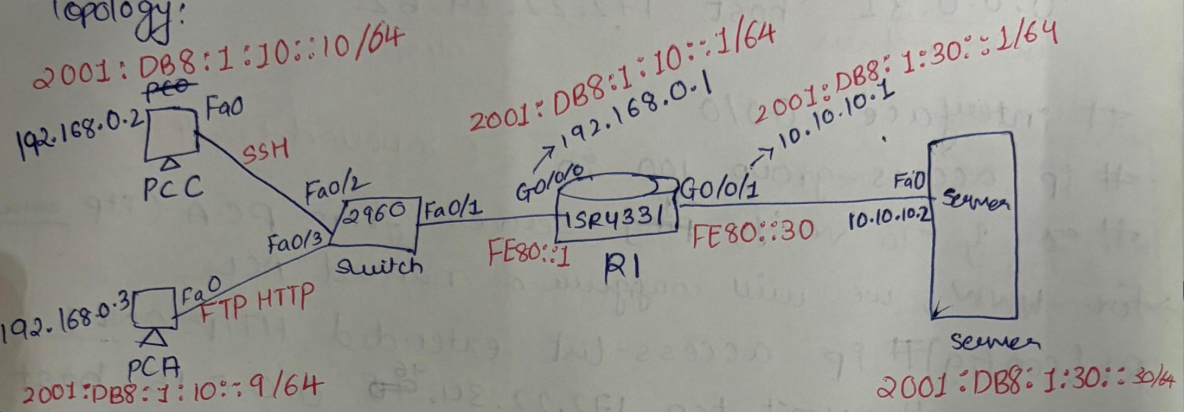
Practical 4

Cofigure IP ACLs to Mitigate Attacks and IPV6 ACLs

a) Verify connectivity among devices before firewall config.
b) Use ACLs to ensure that remote access can only be done PC-C
c) Configure ACLs to mitigate attacks.
d) Configuring IPV6 ACLs.

Topology:



i) Configurations: ISRs provide capabilities like firewall, vpn, etc along with routers.

For R1: Interface: G0/0/0 > On
IPv4 Add: 192.168.0.1 Subnet: Auto

→ Interface: G0/0/1 (Do not On)
IPV4 Add: 10.10.10.1 Subnet: 255.255.255.252 > On

For Server: Desktop > IP Config > Let IPV 4 & 6 remain dfault
IPV4 Add: 10.10.10.2
Subnet: 255.255.255.252 DG: 10.10.10.1

For PC-C: Desktop > IP > Let it remain dfault
IPv4 Add: 192.168.0.2 Subnet: 255.255.255.0
DG: 192.168.0.1

For PC-A: same as above just change the IPV4: 192.168.0.3

→ In R1,
R1(config)# ip route 192.168.0.0 255.255.255.0 10.10.10.2
configure a static route — destination n/w & subnet — next hop address should be
It means, that any traffic destined for destinatn forwarded to the next hop ip address.

→ To verify connection ping the server from both PCs

part b) Since Remote Access is to be done from PC-C:

R1(config)# enable secret enpa55 → (pswd for enable cmd)

#line console 0

~~line~~ password conpa55 (verified before entering the Router (bf enable))

#login

#exit

#ip domain-name ccnasecurity.com (SSH config step)

#username admin secret adminpa55

#line vty 0 4

#login local #transport input ssh

#exit

#crypto key generate rsa

:1024

Go to PC-C command prompt > telnet 10.10.10.1

Connection should fail.

>ssh -l admin 10.10.10.1

password: adminpa55

Part C)

2001:0DB8:0001:0010:0000:0000:0001

n/w portion | host portion

→ Configure IPv6 Address:

→ For PC-A > Desktop > IPv6 > static

Add: 2001:DB8:1:10::9 /64 (states the no. of bits that indicate n/w portion)

Link local address FE80::260:70FF:FE2E:A307 (Default)

DG: FE80::1

→ For Server: ''

Add: 2001:DB8:1:30::30 /64

Link local Address – FE80::230:F2FF:FE24:D043 (Default)

DG: FE80::30

→ For R1

First R1(config)# mode paste the following commands.

#no access-list 1

#access-list 120 permit tcp host 192.168.0.2 host 192.168.0.1

eq (22) SSH Port | only source ip | only destination

ex

conf t

interface G0/0/0

ipv6 address 2001:DB8:1:10::1/64

" " FE80::1 link-local

exit

interface G0/0/1

ipv6 address 2001:DB8:1:30::1/64

ipv6 address FE80::30 link-local

ex

ipv6 unicast-routing

ipv6 route 2001:DB8:1:10::1/64 2001:DB8:1:30::30

→ Go to PCA > Desktop > Browser Url > http://2001:DB8:1:30::30
same for PC-C

→ R1 (config)#

ipv6 access-list HTTP

permit tcp host 2001:DB8:1:10::9 host 2001:DB8:1:30::30
~~eq~~ eq www

" " eq 443 HTTPS port

ex

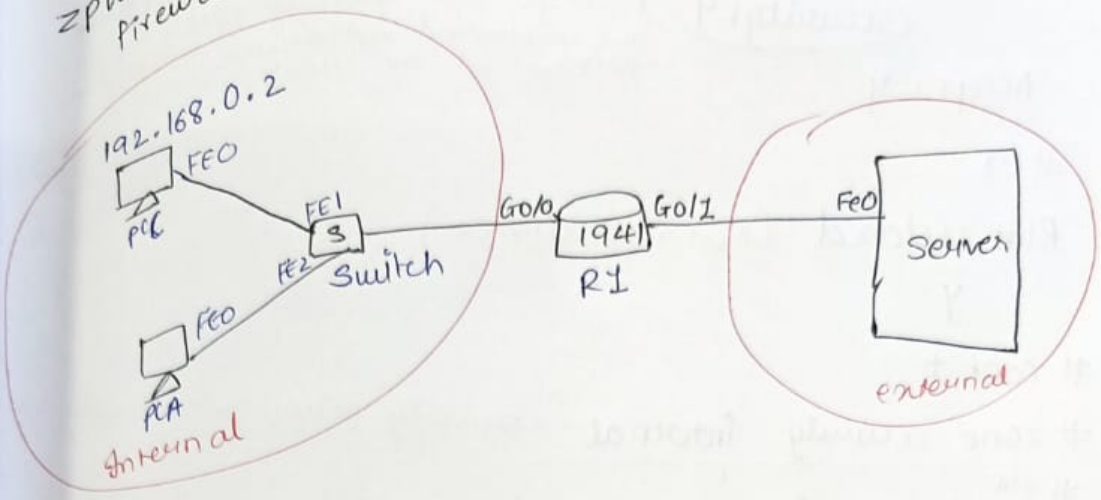
int/f G0/0/0

ipv6 traffic-filter HTTP in

→ Go to PCA > Browser, put the same URl, it should open
→ do the same for PC-C it should not open.

Practical 5

ZPW - A firewall feature of cisco routers. It applies firewall rules on logical zones instead of interfaces



Device Name	IP4 Address	Subnet Mask	Default Gateway
PC-C	192.168.0.2	Auto	192.168.0.1
PC A	192.168.0.3	Auto	192.168.0.1
R1 G0/0	192.168.0.1	Auto	—
R1 G0/1	10.10.10.1	255.255.255.252	—
server	10.10.10.2	255.255.255.252	10.10.10.1

→ Go to R1 to enable SSH connection.

→ R1(config)# enable secret enpa55
line console 0
password conpa55
login
exit
ip domain-name ccnasecurity.com
username admin secret adminpa55
line vty 0 4
login local
exit
crypto key generate rsa

R1 # show version

R1 (config)# license boot module c1900 technology-package securityk9

Router series

package that provides VPN & Firewall capabilities. The command installs the license and package on the router.

Accept: y

ex

R1# reload (Restart device)

y

R1 # conf t

zone security internal — security policy for internal zone

ex

zone security external — external zone

ex # ex

show version.

R1 # Conf t

ip access-list extended 101 — create an ext. ACL named 101 to filter IP traffic

permit ip 192.168.0.0 0.0.0.255 any

source n/w — wildmask

ex → Permits all ip traffic from source range

class-map type inspect match-all 101

create a class-map "101" of type inspect

match access-group name 101

matches the class-map traffic to criteria defined in ACL.

policy-map type inspect 101

create Policy-map "101" of type inspect

class type inspect 101

associate class 101 with Policy 101

inspect # ex # ex

Here, the router is told to perform stateful inspection on traffic flows matched by class-map 101

(config)# zone-pair security 101 source internal destination external. traffic flow from internal to external

service-policy type inspect 101

ex

interface gi 0/0

zone-member security internal

ex

interface gi 0/1
zone-member security external
ex # ex
copy running-config startup-config

Go to pc C and ping the server
ping 10.10.10.2

Class map - Identify specific types of traffic within a network. Used for QOS. Traffic classification

policy-map - The actions to be taken. ~~base~~ on a classified traffic flow

service policy - used for applying the policy map 101 to a particular interface.

~~so, the policy map named 101~~
This means that the traffic passing through that interface / direction will be subject to actions defined in policy map 101.