


No Firewall? Then you don't understand the problem!



Trustix™
COMODO



IBM Advanced Development Partner

Comodo Trustix Limited 
New Court, Regents Place, Regents Road,
Manchester, Salford, M5 4HB,
United Kingdom
Tel Sales: +44 (0) 161 874 7080
Fax Sales: +44 (0) 161 877 1767
sales@trustix.com

www.trustix.com

Please do come in, the key is under the mat!

Connecting a web server and more importantly any part of your internal network to the Internet without the use of a Firewall as protection is rather like leaving your home with all the windows and doors unlocked whilst placing additional neon signs in the road saying *'please, take what you want'*. If it really is that serious, why do some companies still choose not to protect their assets? (Your customer lists, Intellectual Property and daily activities are as much an asset to your business as the physical hardware in the office itself.) Several years ago it was true to say that a lack of awareness could be a possible reason, but in today's increasingly interconnected world a lack of awareness is certainly not the main reason.

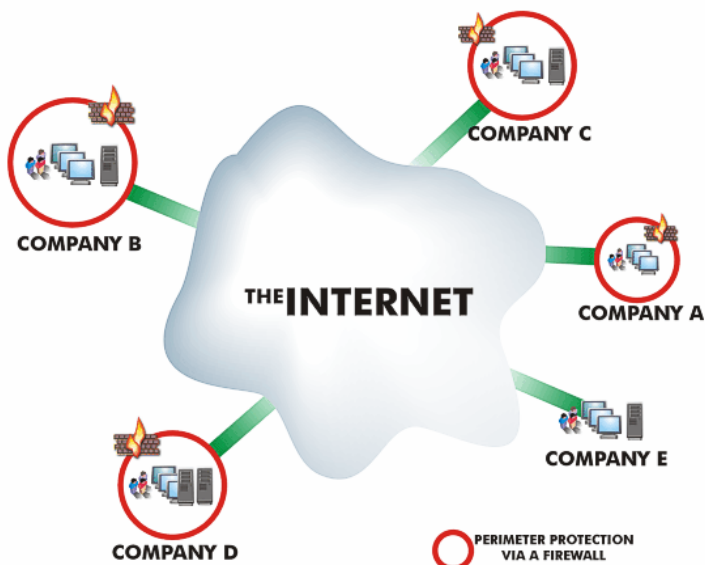
The DTI (Department of Trade and Industry) 2002 Survey on Security Information Breaches reported that only 66% of UK web sites (88% of larger businesses) had any sort of Firewall security in place protecting company web sites. Several reasons compound the problem of adoption. Firstly there is an assortment of vendors in the Firewall space who offer an array of competing products each offering a multitude of alternative features and unique solutions to bamboozle even the most hardened IT professional. Price and availability of a scaleable solution combined with the difficulties of integration and deployment within the company architecture also create uncertainty and doubt. Secondly there is a misconception that the ISP (Internet Service Provider) itself will have necessary security solutions in place and finally some companies do not adequately conceptualize their architecture, meaning that they do not see the benefit of a firewall, maybe having several routes to the Internet from individual dial up accounts etc.

What exactly is a Firewall?

The term "fire wall" originally meant, and still means, a fireproof wall intended to prevent the spread of fire from one room or area of a building to another. The Internet is a volatile and unsafe environment when viewed from a computer-security perspective, therefore "firewall" is an excellent metaphor for network security.

The most important aspect of a firewall is that it is at the entry point of the networked system it protects. In the case of Packet Filtering, it is at the lowest level, or "layer" in the hierarchy (stack) of network processes, called the Network Layer or the Internet Layer. This means essentially that the firewall is the first program or process that receives and handles incoming network traffic, and it is the last to handle outgoing traffic. Firewalls are usually described as providing perimeter protection.

If you had to choose which company NOT to do business with then **COMPANY E** represents the biggest risk as they have no form of protection, so any business information shared/transferred to them would be at risk.



IBM®, eServer and xSeries® are trademarks of International Business Machines Corporation in the United States, other countries, or both. Other trademarks are the property of their respective owners.

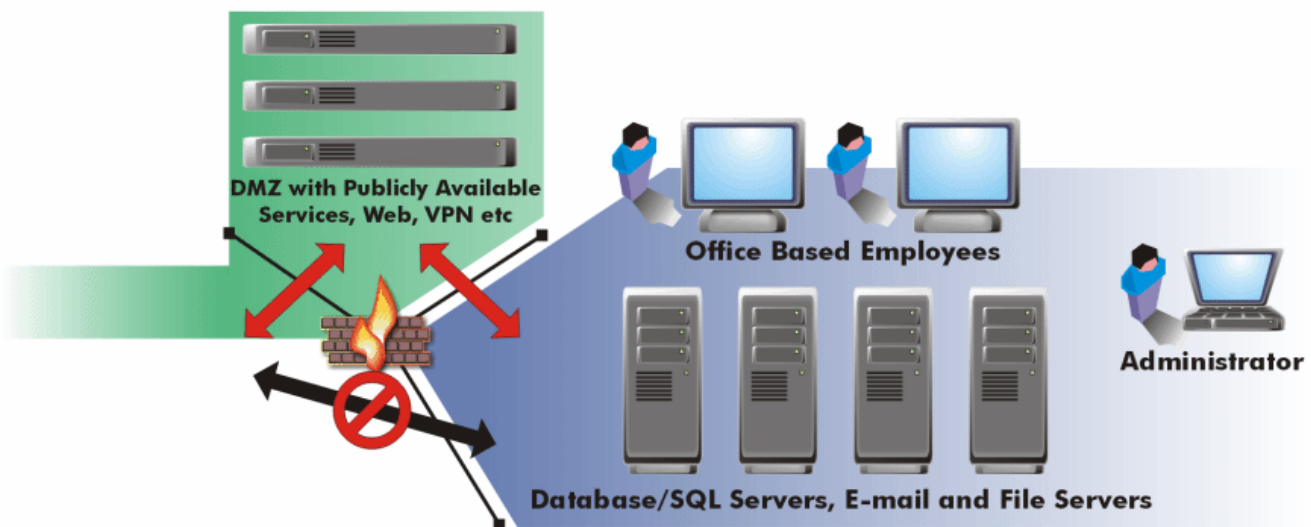
What parts make up a firewall and how do these protect your organisation?

As we have seen, a Firewall is used to protect the point of interconnection between various networks. Although most commonly identified as protecting your network from the Internet, interposing security gateways between the outside world and the organization's inner networks or between distinct sub networks of the same organization meets a fundamental network security need.

Quite simply a firewall is an inspection point allowing filtering and control of network transactions. All traffic* passing through the Firewall point – web accesses, electronic mail, application transactions – is precisely identified, checked, and allowed through or rejected, eventually encrypted, depending on the rules and regulations set out in the security policy.

In order to offer a protection mechanism a Demilitarized zone can be used. Filtering solutions can be used for both Intranet and Internet protection. The Demilitarized Zone (DMZ) is a concept that was introduced as a solution to secure the interconnection of the internal network with the Internet. The aim of a DMZ is to create a safe space between the outside world (usually the Internet) and company IT systems (usually the Intranet). This space is called the DMZ, as it separates two militarized zones: the Intranet and the Internet. The DMZ is therefore the perfect place to authenticate, audit, accredit, encrypt and translate private IP addresses into public IP addresses (NAT otherwise known as Network Address Translation).

The Demilitarized Zone is now a well-known concept for most IT system management and staff and individual DMZs can vary from none to unlimited, although the requirements of the Server (PCI slots etc) do themselves limit the actual number as each zone needs it's own network card. The diagram below shows how a DMZ is set-up to allow Internet Access to the DMZ. Publicly addressable web servers are located here whilst the Internal servers are protected and not directly accessible from the Internet.



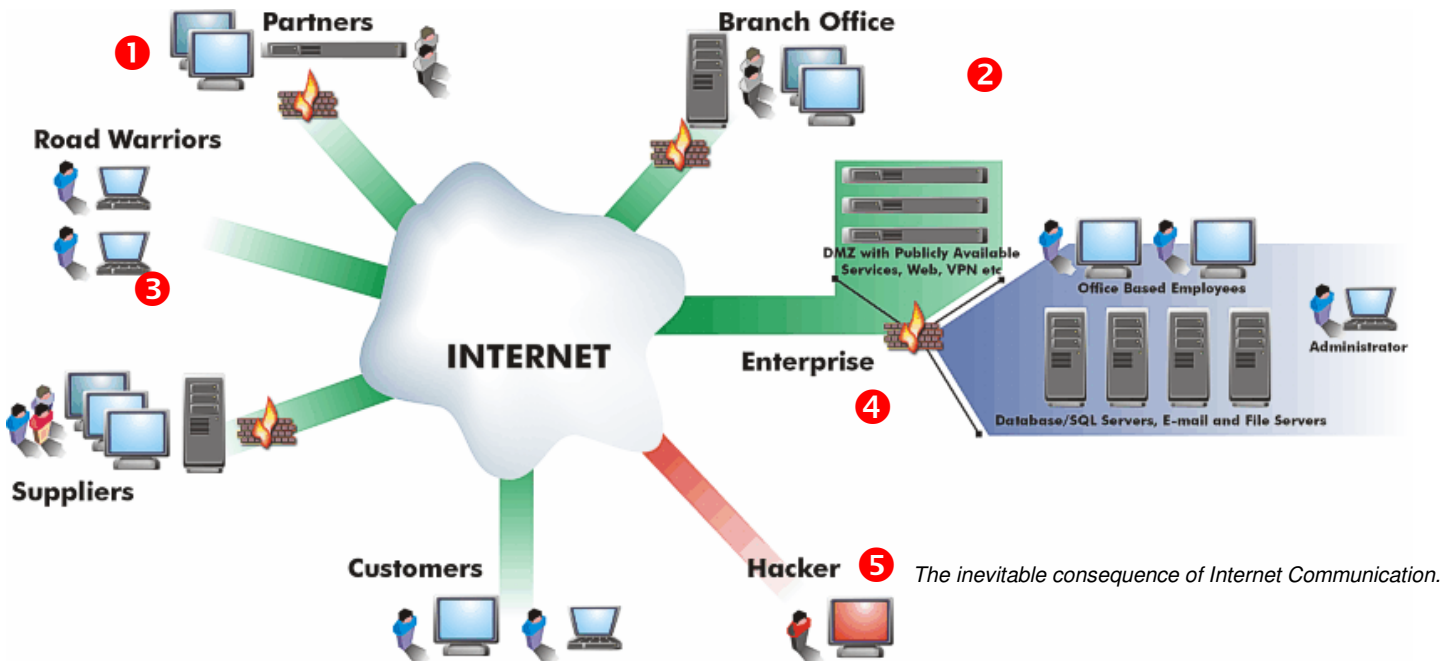
What are the risks from not having a Firewall?

The most obvious risk of not protecting your assets is to lose them; however not having sufficient firewalls in place to protect all parts of your organisation is almost as bad as not having a firewall for the head office. Trojans can be introduced into the network and after all your security is only as good as the weakest point! Ensure you protect all parts of your distributed

* Please note. In-depth technical discussion on packet filtering etc is not the subject of this white paper. More information is available on www.Trustix.com

What would a Firewall enabled Enterprise look like?

In the example below we take a 'typical' SME (Small to Medium Enterprise) and describe how each area benefits from the use of a firewall. (Most notably the Hacker at position 5 would see the least benefit from this!)

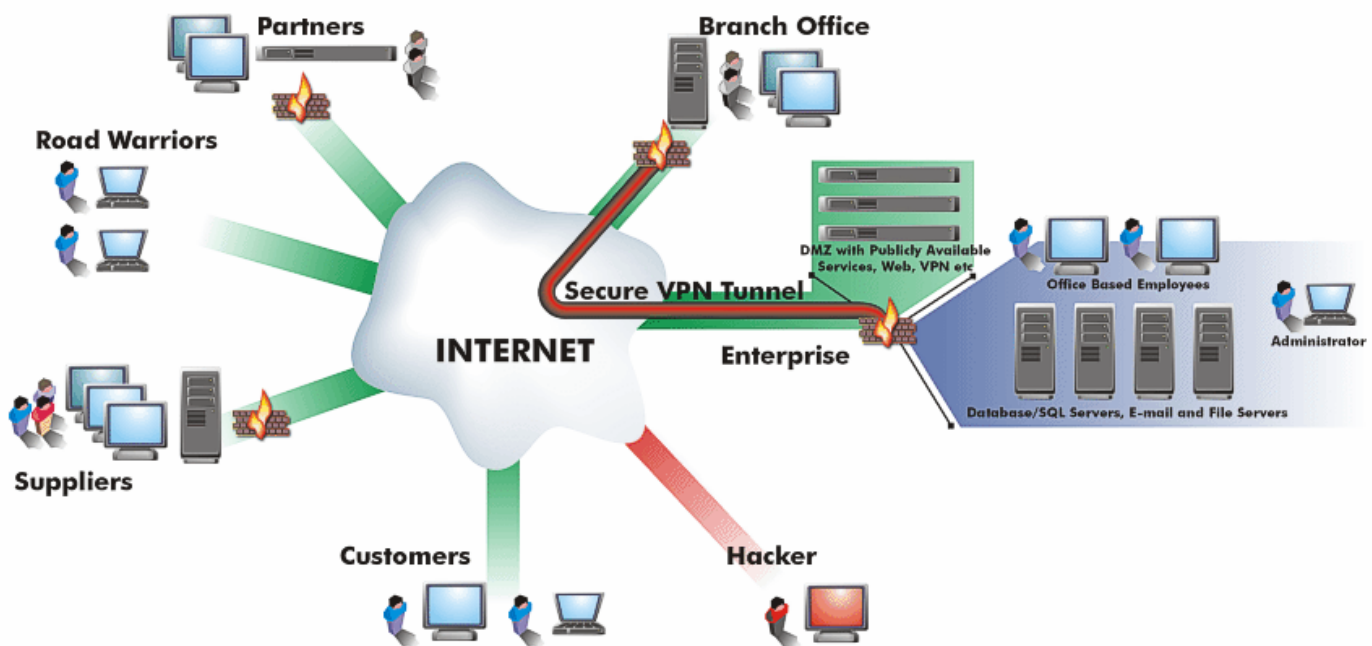


1 2 Suppliers and Partners.

There is a mutual benefit for both parties in having firewalls at either end of the communication line. Partners and suppliers are essential elements in any supply chain. Any enterprise will rely on both of these to operate a successful business. What happens if either has an attack which renders them inactive, or worse still what happens if they have data from you which then becomes open to your competition? It is essential that anyone with whom you deal with protects themselves as much as you would protect yourself.

3 Branch Office.

Setting up branch office communication with the advent of the Internet is simple. No longer is it necessary to use leased lines; however it is vital that security plays a major role in the choice of solution. An essential requirement is for an IPsec VPN tunnel, between the Enterprise firewall and the Branch office firewall. VPN stands for Virtual Private Network, effectively extending the internal network out to the branch office. IPsec is an industry standard secure communications protocol used for securely sending data across the internet. By using digital certificates at either end of the tunnel for authentication it ensures the strongest possible communication is used. A VPN tunnel is shown on the following page.



4 Road Warriors (Sales people who travel)

In a similar way a VPN between branch offices, Road Warriors also need to connect in from Hotels and Airports, grabbing the latest sales figures to clinch the deal. Again an unsecured connection between any of these and the enterprise, so IPsec is also used from the Road Warrior to the Enterprise. One important point to note is that the road warrior must have its own personal firewall software and anti-virus software running. Not having these in place opens a potential tunnel to the enterprise. Application level solutions are also now available such as SSL based VPN. All these issues should be considered in the choice of solution/provider.

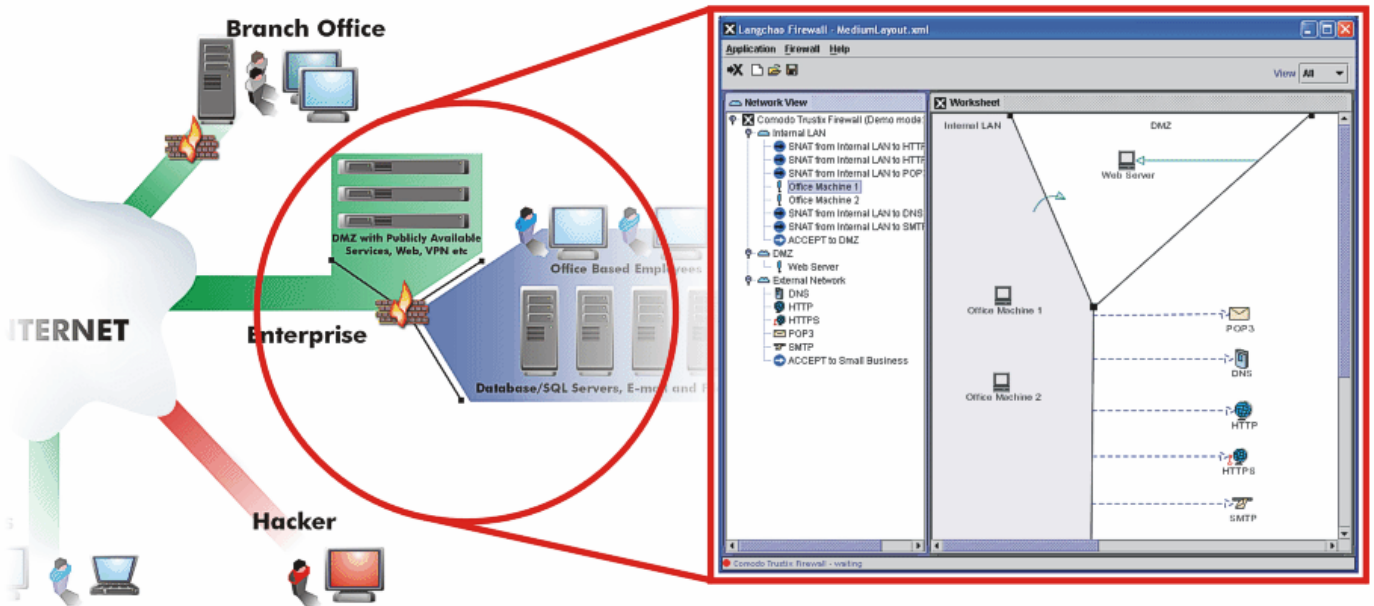
5 The Enterprise itself

The most obvious benefit is to the Enterprise itself. The pressures of new Legislation now drive adoption of solutions which have to meet all sizing requirements, protecting networks which are by their nature highly distributed. The favored business model of having numerous distributed branch offices and small satellite offices in various parts of the country/countries generates its own set of requirements which must be fully addressed by the chosen solution. Each office requires a consistent level of protection. Methods for secure remote administration of any settings must be provided. The solution must be scaleable as Enterprises must protect themselves with solutions that meet their ongoing requirements for growth. A solution must provide immediate security out of the box and finally one of the most important areas, the solution must provide benefits in terms of cost savings through effective simple administration.

In Conclusion.

Question: What single feature above all places any one solution ahead of its rivals?
Answer: The user interface.

It is the user interface alone which has the ability to create an efficient set-up process and effective maintenance/administration tool. A poor user interface can not only double or triple initial device expenditure; it can create extensive additional costs throughout the working life of the solution. Trustix™ Firewall server addresses all the needs of the Enterprise by providing a simple WYSIWYG (What You See Is What You Get) interface that maps real life enterprise architecture onto the administration interface.



Changes to the set-up through the interface are simple, effective and secure. The underlying rules engine optimizes the set-up of the firewall removing inconsistencies and potential gaps in the security policy. The fact that the administrative client is platform independent allows secure SSL encrypted remote administration from any location.

Choose the right Firewall solution for your enterprise. Choose Trustix.

Secure your future in under 25 minutes with a Trustix™ Firewall Server.

IBM®, eServer and xSeries® are trademarks of International Business Machines Corporation in the United States, other countries, or both. Other trademarks are the property of their respective owners.