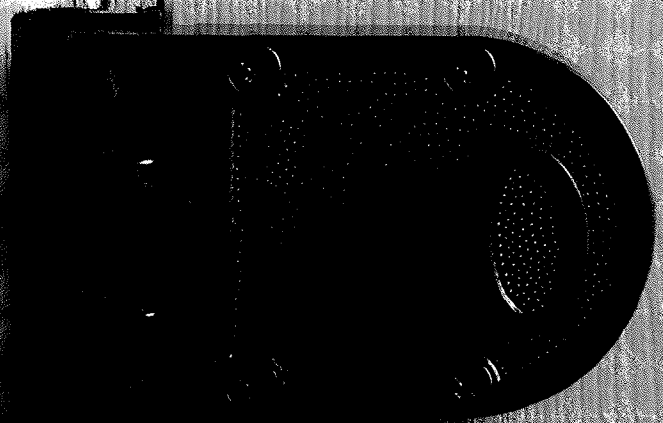
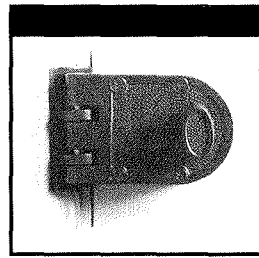


# Implementing IPsec

Making Security  
Work on VPNs,  
Intranets,  
and Extranets

Elizabeth Kaufman  
Andrew Newman





# Implementing IPsec: Making Security Work on VPNs, Intranets, and Extranets

---

Elizabeth Kaufman  
Andrew Newman

**Wiley Computer Publishing**



**John Wiley & Sons, Inc.**

NEW YORK • CHICHESTER • WEINHEIM • BRISBANE • SINGAPORE • TORONTO

Publisher: Robert Ipsen  
Editor: Carol Long  
Assistant Editor: Margaret Hendrey  
Managing Editor: Frank Grazioli  
Text Design & Composition: Benchmark Productions, Inc.

Designations used by companies to distinguish their products are often claimed as trademarks. In all instances where John Wiley & Sons, Inc., is aware of a claim, the product names appear in initial capital or ALL CAPITAL LETTERS. Readers, however, should contact the appropriate companies for more complete information regarding trademarks and registration.

This book is printed on acid-free paper. ♻

Copyright © 1999 by Elizabeth Kaufman and Andrew Newman. All rights reserved.

Published by John Wiley & Sons, Inc.

Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4744. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 605 Third Avenue, New York, NY 10158-0012, (212) 850-6011, fax (212) 850-6008, E-Mail: PERMREQ @ WILEY.COM.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in professional services. If professional advice or other expert assistance is required, the services of a competent professional person should be sought.

**Authors' Disclaimer:** Neither of our employers (Cisco Systems, Inc. and Yale University) had anything to do with this book or its contents. The opinions expressed are our own.

*Library of Congress Cataloging-in-Publication Data:*

ISBN 0-471-34467-2

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1



# Appendix

Network Working Group  
Request for Comments: 2401  
Obsoletes: 1825  
Category: Standards Track

S. Kent  
BBN Corp  
R. Atkinson  
@Home Network  
November 1998

## Security Architecture for the Internet Protocol

### Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

### Copyright Notice

Copyright (C) The Internet Society (1998). All Rights Reserved.

### Table of Contents

1. Introduction.....	3
1.1 Summary of Contents of Document.....	3
1.2 Audience.....	3
1.3 Related Documents.....	4
2. Design Objectives.....	4
2.1 Goals/Objectives/Requirements/Problem Description.....	4
2.2 Caveats and Assumptions.....	5
3. System Overview.....	5
3.1 What IPsec Does.....	6
3.2 How IPsec Works.....	6
3.3 Where IPsec May Be Implemented.....	7

- 4. Security Associations.....8
  - 4.1 Definition and Scope.....8
  - 4.2 Security Association Functionality.....10
  - 4.3 Combining Security Associations.....11
  - 4.4 Security Association Databases.....13
    - 4.4.1 The Security Policy Database (SPD).....14
    - 4.4.2 Selectors.....17
    - 4.4.3 Security Association Database (SAD).....21
  - 4.5 Basic Combinations of Security Associations.....24
  - 4.6 SA and Key Management.....26
    - 4.6.1 Manual Techniques.....27
    - 4.6.2 Automated SA and Key Management.....27
    - 4.6.3 Locating a Security Gateway.....28
  - 4.7 Security Associations and Multicast.....29



# 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.