

io-port 05315612

Abedin, Muhammad; Nessa, Syeda; Khan, Latifur; Thuraisingham, Bhavani
Detection and resolution of anomalies in firewall policy rules.

Damiani, Ernesto (ed.) et al., Data and applications security XX. 20th annual IFIP WG 11.3 working conference on data and applications security, Sophia Antipolis, France, July 31-August 2, 2006. Proceedings. Berlin: Springer (ISBN 978-3-540-36796-3/pbk). Lecture Notes in Computer Science 4127, 15-29 (2006).

Summary: A firewall is a system acting as an interface of a network to one or more external networks. It implements the security policy of the network by deciding which packets to let through based on rules defined by the network administrator. Any error in defining the rules may compromise the system security by letting unwanted traffic pass or blocking desired traffic. Manual definition of rules often results in a set that contains conflicting, redundant or overshadowed rules, resulting in anomalies in the policy. Manually detecting and resolving these anomalies is a critical but tedious and error prone task. Existing research on this problem have been focused on the analysis and detection of the anomalies in firewall policy. Previous works define the possible relations between rules and also define anomalies in terms of the relations and present algorithms to detect the anomalies by analyzing the rules. In this paper, we discuss some necessary modifications to the existing definitions of the relations. We present a new algorithm that will simultaneously detect and resolve any anomaly present in the policy rules by necessary reorder and split operations to generate a new anomaly free rule set. We also present proof of correctness of the algorithm. Then we present an algorithm to merge rules where possible in order to reduce the number of rules and hence increase efficiency of the firewall.

Keywords: packet filters; network security; firewalls; anomalies; security policy
doi:10.1007/11805588.2