# Knowledge Base Documentation

***Release 1***

**Prakash Khadka**

July 25, 2015

Contents

Contents:

CHAPTER 1

# ConfigServer Firewall (CSF)

## 1.1 Installation of csf

If there is any other firewall eg: APF, cphulk,etc then first disable it. No need to disable iptables.

```
# mkdir /root/audit
# cd /root/audit
# wget http://www.configserver.com/free/csf.tgz
# tar -xzvf csf.tgz
# cd csf
# sh install.sh
```

## 1.2 whitelisting the ip

To whitelist the ip in csf, add ip in following file

```
# vi /etc/csf/csf.allow
```

**Note:** lfd can still block above whitelisted ip. Therefore, to tell lfd not to block ip, add ip in below file.

```
# vi /etc/csf/csf.ignore
```

Before doing anything to main configuration file, take a backup of it.

```
# cp /etc/csf/csf.conf /etc/csf/csf.conf_BAK
```

**Note:** After installation of csf, lfd will not start. Since csf, is in TESTING mode, we have to manually disable it. If it is not changed then you may get email like "lfd start failed". To disable TESTING mode go to /etc/csf/csf.conf and change TESTING = "1" to TESTING = "0".

**Note:** Allow 5666 port for nagios monitoring Allow 3306 port for mysql Allow 30000:50000 for ftp in passive mode (go to ftp setting, allow passive mode and restart the ftp service)

```
# vi /etc/csf/csf.conf
```

```
TCP_IN = "20,21,22,25,53,80,110,143,443,465,587,993,995,2077,2078,2082,2083,2086,2087,2095,2096,2525,
```

To change the email address where you get the notification from csf. Insert your email address in following inside /etc/csf/csf.conf file

```
LF_ALERT_TO = ""
```

If you want to change the email address from then insert some email address in following inside /etc/csf/csf.conf

```
LF_ALERT_FROM = ""
```

Change Virtual Memory Size from 200 to 300 in /etc/csf/csf.conf

```
PT_USERMEM = "300"
```

Add following process so that csf will ignore it

```
# vi /etc/csf/csf.pignore
cmd:spamd child (remove "#" sign)
exe:/usr/local/cpanel/3rdparty/php/54/bin/php-cgi (Add this somewhere in file at the end of exe:...)
```

After doing all changes you need, restart the services

```
# csf -r
# service lfd restart
```

To search for blocked-ip

```
# csf -g [ip-address]
```

To allow ip address

```
# csf -a [ip-address]
```

To block ip address

```
# csf -d [ip-address]
```

If you do not wish to get permanent block email notification then change 1 to 0 in following /etc/csf/csf.conf file

```
LF_EMAIL_ALERT = "0"
```

If you want to remove csf and lfd service:

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

## 1.3 How to enable passive mode?

1. Add Passive Port range 30000-35000 to your Pureftp or Proftp configuration file

(i) Pureftpd open `/etc/pure-ftpd.conf`, and this line

```
PassivePortRange    30000 35000
```

(ii) ProFTP Open `/etc/proftpd.conf`, and add this line

```
PassivePorts    30000 35000
```

2. Open the ports from 30000 – 35000 in your CSF firewall configuration file under TCP_IN

```
# vi /etc/csf/csf.conf
```

# Allow incoming TCP ports in /etc/csf/csf.conf file

```
TCP_IN = "20,21,22,25,53,80,110,30000:35000"
```

Then restart firewall and ftp server.

```
# csf -r
# service pureftpd restart (or)
# service proftpd restart
```

## 1.4 whitelisting the process

Whitelisting the running process

If you are receiving a number of "suspicious process" emails that mention the "spamd child" process CSF may identify it as a "suspicious process". This can be avoided by adding the exclusion back into CSF. Here's how:

Go to terminal and add binary full path ( /usr/local/cpanel/3rdparty/perl/514/bin/spamd) of the process to these two files

```
/etc/csf/csf.fignore
/etc/csf/csf.pignore
```

To allow only ip to access port 22.

remove port 22 in /etc/csf/csf.conf under TCP_IN insert following in /etc/csf/csf.allow

```
tcp|in|d=22|d=ip-address # allow port 22 to only ip-address
```

Restart csf and lfd

```
# csf -r
# service lfd restart
```

enabling the firewall

```
# csf -e
```

Disabling the firewall

```
# csf -x
```

Starting firewall / applying rules

```
# csf -s
```

Stopping firewall / flushing rules

```
# csf -f
```

## 1.5 Clustering in csf

If one of the server detects a brute force attack originating from a certain IP address, the others don't need to wait before they too are besieged. They can pass this information along to others to preempt attacks instead. The servers will be sharing white and black lists.

For us our master server will be 192.168.1.1, and slave server will be 192.168.1.2 , 192.168.1.3

All the changes will be done in `/etc/csf/csf.conf` file

In master server

```
CLUSTER_SENDTO = "192.168.1.2,192.168.1.3
CLUSTER_RECVFROM = "192.168.1.2,192.168.1.3
CLUSTER_MASTER = "192.168.1.1"
CLUSTER_PORT = "7777"
CLUSTER_KEY = "01234567890123456789012345678901234567890123456789012345"
CLUSTER_BLOCK = "1"
CLUSTER_CONFIG = "0"
```

**Note:** should be greater than 20 digit and less than 56 digit and same on all servers.

restart csf and lfd

```
#csf -r
#service lfd restart
```

In slave servers

```
CLUSTER_SENDTO = "192.168.1.1
CLUSTER_RECVFROM = "192.168.1.1
CLUSTER_CONFIG = "1"
CLUSTER_MASTER = "192.168.1.1" (optional)
```

restart csf and lfd

```
#csf -r
#service lfd restart
```

When everything is done we need to verify if clustering is working or not

In master server type following:

```
#csf --cping
```

output should be like below:

```
Sent to 192.168.1.2
Sent to 192.168.1.3
```

CHAPTER 2

# Exim CheatSheet

1. To check the number of emails present in the queue:

```
# exim -bpc
```

2. To check the emails present in the queue with the mail id and sender ID:

```
# exim -bp
# exim -bp | less
```

3. To view the header of a particular email using mail ID:

```
# exim -MvH mail_id
```

4. To view the body of a particular email using mail ID:

```
# exim -Mvb mail_id
```

5. To view a message's logs:

```
# exim -Mvl mail_id
```

6. To trace path:

```
# exim -d -bt user@domain.com
```

7. To get sorted list of email sender in exim queue:

```
# exim -bpr | grep "<" | awk {'print $4'} |cut -d "<" -f 2 | cut -d ">" -f 1 | sort -n | uniq -c| so
```

8. To check the script that will originate spam mails:

```
# grep "cwd=" /var/log/exim_mainlog|awk '{for(i=1;i<=10;i++){print $i}}'|sort| uniq -c|grep cwd|sort
```

9. If we need to find out exact spamming script. To do this, run following command:

```
# ps auxwwwe | grep user | grep --color=always "/home/user/public_html/templates/" | head
```

10. To delete the emails of a specific user:

```
# grep -lr 'user@domain.com' /var/spool/exim/input/ | sed -e 's/^.*\/\([a-zA-Z0-9-]*\)-[DH]$/\1/g' |
# exim -bp | grep "user_email-account" | awk '{print $3}' | xargs exim -Mrm
```

11. To delete Frozen emails from the email queue:

```
# grep -R -l '*** Frozen' /var/spool/exim/msglog/*|cut -b26-|xargs exim -Mrm
# exim -bp| grep frozen | awk '{print $3}'| xargs exim -Mrm
# exiqgrep -z -i | xargs exim -Mrm
```

12. To delete Spam emails from the email queue:

```
# grep -R -l [SPAM] /var/spool/exim/msglog/*|cut -b26-|xargs exim -Mrm
```

13. To check the no. of frozen mails:

```
# exiqgrep -z -c
```

14. To check exim logs:

```
# tail -f /var/log/exim_mainlog
```

15. Force delivery of one message:

```
# exim -M mail_id
```

16. Force another queue run:

```
# exim -qf
```

17. Force another queue run and attempt to flush frozen messages:

```
# exim -qff
```

18. To check if there are frozen emails:

```
# exim -bp |awk '/fr[o]zen/ {print}'
```

19. To clear just one email:

```
# exim -Mrm mail_id
```

20. Check the subjects of the emails:

```
# exiqgrep -i |awk '{ print "exim -Mvh "$1 }' |sh |grep -i Subject
```

21. Delete the email which content some string in the message body

```
# grep -lr 'photos to album' /var/spool/exim/input/ | sed -e 's/^.*\/\([a-zA-Z0-9-]*\)-[DH]$/\1/g' |
```

CHAPTER 3

# Git commands

## 3.1 Connect github using ssh key pair

Generate ssh key pair

```
$ ssh-keygen -t rsa -b 4096 -C "your_email@example.com"
```

Follow the steps, we suggest you to leave all the setting to defaults. When passphrase is asked enter one which is very good and secure.

Go to your home directory where keys have been generated with name `id_rsa` and `id_rsa.pub`

Copy you public key `id_rsa.pub`

## 3.2 Add the copied key to Github

In top right corner of ny page, click your profile photo, then click **Setting**

In the user setting sidebar, click **SSH Keys**

Click **Add SSH Key**

In title field, add a descriptive label for new key.

Paste your key intot the `Key` field

Click **Add key**

Confirm the action by entering your Github password.

## 3.3 Test the connection

Open Terminal (Ctrl + alt + T)

```
$ ssh -T git@github.com
```

If successful you will see message as below

```
Hi username! You've successfully authenticated, but GitHub does not
```

provide shell access.

In local do following

```
$ ssh-add ~/.ssh/id_rsa
```

## 3.4 Configuring PC to work locally

In your PC, configure username and email with following command

```
$ git config --global user.name "YOUR NAME"
$ git config --global user.email "YOUR EMAIL ADDRESS"
```

Make a directory in which you will work and initialized git

```
$ mkdir ~/docs
$ cd ~/docs
$ git init
```

### 3.4.1 Add remote

```
$ git remote add origin git@github.com:user/repo.git
```

### 3.4.2 Renaming remote

```
$ git remote -v
$ git remote rename origin destination
$ git remote -v
```

### 3.4.3 Deleting existing remote

```
$ git remote -v
$ git remove rm origin
$ git remote -v
```

### 3.4.4 Remove directory from git and local

```
$ git rm -r one-of-the-directories
$ git commit -m "Remove duplicated directory"
$ git push origin master
```

Above will remove folder from remote repository but not local

CHAPTER 4

# How to install ioncube for WHMCS

```
$ cd
$ mkdir audit
$ cd audit
```

Download the latest ioncube loader from Here

```
$ sudo wget http://downloads3.ioncube.com/loader_downloads/ioncube_loaders_lin_x86-64.tar.gz
```

Extract it

```
$ tar -xzvf ioncube_loaders_lin_x86-64.tar.gz
```

Copy the loader-wizard.php to /var/www/html

```
$ sudo cp ioncube/loader-wizard.php /var/www/html/
```

Copy ioncube module according to your php version$ to /usr/lib64/php/modules

```
$ sudo cp ioncube_loader_lin_5.6.so /usr/lib64/php/modules
```

Make a file inside /etc/php.d/ioncube.ini and paste below :

```
zend_extension = /usr/lib64/php/modules/ioncube_loader_lin_5.6.so
```

Now restart the httpd

```
$ sudo service httpd restart
```

Then, remove these files

```
$ sudo rm /var/www/html/loader-wizard.php
$ sudo rm -rf audit/ioncube*
```

## 4.1 TroubleShooting

### 4.1.1 Error 1

**Warning:** Site error: the file /var/www/html/whmcs/install/install.php requires the ionCube PHP Loader ioncube_loader_lin_5.6.so to be installed by the site administrator.

If you get errors like above, look at error_log, for me above error tells me the error wwas related to permission denied. If you have same error in err-r_log then give the proper permission to module or easy way out is move .so file elsewhere like below:

```
$ cd /usr/share
$ mkdir ioncube
$ mv /usr/lib64/php/modules/ioncube_loader_lin_5.6.so /usr/share/ioncube
```

Also make changes in /etc/php.ini file

```
zend_extension = /usr/share/ioncube/ioncube_loader_lin_5.6.so
```

restart the apache

```
$ sudo /etc/init.d/httpd restart
```

### 4.1.2 Error 2

**Warning:** # php -v PHP Fatal error: [ionCube Loader] The Loader must appear as the first entry in the php.ini file in Unknown on line 0

then it may be because there are two two defination for same module. Try to find the `.ini` file and inside it search for `zend_extension`

If you find two entries, then remove one and restart apache

CHAPTER 5

# Installation of LAMP on centos 6.6

## 5.1 Install wget

```
$ sudo yum install wget
```

## 5.2 Install Apache

To install apache,

```
$ sudo yum install httpd
```

Once it installs, you can start apache running on your VPS:

```
$ sudo service httpd start
$ sudo chkconfig httpd on
```

Edit the `#ServerName www.example.com:80` and put your hostname instead of `www.example.com` in `httpd.conf` file

```
$ sudo vi /etc/httpd/conf/httpd.conf
```

## 5.3 Install MySQL 5.6

Download the yum repo rpm package.

```
$ wget http://repo.mysql.com/mysql-community-release-el6-5.noarch.rpm
```

Install the downloaded rpm package.

```
$ rpm -ivh mysql-community-release-el6-5.noarch.rpm
```

Install the mysql server

```
$ yum install mysql-server
```

After installation start the mysql server

```
$ /etc/init.d/mysqld start
$ sudo chkconfig mysqld on
```

MySQL server is just installed it has blank mysql root password. To reset the mysql root password.

```
$ sudo mysql_secure_installation
```

## 5.4 Install PHP 5.6

Download the repo rpm package

```
$ sudo rpm -Uvh https://mirror.webtatic.com/yum/el6/latest.rpm
```

Install the php with the required extension

```
$ sudo yum install -y php56w php56w-opcache php56w-xml php56w-mcrypt php56w-gd php56w-devel php56w-my
```

Restart Apache:

```
$ sudo service httpd restart
```

To verify that PHP 5.6 is installed:

```
$ php -v
```

For testing php test page

```
$ sudo vi /var/www/html/info.php
```

Add in the following line:

```
<?php
 phpinfo();
?>
```

Then save it and restart apache.

```
$ sudo service httpd restart
```

## 5.5 PHP Modules

PHP also has a variety of useful libraries and modules that you can add onto your server. You can see the libraries that are available by typing:

```
$ sudo yum search php-
```

To see more details about what each module does, type the following command into terminal, replacing the name of the module with whatever library you want to learn about.

```
$ sudo yum info name of the module
```

Once you decide to install the module, type:

```
$ sudo yum install name of the module
```

You can install multiple libraries at once by separating the name of each module with a space.

Now LAMP stack is installed!

Allow port 80

```
$ sudo vi /etc/sysconfig/iptables
```

and add this line

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
```

Visit site at : *http://ip-address*

CHAPTER 6

# Postfix CheatSheet

count mail queue number

```
# mailq | grep -c "^[A-Z0-9]"
```

delete mailq from domain address

```
# postqueue -p | tail -n +2 | awk 'BEGIN { RS = "" } /@domain\.com/ { print $1 }' | tr -d '*!' | post
```

To delete all email in the queue From: a specific email address run this command as root:

```
# postqueue -p | tail -n +2 | awk 'BEGIN { RS = "" } /username@domain\.com/ { print $1 }' | tr -d '*
```

Use following perl script to delete depending upon username or domain name:

```
#!/usr/bin/perl

$REGEXP = shift || die "no email-adress given (regexp-style, e.g. bl.*\@yahoo.com)!";

@data = qx</usr/sbin/postqueue -p>;
for (@data) {
  if (/^(\w+)(\*|\!)?\s/) {
     $queue_id = $1;
  }
  if($queue_id) {
    if (/$REGEXP/i) {
      $Q{$queue_id} = 1;
      $queue_id = "";
    }
  }
}

#open(POSTSUPER,"|cat") || die "couldn't open postsuper" ;
open(POSTSUPER,"|postsuper -d -") || die "couldn't open postsuper" ;

foreach (keys %Q) {
  print POSTSUPER "$_\n";
};
close(POSTSUPER);
```

Usage:

```
./scriptname.pl username
./scriptname.pl domainname
```

CHAPTER 7

# Python

## 7.1 Scan cryptoPHP in centos server

Following script will search cryptoPHP infected themes/plugins based on *social.png* file.

**Note:** To run this script you need to first run *updatedb* command.

```
#!/usr/bin/env python

import os

os.system("mkdir -p /root/audit/cryptoPHP/")
os.system("locate social.png > /root/audit/cryptoPHP/list.txt")
os.system("xargs md5sum < /root/audit/cryptoPHP/list.txt > /root/audit/cryptoPHP/possible-infected.tx

CRYPTOPHP_MD5SUM = ['048a54b0f740991a763c040f7dd67d2b', 'd3c9f64b8d1675f02aa833d83a5c6342', '3a2ca46e

newfile = open("cryptoPHP-infected.txt", "w")

with open('possible-infected.txt') as possible:
        for line in possible:
                if any(crypto in line for crypto in CRYPTOPHP_MD5SUM):
                        newfile.write(line)
```

CHAPTER 8

# How to install Redis in Centos:

```
# yum install gcc make
# yum -y install tcl

# cd /opt
# useradd redis
# passwd redis
```

1. Download latest from here

```
# wget http://download.redis.io/releases/redis-3.0.2.tar.gz
```

2. To verify sha1sum go here

```
# sha1sum redis-3.0.2.tar.gz   (compare the output value to above given link redis version)
```

3. Extract the tar file

```
# tar -xzvf redis-3.0.2.tar.gz
# mv redis-3.0.2 redis
# cd redis
# make
 or
# make install
```

make : will create src folder with different executables make install : will install the redis in `/usr/local/bin`

make install command will create following executables will be available in `/usr/local/bin/` redis-benchmark redis-check-aof redis-check-dump redis-cli redis-sentinel redis-server

```
# make test
```

4. Copy redis.conf file to /etc directory now run

```
# cd src
# ./redis-server ../redis.conf
# ctrl + C
```

Make script to run it

```
# mkdir /scripts
# cd scripts
# vi start-redis
```

Add following

```
nohup runuser -l redis -c "/opt/redis/src/redis-server /opt/redis/redis.conf" > /tmp/redis.log &
```

go to `/opt/redis/redis.conf`

uncomment requirepass and add long pass

```
requirepass asmdgjsagdjkasgdkasgdkjasdgkasd
```

save it

start the script

```
# /scripts/start-redis
# redis-cli

> AUTH asmdgjsagdjkasgdkasgdkjasdgkasd
OK
>ping
PONG
>exit
```

CHAPTER 9

# Indices and tables

- genindex
- modindex
- search