

Firewalls 101 - A Primer

Why you need one?

So, you have purchased the computer and taken it out of the box. You've set up your 'workstation' to be comfortable and now you are ready to connect the telephone line or your cable modem to start cruising on the information superhighway.



Not so fast! What have you done to protect yourself from hackers and others that would like to use your computer without your knowing? I'm not talking about other members of your family, or employees. I'm talking about users from the other end of the cable that brings the Internet into your home or office.

You have most likely gotten an anti-virus program with your computer, many computers come with them pre-installed. But this is not enough! What you need is a piece of software called a firewall.

"What is a firewall", you ask?

A firewall is hardware component or a software package you load onto your computer that allows you to control access from outside network resources, in other words, other computers that are connected to the Internet. This discussion primarily deals with software based firewalls, however the concepts are exactly the same for hardware based firewalls as well.



It doesn't matter what kind of connection you use to connect to the Internet, dial-up modem, ISDN, DSL, 2-way satellite or Cable modem users should all use a firewall. There are many people that will tell you that dial-up users do not need a firewall. **DON'T YOU BELIEVE IT!** Your data is just as vulnerable on a dial-up connection as it is using any other type of connection to the Internet.

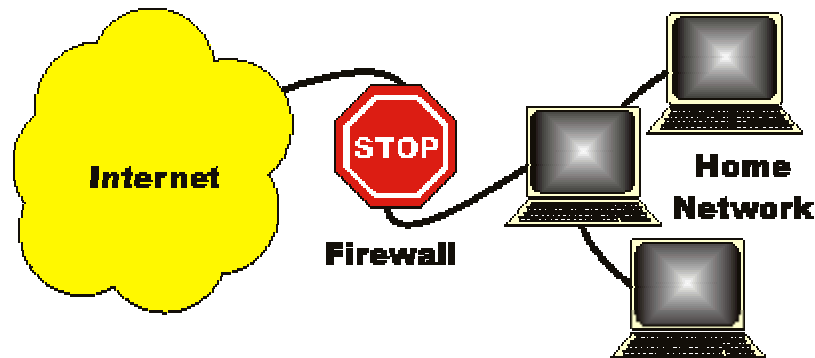
There are many different firewall programs available. Some are free and others require the purchase of a license to use the firewall software. The companies that distribute free firewall programs have specialized licensing agreements, which prohibits the use of the free version for business use. Businesses are expected to pay the required license fees in order to utilize the software.

The reason these companies allow personal users to license the program for free is so they can influence the user on a personal level, thereby increasing the chances that someone using the product will introduce it into a business environment.

Protecting Yourself

The biggest reason to protect your computer from outside intrusion is that you could have personal information on there, which could be very valuable in the hands of the wrong people.

Online banking and shopping information, personal medical profiles, professional correspondence and many other types of data can assist Internet criminals in emptying your bank accounts, destroying your credit rating and, in some rare cases, even lead to stalking and murder.



Using a firewall allows you to control who accesses your computer from the outside as well as giving you the 'last word' in allowing other software you run to access the Internet.

There are many shareware and freeware programs that, while very useful, collect data and attempt to 'phone home' in order to feed massive marketing databases used to target customers. These 'malware' programs send your personal data out of your computer without your knowledge or consent. Using a firewall helps you control the unauthorized use of your personal data.

There are several very good firewall products available to you for download from the Internet or for purchase at your local retailer.

I usually recommend one or a combination of the following products:

BlackICE Defender from Network ICE at <http://www.networkice.com>

Tiny Personal Firewall from Tiny Software at <http://www.tinysoftware.com>

WinRoute Pro from Tiny Software at <http://www.tinysoftware.com>

ZoneAlarm from Zone Labs, at <http://www.zonelabs.com>



There are many other products on the market aside from those mentioned above, however, it is my opinion that these products are the absolute “best of breed”. If you are using another product your mileage may vary. I have found ease of use is just as important as the protection these packages provide. If the product is not easy to use, you will not be motivated to continue using it for very long.

Depending upon the type of protection needed for your situation, all are very good products and they each have pros and cons.

If you would like to find out more about these products, visit their respective web sites and read about what they do prior to making your decision. In some cases, I recommend the use of more than one of the above mentioned products.

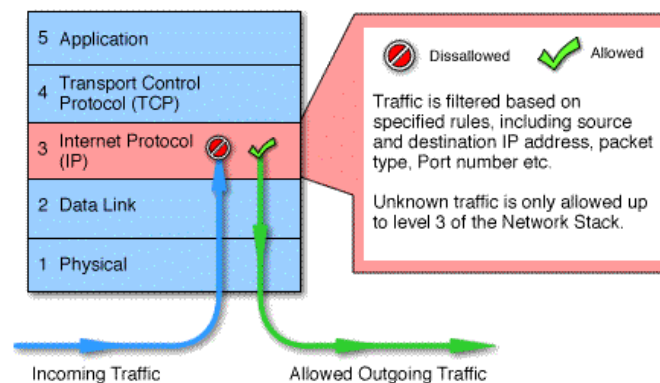
Depending upon which firewall product you use, it will also protect you from certain email viruses and trojans as well as malicious traffic.

Firewall Types – Under the hood.

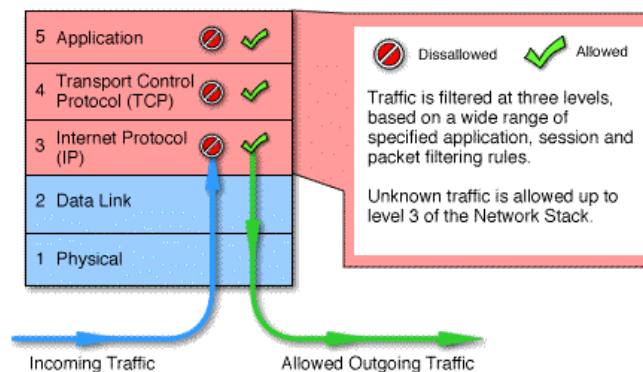
There are static, *rule-based*, firewalls and firewalls that do what is called “*Stateful Packet Inspection*”. The traffic that enters and leaves your computer is comprised of packets of data. The easiest way to describe the difference is to provide an example to which we can all relate.

Let’s use the airport as the basis for our example. The packet or “traffic” is you, the passenger. As a passenger one of the “rules” that would allow you to get on the airplane is that you have a ticket for the particular flight you want to be on.

A static, rule-based, firewall is basically just that. It works based upon the premise that a particular rule is in the firewall database. In our airport example you are allowed to travel because you have a ticket for that flight.



A firewall that does stateful packet inspection, would in our example, be like the airport security scanner that you walk through on your way to the gate. You have your ticket, which means you are in compliance with the “rule” however, you are also “scanned” to make sure that you do not have any weapons or other items that would constitute a danger or security risk. If you do not have anything that the scanners see as a threat then you are allowed to pass through. If the scanner detects something that would be perceived as a risk you would be stopped and investigated further.



Firewall Installed – What next?

Let's assume that you have purchased and / or downloaded the firewall of your choice and have successfully installed it, what next?



A “*trojan*” is a piece of software that is designed to provide some useful functionality to the user but, has hidden functionality that is usually used to intercept data or even allow someone complete control of your machine. It gets its name from the Trojans of ancient Greece who masqueraded as a “gift” inside a giant wooden horse so they could attack Troy. Many times the trojans come in the disguise of a little game or other cutesy program.

Do not be fooled by this tactic.

You may have heard of the **Sub-Seven**, **Netbus**, **Back Orifice** or **BioNet** trojans which allow outside users to take over your computer, delete files, modify Windows settings, steal information, log keystrokes for obtaining passwords and all kinds of nefarious activity. **They can even eavesdrop on the conversations in your home or office using the sound card if you have a microphone connected to your computer!** This is an especially useful exploit if you happen to be a laptop user, as in most cases you may not be aware that your laptop has a built in microphone.

A hacker that infects a computer with one of the trojans mentioned above, can completely take over your computer, deleting or adding files, creating ‘underground’ ftp servers to distribute pirated software, child pornography and all kinds of other things that you would rather not have happen on your computer.

Safe Computing – Now a necessity

The various firewall programs are designed to detect traffic that is used by hackers to communicate with the various trojans that are out 'in the wild' and block that traffic. The best way for you to protect yourself against becoming the victim of a trojan is to practice "**safe computing**".

Safe computing is easy to do and simply requires that we use a bit of common sense.

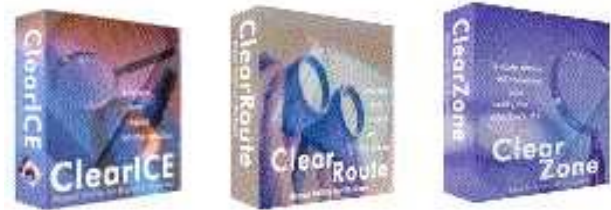
1. Do not open **ANY** email attachments from people that you do not know!
2. If you **DO** receive any email attachments from someone you know, make sure they understand what safe computing is before opening the attachment. If you are in any doubt about the message, do **NOT** open it.
3. Make sure you have a good anti-virus program and be sure to keep the virus definitions updated at least once a week. We recommend:
eTrust EZAnti-Virus from Computer Associates at <http://my-etrust.com> or
PC-Cillin from Trend Micro at <http://www.antivirus.com>
4. Make sure your anti-virus program does **real-time monitoring of memory and floppy disks** as well. Many viruses and trojans are passed from computer to computer by floppy disks that travel from work to home or vice versa.

Firewall Reporting Tools – Empowering the user.

The purpose of the firewall (and anti-virus software) is to protect your computer and in the course of providing that protection, it can capture and log a **lot** of data about the traffic that is coming to and from your computer.

Unfortunately, one of the weaknesses of the many firewall products on the market is a lack of ability in producing meaningful reports or allowing access to the data in a manner that makes it easy to understand. This is why we created our firewall log analysis tools.

ClearICE for BlackICE Defender, **ClearRoute** for WinRoute Pro and **ClearZone** for ZoneAlarm, available from www.firewallreporting.com, allow you to easily obtain information from the firewall log data. Using this knowledge you can determine the level of threat that you have been exposed to in order for you to take action to strengthen your security or report the intrusion attempts to the proper authority, the intruder's ISP.



Depending upon the type or severity of the intrusion attempts, you can have the intruder removed from their Internet account. This would effectively keep them from attacking your computer.

You can also print hard copy reports of the intrusion attempts and graph the data to look for any trends that might indicate a weakness in your computer security efforts.

Using the proper firewall and log reporting tools you can protect yourself and provide valuable information to the authorities that can keep computing safe for everyone.

Firewalls – The primary defense.

In light of the recent events of terrorism against the United States, protecting your computer should be a priority for everyone using the Internet. All it takes is a couple of hundred of infected computers working in concert to wreak havoc with the Internet and computing systems all over the country.

Product Summary:

- ClearICE Report Utility for BlackICE Defender
- ClearRoute Report Utility for WinRoute Pro
- ClearZone Report Utility for ZoneAlarm

More information can be found at the following URL:
<http://www.firewallreporting.com>

Biography:

Ben E. Brady has been programming and developing custom database applications for small businesses for more than 25 years, specializing in the reporting of data to make it easier to understand for end-users.

He can be reached via email at y2kbrady@yahoo.com