International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Review on an Improving Firewall Performance by Eliminating Redundancies in Access Control Lists (ACL)

Priyanka Padole[1], Purnima Selokar[2]

[1]Department of C.S.E., G. H. Raisoni Institute of Engineering and Technology for Women, Nagpur, Nagpur University, Nagpur, Maharashtra, India
[2]Department of C.S.E., G. H. Raisoni Institute of Engineering and Technology for Women, Nagpur, Nagpur University, Nagpur, Maharashtra, India

Abstract: ***For securing private network the firewall have been widely used. Based on the policy a firewall checks each incoming and outgoing packet whether to accept or reject the packet. Optimization of firewall policies is important to improve the performance of the network. There are two types of firewall intra firewall and inter firewall. The prior works on optimization of firewall is based on either intra firewall or inter firewall optimization where the privacy of firewall policies is not a concern within one administrative domain. This paper explores inter firewall optimization between two administrative domains. The firewall policies cannot be shared across domains because a firewall policy contains confidential data and potential security holes, which can be attacked by attackers which is a key technical challenge. In this paper, we introduce the commutative encryption for privacy preserving in firewall optimization. The main objective of the application is to remove the redundant rules from two firewall from two different administrative domains without disclosing the actual value of rules to each other. This method preserves the privacy of each firewall.***

Keywords: Firewall optimization, privacy preserving, Commutative Encryption

1. Introduction

Firewalls are used to secure private networks of businesses, organizations, institutions etc. A firewall is placed between internal LAN and external network. It checks each incoming and outgoing packet whether to accept or reject the packet. The decision is based on its policies. ACL is Address Control List which is a firewall policy usually specified as a sequence of rules, and each rule has a multiple predicate over source IP address, destination IP address, source port ,destination port and a decision is made for the packet that match the predicate. In a firewall policy the rules typically follow first match semantics where the decision of the first rule is the decision of the packet that matches in the policy. The firewall or interface is configured with each physical interface with two ACL's: one for filtering incoming packets and one for filtering outgoing packets. In this paper, we use firewall policies, firewall optimization and ACL's interchangeably.

1.1 Prior Work Limitation

Firewall optimization prior works focuses on either intra firewall optimization or inter firewall optimization within one administrative domain Intra firewall optimization means optimizing a single firewall. It is achieved by either removing redundant rules. Prior work on inter firewall optimization requires two firewall policies without any privacy protection, and thus can only be used within one administrative domain. However, it is common that two firewalls belong to different administrative domains where firewall policies cannot be shared with each other. Keeping firewall policies confidential is important for two reasons.

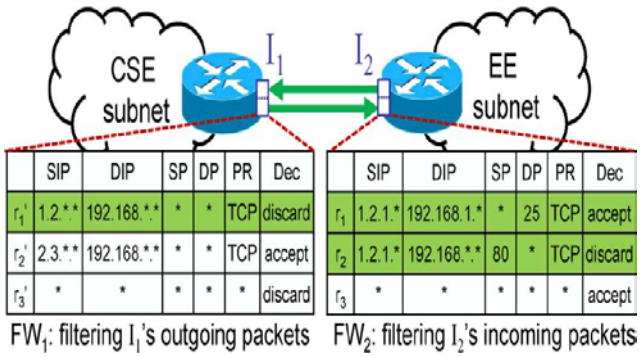

Figure 1: Example inter firewall redundant rules.

Fig. 1 illustrates inter firewall redundancy, where two adjacent routers belong to different administrative domains CSE and EE. The physical interfaces connecting two routers are denoted as I1and, respectively. The rules of the two firewall policies FW1 and FW2 that are used to filter the traffic flowing from CSE to EE are listed in two tables following the format used in Cisco Access Control Lists. Note that SIP, DIP, SP, DP, PR, and Dec denote source IP, destination IP, source port, destination port, Protocol type, and decision, respectively. Clearly, all the packets that match r1 and r2 in FW2 are discarded by r1' in FW1. Thus, r1 and r2 of FW2 are inter firewall redundant with respect to r1' in FW1.

2. Related Work

In paper "Cross-Domain Privacy-Preserving Cooperative Firewall Optimization", Fei Chen, Bezwada Bruhadeshwar, and Alex X. Liu [1] firewalls have been widely deployed on the Internet for securing private networks. A firewall checks each incoming or outgoing packet to decide whether to accept or discard the packet

based on its policy. Optimizing firewall policies is crucial for improving network performance. Prior work on firewall optimization focuses on either intra firewall or inters firewall optimization within one administrative domain where the privacy of firewall policies is not a concern. This paper explores inter firewall optimization across administrative domains for the first time. The key technical challenge is that firewall policies cannot be shared across domains because a firewall policy contains confidential information and even potential security holes, which can be exploited by attackers. In this paper, it propose the first cross-domain privacy-preserving cooperative firewall policy optimization protocol. Specifically, for any two adjacent firewalls belonging to two different administrative domains, the protocol can identify in each firewall the rules that can be removed because of the other firewall.

In paper "Complete Redundancy Removal for Packet Classifiers in TCAMs" Alex X. Liu, Member, IEEE, and Mohamed G. Gouda, Member, IEEE [2] packet classification is the core mechanism that enables many networking services on the Internet such as firewall packet filtering and traffic accounting. Using Ternary Content Addressable Memories (TCAMs) to perform high-speed packet classification has become the de facto standard in the industry. TCAMs classify packets in constant time by comparing a packet with all classification rules of ternary encoding in parallel. Despite their high speed, TCAMs suffer from the well-known interval expansion problem. As packet classification rules usually have fields specified as intervals, converting such rules to TCAM-compatible rules may result in an explosive increase in the number of rules. This is not a problem if TCAMs have large capacities. Unfortunately, TCAMs have very limited capacity, and more rules mean more power consumption and more heat generation for TCAMs. In this paper, it proposes to address the interval expansion problem of TCAMs by removing redundant rules in classifiers. This equivalent transformation can significantly reduce the number of TCAM entries needed by a classifier.

In paper "Privacy Preserving Collaborative Enforcement of Firewall Policies in Virtual Private Networks" A. X. Liu and F. Chen [7] the widely deployed Virtual Private Network (VPN) technology allows roaming users to build an encrypted tunnel to a VPN server, which, henceforth, allows roaming users to access some resources as if that computer were residing on their home organization's network. Although VPN technology is very useful, it imposes security threats on the remote network because its firewall does not know what traffic is flowing inside the VPN tunnel. To address this issue, it proposes VGuard, a framework that allows a policy owner and a request owner to collaboratively determine whether the request satisfies the policy. It first present an efficient protocol, called Xhash, which allows two parties, where each party has a number, to compare whether they have the same number, without disclosing their numbers to each other. Then, it presents the VGuard framework that uses Xhash as the basic building block.

In paper "All-Match Based Complete Redundancy Removal for Packet Classifiers in TCAMs" A. X. Liu, C. R. Meiners, and Y. Zhou [5] this is the first algorithm that attempts to solve first-match problems from an all-match perspective. It formally Packet classification is the core mechanism that enables many networking services on the Internet such as firewall packet filtering and traffic accounting. Using Ternary Content Addressable Memories (TCAMs) to perform high-speed packet classification has become the de facto standard in industry. TCAMs classify packets in constant time by comparing a packet with all classification rules of ternary encoding in parallel. As packet classification rules usually have fields specified as intervals, converting such rules to TCAM- compatible rules may result in an explosive increase in the number of rules. The interval expansion problem of TCAMs can be addressed by removing redundant rules in packet classifiers. This equivalent transformation can significantly reduce the number of TCAM entries needed by a packet classifier. This paper proves that the redundancy removal algorithm guarantees no redundant rules in resulting packet classifiers. These experimental results show that the redundancy removal algorithm is both effective in terms of reducing TCAM entries and efficient in terms of running time.

2.1 Redundancy Removal in Firewall

Prior work on intra firewall redundancy removal aims to detect redundant rules within a single firewall. It identified backward and forward redundant rules in a firewall. Later, Liu et al. pointed out that the redundant rules are incomplete and proposed two methods for detecting all redundant rules. Prior work on inter firewall redundancy removal requires the knowledge of two firewall policies and therefore is only applicable within one administrative domain.

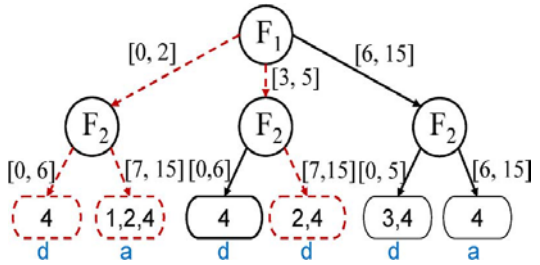

Figure 2: Identification of redundant rules in FW2

After single-rule and multi rule coverage redundancy detection, Net2 identifies the redundant non overlapping rules in FW2. Next, Net2 needs to identify which original rules are inter firewall redundant. As each path in the all-match FDD of FW2 of corresponds to a non overlapping rule, we call the paths that correspond to the redundant non overlapping rules redundant paths and the remaining paths effective paths. For example, in Fig. 2, the dashed paths are the redundant paths that correspond to nr1, nr2, and nr4 respectively. Finally, Net2 identifies redundant rules.

2.2 Proposed Methodology

There are two types of firewall. Intra firewall and inter firewall. In intra firewall the firewall the redundant rules are removed within the same administrative domain. The firewall belongs to only one administrative domain. And

the rules removed from the same administrative domain are called as intra firewall redundant rule removal.

In inter firewall; the removal of redundant rules can be carried out in two different administrative domains. The firewall belongs to two different administrative domains. It removes the redundant rules from each other's firewall without showing each other's actual policies.

3. Conclusion

This paper identified an important problem, cross-domain privacy-preserving inter firewall redundancy detection. We implemented our protocol in Java and conducted extensive evaluation. The System proposes a novel privacy-preserving protocol for detecting redundancy in firewall rules without revealing each other's policies. The application will implement the method for minimizing the difficult steps for removal of redundant rules in intra firewall and inter firewall. It helps to improve the speed and overall performance of the system.

References

[1] Fei Chen, Bezawada Bruhadeshwar, and Alex X. Liu "Cross-Domain Privacy-Preserving Cooperative Firewall Optimization" IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 21, NO. 3, JUNE 2013.
[2] A. X. Liu and M. G. Gouda, "Complete redundancy removal for packet classifiers in TCAMs," IEEE Trans. Parallel Distrib. Syst., vol. 21, no.4, pp. 424–437, Apr. 2010.
[3] A. X. Liu and F. Chen, "Collaborative enforcement of firewall policies in virtual private networks," in Proc. ACM PODC, 2008.
[4] J. Cheng, H. Yang, S. H. Wong, and S. Lu, "Design and implementation of cross-domain cooperative firewall," in Proc. IEEE ICNP, 2007.
[5] A. X. Liu, C. R. Meiners, and Y. Zhou, "All-match based complete redundancy removal for packet classifiers in TCAMs," in Proc. IEEE INFOCOM, 2008, pp. 574–582.
[6] O. Goldreich, "Secure multi-party computations," Working draft, Ver. 1.4, 2002.
[7] Z.Yang, S. Zhong, and R. N. Wright, "Privacy-preserving classification of customer data without loss of accuracy," in Proc. SIAM SDM, 2005, pp. 21–23