CSF Configserver Firewall

CSF: ConfigServer Security & Firewall

Guía básica para usuarios no técnicos

¿Qué es CSF?

CSF (*ConfigServer Security & Firewall*) es un cortafuegos avanzado para servidores Linux. Funciona como una **capa de protección** que filtra conexiones, limita ataques y bloquea IPs maliciosas.

> **Componentes clave**
>
> - **iptables / nftables**: motor de filtrado de red en Linux
> - **LFD (Login Failure Daemon)**: demonio que vigila logs y detecta intentos de acceso fallidos
> - **Integra** con paneles como DirectAdmin, cPanel, Plesk

¿Cómo protege el servidor?

1. **Filtrado de puertos**
   - Solo permite los puertos necesarios (ej. 22, 80, 443, 2222).
2. **Detección de fuerza bruta (LFD)**
   - Cuenta intentos fallidos de SSH, FTP, correo, panel, etc.
   - Si se supera el límite (p. ej. 10 fallos en 5 min), la IP se bloquea.
3. **Alertas por e-mail**
   - Envía notificaciones cuando bloquea o detecta actividad sospechosa.
4. **Rate limiting**

- Limita conexiones simultáneas y velocidad (DoS ligero).

5. **Listas blanca / negra**
   - IPs de confianza (`csf.allow`)
   - IPs bloqueadas permanentemente (`csf.deny`)

Archivos y comandos principales

Archivo / Comando	Descripción
`/etc/csf/csf.conf`	Archivo de configuración principal
`/etc/csf/csf.allow`	Lista blanca de IPs (permitir)
`/etc/csf/csf.deny`	Lista negra de IPs (bloquear)
`csf -r`	Reiniciar CSF (aplica cambios)
`csf -d IP`	Bloquear IP manualmente
`csf -a IP`	Añadir IP a lista blanca
`csf -g IP`	Buscar IP en todas las listas

Parámetros importantes (csf.conf)

Opción	Qué hace	Valor recomendado
`TCP_IN`	Puertos TCP permitidos de entrada	`22,80,443,2222`
`TCP_OUT`	Puertos TCP permitidos de salida	`80,443,53`
`LF_TRIGGER`	Nº de bloqueos antes de alerta	`5`
`LF_SSHD`	Intentos fallidos SSH antes de bloqueo	`5`
`CONNLIMIT`	Límite de conexiones simultáneas por IP	`80;20` (20 conexiones al puerto 80)

> **Nota:** Ajustar estos valores según tus servicios y nivel de riesgo.

Relación CSF ?? BFM (DirectAdmin)

- **BFM** detecta intentos fallidos en DirectAdmin y puede *pasar* la IP a CSF.

- **CSF/LFD** bloquea a nivel de red, impidiendo cualquier conexión desde esa IP.

Buenas prácticas

1. **Mantener CSF y el sistema actualizados**
2. **Revisar las alertas**: identificar falsos positivos o ataques reales
3. **No abrir puertos innecesarios**
4. **Usar listas blanca** para IPs fijas (oficina, hogar)
5. **Verificar logs** de LFD: `/var/log/lfd.log`

Resumen

CSF + LFD actúan como **muralla de defensa**:

- Bloquean puertos no usados
- Detienen ataques de fuerza bruta
- Alertan al admin en tiempo real
- Se integran con DirectAdmin para protección adicional

Configurado correctamente, CSF mantiene el servidor seguro con un impacto mínimo en los usuarios legítimos.

Aviso

Si necesitas soporte profesional puedes contratar con Castris soporte profesional.

Revision #3
Created 2025-06-19 08:28:01 UTC by Abkrim
Updated 2025-06-19 08:47:36 UTC by Abkrim