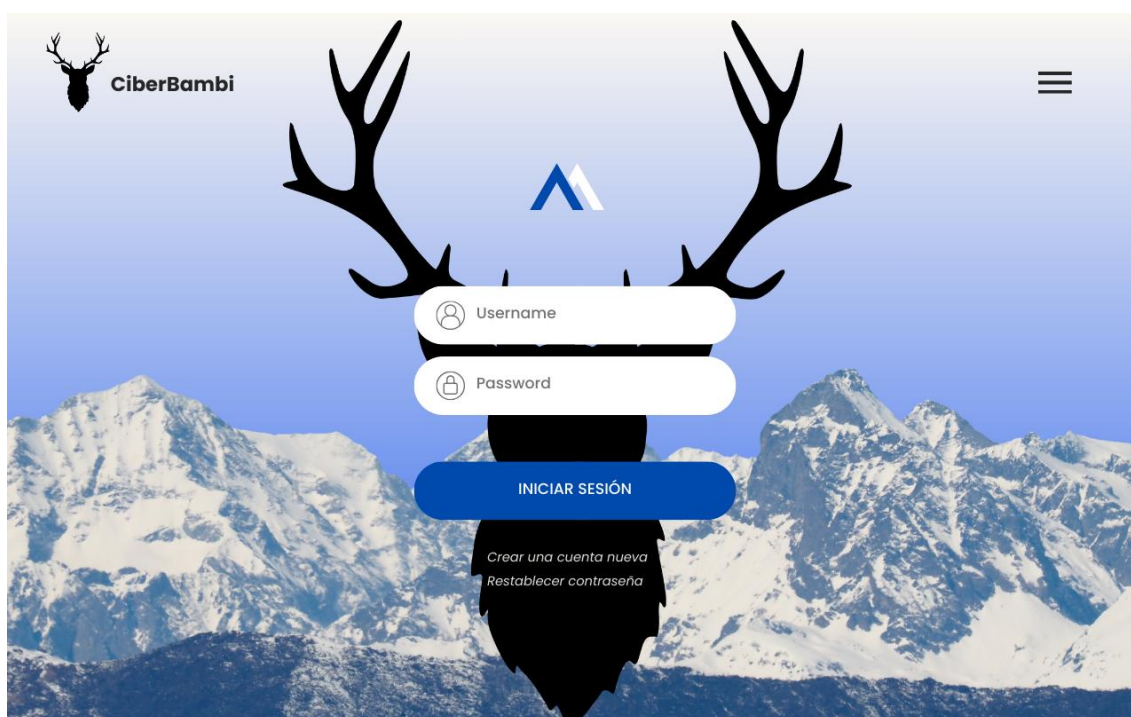


# PROYECTO INTERMODULAR ASIX

## Ciberbambi

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



Configurado por Adam Valien y documentado por Sergi Couto.

Miembros:

Adam Valien, Adam Ahmadi y Sergi Couto.

## Contenido

1.	Introducción .....	3
2.	pfSense: interfaces, reglas y NAT .....	4
2.1	Tarjetas de red .....	4
2.2	Reglas de firewall .....	5
2.3	NAT híbrido (Hybrid Outbound) .....	6
3.	Servidor DNS (BIND).....	7
4.	DHCP y DHCP Relay.....	10
5.	SSH (administración segura).....	12
6.	Servidor Apache + MySQL (WordPress) .....	13
7.	Servidor Samba y FTP .....	16
8.	VPN (OpenVPN con certificados CiberBambi) .....	19
8.1	Creación de certificados .....	19
8.2	Configuración del servidor VPN .....	19
8.3	Exportación e instalación del cliente .....	19
8.4	Pruebas.....	19
9.	Pruebas funcionales .....	20
10.	Conclusión .....	21

## 1. 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**.

## 2. pfSense: interfaces, reglas y NAT

### 2.1 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.

```
Starting CRON... done.
pfSense 2.8.1-RELEASE amd64 20250909-1629
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

KVM Guest - Netgate Device ID: 60a5b194a23dacbb4796

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

WAN (wan)   -> em0 -> v4/DHCP4: 10.0.2.15/24
LAN (lan)   -> em1 -> v4: 192.168.33.1/24
OPT1 (opt1) -> em2 -> v4: 192.168.50.1/24

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address      11) Restart GUI
3) Reset admin account and password 12) PHP shell + pfSense tools
4) Reset to factory defaults        13) Update from console
5) Reboot system                    14) Enable Secure Shell (sshd)
6) Halt system                      15) Restore recent configuration
7) Ping host                        16) Restart PHP-FPM
8) Shell

Enter an option: █
```

## 2.2 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.

The image displays two screenshots of the pfSense web interface, specifically the Firewall Rules configuration page for the LAN and OPT1 interfaces.

**Top Screenshot: Firewall Rules for LAN**

The browser address bar shows `http://192.168.33.1/firewall_rules.php?fif=lan`. The interface shows the "Firewall / Rules / LAN" path. The "Rules (Drag to Change Order)" table lists two rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 5/60 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	[Settings]
✓ 0/0 B	IPv4 *	*	*	*	*	*	none		pERMIRIT	[Add] [Edit] [Delete] [Toggle] [Copy] [Save] [Separator]

**Bottom Screenshot: Firewall Rules for OPT1**

The browser address bar shows `http://192.168.33.1/firewall_rules.php?fif=opt1`. The interface shows the "Firewall / Rules / OPT1" path. The "Rules (Drag to Change Order)" table lists one rule:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/0 B	IPv4 *	*	*	*	*	*	none		Permitir trafico ApacheNet	[Add] [Edit] [Delete] [Toggle] [Copy] [Save] [Separator]

## 2.3 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.

The screenshot displays the pfSense web interface for configuring NAT Outbound and Firewall Rules.

**Top Section: Firewall / NAT / Outbound**

Navigation tabs: Port Forward, 1:1, **Outbound**, NPT.

**Outbound NAT Mode**

Mode selection:

- ☒ Automatic outbound NAT rule generation. (IPsec passthrough included)
- ☒ **Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)**
- ☐ Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
- ☐ Disable Outbound NAT rule generation. (No Outbound NAT rules)

**Mappings**

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input type="checkbox"/>	✓ WAN	OPT1 subnets	*	LAN subnets	*	WAN address	*	✓	prueba	[Edit] [Copy] [Delete]
<input type="checkbox"/>	✓ WAN	LAN subnets	*	OPT1 subnets	*	WAN address	*	✓	no nat entre lan dmz	[Edit] [Copy] [Delete]

**Bottom Section: Firewall / Rules / WAN**

Navigation tabs: Floating, **WAN**, LAN, OPT1.

**Rules (Drag to Change Order)**

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	*	*	none		PERMITIR	[Edit] [Copy] [Delete] [Toggle] [Save] [Separator]

### 3. 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.

```
root@ciberbambidhcp:~# systemctl status isc-dhcp-server
• isc-dhcp-server.service - ISC DHCP IPv4 server
   Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled; preset: enabled)
   Active: active (running) since Thu 2025-10-23 16:07:37 UTC; 36min ago
     Docs: man:dhcpd(8)
  Main PID: 1160 (dhcpd)
    Tasks: 1 (limit: 2265)
   Memory: 4.1M (peak: 4.6M)
      CPU: 103ms
   CGroup: /system.slice/isc-dhcp-server.service
           └─1160 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf enp0s8

oct 23 16:38:03 ciberbambidhcp dhcpd[1160]: DHCPREQUEST for 192.168.50.2 from 08:00:27:8b:1d:e9 via 192.168.50.1
oct 23 16:38:03 ciberbambidhcp dhcpd[1160]: DHCPACK on 192.168.50.2 to 08:00:27:8b:1d:e9 via 192.168.50.1
oct 23 16:39:30 ciberbambidhcp dhcpd[1160]: DHCPREQUEST for 192.168.33.100 from 08:00:27:78:e9:e8 (avalien-virtualbox) v
oct 23 16:39:30 ciberbambidhcp dhcpd[1160]: DHCPACK on 192.168.33.100 to 08:00:27:78:e9:e8 (avalien-virtualbox) via enp0
oct 23 16:43:03 ciberbambidhcp dhcpd[1160]: DHCPREQUEST for 192.168.33.4 from 08:00:27:e0:77:13 via enp0s8
oct 23 16:43:03 ciberbambidhcp dhcpd[1160]: DHCPACK on 192.168.33.4 to 08:00:27:e0:77:13 via enp0s8
oct 23 16:43:04 ciberbambidhcp dhcpd[1160]: DHCPREQUEST for 192.168.50.2 from 08:00:27:8b:1d:e9 via enp0s8
oct 23 16:43:04 ciberbambidhcp dhcpd[1160]: DHCPACK on 192.168.50.2 to 08:00:27:8b:1d:e9 via enp0s8
oct 23 16:43:04 ciberbambidhcp dhcpd[1160]: DHCPREQUEST for 192.168.50.2 from 08:00:27:8b:1d:e9 via 192.168.50.1
oct 23 16:43:04 ciberbambidhcp dhcpd[1160]: DHCPACK on 192.168.50.2 to 08:00:27:8b:1d:e9 via 192.168.50.1
root@ciberbambidhcp:~#
```

```
authoritative;

# Red LAN (GREEN)
subnet 192.168.33.0 netmask 255.255.255.0 {
    range 192.168.33.100 192.168.33.200;
    option routers 192.168.33.1;
    option broadcast-address 192.168.33.255;
    option domain-name "ciberbambi.local";
    option domain-name-servers 192.168.33.2;
}

# Red DMZ (ORANGE)
subnet 192.168.50.0 netmask 255.255.255.0 {
    range 192.168.50.100 192.168.50.200;
    option routers 192.168.50.1;
    option broadcast-address 192.168.50.255;
    option domain-name "ciberbambi.local";
    option domain-name-servers 192.168.33.2;
}
```

```
# Reservas DHCP para servidores fijos
host dhcpdns {
    hardware ethernet 08:00:27:2E:25:29;
    fixed-address 192.168.33.2;
    option routers 192.168.33.1;
}

host sambaftp {
    hardware ethernet 08:00:27:E0:77:13;
    fixed-address 192.168.33.4;
    option routers 192.168.33.1;
}

host apache {
    hardware ethernet 08:00:27:8B:1D:E9;
    fixed-address 192.168.50.2;
    option routers 192.168.50.1;
}
```

```
root@ciberbambiapache:~# ping www.google.com
PING www.google.com (142.250.200.132) 56(84) bytes of data.
64 bytes from mad41s14-in-f4.1e100.net (142.250.200.132): icmp_seq=1 ttl=114 time=19.0 ms
64 bytes from mad41s14-in-f4.1e100.net (142.250.200.132): icmp_seq=2 ttl=114 time=16.2 ms
64 bytes from mad41s14-in-f4.1e100.net (142.250.200.132): icmp_seq=3 ttl=114 time=15.9 ms
^C
[5]+  Stopped                  ping www.google.com
root@ciberbambiapache:~# _
```



```

GNU nano 7.2                                     named.conf
options {
    directory "/var/cache/bind";
    recursion yes;
    allow-query { 192.168.33.0/24; 192.168.50.0/24; 127.0.0.1; };
    forwarders { 8.8.8.8; 1.1.1.1; };
    listen-on { any; };
    listen-on-v6 { none; };
    dnssec-validation no;
    auth-nxdomain no;
};

GNU nano 7.2                                     db.ciberbambi.local *
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns.ciberbambi.local. admin.ciberbambi.local. (
                                3             ; Serial
                                604800        ; Refresh
                                86400         ; Retry
                                2419200       ; Expire
                                604800 )     ; Negative Cache TTL
;
@         IN      NS       ns.ciberbambi.local.

; Servidor DNS
ns        IN      A        192.168.33.2

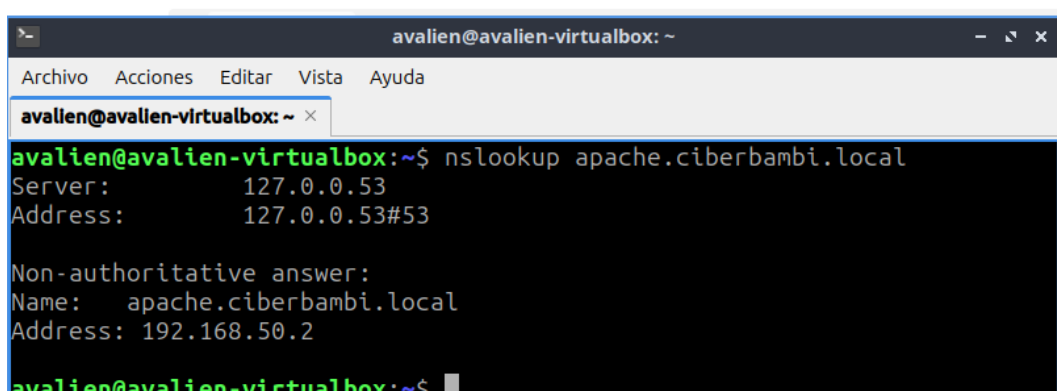
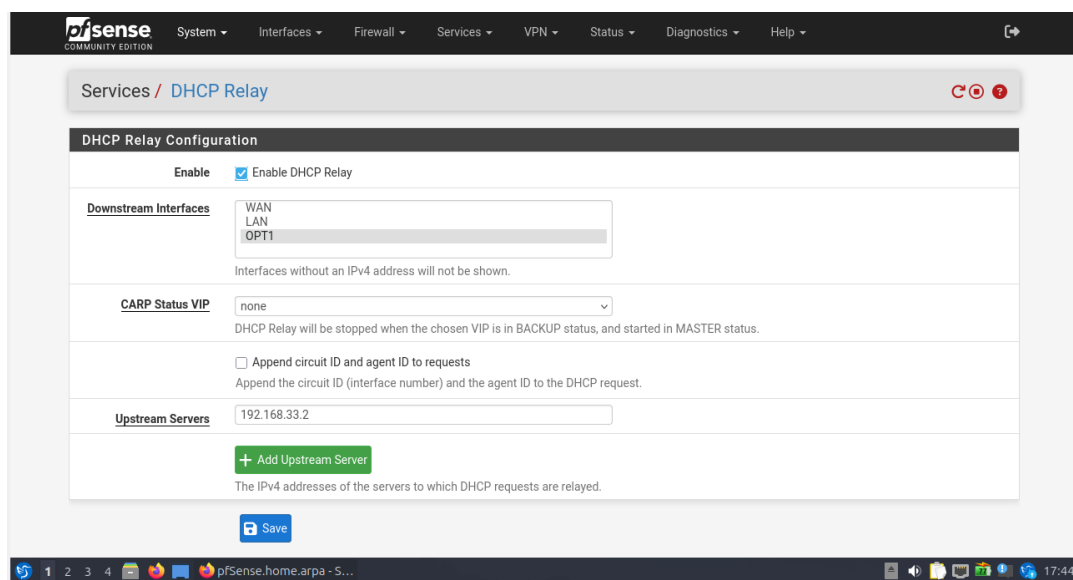
; Servidores y equipos Ciberbambi
dhcpdns   IN      A        192.168.33.2
sambaftp  IN      A        192.168.33.4
ftp       IN      A        192.168.33.4
wordpress IN      A        192.168.50.2
apache    IN      A        192.168.50.2

```

## 4. 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.



```
avalien@avalien-virtualbox: ~  
Archivo Acciones Editar Vista Ayuda  
avalien@avalien-virtualbox: ~ x  
avalien@avalien-virtualbox:~$ ping sambaftp.ciberbambi.local  
PING sambaftp.ciberbambi.local (192.168.33.4) 56(84) bytes of data.  
64 bytes from sambaftp.ciberbambi.local (192.168.33.4): icmp_seq=1 ttl  
=64 time=1.55 ms  
64 bytes from sambaftp.ciberbambi.local (192.168.33.4): icmp_seq=2 ttl  
=64 time=0.624 ms  
^Z  
[2]+ Detenido          ping sambaftp.ciberbambi.local  
avalien@avalien-virtualbox:~$
```

```
-rw-r--r-- 1 root root 237 ago 18 17:02 db.255  
-rw-r--r-- 1 root bind 364 oct 21 14:36 db.33.168.192  
-rw-r--r-- 1 root bind 320 oct 21 14:36 db.50.168.192  
-rw-r--r-- 1 root bind 784 oct 16 04:07 db.sambaftp.ciberbambi.local
```

## 5. 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.

```
root@ciberbambidhcp:~# systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Thu 2025-10-23 15:48:02 UTC; 54min ago
   TriggeredBy: • ssh.socket
   Docs: man:sshd(8)
         man:sshd_config(5)
   Process: 751 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 759 (sshd)
     Tasks: 1 (limit: 2265)
    Memory: 2.1M (peak: 2.3M)
       CPU: 106ms
   CGroup: /system.slice/ssh.service
           └─759 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

oct 23 15:48:02 ciberbambidhcp systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
oct 23 15:48:02 ciberbambidhcp sshd[759]: Server listening on 0.0.0.0 port 22.
oct 23 15:48:02 ciberbambidhcp sshd[759]: Server listening on :: port 22.
oct 23 15:48:02 ciberbambidhcp systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
root@ciberbambidhcp:~# _
```

## 6. 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.

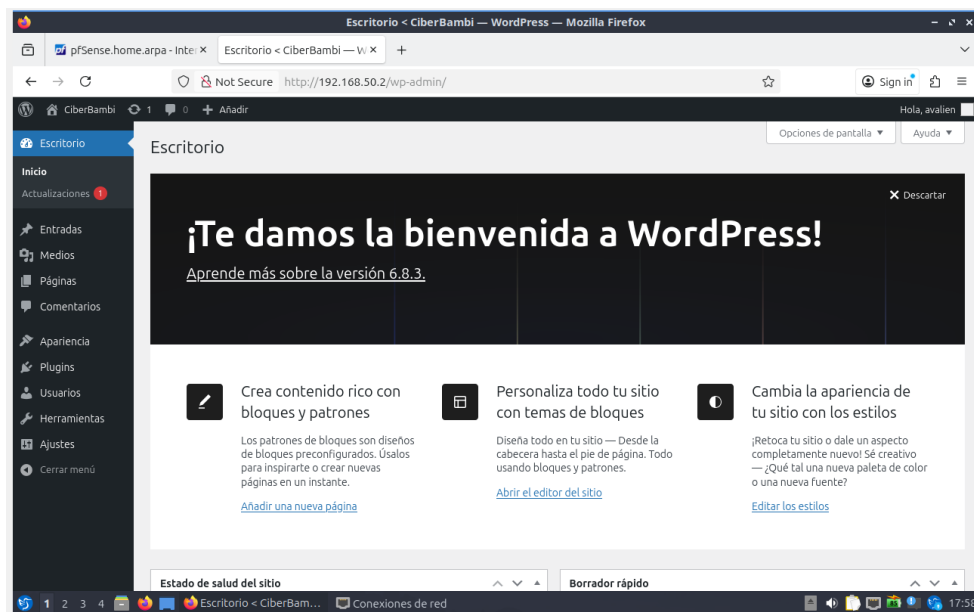
- **PostgreSQL** fue descartado por incompatibilidad con WordPress.
- El sitio es accesible desde LAN y DMZ, por IP y por DNS (wordpress.ciberbambi.local).
- WordPress utiliza MySQL local, comunicando directamente por socket interno.
- Se ha creado un usuario de prueba para validación del entorno.

```
root@ciberbambiapache:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Thu 2025-10-23 15:48:05 UTC; 45s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 952 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 953 (apache2)
     Tasks: 6 (limit: 2265)
    Memory: 21.1M (peak: 21.6M)
       CPU: 320ms
   CGroup: /system.slice/apache2.service
           └─953 /usr/sbin/apache2 -k start
             └─987 /usr/sbin/apache2 -k start
               └─988 /usr/sbin/apache2 -k start
                 └─989 /usr/sbin/apache2 -k start
                   └─990 /usr/sbin/apache2 -k start
                     └─991 /usr/sbin/apache2 -k start

oct 23 15:48:05 ciberbambiapache systemd[1]: Starting apache2.service - The Apache HTTP Server...
oct 23 15:48:05 ciberbambiapache apachectl[973]: AH00112: Warning: DocumentRoot [/var/www/html/wordpress] does not exist
oct 23 15:48:05 ciberbambiapache apachectl[973]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set
oct 23 15:48:05 ciberbambiapache systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)
```

```
root@ciberbambiapache:~# systemctl status mysql
● mysql.service - MySQL Community Server
   Loaded: loaded (/usr/lib/systemd/system/mysql.service; enabled; preset: enabled)
   Active: active (running) since Thu 2025-10-23 15:48:05 UTC; 1min 36s ago
     Process: 689 ExecStartPre=/usr/share/mysql/mysql-systemd-start pre (code=exited, status=0/SUCCESS)
    Main PID: 837 (mysqld)
     Status: "Server is operational"
       Tasks: 37 (limit: 2265)
    Memory: 431.4M (peak: 444.3M)
       CPU: 6.622s
   CGroup: /system.slice/mysql.service
           └─837 /usr/sbin/mysqld

oct 23 15:47:57 ciberbambiapache systemd[1]: Starting mysql.service - MySQL Community Server...
oct 23 15:48:05 ciberbambiapache systemd[1]: Started mysql.service - MySQL Community Server.
root@ciberbambiapache:~#
```

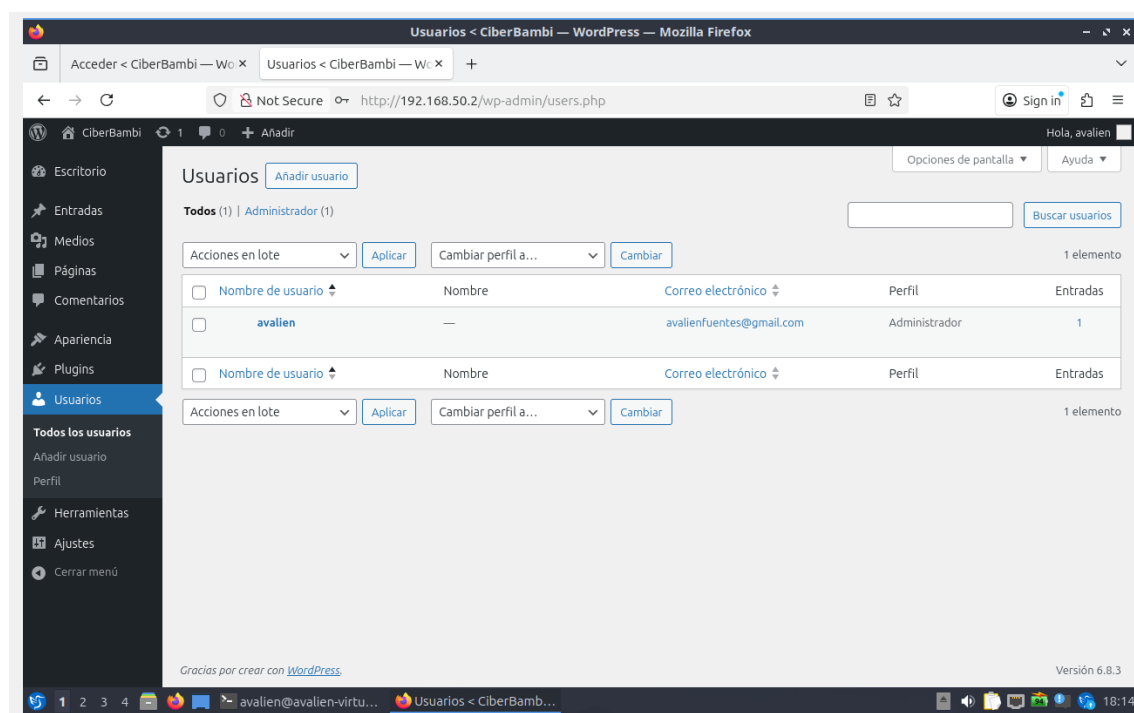
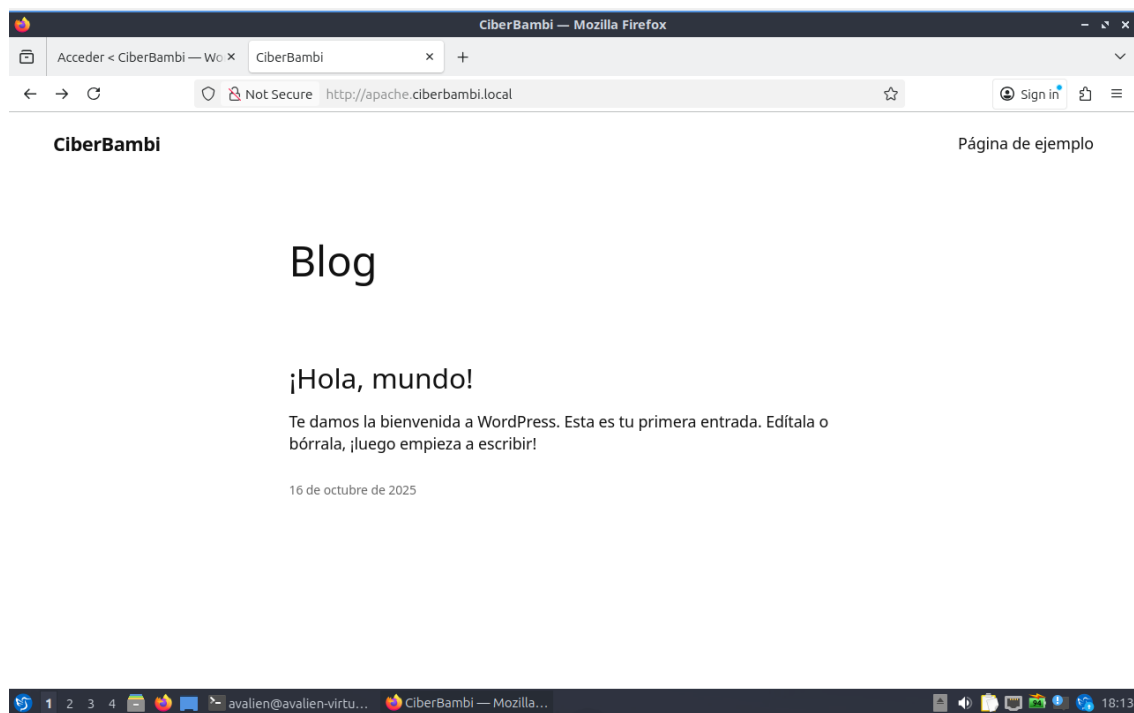


```
mysql> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
| wordpress |
+-----+
5 rows in set (0,01 sec)

mysql> _
```

```
mysql> SHOW TABLES;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta |
| wp_comments |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta |
| wp_terms |
| wp_usermeta |
| wp_users |
+-----+
12 rows in set (0,00 sec)

mysql>
```



## 7. 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.

```
[Ciberbambi_Samba]
comment = Carpeta compartida del dominio Ciberbambi
path = /srv/samba/
browseable = yes
read only = no
guest ok = yes
writable = yes
root@ciberbambisamba:/etc/samba#
```

```
root@ciberbambisamba:/etc/samba# systemctl status smbd
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/smbd.service; enabled; preset: enabled)
   Active: active (running) since Thu 2025-10-23 15:48:04 UTC; 31min ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
  Process: 829 ExecCondition=/usr/share/samba/is-configured smb (code=exited, status=0/SUCCESS)
 Main PID: 831 (smbd)
    Status: "smbd: ready to serve connections..."
     Tasks: 3 (limit: 2265)
  Memory: 12.1M (peak: 12.8M)
     CPU: 284ms
  CGroup: /system.slice/smbd.service
          └─831 /usr/sbin/smbd --foreground --no-process-group
            └─835 "smbd: notifyd"
              └─836 "smbd: cleanupd"

oct 23 15:48:03 ciberbambisamba systemd[1]: Starting smbd.service - Samba SMB Daemon...
oct 23 15:48:03 ciberbambisamba (smbd)[831]: smbd.service: Referenced but unset environment variable evaluates to an empty string: SMBSERVER
oct 23 15:48:04 ciberbambisamba systemd[1]: Started smbd.service - Samba SMB Daemon.
root@ciberbambisamba:/etc/samba#
```



```

GNU nano 7.2 /etc/vsftpd
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=YES
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (:::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=NO
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only

```

```

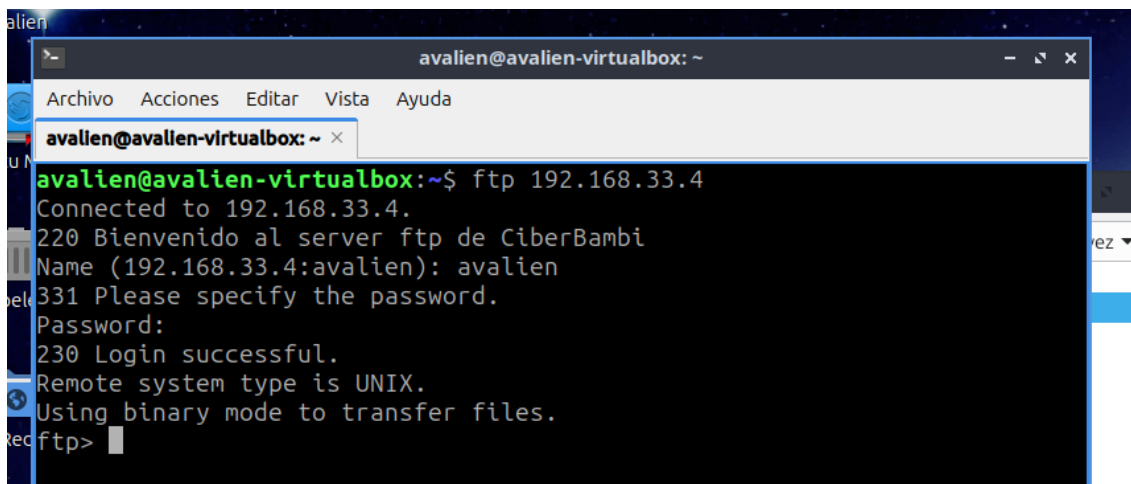
root@ciberbambisamba:~# ftp 192.168.33.4
Connected to 192.168.33.4.
220 Bienvenido al server ftp de CiberBambi
Name (192.168.33.4:avalien): avalien
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||44225|)
150 Here comes the directory listing.
drwxr-xr-x  2 1000      1000          4096 Oct 16 16:04 upload
226 Directory send OK.
ftp> _

```

```

root@ciberbambidhcp:~# ftp 192.168.33.4
Connected to 192.168.33.4.
220 Bienvenido al server ftp de CiberBambi
Name (192.168.33.4:avalien): avalien
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

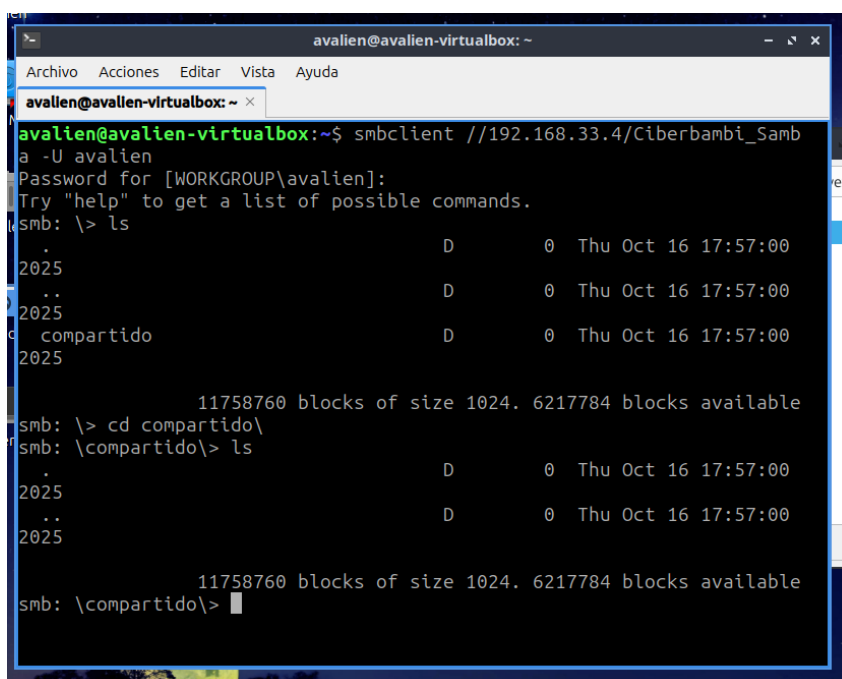
```



```

avalien@avalien-virtualbox: ~
Archivo Acciones Editar Vista Ayuda
avalien@avalien-virtualbox: ~ x
avalien@avalien-virtualbox:~$ ftp 192.168.33.4
Connected to 192.168.33.4.
220 Bienvenido al server ftp de CiberBambi
Name (192.168.33.4:avalien): avalien
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

```



```

avalien@avalien-virtualbox: ~
Archivo Acciones Editar Vista Ayuda
avalien@avalien-virtualbox: ~ x
avalien@avalien-virtualbox:~$ smbclient //192.168.33.4/Ciberbambi_Samba -U avalien
Password for [WORKGROUP\avalien]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0   Thu Oct 16 17:57:00
2025
..               D          0   Thu Oct 16 17:57:00
2025
compartido       D          0   Thu Oct 16 17:57:00
2025
11758760 blocks of size 1024. 6217784 blocks available
smb: \> cd compartido\
smb: \compartido\> ls
.                D          0   Thu Oct 16 17:57:00
2025
..               D          0   Thu Oct 16 17:57:00
2025
11758760 blocks of size 1024. 6217784 blocks available
smb: \compartido\>

```

## 8. 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.

## 9. 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.

```

root@ciberbambidhcp:/etc/bind# cat db.33.168.192
$TTL 604800
@ IN SOA ns.ciberbambi.local. admin.ciberbambi.local. (
    4          ; Serial
    604800     ; Refresh
    86400      ; Retry
    2419200    ; Expire
    604800 )   ; Negative Cache TTL

@ IN NS ns.ciberbambi.local.

; Servidores LAN
2 IN PTR dhcpdns.ciberbambi.local.
4 IN PTR sambatfp.ciberbambi.local.
root@ciberbambidhcp:/etc/bind# cat db.50.168.192
$TTL 604800
@ IN SOA ns.ciberbambi.local. admin.ciberbambi.local. (
    4          ; Serial
    604800     ; Refresh
    86400      ; Retry
    2419200    ; Expire
    604800 )   ; Negative Cache TTL

@ IN NS ns.ciberbambi.local.

; Servidores DMZ
2 IN PTR apache.ciberbambi.local.
root@ciberbambidhcp:/etc/bind# _

```

## 10. 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**”.