By Sean
Published: 2008-06-02 10:57

How To Control Download Of Files And Mime Types In SafeSquid Proxy Server

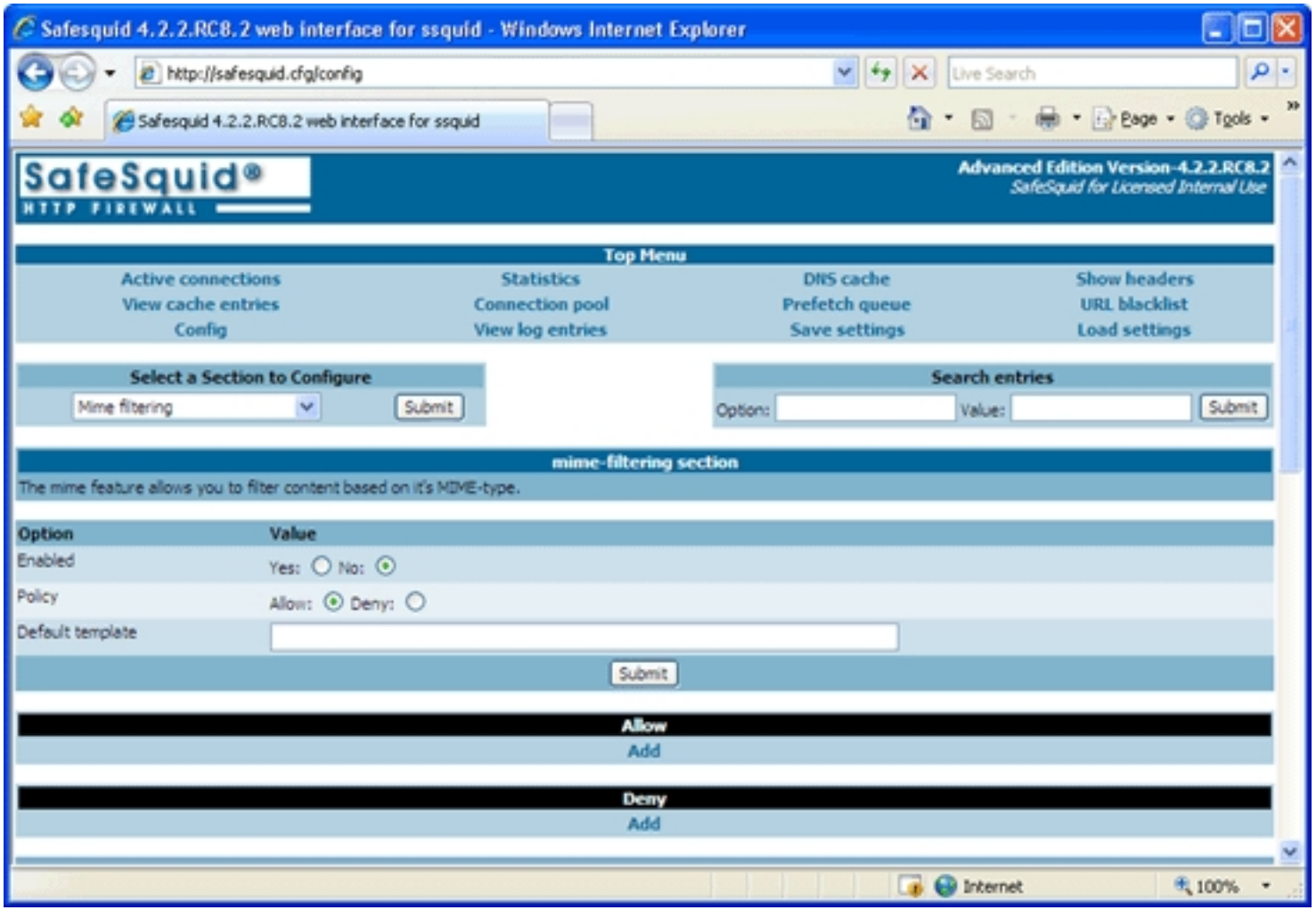
Administrators regularly find themselves in troubled situations, when irresponsible users waste their productive time and Internet bandwidth, on online music, radio, video or downloading large, non-productive contents. They also, knowingly or unknowingly, put other serious users to inconvenience and put the network at risk. Administrators can avoid such situations by controlling what content is allowed or denied, and when.

SafeSquid has a unique *MimeFilter*. *Mime Filter* allows you to create rules that define the nature of thecontent that may be accessed from the Internet. You can create rules for generically blocking or allowing any content that is application, audio, image, message, model, multipart, text, video, as per IANA standards. You can also - implement your own standards or; create rules for a specific file-type.

In this tutorial I will explain howyou can block access to specific files using *Mime filter*.In my earlier tutorials, I have already explained how to create user, group andapplication profiles. So I will not go into details about profiles, and assumethat the reader already knows about profiles. Readers who are not aware ofprofiles, can refer to the earlier tutorials from the list at the bottom of thistutorial.

Open the SafeSquid Web Interface and go to *Config* => *Mime filtering*

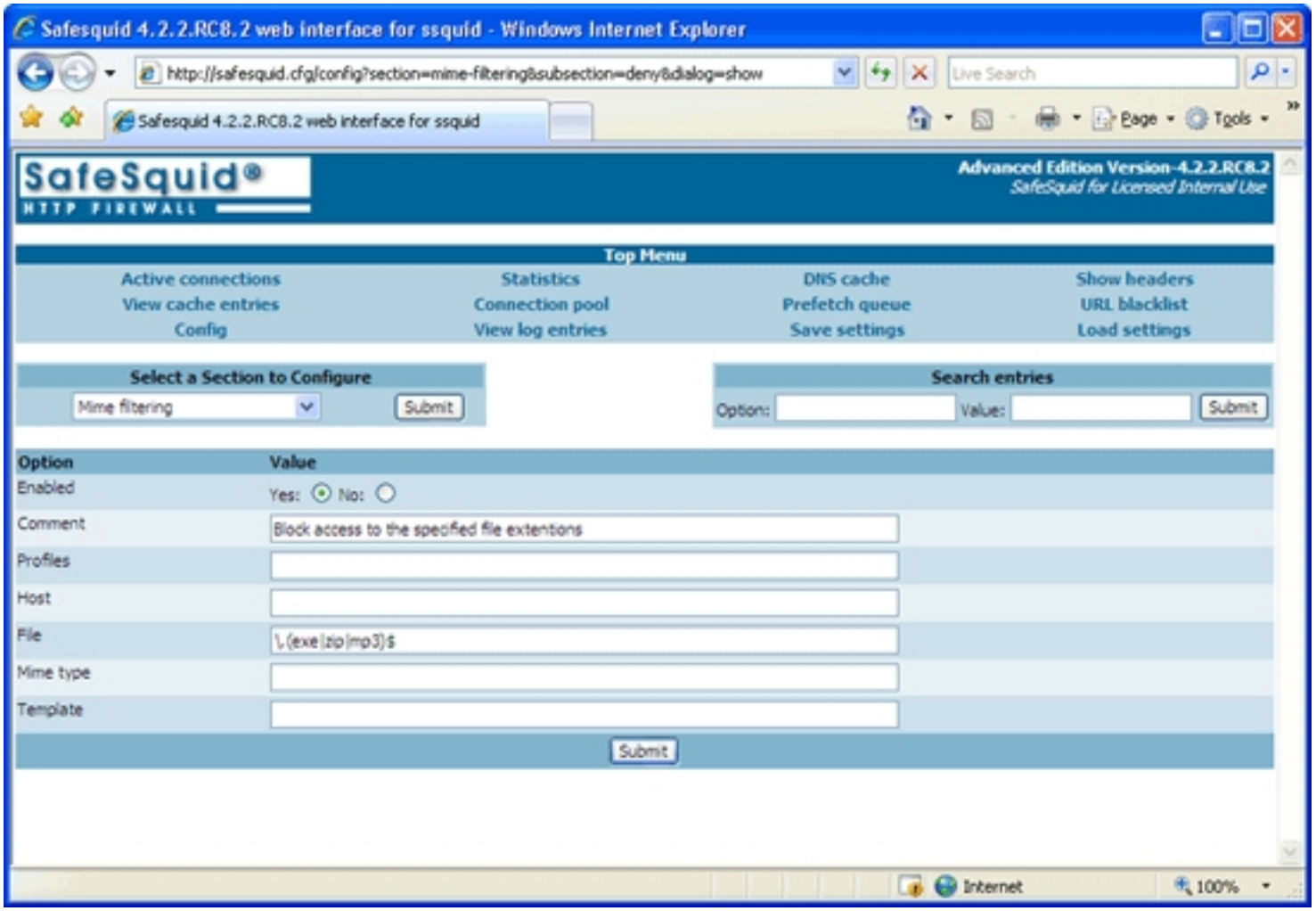
You will see a screen similar to this:



Mime Filtering Section

Like all other sections, `Mime filtering` can alsobe enabled or disabled by setting `Enabled` to `Yes`or `No` respectively. Enable the section if it is disabled. When the Policy is Allow, all file-types or mime-types are allowed, and youdefine what is to be blocked under the Deny sub-section. When the Policy is Deny, all file-types or mime-types are denied, and you definewhat is to be allowed under the Allow sub-section. We will leave the Policy to Allow.

To block access to files based on their extensions, click on Add under theDeny sub-section. The following figure shows the screen that appears -



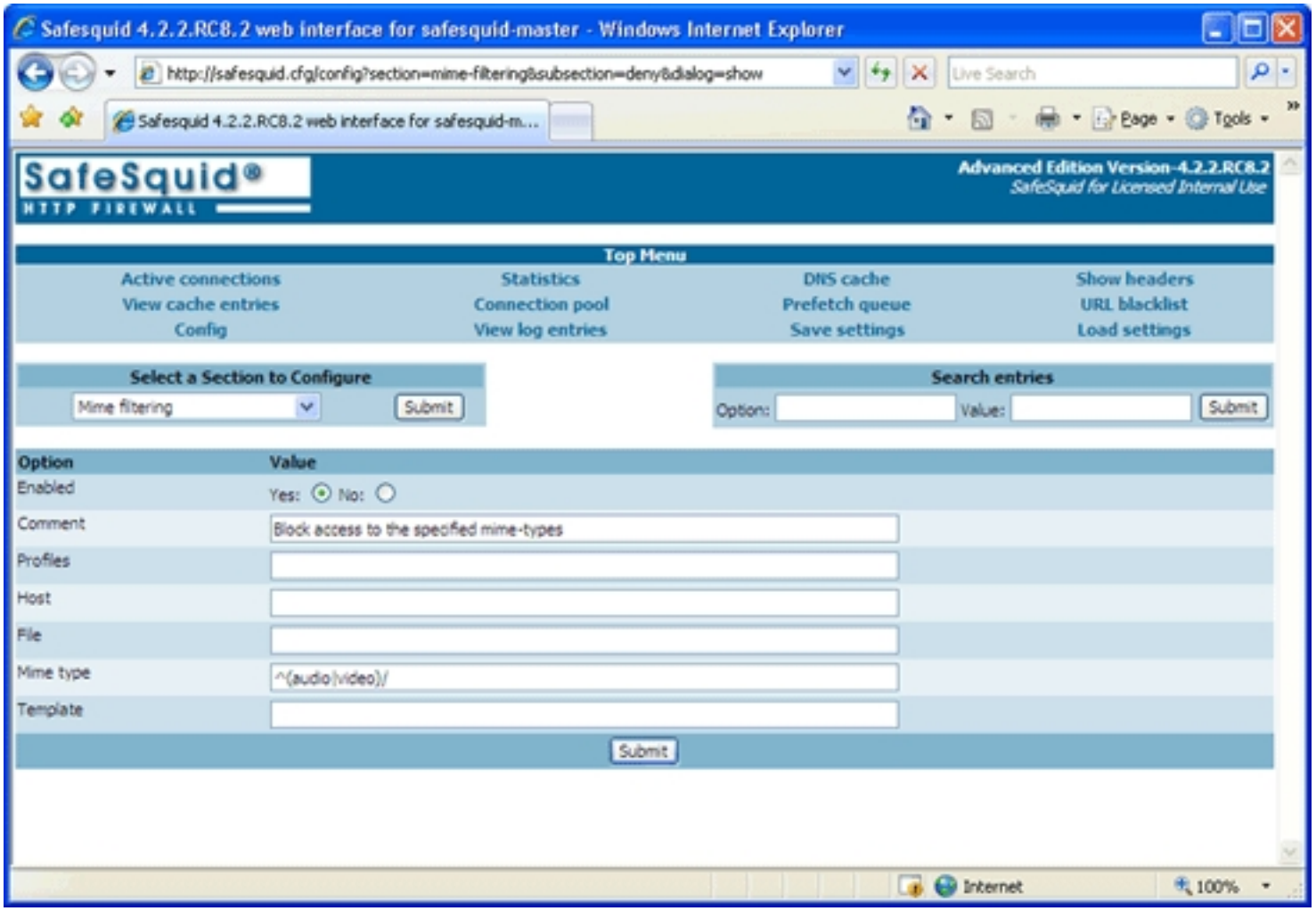
Adding file extentions in Mime Filtering

Simply fill in the fields as they appear in the figure, replacing the fileextensions with the once that you would like to block access to. If you wouldlike to apply this rule to only specific users / groups, mention their userprofile in the `Profiles` field. If you leave the `Profiles`field blank, the rule will apply to all users.

If you would like to deny access to the specified file types only fromspecific websites, then type list of websites in the `Host`field, in this format -

```
(orkut.com|flixster.com|youtube.com)
```

Similarly, to block access to files based on their mime-type, fill in the Mimetype field as shown in the figure below -.



Adding mime-type in Mime Filtering

For a list of mime-types, see **http://www.w3schools.com/media/media_mimeref.asp**

To create a more comprehensive rule, you can use the `Profiles`section to create a profile, and then use it in the `Mimefiltering section`, to take desired action. For example, if you wanted to block all audio & video files during office hours (0900-1700), and allow access during lunch (1300-1400), before and after office hours, you could create the following profiles:

Option

Value

Enabled

true

Comment

Block Audio & Video Content during office hours - 1st half

Mime type

^(audio|video)/

Hour range

9,13

Time match mode

absolutetime

Added profiles

block-audio-video

Edit Delete Clone

Up Down

Top Bottom

Option

Value

Enabled

true

Comment

Block Audio & Video Content during office hours - 2nd half

Mime type

^(audio|video)/

Hour range

14,17

Time match mode

absolutetime

Added profiles

block-audio-video

Edit Delete Clone

Up Down

Top Bottom

The first rule will apply the profile `block-audio-video` to requests for audio and video contents during 0900-1300 hrs. The second rule will do the same, but during 1400-1700 hrs. Now in the `Mime filtering` section, just create a rule in the `Deny` sub-section to block access to the `block-audio-video` profiles.

Option

Value

Enabled

true

Comment

Block Audio & Video Content

Profiles

block-audio-video

Edit Delete Clone

Up Down

Top Bottom

If you would like to allow audio/video content from some specific business websites, then create a rule in profile sectionbelow the above rules, specify the websites in the Hosts field, and specify block-audio-video in the Removed profilesfield.

Option

Value

Comment

Do not apply profile block-audio-video to specified sites

Host

(howtoforge.com|safesquid.com|linux.com)

Time match mode

absolutetime

Removed profiles

block-audio-video

Edit Delete Clone

Up Down

Top Bottom

This will remove the profile block-audio-video from the specified websites, and allow access to audio and video contents from these sites.

Also see:

- **Deploying A Content Filtering Proxy Server To Distribute Controlled Internet Access With SafeSquid**
- **Set Up Gateway Level Virus Security With ClamAV And SafeSquid Proxy**
- **How To Set Up Internet Access Control And Internet Filtering With SafeSquid Proxy Server**
- **How To Control Access To Unwanted Websites Using URL Blacklist With SafeSquid Proxy Server**
- **How To Configure Granular Bandwidth Management Rules In SafeSquid Proxy Server**