PROYECTO INTERMODULAR ASIX

Ciberbambi

Infraestructura de red con pfSense, VLAN única y servicios LAN/DMZ integrados

Imatge que conté captura de pantalla, text, muntanya, neu

Pot ser que el contingut generat per IA no sigui correcte.

Configurado por Adam Valien y documentado por Sergi Couto.

Miembros:

Adam Valien, Adam Ahmadi y Sergi Couto.

Contenido

[1. Introducción 3](#_Toc212477165)

[2. pfSense: interfaces, reglas y NAT 4](#_Toc212477166)

[2.1 Tarjetas de red 4](#_Toc212477167)

[2.2 Reglas de firewall 5](#_Toc212477168)

[2.3 NAT híbrido (Hybrid Outbound) 6](#_Toc212477169)

[3. DHCP y DHCP Relay 7](#_Toc212477170)

[4. Servidor DNS (BIND) 10](#_Toc212477171)

[5. SSH (administración segura) 12](#_Toc212477172)

[6. Servidor Apache + MySQL (WordPress) 13](#_Toc212477173)

[7. Servidor Samba y FTP 16](#_Toc212477174)

[8. VPN (OpenVPN con certificados CiberBambi) 19](#_Toc212477175)

[8.1 Creación de certificados 19](#_Toc212477176)

[8.2 Configuración del servidor VPN 19](#_Toc212477177)

[8.3 Exportación e instalación del cliente 19](#_Toc212477178)

[8.4 Pruebas 19](#_Toc212477179)

[9. Pruebas funcionales 20](#_Toc212477180)

[10. Conclusión 21](#_Toc212477181)

# Introducción

El proyecto **CIBERBAMBI** se ha desarrollado con el objetivo de crear una infraestructura de red **segura, modular y funcional**, basada en **pfSense** como cortafuegos y router principal.  
La red se estructura en una **VLAN única** que interconecta todos los servidores, garantizando visibilidad total entre ellos sin comprometer la seguridad ni la segmentación lógica.

El entorno cuenta con:

* **pfSense** como núcleo de control de tráfico.
* **Servidor principal (192.168.33.2)** con **DNS, DHCP, Samba y FTP**.
* **Servidor DMZ (192.168.50.2)** con **Apache, MySQL y WordPress**.
* **Clientes LAN** y **VPN** que acceden a los servicios internos y externos mediante reglas NAT.

Este diseño permite **centralizar la gestión**, **asegurar la comunicación interna**, y **mantener salida controlada a Internet**.

# pfSense: interfaces, reglas y NAT

## Tarjetas de red

pfSense dispone de tres interfaces configuradas:

* **WAN:** conexión externa, obtiene IP automáticamente del router o proveedor (DHCP).
* **LAN:** red interna (192.168.33.1/24), donde reside el servidor de dominio.
* **OPT1 (DMZ):** red de servicios (192.168.50.1/24), donde está el servidor web.

Esta estructura separa el tráfico interno del externo, asegurando control total de flujo y visibilidad entre redes LAN ↔ DMZ.

Imatge que conté text, captura de pantalla, Font

Pot ser que el contingut generat per IA no sigui correcte.

## Reglas de firewall

Desde un cliente LAN se accede a pfSense para comprobar que todas las **reglas permiten el tráfico completo interno**.  
El objetivo es tener comunicación total dentro de la red y permitir acceso a Internet, **pero sin abrir puertos hacia el exterior**.

* **WAN:** permite tráfico saliente hacia Internet y hacia LAN/OPT1.
* **LAN:** permite comunicación completa interna y salida a Internet.
* **OPT1 (DMZ):** también con tráfico total hacia LAN y salida al exterior.

Este planteamiento permite trabajar y probar servicios internos sin riesgos de exposición.

Imatge que conté text, captura de pantalla, programari, Pàgina web

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, programari, Pàgina web, Lloc web

Pot ser que el contingut generat per IA no sigui correcte.

## NAT híbrido (Hybrid Outbound)

Se configura NAT en modo **Hybrid Outbound**, lo que permite que las redes internas (LAN y DMZ) salgan a Internet bajo la IP pública de pfSense.  
Esto mantiene las direcciones privadas ocultas y permite la navegación y resolución externa.

Imatge que conté text, captura de pantalla, programari, Pàgina web

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, programari, Icona d'ordinador

Pot ser que el contingut generat per IA no sigui correcte.

# DHCP y DHCP Relay

pfSense no asigna direcciones IP directamente. En su lugar, se configura **DHCP Relay** para redirigir las solicitudes al servidor principal (192.168.33.2), que tiene activo el servicio DHCP.

* El servidor DHCP gestiona **dos subredes**:
  + LAN (192.168.33.0/24)
  + DMZ (192.168.50.0/24)
* Cada servidor tiene **IP fija reservada por MAC**, asegurando estabilidad.
* El resto de máquinas reciben IP dinámica dentro del rango configurado.
* El **gateway** es pfSense y el **DNS** apunta al propio servidor interno.

Imatge que conté text, captura de pantalla, pantalla, programari

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, Font, disseny

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, Font

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, Font

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, pantalla, programari

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, programari, Software de multimèdia

Pot ser que el contingut generat per IA no sigui correcte.

# Servidor DNS (BIND)

El DNS interno está alojado en el servidor principal (192.168.33.2) con **BIND9**.  
pfSense **no actúa como DNS**; este servicio se centraliza para mantener un punto de administración.

Configuración clave:

* **allow-query**: permite consultas solo desde LAN, DMZ y localhost.
* **forwarders**: 8.8.8.8 y 1.1.1.1 (Google) para resolución externa.
* **listen-on any**: acepta peticiones desde cualquier interfaz interna.

La **zona directa** (db.ciberbambi.local) asocia nombres con IPs internas.  
Las **zonas inversas** (33.168.192.in-addr.arpa y 50.168.192.in-addr.arpa) permiten resolver IP → nombre, garantizando visibilidad total entre LAN y DMZ.

Imatge que conté text, programari, Pàgina web, Icona d'ordinador

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, programari, Software de multimèdia

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, electrònica, captura de pantalla, programari

Pot ser que el contingut generat per IA no sigui correcte.



# SSH (administración segura)

Toda la administración de servidores y clientes se realiza mediante **SSH**, evitando RDP y garantizando seguridad mediante autenticación cifrada.  
SSH está habilitado en **todas las máquinas** (pfSense, servidores LAN y DMZ), permitiendo una administración unificada desde cualquier cliente de la red.

Imatge que conté text, captura de pantalla, pantalla, programari

Pot ser que el contingut generat per IA no sigui correcte.

# Servidor Apache + MySQL (WordPress)

En la DMZ (192.168.50.2) se ha desplegado un servidor con **Apache y MySQL** sobre el mismo host.  
Este servidor aloja **WordPress**, que sirve como demostración funcional de los servicios web del entorno.

* **PostgreSQL** fue descartado por incompatibilidad con WordPress.
* El sitio es accesible desde LAN y DMZ, por IP y por DNS (wordpress.ciberbambi.local).
* WordPress utiliza MySQL local, comunicando directamente por socket interno.
* Se ha creado un usuario de prueba para validación del entorno.

Imatge que conté text, captura de pantalla, programari, Software de multimèdia

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, electrònica, captura de pantalla, pantalla

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, programari, Icona d'ordinador

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, Font, disseny

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, Font, disseny

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, programari, Icona d'ordinador

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, programari, Icona d'ordinador

Pot ser que el contingut generat per IA no sigui correcte.

# Servidor Samba y FTP

El servidor LAN (192.168.33.2) ofrece servicios de **almacenamiento compartido y transferencia de archivos** mediante **Samba y FTP**.

**Samba:**

* Autenticación por usuario (sin acceso anónimo).
* Repositorio de archivos compartidos entre clientes Linux.
* No se utiliza RDP, las conexiones son vía SSH y Samba.

**FTP:**

* Configurado con **vsftpd**, escuchando localmente.
* Temporalmente habilitado el acceso **anonymous** para entorno de pruebas.
* Permite transferir, editar y mover ficheros desde cliente y servidor.

Imatge que conté text, captura de pantalla, Font

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, pantalla, programari

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, Font

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, pantalla, Font

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, captura de pantalla, Font

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté electrònica, text, captura de pantalla, ordinador

Pot ser que el contingut generat per IA no sigui correcte.

Imatge que conté text, electrònica, captura de pantalla, programari

Pot ser que el contingut generat per IA no sigui correcte.

# VPN (OpenVPN con certificados CiberBambi)

Se ha configurado una **VPN** en pfSense para permitir la conexión remota segura al entorno interno.  
El proceso se realiza íntegramente desde pfSense con certificados creados y firmados localmente.

## 8.1 Creación de certificados

* Crear **CA (Autoridad de Certificación)** llamada **“CiberBambi”**.
* Crear **certificado de servidor** firmado por la CA.

## 8.2 Configuración del servidor VPN

* Configurar el **servidor OpenVPN** usando el certificado de servidor.
* Permitir que la VPN acceda a **Internet** y **redes internas** (reglas en interfaz OpenVPN permiten todo).
* Habilitar **DHCP Relay o bridge** para que los clientes reciban IP del servidor DHCP interno.

## 8.3 Exportación e instalación del cliente

* Descargar el **perfil de conexión (.ovpn)** desde pfSense.
* En el **cliente Linux**, importar el archivo en NetworkManager o ejecutar openvpn --config.
* El cliente recibe una **IP por DHCP** y puede navegar por Internet.

## 8.4 Pruebas

* Verificar IP asignada (ip addr).
* Probar conexión por nombre (nslookup ciberbambi.local).
* Acceso a WordPress y Samba a través de la VPN.

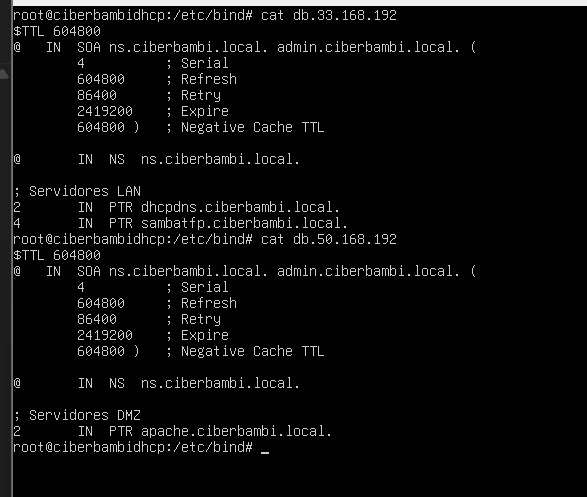
# Pruebas funcionales

Ping a Internet (8.8.8.8) desde LAN, DMZ y VPN.

Ping por nombre (nslookup) entre servidores LAN y DMZ.

Acceso a WordPress por DNS interno desde cualquier cliente.

Comprobación de tráfico NAT: salida a Internet bajo IP pública.



# Conclusión

La red **CiberBambi** queda estructurada de manera **clara, segura y eficiente**, con pfSense como núcleo de control.  
La VLAN única permite que **todos los servidores se vean entre sí**, mientras pfSense **controla el tráfico** y **limita accesos externos**.  
El **DNS y DHCP** centralizados simplifican la administración, el **WordPress** demuestra la conectividad LAN↔DMZ, y los servicios **Samba, FTP y SSH** cubren gestión y colaboración.  
La **VPN CiberBambi**, con certificados internos y entrega DHCP, ofrece acceso remoto seguro y funcional.

El entorno está listo para producción y futuras expansiones, cumpliendo el objetivo de “**Seguridad y Redes Avanzadas**”.