

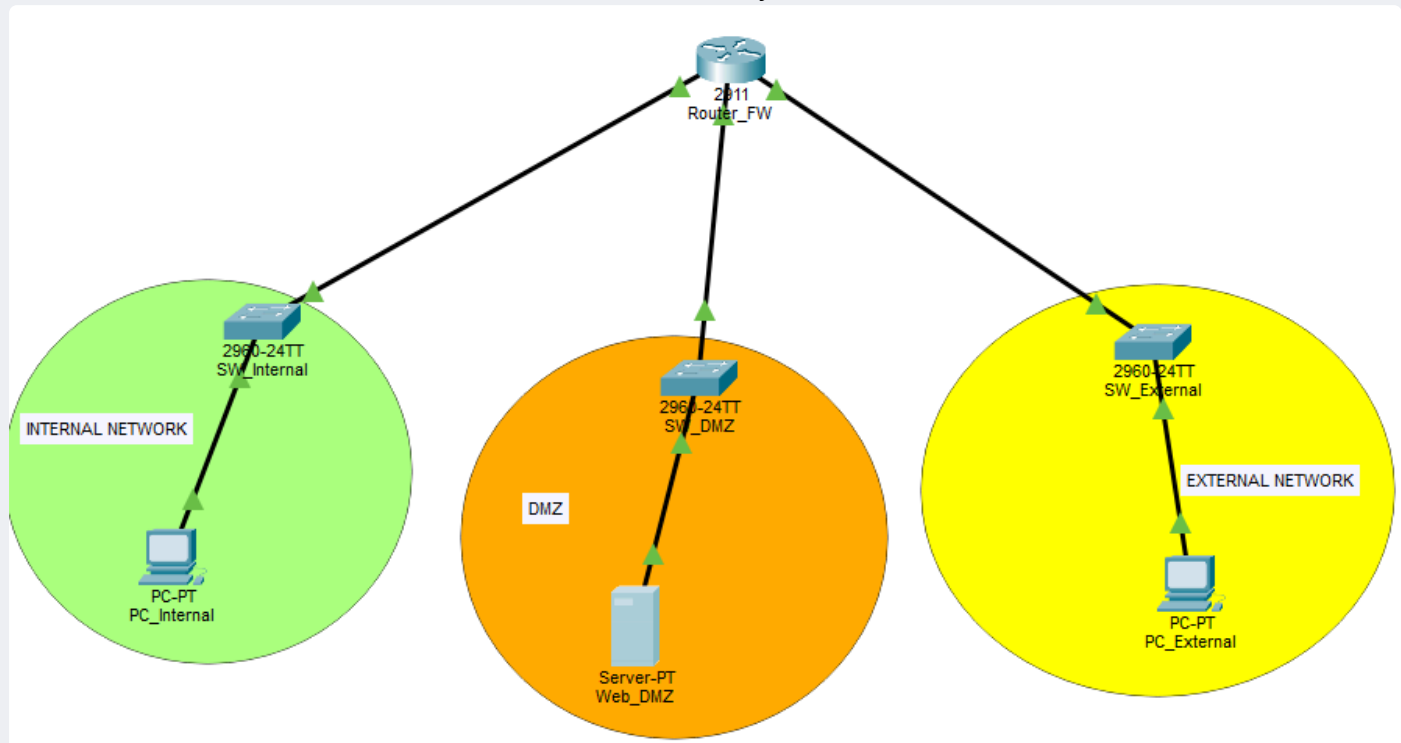
Informe de configuración de DMZ con Cisco Packet Tracer

1. Objetivo del laboratorio

Se buscaba configurar de una forma segura una red DMZ, pudiendo entrar a sus servicios web pero sin comprometer el resto de la seguridad bloqueando paquetes ICMP para evitar, por ejemplo, ataques de denegación de servicio. Además, trabajar en un entorno Cisco y saber aplicar una NAT e introducir ACLs para controlar el tráfico.

2. Topología implementada

La red se conforma de 3 subredes, la interna, la DMZ y la externa.



- Cantidad de redes: 3__
- Dispositivos usados: 3__
- Breve descripción de la función de cada zona (LAN, DMZ, Externa).
 - LAN: Red interna de una organización sin acceso directo a redes externas, pero si al servidor web alojado en la DMZ o servicios que requieran con una conexión al exterior.
 - DMZ: Red que se expone al exterior para aislar la red interna de posibles ataques.
 - Externa: Cualquier usuario ajeno a la organización.

3. Plan de direccionamiento IP

Completa la tabla con las IPs asignadas (puedes copiarla del enunciado si no cambia).

Dispositivo	IP	Máscara	Gateway
PC_Internal	192.168.1.10	255.255.255.0	192.168.1.1
Server_DMZ	192.168.2.10	255.255.255.0	192.168.2.1
PC_External	192.168.3.10	255.255.255.0	192.168.3.1
Router_FW Gi0/0 (LAN)	192.168.1.1	255.255.255.0	0.0.0.0
Router_FW Gi0/1 (DMZ)	192.168.2.1	255.255.255.0	0.0.0.0
Router_FW Gi0/2 (Ext)	192.168.3.1	255.255.255.0	0.0.0.0

4. Configuración aplicada (resumen)

Resume los comandos o pasos más relevantes que ejecutaste. Usa texto + fragmentos de código cuando sea necesario.

- Interfaces configuradas con `ip address`
- NAT:

```
ip nat inside source static 192.168.2.10 192.168.3.1
```

- ACLs:

```
# Bloquea ICMP DMZ->LAN y asegura el orden.
conf t
# Se crea una lista de acceso.
ip access-list extended DMZ_IN_BLOCK
# Solo respuestas TCP (ACK/RST) pasan.
5 permit tcp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 established
# Se bloquea ICMP hacia la lan.
10 deny icmp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
# Se bloquea cualquier otro inicio de conexión DMZ->LAN.
20 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
# Se permite el resto del tráfico hacia otros destinos.
30 permit ip any any
```

5. Verificaciones realizadas

Describe las pruebas y su resultado. Incluye capturas o salidas de comandos si se puede.

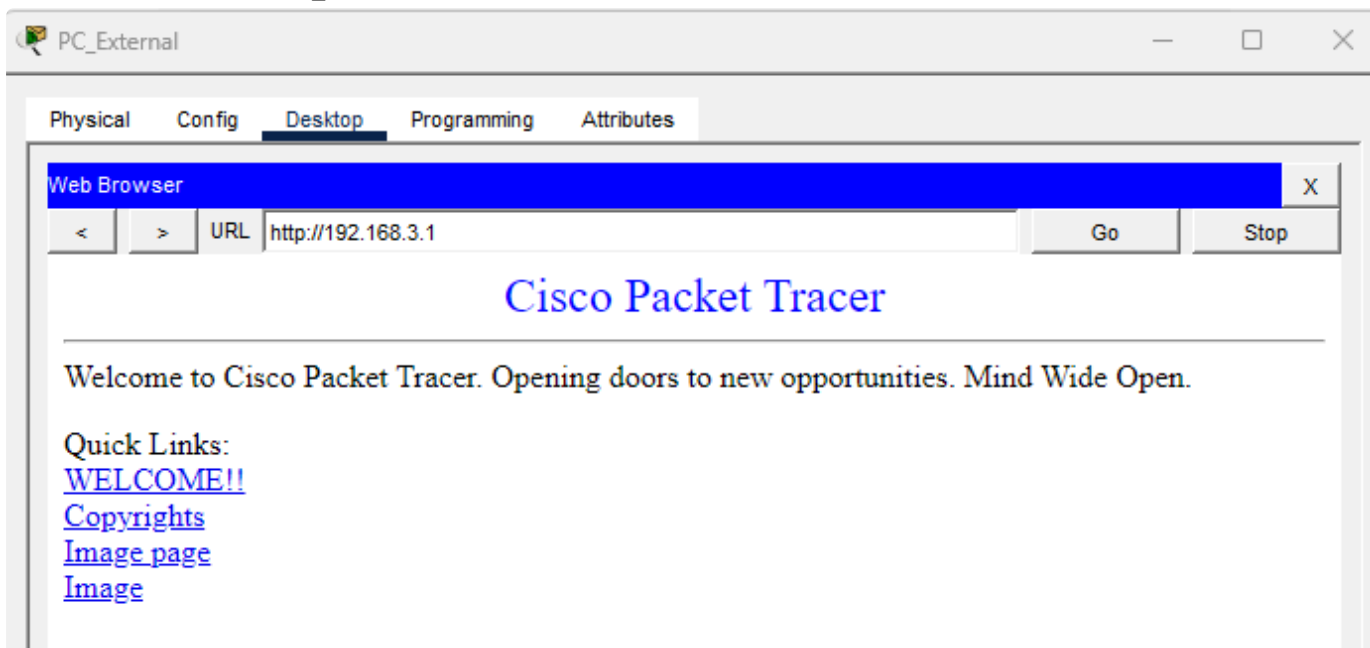
- ping desde PC_Internal al router: Destination host unreachable

```
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
```

- Acceso web desde PC_External: Existoso



- Bloqueo de acceso desde DMZ a LAN: Destination host unreachable

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
```

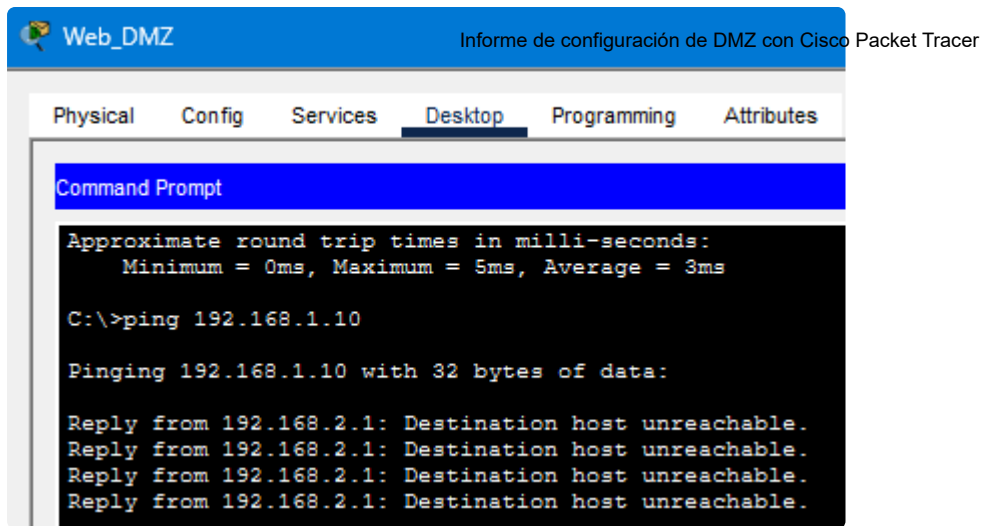
6. Conclusiones y recomendaciones

Aprendí a configurar una red NAT y reglas ACLs en un router Cisco. Recomendando establecer un orden en las reglas para evitar conflicto entre ellas.

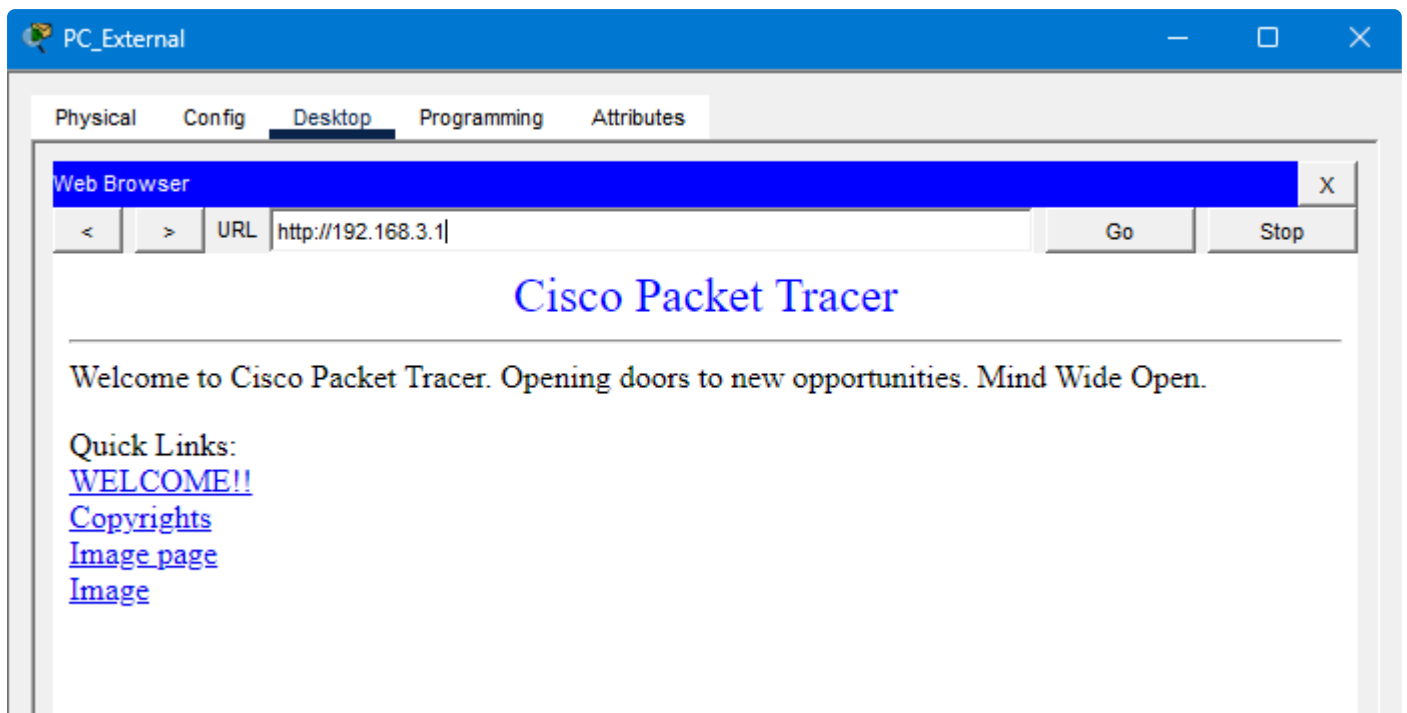
7. Capturas de evidencia

Adjunta aquí (o en un PDF anexo) las capturas solicitadas: pings, navegador, comandos `show`, etc.

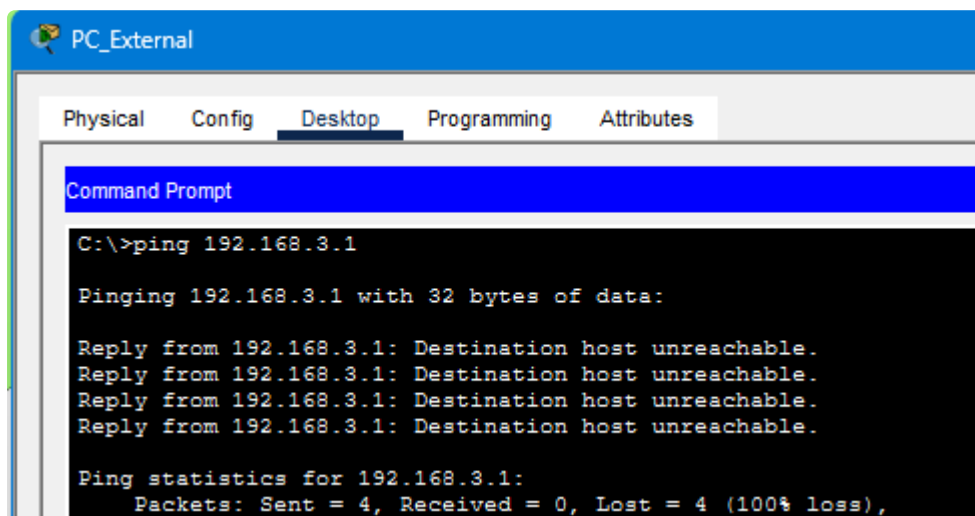
Ping desde el servidor Web_DMZ a la red interna fallido.



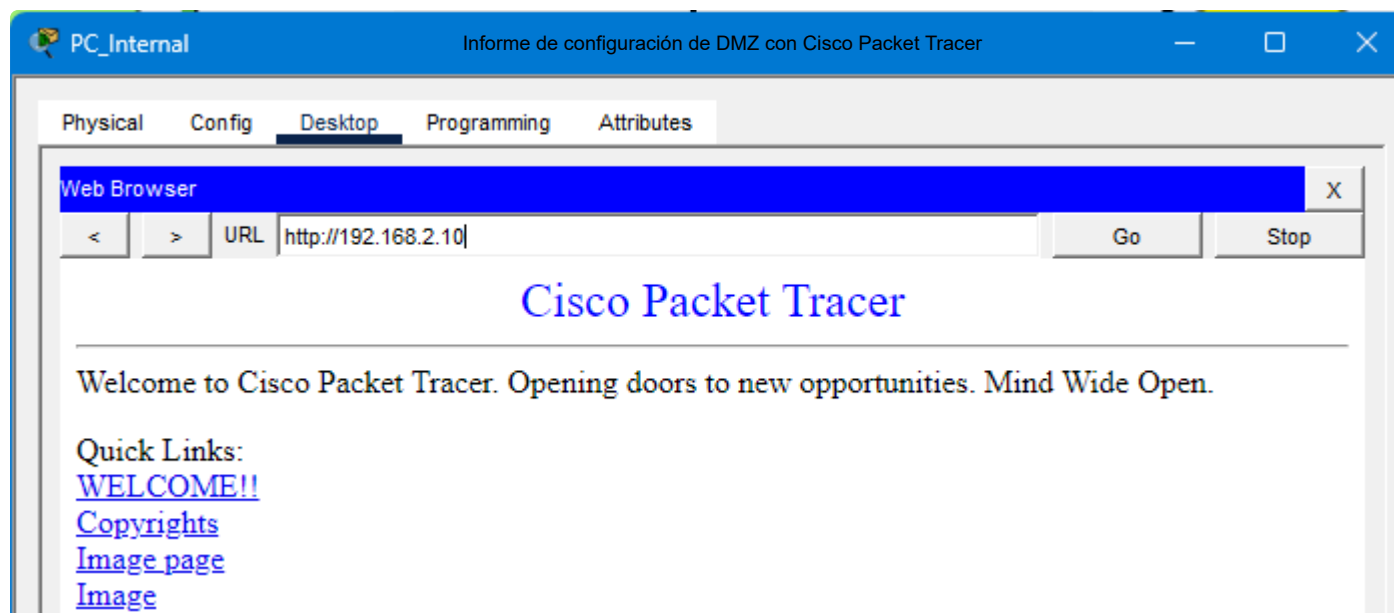
Acceso web desde el PC_External al servidor DMZ redirigido.



Ping al gateway fallido desde PC_External



Acceso a la web DMZ desde PC_Internal



Comandos introducidos

```
Router_FW(config-ext-nacl)#remark
% Incomplete command.
Router_FW(config-ext-nacl)#permit tcp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
established
Router_FW(config-ext-nacl)#deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Router_FW(config-ext-nacl)#exit
Router_FW(config)#end
Router_FW#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Router_FW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router_FW(config)#ip access-list extended DMZ_IN_BLOCK
Router_FW(config-ext-nacl)#5 permit tcp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Router_FW(config-ext-nacl)#10 deny icmp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Router_FW(config-ext-nacl)#5 5conf t
%Invalid hex value
Router_FW(config)#ip access-list extended DMZ_IN_BLOCK
Router_FW(config-ext-nacl)#NONno 5
Router_FW(config-ext-nacl)#no 10
Router_FW(config-ext-nacl)#5 permit tcp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
established
Router_FW(config-ext-nacl)#10 deny icmp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Router_FW(config-ext-nacl)#20 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
% Duplicate sequence number
Router_FW(config-ext-nacl)#d30 permit ip any any
% Duplicate sequence number
Router_FW(config-ext-nacl)#exit
Router_FW(config)#end
Router_FW#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Router_FW#
```

Reglas ACL aplicadas junto con los grupos de acceso.

```
Router_FW>enable
Router_FW#show ip access-lists Informe de configuración de DMZ con Cisco Packet Tracer
Extended IP access list WAN_IN_HTTP
  10 permit tcp any host 192.168.3.1 eq www (49 match(es))
  20 deny ip any any (26 match(es))
Extended IP access list DMZ_IN_BLOCK
  10 deny icmp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 (11 match(es))
  20 permit ip any any (49 match(es))
  30 permit tcp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 established
  40 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

Router_FW#show run | include access-group
ip access-group DMZ_IN_BLOCK in
ip access-group WAN_IN_HTTP in
```

Reglas de la interfaz de red 0/1.

```
Router_FW#show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Internet address is 192.168.2.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is DMZ_IN_BLOCK
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
```

Reglas de la interfaz de red 0/2

```
Router_FW#show ip interface g0/2
GigabitEthernet0/2 is up, line protocol is up (connected)
  Internet address is 192.168.3.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is WAN_IN_HTTP
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
```