REVIEW ON REDUNDANCY REMOVAL OF RULES FOR OPTIMIZING FIREWALL

P.R.Kadam[1], V.K. Bhusari[2]

[1]*PG Student, Department of Computer Engineering, BSIOTR, Wagholi, Maharashtra, India*
[2]*Assistant Professor, Department of Computer Engineering, BSIOTR, Wagholi, Maharashtra, India*

Abstract

Firewalls are such a system, designed to prevent unauthorized internet access to or from private networks. A firewall checks all incoming and outgoing traffic by analyzing the data packets and then by using different policies determines whether to accept or discard the traffic. It is important to boost the firewall policies to improve network performance. The performance of the firewall is critical in enforcing and administrating security when network is under attack. Growth of the Internet with the increasing civilization of the attacks is placing stiff demands on firewall performance. It has been noticed that firewall policies are badly outlined and very erroneous. So it is very important to increase the performance of the firewall with good design of policies. Firewall performance can be optimized using various techniques like, optimizing firewall rules, optimization using data mining techniques. Firewall policies cannot be shared across domains as it contains confidential information and also various security holes are also present. Virtual private network integrated with mutual firewall protect the external network from encipher drift freight with minimum cost. Previous work gives emphasis on cross-domain privacy-preserving interfirewall optimization by removing interfirewall policy redundancies with preserving privacy. This privacy preserving protocol identifies rules of two adjoining firewalls resting between separate domains. This protocol sustains no more online packet process cost and offline process time is also less [16].

Keywords: *Civilization, Redundancies, Adjoining, Privacy, Stiff.*

----------***----------

1. INTRODUCTION

Firewalls are largely used by various institutions, corporate world, personal network etc. So, securing firewalls become a need which will in turn secure our network. In this internet era firewall are settled at entry point of our private network which provides us very secure access to and from network. Which means it will check each and every packet which is coming to the network or packet which is leaving network. According to policies designed network will accept or deny the packets. Designing the policies means designing the sequence of rules and based on this rules firewall will perform its functions. We call these rules as access control list. This list is organized in rule table. Each rule has condition on packet header fields and has decision whether to accept or deny the packet. When packet comes to system according to first match of rule in the policies decision will be taken. Previous researches were dedicated to the developing of coherent data structures. This data structures can speed up the technique of checking of firewall rules when packet get arrive at firewall. Various researches also develop such data structures. Another way of research in firewall design was developing high level languages which will specify firewall rules [3].

Previous work on firewall shows that discovery of policy anomalies [1], how firewall design becomes consistent, complete and compact [13], cross domain cooperative firewall designing and implementing [15], Imposition of firewall policies in Collaborative environment in Virtual Private Networks [14], optimizing the rules of firewall [11], intra and inter firewall optimization with privacy preserving [7], [10], [1], [5]. Our Work is related to the literatures that scrutinize how redundant rules of firewall get reduced to get good performance of firewall. Previous work also give focus on inter firewall optimization without protecting firewall policies. As firewall policies has the security information and contains private information so securing firewalls from attackers is a stringent demand. Various works has been done to address the solution of this problem. First solution shows that, designing and implementing cross domain firewall in cooperative manner in collaborative environment of networks with enforcing each other's firewall rules with preserving the privacy of each other[15]. Second solution shows firewall optimization with privacy preserving and removing redundant rules. In this solution author propose privacy preserving protocol which will detect redundant rules. This model considers each firewall will follow self-protocols correctly but try to disclose policy of other firewall [16].

1.1 Firewall Security Issues

Various technical challenges found during work of firewall security.

- The key problem faced by today's firewall is to outline a protocol that will allow two adjoining firewall to identify the own redundancy with respect to each other without considering the policy of other firewall [8].
- Redundancy removal without knowing the each other's policy even becomes harder [15].

- While designing the threat model we have to consider that two firewalls are not revealing the policies of each other. But the malicious participant may visit.[15]
- As previous work require knowing each other's policies and will get implemented in one administration [15].

2. LITERATURE SURVERRY

2.1 Anomaly Detection Techniques

E. Al-Shaer and H. Hamed [1], describes an approach which provides us advisor of firewall policies. This advisor provides various techniques which purifies and protect firewalls from anomalies of rules. They actually formally define the anomalies in firewall policies in both centralized and distributed firewalls. They also proved that these the only conflicts that could exists in the policies. The algorithm proposed by them detects rules anomalies in inter and intra firewall in the network.

2.2 Traffic Aware Firewall Optimization

Traffic aware firewall optimization techniques proposed by Acharya, S., Wang, J., Zihui Ge; Znati, T.F., Greenberg [2].Framework produced by them upgrade the operation cost of firewalls. They have design the tool set which examines and analyze both rules of multidimensional firewall and traffic logs which will construct the optimal solution which gives us firewall rules based on the traffic characteristics got observed. System administrator configures firewall of organization according to security requirement. Configuring a firewall is critical task.

To extend the above research Qi Duan and Ehab Al-Shaer[3],gives us Traffic-Aware Dynamic policy management of firewall techniques with application. They classify the firewall policies into two categories first is base on goals that matches optimization and previously rejected optimization scheme. Technique of matching optimization tries to reduce time of matching regular normal network traffic and in previous rejection they create minimum policy set of constraint rules which efficiently filter the denied traffic.

As we know in firewall technology packet filtering plays an important rule, so if we increase firewall performance then we are able to get good speed of the packet filtration. Hazem Hamed and Ehab AlShaer [6], found that today's network current techniques are not considering the traffic flow to optimize the data structure search and this technique results in higher complexity work. They proposed a novel approach in which they utilize traffic characteristics to get good performance of firewall in filtering firewall policies.

Considering firewall security issues Lihua Yuan ,Jianning Mai;Zhendong Su, Hao Chen;Chen-Nee Chuah, Prasant Mohapatra[5], designs FIREMAN which is analysis toolkit for analyzing and modeling firewall. FIREMAN investigating on firewall configuration like a special program it applies analysis technique that will check misconfiguration like violation of policies, instability and less efficiency. This technique will apply on both like on single individual firewall or distributed firewalls. While designing this model they have used binary decision diagram and got successful results in implementation of firewall and checking of model. This method gives extensibility and full benefit on all IP packets and data paths. As their algorithms are complete and impressive toolkit has not contain any falsely things. While performing it requires low memory, working of toolkit i\s fast and scalable.

To give extension to above work Alex X. Liu, and Mohamed G. Gouda [8], arrange the rules in upward and downward direction of redundant rules. They propose two algorithms to remove these two types of redundant rules. And in third stage proving of classifier without redundant rules, and at last they apply the algorithms on both synthetic and real life classifiers. Their works get divided into three categories:

1. In first they uses TCAM modification in this modification they changes TCAM hardware circuit.
2. In the second stage they work on range encoding which requires processing of each and every packet but not requires change of hardware circuit.
3. Third stage work on TCAM modification of process it does not require any of the above processing.

An experimental result shows us that algorithm requires only few seconds to remove thousands of redundant rules. This can be used in rule based system like in artificial intelligence system.

Many networking services have core content as packet filtering through firewall and accounting of traffic. So it becomes a standard to use ternary content addressable memories to perform packet classification. By doing comparison of rules with all rules in constant time it performs the classification of packet. Chad R. Meiners Alex X. Liu Eric Torng [7],found that this TCAM suffers from range expansion problem and have limited capacity so more rules requires more power use and heat generation is more. To address this problem they proposed TCAM razor which look into how number of entries get less production of TCAM entries. This technique is very effective and efficient to work. They gave a practical algorithm approach to solve problem in which they use following way. First they draws decision diagram then uses dynamic programming g and then redundancy removal of rules. In first step they convert packet classifier into reduced version of decision diagrams. In second they by using dynamic programming limits the number of prefixes bounded with outgoing edge of each non terminal node. After this generate rules from this decision diagram and at last remove the redundancies between rules.

2.3 Optimizing Firewalls With Changing Designs

A quantitative study about firewall configuration errors by A. Wool [4], shows that various well configured firewalls get affected by different worms and configuration files

rather we can call it as rule sets are highly sensitive so keep limited rule set complexity of firewalls. Install a new dedicated firewall which protects our subnet instead of connecting with main firewall which requires adding more rules.

To get good performance from firewall Tihomir Katic, Predrag Pale [11], developed logic to optimize firewall rules. As network administrator set the firewall configuration he have to check the newly designed rule with existing rules but in large organization as there is large design of rule it is not possible to check the new rule with existing rule. Foe less experienced administrator finds more difficulty to do this. It will work on detecting same rules and merge them accordingly. They notice difficulty in finding the rule redundancies called anomalies as each rule contains another rule in sequence which got matched to all packets. In this research they use log rules and other parameters related to rules instead of using IP address, protocol and ports. They have developed software called FIRO which a command tool related to firewall work with IP tables of LINUX Platform. This software creates rile list in each and every step of optimization process.

As we are using firewalls to protect our private network so design is important issue. Erroneous design of firewall creates a security hole which allows malicious users to disturb network. This will results in tremendous recovery. A. X. Liu and M. G. Gouda [9], observed that firewall policies are poorly outlined with many errors in it. So they propose a diverse firewall design which consists of three stages. In the first stage they give firewall policy specification and requirement to more teams and these teams separately design policies in their own way. These teams create different versions of outlined firewall policies. In second stage whatever design versions created by teams are get compare to find redundancies in policies. Detection of such policies is a comparison phase. And at last phase these redundancies get resolved and design of firewall get generated and all teams have agreed upon the design of firewall. But to get efficient work done in the removing of redundancies they proposed three different algorithms.

A. X. Liu, E. Torng, and C. Meiners, [10], give us the firewall compressor which is a framework. This framework appreciably reduces the rules in firewall which will keep our firewall semantics unchanged. They have proposed this model with three contributions in first they use dynamic programming and gives optimal solution for compressing one dimensional firewall. Second approach gives a systematic compression of multidimensional firewall. And they have evaluated results and achieve compression up to 52.3%.

2.4 Integer Programming Language

By using integer programming language Misherghi, G., Lihua Yuan, Zhendong Su, Chuah, Chen-Nee, Hao [12], proposed detailed constitution of firewall optimization. This work produce optimal reordered rule set which is equal to the original rule set. The model constructed by them considers complex communication between rules present in firewall and depend on the space present in packet given by rules. They evaluate this heuristic approach and got the good results about the firewall optimization. While implementing the model they use heuristic approach and proposed a divide and conquer algorithm for getting good results.

Firewalls should be compact, complete and consistent and this is proposed by M. G. Gouda and A. X. Liu [13]. They proposed first method to design firewall rules to be consistent, compact and complete. Consistent means nothing but order of rules should be correct, completeness means every packet should satisfy at least one rule in the firewall and firewall without redundant rules is compactness. Their methods starts with first designing the firewall decision diagram we can call it as FDD and then they have develop five algorithms to generate FDD, to reduce and clarify the selected rules. Because of this FDD we can easily check firewall's compactness, completeness and consistency. This method supposes that for each visiting packet firewall will assign two decisions either to accept or to deny.

2.5 Cross Domain Firewall Optimization

Roaming user uses tunnels for keeping privacy of communication for example virtual private networks, but this traffic is not properly checked and controlled by foreign network firewall due to its encrypted nature. Because of this various attacks may happen. To prevent these two methods can be used in first, users release their network to foreign network and in second case this network may release firewall rules to tunnel end. But practical implementation of these two methods is not possible. To resolve this problem J. Cheng, H. Yang, S. H.Wong, and S. Lu [14], proposed a solution to this problem. In this they give us a cross domain co-operative firewall in virtual private networks applies firewall policies to virtual private networks tunnel which is encrypted with keeping security of remote network's firewall policies. They actually distribute firewall's primitive rules across network and their result shows that this technique protects outside network from ciphered tunnels.

By using same techniques as above Alex X. Liu Fei Chen [15], proposed us a new technique to remove redundant rules present in interfirewall without knowing each other's policies. They proposed a type of protection framework in which they work collaboratively and enforce the firewall policies. This solution is better than proposed Cross Domain Cooperative Firewall (CDCF) because, the encryption technique used in CDFC is slower than three magnitude order proposed by Alex X. Liu Fei[15],Linear searching of packet processing takes more time than using firewall decision diagrams. So this technique is better than previous one.

As all prior work give focus on optimizing interfirewall or optimizing intrafirewall in one administrative domain without considering privacy metrics of the policies. Intra firewall optimization works on single firewall in which we can achieve firewall optimization either by redundancy

removal or by rewriting 0of these redundant rules. But working on this basis requires one firewall reveal its policies with others or one firewall should know another firewall's policies. But in practical it is not possible firewall present in different domains not share anything. As firewall contains security hole keeping firewall policies confident is very important. So, Fei Chen, Bezawada Bruhadeshwar, and Alex X. Liu [16] proposed a cross domain optimization technique with privacy preserving in cooperative environment. To achieve this they proposed two techniques in first they gave a novel approach and designed a protocol which detect interfirewall redundancy removal in one firewall, and in second part they implemented the protocol and got good result in removing of redundant rules. But while designing this protocol they consider threat model that they consider two firewalls are semi honest. They first convert each firewall into non overlapping rule sequence. After this they work on range comparison for privacy preservation. In next step they detect single rule redundancy and multi rule redundancy detection and at last they remove the redundancy in firewall. This technique is applicable to few thousands of rules up to 2000 rules redundancy get removed and preserving the firewall privacy is the main issue because none of the two firewalls need to tell the policies. In this research they show the firewall optimization from one firewall to second firewall and reverse direction is also possible.

Fei Chen, Bezawada Bruhadeshwar, and Alex X. Liu, got the tremendous results after evaluating this protocol. They evaluate this Protocol to get good efficiency on real and synthetic firewall. They conducted evaluation on five group of firewall. Each will examine the five important fields like source IP, destination IP, source and destination port, source and destination protocol. The number of rules ranges from one to many and for to do encryption they have used Pohling-Hellman algorithm [16]. Protocol designed by them is efficient for processing and comparing real and synthetic firewall. Also it is efficient for communication cost happen between real and synthetic firewall. In this way they have preserve the privacy of rules and also worked on optimization of firewall in two different administrative domains. The system architecture considered in this survey is as follows.

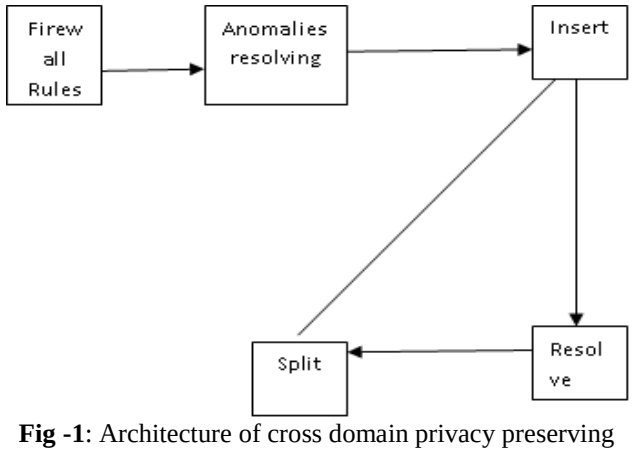

Fig -1: Architecture of cross domain privacy preserving Cooperative Firewall

Mustafa, U. Masud, M.M. , Trabelsi, Z. , Wood, T. , Al Harthi, Z.[17], proposed a data mining techniques for improvement of firewall. As each packet get compared with filtering rules, time required to do this is linearly depends upon the number of firewall filtering rules. So if high bandwidth is required firewall rules can become bottleneck for large firewall with thousands of rules. The technique proposed by authors predicts rule which most like to be match the packet instead of comparing it with rules. Due to this firewall processing work time required by firewall gets reduced and firewall performance gets enhanced.

3. IMPLICATIONS OF THIS SURVEY

This investigation contribute to literature on improving firewall perform by removing redundancies in policies setting which is important angle. Currently various techniques get introduce to optimize firewall technique. According to redundancies present rules get removed and we got tremendous results as we can remove up to 2000 rules according to [16].But in this technique malicious user attacks are not take into account. This survey shows us semi trusted models are used to optimize the firewall but one firewall can disclose its policies to other firewall. There is no any guarantee that there is no such an employee present who tries to disclose the private rules of firewall. In another case someone can observe input sequence and try to know the policies. So we can design such a system which will give us privacy preserving optimization of firewall in which we can use trusted models. We can use various encryption techniques to encrypt the policies of the firewalls and use them or we can keep some digital signatures techniques. So by using security concepts we can secure our policies. For malicious employees we can keep them password generation so we get password for each and every user so to stop revealing the policies to another firewall. So we can extend the work to design a firewall that will give us Reordering of rules according to hit rates.

4. CONCLUSION

After this survey we come to know that lot of work has been done in field of firewall security and firewall optimization. Inter and intra firewall optimization is provided with various techniques. Firewall optimization is done by using removing redundant rules. To keep secrecy of private rules encryption technique is used in both one administrative domain and in two different administrative domains. Optimization of firewall can be done by using removing redundancies in rule or by rewriting the rules. Keeping policies privacy of firewall is very important so later work focuses a work on this. We can extend this work which will work on the finding the malicious user present in the system. These malicious attackers may reveal the private policies of firewalls design such a privacy protecting of firewall we can implement various encryption techniques to enhance the firewall performance.

To get enhanced firewall performance we require more attention towards reordering of rules. We have proposed a firewall model that will reorders the rules that has not been

investigated in the literature. We believe that this work which we are extending will useful to get good performance of firewall with privacy preservation.

REFERENCES

[1] E. Al-Shaer and H. Hamed, "Discovery of policy anomalies in distributed firewalls," in Proc. IEEE INFOCOM, 2004, pp. 2605–2616S. M. Metev and V. P. Veiko, Laser Assisted Micro technology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[2] Acharya, S., Wang, J., Zihui Ge; Znati, T.F., Greenberg "Traffic-Aware Firewall Optimization Strategies", IEEE ICC, 2006.

[3] Qi Duan and Ehab Al-Shaer., "Traffic-Aware Dynamic Firewall policy management: Techniques and Applications" IEEE ICC, 2013.

[4] A. Wool, "A quantitative study of firewall configuration errors," Computer,vol. 37, no. 6, pp. 62–67, Jun. 2004

[5] L. Yuan, H. Chen, J. Mai, C.-N. Chuah, Z. Su, and P. Mohapatra, "Fireman: A toolkit for firewall modeling and analysis," in Proc. IEEE S&P, 2006, pp. 199–213.

[6] Hazem Hamed and Ehab AlShaer, "Dynamic Rule ordering Optimization for High-speed Firewall Filtering" in ASIACCS'06, March 2124,2006, Taipei, Taiwan.

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

[8] 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.

[9] A. X. Liu and M. G. Gouda, "Diverse firewall design," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 8, pp. 1237–1251, Sep. 2008.

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

[11] Tihomir Katic, Predrag Pale, "Optimization of Firewall Rules" in IEEE Trans. Information Technology Interfaces, 2007.

[12] Misherghi, G.; Lihua Yuan; Zhendong Su; Chuah, Chen-Nee; Hao Chen, "A General Framework for Benchmarking Firewall Optimization Techniques" in Network and Service Management, IEEE Transactions on5 2008.

[13] M. G. Gouda and A. X. Liu, "Firewall design: Consistency, completeness and compactness," in Proc. IEEE ICDCS, 2004, pp. 320–327.

[14] 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.

[15] A. X. Liu and F. Chen, "Collaborative enforcement of firewall policies in virtual private networks," in Proc. ACM PODC, 2008, pp. 95–104.

[16] Fei Chen, Bezawada Bruhadeshwar, and Alex X. Liu. "Cross-domain privacy-preserving cooperative firewall optimization" In Proceedings of the IEEE/ACM TRANSACTIONS ON NETWORKING, volume 21, pages 857 – 868, 2013.

[17] Mustafa, U. Masud, M.M. , Trabelsi, Z. , Wood, T. , Al Harthi, Z**,** "Firewall performance optimization using data mining techniques",in IEEE TRANS Wireless Communications and Mobile Computing Conference (IWCMC), 2013