Informe de configuración de DMZ con Cisco Packet Tracer

1. Objetivo del laboratorio

El objetivo de este laboratorio fue diseñar e implementar una Zona Desmilitarizada (DMZ) utilizando un router Cisco ISR para exponer un servidor web a Internet de forma segura, aplicando técnicas de segmentación de red, traducción de direcciones (NAT) y listas de control de acceso (ACL).
El objetivo principal fue permitir el acceso controlado al servidor web desde la red externa y la red interna sin comprometer la seguridad de la red LAN.

2. Topología implementada

La topología implementada está compuesta por tres redes independientes:

- **Cantidad de redes:** 3 (LAN, DMZ y Externa)
- **Dispositivos usados:**
- 1 Router Cisco ISR (Router_FW)
- 3 Switches Cisco 2960
- 1 PC interno (PC_Internal)
- 1 Servidor web en DMZ (Server_DMZ)
- 1 PC externo (PC_External)

Descripción de las zonas:

- **LAN:** Red interna donde se encuentra PC_Internal. Esta red está protegida y no debe ser accesible desde la DMZ ni desde Internet.
- **DMZ:** Zona intermedia donde se aloja el servidor web. Está accesible desde Internet pero aislada de la LAN.
- **Red externa:** Simula Internet y contiene el PC_External.

3. Plan de direccionamiento IP

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	—----------
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	—----------

4. Configuración aplicada (resumen)

Se configuraron las interfaces del router para cada red y se habilitó NAT estático para publicar el servidor DMZ hacia la red externa.

NAT

ip nat inside source static 192.168.2.10 192.168.3.1

Las interfaces se marcaron como:

- **ip nat inside** en Gi0/1 (DMZ)
- **ip nat outside** en Gi0/2 (WAN)

ACLs

ACL 101 (tráfico desde Internet):
Permite únicamente tráfico HTTP y HTTPS hacia el servidor publicado.

permit tcp any host 192.168.3.1 eq 80
permit tcp any host 192.168.3.1 eq 443

ACL 100 (tráfico desde la DMZ):
Permite únicamente respuestas hacia LAN y WAN y bloquea accesos directos desde la DMZ hacia la LAN.

permit tcp any 192.168.1.0 0.0.0.255 established
deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
permit ip any any

5. Verificaciones realizadas

Las siguientes pruebas fueron realizadas para validar la configuración:

- **ping desde PC_Internal al router = correcto**
- **Acceso web desde PC_External a http://192.168.3.1 = correcto**
- **Acceso web desde PC_Internal a http://192.168.2.10 = correcto**
- **Ping desde Server_DMZ a PC_Internal = (bloqueado por seguridad)**
- **Validación automática de Packet Tracer (Check Results) = correcto 100%**

6. Conclusiones y recomendaciones

Este laboratorio permitió comprender cómo implementar una arquitectura DMZ segura mediante el uso de **NAT** y **ACLs** en un **router Cisco**.
Se aprendió a segmentar correctamente una red y a controlar el tráfico entre zonas de diferente nivel de seguridad.

Como recomendación, siempre se debe verificar la conectividad básica antes de aplicar ACLs, ya que una regla mal configurada puede bloquear completamente el acceso a la red.

7. Capturas de evidencia

Las siguientes capturas se incluyen en la carpeta **evidencias** del repositorio:

- Topología de Packet Tracer
- Acceso web desde PC_External
- Acceso web desde PC_Internal
- Ping bloqueado desde Server_DMZ hacia la LAN
- Resultado de “Check Results” al 100%