Performance and information security evolution with firewalls

Vinay T. Patil[#1], Purushottam R. Patil [#2], Vinayak O. Patil[#3], Shweta V. Patil[#4]
[123]*Department of Computer Engineering, D. N. Patel College of Engineering, Shahada.*
[4]*Department of Computer Science, P.S.G.V.P.Mandal's, Arts, Science and Commerce College, Shahada.*

Abstract— *Security concerns are becoming increasingly critical in networked systems. Firewalls provide important defense for network security. Computer firewalls are widely used for security policy enforcement and access control. Current firewalls use various processing models and are configured using their own policy description languages. However, a misconfiguration in firewalls is very common and significantly weakens the desired security. In this paper, a novel methodology called rule-based segmentation technique is proposed to identify policy anomalies, which is articulated with a grid-based representation. It derives effective solutions to avoid anomalies by providing an intuitive cognitive sense about policy anomaly. The experiments shown that, the proposed approach can efficiently discover and resolve anomalies in firewall policies.*

Keywords — **Policy anomaly, Firewall, Firewall log analysis, Internet, Attacks.**

I. INTRODUCTION

A firewall is a system acting as an interface between a network and one or more external networks. It helps implementing the security policy of any network by deciding which packets to let pass through and which to block, based on the set of rules defined by the network administrator. Any error in defining the rules may compromise the system security by letting undesired traffic pass through or blocking the desired traffic. The rules when defined manually often results in a set that contains conflicting, redundant or overshadowed rules, which creates anomalies in the firewall policy. A network firewall protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs, or they may be a combination of the two. Network firewalls guard an internal computer network (home, school, business intranet) against malicious access from the outside. Network firewall may also be configured to limit access to the outside network of internal users. If passwords provide a 'door' to cover the 'doorway' into your 'house', then firewalls provide 'shutters' to cover the 'windows'. A firewall does absolutely nothing to protect the windows you leave open - that's the job of the programs, which provide the services at those windows. The firewall is ideally a separate computer, which exists between a network and the Internet. It can be a purpose- built device - some of them are available as small black boxes which look like network hubs. This computer can be any old 486, with a highly secure operating system that provides an inbuilt firewall. None of the network computers should be able to access the Internet or can be accessed from the Internet without going through the firewall.

II. LITERATURE SURVEY

The endless growth of internet in today's commercial and technical scenario finds the need to secure the data which should be protected against unauthorized access. Firewalls perform this job of protecting any network. A lot of research work has been done in the field of Firewalls. The main problem that arises in firewalls is that anomalies are generated during updating the rules in the rule set. So the main interest of research is the detection and removal of firewall anomalies. There are a number of approaches for this, which varies to each other in some implementation context. Anomaly free editing in firewall policy rules which includes insertion, deletion and modification in rule set with the help of a tool developed Firewall Policy Advisor . All this work was carried out on a single firewall environment. All the anomalies of single and multi-firewall environment were detected and a set of algorithms defined to automate this process by creating a policy tree of rules in the rule set of a firewall. Chotipat and Chomsiri introduced a method of analyzing packets from the filtering rule list by using the concept of Relational Algebra in

2004. They mapped the firewall rules onto relations. Then by performing various relational algebra operations like select, project, join, set difference etc. some anomalies have been discovered and removed. A raining 2D box model was also represented which shows a simulation of packets by rectangular boxes, which fall, like rain.

An open source application implemented which validates large computer networks. It explains the generic network rules and automatically detects the selected anomalies. This work is based on the concept that in every network there are some global variables that can be profitably used for detecting network anomalies irrespective of the type of networks, its users and the equipments used in the networking. This work describes that how the firewall anomalies can be detected and removed by performing the analysis of network behavior using all types of signatures of attacks. The process of protecting a network with the help of a firewall designed by the software called Firm at too. It designs a new anomaly free set of rules based on the present firewall rule set and places a new firewall with this new rule set in between the previous one and the outside network. The drawback of this approach was that it does not provide any user interactions and its performance degrades for large rule sets.

III. METHODOLOGY

The administrator defines the rules and theses are defined manually. Whenever the packet is passed it has to satisfy all the rules, on the criteria defined it is decided whether to accept that packet or deny that packet. Basically it must satisfy the condition and then specific action is performed i.e. <condition, action>.As the rule set is large so there may exists anomaly. Anomalies like shadowing, redundancy; correlation and generalization are detected and removed. Anomalies are detected comparing each rule and then we have to check whether there is matching field values for more than one rule. If the matching rules have different action i.e. for one it is to allow and for other it is deny then there is conflicting rules. Conflicting rules have to be detected and removed based on the risk value. Firewall log analysis has been performed. We record the log data that is entering or leaving the system and analyze all the data which is accessed by the system. In this proposed technique from the log data we can detect the different or irrelevant behavior of the anomalies and then we can find the IP which are depicting the different behavior. The various types of statistical techniques are used for detecting the different anomalies behavior. The next step is dynamic re-ordering. The dynamic rule re-ordering algorithm is followed there i.e. if packet pi matches ri rule set (ri>=x) then reorder ri else ri is not reordered. Firewall log analysis has been performed. The data is logged so that one can detect the behavior from this data. Along with automatic detection of firewall misconfiguration a new feature of dynamic routing information. It provides the complete view of the network that helps in defining optimization to improve the scalability of designed software. Recently a new method of representation of policy rule set by using Direct Acyclic Graphs so that the firewall performance increases by a sorting algorithm which optimizes and reorders the policy rules to achieve a better rule. This gives an optimal ordered rule set which gives better performance in 98% cases. An open source Linux based firewall software for packet filtering which gives a complete graphical user interface for policy rule insertion, removal and to keep the rule set consistent.

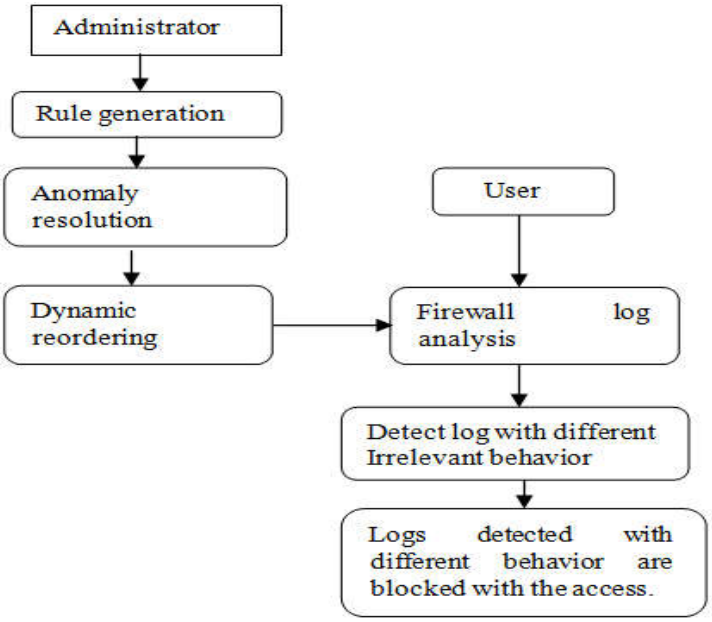

Fig: System architecture of firewall

A. New suggested firewall:

We will implement a two identical firewall in a parallel fashion and the complete security policy applied on every firewall and we divide or distribute the network traffic to two firewalls by specifying every firewall to serve or monitor only a part of network user's traffic not all network users' traffic as in traditional firewall in the second scenario" Proxy firewall".

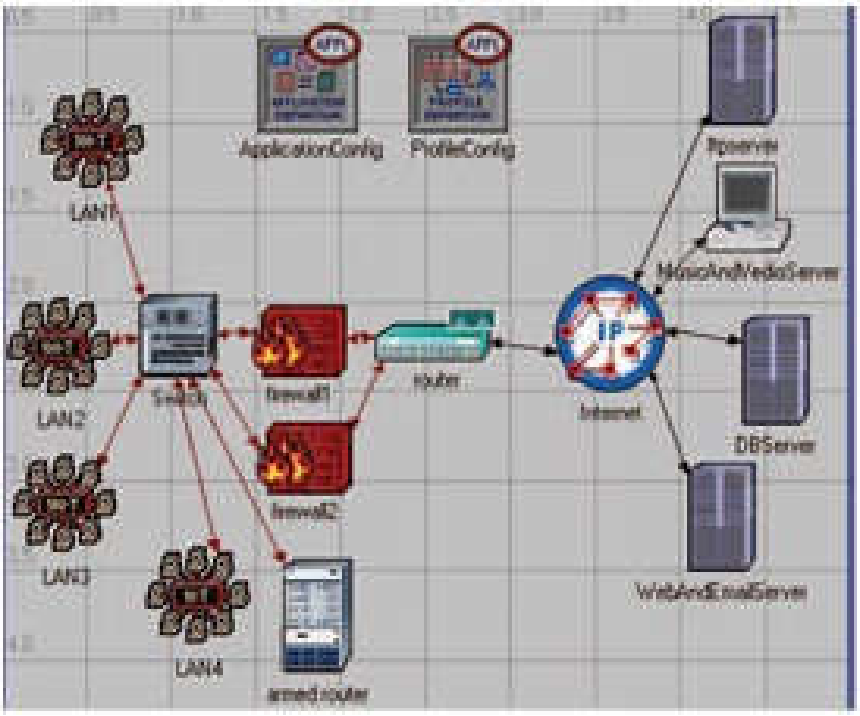

Fig. Network model with two parallel Firewalls

B. Firewall Rules

Whenever a packet is tested by the Firewall, it means that the header of the incoming or outgoing packet is tested against all the rules one by one, which are stored in the Firewall rule set. The rules in the Firewall rule set consists all the header information like source and destination address, source and destination port address and the corresponding action to performed i.e. whether to accept or deny any packet which matches all the other fields of any rule in the rule set. The rules are stored in the rule set in the following format; <order><prtcl><S_ip><S_port><D_ip><D_port><action> Here all the terms have respective meanings with properly defined domains. Order is the number at which the rule is stored in the rule set, prtcl is the type of the protocol specified in the packet's header, s_ip and s_port are the source machines' IP address and port number respectively. Similarly D_ip and D_port are the IP address and port number of the destination. In the last action field defines the resulting action to be performed on the packet which matches all the previous fields. The action field can be either ACCEPT or DENY. These rule sets of any firewall defines the Security Policy of that organization. The security policy of any organization is very dynamic i.e. it can be altered anytime whenever the administrator wants to modify the rules. So such frequent changes are the reason for the inconsistencies in the rule set.

IV. FIREWALL ANOMALIES

As the rule set is very large it becomes difficult to check all the rules for any redundancy. Hence the updating of rule set may generate erroneous set of rules which are unable to perform their intended job i.e. protection from unauthorized access to the network or from the network. These errors in the rule set are called anomalies that have to be detected and removed from rule set for the efficient working of any firewall. Till date, five types of anomalies are discovered and studied namely, Shadowing Anomalies, Correlation Anomalies, Generalization Anomalies, Redundancy Anomalies, and Irrelevance Anomalies.

A. Shadowing anomaly:

Two rules are said to have shadowing anomaly, whenever the rule which comes first in rule set matches all the packets and the second rule which is positioned after the first rule in rule set does not get chance to match any packet because the previous rule has matched all the packets. It is a very critical problem since the rule coming later to the previous rule will never get activated. Hence the traffic to be blocked will be allowed or the traffic to be permitted can be blocked.

B. Correlation anomaly:

Two rules are said to have correlation anomaly if both of them matches some common packets i.e. the rule one matches some packets, which are also matched by the rule second. The problem here is that the action performed by both the rules is different. Hence in order to get the proper action such correlated rules must be detected and should be specified with proper action to be performed.

C. Generalization anomaly:

Two rules which are in order one of them is said to be in generalization of another if the first rules matches all the packets which can be also matched by the second rule but the action performed is different in both the rules. In this case if the order is reversed then the corresponding action will also be changed. The rule, which comes later in the rule list, is shadowed by the previous rule and also it has no effect on incoming packets. The super set rule is called General rule and the subset rule is called Specific rule. If such generalization relation exists between two rules then the super set rule should be placed after the subset rule in the rule list.

D. Redundancy anomaly:

Two rules are said to be redundant if both of them matches some packets and the action performed is also the same. So there is no effect on the firewall policy if one of redundant rules will be removed from the rule set. It is very necessary to search and remove the redundant rules from the rule set because they increase the search time,

space required to store the rule set and thus decrease the efficiency of the firewall. The firewall administrator should detect and remove such redundant rules to increase the performance of the firewall.

E. Irrelevance anomaly:

Any rule is said to be irrelevant if for a given time interval it does not matches any of the packets either incoming or outgoing. Thus if any type of the packets do not match a rule then it is irrelevant i.e. there is no need to put that rule in the rule set. Till now all the above four anomalies are detected and removed successfully but irrelevant anomaly is still not completely defined in any automated software implementation yet. The size of the rule set varies according to the type of the organization. Generally the rule set is very large because different administrators come and modify the policy rules according to their requirements and so is the reason of occurrence of anomalies. Because of the large size of the rule set it is difficult to detect anomalies by manually checking the rules one by one. So there is different software implemented to perform the job of anomaly detection and removal automatically.

V. CONCLUSIONS

Most of the papers discussed are intended to perform the anomaly detection and removal by using different techniques. All of them consider that the rules are written in predicate like language. The policy rules have very simple attribute like fields but in some cases some firewalls define the rules with time parameters defined within the rules, and the actions performed are restricted to be only accept and deny. One more observation was carried out about the anomalies that almost no paper includes irrelevant anomaly as important one, but we observe that due to the effects of it the rule size is increased enormously.

ACKNOWLEDGMENT

The heading of the Acknowledgment section and the References section must not be numbered.
Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template. To see the list of contributors, please refer to the top of file IEEETran.cls in the IEEE LaTeX distribution.

REFERENCES

[1] *Ehab S. Al-Shaer and H. Hamed.“ Management and translation of filtering security policies”. In IEEE International Conference on Communications, (ICC ’03), (2003).*

[2] *E. Al-Shaer and H. Hamed. “Firewall Policy Advisor for Anomaly Detection and Rule Editing.” IEEE/IFIP Integrated Management Conference (IM’2003), March (2003)*

[3] *E.S. Al-Shaer and H.H. Hamed. “Discovery of policy anomalies in distributed firewalls”. In IEEE Infocom(2004).*

[4] *Al-Shaer and H. Hamed, “Conflict classification and Analysis of Distributed Firewall policies”, IEEE J SEL AREA COMM, (2005)*

[5] *ChotipatPornavalai and ThawatchaiChomsiri.”Firewall Rules Analysis”, International Technical Conference on Circuits/ Systems, Computers & Comm. (ITC-CSCC 2004),JULY(2004).*

[6] *ThawatchaiChomsiri, ChotipatPornavalai: Firewall Rules Analysis, International Conference on Security & Management, SAM 2006, Las Vegas, Nevada, USA, June 26-29(2006).*

[7] *Deri Luca and Suin Stefano and Maselli Gaia (2003) Design and implementation of an anomaly detection system: An empirical approach. In Proceedings of Terena TNC.*

[8] *Y. Bartal, A.J. Mayer, K. Nissim, A. Wool, Firmato: A novel firewall management toolkit, in: Proceedings of the IEEE Symposium on Security and Privacy, (1999).*

[9] *Errin W. Fulp. “Optimization of network firewall policies using ordered sets and directed acyclical graphs”. Technical report, Computer Science Department, Wake ForestUniversity, (2004).*

[10] *Mr.Vinay Tila Patil & Gajendra Singh Chandel, Prof. (2014). Implementation of TPA and Data Integrity in Cloud Computing using RSA Algorithm. International Journal of Engineering Trends and Technology. 12. 85-93. 10.14445/22315381/IJETT-V12P215.*

[11] Vinay Tila Patil, Prof. Gajendra Singh Chandel, "Applying Public Auditability for Securing Cloud Data from Modification Attack", IJSRD - International Journal for Scientific Research & Development, Vol. 2, Issue 04, 2014, ISSN (online): 2321-0613