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

Printed on acid-free paper

Springer is part of Springer Science+Business Media (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 polices. 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 polices 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, particulary 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 Ehab Al-Shaer
May 2014

Acknowledgements

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

Contents