Cisco Packet Tracer

Informe Técnico de Laboratorio

Configuración de Zona Desmilitarizada (DMZ)

Autor: *Carlos Navarro*

Institución: *4geeks Academy*

Fecha de realización: *22 de agosto de 2025*

Duración del laboratorio: *1 horas y 15 minutos*

Software utilizado: *Cisco Packet Tracer*

Estado del laboratorio: *Completado*

Índice

1. Objetivo del Laboratorio

Implementar una arquitectura de red segmentada con una zona desmilitarizada (DMZ) utilizando un router Cisco ISR. Se aplican técnicas de NAT y ACLs para controlar el tráfico entre la LAN interna, la DMZ y la red externa, simulando un entorno empresarial seguro.

---

2. Topología Implementada

La red está compuesta por tres zonas conectadas a un router central:

- **LAN Interna (Verde):** Recursos internos
- **DMZ (Naranja):** Servidor accesible desde el exterior
- **Red Externa (Amarillo):** Simulación de Internet

---

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 (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

- Configuración IP de PC_Internal
- Configuración IP de Web_DMZ
- Configuración IP de PC_External

---

4. Configuración Aplicada

4.1 Interfaces del Router

```
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside

interface GigabitEthernet0/1
 ip address 192.168.2.1 255.255.255.0
 ip access-group 120 in
 ip nat inside

interface GigabitEthernet0/2
```

```
 ip address 192.168.3.1 255.255.255.0
 ip access-group 110 in
 ip nat outside
```

4.2 NAT Estático

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

4.3 ACLs

```
access-list 110 permit tcp any host 192.168.3.1 eq www
access-list 110 deny ip any any

access-list 120 permit ip host 192.168.2.10 192.168.3.0 0.0.0.255
access-list 120 permit tcp any 192.168.1.0 0.0.0.255 established
access-list 120 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 120 permit ip 192.168.2.0 0.0.0.255 any
```

4.4 Líneas VTY

```
line vty 0 4
 login
```

---

5. Verificaciones Realizadas

5.1 Pruebas de Conectividad

Estado	Condición	Puntos	Origen	Destino	Tipo
Correcto	Exitosa	1	PC_Internal	192.168.1.1	ICMP
Correcto	Exitosa	1	Web_DMZ	192.168.1.1	ICMP
Correcto	Exitosa	1	PC_External	192.168.1.1	TCP
Correcto	Exitosa	1	PC_Internal	192.168.2.10	TCP
Correcto	Fallida	2	Web_DMZ	192.168.1.10	ICMP
Correcto	Fallida	3	PC_External	192.168.3.1	ICMP

- Resultados de pruebas de conectividad

- Pings y traceroutes desde CMD confirmando conectividad y bloqueos
- Mensaje de finalización del laboratorio
- Puntuación final: 9/9 puntos

---

6. Análisis de Resultados

- Todas las rutas autorizadas funcionan correctamente
- Las ACLs bloquean tráfico no deseado
- NAT estático permite acceso controlado al servidor web
- La segmentación de red está correctamente implementada

---

7. Configuración de Seguridad

- **Internet → DMZ:** Solo tráfico HTTP permitido
- **LAN → DMZ:** Acceso completo
- **DMZ → LAN:** Bloqueado
- **DMZ → Internet:** Permitido

---

8. Conclusiones y Recomendaciones

Logros

- Segmentación efectiva
- Control de acceso exitoso
- NAT funcional
- Conectividad validada

Recomendaciones

- Implementar HTTPS
- Configurar VLANs
- Añadir redundancia
- Activar IDS/IPS

- Realizar respaldos y auditorías periódicas

---

9. Anexos

Evidencias Integradas

1. Topología de red segmentada
2. Configuración IP de todos los dispositivos
3. CLI del Router_FW (`show running-config`)
4. Interfaces del Router_FW
5. Configuración NAT y ACLs
6. Traducciones NAT activas
7. Resultados de conectividad
8. Puntuación final del laboratorio
9. Mensaje de finalización de actividad
10. Pruebas de conectividad desde CMD (ping, tracert, fallos y éxitos)

Comandos utilizados

- `show running-config`
- `show ip nat translations`
- `show access-lists`
- `ping`
- `traceroute`
