

Lab 7

IDPS Lab- pfSense Setup

ITSC 206: Advanced Networking for Offensive and Defensive Environments

Table of Contents

[Lab Setup 2](#_Toc510374345)

[Files/Download 2](#_Toc510374346)

[Reading 2](#_Toc510374347)

[Introduction 2](#_Toc510374348)

[Use pfSense Firewall VM IDPS Setup 2](#_Toc510374349)

[Firewall IDPS (Snort) Installation 3](#_Toc510374350)

[IDPS Snort Setup 7](#_Toc510374351)

[Kali OpenVAS 13](#_Toc510374352)

Lab Setup

* Review architecture for each configuration and optimize.

Files/Download

Reading

* [https://doc.pfsense.org/index.php/Installing\_pfSense#](https://doc.pfsense.org/index.php/Installing_pfSense)

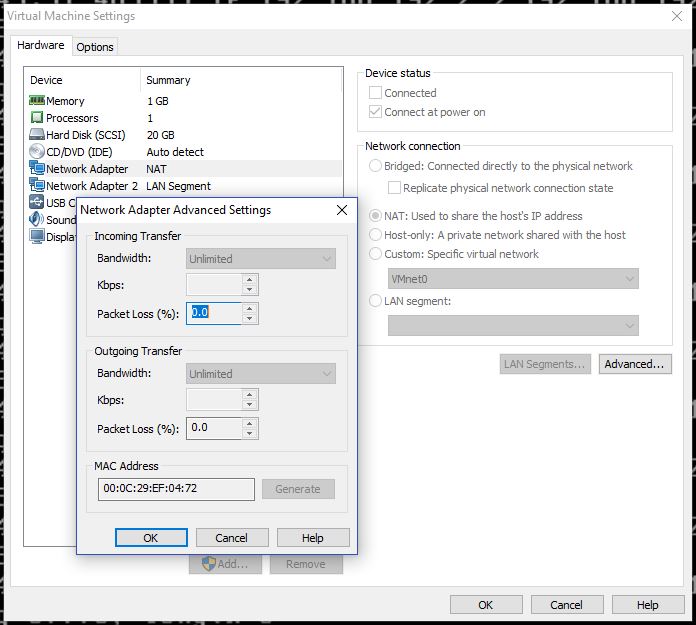
Introduction

This document supports the setup of Lab7 IDPS.

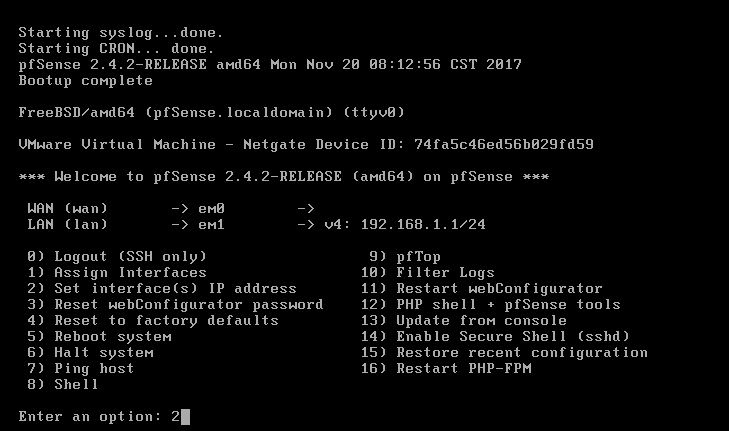
Use pfSense Firewall VM IDPS Setup

Setup pfSense with the following attributes in the VM Player:

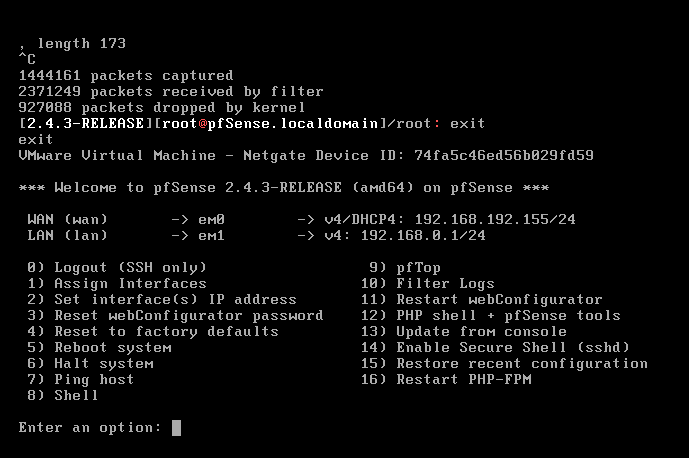
1. Shutdown the VM of the firewall and then change the Network Adapter LANSegment1 (WAN) to NAT



1. Restart the pfSense Firewall VM, confirm that the WAN interface gets an IP address via DHCP, you may need to use step 11 of Lab6 Setup doc and setup DHCP



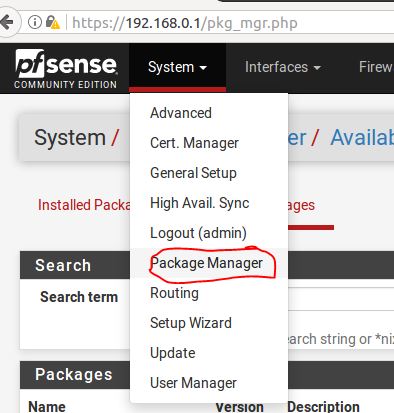
1. Start up the Firewall



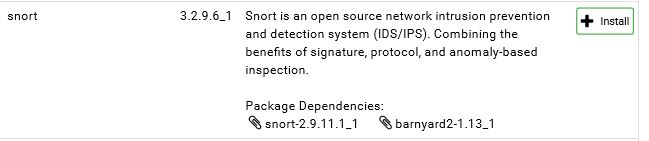
Firewall IDPS (Snort) Installation

Setup pfSense with IDPS following these steps:

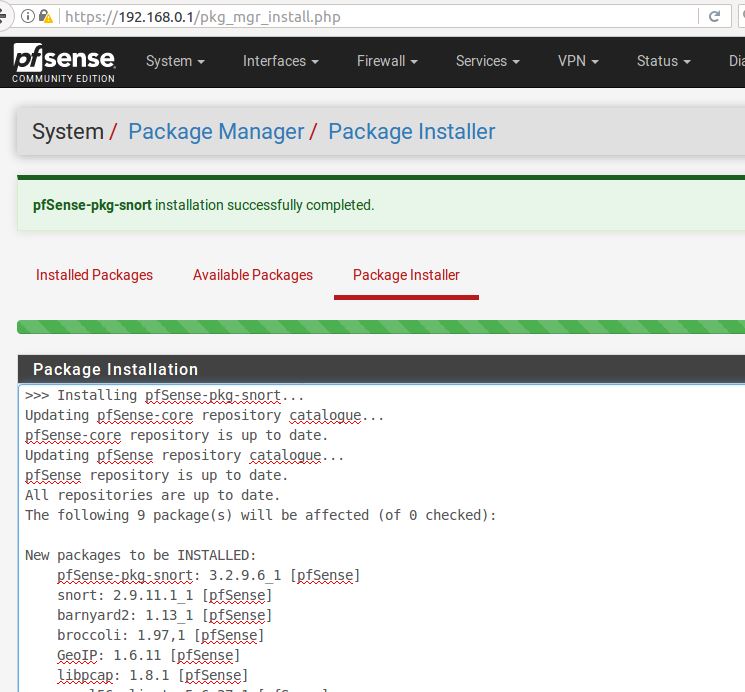
1. From the pfSense Firewall interface, login and select System->Package Manager



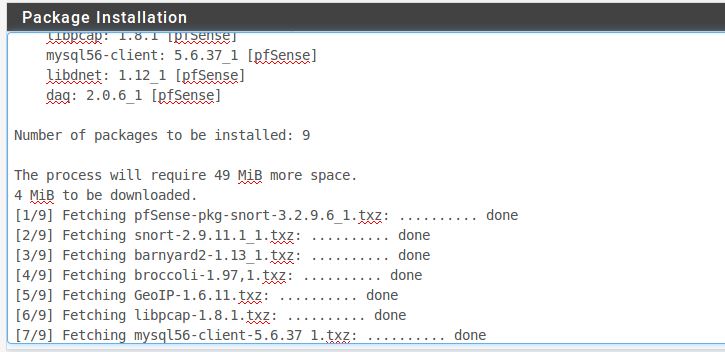
1. Click on Available Packages tab for different category of software to be installed, Snort install



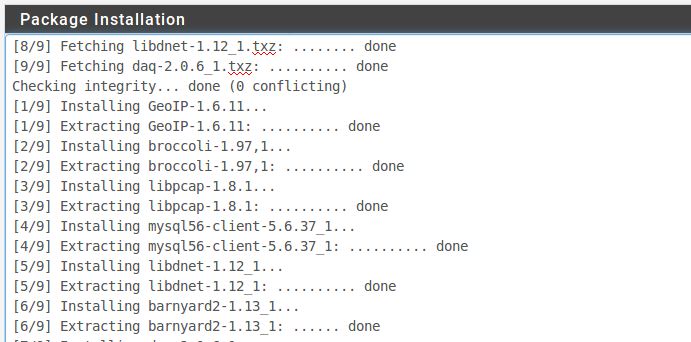
1. pfSense Snort Package Installation status



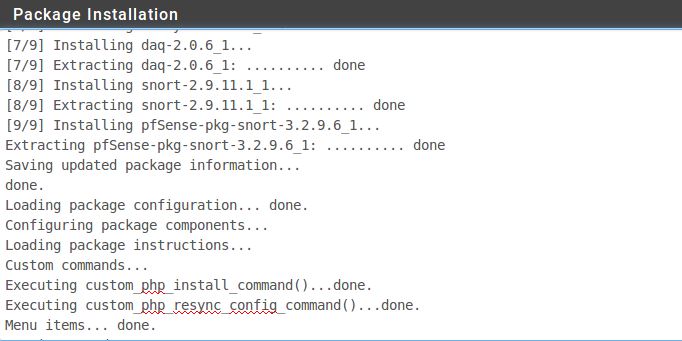
1. pfSense Snort Package Installation status cont



1. pfSense Snort Package Installation status cont



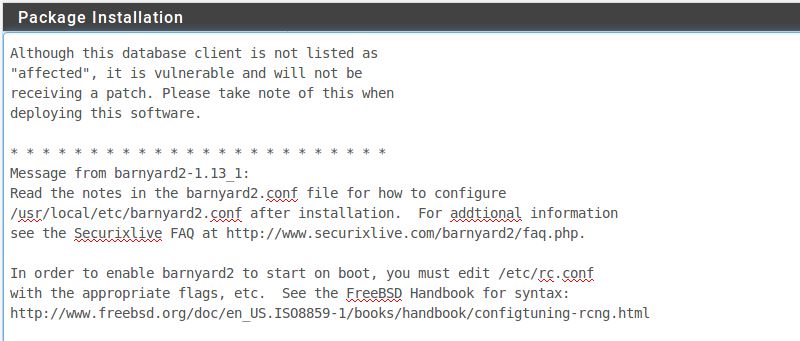
1. pfSense Snort Package Installation status cont



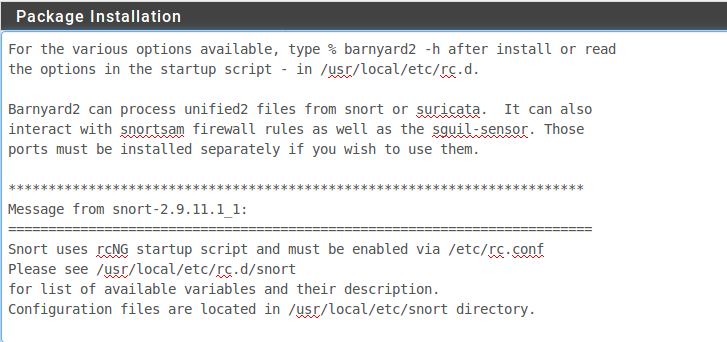
1. pfSense Snort Package Installation status cont



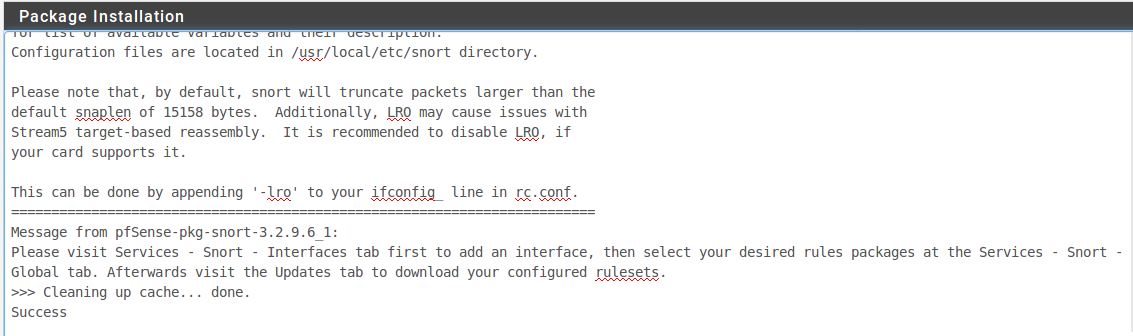
1. pfSense Snort Package Installation status cont



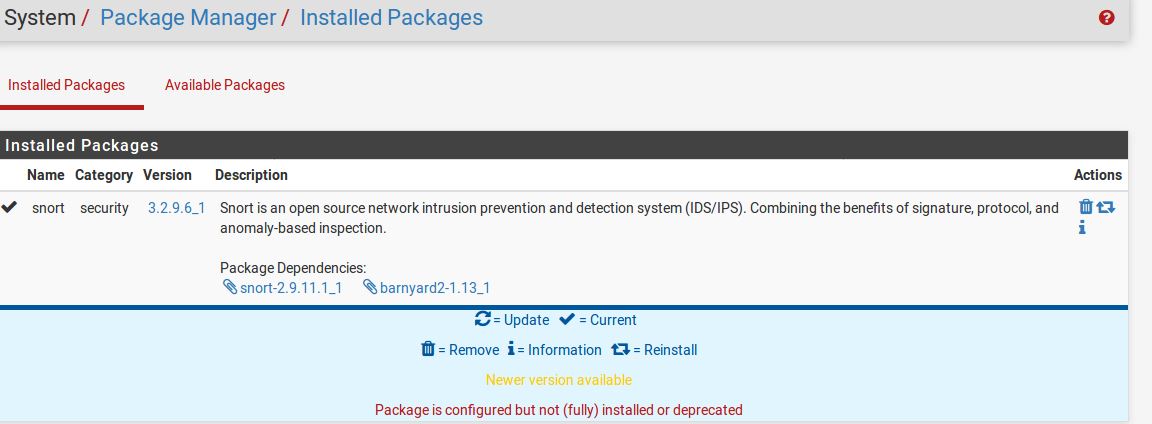
1. pfSense Snort Package Installation status cont



1. pfSense Snort Package Installation status cont

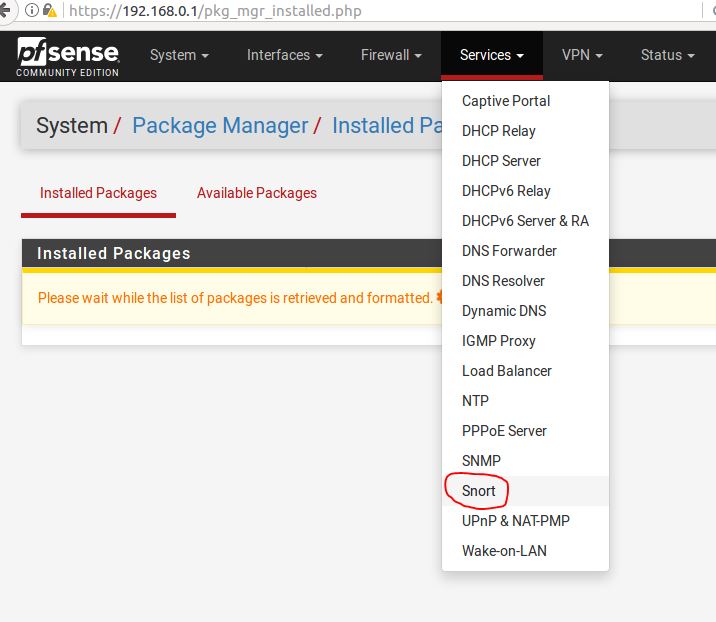


1. pfSense Snort Package Installation status cont

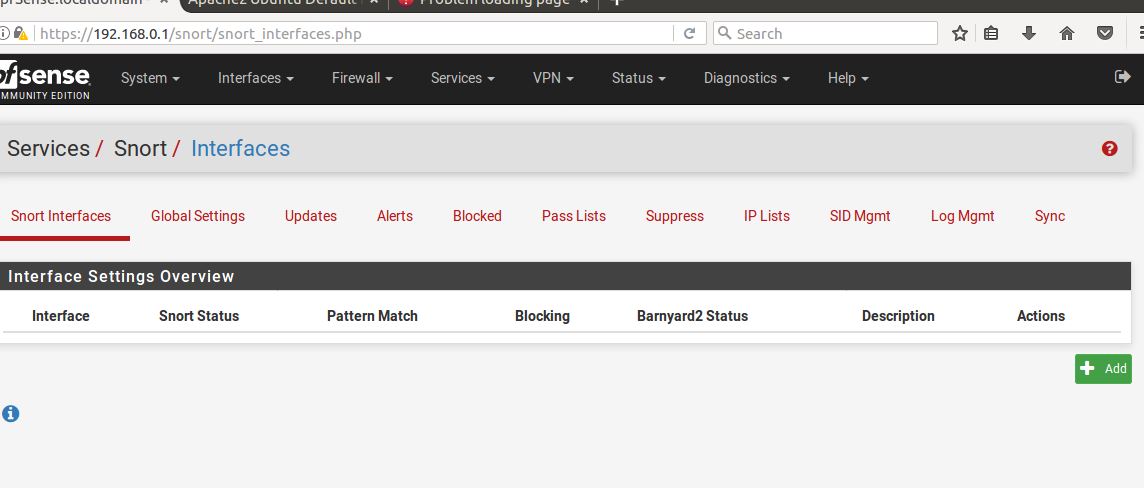


IDPS Snort Setup

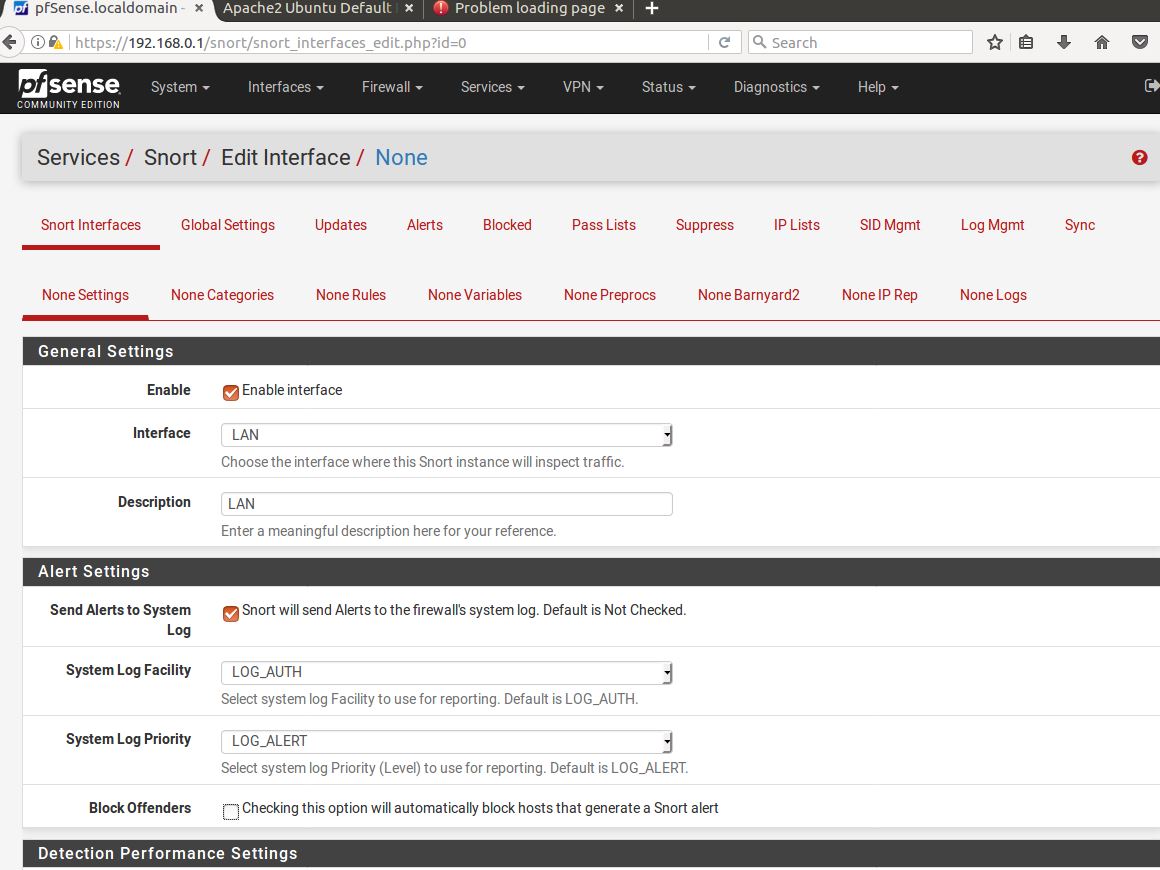
1. pfSense Snort setup, to to Services->Snort



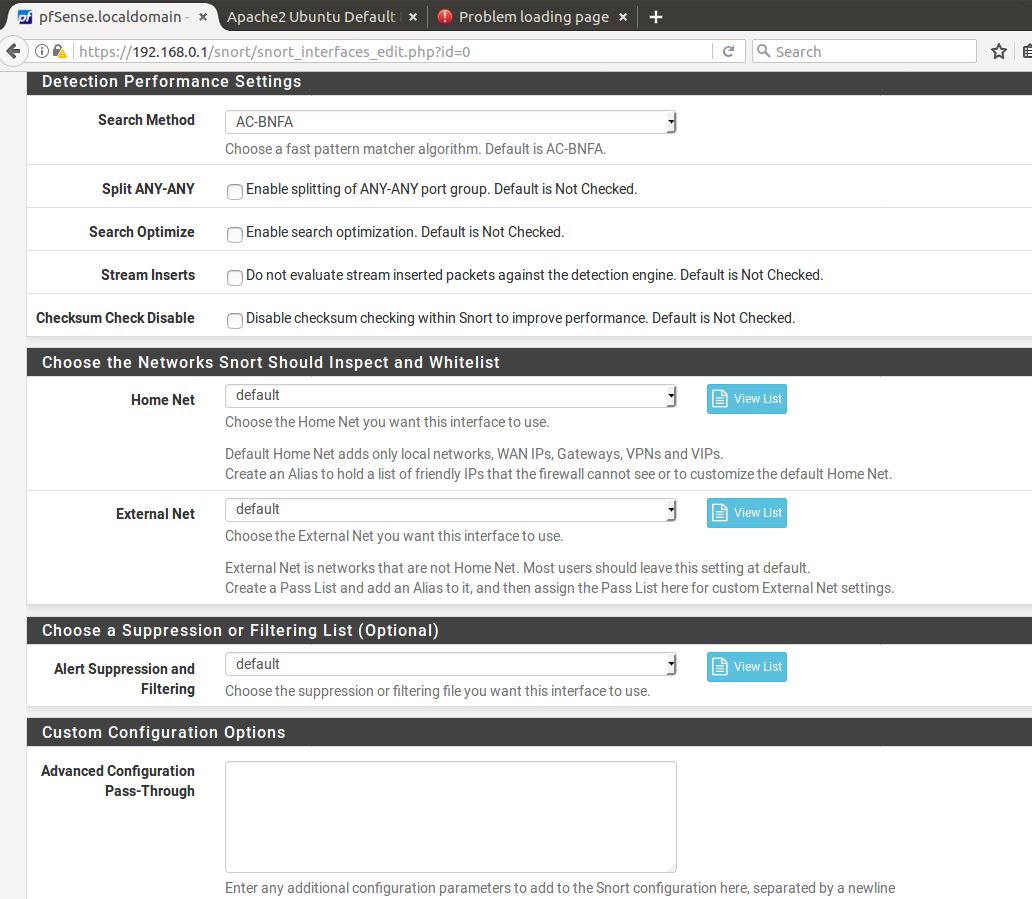
1. Snort Interfaces, click Add



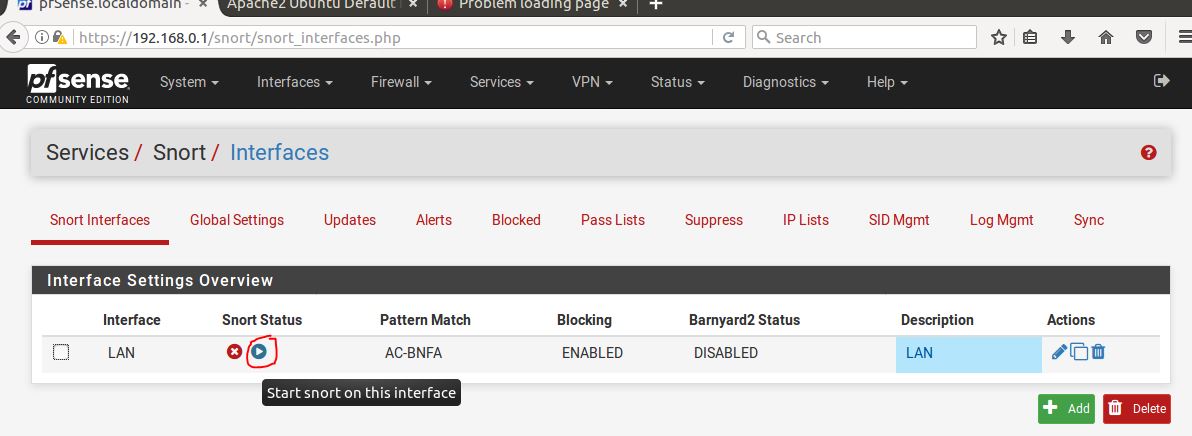
1. See interface settings below:



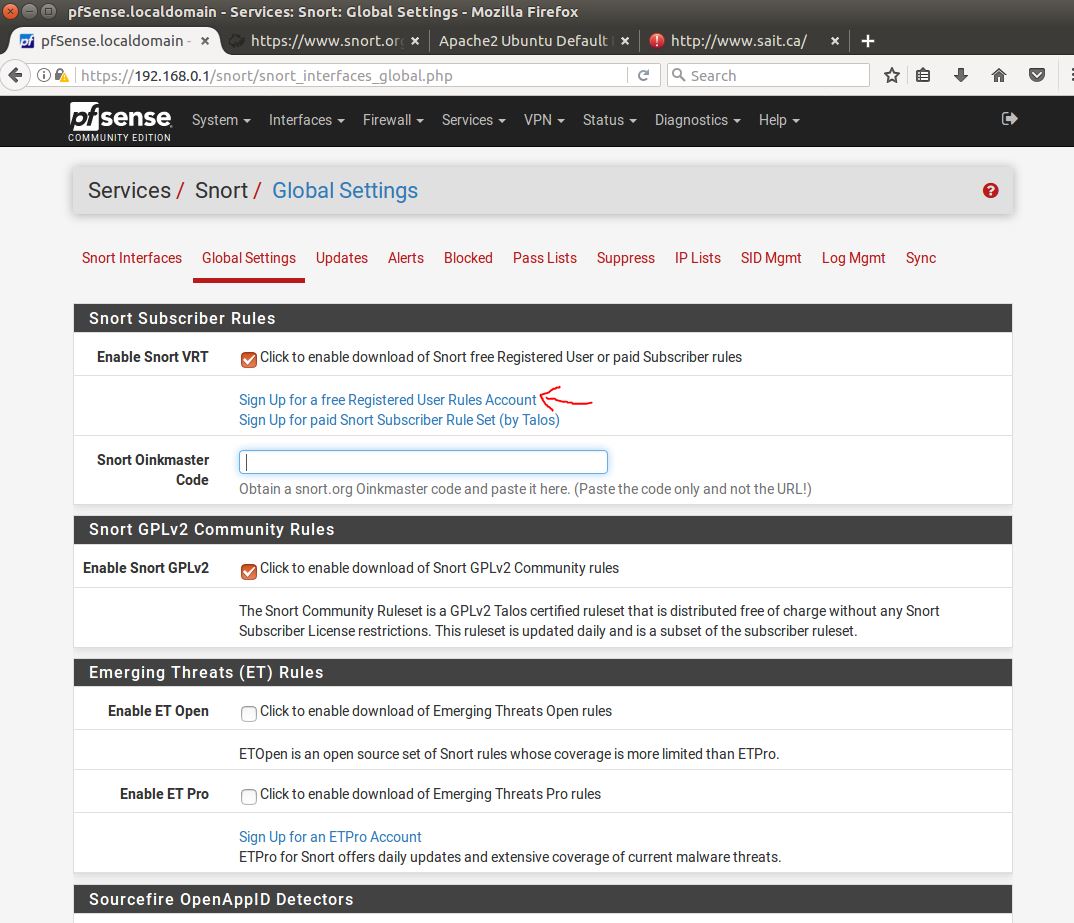
1. Continue with following interface settings and then Save:



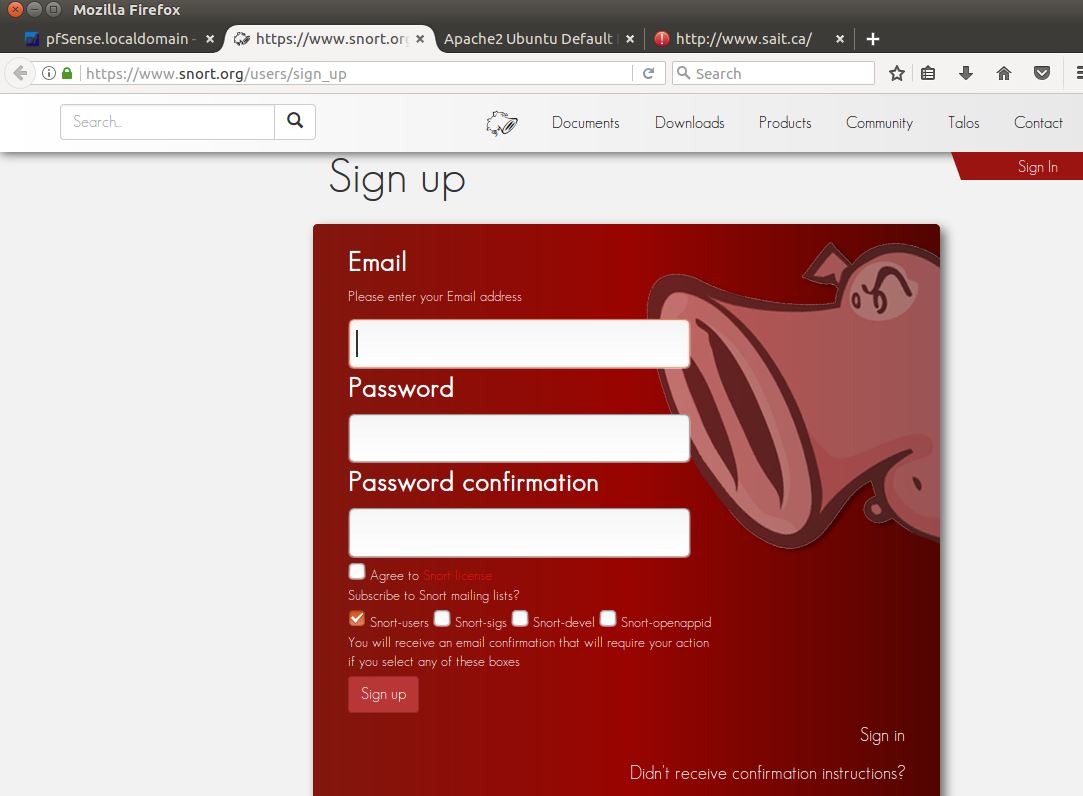
1. pfSense Service Snort Interfaces, press Start



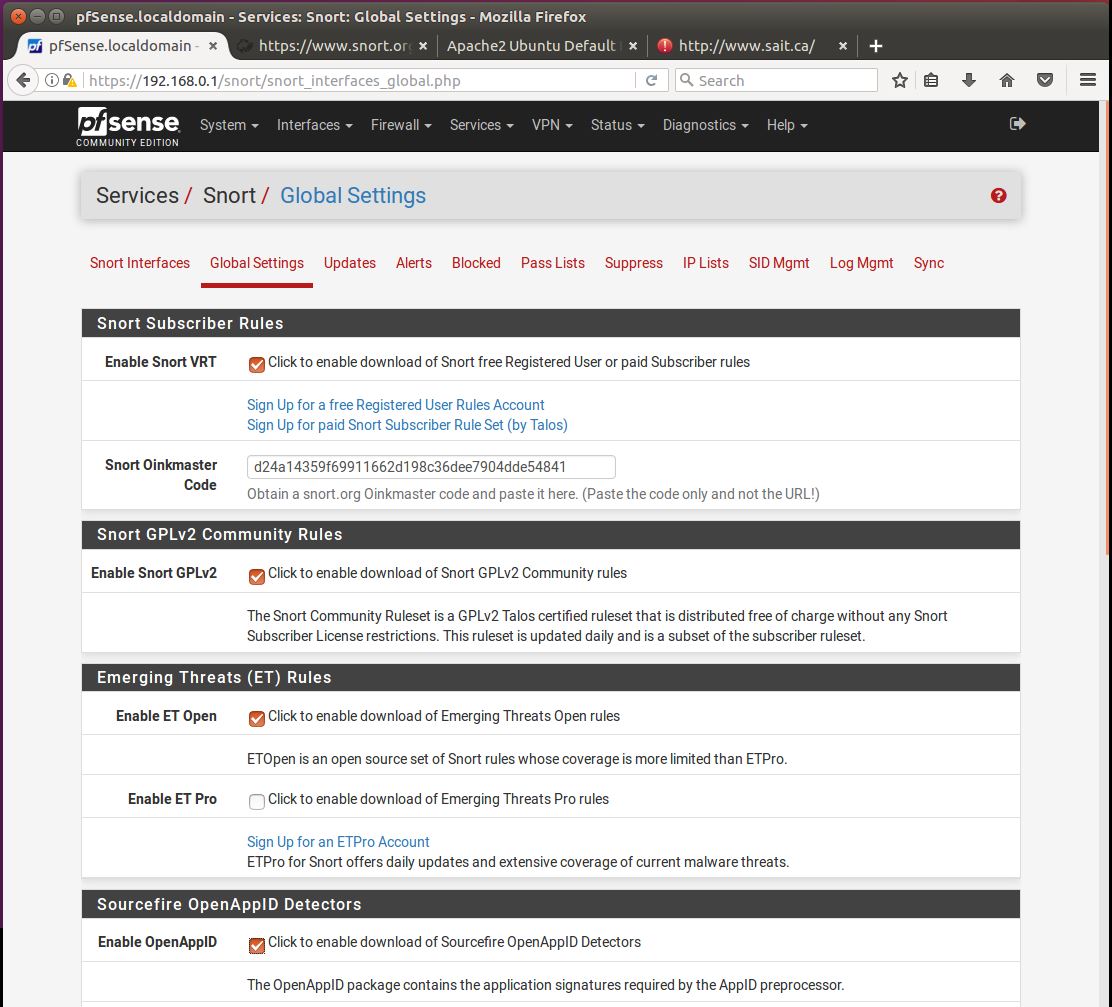
1. pfSense Service Snort Global Settings, click on Sign up for a Registered User Rules Account



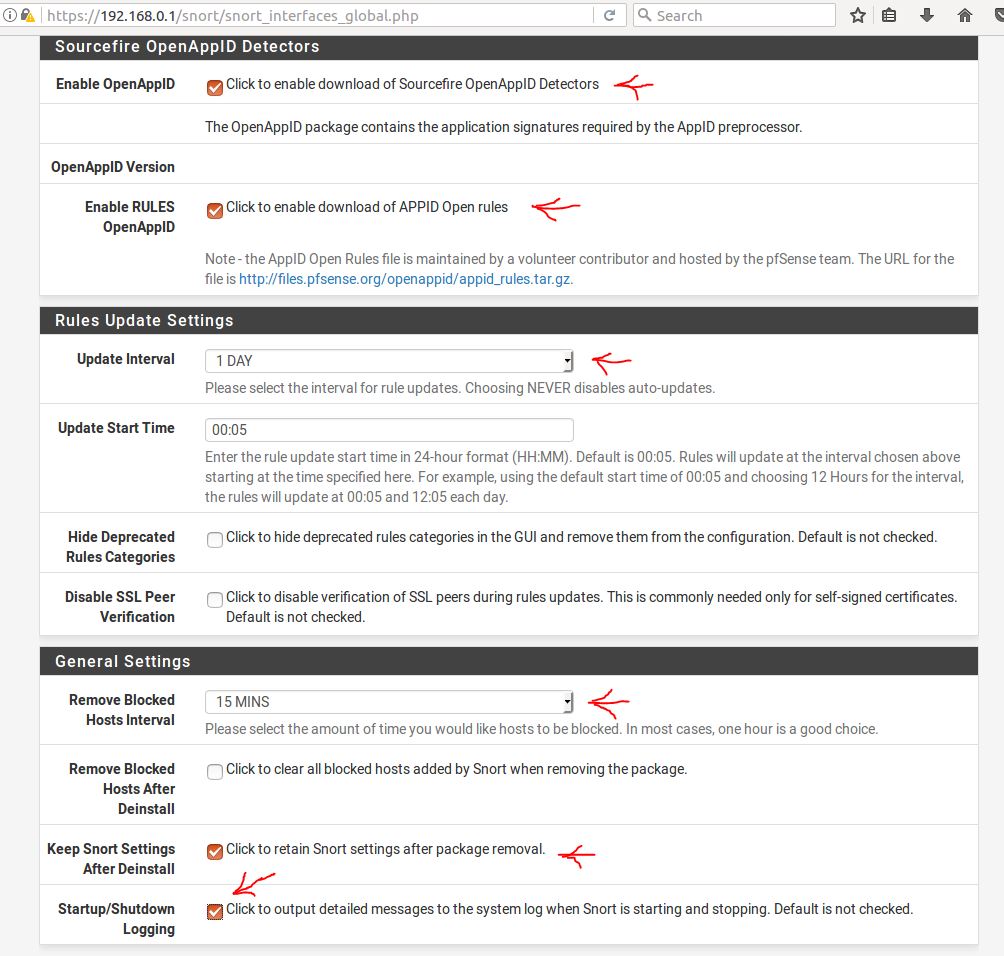
1. Sign up for Snort account to get Oinkmaster Code,



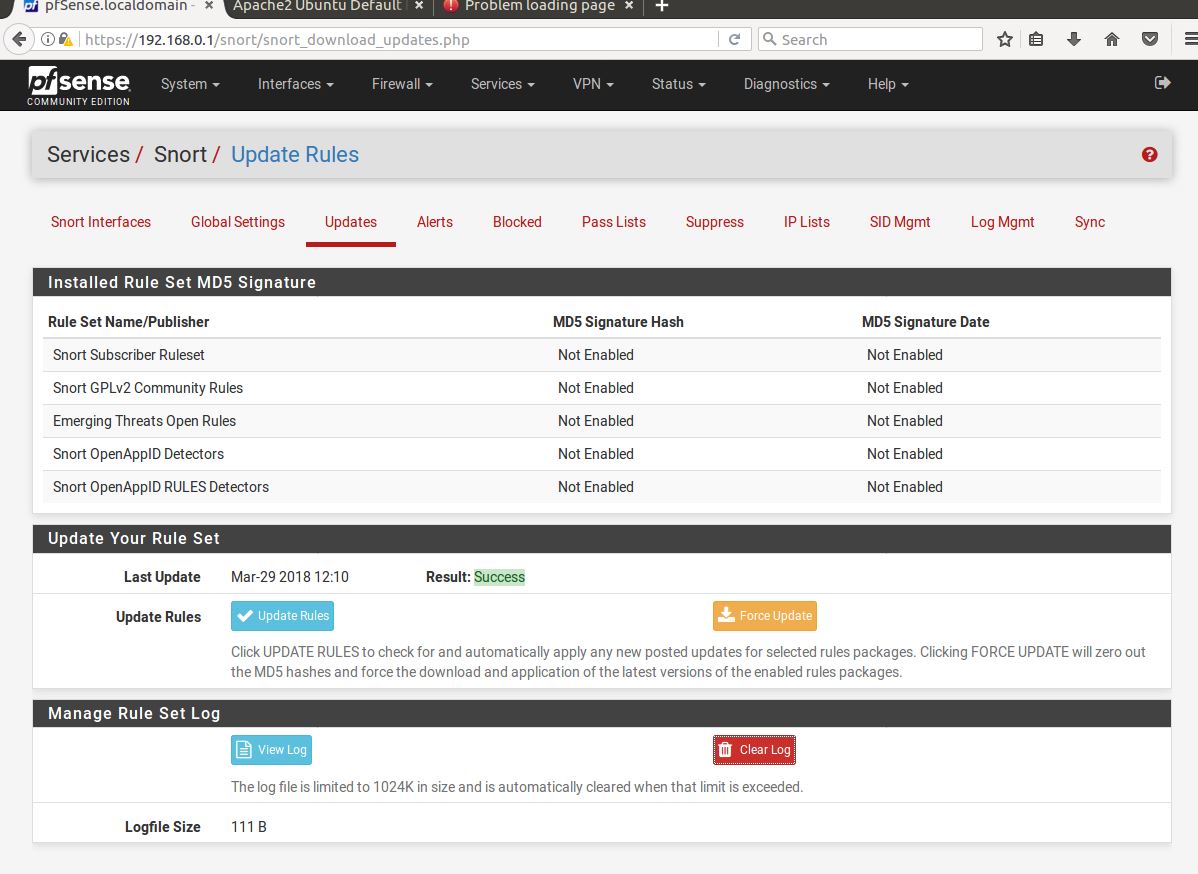
1. pfSense Services Snort Global Settings, Oinkmaster code entered and rest of the settings



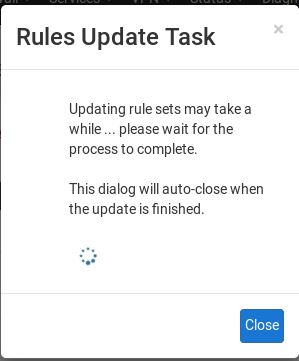
1. pfSense Services Snort Global Settings, Oinkmaster code entered and rest of the settings, cont and click on Save at the bottom



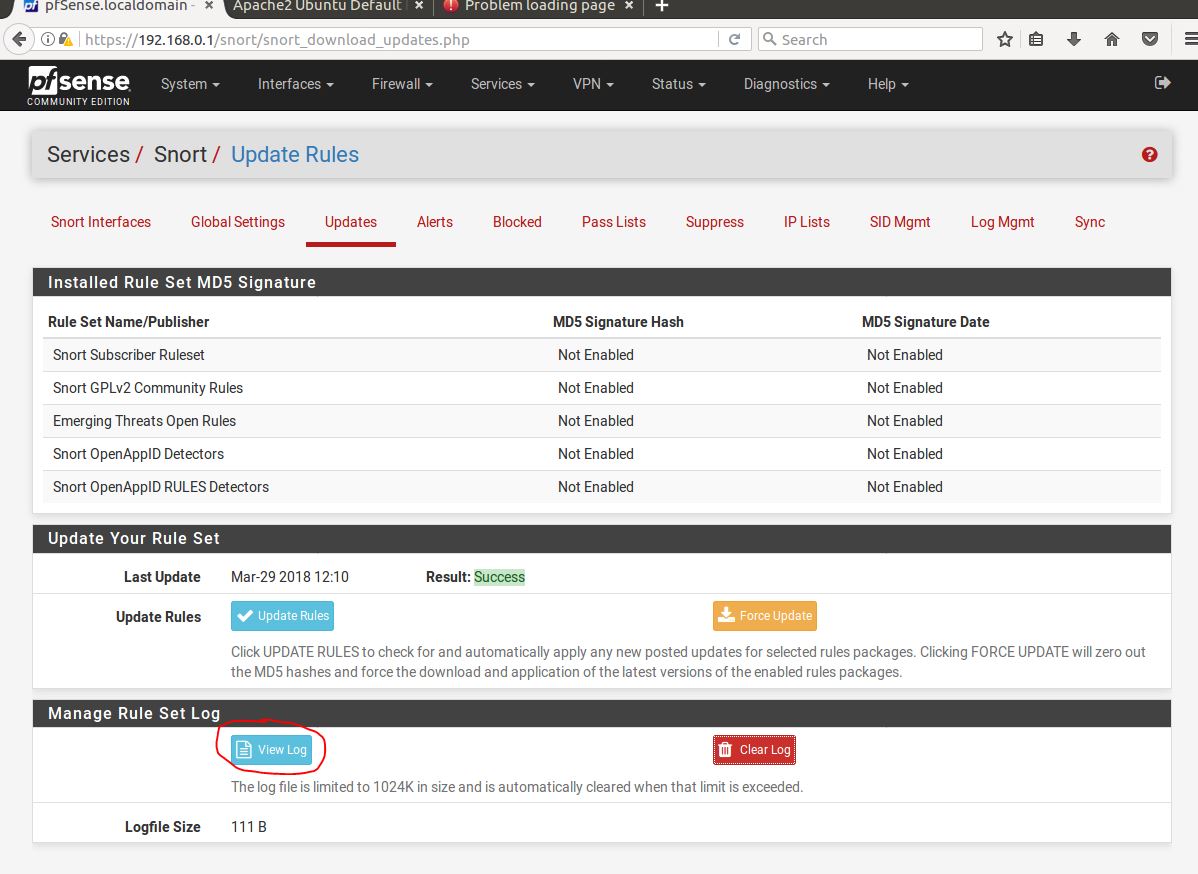
1. pfSense Services Snort Update Rules, click Update Rules



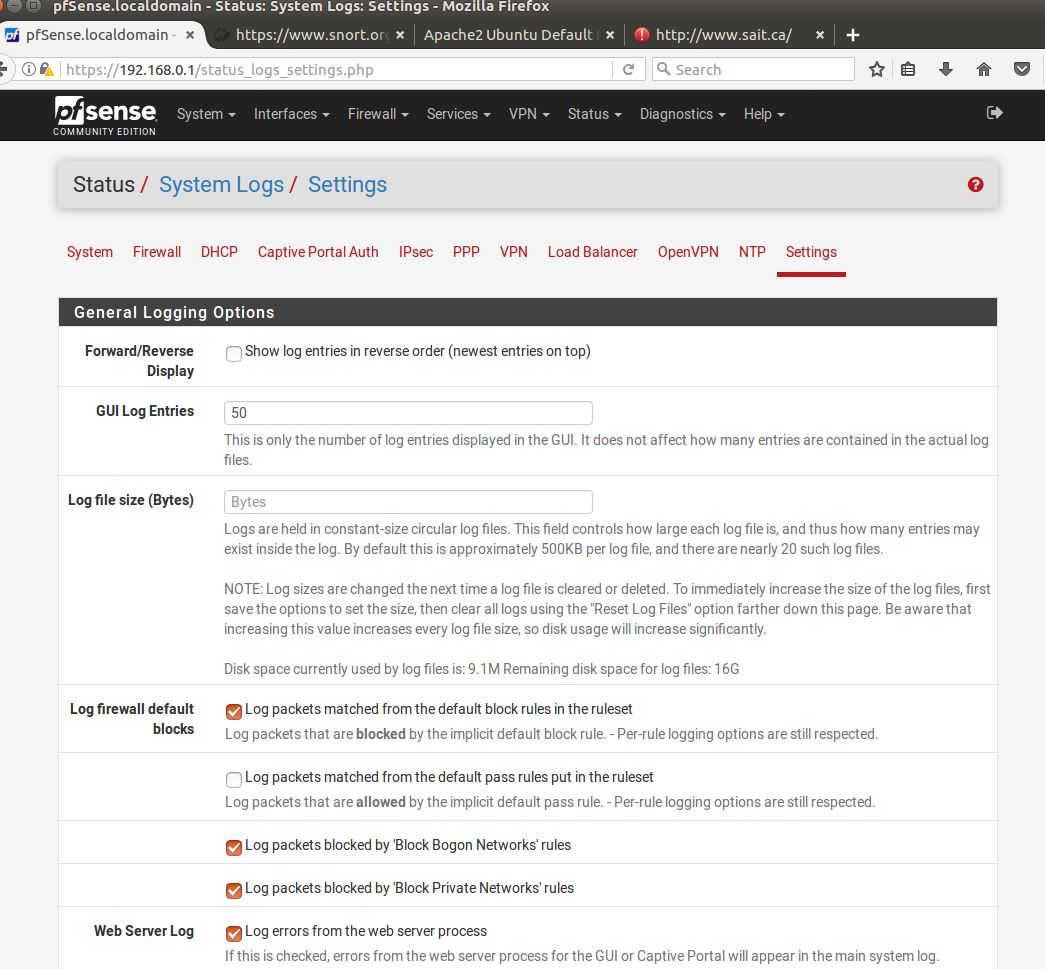
1. pfSense Services Snort Rule update log



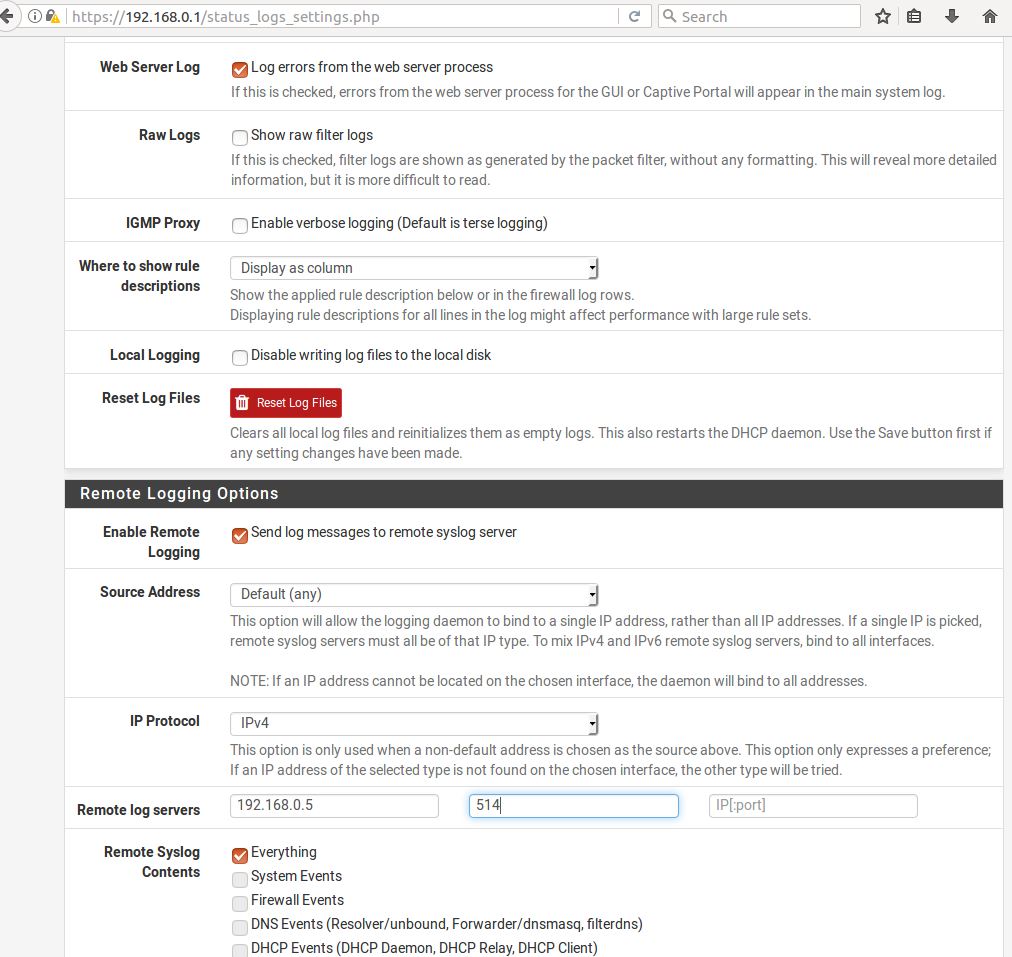
1. pfSense Services Snort Rule View log



1. pfSense Firewall Status->System Logs ->Settings, configure logging options



1. pfSense Firewall Status->System Logs ->Settings, configure logging options, press Save



1. a

Kali OpenVAS

1. Install an Kali by entering the following commands:
   1. sudo apt install openvas
   2. sudo openvas-setup
   3. openvas-check-setup (if errors and missing SCAP database and Cert database)
   4. gsad (depending on the step the error occur, use openvas-check-setup as needed)
   5. greenbone-scapdata-sync
   6. greenbone-certdata-sync
   7. openvas-check-setup (if errors only in step 10 [optional])
   8. service openvas-scanner restart
   9. service openvas-manager restart

Hints:

**DO NOT DELETE THE SECTION BREAK BELOW. DELETING IT MAY IMPACT THE FORMATTING IN THIS DOCUMENT.**