Global Information Assurance Certification Paper

SOHO Firewall Savvy

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b

Maureen F. Lamb
January 26, 2003

Maureen F. Lamb

GIAC Security Essentials Certification (GSEC)
Version 1.4b

Option 1

SOHO Firewall Savvy

Abstract:

A firewall for a SOHO (Small Office Home Office) is the first line of defense and plays an important role in an overall security strategy. Because a SOHO has limited resources, the firewall product they implement must be relatively easy to use and maintain, and be cost-effective. This paper will attempt to provide some guidelines for choosing, installing and configuring a firewall for a small office. Specifically it will do the following: First, define a firewall and explain why a small office needs one. Second, provide a checklist of evaluation criteria for selecting a firewall and explain their importance. Third, explain the implementation and maintenance of a firewall based on a real world example. In addition, this paper will explain the various features of what a firewall can do and why it is essential. The Sonicwall SOHO3[1] firewall was used as an actual example of a hardware firewall installed in a small office. It was chosen because it is ICSA[2] certified and met the criteria for "must have" features in a SOHO firewall, which will be outlined below. This paper will elucidate some of the issues small businesses are faced when considering firewalls as part of their overall security plan.

What a Firewall is

A firewall is a network device that restricts access from a trusted source to an untrusted source. Practically speaking for a company, this usually means a firewall protects its private trusted network from that of the untrusted public network, the Internet[3]. It can filter information coming into a network by the use of rules that restrict which materials are allowed into a network. [4] A firewall by

[1] SOHO3 firewall is produced by the Sonicwall Corporation, http://www.sonicwall.com/products/vpnapp.html
[2] ICSA is a division of TruSecure Corporation (www.truesecure.com) which provides testing and certification of security products
[3] Mandy Andress, Surviving Security: How to Integrate People, Process and Technology (Indianapolis: Sams Publishing, 2002), 142.
[4] Bruce Brown and Marg Brown, "SOHO Security: Small Network Security Concepts," Extreme Tech, 27 Feb. 2002 < http://www.extremetech.com/article2/0,3973,14560,00.asp>.

default is designed to "deny all traffic except that which is explicitly allowed."[5] A firewall can record security threats to your network in a log, allowing a detailed historical analysis of threats made against a network. There should be a distinction made between a software firewall (also known as a personal firewall) versus a hardware firewall. A software firewall is an application that runs on a desktop and primarily checks the outbound connections to the Internet from the PC. A hardware firewall is a network device (commonly called an "appliance") comprised of software, which primarily protects the perimeter of a network. Its main function is to evaluate the inbound connections to the network. The authors Bruce and Mary Brown in their article, "Small Network Security Concepts" explain that despite having a personal software firewall, data packets can reach a PC and invade an Operating System. The authors maintain that it is better if security checks are initiated outside the network by a hardware firewall.[6] Computer experts recommend using both types of firewalls to best protect a network. "For the best security, get both. The hardware guards your network, while the software provides a second line of defense and keeps an eye on your internet-enabled applications."[7] The focus in this paper will be on hardware firewalls and will discuss software firewalls in only a very general manner.

What a Firewall Does and Why a SOHO Needs One

The threats to the security of a network from the Internet are numerous and change almost every day. In an article entitled, "Security Statistics Abound: What Do They Tell Us? " author Mark Joseph Edwards points out that security attacks are increasing for computer systems. In fact they were up 27% in 2002 over the previous year. The Computer Emergency Response Team (CERT) reported 2148 security breaches for the first half of 2002 compared to 2437 for all of 2001 and a total of 1090 in the year 2000. [8] A list of the Top 20 security threats compiled from the SANS group (System Administrator Network Security), FBI and National Infrastructure Protection Center (NIPC) can be found on the SANS website (www.sans.org). [9] One example from the list is that of unprotected sharing of drives in Windows systems. Drives that are not configured properly could allow a hacker to gain access to private information from a business's network.

Applying the latest software patch (antivirus or OS) or turning off a service running on a host machine can eliminate many of these threats. These can be relatively simple fixes for a trained IT person. For many small businesses, however, there may be no dedicated or trained IT person to keep their network

[5] SANS GSEC course Security Essentials Day 3, Information Risk Management, 1-21
[6] Bruce Brown and Marg Brown, "SOHO Security: Small Network Security Concepts," Extreme Tech, 27 Feb. 2002 < http://www.extremetech.com/article2/0,3973,14560,00.asp>.
[7] Konstantinos Karagiannis and Matthew D. Sarrell, "Keep Hackers Out: Part One, Personal Edition", PC Magazine 19 Nov. 2002 < http://www.pcmag.com/article2/0,4149,651565,00.asp >.
[8] Mark Joseph Edwards, "Security Statistics Abound: What Do They Tell Us?" 24 July 2002 http://www.windowswebsolutions.com/Articles/Index.cfm?ArticleID=26037.
[9] SANS, "Sans/FBI Top 20 List" http://www.sans.org/top20/

safe. The demand to keep systems current may be greater than the resources permit. Outsourcing these functions probably is the best option. In a perfect world, all of the up-to-date security patches and fixes should be applied on a regular basis. However, this is not realistic for a small business and thus a firewall can be a buffer from the daily onslaught of Internet threats. "By blocking traffic to these ports [those that are commonly attacked] at the firewall or other network perimeter protection devices, you add an extra layer of defense that helps protect you from configuration mistakes."[10] However, it must be mentioned that a firewall must be part of an overall security plan. It protects the perimeter of the network and as will be discussed later in this paper, it can be still be subverted by either a modem, Trojan software or even attacked from inside a network.

The firewall "multitasks" as it secures a network. It can protect the network from hackers who launch attacks such as DOS (Denial of Service). It can also filter unwanted and potentially dangerous code such as Active X Controls and Java. It can also block access to newsgroups and certain web sites and cookies.

How does it actually accomplish all of the above? It uses a technique called stateful packet inspection. This technique examines the contents of the packets, the source and destination addresses and ports in determining whether a packet will be admitted to the network. The state of the inbound and outbound connection is considered. Incoming packets will be allowed if there is a corresponding legitimate outgoing packet. On the other hand, a "spoofed" incoming packet that does not have a legitimate outgoing packet will be blocked from the network. [11] Now that it has been explained what a firewall is and what it does, the next section will explain how to select one for a small business.

Evaluation Criteria for Selecting a SOHO firewall

There are countless firewall appliances available for the SOHO. Firewalls come equipped with many different types of options and accompanying price tags. They can be either software that run on a desktop or a hardware appliance. The latter options, hardware appliances, are a better option for a SOHO because they require less time to maintain than software on individual desktops. Managing one device is easier and more time-efficient than multiple software applications. As already mentioned, it is preferable to use both firewall software and a hardware firewall for optimum security protection. However, this is a tradeoff between increased security on the one hand and more resources for purchasing, configuring and maintaining on the other. For some businesses, one firewall may be all they can support. If faced with that choice, then a hardware appliance would be a better option for the reasons already cited.

[10] SANS, "Sans/FBI Top 20 List" http://www.sans.org/top20/
[11] http://www.icsalabs.com/html/communities/firewalls/buyers_guide/FWguide99.pdf, 31.

The price for any security option must be considered when evaluating a firewall purchase. Prices for SOHO firewall appliances are in the in the $300-$1, 000 price range the variability being largely whether or not more features or VPN are required.[12]. Firewalls for larger companies, which typically require both VPN and HA (High Availability) are considerably higher priced. In addition, it is advisable to hire someone with firewall experience for installation and checking it periodically to ensure it is working properly.

Narrowing down the choices for purchasing one can be accomplished by using a checklist of essential criteria for a firewall appliance. In her book Surviving Security, Author Mandy Andress provides several criteria for evaluating firewalls.[13] Additionally, a firewall certification guide for Small Businesses is provided by ICSA Labs which tests and certifies security products. [14] Additionally ICSA offers a buyers guide for firewalls, which is also very helpful. [15]
A composite checklist from the above sources is comprised below. A description of each of these criteria follows on the next page.

√ Network Compatibility
- Throughput Speed
- Number of Users
- Supports NAT (Network Address Translation) and HA (High Availability)
- Supports network services (HTTP, FTP, SMTP, etc)

√ Features
- Filtering Technology (Packet Filtering, Proxy, Stateful Inspection or Hybrid)
- It should support Authentication Technologies such as digital certificates or SecurID for example
- Logging and Alerting
- Reporting

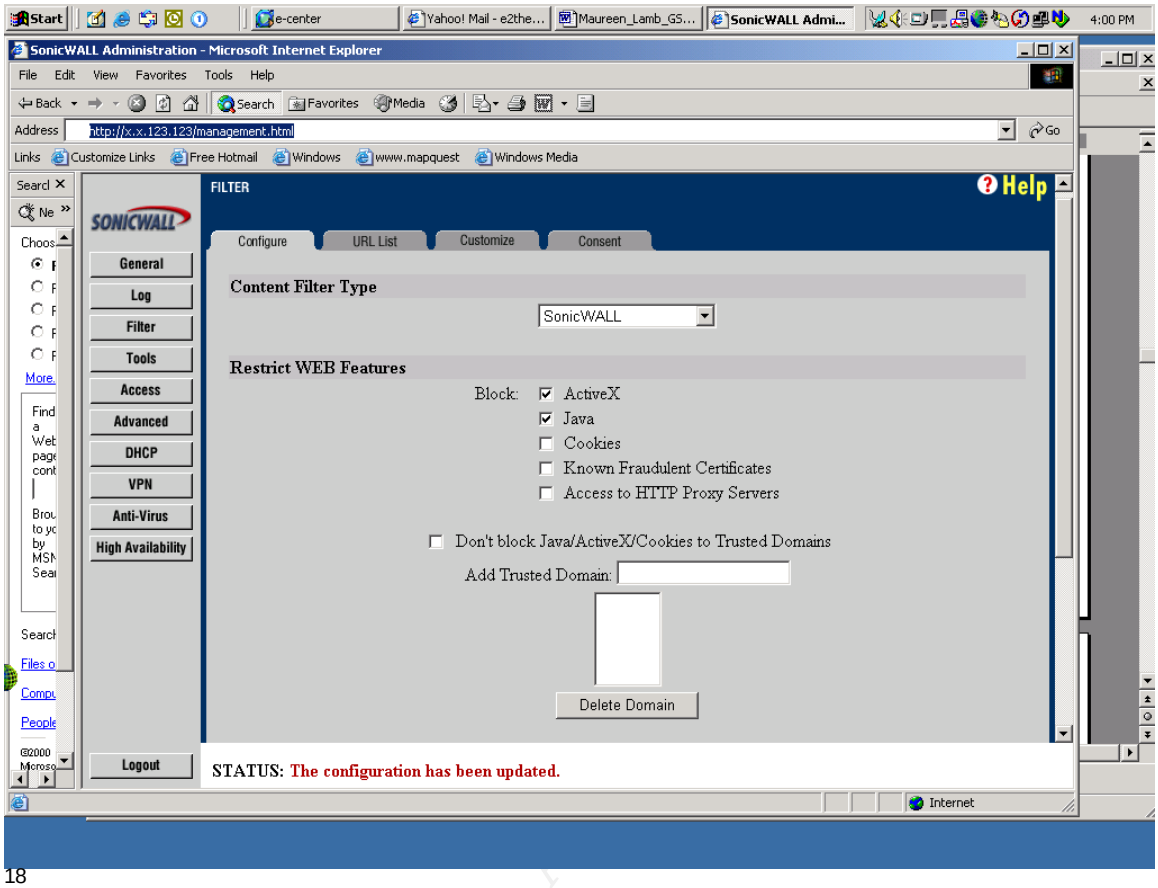
√ Management of Firewall
- Web Browser Interface or Management Console
- Ability to manage several firewalls remotely from one location
- Firewall should be relatively easy to configure when security policies change or firmware upgrades are needed

[12] Nextag Search Engine on SOHO Firewalls Nextag – Compare Prices Before You Buy Home Page http://www.nextag.com/serv/main/buyer/OutPDir.jsp?node=&otherForm=n&doSearch=y&advanced=n&search=soho+firewall&searchnodeid=-1
[13] Mandy Andress, Surviving Security How to Integrate People, Process and Technology (Indianapolis: Sams Publishing, 2002), 161.
[14] ICSA Labs "Required Services Security Policy - Small/Medium Business (SMB) Category module - version 4.0", Dec. 2002 <http://www.icsalabs.com/html/communities/firewalls/certification/criteria/SMB.pdf>
[15] ICSA Labs, "Online Firewall Buyers Guide", Dec.5 2002 http://www.icsalabs.com/html/communities/firewalls/buyers_guide/index.shtml

This section of this paper will now explain these criteria by the use of the Sonicwall SOHO3 firewall. The first criterion, network compatibility, ensures that the firewall can operate as quickly as the network itself. It also will consider the maximum number of connections allowed. [16] The SOHO3 firewall supports an unlimited number of users, 6000 concurrent connections and has a speed of 75 mbps.[17] The actual network configuration for the SOHO (described on page 10) supported 3 users and had a network connection speed of 10 mbps. The actual capacity of the firewall far exceeded the network requirement of the small office. The SOHO3 supports both NAT (Network Address Translation) and HA (High Availability). The chief advantage of NAT is that it hides the true IP addresses of hosts on a network and translates it to a public IP address for the Internet. This capability of hiding the true IP addresses of the network provides an additional layer of security for the network. High Availability refers to the ability to switch over to another backup firewall in the event of failure of the primary firewall. The SOHO3 supports all the standard network protocols: HTTP (web), FTP (file transport) and SMTP (mail), as well as others.

Features of the firewall are another key consideration when evaluating a purchase for one's company. For instance, the ability to filter unwanted or inappropriate information from the Internet based on certain key words or certain web sites is very helpful. The SOHO3 uses a stateful packet inspection filter technology. This means that the content of the network packets as well as the source and destination IP addresses are examined before being delivered. Since the information on the web is constantly changing, it should be relatively easy to make changes to the firewall rule set as required. The following diagram shows the interface for setting up the filter rules on the SOHO3 firewall. Restrictions on Active X, Java, Cookies, etc are easily done by checking the appropriate box on the filters tab.

[16] Andress, Surviving Security, 181
[17] Sonicwall, "Sonicwall SOHO3 Firewall" http://www.sonicwall.com/products/soho3.html



18

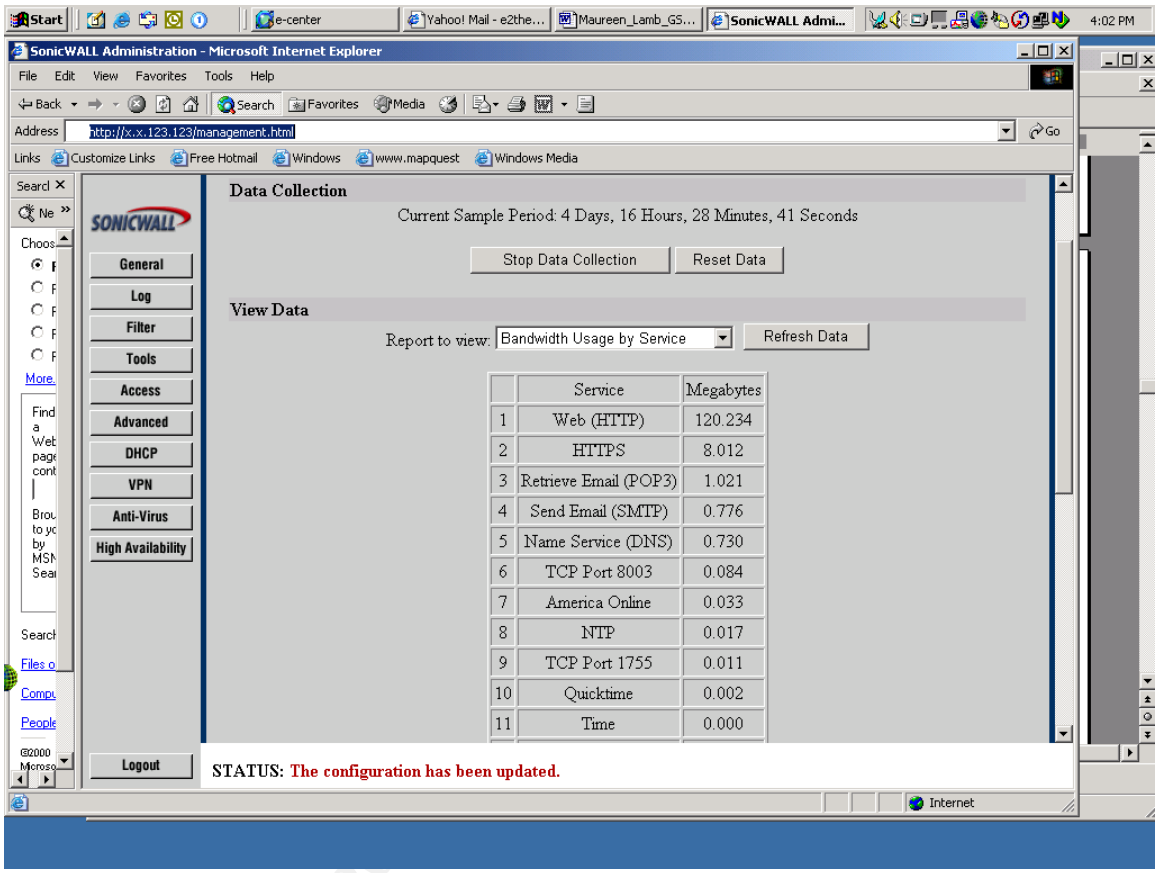
Ease of use or managing a firewall is another important consideration. For example, making changes to the options or settings for the firewall should be easy to do. The ideal situation is to have a web-interface, which calls up the master controls for the firewall from any workstation on the network. The administrative tool available with the SOHO3 product can be viewed using a web browser. Maintaining updates for the firewall (the firmware) is essential and are handled by clicking on "update firmware" in the tools section of the admin tool. Changing settings, viewing the logs and adding additional options to the firewall are easily accomplished through one centrally available tool.

Monitoring What the Firewall is Doing

Other features that are essential to a firewall are logging and reporting. This is necessary to ensure that the firewall is working as designed and to create alerts for any serious attacks on the network. "…an unmonitored firewall is almost as much of a threat to your client's security as no firewall at all, because it can lure them-and you-into a false sense of security about the level of protection that it provides."[19] Reports on Internet activity can be viewed through the

[18] Sonicwall, Sonicwall Management Interface for SOHO3 firewall appliance
[19] Thom Stark, "Locking up Network Security" Var Business November 11, 2002, 58.

administrative tool seen below. A summary of email, web, TCP and other services are available for analysis of network activity.



[20]

Logging the events (i.e. potential intrusions) to your network is an important job of your firewall. Examining log files on a scheduled basis are imperative to ensure that the firewall is working properly and to also identify any potential "holes" in your network security.

Below is a sample of a log of produced by the firewall.

Date/Time	Event	Source IP and Port	Destination IP and Port
01/13/2003 09:42:23.592	Sub Seven Attack Dropped	x.x.123.123, 3040, WAN	x.x.123.123, 27374, WAN
01/13/2003 09:42:23.480	Net Bus Attack Dropped	x.x.123.123, 3039, WAN	x.x.123.123, 12345, WAN

This particular entry is highlighted in yellow to emphasize the seriousness of the potential intrusion. The entry shows an attempt of a Sub Seven attack. This is a

[20] Sonicwall, Sonicwall Management Interface for SOHO3 firewall appliance

Trojan, which attempts to install software on a victim machine, which then allows it to have full control of that machine. The log shows the default port number of 27374, which is one of several this program uses on a system it is attacking. A Net Bus attack is another Trojan, which establishes a TCP connection with a victim machine and has the ability to take remote control of it. It typically uses the port number 12345 or 12346 when launching an attack. [21]

Another example of a log entry is as follows:

01/19/2003 00:06:13.096	ICMP packet dropped	x.x.123.123, 8, WAN	x.x.123.123, 8, WAN	'Ping'

Here is an example of the firewall preventing the network command "ping" from reaching a host on a network. The description of the event is ICMP, which means Internet Control Message Protocol. This protocol provides information about the status of a network. The ping command is a commonly used ICMP command which tests whether a host is functioning or "alive" on a network. A ping command sends an ICMP echo request and an echo reply is expected. Network administrators commonly use this command to troubleshoot hosts on a network. However, it is not a good idea to let a potential hacker know that your host is "alive" because it reveals a machine that can be potentially compromised.[22] The firewall is providing the proper security to the network by preventing this ICMP protocol from occurring. These logs can be viewed through a web browser using the sonic wall administration tool or alternatively can be emailed. Paged alerts about severe attacks can also be set up.

It is a good idea to test the software firewall running on the desktops in a network. They should be tested on a periodic basis to uncover any holes where a potential intrusion could occur. A company called Gibson Research Corporation offers a free test for personal software firewalls called the "Leak Test". This test checks the firewall on a computer to ensure that it is not allowing Trojans, spy ware or other viruses from accessing the Internet. [23]. Another test on the same web site called ShieldsUP! tests a firewall to see if an inbound connection can be made to a computer on the network and identifies any open ports.[24] It is important to ensure that both inbound and outbound connections on the network are adequately protected. Having both software and hardware firewalls provide security in depth. Problems not detected by a hardware firewall hopefully would be caught by the software firewall and vice versa.

Installing a Firewall

[21] SANS Security Essentials Course- Day 3 "Vulnerability Scanning", 2-12-15
[22] Eric Maiwald, Network Security: A Beginner's Guide, (Berkeley: McGraw Hill 2001), 257.
[23] Steve Gibson, "Leak Test", <http://grc.com/default.htm>
[24] Steve Gibson, ShieldsUP! < http://grc.com/default.htm>

This section will detail the installation of the SOHO3 firewall. This firewall was installed on a heterogeneous peer-to-peer network. This firewall was configured without a VPN but it should be noted that it is possible to add that option for additional security for remote users who need access to the network.

The environment was comprised as follows:

Hardware	Memory	OS	Software Applications
WKS 1 Dell	128 MB	Windows 98	MS Office 97 Panda Titanium Antivirus Zone Alarm Pro Firewall
WKS 2 HP Laptop	128 MB	Windows 2000	MS Office 2000 Norton Internet Security Professional (Includes Application Firewall and Antivirus)
WKS 3 IBM	128 MB	Windows 2000	MS Office 2000

All workstations were connected to the SOHO3 firewall appliance with an Ethernet cable and shared a cable-modem Internet connection. The network connections for workstations were a speed of 10 mbps.

The first step in installing a firewall is to get the network information from the Internet service provider. This can be a difficult step. Some Internet providers will tell you that a firewall can be used with their cable modem or DSL. However, they will not support any issues with firewall products. Thus, it can be difficult to get the information needed from the ISP in order to set up a firewall. Conversations with the ISP technical support staff and gleaning information from their website provided the network information needed. This is essential to correctly configure and set up the firewall. The first thing you need to know is which of the following IP addressing methods are used:[25]

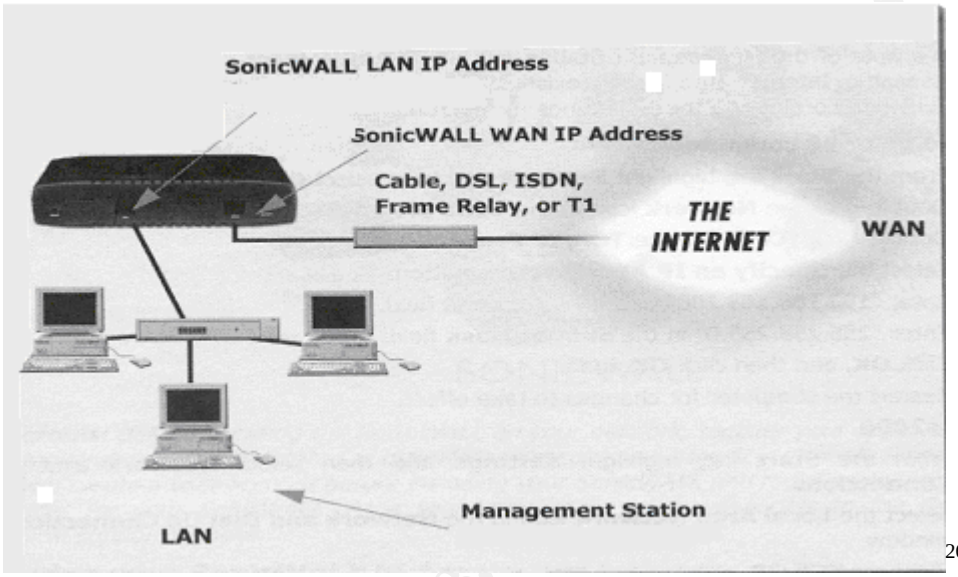
1. Is a static or dynamic IP address provided from your Internet Service Provider?
   If it's static (doesn't change), you also need to obtain the gateway IP address, subnet mask and DNS IP address.

2. DHCP (Dynamic Host Control Protocol), which means you, obtain an ip address from the DHCP server of your ISP. This is the usual addressing mode used by cable modem users. The IP address is not static but changes based on the IP addresses available from the DHCP server.

[25]Sonicwall, Sonicwall InstallationGuide, 26.

3. PPOe also known as Point-to-Point Protocol over Ethernet. A username and password are used to authenticate your machine to the ISP and is typically found with dial-up Internet accounts.

The physical setup of the firewall proceeds as follows: the firewall is connected directly to the cable modem or DSL device with a network cable and then all workstations are connected to the firewall. The diagram bellows shows the setup of the firewall appliance to the network.



[26]

[26] Sonicwall, Sonicwall Installation Guide, 21.

The firewall then needs to be installed with software, which is supplied by the vendor. This configures the hosts to the firewall on the network by specifying the appropriate IP addressing method. The first step for setting up the firewall is to set up the management station on the network that will control the firewall from any PC. The next step is to configure the firewall with the IP addressing information supplied by your ISP. The final step for configuring the firewall is to configure the workstations on the network. The settings will be dependent on whether or not the firewall is being configured with DHCP enabled or not. The firewall used for this paper was configured with the network-addressing mode of NAT with DHCP client. In this configuration, the firewall maintains the system to port mappings which change frequently for the workstations.[27] A diagram displaying how Dynamic Network Address Translation works from the text, Network Security: A Beginner's Guide is shown below[28]:

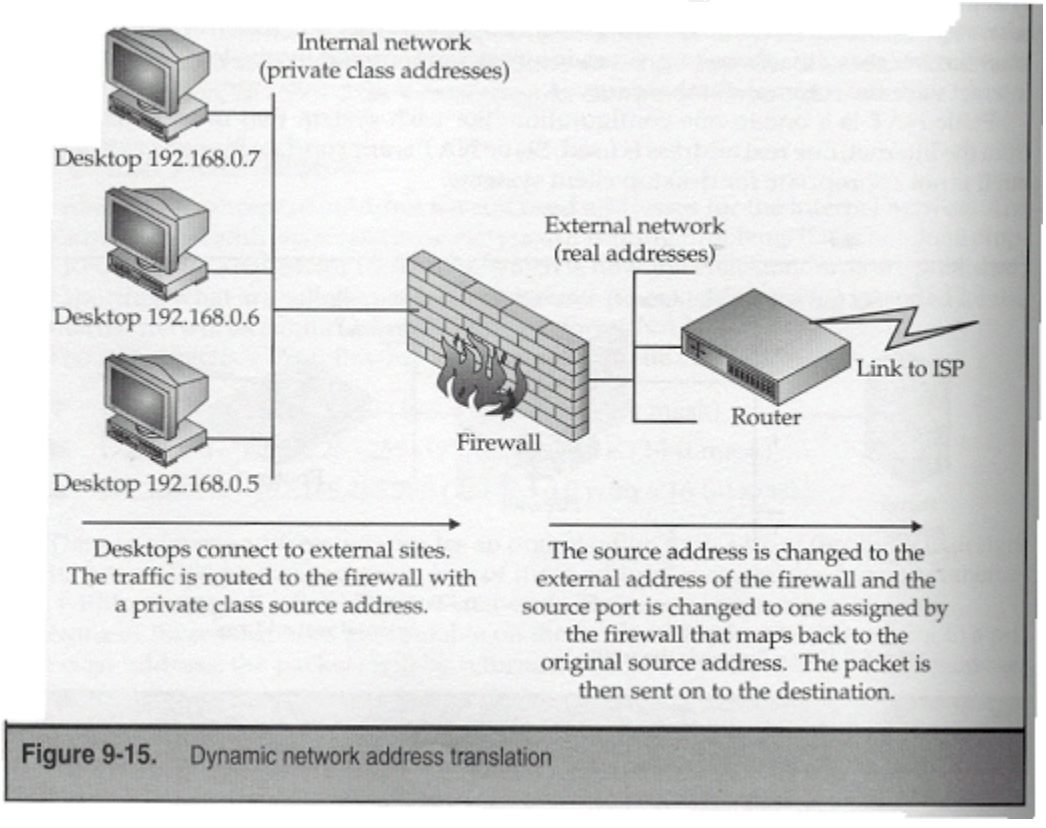
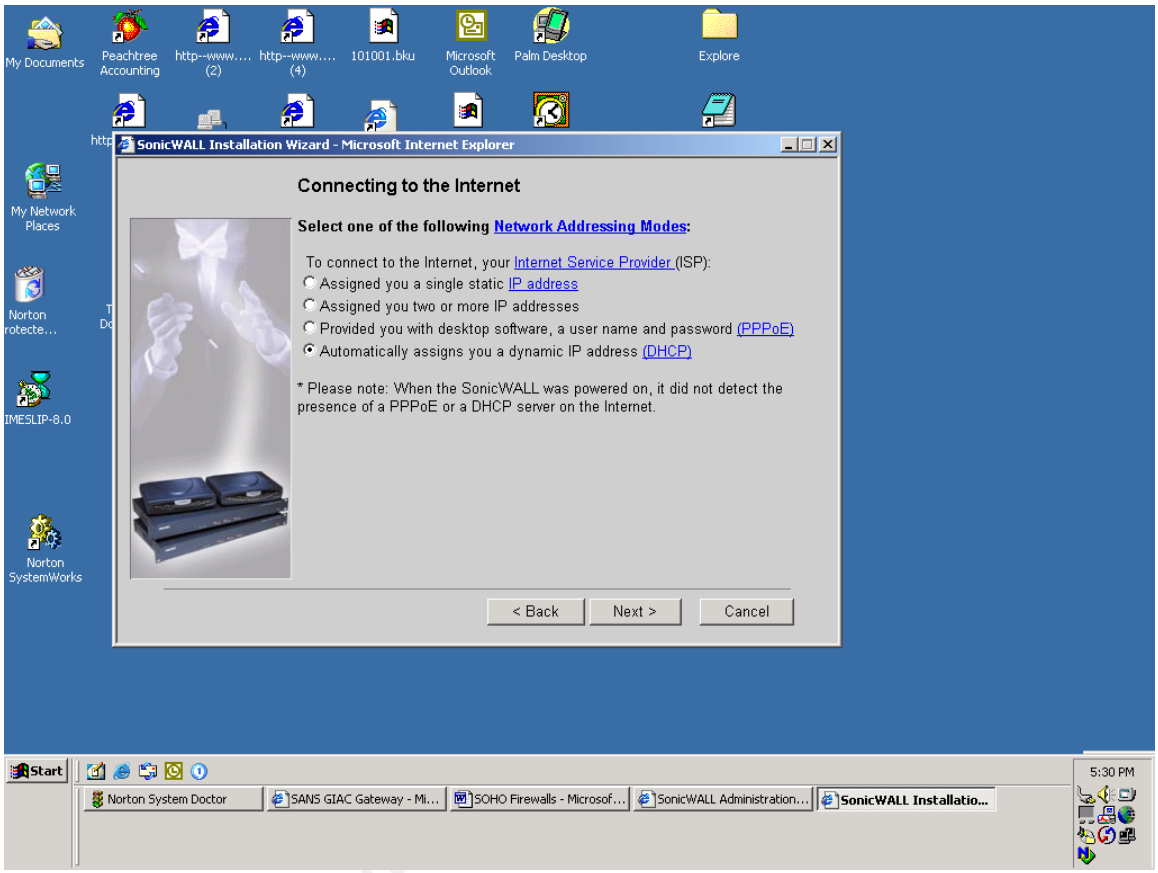


Figure 9-15. Dynamic network address translation

[27] Maiwald, Network Security: A Beginner's Guide, 162.
[28] Eric Maiwald, Network Security: A Beginner's Guide, 162.

The diagram bellows shows one of the installation screens for the SOHO3 during the software setup procedure for specifying the IP addressing mode for connecting to the Internet. As mentioned previously, the firewall was installed with NAT and the dynamic DHCP addressing mode.



Some Cautions about Firewalls

Although a firewall is a significant step towards securing one's network, there are however some issues one needs to be aware of. For example, a dial up modem installed on the network provides an access to the network without going through the firewall. The problems with modems are two-fold: the modem can be left in auto-answer mode and can be accessed by a hacker using war-dialing software. The second problem with modems is that they are an unrestricted connection to an ISP and can be detected on the Internet. [29] Needless to say, modems should be restricted if it can be realistically done because of these security issues. Other ways that users can circumvent firewalls are through wireless network connections or through an Internet file sharing protocol called Gnutella.[30] Additionally, malicious software, viruses or Trojans can be emailed to a user on the network, which again circumvents the security provided by the firewall. Anti-virus software with the proper updates can minimize these issues. Updates to a firewalls like virus updates need to be done on a regular basis. If the latest firmware has not been updated for a firewall, a potential breach of security is possible.

Conclusion

Firewalls needed for a small business differ significantly from those required by a large company. A firewall for a SOHO that is carefully selected to meet the business needs of a small company can be cost-effective and relatively easy to implement and maintain if one has some basic network knowledge. For enhanced security protection I recommend that software and hardware firewalls be installed together on the network.

Firewalls are just one part of an overall network security plan. A firewall coupled with other essential security practices (virus protection, strong passwords, hardened operating system, security policy, etc) is essential to providing appropriate security for a small business and can greatly reduce the security risks to a network. No business large or small can afford not to address this issue.

[29] SANS Security course, Security Essentials Day 3, "Vulnerability Scanning", 2-6.
[30] SANS Security course, Security Essentials Day 3, 1-21.

Works Cited.

Andress, Mandy. Surviving Security: How to Integrate People, Process and Technology. Indianapolis: Sams Publishing, 2002. 161, 181.

Brown, Bruce and Brown Marg. "SOHO Security: Small Network Security Concepts". Extreme Tech. 27 Feb. 2002.
URL: http://www.extremetech.com/article2/0,3973,14560,00.asp

Edwards, Mark Joseph, "Security Statistics Abound: What Do They Tell Us?" 24 July 2002
http://www.windowswebsolutions.com/Articles/Index.cfm?ArticleID=26037

Gibson, Steve. "Leak Test"
URL: http://grc.com/default.htm

Gibson, Steve "ShieldsUP!"
URL: http://grc.com/default.htm
.
ICSA Labs. "ICSA 3rd Annual Firewall Buyer's Guide"
URL:
http://www.icsalabs.com/html/communities/firewalls/buyers_guide/
FWguide99.pdf

ICSA Labs. "Required Services Security Policy - Small/Medium Business (SMB) Category module - version 4.0", Dec. 2002
URL:
http://www.icsalabs.com/html/communities/firewalls/certification/criteria/SMB.pdf

ICSA Labs, "Online Firewall Buyers Guide", Dec.5 2002,
URL:
http://www.icsalabs.com/html/communities/firewalls/buyers_guide/index.shtml

Karagiannis, Konstantinos and Sarrell, Matthew D. "Keep Hackers Out: Part One, Personal Edition", PC Magazine 19 Nov. 2002
URL: http://www.pcmag.com/article2/0,4149,651565,00.asp .

Maiwald, Eric. Network Security: A Beginner's Guide, Berkeley: McGraw Hill 2001. 162, 257.

Nextag Search Engine on SOHO Firewalls Nextag – Compare Prices Before You Buy Home Page
URL:
http://www.nextag.com/serv/main/buyer/OutPDir.jsp?node=&otherForm=n&doSearch=y&advanced=n&search=soho+firewall&searchnodeid=-1

Stark, Thom "Locking up Network Security" Var Business November 11, 2002, 58.

SANS Security Essentials Course, Security Essentials Day 3, Information Risk Management 1-21.

SANS Security Essentials Course, Day 3, Vulnerability Scanning, 2-6, 2-12-15.

SANS, "Sans/FBI Top 20 List"
URL: http://www.sans.org/top20/

Sonicwall, "Sonicwall SOHO3 Firewall"
URL: http://www.sonicwall.com/products/soho3.html

Sonicwall, Sonicwall Installation Guide for SOHO3 firewall appliance, 21, 26.