Report Number: C4-040R-02

Router Security Configuration Guide

Principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco Systems routers

Router Security Guidance Activity
of the
System and Network Attack Center (SNAC)

Authors:
Vanessa Antoine
Raymond Bongiorni
Anthony Borza
Patricia Bosmajian
Daniel Duesterhaus
Michael Dransfield
Brian Eppinger
Kevin Gallicchio
James Houser
Andrew Kim
Phyllis Lee
Tom Miller
David Opitz
Florence Richburg
Michael Wiacek
Mark Wilson
Neal Ziring

September 27, 2002
Version: 1.1

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704

SNAC.Guides@nsa.gov

Warnings

This document is only a guide to recommended security settings for Internet Protocol (IP) routers, particularly routers running Cisco Systems Internet Operating System (IOS) versions 11 and 12. It is not meant to replace well-designed policy or sound judgment. This guide does not address site-specific configuration issues. Care must be taken when implementing the security steps specified in this guide. Ensure that all security steps and procedures chosen from this guide are thoroughly tested and reviewed prior to imposing them on an operational network.

SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This document is current as of August, 2002. The most recent version of this document may always be obtained through `http://www.nsa.gov/`.

Acknowledgements

The authors would like to acknowledge Daniel Duesterhaus, author of the original NSA “Cisco Router Security Configuration Guide,” and the management and staff of the Applications and Architectures division for their patience and assistance with the development of this guide. Special thanks also go to Ray Bongiorni for quality assurance and editorial work, and to Julie Martz for proof-reading and production assistance. Additional contributors to the guide effort include Andrew Dorsett, Charles Hall, Scott McKay, and Jeffrey Thomas. Thanks must also be given to the dozens of professionals outside NSA who made suggestions for the improvement of this document, especially George Jones, John Stewart, and Joshua Wright.

Trademark Information

Cisco, IOS, and CiscoSecure are registered trademarks of Cisco Systems, Inc. in the USA and other countries. Windows 2000 is a registered trademark of Microsoft Corporation in the USA and other countries. All other names are trademarks or registered trademarks of their respective companies.

Revision History

1.0	Sep 2000	First complete draft, extensive internal review.
1.0b	Oct 2000	Revised after review by Ray Bongiorni
1.0e	Jan 2001	First release version.
1.0f	Mar 2001	Second release version: second pre-pub review
1.0g	Apr 2001	Third release version: incorporated external feedback.
1.0h	Aug 2001	Fourth release version; another QA review.
1.0j	Nov 2001	Fifth release version.
1.0k	Mar 2002	Last release of 1.0, another pre-pub review.
1.1	Sep 2002	Major revision and expansion, another pre-pub review

Contents

Preface

Routers direct and control much of the data flowing across computer networks. This guide provides technical guidance intended to help network administrators and security officers improve the security of their networks. Using the information presented here, you can configure your routers to control access, resist attacks, shield other network components, and even protect the integrity and confidentiality of network traffic.

This guide was developed in response to numerous questions and requests for assistance received by the NSA System and Network Attack Center (SNAC). The topics covered in the guide were selected on the basis of customer interest, community concensus, and the SNAC's background in securing networks.

The goal for this guide is a simple one: improve the security provided by routers on US Government operational networks.

Who Should Use This Guide

Network administrators and network security officers are the primary audience for this configuration guide, throughout the text the familiar pronoun "you" is used for guidance directed specifically to them. Most network administrators are responsible for managing the connections within their networks, and between their network and various other networks. Network security officers are usually responsible for selecting and deploying the assurance measures applied to their networks. For this audience, this guide provides security goals and guidance, along with specific examples of configuring Cisco routers to meet those goals.

Firewall administrators are another intended audience for this guide. Often, firewalls are employed in conjunction with filtering routers; the overall perimeter security of an enclave benefits when the configurations of the firewall and router are complementary. While this guide does not discuss general firewall topics in any depth, it does provide information that firewall administrators need to configure their routers to actively support their perimeter security policies. Section 5 includes information on using the firewall features of the Cisco Integrated Security facility.

Information System Security Engineers (ISSEs) may also find this guide useful. Using it, an ISSE can gain greater familiarity with security services that routers can provide, and use that knowledge to incorporate routers more effectively into the secure network configurations that they design.

Sections 4, 5, and 6 of this guide are designed for use with routers made by Cisco Systems, and running Cisco's IOS software. The descriptions and examples in those sections were written with the assumption that the reader is familiar with basic Cisco router operations and command syntax.

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.