

What
you
should
know
about

Firewalls



Before you decide on installing a firewall, there are a few things that you should consider...

LANZen

secure information solutions

So what is firewall?

What features should I look out for when buying a firewall?

A firewall is a barrier between your computer system and the outside world. It controls what is allowed through the barrier by a number of specific policies known as *rules*.

Firewalls can be a piece of software running on your workstations or notebooks, or a hardware “appliance” placed on your network, between your systems and the external network, like the Internet.

A firewall is at its most effective when it prevents everything that is a threat to you and when it does so without hindering your normal day to day operations.

Considering that any form of protection can be beaten, it really isn't good enough to install a bit of software and expect any threat to be put off by it's being there. It just won't work.

Any proper attack will sense the presence of a software firewall and simply use any of the many methods and techniques to circumvent it.

So the first feature to look for is a device that stands apart from the network it is protecting. This makes it very difficult for a hacker to decide what's being protected when it's effectively hidden behind it.

The highest performance firewalls are “appliance” firewalls. The very best of these are designed around a special hardware chip called an “ASIC”, this chip is specifically programmed to perform as a full-time firewall and nothing else.

Don't buy any software-based firewall that runs on a PC or server - even those that cost thousands of pounds. They are now easy to crack by hackers and those who are intent on gaining access to your system for their own benefit, or on behalf of others.

The second feature to look for is the “smart” firewall. This is one that not only stops traffic aimed at specific areas of weaknesses of your system - the open doors known as “ports”, but is actually capable of looking inside the traffic - the packets - to see if they are potentially dangerous.

This is known as “stateful inspection” and is an indication of a powerful firewall. Beware though - some software firewalls offer stateful inspection, too. It still doesn't make them a good idea!

The final feature to look for is the ease of set-up and use after the engineer has installed it. It's no good having a firewall that you don't understand, can't update and can't manage. It will lose its strength.

What's wrong with a software firewall?

Answer this question honestly - do you *really* trust *any* Microsoft software or even the majority of UNIX systems to be *truly* secure?

Most people would quite rightly say “no”. OK, now ask yourself “*why am I contemplating installing a software firewall on an operating system I know to be insecure?*”

A software based firewall runs on a PC - be it a server or some form of “hardened” stripped down operation system designed to originally offer server-type services to users.

Realistically, a software firewall is a firewall 75% of the time and a server the remaining 25% of the time. It's the tasks or services within this 25% that will be exploited by a hacker - not the firewall!

As software firewalls run on PCs or servers, hackers know exactly how to attack their underlying network interfaces so it really doesn't matter how expensive or how effective the software is running on them, they will simply crash through the network to reach your systems now helplessly exposed beyond.

Also, the simple existence of these software firewalls sends a clear signal to hackers that there is something worth attacking beyond.

If you're paying a premium price for a software firewall, do you really want to have something that can be at best only 75% effective?

Hardware firewalls - specifically ASIC-based firewalls - do not possess any PC characteristics. They are just a network device that looks at packets of information - the network traffic and apply rules to it.

They are 100% engaged for 100% of the time as firewalls. They are never servers, or PC's or any derivative thereof. This means the tools used by hackers will be virtually ineffective - but never 100% safe all of the time - this is never possible to achieve. But hardware offers a far higher margin of safety than software.

ASIC hardware appliance firewalls don't give any indication whatsoever of what is beyond. In fact, there is no clue that there is anything there at all. This is the one fundamental feature that makes them so superior. How can you hack what you can't see?

No business should ever consider installing or continuing to run any software based firewall for whatever reason or cost!

What makes a hardware appliance firewall so effective?

Are hardware firewalls more expensive than software firewalls?

How do I choose which firewall to buy and how much should I spend?

The ironic part is - hardware firewalls are no more expensive than a comparable software firewall and usually, considerably cheaper.

This is because for many years the network security industry has ripped-off it's customers by trading on the complexity of the products offered and the fear of attack on its customer's systems.

This resulted in absolutely ridiculous and scandalous prices being charged by these unscrupulous suppliers, making the dealers and security "experts" very rich while their customer suffered from the ever increasingly effectiveness of hacking attacks.

Hardware ASIC firewalls are comparatively new and have emerged as a result of the radically falling costs of the "chips" used within them.

There is a world of difference between knowing that you need a thing and knowing which thing to buy!

The choice of firewall is based on a number of specific criteria. *The least of which should be cost.* Here is a list of things to consider:

- The size of the network beyond
- The sensitivity of the data being protected
- The implications to the business of an attack exposing the systems beyond - regardless of if any information is exposed or not
- The amount of traffic expected
- The planned growth of the network
- Finally, the purchase and running costs.

The golden rule is - if you feel you can't afford a firewall, pull out the network cable. You should not be accessing the Internet. It's as simple as that!

It's essential to engage the services of a security consultant (like LANZen!) to help you decide what to buy. They will know about the latest attack profiles and where the latest gains have been made in firewall design and which offer the best features.

"For many years the network security industry has ripped-off its customers by trading on complexity"

How do I install a firewall onto my network?

The first thing to consider when installing it is - do you understand what you are doing?

Unless you're a security expert and one trained on that specific firewall the answer to that is probably "no".

Always get an expert security engineer to install a firewall. *There are no exceptions to this rule whatsoever.* If you don't, you may as well simply save your money - or rather, give it to the hacker directly, because he'll get into your system very quickly.

Having said that, let's talk about how the engineer will install your firewall. To be any real use, any protection should be placed before the object being protected. Simple? Yes, but this doesn't stop people buying software firewalls and installing them on the same PC they want to protect. This is the worst thing you can do!

Your firewall-protected network is divided into three distinct and unique areas or zones. These are the inside - where your main systems live, the outside, where the hackers live and an area that you want to present to the outside - like your mail and web servers - called the DMZ (dee-emm-zee - or demilitarized zone).

The inside and outside zones are effectively isolated from each other, the DMZ allows traffic into it from both inside and outside, but nothing across it, effectively, a no-man's land, which is where it gets it's name from.

The rules you apply to these zones determine how strong the firewall will be - this is why it is so important to have these professionally set up by an engineer familiar with your firewall.

“Always get an expert security engineer to install a firewall. There are no exceptions to this rule whatsoever.”

How can I test my firewall to if it's working?

There are a number of sites on the Internet that offer testing "probes" or friendly attacks on firewalls to test their effectiveness. This is known as "ethical hacking" and forms an essential part of any firewall installation.

Regular updates should be applied as new threats emerge - this means having your firewall under a maintenance contract that covers such updates. Checks should be made regularly to see if these updates are installed and that your firewall is effective.

Again - use the services of an expert engineer - don't try to save money by scrimping on this expense!

To be able to know which options suit your business, you should contact a network consultant - like us - as we deal with the problems faced by businesses every day and can offer good un-biased advice.

See the LANZen web site for details of our computer and network design and consultancy service.

<http://www.lanzen.co.uk> or mail us on info@lanzen.co.uk