Universidad

Mariano Gálvez

Conoceréis la verdad y la verdad os hará libres

Red de laboratorio que proporcione resolución DNS interna mediante BIND9

ing

Fase Final

Guatemala 8 de noviembre del 2025

Alumno:

Melany Romero Samayoa 7690-22-48

Resumen

El presente proyecto tiene como finalidad diseñar, implementar y documentar una red de laboratorio funcional que integre tres servicios principales: resolución DNS interna mediante BIND9, servidores web con sitios institucional y privado, y acceso remoto seguro a través de una VPN basada en WireGuard o OpenVPN.

Esta infraestructura busca simular el entorno de una red empresarial, donde se manejan dominios internos, segmentación de servicios y acceso remoto seguro.

El proyecto demostrará la integración de servicios de red, control de acceso, seguridad básica y pruebas de disponibilidad, garantizando que los recursos internos solo sean accesibles mediante la VPN configurada.

Objetivos

Objetivo general

Implementar una red de laboratorio con servicios DNS, web y VPN integrados, garantizando la resolución interna de nombres, acceso seguro y controlado a los recursos.

Objetivos específicos

1. **Configurar un servidor DNS autoritativo** utilizando **BIND9**, estableciendo zonas **forward** (directa) y **reverse** (inversa) para el dominio interno lab.local.
2. **Desplegar un servidor web** (Nginx o Apache) con al menos **dos virtual hosts**:
   - ♥ Un sitio **institucional público**, accesible dentro de la red principal.
   - ♥ Un sitio **interno privado**, accesible únicamente mediante la VPN.
3. **Implementar una VPN** basada en **WireGuard o OpenVPN** para permitir **acceso remoto seguro** al entorno y garantizar la **resolución DNS interna** a través del servidor BIND9.
4. **Configurar reglas básicas de firewall** utilizando iptables, nftables o ufw, con el objetivo de proteger la red y limitar el acceso a los servicios según políticas de seguridad definidas.
5. **Realizar pruebas funcionales y de rendimiento** para comprobar la disponibilidad de los servicios, la correcta resolución de nombres y la estabilidad de la VPN.
6. **Documentar todo el proceso técnico**, incluyendo instalación, configuración, topología, pruebas y resultados.

Alcance del proyecto

El proyecto se desarrolla en un entorno **virtualizado o físico**, compuesto por **tres máquinas** interconectadas que representan los componentes principales de la red:

Rol	Función	Dirección IP	Servicios principales
Controlador / Servidor DNS + VPN	Servidor principal que aloja el servicio de nombres (BIND9) y la VPN (WireGuard / OpenVPN)	192.168.10.10	DNS, VPN, firewall
Servidor Web	Aloja los sitios institucional (público) e interno (privado)	192.168.10.20	Nginx o Apache (2 Virtual Hosts)
Equipo Cliente	Simula un usuario remoto que accede vía VPN y realiza pruebas de acceso a servicios internos	10.10.10.x (subred VPN)	Cliente WireGuard / OpenVPN

Marco teórico

BIND9 y resolución DNS

BIND9 (Berkeley Internet Name Domain) es el servidor DNS más utilizado en entornos Linux. Permite gestionar dominios y subdominios mediante archivos de zonas **forward** (resolución directa de nombre a IP) y reverse (resolución inversa de IP a nombre).

En un laboratorio, BIND9 se configura como servidor autoritativo interno, de modo que los equipos conectados —incluyendo los que ingresan por VPN— puedan resolver dominios como web.lab.local o vpn.lab.local.

Servidor web (Nginx o Apache)

Los servidores web permiten alojar páginas o aplicaciones accesibles por HTTP/HTTPS.

Con los **Virtual Hosts**, un solo servidor físico puede alojar múltiples sitios con diferentes nombres de dominio. En este proyecto se utilizarán dos:

- Un sitio institucional público (por ejemplo institucional.lab.local)
- Un sitio interno privado (intranet.lab.local), accesible solo por VPN.

VPN (WireGuard / OpenVPN)

Una VPN crea un **túnel cifrado** entre un cliente y un servidor, permitiendo acceder a recursos internos como si el usuario estuviera físicamente en la red local.

WireGuard destaca por su **simplicidad y rendimiento**, mientras que OpenVPN es ampliamente utilizado por su compatibilidad multiplataforma.

Seguridad y firewall

El firewall controla el tráfico de entrada y salida mediante políticas específicas.

En este proyecto, se deben permitir solo los siguientes puertos:

- **53** (DNS interno)
- **80 / 443** (HTTP/HTTPS)

- **51820 / 1194** (VPN)
- Bloquear cualquier otro tráfico no necesario.

  Además, la autenticación VPN y el cifrado TLS/SSL garantizan la confidencialidad y autenticidad de las conexiones.

Conclusiones

- Se logra integrar múltiples servicios de red (DNS, Web, VPN) en un entorno de laboratorio controlado.
- Se demuestra la importancia del DNS interno en la resolución de servicios privados.
- La VPN garantiza un acceso remoto seguro y segmentado a los recursos de la red.
- La aplicación de políticas de firewall mejora la seguridad y control del tráfico interno.
- El laboratorio puede servir como base para implementaciones reales en entornos empresariales.

Bienvenido al Sitio Institucional de Lab.Local

Esta es la zona pública.