

Explicación de la Topología Actual y Recomendada

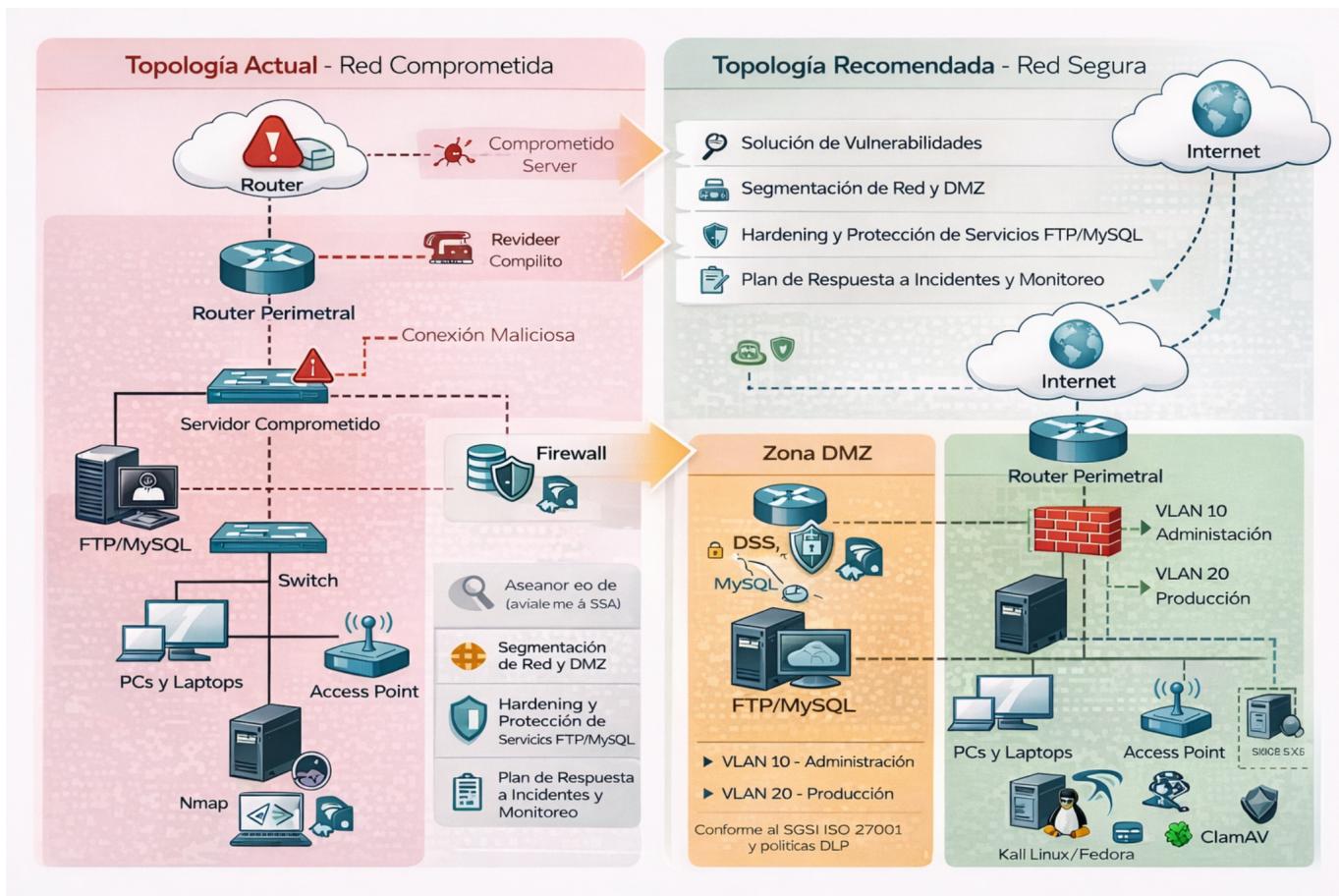
1. Topología Actual - Red Comprometida

En la red comprometida, el servidor crítico está expuesto a vulnerabilidades debido a una mala configuración de servicios como FTP y MySQL.

Los siguientes puntos destacan los riesgos actuales:

- **Conexión maliciosa**: El router está comprometido debido a accesos no autorizados desde el exterior.
- **Servidor comprometido**: El servidor crítico ha sido hackeado y está comprometido.
- **Falta de seguridad**: No hay segmentación adecuada de la red, lo que permite que los ataques se propaguen fácilmente.

El firewall está presente, pero no está configurado adecuadamente para proteger los servicios expuestos.



2. Topología Recomendada - Red Segura

La red segura incluye una serie de cambios críticos para mejorar la protección y resiliencia frente a ataques. Los cambios incluyen:

- **Segmentación de la red y DMZ**: Se crea una zona DMZ que aísla los servicios críticos de la red interna.
- **Hardening de servicios**: Los servicios FTP y MySQL son reforzados para evitar accesos no autorizados, implementando cifrado y autenticación más estricta.
- **Firewall actualizado**: Se configura un firewall más robusto para filtrar el tráfico malicioso y proteger los servicios.
- **VLANs**: Se crean VLANs para separar el tráfico de administración (VLAN 10) y producción (VLAN 20), lo que mejora el control sobre la red.
- **Monitoreo y respuesta a incidentes**: Se implementan herramientas como Kali Linux, Nmap y

ClamAV para escanear vulnerabilidades y proteger la red de futuros ataques.

Esta topología es mucho más segura y asegura la protección de los servicios y datos críticos de la red.