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 =
OffOn

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 Default: 5 [1-60]

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 = 3

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 (restricted UI item)

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 =
Off On

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 =
Off On

Allow incoming TCP ports

TCP_IN = 20,21,22,25,53,80,110,143,443,465,953,993,995,2077,2078,2082,2083,2086,2087,2095,2096,234

Allow outgoing TCP ports

TCP_OUT = 20,21,22,25,37,43,53,80,110,113,443,587,873,953,2087,2089,2703,2345,24441

Allow incoming UDP ports

UDP_IN = 20,21,53,953,2345

Allow outgoing UDP ports
To allow outgoing traceroute add 33434:33523 to this list

UDP_OUT = 20,21,53,113,123,873,953,2345,6277,24441,33434:33523

Allow incoming PING

ICMP_IN =
Off On

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 =
Off On

Set the per IP address outgoing ICMP packet rate (hits per second allowed), e.g. "1/s"

Recommend disabling on cPanel servers as cPanel uses ping test to determine fastest mirrors for various functions

To disable rate limiting set to "0"

ICMP_OUT_RATE = 1/s

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, 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 DOCKER SMTP_REDIRECT

Not supported:
ICMP_IN, ICMP_OUT

IPV6 =
Off On

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 =
Off On

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 TCP6_OUT, UDP6_OUT and ICMP6_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 =
Off On

Allow incoming IPv6 TCP ports

TCP6_IN = 22,25,53,80,110,143,443,465,587

Allow outgoing IPv6 TCP ports

TCP6_OUT = 22,25,53,80,110,113,443,587

Allow incoming IPv6 UDP ports

UDP6_IN = 53

Allow outgoing IPv6 UDP ports
To allow outgoing traceroute add 33434:33523 to this list

UDP6_OUT = 53,113

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 = eth+

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 = eth+

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 =
OffOn

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 between 300 and 3600 seconds is suggested. Set to 0 to disable

SYSLOG_CHECK = 0 Default: 0 [0 or 60-3600]

Enable this option if you do not wish to block all IP's that have authenticated using POP before SMTP (i.e. are valid clients). This option checks for IP addresses in /etc/relayhosts, which last for 30 minutes in that file after a successful POP authentication.

Set the value to 0 to disable the feature

RELAYHOSTS =
OffOn

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 =
OffOn

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 =
OffOn

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 =
OffOn

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 = 200 Default: 100 [10-1000]

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 =
Off On

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 =
Off On

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 =
Off On

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 =
Off On

Versions of iptables greater or equal to v1.4.20 should support the --wait option. This forces iptables commands that use the option to wait until a lock by any other process using iptables completes, rather than simply failing

Enabling this feature will add the --wait option to iptables commands

NOTE: The disadvantage of using this option is that any iptables command that uses it will hang until the lock is released. This could cause a cascade of hung processes trying to issue iptables commands. To try and avoid this issue csf uses a last ditch timeout, WAITLOCK_TIMEOUT in seconds, that will trigger a failure if reached

WAITLOCK = 0

WAITLOCK_TIMEOUT = 300

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 =
Off On

Enable verbose output of iptables commands

VERBOSE =
Off On

Drop out of order packets and packets in an INVALID state in iptables connection tracking

PACKET_FILTER =
Off On

Perform reverse DNS lookups on IP addresses. See also CC_LOOKUPS

LF_LOOKUPS =

OffOn

Custom styling is possible in the csf UI. See the readme.txt for more information under "UI skinning and Mobile View"

This option enables the use of custom styling. If the styling fails to work correctly, e.g. custom styling does not take into account a change in the standard csf UI, then disabling this option will return the standard UI

STYLE_CUSTOM =
OffOn

This option disables the presence of the Mobile View in the csf UI

STYLE_MOBILE =
OffOn

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 =
OffOn

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 =
OffOn

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 =
OffOn

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

Always allow the following comma separated users and groups to bypass SMTP_BLOCK

Note: root (UID:0) is always allowed

SMTP_ALLOWUSER = cpanel

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 achieve 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 =
Off On

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 =
Off On

SYNFLOOD_RATE = 4/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 =
Off On

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

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 =
Off On

Drop target for incoming iptables rules. This can be set to either DROP or 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 Default: DROP [DROP or TARPIT or REJECT]

Drop target for outgoing iptables rules. This can be set to either DROP or REJECT as with DROP, however as such connections are from this server it is better to REJECT connections to closed ports rather than to DROP them. This helps to immediately free up server resources rather than tying them up until a connection times out. It also tells the process making the connection that it has immediately failed

It is possible that some monolithic kernels may not support the REJECT target. If this is the case, csf checks before using REJECT and falls back to using DROP, issuing a warning to set this to DROP instead

DROP_OUT = REJECT

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 =
Off On

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 =
OffOn

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 =
OffOn

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

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 =
OffOn

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 = 67,68,111,113,135:139,445,513,520

Log packets dropped by the packet filtering option PACKET_FILTER
DROP_PF_LOGGING =
OffOn

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 =
OffOn

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

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 =
OffOn

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 = (restricted UI item)

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 = (restricted UI item)

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 =

Off On

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 =
Off On

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 =
Off On

LF_PERMBLOCK_INTERVAL = 86400 Default: 86400 [3600-604800]

LF_PERMBLOCK_COUNT = 4 Default: 4 [1-255]

LF_PERMBLOCK_ALERT =
Off On

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 =
Off On

LF_NETBLOCK_INTERVAL = 86400 Default: 86400 [3600-604800]

LF_NETBLOCK_COUNT = 4 Default: 4 [1-255]

LF_NETBLOCK_CLASS = C Default: C [A or B or C]

LF_NETBLOCK_ALERT =
Off On

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 =

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 =
Off On

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 Default: 0 [0-86400]

To always ignore DYNDNS IP addresses in lfd blocking, set the following option to 1

DYNDNS_IGNORE =
Off On

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 Default: 0 [0 or 60-604800]

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 Default: 600 [60-86400]

To always ignore GLOBAL_DYNDNS IP addresses in lfd blocking, set the following option to 1

GLOBAL_DYNDNS_IGNORE =
Off On

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 = 1

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 GeoLite2 Country database at:
https://dev.MaxMind.com/geoip/geoip2/geolite2/
This feature relies entirely 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. An additional option is also available if you cannot use the MaxMind databases

"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
"4" - Reports: Country Code and Country and Region and City (freegeoip.net)

Note: "4" does not use the MaxMind databases directly for lookups. Instead it uses a URL-based lookup from a third-party provider at https://freegeoip.net and so avoids having to download and process the large databases. Please visit the https://freegeoip.net and read their limitations and respect that this option will either cease to function or be removed by us if that site is abused or overloaded. ONLY use this option if you have difficulties using the MaxMind databases. This option does is ONLY for IP lookups, NOT when using the CC_* options above, which will continue to use the MaxMind databases and can ONLY be used if CC_OLDGEOLITE is set to "0"

CC_LOOKUPS = 1

The following determines whether csf uses the old and soon to be deprecated MaxMind Geolite databases or the new MaxMind Geolite2 databases

See the following link for more information:
https://support.maxmind.com/geolite-legacy-discontinuation-notice/

This option will be removed in a future version of csf and all installations

will then use the new MaxMind Geolite2 databases

Set to "1" to use the old ones, set to "0" to use the new ones

CC_OLDGEOLITE = 1

Display Country Code and Country for reported IPv6 addresses using the MaxMind Country IPv6 Database

"0" - disable
"1" - enable and report the detail level as specified in CC_LOOKUPS

This option must also be enabled to allow IPv6 support to CC_*, MESSENGER and PORTFLOOD

CC6_LOOKUPS =
Off On

This option tells lfd how often to retrieve the MaxMind GeoLite2 Country database for CC_ALLOW, CC_ALLOW_FILTER, CC_DENY, CC_IGNORE and CC_LOOKUPS (in days)

CC_INTERVAL = 7 Default: 14 [1-31]

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 Default: 0 [0-100]

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 Default: 1 [0-604800]

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 =
Off On

Send an email alert if an IP address is blocked by one of the [*] triggers

LF_EMAIL_ALERT =
Off On

[*]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 Default: 5 [0-100]

LF_SSHD_PERM = 1 Default: 1 [0-604800]

[*]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 Default: 10 [0-100]

LF_FTPD_PERM = 1 Default: 1 [0-604800]

[*]Enable login failure detection of SMTP AUTH connections

LF_SMTPAUTH = 5 Default: 5 [0-100]

LF_SMTPAUTH_PERM = 1 Default: 1 [0-604800]

[*]Enable syntax failure detection of Exim connections

LF_EXIMSYNTAX = 10 Default: 10 [0-100]

LF_EXIMSYNTAX_PERM = 1 Default: 1 [0-604800]

[*]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 = 10 Default: 10 [0-100]

LF_POP3D_PERM = 1 Default: 1 [0-604800]

[*]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 = 10 Default: 10 [0-100]

LF_IMAPD_PERM = 1 Default: 1 [0-604800]

[*]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 Default: 5 [0-100]

LF_HTACCESS_PERM = 1 Default: 1 [0-604800]

[*]Enable login failure detection of cpanel, webmail and whm connections

LF_CPANEL = 10 Default: 5 [0-100]

LF_CPANEL_PERM = 1 Default: 1 [0-604800]

[*]Enable failure detection of repeated Apache mod_security rule triggers

LF_MODSEC = 10 Default: 5 [0-100]

LF_MODSEC_PERM = 1 Default: 1 [0-604800]

[*]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 Default: 0 [0 or 60-1000]

LF_BIND_PERM = 1 Default: 1 [0-604800]

[*]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 Default: 0 [0-100]

LF_SUHOSIN_PERM = 1 Default: 1 [0-604800]

[*]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 Default: 1 [0-604800]

[*]Enable detection of repeated Apache mod_qos rule triggers

LF_QOS = 0 Default: 0 [0-100]

LF_QOS_PERM = 1 Default: 1 [0-604800]

[*]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 Default: 0 [0-100]

LF_SYMLINK_PERM = 1 Default: 1 [0-604800]

[*]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 Default: 0 [0-100]

LF_WEBMIN_PERM = 1 Default: 1 [0-604800]

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 =
OffOn

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 =
OffOn

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 =
OffOn

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 =
OffOn

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 Default: 0 [0 or 60-1000]

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 Default: 3600 [0-604800]

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

To disable set to "0"

LF_APACHE_403 = 0 Default: 0 [0 or 60-1000]

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 Default: 3600 [0-604800]

This option will keep track of the number of 401 failures in HTACCESS_LOG. If the number of hits is more than LF_APACHE_401 in LF_INTERVAL seconds then the IP address will be blocked

To disable set to "0"

LF_APACHE_401 = 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_401_PERM = 3600

This option is used to determine if the Apache error_log format contains the client port after the client IP. In Apache prior to v2.4, this was not the case. In Apache v2.4+ the error_log format can be configured using ErrorLogFormat, making the port directive optional

Unfortunately v2.4 ErrorLogFormat places the port number after a colon next to the client IP by default. This makes determining client IPv6 addresses difficult unless we know whether the port is being appended or not

lfd will attempt to autodetect the correct value if this option is set to "0" from the httpd binary found in common locations. If it fails to find a binary it will be set to "2", unless specified here

The value can be set here explicitly if the autodetection does not work:
0 - autodetect
1 - no port directive after client IP
2 - port directive after client IP

LF_APACHE_ERRPORT = 0

Send an email alert if anyone accesses WHM/cPanel via an account listed in LF_CPANEL_ALERT_USERS. An IP address will be reported again 1 hour after the last tracked access (or if lfd is restarted)

LF_CPANEL_ALERT =
Off On

If a LF_CPANEL_ALERT event is triggered, then if the following contains the path to a script, it will run the script and passed the ip and username and the DNS IP lookup result as 3 arguments

The action script must have the execute bit and interpreter (shebang) set

LF_CPANEL_ALERT_ACTION = (restricted UI item)

This is a comma separated list of accounts to send alerts for. To send an alert for all accounts set this to "all"

LF_CPANEL_ALERT_USERS = root

This settings re-enables the cPanel Bandwith chains after iptables is configured. If bandmin is not functioning, or you don't use the bandmin stats you can disable this option

LF_CPANEL_BANDMIN =
Off On

Enable scanning of the exim mainlog for repeated emails sent from scripts. To use this feature the exim log_selector option must at least be set to:

log_selector = +arguments +subject +received_recipients

If you already use extended exim logging, then you need to either include +arguments +received_recipients or use +all

This setting will then send an alert email if more than LF_SCRIPT_LIMIT lines appear with the same cwd= path in them within an hour. This can be useful in identifying spamming scripts on a server, especially PHP scripts running under the nobody account. The email that is sent includes the exim log lines and also attempts to find scripts that send email in the path that may be the culprit

LF_SCRIPT_ALERT =
Off On

The limit afterwhich the email alert for email scripts is sent. Care should be taken with this value if you allow clients to use web scripts to maintain pseudo-mailing lists which have large recipients

LF_SCRIPT_LIMIT = 100 Default: 100 [0-5000]

If an LF_SCRIPT_ALERT event is triggered, then if the following can contain the path to a script, it will be run in a child process and passed the following information as parameters which also appears in the email alert:
Path to the directory containing the script that is sending the email
Count of emails sent
Sample of the first 10 emails
List of possible email scripts within Path

The action script must have the execute bit and interpreter (shebang) set

LF_SCRIPT_ACTION = (restricted UI item)

If this option is enabled, the directory identified by LF_SCRIPT_ALERT will be chmod 0 and chattr +i to prevent it being accessed. Set the option to 1 to enable.

WARNING: This option could cause serious system problems if the identified directory is within the OS directory hierarchy. For this reason we do not recommend enabling it unless absolutely necessary.

LF_SCRIPT_PERM =
OffOn

Checks the length of the exim queue and sends an alert email if the value of settings is exceeded. If the ConfigServer MailScanner configuration is used then both the pending and delivery queues will be checked.

Note: If there are problems sending out email, this alert may not be received
To disable set to "0"

LF_QUEUE_ALERT = 2000 Default: 2000 [0-5000]

The interval between mail queue checks in seconds. This should not be set too low on servers that often have long queues as the exim binary can use significant resources when checking its queue length

LF_QUEUE_INTERVAL = 300 Default: 300 [0 or 30-86400]

This option will send an alert if the ModSecurity IP persistent storage grows excessively large: https://goo.gl/rGh5sF

More information on cPanel servers here: https://goo.gl/vo6xTE

The check is performed at lfd startup and then once per hour, the template used is modsecipdbalert.txt

LF_MODSECIPDB_FILE must be set to the correct location of the database file

Set to "0" to disable this option, otherwise it is the threshold size of the file to report in gigabytes, e.g. set to 5 for 5GB

LF_MODSECIPDB_ALERT = 5

This is the location of the persistent IP storage file on the server, e.g.:
/var/run/modsecurity/data/ip.pag
/var/cpanel/secdatadir/ip.pag
/var/cache/modsecurity/ip.pag
/usr/local/apache/conf/modsec/data/msa/ip.pag
/var/tmp/ip.pag
/tmp/ip.pag

LF_MODSECIPDB_FILE = /var/cpanel/secdatadir/ip.pag

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 Default: 300 [0 or 6-86400]

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 = 300 Default: 3600 [60-86400]

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 Default: 3600 [3600-86400]

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 =
OffOn

CloudFlare

This features provides interaction with the CloudFlare Firewall

As CloudFlare is a reverse proxy, any attacking IP addresses (so far as iptables is concerned) come from the CloudFlare IP's. To counter this, an Apache module (mod_cloudflare) is available that obtains the true attackers IP from a custom HTTP header record (similar functionality is available for other HTTP daemons

However, despite now knowing the true attacking IP address, iptables cannot be used to block that IP as the traffic is still coming from the CloudFlare servers

CloudFlare have provided a Firewall feature within the user account where rules can be added to block, challenge or whitelist IP addresses

Using the CloudFlare API, this feature adds and removes attacking IPs from that firewall and provides CLI (and via the UI) additional commands

See /etc/csf/readme.txt for more information about this feature and the restrictions for its use BEFORE enabling this feature

CF_ENABLE = 0

If the CloudFlare user plugin has been installed, enable this setting to use per cPanel account settings rather than listing each account in /etc/csf/csf.cloudflare

CF_CPANEL =

This can be set to either "block" or "challenge" (see CloudFlare docs)

CF_BLOCK = block

This setting determines how long the temporary block will apply within csf and CloudFlare, keeping them in sync

Block duration in seconds - overrides perm block or time of individual blocks in lfd for block triggers

CF_TEMP = 3600

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 Default: 300 [0 or 30-86400]

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

LF_DIRWATCH_DISABLE =
Off On

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 Default: 0 [0 or 30-86400]

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 Default: 3600 [0 or 120-86400]

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 =
Off
On

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 Default: 1 [0-604800]

Send an email alert if LF_DISTFTP is triggered

LF_DISTFTP_ALERT =
OffOn

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 Default: 1 [0-604800]

Send an email alert if LF_DISTSMTP is triggered

LF_DISTSMTP_ALERT =
OffOn

This is the interval during which a distributed FTP or SMTP attack is measured

LF_DIST_INTERVAL = 300 Default: 300 [60-86400]

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 = (restricted UI item)

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 = 180 Default: 60 [0-180]

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 Default: 0 [0-180]

Send an email alert if an account exceeds LT_POP3D/LT_IMAPD logins per hour per IP

LT_EMAIL_ALERT =
OffOn

If LF_PERMBLOCK is enabled but you do not want this to apply to LT_POP3D/LT_IMAPD, then enable this option

LT_SKIPPERMBLOCK =
OffOn

Relay Tracking

Relay Tracking. This allows you to track email that is relayed through the server. There are also options to send alerts and block external IP addresses if the number of emails relayed per hour exceeds configured limits. The blocks can be either permanent or temporary.

The following information applies to each of the following types of relay check:
RT_[relay type]_ALERT: 0 = disable, 1 = enable
RT_[relay type]_LIMIT: the limit/hour afterwhich an email alert will be sent
RT_[relay type]_BLOCK: 0 = no block;1 = perm block;nn=temp block for nn secs

This option triggers for external email

RT_RELAY_ALERT =
OffOn

RT_RELAY_LIMIT = 100 Default: 100 [2-10000]

RT_RELAY_BLOCK = 1 Default: 0 [0-604800]

This option triggers for email authenticated by SMTP AUTH

RT_AUTHRELAY_ALERT =
OffOn

RT_AUTHRELAY_LIMIT = 100 Default: 100 [2-10000]

RT_AUTHRELAY_BLOCK = 1 Default: 0 [0-604800]

This option triggers for email authenticated by POP before SMTP

RT_POPRELAY_ALERT =

OffOn

RT_POPRELAY_LIMIT = 100 Default: 100 [2-10000]

RT_POPRELAY_BLOCK = 1 Default: 0 [0-604800]

This option triggers for email sent via /usr/sbin/sendmail or /usr/sbin/exim

RT_LOCALRELAY_ALERT =
OffOn

RT_LOCALRELAY_LIMIT = 100 Default: 100 [2-10000]

This option triggers for email sent via a local IP addresses

RT_LOCALHOSTRELAY_ALERT =
OffOn

RT_LOCALHOSTRELAY_LIMIT = 100 Default: 100 [2-10000]

If an RT_* event is triggered, then if the following contains the path to a script, it will be run in a child process and passed the following: information as parameters which also appears in the email alert:
IP Address
Relay Type (RELAY/AUTHRELAY/POPRELAY/LOCALRELAY/LOCALHOSTRELAY)
Block Message (Temporary/Permanent Block)
Count of emails relayed
Sample of the first 10 emails

The action script must have the execute bit and interpreter (shebang) set

RT_ACTION = (restricted UI item)

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 Default: 0 [0 or 10-1000]

Connection Tracking interval. Set this to the the number of seconds between connection tracking scans

CT_INTERVAL = 60 Default: 30 [10-3600]

Send an email alert if an IP address is blocked due to connection tracking

CT_EMAIL_ALERT =
OffOn

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 =
OffOn

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 Default: 1800 [300-86400]

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 =
OffOn

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 =

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 Default: 60 [0-3600]

How frequently processes are checked in seconds

PT_INTERVAL = 60 Default: 60 [10-3600]

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 =
OffOn

If you want to track all linux accounts on a cPanel server, not just users
that are part of cPanel, then enable this option. This is recommended to
improve security from compromised accounts

Set to 0 to disable the feature, 1 to enable it

PT_ALL_USERS =
OffOn

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 =
Off On

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 = (restricted UI item)

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 Default: 10 [0-100]

This User Process Tracking option sends an alert if any user process exceeds the virtual memory usage set (MB). To ignore specific processes or users use csf.pignore

Set to 0 to disable this feature

PT_USERMEM = 0 Default: 256 [0-1024]

This User Process Tracking option sends an alert if any user process exceeds the RSS memory usage set (MB) - RAM used, not virtual. To ignore specific processes or users use csf.pignore

Set to 0 to disable this feature

PT_USERRSS = 0

This User Process Tracking option sends an alert if any cPanel 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 Default: 1800 [0-86400]

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 =
Off On

If you want to disable email alerts if PT_USERKILL is triggered, then set this option to 0

PT_USERKILL_ALERT =
Off On

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 = (restricted UI item)

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 Default: 30 [0-3600]

PT_LOAD_AVG = 5 Default: 5 [1 or 5 or 15]

PT_LOAD_LEVEL = 6

PT_LOAD_SKIP = 3600 Default: 3600 [1800-86400]

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/whm-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 = (restricted UI item)

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 Default: 0 [0 or 100-1000]

Terminate hung SSHD sessions. When under an SSHD login attack, SSHD processes are often left hanging after their connecting IP addresses have been blocked

This option will terminate the SSH processes created by the blocked IP. This option is preferred over PT_SSHDHUNG

PT_SSHDKILL =
Off On

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

This option is now deprecated and will be removed in the future. PT_SSHDKILL should be used instead

PT_SSHDHUNG =
Off On

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 Default: 300 [0 or 60-3600]

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 setting of 0:65535,ICMP,INVALID,OPEN,BRD 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*
BRD - include UDP Broadcast IPs, otherwise they are ignored

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 Default: 1 [1-100]

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 =
OffOn

PS_BLOCK_TIME = 3600 Default: 3600 [300-86400]

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

PS_EMAIL_ALERT =
OffOn

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 Default: 300 [0 or 60-86400]

UID_LIMIT = 10 Default: 10 [1-100]

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

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 Default: 60 [10-3600]

Send alert if a new account is created
AT_NEW =
OffOn

Send alert if an existing account is deleted
AT_OLD =
OffOn

Send alert if an account password has changed
AT_PASSWD =
OffOn

Send alert if an account uid has changed
AT_UID =
OffOn

Send alert if an account gid has changed
AT_GID =
OffOn

Send alert if an account login directory has changed
AT_DIR =
OffOn

Send alert if an account login shell has changed
AT_SHELL =
OffOn

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 =
OffOn

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 Default: 6666 [1023-65535]

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 = ******* (hidden restricted UI item)

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 = ******* (hidden restricted UI item)

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 Default: 300 [60-300]

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 Default: 1 [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 Default: 1 [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 Default: 1 [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:

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:!SSLv2

If cxs is installed then enabling this option will provide a dropdown box to switch between applications

UI_CXS = 0 (restricted UI item)

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 (restricted UI item)

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 =
Off On

Provide this service to temporary IP address blocks

MESSENGER_TEMP =
Off On

Provide this service to permanent IP address blocks

MESSENGER_PERM =
OffOn

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

Note: When using MESSENGERV2, this account must NOT be a valid cPanel account it must be created manually as explained in the csf readme.txt

MESSENGER_USER = csf

This is the maximum concurrent connections allowed to each service server

MESSENGER_CHILDREN = 10 Default: 10 [2-200]

MESSENGERV2. This option is available on cPanel servers running Apache v2.4+ under EA4.

This uses the Apache http daemon to provide the web server functionality for the MESSENGER HTML and HTTPS services. It uses a fraction of the resources that the lfd inbuilt service uses and overcomes the memory overhead of using the MESSENGER HTTPS service

MESSENGER_CHILDREN does not apply to MESSENGER HTML and HTTPS when MESSENGERV2 is enabled

For more information consult readme.txt before enabling this option

MESSENGERV2 = 0

Set this to the port that will receive the HTTPS HTML message. You should configure this port to be >1023 and different from the TEXT and HTML port. Do NOT enable access to this port in TCP_IN. This option requires the perl module IO::Socket::SSL at a version level that supports SNI (1.83+). Additionally the version of openssl on the server must also support SNI

The option uses existing SSL certificates on the server for each domain to maintain a secure connection without browser warnings. It uses SNI to choose the correct certificate to use for each client connection

Warning: On some servers the amount of memory used by the HTTPS MESSENGER service can become significant depending on various factors associated with the use of IO::Socket::SSL including the number of domains and certificates served

MESSENGER_HTTPS = 8887

This comma separated list are the HTTPS 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

Recommended setting "443" plus any end-user control panel SSL ports. So, for cPanel: "443,2083,2096"

MESSENGER_HTTPS_IN =

This option points to the file(s) containing the Apache VirtualHost SSL definitions. This can be a file glob if there are multiple files to search. Only Apache v2 SSL VirtualHost definitions are supported

MESSENGER_HTTPS_CONF = /usr/local/apache/conf/httpd.conf

This options ignores ServerAlias definitions that begin with "mail.". This can help reduce memory usage on systems that do not require the use of

MESSENGER_HTTPS on those subdomains

Set to 0 to include these ServerAlias definitions

MESSENGER_HTTPS_SKIPMAIL = 1

The following options can be specified to provide a default fallback certificate to be used if either SNI is not supported or a hosted domain does not have an SSL certificate. If a fallback is not provided, one of the certs obtained from MESSENGER_HTTPS_CONF will be used

MESSENGER_HTTPS_KEY = /var/cpanel/ssl/cpanel/mycpanel.pem

MESSENGER_HTTPS_CRT = /var/cpanel/ssl/cpanel/mycpanel.pem

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 Default: 8888 [1023-65535]

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 Default: 8889 [1023-65535]

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 activity

See the iptables man page for the correct --limit rate syntax

MESSENGER_RATE = 100/s

MESSENGER_BURST = 150

The RECAPTCHA options provide a way for end-users that have blocked themselves in the firewall to unblock themselves.

A valid Google ReCAPTCHA (v2) key set is required for this feature from: https://www.google.com/recaptcha/intro/index.html

When configuring a new reCAPTCHA API key set you must ensure that the option for "Domain Name Validation" is unticked so that the same reCAPTCHA can be used for all domains hosted on the server. lfd then checks that the hostname of the request resolves to an IP on this server

This feature requires the installation of the LWP::UserAgent perl module (see option URLGET for more details)

The template used for this feature is /etc/csf/messenger/index.recaptcha.html

Note: An unblock will fail if the end-users IP is located in a netblock, blocklist or CC_* deny entry

RECAPTCHA_SITEKEY =

RECAPTCHA_SECRET =

Send an email when an IP address successfully attempts to unblock themselves. This does not necessarily mean the IP was unblocked, only that the post-recaptcha unblock request was attempted

Set to "0" to disable

RECAPTCHA_ALERT = 1

If the server uses NAT then resolving the hostname to hosted IPs will likely not succeed. In that case, the external IP addresses must be listed as comma separated comma separated list here

RECAPTCHA_NAT =

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 = (restricted UI item)

Comma separated list of cluster member IP addresses to receive requests from

CLUSTER_RECVFROM = (restricted UI item)

IP address of the master node in the cluster allowed to send CLUSTER_CONFIG changes

CLUSTER_MASTER = (restricted UI item)

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 = (restricted UI item)

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 (restricted UI item)

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 = ******* (hidden restricted UI item)

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 =
OffOn

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 =
OffOn

Maximum number of child processes to listen on. High blocking rates or large clusters may need to increase this
CLUSTER_CHILDREN = 10 Default: 10 [1-100]

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 =
OffOn

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 =
OffOn

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 =
OffOn

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 Default: hourly [hourly or daily or manual]

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 =
OffOn

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 Default: 5000 [1000-100000]

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 =
OffOn

This option determines how many iptables log lines to store for reports

ST_IPTABLES = 100 Default: 100 [10-1000]

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 =
OffOn

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 =
OffOn

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 Default: 30 [7-366]

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 =
OffOn

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 (restricted UI item)

ST_MYSQL_PASS = (restricted UI item)

ST_MYSQL_HOST = localhost (restricted UI item)

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

ST_APACHE =
OffOn

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 =
OffOn

The number of minutes that elapse between tests. Default is 5, minimum is 1.

ST_DISKW_FREQ = 5 Default: 5 [1-1440]

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=/etc/csf/dd_test bs=1MB count=64 conv=fdatasync (restricted UI item)

Docker Settings

NOTE: This feature is currently in BETA testing, so may not work correctly

This section provides the configuration of iptables rules to allow Docker containers to communicate through the host. If the generated rules do not work with your setup you will have to use a /etc/csf/csfpost.sh file and add your own iptables configuration instead

1 to enable, 0 to disable

DOCKER = 0

The network device on the host

DOCKER_DEVICE = docker0

Docker container IPv4 range

DOCKER_NETWORK4 = 172.17.0.0/16

Docker container IPv6 range. IPV6 must be enabled and the IPv6 nat table available (see IPv6 section). Leave blank to disable

DOCKER_NETWORK6 = 2001:db8:1::/64

OS Specific Settings

Binary locations

IPTABLES = /sbin/iptables (restricted UI item)

IPTABLES_SAVE = /sbin/iptables-save (restricted UI item)

IPTABLES_RESTORE = /sbin/iptables-restore (restricted UI item)

IP6TABLES = /sbin/ip6tables (restricted UI item)

IP6TABLES_SAVE = /sbin/ip6tables-save (restricted UI item)

IP6TABLES_RESTORE = /sbin/ip6tables-restore (restricted UI item)

MODPROBE = /sbin/modprobe (restricted UI item)

IFCONFIG = /sbin/ifconfig (restricted UI item)

SENDMAIL = /usr/sbin/sendmail (restricted UI item)

PS = /bin/ps (restricted UI item)

VMSTAT = /usr/bin/vmstat (restricted UI item)

NETSTAT = /bin/netstat (restricted UI item)

LS = /bin/ls (restricted UI item)

MD5SUM = /usr/bin/md5sum (restricted UI item)

TAR = /bin/tar (restricted UI item)

CHATTR = /usr/bin/chattr (restricted UI item)
UNZIP = /usr/bin/unzip (restricted UI item)
GUNZIP = /bin/gunzip (restricted UI item)
DD = /bin/dd (restricted UI item)
TAIL = /usr/bin/tail (restricted UI item)
GREP = /bin/grep (restricted UI item)
ZGREP = /usr/bin/zgrep
IPSET = /usr/sbin/ipset (restricted UI item)
SYSTEMCTL = /usr/bin/systemctl (restricted UI item)
HOST = /usr/bin/host (restricted UI item)
IP = /sbin/ip (restricted UI item)

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 = /usr/local/apache/logs/error_log (restricted UI item)
MODSEC_LOG = /usr/local/apache/logs/error_log (restricted UI item)
SSHD_LOG = /var/log/secure (restricted UI item)
SU_LOG = /var/log/secure (restricted UI item)
FTPD_LOG = /var/log/messages (restricted UI item)
SMTPAUTH_LOG = /var/log/exim_mainlog (restricted UI item)
SMTPRELAY_LOG = /var/log/exim_mainlog (restricted UI item)
POP3D_LOG = /var/log/maillog (restricted UI item)
IMAPD_LOG = /var/log/maillog (restricted UI item)
CPANEL_LOG = /usr/local/cpanel/logs/login_log (restricted UI item)
CPANEL_ACCESSLOG = /usr/local/cpanel/logs/access_log (restricted UI item)
SCRIPT_LOG = /var/log/exim_mainlog (restricted UI item)
IPTABLES_LOG = /var/log/messages (restricted UI item)
SUHOSIN_LOG = /var/log/messages (restricted UI item)
BIND_LOG = /var/log/messages (restricted UI item)
SYSLOG_LOG = /var/log/messages (restricted UI item)
WEBMIN_LOG = /var/log/secure (restricted UI item)

CUSTOM1_LOG = /var/log/messages (restricted UI item)
CUSTOM2_LOG = /var/log/messages (restricted UI item)
CUSTOM3_LOG = /var/log/messages (restricted UI item)
CUSTOM4_LOG = /var/log/messages (restricted UI item)

CUSTOM5_LOG = /var/log/messages (restricted UI item)

CUSTOM6_LOG = /var/log/messages (restricted UI item)

CUSTOM7_LOG = /var/log/messages (restricted UI item)

CUSTOM8_LOG = /var/log/messages (restricted UI item)

CUSTOM9_LOG = /var/log/messages (restricted UI item)

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 (restricted UI item)

PORTS_imapd = 143,993 (restricted UI item)

PORTS_htpasswd = 80,443 (restricted UI item)

PORTS_mod_security = 80,443 (restricted UI item)

PORTS_mod_qos = 80,443 (restricted UI item)

PORTS_symlink = 80,443 (restricted UI item)

PORTS_suhosin = 80,443 (restricted UI item)

PORTS_cxs = 80,443 (restricted UI item)

PORTS_bind = 53 (restricted UI item)

PORTS_ftpd = 20,21 (restricted UI item)

PORTS_webmin = 10000 (restricted UI item)

PORTS_cpanel = 2077,2078,2082,2083,2086,2087,2095,2096 (restricted UI item)

This list is extended, if present, by the ports defined by /etc/chkservd/exim-*

PORTS_smtpauth = 25,465,587 (restricted UI item)

PORTS_eximsyntax = 25,465,587 (restricted UI item)

This list is replaced, if present, by "Port" definitions in /etc/ssh/sshd_config

PORTS_sshd = 22 (restricted UI item)

For internal use only. You should not enable this option as it could cause instability in csf and lfd

DEBUG = 0 (restricted UI item)

Show All Prev Next

Change

Return

csf: v12.01