THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Detection and Resolution of Firewall Policy Anomalies

Renuka Nagpure
Professor, Information Technology Department
Atharva College of Engineering, Mumbai, Maharashtra, India
Pranali Jaypraksh Dhuri
B.E. Information Technology Department
Atharva College of Engineering, Mumbai, Maharashtra, India
Jagruti Kailas Patil
B.E. Information Technology Department
Atharva College of Engineering, Mumbai, Maharashtra, India
Mansi Prabhakar Kini
B.E. Information Technology Department
Atharva College of Engineering, Mumbai, Maharashtra, India
Aarti Jaywant Patil
B.E. Information Technology Department
Atharva College of Engineering, Mumbai, Maharashtra, India

Abstract: *Firewalls are the most widely deployed security mechanism to ensure the security of private networks in most businesses and institutions. The efficiency of security protection provided by a firewall mainly depends on the quality of policy configured in the firewall. Unfortunately, planning 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, approving a rule-based segmentation technique to identify policy anomalies and derive effective anomaly resolutions.*

Keywords: *Firewall, anomalies, security policy*

1. Introduction

A firewall examines all incoming and outgoing packets based on security rules. 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.

2. Literature Survey

Today near about 80-90 % users are interacting with online networking system. E.g. Public network verses private network. In that huge amount of fraud users are rapidly increases and they share malicious information over the network or in the corresponding system. So it is difficult to know which users are real and which users are frauds among made users list. Hence large number of users list is made and it's tedious task to maintain and isolating the users list and it's time consuming process. To maintaining the huge amount of web traffic over the network are available in Firewall Policy Technique.

Overall survey of the papers concludes that they are uses local Virtual Private Network or Fireman technology for handling incoming and outgoing data in network traffic. But it requires huge time and it only detects the anomalies not resolving it. It can be handled by using Firewall policy analysis which uses Rule Reordering as well as shadowing and correlation to generate new rule.

2.1. Figures

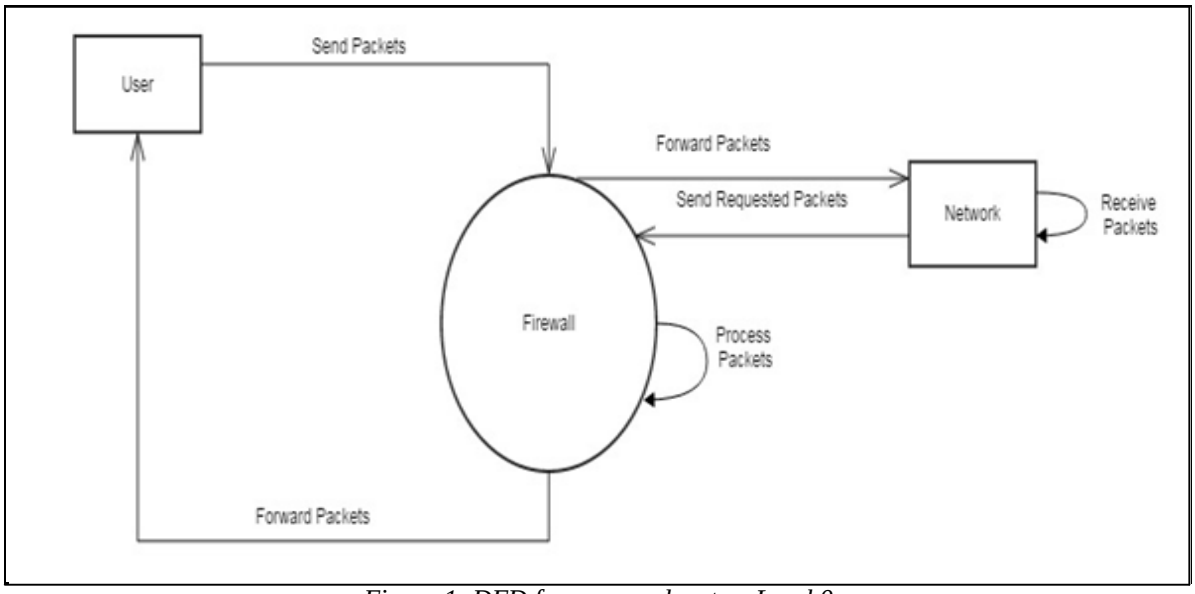

Figure 1: DFD for proposed system Level 0

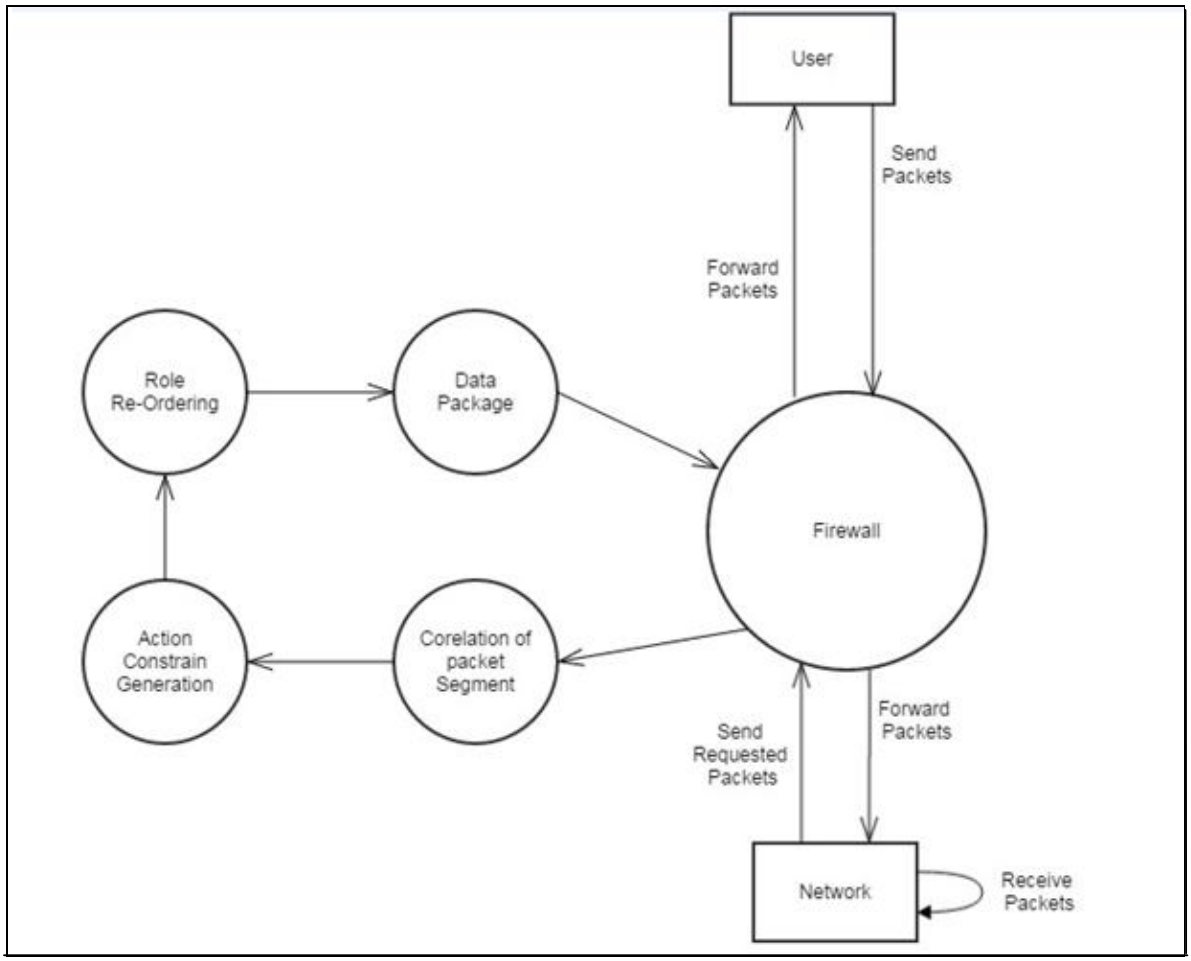

Figure 2: DFD for proposed system Level 1

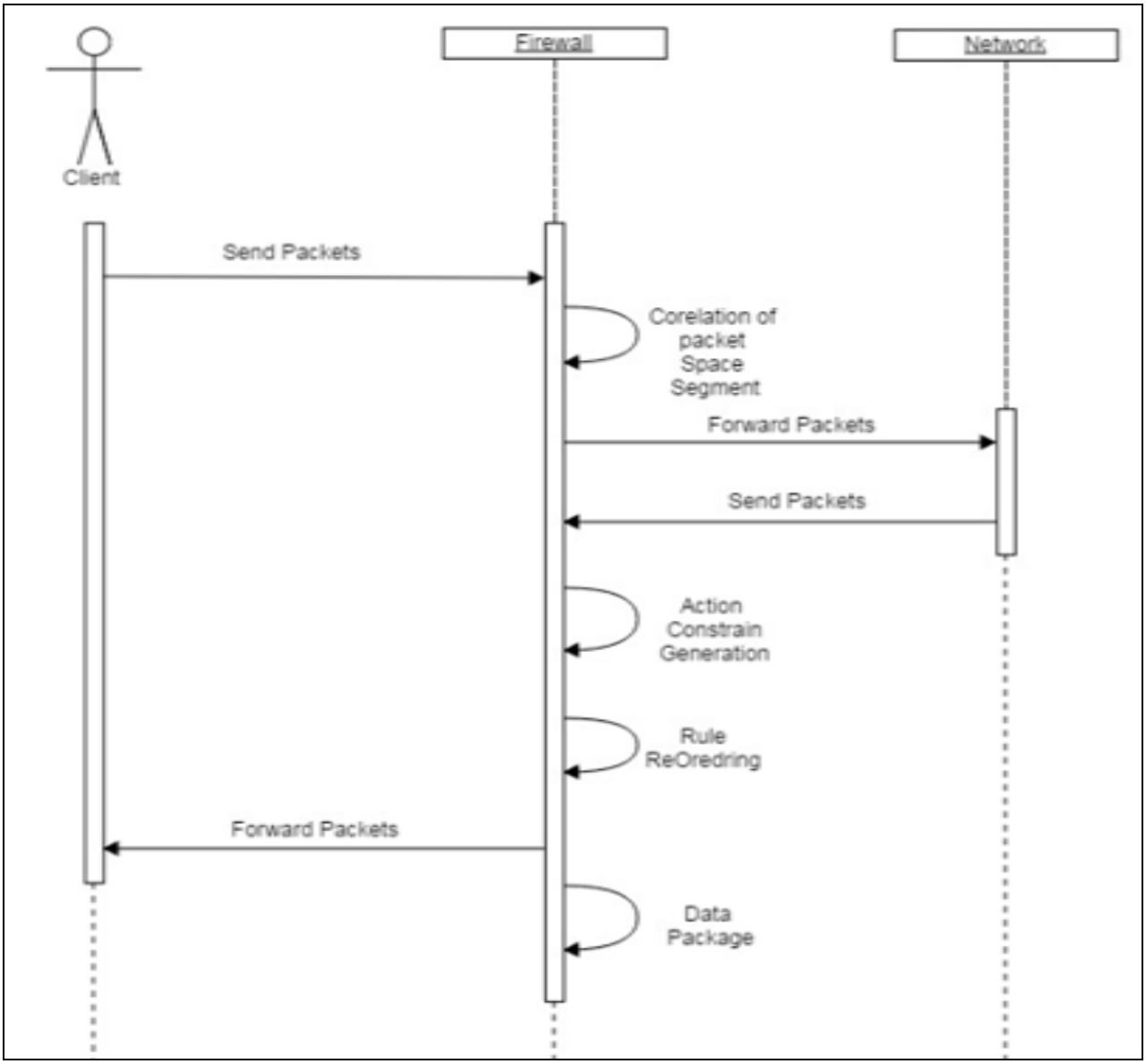

Figure 3: Sequence diagram for proposed method

2.2. Modules

2.2.1. 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 individually, because all correlation groups are independent of each other. Particularly, the searching space for reordering conflicting rules in conflict resolution can be significantly lessened and the efficiency of resolving conflicts can be greatly improved.

2.2.2. Action Constraint Generation

In a firewall policy are discovered and conflict correlation groups are recognized, the risk assessment for conflicts is accomplished. The risk levels of conflicts are in turn utilized for both automated and manual strategy selections. A basic idea of automated policy 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 section. If the risk level is very high, the estimated action should deny packets considering the protection of network perimeters

2.2.3. Rule Reordering

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

2.2.4. Data Package

When conflicts in a procedure 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.

2.3. Other Recommendations

The system we proposed are better than the traditional system as it detects anomalies among multiple rules by analyzing the relationships between one rule and the collections of packet spaces derived from all preceding rules. 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

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.

In future system will be used for hacking prevention and it can be used as an Antivirus on individual machine.

3. Discussion & 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.

Detection of Fraud/Sybil user's activities in a network which is control by Firewall Rule Engine determines the correlated group. Huge amount of web logs are easily managed and identifies real users and fraud users. Granting permission by performing operation (Allow/Deny) and calculating Threshold value. Malicious information is added in a block state. It provides finally secure access to or from the private and public network.

4. References

1. Hongxin Hu, Student Member, IEEE,Gail-JoonAhn, Senior Member, IEEE,andKetanKulkarni," Detecting and Resolving Firewall Policy Anomalies",IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO.3, MAY/JUNE 2012.
2. Rakesh R. Surve et al Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 3(Version 1), March 2014, pp.696-701
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 SECURECOMPUTING 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, 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 inweb 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, p108, 2007.
10. El-Atawy, K. Ibrahim, H. Hamed, and E. Al-Shaer, "Policy segmentation for intelligent firewall testing," in 1stWorkshop on Secure Network Protocols (NPSec 2005), 2005.