Practice cybersecurity

Radu Ștefan-Octavian

Topology

All equipments have standard configurations.

Subnetting

8.8.8.0/24 zone

- 8.8.8.0/30 - r00 - r0
- 8.8.8.4/30 - r01 - r0
- 8.8.8.8/29 - r00/r01 - sw00 / sw01
- 8.8.8.16/29 - r00/r01 - sw00 / sw01

18.18.20.0/27 zone

- 18.18.20.16/30 - r10 - r1
- 18.18.20.20/30 - r11 - r1
- 18.18.20.0/29 - r10/r11 - sw10 / sw11
- 18.18.20.8/29 - r10/r11 - sw10 / sw11

90.90.90.0/29 zone

- 90.90.90.16/30 - r21 - r2
- 90.90.90.20/30 - r20 - r2
- 90.90.90.0/29 - r20/r21 - sw20 / sw21
- 90.90.90.8/29 - r20/r21 - sw20 / sw21

4.4.4.0/24 zone (central zone)

- 4.4.4.0/30 - r0 - r1
- 4.4.4.4/30 - r0 - r2
- 4.4.4.8/30 - r2 - r1

IP allocation (zone 0)

Equipament	Interface	IP	Subnet mask	Default-Gateway
pc00	fa0	8.8.8.18	255.255.255.248	8.8.8.22
pc01	fa0	8.8.8.10	255.255.255.248	8.8.8.14
server00	fa0	8.8.8.11	255.255.255.248	8.8.8.14
sw00	vlan1	8.8.8.20	255.255.255.248	8.8.8.22
sw01	vlan1	8.8.8.12	255.255.255.248	8.8.8.14
r00	g0/0	8.8.8.9	255.255.255.248	n/a
r00	g0/0	8.8.8.14 (virtual ip)	255.255.255.248	n/a
r00	g0/1	8.8.8.17	255.255.255.248	n/a
r00	g0/1	8.8.8.22 (virtual ip)	255.255.255.248	n/a
r00	g0/2	8.8.8.2	255.255.255.252	n/a
r01	g0/0	8.8.8.9	255.255.255.248	n/a
r01	g0/0	8.8.8.14 (virtual ip)	255.255.255.248	n/a
r01	g0/1	8.8.8.17	255.255.255.248	n/a
r01	g0/1	8.8.8.22 (virtual ip)	255.255.255.248	n/a
r01	g0/2	8.8.8.6	255.255.255.252	n/a

IP allocation (zone 1)

Equipament	Interface	IP	Subnet mask	Default-Gateway
pc10	fa0	18.18.20.5	255.255.255.248	18.18.20.6
pc11	fa0	18.18.20.11	255.255.255.248	18.18.20.14
server10	fa0	18.18.20.2	255.255.255.248	18.18.20.6
sw10	vlan1	18.18.20.4	255.255.255.248	18.18.20.6
sw10	vlan1	18.18.20.10	255.255.255.248	18.18.20.14
r10	g0/0	18.18.20.1	255.255.255.248	n/a
r10	g0/0	18.18.20.6 (virtual ip)	255.255.255.248	n/a
r10	g0/1	18.18.20.9	255.255.255.248	n/a
r10	g0/1	18.18.20.14 (virtual ip)	255.255.255.248	n/a
r10	g0/2	18.18.20.18	255.255.255.252	n/a

Equipament	Interface	IP	Subnet mask	Default-Gateway
r11	g0/0	18.18.20.1	255.255.255.248	n/a
r11	g0/0	18.18.20.6 (virtual ip)	255.255.255.248	n/a
r11	g0/1	18.18.20.9	255.255.255.248	n/a
r11	g0/1	18.18.20.14 (virtual ip)	255.255.255.248	n/a
r11	g0/2	18.18.20.12	255.255.255.252	n/a

IP allocation (zone 2)

Equipament	Interface	IP	Subnet mask	Default-Gateway
pc20	fa0	90.90.90.2	255.255.255.248	90.90.90.6
pc21	fa0	90.90.90.3	255.255.255.248	90.90.90.6
server20	fa0	90.90.90.10	255.255.255.248	90.90.90.14
server21	fa0	90.90.90.11	255.255.255.248	90.90.90.14
sw20	vlan1	90.90.90.12	255.255.255.248	90.90.90.14
sw21	vlan1	90.90.90.4	255.255.255.248	90.90.90.6
r20	g0/0	90.90.90.1	255.255.255.248	n/a
r20	g0/0	90.90.90.6 (virtual ip)	255.255.255.248	n/a
r20	g0/1	90.90.90.9	255.255.255.248	n/a
r20	g0/1	90.90.90.14 (virtual ip)	255.255.255.248	n/a
r20	g0/2	90.90.90.22	255.255.255.52	n/a
r21	g0/0	90.90.90.1	255.255.255.248	n/a
r21	g0/0	90.90.90.6 (virtual ip)	255.255.255.248	n/a
r21	g0/1	90.90.90.9	255.255.255.248	n/a
r21	g0/1	90.90.90.14 (virtual ip)	255.255.255.248	n/a
r21	g0/2	90.90.90.18	255.255.255.252	n/a

IP allocation (central zone)

Equipament	Interface	IP	Subnet mask	Default-Gateway
r0	g0/0	8.8.8.1	255.255.255.252	n/a

Equipament	Interface	IP	Subnet mask	Default-Gateway
r0	g0/1	8.8.8.5	255.255.255.252	n/a
r0	g0/2	4.4.4.1	255.255.255.252	n/a
r0	g0/3	4.4.4.5	255.255.255.252	n/a
r1	g0/0	18.18.20.17	255.255.255.252	n/a
r1	g0/1	18.18.20.21	255.255.255.252	n/a
r1	g0/2	4.4.4.9	255.255.255.252	n/a
r1	g0/3	4.4.4.2	255.255.255.252	n/a
r2	g0/0	90.90.90.21	255.255.255.252	n/a
r2	g0/1	90.90.90.17	255.255.255.252	n/a
r2	g0/2	4.4.4.6	255.255.255.252	n/a
r2	g0/3	4.4.4.10	255.255.255.252	n/a

Details

For each of the non-central zones I used the HSRP protocol for redundancy. Thus, each of the r*1 routers is on standby until the corresponding r*0 fails. As such, there are virtual ips used as gateways by the equipments in each zone.

For the central zone I used the 4.4.4.0/24 ip range, as a specific range wasn’t stated among the requirements.

Conectivity

For the central zone I used the EIGRP dynamic routing protocol. To achieve connectivity between any two equipments, some route redistribution configuration had to be performed between each of the used protocols (RIPv2 - EIGRP, EIGRP - EIGRP, OSPF - EIGRP).

For each pair of switches I added the two used interfaces g0/3-4 to an etherchannel for redundancy and increased bandwidth.

Server config

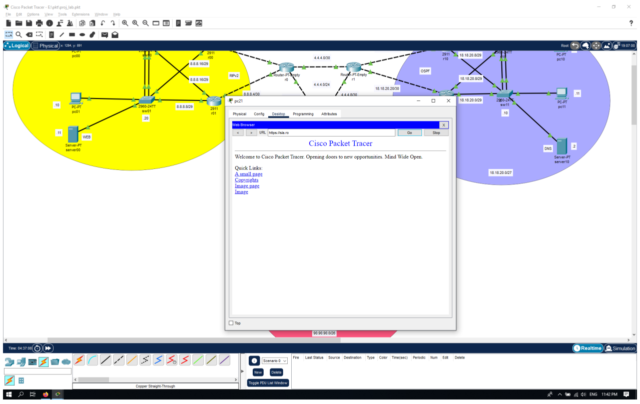
1. Server00 is configured for web (HTTP & HTTPS). All other services disabled.
2. Server10 is configured for DNS. Most of the equipments are added as *A* entries in the DNS table. All other services are disabled.
3. Server20 is configured for EMAIL. Several accounts have been added for use. All other services are disabled.
4. Server21 is used for SSH connections. All services are disabled.

Service filtering

WEB

```
10 permit tcp any host 8.8.8.11 eq www
20 permit tcp any host 8.8.8.11 eq 443
30 deny ip any host 8.8.8.11
40 permit ip any any
```

ACL outbound for the corresponding interface on both routers in zone 0 (yellow)



pc21

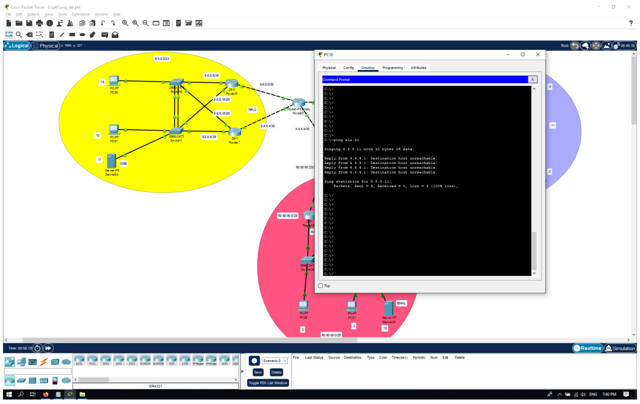
Web Browser

URL https://sla.ro

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image



PC10

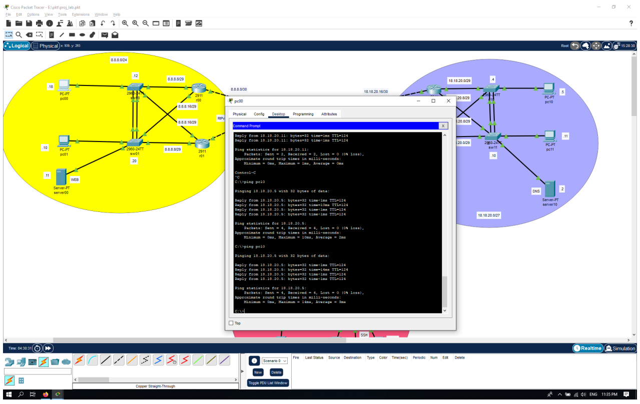
Command Prompt

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping sla.ro

Pinging 8.8.8.11 with 32 bytes of data:

Reply from 4.4.4.1: Destination host unreachable.
Reply from 4.4.4.1: Destination host unreachable.
Reply from 4.4.4.1: Destination host unreachable.
Reply from 4.4.4.1: Destination host unreachable.

Ping statistics for 8.8.8.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

DNS

```
10 permit tcp any host 18.18.20.2 eq domain
20 permit udp any host 18.18.20.2 eq domain
30 deny ip any host 18.18.20.2
40 permit ip any any
```

ACL outbound for the corresponding interface on both routers in zone 1 (blue)



pc00

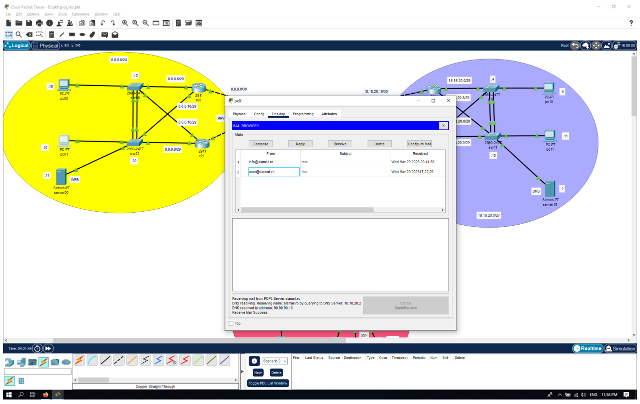
Command Prompt

```
Reply from 18.18.20.11: bytes=32 time=1ms TTL=124
Reply from 18.18.20.11: bytes=32 time<1ms TTL=124

Ping statistics for 18.18.20.11:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

Control-C
^C
C:\>ping pc10

Pinging 18.18.20.5 with 32 bytes of data:

Reply from 18.18.20.5: bytes=32 time<1ms TTL=124
Reply from 18.18.20.5: bytes=32 time=10ms TTL=124
Reply from 18.18.20.5: bytes=32 time<1ms TTL=124
Reply from 18.18.20.5: bytes=32 time<1ms TTL=124

Ping statistics for 18.18.20.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping pc10

Pinging 18.18.20.5 with 32 bytes of data:

Reply from 18.18.20.5: bytes=32 time<1ms TTL=124
Reply from 18.18.20.5: bytes=32 time=14ms TTL=124
Reply from 18.18.20.5: bytes=32 time<1ms TTL=124
Reply from 18.18.20.5: bytes=32 time<1ms TTL=124

Ping statistics for 18.18.20.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 3ms

C:\>
```

EMAIL

```
10 permit tcp any host 90.90.90.10 eq smtp
20 permit tcp any host 90.90.90.10 eq pop3
30 deny ip any host 90.90.90.10
40 permit ip any any
```

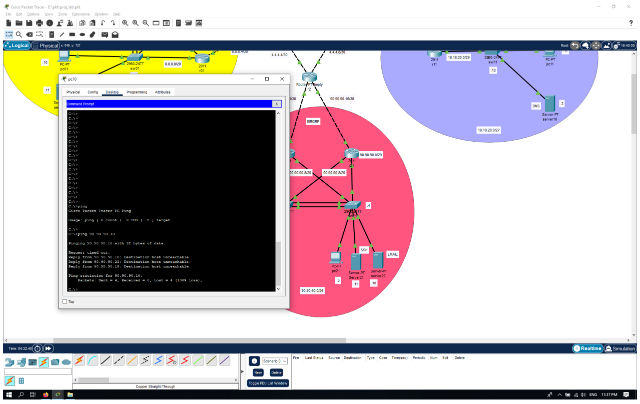
ACL outbound for the corresponding interface on both routers in zone 2 (red)



pc01 — MAIL BROWSER

	From	Subject	Received
1	info@slamail.ro	test	Wed Mar 29 2023 20:41:39
2	user@slamail.ro	test	Wed Mar 29 202317:22:29

Receiving mail from POP3 Server slamail.ro
DNS resolving. Resolving name: slamail.ro by querying to DNS Server: 18.18.20.2
DNS resolved ip address: 90.90.90.10
Receive Mail Success.



pc10 — Command Prompt

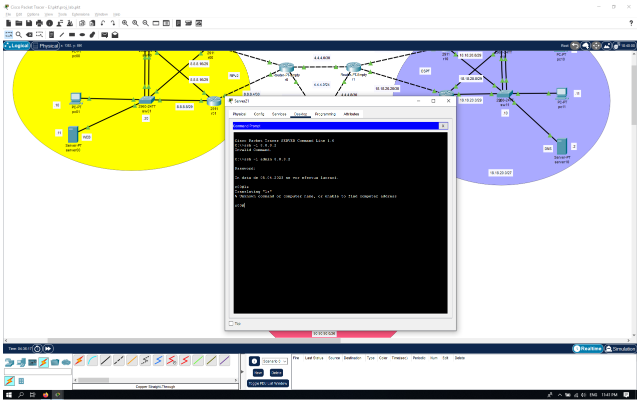
```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping
Cisco Packet Tracer PC Ping

Usage: ping [-n count | -v TOS | -t ] target

C:\>
C:\>ping 90.90.90.10

Pinging 90.90.90.10 with 32 bytes of data:

Request timed out.
Reply from 90.90.90.18: Destination host unreachable.
Reply from 90.90.90.22: Destination host unreachable.
Reply from 90.90.90.18: Destination host unreachable.

Ping statistics for 90.90.90.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

SSH Filtering

```
10 permit tcp host 90.90.90.11 any eq 22
20 deny tcp any host 8.8.8.2 eq 22
30 deny tcp any host 8.8.8.9 eq 22
40 deny tcp any host 8.8.8.14 eq 22
50 deny tcp any host 8.8.8.17 eq 22
60 deny tcp any host 8.8.8.22 eq 22
70 permit ip any any (33 match(es))
```

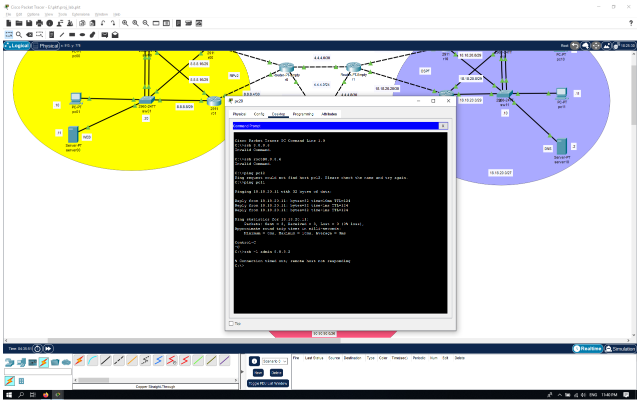
ACL inbound for all interfaces on both routers in zone 0 (yellow)

I added another server for making ssh requests to the yellow zone routers, as the other one’s traffic is limitted to only EMAIL protocols.



Server21 — Command Prompt

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ssh -l 8.8.8.2
Invalid Command.

C:\>ssh -l admin 8.8.8.2

Password:

In data de 05.04.2023 se vor efectua lucrari.

r00#ls
Translating "ls"
% Unknown command or computer name, or unable to find computer address

r00#
```



pc20 — Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh 8.8.8.6
Invalid Command.

C:\>ssh root@8.8.8.6
Invalid Command.

C:\>ping pc12
Ping request could not find host pc12. Please check the name and try again.
C:\>ping pc11

Pinging 18.18.20.11 with 32 bytes of data:

Reply from 18.18.20.11: bytes=32 time=10ms TTL=124
Reply from 18.18.20.11: bytes=32 time<1ms TTL=124
Reply from 18.18.20.11: bytes=32 time<1ms TTL=124

Ping statistics for 18.18.20.11:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

Control-C
^C
C:\>ssh -l admin 8.8.8.2

% Connection timed out; remote host not responding
C:\>
```