

En el siguiente how-to se mostrará la forma de **instalar y configurar CSF** en un servidor que usa cPanel. CSF es un add que nos permite tener un **Firewall** de fácil manejo y de gran ayuda para proporcionar seguridad a nuestro servidor con Cpanel.

¿Qué es CSF?

CSF es un Firewall que nos permite proporcionar de manera sencilla seguridad para servidores nuestros Linux.

La idea de CSF, como con la mayoría de las configuraciones de firewall iptables, es bloquear todo y luego permitir sólo aquellas conexiones que desee. Esto es hecho en iptables al dejar caer todas las conexiones de entrada y salida del servidor en todos protocolos.

En particular, se impide el acceso no autorizado a los demonios de red que queremos para restringir el acceso por dirección IP.

Instalación de CSF

La instalación de CSF es relativamente sencilla y basta con acceder como root mediante SSH y ejecutar la siguiente lista de comandos:

```
wget http://www.configserver.com/free/csf.tgz
tar -xzf csf.tgz
cd csf
sh install.sh
```

Así de simple es la instalación de CSF y luego para poder acceder al mismo vamos a nuestra administración en WHM de nuestro servidor con Cpanel y buscamos la opción **ConfigServer & Firewall** o bien si se quiere hacer una edición directa de las características de CSF podemos editar directamente desde la siguiente ruta ***/etc/csf/****

Configuración de CSF

1. Configura los valores **TCP_IN**, **TCP_OUT**, **UDP_IN** y **UDP_OUT** según el servidor en el que lo instales asegurando que los valores que se coloquen serán los adecuados y sólo los necesarios.
2. **Reinicia** CSF y LFD
3. Configura **TESTING** a **0** hasta que estés contento con tus resultados.

Detalles sobre la configuración

CSF está preconfigurado para trabajar con todos los puertos estándar de cPanel abiertos. También configura el puerto SSH si este difiere del habitual.

También se debe de asegurar que el daemon de registros del kernel (klogd) esté habilitado.

Por último, se debe de acceder **WHM** en tu servidor **cPanel** como root y busca **ConfigServer Security Firewall**

Dentro de **CSF**, realizaremos clic en **Firewall configuration** y estableceremos los siguientes valores:

LF_DSHIELD: Cambia esta opción a **86400**. Esta es una lista actualizada de IPs atacantes. Activando esto evitará que conecten a tu servidor.

Alertas Anti-SPAM

CSF también puede ayudarnos a protegernos del SPAM. Sólo hay que buscar en la configuración los siguientes campos:

LF_SCRIPT_ALERT: Por defecto aparecerá en **0**. Cámbialo a **1** para que el servidor te envíe un email cuando el límite configurado abajo sea alcanzado en una hora.

LF_SCRIPT_LIMIT: Por defecto aparecerá en **100**. Lo recomendable es cambiarlo a **250** aunque depende de los sitios alojados. Esto define el límite para la alerta enviada arriba

Una vez realizados los cambios necesarios se debe de descender hasta el final de la página y hacer clic en **Change** para guardar la configuración. Luego hacer clic en **Restart csf-efd**

Debes ver un gran botón de aceptación y cerca del mismo el mensaje:

```
csf: TESTING mode is enabled - don't forget to disable it in the configuration
```

```
Starting lfd:[ OK ]
```

Luego hacer clic en **Return**

Ahora se deben de probar todos los servicios para asegurar de que están funcionando (SSH, FTP, http, etc.) y luego regresar a la configuración de CSF para buscar el siguiente campo:

TESTING: Por defecto estará en **1**. Lo cambiaremos a **0** para que CSF comience a funcionar. Entonces haremos clic de nuevo en **Restart csf+efd**

Con esto CSF ya debe estar funcionando. Se puede comprobar a través la página principal de CSF en **WHM**, donde debe aparecer:

```
Firewall Status: Running
```

Desinstalar CSF y LFD

Desinstalar CSF y LFD es lo más simple:

```
cd /etc/csf  
sh uninstall.sh
```

TIP's

1. En CSF podemos verificar corriendo un test que valores son los que debemos de configurar tanto en nuestra configuración de CSF como tal como en WHM / Cpanel para proporcionar un grado de seguridad mayor. Esto se realizar haciendo clic en la opción "Check server security", al ingresar en esta sección se realizará un análisis de nuestra seguridad en general y se mostrarán las respectivas leyendas que nos indicarán que partes andan bien y a cuáles debemos de realizar una corrección con sugerencias de parte de CSF.
2. Firewall profiles: Esta opción nos permite activar un perfil predeterminado ya por CSF y que dependiendo de nuestras necesidades proporcionará u mayor grado de restricción y seguridad a nuestro servidor, hay que tener cuidado si se utilizan estos perfiles ya que pueden evitar el buen funcionamiento de WHM / Cpanel.