**Chad Ballay**

Week 8

**Install And Run One of the Following**

I didn’t have access to a windows desktop and failed to get an Azure instance spun up in time. (Not sure what is going on with my personal subscription and spent waaayyyy too much time shaving the yak on figuring that out. However, ZoneAlarm was around when I was in college at the turn of the century so of the three that’ll be the one I try to review using what I can find online. A meta-review of the reviews.

Background of the company (<https://en.wikipedia.org/wiki/ZoneAlarm>). They’ve been around for 20 years now and unfortunately the product surface appeal hasn’t aged well. The user interface can be kindly described as consistent and nostalgic. Unkindly, you can refer to it as being dated.

A screenshot of a cell phone

Description automatically generated

<https://www.cloudwards.net/zonealarm-antivirus-review/>

This unfortunately gets in the way of what it should be judged by. Does it protect your machine and does it do so without affecting your usage of your machine? The results point to that it does indeed perform well and it does indeed do so with minimal invasiveness. Most of the reviews go on to mention that the paid tier is worth the upgrade due to low cost and that features it enables are worth paying for. All in all, ignore the tarnished outside and it’s worth it even at the free tier. At the paid tier it’ll be a steal for what you get.

**Three Types Of Firewalls**

Packet Filtering – Most basic. Each packet is checked against the ACL’s. That’s it. No state is maintained and only packet header is inspected. Dirt cheap and also dirt simple.

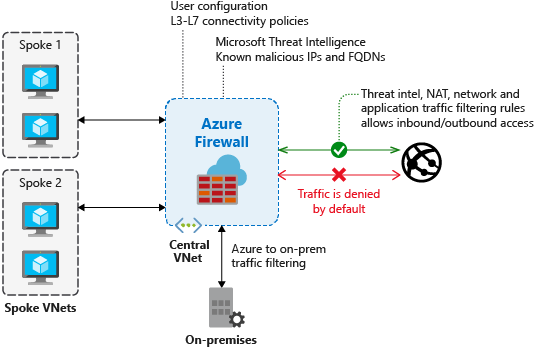
Stateful – These firewalls are more complex and are more resource bound. They inspect the packets down to the application layer. Past communication states are maintained. This level of dynamic filtering can be a burden to setup and teardown so there is overhead that is greater than a the packet filtering type firewalls.

Application Proxy – It acts as the man-in-the-middle between an internal resource and the external world. It is prohibitively resource intensive so very often its use is limited to specific cases where extreme security measures are needed.

**Where To Place Firewalls**

As the name implies, firewalls are meant to compartmentalize sections of your network. The first location is between the external network and your internal resources. This will be the main focus of your firewall effort. Incoming connections should be defaulted to deny all. The next focus is your DMZ area. Some sort of front door has to be setup so limited access is needed but it must be tightly protected and walled off with additional internal and external facing firewalls. Specific internal segments may also have internal firewalls. Think your PCI/HR/etc type areas. Finally exfiltration of data can also be managed to a degree here. It should be just as hard to get connections out as it is to get connections in.

I’ve spent a good chunk of this weekend trying to troubleshoot some Azure issues for work so I’ll reference a doc of theirs that is relevant. (<https://docs.microsoft.com/en-us/azure/firewall/overview>) Specifically this image.



This firewall sits at the chokepoint between the external network, on-prem resources, as well as cloud based resources. Deny by default and then allow specifically enumerated traffic. Etc, etc….