**Project Name: Firewalls: Unified Threat Management (UTM): Delta(s) and Deficienc(y)(ies)**

**Technology: Unified Threat Management (UTM)**

**Market:  Security**

**Name / Group: Gagneet Sahota**

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

**Potential Providers:**

Untangle

a.k.a. Linux (Debian) + iptables + UTM

Sophos XG Firewall

a.k.a. Formerly: (formerly Astaro Security Linux)

**Intended Activities:**

Firewall UTM Appliance Installation: Untangle

**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:

Unified Threat Management (UTM)

* A suite of security/ networking software that’s works together.

Next Generation Firewall (NGFW)

* A fabric type of firewall which include endpoints.

Cloud Generation Firewall

* Filtering, inspection could be on someone else’s machine. Good for businesses that have multiple locations that need to be protected.

**Section 1:  Lab Environment**

Note:  UTM has been in the marketplace and been gaining ground for approximately the last 12 to 15 years.

How would you define Unified Threat Management (UTM)?

* A suite of software all under one firewall or able to communicate to each other to secure the system.

Said differently, What is Unified Threat Management (UTM)?

* A combination of software that work together.

What do UTM firewalls offer our networks and systems in terms of security that older traditional firewalls do not address?

* They can communicate to other components that can take action against the threat. Anti-virus, IDP, sandbox

What are some important performance considerations of UTM firewalls as opposed to older firewalls that largely address Layer 3?

* That UTM firewalls can run in VM’s, as there are snapshots that one could take to rollback if an update goes wrong. A lot more ram needed because they are doing more, also can run on ASIC chips.

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

* Physical such as breaking into a system and transferring data. Does not have endpoints on machines in a organizations. Wouldn’t have protection against attacks within organizations computers.

What is the importance of calculating checksums / sums / hashes on the files that you download that are intended for installation? To ensure that you got the file you intended to download without any third party making changes to the file.

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 Untangle.

* With a paid version of Untangle, you would get good protection if everything was configured correctly and was a low-profile organization. As it provides firewalls, application blocking and virus protection.

Give examples.

What aspects of network protection does it Not provide?

* In user attacks such as a machine in the organizations attacking another computer in the organizations.

**Section 2: Practical**

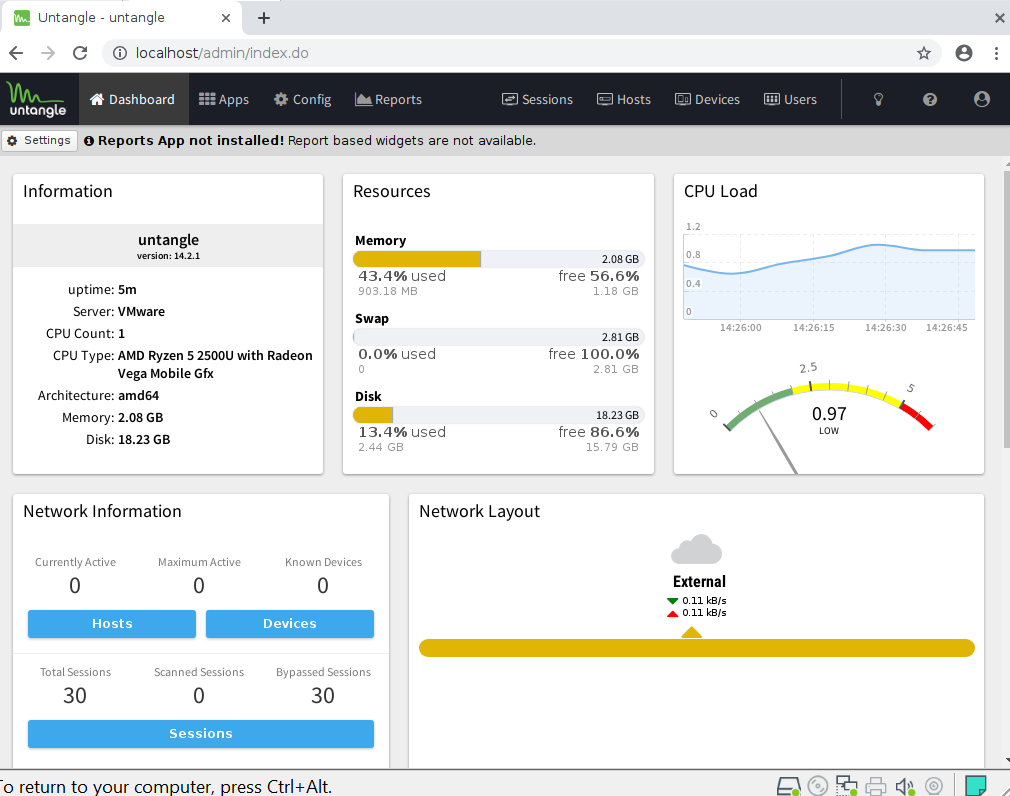
Installation of Untangle

Use graphical installation

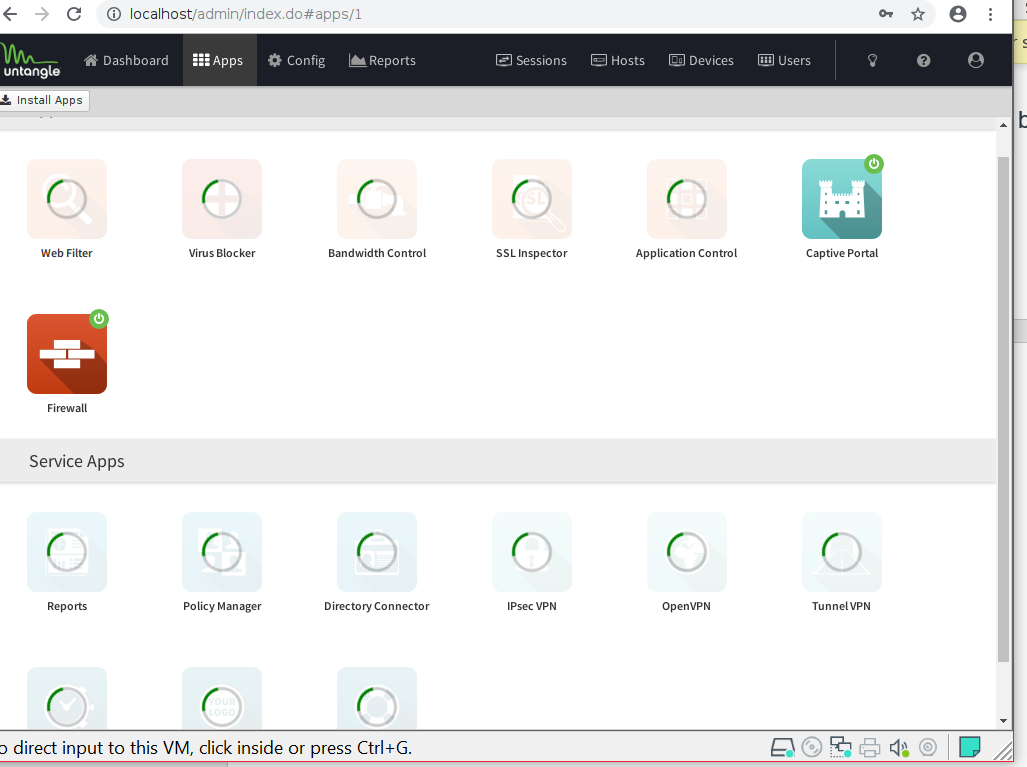
Select Language

Basic Configuration of Untangle

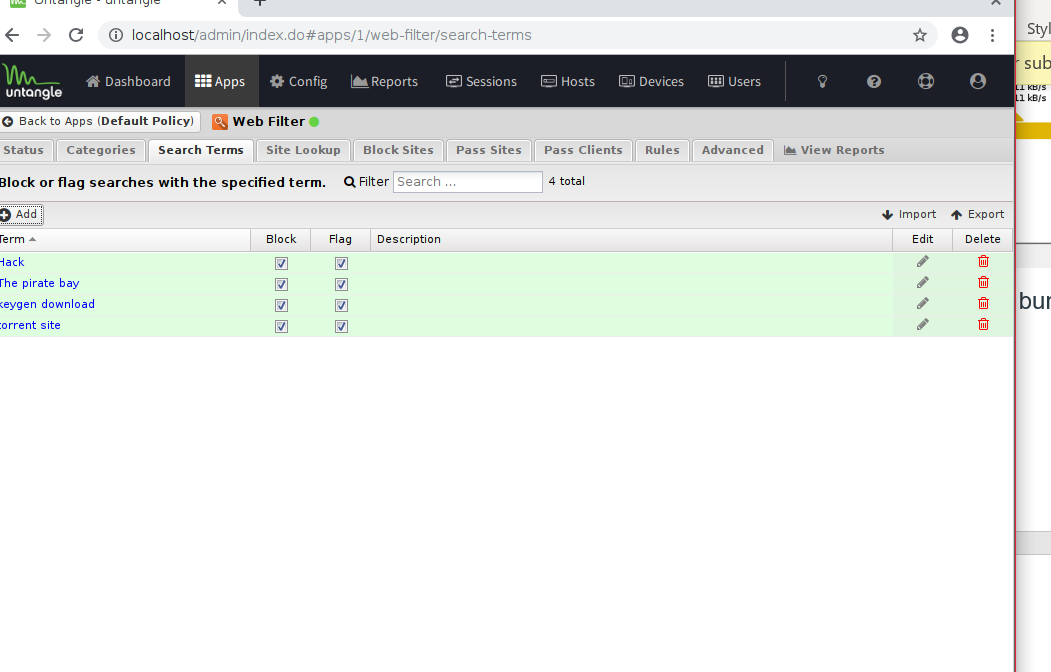
Proceed with the GUI installation, at the end make a password and enter an email to use.



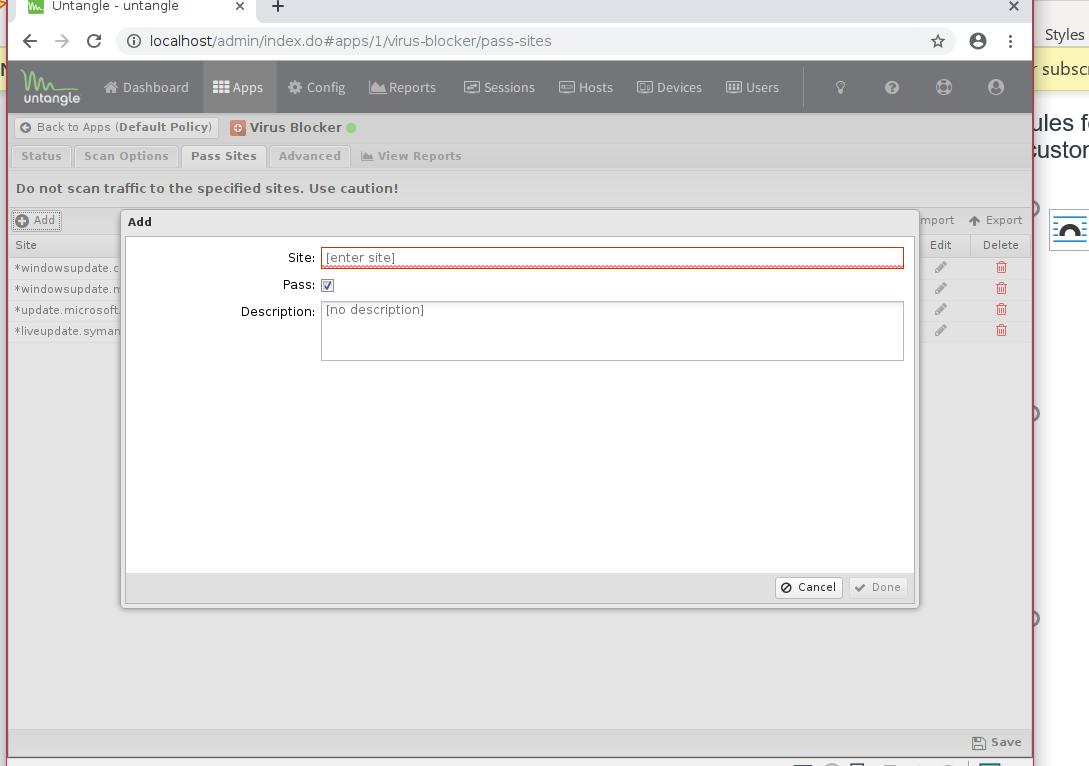
Go under Apps and download the recommended application bundle



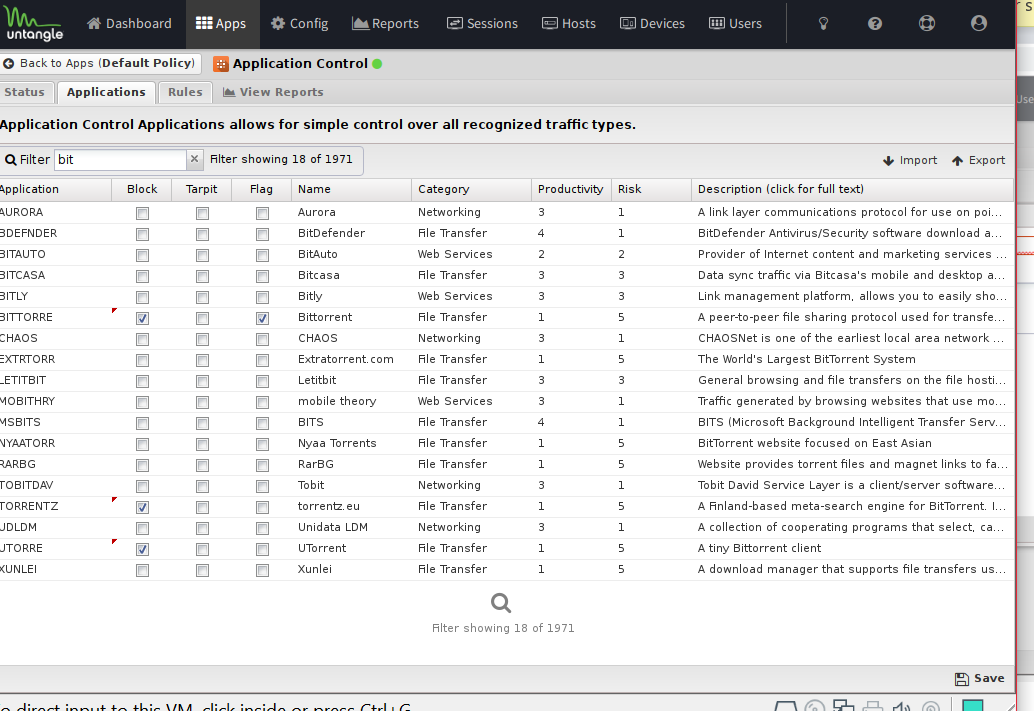
You can then proceed into each applications and configure rules for each application. As an example I have went into the web filter and set some custom rules for search terms which should be blocked



Another Area that should be configured is under the virus blocker, to remove Symantec and add your endpoint security software update url.



Then finally proceed to the application blocker and block all applications not wanted or needed. I blocked all torrent software in my example:



**Useful Sites:**

https://untangle.com