REDUNDANCY REMOVAL OF RULES WITH REORDERING THEM TO INCREASE THE FIREWALL OPTIMIZATION

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 widely getting used for securing the private network. Firewalls check each incoming and outgoing packets and according the rules given by network administrator and it will take the decision whether to accept or discard the packet. As per the huge requirement of services on internet the rule set becomes large and takes more time to process one packet and it affects the throughput of firewall. So firewall optimization has a great demand to get good performance. Exiting research efforts developed techniques for either intra-firewall or inter-firewall optimization within a single administrative domain. In addition, existing techniques are inefficient in reducing packet processing delay, because they optimize firewall rules by only reducing the number of rules, but lack the intelligence to decide the order of rules. This paper proposes an adaptive cross-domain firewall policy optimization technique using statistical analysis, while protecting the policy confidentiality. To the best of our knowledge, we are the first to propose a technique that dynamically decides the order of rules based on the network statistics. The proposed technique not only identifies and removes redundant rules but also identifies the order of rules in the rule set to improve the performance of the system. The optimization process involves two tasks: First, collaboratively reduce the number of rules between multiple firewalls, while protecting confidentiality of them. Second, using network usage statistics, identify the order of rules in the rule set The feasibility of the proposed technique is shown with the help of the prototype implementation. The evaluation results show the effectiveness and efficiency of the proposed solution.

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

---***---

1. INRODUCTION

Firewalls are widely used in securing private networks of organizations, corporate world, and personal networks. These firewalls are keeping at the entry point of private network to our secure network. Firewall checks each incoming and outgoing packet and according to policies set by the network administrator it will gives the decision whether to accept or discard the packet. These policies are nothing but the access control list and each firewall or router have two types of access control list1) for filtering incoming packet 2) for filtering outgoing packets. Firewall checks packet according to first match semantics means packet checks each rule sequentially until it found the match point and so on. So performance of firewall depends on rule set. Due to huge services available on internet network administrator set rules according to need of user and this rule set becomes bulky and packet processing time gets decreased. Optimization of firewall is needed to increase the firewall performance. Various different techniques are used to optimize the firewall like optimization of rules [1], inter firewall optimization [5],[6], intra firewall optimization [2], [3], [4] etc. Intra firewall optimization works on single administrative domain so no need of privacy protection and inters firewall optimization works on two different administrative domains with privacy protection. While working in two different administrative domains we have to look after the privacy protection of firewall policies. Previous work has been done in the area of inter firewall optimization by protecting the privacy of firewall [5], [6]. Moreover, low-cost hardware firewalls have a very small limit on the number of rules. For example, a low-cost hardware firewall, such as TL-ER6020, supports only 32 access rules. Once you hit a maximum limit number, TL-ER6020, will refuse to add more rules. Due to the limitation on the number of rules supported, it is necessary to optimize firewall access control rules.

1.1 Cross Domain Interfirewall Optimization Technique

In this technique the focus is given on working of the firewall in different administrative domains. Optimization is done by removing redundant rules with preserving the privacy of the rules. Let us consider the two different administrative domains CO and IT, F1 denotes the policy on firewall one’s outgoing interface and F2 denotes the policy on firewall two’s incoming interface given in Fig1. The physical interfaces are denoted as I1, I2 connecting two routers respectively. For any rule in F2,if suppose any packet that match rule r but not matches any rule above r in F2 is discarded by F1.Such a packet never cones to F2 and rule becomes the inter firewall redundant rule. While removing the inter firewall redundant rule we have to consider the privacy of the policies designed at the different administrative domains. One should not disclose the firewall policies to other. While doing this privacy protection with encryption we are persevering the policies of firewalls from each other.

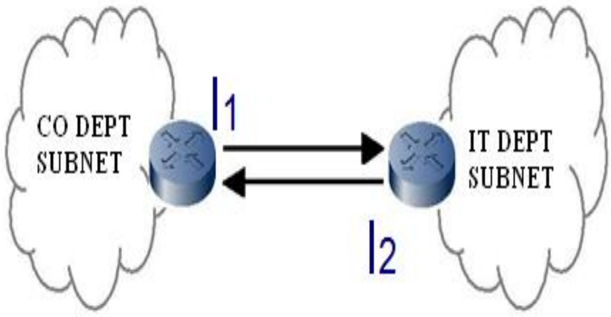

Fig -1: Interfirewall Connectivity

1.2 Challenges for Proposed System

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

Previously lot of work has been done in the area of inter firewall optimization and intra firewall optimization technique. In the intra firewall redundancy removal technique [2], [3], [4] authors aims to remove redundant rules in the single administrative domain. As the work has been done in single administrative domain the privacy of the policies designed is not concerned. The backward and forward redundant rules identification has been done by Gupta [11].

Prior work also shows that the Inter firewall redundancies removal [5], [6].In this techniques work focused on the redundancy removal in the two different administrative domain. When work has been done on the two different administrative domains the policy privacy should be concerned. Therefore it is applicable to one administrative domain only.

Firewall compressor proposed by X. Liu, E. Torng, and C. Meiners, [12] give us a framework and this framework remarkably reduces the rules in firewall. After implementing this technique firewall semantics gets unchanged. They proposed dynamic programming which gives us optimal solution which compresses one dimensional firewall and in second approach he gives a systematic compression of multidimensional firewall.

To get better performance from firewall Tihomir Katic,Predrag Pale [1], proposed logic to optimize firewall rules. As rules of the firewall get set by the network administrator he have to regular check of the newly designed rule with existing rules. In large organization as there is very huge design of rules is present it is not possible to check the so new rule with existing rule. And in case of less experienced administrator, he finds more difficulty to do this. Administrator finds difficulty in finding the rule redundancies. The proposed technique by the author use log rules and other parameters related to rules in replacement of using IP address, protocol and ports. Authors developed software called FIRO which a command tool related to firewall. The work of firewall is related with IP tables of LINUX Platform.

Many other firewall optimization techniques are proposed by researcher in different areas. Some of the famous firewall optimization algorithms are Trie tree-based algorithm [13], Decision Tree-based algorithm [14], and TCAM-based algorithm [15].

Alex X. Liu Fei Chen [23], proposed us a new technique which removes redundant rules present in inter firewall without having any knowledge of each other's policies. They proposed a protective framework. In this model they work collaboratively and enforce the firewall policies. This solution is far better than proposed Cross Domain Cooperative Firewall (CDCF) because, the encryption technique used in CDFC is little bit slower than three magnitude order proposed by Alex X. Liu Fei[23].

Fei Chen,Bezawada Bruhadeshwar, and Alex X. Liu [7] proposed a cross domain optimization technique with preventing the privacy of firewall policies in cooperative environment. To get the goal of this they propose two methods. 1) They propose a novel approach and give a protocol which detects inter firewall redundancy removal in one firewall. 2) They implemented the protocol and got tremendous result in removing of redundant rules.

When they designing this protocol they consider one threat model in that they consider two firewalls are semi honest. For preserving the privacy of the firewall they use the encryption techniques and encrypt the policies of firewall and use Pohling-Hellman Algorithm as encryption technique.

2.1 Our Observations

The existing solutions lack to reorder the rules according to the hit priority of the rule. They mainly focus on reducing the number of rules, while neglecting the priority based decisions of the rules. Firewalls use first-match semantics, as a consequence, if the rules with a highest hit ratio are not up in the rule order, it directly affects the throughput of the firewall.

2.2 Proposed Solution

This paper proposes a solution that not only reduces the number of rules in the firewall ACL, but also reorders firewall rules based on hit-rates of the rules. The set of ACL rules used in a firewall is specified as a sequence of rules. The rules can overlap with each other. Therefore, the proposed approach identifies overlapping spaces of the rules and reduces the number of rules. Furthermore, to provide traffic-aware optimization the proposed solution reorders the firewall rules according to their hit-rates. The proposed approach used statistical analysis to determine hit-rates of each rule. When a lower priority rule r2 conflicts with a higher priority rule r1 that has a different action, we say that r2 depends on r1. Reordering of rules should result in rules that are equivalent to the original ones in the net effect.

3. DESIGN SECTION

The primary objective of the proposed approach to increase the throughput of the firewall To achieve this, we need to minimize the packet processing time of the firewall. In particular, the proposed approach optimizes (reduces) the number of rules and order them according to their hit-ratio.

The steps of the proposed algorithm are given below:
1) Perform statistical analysis on firewall log files to collect information about type of packets and action taken by firewall.
2) Select the rules with highest hit-rate and assign them high priority.
3) Now on the firewall rules, identify overlapping spaces to reduce the number of rules.
4) For each rule from top to bottom, the proposed algorithm is executed.
5) Once dependent rules are identified using overlapping spaces, remove them and create a new rule.
6) Repeat this process until all rules are processed.

Fig-2 illustrates architecture of the proposed technique. The proposed technique contains three modules namely

1. Statistical Analysis Module (SAM)
2. Rule Optimizer Module (ROM)
3. Traffic-aware Optimization Module (TOM)

The SAM is responsible for analysis of log files and generates statistics reports. The generated reports contain statistics about protocol, well-known ports and server IP address. The output of SAM i.e. stat data and this stat data is provided as an input to TOM module. The ROM is responsible for reducing the number of rules in the firewall. The rule extractor rule and iterartor will extract the firewall rules. Afterwards model removes the overlapping spaces by using overlapping rules finder. The overlapping spaces means, the spaces where all packets matches same set of firewall rules but with different decision of at least two rules. After finding these spaces model will generate new rules without policy conflicts. The compressed rules serve as an input to TOM. Based on inputs from SAM and ROM, the TOM module decides the priority of rules to improve the throughput of the firewall by re-arranging the rules. This model takes stat data and optimized rules as an input and check the priority of rules. If higher priority rule is present after lower priority rule then packet processing time get increased so this model will reorder the rules according to priority of rules.

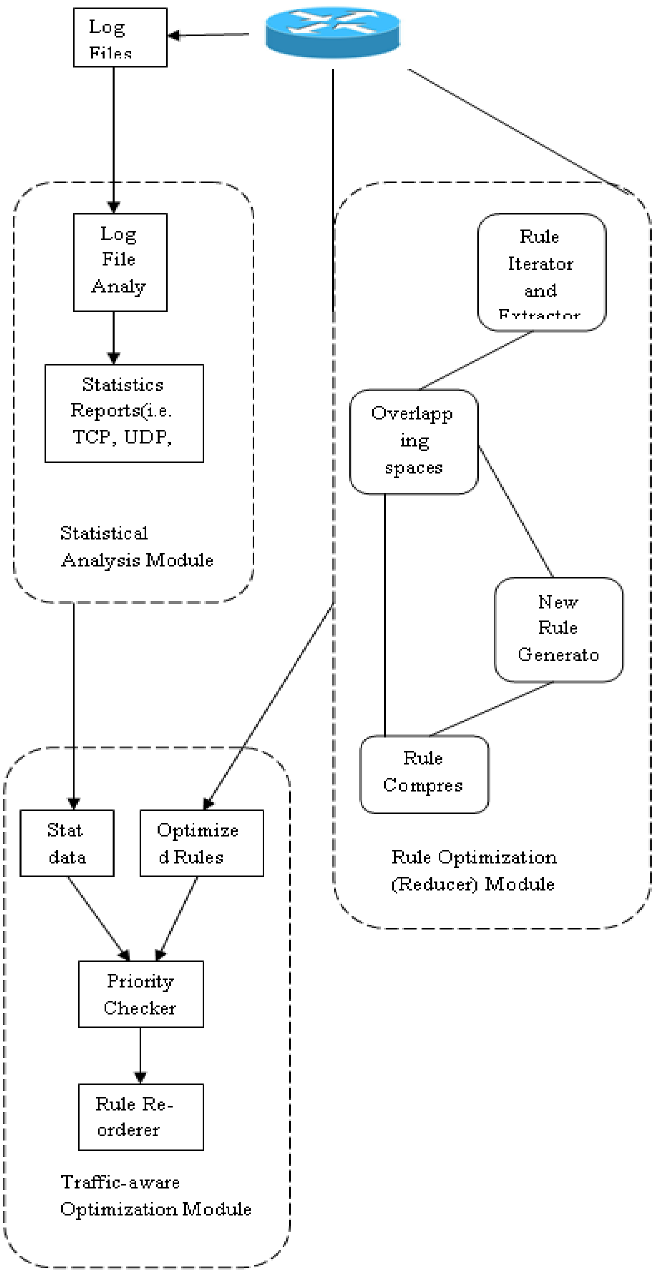
Log Files
Log File Analy
Statistics Reports(i.e. TCP, UDP,
Statistical Analysis Module
Rule Iterator and Extractor
Overlapping spaces
New Rule Generato
Rule Compres
Rule Optimization (Reducer) Module
Stat data
Optimized Rules
Priority Checker
Rule Re-orderer
Traffic-aware Optimization Module

Fig -2: Architecture of the Proposed System

4. EVALUATION AND RESULT

To evaluate effectiveness of the proposed solution, we tested it on synthetic firewalls. In addition, we measured efficiency of the proposed solution using synthetic firewalls. The prototype of the proposed solution is implemented using Java on Ubuntu 12.04 LTS (long term support) operating system. The evaluation experiments were carried on a Desktop computer running Ubuntu with quad-core process and 8 GB RAM.

Due to security concerns, it is hard to obtain access to real adjacent cross-domain firewalls managed by different administrative groups. Therefore, to evaluate effectiveness and efficiency, we generated a large number of synthetic firewalls. Each synthetic firewall rules examine five header fields from a network packet namely source IP address, destination IP address, source port number, destination port number and protocol of the packet. The number of rules used in the synthetic firewalls varies from 100 to 250. To measure the efficiency, the processing time and communication cost of every synthetic firewall was measured. Fig-3 shows average processing time on the synthetic firewalls. Fig-4 shows the average communication cost on the synthetic firewall. We used two synthetic firewalls namely firewall1 and firewall2 to find the communication cost.

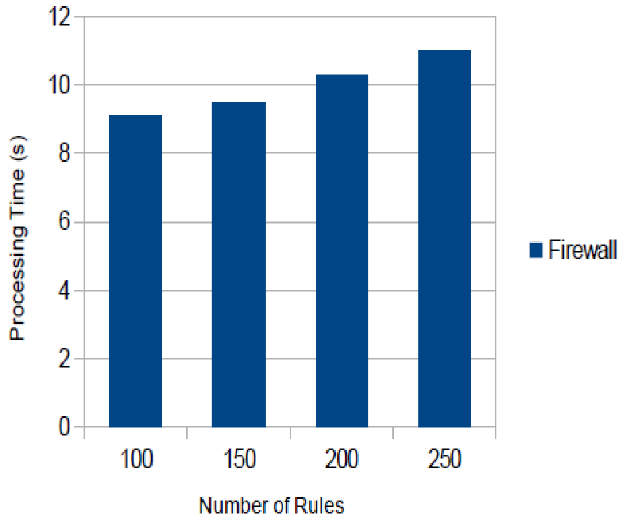

Fig-3 Average processing time for the synthetic firewall.

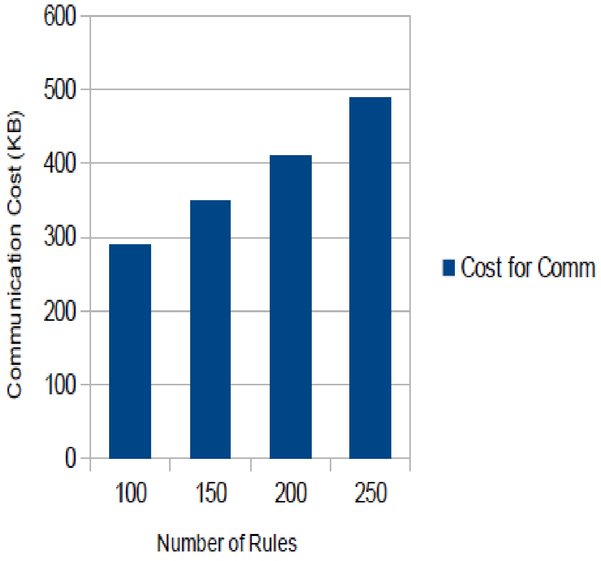

Fig-4 Average communication cost for the synthetic firewalls

5. CONCLUSION

Firewalls play a key role in network security and access control. Existing optimization techniques are inefficient in increasing the throughput for the firewall by reducing the packet processing time. This paper proposes an adaptive cross domain firewall policy optimization technique using statistical analysis, while protecting the policy confidentiality. The proposed technique not only identifies and removes redundant rules but also identifies the order of rules in the rule set to improve the performance of the system. The optimization process involves two tasks: First, collaboratively reduce the number of rules between multiple firewalls, while protecting confidentiality of them. Second, using network usage statistics, identify the order of rules in the rule set. We showed the feasibility of the proposed approach with the help of our prototype implementation. The evaluation results showed the efficiency of the proposed solution.

ACKNOWLEDGMENTS

We thank colleagues of BSIOTR Wagholi, Pune, for their constant feedback on the paper. We also thank the anonymous reviewers for their valuable comments.

REFERENCES

[1]. Bremler-Barr A and Hendler D. Space-efficient tcam-based classification using gray coding. In Proceedings of the IEEE INFOCOM, 2007.

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

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

[4]. E. Al-Shaer and H. Hamed. Discovery of policy anomalies in distributed firewalls. In Proceedings of the IEEE INFOCOM, pages 2605 – 2616, 2004.

[5]. 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.

[6]. J. Cheng, H. Yang, S. H.Wong, and S. Lu. Design and implementation of cross-domain cooperative firewall. In Proceedings of the IEEE ICNP, pages 284 – 293, 2007.

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

[8]. A. X. Liu and F. Chen. Collaborative enforcement of firewall policies in virtual private networks. In Proceedings of the ACM PODC, pages 95 – 104, 2008.

[9]. A. X. Liu and M. G. Gouda. Complete redundancy removal for packet classifiers in tcams. In Proceedings of the IEEE Transaction on Parallel Distributed Systems, volume 21, pages 424–437, 2010.

[10]. A. X. Liu, C. R. Meiners, and E. Torng. Tcam razor: A systematic approach towards minimizing packet classifiers in tcams. In Proceedings of the IEEE/ACM Transaction on Network, volume 18, pages 490–500, 2010.
[11]. nf HiPAC. Firewall throughput test. http://www.hipac.org/performance tests/results.html, 2012.
[12]. Fengjun S, Yingjun P, and Xuezeng P. tudy on an absolute aon-collision hash ip classification algorithms. In Proceedings of the Journal of Communications, 2005.
[13]. Singh S, Baboescu F, and Varghese G. Packet classification using multidimensional cutting. In Proceedings of the ACM SIGCOMM, 2003.
[14]. L. Yuan, H. Chen, J. Mai, C.-N. Chuah, Z. Su, and P. Mohapatra. Fireman: A toolkit for firewall modeling and analysis. In Proceedings of the IEEE Security and Privacy, pages 199–213, 2006.