Experiment 4: SQUID

Richard Roy

22UBCA7337

Aim: To create and configure Squid -proxy server Description:

SQUID – PROXY SERVER

Squid is a full-featured web proxy cache server application which provides proxy and cache services for HyperText Transport Protocol (HTTP), File Transfer Protocol (FTP), and other popular network protocols. Squid can implement caching and proxying of Secure Sockets Layer (SSL) requests and caching of Domain Name Server (DNS) lookups, and perform transparent caching. Squid also supports a wide variety of caching protocols, such as Internet Cache Protocol (ICP), the HyperText Caching Protocol (HTCP), the Cache Array Routing Protocol (CARP), and the Web Cache Coordination Protocol (WCCP). The Squid proxy cache server is an excellent solution to various proxy and caching server needs, and scales from the branch office to enterprise-level networks while providing extensive, granular access control mechanisms, and monitoring of critical parameters via the Simple Network Management Protocol (SNMP). When selecting a computer system for use as a dedicated Squid caching proxy server for many users ensure it is configured with a large amount of physical memory as Squid maintains an in-memory cache for increased performance.

Port No: 3128

Package name: squid

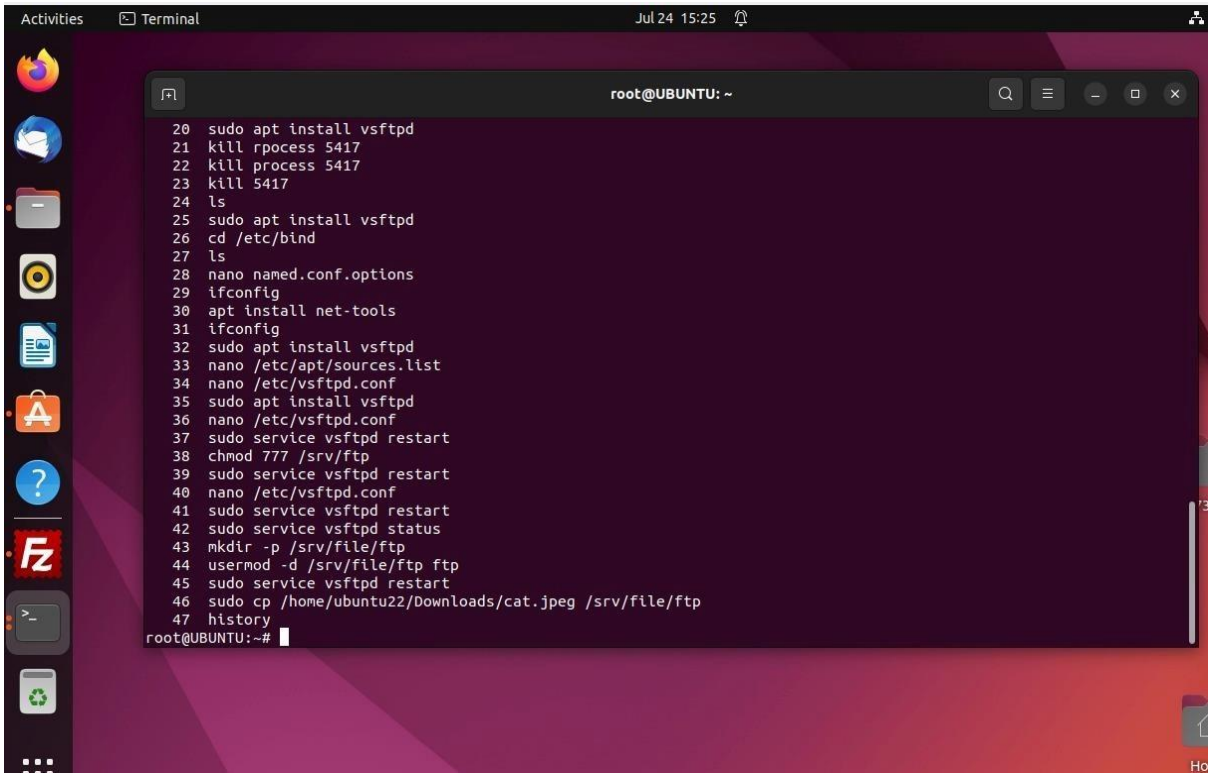
Configuration file: /etc/squid/squid.conf

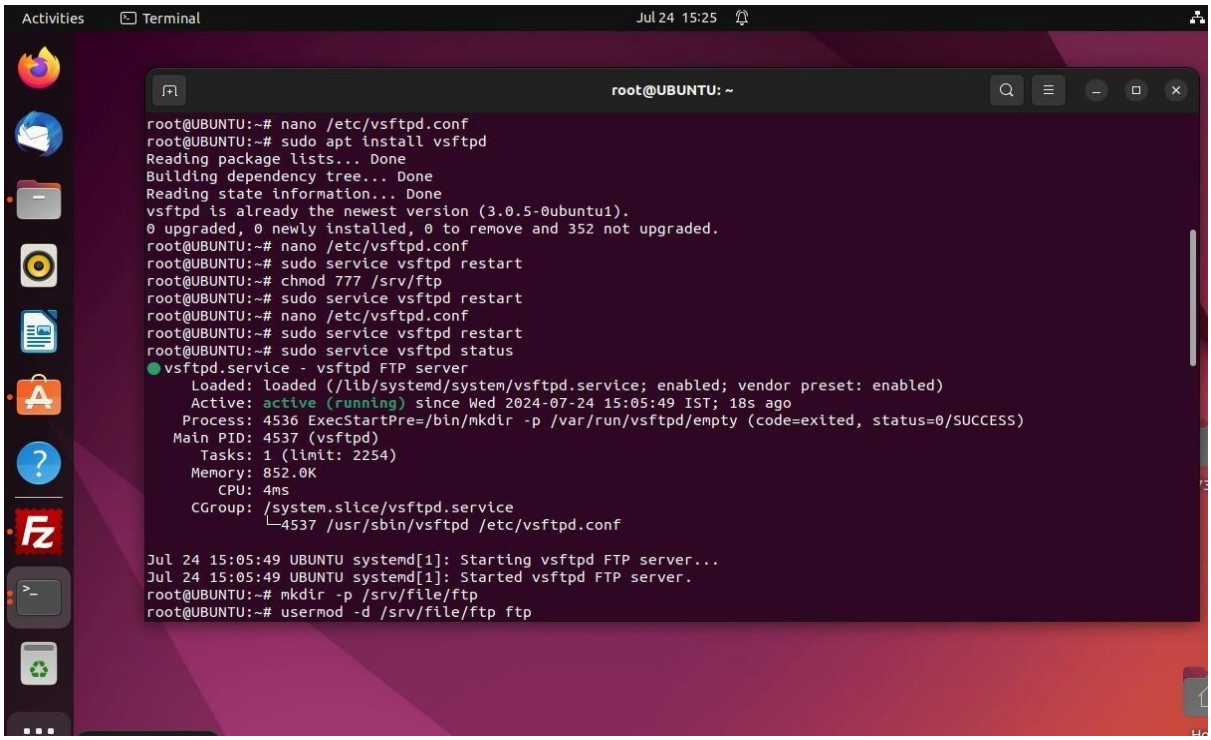
Procedure:

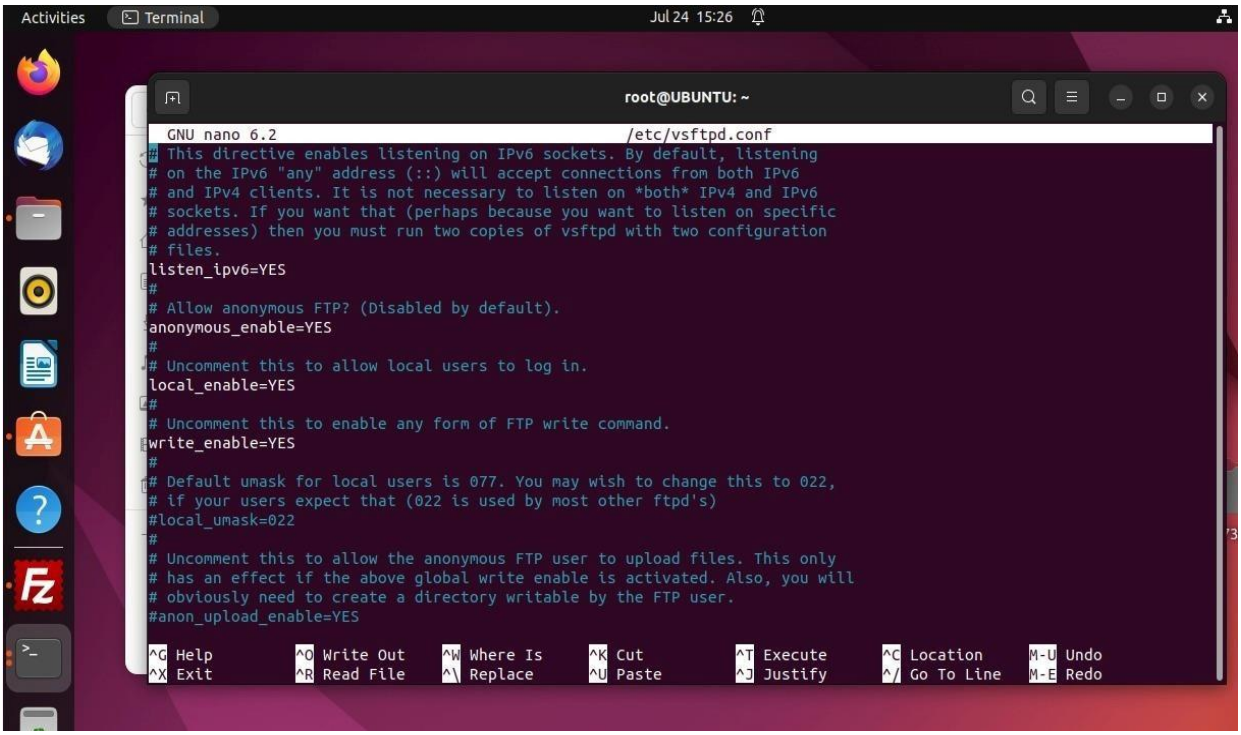
1. At a terminal prompt, enter the following command to install the Squid server: $sudo apt install squid
2. Squid is configured by editing the directives contained within the /etc/squid/squid.conf configuration file.
3. Change the access as shown below: acl localnet src 192.168.234.139(your ip address) acl blocksite dstdomain "/etc/squid/blocksite" http_access deny blocksite http_access allow localnet #http_access deny all http_access allow all
4. To block access to the website we must configure using "/etc/squid/blocksite” we edit the file by running: $cd /etc/squid $sudo gedit blocksite
5. Add the websites to block: in this case, I am blocking youtube, facebook, google

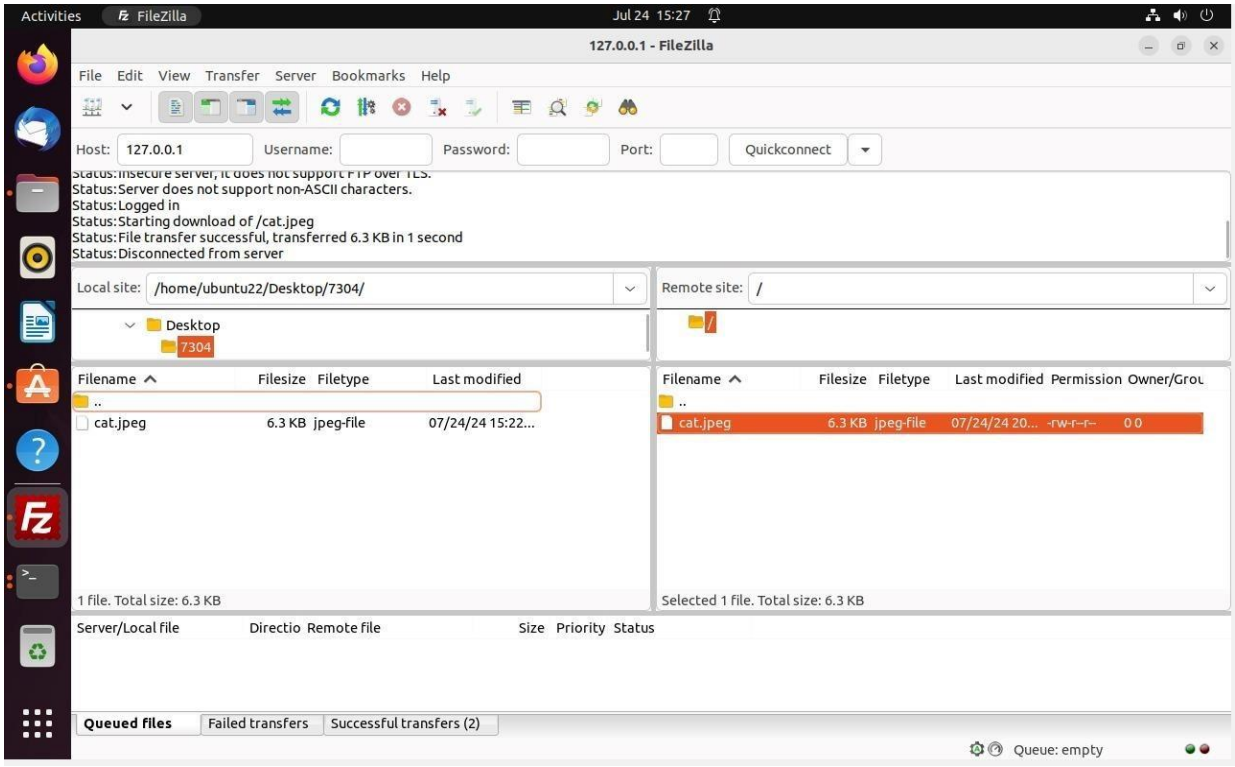
6. To check the actual functioning of the proxy server go to the browser and click settings, search proxy in connection settings.
7. To configure Proxy access to the internet
8. Select Manual Proxy configuration
9. Type your HTTP Proxy(IP Address) and Port number as 3128.
10. Select SOCKS v5 CONNECTING TO WEBSITE
11. Search for the blocked websites 12. Access is denied to the above websites.

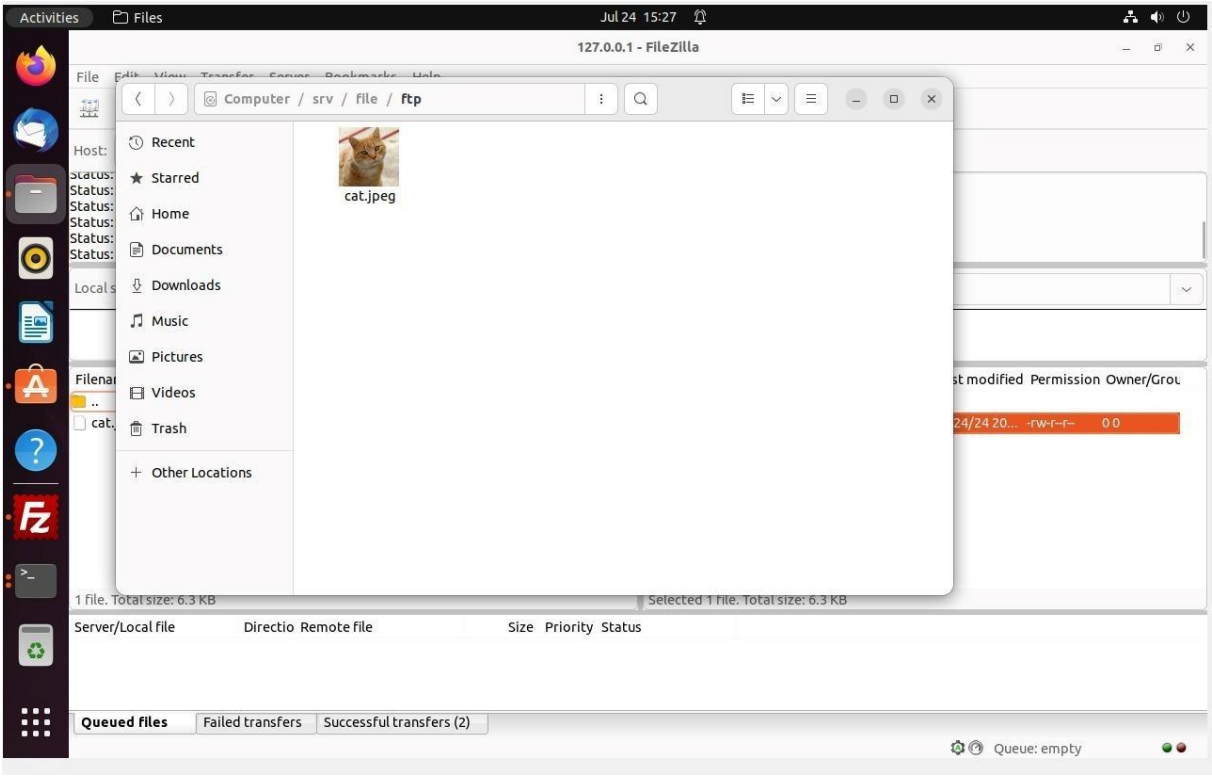
Result:

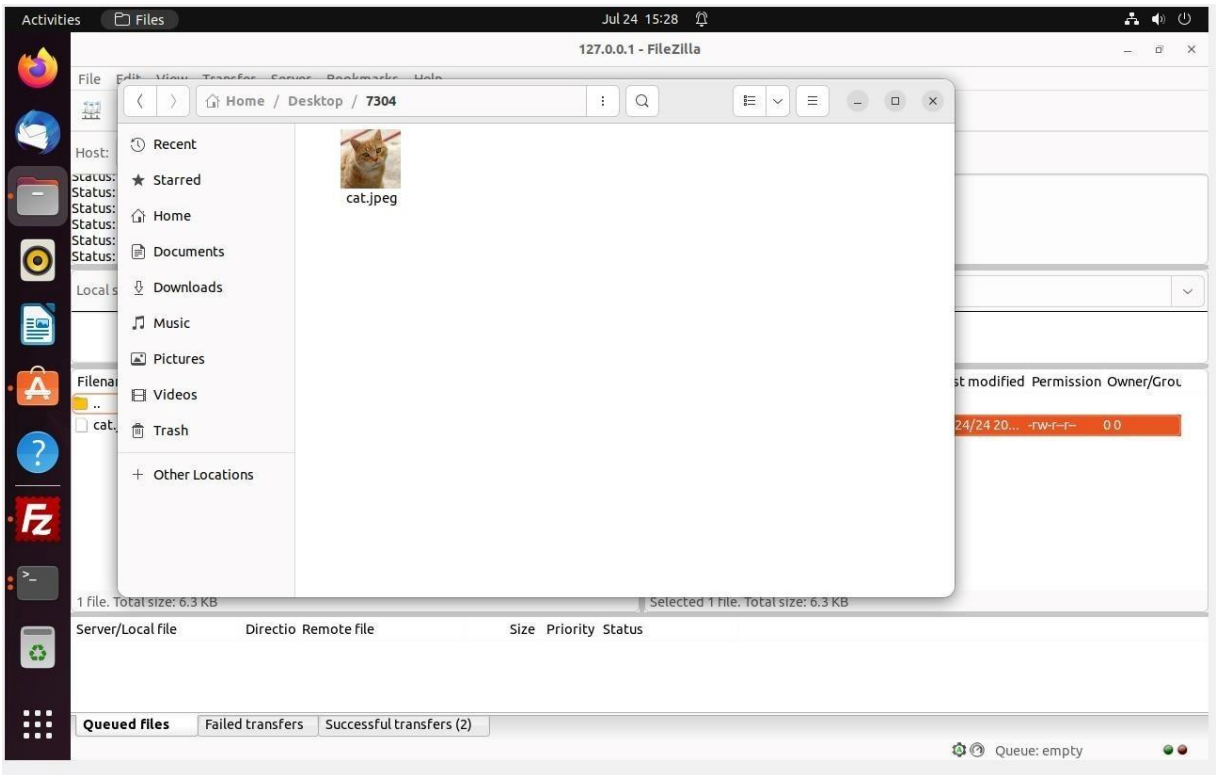



Activities
Terminal
Jul 24 15:25
root@UBUNTU: ~
root@UBUNTU:~# nano /etc/vsftpd.conf
root@UBUNTU:~# sudo apt install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
vsftpd is already the newest version (3.0.5-0ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 352 not upgraded.
root@UBUNTU:~# nano /etc/vsftpd.conf
root@UBUNTU:~# sudo service vsftpd restart
root@UBUNTU:~# chmod 777 /srv/ftp
root@UBUNTU:~# sudo service vsftpd restart
root@UBUNTU:~# nano /etc/vsftpd.conf
root@UBUNTU:~# sudo service vsftpd restart
root@UBUNTU:~# sudo service vsftpd status
vsftpd.service - vsftpd FTP server
Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
Active: active (running) since Wed 2024-07-24 15:05:49 IST; 18s ago
Process: 4536 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
Main PID: 4537 (vsftpd)
Tasks: 1 (limit: 2254)
Memory: 852.0K
CPU: 4ms
CGroup: /system.slice/vsftpd.service
└4537 /usr/sbin/vsftpd /etc/vsftpd.conf
Jul 24 15:05:49 UBUNTU systemd[1]: Starting vsftpd FTP server...
Jul 24 15:05:49 UBUNTU systemd[1]: Started vsftpd FTP server.
root@UBUNTU:~# mkdir -p /srv/file/ftp
root@UBUNTU:~# usermod -d /srv/file/ftp ftp


Activities
Terminal
Jul 24 15:26
root@UBUNTU: ~
GNU nano 6.2 /etc/vsftpd.conf
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
Default umask for local users is 077. You may wish to change this to 022,
if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
Uncomment this to allow the anonymous FTP user to upload files. This only
has an effect if the above global write enable is activated. Also, you will
obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo


Activities
FileZilla
Jul 24 15:27
127.0.0.1 - FileZilla
File Edit View Transfer Server Bookmarks Help
Host: 127.0.0.1 Username: Password: Port: Quickconnect
Status: Server does not support non-ASCII characters.
Status: Logged in
Status: Starting download of /cat.jpeg
Status: File transfer successful, transferred 6.3 KB in 1 second
Status: Disconnected from server
Local site: /home/ubuntu22/Desktop/7304/
Remote site: /
Desktop
7304
Filename Filesize Filetype Last modified
..
cat.jpeg 6.3 KB jpeg-file 07/24/24 15:22...
Filename Filesize Filetype Last modified Permission Owner/Grou
..
cat.jpeg 6.3 KB jpeg-file 07/24/24 20... -rw-r--r-- 0 0
1 file. Total size: 6.3 KB
Selected 1 file. Total size: 6.3 KB
Server/Local file Directio Remote file Size Priority Status
Queued files Failed transfers Successful transfers (2)
Queue: empty





Conclusion:

All the commands have been executed and the output has been obtained successfully.