JADHUSAN M S

11/3/2021

# Proxy Server

## System Administration

Jadhusan M.S

# 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

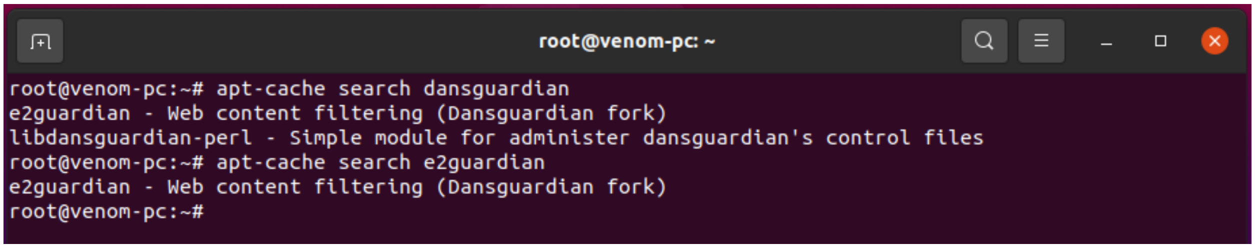
**Words/Phrase list**

- 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**

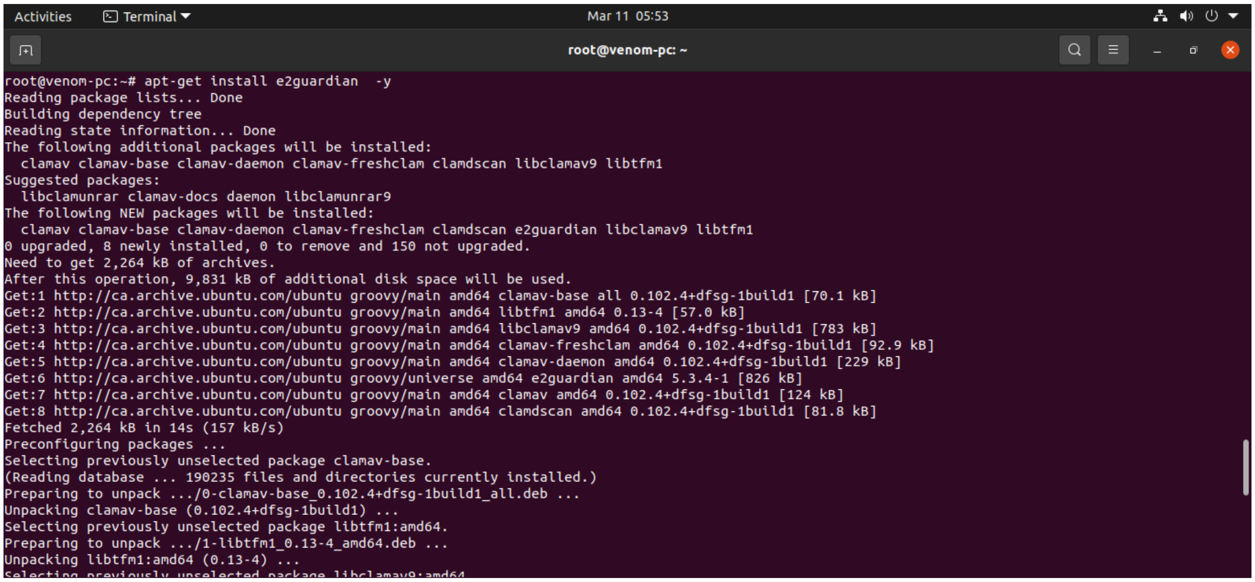
- The main configuration file for e2g is called e2guardian.conf. If you are running a simple filter with just one group on standard ports, there isn't actually anything to change in this file.

## Checking for E2Guardian



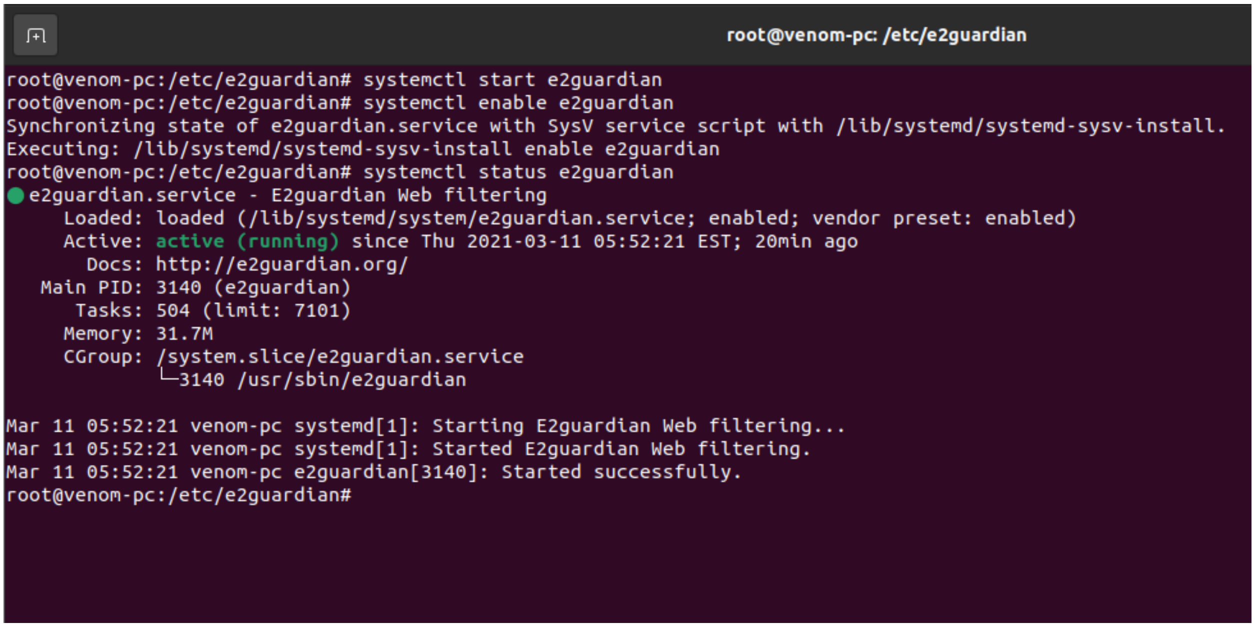
```
root@venom-pc:~# apt-cache search dansguardian
e2guardian - Web content filtering (Dansguardian fork)
libdansguardian-perl - Simple module for administer dansguardian's control files
root@venom-pc:~# apt-cache search e2guardian
e2guardian - Web content filtering (Dansguardian fork)
root@venom-pc:~#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

## Installing E2Guardian



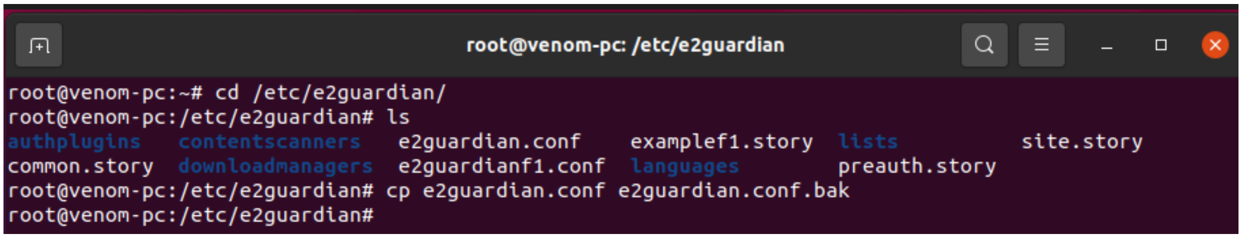
```
root@venom-pc:~# apt-get install e2guardian  -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  clamav clamav-base clamav-daemon clamav-freshclam clamdscan libclamav9 libtfm1
Suggested packages:
  libclamunrar clamav-docs daemon libclamunrar9
The following NEW packages will be installed:
  clamav clamav-base clamav-daemon clamav-freshclam clamdscan e2guardian libclamav9 libtfm1
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 libtfm1 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 clamdscan 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 libtfm1:amd64.
Preparing to unpack .../1-libtfm1_0.13-4_amd64.deb ...
Unpacking libtfm1:amd64 (0.13-4) ...
Selecting previously unselected package libclamav9:amd64
```

## Start / Enable and Check the status of E2Guardian Service.



```
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#
```

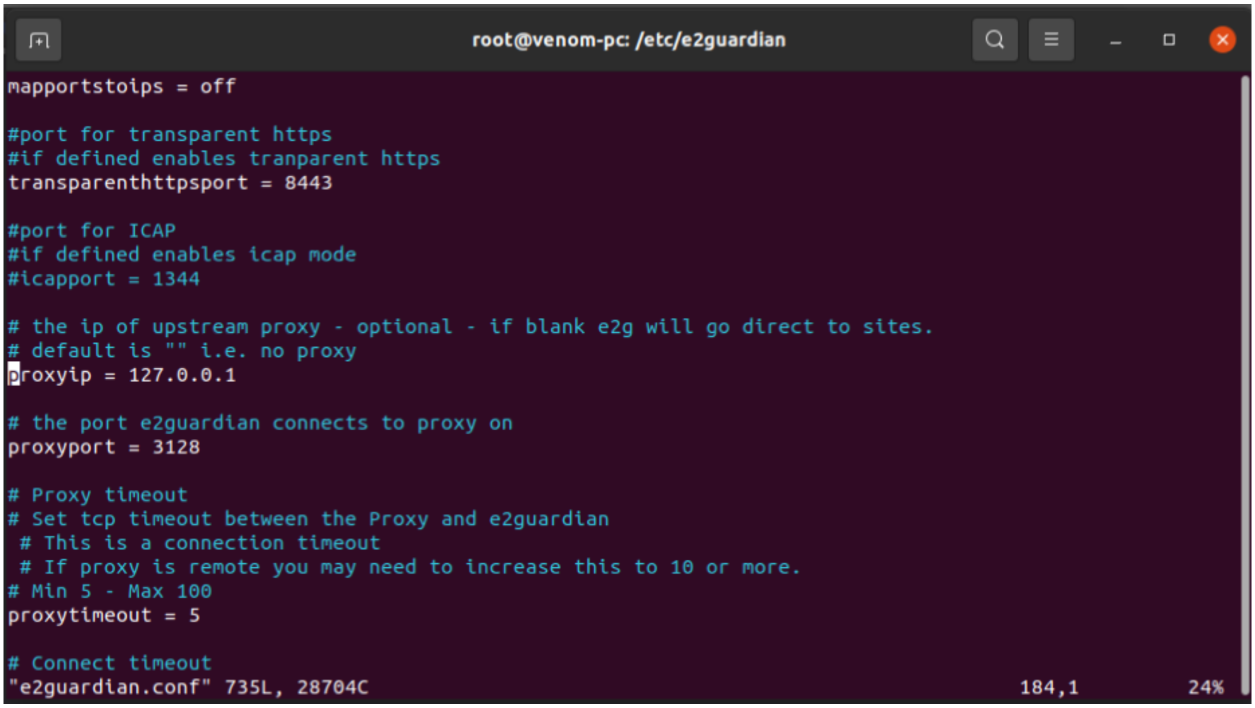
Backed up the config file



```
root@venom-pc:~# 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#
```

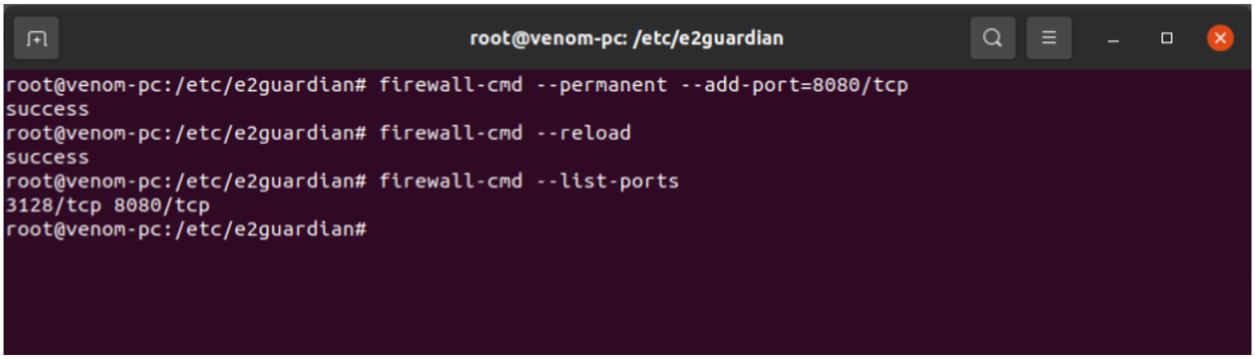
FORWARDING all the conn from 8080 to access 3128.

If both services are configured in  same server, the proxy ip would be localhost ifnot you have to define the ip of squid service.  Both connection works through socket .



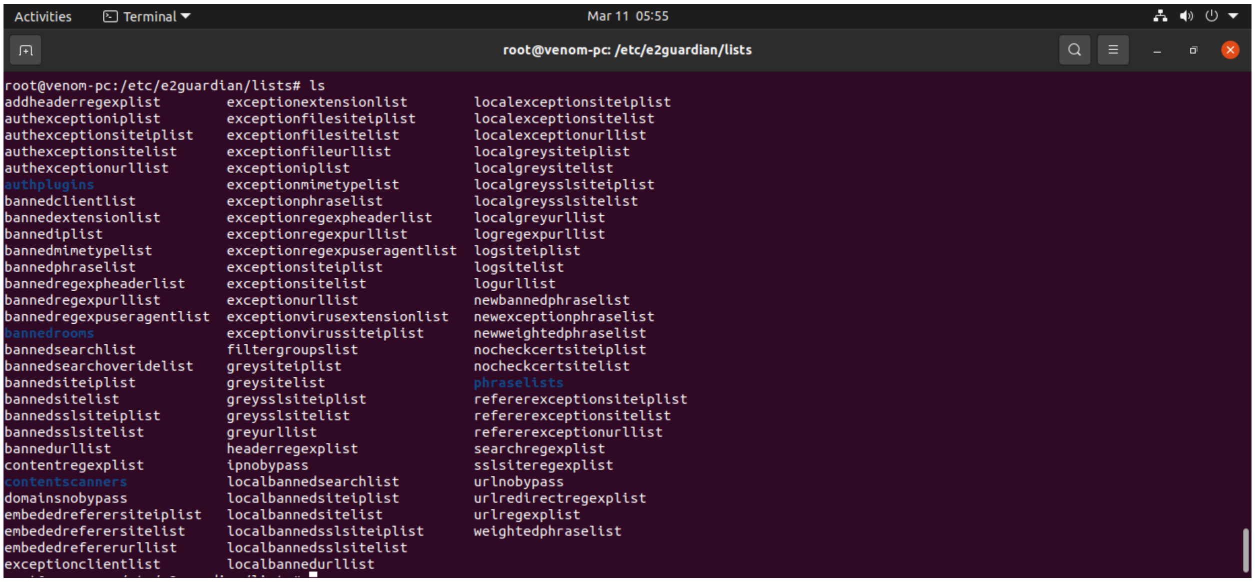
```
mapportstoips = off

#port for transparent https
#if defined enables tranparent 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.



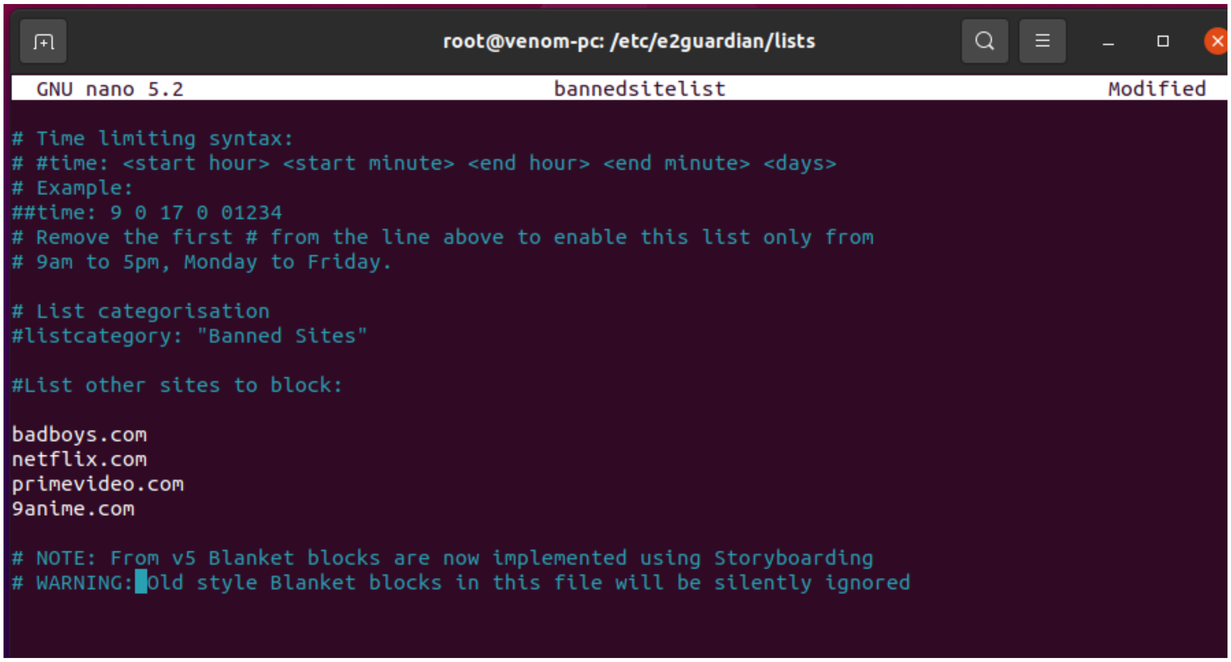
```
root@venom-pc:/etc/e2guardian# firewall-cmd --permanent --add-port=8080/tcp
success
root@venom-pc:/etc/e2guardian# firewall-cmd --reload
success
root@venom-pc:/etc/e2guardian# firewall-cmd --list-ports
3128/tcp 8080/tcp
root@venom-pc:/etc/e2guardian#
```

## THE FILTERING LIST



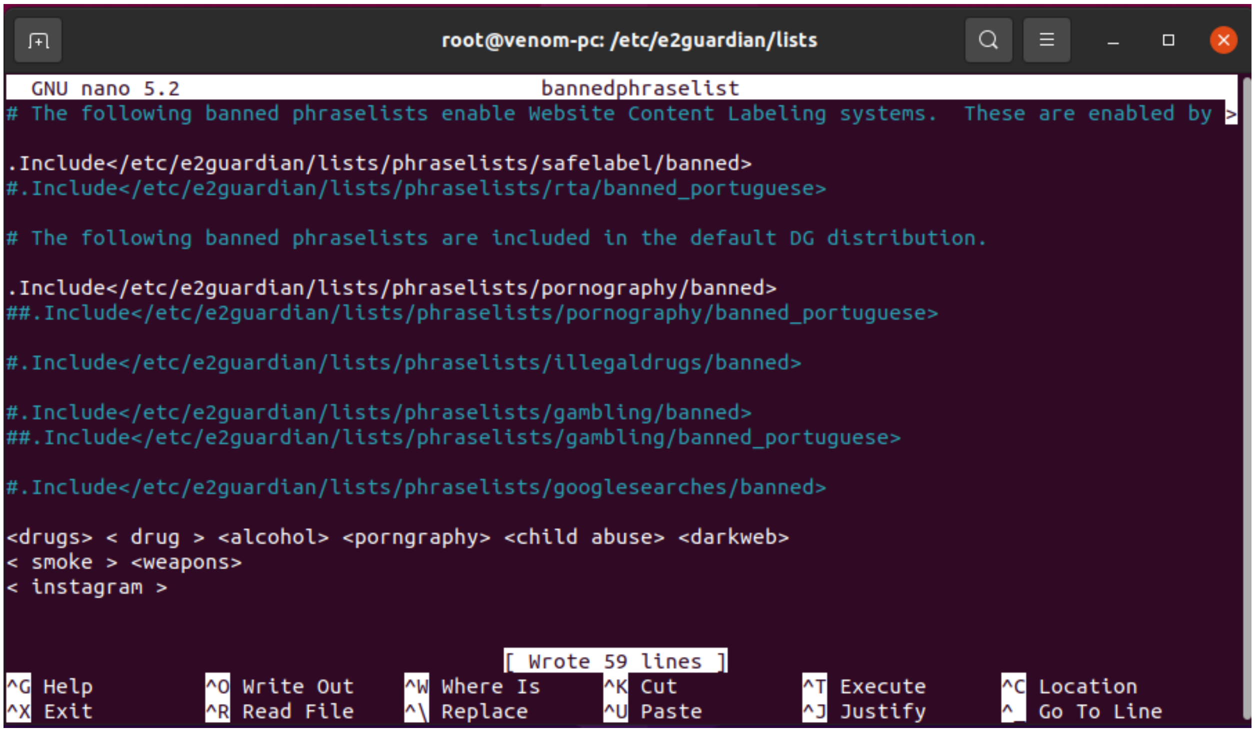
```
root@venom-pc:/etc/e2guardian/lists# ls
addheaderregexplist        exceptionextensionlist        localexceptionsiteiplist
authexceptioniplist        exceptionfilesiteiplist       localexceptionsitelist
authexceptionsiteiplist    exceptionfilesitelist         localexceptionurllist
authexceptionsitelist      exceptionfileurllist          localgreysiteiplist
authexceptionurllist       exceptioniplist               localgreysitelist
authplugins                exceptionmimetypelist         localgreysslsiteiplist
bannedclientlist           exceptionphraselist           localgreysslsitelist
bannedextensionlist        exceptionregexpheaderlist     localgreyurllist
bannediplist               exceptionregexpurllist        logregexpurllist
bannedmimetypelist         exceptionregexpuseragentlist  logsiteiplist
bannedphraselist           exceptionsiteiplist           logsitelist
bannedregexpheaderlist     exceptionsitelist             logurllist
bannedregexpurllist        exceptionurllist              newbannedphraselist
bannedregexpuseragentlist  exceptionvirusextensionlist   newexceptionphraselist
bannedrooms                exceptionvirussiteiplist      newweightedphraselist
bannedsearchlist           filtergroupslist              nocheckcertsiteiplist
bannedsearchoveridelist    greysiteiplist                nocheckcertsitelist
bannedsiteiplist           greysitelist                  phraselists
bannedsitelist             greysslsiteiplist             refererexceptionsiteiplist
bannedsslsiteiplist        greysslsitelist               refererexceptionsitelist
bannedsslsitelist          greyurllist                   refererexceptionurllist
bannedurllist              headerregexplist              searchregexplist
contentregexplist          ipnobypass                    sslsiteregexplist
contentscanners            localbannedsearchlist         urlnobypass
domainsnobypass            localbannedsiteiplist         urlredirectregexplist
embededreferersiteiplist   localbannedsitelist           urlregexplist
embededreferersitelist     localbannedsslsiteiplist      weightedphraselist
embededrefererurllist      localbannedsslsitelist
exceptionclientlist        localbannedurllist
```

## BANNED SITE LIST



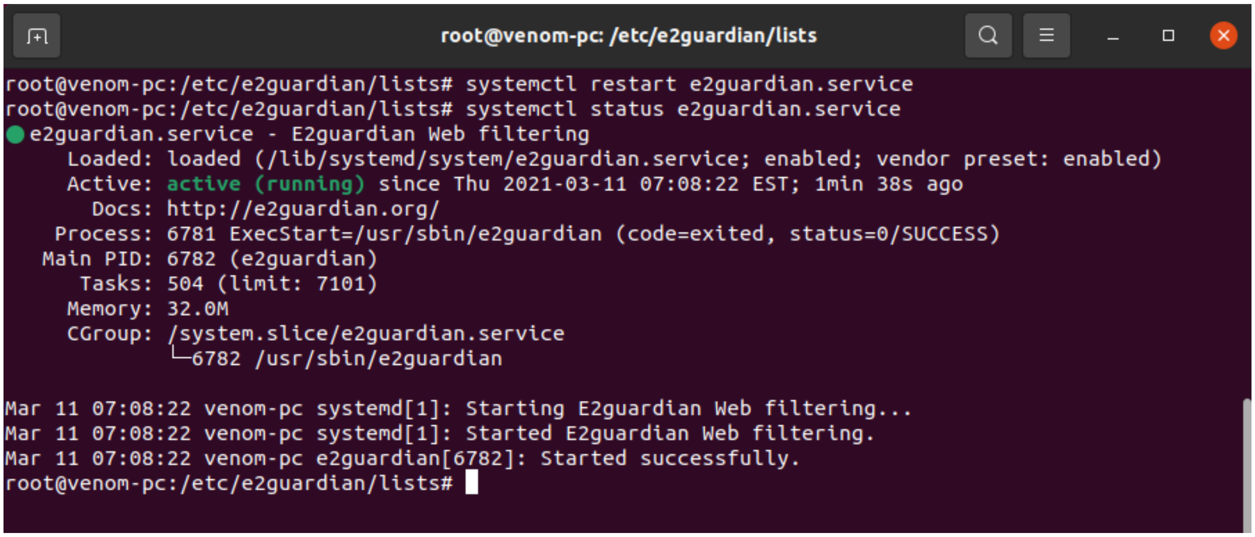
```
  GNU nano 5.2                      bannedsitelist                          Modified

# 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



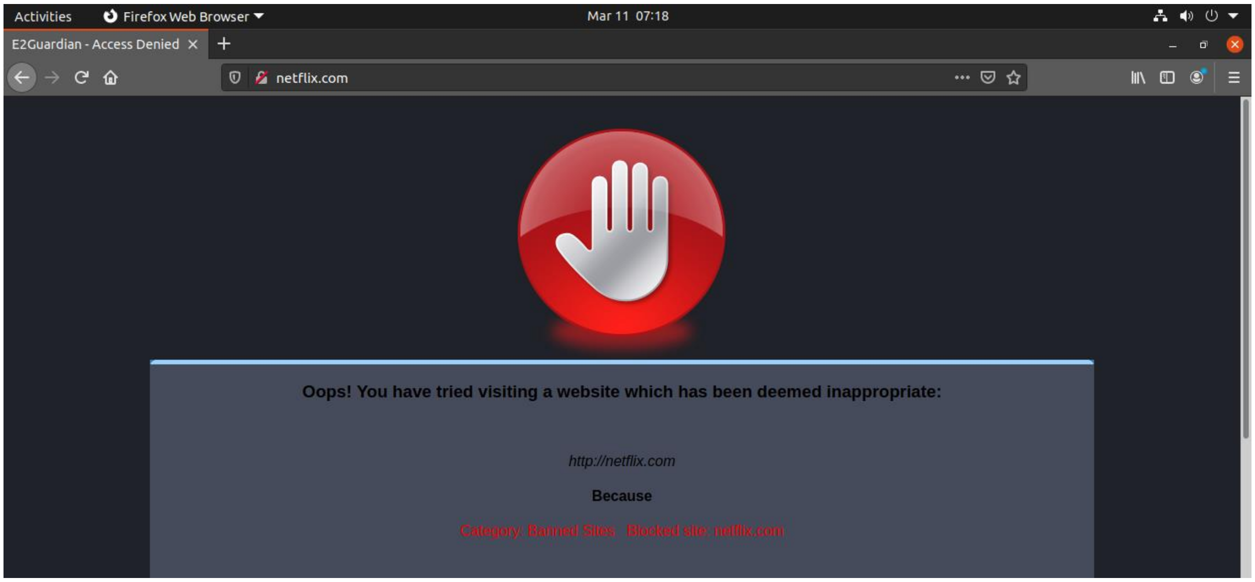
```
 GNU nano 5.2                          bannedphraselist
# The following banned phraselists enable Website Content Labeling systems.  These are enabled by >

.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> <porngraphy> <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# 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



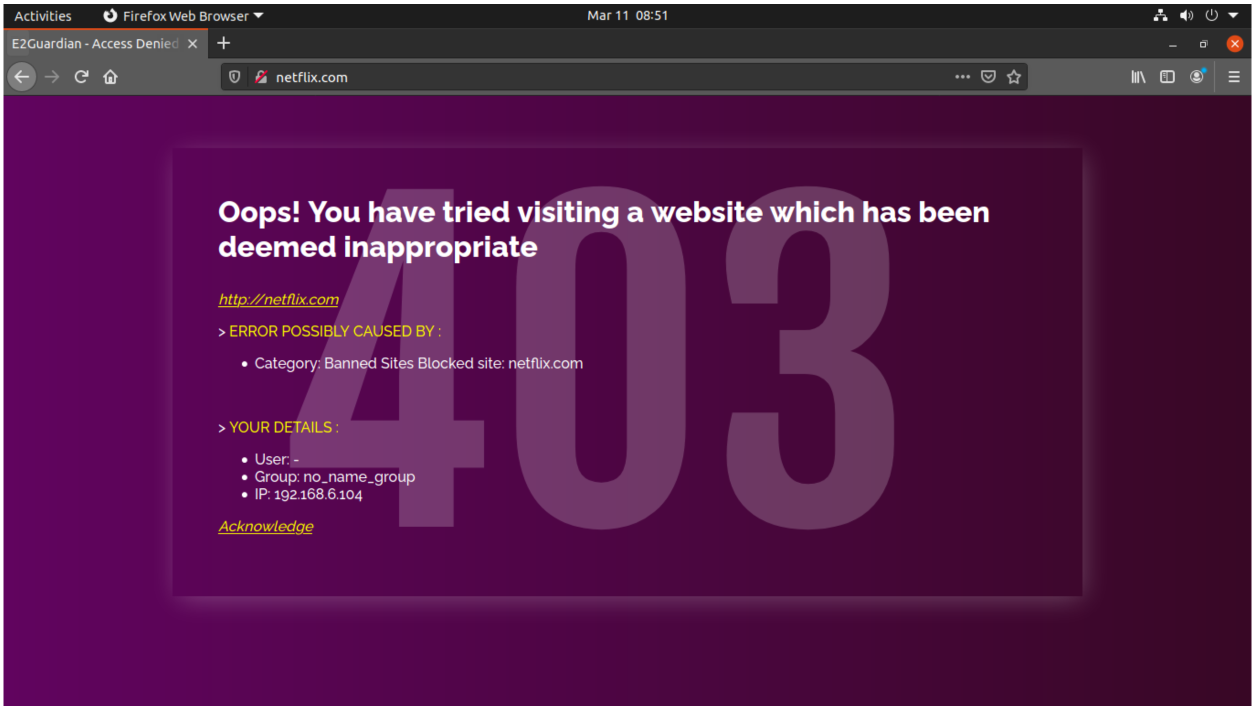
Oops! You have tried visiting a website which has been deemed inappropriate:

*http://netflix.com*

**Because**

Category: Banned Sites Blocked site: netflix.com

## MODIFIED TEMPLATE FOR BLOCKED SITES



**Oops! You have tried visiting a website which has been deemed inappropriate**

*http://netflix.com*

> ERROR POSSIBLY CAUSED BY :

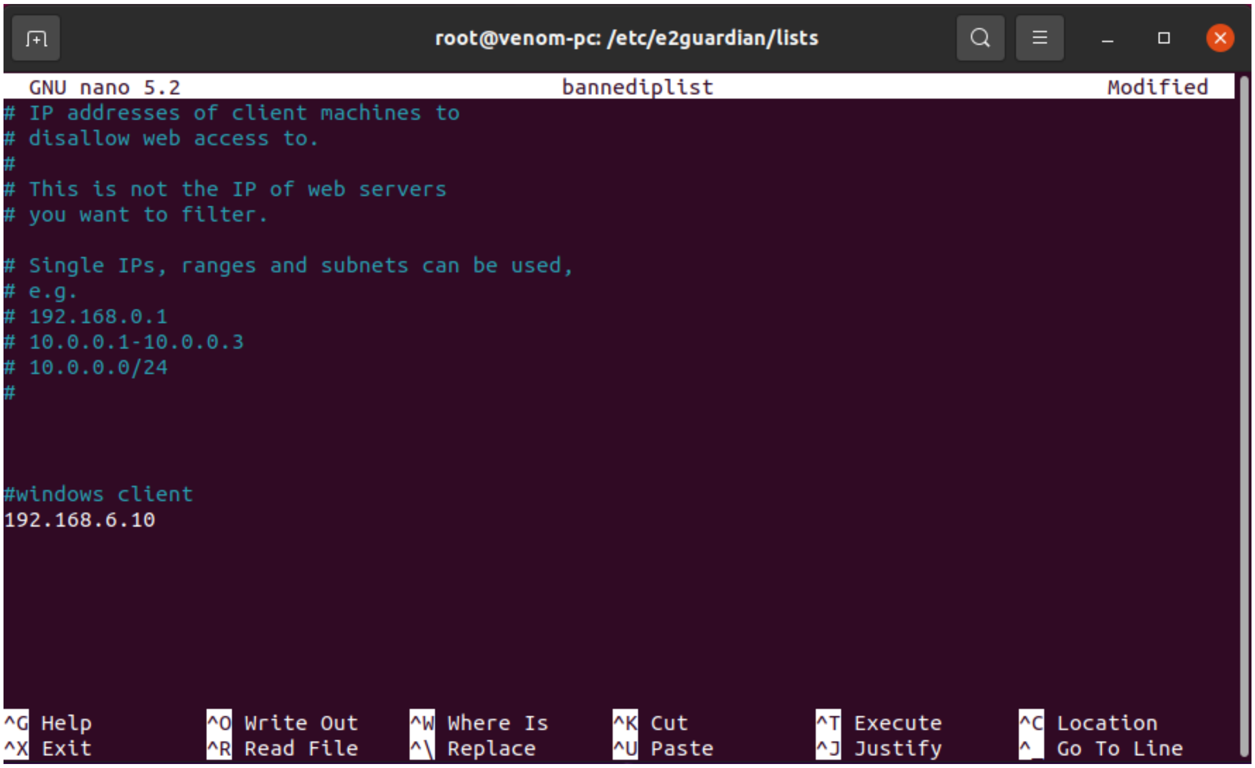
- Category: Banned Sites Blocked site: netflix.com

> YOUR DETAILS :

- User: -
- Group: no_name_group
- IP: 192.168.6.104

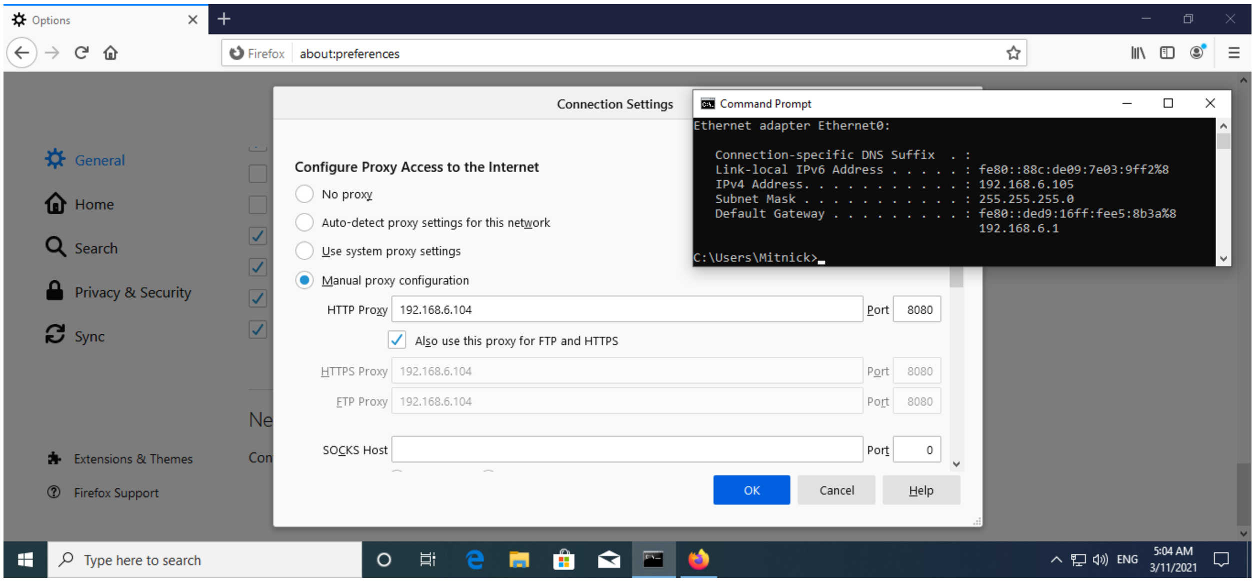
*Acknowledge*

## BANNED IP LIST.



```
  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.



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 192.168.6.104 Port 8080

☑ Also use this proxy for FTP and HTTPS

HTTPS Proxy 192.168.6.104 Port 8080

FTP Proxy 192.168.6.104 Port 8080

SOCKS Host Port 0

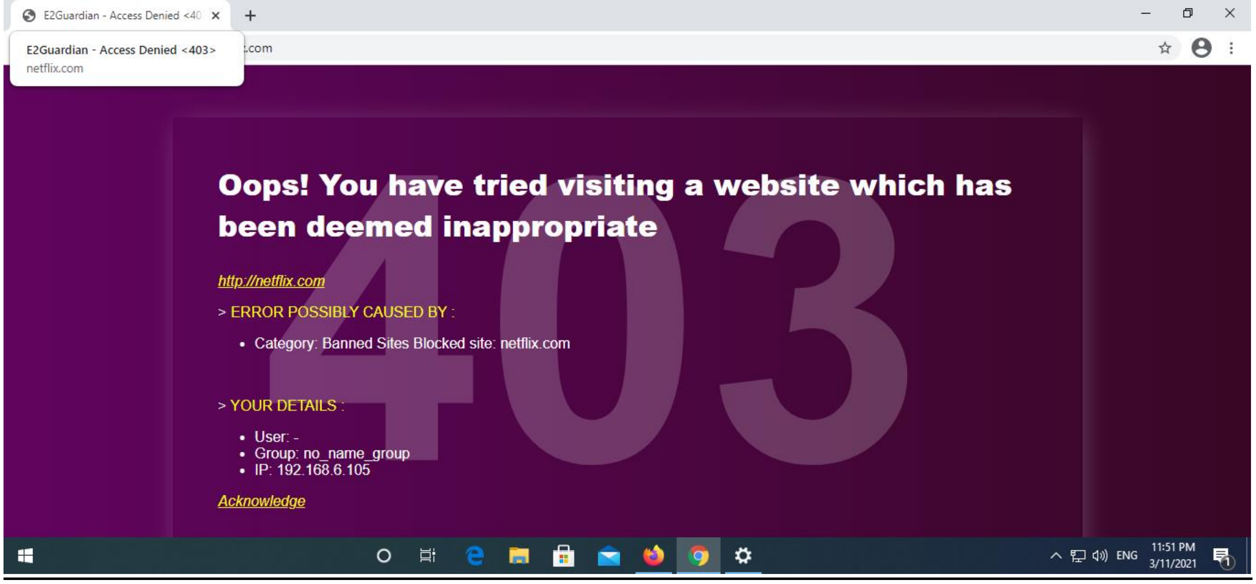
OK Cancel Help

Command Prompt

```
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::88c:de09:7e03:9ff2%8
   IPv4 Address. . . . . . . . . . . : 192.168.6.105
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::ded9:16ff:fee5:8b3a%8
                                       192.168.6.1

C:\Users\Mitnick>_
```

## BLOCKED NETFLIX SITE IN WINDOWS MACHINE.

- E2 GUARDIAN BLOCKED SITE


E2Guardian - Access Denied <40
E2Guardian - Access Denied <403>
netflix.com
.com
403
11:51 PM
3/11/2021
ENG

**Oops! You have tried visiting a website which has been deemed inappropriate**

http://netflix.com

> ERROR POSSIBLY CAUSED BY :

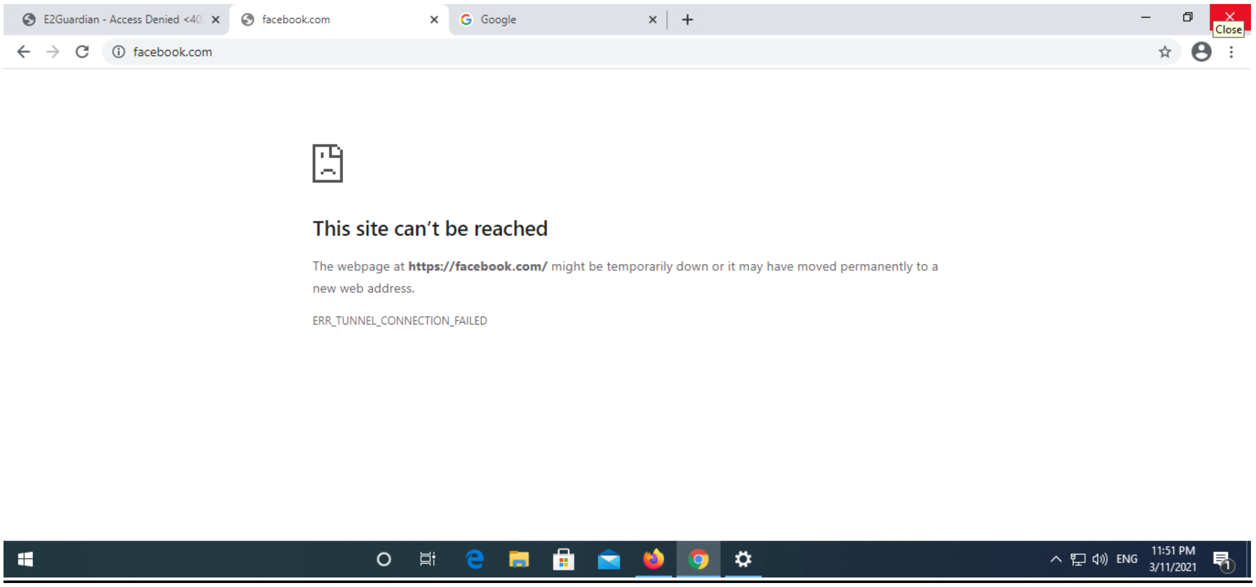
- Category: Banned Sites Blocked site: netflix.com

> YOUR DETAILS :

- User: -
- Group: no_name_group
- IP: 192.168.6.105

Acknowledge

- SQUID SERVICE BLOCKED SITE



This site can’t be reached

The webpage at **https://facebook.com/** might be temporarily down or it may have moved permanently to a new web address.

ERR_TUNNEL_CONNECTION_FAILED