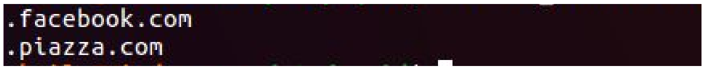
Parental Controls on the Network Level

group: apurai2

The goal of this project was to create a system where if someone is on a website for too long, then the network would stop any further connections to that specific url. Initially, the plan was to use tcpdump filters to calculate the network usage, however, there was no way to stop the network from preventing those connections. A DHCP server could be used to grab everyone on the network and split them up from there but, after spending way too long on unsuccessful run attempts, the idea was scrapped and squid proxy was used instead.

1. $ sudo apt-get install squid
2. $ sudo vim /etc/squid/squid.conf
3. Change squid.conf to the code in the github
4. $ touch /etc/squid/ban_domains.txt
5. In ban_domains.txt we want to specify what URLs we want to block, they have to be in the format of .example.com

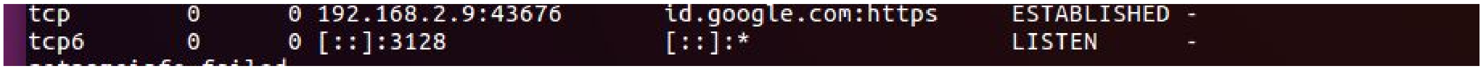


```
.facebook.com
.piazza.com
```

6. $ sudo service squid restart
7. $ sudo service squid status

   Make sure that status shows that squid is running, otherwise goto step 2

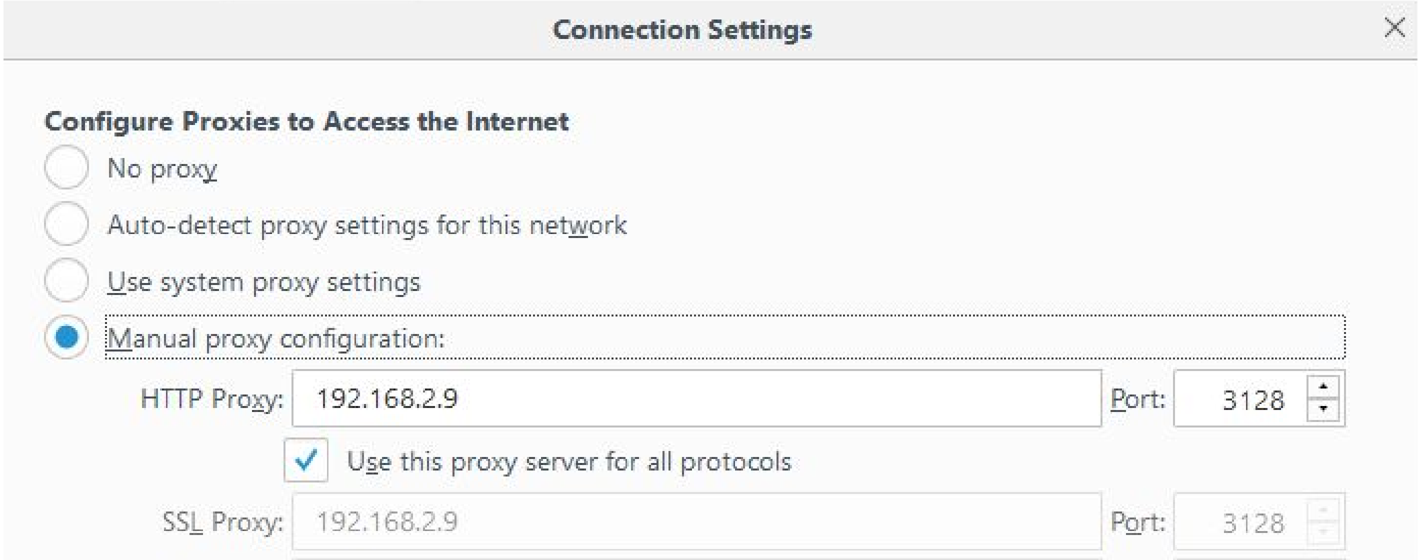
   $ netstat -tap ← can also be used to check if squid is running successfully on its port of 3128



```
tcp        0      0 192.168.2.9:43676       id.google.com:https     ESTABLISHED -
tcp6       0      0 [::]:3128               [::]:*                  LISTEN      -
```

8. Goto any pc on the network and set their browser's proxy settings.

Firefox's example: [192.168.2.9 is the ip of the pc hosting squid]



Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

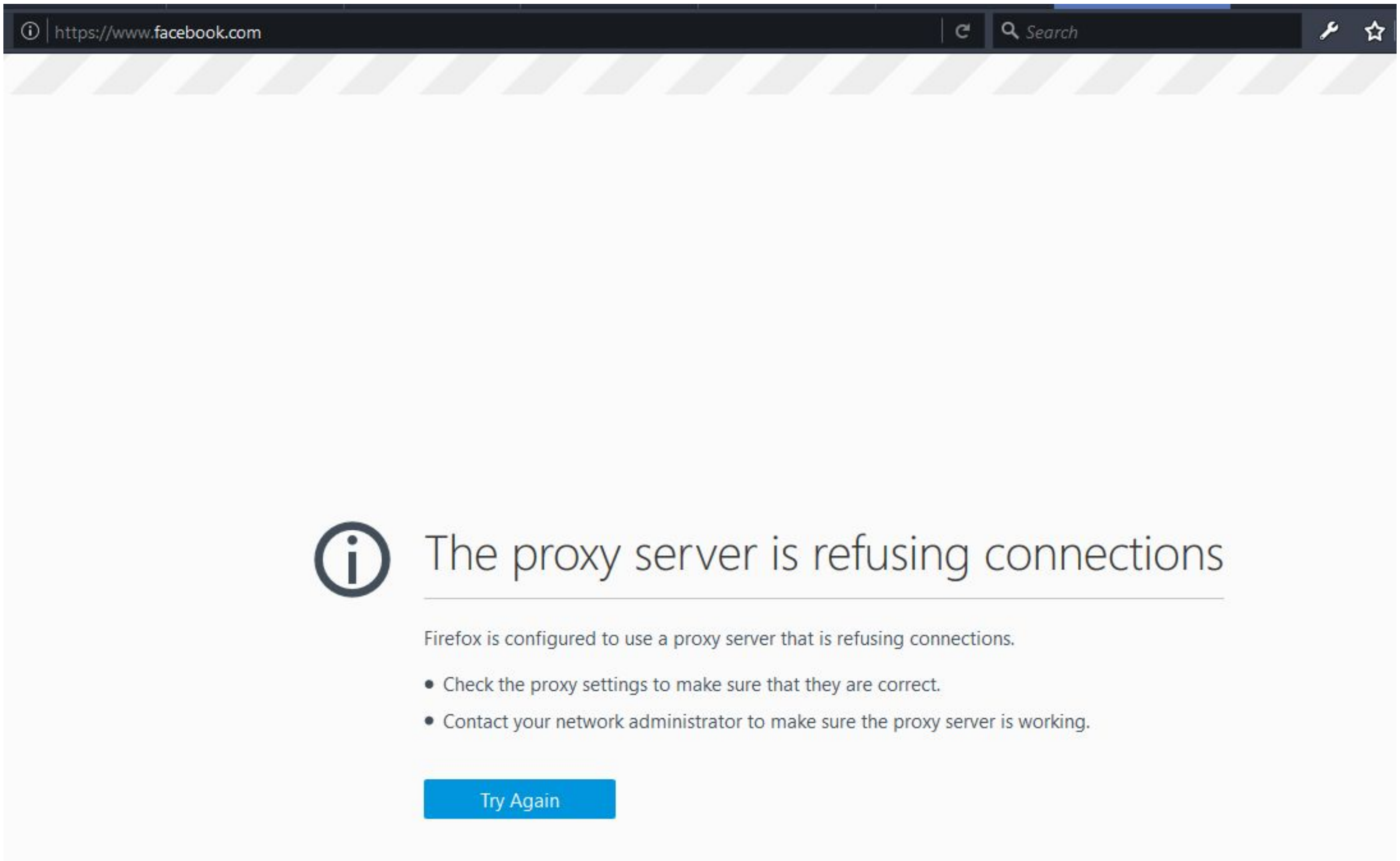
● Manual proxy configuration:

HTTP Proxy: 192.168.2.9 Port: 3128

☑ Use this proxy server for all protocols

SSL Proxy: 192.168.2.9 Port: 3128

Here's how a blocked website should look:



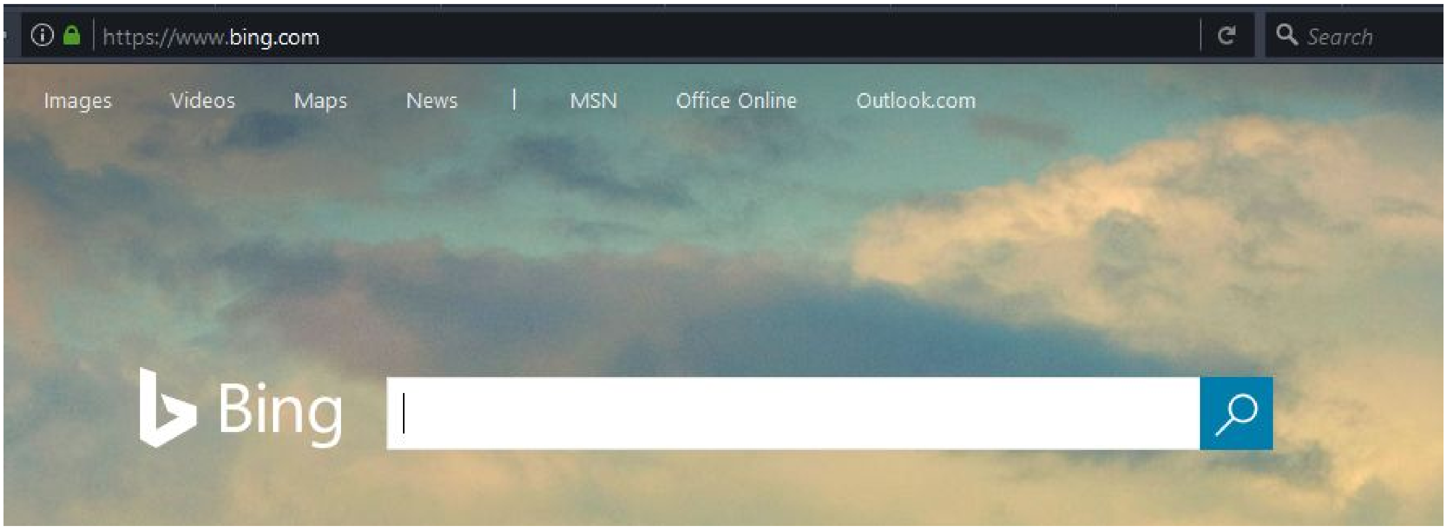
https://www.facebook.com

The proxy server is refusing connections

Firefox is configured to use a proxy server that is refusing connections.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

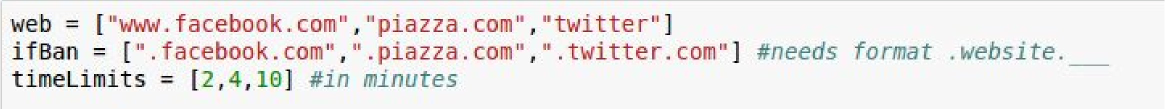
And here's an allowed website:



https://www.bing.com

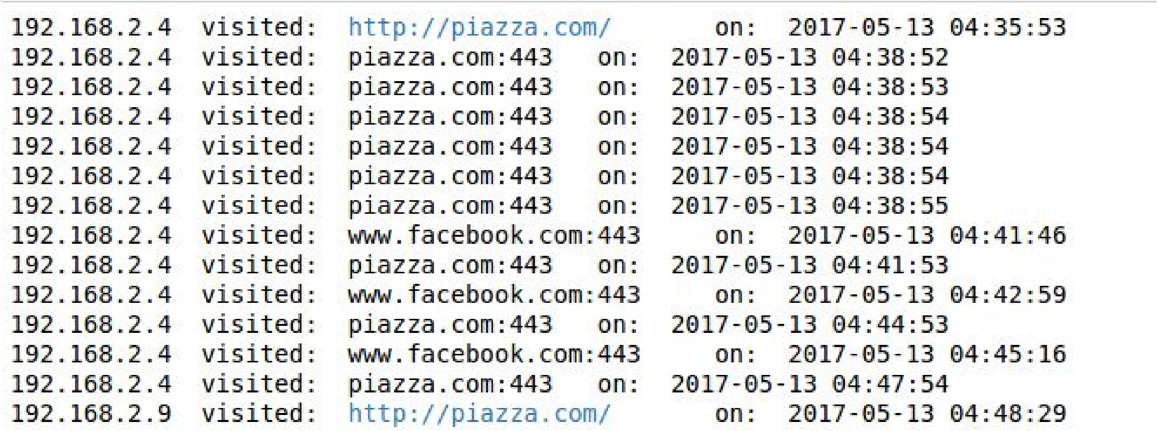
In the next steps, using the log information from squid, a python script will run through and find any URLs that are breaking their allowed time limit. Then those URLs will be placed in the ban_domains.txt file.

9. $ sudo chmod a+w /etc/squid/ban_domains.txt
10. $ sudo chmod a+r /var/log/squid/access.log
11. $ touch squidParser.py
12. Edit squidParser.py as included in github, including time limits of various websites in the process

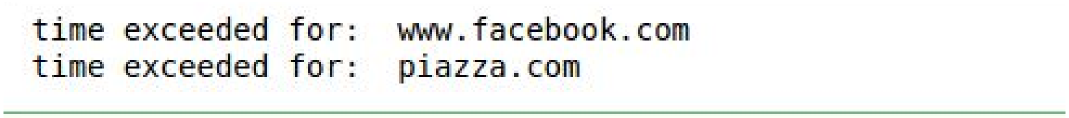


```
web = ["www.facebook.com","piazza.com","twitter"]
ifBan = [".facebook.com",".piazza.com",".twitter.com"] #needs format .website.
timeLimits = [2,4,10] #in minutes
```

13. Running squidParser.py, we obtain the ip, website, and timestamp of each website that we wanted to keep track of:



```
192.168.2.4  visited:  http://piazza.com/       on:  2017-05-13 04:35:53
192.168.2.4  visited:  piazza.com:443   on:  2017-05-13 04:38:52
192.168.2.4  visited:  piazza.com:443   on:  2017-05-13 04:38:53
192.168.2.4  visited:  piazza.com:443   on:  2017-05-13 04:38:54
192.168.2.4  visited:  piazza.com:443   on:  2017-05-13 04:38:54
192.168.2.4  visited:  piazza.com:443   on:  2017-05-13 04:38:54
192.168.2.4  visited:  piazza.com:443   on:  2017-05-13 04:38:55
192.168.2.4  visited:  www.facebook.com:443     on:  2017-05-13 04:41:46
192.168.2.4  visited:  piazza.com:443   on:  2017-05-13 04:41:53
192.168.2.4  visited:  www.facebook.com:443     on:  2017-05-13 04:42:59
192.168.2.4  visited:  piazza.com:443   on:  2017-05-13 04:44:53
192.168.2.4  visited:  www.facebook.com:443     on:  2017-05-13 04:45:16
192.168.2.4  visited:  piazza.com:443   on:  2017-05-13 04:47:54
192.168.2.9  visited:  http://piazza.com/       on:  2017-05-13 04:48:29
```



```
time exceeded for:  www.facebook.com
time exceeded for:  piazza.com
```

Although any time exceeds will be automatically added to ban_domains.txt, it is up to us to restart the squid server in order to implement these changes.

14. $ sudo service squid restart

Next Steps:

The next steps in this project would be setting up squid as transparent with iptables:

```
iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

It will cause everyone on the network to have to go through our squid proxy, without having to setup the proxy settings in each browser.