**INSTALATION OF CONFIG SERVER FIREWALL**

**Step 1:- About the firewall what it does.**

**1. 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.

**2. 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.

**3. 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.

**4. 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.

**5. 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.

**6. 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.

**7. 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).

**8. 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.

**9. IP block lists:-** This feature allows CSF to download lists of blocked IP addresses automatically from sources defined by you.

**Step 2:- Download the package.**

#wget <http://www.configserver.com/free/csf.tgz>

**Step 3:- Uncompress the package.**

#tar -xzf csf.tgz

**Step 4:- Installation.**

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

#cd csf

#chmod +x install.sh

#sh install.sh

**Step 5:- Check the iptables module.**

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

#perl /usr/local/csf/bin/[csftest.pl](http://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.

**Step 6:- Configure the firewall.**

#nano /etc/csf/csf.conf

The changes can be applied with command:

#csf -r

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.

**Step 7:- Additional Configuration.**

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.

22;5;443;20

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

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

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 8:- Reloading the firewall.**

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.

#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

**Step 9:- Blocking and Allowing ip address.**

**Blocking IP addresses**

#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](http://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

#csf -r

#>>>For Windows 7 see the below link.>>>>

<https://www.vultr.com/docs/setup-csf-on-centos-7>

###THE END.....