

# Recomendaciones para un Servidor FTP en Producción

## Introducción

Un servidor FTP en producción necesita estar bien configurado para que funcione de forma segura, disponible y fiable. He preparado estas recomendaciones basándome en cuatro aspectos fundamentales: límites de conexión, logs y auditoría, copias de seguridad, y firewall/NAT.

## 1. Límites de Conexión (Para que no se sature)

Tenemos que evitar que demasiadas personas o programas se conecten al mismo tiempo y colapsen el servidor.

### ¿Qué configurar?

#### Poner un tope de conexiones:

- Configurar el servidor para que solo acepte un número máximo de conexiones simultáneas (concurrentes)
- Por ejemplo: máximo 50 clientes conectados a la vez
- Así, si hay un ataque o un error, el servidor no se cae
- En vsftpd se configura con: `max_clients=50`

#### Limitar por usuario/IP:

- Poner un límite a cuántas conexiones puede abrir un solo usuario o una sola dirección IP
- Por ejemplo: máximo 3 conexiones por IP
- Esto evita que alguien abuse del servicio
- En vsftpd: `max_per_ip=3`

#### Tiempo de espera (Timeout):

- Establecer un tiempo máximo que puede estar inactiva una conexión antes de cerrarse automáticamente
- Por ejemplo: 10 minutos de inactividad
- Así liberamos recursos para otros usuarios
- En vsftpd: `idle_session_timeout=600` y `data_connection_timeout=300`

### Límites de velocidad (opcional):

- Si queremos que todos los usuarios tengan velocidad equitativa
- Por ejemplo: máximo 1 MB/s por usuario
- En vsftpd: `local_max_rate=1048576`

### ¿Por qué es importante?

- Protege contra ataques de denegación de servicio (DoS)
- Garantiza que el servidor siga funcionando aunque haya muchas conexiones
- Evita que un usuario acapare todos los recursos

## 2. Logs y Auditoría (Saber qué pasa)

Necesitamos saber quién hace qué, cuándo y desde dónde, especialmente si hay problemas o ataques.

### ¿Qué configurar?

#### Logs detallados:

Configurar el servidor para que guarde un registro de todo:

- Accesos correctos e incorrectos
- Fallos de login (intentos de contraseña incorrecta)
- Archivos subidos y descargados
- Errores del sistema

En vsftpd se activan con: `xferlog_enable=YES, log_ftp_protocol=YES`

#### Revisión periódica:

- Al menos una vez a la semana, alguien debería revisar los archivos de logs
- Buscar patrones extraños o intentos de acceso fallidos repetidos
- Detectar posibles ataques de fuerza bruta
- Los logs se guardan en archivos que podemos revisar

#### Rotación de logs:

- Los logs no pueden crecer infinitamente
- Configurar rotación automática: guardar 30 días y eliminar lo antiguo
- Comprimir logs antiguos para ahorrar espacio

**Almacenamiento seguro:**

- Los logs deben guardarse en un lugar seguro y diferente al propio servidor
- Si pasa algo con el servidor, no se pierden los logs
- Idealmente, copiarlos a otro servidor o a la nube

**Alertas automáticas:**

- Configurar herramientas como fail2ban para bloquear IPs con muchos intentos fallidos
- Recibir avisos cuando haya actividad sospechosa

**¿Qué información registran los logs?**

- Fecha y hora exacta de cada conexión
- Usuario que se conecta
- Dirección IP de origen
- Qué comandos ejecutó (listar, descargar, subir)
- Qué archivos se transfirieron y su tamaño
- Si el login fue exitoso o falló

### 3. Copias de Seguridad (Salvavidas)

Si algo se borra, se corrompe o hay un ataque, tenemos que poder recuperarlo todo rápidamente.

**¿Qué hacer backup?****Archivos de configuración:**

- `/etc/vsftpd.conf` - configuración principal
- `/etc/vsftpd.user_list` - lista de usuarios
- Configuraciones por usuario
- Certificados SSL (si usamos FTPS)

**Datos de usuarios:**

- Todos los archivos subidos por los usuarios
- Directorios home de cada usuario FTP
- Contenido web (si el FTP sirve una web)

**Logs:**

- Archivos de log para tener histórico de auditoría

## Frecuencia recomendada

Estrategia:

- Copia completa semanal: Todos los domingos a las 2:00 AM
- Copias incrementales diarias: Solo lo que cambió ese día
- Backup de configuración: Cada vez que se modifica + una vez por semana

## Regla 3-2-1

Esta es una regla de oro para backups:

- 3 copias de los datos (original + 2 backups)
- En 2 tipos de medios diferentes (disco local + nube, por ejemplo)
- 1 copia fuera del servidor (offsite)

## Automatización

Crear un script que se ejecute automáticamente:

- Hace el backup cada noche a las 2:00 AM
- Guarda los últimos 30 días
- Elimina automáticamente backups más antiguos
- Registra en un log si el backup fue exitoso o falló

## Pruebas (Muy importante)

No vale solo con hacer backups, tenemos que comprobar que funcionan:

- Una vez al mes, hacer una prueba de restauración
- Intentar recuperar archivos del backup en un servidor de pruebas
- Verificar que se pueden abrir y que no están corruptos
- Si el backup no funciona, ¡es como no tenerlo!

## Guardar lejos (offsite)

Las copias de seguridad (backups) deben almacenarse fuera del servidor:

- En otro servidor diferente
- En almacenamiento en la nube (Google Drive, Dropbox, etc.)
- En un disco duro externo guardado en otro sitio físico

Si hay un incendio, robo o fallo grave del servidor, los backups estarán a salvo.

## 4. Firewall y NAT (Puertas de seguridad)

El firewall es como el vigilante que solo deja entrar y salir a quien tiene permiso.

### Configuración del firewall

#### **Política por defecto:**

- Denegar todo el tráfico entrante que no esté expresamente permitido
- Permitir todo el tráfico saliente

#### **Puertos necesarios (solo abrir estos):**

- Puerto 22 (SSH) - para administración remota del servidor
- Puerto 21 (FTP) - canal de control
- Rango 40000-40100 (TCP) - canal de datos en modo pasivo

#### **Cerrar todo lo que no se use**

Si un puerto no es necesario, debe estar cerrado. Cada puerto abierto es una posible entrada para ataques.

### Modo Pasivo (imprescindible con firewall)

Para que FTP funcione correctamente con firewall, es obligatorio configurar el modo pasivo.

En vsftpd:

```
pasv_enable=YES  
pasv_min_port=40000  
pasv_max_port=40100
```

Esto hace que el servidor use siempre puertos del rango 40000-40100 para datos, y nosotros los tenemos abiertos en el firewall.

### Filtrado de IP (si es posible)

Si conocemos desde dónde se van a conectar los usuarios:

- Restringir el acceso al FTP solo a direcciones IP de confianza
- Por ejemplo: solo desde la red de la oficina (192.168.1.0/24)
- Bloquear IPs maliciosas conocidas

## Configuración del NAT

Si el servidor está detrás de un NAT (router), tenemos que configurarlo bien:

### **1. Port Forwarding en el router:**

- Puerto 21 → IP del servidor FTP (ej: 192.168.1.100)
- Rango 40000-40100 → IP del servidor FTP

### **2. Indicar la IP pública en vsftpd:**

El servidor necesita saber su IP pública para decírsela a los clientes en modo pasivo:

`pasv_address=IP_PUBLICA_DEL_SERVIDOR`

Por ejemplo: `pasv_address=203.0.113.45`

¿Por qué es importante?

Cuando un cliente se conecta desde Internet, el servidor le dice "conéctate a mi puerto 40050 para los datos". Si no sabe su IP pública, le dirá su IP privada (192.168.1.100) y el cliente no podrá conectarse.

Revisión recomendada:

- Revisar la configuración del NAT antes de poner el servidor en producción
- Hacer pruebas desde fuera de la red local
- Verificar que el modo pasivo funciona correctamente

## Protección contra ataques de fuerza bruta

Configurar fail2ban para que bloquee automáticamente IPs sospechosas:

- Si alguien falla el login 3 veces en 10 minutos
- Se bloquea su IP durante 1 hora
- Protege contra intentos de adivinar contraseñas