Université Abdelmalek Essaâdi

Faculté des Sciences et Techniques-Tanger

Département Génie Informatique

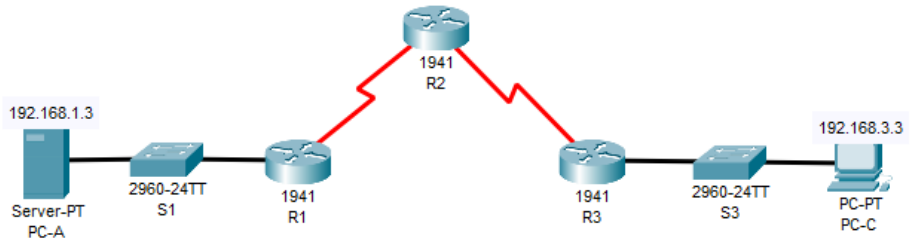
Cryptographie-Sécurité Services

Zone-Based Policy Firewall-2

Réalisé Par :

Yossra safi chetouan

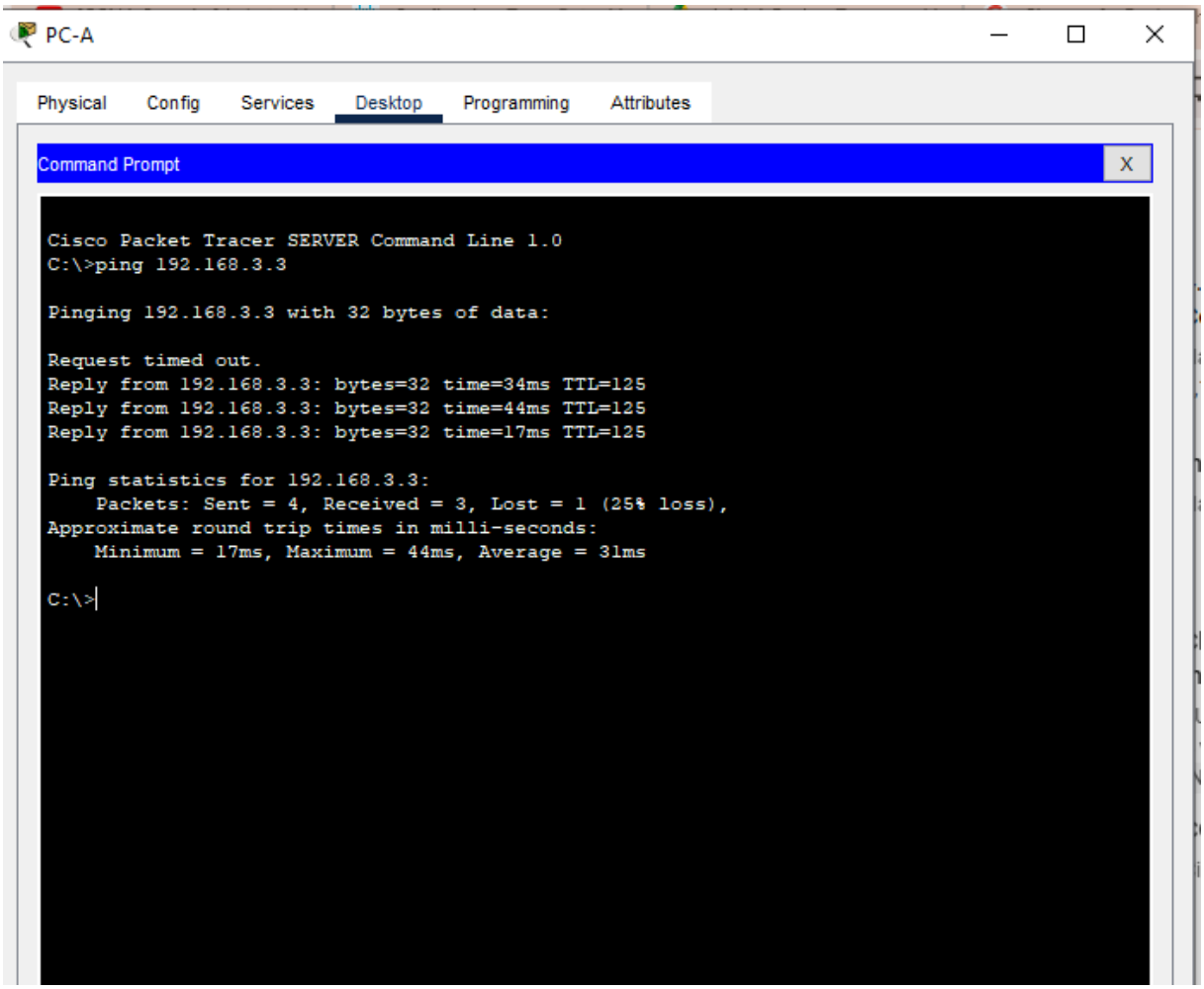
LAB : Packet Tracer-Configuring a Zone-Based Policy Firewall (ZPF)



Part 1: Verify Basic Network Connectivity

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

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



Step 2: Access R2 using SSH.

a. From the PC-C command prompt, SSH to the S0/3/1 interface on R2 at 10.2.2.2. Use the username Admin and password Adminpa55 to log in.

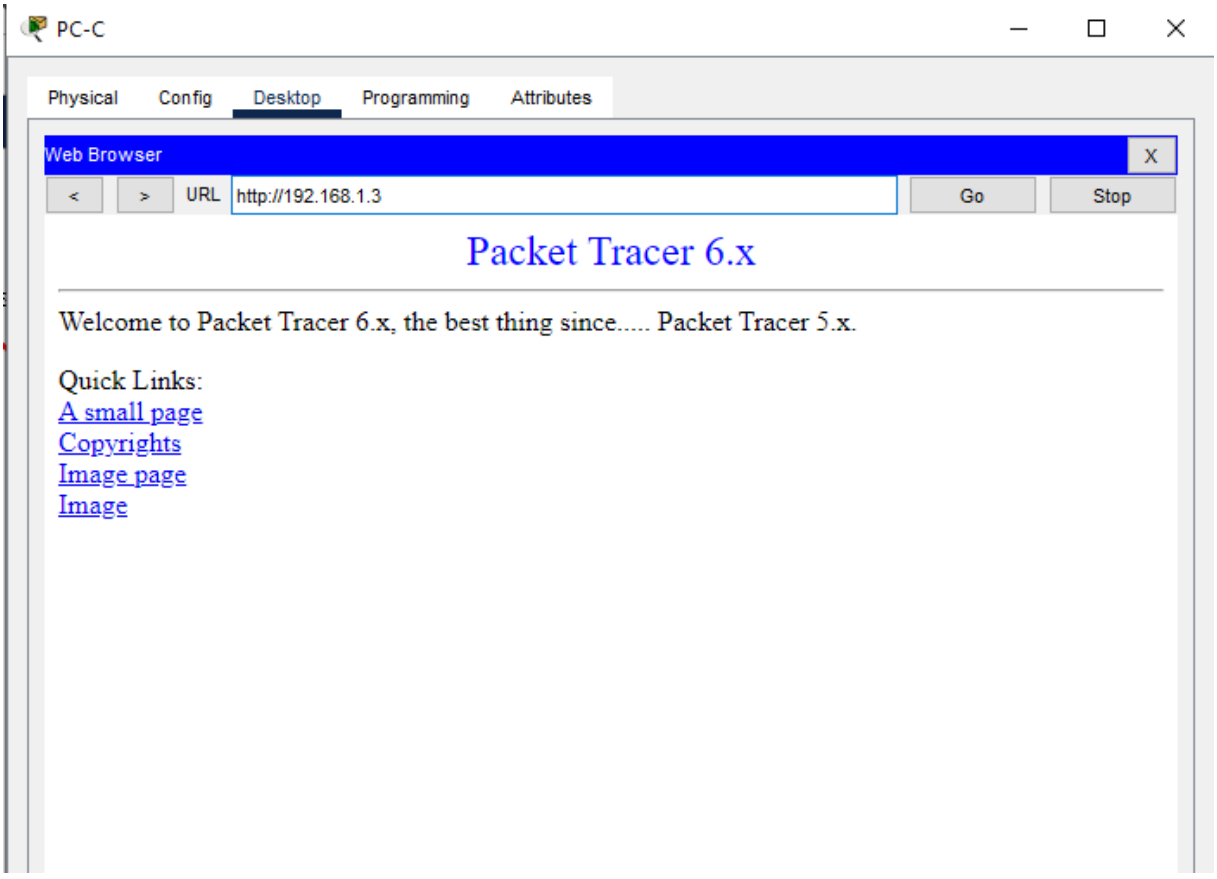
PC>ssh -l Admin 10.2.2.2

b. Exit the SSH session.

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

a. Click the Desktop tab and then click the Web Browserapplication. 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.

b. Close the browser on PC-C.



Part 2: Create the Firewall Zones on R3

```
License Info:

License UDI:

-------------------------------------------------
Device#    PID                   SN
-------------------------------------------------
*0         CISCO1941/K9          FTX1524Q024-


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


R3#
```

Step 1: 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

Step 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

IOS Command Line Interface

```
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                 SN
-------------------------------------------------
*0        CISCO1941/K9        FTX1524Q024-


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


R3#
R3#
R3#
R3#
R3#
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)#
```

Part 3: Identify Traffic Using a Class-Map

Step 1: Create an ACL that defines internal traffic.

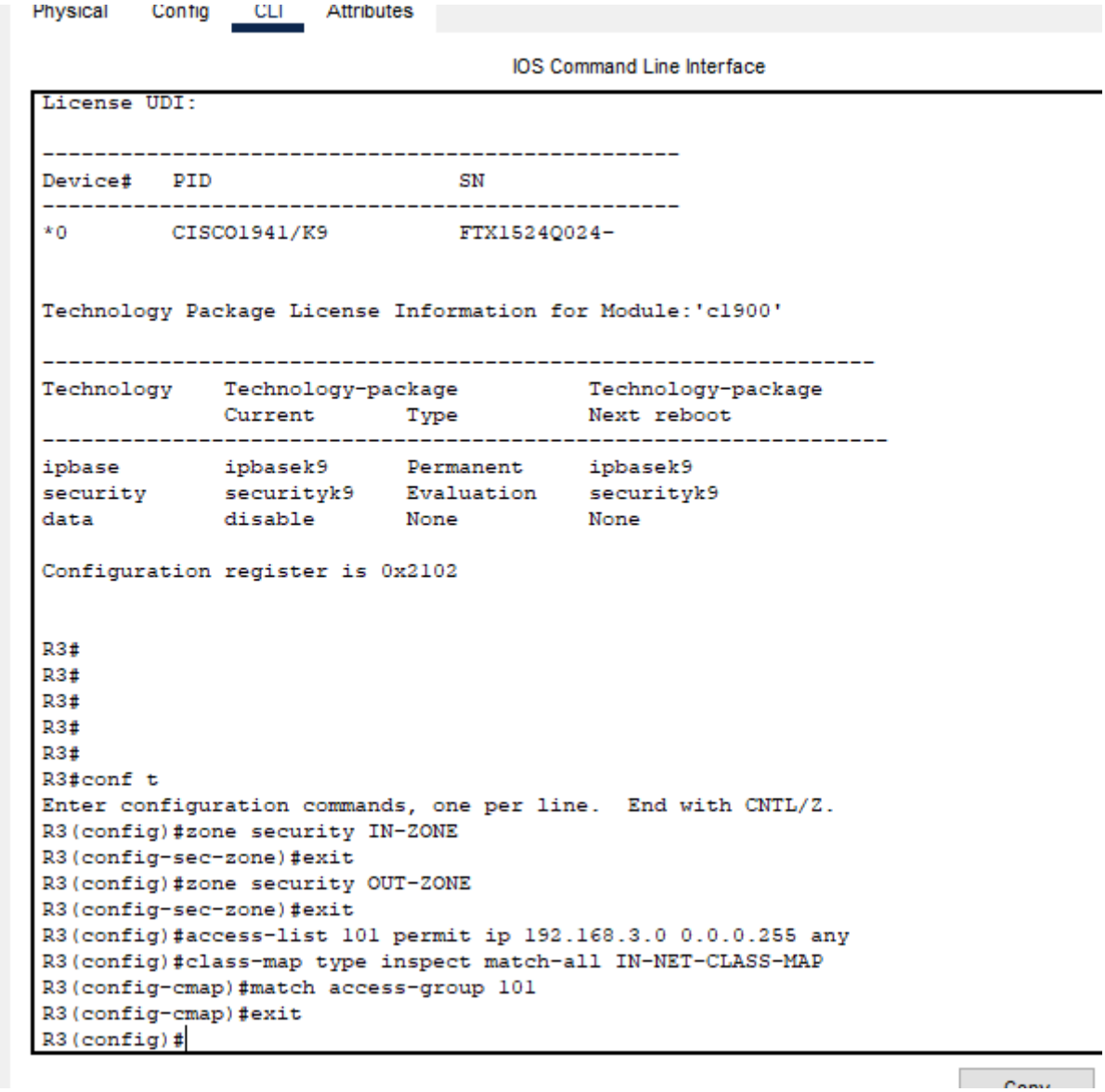
Use the access-list command to create extended ACL 101 to permit all IP protocols from the 192.168.3.0/24
source network to any destination.

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

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

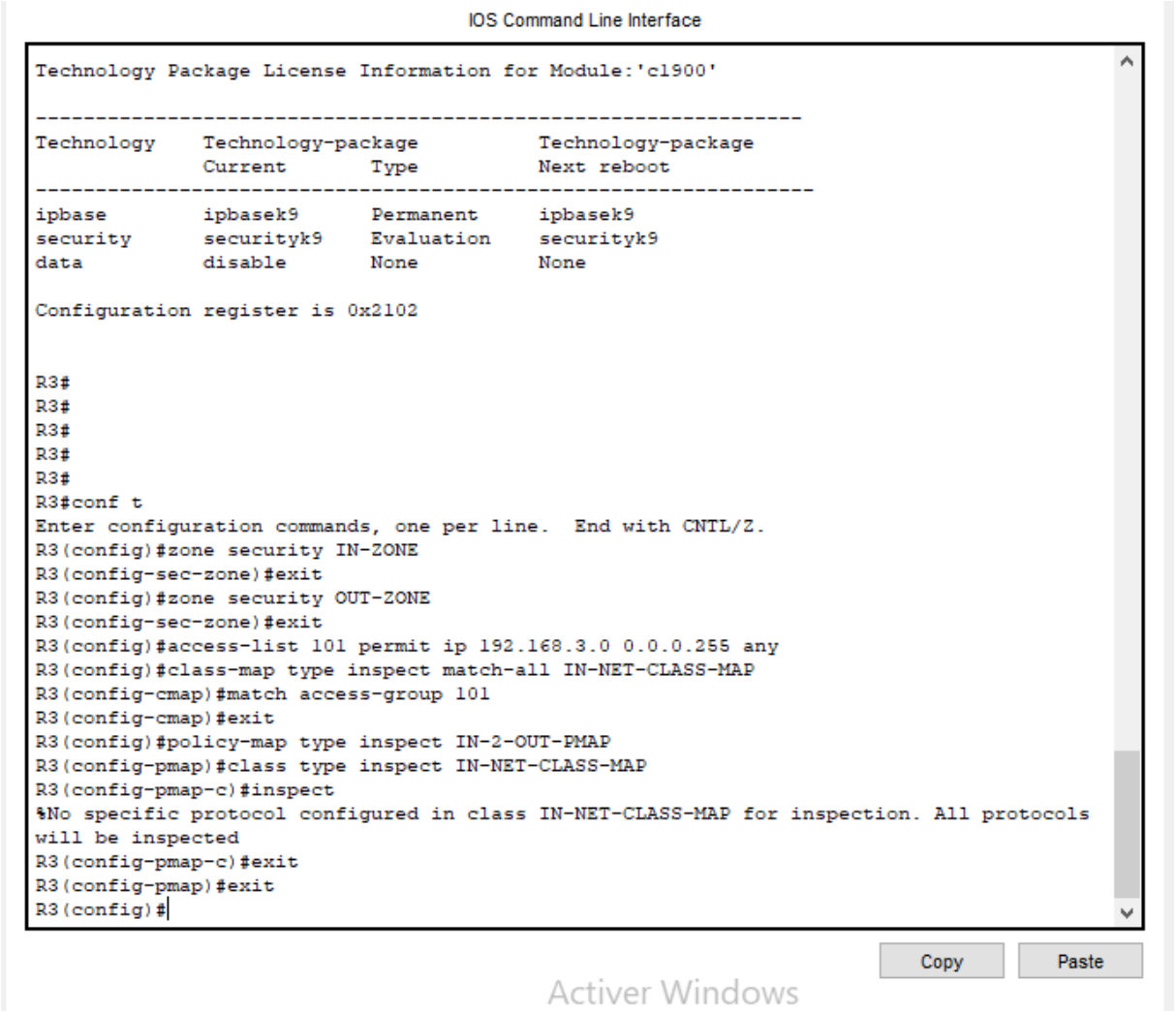
Use the class-map type inspect command with the match-all option to create a class map named IN-NET-
CLASS-MAP. Use the match access-group command to match ACL 101.

R3(config)# class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)# match access-group 101
R3(config-cmap)# exit



Part 4: Specify Firewall Policies

Step 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
Step 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
Step 3: Specify the action of inspect for this policy map.
R3(config-pmap-c)# inspect
R3(config-pmap-c)# exit
R3(config-pmap)# exit



Part 5: Apply Firewall Policies

Step 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

Step 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)#

Step 3: Assign interfaces to the appropriate security zones.

Use the zone-member security command in interface configuration mode to assign F0/1 to IN-ZONE and

S0/3/1 to OUT-ZONE.

R3(config)# interface f0/1

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

R3(config-if)# exit

R3(config)# interface s0/3/1

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

R3(config-if)# 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 f0/1
%Invalid interface type and number
R3(config)#int f0/1
%Invalid interface type and number
R3(config)#int g0/1
R3(config-if)#zone-member security IN-ZONE
R3(config-if)#exit
R3(config)#interface s0/3/1
%Invalid interface type and number
R3(config)#interface s0/0/1
R3(config-if)#zone-member security OUT-ZONE
R3(config-if)#exit
R3(config)#
```

Copy Paste

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

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

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

From the PC-Ccommand prompt, ping PC-A at 192.168.1.3. The ping should succeed.

Step 2: From internal PC-C, SSH to the R2 S0/3/1 interface.

From the PC-Ccommand 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:\>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=3ms TTL=125
Reply from 192.168.1.3: bytes=32 time=3ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms 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 = 2ms, Maximum = 3ms, Average = 2ms

C:\>ssh -l Admin 10.2.2.2

Password:



R2#
```

Top

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

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

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

From the PC-Acommand prompt, ping PC-C at 192.168.3.3. The ping should fail.

```
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),

C:\>
```

Step 2: From R2, ping PC-C.

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

```
Press RETURN to get started!

.
Success rate is 0 percent (0/5)



User Access Verification

Password:
Password:

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)

R2>
```