**Project Name:  Firewalls and PfSense Lab**

**Technology:  Firewalls**

**Market:  Security**

**Name / Group: Gagneet sahota**

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

**Directions:**

Answer the questions below in preparation for the practical portion of your lab (in Section B).  All responses are individual / no group work.

**Section A: Questions to Answer**

**Part 01:  NGFW / Cloud for Large(r) Retail / Org**

Differentiate Next Generation Firewalls (NGFW) (Palo Alto Networks, Fortinet, etc.) from Cloud Generation Firewalls (like ZScaler).  Within your answer, consider that you own a large retailer with somewhere between 100 to 400 sites across the nation / world.

NGFW:

* Application packet filtering
* Multi-gigabit speed
* Communicate between endpoints with firewall
* Alert of intrusions on network.
* SSL decryption to find signatures of applications
* Identity awareness such as which user/ what group
* Can prevent traffic from coming into the network.

Cloud Gen Firewall

* Hosted in the cloud
* Managed by cloud provider
* Has all the features of NGFW

Identify the primary reasons that you would choose a particular selection (“NGFW / CloudGenFW”).

If I had about 400 sites across the world then I would choose a cloud gen firewall as it would give easier accessibility to other branches of the company to manage the firewall rules. Although some of the drawbacks would be the cost, or not being able to do anything if the host company gets hacked.

Be sure to highlight the benefits as well as any drawbacks that a given solution offers.

**Part 02:  Architecture and Performance**

Make note of where performance considerations have led to certain network security architectural decisions.  Highlight how these considerations have led to some organizations having a less than ideal security posture.

Be specific on how you could remedy these situations when advising organizations how to correct issues within their information security architecture.

* When the network traffic for an organization is going through a single point such as a pc that analyzes the traffic before letting it leave the network. A better solution would be to mirror the traffic on a TAP to not interrupt the performance of the network while being able to monitor the network in real time.

**Part 03:  Budget Strategy**

An organization that you advise has taken the stance that it does not need to continue to invest in its information security infrastructure.  Make the case that informs them of the issues that many municipalities (140 + in the U.S.) have been affected by ransomware and other outage creating malware.  In this example, consider that the organization states that they no longer have interest in solutions that require subscriptions.

* I would make the case that the cost of subscriptions will be cheaper then having a companywide outage because a new strand of ransomware took over the systems and now all the company I locked forever or a huge price to retrieve the data. And even when the data is retrieved the confidentiality of the data is lost along with the customers trust in the company which can be more then any cost of subscriptions.

**Part 04:  Software and Configuration Integrity**

Develop a statement to inform organizations regarding the risks of assuming that software and configurations have integrity.  Detail how they can validate their downloads of software installation files (ISOs, etc.) from various vendors (Microsoft, Oracle, various Linux / BSD Unix variants).  Also apply this concept to form an internal opinion and operational practice of keeping an eye on current configurations (i.e. current running configurations of firewalls, routers, switches, etc.) from the standpoint of configuration integrity.

* It is important to ensure any software installation files have verified checksums as if they are different from the official download source that means someone has compromised the download, which result in introducing malware/ an open door into your network. This also applies with firewall configs where they should be verified once a week to ensure they are still the same configs loaded into the system, if the checksums do not match then that meets an attackers has changed the configuration of the firewall or uploaded their own.

**Part 05:  Management and Orchestration**

Make the case to an organization that is currently / potentially using manual configuration of each of their devices (Firewalls and related security appliances) that other viable and more efficient solutions (at scale) exist.  Integrate the concept of “Zero Touch” provisioning as well as Vendor Hosted Portals (i.e. think FortiCloud and Meraki, etc. as examples).

* By having a manual configuration firewall you may still be at risked for threats as over 100k new virus signatures/ bad websites are detected every day, and a firewall that’s not getting the new signatures would be at risk for these. And with a subscription-based portal, little to none time is spent configuring firewall rules saving salary time for network admins which they could spend doing other things to protect the network. Examples of that would be FortiCloud which you pay an annual fee and they upgrade signatures, whitelist/blacklist of websites to better protect the user.

**Part 06:  Zero Trust**

Provide an overview of the concept of “Zero Trust” and how it informs your overall firewall configuration(s).  Be specific about the ways that this mindset impacts your resulting security posture for a specific device and the network overall.

* Zero Trust is the concept that no computer, actor or user inside an organization is trusted so everything needs to be verified before connecting to the network. It informs you by using who, what, when, where and why, which allows you to understand why something needs access to a important resource. This impacts a network overall as the most important resources of a network such as a password server or Classified information server would implement a zero trust to not trust any device, even if it has been connected before.

**Section B: Questions to Answer**

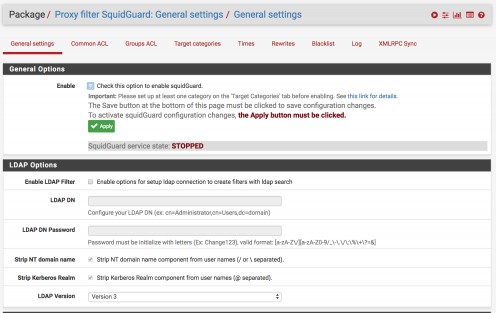
Indicate ways to make pfSense have more of a UTM or NGFW Feature set.  Think in terms of packages (pkg) and additions that you would make to a given install.

For packages that exist (as packages that you can easily add to your system), make note of the package name(s) and why you would include them.

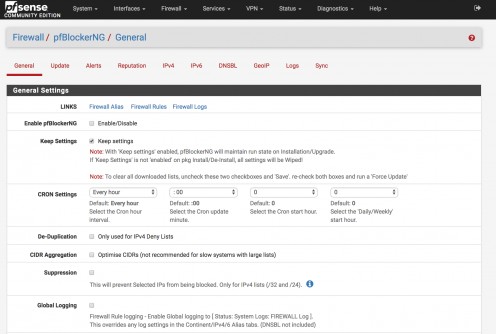
* Squid- Runs traffic on a proxy to ensure your IP isn’t revealed to bad actors.
* pfBlockerNG- Blocks incoming/outgoing traffic based on domain names to black list threats, malware or even ads.
* SquidGuard- Allows automatic redirects based on url’s visited or even time based url redirects, good for organizations who don’t want anyone on the location before hours.
* Darkstat- A network monitor that captures traffic and gives you network stats on them.
* Snort- A IDS/ IPS that can detect attacks or port scans from bad actors.

As part of the practical section, add these packages to your installation (of pfSense) and document accordingly with relevant command line examples or screenshots of web based GUI, etc.

SquidGaurd installed



PfBlocker



**Useful Sites:**

https://pfsense.org

https://docs.netgate.com/pfsense/en/latest/packages/package-list.html