How to install CSF in Ubuntu 18.04 / 20.04 / 22.04

Linux system administration (https://www.webhi.com/how-to/tutorial/linux-sysadmin/), Security (https://www.webhi.com/how-to/tutorial/cyber-security/)

The **ConfigServer Security & Firewall (CSF)** is a firewall tool that provides an easy way to configure your server's security settings. This guide will walk you through the installation and configuration of the CSF firewall on Ubuntu.

CSF offers various features to protect your VPS. These include:

- **Login authentication failure daemon**: CSF checks for unauthorized attempts to access your cloud server and allows you to define the desired action to take after a specified number of attempts. This feature supports various applications and allows you to define your own login files.
- **Process tracking**: CSF can track processes to detect suspicious processes or open network ports and notify the system administrator.
- **Directory watching**: CSF monitors relevant folders for malicious scripts and notifies the system administrator when one is detected.

- **Messenger service**: Enabling this feature provides more information to the client and may prevent frustration in case of failed logins. However, it also makes 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, and allows you to specify the amount of allowed connections on each port within a time period of your liking.
- **Port knocking**: This feature allows clients to establish connections with no ports open and allows connections to main ports only after a successful port knock sequence.
- **Connection limit protection**: This feature limits the number of concurrent active connections from an IP address to each port and may prevent abuses on the server.
- **Port/IP address redirection**: CSF can redirect connections to an IP/port to another IP/port.
- **UI integration**: CSF offers UI integration for cPanel and Webmin in addition to the command line interface.
- **IP block lists**: This feature allows CSF to download lists of blocked IP addresses automatically from sources defined by you.

Step 1: Update your system

Before installing any new software, it is always a good idea to update your system packages. Run the following command to update your Ubuntu system:

```
$ sudo apt update
$ sudo apt upgrade
```

Step 2: Install CSF Firewall

Once the system is up-to-date, we can proceed with the installation of CSF Firewall. The following steps will guide you through the process:

- Download the latest version of CSF Firewall from their official website using the following command:

```
$ wget https://download.configserver.com/csf.tgz
```

To download the latest version of CSF Firewall

- Extract the downloaded file using the following command:

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

- Change to the extracted directory:

```
$ cd csf
```

- Run the installation script:

```
$ sudo sh install.sh
```

- Verify the installation by running the following command:

```
$ sudo csf -v
```

With these steps, you have successfully installed CSF Firewall on your Ubuntu system.

Step 3: Configuring Additional Settings

CSF provides a wide range of configuration options that can be used to fine-tune the firewall according to your specific requirements. Here are some of the most commonly used settings that you can configure.

ICMP_IN

Setting ICMP_IN to 1 allows incoming ICMP requests, such as ping, to your server. If you are hosting public services, it is recommended to allow ICMP requests as they can be used to verify the availability of your services. Setting ICMP_IN to 0 blocks all incoming ICMP requests.

ICMP_IN_LIMIT

ICMP_IN_LIMIT sets the number of incoming ICMP requests that are allowed from a single IP address within a specified amount of time. The default value of 1/s is usually sufficient, but you can adjust it if necessary.

DENY_IP_LIMIT

DENY_IP_LIMIT sets the maximum number of blocked IP addresses that CSF keeps track of. It is recommended to limit the number of blocked IP addresses as having too many blocks can affect server performance.

DENY_TEMP_IP_LIMIT

DENY_TEMP_IP_LIMIT is similar to DENY_IP_LIMIT, but applies to temporary IP address blocks. It is recommended to keep this value lower than DENY_IP_LIMIT.

PACKET_FILTER

PACKET_FILTER is a powerful feature that filters out invalid, unwanted, and illegal packets before they can reach your server. Enabling this feature can improve server security by reducing the number of potential attacks.

SYNFLOOD, SYN_FLOOD_RATE and SYN_FLOOD_BURST

These settings offer protection against SYN flood attacks, which can slow down or even crash your server. Enabling these settings will slow down the initialization of every connection, so you should only enable them if you know your server is under attack.

CONNLIMIT

CONNLIMIT sets limits on the number of concurrent active connections on specific ports. For example, the value:

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

would allow up to 5 concurrent connections on port 22 and up to 20 concurrent connections on port 443. You can add more ports by separating them with commas.

PORTFLOOD

PORTFLOOD limits the number of connections per time interval that new connections can be made to specific ports. For example, the value:

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

Would block an IP address if more than 5 connections are established on port 22 using the 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 can add more ports by separating them with commas, like this:

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

Step 4: Configuring ports

To enhance the security of your VPS, it is recommended to limit the number of open ports. However, some ports must remain open to allow clients to access your services. By default, the following ports are open:

```
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"
```

These ports are used by various services such as FTP, SSH, SMTP, DNS, HTTP, and more. You may not be using all these services, so it is recommended to close any ports that are not in use. It is best to remove all port numbers from the list and then only add the ones you need.

Below are the recommended port sets to open for specific services:

For 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
```

An FTP server:

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

A mail server:

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

For a MySQL server (if remote access is required):

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

Step 5: Blocking and Allowing IP Addresses

Blocking and allowing IP addresses is one of the most basic features of a firewall. To block or allow IP addresses in CSF firewall, you can edit the configuration files `csf.deny` and `csf.allow` respectively. Additionally, you can also exclude IP addresses from firewall filters by editing `csf.ignore` file.

Blocking IP addresses

To block an IP address or range, open the `csf.deny` file using a text editor such as nano:

```
$ sudo nano /etc/csf/csf.deny
```

Each IP address or range that you want to block should be added on a new line in the file. For example, to block IP address 1.2.3.4 and IP range 2.3.0.0/16, you should add the following lines:

```
1.2.3.4
2.3.0.0/16
```

IP ranges are represented using the CIDR notation (https://en.wikipedia.org/wiki/CIDR_notation#CIDR_notation).

Allowing IP addresses

To allow an IP address or range to bypass all blocks and filters, you can add it to the `csf.allow` file. Please note that allowed IP addresses will be allowed even if they are explicitly blocked in the `csf.deny` file.

To allow an IP address or range, open the `csf.allow` file using a text editor:

```
$ sudo nano /etc/csf/csf.allow
```

Each IP address or range that you want to allow should be added on a new line in the file. For example, to allow IP address 1.2.3.4 and IP range 2.3.0.0/16, you should add the following lines:

```
1.2.3.4
2.3.0.0/16
```

Ignoring IP addresses

You can exclude IP addresses from the firewall filters by adding them to the csf.ignore file. IP addresses listed in `csf.ignore` will bypass the firewall filters and can only be blocked if listed in the `csf.deny` file.

To ignore an IP address or range, open the csf.ignore file using a text editor:

```
$ sudo nano /etc/csf/csf.ignore
```

Each IP address or range that you want to ignore should be added on a new line in the file. For example, to ignore IP address 1.2.3.4 and IP range 2.3.0.0/16, you should add the following lines:

```
1.2.3.4
2.3.0.0/16
```

Restarting CSF

After editing any of the above files, you need to restart CSF for the changes to take effect. You can restart CSF using the following command:

```
$ sudo csf -r
```

This will reload the firewall rules and apply any changes made to the configuration files.

Testing Mode

By default, CSF is in testing mode, which means it will not block any IP address permanently. Once you have verified that your settings are correct, you should change the `TESTING` setting to `0`:

```
TESTING = "0"
```

Testing Configuration

Once you have made changes to the `csf.conf` file, you can test the configuration by running the following command:

```
$ sudo csf --check
```

If there are any errors in your configuration, CSF will report them and suggest how to fix them.

Restarting CSF Firewall

Once you have made changes to the configuration, you can restart the CSF firewall by running the following command:

```
$ sudo csf -r
```

Conclusion

In this guide, we have walked through the installation and configuration of the CSF firewall on Ubuntu. By configuring the CSF firewall, you can secure your Ubuntu system and ensure that only authorized traffic is allowed through.

<< Install OpenLiteSpeed on Ubuntu and CentOS/Alma Linux (https://www.webhi.com/how-to/install-openlitespeed-on-ubuntu-and-centos-alma-linux/)
Install PostgreSQL in Ubuntu 18.04/ 20.4/ 22.04 >> (https://www.webhi.com/how-to/install-postgresql-in-ubuntu-18-04-20-4-22-04/)

LEAVE A COMMENT

Comment*

Your Name*

E-Mail

□ **Save my name, email, and website in this browser for the next time I comment.**

Submit Comment

Sections

CMS & Web development (https://www.webhi.com/how-to/tutorial/cms-web-development/)

Databases (https://www.webhi.com/how-to/tutorial/database/)

Linux system administration (https://www.webhi.com/how-to/tutorial/linux-sysadmin/)

Security (https://www.webhi.com/how-to/tutorial/cyber-security/)

SSL Certificate (https://www.webhi.com/how-to/tutorial/ssl-certificate/)

Virtualization & Cloud computing (https://www.webhi.com/how-to/tutorial/virtualization-cloud-computing/)

Web hosting Panels (https://www.webhi.com/how-to/tutorial/web-hosting-panel/)

Web servers (https://www.webhi.com/how-to/tutorial/web-server/)

Windows system administration (https://www.webhi.com/how-to/tutorial/windows-sys-admin/)

Recent tutorials

Essential Docker commands for beginners (https://www.webhi.com/how-to/most-used-docker-commands-tutorial/)

How to Install CodeIgniter on Linux (https://www.webhi.com/how-to/how-to-install-codeigniter-linux/)

How to Install Docusaurus on linux (https://www.webhi.com/how-to/how-install-docusaurus-linux/)

How to install & configure LiteSpeed web server with DirectAdmin (https://www.webhi.com/how-to/setup-configure-litespeed-web-server-directadmin/)

A Step-by-Step Guide to install cPanel DNS Only on Linux (https://www.webhi.com/how-to/tutorial-guide-installing-cpanel-dns-only-linux/)

Change language

- Français (/how-to/fr)
- English (/how-to)
- العربية (/how-to/ar)

Our products

- Web hosting (https://www.webhi.com/web-hosting-maroc)
- Dedicated Server (https://www.webhi.com/dedicated-server)
- Linux VPS (https://www.webhi.com/virtual-server-linux-vps)
- Windows VPS (https://www.webhi.com/virtual-server-windows-vps)
- Hostname dynamic DNS (https://www.webhi.com/hostname-dynamic-dns)
- Website development (https://www.webhi.com/build-website)
- Mobile app development (https://www.webhi.com/build-mobile-app)
- Domain name (https://www.webhi.com/register-domain-name)
- SSL certificate (https://www.webhi.com/cheap-ssl-certificate)
- cPanel License (https://www.webhi.com/cpanel-whm-license)

About

- About the company (https://www.webhi.com/about-us)
- Tutorials & Guides (https://www.webhi.com/how-to)
- Terms of use (https://www.webhi.com/terms-of-service)
- Contact us (https://www.webhi.com/contact.php)

Follow us

- Webhi.Technology (https://www.facebook.com/webhi
- @WebHiTechnology (https://twitter.com/WebHiTechnol