Firewalls for the Home & Small Business

Gordon Giles

DTEC 6810

Professor: Dr. Tijjani Mohammed

Abstract

A firewall can be in the form of hardware, software or a combination of the two. It is basically used to prevent, block, and keep out unwanted intruders from entering a network. This applies to a home, small business, or a large corporation network. A firewall monitors all of the incoming and outgoing traffic from a personal computer or a local area network. The majority of people are not afraid of their Internet connection being hacked by an outsider. The chances of suffering from some type of Internet hack are on the rise, especially when connected to the Internet using a cable modem or some type of broadband service. People are surprised when they discover that their newly installed personal firewall reports that their home computer is being scanned from the Internet many times per day. This is why it's so important to select and install a good firewall for your home or small business. The reason is simple: A firewall will help control the Spyware and Spam problems that have become so annoying with Internet usage. The research presented here will elaborate on some of the better software and hardware firewalls on the market. In today's society it is essential to have some type of firewall to protect your valuable data from the outside world.

Introduction

There are basically three ways that a firewall can allow or deny who or what gets into or out of a network. Packet filtering works as follows. Information is sent from one computer to the next, the information is not sent all at one time but broken down into what is called packets or sections of the entire message and sent along a path through the Internet. If a packet filtering firewall is used, it will examine each packet as it passes through the firewall and compares it to the filter to see if that packet is allowed to continue or not. A packet filtering firewall is vulnerable to spoofing. Spoofing is when someone like a hacker finds a way to hide his true Internet Protocol (IP) address so that he or she can get through your filter. A hacker could potentially intercept a message, alter the message, and then retransmit it taking information out or copying the message and then forwarding the message on to the intended recipient. When the hacker gets the information he can make his message seem to come from you or a trusted IP address that the filter will allow into the network (Tyson, 2005).

A proxy server is another type of firewall protection. A proxy server is a server that receives information directly from the Internet. A server is a computer that sends and receives requests for information to another computer or server. There are several different types of servers: mail, web pages, secure, and many more. There are some companies that only have one server to perform multiple functions (Mangis & Kavin, 2004). Once the proxy server examines the information and finds that the information is safe according to a set of rules that it goes by. The proxy server will then pass the information on to the client (computer) that originally requested the information. Remember if you are using a proxy server the Internet will never have a direct connection to any computer in your network. The Internet will have to talk to the proxy server first and then the information (packets) is passed on to the network (Tyson, 2005).

Another type of firewall uses what is called a Stateful inspection. A stateful inspection looks at the data packets and examines parts of the packet against known good information. This is kind of like using virus protection and keeping you virus definitions up to date. By keeping your information up to date in your firewall will know about any new threats that exist. The one thing about a stateful inspection is that if a new attack comes out before you get a chance to download the new detection you are vulnerable to an attack (Tyson, 2005).

Hardware Vs. Software Firewalls

Software firewalls are available but firewall appliances are considered to be the best choice for a small business. WatchGuard, SonicWall, and Symantec manufacture some of the best small business firewalls on the market (Ryan, 2003).

Another product type that is rapidly gaining popularity is the firewall-LAN switch combination. It serves as a firewall but also connects network devices such as workstations and printers to the network. Most of these smaller scale firewalls are plug and play but some require configuration, which is usually best left up to technical experts in order to properly configure them. The biggest lesson that small businesses can learn from firewalls is that they are only one small piece of the puzzle when it comes to network security. There are many other threats such as virus scanning, intrusion detection, and web filtering that firewalls do not address. These security concerns cannot be avoided and must be dealt with to secure even the smallest of networks (Ryan, 2003).

Hardware Firewall Advantages & Disadvantages

Advantages:

- they do not require any resources from other machines connected to the network.
- Initial configuration is complex, but limited intervention is required once it is up and running.
- a single hardware firewall can protect all the computers on a home or small office network (Zisman, 2003)

Disadvantages:

- If modifications need to be made to the firewall it can be overwhelming to the typical non-technical
- More expensive than software firewalls.
- Usually no filtering is set for outgoing traffic.
- Home models do not report on break in attempts.
- Cannot use on the road.
- No virus or Spam protection (Zisman, 2003)

Software firewalls are seen more frequently with home computers and networks. Microsoft has included an Internet Firewall Connection with its XP version operating system. "Most firewall software will come with a set of pre-established rules for well-known software on your computer that connects to the Internet." Some of the popular vendors of software firewalls are Symantec's Norton Internet Security Suite 20, ZoneAlarm, and Sygate Personal Firewall to name a few (Dowler, 2004). If you are using a home network it's best to use the firewall on the router as well as the individual software installation firewall on all your systems for added security, this will also allow you to check outgoing traffic and to protect notebooks when they're

on the road (Zisman, 2003). There are some systems that neither software nor hardware firewalls will protect them from viruses or spam. If you download a Trojan Horse or spyware program and install it on your system, you've let the 'bad guys' in past the firewall-- though a software firewall may keep the spyware from being able to report back on you (Zisman, 2003)

Software Firewall Advantages & Disadvantages

Advantages:

- They are generally very inexpensive
- They are very easy to configure (Lowe, 2001)

Disadvantages:

- Since they run on your computer they require resources (CPU, memory and disk space) from your system.
- They can introduce incompatibilities into your operating system.
- You must install exactly the correct version for your operating system.
- You must purchase one copy for each system on your home network (Lowe, 2001)

The big question that new broadband users search for is which type of firewall, hardware or software, is the best protection for their computers. The answer is both. One type of firewall is not necessarily better than the other for home use. “One downside to software firewalls is that they can only protect the computer they’re installed on, so if you have multiple computers, you need to buy, install, and configure a software firewall separately on each machine. This can get expensive and can be difficult to manage if you have a lot of computers (Pacchiano, 2001).” The perfect scenario is to have a hardware firewall for protection against attacks from the outside world and a software firewall for protection of your applications that you will be using on the Internet from your PC. Whether you end up

using a software firewall, a hardware firewall, or both you should always supplement it with anti-virus software (Pacchiano, 2001).

Case Study: Troy School District Gives High Marks to Check Point

Troy School District needed a firewall that could be managed centrally for the entire network. Troy School developed and implemented a security architecture based on the Check Point FireWall-1 security suite. The Check Point firewall allows or disallows user requests to access facilities and data inside the District's intranet and controls the resources available to users who are outside the system. Troy has developed over 20 specific firewall policies to ensure that there is only one way in and one way out of the district's IT system. “The firewall specifications were built around the Check Point FireWall-1 as Check Point is the industry leader “No other product matched up to the reliability and performance of their firewall (Troy School District, 2001).

Firewall Features To Consider

“Architecture: do you prefer a software firewall that you can install on a new or existing PC or a dedicated appliance? How many concurrent firewall sessions does the firewall need to support? How many VPN tunnels do you need to be able to run concurrently? What VPN protocols do you want to use (IPSec, PPTP, L2TP)? Do you need integration with Exchange mail servers or SharePoint collaboration servers? What type of management user interface (UI) do you prefer: command line interface (CLI), graphical management console, Web-based interface? Do you need to manage the firewall via SSH, Telnet, or SNMP? Do you need centralized management of multiple firewalls? Do you need high availability (load balancing, failover) features (Shinder, 2004)?”

Conclusion

The following questions should be considered when you are choosing a firewall. The above research should answer most of these questions. What will this firewall protect me against? Is it upgradeable? What will this cost me? Will my IT department be able to implement this firewall in a minimal amount of time? What type of training will be needed for my employees? Is the firewall that I am considering going to cost more than the resources that I am trying to protect? How much risk (company loss) am I willing to take if I go with a cheap firewall? These questions are important but whatever you can afford and implement is better than having nothing at all. I would recommend that no matter what type of firewall you get for your home or small business that in order to have the best protection your firewall should attempt to provide a multiple layer of protection instead of just one type of protection. You should consider having a packet filter and a proxy if you can swing it along with a stateful inspection type of firewall.

References

Tyson, Jeff (2005). How Firewalls Work. Retrieved November 25, 2005 from http://www.howstuffworks.com/firewall.htm

Zisman, Alan. (2003). CyberSafety: Firewalls. Retrieved October 15, 2005 from http://www.zisman.ca/Security/firewalls.htm

Ryan, Vincent. (2003). Best Firewalls for Small Business's. Retrieved October 15, 2005 from http://www.firewallguide.com/software.htm

Pacchiano, Ronald. (2003). Firewall Debate: Hardware vs. Software. Retrieved October 17, 2005 from http://www.smallbusinesscomputing.com/webmaster/article.php/3103431

Lowe, Richard. (2001). Firewalls. Retrieved 2001 from http://www.afterzed.com/lessons/firewalls.html

Troy School District Gives High Marks to Check Point. Retrieved 2001 from http://www.checkpoint.com/corporate/success/docs/troyschool.pdf

UW Firewall Configuration Diagram. Retrieved September 2004 from http://uwadmnweb.uwyo.edu/Firewall/FireWallDiagram.htm

Shinder, Deb, (2004). Comparing Firewall Features. Retrieved October 20, 2005 from http://www.windowsecurity.com/articles/Comparing_Firewall_Features.html

Mangis, Carol A. & Kaven, Oliver. (2004), Firewalls. Retrieved October 20, 2005 from http://www.pcmag.com/article2/0,1759,1618583,00.asp

Dowler M., (2004). Beginners Guides: Firewalls and Internet Security. Retrieved October 15, 2005 from http://www.pcstats.com/articleview.cfm?articleID=1450