

PRACTICAL NO 5: Configuring a Zone-Based Policy Firewall (ZPF)

Cisco IOS® Software Release 12.4(6)T introduced Zone-Based Policy Firewall (ZFW), a new configuration model for the Cisco IOS Firewall feature set. This new configuration model offers intuitive policies for multiple-interface routers, increased granularity of firewall policy application, and a default deny-all policy that prohibits traffic between firewall security zones until an explicit policy is applied to allow desirable traffic.

Nearly all classic Cisco IOS Firewall features implemented before Cisco IOS Software Release 12.4(6)T are supported in the new zone-based policy inspection interface:

- 1) Stateful packet inspection
- 2) VRF-aware Cisco IOS Firewall
- 3) URL filtering
- 4) Denial-of-Service (DoS) mitigation

Cisco IOS Software Release 12.4(9)T added ZFW support for per-class session/connection and throughput limits, as well as application inspection and control:

- 1) HTTP
- 2) Post Office Protocol (POP3),
- 3) Internet Mail Access Protocol (IMAP),
- 4) Simple Mail Transfer Protocol / Enhanced Simple Mail Transfer Protocol (SMTP/ESMTP)
- 5) Sun Remote Procedure Call (RPC)
- 6) Instant Messaging (IM) applications:
 - i) Microsoft Messenger
 - ii) Yahoo! Messenger
 - iii) AOL Instant Messenger
- 7) Peer-to-Peer (P2P) File Sharing:
 - i) Bittorrent
 - ii) KaZaA
 - iii) Gnutella
 - iv) eDonkey

Cisco IOS Software Release 12.4(11)T added statistics for easier DoS protection tuning.

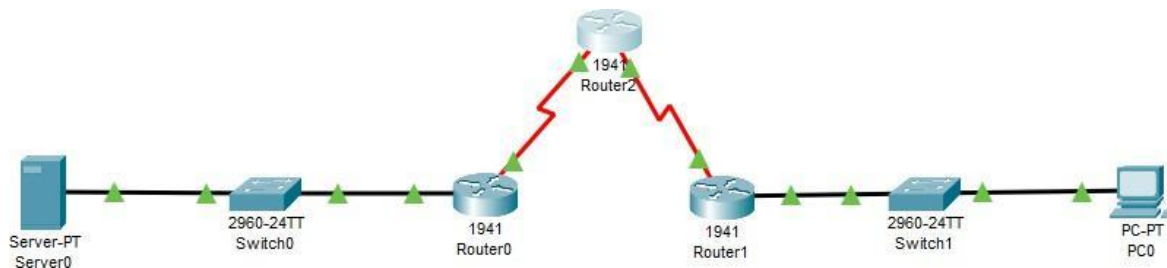
Some Cisco IOS Classic Firewall features and capabilities are not yet supported in a ZFW in Cisco IOS Software Release 12.4(15)T:

- i) Authentication proxy
- ii) Stateful firewall failover
- iii) Unified firewall MIB
- iv) IPv6 stateful inspection
- v) TCP out-of-order support



ZFW generally improves Cisco IOS performance for most firewall inspection activities. Neither Cisco IOS ZFW or Classic Firewall include stateful inspection support for multicast traffic.

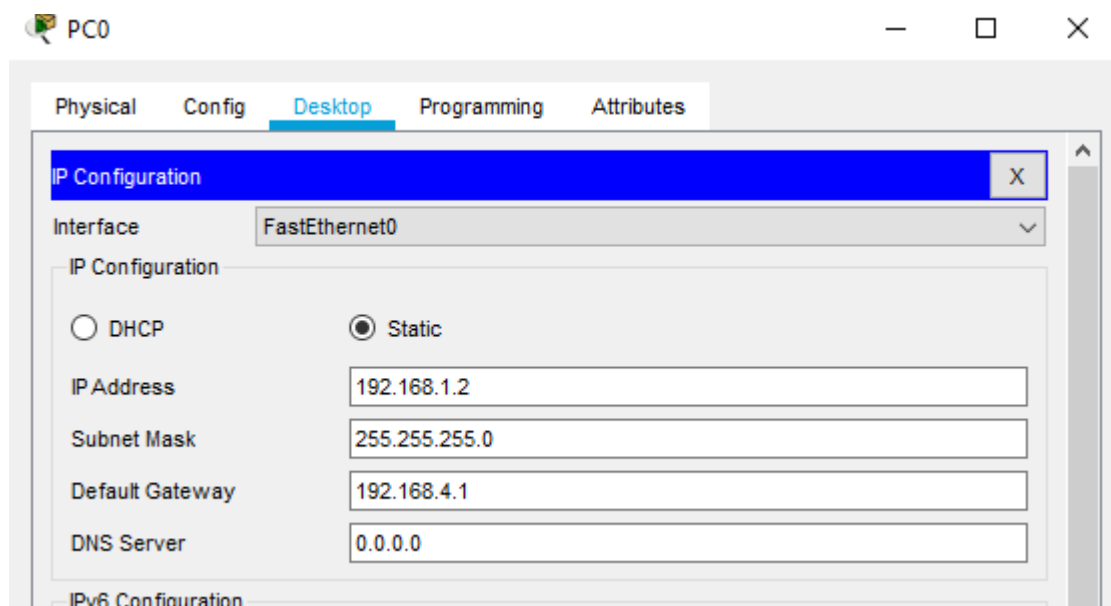
We use the following topology



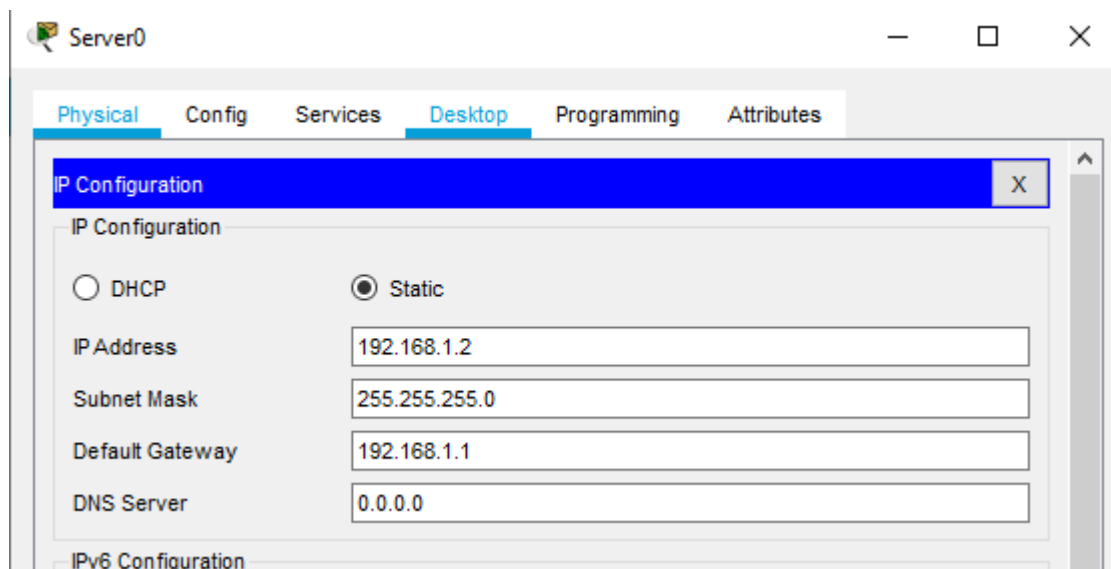
Let us consider the following Address table to configure the network devices:

Device	Interface	IP Address	Subnet Mask	Default gateway	Switch Port
PC 0	NA	192.168.4.2	255.255.255.0	192.168.4.1	Switch1 F0/1
Server0	NA	192.168.1.2	255.255.255.0	192.168.1.1	Switch0 F0/1
Router0	GE0/0	192.168.1.1	255.255.255.0	NA	Switch0 F0/5
	S0/1/0	192.168.2.1	255.255.255.0	NA	NA
Router2	S0/1/0	192.168.2.2	255.255.255.0	NA	NA
	S0/1/1	192.168.3.1	255.255.255.0	NA	NA
Router1	S0/1/1	192.168.3.2	255.255.255.0	NA	NA
	GE0/0	192.168.4.1	255.255.255.0	NA	Switch1 F0/5

Configuring PC0



Configuring Server0



Configuring Router0

Router0

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

GigabitEthernet0/0

Port Status ☒ On

Bandwidth ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 00D0.BABE.0E01

IP Configuration

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Router0

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

Serial0/1/0

Port Status ☒ On

Duplex ☒ Full Duplex

Clock Rate 2000000

IP Configuration

IP Address 192.168.2.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Configuring Router1

Router1

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

GigabitEthernet0/0

Port Status ☒ On

Bandwidth ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0001.4267.6A01

IP Configuration

IP Address 192.168.4.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Router1

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

Serial0/1/1

Port Status ☒ On

Duplex ☒ Full Duplex

Clock Rate 1200

IP Configuration

IP Address 192.168.3.2

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Configuring Router2

Router2

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

Serial0/1/0

Port Status ☒ On

Duplex ☐ Full Duplex

Clock Rate 1200

IP Configuration

IP Address 192.168.2.2

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Router2

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

Serial0/1/1

Port Status ☒ On

Duplex ☐ Full Duplex

Clock Rate 2000000

IP Configuration

IP Address 192.168.3.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Part 1: Static Routing

Static Routing is done using the following procedure for each Router

Router 0: Add the following in the Static mode of Router0

Type this

Click Add

The screenshot shows the Router0 configuration window with the 'Config' tab selected. On the left, the 'ROUTING' section is expanded, and 'Static' is selected. In the 'Static Routes' section, the 'Network' field is 192.168.3.0, 'Mask' is 255.255.255.0, and 'Next Hop' is 192.168.2.2. The 'Add' button is highlighted. Below, the 'Network Address' field displays '192.168.3.0/24 via 192.168.2.2'.

N/W address will be displayed here

Type this

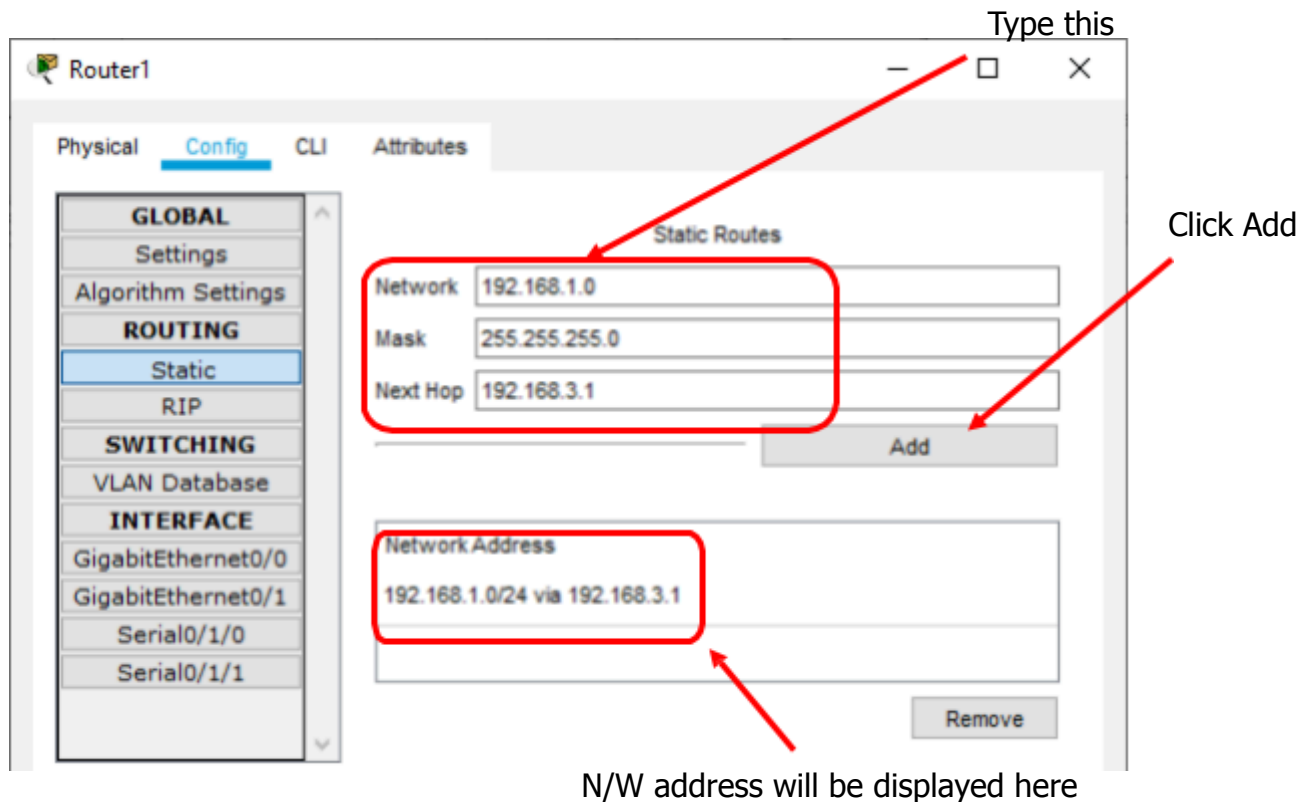
Click Add

The screenshot shows the Router0 configuration window with the 'Config' tab selected. On the left, the 'ROUTING' section is expanded, and 'Static' is selected. In the 'Static Routes' section, the 'Network' field is 192.168.4.0, 'Mask' is 255.255.255.0, and 'Next Hop' is 192.168.2.2. The 'Add' button is highlighted. Below, the 'Network Address' field displays two entries: '192.168.3.0/24 via 192.168.2.2' and '192.168.4.0/24 via 192.168.2.2'.

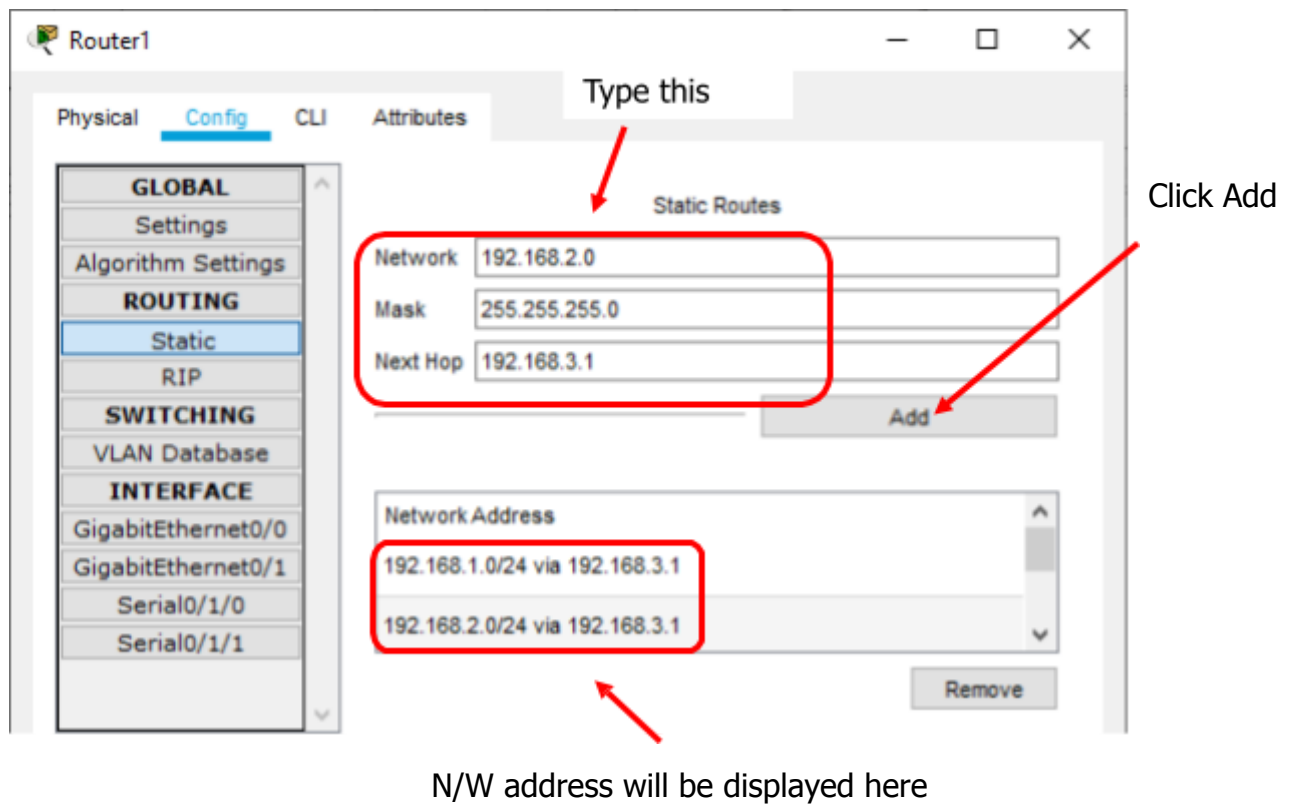
N/W address will be displayed here



Router 1: Add the following in the Static mode of Router1



The screenshot shows the Router1 configuration window with the 'Config' tab selected. The left sidebar shows the 'ROUTING' section with 'Static' selected. The 'Static Routes' section is active, showing fields for 'Network' (192.168.1.0), 'Mask' (255.255.255.0), and 'Next Hop' (192.168.3.1). A red box highlights these fields, with an arrow pointing to the text 'Type this'. Below the fields is an 'Add' button, with an arrow pointing to it from the text 'Click Add'. The 'Network Address' list below shows the added route: '192.168.1.0/24 via 192.168.3.1', which is highlighted by a red box with an arrow pointing to it from the text 'N/W address will be displayed here'.



The screenshot shows the Router1 configuration window with the 'Config' tab selected. The left sidebar shows the 'ROUTING' section with 'Static' selected. The 'Static Routes' section is active, showing fields for 'Network' (192.168.2.0), 'Mask' (255.255.255.0), and 'Next Hop' (192.168.3.1). A red box highlights these fields, with an arrow pointing to the text 'Type this'. Below the fields is an 'Add' button, with an arrow pointing to it from the text 'Click Add'. The 'Network Address' list below shows two routes: '192.168.1.0/24 via 192.168.3.1' and '192.168.2.0/24 via 192.168.3.1'. The second route is highlighted by a red box with an arrow pointing to it from the text 'N/W address will be displayed here'.

Router 2: Add the following in the Static mode of Router2

Type this

Router2

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

Static Routes

Network 192.168.1.0

Mask 255.255.255.0

Next Hop 192.168.2.1

Add

Network Address

192.168.1.0/24 via 192.168.2.1

Remove

Click Add

N/W address will be displayed here

Router2

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

Static Routes

Network 192.168.4.0

Mask 255.255.255.0

Next Hop 192.168.3.2

Add

Network Address

192.168.1.0/24 via 192.168.2.1

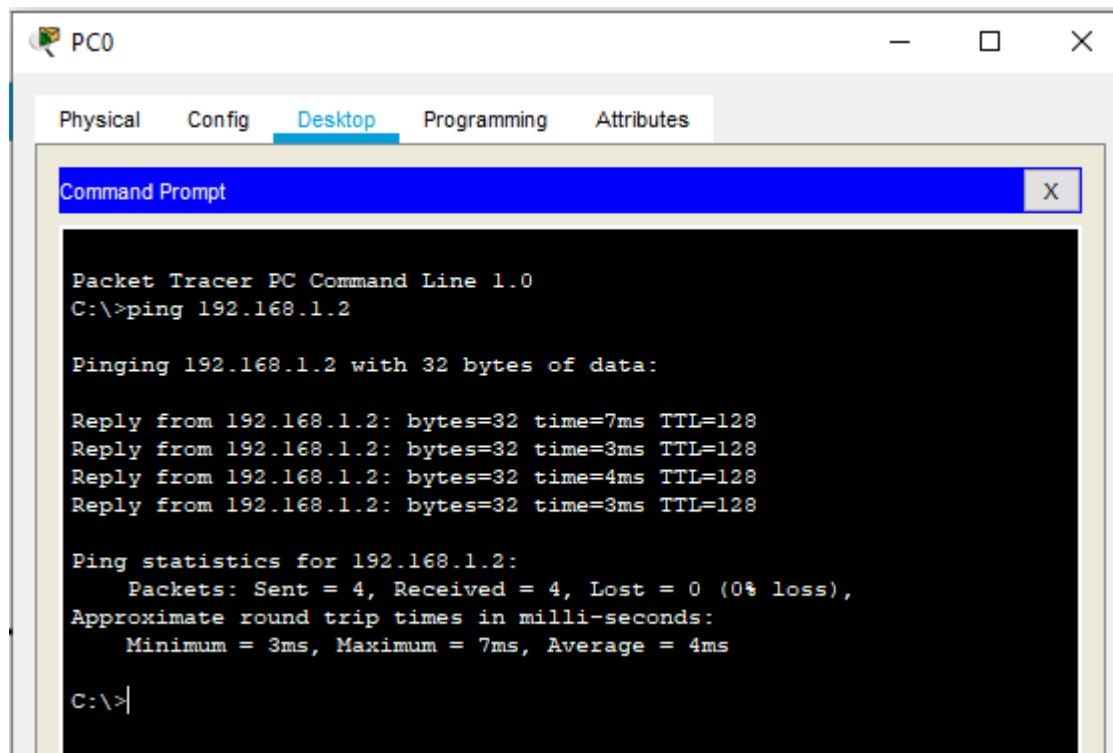
192.168.4.0/24 via 192.168.3.2

Remove

Click Add

N/W address will be displayed here

Now we check the connectivity by pinging the Server from the PC and from PC to Server



The screenshot shows a Packet Tracer PC configuration window for PC0. The 'Desktop' tab is selected, and a Command Prompt window is open. The Command Prompt displays the output of a ping command to 192.168.1.2. The output shows four successful replies with varying round-trip times (3ms to 7ms) and a 0% loss rate. The ping statistics confirm that all four packets were received.

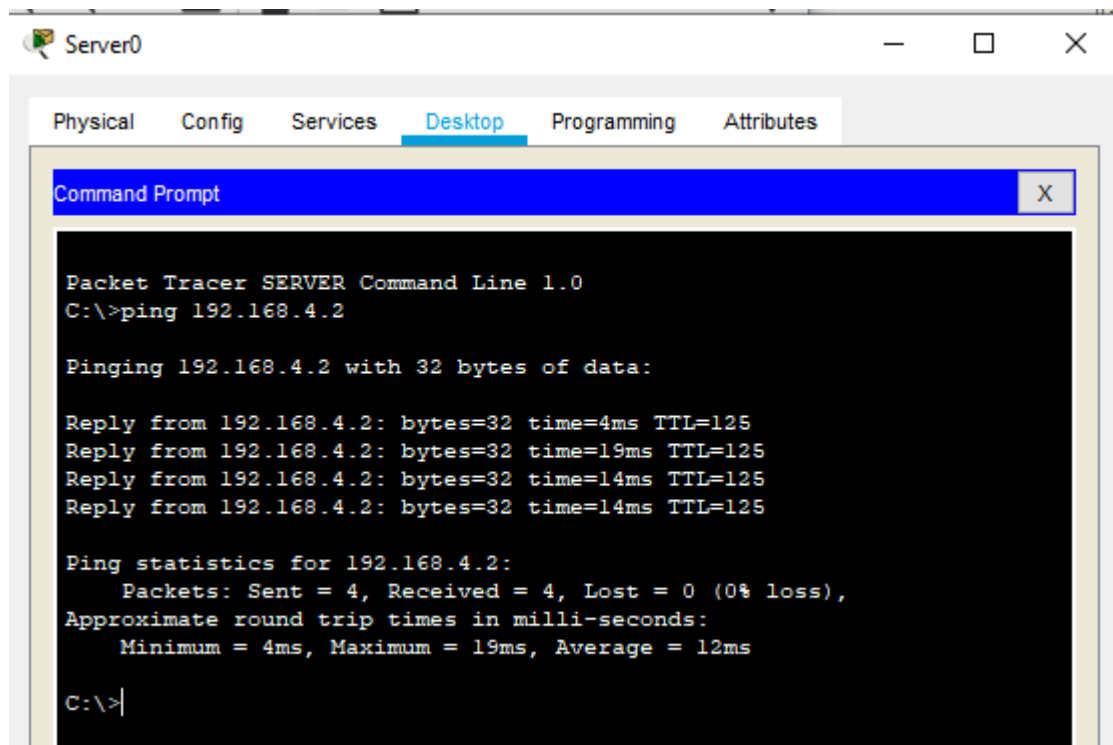
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=7ms TTL=128
Reply from 192.168.1.2: bytes=32 time=3ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128
Reply from 192.168.1.2: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 7ms, Average = 4ms

C:\>|
```



The screenshot shows a Packet Tracer Server configuration window for Server0. The 'Desktop' tab is selected, and a Command Prompt window is open. The Command Prompt displays the output of a ping command to 192.168.4.2. The output shows four successful replies with varying round-trip times (4ms to 19ms) and a 0% loss rate. The ping statistics confirm that all four packets were received.

```
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time=4ms TTL=125
Reply from 192.168.4.2: bytes=32 time=19ms TTL=125
Reply from 192.168.4.2: bytes=32 time=14ms TTL=125
Reply from 192.168.4.2: bytes=32 time=14ms TTL=125

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 19ms, Average = 12ms

C:\>|
```

Part 2: Configuring SSH on Router 2

Type the following commands in the CLI mode of Router2

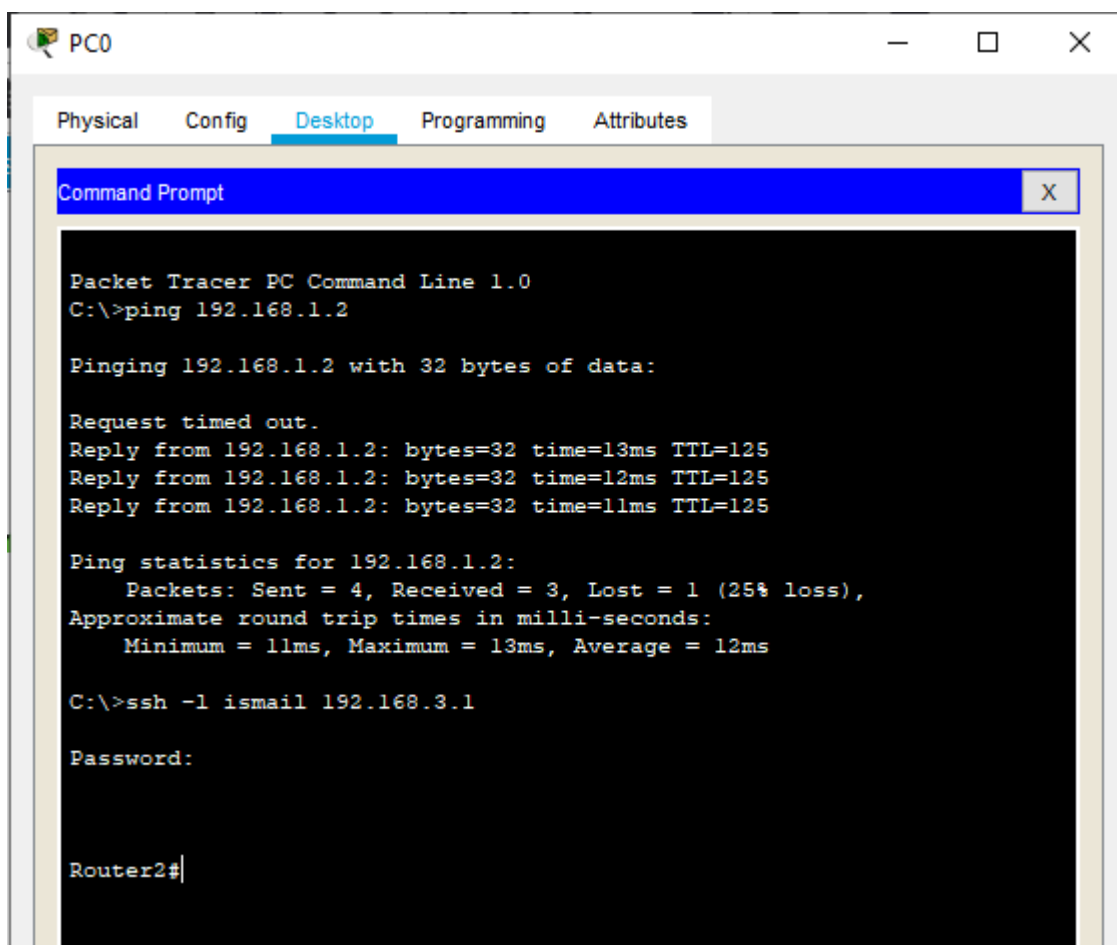
```
Router>enable
Router#configure terminal
Router(config)#ip domain-name .com
Router(config)#hostname Router2
Router2(config)#crypto key generate rsa
```

```
Router2 (config)#line vty 0 4
Router2 (config-line)#transport input ssh
Router2 (config-line)#login local
Router2 (config-line)#exit
```

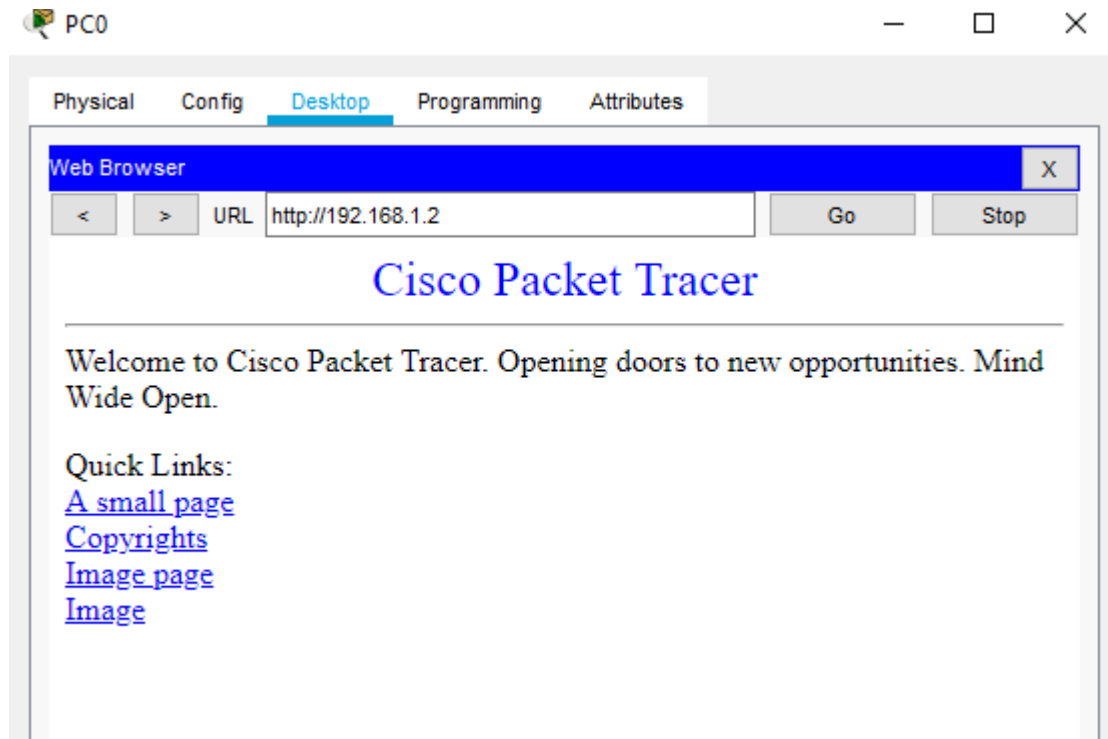
```
Router2 (config)#username ismail privilege 15 password cisco
```

Now verify ssh from PC0 by typing the following command

```
ssh -l ismail 192.168.3.1
```



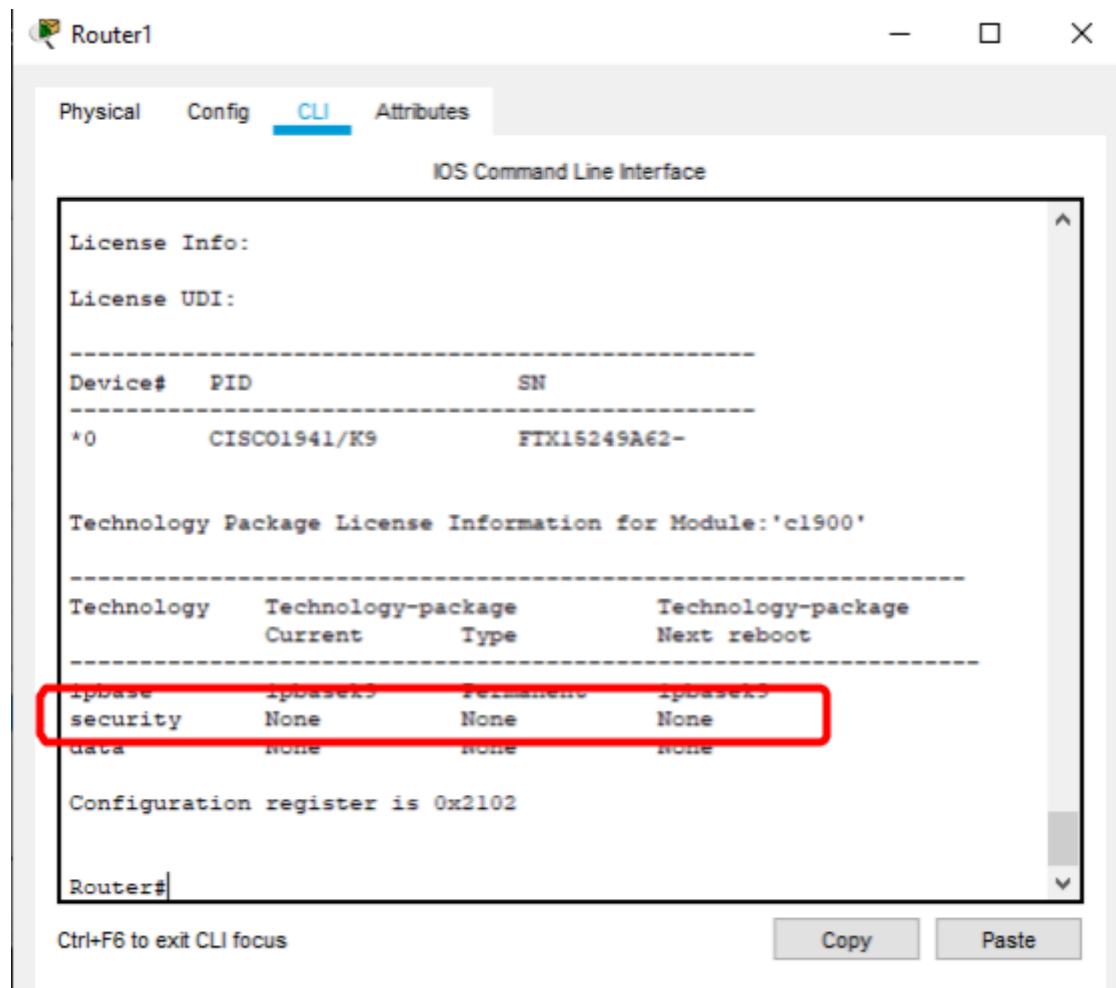
Next we access the web services of the Server using the web browser of PC using the following



Part 3: Create the Firewall Zones on Router1

Type the following commands in the CLI mode of Router1

```
Router>enable  
Router#configure terminal  
Router(config)#show version
```



```
Router#configure terminal  
Router (config)#license boot module c1900 technology-package securityk9  
ACCEPT? [yes/no]: y
```

```
Router(config)#exit  
Router>enable
```

```
Router#reload  
Router>enable
```


Router#show version



Router# Router#configure
terminal

Router(config)#zone security in-zone
Router(config-sec-zone)#exit

Router(config)#zone security out-zone
Router(config-sec-zone)#exit

Router(config)#access-list 101 permit ip
192.168.4.0 0.0.0.255 any Router(config)#class-
map type inspect match-all in-map Router(config-
cmap)#match access-group 101
Router(config-cmap)#exit

Router(config)#policy-map type
inspect in-out Router(config-
pmap)#class type inspect in-



```
map Router(config-pmap-  
c)#inspect  
Router(config-pmap-c)#exit  
Router(config-pmap)#exit  
Router(config)#
```

```
Router(config)#zone-pair security in-out-zone source in-zone destination out-zone  
Router(config-sec-zone-pair)#service-policy type inspect in-out  
Router(config-sec-zone-pair)#exit  
Router(config)#
```

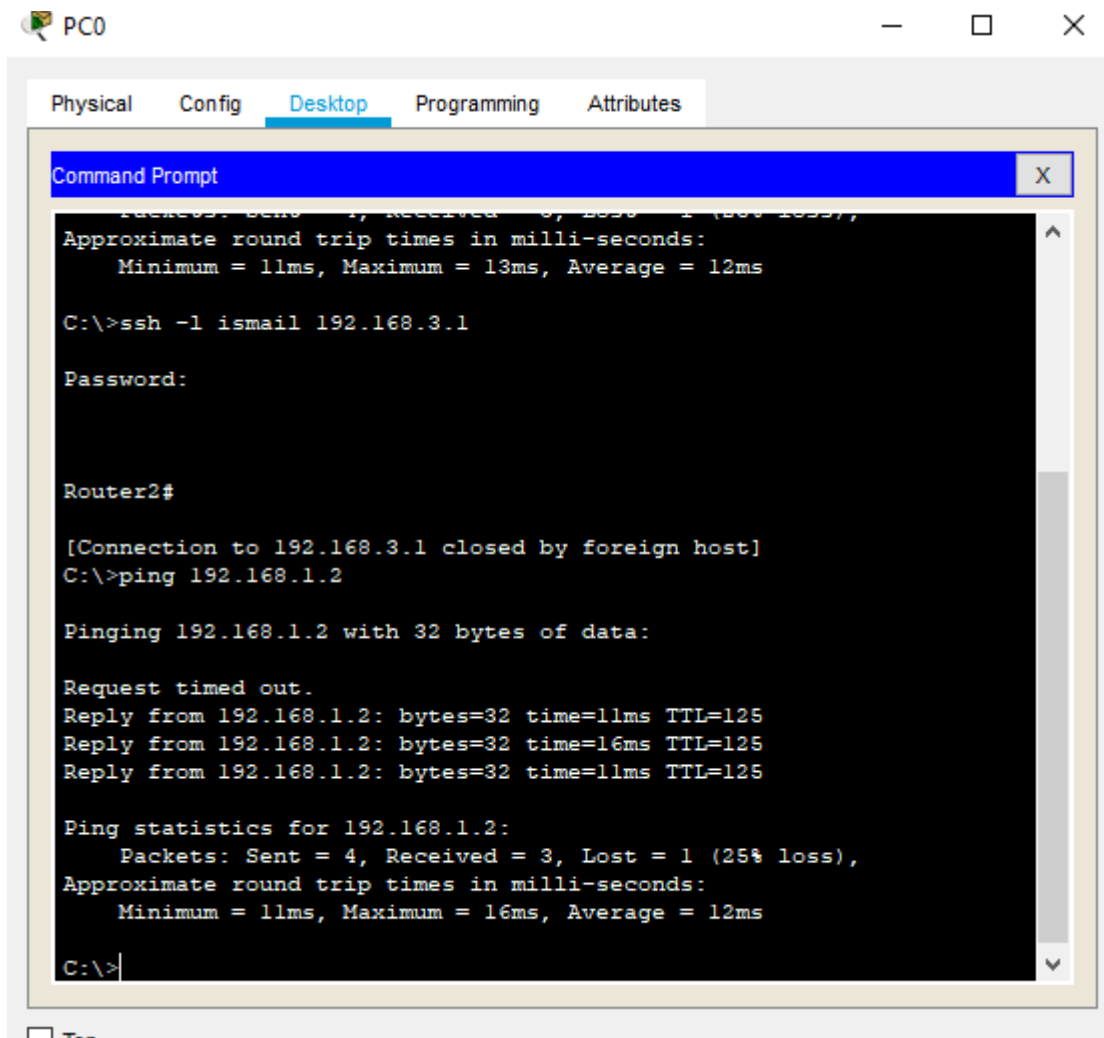
```
Router(config)#interface GigabitEthernet0/0  
Router(config-if)#zone-member security in-zone  
Router(config-if)#exit  
Router(config)#
```

```
Router(config)#interface Serial0/1/1  
Router(config-if)#zone-member security out-zone  
Router(config-if)#exit  
Router(config)#exit
```

```
Router#copy running-config startup-config
```

Part 4: Testing the Firewall Functionality (from in-zone to out-zone) by the following steps

Step 1: Pinging SERVER from PC (it will succeed)



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
  Minimum = 11ms, Maximum = 13ms, Average = 12ms

C:\>ssh -l ismail 192.168.3.1

Password:

Router2#

[Connection to 192.168.3.1 closed by foreign host]
C:\>ping 192.168.1.2

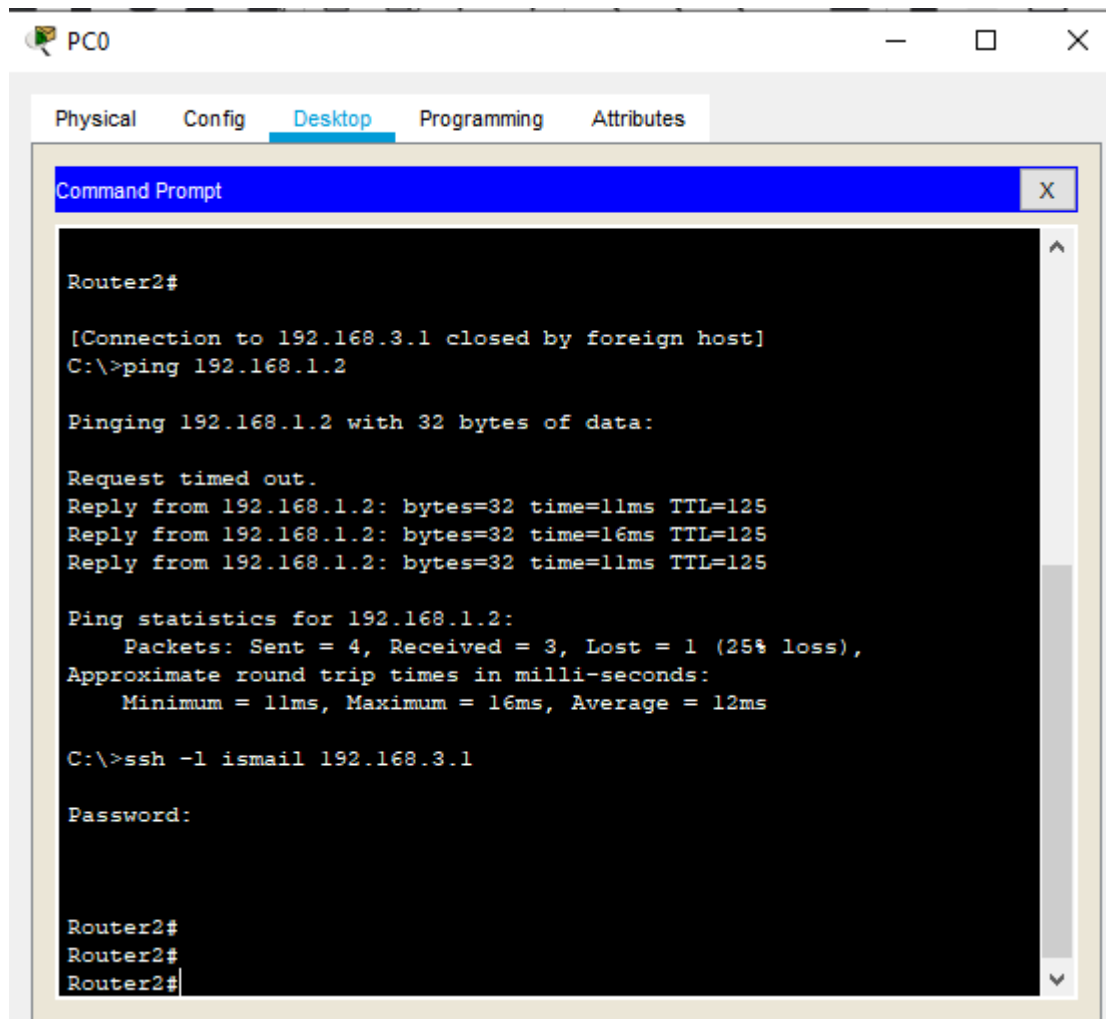
Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=11ms TTL=125
Reply from 192.168.1.2: bytes=32 time=16ms TTL=125
Reply from 192.168.1.2: bytes=32 time=11ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 16ms, Average = 12ms

C:\>
```



Step 2: Start an SSH session from PC to Router 2 (192.168.3.1)

The screenshot shows a PC0 desktop environment with a window titled 'PC0'. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The window contains the following text:

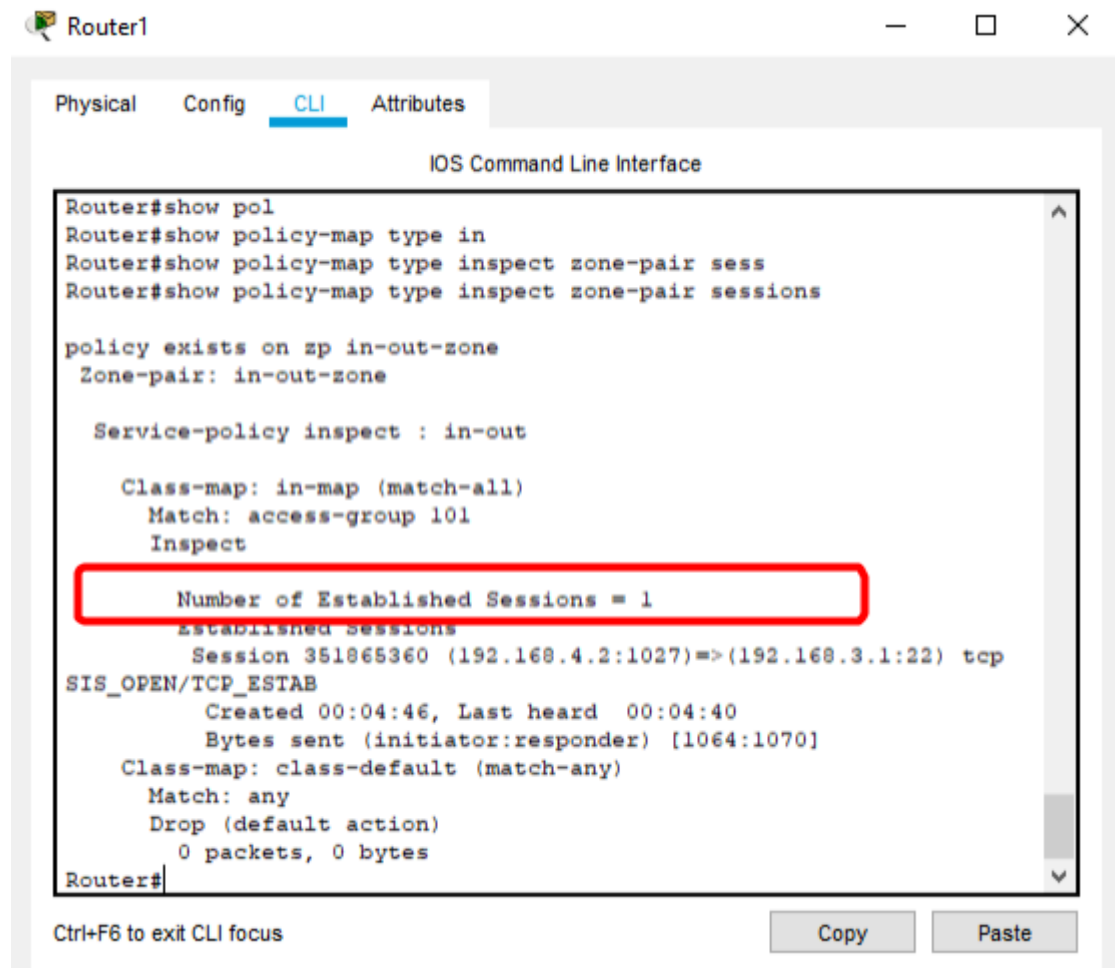
```
Router2#  
  
[Connection to 192.168.3.1 closed by foreign host]  
C:\>ping 192.168.1.2  
  
Pinging 192.168.1.2 with 32 bytes of data:  
  
Request timed out.  
Reply from 192.168.1.2: bytes=32 time=11ms TTL=125  
Reply from 192.168.1.2: bytes=32 time=16ms TTL=125  
Reply from 192.168.1.2: bytes=32 time=11ms TTL=125  
  
Ping statistics for 192.168.1.2:  
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 11ms, Maximum = 16ms, Average = 12ms  
  
C:\>ssh -l ismail 192.168.3.1  
  
Password:  
  
Router2#  
Router2#  
Router2#
```

As seen above the session becomes active and we get access to Router2 (Do not exit and the session and continue to Step 3)

Step 3: Type the following command in the CLI mode of Router1

Router#show policy-map type inspect zone-pair sessions

We will get the following output



Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router#show pol
Router#show policy-map type in
Router#show policy-map type inspect zone-pair sess
Router#show policy-map type inspect zone-pair sessions

policy exists on zp in-out-zone
Zone-pair: in-out-zone

Service-policy inspect : in-out

Class-map: in-map (match-all)
Match: access-group 101
Inspect

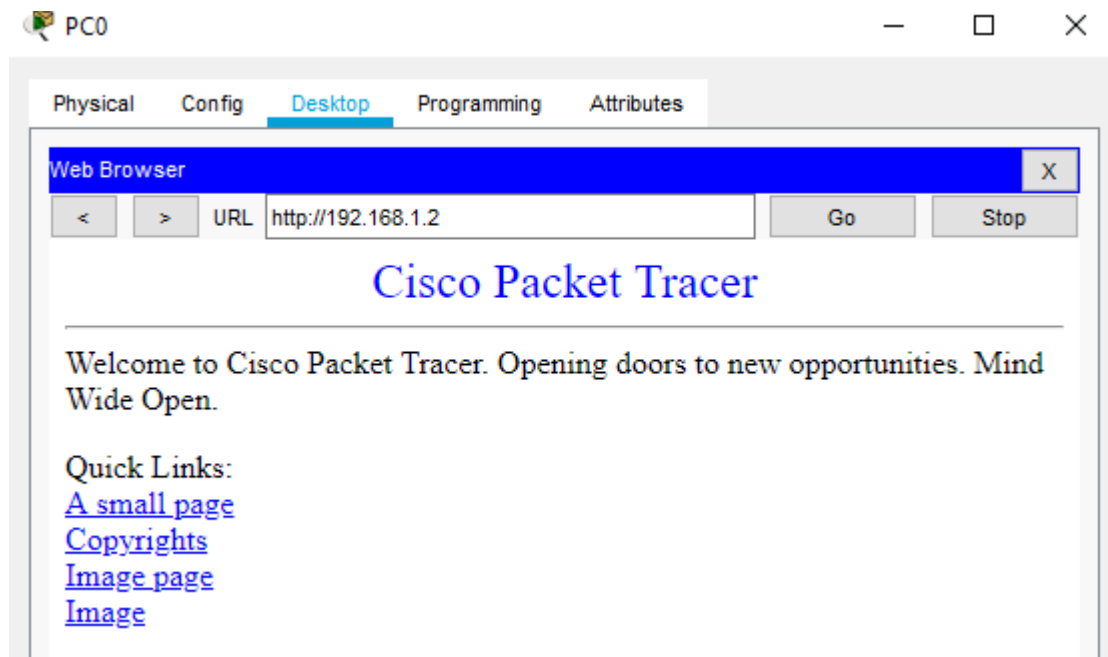
Number of Established Sessions = 1
Established Sessions
Session 351865360 (192.168.4.2:1027)=>(192.168.3.1:22) tcp
SIS_OPEN/TCP_ESTAB
Created 00:04:46, Last heard 00:04:40
Bytes sent (initiator:responder) [1064:1070]
Class-map: class-default (match-any)
Match: any
Drop (default action)
0 packets, 0 bytes
Router#
```

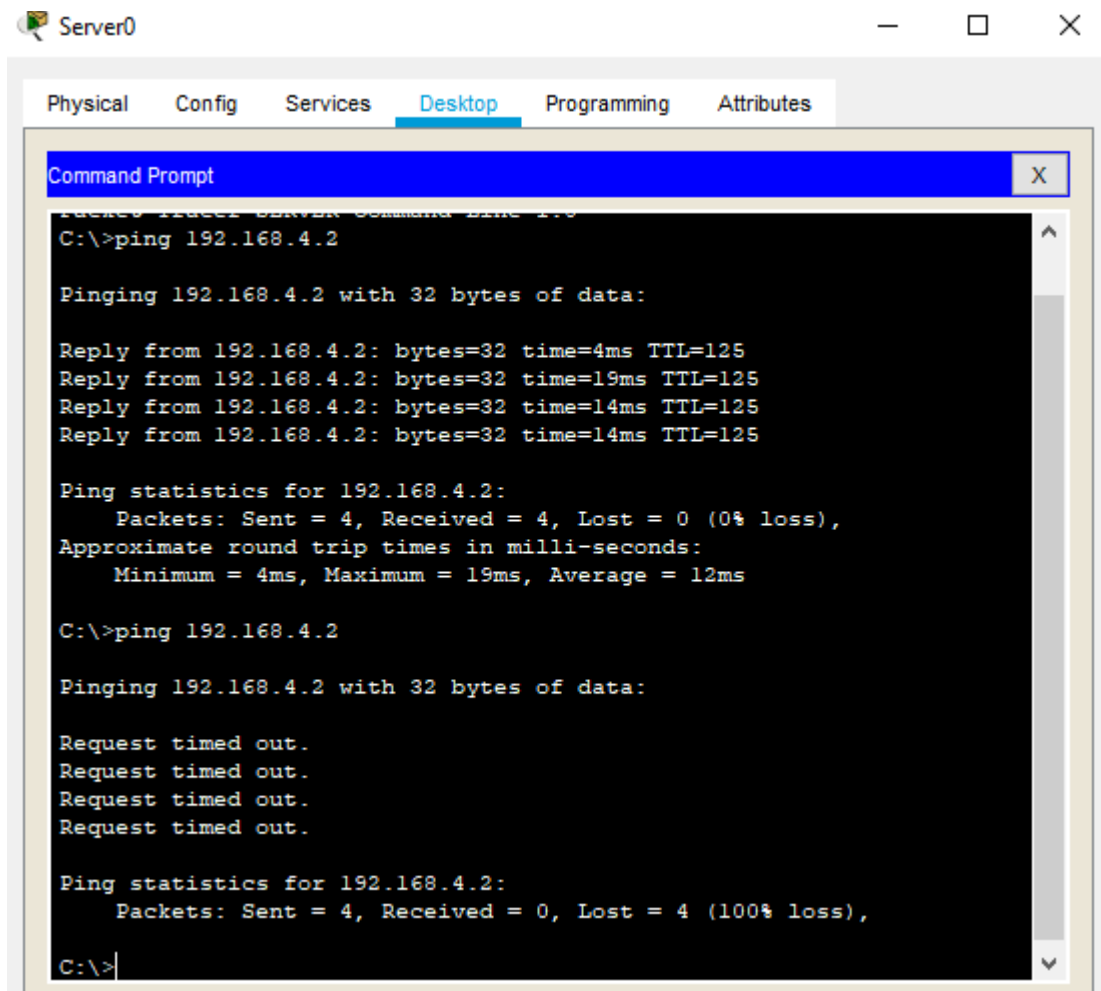
Ctrl+F6 to exit CLI focus

Copy Paste



Step 4: We close the SSH connection and open the web browser and access the server address (192.168.1.2) and get the following



Part 5: Testing the Firewall Functionality (from out-zone to in-zone) by the following steps**Step 1: Ping PC0 from the SERVER (ip 192.168.4.2) (it will result in Failure)**

Hence the Firewall functionality has been verified