IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN : 2278-0661, p-ISSN : 2278-8727
PP 42-46
www.iosrjournals.org

A Survey On Various Techniques For Effective Optimization Of Cross Domain Network Protocol For Redundancy Removal In Firewall Policies

Swati Kobal, Sucheta More, Shraddha Kumbhar, Jyoti Sonawane
Department of Information Technology, JSPM'S Rajarshi Shahu College of Engineering, Tathawade, Pune-411033

Abstract: *In today's progressing world, internet is used as a medium for almost every operation. Firewalls are a piece of code that checks the data flow from start to end. Firewalls are extensively implemented to prevent unauthorized access to concealed networks and secure them. Firewalls are made of set of rules or policies. Based upon those applied policies a firewall can approve or decline the data packet by scaning them. If the number of rules is increased rapidly which are turns degrades the throughput of a firewall and also results to complex firewall policies. Optimizing these policies is crucial for improving the network performance. There is a need to come up with a better solution to solve this problem. Undoubtedly the following discussed techniques are extremely good. A collaborative approach using few of them can be a better solution.*

Index Terms: *Cross domain firewall optimization; privacy; protocol optimization; redundancy removal.*

I. Introduction

A firewall is acting as an interface amongst a network and one or additional exterior networks. It helps apply the safe policies of network by deciding which packets to approved and which to block, on the bases of some set of rules decided by the network supervisor. Any mistake in defining the rules may compromise the system security by allowing undesired traffic to pass through or block the anticipated traffic. The rules when defined physically often results in a set that contains incompatible, jobless or overshadowed rules, which generates irregularities in the firewall policy. A network firewall protects a computer network from unlawful access. Network firewalls can be hardware strategies, software packages, or they can be a group of both. System firewalls protects an internal processer network such as home network or school network in contradiction of hateful access from the outdoor. Network firewall might also be arranged to limit entrance to the outside network of interior users. Preceding work on intra firewall severance removal aims to sense redundant rules within only firewall Gupta recognized backward and onward redundant instructions in a firewall pointed out that the fired. Rules identified by Gupta are imperfect and planned two approaches for detecting all non-functioning rules Prior work on interfirewall non-functioning removal requires the information of two firewall strategies and therefore is only appropriate within one administrative domain. Given research work on collaborative firewall implementation in VPNs imposes firewall policies finished encoded VPN tunnels deprived of leaking the confidentiality of the remote network's rule. The difficulties of collaborative firewall execution in VPNs and confidentiality preserving entomb firewall optimization are fundamentally different. The previous focuses on imposing a firewall policy over VPN tunnels in a confidentiality preserving method, whereas the latter emphases on removing interfirewall dismissed rules without exposing their guidelines to each further. Second, their requirements are different. The former conserves the privacy of the isolated network's procedure, whereas the latter conserves the privacy of both strategies.

II. System Architecture:

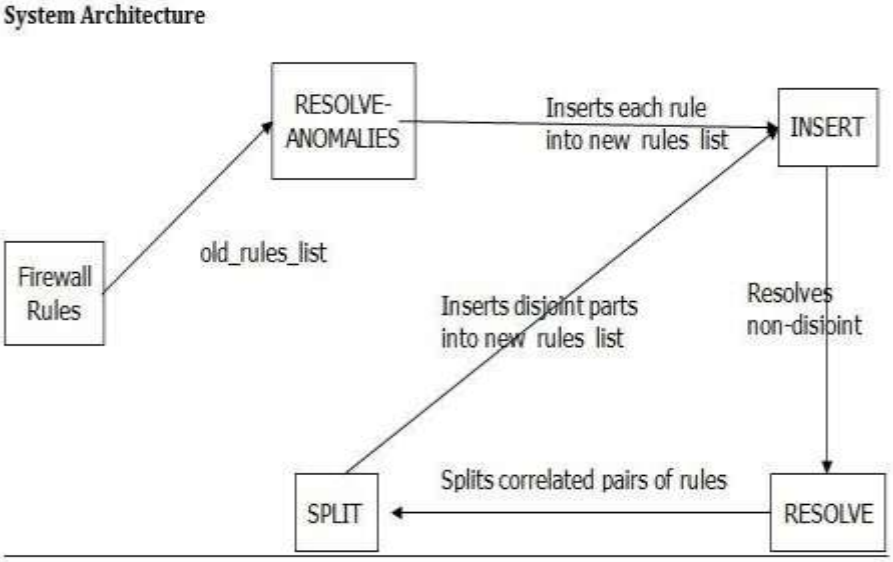

Fig 1. Firewall system flow architecture

Recently Implemented Techniques Helps In Reducing The Firewall Rules

Information Sharing Across Private Databases [1]

Sharing of information is an increasing need across various entities, such that no information part from the answer to the query is revealed i.e. no more information than necessary is revealed from each database to the other databases. Here notion of minimal information sharing across private databases, and protocols for the intersection, equijoin, intersection size, and equijoin size are described. The current techniques use the concept of third party. The main parties give the data to a "trusted" third party and have the third party to do the computation. However, the third party has to be completely trusted. The level of trust required is too high for this solution to be acceptable. The solution for the above problem is avoiding the use of third party. The main parties will directly execute a protocol, which is designed to guarantee that they do not learn any more than they would have learnt they given the data to a trusted third party and got back the answer. The parties follow the protocol properly and in special cases they may keep a record of all the intermediate computations and received messages, and scan the messages to try to know about extra information. A protocol for computing equijoin size leaks some information of which tuples joined based on the distribution of duplicates.

Interfirewall optimization across various administrative domain for enabling security and privacy preserving [2]

Firewall protects Network security, which checks in-out packets against a set of defined rules. Hence, rule management decides the overall performance of the firewall. For example, the performance can be decreased when there are deviations in firewall rule. The deviation may happen when two sets of firewall rules clashes or their decision parts are both an adoption and a rejection occurring at the same time. Firewall optimization focuses on either inter-firewall or intra-firewall optimization within organisation domain. Here the privacy of firewall policies is not a concern. Interfirewall examine optimization process in which cooperative computation between the two firewall without any party disclosing its policy to the other party. Then the proficient challenge is that firewall policy has be distinct across domains. Because a firewall policy contains secret information and even possible security holes. This can be accessed by attackers. Interfirewall redundant rule are used to defeat the previous difficulties. Also propose the first cross domain cooperative firewall (CDCF) policy optimization protocol. Implementing the protocol in java and conducting extensive evolution we can

remove many of redundant rules. However it is much complex, reducing complexity of protocol needs to be helpful in increasing the performance of firewall.

Firewall Optimization in Inter-Administrative Domains [3]

In the existing system mainly focus on reducing the number of rules, while neglecting the priority based decisions of the rules. Firewalls use first-match semantics; as significance, if the rules with a highest Risk-value are not up in the rule order, it affects the throughput of the firewall. An Author proposed a inter domain privacy preserving protocol for detecting inter firewall redundant rules in one firewall with respect to another firewall. And provide security using cryptography techniques. Optimizing firewall is essential for improve network performance. Similar way, Security and privacy are two major concerns in supporting users across administrative domains. In the proposed system, not only decrease the number of rules in the firewall ACL, but also reorders firewall rules based on risk -value of the rules. Thus, the proposed method recognizes redundant rules and remove the redundant the number of rules. Also, to provide updating rules the proposed method reorders the firewall rules according to their risk-value. The proposed approach used risk assessment to determine risk-value of the rule. When a lower value rule r2 conflicts with a higher value rule r1 that has a dissimilar action, say that r2 depends on r1. Reordering of rules should result in rules that are equivalent to the original ones in the net effect. It directly affects the throughput of the firewall.

Structured firewall design [4]

A firewall is a security guard or a wall placed at the entry point of a private network and the public network such as Internet so that it will check all incoming and outgoing packets. The task of a firewall is to inspect every packet and decide whether to accept or discard the packet. Previously this task is specified by a sequence of rules, where rules often conflict. This approach ensures that every packet has at least one matching rule in a firewall. Designing a firewall directly as a sequence of rules suffers from following problems: the consistency problem, completeness problem, and compactness problem.

Here a new method is proposed called structured firewall design, consisting two steps. First, designs a firewall using a firewall decision diagram instead of a sequence of conflicting rules. And second, a program converts the firewall decision diagram into a compact, and functionally equivalent, sequence of rules.

This method solves the consistency problem because structure of firewall decision diagram is conflict-free. It solves the completeness problem because the designer considers syntactic requirements of a firewall decision diagram that covers all types of traffic. It also solves the compactness problem because in the second step two algorithms are used to combine rules together, and one algorithm to remove redundant rules.

Firewall design method begins when a user specifies a FDD f. The consistency and completeness properties of f can be verified automatically based on the syntactic requirements of an FDD. After the FDD specifications, it moves from five steps. In the first step, FDD Reduction algorithm is applied to user specified FDD. In the second step FDD Marking algorithm is applied to resultant FDD where each non terminal has one outgoing edge that is marked all. In the third step FDD Generation algorithm is applied. In the fourth step is Firewall compaction Algorithm is applied to resultant firewall. In the fifth step Firewall simplification Algorithm is used. Then the final result of all the above five steps will be simple firewall that is equivalent to user specified FDD.

Diverse Firewall Design [5]

This paper shows the conversion of firewalls to FIREWALL DECISION DIAGRAM which is a key part in the comparison phase. In comparison phase comparison of two firewall find out all the distinctiveness between them, then each distinctiveness is further investigated. The technical challenge shown in the method of diverse firewall design is how to discover all the distinctiveness between two given firewalls. They had presented a series of three efficient algorithms for solving this problem:(1) an algorithm for constructing an equivalent ordered firewall decision diagram which is an acyclic and directed graph drawn from a sequence of rules, (2) a shaping algorithm for converting two ordered firewall decision diagrams to become non-overlapping without changing their semantics, and (3) a comparison algorithm for detecting all the distinctiveness between two non-overlapping firewall decision diagrams. This helps to allow the two firewalls to detect the redundant rules in a privacy preserving manner and also in turn optimize the rules by removing them.

Dynamic Rule based Interfirewall Optimization using Redundancy Removal Algorithm [6]

Firewall is a system used to secure private networks. Firewall analyzes every packet and decide whether to accept or discard it. This is decided by policy which is a set of rules. Our work focuses on inter-firewall optimization over different administrative domain without accessing the privacy policies. As Internet-based applications has grown widely, the number of rules in firewalls has been increasing in a rapid rate. It reduces the network performance. A dynamic rules estimation algorithm is proposed to limit number of rule of validation for every session. However, an error in a firewall either discloses secret information from its network. Also interrupts proper communication between its network and the Internet. The redundancy removal algorithm reduces the redundant rules in the firewall with multi-rule coverage. The optimization process involves fair computation between the two firewalls by keeping privacy of the each party firewall policies separate. The algorithm used will avoid the rules overhead and also increases the efficiency by optimizing the firewall. The algorithm requires no additional online packet analyzing overhead and the offline analyzing time is lower than a few hundred seconds to reduce the redundancy and to improve the firewall operation.

Redundancy removal of rules for optimizing firewall [7]

In this paper Author proposed a new technique to remove redundant rules present in interfirewall without knowing other firewall policies. In this technique proposed framework is work concurly and impose the firewall policies. This solution is more effective than cross domain cooperative firewall because it is slower than other techniques. Linear searching of packet processing work leisurely than firewall decision diagrams. Our all prior work is focus on the optimizing either interfirewall or intrafirewall policies within one administrative domain. Intra firewall optimization works on one firewall and they can achieve firewall optimization either by removing redundant rule or by rewriting of these redundant rules. But going on this premises requires one firewall disclose its private policies with other. But practically it is impossible to share the policies with firewall which are in different domain. He proposed a cross domain optimization technique with privacy preserving in cooperative environment. To accomplished this they proposed two techniques: (1) They gave a novel approach based protocol which detect interfirewall redundancy removal in one firewall. (2) They implemented the protocol which gave good result in removing of redundant rules. But while designing this protocol they consider threat model in which they first convert each firewall into non overlapping rule sequence. After they work on range comparison for privacy preservation. Secondly,they detect single rule redundancy and multi rule redundancy detection and at last they remove the redundant rules from firewall.This method is applicable to few thousands of rules redundancy get removed and preserving the firewall privacy is the main drawback because no two firewalls need to tell the policies. In this analysis author present the firewall optimization from one firewall to second firewall and reverse direction is also possible**.**

Privacy Preserving Clustering [8]

In this paper, they have present the design and analysis of a privacy-preserving *k*-means clustering algorithm, where clustering causes the grouping of similar data and the important privacy-preserving *k*-means causes computation of cluster. For that they have presented two protocols for privacypreserving computation of cluster means are:

1) oblivious polynomial evaluation based protocol and
2) homomorphic encryption based protocol.

They have a JAVA implementation of these algorithm. Using that implementation, they have performed a thorough evaluation of privacy-preserving clustering algorithm on three data sets. Their evaluation demonstrates that privacy-preserving clustering is feasible, i.e., homomorphic-encryption based algorithm finished clustering a large data set in approximately 66 seconds. This gives an idea to maintain the privacy while computing the rules of firewall without exploring them to another firewall.

III. Conclusion

Firewall security, requires proper management in order to provide proper security services. Hence we required a unique privacy-preserving protocol for identifying redundancy in firewall rules. If the rule exists, a cross domain cooperative firewall protocol can be used to increase network performance. But, the network performance slumps down if the rule does not exist. And the protocol will try to improve the network performance to safeguard firewall policies.

Undoubtedly the techniques discussed above are extremely useful, a next step in this path would be to compare and evaluate all these various mechanisms by creating sets of data to come up with a collaborative approach

which will provide security along with increase in response time of communication and processing much better when compared with previous methods.

References

[1] Rakesh Agrawal, Alexandre Evfimievski,Ramakrishnan Srikant "Information Sharing Across Private Database International Journal of Research in Engineering and Technology.
[2] Kalaivani.M, Rohini.R "Interfirewall optimization across various administrative domain for enabling security and privacy preserving" Scientific Journal Impact Factor (SJIF): 1.711
[3] P.Venkata Ramalakshmi, Mr. Ch.Vijaya Krishna "Firewall Optimization in Inter-Administrative Domains" Technologies ISSN .
[4] Ehab S. Al-Shaer and Hazem H. Hamed "Discovery of Policy Anomalies in Distributed Firewalls" {ehab, hhamed}@cs.depaul.edu.
[5] Mohamed G. Gouda, Alex X. Liu, "Structured firewall design".
[6] Alex X. Liu Mohamed G. Gouda "Diverse Firewall Design" IEEE RANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 19, NO. 9, SEPTEMBER 2008.
[7] P.R.Kadam, V.K. Bhusari "Review On Redundancy Removal Of Rules For Optimizing Firewall" International Journal of Research in Engineering and Technology.
[8] S. Jha, L. Kruger, and P. McDaniel "Privacy Preserving Clustering" International Journal of Research in Engineering and Technology.
[9] Y.-K. Chang, "Fast binary and multiway prefix searches for packet forwarding," *Comput. Netw.*, vol. 51, no. 3, pp. 588–605, 2007.
[10] J. Brickell and V. Shmatikov "Privacy-preserving graph algorithms in the semi honest model," in Proc. ASIACRYPT,2010, pp. 236-252.
[11] J. Cheng, H. Yang, S.H. Wong, and S. Lu, "Design and implementation of cross-domain cooperative firewall," in Proc. IEEE ICNP,2007, pp.284.