IPHV1I90004x
International Journal Of Advanced Research and Innovations Vol.1, Issue .9
ISSN Online: 2319 – 9253
Print: 2319 – 9245

Improvements in Firewall Policy Rules to Identifying and Resolving Anomalies

D. KumaraSwamy[1] T.Narender[2]

1. [M.Tech(cs)], Dept. of CSE, Vivekananda Institute of Technology & Science
2. Asst.Professor, Dept. of CSE, Vivekananda Institute of Technology & Science

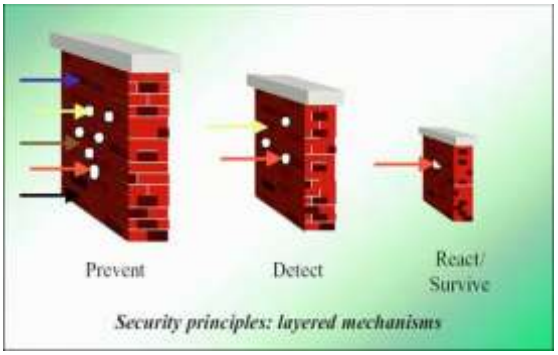
ABSTRACT

Firewalls are the most common component to provide security to the systems in local and global environment. Firewall implements the policy to protect the resources but it does not have the systematic analysis mechanisms and tools. We propose complete set of definitions of relations between rules and possible anomalies. A set of algorithms to simultaneously detect and resolve anomalies in a given rule set. An algorithm to merge the rules whenever possible to reduce the number of rules.

Keywords: *firewall, anomalies, policy rules, Correlation of Packet Space Segment , Rule Reordering*

INTRODUCTION

Firewall is a System acting as an interface of a network to one or more external networks. Implements the security policy of the network By deciding which packets to let through Based on rules defined by the network administrator.



Firewall Rules

- Mostly Custom-designed and Hand-written.
- Must be defined and maintained carefully.

Result of any slight mistake in defining the rules:

Allow unwanted traffic to be able to enter or leave the network, Deny passage to quite legitimate traffic.

Manual Definition and Maintenance

Complex, Error-prone, Costly, Inefficient, As number of rules increase, Becomes virtually unmanageable.

Automating the maintenance of Firewall Rule Set

- Making the rule set error-free
- Detecting the conflicts and anomalies in the rules
- Resolving the errors found
- Increasing the efficiency
- Reducing the number of rules in the set.

EXISTING WORK

Firewall policy management is a challenging task due to the complexity and interdependency of policy rules. This is further exacerbated by the continuous evolution of network and system environments.

The process of configuring a firewall is tedious and error prone. Therefore, effective mechanisms and tools for policy management are crucial to the success of firewalls.

Existing policy analysis tools, such as Firewall Policy Advisor and FIREMAN, with the goal of detecting policy anomalies have been introduced. 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. For each firewall rule, FIREMAN only examines all 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 one rule and its preceding rules, but cannot accurately indicate all rules involved in an anomaly.

DISADVANTAGES

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. For each firewall rule, FIREMAN only examines all preceding rules but ignores all subsequent rules when performing anomaly analysis.

ARCHITECTURE

AIM

To provide an innovative policy anomaly management framework for firewalls, adopting a rule-based segmentation technique

to identify policy anomalies and derive effective anomaly resolutions.

Anomaly Management

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.

PROPOSED MODELS/WORK

In this paper, 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 (either conflicting or redundant) 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.

ADVANTAGES

In our framework conflict detection and resolution, conflicting segments are identified in the first step. Each conflicting segment associates with a policy conflict and a set of conflicting rules. Also, the correlation relationships among conflicting segments are identified and conflict correlation groups are derived. Policy conflicts belonging to different conflict correlation groups can be resolved separately, thus the searching space for resolving conflicts is reduced by the correlation process.

- A rule contains

Set of criteria

- Direction, Protocol, Source IP, Source Port, Destination IP, Destination Port.
  - Action performed on a packet matching the criteria

ACCEPT or REJECT.

- We present the following algorithms to resolve the anomalies

RESOLVE-ANOMALIES

Processes the *old_rules_list* to produce the anomaly-free *new_rules_list*.

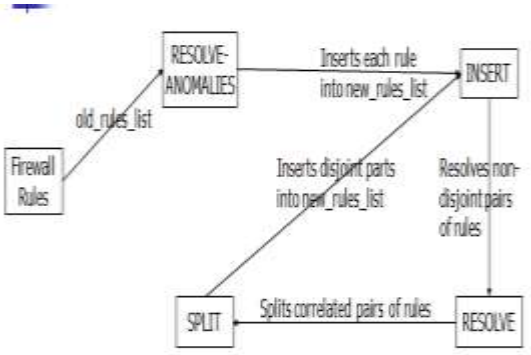
INSERT

Inserts a rule into the *new_rules_list* in such a way that the list remains anomaly free.

RESOLVE

Detects and resolves anomalies between two given non-disjoint rules.

SPLIT Splits two non-disjoint rules into disjoint parts for a given attribute.



Approaches

- Correlation of Packet Space Segment
- Action Constraint Generation
- Rule Reordering
- Data Package

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.

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

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.

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.

Conclusion

We have proposed a novel anomaly management framework that facilitates systematic detection and resolution of firewall policy anomalies. The approaches Correlation of Packet Space Segment, Action Constraint Generation, Rule Reordering effectively resolve the anomalies. We would like to extend our anomaly analysis approach to handle distributed firewalls.

REFERENCES

[1] Hongxin 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.

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

[3] J. Alfaro, N. Boulahia-Cuppens, and F. Cuppens, "Complete analysis of configuration rules to guarantee reliable network security policies," International Journal of 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. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING 14

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

[6] E. Lupu and M. Sloman, "Conflicts in policy-based distributed systems management," IEEE Transactions on Software Engineering, vol. 25, no. 6, pp. 852–869, 1999.

[7] Herman, G. Melanc¸on, and M. Marshall, "Graph visualization and navigation in information visualization: A survey," IEEE Transactions on Visualization and Computer Graphics, pp. 24–43, 2000.

[8] H. Hu, G. Ahn, and K. Kulkarni, "Anomaly discovery and resolution in web access control policies," in Proceedings of the 16th ACM symposium on Access control models and technologies. ACM, 2011, pp. 165–174.

[9] L. Yuan, C. Chuah, and P. Mohapatra, "ProgME: towards programmable network measurement," ACM SIGCOMM Computer Communication Review, vol. 37, no. 4, p. 108, 2007.

[10] El-Atawy, K. Ibrahim, H. Hamed, and E. Al-Shaer, "Policy segmentation for intelligent firewall testing," in 1st Workshop on Secure Network Protocols (NPSec 2005), 2005.

[11] G. Misherghi, L. Yuan, Z. Su, C.-N. Chuah, and H. Chen, "A general framework for benchmarking firewall optimization techniques," IEEE Transactions on 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," in Proceedings of the 4th ACM workshop on Quality of protection. ACM, 2008.

[13] M. Sahinoglu, "Security meter: A practical decision-tree model to quantify risk," IEEE security & privacy, pp. 18–24, 2005.

[14] R. Sawilla and X. Ou, "Identifying Critical Attack Assets in Dependency Attack Gaphs," in 13th European Symposium on Research in Computer Security (ESORICS). Springer, 2008.

[15] P. Mell, K. Scarfone, and S. Romanosky, "A complete guide to the common vulnerability scoring system version 2.0," in Published by FIRST-Forum of Incident Response and Security Teams, June, 2007.

[16] Fundulaki and M. Marx, "Specifying access control policies for XML documents with XPath," in Proceedings of the ninth ACM symposium on Access control models and technologies. ACM, 2004,pp. 61–69.

[17] S. Jajodia, P. Samarati, and V. S. Subrahmanian, "A logical language for expressing authorizations," in IEEE Symposium on Security and Privacy, Oakland, CA, May 1997, pp. 31–42.

[18] T. Moses, "eXtensible Access Control Markup Language (XACML), version 2.0, Oasis Standard," Internet http://docs. oasis-open. org/xacml/2.0/access control-xacml-2.0-core-spec-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," in Proceedings of the 14th ACM symposium on Access control modelsand technologies. ACM, 2009, pp. 135–144.

[20] Jin, G. Ahn, H. Hu, M. Covington, and X. Zhang, "Patient-centric authorization framework for sharing electronic health records," in Proceedings of the 14th ACM symposium on Access control models and technologies. ACM, 2009, pp. 125–134.