International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 4, Issue 2, February 2015 **ISSN 2319 - 4847**

Firewall Policy Anomaly Management with Optimizing Rule Order

[1].Ms. Swati S. Kachare, [2] Dr. P.K. Deshmukh

[1],Computer Department - Rajarshi Shahu College of Engg. Pune

[2].Computer Department - Rajarshi Shahu College of Engg. Pune

ABSTRACT

Security policy of any network is implemented by Firewall which can filter out unwanted traffic. A set of filtering rules written based on predefined security policy requirement used for filtering decision. If Polices are managed in incorrectly manner then Firewall can't be significantly effective in protecting networks. It's very necessary to have a policy management technique that users can use to verify the correctness of written firewall filtering rules. This paper represents Rule-based segmentation for firewall policy anomaly identification and Optimizing rule order which not only identify and remove Firewall Policy Anomalies but also reduces Packet-Rule searching time to improve system performance. The proposed set of firewall policy supports efficient working environment of firewalls. The Heuristic Approximation Algorithm is used to Optimize Rule list. The packet matching cost in all cases has been improved by this algorithm.

Keywords: Anomaly Management, Firewall Policy, Optimization, Segmentation, Heuristic approximation

1.INTRODUCTION

A Firewall most commonly used to protect any network. A firewall can be a hardware device or a software application that monitor incoming and outgoing traffic. Firewall work like a filter between our computer/network and the Internet. A Firewall Access Policy consist a sequence of rules that define the action performed on packets that satisfy certain condition. There are several different formats of rules that are used by firewall to filter out information, and some are used in combination. These set of rules are used for specific filtering. Firewall rules have fixed network fields. Firewalls have been the frontier defiance for secured networks against attacks and unauthorized traffic by filtering unwanted network traffic coming from or going to the secured network. The filtering decision is based on a set of ordered filtering rules defined according to the predefined security policy requirements. Conflict occurs in the list of firewall rule list due to different action within same network packet space. Dependency relations are checked between rules in the policy. Firewalls are protecting devices which ensure an access control. System administrators often face problem while setting the rules for firewalls. 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.

Firewall policy management is a challenging task due to the complexity and interdependency of policy rules. It is very difficult for system administrator to set its own rules on firewall for protecting the network. In this paper, we identify all anomalies that could exist in firewall environment. We also present a set of techniques and algorithms to automatically discover policy anomalies in centralized environment and resolve anomalies by Reordering of rules and redundancy elimination that simplifies the management of filtering rules and maintains the security of firewalls. The risk value of each conflicting segment is calculated then action constraints are generated .Firewall policy conflict should be resolved by reordering which is combination of Greedy and Permutation algorithm. The optimization of rule list is achieved by Heuristic Approximation algorithm which set the highest order rules at top of the list and reduces the packet matching time thus improves system performance.

2.LITERATURE SURVEY

Firewalls are core security elements of any network. Firewall policy consist a sequence of rules that perform action that satisfy particular criteria. Management of Firewall policy is very critical and error-pron task. Number of research has been done towards anomaly detection and resolution including with tools and methodology. The existing anomaly detection methods could not accurately point out the anomaly portions caused by a set of overlapping rules. In order to precisely identify policy anomalies and enable a more effective anomaly resolution, the tool implemented by Hongxin Hu, Gail-Joon Ahn and Ketan Kulkarni [1] detect and resolve firewall policy anomaly by using rule - based segmentation technique to accurately identify policy anomalies and derive effective anomaly resolutions. But this methodology they have not applied to larger rule list or distributed firewall. E.Al-Share and Hamed [2] presented 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 maintain the security of next-generation firewalls but detect only pairwise Anomalies of Firewall. L.Yuan, H.Chen, J.Mai, C.Chuah, Z.Su, P.Mohapatra and C.Davis [3] implemented FIREMAN which can detect anomalies among multiple rules by analyzing the relationship between one rule and collection of packet space derived from all preceding rules and ignores all subsequent rules when performing anomaly detection. The first quantatives evaluation of quality of firewall configuration based on Check point is done by A. Wool [4].Their current study contain firewall complexity with poor configuration and complexity is correlated with several configuration errors. However, unlike 2004 study, the current study doesn't have with later software versions which have less error. Distributed Firewall has larger rule set which has detrimental effect on performance of firewall as well as more expensive hardware that can process a large number of firewall packet matching. The existing number of packet matching techniques does not inform about relative frequency of matched packets and review of them is given by Gupta and McKeowm [5]. H. Hu, G. Ahn, and K. Kulkarni [6] represented an innovative policy anomaly analysis approach for Web access control policies, focusing on XACML (Extensible Access Control Markup Language) policy. However, we still suffer from unintended security leakages by unauthorized actions in business services while providing more convenient services to Internet users through such a cutting-edge technological growth. F. Baboescu and G. Varghese, [7] Packet filters provide rules 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. There has been prior work on efficient conflict detection for two-dimensional classifiers. However, the best known algorithm for conflict detection for general classifiers is the naive O (N2) algorithm of comparing each pair of rules for a conflict. Hamed and Al-Shaer [8] describe two further measurements for firewall rule sets: dependency depth and dependency ratio - we have defined them in more detail below. These measurements can be used to quantify the complexity of firewall rule sets. To manage the firewall in complex and multi firewall environment, Bartal et al.presented a firewall management toolkit termed as Firmatos [9] which resolve the lacking of firewall security management.

3.ANOMALY IDENTIFICATION AND RESOLUTION

Anomalies of firewall are classifies as Conflict and redundancy identification and resolution. Firewall policy is the set of rule that perform actions (Allow or Block) by satisfying certain condition. The rules are defined in the form of <Condition, Action>. The condition is composed by using network fields like Source IP address, Source Port Num, Destination IP address, Destination Port Number, and Protocol Type. Firewall policies Anomalies are identified as conflicting segments discovery & resolution and Redundancy identification & removable.

A. Conflicting Segments Discovery and Resolution

The segmentation methodology is used for Anomaly detection and resolution. In this technique network packet space are divided into disjoint network packet segment. Each segment associate with unique set of firewall policy rules represents an overlap relation; it may be either conflicting or redundant. Various set operations are performed to convert rule list into disjoint network packet space. For Example various set operations like subset, superset, partiall match or disjoint are used to convert overlapped spaces into disjoint spaces. A Policy Conflicts is defined as "a policy conflict in a Firewall associates with unique set of rules, which can derive a common network packet space .All the packets within this network packet space have same action but at least two rules have different actions either Allow or Deny".

1. Conflicting Correlation Group Generation

After generation of segments, conflicting correlation relationships are identified among conflicting segments and conflict correlation groups (CG) are identified. Searching spaces for resolving conflicting segments are reduced by this correlation process.

2. Risk Level Calculation

By observing characteristics of conflicting segments, action constraints are taken by applying Allow or Block action. A strategy based method is used for action generation. In this method risk level of each conflicting segments is calculated according to Common Vulnerability Scoring System (CVSS) and also set upper thresholds and lower thresholds.

3. Reordering

All conflicting segments assigned with action constraints are resolved by reordering conflicting rule. Combination Algorithm like Greedy Algorithm and permutation Algorithm are used for reordering conflicting rule. Permutation Algorithm has limitations like its computational complexity is high so it can be used only to identify an optimal reordering for a small set of correlated conflicting rule. Combination Algorithm is as

1. Calculate a resolving score for each conflicting rule
   a. Generation of position indicator for each conflicting segment
   b. Generation of position ranges.

c. Calculate resolving sore for each position range
d. choosing max resolving sores

2. If no. Of conflicting rules < N then utilize Permutation Algorithm otherwise Greedy Algorithm.

B. Redundancy Identification & Removable

In the network packet space if the same or more general rule is available then that is redundant rule. Property assignment is performed on each rule's subspace and finally redundant rules identified and then removed.

The overall system Architecture is as.

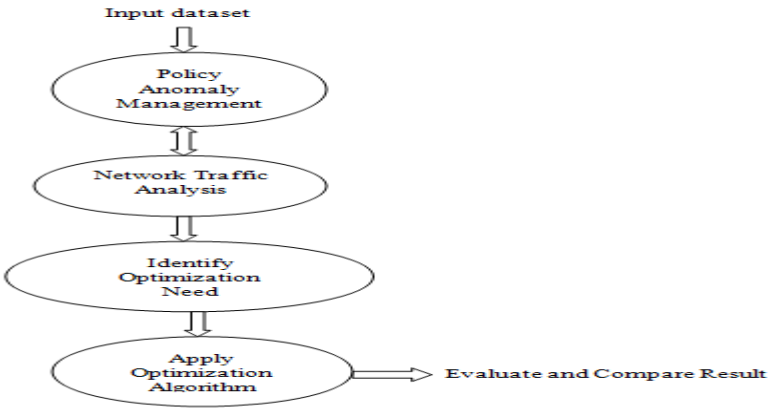

Fig.1 System Overflow Diagram.

4.OPTIMIZATION OF RULE ORDER

The firewall optimisation problem statement is to place the rules in such order that the most frequently used rules are near to the top of the rule set and therefore reduce the packet-rule searching time. To achieve this, the rules are associated with the number of matches is called weight of that rule. The performance of system is calculated in terms of cost which is calculated as position of that rule and associated weight of rule. The heuristic approximation algorithm is used to obtain optimization of rule order of firewall policy which places more frequently used rule at top of list with highest weight. Consider resolved policy anomaly as an un-optimized rule list and weights are calculated from matching number of rule-packet then Heap is created. Cost of rule is calculated by considering weight and position of that respective rule.

Heuristic Approximation Algorithm

step1: Cerate start_list

step2: Create a Heap (H) which sorted by weight of rule but not rule dependency.

Step3: Define Base rule R_b with highest weight.

Step4: Rule_list is created.

Step5: Proceeds precedence rule.

Step6: Calculate cost and position of rules by using following equation (2).

$$R_{ci} = \sum_{i=0}^{N-1} W_i P_i \qquad (2)$$

where, R_{ci} = Cost of Rule i
N = Unoptimized rule list
W_i = Weight of rules R_i
P_i = Order of rules R_i

Step7: Test Rule_list cost and insert point.

Step8: Calculate Best position for Base rule.

Step9: Obtain optimized rule list.

5.RESULT

5.1Dataset: We have taken rule list and captured packets as dataset.

5.2Resultset: The proposed rule based segmentation and optimization methodology provides good solution in term of lower cost and minimum time for packet matching of the firewall. The graphical representation of our proposed rule based segmentation and optimization methodology with previous Rule based segmentation for anomaly resolution and optimizing rule order is given as: the proposed system provides greater resolution of firewall anomalies as well as risk level is reduced as compared to previous. This provides efficient performance by optimizing rule order. We have compared on factors like Risk, Resolution Rate and packet capturing time Analysis.

1. Resolution Rate

As the rule list increases the number of conflict are resolved efficiently as compared to first match mechanism as shown in the following fig. 2.

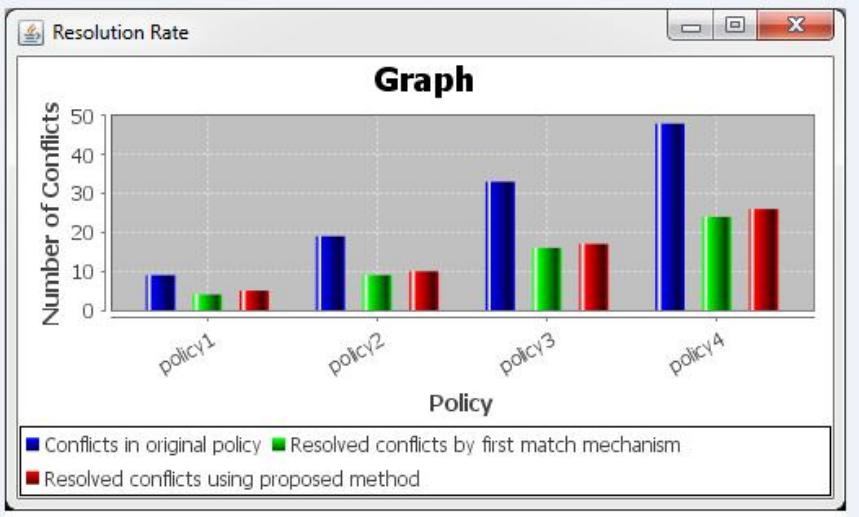

Fig.2 Resolution Rate

2. Packet capturing time Analysis

The number of packets are captured as 50,100,150,200 and then shown that in what time they are processed as the packets increase. The time is considered here is in seconds.

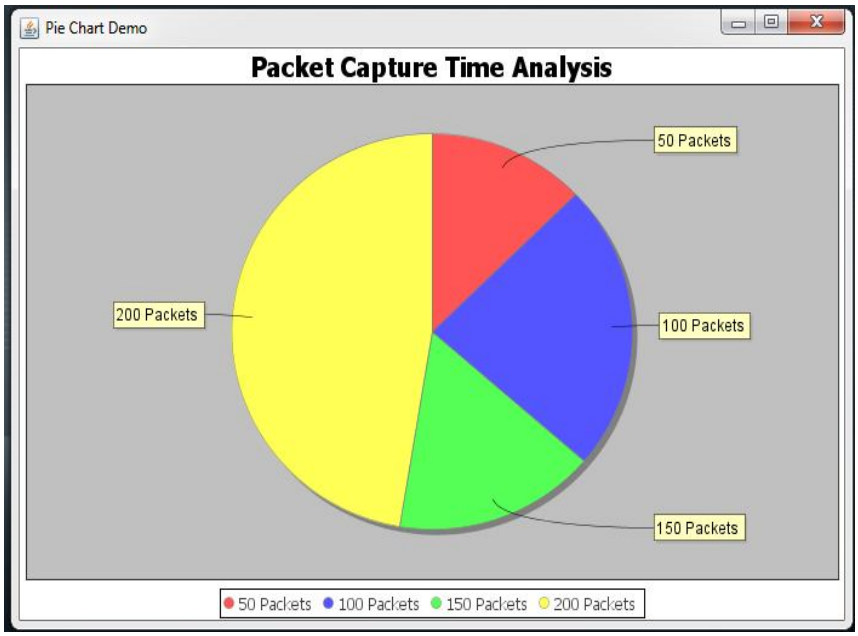

Fig.3. Packet capturing time Analysis

6.CONCLUSION

In this paper we have implemented rule based segmentation and optimization methodology. We have identified and removed anomalies of larger firewall policy in efficient manner. Rule order is optimized for improved performance by reducing time and cost of rule-packet matching. We can extend by applying this to other kinds of access control policy. For the offline optimisation of a firewall the increased runtime complexity is unlikely to be significant is the extended work of proposed system.

ACKNOWLEDGMENT

I thank my project guide and M.E Co-coordinator Prof. Dr. P. K. Deshmukh M.E (PhD),my H.O.D Prof. Dr. A. B. Bagwan, who are members of faculty with the Department of Computer Engineering, Rajarshi Shahu College of Engineering , without whose guidance, this paper would not have been possible. I also wish to record my thanks for their consistent encouragement and ideas. I would like to express my gratitude to all those who helped me make this paper a reality and gave me the opportunity to publish this paper.

References

[1] Hongxin Hu,Student Member,IEEE,Gail-Joon Ahn,Senior Member,IEEE,and Ketan Kulkarni," Detecting and Resolving Firewall Policy Anomalies" IEEE Transaction On Dependable And Secure Computing,Vol.9 ,No.3,MAY/JUNE 2012

[2] E.Al-Shaer and H.Hamed,"Firewall policy advisor for anomaly discovery and rule editing" in IFIP/IEEE 8th International Symposium on Integrated Network Management, March 2003,pp. 17-30

[3] A. Wool ,"Treands in Firewall Configuration Errors: Measuring the Holes in Swisschees",IEEE Internet Computing, vol.14,no. 4,pp.58-65, July/August 2010

[4] J.Alfaro, N.Boulahia-Cuppens, and F.Cuppens,"Complect Analysis of Configuration Rules to Guarantee Reliable Network Secutity Policies",Int'1 J.Information Security,Vol.7,no.2,pp.103-122,2008

[5] P. Gupta and N. McKeown, "Algorithms for packet classification," IEEE Network Magazine, vol. 15, no. 2, pp. 24–32, March/April 2001.

[6] H.Hu, G.Ahn, and K.Kulkarni, Anomaly Discovery and Resolution in web access control policy, Pp.165-174, 2011.

[7] F.Baboescu and G.Varghese,"Fast and Scalable Conflict Detection for Packet Classifiers," Computer Networks, vol.42, no.6, pp-717-735, 2003.

[8] L.Yuan, H.Chen, J.Mai, C.Chuah, Z.Su, P.Mohapatra and C.Davis."FIREMAN: A Toolkit for Forewall Modeling and Analysis," Proc.IEEESymp, Security and Privacy, p.15, 2006.

[9] Y. Bartal, A. Mayer, K. Nissim, and A. Wool, Firmato: A novel firewall management toolkit, in Security and Privacy, 1999.Proceedings of the 1999 IEEE Symposium, pp. 17-31, 1999.

[10] Herman, G. Melanc¸on, and M. Marshall, "Graph Visualization and Navigation in Information Visualization: A Survey," IEEE Trans. Visualization and Computer Graphics, vol. 6, no. 1, pp. 24-43, Jan.-Mar. 2000.

[11] A. Tarko and N. Rouphail, "Travel time fusion in ADVANCE," in Proc. Pacific Rim TransTech Conf., Seattle, WA, 1993, pp. 36–42.

[12] R. Herring, A. Hofleitner, P. Abbeel, and A. Bayen, "Estimating arterial traffic conditions using sparse probe data," in Proc. 13th Int. IEEE Annu. Conf. Intell. Transp. Syst., Madeira Island, Portugal, 2010, pp. 929–936.