Informe Técnico: Configuración y Aseguramiento de una DMZ

Estudiante: Samuel Quetzni López López

Fecha: 01-01-26

Laboratorio: Construyendo y Asegurando una Red con una DMZ

1. Introducción

Este informe detalla el proceso de configuración de una Zona Desmilitarizada (DMZ) utilizando Cisco Packet Tracer. El objetivo principal fue aislar servicios críticos, controlar el tráfico mediante Listas de Control de Acceso (ACL) y configurar NAT estático para permitir el acceso controlado desde una red externa.

2. Topología y Direccionamiento

Se configuraron tres zonas distintas en el router central Router_FW:

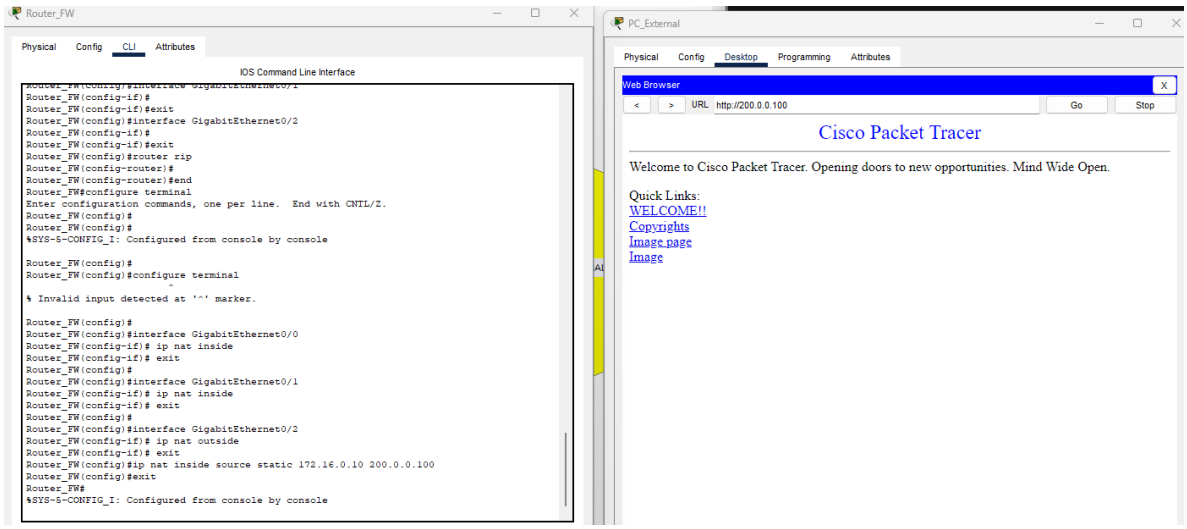
Dispositivo	Interfaz	Dirección IP	Gateway
PC_Internal (LAN)	G0/0	192.168.10.10	192.168.10.1
Server-PT Web_DMZ	G0/1	172.16.0.10	172.16.0.1
PC_External (Internet)	G0/2	200.0.0.10	200.0.0.1

3. Configuración de NAT Estático

Para permitir que el servidor web sea accesible desde el exterior (Internet) sin exponer su IP privada real, se configuró un mapeo NAT estático.

Comandos aplicados:

- ✓ ip nat inside source static 172.16.0.10 200.0.0.100



4. Implementación de Seguridad (ACLs)

Se aplicaron Listas de Control de Acceso para restringir el tráfico innecesario y proteger la red interna.

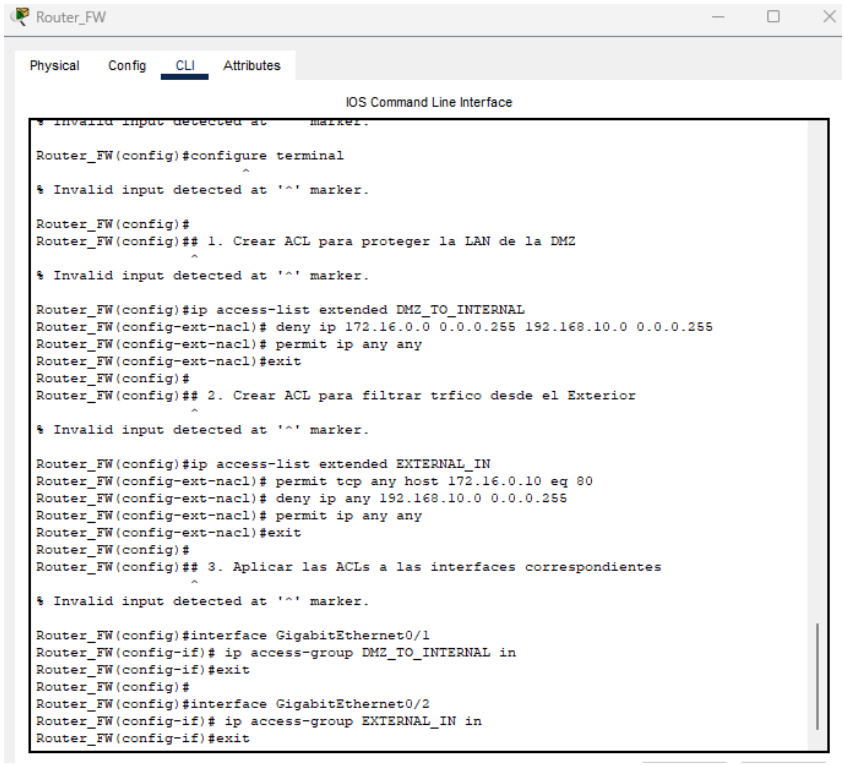
ACL: DMZ_TO_INTERNAL (Entrante en G0/1)

Bloquea cualquier tráfico originado en la DMZ que intente llegar a la red LAN interna.

- **Resultado esperado:** El servidor no puede hacer ping a la PC interna.
- **Estado:** Verificado.

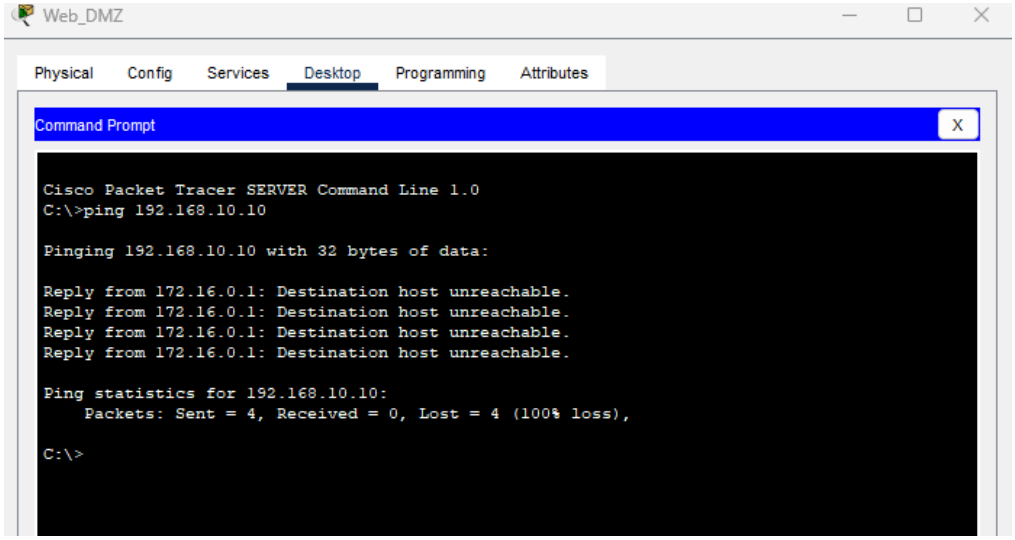
ACL: EXTERNAL_IN (Entrante en G0/2)

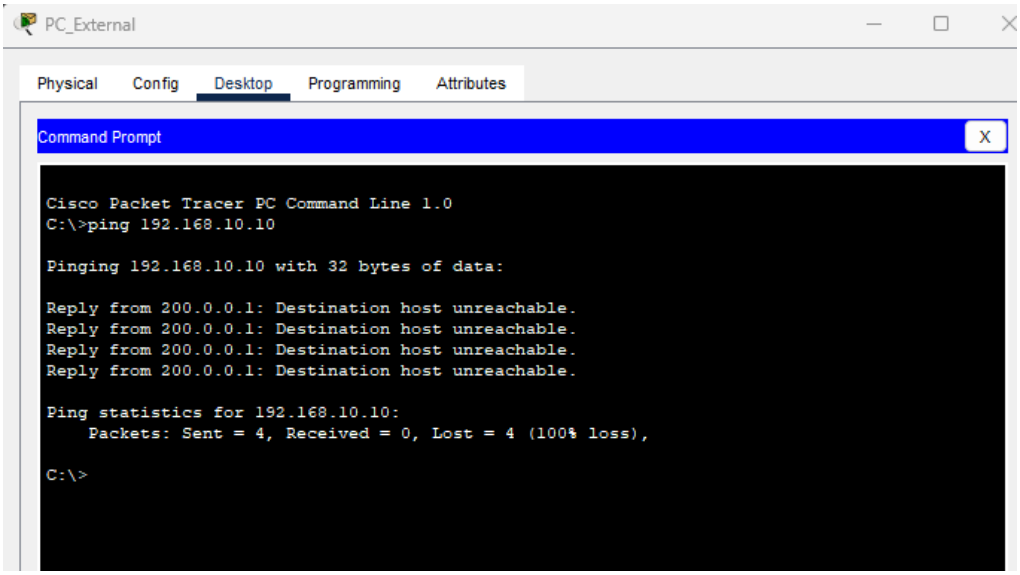
Solo permite tráfico HTTP (puerto 80) hacia el servidor y bloquea el acceso directo a la LAN interna.



5. Pruebas de Validación (Resultados)

Origen	Destino	Tipo de Tráfico	Resultado
PC_External	200.0.0.100	HTTP (Puerto 80)	**ÉXITO**
PC_Internal	172.16.0.10	Ping (ICMP)	**ÉXITO**
Server_DMZ	192.168.10.10	Ping (ICMP)	**BLOQUEADO**
PC_External	192.168.10.10	Ping (ICMP)	**BLOQUEADO**





6. Conclusiones

La implementación de la DMZ fue exitosa. Se logró un equilibrio entre **disponibilidad** (el servidor web es visible para el mundo) y **seguridad** (la red interna está protegida mediante ACLs). El uso de NAT estático permitió ocultar la topología interna, mientras que las reglas de filtrado garantizaron que un compromiso potencial del servidor en la DMZ no se propague lateralmente hacia la red interna.