

SYNGRESS®

SECURITY SAGE'S **Guide** **to**

Hardening the Network Infrastructure

Steven Andrés
Brian Kenyon

Foreword by
Erik Pace Birkholz
Series Editor

Jody Marc Cohn
Nate Johnson
Justin Dolly

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively “Makers”) of this book (“the Work”) do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, “Career Advancement Through Skill Enhancement®,” “Ask the Author UPDATE®,” and “Hack Proofing®,” are registered trademarks of Syngress Publishing, Inc. “Syngress: The Definition of a Serious Security Library”™, “Mission Critical™,” and “The Only Way to Stop a Hacker is to Think Like One™” are trademarks of Syngress Publishing, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY	SERIAL NUMBER
-----	---------------

001	KLBR4D87NF
002	829KM8NJH2
003	JOY723E3E3
004	67MCHHH798
005	CVPL3GH398
006	V5T5T53455
007	HJJE5768NK
008	2987KGHUIN
009	6P5SDJT77Y
010	I295T6TGHN

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

Security Sage’s Guide to Hardening the Network Infrastructure

Copyright © 2004 by Syngress Publishing, Inc. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0
ISBN: 1-931836-01-9

Series Editor: Erik Pace Birkholz
Technical Editor: Justin Dolly
Page Layout and Art: Patricia Lupien

Cover Designer: Michael Kavish
Copy Editor: Beth Roberts
Indexer: Nara Wood

Distributed by O’Reilly & Associates in the United States and Jaguar Book Group in Canada.

Foreword

When I created the book *Special Ops: Host and Network Security for Microsoft, UNIX and Oracle*, I attempted to include a chapter to cover each common yet critical component of a corporate network. More specifically, I coined the phrase *internal network security*; which was really just an asset-centric approach to securing your hosts and networks from the inside-out. After the release of *Special Ops* it became clear (to Syngress and me) that some of the topics covered in *Special Ops* warranted an entire book. To satisfy this need, we have created the exciting new series entitled: *Security Sage's Guides*.

Security Sage's Guide to Hardening the Network Infrastructure is the first book in this series; concentrating on the bottom OSI layers that provide a solid foundation to any sound security posture. The next book in the series is *Security Sage's Guide to Attacking and Defending Windows Server 2003*. This book will give readers the practical knowledge they need to defend their resources from both a management and operational level using Microsoft's new Windows Server 2003. In *Hacking Exposed* I stated, "The majority of my (security) concerns, in most cases, are not a result of poor products but products being implemented poorly." The *Security Sage's Guides* aim to deliver you the information you need to fight host and network negligence.

Drawing from their extensive real world experiences and showcasing their successes as well as their failures, Steven Andrés and Brian Kenyon provide the reader with a comprehensive tactical and strategic guide to securing the core of the network infrastructure. This book details how to attack, defend and securely deploy routers, firewalls, switches, Intrusion Detection Systems (IDS), and the network protocols that utilize them. The goal was to create a readable and usable book that would empower its readers to mitigate risk by reducing attack vectors, remediation of known vulnerabilities, and segmenting critical assets from known threats. *Security Sage's Guide to Hardening the Network Infrastructure* is

an indispensable reference for anyone responsible for the confidentiality, integrity, and availability of critical business data.

UNIX or Windows? Apache or IIS? Oracle or MySQL? . . . Regardless of where you draw your political line, you need a solid foundation to communicate securely and reliably with your corporation's networks, servers, and users. Network infrastructure is the foundation and underlying base of all organizations. Unless you were blessed by the Network Fairy, it is likely you are faced with supporting, securing, and monitoring an infrastructure designed for usability rather than security. Shifting this network paradigm is not a simple task; expect heavy resistance from users and administrators while reducing their usability to increase their security.

A great network doesn't just happen—but a bad one does. Some of the worst network designs have reared their ugly heads because of a lack of forethought as to how the network should ultimately look. Instead, someone said, 'Get these machines on the network as cheaply and quickly as possible.'

—Chapter 11 "Internal Network Design"

On January 28th 1986, a similar mentality cost America the lives of seven pioneers when the space shuttle Challenger exploded just 73 seconds into its mission. The real tragedy was that the whole thing was avoidable; the potential for cold temperature O-ring failure was a known vulnerability. The engineers at Thiokol issued a written recommendation advising against a shuttle launch in temperatures below 53 degrees Fahrenheit. Some would argue it was a break down in the communication process that held these facts from the final decision makers, but others point to the fact that the previous three launch cancellations had severely damaged the image and publicity of the whole event; in turn affecting potential future funding of NASA. Whatever the case, the temperature on January 28th was a shivery 36 degrees and usability won out at the cost of security.

Over the past two years, network based worms opened the eyes of executives in boardrooms around the globe. From management's perspective; the security of a corporate network can exist in two states; *working* and *not working*. When business operations halt due to a security issue, management is forced to re-assess the funds and resources they allocated to ensure they are adequately protecting their critical host and network based operations. In this case, wealthy corporations won't hesitate to throw money at the problem of security;

expecting to find a panacea in the industry's newest security solution. Alternatively, corporations concerned with ROI and TCO for IT investments would be better served to empower their InfoSec staff; Asking them to assess their current network architecture and rearchitect low cost yet secure solutions that keep the corporate packets moving securely, day after day.

The good news is that everyone is finally thinking about security; now is our time to execute. *Security Sage's Guide to Hardening the Network Infrastructure* is dedicated to delivering the most up-to-date network layer attacks and mitigation techniques across a wide assortment of vendors, and not just the typical attention paid to market leaders such as Cisco and Checkpoint (although these are obviously covered in great detail). This expanded breadth will help reach a wider range of network engineers who may not have the budget to purchase and install best-of-breed hardware, but want to know how to make the most out of what they do have.

In the early parts of my career I worked as a young auditor for two of the Big 5 accounting firms. I assisted the audit teams by reviewing the effectiveness of information security controls as part of the larger General Control Reviews (GCR). Large client after large client, I found the state of InfoSec controls was worse than I could have imagined.

I would find critical choke routers protecting the financial servers, and was able to gain complete control of the router with default SNMP community strings of *private*. This little oversight allowed me to download or modify router configurations and access control lists. Frequently, financial servers were running on Windows and were therefore part of an NT Domain. After a cursory assessment of the PDC or BDC, I would find *Domain Admin* accounts with weak or blank passwords. I developed quite a talent for divining privileged windows accounts with poor passwords. As an all-powerful *Domain Admin*, I connected directly to the financial servers with the ability to view, modify or delete critical corporate data. Finally, I can't count how many poor Solaris boxes running an Oracle database were easily compromised because the administrator didn't bother to change the password for the Oracle user account. Our running joke was something about how all you needed to know to hack UNIX was *oracle:oracle*.

After each engagement I would carefully document my findings and deliver them as draft to my manager or the regional partner for inclusion in the audit report. What a joke. Did my ineffective security control findings cause the

auditors to take a closer look at the integrity of this data the controls were failing to protect? Not even close, the information was “adjusted” up the line before it ever saw a genuine audit report. How bad was it? Let’s just say that no matter how many high risk or critical vulnerabilities I uncovered, the end result communicated to the audit team and eventually the customer was always effective internal controls.

New SEC legislation such as Sarbanes–Oxley will force infrastructure accountability by requiring management to report on the effectiveness of their corporate internal controls over financial data and systems. Hopefully, the days of ineffective control “adjustments” will dwindle once executives are accountable for the disclosure and integrity of these controls. Just maybe this new found accountability will force companies to create, review, implement and enforce effective corporate security policies and procedures supported by securely architected network infrastructures. If it does and you have read this book; executing on your infrastructure initiatives should be a snap.

—*Erik Pace Birkholz, CISSP*

Series Editor

Foundstone Inc. & Special Ops Security

Author of *Special Ops: Host and Network Security for Microsoft, UNIX and Oracle*

Co-author of *SQL Server Security* and *Hacking Exposed*

Selecting the Correct Firewall

Solutions in this Chapter:

- Understanding Firewall Basics
- Exploring Stateful Packet Firewalls
- Explaining Proxy-Based Firewalls
- Examining Various Firewall Vendors

Related Chapters:

- Chapter 4 Attacking Firewalls
- Chapter 7 Network Switching
- Chapter 10 Perimeter Network Design
- Chapter 11 Internal Network Design

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

Introduction

Early in human history, people recognized fire as both a tool and a danger. We could easily say the same thing about information—the right information in the wrong hands has probably destroyed almost as many companies as fires have. Therefore, borrowing an architectural term used to denote a structure for containing a potential disaster seems apropos. A *firewall*, when discussed in the realm of computers, prevents unauthorized access to protected networks from users outside the protected network.

Firewalls likely serve as the most important component to network security, second only to the physical security of the network. Prior to the Internet, most firewalls were used in networks that protected high-security installations where employees had distinct security ratings, such as defense contractors. Firewalls were originally employed for the purpose of allowing certain employees to connect to the inner sanctum of the company's data as a form of access control.

The Internet has changed the purpose and function of the firewall. By plugging in a single cable, a network administrator has the potential to make a company's data as accessible to the CEO as it is to the other six billion people on the planet. The new breed of firewall needs to allow a small population of that six billion to have expanded access, and the rest must be stopped at the door. All this must be accomplished with the flexibility to protect against attacks that hackers haven't even invented yet. Of course, a piece of hardware cannot take the place of a well-crafted security policy that incorporates all aspects of the network. However, in many installations the firewall *is* the only manifestation of the security policy.

To that end, we are going to examine the basic building blocks of modern firewalls. Once we understand what makes a firewall tick, we have to find out which of the two major types of firewalls—proxy or stateful inspection—are right for your organization. There's a big difference between the two, and it comes down to a trade-off between functionality and performance. Finally, we'll round out this firewall festival with a discussion on all the major vendors and what makes them so special.

Understanding Firewall Basics

Firewalls need to do more than just protect the good guys from the bad guys. The United States government has taken an active interest in computer security since well before the first integrated circuit rolled off the assembly lines. With this in mind, it makes sense to examine the government's regulations on

firewalls...except there aren't any. Similar to the movie industry, firewall manufacturers police themselves.

Seal of Approval

ICSA Labs, a division of TruSecure Corporation, provides firewall certification based on the input of the Firewall Product Developer's Consortium (FWPD), a 46-member organization of the who's who in network security (www.icsalabs.com/html/communities/firewalls/membership). This certification is an important seal of approval for the industry but does not imply that a particular firewall is fit for your network. The goal of the ICSA Labs certification is to ensure that what a vendor markets as a firewall actually operates in a firewall capacity. The network firewall criteria are available for download and center on a set of feature tests. The specific objectives for personal firewalls spells things out more clearly:

- Capability to support Microsoft Networking capabilities while providing endpoint protection
- Capability to support concurrent dial-up and LAN connectivity
- Capability to block common external network attacks
- Capability to restrict outgoing network communications
- Capability to maintain consistent protection across multiple successive dial-up connections
- Capability to log events in a consistent and useful manner

All the firewalls that we discuss later in this chapter have attained ICSA Labs certification. Being the only barometer for the industry, you should demand that your next firewall vendor has passed this important baseline certification. Attaining this certification is not so much an award the vendor receives, but a seal of approval that their product will perform as anyone would expect a modern firewall to perform. To aid you in selecting a firewall, after reading this chapter you should also check out the *Firewall Buyers' Guide* produced by ICSA Labs (www.trusecure.com/cgi-bin/download.cgi?ESCD=W0048&file=doc594.pdf).

A firewall has to do more than just protect a secure network from a less-secure network. If a firewall only needed to do that, couldn't you just cut the cable connecting the two networks? That would protect the secure network from any computer that couldn't lob nuclear missiles. Firewalls need to allow computers from the secure side to access information on the public side: "Packets get

out but they don't get in." All firewalls must allow access to the outside world. Conceivably, this would include full, unfettered access, which some firewalls do provide, but the ICSA 4.0 criteria only test firewalls against the following services: Telnet, Active and Passive FTP, HTTP, HTTPS, SMTP, DNS, POP3, and IMAP. Unless allowed by a security rule, a firewall needs to prevent all access into the network from the outside world.

Security Rules

Every firewall processes traffic based on an ordered set of rules. These rules could be considered the heart of the firewall. A body of security rules specifies not only what can come into a site but also what is allowed to leave a site. Most people would think that a proper security policy concentrates only on what can come into a site. Most network administrators trust their internal networks, so they usually don't consider outgoing traffic a problem. Unfortunately, that assumption is exactly what has made worms such as SQL Slammer, mass-mailing viruses like Melissa, and other malicious traffic possible.

A proper set of security rules should consider what type of traffic needs to leave the organization. A common security policy allows all outbound traffic to be permitted. The reason is simple—at 3 A.M. when configuring the firewall, the last thing you want to do is guess at what services to which your users are going to want access. Sure, it's easy to assume that they will want Web access (outbound HTTP and HTTPS), but what else? Do you want to make a rule for every flavor of instant messaging program that lives on your users' desktops? Certainly not. Therefore, we just allow all forms of traffic outbound and call it a night.

Unfortunately, this means that you've not only allowed legitimate traffic (such as Web browsing and FTP downloads), you also open your network up to Trojan programs. Malicious code writers know that most companies allow everything out, so they create their evil programs and hide them in pretty screen savers. Your users download and execute the screen saver, and in the background, the Trojan program starts up. To communicate back to the author, it starts an outbound session from your network to his machine. Since everything was allowed, the peculiar traffic destined for port 31337 isn't stopped by the firewall because it is traveling *from* the trusted internal network to the *untrusted* external network.

A much better plan would be to follow the "most restrictive" strategy: allow only what your users need and block everything else by default. This *will* result in more phone calls to your helpdesk, but it is the most secure method of operating. Start out with only allowing common outbound services: DNS, FTP, HTTP, and

HTTPS. When a request comes in for additional access (for example, outbound on port 5190 for ICQ chat services), evaluate the request in a business context and determine whether it should be allowed. Document the requestor and his stated purpose for the added access. Then, determine if you would be better served opening up this access to all users (if it's a common request) or just for this user.

This strategy is not limited to user workstations, however. For example, why should your corporate Web server need to access other external Web servers? HTTP traffic on Transmission Control Protocol (TCP) port 80 coming from your Web server and headed toward the Internet could be an indication of an infected host. Some worms (in particular, Code Red and NIMDA) spread by having one Web server contact other Web servers and attempt to infect these foreign targets. A firewall rule that only allows the corporate Web server to respond to Web requests, but not initiate any of its own, would prevent such a problem.

Notes from the Underground...

Outbound 31337 Is Not Very Elite

In August 1998 (yes, ancient by Internet calendars), the smart folks over at the Cult of the Dead Cow group (some would call them hackers) created "Back Orifice," a Trojan program that allows remote attackers to control a victim's machine. Borrowing its name from the Microsoft Windows BackOffice suite of applications, Back Orifice is installed on a machine after it has been compromised, leaving the attacker with back-door access at some point in the future. While the listening port is configurable, many amateur attackers leave the default port of TCP 31337 running. Upon hearing this, one can easily draw the conclusion that any inbound traffic on TCP 31337 showing up in IDS logs is malicious in nature (either someone probing for Back Orifice or someone using Back Orifice). However, this is still reactionary—looking at logs of a problem and taking action (hopefully) after the machine is infected.

The question that sage firewall admins should be asking is, "Does our corporate Web server have *any* reason to be communicating outbound on port 31337? For that matter, does it have any business communicating outbound from any ports other than TCP 80 and 443?" Construct your firewall rules such that Web servers are only allowed specific outbound ports on which to communicate. This will give you an important layer of

Continued

defense should your server fall victim to Back Orifice. And, for those who are curious but haven't figured it out yet, 31337 was picked because if you stare at the numbers long enough (and change 3 to "e," 1 to "l," and 7 to "t"), it spells out the word *elite*, a common term of distinction among the hacker community.

Hardware or Software

Firewalls usually take the form of either a computer running a common operating system (OS) with the firewall software installed on top, or a purpose-built hardware appliance that the manufacturer intended as a firewall from the ground up. Those that fall into the latter category either run on pre-hardened versions of a common, general-purpose OS (such as NetBSD or Solaris), or they run a customized, real-time OS that was only intended to run the firewall. Table 3.1 introduces the major vendors and where their products line up in the marketplace.

Table 3.1 Firewall Vendors and Types

Firewall Vendor	Form	OS
3Com Corporation & SonicWALL	Hardware	Custom
Check Point Software Technologies	Both	Windows, Solaris, IPSO
Cisco Systems, Inc.	Hardware	Custom
CyberGuard	Hardware	Custom
Microsoft	Software	Windows 2000 Server
NetScreen	Hardware	Custom
Novell	Software	NetWare
Secure Computing	Hardware	Custom
Stonesoft, Inc.	Software	Linux
Symantec Corporation	Software	Windows, Solaris
WatchGuard Technologies, Inc.	Hardware	Custom

Microsoft ISA Server and Symantec Enterprise Firewall fall into the software category, while the Cisco PIX firewalls fall into the hardware appliance category. Interestingly enough, Check Point FireWall-1 falls into both categories: it can be installed on a common OS (Solaris or Windows), but through a partnership with Nokia, most Check Point firewalls actually run on Nokia IPSO appliances.

The vendors that do run as pure software installed on a common, general-purpose OS usually employ some form of hardening process so that hackers do not

compromise the security of the underlying OS. Rather than try to subvert the firewall, they could just attack the OS that is hosting the firewall and cause that machine to route packets before the firewall sees them, or just obtain a remote terminal session with the desktop and change the security policy altogether.

Axent Raptor, the predecessor to Symantec's Enterprise Firewall, runs a service called "Vulture" to kill any rogue processes (such as viruses, Trojans, or other malicious applications) that attempt to start. Rather than lock the Windows OS down such that outside programs can't infect the server, the Vulture "watchdog" process just makes sure that no new processes start up once the firewall is installed. Similarly, Novell's BorderManager, which runs on NetWare, requires a special version of the NetWare core SERVER.EXE file to prevent access to the console before authenticating to the machine.

Manufacturers that specialize in hardware appliances will often flaunt the security holes in general-purpose OS as a weakness of products that run on those platforms. Furthermore, they'll usually state that hardware appliances have better security since the firmware that runs them has no other function. The argument seems to make sense, but it doesn't cover every situation. Check Point Firewall-1 and Symantec Enterprise Firewall easily exceed the minimum ICSA requirements, while numerous hardware appliances have needed firmware upgrades to fix security holes. Therefore, you cannot make a judgment about a firewall's security based mainly on this one aspect. You do, however, need to know into which category your firewall falls because each type presents a different challenge to hackers.

In the end, the decision of which firewall type to use is more of a personal preference. You should select your firewall according primarily to which features you need. Only as a secondary or tertiary criteria should you consider the delivery format—hardware or software. For many, us included, the ease of a plug-and-play hardware appliance is very attractive. If something goes wrong, just slide in a new appliance and off you go. Others might not want to pay the extra money for a purpose-built custom appliance, and instead would like to repurpose some of their old servers that can be converted to use as a firewall. Depending on your organization and the budget you have for your firewall, you will naturally gravitate to either the hardware (more expensive, usually higher performance) or software (able to repurpose old hardware at substantial savings) types of firewall.

Administrative Interfaces

For the most part, any firewall will not work the way you need it to for your individual organization straight out of the box. Firewalls are not a “one size fits all” solution; each firewall requires individual tinkering and tweaking so that it fits your needs. Therefore, all firewalls require an administrative interface to make these changes to their configuration and security policies. Administrative interfaces can take many forms. Hardware appliances can use a simple serial connection for the initial setup and then allow the user to switch to Telnet or a graphical user interface (GUI) installed on an administrative machine. The GUI could be a proprietary application or an open standard, such as a Web browser. Software firewalls will typically have an interface directly on the machine, but many also allow for remote access configuration. (See Figures 3.1 through 3.4.)

Figure 3.1 Initial Serial Connection

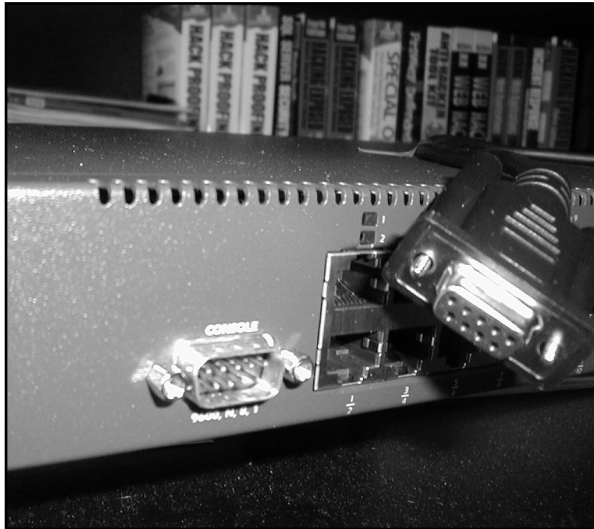


Figure 3.2 SonicWALL Administrative GUI Using a Web Browser

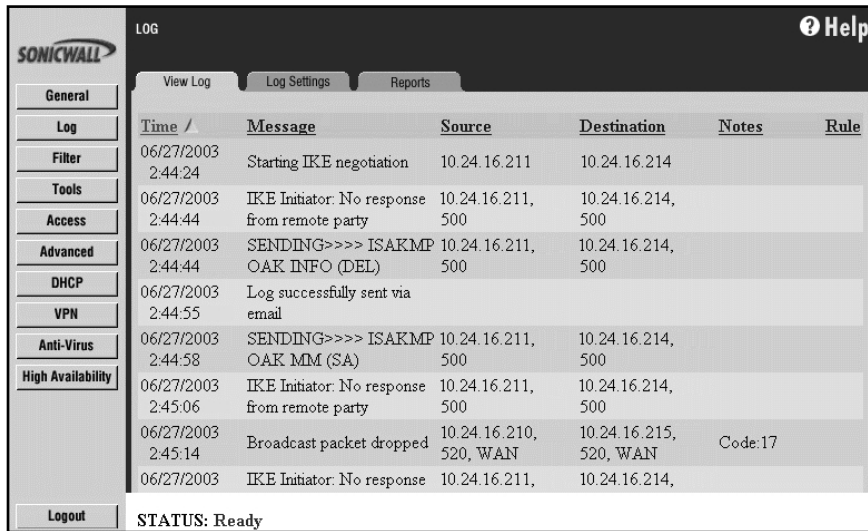


Figure 3.3 Cisco PIX Administrative GUI Using a Java Web Applet

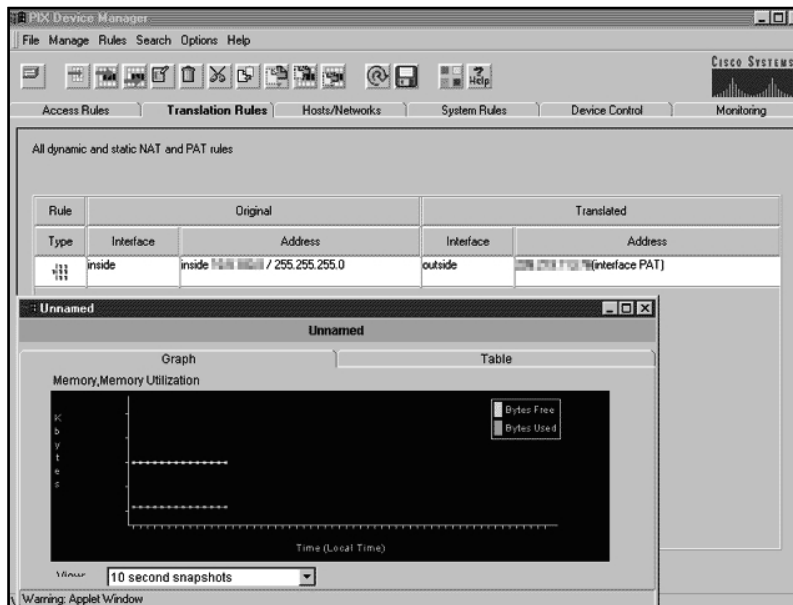
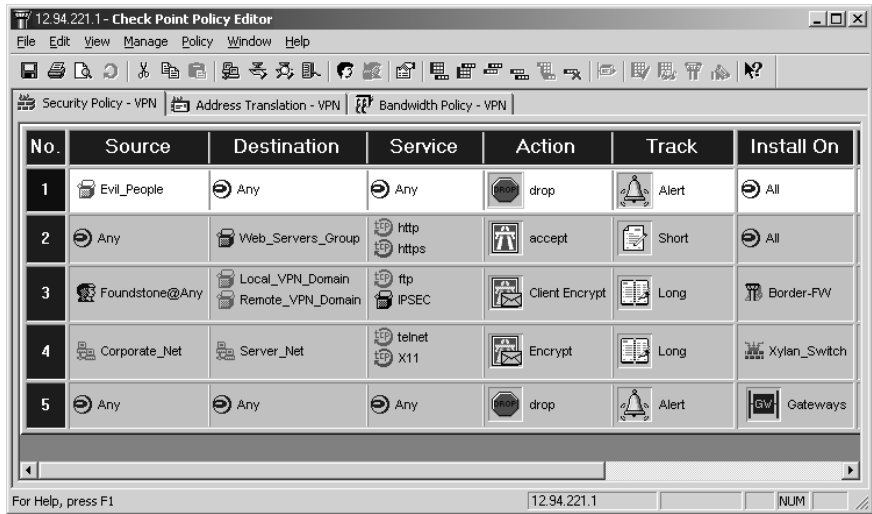
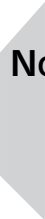


Figure 3.4 Check Point Firewall-1 Administrative GUI Using Proprietary Application



Since the administrative interface allows the user to configure the firewall, this feature needs special security to protect itself from hackers. All decent firewalls need at the very least an option to prevent reconfiguration of the firewall from an untrusted network. Better firewalls will allow for secure remote administration, such as through proprietary software or an open standard such as SSL. You must understand all remote access features of your firewall because hackers will often attack these first. We will look at the types of administrative interfaces for major firewall vendors later in this chapter.



NOTE

If you can easily change your firewall rules from outside your trusted network, a hacker might be able to do the same. Before enabling remote administration of your firewall, carefully weigh the risks versus the rewards. If you work 60 hours a week onsite, you probably have ample time to craft your security policies in the office, so you probably don't need remote administration. If you work as a consultant, administering dozens of networks for your customers, you probably couldn't do your job without it. Moreover, if you're not sure what you have to worry about with remote administration, keep reading...

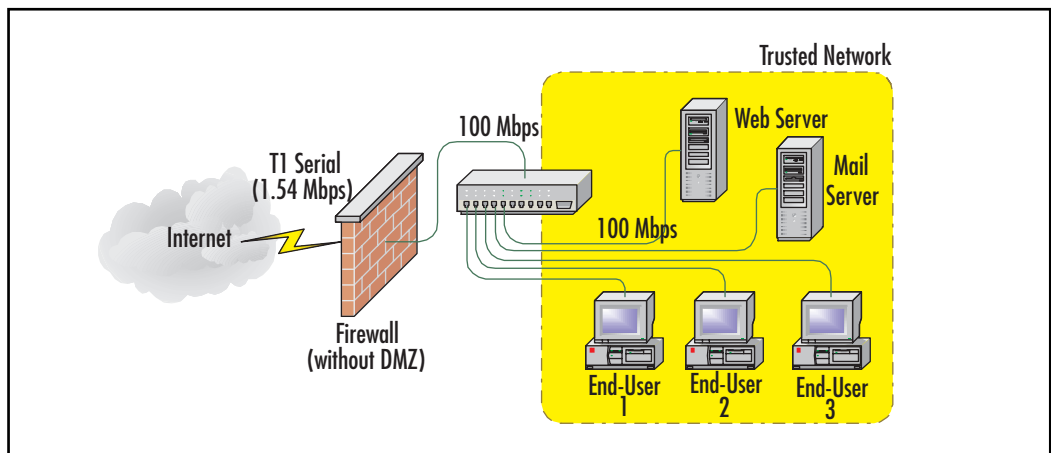
Traffic Interfaces

Firewalls protect resources by delineating what needs protecting versus from where the attacks could come. Many people refer to this as “us” versus “them.” Firewalls usually do this by acting as a highly selective router between the trusted network that needs protecting and the untrusted network full of potential hackers. Standard routers can add a great deal of latency to a network, so a firewall could make this worse. Firewalls work with complex rule sets that require fast processors and fast connections. Network administrators need to make sure that the firewall they choose can process information quickly enough to keep up with their network. Many firewalls now have 100 Mbps interfaces, so network administrators often assume that their firewalls can pass traffic that quickly. In most cases, this simply isn’t true. Fortunately, most networks probably don’t need a firewall that moves traffic that quickly.

DMZ Interfaces

Network engineers often speak of a network gray area called the “demilitarized zone,” or DMZ. The DMZ contains resources that need protecting from the outside world but from which the majority of the inside world needs protecting. For example, a company that hosts its Web server onsite needs to allow traffic from the outside world into the Web server. A typical setup will look something like Figure 3.5.

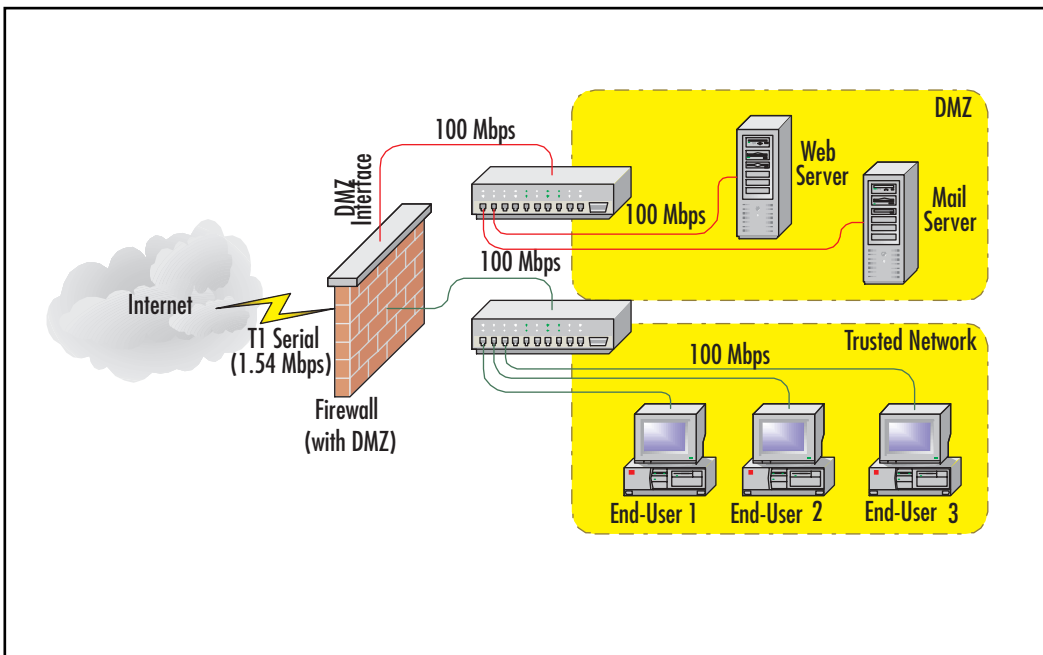
Figure 3.5 Firewall without a DMZ



At a minimum, the firewall needs to pass Hypertext Transfer Protocol (HTTP) traffic on TCP port 80. However, what happens when a security hole in the operating system allows a hacker to take control of the Web server through traffic sent as a Web request? Once this happens, the hacker can then use the Web server as a stage to mount an attack against the rest of the network. If we re-examine Figure 3.5, we immediately see that the Web server sits on the trusted network. The firewall cannot protect any of the workstations from the Web server, so once the hacker controls the Web server, all of the attacks come from inside the protected network.

Let's compare this to Figure 3.6. Here, the firewall has a DMZ interface for the Web server so that the Web server is not on the same network as the workstations. Since all traffic from the Web server to the trusted network must travel through the firewall, the network administrator can set up security policies to prevent a rogue machine in the DMZ from compromising the entire network.

Figure 3.6 Firewall with DMZ



Now, speed becomes an issue. In Figure 3.5, the firewall could only accept traffic to and from the Internet at T1 speeds (1.54 Mbps). Most decent firewalls can handle this amount of traffic without slowing the network. However, in

Figure 3.6, the workstations must go through the firewall to get to the Web server, just as the computers from the Internet. However, unlike the Internet, the path from the trusted network to the Web server use only 100 Mbps links. This presents a network design challenge.

Need for Speed

Almost any firewall will pass the traffic, but only the better firewalls will do it without significantly compromising the speed. Does your network need this much speed? Can your CFO afford this much speed? This is the challenge. Of course, even the best firewall will introduce latency to the network. What if your network needs even more speed than the best firewall can achieve, but you still want a DMZ? Some switch vendors produce equipment that can do multilayer switching (MLS), which you can use to create DMZs that need more speed than security policy flexibility. We'll take a look at these closer in Chapter 7, "Network Switching."

Additional Interfaces

Not all firewalls have the capacity to create a DMZ, while for others the DMZ is not a singular entity. Some firewalls have more than three interfaces allowing for multiple DMZs. Software firewalls usually have an advantage here since most of these are built on computers that can easily accommodate additional network interface cards (NICs), which the firewall turns into the various networks (Figure 3.7). Some firewalls also include an auxiliary port (Cisco even names theirs "AUX") for plain old modem or ISDN backup in case the primary interfaces die.

Figure 3.7 WatchGuard Firebox X1000 Integrated Security Appliance, Showing Multiple DMZ Interfaces



Logging

All firewalls need to keep track of what they see happening on the network. Without a log, an administrator would have little warning of an attack in progress. Low-end firewalls will only log security exceptions and don't have the capacity to keep the logs for an extended period of time. High-end firewalls generally have richer logging features that show both potential problems and usage trends. These enhanced logs can also track the traffic leaving your site. Beyond just security, these logs can give you an idea of how much of your bandwidth is being used, who's using it, and when. These statistics can help you in your next budget meeting with the CFO when you want to ask for a faster connection to the Internet.

Damage & Defense...

You Can't Just Track the Inbound Traffic

Most network administrators take a quick look at the logs to check for hacking attempts, and then ignore them, never realizing that they should also track what leaves the company. Believe it or not, not everyone at work works all of the time—say it ain't so! Santa didn't install the Christmas Light desktop decorations and his little helpers didn't download Elf bowling by themselves. These things might merely annoy you, but some employees take a big step past this and actually commit cyber crimes from within your network. When the police, or the lawyers, or the police with lawyers trace this back, they'll probably only know that it came from your network. Then, they'll eventually come to you to trace it to the real perpetrator. If your firewall tracks this activity, you can easily feed the right person to the wolves and the company can put the whole sordid mess behind it. If your firewall doesn't track this information—and you were overlooked for a promotion last year—you can always just point the authorities at your boss and solve two problems at once!

Optional Features

Just about every firewall has the previous features, but the following optional categories help to differentiate the products:

- Network Address Translation
- Port Address Translation
- Advanced routing
- Point to Point Protocol over Ethernet
- Dynamic Host Configuration Protocol Client and Server
- Virtual private networks
- Clustering and high availability
- URL filtering
- Content filtering
- Antivirus protection

When buying a firewall, nothing substitutes for security, but with all other things being equal, the extras can tip the balance.

Network Address

Translation and Port Address Translation

Every machine that communicates across the Internet needs a unique Internet Protocol (IP) address—or so the story goes. Engineers started noticing that even though a 32-bit address space creates up to 4,294,967,294 ($2^{32} - 2$) usable IP addresses, many of these addresses get wasted by organizations taking huge blocks that they barely use. As a result, the rulers of the Internet foresaw a time when we would run out of IP addresses and have to abandon IPv4 (which we all know and love) for IPv6, with a much greater capacity for addresses. In the short term, the Internet Engineering Task Force (IETF) established what eventually evolved into Request For Comment (RFC) 1918.

RFC 1918 (<ftp://ftp.rfc-editor.org/in-notes/rfc1918.txt>) specifies which IP addresses network administrators can use privately. These addresses allow companies to give each of their machines a unique IP address within the company without having to pay for them and without having to worry about conflicting with another machine at another company. The addresses don't conflict because,

as per RFC 1918, Internet routers do not route these IP addresses. Therefore, these IP addresses work fine for companies internally, but they do not allow users to access information on the Internet.

Notes from the Underground...

1918: A Year to Remember?

An important reason to remember RFC 1918 is the near ubiquity with which it is used in internal networks. As you can see from Table 3.2, RFC 1918 provides more than enough address space for even the largest organizations to uniquely identify every network device on their internal network.

Table 3.2 RFC 1918 Private Address Space

IP Address Range	Number of Usable Hosts	Number of Class C Subnets
10.0.0.0–10.255.255.255	16,777,214	65,536
172.16.0.0–172.31.255.255	1,048,574	4,096
192.168.0.0–192.168.255.255	65,534	256

Most people select the 10.0.0.0 network for the simplicity of the numbers involved (it’s much easier to remember your corporate IP address space as being “ten-dot-something” instead of “one-nine-two-dot-one-six-eight-dot-something”). However, most organizations never even dream of having more than 16 million network devices. Most home users will recognize the 192.168.0.0 address space because it is most often used with SOHO routers and firewalls.

So, you have RFC 1918 private addresses on your internal hosts, but we just said that these special addresses are not allowed on the Internet. So, how do we convert from private to public address space? Network Address Translation (NAT) solves this by proxying the internal requests for Internet services using a registered public address (or addresses) controlled by the device performing NAT. In short, NAT allows all of the private addresses to act as public addresses for

outgoing requests. Since the Internet does not route private addresses, this also adds a layer of security to the workstations since the Internet community never sees the true IP address of the workstations. If a hacker tries to access a NATed workstation using the reported public IP address, the hacker merely attacks the device doing the NATing, which, in the case of firewalls, is designed to withstand these attacks.

Private addresses may add security because no one can route to them, but this would also prevent users from accessing Web servers behind a firewall. NAT takes this into account and can map a public address back to a private address if necessary. In the case of a Web server, an administrator would probably only want to accept HTTP traffic for a Web server not running Secure Sockets Layer (SSL). In this case, only TCP port 80 would get mapped. Many vendors refer to this as *Port Address Translation* (PAT) instead of NAT.

Tools & Traps...

Creative IP Addressing with RFC 1918

You could just take the RFC 1918 private address space at face value and start handing out addresses with the first available one, and continue from there. A much more effective IP addressing schema would be to use the flexibility that all those extra IP addresses provides. For most of our customer networks that we design, we usually set aside distinct class C subnet “chunks” to represent different classes of network devices. For example, 172.16.x.x could represent your Los Angeles office, and 172.17.x.x could be New York, and so on. Further breaking down the network into “purpose” classes can help administration as well. For example, x.x.0.x can be networking devices such as routers, x.x.8.x can be servers, x.x.16.x can be peripherals like network printers or copiers, and x.x.32.x can be the average user range. The value comes in later during log analysis. If you get an alert from your SNMP management console (see Chapter 12, “Secure Network Management” for more information), you can instantly tell that a brute-force password attempt coming from 172.17.32.14 is a user workstation in your New York office, and that a high amount of outbound SMTP traffic from any network other than your Los Angeles mail server at 172.16.8.11 should be investigated.

Advanced Routing

Most firewalls also need to act as routers since they usually connect at least two different subnets. A simple network can set up all of the routers to use static routing tables, but a large network needs more flexibility. Since the firewall works as a router, the firewall might also need to run routing protocols such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) just as the rest of the networking equipment does. Not all firewalls do this, so if you need this feature, check the specifications carefully.

NOTE

For more information on routing tables and routing protocols, refer to Chapter 5, "Routing Devices and Protocols."

Point to Point Protocol over Ethernet (PPPoE)

Telecommunication providers at the consumer level use PPPoE on Digital Subscriber Line (DSL) broadband connections to force their broadband customers to authenticate their connections as though they're using a dial-up connection. This allows the regional telecommunication providers to only allocate the IP address as a station needs it. This works great for the phone company, but for consumers it's just one more thing to go wrong. Often, firewalls connect directly into the telecommunication provider's DSL modem, which means that the firewall must have PPPoE capabilities for the connection to work.

Fortunately, most business-class DSL services do not use PPPoE, so you probably won't see this in most offices. As for residential broadband, if the DSL provider in your area uses PPPoE, check to see if you can get a cable modem in your area, since those never use PPPoE and the speed is usually as good or better than DSL.

Dynamic Host Configuration Protocol (DHCP) Client and Server

DHCP allows machines to automatically get IP addresses or assign addresses, depending on whether the machine acts as a client or a server. Most firewalls today can do both simultaneously, although from different interfaces. If a site gets

a dynamic address from the ISP, the firewall will need to act as a DHCP client on the outside interface. To ease configuration on the inside equipment, many firewalls can dole out private addresses on the inside interface. This can make for easy configurations since the firewall can then dispense information that it gleaned from connecting to the Internet, such as Domain Name Services (DNS) servers, to the machines on the trusted network. Administrators at large networks probably have another machine doing this already (perhaps even one integrated with your Microsoft Active Directory), but smaller networks might need this. Note too, that DHCP does provide a slight information security risk in the ease in which an attacker can receive valuable reconnaissance information about your network. However, each company's individual security policy must balance the ease of use with protection of IP addressing information.

Virtual Private Networks

Virtual private networks (VPNs) allow remote users or remote sites to connect to each other securely over the Internet. In the beginning, companies rolled out VPNs for employees who wanted to work from home, but they still connected remote offices to each other through expensive WAN links, such as point-to-point T1s. Today's VPNs can create secure tunnels to each other using relatively inexpensive links to the Internet instead of paying for a dedicated link between offices.

Some companies produce VPNs as separate products from their firewalls and recommend running these devices in parallel or behind a firewall. These vendors usually recommend removing the VPN functions from the firewall due to the processor-intensive nature of the VPN connections. This makes sense in some situations, but current high-end firewalls have enough processing power to handle both functions. Generally, a firewall with a built-in VPN costs less than a comparable firewall without VPN capabilities and a separate VPN. In addition, it usually takes less effort to configure and maintain one box instead of two.

Clustering and High Availability

Most administrators have heard of clustering servers, but not everyone has heard of clustering firewalls. Any network is only as resilient as its weakest link. Most networks lose access to the Internet when the firewall dies, which might inconvenience many companies, but won't kill the business if it doesn't come up for a few hours. However, if your business involves a Web site taking credit card orders, every minute that customers can't see the site costs your company money. You might have "five nines" uptime on your servers, but—proverbially—if a server falls in the

woods with no one around to hear it, will your company have enough cash for your paycheck to clear?

Clustering firewalls allows for a hot-standby firewall to take up the slack if one dies. In some advanced setups, multiple firewalls can load balance, and if any one firewall dies, the remaining firewalls take up the slack. Most times, firewalls are mirrored in an “HA” or *high availability* setup, where one firewall is the “active” member (passing traffic) and the other is the “standby” member waiting in the wings. We cover this topic more later in the section *Stateful Failover*.

URL Filtering, Content Filtering, and Antivirus Protection

Most firewalls can block simple Universal Resource Locators (URLs), but most cannot block specific content or even recognize viruses. Many firewalls, however, have third-party support for companies that compile databases of Web sites and then categorize the sites (WebSense and SurfControl, to name just two).

Administrators can then subscribe to this service and download the lists to the firewall. Once the firewall has these lists, the administrator can then determine the type of content permissible for viewing. Usual categories include sexually explicit material, hate sites, gambling, drug use, and things of that nature. High-end firewalls will often allow the administrator to match the content rules to specific workstations based on an IP address, but even better firewalls (or third-party applications) will take this a step further and integrate this information into the company’s directory (for example, Microsoft’s Active Directory or Novell’s eDirectory) and allow the administrator to make exceptions based on users rather than computers.

Notes from the Underground...

Think about the Children

Many network administrators consider inappropriate content a social problem and not a technological one. Everyone's an adult here, so what's the harm? However, if you run a school network, now you have kids accessing the Internet, so everything changes. Some schools will cry poverty and claim that they can't afford filtering software, but the reality is that the poorest schools qualify for Federal subsidies (E-rate) for Internet access. One caveat is, though, that the site must have filtering software installed as per the Children's Internet Protection Act (CIPA), www.sl.universalservice.org/reference/CIPA.asp. For a coherent explanation of E-rate, see www.kelloggllc.com/erate/primer_02.pdf.

Better firewalls will also allow administrators to subscribe to third-party products that scan all traffic for viruses and hostile applets and then kill them before they ever reach the users. Even if you have antivirus protection on the machines, it doesn't hurt to eradicate these bugs before they ever hit your network.

Exploring Stateful Packet Firewalls

Quite possibly, the most underrated feature among modern firewalls is their capability to be "stateful" with their routing and pass/drop decisions. In other words, modern firewalls are able to ascertain if a transmission is in response to a request that originated on the trusted network, or a transmission that originated on the scary "outside" network. This might sound simple since this is what we expect from our firewalls when we write in our security policy "must allow outbound connections but no inbound connections." In reality, what we are asking our firewalls to do is to "allow all outbound connections, allow all inbound responses to those outbound connections, and block all other inbound attempts."

What Is a Stateless Firewall?

Any conversation on stateful firewalls should really begin with a look at how bad it really could be: stateless firewalls. Although you won't find anyone selling a

stateless firewall, it does exist as a concept. Basically, it would involve a very literal interpretation to your security policy without much “business logic” to make the device perform adequately. In essence, a stateless firewall would do “what you told it to do and nothing more,” when what you really want is a firewall that will “do what I mean, not what I say.”

For an example of a stateless firewall, imagine a router that is being forced to perform firewall-like functions. The following example uses notation that appears alarmingly similar to Cisco IOS, but it is purely for illustration. In Cisco’s defense, their routers (with the appropriate Firewall Feature Set) include the Adaptive Security Algorithm (ASA), which allows them to operate more securely than the following demonstration. Let’s start with a basic security policy for Company XYZ:

```
10. permit outbound from 172.17.0.0/16 on any_port to any_ip on any_port
20. permit inbound from any_ip on any_port to host 172.17.8.11 on smtp
30. permit inbound from any_ip on any_port to host 172.17.8.13 on http
40. deny all
```

Pretty basic—we have two rules to allow Web and e-mail to flow to our servers, we have the obligatory *deny all* statement for completeness at the end, and we have the rule to allow outbound connections from our network to foreign locations on the Internet. We’ve even gone so far as to practice good security policies by specifying the source network (172.17.x.x) where our internal hosts are coming from. So, why can’t the CEO get to eBay? A quick peek at the firewall log gives us a clue:

```
12:01:14 src=172.17.32.142:1025 dst=4.2.2.2:53 action=PASS rule=10
12:01:15 src=4.2.2.2:53 dst=172.17.32.142:1025 action=DROP rule=40
12:01:16 src=172.17.32.142:1025 dst=4.2.2.2:53 action=PASS rule=10
12:01:17 src=4.2.2.2:53 dst=172.17.32.142:1025 action=DROP rule=40
```

Right away we can see that to get to www.eBay.com, his machine must first do a lookup on his ISP-provided DNS server (4.2.2.2, the Genuity DNS server with the most memorable IP address ever). When the DNS server attempts to respond, the firewall is dropping the packets. Therefore, we add this rule, just above rule 20:

```
19. permit inbound from any_ip on dns to 172.17.0.0/16 on any_port
```

Now, we head over to the CEO, confident in our abilities, and ask him to try it again. Still nothing. Now the CEO is getting steamed because the auction close is coming soon, and he needs a new leather laptop bag. Back to the firewall log:

```
12:08:21 src=172.17.32.142:1027 dst=4.2.2.2:53 action=PASS rule=10
12:08:22 src=4.2.2.2:53 dst=172.17.32.142:1027 action=PASS rule=19
12:08:23 src=172.17.32.142:1027 dst=66.135.208.101:80 action=PASS rule=10
12:08:24 src=66.135.208.101:80 dst=172.17.32.142:1027 action=DROP rule=40
```

We forgot to allow for Web traffic to respond back. With little time to spare, you react without thinking and add another ill-conceived *permit* statement to your access list, and another, and another, until the CEO is able to bid on his item and chat with his daughter on AOL Instant Messenger:

```
16. permit inbound from any_ip on http to 172.17.0.0/16 on any_port
17. permit inbound from any_ip on https to 172.17.0.0/16 on any_port
18. permit inbound from any_ip on 5190 to 172.17.0.0/16 on any_port
```

The CEO is happy, you're happy, and you go home feeling on top of the world. Later that night, the 13-year-old in southern Yemen who just got infected with the latest HTTP-borne worm leaves his computer on while he goes to school. The worm sends packets to your network, infects your Accounting server, infects your CEO's computer, and manages to transmit sensitive documents across e-mail to a hacker in Western Fraudikstan, just outside Moscow. Let's watch that again, in slow motion:

```
23:13:02 src=147.45.35.40:53 dst=172.17.32.142:139 action=PASS rule=19
23:13:03 src=147.45.35.40:80 dst=172.17.8.18:80 action=PASS rule=19
23:13:04 src=172.17.32.142:1034 dst=147.45.35.40:25 action=PASS rule=10
23:13:05 src=172.17.8.18:1026 dst=147.45.35.40:25 action=PASS rule=10
```

The rules you added were *too permissive* and while they did let in the responses to your CEO's Web requests, they also allowed packets that originated outside the firewall to walk right in. Since your outbound policy does not specify that workstations cannot transmit mail directly to the outside world (even though you have a corporate mail server), your trade secrets are now sitting in some evil-doers' Inbox. But what else are you to do? If only there was a way to keep track of the outbound conversations.

Keeping Track of Conversations

We've seen that allowing a broad selection of network traffic (such as HTTP inbound) is a really bad idea due to the security implications. If we instruct the router to keep track of packets (or more specifically, of *conversations*) that exit the network, we will be able to allow the response to those queries to enter the network. This is most commonly implemented in a *sessions table*. Sometimes referred to as a *state table*, this is the essence of “keeping state” of the conversations. This is what separates a simple packet filtering firewall/router from a stateful inspection firewall.

When network requests pass from the internal segment to the external segment, the firewall makes a note of the host that initiated the request, the target, and the corresponding ports (source and destination). Then, it alters the security policy just slightly to allow a “pinhole” entrance for the return traffic. Let's look at our previous example of our CEO attempting to reach eBay, but with a stateful firewall. This time, let's start with the original security policy:

```
10. permit outbound from 172.17.0.0/16 on any_port to any_ip on any_port
20. permit inbound from any_ip on any_port to host 172.17.8.11 on smtp
30. permit inbound from any_ip on any_port to host 172.17.8.13 on http
40. deny all
```

We are allowing everything outbound from our internal network and only allowing external access to our mail and Web server—looks good so far. Now let's watch as our CEO's laptop performs a DNS request to resolve www.eBay.com:

```
14:38:39 src=172.17.32.142:1025 dst=4.2.2.2:53 action=PASS rule=10
```

Upon seeing this traffic exit the router, an entry in the session table will be made, indicating that 172.17.32.142 has sent traffic to 4.2.2.2 on port 53. The result can best be visualized if we assume that the router quickly rewrites the security policy and inserts the following rule at the very top, before rule 10:

```
9. permit inbound from host 4.2.2.2 on dns to host 172.17.32.142 on 1025
```

This “pinhole” window in the security policy is what the DNS server needs to respond to the query. After the traffic passes through the router, from the outside to the internal segment, the rule is immediately deleted to prevent someone from piggybacking on that rule. The response comes back to the CEO's laptop and then a Web request goes out:

```
14:38:40 src=4.2.2.2:53 dst=172.17.32.142:1025 action=PASS rule=9
14:38:41 src=172.17.32.142:1027 dst=66.135.208.101:80 action=PASS rule=10
```

Again, the “pinhole” opens:

```
8. permit inbound from host 66.135.208.101 on http to host 172.17.32.142 on
1027
```

and the return traffic is able to come back in to your network:

```
14:38:43 src=66.135.208.101:80 dst=172.17.32.142:1027 action=PASS rule=8
```

What is most important to realize about this whole transaction is that no administrator intervention was needed to modify the security policy. The best part is that after the return Web traffic reached the laptop, the security policy is back to the original rule set with the pinhole permit statements removed:

```
8. <deleted>
9. <deleted>
10. permit outbound from 172.17.0.0/16 on any_port to any_ip on any_port
20. permit inbound from any_ip on any_port to host 172.17.8.11 on smtp
30. permit inbound from any_ip on any_port to host 172.17.8.13 on http
40. deny all
```

Too Much Chatter

This previous example of processing network traffic works great if you just have one host accessing external resources at any given time. What happens when multiple hosts try to reach external resources simultaneously? Well, the router or firewall must then store the requests in a First in First Out (FIFO) buffer and store more lines in the sessions table. Many modern firewalls can handle incredible amounts of simultaneous conversations measured in the maximum size of their sessions table. The higher-end firewalls have more memory and can store many more sessions than a SOHO firewall that perhaps is better suited for home networks of 10 or less machines.

When the number of sessions exceeds the memory available for the state table, the oldest session is dropped from the table and no longer tracked. This means that when the response to that particular request (perhaps the HTTP traffic back from a Web server) gets to the firewall/router, there will be no pinhole *permit* statement to allow that traffic through the firewall. Thus, the traffic will be dropped and the end user will experience a loss of connectivity.

Stateful Failover

In larger firewall deployments, high availability is mandatory, which means at a minimum, two firewalls in a mirrored configuration. As mentioned previously, you could also cluster firewalls (three or more) to balance the load of traffic across many firewalls. In either case, there needs to be a mechanism to determine when there is a failure in the system. In mirrored firewall configurations, a *heartbeat* function allows the standby firewall(s) to determine if there was a failure in the primary firewall. Most times, this is a simple one-packet “ping” to determine whether the other firewall is online.

If there is a lot of traffic going to the firewalls, there exists a possibility for this ping packet to be lost in the noise of regular traffic. Therefore, most heartbeat implementations will have a dedicated crossover cable between the mirrored pairs so that there is no chance of latency or dropped packets. This dedicated heartbeat network offers a nice secondary benefit: a high-speed data transfer method for state or session table information.

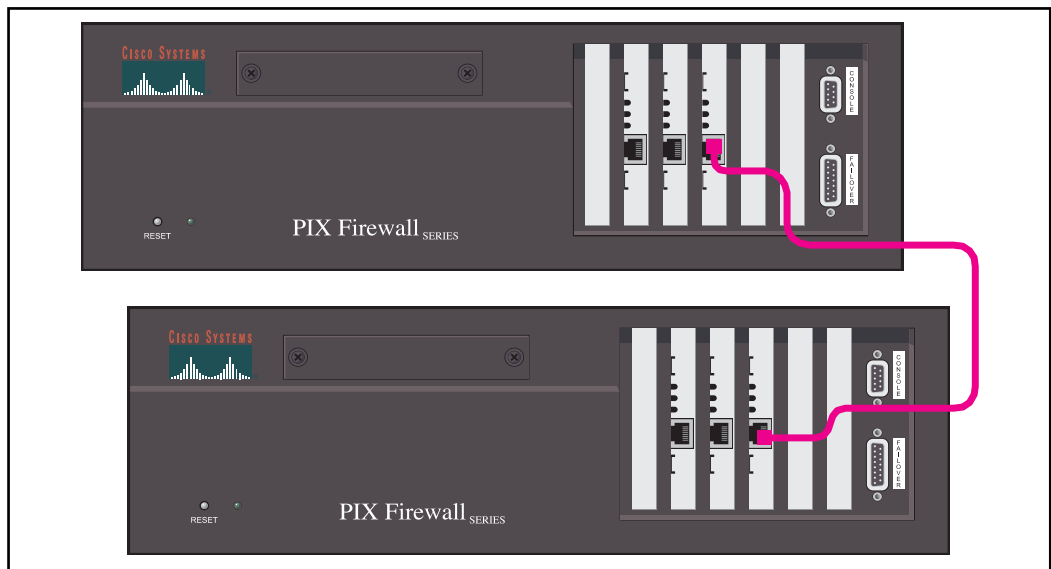
Even if a vendor claims that their firewall has failover capabilities, only the very best will offer *stateful failover*. The difference between the two is simple:

- Normal failover simply boots up the standby firewall when the primary is down.
- Stateful failover means that the session table and other operational information is transferred to the secondary firewall so that it can pick up exactly where the other firewall left off.

When stateful failover happens, the end user should not notice any difference. Many times, the only way to know that a stateful failover happened is by looking at the log file. In contrast, a stateless failover (or just a regular failover) will be noticed by LAN users because they will have a momentary loss of network connection (2 to 10 seconds) and might have to retry their most recent Web request or e-mail transmission. The reason is that in stateless failover, the newly activated firewall (the standby one) springs to life without any prior knowledge of active sessions. Therefore, when HTTP requests leave via the primary firewall, the failover happens, and then HTTP responses come in via the secondary firewall, they will appear to be unauthorized access attempts and will be blocked. If there were any VPN connections to the firewall from remote clients or from distant partner networks, these will have to be manually reestablished and a new key exchange will have to take place. This can introduce a level of latency or LAN-to-LAN VPN failure that is unacceptable to very integrated business partners.

In stateful failover, the newly activated firewall will have an up-to-the-second session table so it will be able to process that return HTTP traffic immediately. VPN sessions and key exchange information will also be preserved so no connections will be dropped. As stated previously, the easiest and most common way that firewall vendors implement this is via a dedicated cross-over cable, as illustrated in Figure 3.8. Part of the heartbeat process includes sending updates of the session table to the secondary firewall so it has a mostly updated table. When the primary reaches a fatal error and needs to shut down, it sends a copy of its routing table, session table, and other pertinent information over the dedicated link and then dies. In the case of a catastrophic failure (such as power failure) where the primary doesn't have a chance to send this last batch of information, at least the secondary firewall has a recent copy of the session table (perhaps 5 to 10 seconds old).

Figure 3.8 Wiring Diagram Showing Stateful Failover Heartbeat Cable between Two Cisco devices

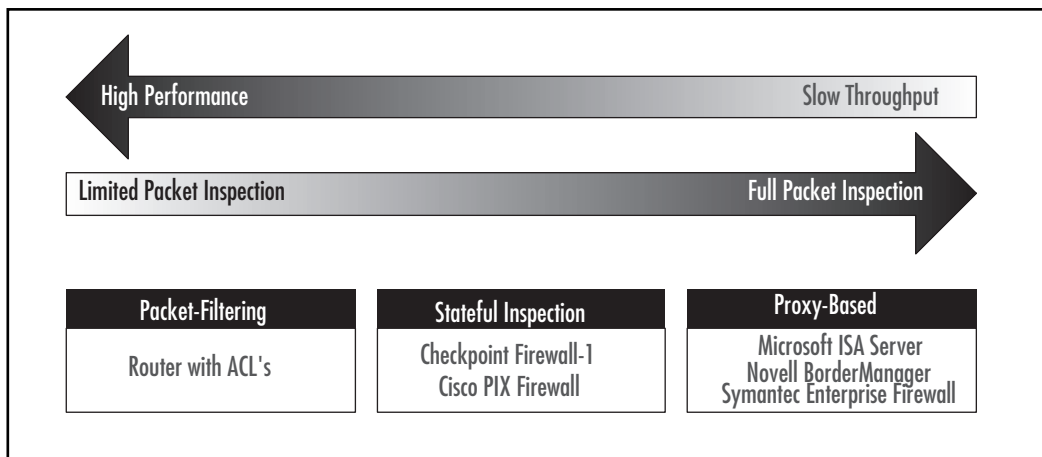


Explaining Proxy-Based Firewalls

Until now, we've discussed the firewalls that examine packets at the lower end of the OSI layers and make their forwarding decisions based on port, protocol, and session information. There exists an entirely separate class of firewall that makes decisions based on very high-level information provided by Layer 7, the application layer. This allows for a richer feature set but at the expense of performance.

A packet filtering firewall will be the best performance possible, but has limited use in today's networks (see the earlier stateless firewalls example). A stateful inspection firewall will always outperform a proxy firewall just based on the amount of work involved for each technology. However, which is better for your organization? Figure 3.9 gives an indication of the performance tradeoff when a firewall performs deep inspection into the upper OSI layers.

Figure 3.9 Tradeoff between Performance and Packet Inspection



Gophers

If you looked at network architecture in the early 1990s, you would find that the Internet still hadn't reached "critical mass" as a vital part of business. Some organizations didn't have an ISP and managed to turn a profit. The ones that did usually had a dial-up line connected to one machine appropriately called the gateway host. This machine would usually provide the e-mail exchange between your organization's private e-mail (something like the antiquated MS Mail or cc:Mail) and the Internet at large. Prior to Web sites, many research institutions, libraries, and universities ran *gopher* servers to provide information (aptly named both due to the action of "going for" the data, and because most gopher server

admins rarely saw the light of day). A gopher server was an efficient method of posting information about your organization in an organized manner. For universities and research institutions, the first inhabitants of the Internet, this was a great place to publish research documents or student theses. As time passed, people inside the LAN wanted access to these gopher servers, but obtaining Internet access for each computer became cost-prohibitive. There, the concept of an Internet proxy was born.

Software, such as Microsoft Proxy Server, would be installed on a dual-homed gateway machine and provide the link from the external network to the internal one. Requests from the inside network would be routed to the proxy. Then, the proxy would establish its own connection to the target gopher server. The response from the gopher server would be sent to the proxy and then the proxy would respond to the original LAN machine. What is very important to note here is that at no point in time are any internal machines (save the gateway machine) connected to the outside world.

Modernization: The Evolution of Gophers

Gopher servers have come and gone, but the Internet has only increased in importance to an organization. The original need for proxy servers has disappeared, but today's proxy-based firewalls are much like their predecessors. When a request comes in from the outside to deliver e-mail to a company's mail server, the proxy-based firewall will actually open another connection, sourced from itself, to the destination mail server. Once the TCP handshake is complete, it will proxy the connection by copying packets from one connection to the other. When the transmission is complete, the firewall will tear down both connections. Again, it is very important to note that at no time is the remote host ever connected to the company's mail server.

Some vendors will tell you that by definition this is more secure. Well, there is always something to be said for security by obscurity, but a malicious attack on a Web server using a Code Red type attack will still be successful if the firewall is copying all packets from one connection to the other. The only way a Code Red attack would be stopped prior to reaching the Web server would be for advanced packet inspection rules to peek into the upper layers of the Web request and note the offending URL string.

Since each packet must be processed at Layer 7, the top of the OSI reference model, the firewall has access to all the packet information. The downside is that processing each layer takes time, with more time taken in the higher layers

because data must be interpreted rather than just read; looking at an IP address to match a *permit* list is relatively trivial, but dissecting the parts of an HTTP request searching for a malformed *content-type* string is more CPU intensive. After the packet has been flagged as allowed traffic, it needs to be packaged in all seven layers into another connection. This explains the large performance difference between proxy and packet-filtering firewalls.

Explaining Packet Layers: An Analogy

Any discussion on the benefit of proxy-based firewalls and their ability to peer into the upper layers of a packet must include a definition of these layers. In the early 1980s, the International Standards Organization (www.iso.ch), headquartered in Geneva, Switzerland, designed their Basic Reference Model as part of their suite of networking standards known as Open Systems Interconnection (OSI). The reason why the 147 countries that the ISO represents wanted to define a standard was simple: many very different networking systems were starting to be developed and they needed to connect with one another. What the OSI Basic Reference Model (now known as the seven layers of OSI) provided was a common vocabulary of network transmission components across vendors and technologies. From its humble beginnings designed to enable large, clunky mainframes to talk with one another, the OSI layers still serve a valuable purpose today in explaining complex network communications with a logical abstraction. Every book on networking has a section on OSI—it's almost a law. However, rather than throw figures and tables out, a gastronomical analogy would work much better.

Chips n' Salsa

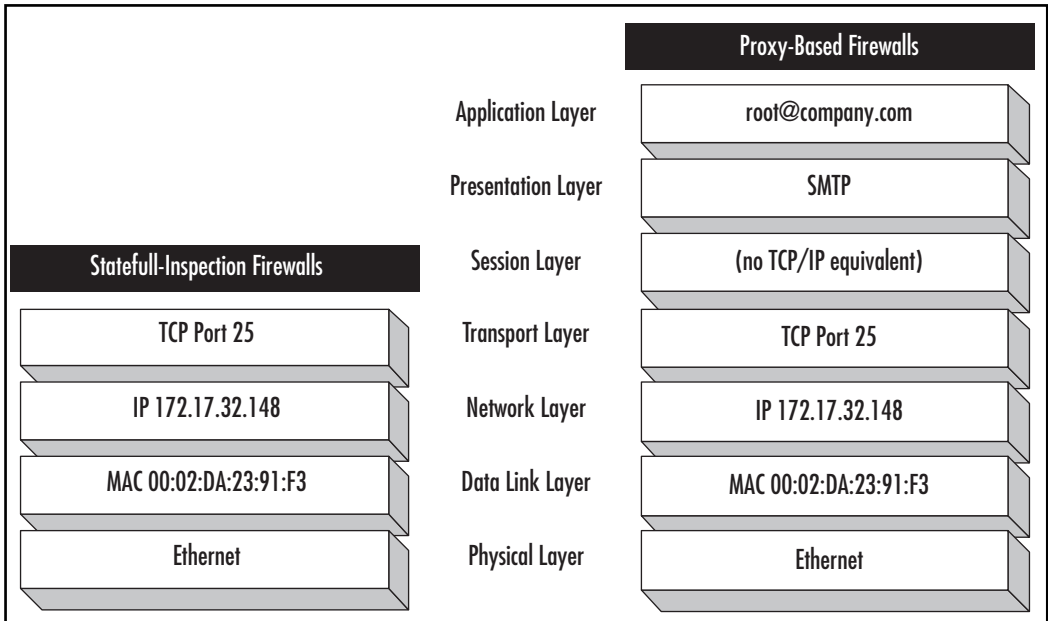
A Super Bowl party staple is the cacophony of calories that is known as the 7-Layer Dip. This melding of cheese, guacamole, sour cream, and other waist-expanding foods goes great on a chip and has—okay, bear with us here—a rich “feature set” of flavors. In one bite, you're able to examine all the ingredients (from the tortilla chip as the physical layer to the all-important presentation layer with the solitary sliced black olive) and how they interact with one another. This might seem entirely silly, but it does illustrate how proxy-based firewalls are given a lot more ingredients on which to base their forwarding decisions. Just as you can say that you will only enjoy a cheese layer if it is of the cheddar variety and only if the bite occurs on Super Bowl Sunday, you can also be very specific with proxy firewall rules: allow Web traffic but only if it is HTTPS and only on week-

ends. A packet-filtering firewall is just like salsa—gets the job done but just isn't as rich. Let's look at both methodologies.

Cheddar, American, Swiss, or Jack?

When it comes down to it, cheese is cheese, so who cares what variety is used in our favorite party snack? Well, the answer depends on your security policy. Perhaps your company has stated that it doesn't mind audio files being downloaded from the Internet, as long as they are WAV and not MP3. In this case, a packet-filtering firewall won't be able to help you because that information is stored in higher levels that are ignored. Figure 3.10 shows the layers involved in an e-mail transmission.

Figure 3.10 Comparing Packet Inspection between Firewall Types



In Figure 3.10, we see the same packet but from the point of view of both firewalls. In most cases, you can get away with just port and protocol information. However, what if we wanted to filter out all e-mail bound for root@company.com? We would have to examine Layer 7 to find out the recipient of the information. Perhaps you don't want anyone on the outside sending mail to the root account and want to avoid any possibility of a virus infecting that mail account; using a Layer 7 packet inspection rule would work quite nicely.

Mild or Extra Spicy?

Even the humble salsa has undergone a recent makeover. A decade ago, salsa came in “chunky” and “extra chunky” varieties. That seemed a little plain sitting on the coffee table next to the seven-layer dip. Now you have a salsa bar that ranges from mild, extra hot, low sodium, and chipotle blends. The same modernization can be seen in packet filtering firewalls.

The advanced high-level packet inspection that was a strong selling point for proxy-based firewalls has been incorporated into some packet-filtering software. While still fundamentally different from proxy firewalls, the added features do erode some of the advantage that proxy firewall vendors would like you to believe they have. This goes by many names (Stonesoft calls it Multi-Level Inspection, Symantec calls it Full Inspection), but in the end it means a hybrid that combines the speed of stateful inspection with very specific agents or application proxies that can be selectively enabled.

Employee Monitoring

One last perceived advantage of proxy-based firewalls is their capability to document the most visited Web sites and—since most proxies require some form of login—who is visiting which sites. This is the feature that usually makes the HR department salivate and the IT Director cringe.

Since the firewall itself is making the connection to these sites on behalf of the internal host, it can easily document the requestor’s username, the destination URL, and classify the content of the site using keyword searches or a database of naughty sites. All this information gets converted into a variety of graphs, charts, and reports of your choosing that can then be discussed at length during management meetings.

Just as we saw with the Layer 7 inspection features, packet-filtering vendors have stepped up to the plate and incorporated some of the proxy-based firewall features in their software. Modern packet-filtering firewalls can use plug-ins such as WebSense and SurfControl to determine inappropriate Web site access. Rather than worrying about the URLs, the firewall will ask the URL filter for permission before completing any outbound HTTP request. These third-party filters are updated on a weekly or daily basis and can offer detailed reporting just as well as their proxy-based counterparts can. Using integration plug-ins between DHCP servers and Microsoft Active Directory or Novell NDS Directory Service, these filters can also correlate a username with a source IP address to document who is

visiting the inappropriate sites. Moreover, the user isn't forced to authenticate using yet another username/password. The final decision on proxy versus packet-filtering firewalls rests within your security policy and an informed balance between features and performance.

Examining Various Firewall Vendors

Armed with a thorough overview of what goes into a firewall and the different types of firewalls, the only thing left to do is to select the right one for your needs. Before examining the field from which to choose, you should write down what the “must have” features are for your organization and not get distracted by extra bells and whistles that might be helpful but not necessary. By no means is this an exhaustive list of firewall vendors, but it does represent the majority of products out there.

3Com Corporation and SonicWALL, Inc.

3Com and SonicWALL have similar product offerings; many of the 3Com small office firewalls are really SonicWALL devices that have been re-branded as 3Com products through a partnership agreement. Solid performers, they all have support for VPN tunnels in the same hardware (with the use of an unlocking license code). The Web-based user interface really takes the guesswork out of a complex task like setting up IP Security (IPSec) tunnels, Internet Key Exchange (IKE), and Internet Security Association and Key Management Protocol (ISAKMP) settings. Web filtering is also provided in the same box, which makes this a very compelling choice for small offices that cannot afford a more robust external URL filter. A yearly subscription is required, but updates are downloaded to the firewall weekly and violations to the content filter can be sent via e-mail to an administrator.

One unique offering from 3Com that really brings the concept of “defense in depth” to the market is their Firewall Desktop PCI Card (model 3CRFW200, also available in PCMCIA versions). This allows you to deploy a strong hardware firewall on all of your critical servers without taking any valuable rack space or altering your network infrastructure. Since the OS recognizes the card as just another network card, compatibility is not an issue. All the cards are managed centrally by a Firewall Policy Server to ease administration. The best part is that no “wandering hands” in the data center can accidentally subvert this firewall because it is not inline. It lives within the server case and thus would be very difficult to

bypass without obvious detection (server shut down, case opened up, and so forth). (See Table 3.3.)

Table 3.3 3Com / SonicWALL at-a-Glance

Web site	www.3com.com/products/en_US/prodlist.jsp?tab=cat&pathtype=purchase&cat=134482 www.sonicwall.com/products/vpnapp.html
Models	3Com OfficeConnect Internet Firewall 25 3Com SuperStack 3 Firewall 3Com Firewall Server PCI Card SonicWALL SOHO3 Firewall SonicWALL PRO330 Firewall
Pros	Innovative embedded firewall is industry first
Cons	Best suited for smaller networks

Check Point Software Technologies

Depending on which survey you read, the Cisco PIX and Check Point Firewall-1 share market dominance. In our experience, most networks that we run across (that are larger than the SOHO class) have Check Point running on Nokia IPSO appliances. Claiming to have invented stateful inspection, FireWall-1 is a hybrid stateful inspection firewall that has configurable application-layer proxies to perform inspection. The software can be installed on Solaris or Windows NT, but is most often deployed on hardened NetBSD appliances provided by Nokia (formerly manufactured by Ipsilion). (See Table 3.4.)

Table 3.4 Check Point Software Technologies at-a-Glance

Web site	www.checkpoint.com/products/protect/firewall-1.html
Models	Check Point Firewall-1 NG Check Point Provider-1 NG Nokia IPSO 350 appliance Nokia IPSO 650 appliance
Pros	Market leader, high performance with good balance of rich features
Cons	Product licensing is second only to differential calculus in difficulty

The Check Point Policy Editor, their administrative GUI, is very well thought out, with logical groupings of commands and a simple tabular display of

security rules in columns with headings in plain English. This management console is so nicely designed and well received by the industry that competitors are starting to duplicate the “look and feel” of the Check Point console. The security policy screen of the Cisco PIX Device Manager (see next section) was modeled heavily after this GUI.

FireWall-1 has an innovative attack-forecasting feature called SmartDefense. Using this technology, your firewall can connect to one of several Internet Storm Centers, such as the one operated by the SANS Institute, Dshield.org. You can contribute anonymous logs to the community effort, but more importantly, you can download a list of top attackers and use that to block future attacks on your network. This mimics the idea of a collaborative blacklist for firewalls, much like the SPAM blacklist services that exist. Using a mixture of hardware accelerators and software enhancements, the SecureXL feature set can enable FireWall-1 to process up to 3.2 Gbps of throughput. Most discomfort in Check Point installations comes from a very restrictive and difficult-to-understand licensing policy.

NOTE

For more dedicated information on the suite of products available from Check Point and Nokia, refer to the following other books also available from Syngress Publishing.

Check Point Next Generation Security Administration, ISBN 1-928994-74-1.

Nokia Network Security Solutions Handbook, 1-931836-70-1.

Check Point NG VPN-1/Firewall-1 Advanced Configuration and Troubleshooting, 1-931836-97-3.

Check Point Next Generation with Application Intelligence Security Administration, 1-932266-89-5.

Cisco Systems, Inc.

Cisco has been known as the most unfriendly but powerful firewall in the industry for quite some time. While certainly not glamorous, the PIX Firewall configuration commands are fairly easy to understand if you have knowledge of the Cisco IOS command set. With the exception of NetScreen, the PIX is the only firewall that runs on a custom real-time operating system (referred to as PIX OS, but in reality it is the brainchild of one of Cisco's acquisitions and they called it Finesse) rather

than a hardened off-the-shelf OS. Many people believe in the power and features of PIX, but up until recently, the only way to fully configure the firewall was to use a command-line interface (CLI) on their text-based administrative interface (serial or Telnet connection). This might have been a bit daunting for some users, so Cisco recently introduced a Web-based Java applet called the PIX Device Manager (PDM) that hopes to win back some of the market share that was lost to Check Point based on user interface. (See Table 3.5.)

Table 3.5 Cisco at-a-Glance

Web site	www.cisco.com/en/US/products/hw/vpndevc/ps2030
Models	Cisco PIX 501 Cisco PIX 506 Cisco PIX 515 Cisco PIX 525 Cisco PIX 535
Pros	Market leader, fantastic performance, interacts with Cisco routers; can shun active attacks
Cons	Command line can be difficult for beginners

PIX appliances are all solid-state and have no hard drives in them (unlike the Nokia IPSO). To their advantage, this means fewer parts to wear out or worry about during an abrupt power outage. A slight disadvantage is that firewall logging cannot be performed locally. Instead, the PIX will stream log entries to any SYSLOG daemon of your choosing.

The PIX product line ranges from the SOHO to large enterprise levels. The PIX 501 is about the size of a VHS cassette tape, yet runs the complete PixOS just like the larger counterparts. The PIX 515, previously the entry point to the PIX product line, is a popular inhabitant of data centers across the country due to its compact, 1U design. For companies that have high demands of their firewalls, the PIX 525 is a good compromise between the sometimes overwhelming power of the 535 and the always overwhelming price tag. The high-end Cisco PIX 535 will provide 1.7 Gbps of throughput and 500,000 simultaneous connections in the session table. Along with Symantec, it also supports the new *Advanced Encryption Standard* (AES, or Rijndael) encryption method for VPN components. Most firewalls only support the older NIST standard, Triple DES. The PIX 520, now obsolete and unsupported, is the last of the PIX models to still “look” like a normal PC, complete with floppy drive in the front. All the newer models are based on purpose-built chassis design.

CyberGuard

This line of proxy-based firewalls is likely one of the best for this category, earning the prestigious *SC Magazine* Best Firewall award (www.westcoast.com/events/awards) for the second year in a row t (2002 and 2003). They stress the importance of protocol and application awareness during the firewall packet-forwarding decision. One of the largest (physically) firewalls out there, this 4U behemoth boasts up to four SCSI drives in a RAID 5 hot-swappable configuration and can support up to 12—yes a dozen—Ethernet 10/100 interfaces running on a derivative of UnixWare. The high end of the CyberGuard spectrum includes some very helpful smart proxies that are preconfigured (for Telnet, HTTPS, and FTP) to click-and-install. The WebSense URL filtering software can be purchased in a bundle to allow for greater control over what your users are doing with their time. Additionally, the F-Secure Anti-Virus system enables scanning for evil e-mail attachments at the gateway. This allows you to regain control over these malicious attachments before they get distributed to the internal e-mail server. (See Table 3.6.)

Table 3.6 CyberGuard at-a-Glance

Web site	www.cyberguard.com/solutions/product_overview.cfm
Models	CyberGuard FS250 CyberGuard SL3200 CyberGuard KS1500
Pros	Common Criteria EAL4+ Fantastic performance Interacts with Cisco routers; can shun active attacks
Cons	Command line can be difficult for beginners

Microsoft ISA Server

Regardless of what the marketing documents say, ISA Server is really nothing more than the old Microsoft Proxy Server with better wizards. However, ISA Server's integration with the Active Directory provides centralized management and control over ISA settings, Windows network username logging for firewall traffic, and built-in availability features based on the resiliency of Active Directory. The “publishing” wizards are helpful in creating a rule set, but are specified using the opposite terminology than the rest of the industry. (See Table 3.7.)

Table 3.7 Microsoft at-a-Glance

Web site	www.microsoft.com/ISAServer
Models	Microsoft Internet Security & Acceleration Server
Pros	Integrated with Active Directory to provide resiliency of fire-wall information
Cons	Rule sets might be hard for veteran firewall admins to understand; appear to be written from the wrong point of view

NetScreen

NetScreen has always been known for performance. Their high-end packet-filtering firewalls can process an insane 12 Gbps and have earned them the 2003 *Network Magazine* Product of the Year award (www.infoxpress.com/reviewtracker/reprints.asp?page_id=1538). Most of their performance boost can be attributed to their highly optimized ScreenOS operating system and custom ASICs that perform the forwarding decisions for the firewall. NetScreen's high availability solutions include the typical active-standby configurations but also a nice active-active one where the two firewalls share the network load cooperatively. Their SOHO offerings even include an innovative anti-virus scanning functionality usually found on higher-end firewalls. The Trend Micro AV engine is featured on the NetScreen 5GT and can scan SMTP, POP3, and Web traffic. (See Table 3.8.)

Table 3.8 NetScreen at-a-Glance

Web site	www.netscreen.com/products/firewall
Models	NetScreen-25 NetScreen-208 NetScreen-500 NetScreen-5400
Pros	Extremely optimized for speed FIPS as well as Common Criteria certification
Cons	Configuration language hard to use if you have deep understanding of the Cisco IOS command set. Users with no prior IOS experience should not have a problem

Novell

Novell, famous for the very successful NetWare network operating system and later the highly scalable NDS Directory service, also offers a firewall solution called BorderManager. One of the nice features of BorderManager is the tight integration with NDS. We don't mean just integrating firewall logs with usernames from NDS. All the firewall features can be controlled from within your favorite NDS browser, which really cuts down on administrative headache. Starting with version 3.7, BorderManager has the SurfControl content database integrated into the firewall, which makes URL filtering as easy as the 3Com with the power of a third-party solution. BorderManager is still a proxy-based firewall, so performance does suffer. However, if you're an all-Novell shop it is a great solution that will reduce the strain on your IT department. Since BorderManager is offered as part of the Novell Small Business Solution, small offices that don't have an IT department can get a firewall for free with their network operating software package. (See Table 3.9.)

Table 3.9 Novell at-a-Glance

Web site	www.novell.com/products/bordermanager
Models	Novell BorderManager
Pros	Heavily Integrated with Novell NDS and that provides an easy administration task SurfControl for content screening
Cons	Specialized knowledge of NetWare 5.1 or later is required

Secure Computing

Another firewall in the hybrid category, Secure Computing has a stateful packet inspection firewall that has intelligent adaptive proxies that can perform Layer 7 inspection without slowing the network connectivity to the speed of a pure proxy solution. A mature solution, the Sidewinder has been around since 1994 and keeps getting better each year. Their Sidewinder G2 firewall has won the *Network Computing* magazine's Well-Connected Award for 2003 (www.nwcwell-connected.com). Primarily delivered as a ready-to-go hardware appliance, the Sidewinder G2 is different from the other hardware appliances listed here in that it is really just a Dell PowerEdge 2650 server that has been preinstalled with their special SecureOS UNIX variant. The software can also be purchased separately,

to run on your own hardware. We would stick to using what they're calling an appliance just to reduce the headache of any strange SCSI card in your flavor of server that might not be supported in SecureOS. (See Table 3.10.)

Table 3.10 Secure Computing at-a-Glance

Web site	www.securecomputing.com/index.cfm?sk=232
Models	Secure Computing Sidewinder G2
Pros	Automated response engine can react in real time to attacks EAL4 common criteria certified
Cons	Because of a very detailed method of inspecting packets, Sidewinder is slower than other firewalls Lack of a solid state "true" hardware appliance means you might have to manage different hardware platforms for all your different Sidewinder firewalls

Stonesoft, Inc.

Stonesoft products are obsessed with high availability. Everything they do has an eye toward failover, and this doomsday view of life makes for some very robust offerings. StoneGate, their high availability clustered firewall, has a mix of application-layer agents that provide information to their stateful inspection engine (they call this multilayer inspection) that we mentioned earlier. Running on a hardened version of Debian Linux, StoneGate performs heartbeat functions (discussed earlier) with all members (up to 16) of the firewall cluster and has won *SC Magazine's* Best Buy award (www.stonesoft.com/products/StoneGate/Certifications_and_Awards/SC_Magazine_-_Best_Buy). StoneGate is also the only firewall offering to be available for the IBM zSeries mainframe. This is a huge plus for financial organizations that might be forced to keep their large mainframes around to support legacy applications, and don't want to manage yet another device in front of the mainframe to protect it from network attacks. In Q2 of 2004 (right around the time you'll be reading this sentence), Stonesoft will have a product offering on Linux, designed to run on the IBM eServer iSeries. (See Table 3.11.)

Table 3.11 Stonesoft at-a-Glance

Web site	www.stonesoft.com/products
Models	Stonesoft StoneGate
Pros	Very strong clustering and high-availability features, based on the work they have done with clustering other vendors' devices as well Available for IBM z990 mainframe
Cons	Does not come in its own appliance; users must supply their own server

If the emphasis on high availability seems intense, it's because Stonesoft began by providing third-party clustering solutions (called StoneBeat) for Check Point Firewall-1, Microsoft ISA Server, Raptor (now Symantec Enterprise Firewall), and Secure Computing's Gauntlet. Even if you decide not to use the Stonesoft firewall, you should definitely look into their clustering technology to complement an installation of any of those four products.

Symantec Corporation

Symantec purchased the Raptor firewall product and renamed it Enterprise Firewall. With version 7.0, Enterprise Firewall is EAL-4 certified for Common Criteria compliance (important for government facilities). Symantec describes their firewall as "full inspection" as opposed to stateful inspection firewalls. This just means that they are much like StoneGate and FireWall-1 by being a stateful inspection firewall that has elements of Layer 7 inspection to allow it to make intelligent forwarding decisions. Enterprise Firewall, much like BorderManager, teamed up with a content filtering provider and includes the WebNOT technology with its firewall and is one of only a few vendors that use AES for VPN connections. The software can be installed on Solaris or Windows NT platforms, but is also offered in a VelociRaptor appliance that is more attractive (much like the Nokia IPSO platform). (See Table 3.12.)

Table 3.12 Symantec at-a-Glance

Web Site	http://enterprisesecurity.symantec.com/content/ProductJump.cfm?Product=47&EID=0
Models	Symantec Gateway Security 5200 Symantec VelociRaptor 1200 Symantec Enterprise Firewall 100
Pros	As part of the Symantec Gateway Security offering, the firewall component has some good company, including Symantec AntiVirus and other intrusion prevention methods
Cons	User interface can be hard to navigate at times

WatchGuard Technologies, Inc.

With its distinctive bright red appliance chassis, the WatchGuard firewall can be identified from clear across the data center floor. Their lower-end Firebox SOHO 6 Wireless is a great idea for small remote offices that need to connect to headquarters using LAN-to-LAN VPN tunnels. Not only does it allow for IPSec encryption of the wireless and wired sides, but through a partnership with McAfee the Firebox has a VirusScan ASaP subscription to help with virus issues at the remote office with little or no IT support. On the high end of the spectrum, WatchGuard has really stepped up to the ISP and large organization level and introduced their Firebox V200 that can provide up to 2 Gbps of throughput and support up to 40,000 branch office VPN connections. The Firebox 4500, while supporting less capacity, still has an impressive 200 Mbps throughput and uses application layer proxies to complement its stateful inspection engine. They include Web content filtering as well, provided by CyberPatrol. (See Table 3.13.)

Table 3.13 WatchGuard at-a-Glance

Web site	www.watchguard.com/products/wgls.asp
Models	Firebox SOHO 6 Firebox III Firebox X Firebox vClass
Pros	With the Firebox X, you can easily grow your firewall in pace with the growth of your networks High availability active/active configurations Four embedded RISC processors on the vClass line, for extra number crunching power
Cons	Management software is Windows based only

The most exciting product offering from WatchGuard is their new line of Firebox X devices. Distancing themselves from the almost cartoonish front panel design of the Firebox III, the X has a crisp appearance, an LCD screen, and expandable capacity for two to six NICs. As your network grows, entering in a software license activation key will enable the additional NICs and additional capabilities. Spam filtering, antivirus, VPN, intrusion prevention, and Web filtering can also be activated easily, as your company grows, using just an activation key.

Checklist

- ☑ Decide what is more important to your organization (performance, or packet inspection) and select accordingly.
- ☑ Plan ahead and don't paint yourself into a corner when doing an eval; know what targets you're trying to hit and clearly articulate these to your vendors.
- ☑ Understand the pros and cons of each firewall technology.
- ☑ Visit the vendor Web sites listed in this chapter to find out the features provided on each model.
- ☑ Visit the mailing lists and message boards listed at the end of this chapter to hear the real skinny from the trenches on using and maintaining different firewall types.

Summary

The firewall is your front lines of defense against attackers on the Internet. Everyone knows that you need a firewall, but who has stopped to examine the reasons behind that need? More than just “keeping the bad guys out,” a sound firewall policy will make your network more efficient by only dealing with the traffic that is truly essential to your business operations. In essence, a firewall can concentrate your networking efforts and turn a noisy network into a laser-beam focused data delivery service.

Through the course of this chapter, we explained the different types of firewalls and their inner workings. Certifications, in the firewall industry, are an important way to show third-party acceptance of your product. Restricting your Web servers to only performing Web-related services, and your mail servers restricted to performing mail-delivery services, you will have less cause for alarm at night. This makes both good business and technological sense; you would only give particular employees the key to the NOC, so too should you be particularly discriminating about the ports to which you allow servers to make outbound connections.

While some vendors have a hardware appliance offering, others concentrate on the software only and leave the hardware to the end customer (still a couple of others will offer the software in both variations). All firewalls will have some form of administrative interface or GUI to configure the firewall for your company's particular needs. Most firewalls will provide a third NIC to define a service network, or DMZ, for your mail servers and other trusted-but-feared machines.

The differences between proxy-based and stateful packet inspection firewalls make for good debate. However, other, less controversial issues tend to get equal press in the security publications: logging, VPN, clustering, high availability, content filtering, and antivirus features are all powerful add-ons to look for when choosing your next firewall. Just remember not to sacrifice stable performance and a track record for quality software for the latest and greatest command-line utility that masquerades as a firewall.

Good ol' RFC 1918 makes it easy to segment your network according to functional business units, rather than arcane network address range assignments. Stateful failover, a feature often reserved for very high-end firewalls, is critical in a 24/7 operations center. Finally, go through the Web sites for all the vendors listed here and discover the solution that works best in your environment. Don't be afraid to kick the tires and make sure you're getting what your network needs today and this year. A pushy salesperson convincing your company of 10

employees that they need the PIX 535 is just criminal. Make sure you don't fall victim to the same tactics.

Solutions Fast Track

Understanding Firewall Basics

- ☑ A firewall must make packet routing decisions based on its preconfigured security profile.
- ☑ Better firewalls include features like detailed reporting and URL content filtering.

Exploring Stateful Packet Firewalls

- ☑ Although attributed to Check Point, the advent of stateful packet filtering firewalls allows us to be very restrictive in our security policy and yet know that return traffic will be handled.

Explaining Proxy-Based Firewalls

- ☑ Proxy firewalls will always be slower than the competition.
- ☑ Detailed reporting is possible due to the full-packet inspection process involved.

Examining Various Firewall Vendors

- ☑ Each vendor has its strengths and a weaknesses—what works for your organization will vary.
- ☑ Look for content filtering software pre-bundled with firewalls today.
- ☑ Use embedded PCI NIC firewalls for maximum security.

Links to Sites

- www.sl.universalservice.org/reference/CIPA.asp
e-Rate Federal subsidized Internet access for schools.

- **www.websense.com** WebSense provides Web content filtering software that can plug in to firewalls like Cisco PIX.
- **www.surfcontrol.com** SurfControl also provides content filtering software to prevent users from navigating to inappropriate Web sites.
- **www.cyberpatrol.com** CyberPatrol produces content filtering software dubbed “Parental Control Software” due to its home-computer target, rather than Enterprise deployment.
- **www.cisco.com/en/US/products/hw/vpndevc/ps2030** Information on the entire Cisco PIX product line.
- **www.checkpoint.com/products/protect/firewall-1.html** Check Point Firewall-1 is one of the best selling firewalls around.
- **http://secure.dshield.org** By correlating a massive amount of data from user-submitted firewall logs, DShield can show the current “weather” condition of the Internet.
- **www.watchguard.com/products/wgls.asp** More information on the WatchGuard family of firewalls.
- **http://enterprisesecurity.symantec.com/content/ProductJump.cfm?Product=47&EID=0** Symantec Enterprise Firewall information and detailed product specifications.
- **www.novell.com/products/bordermanager** Novell BorderManager is the only product (oddly enough) to integrate seamlessly with Novell NDS.
- **www.stonesoft.com/products** Stonesoft provides highly redundant firewall architectures.
- **www.netscreen.com/products/firewall** NetScreen firewalls range from small office to data-center grade performance.
- **www.microsoft.com/ISAServer/** Microsoft Internet Security and Acceleration Server information.

- **www.sonicwall.com/products/vpnapp.html** SonicWALL makes a range of firewall appliances to fit any budget, from home office to large company.
- **www.3com.com/products/en_US/productsindex.jsp?tab=cat&pathtype=purchase** Information on the 3Com Firewall Desktop PCI card, allowing all of your servers to have a robust hardware firewall-on-a-NIC.
- **www.icsalabs.com/html/communities/firewalls/** ICSA Certification criteria for network firewalls.
- **www.icsalabs.com/html/communities/pcfirewalls/** ICSA Certification criteria for PC firewalls.

Mailing Lists

- **firewalls@securityfocus.com** A great, vendor-neutral discussion that has contributions from people all over the globe.
- **firewalls@lists.gnac.net** Smaller membership than SecurityFocus, this list also has some useful information.
- **www.snpx.com/newsticker.html** This continuously updating news ticker is specifically geared toward the security industry. You can embed this little applet on your company's intranet and always stay up to the minute on the latest exploits and vulnerabilities.
- **<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>** ICSA Labs is the major certification for firewall products, and as such, this mailing list provides many useful tips and tricks from the firewall veterans.
- **www.isc.org/services/public/lists/firewalls.html** ISC, the organization behind the prestigious CISSP certification, maintains a firewall mailing list that tends to be more academic and theory than vendor-specific issues, but it still quite useful.

- www.securitynewsportal.com/pagetwo.shtml The lighter side of the security industry news, this is the place to keep up with the latest gossip or Web site defacements.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to www.syngress.com/solutions and click on the “Ask the Author” form. You will also gain access to thousands of other FAQs at ITFAQnet.com.

Q: What makes a proxy-based firewall so slow?

A: Remember the diagram explaining OSI layers earlier in the chapter? Of course you do—it was so concise and well written, it’s resonating in your brain as we speak. Each time a software process must travel up or down the OSI layers, there is going to be a performance hit. Traveling between layers means either opening the lower layer’s data packet “envelope” or wrapping a higher layer’s data in its own envelope. To send a packet between two hosts, the proxy-based firewall must unwrap these envelopes all the way up at Layer 7, copy the data to another buffer, and reseal all seven envelopes. Anyone who has worked in accounts payable can tell you—licking that many envelopes will definitely slow you down (and might cause a nasty paper cut on your tongue).

Q: I’ve heard rumors that Check Point firewalls have back doors built into them; is this true?

A: You should keep out of the Cisco booth at trade shows! There have been rumors floating around for years (mostly from San Jose residents) that the Mossad, the Israeli equivalent of the United States’ Central Intelligence Agency, wrote the Check Point software and has a back-door password to get into any Firewall-1 protected network in the world. If such a back door existed, the amount of scrutiny that modern firewalls endure would almost certainly flush out this fact in a number of online forums known for pointing out flaws in security design. While we cannot say anything about Check Point source code with certainty, we know that if you throw enough smart people at an issue (say, for instance, the worldwide population of hackers),

you're bound to find out if there's a back door. Check out Chapter 4, "Attacking Firewalls," for a description of a Check Point vulnerability that is more of a "front door" hole than a back door one.

Q: Wow—security software written by Israeli intelligence agencies! This sounds like a Tom Clancy novel. How can I find out more?

A: We're not going to perpetuate any rumors about ties to the Mossad, but we will tell you this: in April 2001, the Mossad published advertisements in major publications, encouraging electronic engineers and computer scientists to apply to their special "Technology Department." The ad stated "The Mossad is open / Only to 13 engineers ... The Mossad is open. Not to everyone. Not to many. Maybe to you." You draw your own ending to this novella; just make sure nobody discovers your true identity, 007.

Q: Who invented stateful inspection firewall technology?

A: Again, our friends at the Mossad, er... we mean Check Point take credit for this one. Although nobody really should be allowed to take credit for a type of technology, many Check Point publications reference the assertion that they "invented" this technology. In fact, they do hold the patent on stateful inspection firewall technology—but that does not necessarily mean they invented it. It just means they were the first to patent the technology. It would be the same thing as if we said "We're going to patent the process of logging in to a Web site so that it can show us personalized content." You would say, "You're crazy—that's just a concept. You can't patent the concept of logging in. Any dynamic site on the Internet today has some mechanism of logging in and having pre-stored preferences recalled. I mean, even something as simple as MyYahoo would be infringing upon that patent! You're crazy!" You can stop yelling at us—we won't try to patent that idea. But only because Gateway Computer beat us to it (U.S. Patent 6,530,083). And as soon as you stop yelling about how ridiculous that sounds, remember that the BT Group went to court against the Prodigy online service in February 2002 because they claimed to own the patent on hyperlinks.

Q: Where is future firewall technology headed?

A: If you ask us (and well, we guess you just did), firewalls are going to become smaller and more pervasive. Right now, you'll only find personal firewalls on very smart home users or very security savvy business users. In a year's time,

nobody would think of powering on his or her machine without a personal firewall set on “red alert.” The emphasis of choke points on your network where all traffic must filter through one device (the firewall) will disappear as that technology gets pushed out to the end points. A real big winner in this field is 3Com; they’ve already designed the product (the firewall-on-a-NIC described earlier) and are just waiting for the industry to take off. Soon, your data center won’t have a single firewall in it! Instead, it will have 85 firewalls, one on each NIC port. They will all report back to a centralized management console and it will provide for the ultimate in granular manageability.