Detecting and Resolving Firewall Policy Anomalies

M.Meera[#1], Mrs. M.Kamarunisha, MCA.,M.Phil.,Ph.D., [#2]
Pg Scholar, Head of the Department &DSCASW College
Department of MCA &Dhanalakshmi Srinivasan College of Arts and Science for Women's- Perambalur, Tamilnadu, India
[1]sumathimeera121295,[2]kamar6672@gmail.com

Abstract

The advent of emerging computing technologies such as service-oriented architecture and cloud computing has enabled us to perform business services more efficiently and effectively. However, we still suffer from unintended security leakages by unauthorized actions in business services. Firewalls are the most widely deployed security mechanism to ensure the security of private networks in most businesses and institutions. The effectiveness of security protection provided by a firewall mainly depends on the quality of policy configured in the firewall. Unfortunately, designing and managing firewall policies are often error prone due to the complex nature of firewall configurations as well as the lack of systematic analysis mechanisms and tools. In this paper, we represent an innovative policy anomaly management framework for firewalls, adopting a rule-based segmentation technique to identify policy anomalies and derive effective anomaly resolutions. In particular, we articulate a grid-based representation technique, providing an intuitive cognitive sense about policy anomaly. We also discuss a proof-of-concept implementation of a visualization-based firewall policy analysis tool called Firewall Anomaly Management Environment (FAME). In addition, we demonstrate how efficiently our approach can discover and resolve anomalies in firewall policies through rigorous experiments.

Keywords: Firewall, policy anomaly management, access control, visualization tool

INTRODUCTION

As one of essential elements in network and information system security, firewalls have been widely deployed in defending suspicious traffic and unauthorized access to Internet-based enterprises. Sitting on the border between a private network and the public Internet, a firewall examines all incoming and outgoing packets based on security rules. To implement a security policy in a firewall, system administrators define a set of filtering rules that are derived from the organizational network security requirements. This is further exacerbated by the continuous evolution of network and system environments. For instance, Al-Shaer and Hammed reported that their firewall policies contain anomalies even though several administrators including nine experts maintained those policies. In addition, Wool recently inspected firewall policies collected from different organizations and indicated that all examined firewall policies have security flaws.Firewall Policy Advisor only has the capability of detecting pair wise 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 preceding rules. However, FIREMAN also has limitations in detecting anomalies. First, the number of conflicts in a firewall is potentially large, since a firewall policy may consist of thousands of rules, which are often logically entangled with each other. Second, policy conflicts

are often very complicated. One rule may conflict with multiple other rules, and one conflict may be associated with several rules. Besides, firewall policies deployed on a network are often maintained by more than one administrator, and an enterprise firewall may contain legacy rules that are designed by different administrators. Since the policy conflicts in firewalls always exist and are hard to be eliminated, a practical resolution method is to identify which rule involved in a conflict situation should take precedence when multiple conflicting rules can filter a particular network packet simultaneously. To resolve policy conflicts, a firewall typically implements a first-match resolution mechanism based on the order of rules. We represent a novel anomaly management framework for firewalls based on a rule-based segmentation technique to facilitate not only more accurate anomaly detection but also effective anomaly resolution. Based on this technique, a network packet space defined by a firewall policy Can be divided into a set of disjoint packet space segments. Each segment associated with a unique set of firewall rules accurately indicates an overlap relation among those rules. We also introduce a flexible conflict resolution method to enable a fine-grained conflict resolution with the help of several effective resolution strategies with respect to the risk assessment of protected networks and the intention of policy definition. Besides, a more effective redundancy elimination mechanism is provided in our framework, and our experimental results show that our redundancy discovery mechanism can achieve approximately 70 percent improvement compared to traditional redundancy detection approaches. Since the policy conflicts in firewalls always exist and are hard to be eliminated, a practical resolution method is to identify which rule involved in a conflict situation should take precedence when multiple conflicting rules (with different actions) can filter a particular network packet simultaneously. To resolve policy conflicts, a firewall typically implements a first-match resolution mechanism based on the order of rules. In this way, each packet processed by the firewall is mapped to the decision of the first rule that the packet matches. However, applying the first-match strategy to cope with policy conflicts has limitations. When a conflict occurs in a firewall, the existing first matching rule may not be a desired rule that should take precedence with respect to conflict resolution. In particular, the existing first matching rule may perform opposite action to the rule which should be considered to take precedence. This situation can cause severe network breaches such as permitting harmful packets to sneak into a private network, or dropping legal traffic which in turn could encumber the availability and utility of network services. Obviously, it is necessary to seek a way to bridge a gap between conflict detection and conflict resolution with the first-match mechanism in firewalls.

RELATED WORK

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

Firewalls are core elements in network security. However, managing 6rewall rules, particularly in multi-firewall enterprise networks, has become a complex and error-prone task. Firewall filtering rules have to be written. Ordered and distributed carefully in order to avoid firewall policy anomalies that might cause network vulnerability. Therefore, inserting or modifying filtering rules w any firewall requires thorough intra- and inter-firewsll analysis to determine the proper rule placement and ordering in the firewalk. In this paper, we identify all anomalies that could exist in a single- or multi-firewall environment. We also present a set of techniques and algorithms to automatically discover policy anomalies in centralized and distributed legacy firewalls. These techniques are implemented in a software tool called the "Firewall Policy Advisor" that simplifies

Available@ www.ijrse.org Mail: info@ijrse.org ISSN: 2212-4012

the management of filtering rules and maintaias the security of next-generation firewalls.

[2] A. Wool, "Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese," IEEE Internet Computing, vol. 14, no. 4, pp. 58-65, July/Aug. 2010.

Security experts generally agree that corporate firewalls often enforce poorly written rule sets. This article revisits a 2004 survey of corporate firewall configurations that quantified the extent of this issue. In addition to being much larger, the current study includes configurations from two major vendors. It also introduces a new firewall complexity measure that applies to both types of firewalls. The study's findings validate the 2004 study's main observations: firewalls are (still) poorly configured, and a rule set's complexity is (still) positively correlated with the number of detected configuration errors. However, unlike the 2004 study, the current study doesn't suggest that later software versions have fewer errors.

[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.

The use of different network security compo-nents, such as firewalls and network intrusion detection systems (NIDSs), is the dominant method to monitor and guarantee the security policy in current corporate networks. To properly configure these components, it is necessary to use several sets of security rules. Never- theless, the existence of anomalies between those rules, particularly in distributed multi-component scenarios, is very likely to degrade the network security policy. The discovery and removal of these anomalies is a serious and complex problem to solve. In this paper, we present a complete set of mechanisms for such a management.**[4] F. Baboescu and G. Varghese, "Fast and Scalable Conflict Detection for Packet Classifiers," Computer Networks, vol. 42, no. 6, pp. 717-735, 2003.**

Packet filters provide roles for classifying packets based on header fields. High speed packet classification has received much study. However, the twin problems of fast updates and fast conflict detection have not received much attention. A conflict occurs when two classifiers overlap, potentially creating ambiguity for packets that match both filters. For example, if Rule 1 specifies that all packets going to CNN be rote controlled and Rule 2 specifies that all packets coming from Walmart be given high priority, the roles conflict for traffic from Walmart to CNN. There has been prior work on efficient conflict detection for two dimensional classifiers. However, the best known algorithm for conflict detection for general classifier is the naive O(N2) algorithm of comparing each pair of rues for a conflict. In this paper, we describe an efficient and scalable conflict detection algorithm for the general case that is significantly faster. For example, for a database of 20,000 roles, our algorithm is 40 times faster than the effective implementation. Even without considering conflicts, our algorithm also provides a packet classifier with fast updates and fast lookups that can be used for stateful packet filtering.

EXISITING PROCESS

Firewalls are the most widely deployed security mechanism to ensure the security of private networks in most businesses and institutions. The effectiveness of security protection provided by a firewall mainly depends on the quality of policy configured in the firewall. Unfortunately, designing and managing firewall policies are often error prone due to the complex nature of firewall configurations as well as the lack of systematic analysis mechanisms and tools.

DISADVANTAGES OF EXISITNG SYSTEM

- Admin can detect anomalies among multiple rules by analyzing the relationships between one rule and the collections of packet spaces derived from all preceding rules.
- For each firewall rule, FIREMAN only examines all preceding rules but ignores all subsequent rules when performing anomaly analysis

PROPOSED PROCESS

In this proposed system, represent an innovative policy anomaly management framework for firewalls, adopting a rule-based segmentation technique to identify policy anomalies and derive effective anomaly resolutions. In particular, we articulate a grid-based representation technique, providing an intuitive cognitive sense about policy anomaly. We also discuss a proof-of-concept implementation of a visualization-based firewall policy analysis tool called Firewall Anomaly Management Environment (FAME). In addition, we demonstrate how efficiently our approach can discover and resolve anomalies in firewall policies through rigorous experiments.

ADVANTAGES OF PROPOSED

- Detection and resolution
- Set of conflicting rules

PROCESS

1. Rule Generation

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.

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(s) but taking a different action. 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.

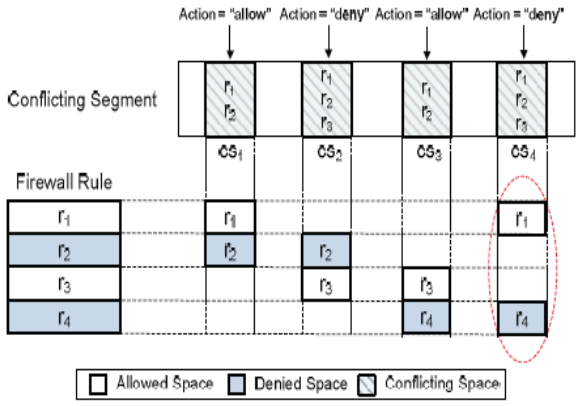

Fig 1 Rule Generation

2. Update Conflict

Each conflicting segment indicates a policy conflict as well as a set of conflicting rules involved in the conflict. Once conflicts are identified, a possible way for a system administrator to resolve conflicts is to manually change the conflicting rules. Resolving all conflicts manually is a tedious task and even impractical due to the complicated nature of policy conflicts. Thus, a practical and effective method to resolve a policy conflict is to determine which rule should take precedence when a network packet is matched by a set of rules involved in the conflict. In order to utilize the existing first-match conflict resolution mechanism implemented in common firewalls, the rule expected to take precedence needs to be moved to the first-match rule .Generating position indicators for each conflicting

segment. A position indicator of a rule for a conflicting segment indicates a position range in which this rule can stay so that the action constraint of the conflicting.

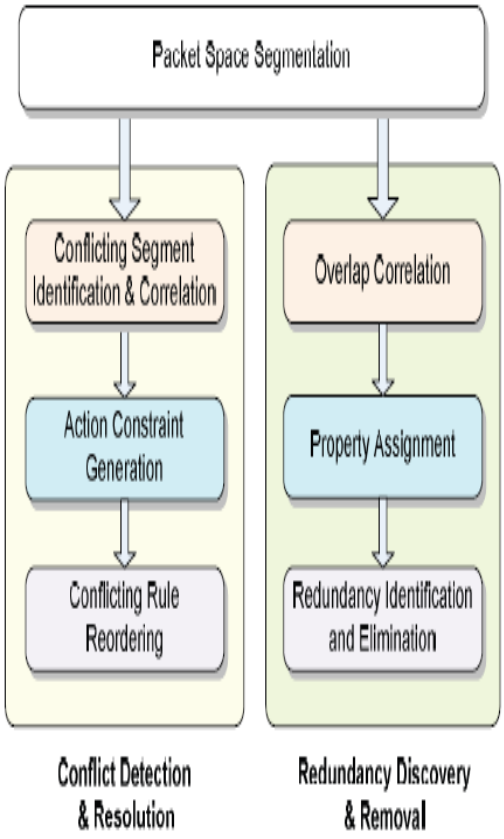

Fig 2 Update Conflict

3) Correlation of Packet Space Segment

The major benefit of generating correlation groups for the anomaly analysis is that anomalies can be examined within each group independently, because all correlation groups are independent of each other. Especially, the searching space for reordering conflicting rules in conflict resolution can be significantly lessened and the efficiency of resolving conflicts can be greatly improved.

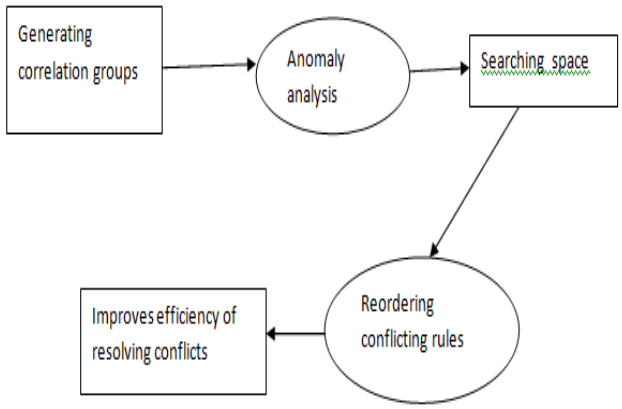

Fig 3 Update Conflict

4) Data Package

When conflicts in a policy are resolved, the risk value of the resolved policy should be reduced and the availability of protected network should be improved comparing with the situation prior to conflict resolution based on the threshold value data will be received in to the server.

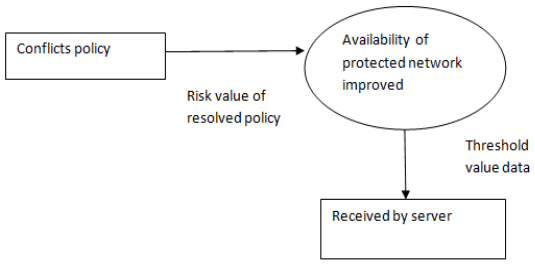

Fig 4 Data Package

5) Action Constraint Generation

In a firewall policy are discovered and conflict correlation groups are identified, the risk assessment for conflicts is performed. The risk levels of conflicts are in turn utilized for both automated and manual strategy selections. A basic

idea of automated strategy selection is that a risk level of a conflicting segment is used to directly determine the expected action taken for the network packets in the conflicting segment. If the risk level is very high, the expected action should deny packets considering the protection of network perimeters

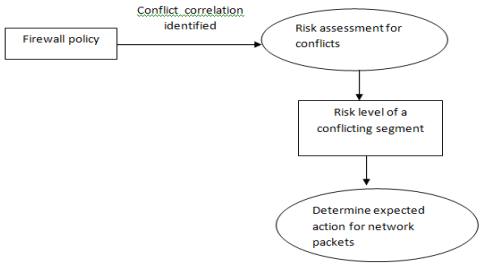

Fig 5 Action Constraint Generation

6) Rule Reordering

The solution for conflict resolution is that all action constraints for conflicting segments can be satisfied by reordering conflicting rules. In conflicting rules in order that satisfies all action constraints, this order must be the optimal solution for the conflict resolution.

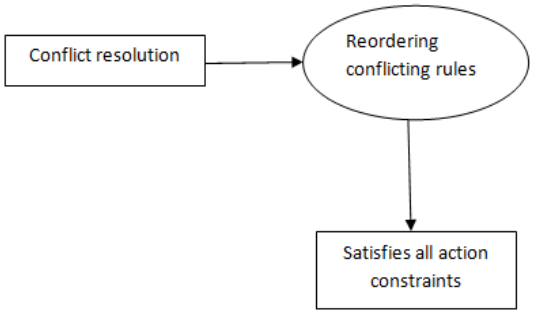

Fig 6 Rule Reordering

ARCHITECTURE DIAGRAM

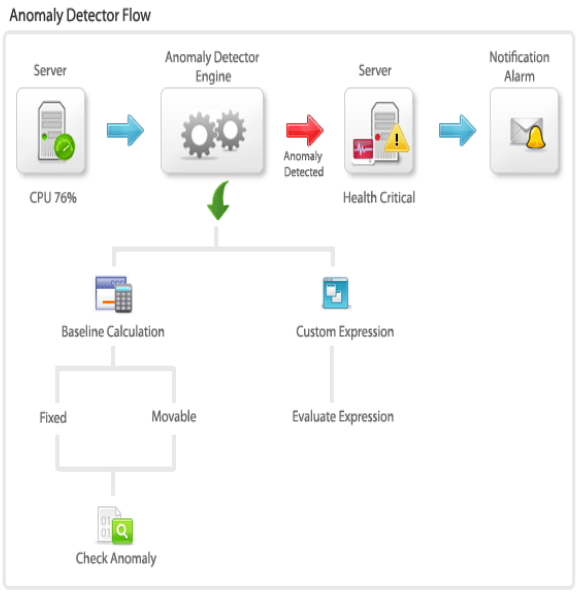

Fig 7 Architecture Diagram

CONCLUSION

We have proposed a novel anomaly management framework that facilitates systematic detection and resolution of firewall policy anomalies. We represent a novel anomaly management framework for firewalls based on a rule-based segmentation technique to facilitate not only more accurate anomaly detection but also effective anomaly resolution. A rule-based segmentation mechanism and a grid-based representation technique were introduced to achieve the goal of effective and efficient anomaly analysis. We also introduce a flexible conflict resolution method to enable a fine-grained conflict resolution.

REFERENCE

[1] E. Al-Shaer and H. Hamed, “Discovery of Policy Anomalies in Distributed Firewalls,” IEEE INFOCOM ’04, vol. 4, pp. 2605-2616, 2004.

[2] A. Wool, “Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese,”

Available@ www.ijrse.org Mail: info@ijrse.org ISSN: 2212-4012

IEEE Internet Computing, vol. 14, no. 4, pp. 58-65, July/Aug. 2010.

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

[5] 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.

[6] E. Lupu and M. Sloman, "Conflicts in Policy-Based Distributed Systems Management," IEEE Trans. Software Eng., vol. 25, no. 6, pp. 852-869, 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] A. El-Atawy, K. Ibrahim, H. Hamed, and E. Al-Shaer, "Policy Segmentation for Intelligent Firewall Testing," Proc. First Workshop Secure Network Protocols (NPSec '05), 2005.

[11] G. Misherghi, L. Yuan, Z. Su, C.-N. Chuah, and H. Chen, "A General Framework for Benchmarking Firewall Optimization Techniques," IEEE Trans. Network and Service Management, vol. 5, no. 4, pp. 227-238, Dec. 2008. [12] M. Frigault, L. Wang, A. Singhal, and S. Jajodia, "Measuring Network Security Using Dynamic Bayesian Network," Proc. Fourth ACM Workshop Quality of Protection, 2008.

[13] M. Sahinoglu, "Security Meter: A Practical Decision-Tree Model to Quantify Risk," IEEE Security and Privacy, vol. 3, no. 3, pp. 18-24, May 2005.

[14] R. Sawilla and X. Ou, "Identifying Critical Attack Assets in Dependency Attack Graphs," Proc. 13th European Symp. Research in Computer Security (ESORICS), 2008.

[15] P. Mell, K. Scarfone, and S. Romanosky, "A Complete Guide to the Common Vulnerability Scoring System Version 2.0," Published by FIRST—Forum of Incident Response and Security Teams, June 2007.

[16] I. Fundulaki and M. Marx, "Specifyir Access Control Policies for XML Documents wi Xpath," Proc. Ninth ACM Symp. Access Control Models and Technologies, pp. 61-69, 2004.

[17] S. Jajodia, P. Samarati, and V.S. Subrahmanian, "A Logical Language for Expressing Authorizations," Proc. IEEE Symp. Security and Privacy, pp. 31-42, May 1997.

[18] T. Moses, "Extensible Access Control Markup Language (XACML), Version 2.0, Oasis Standard," Internet, http:// docs.oasis-open.org/xacml/2.0/accesscontrol-xacml-2.0-corespec- os.pdf, 2005.

[19] 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.

[20] 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.

BIOGRAPHICAL NOTES

	Mrs.Kamarunisha.M.A-Received M.C.A.,M.Phil.,Degree in computer Science. She has 19 Years of Teaching Experience.She is Guided 7 Students in M.Phil.,She had Presented 8 Papers in International Conference and also She Presented 7 Papers in National Conference.She is Currently Working has Associate Professor in Department of Computer Applications in Dhanalakshmi Srinivasan College of Arts & Science for Women,Perambalur,TamilNadu,India.
	Miss.Meera.M.PG Scholar,[Department of Computer Applicatons],pursuing MCA in Dhanalakshmi Srinivasan College of Arts & Science for Women,Perambalur-621212,TamilNadu,(India)