

Installing CSF Firewall Asterisk Based Systems

I have been using CSF firewall for a number of years with all flavours of asterisk and touch wood none have ever been compromised. This is not a complete Guide but will get your system locked down

Firstly we need to install Webmin and CSF so log into console.

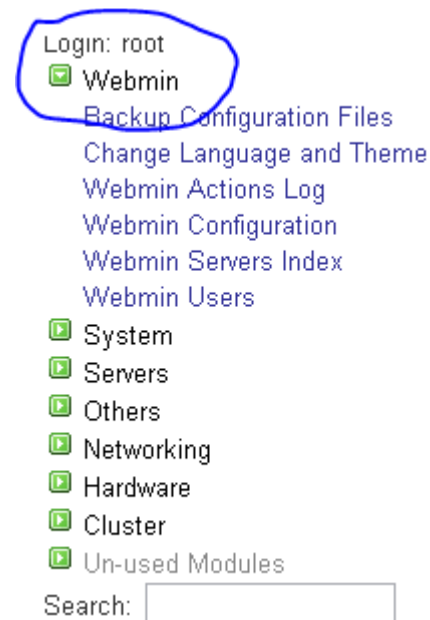
```
wget http://prdownloads.sourceforge.net/webadmin/webmin-1.580-1.noarch.rpm  
rpm -U webmin-1.580-1.noarch.rpm
```

Now we will do CSF while we are in console.

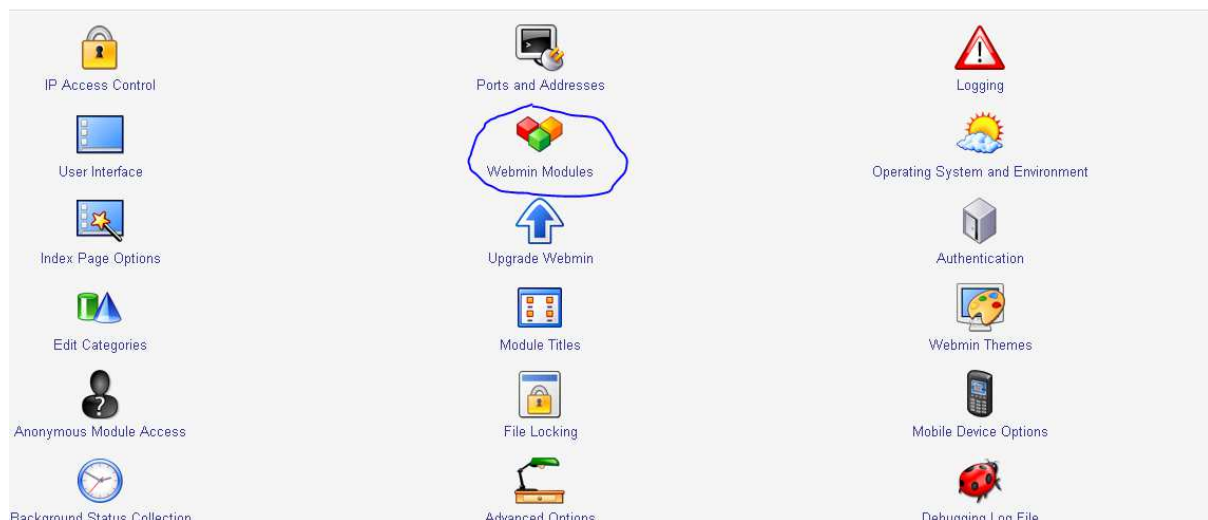
```
wget http://www.configserver.com/free/csf.tgz  
tar xzf csf.tgz  
cd csf  
sh install.sh
```

If all that went smooth we need to now log into Webmin from your web browser
<https://your server ip:10000/>

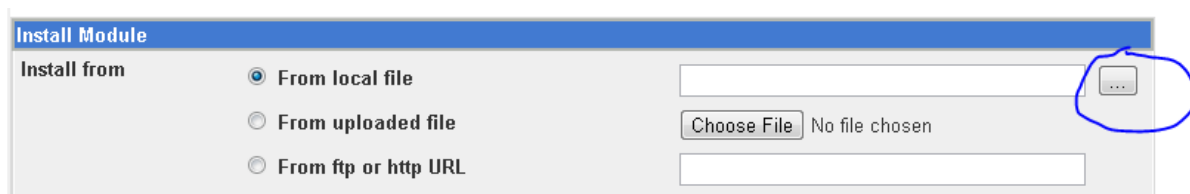
User will be root and whatever pass you set
Now we need to install the CSF Gui into Webmin



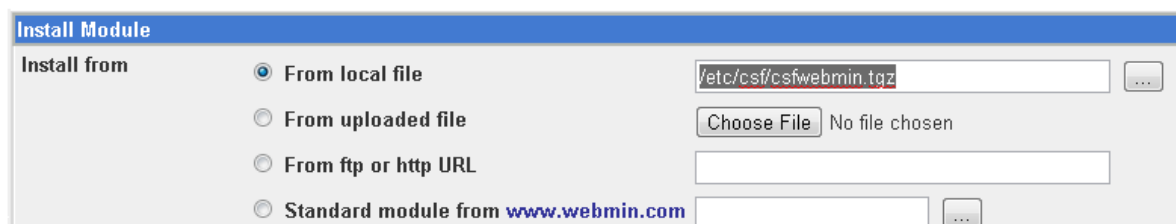
Click on Webmin as seen above, you will then see



Click on Webmin modules This will allow us to install module



Click to browse for the file



If you wish just copy this path and paste it in /etc/csf/csfwebmin.tgz

Now just click install and leave everything as defaults, when done you will now see under system in Webmin

```

Login: root
[+] Webmin
[+] System
    Bootup and Shutdown
    Change Passwords
    ConfigServer Security & Firewall
    Disk Quotas
    Disk and Network Filesystems
    Filesystem Backup
    Initial System Bootup
    Log File Rotation
    M4M5 Tools
  
```

Click on Configserver



ConfigServer
Security &
Firewall

ConfigServer Security & Firewall - csf v5.48

Firewall Status: Enabled and Running

Server Security Information

Check Server Security	Perform a basic security, stability and settings check on the server
Firewall Information	View the csf-lfd readme.txt file
View iptables Rules	Display the active iptables rules
View lfd Log	View the last <input type="text" value="30"/> lines of the Login Failure Daemon (lfd) log file and <input type="checkbox"/> auto-refresh the log view
View iptables Log	View the last 100 iptables log lines

Upgrade

You are running the latest version of csf. An Upgrade button will appear here if a new version becomes available

csf - ConfigServer Firewall

Firewall Security Level	Pre-configured settings for Low, Medium or High firewall security
Firewall Configuration	Edit the configuration file for the csf firewall and lfd
Quick Allow	Allow IP address <input type="text" value=""/> through the firewall and add to the allow file (csf.allow)
Quick Deny	Block IP address <input type="text" value=""/> in the firewall and add to the deny file (csf.deny)
Quick Ignore	Ignore IP address <input type="text" value=""/> in lfd, add to the ignore file (csf.ignore) and restart lfd
Firewall Allow IPs	Edit csf.allow, the IP address allow file
Firewall Deny IPs	Edit csf.deny, the IP address deny file (Currently: 13 permanent IP bans)
Firewall Enable	Enables csf and lfd if previously Disabled
Firewall Disable	Completely disables csf and lfd
Firewall Restart	Restart the csf iptables firewall

Now we get down to the Nitty gritty of setting our firewall up, you will need to add your local ip range into the allow field and click allow to add it

```
# 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 =

```
# 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 = Default: 5 [1-60]

```
# 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. Updates do not overwrite configuration
# files or email templates. An email will be sent to the root account if an
# update is performed
#
# You should check for new version announcements at http://blog.configserver.com
```

AUTO_UPDATES = Default: 1 [0-1]

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

```
# Allow incoming TCP ports
```

TCP_IN =

```
# Allow outgoing TCP ports
```

TCP_OUT =

```
# Allow incoming UDP ports
```

UDP_IN =

```
# Allow outgoing UDP ports
```

```
# To allow outgoing traceroute add 33434:33523 to this list
```

UDP_OUT =

Set testing to "0" this will enable the firewall out of test mode

Remove inbound ports in TCP and also UDP leave blank, this will stop anyone connecting to your system unless you allow the IP

In UDP outbound I added 1000:65000 just for ease, it doesn't really matter as nothing can connect until I allow it

[Show All](#) [Prev](#) Global Lists/DYNDNS/Blacklists [Next](#)

#####

#####

- - - - -

Next this is if you use DynDNS names for remote extensions with dynamic IP's , set DynDNS to 300 to check for change of address

Also set `DYNDNS_IGNORE = 1` this will ignore dynDNS names and allow them through
Next you really should disable this unless you want thousand of emails

```
#####
# SECTION:Directory Watching & Integrity
#####
# Enable Directory Watching. This enables lfd to check /tmp and /dev/shm
# directories for suspicious files, i.e. script exploits. If a suspicious
# file is found an email alert is sent. One alert per file per LF_FLUSH
# interval is sent
#
# To enable this feature set the following to the checking interval in seconds.
# To disable set to "0"
LF_DIRWATCH =  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
# /etc/csf/suspicious.tar
LF_DIRWATCH_DISABLE =  Default: 0 [0-1]

# 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 =  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 =  Default: 3600 [0 or 120-86400]
```

Next 1 to disable is process tracking or you will get flooded with mail

```
# 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 =  Default: 60 [0-3600]
```

```
# How frequently processes are checked in seconds
```

```
PT_INTERVAL =  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 =  Default: 0 [0-1]
```

That is all that is needed to lock down your asterisk system, so any SIP trunks or remote connections you will need to add into the allow list

This is a quick rundown so if anyone finds errors or has any suggestions feel free to contact me and I will try to respond when I get some time

dave@itshack.com.au

DaveD