Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.134 – 137

RESEARCH ARTICLE

Detecting and Resolving Firewall Policy Anomalies Using Rule-Based Segmentation

Anbarasan.A[1], Balasubramani.G[2], Madhan.C[3], Naveenkumar.P[4], Mrs. N.S.Nithya[5]
[1,2,3,4] Department Of Computer Science and Engineering, Anna University Chennai, India
[5]Assistant Professor, Department Of Computer Science and Engineering,
K.S.R. College Of Engineering, Tiruchengode, India

[1] anburocks.009@gmail.com; [2] srdbala@gmail.com; [3] madhanvc8@gmail.com;
[4] nvnsft@gmail.com; [5] sachinnithya@yahoo.com

Abstract— In this paper we present an 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. 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. .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.

Key Terms: - Segmentation; Correlation; Packet space; conflict; Distributed

I. INTRODUCTION

Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures. While firewalls are often discussed in the context of Internet connectivity, they may also have applicability in other network environments. At one time, most firewalls were deployed at network perimeters. This provided some measure of protection for internal hosts, but it could not recognize all instances and forms of attack, 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 security, as well as to protect mobile devices that are placed directly onto external networks

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 defence for secure networks against 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 defined based on predefined security policy requirements. 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 guarantee correct security policy semantics. As the number of filtering rules increases, the difficulty of writing a new rule or modifying an existing one also increases. It is very likely; in this case, to introduce conflicting rules such as

rules having the same filtering part but different actions, one general rule shadowing another specific related rule or correlated rules whose relative ordering determines different actions for the same packets.

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. Firewall policy management is a challenging task due to the complexity and interdependency of policy rules. 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. Due to the complex nature of policy anomalies, system administrators are often faced with a more challenging problem in resolving anomalies and also in resolving policy conflicts.

II. STRUCTURE AND TECHNIQUE

Our policy anomaly management framework is composed of two core functionalities. One is conflict detection and resolution, and the other is redundancy discovery and removal. Both functionalities are based on the rule-based segmentation technique.

For 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 (CG) are derived.

Policy conflicts belonging to different conflict correlation groups can be resolved, thus the searching space for resolving conflicts is reduced by the correlation process. The second step generates an action constraint for each conflicting segment by examining the characteristics of each conflicting segment. A strategy-based method is introduced for generating action

A. Packet Space Segmentation and Classification

As we stated earlier that 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 technique, 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.

This technique has been recently introduced to deal with several research problems such as network traffic measurement, firewall testing and optimization. Inspired by those successful applications, we leverage this technique for the purpose of firewall policy anomaly analysis.

Algorithm 1 shows the pseudocode of generating packet space segments for a set of firewall rules R adding a network packet space s derived from this algorithm works by a rule r to a packet space set S. A pair of packet spaces must satisfy one of the following relations: subset (line 5), superset (line 10), partial match (line 13), or disjoint (line 17). Therefore, one can utilize set operations to separate the overlapped spaces into disjoint spaces.

Algorithm 1: Segment Generation for Network Packet Space of a Set of Rule R: Partition(R)

```
   Input: A set of rules, R.
   Output: A set of packet space segments, S.
1  foreach r ∈ R do
2      s_r ⟵ PacketSpace(r);
3      foreach s ∈ S do
4          /* s_r is a subset of s*/
5          if s_r ⊂ s then
6              S.Append(s \ s_r);
7              s ⟵ s_r;
8              Break;
9          /* s_r is a superset of s*/
10         else if s_r ⊃ s then
11             s_r ⟵ s_r \ s;
12         /* s_r partially matches s*/
13         else if s_r ∩ s ≠ ∅ then
14             S.Append(s \ s_r);
15             s ⟵ s_r ∩ s;
16             s_r ⟵ s_r \ s;
17     S.Append(s_r);
18 return S;
```


B. Grid Representation of Policy Anomaly

To enable an effective anomaly resolution, complete and accurate anomaly diagnosis information should be represented in an intuitive way. When a set of rules interacts, one overlapping relation may be associated with several rules. Meanwhile, one rule may overlap with multiple other rules and can be involved in a couple of overlapping relations (overlapping segments).

Different kinds of segments and associated rules can be viewed in the uniform representation of anomalies. However, it is still difficult for an administrator to figure out how many segments one rule is involved in. To address the need of a more precise anomaly representation, we additionally introduce a grid representation that is a matrix-based visualization of policy anomalies, in which space segments are displayed along the horizontal constraints.

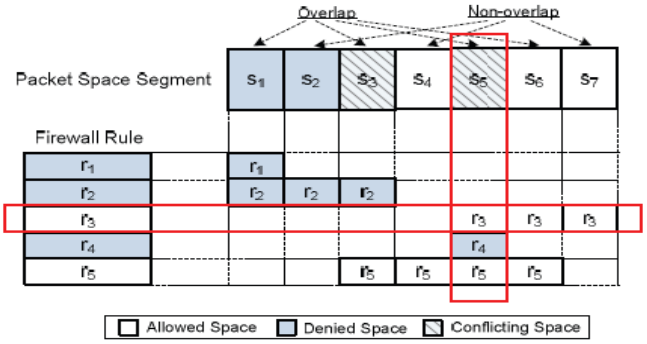

Figure I an illustration for Grid Representation of policy Anomaly

C. Correlation of Packet Space Segment

Technically, one rule may get involved in multiple policy anomalies. In this case, resolving one anomaly in an isolated manner may cause the unexpected impact on other anomalies. Similarly, we cannot resolve a conflict individually by only reordering conflicting rules associated with one conflict without considering possible impacts on other conflicts.

On the other hand, it is also inefficient to deal with all conflicts together by reordering all conflicting rules simultaneously. Therefore, it is necessary to identify the dependency relationships among packet space segments for efficiently resolving policy anomalies.

D. Conflict Resolution

Each conflicting segment indicates a policy conflict as well as a set of conflicting rules involved in the conflict. Once conflicts are identified with 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.

Our conflict resolution mechanism introduces that an action constraint is assigned to each conflicting segment. An action constraint for a 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 a conflict, we only assure that the action taken for each packet within the conflicting segment can satisfy the corresponding action constraint.

E. Redundancy Elimination

In this step, every rule subspace covered by a policy segment is assigned with a removable property. . Removable property is used to indicate that a rule subspace is removable. In other words, removing such a rule subspace does not make any impact on the original packet space of an associated policy.

Strong irremovable property means 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. That means a rule subspace becomes irremovable due to the reason that other portions of this rule cannot be removed.

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. We next introduce three processes to perform the property assignments to all of rule subspaces within the segments of a firewall policy, considering different categories of policy segments.

1. Property assignment for the rule subspace covered by a nonoverlapping segment. A nonoverlapping segment contains only one rule subspace. Thus, this rule subspace is assigned with strong irremovable property. Other rule subspaces associated with the same rule are assigned with weak irremovable property, except for the rule subspaces that already have strong irremovable property.

2. Property assignment for rule subspaces covered by a conflicting segment. The first rule subspace covered by the conflicting segment is assigned with strong irremovable property. Other rule subspaces in the same segment are assigned with removable property. Meanwhile, other rule subspaces associated with the first rule are assigned with weak irremovable property except for the rule subspaces with strong irremovable property.

3. Property assignment for rule subspaces covered by a nonconflicting overlapping segment. If any rule subspace has been assigned with weak irremovable property, other rule subspaces without any irremovable property are assigned with removable property. Otherwise, all subspaces within the segment are assigned with correlated property.

III. CONCLUSIONS

With rule based segmentation and grid based technique we made a novel static analysis approach to check firewall configurations. First, we have proposed a framework for modelling individual and distributed firewalls that can automatically correct all or part of the misclassified packets of a faulty firewall policy. Second, we have designed a static method to discover various misconfigurations such as policy violations, inconsistencies and inefficiencies.

In Future we would like to improve the performance of the firewall conflict detection and auto healing of conflicts technique. We would like to implement this in a cloud based schemes so that it can be used to overcome these issues and that are present in the existing systems so as to increase security.

REFERENCES

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

[2] 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.

[3] 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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] A. Hari, S. Suri, and G. Parulkar, "Detecting and Resolving Packet Filter Conflicts," Proc. IEEE INFOCOM, pp. 1203-1212, 2000.

[9] Z. Fu, S. Wu, H. Huang, K. Loh, F. Gong, I. Baldine, and C. Xu, "IPSec/VPN Security Policy: Correctness, Conflict Detection and Resolution," Proc. Int'l Workshop Policies for Distributed Systems and Networks (POLICY '01), pp. 39-56, 2001.

[10] R. Reeder, L. Bauer, L. Cranor, M. Reiter, K. Bacon, K. How, and H. Strong, "Expandable Grids for Visualizing and Authoring Computer Security Policies," Proc. 26th Ann. SIGCHI Conf. Human Factors in Computing Systems, pp. 1473-1482, 2008.

