Squid Proxy Server Checklist (Linux)

1. -Go into the configuration file with sudo gedit /etc/squid/squid.conf &

-Find the #acl localnet src line that corresponds to your network/IP address and ensure that it is uncommented

-For example, if my network is 192.168.1.0/255.255.255.0, uncomment #acl localnet src 192.168.1.0/24

1. Modify configuration file

-Reduce Squid’s configuration file to a more readable/useful one that takes out empty lines and documentation

mv /etc/squid/squid.conf /etc/squid/squid.conf.bkp

grep –Eiv ‘(^#|^$)’ /etc/squid/squid.conf.bkp > /etc/squid/squid.conf

-This creates a .bkp file that is the original file, and squid.conf now only contains the useful lines.

1. Restart Squid

sudo service squid restart

-Every time the configuration file is changed, restart Squid.

1. Check the version of Squid

-In the terminal, execute

/usr/sbin/squid –v

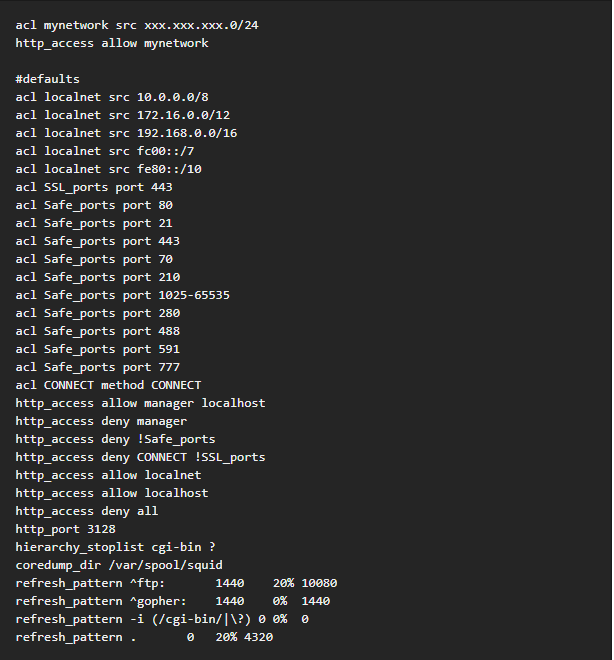
-You should see anything from version 2.6 to the most current version, 3.5. These versions are pretty stable and do not have serious vulnerabilities. Earlier versions like 2.5, however, do have some issues. These are not vulnerabilities so much as problems with the program itself that may result in the proxy doing something you didn’t think you configured it to do. For instance, it “does not trigger a fatal error when it identifies missing or invalid ACLs in the http\_access configuration, which could lead to less restrictive ACLs than intended by the administrator.” The worst issue is that “when processing the configuration file, Squid 2.5 parses empty Access Control Lists (ACLs), including proxy\_auth ACLs without defined auth schemes, in a way that effectively removes arguments, which could allow remote attackers to bypass intended ACLs if the administrator ignores the parser warnings.” These problems are good to look for, but even if you have Squid 2.5 or below, following the steps below will still result in a good configuration setup.

1. Check configuration file

-Go back into the config file

sudo gedit /etc/squid/squid.conf &

-If you have version 3.5, the most current version, you should see something like this:



-These are the default settings for Squid. Earlier versions of squid have similar default files, except sometimes the order changes for the commands. Either way, this should generally be what it looks like. Check to see if there are any significant changes that look out of place. One example from a previous competition is that there were a few ACLs in the Squid configuration file that were blocking a few websites from being accessed. Simply remove those lines to get back to the default stage.

1. To use Squid with Firefox, complete the following commands in the Firefox browser:

-Edit

-Preferences

-Advanced

-Network

-Settings

-Check Manual proxy configuration

-Next to HTTP Proxy, enter your IP address, and enter Port 3128.

-OK

-Close

1. Basic Configurations
   1. To see what squid is doing on the network, you can look at /var/log/squid/access.log or /var/log/squid/cache.log
   2. Configure an ACL to block certain IPs

-Make a new file called bad\_hosts.txt and put it in /etc/squid (cd /etc/squid, then cat > bad\_hosts.txt)

-Add to that new file a list of IPs to block

-Edit squid.conf (sudo gedit /etc/squid/squid.conf &) and add the following lines:

acl bad\_hosts src “/etc/squid/bad\_hosts.txt”

http access deny bad\_hosts

1. Add Squid to the firewall

firewall-cmd –add-port=3128/tcp –permanent

-This will only work if the firewall is already enabled.

1. Restrict access by user authentication

-Go back into squid.conf with sudo gedit /etc/squid/squid.conf &

-Add the following lines:

auth\_param basic program /usr/lib/squid/ncsa\_auth /etc/squid/passwd

auth\_param basic credentialsttl 30 minutes

auth\_param basic casesensitive on

auth\_param basic realm Squid proxy-caching web server for Tecmint’s LFCE series

acl ncsa proxy\_auth REQUIRED

http\_access allow ncsa

-Then back in the console, type in the following command to add credentials for a given user (in this case Username) that will be accepted by Squid:

htpasswd –c /etc/squid/passwd Username

-You will be prompted to create a password.

-Now, anytime you need to use a web browser, you will need to enter the username and password you specified to gain access.

AnalogX Proxy Server Checklist (Windows)—Use if you see a green P in the taskbar

For windows in general, proxy servers are largely handled at the firewall level. Likely the best approach is to do a cursory check of the proxy setup and then consult the firewall checklist for further configurations.

1. HTTP’s proxy server is at port 6588.
2. How to test if the proxy server’s connection is working/configure your browser to use the proxy:
   1. Hit the windows button, and search “Internet Options”
   2. Click on “Internet Options”
   3. Click on the Connections tab
   4. Click on LAN settings
   5. Under Proxy server, check the box that says “Use a proxy server for your LAN”
   6. In the address box, type in the IP address of that computer
   7. In the Port box type: 6588
   8. Click Ok, then Ok
   9. Open a web browser and you should be able to access the internet

Other port numbers for services that AnalogX can support:

|  |  |
| --- | --- |
| HTTP/HTTPS | 6588 |
| SOCKS4 (TCP proxying) | 1080 |
| SOCKS4a (TCP proxying w/ DNS lookups) | 1080 |
| SOCKS5 (only partial support, no UDP) | 1080 |
| NNTP (usenet newsgroups) | 119 |
| POP3 (receiving email) | 110 |
| SMTP (sending email) | 25 |
| FTP (file transfers) | 21 |

1. Configuring the proxy:
   1. Make sure the proxy is on by searching for “AnalogX” and clicking on Proxy
   2. There should be a green P in the taskbar (up arrow in the bottom right-hand corner)
   3. All configurations are completed through the “Configure” menu
   4. When in this menu the proxy is disabled (you'll notice the tray icon will be red), and when done, it will automatically start back up.
   5. Security Configurations:
      1. By default the proxy binds to all TCP/IP interfaces on your computer - this is primarily to make it easy to get running, but it also means that it will service requests from the Internet as well. You can force Proxy to only bind to your local IP address in the Configuration menu, at the 'Proxy Bind' option. If this is set to 'disabled', then it will bind to all interfaces, but if a valid TCP/IP address is entered, the proxy will ONLY bind to that - so if you enter 10.0.0.1, and that's your server's IP address, then the proxy will only talk to machines that connect to that IP, in other words, only your local network.

Squid Proxy Server Checklist (Windows)—Use if you see a blue squid in the taskbar

-Again, check the firewall with the firewall checklist.

-Search for “Windows Firewall with Advanced Security” and open up the Rules (both Inbound and Outbound).

-Check for a rule with a Name with the word “Squid” in it. This is where you will see ACLs associated with the Squid proxy. Examine this rule to check for discrepancies similar to the ones described in the Linux section for Squid.

-Besides that, configuration is the same as for AnalogX, so look at that checklist for advice on how to use that for internet browsing.