Challenges in Managing Firewalls

Artem Voronkov(✉), Stefan Lindskog, and Leonardo A. Martucci

Karlstad University, Karlstad, Sweden
{artem.voronkov,stefan.lindskog,leonardo.martucci}@kau.se

Abstract. Firewalls are essential security devices that can provide protection against network attacks. To be effective, a firewall must be properly configured to ensure consistency with the security policy. However, configuring is a complex and error-prone process. This work tries to identify the reasons behind firewall misconfigurations. To achieve our goal, we conducted a series of semi-structured interviews with system administrators that manage access control lists in networks of different sizes. The paper discusses our interview results and describes future work.

1 Introduction

Network security is essential for all types of organizations. Making sure that the network's perimeter is properly defended is an important measure to prevent leakage of sensitive information. One common solution to mitigate attacks is a firewall. The main function of firewalls is to inspect the network traffic and prevent unauthorized access from outside the organization's secure domain. However, configuring a firewall has proven to be an error-prone task [4,5].

Firewall filtering actions, such as accepting or rejecting packets, are performed according to a set of static configuration rules that use only information contained in the packet, such as source and destination network addresses, port and protocol. The constant growth of networks forces firewall rule sets to expand over time. These rule sets can be tangled, and this complicates their readability and finding the right place for a new rule in case of policy expansion.

This paper investigates the complexity of the process of configuring firewalls. We address the question: what are the main difficulties network security specialists deal with? The answer to this question will significantly help in further research on firewall usability.

The remainder of the paper discusses related work in Sect. 2. The methodology used and an outline of the conducted interviews are given in Sect. 3. In Sect. 4 we describe the data obtained from our semi-structured interviews and discuss the outcome. Concluding remarks are given in Sect. 5.

The work was partially funded by the High Quality Networked Services in a Mobile World (HITS), a research project of the Knowledge Foundation of Sweden.

The authors would like to thank Zeeshan Afzal for his time and input to this work.

S. Buchegger and M. Dam (Eds.): NordSec 2015, LNCS 9417, pp. 191–196, 2015.
DOI: 10.1007/978-3-319-26502-5_13

2 Related Work

Over the past few year, several studies have focused on a firewall configuring process and some other related topics. Wool [4,5] gives an overview of the most common firewall misconfigurations among system administrators and, according to him, most misconfigurations belong to inbound traffic. This is the worst case scenario, because filtering incoming traffic is the main function of firewalls. For that reason, research on firewall misconfiguration detection, such as [2], have been conducted. There are no studies however on understanding the reasons for misconfigurations.

Access Control Policy Management was studied by Bauer et al. [1]. Access control professionals were divided into two groups: policy makers and policy implementers. Policy makers design access control rule sets and policy implementers are responsible for realizing them. By conducting semi-structured interviews, Bauer et al. identified three factors that lead to unmanageable access control rule sets: (1) policies are made by several people, (2) policy makers and policy implementers are different people, and (3) current access control systems can not always implement the desired policy. In contrast to the work of Bauer et al., we focus on firewall misconfigurations and understanding the reasons behind them.

3 Methodology and Interview Details

To identify problems in configuring firewalls, real data must be obtained directly from system administrators, since the literature does not provide an answer to our research question. We considered two possible alternatives: a quantitative method (questionnaire) and a qualitative method (interviews). An advantage of a questionnaire is mainly the low cost of data collection and processing. However, using semi-structured interviews, we get much more information and do not need so many respondents. Since it was not easy to recruit system administrators for the user study, we decided to use semi-structured interviews as a main approach for obtaining the data. Interviews allow us to focus on primary questions and gives the opportunity for multiple comments about the problem from the respondents. Nevertheless, a questionnaire was designed to identify the main difficulties specialists in network security deal with on a daily basis. The questionnaire will be used as a subsidiary method to include people who lack the time to take part in our ordinary interviews.

3.1 Semi-structured Interviews

We designed our questions not only to explore our topics of interest but also to encourage the respondents to elaborate on specific problems they encounter. While conducting the interviews, we followed the best practices and recommendations found in the literature [3]. The interviews were audio recorded and later used to produce the transcripts for data analysis. The interviews focus on the following topics:

– Overview of the respondent's experience of working with firewalls.
– Efforts to maintain firewalls.
– Solutions used to provide protection to the network.
– Difficulties they face in the process of configuring/maintaining firewalls.
– Interaction within the groups of system administrators.
– Security incidents that have happened in the organization.
– Formal and informal procedures for simplifying the management of rule sets.

3.2 Respondents

Six system administrators (all males) from different organizations who are responsible for networks of different sizes were recruited. They voluntarily agreed to take part in our research. The interviews lasted 40 minutes approximately. It is worth noting that all the respondents are independent from our research group and no financial compensation was offered. All the answers in the interview are anonymous and the respondents are identified by numbers #{1–6}. Table 1 shows participants, their experience of working with firewalls, network size that they manage, effort for support and type of organization they work in.

It should be mentioned that this is a pilot study. To validate our initial results, additional interviews will be conducted with respondents from different organizations including people that also are involved in education on firewall configurations.

Table 1. List of respondents

Respondent	Experience	Network size	Effort	Organization
#1	12 years	≈50 nodes	1 hour/week	Institute
#2	8 years	≈400 nodes	2 hours/week	Institute
#3	19 years	≈850 nodes	0.5 hour/week	University
#4	17 years	≈450 nodes	9 hours/week	Enterprise
#5	3 years	≈70 nodes	1 hour/week	University
#6	20 years	≈500 nodes	0.5 hour/week	University

The responsibilities of all system administrators interviewed are almost identical: they administrate security devices, such as firewalls and intrusion detection systems, and quite often also switches and routers. All have extensive experience of managing firewalls and have created configuration files on their own. The "Effort" column in Table 1 represents the average amount of time spent by these professionals on maintaining firewalls. All the specialists had implemented firewall policies that have been used for a long time. That is the reason why they are nearly static and their maintenance does not require much effort. Another reason why the numbers in this column are low is that five of six system administrators from the list have colleagues they cooperate with. The only exception is respondent #4, who works alone and thus spends a considerable amount of time on managing firewalls.

We conducted interviews with people from three different types of organizations, e.g., universities, international research institutes and enterprises. The size of the organizations varies from 16,000–18,000 faculty, staff and students for universities, 2,500–3,000 staff members for institutes and more than 100 employees in the enterprise.

4 Results and Discussion

This section reports our findings and discusses the results.

4.1 Results of the Semi-structured Interviews

1. **Having more people responsible for security measures is not always beneficial.** Five respondents mentioned that some difficulties occur when there is more than one person responsible for firewalls. It is then necessary to have well adjusted mechanisms of interaction, such as frequent personal communication and good documentation. Nevertheless, almost all our respondents use either the first or the second mechanism of interaction, but not both at the same time. Another issue is that the availability of several system administrators generates the problem of distribution of roles. It does not work properly for four respondents and they have been confronted, at least once, with this issue.
2. **A variety of approaches is used to simplify the process of maintaining firewalls.** All the respondents use different ways to spend less resources on maintenance of security measures. However, the approaches are not equally distributed among the respondents, see Table 2.

Table 2. List of approaches used by respondents

Respondent	Documentation	Comments in configuration files	Firewall management/ testing tools	Revision history	Frequent personal communication
#1	Yes	Yes	No	No	No
#2	Yes	Yes	Yes	No	No
#3	Yes	Yes	No	No	Yes
#4	No	Yes	Yes	Yes	Not applicable
#5	No	Yes	No	No	Yes
#6	No	Yes	No	No	Yes

"Frequent personal communication" means the interaction in one group of system administrators. By "Documentation" we refer to electronically or hand-written security policies and more detailed instructions and procedures

for how to handle a particular system. It is worth noting that system administrators that do not yet have a documentation of the configurations and practices mentioned that they will start working on this.
Another issue that needs clarification is why many of our respondents do not use "Firewall management/testing tools" and "Revision history" approaches. For the first approach, most of respondents mentioned that it is too expensive to use it. For instance, respondent #6 answered: "Too expensive, but, to be honest, we do not know the costs of configuration mistakes". For the second approach, two respondents answered that they use configuration management systems, i.e., Ansible[1] and Puppet[2], and they do not need to manually write a "Revision history" separately for firewall configuration files, since such systems have a built-in version control of files. Another respondent answered: "All changes are written in a simple text file, newest on top".

3. **Firewall misconfigurations are still common.** All the respondents have experienced mistakes in firewall configuration files and different types of misconfigurations continue to occur despite the presence of a large number of auxiliary mechanisms. Too strict/permissive, redundant rules and unauthorized access to some nodes were a few reasons given by the respondents. The most common case is too strict rules. However, these misconfigurations usually do not have severe consequences and it does not require much time to figure them out. Since system administrators serve people, they will immediately start receiving complaints from users when this type of misconfiguration occurs. This implies that they will have an opportunity to make changes to the configuration file without prolonged delay. Too permissive rules is far worse in terms of discovery time. Two of our respondents stated that they have dealt with this error and found it out either during a scheduled manual check or from colleagues who discovered it by chance. The main reason for firewall misconfigurations is the human factor. Five respondents encountered the problems when they tried to multitask while configuring firewalls at the same time.
4. **Policy creators and implementers are the same people.** According to our results, among all our respondents there is no one who is responsible for creating security policies. The responsibility for the policy lies solely on the system administrators.
5. **It is easy to configure a firewall.** Only two of six of our respondents answered that it is difficult to configure firewalls. Both of them agreed that the most complicated part is "reading firewall rules" in order to find a suitable position for a new rule to be placed. Four respondents argued that they had no difficulties configuring firewalls. Respondents #3 and #4 stated: "I have been doing it for almost twenty years. For me it is quite straightforward" and "Once you get used to it, you can do pretty much everything", respectively. Respondent #5 answered: "It is not really difficult for use cases we have. We do not do anything fancy and do not use any advanced features".

[1] http://www.ansible.com
[2] http://www.puppetlabs.com

4.2 Discussion

The first and third findings reported above correspond to the findings from [1] and [5], respectively. The first finding showed that it is not a good idea to have several people responsible for firewalls. In our pilot study we also had a case with only one professional being responsible for the network. Respondent #4 mentioned that the knowledge of all procedures and configurations is inside his head, since they do not have any kind of formal documentation. From his point of view, it is better to have more people and as a result a good redundancy of the knowledge, despite the fact that it will initially require a lot of work for him. Finding four deviates from what Bauer et al. [1] stated. It seems that committing a security policy creation to firewall configuration implementers is normal practice among system administrators. There are many ways to simplify the process of configuring firewalls, and thus the second result was expected as well.

Unexpectedly, four respondents reported that it is easy to configure firewalls. However, all of them have discovered misconfigurations several times. It would be interesting to investigate where errors come from if it is not the complexity of the process of configuring firewalls. To answer the question "If firewalls are easy to configure, why are there so many misconfigurations?" we need to continue conducting interviews. We believe that it might be easy to manage firewalls when configurations are almost static. Another source of misconfigurations could be some approaches that are used to simplify the process of configuring firewalls. Actually, none of them guarantee that the firewall configuration is fully consistent.

5 Concluding Remarks

We described the ongoing work on understanding the challenges of firewall management. A number of semi-structured interviews with system administrators have been conducted. Both expected and unexpected results were obtained. We were not aware that experienced system administrators claim that it is easy to configure firewalls. In our future work, we are interested in further exploring the issue. Our intention is to propose a concept of a visualization to our respondents and collect their opinions and suggestions on it.

References

1. Bauer, L., Cranor, L.F., Reeder, R.W., Reiter, M.K., Vaniea, K.: Real life challenges in access-control management. In: CHI 2009. ACM (2009)
2. Chao, C.: A flexible and feasible anomaly diagnosis system for internet firewall rules. In: APNOMS 2011. IEEE (2011)
3. Galletta, A.: Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication (Qualitative Studies in Psychology). NYU Press (2013)
4. Wool, A.: A quantitative study of firewall configuration errors. Computer **37**(6), 62–67 (2004)
5. Wool, A.: Trends in firewall configuration errors: Measuring the holes in swiss cheese. IEEE Internet Computing **14**(4), 58–65 (2010)