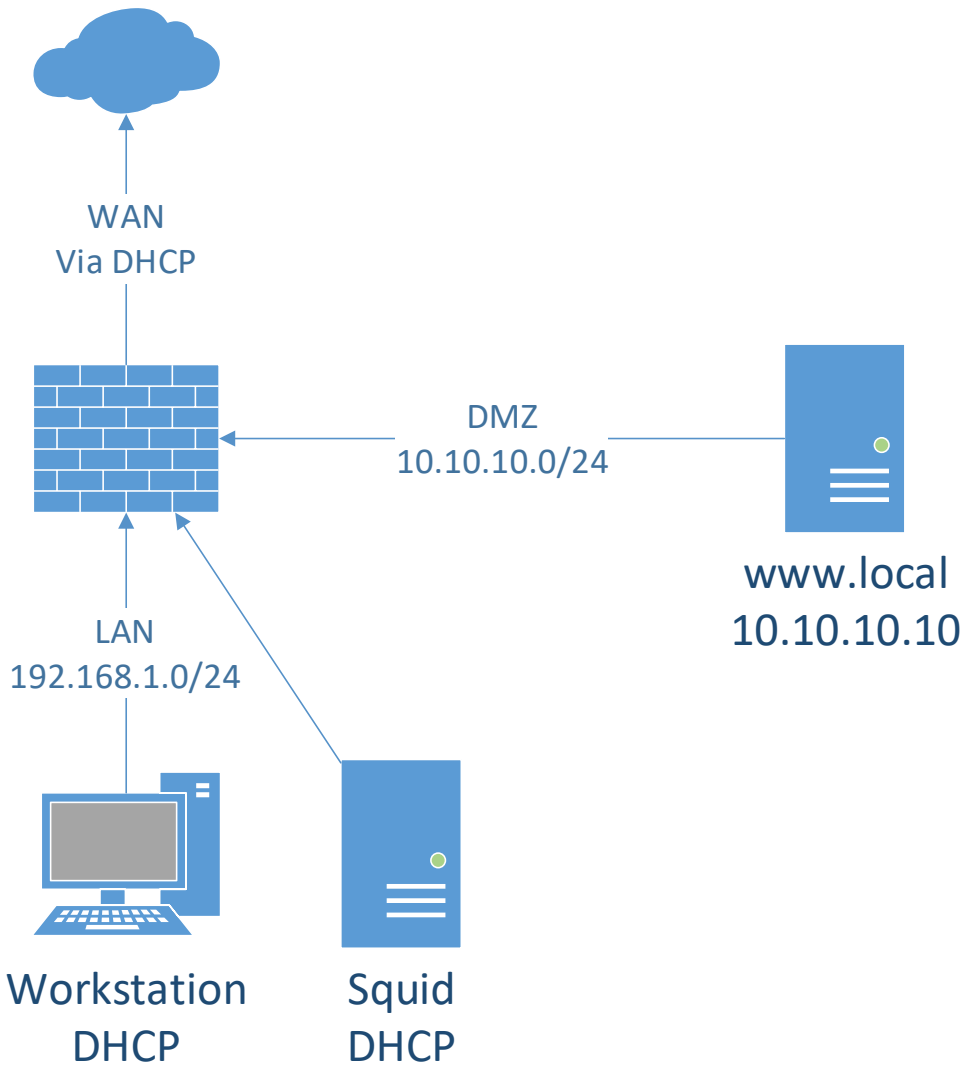
Lab4 – Content filtering

Document your commands or take screenshots. Answer questions in english or finnish. Replace student-id with your own student-id in the labs.

The labs use the following topology, some VMs are already installed in the previous labs:



- ## DNS Blocking (1p)

We will deny access to iltalehti.fi and iltasanomat.fi using DNS. Boot up the VMs and go to PfSense web configuration. At DNS Forwarder, add Host override for both www.iltasanomat.fi, iltasanomat.fi, www.iltalehti.fi and iltalehti.fi. Point all these hostnames to your own webserver 10.10.10.10. Remember to apply the settings.

On the Webserver VM, install php:

```
yum install php
```

```
[root@www ~]# yum install -y php
```

```
systemctl restart httpd
```

```
[root@www ~]# systemctl restart httpd
```

Then create a file `/var/www/html/index.php` with the following code:

```
<?php

$domain=$_SERVER['HTTP_HOST'];
echo "Access to $domain is prohibited!";
?>
```

```
  GNU nano 2.3.1          File: /var/www/html/index.php

<?php

$domain=$ SERVER['HTTP_HOST'];
echo "Acces to $domain is prohibited";
?>
```

Save the file and test that iltasanomat.fi/iltalehti.fi resolves to 10.10.10.10 with nslookup. Then test browsing to those sites. You should get the page configured above as a result.

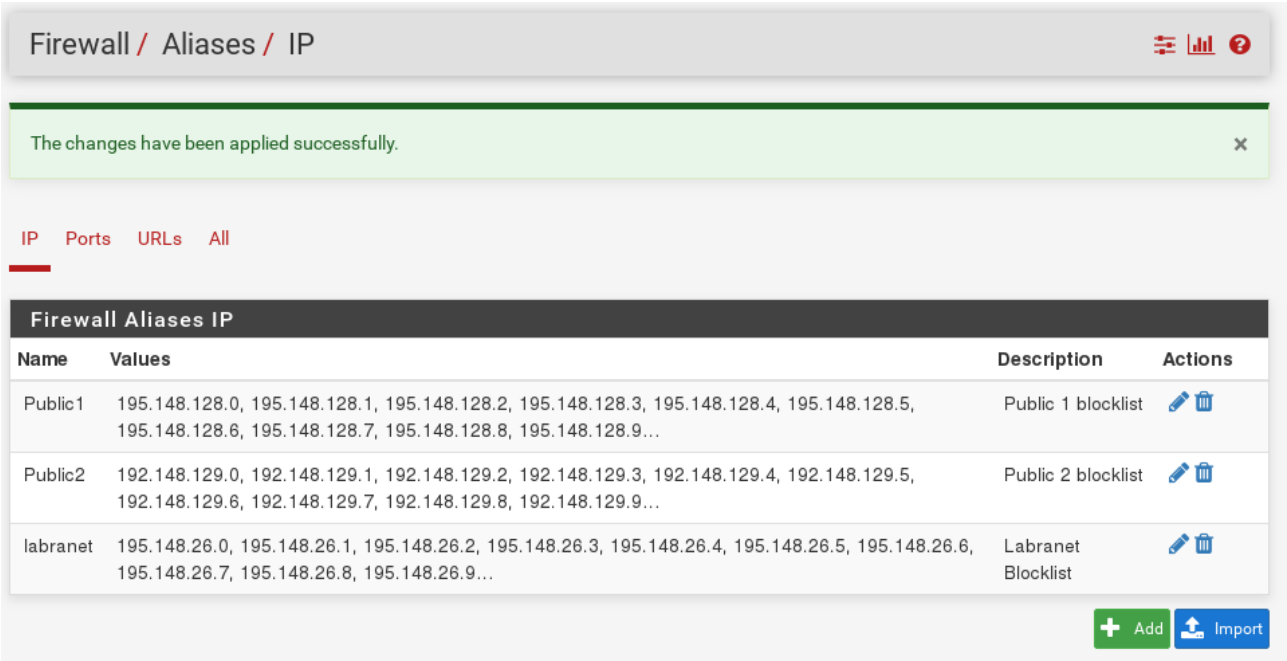
```
[root@www ~]# nslookup iltalehti.fi
Server:         10.10.10.1
Address:        10.10.10.1#53

Non-authoritative answer:
Name:   iltalehti.fi
Address: 178.217.128.81

[root@www ~]# nslookup iltasanomat.fi
Server:         10.10.10.1
Address:        10.10.10.1#53
```

- ## IP blocklisting (1p)

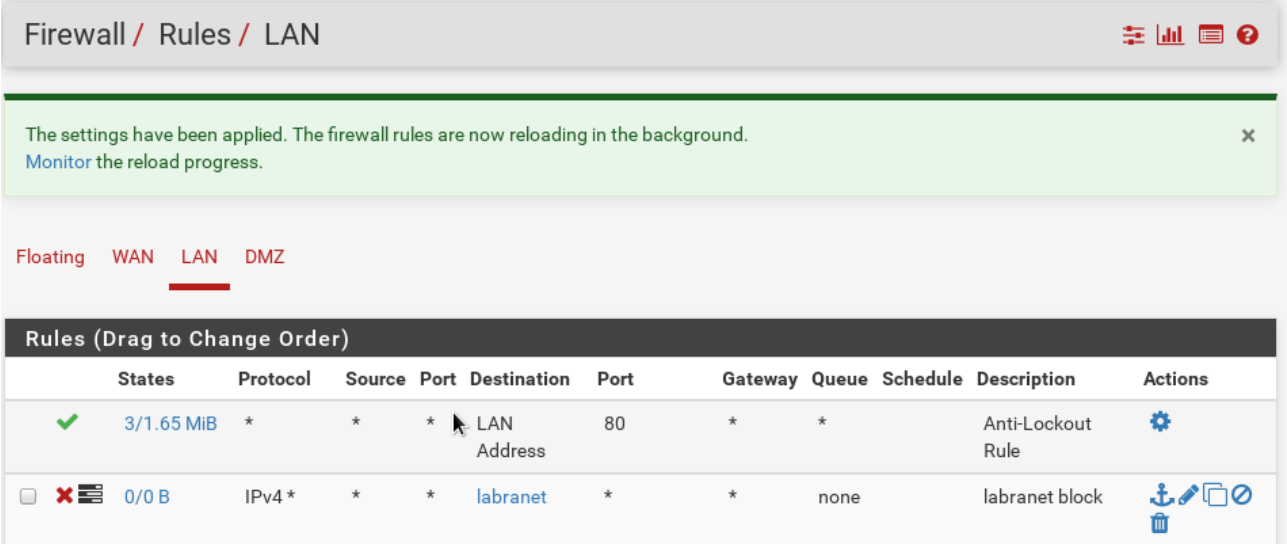
Let's try blocklisting JAMK public IP blocks. Go to Pfsense management, Firewall - Aliases. Create an IP alias with the name "Blocklist" and choose type as Network(s). Add at least the following IP blocks:

- 195.148.26.0/24 - description: LabraNet

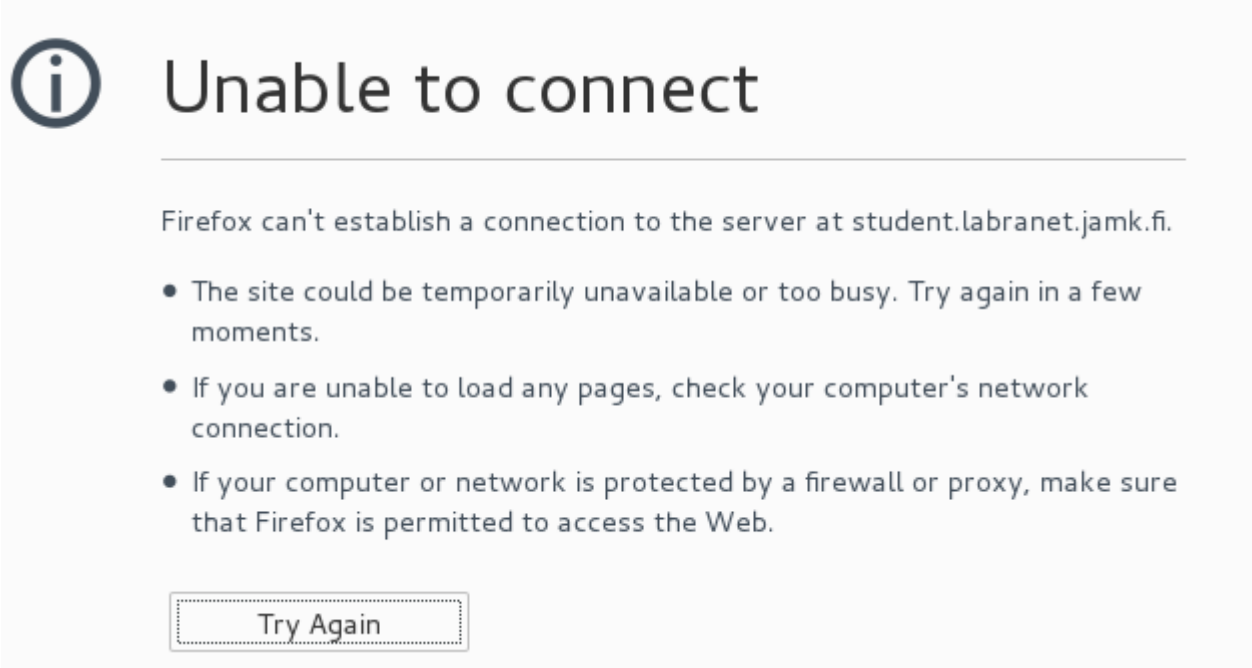
- 195.148.128.0/24 - Public services 1
- 195.148.129.0/24 - Public services 2



Save and Apply. Then create a firewall rule on LAN. Set Action as Block, Protocol: any and destination: alias Blocklist. NOTE! This rule must be at the top of the list (it's okay if it is below the anti-lockout rule).

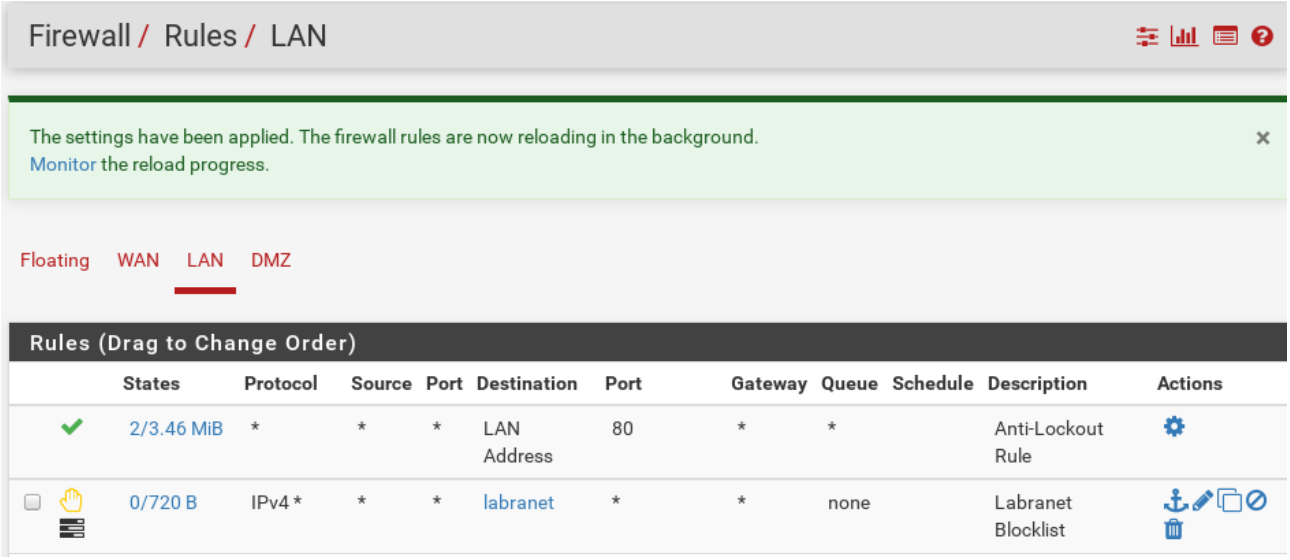


Apply changes and try to use JAMK services (www.jamk.fi, student.labranet.jamk.fi, etc.). If you find a service that still works, find out its IP block/address and add it to the alias.



www. Jamk.fi sivustolle erillinen alias:

Lastly, change the Action on the rule to Reject. Try accessing the pages now and see how this changes the response.



- **squidGuard URL filtering (2p)**

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 squidGuard
```

```
[root@localhost ~]# yum install -y squidGuard
```

Modify the configuration in /etc/squid/squidGuard.conf and remove the default 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 {
    domainlist deny/domains
    urllist deny/urls
    }

# ACL control using the previous deny
acl {
    default {
        pass !deny all
        redirect http://10.10.10.10/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 {
        domainlist deny/domains
        urllist deny/urls
}

# ACL control using the previous deny
acl {
        default {
                pass !deny all
                redirect http://10.10.10.10/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/domains
touch /var/lib/squidGuard/db/deny/urls
```

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

Now we can put URL blocklists in place. Let’s play totalitarian government. We want to block users to not see news, so put the following in the domains file:

```
yle.fi
ksml.fi
```

```
  GNU nano 2.3.1      File: /var/lib/squidGuard/db/deny/domains

yle.fi
ksml.fi_
```

We want to block politics and news on Reddit. We don't want to block the whole domain (leave an illusion of freedom), but luckily the Reddit uses subreddits. So put the following in the urls file:

```
reddit.com/r/politics
reddit.com/r/news
```

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

reddit.com/r/politics
reddit.com/r/news_
```

Update the databases and change ownership:

```
squidGuard -d -C all
chown -R squid. /var/lib/squidGuard/db/deny
```

```
[root@localhost ~]# squidGuard -d -C all
2017-02-02 12:28:25 [2775] New setting: dbhome: /var/lib/squidGuard/db
2017-02-02 12:28:25 [2775] New setting: logdir: /var/log/squidGuard
2017-02-02 12:28:25 [2775] init domainlist /var/lib/squidGuard/db/deny/
2017-02-02 12:28:25 [2775] create new dbfile /var/lib/squidGuard/db/de
.db
2017-02-02 12:28:25 [2775] init urllist /var/lib/squidGuard/db/deny/ur
2017-02-02 12:28:25 [2775] create new dbfile /var/lib/squidGuard/db/de
2017-02-02 12:28:25 [2775] squidGuard 1.4 started (1486031305.278)
2017-02-02 12:28:25 [2775] db update done
2017-02-02 12:28:25 [2775] squidGuard stopped (1486031305.296)
```

```
[root@localhost ~]# chown -R squid. /var/lib/squidGuard/db/deny/
```

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

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

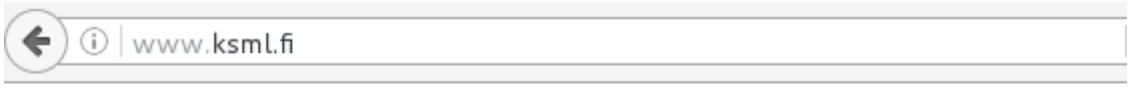
```
  GNU nano 2.3.1          File: /etc/squid/squid.conf                Modified

refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .               0       20%     4320

refresh_pattern -i \.(gif|png|jpg|jpeg|ico|bmp|)$ 260000 90% 260009 override-ex$

http_port 8080 ssl-bump cert=/etc/squid/ssl_cert/squidCA.pem generate-host-cert$
acl step1 at_step SslBump1
ssl_bump peek step1
ssl_bump bump all

# Rewrite rule

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

And restart squid:

```
systemctl restart squid
```

```
[root@localhost ~]# systemctl restart squid
```

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



Not Found

The requested URL /blocked.php was not found on this server.

Not Found

The requested URL /blocked.php was not found on this server.

Acces to is prohibited!
Your IP address is 192.168.1.101
This violation has been logged

Acces to is prohibited!
Your IP address is 192.168.1.101
This violation has been logged

- **Custom block page (1p)**

Let's create a custom page for the squidGuard to show to users. On the webserver, 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";
```

```
?>
```

Webserver [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

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

<?php

$address=$_GET['address'];
$url=$_GET['url'];
echo "Acces 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://10.10.10.10/blocked.php?url=%u&address=%a&n=%n
```

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

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

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

# ACL control using the previous deny
acl {
        default {
                pass !deny all
                redirect http://10.10.10.10/blocked.php?url=%i&address=%a&n=%n_
}
}
```

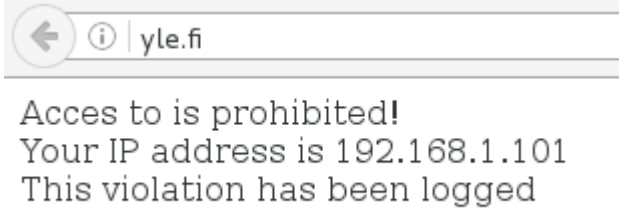
Let's also add logging, add the following after domain/urllists in dest deny:

```
log violations
```

```
  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 {
        domainlist deny/domains
        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.

```
[root@localhost ~]# systemctl restart squid
```




```
  GNU nano 2.3.1        File: /var/log/squidGuard/violations

2017-02-02 12:43:14 [3267] Request(default/deny/-) http://yle.fi/ 192.168.1.101$
2017-02-02 12:43:14 [3267] Request(default/deny/-) http://yle.fi/favicon.ico 19$
2017-02-02 12:43:14 [3267] Request(default/deny/-) http://yle.fi/favicon.ico 19$
```

BONUS: Install PfBlockerNG packet to PfSense and use it to block internet access to a whole country.