Global Information Assurance Certification Paper

Firewall on a Budget

GSEC V1.4b

Scott Schimkowitsch

Table of Contents

Firewall on a Budget

Abstract

The objective of this document is to investigate an affordable firewall solution for small businesses. Additionally it is an important component in a company's security policy. Our goal is to make this one facet as affordable as possible. While implementing a firewall is by no means an end-all solution that will secure a company's intellectual assets, "a firewall is considered a first line of defense in protecting private information". [7]

Introduction

Security awareness has increased significantly within the last year. Companies are concerned with all aspects of security, from physical to virtual breaches. In a recent survey from NetworkWorld, network executives were surveyed on what concerns them most. The number one response is not surprising, 81% of the individuals that participated in the survey responded, "securing the corporate network". The same survey went further and discovered that 47% of network executives queried did not believe that their company's firewall and filtering software met the security requirements of their organization. Additionally, over 40% of the companies surveyed planned to purchase additional security software by the end of the year. [2]

A 2002 Computer Crime and Security survey performed by the Computer Security Institute had the following highlights: [3]

- Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.
- Eighty percent acknowledged financial losses due to computer breaches.
- Forty-four percent (223 respondents) were willing and/or able to quantify their financial losses. These 223 respondents reported $455,848,000 in financial losses.
- As in previous years, the most serious financial losses occurred through theft of proprietary information (26 respondents reported $170,827,000) and financial fraud (25 respondents reported $115,753,000).
- For the fifth year in a row, more respondents (74%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%).

Throughout the industry, in similar surveys and media coverage, the IT community paints a dismal picture of security breaches that happen on a daily basis. Although most surveys focus on larger businesses, smaller businesses are just as susceptible to security breaches. What about the security needs of these small businesses? The idea of having to protect their network seems daunting, unrealistic and cost prohibitive to most small business

owners. Most small businesses have the same requirements as their larger counterparts, but do not have the budget or resources to spend thousands of dollars to secure their network.

Firewall Components

In the following analysis, firewall components will be broken down into three categories: hardware, operating system, and software. All components will first be evaluated on cost. After the pool of components has narrowed the three categories of components will also be individually screened and selected based on their reliability, ease of installation, configuration and maintenance.

Firewall Hardware

The hardware selected for our budget firewall will be an Intel-based computer, (at least a x586) with two network interface cards (NIC). An Intel-based hardware platform is chosen simply because of its ready availability and open standards. A new name brand server can cost several thousand dollars, but for our requirements generic or previously used equipment can meet our needs. Many companies, including small ones generally have access to a retired machine. In our case the machine for our budget firewall was obtained at no cost, including the two NICs. The PC has an Intel 233 MH processor 64 MB of RAM and a two gig hard drive. If an extra machine is not readily available, several online vendors can usually provide adequate hardware for one hundred dollars or less (US currency).

Firewall Operating System

Now that the hardware platform has been chosen and procured, an operating system must be decided upon. Vendor specific operating systems can cost several hundred if not thousands of dollars for a single license. For this reason a Linux OS is chosen because a copies can be legally obtained for free at www.linuxiso.org. There are dozens distributors of Linux and when deciding on which version of Linux is best for you, research pays off: download, install, and test as many different versions as time will allow. A great resource for comparing the various distributors of Linux is www.distrowatch.com. [4] The distribution of Linux that was chosen for our budget firewall was Redhat and was obtained for free. The drawback is that the free download is completely unsupported. Any issues that we may run into must be resolved on our own unless a support agreement is purchased. Arguing which distribution is best could easily be a paper within itself and is ultimately an individual decision. Redhat is the most widely used distributor, extremely easy to install compared to other distributions, and has an enormous amount of free resources available on the web for support.

Firewall Software

The third and final component of our firewall component is the firewall software itself. According to www.webopedia.com, the definition of a firewall is:

> "A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria." [12]

Firewall Technologies

There are three different kinds of firewall technologies: packet filtering, proxy service, and stateful inspection.

Packet Filtering

A packet filtering firewall examines network traffic's packets through the third, or network layer in the OSI reference model. (See appendix B for details on the OSI reference model). An example of a packet filtering firewall is a router. Many routers have the capability to limit certain traffic with a user predefined list call an access control list (ACL). Devices acting as a packet filtering firewall examine each packet that enters or leaves the network and either allows or denies the traffic based on the access list.

There are several advantages to a packet filtering firewall. A packet filtering firewall can be reasonably effective and is generally inexpensive. Packet filtering is faster than application layer gateways, or proxy firewalls, and is generally transparent to the end users as far as network performance is concerned.

The disadvantage of a packet filtering firewall is the limited security due to the limited packet screening that occurs above the network layer. Packet filtering firewalls generally have limited logging capabilities and become difficult to manage as the access list becomes larger. It is not uncommon to see access lists that have grown to several hundred lines that are extremely challenging to maintain, especially when multiple administrators are involved.

Packet filtering firewalls are also susceptible to IP spoofing. IP spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host. [13]

Application Layer Gateways

Proxy or application layer gateways are firewalls that work from the network layer up through the application layer of the OSI model. Proxy servers work by making requests on the behalf of your clients. An example would be a server that sits between a client application, such as a Web browser, and a real server. The proxy server intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server. [12]

The advantages of a proxy are that it offers better security than a packet filtering firewall. Proxies accomplish this by examining all content from the application layer.

The disadvantages of a proxy application layer gateway are that network performance generally suffers and firewall tasks are not transparent to the end user. Scalability is limited because each service requires its own application gateway, so if a new application is added then an additional application gateway must be added to accommodate the new service. Proxies also neglect information contain in the lower layer of the OSI model.

Stateful Inspection

The third kind of firewall type is known as stateful inspection or alternately as dynamic packet filtering. This method does not examine the contents of each and every packet, but instead compare certain key parts of the packet to a database of trusted information. [14] Stateful inspection firewall works at the network layer of the OSI model, examining not only packet header like a packet filtering firewall, but the contents of the packet up through the application layer as well. Since the contents of packets are examined all the way up through the application layer, more information is gathered than just the source and destination on the packet. A stateful firewall examines a network connection, uses that information to build a state table. The state table is then used to determine what packets are allowed and which ones are denied by what packets have previously passed.

Stateful evaluations can be based on the following four states: new, related, established, and invalid. Any new attempt to connect to the network through a stateful firewall will be examined when attempting the new connection. Connections related to an existing connection and going in the original direction will be examined. Established state is the attempt to match a part of existing connection. An invalid state exists when a connection attempt doesn't match any known prior connection. [13]

Benefits of a stateful inspection firewall include excellent security due to the full application layer awareness. Second, stateful inspection provides transparent protection in that end users should not notice any performance changes on the network.

However, stateful inspection firewalls are costly. Most stateful inspection firewall vendors charge several hundred, even thousands of dollars for a license that would accommodate a small business.

For our firewall we must choose a firewall with stateful inspection if possible. There are numerous firewall software options to choose from. A large assortment of research and comparison of products can be found on the Internet. A great place to compare and research is http://www.networkbuyersguide.com/search/105242.htm or http://www.spirit.com/cgi-new/report.pl?dbase=fw&function=view. [6], [5]

Considerations

An additional consideration is that most small business will be using Network Address Translation, or NAT. NAT is an industry standard that allows the translation of one IP address to another. Generally a company will use private network range for internal traffic, their Intranet, and use NAT to share one registered IP address to external traffic, the Internet. An added benefit of using NAT is that it acts as an extra security measure by hiding the IP addresses of devices on the internal network to outside intruders. Firewalls, routers, servers, and devices solely dedicated to provide network address translation.

To conform to the needs of an inexpensive firewall solution it would be preferred that the chosen firewall solution run on a Linux based operating system. With these criteria we scoured the web for a possible solution and found a Linux based firewall solution project called IPTables. The IPTables solution is a stateful firewall without the major drawback, cost. IPTables firewall has a memory of each connection passing through it, therefore meeting our stateful inspection criteria. A web site that compares several different IPTable configuration tools can be found at: http://online.securityfocus.com/infocus/1410.

Finial Firewall Component Selection

As mentioned previously, an Intel based machine utilizing Linux Redhat operating system will be used. The firewall software chosen for the budget firewall is called gShield. GShield was written by Godot and can be down loaded from http://muse.linuxmafia.org/ at no cost. [8] gShield is an IPTables firewall script that utilizes Linux's built in firewall capabilities. gShield is presented as being easy to set up "out of the box" with minimal configuration for the average user.

gShield has many addition benefits. First, gShield also has the ability to support NAT for multiple private IP ranges. Second, the standard "out of the box" configuration comes with aggressive blocking of both incoming and outgoing traffic. Third, gShield supports both static IP address and dynamically assigned addresses. Fourth, the set up and configuration is support by a well- commented BSD-style configuration file. Lastly, gShield has a TCP wrapper like functionality that is added for access to services. A wrapper is software that accompanies resources or other software for the purposes of improving convenience, compatibility, or in this case, security [4]

Installing Redhat Linux

A standard install of Linux is assumed. There are many books that have several chapters dedicated to installation instructions and troubleshooting. For the purpose of this paper there will only be a brief overview of installing Linux. Not all Linux installations are trouble free. The good news is there is a good chance that others have run across your exact problem. The Internet has thousands of Web pages and User groups dedicated to free Linux support.

The first step is to check and make sure that your hardware is compatible with the Redhat Linux operating system. A hardware compatibility list can be obtained from Redhat at http://hardware.redhat.com/hcl/. [9] The GNOME or KDE environment installation requires minimum of 1.5 Gigabytes (GB) of hard drive space. (See appendix A for explanation of both GNOME and KDE). If installing both GNOME and KDE environments it is necessary to have a minimum of 1.8GB of free disk space available.

Once the hardware is ready place the Linux CD in the machine and boot to the CD. Press **Enter** to start a new install and follow all default settings. The installation of Redhat 7.3 is well documented and answers most installation questions. If all questions are not answered in full, there are several places to find help mentioned above.

Installing gShield

After downloading gShield 2.8 unzip the files by using the command '*gunzip filename.tgz*'. Once the files are unzipped, untar them by using the command '*tar xvf filename.tar'*. When untaring the files, place them in the /etc/firewall directory. Although untested during this installation, the installation notes state that placing the tarball in the /etc directory will install the files automatically in the /etc/firewall directory. The gShield installation notes recommend installing and configuring gShield locally and strongly warns users against trying a remote installation. Individuals who attempt a remote installation could easily find themselves unable to access their machine. With this in mind, take the installations notes warning seriously and do not attempt a remote installation.

Configuring gShield

After installing gShield, open a new terminal and use an editor (vi was used in our configuration) to view and make necessary changes to the gShield configuration file. All configuration settings are located in /etc/firewall/gShield.conf. The configuration file is very well documented and makes configuration easy to accomplish.

While gShield's instructions state that the default settings will work for most Users' needs, they do recommend to take the time and look at the default configuration so that it is clearly understood by the installer what actually is being allowed and what is blocked. The default settings are geared more toward the individual user, which will of course be the vast majority of the individuals using gShield. To accommodate our small business, several modifications were made.

Interface Configuration

The business for our firewall setup has a registered static IP address; so a few interface configurations must be made. A change to the default setting of STATIC=”NO” to STATIC=”YES” must be made. Since our machine is multi-homed, meaning it has multiple NIC cards, we must first change the default setting of MULTI=”NO” to MULTI=”YES”. This will let gShield recognize and work with a second network interface. Next, each interface must be configured. To configure which interface connects to the outside world, or Internet, the local interface or LOCALIF must be modified. The default configuration is LOCALIF=”eth0”. The internal interface, the one connected to the private LAN, must be configured. The default is INTIF=’eth1”.

DNS Server Configuration

gShield is configured to automatically detect and configure domain name service (DNS) servers that are provided by the Internet service provider (ISP). The security policy of our small business would prefer that specific DNS server’s IP addresses be manually entered into the firewall’s configuration. This is accomplished by changing the default setting of DNS=”auto”, to simply inserting each specific DNS server’s IP address in place of the word “auto”. If multiple DNS server’s addresses need to be listed, separate the addresses with a space.

DHCP Configuration

Dynamic Host Configuration Protocol (DHCP) is used to ease administration of IP address by temporally leasing them to clients instead of assigning them a permanent IP address. gShield is set up by default to obtain IP address automatically from the ISP. Since this is not necessary for our deployment, the default setting ALLOW_DHCP_LEASES=”yes” to ALLOW_DHCP_LEASES=”no”. gShield is also setup to provide NAT services by default. Since this service is already provided by another device, disabling this feature is necessary. To turn off the NAT attribute, change to configuration from NAT=”yes” NAT=”no”

Remote Access Configuration

A tremendous advantage that gShield has incorporated is the administrator feature. gShield allows specific hosts complete and unrestricted access. This feature can be used by changing the default setting ADMIN_HOST=”no” to ADMIN_HOST=”yes”. gShield provides a high level of security against IP spoofing by requiring not only a specific IP address, but also the host’s machine’s MAC address. The configuration for each are as follows: ADMIN_HOST_IP=”x.x.x.x” and AMIN_HOST_MAC=”xx:xx:xx:xx:xx:xx”

Mail Configuration

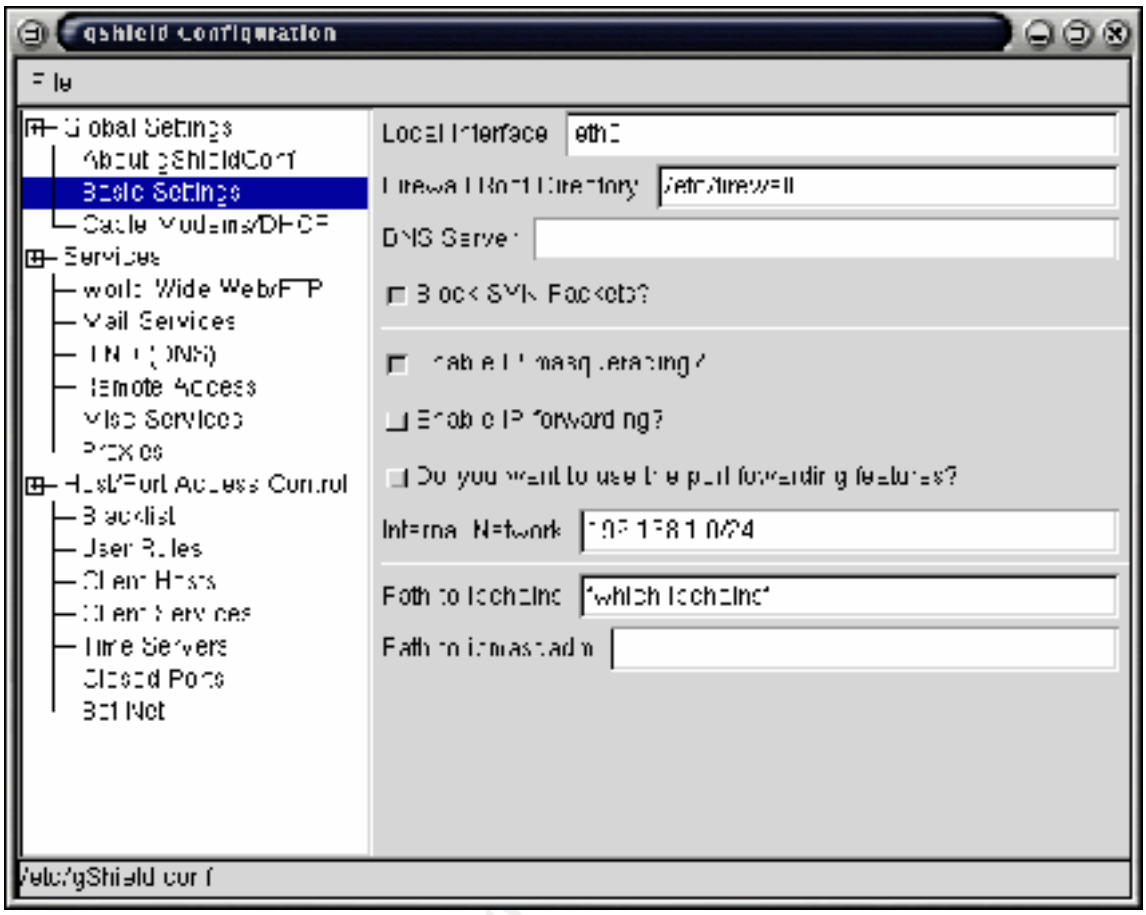
Since the company this deployment is being done for uses a Web-based email solution provided by its ISP, configuring mail is not an issue for this particular install. It is common for business, even small businesses, to use SMTP services for email. Some small companies even implement and support their own email. Be aware that SMTP services are disabled by default in gShield.

Blocking High Ports

gShield's standard settings drop all high port traffic. High port traffic is defined as any port number that is greater than 1024. In most cases this setting would not affect the average user. In our case our company needs to make allowances for certain clients that use collaboration software with other users outside of the private network. To add these clients access to high port numbers, change the setting ALLOW_ALL_HIGHPORTS to the conf/highport_access. To allow these users access to the high ports we must change the default settings. Replace the "no" in ALLOW_ALL_HIGHPORT="no" to reflect which specific hosts can access these high ports. If the setting is changed to "yes" this will disable the high port protection and open all high ports to the outside world.

GUI Interface

There is a graphical user interface (GUI) interface that is offered for previous releases of gShield. As of this writing the GUI interface was not available for the latest gShield release 2.8. The previous release, 2.7.1, does however have the GUI interface available. Setting up the GUI interface will still require someone familiar with Linux to install, but once installed the GUI interface makes administrating, especially those who are uncomfortable with Linux, much more user friendly. The following is a screen shot of gShield Configuration GUI taken from the creator, Vince Hodges's Web site: [10]



[10]

When deploying gShield the pros and cons must be weighed when deciding on if to use the previous release with the GUI interface available or use the latest version. The pros are that the administrator taking over the installation can easily do so. The con of using the GUI interface is the fact that the latest version will not be used. In our installation the latest version of gShield was decided on because the administrator is the same person setting it up and the company does not except any changes in the near future i.e., future growth, change in ISP, etc.

Deployment

The default set-up of gShield is designed for an individual setting up a firewall on their personal machine, so minor adjustments must be made. In our test deployment we found out that certain users were using collaboration software that used certain high ports that are automatically blocked by default settings. Although a minor set back, it could be very troublesome for someone without a lot of experience with firewalls.

Conclusion

Overall the budget firewall project was successful. The small company was able to utilize the security benefits of a firewall without an excessive outlay of funds. It is important to keep in mind that a firewall is by no means an end-all solution. A firewall

should be coupled with a security policy and procedures that must be stringently enforced. The ease of administration will continue to depend on the experience of the individual administering the firewall. Initial deployment is a much more difficult venture than managing the firewall once it is set up. An individual who is new to the Linux operating system will definitely need to reference online help or someone experienced in Linux. Even after weighing in the skills needed installation and maintenance, gShield is strongly recommended as a Budget firewall solution.

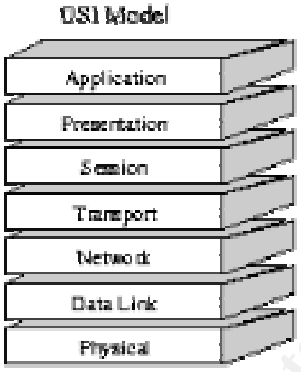
Appendix A

GNOME is an Acronym for GNU Network Object Model Environment. GNOME is part of the GNU project and part of the open source movement. GNOME is a Windows-like desktop system and is not dependent on any one-window manager. The main objective of GNOME is to provide a user-friendly suite of applications and an easy-to-use desktop. [11]

KDE is an Acronym for K Desktop Environment. KDE is a network-transparent contemporary desktop environment for Linux and UNIX workstations, and it is part of the open source movement. [11]

Appendix B

Basic Network Design - The OSI Model



[1]

International Organization for Standardization (ISO) created the **Open Systems Interconnection (OSI) reference model** as a framework for defining standards for connecting computers. [16]

ISO defined OSI as a **seven-layer model** that can be broken down into upper layers and lower layers. The three upper layers are typically referred to as the Application layers, the four lower layers are known as Data Transport. Each layer performs functions to communicate with its appropriate peer layer in the other system, i.e. PC. Further each layer of the model provides services to the next higher layer. [16]

References

1.) "Basic Network Design - The OSI Model." URL: http://www.compnetworking.about.com/library/weekly/aa052800a.htm (1 August 2002).

2.) Cox, John. "Survey: Security remain Job 1." 20 May 2002. URL: http://www.nwfusion.com/news/2002/0520nw500.html (22 July 2002)

3.) "Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row." 7 April 2002. URL: http://www.gocsi.com/press/20020407.html (22 July 2002)

4.) DistroWatch.com. 29 July 2002. URL: http://www.distrowatch.com/ (29 July 2002)

5.) "Firewalls." Network Security Buyer's Guide. URL: http://www.networkbuyersguide.com/search/105242.htm (29 July 2002)

6.) "Firewall Product Selector." Spirit.com. 28 March 2002. URL: http://www.spirit.com/cgi-new/report.pl?dbase=fw&function=view (29 July 2002)

7.) "firewall." Webopedia. 5 February 2002. URL: http://www.webopedia.com/TERM/f/firewall.html (30 July 2002)

8.) "Godot's Muse" 5 May 2002. URL: http://muse.linuxmafia.org/ (22 July 2002)

9.) "Hareware: main." Support and Docs. URL: http://hardware.redhat.com/hcl/ (23 July 2002)

10.) Hodges, Vince. "gShieldConf," URL: http://members.shaw.ca/vhodges/gshieldconf.html (1 August 2002).

11.) "Is Your Hardware Compatible?" Red Hat Linux 7.3: The Official Red Hat Linux x86 Installation Guide. URL: http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/install-guide/s1-steps-hardware.html (5 August 2002)

12.)"IP spoofing." Webopedia. 4 June 2002. URL: http://www.webopedia.com/TERM/I/IP_spoofing.html (31 July 2002)

13.) "Proxy Server." Webopedia. 4 August 2002. URL:

http://www.webopedia.com/TERM/p/proxy_server.html (31 July 2002)

14.) Sully, Bob. "IPTables Firewalling." 11 August 2001. URL: http://www.malibyte.net/iptables/iptables.html (5 August 2002)

15.) Tyson, Jeff. "How Firewalls Work" URL: http://www.howstuffworks.com/firewall1.htm (30 July 2002)

16.) Vinny. "OSI Model Overview." URL: http://compnetworking.about.com/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.routeru.com%2Find%2Fosimodel%2Fosi_model.htm (25 August 2002).