Survey on Cooperative Firewall Anomaly Detection and Redundancy Management

J. Sethuram[1] G. Sankareeswari[2]
[1]PG Scholar [2]Assistant professor
[1,2]Department of Computer Science & Engineering
[1,2]Sri Vidya College of Engineering & Technology
Virudhunagar, TN, India.

Abstract— Network security is essential for protecting the private and public networks such as banking and educational zones. Network can use different kinds of security mechanism. Among this firewall is one of the security mechanisms. The Firewalls are used as a protection barrier among the two different networks. The performance of firewall is mainly based on firewall policies. The firewall policies are used to decide whether the packets can be permitted or to be refused. These rules are crucial for the operation of firewall policies. The firewall policy contains erroneous configurations like rule redundancies, errors and conflicts. Such, conflicts are resolved by various mechanisms based on their errors. The following techniques are used for some error detection and correction process like cross-domain cooperative firewall, firewall compression, firewall decision diagrams, firewall verification tool and anomaly detection tools like FAME(Firewall Anomaly Management Environment),FPA(Firewall Policy Advisor, Fireman etc.

Key words: Firewall policy, Anomaly detection, Firewall decision diagrams, policy conflicts

I. INTRODUCTION

Network security is essential for providing security for networks through authentication mechanisms. It contains certain policies adopted by a network administrator to prevent and monitor malicious access, attacks and provides the authorization to access the data in a network, which is managed by the network administrator. Network security provides security in variety of computer networks, such as public and private networks.

Network security is involved in organizations, institutions, banking etc. This network security is done by using one of the security mechanisms called firewall. A firewall is a software which is used to monitors the network traffic. A firewall contains set of rules which are applied to each packet. These firewall rules decide if a packet can passed, or rejected. Usually a firewall is placed between the networks.

A firewall is a security mechanism which acts as a mediator between two different networks. A firewall is a hardware or software system that prevents unauthorized access to or from a network. Firewalls can be implemented in hardware and software, or a combination of two. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. Generally, firewalls are configured to protect against unauthenticated interactive logins from the outside world.

Firewall helps to prevent hackers from outside into the network. Firewalls block traffic from the outside to the inside network, but authorize users on the inside to communicate a little more freely with the outside. Firewalls provide an important logging and auditing function and also provide details to the administrator about what type/volume of traffic has been processed through it. Data travels on the internet in small pieces; these are called packets.

Each packet contains some metadata information for representing the details of the packets. Based on rules, certain packets are then dropped or rejected. This firewall is classified into three types as Packet filtering firewalls, circuit level firewalls, application level firewalls. Packet filtering firewall is used in network layer. It maintains the security of the networks through firewall policies that contains set of rules constructed by the administrator. The firewall policy contains erroneous configurations like redundancies, conflicts, etc. It affects the system security and unauthorized access can be done easily.

The decisions that can be taken by firewall to access the packets are based on the filtering rules that are policies predefined inside the firewall. Firewalls use access control mechanism to provide the access control between different types of networks. Firewalls can be used in centralized and distributed networks. It acts as a protection guard against malicious access.

II. FIREWALL RULE SET

A firewall policy is a set of rules contains two parts (i.e) <condition and action). When the packet is transferred among the networks the rule in the header of the packet is tested with rules in firewall rule set. The rules in firewall rule set consist of all header information like source and destination address, source and destination port, protocol, action, and rule order etc.

The rules that are defined inside the rule set are in the form of,

<Rule><Protocol><Sourceip><Sourceport><Destination ip><Destination port><action>

Here, the <Rule> specifies the order or the no. of rules such as rule1,rule2 etc.<Protocol>specifies the protocols 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 <Deny>.The security policies (ie) firewall policies in the firewalls is dynamic. because it can be modified by the administrator for security issues. So these frequent changes also cause inconsistencies in the firewall rule set.

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

A. Firewall Anomalies

The rule set of firewall is too large that it becomes very complex. Hence the firewall rule generated by firewall rule set becomes error. It affects the system performance. These erroneous rules are represented as redundant rules or anomalies which can be detected and overcome by various techniques such as Shadowing Anomalies, Correlation Anomalies, Generalization Anomalies, Redundancy Anomalies and Irrelevance Anomalies etc

B. Shadowing Anomaly

Since the first rule r1 in the rule set that matches all the packets then the remaining rules such as r2, r3 etc from the rule set containing same properties to match packets and it does not perform any action then the rules are said to be as shadowing anomalies.

C. Redundancy Anomaly

Since the two rules in a firewall rule set that match the same packet and performs the same action, the anomaly is said to be as Redundancy Anomaly.

D. Correlation Anomaly

In this, we come to understand that the two rules in a firewall rule set that matches the same packet. but it performs different action such as permit or deny is called as Correlation Anomaly.

E. Generalization Anomaly

Since the two rules in firewall rule set are in order such as r1,r2, it performs different actions. if the order of the rule is changed as r2,r1, then their corresponding actions will also be changed. These rules are referred to as Generalization Anomaly.

F. Irrelevance Anomaly

If any rule in a firewall rule set does not matches the packets with in the given particular interval time. That type of rules are said to be as irrelevance Anomalies.

III. RELATED WORK

The internet is very essential to society now a days and data security is a challenging task against the unauthorized access. firewall is a mechanism which maintains the security on the networks. This firewall contains several problems such as errors, conflicts when generating and updating its rule set. so this research focuses on such errors, conflicts and redundancies. There are various numbers of mechanisms to overcome these problems. But it can vary based on their implementations.

A. X. Liu, E. Torng and C. Meiners introduced a concept of firewall compression to reduce the size of rule set using firewall scheduling algorithm and firewall decision diagrams(FDD) in 2008.It represents one dimension firewall compression using dynamic programming techniques for optimal solution and multidimensional firewall compression using systematic approach such as Access control list(ACL)mechanism. It achieves only 52.3% compression on firewall rules [2].

J. Cheng, H. Yang, S. H. Wong and S. Lu introduced a cross domain cooperative firewall for secured communication using encrypted tunnel generating secret keys with the help of oblivious membership verification mechanism in 2007.It focuses on rule matching between the networks. The cross domain cooperative firewall is used to prove the membership verification. It only performs the equality test [1].

Alex X. Liu introduced firewall verification tool in 2008 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 The verification tools in firewall can possibly catch illegimate access in private networks, and it does not find the errors in legimate communication among the private and public network.[9].

Mohamed G. Gouda, Alex X. Liu introduced structured firewall design in 2007 to maintain the quality of firewall policies such as consistency, completeness and compactness using firewall decision diagrams at the time of redundancy removal in policy set. In structured firewall the redundancies and anomalies are only detected by the soft wares and it can be overcome by manual process [3].

Alex X. Liu and Mohamed G. Gouda introduced diverse firewall design concept in 2008 to discover 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 FAME (Firewall Anomaly Management Environment) concept in 2010 for detecting the policy anomalies using rule based segmentation technique for identify and overcome such policy anomalies[10].

Alex X. Liu and Mohamed G. Gouda introduced complete redundancy detection in firewall policies the rules redundancy detection in 2005 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].

Lihua yuan, Jianning mai, Zhen dong Su, Hao Chen, Chen Nee Chauh, Prasant Mohapatra proposes a Fireman tool detect errors and conflicts in firewall policies using static analysis techniques. It performs symbolic model checking of firewall configuration. Fireman uses binary decision diagrams for modelling the firewall rules. Fireman detects the anomalies in multiple rules such as relationship between two rules. Fireman examines only the preceding rules not subsequent rules in the policy set[11].

Mohamed G.Gouda and Xiang-Yang Alex Liu introduced Firewall Design in 2004 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 represents the anomaly detection and resolution using rule base segmentation technique for accurate detection and resolution in 2014[4].

M. Malathy and R. Suresh propose a statistical analysis of inter firewall optimization in 2014 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].

IV. CONCLUSION

In this paper various techniques are used for some error detection and correction processes in firewall policies like cross-domain cooperative firewall, firewall compression, firewall decision diagrams, firewall verification tool and anomaly detection tools like FAME(Firewall Anomaly Management Environment), FPA(Firewall Policy Advisor), Fireman etc. The above techniques provide efficient detection and correction of anomalies and redundancies. Depending upon the rule set error, we specify the particular technique. The firewall policy set is used to improve the performance of our anomaly detection technique.

REFERENCE

[1] Firewall throughput test, www.hipac.org/performance tests/results.html.
[2] .J. Cheng, H. Yang, S. H. Wong, and S. Lu. Design and implementation of cross-domain cooperative firewall. In *IEEE ICNP, 2007.*
[3] X. Liu, E. Torng, and C. Meiners. Firewall compressor: An algorithmfor minimizing firewall policies. In *IEEE INFOCOM, 2008.*
[4] M. G. Gouda and A. X. Liu. Structured firewall design. *ComputerNetworks Journal (Elsevier), 51(4):1106–1120, 2007.*
[5] R.V. Darade and P.B. Kumbharkar.Firewall policy anomaly detection and resolution,2014
[6] X. Liu and M. G. Gouda. Complete redundancy removal for packet classifiers in tcams. *IEEE TPDS*, in press.
[7] X. Liu and M. G. Gouda. Diverse firewall design. *IEEE TPDS*, 19(8), 2008.
[8] M. G. Gouda and A. X. Liu. Firewall design: consistency, completeness and compactness. In *IEEE ICDCS*, pages 320–327, 2004.
[9] M. Malathy and R. Suresh.v Statistical analysis of interfirewall optimization,2014.
[10] Alex X.Liu. Formal verification of firewall policies. In IEEE ICC,2008.
[11] Hongxin Hu,Gail-Joon Ahn and Ketan Kulkarni FAME:Firewall Anomaly Management Environment,2008.
[12] Lihua yuan, Jianning mai, Zhen dong Su, Hao Chen, Chen Nee Chauh, Prasant Mohapatra Fireman:A Toolkit for firewall modelling and analysis.
[13] .Hongx Hu, Student Member, IEEE, Gail-Joon Ahn, Senior Member, IEEE, and Ketan Kulkarni ,"Detecting and Resolving Firewall Policy Anomalies" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 3, MAY/JUNE 2012.
[14] 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.
[15] Y. Bartal, A. J. Mayer, K. Nissim, and A. Wool. Firmato: A novel firewall management toolkit. *Technical Report EES2003-1, Dept. of Electrical Engineering Systems, Tel Aviv University*, 2003.
[16] E. Al-Shaer and H. Hamed. "Firewall Policy Advisor for Anomaly Detection and Rule Editing." IEEE/IFIP Integrated Management Conference (IM'2003), March(2003).
[17] "Fireman: A Toolkit for Firewall Modeling and Analysis," L.Yuan, H. Chen, J. Mai, C. Chuah, Z. Su, P. Mohapatra, and C.Davis, Proc. IEEE Symp. Security and Privacy, p. 15,2006.
[18] 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.
[19] . L. Yuan, H. Chen, J. Mai, C.-N. Chuah, Z. Su, and P. Mohapatra. Fireman: a toolkit for firewall modeling and analysis. In *IEEE S&P*, pages 199 – 213, 2006.
[20] H. Hamed, E. Al-Shaer "Taxonomy of Conflicts in Network Security Policies." IEEE Communications Magazine Vol.44, No.3, 2006.

