

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
yum install squidGuard
```

```
144 yum install epel-release
145 yum install squidGuard
146 history
[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?
    }
}
```

```
GNU nano 2.3.1 File: /etc/squid/squidGuard.conf

# 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://192.168.44.235/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 ~]# nano /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
chown -R squid. /var/lib/squidGuard/db/deny
[root@localhost.localdomain ~]# squidGuard -d -C all
2020-02-13 10:45:57 [1515] New setting: dbhome: /var/lib/squidGuard/db
2020-02-13 10:45:57 [1515] New setting: logdir: /var/log/squidGuard
2020-02-13 10:45:57 [1515] init urllist /var/lib/squidGuard/db/deny/urls
2020-02-13 10:45:57 [1515] create new dbfile /var/lib/squidGuard/db/deny/urls.db
2020-02-13 10:45:57 [1515] squidGuard 1.4 started (1581590757.250)
2020-02-13 10:45:57 [1515] db update done
2020-02-13 10:45:57 [1515] squidGuard stopped (1581590757.255)
[root@localhost.localdomain ~]# chown -R squid. /var/lib/squidGuard/db/deny
[root@localhost.localdomain ~]#
```

Fix SELinux contexts:

```
yum install policycoreutils-python
semanage fcontext -a -t squid_cache_t "/var/lib/squidGuard(/.*)?"
restorecon -R /var/lib/squidGuard
153 yum install policycoreutils-python
154 semanage fcontext -a -t squid_cache_t "/var/lib/squidGuard(/.*)?"
155 restorecon -R /var/lib/squidGuard
156 history
[root@localhost.localdomain ~]#
```

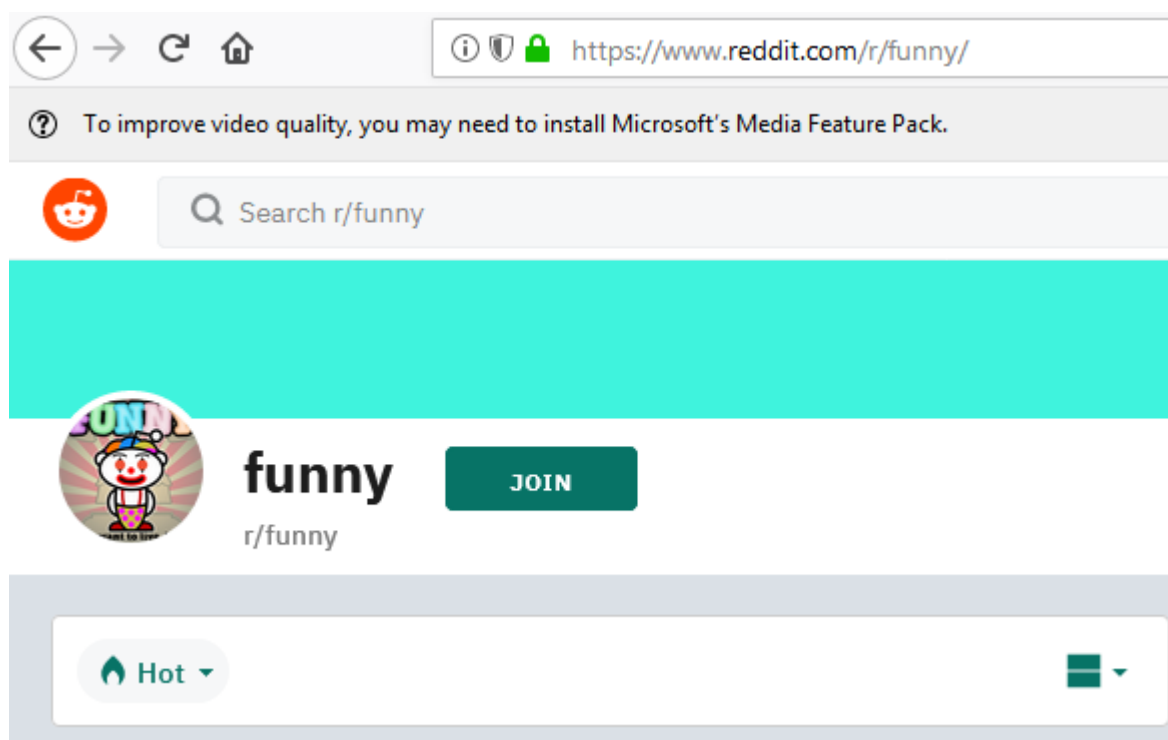
Now add the following line to */etc/squid/squid.conf* to make squid use the rules (add to *squid.conf*):

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

And restart squid:

```
systemctl restart squid
```

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!

- **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
```

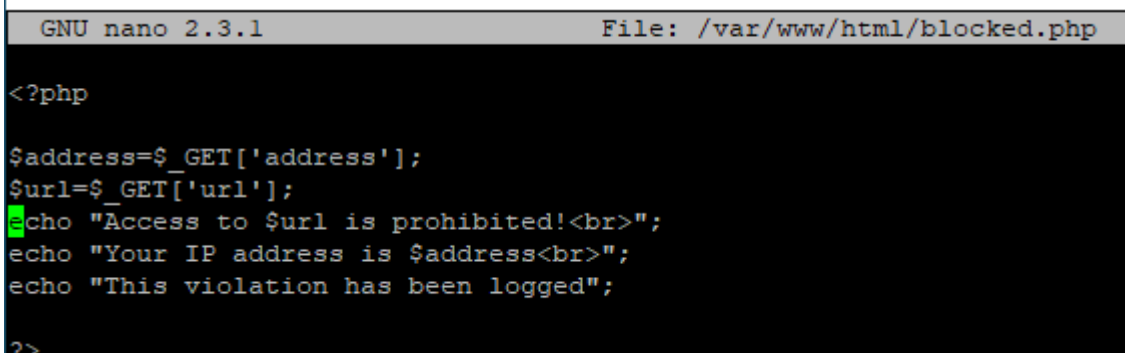
```
[root@localhost.localdomain ~]# systemctl start httpd
[root@localhost.localdomain ~]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service
ce.
[root@localhost.localdomain ~]# firewall-cmd --add-service=http --permanent
success
[root@localhost.localdomain ~]# firewall-cmd --reload
success
[root@localhost.localdomain ~]#
```

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
```

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

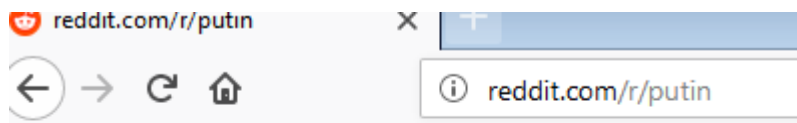
```
log violations
```

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

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

# ACL control using the previous deny
acl {
    default {
        pass !deny all
        redirect http://192.168.44.235/blocked.php?url=%u&address=%a&n=%n?
    }
}
```

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



```
"; echo "Your IP address is $address
"; echo "This violation has been logged"; ?>
```

- En saanut PHP:tä toimimaan kunnolla, mutta redirect, ja logiikka toimii kyllä.

```
2020-02-13 11:42:00 [1343] Request(default/deny/-) http://www.iltalehti.fi/favic
on.ico 192.168.44.110/192.168.44.110 - GET REDIRECT
2020-02-13 11:42:14 [1343] Request(default/deny/-) http://reddit.com/r/putin 192
.168.44.110/192.168.44.110 - GET REDIRECT
```