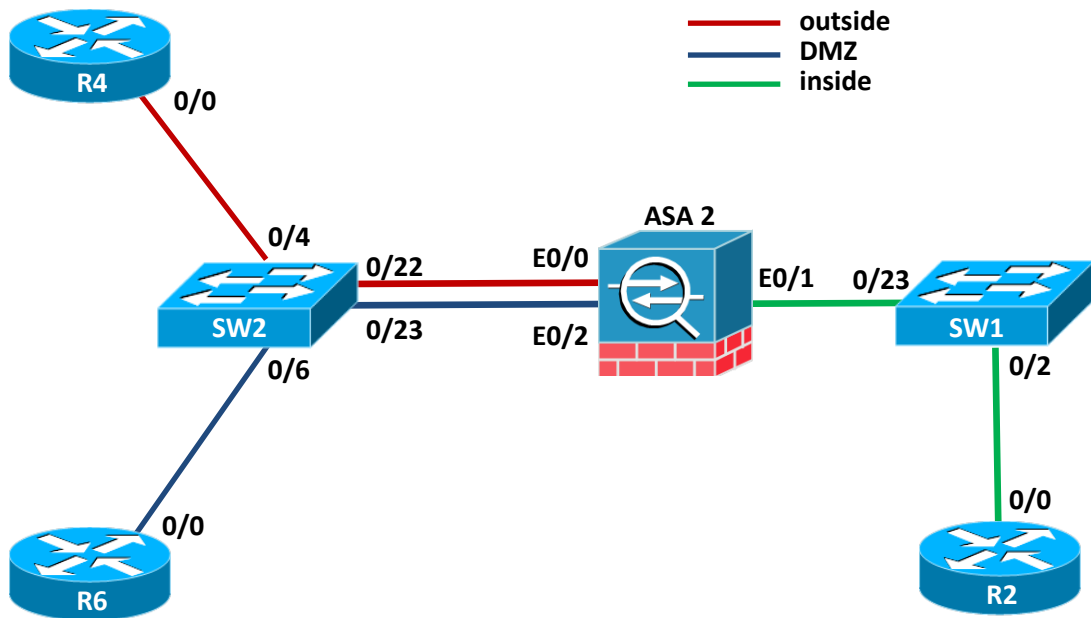
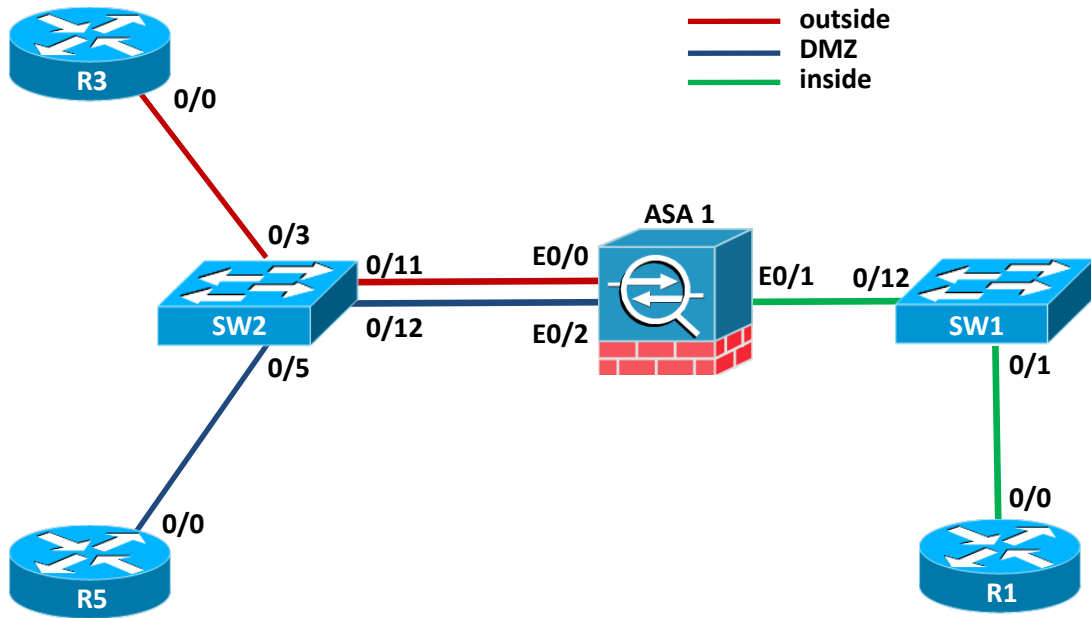


# MSSR Cisco Lab 1 – Introducere în ASA OS și nivele de securitate

## 1 Topologie



## 2 Rezolvări

Rezolvările de mai jos sunt realizate pentru topologia ASA 1. Pentru ASA2 configurațiile sunt asemănătoare.

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](http://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 învăța cum să realizeze configurațiile de bază pe un echipament ASA.
  - a. [2p] Configurați hostname-ul ASA-ului folosind prenumele vostru

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

- b. [5p] Determinați informațiile de mai jos despre ASA-ul vostru:
  - versiunea sistemului de operare
  - modelul device-ului
  - cantitatea de memorie RAM,
  - capacitatea CPU-ului
  - cantitatea memoriei FLASH
  - numărul maxim de VLAN-uri pe care le puteți crea
  - tipul de licență instalat

```
bogdan(config)# show version

Cisco Adaptive Security Appliance Software Version 8.0(4)
Device Manager Version 6.1(3)

Compiled on Thu 07-Aug-08 20:53 by builders
System image file is "disk0:/asa804-k8.bin"
Config file at boot was "startup-config"
```

**bogdan up 1 day 2 hours**

**Hardware: ASA5510, 256 MB RAM, CPU Pentium 4 Celeron 1600 MHz**

**Internal ATA Compact Flash, 256MB**

**BIOS Flash Firmware Hub @ 0xffe00000, 1024KB**

**Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)**

**Boot microcode : CN1000-MC-BOOT-2.00**

**SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03**

**IPSec microcode : CNlite-MC-IPSECm-MAIN-2.05**

**0: Ext: Ethernet0/0 : address is 0026.0bde.661a, irq 9**

**1: Ext: Ethernet0/1 : address is 0026.0bde.661b, irq 9**

**2: Ext: Ethernet0/2 : address is 0026.0bde.661c, irq 9**

**3: Ext: Ethernet0/3 : address is 0026.0bde.661d, irq 9**

**4: Ext: Management0/0 : address is 0026.0bde.661e, irq 11**

**5: Int: Not used : irq 11**

**6: Int: Not used : irq 5**

**Licensed features for this platform:**

**Maximum Physical Interfaces : Unlimited**

**Maximum VLANs : 100**

**Inside Hosts : Unlimited**

**Failover : Active/Active**

**VPN-DES : Enabled**

**VPN-3DES-AES : Enabled**

**Security Contexts : 2**

**GTP/GPRS : Disabled**

**VPN Peers : 250**

**WebVPN Peers : 2**

**AnyConnect for Mobile : Disabled**

**AnyConnect for Linksys phone : Disabled**

**Advanced Endpoint Assessment : Disabled**

**UC Proxy Sessions : 2**

**This platform has an ASA 5510 Security Plus license.**

**Serial Number: JMX1341L16M**

**Running Activation Key: xxx**

**Configuration register is 0x1**

**Configuration last modified by enable\_15 at 18:02:27.797 UTC Fri Feb 18 2011**

- c. [8p]Afișați conținutul configurației active în acest moment pe ASA. Care sunt protocoalele pe care ASA le inspectează în mod implicit?

```
bogdan(config)# sh run
--- output omis ---
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

- d. [10p]Afișați conținutul memoriei flash (Hint: la fel ca în cmd.exe)

```
bogdan(config)# dir flash:

Directory of disk0:/

202  -rwx 14137344  00:06:10 Jan 01 2003  asa804-k8.bin
203  -rwx 2015      11:05:42 Dec 03 2010  old_running.cfg
75   drwx 4096      11:43:00 Oct 08 2009  log
79   drwx 4096      11:43:14 Oct 08 2009  crypto_archive
204  -rwx 7562988    11:44:48 Oct 08 2009  asdm-613.bin
206  -rwx 1470       12:18:08 Dec 03 2010  admin.cfg
209  -rwx 2397046    11:46:34 Oct 08 2009  anyconnect-wince-ARMv4I-2.3.0254-k9.pkg
210  -rwx 2648712    11:46:34 Oct 08 2009  anyconnect-win-2.3.0254-k9.pkg
211  -rwx 4217694    11:46:36 Oct 08 2009  anyconnect-macosx-i386-2.3.0254-k9.pkg
212  -rwx 4259411    11:46:38 Oct 08 2009  anyconnect-linux-2.3.0254-k9.pkg
```

```
213 -rwx 1637    02:37:54 Mar 22 2010 CtxA.cfg
214 -rwx 1637    02:37:56 Mar 22 2010 CtxB.cfg
215 -rwx 1640    11:37:38 Aug 05 2010 CTX1.cfg
216 -rwx 1671    16:07:06 Aug 05 2010 cx1.cfg
217 -rwx 1670    16:08:26 Aug 05 2010 cx2.cfg
218 -rwx 1685    12:18:08 Dec 03 2010 ctx2.cfg
```

255844352 bytes total (205651968 bytes free)

- e. [15p]Configurați parola „cisco” pentru protejarea modului privilegiat. Testați configurația realizată.

```
bogdan(config)# enable password cisco
```

- f. [20p]Configurați parola „class” pentru protejarea accesului prin telnet și SSH (Încă nu veți putea testa această configurație).

```
bogdan(config)# passwd class
```

- g. [25p]Cum sunt păstrate cele 2 parole configurate mai devreme în fișierul de configurare?

```
bogdan(config)# sh run | i passw
enable password 2KFQnbNIdl.2KYOU encrypted
passwd PmNe1e0C3tJdCLE8 encrypted
```

3. În cadrul acestui task studenții vor învăța cum să realizeze configurațiile de bază pentru a activa interfețele unui sistem ASA.
- a. [35p]Configurați următoarele adrese IP pentru cele 3 interfețe ale ASA și activați interfețele folosind comanda **no shutdown**
- E0/0: 141.85.99.1/24
  - E0/1: 192.168.1.1/24
  - E0/2: 10.10.10.1/24

```
bogdan(config)# int e0/0
bogdan(config-if)# no sh
bogdan(config-if)# ip add
bogdan(config-if)# ip address 141.85.99.1 255.255.255.0
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)# int e0/2
bogdan(config-if)# no sh
```

```
bogdan(config-if)# ip add
bogdan(config-if)# ip address 10.10.10.1 255.255.255.0
```

- b. [40p] Afișați un sumar al statusului interfețelor folosind comanda **show interface ip brief**. De ce nu apar IP-urile pe care le-ați configurat? Comenzile date apar în running-config?

```
bogdan(config-if)# show interface ip brief
Interface      IP-Address  OK? Method Status      Protocol
Ethernet0/0    unassigned  YES manual up          up
Ethernet0/1    unassigned  YES manual up          up
Ethernet0/2    unassigned  YES manual up          up
Ethernet0/3    unassigned  YES unset  administratively down down
Management0/0 unassigned  YES unset  administratively down up
```

Răspuns: pentru că interfețele nu sunt încă activate la nivel 3 de către firewall. Pentru a putea fi activate fiecare interfață are nevoie de un nume și un nivel de securitate configurat.

- c. [50p] Denumiți interfețele dispozitivului ASA precum în topologia de mai sus (inside, dmz, outside).

```
bogdan(config-if)# int e0/0
bogdan(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
bogdan(config-if)# int e0/2
bogdan(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
bogdan(config-if)# int e0/1
bogdan(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
```

- d. [55p] Afișați numele interfețelor și nivelele de securitate ale acestora fără a folosi comanda **show running-config**.

```
bogdan(config-if)# show nameif
Interface      Name      Security
Ethernet0/0    outside   0
Ethernet0/1    inside    100
Ethernet0/2    dmz       0
```

- e. [65p] Configurați nivelul de securitate al interfeței denumită „dmz” la valoarea 50

```
bogdan(config-if)# int e0/2
bogdan(config-if)# sec
bogdan(config-if)# security-level 50
```

- f. [70p] Afișați toate nivele de securitate din fișierul de configurare folosind comanda show running-config și aplicând un filtru „include”.

*Hint: folosiți separatorul “|” după comandă urmat de litera ce selectează filtrul include și un cuvânt cheie care să va selecteze doar comenzile “security-level” din fișier*

```
bogdan(config-if)# sh run | i security-level
security-level 0
security-level 100
security-level 50
no security-level
no security-level
```

- g. [75p] Afișați toate comenzile date pe interfața E0/2 fără a folosi filtre

*Hint: show running-config ?*

```
bogdan(config-if)# sh run int e0/2
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 10.10.10.1 255.255.255.0
```

4. În cadrul acestui task studenții vor învăța cum să asigure accesul remote la echipamentele ASA
- a. [85p] Configurați adrese IP pe fiecare dintre cele 3 rutere folosind spațiul /24 adresat pe ASA și valoarea 100 în ultimul octet.

```
R1(config)#int fa0/0
R1(config-if)#no sh
R1(config-if)#ip address 192.168.1.100 255.255.255.0

R5(config)#int fa0/0
R5(config-if)#ip address 10.10.10.100 255.255.255.0
R5(config-if)#no sh

R3(config)#int fa0/0
R3(config-if)#no sh
R3(config-if)#ip address 141.85.99.100 255.255.255.0
```

- b. [90p] Permiteți accesul pe interfațe „inside” prin telnet la ASA pentru adrese din spațiul 192.168.1.0/24. Testați folosind R1, respectiv R2, funcție de topologia pe care sunteți.

```
bogdan(config)# telnet 192.168.1.0 255.255.255.0 inside
```

- c. [95p] Configurați ASA pentru a permite accesul pe interfața „outside” prin telnet pentru adrese din spațiul extern 141.85.99.1/24. Verificați folosind R3, respectiv R4. Funcționează? De ce nu?

```
bogdan(config)# telnet 141.85.99.0 255.255.255.0 outside
```

- d. [100p] Configurați ASA pentru a permite accesul prin SSH versiunea a 2-a pentru adrese din spațiul extern 141.85.99.1/24. Funcționează? De ce?

```
bogdan(config)# crypto key generate rsamodulus 1024  
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.  
Do you really want to replace them? [yes/no]: yes  
Keypair generation process begin. Please wait...  
bogdan(config)# ssh 141.85.99.0 255.255.255.0 outside  
bogdan(config)# ssh version 2
```