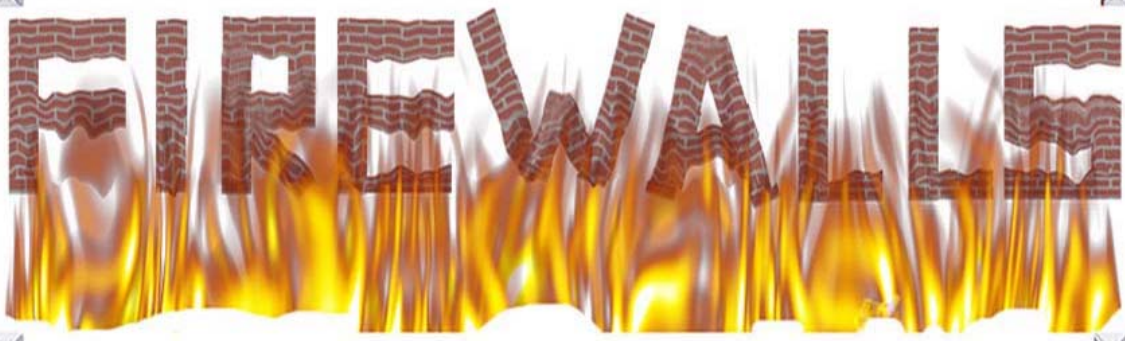
By Liquid Rockface



FIREWALLS

Introduction:

A firewall is either a program or piece of hardware designed to prevent hackers from gaining access to your computer and to prevent unauthorized programs from accessing the Internet. A good example of such a program is a trojan horse. A trojan horse is a program which may look legitimate, but contains code that allows a hacker to operate your computer remotely.

The word firewall has its origins in construction of buildings and vehicles. Many buildings have firewalls to prevent a fire from spreading too far and causing damage. Cars also have a firewall to prevent engine fires from spreading into the cockpit.

If you ask many people why they do not have a firewall, their response is, "The internet is a vast place; what are the chances of somebody finding me and hacking me?" The answer is simple: Hackers use port scanners to search vast numbers of computers for security vulnerabilities. They can scan thousands of computers in a single day, and people without firewalls appear as easy pickings. Many hackers also use port scanning to check if you have an active trojan (i.e. an open port that belongs to a trojan horse) on your computer, and if you do, they as well can also control you!

Hackers may have a number of reasons for wanting to gain access to your computer:

1. To steal information – This information could be classified information in a government computer, credit card numbers, bank accounts, school reports and so on.

2. To use your computer to hack other people's computers – A classic reason that a hacker may want to do this is to launch a DDOS (Distributed Denial Of Service) attack. A DDOS attack is where the hacker infects a large number of computers (called "zombies") with a program. This program allows him to attack a website or server with a huge amount of information (generated by the zombies) causing it to crash.

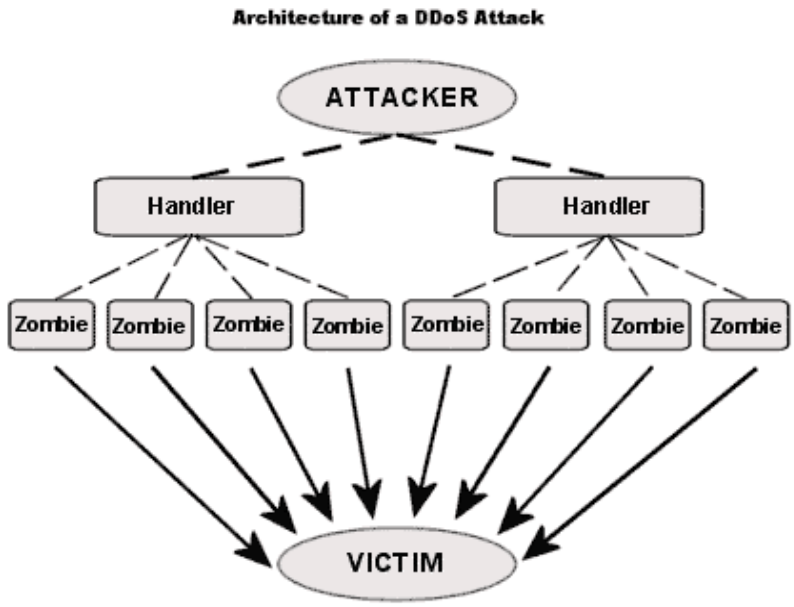


Figure 1 - Architecture of a DDOS attack - http://www.cs3-inc.com/pk_whatisddos.html

3. He might just be trying to mask his identity to avoid conviction for his crimes.

4. To annoy you. Some people hack just for the sake of ruining your information for the fun of it. They are not concerned as to whom their victim is, as long as they get to cause them the maximum inconvenience.

The next decision is whether to get a hardware or software firewall. Hardware firewalls are less susceptible to exploits than software firewalls, for the simple reason that you can't "corrupt" the hardware in the same way that you can just corrupt a piece of software. Hardware firewalls, however, are a lot more expensive than the software variety, and can be more difficult to set up. Hardware files often contain their own Operating System inside them.

On the other hand, software firewalls are more customisable, which may or may not be a good thing. Personally, I like to personalize my firewall as I can block specific programs, ports and addresses. Obviously, the more expensive your hardware firewall is, the more options there will be.

Ports

It is impossible to fully understand firewalls, without some knowledge of ports. Computers can be thought of as houses, with ports being the doors. It is not illegal to use a port scanner, as it is akin to going down your road trying all the doors of the houses to check if any of them are unlocked. It is suspicious, and often the first sign of an impending attack, but it is not entirely illegal. It is, however, illegal to use an exploit to gain access to a port, the same way as it is illegal to bash down your neighbour's door.

Ports on a computer are either open, closed or stealth:

Open is when anybody can send information to or from that port, effectively like an open door in a house. A port could be open because a hacker is running a service on that port, or it could just be open for a legitimate reason.

Closed is when nobody can send information to or from the port, but they know that the port (and therefore your computer) exists, and they can use an exploit or brute force to crash your computer and gain access. Closed is the most secure you can get without a firewall.

Stealth is when no information can be sent to or from the port, and nobody can even detect that the port exists. If you use a firewall, your whole computer can be "stealthed", thus making it impossible for a hacker to determine if your computer even exists!

Just because a port is closed or stealthed, does not mean that no information whatsoever can be sent or received, just that there has to be a program on your computer to allow the passage of data. In the case of internet, Internet Explorer (or whatever web browser you use) will allow incoming Port 80 (HTTP) connections to your computer, but will still not open your port for the world to see.

Again, you can compare it to standing at your front door, and only allowing authorized people access to and from your house. The door is open, but only to those people that you trust.

Packets and IP Numbers

Before I explain the Internet protocols, let me briefly explain IP numbers and packets.

A packet is a unit of data that is transferred from one computer to another.

An IP number is a unique identifying number used by computers to set up a connection. For instance, www.yahoo.com is really 64.58.76.179, but it would be very difficult to remember all the IP addresses of all the websites you go to, therefore a system called DNS was devised, that translates the website address (URL) into the IP address, to initialise the connection.

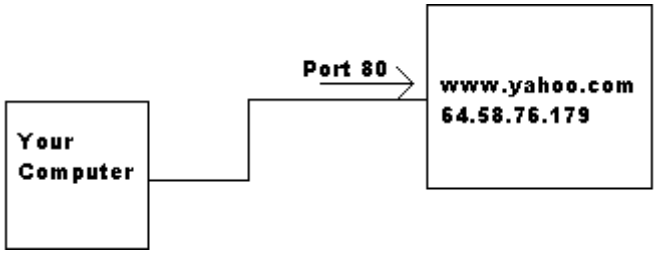


Figure 2 – Basic diagram showing how a computer connects to a website

If you look really carefully at the status bar in your web browser when you connect to a website, you may see the IP number of the website appear for a moment.

Internet Protocols

It is quite essential to learn a little about protocols, before you can set up your firewall properly. There is probably enough information to write an entire project on Internet Protocols, but I will keep it very brief and simple.

There are three basic protocols: TCP, UDP and ICMP:

TCP protocol is used for the transfer of data. The connection from Internet Explorer to the Internet, for example, is an outbound TCP connection on Port 80 (HTTP). The data from the websites is sent along this TCP connection. TCP is by far the most commonly transmitted and received protocol. It makes up for the vast majority of data transferred in a connection. TCP is very reliable, and has error-checking to ensure integrity of data. It requires the two computers to connect to transmit and receive data.

UDP protocol does not need a connection, and does not transmit any real data. It is used to send brief messages where it is not entirely important if data gets lost. For instance when you connect to a website, your computer sends out a UDP packet to determine the IP address of the website. After that is established, the TCP packets may be transmitted from the website to

your computer. As it says at
http://java.sun.com/docs/books/tutorial/networking/overview/networking.html,
"Sending datagrams is much like sending a letter through the postal service: The order of delivery is not important and is not guaranteed, and each message is independent of any other."

ICMP protocol is used to report on errors in communication between the two computers. It will inform the computer that a packet has got lost, or maybe that the destination computer is unreachable. ICMP is also used for ping and traceroute functions, that can be used to determine the IP address of websites, check if a computer or website exists and see how long it takes for data to reach the destination computer and where that data goes to reach it.

Setting up a Firewall

The way a firewall processes connections is through a set of rules. This allows a port to be closed or stealthed, but still allow access to legitimate programs. You can have full access over which ports are available for connections, and to which programs. This is very important as it prevents hackers from being able to control your machine via a trojan horse. This is called "Packet Filtering".

A trojan horse pretends to be legitimate, and opens ports for communication between the server (your computer) and the client (the hacker's computer). If you wish to take up the house analogy again, you could say it's the same as a burglar sneaking into your house, and then opening your door for all his evil friends to come and take what they want.

Most firewalls give you the option to be alerted when a connection is made, and to make a rule based on that alert. This is one of the easiest ways to set up rules, but you need to apply a little of your knowledge of ports and protocols to set everything up securely. Many people don't realize that an incorrectly set up firewall is worse than no firewall at all, in some cases.

Just to give a brief example, a friend of mine once was boasting about his new Zone Alarm Pro firewall and how he was now "un-hackable". I scanned his computer, and found that he had set up his rules so badly, that virtually all of his most vital ports were wide open for anybody to hack him! It goes without saying that it is imperative to test your firewall after you have set up your rules, to ensure that you are indeed secure. I recommend either getting a friend with a port scanner to scan you (although this may take ages), or you can go to www.grc.com/default.htm to have an online security scan that takes 10 seconds.

First thing to do when you get a firewall alert is to determine if the program that is trying to access the Internet is legitimate. If you see that it is Internet Explorer, Outlook Express, or any chat programs and the like that you are trying to access the internet with, then you can be assured that it is legitimate. If it is some odd program that you have never heard of, and you are not doing anything when the alert pops up, then it may be a trojan horse.

In the case that it is a program that you do not want to access the internet, for whatever reasons, you can tell the firewall to block the program access to all ports (sometimes called services), all protocols and all addresses, incoming and outbound. That will effectively shut it out from the Internet.

If it is a program that you have opened, like your e-mail client, and you want it to access the Internet, then you have to make a rule to allow certain connections. I recommend that the first time that you get alerts for a legitimate program, tell the firewall to allow the connection that time **only**. Then you can go to your firewall logs, and check what connections were made.

If there are more than one or two connections on a single port, then just allow access to that port on only that protocol and direction for all addresses. If there are many, many ports, with many, many different addresses, it might just be best to allow the program all access to the Internet, and just block whatever specific connections you don't want, for example adverts. If there are few connections, like with Outlook Express or Internet Explorer, you may wish to only allow those specific connections.

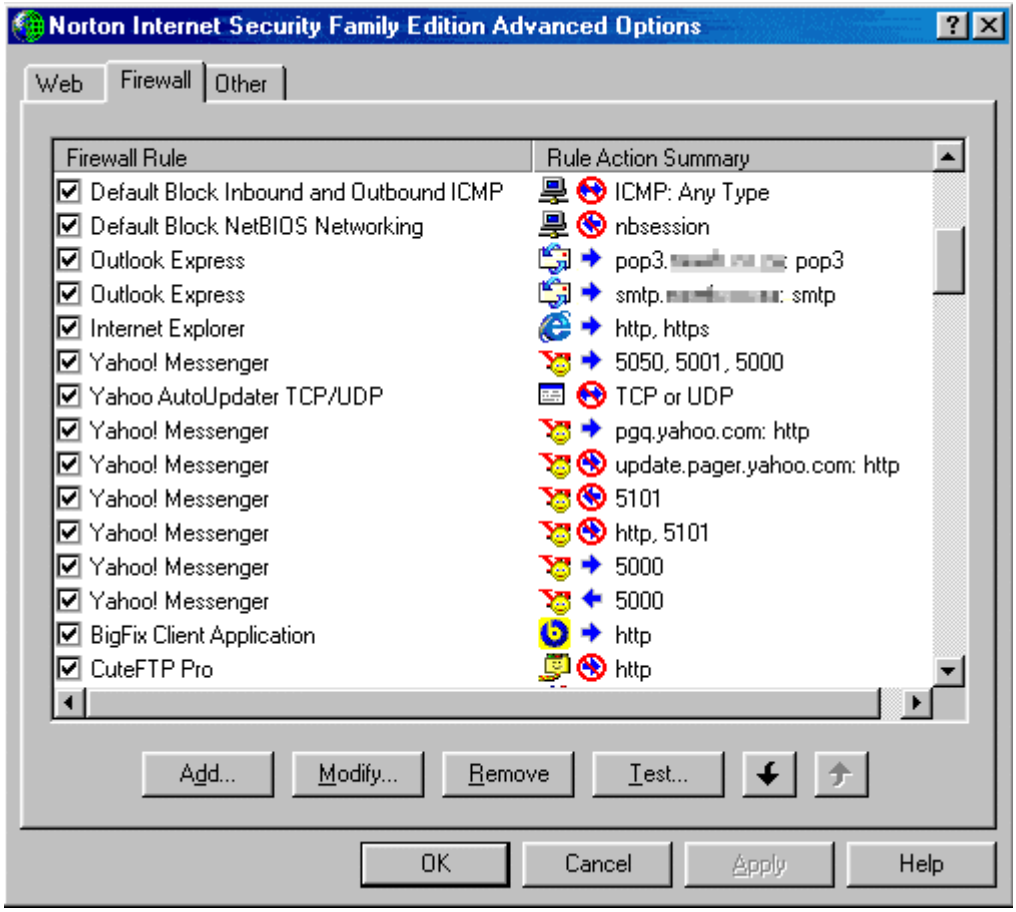


Figure 3 - A screenshot of some of my firewall rules

Also, if you are making an outbound connection, that is a connection from your computer to another computer, then you will be concerned with which port you are connecting to on **their** computer. If the connection is an inbound connection, the port that concerns you is the port on **your** computer, to which they are connecting.

Here are a couple of examples that I will commentate on. They illustrate a number of things to be considered when setting up rules:

Internet Explorer

The connection to the Internet with Internet Explorer, as I mentioned earlier, is an outbound TCP connection to Port 80 (on the remote computer). When you surf the Internet, you visit many websites. Therefore, you don't want to make the rule specific to any address.

The rule will look something like this:

Permit: Yes
Protocol: TCP
Port: 80
Direction: Outbound
Address: Any
Application: Internet Explorer (You will write the full file name and path here)

This is saying that it will permit this connection, as long as it's only TCP protocol, the connection is from your computer outwards, and the application is Internet Explorer. It is irrelevant what address it is going to. You don't want to be alerted for every single website you visit! It is best only to allow the ports that you require access, because otherwise it may be possible to be exploited through the other ports. Set it to only allow Internet Explorer access, because you don't want every single application on your computer to be able to use that connection, because then trojans can use it.

Outlook Express

The connection to receive your E-mail with Outlook Express is an outbound TCP connection to Port 110 (POP3). You only connect to one POP3, which is the one at your ISP (unless you have more than one ISP, of course). This means you will only need to allow the connection for one address. Sending your mail is also an outbound TCP connection, this time to Port 25 (SMTP). Again, only one address is required.

The rule will be:

Permit: Yes
Protocol: TCP
Port: 110, 25
Direction: Outbound
Address: pop3.yourisp.com, smtp.yourisp.com
Application: Outlook Express

This rule will allow you to receive and send your e-mail. However, you won't be able to connect to any other ISP's e-mail account. I like this so that if anything changes my e-mail settings, I won't find myself downloading or sending mail to any other account except my own. A hacker, for example, could use your computer to download somebody else's e-mail, and you could even be implicated for stealing somebody's e-mail account!

Download Accelerator Plus

Now with this program I'll demonstrate what you do when there are many different addresses, and many different ports it connects to, but you want to block advertisements. Adverts are **always** either in two places: On your hard drive, or on the Internet. If it's on your hard drive you can delete it, and if it's on the Internet you can block it with your firewall. Download Accelerator Plus uses a mixture of both methods. It connects to the Internet, and then downloads new adverts to your hard drive. It then runs these adverts.

The rule will look like this:

Permit:	Yes
Protocol:	TCP
Port:	All
Direction:	Outbound
Address:	Any **except** ads.downloadaccelerator.com
Application:	Download Accelerator Plus

Because Download Accelerator uses many different ports and addresses, I allowed everything through, but I didn't want the adverts. When I first opened the program, I allowed each connection through "that time only". That way I could refer to the log to see what connections were made. It was obvious to see that ads.downloadaccelerator.com was not a vital connection, so I blocked it, and voila! No more adverts for me!

Testing Your Firewall

Once your firewall is up and running, it is vital to check that you have not left open any holes. I always test my firewall after I suspect I may have caught a virus or after I have added new firewall rules. I routinely run checks every couple of months as well.
There are a couple of ways that you can test your firewall. You can get a hacker friend to try and hack you, you can get a friend to scan your ports with a port scanner like NTO Scanner or AutoNOC Port Scanner, you can use a network scanner like LAN Network Scanner or you can visit one of numerous websites that will run security tests for you online.
My favourite websites for testing my firewall are www.grc.com/default.htm, and www.pcflank.com. GRC has a very quick and basic port scan (called NanoProbe) that tests some 13-odd popular ports. It also has the famous ShieldsUp!, which tests your computer privacy and networking security. You can also download the Leak Test, which will determine whether a trojan would be able to "phone home".

PC Flank has a number of port scanners, a trojan scan, an Internet privacy scan, and, very importantly, an exploits test that barrages your computer with a large number of popular exploits. My computer passed all these tests with flying colours!

I think that McAfee (www.mcafee.com) also have some security testing features, but I don't think they have anything that is not already covered by GRC and PC Flank.

Comparison Between Various Software Firewalls:

In this chapter I will discuss the various pros and cons of a number of software firewalls. Note that this is just a few of the many software firewalls available.

Norton Personal Firewall 2003

I use Norton Internet Security 2001 (which includes the Personal Firewall) and I must say I am extremely happy. The new Norton Firewall includes Privacy Control, that protects your confidential information, a Security Monitor, which shows you that your firewall is working, an Alert Assistant, which lets you set up your new rules, Visual Tracking to reveal where attacks came from on a world map, Ad Blocking to stop pop-ups and other windows, and a One Button Disconnect (they obviously got that idea from Zone Alarm) that instantly stops or starts Internet traffic. The firewall also includes LiveUpdate (with a year's free subscription), to get all the latest security fixes for the program, and a feature that notifies you when your computer connects to another network.

If there are any pitfalls in this program, I would say that they lie in the fact that it automatically determines for you what programs it thinks should be allowed access to the Internet. While this may save time, it can leave gaping security holes by allowing trojans to access the Internet. I would say that, overall, this is a superb program with loads of extra features over and above the firewall part.

Norton Personal Firewall 2003 costs about R500.

Zone Alarm

Zone Alarm is well known as one of the best free firewalls around. There is a Zone Alarm Plus and Zone Alarm Pro edition.

Zone Alarm Pro includes cookie blocking, advert blocking, e-mail protection, a pop-up advert stopper, a hacker tracker, and, most interesting of all, a spyware remover. Without going into much detail in spyware, it is basically unsolicited software (like Bonzi Buddy) that lurks in your computer and spies on your activities, sending information about you back to the advertisers. Zone Alarm Pro costs about R500.

Zone Alarm Plus is similar to Pro, except that it does not have as many privacy features. It has e-mail virus protection, hacker tracking and program validation, so that trojans can't masquerade as legitimate files. This is one of Zone Alarm's best selling points, but I'm not sure if the other firewalls have this feature. Zone Alarm Plus costs about R400.

Zone Alarm (normal edition) is the free version. It has e-mail virus protection, network managing and AlertAdvisor to help you deal with security alerts. You cannot set individual rules, however, and this is where the program falls down. However, considering it's free, it's a lot better than having no firewall at all.

Tiny Personal Firewall

I could not find very much information on Tiny Personal Firewall at their website, but from what I can see it is very basic. Their main selling point is what they call "Sandbox Protection". They claim that they are the only firewall with such a feature, but to be honest, I think they're only trying to find a way to push their product. They are very vague about what it really is, but it seems to just be their way of saying that they filter connections and applications' access to the Internet. That is no great feature! It does, however, include protection against malicious code: very much a plus in today's world of website viruses. Tiny Personal Firewall costs about R400. I would not really recommend this firewall, as it does not contain many features that Zone Alarm Plus (same price) contains, for example.

Black Ice Defender

Black Ice Defender protects your privacy with password and credit card number theft protectors. It also supports securing a wireless network, which is useful. Their website hardly listed any features, and I couldn't help feeling that there aren't very many features in this program. Considering that Black Ice Defender costs about R400 I can't help feeling that it is extremely limited and simple. It might be good for the beginner, but then I'd rather recommend the free Zone Alarm.

McAfee Firewall 4

McAfee Firewall 4 has a very useful hacker tracing facility that let's you see where the hackers come from, on a world map. It also has a facility to check that your firewall is secure, a wizard for creating firewall rules, a program for checking what programs on your computer can connect to the Internet and colour coded firewall alerts, to make it easier to sort out what each alert is, and how severe it is. McAfee Firewall 4 costs about R400, and definitely seems to be one of the more thorough and definitive firewall programs.

My Conclusion (to the firewall comparison)

If you are looking for a totally free firewall that will get the job done without any frills, then I would recommend Zone Alarm's free version. If you are a little more serious about your security, and you should be, I'd recommend either McAfee Firewall 4, or Norton Personal Firewall 2003. I have to admit that from past experience, however, I tend to think that the Norton option may be better, as I have found that McAfee sometimes advertises features in its programs that are either non-existent, or totally useless. They do, however, create programs with excellent, easy-to-use interfaces. I would steer clear of Black Ice Defender and Tiny Personal Firewall, as they do not provide comprehensive coverage of all the security aspects.

Table of Comparison Between Firewalls

Features:	NPF 2003*	ZA*	ZA Plus*	ZA Pro*	TPF*	BID*	McAfee Firewall 4
Hacker Tracing	Yes	No	Yes	Yes	No	No	Yes
Privacy Protection	Yes	No	Partial	Yes	No	Yes	No
Firewall Rule Creation	Yes	No	No	Yes	Yes	Partial	Yes
Malicious Code Protection	Yes	No	No	Yes	Yes	No	No
E-Mail Protection	Yes	No	Yes	Yes	No	No	No
Advert/Pop-up Blocking	Yes	No	No	Yes	No	No	No
Price	R500	Free	R400	R500	R400	R400	R400

*NPF 2003 = Norton Personal Firewall 2003
ZA = Zone Alarm
ZA Plus = Zone Alarm Plus
ZA Pro = Zone Alarm Pro
TPF = Tiny Personal Firewall
BID = Black Ice Defender

Overall Conclusion

In this day and age, it is essential for anybody connected to the Internet to have a firewall. I stay connected to the Internet the entire weekend and during this time my firewall log often reports that I have been scanned by many computers. Sometimes I have people blatantly trying to gain access.

Which firewall you get is up to you. If you are a large corporation, you may want to invest in a heavy-duty (and highly expensive) hardware firewall. If you are a home user, you can choose from one of the many software firewalls available on the market.

It is important to remember that you are **never** immune to hacking. Do not start taunting or provoking hackers, thinking that you are safe and cosy behind your firewall; you never know who they are!

It is also important to make sure that you cover all your bases as far as general security goes: A firewall is useless if you have a weak password to your administrator account, and somebody in your company cracks it from the inside. A firewall only protects you from external threats. You can test the strength of your password at this website: http://www.securitystats.com/tools/password.asp.

It is also vital to download the latest security patches. Many exploits can be manipulated to bypass your firewall and gain access to your computer. Microsoft products are notoriously vulnerable, so ensure that you visit www.microsoft.com/technet/security to download all the latest security fixes. You can also get a 3rd-party program like I have called Bigfix (www.bigfix.com) to find and download all the patches for you.

In conclusion, I strongly recommend to anybody — even just a home user — to invest in a firewall. If you only use your computer to send the odd e-mail, and you spend less than 15 minutes online, then it is probably unnecessary. If you stay on for around an hour at a time, it is quite necessary, but not essential. If you stay on for a number of hours at a time or if you have a leased line (i.e. broadband: ADSL, Cable etc), then it is critical that you have a secure firewall.

Bibliography

http://www.cs3-inc.com/pk_whatisddos.html
http://www.genealogy.com/67_gary.html?Welcome=1035653931
http://grc.com/x/ne.dll?rh1ck2l2
http://www.cisco.com/univercd/cc/td/ doc/cisintwk/ito_doc/ip.pdf
Norton Internet Security 2002 Help Guide
http://java.sun.com/docs/books/tutorial/networking/overview/networking.html
http://www.ee.siue.edu/~rwalden/networking/icmp.html
http://www.tampa-bay.net/BitsAndBytes/Archives/FirewallBasics.htm
http://www.networkmagazineindia.com/200107/focus2.htm
South African Computer Magazine – October 2001 Vol. 9 No. 9
http://www.securitystats.com/tools/portsearch.asp
http://www.symantec.com/sabu/nis/npf/features.html
http://www.zonelabs.com

www.tinysoftware.com
http://www.mcafee.com/myapps/fw4/default.asp
http://blackice.iss.net/product_pc_protection.php

✔ ✔ ✔ ✔