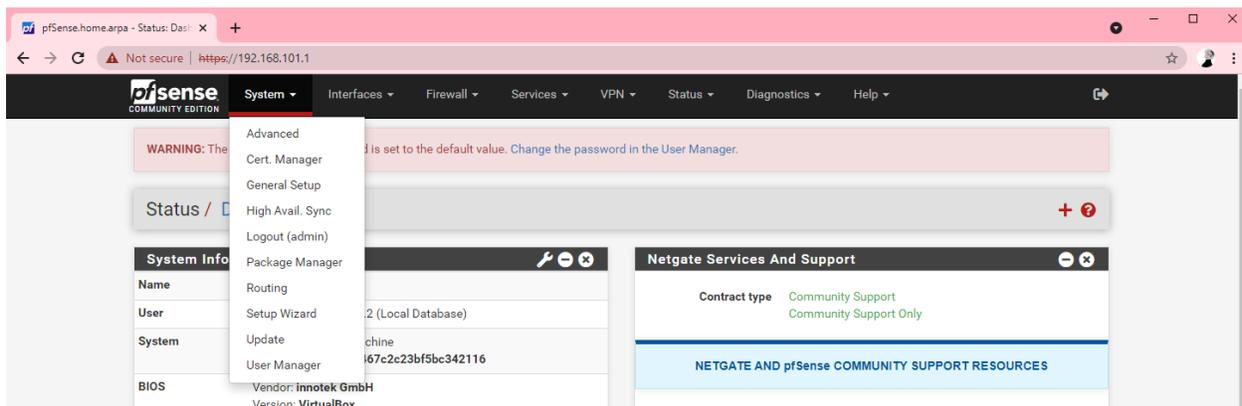


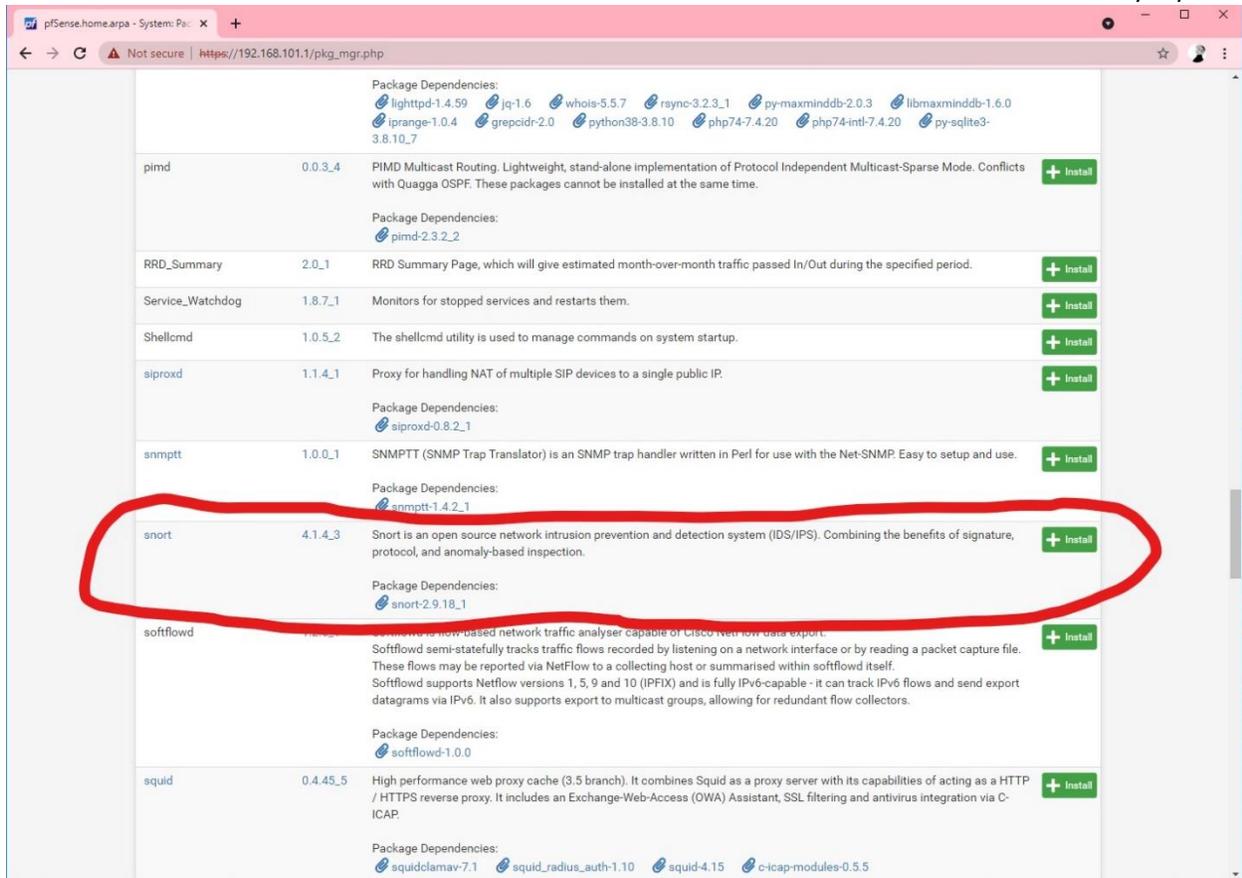
## Intrusion Detection/Prevention

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.

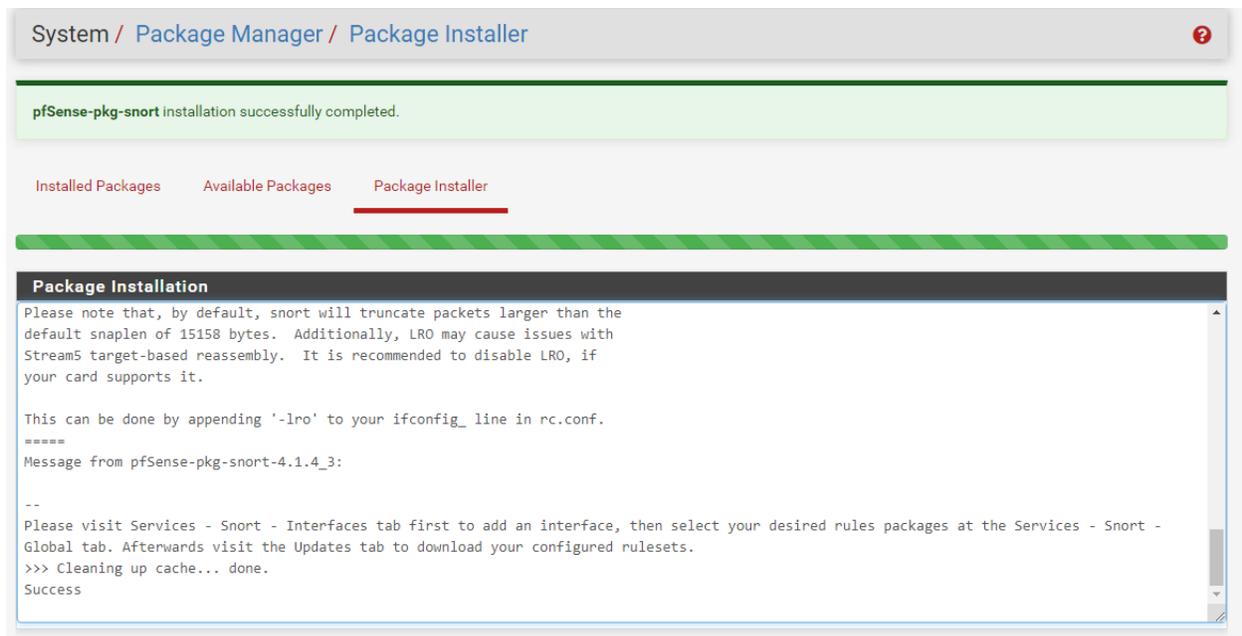
The first step is to locate the package manager in pfsense. From your internal network, open a browser window and type in the LAN interface IP address for pfsense (your firewall) and hit enter. To locate Package Manager, click on System>Package Manager in pfsense (screenshot below).



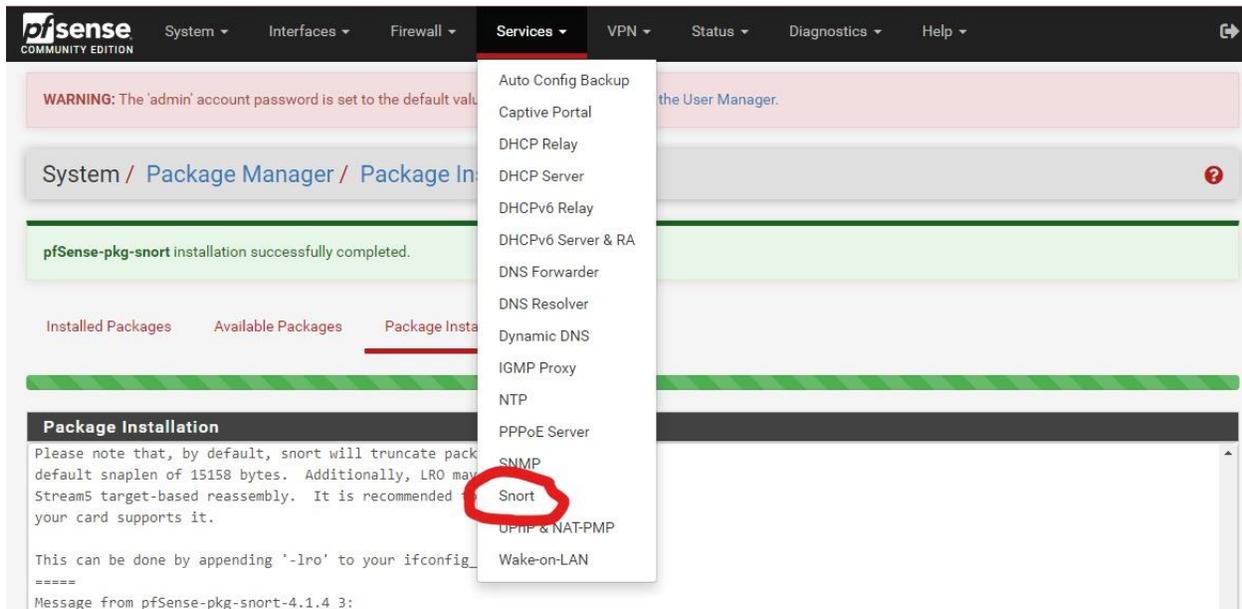
Under available packages, locate Snort and select Install (screenshot next page).



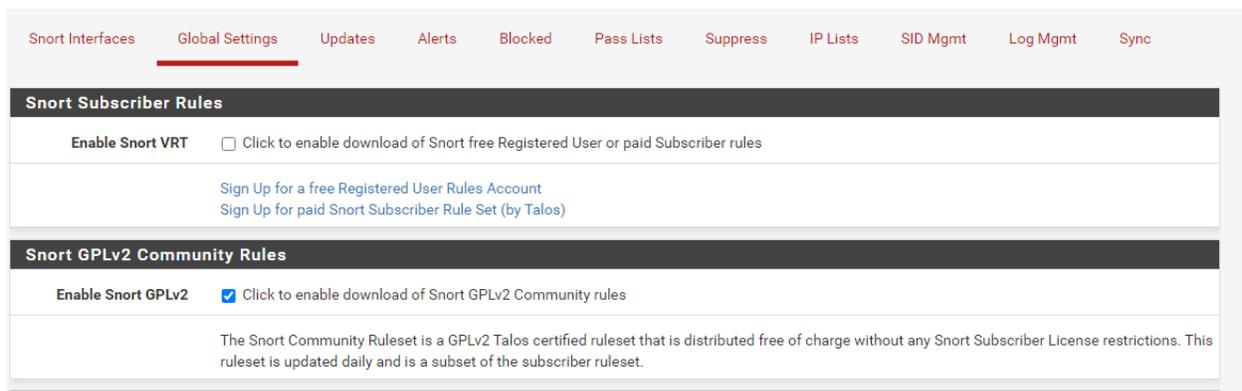
Hit confirm install and you should see the following screen when completed (below).



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).



### Rules Update Settings

**Update Interval**   
Please select the interval for rule updates. Choosing NEVER disables auto-updates.

**Update Start Time**   
Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.

**Hide Deprecated Rules Categories**  Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.

**Disable SSL Peer Verification**  Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

### General Settings

**Remove Blocked Hosts Interval**   
Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.

**Remove Blocked Hosts After Deinstall**  Click to clear all blocked hosts added by Snort when removing the package. Default is checked.

**Keep Snort Settings After Deinstall**  Click to retain Snort settings after package removal.

**Startup/Shutdown Logging**  Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

[Save](#)

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

Services / [Snort](#) / [Updates](#) ?

[Snort Interfaces](#) [Global Settings](#) [Updates](#) [Alerts](#) [Blocked](#) [Pass Lists](#) [Suppress](#) [IP Lists](#) [SID Mgmt](#) [Log Mgmt](#) [Sync](#)

### Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	Not Downloaded	Not Downloaded
Emerging Threats Open Rules	Not Enabled	Not Enabled
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

### Update Your Rule Set

**Last Update** Unknown      **Result:** Unknown

**Update Rules**      

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

### Manage Rule Set Log

The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

**Logfile Size** Log file is empty

The following is what it should look like once completed:

**Update Your Rule Set**

Last Update: Nov-16 2021 20:55      Result: **Success**

Update Rules:      

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

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.

**pfSense** COMMUNITY EDITION    System ▾    Interfaces ▾    Firewall ▾    Services ▾    VPN ▾    Status ▾    Diagnostics ▾    Help ▾

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Aliases / Edit

**Properties**

**Name:** pfsense interfaces  
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".

**Description:** WAN and LAN for pfsense  
A description may be entered here for administrative reference (not parsed).

**Type:** Host(s)

**Host(s)**

**Hint:** Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN		
10.4.19.101	WAN IP	Delete
192.168.101.1	LAN IP	Delete

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).

Services / Snort / Pass List / Edit ?

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

### General Information

Name	<input type="text" value="passlist_48475"/>
The list name may only consist of the characters 'a-z, A-Z, 0-9 and _'.	
Description	<input type="text"/>
You may enter a description here for your reference.	

### Auto-Generated IP Addresses

Local Networks	<input checked="" type="checkbox"/> Add firewall Locally-Attached Networks to the list (excluding WAN). Default is Checked.
WAN Gateways	<input checked="" type="checkbox"/> Add WAN Gateways to the list. Default is Checked.
WAN DNS Servers	<input checked="" type="checkbox"/> Add WAN DNS servers to the list. Default is Checked.
Virtual IP Addresses	<input checked="" type="checkbox"/> Add Virtual IP Addresses to the list. Default is Checked.
VPN Addresses	<input checked="" type="checkbox"/> Add VPN Addresses to the list. Default is Checked.

### Custom IP Addresses and Configured Firewall Aliases

**Hint** Enter as many IP addresses or alias names as desired. Enter ONLY an IP address, IP subnet or alias name! Do NOT enter a FQDN (fully qualified domain name) directly! To use a FQDN, first create the necessary firewall alias, and then provide the alias name here. FQDN aliases are periodically re-resolved and updated by the firewall. You can also provide an IP subnet with a proper netmask of the form network/mask such as 1.2.3.0/24.

IP or Alias	<input type="text" value="pfsenseInterfaces"/>	<input type="button" value="Delete"/>
-------------	--	---------------------------------------

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).

### General Settings

Enable	<input checked="" type="checkbox"/> Enable interface
Interface	<input type="text" value="WAN (em0)"/>
Choose the interface where this Snort instance will inspect traffic.	
Description	<input type="text" value="WAN"/>
Enter a meaningful description here for your reference.	
Snap Length	<input type="text" value="1518"/>
Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.	

### Alert Settings

Send Alerts to System Log	<input type="checkbox"/> Snort will send Alerts to the firewall's system log. Default is Not Checked.
Enable Packet Captures	<input checked="" type="checkbox"/> Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Packet Capture File Size	<input type="text" value="128"/>
Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort_em055794 is rotated and a new file opened.	
Enable Unified2 Logging	<input type="checkbox"/> Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.
Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.	

### Block Settings

Block Offenders	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
-----------------	--

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

Services / Snort / Interface Settings / WAN - Categories

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

WAN Settings WAN Categories WAN Rules WAN Variables WAN Preprocs WAN IP Rep WAN Logs

### Automatic Flowbit Resolution

**Resolve Flowbits**  If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.  
Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

### Select the rulesets (Categories) Snort will load at startup

- Category is auto-enabled by SID Mgmt conf files  
 - Category is auto-disabled by SID Mgmt conf files

Select All Unselect All Save

Enable Ruleset: Snort GPLv2 Community Rules

Snort GPLv2 Community Rules (Talos certified)

rules are not enabled. Snort Subscriber rules are not enabled. Snort OPENAPPID rules are not enabled.

Save

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).

COMMUNITY EDITION

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Services / Snort / Interface Settings / WAN - Rules

Snort is 'live-reloading' the new rule set.

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

WAN Settings WAN Categories **WAN Rules** WAN Variables WAN Preprocs WAN IP Rep WAN Logs

**Available Rule Categories**

Category Selection: GPLv2\_community.rules  
Select the rule category to view and manage.

**Rule Signature ID (SID) Enable/Disable Overrides**

SID Actions

When finished, click APPLY to save and send any SID enable/disable changes made on this tab to Snort.

**Rules View Filter**

**Selected Category's Rules**

Legend:  Default Enabled  Enabled by user  Auto-enabled by SID Mgmt  Action/content modified by SID Mgmt  Rule action is alert  
 Default Disabled  Disabled by user  Auto-disabled by SID Mgmt

State	Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	105	tcp	\$HOME_NET	2589	\$EXTERNAL_NET	any	MALWARE-BACKDOOR-Dagger_1.4.0
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	108	tcp	\$EXTERNAL_NET	any	\$HOME_NET	7597	MALWARE-BACKDOOR-QAZ Worm Client Login access
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	110	...	\$EXTERNAL_NET	...	\$HOME_NET	13345-13346	MALWARE-BACKDOOR-...



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).

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

**LAN Settings**

**General Settings**

Enable  Enable interface

Interface LAN (em1)  
Choose the interface where this Snort instance will inspect traffic.

Description LAN  
Enter a meaningful description here for your reference.

Snap Length 1518  
Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

**Alert Settings**

Send Alerts to System Log  Snort will send Alerts to the firewall's system log. Default is Not Checked.

Enable Packet Captures  Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Packet Capture File Size 128  
Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort\_em115959 is rotated and a new file opened.

Enable Unified2 Logging  Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.  
Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

**Choose the Networks Snort Should Inspect and Whitelist**

**Home Net**  [View List](#)  
default  
passlist\_48475  
Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs.  
Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.

**External Net**  [View List](#)  
Choose the External Net you want this interface to use.  
External Net is networks that are not Home Net. Most users should leave this setting at default.  
Create a Pass List and add an Alias to it, and then assign the Pass List here for custom External Net settings.

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).

Services / Snort / Interfaces ?

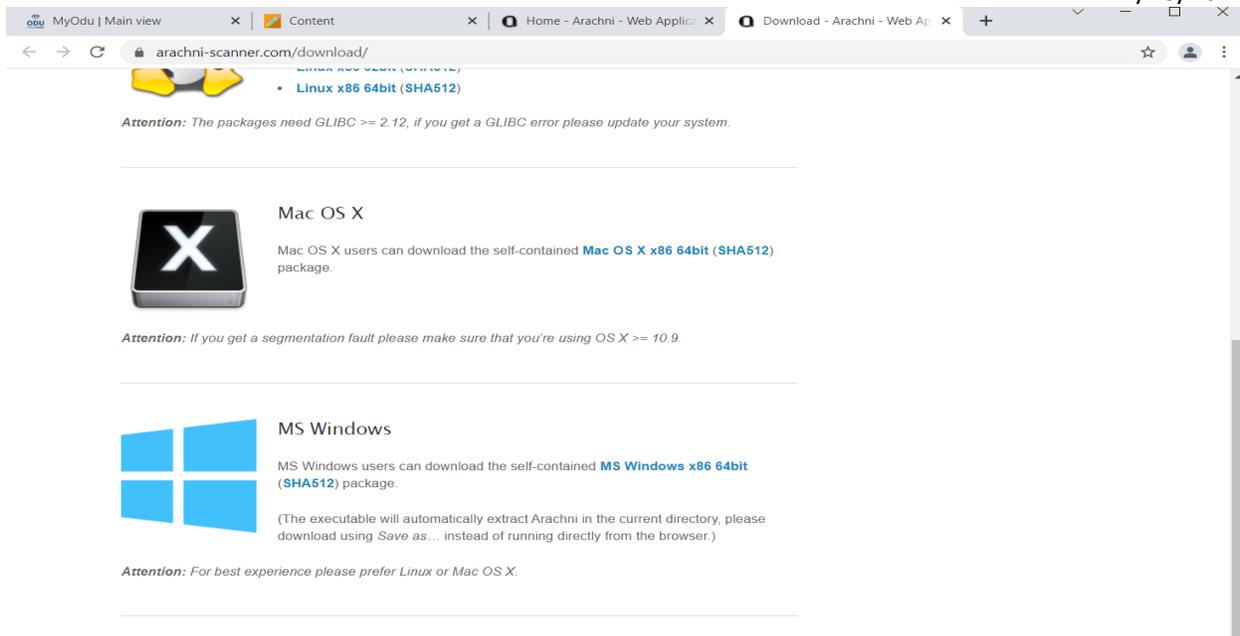
[Snort Interfaces](#) [Global Settings](#) [Updates](#) [Alerts](#) [Blocked](#) [Pass Lists](#) [Suppress](#) [IP Lists](#) [SID Mgmt](#) [Log Mgmt](#) [Sync](#)

**Interface Settings Overview**

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input checked="" type="checkbox"/> WAN (em0)	<span style="color: green;">✔</span> <span>↻</span> <span>🔒</span>	AC-BNFA	LEGACY MODE	WAN	<span>✎</span> <span>🗑️</span>
<input type="checkbox"/> LAN (em1)	<span style="color: green;">✔</span> <span>↻</span> <span>🔒</span>	AC-BNFA	DISABLED	LAN	<span>✎</span> <span>🗑️</span>

🗑️ Delete

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).



Attention: The packages need GLIBC >= 2.12, if you get a GLIBC error please update your system.

---

 **Mac OS X**

Mac OS X users can download the self-contained [Mac OS X x86 64bit \(SHA512\)](#) package.

Attention: If you get a segmentation fault please make sure that you're using OS X >= 10.9.

---

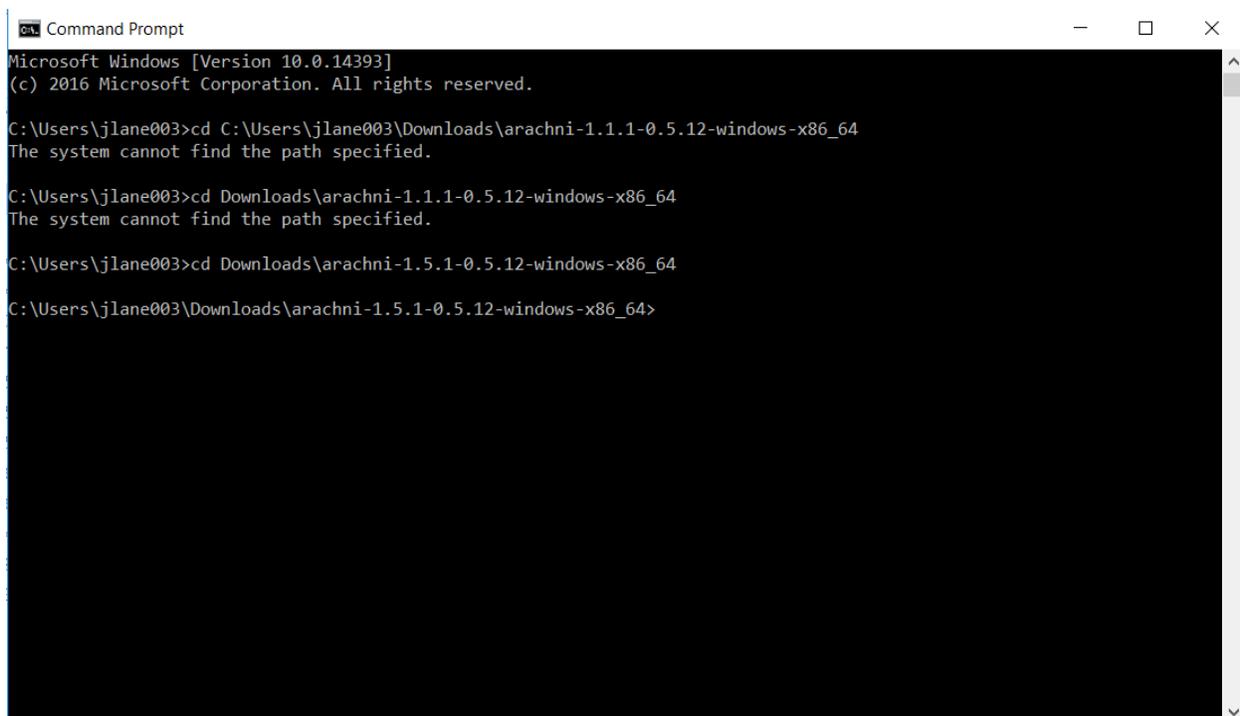
 **MS Windows**

MS Windows users can download the self-contained [MS Windows x86 64bit \(SHA512\)](#) package.

(The executable will automatically extract Arachni in the current directory, please download using Save as... instead of running directly from the browser.)

Attention: For best experience please prefer Linux or Mac OS X.

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).



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\jlane003>cd C:\Users\jlane003\Downloads\arachni-1.1.1-0.5.12-windows-x86_64
The system cannot find the path specified.

C:\Users\jlane003>cd Downloads\arachni-1.1.1-0.5.12-windows-x86_64
The system cannot find the path specified.

C:\Users\jlane003>cd Downloads\arachni-1.5.1-0.5.12-windows-x86_64
C:\Users\jlane003\Downloads\arachni-1.5.1-0.5.12-windows-x86_64>
```

```
C:\Users\jlane003\Downloads\arachni-1.5.1-0.5.12-windows-x86_64>cd bin
C:\Users\jlane003\Downloads\arachni-1.5.1-0.5.12-windows-x86_64\bin>dir
Volume in drive C has no label.
Volume Serial Number is 266B-6AEB

Directory of C:\Users\jlane003\Downloads\arachni-1.5.1-0.5.12-windows-x86_64\bin

03/28/2017  10:58 PM  <DIR>          .
03/28/2017  10:58 PM  <DIR>          ..
03/28/2017  10:58 PM                108 arachni.bat
03/28/2017  10:58 PM                108 arachni_console.bat
03/28/2017  10:58 PM                108 arachni_multi.bat
03/28/2017  10:58 PM                108 arachni_reporter.bat
03/28/2017  10:58 PM                108 arachni_reproduce.bat
03/28/2017  10:58 PM                108 arachni_restore.bat
03/28/2017  10:58 PM                108 arachni_rest_server.bat
03/28/2017  10:58 PM                108 arachni_rpc.bat
03/28/2017  10:58 PM                108 arachni_rpcd.bat
03/28/2017  10:58 PM                108 arachni_rpcd_monitor.bat
03/28/2017  10:58 PM                108 arachni_script.bat
03/28/2017  10:58 PM                141 arachni_shell.bat
03/28/2017  10:58 PM                139 arachni_web.bat
03/28/2017  10:58 PM                127 arachni_web_change_password.bat
03/28/2017  10:58 PM                123 arachni_web_create_user.bat
```

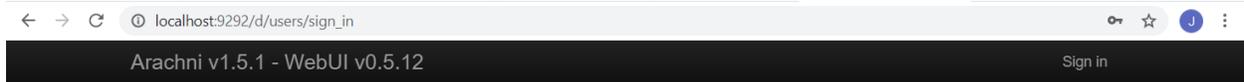
As shown in the screenshot above, proceed to use arachni\_web command to start the scan. Once this is done, you will see a “accessible by tcp.localhost:9292” or similar syntax. Open a web browser and proceed to type <http://localhost:9292> and it should bring you to a web UI for arachni. Log in with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



## Sign in

Please consult the Wiki for default credentials.

Email

admin@admin.admin

Password

.....

Remember me

Sign in

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

http://192.168.101.2/

Edit description

✓ The scan completed in 00:00:22 .

## Issues [3]

All [3]

\* Fixed [0]

✓ Verified [0]

ⓘ Pending verification [0]

✗ False positives [0]

ⓘ Awaiting review [0]

Listing all logged issues.

TOGGLE BY SEVERITY

Reset Show all Hide all

Low 1

Informational 2

NAVIGATE TO

Missing 'X-Frame-Options' h 1

Interesting response 1

Allowed HTTP methods 1

URL

Input

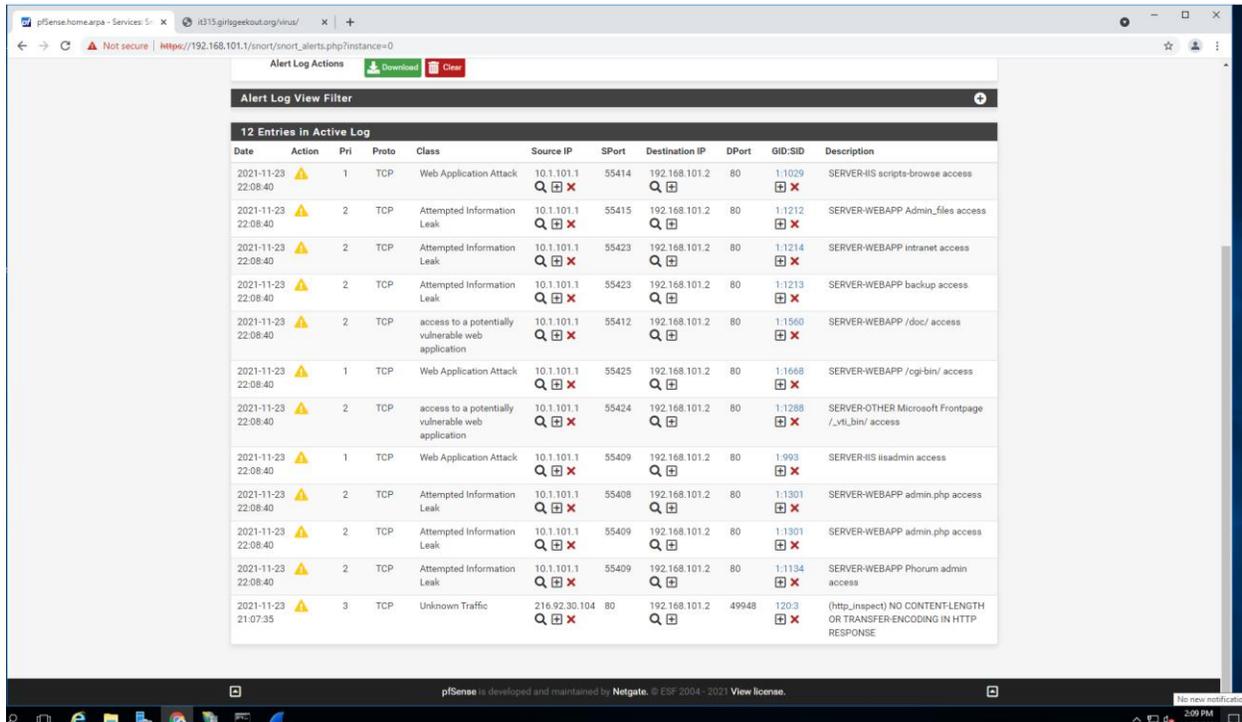
Element

Missing 'X-Frame-Options' header 1

Interesting response 1

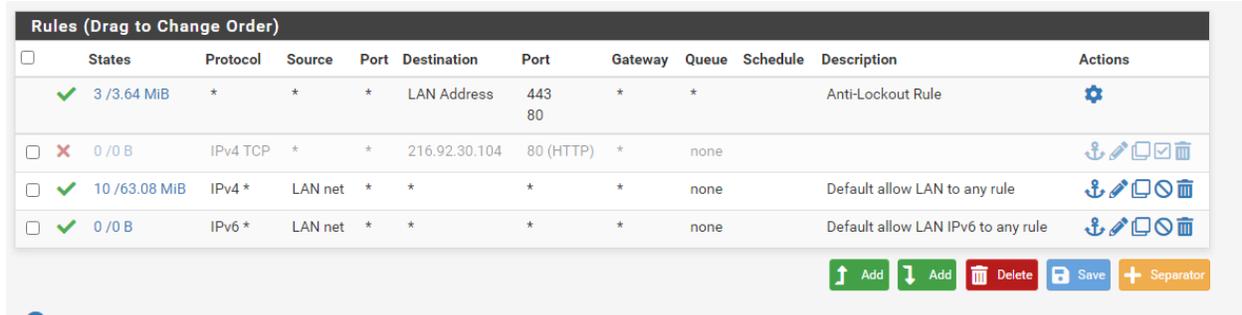
Allowed HTTP methods 1

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

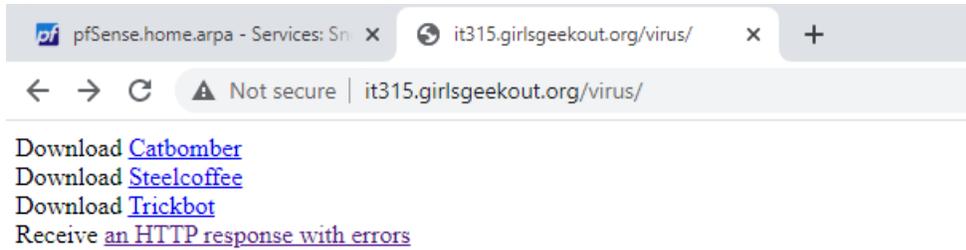


You can then create a rule under firewall rules on the WAN interface for blocking this IP address that scanned the internal network. It is possible to spoof your IP address, so this may not be an ample rule if the attacker has more resources at their disposal.

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/](http://it315.girlsgeekout.org/virus/)) and click HTTP response with errors (below).



Here is the alert generate from this download on Snort:

A screenshot of the pfSense web interface showing the Snort Alerts page. The breadcrumb trail is "Services / Snort / Alerts". The "Alerts" tab is selected in the navigation menu. The "Alert Log View Settings" section shows "Interface to Inspect" set to "WAN (em0)", "Auto-refresh view" unchecked, and "Alert lines to display" set to "250". The "Alert Log Actions" section has "Download" and "Clear" buttons. The "Alert Log View Filter" section has a "+" button. Below, the "1 Entries in Active Log" section shows a table with one entry:

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2021-11-23 21:07:35		3	TCP	Unknown Traffic	216.92.30.104	80	192.168.101.2	49948	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE

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:

Think the difference between block and reject is that with reject, a packet (for TCP or ICMP) gets unacknowledged (or sent) returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**  **Disable this rule**  
Set this option to disable this rule without removing it from the list.

**Interface**   
Choose the interface from which packets must come to match this rule.

**Address Family**   
Select the Internet Protocol version this rule applies to.

**Protocol**   
Choose which IP protocol this rule should match.

**Source**

**Source**  **Invert match**   /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

**Destination**

**Destination**  **Invert match**   /

**Destination Port Range**      
From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**Extra Options**

**Log**  **Log packets that are handled by this rule**  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

**Description**   
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** [Display Advanced](#)

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

System / [Advanced](#) / [Admin Access](#) ?

[Admin Access](#) [Firewall & NAT](#) [Networking](#) [Miscellaneous](#) [System Tunables](#) [Notifications](#)

**webConfigurator**

**Protocol**  HTTP  HTTPS (SSL/TLS)

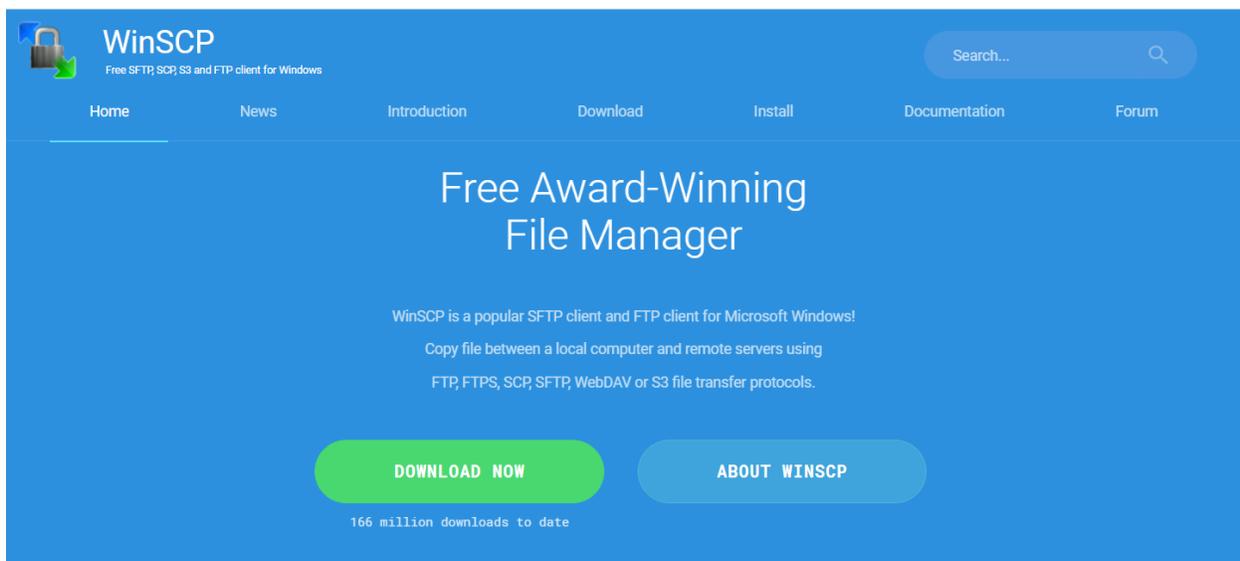
**SSL/TLS Certificate**   
Certificates known to be incompatible with use for HTTPS are not included in this list.

**TCP port**   
Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.

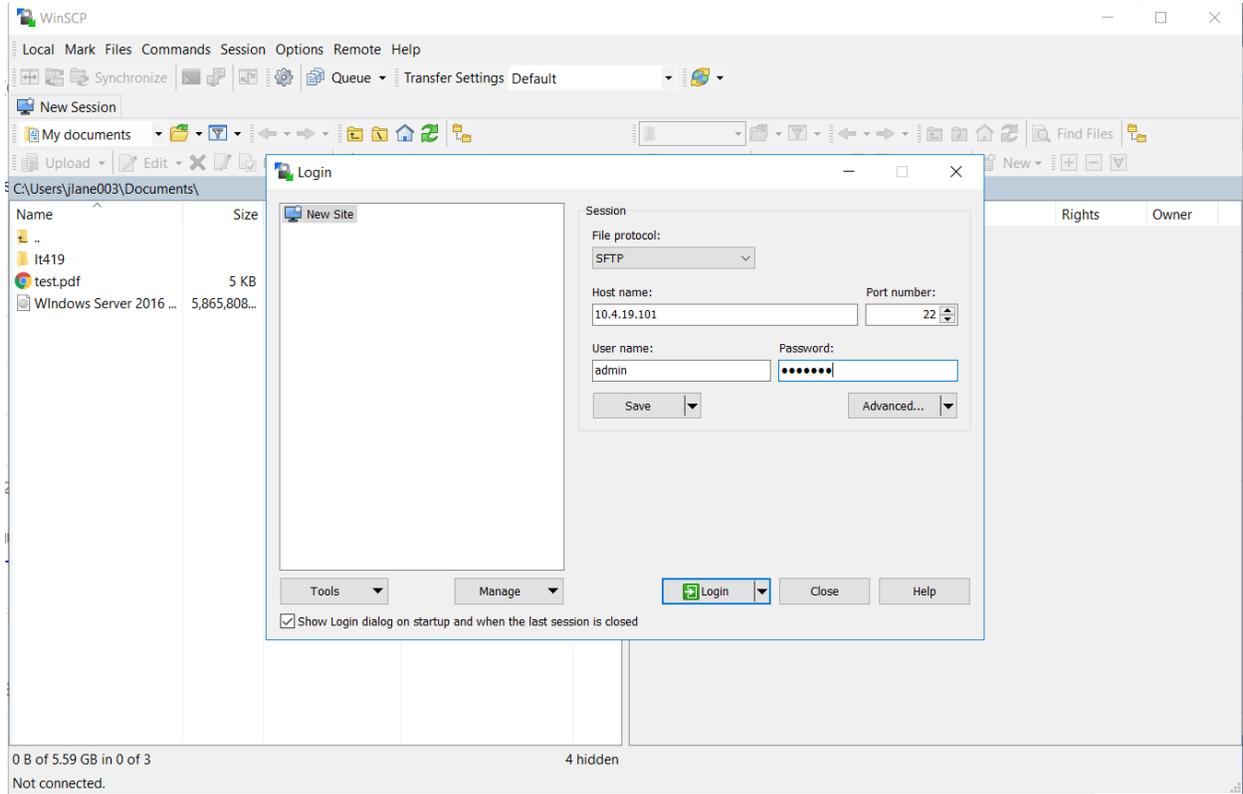
Secure Shell	
Secure Shell Server	<input checked="" type="checkbox"/> Enable Secure Shell
SSHD Key Only	<input type="text" value="Password or Public Key"/> <small>When set to <i>Public Key Only</i>, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to <i>Require Both Password and Public Key</i>, the SSH daemon requires both authorized keys <b>and</b> valid passwords to gain access. The default <i>Password or Public Key</i> setting allows either a valid password or a valid authorized key to login.</small>
Allow Agent Forwarding	<input type="checkbox"/> Enables ssh-agent forwarding support.
SSH port	<input type="text" value="22"/> <small>Note: Leave this blank for the default of 22.</small>

Login Protection

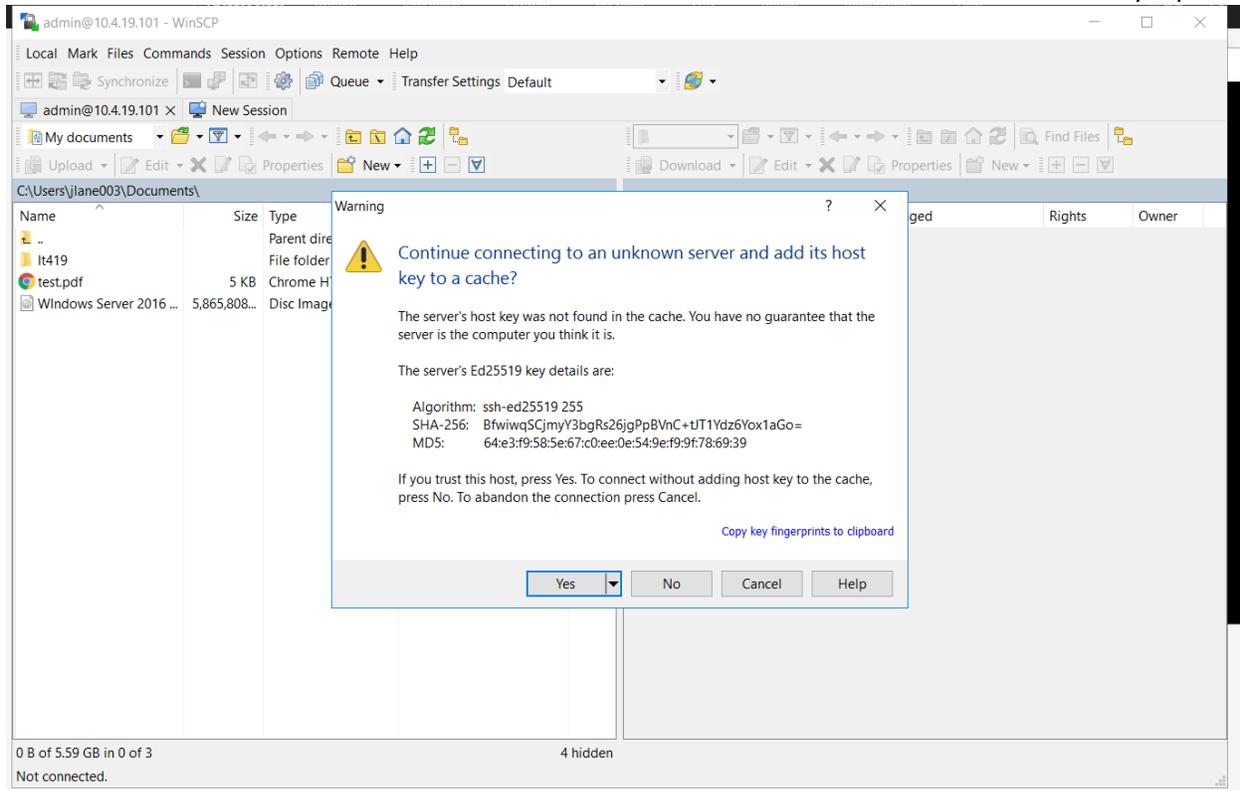
Next, download SFTP client as shown on the next page:



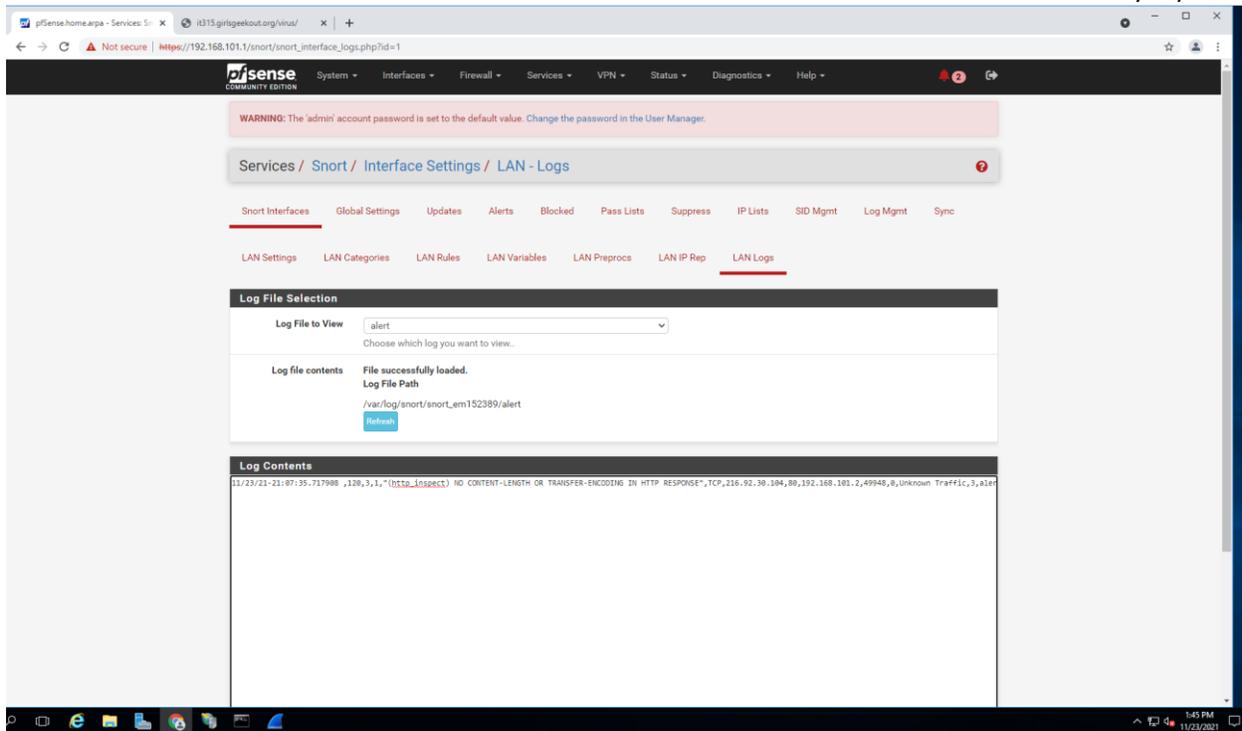
Once this is downloaded and installed, proceed to connect to your pfSense firewall through the SFTP client. Click the folder with 2 dots and type in the Public IP address for your pfSense firewall in the host box. Insert your credentials for pfSense and click Login (screenshot on next page).



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

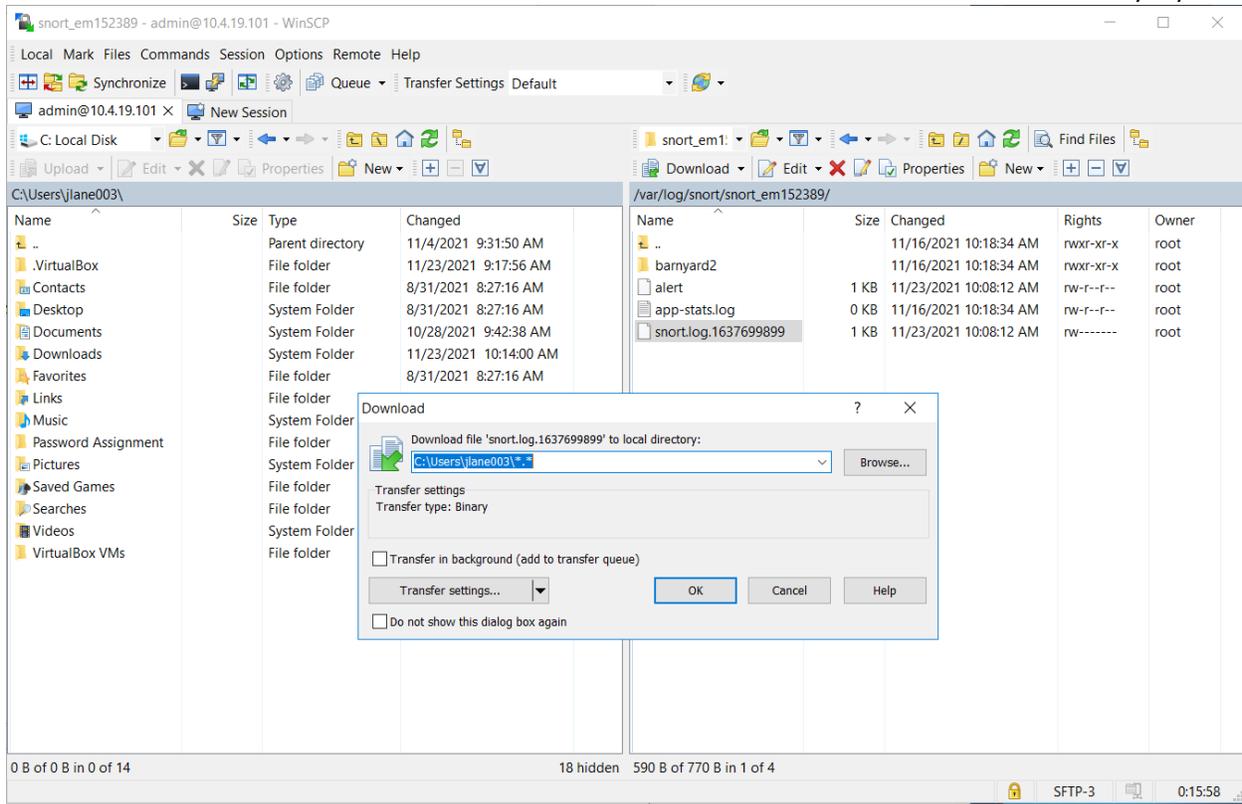


In order to locate exactly where the alert log you want is, you must navigate to Services>Snort>Interface Settings>LAN – Logs. The file path will be displayed there (screenshot on next page):

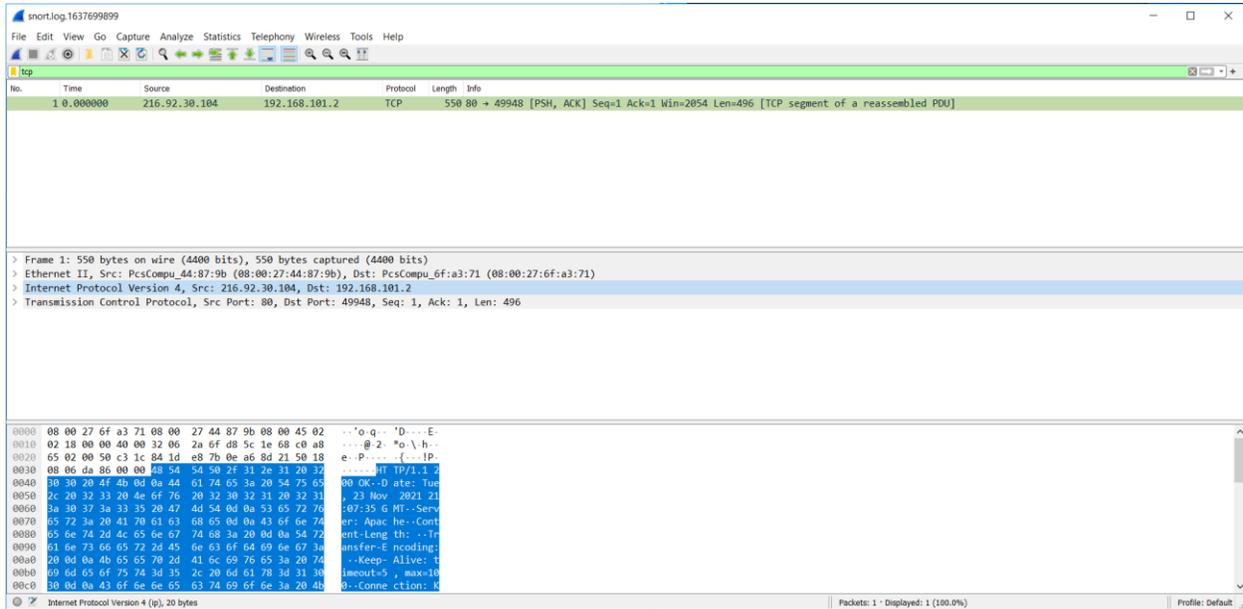


Go back into the SFTP client and navigate to the file path previously as shown and click OK

(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).