**Firewalls**

The traditional definition of a firewall is a structure that prevents the spread of a fire from an affected area, to a secure or safe area. This helps mitigate the spread of a dangerous situation and protect people from injury and assets from further damage. The world of networks has adopted the term firewall to describe a tool for protecting networks from the outside world. A formal definition of a network firewall is “to provide a method enforcing an access control policy” [1], or essentially, they “are nothing more than access control policy enforcement points” [1]. Comparing this to our traditional definition of a firewall we can see that a network firewall still acts as a barrier from one side to another. It can help protect people and assets from damage or theft. For networks, this is important because of how open the internet is by default. There are many people who scan networks with the desire to find open points allowing them into areas with valuable information to be stolen. “Firewalls enable you to define an access control requirement and ensure that only traffic or data that meets the requirement can traverse the firewall…or access the protected system.” [1]. From here on, we will be focusing on firewalls as seen in networks.

In order for a firewall to be effective, it must be capable of the following: “Manage and control network traffic, authenticate access, act as an intermediary, protect resources, and record and report on events.” [1].

Managing and controlling network traffic is essentially a method of controlling “network traffic that is allowed to access the protected network or host” [1]. Firewalls can accomplish this by inspecting network packets [1]. A network packet is a digital container that contains information to be transferred over a network from a source location to a destination [2]. When the firewall inspects packets, it can find useful information such as the source IP address, destination IP address, and other useful information that helps in filtering what gets accepted [1].

Authenticating access involves more than just checking the source IP address from packets, it is easy for a thief to manipulate a packet to fake an IP address [1]. Firewalls must do something better for actual authentication. In addition to checking IP address, it is imperative they only allow access to users that have a valid username or password [1]. This is an additional measure to verify the person connection has been granted privileges with the network. Usernames and passwords can be inconvenient since they need to be remembered and entered often. An alternative, but very secure, method of authorizing with set credentials is to use public and private keys [1]. These are keys stored on both the host and guest machines that get matched to handle “automatic” authentication.

“A firewall can be configured to act as an intermediary”, also known as a proxy [1]. This essentially lets the proxy act like the protected host, but it “receives packets destined for the protected host, strips out the relevant data, and builds a brand new packet that is then forwarded to the protected host” [1]. This becomes especially helpful when the firewall itself “is capable of inspecting the actual application data to ensure that it is legitimate and nonmalicious data” [1]. This leads to how firewalls should help protect resources.

“Access control rules, stateful packet inspection, application proxies” are all methods that can help protect resources from malicious access [1]. It is important to remember that even the firewall has its limits. Especially if the host being protected is missing security patches, there could be things the firewall can miss [1].

Lastly, firewalls should be capable of recording a reporting on events. In any system, it is important to log different occurring events or actions so when an issue or bug occurs, the developers can easily see what happened in addition to the state of the machine when the issue occurred. The same applies to firewalls. In the real world, something will be missed, a rule will be left out, and an attacker will find a way around checkpoints. Thus, “all firewalls should have a method of recording all communications that occur to enable the administrator to review the recorded data in an attempt to ascertain what transpired [1]. In addition to logs, firewalls should implement some sort of alarm system [1]. This allows administrators to be automatically notified when a special event of interest occurs [1].

So far, we have discussed what is a firewall, and what features it should implement, but we haven’t mentioned the two types of firewalls mainly available. There are both hardware and software firewalls. The hardware firewall can typically “provide a first line of defense against common forms of attack coming from the outside world. Plus, they can generally be effective with little or no configuration and they protect every machine on a local network” [3]. It has a limitation where “it typically treats any kind of traffic traveling from the local network out to the Internet as safe” [3]. An example would be an email containing a malicious attachment, the email would appear safe since it was opened from inside the local network [3]. Software firewalls aren’t as limited since they have more information. The software firewall can “know what program is trying to access the Internet and whether it’s legit or malicious (it consults a regularly updated database to determine this)” [3]. Software firewalls can screen what a program can send and receive [3]. Software firewalls can hone into more data regarding malicious traffic [3]. Yet, software firewalls also have their drawbacks. They only protect the machine they’re installed and configured on [3]. It can be beneficial to take advantage of the pros from both types of firewall by implementing both hardware and software firewalls [3].

To better understand the importance of implementing security measures through the use of firewalls, we can look at some statistics. “In 2011, 855 data breaches occurred globally, compromising 174 million records, according to the 2012 Data Breach Investigations Report”, “72 percent of exposed companies employed 100 or fewer individuals.” [4]. It makes sense that smaller companies are being targeted. They still store sensitive information, but might not employ the technical expertise to adequately protect it. For attackers, they are an easy target compared to a giant such as Google or Microsoft who implement numerous security measures and have entire teams devoted to security. The “average cost of a data breach was $5.5 million in 2011, according to the 2011 Cost of a Data Breach report” [4]. “Hackers and criminals were responsible for 32 percent of breaches; rogue employees caused 19 percent of breaches; and theft of mobile computer equipment like laptops and memory sticks carrying unencrypted data caused 33 percent of breaches” [4]. It is evident that not only do networks need to be protected on the outside, but also from the inside.

So, your company implements a firewall. It has all of the features mentioned thus far. You should be safe, right? Wrong. Just because the firewall has all of the right features, and is turned on, doesn’t automatically make you safe. It is an active effort to prevent breaches. “If you misconfigure or not maintain a firewall properly, it makes an easy way in for hackers” [5]. “If an expert firewall administrator configures a firewall, it does not respond to Internet Control Message Protocol (ICMP) echo requests to keep it safe from being hacked” [5]. There are a number of tool available to check your firewall for vulnerabilities. These tools can also be used by hackers. Some of these tools include: Firewalk, H-Pinging, Stateless Firewalls & Source Port Scanning, and Rootkit. Firewalk finds “open ports on” a “firewall…Firewalk also maps the remote network behind the firewall. A hacker can create an accurate topology of the network behind the firewall by sending packets to every host behind the firewall” [5]. H-Pinging “permits the user to explore some options of the TCP packet that may allow it to penetrate through some filtering devices even if it is blocked” [5]. The rootkit is a “critical segment of code injected into your computer system, designed to conceal any unauthorized activity taking place” [5].

These concerns are serious, as one company, TJX found out the difficult way. TJX was a “$17 billion-a-year parent company of T.J. Maxx, Marshall’s, and several other discount retail chains” [6]. Over a number of years, customer data was being stolen [6]. “The firewalls on TJX’s main network weren’t set to defend against malicious traffic coming from…kiosks” [6]. Coupled with other vulnerabilities in their kiosk systems this breach caused “account information for about 45.7 million separate payment cards…driver’s license numbers, military IDs, and state IDs for 455,000 customers, together with their names and addresses” to be stolen [6].

Data security is important not just to protect your own assets, but also the assets and personal information of others. Firewalls are only one step in the process of securing assets, and should be taken seriously.

# References

|  |  |
| --- | --- |
| [1] | W. Noonan and I. Dubrawsky, Firewall Fundamentals, Cisco Press, 2006. |
| [2] | "Packet," Techopedia, [Online]. Available: https://www.techopedia.com/definition/5380/packet. [Accessed 11 02 2017]. |
| [3] | R. Pacchiano, "Firewall debate: Hardware vs. Software," Small Business Computing, 2011. [Online]. Available: http://www.smallbusinesscomputing.com/webmaster/article.php/3103431/Firewall-Debate-Hardware-vs-Software.htm. [Accessed 4 02 2017]. |
| [4] | K. Hunt, "Firewall Under Fire: Could a Cybercrime Send You Up in FLAMES?," *Journal of Property Management,* vol. 78, no. 1, pp. 48-53, 2013. |
| [5] | L. Williams, "Your company's Firewall security is vulerable to hacking," ExternetWorks, [Online]. Available: http://blog.externetworks.com/your-companys-firewall-security-is-vulnerable-to-hacking/. [Accessed 04 02 2017]. |
| [6] | L. Greenemeier, "The TJX effect," InformationWeek, 2017. [Online]. Available: http://www.informationweek.com/the-tjx-effect/d/d-id/1058033?. [Accessed 04 02 2017]. |