Exercise 1

Stewart Johnston
CIS 127 – Intro to Information Security
NCMC
johnstons1@student.ncmich.edu

September 12, 2018

1 The Next Generation Firewall

By definition, a Next Generation Firewall includes the base functionality of a firewall, so it is more useful to work backwards in definition. A firewall monitors and controls incoming and outgoing network traffic. First generation firewalls were more limited in scope, and its security rules were defined in terms of source, destination, protocol, and port number information as carried by packets. A NGFW is the result of sticking that and other functionality, like Intrusion Prevention Systems or proxies in a blender.

A NGFW by comparison uses more advanced filtering techniques. One such technique is application filtering via deep packet inspection. Deep packet inspection borders examines in detail the meaty data each packet carries, rather than just the packet headers. This borders on the invasive, but can be an effective tool for ensuring the safety of devices on its network. Other methods include inspecting encrypted traffic, website filtering, Quality of Service management, and others. Live antivirus or advertisement filtering is one possible use of technology like this.

1.1 Network perimeter and the cloud

The network perimter is primarily the notion of a clear traffic and information boundary between an organization's internal assets and the rest of the world. As Software as a Service, IoT, and Bring Your Own Device becomes increasingly ubiquitous, the line of what is an internal asset becomes increasingly blurry. The access to one's internal assets are increasingly remote and distributed. More to the point, many workhorse "internal assets" are offered by some external organization and are not inherently under your own control.

The NGFW and other pieces of hardware like it were what primarily defined the boundaries of the network perimeter. So many assets are so outside of their scope of influence that the perimeter has effectively become either too blurry to consider or broken entirely. Not to mention, other organizations servicing assets seek to offer NGFW servicing of their own.

1.2 Author's supporting points

The author of the article supposes that NGFWs are ineffective. They don't fault the NGFWs themselves, but the structure and scaffolding around them. That structure results in numerous

paths around NGFWs. Third parties wanting unrestricted access don't want to deal with NGFWs at all. Network administrators crafting the rules for an NGFW often have to be incredibly light-handed for fear of blocking legitimate traffic, and angering the users as a result. Users are already vulnerable, angry users wishing to get around their restrictions are dangerous. He also speaks to the imbalance of an overwhelming amount of security alerts and not enough staff to see to them.

1.3 NGFW vs the Cloud

As mentioned in the article, Amazon, in addition to offering AWS, now also offers Guard Duty. Guard Duty is an additional service for sale, built to run and protect the AWS machines and applications a given organization is using. Buying both the hosting service and the security service from one provider will allow them to optimize and increase the efficiency of both services. An in-house NGFW solution, then, will have increasingly diminishing returns.