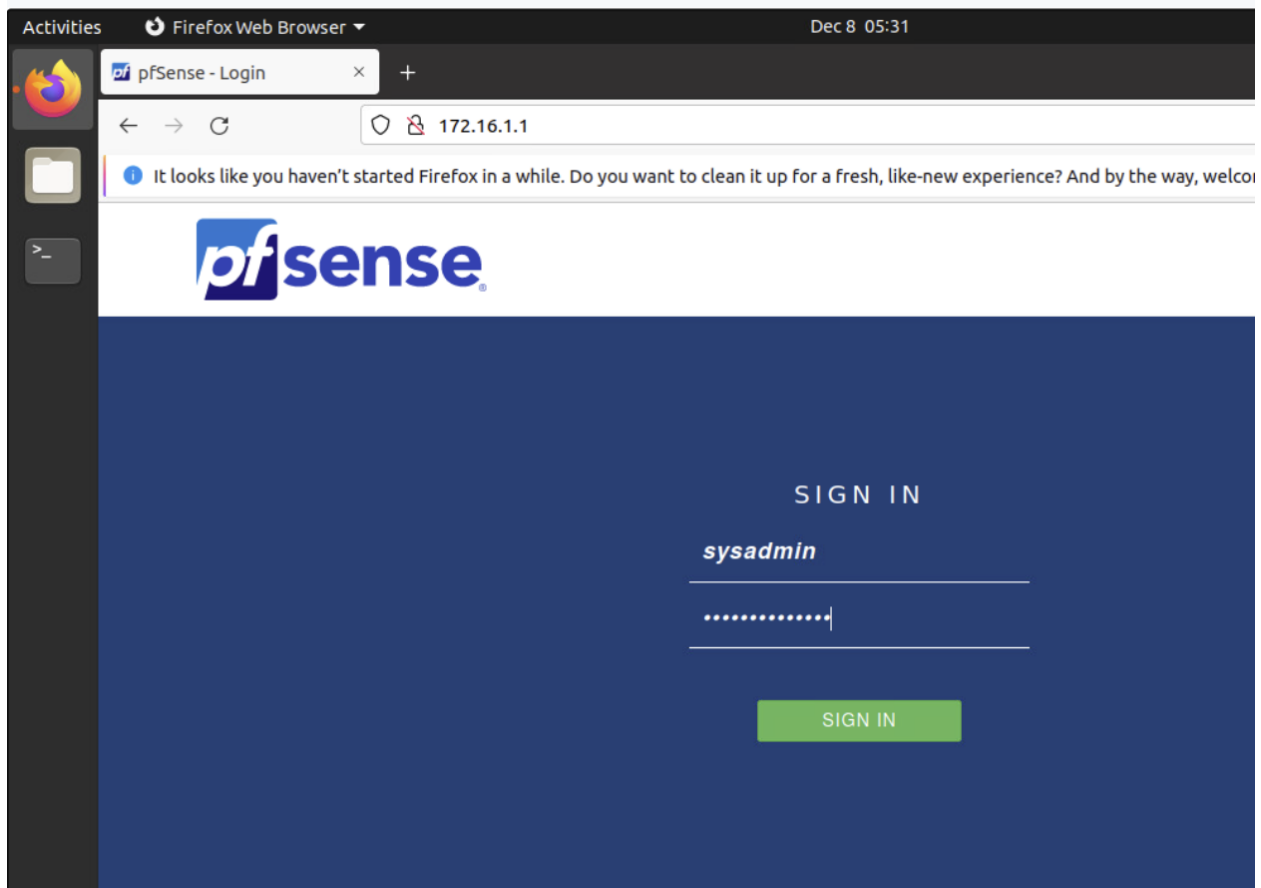


Peter Sanford
IT 2700
NetLab Lab 15
12/07/2023

1.1

Step 5:



Step 12:

Select the IP version Squid will use to select addresses for accepting client connections.

CARP Status VIP	<input type="text" value="none"/>
Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP	
Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC	
Proxy Interface(s)	<div><div>WAN</div><div>LAN</div><div>DMZ</div><div>loopback</div></div>
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.	
Outgoing Network Interface	<input type="text" value="LAN"/>
The interface the proxy server will use for outgoing connections.	

Step 19:

Log Pages Denied by SquidGuard

☐ Makes it possible for SquidGuard denied log to be included on Squid logs.

[Click Info for detailed instructions.](#) 

Headers Handling, Language and Other Customizations

Visible Hostname

This is the hostname to be displayed in proxy server error messages.

Administrator's Email

This is the email address displayed in error messages to the users.

Error Language

Select the language in which the proxy server will display error messages to users.

Step 22:

[General](#) [Remote Cache](#) [Local Cache](#) [Antivirus](#) [ACLs](#) [Traffic Mgmt](#) [Authentication](#)

Squid Access Control Lists

Allowed Subnets

Enter subnets that are allowed to use the proxy in CIDR format. All the other subnets won't be allowed.
Put each entry on a separate line.

When 'Allow Users on Interface' is checked on 'General' tab, there is no need to add the 'Proxy' rule.

Step 27:

Squid Traffic Management Settings

Maximum Download Size

Limit the maximum total download size to the size specified here (in kilobytes). Set to 0 to disable.

Traffic control settings mainly work with universal HTTP, so it may not work without HTTPS interception, if HTTP with dynamic content (javascript).

Maximum Upload Size

Limit the maximum total upload size to the size specified here (in kilobytes). Set to 0 to disable.

1.2

Step 2:

General Options

Enable



Check this option to enable squidGuard.

Important: Please set up at least one category on the 'Target Categories' page. The Save button at the bottom of this page must be clicked. To activate squidGuard configuration changes, **the Apply**

✓ Apply

Step 6:

Enable



Check this option to enable squidGuard.

Important: Please set up at least one category on the 'Target Categories' page. The Save button at the bottom of this page must be clicked. To activate squidGuard configuration changes, **the Apply**

✓ Apply

Step 12:

Enter word fragments of the destination URL. To separate them use | . **Example:** mail|casino|game|

Redirect mode

int error page (enter error message) ▾

Select redirect mode here.

Note: if you use 'transparent proxy', then 'int' redirect mode will not be accessible.

Options: [ext url err page](#), [ext url redirect](#), [ext url as 'move'](#), [ext url as 'found'](#).

Step 17:

Target Categories

[Blist1]

Default access [all]

Do not allow IP-
addresses in URL



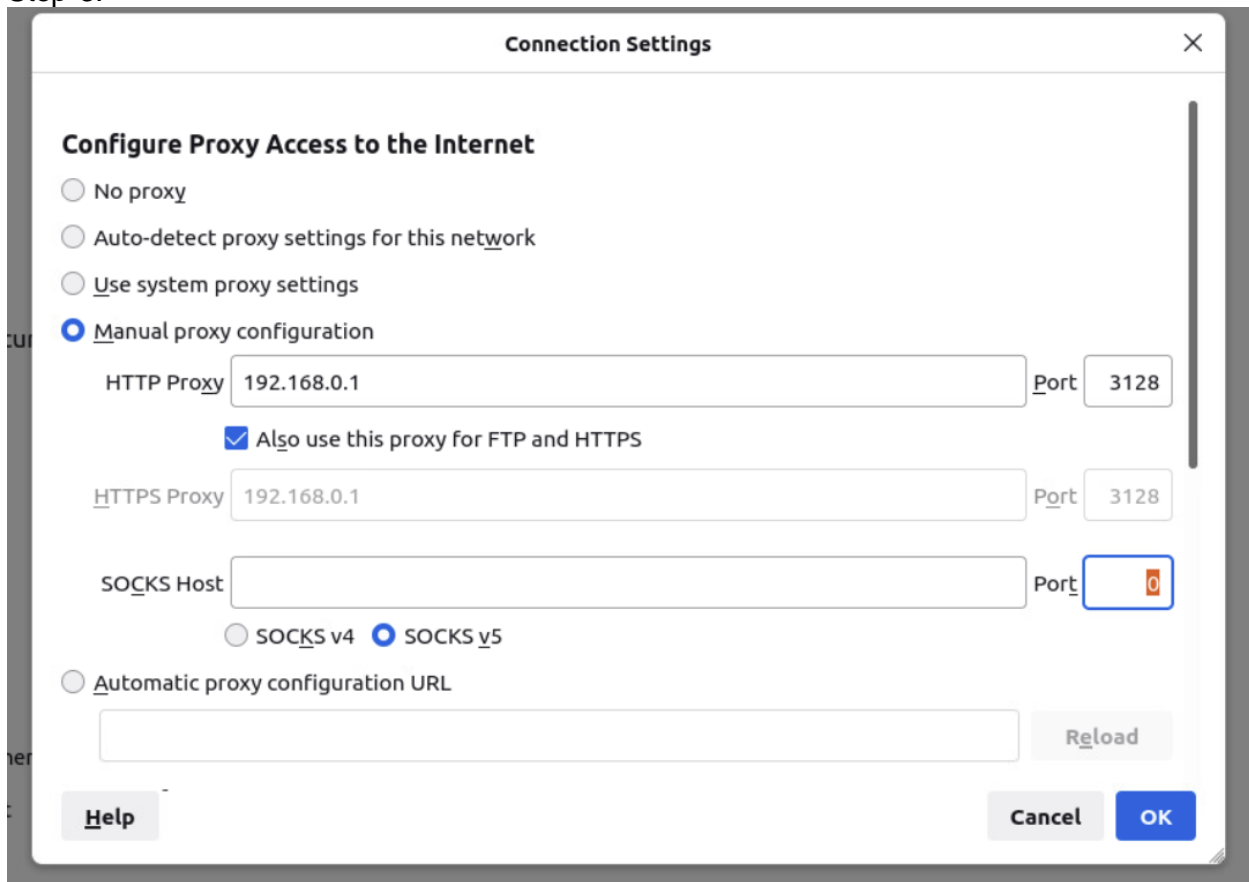
To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.

Denied Error

Request denied by the XYZ Security proxy

The first part of the error message displayed to clients when access was denied. Defaults to "Request denied by \$glproduct_name".

Step 3:



The image shows a 'Connection Settings' dialog box with a close button (X) in the top right corner. The title is 'Connection Settings'. Below the title is a section 'Configure Proxy Access to the Internet'. There are four radio buttons: 'No proxy', 'Auto-detect proxy settings for this network', 'Use system proxy settings', and 'Manual proxy configuration'. The 'Manual proxy configuration' option is selected. Below this, there are three proxy configuration sections. The first is 'HTTP Proxy' with a text field containing '192.168.0.1' and a 'Port' field containing '3128'. Below this is a checked checkbox 'Also use this proxy for FTP and HTTPS'. The second is 'HTTPS Proxy' with a text field containing '192.168.0.1' and a 'Port' field containing '3128'. The third is 'SOCKS Host' with an empty text field and a 'Port' field containing '0'. Below this are two radio buttons: 'SOCKS v4' and 'SOCKS v5', with 'SOCKS v5' selected. At the bottom, there is an 'Automatic proxy configuration URL' section with an empty text field and a 'Reload' button. At the very bottom are three buttons: 'Help', 'Cancel', and 'OK'.

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 192.168.0.1 Port 3128

☒ Also use this proxy for FTP and HTTPS

HTTPS Proxy 192.168.0.1 Port 3128

SOCKS Host Port 0

☐ SOCKS v4 ☒ SOCKS v5

☐ Automatic proxy configuration URL

Reload

Help Cancel OK

Step 5:



The image shows a Firefox Web Browser window. The title bar says 'Firefox Web Browser'. The address bar shows 'casino.com'. The main content area displays a 'Request denied by the XYZ Security proxy: 403 Forbidden' error. Below the error message is a section titled '; Reason:' which contains the following information: 'Client address: 172.16.1.10', 'Client name: 172.16.1.10', 'Client group: default', 'Target group: Blist1', and 'URL: http://casino.com/'.

Firefox Web Browser

squidGuard Error page

casino.com

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like

Request denied by the XYZ Security proxy: 403 Forbidden

; Reason:

Client address: 172.16.1.10

Client name: 172.16.1.10

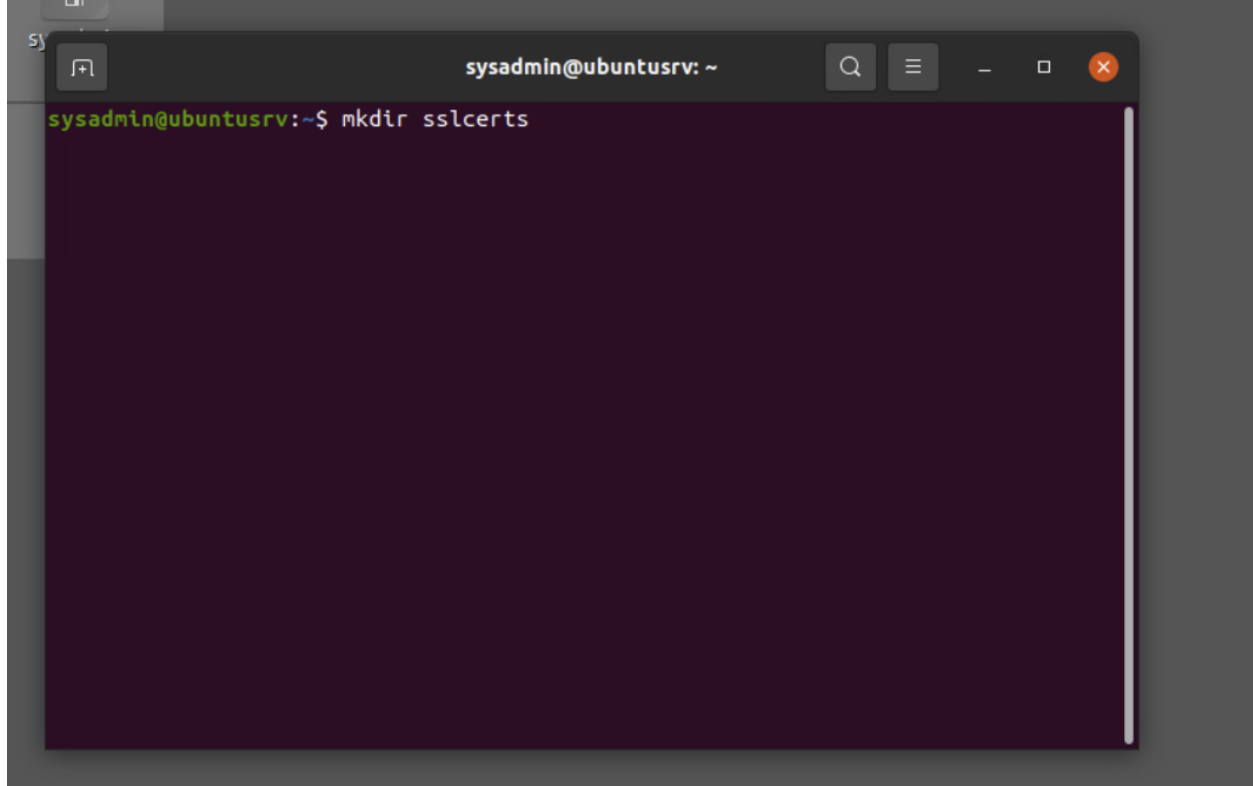
Client group: default

Target group: Blist1

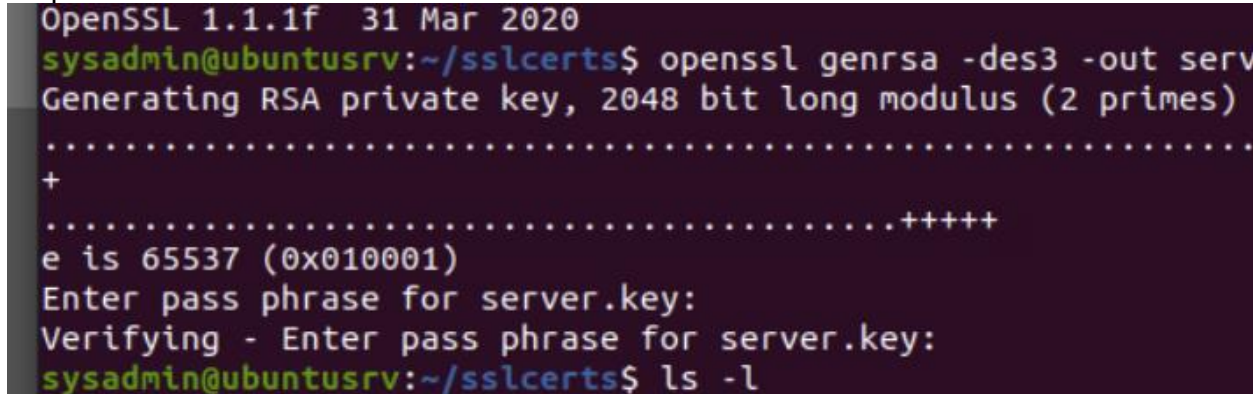
URL: http://casino.com/

2.1

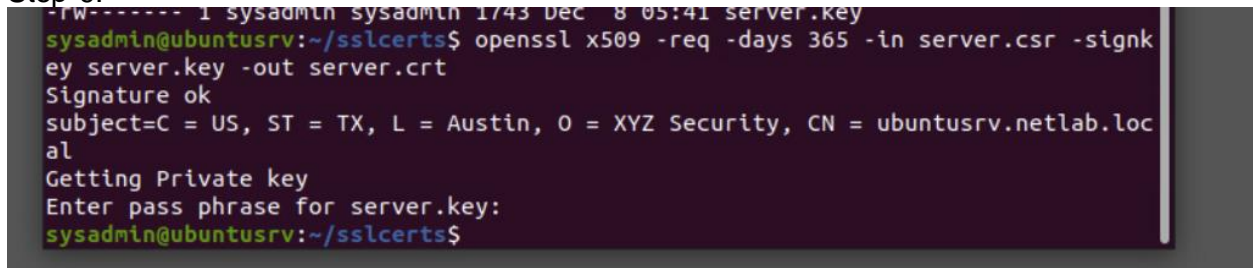
Step 1:

A terminal window titled 'sysadmin@ubuntusrv: ~' with search, menu, and window control icons. The command 'mkdir sslcerts' has been entered and executed, creating a new directory. The prompt is now 'sysadmin@ubuntusrv:~\$'.

Step 5:

A terminal window showing the execution of 'openssl genrsa -des3 -out server.key'. The output indicates a 2048-bit RSA private key is being generated. It prompts for a pass phrase, which is entered and verified. The command 'ls -l' is then run, showing the newly created 'server.key' file. The prompt is 'sysadmin@ubuntusrv:~/sslcerts\$'.

Step 9:

A terminal window showing the execution of 'openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt'. The output shows the signature is OK and the certificate is being generated. It prompts for a pass phrase for the private key. The command 'ls -l' is then run, showing the newly created 'server.crt' file. The prompt is 'sysadmin@ubuntusrv:~/sslcerts\$'.

Step 11:

```
sysadmin@ubuntu: ~/sslcerts$ cat /etc/ssl/certs/ssl-cert.pem
-----BEGIN CERTIFICATE-----
MIIDBTCCAeGgAwIBAgIQDzUwZDQwMjYwMjYwMjYwMjYwMjYwMjYwMjYwMjYw
44:ad:8f:0c:99:25:fd:a7:03:2b:5b:fc:5c:11:30:
6c:a9:e0:4a:99:e3:db:fb:e7:11:e5:a6:60:b0:2d:
f3:8c:ad:11:48:7b:3d:51:a4:95:b6:32:5a:48:d5:
4c:55:8a:9e:67:69:f5:88:d0:22:06:dd:04:4a:9c:
37:52:90:ef:be:f9:56:9d:71:52:d7:b6:e8:f0:da:
cf:15
-----END CERTIFICATE-----
Exponent: 65537 (0x10001)
Signature Algorithm: sha256WithRSAEncryption
0b:77:43:b3:72:08:62:2e:c1:6b:f5:c8:f9:ad:7e:73:02:40:
23:d8:3b:f1:c9:7f:aa:35:5d:6b:d4:56:8a:ce:d8:90:8b:f0:
3c:1b:2e:e0:59:4f:b1:d4:b1:86:9d:18:ff:da:6c:83:36:84:
2e:ba:56:54:0c:ee:54:4f:1b:c2:df:81:7a:98:0e:f7:b0:d0:
90:88:3a:a4:0d:d4:e1:48:46:ab:b7:f3:55:f6:62:bb:9b:e3:
94:12:ac:51:83:54:ef:2a:06:de:f7:1e:ab:0a:6c:a8:4c:a8:
ac:6e:44:69:4e:5b:15:d1:a2:eb:bd:ec:3a:3b:85:aa:78:59:
4b:5c:e9:16:e4:a6:3d:a3:31:b3:b9:cf:dc:b2:72:e1:dd:9a:
e0:3d:16:28:9b:40:ad:a1:d5:91:ce:8b:2d:1e:0d:b0:5d:39:
db:a3:d4:89:22:ed:6f:3c:32:42:26:d4:ea:69:a0:8d:f4:0f:
ee:58:c4:71:18:bc:76:41:dc:2a:3b:b9:b2:02:cc:f5:16:3f:
33:6e:9a:36:95:27:46:8a:7b:5e:d1:26:17:70:4d:44:59:3a:
7b:1b:17:50:db:91:a2:ef:6a:65:f6:e9:df:1c:db:a7:52:b3:
4b:f6:9c:a9:f7:bb:e0:b4:77:1e:6a:b6:68:6c:07:73:63:a2:
33:4e:d3:85
sysadmin@ubuntu: ~/sslcerts$
```

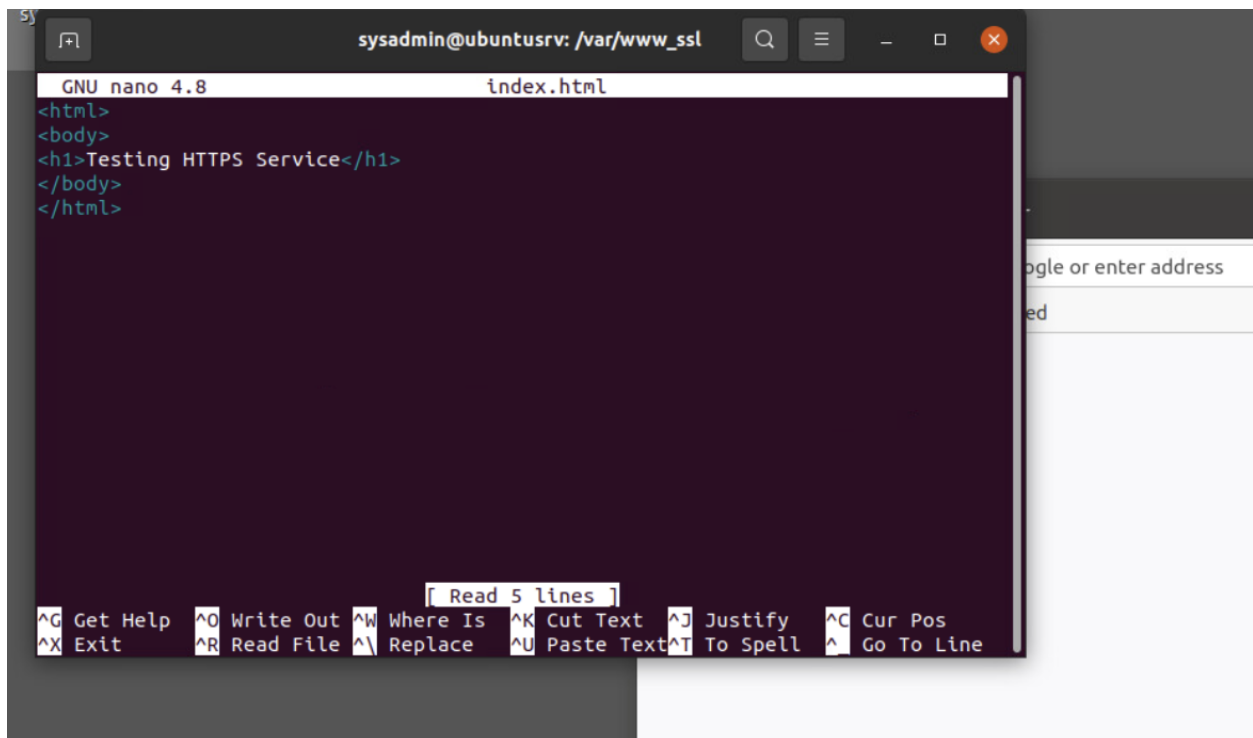
2.2

Step 11:

```
sysadmin@ubuntu: /etc/apache2/ssl_certs$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create s
elf-signed certificates.
To activate the new configuration, you need to run:
systemctl restart apache2
sysadmin@ubuntu: /etc/apache2/ssl_certs$ sudo service apache2 restart
sysadmin@ubuntu: /etc/apache2/ssl_certs$
```

2.3

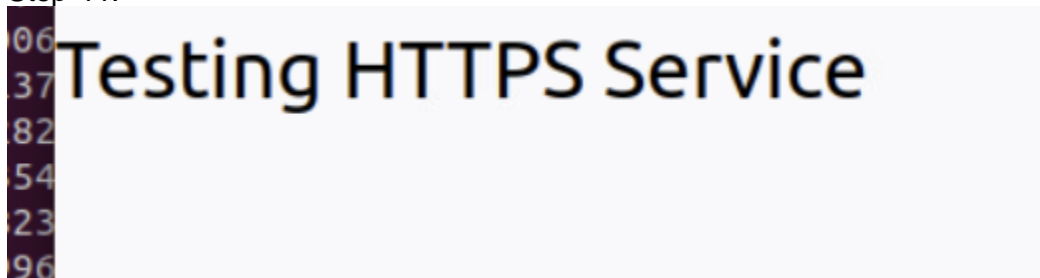
Step 3:



```
sysadmin@ubuntu: /var/www/ssl
GNU nano 4.8 index.html
<html>
<body>
<h1>Testing HTTPS Service</h1>
</body>
</html>

[ Read 5 lines ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line
```

Step 11:



Commentary:

In this lab we looked at proxy servers and implementing secure protocols. I learned that it can be a little complicated making everything go through a proxy server but can give you a lot of control over the packets and the users. I also learned that secure protocols are a great way to increase your security without too much hassle. Knowing this information, companies can use proxy servers and secure protocols to gain more control over the security and also maintain security best practices using the most up-to-date protocols.