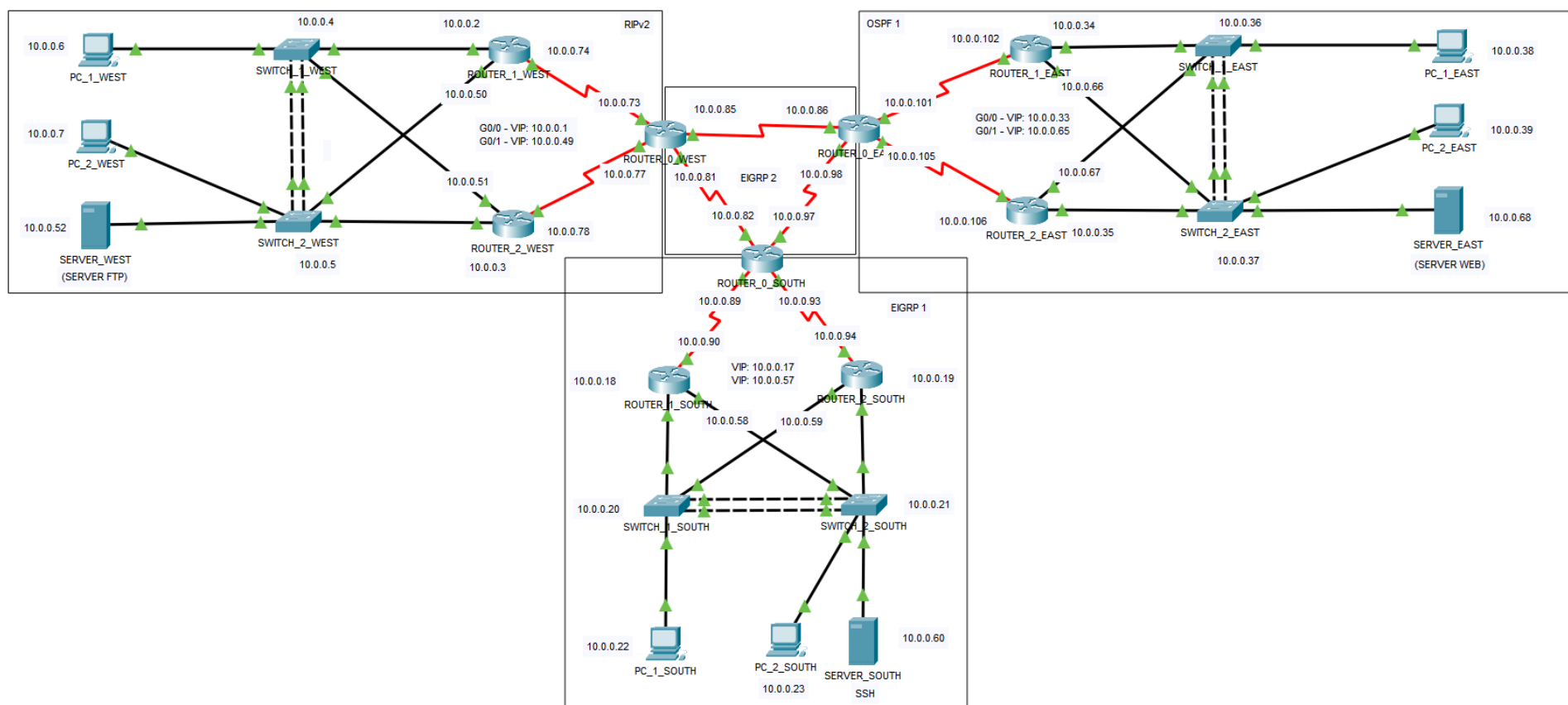


Temă Cybersecurity

Preliminarii

1) Se va construi topologia transmisă respectând tipul echipamentelor (nu este o constrângere legată de model) și conexiunile definite (pot fi adăugate PC-uri suplimentare). Fiecare echipament trebuie să aibă configurațiile standard (securitate, interfețe, mesaje, banner etc.)

Topologie:



II) Vor fi folosite ip-uri doar din range-ul 10.0.0.0/8, limitând pe cat posibil alocarea de ip-uri neutilizate (VLSM). În documentul transmis trebuie să apară explicit asocierea ip-urilor.

Rețele principale

(7 IP-uri necesare – un IP virtual, două IP-uri routere, 2 IP-uri switch-uri, 2 IP-uri pc-uri)

WEST - 10.0.0.0/28: 10.0.0.1 - 10.0.0.14

SOUTH - 10.0.0.16/28: 10.0.0.17 - 10.0.0.30

EAST - 10.0.0.32/28: 10.0.0.33 - 10.0.0.46

(4 IP-uri necesare – un IP virtual, două IP-uri routere, 1 IP server)

WEST - 10.0.0.48/29: 10.0.0.49 - 10.0.0.54

SOUTH - 10.0.0.56/29: 10.0.0.57 - 10.0.0.62

EAST - 10.0.0.64/29: 10.0.0.65 - 10.0.0.70

Obs.: Decizia de a utiliza IP-uri virtuale este motivată de dorința de a obține redundanță. În acest sens, a fost folosit protocolul HSRP (Hot Standby Routing Protocol), care permite posibilitatea de a avea default gateway-uri redundante pentru end-device-uri în cazul în care unul dintre routere cedează. ROUTER_1 a fost configurat cu o prioritate mai mare în toate cele 3 zone, ROUTER_2 fiind “copia” sa în standby.

Rețele de legătură

(2 IP-uri necesare)

10.0.0.72/30: 10.0.0.73 - 10.0.0.74

10.0.0.76/30: 10.0.0.77 - 10.0.0.78

10.0.0.80/30: 10.0.0.81 - 10.0.0.82

10.0.0.84/30: 10.0.0.85 - 10.0.0.86

10.0.0.88/30: 10.0.0.89 - 10.0.0.90

10.0.0.92/30: 10.0.0.93 - 10.0.0.94

10.0.0.96/30: 10.0.0.97 - 10.0.0.98

10.0.0.100/30: 10.0.0.101 - 10.0.0.102

10.0.0.104/30: 10.0.0.105 - 10.0.0.106

Tabelă de adresare

Dispozitiv	Interfață	Adresă IP	Subnet Mask	Default Gateway
ROUTER_0_WEST	S0/0/0	10.0.0.73	255.255.255.252	N/A
	S0/0/1	10.0.0.77	255.255.255.252	N/A
	S0/1/0	10.0.0.85	255.255.255.252	N/A
	S0/1/1	10.0.0.81	255.255.255.252	N/A
ROUTER_1_WEST	S0/0/1	10.0.0.74	255.255.255.252	N/A
		10.0.0.2	255.255.255.240	N/A
	G0/1	VIP: 10.0.0.1	255.255.255.240	N/A
		10.0.0.50	255.255.255.248	N/A
		VIP: 10.0.0.49	255.255.255.248	N/A
ROUTER_2_WEST	S0/0/0	10.0.0.78	255.255.255.252	N/A
		10.0.0.3	255.255.255.240	N/A
		VIP: 10.0.0.1	255.255.255.240	N/A
	G0/1	10.0.0.51	255.255.255.248	N/A
		VIP: 10.0.0.49	255.255.255.248	N/A
SWITCH_1_WEST	VLAN 1	10.0.0.4	255.255.255.240	10.0.0.1
SWITCH_2_WEST	VLAN 1	10.0.0.5	255.255.255.240	10.0.0.1
PC_1_WEST	NIC	10.0.0.6	255.255.255.240	10.0.0.1
PC_2_WEST	NIC	10.0.0.7	255.255.255.240	10.0.0.1
SERVER_WEST	NIC	10.0.0.52	255.255.255.248	10.0.0.49
ROUTER_0_SOUTH	S0/0/0	10.0.0.89	255.255.255.252	N/A
	S0/0/1	10.0.0.93	255.255.255.252	N/A
	S0/1/0	10.0.0.82	255.255.255.252	N/A
	S0/1/1	10.0.0.97	255.255.255.252	N/A
ROUTER_1_SOUTH	S0/0/1	10.0.0.90	255.255.255.252	N/A
		10.0.0.18	255.255.255.240	N/A
	G0/1	VIP: 10.0.0.17	255.255.255.240	N/A
		10.0.0.58	255.255.255.248	N/A
		VIP: 10.0.0.57	255.255.255.248	N/A
ROUTER_2_SOUTH	S0/0/0	10.0.0.94	255.255.255.252	N/A
		10.0.0.19	255.255.255.240	N/A
		VIP: 10.0.0.17	255.255.255.240	N/A
	G0/1	10.0.0.59	255.255.255.248	N/A
		VIP: 10.0.0.57	255.255.255.248	N/A
SWITCH_1_SOUTH	VLAN 1	10.0.0.20	255.255.255.240	10.0.0.17
SWITCH_2_SOUTH	VLAN 1	10.0.0.21	255.255.255.240	10.0.0.17
PC_1_SOUTH	NIC	10.0.0.22	255.255.255.240	10.0.0.17
PC_2_SOUTH	NIC	10.0.0.23	255.255.255.240	10.0.0.17
SERVER_SOUTH	NIC	10.0.0.60	255.255.255.248	10.0.0.57
ROUTER_0_EAST	S0/0/0	10.0.0.101	255.255.255.252	N/A
	S0/0/1	10.0.0.105	255.255.255.252	N/A
	S0/1/0	10.0.0.98	255.255.255.252	N/A
	S0/1/1	10.0.0.86	255.255.255.252	N/A
ROUTER_1_EAST	S0/0/1	10.0.0.102	255.255.255.252	N/A
		10.0.0.34	255.255.255.240	N/A
		VIP: 10.0.0.33	255.255.255.240	N/A

	G0/1	10.0.0.66	255.255.255.248	N/A
		VIP: 10.0.0.65	255.255.255.248	N.A
ROUTER_2_EAST	S0/0/0	10.0.0.106	255.255.255.252	N/A
	G0/0	10.0.0.35	255.255.255.240	N/A
		VIP: 10.0.0.33	255.255.255.240	N/A
	G0/1	10.0.0.67	255.255.255.248	N/A
		VIP: 10.0.0.65	255.255.255.248	N/A
SWITCH_1_EAST	VLAN 1	10.0.0.36	255.255.255.240	10.0.0.33
SWITCH_2_EAST	VLAN 1	10.0.0.37	255.255.255.240	10.0.0.33
PC_1_EAST	NIC	10.0.0.38	255.255.255.240	10.0.0.33
PC_2_EAST	NIC	10.0.0.39	255.255.255.240	10.0.0.33
SERVER_EAST	NIC	10.0.0.68	255.255.255.248	10.0.0.65

III) Conectivitatea din fiecare "zonă" se va realiza prin intermediul unui protocol de routare dinamic (galben RIPv2, albastru OSPF, roșu EIGRP). Pentru zona centrală se poate alege între routare statică sau dinamică, este important sa existe conectivitate între oricare 2 echipamente.

Pentru zona centrală a fost ales protocolul de routare dinamică EIGRP, s-a realizat redistribuirea mutuală a rutelor între protocoalele din zone diferite (RIPv2 și EIGRP 2 între WEST și zona centrală, OSPF 1 și EIGRP 2 între EAST și zona centrală, EIGRP 1 și EIGRP 2 între SOUTH și zona centrală) și s-a obținut conectivitatea între oricare 2 echipamente.

Cerințe ACL

I) Pe fiecare server activați serviciul indicat (galben FTP, albastru WEB).

SERVER_WEST are configurat serviciul FTP, iar SERVER_EAST are configurat serviciul WEB (atât HTTP, cât și HTTPS), ambele având dezactivate serviciile neutilizate.

II) Adăugați configurațiile necesare astfel încât către serverele de mai sus să fie permis doar traficul corespunzător serviciului activat.

Pentru a permite doar traficul FTP către server-ul SERVER_WEST, a fost construit următorul ACL:

```
ip access-list extended "only-ftp"
permit tcp any host 10.0.0.52 eq 21
permit tcp any host 10.0.0.52 eq 20
deny ip any host 10.0.0.52
permit ip any any
```

care permite traficul către server pe porturile TCP 20 și 21 (pentru FTP), respingând orice alt tip de trafic transmis către același server și nefiltrând traficul adresat oricărei alte adrese diferite de cea a server-ului. ACL-ul a fost aplicat outbound pe toate interfețele ne-seriale ale celor două routere din zona server-ului țintă (*ip access-group only-ftp out*).

Similar, pentru a permite doar traficul WEB către server-ul SERVER_EAST, a fost construit următorul ACL:

```
ip access-list extended "only-web"  
permit tcp any host 10.0.0.68 eq 80  
permit tcp any host 10.0.0.68 eq 443  
deny ip any host 10.0.0.68  
permit ip any any
```

care permite traficul către server pe porturile TCP 80 și 443 (pentru HTTP, respectiv HTTPS), respingând orice alt tip de trafic adresat către același server și nefiltrând traficul adresat oricărei adrese diferite de cea a server-ului. Și acesta a fost aplicat outbound pe toate interfețele ne-seriale ale celor două routere din aceeași zonă cu server-ul țintă (*ip access-group only-web out*).

(capturi atașate la IV))

III) Adăugați reguli ACL astfel încât conexiunea SSH la router-ele din zona albastră să fie permisă doar din serverul din zona roșie.

ACL-ul configurat este următorul:

```
ip access-list extended "ssh-restriction"  
permit tcp host 10.0.0.60 any eq 22  
deny tcp any host 10.0.0.34 eq 22  
deny tcp any host 10.0.0.66 eq 22  
deny tcp any host 10.0.0.102 eq 22  
deny tcp any host 10.0.0.35 eq 22  
deny tcp any host 10.0.0.67 eq 22  
deny tcp any host 10.0.0.106 eq 22  
deny tcp any host 10.0.0.33 eq 22  
deny tcp any host 10.0.0.65 eq 22  
permit ip any any
```

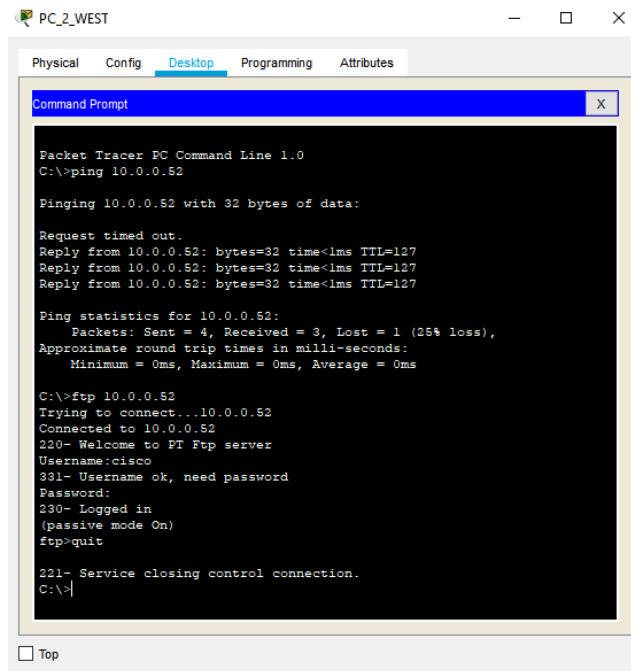
Acesta permite explicit traficul inițiat de către server-ul din zona roșie (SERVER_SOUTH) către orice destinație pe portul TCP 22 (pentru SSH), respingând traficul pe același port din orice altă sursă având destinația oricare dintre IP-urile deținute de cele două routere din zona albastră (ROUTER_1_EAST, ROUTER_2_EAST) și nefiltrând orice alt tip de trafic ce nu se încadrează în regulile precedente. Acest ACL a fost aplicat inbound pe toate interfețele celor două routere din zona albastră (*ip access-group ssh-restriction in*).

(capturi atașate la IV))

IV) Vor fi salvate capturi de ecran din care să rezulte că regulile adăugate filtrează traficul.

Capturi filtrare FTP

A fost testat traficul ICMP, respectiv FTP, inițiat de la sursa PC_2_WEST (10.0.0.7), înainte și după aplicarea ACL-ului only-ftp pe interfețe.



PC_2_WEST

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.52

Pinging 10.0.0.52 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.52: bytes=32 time<1ms TTL=127
Reply from 10.0.0.52: bytes=32 time<1ms TTL=127
Reply from 10.0.0.52: bytes=32 time<1ms TTL=127

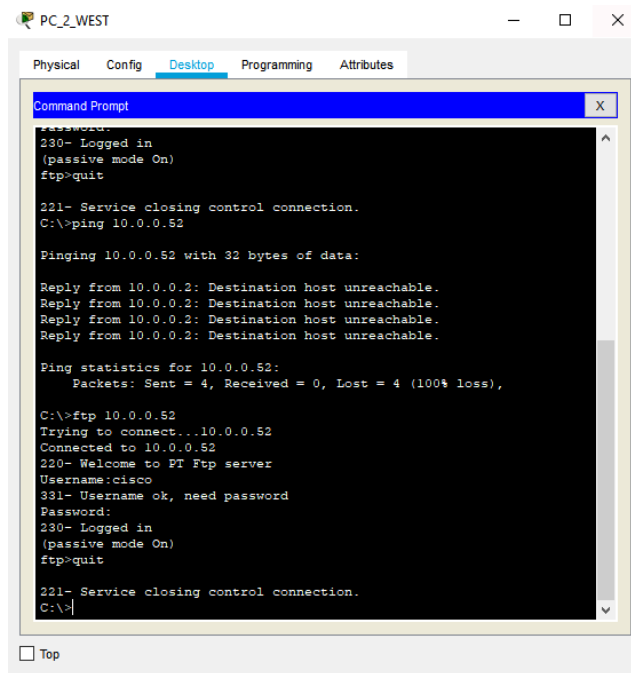
Ping statistics for 10.0.0.52:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ftp 10.0.0.52
Trying to connect...10.0.0.52
Connected to 10.0.0.52
220- Welcome to FT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:\>
```

☐ Top

Captura 1: Testare trafic ICMP și FTP înainte de aplicare ACL (ambele tipuri de pachete ajung la destinație)



PC_2_WEST

Physical Config **Desktop** Programming Attributes

Command Prompt

```
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:\>ping 10.0.0.52

Pinging 10.0.0.52 with 32 bytes of data:

Reply from 10.0.0.2: Destination host unreachable.
Reply from 10.0.0.2: Destination host unreachable.
Reply from 10.0.0.2: Destination host unreachable.
Reply from 10.0.0.2: Destination host unreachable.

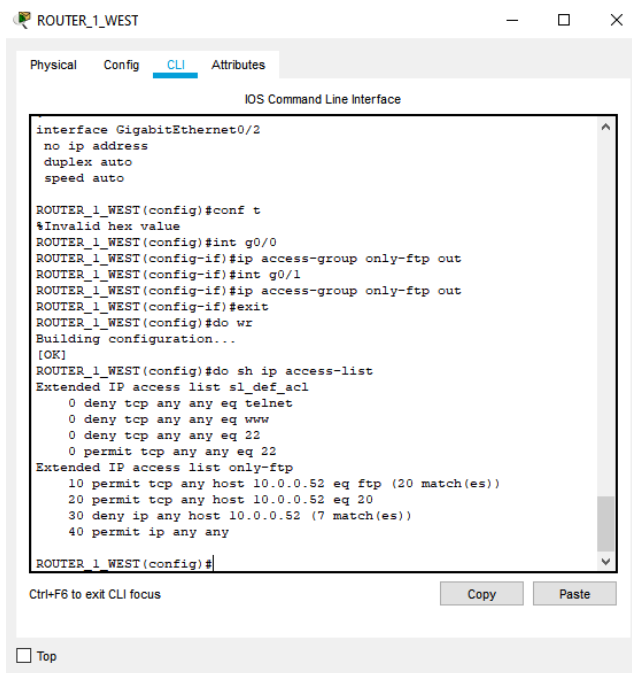
Ping statistics for 10.0.0.52:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ftp 10.0.0.52
Trying to connect...10.0.0.52
Connected to 10.0.0.52
220- Welcome to FT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:\>
```

☐ Top

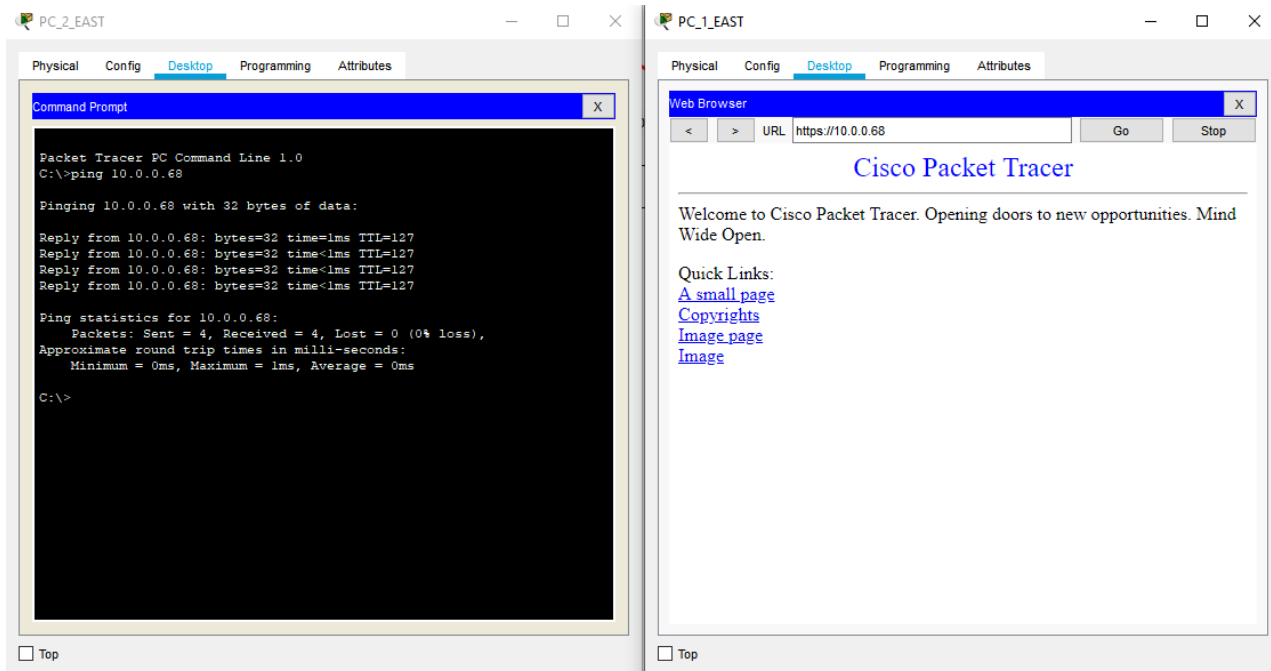
Captura 2: Testare trafic ICMP și FTP după aplicare ACL (pachetele ICMP nu ajung la destinație)



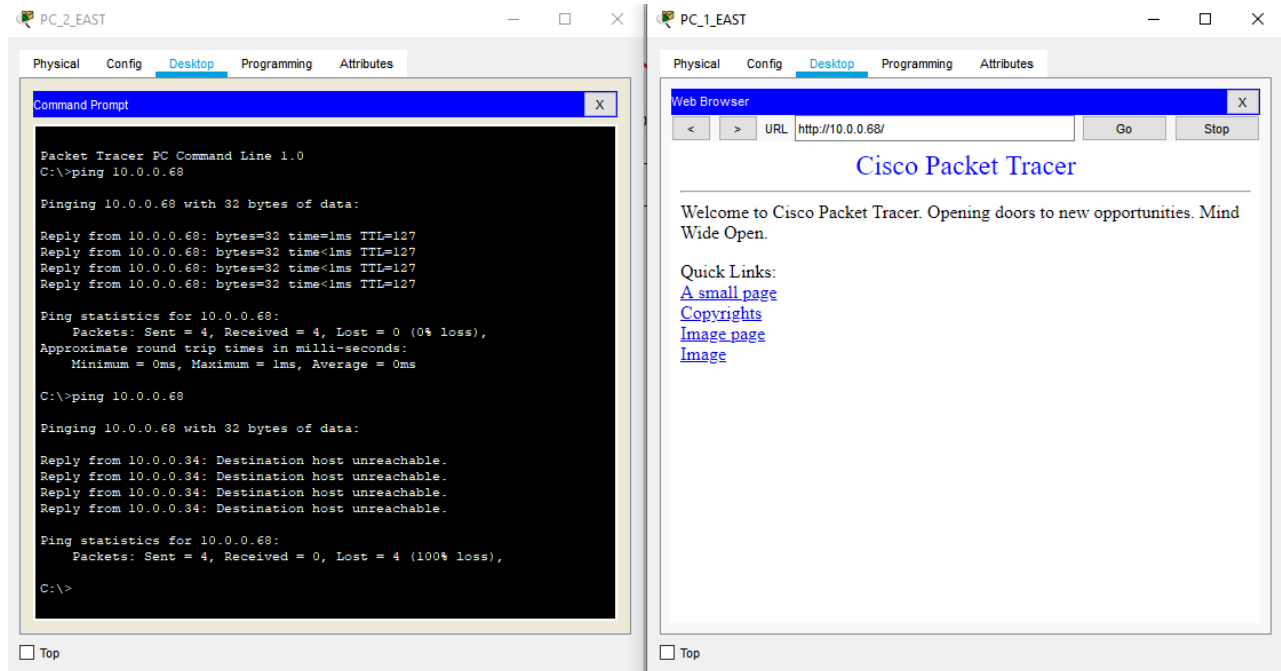
Captura 3: Numărul de match-uri de pe router-ul care a realizat filtrarea

Capturi filtrare WEB

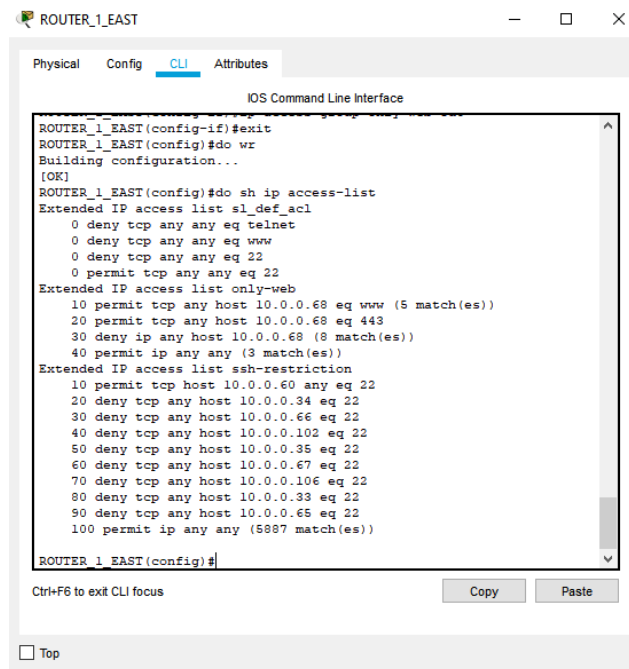
A fost testat traficul ICMP, respectiv HTTP/S, inițiat de la sursele PC_1_EAST (10.0.0.38) și PC_2_EAST (10.0.0.39), înainte și după aplicarea ACL-ului only-web pe interfețe.



Captura 4: Testare trafic ICMP și HTTPS înainte de aplicare ACL (ambele tipuri de pachete ajung la destinație)



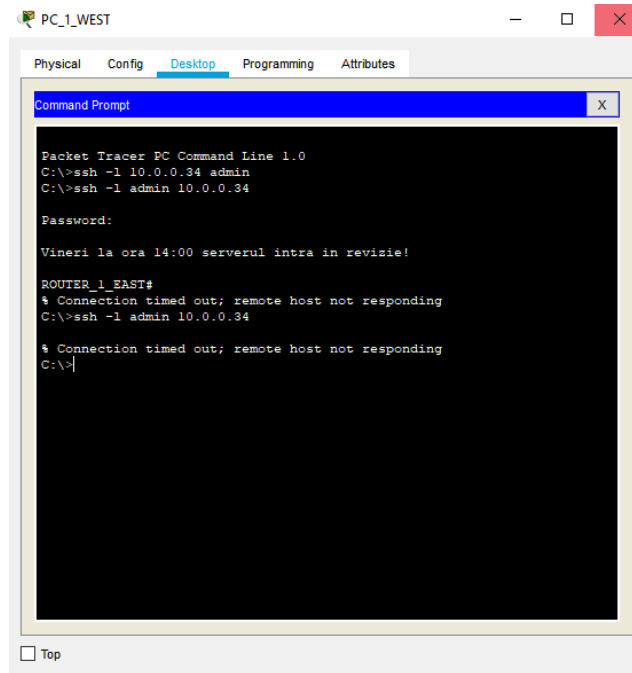
Captura 5: Testare trafic ICMP și HTTP după aplicare ACL (pachetele ICMP nu ajung la destinație)



Captura 6: Numărul de match-uri de pe router-ul care a realizat filtrarea

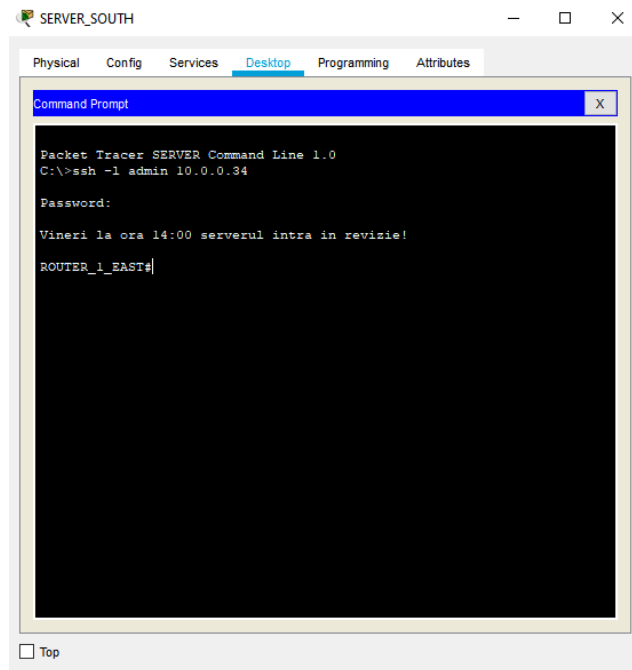
Capturi filtrare SSH

Ca modalitate de testare, a fost inițiată conexiunea SSH către unul din routerele din zona albastră (ROUTER_1_EAST) înainte de a fi aplicat ACL-ul ssh-restriction. După aplicarea ACL-ului pe interfețe, se poate observa cum conexiunea a fost terminată brusc, cu mesajul “remote host not responding”, fără a se interveni de pe client.

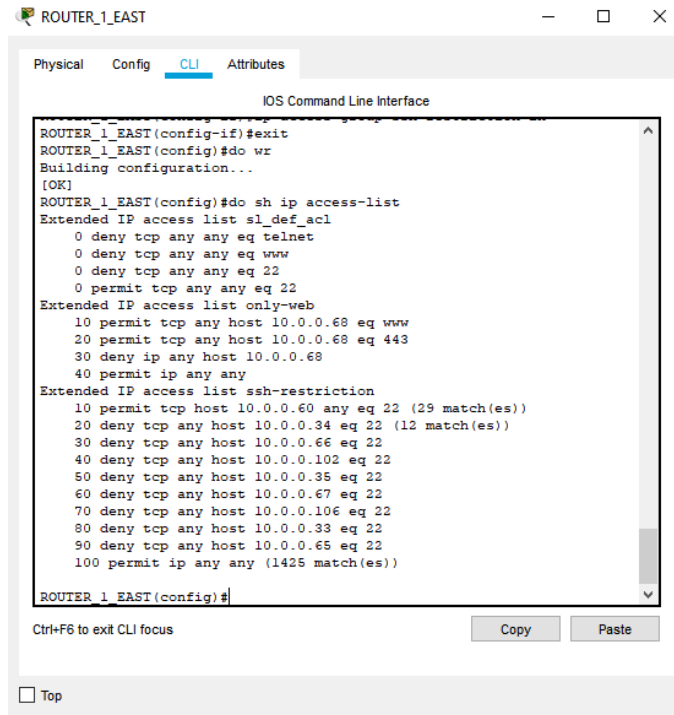


Captura 7: Testare trafic SSH de pe un PC oarecare (conexiunea este încheiată brusc după aplicarea ACL-ului)

S-a verificat și ca server-ul din zona roșie (SERVER_SOUTH) să mai poată iniția conexiuni SSH la router și după aplicarea ACL-ului.



Captura 8: Testare conexiune SSH de pe server-ul roșu (după aplicarea ACL-ului)



```
ROUTER_1_EAST
Physical Config CLI Attributes
IOS Command Line Interface
ROUTER_1_EAST(config-if)#exit
ROUTER_1_EAST(config)#do wr
Building configuration...
[OK]
ROUTER_1_EAST(config)#do sh ip access-list
Extended IP access list sl_def_acl
 0 deny tcp any any eq telnet
 0 deny tcp any any eq www
 0 deny tcp any any eq 22
 0 permit tcp any any eq 22
Extended IP access list only-web
10 permit tcp any host 10.0.0.68 eq www
20 permit tcp any host 10.0.0.68 eq 443
30 deny ip any host 10.0.0.68
40 permit ip any any
Extended IP access list ssh-restriction
10 permit tcp host 10.0.0.60 any eq 22 (29 match(es))
20 deny tcp any host 10.0.0.34 eq 22 (12 match(es))
30 deny tcp any host 10.0.0.66 eq 22
40 deny tcp any host 10.0.0.102 eq 22
50 deny tcp any host 10.0.0.35 eq 22
60 deny tcp any host 10.0.0.67 eq 22
70 deny tcp any host 10.0.0.106 eq 22
80 deny tcp any host 10.0.0.33 eq 22
90 deny tcp any host 10.0.0.65 eq 22
100 permit ip any any (1425 match(es))
ROUTER_1_EAST(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Captura 9: Numărul de match-uri de pe router-ul care a realizat filtrarea