Firewall Security

Saint Leo University

COM 450- Network Defense and Security

Instructor: Dr. Omar

Kanokwan Budsarakoon

Abstract

This paper will talk about firewall security. It will start with the definition of firewall and general details. Then, continue with the reason why do we need a firewall in order to secure our network and example of the risk zone. Following the explanation of how the firewall works and types of firewalls. After that we will go through the ingress and egress filtering with some examples of firewall filtering types.

Introduction

In order to know about firewall security, first, learning about the definition of firewall security. Second, understanding why we need to use a firewall and which area of work that needs the firewall system the most. Third, knowing how a firewall works and types of firewalls. Then, researching more about the types of firewall filtering. All of these will help the learner to earn some needed knowledge about firewall security.

Firewall Security

Liu (2010) presents that firewall is an important element in network security. Many people give the simple definition of firewall as a wall, gateway, or border. Firewall has been using for securing private networks in most business. We are not only use firewall in the business area, but we also use it as a tool to secure individual user networks. According to Stewart (2014), a firewall work as a traffic device controller that has filters to enforce an access control policy and protect the network from outside attacks like malicious attacks.

Why You Need Firewall

According to Stewart (2014), everyone who uses a computer to connect with or exchange resources with another computer need firewall to protect themselves. Without a doubt, most of the computers or electrical devices that people using nowadays like smartphones, tablets, or even smartwatch have access through the internet and mostly are always online. As a system is always being connected, it can be concerned as a vulnerable security. For example, there are tons of hackers outside are waiting to attack or find new weak targets. They use malicious programs such as bots, agents or

zombies that can scan and attack their target automatically. In addition, high speed internet is another weakness point because high-speed connection lead to high-speed attack. In the past when we had slower internet connection, there were also many risks existed but slower and simpler compare to currently harm. Not only using a firewall for internet protection but also defend versus network segments inside the private network. These are some reasons why we all need firewall security.

Zone of Risk

According to Stewart (2014), “A zone of risk is any segment, subnet, network, or collection of networks that represents a certain level of risk” (p. 56). We will definitely need more protection at the high-risk area, and lower secure at the low-risk area called as a zone of trust. Stewart (2014) recommends that each risk zone needs to be specifically and distinctly separated from some other danger zone, particularly because there are various degrees of risk in certain areas as we can see from Table 1.

Table 1. *Risk and trust levels of common network zones.*

ZONE	RISK LEVEL	TRUST LEVEL
LAN	Low	High
Extranet	Medium-low	Medium-high
DMZ	Medium-high	Medium-low
Internet	High	Low

Note. Reprinted from Table 2-1 Risk and trust levels of common network zones, by Stewart, J. M., retrieved from *Network security, firewalls, and VPNs*. Burlington, MA: Jones & Bartlett Learning.

How Firewalls Work

As mention in the beginning that firewalls work as the security guards at the entrance of the building. Basically, firewalls will first scan each data packet that wants to pass through the gate. Then, firewalls will make the decision if the packet can pass through based on some parameters such as the packet's source address, packet's destination address, port number, or application associated (Lynch, 2000). Stewart explains that the packet will keep continuing to the destination if it is authorized, but the packet will be blocked and dropped if it is unauthorized (2014).

Types of Firewalls

There are so many types of firewalls that sometimes can be divided by its version, variations, and models. However, after the experts debated the firewall type, they got to the conclusion that firewalls have two main types of firewalls which are personal firewalls and commercial firewalls.

According to the Stewart (2014), a personal firewall is a firewall that design to protect a single system or a small business network like SOHO network. A personal firewall normally not required certification or special training. A personal firewall commonly uses a user-friendly interface like GUI—Graphical User Interface.

A commercial firewall is a firewall that design to protect a medium to large business network. A commercial firewall mostly needed certification or special training in order to the get full benefits features. A commercial firewall regularly uses a Unix-like command line interface or CLI (Stewart, 2014).

Ingress and Egress Filtering

According to the Stewart (2014), Ingress and egress filters is a standard spoof filtering method. Ingress filtering is used to check when the packet from outside wants to get into the network. Additionally, egress filtering is used to monitor the packet that try to leave a network. Plus, the work area of ingress and egress filtering may spread to cover spoofing security and a broad variety of inbound and outbound traffic investigations. These could involve blacklist and whitelist screening, protocol and port blocking, and proof of authentication.

Types of Filtering

Filtration is the main feature of a firewall. There are lots of types of filter in firewall, however, this paper will show some of them such as static packet filtering, application proxy, and circuit proxy.

First example of filtering is static packet filtering, Stewart states that a static packet filtering is the simplest type of filtration and it uses fixed filtering rules for network traffic. Static packet filter relies on the network layer (layer 3) and also involves the layer of transport (layer 4) (2014). Lynch (2000) also explains that this type of filter normally is the one who makes the decision on what to do with the packet like either let the packet pass through its destination or stop it. The decision will typically base on the packet source address and packet destination address. The advantages of this packet filter are in terms of speed and low cost. On the other hand, the packet filter's downside is the lack of granularity. Stewart (2014) says that filtering the static packets do need the firewall administrator to identify and adjust the collection of rules. The issue with the rule sets can occur when the sets get too huge and the rules are in the wrong order because they may generate loopholes or accidentally disregard authorized traffic.

Secondly, application proxy is packet filter system-specific edition. An application proxy will observe traffic across the entire seven layers of OSI which is different from a static filter packet that can only track the packet's header or segment (Stewart, 2014). Lynch (2000) explains that, at the application layer, the data is transmitted to a proxy program related to the framework utilized for the data packet. The proxy application will be the one who make the decision if the packet is allowed to go or need to be blocked.

Last example of filter is a circuit proxy, according to Stewart (2014) a circuit proxy concentrates on the initial setup process of the session, state, or circuit. Lynch (2000) also states that a circuit proxy allows more control than a packet filter. In this case, the packets will need to go through the proxy instead of going directly into the server. Before sending to the network, each packet would need to be detected and re-addressed when it travels through the proxy program.

Conclusion

A firewall is a network protection device that watches and controls sending and receiving network traffic based on defined security rules. We all do need firewall security in order to protect the organization or individual network. Not only realize that we need a firewall, but we also need to understand why we need it and learn how it works.

References

Liu, A. X. (2010). *Firewall design and analysis*. Retrieved from https://ebookcentral.proquest.com

Lynch, H. M. (2000). Firewall Fundamentals. *Information Systems Security*, *9*(5), 24. https://doi-org.saintleo.idm.oclc.org/10.1201/1086/43312.9.5.20001112/31374.6

Stewart, J. M. (2014). *Network security, firewalls, and VPNs*. Burlington, MA: Jones & Bartlett Learning.