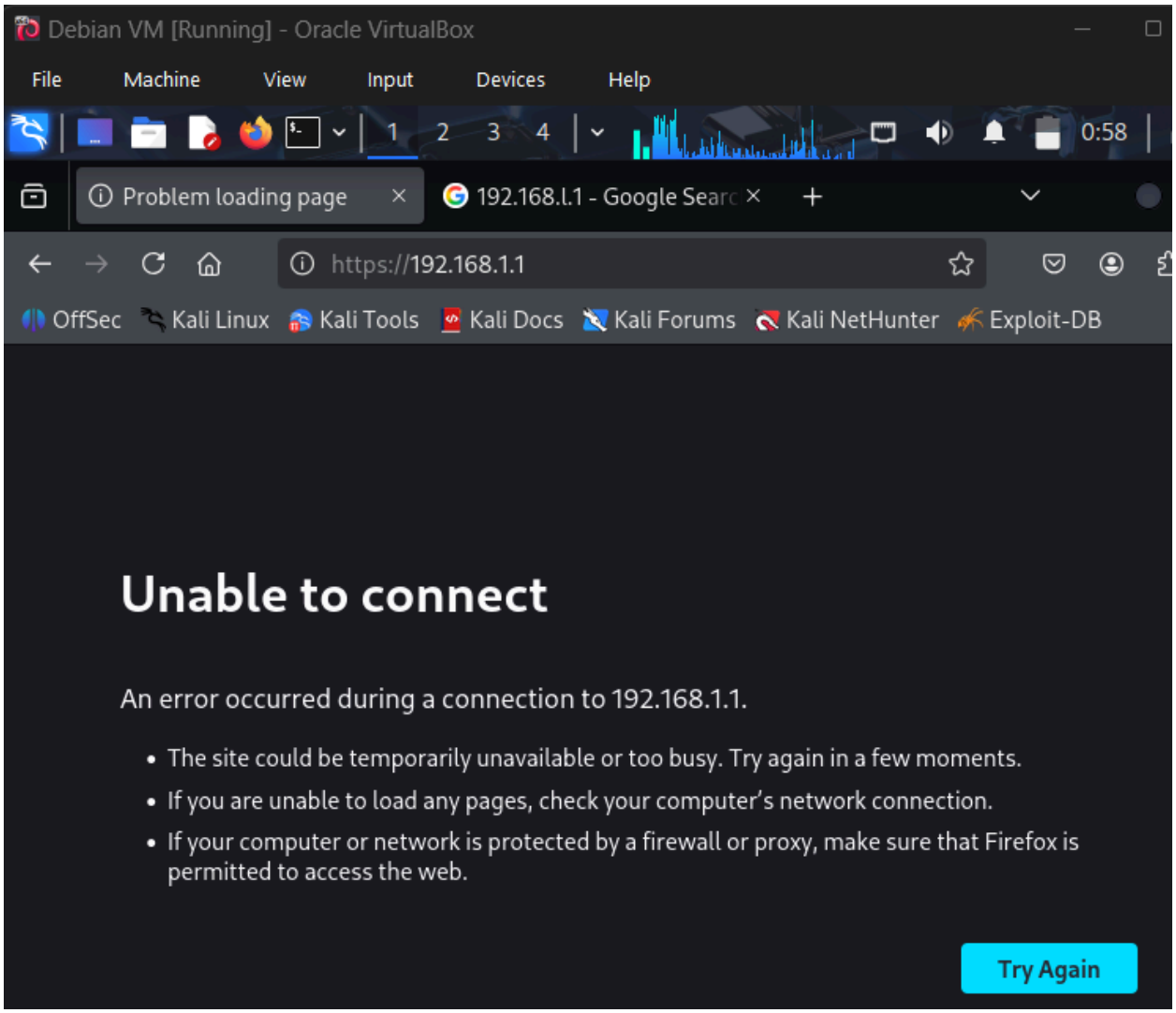
Cristian Carrizales
Lab 4
CS 345
11/13/2025

During the lab I ran into a few problems while trying to execute all the steps required of me. The first of which occurred after opening my client vm named “Debian VM” and trying to access the pFSense GUI. As shown in the photo directly below entering 192.168.1.1 into my browser leaves me unable to connect, this is because my client VM is not on the same virtual network as the pfSense LAN interface. The solution was to swap the client VM network settings to internal network inet-lan(Same as pfsense vm) on adapter 1 and disable NAT(not sure if having NAT enabled it would interfere with the lab) after verifying that I only have adapter 1 enabled I rebooted my client VM and was able to access the pfSense GUI(Deliverable 2).

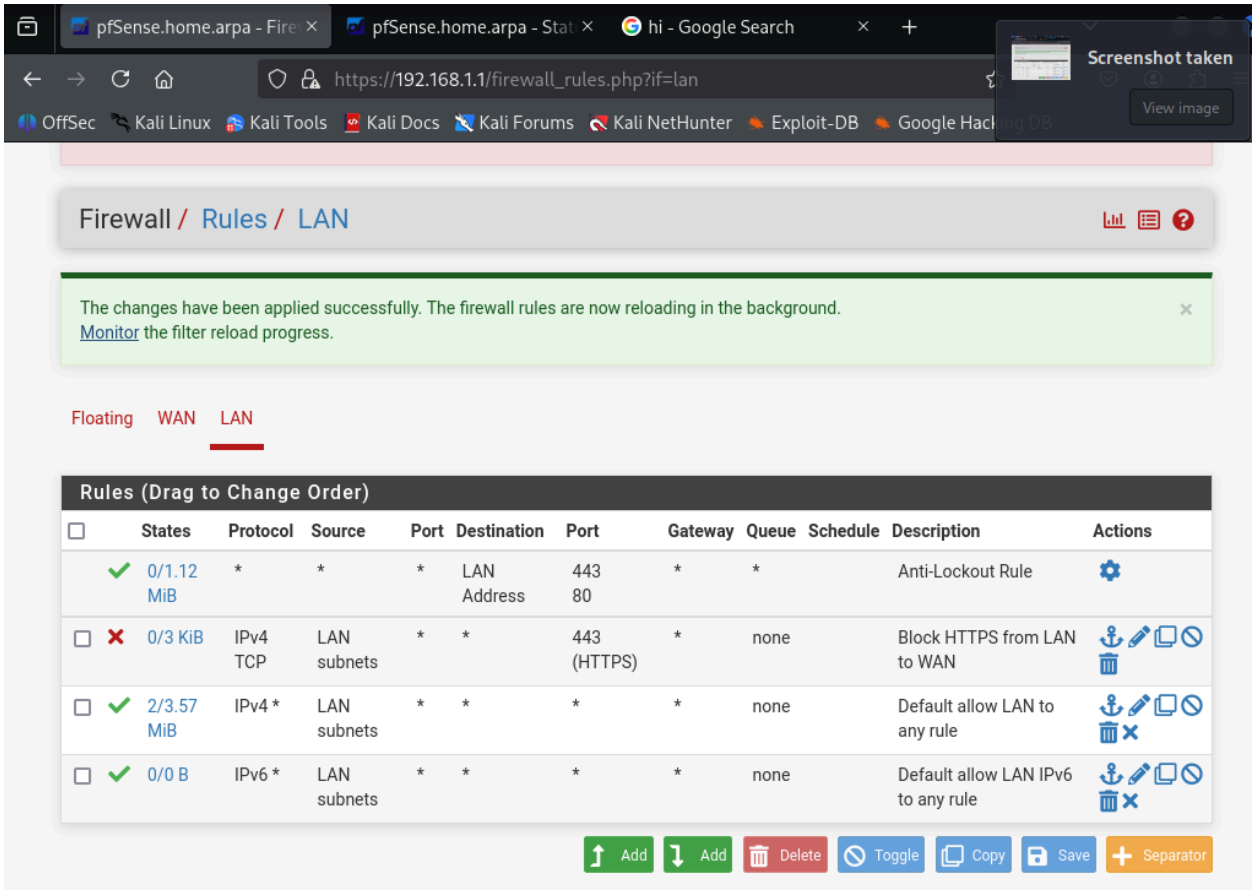


During the configuration of the pfSense firewall rules I ran into a more complex problem with a

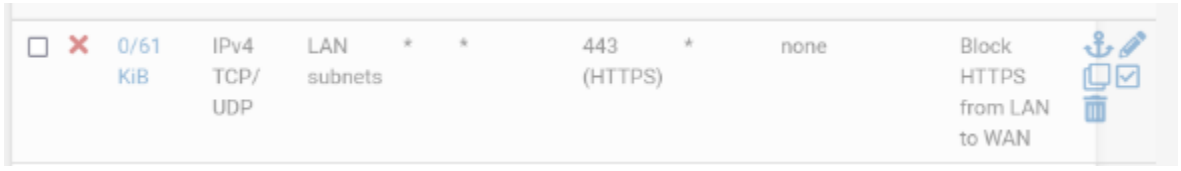
pretty simple solution. The initial step was to create a rule to block HTTPS traffic which was configured to block TCP port on destination port 443. However, after applying the rule https sites like google.com remained accessible(Shown in the photo labeled hi). The first step I took in trouble shooting was to reset the firewalls state table from the pfSense GUI. This was done because I was accessing the web before applying the firewall and perhaps my firewall was still honoring a state from a connection that was established before my block rule was applied. Resetting this did not resolve the issue and I can still access google and my new block rule was not processing any traffic (Showing 0/0 B under states column after reset) My allow rule was still processing HTTPS traffic. Eventually the solution to the problem was to modify the rule I had set(per lab instruction). I had to swap the protocol being blocked from TCP to TCP/UDP on port 443. This was done because a web service like Google uses the QUIC protocol which runs over UDP/443. After applying the new change an attempt to access google.com failed and the block rules counter had increased confirming the block(shown on the photo labeled block). A test to see if the block was only done to https and not all internet traffic so an http website was attempted to be reached and it was, successfully (Deliverable 5.) Afterwards one final verification step was done to confirm that it was the rule I added that was one blocking google from being accessed. I disabled the firewall (deliverable 6) and afterwards I attempted to reach the website which was successful(Deliverable 7) confirming that my rule was responsible for controlling traffic.

Note* I did try to briefly test another search engine like bing before swapping tcp to tcp/udp and was still able to access the website for the most part but some areas were not functioning properly on the sure

Hi(Can see I was able to search for hi on google in the tabs)



Block



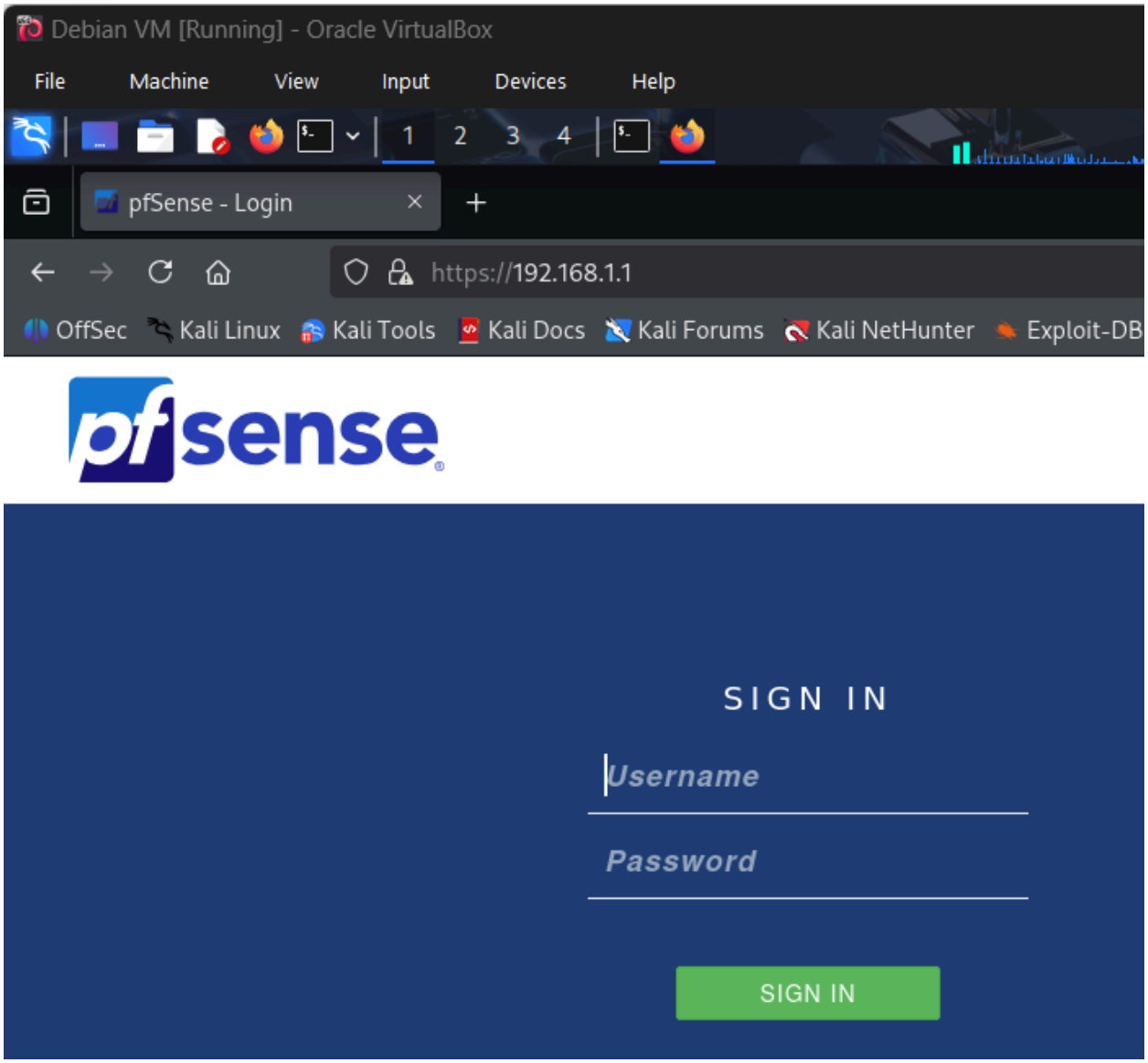
Deliverable 1 pfSense VM

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: c0f6b019fb7a026b57c2

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 10.0.2.15/24
                                  v6/DHCP6: fd17:625c:f037:2:a00:27ff:fe51:d7f5/
64
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

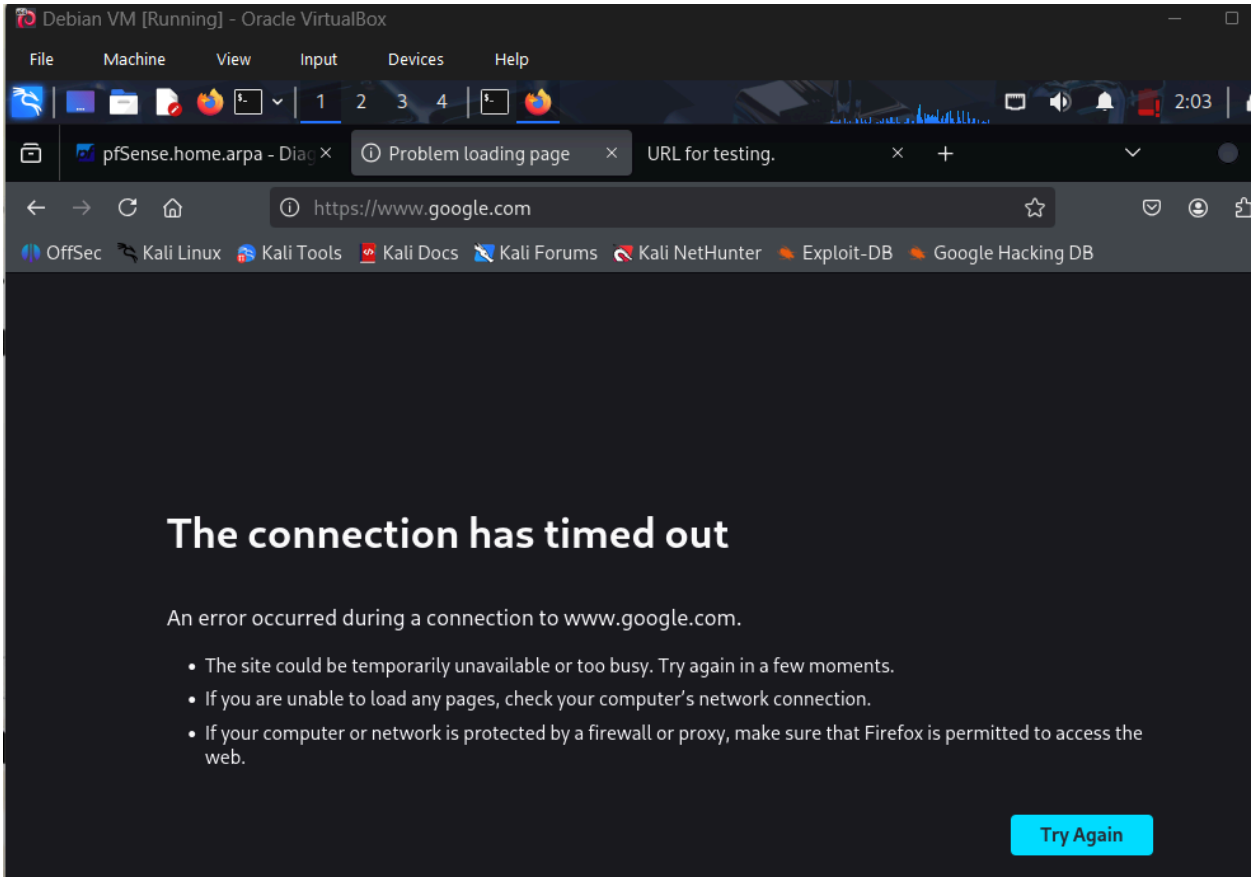
Deliverable 2 Ip from client vm

```
File  Actions  Edit  View  Help
┌──(cristian㉿kali)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:a4:b2:5c brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic noprefixrout
e eth0
       valid_lft 7130sec preferred_lft 7130sec
    inet6 fe80::a00:27ff:fea4:b25c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

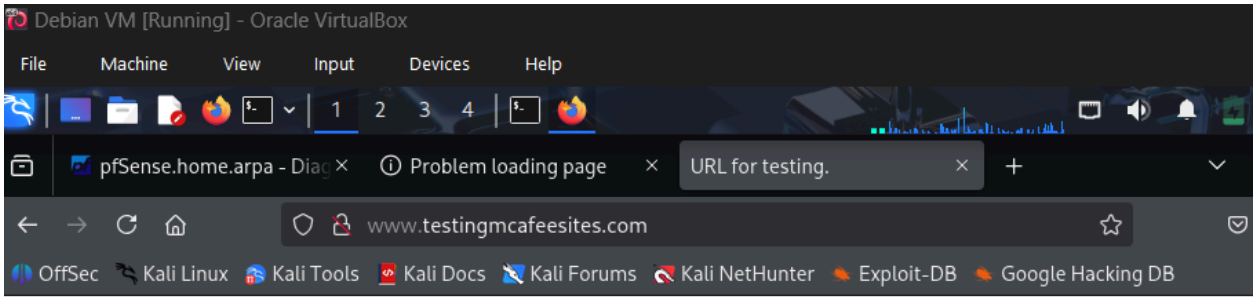
Deliverable 3 psSense GUI successfully accessed


Debian VM [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
1
2
3
4
pfSense - Login
https://192.168.1.1
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
pfsense
SIGN IN
Username
Password
SIGN IN

Deliverable 4 Blocked google successfully



Deliverable 5 Showing that I can access an HTTP website still



http://www.testingmcafeesites.com/index.html

This is an index url which gives an overview of the different test urls available.

http://www.testingmcafeesites.com/testcat_ac.html
-This is an example URL which should be categorized as an art/culture website with a minimal risk reputation score.

http://www.testingmcafeesites.com/testcat_al.html
-This is an example URL which should be categorized as an alcohol website with a low risk reputation score.

http://www.testingmcafeesites.com/testcat_an.html
-This is an example URL which should be categorized as an anonymizer website with a low risk reputation score.

http://www.testingmcafeesites.com/testcat_au.html
-This is an example URL which should be categorized as an Anonymizing Utilities website with a low risk reputation score.

http://www.testingmcafeesites.com/testcat_be.html
-This is an example URL which should be categorized as Browser Exploits website with a low risk reputation score.

http://www.testingmcafeesites.com/testcat_bl.html
-This is an example URL which should be categorized as a Blogs/Wiki website with a low risk reputation score.

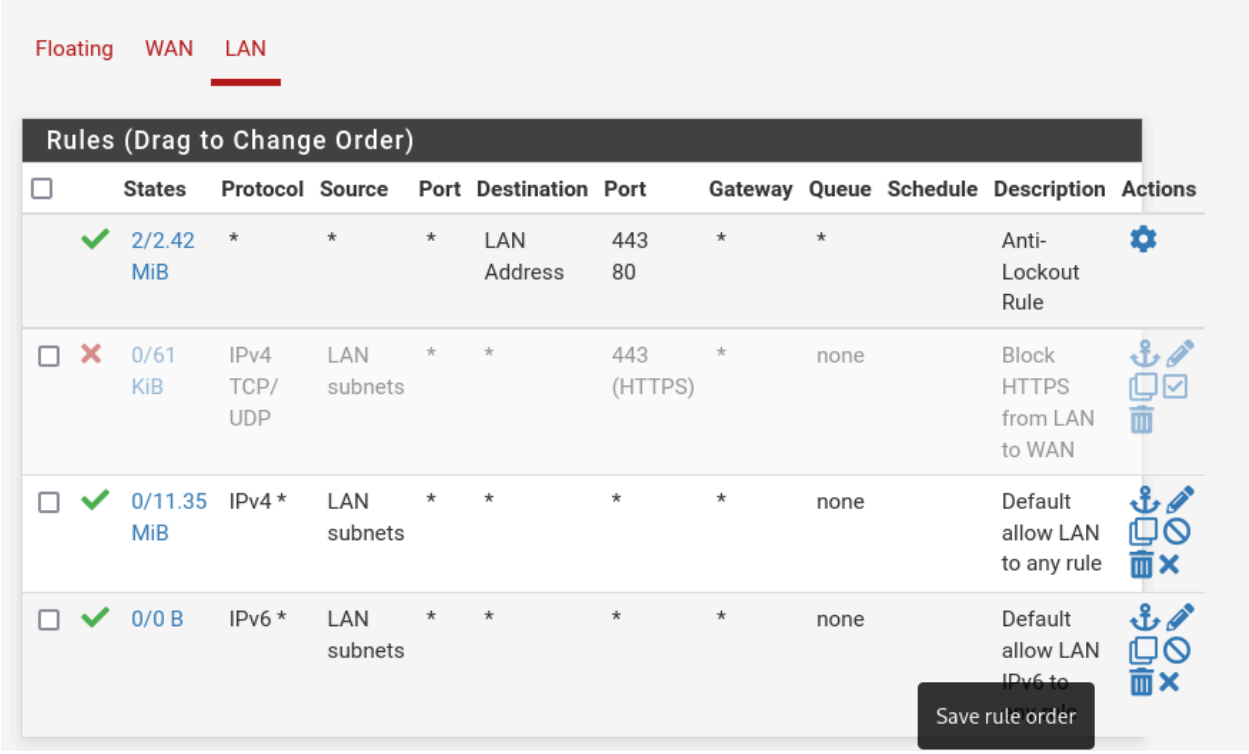
http://www.testingmcafeesites.com/testcat_bu.html
-This is an example URL which should be categorized as a Business website with a low risk reputation score.

http://www.testingmcafeesites.com/testcat_ch.html
-This is an example URL which should be categorized as a Chat website with a low risk reputation score.

http://www.testingmcafeesites.com/testcat_cm.html
-This is an example URL which should be categorized as a Public Information website with a low risk reputation score.

http://www.testingmcafeesites.com/testcat_co.html
-This is an example URL which should be categorized as a Controversial Opinions website with a low risk reputation score.

Deliverable 6 Disabling the Rule(Grayed)



Deliverable 7 Accessing google after disabling the rule to block