

Firewall Policy & Specification

for

XXXXXXXX

CONFIDENTIAL



Contents

ISSUE STATUS	2
DISTRIBUTION LIST	2
APPROVALS	2
CONTENTS	3
OBJECTIVE OF THE FIREWALL POLICY AND SPECIFICATION	4
INTRODUCTION	5
FIREWALL TESTING.....	6
FIREWALL MAINTENANCE AND ADMINISTRATION.....	7
FIREWALL IMPLEMENTATION	8
FIREWALL CHANGE CONTROL.....	9
XXXXXXX FIREWALL OVERVIEW	11
XXXXXXX FIREWALL RULES	12
PRODUCT SHOPPING LIST	14
IMPLEMENTATION CHECK LIST.....	15



Objective of the Firewall Policy and Specification

1. To provide detailed guidance for the selection, implementation and change control of firewall components, based on the statement of requirements in the Security Requirements Document for XXXXXXX.



Introduction

1. A firewall is a system or group of systems that enforces an access control policy between two or more networks. The most important thing to recognise about a firewall is that it implements a policy. If you do not have a formal description of 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.
2. Firewalls are important since they can provide a single “choke point” where security and audit can be imposed. Firewalls provide an important logging and auditing function; they provide summaries about what kinds and amount of traffic passed through, how many penetration attempts there were, etc.
3. 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.
4. Firewalls cannot 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 avoid software controls on internal networks or ignore host security on servers. Tunnelling over HTTP, SMTP, and other protocols is quite simple and trivially demonstrated. Security is not fire and forget.
5. 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.



Firewall Testing

6. 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. Attacks on the firewall by a firm specialising in such services, using reputable testing software, should be carried out immediately after implementation and on a regular (preferably monthly) basis thereafter.
7. Implement an alerting system to warn of attempted attacks. Ideally, alerts should be generated by the firewall and by the proxy servers. Penetration tests should trigger these alerts.



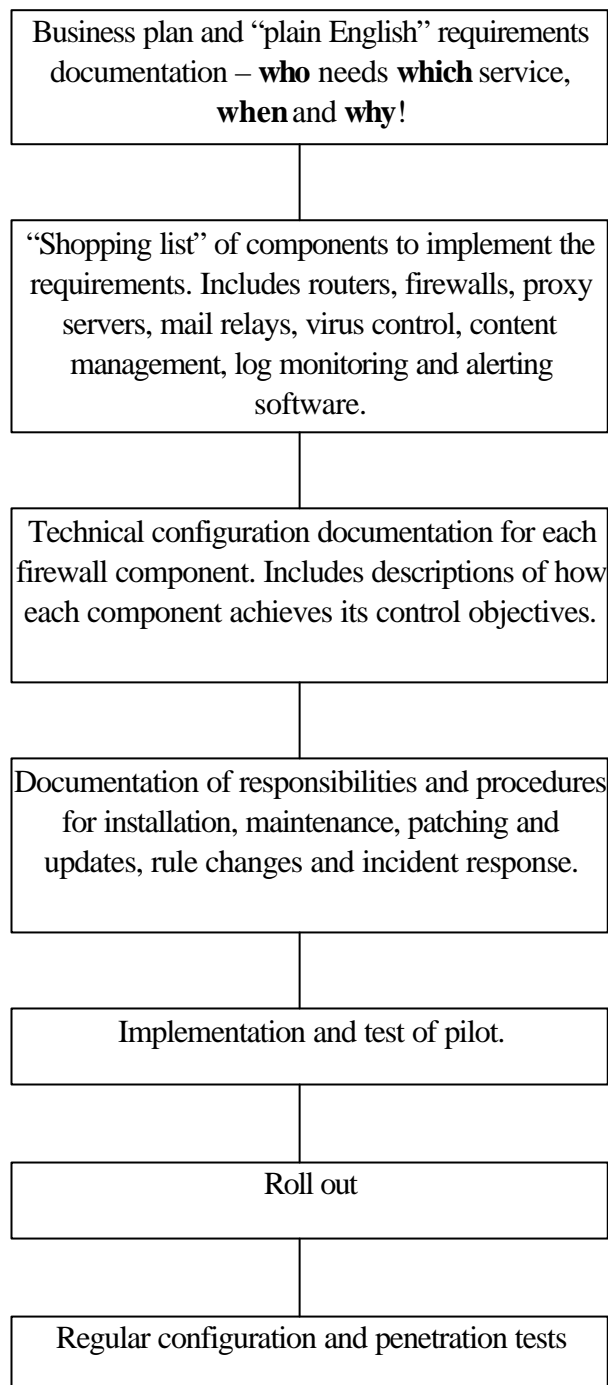
Firewall Maintenance and Administration

8. Careful screening of anyone who is to have physical or logical access to the firewall components or their documentation must be conducted. This should include at least two references (one business, one character), an identity check (passport or driving license) and a credit check.
9. Anyone who is to have physical or logical access to the firewall components or their documentation must sign a non-disclosure and confidentiality agreement.
10. Policies and procedures must be applied to contractors and third-party employees as thoroughly as to permanent staff. Third-party organisations must be asked to sign “like measures” contracts to ensure that they apply similar controls to the company’s.
11. All firewall components should be located in a secure room with controlled and limited access.
12. Remote management of any component in the firewall must not be permitted, unless via an encrypted and authenticated dial-up connection.
13. If firewall 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.
14. 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.



Firewall Implementation

15. Be sure to implement the following stages:





Firewall Change Control

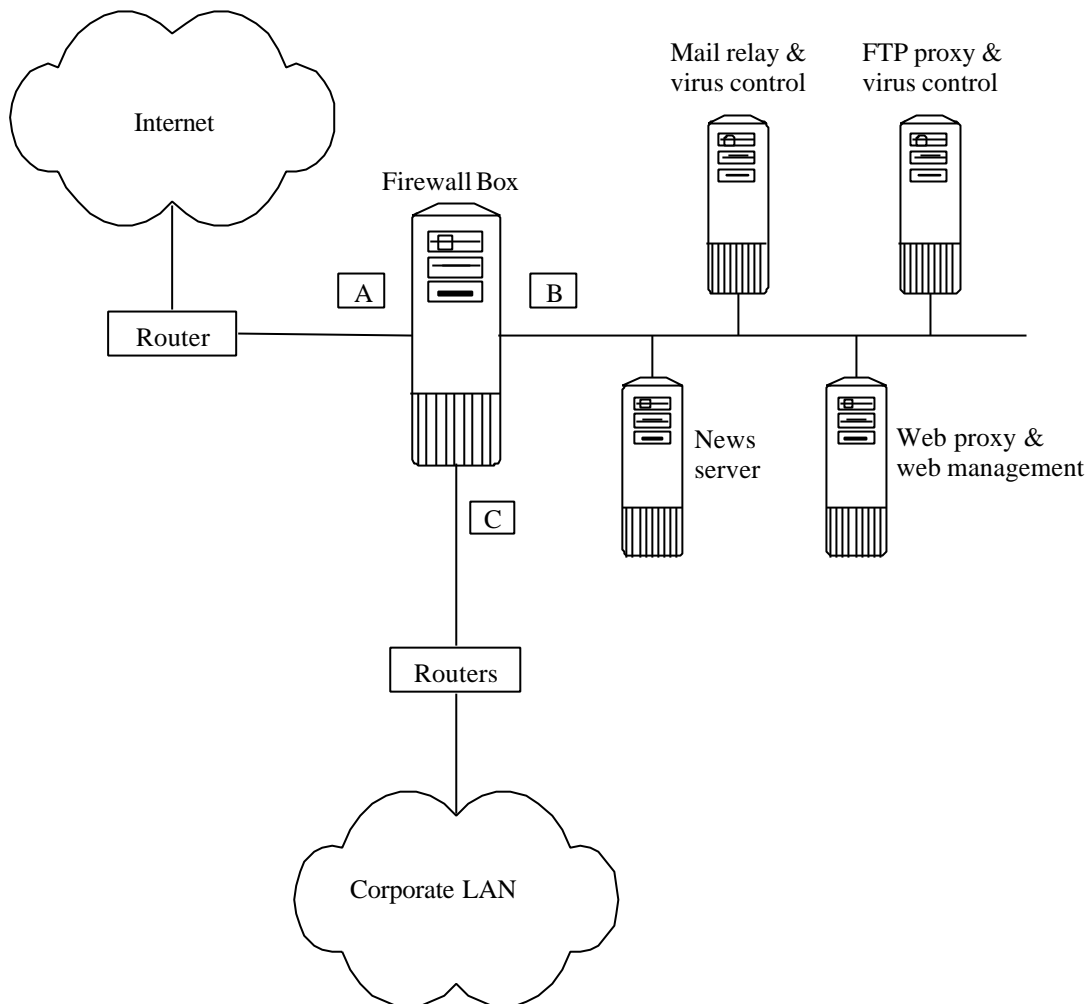
16. The firewall documentation must be regarded as a **controlled system**. The firewall documentation will comprise:
- the *Security Requirements of xxxxxxxxx*
 - the *Firewall Policy and Specification for xxxxxxxxx*
 - the *xxxxxxx Firewall Change Log*
 - the printed configuration of the firewall operating system (including all user accounts)
 - the configuration of the firewall software and its rules
17. When a controlled document is updated, the obsolete document must be recalled and the updated document issued. All old copies must be destroyed except one, which must be marked “Obsolete” and retained in the Document Change file.
18. “Changes” means any changes in the firewall system **whatsoever**, including (but not limited to):
- hardware
 - operating system
 - firewall software
 - proxy software
 - firewall rules
 - use or number of administrative accounts
 - physical location of the firewall components
19. Any changes to the firewall configuration **whatsoever** must be validated against the Requirements Document and the Firewall Policy and Specification (this document). If necessary these documents must be updated and re-approved to reflect the changes.
20. Any changes to the firewall configuration **whatsoever** must be recorded in the firewall change log.
21. Each controlled document shall contain the following information:
- Document name and location (in the header)
 - Issue date (in the header)
 - Issue number (in the footer)
 - Page number and total number of pages (in the footer)



22. Document change records must be retained for a period of 5 years.



XXXXXX Firewall Overview



23. The firewall box (“the XXXXXX Firewall”), controls the traffic between XXXXXX users (interface “C”), the demilitarised zone (interface “B”) and the Internet (interface “A”)
24. Proxy hosts are located on the demilitarised zone (DMZ). *Although each proxy is shown as a separate computer, proxy functions may be combined where product compatibility, performance and traffic volume permit.*
25. The firewall will be configured to block all traffic, with the exception of the rules in the table shown in this document.



XXXXXX Firewall Rules

26. Only the following traffic will be permitted in the XXXXXX firewall.

Ref No	From	To	Protocol	Restrictions
1	A	B	HTTP/HTTPS	To web proxy only (by IP address)
2	B	A	HTTP/HTTPS	From web proxy only (by IP address)
3	C	B	HTTP/HTTPS	To web proxy only (by IP address)
4	B	C	HTTP/HTTPS	From web proxy only (by IP address)
5	A	B	FTP	To FTP proxy only (by IP address)
6	B	A	FTP	From FTP proxy only (by IP address)
7	C	B	FTP	To FTP proxy only (by IP address)
8	B	C	FTP	From FTP proxy only (by IP address) (download B to C only)
9	A	B	NNTP	To news server only (by IP address)
10	B	A	NNTP	From news server only (by IP address)
11	C	B	NNTP	To news server only (by IP address)
12	B	C	NNTP	From news server only (by IP address)
13	A	B	SMTP	To mail relay only (by IP address)
14	B	A	SMTP	From mail relay only (by IP address)
15	C	B	SMTP	To mail relay only (by IP address)
16	B	C	SMTP	From mail relay only (by IP address)

27. The mail relay will be configured to log all mail traffic and to virus scan (and quarantine where appropriate) all e-mail attachments.

28. The web proxy will utilise web management software to block access to libellous, offensive or pornographic material and to non-business sites. The web management software will also be configured to monitor web use.

29. The FTP proxy will be configured to monitor all FTP traffic and to virus scan (and quarantine where appropriate) all file transfers.



30. The news server will be configured to block access to non-business sites and to monitor newsgroup use.



Product Shopping List

31. The firewall computer must be of reputable manufacture and have a formal maintenance contract.
32. The firewall computer must run either a hardened Microsoft NT 4.0 operating system or a hardened commercial UNIX operating system. (Hardening documents are available from www.sans.org.)
33. The firewall software must be a well-proven product with stateful inspection functionality (e.g. FireWall-1) and should be proof against denial of service attacks.
34. The mail relay software must be a well-proven product (e.g. MAILsweeper) with the facility to log and virus scan e-mails. The virus software used must be a well-proven product (e.g. Sophos) with regular (daily) updates.
35. The web proxy and content management software must be a well-proven product (e.g. WEBSweeper) with the facility to monitor and control web access.
36. The FTP proxy software must be a well-proven product (e.g. WEBSweeper) with the facility to monitor and virus scan file transfers. The virus software used must be a well-proven product (e.g. Sophos) with regular (daily) updates.
37. The news server software must be a well-proven product configured to exclude non-business related newsgroups.
38. An alerting and reporting system should be implemented to manage the logs of all the firewall components.



Implementation Check List

39. Use the following check list to determine that users are correctly prepared for use of the firewalled service:

Are there written guidelines for the use of firewalled services?

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

Are all users of firewalled services formally authorised to do so by their management?

No Some Yes

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

No Some Yes

40. Use the following check list to determine that the firewall is properly implemented:

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

No Yes

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

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

Firewall Policy and Specification for XXXXXX



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

€ No € Yes