DISPONIBILIDAD Y BUENAS PRÁCTICAS PARA UN SERVIDOR FTP EN PRODUCCIÓN

Javier Morales Simón – 2º CFGS Desarrollo de Aplicaciones Web

ÍNDICE

Límites de conexión

El objetivo aquí es prevenir ataques de Denegación de Servicio (DoS) y asegurar que los recursos del sistema no se agoten por usuarios malintencionados o procesos colgados:

- **Límite de conexiones simultáneas por IP:** Restringe a un máximo razonable (ej. 2 a 5 conexiones) para evitar que un solo usuario sature el ancho de banda.
- **Tiempo de espera de inactividad (Timeout):** Configura el servidor para cerrar sesiones inactivas tras 5 o 10 minutos. Esto libera sockets y memoria.
- **Control de ancho de banda:** Implementa "Throttling" (limitación de velocidad) tanto para subidas como para descargas, protegiendo así el desempeño de otros servicios en la misma red.
- **Límites de reintentos de login:** Bloquea temporalmente IPs que fallen más de 3 veces en un minuto (integración ideal con herramientas como *Fail2Ban*).

Logs y auditoría

Si no puedes medirlo, no puedes asegurarlo. Los registros son tu "caja negra" en caso de incidentes.

- **Nivel de detalle (Verbosity):** Activa el registro detallado de transferencias (xferlog) que incluya: IP de origen, usuario, nombre del archivo, tamaño y si la operación fue exitosa.
- **Centralización de Logs:** No guardes los logs solo en el servidor. Envíalos a un servidor externo (SIEM o un servidor Syslog dedicado) para evitar que un atacante borre sus huellas tras comprometer el sistema.
- **Rotación de Logs:** Configura una política de rotación (diaria o semanal) y retención (mínimo 90 días por cumplimiento legal/seguridad) para evitar que el disco se llene.
- **Monitoreo en tiempo real:** Establece alertas para patrones sospechosos, como múltiples accesos fallidos desde rangos de IP inusuales.

Copias de seguridad

El almacenamiento FTP suele ser dinámico; perder los datos puede paralizar flujos de trabajo críticos.

- **Backup de Configuración:** Resguarda los archivos de configuración del servicio (vsftpd.conf, proftpd.conf, etc.) y las bases de datos de usuarios virtuales si los usas.
- **Regla 3-2-1:** Mantén 3 copias de los datos, en 2 soportes diferentes, con 1 copia fuera de la ubicación física (off-site o cloud).
- **Integridad de Datos:** Realiza verificaciones de integridad mediante sumas de comprobación (Hashes) para asegurar que los archivos respaldados no estén corruptos.
- **Pruebas de restauración:** Un backup que no se ha probado no es un backup. Realiza simulacros de restauración trimestrales.

Firewall y NAT

El FTP es famoso por ser "problemático" con los Firewalls debido a que utiliza canales separados para control y datos:

- **Uso exclusivo de Modo Pasivo:** En entornos con NAT, el modo activo suele fallar. Configura un rango específico de puertos para el modo pasivo (ej. 50000-51000) en el servidor.
- **Apertura Estricta de Puertos:**
  - **Puerto 21:** Para control (solo si usas FTPS).
  - **Rango Pasivo:** Abre en el Firewall solo el rango definido anteriormente.
- **Publicación de IP Pasiva:** Si el servidor está detrás de un NAT, debes configurar la directiva pasv_address (en vsftpd) o equivalente para que el servidor informe su IP pública y no la privada a los clientes.
- **Prioriza SFTP o FTPS:** Si es posible, bloquea el FTP estándar (puerto 21 sin cifrar) y utiliza SFTP (puerto 22 - SSH), que es mucho más amigable con los firewalls al usar un solo puerto para todo.