

Informe de configuración de DMZ con Cisco Packet Tracer

Proyecto: Informe de configuración de DMZ con Cisco Packet Tracer

Fecha: 25-08-2025

Autor: Jean Franco

Índice

- 1. Objetivo del laboratorio**
- 2. Topología implementada**
- 3. Plan de direccionamiento IP**
- 4. Configuración aplicada (resumen)**
- 5. Verificaciones realizadas**
- 6. Conclusiones y recomendaciones**
- 7. Capturas de evidencia**

1. Objetivo del laboratorio

El objetivo principal de este laboratorio era configurar una Zona Desmilitarizada (DMZ) utilizando un router Cisco ISR. Para lograr esto, implementaste y aplicaste los siguientes conceptos:

- Configuración de direccionamiento IP en una topología compleja.
- Implementación de NAT estático para exponer el servidor web de forma segura.
- Aplicación de Listas de Control de Acceso (ACLs) para controlar el flujo de tráfico y asegurar la red.

1. Objetivo del laboratorio

El objetivo principal de este laboratorio fue configurar una Zona Desmilitarizada (DMZ) segura y funcional utilizando un router Cisco ISR. Para lograrlo, se aplicaron tres conceptos clave de redes: la configuración de direccionamiento IP, la implementación de NAT estático para exponer un servicio web, y la creación y aplicación de Listas de Control de Acceso (ACLs) para asegurar la red.

2. Topología implementada

- **Cantidad de redes: 3.**
- **Dispositivos usados:**
 - **Router Central (Router_FW)**
 - **3 switches (uno para cada segmento)**
 - **3 dispositivos finales (PC_Internal, Server-PT Web_DMZ, PC_External)**
- **Breve descripción de la función de cada zona:**
 - **LAN Interna: Representa la red segura de la organización.**
 - **DMZ: Una red intermedia que aloja servicios públicos accesibles desde el exterior.**
 - **Red Externa: Simula el entorno de Internet.**

3. Plan de direccionamiento IP

La siguiente tabla resume el esquema de direccionamiento IP implementado en todos los dispositivos de la topología:

Dispositivo	IP	Mascara	Gateway
PC_Internal	192.168.1.10	255.255.255.0	192.168.1.1
Server-PT Web_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 (resumen)

Los siguientes comandos clave se aplicaron al **Router_FW** para establecer la conectividad y la seguridad:

- **Configuración de Interfaces:** Se asignaron direcciones IP a cada interfaz del router y se activaron con el comando no shutdown.
- **NAT Estático:** Se implementó NAT estático para traducir el tráfico de la red externa a la dirección interna del servidor web.

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

ACLs: Se crearon y aplicaron dos ACLs para controlar el flujo de tráfico:

- La primera ACL (access-list 100) se aplicó a la interfaz externa (GigabitEthernet0/2) en sentido de entrada para permitir únicamente el tráfico web (HTTP) hacia el servidor de la DMZ.

```
access-list 100 permit tcp any host 192.168.3.1 eq www
```

- La segunda ACL (access-list 101) se aplicó a la interfaz de la DMZ (GigabitEthernet0/1) en sentido de entrada para denegar todo el tráfico proveniente de la DMZ hacia la red LAN interna, protegiendo así la red corporativa de posibles compromisos.

```
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
```

5. Verificaciones realizadas

Se realizaron pruebas exhaustivas para confirmar el éxito de la configuración. Los resultados fueron los siguientes:

- El ping desde PC_Internal a su *gateway* (192.168.1.1) fue exitoso.
- El ping desde Server-PT Web_DMZ a su *gateway* (192.168.2.1) fue exitoso.
- El ping desde PC_External a su *gateway* (192.168.3.1) fue exitoso.
- El acceso al servidor web desde PC_External usando su IP pública (192.168.3.1) fue exitoso.
- El acceso al servidor web desde PC_Internal usando su IP interna (192.168.2.10) fue exitoso.
- El ping desde PC_External a la IP pública del servidor falló, lo que confirma que la ACL externa está bloqueando el tráfico ICMP como se esperaba.
- El ping desde el servidor DMZ (Server-PT Web_DMZ) hacia el PC_Internal (192.168.1.10) falló, demostrando que la ACL de seguridad entre la DMZ y la LAN está funcionando correctamente.

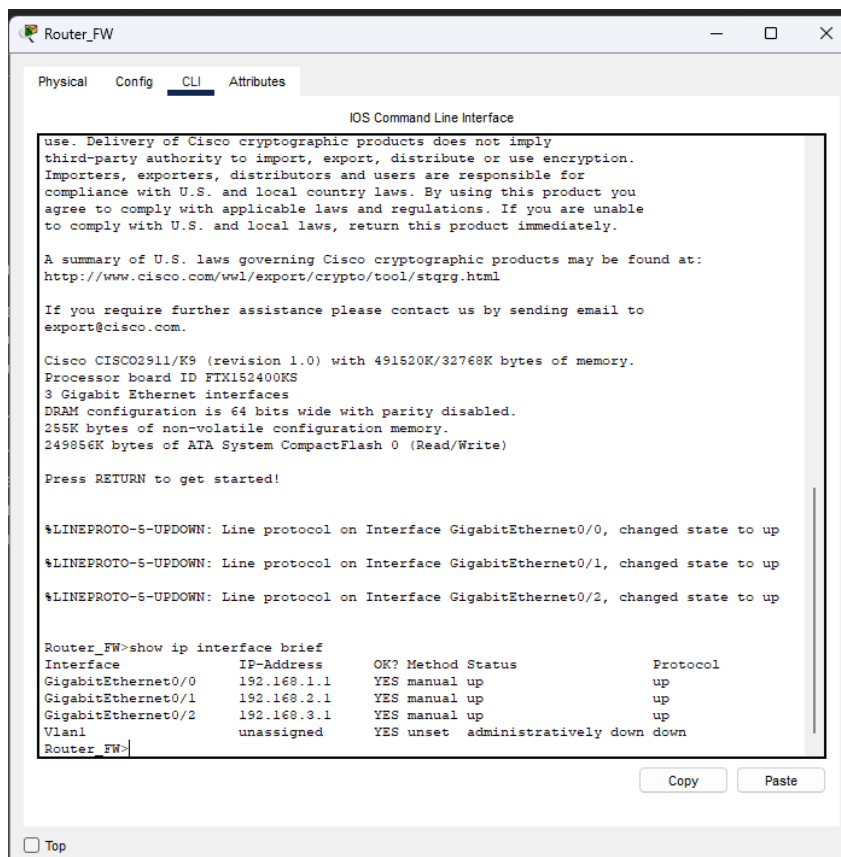
6. Conclusiones y recomendaciones

Este laboratorio demostró la importancia de una planificación de seguridad en redes. Al implementar NAT y ACLs en una DMZ, se logró el objetivo de exponer un servicio público sin comprometer la seguridad de la red interna. Una recomendación clave para futuros proyectos es siempre verificar la conectividad básica de la red antes de implementar reglas de firewall, ya que un error en la configuración IP podría bloquear completamente el acceso y la depuración.

7. Capturas de evidencia

1. Verificación de la configuración de interfaces

Para confirmar que todas las interfaces del Router_FW se configuraron con la dirección IP correcta y que su estado es "UP", se ejecutó el siguiente comando en la CLI del router.



Como se puede ver en la imagen, las interfaces GigabitEthernet0/0, GigabitEthernet0/1 y GigabitEthernet0/2 tienen las direcciones IP asignadas y su estado administrativo y de protocolo es "up", lo que indica que están operativas y listas para enrutar el tráfico.

2. Verificación de la traducción de direcciones (NAT)

Para confirmar que el NAT estático se configuró correctamente, se ejecutó el comando show ip nat translations en la CLI del Router_FW.

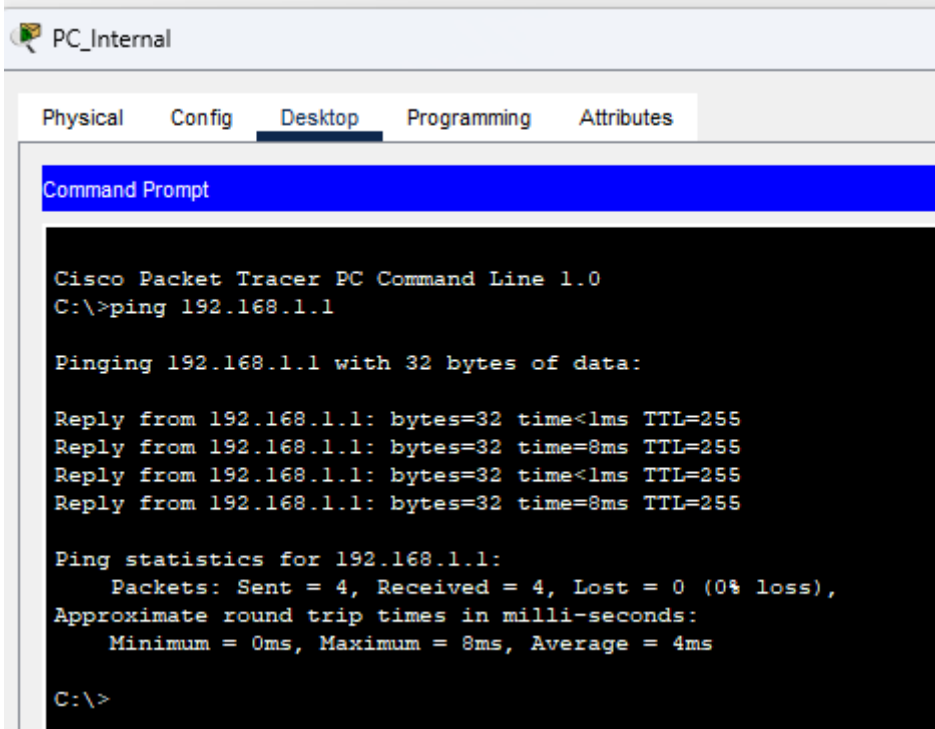
```
Router_FW>show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 192.168.3.1        192.168.2.10     ---               ---
Router_FW>
```

Como se muestra en el resultado, existe un mapeo NAT activo. La dirección IP interna (Inside local) **192.168.2.10** se está traduciendo a la dirección IP pública (Inside global) **192.168.3.1**. Esto demuestra que el tráfico que llega a la interfaz externa (GigabitEthernet0/2) en la dirección **192.168.3.1** será redirigido correctamente al servidor web en la DMZ.

Verificación de Conectividad Básica

1. Ping desde PC_Internal a su Gateway

Se ejecutó un comando ping desde el **Símbolo del sistema** de la PC_Internal para verificar la conectividad con su *gateway* predeterminado (192.168.1.1).



```
PC_Internal
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=8ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=8ms TTL=255

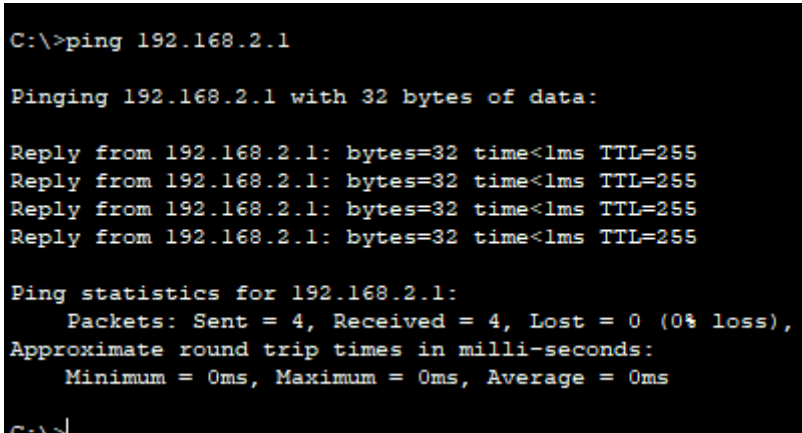
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 4ms

C:\>
```

Como se observa, la prueba fue exitosa, lo que confirma que la PC_Internal tiene conectividad de capa 3 con su Router_FW y que la dirección IP y el *gateway* están configurados correctamente.

2. Ping desde Web_DMZ a su Gateway

Se realizó un ping desde el **Símbolo del sistema** del Server-PT Web_DMZ a su *gateway* (192.168.2.1) para confirmar la conectividad de la red de la DMZ.



```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

La prueba fue exitosa, lo cual verifica que el servidor web puede comunicarse correctamente con el router a través de la DMZ.