

Lab11 – Content filtering (@Home version)

You can use this lab manual for your personal documentation. Use screenshots for your own documentation, there will be questions later on that may point to this lab manual. Take care to check if you need to collect some information from the lab for the answers.

\ at the end of the line is used to mark that the command needs to be on one line. Replace **student-id** with your own student-id and **x** or **y** as your VMs correct IP in the labs.

No new VMs are needed for this lab, you can reuse existing ones from previous labs.



squid.student-id.zz
(Centos7)



Workstation
W7-VM

You'll continue with the Squid VM from the previous lab and configure both DNS and URL filtering. This Lab also requires you to change the DNS settings of the client machine, so using the W7-VM is highly recommended.

All templates for VMs can be found in [\\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\](https://ghost.labranet.jamk.fi/virtuaalikoneet/TTKS/)

- **squidGuard URL filtering**

squidGuard can be used for URL filtering when the traffic is handled by the squid proxy server. On the Squid VM, install squidGuard:

```
yum install epel-release
```

```
Updated:
  epel-release.noarch 0:7-12

Complete!
[root@localhost.localdomain ~]#
```

```
yum install squidGuard
```

```
Installed:
  squidGuard.x86_64 0:1.4-36.el7

Dependency Installed:
  perl-DB_File.x86_64 0:1.830-6.el7

Complete!
[root@localhost.localdomain ~]#
```

Modify the configuration in /etc/squid/squidGuard.conf and remove ALL lines. Add the following configuration (you can leave the comments out if you want):

```
# Database and log directory
dbhome /var/lib/squidGuard/db
logdir /var/log/squidGuard

# What is denied
dest deny {
    urllist deny/urls
}

# ACL control using the previous deny
acl {
    default {
        pass !deny all
        redirect http://your-squid-vm-ip/blocked.php?
    }
}
```

```

# Database and log directory
dbhome /var/lib/squidGuard/db
logdir /var/log/squidGuard

# What is denied
dest deny {
    urllist deny/urls
}

# ACL control using the previous deny
acl {
    default {
        pass !deny all
        redirect http://192.168.44.230/blocked.php?
    }
}

```

Save the file and create the deny list directory and the files in it:

```

mkdir -p /var/lib/squidGuard/db/deny
touch /var/lib/squidGuard/db/deny/urls
[root@localhost.localdomain ~]# mkdir -p /var/lib/squidGuard/db/deny
[root@localhost.localdomain ~]# touch /var/lib/squidGuard/db/deny/urls
[root@localhost.localdomain ~]#

```

The *urls* file can be used to block certain url patterns, such as subreddits (add these to the file):

```

reddit.com/r/the_donald
reddit.com/r/putin

```

```

GNU nano 2.3.1      File: /var/lib/squidGuard/db/deny/urls

reddit.com/r/the_donald
reddit.com/r/putin

```

Update the databases and change ownership (run at commandline):

```

squidGuard -d -C all
[root@localhost.localdomain ~]# squidGuard -d -C all
2020-02-13 10:59:47 [3548] New setting: dbhome: /var/lib/squidGuard/db
2020-02-13 10:59:47 [3548] New setting: logdir: /var/log/squidGuard
2020-02-13 10:59:47 [3548] init urllist /var/lib/squidGuard/db/deny/urls
2020-02-13 10:59:47 [3548] create new dbfile /var/lib/squidGuard/db/deny/urls.db
2020-02-13 10:59:47 [3548] squidGuard 1.4 started (1581591587.869)
2020-02-13 10:59:47 [3548] db update done
2020-02-13 10:59:47 [3548] squidGuard stopped (1581591587.872)
[root@localhost.localdomain ~]#

chown -R squid. /var/lib/squidGuard/db/deny
[root@elek-431-nd-49.labranet.jamk.fi ~]# chown -R squid. /var/lib/squidGuard/db/deny

```

Fix SELinux contexts:

```

yum install policycoreutils-python

```

```

Installed:
  policycoreutils-python.x86_64 0:2.5-33.el7

Dependency Installed:
  audit-libs-python.x86_64 0:2.8.5-4.el7  checkpolicy.x86_64 0:2.5-8.el7
  libcgroupp.x86_64 0:0.41-21.el7          libsemanage-python.x86_64 0:2.5-14.el7
  python-IPy.noarch 0:0.75-6.el7          setools-libs.x86_64 0:3.3.8-4.el7

Dependency Updated:
  audit.x86_64 0:2.8.5-4.el7          audit-libs.i686 0:2.8.5-4.el7
  audit-libs.x86_64 0:2.8.5-4.el7     policycoreutils.x86_64 0:2.5-33.el7

Complete!
[root@elek-431-nd-49.labranet.jamk.fi ~]#
semanage fcontext -a -t squid_cache_t "/var/lib/squidGuard(/.*)?"
restorecon -R /var/lib/squidGuard
[root@elek-431-nd-49.labranet.jamk.fi ~]# semanage fcontext -a -t squid_cache_t
"/var/lib/squidGuard(/.*)?"
[root@elek-431-nd-49.labranet.jamk.fi ~]# restorecon -R /var/lib/squidGuard/
[root@elek-431-nd-49.labranet.jamk.fi ~]#

```

Now add the following line to /etc/squid/squid.conf to make squid use the rules (add to squid.conf):

```

url_rewrite_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf
url_rewrite_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf

```

And restart squid:

```




systemctl restart squid
[root@elek-431-nd-49.labranet.jamk.fi ~]# systemctl restart squid
[root@elek-431-nd-49.labranet.jamk.fi ~]#

```

Now try to browse to the social media sites and test that you can access other subreddits except the ones in the blacklist. You can add more domains/urls in the files but remember to update the databases like above.

NOTE: If you add a domain by itself, add it as www.domain.com/ with the trailing slash!



   <https://www.reddit.com/r/putin>

ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: <http://192.168.44.230/blocked.p>

Connection to 192.168.44.230 failed.

The system returned: *(111) Connection refused*

The remote host or network may be down. Please try the request again.

Your cache administrator is [root](#).

Search r/cats

Posted by u/chrispega 8 hours ago

Seeing snow for the first time Cat Picture



- **Custom block page**

To show the user a reason or warning message for blocked sites, create a custom page for the squidGuard to show to users. Install httpd:

```
yum install httpd php  
  
systemctl start httpd  
systemctl enable httpd  
firewall-cmd --add-service=http --permanent  
firewall-cmd -reload
```

```

Installed:
  httpd.x86_64 0:2.4.6-90.el7.centos      php.x86_64 0:5.4.16-46.1.el7_7

Dependency Installed:
  apr.x86_64 0:1.4.8-5.el7                apr-util.x86_64 0:1.5.2-6.el7
  httpd-tools.x86_64 0:2.4.6-90.el7.centos  libzip.x86_64 0:0.10.1-8.el7
  mailcap.noarch 0:2.1.41-2.el7            php-cli.x86_64 0:5.4.16-46.1.el7_7
  php-common.x86_64 0:5.4.16-46.1.el7_7

Complete!
[root@elek-431-nd-49.labranet.jamk.fi ~]# systemctl start httpd
[root@elek-431-nd-49.labranet.jamk.fi ~]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service
to /usr/lib/systemd/system/httpd.service.
[root@elek-431-nd-49.labranet.jamk.fi ~]# firewall-cmd --add-service=http --pe
anant
success
[root@elek-431-nd-49.labranet.jamk.fi ~]# firewall-cmd --reload
success
[root@elek-431-nd-49.labranet.jamk.fi ~]# █

```

Then create the `/var/www/html/blocked.php` with following code:


```

<?php

$address=$_GET['address'];
$url=$_GET['url'];
echo "Access to $url is prohibited!<br>";
echo "Your IP address is $address<br>";
echo "This violation has been logged";

?>

```



```

GNU nano 2.3.1      File: /var/www/html/blocked.php

<?php

$address=$_GET['address'];
$url=$_GET['url'];
echo "Access to $url is prohibited!<br>";
echo "Your IP address is $address<br>";
echo "This violation has been logged";

?>

```

Then modify `squidGuard.conf` and change the redirect to:

```

redirect http://your-squid-ip/blocked.php?url=%u&address=%a&n=%n

```

```

acl {
  default {
    pass !deny all
    redirect http://192.168.44.230/██/blocked.php?url=%u&address=%a&n=%n
  }
}

```

Let's also add logging, add the following after domain/urllists in dest deny:

```
log violations
```

```
# What is denied
```

```
dest deny {
```

```
    urllist deny/urls
```

```
    log violations
```

```
}
```

Restart squid and try to browse to the blocked pages now. Check /var/log/squidGuard/violations file and see how the access is logged.

Access to <https://www.reddit.com/r/putin> is prohibited!

Your IP address is 192.168.44.115

This violation has been logged

```
2020-02-13 11:30:27 [32656] Request(default/deny/-) https://www.reddit.com/r/putin 192.168.44.115/192.168.44.115 - GET REDIRECT
```