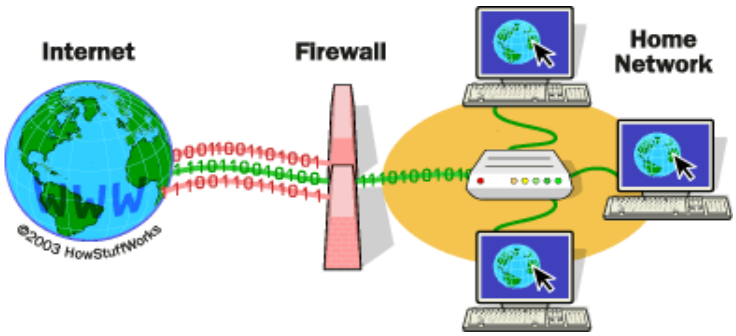
Firewalls for small business

By James Thomas
DTEC 6823
Summer 2004

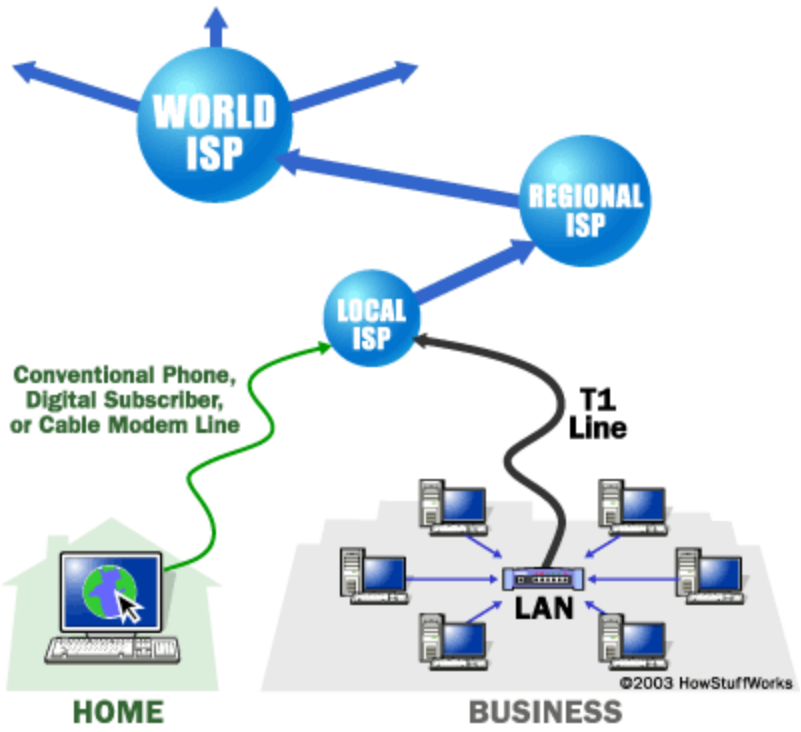
What is a firewall?

A firewall is either hardware, software or a combination of both that is used to prevent, block or should I say try to prevent unwanted information from entering your network. This applies to a home, small business, or a large corporation network. A firewall monitors all of the incoming and outgoing traffic (information) to the local area network. Notice that the firewall is located between your network and the Internet. As you can see from the illustration the firewall is filtering the information that it sees.



[1]

The following picture shows you what a typical home or big or small business Internet connection might look like and how they interact with the local Internet Service Provider (ISP).



[2]

Well before I get into the different ways that a firewall works. I do want to mention briefly how a computer sends information. First of all a computer is a digital device. What this means is that a computer processes ones and zeros only. Your computer's digital system cannot talk to your telephone company's analog system. But we do have device that translates your computers digital information into an analog signal that the telephone company's equipment will understand. That device is called a modem. The letters "MO-DEM" stands for modulation demodulation. A modem is a device that takes your computers coded ones and zeros (1, 1, 1, 0, 0, 1, 0, 1) and converts or modulates that information into an analog signal for the phone line. The modem on the other end receives that analog signal and demodulates that signal back to a digital signal for that computer on the other end.

Have you ever listen to a fax machine when it is sending information and you hear different sounds high and low pitched, if you have then your modem makes sounds

that are similar to a fax machine when it is talking to the equipment on the other end. If you did not know, we speak in an analog tone not a digital tone. One more piece of information is that an analog signal can be anything from 0 – 1. I mean that your analog signal can be .8, .5, or .3, but a digital signal is either a 0 or a 1 and nothing in between. Hence the phone line is an analog device and that is why we are able to talk into it.

Firewall types

Here are a three ways that a firewall can allow or deny what gets into or out of your network. A firewall can use packet filtering. As information is sent from one computer to the next the information is not sent all at one time it is sent in packets or sections of the entire message along the Internet. If you are using a packet filtering firewall, 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. If you are sending someone a message a hacker could intercept your message and then retransmit your message either taking information out of the message or copying the message and then forwarding the message on to the intended recipient. Either way you look at it once 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 your network.

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. I briefly want to tell you that there a could be several different types of servers: mail, web pages, secure, and

so on. There are some companies that only have one server to perform multiple functions. If were to type in www.msn.com into your Internet browser. You are actually sending a request for information from the msn web server. The msn web server acknowledges your request and then sends you the appropriate information that you requested. There are quite a bit more that takes place but that is beyond the scope of this article. 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. 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 know 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.

Who needs a firewall?

In a small business environment you might have anywhere form one to several employees. Just imagine that you spent a lot of money on some new computers for your business. You decided that since you got a great deal from the computer vendor you would upgrade your office so that your office staff will finally be able to do their in the minimal amount of time. Keep in mind that your employees have been with you for a

long time. As your business expands you decide to hire more employees and buy new software to improve productivity. All is going well until you find out that your network does not work like it use to. One of your employees went to an Internet site that not only compromised your network but it put a virus on your system and wiped your system out completely. Something that you did not think about was training, policies, and at the minimum some type of firewall.

Just imagine that when you go home today you open the door and the house is empty. You try to figure out what happen and how did someone get into your house and steal all of your valuables. This is the one time that you forgot and YOU left your door unlocked. So what happen, someone evidently checked the door to your house and found it to be open. Let's think about this situation. A computer system is the same thing as your house. Your computer information is the same thing as your valuables inside of your house. Remember you can replace the contents in your house but what about the hard work or customer files that might have been on the server, network or local hard drives of one of the computers in your company. If this has happen to you then you know what I am talking about. If this has happen to someone that you know then you need to be aware of how costly this can be to a company now matter how big or small.

If you have information that is worth having it is worth saving. If you are responsible for keeping someone's private information confidential which is a part of the government's privacy act of 1974, meaning that you are required to safeguard: social security numbers, personal data, etc. Then you need to consider securing your information with some type of firewall to help you block a lot of unwanted traffic. Unwanted traffic can be anything from someone that is: pinging your network (checking

or trying all the doors in your house), sending you annoying pop-ups, sending you web pages that you do not want into your network. The list could go on and on. I do want to make a comment here. No matter how much money you spend on your system. There will is still a chance that someone one day will find a hole or a back door into your system. Take Microsoft as an example from time to time you need to download a patch. Why? Because someone found a way to get into something that you wanted to keep private.

There are a lot of companies that sell firewalls. I am not endorsing any of these products in any way. I am merely trying to show some of the firewall products on the market and where you might be able to turn to in order to get help if you need it for your small business.

Conclusion

I am going to recommend that no matter what type of firewall you get for your company. I believe 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. What I mean is that you should consider having a packet filter and a proxy if you can afford it along with a stateful inspection type of firewall. I want you to consider these things whenever you are choosing a firewall. 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 low end firewall?

Reference page

[1] http://www.howstuffworks.com/firewall.htm
[2] http://computer.howstuffworks.com/web-server3.htm
Leak test
http://www.grc.com/lt/scoreboard.htm
Small business firewalls – good information
http://www.pcmag.com/article2/0,1759,1618583,00.asp
Firewall and Proxy Server how to
http://www.tldp.org/HOWTO/Firewall-HOWTO.html
Definition of a proxy server
http://www.webopedia.com/TERM/P/proxy_server.html
Best Firewalls for small business
http://www.newsfactor.com/perl/story/21741.html

Here is a list of places where you can find different vendors that sell firewalls
Network Security Store
http://www.networksecuritystore.com/
Firewall product selector
http://www.spirit.com/cgi-new/report.pl?dbase=fw&function=view
Datamation Product watch
http://products.datamation.com/security//firewalls/
Norton Internet security
http://www.symantec.com/sabu/nis/nis_pe/
Zone Alarm
http://www.zonelabs.com/store/content/home.jsp

Articles for a better understanding on firewalls and possible problems
Beginners guides to firewalls and Internet security
http://www.pcstats.com/articleview.cfm?articleID=1450#
Principles of information security – by: Michael Whitman and Herbert Mattford
Firewall support
http://service.real.com/firewall/
How firewalls work
http://www.howstuffworks.com/firewall.htm
Small Business Security
http://www.keepmedia.com:/Register.do?oliID=225
Cyber Intrusion
http://www.smallbusinesscomputing.com/biztools/article.php/3092501