Seth Ayers

04/24/2018

IT 430

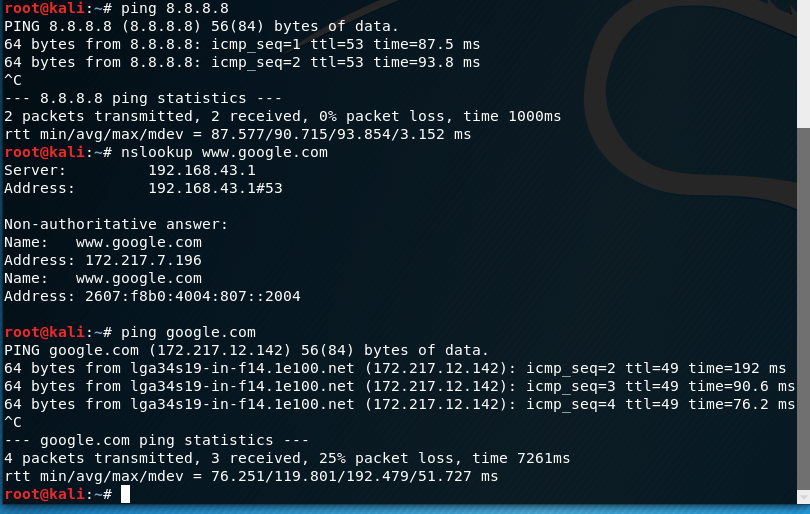
Lab 9

SAyers\_lab09.docx

**Lab 9: Firewall Management Using pfSense**

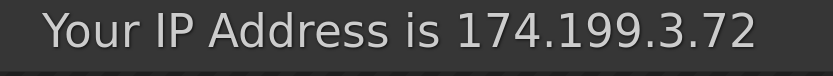
|  |  |
| --- | --- |
| VM Interface | IP Address |
| pfSense WAN | 192.168.43.178 |
| pfSense LAN | 192.168.64.1 |
| WIN 7 LAN | 192.168.64.9 |
| WINXP LAN | 192.168.64.8 |
| WIN SERVER LAN | 192.168.64.10 |

*IP addresses of individual VM’s*

  
*Kali VM ping tests*

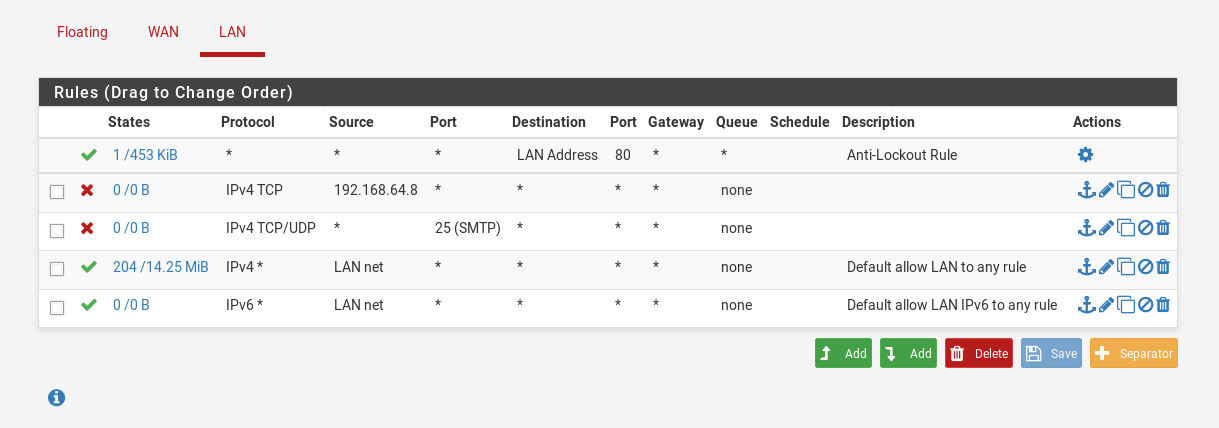


*WIN7 VM ping test*

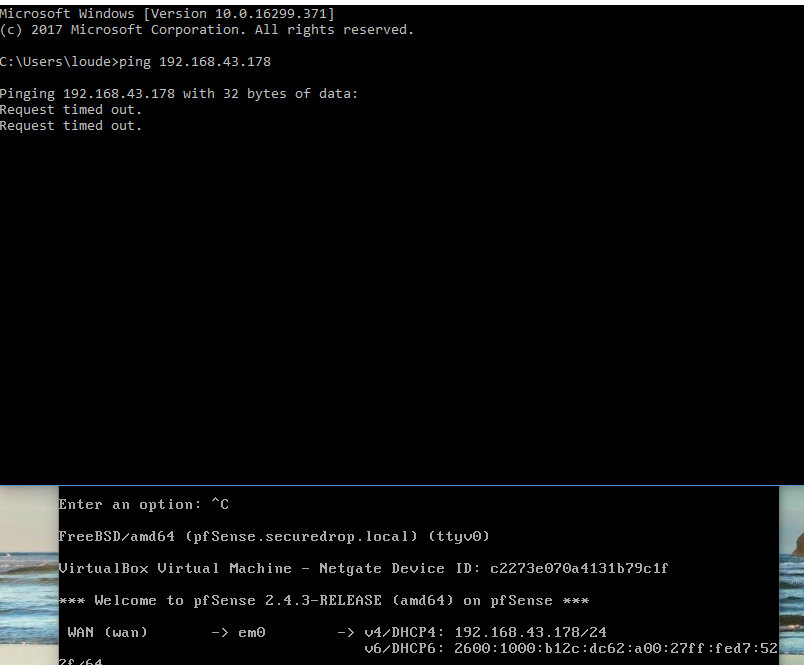


**Question 1: What IP address did you get? Explain why you see the address above.**

The address that was read on the whatsmyip site is different than any of my currently running VM’s. For instance, the site was accessed from my Kali VM’s, which is 192.168.64.7. Because this is a private network, with private network IPv4 addresses, the IP belongs to the device that is outward facing to the internet. In this case, it’s my tether enabled cell phone.

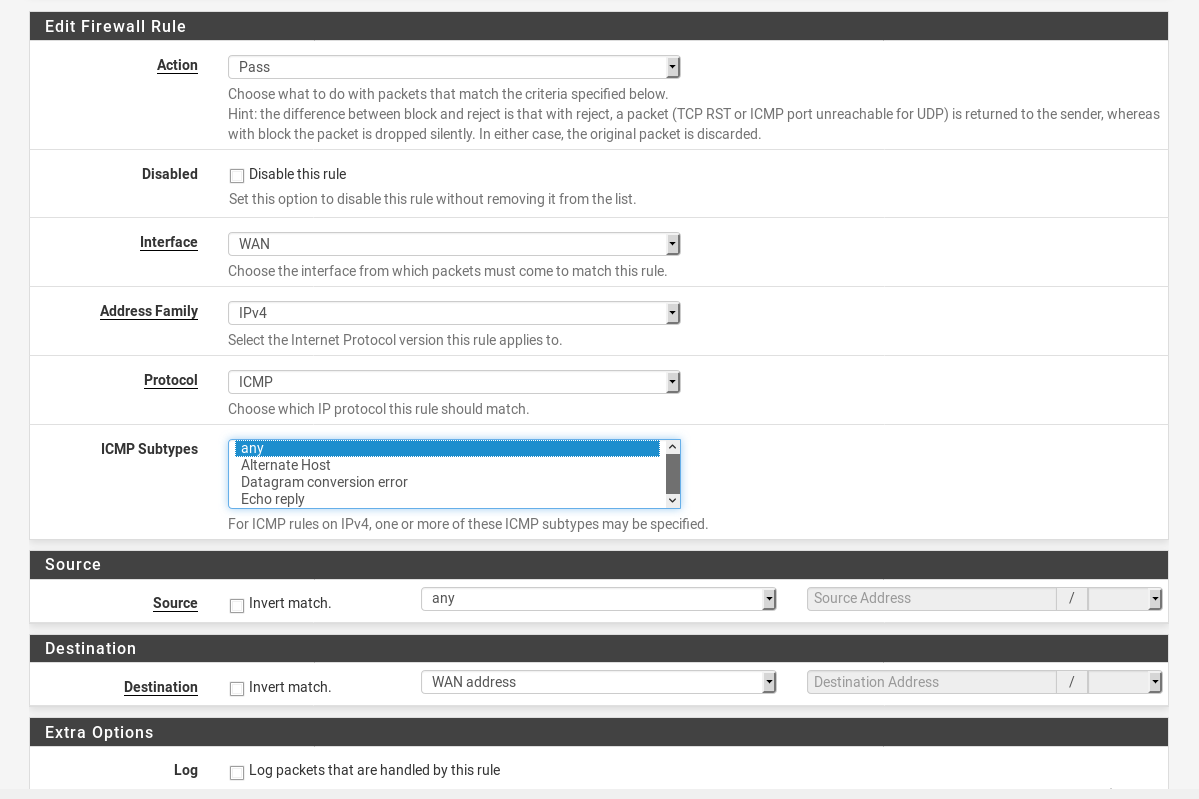


*WINXP and SMTP block rules on pfSense GUI*

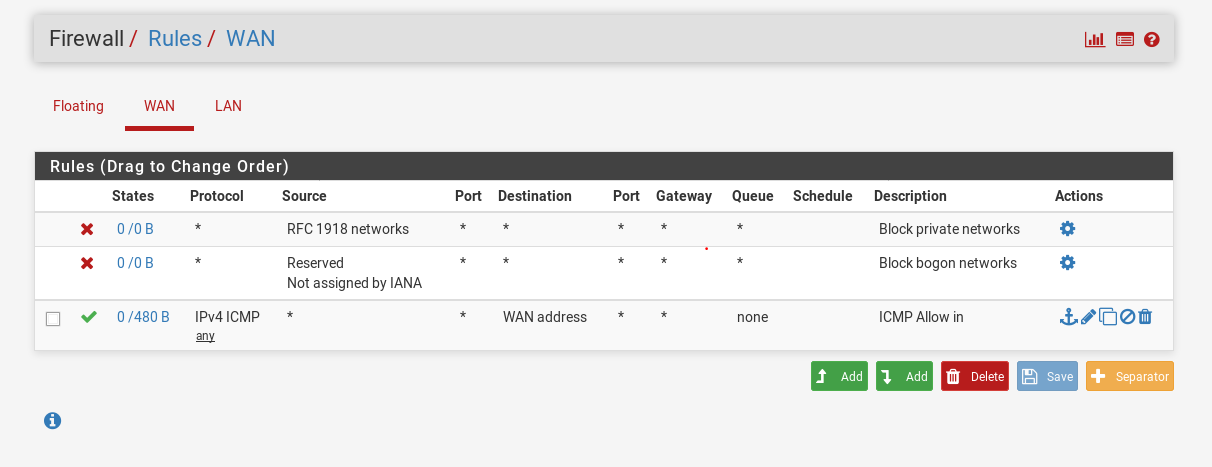


**Question 2: Did the ping succeed? Why didn’t the ping work?**

The ping failed due to the ping request originating from a private network IP, IE my laptop. Furthermore, the IP hasn’t been assigned via IANA and therefor a bogon IP. The pfSense default WAN firewall rules prevent all incoming private network and bogon requests.



*Rule edit page for the new WAN rule, enabling pings*



**Question 3: Did the ping work?**

The ping wouldn’t work with this current setup. The issue is that the top two rules, which are a part of our WAN interface, are configured to stop private network/bogon pings. Although the rule is included to access the pings, the rule is located at the bottom on the ruleset. In other words, the ping request is dropped by the top rules before it is accepted by the created pass rule. This can be worked around by disabling the setting in the interface, thus removing the block rules, placing our pass rule to the top of the ruleset. I did this and was able to ping the WAN IP. (I reverted the settings back to keep on track with the lab)

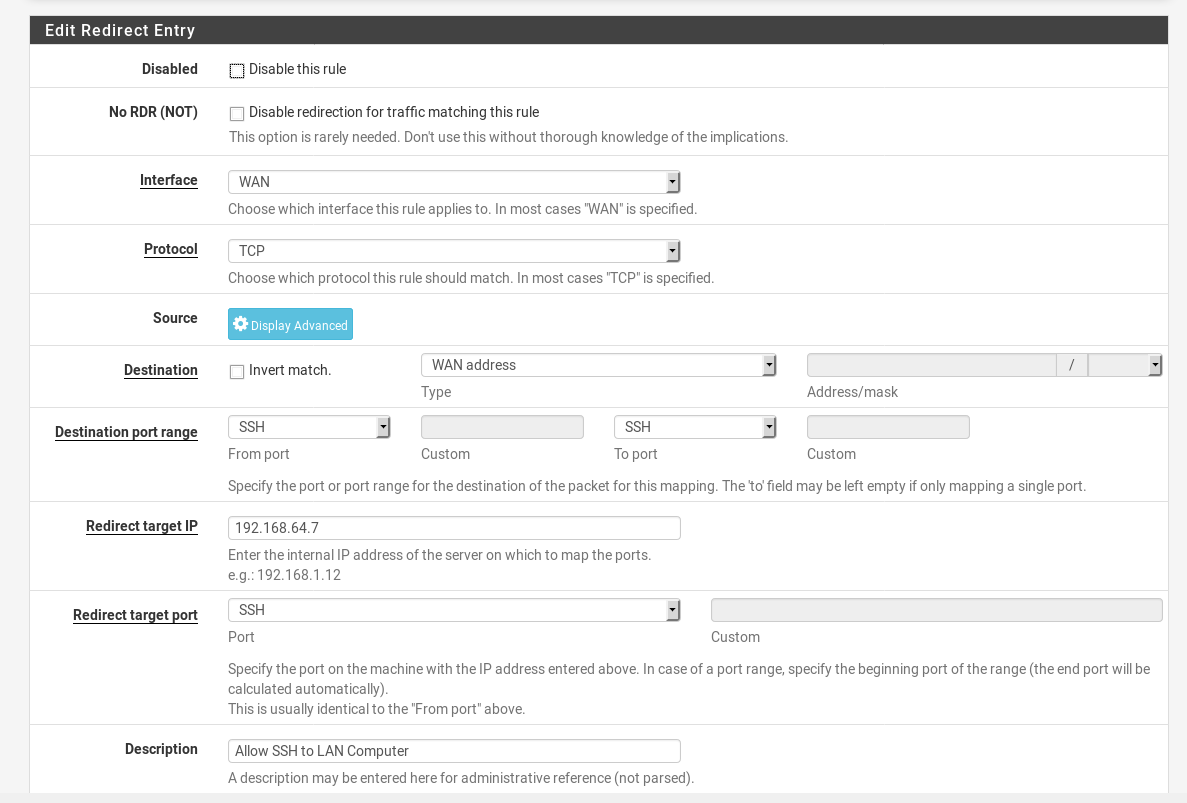


**Question 4: What IP address is the “sshd” daemon bound to? Why does it not match the LAN IP address?**

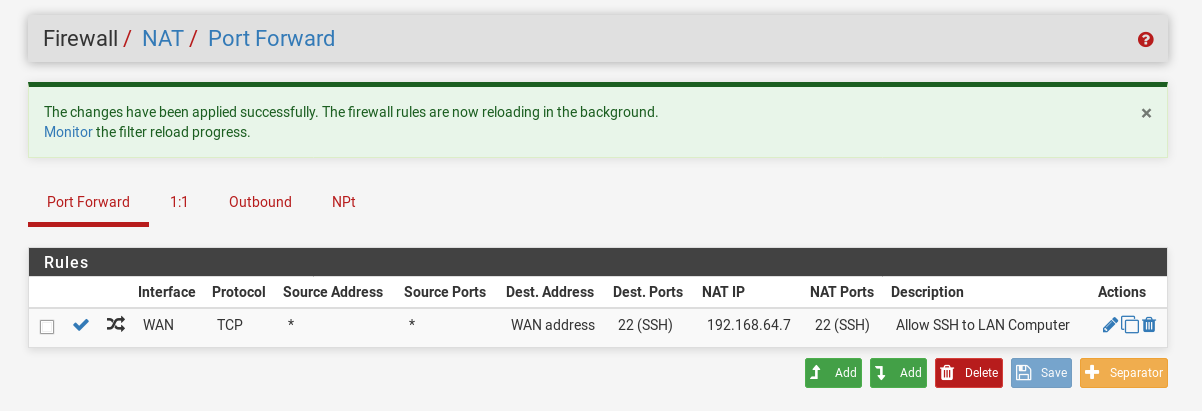
The SSH daemon is bound to the default address of 0.0.0.0. This allows the daemon to listen on all configured network interfaces on the network.



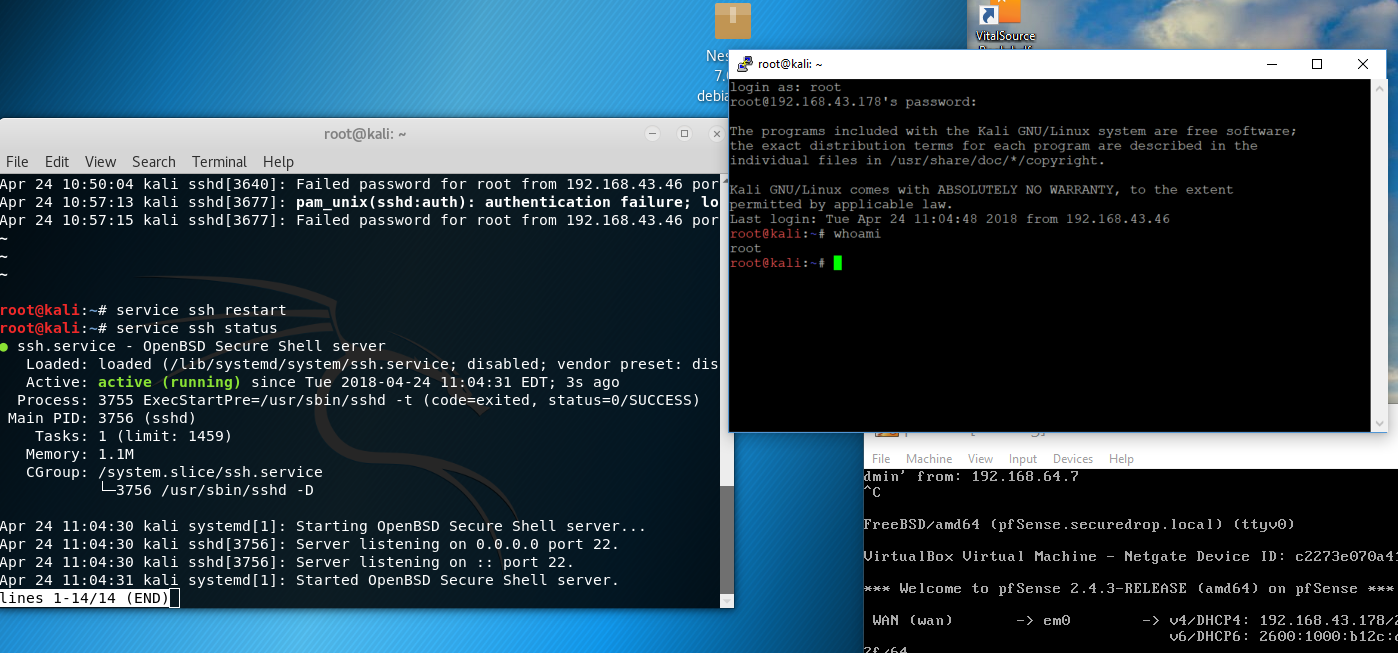
Verifying that the SSH daemon is active and running



*Configuring the NAT/PORT FORWARDING settings in pfSense*

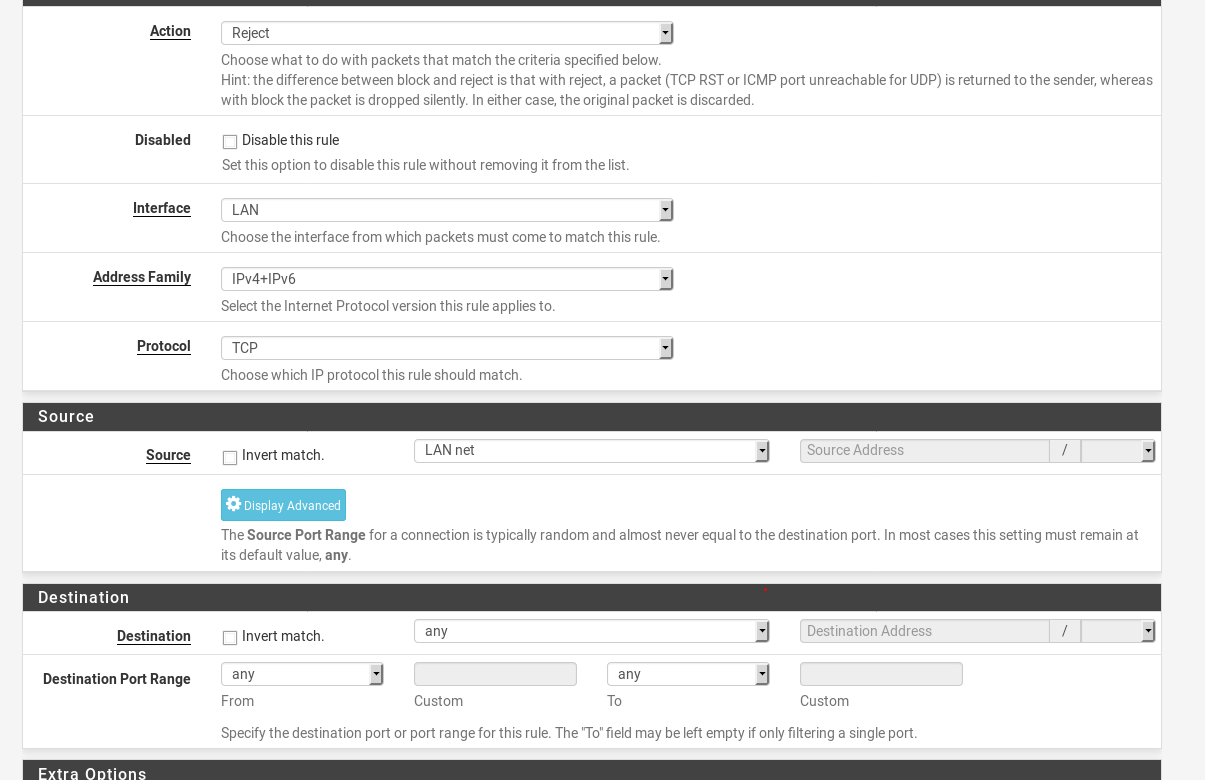


*Rule table depicting the configured rule*

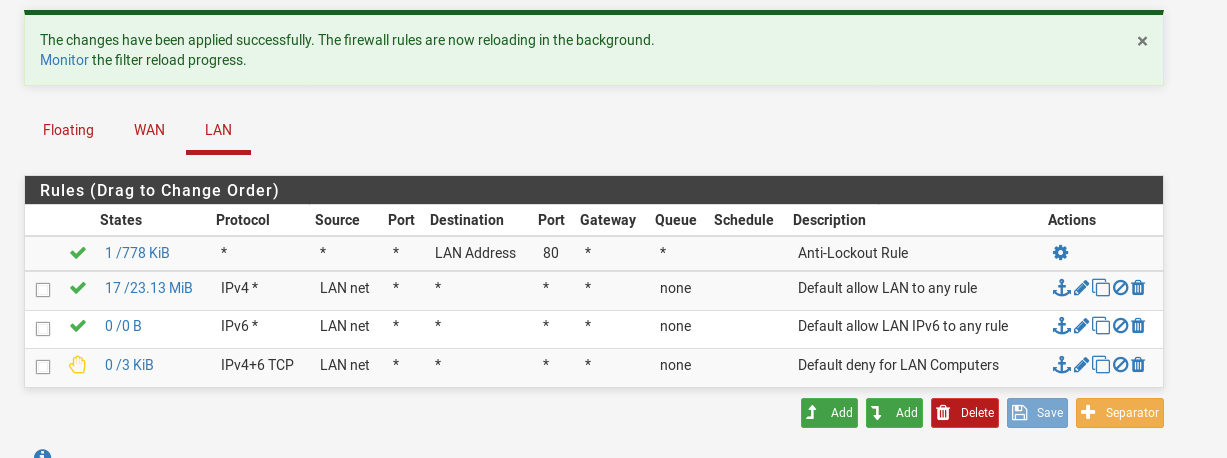


*SSH connection, forwarded by the pfSense firewall, directed to the Kali VM.*

*(Some modification had to be made in the /etc/ssh/sshd\_conifg/ file to make this work)*



*Setting page for default-deny firewall rule*



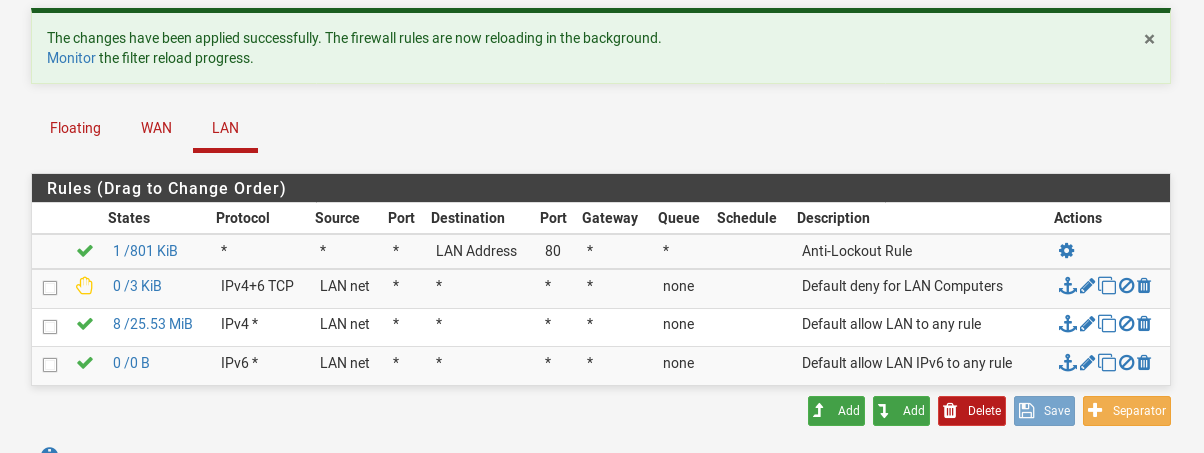
*New deny rule added to the LAN rule table*

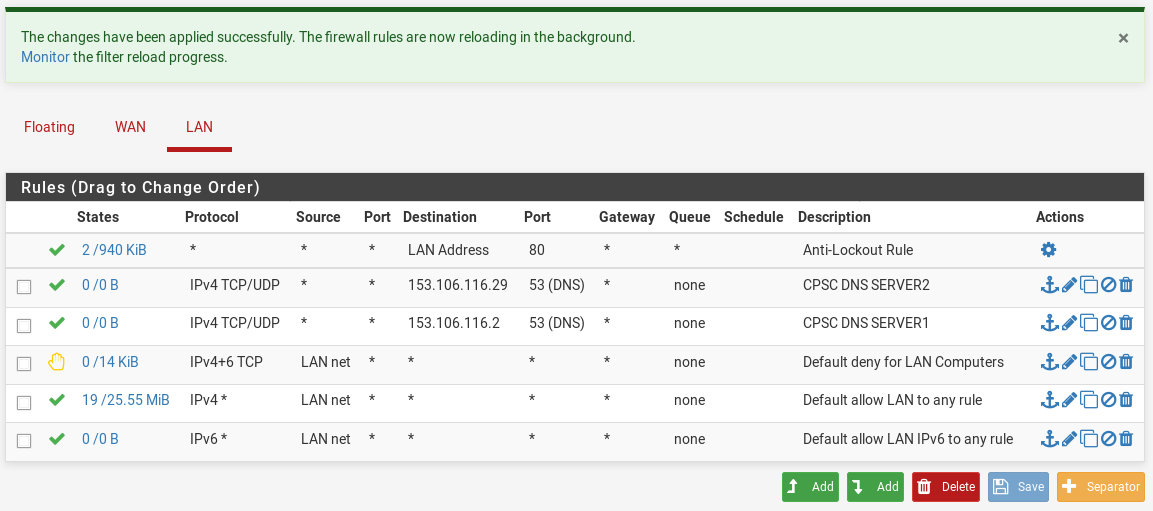
**Question 5: Did your LAN firewall rule work? Why, why not?**

The firewall rule did not work. As shown above, the rule is set at a position lower than the rules that permit traffic. One a transmission meets the parameters of a rule; the firewall accepts the traffic. So, the new deny firewall rule wasn’t checked.

**Question 6: What do you need to do to fix this?**

The new deny rule must be at the top of the firewall list, above the two allow rules, to take effect. I.E.:





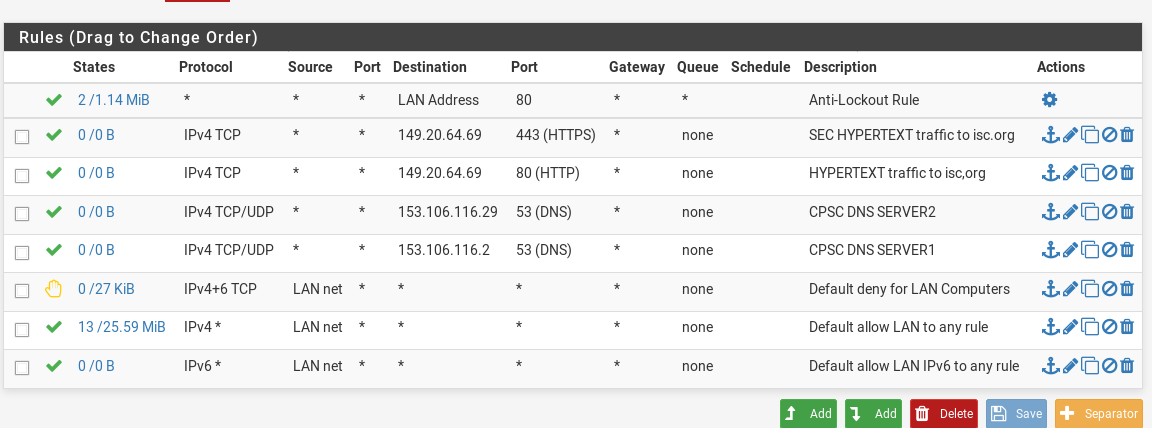
*New firewall rules for DNS server traffic*

**Question 7: Describe the rule(s) you added, including the protocol and port you used?**

Firstly, I added two rules to accommodate the requirements of handling DNS queries, one for each specific server. For each, I wanted TCP and UDP to be active protocols since, despite the fact DNS (port 53) normally uses UPD for requests, TCP can also be used if a response is not given from the DNS server using UDP.

**Question 8: What addresses are used by** [**www.isc.org**](http://www.isc.org)**?**

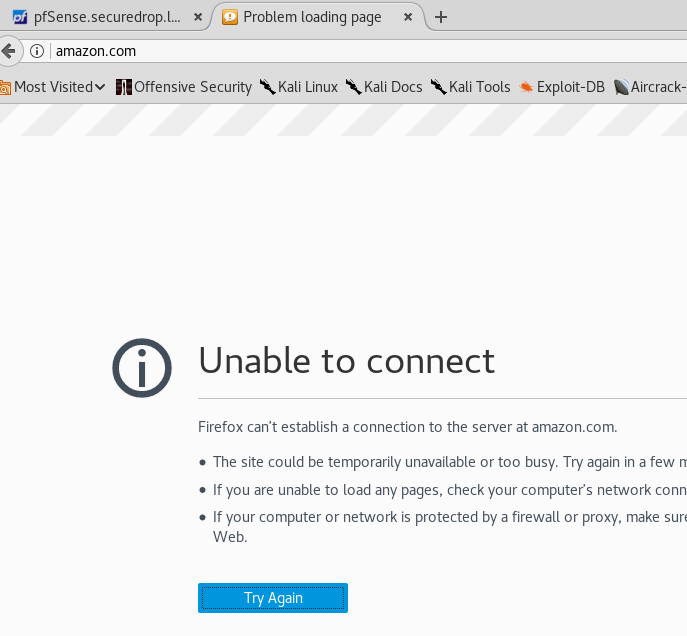
Per nslookup and netcraft, isc.org uses the IP address of 149.20.64.69.



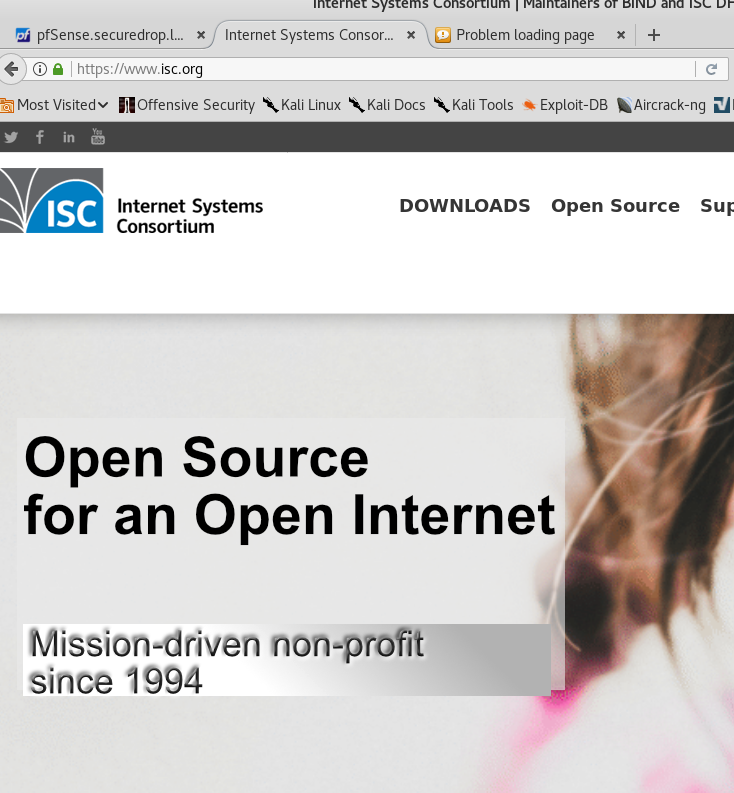
*Rules to allow HTTP(80)/HTTPS(443) traffic to isc.org*

**Question 9: Describe the rules you added, in detail.**

Due to having to accept traffic from two protocols, HTTP(80)/HTTPS(443), I made two rules to allow web requests from LAN sources to isc.org. The basic rule settings apply: allow(pass), IPv4, TCP, singlehost/ailias, description.



*Denied traffic to access amazon.com by current firewall rules*



*Approved HTTP/HTTPS traffic to the isc.org site! The firewall is a success!*