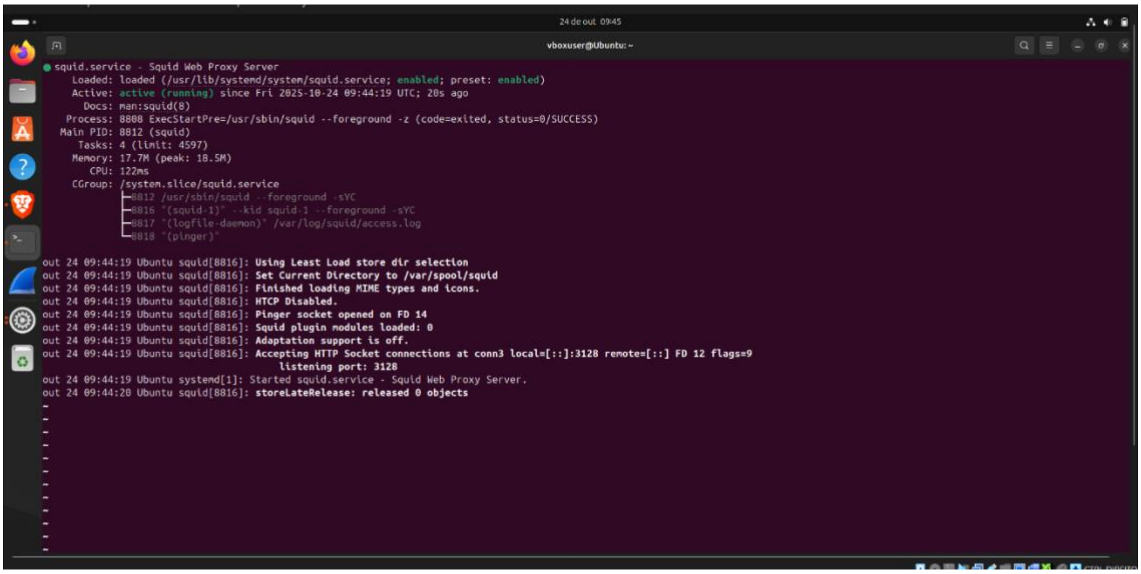
Francisco Martins

Miguel Marques

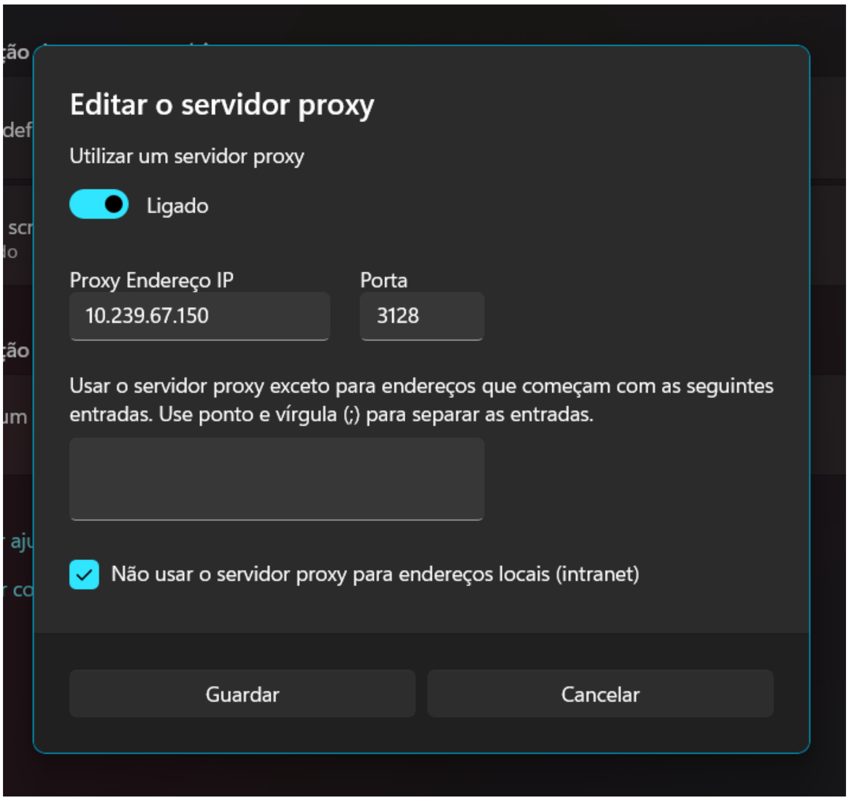
HTTP Proxy

Menu de status do Squid



```
● squid.service - Squid Web Proxy Server
     Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-10-24 09:44:19 UTC; 20s ago
       Docs: man:squid(8)
    Process: 8808 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
   Main PID: 8812 (squid)
      Tasks: 4 (limit: 4597)
     Memory: 17.7M (peak: 18.5M)
        CPU: 122ms
     CGroup: /system.slice/squid.service
             ├─8812 /usr/sbin/squid --foreground -sYC
             ├─8816 "(squid-1)" --kid squid-1 --foreground -sYC
             ├─8817 "(logfile-daemon)" /var/log/squid/access.log
             └─8818 "(pinger)"

out 24 09:44:19 Ubuntu squid[8816]: Using Least Load store dir selection
out 24 09:44:19 Ubuntu squid[8816]: Set Current Directory to /var/spool/squid
out 24 09:44:19 Ubuntu squid[8816]: Finished loading MIME types and icons.
out 24 09:44:19 Ubuntu squid[8816]: HTCP Disabled.
out 24 09:44:19 Ubuntu squid[8816]: Pinger socket opened on FD 14
out 24 09:44:19 Ubuntu squid[8816]: Squid plugin modules loaded: 0
out 24 09:44:19 Ubuntu squid[8816]: Adaptation support is off.
out 24 09:44:19 Ubuntu squid[8816]: Accepting HTTP Socket connections at conn3 local=[::]:3128 remote=[::] FD 12 flags=9
                                        listening port: 3128
out 24 09:44:19 Ubuntu systemd[1]: Started squid.service - Squid Web Proxy Server.
out 24 09:44:20 Ubuntu squid[8816]: storeLateRelease: released 0 objects
~
~
~
~
~
~
~
~
~
~
~
~
```

IP e Porta do proxy na maquina real



Editar o servidor proxy

Utilizar um servidor proxy

● Ligado

Proxy Endereço IP: 10.239.67.150

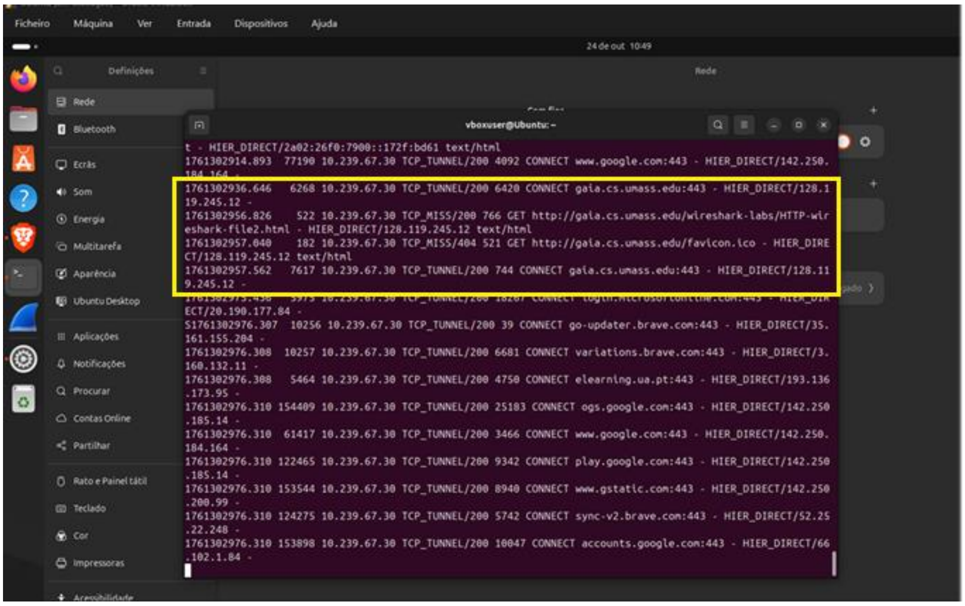
Porta: 3128

Usar o servidor proxy exceto para endereços que começam com as seguintes entradas. Use ponto e vírgula (;) para separar as entradas.

☑ Não usar o servidor proxy para endereços locais (intranet)

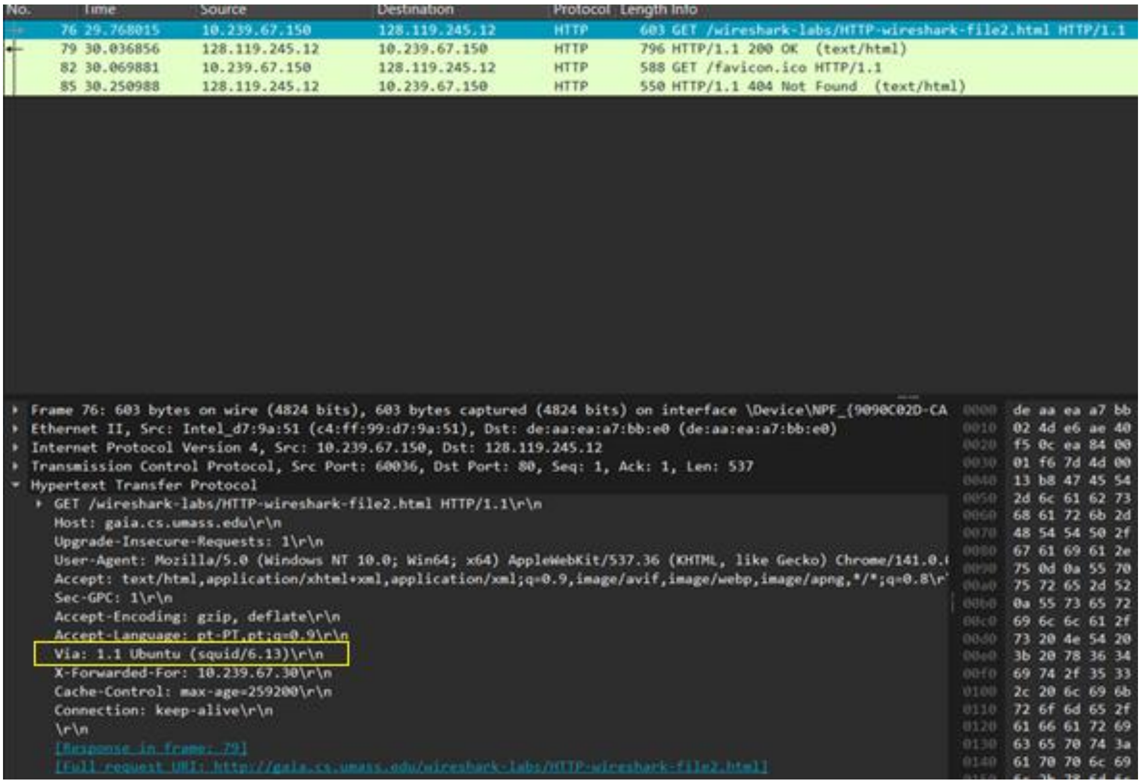
EX4:

Foi usado este código “sudo tail -f /var/log/squid/access.log” para ver se o proxy estava a funcionar e abriu a seguinte aba:



```
t - HIER_DIRECT/2a02:26f0:7900::172f:bd61 text/html
1761302914.893  77190 10.239.67.30 TCP_TUNNEL/200 4092 CONNECT www.google.com:443 - HIER_DIRECT/142.250.
184.164 -
1761302936.646   6268 10.239.67.30 TCP_TUNNEL/200 6420 CONNECT gaia.cs.umass.edu:443 - HIER_DIRECT/128.1
19.245.12 -
1761302956.826    522 10.239.67.30 TCP_MISS/200 766 GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wir
eshark-file2.html - HIER_DIRECT/128.119.245.12 text/html
1761302957.040    182 10.239.67.30 TCP_MISS/404 521 GET http://gaia.cs.umass.edu/favicon.ico - HIER_DIRE
CT/128.119.245.12 text/html
1761302957.562   7617 10.239.67.30 TCP_TUNNEL/200 744 CONNECT gaia.cs.umass.edu:443 - HIER_DIRECT/128.11
9.245.12 -
1761302975.436   5975 10.239.67.30 TCP_TUNNEL/200 18267 CONNECT login.microsoftonline.com:443 - HIER_DIR
ECT/20.190.177.84 -
S1761302976.307  10256 10.239.67.30 TCP_TUNNEL/200 39 CONNECT go-updater.brave.com:443 - HIER_DIRECT/35.
161.155.204 -
1761302976.308  10257 10.239.67.30 TCP_TUNNEL/200 6681 CONNECT variations.brave.com:443 - HIER_DIRECT/3.
160.132.11 -
1761302976.308   5464 10.239.67.30 TCP_TUNNEL/200 4750 CONNECT elearning.ua.pt:443 - HIER_DIRECT/193.136
.173.95 -
1761302976.310 154409 10.239.67.30 TCP_TUNNEL/200 25183 CONNECT ogs.google.com:443 - HIER_DIRECT/142.250
.185.14 -
1761302976.310  61417 10.239.67.30 TCP_TUNNEL/200 3466 CONNECT www.google.com:443 - HIER_DIRECT/142.250.
184.164 -
1761302976.310 122465 10.239.67.30 TCP_TUNNEL/200 9342 CONNECT play.google.com:443 - HIER_DIRECT/142.250
.185.14 -
1761302976.310 153544 10.239.67.30 TCP_TUNNEL/200 8940 CONNECT www.gstatic.com:443 - HIER_DIRECT/142.250
.200.99 -
1761302976.310 124275 10.239.67.30 TCP_TUNNEL/200 5742 CONNECT sync-v2.brave.com:443 - HIER_DIRECT/52.25
.22.248 -
1761302976.310 153898 10.239.67.30 TCP_TUNNEL/200 10047 CONNECT accounts.google.com:443 - HIER_DIRECT/66
.102.1.84 -
```

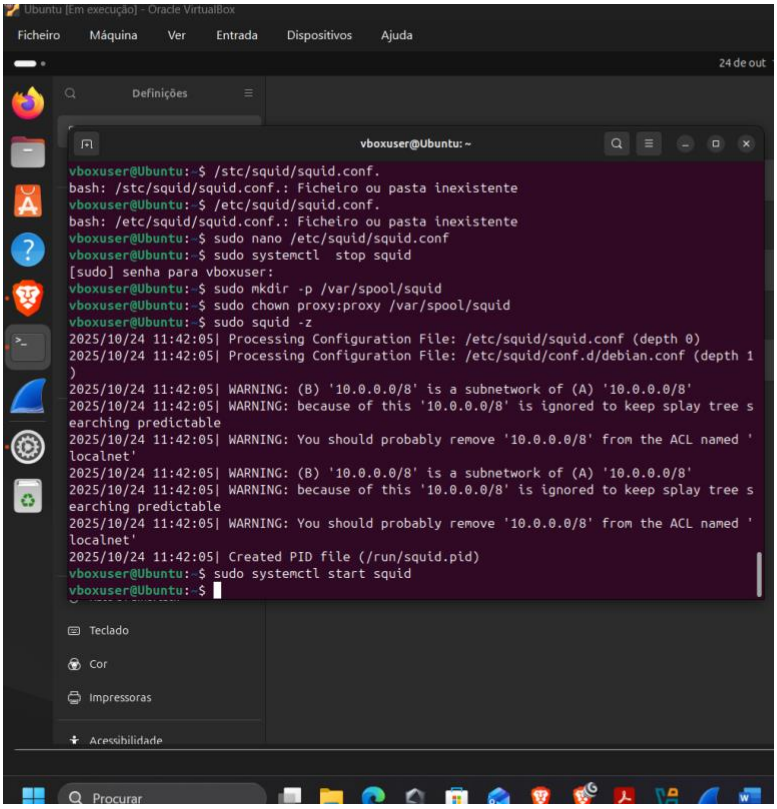
De seguida fomos ao wireshark para confirmar e ver as diferenças, como esta marcado



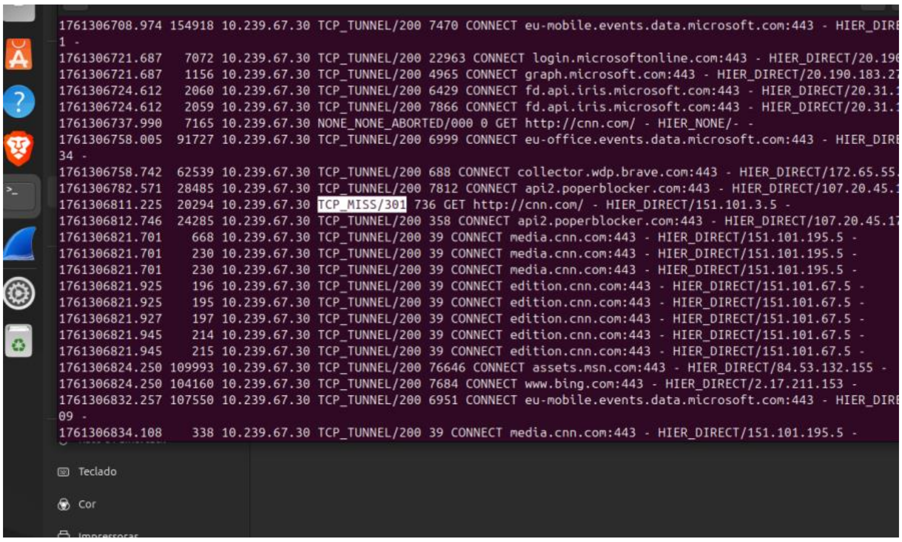
```
No.   Time        Source           Destination      Protocol Length Info
  76 29.768015   10.239.67.150    128.119.245.12   HTTP      603 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  79 30.036856   128.119.245.12   10.239.67.150    HTTP      796 HTTP/1.1 200 OK  (text/html)
  82 30.069881   10.239.67.150    128.119.245.12   HTTP      588 GET /favicon.ico HTTP/1.1
  85 30.250988   128.119.245.12   10.239.67.150    HTTP      550 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 76: 603 bytes on wire (4824 bits), 603 bytes captured (4824 bits) on interface \Device\NPF_{9090C02D-CA   0000  de aa ea a7 bb
> Ethernet II, Src: Intel_d7:9a:51 (c4:ff:99:d7:9a:51), Dst: de:aa:ea:a7:bb:e0 (de:aa:ea:a7:bb:e0)             0010  02 4d e6 ae 40
> Internet Protocol Version 4, Src: 10.239.67.150, Dst: 128.119.245.12                                           0020  f5 0c ea 84 00
> Transmission Control Protocol, Src Port: 60036, Dst Port: 80, Seq: 1, Ack: 1, Len: 537                         0030  01 f6 7d 4d 00
v Hypertext Transfer Protocol                                                                                    0040  13 b8 47 45 54
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n                                                   0050  2d 6c 61 62 73
    Host: gaia.cs.umass.edu\r\n                                                                                  0060  68 61 72 6b 2d
    Upgrade-Insecure-Requests: 1\r\n                                                                             0070  48 54 54 50 2f
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.(  0080  67 61 69 61 2e
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8\r'  0090  75 0d 0a 55 70
    Sec-GPC: 1\r\n                                                                                               00a0  75 72 65 2d 52
    Accept-Encoding: gzip, deflate\r\n                                                                           00b0  0a 55 73 65 72
    Accept-Language: pt-PT,pt;q=0.9\r\n                                                                          00c0  69 6c 6c 61 2f
    Via: 1.1 Ubuntu (squid/6.13)\r\n                                                                             00d0  73 20 4e 54 20
    X-Forwarded-For: 10.239.67.30\r\n                                                                            00e0  3b 20 78 36 34
    Cache-Control: max-age=259200\r\n                                                                            00f0  69 74 2f 35 33
    Connection: keep-alive\r\n                                                                                   0100  2c 20 6c 69 6b
    \r\n                                                                                                         0110  72 6f 6d 65 2f
    [Response in frame: 79]                                                                                      0120  61 66 61 72 69
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]                        0130  63 65 70 74 3a
                                                                                                                 0140  61 70 70 6c 69
```

Fomos ver o cache do Proxy

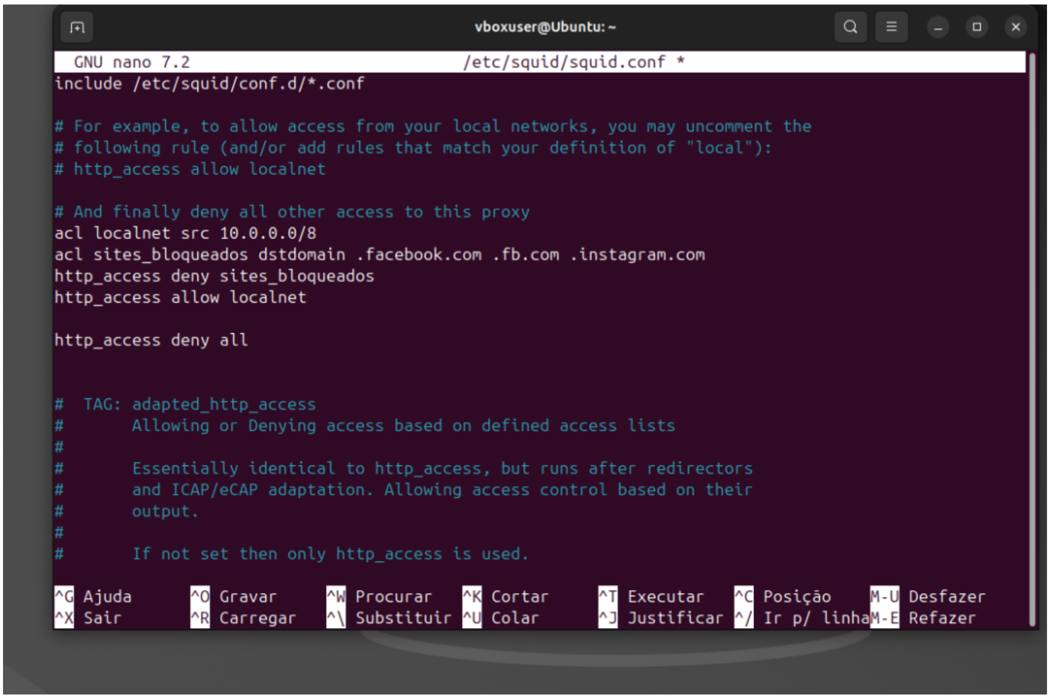


```
vboxuser@Ubuntu:~$ /stc/squid/squid.conf.
bash: /stc/squid/squid.conf.: Ficheiro ou pasta inexistente
vboxuser@Ubuntu:~$ /etc/squid/squid.conf.
bash: /etc/squid/squid.conf.: Ficheiro ou pasta inexistente
vboxuser@Ubuntu:~$ sudo nano /etc/squid/squid.conf
vboxuser@Ubuntu:~$ sudo systemctl  stop squid
[sudo] senha para vboxuser:
vboxuser@Ubuntu:~$ sudo mkdir -p /var/spool/squid
vboxuser@Ubuntu:~$ sudo chown proxy:proxy /var/spool/squid
vboxuser@Ubuntu:~$ sudo squid -z
2025/10/24 11:42:05| Processing Configuration File: /etc/squid/squid.conf (depth 0)
2025/10/24 11:42:05| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1
)
2025/10/24 11:42:05| WARNING: (B) '10.0.0.0/8' is a subnetwork of (A) '10.0.0.0/8'
2025/10/24 11:42:05| WARNING: because of this '10.0.0.0/8' is ignored to keep splay tree s
earching predictable
2025/10/24 11:42:05| WARNING: You should probably remove '10.0.0.0/8' from the ACL named '
localnet'
2025/10/24 11:42:05| WARNING: (B) '10.0.0.0/8' is a subnetwork of (A) '10.0.0.0/8'
2025/10/24 11:42:05| WARNING: because of this '10.0.0.0/8' is ignored to keep splay tree s
earching predictable
2025/10/24 11:42:05| WARNING: You should probably remove '10.0.0.0/8' from the ACL named '
localnet'
2025/10/24 11:42:05| Created PID file (/run/squid.pid)
vboxuser@Ubuntu:~$ sudo systemctl start squid
vboxuser@Ubuntu:~$ 
```

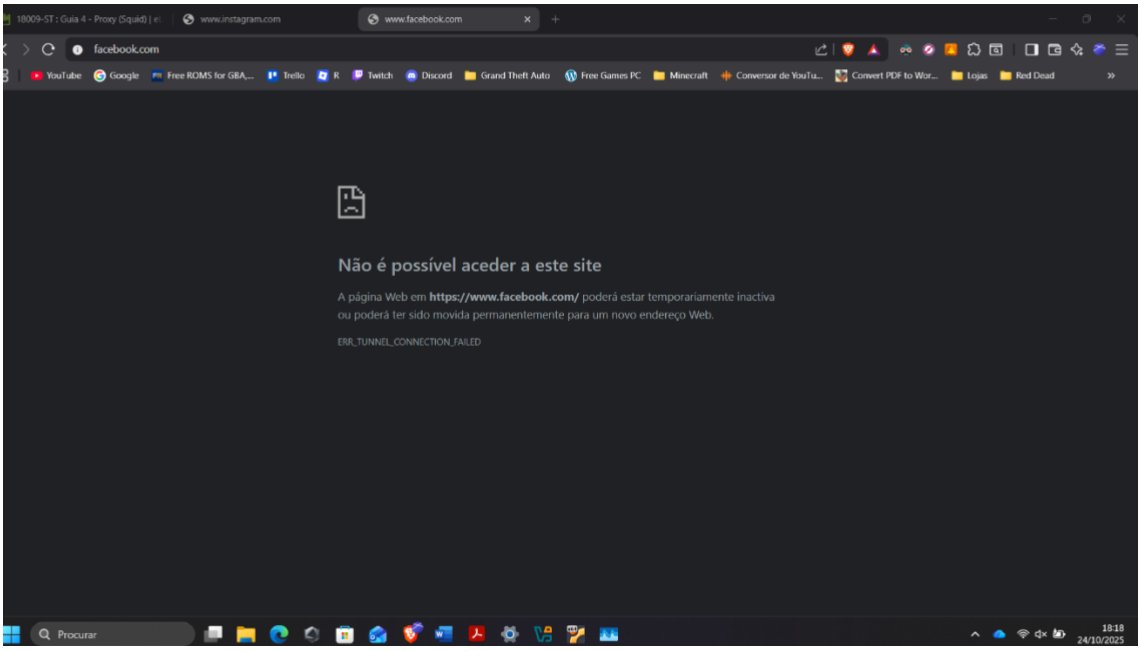


```
1761306708.974 154918 10.239.67.30 TCP_TUNNEL/200 7470 CONNECT eu-mobile.events.data.microsoft.com:443 - HIER_DIRE
1 -
1761306721.687   7072 10.239.67.30 TCP_TUNNEL/200 22963 CONNECT login.microsoftonline.com:443 - HIER_DIRECT/20.190
1761306721.687   1156 10.239.67.30 TCP_TUNNEL/200 4965 CONNECT graph.microsoft.com:443 - HIER_DIRECT/20.190.183.2
1761306724.612   2060 10.239.67.30 TCP_TUNNEL/200 6429 CONNECT fd.api.iris.microsoft.com:443 - HIER_DIRECT/20.31.
1761306724.612   2059 10.239.67.30 TCP_TUNNEL/200 7866 CONNECT fd.api.iris.microsoft.com:443 - HIER_DIRECT/20.31.
1761306737.990   7165 10.239.67.30 NONE_NONE_ABORTED/000 0 GET http://cnn.com/ - HIER_NONE/- -
1761306758.005  91727 10.239.67.30 TCP_TUNNEL/200 6999 CONNECT eu-office.events.data.microsoft.com:443 - HIER_DIRE
34 -
1761306758.742  62539 10.239.67.30 TCP_TUNNEL/200 688 CONNECT collector.wdp.brave.com:443 - HIER_DIRECT/172.65.55.
1761306782.571  28485 10.239.67.30 TCP_TUNNEL/200 7812 CONNECT api2.poperblocker.com:443 - HIER_DIRECT/107.20.45.
1761306811.225  20294 10.239.67.30 TCP_MISS/301 736 GET http://cnn.com/ - HIER_DIRECT/151.101.3.5 -
1761306812.746  24285 10.239.67.30 TCP_TUNNEL/200 358 CONNECT api2.poperblocker.com:443 - HIER_DIRECT/107.20.45.1
1761306821.701    668 10.239.67.30 TCP_TUNNEL/200 39 CONNECT media.cnn.com:443 - HIER_DIRECT/151.101.195.5 -
1761306821.701    230 10.239.67.30 TCP_TUNNEL/200 39 CONNECT media.cnn.com:443 - HIER_DIRECT/151.101.195.5 -
1761306821.701    230 10.239.67.30 TCP_TUNNEL/200 39 CONNECT media.cnn.com:443 - HIER_DIRECT/151.101.195.5 -
1761306821.925    196 10.239.67.30 TCP_TUNNEL/200 39 CONNECT edition.cnn.com:443 - HIER_DIRECT/151.101.67.5 -
1761306821.925    195 10.239.67.30 TCP_TUNNEL/200 39 CONNECT edition.cnn.com:443 - HIER_DIRECT/151.101.67.5 -
1761306821.927    197 10.239.67.30 TCP_TUNNEL/200 39 CONNECT edition.cnn.com:443 - HIER_DIRECT/151.101.67.5 -
1761306821.945    214 10.239.67.30 TCP_TUNNEL/200 39 CONNECT edition.cnn.com:443 - HIER_DIRECT/151.101.67.5 -
1761306821.945    215 10.239.67.30 TCP_TUNNEL/200 39 CONNECT edition.cnn.com:443 - HIER_DIRECT/151.101.67.5 -
1761306824.250 109993 10.239.67.30 TCP_TUNNEL/200 76646 CONNECT assets.msn.com:443 - HIER_DIRECT/84.53.132.155 -
1761306824.250 104160 10.239.67.30 TCP_TUNNEL/200 7684 CONNECT www.bing.com:443 - HIER_DIRECT/2.17.211.153 -
1761306832.257 107550 10.239.67.30 TCP_TUNNEL/200 6951 CONNECT eu-mobile.events.data.microsoft.com:443 - HIER_DIRE
09 -
1761306834.108    338 10.239.67.30 TCP_TUNNEL/200 39 CONNECT media.cnn.com:443 - HIER_DIRECT/151.101.195.5 -
```

Bloqueamos o domínio



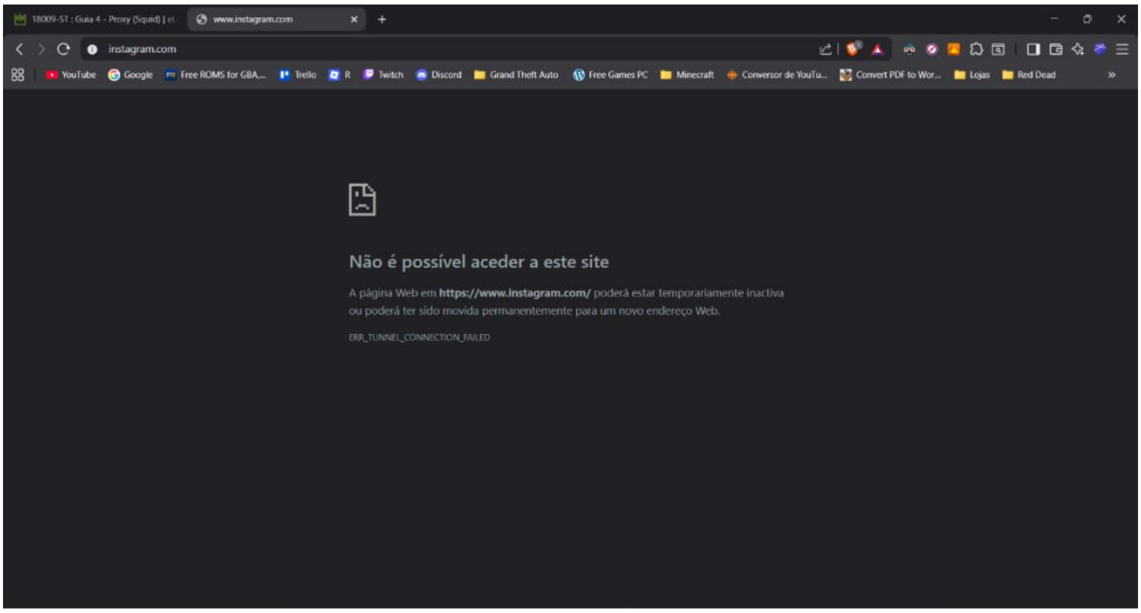
```
  GNU nano 7.2                        /etc/squid/squid.conf *
include /etc/squid/conf.d/*.conf

# For example, to allow access from your local networks, you may uncomment the
# following rule (and/or add rules that match your definition of "local"):
# http_access allow localnet

# And finally deny all other access to this proxy
acl localnet src 10.0.0.0/8
acl sites_bloqueados dstdomain .facebook.com .fb.com .instagram.com
http_access deny sites_bloqueados
http_access allow localnet

http_access deny all


#  TAG: adapted_http_access
#       Allowing or Denying access based on defined access lists
#
#       Essentially identical to http_access, but runs after redirectors
#       and ICAP/eCAP adaptation. Allowing access control based on their
#       output.
#
#       If not set then only http_access is used.

^G Ajuda      ^O Gravar     ^W Procurar   ^K Cortar     ^T Executar   ^C Posição    M-U Desfazer
^X Sair       ^R Carregar   ^\ Substituir ^U Colar      ^J Justificar ^/ Ir p/ linhaM-E Refazer
```



Não é possível aceder a este site

A página Web em **https://www.facebook.com/** poderá estar temporariamente inactiva ou poderá ter sido movida permanentemente para um novo endereço Web.

ERR_TUNNEL_CONNECTION_FAILED



Não é possível aceder a este site

A página Web em **https://www.instagram.com/** poderá estar temporariamente inactiva ou poderá ter sido movida permanentemente para um novo endereço Web.

ERR_TUNNEL_CONNECTION_FAILED