International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 5, Sep - Oct. 2013 pp-2916-2919 ISSN: 2249-6645

An Effective Policy Anomaly Management Framework for Firewalls

Akula Kranthi Kumar[1], Syed Gulam Gouse[2]
[1]*M.Tech, Nimra College of Engineering & Technology, Vijayawada, A.P., India.*
[2]*Professor, Dept.of CSE, Nimra College of Engineering & Technology, Vijayawada, A.P., India.*

ABSTRACT: *Firewalls are devices or programs that control the flow of network traffic between hosts or networks that employ differing security postures. While firewalls are often discussed in the context of Internet connectivity, they may also have applicability in various other network environments. At one time, most firewalls were deployed at the network perimeters. This provided some measure of protection for internal hosts, but it could not recognize all instances and forms of attacks, and attacks sent from one internal host to another often do not pass through network firewalls. Because of these and other factors network designers now often include firewall functionality at places other than the network perimeter to provide an additional layer of network security. Due to the increasing threat of network attacks, firewalls have become important integrated elements not only in the enterprise networks but also in small-size and home networks. Firewalls have been the frontier defense for secure networks against attacks and unauthorized traffic by filtering out unnecessary network traffic coming into or going from the secured network. In this paper, we represent an effective policy anomaly management framework for firewalls, adopting a rule-based segmentation technique to identify policy anomalies and derive effective anomaly resolutions.*

Keywords: *Anomalies, FAME, Firewall, Policies.*

I. INTRODUCTION

With the global Internet connection, network security has gained significant attention in both the research and industrial communities. Due to the increasing threat of network attacks, firewalls have become important integrated elements not only in the enterprise networks but also in small-size and home networks. A firewall is a security guard placed at the point of entry between a private network and the outside Internet so that all incoming and outgoing traffic have to pass through it. A packet can be viewed as a tuple with a finite number of fields; examples of these fields are source/destination IP address, source/destination port number, and protocol type. By examining the values of these fields for each incoming and outgoing packet, a firewall accepts legal packets and discards illegitimate ones according to its configuration.

A firewall configuration defines which packets are legal and which are illegal. An error in a firewall configuration means a wrong definition of being legitimate or illegitimate for some packets, which will either allow unauthorized access from the outside Internet to the private network, or disable some legitimate communication between the private network and the outside network. How to design a correct firewall configuration is therefore a very important security issue. Firewalls have been the frontier defense for secure networks against many attacks and unauthorized traffic by filtering out unwanted network traffic coming into or going from the secured network. The filtering decision is taken according to a set of ordered filtering rules written based on the predefined security policy requirements. Although deployment of firewall technology is an important step toward securing the networks, the complexity of managing firewall policy might limit the effectiveness of firewall security. A firewall policy may include anomalies, where a network packet may match with two or more different filtering rules.

When the filtering rules are defined, serious attention has to be given to rule relations and interactions in order to determine the proper rule ordering and to guarantee correct security policy semantics. As the number of filtering rules increases, then the difficulty of writing a new rule or modifying an existing one also increases. It is very likely, in this case, to introduce the conflicting rules such as one general rule shadowing another specific rule, or correlated rules whose relative ordering determines different actions for the same packet. In addition, a typical large-scale enterprise network might involve hundreds of rules that might be written by various administrators in various times. This significantly increases the potential of the anomaly occurrence in the firewall policy, jeopardizing the security of the protected network [1]. Therefore, the effectiveness of the firewall security is dependent on providing policy management techniques and tools that enable network administrators to analyze and verify the correctness of written firewall legacy rules.

II. RELATED WORK

Effective mechanisms and tools for policy management are crucial to the success of the firewalls. Recently, policy anomaly detection has received a great deal of attention [2], [3], [4], [5]. Corresponding policy analysis tools, such as Firewall Policy Advisor [2] and FIREMAN [3], with the goal of detecting the policy anomalies have been introduced. Firewall Policy Advisor only has the capability of detecting pairwise anomalies in firewall rules. FIREMAN can detect anomalies among multiple rules by analyzing the relationships between one rule and the collections of packet spaces derived from all the preceding rules. However, FIREMAN also has several limitations in detecting anomalies [4]. For each firewall rule, FIREMAN only examines all the preceding rules but ignores all subsequent rules when performing anomaly analysis. In addition, each analysis result from FIREMAN can only show that there is a misconfiguration between oner ule and its preceding rules, but cannot accurately indicate all the rules involved in an anomaly.

A first approach to addressing our problem domain is the use of the refinement mechanisms. In this way, we can perform a top-down deployment of the rules by unfolding a global set of security policies into the configurationsof several components and guaranteeing that those deployed configurations are free of anomalies. In [6], for example, the authors present a refinement method that uses a formal model for the generation of filtering rules by transforming general rules into specific configuration rules. Indeed, the authors propose the use of roles to better define of network capabilities, and the use of an inheritance mechanism through a hierarchy of entities to automatically generate permissions and prohibitions. A second refinement approach based on the concept of roles is also presented in [7]. However, and although the authors claim that their work is based on the Role Base Access Control (RBAC) model, their specification of the network entities, roles, and permission assignments are not rigorous and does not fit any reality. Most of these limitations are solved in the approach as presented in [8], where a global set of rules based on theOrganization Based Access Control (OrBAC) model [2] are further deployed into specific firewall configuration files through a transformation process. Generally, the administrators are reluctant to set up from scratch a whole network security policy, and prefer recycling existing configurations.

III. FIREWALL POLICIES AND ANOMALIES

A firewall policy rule is defined as a set of criteria and an action to perform when a network packet matches the criteria. The criteria of a rule consist of the elements direction, protocol, source port, source IP, destination IP and destination port. Therefore a complete rule may be defined by the ordered tuple <direction, protocol, source IP, source port, destination IP, destination port, action>. Each attribute can be defined as a range of values, which can be represented and analyzed as the sets. The relation between two rules essentially mean that the relation between the set of packets they match. Thus the action field does not come into play when considering the relation between the two rules. Firewall policy anomaly is defined as the existence of two or more firewall filtering rules that may match the same packet . The existence of a rule that can never match any network packet on the network paths that cross the firewall also cause anomaly. Till date, five types of anomalies are discovered – they are: Shadowing Anomalies, Correlation Anomalies, Generalization Anomalies, Redundancy Anomalies, and Irrelevance Anomalies.

Shadowing anomaly: Two rules are said to have shadowing anomaly ,whenever the rule which comes first in the 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.

Correlation anomaly: Two rules are said to have correlation anomaly if both of the rules matches some common packets that is the rule one matches some packets, which are also matched by the rule second.

Generalization anomaly: Two rules which are in order one of them is said to be in the 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.

Redundancy anomaly: Two rules are said to be redundant if both of the rules matches some packets and the action performed is also the same. So there is no effect on the firewall policy if one of the redundant rules will be removed from the rule set.

Irrelevance anomaly: Any rule is said to be irrelevant if for a given time interval it does not matches any of the network packets either incoming or outgoing. Thus if any type of the packets do not match the rule then it is irrelevant i.e. there is no need to put that rule in the rule set.

IV. ANOMALY MANAGEMENT FRAMEWORK

In our proposed policy anomaly management framework is composed of two core functionalities: conflict detection and resolution, and redundancy discovery and removal, as depicted in Figure 1. Both of the functionalities are based on the rule-based segmentation technique. For conflict detection and resolution, conflicting segments are identified only in the first step. Each conflicting segment associates with the policy conflict and a set of conflicting rules. Also, the correlation relationships among the conflicting segments are identified and conflict correlation groups (CG) are derived. Policy conflicts belonging to different conflict correlation groups can be resolved separately; thus, the searching space for resolving the conflicts is reduced by the correlation process. The second step generates an action constraint for each of the conflicting segment by examining the characteristics of each conflicting segment. A strategy-based method is introduced for generating the action constraints. The third step utilizes a reordering algorithm, which is a combination of the permutation algorithm and a greedy algorithm, to discover a near-optimal conflict resolution solution for policy conflicts. Regarding redundancy discovery and removal, the segment correlation groups are first identified. Then, the process of the property assignment is performed to each rule's subspaces.

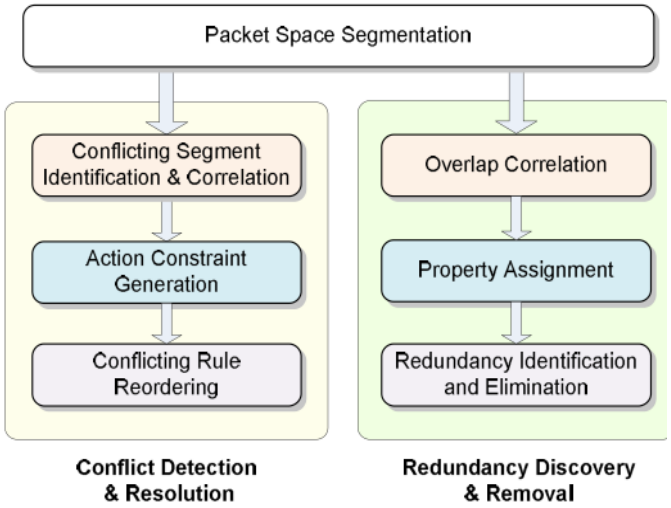

Figure 1: Policy anomaly management framework

A. Conflict Resolution

Our conflict resolution mechanism introduces that an action constraint is assigned to each of the conflicting segment. An action constraint for the conflicting segment defines a desired action (either Allow or Deny) that the firewall policy should take when any packet within the conflicting segment comes to the firewall. Then, to resolve the conflict, we only assure that the action taken for each packet within the conflicting segment can satisfy the corresponding action constraint. To generate action constraints for conflicting segments, we propose a strategy-based conflict resolution method, which generates the action constraints with the help of effective resolution strategies based on the minimal interaction with system administrators. Figure 2 shows the main processes of this method, which incorporates both automated and manual strategy selections. Once conflicts in the firewall policy are discovered and conflict correlation groups are identified, the risk assessment for conflicts is performed.

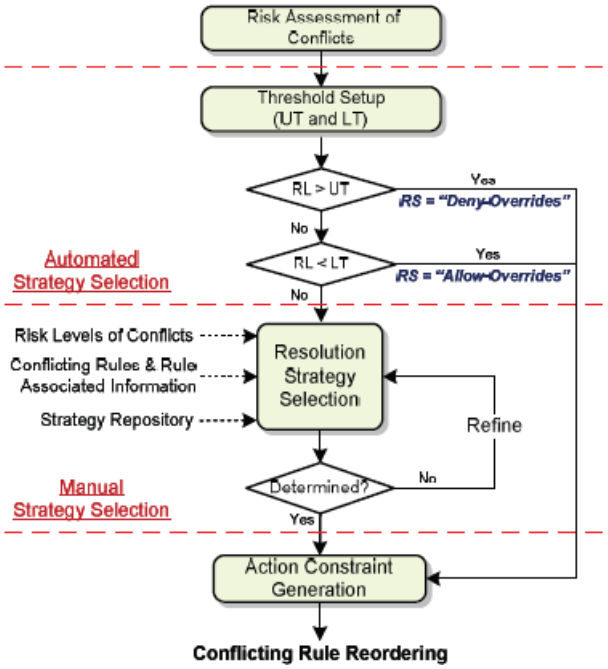

Figure 2: Strategy-based conflict resolution

B. Implementation of FAME

FAME was implemented in Java language. Based on our policy anomaly management framework, it consists of 6 components: segmentation module, correlation module, risk assessment module, action constraint generation module, rule reordering module, and property assignment module. The segmentation module takes the firewall policies as an input and identifies the packet space segments by partitioning the packet space into disjoint subspaces. Our framework is realized as a proof-of-concept prototype called as Firewall Anomaly Management Environment. Figure 3 shows a high-level architecture of FAME with two levels. The upper level is the visualization layer, which visualizes the results of the policy anomaly analysis to system administrators. Two visualization interfaces, policy conflict viewer and the policy redundancy viewer, are designed to manage policy conflicts and redundancies, respectively. The lower level of the architecture provides underlying

functionalities addressed in our proposed policy anomaly management framework and relevant resources including rule information, strategy repository, network asset information, and vulnerability information.

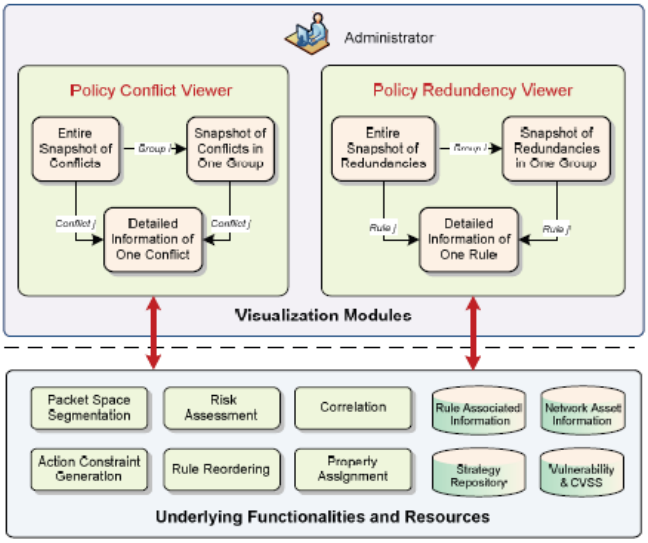

Figure 3: Architecture of FAME

V. CONCLUSION

A firewall is a system acting as an interface of a network to one or more external networks, for example, Internet. It implements the security policies of the network by deciding which packets to let through based on rules defined by the network administrator. Any error in defining the rules may compromise the system security by letting unwanted network traffic pass or blocking desired traffic. Manual definition of the rules often results in a set that contains conflicting, redundant or overshadowed rules, resulting in anomalies in the policy. Manually detecting and resolving these anomalies is a critical task but tedious and error prone task. Existing research on this problem have been focused on the analysis and detection of the anomalies in the firewall policy. A rule-based segmentation mechanism and a grid-based representation technique were introduced to achieve the goal of effective and efficient firewall anomaly analysis. In addition, it is demonstrated that our proposed work is practical and helpful for system administrators to enable an assurable network management.

REFERENCES

[1] E. Al-Shar and H. Hemed. “Firewall Policy Advisor for Anomaly Detection and Rule Editing.” Proc.of IEEE/IFIP Integrated Management Conference (IM’2003), March 2003.
[2] E. Al-Shaer and H. Hamed, “Discovery of Policy Anomalies inDistributed Firewalls,” IEEE INFOCOM ’04, vol. 4, pp. 2605-2616,2004.
[3] L. Yuan, H. Chen, J. Mai, C. Chuah, Z. Su, P. Mohapatra, and C.Davis, “Fireman: A Toolkit for Firewall Modeling and Analysis,”Proc. IEEE Symp. Security and Privacy, p. 15, 2006.
[4] J. Alfaro, N. Boulahia-Cuppens, and F. Cuppens, “CompleteAnalysis of Configuration Rules to Guarantee Reliable NetworkSecurity Policies,” Int’l J. Information Security, vol. 7, no. 2, pp. 103122,2008.
[5] F. Baboescu and G. Varghese, “Fast and Scalable ConflictDetection for Packet Classifiers,” Computer Networks, vol. 42,no. 6, pp. 717- 735, 2003.
[6] Bartal, Y., Mayer, A., Nissim, K., and Wool, A. Firmato: A novel firewall management toolkit. In IEEE Symposiumon Security and Privacy, pp. 17–31, Oakland, California, May, 1999.
[7] Reed, D. IP Filter. [Online]. Available from:http://www.ja.net/CERT/Software/ipfilter/ip-filter.html
[8] Hassan, A. and Hudec, L. Role Based Network Security Model: A Forward Step towards Firewall Management.In Workshop On Security of Information Technologies, Algiers, December, 2003.