Conflict Detection Using Rule-Based Segmentation Technique for Cooperative Firewall Optimization

Thangavel K S[1], Sudha S[2]

1Assistant Professor, Dr.APJ Abdul Kalam Centre for Research, Adhi College of Engineering & Technology, Chennai.
Email: thangavel.ks@gmail.com
[2]Assistant Professor, Adhi College of Engineering & Technology, Chennai.
Email:sudhatech19@gmail.com

Abstract

Firewalls have been widely used on the Internet for securing private networks. A firewall checks each incoming or outgoing packet to decide based on its policy whether to accept or discard the packet. Optimizing firewall policies is crucial for improving network performance. Former work on firewall optimization focuses on either interfirewall or intrafirewall optimization where the privacy of firewall policies is not a concern within one administrative domain. This paper probes interfirewall optimization across administrative domains for the first time. The key technical defiance is that firewall policies cannot be shared across domains because a firewall policy consist of confidential information and even potential security holes, which can be exploited by attackers. We propose the first cross-domain privacy-preserving cooperative firewall policy optimization protocol. Exactly, for any two adjacent firewalls belonging to two different administrative domains, our protocol can identify in each firewall the rules that can be removed because of the other firewall. In this paper Network Address Translation (NAT) modifies the IP address information in packets, it has serious consequences on the quality of Internet connectivity and desires careful attention to the details of its implementation. NAT implementations vary widely in their specific behavior in various addressing modes and their effect on network traffic. The specifics of NAT behavior is not commonly documented by vendors of equipment containing implementations.

Keywords- firewall policy, NAT, anomaly management framework, rule-based segmentation technique, VPN

INTRODUCTION

A novel anomaly management framework for firewalls to facilitate not only more accurate anomaly detection but also effective anomaly resolution based on a rule-based segmentation technique. 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.

LIMITATION OF PRIOR WORK

Prior work on firewall optimization focuses on either interfirewall optimization or intrafirewall optimization where the privacy of firewall policies is not a concern within one administrative domain. Firewall policy management is a challenging task due to the interdependency and complexity of policy rules. This is further exacerbated by the continuous evolution of system and network environments.

The process of configuring a firewall is error prone and tedious. Therefore, policy management effective mechanisms and tools are crucial to the success of firewalls. Existing policy analysis tools, such as Firewall Policy Advisor and FIREMAN, with the goal of detecting policy anomalies have been introduced. Firewall Policy Advisor only has the capability of detecting pair wise anomalies in firewall rules. FIREMAN can detect anomalies among multiple rules by analyzing the relationships between one rule and the collections of packet spaces derived from all preceding rules.

However, FIREMAN also has limitations in detecting anomalies. For each firewall rule, FIREMAN only examines all preceding rules but ignores all subsequent rules when performing anomaly analysis. In addition, each analysis result from FIREMAN can only show that there is a misconfiguration between one rule and its preceding rules, but cannot accurately indicate all rules involved in an anomaly.

Cross-Domain Inter-Firewall Optimization

To our best knowledge, no prior work focuses on cross domain privacy-preserving inter-firewall optimization. This paper represents the first step in exploring this unknown space. Specifically, we focus on removing inter-firewall policy redundancies in a privacy-preserving manner. Consider two adjacent firewalls 1 and 2 belonging to different administrative domains Net_1 and Net_2. Let FW_1 denote the policy on firewall 1's outgoing interface to firewall 2 and FW_2 denote the policy on firewall 2's incoming interface from firewall 1. For a rule r in FW_2, if all the packets that match r but do not match any rule above r in FW_2 are discarded by FW_1, rule r can be removed because such packets never come to FW_2. We call rule r an *inter-firewall redundant rule* with respect to FW_1. Note that FW_1 and FW_2 only filter the traffic from FW_1 to FW_2; the traffic from firewall 2's outgoing interface to firewall 1's incoming interface is guarded by other two separate policies. For simplicity, we assume that FW_1 and FW_2 have no intra-firewall redundancy as such redundancy can be removed using the proposed solutions [15], [17].