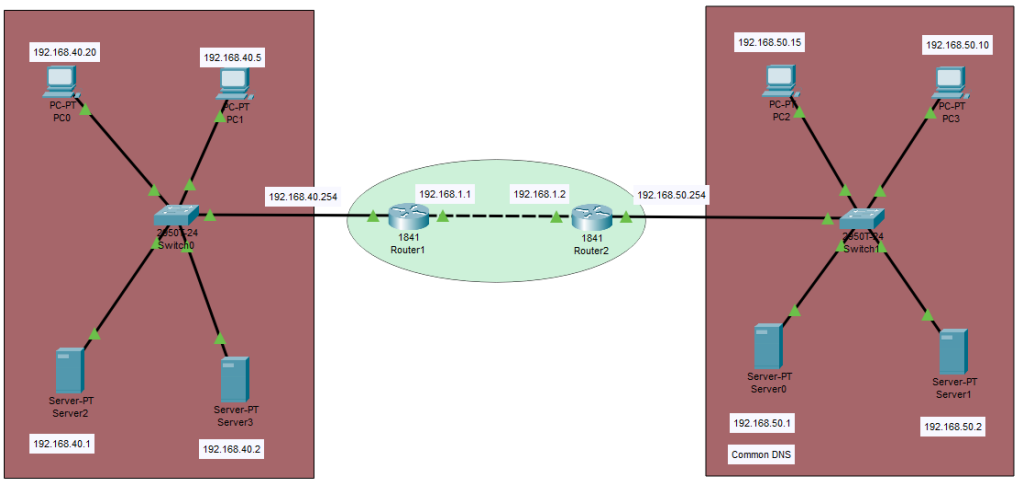
-**********DAY-02_STM**********

****



Rule 1:

Allow DNS traffic.(e.g: access-list 100 permit udp 192.168.40.0 0.0.0.255 host 192.168.50.1 eq domain**) as it allows for domain name mapping for IP.**

Q1-Allow 192.168.40.0 network to access DNS on server 0.

A- access-list 100 permit udp 192.168.40.0 0.0.0.255 host 192.168.50.1 eq domain

Q2- PC2 and PC3 can access the website on server 2.

A- In Router 2

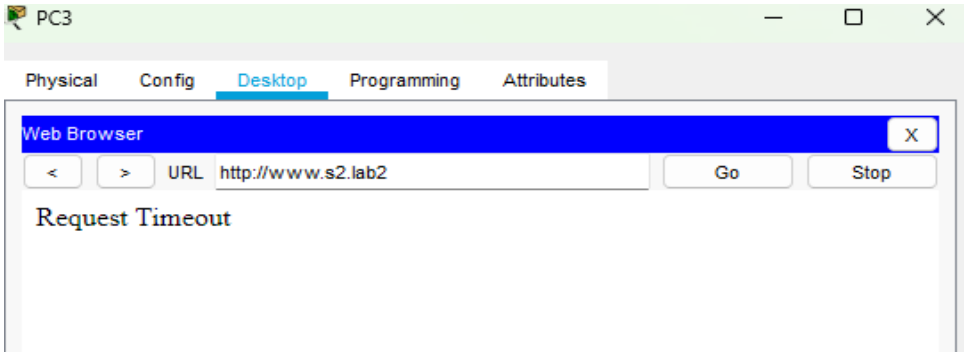
PC2- access-list 100 permit tcp host 192.168.50.15 host 192.168.40.1 eq www

PC3- access-list 100 permit tcp host 192.168.50.10 host 192.168.40.1 eq www

In Router 1

For PC2: access-list 100 permit tcp host 192.168.40.1 host 192.168.50.15

For PC3: if the below code not given, then



access-list 100 permit tcp host 192.168.40.1 host 192.168.50.10

Q3- PC0 can access server1 website

Router 1	**Router 2**
Source-192.168.40.20	Source-192.168.50.2
Destination- 192.168.50.2	Destination- 192.168.40.20
Protocol And Port –tcp 80	Protocol And Port –tcp

R1- access-list 100 permit tcp host 192.168.40.20 host 192.168.50.2 eq 80

R2- access-list 100 permit tcp host 192.168.50.2 host 192.168.40.20

Q4.PC1 can access server 0 website

Router 1	**Router 2**
Source-192.168.40.5	Source-192.168.50.1
Destination- 192.168.50.1	Destination- 192.168.40.5
Protocol And Port –tcp 80	Protocol And Port –tcp

R1- access-list 100 permit tcp host 192.168.40.5 host 192.168.50.1 eq www

R2- access-list 100 permit tcp host 192.168.50.1 host 192.168.40.5

Q5.PC1 can ping server 0 and server 1

Router 1	**Router 2**
Source-192.168.40.5	Source(S0)-192.168.50.1
Destination(Server0)-192.168.50.1	Source(S1)-192.168.50.2
Destination(Server1)-192.168.50.2	Destination192.168.40.5
Protocol And Port –icmp echo	Protocol And Port –icmp echo-reply

R1(S -0)- access-list 100 permit icmp host 192.168.40.5 host 192.168.50.1 echo

R1(S-1)- access-list 100 permit icmp host 192.168.40.5 host 192.168.50.2 echo

R2(S-0)- access-list 100 permit icmp host 192.168.50.1 host 192.168.40.5 echo-reply

R2(S-1)-access-list 100 permit icmp host 192.168.50.2 host 192.168.40.5 echo-reply

NOTE: Here the firewall is configured in router so, it is known as Network Firewall.

Because, access-list is configured for network.

----------Session-2----------

Host Based Firewall (E.g., CDAC office and HPCSA lab computers)

- systemctl status firewalld
- firewall-cmd - -list-all (to see current configuration)

```
[root@localhost ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

NAT == masquerade (in Linux)

- firewall-cmd - -list-all-zones | less (to see zones of the network card)

Default zone is PUBLIC.

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-using_firewalls#sec-Zones

- firewall-cmd - -list-interfaces (To see the n/w cards if up.)
- firewall-cmd - -list-services (For public zones as public is default)
- firewall-cmd - -list-services –zone=external (For external services)
- firewall-cmd - -get-services (Regular used services)
- firewall-cmd - -get-services | grep <service name> (To find specific service)

- yum install httpd –y (**Install apache server:**)
- systemctl status httpd
- cd /var/www/html
- vi index.html
- curl http://localhost
- curl http:// <ip of first machine> (Failed due to closed port 80)
- firewall-cmd - -add-service=http (to allow connection of http)
- firewall-cmd - -list - -all (service checkup)
- firewall-cmd - - remove-service=http (to remove service)
- firewall-cmd - -add-port=80/tcp (to add port)
- firewall-cmd - -add-port= {2379/tcp,6443/tcp,8472/udp...}(add multiple ports)
- firewall-cmd - -remove-port= {2379/tcp,6443/tcp,8472/udp}(remove multiple ports)
- firewall-cmd - -add-port=5000-5100/tcp (open range)
- firewall-cmd - -add-port={5000-5100/tcp,5000-5100/udp,10255/tcp}
- firewall-cmd - -reload (re-read the configuration file, all previous config. gone)
- firewall-cmd - -add-port=5000/tcp --permanent (saved in config file)
- To see the above first reload then list all to see the port.
- firewall-cmd - -remove-port=5000/tcp --permanents

https://docs.oracle.com/en/operating-systems/olcne/1.1/start/ports.html#:~:text=The%20ports%20required%20for%20a,Kubernetes%20API%20server%20(master%20nodes)

- **To change one network adapter from one zone to another.**
- **Add another network card in the main machine.**
- Systemctl restart httpd
- firewall-cmd –list-all
- firewall-cmd –add-port=80/tcp
- From vm2 check for both ip – curl http://xxx.xxx.xxx.xxx
- firewall-cmd - -list-all
- firewall-cmd - -remove-interface=ens36 - -zone=public (can’t remove the assigned zone to another so remove it first)
- **Now add the new zone**
- firewall-cmd - -add-interface=ens36 - -zone=block ()
-
- Firewall-cmd - -reload (Website not access from client)
- Firewall-cmd - -add-interface=ens36 - -zone=internal ()
- Firewall-cmd - -remove-interface=ens36 - -zone=internal
- Firewall-cmd - -add-interface=ens36 - -zone=public (access by the client)
-
-