Global Information Assurance Certification Paper

Firewalls: What I Wish I'd Known When I Was Getting Started

William S. Davis

September 20, 2000

Introduction:

I knew I needed a firewall even before my first detected root compromise, I just wasn't sure where to begin or what I needed to know. It took six months after this precipitous event before I had a firewall in place. In retrospect, if I had had a simple roadmap to point me in the direction of the issues I needed to understand, the learning curve might not have been as steep, and the process completed more quickly.

The purpose of this paper is to be a preparatory guide for implementing a firewall. I intend to identify important issues and concepts encountered while designing and implementing a firewall, and point to resources that will assist in the process. The sections further below break this process into three parts, the preliminary skills, firewall design and implementation.

What is a Firewall?

Most everyone has heard the term and has some idea of what it does, but a common misconception is that a "firewall" is a **single** machine that you drop into your network to protect you from malicious internet activity. A firewall is more accurately a logical gateway that allows you to control access into and out of an internal network.

To quote directly from Zwicky, Cooper and Chapman(1):

"A firewall is very rarely a single physical object, it is a logical choke point. Usually, it has multiple parts, and some of these parts may do other tasks besides act as a firewall."

A common firewall design consists of a perimeter network positioned between the internet and the internal network. The perimeter network is connected to the internet by an exterior router, and to the internal network by an interior router. This interior router filters and controls traffic to the internal network. Additional hosts on the perimeter network provide various services such as email and web access. The "firewall" in this example consists of two routers and one or more additional hosts, all on a perimeter network.

There is often some confusion about what a firewall can and cannot do. A firewall can reduce the risk of unwanted outside intrusion but cannot protect against threats that occur from within. Firewalls are only part of what is commonly referred to as "defense in depth," e.g. physical security, host security, user education and the need for an overall security policy. A firewall implements a security policy, it does not define that policy. A firewall allows you to control and log only traffic that passes through it and cannot control or detect traffic that bypasses it. Firewall logs can be a great help in intrusion detection. Firewalls can't fully protect against all threats, especially viruses. The advent of new vulnerabilities means that firewalls must be maintained and routinely reevaluated if they are to be effective.(1)

Another common misconception is that the more expensive the firewall is, the better security it provides. The diverse market provides for a variety of solutions. The best solution for you will depend on your needs and network environment.(2)

By understanding your security needs, the capability and limitations of firewall technology, and the level of expertise necessary will be a great benefit in the design and implementation of a firewall. I'll begin with the level of expertise needed.

Preliminary Skills:

I started my initial research into firewalls in the typical manner, reading books and taking some tutorials offered at conferences (see Firewall 101 below). However, I would have absorbed the material more thoroughly if I had a better grasp on some of the basic internet services and network management skills.

Basic Skills:

This paper assumes at least a familiarity with the basic System Administrator's skills, but as a bare minimum, you must know how to download, configure, compile and install software on your system to be able to implement a firewall. Of course, the level of expertise required depends on the complexity of the environment.

Basic Internet Services:

The IP protocols define the transport mechanisms and services that will be allowed or blocked by the firewall. The terms ICMP, TCP, UDP, DNS, FTP, HTTP, NetBIOS, NNTP, NTP, SMTP, SSH, and Telnet, should all be very familiar to you. These are some of the most predominant protocols and services that traverse the internet. Each of these protocols are defined in documents called Requests for Comments (RFC). An index of these can be found at http://www.cis.ohio-state.edu/htbin/rfc/INDEX.rfc.html.

Additionally, it is critical to understand the mechanism for initiating communications between two hosts on the internet, especially the TCP "three way handshake," and the various TCP "flags."

Excellent references for detailed explanations of these protocols are Steven's TCP/IP Illustrated, Volume 1. (see http://www.kohala.com/start/) or the online IBM reference at http://www.redbooks.ibm.com/pubs/pdfs/redbooks/gg243376.pdf (a free registration is required.)

Associated with these protocols and services are a bewildering array of numbers. There are ICMP type and code numbers which define request and error messages, commonly used TCP and UDP port numbers which identify services, and a large body of other options and address of significance to the internet. It may be helpful to stick some of these to the side of your monitor, but a web page at http://www2.dgsys.com/~lkh/ipnumb.html, has compiled a comprehensive list.

Network Management:

Three important network management concepts I found I needed to master were the configuration of multiple network interface cards (NICs) within a single host, variable length subnet masks (VLSM), and Network Address/Port Translations (NAT/PAT). These are critical interdependent issues when designing and implementing a firewall, so it is essential to understand these concepts.

When a machine has multiple NICs the network traffic can be directed to another router on the network, or to another NIC within the machine. If forwarding of traffic is allowed between the NICs, the machine acts as a router. If forwarding is disabled, an application can act to transfer traffic between the NICs. The concept is important, as this distinguishes between a "packet filter" or "proxy server" component of a firewall.

These multiple interface cards are the gateways to the various partitions, or subnets, of your local area network (LAN.) How your firewall is designed will determine how many interface cards are needed, how they are configured and how your network is partitioned. In the example mentioned in the introduction, only two NICs might be required for an interior router, one to connect to the perimeter network and one to connect to the internal network.

There are two references by O'Reilly and Associates on TCP/IP Network Management, one for Unix and one for NT that provide detailed information on configuring the network interfaces and routing tables. (See Reference Books below)

How a LAN is partitioned depends on the network address space available. In most cases, it will be necessary to subdivide the address space. This is done using VSLM. A LAN can be partitioned into multiple subnets with a single subnet containing as few as two, but usually more, usable addresses. Subnet size is independent of other subnets, but the number of addresses and boundaries that can be assigned to a subnet are based on binary arithmetic. The resultant subnet mask, when assigned to an NIC, will limit it's inward traffic to only that specific subnet address space. Excellent articles on VSLM are:

Demystifying Netmasks http://swexpert.com/C4/SE.C4.MAY.98.pdf
Variable-Length Subnet Masking http://swexpert.com/C4/SE.C4.NOV.98.pdf
Variable Length Subnet Masking
http://www.geek-speak.net/subnet_mask/vlsm3.htm

Finally, Network and Port Address Translation (NAT/PAT) is the concept of changing the source or destination address for NAT, or port number for PAT, of an internet connection. This allows for a legitimate exchange between two hosts on the internet, while one, or both of those host are not revealing their actual network address. This is a method that can not only improve security when used with the RFC 1918 non-routable address space(3), but can be used to increase the number of available IP address for your network by mapping many IP addresses into one, or many into a small pool of addresses.(4)

For more on NAT see the article Network Address Translation at:
http://www.sans.org/infosecFAQ/net_add.htm

Microsoft has also put together an introduction on TCP/IP that covers much of the above mentioned concepts, especially in regards to NetBIOS, and includes an extensive VLSM section. It can be found at:
http://www.microsoft.com/technet/deploy/tcpintro1.asp

Firewall 101 (Conferences and References):

There are numerous courses on Firewalls that will immerse you in the vocabulary and basic principles of firewalls. If funding is available, a conference track on firewalls will get you started quickly. Additionally, getting away from the office can allow you to concentrate on the material.

The SANS (System Administration, Networking, and Security) Institute offers a number of conferences across the United States each year. The SANS GIAC (Global Incident Analysis Center) certification and training program offers their

curriculum at these conferences, and most recently, the program is also available online. The current locations and dates of events can be found on their web site at http://www.sans.org. Be prepared to study at night rather than visiting all those vendor hospitality suites.

The USENIX Association and SAGE (System Administrator's Guild) also jointly sponsor a number of conferences in the United States each year. The LISA and LISA-NT conferences focus on Unix and Windows NT environments respectively, though not exclusively. Many of the same experts who lecture for SANS also lecture at these conferences. See http://www.usenix.org/events/events.html for a calendar of sponsored conferences.

Other conference sponsors include:

CERT http://www.cert.org/nav/training.html

Internet Society http://www.isoc.org/isoc/conferences/

Interop http://www.interop.com

Great Circle Association http://www.greatcircle.com/tutorials/bif.html

(a Firewall Course taught by Brent Chapman!)

A list of reference books worth having in you library are listed at the end of this paper under the heading "Reference Books."

Firewall Design:

As I mentioned above, a firewall is rarely just a single machine, although some vendors may try to put all they can onto one machine. A firewall is usually made up of a combination of methods that address your security needs. What solutions you use will depend on what services you wish to provide and the level of risk you can tolerate, as well as the financial and personnel resources that are available.(5)

The following describes the firewall design process in its three aspects, the security policy, the "buy or build" dilemma, and the network design.

Defining your needs, the security policy:

It is during this phase that a site survey should be made to determine what services already exist. Deciding what services will continue to be provided, what will be prohibited and what new services are needed, will go a long way in defining a firewall. However, it is a security policy that defines what your firewall will allow or disallow. The firewall implements and enforces this security policy.

A good introduction to writing security policies is:

What Do I Put in a Security Policy? http://www.sans.org/infosecFAQ/policy.htm

while a more formal and technical document is:

"NIST Special Publication 800-XX INTERNET SECURITY POLICY: A TECHNICAL GUIDE" http://csrc.nist.gov/isptg/html/ISPTG-6.html#Heading66

One important aspect which sets the tone of your security policy is your initial firewall stance. It is usually one of the following:

Everything not specifically permitted is denied.

Everything not specifically denied is permitted.(6)

Often, it may seem easier to permit everything and tighten the firewall policy as you gain experience. By going thoroughly through the creation of a security policy, you can define exactly what you need, making decisions about what is really critical, and what you are able to deliver in a secure enough manner. It is generally recommended that the "default denied" stance be chosen. If you can get management and users to sign onto the security policy, it provides the authority to implement the firewall and will help blunt the complaints when services that had been available are no longer allowed. It can also provide a process for adding new services that meet the established criteria.

Evaluate the available products, Buy or Build:

The question of buying a commercial product or building your own firewall from freeware comes down to more a question of time, money and expertise. There are many firewall products to choose from. The "Firewall Buyers guide" http://www.icsa.net/html/communities/firewalls/buyers_guide/index.shtml provides a two part document that defines the terms and technology of firewalls in Part I and then in Part II uses standardized descriptions of the firewall products to allow for comparisons.

Unfortunately, it does not include some of the common freeware products such as:

Linux IP Chains	http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html
IP Filter	http://coombs.anu.edu.au/~avalon/ip-filter.html
Firewall Toolkit	http://www.fwtk.org/

Two points are worth mentioning. First, you can mix and match the commercial and freeware products as you need, you aren't locked into one product line. Second, you must understand how each one works and what their capabilities are to make an informed decision and justify the purchase. The amount of time spent evaluating may be greater than the time required to build your own.(1)

If you have the time, but not the money, building your own will be a great educational opportunity. However, make sure to keep a journal of the process to document the issues encountered and decisions that had to be made. It will be of great help to those who follow.

If you have the money, but lack the expertise or time, you will still learn a great deal during the evaluation period. Make sure to define your needs and know that the product(s) will perform as needed.

Network design:

Laying out the firewall design requires an understanding of the firewall technologies as well as the network infrastructure required. This is when you will need to determine the firewall architecture that best suites the services and products you have settled on. This is where the studying you did in Firewall 101 will pay off.

There are a number of terms that are used, such as bastion hosts, screened subnets, DMZ, or perimeter networks that can be confusing, especially when used together, like a split-screened subnet with dual-homed host.

The term "screened" usually refers to packet filtering, where a multi-interfaced host is acting as a router. The term "dual-homed host" refers to a multi-

interfaced proxy server with forwarding between interfaces disabled. The term "bastion host" indicates a system which acts as a receiver for incoming connections from the internet. As such, they require a high level of security. Bastion hosts may function as servers for services such as DNS, FTP, HTTP, SMTP, Telnet or SSH, but may also act as proxy servers for the internal network. A perimeter network is a subnet on which various firewall components are connected.

Another term that may often causes confusion is the DMZ (demilitarized zone), as opposed to a screened subnet. A true DMZ is a network that contains hosts accessible from the internet with only the exterior, or boarder, router between them. These hosts are not protected by a screening router. As such these hosts are vulnerable, and should have tight security. A screened subnet may also be a collection of hosts on a subnet, but these are located behind a screening router. The term DMZ may be used by a vendor to mean either, so it is best to verify which they mean.(7)

A simple design would be to have a boarder router leading to a DMZ which contains a screening router for an internal subnet, and several bastion hosts that act as server for DNS, FTP, HTTP, SMTP and SSH. The HTTP server might act as both a Web server to the internet and a Web proxy server to allow web access from the internal hosts to web sites on the internet.

There is a great section of do's and don'ts in Chapter 6 of Zwicky, Cooper and Chapman's *Building Internet Firewalls* (see Reference Books above) entitled "Variations on Firewall Architectures" that is valuable reading, especially in the design phase. I highly recommend it.

Implementation:

Implementation issues have a lot to do with planning, human factors and most importantly, verification that the firewall is really working.

Planning and Human Factors:

You did the research, you designed the firewall, you got all the pieces, and now you are ready to put it all together and get it running. There is going to be some down time, so let everyone know what you're doing. One additional step I took, and which still helps out in an emergency, is I used an old spare Cisco router to act as an emergency bypass for my screening router. It didn't provide much security, but it did allow me to configure some basic access control lists. With it configured and ready to boot, I could power up and patch in the old router, keeping the network up, while I dealt with the misconfigured, or crashed, screening router offline. Another approach would be to have a mirrored system available, but it is generally recommended that you do not have two screened routers attached and functioning for the same internal network.

Verification:

A firewall is only a good security tool if it is properly configured to perform the tasks defined by the security policy. If it is poorly configured, a false sense of security could make a bad situation even worse. It is important to not only verify that the firewall implementation is working, but it needs to be done routinely.

The logging capabilities are a key factor of the firewall. If you don't log firewall policy violations, how can you detect a hole in your firewall? Initially, it may be beneficial to log liberally and spend some time getting acquainted with what is normal legitimate traffic for your environment. As the

verification process continues, cutting back on logging "understood" events will help reduce "false positives" and encourage the continued examination of the logs.

In the course of normal traffic, you will start to see the nefarious incidents that occur daily, letting you know that the firewall is acting as planned. It is prudent to do some proactive testing, trying to defeat some of the security policies strictures. It is better you find a misconfiguration, or vulnerability, before someone else does. Use tools installed on a host in your perimeter network to probe you defenses, even such tools as ping, traceroute, telnet, or scanning tools like Nmap or Satan. (See "Nmap – The Tool, It's Author and It's Implications" at http://www.sans.org/infosecFAQ/nmap.htm.)

Finally, these firewall logs can be an additional log file used for intrusion detection purposes. They should be archived and referred to when tracking down a security incident. They may also come in handy if you need to prove your system did not victimize another system.

Summary:

This paper has pointed out a number of issues and concepts that should be understood while designing and implementing a firewall. A firewall is not just a box to plug into your network, but is a collection of techniques and services that provide a logical gateway between an internal network and the internet. It is important to understand not only the protocols you wish to use, but the network management issues of NIC configuration, variable length subnet masks and network address translation. These services and concepts can be combined in a variety of products and architectures to implement a security policy. The firewall will continue to need to evolve. Through testing and monitoring for vulnerabilities and new threats, as well as repeated iterations of the design process, you can maintain the level of security required by your security policy. Hopefully, by knowing of these issues before beginning to design and implement a firewall, the time required will be shortened and a more secure firewall design achieved.

References:

(1) Zwicky, Cooper and Chapman. *Building Internet Firewalls*. Second Edition. Sebastopol, CA: O'Reilly and Associates, 2000. pp. 21-32

(2) Ranum, Marcus. "How to Pick an Internet Firewall." October, 1998. http://www.icsa.net/html/communities/firewalls/buyers_guide/app_b.shtml (18 Sep. 2000)

(3) Stewart, John N., "NAT/PAT—How Can It Help Web Security?" April, 1998. http://webserver.cpg.com/ws/3.4/index.html (18 Sep. 2000)

(4) Conoboy, Brendan. "IP Filter Based Firewalls HOWTO." Sep. 2, 2000. http://www.obfuscation.org/ipf/ipf-howto.txt (18 Sep. 2000)

(5) Zwicky and Chapman., "Firewall Design." SunWorld August, 1996. http://www.sunworld.com/sunworldonline/swol-01-1996/swol-01-firewall_p.html (18 Sep. 2000)

(6) Semeria, Chuck. "Internet Firewalls and Security, A Technology Overview." 1996. http://www.3com.com/nsc/500619.html (18 Sep. 2000)

(7) Cole, Eric. "Firewalls and Perimeter Protection" December, 1999. SANS SNAP Conference Notes Course 2.2, Colorado Springs, Colorado.

Reference Books:

Albitz and Liu. *DNS and BIND*. Third Edition. Sebastopol, CA: O'Reilly and Associates, 1998.

Cheswick, and Bellovin. *Firewalls and Internet Security*. Reading, MA: Addison-Wesley, 1994.

Hunt, Craig. *TCP/IP Network Administration*. Second Edition. Sebastopol, CA: O'Reilly and Associates, 1998.

Hunt and Thompsom. *Windows NT TCP/IP Network Administration*. First Edition. Sebastopol, CA: O'Reilly and Associates, 1998.

Zwickey, Cooper and Chapman. *Building Internet Firewalls*. Second Edition. Sebastopol, CA: O'Reilly and Associates, 2000.

The new edition of Zwicky, Cooper and Chapman's *Building Internet Firewalls* is a updated version of the comprehensive guide to understanding the concepts and mechanics of a firewall. Additionally, it contains a very nice appendix that lists resources, giving a brief description of each. It includes web pages, FTP sites, mailing lists, newsgroups, organizations, papers, conferences and books. (http://www.oreilly.com/catalog/fire2)

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor