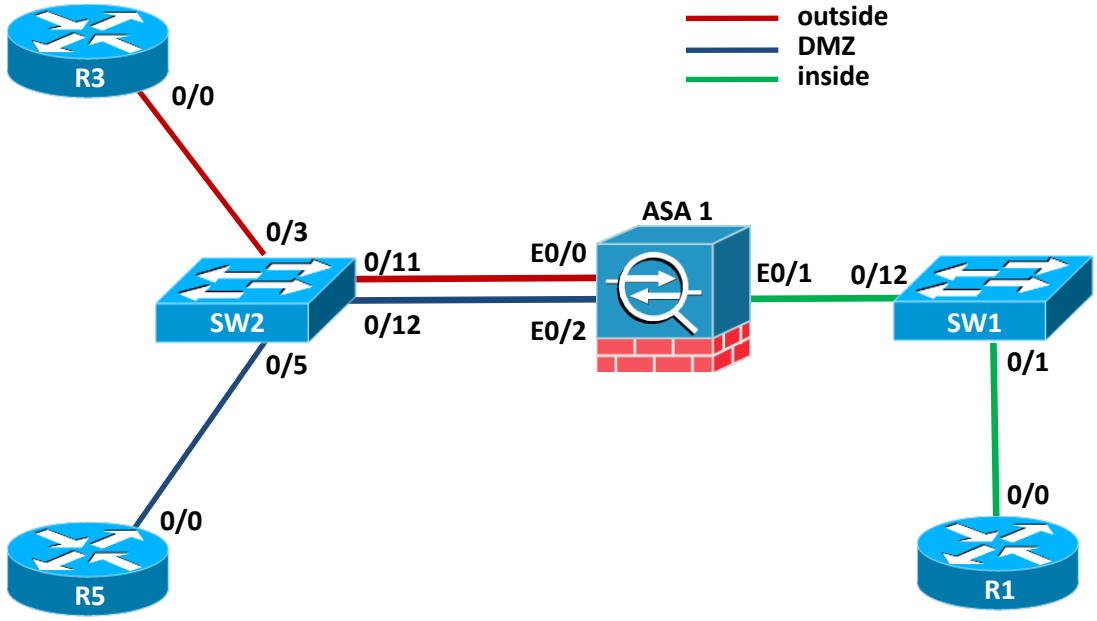
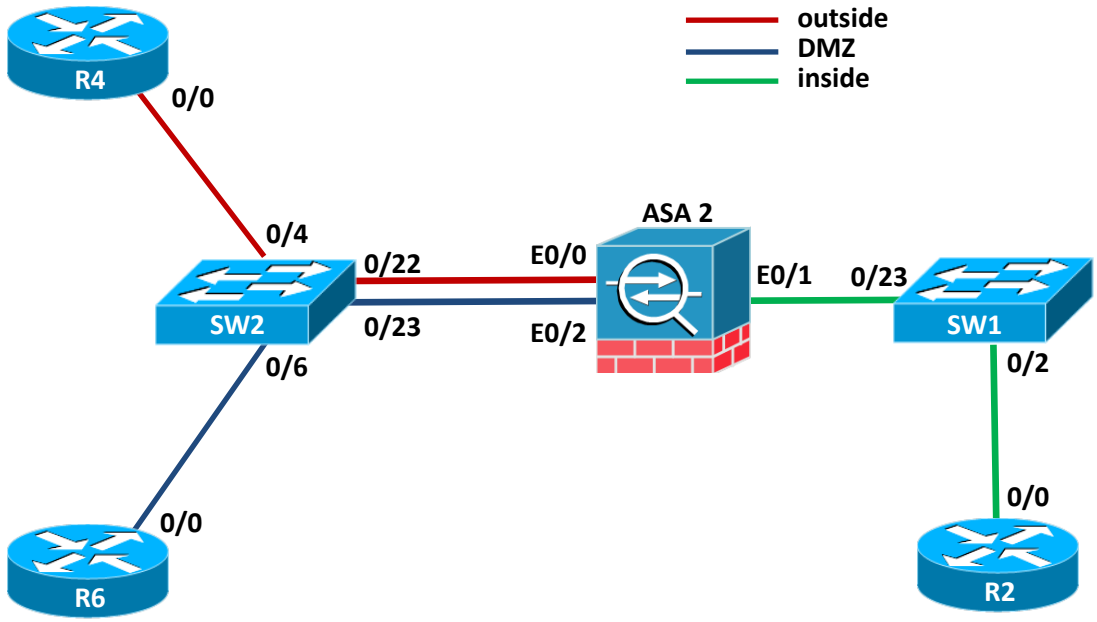
MSSR Cisco Lab 4 – Modular policy framework

1 Topologie





2 Obiective

În acest laborator studenții vor învăța să folosească Modular Policy Framework pentru a controla inspecția pe dispozitive ASA. Se vor studia metoda de Advanced Protocol Handling pentru a bloca anumite tipuri de mesaje HTTP și pentru a configura inspecția de protocoale pe porturi ne-standard.

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

- Configurarea de class-map-uri L3/L4 pentru a identifica trafic
- Configurarea de policy-map-uri pentru a aplica acțiunile MPF
- Implementarea unei politici de inspecție pentru un anumit protocol
- Configurarea inspecției unui protocol pe un port ne-standard
- Configurarea ASA pentru a activa inspecția de ICMP folosind MPF
- Configurarea limitelor pe numărul de conexiuni ce se pot realiza printr-un dispozitiv ASA
- Limitarea numărului de conexiuni TCP și UDP pentru translațiile configurate
- Configurarea obiectelor REGEX pentru a identifica câmpuri de text la nivel 7

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 realiza configurațiile necesare pentru a oferii acces la Internet rețelelor DMZ și LAN printr-un model standard de stateful firewall.

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

    b. [7p]Configurați rețeaua internă (interfața ASA și ruterul direct conectat) cu adrese din pool-ul de adrese private 192.168.1.0/24.

c. [12p]Configurați rețeaua DMZ (interfața ASA și ruterul direct conectat) cu adrese din pool-ul de adrese private 10.10.10.0/24.

d. [17p]Configurați rețeaua externă (interfața ASA și ruterul direct conectat) cu adrese din pool-ul de adrese publice 141.85.99.0/24

e. [23p]Configurați dispozitivul ASA astfel încât următoarele tipuri de comunicații să fie posibile prin aceasta:

   i. Rețeaua internă să poată iniția conexiuni în DMZ și rețeaua externă

   ii. Rețeaua DMZ să poată iniția conexiuni în rețeaua externă, dar nu în rețeaua internă

   iii. Rețeaua externă să nu poată iniția conexiuni către DMZ sau către rețeaua internă

f. [25p]Creați rute default de la fiecare ruter către ASA.

3. În cadrul acestui task studenții vor configura limite de conexiune pentru politica globală a firewall-ului

   a. [30p]Editați politica global_policy pentru a impune un total de 1000 de conexiuni TCP și 100 embryonic. Funcționează modificarea? De ce primiți eroare?

4. În cadrul acestui task studenții vor configura inspecția ICMP folosind MPF.

   a. [35p]Creați un class-map numit identificare_icmp prin care să realizați match pe orice mesaj ICMP. Configurați un ACL pentru a defini acest criteriu.

   b. [40p]Creați un policy-map numit „mssr_map” cu acțiunea „inspect” pentru class-mapul identificare_icmp

   c. [45p]Aplicați policy-map-ul pe interfața de LAN.

   d. [50p]Testați inspecția folosind ping.

5. În cadrul acestui task studenții vor realiza configurațiile necesare pentru a inspecta HTTP pe portul 8080.

   a. [55p]Rulați un server HTTP în DMZ pe portul 8080.

      Hint: ***ip http ?***

   b. [60p]Creați un class-map numit http_8080 ce identifică tot traficul TCP trimis către portul 8080.

c. [65p]Editați policy-map-ul „mssr_map” pentru a adăuga acțiunea de inspect pentru class-map-ul http_8080.

d. [70p]Testați conectivitatea către server pe portul 8080 folosind telnet.

6. În cadrul acestui task studenții vor realiza configurațiile necesare pentru a nu permite accesarea unui executabil peste un URL HTTP.

   a. [75p]Configurați un obiect de tip REGEX numit „exe” care să facă match pe orice fișier cu extensia „.exe”.

   b. [80p]Configurați un class-map type regex numit „identificare_exe” căreia să îi fie asociat obiectul REGEX „indetificare_exe”.

   c. [85p]Configurați un class-map type inspect pentru protocolul HTTP numit „get_exe” care să facă match pe obiectul REGEX atunci când acesta apare în URI.

   d. [90p]Configurați un policy-map type inspect pentru protocolul HTTP numit „drop_exe” care să folosească class-mapul „get_exe” și să aplice acțiunea drop-connection

   e. [95p]Editați policy-map-ul „mssr_map” pentru a inspecta HTTP pe portul 8080 folosind policy-mapul „drop_exe”.

   f. [100p]Testați configurația trimitând comanda „GET /fisier.exe HTTP/1.0 <crlf><crlf>”.