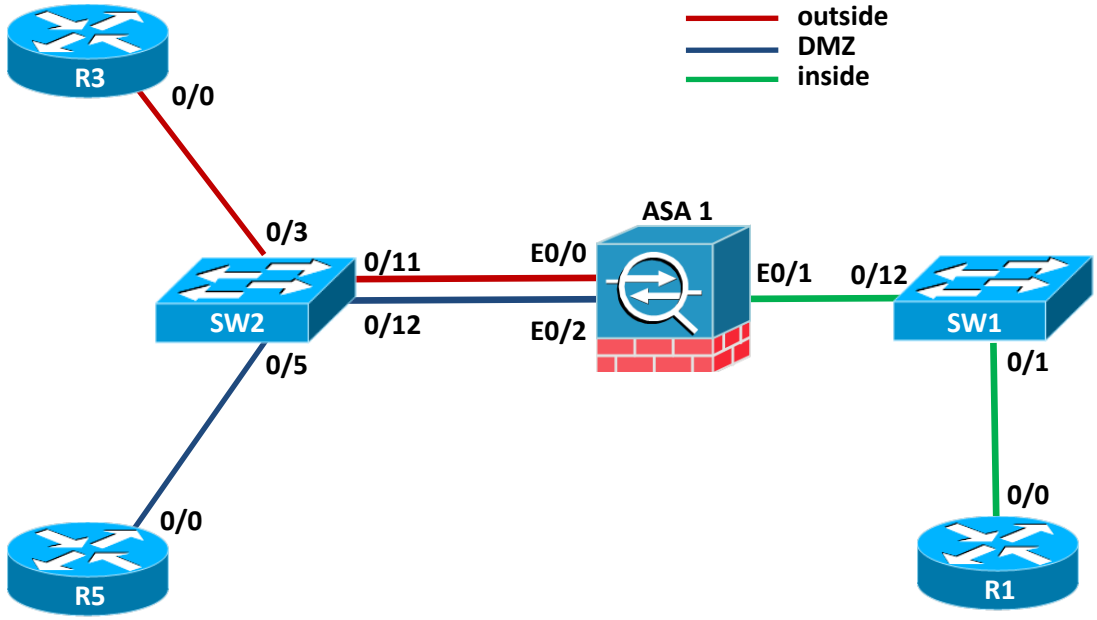
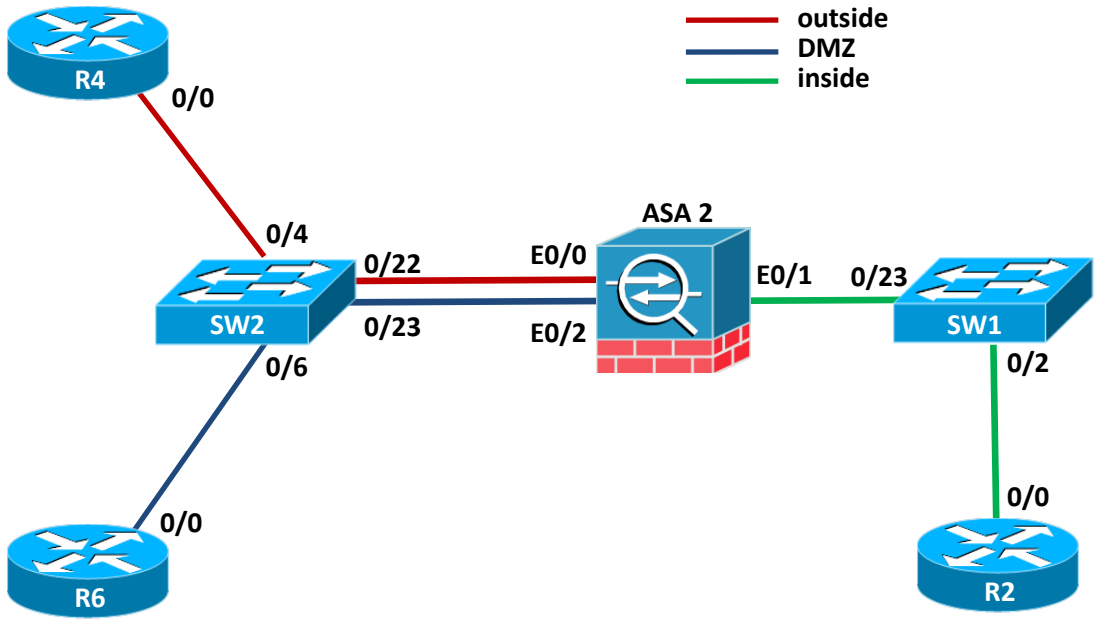
MSSR Cisco Lab 2 – Basic firewalling - rezolvări

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

```
ciscoasa(config)# hostname Bogdan
Bogdan(config)#
```

b. 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. Denumiți interfețele dispozitivului ASA precum în topologia de mai sus (inside, dmz, outside).

d. Configurați nivelul de securitate al interfeței DMZ la valoarea 50. Verificați configurațiile realizate folosind comenzile:

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

```
Bogdan(config)# int e0/0
Bogdan(config-if)# no sh
Bogdan(config-if)# ip address 141.85.99.1 255.255.255.0
Bogdan(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
Bogdan(config-if)# int e0/1
Bogdan(config-if)# no sh
Bogdan(config-if)# ip address 192.168.1.1 255.255.255.0
Bogdan(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
Bogdan(config-if)# int e0/2
Bogdan(config-if)# no sh
Bogdan(config-if)# ip address 10.10.10.1 255.255.255.0
Bogdan(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
Bogdan(config-if)# security-level 50
```

3. În cadrul acestui task studenții vor învăța cum să controleze mesajele ICMP destinate dispozitivului ASA.

a. Configurați adrese IP pe fiecare dintre cele 3 rutere folosind spațiul /24 adresat pe ASA și valoarea 100 în ultimul octet.

```
R5(config)#int fa0/0
R5(config-if)#no sh
*Mar  1 10:30:09.811: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to up
*Mar  1 10:30:10.811: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up255.255.255
R5(config-if)#ip address 10.10.10.100 255.255.255.0

R1(config)#int fa0/0
```

```
  R1(config-if)#no sh
  *Mar  1 10:27:56.151: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to up
  *Mar  1 10:27:57.151: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up100 255
  R1(config-if)#ip address 192.168.1.100 255.255.255.0

  R3(config)#int fa0/0
  R3(config-if)#no sh
  *Mar  1 10:26:19.815: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to up
  *Mar  1 10:26:20.815: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state t
  R3(config-if)#ip address 141.85.99.100 255.255.255.0
```

b. Testați folosind ping conectivitatea de la fiecare ruter la interfața ASA direct conectată. Funcționează ping pe toate interfețele?

```
  R3#ping 141.85.99.1

  Type escape sequence to abort.
  Sending 5, 100-byte ICMP Echos to 141.85.99.1, timeout is 2 seconds:
  .!!!!
  # Ping-ul funcționează asemănător pe toate interfețele ASA
```

c. 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.

```
  R3#ping 141.85.99.1
  *Mar  1 10:30:47.587: %SYS-5-CONFIG_I: Configured from console by console

  Type escape sequence to abort.
  Sending 5, 100-byte ICMP Echos to 141.85.99.1, timeout is 2 seconds:
  .....
  Success rate is 0 percent (0/5)
```

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. Creați rute default pe fiecare dintre cele 3 rutere definite **prin interfața de ieșire**

```
  R3(config)#ip route 0.0.0.0 0.0.0.0 fa0/0
  # Asemănător și pe celalalte rutere
```

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

```
  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:
.....
```

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

```
Bogdan(config)# capture test_list interface inside
```

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

```
Bogdan(config)# show capture test_list
5 packets captured
   1: 03:05:00.816013 arp who-has 141.85.99.100 tell 192.168.1.100
   2: 03:05:02.815097 arp who-has 141.85.99.100 tell 192.168.1.100
   3: 03:05:04.815112 arp who-has 141.85.99.100 tell 192.168.1.100
   4: 03:05:06.815112 arp who-has 141.85.99.100 tell 192.168.1.100
   5: 03:05:08.815112 arp who-has 141.85.99.100 tell 192.168.1.100
#Concluzie: ASA nu are Proxy-ARP pe interfețele sale, rutele trebuie să fie
cu adresă IP next-hop.
```

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

```
R1(config)#no ip route 0.0.0.0 0.0.0.0 fa0/0
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
R3(config)#no ip route 0.0.0.0 0.0.0.0 fa0/0
R3(config)#ip route 0.0.0.0 0.0.0.0 141.85.99.1
R5(config)#no ip route 0.0.0.0 0.0.0.0 fa0/0
R5(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.1
```

f. 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.

```
Bogdan# sh capture test_list
5 packets captured
   1: 02:14:21.299346 192.168.1.100 > 141.85.99.100: icmp: echo request
   2: 02:14:23.295684 192.168.1.100 > 141.85.99.100: icmp: echo request
   3: 02:14:25.295684 192.168.1.100 > 141.85.99.100: icmp: echo request
   4: 02:14:27.295639 192.168.1.100 > 141.85.99.100: icmp: echo request
   5: 02:14:29.295715 192.168.1.100 > 141.85.99.100: icmp: echo request
5 packets shown
```

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

h. Pentru a putea funcționa ping peste ASA, 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**.*

```
Bogdan(config)# policy-map global_policy
Bogdan(config-pmap)# cl
Bogdan(config-pmap)# clas
Bogdan(config-pmap)# class
Bogdan(config-pmap)# class insp
Bogdan(config-pmap)# class inspection_default
Bogdan(config-pmap-c)# inspect icmp
```

i. 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. Activați un server HTTP pe ruterul conectat la interfața DMZ folosind comanda **ip http server**.

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

```
R1#telnet 10.10.10.100 80
Trying 10.10.10.100, 80 ... Open
```

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

```
R3#telnet 10.10.10.100 80
Trying 10.10.10.100, 80 ...
% Connection timed out; remote host not responding
#Pentru că se încearcă conectarea de pe o interfață cu security-level 0 pe una cu security-level 50
```

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

```
Bogdan(config)# access-list permit_http_dmz line 1 extended permit tcp 141.85.99.100 255.255.255.255 10.10.10.100 255.255.255.255 eq 80
Bogdan(config)# access-group permit_http_dmz in interface outside
R3#telnet 10.10.10.100 80
Trying 10.10.10.100, 80 ... Open
```