Lab 07

Configuring a Zone-Based Policy Firewall (ZPF)

Name: Syed Asghar Abbas Zaidi	**Student ID: 07201**

7.1 Objective

The Objectives of this lab are:

- Verify connectivity among devices before firewall configuration.
- Configure a zone-based policy (ZPF) firewall on R3.
- Verify ZPF firewall functionality using ping, SSH (Secure Shell), and a web browser

ZPFs are the latest development in the evolution of Cisco firewall technologies. In this activity, you will configure a basic ZPF on an edge router R3 that allows internal hosts access to external resources and blocks external hosts from accessing internal resources. You will then verify firewall functionality from internal and external hosts.

The routers have been pre-configured with the following:

- Console password: **ciscoconpa55**
- Password for vty lines: **ciscovtypa55**
- Enable password: **ciscoenpa55**
- Host names and IP addressing
- Local username and password: **Admin** / **Adminpa55**
- Static routing

Topology

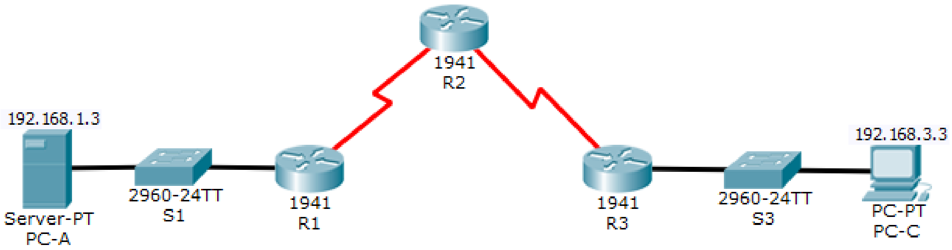


Figure 1: Topology

Addressing Table

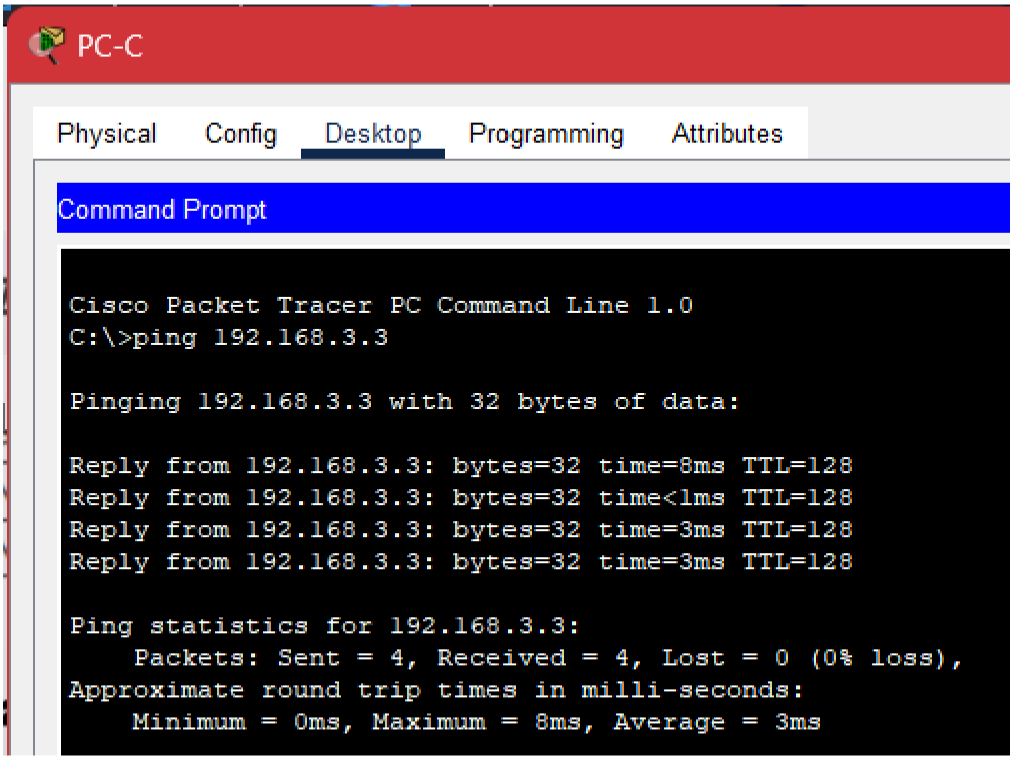
Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Table 1: Addressing Table

Task 1: Verify Basic Network Connectivity

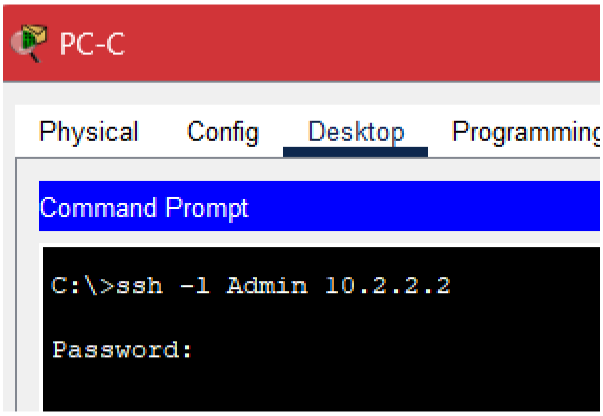
Verify network connectivity prior to configuring the zone-based-policy firewall.

1. From the PC-A command prompt, ping PC-C at 192.168.3.3



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=8ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time=3ms TTL=128
Reply from 192.168.3.3: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 3ms
```

2. Access R2 using SSH.
   a. From the **PC-C** command prompt, SSH to the S0/0/1 interface on **R2** at **10.2.2.2**. Use the username **Admin** and password **Adminpa55** to log in.

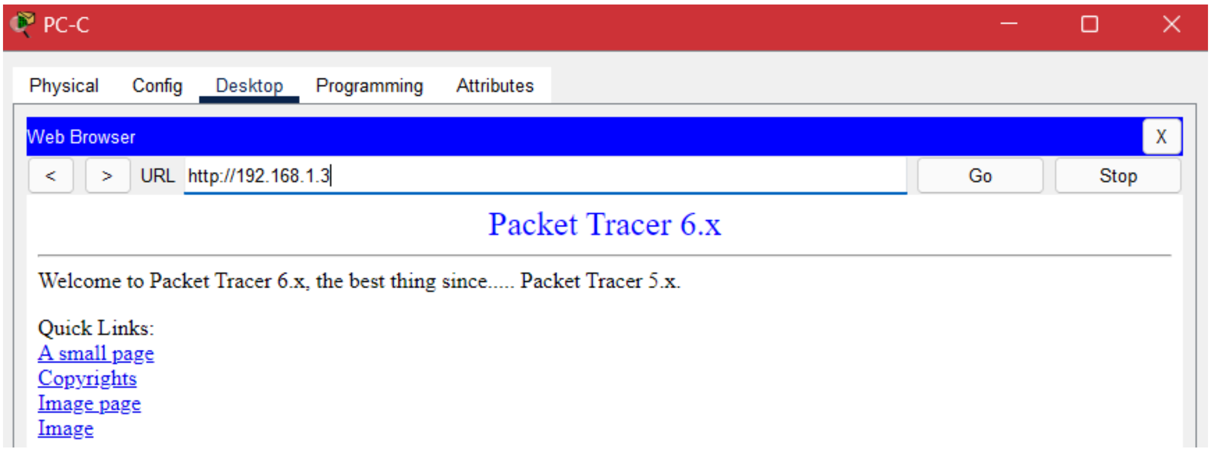


```
C:\>ssh -l Admin 10.2.2.2

Password:
```

b. Exit the SSH session.

3. From PC-C, open a web browser to the PC-A server.

   a. Click the **Desktop** tab and then click the **Web Browser** application. Enter the **PC-A** IP address **192.168.1.3** as the URL. The Packet Tracer welcome page from the web server should be displayed.



http://192.168.1.3

Packet Tracer 6.x

Welcome to Packet Tracer 6.x, the best thing since..... Packet Tracer 5.x.

Quick Links:
A small page
Copyrights
Image page
Image

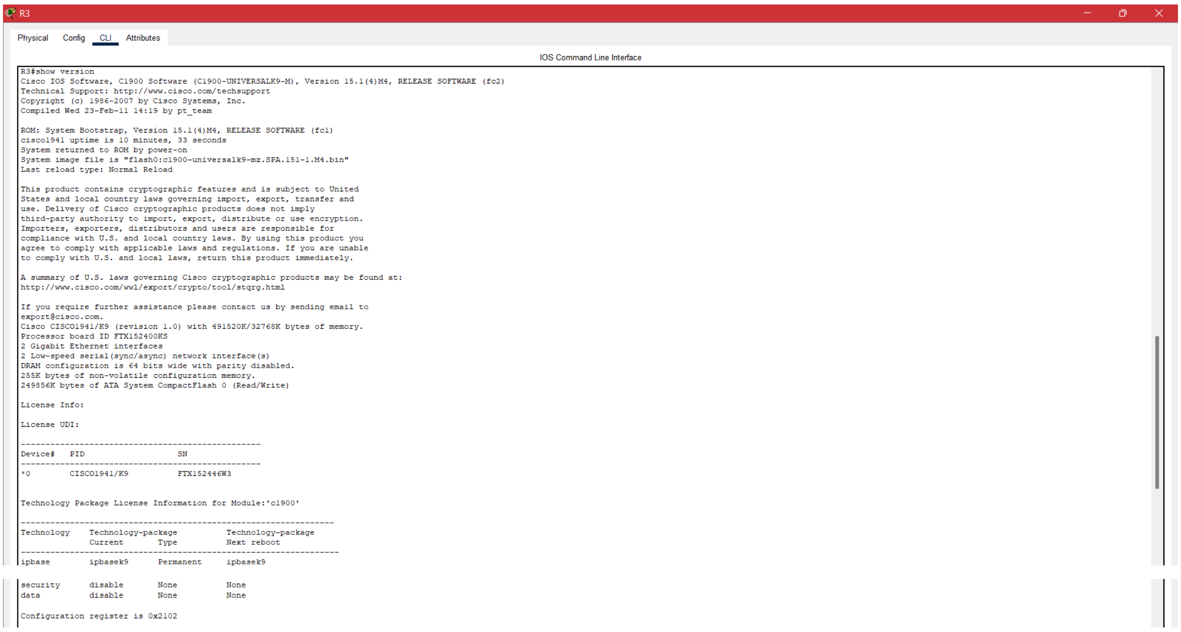
   b. Close the browser on **PC-C.**

Task 2: Create the Firewall Zones on R3

Note: For all configuration tasks, be sure to use the exact names as specified.

1. Enable the Security Technology package.

   a. On R3, issue the show version command to view the Technology Package license information.



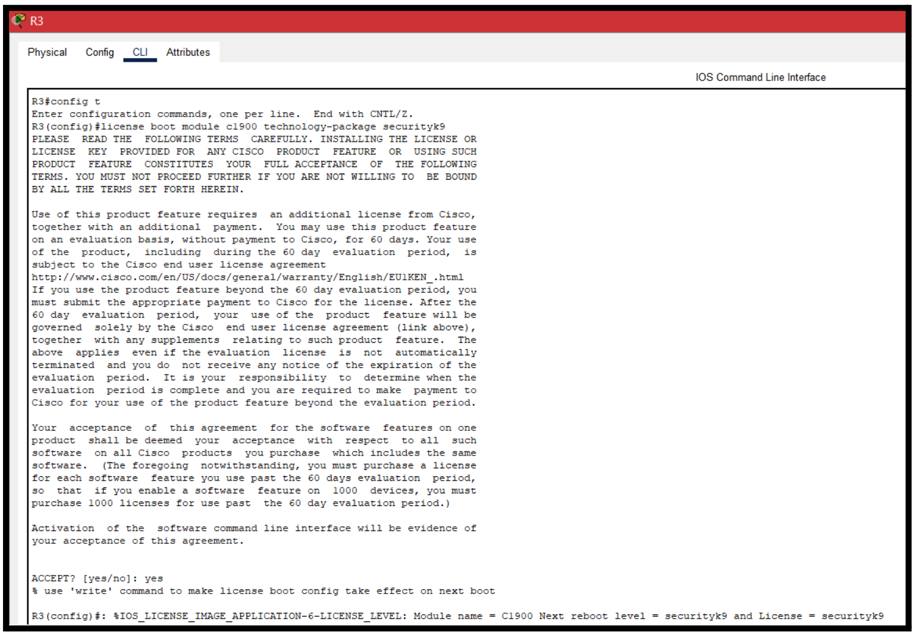
```
R3#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 10 minutes, 33 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX152446W3


Technology Package License Information for Module:'c1900'

----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9

security      disable       None          None
data          disable       None          None

Configuration register is 0x2102
```

The `show version` output for R3 indicates that the IP Base technology package (`ipbasek9`) is currently enabled and licensed as a permanent feature. However, the security and data technology packages are both disabled and unlicensed, meaning that their respective features are not available for use on the device.

b. If the Security Technology package has not been enabled, use the following command to enable the package.

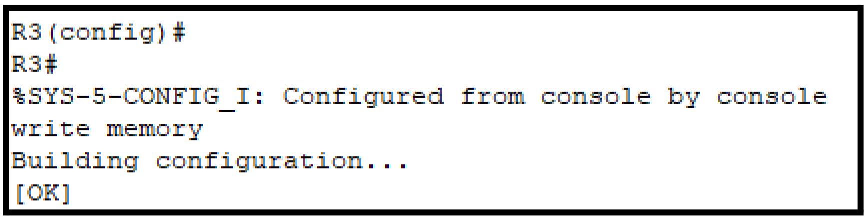
```
R3(config)# license boot module c1900 technology-package securityk9
```

c. Accept the end-user license agreement.



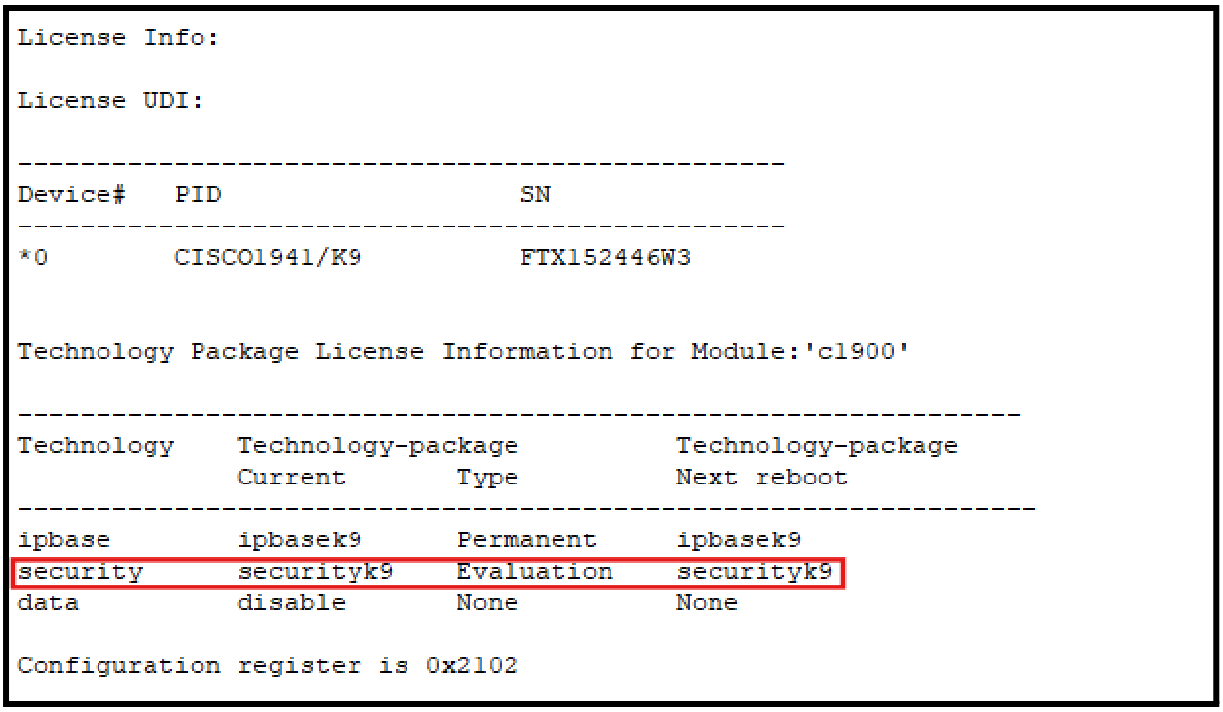
```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period.  It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot

R3(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900 Next reboot level = securityk9 and License = securityk9
```

d. Save the running-config and reload the router to enable the security license.



```
R3(config)#
R3#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
```

e. Verify that the Security Technology package has been enabled by using the show version command

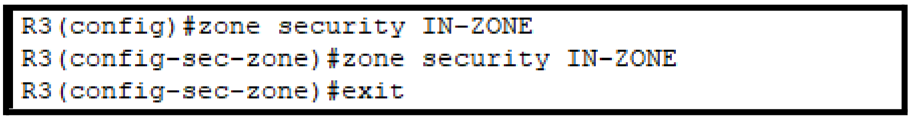


```
License Info:

License UDI:

-------------------------------------------------
Device#   PID                  SN
-------------------------------------------------
*0        CISCO1941/K9         FTX152446W3


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
```

2. Create an internal zone.

Use the zone security command to create a zone named **IN-ZONE.**

```
R3(config)# zone security IN-ZONE

R3(config-sec-zone) exit
```



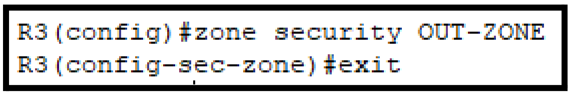
```
R3(config)#zone security IN-ZONE
R3(config-sec-zone)#zone security IN-ZONE
R3(config-sec-zone)#exit
```

3. Create an external zone.

Use the zone security command to create a zone named **OUT-ZONE.**

```
R3(config-sec-zone)# zone security OUT-ZONE
```

```
R3(config-sec-zone)# exit
```



```
R3(config)#zone security OUT-ZONE
R3(config-sec-zone)#exit
```

Task 3: Identify Traffic Using a Class-Map

1. Create an ACL that defines internal traffic.

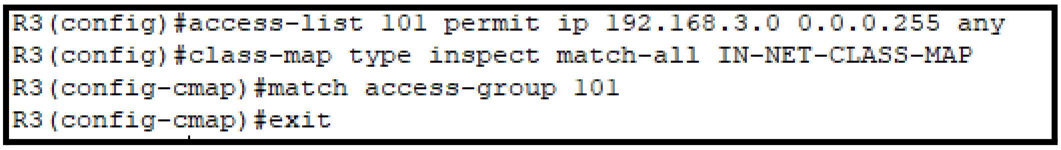
   Use the **access-list** command to create extended ACL **101** to permit all IP protocols from the **192.168.3.0/24** source network to any destination.

   ```
   R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 any
   ```

2. Create a class map referencing the internal traffic ACL.

   Use the class-map type inspect command with the match-all option to create a class map named **IN-NET-CLASS-MAP.** Use the **match access-group** command to match ACL **101**.

   ```
   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)#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
```

The command `class-map type inspect match-all IN-NET-CLASS-MAP` is used in Cisco IOS to define a class map for traffic classification, specifically for an inspection policy. This command creates a new class map named `IN-NET-CLASS-MAP` that matches all traffic types (as indicated by `match-all`), meaning that any traffic that meets the specified match criteria defined later in the configuration will be included in this class. The `type inspect` designation indicates that this class map is intended for use with the Modular QoS Command Line Interface (MQC) to support Layer 7 application inspection, which allows the router or switch to evaluate and manage traffic based on application-level attributes. This configuration is essential for implementing policies such as traffic shaping, access control, or QoS, enabling more granular control over how different types of network traffic are handled.

Task 4: Specify Firewall Policies

1. Create a policy map to determine what to do with matched traffic.

   Use the **policy-map type inspect** command and create a policy map named **IN-2-OUT-PMAP**.

   ```
   R3(config)# policy-map type inspect IN-2-OUT-PMAP
   ```

2. Specify a class type of inspect and reference class map IN-NET-CLASS-MAP.

   ```
   R3(config-pmap)# class type inspect IN-NET-CLASS-MAP
   ```

3. Specify the action of inspect for this policy map.

   The use of the **inspect** command invokes context-based access control (other options include pass and drop).

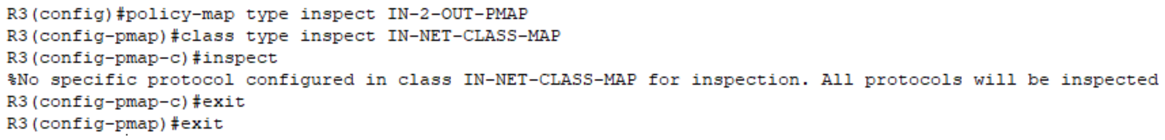
   ```
   R3(config-pmap-c)# inspect
   ```

   %No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols will be inspected.

   Issue the **exit** command twice to leave **config-pmap-c** mode and return to **config** mode.

   ```
   R3(config-pmap-c)# exit
   ```

   ```
   R3(config-pmap)# 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
```

In the provided sequence of commands, we are configuring a policy map on Cisco router R3 to manage traffic inspection for firewall policies. First, we enter global configuration mode to access the router's settings. Then, we create a new policy map named IN-2-OUT-PMAP, which is designated for traffic inspection.

This map references an existing class map called IN-NET-CLASS-MAP, which defines specific traffic flows that you want to monitor. By issuing the inspect command, you instruct the router to analyze and monitor the matched traffic rather than simply allowing it to pass through or dropping it; this action is part of context-based access control (CBAC) that enhances security by allowing for deeper inspection of packets.

After setting the inspection action, you exit the class configuration mode to return to global configuration mode. The purpose of this setup is to enable the router to enforce security checks and apply rules based on the characteristics of the incoming traffic, thereby improving overall network security and traffic management.

A warning message indicates that no specific protocols have been defined for inspection, meaning that all protocols matching the class map will be inspected by default, ensuring comprehensive traffic monitoring without protocol-specific filtering.

Task 5: Apply Firewall Policies

1. **Create a pair of zones.**

   Using the **zone-pair security** command, create a zone pair named **IN-2-OUT-ZPAIR**. Specify the source and destination zones that were created in Task 1.

   ```
   R3(config)# zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination
   OUT-ZONE
   ```

2. **Specify the policy map for handling the traffic between the two zones.**

   Attach a policy-map and its associated actions to the zone pair using the **service-policy type inspect** command and reference the policy map previously created, **IN-2-OUT-PMAP**.

   ```
   R3(config-sec-zone-pair)# service-policy type inspect IN-2-OUT-PMAP

   R3(config-sec-zone-pair)# exit

   R3(config)#
   ```

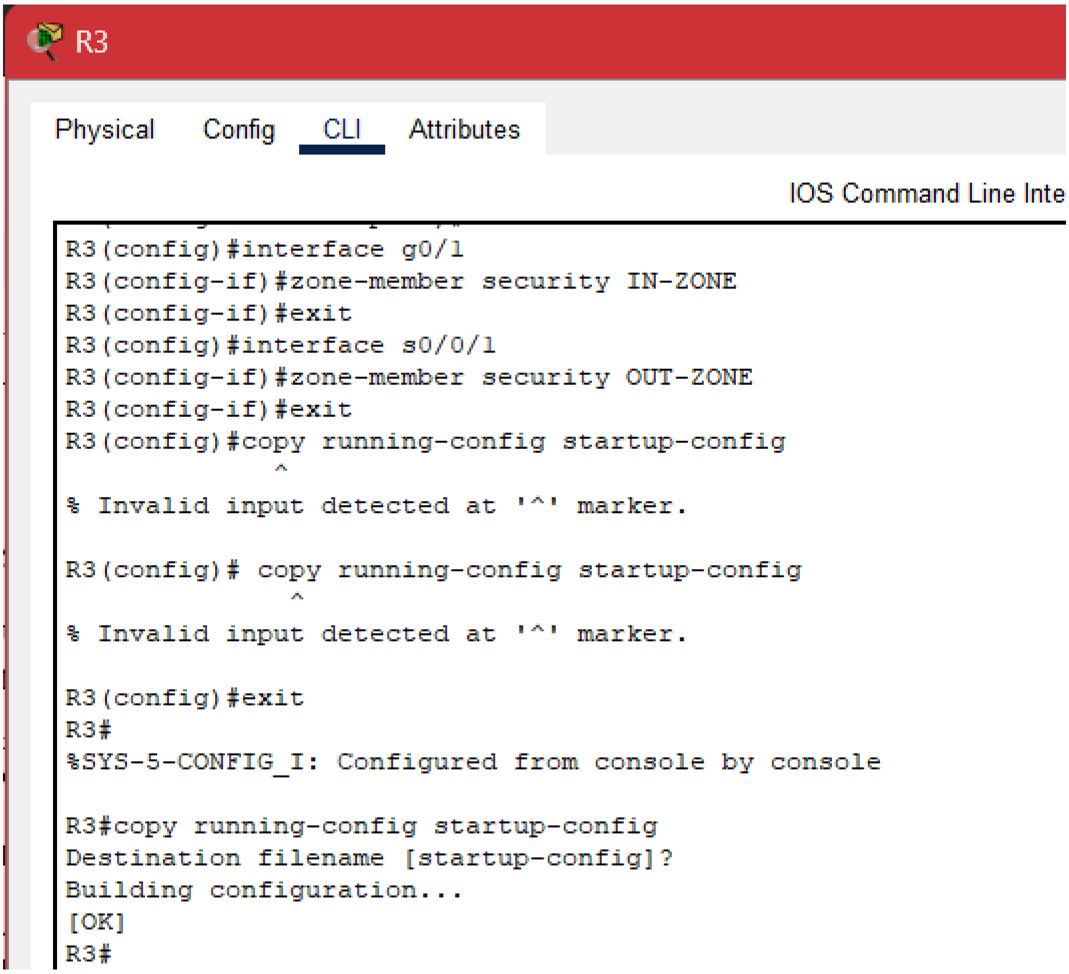
3. **Assign interfaces to the appropriate security zones.**

   Use the zone-member security command in interface configuration mode to assign G0/1 to IN-ZONE and S0/0/1 to OUT-ZONE.

   ```
   R3(config)# interface g0/1

   R3(config-if)# zone-member security IN-ZONE

   R3(config-if)# exit

   R3(config)# interface s0/0/1

   R3(config-if)# zone-member security OUT-ZONE
   ```

```
R3(config-if)# exit
```

4. Copy the running configuration to the startup configuration.



```
R3(config)#interface g0/1
R3(config-if)#zone-member security IN-ZONE
R3(config-if)#exit
R3(config)#interface s0/0/1
R3(config-if)#zone-member security OUT-ZONE
R3(config-if)#exit
R3(config)#copy running-config startup-config
             ^
% Invalid input detected at '^' marker.

R3(config)# copy running-config startup-config
              ^
% Invalid input detected at '^' marker.

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#
```

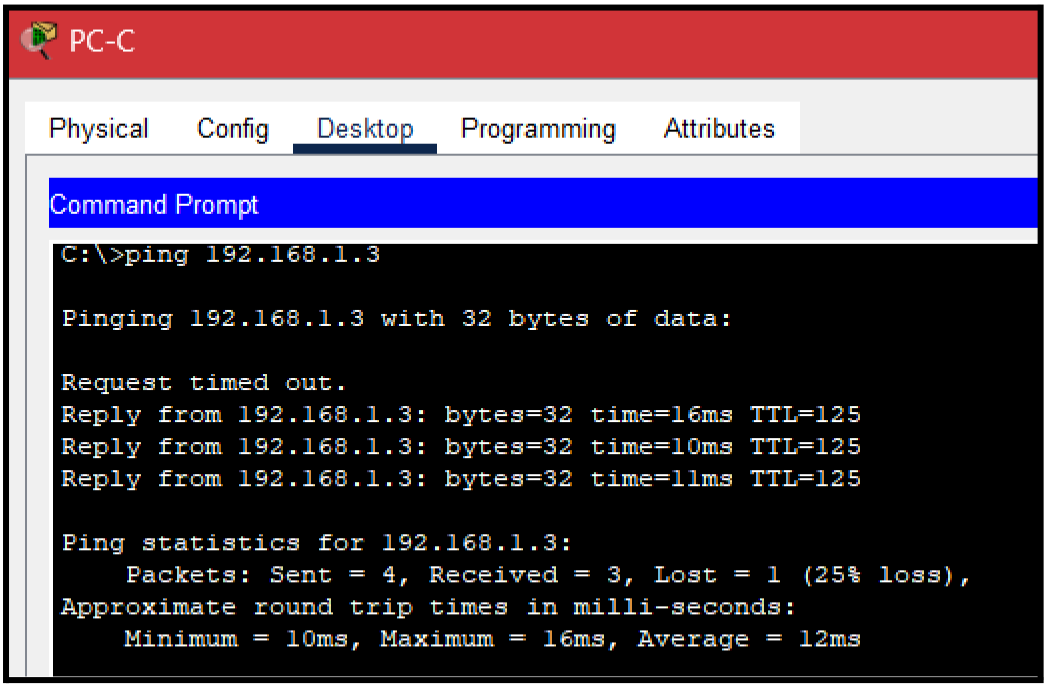
In this sequence of commands, we are configuring two interfaces on the Cisco router R3 to assign them to specific security zones, which help manage traffic and apply security policies. First, we enter the configuration for interface G0/1, where we specify that this interface belongs to the `IN-ZONE`. This means that any traffic coming through G0/1 will be treated according to the rules and policies defined for the `IN-ZONE`. After completing this assignment, we exit the interface configuration mode. Next, we move on to configure interface S0/0/1, assigning it to the `OUT-ZONE`. This designates S0/0/1 for outgoing traffic, meaning that traffic leaving through this interface will follow the rules of the `OUT-ZONE`. After configuring both interfaces, we exit the interface configuration mode again. This setup allows the router to differentiate between incoming and outgoing traffic, applying appropriate security measures based on the zone assignments.

Task 6: Test Firewall Functionality from IN-ZONE to OUT-ZONE

Verify that internal hosts can still access external resources after configuring the ZPF.

1. From internal PC-C, ping the external PC-A server.

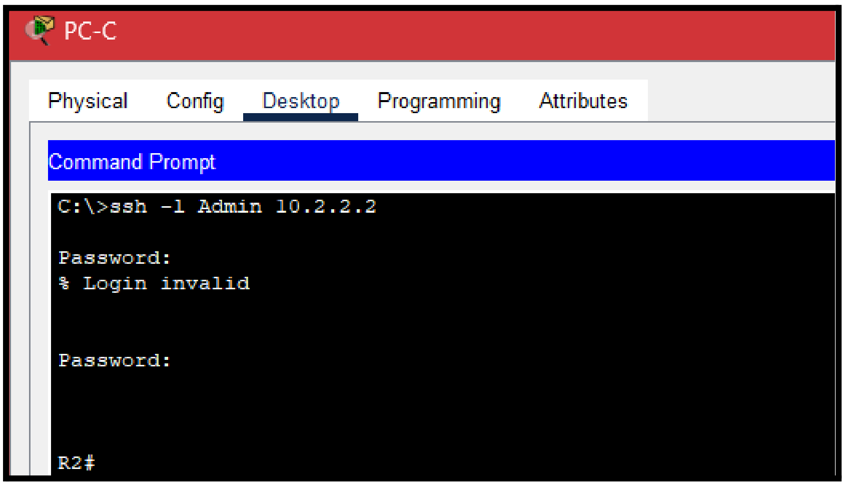
   From the PC-C command prompt, ping PC-A at 192.168.1.3. The ping should succeed. ￼



```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time=16ms TTL=125
Reply from 192.168.1.3: bytes=32 time=10ms TTL=125
Reply from 192.168.1.3: bytes=32 time=11ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 16ms, Average = 12ms
```

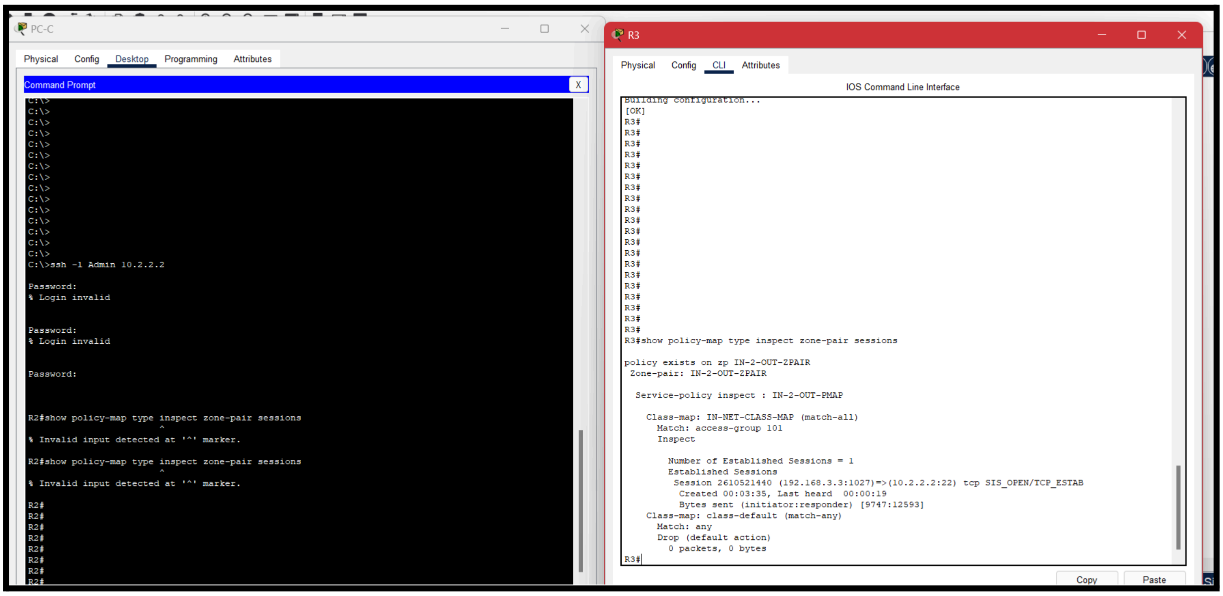
2. From internal PC-C, SSH to the R2 S0/0/1 interface.

a. From the **PC-C** command prompt, SSH to **R2** at 10.2.2.2. Use the username **Admin** and the password **Adminpa55** to access R2. The SSH session should succeed.



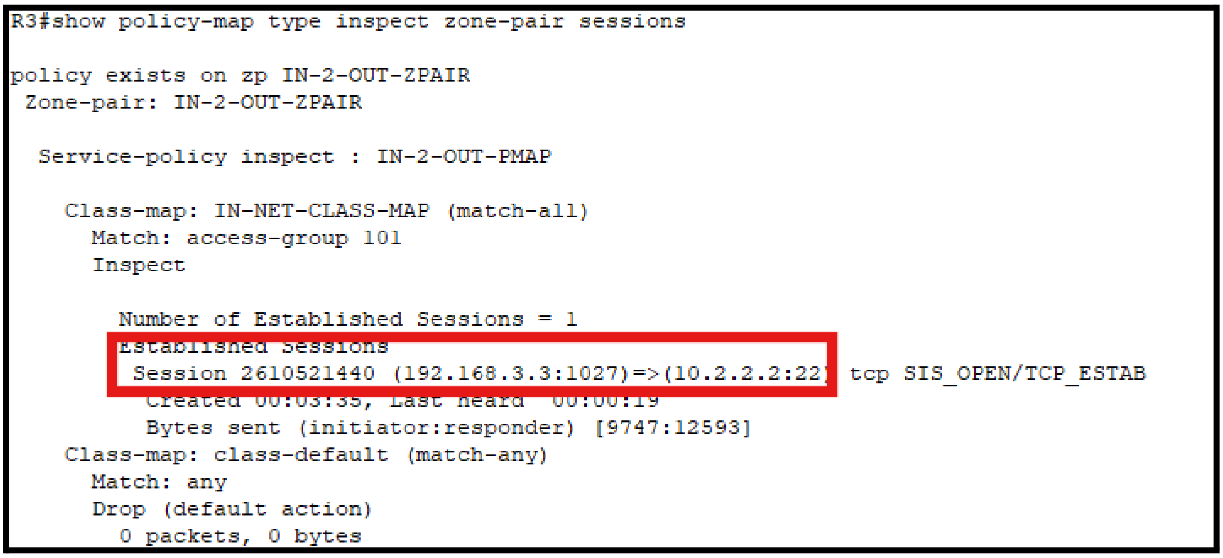
```
C:\>ssh -l Admin 10.2.2.2

Password:
% Login invalid


Password:



R2#
```

b. While the SSH session is active, issue the command **show policy-map type inspect zone-pair sessions** on **R3** to view established sessions.



```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ssh -l Admin 10.2.2.2

Password:
% Login invalid


Password:
% Login invalid


Password:



R2#show policy-map type inspect zone-pair sessions
                          ^
% Invalid input detected at '^' marker.

R2#show policy-map type inspect zone-pair sessions
                          ^
% Invalid input detected at '^' marker.

R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
```

```
Building configuration...
[OK]
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
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

        Number of Established Sessions = 1
        Established Sessions
         Session 2610521440 (192.168.3.3:1027)=>(10.2.2.2:22) tcp SIS_OPEN/TCP_ESTAB
          Created 00:03:35, Last heard  00:00:19
          Bytes sent (initiator:responder) [9747:12593]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
R3#
```



```
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

        Number of Established Sessions = 1
        Established Sessions
         Session 2610521440 (192.168.3.3:1027)=>(10.2.2.2:22) tcp SIS_OPEN/TCP_ESTAB
          Created 00:03:35, Last heard  00:00:19
          Bytes sent (initiator:responder) [9747:12593]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

What is the source IP address and port number? What is the destination IP address and port number?

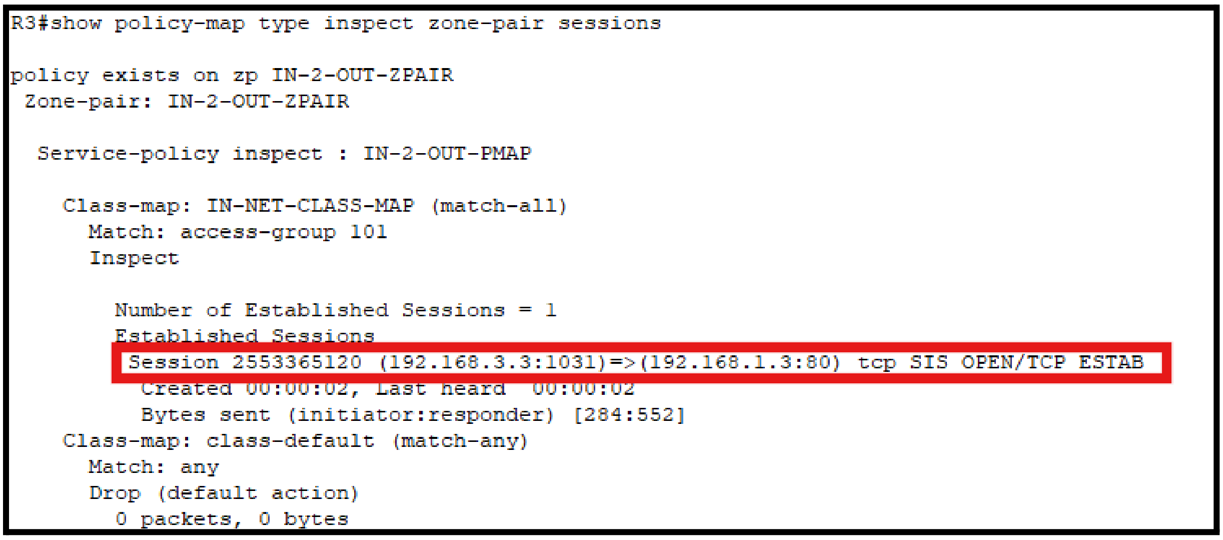
Source IP address and port number:
IP Address: 192.168.3.3
Port Number: 1027

Destination IP address and port number:
IP Address: 10.2.2.2
Port Number: 22

3. From PC-C, exit the SSH session on R2 and close the command prompt window.
4. **From internal PC-C, open a web browser to the PC-A server web page.**

   Enter the server IP address **192.168.1.3** in the browser URL field, and click **Go**. The HTTP session should succeed. While the HTTP session is active, issue the command **show policy-map type inspect zone-pair sessions** on **R3** to view established sessions.

   Note: If the HTTP session times out before you execute the command on **R3**, you will have to click the **Go** button on **PC-C** to generate a session between **PC-C** and **PC-A**.



```
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

        Number of Established Sessions = 1
        Established Sessions
         Session 2553365120 (192.168.3.3:1031)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:02, Last heard  00:00:02
          Bytes sent (initiator:responder) [284:552]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

What is the source IP address and port number? What is the destination IP address and port number?

Source IP address and port number:
IP Address: 192.168.3.3
Port Number: 1031

Destination IP address and port number:
IP Address: 192.168.1.3:80
Port: 80

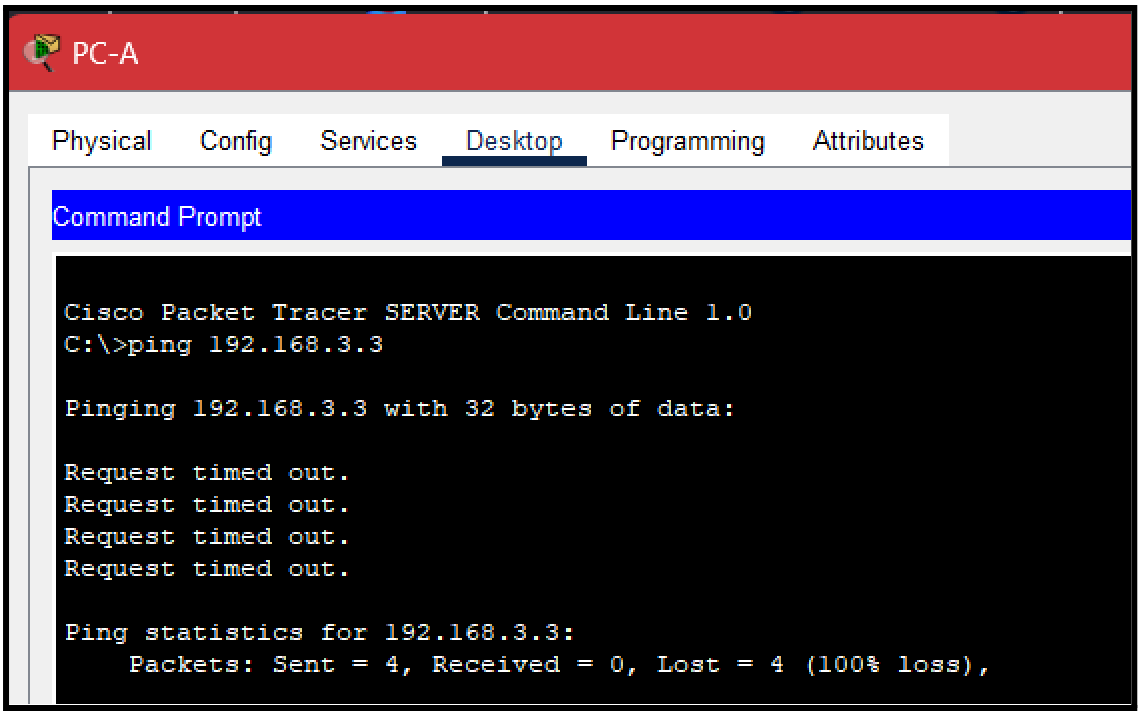
5. Close the browser on PC-C.

Task 7: Test Firewall Functionality from OUT-ZONE to IN-ZONE

Verify that external hosts CANNOT access internal resources after configuring the ZPF.

1. From the PC-A server command prompt, ping PC-C.

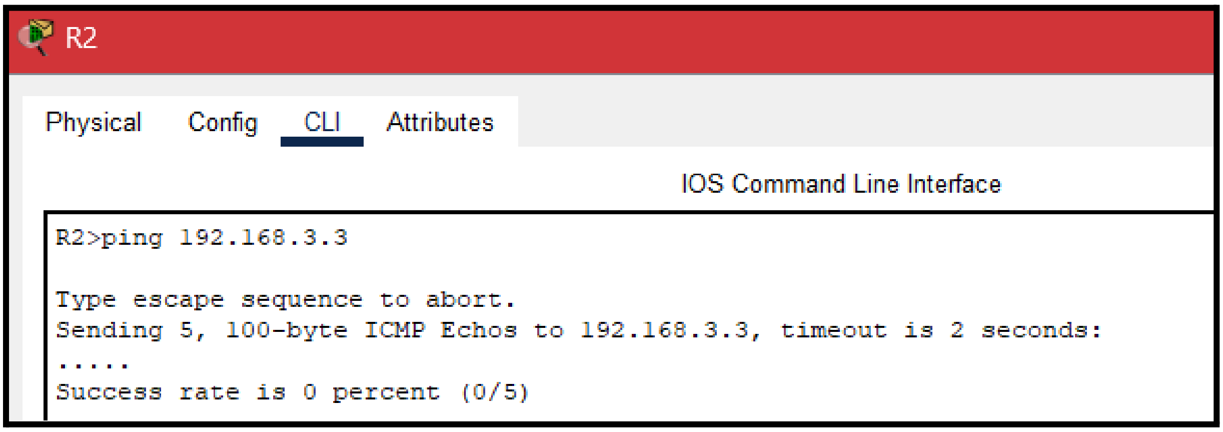
   From the **PC-A** command prompt, ping **PC-C** at 192.168.3.3. The ping should fail.



```
Cisco Packet Tracer SERVER Command Line 1.0
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),
```

2. From R2, ping PC-C.

   From R2, ping PC-C at 192.168.3.3. The ping should fail.

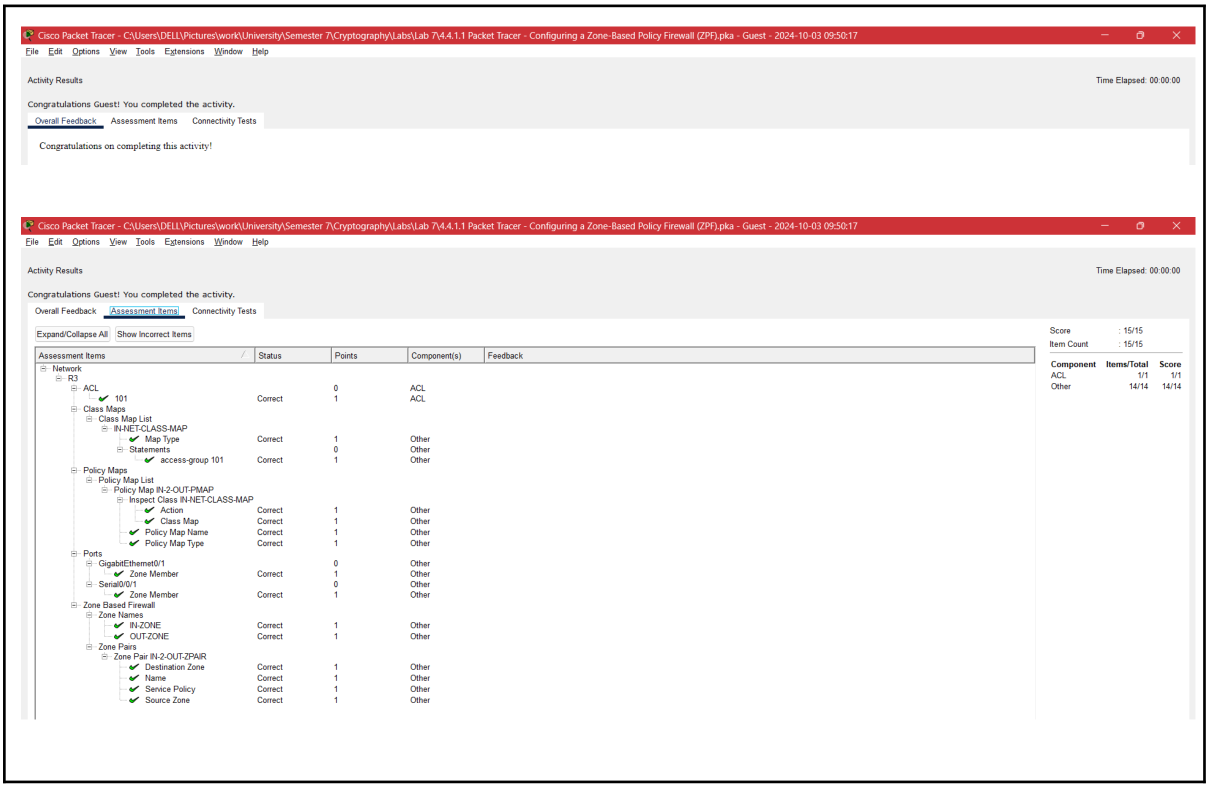


```
R2>ping 192.168.3.3

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)
```

3. Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

PROOF OF COMPLETING THE ACTIVITY



Cisco Packet Tracer - C:\Users\DELL\Pictures\work\University\Semester 7\Cryptography\Labs\Lab 7\4.4.1.1 Packet Tracer - Configuring a Zone-Based Policy Firewall (ZPF).pka - Guest - 2024-10-03 09:50:17

Activity Results

Time Elapsed: 00:00:00

Congratulations Guest! You completed the activity.

Congratulations on completing this activity!

Cisco Packet Tracer - C:\Users\DELL\Pictures\work\University\Semester 7\Cryptography\Labs\Lab 7\4.4.1.1 Packet Tracer - Configuring a Zone-Based Policy Firewall (ZPF).pka - Guest - 2024-10-03 09:50:17

Activity Results

Time Elapsed: 00:00:00

Congratulations Guest! You completed the activity.

Assessment Items	Status	Points	Component(s)	Feedback
Network				
R3				
ACL		0	ACL	
✓ 101	Correct	1	ACL	
Class Maps				
Class Map List				
IN-NET-CLASS-MAP				
✓ Map Type	Correct	1	Other	
Statements		0	Other	
✓ access-group 101	Correct	1	Other	
Policy Maps				
Policy Map List				
Policy Map IN-2-OUT-PMAP				
Inspect Class IN-NET-CLASS-MAP				
✓ Action	Correct	1	Other	
✓ Class Map	Correct	1	Other	
✓ Policy Map Name	Correct	1	Other	
✓ Policy Map Type	Correct	1	Other	
Ports				
GigabitEthernet0/1		0	Other	
✓ Zone Member	Correct	1	Other	
Serial0/0/1		0	Other	
✓ Zone Member	Correct	1	Other	
Zone Based Firewall				
Zone Names				
✓ IN-ZONE	Correct	1	Other	
✓ OUT-ZONE	Correct	1	Other	
Zone Pairs				
Zone Pair IN-2-OUT-ZPAIR				
✓ Destination Zone	Correct	1	Other	
✓ Name	Correct	1	Other	
✓ Service Policy	Correct	1	Other	
✓ Source Zone	Correct	1	Other	

Score : 15/15

Item Count : 15/15

Component	Items/Total	Score
ACL	1/1	1/1
Other	14/14	14/14

Assessment Rubric

Lab 07

Configuring a Zone-Based Policy Firewall (ZPF)

Name: Syed Asghar Abbas Zaidi	**Student ID: 07201**

Points Distribution

Task No.	**LR 2** **Simulation**	**LR5** **Results/Plots**	**LR9** **Report**
Task 1	-	5	
Task 2	5	5	
Task 3	10	-	
Task 4	10	-	
Task 5	10	-	
Task 6	15	5	
Task 7	10	5	
Total	/60	/20	/10
CLO Mapped	CLO 3	CLO 3	CLO3

Affective Domain Rubric		**Points**	**CLO Mapped**
AR 7	Report Submission	/10	CLO 3

CLO	**Total Points**	**Points Obtained**
3	100	
Total	**100**	

For description of different levels of the mapped rubrics, please refer the provided Lab Evaluation Assessment Rubrics and Affective Domain Assessment Rubrics.

Lab Evaluation Assessment Rubric

#	Assessment Elements	Level 1: Unsatisfactory Points 0-1	Level 2: Developing Points 2	Level 3:Good Points 3	Level 4:Exemplary Points 4
LR2	**Program/Code / Simulation Model/ Network Model**	Program/code/simulation model/network model does not implement the required functionality and has several errors. The student is not able to utilize even the basic tools of the software.	Program/code/simulation model/network model has some errors and does not produce completely accurate results. Student has limited command on the basic tools of the software.	Program/code/simulation model/network model gives correct output but not efficiently implemented or implemented by computationally complex routine.	Program/code/simulation /network model is efficiently implemented and gives correct output. Student has full command on the basic tools of the software.
LR5	**Results & Plots**	Figures/ graphs / tables are not developed or are poorly constructed with erroneous results. Titles, captions, units are not mentioned. Data is presented in an obscure manner.	Figures, graphs and tables are drawn but contain errors. Titles, captions, units are not accurate. Data presentation is not too clear.	All figures, graphs, tables are correctly drawn but contain minor errors or some of the details are missing.	Figures / graphs / tables are correctly drawn and appropriate titles/captions and proper units are mentioned. Data presentation is systematic.
LR9	**Report**	All the in-lab tasks are not included in report and / or the report is submitted too late.	Most of the tasks are included in report but are not well explained. All the necessary figures / plots are not included. Report is submitted after due date.	Good summary of most the in-lab tasks is included in report. The work is supported by figures and plots with explanations. The report is submitted timely.	Detailed summary of the in-lab tasks is provided. All tasks are included and explained well. Data is presented clearly including all the necessary figures, plots and tables.