How to setup and configure CSF/LFD

Please follow the below steps to install CSF / LFD

Login to your server with 'root' user and issue below commands :

Change directory to either /root or /usr/local/src , which ever you normally use for such installations
cd /usr/local/src

Remove any old source that might be present
rm -fv csf.tgz

Download the source for installation
wget https://download.configserver.com/csf.tgz

unzip/untar the source
tar -xzf csf.tgz

Running installation script
cd csf
sh install.sh

Once the installation complete, you can run the below scripts provided by vendor to check if your server/vps has required iptables modules available :

perl /etc/csf/csftest.pl

CSF provides the script to remove the other popular combination I talked about above i.e. apf/bfd :

sh /etc/csf/remove_apf_bfd.sh

The above script will remove apf/bfd from your server/vps.

---------- Common Setting ----------
Conffig file: /etc/csf/csf.conf

ETH_DEVICE = "eth1"

ETH_DEVICE_SKIP = "eth0"

Allow incoming TCP ports

TCP_IN = "20,21,25,53,80,106,110,111,143,443,465,587,865,873,993,995,5224,8443,8880"

# Allow outgoing TCP ports
TCP_OUT = "20,21,22,25,80,110,443,43,873,5224,8443"

# Allow incoming UDP ports
UDP_IN = "53,111,123,230,631,859,862,2109,5353"

# Allow outgoing UDP ports
# To allow outgoing traceroute add 33434:33523 to this list
UDP_OUT = "20,21,53,113,123,2109"

 # traceroute send operation not permitted for remote server

For allow outgoing traceroute add 33434:33523 **(outgoing UDP ports)**

Also we have to open port - 161 in the CSF firewall

# Allow incoming PING
ICMP_IN = "1"

# Set the per IP address incoming ICMP packet rate
# To disable rate limiting set to "0"
ICMP_IN_RATE = "0"

# Allow outgoing PING
ICMP_OUT = "1"

# Set the per IP address outgoing ICMP packet rate
# To disable rate limiting set to "0"
ICMP_OUT_RATE = "0"

---------- Enable SMTP BLOCK ----------

SMTP_BLOCK = "1"
SMTP_ALLOWLOCAL = "1"
SMTP_PORTS = "25,587"

---------- Allowing Qmail ----------

SMTP_ALLOWUSER = "qmaild,qmaill,qmailp,qmailq,qmailr,qmails"
SMTP_ALLOWGROUP = "qmail,nofiles,mail,mailman"

---------- Allowing Postfix ----------

SMTP_ALLOWUSER = "postfix"

SMTP_ALLOWGROUP = "postfix,postdrop,mail,mailman"

Set LFD reporting FROM/TO ID as below [**** Need to set for Plesk]

LF_ALERT_TO = "supportteam@diadem.co.in"

LF_ALERT_FROM = "csf_LFD@diadem.co.in"

---------- Allowing Thirdparty Block list ----------

# Enable IP range blocking using the DShield Block List at
LF_DSHIELD = "86400"

# Enable IP range blocking using the Spamhaus DROP List at
LF_SPAMHAUS = "86400"

# Enable IP range blocking using the BOGON List at
LF_BOGON = "86400"

Now Add the LFD ignore list for qmail/plesk mail user/process in csf.pignore file.

vim /etc/csf/csf.pignore

Custom for Plesk
user:admin
exe:/usr/sbin/clamd
cmd:clamd
user:qscand
exe:/usr/sbin/avahi-daemon
user:avahi
exe:/usr/local/sbin/zabbix_agentd
cmd:/usr/local/sbin/zabbix_agentd
user:zabbix
exe:/usr/bin/sw-engine-cgi
cmd:/usr/bin/sw-engine-cgi
user:sso
exe:/usr/sbin/sw-cp-serverd
cmd:/usr/sbin/sw-cp-serverd -f /etc/sw-cp-server/config
user:sw-cp-server
exe:/usr/bin/sw-engine-cgi
cmd:/usr/bin/sw-engine-cgi -c /usr/local/psa/admin/conf/php.ini -d

auto_prepend_file=auth.php3 -u psaadm
user:psaadm
exe:/usr/libexec/mysqld
cmd:/usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --socket=/var/lib/mysql/mysql.sock
user:mysql
exe:/usr/libexec/hald-addon-acpi
exe:/usr/sbin/hald
cmd:hald
user:haldaemon
exe:/usr/bin/postgres
user:postgres
exe:/sbin/portmap
cmd:portmap
user:rpc
exe:/usr/bin/xfs
cmd:xfs -droppriv -daemon
user:xfs
exe:/usr/bin/python
cmd:/usr/bin/python /usr/lib/mailman/bin/qrunner --runner=VirginRunner:0:1 -s
user:mailman
exe:/usr/java/jdk1.6.0_20/bin/java
user:tomcat
For courier-imap common for qmail and postfix
exe:/usr/bin/imapd
exe:/usr/bin/pop3d
user:popuser

For Qmail
exe:/var/qmail/bin/qmail-smtpd
exe:/var/qmail/bin/qmail-queue
exe:/var/qmail/bin/qmail-send
exe:/var/qmail/bin/qmail-rspawn
exe:/var/qmail/bin/qmail-clean
exe:/var/qmail/bin/splogger
exe:/var/qmail/bin/qmail-remote.moved
cmd:qmail-send
cmd:/usr/bin/pop3d Maildir
cmd:/var/qmail/bin/qmail-queue
cmd:/var/qmail/bin/qmail-smtpd /var/qmail/bin/smtp_auth /var/qmail/bin/true /var/qmail/bin/cmd5checkpw /var/qmail/bin/true
cmd:/usr/bin/imapd Maildir

cmd:qmail-rspawn
cmd:qmail-clean
cmd:splogger qmail
user:qmaill
user:qmaild
user:qmails
user:qmailr
user:qmailq

For postfix
exe:/usr/lib/plesk-9.0/postfix-queue
cmd:/usr/lib/plesk-9.0/postfix-queue 127.0.0.1 10027 before-queue
cmd:/usr/lib/plesk-9.0/postfix-queue 127.0.0.1 10026 before-remote
user:mhandlers-user
exe:/usr/sbin/uuidd
cmd:/usr/sbin/uuidd
user:uuidd

Note: You may need to add few more process/user as per your requirement.

Now start the CSF

csf -s

Restart LFD

service lfd restart

Disable TESTING mode

vim /etc/csf/csf.conf

And set the

TESTING = "0"

Restart CSF/LFD

csf -r

service lfd restart

Installation is done, now check the site amd mail usages.

Note: If you are replacing your current firewall system (e.g. apf) then you need to backup the incoming/outgoing TCP/UDP port and allow/deny IP list from old firewall system and restore IP/PORT setting from old firewall system.

I will list below some of very common commands you will need to use/manage csf firewall :

Enabling the firewall

csf –enable OR

csf -e

Disabling the firewall

csf –disable

csf -x

Starting firewall / applying rules

csf –start

csf -s

- stopping firewall / flushing rules

csf –stop

csf -f

Adding an IP in firewall

csf -d 2.3.4.5 "Reason for blocking the IP"

csf –deny 2.3.4.5 "Reason for blocking the IP"

where 2.3.4.5 is the IP you want to block.

Removing IP from deny list

csf -dr 2.3.4.5

Article ID: 97
Last updated: 18 Aug, 2016
Linux Server Management -> How to setup and configure CSF/LFD
http://kb.diadem.co.in/entry/97/