By Sean

Published: 2008-03-28 12:42

How To Set Up Internet Access Control And Internet Filtering With SafeSquid Proxy Server

SafeSquid - Content Filtering Internet Proxy, has many content filtering features that can be used to decide who is allowed what, when and how much on the net. In this tutorial I will describe how to create user profiles, and give them access to specific websites only, while blocking access to all other websites.

Note: See **'Deploying A Content Filtering Proxy Server To Distribute Controlled Internet Access With SafeSquid'** for the procedure ofinstalling Content Filtering Proxy - **SafeSquid**.

To help you understand the procedure, I will use this short example:

User

Job Profile

Required Websites

Admin

Proxy Administrator

No restrictions. Allowed all websites.

John

IT Support

howtoforge.com, safesquid.com, symantec.com & microsoft.com

Sam

Finance

moneycontrol.com, capitalmarket.com, finance.yahoo.com & hdfcbank.com

SafeSquid has a browser based GUI Interface for management of rules and filters. Although it has many features, in this tutorial I will be introduce you to three important features, viz. *`Access Restriction`*, *`Profiles`* and *`URL Filtering`*.

Access Restriction:

This is where you define who is allowed to access SafeSquid Proxy, based on client IP, username & password or authenticating users from an external user database like ADS, LDAP, Radius, POP3 Server, MySQL database, etc. Here, we will create user accounts for Admin, John and Sam.

Open the SafeSquid Web Interface with *`http://safesquid.cfg`*. Click on *`Config`*. From the drop-down menu that appears, select *`Access Restriction`* and click on *`Submit`*. You enter the *`Access Restriction`* Section. This section has three parts -

-

access sub-section: Defines the default policy
Allow: allow all and block what is defined under the Deny sub-section
Deny: deny all and allow what is defined under the Allow sub-section

-

Allow sub-section: When the Policy is Deny, this is where you define who is allowed access.

-

Deny sub-section: When the Policy is Allow, this is where you define who is denied access.

We will leave the *`Policy`* to *`Deny`*, and create user accounts for Admin, John and Sam under the *`Allow`* sub-section, to give access to these users.

Default Allow Rule

Option	**Value**
Enabled	true
Comment	This default rule allows access to every users of the network with IP address and username field left blank.
PAM authentication	false
Access	config,proxy,http,transparent,connect,bypass,urlcommand

Edit Delete CloneUp DownTop Bottom

Although the `Policy` is `Deny`, the first rule under `Allow` sub-section allows unrestricted access to everyone. `Access Restriction` functions in top-down hierarchy. The first rule that matches a user is applied. So, onces you have created user accounts, you will have to edit this rule and make `Enable > false` to disable this rule, or delete it. But do not disable or delete this rule, until you have created atleast the Admin account, or you will lock yourself out of the web interface. If, by chance, this happens, just restart SafeSquid with the command -

```
/etc/init.d/safesquid restart
```

This will restart the proxy with the default, or last saved rules. This happens because any changes that you make in the web interface, is applied in real time to the configuration file (confi.xml) that resides in the server's memory, and the changes are permanently stored to configuration file on the disk, only when you save the changes by clicking on the like *Save settings*in the top menu of the interface.

Creating User Account:

Click on *Add* under *Allow* to create a user account. In the form that appears, fill in the following fields:

Comment: This rule is for the proxy administrator
User name: admin
Password: admin
Added profile: administrator

Leave the other fields as it is. Click on *Submit* at the bottom of the form to save the rule. The new rule appears at the bottom of the *Allow* sub-section and will look like this:

Option

Value

Enabled

true

Comment

This rule is for the proxy administrator

PAM authentication

false

User name

admin

Password

admin

Access

config,proxy,http,transparent,connect,bypass,urlcommand

Added profiles

Administrator
Edit Delete CloneUp DownTop Bottom

In the above rule, we have created an administrator account with username and password. When ever a user logs in using this username and password, he will be allotted the Profile *`administrator`*. This profile will be used to define what is allowed to this user later.

Similarly add accounts for John and Sam. But this time, remove the tick from the options *`Web interface`* (will deny access to SafeSquid web interface) and *`Allow bypassing`*, which is a special SafeSquid *`URL command`*,which can be used to bypass a filter and is used by administrators for diagnostic purpose. The two rules thus created, should look like this -

Option	**Value**
Enabled	true
Comment	This rule is for the proxy administrator
PAM authentication	false
User name	john
Password	john

Access

proxy,http,transparent,connect,urlcommand

Added profiles

Finance
Edit Delete CloneUp DownTop Bottom

Option

Value

Enabled

true

Comment

This rule is for the proxy administrator

PAM authentication

false

User name

sam

Password

sam

Access

proxy,http,transparent,connect,urlcommand

Added profiles

Finance
Edit Delete CloneUp DownTop Bottom

Notice the difference in the *Access* field of these two users and admin. You can see that *config* and *bypass* is missing in the rules for John and Sam. This is because we removed the tick from *Webinterface* and *Allow Bypassing*, and signifies that these users are not allowed to access the SafeSquid web interface and use the *bypass* URL Command

Now you can disable or delete the default rule that allows access to everyone.

Click *Save settings* in the Top Menu. On the page that is displayed, click on *Submit* without making any changes in the *Filename* field. This will make the changes permanent.

TIP: The *Added profiles* Administrator, IT-Support and Finance can also be used as User Groups. To add other members to this group, click on *clone* under the rule. This will create a duplicate or clone of the rule. Now, edit theduplicate rule, and change the *User name* and *Password*. You can create as many users as you want. Now all the users thus created, will have the same *Added profiles* value, e.g. IT-Support or Finance. Now what everaccess rights you give to these profiles, will be inherited by these users.

Profiles Section

The Profiles section is one of the most important section of SafeSquid. Profiles allow you to create extremely granular rules with ease. This is where you define a 'situation' for *`Profiles`* created in *`Access Restriction`*. The options available for defining a situation are *`Protocol, Host, File, Mime type, Port range list, URL Command, Proxy host, Request header pattern, Response header pattern, Month range, Day range, Weekday range, Hour range`* and *`Minute range`*. But since we are only defining the websites that each user or group is allowed, we are only concerned with the *`Profile`* and *`Host`* options.

We can use this section to apply an additional profile, which I will call *`allowed-site`*, for each previously created profile (Administrator, IT-Support and Finance), **ONLY** when they request for a website that is allowed to them.

We will start with Administrator profile. Click on *`Config`*, and from the drop-down menu that appears, select *`Profiles`* and click on *`Submit.`* You enter the *`Profiles`* section. Click on *`Add`*under the *`Profile`* sub-section. Fill the following fields in the form that appears -

`Comment:` This rule defines websites allowed to Administrator
Profiles: Administrator
Added profiles: allowed-site

You see that there are many fields, as listed above, that we left blank. When you leave a field blank, it means anything or does not matter. So, when we leave the Host field blank, it means any host. So this rule says that when Administrator requests any website, apply an additional profileallowed-site to the request. This will be made clear when we create rules for IT-Support and Finance.

Click on Add to create a new rule or clone the above rule and edit the cloned rule for IT-Support, like this -

`Comment:` This rule defines websites allowed to IT-Support
Profiles: IT-Support
Host: (howtoforge.com|safesquid.com|symantec.com|microsoft.com)
Added profiles: allowed-site

This rule says that when IT-Support requests specifically for websites listed in the Host field, apply the profile allowed-site to the request. Requests for any other website, will not be applied allowed-site profile.

Similarly, create rule for Finance, like this -

`Comment:` This rule defines websites allowed to Finance

Profiles: Finance
Host: (moneycontrol.com|capitalmarket.com|finance.yahoo.com|hdfcbank.com)
Added profiles: allowed-site

The three rules must look like this -

Option

Value

Enabled

true

Comment

This rule defines websites allowed to Administrator

Profiles

Administrator

Time match mode

absolutetime

Added profiles

allowed-site
Edit Delete CloneUp DownTop Bottom

Option

Value

Enabled

true

Comment

This rule defines websites allowed to IT-Support

Profiles

IT-Support

Host

(howtoforge.com|safesquid.com|symantec.com|microsoft.com)

Time match mode

absolutetime

Added profiles

allowed-site
Edit Delete CloneUp DownTop Bottom

Option

Value

Enabled

true

Comment

This rule defines websites allowed to Finance

Profiles

Finance

Host

(moneycontrol.com|capitalmarket.com|finance.yahoo.com|hdfcbank.com)

Time match mode

absolutetime

Added profiles

allowed-site
Edit Delete CloneUp DownTop Bottom

Note that by creating the above rule, we are not allowing or blocking anything, but just defining situations, and applying a profile. The actual action, allow or deny, is done in the URL Filter section. Let us move on to the URL filter section, to complete the action to be taken.

URL Filter

This is where you can define what is to be allowed or denied. URL Filter section has three parts -

Open the SafeSquid Web Interface with `http://safesquid.cfg`. Click on `Config`. From the drop-down menu that appears, select `Access Restriction` and click on `Submit`. You enter the `Access Restriction` Section. This section has three parts -
-

url-filterig sub-section:
-

Enabled: Yes / No - Allows you to completly enable or disable the URL filter section
-

Policy: Defines the default policy
Allow: allow all and block what is defined under the Deny sub-section
Deny: deny all and allow what is defined under the Allow sub-section

-

Allow sub-section: When the Policy is Deny, this is where you define what is allowed access.

-

Deny sub-section: When the Policy is Allow, this is where you define what is denied access.

We can now keep the *Policy* as *Allow*, and add a rule under *Deny* sub-section to deny everything except allowed-site profile, or set the *Policy* to *Deny*and add a rule under *Allow* sub-section to allow only allowed-site profile. We will leave the *policy* to *Allow*. Now, click on *Add* under *Deny* sub-section and addthis rule -

Comment: This rule denies access to everything except allowed-site profile
Profiles: !allowed-site

Option

Value

Enabled

true

Comment

This rule denies access to everything except allowed-site profile

Profiles

!allowed-site

Edit Delete CloneUp DownTop Bottom

Notice the '!' before 'allowed-site' in Profiles field. '!' means NOT or except. So the above rule blocks all requests that do not carry the *`allowed-site`* profile.

We have already defined that allowed-site profile will be applied only when -

-

Finance requests for moneycontrol.com, capitalmarket.com, finance.yahoo.com & hdfcbank.com

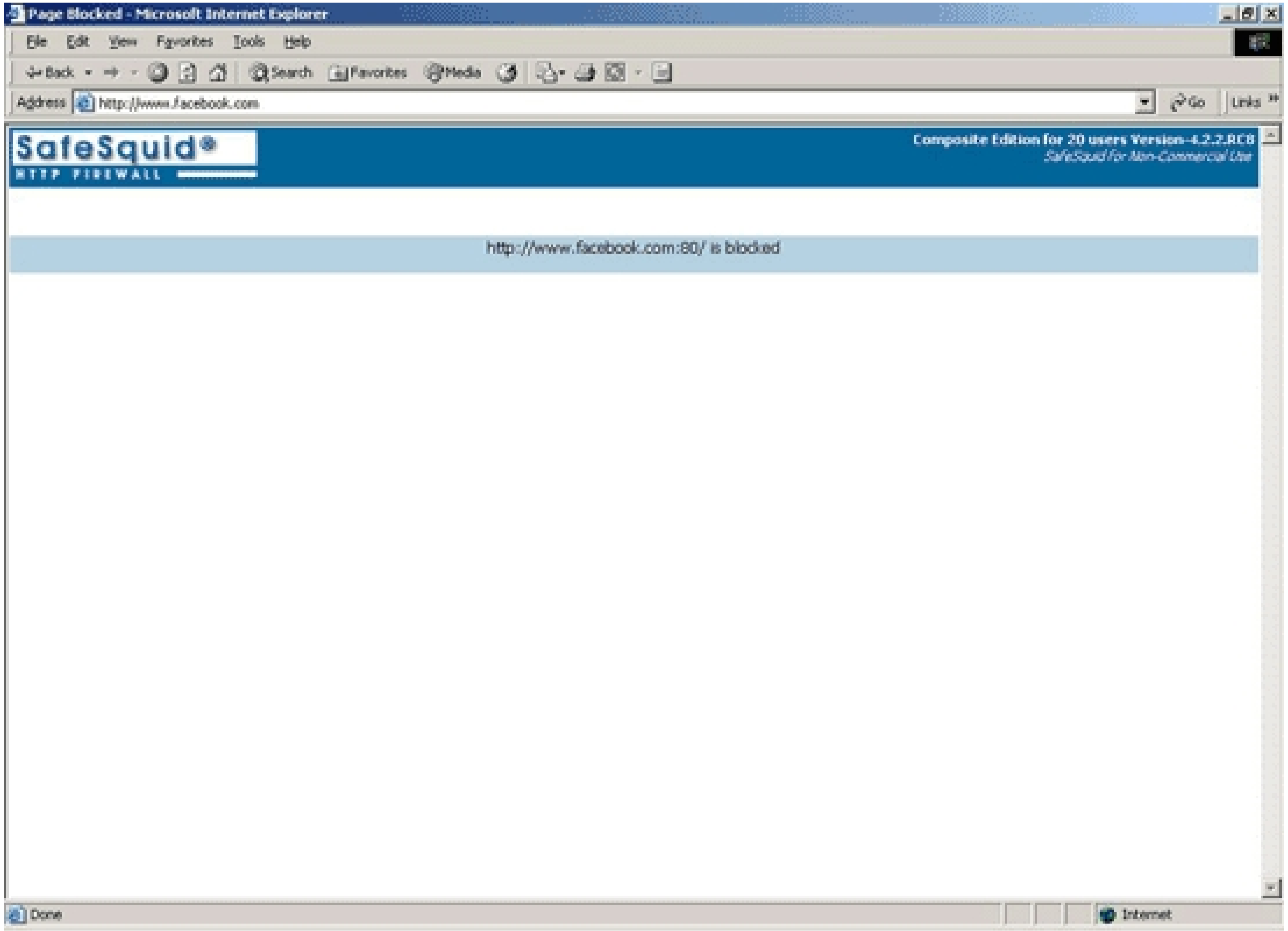
-

IT-Support requests for howtoforge.com, safesquid.com, symantec.com & microsoft.com, and

-

Administrator requests for any website.

When a user visits a website that is not defined in his allowed-site profile, URL filter denies the request, and the user is send a template, like the one shown below -



Page Blocked - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.facebook.com
Go Links
SafeSquid®
HTTP FIREWALL
Composite Edition for 20 users Version-4.2.2.RC8
SafeSquid For Non-Commercial Use
Done
Internet

http://www.facebook.com:80/ is blocked