

## Set Up Gateway Level Virus Security With ClamAV And SafeSquid Proxy

*By Sean*

Published: 2008-03-17 17:51

# Set Up Gateway Level Virus Security With ClamAV And SafeSquid Proxy

In an earlier HowTo ['Deploying A Content Filtering Proxy Server To Distribute Controlled Internet Access With SafeSquid'](#), I had explained the procedure for installing Content Filtering Proxy - [SafeSquid](#). In this HowTo, I will explain how you can secure your network from virus and other malware, by installing [ClamAV](#) and integrating it with SafeSquid, to scan all in-coming content for virus, and block all infected content at the HTTP Gateway, even before it enters your network.

## Virus Security In SafeSquid

SafeSquid has built-in connectivity to various daemon based anti virus software like [ClamAV](#), Sophos, Avast, F-Prot, NOD32 and Kaspersky. It also has a universal ICAP (Internet Content Adaptation Protocol) client that can be used to connect to ICAP based security software like [Dr.Web ICAP](#), [Kaspersky Antivirus for Proxy Server](#), [Trend Micro InterScan WebSecurity](#) and [Symantec Scan Engine](#).

You can even use multiple anti virus software with SafeSquid to simultaneously scan in-coming content. This does not cause any significant latency, since SafeSquid has a multi-threaded architecture.

## Installing ClamAV And Integrating With SafeSquid

Change directory to `/usr/local/src`:

```
cd /usr/local/src
```

Download ClamAV:

```
wget -nd http://freshmeat.net/redirect/clamav/29355/url_tgz/clamav-0.91.tar.gz
```

Decompress the tar file using command:

```
tar -xvzf clamav-0.91.tar.gz
```

Add user 'clamav':

```
useradd clamav
```

Change to 'clamav-0.91' directory:

```
cd clamav-0.91/
```

Install clamav:

```
./configure && make && make install
```

After the installation is complete, copy "contrib/init/RedHat/clamd" file to "/etc/init.d/":

```
cp contrib/init/RedHat/clamd /etc/init.d/clamd
```

Configure clamav to auto-run on startup:

```
chkconfig --add clamd
```

Edit clamd.conf and comment the line 'EXAMPLE':

```
vi /usr/local/etc/clamd.conf
```

```
EXAMPLE => # EXAMPLE
```

Edit `freshclam.conf` and comment the line 'EXAMPLE':

```
vi /usr/local/etc/freshclamd.conf
```

```
EXAMPLE => # EXAMPLE
```

Run `freshclam` to update database:

```
freshclam -v
```

The output should be similar to -

```
Current working dir is /usr/local/share/clamav
Max retries == 3
ClamAV update process started at Mon Mar 10 03:11:09 2008
Querying current.cvd.clamav.net
TTL: 208
Software version from DNS: 0.92.1
DON'T PANIC! Read http://www.clamav.net/support/faq
main.cvd version from DNS: 45
main.inc is up to date (version: 45, sigs: 169676, f-level: 21, builder: sven)
daily.cvd version from DNS: 6189
Downloading daily.cvd [10%...]
daily.cvd is up to date (version: 6190, sigs: 59083, f-level: 26, builder: ccordes)
```

Add a cron job for daily auto update:

```
vi /etc/crontab
```

Add the following lines to run freshclam daily at 10 hours:

```
00 10 * * * root /usr/local/bin/freshclam
```

Start Clamav daemon:

```
/etc/init.d/clamd start
```

Check status:

```
/etc/init.d/clamd status
```

The output should be similar to -

```
clamd (pid 1525) is running...
```

So now your ClamAV daemon is up and running. The next step is to configure SafeSquid to use ClamAV daemon.

Check the socket path of ClamAV:

```
netstat -lnp | grep clamd
```

Check for this output -

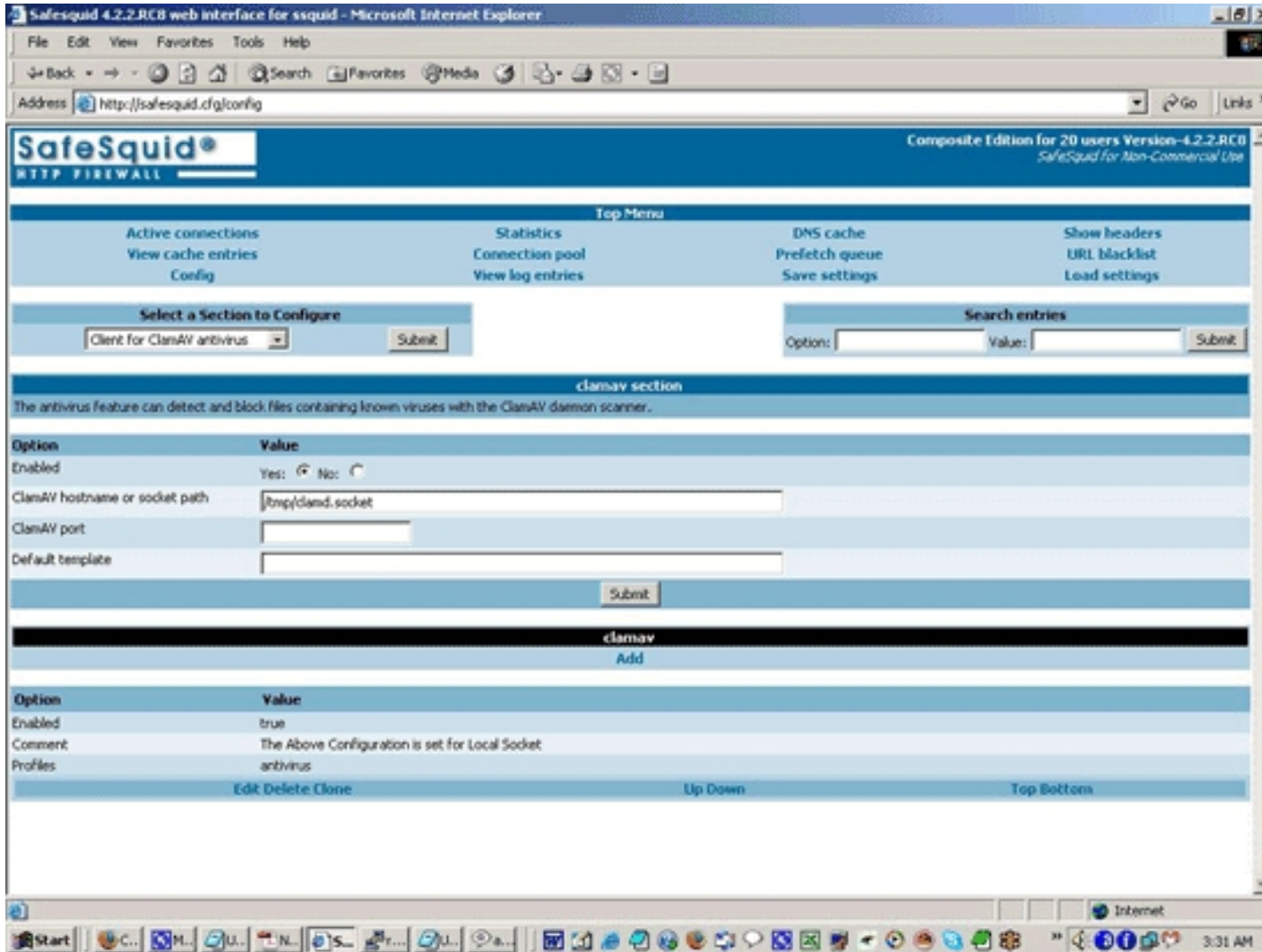
```
'unix 2 [ ACC ] STREAM LISTENING 29235 5643/clamd /tmp/clamd.socket'
```

So the socket path is `/tmp/clamd.socket`.

Open the SafeSquid Web Interface, click on 'Config' in the main menu, select 'Client for ClamAV Antivirus' and click on 'Submit' to open ClamAV section. Normally you will find this section already configured with a default rule, but disabled (Enabled = No). You only have to enable this section ( Enable = Yes)

It should have the following setting. If not, then edit accordingly:

```
'clamav section'  
Enabled = Yes  
ClamAV hostname or socket path = /tmp/clamd.socket  
  
'clamav sub-section'  
Enabled = Yes  
Profiles = antivirus (this profile is defined in 'Profiles' section, which is generated by another profile 'application-filter', which defines the type of files to be scanned)
```



The screenshot shows the SafeSquid web interface in Microsoft Internet Explorer. The browser address bar shows <http://safesquid.cgi/config>. The page title is "SafeSquid Composite Edition for 20 users Version-4.2.2-RCB". The interface includes a top menu with options like "Active connections", "Statistics", "DNS cache", and "Show headers". A "Select a Section to Configure" dropdown menu is set to "Client for ClamAV antivirus". The "clamav section" is expanded, showing a table of configuration options:

Option	Value
Enabled	Yes: <input checked="" type="radio"/> No: <input type="radio"/>
ClamAV hostname or socket path	<input type="text" value="/tmp/clamd.socket"/>
ClamAV port	<input type="text"/>
Default template	<input type="text"/>

Below the configuration table, there is a "clamav" section with a table of installed entries:

Option	Value
Enabled	true
Comment	The Above Configuration is set for Local Socket
Profiles	antivirus

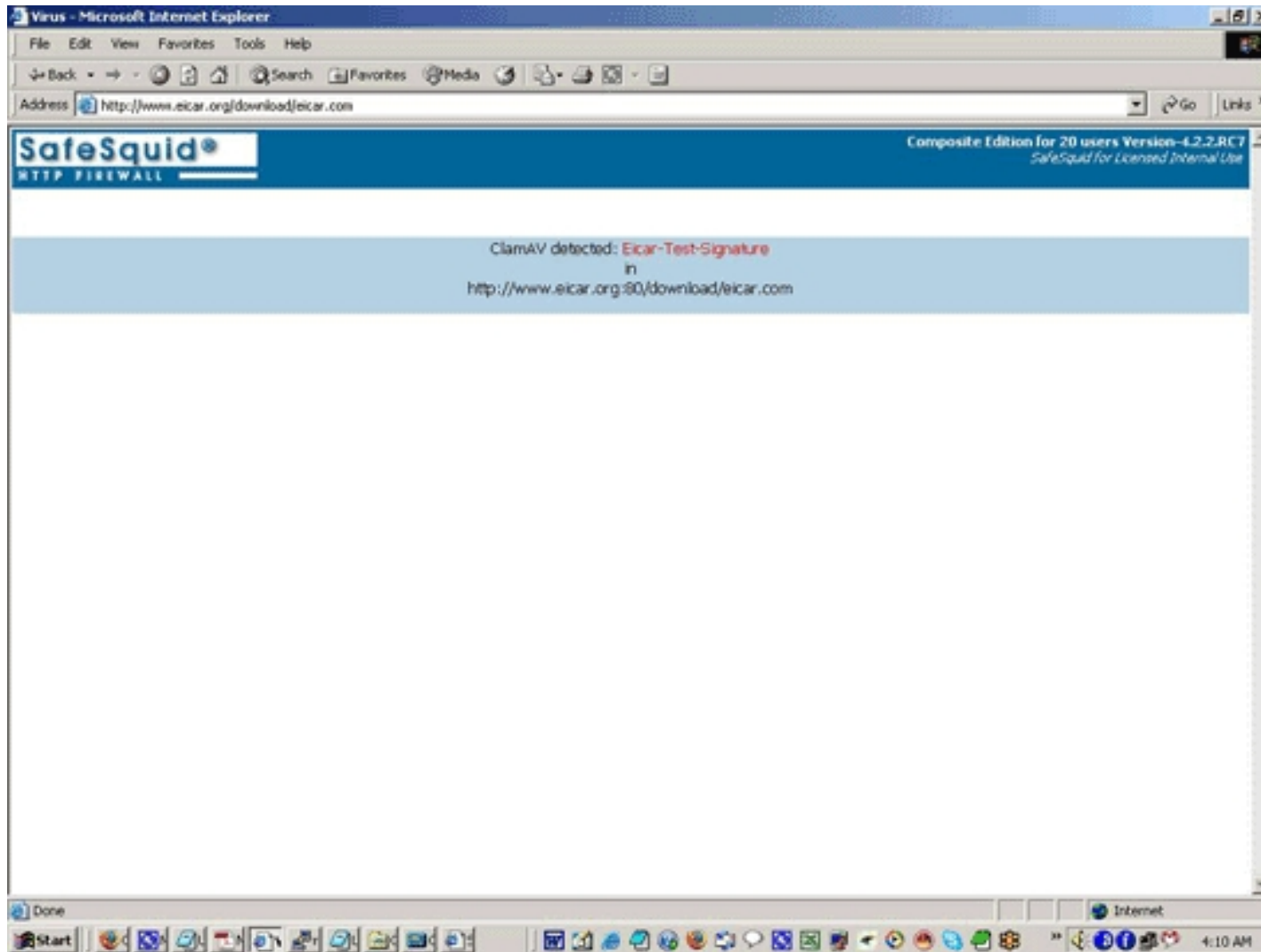
At the bottom of the clamav section, there are buttons for "Edit", "Delete", "Clone", "Up Down", and "Top Bottom". The Windows taskbar at the bottom shows the time as 3:31 AM.

## ClamAV Section In SafeSquid Web Interface

To test your installation, visit [http://eicar.org/anti\\_virus\\_test\\_file.htm](http://eicar.org/anti_virus_test_file.htm) and scroll down to "Download area using the standard protocol http". Click on the

files listed under this section. You should get a message -

```
ClamAV detected: Eicar-Test-Signature  
in  
http://www.eicar.org:80/download/eicar.com
```



EICAR Antivirus Test Page

Congratulations!



You have just set up the first layer of security from virus and malware for your network.