Informe de configuración de DMZ con Cisco Packet Tracer

1. Objetivo del laboratorio

El objetivo principal de este laboratorio fue diseñar e implementar una arquitectura de red segura dividida en zonas. Se buscó aislar el Servidor Web en una Zona Desmilitarizada (DMZ) utilizando un Router Cisco, configurando **NAT Estático** para la publicación del servicio y aplicando **Listas de Control de Acceso** para restringir el tráfico no autorizado desde Internet y proteger la red LAN interna de posibles compromisos en la DMZ.

2. Topología implementada

Se implementó una topología en estrella centrada en un router de borde (Router_FW).

- **Cantidad de redes:** 3 subredes distintas (192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24).
- **Dispositivos usados:** 1 Router ISR, 3 Switches 2960, 1 PC, 1 Servidor, 1 Laptop externa.
- **Descripción de zonas:**
    - **LAN (Internal):** Zona de alta confianza donde residen los usuarios internos. Debe estar protegida de accesos externos.
    - **DMZ (Demilitarized Zone):** Zona de confianza media donde reside el servidor web. Es accesible desde Internet pero no tiene acceso a la LAN.
    - **Externa (WAN):** Zona de nula confianza (Internet) desde donde provienen las peticiones de los clientes.

3. Plan de direccionamiento IP

Se configuraron las siguientes direcciones estáticas según los requisitos del laboratorio:

Dispositivo	IP	Máscara	Gateway
PC_Internal	192.168.1.10	255.255.255.0	192.168.1.1
Server_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)

A continuación se detallan los comandos clave ejecutados en el Router_FW:

- **Interfaces y Direccionamiento:**
  Se activaron las interfaces Gi0/0, Gi0/1 y Gi0/2 con sus respectivas IPs y máscaras /24.

- **Configuración de NAT (Network Address Translation):**
  Se definieron las interfaces internas (ip nat inside en Gi0/1) y externas (ip nat outside en Gi0/2). Se aplicó NAT estático para exponer el servidor:

ip nat inside source static 192.168.2.10 192.168.3.1

- **Configuración de ACLs (Firewall):**

1. **Regla Externa:** Permite solo tráfico HTTP (TCP 80) hacia el servidor. Bloquea implícitamente el resto (incluido Ping).

```
ip access-list extended REGLA_INTERNET
 permit tcp any host 192.168.3.1 eq 80
! Aplicada en Gi0/2 (inbound)
```

2. **Regla Interna (BLOQUEO_DMZ_A_LAN):** Impide que la DMZ inicie conexiones hacia la red interna.

```
ip access-list extended BLOQUEO_DMZ_A_LAN
 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
 permit ip any any
! Aplicada en Gi0/1 (inbound)
```

5. Verificaciones realizadas

Se realizaron las siguientes pruebas funcionales para validar la seguridad:

1. **Acceso Web Externo:** Desde PC_External hacia 192.168.3.1.

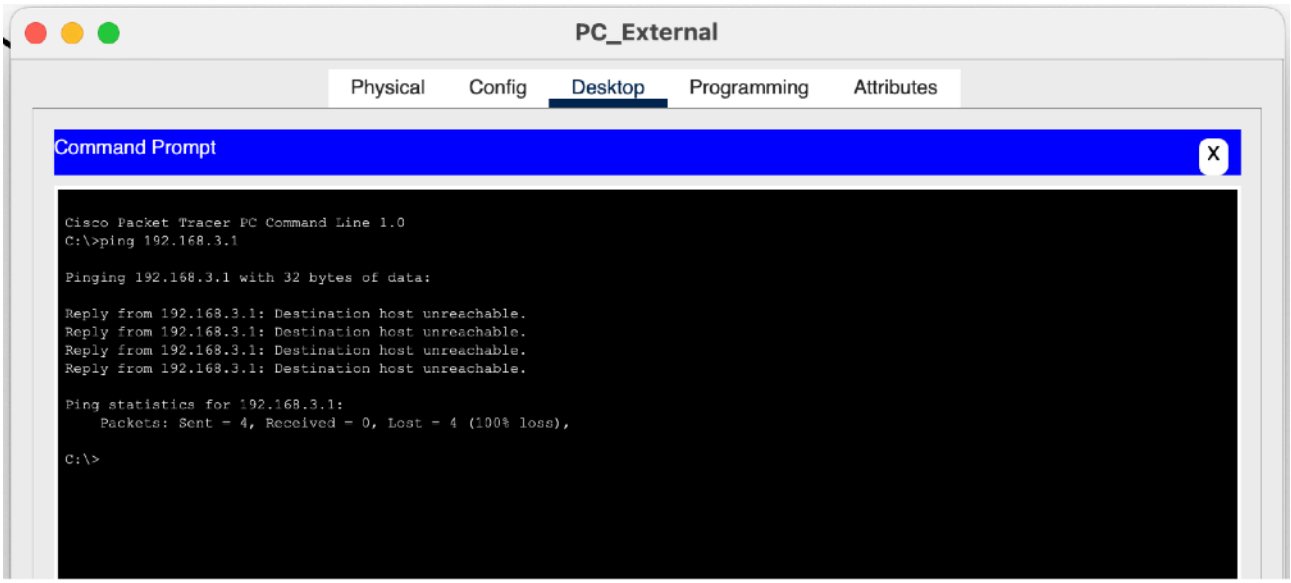
    - Resultado: ✅ (La página web carga correctamente).
2. **Ping Externo:** Desde PC_External hacia 192.168.3.1.
    - Resultado: ✅ (Request timed out)
3. **Aislamiento DMZ:** Ping desde Server_DMZ hacia PC_Internal (192.168.1.10).
    - Resultado: ✅
4. **Acceso Interno:** Navegación desde PC_Internal hacia el servidor.
    - Resultado: ✅ (La página web carga correctamente).

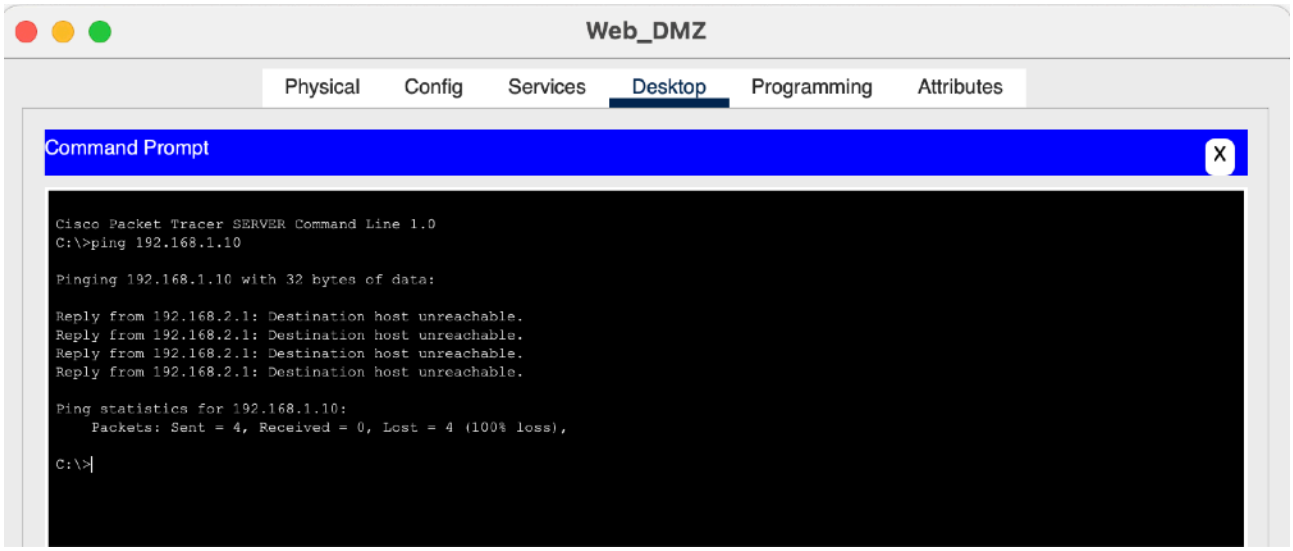
6. Conclusiones y recomendaciones

Conclusiones:

A través de este laboratorio, he aprendido la importancia de segmentar la red. Configurar una DMZ y aplicar reglas. El uso de NAT Estático permitió ocultar la IP real del servidor, exponiendo solo la IP pública del router, y las ACLs funcionaron eficazmente como un firewall de estado, permitiendo solo el servicio necesario (Web) y bloqueando vectores de ataque como el escaneo por Ping .

7. Capturas de evidencia


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:\>


Web_DMZ
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Ping statistics for 192.168.1.10:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>


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.
Quick Links:
WELCOME!!
Copyrights
Image page
Image