Informe de Configuración de DMZ con Cisco Packet Tracer

1. Objetivo del laboratorio

El objetivo principal de este laboratorio fue configurar una Zona Desmilitarizada (DMZ) segura utilizando un router Cisco ISR en Cisco Packet Tracer. Se buscó implementar y verificar la funcionalidad de la Traducción de Direcciones de Red (NAT) y las Listas de Control de Acceso (ACLs) para controlar y asegurar el flujo de tráfico de red entre la red LAN interna, la DMZ y la red externa (Internet simulado). Específicamente, se puso énfasis en permitir el acceso seguro a servicios web en la DMZ desde el exterior, mientras se protegía la red interna de accesos no autorizados originados en la DMZ.

2. Topología implementada

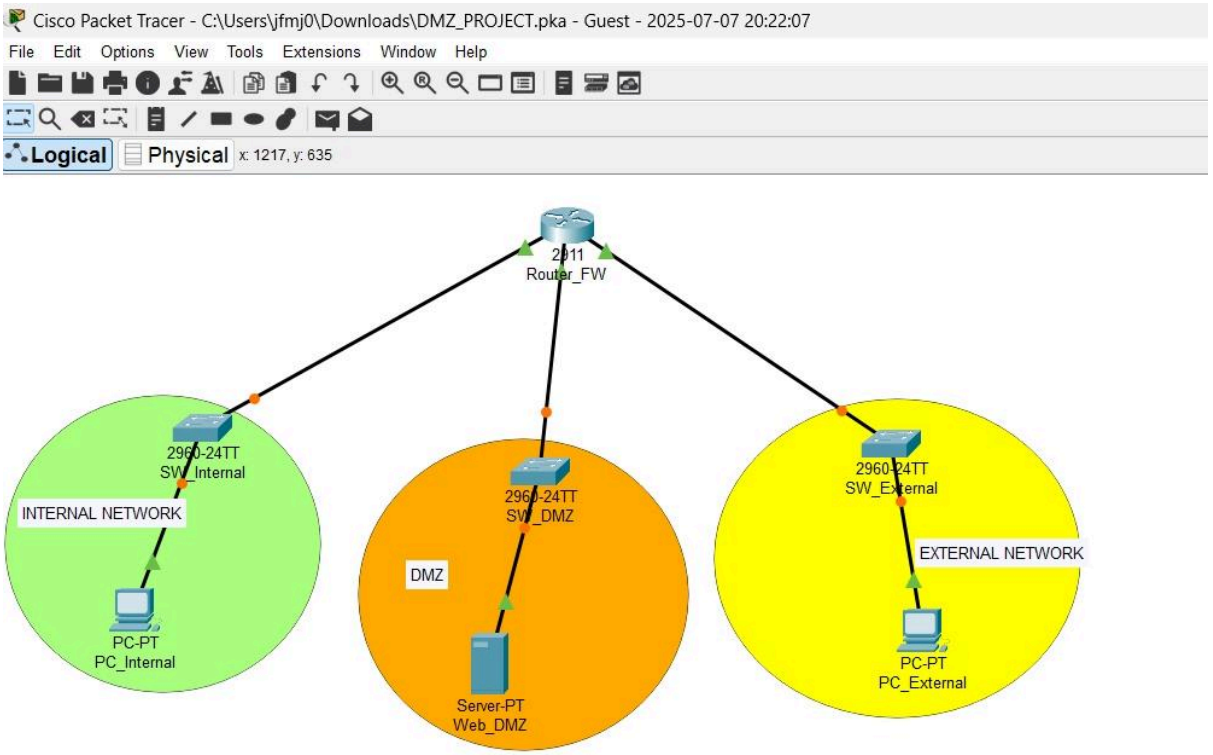
La red implementada consiste en una topología de tres zonas bien diferenciadas:

- **Cantidad de redes:** 3 (LAN interna, DMZ y Externa/WAN)
- **Dispositivos utilizados:**
    - 1 enrutador Cisco ISR (modelo 2911, que actúa como firewall/enrutador de borde)
    - 3x Switches 2960-24TT (uno para la red interna, uno para la DMZ y uno para la red externa)
    - 1x PC de usuario interno (PC_Internal)
    - 1x Servidor web en la DMZ (Server-PT Web_DMZ)
    - 1x PC externo (PC_External)

Breve descripción de la función de cada zona:

- **LAN Interna (INTERNAL NETWORK - Verde):** Representa la red local de la organización. Contiene estaciones de trabajo (PC_Internal) que necesitan acceso seguro a Internet y a los servicios en la DMZ, pero deben estar protegidas de accesos no deseados desde la DMZ o la red externa.

- **DMZ (Naranja):** Zona de seguridad intermedia donde se alojan servidores accesibles desde Internet (Server-PT Web_DMZ). Esta zona está aislada de la LAN interna por el firewall, permitiendo un acceso controlado desde el exterior sin exponer directamente la red interna. También tiene una dirección IP pública simulada (192.168.3.1, según el plan de direccionamiento) para el acceso externo al servidor web.
- **Red Externa (EXTERNAL NETWORK - Amarilla/Naranja):** Representa Internet. Contiene un host (PC_External) que intenta acceder a los servicios de la DMZ y verificar el bloqueo de otros tipos de tráfico.



3. Plan de direccionamiento IP

A continuación, se detalla el plan de direccionamiento IP implementado para cada dispositivo y zona de la red.

Dispositivo	Propiedad intelectual	Mascarilla	Puerta
PC_Internal	192.168.1.10	255.255.255.0	192.168.1.1
Servidor_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	N / A
Router_FW Gi0/1 (DMZ)	192.168.2.1	255.255.255.0	N / A
Router_FW Gi0/2 (Ext.)	192.168.3.1	255.255.255.0	N / A

4. Configuración aplicada

A continuación, se resumen los comandos de configuración clave aplicados en el Router_FW.

4.1. Configuración de Interfaces IP:

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

Router_FW(config)# interface GigabitEthernet0/1
Router_FW(config-if)# ip address 192.168.2.1 255.255.255.0
Router_FW(config-if)# ip nat inside
Router_FW(config-if)# ip access-group 101 in  // Aplicación de ACL para DMZ a LAN
Router_FW(config-if)# no shutdown

Router_FW(config)# interface GigabitEthernet0/2
Router_FW(config-if)# ip address 192.168.3.1 255.255.255.0 // (O la IP pública asignada)
Router_FW(config-if)# ip nat outside
Router_FW(config-if)# ip access-group 100 in  // Aplicación de ACL para Internet a DMZ
Router_FW(config-if)# no shutdown
```

4.2. Configuración de NAT (Traducción de Direcciones de Red):

Se configuró NAT estático para el servidor web de la DMZ, permitiendo que la IP privada del servidor (192.168.2.10) sea accesible desde la red externa a través de una IP pública simulada (192.168.3.1).

Router_FW(config)# ip nat inside source static 192.168.2.10 192.168.3.1

4.3. Configuración de ACLs (Listas de Control de Acceso):

a) ACL para Acceso Web desde Internet a DMZ (ACL 100): Aplicada a la interfaz GigabitEthernet0/2 (WAN) en sentido inbound. Esta ACL solo permite el tráfico HTTP (puerto 80) hacia el servidor web de la DMZ (192.168.3.1) y deniega todo lo demás, incluyendo ICMP (ping), desde Internet.

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

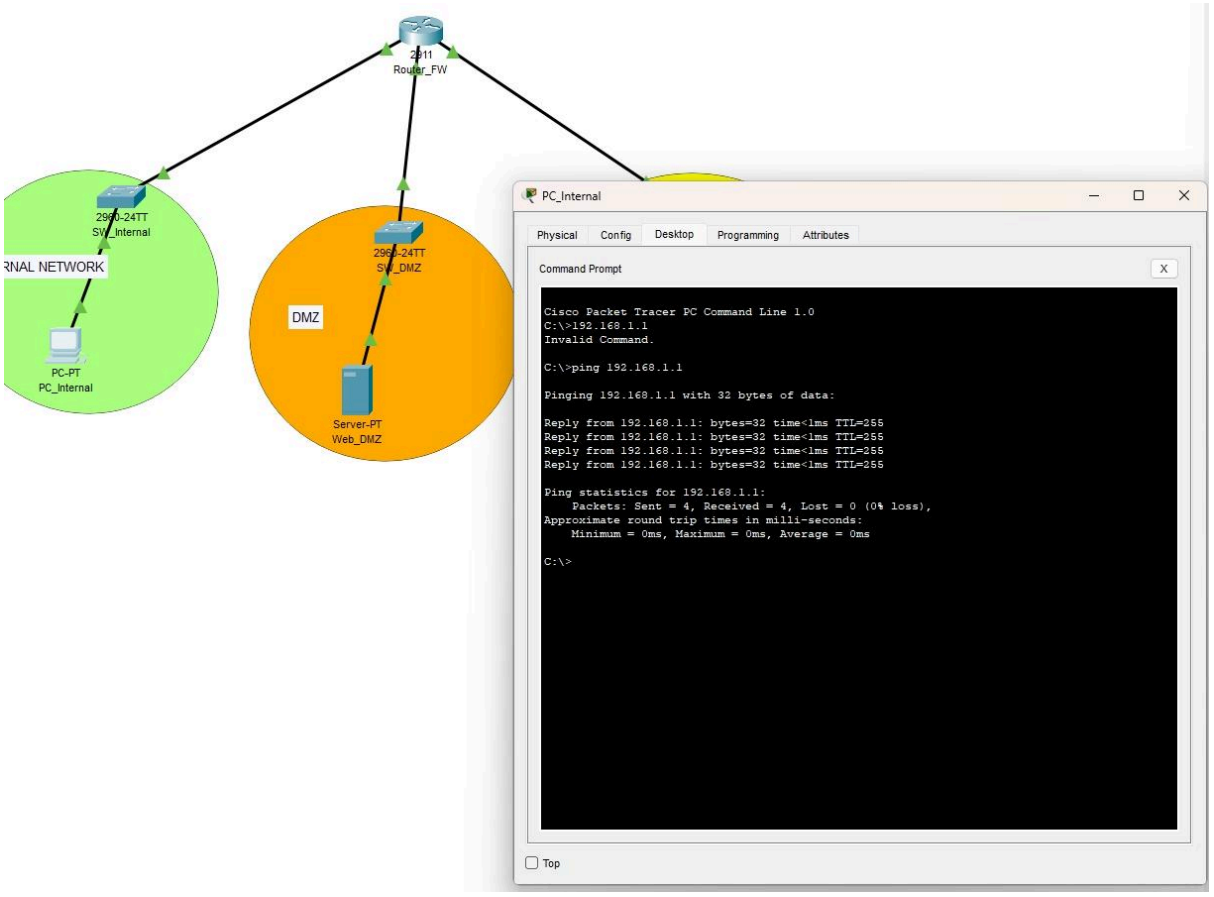
b) ACL para Seguridad DMZ a LAN (ACL 101): Aplicada a la interfaz GigabitEthernet0/1 (DMZ) en sentido inbound. Esta ACL es crítica para la seguridad, denegando cualquier intento de comunicación iniciado desde la DMZ (192.168.2.0/24) hacia la red LAN interna (192.168.1.0/24). Además, incluye una regla para permitir el tráfico de respuesta para conexiones TCP iniciadas por la LAN hacia la DMZ.

Router_FW(config)# access-list 101 permit tcp any 192.168.1.0 0.0.0.255 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

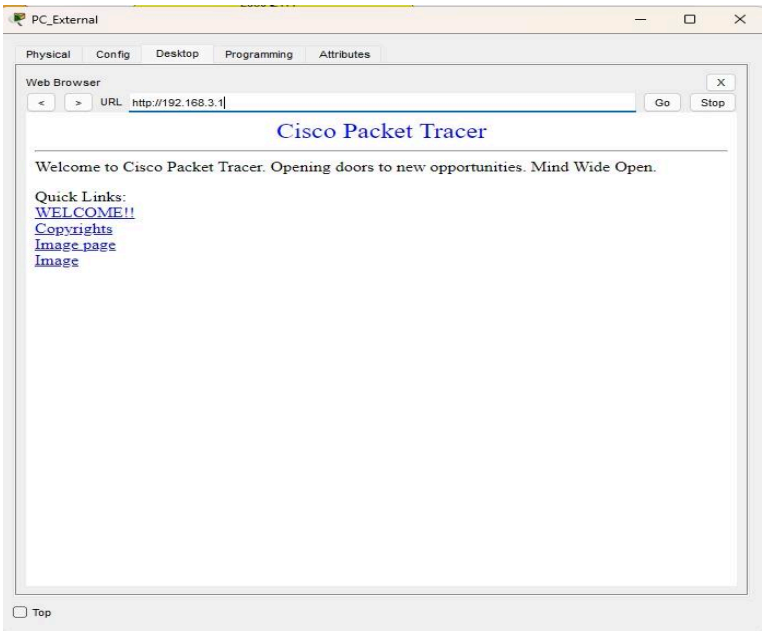
5. Verificaciones realizadas

Se realizaron diversas pruebas de conectividad y seguridad para validar la configuración.

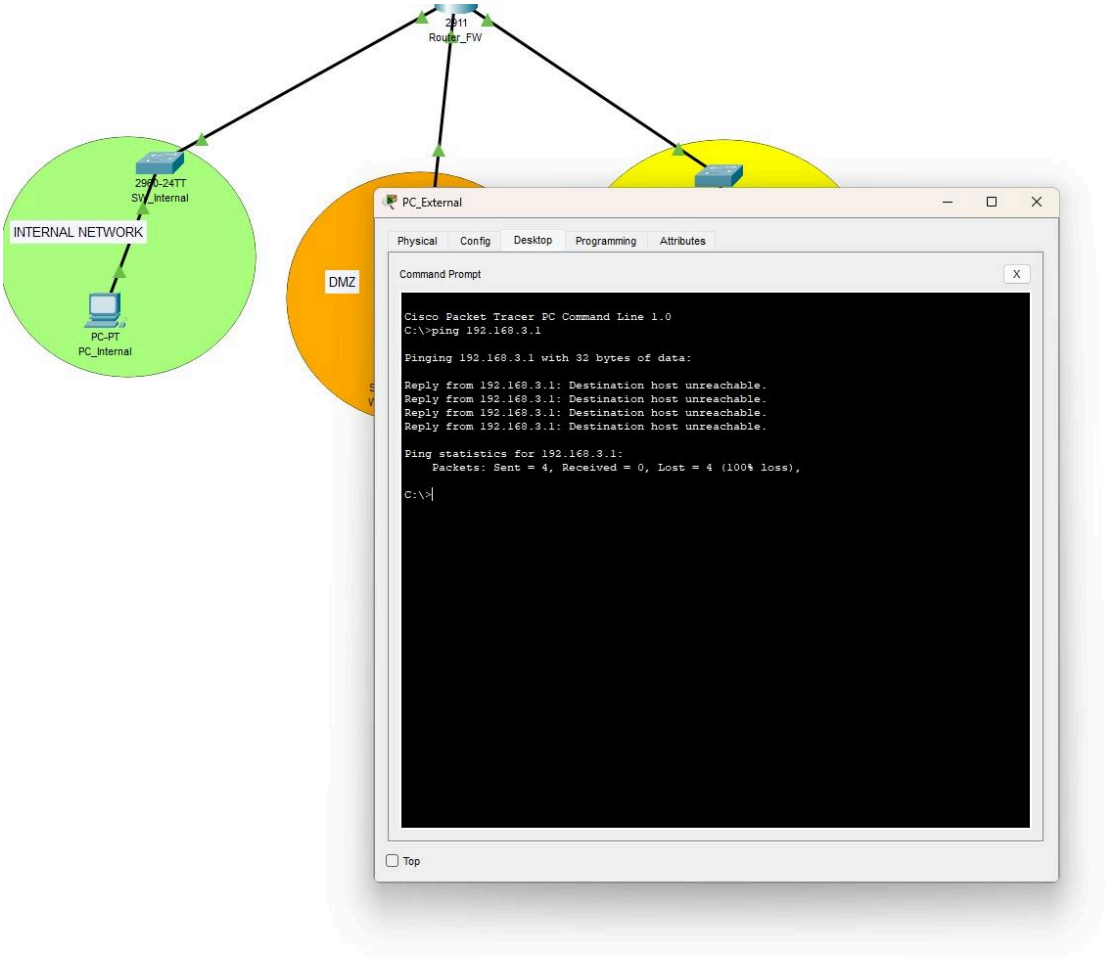
- **ping desde PC_Internal al router:**
    - **Comando:** ping 192.168.1.1 (desde PC_Internal)
    - **Resultado esperado:** Éxito (Reply from...).



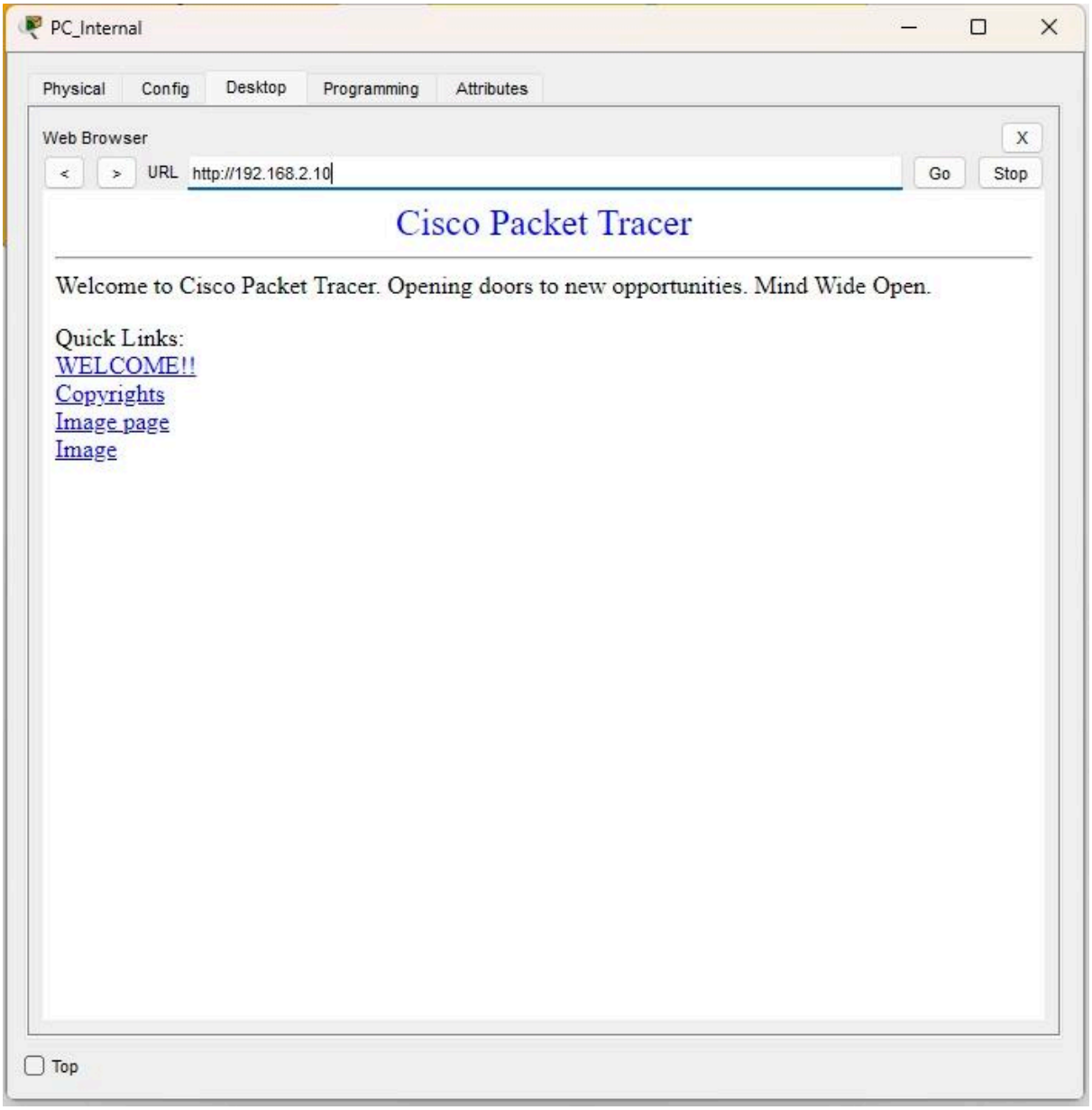
- **Acceso web desde PC_External al servidor DMZ:**
  - **Comando:** Abrir navegador web en PC_External y acceder a 192.168.3.1.
  - **Resultado esperado:** La página web debe cargar correctamente.



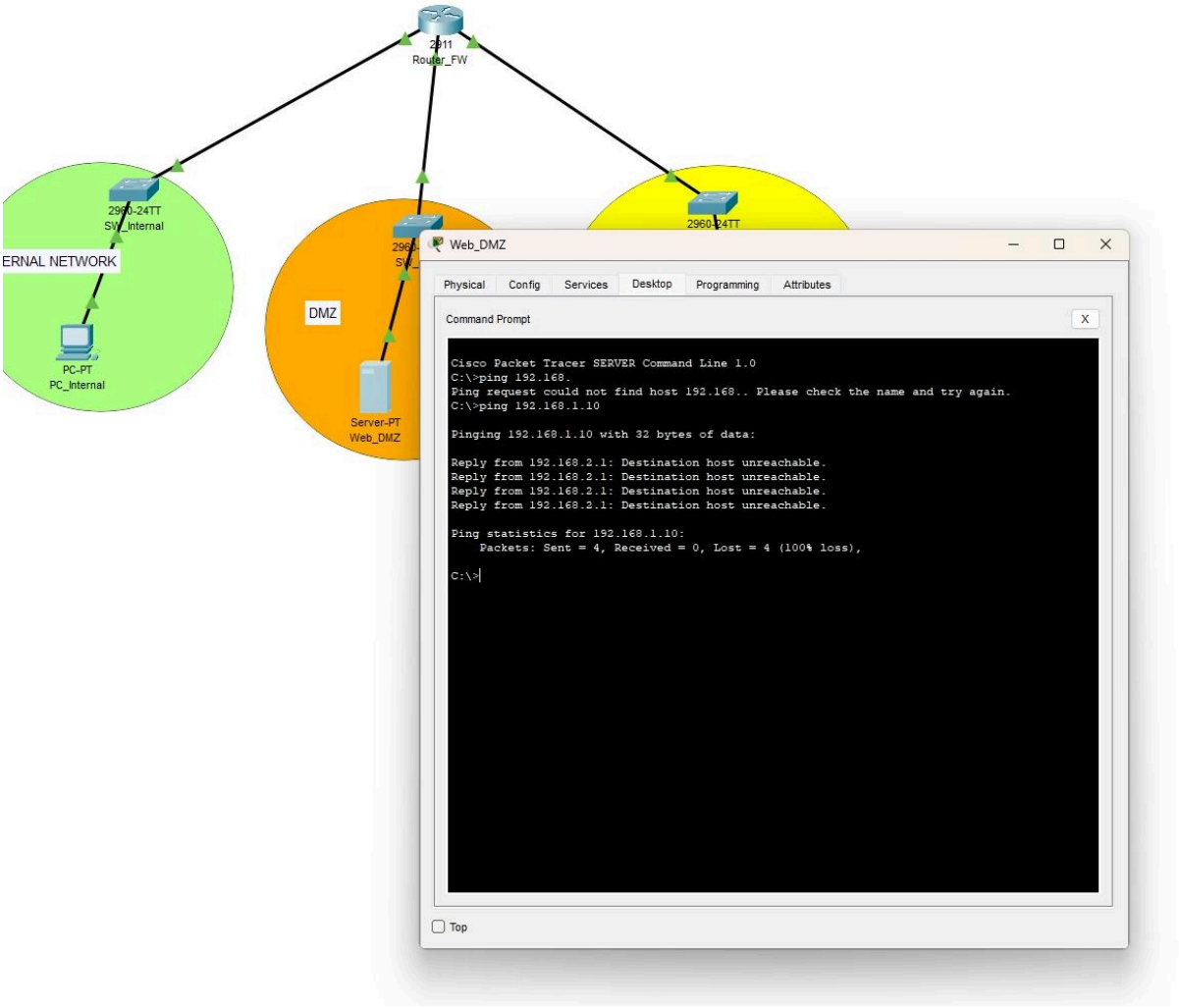
- **Bloqueo de ICMP (ping) desde PC_External al servidor DMZ (IP pública):**
    - **Comando:** ping 192.168.3.1 (desde PC_External)
    - **Resultado esperado:** Request timed out (o Destination host unreachable), indicando que el tráfico ICMP es denegado por la ACL.



- **Acceso web desde PC_Internal al servidor DMZ:**
    - **Comando:** Abrir navegador web en PC_Internal y acceder a 192.168.2.10.
    - **Resultado esperado:** La página web debe cargar correctamente.



- **Bloqueo de acceso desde DMZ a LAN (ping de Server_DMZ a PC_Internal):** ✅
    - **Comando:** ping 192.168.1.10 (desde Server_DMZ)
    - **Resultado esperado:** Request timed out (o Destination host unreachable), confirmando que el tráfico iniciado desde la DMZ hacia la LAN es denegado. Este fue un punto clave de verificación de seguridad.



6. Conclusiones y recomendaciones

Este laboratorio fue fundamental para comprender la importancia de una DMZ en la arquitectura de red y cómo las herramientas de seguridad como NAT y ACLs son aplicadas en un router Cisco. Aprendí a:

- Configurar interfaces de red y gateways en diferentes segmentos de red.
- Implementar NAT estático para exponer servicios internos de forma segura a Internet.
- Diseñar y aplicar ACLs extendidas para filtrar tráfico basado en protocolo, puertos, y direcciones de origen/destino, crucial para la micro-segmentación de la red.

- Entender la diferencia entre las direcciones "inside" y "outside" para la funcionalidad NAT.
- Reconocer la importancia del orden de las reglas en una ACL y cómo una regla general (permit ip any any) debe ubicarse estratégicamente.
- Validar la seguridad a través de pruebas de conectividad específicas, identificando cuándo el tráfico debe ser permitido y cuándo debe ser bloqueado.

Recomendaciones para futuras implementaciones:

- **Verificación incremental:** Es crucial verificar la conectividad básica (IPs, gateways, rutas) antes de aplicar cualquier ACL compleja para aislar problemas de configuración.
- **Logging en ACLs:** Para entornos reales, usar la opción log en las reglas deny de las ACLs es altamente recomendable para auditar intentos de acceso no autorizados y diagnosticar problemas de seguridad.
- **Seguridad por Capas:** Una DMZ es un componente, pero la seguridad general de la red debe ser una estrategia multicapa que incluya firewalls de aplicaciones, sistemas de detección de intrusiones (IDS/IPS), y políticas de acceso de usuarios.
- **Documentación exhaustiva:** Mantener una documentación detallada de cada regla de ACL y su propósito es vital para la gestión y el mantenimiento a largo plazo de la seguridad de la red.