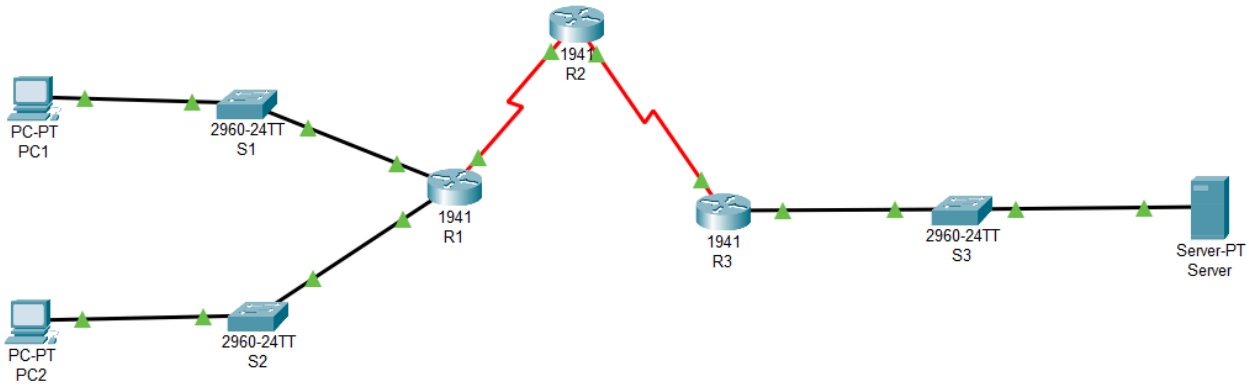
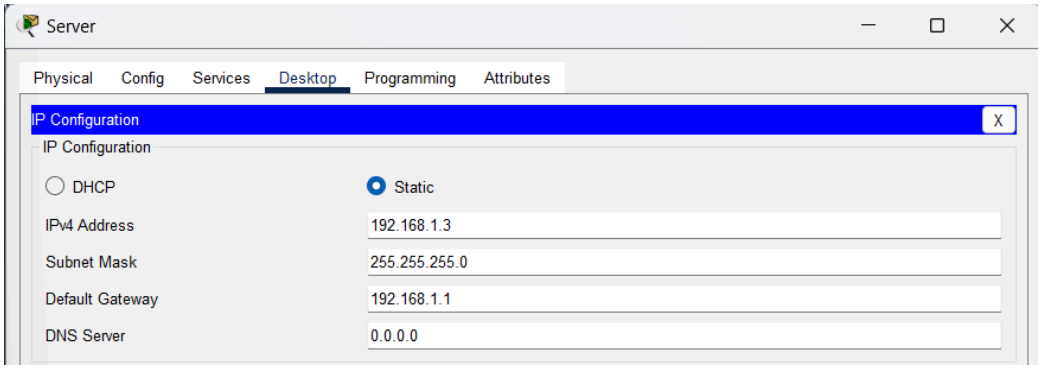
Security in Computing
Practical - 6

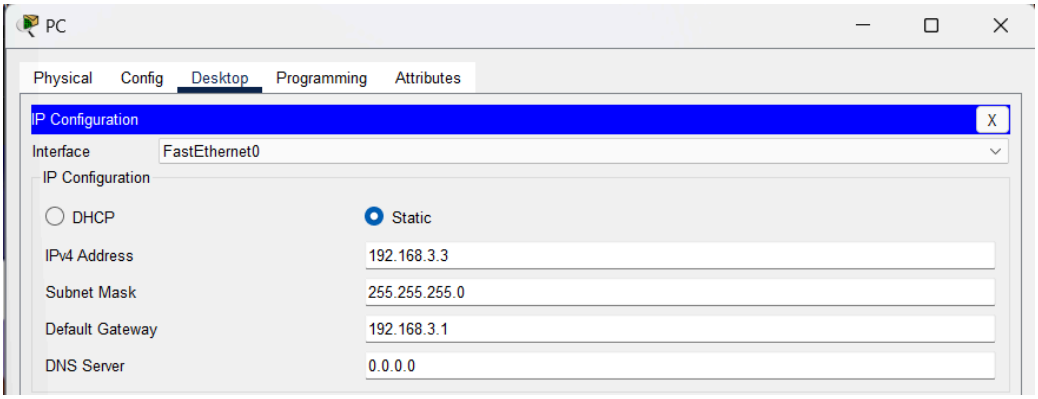
➢Aim: Configuring a Zone-Based Policy Firewall

Topology Diagram:



Assign IP Addresses:





```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host R1
R1(config)#interface Serial0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#interface GigabitEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit
```

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host R2
R2(config)#interface Serial0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2(config-if)#interface Serial0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit
```

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host R3
R3(config)#interface Serial0/0/0
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R3(config-if)#interface GigabitEthernet0/0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R3(config-if)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit
```

Displaying IP Address Details on Routers:

```
R1>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.1.1     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            10.1.1.1        YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

```
R2>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            10.1.1.2        YES manual up                    up
Serial0/0/1            10.2.2.2        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

```
R3>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.3.1     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            10.2.2.1        YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

Configure RIP on Routers:

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 10.1.1.0
R1(config-router)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit
```

```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router rip
R2(config-router)#network 10.1.1.0
R2(config-router)#network 10.2.2.0
R2(config-router)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit
```

```
R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router rip
R3(config-router)#network 10.2.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit
```

Displaying routing tables for Routers:

```
R1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:06, Serial0/0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
R    192.168.3.0/24 [120/2] via 10.1.1.2, 00:00:06, Serial0/0/0
```

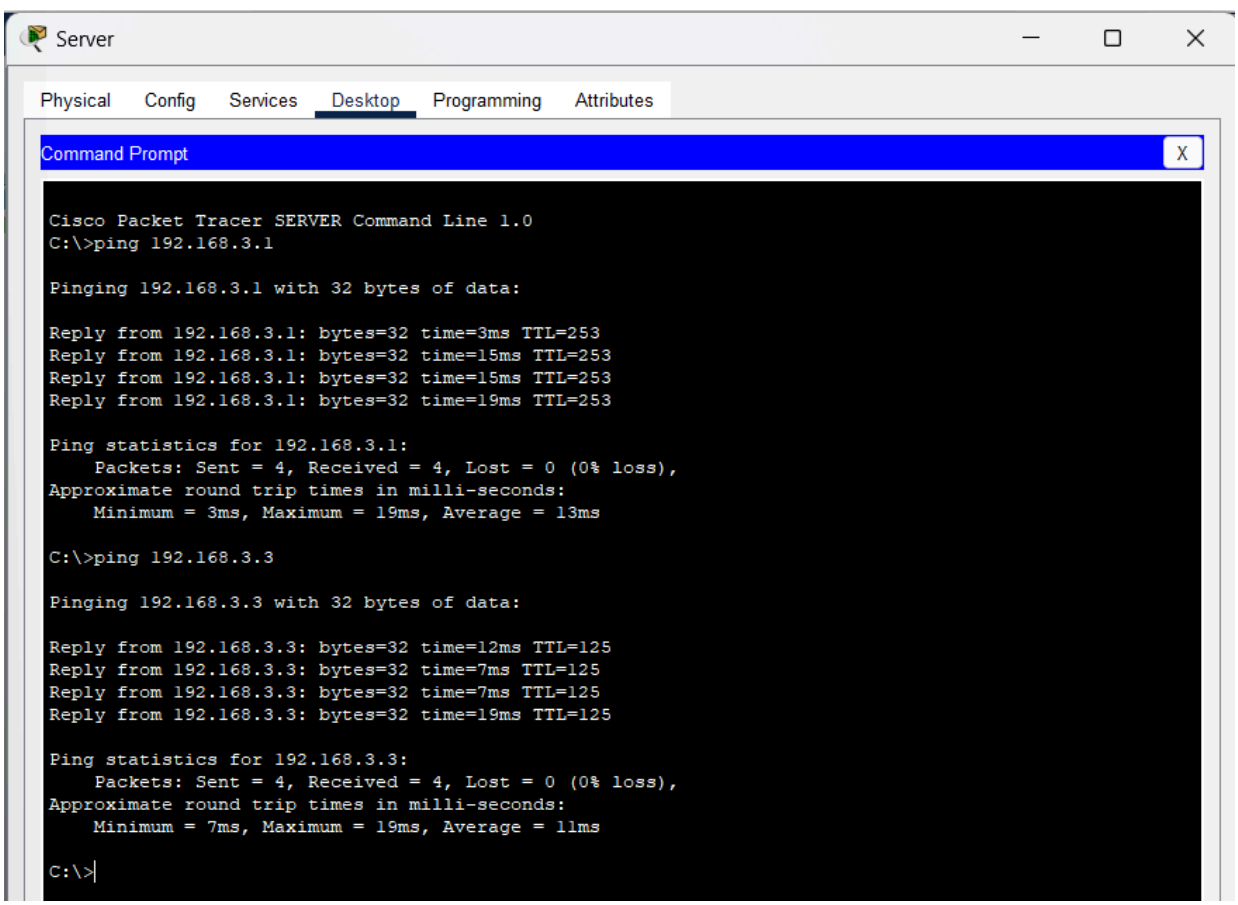
```
R2>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
R    192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:12, Serial0/0/0
R    192.168.3.0/24 [120/1] via 10.2.2.1, 00:00:20, Serial0/0/1
```

```
R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:27, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/0
L       10.2.2.1/32 is directly connected, Serial0/0/0
R    192.168.1.0/24 [120/2] via 10.2.2.2, 00:00:27, Serial0/0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
```

Configure SSH on R2:

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host R2
R2(config)#interface Serial0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2(config-if)#interface Serial0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit
```

Verify basic network connectivity before ACL configuration:



PC

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=4ms TTL=125
Reply from 192.168.1.3: bytes=32 time=9ms TTL=125
Reply from 192.168.1.3: bytes=32 time=18ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 18ms, Average = 8ms

C:\>ssh -l admin 10.2.2.2

Password:



R2>exit

[Connection to 10.2.2.2 closed by foreign host]
C:\>
```

PC

Physical Config Desktop Programming Attributes

Web Browser

< > URL http://192.168.1.3 Go Stop

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

Enable the Security Technology package on R3:

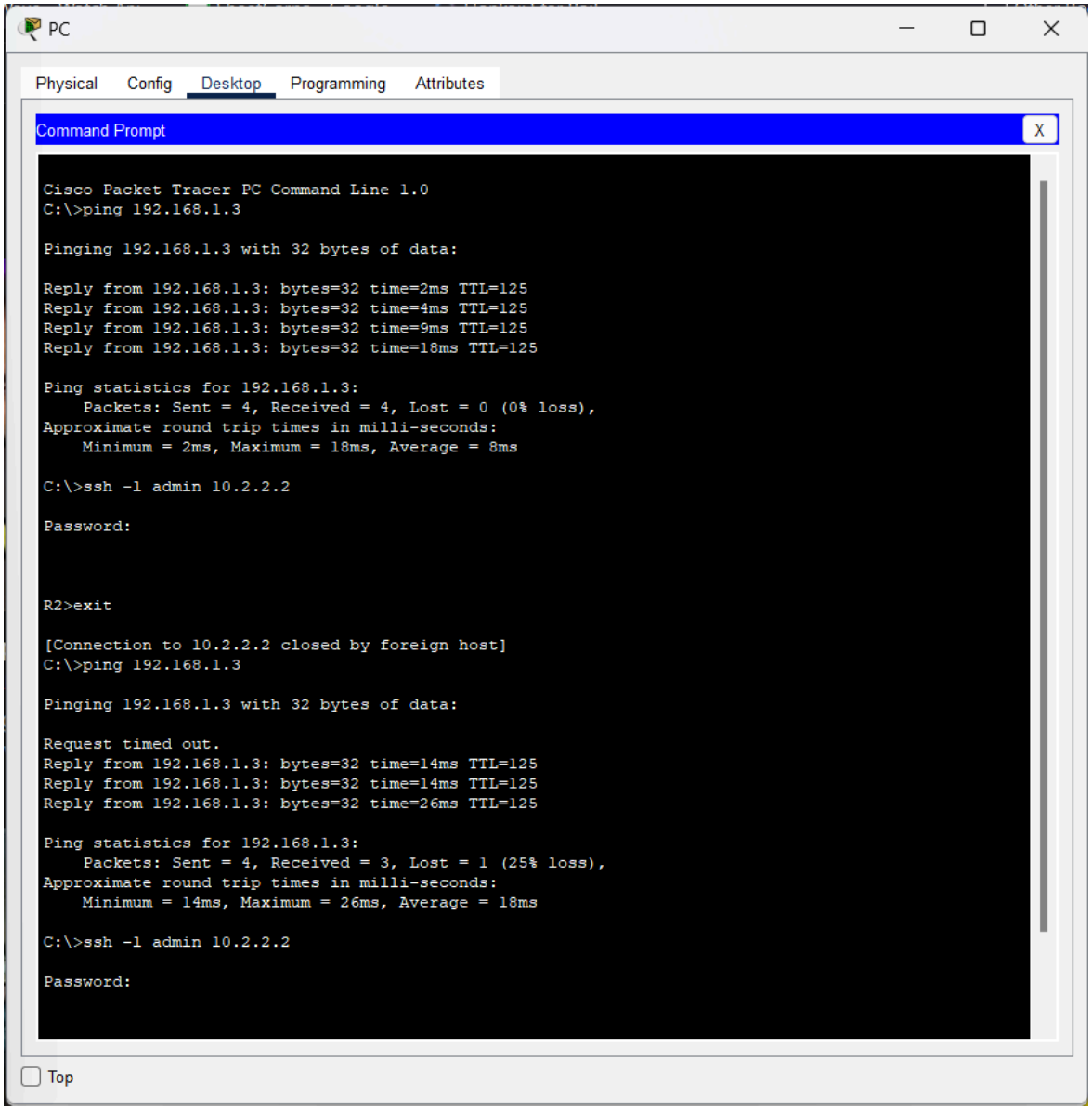
```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
data          None          None          None

Configuration register is 0x2102
```

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None

Configuration register is 0x2102
```

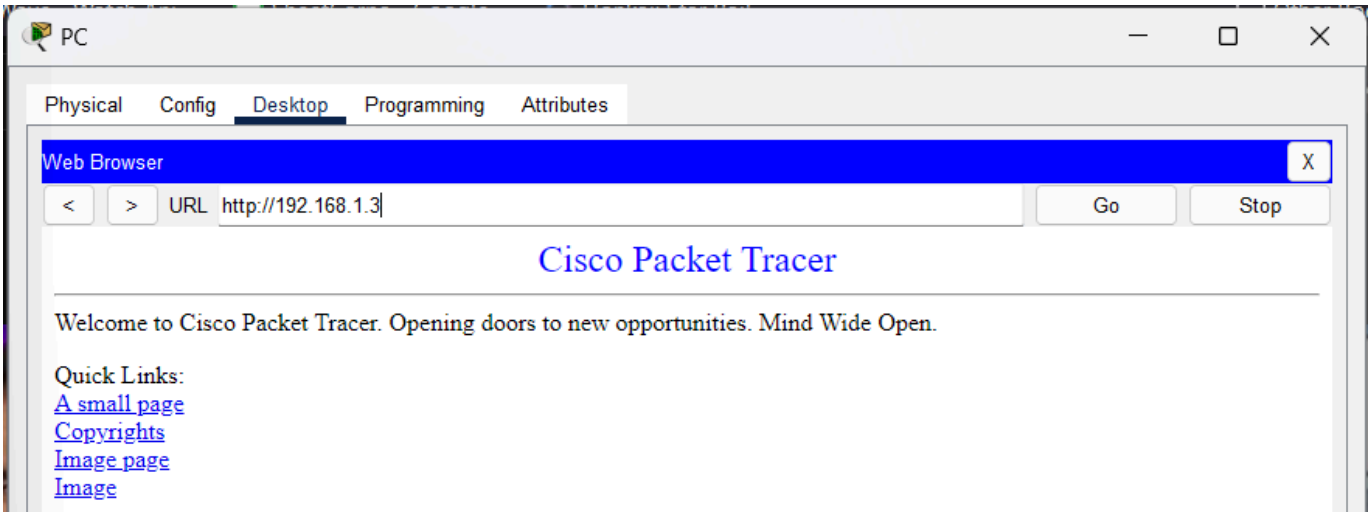
Create the Firewall Zones, Class Maps and ACLs on R3:

```
R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#zone security IN-ZONE
R3(config-sec-zone)#exit
R3(config)#zone security OUT-ZONE
R3(config-sec-zone)#exit
R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)#match access-group 101
R3(config-cmap)#exit
R3(config)#policy-map type inspect IN-2-OUT-PMAP
R3(config-pmap)#class type inspect IN-NET-CLASS-MAP
R3(config-pmap-c)#inspect
%No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols will be
inspected
R3(config-pmap-c)#exit
R3(config-pmap)#exit
R3(config)#zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
R3(config-sec-zone-pair)#service-policy type inspect IN-2-OUT-PMAP
R3(config-sec-zone-pair)#exit
R3(config)#interface GigabitEthernet0/0
R3(config-if)#zone-member security IN-ZONE
R3(config-if)#exit
R3(config)#interface Serial0/0/0
R3(config-if)#zone-member security OUT-ZONE
R3(config-if)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#exit
```

Test Firewall Functionality from IN-ZONE to OUT-ZONE:




```
R3>en
R3#show policy-map type inspect zone-pair sessions

policy exists on zp IN-2-OUT-ZPAIR
 Zone-pair: IN-2-OUT-ZPAIR

  Service-policy inspect : IN-2-OUT-PMAP

    Class-map: IN-NET-CLASS-MAP (match-all)
      Match: access-group 101
      Inspect

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```



Test the Firewall Functionality from OUT-ZONE to IN-ZONE:

```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
R2>ping 192.168.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```