Berkas Konfigurasi Config Server firewall

csf.conf

```
###############################################################################
########
# SECTION:Initial Settings
###############################################################################
########
# Testing flag - enables a CRON job that clears iptables incase of
# configuration problems when you start csf. This should be enabled
until you
# are sure that the firewall works - i.e. incase you get locked out of
your
# server! Then do remember to set it to 0 and restart csf when you're
sure
# everything is OK. Stopping csf will remove the line from /etc/crontab
#
# lfd will not start while this is enabled
TESTING = "0"

# The interval for the crontab in minutes. Since this uses the system
clock the
# CRON job will run at the interval past the hour and not from when you
issue
# the start command. Therefore an interval of 5 minutes means the
firewall
# will be cleared in 0-5 minutes from the firewall start
TESTING_INTERVAL = "5"

# SECURITY WARNING
# ================
#
# Unfortunately, syslog and rsyslog allow end-users to log messages to
some
# system logs via the same unix socket that other local services use.
This
# means that any log line shown in these system logs that syslog or
rsyslog
# maintain can be spoofed (they are exactly the same as real log
lines).
#
# Since some of the features of lfd rely on such log lines, spoofed
messages
# can cause false-positive matches which can lead to confusion at best,
or
# blocking of any innocent IP address or making the server inaccessible
at
# worst.
```

```
#
# Any option that relies on the log entries in the files listed in
# /etc/syslog.conf and /etc/rsyslog.conf should therefore be considered
# vulnerable to exploitation by end-users and scripts run by end-users.
#
# NOTE: Not all log files are affected as they may not use
syslog/rsyslog
#
# The option RESTRICT_SYSLOG disables all these features that rely on
affected
# logs. These options are:
# LF_SSHD LF_FTPD LF_IMAPD LF_POP3D LF_BIND LF_SUHOSIN
LF_SSH_EMAIL_ALERT
# LF_SU_EMAIL_ALERT LF_CONSOLE_EMAIL_ALERT LF_DISTATTACK LF_DISTFTP
# LT_POP3D LT_IMAPD PS_INTERVAL UID_INTERVAL WEBMIN_LOG
LF_WEBMIN_EMAIL_ALERT
# PORTKNOCKING_ALERT
#
# This list of options use the logs but are not disabled by
RESTRICT_SYSLOG:
# ST_ENABLE SYSLOG_CHECK LOGSCANNER CUSTOM*_LOG
#
# The following options are still enabled by default on new
installations so
# that, on balance, csf/lfd still provides expected levels of security:
# LF_SSHD LF_FTPD LF_POP3D LF_IMAPD LF_SSH_EMAIL_ALERT
LF_SU_EMAIL_ALERT
#
# If you set RESTRICT_SYSLOG to "0" or "2" and enable any of the
options listed
# above, it should be done with the knowledge that any of the those
options
# that are enabled could be triggered by spoofed log lines and lead to
the
# server being inaccessible in the worst case. If you do not want to
take that
# risk you should set RESTRICT_SYSLOG to "1" and those features will
not work
# but you will not be protected from the exploits that they normally
help block
#
# The recommended setting for RESTRICT_SYSLOG is "3" to restrict who
can access
# the syslog/rsyslog unix socket.
#
# For further advice on how to help mitigate these issues, see
# /etc/csf/readme.txt
#
# 0 = Allow those options listed above to be used and configured
# 1 = Disable all the options listed above and prevent them from being
used
```

```
# 2 = Disable only alerts about this feature and do nothing else
# 3 = Restrict syslog/rsyslog access to RESTRICT_SYSLOG_GROUP **
RECOMMENDED **
RESTRICT_SYSLOG = "1"

# The following setting is used if RESTRICT_SYSLOG is set to 3. It
restricts
# write access to the syslog/rsyslog unix socket(s). The group must not
already
# exists in /etc/group before setting RESTRICT_SYSLOG to 3, so set the
option
# to a unique name for the server
#
# You can add users to this group by changing /etc/csf/csf.syslogusers
and then
# restarting lfd afterwards. This will create the system group and add
the
# users from csf.syslogusers if they exist to that group and will
change the
# permissions on the syslog/rsyslog unix socket(s). The socket(s) will
be
# monitored and the permissions re-applied should syslog/rsyslog be
restarted
#
# Using this option will prevent some legitimate logging, e.g. end-user
cron
# job logs
#
# If you want to revert RESTRICT_SYSLOG to another option and disable
this
# feature, change the setting of RESTRICT_SYSLOG and then restart lfd
and then
# syslog/rsyslog and the unix sockets will be reset
RESTRICT_SYSLOG_GROUP = "mysyslog"

# This options restricts the ability to modify settings within this
file from
# the csf UI. Should the parent control panel be compromised, these
restricted
# options could be used to further compromise the server. For this
reason we
# recommend leaving this option set to at least "1" and if any of the
# restricted items need to be changed, they are done so from the root
shell
#
# 0 = Unrestricted UI
# 1 = Restricted UI
# 2 = Disabled UI
RESTRICT_UI = "1"

# Enabling auto updates creates a cron job called
```

```
/etc/cron.d/csf_update which
# runs once per day to see if there is an update to csf+lfd and
upgrades if
# available and restarts csf and lfd
#
# You should check for new version announcements at
http://blog.configserver.com
AUTO_UPDATES = "1"

###############################################################################
########
# SECTION:IPv4 Port Settings
###############################################################################
########
# Lists of ports in the following comma separated lists can be added
using a
# colon (e.g. 30000:35000).

# Some kernel/iptables setups do not perform stateful connection
tracking
# correctly (typically some virtual servers or custom compiled
kernels), so a
# SPI firewall will not function correctly. If this happens, LF_SPI can
be set
# to 0 to reconfigure csf as a static firewall.
#
# As connection tracking will not be configured, applications that rely
on it
# will not function unless all outgoing ports are opened. Therefore,
all
# outgoing connections will be allowed once all other tests have
completed. So
# TCP_OUT, UDP_OUT and ICMP_OUT will not have any affect.
#
# If you allow incoming DNS lookups you may need to use the following
# directive in the options{} section of your named.conf:
#
#       query-source port 53;
#
# This will force incoming DNS traffic only through port 53
#
# Disabling this option will break firewall functionality that relies
on
# stateful packet inspection (e.g. DNAT, PACKET_FILTER) and makes the
firewall
# less secure
#
# This option should be set to "1" in all other circumstances
LF_SPI = "1"

# Allow incoming TCP ports
```

```
TCP_IN = "20,21,25,53,80,443,465,212,5758"

# Allow outgoing TCP ports
TCP_OUT = "20,21,212,25,53,80,113,443,5758"

# Allow incoming UDP ports
UDP_IN = "20,21,53,5758"

# Allow outgoing UDP ports
# To allow outgoing traceroute add 33434:33523 to this list
UDP_OUT = "20,21,53,113,123,5758"

# 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 = "1/s"

# Allow outgoing PING
ICMP_OUT = "1"

# Set the per IP address outgoing ICMP packet rate (hits per second
allowed),
# e.g. "1/s"
# To disable rate limiting set to "0"
ICMP_OUT_RATE = "0"

##############################################################################
########
# SECTION:IPv6 Port Settings
##############################################################################
########
# IPv6: (Requires ip6tables)
#
# Pre v2.6.20 kernels do not perform stateful connection tracking, so a
static
# firewall is configured as a fallback instead if IPV6_SPI is set to 0
below
#
# Supported:
# Temporary ACCEPT/DENY, GLOBAL_DENY, GLOBAL_ALLOW, SMTP_BLOCK,
LF_PERMBLOCK,
# PACKET_FILTER, WATCH_MODE, Advanced Allow/Deny Filters, RELAY_*,
CLUSTER_*,
# CC6_LOOKUPS, SYNFLOOD, LF_NETBLOCK
#
# Supported if CC6_LOOKUPS and CC_LOOKUPS are enabled
# CC_DENY, CC_ALLOW, CC_ALLOW_FILTER, CC_IGNORE, CC_ALLOW_PORTS,
CC_DENY_PORTS,
# CC_ALLOW_SMTPAUTH
```

```
#
# Supported if ip6tables >= 1.4.3:
# PORTFLOOD, CONNLIMIT
#
# Supported if ip6tables >= 1.4.17 and perl module IO::Socket::INET6 is
# installed:
# MESSENGER
#
# Not supported:
# ICMP_IN, ICMP_OUT
#
IPV6 = "0"

# IPv6 uses icmpv6 packets very heavily. By default, csf will allow all
icmpv6
# traffic in the INPUT and OUTPUT chains. However, this could increase
the risk
# of icmpv6 attacks. To restrict incoming icmpv6, set to "1" but may
break some
# connection types
IPV6_ICMP_STRICT = "0"

# Pre v2.6.20 kernel must set this option to "0" as no working state
module is
# present, so a static firewall is configured as a fallback
#
# A workaround has been added for CentOS/RedHat v5 and custom kernels
that do
# not support IPv6 connection tracking by opening ephemeral port range
# 32768:61000. This is only applied if IPV6_SPI is not enabled. This is
the
# same workaround implemented by RedHat in the sample default IPv6
rules
#
# As connection tracking will not be configured, applications that rely
on it
# will not function unless all outgoing ports are opened. Therefore,
all
# outgoing connections will be allowed once all other tests have
completed. So
# TCP_OUT, UDP_OUT and ICMP_OUT will not have any affect.
#
# If you allow incoming ipv6 DNS lookups you may need to use the
following
# directive in the options{} section of your named.conf:
#
#       query-source-v6 port 53;
#
# This will force ipv6 incoming DNS traffic only through port 53
#
# These changes are not necessary if the SPI firewall is used
```

```
IPV6_SPI = "1"

# Allow incoming IPv6 TCP ports
TCP6_IN = "20,21,22,25,53,80,110,143,443,465,587,993,995,212"

# Allow outgoing TCP ports
TCP6_OUT = "20,21,22,25,53,80,110,113,443,587,993,995"

# Allow incoming UDP ports
UDP6_IN = "20,21,53"

# Allow outgoing UDP ports
# To allow outgoing traceroute add 33434:33523 to this list
UDP6_OUT = "20,21,53,113,123"

##############################################################################
########
# SECTION:General Settings
##############################################################################
########
# By default, csf will auto-configure iptables to filter all traffic
except on
# the loopback device. If you only want iptables rules applied to a
specific
# NIC, then list it here (e.g. eth1, or eth+)
ETH_DEVICE = ""

# By adding a device to this option, ip6tables can be configured only
on the
# specified device. Otherwise, ETH_DEVICE and then the default setting
will be
# used
ETH6_DEVICE = ""

# If you don't want iptables rules applied to specific NICs, then list
them in
# a comma separated list (e.g "eth1,eth2")
ETH_DEVICE_SKIP = ""

# To switch from the deprecated iptables "state" module to the
"conntrack"
# module, change this to 1
USE_CONNTRACK = "1"

# Check whether syslog is running. Many of the lfd checks require
syslog to be
# running correctly. This test will send a coded message to syslog
every
# SYSLOG_CHECK seconds. lfd will check SYSLOG_LOG log lines for the
coded
# message. If it fails to do so within SYSLOG_CHECK seconds an alert
```

```
using
# syslogalert.txt is sent
#
# A value of betwen 300 and 3600 seconds is suggested. Set to 0 to
disable
SYSLOG_CHECK = "0"

# Enable this option if you want lfd to ignore (i.e. don't block) IP
addresses
# listed in csf.allow in addition to csf.ignore (the default). This
option
# should be used with caution as it would mean that IP's allowed
through the
# firewall from infected PC's could launch attacks on the server that
lfd
# would ignore
IGNORE_ALLOW = "0"

# Enable the following option if you want to apply strict iptables
rules to DNS
# traffic (i.e. relying on iptables connection tracking). Enabling this
option
# could cause DNS resolution issues both to and from the server but
could help
# prevent abuse of the local DNS server
DNS_STRICT = "0"

# Enable the following option if you want to apply strict iptables
rules to DNS
# traffic between the server and the nameservers listed in
/etc/resolv.conf
# Enabling this option could cause DNS resolution issues both to and
from the
# server but could help prevent abuse of the local DNS server
DNS_STRICT_NS = "0"

# Limit the number of IP's kept in the /etc/csf/csf.deny file
#
# Care should be taken when increasing this value on servers with low
memory
# resources or hard limits (such as Virtuozzo/OpenVZ) as too many rules
(in the
# thousands) can sometimes cause network slowdown
#
# The value set here is the maximum number of IPs/CIDRs allowed
# if the limit is reached, the entries will be rotated so that the
oldest
# entries (i.e. the ones at the top) will be removed and the latest is
added.
# The limit is only checked when using csf -d (which is what lfd also
uses)
```

```
# Set to 0 to disable limiting
#
# For implementations wishing to set this value significantly higher,
we
# recommend using the IPSET option
DENY_IP_LIMIT = "200"

# Limit the number of IP's kept in the temprary IP ban list. If the
limit is
# reached the oldest IP's in the ban list will be removed and allowed
# regardless of the amount of time remaining for the block
# Set to 0 to disable limiting
DENY_TEMP_IP_LIMIT = "100"

# Enable login failure detection daemon (lfd). If set to 0 none of the
# following settings will have any effect as the daemon won't start.
LF_DAEMON = "1"

# Check whether csf appears to have been stopped and restart if
necessary,
# unless TESTING is enabled above. The check is done every 300 seconds
LF_CSF = "1"

# This option uses IPTABLES_SAVE, IPTABLES_RESTORE and IP6TABLES_SAVE,
# IP6TABLES_RESTORE in two ways:
#
# 1. On a clean server reboot the entire csf iptables configuration is
saved
#    and then restored where possible to provide a near instant
firewall
#    startup[*]
#
# 2. On csf restart or lfd reloading tables, CC_* as well as SPAMHAUS,
DSHIELD,
#    BOGON, TOR are loaded using this method in a fraction of the time
than if
#    this setting is disabled
#
# [*]Not supported on all OS platforms
#
# Set to "0" to disable this functionality
FASTSTART = "1"

# This option allows you to use ipset v6+ for the following csf
options:
# CC_* and /etc/csf/csf.blocklist, /etc/csf/csf.allow,
/etc/csf/csf.deny,
# GLOBAL_DENY, GLOBAL_ALLOW, DYNDNS, GLOBAL_DYNDNS, MESSENGER
#
# ipset will only be used with the above options when listing IPs and
CIDRs.
```

```
# Advanced Allow Filters and temporary blocks use traditional iptables
#
# Using ipset moves the onus of ip matching against large lists away
from
# iptables rules and to a purpose built and optimised database matching
# utility. It also simplifies the switching in of updated lists
#
# To use this option you must have a fully functioning installation of
ipset
# installed either via rpm or source from http://ipset.netfilter.org/
#
# Note: Using ipset has many advantages, some disadvantages are that
you will
# no longer see packet and byte counts against IPs and it makes
identifying
# blocked/allowed IPs that little bit harder
#
# Note: If you mainly use IP address only entries in csf.deny, you can
increase
# the value of DENY_IP_LIMIT significantly if you wish
#
# Note: It's highly unlikely that ipset will function on
Virtuozzo/OpenVZ
# containers even if it has been installed
#
# If you find any problems, please post on forums.configserver.com with
full
# details of the issue
LF_IPSET = "0"

# The following sets the hashsize for ipset sets, which must be a power
of 2.
#
# Note: Increasing this value will consume more memory for all sets
# Default: "1024"
LF_IPSET_HASHSIZE = "1024"

# The following sets the maxelem for ipset sets.
#
# Note: Increasing this value will consume more memory for all sets
# Default: "65536"
LF_IPSET_MAXELEM = "65536"

# If you enable this option then whenever a CLI request to restart csf
is used
# lfd will restart csf instead within LF_PARSE seconds
#
# This feature can be helpful for restarting configurations that cannot
use
# FASTSTART
LFDSTART = "0"
```

```
# Enable verbose output of iptables commands
VERBOSE = "1"

# Drop out of order packets and packets in an INVALID state in iptables
# connection tracking
PACKET_FILTER = "1"

# Perform reverse DNS lookups on IP addresses. (See also CC_LOOKUPS)
LF_LOOKUPS = "1"

##############################################################################
########
# SECTION:SMTP Settings
##############################################################################
########
# Block outgoing SMTP except for root, exim and mailman (forces
scripts/users
# to use the exim/sendmail binary instead of sockets access). This
replaces the
# protection as WHM > Tweak Settings > SMTP Tweaks
#
# This option uses the iptables ipt_owner/xt_owner module and must be
loaded
# for it to work. It may not be available on some VPS platforms
#
# Note: Run /etc/csf/csftest.pl to check whether this option will
function on
# this server
SMTP_BLOCK = "0"

# If SMTP_BLOCK is enabled but you want to allow local connections to
port 25
# on the server (e.g. for webmail or web scripts) then enable this
option to
# allow outgoing SMTP connections to the loopback device
SMTP_ALLOWLOCAL = "1"

# This option redirects outgoing SMTP connections destined for remote
servers
# for non-bypass users to the local SMTP server to force local relaying
of
# email. Such email may require authentication (SMTP AUTH)
SMTP_REDIRECT = "0"

# This is a comma separated list of the ports to block. You should list
all
# ports that exim is configured to listen on
SMTP_PORTS = "25,465,587"

# Always allow the following comma separated users and groups to bypass
```

```
# SMTP_BLOCK
#
# Note: root (UID:0) is always allowed
SMTP_ALLOWUSER = ""
SMTP_ALLOWGROUP = "mail,mailman"

# This option will only allow SMTP AUTH to be advertised to the IP
addresses
# listed in /etc/csf/csf.smtpauth on EXIM mail servers
#
# The additional option CC_ALLOW_SMTPAUTH can be used with this option
to
# additionally restrict access to specific countries
#
# This is to help limit attempts at distributed attacks against SMTP
AUTH which
# are difficult to achive since port 25 needs to be open to relay email
#
# The reason why this works is that if EXIM does not advertise SMTP
AUTH on a
# connection, then SMTP AUTH will not accept logins, defeating the
attacks
# without restricting mail relaying
#
# Note: csf and lfd must be restarted if /etc/csf/csf.smtpauth is
modified so
# that the lookup file in /etc/exim.smtpauth is regenerated from the
# information from /etc/csf/csf.smtpauth plus any countries listed in
# CC_ALLOW_SMTPAUTH
#
# NOTE: To make this option work you MUST make the modifications to
exim.conf
# as explained in "Exim SMTP AUTH Restriction" section in
/etc/csf/readme.txt
# after enabling the option here, otherwise this option will not work
#
# To enable this option, set to 1 and make the exim configuration
changes
# To disable this option, set to 0 and undo the exim configuration
changes
SMTPAUTH_RESTRICT = "0"

##############################################################################
########
# SECTION:Port Flood Settings
##############################################################################
########
# Enable SYN Flood Protection. This option configures iptables to offer
some
# protection from tcp SYN packet DOS attempts. You should set the RATE
so that
```

```
# false-positives are kept to a minimum otherwise visitors may see
connection
# issues (check /var/log/messages for *SYNFLOOD Blocked*). See the
iptables
# man page for the correct --limit rate syntax
#
# Note: This option should ONLY be enabled if you know you are under a
SYN
# flood attack as it will slow down all new connections from any IP
address to
# the server if triggered
SYNFLOOD = "0"
SYNFLOOD_RATE = "100/s"
SYNFLOOD_BURST = "150"

# Connection Limit Protection. This option configures iptables to offer
more
# protection from DOS attacks against specific ports. It can also be
used as a
# way to simply limit resource usage by IP address to specific server
services.
# This option limits the number of concurrent new connections per IP
address
# that can be made to specific ports
#
# This feature does not work on servers that do not have the iptables
module
# xt_connlimit loaded. Typically, this will be with MONOLITHIC kernels.
VPS
# server admins should check with their VPS host provider that the
iptables
# module is included
#
# For further information and syntax refer to the Connection Limit
Protection
# section of the csf readme.txt
#
# Note: Run /etc/csf/csftest.pl to check whether this option will
function on
# this server
CONNLIMIT = ""

# Port Flood Protection. This option configures iptables to offer
protection
# from DOS attacks against specific ports. This option limits the
number of
# new connections per time interval that can be made to specific ports
#
# This feature does not work on servers that do not have the iptables
module
# ipt_recent loaded. Typically, this will be with MONOLITHIC kernels.
```

```
VPS
# server admins should check with their VPS host provider that the
iptables
# module is included
#
# For further information and syntax refer to the Port Flood Protection
# section of the csf readme.txt
#
# Note: Run /etc/csf/csftest.pl to check whether this option will
function on
# this server
PORTFLOOD = ""

# Outgoing UDP Flood Protection. This option limits outbound UDP packet
floods.
# These typically originate from exploit scripts uploaded through
vulnerable
# web scripts. Care should be taken on servers that use services that
utilise
# high levels of UDP outbound traffic, such as SNMP, so you may need to
alter
# the UDPFLOOD_LIMIT and UDPFLOOD_BURST options to suit your
environment
#
# We recommend enabling User ID Tracking (UID_INTERVAL) with this
feature
UDPFLOOD = "0"
UDPFLOOD_LIMIT = "100/s"
UDPFLOOD_BURST = "500"

# This is a list of usernames that should not be rate limited, such as
"named"
# to prevent bind traffic from being limited.
#
# Note: root (UID:0) is always allowed
UDPFLOOD_ALLOWUSER = "named"

##############################################################################
########
# SECTION:Logging Settings
##############################################################################
########
# Log lfd messages to SYSLOG in addition to /var/log/lfd.log. You must
have the
# perl module Sys::Syslog installed to use this feature
SYSLOG = "0"

# Drop target for iptables rules. This can be set to either DROP ot
REJECT.
# REJECT will send back an error packet, DROP will not respond at all.
REJECT
```

```
# is more polite, however it does provide extra information to a hacker
and
# lets them know that a firewall is blocking their attempts. DROP hangs
their
# connection, thereby frustrating attempts to port scan the server.
DROP = "DROP"

# Enable logging of dropped connections to blocked ports to syslog,
usually
# /var/log/messages. This option needs to be enabled to use Port Scan
Tracking
DROP_LOGGING = "1"

# Enable logging of dropped incoming connections from blocked IP
addresses
#
# This option will be disabled if you enable Port Scan Tracking
(PS_INTERVAL)
DROP_IP_LOGGING = "0"

# Enable logging of dropped outgoing connections
#
# Note: Only outgoing SYN packets for TCP connections are logged, other
# protocols log all packets
#
# We recommend that you enable this option
DROP_OUT_LOGGING = "1"

# Together with DROP_OUT_LOGGING enabled, this option logs the UID
connecting
# out (where available) which can help track abuse
DROP_UID_LOGGING = "1"

# Only log incoming reserved port dropped connections (0:1023). This
can reduce
# the amount of log noise from dropped connections, but will affect
options
# such as Port Scan Tracking (PS_INTERVAL)
DROP_ONLYRES = "0"

# Commonly blocked ports that you do not want logging as they tend to
just fill
# up the log file. These ports are specifically blocked (applied to TCP
and UDP
# protocols) for incoming connections
DROP_NOLOG = "67,68,111,113,135:139,445,500,513,520"

# Log packets dropped by the packet filtering option PACKET_FILTER
DROP_PF_LOGGING = "0"

# Log packets dropped by the Connection Limit Protection option
```

```
CONNLIMIT. If
# this is enabled and Port Scan Tracking (PS_INTERVAL) is also enabled,
IP
# addresses breaking the Connection Limit Protection will be blocked
CONNLIMIT_LOGGING = "0"

# Enable logging of UDP floods. This should be enabled, especially with
User ID
# Tracking enabled
UDPFLOOD_LOGGING = "1"

# Send an alert if log file flooding is detected which causes lfd to
skip log
# lines to prevent lfd from looping. If this alert is sent you should
check the
# reported log file for the reason for the flooding
LOGFLOOD_ALERT = "0"

# Configure csf to watch IP addresses (with csf -w [ip]). This option
will add
# overhead to packet traversal through iptables and syslog logging, so
should
# only be enabled while actively watching IP addresses. See readme.txt
for more
# information on the use of this option
WATCH_MODE = "0"

##############################################################################
########
# SECTION:Reporting Settings
##############################################################################
########
# By default, lfd will send alert emails using the relevant alert
template to
# the To: address configured within that template. Setting the
following
# option will override the configured To: field in all lfd alert emails
#
# Leave this option empty to use the To: field setting in each alert
template
LF_ALERT_TO = ""

# By default, lfd will send alert emails using the relevant alert
template from
# the From: address configured within that template. Setting the
following
# option will override the configured From: field in all lfd alert
emails
#
# Leave this option empty to use the From: field setting in each alert
template
```

```
LF_ALERT_FROM = ""

# By default, lfd will send all alerts using the SENDMAIL binary. To
send using
# SMTP directly, you can set the following to a relaying SMTP server,
e.g.
# "127.0.0.1". Leave this setting blank to use SENDMAIL
LF_ALERT_SMTP = ""

# Block Reporting. lfd can run an external script when it performs and
IP
# address block following for example a login failure. The following
setting
# is to the full path of the external script which must be executable.
See
# readme.txt for format details
#
# Leave this setting blank to disable
BLOCK_REPORT = ""

# To also run an external script when a temporary block is unblocked.
The
# following setting can be the full path of the external script which
must be
# executable. See readme.txt for format details
#
# Leave this setting blank to disable
UNBLOCK_REPORT = ""

# In addition to the standard lfd email alerts, you can additionally
enable the
# sending of X-ARF reports (see http://www.x-
arf.org/specification.html). Only
# block alert messages will be sent. The reports use our schema at:
# https://download.configserver.com/abuse_login-attack_0.2.json
#
# These reports are in a format accepted by many Netblock owners and
should
# help them investigate abuse. This option is not designed to
automatically
# forward these reports to the Netblock owners and should be checked
for
# false-positive blocks before reporting
#
# If available, the report will also include the abuse contact for the
IP from
# the Abusix Contact DB: https://abusix.com/contactdb.html
#
# Note: The following block types are not reported through this
feature:
# LF_PERMBLOCK, LF_NETBLOCK, LF_DISTATTACK, LF_DISTFTP, RT_*_ALERT
```

```
X_ARF = "0"

# By default, lfd will send emails from the root forwarder. Setting the
# following option will override this
X_ARF_FROM = ""

# By default, lfd will send emails to the root forwarder. Setting the
following
# option will override this
X_ARF_TO = ""

# If you want to automatically send reports to the abuse contact where
found,
# you can enable the following option
#
# Note: You MUST set X_ARF_FROM to a valid email address for this
option to
# work. This is so that the abuse contact can reply to the report
#
# However, you should be aware that without manual checking you could
be
# reporting innocent IP addresses, including your own clients, yourself
and
# your own servers
#
# Additionally, just because a contact address is found, does not mean
that
# there is anyone on the end of it reading, processing or acting on
such
# reports and you could conceivably reported for sending spam
#
# We do not recommend enabling this option. Abuse reports should be
checked and
# verified before being forwarded to the abuse contact
X_ARF_ABUSE = "0"

###############################################################################
########
# SECTION:Temp to Perm/Netblock Settings
###############################################################################
########
# Temporary to Permanent IP blocking. The following enables this
feature to
# permanently block IP addresses that have been temporarily blocked
more than
# LF_PERMBLOCK_COUNT times in the last LF_PERMBLOCK_INTERVAL seconds.
Set
# LF_PERMBLOCK  to "1" to enable this feature
#
# Care needs to be taken when setting LF_PERMBLOCK_INTERVAL as it needs
to be
```

```
# at least LF_PERMBLOCK_COUNT multiplied by the longest temporary time
setting
# (TTL) for blocked IPs, to be effective
#
# Set LF_PERMBLOCK to "0" to disable this feature
LF_PERMBLOCK = "1"
LF_PERMBLOCK_INTERVAL = "86400"
LF_PERMBLOCK_COUNT = "4"
LF_PERMBLOCK_ALERT = "1"

# Permanently block IPs by network class. The following enables this
feature
# to permanently block classes of IP address where individual IP
addresses
# within the same class LF_NETBLOCK_CLASS have already been blocked
more than
# LF_NETBLOCK_COUNT times in the last LF_NETBLOCK_INTERVAL seconds. Set
# LF_NETBLOCK  to "1" to enable this feature
#
# This can be an affective way of blocking DDOS attacks launched from
within
# the same network class
#
# Valid settings for LF_NETBLOCK_CLASS are "A", "B" and "C", care and
# consideration is required when blocking network classes A or B
#
# Set LF_NETBLOCK to "0" to disable this feature
LF_NETBLOCK = "0"
LF_NETBLOCK_INTERVAL = "86400"
LF_NETBLOCK_COUNT = "4"
LF_NETBLOCK_CLASS = "C"
LF_NETBLOCK_ALERT = "1"

# Valid settings for LF_NETBLOCK_IPV6 are "/64", "/56", "/48", "/32"
and "/24"
# Great care should be taken with IPV6 netblock ranges due to the large
number
# of addresses involved
#
# To disable IPv6 netblocks set to ""
LF_NETBLOCK_IPV6 = ""

##############################################################################
########
# SECTION:Global Lists/DYNDNS/Blocklists
##############################################################################
########
# Safe Chain Update. If enabled, all dynamic update chains (GALLOW*,
GDENY*,
# SPAMHAUS, DSHIELD, BOGON, CC_ALLOW, CC_DENY, ALLOWDYN*) will create a
new
```

```
# chain when updating, and insert it into the relevant
LOCALINPUT/LOCALOUTPUT
# chain, then flush and delete the old dynamic chain and rename the new
chain.
#
# This prevents a small window of opportunity opening when an update
occurs and
# the dynamic chain is flushed for the new rules.
#
# This option should not be enabled on servers with long dynamic chains
(e.g.
# CC_DENY/CC_ALLOW lists) and low memory. It should also not be enabled
on
# Virtuozzo VPS servers with a restricted numiptent value. This is
because each
# chain will effectively be duplicated while the update occurs,
doubling the
# number of iptables rules
SAFECHAINUPDATE = "0"

# If you wish to allow access from dynamic DNS records (for example if
your IP
# address changes whenever you connect to the internet but you have a
dedicated
# dynamic DNS record from the likes of dyndns.org) then you can list
the FQDN
# records in csf.dyndns and then set the following to the number of
seconds to
# poll for a change in the IP address. If the IP address has changed
iptables
# will be updated.
#
# If the FQDN has multiple A records then all of the IP addresses will
be
# processed. If IPV6 is enabled, then all IPv6 AAAA IP address records
will
# also be allowed.
#
# A setting of 600 would check for IP updates every 10 minutes. Set the
value
# to 0 to disable the feature
DYNDNS = "0"

# To always ignore DYNDNS IP addresses in lfd blocking, set the
following
# option to 1
DYNDNS_IGNORE = "0"

# The follow Global options allow you to specify a URL where csf can
grab a
# centralised copy of an IP allow or deny block list of your own. You
```

```
need to
# specify the full URL in the following options, i.e.:
# http://www.somelocation.com/allow.txt
#
# The actual retrieval of these IP's is controlled by lfd, so you need
to set
# LF_GLOBAL to the interval (in seconds) when you want lfd to retrieve.
lfd
# will perform the retrieval when it runs and then again at the
specified
# interval. A sensible interval would probably be every 3600 seconds (1
hour).
# A minimum value of 300 is enforced for LF_GLOBAL if enabled
#
# You do not have to specify both an allow and a deny file
#
# You can also configure a global ignore file for IP's that lfd should
ignore
LF_GLOBAL = "0"

GLOBAL_ALLOW = ""
GLOBAL_DENY = ""
GLOBAL_IGNORE = ""

# Provides the same functionality as DYNDNS but with a GLOBAL URL file.
Set
# this to the URL of the file containing DYNDNS entries
GLOBAL_DYNDNS = ""

# Set the following to the number of seconds to poll for a change in
the IP
# address resoved from GLOBAL_DYNDNS
GLOBAL_DYNDNS_INTERVAL = "600"

# To always ignore GLOBAL_DYNDNS IP addresses in lfd blocking, set the
following
# option to 1
GLOBAL_DYNDNS_IGNORE = "0"

# Blocklists are controlled by modifying /etc/csf/csf.blocklists
#
# If you don't want BOGON rules applied to specific NICs, then list
them in
# a comma separated list (e.g "eth1,eth2")
LF_BOGON_SKIP = ""

# The following option can be used to select either HTTP::Tiny or
# LWP::UserAgent to retrieve URL data. HTTP::Tiny is much faster than
# LWP::UserAgent and is included in the csf distribution.
LWP::UserAgent may
# have to be installed manually, but it can better support https://
```

```
URL's
# which also needs the LWP::Protocol::https perl module
#
# For example:
#
# On rpm based systems:
#
#   yum install perl-libwww-perl.noarch perl-LWP-Protocol-https.noarch
#
# On APT based systems:
#
#   apt-get install libwww-perl liblwp-protocol-https-perl
#
# Via cpan:
#
#   perl -MCPAN -eshell
#   cpan> install LWP LWP::Protocol::https
#
# We recommend setting this set to "2" as upgrades to csf will be
performed
# over SSL to https://download.configserver.com
#
# "1" = HTTP::Tiny
# "2" = LWP::UserAgent
URLGET = "2"

##############################################################################
########
# SECTION:Country Code Lists and Settings
##############################################################################
########
# Country Code to CIDR allow/deny. In the following two options you can
allow
# or deny whole country CIDR ranges. The CIDR blocks are generated from
the
# Maxmind GeoLite Country database
http://www.maxmind.com/app/geolitecountry
# and entirely relies on that service being available
#
# Specify the the two-letter ISO Country Code(s). The iptables rules
are for
# incoming connections only
#
# Additionally, ASN numbers can also be added to the comma separated
lists
# below that also list Country Codes. The same WARNINGS for Country
Codes apply
# to the use of ASNs. More about Autonomous System Numbers (ASN):
# http://www.iana.org/assignments/as-numbers/as-numbers.xhtml
#
# You should consider using LF_IPSET when using any of the following
```

```
options
#
# WARNING: These lists are never 100% accurate and some ISP's (e.g.
AOL) use
# non-geographic IP address designations for their clients
#
# WARNING: Some of the CIDR lists are huge and each one requires a rule
within
# the incoming iptables chain. This can result in significant
performance
# overheads and could render the server inaccessible in some
circumstances. For
# this reason (amongst others) we do not recommend using these options
#
# WARNING: Due to the resource constraints on VPS servers this feature
should
# not be used on such systems unless you choose very small CC zones
#
# WARNING: CC_ALLOW allows access through all ports in the firewall.
For this
# reason CC_ALLOW probably has very limited use and CC_ALLOW_FILTER is
# preferred
#
# Each option is a comma separated list of CC's, e.g. "US,GB,DE"
CC_DENY = ""
CC_ALLOW = ""

# An alternative to CC_ALLOW is to only allow access from the following
# countries but still filter based on the port and packets rules. All
other
# connections are dropped
CC_ALLOW_FILTER = ""

# This option allows access from the following countries to specific
ports
# listed in CC_ALLOW_PORTS_TCP and CC_ALLOW_PORTS_UDP
#
# Note: The rules for this feature are inserted after the allow and
deny
# rules to still allow blocking of IP addresses
#
# Each option is a comma separated list of CC's, e.g. "US,GB,DE"
CC_ALLOW_PORTS = ""

# All listed ports should be removed from TCP_IN/UDP_IN to block access
from
# elsewhere. This option uses the same format as TCP_IN/UDP_IN
#
# An example would be to list port 21 here and remove it from
TCP_IN/UDP_IN
# then only counties listed in CC_ALLOW_PORTS can access FTP
```

```
CC_ALLOW_PORTS_TCP = ""
CC_ALLOW_PORTS_UDP = ""

# This option denies access from the following countries to specific
ports
# listed in CC_DENY_PORTS_TCP and CC_DENY_PORTS_UDP
#
# Note: The rules for this feature are inserted after the allow and
deny
# rules to still allow allowing of IP addresses
#
# Each option is a comma separated list of CC's, e.g. "US,GB,DE"
CC_DENY_PORTS = ""

# This option uses the same format as TCP_IN/UDP_IN. The ports listed
should
# NOT be removed from TCP_IN/UDP_IN
#
# An example would be to list port 21 here then counties listed in
# CC_DENY_PORTS cannot access FTP
CC_DENY_PORTS_TCP = ""
CC_DENY_PORTS_UDP = ""

# This Country Code list will prevent lfd from blocking IP address hits
for the
# listed CC's
#
# CC_LOOKUPS must be enabled to use this option
CC_IGNORE = ""

# This Country Code list will only allow SMTP AUTH to be advertised to
the
# listed countries in EXIM. This is to help limit attempts at
distributed
# attacks against SMTP AUTH which are difficult to achive since port 25
needs
# to be open to relay email
#
# The reason why this works is that if EXIM does not advertise SMTP
AUTH on a
# connection, then SMTP AUTH will not accept logins, defeating the
attacks
# without restricting mail relaying
#
# This option can generate a very large list of IP addresses that could
easily
# severely impact on SMTP (mail) performance, so care must be taken
when
# selecting countries and if performance issues ensue
#
# The option SMTPAUTH_RESTRICT must be enabled to use this option
```

```
CC_ALLOW_SMTPAUTH = ""

# Set this option to a valid CIDR (i.e. 1 to 32) to ignore CIDR blocks
smaller
# than this value when implementing CC_DENY/CC_ALLOW/CC_ALLOW_FILTER.
This can
# help reduce the number of CC entries and may improve iptables
throughput.
# Obviously, this will deny/allow fewer IP addresses depending on how
small you
# configure the option
#
# For example, to ignore all CIDR (and single IP) entries small than a
/16, set
# this option to "16". Set to "" to block all CC IP addresses
CC_DROP_CIDR = ""

# Display Country Code and Country for reported IP addresses. This
option can
# be configured to use the MaxMind Country Database or the more
detailed (and
# much larger and therefore slower) MaxMind City Database
#
# "0" - disable
# "1" - Reports: Country Code and Country
# "2" - Reports: Country Code and Country and Region and City
# "3" - Reports: Country Code and Country and Region and City and ASN
CC_LOOKUPS = "1"

# Display Country Code and Country for reported IPv6 addresses using
the
# MaxMind Country IPv6 Database
#
# "0" - disable
# "1" - Reports: Country Code and Country
#
# This option must also be enabled to allow IPv6 support to CC_*,
MESSENGER and
# PORTFLOOD
CC6_LOOKUPS = "0"

# This option tells lfd how often to retrieve the Maxmind GeoLite
Country
# database for CC_ALLOW, CC_ALLOW_FILTER, CC_DENY, CC_IGNORE and
CC_LOOKUPS (in
# days)
CC_INTERVAL = "7"

##############################################################################
########
# SECTION:Login Failure Blocking and Alerts
```

```
###############################################################################
########
# The following[*] triggers are application specific. If you set
LF_TRIGGER to
# "0" the value of each trigger is the number of failures against that
# application that will trigger lfd to block the IP address
#
# If you set LF_TRIGGER to a value greater than "0" then the
following[*]
# application triggers are simply on or off ("0" or "1") and the value
of
# LF_TRIGGER is the total cumulative number of failures that will
trigger lfd
# to block the IP address
#
# Setting the application trigger to "0" disables it
LF_TRIGGER = "0"

# If LF_TRIGGER is > "0" then LF_TRIGGER_PERM can be set to "1" to
permanently
# block the IP address, or LF_TRIGGER_PERM can be set to a value
greater than
# "1" and the IP address will be blocked temporarily for that value in
seconds.
# For example:
# LF_TRIGGER_PERM = "1" => the IP is blocked permanently
# LF_TRIGGER_PERM = "3600" => the IP is blocked temporarily for 1 hour
#
# If LF_TRIGGER is "0", then the application LF_[application]_PERM
value works
# in the same way as above and LF_TRIGGER_PERM serves no function
LF_TRIGGER_PERM = "1"

# To only block access to the failed application instead of a complete
block
# for an ip address, you can set the following to "1", but LF_TRIGGER
must be
# set to "0" with specific application[*] trigger levels also set
appropriately
#
# The ports that are blocked can be configured by changing the PORTS_*
options
LF_SELECT = "0"

# Send an email alert if an IP address is blocked by one of the [*]
triggers
LF_EMAIL_ALERT = "1"

# [*]Enable login failure detection of sshd connections
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
```

```
Read
# this file about RESTRICT_SYSLOG before enabling this option:
LF_SSHD = "5"
LF_SSHD_PERM = "1"

# [*]Enable login failure detection of ftp connections
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
Read
# this file about RESTRICT_SYSLOG before enabling this option:
LF_FTPD = "10"
LF_FTPD_PERM = "1"

# [*]Enable login failure detection of SMTP AUTH connections
LF_SMTPAUTH = "5"
LF_SMTPAUTH_PERM = "1"

# [*]Enable syntax failure detection of Exim connections
LF_EXIMSYNTAX = "10"
LF_EXIMSYNTAX_PERM = "1"

# [*]Enable login failure detection of pop3 connections
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
Read
# this file about RESTRICT_SYSLOG before enabling this option:
LF_POP3D = "1"
LF_POP3D_PERM = "1"

# [*]Enable login failure detection of imap connections
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
Read
# this file about RESTRICT_SYSLOG before enabling this option:
LF_IMAPD = "1"
LF_IMAPD_PERM = "1"

# [*]Enable login failure detection of Apache .htpasswd connections
# Due to the often high logging rate in the Apache error log, you might
want to
# enable this option only if you know you are suffering from attacks
against
# password protected directories
LF_HTACCESS = "5"
LF_HTACCESS_PERM = "1"

# [*]Enable failure detection of repeated Apache mod_security rule
triggers
LF_MODSEC = "5"
LF_MODSEC_PERM = "1"
```

```
# [*]Enable detection of repeated BIND denied requests
# This option should be enabled with care as it will prevent blocked
IPs from
# resolving any domains on the server. You might want to set the
trigger value
# reasonably high to avoid this
# Example: LF_BIND = "100"
LF_BIND = "0"
LF_BIND_PERM = "1"

# [*]Enable detection of repeated suhosin ALERTs
# Example: LF_SUHOSIN = "5"
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
Read
# this file about RESTRICT_SYSLOG before enabling this option:
LF_SUHOSIN = "0"
LF_SUHOSIN_PERM = "1"

# [*]Enable detection of repeated cxs ModSecurity mod_security rule
triggers
# This option will block IP addresses if cxs detects a hits from the
# ModSecurity rule associated with it
#
# Note: This option takes precedence over LF_MODSEC and removes any
hits
# counted towards LF_MODSEC for the cxs rule
#
# This setting should probably set very low, perhaps to 1, if you want
to
# effectively block IP addresses for this trigger option
LF_CXS = "0"
LF_CXS_PERM = "1"

# [*]Enable detection of repeated Apache mod_qos rule triggers
LF_QOS = "0"
LF_QOS_PERM = "1"

# [*]Enable detection of repeated Apache symlink race condition
triggers from
# the Apache patch provided by:
# http://www.mail-archive.com/dev@httpd.apache.org/msg55666.html
# This patch has also been included by cPanel via the easyapache
option:
# "Symlink Race Condition Protection"
LF_SYMLINK = "0"
LF_SYMLINK_PERM = "1"

# [*]Enable login failure detection of webmin connections
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
```

```
Read
# this file about RESTRICT_SYSLOG before enabling this option:
LF_WEBMIN = "0"
LF_WEBMIN_PERM = "1"

# Send an email alert if anyone logs in successfully using SSH
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
Read
# this file about RESTRICT_SYSLOG before enabling this option:
LF_SSH_EMAIL_ALERT = "1"

# Send an email alert if anyone uses su to access another account. This
will
# send an email alert whether the attempt to use su was successful or
not
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
Read
# this file about RESTRICT_SYSLOG before enabling this option:
LF_SU_EMAIL_ALERT = "1"

# Send an email alert if anyone accesses webmin
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
Read
# this file about RESTRICT_SYSLOG before enabling this option:
LF_WEBMIN_EMAIL_ALERT = "1"

# Send an email alert if anyone logs in successfully to root on the
console
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
Read
# this file about RESTRICT_SYSLOG before enabling this option:
LF_CONSOLE_EMAIL_ALERT = "1"

# This option will keep track of the number of "File does not exist"
errors in
# HTACCESS_LOG. If the number of hits is more than LF_APACHE_404 in
LF_INTERVAL
# seconds then the IP address will be blocked
#
# Care should be used with this option as it could generate many
# false-positives, especially Search Bots (use csf.rignore to ignore
such bots)
# so only use this option if you know you are under this type of attack
#
# A sensible setting for this would be quite high, perhaps 200
#
# To disable set to "0"
```

```
LF_APACHE_404 = "0"

# If this option is set to 1 the blocks will be permanent
# If this option is > 1, the blocks will be temporary for the specified
number
# of seconds
LF_APACHE_404_PERM = "3600"

# This option will keep track of the number of "client denied by server
# configuration" errors in HTACCESS_LOG. If the number of hits is more
than
# LF_APACHE_403 in LF_INTERVAL seconds then the IP address will be
blocked
#
# Care should be used with this option as it could generate many
# false-positives, especially Search Bots (use csf.rignore to ignore
such bots)
# so only use this option if you know you are under this type of attack
#
# A sensible setting for this would be quite high, perhaps 200
#
# To disable set to "0"
LF_APACHE_403 = "0"

# If this option is set to 1 the blocks will be permanent
# If this option is > 1, the blocks will be temporary for the specified
number
# of seconds
LF_APACHE_403_PERM = "3600"

# System Exploit Checking. This option is designed to perform a series
of tests
# to send an alert in case a possible server compromise is detected
#
# To enable this feature set the following to the checking interval in
seconds
# (a value of 300 would seem sensible).
#
# To disable set to "0"
LF_EXPLOIT = "300"

# This comma separated list allows you to ignore tests LF_EXPLOIT
performs
#
# For the SUPERUSER check, you can list usernames in csf.suignore to
have them
# ignored for that test
#
# Valid tests are:
# SUPERUSER,SSHDSPAM
#
```

```
# If you want to ignore a test add it to this as a comma separated
list, e.g.
# "SUPERUSER,SSHDSPAM"
LF_EXPLOIT_IGNORE = ""

# Set the time interval to track login and other LF_ failures within
(seconds),
# i.e. LF_TRIGGER failures within the last LF_INTERVAL seconds
LF_INTERVAL = "3600"

# This is how long the lfd process sleeps (in seconds) before
processing the
# log file entries and checking whether other events need to be
triggered
LF_PARSE = "5"

# This is the interval that is used to flush reports of usernames,
files and
# pids so that persistent problems continue to be reported, in seconds.
# A value of 3600 seems sensible
LF_FLUSH = "3600"

# Under some circumstances iptables can fail to include a rule
instruction,
# especially if more than one request is made concurrently. In this
event, a
# permanent block entry may exist in csf.deny, but not in iptables.
#
# This option instructs csf to deny an already blocked IP address the
number
# of times set. The downside, is that there will be multiple entries
for an IP
# address in csf.deny and possibly multiple rules for the same IP
address in
# iptables. This needs to be taken into consideration when unblocking
such IP
# addresses.
#
# Set to "0" to disable this feature. Do not set this too high for the
reasons
# detailed above (e.g. "5" should be more than enough)
LF_REPEATBLOCK = "0"

# By default csf will create both an inbound and outbound blocks
from/to an IP
# unless otherwise specified in csf.deny and GLOBAL_DENY. This is the
most
# effective way to block IP traffic. This option instructs csf to only
block
# inbound traffic from those IP's and so reduces the number of iptables
rules,
```

```
# but at the expense of less effectiveness. For this reason we
recommend
# leaving this option disabled
#
# Set to "0" to disable this feature - the default
LF_BLOCKINONLY = "0"

###############################################################################
########
# SECTION:Directory Watching & Integrity
###############################################################################
########
# Enable Directory Watching. This enables lfd to check /tmp and
/dev/shm
# directories for suspicious files, i.e. script exploits. If a
suspicious
# file is found an email alert is sent. One alert per file per LF_FLUSH
# interval is sent
#
# To enable this feature set the following to the checking interval in
seconds.
# To disable set to "0"
LF_DIRWATCH = "300"

# To remove any suspicious files found during directory watching,
enable the
# following. These files will be appended to a tarball in
# /var/lib/csf/suspicious.tar
LF_DIRWATCH_DISABLE = "0"

# This option allows you to have lfd watch a particular file or
directory for
# changes and should they change and email alert using watchalert.txt
is sent
#
# To enable this feature set the following to the checking interval in
seconds
# (a value of 60 would seem sensible) and add your entries to
csf.dirwatch
#
# Set to disable set to "0"
LF_DIRWATCH_FILE = "0"

# System Integrity Checking. This enables lfd to compare md5sums of the
# servers OS binary application files from the time when lfd starts. If
the
# md5sum of a monitored file changes an alert is sent. This option is
intended
# as an IDS (Intrusion Detection System) and is the last line of
detection for
# a possible root compromise.
```

```
#
# There will be constant false-positives as the servers OS is updated
or
# monitored application binaries are updated. However, unexpected
changes
# should be carefully inspected.
#
# Modified files will only be reported via email once.
#
# To enable this feature set the following to the checking interval in
seconds
# (a value of 3600 would seem sensible). This option may increase
server I/O
# load onto the server as it checks system binaries.
#
# To disable set to "0"
LF_INTEGRITY = "3600"

################################################################################
########
# SECTION:Distributed Attacks
################################################################################
########
# Distributed Account Attack. This option will keep track of login
failures
# from distributed IP addresses to a specific application account. If
the
# number of failures matches the trigger value above, ALL of the IP
addresses
# involved in the attack will be blocked according to the temp/perm
rules above
#
# Tracking applies to LF_SSHD, LF_FTPD, LF_SMTPAUTH, LF_POP3D,
LF_IMAPD,
# LF_HTACCESS
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
Read
# this file about RESTRICT_SYSLOG before enabling this option:
LF_DISTATTACK = "0"

# Set the following to the minimum number of unique IP addresses that
trigger
# LF_DISTATTACK
LF_DISTATTACK_UNIQ = "2"

# Distributed FTP Logins. This option will keep track of successful FTP
logins.
# If the number of successful logins to an individual account is at
least
# LF_DISTFTP in LF_DIST_INTERVAL from at least LF_DISTFTP_UNIQ IP
```

```
addresses,
# then all of the IP addresses will be blocked
#
# This option can help mitigate the common FTP account compromise
attacks that
# use a distributed network of zombies to deface websites
#
# A sensible setting for this might be 5, depending on how many
different
# IP addresses you expect to an individual FTP account within
LF_DIST_INTERVAL
#
# To disable set to "0"
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
Read
# this file about RESTRICT_SYSLOG before enabling this option:
LF_DISTFTP = "0"

# Set the following to the minimum number of unique IP addresses that
trigger
# LF_DISTFTP. LF_DISTFTP_UNIQ must be <= LF_DISTFTP for this to work
LF_DISTFTP_UNIQ = "3"

# If this option is set to 1 the blocks will be permanent
# If this option is > 1, the blocks will be temporary for the specified
number
# of seconds
LF_DISTFTP_PERM = "1"

# Send an email alert if LF_DISTFTP is triggered
LF_DISTFTP_ALERT = "1"

# Distributed SMTP Logins. This option will keep track of successful
SMTP
# logins. If the number of successful logins to an individual account
is at
# least LF_DISTSMTP in LF_DIST_INTERVAL from at least LF_DISTSMTP_UNIQ
IP
# addresses, then all of the IP addresses will be blocked. These
options only
# apply to the exim MTA
#
# This option can help mitigate the common SMTP account compromise
attacks that
# use a distributed network of zombies to send spam
#
# A sensible setting for this might be 5, depending on how many
different
# IP addresses you expect to an individual SMTP account within
LF_DIST_INTERVAL
```

```
#
# To disable set to "0"
LF_DISTSMTP = "0"

# Set the following to the minimum number of unique IP addresses that
trigger
# LF_DISTSMTP. LF_DISTSMTP_UNIQ must be <= LF_DISTSMTP for this to work
LF_DISTSMTP_UNIQ = "3"

# If this option is set to 1 the blocks will be permanent
# If this option is > 1, the blocks will be temporary for the specified
number
# of seconds
LF_DISTSMTP_PERM = "1"

# Send an email alert if LF_DISTSMTP is triggered
LF_DISTSMTP_ALERT = "1"

# This is the interval during which a distributed FTP or SMTP attack is
# measured
LF_DIST_INTERVAL = "300"

# If LF_DISTFTP or LF_DISTSMTP is triggered, then if the following
contains the
# path to a script, it will run the script and pass the following as
arguments:
#
# LF_DISTFTP/LF_DISTSMTP
# account name
# log file text
#
# The action script must have the execute bit and interpreter (shebang)
set
LF_DIST_ACTION = ""

##############################################################################
########
# SECTION:Login Tracking
##############################################################################
########
# Block POP3 logins if greater than LT_POP3D times per hour per account
per IP
# address (0=disabled)
#
# This is a temporary block for the rest of the hour, afterwhich the IP
is
# unblocked
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
Read
# this file about RESTRICT_SYSLOG before enabling this option:
```

```
LT_POP3D = "0"

# Block IMAP logins if greater than LT_IMAPD times per hour per account
per IP
# address (0=disabled) - not recommended for IMAP logins due to the
ethos
# within which IMAP works. If you want to use this, setting it quite
high is
# probably a good idea
#
# This is a temporary block for the rest of the hour, afterwhich the IP
is
# unblocked
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
Read
# this file about RESTRICT_SYSLOG before enabling this option:
LT_IMAPD = "0"

# Send an email alert if an account exceeds LT_POP3D/LT_IMAPD logins
per hour
# per IP
LT_EMAIL_ALERT = "1"

# If LF_PERMBLOCK is enabled but you do not want this to apply to
# LT_POP3D/LT_IMAPD, then enable this option
LT_SKIPPERMBLOCK = "0"

##############################################################################
########
# SECTION:Connection Tracking
##############################################################################
########
# Connection Tracking. This option enables tracking of all connections
from IP
# addresses to the server. If the total number of connections is
greater than
# this value then the offending IP address is blocked. This can be used
to help
# prevent some types of DOS attack.
#
# Care should be taken with this option. It's entirely possible that
you will
# see false-positives. Some protocols can be connection hungry, e.g.
FTP, IMAPD
# and HTTP so it could be quite easy to trigger, especially with a lot
of
# closed connections in TIME_WAIT. However, for a server that is prone
to DOS
# attacks this may be very useful. A reasonable setting for this option
might
```

```
# be around 300.
#
# To disable this feature, set this to 0
CT_LIMIT = "0"

# Connection Tracking interval. Set this to the the number of seconds
between
# connection tracking scans
CT_INTERVAL = "30"

# Send an email alert if an IP address is blocked due to connection
tracking
CT_EMAIL_ALERT = "1"

# If you want to make IP blocks permanent then set this to 1, otherwise
blocks
# will be temporary and will be cleared after CT_BLOCK_TIME seconds
CT_PERMANENT = "0"

# If you opt for temporary IP blocks for CT, then the following is the
interval
# in seconds that the IP will remained blocked for (e.g. 1800 = 30
mins)
CT_BLOCK_TIME = "1800"

# If you don't want to count the TIME_WAIT state against the connection
count
# then set the following to "1"
CT_SKIP_TIME_WAIT = "0"

# If you only want to count specific states (e.g. SYN_RECV) then add
the states
# to the following as a comma separated list. E.g. "SYN_RECV,TIME_WAIT"
#
# Leave this option empty to count all states against CT_LIMIT
CT_STATES = ""

# If you only want to count specific ports (e.g. 80,443) then add the
ports
# to the following as a comma separated list. E.g. "80,443"
#
# Leave this option empty to count all ports against CT_LIMIT
CT_PORTS = ""

##################################################################
########
# SECTION:Process Tracking
##################################################################
########
# Process Tracking. This option enables tracking of user and nobody
processes
```

```
# and examines them for suspicious executables or open network ports.
Its
# purpose is to identify potential exploit processes that are running
on the
# server, even if they are obfuscated to appear as system services. If
a
# suspicious process is found an alert email is sent with relevant
information.
# It is then the responsibility of the recipient to investigate the
process
# further as the script takes no further action
#
# The following is the number of seconds a process has to be active
before it
# is inspected. If you set this time too low, then you will likely
trigger
# false-positives with CGI or PHP scripts.
# Set the value to 0 to disable this feature
PT_LIMIT = "60"

# How frequently processes are checked in seconds
PT_INTERVAL = "60"

# If you want process tracking to highlight php or perl scripts that
are run
# through apache then disable the following,
# i.e. set it to 0
#
# While enabling this setting will reduce false-positives, having it
set to 0
# does provide better checking for exploits running on the server
PT_SKIP_HTTP = "0"

# lfd will report processes, even if they're listed in csf.pignore, if
they're
# tagged as (deleted) by Linux. This information is provided in Linux
under
# /proc/PID/exe. A (deleted) process is one that is running a binary
that has
# the inode for the file removed from the file system directory. This
usually
# happens when the binary has been replaced due to an upgrade for it by
the OS
# vendor or another third party (e.g. cPanel). You need to investigate
whether
# this is indeed the case to be sure that the original binary has not
been
# replaced by a rootkit or is running an exploit.
#
# Note: If a deleted executable process is detected and reported then
lfd will
```

```
# not report children of the parent (or the parent itself if a child
triggered
# the report) if the parent is also a deleted executable process
#
# To stop lfd reporting such process you need to restart the daemon to
which it
# belongs and therefore run the process using the replacement binary
(presuming
# one exists). This will normally mean running the associated startup
script in
# /etc/init.d/
#
# If you do want lfd to report deleted binary processes, set to 1
PT_DELETED = "0"

# If a PT_DELETED event is triggered, then if the following contains
the path to
# a script, it will be run in a child process and passed the
executable, pid,
# account for the process, and parent pid
#
# The action script must have the execute bit and interpreter (shebang)
set. An
# example is provided in /usr/local/csf/bin/pt_deleted_action.pl
#
# WARNING: Make sure you read and understand the potential security
# implications of such processes in PT_DELETED above before simply
restarting
# such processes with a script
PT_DELETED_ACTION = ""

# User Process Tracking. This option enables the tracking of the number
of
# process any given account is running at one time. If the number of
processes
# exceeds the value of the following setting an email alert is sent
with
# details of those processes. If you specify a user in csf.pignore it
will be
# ignored
#
# Set to 0 to disable this feature
PT_USERPROC = "10"

# This User Process Tracking option sends an alert if any linux user
process
# exceeds the memory usage set (MB). To ignore specific processes or
users use
# csf.pignore
#
# Set to 0 to disable this feature
```

```
PT_USERMEM = "256"

# This User Process Tracking option sends an alert if any linux user
process
# exceeds the time usage set (seconds). To ignore specific processes or
users
# use csf.pignore
#
# Set to 0 to disable this feature
PT_USERTIME = "1800"

# If this option is set then processes detected by PT_USERMEM,
PT_USERTIME or
# PT_USERPROC are killed
#
# Warning: We don't recommend enabling this option unless absolutely
necessary
# as it can cause unexpected problems when processes are suddenly
terminated.
# It can also lead to system processes being terminated which could
cause
# stability issues. It is much better to leave this option disabled and
to
# investigate each case as it is reported when the triggers above are
breached
#
# Note: Processes that are running deleted excecutables (see
PT_DELETED) will
# not be killed by lfd
PT_USERKILL = "0"

# If you want to disable email alerts if PT_USERKILL is triggered, then
set
# this option to 0
PT_USERKILL_ALERT = "1"

# If a PT_* event is triggered, then if the following contains the path
to
# a script, it will be run in a child process and passed the PID(s) of
the
# process(es) in a comma separated list.
#
# The action script must have the execute bit and interpreter (shebang)
set
PT_USER_ACTION = ""

# Check the PT_LOAD_AVG minute Load Average (can be set to 1 5 or 15
and
# defaults to 5 if set otherwise) on the server every PT_LOAD seconds.
If the
# load average is greater than or equal to PT_LOAD_LEVEL then an email
```

```
alert is
# sent. lfd then does not report subsequent high load until
PT_LOAD_SKIP
# seconds has passed to prevent email floods.
#
# Set PT_LOAD to "0" to disable this feature
PT_LOAD = "30"
PT_LOAD_AVG = "5"
PT_LOAD_LEVEL = "6"
PT_LOAD_SKIP = "3600"

# This is the Apache Server Status URL used in the email alert.
Requires the
# Apache mod_status module to be installed and configured correctly
PT_APACHESTATUS = "http://127.0.0.1/server-status"

# If a PT_LOAD event is triggered, then if the following contains the
path to
# a script, it will be run in a child process. For example, the script
could
# contain commands to terminate and restart httpd, php, exim, etc
incase of
# looping processes. The action script must have the execute bit an
# interpreter (shebang) set
PT_LOAD_ACTION = ""

# Fork Bomb Protection. This option checks the number of processes with
the
# same session id and if greater than the value set, the whole session
tree is
# terminated and an alert sent
#
# You can see an example of common session id processes on most Linux
systems
# using: "ps axf -O sid"
#
# On cPanel servers, PT_ALL_USERS should be enabled to use this option
# effectively
#
# This option will check root owned processes. Session id 0 and 1 will
always
# be ignored as they represent kernel and init processes. csf.pignore
will be
# honoured, but bear in mind that a session tree can contain a variety
of users
# and executables
#
# Care needs to be taken to ensure that this option only detects
runaway fork
# bombs, so should be set higher than any session tree is likely to get
(e.g.
```

```
# httpd could have 100s of legitimate children on very busy systems). A
# sensible starting point on most servers might be 250
PT_FORKBOMB = "0"

# Terminate hung SSHD sessions. When under an SSHD login attack, SSHD
processes
# are often left hung after their connecting IP addresses have been
blocked
#
# This option will terminate all processes with the cmdline of "sshd:
unknown
# [net]" or "sshd: unknown [priv]" if they have been running for more
than 60
# seconds
#
# Note: It is possible that enabling this option may have adverse
effects on
# valid SSHD processes. If this is the case, this option should be
disabled
#
# Note: Due to the nature of this type of attack, no email reports are
sent
# when the processes are terminated, however the event is logged in
lfd.log
# with a line prefix of "*PT_SSHDHUNG*"
PT_SSHDHUNG = "0"

##############################################################################
########
# SECTION:Port Scan Tracking
##############################################################################
########
# Port Scan Tracking. This feature tracks port blocks logged by
iptables to
# syslog. If an IP address generates a port block that is logged more
than
# PS_LIMIT within PS_INTERVAL seconds, the IP address will be blocked.
#
# This feature could, for example, be useful for blocking hackers
attempting
# to access the standard SSH port if you have moved it to a port other
than 22
# and have removed 22 from the TCP_IN list so that connection attempts
to the
# old port are being logged
#
# This feature blocks all iptables blocks from the iptables logs,
including
# repeated attempts to one port or SYN flood blocks, etc
#
# Note: This feature will only track iptables blocks from the log file
```

```
set in
# IPTABLES_LOG below and if you have DROP_LOGGING enabled. However, it
will
# cause redundant blocking with DROP_IP_LOGGING enabled
#
# Warning: It's possible that an elaborate DDOS (i.e. from multiple
IP's)
# could very quickly fill the iptables rule chains and cause a DOS in
itself.
# The DENY_IP_LIMIT should help to mitigate such problems with
permanent blocks
# and the DENY_TEMP_IP_LIMIT with temporary blocks
#
# Set PS_INTERVAL to "0" to disable this feature. A value of between 60
and 300
# would be sensible to enable this feature
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
Read
# this file about RESTRICT_SYSLOG before enabling this option:
PS_INTERVAL = "0"
PS_LIMIT = "10"

# You can specify the ports and/or port ranges that should be tracked
by the
# Port Scan Tracking feature. The following setting is a comma
separated list
# of those ports and uses the same format as TCP_IN. The default
setting of
# 0:65535,ICMP,INVALID,OPEN covers all ports
#
# Special values are:
#   ICMP    - include ICMP blocks (see ICMP_*)
#   INVALID - include INVALID blocks (see PACKET_FILTER)
#   OPEN    - include TCP_IN and UDP_IN open port blocks - *[proto]_IN
Blocked*
PS_PORTS = "0:65535,ICMP"

# To specify how many different ports qualifies as a Port Scan you can
increase
# the following from the default value of 1. The risk in doing so will
mean
# that persistent attempts to attack a specific closed port will not be
# detected and blocked
PS_DIVERSITY = "1"

# You can select whether IP blocks for Port Scan Tracking should be
temporary
# or permanent. Set PS_PERMANENT to "0" for temporary and "1" for
permanent
# blocking. If set to "0" PS_BLOCK_TIME is the amount of time in
```

```
seconds to
# temporarily block the IP address for
PS_PERMANENT = "0"
PS_BLOCK_TIME = "3600"

# Set the following to "1" to enable Port Scan Tracking email alerts,
set to
# "0" to disable them
PS_EMAIL_ALERT = "1"

###############################################################################
########
# SECTION:User ID Tracking
###############################################################################
########
# User ID Tracking. This feature tracks UID blocks logged by iptables
to
# syslog. If a UID generates a port block that is logged more than
UID_LIMIT
# times within UID_INTERVAL seconds, an alert will be sent
#
# Note: This feature will only track iptables blocks from the log file
set in
# IPTABLES_LOG and if DROP_OUT_LOGGING and DROP_UID_LOGGING are
enabled.
#
# To ignore specific UIDs list them in csf.uidignore and then restart
lfd
#
# Set UID_INTERVAL to "0" to disable this feature. A value of between
60 and 300
# would be sensible to enable this feature
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
Read
# this file about RESTRICT_SYSLOG before enabling this option:
UID_INTERVAL = "0"
UID_LIMIT = "10"

# You can specify the ports and/or port ranges that should be tracked
by the
# User ID Tracking feature. The following setting is a comma separated
list
# of those ports and uses the same format as TCP_OUT. The default
setting of
# 0:65535,ICMP covers all ports
UID_PORTS = "0:65535,ICMP"

###############################################################################
########
# SECTION:Account Tracking
```

```
###############################################################################
########
# Account Tracking. The following options enable the tracking of
modifications
# to the accounts on a server. If any of the enabled options are
triggered by
# a modifications to an account, an alert email is sent. Only the
modification
# is reported. The cause of the modification will have to be
investigated
# manually
#
# You can set AT_ALERT to the following:
# 0 = disable this feature
# 1 = enable this feature for all accounts
# 2 = enable this feature only for superuser accounts (UID = 0, e.g.
root, etc)
# 3 = enable this feature only for the root account
AT_ALERT = "2"

# This options is the interval between checks in seconds
AT_INTERVAL = "60"

# Send alert if a new account is created
AT_NEW = "1"

# Send alert if an existing account is deleted
AT_OLD = "1"

# Send alert if an account password has changed
AT_PASSWD = "1"

# Send alert if an account uid has changed
AT_UID = "1"

# Send alert if an account gid has changed
AT_GID = "1"

# Send alert if an account login directory has changed
AT_DIR = "1"

# Send alert if an account login shell has changed
AT_SHELL = "1"

###############################################################################
########
# SECTION:Integrated User Interface
###############################################################################
########
# Integrated User Interface. This feature provides a HTML UI to csf and
lfd,
```

```
# without requiring a control panel or web server. The UI runs as a sub
process
# to the lfd daemon
#
# As it runs under the root account and successful login provides root
access
# to the server, great care should be taken when configuring and using
this
# feature. There are additional restrictions to enhance secure access
to the UI
#
# See readme.txt for more information about using this feature BEFORE
enabling
# it for security and access reasons
#
# 1 to enable, 0 to disable
UI = "0"

# Set this to the port that want to bind this service to. You should
configure
# this port to be >1023 and different from any other port already being
used
#
# Do NOT enable access to this port in TCP_IN, instead only allow
trusted IP's
# to the port using Advanced Allow Filters (see readme.txt)
UI_PORT = "6666"

# Optionally set the IP address to bind to. Normally this should be
left blank
# to bind to all IP addresses on the server.
#
# If the server is configured for IPv6 but the IP to bind to is IPv4,
then the
# IP address MUST use the IPv6 representation. For example 1.2.3.4 must
use
# ::ffff:1.2.3.4
#
# Leave blank to bind to all IP addresses on the server
UI_IP = ""

# This should be a secure, hard to guess username
#
# This must be changed from the default
UI_USER = "username"

# This should be a secure, hard to guess password. That is, at least 8
# characters long with a mixture of upper and lowercase characters plus
# numbers and non-alphanumeric characters
#
# This must be changed from the default
```

```
UI_PASS = "password"

# This is the login session timeout. If there is no activity for a
logged in
# session within this number of seconds, the session will timeout and a
new
# login will be required
#
# For security reasons, you should always keep this option low (i.e
60-300)
UI_TIMEOUT = "300"

# This is the maximum concurrent connections allowed to the server. The
default
# value should be sufficient
UI_CHILDREN = "5"

# The number of login retries allowed within a 24 hour period. A
successful
# login from the IP address will clear the failures
#
# For security reasons, you should always keep this option low (i.e
0-10)
UI_RETRY = "5"

# If enabled, this option will add the connecting IP address to the
file
# /etc/csf/ui/ui.ban after UI_RETRY login failures. The IP address will
not be
# able to login to the UI while it is listed in this file. The UI_BAN
setting
# does not refer to any of the csf/lfd allow or ignore files, e.g.
csf.allow,
# csf.ignore, etc.
#
# For security reasons, you should always enable this option
UI_BAN = "1"

# If enabled, only IPs (or CIDR's) listed in the file
/etc/csf/ui/ui.allow will
# be allowed to login to the UI. The UI_ALLOW setting does not refer to
any of
# the csf/lfd allow or ignore files, e.g. csf.allow, csf.ignore, etc.
#
# For security reasons, you should always enable this option and use
ui.allow
UI_ALLOW = "1"

# If enabled, this option will trigger an iptables block through csf
after
# UI_RETRY login failures
```

```
#
# 0 = no block;1 = perm block;nn=temp block for nn secs
UI_BLOCK = "1"

# This controls what email alerts are sent with regards to logins to
the UI. It
# uses the uialert.txt template
#
# 4 = login success + login failure/ban/block + login attempts
# 3 = login success + login failure/ban/block
# 2 = login failure/ban/block
# 1 = login ban/block
# 0 = disabled
UI_ALERT = "4"

# This is the SSL cipher list that the Integrated UI will negotiate
from
UI_CIPHER = "ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP:!kEDH"

# This is the SSL protocol version used. See IO::Socket::SSL if you
wish to
# change this and to understand the implications of changing it
UI_SSL_VERSION = "SSLv23:!SSLv3:!SSLv2"

# If cxs is installed then enabling this option will provide a dropdown
box to
# switch between applications
UI_CXS = "0"

# There is a modified installation of ConfigServer Explorer (cse)
provided with
# the csf distribution. If this option is enabled it will provide a
dropdown
# box to switch between applications
UI_CSE = "0"

##############################################################################
########
# SECTION:Messenger service
##############################################################################
########
# Messenger service. This feature allows the display of a message to a
blocked
# connecting IP address to inform the user that they are blocked in the
# firewall. This can help when users get themselves blocked, e.g. due
to
# multiple login failures. The service is provided by two daemons
running on
# ports providing either an HTML or TEXT message.
#
# This feature does not work on servers that do not have the iptables
```

```
module
# ipt_REDIRECT loaded. Typically, this will be with MONOLITHIC kernels.
VPS
# server admins should check with their VPS host provider that the
iptables
# module is included.
#
# For further information on features and limitations refer to the csf
# readme.txt
#
# Note: Run /etc/csf/csftest.pl to check whether this option will
function on
# this server
#
# 1 to enable, 0 to disable
MESSENGER = "0"

# Provide this service to temporary IP address blocks
MESSENGER_TEMP = "1"

# Provide this service to permanent IP address blocks
MESSENGER_PERM = "1"

# User account to run the service servers under. We recommend creating
a
# specific non-priv, non-shell account for this purpose
MESSENGER_USER = "csf"

# This is the maximum concurrent connections allowed to each service
server
MESSENGER_CHILDREN = "10"

# Set this to the port that will receive the HTML message. You should
configure
# this port to be >1023 and different from the TEXT port. Do NOT enable
access
# to this port in TCP_IN
MESSENGER_HTML = "8888"

# This comma separated list are the HTML ports that will be redirected
for the
# blocked IP address. If you are using per application blocking
(LF_TRIGGER)
# then only the relevant block port will be redirected to the messenger
port
MESSENGER_HTML_IN = "80,2082,2095"

# Set this to the port that will receive the TEXT message. You should
configure
# this port to be >1023 and different from the HTML port. Do NOT enable
access
```

```
# to this port in TCP_IN
MESSENGER_TEXT = "8889"

# This comma separated list are the TEXT ports that will be redirected
for the
# blocked IP address. If you are using per application blocking
(LF_TRIGGER)
# then only the relevant block port will be redirected to the messenger
port
MESSENGER_TEXT_IN = "21"

# These settings limit the rate at which connections can be made to the
# messenger service servers. Its intention is to provide protection
from
# attacks or excessive connections to the servers. If the rate is
exceeded then
# iptables will revert for the duration to the normal blocking actiity
#
# See the iptables man page for the correct --limit rate syntax
MESSENGER_RATE = "30/m"
MESSENGER_BURST = "5"

##############################################################################
########
# SECTION:lfd Clustering
##############################################################################
########
# lfd Clustering. This allows the configuration of an lfd cluster
environment
# where a group of servers can share blocks and configuration option
changes.
# Included are CLI and UI options to send requests to the cluster.
#
# See the readme.txt file for more information and details on setup and
# security risks.
#
# Comma separated list of cluster member IP addresses to send requests
to
CLUSTER_SENDTO = ""

# Comma separated list of cluster member IP addresses to receive
requests from
CLUSTER_RECVFROM = ""

# IP address of the master node in the cluster allowed to send
CLUSTER_CONFIG
# changes
CLUSTER_MASTER = ""

# If this is a NAT server, set this to the public IP address of this
server
```

```
CLUSTER_NAT = ""

# If a cluster member should send requests on an IP other than the
default IP,
# set it here
CLUSTER_LOCALADDR = ""

# Cluster communication port (must be the same on all member servers).
There
# is no need to open this port in the firewall as csf will
automatically add
# in and out bound rules to allow communication between cluster members
CLUSTER_PORT = "7777"

# This is a secret key used to encrypt cluster communications using the
# Blowfish algorithm. It should be between 8 and 56 characters long,
# preferably > 20 random characters
# 56 chars:    01234567890123456789012345678901234567890123456789012345
CLUSTER_KEY = ""

# Automatically send lfd blocks to all members of CLUSTER_SENDTO. Those
# servers must have this servers IP address listed in their
CLUSTER_RECVFROM
#
# Set to 0 to disable this feature
CLUSTER_BLOCK = "1"

# This option allows the enabling and disabling of the Cluster
configuration
# changing options --cconfig, --cconfigr, --cfile, --ccfile sent from
the
# CLUSTER_MASTER server
#
# Set this option to 1 to allow Cluster configurations to be received
CLUSTER_CONFIG = "0"

# Maximum number of child processes to listen on. High blocking rates
or large
# clusters may need to increase this
CLUSTER_CHILDREN = "10"

##############################################################################
########
# SECTION:Port Knocking
##############################################################################
########
# Port Knocking. This feature allows port knocking to be enabled on
multiple
# ports with a variable number of knocked ports and a timeout. There
must be a
# minimum of 3 ports to knock for an entry to be valid
```

```
#
# See the following for information regarding Port Knocking:
# http://www.portknocking.org/
#
# This feature does not work on servers that do not have the iptables
module
# ipt_recent loaded. Typically, this will be with MONOLITHIC kernels.
VPS
# server admins should check with their VPS host provider that the
iptables
# module is included
#
# For further information and syntax refer to the Port Knocking section
of the
# csf readme.txt
#
# Note: Run /etc/csf/csftest.pl to check whether this option will
function on
# this server
#
# openport;protocol;timeout;kport1;kport2;kport3[...;kportN],...
# e.g.: 22;TCP;20;100;200;300;400
PORTKNOCKING = ""

# Enable PORTKNOCKING logging by iptables
PORTKNOCKING_LOG = "1"

# Send an email alert if the PORTKNOCKING port is opened.
PORTKNOCKING_LOG must
# also be enabled to use this option
#
# SECURITY NOTE: This option is affected by the RESTRICT_SYSLOG option.
Read
# this file about RESTRICT_SYSLOG before enabling this option:
PORTKNOCKING_ALERT = "0"

##############################################################################
########
# SECTION:Log Scanner
##############################################################################
########
# Log Scanner. This feature will send out an email summary of the log
lines of
# each log listed in /etc/csf/csf.logfiles. All lines will be reported
unless
# they match a regular expression in /etc/csf/csf.logignore
#
# File globbing is supported for logs listed in /etc/csf/csf.logfiles.
However,
# be aware that the more files lfd has to track, the greater the
performance
```

```
# hit. Note: File globs are only evaluated when lfd is started
#
# Note: lfd builds the report continuously from lines logged after lfd
has
# started, so any lines logged when lfd is not running will not be
reported
# (e.g. during reboot). If lfd is restarted, then the report will
include any
# lines logged during the previous lfd logging period that weren't
reported
#
# 1 to enable, 0 to disable
LOGSCANNER = "0"

# This is the interval each report will be sent based on the
logalert.txt
# template
#
# The interval can be set to:
# "hourly" - sent on the hour
# "daily"  - sent at midnight (00:00)
# "manual" - sent whenever "csf --logrun" is run. This allows for
scheduling
#            via cron job
LOGSCANNER_INTERVAL = "hourly"

# Report Style
# 1 = Separate chronological log lines per log file
# 2 = Simply chronological log of all lines
LOGSCANNER_STYLE = "1"

# Send the report email even if no log lines reported
# 1 to enable, 0 to disable
LOGSCANNER_EMPTY = "1"

# Maximum number of lines in the report before it is truncated. This is
to
# prevent log lines flooding resulting in an excessively large report.
This
# might need to be increased if you choose a daily report
LOGSCANNER_LINES = "5000"

###############################################################################
# SECTION:Statistics Settings
###############################################################################
# Statistics
#
# Some of the Statistics output requires the gd graphics library and
the
```

```
# GD::Graph perl module with all dependent modules to be installed for
the UI
# for them to be displayed
#
# This option enabled statistical data gathering
ST_ENABLE = "1"

# This option determines how many iptables log lines to store for
reports
ST_IPTABLES = "100"

# This option indicates whether rDNS and CC lookups are performed at
the time
# the log line is recorded (this is not performed when viewing the
reports)
#
# Warning: If DROP_IP_LOGGING is enabled and there are frequent
iptables hits,
# then enabling this setting could cause serious performance problems
ST_LOOKUP = "0"

# This option will gather basic system statstics. Through the UI it
displays
# various graphs for disk, cpu, memory, network, etc usage over 4
intervals:
#  . Hourly (per minute)
#  . 24 hours (per minute)
#  . 7 days (per minute averaged over an hour)
#  . 30 days (per minute averaged over an hour) - user definable
# The data is stored in /var/lib/csf/stats/system and the option
requires the
# perl GD::Graph module
#
# Note: Disk graphs do not show on Virtuozzo/OpenVZ servers as the
kernel on
# those systems do not store the required information in
/proc/diskstats
# On new installations or when enabling this option it will take time
for these
# graphs to be populated
ST_SYSTEM = "0"

# Set the maximum days to collect statistics for. The default is 30
days, the
# more data that is collected the longer it will take for each of the
graphs to
# be generated
ST_SYSTEM_MAXDAYS = "30"

# If ST_SYSTEM is enabled, then these options can collect MySQL
statistical
```

```
# data. To use this option the server must have the perl modules DBI
and
# DBD::mysql installed.
#
# Set this option to "0" to disable MySQL data collection
ST_MYSQL = "0"

# The following options are for authentication for MySQL data
collection. If
# the password is left blank and the user set to "root" then the
procedure will
# look for authentication data in /root/.my.cnf. Otherwise, you will
need to
# provide a MySQL username and password to collect the data. Any MySQL
user
# account can be used
ST_MYSQL_USER = "root"
ST_MYSQL_PASS = ""
ST_MYSQL_HOST = "localhost"

# If ST_SYSTEM is enabled, then this option can collect Apache
statistical data
# The value for PT_APACHESTATUS must be correctly set
ST_APACHE = "0"

# The following options measure disk write performance using dd
(location set
# via the DD setting). It creates a 64MB file called
/var/lib/dd_write_test and
# the statistics will plot the MB/s response time of the disk. As this
is an IO
# intensive operation, it may not be prudent to run this test too
often, so by
# default it is only run every 5 minutes and the result duplicated for
each
# intervening minute for the statistics
#
# This is not necessrily a good measure of disk performance, primarily
because
# the measurements are for relatively small amounts of data over a
small amount
# of time. To properly test disk performance there are a variety of
tools
# available that should be run for extended periods of time to obtain
an
# accurate measurement. This metric is provided to give an idea of how
the disk
# is performing over time
#
# Note: There is a 15 second timeout performing the check
#
```

```
# Set to 0 to disable, 1 to enable
ST_DISKW = "0"

# The number of minutes that elapse between tests. Default is 5,
minimum is 1.
ST_DISKW_FREQ = "5"

# This is the command line passed to dd. If you are familiar with dd,
or wish
# to move the output file (of) to a different disk, then you can alter
this
# command. Take great care when making any changes to this command as
it is
# very easy to overwrite a disk using dd if you make a mistake
ST_DISKW_DD = "if=/dev/zero of=/var/lib/csf/dd_test bs=1MB count=64
conv=fdatasync"

###############################################################################
# SECTION:OS Specific Settings
###############################################################################
# Binary locations
IPTABLES = "/sbin/iptables"
IPTABLES_SAVE = "/sbin/iptables-save"
IPTABLES_RESTORE = "/sbin/iptables-restore"
IP6TABLES = "/sbin/ip6tables"
IP6TABLES_SAVE = "/sbin/ip6tables-save"
IP6TABLES_RESTORE = "/sbin/ip6tables-restore"
MODPROBE = "/sbin/modprobe"
IFCONFIG = "/sbin/ifconfig"
SENDMAIL = "/usr/sbin/sendmail"
PS = "/bin/ps"
VMSTAT = "/usr/bin/vmstat"
NETSTAT = "/bin/netstat"
LS = "/bin/ls"
MD5SUM = "/usr/bin/md5sum"
TAR = "/bin/tar"
CHATTR = "/usr/bin/chattr"
UNZIP = "/usr/bin/unzip"
GUNZIP = "/bin/gunzip"
DD = "/bin/dd"
TAIL = "/usr/bin/tail"
GREP = "/bin/grep"
IPSET = "/sbin/ipset"
SYSTEMCTL = "/bin/systemctl"
HOST = "/usr/bin/host"
IP = "/bin/ip"

# Log file locations
#
```

```
# File globbing is allowed for the following logs. However, be aware
that the
# more files lfd has to track, the greater the performance hit
#
# Note: File globs are only evaluated when lfd is started
#
HTACCESS_LOG = "/var/log/apache2/error.log"
MODSEC_LOG = "/var/log/apache2/error.log"
SSHD_LOG = "/var/log/auth.log"
SU_LOG = "/var/log/messages"
FTPD_LOG = "/var/log/messages"
SMTPAUTH_LOG = "/var/log/secure"
POP3D_LOG = "/var/log/mail.log"
IMAPD_LOG = "/var/log/mail.log"
IPTABLES_LOG = "/var/log/messages"
SUHOSIN_LOG = "/var/log/messages"
BIND_LOG = "/var/log/messages"
SYSLOG_LOG = "/var/log/messages"
WEBMIN_LOG = "/var/log/auth.log"

CUSTOM1_LOG = "/var/log/customlog"
CUSTOM2_LOG = "/var/log/customlog"
CUSTOM3_LOG = "/var/log/customlog"
CUSTOM4_LOG = "/var/log/customlog"
CUSTOM5_LOG = "/var/log/customlog"
CUSTOM6_LOG = "/var/log/customlog"
CUSTOM7_LOG = "/var/log/customlog"
CUSTOM8_LOG = "/var/log/customlog"
CUSTOM9_LOG = "/var/log/customlog"

# The following are comma separated lists used if LF_SELECT is enabled,
# otherwise they are not used. They are derived from the application
returned
# from a regex match in /usr/local/csf/bin/regex.pm
#
# All ports default to tcp blocks. To specify udp or tcp use the
format:
# port;protocol,port;protocol,... For example, "53;udp,53;tcp"
PORTS_pop3d = "110,995"
PORTS_imapd = "143,993"
PORTS_htpasswd = "80,443"
PORTS_mod_security = "80,443"
PORTS_mod_qos = "80,443"
PORTS_symlink = "80,443"
PORTS_suhosin = "80,443"
PORTS_cxs = "80,443"
PORTS_bind = "53;udp,53;tcp"
PORTS_ftpd = "20,21"
PORTS_webmin = "10000"
PORTS_smtpauth = "25,465,587"
PORTS_eximsyntax = "25,465,587"
```

```
# This list is replaced, if present, by "Port" definitions in
# /etc/ssh/sshd_config
PORTS_sshd = "212"

# This configuration is for use with generic Linux servers, do not
change the
# following setting:
GENERIC = "1"

# If you find ever increasing numbers of zombie lfd processes you may
need to
# revert to the old child reaper code by enabling this option
OLD_REAPER = "0"

# For internal use only. You should not enable this option as it could
cause
# instability in csf and lfd
DEBUG = "0"
###############################################################################
########
```