Firewall Redundancy Rules Filtering using Integrity Rules Checking

Zarina Dzolkhifli, Wan Nurul Safawati Wan Manan, Mohd Hafiz Mohd Hassin, Dhia Syafiqah Mohd Jaafar
Faculty of Computer System & Software Engineering, Universiti Malaysia Pahang, Malaysia
Corresponding author Email: dzarina@ump.edu.my
Received: 22 July 2017   Accepted: 26 September 2017

Securing your network plays a very crucial role in organizations, institutions, and personal home networks. A firewall is a first network defender that located at the entrance between a private network and the public network. Firewall had this job to monitor the arriving or leaving packet into and from the network, while making a decision whether to give permission or deny the packet based on its rules policy requirements. Commonly, there will be a large of firewall rules set are stored inside the firewall which each packet need to be compared sequentially with filtering until matching rules is found. A new strategy of integrity rules checking is proposed to reduce a firewall rules by analyzing the integrity among the firewall rules relationship to be checked for incoming packet. We believe that the proposed strategy will minimize the firewall rules set and undoubtedly optimize the time of firewall rules filtering.

Keywords: Secure Network, Firewall Rules, Integrity Rules, Relation.

1. INTRODUCTION

Recently, there has been increasing debate on security issues due to rapid advanced in technology which lead to people concerning on safety on their device. A secure network is any home, business, school, or another network that has security measures in place that help protect it from outside attackers. Network security consists of the regulation and standard practice that must be follow in order to avoid and monitor illegal access, misuse, modification, or denial of a computer network and network-accessible resources. Meanwhile, the practice to ensure the network secure to be controlled, firewall is needed to limits network access of incoming and outgoing traffic. It will decide whether to allow or block the specific traffics called packets through that firewall based on predetermined security rules.

Every organization need to have firewall to control the allowed and disallowed traffic. Each of the traffic differ requirement from organization.

Based on the requirement of the organization different policies or rules needed to create accordingly, which also must be change over the time. Inconsistency of rules changes from network administrator lead to mixture and different rule list is being created.

There are many types of rules in the network traffic which one is different form another. The networks traffic consist of many types of packets. Every network packet that arrived will be checked against firewall rules until the matching is established and the packet will follow the action specified by the rules. Usually firewall rules in the organization always bulk and complex, which will lead to the network administrator couldn’t manage the large firewall rules. These will lead to redundancies happen of the firewall rules, also been called anomalies. There are five anomalies which are shadowing anomaly, correlation anomaly, redundancy anomaly, generalization anomaly and irrelevance anomaly. Each of anomalies has their own task. For this research study, we focus only on redundancy anomaly.