Informe de configuraciÃ³n de DMZ con Cisco Packet Tracer

1. Objetivo del laboratorio

Diseñar, configurar y asegurar una arquitectura de red con DMZ utilizadno el rpouter.
el objetivo principal ha sido permitir el acceso publico a un servidor web situado en la DMZ mediante el NAT estatico protegiendo a su vez la red lan interna de accesos no autorizados medaite el uso de ACLs y filtrado de trafico.

Ejemplo:

Configurar una DMZ segura usando un router Cisco ISR, aplicando NAT y ACLs para controlar el trÃ¡fico entre LAN, DMZ y red externa.

---

2. TopologÃa implementada

Cantidad de redes: 3 segmentos distintos.

Dispositivos usados: 1 Router Cisco, 3 Switches Cisco 2960, 1 Servidor, 2 PCs.

Descripción de zonas:

- **LAN Interna (192.168.1.0/24):** Zona de confianza donde residen los usuarios (PC_Internal). Debe estar protegida de Internet y de la DMZ.
- **DMZ (192.168.2.0/24):** Zona de seguridad media donde reside el servidor web. Es accesible desde Internet pero no tiene permisos para iniciar conexiones hacia la LAN.
- **Red Externa (192.168.3.0/24):** Simulación de Internet (ISP) y usuarios remotos.

- Cantidad de redes: _____

- Dispositivos usados: _____

- Breve descripciÃ³n de la funciÃ³n de cada zona (LAN, DMZ, Externa).

3. Plan de direccionamiento IP

Completa la tabla con las IPs asignadas (puedes copiarla del enunciado si no cambiÃ³).

Dispositivo	IP	MÃ¡scara	Gateway
PC_Internal			
Server_DMZ			
PC_External			
Router_FW Gi0/0 (LAN)	192.168.1.1	255.255.255.0	
Router_FW Gi0/1 (DMZ)	192.168.2.1	255.255.255.0	
Router_FW Gi0/2 (Ext)	192.168.3.1	255.255.255.0	

PC_Internal192.168.1.10 | 255.255.255.0 | 192.168.1.1

Server_DMZ192.168.2.10 | 255.255.255.0 | 192.168.2.1

PC_External192.168.3.10 | 255.255.255.0 | 192.168.3.1

4. ConfiguraciÃ³n aplicada (resumen)

> Resume los comandos o pasos mÃ¡s relevantes que ejecutaste. Usa texto + fragmentos de cÃ³digo cuando sea necesario.

- Interfaces configuradas con `ip address`

NAT Estático (Publicación del Servicio): Se mapeó la IP privada del servidor a la IP pública de la interfaz WAN para permitir acceso externo.
Listas de Control de Acceso (ACLs):

ACL 100 (Externa - Inbound): Permite solo tráfico web (Puerto 80) destinado a la IP pública.

CL 101 (DMZ - Inbound): Esta fue la configuración crítica. Se tuvo que permitir el tráfico de retorno para que los usuarios internos pudieran ver la web, bloqueando al mismo tiempo ataques iniciados desde la DMZ

! 1. Permitir respuestas a conexiones legítimas de la LAN

access-list 101 permit tcp any 192.168.1.0 0.0.0.255 established

! 2. Bloquear cualquier intento de inicio de conexión DMZ -> LAN

access-list 101 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

! 3. Permitir tráfico hacia Internet

access-list 101 permit ip any any

5. Verificaciones realizadas

Acceso Web	PC_External	192.168.3.1	Éxito (Carga web)
Seguridad (Ping)	PC_External	192.168.3.1	Fallo (Bloqueado)
Seguridad Crítica	Server_DMZ	192.168.1.10	Fallo (Bloqueado)
Funcionalidad Interna	PC_Internal	192.168.2.10	Éxito (Carga web)

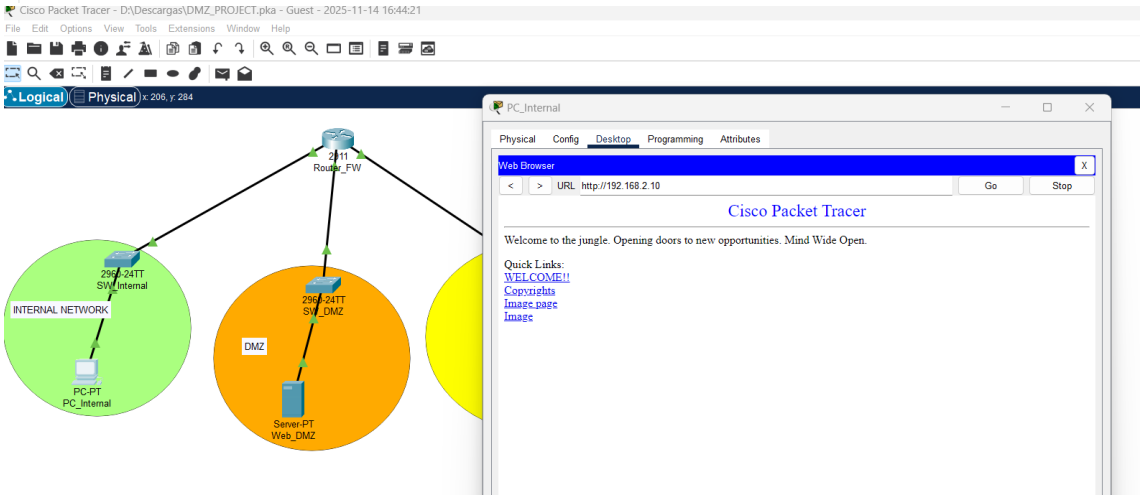
6. Conclusiones y recomendaciones

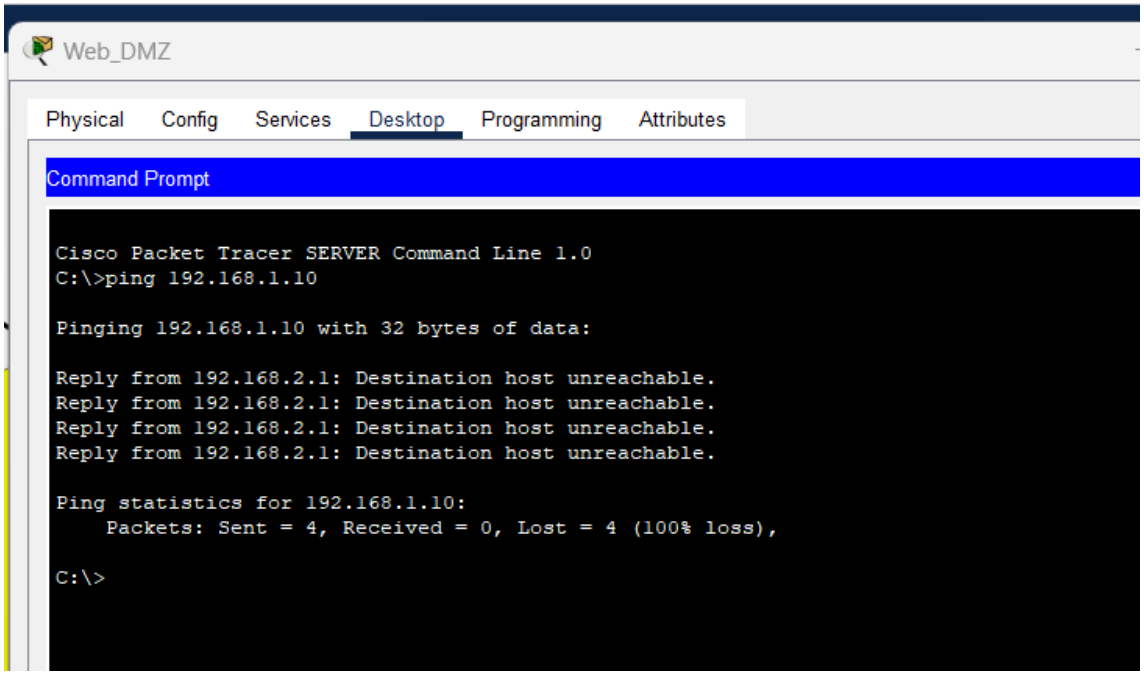
Aprendí que las ACLs bloquean paquetes en ambas direcciones si no se tiene cuidado. Lo complicado fue que la ACL de la DMZ bloqueaba las respuestas del servidor hacia la LAN.

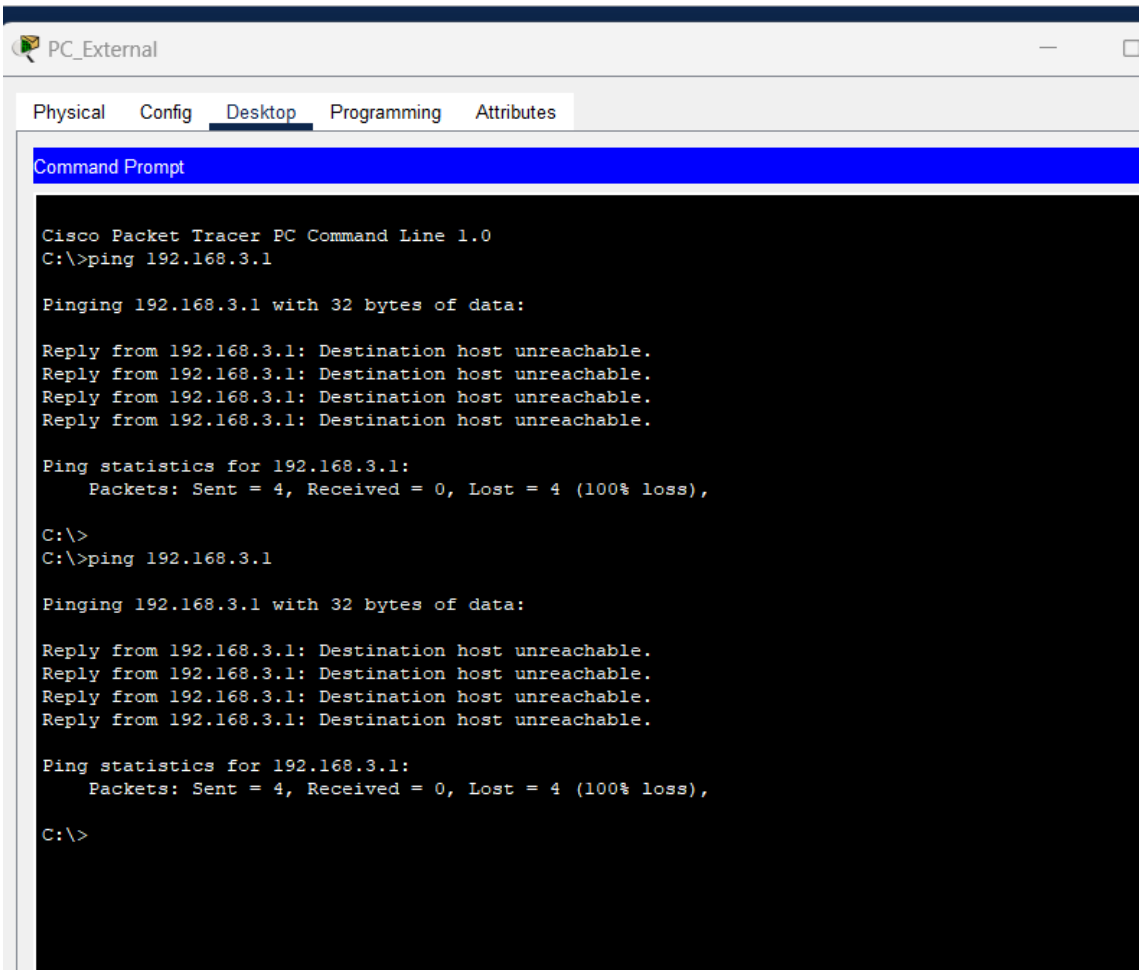
7. Capturas de evidencia

ow are the results of your connectivity tests:

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






PC_External
Physical
Config
Desktop
Programming
Attributes
Command Prompt
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:\>
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:\>