SquidGuard

1. Most simple configuration

   Most simple config uration: one category, one rule for all

```
#
# CONFIG FILE FOR SQUIDGUARD
#

dbhome /usr/local/squidGuard/db
logdir /usr/local/squidGuard/logs

dest porn {
        domainlist porn/domains
        urllist porn/urls
        }

acl {
        default {
                pass !porn all
                redirect
http://localhost/block.html
        }
 }
```

Make always sure that the very first line of your squidGuard.conf is not empty!
The entries have the following meaning:

`dbhome`	Location of the blacklists
`logdir`	Location of the logfiles
`dest`	Definition of a category to block. You can enter the domain and url file along with a regular expression list (talk about regular expressions later on).
`acl`	The actual blocking defintion. In our example only the default is displayed. You can have more than one `acl` in place. The category porn you defined in `dest` is blocked by the expression `!porn`. You have to add the identifier `all` after the

	blocklist or your users will not be able to surf anyway. The `redirect` directive is madatory! You must tell SquidGuard which page to display instead of the blocked one.

2. Choosing more than one category to block

   First you define your categories. Just like you did above for porn. For example:

   Defining three categories for blocking

```
dest adv {
        domainlist      adv/domains
        urllist         adv/urls
}
dest porn {
        domainlist      porn/domains
        urllist         porn/urls
}
dest warez {
        domainlist      warez/domains
        urllist         warez/urls
}
```

   Now your `acl` looks like that:

```
acl {
        default {
                pass    !adv !porn !warez
all
                redirect
http://localhost/block.html
                }
}
```

3. Whitelisting

   Sometimes there is a demand to allow specific URLs and domains although they are part of the blocklists for a good reason. In this case you want to whitelist these domains and URLs.

   Defining a whitelist

```
dest white {
        domainlist      white/domains
        urllist         white/urls
}

acl {
        default {
                pass    white !adv !porn
!warez all
                redirect
http://localhost/block.html
                }
}
```

In this example we assumed that your whitelists are located in a directory called `white` whithin the blacklist directory you specified with `dbhome`.
Make sure that your `white` identifier is the first in the row of the `pass` directive. It must not have an exclamation mark in front (otherwise all entries belonging to `white` will be blocked, too).

4. Initializing the blacklists

   Before you start up your squidGuard you should initialize the blacklists i.e. convert them from the textfiles to db files. Using the db format will speed up the checking and blocking.
   The initialization is performed by the following command:

   Initializing the b lacklists

```
squidGuard -C all
chown -R <squiduser>
/usr/local/squidGuard/db/*
```

The second command ensures that your squid is able to access the blacklists. Please for <squiduser> the uid of your squid.
Depending on the size of your blacklists and the power of your computer this may take a while. If anything is running fine you should see something like the following output in your logfile:

```
2006-01-29 12:16:14 [31977] squidGuard
1.2.0p2 started (1138533256.959)
2006-01-29 12:16:14 [31977] db update done
2006-01-29 12:16:14 [31977] squidGuard
stopped (1138533374.571)
```

If you look into the directories holding the files `domains` and `urls` you see that additional files have

been created: `domains.db` and `urls.db`. These new files must not be empty!
Only those files are converted you specified to block or whitelist in your `squidGuard.conf` file.