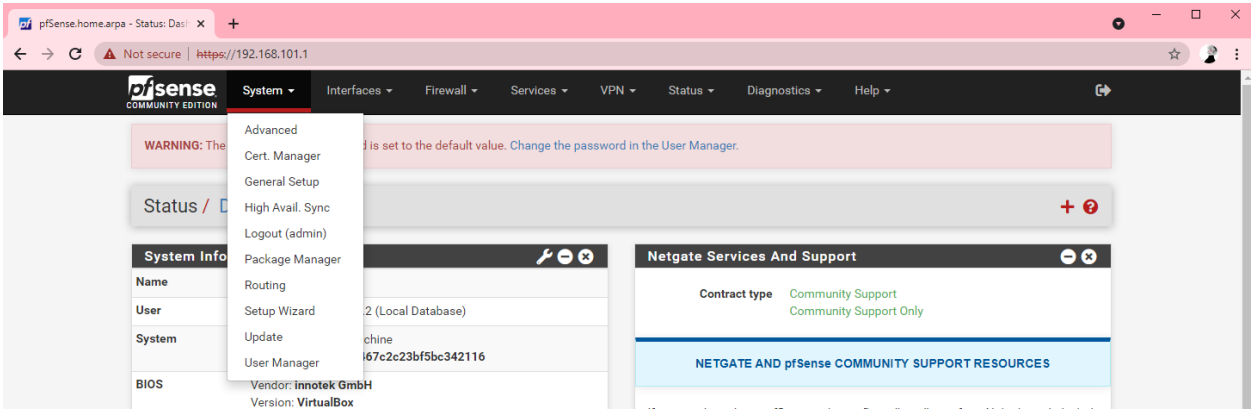
Joshua Lane
IT419
11/23/2021

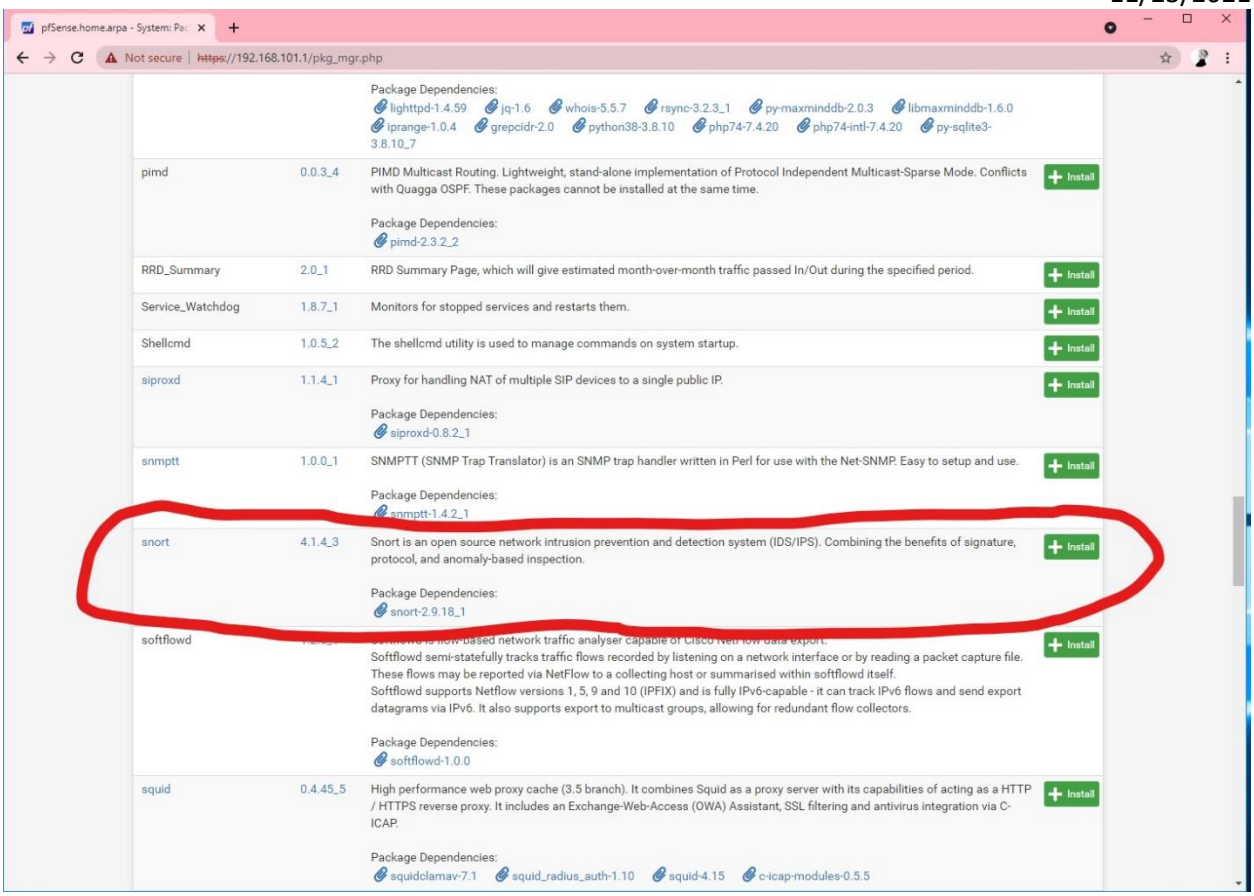
Intrusion Detection/Prevention

Intrusion detection and prevention can save companies heaps of money that would be spent on damages/recovery of a network. Using Snort (for detection/prevention) in tandem with Wireshark (for looking at the contents of the alert) allows for a cybersecurity/IT professional to determine the origins and causes of an intrusion. Even simply scanning a network for vulnerabilities can be detected (any good hacker scans first to determine a plan of action). In order to properly set up a program through pfsense (Snort) that detects/prevents intrusions, it must first be configured with the proper settings.

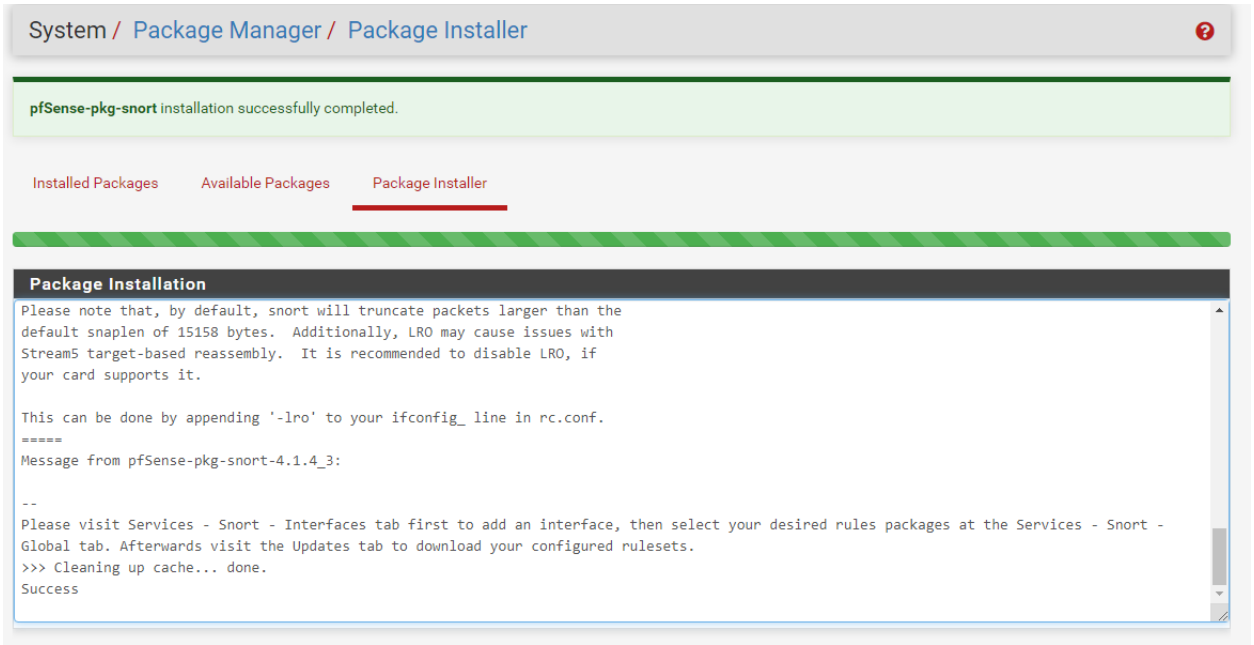
The first step is to locate the package manager in pfsense. From your internal network, open a browser window and type in the LAN interface IP address for pfsense (your firewall) and hit enter. To locate Package Manager, click on System>Package Manager in pfsense (screenshot below).



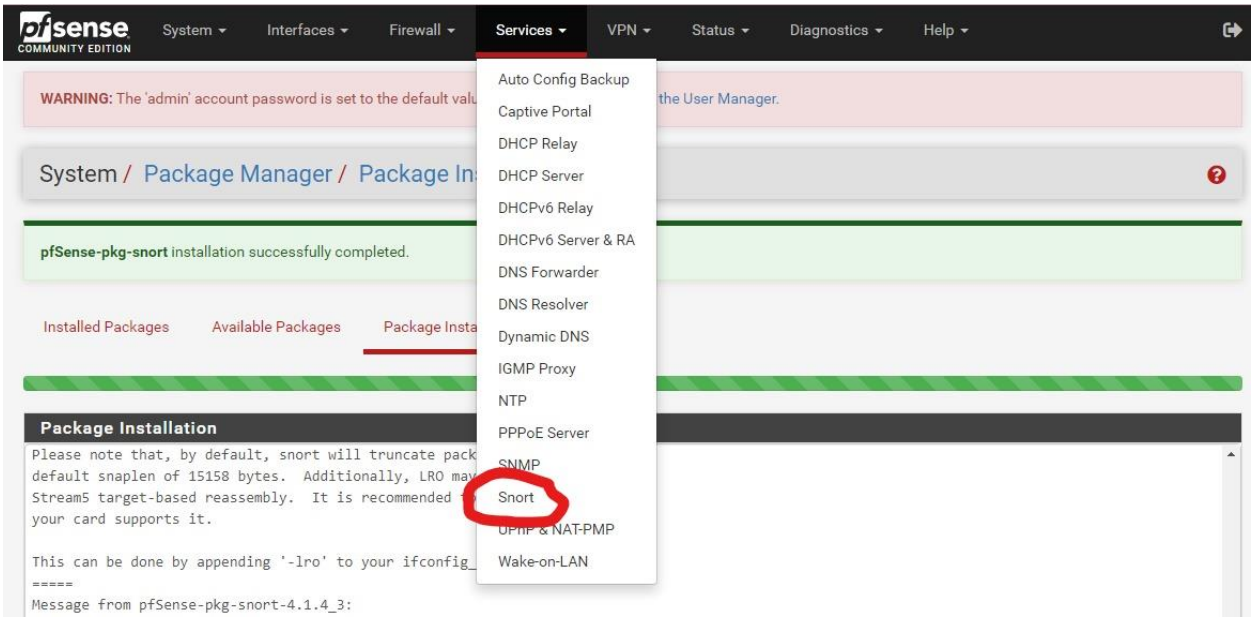
Under available packages, locate Snort and select Install (screenshot next page).



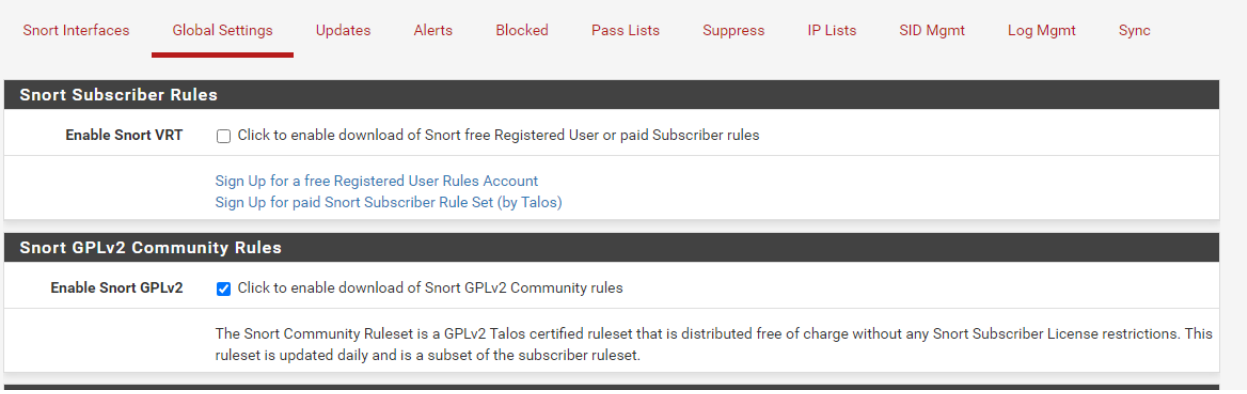
Hit confirm install and you should see the following screen when completed (below).

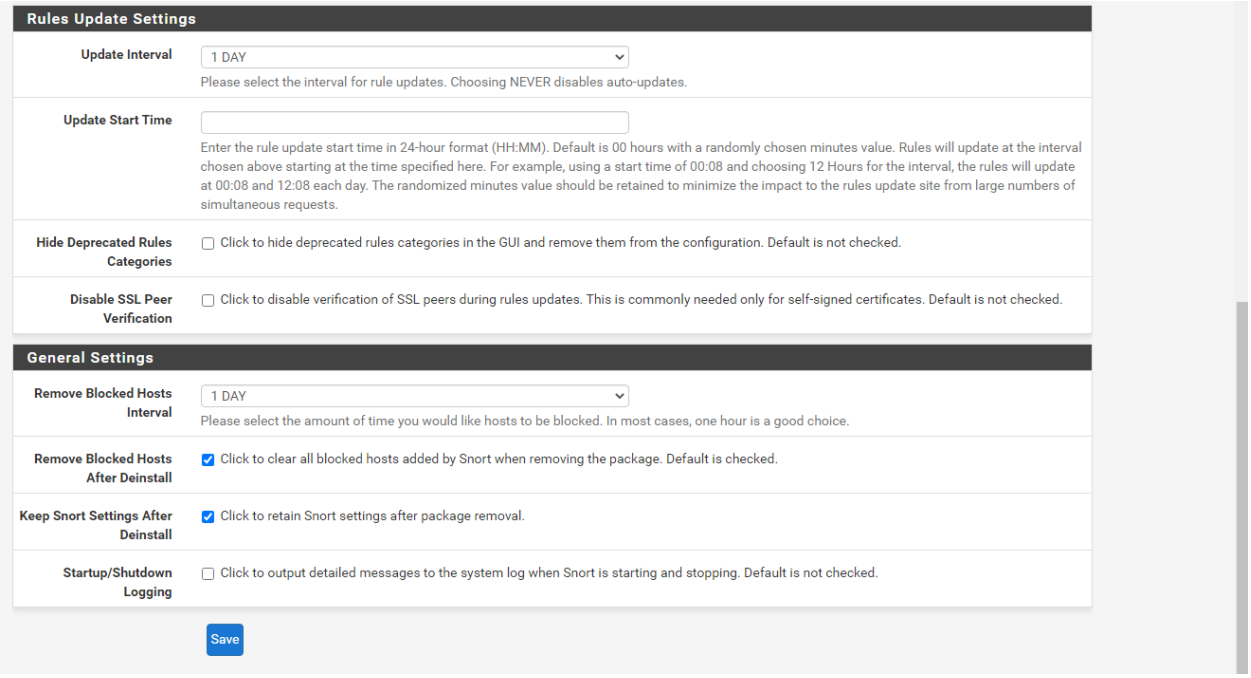


Once installed, Snort will be located under Services (below).

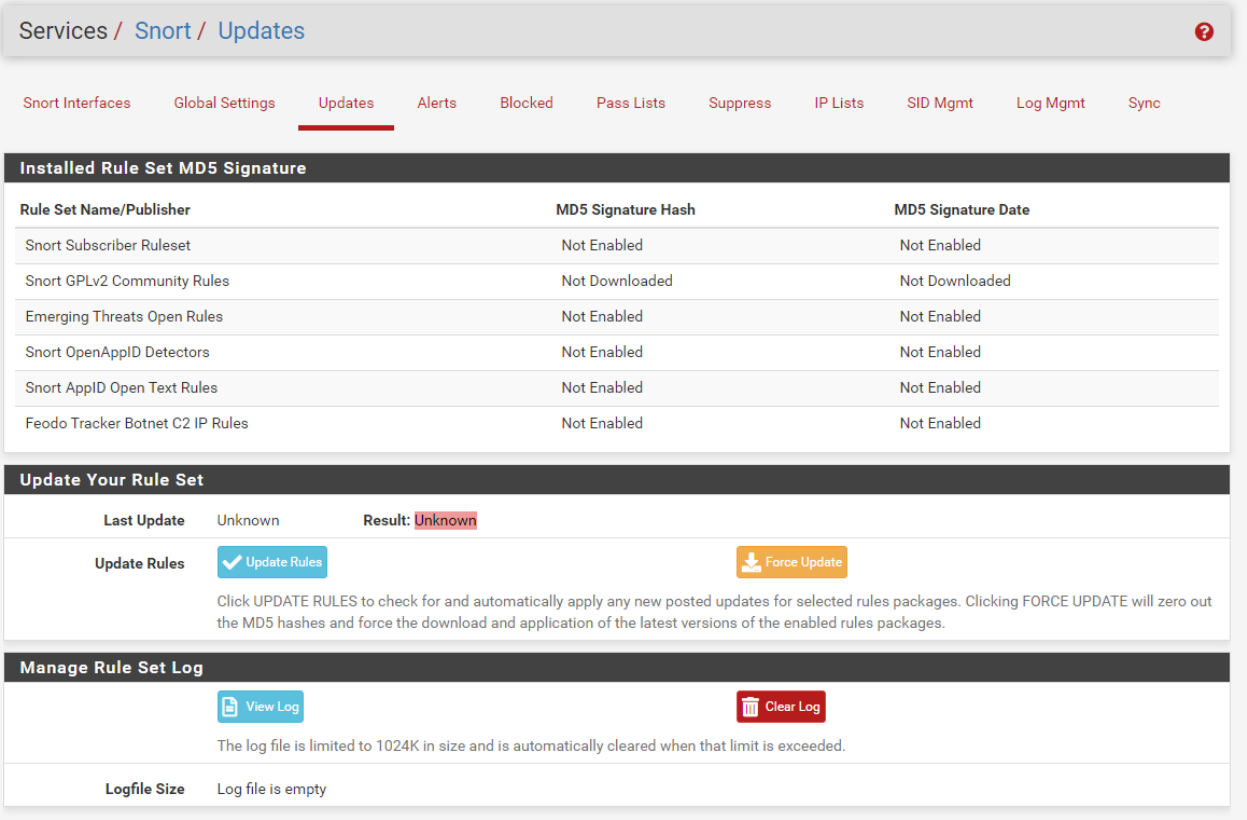


Click Global settings in Snort, enable GPLv2 and set Rules Update to everyday and set remove blocked hosts to everyday. Make sure to save/apply changes (below and next page).

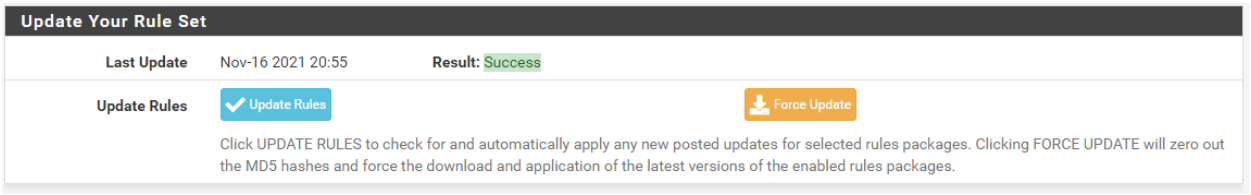




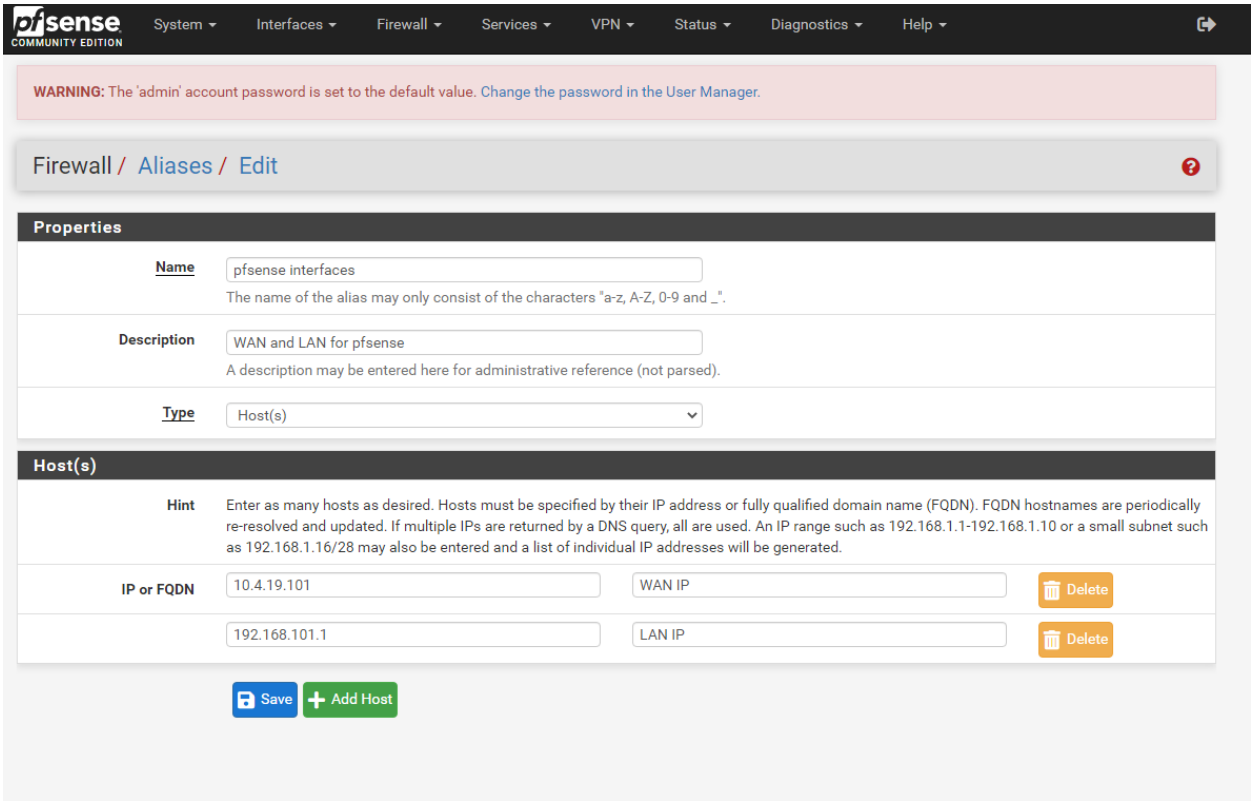
Under Updates, update the rule set (you may need to click Force Update) (below).



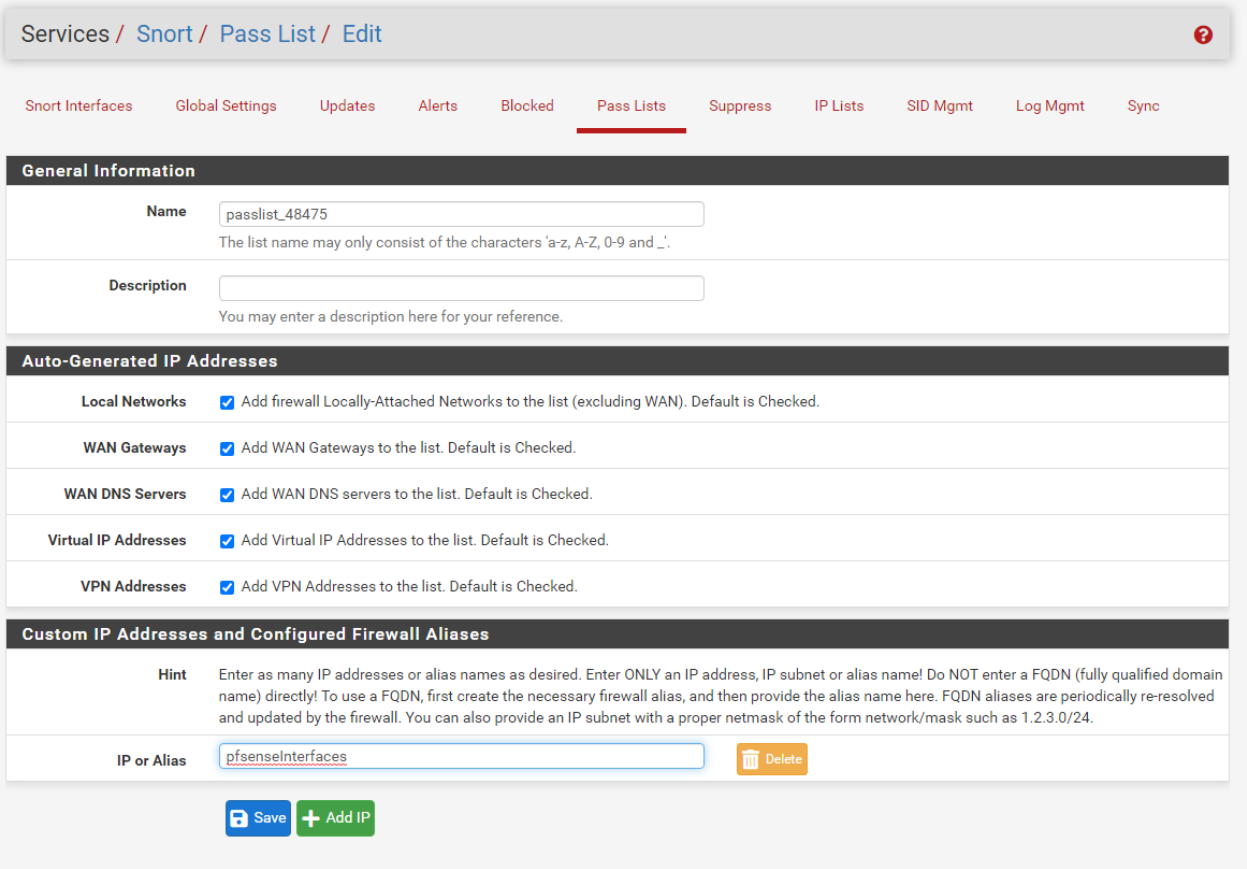
The following is what it should look like once completed:



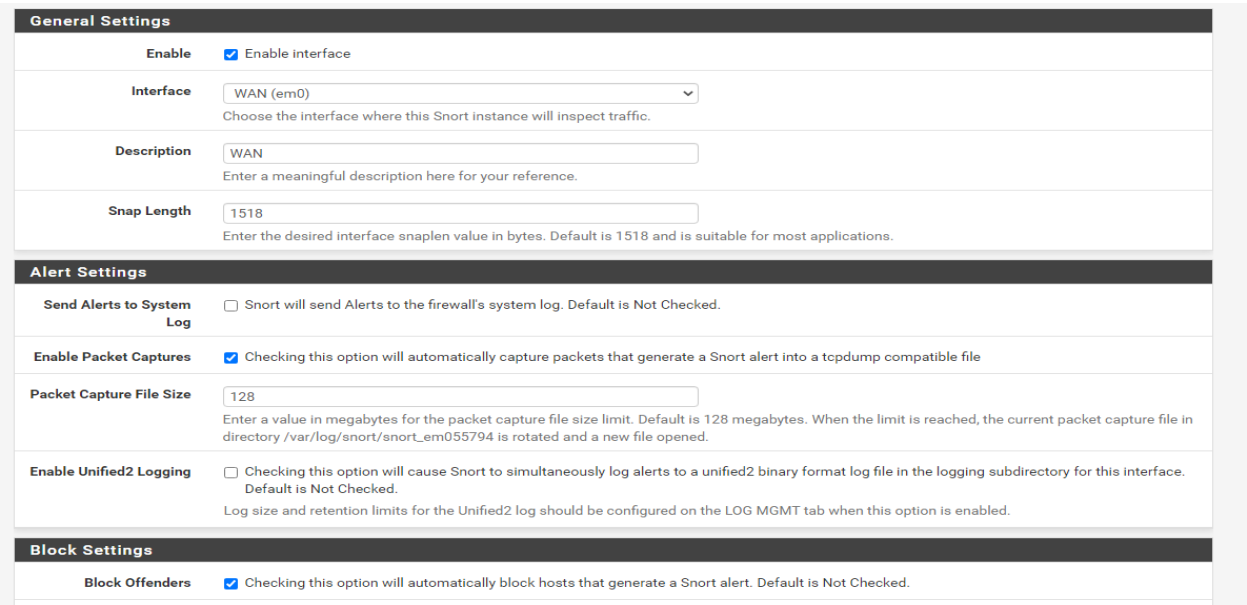
The next step is to create an alias for both interfaces (WAN and LAN) of pfsense. Navigate to Firewall>Aliases>Edit in pfsense and select Add Host. In the screenshot below, you can see I have added both interfaces and labeled them accordingly. Now hit save.



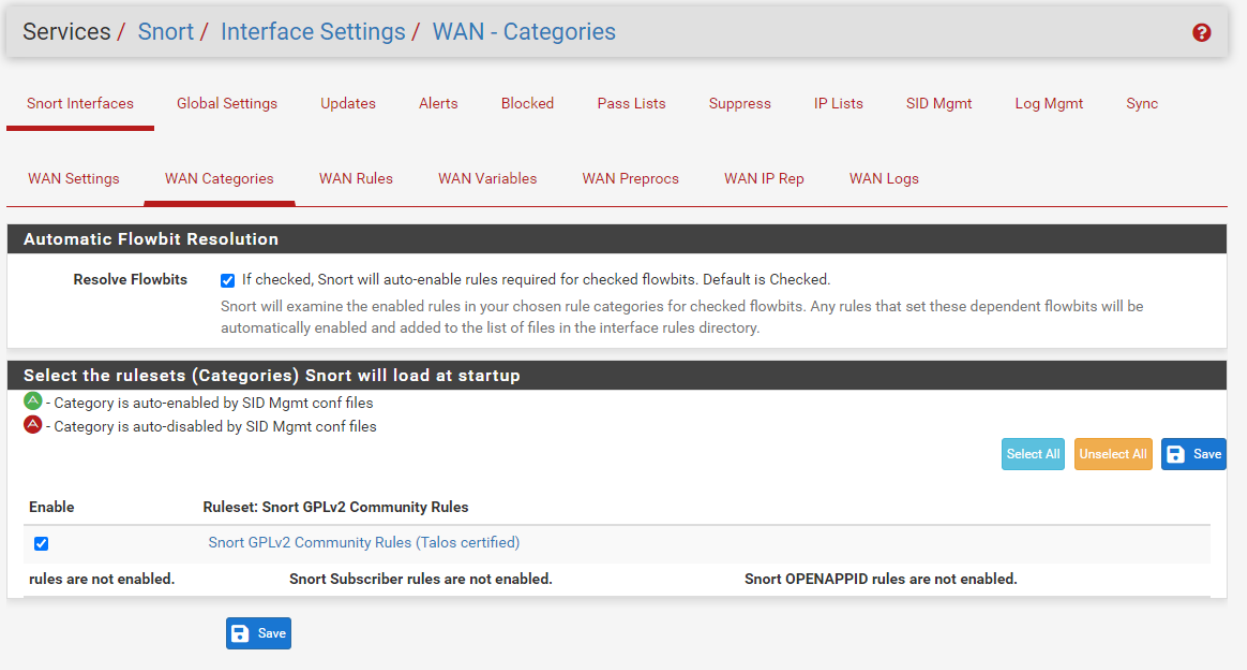
After this completed, you must locate Pass Lists under Services>Snort>Pass List>Edit. Select the Alias you just made and hit save. Make sure to uncheck LAN subnet to allow for alert logging (next page).



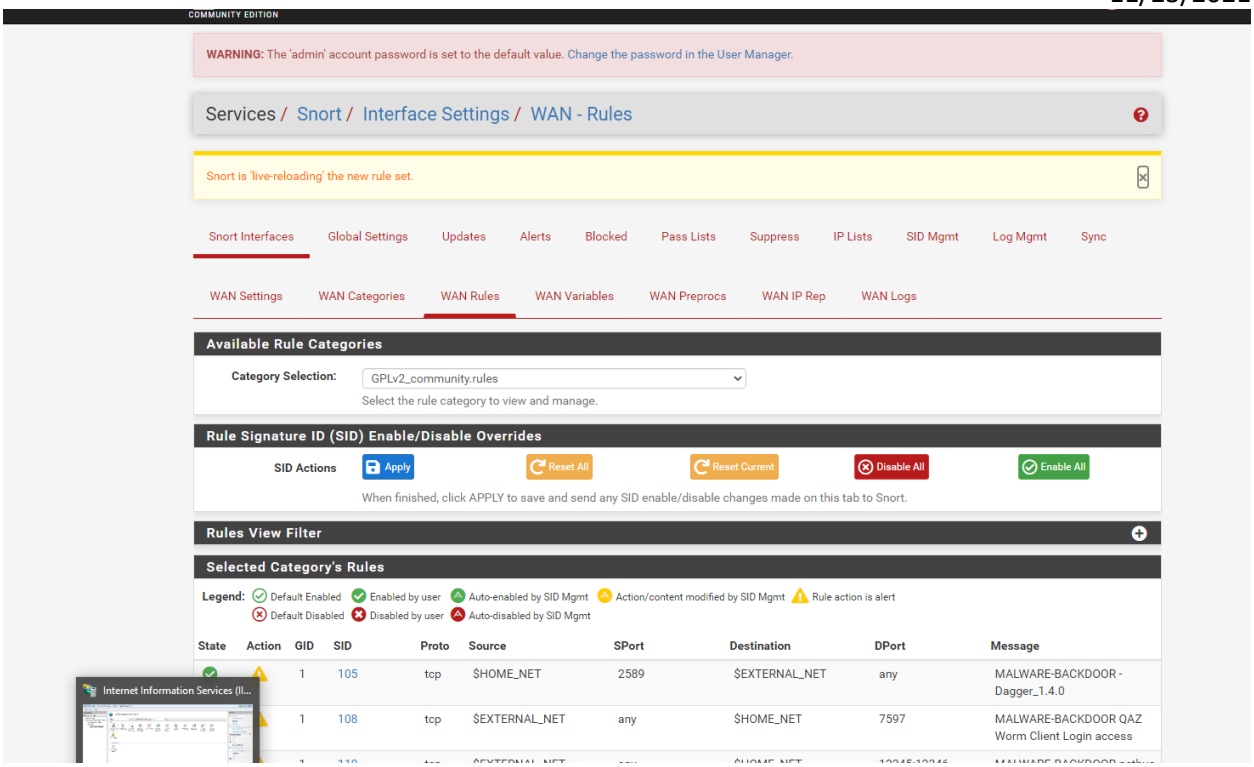
Next, add a Snort interface for WAN by selecting add interface. Open WAN settings and make sure to check Enable Packet Captures and Block Offenders (below).



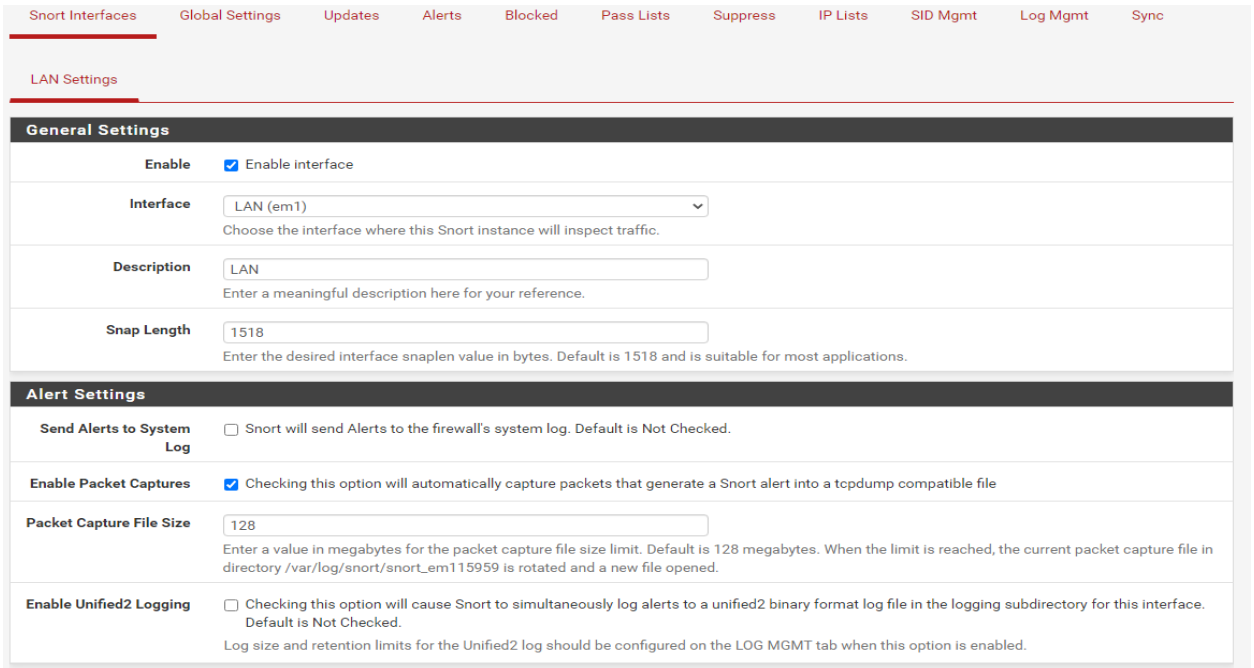
Next, navigate to Services>Snort>Interface Settings>WAN – Categories. Check the box to enable Snort GPLv2 Community Rules (below).

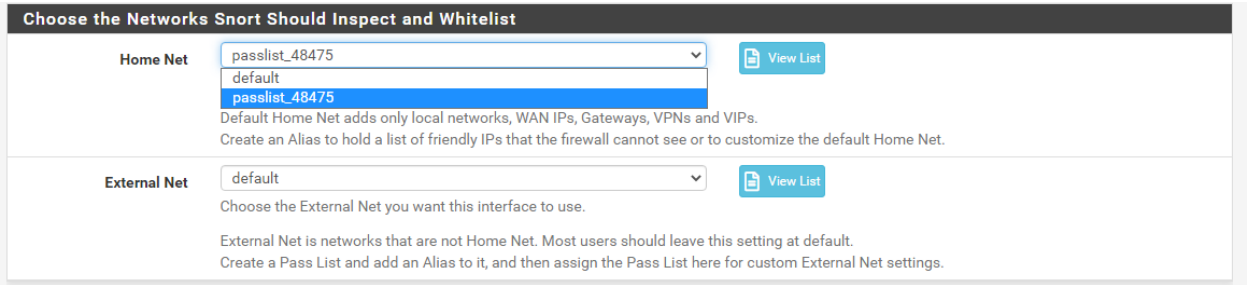


Proceed to WAN Rules under Interface Settings. Under Category Selection use the drop-down menu to select GPLv2_community.rules. Select enable all (next page).



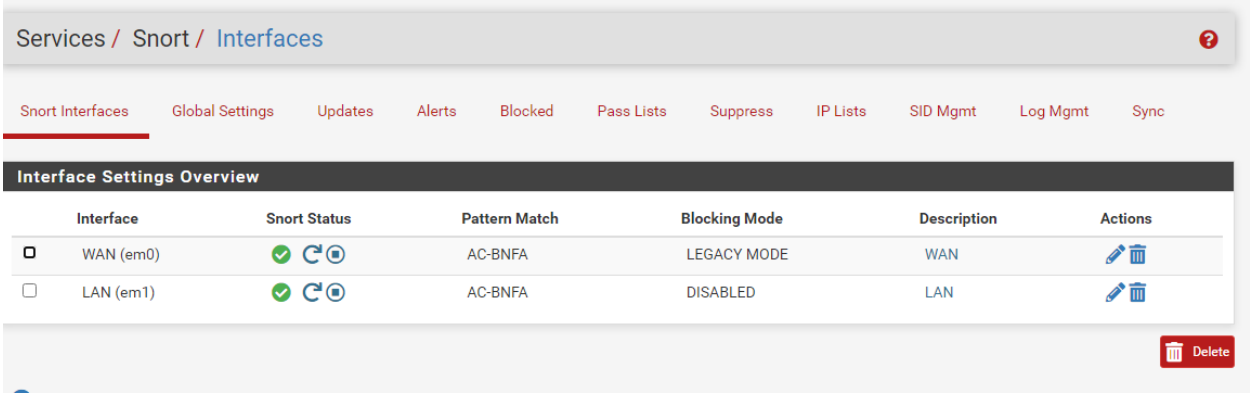
Next, add a Snort interface for LAN and open LAN settings. Check Enable Packet Captures and set Home Net to the pfSense only pass list (below and next page).



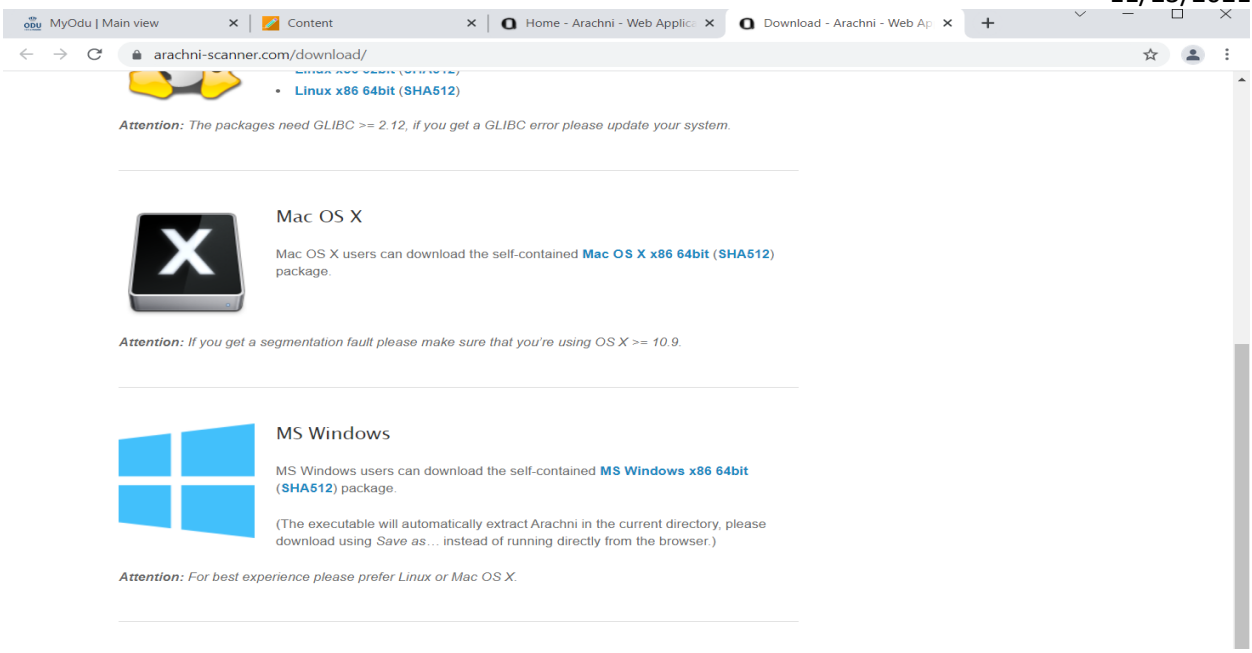


Repeat the steps you did for WAN Categories on LAN categories (enable ruleset for GPLv2 and under LAN Rules select GPLv2 from the drop-down menu, click enable all and apply).

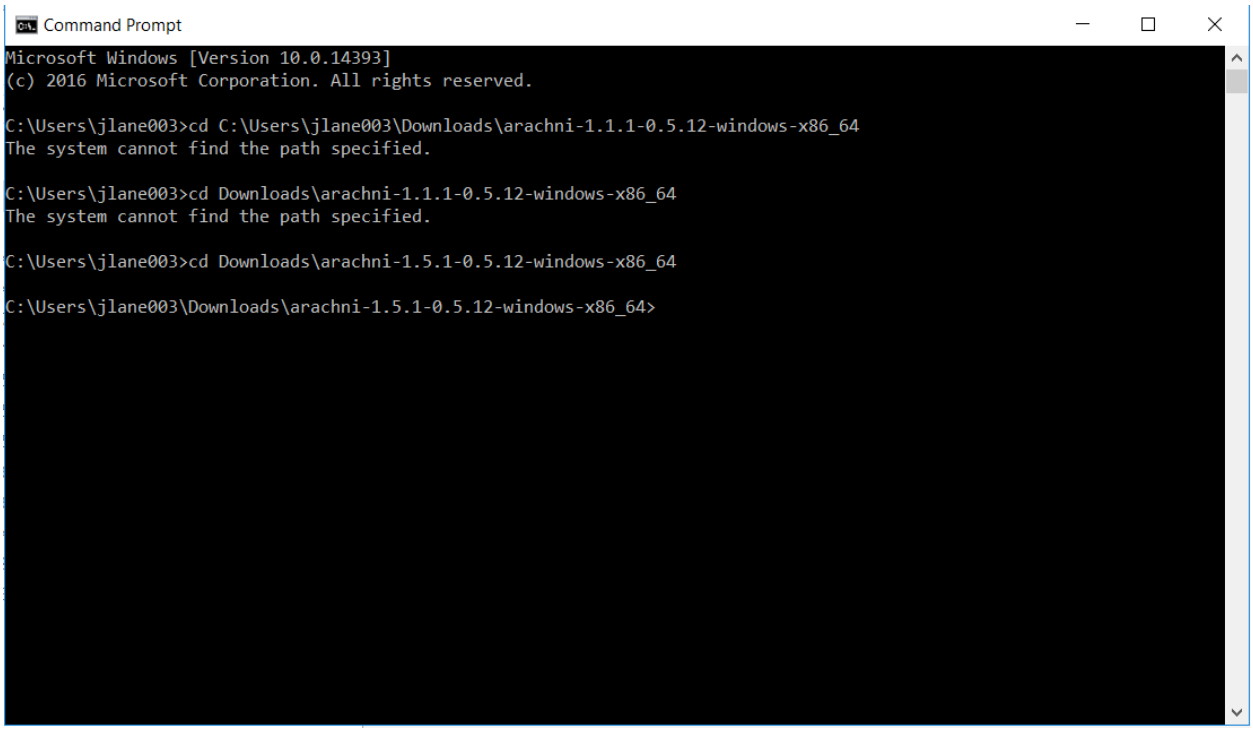
Once this is completed, click Start Snort on this interface for both LAN and WAN (below).

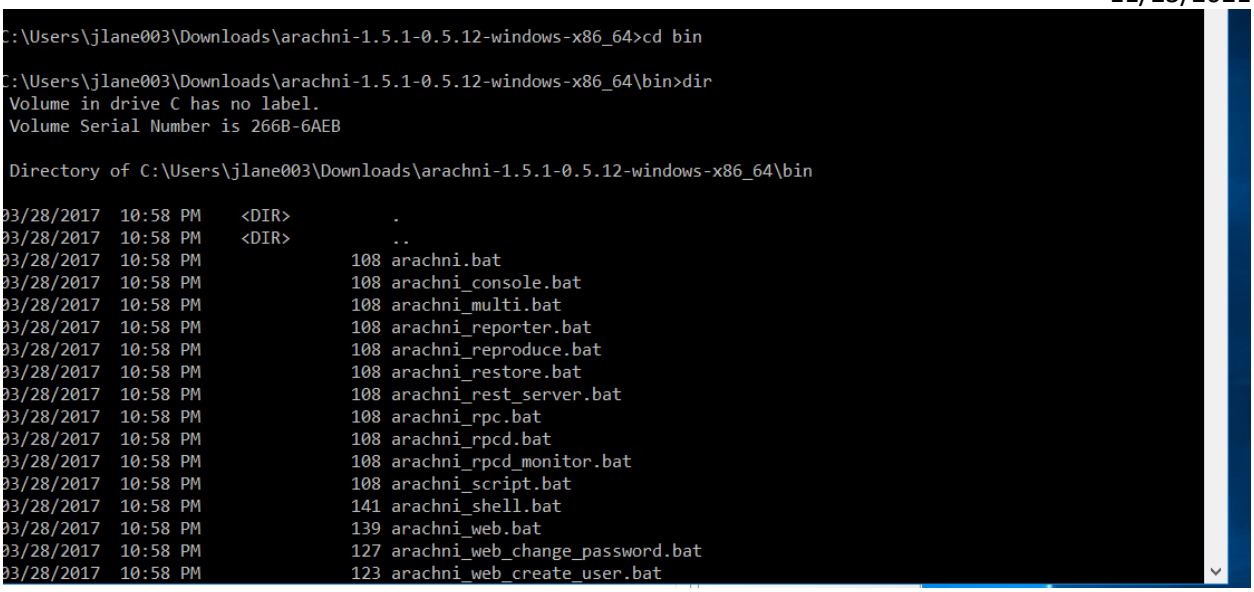


In order to simulate a threat, you need to download arachni to for vulnerabilities on your internal network. Make sure to download for the correct OS (download screenshot next page).



Open a command prompt window and change your directory to the location of arachni in your downloads. Once this is done, change directories to bin under arachni (next page two pages).

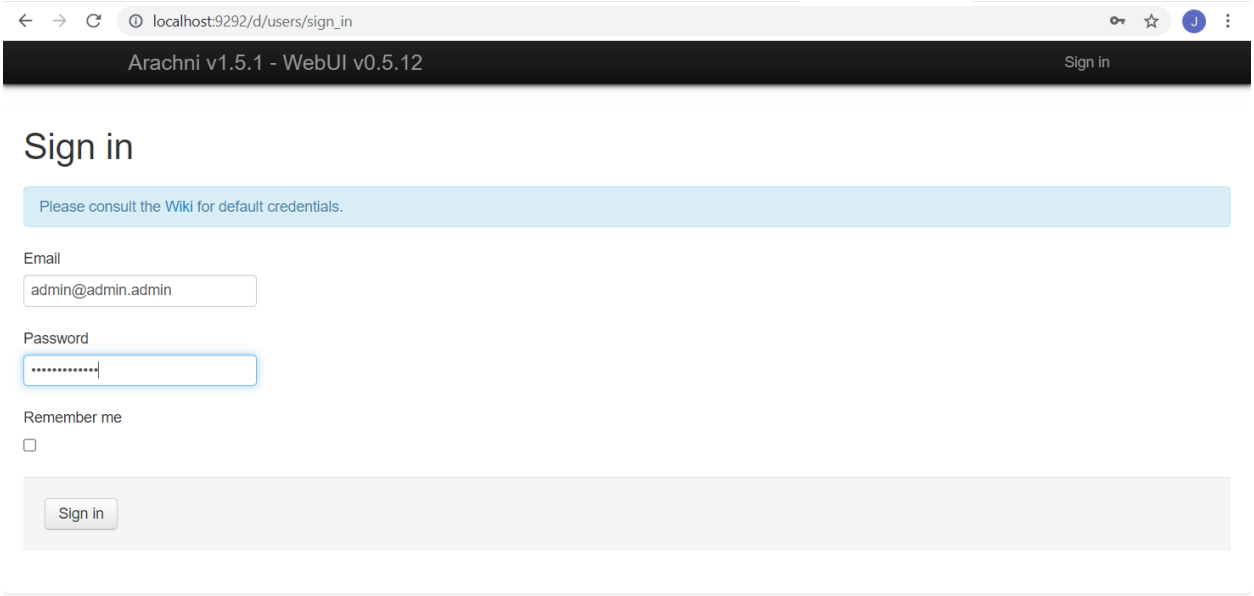




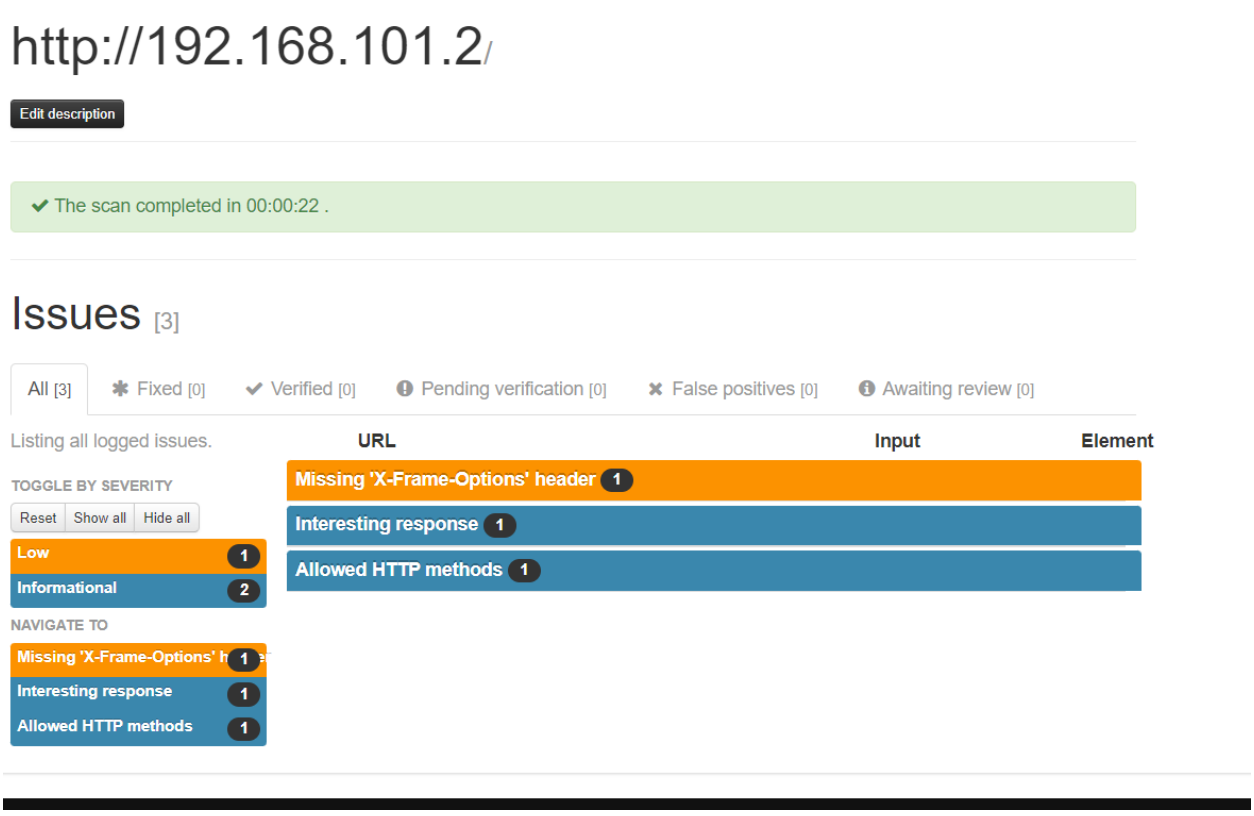
As shown in the screenshot above, proceed to use arachni_web command to start the scan. Once this is done, you will see a “accessible by tcp.localhost:9292” or similar syntax. Open a web browser and proceed to type http://localhost:9292 and it should bring you to a web UI for arachni. Log in with the default credentials (below and next page).

User Name: admin@admin.admin
Password: administrator

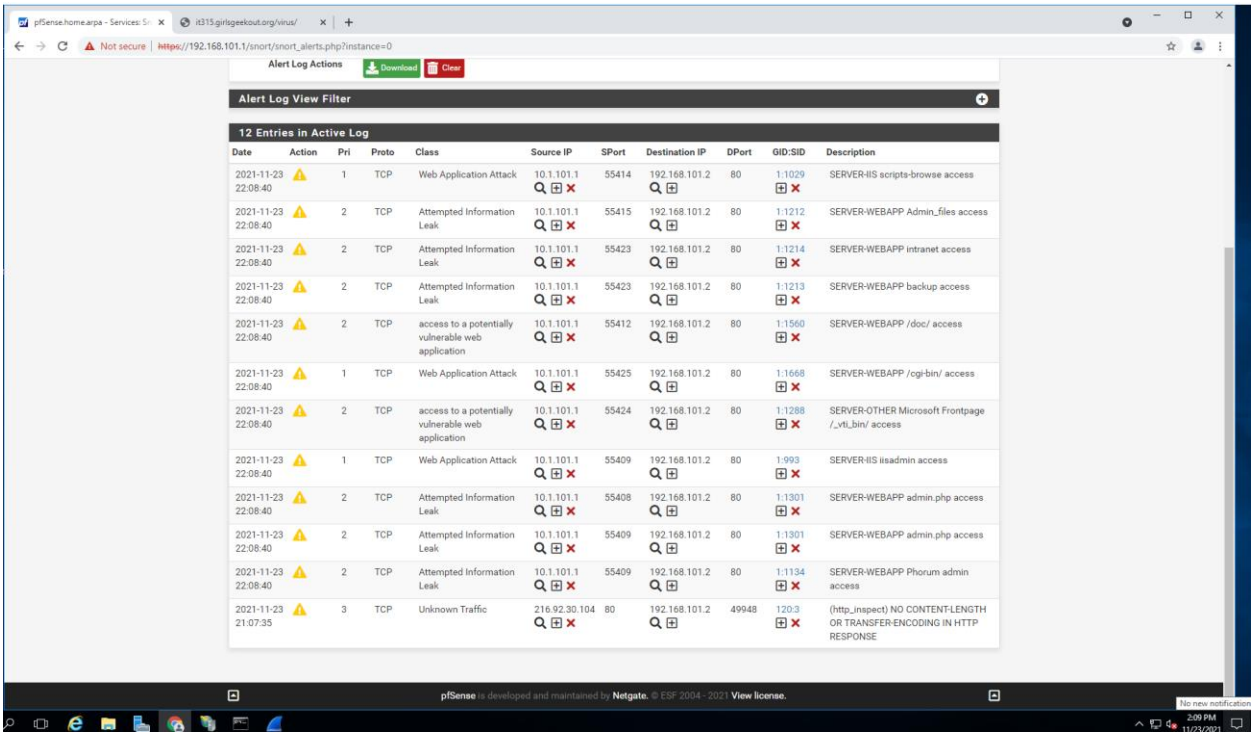
Once logged in, we are greeted with a Welcome page that has some useful information on the homepage, such as Issues per scans and notifications about what you are involved with.



Type in the IP address of your windows server and click scan. The following screen will show when the scan is completed:

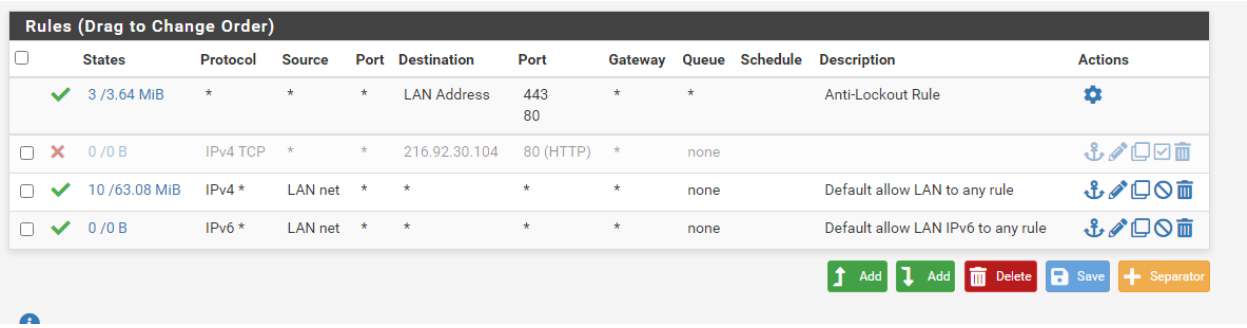


Navigate to alerts under snort to view the alert logs that take place when this vulnerability scan was done (below).

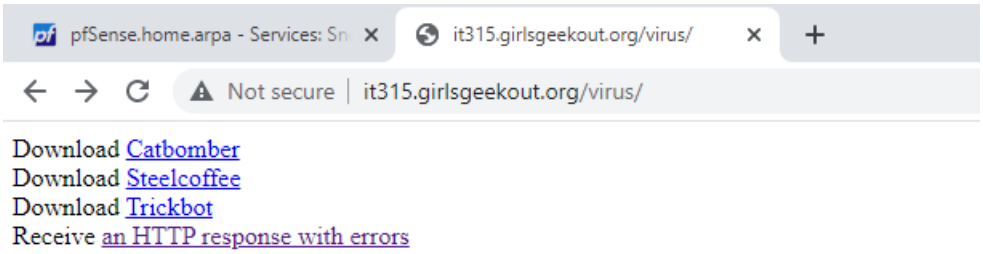


You can then create a rule under firewall rules on the WAN interface for blocking this IP address that scanned the internal network. It is possible to spoof your IP address, so this may not be an ample rule if the attacker has more resources at their disposal.

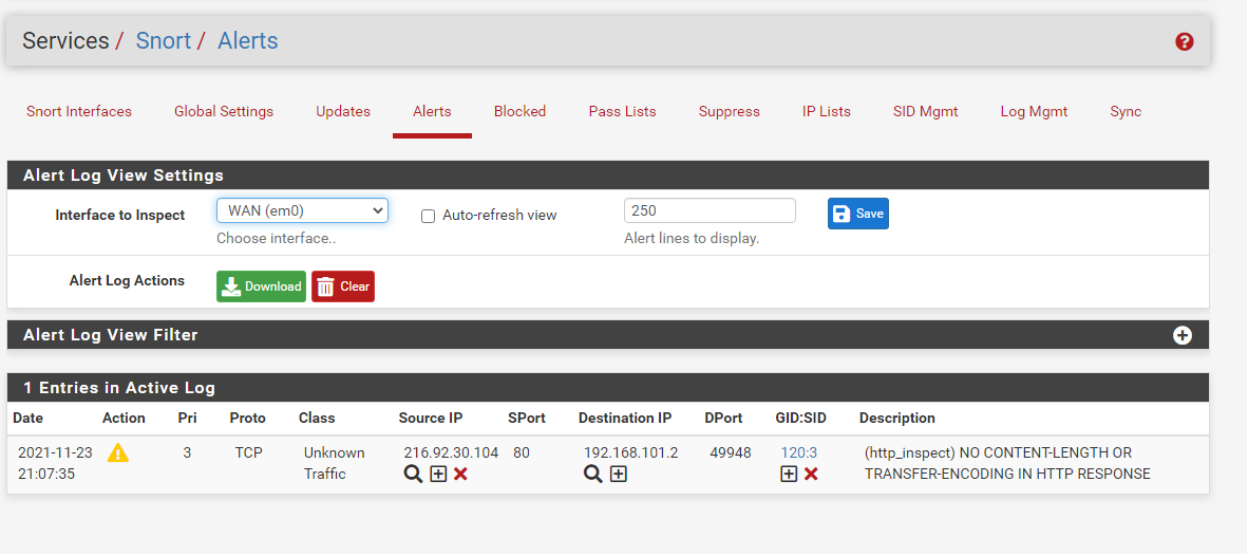
Next, proceed to access a website with a ‘virus’ to click on from the internal network. Make sure to disable any blocking rules preventing this to simulate a real intrusion (below).



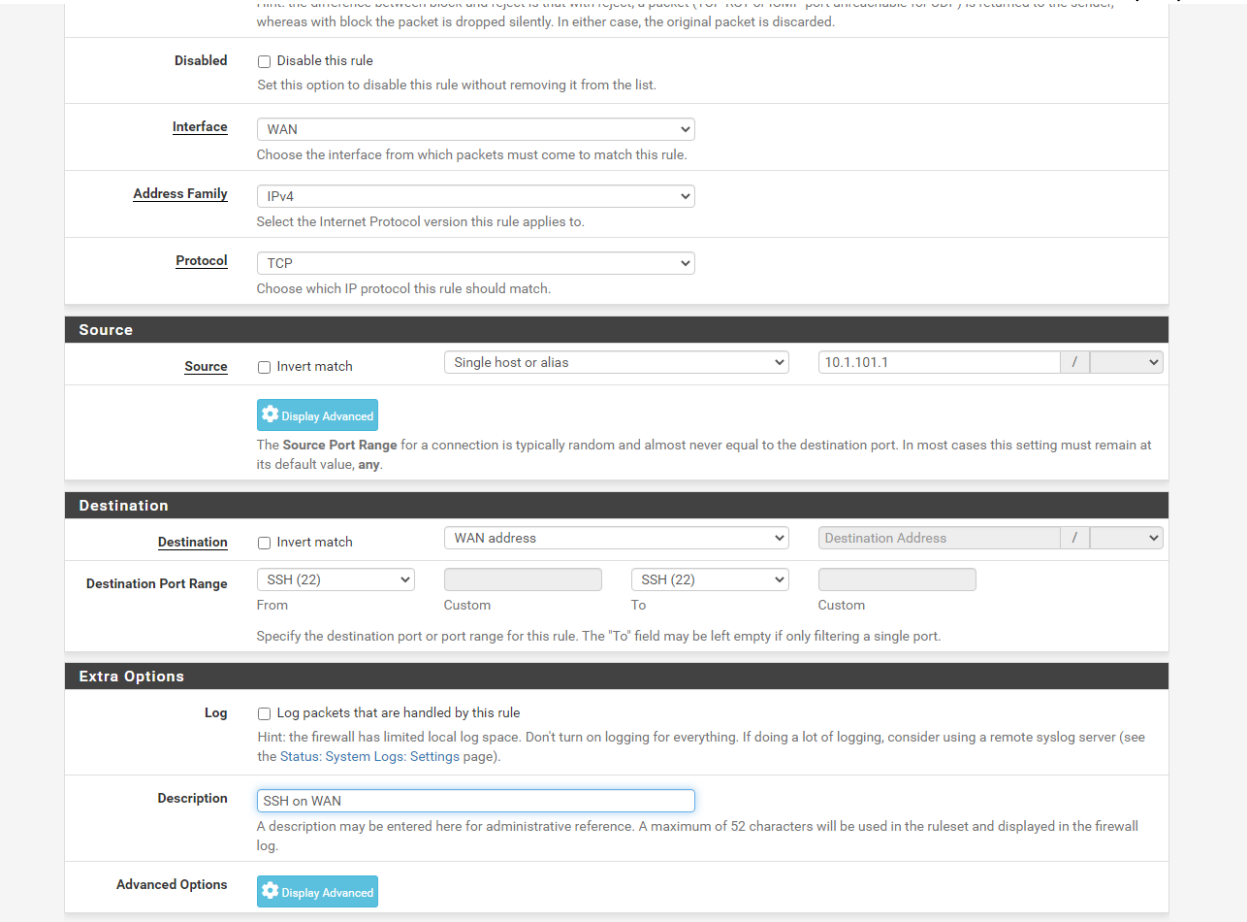
Once you navigate to the virus (here we used it315.girlsgeekout.org/virus) and click HTTP response with errors (below).



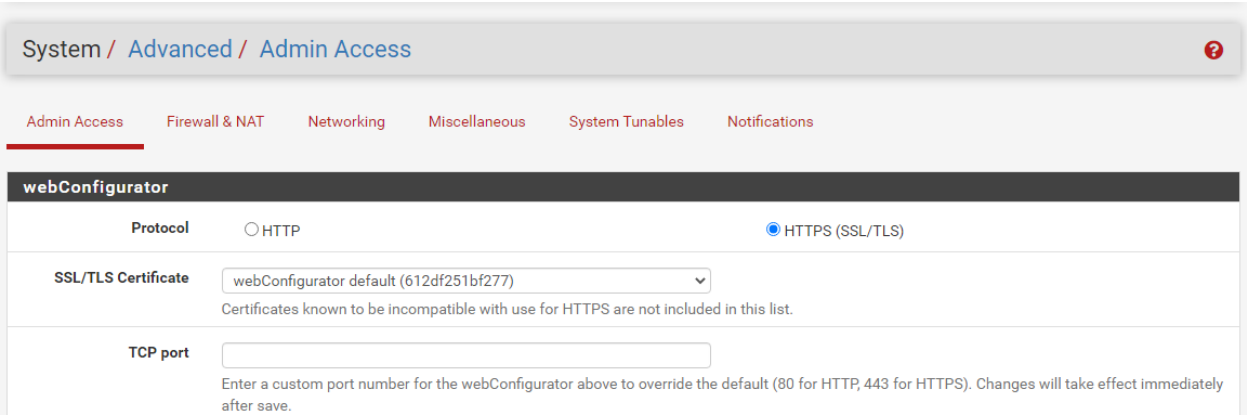
Here is the alert generate from this download on Snort:

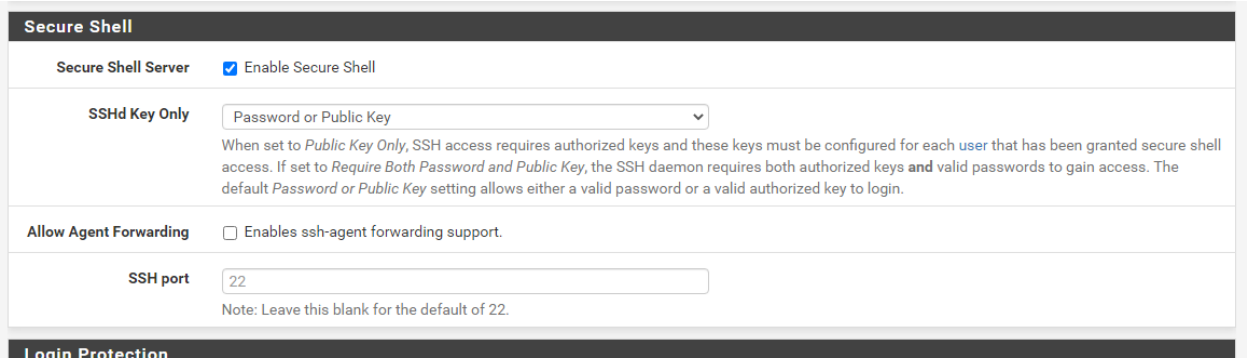


Before you begin with trying to view a log to investigate with Wireshark, you must first change firewall rules to allow a secure shell connection on WAN as well as download an SFTP client to connect to your pfSense firewall. Navigate to Firewall>Rules and add the following rule, click save and apply changes:

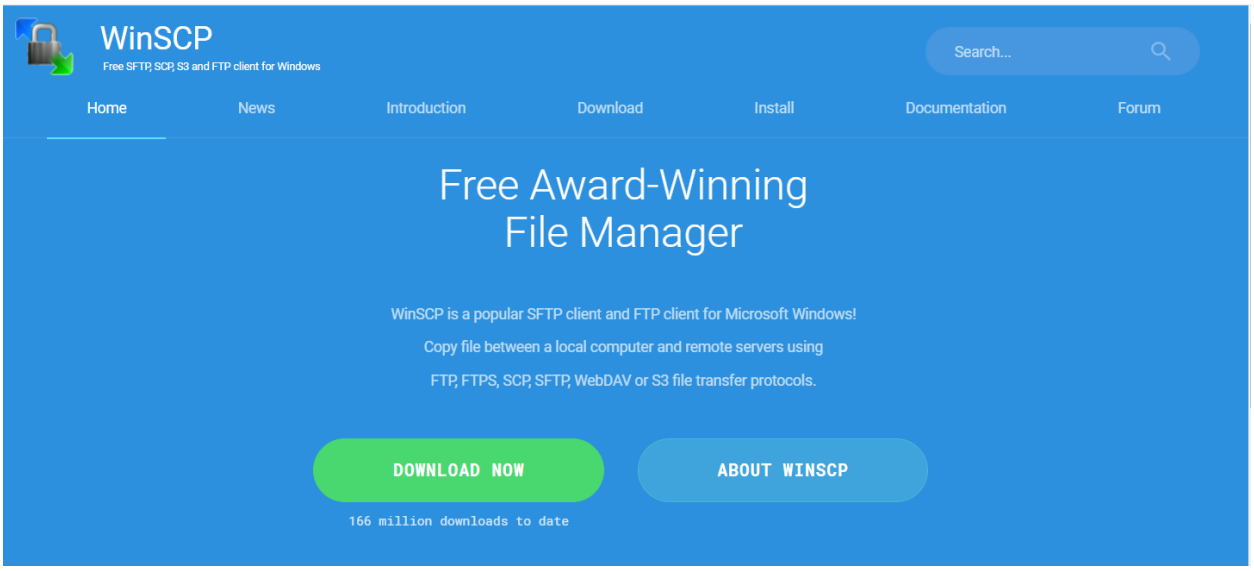


Navigate to System>Advanced>Admin Access to enable Secure Shell:

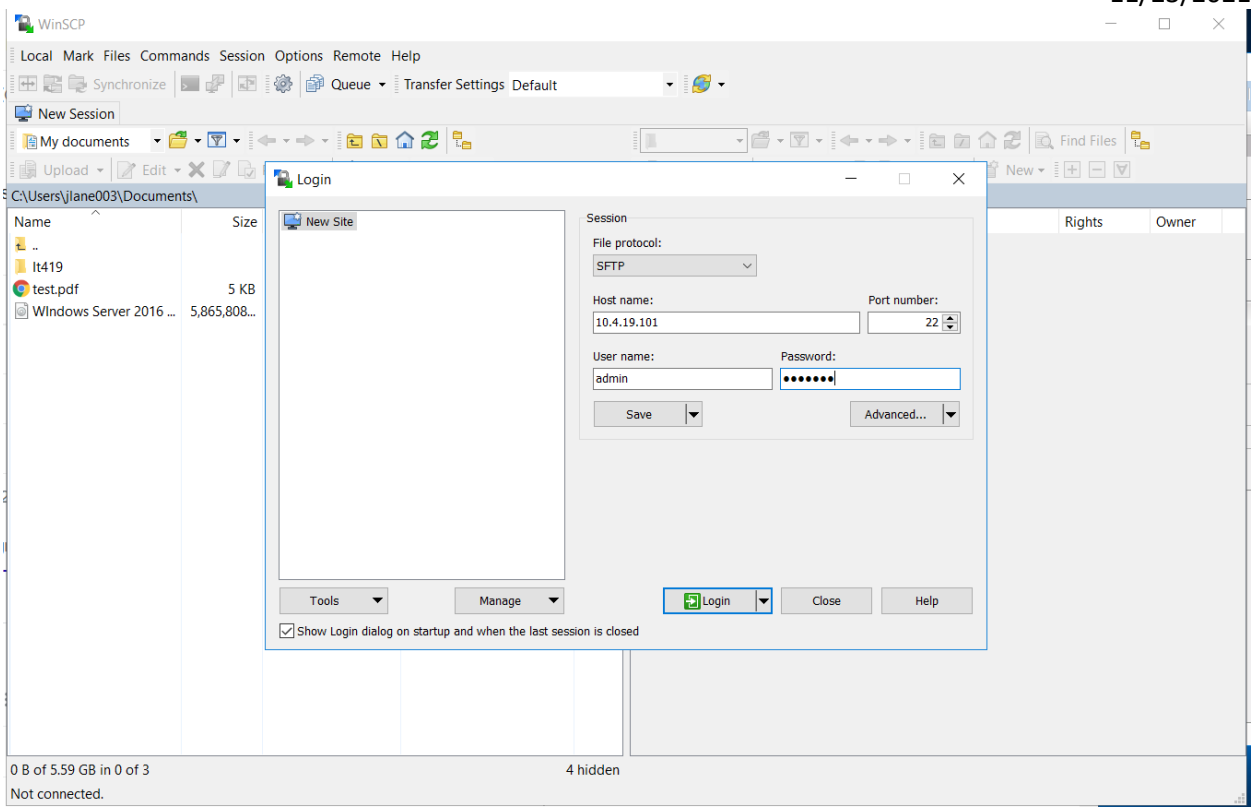




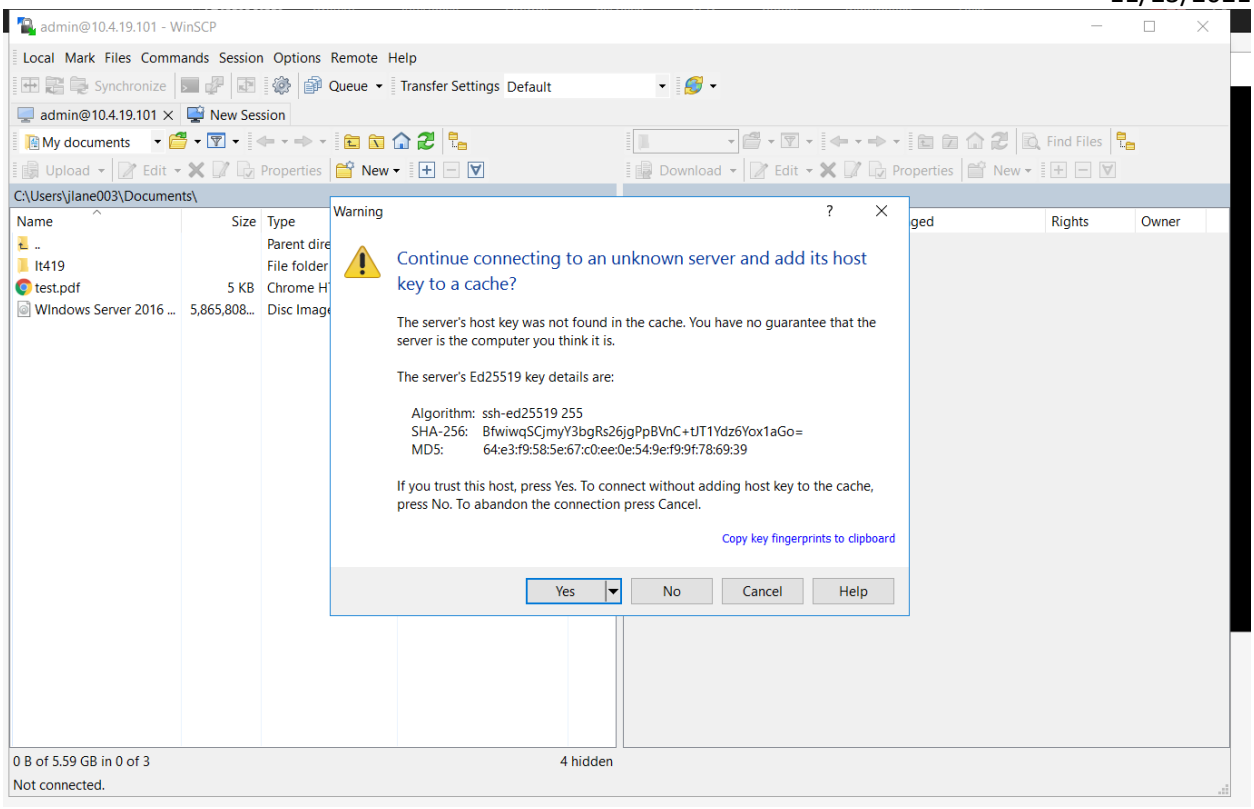
Next, download SFTP client as shown on the next page:



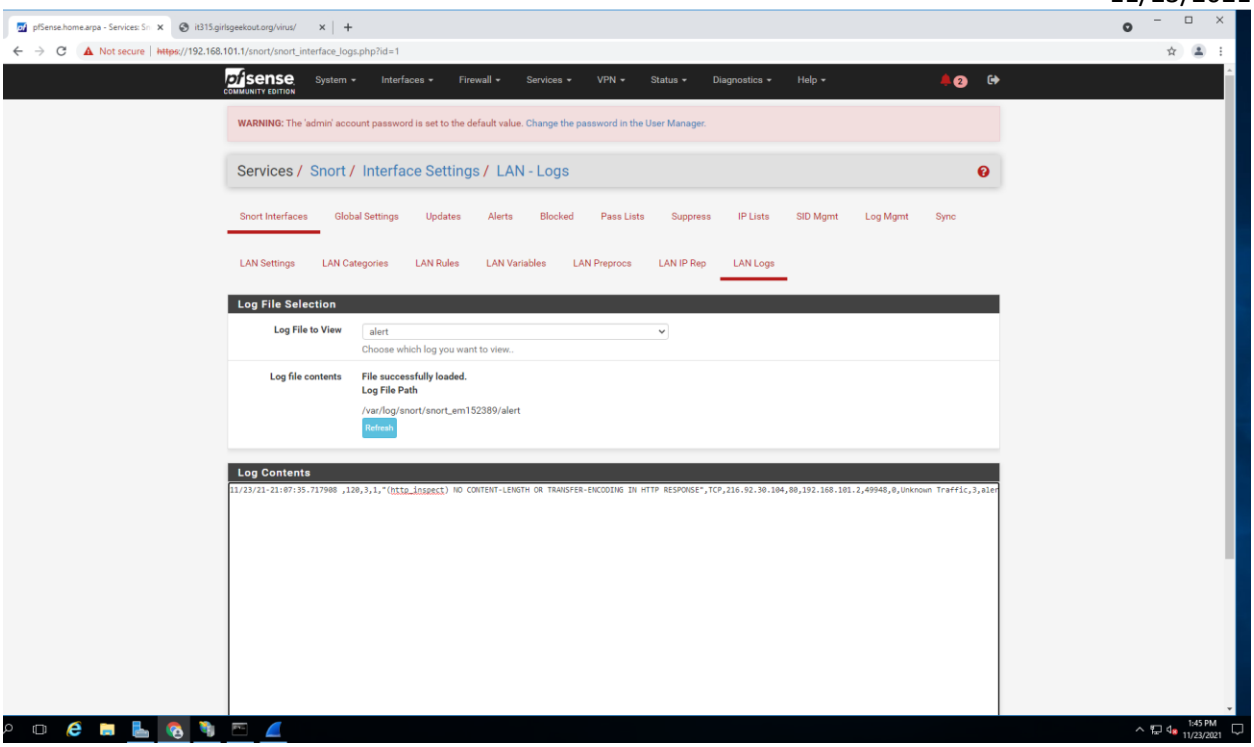
Once this is downloaded and installed, proceed to connect to your pfSense firewall through the SFTP client. Click the folder with 2 dots and type in the Public IP address for your pfSense firewall in the host box. Insert your credentials for pfSense and click Login (screenshot on next page).



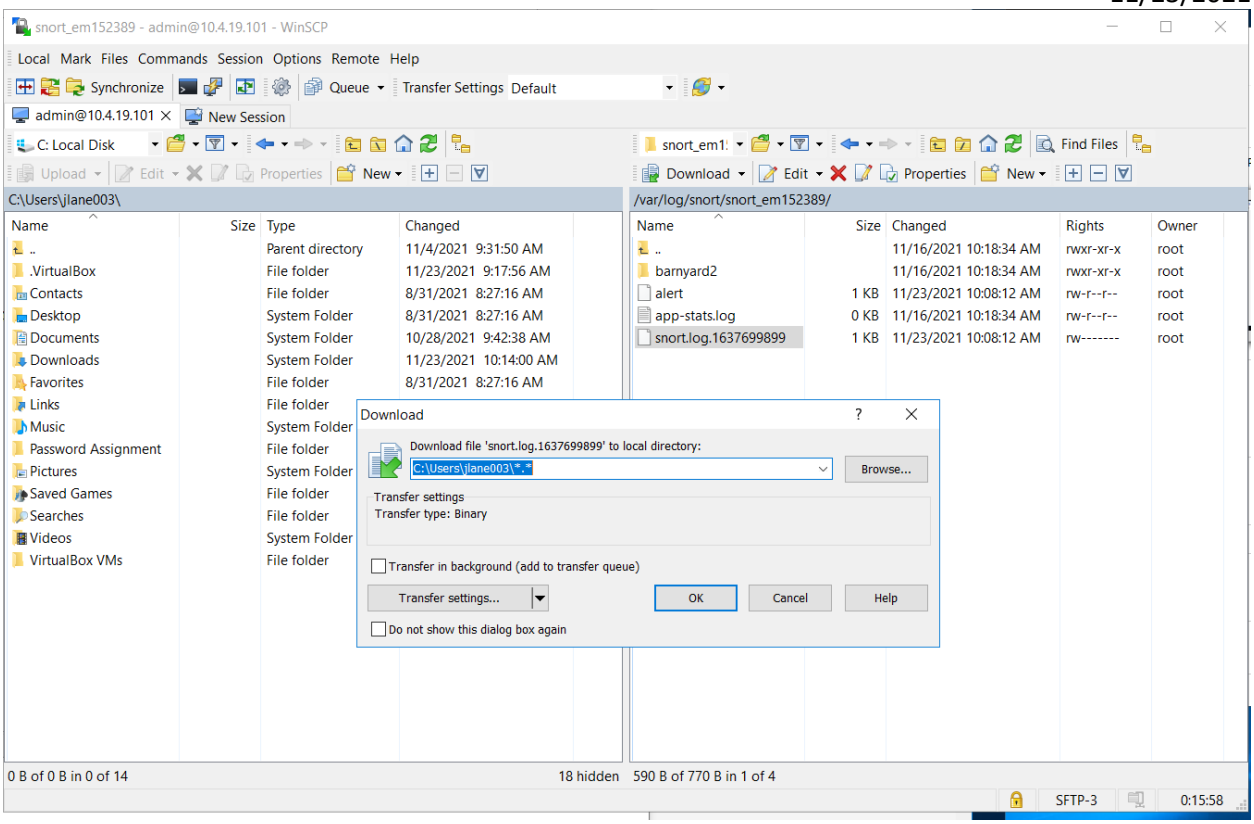
Click Yes at the Unknown Server prompt (next page):



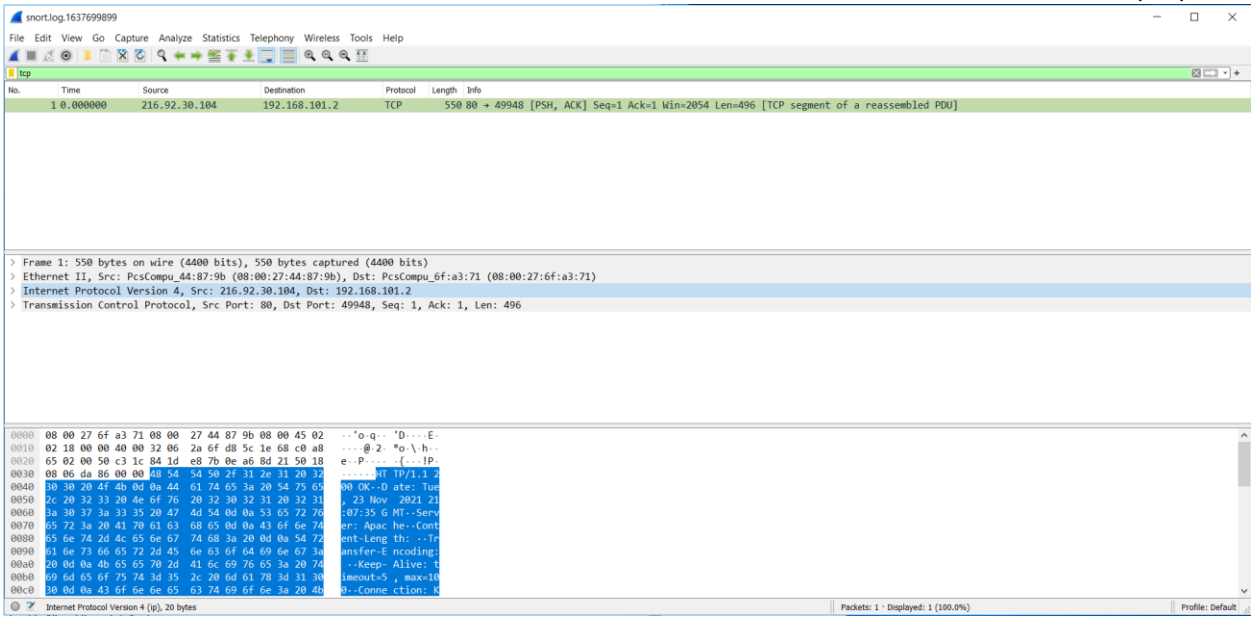
In order to locate exactly where the alert log you want is, you must navigate to Services>Snort>Interface Settings>LAN – Logs. The file path will be displayed there (screenshot on next page):



Go back into the SFTP client and navigate to the file path previously as shown and click OK (next page):



Once this is done, the file should be transferred and observable in Wireshark. Open up the Wireshark Application and look at the file as shown. Here you can see the destination IP address that shows who downloaded the ‘virus’ from a bad website (on next page):



Adding these various rules can keep clients/staff from accidentally downloading viruses and protect your enterprise from outside threats. Snort and custom firewall rules can go a long way prohibiting misuse and making up for the weakest link in the cybersecurity chain (humans).