# 🌐 *Laboratorio de Red Profesional – VPN + IDS/IPS*

*📖 Documentación en Español*

---

## 📖 Descripción del Proyecto

Soy **ivansalpe** y he diseñado este laboratorio de red con el objetivo de demostrar mis habilidades en **seguridad informática, redes y virtualización**.

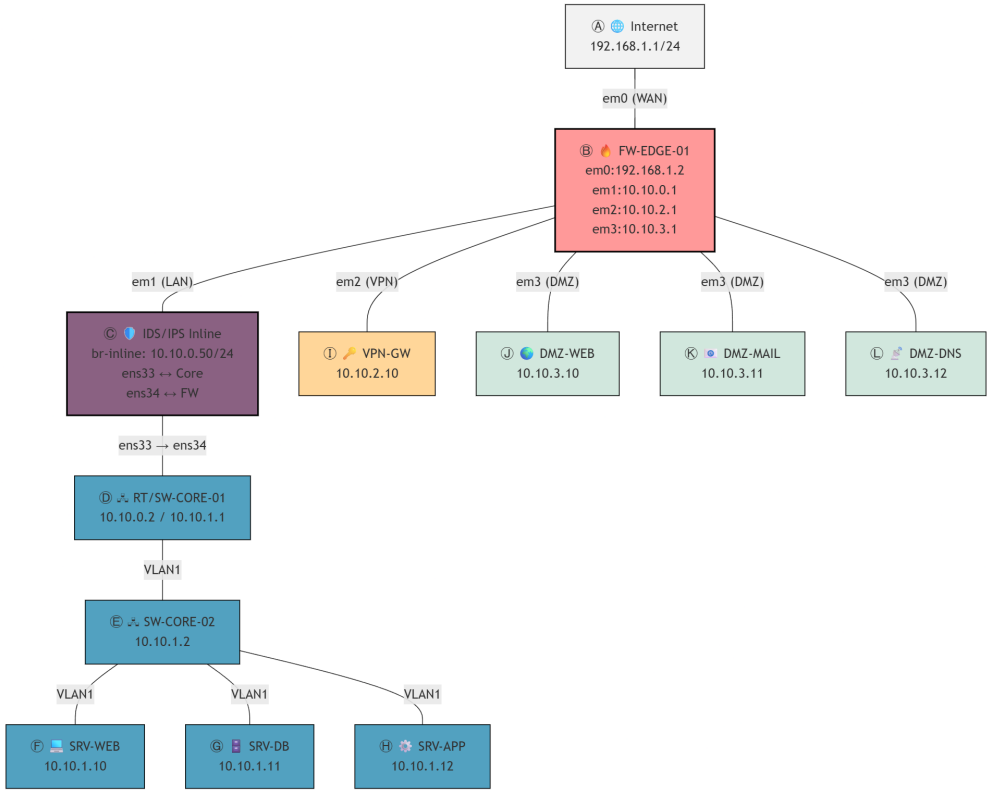
La topología implementada incluye:

- 🔥 Un firewall de perímetro (FW-EDGE-01) con OPNsense.
- 🛡️ Un IDS/IPS inline (Suricata) dedicado, que inspecciona y bloquea tráfico en tiempo real.
- 🖧 Un núcleo de red con routers/switches virtualizados para segmentar VLANs.
- 🌍 Una DMZ para servicios públicos expuestos.
- 🔑 Una VPN (IPsec/IKEv2) para acceso remoto seguro.

Este proyecto busca simular un **entorno empresarial real**, combinando seguridad perimetral, segmentación y monitorización avanzada de amenazas.

---

## 📊 Topología de Red




## 🛠️ Componentes del Laboratorio

| Componente | Función / Rol |
|---|---|
| FW-EDGE-01 (OPNsense) | Firewall perimetral, NAT, control de tráfico, terminación de VPN IKEv2/IPsec |

| Componente | Función / Rol |
|---|---|
| IDS/IPS Inline (Suricata) | Inspección profunda de paquetes, reglas ET Open, bloqueo de amenazas |
| RT/SW-CORE-01 | Routing interno, manejo de VLANs entre LAN, DMZ y VPN |
| SW-CORE-02 | Switch de distribución en VLAN1 |
| Servidores LAN | WEB, DB, APP → servicios internos críticos |
| Servidores DMZ | WEB, MAIL, DNS → servicios expuestos y monitorizados |
| VPN-GW / Clientes VPN | Acceso remoto seguro, NAT opcional para Internet |

---

## 🎯 Objetivos del Proyecto

Simular un entorno empresarial real con seguridad perimetral y segmentación de red.

Demostrar habilidades en:

- 🔐 VPNs seguras (IKEv2/IPsec)
- 🛡️ Detección y respuesta ante amenazas (Suricata)
- 🖧 Diseño y operación de VLANs
- 📝 Documentar el laboratorio de forma clara y profesional para portafolios

---

## 🛠️ Modos de Operación

- **FW-EDGE-01** → Segmentación de red, NAT, VPN IKEv2, reglas de firewall
- **IDS/IPS Inline** → Análisis y bloqueo de tráfico LAN/DMZ/VPN, reglas ET Open
- **Core / Switches** → VLANs separadas (LAN, VPN, DMZ) y enrutamiento interno
- **Servidores LAN y DMZ** → Servicios internos y públicos, protegidos por FW e inspeccionados por IDS/IPS
- **VPN-GW / Clientes VPN** → Conexión remota segura, NAT opcional para Internet

---

## 📝 Manual Paso a Paso

### 1️⃣ FW-EDGE-01 (OPNsense)

- **Recursos:** 2 vCPU, 2GB RAM, 20GB disco, 4 NICs
- **IPs:** em0:192.168.1.2, em1:10.10.0.1, em2:10.10.2.1, em3:10.10.3.1
- **Configuración:** VPN IKEv2/IPsec, reglas de firewall, NAT, logs
- **Pruebas:** Ping LAN/DMZ/VPN, clientes remotos

### 2️⃣ IDS/IPS Inline (Suricata)

- **Recursos:** 2 vCPU, 2GB RAM, 20GB disco, 2 NICs
- **IPs:** eth0:10.10.0.50, eth1:10.10.0.51
- **Configuración:** Suricata inline, reglas ET Open, logging
- **Pruebas:** Ping FW ↔ Core, tráfico HTTP/DB/APP

### 3 Core Router/Switch

- **Recursos:** VyOS o Linux Router
- **IPs:** eth0:10.10.0.2, eth1:10.10.1.1
- **Configuración:** VLANs, rutas estáticas
- **Pruebas:** Ping entre servidores, FW e IDS/IPS

### 4 Servidores LAN y DMZ

- **LAN:** SRV-WEB 10.10.1.10, SRV-DB 10.10.1.11, SRV-APP 10.10.1.12
- **DMZ:** DMZ-WEB 10.10.3.10, DMZ-MAIL 10.10.3.11, DMZ-DNS 10.10.3.12
- **Servicios:** Apache, MySQL, PHP, Postfix, Bind9
- **Pruebas:** Conectividad LAN/DMZ, acceso desde FW

### 5 VPN-GW / Clientes VPN

- **IP:** 10.10.2.10 — Gateway: 10.10.2.1
- **Cliente:** StrongSwan, certificados X.509
- **Pruebas:** Ping LAN/DMZ, acceso Internet vía NAT, tráfico inspeccionado

---

## 📓 Notas Finales

- IDS/IPS inline entre **FW y Core** → inspección total de tráfico
- VLANs separadas: LAN (10.10.1.0/24), DMZ (10.10.3.0/24), VPN (10.10.2.0/24)
- FW gestiona VPN y NAT si es necesario
- Logs activos de Suricata y FW para auditoría
- Topología realista, ideal para **portafolio profesional**

---