**Project Name:  Understanding Firewalls, Initial Review**

**Technology:  Packet Filtering**

**Market:  Security**

**Name / Group: Gagneet Sahota**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Potential Providers:**

pf

a.k.a. Packet Filter, from OpenBSD, available in (OpenBSD, FreeBSD, NetBSD, Mac OS, Solaris, etc.)

iptables

a.k.a. Formerly: ipchains, Future: netfilter tables (Linux)

IPFilter

a.k.a. ipf (OpenBSD, FreeBSD, Solaris, Linux, etc.)

**Intended Activities:**

Firewall Appliance Installation: pfsense

**Design:**

The goal of this lab is to begin to become familiar with one of the primary environments that will be used in this course.  In order to do so, we must become accustomed to installing and updating a firewall. Even if people have been working systems for a long period of time, they will notice changes in the evolution of systems over the years.

**Directions:**

Answer the questions below in preparation for the practical portion of your lab (in Section 3).

**Questions to Answer:**

**Section 0:  Lab Basics**

Explain the following terms:

Checksums / Sums / Hashes- A number to identify if a file has been modified, if the number on your machine is the same as the location of the download, your file has not been modified and is ensured confidentiality .

ISO Image- An collection of files that are able to give the user an OS through a single file.

Firewall – a filter that runs on a configuration file.

Packet Filter- Something that filters packets

Unified Threat Management (UTM)- Adding more software to protect rather then just the layer 3 protection.

Next Generation Firewall (NGFW)- Having multiple built in defense mechanism’s such as a sandbox firewall.

Cloud Generation Firewall

* Allows traffic to passthrough an agency of a centralized location, works when may locations need to be protected.

**Section 1:  Lab Environment**

How would you define a firewall?

* A software that filters out traffic to prevent against attacks.

Said differently, What is a firewall?

* A network security device that monitors traffic to block traffic based on defined security rules.

What do firewalls offer our networks and systems in terms of security?

Where in your network is it important to place firewalls?

* In the fabric of the security and perimeter of traffic.

What aspects of security does a firewall not cover / protect against?

* Against users downloading malware or security vulnerabilities.

What is the importance of calculating checksums / sums / hashes on the files that you download that are intended for installation?

* TO ensure the software has not been tampered with

How do you calculate checksums for the file(s) that you downloaded.

Be specific.  Illustrate commands, etc.

In windows go the CMD and paste Get-FileHash C:\path\to\file.iso -Algorithm SHA1

Did you find that your checksums match your ISO image?

If so, indicate your matching checksum here.

* a4bac4b9cde96b1775141666f92b40992437303520a1bad2f2b8e7f50f775834

What does it mean if your checksums match?

* You know the file’s are identical and haven’t been modified by someone else

What does it mean if your checksums do not match?

* The file has been modified, potentially by the bad guys.

What is the scope of network protection that you believe can be accomplished with pfSense.

Give examples.

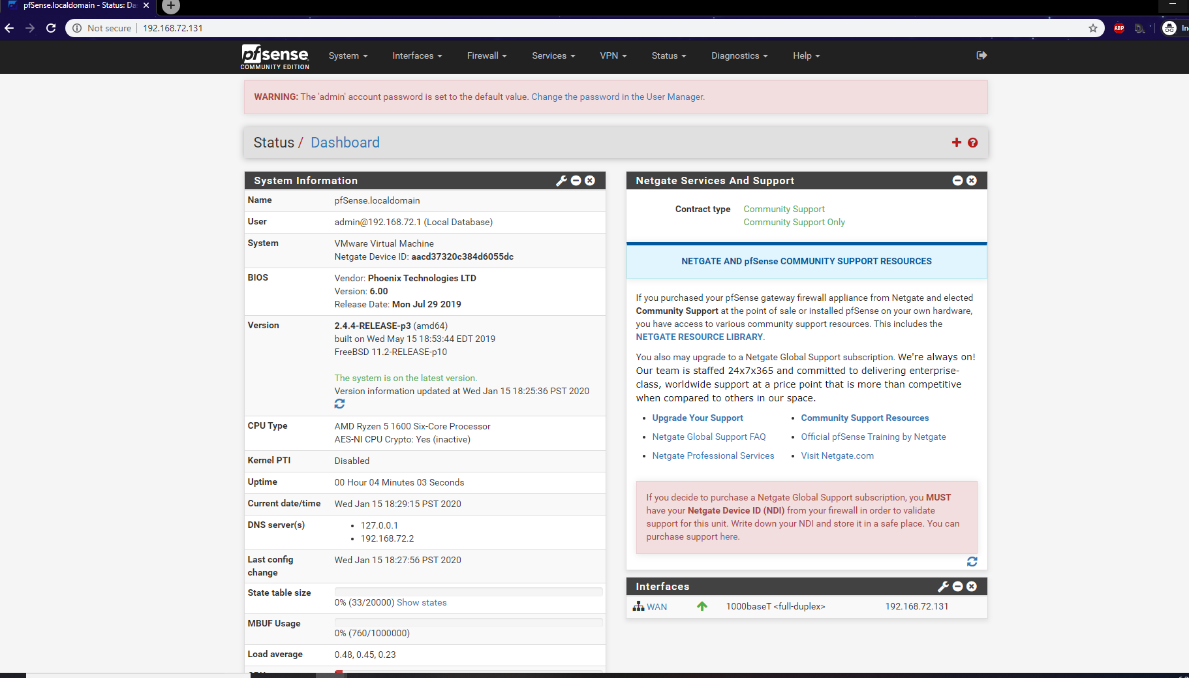
* Add features that make it more UTM
* Add protection at different layers

What aspects of network protection does it Not provide?

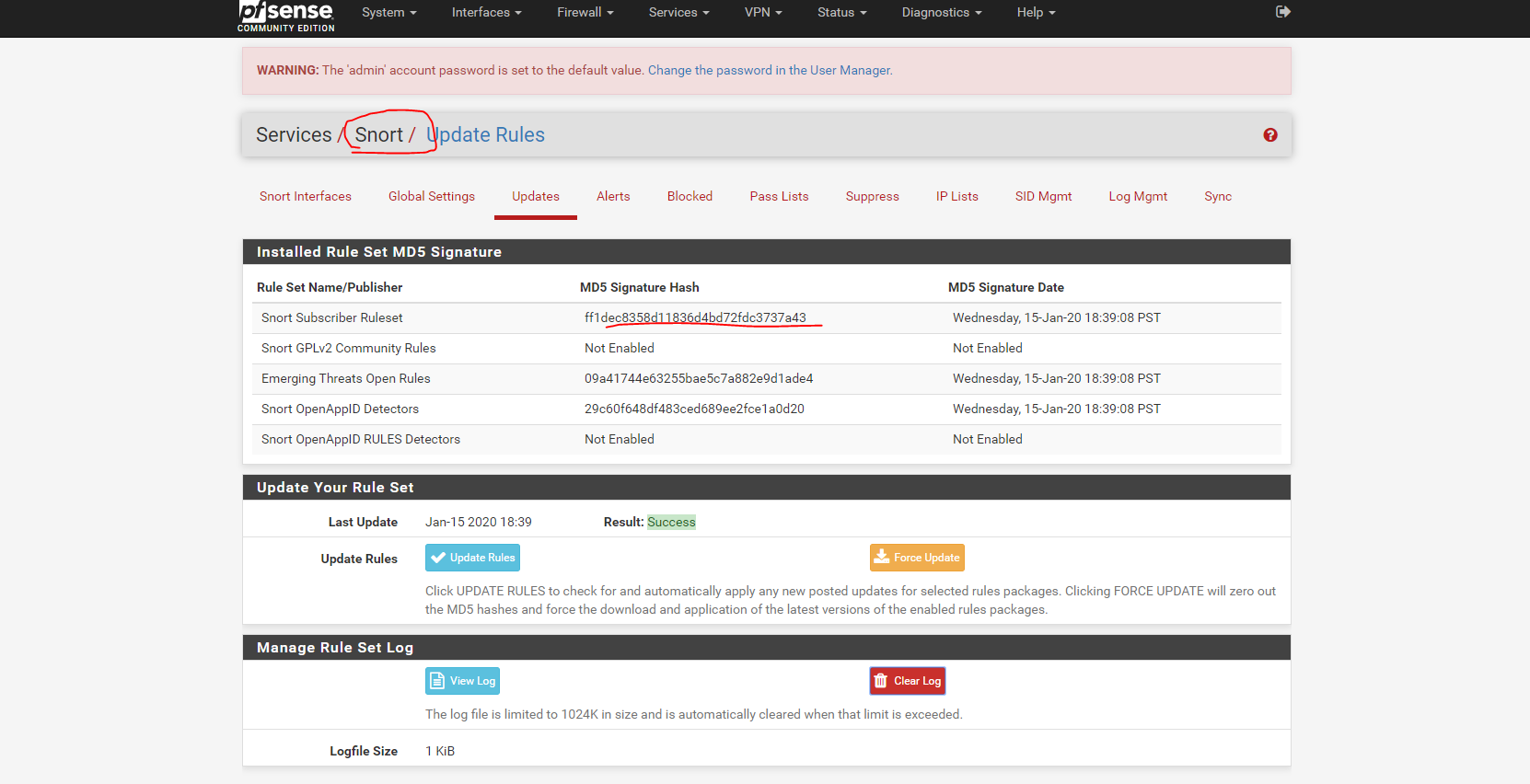
* A security client, against users who bypass or download things which shouldn’t be.
* Does not have security fabric

**Section 2: Practical**

Installation of pfSense



Snort configured and installed, with latest rules downloaded and configured.



**Useful Sites:**

https://pfsense.org

**Deliverable(s):**

Use this document as a base and include your ideas here.

(1.) Answer Questions

(2.) Document your Installation (with command line examples and screenshots, where relevant).

Remember that the more clear that your documentation is, the better that it will serve you in the long run.

Submit and upload to Canvas in the assignment area for this project.

[Previous](https://oit.instructure.com/courses/4007/modules/items/289002)