digitalocean.com

How To Install and Configure Config Server Firewall (CSF) on Ubuntu

Article Submitted by: Lassi

https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-config-server-firewall-csf-on-ubuntu

Introduction

Config Server Firewall (or CSF) is a free and advanced firewall for most Linux distributions and Linux based VPS. In addition to the basic functionality of a firewall – filtering packets – CSF includes other security features, such as login/intrusion/flood detections. CSF includes UI integration for cPanel, DirectAdmin and Webmin, but this tutorial only covers the command line usage. CSF is able to recognize many attacks, such as port scans, SYN floods, and login brute force attacks on many services. It is configured to temporarily block clients who are detected to be attacking the cloud server.

The full list of supported operating systems and features can be found on ConfigServer's website.

This tutorial is written for Debian based VPS, such as Debian and Ubuntu. The commands should be executed with root permissions, by logging in as root, or initiating a root shell with the following command if sudo is installed:

```
sudo su
```

Note: *This tutorial covers IPv4 security. In Linux, IPv6 security is maintained separately from IPv4. For example, "iptables" only maintains firewall rules for IPv4 addresses but it has an IPv6 counterpart called "ip6tables", which can be used to maintain firewall rules for IPv6 network addresses.*

If your VPS is configured for IPv6, please remember to secure both your IPv4 and IPv6 network interfaces with the appropriate tools. For more information about IPv6 tools, refer to this guide: How To Configure Tools to Use IPv6 on a Linux VPS

Features

Config Server Firewall offers a wide range of protections for your VPS.

Login authentication failure daemon:

CSF checks the logs for failed login attempts at regular time interval, and is able to recognize most unauthorized attempts to gain access to your cloud server. You can define the desired action CSF takes and after how many attempts in the configuration file.

The following applications are supported by this feature:

- Courier imap, Dovecot, uw-imap, Kerio
- openSSH
- cPanel, WHM, Webmail (cPanel servers only)
- Pure-ftpd, vsftpd, Proftpd
- Password protected web pages (htpasswd)
- Mod_security failures (v1 and v2)
- Suhosin failures
- Exim SMTP AUTH

In addition to these, you are able define your own login files with regular expression matching. This can be helpful if you have an application which logs failed logins, but does block the user after specific number of attempts.

Process tracking

CSF can be configured to track processes in order to detect suspicious processes or open network ports, and send an email to the system administrator if any is detected. This may help you to identify and stop a possible exploit on your VPS.

Directory watching

Directory watching monitors the /temp and other relevant folders for malicious scripts, and sends an email to the system administrator when one is detected.

Messenger service

Enabling this feature allows CSF to send a more informative message to the client when a block is applied. This feature has both pros and cons. On one hand, enabling it provides more information to the client, and thus may cause less frustration for instance in case of failed logins. On the other hand, this provides more information, which might make it easier for an attacker to attack your VPS.

Port flood protection

This setting provides protection against port flood attacks, such as denial of service (DoS) attacks. You may specify the amount of allowed connections on each port within time period of your liking. Enabling this feature is recommended, as it may possibly prevent an attacker forcing your services down. You should pay attention to what limits you set, as too restrictive settings will drop connections from normal clients. Then again, too permissive settings may allow an attacker to succeed in a flood attack.

Port knocking

Port knocking allows clients to establish connections a server with no ports open. The server allows clients connect to the main ports only after a successful port knock sequence. You may find this useful if you offer services which are available to only limited audience.

Read more about port knocking

Connection limit protection

This feature can be used to limit the number concurrent of active connections from an IP address to each port. When properly configured, this may prevent abuses on the server, such as DoS attacks.

Port/IP address redirection

CSF can be configured to redirect connections to an IP/port to another IP/port. Note: After redirection, the source address of the client will be the server's IP address. This is not an equivalent to network address translation (NAT).

UI integration

In addition to command line interface, CSF also offers UI integration for cPanel and Webmin. If you are not familiar with Linux command line, you might find this feature helpful.

IP block lists

This feature allows CSF to download lists of blocked IP addresses automatically from sources defined by you.

Installing ConfigServer Firewall

Step 1: Downloading

Config Server Firewall is not currently available in Debian or Ubuntu repositories, and has to be downloaded from the ConfigServer's website.

```
wget http://download.configserver.com/csf.tgz
```

This will download CSF to your current working directory.

Step 2: Uncompressing

The downloaded file is a compressed from of tar package, and has to be uncompressed and extracted before it can be used.

```
tar -xzf csf.tgz
```

Step 3: Installing

If you are using another firewall configuration scripts, such as UFW, you should disable it before proceeding. Iptables rules are automatically removed.

UFW can be disabled by running the following command:

```
ufw disable
```

Now it is time to execute the CSF's installer script.

```
cd csf
```

```
sh install.sh
```

The firewall is now installed, but you should check if the required iptables modules are available.

```
perl /usr/local/csf/bin/csftest.pl
```

The firewall will work if no fatal errors are reported.

Note: Your IP address was added to the whitelist if possible. In addition, the SSH port has been opened automatically, even if it uses custom port. The firewall was also configured to have testing mode enabled, which means that the iptables rules will be automatically removed five minutes after starting CSF. This should be disabled once you know that your configuration works, and you will not be locked out.

Basic Configuration

CSF can be configured by editing its configuration file csf.conf in /etc/csf:

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

The changes can be applied with command:

```
csf -r
```

Step 1: Configuring ports

The less access there is to your VPS, the more secure your server is. However, not all ports can be closed as the clients must be able to use your services.

The ports opened by default are the following:

```
TCP_IN = "20,21,22,25,53,80,110,143,443,465,587,993,995"
```

```
TCP_OUT = "20,21,22,25,53,80,110,113,443"
```

```
UDP_IN = "20,21,53"
```

```
UDP_OUT = "20,21,53,113,123"
```

Services using the open ports:

- Port 20: FTP data transfer
- Port 21: FTP control
- Port 22: Secure shell (SSH)
- Port 25: Simple mail transfer protocol (SMTP)
- Port 53: Domain name system (DNS)

- Port 80: Hypertext transfer protocol (HTTP)
- Port 110: Post office protocol v3 (POP3)
- Port 113: Authentication service/identification protocol
- Port 123: Network time protocol (NTP)
- Port 143: Internet message access protocol (IMAP)
- Port 443: Hypertext transfer protocol over SSL/TLS (HTTPS)
- Port 465: URL Rendesvous Directory for SSM (Cisco)
- Port 587: E-mail message submission (SMTP)
- Port 993: Internet message access protocol over SSL (IMAPS)
- Port 995: Post office protocol 3 over TLS/SSL (POP3S)

It is possible that you are not using all of these services, so you can close the ports that are not used. I would recommend closing all ports (removing port number form the list), and then adding the ports you need.

Below are port sets that should be opened if you are running the listed service:

On any server:

```
TCP_IN: 22,53
TCP_OUT: 22,53,80,113,443
UPD_IN: 53
UPD_OUT: 53,113,123
```

Apache:

```
TCP_IN: 80,443
```

FTP server:

```
TCP_IN: 20,21
TCP_OUT: 20,21
UPD_IN: 20,21
UPD_OUT:20,21
```

Mail server:

```
TCP_IN: 25,110,143,587,993,995
TCP_OUT: 25,110
```

MySQL server (if remote access is required)

```
TCP_IN: 3306
TCP_OUT: 3306
```

Note: If you are using IPv6 for your services, you should also configure TCP6_IN, TCP6_OUT, UPD6_IN, and UPD6_OUT similarly to how IPv4 ports were configured earlier.

You can find a comprehensive list of TCP and UDP ports on Wikipedia. You should open the ports of all the services you use.

Step 2: Additional settings

CSF offers a vast number of different options in its configuration files. Some of the most commonly used settings are explained below.

ICMP_IN Setting ICMP_IN to 1 allows ping to your server and 0 refuses are such requests. If you are hosting any public services, it is recommended to allow ICMP requests, as these can be used to determine whether or not your service is available.

ICMP_IN_LIMIT Sets the number of ICMP (ping) requests allowed from one IP address within a specified amount of time. There is usually no need to change the default value (1/s)

DENY_IP_LIMIT Sets the number of blocked IP addresses CSF keeps track of. It is recommended to limit the number of denied IP addresses as having too many blocks may slow down the server performance.

DENY_TEMP_IP_LIMIT Same as above, but for temporary IP address blocks.

PACKET_FILTER Filter invalid, unwanted and illegal packets.

SYNFLOOD, SUNFLOOD_RATE and SYNFLOOD_BURST This offers protection against SYN flood attacks. This slows down the initialization of every connection, so you should enable this only if you know that your server is under attack.

CONNLIMIT Limits the number of concurrent active connections on port.

Value:

```
22;5;443;20
```

would allow 5 concurrent connections on port 22 and 20 concurrent connections on port 443.

PORTFLOOD Limits the number of connections per time interval that new connections can be made to specific ports.

Value:

```
22;tcp;5;250
```

would limit block the IP address if more than 5 connections are established on port 22 using TCP protocol within 250 seconds. The block is removed once 250 seconds have passed after the last packet sent by the client to this port. You may add more ports by separating them by commas like described below.

```
port1;protocol1;connection_count1;time1,port2;protocol2;connection_count2;time2
```

More settings

CSF offers a wide range of settings which are not covered in this tutorial. The default values are generally good, and can be used on almost any server. The default settings are configured to prevent most flood attacks, port scans and unauthorized access attempts.

If you would, however, like to adjust the configuration in more detail, please read the comments in /etc/csf/csf.conf and edit them as you like.

Step 3: Applying the Changes

Whenever you are altering the settings in csf.conf, you should save the files and restart CSF in order for the changes to take effect.

Once you are ready with the configuration, close the file by pressing Ctrl + X. When you are asked whether to save the changes or not, press Y to save the changes.

After this, you should apply the changes by restarting CSF with command:

```
csf -r
```

If everything went like planned, and you are still able to access the server, open the configuration file once more:

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

and change setting TESTING at the beginning of the configuration file to 0 as shown below:

```
TESTING = "0"
```

Save the file, and apply the changes with command:

```
csf -r
```

Blocking and Allowing IP Addresses

One of the most basic features of a firewall is the ability to block certain IP addresses. You may deny (blacklist), allow (whitelist) or ignore IP addresses by editing the configuration files csf.deny, csf.allow and csf.ignore.

Blocking IP addresses

If you would like to block an IP address or range, open csf.deny.

```
nano /etc/csf/csf.deny
```

Blocked IP addresses or ranges all reserve one line in csf.deny file. If you would like to block IP address 1.2.3.4 as well as IP range 2.3.*.*, you should add the following lines to the file:

```
1.2.3.4
2.3.0.0/16
```

IP ranges are represented using the CIDR notation

Allowing IP addresses

If you would like an IP address or range to be excluded from all blocks and filters, you may add them to csf.allow file. Please note that allowed IP addresses are allowed even if they are explicitly blocked in csf.deny file.

Allowing IP addresses works similarly to blocking them. The only difference is that you should edit /etc/csf/csf.allow instead of csf.deny.

```
nano /etc/csf/csf.allow
```

Ignoring IP addresses

CSF also offers ability to exclude IP addresses from the firewall filters. IP addresses in csf.ignore will bypass the firewall filters, and can only be blocked if listed in csf.deny file.

```
nano /etc/csf/csf.ignore
```

In order to changes take effect, you should restart CSF after editing any of the files described above with command:

```
csf -r
```