Firewall Classifications

Bernard Ayuyao

Old Dominion University

CYSE 600 36666 Cybersecurity Principles

June 19, 2021

Firewall Classifications

Today, we are fortunate to have the use of the internet and what it does. It helps us do our work anytime anywhere at our own comfort. Several tasks that we get to do are for online shopping, online courses, online banking, business, staying connected with family and friends and many more. Although, with the use of the internet increasing, it's time has been spent more on activities like playing video games, gambling, chatting and many more. As the increase of the use of the internet, someone is always learning new things that can be harmful to us, like hacking. Furthermore, hackers try to force themselves into a company's network and take all the important documents or cause damage to the network which causes the company to suffer in their value. In order to prevent this, the company uses a firewall. The firewall is a security perimeter on the network which everyone is familiar with. The firewall can be used for the hardware or software or a combination of both. There are three groups in which a firewall can be utilized and they are features, usage, and budget. Under each group has their different uses of the firewall.

The first way a firewall can be utilized is on the features and the first feature is packet filtering firewalls. "Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports" (Sharma & Parekh, 2017, p. 1979). This shows that as packets come in, they are filtered and monitored to see if they are ok to pass through. It is like having a bouncer at the club looking at your drivers license. They filter out who are allowed to be in the club by looking at your driver's license. If the photo and age match, then you may pass through and proceed into the club with other allowed members.

The second type of firewall based on features is circuit-level gateway. “They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to a remote computer through a circuit-level gateway appears to have originated from the gateway” (Sharma & Parekh, 2017, p. 1979). This shows that a three way hand shake is looked at to ensure a session is legitimate when connecting from a node to note. This happens at the OSI model because the three way handshake is introduced at the transport layer which is the fourth layer of the OSI model. This also provides a connection based error checking transport of data.

The third type of firewall based on features is stateful inspection firewall. “Stateful inspection, on the other hand, analyses packets down to the application layer” (Sharma & Parekh, 2017, p. 1980). This shows that this type of firewall look at both incoming and outgoing packets over a period of time on the seventh layer of the OSI model. This is where it looks at the specific application such as web browsers, e-mail applications, and many more for analyses of packets.

The fourth type of firewall under features is application-level gateways. “An application gateway or application level gateway (ALG) is a firewall proxy which provides network security. It filters incoming node traffic to certain specifications which mean that only transmitted network application data is filtered” (Sharma & Parekh, 2017, p. 1980). This shows that the filters used on the application level to route traffic based off of incoming URL. If there is a URL for images, it can filter or route to a known pool of images. This also happens in the fourth layer of the OSI model which is the transport layer.

The fifth type of firewall under features is multilayer inspection firewall. “The stateful multi-layer inspection (SMLI) firewall uses a sophisticated form of packet-filtering that

examines all seven layers of the Open System Interconnection (OSI) model" (Sharma & Parekh, 2017, p. 1980). This shows that since this type of firewall filters through all seven layers of the OSI model, it is observed fully throughout the process for greater protection. The packets are looked and compared with known friendly packets. It is like knowing your enemies have a certain color like red and friendly forces are green. You know that you can allow green to your territory.

The last type of firewall under feature is dynamic firewall. "A dynamic packet filter is a firewall facility that can monitor the state of active connections and use this information to determine which network packets to allow through the firewall" (Sharma & Parekh, 2017, p. 1980). This is a type of firewall that is located in a physical place and in this case, a facility. There are people monitoring the connections and gather information to decide what packets are allowed through the firewall.

The second way a firewall can be utilized based on usage and there are two groups on here which are software firewall and hardware firewall. Their definition are both on their names and self-explanatory. Software firewalls uses software that are installed on your computer while hardware firewalls are devices that you connect to your computer or network so that you can protect your computer or network from unauthorized access.

Finally, the last way a firewall can be utilized is based on budgets. There are two types of groups of firewall based on budgets as well and they are commercial or paid firewall and free or open source firewall. "A firewall which possess a fully fledge properties and any users can use it but they have to pay to use those services. The firewall which is available freely and can be used by anyone and anyone can modify the source code and even find bugs and report them" (Sharma & Parekh, 2017, p. 1980). These services are both self-explanatory as well. I like to think of

commercial firewalls as pay to play or use their services. Companies like Norton can be free or AVG but if you want to upgrade to their better services it will cost you money. Also, free open source firewall are basically free for use. You can just download the software and it is ready for use. You probably just won't have the features an paid version has but at least you will have some kind of protection on your network or computer.

A firewall is a security system with a purpose to prevent unauthorized access from or to a network. There are three ways they can be utilized and they are features, usage, and budgets. Features has four groups under them which are stateful inspection firewall, application-level gateways, multilayer inspection firewalls, and dynamic firewalls. For firewalls based on usage, there are two groups under this category which are software and hardware firewall. The last way they can be utilized is based on budgets and under this category there are commercial or paid firewall and free or open source firewall. There are different utilizations and groups for firewalls and just having a firewall for protection that fits the best use for you would harden your protection or security of your computer or network.

References

Sharma, R., & Parekh, C. (2017, May). Firewalls: A Study and Its Classification. *International Journal of Advanced Research in Computer Science, 8*(4). Retrieved from http://web.b.ebscohost.com.proxy.lib.odu.edu/ehost/pdfviewer/pdfviewer?vid=1&sid=6dba9e04-b91e-43b0-8fa1-505ad05a40a8%40sessionmgr103