

SP
SILICON PRESS
www.silicon-press.com

*Information to
Understand
Technology*

Firewalls

Technology Report
2002

ISBN 0-929306-23-6

M. S. Sriram
info@silicon-press.com

Copyright © 2002 by Silicon Press. All Rights Reserved.

The Customer may excerpt, paraphrase, or quote up to 80 words and 3 charts from a Report, in total and collectively in various forums, with the remark appropriately attributed, with no single excerpt or quote of more than 40 words, provided that the Silicon Press copyright notice is affixed thereto and that no such excerpt, paraphrasing, or quotation shall (a) modify or alter the general impressions of the Report or (b) imply sponsorship, approval, or endorsement by Silicon Press. Except as permitted by the prior sentence, the Customer is not permitted copy, duplicate, distribute, or create derivative works of the report or any portion thereof. Except for the permission above, all other rights, including title and interest in and to the reports, remain the sole and exclusive property of Silicon Press. This includes all copyright, trade secret, trademark, patent, and other proprietary rights therein. The Customer may not remove or alter any logo, trademark, or copyright or any other proprietary notices on the Report. Inquiries regarding permission to copy or use the Report in any other manner should be directed to Silicon Press's marketing department (info@silicon-press.com).

The Customer hereby acknowledges that a breach of obligations under this section would cause Silicon Press irreparable damage for which remedies other than injunctive relief would be inadequate, and agree that in any such event, Silicon Press will be entitled to an injunction or similar equitable relief immediately upon request to a court of competent jurisdiction, without having to show anything other than the fact of such breach.

Silicon Press Reports are protected by the copyright laws of the United States and international treaty provisions. Copyright infringement can be both civilly and criminally prosecuted, and Silicon Press will take all steps necessary to protect its rights.

The information contained in this Report is believed to be reliable but its accuracy and completeness is not guaranteed.

ISBN 0-929306-23-6

Firewalls

Executive Summary

Corporate networks are facing serious threats from hackers with a variety of motivations and agendas such as industrial espionage, political “hactivism”, terrorism, or just for the “fun” of it. Even home computers and networks are not immune from such attacks and they are frequently used as a launching pad for more “attractive” targets. Unauthorized access to networks can result in substantial business losses arising from theft, destruction, or corruption of corporate data, or from damage to the network. Consequently, network security is key to business integrity and, in some cases, business survival.

Firewalls represent the first line of defense against network attacks, and represent the network equivalent of a strong perimeter defense. A properly configured firewall can be one of the most useful defensive weapons, in a network administrator’s arsenal, to ensure the integrity of a corporate network.

In this report, we will discuss the importance of firewalls, how firewalls work, and how they are used. We will describe the different types of firewalls, how they are deployed in a network, the protection they offer, and their relationship to other network components. We will then discuss how to select, deploy, administer, and maintain a firewall solution. We will also examine some of the vulnerabilities and limitations of firewalls and discuss issues related to selecting a firewall. The common attacks on networks are listed in an appendix.

The goal of this report is to help make the decision maker conversant with firewall technology to facilitate and help in making decisions relating to firewalls and network security.

Contents

What is a Firewall?	1
What Can Firewalls Do?	2
How Do Firewalls Work?	3
Data on the Internet	3
Packet Filtering	5
Other services	6
Network and Application Level Firewalls	6
Firewall Configuration: Rules	7
Types of Firewalls	8
Personal Firewalls	8
Firewall Appliances	9
Firewall Kits	10
Software Firewalls	11
Internet Appliances with Firewalls	12
Enterprise Class Firewalls	13
Firewall Comparison	14
Firewalls and Other Network Components	14
Routers	14
Gateways	15
Proxy Servers (Proxies)	15
Web Blockers	16
Anti-Virus and Anti-Trojan Software	17
Firewall and Network Architecture	17
Home Computers	18
Home Networks	18
SOHO (Small Office Home Office) Network	20
Bastion Hosts	22
Enterprise Networks	23
Enterprise with Geographically Separate Networks	25
Isolating Departments	27
Merging Networks	29
Vulnerabilities & Limitations of Firewalls	30
Outdated Configuration	30
Subversion	30
Trojan Horses	31
Perimeter Violations	32
Advanced Web Services	32
Authentication Failures	33
Physical Security	33
Firewall Operating System Vulnerabilities	33

Performance.....	34
Firewall Maintenance and Monitoring	34
Cost of Deploying a Firewall	35
Purchase	35
Maintenance.....	35
Standards and Certification	36
Selecting a Firewall	36
Final Comments	37
Where Can I Get More Information?	38
Appendix A: Common Attacks	39
Appendix B: Glossary.....	41

Preview