Building Internet Firewalls

D. Brent Chapman and Elizabeth D. Zwicky

O'Reilly & Associates, Inc.
103 Morris Street, Suite A
Sebastopol, CA 95472

Building Internet Firewalls
by D. Brent Chapman and Elizabeth D. Zwicky

Editor: Deborah Russell

Production Editor: Mary Anne Weeks Mayo

Printing History:

September 1995: First Edition.
November 1995: Minor corrections.

This book is printed on acid-free paper with 85% recycled content, 15% post-consumer waste. O'Reilly & Associates is committed to using paper with the highest recycled content available consistent with high quality.

ISBN: 1-56592-124-0 [1/96]

Forew
Prefa

I: N

1: W

Wh
Wh
Ho
Wh

2: In

Ele
File
Ren
Use
The
Oth
Info
Rea
Nan
Net
Tim
Net

6

Packet Filtering

In This Chapter:

- *Why Packet Filtering?*
- *Configuring a Packet Filtering Router*
- *What Does a Packet Look Like?*
- *What Does the Router Do with Packets?*
- *Conventions for Packet Filtering Rules*
- *Filtering by Address*
- *Filtering by Service*
- *Choosing a Packet Filtering Router*
- *Where to Do Packet Filtering*
- *Putting It All Together*

Packet filtering is a network security mechanism that works by controlling what data can flow to and from a network. We provide a very brief introduction to high-level IP networking concepts (a necessity for understanding packet filtering) here, but if you're not already familiar with the topic, then before continuing, you should refer to Appendix C for a more detailed discussion.

To transfer information across a network, the information has to be broken up into small pieces, each of which is sent separately. Breaking the information into pieces allows many systems to share the network, each sending pieces in turn. In IP networking, those small pieces of data are called *packets*. All data transfer across IP networks happens in the form of packets.

The basic device that interconnects IP networks is called a *router*. A router may be a dedicated piece of hardware that has no other purpose, or it may be a piece of software that runs on a general-purpose UNIX or PC (MS-DOS, Windows, Macintosh, or other) system. Packets traversing an internetwork (a network of networks) travel from router to router until they reach their destination. The Internet itself is sort of the granddaddy of internetworks—the ultimate "network of networks."

A router has to make a routing decision about each packet it receives; it has to decide how to send that packet on towards its ultimate destination. In general, a packet carries no information to help the router in this decision, other than the IP

address of the packet's ultimate destination. The packet tells the router where it wants to go, but not how to get there. Routers communicate with each other using "routing protocols" such as the Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) to build *routing tables* in memory to determine how to get the packets to their destinations. When routing a packet, a router compares the packet's destination address to entries in the routing table and sends the packet onward as directed by the routing table. Often, there won't be a specific route for a particular destination, and the router will use a "default route;" generally, such a route directs the packet towards smarter or better-connected routers. (The default routes at most sites point towards the Internet.)

In determining how to forward a packet towards its destination, a normal router looks only at a normal packet's destination address and asks only "*How* can I forward this packet?" A packet filtering router also considers the question "*Should* I forward this packet?" The packet filtering router answers that question according to the security policy programmed into the router via the packet filtering rules.

NOTE

Some unusual packets do contain routing information about how they are to reach their destination, using the "source route" IP option. These packets, called *source-routed packets*, are discussed in the section called "IP Options" below.

Why Packet Filtering?

Packet filtering lets you control (allow or disallow) data transfer based on:

- The address the data is (supposedly) coming from
- The address the data is going to
- The session and application protocols being used to transfer the data

Most packet filtering systems don't do anything based on the data itself; they **don't** make content-based decisions.* Packet filtering will let you say:

Don't let anybody use Telnet (an application protocol) to log in from the outside.

or:

Let everybody send us email via SMTP (another application protocol).

or even:

That machine can send us news via NNTP (yet another application protocol), **but** no other machines can do so.

* Some packages, like CheckPoint's FireWall-1 product, are limited exceptions to this **rule**.

However, it won't let you say:

> This user can Telnet in from outside, but no other users can do so.

because "user" isn't something a packet filtering system can identify. And, it won't let you say:

> You can transfer these files but not those files.

because "file" also isn't something the packet filtering system can identify.

The main advantage of packet filtering is leverage: it allows you to provide, in a single place, particular protections for an entire network. Consider the Telnet service as an example. If you disallow Telnet by turning off the Telnet server on all your hosts, you still have to worry about someone in your organization installing a new machine (or reinstalling an old one) with the Telnet server turned on. On the other hand, if Telnet is not allowed by your filtering router, such a new machine would be protected right from the start, regardless of whether or not its Telnet server was actually running. This is an example of the kind of "fail safe" stance we discussed in Chapter 3.

Routers also present a useful choke point (also discussed in Chapter 3) for all of the traffic entering or leaving a network. Even if you have multiple routers for redundancy, you probably have far fewer routers, under much tighter control, than you have host machines.

Certain protections can be provided *only* by filtering routers, and then only if they are deployed in particular locations in your network. For example, it's a good idea to reject all packets that have internal source addresses—that is, packets that claim to be coming from internal machines but that are actually coming in from the outside—because such packets are usually part of address-spoofing attacks. In such attacks, an attacker is pretending to be coming from an internal machine. Decision-making of this kind can be done only in a filtering router at the perimeter of your network. Only a filtering router in that location (which is, by definition, the boundary between "inside" and "outside") is able to recognize such a packet, by looking at the source address and whether the packet came from the inside (the internal network connection) or the outside (the external network connection). Figure 6-1 illustrates this type of source address forgery.

Advantages of Packet Filtering

Packet filtering has a number of advantages.

One screening router can help protect an entire network

One of the key advantages of packet filtering is that a single, strategically placed packet filtering router can help protect an entire network. If there is only one

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.