Introduction to Easy iptables Management with Shorewall

Roberto C. Sánchez

Connexer, Ltd.

http://www.connexer.com

roberto@connexer.com

June 14, 2012

Presented at NYLUG June Meeting

New York, NY

What Is This All About?

`iptables` got you down? There's an easier (and very flexible) way. What you need is Shorewall! It slices, it dices, it even pureés, making your most challenging household chores a breeze!

Overview

- Objective
- A Little Bit About the Presenter
- A Little Bit About Shorewall
- Getting and Installing Shorewall
- Shorewall Basics
- Shorewall for Protecting a Single Host
- Shorewall for Protecting your LAN
- Advanced Features of Shorewall
- Documentation
- Getting Additional Help
- Pitching In to Help
- Summary

Objective

- What this presentation is:
  - An introduction to using Shorewall to manage your iptables configuration.
- What this presentation is not:
  - A HOWTO on converting your specific iptables or other firewall configuration to Shorewall.
- When this presentation is over:
  - You should know how to get Shorewall, get started with a simple configuration, and where to go for additional help.

A Little Bit About the Presenter

- Using Debian since 2002
- Contributing to Debian since 2003
- Entered Debian New Maintainer queue on June 20, 2005
- Started *Connexer, Ltd.* in January, 2006
- Became official Debian Developer on March 13, 2007
- Currently maintain 51 Debian packages and sponsor uploads for several prospective Debian Developers

A Little Bit About Shorewall

- History
  - Primary (sometimes only) developer is Tom Eastep
  - Originally called "Seattle Firewall," or Seawall for short
  - When Tom moved to Shoreline, renamed to "Shoreline Firewall," or Shorewall as we now know it
- What Shorewall is
  - An "interface" to `iptables`
  - Simple, Powerful, Flexible
  - Very well documented, and implemented in Perl
- What Shorewall is not
  - A daemon (or service)
  - A substitute for understanding networking principles
- Key features
  - Support for IPv4 (including NAT) and IPv6
  - Support for routing, bridging, and virtualization
  - Support for traffic shaping, multiple providers, etc.
  - No need to use `iptables` directly

Getting and Installing Shorewall

- Visit the Shorewall Download page
    - Follow links/instructions for your specific distro
    - Or, download RPM or tarball direct from upstream site and install manually
- Many distros incorporate official Shorewall packages
    - Some may be outdated, YMMV
    - If you do not need latest features, distro-provided packages should work
- In any case, read the installation instructions for info on distro-specific configuration and upgrading

Shorewall Basics

- Start by reading the documentation
- Best place to start is with the beginner documentation
    - Introductory documentation
    - Several quick start guides
- Read FAQs
- In case of problems, read the troubleshooting guide
- Check out the man pages (they ship with upstream tarball and most, if not all, distro packages)

Shorewall for Protecting a Single Host

- Use the universal configuration documentation
  - Includes instructions on how to install the configuration
  - Includes explanation of what it does
  - Includes answers to common questions
  - Includes instructions on how to make common tweaks (e.g., how to open specific ports, how to configure logging, etc.)
- In short, protecting your system with a firewall is nearly trivial

Shorewall for Protecting your LAN

- Use the two-interface configuration documentation
- Assumes only one public IP address for your network
    - Multiple IP addresses handled in different configuration-dependent ways
    - Additional documentation available for multiple public IP addresses
- Covers important Shorewall concepts (e.g., zones, policy, interfaces, etc.)
- Provides info on masquerading (SNAT), port forwarding (DNAT), and adding a wireless segment

Advanced Features of Shorewall

- Accounting
  - Count packets and bytes using categories and rules defined by the admin
- Blacklisting
  - Prevent particular hosts from connecting, based on IP, address range, subnet, or MAC
- Multiple providers
  - Allows traffic to flow over multiple interfaces to balance bandwidth usage
- Rate Limiting
  - Limit the number of connections to a particular port in a given period of time
- Traffic Control/Policy Routing
  - Prioritize traffic and/or send it out over specified provider links in a multiple provider configuration

Advanced Features of Shorewall - continued

- Tunneling
  - Create tunnels for VPN (e.g., IPsec, PPTP, OpenVPN, etc.), IPv6-over-IPv4, IPv4-over-IPv4, and others
- Shorewall-lite and Shorewall6-lite
  - Requires only Bourne-compatible shell (in place of full Perl installation)
  - Useful for embedded systems and large installations consisting of many hosts
  - Requires a "management" host to run the full Shorewall or Shorewall6
  - Configuration for the "lite" host is kept and compiled on the "management" host, then transferred to the "lite" host via `ssh`

Documentation

- Tom has spent literally thousands of hours documenting Shorewall
- Documentation is available in man pages, HTML (on the web and in -doc packages), and in many HOWTOs across the web
- Nearly every imaginable configuration, problem, etc., is already documented, so consult the documentation and/or Google
- Many of the most commom/basic problems and questions are addressed by the FAQs, so consult them as well
- Mailing lists are hosted/archived on SourceForge and provide a great source of information

Getting Additional Help

- Where to go
  - IRC
  - Mailing lists
  - Other
- How to go about requesting help
  - Troubleshooting - read the troubleshooting guide
  - Figuring out how to ask your question
    - Think about exactly what you expect to happen and compare that to what you are observing
    - Confirm that Shorewall is actually the problem
  - Making your request
    - Be polite - the few folks who support Shorewall are not your employees
    - Be patient - do not expect someone to drop everything just to help you, especially if your problem is complex
    - Make sure to include the output of `'shorewall dump'`

Pitching In to Help

- Monitor the -devel list for bug reports and feature requests
- Submit patches
- Monitor the IRC channel and -users list for support requests
- Test Beta releases and Release Candidates (espcially if you exercise Shorewall's more advanced features)

Summary

Shorewall makes firewalling with `iptables` much simpler than dealing with `iptables` directly by allowing the admin to specify the configuration in a set of text files and then compiling to a script that can be executed to implement the desired configuration.

Questions?

Questions?