

# Automated Firewall Analytics



Ehab Al-Shaer

# Automated Firewall Analytics

Design, Configuration and Optimization



Springer

Ehab Al-Shaer  
University of North Carolina Charlotte  
Charlotte, NC, USA

ISBN 978-3-319-10370-9 ISBN 978-3-319-10371-6 (eBook)  
DOI 10.1007/978-3-319-10371-6  
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014949240

© Springer International Publishing Switzerland 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media ([www.springer.com](http://www.springer.com))

*To my wife Ruba and my daughters Abrar,  
Rawan, Maram, Noor, and Haneen without  
whom this book would have been completed  
at least a year ago.*



# Preface

Firewalls provide the frontier security defense for enterprise networks. Firewalls provide the most critical cybersecurity functions for filtering out unwanted network traffic, which includes attacks and/or unauthorized traffic, coming to or leaving out the secured network. As firewalls on the network border to protect the system from external attacks, they are also used inside the enterprise networks to protect the system from internal attacks by isolating domains of varying security risk levels. In addition, IPSec extends the basic firewall access controls to provide secure communications, providing traffic integrity, confidentiality, and authentication over the Internet.

However, the complexity of managing firewall policies is significant, which limits the effectiveness of firewall security. Typical enterprise networks have hundreds of firewalls and IPSec devices which contain thousands of policy rules. Ad hoc or manual design and configuration management of firewalls is highly subject to human errors. The impact of such complexity has been evidently shown in the increasing number of security vulnerability reports due to operator misconfigurations. For example, a report from the Center for Strategic and International Studies “Securing Cyberspace for the 44th Presidency” in December 2008 states that “inappropriate or incorrect security configurations were responsible for 80 % of United States Air Force vulnerabilities”. A Juniper Networks report “What is Behind Network Downtime?” states that “human errors are blamed for 50–80 % of network outages”. Most recent study by Tufin Technologies in 2011 reported that “Nearly 85 % of network administrators in the 2011 Firewall Management report said half of their firewall rule changes need to be fixed because they were configured incorrectly”. Thus, managing firewall complexity induces significant impact on budget increase for many enterprises. It has also been stated that “more than 40 % of the total IT budget of a \$1 billion-plus company going to human labor and IT operations accounting for 80–90 % of the budget”. Moreover, the static rule order in the firewall access control list can cause significant degradation in firewall

performance because most-frequently-matched rules could be placed at the end of the policy. Manual reordering based on traffic statistics will be inefficient due to the rapidly changing traffic dynamics.

This book provides a comprehensive and in-depth study for automated firewall policy analysis for designing, configuring, and managing distributed firewalls in large-scale enterpriser networks. The book presents methodologies, techniques, and tools for researchers as well as professionals to understand the challenges and improve the state of the art of managing firewalls systematically in both research and application domains. In Chap. 1, we present techniques based on set theory to automatically detect firewall anomalies (i.e., conflicts) in single or distributed firewalls, and to manage firewall configuration changes globally and consistently. Chapter 2 extends the analysis in Chap. 1 to consider access control list with encryption and authentication such as IPSec policies. This chapter shows the analytical power of modeling firewall and IPSec policies using Binary Decision Diagrams (BDD) to provide compositional verification of conflict-free network access control lists. In Chap. 3, we present a high-level service-oriented firewall configuration language (called FLIP) to enforce firewall security policies globally and correctly in a friendly manner. FLIP allows for defining high-level policies across multiple firewalls in a centralized fashion, which are then translated into access control rules and distributed to the appropriate firewalls with conflict-free guarantees. In Chap. 4, we describe a methodology and framework for designing optimal distributed firewall architecture that minimizes risk while satisfying business connectivity, user usability, and budget constraints. As a result, our presented technique offers a high-level top-down firewall design tool that determines the minimum number, locations, and configurations of firewalls that are required to enforce least-access (or risk) security property while satisfying connectivity, usability, and cost requirements. In each chapter, the book illustrates the concept, algorithm, implementation and case studies and evaluation for each present technique. Chapter 5 presents a practical technique for optimizing firewall performance by reordering firewall rules dynamically based on the real-time traffic statistics, in order to adaptively make the most-frequently-used rules matched first in the access control list. The chapter also presents a taxonomy and comparison of existing dynamic firewall policy configuration techniques based on on-line and off-line traffic analyses.

We would like to acknowledge the contribution of many people to the conception and completion of this book, particularly my colleagues Will Marrero, Radha Jagadeesan, James Riely, and Corin Pitcher for their contributions and comments on the original papers of this book, my students Hazem Hamed and Bin Zhang for their hard work and dedication in their research and running experiments used in this book, and Fadi Mohsen for his editorial help. We gratefully acknowledge NSF, Cisco, and Intel for their in-part support of this work. Finally, we would like to thank my families and our parents for their love and support.

Charlotte, NC, USA  
May 2014

Ehab Al-Shaer



# Acknowledgements

We gratefully acknowledge NSF, Cisco Systems, and Intel for their funding support of part of this research work.



# Contents

<b>1</b>	<b>Classification and Discovery of Firewalls Policy Anomalies</b>	<b>1</b>
1.1	Introduction	1
1.2	Firewall Background	3
1.3	Firewall Policy Modelling Using Set Theory	4
1.3.1	Formalization of Firewall Rule Relations	4
1.3.2	Firewall Policy Representation	5
1.4	Intra-firewall Anomaly Discovery	6
1.4.1	Intra-firewall Anomaly Classification	7
1.4.2	Intra-firewall Anomaly Discovery Algorithm	9
1.5	Inter-firewall Anomaly Discovery	11
1.5.1	Inter-firewall Anomaly Definition	11
1.5.2	Inter-firewall Anomaly Classification	12
1.5.3	Inter-firewall Anomaly Discovery Algorithm	16
1.6	Anomaly-Free Firewall Policy Editing	17
1.6.1	Rule Insertion	18
1.6.2	Rule Removal	19
1.7	Firewall Policy Advisor: Implementation and Evaluation	19
1.8	Summary	22
	References	23
<b>2</b>	<b>Modeling and Verification of Firewall and IPSec Policies</b>	
	<b>Using Binary Decision Diagrams</b>	<b>25</b>
2.1	Introduction	25
2.2	Modeling of Filtering Security Policies Using BDDs	27
2.2.1	IPSec Policy Components	27
2.2.2	Filtering Policy Representation	29
2.3	IPSec Intra-policy Analysis	31
2.3.1	Classification and Discovery of Access-List Conflicts	32
2.3.2	Classification and Discovery of Map-List Conflicts	36

2.4	IPSec Inter-policy Analysis .....	38
2.4.1	Classification and Discovery of Access-List Conflicts .....	38
2.4.2	Classification and Discovery of Map-List Conflicts .....	41
2.5	Usability and Performance Evaluation .....	43
2.6	Summary .....	46
	References .....	47
<b>3</b>	<b>Specification and Refinement of a Conflict-Free Distributed Firewall Configuration Language .....</b>	<b>49</b>
3.1	Introduction .....	49
3.2	FLIP System Architecture .....	51
3.2.1	Policy Designator .....	51
3.2.2	Policy Refinement and Translation .....	59
3.2.3	Results .....	64
3.2.4	Policy Distributor .....	65
3.3	A Case Study .....	67
3.4	Implementation and Evaluation .....	69
3.4.1	FLIP Usability .....	70
3.4.2	Scalability and Performance .....	70
3.4.3	The Number of Rules Generated by FLIP .....	71
3.5	Summary .....	72
	References .....	73
<b>4</b>	<b>Design and Configuration of Firewall Architecture Under Risk, Usability and Cost Constraints .....</b>	<b>75</b>
4.1	Introduction .....	75
4.2	System Model and Problem Formulation .....	76
4.2.1	Formal Problem Definition .....	77
4.2.2	Metrics and Parameters for Design Synthesis .....	78
4.2.3	FireBlanket Framework .....	79
4.2.4	Computational Complexity .....	83
4.2.5	Demilitarized Zones Creation .....	83
4.3	Heuristic Algorithms .....	86
4.3.1	Heuristic Algorithm for DFSP .....	86
4.3.2	Incremental Design Synthesis .....	89
4.4	Evaluation .....	90
4.4.1	Accuracy and Scalability of the Heuristic Algorithm .....	90
4.4.2	A Case Study .....	92
4.4.3	Incremental Updating .....	92
4.5	Summary .....	93
	References .....	94
<b>5</b>	<b>Dynamic Firewall Configuration Optimization .....</b>	<b>95</b>
5.1	Introduction .....	95
5.2	Background .....	97
5.3	Motivation for Dynamic Firewall Configuration .....	99

5.4	Taxonomy of Dynamic Firewall Configuration Techniques .....	100
5.4.1	Matching Optimization Techniques.....	100
5.4.2	Field Based Optimization .....	103
5.4.3	Early Rejection Optimization Techniques .....	104
5.4.4	A Comparative Study .....	106
5.5	Dynamic Firewall Rule Ordering (DRO) .....	110
5.5.1	Optimal Rule Ordering Problem .....	110
5.5.2	Heuristic ORO Algorithm .....	111
5.5.3	Implementation of Dynamic Rule Ordering .....	113
5.5.4	Performance Evaluation .....	119
5.6	Summary .....	125
	References .....	126
<b>Index</b>	.....	<b>129</b>