Install ConfigServer Firewall On A cPanel Server

ConfigServer Firewall (CSF) is a popular Linux firewall security suite. It is easy to install, flexible to configure and secure with extra checks. CSF helps control exactly how much traffic is allowed in and out of the server to protect the server from malicious attack. It can also specify the type of traffic that comes in.

The CSF installation includes control panel user interface available via WHM, and login failure daemon process (lfd) that runs periodically to scan the latest log file entries for login attempts that continually fail within a short period of time. Such attempts are often called "Brute-force attacks" and the daemon process responds very quickly to such patterns and blocks offending IPs quickly.

See the end of this article for command-line instructions.

Log into your server via ssh or via console to get started with CSF installation.

Change to temp directory:

```
# cd /tmp
```

Download the file:

```
# wget http://configserver.com/free/csf.tgz
```

```
root@vps [/tmp/csf]# cd /tmp
root@vps [/tmp]# wget http://configserver.com/free/csf.tgz
```

```
root@vps [/tmp/csf]# cd /tmp
root@vps [/tmp]# wget http://configserver.com/free/csf.tgz
--2016-05-05 15:51:15--  http://configserver.com/free/csf.tgz
Resolving configserver.com... 2a01:c0:2:22::3, 109.70.137.78
Connecting to configserver.com|2a01:c0:2:22::3|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://download.configserver.com/csf.tgz [following]
--2016-05-05 15:51:15--  http://download.configserver.com/csf.tgz
Resolving download.configserver.com... 85.10.199.177
Connecting to download.configserver.com|85.10.199.177|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 690967 (675K) [application/x-gzip]
Saving to: "csf.tgz.1"

100%[=====================================================>] 690,967      353K/s   in 1.9s

2016-05-05 15:51:18 (353 KB/s) - "csf.tgz.1" saved [690967/690967]

root@vps [/tmp]#
```

Unpack the archive:

```
# tar xfz csf.tgz
```

Navigate to the uncompressed csf directory:

```
# cd csf
```

Run the installer:

```
# sh install.sh
```

```
root@vps [/tmp/csf]# cd ../
root@vps [/tmp]# tar xfz csf.tgz
root@vps [/tmp]# cd csf
root@vps [/tmp/csf]# sh install.sh
```

This will create a configuration file and add all required cPanel services to the allow list.

Next, disable testing mode by editing the main CSF configuration file. Open the file using any editor (vi, nano, etc):

```
# nano /etc/csf/csf.conf
```

Scroll down and find: TESTING = "1" and change to TESTING = "0"

Note: keep the quotations ("") enclosing the number.

```
###############################################################################
# SECTION:Initial Settings
###############################################################################
# Testing flag - enables a CRON job that clears iptables incase of
# configuration problems when you start csf. This should be enabled until you
# are sure that the firewall works - i.e. incase you get locked out of your
# server! Then do remember to set it to 0 and restart csf when you're sure
# everything is OK. Stopping csf will remove the line from /etc/crontab
#
# lfd will not start while this is enabled
TESTING = "0"

# The interval for the crontab in minutes. Since this uses the system clock the
# CRON job will run at the interval past the hour and not from when you issue
# the start command. Therefore an interval of 5 minutes means the firewall
# will be cleared in 0-5 minutes from the firewall start
TESTING_INTERVAL = "5"
```

To save, press 'Ctrl O'.

Hit 'Enter' when your screen asks "File Name to Write: /etc/csf/csf.conf".

Next, hit 'Ctrl X' to exit.

When done, restart CSF:

```
# csf -r
```

Now CSF is installed and ready. You can simply manage it via cPanel WHM interface WHM > Config Security & Firewall.

OR via command-line:

ALLOW / BLOCK IP with CSF:

In the event that you need to allow/block IP address using command line, the options are as follows:

To add your IP address to a permanent allow list:

```
# csf -a 123.45.67.89
```

To block the IP:

```
# csf -d 123.45.67.89
```

To clear blocked IPs:

```
# csf -f
```

Additional Options:

Via Command line you can type: csf -[option]

Commands to Know:

cd = change directory

cd ../ = change up a directory

wget = fetches a download link

tar = tar is to uncompress archived files

csf = run commands for the csf firewall followed by an option

ls = list, which shows the contents in the directory you're in.

pwd = shows the directory you're currently in.

For more information about CSF, see: http://configserver.com/cp/csf.html

For more information about Basic linux Commands

See: http://www.comptechdoc.org/os/linux/usersguide/linux_ugbasics.html