Proyecto Final de Ciberseguridad

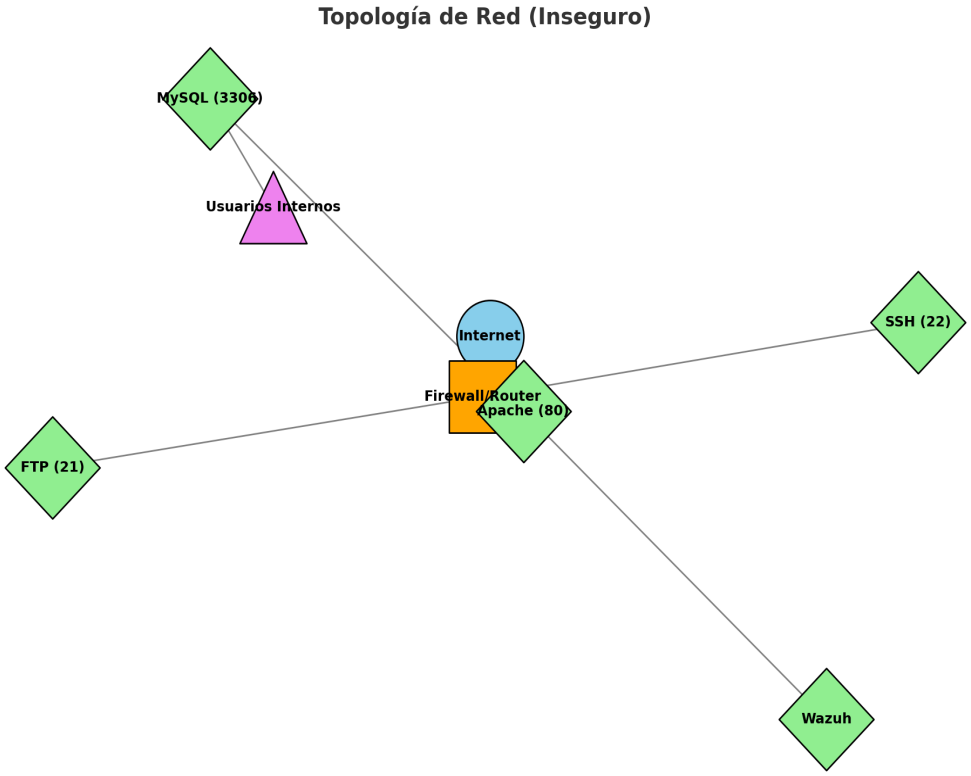
Diagramas de Red Cisco (Escenario inseguro y seguro)

Autor: Carlos Navarro
4Geeks Academy - 2025

Índice

1. Escenario Inseguro (Antes)

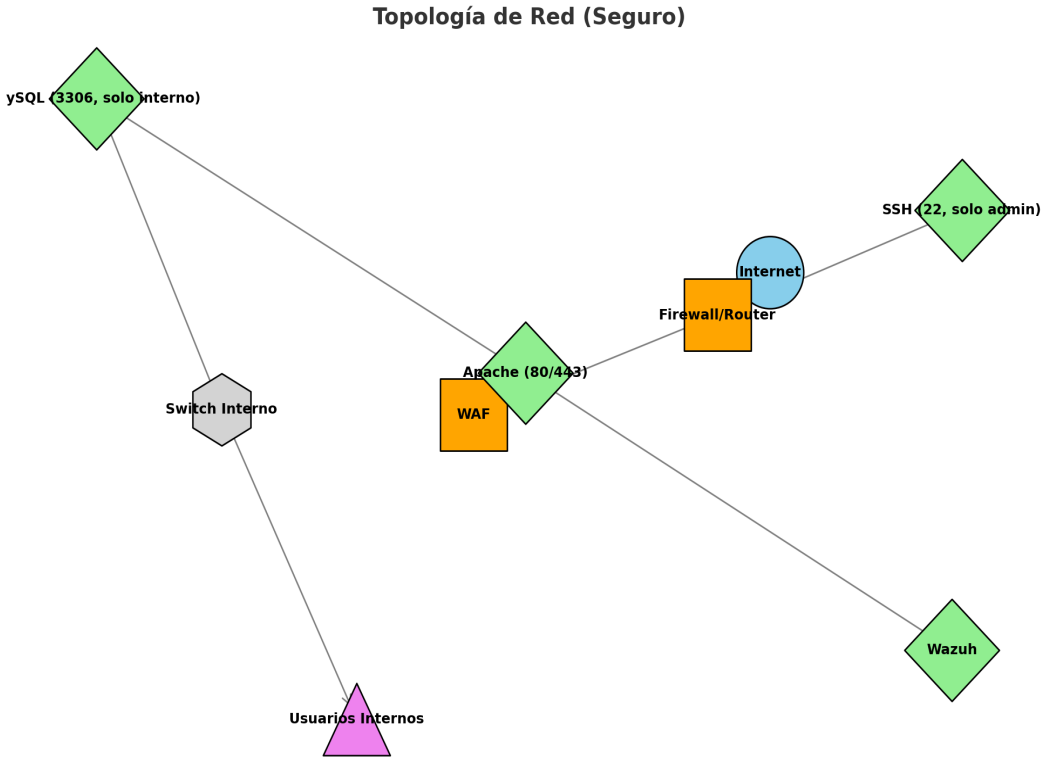
Topología actual con servicios expuestos (FTP, SSH, Apache, MySQL, Wazuh).



Comandos de verificación:
- nmap -sV -p 21,22,80,3306
- ss -tuln | grep LISTEN
- systemctl status vsftpd
- cat /etc/passwd | grep hacker

2. Escenario Seguro (Después)

Topología mejorada con WAF, segmentación interna, SSH restringido y FTP eliminado.



Comandos de hardening:
- ufw deny 21/tcp
- nano /etc/ssh/sshd_config → PermitRootLogin no
- systemctl restart sshd
- iptables -A INPUT -p tcp --dport 3306 -s 10.10.30.0/24 -j ACCEPT
- iptables -A INPUT -p tcp --dport 3306 -j DROP

3. Comparativa y Conclusión

Aspecto	Escenario Inseguro	Escenario Seguro
FTP	Abierto (21)	Eliminado
SSH	Acceso desde Internet	Restringido solo admin
Apache	HTTP expuesto	HTTP/HTTPS con WAF
MySQL	Acceso amplio	Solo red interna
Firewall	Básico	Restrictivo con reglas específicas

La nueva arquitectura reduce la superficie de ataque, eliminando FTP, segmentando la red interna, limitando SSH y colocando un WAF frente a Apache.