

An Evaluation of Firewall Technologies

Final Term Paper - Bus 503

University of Virginia

Matt Warnock

2 Jan 2005

Table of Contents

Table of Contents	2
Executive Summary	3
Introduction.....	3
Defense in Depth.....	5
OSI Model.....	5
Packet Filtering Firewall.....	8
Circuit Level Gateways.....	8
Stateful Packet Inspection.....	9
Application Level Gateway	10
Stateful Multilevel Inspection.....	11
Conclusion	13
References.....	14

Executive Summery

There are four main types of firewall technologies. Packet filtering firewalls are simple and cheap solutions. They provide good security to protect one device, such as a workstation or sever, but can only allow or deny connections by network address or port number. Circuit Level Gateways provide more protection than packet filtering devices and can protect several workstations by hiding the originators network address. They check connections at the session level by checking the “handshake” before allowing data to be sent. They are well suited to protect a home network. Application level firewalls provide protection for large networks by inspecting the data that passes through the network device. This provides a more complex configuration which can protect better, but requires more resources to implement. The most secure and efficient firewall device is the Stateful Multilayer Inspection firewall. This device implements protection found in the other three types of firewalls, and provides a faster, more efficient way of inspecting data. These devices are the most expensive and complicated to configure. Each device is useful when placed in the proper place on a network. Firewalls must never be used as the only source of security and are just a part of the multi-layer defenses on a network.

Introduction

Firewalls are one of the most popular security devices in any architecture from the personal firewall included with some operating systems (OS) to the array of firewalls used to protect large networks in companies and government organizations. A firewall is used to separate a computer or network from another computer or network by using rules to decide what kind of connections are allowed and what kind should be dropped. While

these devices do not protect against everything, this paper will review four firewall technologies to compare and contrast their functionality, configurability and effectiveness. Figure 1 – Network Firewall Location, shows an example of where a network firewall should be located, while Figure 2 – Personal Firewall location, shows how a software, or personal firewall, separates the computer from the rest of the internet.

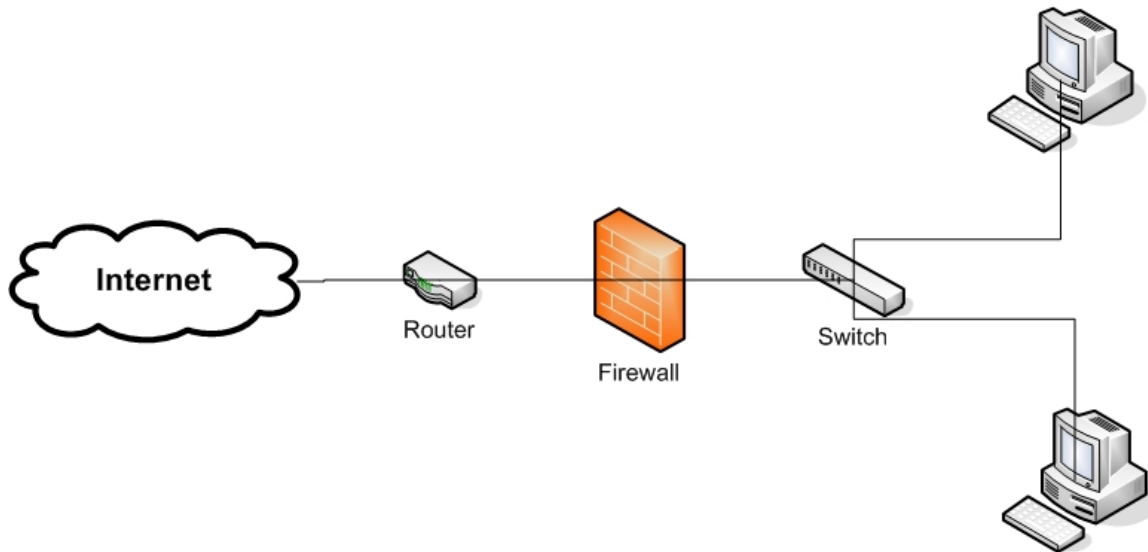


Figure 1 – Network Firewall Location

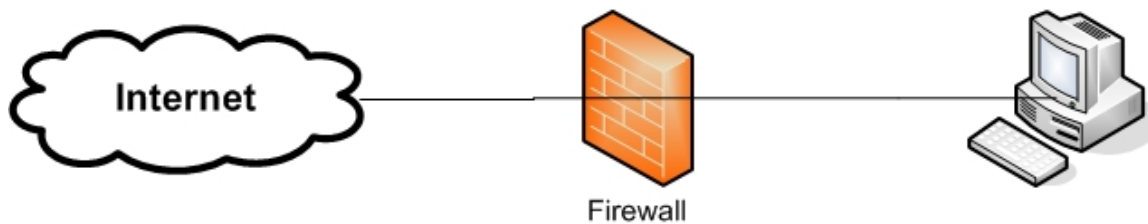


Figure 2 – Personal Firewall Location

Defense in Depth

The true definition of Defense in Depth comes from the military strategy in which you build several layers of defenses to slow an enemy. The Information Assurance (IA) version of defense in depth means creating different levels of network defenses, and not just relying on one particular product, technology or barrier to protect assets. Defense in Depth requires a balance of People, Technology and Operations. The definition of Defense in Depth means that relying on one thing, such as a firewall, or even several firewalls distributed across a network could be detrimental. Each technology has its own benefits but they are only part of the entire network architecture. Also, each firewall technology has different requirements from the people in an organization, the firewall technologies are examples of a range of technologies, and operations are required to be in place, along with firewalls, to keep the network running. Defense in Depth is taken into consideration for each firewall technology.

OSI Model

To better understand how each firewall technology works, you must understand the Open System Interconnection (OSI) reference model. This is a concept by which each task in a network connection, from a piece of software requesting information, to the electrons moving across the country, is separated into 7-layers. These layers include the Application, Presentation, Session, Transport, Network, Data Link and Physical layers. To understand the firewall technologies, you must understand the Application, Session, and Network layers.

The network layer in the OSI model performs the functions that route packets to certain destinations by their network address. A good example of this is the Internet Protocol (IP) in which each computer has an IP address and other computers on the network use this address to communicate. Each packet will have a source and destination IP address and the network layer uses this information to move packets around a network. After a packet knows where to go in a network, the session must be initiated. The session layer is used by a network system to start and stop the network session. This includes initiating the connection, the “handshake” and ultimately termination. This layer includes the Transport Control Protocol (TCP). The most high-level layer in the OSI model is the application layer. The application layer is used by software to perform network activity. This is what the user directly works with. Programs like Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP) and other software run on the application layer. Figure 3 – Layers of the OSI model, visually describes how each layer stacks, and each piece of data is passed to and from each layer.

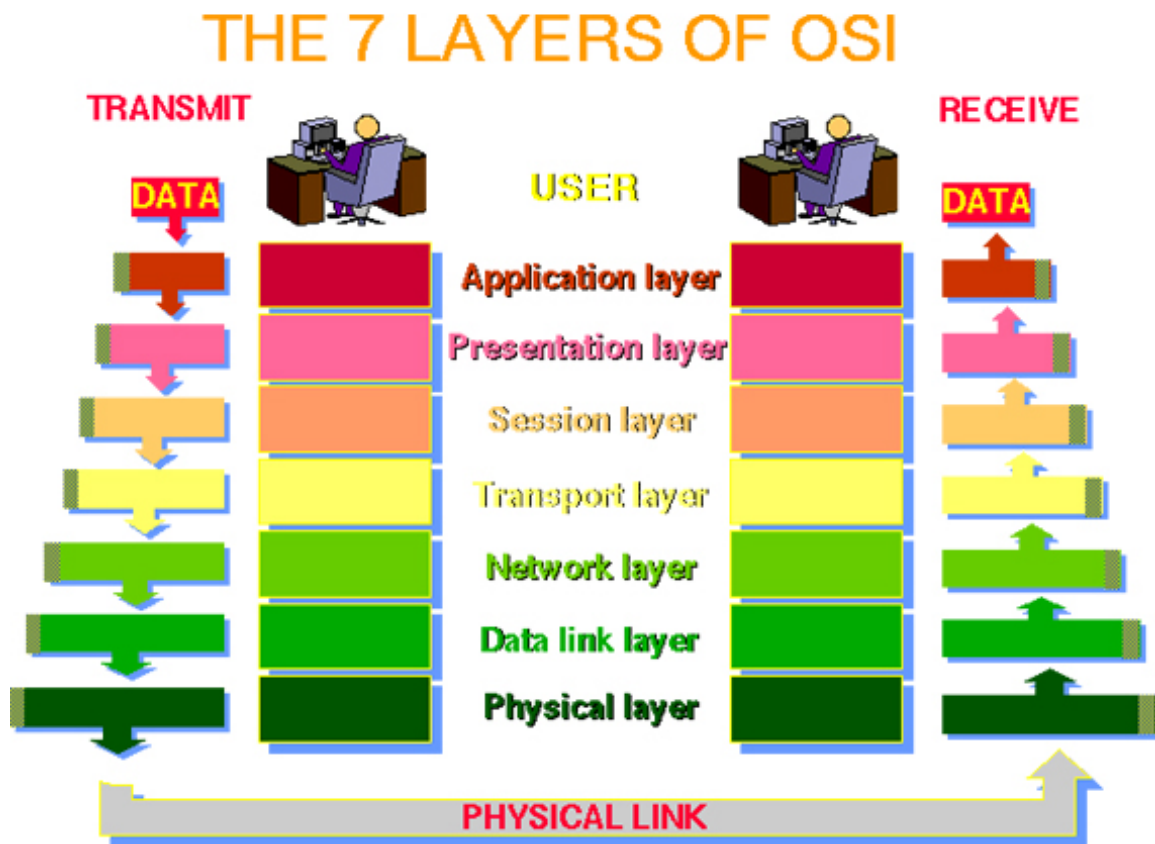


Figure 3 – 7 Layers of the OSI model (from The Abdus Salam International Centre for Theoretical Physics -

http://www.ictp.trieste.it/~radionet/1998_school/networking_presentation/index.html.)

Now that you understand Defense in Depth and the OSI model, you will see how each firewall technology utilizes both.

Packet Filtering Firewall

The simplest and most popular type of firewall is the Packet Filtering firewall. The name “Packet filtering” says a lot about this technology. Data goes over a network as frames or packets. These packets have headers with information. At the network layer of the OSI model, the IP header contains information about the source and destination IP address, and the TCP header has information about the source and destination port. This information is used by a packet filtering firewall to determine if the packet is forwarded or if it will be dropped. For example, if an internal web server is located on a network and was running a packet filtering firewall, the firewall policy may say that any computer connecting from an IP address inside the network to the web server over the HTTP port, port 80, is allowed. All other incoming traffic is denied and therefore is dropped.

This protects the web server from certain kinds of attacks, but does not allow for complicated rules and policies. It will not protect against the more sophisticated attacks which will be discussed later. The logging capability of a packet filtering firewall is also very poor. The firewall will be able to log packets and time, and whether they were denied or allowed. An example of Packet Filtering firewalls includes Windows Firewall and iptables/Netfilter for Linux.

Circuit Level Gateways

Circuit Level Gateways are a bit more sophisticated than Packet Filtering firewalls. They are able to filter network traffic by address and port, just like packet filtering firewalls, but also review the TCP handshakes found at the Session level. The source computer initiates the connection, the gateway reviews the connection information

and checks it against the rules and if it is allowed, the gateway makes the connection to the destination. The destination server sees the connection come from the gateway, not the source computer. No data is transferred until the gateway validates the connection. Then the data is forwarded to the source computer. This adds security by checking for a valid TCP handshake. Unlike Packet Filtering firewalls, IP spoofing is difficult through a Circuit Level Gateway. A Circuit Level Gateway is more secure than Packet Filtering because it only opens the port for an incoming connection after the outgoing connection is made. This prevents unwanted traffic from coming into your network. While Circuit Level Gateways protect against invalid sessions and hides the originator, it still does not protect against certain attacks, which will be discussed later.

Network Address Translation (NAT) is an example of a Circuit Level Gateway. NAT hides the IP address of the internal network from the destination host so the destination only sees the IP address of the gateway. It then uses packet filtering to move the packet to the correct originator. Cable modem and DSL routers used in many homes are examples of Circuit Level Gateways.

Stateful Packet Inspection

Stateful Packet Inspection (SPI) is an advance in Packet Filtering technology. Created by Checkpoint in 1993, SPI does the same packet filtering as simpler firewall systems, but also includes memory to remember what connections were made, and then follows the connection from beginning to end. This prevents bad incoming packets from being accepted, because the SPI firewall records outgoing connections and what should be returning. This is useful for preventing external computers from sending data to an internal computer by appearing to be a reply to a request from the internal network.

Application Level Gateway

The two previous firewall technologies looked at the network and session headers to decide if the connection was valid, but neither of them looked at what was actually being sent across a network. They did not look at the data or payload of a packet. Until recently, firewall hardware was not powerful enough to look at the data portion of the packet. This means that if a connection was made from a valid source IP address, across a valid port, and used a valid session handshake, the connection would be made, regardless if the correct data was being sent. This can open up the firewall and network to certain kinds of exploits and attacks. For instance, if a Packet Filtering or Circuit Level Gateway firewall did not allow incoming telnet traffic and allowed HTTP traffic, and a telnet server was running on the non-standard telnet port of 23, but on the standard HTTP port of 80, the connection would be valid. This is because these firewalls do not look at the content going over port 80 and assumes that it is HTTP traffic.

An Application Level Gateway, or proxy, takes the connection inspection to a new level by reviewing the application layer of a connection and thus providing a high level of security. Proxies can inspect specific commands made by an application such as GET and POST commands in HTTP. It can also inspect user activity such as logins and file access and different rules can be applied for different authenticated users. Very detailed logs about network activity can be generated from an Application Level Gateway but because of this level of detail and complexity, network performance can be impacted significantly. Also, the firewall must be configured for every type of application being used on the network. If a new type of application is created, a module or upgrade must

be added to the device. Microsoft Internet Security and Acceleration (ISA) is a good example of an Application Level Gateway.

Stateful Multilevel Inspection

Stateful Multilevel Inspection (SMLI) firewalls are devices that utilize aspects from Packet Filtering, Circuit Level Gateways, and Application Level Gateways. A SMLI can filter packets at the Network, Session and Application Layer. Connections made through the SMLI are transparent to the destination host and source and compatibility is almost never an issue. Also, instead of using the same application level filtering in other firewalls, SMLI devices use algorithms that reduce the amount of resources required to inspect packets at the application level. It also means that there are no application specific proxies that need to be installed every time a new application is used on the network. SMLI devices create the highest level of security and also have good performance but they are very expensive. This includes the resources to configure the device. The SMLI rule set is very complicated and if it is not properly configured, the firewall may not be secure. The complex rules allow for a more secure perimeter, however, requires a skilled security team or the rules will not be properly configured and may result in a less secure network. The latest version of Checkpoint Firewall-1 is an example of SMLI firewall technology.

With regard to Defense in Depth, each firewall technology has its own balance of People, Technology and Operations. Packet filtering requires the least amount of training and configuration, so the amount of resources given by people is low; however the technology it provides is not very powerful. Circuit Level Gateways require a bit more configuration time and provides a bit more protection from the technology than Packet

Filtering. Application Level Gateways require a lot of resources from people including training, configurations and policy, but the technology itself will protect better than Packet Filtering and Circuit Level Gateways. Following the same trend, Stateful Multilayer Inspection requires the most resources from people, but the technology protects better than any other firewall technology. Operations, including security policy, C&A and security management, must be included with any security configuration and therefore must be included with each firewall technology, but firewalls affect people and technology more than operations. That is why firewalls must never be the only line of defense on a network.

Conclusion

The most important thing to remember about firewall technologies is that they must be implemented by taking Defense in Depth into consideration. Each firewall technology is the best solution for different applications. The packet filtering firewall is the simplest so it is easy to configure, and is very cheap, but is the least secure. A packet filtering firewall can be used on each device to protect against a mis-configured device somewhere else in the network. A circuit level gateway firewall is also very simple and cheap to implement, but can provide added security to several computers. A circuit level gateway used for NAT can protect a home network, while each computer on the home network can use packet filtering firewalls. An application level firewall is more complicated and more expensive to implement, but provides better security. It is well suited for a large network where one configuration can protect many people and many servers. Packet filtering firewalls can still be installed on each workstation and server for more security. Lastly, a large, diverse network, which requires more protection than a network protected by an application level firewall, is well-suited to be protected by the Stateful Multilayer Inspection device.

References

“Defense in Depth”, National Security Agency – Information Assurance Solutions Group

“Packet Filtering Firewall”, National Institute for Standards and Technology,

<http://csrc.nist.gov/publications/nistpubs/800-10/node55.html>, Accessed 2 Jan 2005

“The 7 Layers of the OSI Model”,

http://www.webopedia.com/quick_ref/OSI_Layers.asp, Accessed 2 Jan 2005.

“What different types are there?”, Vicomsoft,

<http://www.vicomsoft.com/knowledge/reference/firewalls1.html>, Accessed 2 Jan 2005

“What is a firewall?”, <http://www.pc->

[help.org/www.nwinternet.com/pchelp/security/firewalls.htm](http://www.nwinternet.com/pchelp/security/firewalls.htm), Accessed 2 Jan 2005.