Firewalls Security

Saint Leo University

COM 450- Network Defense and Security

Instructor: Dr. Omar

Group members:

Monica Figueroa-Santos

Antonina Spinella

Karyliz Rosario

March 30, 2016

Abstract

Our paper is going to talk about what Firewalls are and how Firewalls are the first line of defense when keeping a network safe. We will state how Firewalls determine what is safe and what is not allowed into the network based on security protocols by explaining segmentation. We will discuss the brief history of how Firewalls came about and how they changed network security. As well as decipher the four different types of Firewalls: packet-filtering, Circuit-level gateways, stateful inspection, and application-level firewalls.

Introduction

Security has become a major concern in today's business owners. With the ongoing improvement of the Internet, and multiple ways to access and store information, has raised a problem to many users “how can one protect the company’s network from external attacks?" It is important that critical information does not leak out to the world and get into the wrong hands of an attacker. Hence Firewalls were created, which boosted security to levels that were unreachable in the past. Firewalls were designed to protect the internal network and filter out what goes into the network from the outside.

Background

A firewall is a network traffic control device or service, it enforces network security policies, protects the network against external attacks, establishes control over network traffic, and prevents connections from unauthorized sources to protected network systems, services, and resources (Jones & Bartlett, 2014). Firewalls are one of the common network security components used to avoid threats. Their purpose is to be the first layer of defense and filter traffic and separate communication through segmentation (Jones & Bartlett, 2014). Firewalls benefit to the hardware and software for protection since they are the first line of defense and keep noise out. But firewalls are limited to only the perimeter defense, also not content oriented, and only have a yes or no response (Jones & Bartlett, 2014).

History of a Firewall

Firewalls did not first come from the internet first, it came from another instruction, such as housing (Avolio 2). They can also be used as barricades for fire (Avolio 2). Another are firewalls in engine sections, such as separation of passenger all within an automobile. Cheswick and Bellovin have said that firewalls dealing with Internet are said to "… [have] the following properties: single point between 2 or more networks where all traffic must pass; and traffic that can be controlled by and maybe authenticated through the device, and all traffic is logged" (Avolio 2). In the 1980s, the initial network firewalls surfaced, which were routers that had the usage to divide a network into LAN's that are smaller (Avolio 2). Firewalls similar to this were placed to put a restraint on the problem dealing with a single LAN overturn to affect the network as a whole (Avolio 2). At the beginning of the 1990s the initial security firewalls were put into use. It was IP routers that had rules dealing with filtering (Avolio 2). The principle policy for security is that the allowance of anyone in the 'out access' can be reachable (Avolio 2). The firewalls here do not have a restriction, but with this came the hardship of rules dealing with what could be accepted and what could not (Avolio 2). With that it was difficult to recognize the different aspects of the application that are necessary to limit (Avolio 2).

As security firewalls grew they became more complex and tunable too (Avolio 2). With this there was the creation of firewalls on a host called bastion (Avolio 2). Chances are that it was the initial commercial firewall type, with the usage of application gateways and filters (Avolio 2). This was built from the DEC or Digital Equipment

Corporation (Avolio 2). The paramount commercial firewall was put together and commit to the primary customer (Avolio 2). They were an enormous East Coast root chemical company and all of this happened on June 13, 1991 (Avolio 2). The firewall was made and was nicknamed DEC SEAL, with SEAL as an acronym for Secure External Access Link. DEC SEAL was built with a system that is external, also known as a gateway (Avolio 2). Then later in October 1st of 1993 the TIS FWTK was let loose in the source code structure to the community within the internet (Avolio 3). This gives the premise for the commercial firewall TIS (Avolio 3). The usage of FWTK is still done by experimenters, along with government and also the industry with a core for security dealing with the internet.

Identities of a Firewall

When it comes to internet firewalls there are four types of Firewalls (Avolio 3). One type of firewall uses packet-filtering (Avolio 3). Filtering firewalls display packages built on addresses and package choices (Avolio 3). They run at the IP packages and construct security resolution built on the headers packages (Avolio 3). When it comes to firewall filtering there are 3 subtypes: stateful inspection, dynamic filtering, and static filtering (Avolio 3). A technology that's alike to filtering dynamic, with an inclusion of more gritty inspection of data included in the IP packages is a stateful inspection (Avolio 3). Filtering that is dynamic is an outside process that alters the regulations of filtering dynamically built on events that are router observant (Avolio 3). Static filtering is filtering many router devices with filtering regulations that have to be changed by hand (Avolio 3).

Circuit gateways run in the transport network layer (Avolio 3). Similar to filtering gateways, generally gateways can't observe data traffic flow among a single network and another one (Avolio 3). But gateways prevent unbroken connections among a single network and another network (Avolio 3). Application gateways or firewalls that are proxy built utilize the application level and have the ability to review information when in the data application level (Avolio 4). Application gateways can create choices built on data applications (Avolio 4). For example, commands proceed to FTP, or URL to HTTP (Avolio 4).

Firewalls that have hybrid capabilities have elements usage of more than a single type of firewall (Avolio 4). The primary firewall that is commercial is DEC SEAL (Avolio 4). This was a hybrid with the usage of proxies on a host bastion and package filtering working with the gateway machine (Avolio 4). Circuit gateways or package filtering might be added by an individual to a firewall gateway application (Avolio 4). This is because it needs new proxy code recorded for each service that is new (Avolio 4). But an individual could have an addition of a powerful user authentication that is stateful package filter with adding proxies for service (Avolio 4). A firewall essentially acts as a dominance gateway among 2 or more systems in which majority of traffic must pass (Avolio 4). A firewall implies a policy with security and is kept on an audit chain (Avolio 4).

To continue we should learn a little bit more about firewalls. So far, we have learned the different type of firewalls and how the help construct our networks. However, we have yet to learn how these firewalls are tested and what situations can

better or compromise their performance. Just like everything in a network firewalls, if not monitored can be fragile and easily interrupted by damaging effects.

To best test the performance and security of firewalls we must have some type of policy to follow. This will ensure and identify what our firewalls are meant to do and view if the policy is being followed. For example, the firewall must first be able to identify and follow the security policies. Then, ranking the security policies by most to least in importance. Which is the, followed by having the main context of the policy identified and seeing if the proxy services are needed to be installed, or not. Followed by making sure that there are no other controls needed such as, restricting internal access to some internets services or just something obvious like denying unauthorized access from an outside host. Lastly, you would have placed a set of screening rules in the router. This would ensure the security the firewalls would obtain regarding following the policy accordingly.

We know security is the goal, but how do we ensure that the goal is achieved? With security testing we can check up and keep up with maintenance. It also seems that we perform penetration testing to ensure our security of firewalls. Why penetration testing? Penetration testing seems to use such techniques that it allows to enter and compromise the firewalls security to identify if one the security is effective and secondly better, the firewall security so such things like unauthorized entries and vulnerable behavior does not occur. Penetration testing regarding firewalls is not one-hundred percent ensured. It is difficult to simulate/imitate a real live attacker’s process to an experimental LAN. Nevertheless, there are efficient ways to check for any vulnerable areas that a specific firewall might obtain. Scanning tools, are great tools for such

situations. Scanning tools can simulate real invasions. After the scanning tool test are through simulating the false attacks then they are also able to identify any warnings found. Which then is continued by the routine elimination of faulty security holes which are usually extracted by adding some screening rules to the firewall.

Other than checking the security levels of a firewall, you will also have to routinely check the performance of a firewall. This allows for us to measure firewalls services (HTTP, FTP). What performance testing does is, imitate the firewall by sending a ton of traffic through the firewall. What really determine the performance of a firewall are its performance/elapsed time which are taken by seeing how fast or slow the traffic is being monitored by the firewall.

Firewalls are a great source of protection. Once all loops, breaks and vulnerabilities are checked and it is working according to the policy. Keep in mind that firewalls are high maintenance because of the constant breeches that it faces every day. Which means firewall have to be closely monitored and taken care of by introducing it to penetration testing, scanning tools and also testing the firewalls performance.

References

Avolio, F. (2011, April 26). Firewalls and Internet Security – The Internet Protocol Journal – Volume 2, No. 2. Retrieved March 7, 2018. https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-1/ipj-archive/article09186a00800c85ae.html

Cocosel, B. (1996, December 9). Analysis of Firewall Security. Retrieved February 20, 2018. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.135.4808&rep=rep1&type=pdf

Jones & Bartlett (2014). Network Security, Firewalls, and VPNs. Lesson 2 Firewall Fundamentals. Retrieved January 20, 2018. http://www.jblearning.com/

Michael R. Lyu and Lorrien K. Y. Lau (2001). Firewall Security: Policies, Testing and Performance Evaluation. Retrieved March 10, 2018. www.researchgate.net/publication