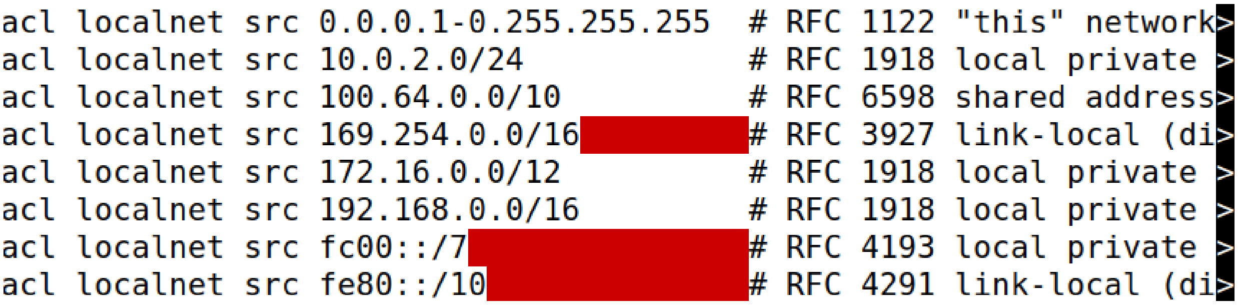
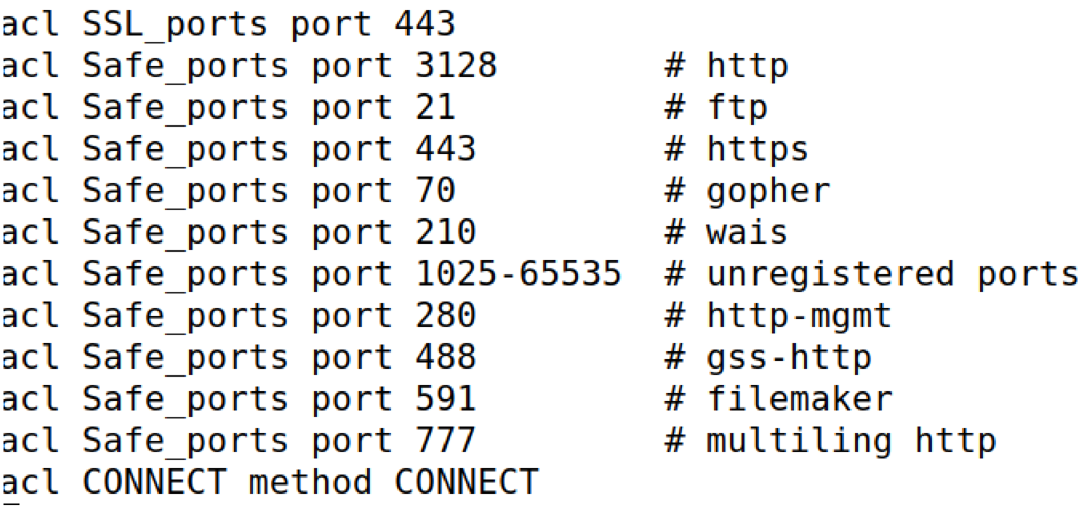
Aiden Green

- I decided to create a proxy in Ubuntu. I had configured a squid proxy to catch all the traffic and show the logs of what happened.



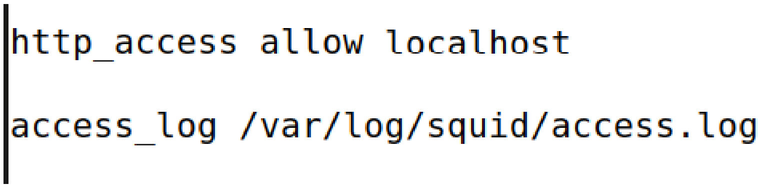
```
acl localnet src 0.0.0.1-0.255.255.255  # RFC 1122 "this" network>
acl localnet src 10.0.2.0/24            # RFC 1918 local private >
acl localnet src 100.64.0.0/10          # RFC 6598 shared address>
acl localnet src 169.254.0.0/16         # RFC 3927 link-local (di>
acl localnet src 172.16.0.0/12          # RFC 1918 local private >
acl localnet src 192.168.0.0/16         # RFC 1918 local private >
acl localnet src fc00::/7               # RFC 4193 local private >
acl localnet src fe80::/10              # RFC 4291 link-local (di>
```

- /etc/squid/squid.conf
- Above was configured for our designated IP address.
- It is the 10.0.2.0/24



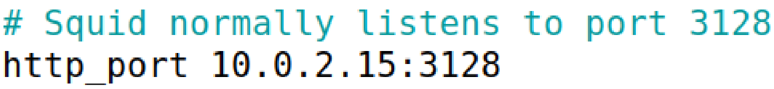
```
acl SSL_ports port 443
acl Safe_ports port 3128        # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
```

- This is just an added change to the port number



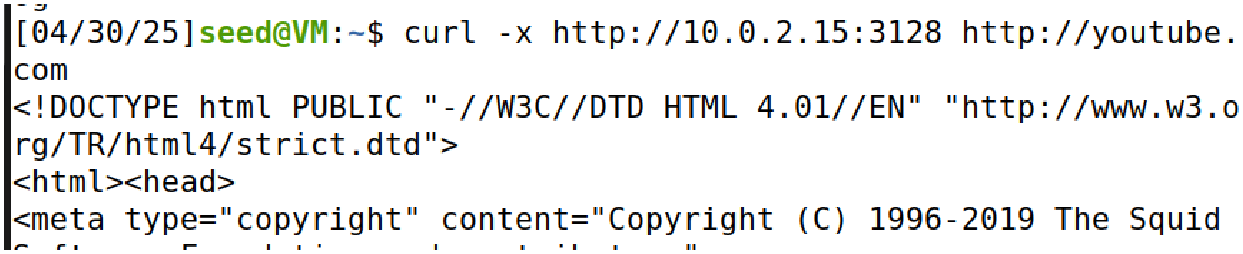
```
http_access allow localhost

access_log /var/log/squid/access.log
```

- This is added to allow me to access http and catch them in the log file



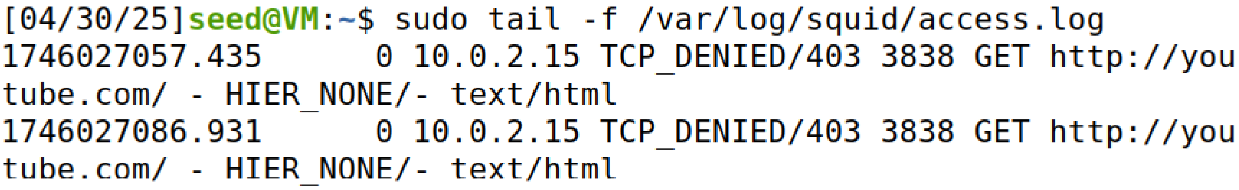
```
# Squid normally listens to port 3128
http_port 10.0.2.15:3128
```

- This is where the squid will be listening on port 3128



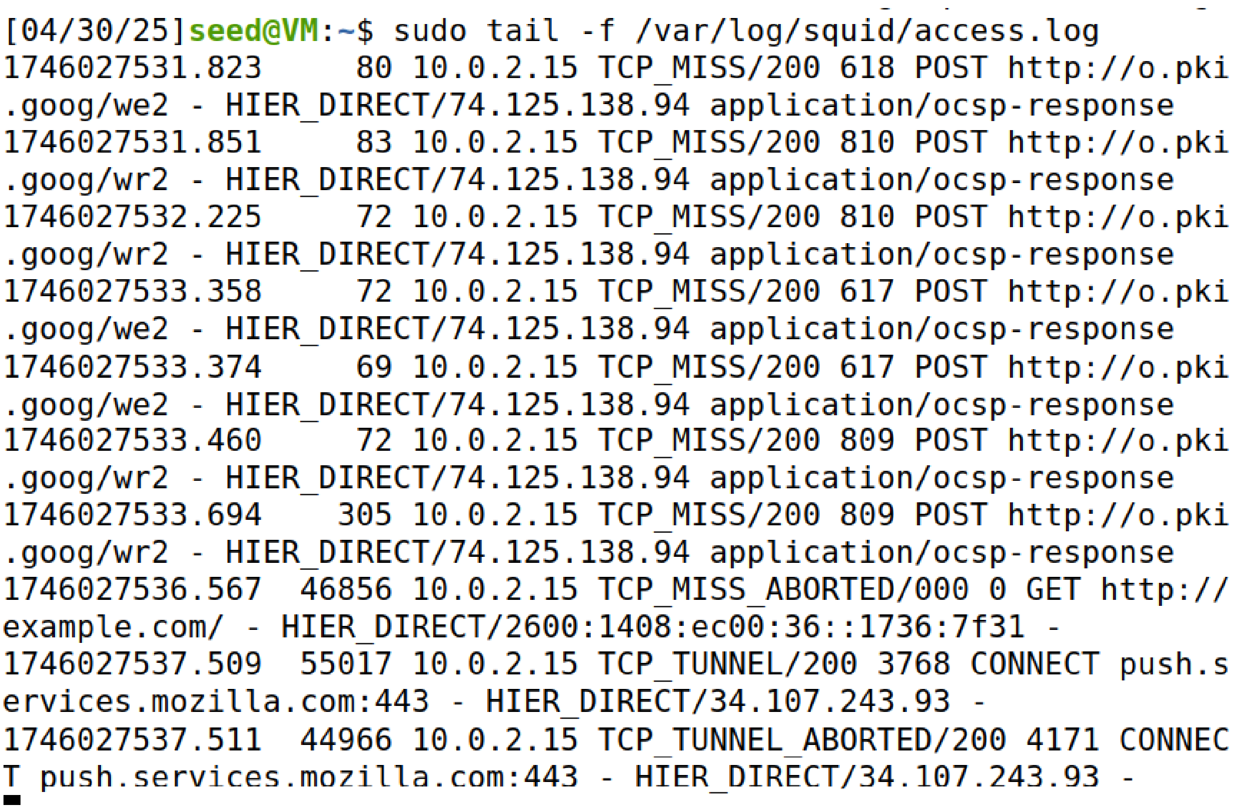
```
[04/30/25]seed@VM:~$ curl -x http://10.0.2.15:3128 http://youtube.
com
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.o
rg/TR/html4/strict.dtd">
<html><head>
<meta type="copyright" content="Copyright (C) 1996-2019 The Squid
```

- This is an example in terminal of accessing youtube through the proxy server



```
[04/30/25]seed@VM:~$ sudo tail -f /var/log/squid/access.log
1746027057.435      0 10.0.2.15 TCP_DENIED/403 3838 GET http://you
tube.com/ - HIER_NONE/- text/html
1746027086.931      0 10.0.2.15 TCP_DENIED/403 3838 GET http://you
tube.com/ - HIER_NONE/- text/html
```

- You can see TCP DENIED and the link address
- However, when access through a browser and configured with the proxy you can see this in the log file below



```
[04/30/25]seed@VM:~$ sudo tail -f /var/log/squid/access.log
1746027531.823     80 10.0.2.15 TCP_MISS/200 618 POST http://o.pki
.goog/we2 - HIER_DIRECT/74.125.138.94 application/ocsp-response
1746027531.851     83 10.0.2.15 TCP_MISS/200 810 POST http://o.pki
.goog/wr2 - HIER_DIRECT/74.125.138.94 application/ocsp-response
1746027532.225     72 10.0.2.15 TCP_MISS/200 810 POST http://o.pki
.goog/wr2 - HIER_DIRECT/74.125.138.94 application/ocsp-response
1746027533.358     72 10.0.2.15 TCP_MISS/200 617 POST http://o.pki
.goog/we2 - HIER_DIRECT/74.125.138.94 application/ocsp-response
1746027533.374     69 10.0.2.15 TCP_MISS/200 617 POST http://o.pki
.goog/we2 - HIER_DIRECT/74.125.138.94 application/ocsp-response
1746027533.460     72 10.0.2.15 TCP_MISS/200 809 POST http://o.pki
.goog/wr2 - HIER_DIRECT/74.125.138.94 application/ocsp-response
1746027533.694    305 10.0.2.15 TCP_MISS/200 809 POST http://o.pki
.goog/wr2 - HIER_DIRECT/74.125.138.94 application/ocsp-response
1746027536.567  46856 10.0.2.15 TCP_MISS_ABORTED/000 0 GET http://
example.com/ - HIER_DIRECT/2600:1408:ec00:36::1736:7f31 -
1746027537.509  55017 10.0.2.15 TCP_TUNNEL/200 3768 CONNECT push.s
ervices.mozilla.com:443 - HIER_DIRECT/34.107.243.93 -
1746027537.511  44966 10.0.2.15 TCP_TUNNEL_ABORTED/200 4171 CONNEC
T push.services.mozilla.com:443 - HIER_DIRECT/34.107.243.93 -
```

- 10.0.2.15 = Client IP address
- HIER_DIRECT/172.217.4.35 = Squid connected directly to Google's IP