Humayun Kabir

Protect Yourself:
The Benefits of a Firewall

In modern society, most individuals have a technological device that has a wireless connection to the internet. However, many are not aware of the security precautions that were implemented into their devices. A feature known as a firewall is programmed into many devices to help protect its hardware and software.

What is a firewall?

A **firewall** is a security device that monitors the incoming or outgoing network traffic. Depending on your device's security rules, the firewall decides either to allow or block the flow of **network**. In Figure 1, it shows a simple layout of how a firewall works with a network and your device. There is a set criterion needed to be met in order for a network to get access to your device.

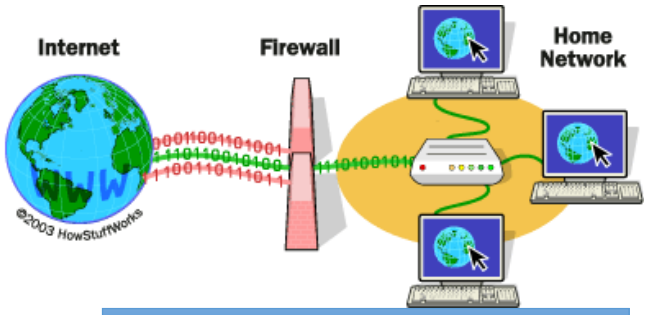

Figure 1: Pictorial of Simple Firewall
https://computer.howstuffworks.com/firewall.htm

Figure 2: Security Threats
https://www.dataiq.co.uk/news/news/government-sites-leave-users-open-to-email-fraud

Why do we need firewalls?

Firewalls enable security protocols that help your devices be protected from incoming or outgoing network traffic. Without a firewall installed, your device is open to all network traffic because there are no security protocols. This enables hackers and viruses to have access to your data such as your personal identity, bank accounts, credit cards, and any personal information you contain on your device.

Different Types of Firewalls

- Proxy Server
- Packet Filtering
- Gateway Implementation
- Web Application Firewall
- Host Based
- NAT

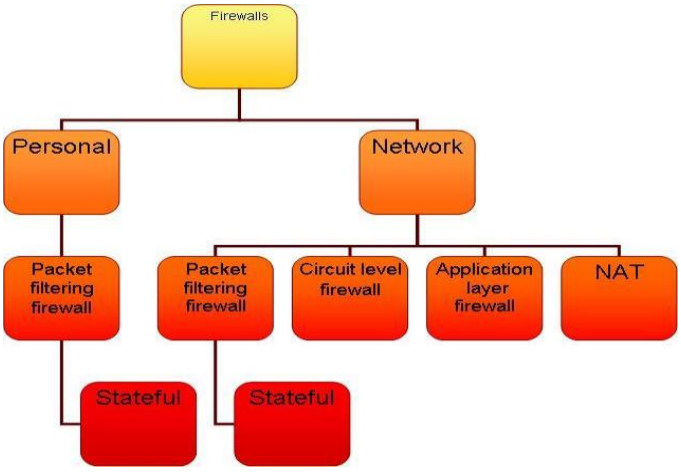

Figure 3: Breakdown Chart of Different Firewalls
http://sankar-information-security.blogspot.com/2012/09/types-of-firewalls-and-their-functions.html

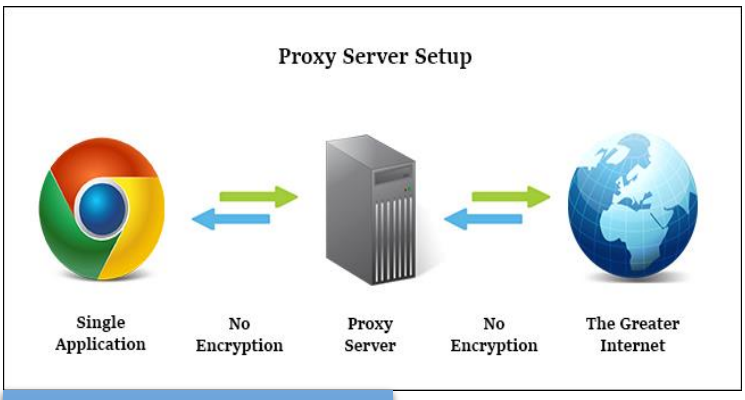

Figure 4: Proxy Server Outline
https://medium.com/@satheeshkumar_69375/what-is-a-proxy-or-proxy-server-2ac113e25876

Proxy Server

A **proxy server** requests the internet to use a website on a **browser**. In Figure 4, it shows a proxy server requesting the internet and it analyzes the network to make sure it meets the security criteria before being connected to a browser. However, one setback is that it can decrease the speed of your computer because it is actively analyzing the network for your protection.

Packet Filtering

The system of **packet filtering** is used towards examining each **packet** that is entering and exiting the network. A packet is data that is part of the network you are retrieving. The packet filtering system accepts or denies packets depending on the computers security protocols. In Figure 5 it displays a **router** being used to filter packets being retrieved from the internet.

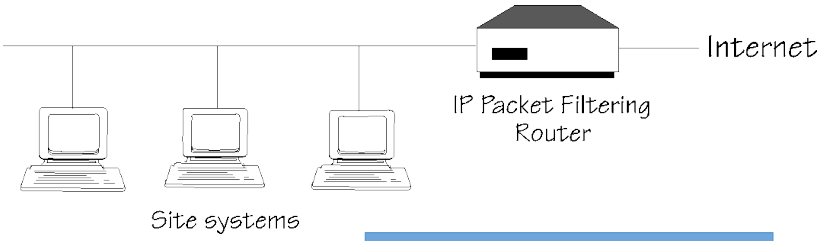

Figure 5: Packet Filtering Outline
http://www.vtcif.telstra.com.au/pub/docs/security/800-10/node55.html

Conclusion

The firewall is an important security device that everyone should install on all of their devices. This device monitors all incoming or outgoing network traffic and decides to either allow or deny access to your device based on security protocols. Without a firewall your system is open to being attacked by viruses destroying your files, software, and hardware. Also, open to hackers that can gain access to your personal data and cause you to be a victim of identity theft, or email fraud. Without the help of a firewall our devices would be vulnerable to all threats from the great internet.

References

Boston University. *How Firewalls Work*. (n.d.). Retrieved from https://www.bu.edu/tech/about/security-resources/host-based/intro/

Cisco. *What Is a Firewall?* (2019, April 12). Retrieved from https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

DataIQ News. *Government Site "leaves users open to email fraud".* (n.d.). Retrieved from https://www.dataiq.co.uk/news/news/government-sites-leave-users-open-to-email-fraud

Indiana University. (n.d.). *About Firewalls* Retrieved from https://kb.iu.edu/d/aoru