

11/3/2021

Proxy Server

System Administration

PROXY SERVER

A proxy server acts as a gateway between you and the internet. It is an intermediary server separating end users from the websites they browse.

First, we must install SQUID SERVICE

- Because We cannot configure the Packages without squid services.

For Proxy Packages

- We can Use Packages like - e2 guardian or dans guardian.
- e2 guardian only in Debian Version (UBUNTU) not in RPM.

E2 GUARDIAN and DANSGUARDIAN USED FOR WEB CONTENT FILTERING

- Filtering based on filetypes, download bandwidth, search patterns and much more.

SQUID SERVICES USED FOR WEB PAGE FILTERING

- Using ACL, we can restrict and allow based on source, dst, domain and much more.

MYSAR / SARG USED FOR REPORT SERVICES

- IP based and USER based.

To Verify

Debian Base OS

apt-cache search squid

Centos

rpm -qi squid

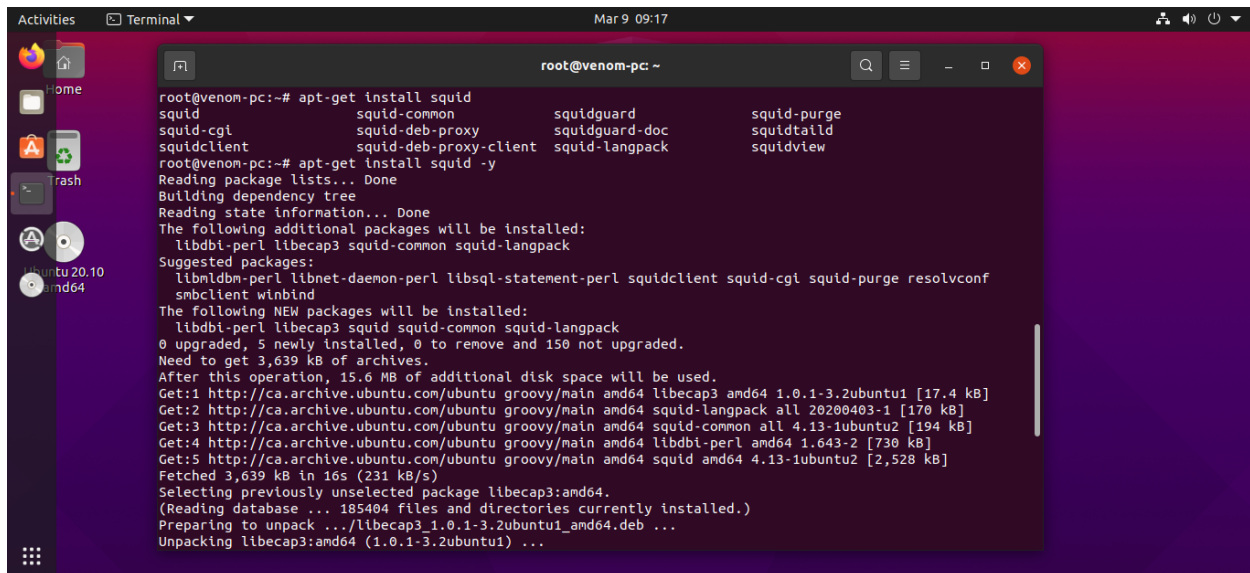
Configuring On

Ubuntu Version 20.10 in Virtual Machine Workstation 16 Pro.

Network Bridged from Host pc to Ubuntu VM.

SQUID SERVICE

Installing Squid Service in Ubuntu Machine

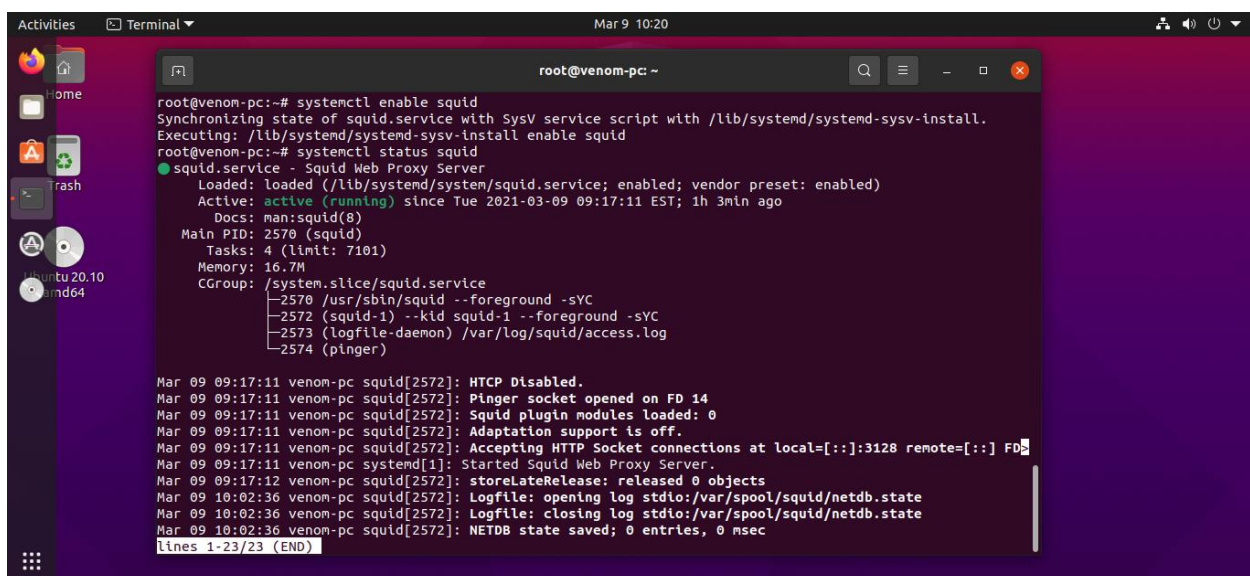


A terminal window titled 'root@venom-pc: ~' showing the command 'apt-get install squid' and its output. The output lists additional packages to be installed, suggested packages, and the disk space requirements. The installation is successful, and the package 'libcap3:amd64' is unpacked.

```
root@venom-pc:~# apt-get install squid
squid                  squid-common          squidguard             squid-purge
squid-cgi              squid-deb-proxy       squidguard-doc         squidtaild
squidclient            squid-deb-proxy-client squid-langpack         squidview

root@venom-pc:~# apt-get install squid -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libdbi-perl libcap3 squid-common squid-langpack
Suggested packages:
  libmldbm-perl libnet-daemon-perl libsql-statement-perl squidclient squid-cgi squid-purge resolvconf
  smbclient winbind
The following NEW packages will be installed:
  libdbi-perl libcap3 squid squid-common squid-langpack
0 upgraded, 5 newly installed, 0 to remove and 150 not upgraded.
Need to get 3,639 kB of archives.
After this operation, 15.6 MB of additional disk space will be used.
Get:1 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 libcap3 amd64 1.0.1-3.2ubuntu1 [17.4 kB]
Get:2 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 squid-langpack all 20200403-1 [170 kB]
Get:3 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 squid-common all 4.13-1ubuntu2 [194 kB]
Get:4 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 libdbi-perl amd64 1.643-2 [730 kB]
Get:5 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 squid amd64 4.13-1ubuntu2 [2,528 kB]
Fetched 3,639 kB in 16s (231 kB/s)
Selecting previously unselected package libcap3:amd64.
(Reading database ... 185404 files and directories currently installed.)
Preparing to unpack .../libcap3_1.0.1-3.2ubuntu1_amd64.deb ...
Unpacking libcap3:amd64 (1.0.1-3.2ubuntu1) ...
```

Start / Enable and Check the status of Squid Service.

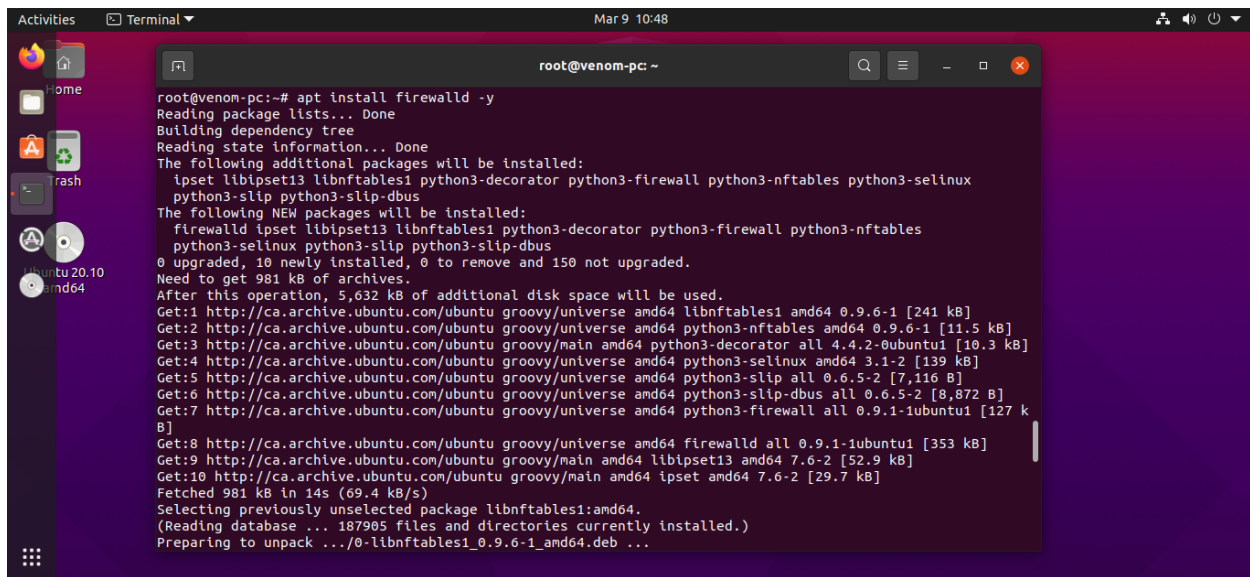


A terminal window titled 'root@venom-pc: ~' showing the command 'systemctl enable squid' and its output. The output indicates that the service is enabled and running. The status of the service is shown as 'active (running)' since Tue 2021-03-09 09:17:11 EST. The main PID is 2570 (squid), and the tasks are 4 (limit: 7101). The memory usage is 16.7M, and the CGroup is /system.slice/squid.service. The output also shows the log file path and the state of the service.

```
root@venom-pc:~# systemctl enable squid
Synchronizing state of squid.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable squid
root@venom-pc:~# systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-03-09 09:17:11 EST; 1h 3min ago
     Docs: man:squid(8)
    Main PID: 2570 (squid)
      Tasks: 4 (limit: 7101)
     Memory: 16.7M
        CGroup: /system.slice/squid.service
                └─2570 /usr/sbin/squid --foreground -sYC
                  └─2572 (squid-1) --kid squid-1 --foreground -sYC
                    └─2573 (logfile-daemon) /var/log/squid/access.log
                      └─2574 (pinger)

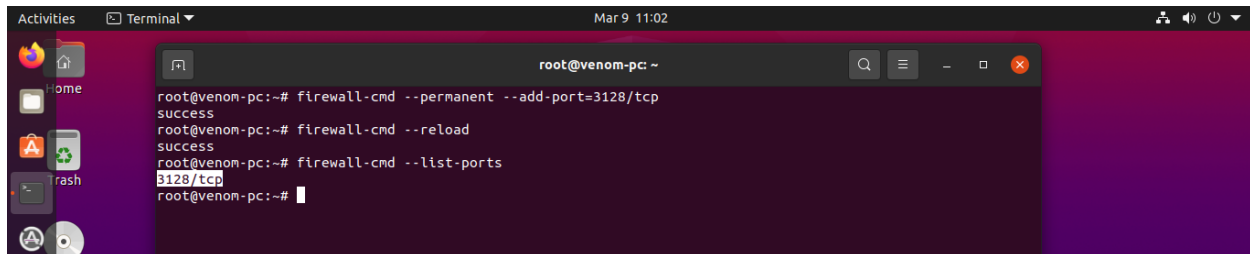
Mar 09 09:17:11 venom-pc squid[2572]: HTTP Disabled.
Mar 09 09:17:11 venom-pc squid[2572]: Pinger socket opened on FD 14
Mar 09 09:17:11 venom-pc squid[2572]: Squid plugin modules loaded: 0
Mar 09 09:17:11 venom-pc squid[2572]: Adaptation support is off.
Mar 09 09:17:11 venom-pc squid[2572]: Accepting HTTP Socket connections at local=[::]:3128 remote=[::] FD
Mar 09 09:17:11 venom-pc systemd[1]: Started Squid Web Proxy Server.
Mar 09 09:17:12 venom-pc squid[2572]: storeLateRelease: released 0 objects
Mar 09 10:02:36 venom-pc squid[2572]: Logfile: opening log stdio:/var/spool/squid/netdb.state
Mar 09 10:02:36 venom-pc squid[2572]: Logfile: closing log stdio:/var/spool/squid/netdb.state
Mar 09 10:02:36 venom-pc squid[2572]: NETDB state saved; 0 entries, 0 msec
lines 1-23/23 (END)
```

Install Firewall .

A terminal window titled 'root@venom-pc: ~' showing the command 'apt install firewalld -y'. The output lists additional packages to be installed (ipset, libipset13, libnftables1, python3-decorator, python3-firewall, python3-nftables, python3-selinux, python3-slip, python3-slip-dbus) and new packages to be installed (firewalld, ipset, libipset13, libnftables1, python3-decorator, python3-firewall, python3-nftables, python3-selinux, python3-slip, python3-slip-dbus). It also shows disk space requirements and the progress of downloading and unpacking the packages.

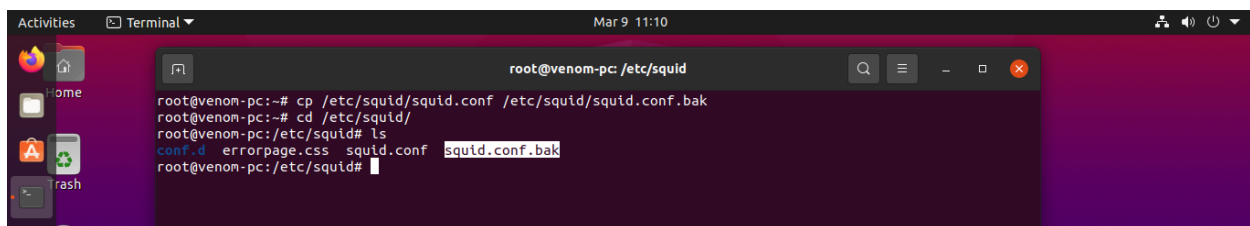
```
root@venom-pc:~# apt install firewalld -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ipset libipset13 libnftables1 python3-decorator python3-firewall python3-nftables python3-selinux
  python3-slip python3-slip-dbus
The following NEW packages will be installed:
  firewalld ipset libipset13 libnftables1 python3-decorator python3-firewall python3-nftables
  python3-selinux python3-slip python3-slip-dbus
0 upgraded, 10 newly installed, 0 to remove and 150 not upgraded.
Need to get 981 kB of archives.
After this operation, 5,632 kB of additional disk space will be used.
Get:1 http://ca.archive.ubuntu.com/ubuntu groovy/universe amd64 libnftables1 amd64 0.9.6-1 [241 kB]
Get:2 http://ca.archive.ubuntu.com/ubuntu groovy/universe amd64 python3-nftables amd64 0.9.6-1 [11.5 kB]
Get:3 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 python3-decorator all 4.4.2-0ubuntu1 [10.3 kB]
Get:4 http://ca.archive.ubuntu.com/ubuntu groovy/universe amd64 python3-selinux amd64 3.1-2 [139 kB]
Get:5 http://ca.archive.ubuntu.com/ubuntu groovy/universe amd64 python3-slip all 0.6.5-2 [7,116 B]
Get:6 http://ca.archive.ubuntu.com/ubuntu groovy/universe amd64 python3-slip-dbus all 0.6.5-2 [8,872 B]
Get:7 http://ca.archive.ubuntu.com/ubuntu groovy/universe amd64 python3-firewall all 0.9.1-1ubuntu1 [127 kB]
Get:8 http://ca.archive.ubuntu.com/ubuntu groovy/universe amd64 firewalld all 0.9.1-1ubuntu1 [353 kB]
Get:9 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 libipset13 amd64 7.6-2 [52.9 kB]
Get:10 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 ipset amd64 7.6-2 [29.7 kB]
Fetched 981 kB in 14s (69.4 kB/s)
Selecting previously unselected package libnftables1:amd64.
(Reading database ... 187905 files and directories currently installed.)
Preparing to unpack .../0-libnftables1_0.9.6-1_amd64.deb ...
```

Assign the squid service port number to firewall.

A terminal window titled 'root@venom-pc: ~' showing three commands: 'firewall-cmd --permanent --add-port=3128/tcp', 'firewall-cmd --reload', and 'firewall-cmd --list-ports'. The output shows 'success' for the first two commands and '3128/tcp' for the third.

```
root@venom-pc:~# firewall-cmd --permanent --add-port=3128/tcp
success
root@venom-pc:~# firewall-cmd --reload
success
root@venom-pc:~# firewall-cmd --list-ports
3128/tcp
root@venom-pc:~#
```

Before Configuring the squid service, get a backup of the config file.

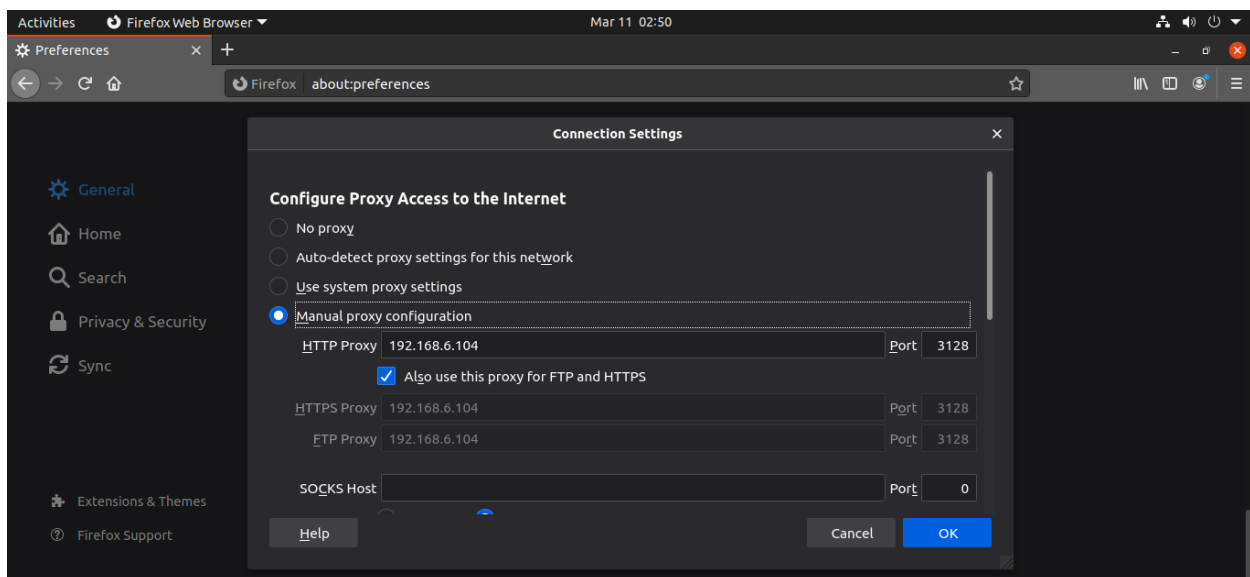
A terminal window titled 'root@venom-pc: /etc/squid' showing the command 'cp /etc/squid/squid.conf /etc/squid/squid.conf.bak'. The output shows the command was executed successfully.

```
root@venom-pc:~# cp /etc/squid/squid.conf /etc/squid/squid.conf.bak
root@venom-pc:~# cd /etc/squid/
root@venom-pc:/etc/squid# ls
conf.d  errorpage.css  squid.conf  squid.conf.bak
root@venom-pc:/etc/squid#
```

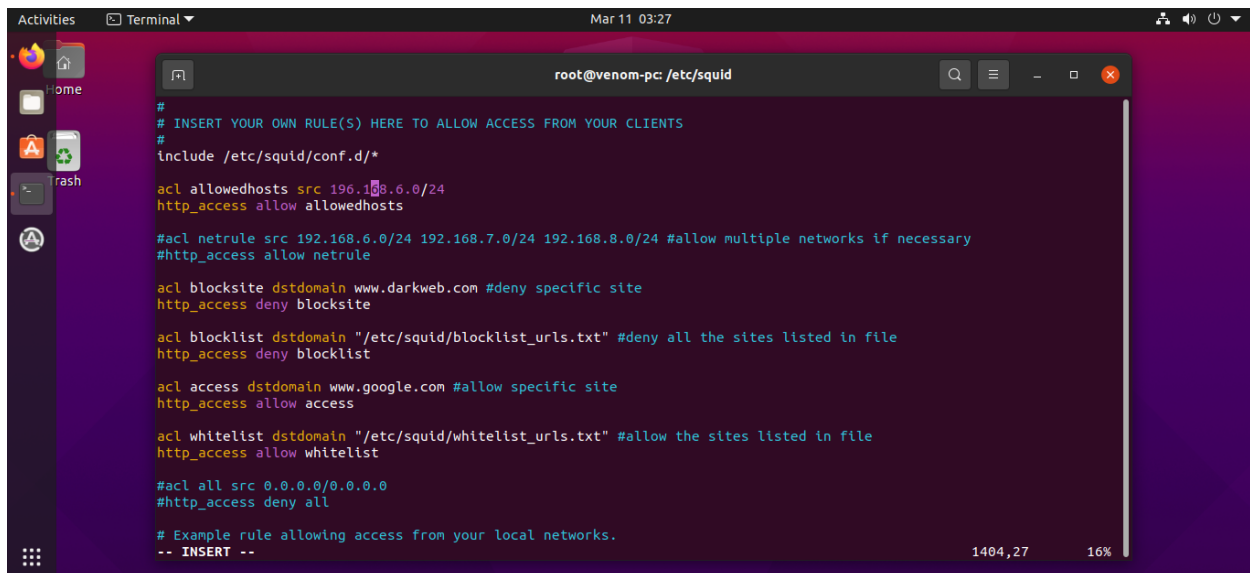
Ipaddress verifying in ubuntu.

```
root@venom-pc: ~  
root@venom-pc:~# ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.6.104 netmask 255.255.255.0 broadcast 192.168.6.255  
    inet6 fe80::67fd:6539:81ec:711d prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:ea:cb:42 txqueuelen 1000 (Ethernet)  
    RX packets 1403 bytes 1510831 (1.5 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1658 bytes 130427 (130.4 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 1170 bytes 102188 (102.1 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1170 bytes 102188 (102.1 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@venom-pc:~# ip r  
default via 192.168.6.1 dev ens33 proto dhcp metric 100  
169.254.0.0/16 dev ens33 scope link metric 1000  
192.168.6.0/24 dev ens33 proto kernel scope link src 192.168.6.104 metric 100  
root@venom-pc:~#
```

Manually Assinging Proxy Server to firefox.



Configuring the SQUID SERVICES.



```
root@venom-pc: /etc/squid

# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*

acl allowedhosts src 196.168.6.0/24
http_access allow allowedhosts

#acl netrule src 192.168.6.0/24 192.168.7.0/24 192.168.8.0/24 #allow multiple networks if necessary
#http_access allow netrule

acl blocksite dstdomain www.darkweb.com #deny specific site
http_access deny blocksite

acl blocklist dstdomain "/etc/squid/blocklist_urls.txt" #deny all the sites listed in file
http_access deny blocklist

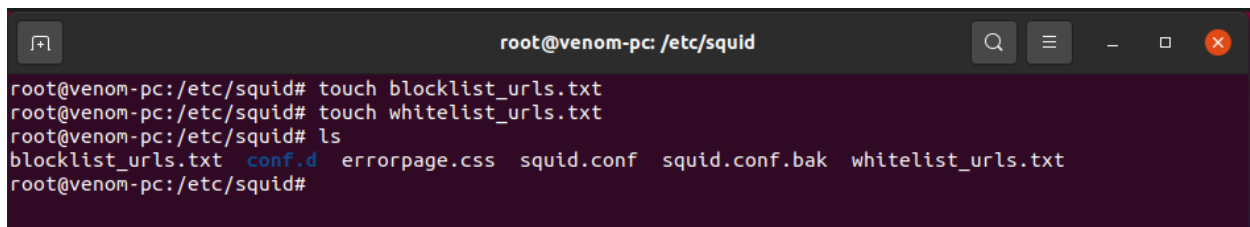
acl access dstdomain www.google.com #allow specific site
http_access allow access

acl whitelist dstdomain "/etc/squid/whitelist_urls.txt" #allow the sites listed in file
http_access allow whitelist

#acl all src 0.0.0.0/0.0.0.0
#http_access deny all

# Example rule allowing access from your local networks.
-- INSERT --
```

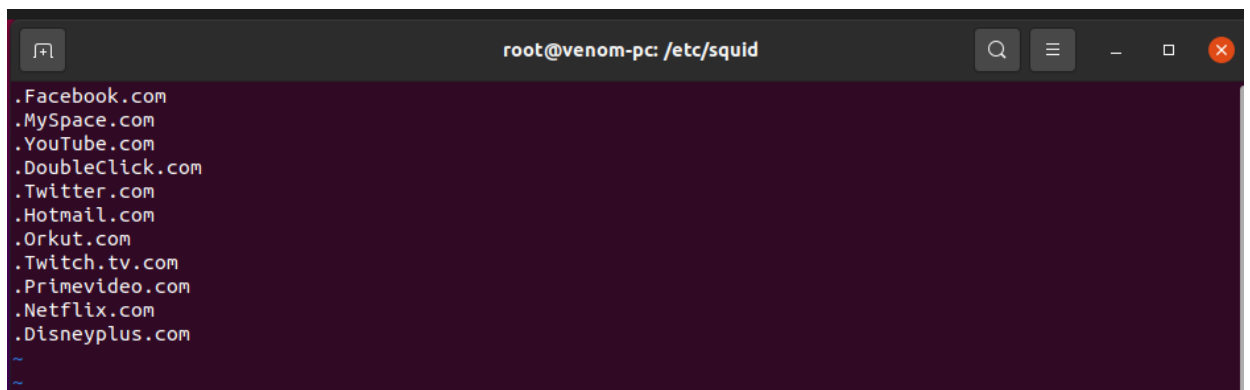
Creating URL files.



```
root@venom-pc: /etc/squid

root@venom-pc:/etc/squid# touch blocklist_urls.txt
root@venom-pc:/etc/squid# touch whitelist_urls.txt
root@venom-pc:/etc/squid# ls
blocklist_urls.txt  conf.d  errorpage.css  squid.conf  squid.conf.bak  whitelist_urls.txt
root@venom-pc:/etc/squid#
```

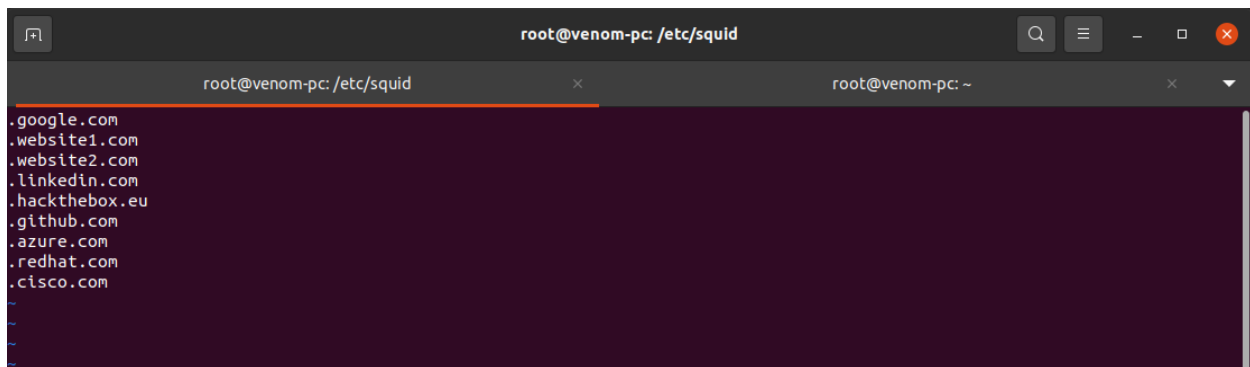
Vim blocklist_urls.txt



```
root@venom-pc: /etc/squid

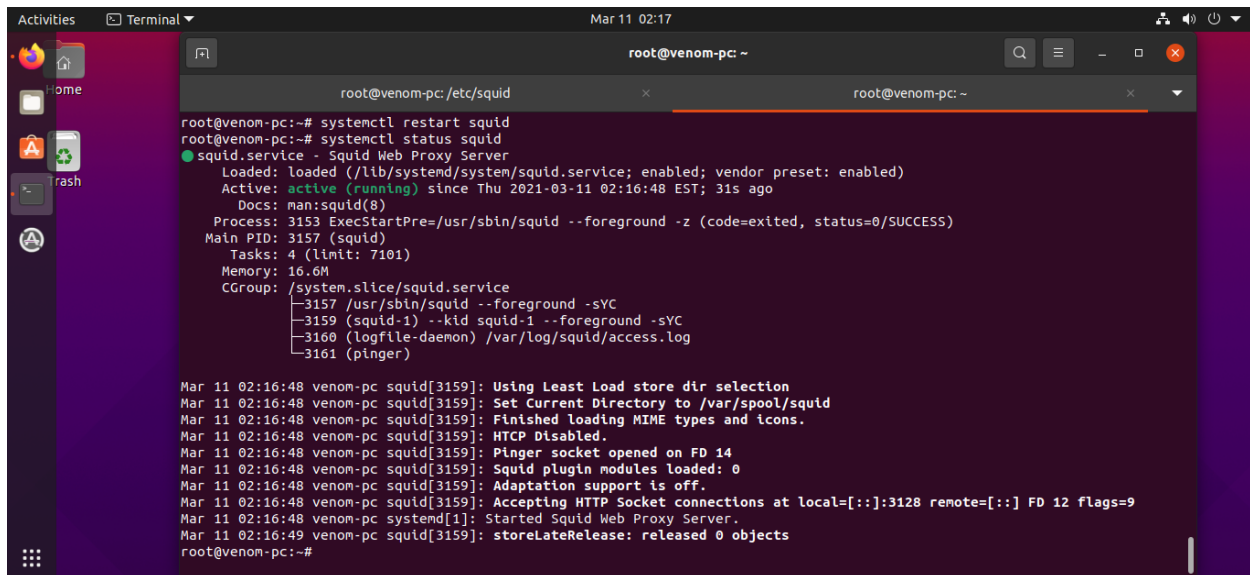
.Facebook.com
.MySpace.com
.YouTube.com
.DoubleClick.com
.Twitter.com
.Hotmail.com
.Orkut.com
.Twitch.tv.com
.Primevideo.com
.Netflix.com
.Disneyplus.com
~
~
```

vim whitelist urls.txt.



```
root@venom-pc: /etc/squid
root@venom-pc: /etc/squid
root@venom-pc: ~
.google.com
.website1.com
.website2.com
.linkedin.com
.hackthebox.eu
.github.com
.azure.com
.redhat.com
.cisco.com
~
~
~
```

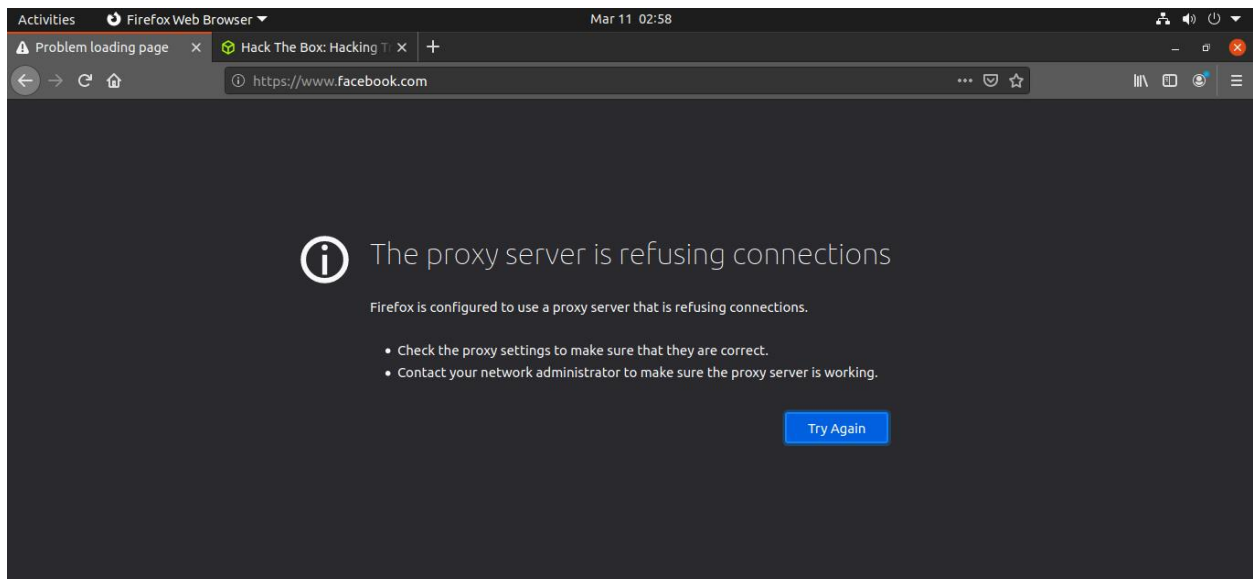
Restart the services And Check the status.



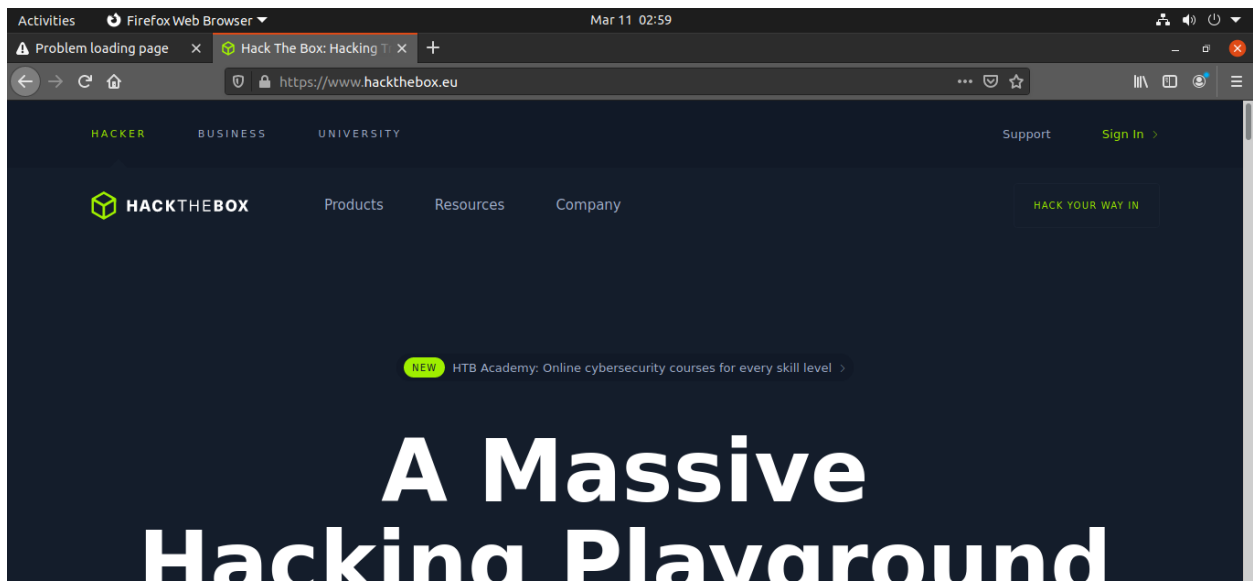
```
Activities Terminal Mar 11 02:17
root@venom-pc: ~
root@venom-pc: /etc/squid
root@venom-pc: /etc/squid
root@venom-pc: ~
root@venom-pc:~# systemctl restart squid
root@venom-pc:~# systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2021-03-11 02:16:48 EST; 31s ago
     Docs: man:squid(8)
   Process: 3153 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
  Main PID: 3157 (squid)
    Tasks: 4 (limit: 7101)
   Memory: 16.6M
    CGroup: /system.slice/squid.service
            └─3157 /usr/sbin/squid --foreground -sYC
              └─3159 (squid-1) --kid squid-1 --foreground -sYC
                └─3160 (logfile-daemon) /var/log/squid/access.log
                  └─3161 (pinger)

Mar 11 02:16:48 venom-pc squid[3159]: Using Least Load store dir selection
Mar 11 02:16:48 venom-pc squid[3159]: Set Current Directory to /var/spool/squid
Mar 11 02:16:48 venom-pc squid[3159]: Finished loading MIME types and icons.
Mar 11 02:16:48 venom-pc squid[3159]: HTTP Disabled.
Mar 11 02:16:48 venom-pc squid[3159]: Pinger socket opened on FD 14
Mar 11 02:16:48 venom-pc squid[3159]: Squid plugin modules loaded: 0
Mar 11 02:16:48 venom-pc squid[3159]: Adaptation support is off.
Mar 11 02:16:48 venom-pc squid[3159]: Accepting HTTP Socket connections at local=[::]:3128 remote=[::] FD 12 flags=9
Mar 11 02:16:48 venom-pc systemd[1]: Started Squid Web Proxy Server.
Mar 11 02:16:49 venom-pc squid[3159]: storeLateRelease: released 0 objects
root@venom-pc:~#
```

DENIED SITE



ALLOWED SITE



E2 GUARDIAN

E2 Guardian is the advanced version of Dans Guardian for web content filtering.

Filtering group

- A filtering group is a way to identify one or more users who will share some settings, for example what's banned and what's allowed.

Filtering lists

- When you install E2G you will find a directory called lists containing various lists to help you define what's allowed and what's blocked.
 - ban lists, to completely ban something
 - exception list, to trust something so that it's always allowed
 - a grey list, something in between a ban and exception (white) list, which trusts a site but still subjects it to content checking
 - phrase lists, that help you allow or ban pages based on the content (words) appearing on the page

For ban, exception and grey lists, there are 4 ways you can express them:

- a straight site ban, ie example.com , which would ban example.com and any subdomain
- a regular expression, ie *.css, which would allow all the css files
- a url, to allow or ban a page, while the rest of the domain can be allowed/banned.
- a mime type, especially useful for files

Words/Phrase list

- if you were to visit a page containing the words "cussing", "leaning linux" and "badness" its total score would be $+100-100+100=100$. If your naughtiness level is 50, ie less than the total, the page will be blocked, otherwise it will be allowed.

E2G configuration

- The main configuration file for e2g is called e2guardian.conf. If you are running a simple filter with just one group on standard ports, there isn't actually anything to change in this file.

Checking for E2Guardian

```
root@venom-pc: ~  
root@venom-pc:~# apt-cache search dansguardian  
e2guardian - Web content filtering (Dansguardian fork)  
libdansguardian-perl - Simple module for administer dansguardian's control files  
root@venom-pc:~# apt-cache search e2guardian  
e2guardian - Web content filtering (Dansguardian fork)  
root@venom-pc:~#
```

Installing E2Guardian

```
Activities Terminal Mar 11 05:53  
root@venom-pc: ~  
root@venom-pc:~# apt-get install e2guardian -y  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
  clamav clamav-base clamav-daemon clamav-freshclam clamscan libclamav9 libtbfm1  
Suggested packages:  
  libclamunrar clamav-docs daemon libclamunrar9  
The following NEW packages will be installed:  
  clamav clamav-base clamav-daemon clamav-freshclam clamscan e2guardian libclamav9 libtbfm1  
0 upgraded, 8 newly installed, 0 to remove and 150 not upgraded.  
Need to get 2,264 kB of archives.  
After this operation, 9,831 kB of additional disk space will be used.  
Get:1 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 clamav-base all 0.102.4+dfsg-1build1 [70.1 kB]  
Get:2 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 libtbfm1 amd64 0.13-4 [57.0 kB]  
Get:3 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 libclamav9 amd64 0.102.4+dfsg-1build1 [783 kB]  
Get:4 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 clamav-freshclam amd64 0.102.4+dfsg-1build1 [92.9 kB]  
Get:5 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 clamav-daemon amd64 0.102.4+dfsg-1build1 [229 kB]  
Get:6 http://ca.archive.ubuntu.com/ubuntu groovy/universe amd64 e2guardian amd64 5.3.4-1 [826 kB]  
Get:7 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 clamav amd64 0.102.4+dfsg-1build1 [124 kB]  
Get:8 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 clamscan amd64 0.102.4+dfsg-1build1 [81.8 kB]  
Fetched 2,264 kB in 14s (157 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package clamav-base.  
(Reading database ... 190235 files and directories currently installed.)  
Preparing to unpack .../0-clamav-base_0.102.4+dfsg-1build1_all.deb ...  
Unpacking clamav-base (0.102.4+dfsg-1build1) ...  
Selecting previously unselected package libtbfm1:amd64.  
Preparing to unpack .../1-libtbfm1_0.13-4_amd64.deb ...  
Unpacking libtbfm1:amd64 (0.13-4) ...  
Selecting previously unselected package libclamav9:amd64.  
Preparing to unpack .../2-libclamav9_0.102.4+dfsg-1build1_amd64.deb ...  
Unpacking libclamav9:amd64 (0.102.4+dfsg-1build1) ...  
Selecting previously unselected package clamav-daemon.  
Preparing to unpack .../3-clamav-daemon_0.102.4+dfsg-1build1_amd64.deb ...  
Unpacking clamav-daemon (0.102.4+dfsg-1build1) ...  
Selecting previously unselected package clamav-freshclam.  
Preparing to unpack .../4-clamav-freshclam_0.102.4+dfsg-1build1_amd64.deb ...  
Unpacking clamav-freshclam (0.102.4+dfsg-1build1) ...  
Selecting previously unselected package clamscan.  
Preparing to unpack .../5-clamscan_0.102.4+dfsg-1build1_amd64.deb ...  
Unpacking clamscan (0.102.4+dfsg-1build1) ...  
Selecting previously unselected package e2guardian.  
Preparing to unpack .../6-e2guardian_5.3.4-1_amd64.deb ...  
Unpacking e2guardian (5.3.4-1) ...  
Setting up clamav-base (0.102.4+dfsg-1build1) ...  
Setting up libtbfm1:amd64 (0.13-4) ...  
Setting up libclamav9:amd64 (0.102.4+dfsg-1build1) ...  
Setting up clamav-daemon (0.102.4+dfsg-1build1) ...  
Setting up clamav-freshclam (0.102.4+dfsg-1build1) ...  
Setting up clamscan (0.102.4+dfsg-1build1) ...  
Setting up e2guardian (5.3.4-1) ...  
Created symlink /etc/systemd/system/multi-user.target.wants/e2guardian.service → /usr/lib/systemd/system/e2guardian.service.  
Processing triggers for libc-bin (2.34-0ubuntu2) ...
```

Start / Enable and Check the status of E2Guardian Service.

```
root@venom-pc: /etc/e2guardian  
root@venom-pc:/etc/e2guardian# systemctl start e2guardian  
root@venom-pc:/etc/e2guardian# systemctl enable e2guardian  
Synchronizing state of e2guardian.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable e2guardian  
root@venom-pc:/etc/e2guardian# systemctl status e2guardian  
● e2guardian.service - E2guardian Web filtering  
   Loaded: loaded (/lib/systemd/system/e2guardian.service; enabled; vendor preset: enabled)  
   Active: active (running) since Thu 2021-03-11 05:52:21 EST; 20min ago  
     Docs: http://e2guardian.org/  
    Main PID: 3140 (e2guardian)  
      Tasks: 504 (limit: 7101)  
     Memory: 31.7M  
    CGroup: /system.slice/e2guardian.service  
            └─3140 /usr/sbin/e2guardian  
  
Mar 11 05:52:21 venom-pc systemd[1]: Starting E2guardian Web filtering...  
Mar 11 05:52:21 venom-pc systemd[1]: Started E2guardian Web filtering.  
Mar 11 05:52:21 venom-pc e2guardian[3140]: Started successfully.  
root@venom-pc:/etc/e2guardian#
```

Backed up the config file

```
root@venom-pc: /etc/e2guardian
root@venom-pc:~# cd /etc/e2guardian/
root@venom-pc:/etc/e2guardian# ls
authplugins  contentscanners  e2guardian.conf  examplef1.story  lists  site.story
common.story  downloadmanagers  e2guardianf1.conf  languages  preauth.story
root@venom-pc:/etc/e2guardian# cp e2guardian.conf e2guardian.conf.bak
root@venom-pc:/etc/e2guardian#
```

FORWARDING all the conn from 8080 to access 3128.

If both services are configured in same server, the proxy ip would be localhost if not you have to define the ip of squid service. Both connection works through socket .

```
root@venom-pc: /etc/e2guardian
mapportstoips = off

#port for transparent https
#if defined enables transparent https
transparenthttpsport = 8443

#port for ICAP
#if defined enables icap mode
#icapport = 1344

# the ip of upstream proxy - optional - if blank e2g will go direct to sites.
# default is "" i.e. no proxy
proxyip = 127.0.0.1

# the port e2guardian connects to proxy on
proxyport = 3128

# Proxy timeout
# Set tcp timeout between the Proxy and e2guardian
# This is a connection timeout
# If proxy is remote you may need to increase this to 10 or more.
# Min 5 - Max 100
proxytimeout = 5

# Connect timeout
"e2guardian.conf" 735L, 28704C 184,1 24%
```

ASSIGN PORT TO FIREWALL.

```
root@venom-pc: /etc/e2guardian
root@venom-pc:/etc/e2guardian# firewall-cmd --permanent --add-port=8080/tcp
success
root@venom-pc:/etc/e2guardian# firewall-cmd --reload
success
root@venom-pc:/etc/e2guardian# firewall-cmd --list-ports
3128/tcp 8080/tcp
root@venom-pc:/etc/e2guardian#
```

THE FILTERING LIST

```
Activities Terminal Mar 11 05:55
root@venom-pc: /etc/e2guardian/lists

root@venom-pc: /etc/e2guardian/lists# ls
addheaderregexplist      exceptionextensionlist    localexceptionsitelist
authexceptionlist        exceptionfileitelist      localexceptionsitelist
authexceptionsitelist     exceptionfileitelist      localexceptionurllist
authexceptionsitelist     exceptionfileurllist      localgreysitelist
authexceptionurllist      exceptioniplist           localgreysitelist
authplugins              exceptionmimetypelist     localgreysitelist
bannedclientlist         exceptionphraselist       localgreysitelist
bannedextensionlist      exceptionregexphheaderlist localgreysurllist
bannediplist             exceptionregexpurllist    logregexpurllist
bannedmimetypelist       exceptionregexpuseragentlist logsiteip
bannedphraselist         exceptionsitelist        logsiteip
bannedregexphheaderlist  exceptionsitelist        logurllist
bannedregexpurllist      exceptionurllist         newbannedphraselist
bannedregexpuseragentlist exceptionvirusextensionlist newexceptionphraselist
bannedrooms             exceptionvirusitelist     newweightedphraselist
bannedsearchlist        filtergroupslist         nocheckcertsitelist
bannedsearchoveridelist greysitelist              nocheckcertsitelist
bannedsiteip            greysitelist              phraselists
bannedsitelist           greysitelist              refererexceptionsitelist
bannedsslsitelist       greysitelist              refererexceptionsitelist
bannedsslsitelist       greysurllist              refererexceptionurllist
bannedurllist            headerregexplist          searchregexplist
contentregexplist        ipnobypass                ssliteregexplist
contentscanners          localbannedsearchlist     urlnobypass
domainsnobypass         localbannedsitelist       urlredirectregexplist
embededreferersitelist  localbannedsitelist       urlregexplist
embededreferersitelist  localbannedsslsitelist    weightedphraselist
embededrefererurllist   localbannedsslsitelist
exceptionclientlist      localbannedurllist
```

BANNED SITE LIST

```
root@venom-pc: /etc/e2guardian/lists

GNU nano 5.2 bannedsitelist Modified

# Time limiting syntax:
# #time: <start hour> <start minute> <end hour> <end minute> <days>
# Example:
##time: 9 0 17 0 01234
# Remove the first # from the line above to enable this list only from
# 9am to 5pm, Monday to Friday.

# List categorisation
#listcategory: "Banned Sites"

#List other sites to block:

badboys.com
netflix.com
primevideo.com
9anime.com

# NOTE: From v5 Blanket blocks are now implemented using Storyboarding
# WARNING: Old style Blanket blocks in this file will be silently ignored
```

BANNED PHRASE LIST

```
root@venom-pc: /etc/e2guardian/lists
GNU nano 5.2 bannedphraselist
# The following banned phraselists enable Website Content Labeling systems.  These are enabled by >

.Include</etc/e2guardian/lists/phraselists/safelabel/banned>
#.Include</etc/e2guardian/lists/phraselists/rta/banned_portuguese>

# The following banned phraselists are included in the default DG distribution.

.Include</etc/e2guardian/lists/phraselists/pornography/banned>
##.Include</etc/e2guardian/lists/phraselists/pornography/banned_portuguese>

#.Include</etc/e2guardian/lists/phraselists/illegaldrugs/banned>

#.Include</etc/e2guardian/lists/phraselists/gambling/banned>
##.Include</etc/e2guardian/lists/phraselists/gambling/banned_portuguese>

#.Include</etc/e2guardian/lists/phraselists/googlesearches/banned>

<drugs> < drug > <alcohol> <pornography> <child abuse> <darkweb>
< smoke > <weapons>
< instagram >

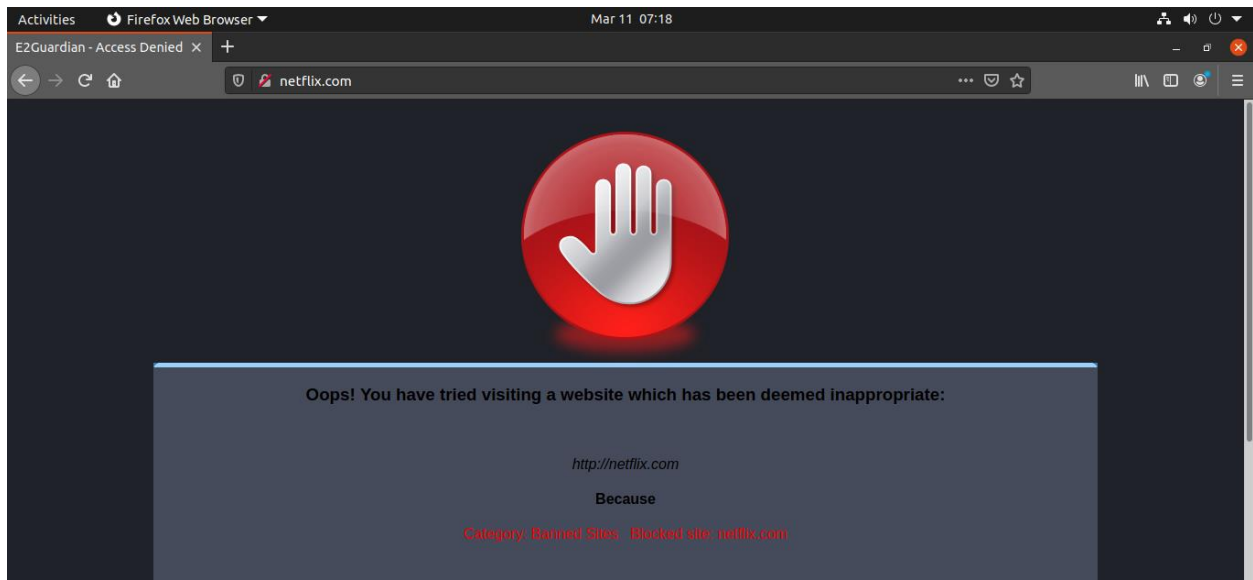
Wrote 59 lines
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

RESTART THE SERVICE

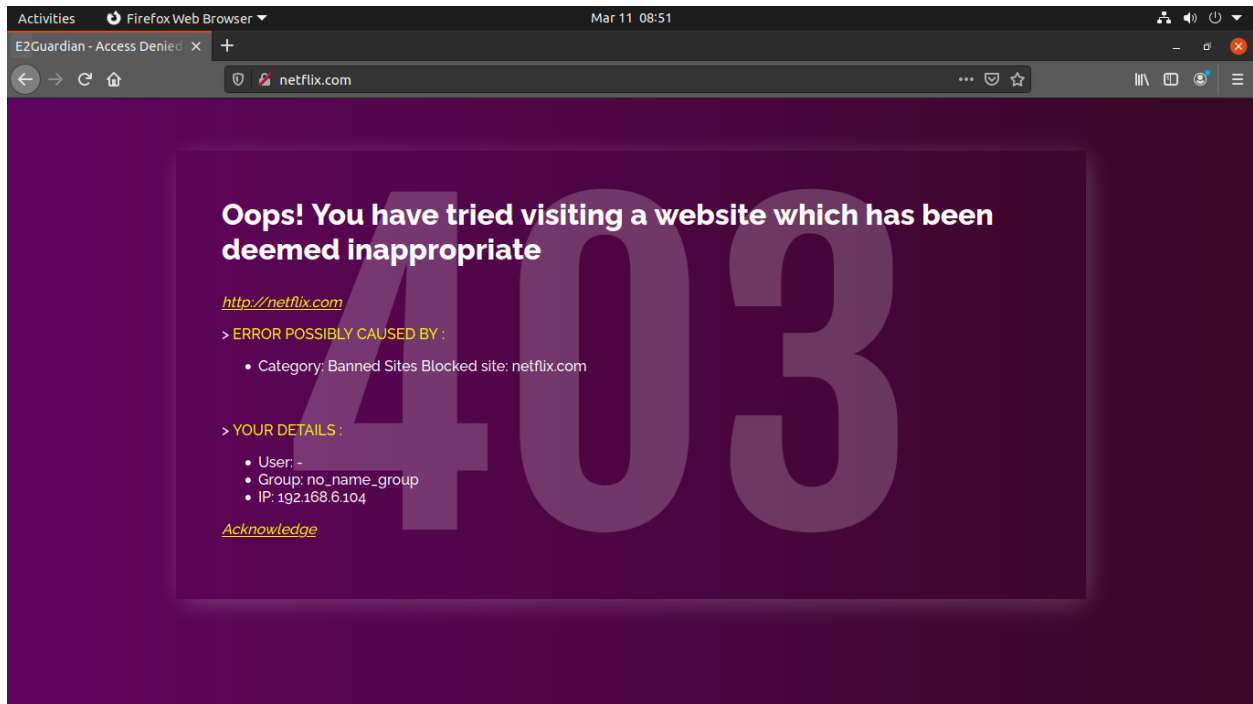
```
root@venom-pc: /etc/e2guardian/lists
root@venom-pc:/etc/e2guardian/lists# systemctl restart e2guardian.service
root@venom-pc:/etc/e2guardian/lists# systemctl status e2guardian.service
● e2guardian.service - E2guardian Web filtering
   Loaded: loaded (/lib/systemd/system/e2guardian.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2021-03-11 07:08:22 EST; 1min 38s ago
     Docs: http://e2guardian.org/
   Process: 6781 ExecStart=/usr/sbin/e2guardian (code=exited, status=0/SUCCESS)
  Main PID: 6782 (e2guardian)
    Tasks: 504 (limit: 7101)
   Memory: 32.0M
   CGroup: /system.slice/e2guardian.service
           └─6782 /usr/sbin/e2guardian

Mar 11 07:08:22 venom-pc systemd[1]: Starting E2guardian Web filtering...
Mar 11 07:08:22 venom-pc systemd[1]: Started E2guardian Web filtering.
Mar 11 07:08:22 venom-pc e2guardian[6782]: Started successfully.
root@venom-pc:/etc/e2guardian/lists#
```

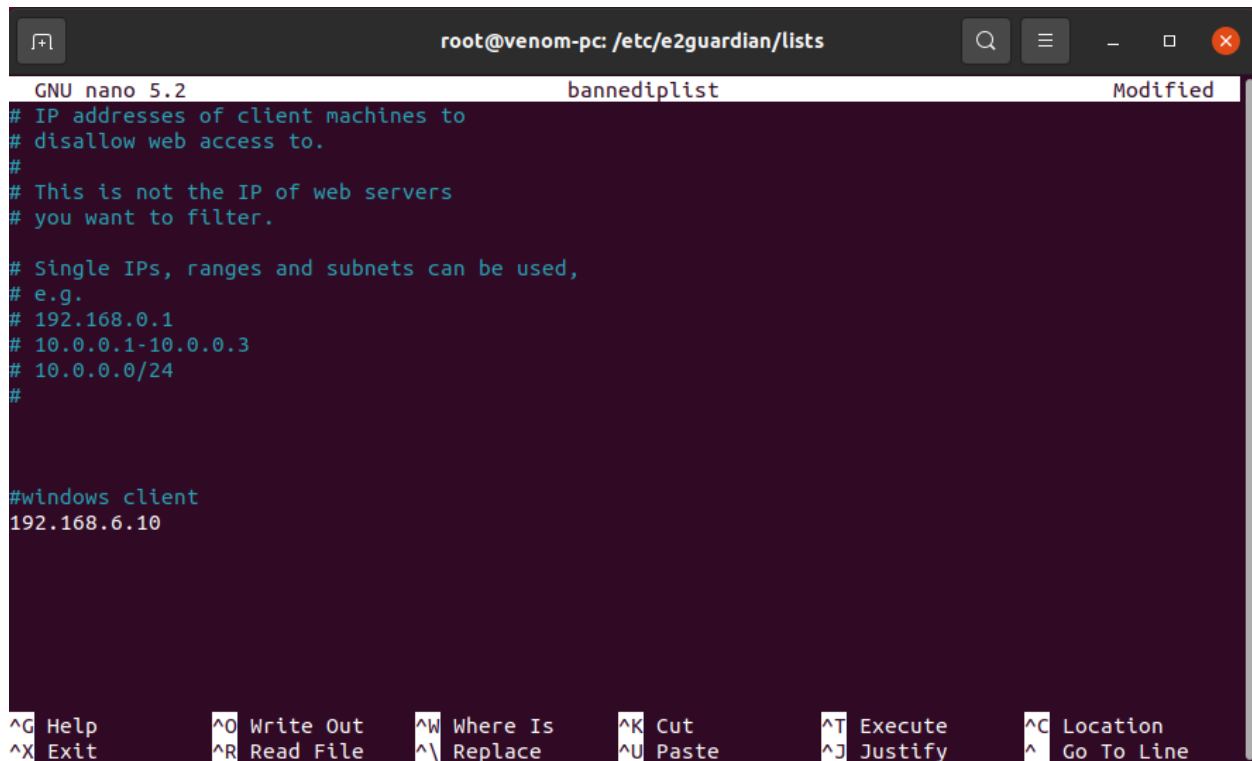
DEFAULT TEMPLATE WHEN BLOCKING SITE



MODIFIED TEMPLATE FOR BLOCKED SITES



BANNED IP LIST.

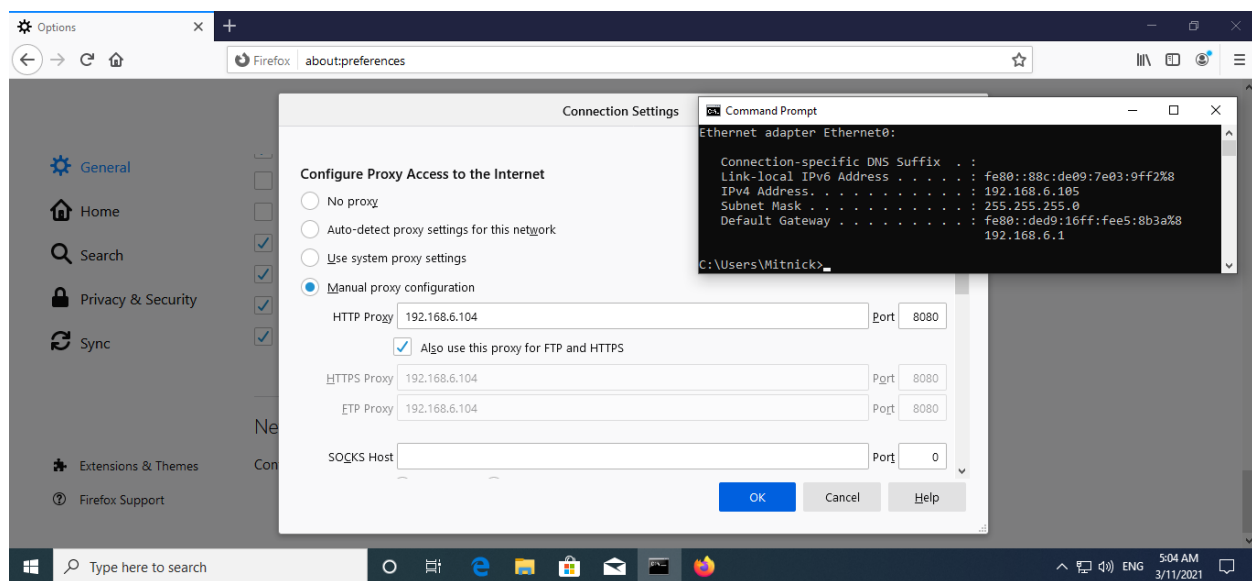


The screenshot shows a terminal window titled "root@venom-pc: /etc/e2guardian/lists" with a nano 5.2 editor open to a file named "bannediplist". The file contains comments and IP addresses. The terminal window has a dark background with light-colored text. The nano editor's status bar at the bottom shows various keyboard shortcuts like ^G Help, ^O Write Out, etc.

```
GNU nano 5.2 bannediplist Modified
# IP addresses of client machines to
# disallow web access to.
#
# This is not the IP of web servers
# you want to filter.
#
# Single IPs, ranges and subnets can be used,
# e.g.
# 192.168.0.1
# 10.0.0.1-10.0.0.3
# 10.0.0.0/24
#
#windows client
192.168.6.10

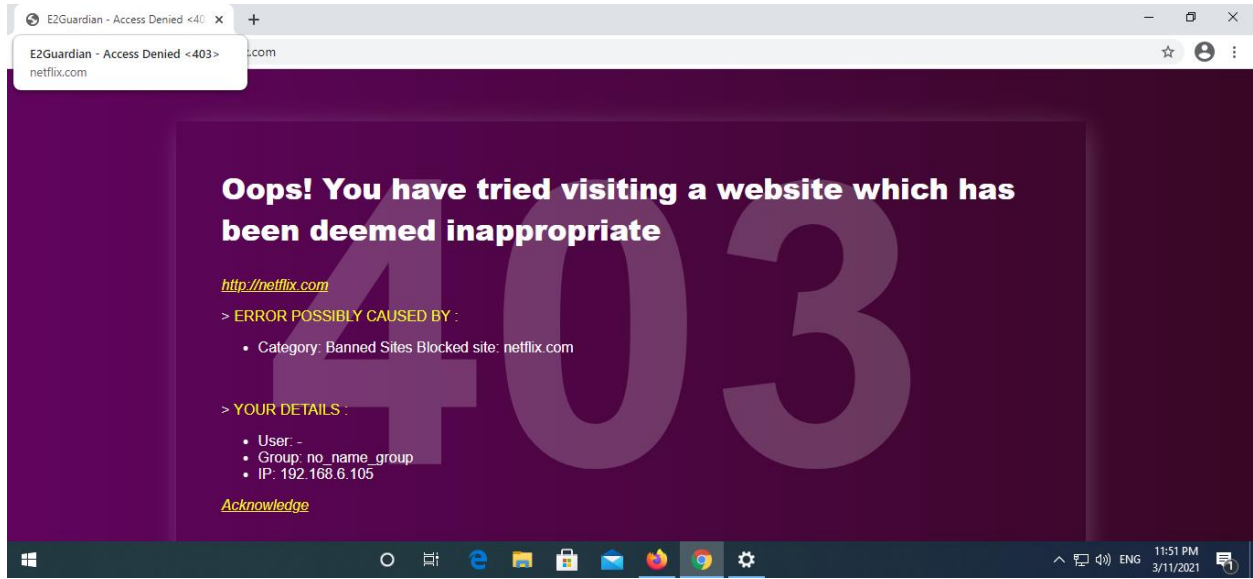
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

WINDOWS MACHINE.



BLOCKED NETFLIX SITE IN WINDOWS MACHINE.

- E2 GUARDIAN BLOCKED SITE



- SQUID SERVICE BLOCKED SITE

