Abstract: Firewalls playing very important role to provide security to private networks and organizations. But the firewall policies cannot be communal across domains because it contains confidential information and security holes also, which leads to various attacks by attacker. In this project, we propose the cross-domain privacy-preserving cooperative firewall policy optimization protocol and a rule-based segmentation technique. Specifically, for any two adjacent firewalls belonging to different administrative domains, our protocol can identify in each firewall the rules that can be removed because of the other firewall. The optimization process involves cooperative computation between the two firewalls without any party disclosing its policy to the other but firewall mainly depends on the quality of policy configured in the firewall. Designing and managing firewall policies are often difficult due to the complex nature of firewall configurations as well as the lack of systematic analysis mechanisms and tools. A rule-based segmentation technique to identify policy anomalies and provide effective anomaly resolutions.

1. 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. 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. For instance, Al-Shaer and Hamed 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. 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. Recently, policy anomaly detection has received a great deal of attention. Corresponding 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 pairwise 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. On the other hand, due to the complex nature of policy anomalies, system administrators are often faced with a more challenging problem in resolving anomalies, in particular, resolving policy conflicts. An intuitive means for a system administrator to resolve policy conflicts is to remove all conflicts by modifying the conflicting rules. However, changing the conflicting rules is significantly difficult, even impossible, in practice from many aspects. 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. Thus, without a priori knowledge on the administrators’ intentions, changing rules will affect the rules’ semantics and may not resolve conflicts correctly. Furthermore, in some cases, a system administrator may intentionally introduce certain overlaps in firewall rules knowing that only the first rule is important. In reality, this is a commonly used technique to exclude specific parts from a certain action, and the proper use of this technique could result in a fewer number of compact rules. In this case, conflicts are not an error, but intended, which would not be necessary to be changed. 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. In this paper, we present 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. 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. Moreover, the outputs of prior policy analysis tools are mainly a list of possible anomalies, which does not give system administrators a clear view of the origination of policy anomalies. Since information visualization technique enables users to explore, analyze, reason, and explain abstract information by taking advantage of their visual cognition, our policy analysis tool adopts an information visualization technique to facilitate policy analysis. A grid based visualization approach is introduced to represent policy anomaly diagnosis information in an intuitive way, enabling an efficient anomaly management. In addition, we implement a visualization-based firewall anomaly management environment (FAME) based on our approach. To evaluate the practicality of our tool, our extensive experiments deal with a set of real-life firewall policies.

2. Related Work

Prior work on intrafirewall redundancy removal aims to detect redundant rules within a single firewall. Gupta identified backward and forward redundant rules in a firewall. Later, Liu et al. pointed out that the redundant rules identified by Gupta are incomplete and proposed two methods for detecting all redundant rules. Prior work on interfirewall redundancy removal requires the knowledge of two firewall policies and therefore is only applicable within one administrative domain. First, their purposes are different. The former focuses on enforcing a firewall policy over VPN tunnels in a privacy preserving manner, whereas the latter focuses on removing interfirewall redundant rules without disclosing their policies to each other. Second, their requirements are different. The former preserves the privacy of the remote network’s policy, whereas the latter preserves the privacy of both policies. For two adjacent firewalls, we assume that they are semi-honest, i.e., each firewall follows our protocol correctly, but each firewall may try to reveal the policy of the other firewall. The semi-honest model is realistic and well adopted. In threat model, the inputs to the protocol are honest, and crafting inputs to reveal the firewall policies is beyond our threat model. We leave investigation of privacy-preserving firewall optimization in the model with malicious participants to future work.

Literature Survey

Firewalls are core elements in network security. However, managing firewall 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 in any firewall requires thorough intra- and inter-firewall analysis to determine the proper rule placement and ordering in the firewalls. 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 the management of filtering rules and maintains the security of next-generation firewalls.

The first quantitative evaluation of the quality of corporate firewall configurations appeared in 2004, based on Check Point Firewall-1 rule sets. In general, that survey indicated that corporate firewalls often enforced poorly written rule sets. This article revisits the first survey. In addition to being larger, the current study includes configurations
from two major vendors. It also introduces a firewall complexity. 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.

The use of different network security components, 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. Nevertheless, 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.

3. Existing System

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

- Lack of systematic analysis, mechanisms and tools.
- Existing technique like FIREMAN having limitations.

4. Proposed System

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.

Advantage

- Providing resolution for anomaly policy.
- It examines all preceding rules as well as all subsequent rules.

ALGORITHM:

Policy Anomaly Discovery

Input: A set \( P \) of rules \( r_1, r_2, \ldots, r_n \)
Output: A set \( P \) of ordered rules, and \( P \) of correlated rules

1. Order rules according to their dependencies →
2. Construct graphs \( U \) and \( D \).
3. While \( D \) contains terminal nodes →
4. For every terminal node \( (i, j) \) \( \in D \)
5. Do color \( v \) red;
6. Do color link \( (i, j) \) \( \in U \) red;
7. \( C \leftarrow \) discover connected components(\( U \));
8. If \( C \) doesn’t contain new components, return “Rules conflict” → \( P \);
9. While \( C \neq \emptyset \)
10. Select node \( u \) randomly from \( C \);
11. Set \( P \leftarrow P \cup \{r_u\} \);
12. Return \( P \);
5. Modules

MODULES DESCRIPTION:

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.

7. Conclusion

In this paper, we identified an important problem, cross-domain privacy-preserving inter firewall redundancy detection. We propose a novel privacy-preserving protocol for detecting such redundancy. We implemented our protocol in Java and conducted extensive evaluation. The results on real firewall policies show that our protocol can remove as many as 49% of the rules in a firewall whereas the average is 19.4%.

Our protocol is applicable for identifying the interfirwall redundancy of firewalls with a few thousands of rules, e.g. 2000 rules. However, it is still expensive to compare two firewalls with many thousands of rules, e.g. 5000 rules. Reducing the complexity of our protocol needs to be further studied. In our work, we have demonstrated rule optimization, from FW1 to FW2 and we note that a similar rule optimization is possible in the opposite direction, i.e., FW2 to FW1. In the first scenario, FW1 to FW2 it is FW1 that is improving the performance load of FW2, and in return FW2 is improving the performance of FW1 in a vice-versa manner. All this is being achieved the without FW1 or FW2 revealing each other’s policies thus allowing for a proper administrative separation.

8. FUTURE WORK:

Our protocol is most beneficial if both parties are willing to benefit from it and can collaborate in a mutual manner. There are many special cases that could be explored based on our current protocol. For example, there may be hosts or Network Address Translation (NAT) devices between two adjacent firewalls. Our current protocol cannot be directly applied to such cases. Extending our protocol to these cases could be an interesting topic and requires further investigation.

References


Mrs. Jyothirmayi is a student of Sri Aditya College of Engineering, Surampalem. Presently she is pursuing her M.Tech [Computer Science and Engineering] from this college and she received her B.Tech from ASR college of Engineering, affiliated to JNT University, Hyderabad. Her area of interest includes Computer Networks and Object oriented Programming languages, all current trends and techniques in Computer Science.

Mrs Sadineni Neelima an excellent teacher received her M.Tech (CSE) from Gokula college of Engineering and is working as Associate Professor, Department of CSE at Sri Aditya college Of Engineering .She has 8 years of teaching experience in various engineering colleges. Her area of Interest includes Data Warehouse and Data Mining.