Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.134 – 137

RESEARCH ARTICLE

Detecting and Resolving Firewall Policy Anomalies Using Rule-Based Segmentation

Anbarasan.A[1], Balasubramani.G[2], Madhan.C[3], Naveenkumar.P[4], Mrs. N.S.Nithya[5]
[1,2,3,4] Department Of Computer Science and Engineering, Anna University Chennai, India
[5]Assistant Professor, Department Of Computer Science and Engineering,
K.S.R. College Of Engineering, Tiruchengode, India

[1] anburocks.009@gmail.com; [2] srdbala@gmail.com; [3] madhanvc8@gmail.com;
[4] nvnsft@gmail.com; [5] sachinnithya@yahoo.com

Abstract— In this paper we present an anomaly management framework for firewalls based on a rule-based segmentation technique to facilitate not only more accurate anomaly detection but also effective anomaly resolution. We represent an innovative policy anomaly management framework for firewalls, adopting a rule-based segmentation technique to identify policy anomalies and derive effective anomaly resolutions. .Based on this technique, a network packet space defined by a firewall policy can be divided into a set of disjoint packet space segments. Each segment associated with a unique set of firewall rules accurately indicates an overlap relation among those rules. We also introduce a flexible conflict resolution method to enable a fine-grained conflict resolution with the help of several effective resolution strategies with respect to the risk assessment of protected networks and the intention of policy definition.

Key Terms: - Segmentation; Correlation; Packet space; conflict; Distributed

Full Text: http://www.ijcsmc.com/docs/papers/April2013/V2I4201337.pdf