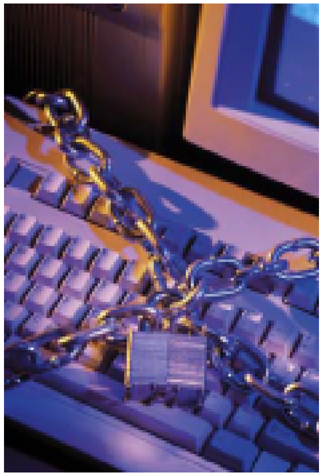
Cyber Security

Beginners Guide to Firewalls

A Non-Technical Guide

Essential for
Business Managers
Office Managers
Operations Managers



Multi-State Information
Sharing and Analysis Center
(MS-ISAC)

U.S. Department of Homeland
Security
National Cyber Security Division

This appendix is a supplement to the *Cyber Security: Getting Started Guide,* a non-technical reference essential for business managers, office managers, and operations managers. This appendix is one of many produced in conjunction with the *Guide* to help those in small business and agencies to further their knowledge and awareness regarding cyber security. For more information visit: *http://www.msisac.org*

Produced by:
Multi-State Information Sharing and Analysis Center and United States Computer Emergency Readiness Team

References

NYS Office of Cyber Security and Critical Infrastructure Coordination Best Practices and Assessment Tools for the Household Sector:
http://www.cscic.state.ny.us/lib/reports/

NYS Office of Cyber Security and Critical Infrastructure Coordination Cyber Security Awareness:
http://www.cscic.state.ny.us/lib/awareness/

CERT: Information for New and Home Users:
http://www.cert.org/homeusers/

Washington Post Protecting Your Home Computer or Laptop:
http://www.washingtonpost.com/wp-srv/technology/interactives/upgradesp05/security_2005.html

Microsoft Protecting Your Home Network:
http://www.microsoft.com/windowsxp/using/networking/learnmore/protecthomenet.mspx

Microsoft Wireless Network Security:
http://www.microsoft.com/athome/security/online/homewireless.mspx

The HoneyNet Project & HoneyNet Research Alliance Know Your Enemy – Trend Analysis:
http://www.honeynet.org/papers/trends/life-linux.pdf

Official site for Personal Firewall Day
http://personalfirewallday.org/

Acknowledgement

Special thank you to David Leach, NYS Cyber Security and Critical Infrastructure Coordination, for his contribution to this paper.
Portions of this article are taken directly from How Firewalls Work by Jeff Tyson and reprinted with permission. The full article may be found at www.HowStuffWorks.com.

Any product-specific resources mentioned in this paper are provided as a general reference only. We do not endorse or promote the advertising of any resources.

Photos By: © 2008 Jupiterimages Corporation

adaptor in your computer(s) has a 12-character MAC address. This number is usually found printed on the wireless adaptor or you can find it when you run the software that came with the adaptor. It may look like 000CFD4A68DD or 00-0C-FD-4A-68-DD. When configuring your firewall, enter the MAC address of each computer authorized to use the wireless connection. Generally, every computer on your network with a wireless access card is usually included in the authorization list.

- Enable the feature to encrypt information sent between your wireless computer and firewall. This may be referred to as either WPA or WEP. Whenever possible using WPA is preferred over the older type of encryption, WEP. When you enable this feature on your firewall, you will be prompted to enter a "key" which is similar to a password. This exact same "key" must be entered in the wireless adaptor software on all your wireless computers otherwise they will not be able to communicate with the wireless firewall.

Summary

So what can you do to protect your computer? Protecting your computer is about layers of security. A firewall is a critical layer. However, you must ensure that you do **all** of the following:

- Install and use a firewall. Set your firewall to automatically check for new updates.
- Install and use anti-virus software – a firewall is not a substitute for anti-virus software.
- Set your computer to automatically update to ensure you have the latest security patches applied to your computer.

These steps will help protect you from the threats that lurk on the Internet. It's important to remember that there is no such thing as a perfectly secure network, so it's best to be cautious.

Introduction

If you own a computer, you may have heard about FIREWALLS. A firewall is used to add a layer of protection between your computer or network and potential hackers. As you read through this document, you will learn more about firewalls, how they work, and what kinds of threats they can protect you from.

What Is a Firewall?

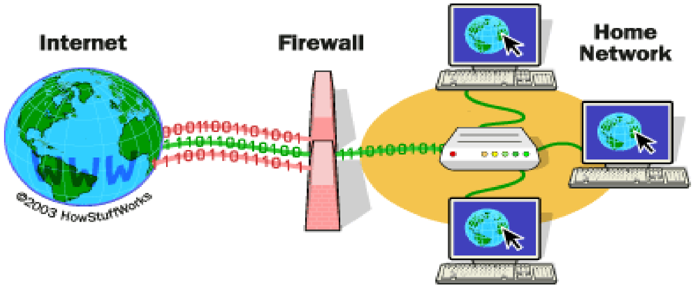
A firewall can be viewed as a traffic cop controlling the flow of cars at a highway intersection, ensuring that they obey the rules of the road.

A firewall is a hardware or software solution to enforce security policies. Or, another way to look at it is in a physical security analogy: a firewall is equivalent to a door lock on a perimeter door or on a door to a room inside of the building - it permits only authorized users such as those with a key or access card to enter. A firewall blocks unauthorized and potentially dangerous material from entering the system. If enabled, it will also log attempted intrusions.

When surfing the Internet or sending email, information is broken up and sent in small packets, similar to cars traveling on a highway. Just as a traffic cop controls the flow of vehicles, a firewall controls the flow of packets of information that travel between your computer or network (more than one computer connected together) and the Internet. When packets coming into (or going out of) your computer are not obeying the "safety rules," the firewall can block them to help protect your computer.

What It Does

A firewall is a software program or hardware device that filters the information coming from the Internet connection into your network or computer system. It can also filter information outgoing to the Internet. For example, if an incoming packet of information is flagged by the filters, it is not allowed through.



Just as we need to drive our cars defensively on the highway to prevent accidents and injury, so do we need to "surf" the Internet defensively from our computers to prevent someone from stealing our personal, financial, or other sensitive information. This information might be used to commit identity theft or our computers might be used to attack other computers or networks.

At this point, you may be thinking "why would anyone want to attack _my_ computer?" Here are just some of the reasons:

1. to steal your credit card and bank account numbers to purchase goods and services in your name;
2. to store illegal copies of software, music and movies for other Internet users to download;
3. to use your computer to launch an attack on other computers causing them to become infected or crash;
4. because they can!

In examples 2 and 3 above, a malicious person may also be covering their tracks by setting you up to look like the guilty party. Generally, attacks on computers are growing and are designed to compromise your computer without you ever knowing it. Users tend to be vulnerable today because they have powerful computers directly connected to the Internet.

Why Should I Use a Firewall? Think of writing a book with thousands of pages. What are the chances that the spelling, grammar and punctuation will be 100% correct?

- Enable the logging feature. Reviewing the logs regularly will help you discern if unusual activity is appearing on your network.

Unlike a software firewall, you won't get any immediate alerts from a hardware firewall. All the activity is stored in a log file on the firewall. You should periodically review this information for unusual activity such as:

- Successful inbound connections from the Internet to one of your computers. Generally this is suspicious unless you have specifically allowed someone to do this.
- If you see outbound activity from your computer at 2:00 a.m., for example, and you know no one was using it at that hour, it may indicate someone has broken Into your computer or your computer is infected with a virus. Be sure to check that this traffic is not related to automatic software updates before taking further action.

Installing and Using a Wireless Hardware Firewall

Wireless hardware firewalls follow the same steps as wired hardware firewalls, however, wireless radio signals are not confined to inside your office or building, or the immediate surrounding area outside. Please note, generally, wireless firewalls are not as robust as conventional hardware/software firewalls. More information about wireless hardware firewalls will be coming in the future appendices.

To prevent your neighbors from using your wireless Internet access or from viewing information you send between your wireless computer and your wireless hardware firewall, you should:

- Enable the feature called Media Access Control (MAC) address filtering that only allows your wireless computers to use your firewall. The wireless card or

Internet Explorer is attempting to access the Internet, select the OK option (it may be called "do not block" or "allow"). However, if the alert is for an application you don't recognize, type the name of the software into your Internet search engine, such as Google, Yahoo, etc., to see if you can learn more about this application. If your search indicates that the application may not be legitimate or if you just can't tell, play it safe and click on the BLOCK option (it may be called "do not allow" or "deny").

Installing and Using a Wired Hardware Firewall

Some hardware firewalls also use a "wizard" to walk you through their setup. Often they require different information than a software firewall, including information about your Internet connection. A word of caution, if your broadband provider manages your firewall/router, please contact them before making any of the changes suggested in this section. Here are some guidelines to follow:

- Check the support area of your firewall vendor's web site to ensure you have the latest updates for your firewall model. If not, follow the vendor's instructions to upgrade your firewall.
- Change the default administrator (or admin) password. These passwords are well known and could be used by a malicious person to take control of your firewall. Use a hard-to-guess password that includes letters, numbers and special characters.
- Make sure the option allowing remote management is disabled. Enabling remote management would allow someone coming from the Internet (sometimes referred to as the WAN interface) to configure the firewall.
- If you use applications that require a network, such as instant messaging, and/or file sharing, you may have to enable certain features in the firewall. Check your firewall settings to see if there are settings for that specific application that will not disable other security features in the firewall.

Computer software is like hundreds of authors writing a single, very complicated book and, unfortunately, errors (called bugs or vulnerabilities) are invariably introduced. Malicious people spend a lot of time trying to find and exploit these errors to attack your computer for fun, profit or to cause harm. A properly configured firewall can help block many of these attacks by preventing malicious computers on the Internet from connecting to your computer.

Even with a firewall, there are still ways your computer can be attacked or infected with a virus. For example, if you are not running up-to-date anti-virus software, a firewall will not stop a virus sent in an email message from infecting your computer.

What It Protects You From

There are many ways that unscrupulous people access or abuse unprotected computers:

- **Trojans** – programs that have a hidden malicious purpose. They may replace existing files with malicious code or add new malicious files to the computer. They may install other hacker tools or install backdoors on infected computers.
- **Backdoors** – often employed by Trojans, backdoors are programs that create hidden access capabilities which allow a hacker to remotely control your computer.
- **Key loggers** – software that tracks your key strokes (including user names, passwords, credit card information, etc.) and sends them to a third party without your knowledge and consent. Not all firewalls protect against this threat.

I Use Dial-up to Access the Internet. Do I Still Need a Firewall?

Yes. A computer running Microsoft Windows without a firewall and anti-virus software can be discovered and attacked and compromised in as little as a few minutes.

Regardless of your connection method (dial-up or broadband), it only takes a few minutes for a computer without a firewall to allow intruders access to your computer. A firewall will help protect your computer from successful attacks.

I Use an Apple MAC. Do I Still Need a Firewall?

Yes. MAC's are not immune to attacks and are just as susceptible to compromise as a Microsoft Windows system, therefore a firewall is necessary.

What Type of Firewall Should I Use?

Basically there are two types of firewalls: software and hardware firewalls.

A **software firewall** (also called a personal firewall) runs directly on your computer. This firewall is the most common type for users. Software firewalls typically require very little technical knowledge and therefore are relatively easy to get up and running. Many firewalls have default configurations for the user. To get started, either purchase a firewall or download a free one from a trusted site.

For most users, the default installation settings are sufficient.

A **hardware firewall** is usually an external device such as a firewall/router. This is typically used with an "always on" Internet connection such as those available from your cable TV or telephone company (also called broadband Internet connections). A hardware firewall is an appliance that sits between your computer and the cable or DSL modem installed by the cable TV or telephone company respectively.

Hardware firewalls typically require more technical knowledge to configure and maintain than software firewalls. They usually come set up by default to block all attempts from the Internet to connect to your computers but often allow any software on your computer(s) to connect to the Internet.

Installing and Using a Personal (Software) Firewall

The level of security you establish on your firewall will determine how many threats can be stopped by your firewall. The highest level of security would be to simply block all incoming and outgoing communications. Obviously, that defeats the purpose of having an Internet connection. You can restrict traffic so that only certain types of information, such as e-mail, can get through the firewall. A good rule for businesses that have an experienced network administrator who understands the business needs is to begin by blocking all traffic and then begin to select which types of traffic you will allow. For most of us, it is probably better to work with the defaults provided by the firewall vendor unless there is a specific reason to change them.

Software firewalls typically use a "wizard" to ask you some basic questions to set up your firewall. Whenever in doubt, take the "default" or "recommended" answer. Here are some guidelines to follow:

- If you are prompted to set up a network, answer "NO" unless you have multiple computers which are connected together and used to share printers, files or other resources.
- If the firewall includes an automatic update feature, turn it on or enable it.
- Periodically check the support area of your firewall vendor's web site to ensure you have the latest soft ware updates for your firewall model. If not, follow the vendor's instructions to upgrade your firewall.
- Enable the logging feature. Reviewing the logs regularly will help discern if unusual activity is going on your network

Once installed, the firewall will usually alert you the first time an application attempts to access the Internet. For example, if you just clicked on Internet Explorer and the alert says