IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 5 (Mar. - Apr. 2013), PP 56-60
www.iosrjournals.org

Auto Finding and Resolving Distributed Firewall Policy

Arunkumar.k[1], Suganthi.B[2]
PG Scholar[1] , Department of Electronics and Communication, Dhanalakshmi Srinivasan Engineering College, perambalur.
Associate Professor[2] ,Department of Electronics and Communication, Dhanalakshmi Srinivasan Engineering College, perambalur.

Abstract:*-In the network environment firewall is one of the protection layers. A firewall policy defines how an organization's firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization's information security policies. In this paper, we propose a set of firewall policy to support distributed environment of firewalls. We also represent a set of firewall policies to automatically detecting and resolving anomalies in the network layer. we adopt a rule-based segmentation technique to identify policy anomalies and derive effective anomaly resolutions. we demonstrate how efficiently our approach can discover and resolve anomalies with conflict packet and resolved packets.*

Index terms*- Firewall, policy anomaly management, access control, visualization tool, anomaly.*

I. Introduction

A firewall is basically the first line of defense for any network. A firewall can be a hardware device or a software application and generally is placed at the perimeter of the network to act as the gatekeeper for all incoming and outgoing traffic. A firewall allows any one to establish certain rules to determine what traffic should be allowed in or out of the private network. Depending on the type of firewall implemented, any one could restrict access to only certain IP addresses, domain names and can block certain types of traffic by blocking the TCP/IP ports they use. There are basically four mechanisms used by firewalls to restrict traffic such as packet-filtering, circuit-level gateway, proxy server and application gateway[1]. A device or an application may use more than one of these to provide more in-depth protection. With the global Internet connection, network security has gained significant attention in research and industrial communities. Due to the increasing threat of network attacks, firewalls have become important integrated elements not only in enterprise networks but also in small-size and home networks. Firewalls have been the frontier defense 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 [2]. Firewalls are protecting devices which ensure an access control. They manage the traffic between the public network and the private network zones on one hand and between private zones in the local network on the other hand. Network identifiers are detection devices that monitor the traffic and generate alerts in the case of suspicious traffic. The attributes used to block or to generate alerts are almost the same. When these two components coexist in the security architecture of an information system the challenge is to avoid inter-configuration anomalies [3]. In the network environment the firewalls are the cornerstone of corporate intranet security. This mode of firewalls is not able to detect all type of unauthorized entries, and can only measures the network performance. A rule set's complexity is positively correlated with the number of detected configuration errors [4].

II. Related Works

In [5] Fast and Scalable Conflict Detection for Packet Classifiers is proposed, It address the problem of handling large size data base, conflict detection and packet classification in the bit vector schemes. Conflicts in policy based distributed systems management focus on conflicts arising from positive and negative policies and application specific conflicts [6].An innovative policy anomaly analysis approach for web control policy [7] utilizes policy based segmentation technique into order to accurately identify policy anomalies. In [8] a frame work for programmable network measurement is proposed. Here traffic statistic is considered based one flow set. A tool kit for firewall modeling analysis [9] applies static analysis to check miss configurations. The implementation is achieved by firewall rules using binary decision diagram. In [10] an innovative policy anomaly management frame work for firewalls is proposed. It adopts a rule based segmentation technique to identify policy anomalies. How ever it supports a centralized firewall system in failed to support distributed environment.

III. Distributed Firewalls:

In the distributed firewall system the enforcement of policy is done by network endpoints. Distributed systems may contain a large number of objects and potentially cross organizational boundaries. New components and services are added or removed from the system dynamically, thus changing the requirements of the management system over a potentially long lifetime. There has been considerable interest recently in policy-based management for distributed systems. A Policy is information which can be used to modify the behavior of a system. Separating policies from the managers permits the modification of the policies to change the behavior and strategy of the management system without re-coding the managers.

The management system can then adapt to changing requirements by disabling policies or replacing old policies with new one without shutting down the system. We are concerned with two types of policies. Authorization policies are essentially security policies related to access-control and specify what activities a subject is permitted or forbidden to do to a set of target objects. Obligation policies specify what activities a subject must or must not do to a set of target objects and define the duties of the policy subject. We permit the specification of both positive and negative authorization policies which requires an explicit authorization.

III. A. Anomalies In Distributed Firewall Policy

A firewall policy consists of a sequence of rules that define the actions performed on packets that satisfy certain conditions. The rules are specified in the form of _condition, action_. A condition in a rule is composed of a set of fields to identify a certain type of packets matched by this rule. Table 2 shows an example of a firewall policy, which includes five firewall rules r1, r2, r3, r4 and r5.

TABLE 2
An example firewall policy.

Rule	Source		Source	Destination	Action
	Destination Protocol	IP	Port IP	Port	
r1	UDP	20.1.2.*	* 172.32.1.*	43	deny
r2	UDP	20.1.*.*	* 172.32.1.*	43	deny
r3	TCP	20.1.*.*	* 192.168.*.*	15	allow
r4	TCP	20.1.1.*	* 192.168.*.*	15	deny
r5	*	20.1.1.*	* *	*	allow

Based on following classification, we articulate the typical firewall policy anomalies.

A rule can be shadowed by one or a set of preceding rules that match all the packets which also match the shadowed rule, while they perform a different action. In this case, all the packets that one rule intends to deny (accept) can be accepted (denied) by previous rule(s), thus the shadowed rule will never be taken effect. In Table 2, r4 is shadowed by r3 because r3 allows every TCP packet coming from any port of 20.1.1.* to the port 15 of 192.168.1.*, which is supposed to be denied by r4.

Generalization:

A rule is a generalization of one or a set of previous rules if a subset of the packets Matched by this rule is also matched by the preceding Rule but taking a different action. For example, r5 is a generalization of r4 in Table 1. These two rules indicate that all the packets from 10.1.1.* are allowed, except TCP packets from 10.1.1.* to the port 25 of 192.168.1.*. Note that, as we discussed earlier, generalization might not be an error.

IV. Fame Tool

Our framework is realized as a proof-of-concept prototype called Firewall Anomaly Management Environment (FAME). FAME has two levels. The upper level is the visualization layer, which visualizes the results of policy anomaly analysis to system administrators. Two visualization interfaces, policy conflict viewer and policy redundancy viewer, are designed to manage policy conflicts and redundancies, respectively.

The lower level of the architecture provides underlying functionalities addressed in our policy anomaly management framework and relevant resources including rule information, strategy repository, network asset information, and vulnerability information. FAME is implemented in Java. Based on our policy anomaly management framework, it consists of six components: segmentation module, correlation module, risk assessment module, action constraint generation module, rule reordering module, and property assignment module. The segmentation module takes firewall policies as an input and identifies the packet space segments by partitioning the packet space into disjoint subspaces.

V. IMPLEMENTATION

The distributed firewall anomaly detection is implemented in Java Net Beans.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, we introduce a rule-based segmentation techniques and grid based segmentation, which adopts a binary decision diagram (BDD)-based data structure to represent rules and perform various set operations, to convert a list of rules into a set of disjoint network packet spaces.

Rule Reordering

The most ideal solution for conflict resolution is that all action constraints for conflict segments can be satisfied by reordering conflict rules. Unfortunately, in practice an action constraints for conflict segments can only be satisfied partially in some cases.

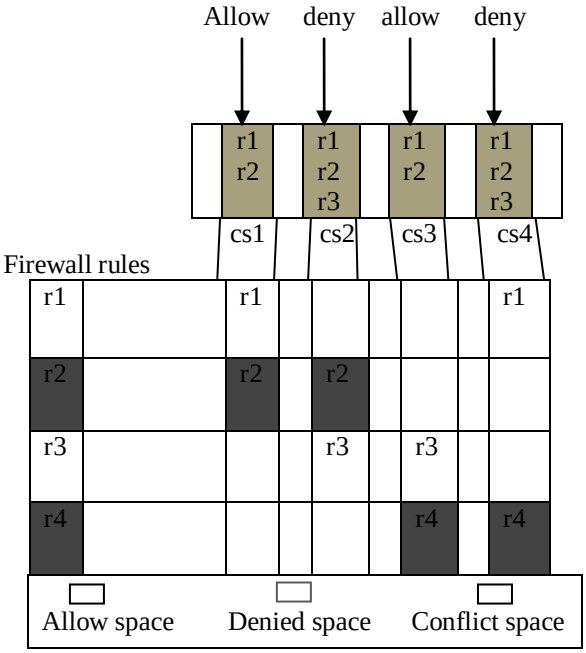

Fig.4.3.1. Partial sat isfaction of action constraints.

Redundancy Elimination

In this step, every rule subspace covered by a policy segment is assigned with a property value: removable(R), strong irremovable (SI), Weak irremovable (WI) and Correlated (C). These are defined to reflect different characteristics of each rule subspace. Removable property is used to indicate that, removing such a rule subspace does not make any impact on the original packet space of an associated policy.

Strong irremovable property indicates that a rule subspace cannot be removed because the action of corresponding policy segment can be decided only by this rule. Weak irremovable property is assigned to a rule subspace when any subspace belonging to the same rule has Strong irremovable property. Correlated property is assigned to multiple rule subspaces covered by a policy segment, if the action of this policy segment can be determined by any of these rules.

VI. Result And Discussion

The performance of distributed firewall policy is analyses with the help of the performance metric namely security risk value.

Fig.5.1. Risk Reduction

The security risk value indicates the protection level of transfer of packets. The policy parameter denotes the types of rule assignments. Simulation is carried for worst case (packet transmission along with threats) and best case(transmission of resolved packets). In Figure 5.1,it is observed that the security risk values of the conflict-resolved policies are always reduced compared to the security risk value of the original policies. The experiment shows that FAME could achieve an average 45% of risk reduction by using FAME tool compared with existing firewall system.

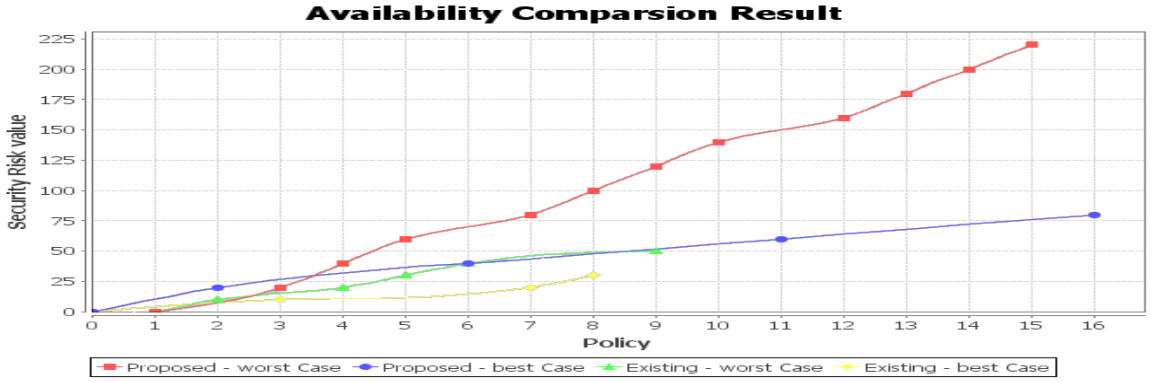

Fig.5.2. Availability improvement

In Figure 5.2, clearly show that the availability loss value for each resolved policy is lower than that of corresponding original policy, which supports our hypothesis that resolving policy conflicts can always improve the availability of protected network.

VII. Conclusions

In this paper, we have proposed a novel anomaly management framework that facilitates systematic detection and resolution of distributed firewall policy anomalies. A rule-based segmentation mechanism and a grid-based representation technique were introduced to achieve the goal of effective and efficient anomaly analysis. Our experimental results show that around 92% of conflicts can be resolved by using our FAME tool. There may still exist requirements for a complete conflict resolution, especially for some firewalls in protecting crucial networks. The FAME tool can help achieve this challenging goal. First, FAME provides a grid-based visualization technique to accurately represent conflict diagnostic information and the detailed information for unresolved conflicts that are very useful, even for manual conflict resolution. Second, FAME resolves conflicts in each conflict correlation group independently, i.e. a system administrator can focus on analyzing and resolving conflicts belonging to a conflict correlation group individually. Our future work is extending the distributed firewall system to wireless distributed firewall security system.

Acknowledgments

I would like to thank Mrs. B. Suganthi, Associate professor in Dhanalakshmi Srinivasan Engineering College for guiding me to bring this paper successful.

References

[1] M. Frigault, L. Wang, A. Singhal, and S. Jajodia, "Measuring Network Security Using Dynamic Bayesian Network," Proc. Fourth ACM Workshop Quality of Protection, 2008

[2] E. Al-Shaer and H. Hamed, "Discovery of Policy Anomalies in Distributed Firewalls," IEEE INFOCOM '04, vol. 4, pp. 2605-2616, 2004.

[3] J. Alfaro, N. Boulahia-Cuppens, and F. Cuppens, "Complete Analysis of Configuration Rules to Guarantee Reliable Network Security Policies," Int'l J. Information Security, vol. 7, no. 2, pp. 103- 122, 2008.

[4] A. Wool, "Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese," IEE internet computing, vol. 14, no. 4, pp. 58–65, 2010

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

[6] E. Lupu and M. Sloman, "Conflicts in Policy-Based Distributed Systems Management," IEEE Trans. Software Eng., vol. 25, no. 6, Nov./Dec. 1999.

[7] I. 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.

[8] H. Hu, G. Ahn, and K. Kulkarni, "Anomaly Discovery and Resolution in Web Access Control Policies," Proc. 16th ACM Symp. Access Control Models and Technologies, pp. 165-174, 2011.

[9] L. Yuan, C. Chuah, and P. Mohapatra, "ProgME: Towards Programmable Network Measurement," ACM SIGCOMM Computer Comm. Rev., vol. 37, no. 4, p. 108, 2007.

[10] L. Yuan, H. Chen, J. Mai, C. Chuah, Z. Su, P. Mohapatra, and C. Davis, "Fireman: A toolkit for firewall modeling and analysis," in ,2006IEEE Symposium on security and privacy, 2006, p. 15.

[11] Hongxin Hu, Gail-joon Ahn, Ketan Kulkarni, "Detecting and Resolving Firewall Policy anomalies" IEEE Secure Computing, may 2012

[12] S. Ioannidis, A. Keromytis, S. Bellovin, and J. Smith, "Implementing a distributed firewall," in Proceedings of the 7th ACM conference on computer and communication security. ACM, 2000, p. 199.

[13] N. Li, Q. Wang, W. Qardaji, E. Bertino, P. Rao, J. Lobo, and D. Lin,"Access Control Policy Combining: Theory Meets Practice," Proc.14th ACM Symp. Access Control Models and Technologies, pp. 135-144, 2009.

[14] J. Jin, G. Ahn, H. Hu, M. Covington, and X. Zhang, "Patient-Centric Authorization Framework for Sharing Electronic Health Records," Proc. 14th ACM Symp. Access Control Models and Technologies, pp. 125-134, 2009.

[15] J. Jin, G. Ahn, H. Hu, M. Covington, and X. Zhang, "Patient-Centric Authorization Framework for Electronic Healthcare Services," Computers and Security, vol. 30, no. 2, pp.16-127, 2011.