International Journal of Electronics Communication and Computer Engineering
Volume 6, Issue (5) Sept., NCRTCST-2015, ISSN 2249–071X

3rd National Conference on Research Trends in Computer Science & Technology NCRTCST-2015

A Novel Privacy-Preserving Protocol for Detecting Interfirewall

Poreddy Suvarna
M.Tech Student, Department of CSE
CMR College Of Engineering and Technology,
JNTUH Kandlakoya, Medchal, Ranga Reddy,T.S, India.

Mr. S. Siva Skandha
Assistant Professor, Department of CSE
CMR College Of Engineering And Technology,
JNTUH Kandlakoya, Medchal, Ranga Reddy, T.S, India

***Abstract* – Firewalls are broadly utilized as a part of web for giving security and protection. A firewall basing on its arrangement checks each approaching parcel and choose whether to acknowledge or decay the bundle. The firewall arrangement got to be main consideration in enhancing the nature of the system execution. This paper studies interfirewall enhancement crosswise over regulatory spaces interestingly. The imperative specialized test is that firewall approaches can't be shared crosswise over areas on the grounds that a firewall strategy contains private data and even potential security openings, which can be misused by assailants. In this paper, we propose the first cross-area protection safeguarding agreeable firewall arrangement streamlining convention. In particular, for any two contiguous firewalls fitting in with two diverse regulatory areas, our convention can recognize in every firewall the principles that can be evacuated in light of the other firewall. The enhancement procedure includes agreeable calculation between the two firewalls with no gathering revealing its strategy to the next.**

***Keywords* – Firewall optimization, privacy, Firewall Policy, Cooperative Firewall, Administrative Domains.**

INTRODUCTION

A firewall is a system security framework that channels the verifying so as to ape and active system movement the information parcels and choose it is possible that they ought to be permitted or disposed of, based upon the guideline set. A firewall works as an obstruction between a protected and trusted interior system and different systems (e.g., the Internet) that is thought to be unsecured. A few PCs incorporate programming based firewalls with a specific end goal to shield over dangers from people in general Internet which is of tremendous utilization. Numerous switches that pass information between systems contain firewall and in this way numerous firewalls can perform fundamental steering capacities which are identified with that specific system and its capacity. As far as PC security, a firewall is a bit of programming which screens the activity over the system. A firewall has an arrangement of guidelines which are connected to every last bundle. The guidelines choose if a bundle can be acknowledged or in the event that it is disposed of. When all is said in done, a firewall is set between two or more systems in which one is secured and the other are unsecure. A firewall is regularly put at the passageway between a private system and the outer system with the goal that it can check every approaching or active parcel and chooses whether to permit or dispose of the bundle based upon its strategy.

A firewall approach is for the most part determined as an arrangement of tenets, called Access Control List (ACL), and every standard has a predicate over numerous parcel header fields (i.e., source IP, destination IP, source port, destination port, and convention sort) and a choice (i.e., acknowledge and dispose of) for the bundles that match the predicate. A firewall can't forward a parcel until examination has wrapped up. Along these lines, it will bring about extra dormancy to bundles. With restricted cradle size, constant parcel examining time might likewise bring about the firewall to drop bundles genuinely. The execution of a firewall ought not be relieved when under assault; generally its motivation would have been crushed. Here we utilize the terms firewalls, firewall approaches, and ACLs tradable. The quantity of tenets in a firewall is dependably conversely corresponding to its throughput. The guidelines in a firewall approach ordinarily take after the first-coordinate technique where the choice of the tenet is the choice for the parcel matches over the arrangement.

II. LITERATURE SURVEY

a) Discovery of Policy Anomalies in Distributed Firewalls:

Firewalls are core elements in network security. However, managing firewall rules, particularly in multi-firewall enterprise networks, has become a complex and error-prone task. Firewall filtering rules have to be written, ordered and distributed carefully in order to avoid firewall policy anomalies that might cause network vulnerability. Therefore, inserting or modifying filtering rules in any firewall requires thorough intra- and inter-firewall analysis to determine the proper rule placement and ordering in the firewalls. We identify all anomalies that could exist in a single- or multi-firewall environment. We also present a set of techniques and algorithms to automatically discover policy anomalies in centralized and distributed legacy firewalls. These techniques are implemented in a software tool called the "Firewall Policy Advisor" that simplifies the management of filtering rules and maintains the security of next-generation firewalls.

b) Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese:

The first quantitative evaluation of the quality of corporate firewall configurations appeared in 2004, based on Check Point Firewall-1 rule sets. In general, that survey indicated that corporate firewalls often enforced poorly written rule sets. This article revisits the first survey. In addition to being larger, the current study includes configurations from two major vendors. It also introduces a firewall complexity. The study's findings validate the 2004 study's main observations: firewalls are (still) poorly configured, and a rule -set's complexity is (still) positively correlated with the number of detected configuration errors. However, unlike the 2004 study, the current study doesn't suggest that later software versions have fewer errors.

c) Complete Analysis of Configuration Rules to Guarantee Reliable Network Security Policies:

The use of different network security components, such as firewalls and network intrusion detection systems (NIDSs), is the dominant method to monitor and guarantee the security policy in current corporate networks. To properly configure these components, it is necessary to use several sets of security rules. Nevertheless, the existence of anomalies between those rules, particularly in distributed multi-component scenarios, is very likely to degrade the network security policy. The discovery and removal of these anomalies is a serious and complex problem to solve. In this paper, we present a complete set of mechanisms for such a management.

d) Fast and Scalable Conflict Detection for Packet Classifiers:

Packet filters provide roles for classifying packets based on header fields. High speed packet classification has received much study. However, the twin problems of fast updates and fast conflict detection have not received much attention. A conflict occurs when two classifiers overlap, potentially creating ambiguity for packets that match both filters. For example, if Rule 1 specifies that all packets going to CNN be rote controlled and Rule 2 specifies that all packets coming from Wal-Mart be given high priority, the roles conflict for traffic from Wal-Mart to CNN. There has been prior work on efficient conflict detection for two dimensional classifiers. However, the best known algorithm for conflict detection for genial classifiers is the naive $O(N^2)$ algorithm of comparing each pair of rules for a conflict. In this paper, we describe an efficient and scalable conflict detection algorithm for the general case that is significantly faster. For example, for a database of 20,000 roles, our algorithm is 40 times faster. than the naive implementation. Even without considering conflicts, our algorithm also provides a packet classifier with fast updates and fast lookups that can be used for stateful packet filtering.

e) Fireman: A Toolkit for Firewall Modeling and Analysis:

Security concerns are becoming increasingly critical in networked systems. Firewalls provide important defense for network security. However, mis-configurations in firewalls are very common and significantly weaken the desired security. This paper introduces FIREMAN, a static analysis toolkit for firewall modeling and analysis. By treating firewall configurations as specialized programs, FIREMAN applies static analysis techniques to check misconfigurations, such as policy violations, inconsistencies, and inefficiencies, in individual firewalls as well as among distributed firewalls. FIREMAN performs symbolic model checking of the firewall configurations for all possible IP packets and along all possible data paths. It is both sound and complete because of the finite state nature of firewall configurations. FIREMAN is implemented by modeling firewall rules using binary decision diagrams (BDDs), which have been used successfully in hardware verification and model checking. We have experimented with FIREMAN and used it to uncover several real misconfigurations in enterprise networks, some of which have been subsequently confirmed and corrected by the administrators of these networks.

III. LIMITATION OF PRIOR WORK

Prior work focuses on intrafirewall optimization or interfirewall optimization within one administrative domain, where privacy of firewall policies is not considered. In intrafirewall it contains only the single firewall, where optimization is done and in interfirewall it includes two firewalls but they are in one network and optimization is done without any privacy preserving. But no prior work focuses on interfirewall optimization between more than one administrative domains and major concern is that firewall policies are not known to each other so that privacy is preserved. Also in the previous work numbers of rules in the firewall are not the concern. The number of rules in a firewall significantly affects its throughput.

IV. EXISTING SYSTEM

Prior work on firewall optimization focuses on either intra firewall optimization, or inter firewall optimization within one administrative domain where the privacy of firewall policies is not a concern. Firewall policy management is a challenging task due to the complexity and interdependency of policy rules. This is further exacerbated by the continuous evolution of network and system environments. The process of configuring a firewall is tedious and error prone. Therefore, effective mechanisms and tools for policy management 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 mis-configuration between one rule and its preceding rules, but cannot accurately indicate all rules involved in an anomaly.

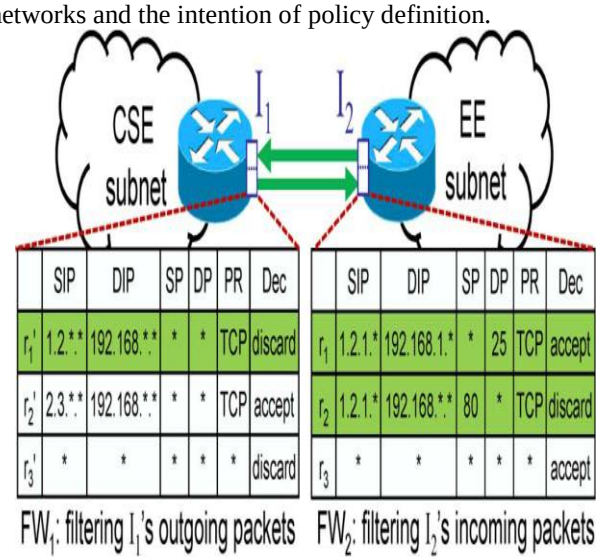
Drawbacks:

The number of rules in a firewall significantly affects its throughput.

- 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.
- 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

V. Proposed System

In this paper, we represent a novel anomaly management framework for firewalls based on a rule-based segmentation technique to facilitate not only more accurate anomaly detection but also effective anomaly resolution. 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 (either conflicting or redundant) 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.



Advantages:

- In our framework conflict detection and resolution, conflicting segments are identified in the first step.
- Each conflicting segment associates with a policy conflict and a set of conflicting rules. Also, the correlation relationships among conflicting segments are identified and conflict correlation groups are derived
- Policy conflicts belonging to different conflict correlation groups can be resolved separately, thus the searching space for resolving conflicts is reduced by the correlation process.
- Efficient in detection of anomalies.
- 92 percent of conflicts can be resolved by using our FAME tool.
- The proposed system resolves conflicts in each conflict correlation group independently.

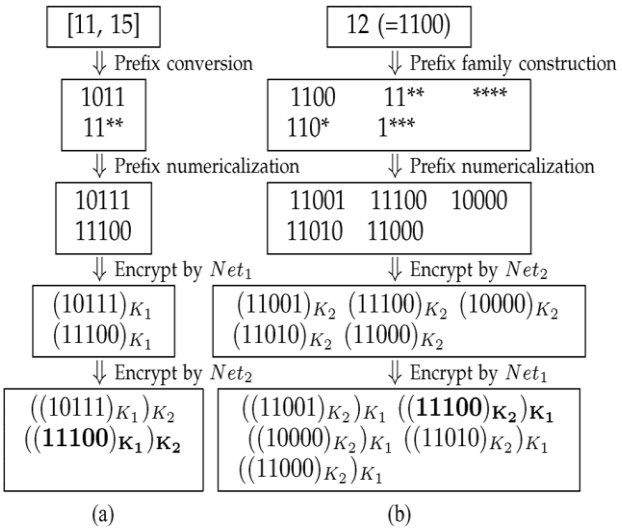
VI. Techniques and Algorithm

1. Firewall Redundancy Removal:

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

2. Collaborative Firewall Enforcement in Virtual Private Networks (VPNs):-

Prior work on collaborative firewall enforcement in VPNs enforces firewall policies over encrypted VPN tunnels without leaking the privacy of the remote network's policy The problems of collaborative firewall enforcement in VPNs and privacy-preserving interfirewall optimization are fundamentally different. First, their purposes are different. The former focuses on enforcing a



firewall policy over VPN tunnels in a privacy-preserving manner, whereas the latter focuses on removing interfirewall redundant rules without disclosing their policies to each other. Second, their requirements are different. The former preserves the privacy of the remote network's policy, whereas the latter preserves the privacy of both policies

Algorithm : Computation of the set of largest rules
Input: non-overlapping rules .
Output: The set of all the largest rules
Initialize , ;
while has been changed do
for every two rules , in do
compute the largest rules from and ;
add the largest rules to ;
for each rule in do
if there is a rule in such that
then
remove from ;
return ;

VII. IMPLEMENTATION

a. Correlation of Packet Space Segment:

The major benefit of generating correlation groups for the anomaly analysis is that anomalies can be examined within each group independently, because all correlation groups are independent of each other. Especially, the searching space for reordering conflicting rules in conflict resolution can be significantly lessened and the efficiency of resolving conflicts can be greatly improved.

b. Action Constraint Generation:

In a firewall policy are discovered and conflict correlation groups are identified, the risk assessment for conflicts is performed. The risk levels of conflicts are in turn utilized for both automated and manual strategy selections. A basic idea of automated strategy selection is that a risk level of a conflicting segment is used to directly determine the expected action taken for the network packets in the conflicting segment. If the risk level is very high, the expected action should deny packets considering the protection of network perimeters.

c. Rule Reordering:

The solution for conflict resolution is that all action constraints for conflicting segments can be satisfied by reordering conflicting rules. In conflicting rules in order that satisfies all action constraints, this order must be the optimal solution for the conflict resolution.

d. Data Package:

When conflicts in a policy are resolved, the risk value of the resolved policy should be reduced and the availability of protected network should be improved comparing with the situation prior to conflict resolution based on the threshold value data will be received in to the server.

VIII. CONCLUSION

Hence by using cross-domain cooperative privacy preserving protocol we have identified and remove the redundant rules in firewall 1 with respect to firewall 2 without disclosing policies to each other. But again we have identified and remove the redundant rules in the same way in firewall 2 with respect to firewall 1. As redundant rules are removed the network performance is improved. The response time is also improved and the communication cost and processing time is reduced.

FUTURE ENCHANTEMENTS

Prior work on firewall optimization focuses on either intra firewall optimization, or interfirewall optimization within one administrative domain where the privacy of firewall policies is not a concern. Firewall policy management is a challenging task due to the complexity and interdependency of policy rules. This is further exacerbated by the continuous evolution of network and system environments. The process of configuring a firewall is tedious and error prone. Therefore, effective mechanisms and tools for policy management are crucial to the success of firewalls .In our framework conflict detection and resolution, conflicting segments are identified in the first step. Each conflicting segment associates with a policy conflict and a set of conflicting rules. The correlation relationships among conflicting segments are identified and conflict correlation groups are derived. Policy conflicts belonging to different conflict correlation groups can be resolved separately, thus the searching space for resolving conflicts is reduced by the correlation process.

REFERENCES

[1] nf-HiPAC, "Firewall throughput test," 2012 [Online].Available:http://www.hipac.org/performance_tests/results.html
[2] R. Agrawal, A. Evfimievski, and R. Srikant, "Information sharing across private databases," in Proc. ACM SIGMOD, 2003, pp. 86–97.
[3] E. Al-Shaer and H. Hamed, "Discovery of policy anomalies in distributed firewalls," in Proc. IEEE INFOCOM, 2004, pp. 2605–2616.
[4] J. Brickell and V. Shmatikov, "Privacy-preserving graph algorithms in the semi-honest model," in Proc. ASIACRYPT, 2010, pp. 236–252.
[5] Y.-K. Chang, "Fast binary and multiway prefix searches for packet forwarding," Comput. Netw., vol. 51, no. 3, pp. 588–605, 2007.
[6] J. Cheng, H. Yang, S. H.Wong, and S. Lu, "Design and implementation of cross-domain cooperative firewall," in Proc. IEEE ICNP, 2007, pp. 284–293.
[7] Q. Dong, S. Banerjee, J. Wang, D. Agrawal, and A. Shukla, "Packet classifiers in ternary CAMs can be smaller," in Proc. ACM IGMETRICS, 2006, pp. 311–322.
[8] O. Goldreich, "Secure multi-party computations," Working draft, Ver. 1.4, 2002.
[9] O. Goldreich, Foundations of Cryptography: Volume II (Basic Applications). Cambridge, U.K.: Cambridge Univ. Press, 2004.

[10] M. G. Gouda and A. X. Liu, "Firewall design: Consistency, completeness and compactness," in Proc. IEEE ICDCS, 2004, pp. 320–327.
[11] M. G. Gouda and A. X. Liu, "Structured firewall design," Comput. Netw., vol. 51, no. 4, pp. 1106–1120, 2007.
[12] P. Gupta, "Algorithms for routing lookups and packet classification," Ph.D. dissertation, Stanford Univ., Stanford, CA, 2000.
[13] A. X. Liu and F. Chen, "Collaborative enforcement of firewall policies in virtual private networks," in Proc. ACM PODC, 2008, pp. 95–104.
[14] A. X. Liu and M. G. Gouda, "Diverse firewall design," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 8, pp. 1237–1251, Sep. 2008.