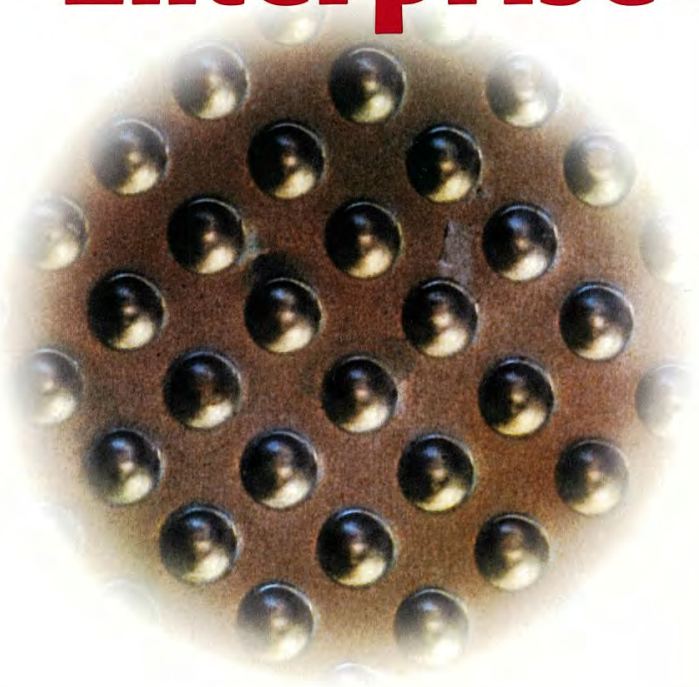
WILEY

TIMELY. PRACTICAL. RELIABLE.

Firewall Architecture for the Enterprise



Norbert Pohlmann
Tim Crothers

Firewall Architecture for the Enterprise

Norbert Pohlmann and Tim Crothers

Wiley Publishing, Inc.

Best-Selling Books • Digital Downloads • e-Books • Answer Networks
e-Newsletters • Branded Web Sites • e-Learning

Firewall Architecture for the Enterprise
Published by
Wiley Publishing, Inc.
909 Third Avenue
New York, NY 10022
www.wiley.com

Library of Congress Control Number: 2002102445
ISBN: 0-7645-4926-X
Manufactured in the United States of America
10 9 8 7 6 5 4 3 2 1
1O/QT/QX/QS/IN
Published by Wiley Publishing, Inc., Indianapolis, Indiana
Published simultaneously in Canada

extended state-oriented packet filters as *stateful inspection*, *smart filtering*, or *adaptive screening*. With this extended functionality, they are often offered as user-oriented packet filters. Figure 4-15 illustrates state-oriented packet filters.

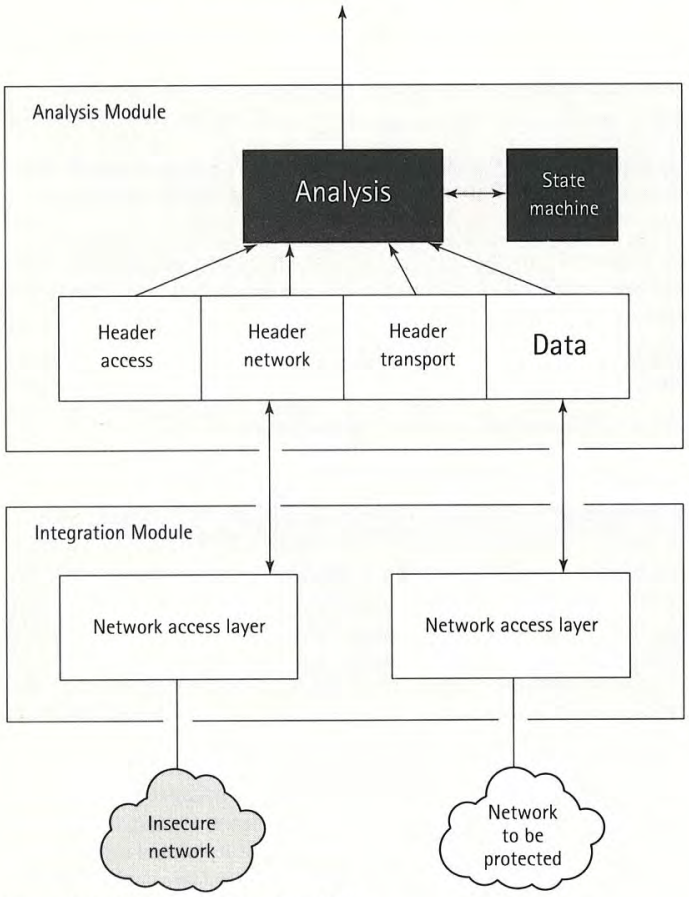


Figure 4-15: State-oriented packet filters

State-oriented packet filters have the same advantages as packet filters, but they can also check the applications. Some risks remain because the services are not directly isolated from each other.

Because it is a complex matter to simultaneously hold and interpret the communications data in the different communications layers, state-oriented packet filters generally have a shallower depth of analysis, or they are particularly prone to

errors connected with their very powerful software. Basically, you can't test the complex software of state-oriented packet filters sufficiently or comprehensively to prove that errors cannot occur in any operating state. For this reason, one must continue to assume that the complex programs contain potential security risks that could be used to perpetrate an attack.

A better and more secure way to analyze the application data is to use application gateways with proxies. This approach is described in the next section.

Network Address Translation

As its name implies, *NAT (Network Address Translation)* works by using one set of addresses for communications on the Internet and a separate set of addresses for communications on the internal network. To fully support this translation, the IANA set aside three ranges of IP addresses in RFC 1918:

- 10.0.0.0 through 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 through 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 through 192.168.255.255 (192.168.0.0/16)

These addresses are reserved for internal use only and, as a consequence, are nonroutable on the Internet. Attempts to communicate with any of these ranges through the Internet result in ICMP "network unreachable" errors.

An organization implementing NAT uses one of the preceding ranges for their internal network addressing. The external interface of the firewall is assigned a normal routable IP address. When the firewall transmits a packet from the internal network to the Internet, it actually creates a new packet destined for the same address but originating from the external address(es) of the firewall. This packet is then transmitted to the destination. The firewall keeps a table of current communications so that when the return communications reach the firewall, they are taken and placed into a new packet destined for the internal computer and transmitted internally.

The NAT process affords a substantial degree of security. Since all direct communications are prevented (as long as the systems are properly configured), an external attacker is forced to compromise the firewall or find a means of passing his communications through it successfully rather than attacking the internal host directly. Given the firewall protection module and hardening, this is a relatively significant challenge.

Not inconsequentially, NAT prolongs the life expectancy of IPv4 on the Internet. Were it not for address translation, the supply of Internet addresses would have been exhausted long ago. Using NAT, a company with hundreds of internal computers can communicate fully with the Internet using only a handful of routable addresses.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.