Redundancy Management and Anomaly Detection on Firewall Ruleset using Fame

J. Sethuram
PG Scholar
Department of Computer Science & Engineering
Sri Vidya College of Engineering & Technology
Virudhunagar, TN, India

G. Sankareeswari
Assistant Professor
Department of Computer Science & Engineering
Sri Vidya College of Engineering & Technology
Virudhunagar, TN, India

Abstract

Network security is essential for protecting the private and public networks such as banking, storage environments and educational zones. Network uses different types of security mechanisms for providing security to the network. The firewall is one of the security mechanism is used in the network security. The Firewalls are used as a protection barrier among the two different networks. The recital of firewall is mainly based on firewall policies. The firewall rules are used to decide whether the packets to be permit or refuse. These rules are crucial for the operation of firewall policies. The firewall policy contains some misconfigurations like rule redundancies, anomalies and conflicts. Such, conflicts are resolved by various mechanisms based on their errors. In this paper, we articulate a redundancy removal algorithm to manage such redundancies and a novel anomaly detection tool namely FAME (Firewall Anomaly Management Environment) uses segmentation technique to resolve anomalies.
Keywords: Firewall policy, Anomaly detection, Firewall decision diagrams, Policy conflicts, FAME

I. INTRODUCTION

Network security plays a vital role in providing security for networks through authentication mechanisms. It contains certain policies adopted by the administrator of the network to prevent and monitors the malicious access. It uses one of the security mechanism called firewall. A firewall is a security mechanism is used in the networks for filtering the outgoing and incoming data packets. The firewall contains certain set of rules called access control list to decide whether the data packets should be discard or allowed. It should protect the network and data packets from the malicious access. A firewall is placed in between the public and private networks. The firewall maintains the important logging and auditing function and provides the details about the type and volume of data to be processed in the network to the network administrator.

II. FIREWALL RULESET

The firewall rule set contains set of rules contains two parts specifically <condition and action>.The condition defines the rules in the packets from the outside network with in a specific range and action defines whether the packet to be reject or accept. The rules in the firewall rule set consists of all header information's like source and destination address of the network, source and destination port, protocol type, rule order and action etc. The rules in the rule set are defined in the form of,

<Ruleid><Protocol><Sourceip><Destination ip><Sourceport><Destinationport><Action>.

Here, the <Ruleid> specifies the no. of rules in the ruleset such as rule1,rule2 etc in the firewall ruleset.<Protocol>represents the type of protocols used for communication such as TCP,UDP etc,<Source ip> represents the sender's ip address,<Source port> represents the sender's port number,<Destination ip> represents the receiver's ip address,<Destination port> represents the receiver's port number and <Action> denotes the action constraints such as <Permit> or <reject>.The security policies (ie) firewall policies in the firewalls is dynamic. because it can be modified by the administrator for security issues. Through these numerous changes the firewall rule set gets conflicts.

Example of Firewall Ruleset

Rule	Protocol	Source Ip	Source Port	Destination Ip	Destination Port	Action
r1	TCP	192.168.1.3	25	10.2.1.3	55	PERMIT
r2	TCP	192.168.1.5	25	10.2.1.1	55	DENY
r3	UDP	172.168.2.1	52	10.2.2.1	36	DENY
r4	UDP	172.168.2.3	52	10.2.2.3	36	PERMIT
r5	*	*	*	*	*	PERMIT

III. FIREWALL ANOMALIES

The rule set of firewall is excessively large and it becomes very complex. Hence the firewall rule generated by firewall becomes error. It affects the system performance and security. These erroneous rules are represented as redundant rules or anomalies which can be detected and overcome by various anomaly management techniques like fireman, fame, firewall policy advisor etc. These techniques detect and rectify the various anomalies in the firewall ruleset such as Redundancy Anomalies, Correlation Anomalies, Irrelevance Anomalies, Generalization Anomalies and Shadowing Anomalies etc.

A. Shadowing Anomaly:

Since the first rule r1 in the rule set A that matches all the packets from the ruleset B then the remaining rules in the firewall ruleset such as r2, r3 etc also containing identical properties to match packets and it does not carry out any achievement then these type of rules are said to be as shadowing anomalies.

B. Redundancy Anomaly:

If the two rules in a firewall rule set that match the similar packet and it done the equivalent action, then this type of anomaly is said to be as Redundancy Anomaly.

C. Correlation Anomaly:

The correlation anomaly is defined as, if the two rules in a firewall rule set that matches the same packet. but it performs different action such as permit or reject.

D. Generalization Anomaly:

While the two rules in a firewall rule set are present in a particular order such as r1, r2, it performs different actions. if the order of the rule is altered as r2,r1, then their resultant dealings will also be changed. Then this type of rules is referred to as Generalization Anomaly.

E. Irrelevance Anomaly:

If some rules in a firewall rule set does not matches the packets with in the given exacting interval time. Then this type of rules are categorized as irrelevance Anomalies.

IV. RELATED WORK

Now a days the internet plays a vital role in the society and data security is a challenging task against the illegal access. The firewall is a security mechanism which maintains the security on the networks. This firewall contains some harms such as errors, conflicts when generating and updating its rule set. so this research focuses on such errors, conflicts and redundancies. It contains a variety of mechanisms to overcome these problems. But it can differ depends on their implementations.

A. X. Liu, E. Torng and C. Meiners(2008) introduced a idea of firewall compression to shrink the size of rule set using firewall scheduling algorithm and firewall decision diagrams(FDD).It represents one dimensional firewall compression using dynamic programming techniques for optimal solution and multidimensional firewall compression using systematic approach such as Access control list(ACL)mechanism. [2].

J. Cheng, H. Yang, S. H. Wong and S. Lu(2007) introduced a cross domain cooperative firewall for secured communication using encrypted tunnel by generating the secret keys with the help of oblivious membership verification mechanism.It focuses on rule matching between the networks.[1].

Alex X. Liu(2008) introduced firewall verification tool to verify the firewall rule sets using firewall verification algorithm and decision diagrams to design and analyze the firewall policies for detecting and overcome conflicts in the rules of firewall. [9].

Mohamed G. Gouda, Alex X. Liu (2007)introduced structured firewall design to maintain the quality of firewall policies such as consistency, completeness and compactness using firewall decision diagrams at the time of redundancy removal in firewall rule set. [3].

Alex X. Liu and Mohamed G. Gouda(2008) introduced diverse firewall design concept to find out the all functional discrepancies between the two firewall rule sets for impact analysis using construction, shaping and comparison algorithms. In diverse firewall design three steps to be processed as, define the term policy, identify the error, then remove the redundancy using three algorithms [6].

Hongxin Hu, Gail-Joon Ahn and Ketan Kulkarni(2010) FAME (Firewall Anomaly Management Environment) concept for detecting the policy anomalies using rule based segmentation technique to recognize and overcome such policy anomalies[10].

Alex X. Liu and Mohamed G. Gouda(2005) introduced complete redundancy detection in firewall policies. In these concept the rules redundancy detection based on some condition. It categorizes upward redundant rules and downward redundant rules. It uses a method to represent firewall as tree structure called as firewall decision trees[5].

Mohamed G.Gouda and Xiang-Yang Alex Liu(2004) introduced Firewall Design for maintaining consistency, completeness and compactness on firewall policies to make an efficient firewall policy set using various algorithms as reduction, marking ,generation, compaction, simplification.[7].

R.V. Darade and P.B. Kumbharkar(2014) represents the anomaly detection and resolution using rule base segmentation technique for accurate detection and resolution[4].

M. Malathy and R. Suresh(2014) proposed a statistical analysis of inter firewall optimization by using Redundancy Removal Algorithm for reduce number of redundant rules in a firewall policy set to find the optimal solution on firewall rules[8].

V. REDUNDANCY DETECTION ALGORITHM

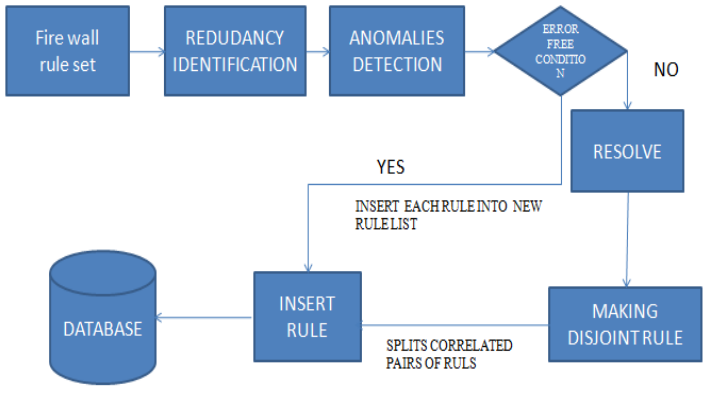
Firewalls are commonly used for securing the private and public networks. It checks each and every data packets that transferred among the networks. Based on certain policies the packets from the inside and outside network to be pass or reject. The firewall contains some erroneous rules and conflicts. Through this unauthorized users can easily access the networks. Our redundancy detection algorithm detects and overcomes the redundant rules and anomalies in the firewall rule set.

A. Algorithm for Proposed System:

Rule set R1, R2;
Firewall F1,F2;
If(P1→F1 && F1R1→R2); //check the condition
{
{
Compare(P1: r1,r2,-----rn); //Match rule satisfied.
Higher priority rule accepted;
Remaining rules are omitted;
Else
Distinct rule accepted;
}
{
if(p1: r1=ø);//Does not match some rules.
It can be represented as anomalies or error rules.

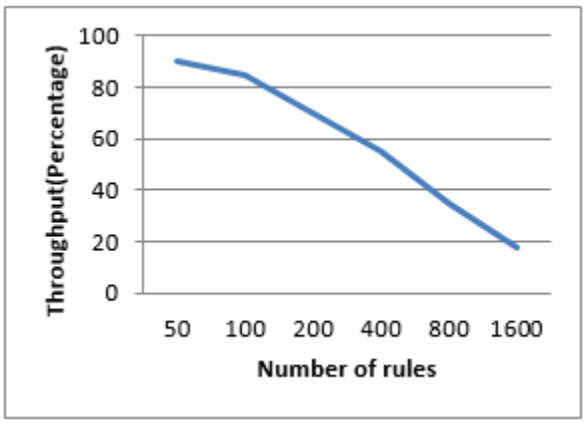
The proposed architecture diagram is used for detecting the redundant rules as well as anomalies in the firewall ruleset. The redundancy management can be done by using redundancy detection algorithm. It process the rules that are same. Once the packet matches with the rules and the other rules are not performing any action on the packets (or) idle rules and anomalies are detected and overcome by Firewall Anomaly Management Environment (FAME) tool. After the completion of redundancy and anomaly removal check whether the rulesset contains optimal rules. If the rules are optimal then insert into the new ruleset or otherwise resolve and making the rules as disjoint rules and stored into new ruleset It detects the error rules or conflicts rules independent to the ruleset. After completing the redundancy removal and anomaly detection process the firewall rules set contains optimal rules for matching the packets from the outside network.

B. Proposed Architecture Diagram:



VI. RESULTS AND DISCUSSION

Through redundancy detection algorithm the firewall optimization is achieved no. of clients can accessed the system. The algorithm detects the redundant rules in the firewall ruleset and anomalies and finally generates a optimal ruleset.Based on the obtained output, the graph has been generated as follows,



VII. CONCLUSION

Our project focuses on redundancy management and anomaly detection in firewall ruleset to improve the performance of the system and increased the security of the network. By using Redundancy detection algorithm and Firewall Anomaly Management Environment (FAME) concept reconstructs a optimal rule in the firewall ruleset.

REFERENCES

[1] Fei Chen, Bezawada Bruhadeshwar, Alex X. Liu, "Cross Domain Privacy Preserving Cooperative Firewall Optimization". In ieee Transactions on Networking, 2013.
[2] R.V. Darade and P.B. Kumbharkar," Firewall policy anomaly detection and resolution", 2014.
[3] M. Malathy and R. Suresh.v," Statistical analysis of interfirewall Optimization", 2014.
[4] Hongxin Hu, Gail-Joon Ahn, and Ketan Kulkarni, "Detecting and Resolving Firewall Policy Anomalies" ieee transactions on dependable and secure computing, vol. 9, no. 3, may/june 2012.
[5] Myungkeun Yoon, Shigang Chen, and Zhan Zhang,"Minimizing the Maximum Firewall Rule Set in a Network with Multiple Firewalls", ieee transactions on computers, vol. 59, no. 2, february 2010.
[6] Hongxin Hu,Gail-Joon Ahn and Ketan Kulkarni,"FAME:Firewall Anomaly Management Environment",2008.
[7] A. X. Liu, E. Torng, and C. Meiners,"Firewall compressor: An algorithmfor minimizing firewall policies". In ieee infocom, 2008.
[8] A. X. Liu and M. G. Gouda, "Diverse firewall design". ieee tpds, 19(8), 2008.
[9] Alex X.Liu," Formal verification of firewall policies". In ieee icc,2008.
[10] J. Cheng, H. Yang, S. H. Wong, and S. Lu, "Design and s of cross-domain cooperative firewall". In ieee icnp, 2007.