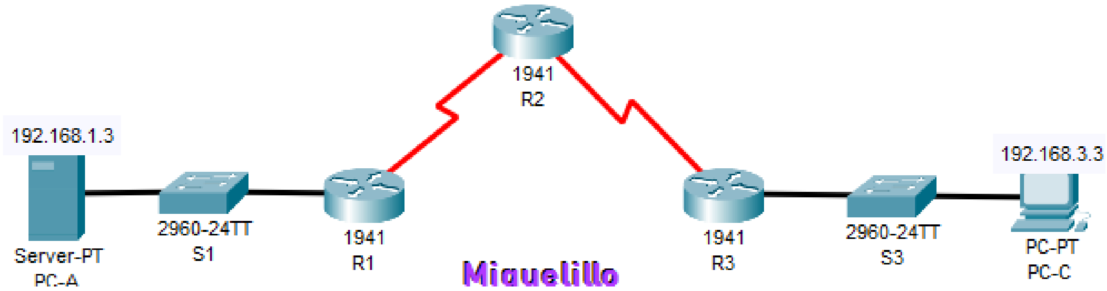
Índice:

Ejercicio 1

a) Resolución de Laboratorio 10.3.11 del curso CISCO Network Security en Packet Tracer – Configuración ZPF

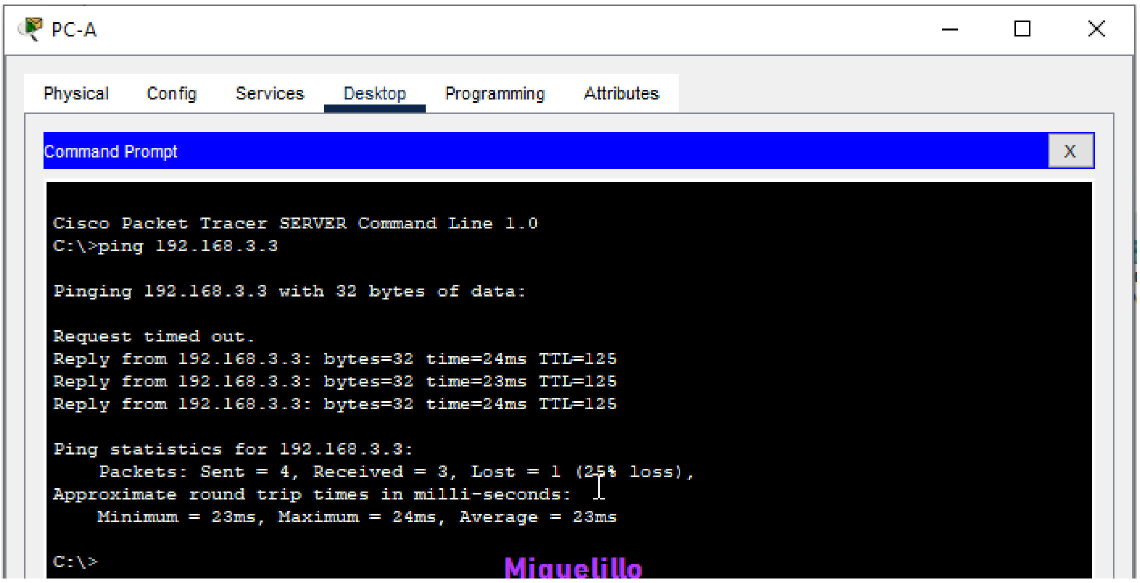
Solución:

Escenario



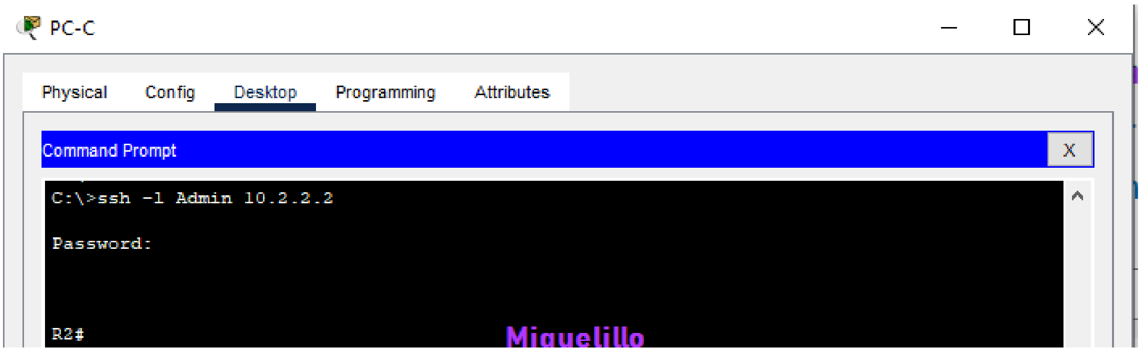
Parte 1: Verificar Conectividad Básica de la Red

Paso 1 Desde el símbolo del sistema de PC-A, realiza un ping a PC-C en 192.168.3.3.



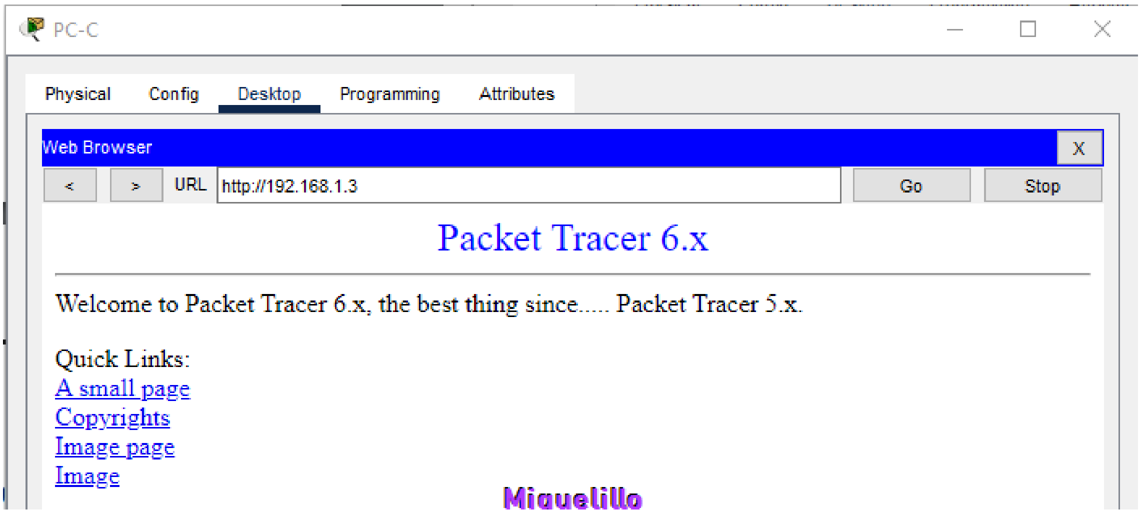
```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.3: bytes=32 time=24ms TTL=125
Reply from 192.168.3.3: bytes=32 time=23ms TTL=125
Reply from 192.168.3.3: bytes=32 time=24ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 24ms, Average = 23ms

C:\>
```

Paso 2 Accede a R2 usando SSH desde el símbolo del sistema de PC-C.



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

Password:


R2#
```

Paso 3 de PC-C, abre un navegador web a PC-A server



http://192.168.1.3

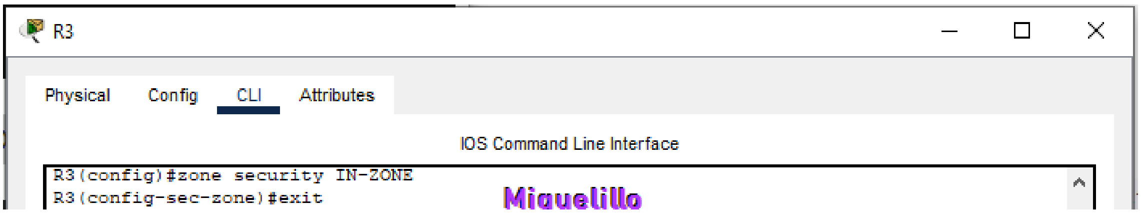
Packet Tracer 6.x

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

Quick Links:
A small page
Copyrights
Image page
Image

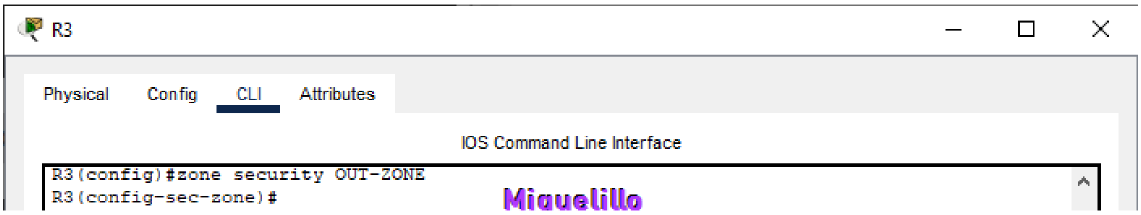
Parte 2: Crear las Zonas de Firewall en R3

Paso 1: Crea una zona interna (IN-ZONE).



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

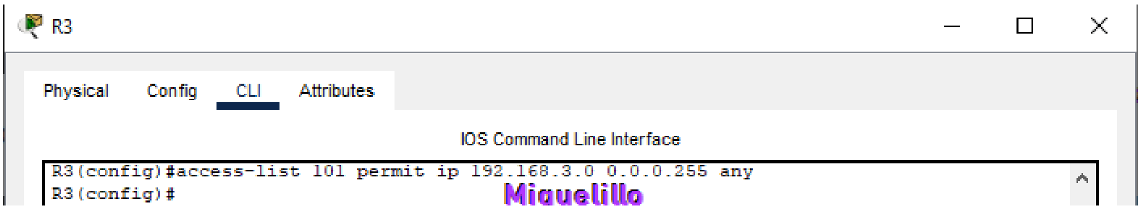
Paso 2: Crea una zona externa (OUT-ZONE).



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

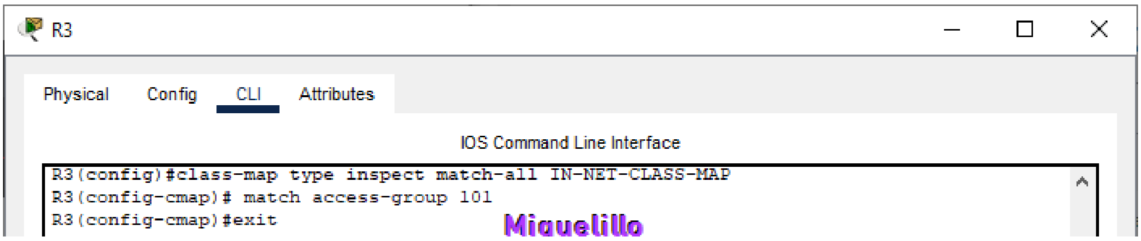
Parte 3: Identificar Tráfico con un Class-Map

Paso 1: Crea una ACL que defina el tráfico interno.



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

Paso 2: Crea un class map referenciando la ACL de tráfico interno.



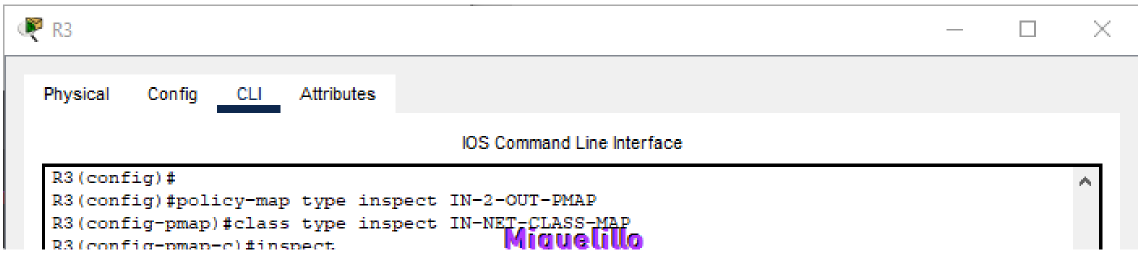
```
R3(config)#class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)# match access-group 101
R3(config-cmap)#exit
```

Parte 4: Especificar Políticas del Firewall

Paso 1: Crea un policy map para determinar qué hacer con el tráfico coincidente.

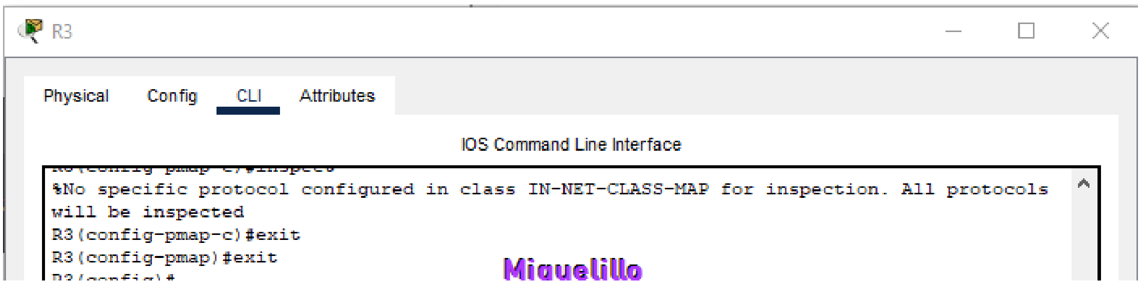
Paso 2: Especifica una clase de tipo inspect y referencia class map IN-NET-CLASS-MAP.

Paso 3: Especifica la acción de inspect para este policy map.



```
R3(config)#
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
```

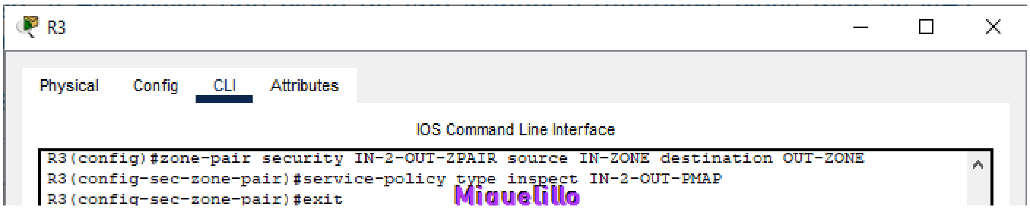
Paso 4: Sal del modo de configuración de clase y de policy map.



```
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)#
```

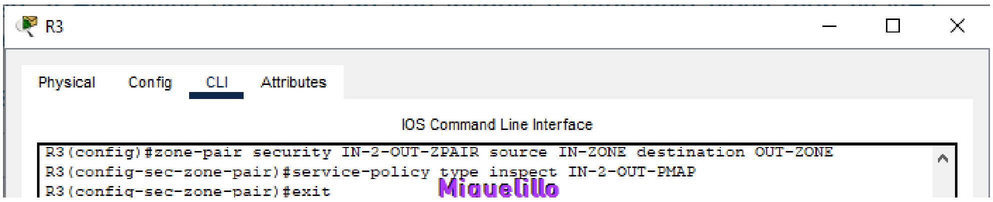
Parte 5: Aplicar Políticas del Firewall

Paso 1: Crea un par de zonas.



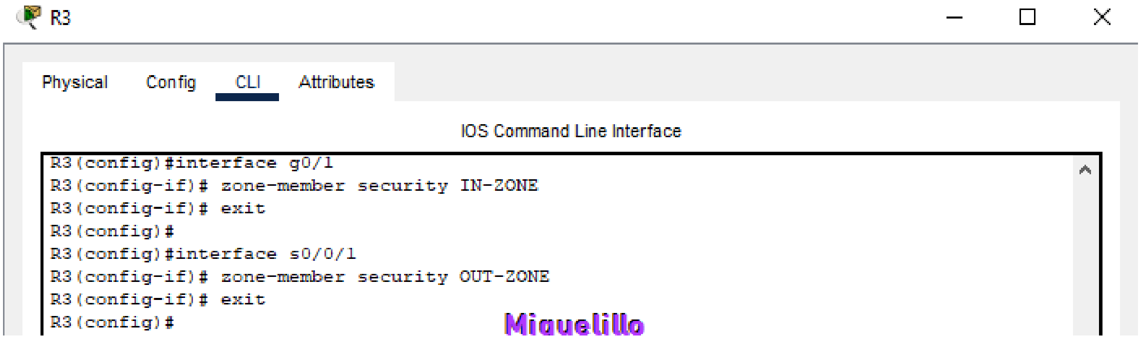
```
R3(config)#zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
R3(config-sec-zone-pair)#service-policy type inspect IN-2-OUT-PMAP
R3(config-sec-zone-pair)#exit
```

Paso 2: Especifica el policy map para manejar el tráfico entre las dos zonas.



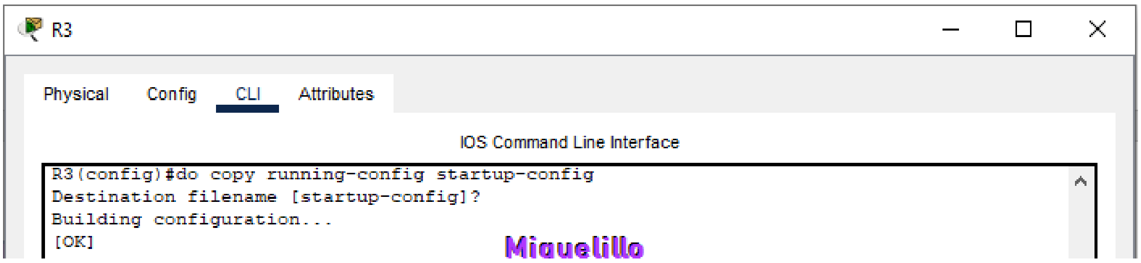
```
R3(config)#zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
R3(config-sec-zone-pair)#service-policy type inspect IN-2-OUT-PMAP
R3(config-sec-zone-pair)#exit
```

Paso 3: Asigna interfaces a las zonas de seguridad correspondientes.



```
R3(config)#interface g0/1
R3(config-if)# zone-member security IN-ZONE
R3(config-if)# exit
R3(config)#
R3(config)#interface s0/0/1
R3(config-if)# zone-member security OUT-ZONE
R3(config-if)# exit
R3(config)#
```

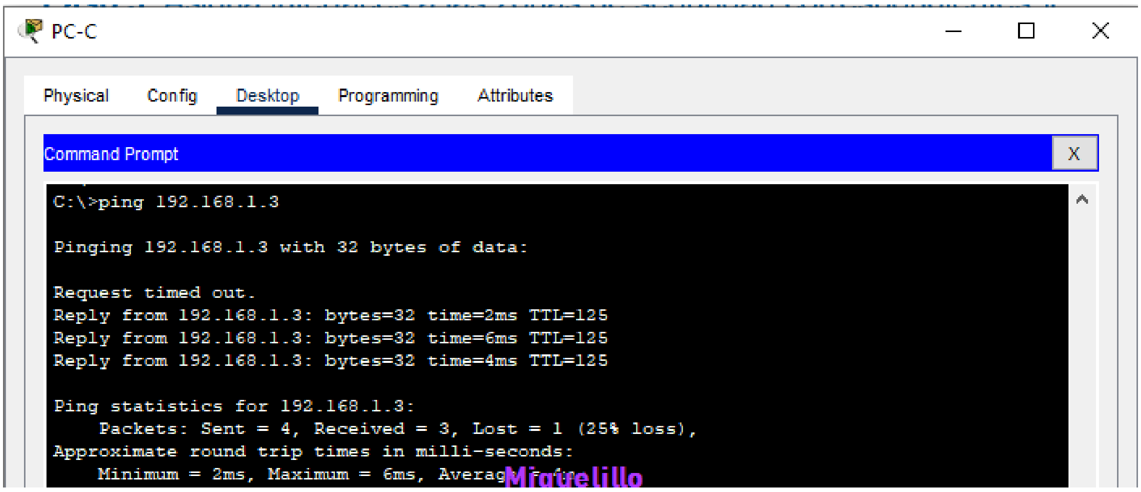
Paso 4: Guarda la configuración en la memoria



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

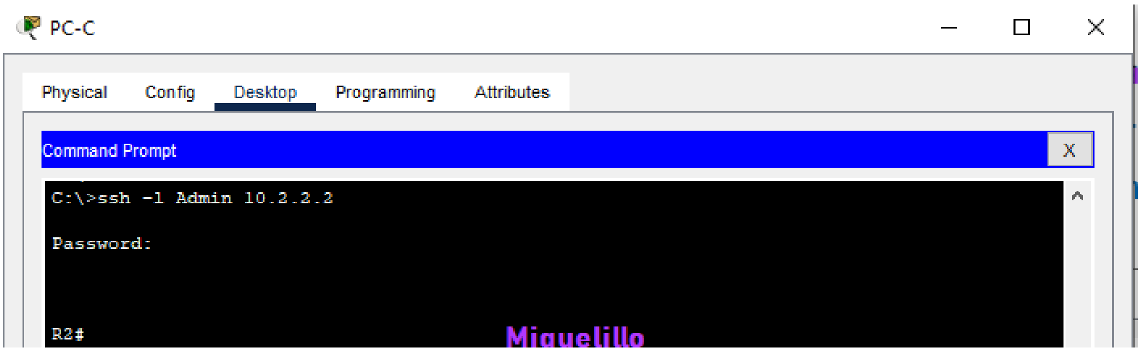
Parte 6: Probar la Funcionalidad del Firewall de IN-ZONE a OUT-ZONE

Paso 1: Desde PC-C, realiza un ping al servidor externo PC-A.



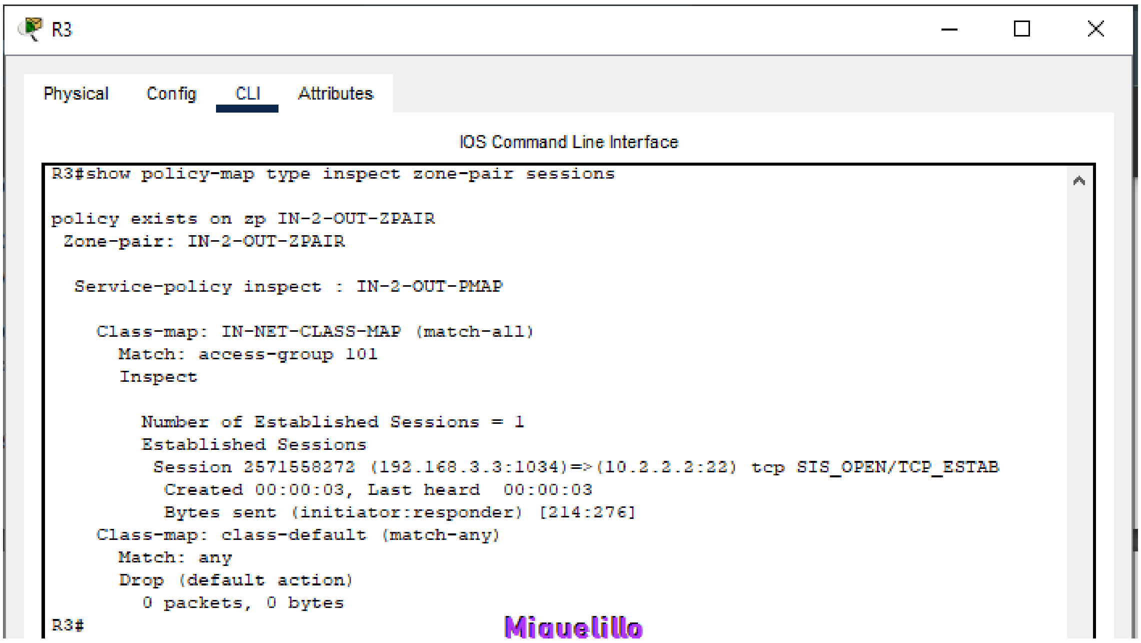
```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=6ms TTL=125
Reply from 192.168.1.3: bytes=32 time=4ms 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 = 6ms, Averag
```

Paso 2: Desde PC-C, SSH a la interfaz S0/0/1 de R2



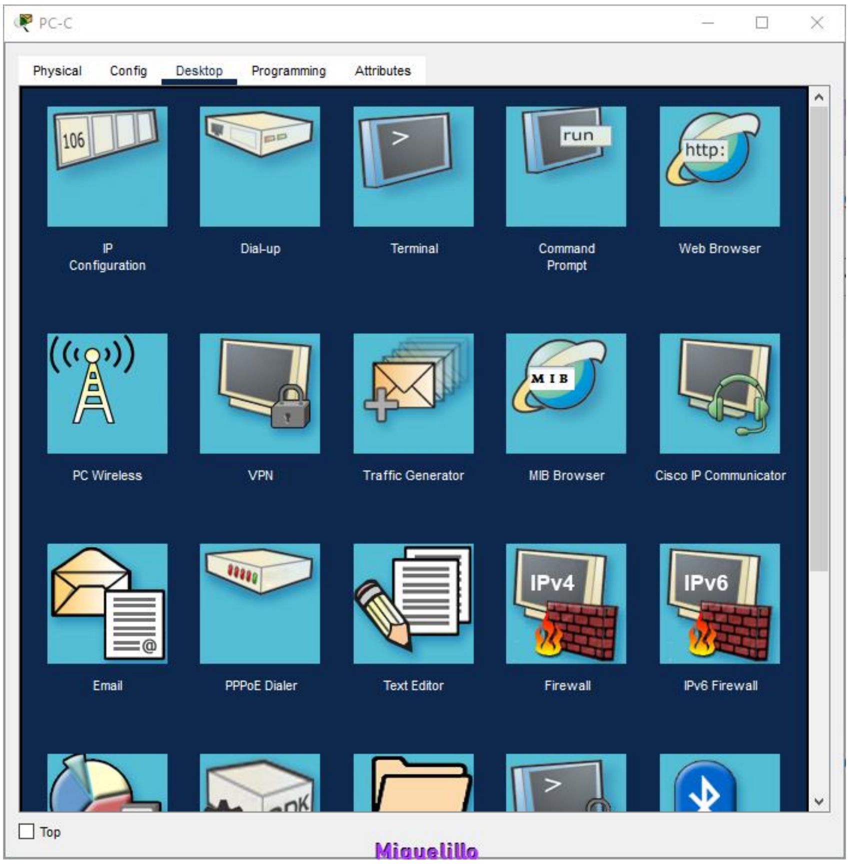
```
C:\>ssh -l Admin 10.2.2.2

Password:


R2#
```

Mientras la sesión de SSH esté activa, emite el comando show policy-map type inspect zone-pair sessions en R3 para ver las sesiones establecidas.

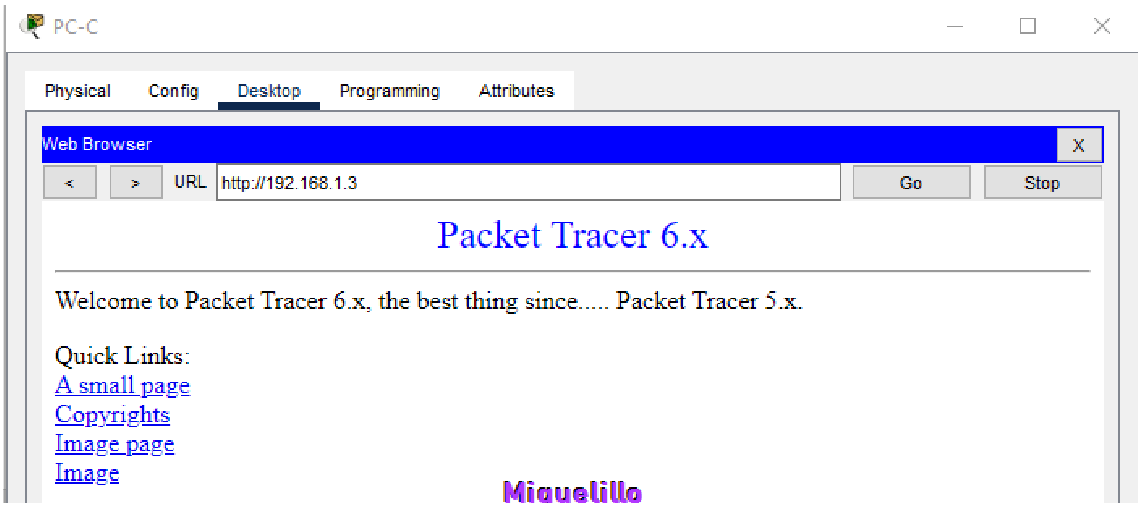


```
R3#show policy-map type inspect zone-pair sessions

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 2571558272 (192.168.3.3:1034)=>(10.2.2.2:22) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:03, Last heard  00:00:03
          Bytes sent (initiator:responder) [214:276]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
R3#
```

Paso 3: Desde PC-C, sal de la sesión SSH en R2 y cierra la ventana del símbolo del sistema.



Paso 4: Desde PC-C, abre un navegador web en la página del servidor PC-A.



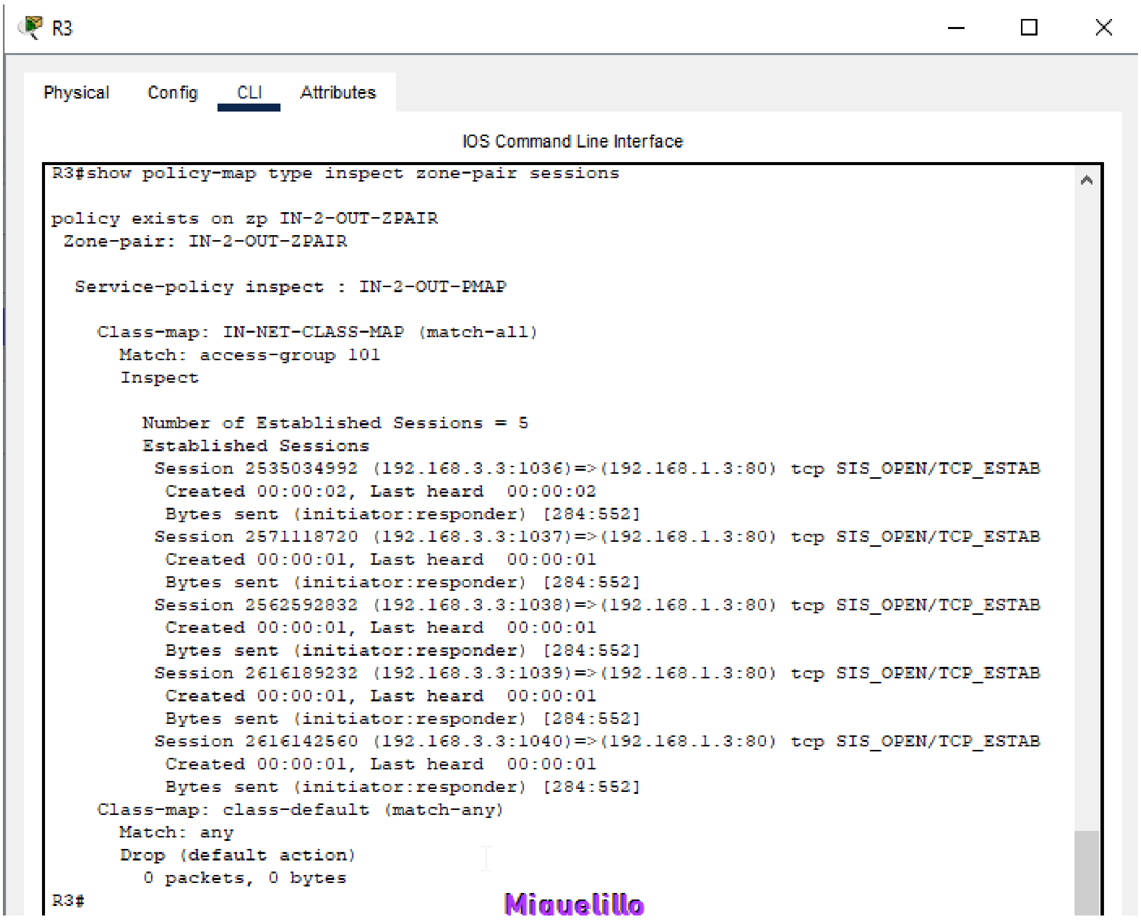
http://192.168.1.3

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

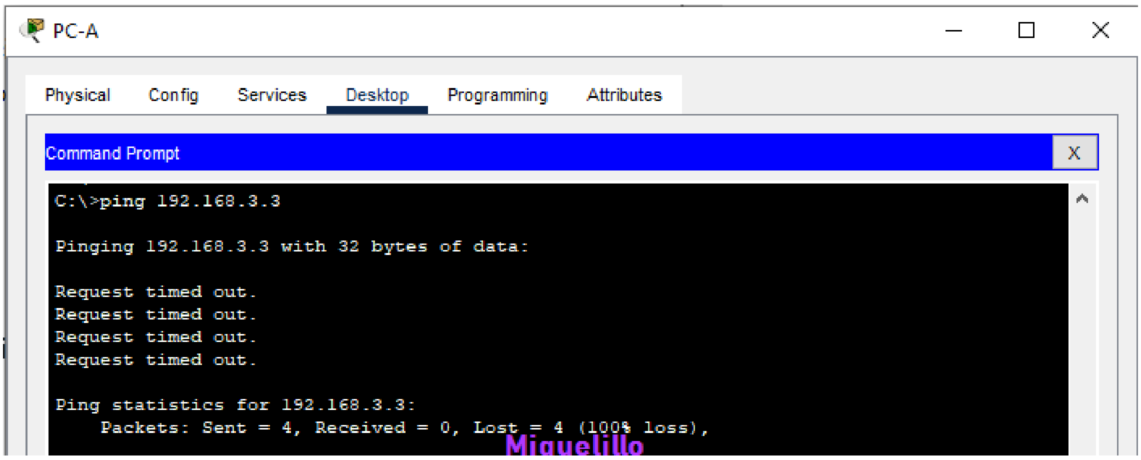
Mientras la sesión HTTP esté activa, emite el comando show policy-map type inspect zone-pair sessions en R3 para ver las sesiones establecidas.



```
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 = 5
        Established Sessions
         Session 2535034992 (192.168.3.3:1036)=>(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]
         Session 2571118720 (192.168.3.3:1037)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:01, Last heard  00:00:01
          Bytes sent (initiator:responder) [284:552]
         Session 2562592832 (192.168.3.3:1038)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:01, Last heard  00:00:01
          Bytes sent (initiator:responder) [284:552]
         Session 2616189232 (192.168.3.3:1039)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:01, Last heard  00:00:01
          Bytes sent (initiator:responder) [284:552]
         Session 2616142560 (192.168.3.3:1040)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:01, Last heard  00:00:01
          Bytes sent (initiator:responder) [284:552]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
R3#
```

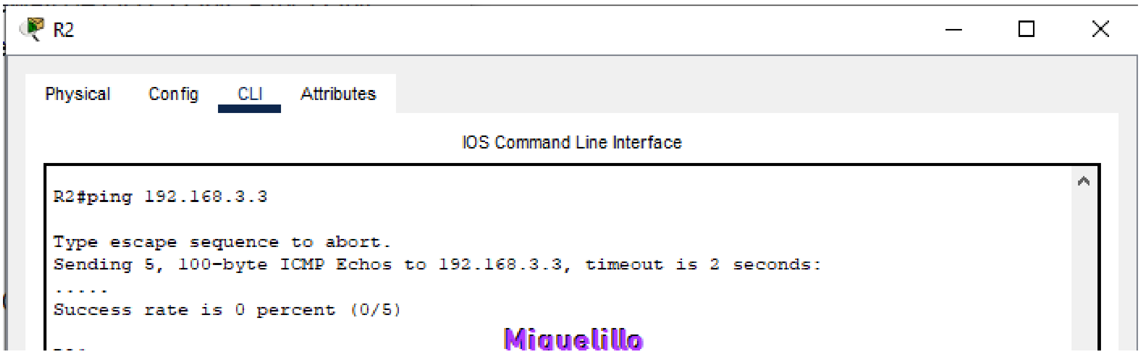
Parte 7: Probar la Funcionalidad del Firewall de OUT-ZONE a IN-ZONE

Paso 1: Desde el símbolo del sistema del servidor PC-A, realiza un ping a PC-C. (Este ping debería fallar)



```
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),
```

Paso 2: Desde R2, realiza un ping a PC-C. (Este ping debería fallar)



```
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)
```