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
```

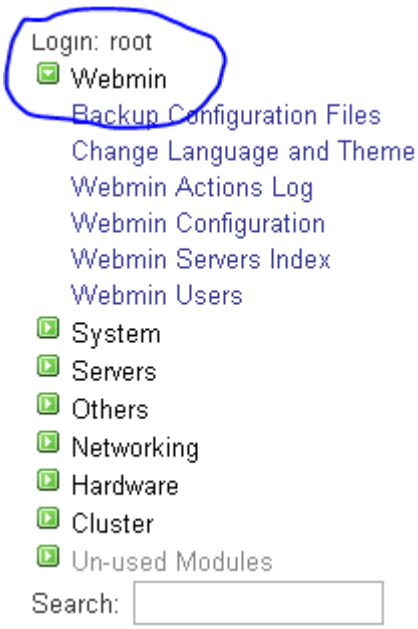
```
rpm -U webmin-1.580-1.noarch.rpm
```

Now we will do CSF while we are in console.

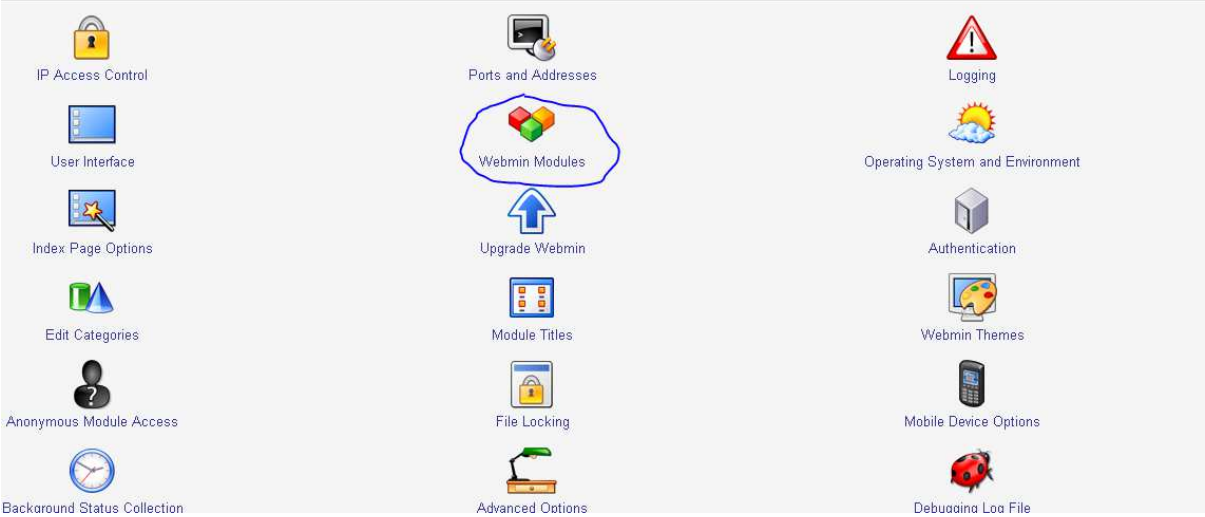
```
wget http://www.configserver.com/free/csf.tgz
tar zxf csf.tgz
cd csf
sh install.sh
```

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

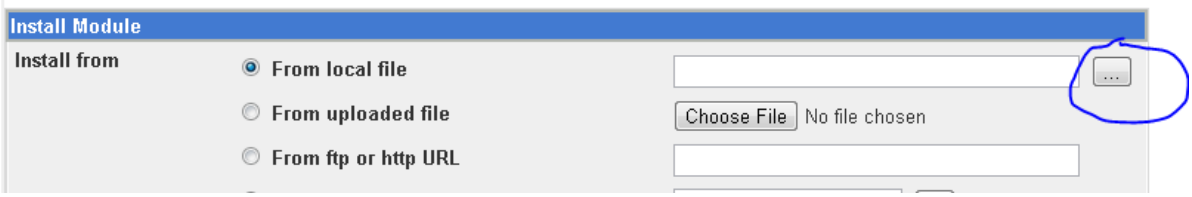
User will be root and whatever pass you set
Now we need to install the CSF Gui into Webmin



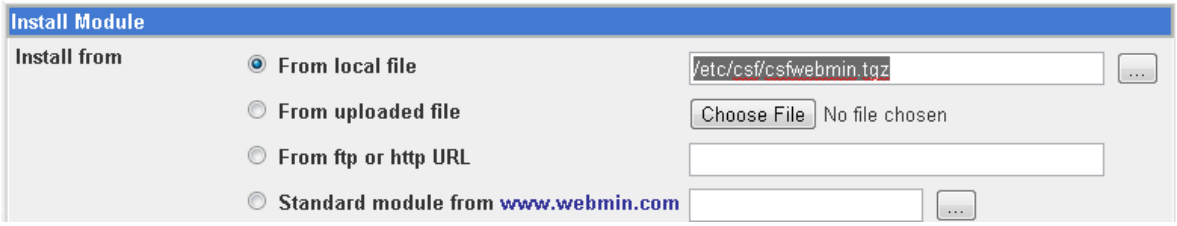
Click on Webmin as seen above, you will then see



Click on Webmin modules This will allow us to install module



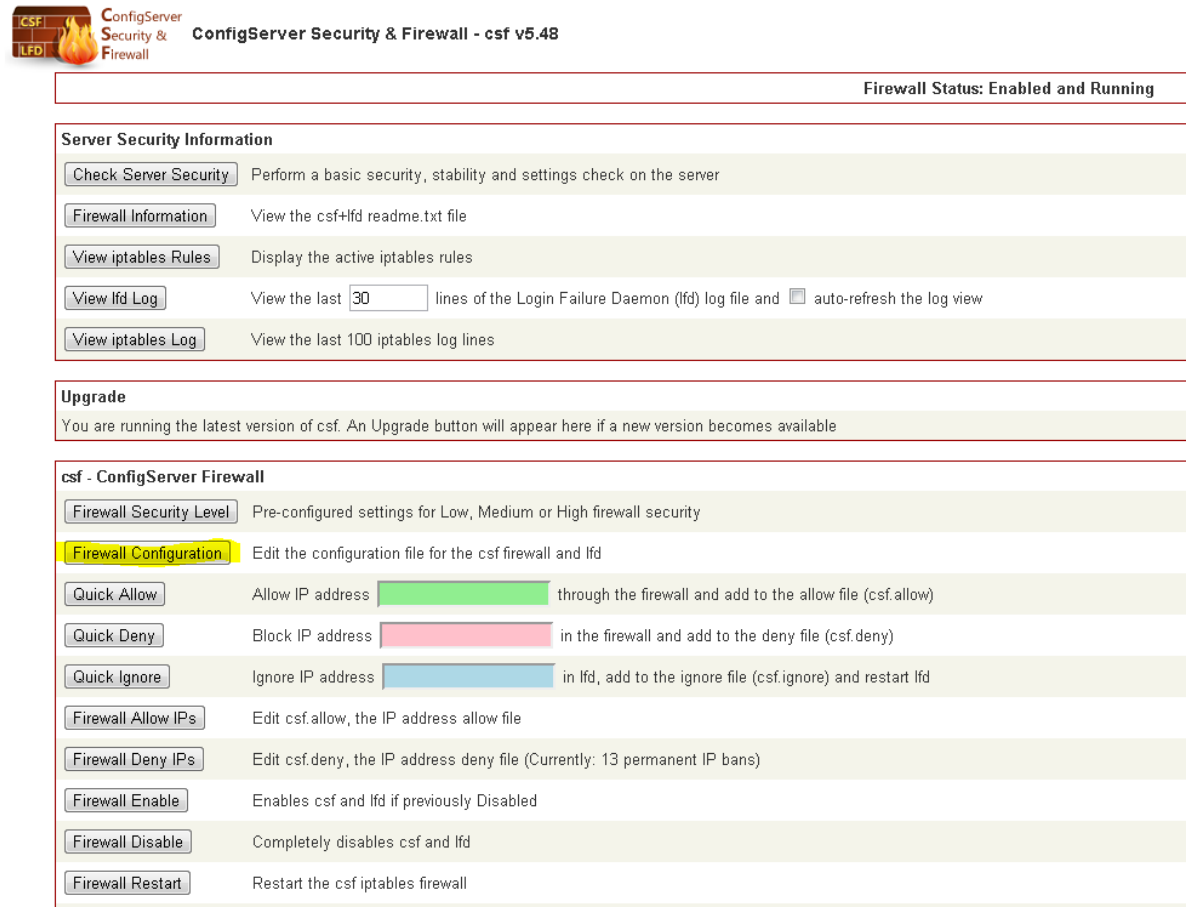
Click to browse for the file



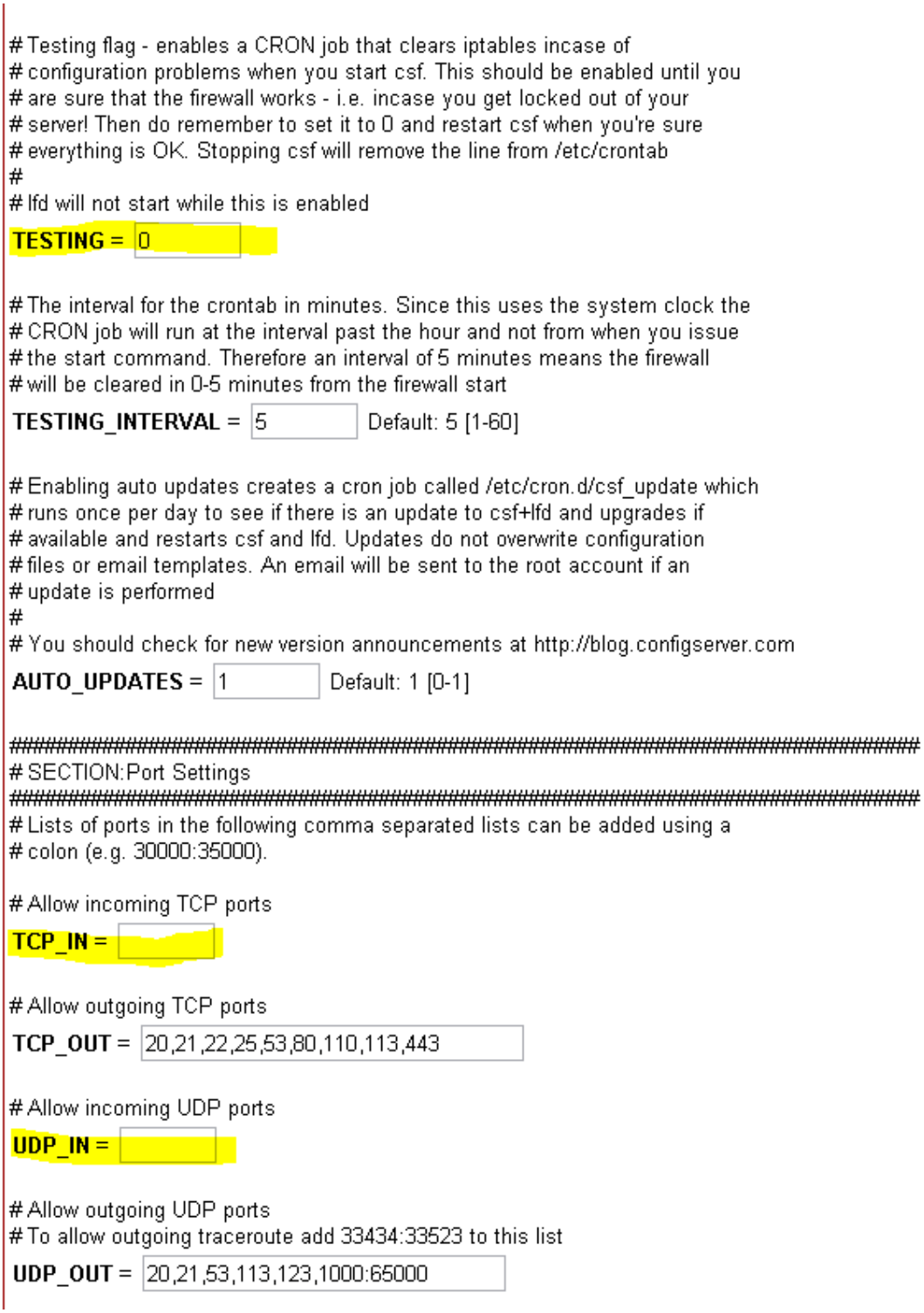
If you wish just copy this path and paste it in /etc/csf/csfwebmin.tgz

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

Click on Configserver



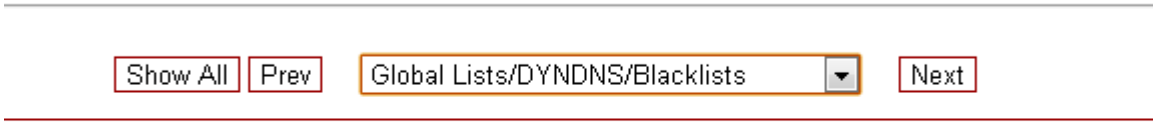
Now we get down to the Nitty gritty of setting our firewall up, you will need to add your local ip range into the allow field and click allow to add it



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



#########

#########

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

Show /

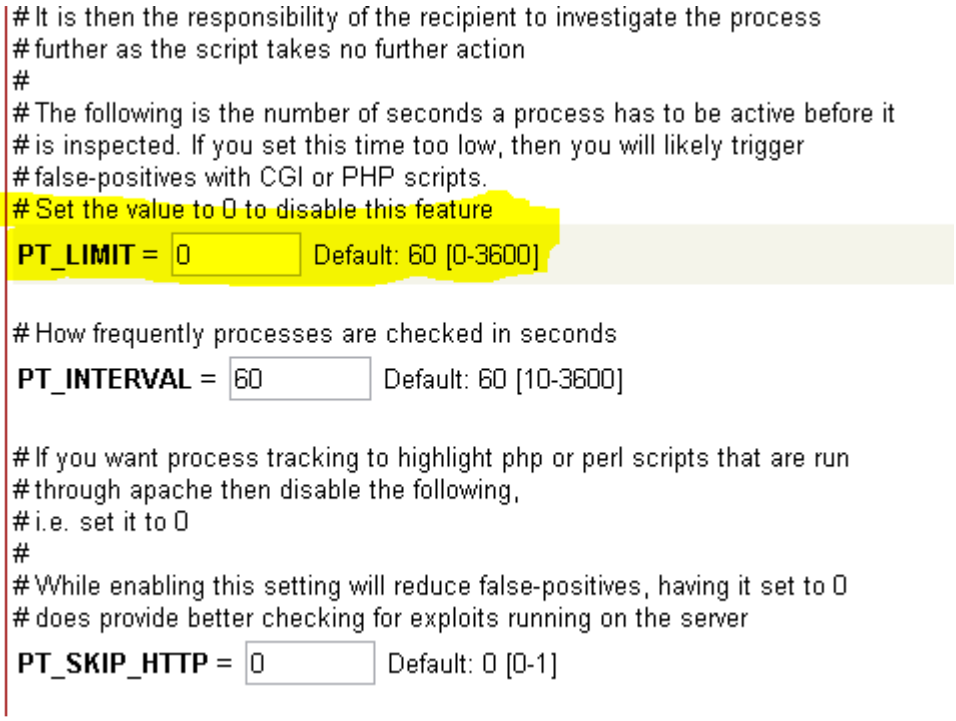
```
###############################################################################
# SECTION:Directory Watching & Integrity
###############################################################################
# Enable Directory Watching. This enables lfd to check /tmp and /dev/shm
# directories for suspicious 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 = 0  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 = 0  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 = 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 = 0  Default: 3600 [0 or 120-86400]
```

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



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