Policy Optimization and Anomaly Detection of Firewall

Akshay Dattatray Kachare[1], Geeta Atkar[2]

[1]M.E. Computer Network Student, GHRCEM Wagholi, University of Pune, Pune, India

[2]Asst. Professor in Computer Engineering Department, GHREM Wagholi, University of Pune, Pune ,India

Abstract: ***Firewalls are core entity in network security. Though, management of firewall rules/policies, mainly in multiple firewall enterprise networks, has grown to be a complex and error-prone task. A firewall always checks every incoming or outgoing packet to decide which packet should be accept or discard based on its policy. To avoid policy anomalies, it must be consider that firewall filtering rules must be written, well-organized and distributed suspiciously. These firewall policy anomalies might cause network vulnerability. Hence, insertion or modification of filtering rules in every firewall requires thorough intra-firewall and inter-firewall analysis. This analysis determines the correct rule position and order in the firewalls. In this paper, firstly, identification of all anomalies which may exist in a single or multiple firewall environments is addressed with various anomaly detection techniques. Secondly, this paper describes the cross-domain privacy-preserving protocol for cooperative firewall policy optimization. Specially, for several two neighbouring firewalls belonging to two different administrative domains, protocol which is define in this paper may identify in every firewall policies that can be eliminated because of the another firewall.***

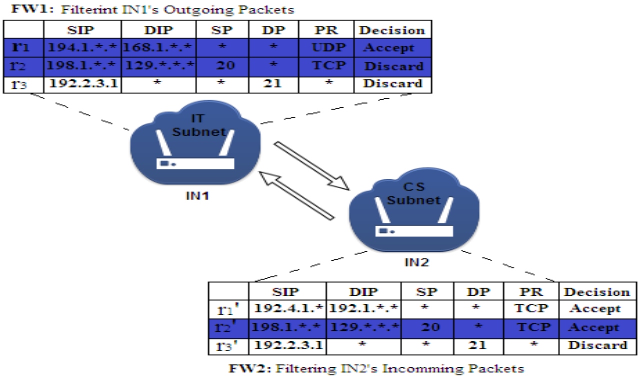
Keywords: firewall optimization; anomaly detection; privacy preservation

1. Introduction

a) Background

A firewall is the network element that controls the packets which are passed across the restrictions of a secured network derived from an explicit security policy. A firewall is frequently placed at the doorway in between a private network and the outside network with the intention that it can check every incoming or outgoing packet and make a decision whether to accept or discard that packet based on firewalls policy. A firewall policy is generally defined as a sequence of rules, called as Access Control List (ACL), and every rule has a predicate above numerous packet header fields (source IP address, destination IP address, source port (SP), destination port (DP), and type of protocol) and a decision (i.e., accept and discard) for the packets that match the predicate. Because of the rising threat of network attacks, firewalls have grown to be key elements not only in small-size and home networks but also in enterprise networks. Firewalls have been the limit protection for secure networks beside attacks and unauthorized traffic of packets in network by filtering out unwanted network traffic coming from or going to the secured network. The filtering conclusion is completely based on a set of ordered filtering rules set defined according to previously defined security policy desires.The number of rules used in a firewall considerably affects its throughput. It shows that as number of rules in firewall increases, a firewall policy significantly reduces the firewall throughput. Unfortunately, through the explosive increase of services set up on Internet, firewall rules are also increasing rapidly in size. Hence, optimization of firewall policies is crucial for improvement in network performance. Therefore, firewall optimization and anomaly detection becomes two important concepts.

b) Firewall Policy Optimization



FW1: Filterint IN1's Outgoing Packets

	SIP	DIP	SP	DP	PR	Decision
r1	194.1.*.*	168.1.*.*	*	*	UDP	Accept
r2	198.1.*.*	129.*.*.*	20	*	TCP	Discard
r3	192.2.3.1	*	*	21	*	Discard

	SIP	DIP	SP	DP	PR	Decision
r1'	192.4.1.*	192.1.*.*	*	*	TCP	Accept
r2'	198.1.*.*	129.*.*.*	20	*	TCP	Accept
r3'	192.2.3.1	*	*	21	*	Discard

FW2: Filtering IN2's Incomming Packets

Figure 1: Example inter-firewall redundant rules.

In particular, the focus must be on elimination of inter-firewall policy redundancies in purpose of firewall privacy-preserving To understand cross-domain firewall redundancies consider two adjacent firewalls 1 and firewall 2 belonging to diverse dministrative domains Net1 and Net2. Fig. 1 illustrates inter-firewall redundancy. In this fig. two neighboring routers which are belong to different administrative domains called IT and CS. The physical interfaces which connecting these two routers are declare as IN1 and IN2, respectively. The rules (policies) of the two firewall policies FW1 and FW2, which are used to sort out the traffic flow from IT to CS, are scheduled in two tables. The format used in table is followed as in Cisco ACL. Note that SIP denote source IP address, DIP destination IP address, SP denotes source port, DP denotes destination port, PR denotes protocol type, and Dec denotes decision, respectively. Obviously, each and every one packet which matches rule r_1 and r_2 in FW2 are discarded by r'_1 in FW1. As a result, rule r_1 and r_2 of FW2 both are inter-firewall redundant regarding r'_1 in FW1 [1].

c) Discovery of Policy Anomalies Within Firewall

With the worldwide Internet association, network security has gained large concentration in explore and industrial communities. Because of the rising threat of network attacks, firewalls have become important elements networks expanded in every section. Firewalls have been the leading edge protection for the secure networks against attacks and unauthorized. The filtering rules are defined according to predefined policy requirements for security, thus ordering of set of rules is also important task.

Even though use of firewall tools is an essential step in the direction of securing networks, the convolution or complexity of administration firewall policies might limit the efficiency of firewall security. In a particular firewall situation, the local firewall rule may contain intra-firewall anomalies, where the identical packet could match above one filtering rule. Furthermore, in distributed firewall situations, firewalls might also have inter-firewall anomalies, where individual firewalls in the equivalent path execute dissimilar filtering procedures on the equivalent traffic. Hence, the administrator have to give special interest not only to the entire rule relations in the similar firewall in order to find out the right rule order, but also to the entire relations among rules in different firewalls in order to verify the correct rule position in the correct firewall. As the number of filtering policies increases, the problem of adding a new policy or updating an existing one considerably increases.

The paper is organized as follows. In Section II review on Firewall redundancy, optimization and security techniques is addressed. In Section III Problem definition and proposed system architecture is explained. In section IV mathematical model is introduced. In Section V Conclusion is given.

2. Literature Review

2.1 Firewall Redundancy Removal

Previous work on intra-firewall redundancy was aims to removal detected redundant rules inside a single firewall, in [19] author presents two different algorithms for identifying and eliminating the two types of redundant rules. Paper [9] presents a set of mechanisms and algorithms to automatically find out anomalies in policy within centralized and distributed inheritance firewalls. In paper [18] author P. Gupta identified forward and backward redundant policies in a firewall. Afterward, Liu et al. [6] pointed out that the redundant policies identified by P. Gupta are not complete, and projected two different methods for detecting entire redundant rules [19], [6]. In the previous work [14] L. Yuan, et al. introduces FIREMAN, a static analysis tool for firewall designing and analysis, there was requirement for knowledge of two firewall policies for inter-firewall redundancy removal and hence is just applicable within single administrative domain [16], [14].

2.2 Firewall Policy Optimization

In paper [10], C. R. Meiners et al. proposed a systematic way known as the TCAM Razor. According to them this TCAM Razor system can be simply deployed because it does not need any modification to presented packet classification mechanisms, unlike numerous preceding range encoding mechanisms. In paper [13] Qunfeng Dong et al. addressed optimize packet classification technique configurations by describing semantically equivalent policy sets that lead to decrease number of TCAM entries when served as in hardware. Earlier research on firewall policy optimization focuses on both intra-firewall optimizations [4], [5], [6], [7] and inter-firewall optimization [16], inside single administrative domain where the firewall policies preservation is not disquiet. Intra-firewall optimization is defined as the optimization of a single firewall. It is obtained by whichever removing redundant rules [18] or rewriting rules [4], [5], [6], [7], and [10]. Earlier study on inter-firewall optimization needs two firewall policies with no any privacy protection, with therefore can only be used in one administrative domain. Though, in actuality, it is general that two firewalls which are belong to different administrative domains cannot shares firewall policies with each other. Maintaining firewall policies secret is very essential for two reasons. A firewall policy can have preservation holes that can be oppressed by attackers. Second, quantitative analysis have exposed that the majority firewalls are miss-configured and contain security holes [17].

2.3 Firewall Security Or Preservation

Previously existing anomaly detection techniques could not exactly point out the anomaly parts caused by a set of overlapping rules [16]. For example, Al-Shaer et al. [16] also reported that their firewall policies hold anomalies yet some administrators counting nine experts manage those policies. In addition, Wool [3] newly inspected firewall policies composed from different organizations and showed that all analysed firewall policies contain security flaws. Rule-based segmentation method, which adopts a BDD based data structure to characterize rules and carry out various set operations, to convert a list of policies of firewall into a set of disjoint network packet spaces has been recently mentioned to contract with some research issues such as network traffic measurement [11], firewall testing [15] and optimization [8]. The process of firewall configuration is very tedious and contains error. Thus, effectual techniques and tools for firewall policy management are vital to the achievement of firewalls. In recent times, policy anomaly detection has received a huge deal of interest [9], [16].

3. Proposed Work

3.1 Problem Definition

The main challenge is to propose a protocol which allows two contiguous firewalls to recognize the inter-firewall redundancy relating to each other without knowing each other’s policy. Whereas intra-firewall redundancy removal is already difficult task, inter-firewall redundancy removal by means of the privacy-preserving constraint is still harder. As well, not any of the earlier study has an important attempt to deal with anomalies in distributed firewalls. Consequently, in the paper consideration is on significant development in the area as it offers a new and complete framework to mechanize anomaly discovery and rule suppression in together centralized and distributed inheritance firewalls. Making of firewall policy relations is essential for analysis of the firewall policy and manipulative management techniques such as policy editing and anomaly discovery.

3.2 Proposed Architecure

The paper focuses on two key contributions. First, propose a privacy-preserving protocol for the detection of inter-firewall redundant rules in single firewall with respect to its adjacent firewall. Secondly, recognize all anomalies that might exist in a single-firewall or multi-firewall environment. In this there are different techniques for discovering these anomalies. Both functionalities are based on the rule-based segmentation technique.

3.2.1 Conflict detection and resolution,

Conflict resolution techniques is used to enable a fine grained resolution of conflict with the assist of numerous effectual decision strategies regarding the risk evaluation of protected networks and the purpose of policy description.

3.2.2 Redundancy discovery and removal.

This technique is used to detect redundancies in policies and removed to improve effective result.

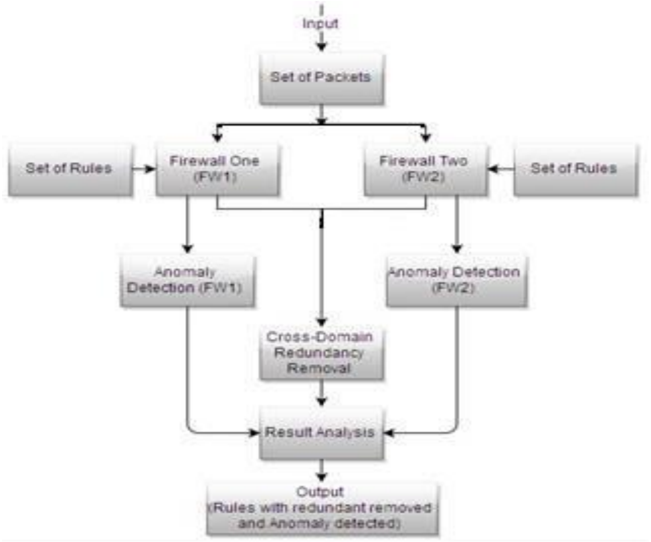


Figure 2: Proposed Architecture

3.3 Anomalies in Firewall Policies

Firewall policies are classified in to three different categories

Generalization-
If subset of packets is matched by the rule is also matched by subsequent rule but each rule taking different action then this rule is generalisation of one or set of previous rules.

Correlation-
If a one rule intersects with other rules and each rule defining a different actions then that rule correlated with other rules.

Redundancy-
In the same Firewall or same environment more than one rules are available and all those rules has the same effect then there is rule redundancy is defined.

3.4 Representation of Policy Anomaly

For effective anomaly detection, complete and accurate anomaly information diagnosis is represented in the Fig 3. When a more than one rule or number of rules interacts with each other, one overlapping relation may be associated with several rules. In anomaly detection technique there is possibility of one rule may overlap with multiple other rules and it and can be involved in other overlapping relations (overlapping segments).

Figure 3 shows a representation of policy anomalies. We can easily determine which rules are covered by a which segment, and which segments are associated with a which rule. we can notice that a conflicting segment *s*5, which points out a conflict, is related to a rule set consisting of three conflicting rules *r*3, *r*4 and *r*5 (highlighted with a horizontal red rectangle), and a rule *r*3 is involved in three segments *s*5, *s*6 and *s*7 (highlighted with a vertical red rectangle). Our representation provides a better understanding of policy anomalies to system administrators with an overall view of related segments and rules.

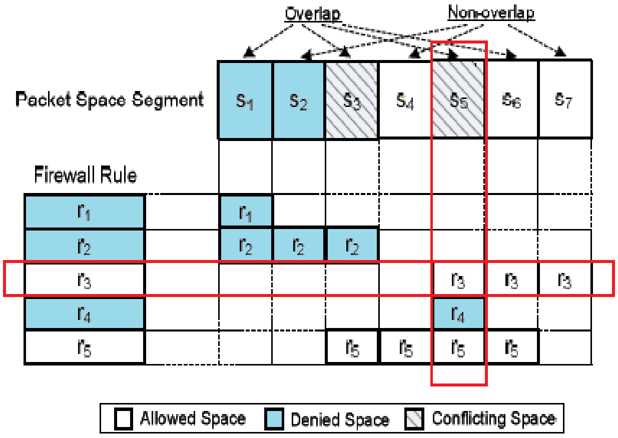


Figure 3: Representation of Policy Anomaly

4. Mathematical Model

Input: S = {FW1, FW2, r, M(r_i), R(r_i) }
Where,

S is a set,
FW1 indicates Firewall 1,
FW2 indicates Firewall 2,
r indicates rules,
M(r_i) indicates set of packets match with rule r_i
R(r_i) indicates set of packets match with set r_i but not match with r_j above r_i where j<i.

Process:

Privacy inter-firewall redundancy Removal
Convert each firewall to an equivalent sequence of non-overlapping rules.

$$M(nr) = R(nr)$$

Where, nr = non overlapping rules.

Firstly, this paper explains the privacy-preserving protocol for comparing a number and a range. To make sure whether a number from FW2 is in between the range [a′, b′] from FW1, where, a' and b' are number from FW1, use a method similar to the prefix membership verification.

Prefix conversion

In this convert [a′, b′] to a minimum number of prefixes, denoted as S([a′, b′]), whose union corresponds to [a′, b′]. For instance, S([11, 15])={1011, 11**}.

Prefix family construction

This generates entire the prefixes which contains a with a itself. This set of prefixes is known as the prefix family of number a, denoted as F(a).

Let bit length of a is equal to k. The prefix family F(a) consists of k +1 prefixes where the ith prefix is obtained by replacing the last i−1 bits of a by ∗. For instance, as the binary representation of 12 is 1100, then F(12)={1100, 110*, 11**, 1***, ****}. It is not difficult to prove that a ∈ [a′, b′] if and only if F(a) ∩ S([a′, b′]) ≠ ∅.

Prefix numericalization

This converts the prefixes obtained in the previous steps to existing numbers such that one can encrypt them in the next step. For this the prefix numericalization technique is used [19].

Given a prefix $b_1b_2 \cdot\cdot\cdot b_k{*}\cdot \cdot\cdot{*}$ of w bits, first insert 1 after b_k. The bit 1 represent a divider (saperator) between $b_1b_2 \cdot\cdot\cdot b_k$ and* · · ·*. Then replace every ∗ by 0. For instance, 11** is converted to 11100. If the prefix does not contain *s, place 1 at the end of the prefix. For example, 1100 is converted to 11001.

Comparison

This checks whether a ∈ [a′, b′] by checking whether F(a) ∩ S([a′, b′]) ≠ ∅, which boils down to checking whether two numbers are equal. To do this checking use commutative encryption in a privacy-preserving method. Specified a number x and two encryption keys K1 and K2, a commutative encryption is a function that satisfies the condition ((x)K1)K2 = ((x)K2)K1 , i.e., encryption with key K1 first and then K2 is equivalent to encryption with key K2 first and then K1.

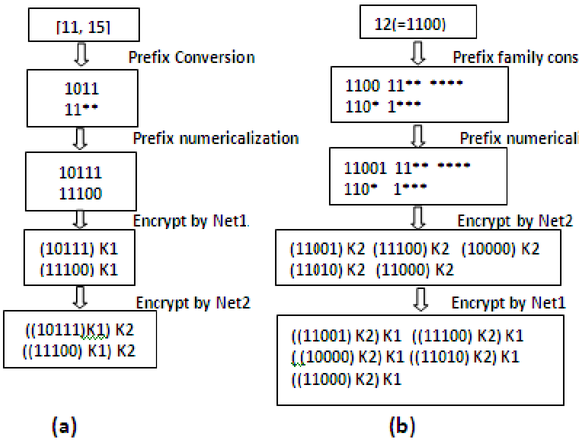


Figure 4: Prefix membership verification.

5. Experimental Setup

Input:

Set of Packets: Dataset consist of packets. Following table I shows the experimental setup of set of packets which are used for practical analysis.

SIP- Source Internet Protocol
DIP-Destination Internet Protocol
SP-Source Port
DP-Destination Port

Table 1: Packet Pattern

Sr. No.	Packet				
	SIP	***DIP***	***SP***	***DP***	***Protocol***
1	1.1.139.239	1.1.236.8	22	32	TCP
2	1.1.139.143	1.1.236.8	6077	3923	UDP

Set of Rules: Following table shows the example of set of rules which are used for practical analysis

Table 2: Rules

Sr. No	**Packet**					
	SIP	***DIP***	***SP***	***DP***	***Protocol***	***Action***
R1	1.1.139.*	1.1.236.*	22	*	TCP	Accept
R2	1.1.139.143	1.1.*.*	*	*	UDP	Discard

6. Result

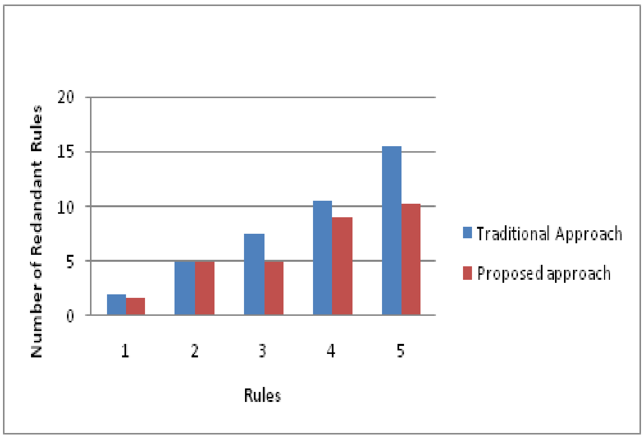


Figure 5: Number of redundant rule

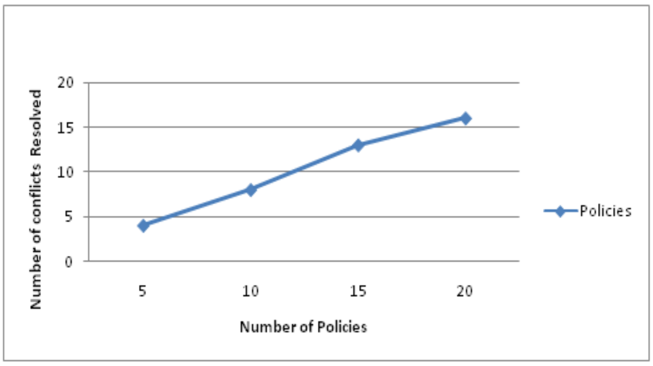


Figure 6: Average Conflict Detection and Resolution

7. Conclusion

The paper represents two important mechanisms like two Cooperative firewall Optimization and Firewall security. As a result it is analyzed that the security and optimization issue are resolved effectively in the paper. The Cooperative Firewall is used to remove redundancies between two adjacent firewall policies with protecting privacy of policies. And also firewall anomaly detection techniques make secure each firewall.

References

[1] Fei Chen, Bezawada Bruhadeshwar, Alex X. Liu, "A Cross-Domain Privacy-Preserving Protocol for Cooperative Firewall Optimization," 2013.

[2] Hongxin Hu, Gail-Joon Ahn, and Ketan Kulkarni, " Detecting and Resolving Firewall Policy Anomalies", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, 2012.

[3] A. Wool, "Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese," IEEE Internet Computing, vol. 14, no. 4, pp. 58–65, 2010.

[4] C. R. Meiners, A. X. Liu, and E. Torng. Bit weaving: A non-prefix approach to compressing packet classifiers in TCAMs. In IEEE ICNP, pages 93–102, 2009.

[5] C. R. Meiners, A. X. Liu, and E. Torng. Topological transformation approaches to optimizing tcam-based packet processing systems. In ACM SIGMETRICS, pages 73–84, 2009.

[6] A. X. Liu, C. R. Meiners, and Y. Zhou. All-match based complete redundancy removal for packet classifiers in TCAMs. In IEEE INFOCOM, pages 574–582, 2008.

[7] A. X. Liu, E. Torng, and C. Meiners. Firewall compressor: An algorithm for minimizing firewall policies. In IEEE INFOCOM, 2008.

[8] G. Misherghi, L. Yuan, Z. Su, C.-N. Chuah, and H. Chen, "A general framework for benchmarking firewall optimization techniques," IEEE Transactions on Network and Service Management, vol. 5, no. 4, pp. 227–238, Dec. 2008.

[9] J. Alfaro, N. Boulahia-Cuppens, and F. Cuppens, "Complete analysis of configuration rules to guarantee reliable network security policies," International Journal of Information Security, vol. 7, no. 2, pp. 103–122, 2008.

[10] C. R. Meiners, A. X. Liu, and E. Torng. TCAM Razor: A systematic approach towards minimizing packet classifiers in TCAMs. In IEEE ICNP, pages 266–275, 2007.

[11] L. Yuan, C. Chuah, and P. Mohapatra, "ProgME: towards programmable network measurement," ACM SIGCOMM Computer Communication Review, vol. 37, no. 4, p. 108, 2007.

[12] Y.-K. Chang. Fast binary and multiway prefix searches for packet forwarding. Computer Networks, 51(3):588–605, 2007.

[13] Q. Dong, S. Banerjee, J. Wang, D. Agrawal, and A. Shukla. Packet classifiers in ternary CAMs can be smaller. In ACM SIGMETRICS, pages 311–322, 2006.

[14] L. Yuan, H. Chen, J. Mai, C.-N. Chuah, Z. Su, and P. Mohapatra. Fireman: a toolkit for firewall modeling and analysis. In IEEE S&P, pages 199 – 213, 2006.

[15] A. El-Atawy, K. Ibrahim, H. Hamed, and E. Al-Shaer, "Policy segmentation for intelligent firewall testing," in 1st Workshop on Secure Network Protocols (NPSec 2005), 2005.

[16] Ehab S. Al-Shaer and Hazem H. Hamed, "Discovery of Policy Anomalies in Distributed Firewalls", IEEE INFOCOM 2004.

[17] A. Wool. A quantitative study of firewall configuration errors. IEEE Computer, 37(6):62–67, 2004.

[18] P. Gupta. Algorithms for Routing Lookups and Packet Classification. PhD thesis, Stanford University, 2000.

[19] A. X. Liu and M. G. Gouda. Complete redundancy removal for packet classifiers in tcams. IEEE TPDS, in press

Author Profile

Akshay D. Kachare received the B.E. degree in Computer Science and Engineering from Satara College of Engineering, Shivaji University and currently student of the second year M.E. in Computer Network from GH Raisoni College of Engineering and Management, Wagholi, University of Pune.

Prof. Geeta Atkar working as Asst. Professor in Computer Engineering department in GH Raisoni College of Engineering and Management, Wagholi, University of Pune.