Firewalls research paper

Law, Security

\n[toc title="Table of Contents"]\n

\n \t

1. Introduction \n \t
2. How It Works \n \t
3. Types of Firewall \n \t
4. Conclusion \n \t
5. References \n

\n[/toc]\n \n

Introduction

Firewalls are responsible for keeping a check on the data that is sent to and from a private network. Firewalls are used by all big and small companies to keep their data safe from hackers. Home users can also use a firewall to protect their home network and family from unwanted users and offensive Web sites. Both hardware and software can be protected with the use of firewalls.

Every message that enters an Intranet needs to pass through a firewall. The job of a firewall is to examine each message and block anything that does not meet the set security criteria. This technology came into existence in the late 1980s after several virus attacks were reported in some of the big companies.

We have divided this paper into three parts. The first part tells about the technical specifications of firewalls. The second part lists the types of firewalls. The third part concludes the paper.

How It Works

In general, firewalls use either one or a combination of all these methods to manage traffic of a network:

- Packet filtering: This is the most basic type of firewall software. It creates filters using some pre-set rules. Packets that meet these pre-set criteria are only allowed to pass, others are flagged and discarded.
- Proxy service: A firewall proxy server is an application that acts as an intermediary between systems (Bullguard. com, 2013). As discussed, firewalls work by receiving data from the internet and sending them to the requesting system or vice versa. Here, computers first need to connect to the proxy. The proxy then initiates a new network connection, which acts as a mirror of the transfer of the information. This process does not allow both parties to directly connect with each other, which makes information all the more secure.
- Stateful inspection: This is the latest method of firewall scanning, which operates at the network layer. It is also known as dynamic packet filtering. Stateful inspection keeps a record of all network connections around a firewall. It has the unique ability to segregate packets for different connections.

Types of Firewall

There are two main types of firewalls: network firewalls and host-based firewalls (Technet. microsoft. com, 2013).

- Network firewalls: Network firewalls helps protect networks by keeping a close eye at the traffic that enters and leaves. Examples of network firewalls include Microsoft’s Internet Security and Acceleration (ISA) Server, which is

software-based and Nortel Networks Alteon Switched Firewall System, which is hardware-based.

- Host-based firewalls. Host-based firewalls are responsible for protecting individual computer regardless of the network they are connected to. Internet Connection Firewall (ICF), which comes with Windows XP and Windows Server 2003 is an example of a host-based firewall.

Conclusion

Just like a physical wall protects unwanted people from entering restricted places, a firewall protects unwanted users from getting into a private network. Whether you own an organization or you are a home user, firewalls are a must everywhere.

Firewalls protect data from being accessed by hackers and unwanted users. Firewalls are used in private networks or Intranets. They are responsible for checking every piece of information that goes through an Intranet. Only after the data meets the security criteria set on the firewall, it can go any further.

References

Technet. microsoft. com (2013). Firewalls. Retrieved from http://technet. microsoft. com/en-us/library/cc700820. aspx

Bullguard. com (2013). How does a firewall work?. Retrieved from http://www. bullguard. com/bullguard-security-center/pc-security/computer-security-resources/how-does-a-firewall-work. aspx