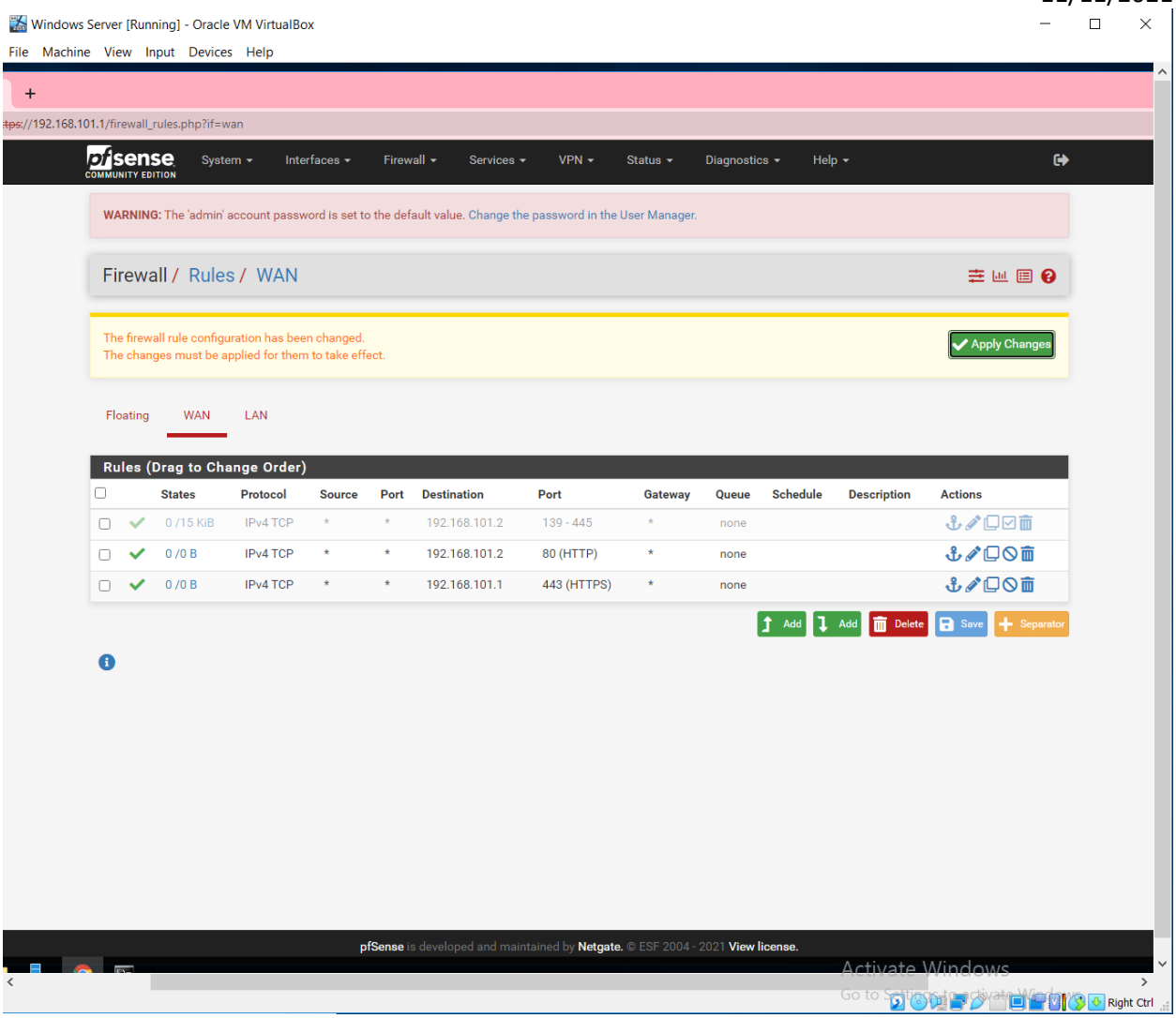
Joshua Lane
IT419
11/11/2021

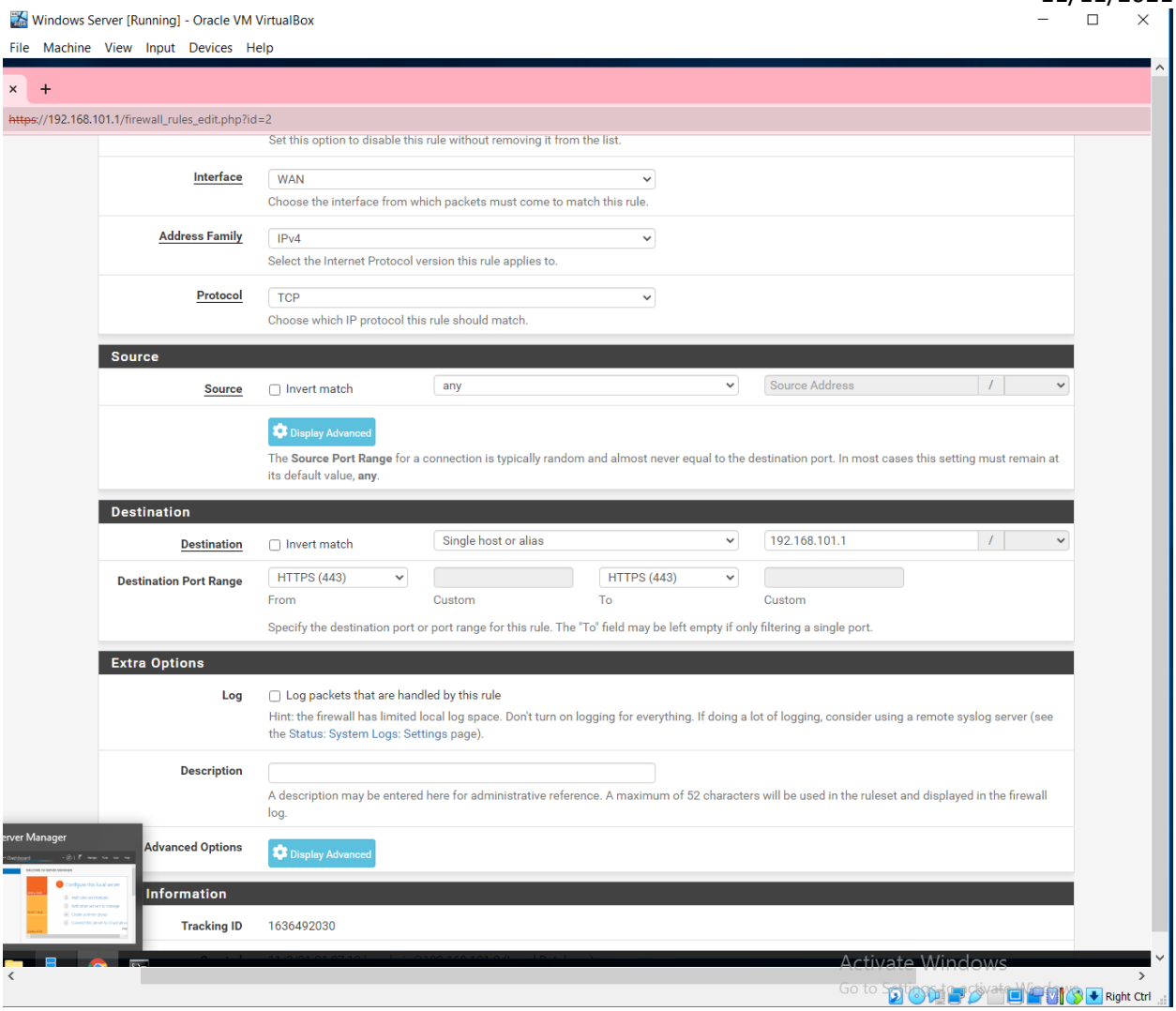
Use and Usefulness of Firewall Rules

Firewalls have more than just the purpose of keeping the bad guys out, they also keep legitimate users from deviating from their responsibilities. With the human layer being the weakest one, certain rules should be implemented to keep users from visiting risky sites/sites that have nothing to do with work or the use of that specific network. For instance, if you want clients outside your network to have access to your web server but deny access to other things such as file sharing and pinging; add rules to pfsense (your firewall) through the Graphic User Interface.

From the internal network (in our case from the Windows Web Server 2016), access your pfsense and log into the admin account via Chrome or some other browser. The goal is to use firewall rules in pfsense to limit access from the outside first, so we address the WAN (Wide Area Network) interface of the firewall rules. In the screenshot on the next page, I disabled a rule that allowed filesharing in the common file sharing ports in Windows (139 to 445) on the WAN interface of pfsense (the firewall). You can make a similar rule but make it a blocking rule and that will achieve the same result. Make sure it is at the top of the list of rules so that it is prioritized. The idea is to minimize privileges to the least amount needed to do the necessary tasks. This further secures the network. Go to Firewalls>Rules>Add rule. The protocol is TCP and applies to “any” client outside the private network, so that is the selection you make. Make sure to click “apply changes” after making each rule.

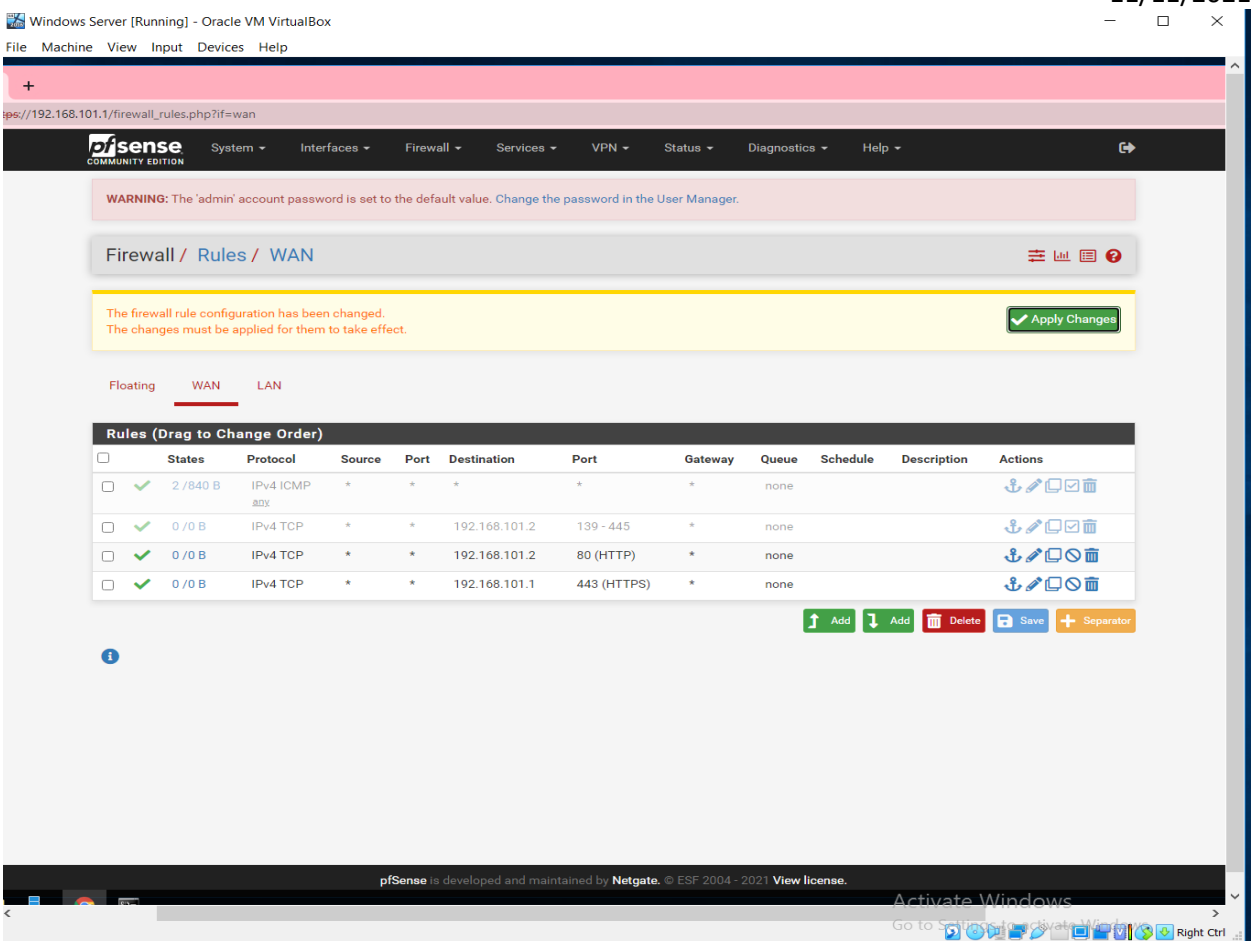
Joshua Lane
IT419
11/11/2021

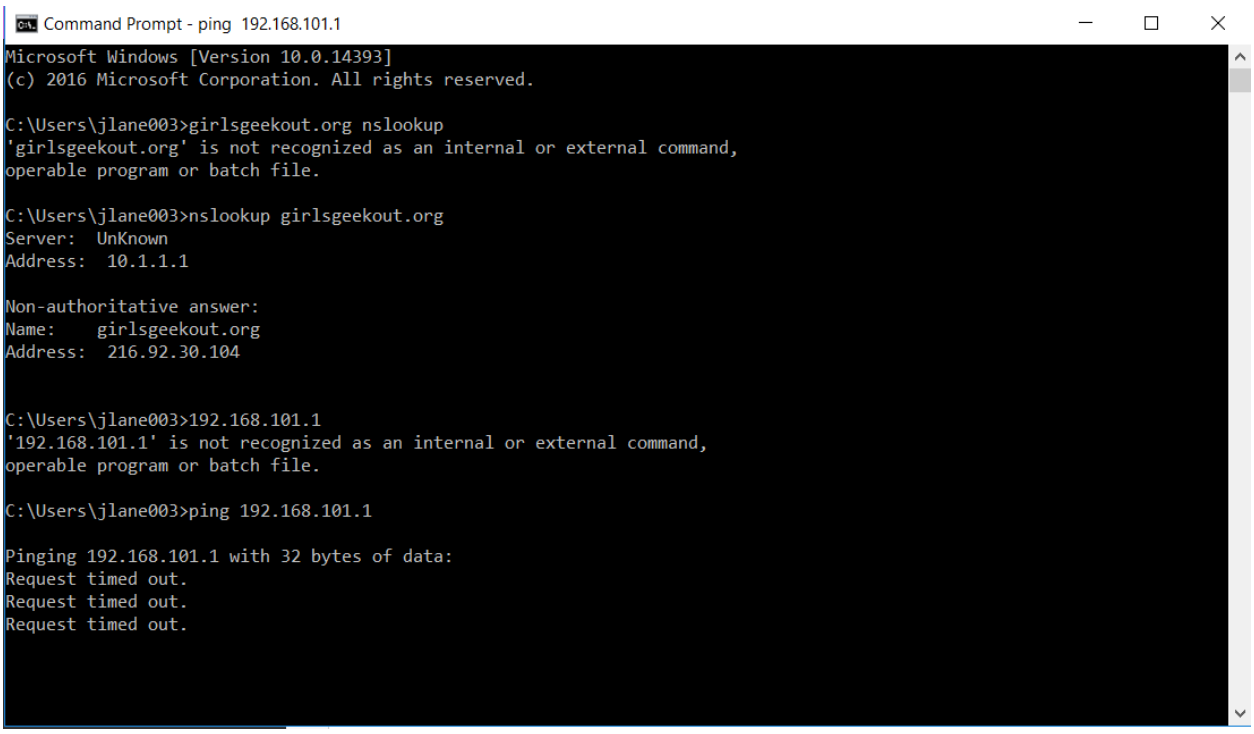




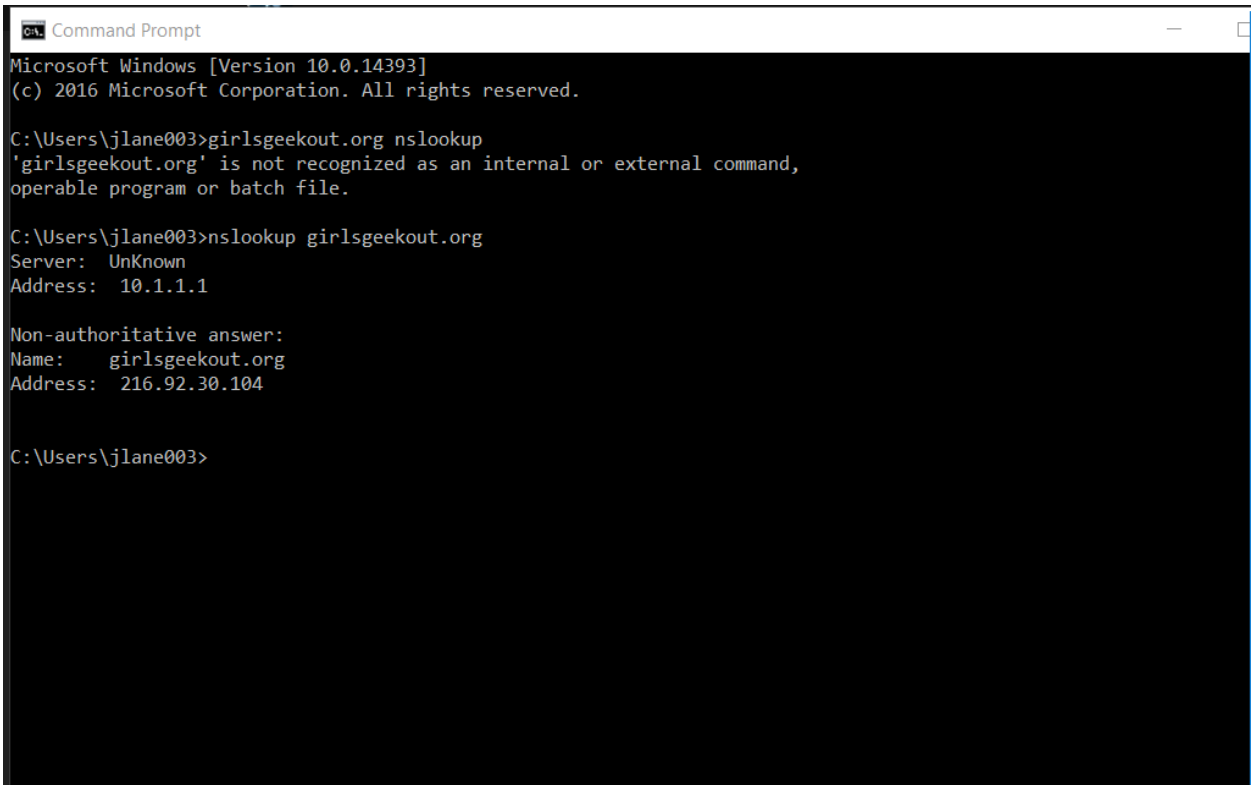
Above we address what clients can have access to. We allow them to access the webserver through port 443 (a common HTTPS port) and we do the same with port 80 (for HTTP). The source will be “any” (as in any client) etc. Another good rule-of-thumb is to disable anything allowing pinging through the firewall. This helps stop unwanted traffic bogging down your network. The protocol to make a rule for blocking this is ICMP. I had a passing rule, so I simply disabled it, and pinging was unsuccessful afterwards. This is shown on the next page in two screenshots.

Joshua Lane
IT419
11/11/2021

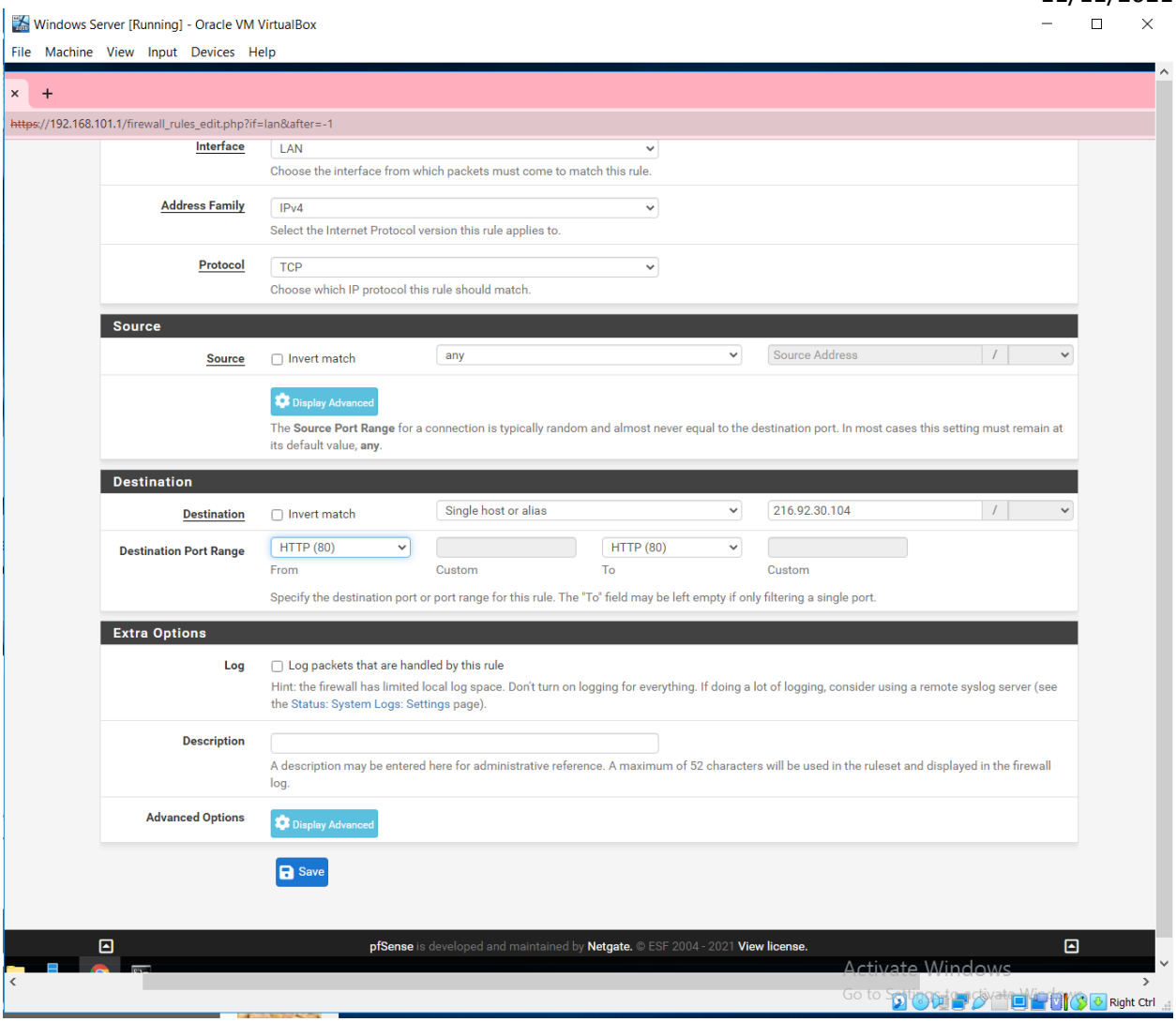




Next, you want to take care of your clients in your private network. You can blacklist (prohibit access to) certain sites, but professionals recommend whitelisting (allowing access to) to save time and effort. There will always be new sites for clients to abuse, access, etc. For this reason, it takes fewer rules to allow access to the necessary websites. For the following example, however, I will simply show how to prohibit access to certain sites/create a loopback feature that keeps clients from misusing the network. Say, for instance, I wanted to block access to girlsgeekout.org. First, I want to find the IP address of the website, I do this by using "nslookup girlsgeekout.org" in a command prompt window as shown below.

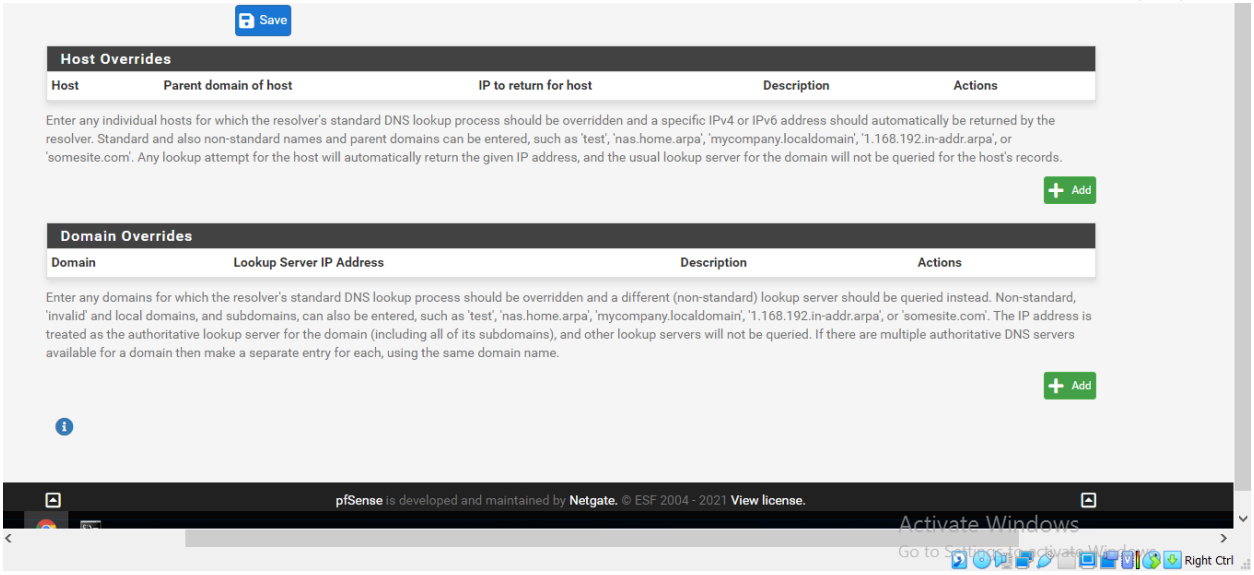


Now we go to the LAN interface of pfsense, and we add a rule blocking that specific IP address (216.92.30.104) as a destination. The source is set to "any", and the port is set to 80 since the website is HTTP. This rule is shown on the next page.

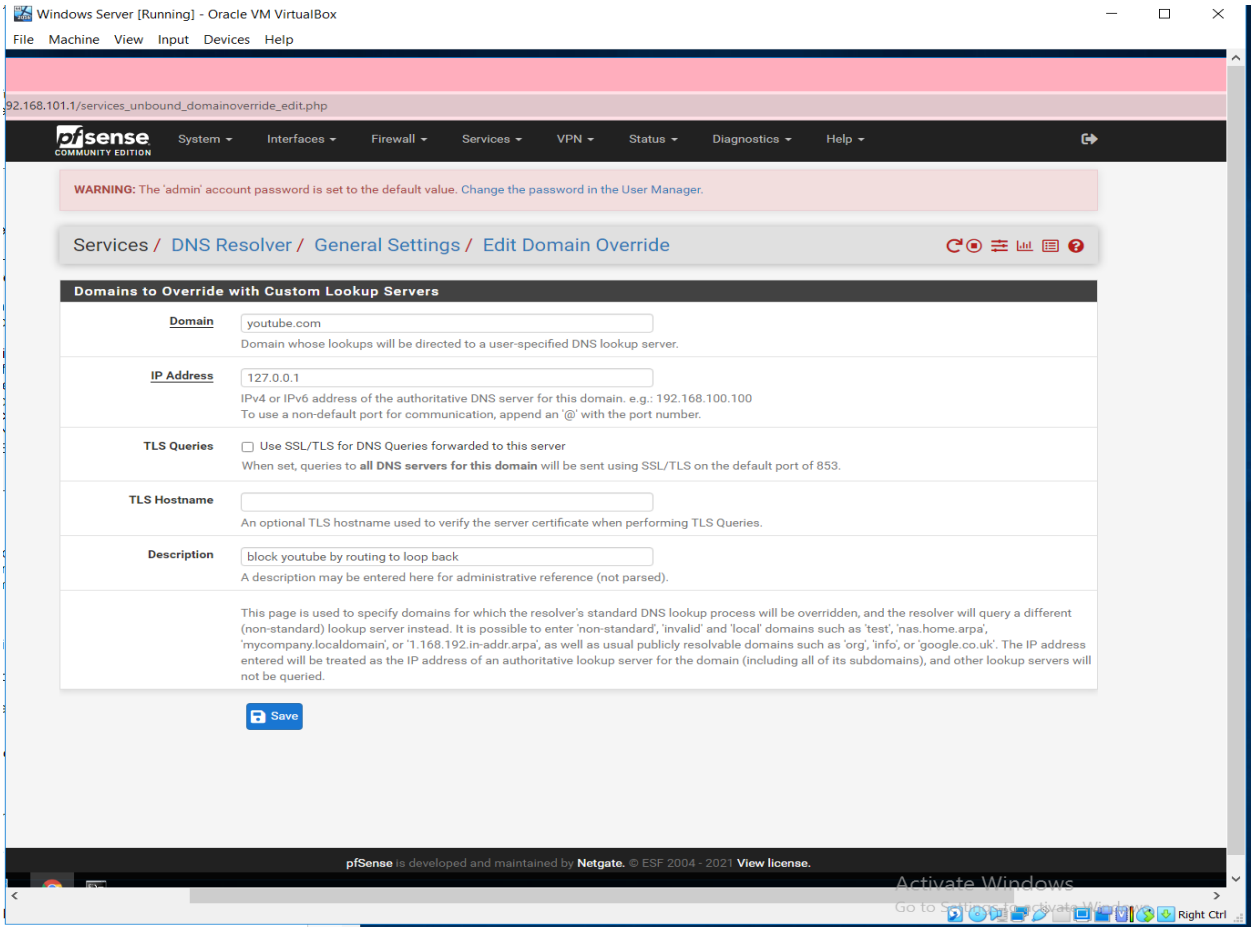


Hit save and apply changes (same as the rest of the rules).

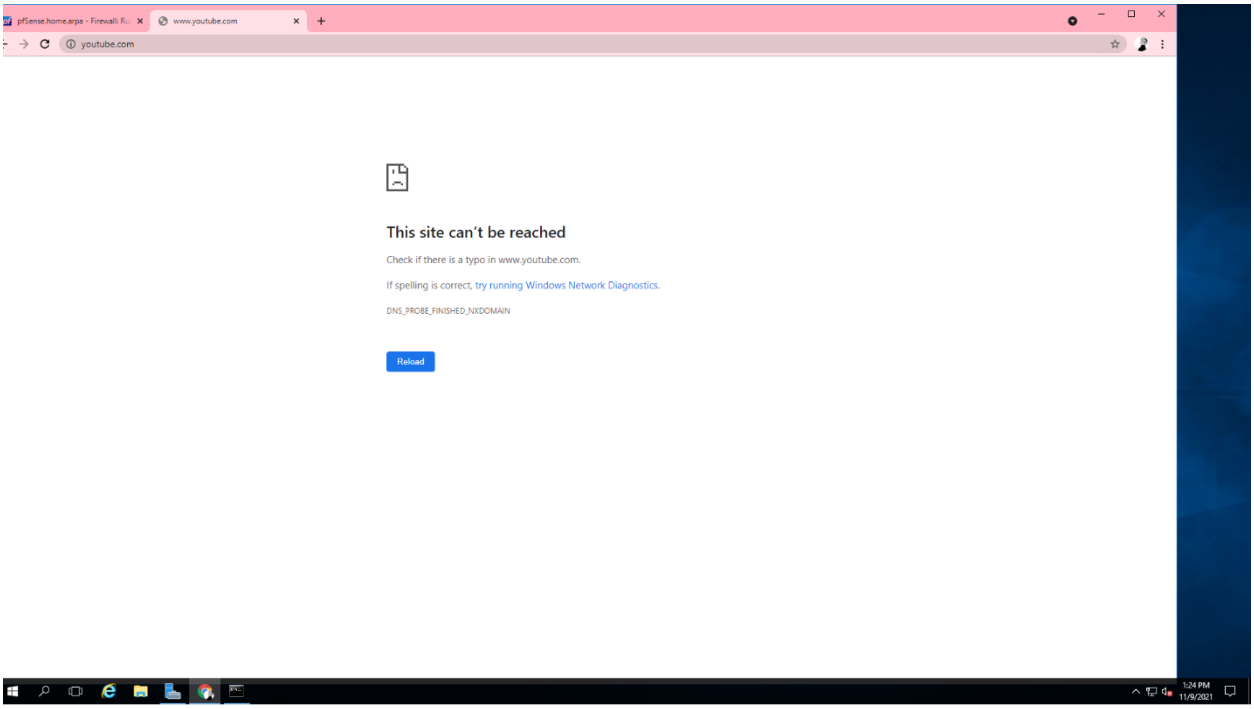
Next, we look at blocking access to a popular site such as youtube.com. Here we want to use the domain override feature to simply show a “This site can’t be reached” message to the client. First, you select “Services” from the pfsense GUI, then select DNS Resolver>General Settings>add domain override. The screenshot on the next page shows the domain override location.



Next, set the domain entry to youtube.com, the IP address to 127.0.0.1, hit save and apply changes. This is shown below.



Once this is implemented, you can test it by trying to access youtube.com from inside the network. This is shown below.



In these ways, you can block access to risky sites or sites you simply do not want your clients accessing. This provides a more productive and safe work environment.