Informe de Laboratorio

Práctica: Implementación de una DMZ Segura y Funcional
Herramienta: Cisco Packet Tracer
Objetivo: Configurar una zona desmilitarizada (DMZ) para alojar un servidor web accesible desde Internet, garantizando seguridad y conectividad controlada mediante NAT y ACLs.

1. Objetivos del laboratorio

- Configurar direccionamiento IP en todos los dispositivos finales y en el router de seguridad (Router_FW).
- Implementar NAT estático para exponer el servidor web DMZ hacia Internet.
- Activar y probar los servicios web en el servidor de la DMZ.
- Aplicar ACLs que controlen acceso seguro: solo HTTP desde Internet, bloquear ICMP, y denegar tráfico DMZ → LAN.
- Verificar conectividad y seguridad mediante pruebas de navegador y ping.

2. Topología de red

Segmento	Dispositivo	Dirección IP / Gateway
LAN Interna (192.168.1.0/24)	PC_Internal	192.168.1.10 / GW: 192.168.1.1
DMZ (192.168.2.0/24)	Server_DMZ	192.168.2.10 / GW: 192.168.2.1
WAN (192.168.3.0/24)	PC_External	192.168.3.10 / GW: 192.168.3.1
Router_FW	Interfaces	G0/0: 192.168.1.1 | G0/1: 192.168.2.1 | G0/2: 192.168.3.1

3. Configuración realizada

a) NAT estático:

```
ip nat inside source static tcp 192.168.2.10 80 192.168.3.1 80
```

b) ACLs aplicadas:

```
access-list 100 permit tcp any host 192.168.3.1 eq 80
access-list 100 deny icmp any host 192.168.3.1
access-list 100 deny ip any any
interface g0/2
ip access-group 100 in
```

```
access-list 110 permit tcp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
established
access-list 110 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 110 permit ip any any
interface g0/1
ip access-group 110 in
```

4. Resultados de verificación

- Desde PC_External (Web Browser) → Página web cargada correctamente.
- Desde PC_External (Ping a 192.168.3.1) → Request Timed Out (ICMP bloqueado).
- Desde PC_Internal (Web Browser a 192.168.2.10) → Página web cargada correctamente.
- Desde Server_DMZ (Ping a PC_Internal) → Request Timed Out (bloqueado por ACL).

5. Conclusión

La DMZ fue implementada de forma segura y funcional. Se permitió acceso HTTP desde Internet al servidor web, se bloqueó ICMP externo, y se restringió el tráfico desde la DMZ hacia la LAN interna. Los objetivos de seguridad y funcionalidad fueron alcanzados.