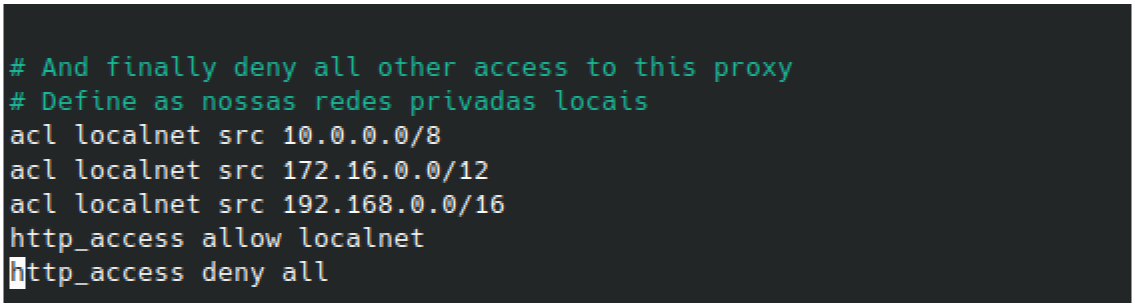
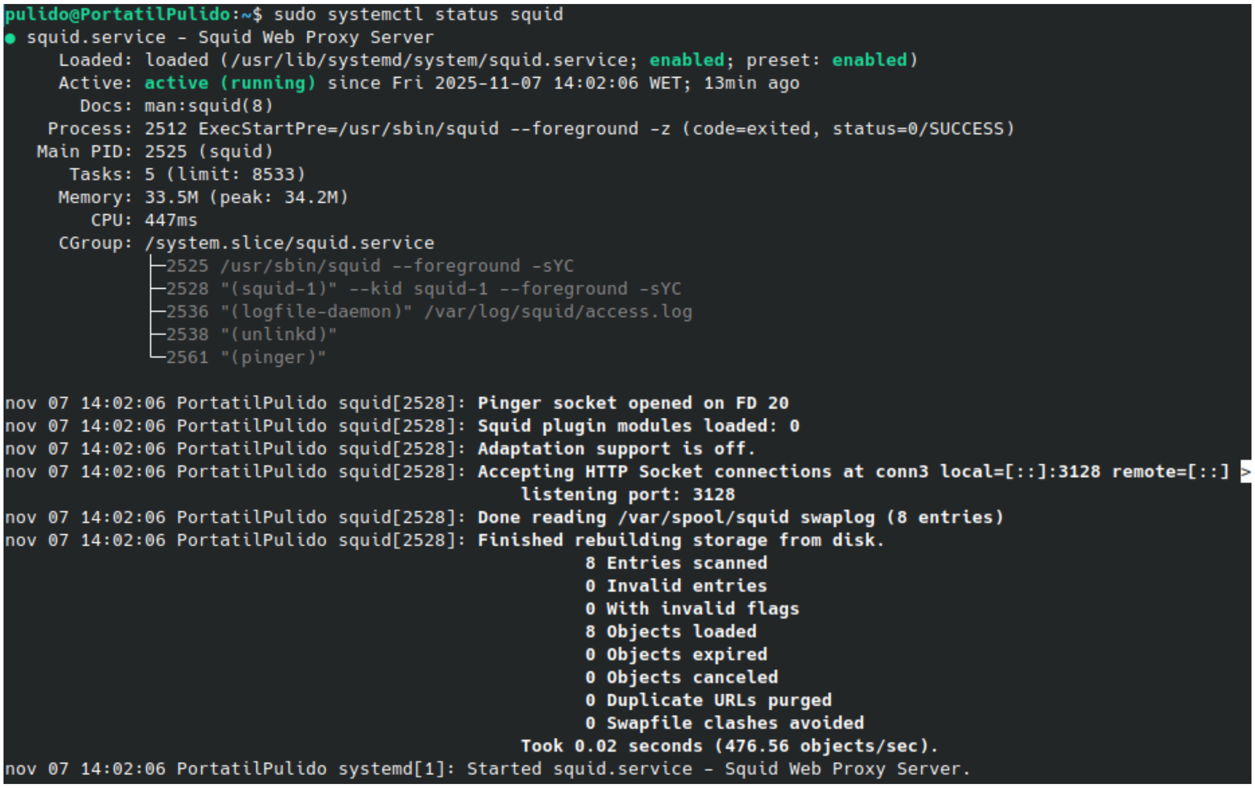
Guião 4 Squid Proxy **Ricardo Pulido**

Usando a mesma maquina para proxy e para cliente.

2.

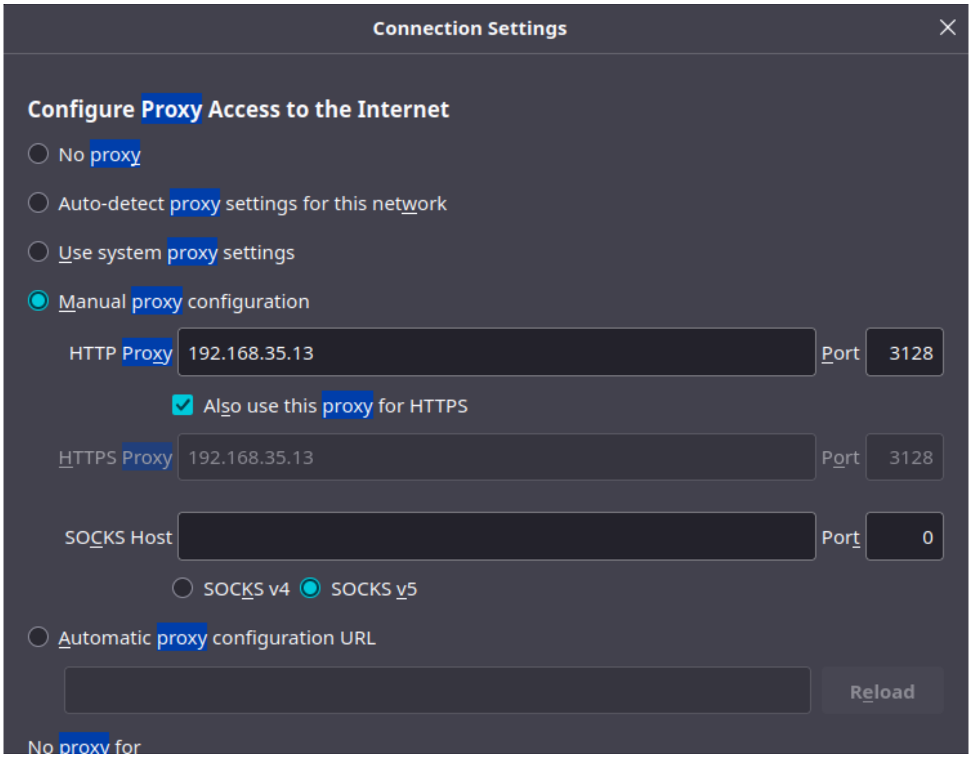


```
# And finally deny all other access to this proxy
# Define as nossas redes privadas locais
acl localnet src 10.0.0.0/8
acl localnet src 172.16.0.0/12
acl localnet src 192.168.0.0/16
http_access allow localnet
http_access deny all
```



```
pulido@PortatilPulido:~$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
     Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-11-07 14:02:06 WET; 13min ago
       Docs: man:squid(8)
    Process: 2512 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
   Main PID: 2525 (squid)
      Tasks: 5 (limit: 8533)
     Memory: 33.5M (peak: 34.2M)
        CPU: 447ms
     CGroup: /system.slice/squid.service
             ├─2525 /usr/sbin/squid --foreground -sYC
             ├─2528 "(squid-1)" --kid squid-1 --foreground -sYC
             ├─2536 "(logfile-daemon)" /var/log/squid/access.log
             ├─2538 "(unlinkd)"
             └─2561 "(pinger)"

nov 07 14:02:06 PortatilPulido squid[2528]: Pinger socket opened on FD 20
nov 07 14:02:06 PortatilPulido squid[2528]: Squid plugin modules loaded: 0
nov 07 14:02:06 PortatilPulido squid[2528]: Adaptation support is off.
nov 07 14:02:06 PortatilPulido squid[2528]: Accepting HTTP Socket connections at conn3 local=[::]:3128 remote=[::] >
                                                listening port: 3128
nov 07 14:02:06 PortatilPulido squid[2528]: Done reading /var/spool/squid swaplog (8 entries)
nov 07 14:02:06 PortatilPulido squid[2528]: Finished rebuilding storage from disk.
                                                      8 Entries scanned
                                                      0 Invalid entries
                                                      0 With invalid flags
                                                      8 Objects loaded
                                                      0 Objects expired
                                                      0 Objects canceled
                                                      0 Duplicate URLs purged
                                                      0 Swapfile clashes avoided
                                                Took 0.02 seconds (476.56 objects/sec).
nov 07 14:02:06 PortatilPulido systemd[1]: Started squid.service - Squid Web Proxy Server.
```

3.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 192.168.35.13 Port 3128

☑ Also use this proxy for HTTPS

HTTPS Proxy 192.168.35.13 Port 3128

SOCKS Host Port 0

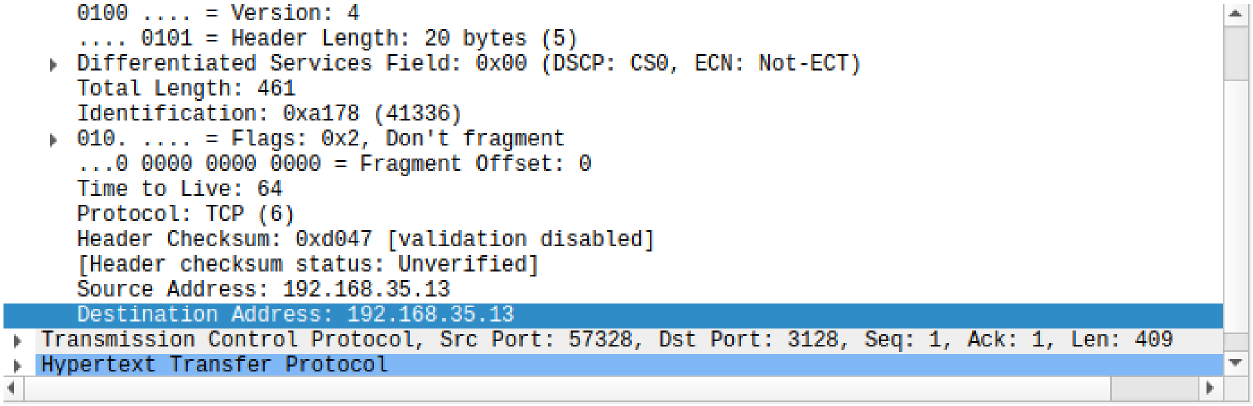
○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

Reload

No proxy for

4.

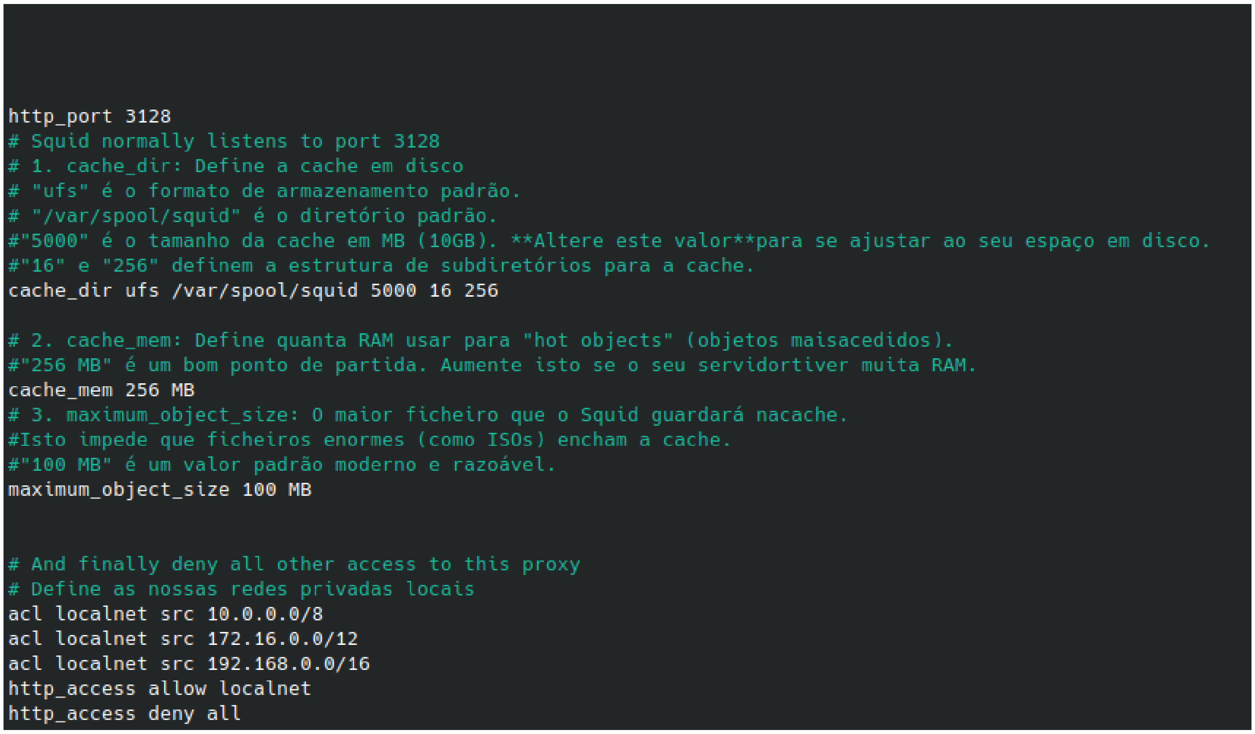


```
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 461
      Identification: 0xa178 (41336)
    ▸ 010. .... = Flags: 0x2, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 64
      Protocol: TCP (6)
      Header Checksum: 0xd047 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.35.13
      Destination Address: 192.168.35.13
▸ Transmission Control Protocol, Src Port: 57328, Dst Port: 3128, Seq: 1, Ack: 1, Len: 409
▸ Hypertext Transfer Protocol
```

R: Aqui é possivel observar que a source address e a destination address são a mesma, ou seja a proxy está a funcionar pois foi buscar a informação à cache da proxy.

Note: Captura efectuada na parte de Loopback

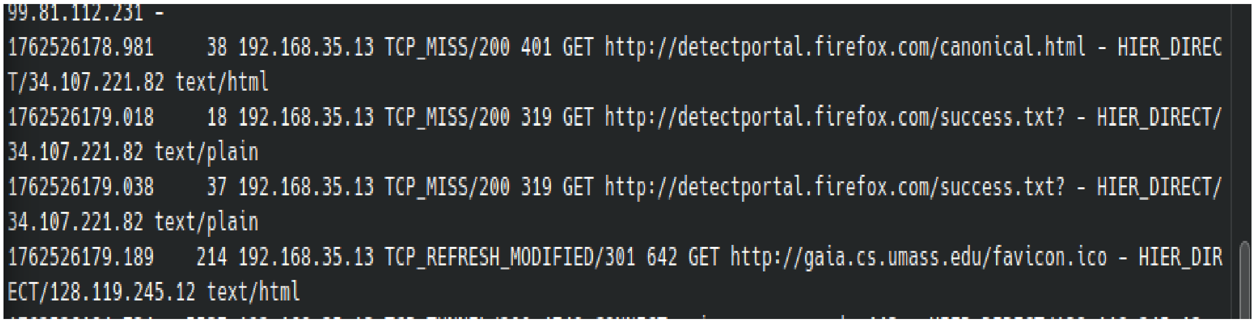
5. Cache configurada



```
http_port 3128
# Squid normally listens to port 3128
# 1. cache_dir: Define a cache em disco
# "ufs" é o formato de armazenamento padrão.
# "/var/spool/squid" é o diretório padrão.
#"5000" é o tamanho da cache em MB (10GB). **Altere este valor**para se ajustar ao seu espaço em disco.
#"16" e "256" definem a estrutura de subdiretórios para a cache.
cache_dir ufs /var/spool/squid 5000 16 256

# 2. cache_mem: Define quanta RAM usar para "hot objects" (objetos maisacedidos).
#"256 MB" é um bom ponto de partida. Aumente isto se o seu servidortiver muita RAM.
cache_mem 256 MB
# 3. maximum_object_size: O maior ficheiro que o Squid guardará nacache.
#Isto impede que ficheiros enormes (como ISOs) encham a cache.
#"100 MB" é um valor padrão moderno e razoável.
maximum_object_size 100 MB


# And finally deny all other access to this proxy
# Define as nossas redes privadas locais
acl localnet src 10.0.0.0/8
acl localnet src 172.16.0.0/12
acl localnet src 192.168.0.0/16
http_access allow localnet
http_access deny all
```

Guião 4 Squid Proxy **Ricardo Pulido**

6.



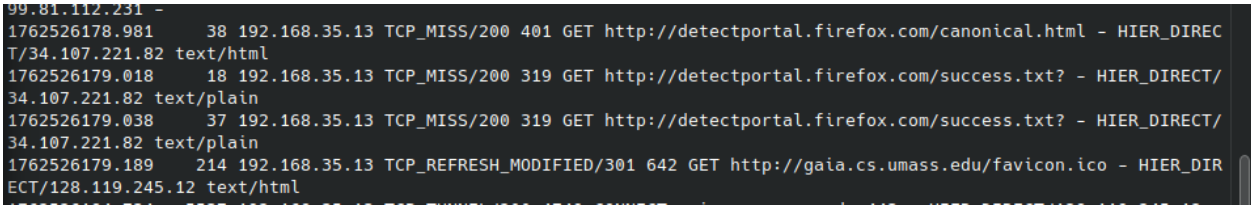
```
99.81.112.231 -
1762526178.981     38 192.168.35.13 TCP_MISS/200 401 GET http://detectportal.firefox.com/canonical.html - HIER_DIREC
T/34.107.221.82 text/html
1762526179.018     18 192.168.35.13 TCP_MISS/200 319 GET http://detectportal.firefox.com/success.txt? - HIER_DIRECT/
34.107.221.82 text/plain
1762526179.038     37 192.168.35.13 TCP_MISS/200 319 GET http://detectportal.firefox.com/success.txt? - HIER_DIRECT/
34.107.221.82 text/plain
1762526179.189    214 192.168.35.13 TCP_REFRESH_MODIFIED/301 642 GET http://gaia.cs.umass.edu/favicon.ico - HIER_DIR
ECT/128.119.245.12 text/html
```

Miss: Significa que não encontrou o ficheiro na cache da proxy

Hit: Significa que encontrou o ficheiro na cache da proxy

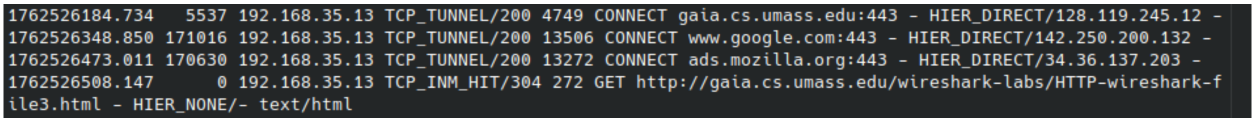
Hit_Ram: Significa que encontrou e foi servido a partir da ram do servidor proxy

7.



```
99.81.112.231 -
1762526178.981     38 192.168.35.13 TCP_MISS/200 401 GET http://detectportal.firefox.com/canonical.html - HIER_DIREC
T/34.107.221.82 text/html
1762526179.018     18 192.168.35.13 TCP_MISS/200 319 GET http://detectportal.firefox.com/success.txt? - HIER_DIRECT/
34.107.221.82 text/plain
1762526179.038     37 192.168.35.13 TCP_MISS/200 319 GET http://detectportal.firefox.com/success.txt? - HIER_DIRECT/
34.107.221.82 text/plain
1762526179.189    214 192.168.35.13 TCP_REFRESH_MODIFIED/301 642 GET http://gaia.cs.umass.edu/favicon.ico - HIER_DIR
ECT/128.119.245.12 text/html
```

Não encontrou na cache

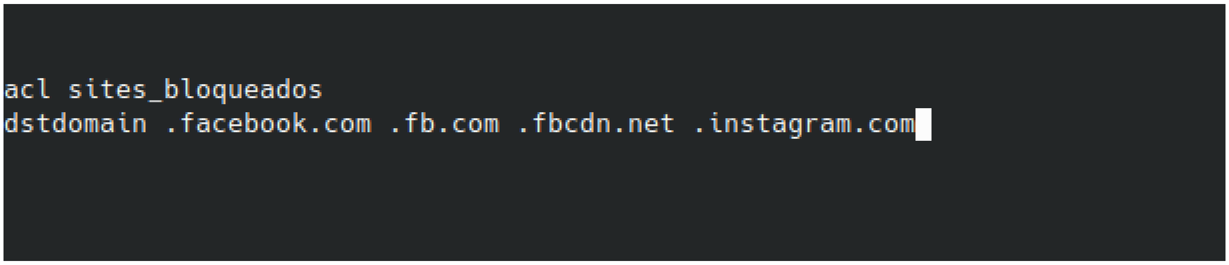


```
1762526184.734   5537 192.168.35.13 TCP_TUNNEL/200 4749 CONNECT gaia.cs.umass.edu:443 - HIER_DIRECT/128.119.245.12 -
1762526348.850 171016 192.168.35.13 TCP_TUNNEL/200 13506 CONNECT www.google.com:443 - HIER_DIRECT/142.250.200.132 -
1762526473.011 170630 192.168.35.13 TCP_TUNNEL/200 13272 CONNECT ads.mozilla.org:443 - HIER_DIRECT/34.36.137.203 -
1762526508.147      0 192.168.35.13 TCP_INM_HIT/304 272 GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-f
ile3.html - HIER_NONE/- text/html
```

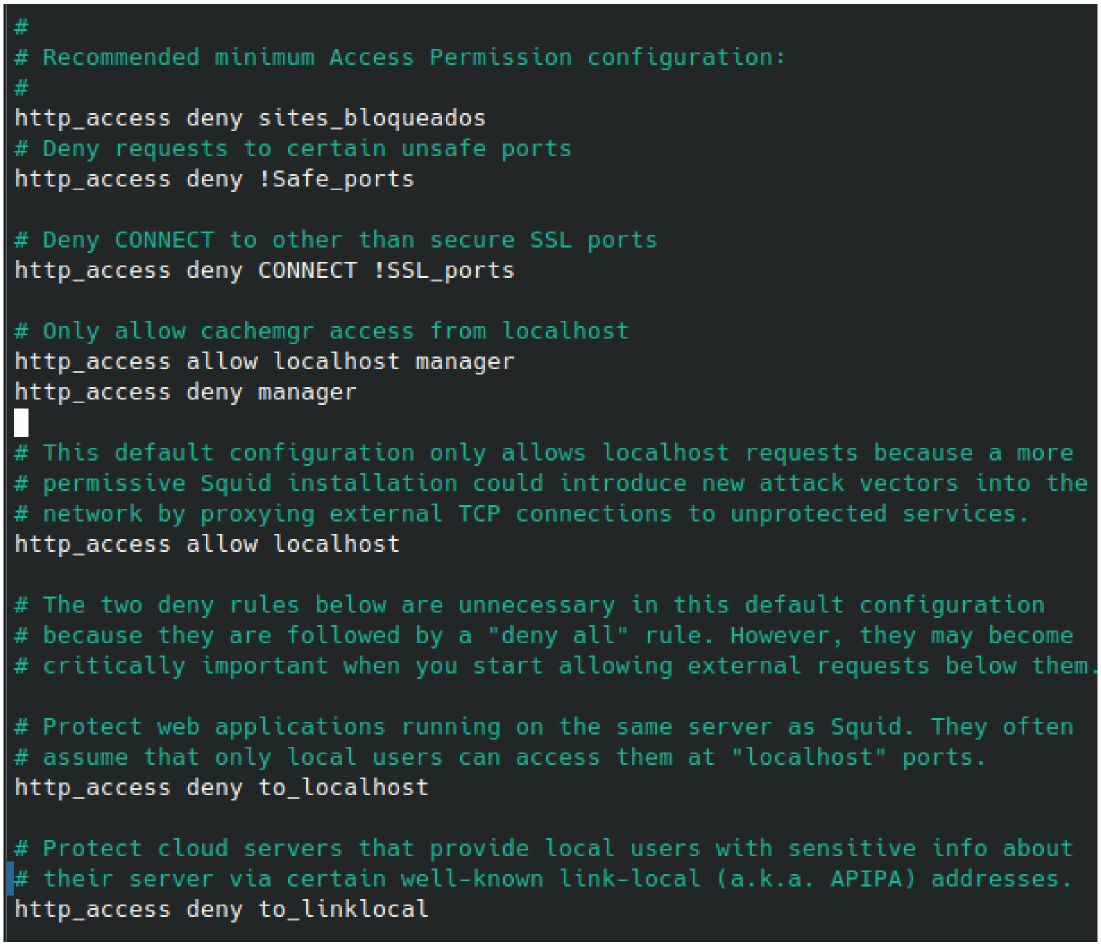
Agora podemos ver um “HIT” significa que encontrou o ficheiro na cache

Bloquear Domínios Especificos

1. / 2. / 3.



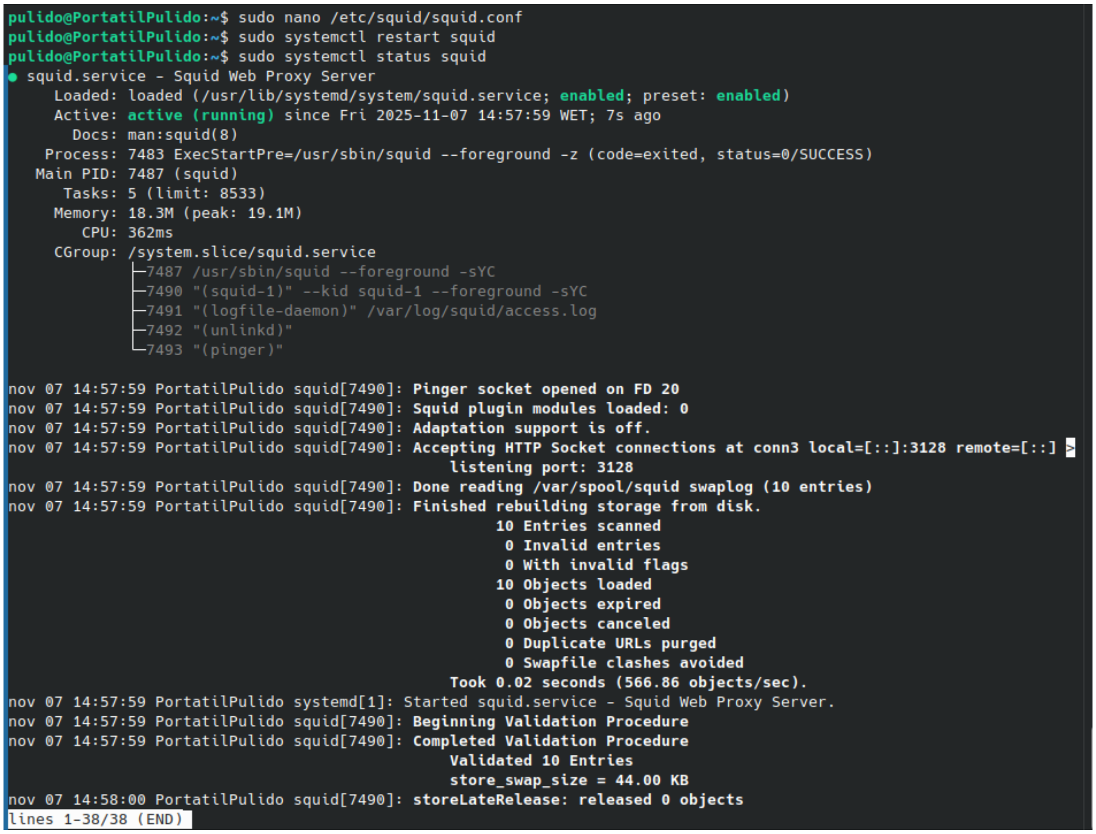
```
acl sites_bloqueados
dstdomain .facebook.com .fb.com .fbcdn.net .instagram.com
```



```
#
# Recommended minimum Access Permission configuration:
#
http_access deny sites_bloqueados
# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# This default configuration only allows localhost requests because a more
# permissive Squid installation could introduce new attack vectors into the
# network by proxying external TCP connections to unprotected services.
http_access allow localhost

# The two deny rules below are unnecessary in this default configuration
# because they are followed by a "deny all" rule. However, they may become
# critically important when you start allowing external requests below them.

# Protect web applications running on the same server as Squid. They often
# assume that only local users can access them at "localhost" ports.
http_access deny to_localhost

# Protect cloud servers that provide local users with sensitive info about
# their server via certain well-known link-local (a.k.a. APIPA) addresses.
http_access deny to_linklocal
```

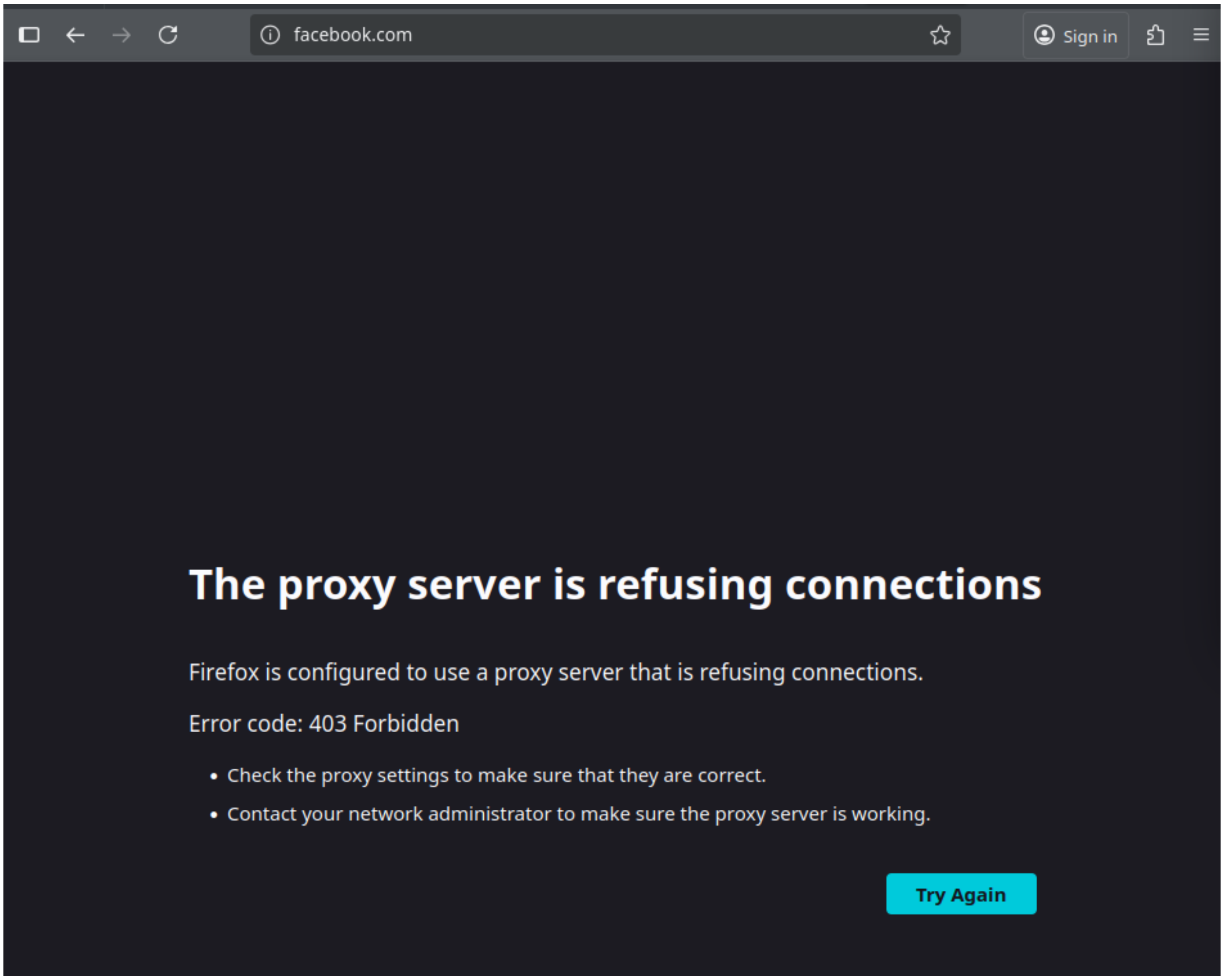
Guião 4 Squid Proxy **Ricardo Pulido**

4.



```
pulido@PortatilPulido:~$ sudo nano /etc/squid/squid.conf
pulido@PortatilPulido:~$ sudo systemctl restart squid
pulido@PortatilPulido:~$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
     Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-11-07 14:57:59 WET; 7s ago
       Docs: man:squid(8)
    Process: 7483 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
   Main PID: 7487 (squid)
      Tasks: 5 (limit: 8533)
     Memory: 18.3M (peak: 19.1M)
        CPU: 362ms
     CGroup: /system.slice/squid.service
             ├─7487 /usr/sbin/squid --foreground -sYC
             ├─7490 "(squid-1)" --kid squid-1 --foreground -sYC
             ├─7491 "(logfile-daemon)" /var/log/squid/access.log
             ├─7492 "(unlinkd)"
             └─7493 "(pinger)"

nov 07 14:57:59 PortatilPulido squid[7490]: Pinger socket opened on FD 20
nov 07 14:57:59 PortatilPulido squid[7490]: Squid plugin modules loaded: 0
nov 07 14:57:59 PortatilPulido squid[7490]: Adaptation support is off.
nov 07 14:57:59 PortatilPulido squid[7490]: Accepting HTTP Socket connections at conn3 local=[::]:3128 remote=[::] >
                                                listening port: 3128
nov 07 14:57:59 PortatilPulido squid[7490]: Done reading /var/spool/squid swaplog (10 entries)
nov 07 14:57:59 PortatilPulido squid[7490]: Finished rebuilding storage from disk.
                                                     10 Entries scanned
                                                      0 Invalid entries
                                                      0 With invalid flags
                                                     10 Objects loaded
                                                      0 Objects expired
                                                      0 Objects canceled
                                                      0 Duplicate URLs purged
                                                      0 Swapfile clashes avoided
                                                Took 0.02 seconds (566.86 objects/sec).
nov 07 14:57:59 PortatilPulido systemd[1]: Started squid.service - Squid Web Proxy Server.
nov 07 14:57:59 PortatilPulido squid[7490]: Beginning Validation Procedure
nov 07 14:57:59 PortatilPulido squid[7490]: Completed Validation Procedure
                                                Validated 10 Entries
                                                store_swap_size = 44.00 KB
nov 07 14:58:00 PortatilPulido squid[7490]: storeLateRelease: released 0 objects
lines 1-38/38 (END)
```

5.



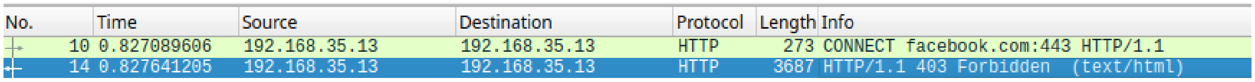
The proxy server is refusing connections

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

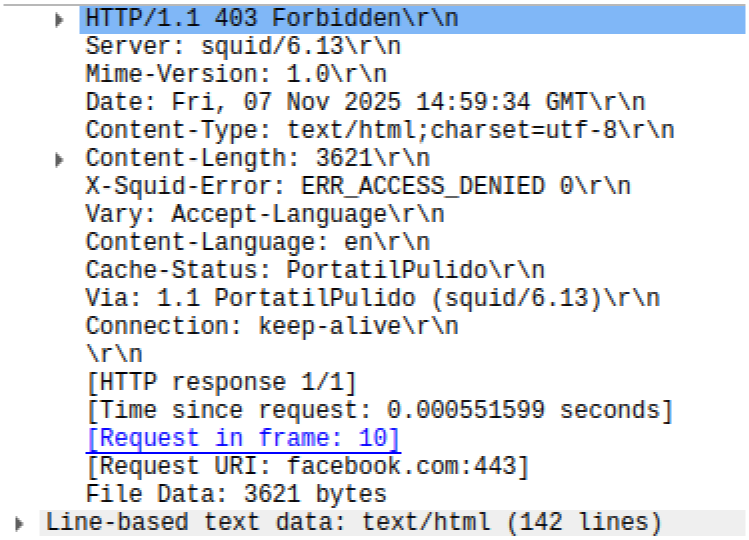
Error code: 403 Forbidden

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

Guião 4 Squid Proxy **Ricardo Pulido**



```
No.   Time          Source          Destination     Protocol  Length Info
   10 0.827089606   192.168.35.13   192.168.35.13   HTTP         273 CONNECT facebook.com:443 HTTP/1.1
   14 0.827641205   192.168.35.13   192.168.35.13   HTTP        3687 HTTP/1.1 403 Forbidden  (text/html)
```



```
    HTTP/1.1 403 Forbidden\r\n
    Server: squid/6.13\r\n
    Mime-Version: 1.0\r\n
    Date: Fri, 07 Nov 2025 14:59:34 GMT\r\n
    Content-Type: text/html;charset=utf-8\r\n
    Content-Length: 3621\r\n
    X-Squid-Error: ERR_ACCESS_DENIED 0\r\n
    Vary: Accept-Language\r\n
    Content-Language: en\r\n
    Cache-Status: PortatilPulido\r\n
    Via: 1.1 PortatilPulido (squid/6.13)\r\n
    Connection: keep-alive\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.000551599 seconds]
    [Request in frame: 10]
    [Request URI: facebook.com:443]
    File Data: 3621 bytes
 Line-based text data: text/html (142 lines)
```

R: É possível observar quando tentamos aceder ao website que a proxy está a negar o acesso, e tambem na captura que o acesso é negado e surge um 403 Forbidden