

Firewalls

Firewalls are simply a way of securing your businesses network just as you would secure your home, writes Mark Rogers from More Solutions.

The analogy

I live in a modest house in a normal street. My home has a front door, secured with a Yale lock, and back doors and several windows, all of which can also be locked. It also has a fenced garden with a locked gate. While at home I can see more or less unimpeded through my windows, although passers-by cannot easily see in through the net curtains. My girlfriend and a few family members have keys to the house, and know the code to my alarm. Other than that I have few visitors, including the postal worker who leaves me a never-ending stream of bills and junk mail, and the newspaper deliverer who drops a free local paper through my door once a week. I also have a gardener who visits once a week, and my windows are cleaned every month or so.

I am reasonably happy about this level of security, although I am well aware that there are shortcomings and should anyone have a deep desire to get into my house they will do so.

If I were a computer then I could achieve most of this in virtual terms with a *firewall*.

What is a firewall?

You probably do not care about the security of my house, but if your office network is connected to the Internet you certainly *do* worry that you do not really know who can get in or what they could do if they did. You have probably heard of firewalls, but you do not have time to take a technology degree to work out whether you need one, so let us look again at the analogy.

Your office is your house and garden, and your firewall is what controls the boundary between this and the rest of the world. Striking a balance between security and convenience has many similarities between the two, but worryingly many organizations provide access to their network in ways that would seem cavalier in home security.

Some basics

In theory, at least, my house is secure to anyone who does not have a key. In practice, complete security could not even be guaranteed in a house with no windows or doors (the equivalent of an office network not connected to the Internet). However, while I know that every door or window makes intrusion much simpler I live in a real world where the benefits in having access to the outside world from my house outweigh the risks, provided that I take reasonable steps to manage those risks.

My front door Yale lock is good at stopping people getting in, and at the same time allows anyone inside to get out without a key. This is similar to many basic network configurations, where access to everything on the Internet is allowed to those on the network, with nobody on the Internet allowed access to the office. This may or may not actually be desirable; if I had small children I would be keen to ensure they could not just leave the house when they felt like it, and similarly there may be certain people who you wish to prevent accessing certain services on the Internet (maybe a blanket ban for some people, or Web browsing but no downloading of movies and games by others). This is a decision based more on personnel management than security, though, and we will return to this later.

In firewall terms, it is common to allow access to the outside world for specific purposes. This is done by applying criteria which must be met in order for access to be allowed, and at a basic level relates to IP addresses and TCP ports. Using a different analogy for a moment, IP addresses are like telephone numbers and TCP ports are like extension numbers; to ring me you need to know both my telephone number and my extension, as without the former you cannot make the call and without the latter our receptionist will not put you through. IP addresses are simply the addressing system used on the Internet, and allowing access to specific addresses is a bit like giving access to certain people.

Returning to the original analogy, appropriately enough the comparison here is between my postal mail and business e-mail. The standard TCP port for incoming e-mail is port 25, and 'opening port 25' on the firewall is the equivalent of having a letterbox on my front door. Unfortunately, it does nothing at this level to ensure that what comes through the port is genuine and wanted e-mail, and this is why firewalls are almost useless at preventing e-mail-borne viruses unless they prevent e-mail altogether. Some firewalls are 'stateful' – that is they do more than just open the letterbox but also check that what comes in them is mail (preventing newspapers or less savoury items passing through), but even then this does nothing to ensure that the mail you receive is mail you want.

Outward bound

Even basic firewalls are able to decide what to do based on the direction data is flowing, and more importantly, which side of the firewall initiated the connection. For example, browsing the Web is clearly bi-directional; your browser 'uploads' the address of the page you want to view, and the graphics and text of the Web page are then 'downloaded' back to the browser for display. Since the connection was initiated by your browser, inside your protected network, it is often safe to assume that data coming in through a connection initiated within the network can be allowed in, unchecked.

On the other hand, if an external device tries to access your computer without a request from you, then the firewall can inhibit the attempted access as being unwanted (most office networks do not usually need to allow any incoming connections at all). This results in a very simple configuration where all un-initiated incoming access is inhibited. However, in practice, this is over-simplistic for all but the smallest networks.

The data transfer capacity ('bandwidth') of the connection between your network and the Internet is finite, and some users can consume disproportionate amounts of this capacity. For example, 'peer-to-peer' (or P2P) protocols allow users to share files with others elsewhere on the Internet with little control or accountability. As well as consuming resources these protocols also allow – even encourage – sharing of copyrighted materials such as film and music files. A firewall, blocking outbound access to the ports used by these protocols, can be an invaluable (if not foolproof) weapon to prevent such abuse. Additionally, many e-mail-borne viruses contain software that, when triggered, makes outgoing connections to pass on passwords or allow external control of the infected PC, so leaving most outbound ports closed brings a degree of protection.

In summary, by acting at the boundary between your network and the Internet a basic firewall can restrict access to certain types of internally initiated connection (such as e-mail and the Web).

What a firewall looks like

Conceptually all firewalls can be seen as a black box with two network ports. One is connected to your local network, the other to the Internet, and their sole job is to monitor and limit the data flowing from one to the other.

There are many firewall vendors such as Cisco, Watchguard and Nokia, each with a range of hardware options to suit a range of medium to large budgets, although comparing the options is beyond the scope of this article.

Also worth considering are the increasing number of PC-based firewalls, often based around the free Linux operating system. All worthwhile firewalls of this type require a dedicated PC (that is they do not run alongside other applications on the same hardware) since any additional software is a potential weak point. These packages (for instance, IPCop and Smoothwall) are ideal for lower budgets since they typically cost little if anything above the cost of a basic PC and provide more than adequate protection for many enterprises.

Some enterprises have areas of their network that need to provide services to the outside world, and therefore need different firewall rules from the network core. Recalling our analogy, this is akin to my garden – an area where security is reduced to allow access to the gardener and window cleaner, but with additional security maintained between the garden and the house. In firewall terminology this is often called a ‘demilitarized zone’ (DMZ), and it is achieved by having two firewalls, one between the outside world and the DMZ, and another with tighter controls between the DMZ and the core. Some firewall hardware combines these two (or more firewalls) in one box with separate network ports for separate zones.

The weakest link

]Securing a network almost always makes life a little more difficult because it restricts the things you can do or the ease with which you can do them. We accept this with home security of course; many a time I have returned home in the rain and wished I did not have to stand out in the cold, fumbling for my keys, but however frustrating it is I would not just leave the house unlocked instead.

If firewalls have weak spots it is usually because humans, who create holes to make life easier without proper regard for their consequences, manage them. They are often a temporary measure ‘just to get this working’, and temporary fixes frequently become permanent. For example, it is possible to set up secure ‘tunnels’ into and between networks (for instance, to allow network access to home workers or travelling salespeople). These Virtual Private Networks (VPNs) are efficient and secure methods of allowing external access in a controlled fashion, but they can be complicated to set up compared with just opening a few ports for remote access using remote control software, so the simpler (and less secure) approach gets chosen, offering a relatively easy approach for hackers.

Therefore, an essential part of any security configuration is a routine audit of holes in your firewall. It is a minor task to run a basic scan across the ports of your firewall (from outside your network) to see if any are open, and this should be done regularly (and weaknesses corrected), as it will almost certainly be scanned (and weaknesses exploited) by someone else if you do not. Companies such as ESoft provide subscription services (www.securityspace.com) that can run these scans automatically.

Summary

Conceptually, a firewall is a very simple product that does a very simple job. In practice, the job it does is difficult to achieve, and as attacks get more sophisticated so too must the firewalls; however this is a job for the people who build firewalls, not for those who deploy them.

It is the nature of the job that firewalls do, that results in them being surrounded by jargon and acronyms. If they seemed complicated as a result, hopefully they seem less daunting now.

Now, where did I put my keys?

Mark Rogers is a senior developer at More Solutions Ltd, a company dedicated to designing and deploying software solutions for industry that use the Internet as a communications medium. With many applications involving stand-alone, unattended equipment installed miles from the nearest IT department, security and reliability are essential aspects of their business.

For further information contact More Solutions Ltd, 6 Belgic Square, Fengate, Peterborough, PE1 5XF, Tel: 0845 45 89 555, E-mail: mark@more-solutions.co.uk, Web: www.more-solutions.co.uk

This article was published in **The Secure Online Business Handbook, 2nd and 3rd editions** and is published by Kogan Page.