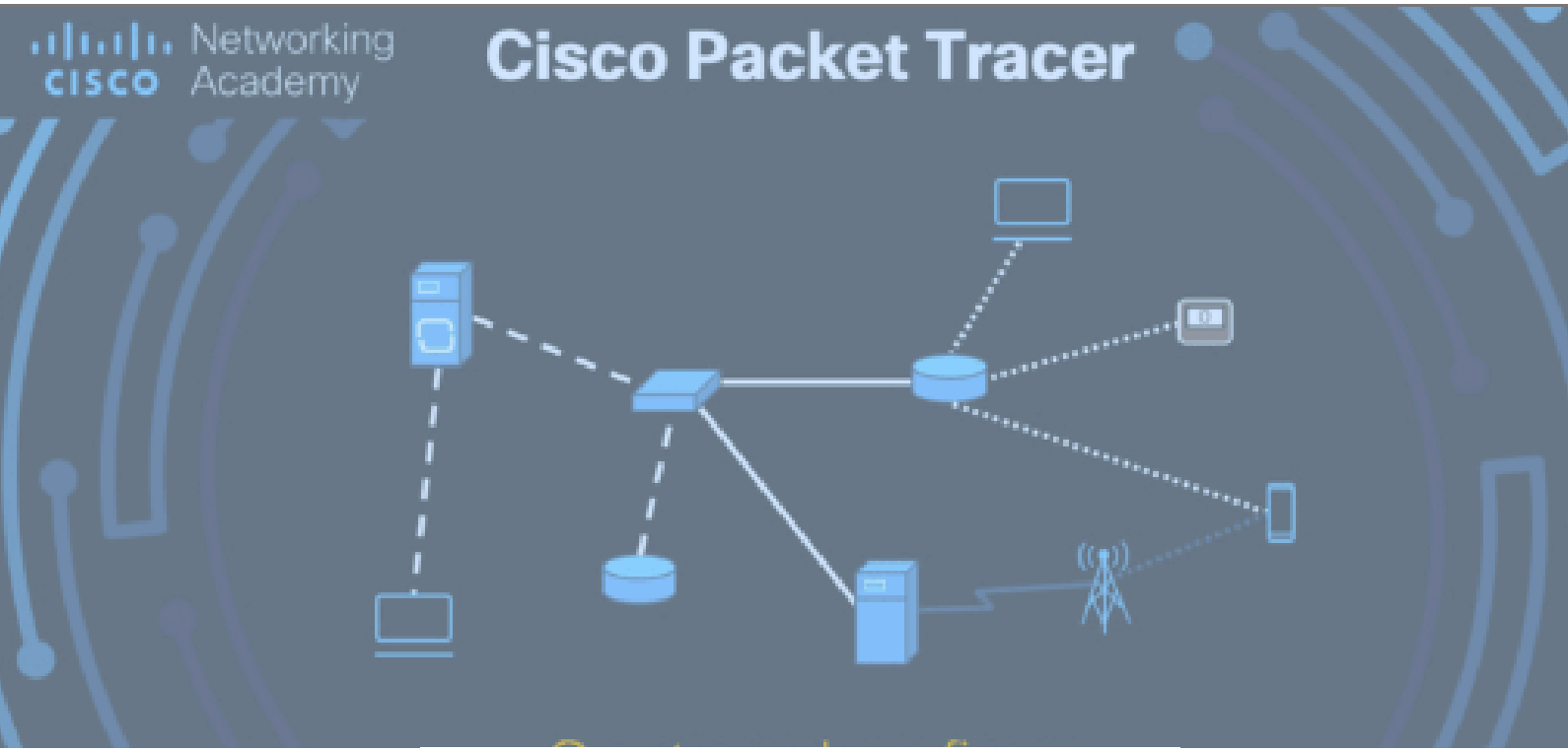
Informe de configuración de DMZ con Cisco Packet Tracer

Elaborado por:

Omar Gallardo

Fecha:

25/08/2025



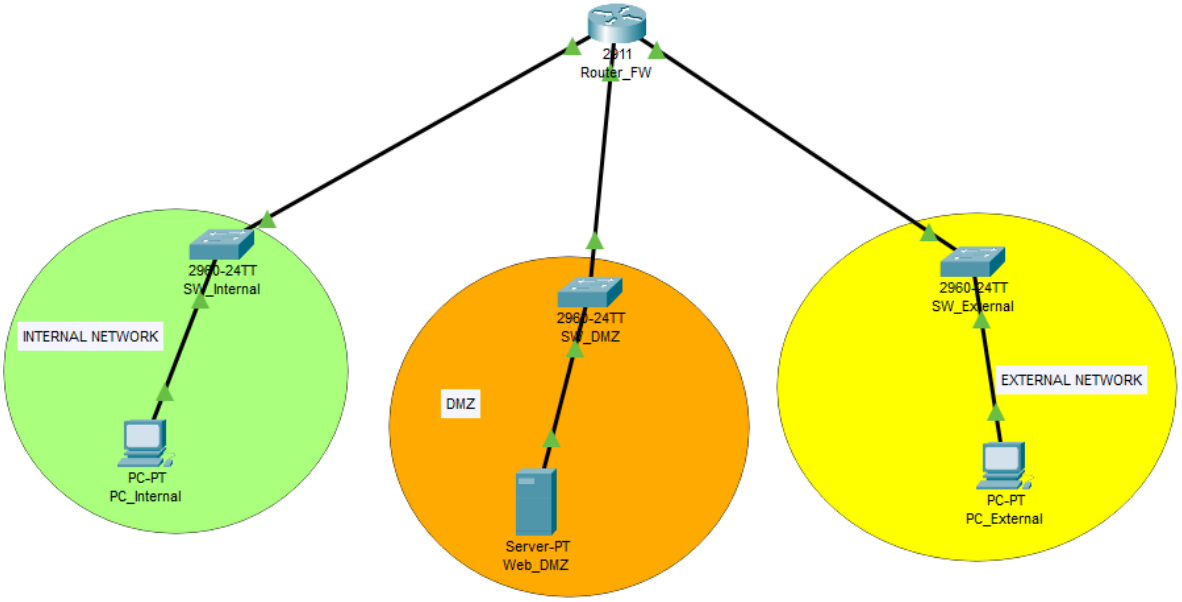
Cisco Packet Tracer

1. Objetivo del laboratorio

La actividad realizada consistió en la configuración de una zona desmilitarizada, como tal es una subred que sirve a un entorno como una capa de seguridad extra entre 2 redes distintas, una interna y una externa. El objetivo del laboratorio fue justamente configurar la DMZ y entender cómo se puede configurar desde las direcciones IP, pings y peticiones.

2. Topología implementada

Como se puede observar en la imagen siguiente, la topología a estudiar se conoce como una topología DMZ de firewall único de tipo **ÁRBOL.** Esta configuración es la más utilizada y práctica debido a su facilidad y versatilidad en la configuración, punto clave para nuestra DMZ, con 1 router que divide en 3 secciones Server Web, Red Interna y Red Externa



3. Plan de direccionamiento IP

A continuación se muestran las interfaces con un único router y sus direcciones IP's

Interfaz	Red conectada	IP asignada	Función
GigabitEthernet0/0	Red interna (LAN)	192.168.1.1	Gateway para PC_Internal
GigabitEthernet0/1	DMZ	192.168.2.1	Gateway para Server_DMZ
GigabitEthernet0/2	Red externa	192.168.3.1	Gateway para PC_External + NAT pública

Esta es una configuración típica de entornos que buscan separar y controlar el acceso a un servicio, en este caso concreto al servicio web y en base a eso permitir o denegar el acceso a este servicio mediante la configuración ACL que veremos a continuación.

4. Configuración aplicada (resumen)

Para realizar la configuración de manera adecuada se siguieron las recomendaciones básicas establecidas por la academia. Primeramente se asignaron las direcciones IP y máscara de subred a cada instancia de la red DMZ teniendo como resultado cada interfaz, dirección IP y red conectada mencionadas anteriormente en la tabla.

Posterior a eso, se configuró desde la terminal CLI del router, las interfaces correspondientes con la configuración básica siguiente:

```
Router> enable
Router# configure terminal
Router(config)# hostname Router_FW

Router_FW(config)# interface GigabitEthernet0/0
Router_FW(config-if)# ip address 192.168.1.1 255.255.255.0
Router_FW(config-if)# no shutdown
Router_FW(config-if)# exit
```

Nota: Importantísimo, al finalizar la configuración escribir write memory para guardar cambios

5. Verificaciones realizadas

En cuanto a las verificaciones, se tuvo que revisar si las conexiones entrantes al servidor web estaban debidamente configuradas, para eso se establecieron 4 parámetros principales:

1. Permitir el acceso al servidor web DMZ (192.168.3.1). Resultado esperado: La página web debe cargar.
2. Desde PC_External (Command Prompt): ping 192.168.3.1 (Ping a la interfaz WAN/IP pública del servidor). Resultado esperado: Request timed out (Debe FALLAR si tu ACL externa bloquea ICMP).
3. Desde PC_Internal (Web Browser): Accede al servidor web DMZ (192.168.2.10). Resultado esperado: La página web debe cargar.
4. Desde Server-PT Web_DMZ (Command Prompt): ping 192.168.1.10 (Ping a PC_Internal). Resultado esperado: Request timed out

Como se ve en la siguiente tabla el test de conectividad de las instancias de la red en cisco marca como aprobadas las configuraciones:

Below are the results of your connectivity tests:

	Status	Test Condition	Points	Source	Destination	Type
1	Correct	Successful	1	PC_Internal	192.168.1.1 : 192.168.1.1	ICMP
2	Correct	Successful	1	Web_DMZ	192.168.2.1 : 192.168.2.1	ICMP
3	Correct	Successful	1	PC_External	192.168.3.1 : 192.168.3.1	TCP
4	Correct	Successful	1	PC_Internal	192.168.2.10 : 192.168.2.10	TCP
5	Correct	Fail	2	Web_DMZ	PC_Internal : 192.168.1.10	ICMP
6	Correct	Fail	3	PC_External	192.168.3.1 : 192.168.3.1	ICMP
7						
8						

6. Conclusiones y recomendaciones

Este ejercicio ha servido como referencia para entender desde las bases, cómo se aplican las reglas que pueden proteger una red, creando así una zona desmilitarizada o DMZ. Esto nos permite elaborar planes de acción adecuados al momento de configurar una red, ya sea para entornos empresariales pero también para poder interpretar la lógica detrás de los comandos.

Cabe resaltar que el ejercicio requiere de precisión en cuanto a los comandos ejecutados, de ahí la importancia de el test de configuraciones, una mala configuración puede suponer un fallo grande en la red y una vulnerabilidad explotable. Se recomienda entonces trabajar con proyectos más complejos que impliquen una cantidad mayor de instancias para aumentar su complejidad y así también su entendimiento.

7. Capturas de evidencia

A continuación se muestran las capturas correspondientes a los pasos realizados para elaborar el proceso de configuración de la red :

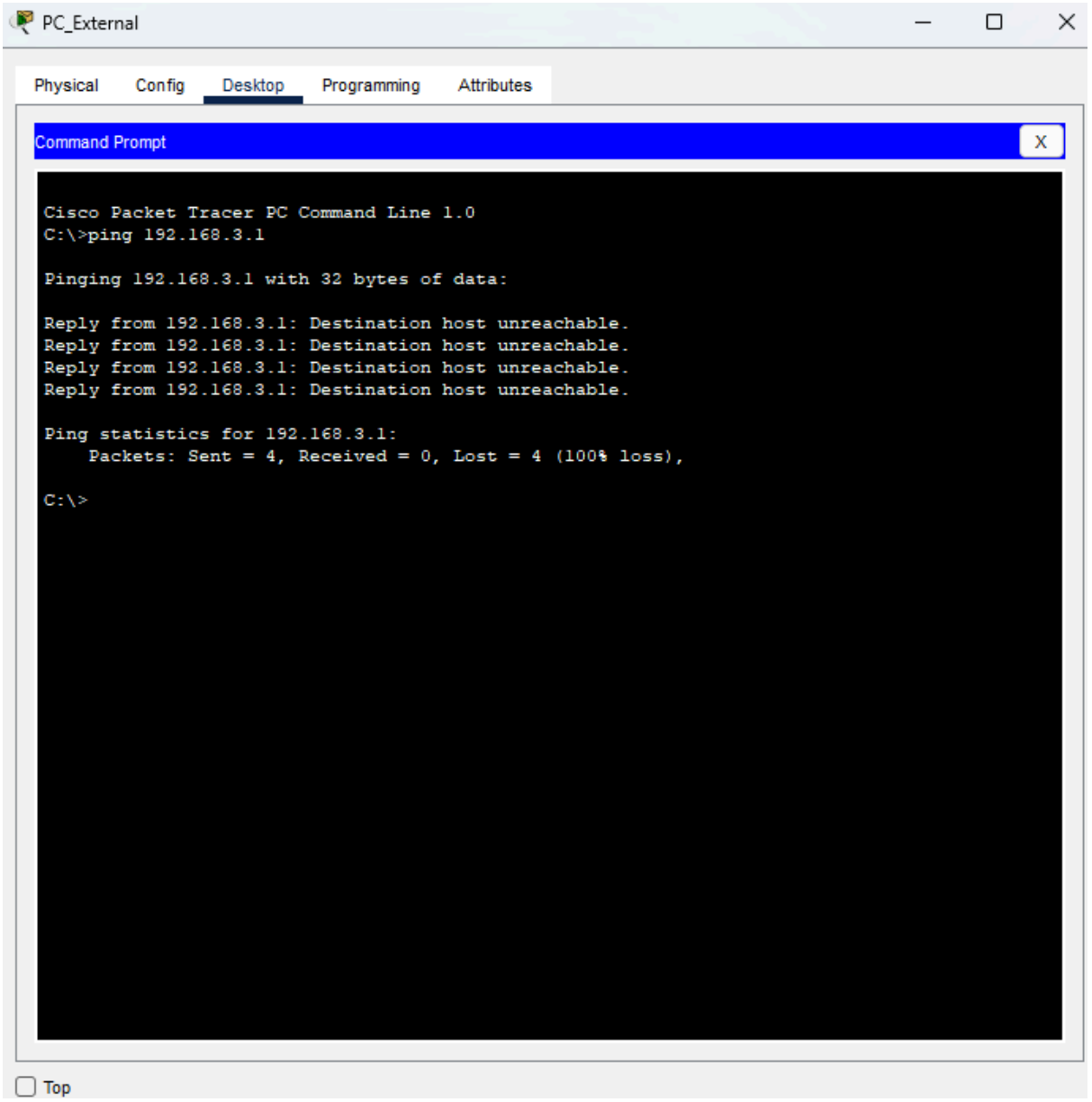
Comando clave del ejercicio

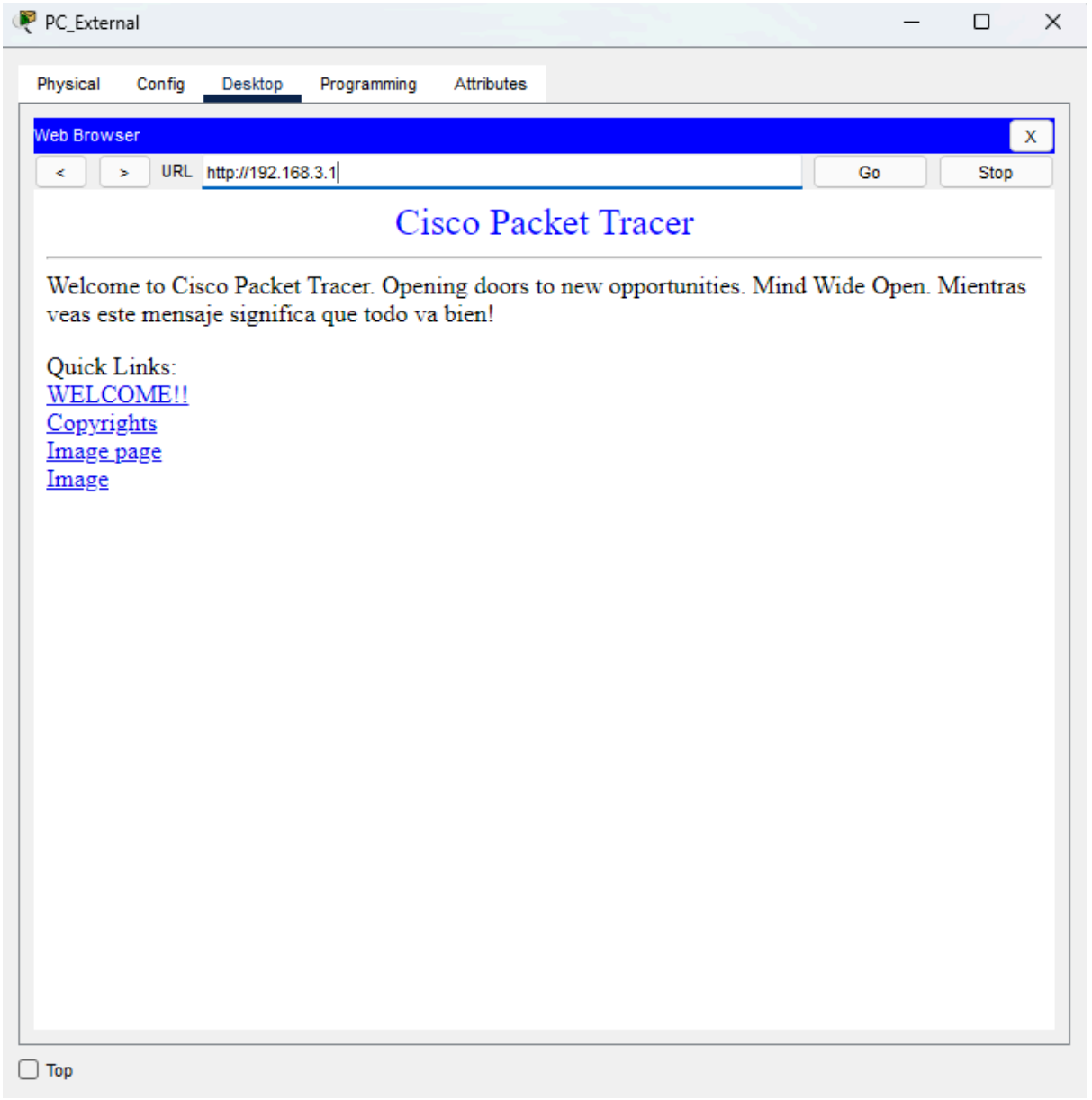
plaintext Copy Edit

```
no access-list 101
access-list 101 permit tcp any any established
access-list 101 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 101 permit ip any any
```

Configuraciones de las Access control lists:

```
Router_FW(config-if)# no shutdown
Router_FW(config-if)# exit
Router_FW(config)#
Router_FW(config)#! NAT esttico: publica 192.168.2.10 como 192.168.3.1
Router_FW(config)#ip nat inside source static 192.168.2.10 192.168.3.1
Router_FW(config)#
Router_FW(config)#! ACL 100: permite nicamente trfico HTTP hacia la IP pblica del
servidor
Router_FW(config)#access-list 100 permit tcp any host 192.168.3.1 eq 80
Router_FW(config)#access-list 100 deny ip any any
Router_FW(config)#
Router_FW(config)#! ACL 101: permite trfico TCP de retorno y bloquea nuevos inicios desde
la DMZ a la LAN
Router_FW(config)#access-list 101 permit tcp any any established
Router_FW(config)#access-list 101 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Router_FW(config)#access-list 101 permit ip any any
Router_FW(config)#emd

Router_FW#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router_FW(config)#no access-list 101
Router_FW(config)#access-list 101 permit tcp any any established
Router_FW(config)#access-list 101 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Router_FW(config)#access-list 101 permit ip any any
Router_FW(config)#end
Router_FW#
%SYS-5-CONFIG_I: Configured from console by console

Router_FW#write memory
Building configuration...
[OK]
Router_FW#
```


PC_External
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
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.
Ping statistics for 192.168.3.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top


PC_External
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://192.168.3.1
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open. Mientras veas este mensaje significa que todo va bien!
Quick Links:
WELCOME!!
Copyrights
Image page
Image
Top

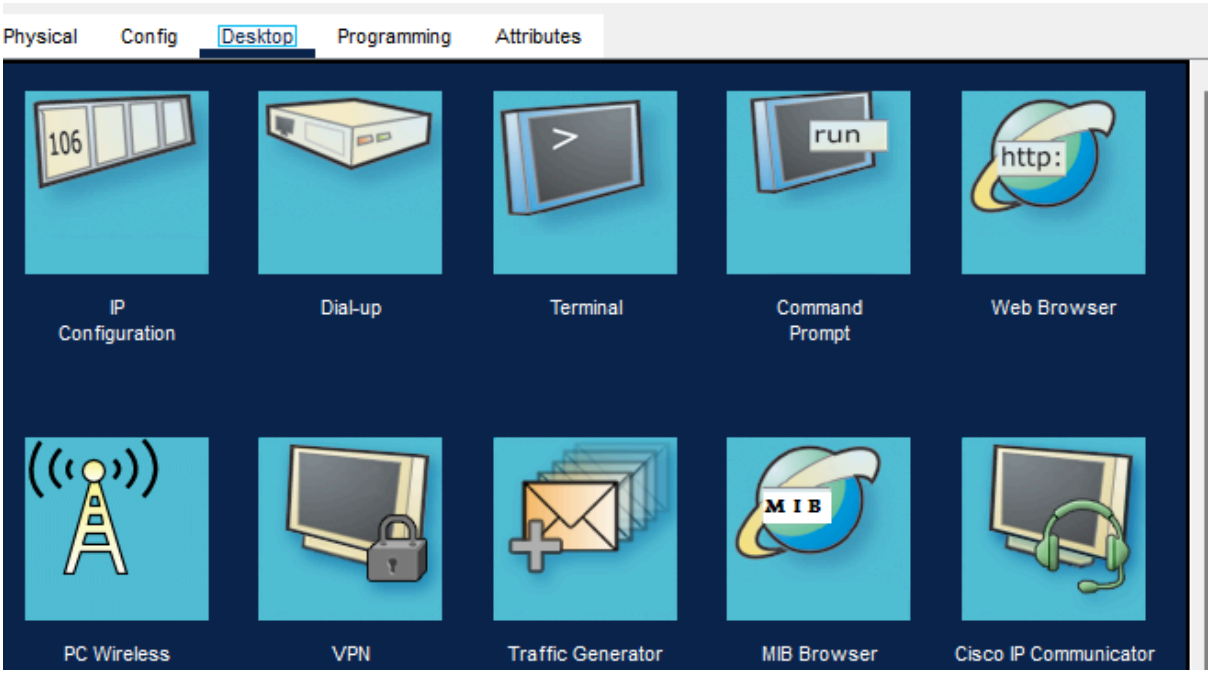
```
Router_FW#show access-lists
Extended IP access list 101
    10 permit tcp any host 192.18.3.1 eq www

Router_FW#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router_FW(config)#access-list 102 deny ip 192.168.2.0 0.0.255 192.168.1.0 0.0.255
                                                       ^
% Invalid input detected at '^' marker.

Router_FW(config)#access-list 102 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.255
                                                                             ^
% Invalid input detected at '^' marker.

Router_FW(config)#access-list 102 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Router_FW(config)#access-list 102 permit ip any any
Router_FW(config)#interface GigabitEthernet0/1
Router_FW(config-if)#ip access-group 102 in
Router_FW(config-if)#exit
Router_FW(config)#end
Router_FW#
%SYS-5-CONFIG_I: Configured from console by console
show
% Incomplete command.
Router_FW#show access-list
Extended IP access list 101
    10 permit tcp any host 192.18.3.1 eq www
Extended IP access list 102
    10 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
    20 permit ip any any

Router_FW#
```

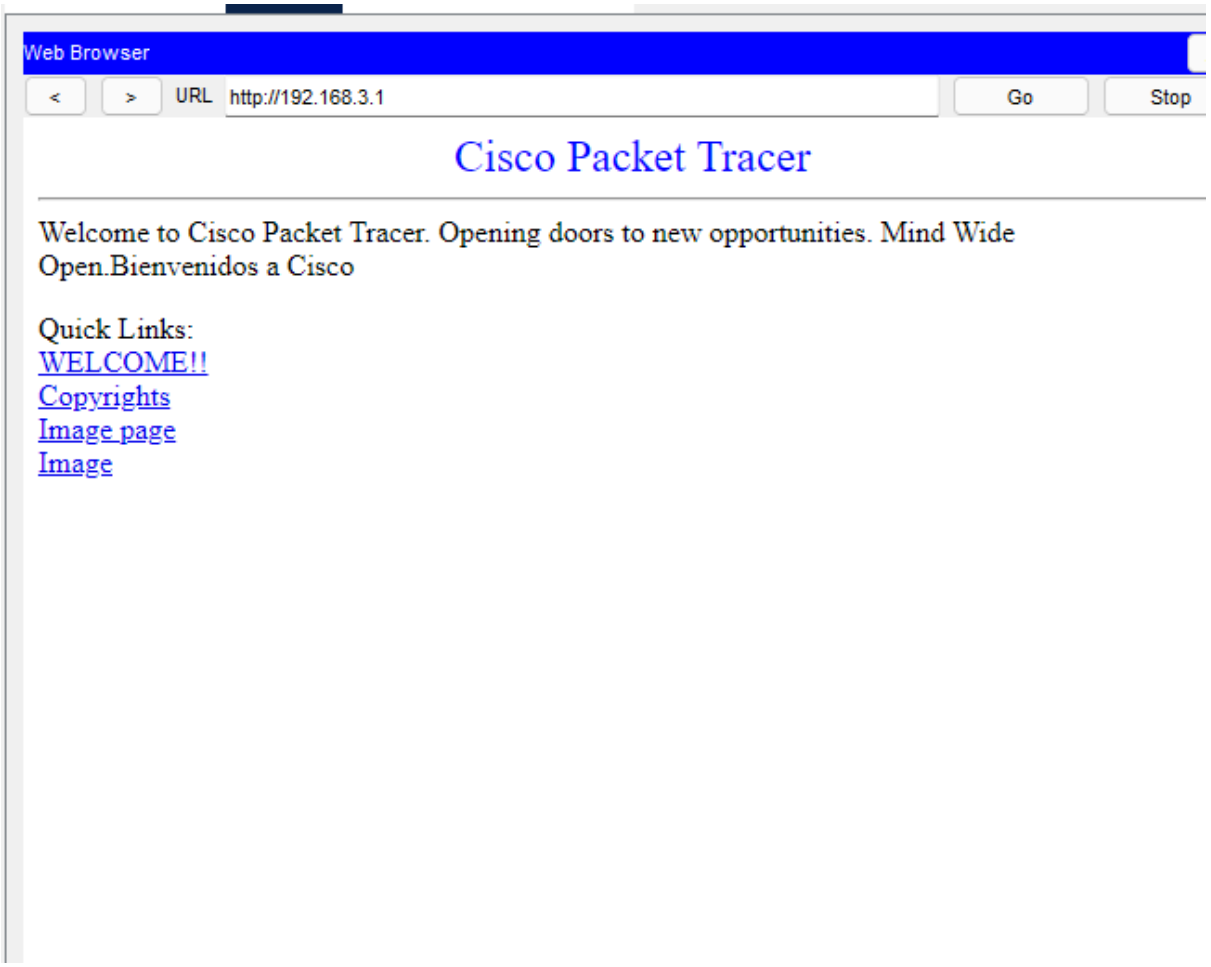
- **Acceso Web desde Internet a DMZ:**
    - Crea una ACL que permita **solamente** el tráfico HTTP (puerto 80) desde *cualquier origen* (`any`) hacia la IP pública de tu servidor web DMZ (`192.168.3.1`).
    - Esta ACL debe aplicarse a la interfaz `GigabitEthernet0/2` (WAN) en sentido `inbound`.
    - Por defecto, esta ACL implícitamente denegará otros tipos de tráfico desde Internet (incluido ICMP/ping).

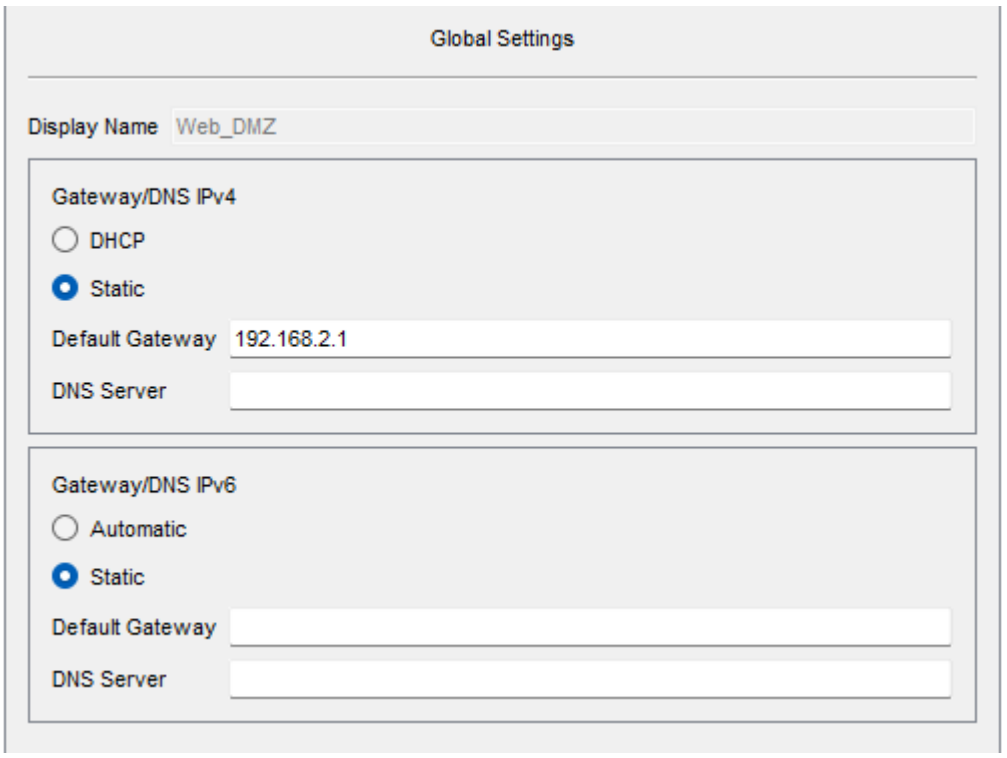
Cisco Packet Tracer

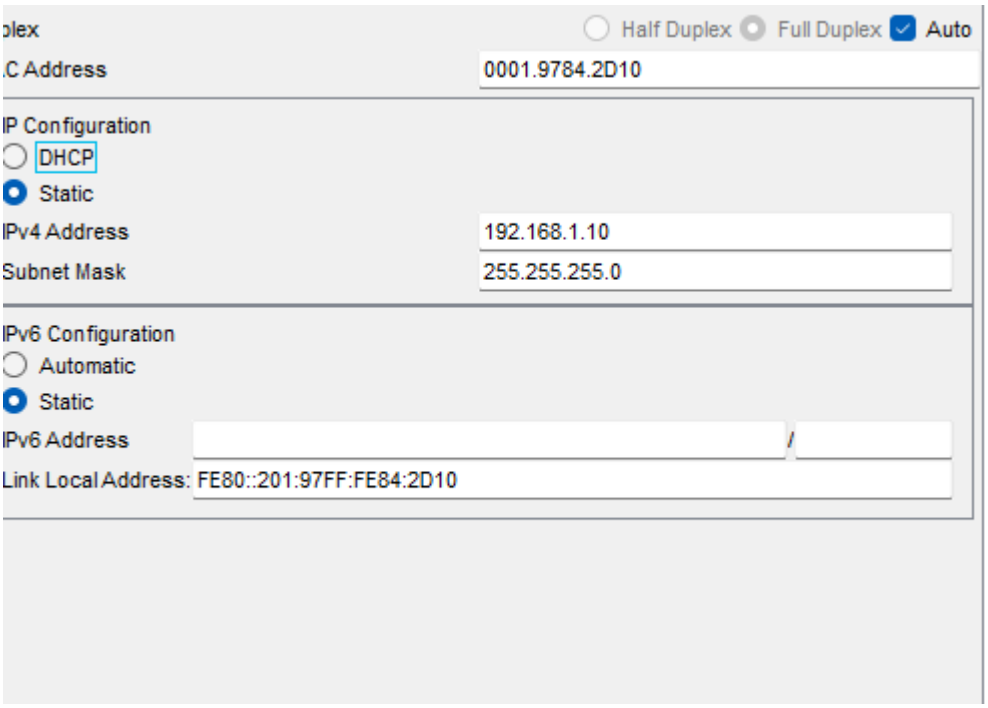
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.Bienvenidos a Cisco

Quick Links:
WELCOME!!
Copyrights
Image page
Image


Physical
Config
Desktop
Programming
Attributes
106
IP Configuration
Dial-up
Terminal
run
Command Prompt
http:
Web Browser
PC Wireless
VPN
Traffic Generator
MIB
MIB Browser
Cisco IP Communicator


Web Browser
<
>
URL
http://192.168.3.1
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.Bienvenidos a Cisco
Quick Links:
WELCOME!!
Copyrights
Image page
Image


Global Settings
Display Name
Web_DMZ
Gateway/DNS IPv4
DHCP
Static
Default Gateway
192.168.2.1
DNS Server
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server


lex
Half Duplex
Full Duplex
Auto
C Address
0001.9784.2D10
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.10
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address:
FE80::201:97FF:FE84:2D10

Paso 1: Configuración de Direccionamiento IP en Dispositivos Finales

Configura las direcciones IP estáticas en tus dispositivos finales. **¡Presta especial atención a estas IPs, ya que son cruciales para la evaluación automática!**

- **En `PC_Internal` (Desktop -> IP Configuration):**
  - `IP Address`: **192.168.1.10**
  - `Subnet Mask`: **255.255.255.0**
  - `Default Gateway`: **192.168.1.1**
- **En `Server-PT Web_DMZ` (Desktop -> IP Configuration):**
  - `IP Address`: **192.168.2.10**
  - `Subnet Mask`: **255.255.255.0**
  - `Default Gateway`: **192.168.2.1**
- **En `PC_External` (Desktop -> IP Configuration):**
  - `IP Address`: **192.168.3.10**
  - `Subnet Mask`: **255.255.255.0**
  - `Default Gateway`: **192.168.3.1**