

## Enhance Security By Removing ActiveX Control Codes From Web Pages With SafeSquid Proxy Server

*By Sean*

Published: 2008-07-08 13:33

# Enhance Security By Removing ActiveX Control Codes From Web Pages With SafeSquid Proxy Server

Allowing free access to ActiveX Control content, can be a security risk. ActiveX can be used to deposit spyware, adware and other malware into users system, when they visit innocent looking websites. A google search for *dangers of activex* would be very informative.

The *Rewrite Document* feature of [SafeSquid](#)- Content Filtering Internet Proxy, allows you to alter the html codes of a webpage on the fly, and send the modified content to the requesting user. This feature can be used to search for ActiveX codes in web pages served by non-trusted websites, remove or replace them with some other codes, and serve the modified web pages to the user.

### Procedure:

Open the SafeSquid Web Interface, go to *Config=> Profiles*, and create the following profile:

<u>Option</u>	<u>Value</u>
Enabled	true
Comment	Add profile 'BlockActiveX' to all requests, except the ones with 'Main-Sites' profile
Profiles	!Main-Sites
Time match mode	absolutetime
Added profiles	BlockActiveX

The above rule will add the profile *BlockActiveX* to requests for all websites, except the ones specified in the *Main-Sites* profile (Profiles=!Main-Sites, where '!' means NOT or EXCEPT). The *Main-Sites* profile is normally created under *Profiles* section, to bypass a few business related and trusted websites, from filtering rules, like the ones that block ads and banners, pop-ups, and rules defined under *Keyword filter* section. The rule simply specifies the hosts and adds the profile *Main-Sites* to requests for these hosts (note that the rule for *Main-Sites* should be above the rule for *BlockActiveX*):

<u>Option</u>	<u>Value</u>
---------------	--------------

Enabled	true
Comment	Add profile 'Main-Sites' to requests for specified, Trusted websites
Host	(safesquid.com howtoforge..* linux.com)
Time match mode	absolutetime
Added profiles	Main-Sites

Now, we can use the *BlockActiveX* profile, under *Rewritedocument* section. In the SafeSquid Interface, go to *Config=> Rewrite document*, and create the following rule:

<u>Option</u>	<u>Value</u>
Enabled	true
Comment	Remove ActiveX Control codes
Profiles	BlockActiveX
Pattern	(?!(*.macromedia))<object[^>]*>(.*</object>
Replace	<b>SafeSquid restricting ActiveX download</b>
Applies to	body

The above rule will look for the codes specified in the *Pattern* field above, which is a regular expression for ActiveX control codes, and replace them with the expression 'SafeSquid restricting ActiveX download'. Note the expression *(?!(\*.macromedia))*. This excludes the codes for Macromedia Flash, which is similar to ActiveX, except that it contains the word *macromedia*. If the pattern is altered to *<object[^>]\*>(.\*</object>* it will block both, ActiveX as well as Macromedia Flash.

#### 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](#)
- [How To Control Download Of Files And Mime Types In SafeSquid Proxy Server](#)
- [How To Block Ads And Banners In SafeSquid Proxy Server](#)
- [How To Block Cookies From Unwanted Websites With SafeSquid Proxy Server](#)