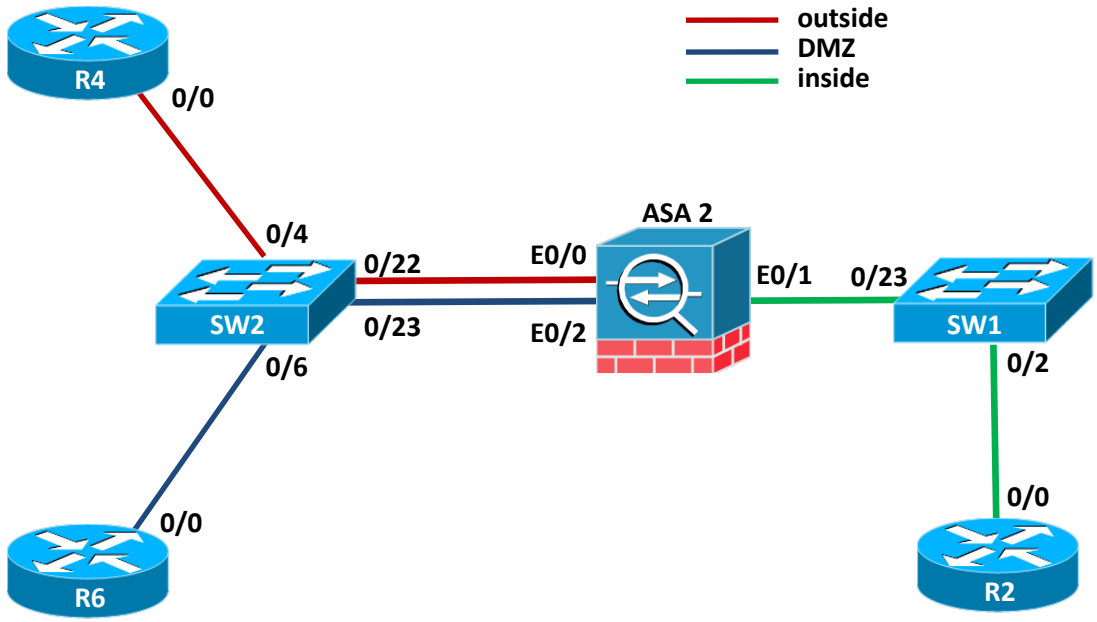
MSSR Cisco Lab 2 – Basic firewalling

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 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.

   - E0/0: 141.85.99.1/24
   - E0/1: 192.168.1.1/24
   - 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.

4. 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.

5. 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).