



Firewall Basics

What is a network firewall?

A firewall is a system or group of systems that enforces an access control policy between two networks. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasise permitting traffic. Probably the most important thing to recognise about a firewall is that it implements an access control policy. If you don't have a good idea what kind of access you want to permit or deny, or you simply permit someone or some product to configure a firewall based on what they or it think it should do, then they are making policy for your organisation as a whole.

Why would I want a firewall?

The Internet, like any other society, is plagued with the kind of jerks who enjoy the electronic equivalent of writing on other people's walls with spray paint, tearing their mailboxes off, or just sitting in the street blowing their car horns. Some people try to get real work done over the Internet, and others have sensitive or proprietary data they must protect. Usually, a firewall's purpose is to keep the jerks out of your network while still letting you get your job done.

Many traditional-style corporations and data centres have computing security policies and practices that must be adhered to. In a case where a company's policies dictate how data must be protected, a firewall is very important, since it is the embodiment of the corporate policy. Frequently, the hardest part of hooking to the Internet, if you're a large company, is not justifying the expense or effort, but convincing management that it's safe to do so. A firewall provides not only real security - it often plays an important role as a security blanket for management.

Lastly, a firewall can act as your corporate "ambassador" to the Internet. Many corporations use their firewall systems as a place to store public information about corporate products and services, files to download, bug-fixes, and so forth. Several of these systems have become important parts of the Internet service structure (e.g.: UUnet.uu.net, whitehouse.gov, gatekeeper.dec.com) and have reflected well on their organisational sponsors.

What can a firewall protect against?

Some firewalls permit only Email traffic through them, thereby protecting the network against any attacks other than attacks against the Email service. Other firewalls provide less strict protections, and block services that are known to be problems.



Generally, firewalls are configured to protect against unauthenticated interactive logins from the "outside" world. This, more than anything, helps prevent vandals from logging into machines on your network. More elaborate firewalls block traffic from the outside to the inside, but permit users on the inside to communicate freely with the outside. Of course a firewall can't protect you against any type of network-borne attack if you unplug it!

Firewalls are also important since they can provide a single "choke point" where security and audit can be imposed. Unlike in a situation where a computer system is being attacked by someone dialling in with a modem, the firewall can act as an effective "phone tap" and tracing tool. Firewalls provide an important logging and auditing function; often they provide summaries to the administrator about what kinds and amount of traffic passed through it, how many attempts there were to break into it, etc.

What can't a firewall protect against?

Firewalls can't protect against attacks that don't go through the firewall. Many corporations that connect to the Internet are very concerned about proprietary data leaking out of the company through that route. Unfortunately for those concerned, a magnetic tape can just as effectively be used to export data. Many organisations that are terrified (at a management level) of Internet connections have no coherent policy about how dial-in access via modems should be protected. It's silly to build a 6-foot thick steel door when you live in a wooden house, but there are a lot of organisations out there buying expensive firewalls and neglecting the numerous other back-doors into their network. For a firewall to work, it must be a part of a consistent overall organisational security architecture. Firewall policies must be realistic, and reflect the level of security in the entire network. For example, a site with top secret or classified data doesn't need a firewall at all: they shouldn't be hooking up to the Internet in the first place, or the systems with the really secret data should be isolated from the rest of the corporate network.

Another thing a firewall can't really protect you against is traitors or idiots inside your network. While an industrial spy might export information through your firewall, he's just as likely to export it through a telephone, FAX machine, or floppy disk. Floppy disks are a far more likely means for information to leak from your organisation than a firewall! Firewalls also cannot protect you against stupidity. Users who reveal sensitive information over the telephone are good targets for social engineering; an attacker may be able to break into your network by completely bypassing your firewall, if he can find a "helpful" employee inside who can be fooled into giving access to a modem pool.

Lastly, firewalls can't protect against tunnelling over most application protocols to trojaned or poorly written clients. There are no magic bullets, and a firewall is not an excuse to not implement software controls on internal networks or ignore host security on servers. Tunnelling "bad" things over HTTP, SMTP, and other protocols is quite simple and trivially demonstrated. Security isn't fire and forget.



What about viruses?

Firewalls can't protect very well against things like viruses. There are too many ways of encoding binary files for transfer over networks, and too many different architectures and viruses to try to search for them all. In other words, a firewall cannot replace security-consciousness on the part of your users. In general, a firewall cannot protect against a data-driven attack -- attacks in which something is mailed or copied to an internal host where it is then executed. This form of attack has occurred in the past against various versions of sendmail and ghostscript, a freely-available PostScript viewer.

Organisations that are deeply concerned about viruses should implement organisation-wide virus control measures. Rather than trying to screen viruses out at the firewall, make sure that every vulnerable desktop has virus scanning software that is run when the machine is rebooted. Blanketing your network with virus scanning software will protect against viruses that come in via floppy disks, modems, and Internet. Trying to block viruses at the firewall will only protect against viruses from the Internet -- and the vast majority of viruses are caught via floppy disks.

Nevertheless, an increasing number of firewall vendors are offering "virus detecting" firewalls. They're probably only useful for naive users exchanging Windows-on-Intel executable programs and malicious-macro-capable application documents. Do not count on any protection from attackers with this feature.

Do I really want to allow everything that my users ask for?

It's entirely possible that the answer is "no". Each site has its own policies about what is and isn't needed, but it's important to remember that a large part of the job of being an organisation's gatekeeper is education. Users want streaming video, real-time chat, and to be able to offer services to external customers that require interaction with live databases on the internal network.

That doesn't mean that any of these things can be done without presenting more risk to the organisation than the supposed "value" of heading down that road is worth. Most users don't want to put their organisation at risk. They just read the trade rags, and see advertisements, and they want to do those things, too. It's important to look into what it is that they really want to do, and help them understand how they might be able to accomplish their real objective in a more secure manner.

You won't always be popular, and you might even find yourself being given direction to do something incredibly stupid, like "just open up ports foo through bar", and don't worry about it. It would be wise to keep all of your exchanges on such an event so that when a 12-year-old script kiddie breaks in, you'll at least be able to separate yourself from the whole mess.

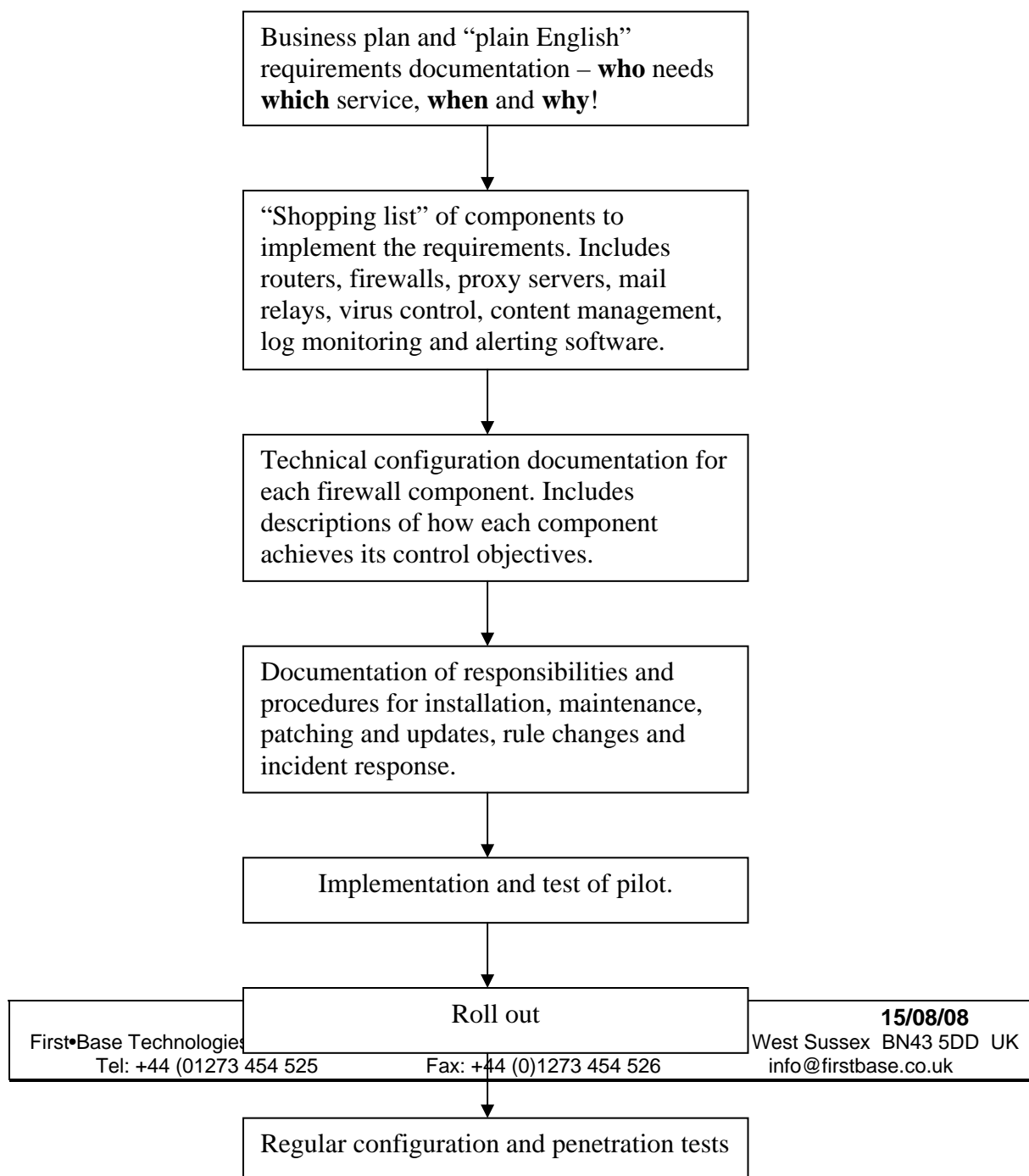


General Guidance

1. Firewalls are only as sound as their supporting firewall policies. It is imperative that the rules concerning the configuration of every component in the firewall (Internet router, firewall, proxy server, virus software) are properly understood, fully documented and carefully implemented. Independent testing of the firewall on a regular basis, and especially immediately after installation, is essential. The majority of successful hacking attempts are due to inadequate or faulty configuration of one or more firewall components. Apply the following in your firewall strategy:
 - 1.1. Implement an address translating router, configured to pass only packets destined for the firewall computer
 - 1.2. A firewall computer supporting at least two (preferably three) network cards, one connecting only to the external router, one to the corporate network and (optionally) one to the demilitarised zone (DMZ), to which any proxy servers are connected
 - 1.3. Implement an alerting system to warn of attempted attacks. Alerts should ideally be generated by the router, firewall and proxy servers.
 - 1.4. The firewall should be proof against denial of service attacks (either by rejecting packets or by shutting down)
 - 1.5. Remote management of any component in the firewall should not be permitted.
 - 1.6. Independent testing of the firewall configuration is essential. Attacks on the firewall by a firm specialising in such services should be carried out immediately after implementation and on a regular basis thereafter.
 - 1.7. Careful screening of employees who are to have physical or logical access to the firewall components or their documentation is most important.
 - 1.8. All firewall components should be located in a secure room with controlled and limited access.
 - 1.9. If Internet downtime is perceived as a potential problem, a duplexed installation might be considered. Bear in mind that the opportunity for configuration error is also doubled in this situation and extra care should be taken in documenting, implementing and testing such an installation.
2. The bottleneck effect of each firewall component must be carefully measured to ensure that future traffic volumes are not constrained by today's choice of product. Performance is as important as security in each of these components.
3. Remote access via dial-in directly to company premises must be carefully controlled. A "dial back" policy, requiring the user to be accessing from a known telephone number, further protected by user name and password is strongly recommended. If this is impractical then tokenised (e.g. SecurID) remote access devices should be employed. In any event, proper records of users permitted remote access, controls regarding access time of day, location, etc. must be instigated. Passwords must be changed regularly (most remote access passwords are not) and user names must be unique to each individual. Where possible, audit trails should be generated (and inspected!) for any remote access devices.



4. Staff must be made aware of their responsibilities in using the Internet (and any other remote connection) via a thorough Internet Security Policy.
5. Policies and procedures must be applied to contractors and third-party employees as thoroughly as to staff. Third-party organisations must be asked to sign “like measures” contracts to ensure that they apply similar controls to the company’s.
6. Firewalls can't protect against attacks that don't go through the firewall. Many corporations that connect to the Internet are very concerned about proprietary data leaking out of the company through that route. Unfortunately for those concerned, a magnetic tape or diskette can just as effectively be used to export data.
7. In summary, be sure to implement the following stages:





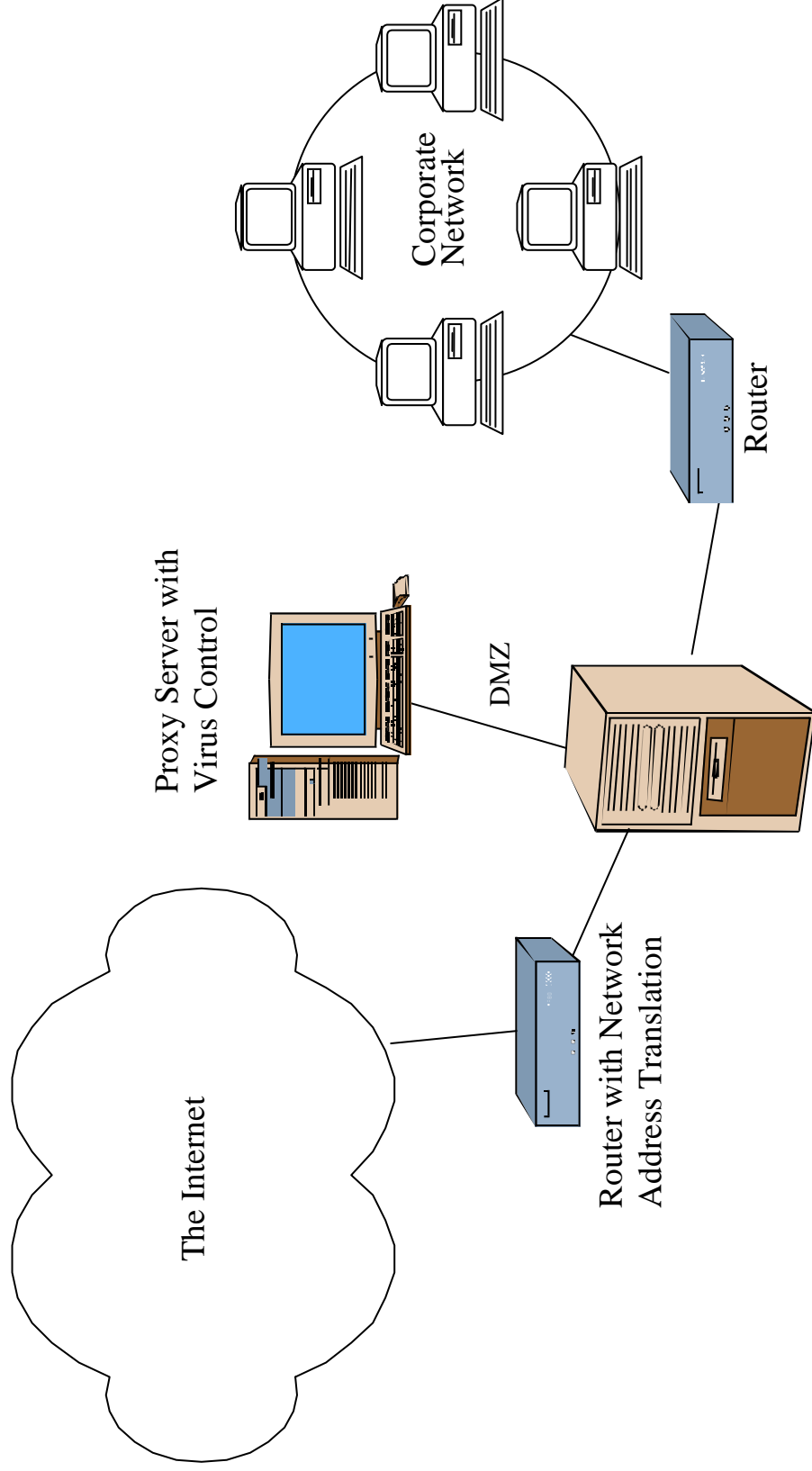
Example “Shopping List”

1. An Internet router with Network Address Translation (NAT)¹ and static route table to firewall box.
2. All firewall software to run on hardened Microsoft NT 4.0 operating system installed on Compaq or HP Intel hardware **or** on hardened Sun Solaris UNIX boxes.
3. Primary firewall box to have three network interface cards (external, internal and DMZ). Static routing to all DMZ boxes.
4. Primary firewall box to run FireWall-1 firewall software.
5. Content management to be delivered by MIMESweeper 3.2 content control software located on the DMZ. Static routing to the primary firewall box.
6. Dr Solomon’s anti-virus installed on the MIMESweeper host.
7. URL screening and reporting to be delivered by WebSENSE URL-screening software located on the DMZ.
8. An internal router with a static route table to firewall box.

¹ Alternatively NAT may be implemented in the firewall box.



Block Diagram of a Minimum Firewall Implementation



Firewall computer

15/08/08



Audit Plan

Internet Access

Are there written guidelines for the use of Internet services?

- No Draft Finalised (not issued) Issued (not trained) Issued & trained

Is secure access to the Internet provided by using a firewall between internal networks and the Internet?

- No Yes

Are users strictly forbidden to bypass the firewall, e.g. by using a locally attached modem for direct access to the Internet?

- No Yes N/A

Are all users of the Internet formally authorised to do so by their management?

- No Some Yes

Are limitations on use specified?

- No Yes

Are all risks associated with usage of the Internet assessed before use of the service?

- No Sometimes Always

Are PCs accessing the Internet required to run resident virus protection software?

- No Some Yes

Does each user have a dedicated username and password for access to the service?

- No Some Yes

Are all staff required to log off from the Internet when they leave the office or when leaving their computer unattended for lengthy periods of time?

- No Yes

Are licence conditions related to the commercial use of software available on the Internet observed?

- No Sometimes Always

Are all software programs or scripts downloaded from the Internet required to be approved by the IT department before use?

- No Some Yes

Is copyrighted or sensitive material required to be encrypted before being sent, received or copied via the Internet?

- No Some Yes



Is any software program or script downloaded from the Internet required to be separately virus checked?

- No Yes

Use of Internet e-mail

Are there written guidelines for the use of e-mail?

- No Draft Finalised (not issued) Issued (not trained) Issued & trained

Are staff forbidden to include the following in e-mail messages:

indecent material?

- No Yes

obscene material?

- No Yes

libellous material?

- No Yes

material likely to cause offence?

- No Yes

material which harasses any other employee or third party on the basis of sex, race or disability?

- No Yes

Are staff strictly forbidden to send or deliberately attempt to receive e-mail known to contain a virus?

- No Yes

Are staff forbidden to use e-mail for:

gambling?

- No Yes

conducting illegal activities?

- No Yes

soliciting for personal profit?

- No Yes

Are staff forbidden to reveal or publicise information which is confidential either to the Company or its customers and clients?

- No Yes

Are staff forbidden to forward e-mail chain letters?

- No Yes

Are staff forbidden to access confidential information using the password of another user?

- No Yes

Firewall Configuration & Management



Are staff forbidden to use Company e-mail systems for personal use?

- No Yes

Have staff been advised that they should only send information by Internet e-mail which they would be prepared to send on the Company's headed paper?

- No Yes

Have staff been advised that they should not buy or sell goods or services via Internet e-mail?

- No Yes

Have staff been advised that scanned signatures must not be appended to Internet e-mail messages?

- No Yes

Have staff been advised not to open e-mail attachments unless they know who they are from and are expecting to receive them?

- No Yes

Have staff been advised that e-mail messages sent via the Internet should only be used for information which is not commercially sensitive or covered by the Data Protection Act?

- No Yes

Have staff been advised that e-mail containing sensitive information may need to be encrypted?

- No Yes

Are there controls to ensure that e-mail names are not the same as system logons?

- No Yes

Have staff been advised that business standards should be observed in e-mail messages?

- No Yes

Have staff been advised that before forwarding a single e-mail to a new or revised distribution, they should make sure that they read all the earlier messages, as they may contain personal comments that should not be redistributed?

- No Yes

Are staff required to regularly review stored e-mail and delete unwanted material?

- No Yes

Firewall Documentation

Is there a business plan, containing "plain English" requirements documentation? (detailing who needs which service, when and why)

- No Yes

Firewall Configuration & Management



Is there a “shopping list” of components required to implement the requirements of the business plan? (detailing routers, firewalls, proxy servers, mail relays, virus control, content management, log monitoring and alerting software)

No Yes

Is there thorough technical configuration documentation for each firewall component? (detailing descriptions of how each component achieves its control objectives)

No Yes

Firewall Configuration & Management



Is there documentation of responsibilities and procedures for:

installation?

No Yes

maintenance?

No Yes

patching and updates?

No Yes

rule changes?

No Yes

incident response?

No Yes

Are there regular configuration and penetration tests of all firewall components?

No Yes

Are there configuration and penetration tests of all firewall components after each change of configuration or update?

No Yes