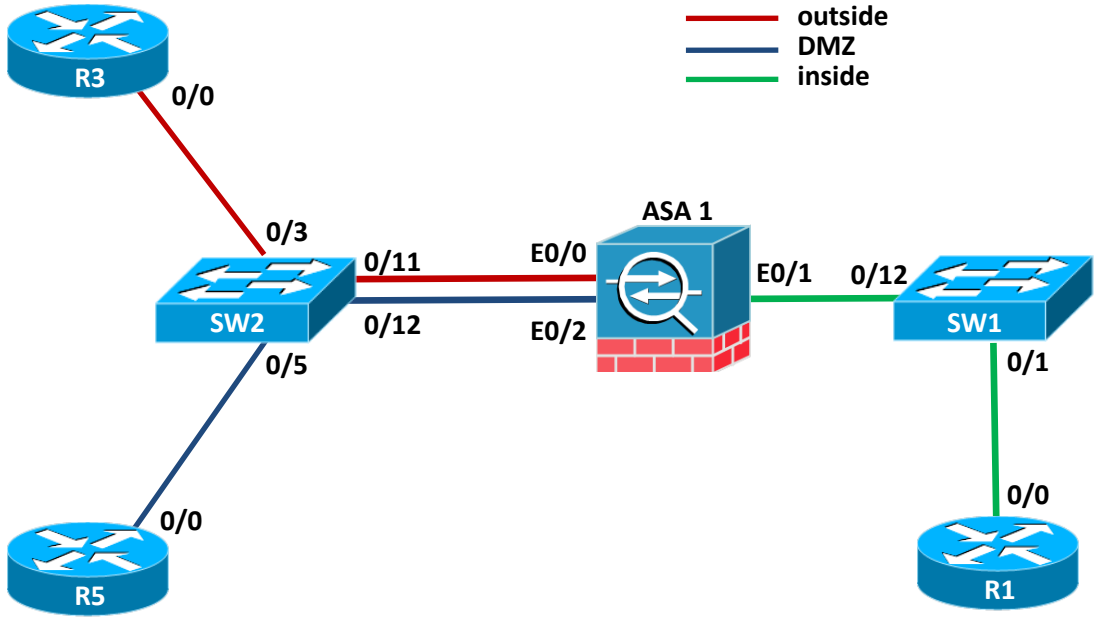
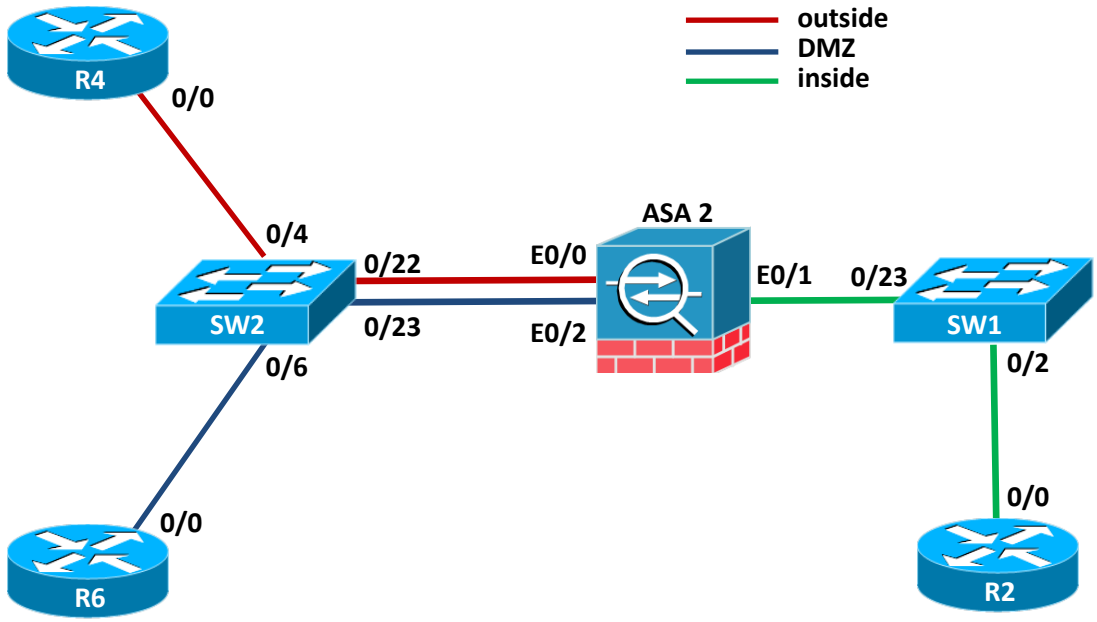
MSSR Cisco Lab 4 – Modular policy framework

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.

```
ciscoasa# conf t
ciscoasa (config)# hostname bogdan
bogdan(config)#
```

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

```
R3(config)#int fa0/0
R3(config-if)#ip address 141.85.99.100 255.255.255.0
R3(config-if)#no sh
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 141.85.99.1
R5(config)#int fa0/0
R5(config-if)#ip address 10.10.10.100 255.255.255.0
R5(config-if)#no sh
R5(config-if)#exit
R5(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.1
R1(config)#int fa0/0
R1(config-if)#ip address 192.168.1.100 255.255.255.0
R1(config-if)#no sh
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

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

```
ciscoasa(config)# int e0/1
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# no sh
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# int e0/0
ciscoasa(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)# no sh
ciscoasa(config-if)# ip address 141.85.99.1 255.255.255.0
ciscoasa(config-if)# int e0/2
ciscoasa(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
```

```
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.10.10.1 255.255.255.0
ciscoasa(config-if)# no sh
```

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?

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# set connection conn-max 1000 embryonic-conn-max
100
ERROR: Only 'inspect' action is allowed for the class with 'match default-
inspection-traffic'.
```

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.

```
ciscoasa(config)# access-list all_icmp extended permit icmp any any
ciscoasa(config)# class-map identificare_icmp
ciscoasa(config-cmap)# match access-list all_icmp
```

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

```
ciscoasa(config)# class-map identificare_icmp
ciscoasa(config-cmap)# match access-list all_icmp
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map mssr_map
ciscoasa(config-pmap)# class identificare_icmp
ciscoasa(config-pmap-c)# inspect icmp
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy mssr_map interface inside
```

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

   d. [50p]Testați inspecția folosind ping.

```
R1#ping 10.10.10.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.100, timeout is 2 seconds:
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
R1#ping 141.85.99.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 141.85.99.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms
```

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 ?***

```
R5(config)#ip http server
R5(config)#ip http port 8080
```

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

```
ciscoasa(config)# class-map http_8080
ciscoasa(config-cmap)# match port tcp eq 8080
ciscoasa(config-cmap)# exit
```

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

```
ciscoasa(config)# policy-map mssr_map
ciscoasa(config-pmap)# class http_8080
ciscoasa(config-pmap-c)# inspect http
```

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

```
R1#telnet 10.10.10.100 8080
Trying 10.10.10.100, 8080 ... Open
```

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”.

```
ciscoasa(config)# regex exe ".+\.exe"
ciscoasa(config)# test regex fisier.exe ".+\.exe"
INFO: Regular expression match succeeded.
```

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

```
ciscoasa(config)# class-map type regex match-any identificare_exe
ciscoasa(config-cmap)# match regex 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.

```
ciscoasa(config)# class-map type inspect http match-any get_exe
ciscoasa(config-cmap)# match request uri regex class identificare_exe
ciscoasa(config-cmap)# exit
```

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

```
ciscoasa(config)# policy-map type inspect http drop_exe
ciscoasa(config-pmap)# class get_exe
ciscoasa(config-pmap-c)# drop-connection
ciscoasa(config-pmap-c)# exit
```

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

```
ciscoasa(config)# policy-map mssr_map
ciscoasa(config-pmap)# class http_8080
ciscoasa(config-pmap-c)# no inspect http
ciscoasa(config-pmap-c)# inspect http drop_exe
```

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

```
R1#telnet 10.10.10.100 8080
Trying 10.10.10.100, 8080 ... Open
GET /fisier.exe HTTP/1.0


[Connection to 10.10.10.100 closed by foreign host]
```