Network security is an important aspect that must be taken into account. Firewalls are systems that are used to make sure that authorized network traffic is allowed and unauthorized traffic is prohibited. However, setting up a firewall correctly is a challenging task. Their configuration files might be hard to understand even for system administrators.

The overall aim of this thesis is to identify firewall usability gaps and to mitigate them. To achieve the first part of the objective, we conduct a series of interviews with system administrators. In the interviews, system administrators are asked about the problems they face when dealing with firewalls. After having ascertained that the usability problems exist, we conduct a systematic literature review to get an understanding on the state of the art of the field. This review classifies available solutions and identifies open challenges. To achieve the second part of the objective, a set of usability metrics is proposed and mathematically formalized. A strong correlation between our metrics and how system administrators describe usability is identified.
Usable Firewall Rule Sets

Artem Voronkov
Usable Firewall Rule Sets

Artem Voronkov

LICENTIATE THESIS

Karlstad University Studies | 2017:40

urn:nbn:se:kau:diva-64703

ISSN 1403-8099

ISBN 978-91-7063-817-6 (Print)


© The author

Distribution:
Karlstad University
Faculty of Health, Science and Technology
Department of Mathematics and Computer Science
SE-651 88 Karlstad, Sweden
+46 54 700 10 00

Print: Universitetstryckeriet, Karlstad 2017

WWW.KAU.SE
Usable Firewall Rule Sets

Artem Voronkov
Department of Mathematics and Computer Science
Karlstad University

Abstract

Most companies have access to the Internet and their corporate networks connected to it. There are many threats to computer systems that may entail, for example, confidential data theft, service disruption and financial losses. A main concern of network security is to prevent unauthorized access to a computer network or network-accessible resources. Therefore, network security is an important aspect that must be borne in mind. Firewalls are an important component of network security that protect networks by controlling incoming and outgoing traffic.

The level of security provided by a firewall depends to a large extent on how well it is configured. However, setting up firewalls correctly is a challenging task. Their configuration files consist of so-called rule sets that might be hard to understand even for system administrators. The main reason for this is that most firewall rule sets have a certain structure: the higher the position of a rule in the rule set, the higher priority it has. Challenging problems arise when a new rule is added to the set, and a proper position for it needs to be found or existing rules are removed due to a security policy change. This brings us to the usability problem associated with the configuration of firewalls.

The overall aim of this thesis is to (i) identify firewall usability problems and (ii) address them. To achieve the first part of the objective, we conduct a series of semi-structured interviews with system administrators. In the interviews, system administrators are asked about the problems they face when dealing with firewalls. After having ascertained that the usability problems exist, we conduct a systematic literature review to get an understanding on the state of the art of the field. This review classifies available solutions and identifies open challenges. To achieve the second part of the objective, a set of usability metrics is proposed and mathematically formalized. We show that there is a strong correlation between our metrics and how system administrators perceive usability.

Keywords: Network Security, Usable Security, Firewall Configuration, Systematic Literature Review, Usability Metrics, User Studies.
Acknowledgements

My journey started in the summer of 2014 when I took the decision to move to Karlstad and pursue a doctoral degree at Karlstad University. I will never regret time spent here. I would like to say great thanks to my dearly loved wife, Veronika, and my family for their constant overwhelming support, despite some of my sudden decisions (like moving to Karlstad) and inspiration towards pursuing an academic career. I am thankful to Susanne, who allowed me to stay in her home when I first came to Karlstad.

I express my gratitude to my supervisor Stefan Lindskog for believing in me, for his support and feedback throughout my studies. I am also grateful to my co-supervisor Leonardo Martucci for all the effort he put in order to make this thesis possible. I would like to thank both of you for everything you did and for the opportunity to pursue my licentiate. You have helped me to gain valuable skills that have greatly added to my success.

Finally, I would like to thank all my colleagues at the Department of Mathematics and Computer Science for the remarkable working environment. I would especially like to thank the members of the PriSec group for great discussions, scientific and non-scientific alike.

The work in this thesis was carried out as a part of the High Quality Networked Services in a Mobile World (HITS) project, funded partly by the Knowledge Foundation of Sweden.

Karlstad University, November 2, 2017
Artem Voronkov
List of Appended Papers

This thesis is based on the work presented in the following papers:


The papers have been subjected to minor editorial changes.

Comments on my Participation

Paper I The idea for this paper as well as the design of the experiment originated from a discussion with my supervisors Stefan Lindskog and Leonardo A. Martucci. I conducted the interviews, analyzed the obtained data and did the majority of the writing.

Paper II This paper was written in collaboration with Leonardo Horn Iwaya, who came up with the initial idea and the methodology suggestion. I, in turn, did the practical part of the work and most of the writing. My co-authors helped me with the verification of the results as well as revising the paper during the rebuttal.

Paper III A discussion with my co-supervisor Leonardo A. Martucci led to an idea for this work. I made most of the user studies’ design decisions. All the user studies and the following analysis of the data were also performed by me. Matthias Beckerle helped with the formalization, while Stefan Lindskog and Leonardo A. Martucci were giving their feedback throughout the whole process and helped out with writing the paper.
# Contents

List of Appended Papers  

**INTRODUCTORY SUMMARY**  

1 Introduction  

2 Background and Related Work  
   2.1 Firewall Rule Sets  
   2.2 Usability  

3 Research Questions  

4 Research Methodology  

5 Contributions  

6 Summary of Appended Papers  

7 Concluding Remarks and Outlook  

**Paper I:**  
Challenges in Managing Firewalls  

1 Introduction  

2 Related Work  

3 Methodology and Interview Details  
   3.1 Semi-structured Interviews  
   3.2 Respondents  

4 Results and Discussion  
   4.1 Results of the Semi-structured Interviews  
   4.2 Discussion  

5 Concluding Remarks  

**Paper II:**  
Systematic Literature Review on Usability of Firewall Configuration  

1 Introduction
# Systematic Literature Review Methodology

## 2.1 Research Questions

## 2.2 Search Strategy

## 2.3 Search Terms

## 2.4 Quality Assessment and Data Extraction

# Primary Selection

# Secondary Selection

## 4.1 Removing Overlapping Works

## 4.2 Data Extraction

# Summary of Selected Papers

## 5.1 Personal Firewalls

## 5.2 Network Firewalls

## 5.3 Excluded Papers

# SLR Synthesis and Discussion

## 6.1 SLR Overall Discussion

## 6.2 On Usability of Firewall Configuration

# Concluding Remarks

# Appendix

## A Primary Selection Search Details

### A.1 ACM Digital Library

### A.2 IEEE Xplore

### A.3 dblp

### A.4 Inspec

---

## Paper III: Measuring the Usability of Firewall Rule Sets

### 1 Introduction

### 2 Background

### 3 Pilot Study

#### 3.1 Participants

#### 3.2 Method

#### 3.3 Results
4 Usability Factors
  4.1 Human Perceived Complexity ............................................ 79
  4.2 Conflicts in the Rule Set ................................................. 80
  4.3 Comments in the Rule Set ................................................. 80
  4.4 Structural Complexity .................................................... 81

5 Formalization
  5.1 Basic Building Blocks ..................................................... 82
  5.2 Derived Building Blocks ................................................... 82
  5.3 Usability Metrics ........................................................... 84

6 Testing the Cognitive Effort
  6.1 Participants ................................................................. 86
  6.2 Method ...................................................................... 87
  6.3 Results ....................................................................... 88

7 Validation
  7.1 Participants ................................................................. 91
  7.2 Method ...................................................................... 91
  7.3 Results ....................................................................... 92

8 Discussion
  8.1 About the User Studies .................................................... 93
  8.2 Limitations ................................................................. 93

9 Concluding Remarks ........................................................... 94

Appendix ................................................................. 96

A Damerau-Levenshtein Distance ........................................... 96
1 Introduction

There are a huge number of threats to computer systems on the Internet. Thus, network security is an important aspect that must be taken into account. One of the means of network security is a firewall, which can be implemented in software, hardware or as a combination of both. Its main task is to protect segments of the network or individual computers from unauthorized access by controlling incoming and outgoing traffic. Firewalls accept or drop packages based on a set of predefined rules [9]. The level of protection provided by the firewall depends heavily on the quality of its configuration file. A report on firewall configuration files [33] showed that all 12 rule sets investigated in the study contained errors. This result was later confirmed by another study with 36 rule sets [34]. The latter study showed that "firewalls are still poorly configured, a rule set's complexity is positively correlated with the number of errors." Errors in rule sets are often referred to as either misconfigurations or anomalies [2, 3, 17].

System administrators typically use a multi-phased approach for firewall planning and implementation [15]. The NIST guideline on firewalls and firewall policy [26] suggests five phases for this process: 1) Planning, 2) Configuration, 3) Implementation, 4) Initial deployment and 5) Management. In this thesis, we focus on the process of configuring a firewall, i.e. creating a rule set that correctly implements a higher level security policy, and managing it. Our main goal is to offer system administrators more usable solutions that can facilitate their daily work. We look at the process of working with firewalls from the system administrators’ perspective in order to understand the reasons behind misconfigurations. This is described in more detail in Paper I. We also conduct a systematic literature review (SLR) to find existing solutions that can potentially reduce the amount of effort spent by administrators and at the same time improve the quality of rule sets. Moreover, this review identifies gaps and issues that have not been adequately addressed in the literature. See Paper II for further details. We pick out one of the identified challenges, i.e. the lack of tools for measuring usability, and address it. Based on the results obtained in Paper I, we propose four metrics for evaluating the usability of a rule set. We mathematically formalize the proposed metrics and assess the coherence of the metrics with what system administrators think about usability. More details can be found in Paper III.

The rest of this introductory summary is organized as follows. Section 2 provides the required background information and discusses related work. The research questions addressed are outlined in Section 3. In Section 4 we describe the research methods used in the thesis. The main contributions of this work are given in Section 5. The summaries of the papers are presented in Section 6. Finally, in Section 7 we present concluding remarks and future work.
2 Background and Related Work

This section provides the necessary background to understand the research domain discussed in this thesis. Section 2.1 provides a comprehensive understanding of firewall rule sets and their peculiarities, which is crucial for the entire research presented in the thesis. Another crucial aspect, usability, is presented in Section 2.2, where we give its definition and discuss related work.

2.1 Firewall Rule Sets

Firewalls are systems that filter incoming and outgoing network traffic. The decision taken by firewalls as to whether to allow or block network traffic follows a set of rules. A firewall rule consists of: a set of conditions (e.g. on IP addresses, mac-addresses, protocols) and a decision that usually is to accept or block traffic (other decisions such as logging events or further examination of a packet are also possible). A firewall parses the headers of packets that pass through it and compares the output with its rule set. For most firewalls, comparisons are performed in a certain order—from the beginning of the rule set until a rule is triggered. If no matching rule was found, the standard rule (usually drop packet) is applied.

Rule sets are usually dynamic, i.e. they change over time, due to the fact that security policies, topologies, etc. might change. Challenging problems arise when you, for instance, add a new rule to the policy. Errors might occur when modifying a rule set and this will likely result in inappropriate system security. Such errors can be categorized into five types [4]: 1) Shadowing, 2) Correlation, 3) Generalization, 4) Redundancy and 5) Irrelevance.

2.2 Usability

The term usability can be defined in several ways. For example, it is defined by ISO 9241-11 [18] as:

“\[The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.\]”

where effectiveness means how successfully goals were achieved, efficiency means how properly time was utilized and satisfaction means how eager a user is to use a system. Nielsen [20] brings in additional usability aspects: learnability—how easy it is to get familiar with the system; memorability—how easy it is to remember details about the system after a period of nonuse; safety—how many mistakes a user makes. Similarly, Shneiderman and Plaisant [27] introduce their five usability aspects: 1) Speed of performance, 2) Time to learn, 3) Retention over time, 4) Rate of errors by users and 5) Subjective satisfaction. All these definitions are closely related and were summarized [30].

Since 1975, when Saltzer and Schroeder [24] brought in psychological acceptability as one of the eight design principles of information protection systems,
usability and security started to align in an area that is called *usable security*. Usable security for ordinary end users [32, 35] and advanced users (e.g. system administrators) [5, 7, 10] have been studied. Visualization techniques became one of the most widely used approaches for usable security [12, 23], in particular, in the management of security policies [22, 31].

Research on firewalls often focuses on issues other than usability, for example: filtering performance issues [16, 29] and anomaly detection [3, 17, 21]. However, as mentioned by Sasse and Smith [25]:

“Security mechanisms are often too time consuming for people to bother with, or so complex that even those willing to use them make mistakes.”

In other words, usability is an important property of security mechanisms. To be able to measure usability, a set of metrics is required. Although several attempts have been undertaken [1, 6, 8] to introduce some firewall complexity (usability) metrics, they all lack proper formalization and evaluation.

3 Research Questions

The overall objective of this dissertation is to provide usable tools to help system administrators better manage firewalls. Hence, the research questions addressed in the thesis are:

1. **What are the reasons behind firewall misconfigurations?**
   
   It has been demonstrated in the literature [33, 34] that firewall configuration files often contain errors. We need to know why this happens and to investigate the complexity of the process of configuring firewalls. In particular, we want to identify the main difficulties system administrators deal with when working with firewalls and to check whether there are usability issues involved.

2. **How to improve the usability of the firewall configuration process?**
   
   We turn to literature to see what has already been done towards improving the usability of firewalls. We set off to identify existing solutions that help users to create and manage firewall configuration files, and to analyze them in respect of usability. That allows us to pinpoint the open challenges in the field and thereby to answer the question of how the usability of the firewall configuration process can be improved.

4 Research Methodology

Computer science deals with the understanding and design of computers and computational processes. It can be considered as a mathematical, a scientific and an engineering discipline [13, 28]. Computer science is often divided into two major fields: *theoretical* and *applied* [11] and embraces a range of topics such as
The research work described in this thesis follows the traditional scientific approach that includes observations, hypotheses formulation, testing and verification. We start with formulating the initial hypothesis: “There are usability problems with firewall configuration.” The following hypotheses are formulated after testing the preceding hypothesis.

We test and verify the hypotheses using qualitative and quantitative together with statistical research methods. In Paper I, we use semi-structured interviews, a qualitative method of inquiry, to test the initial hypothesis. Semi-structured interviews usually consist of a set of predetermined questions and other questions that emerge from the dialogue between an interviewer and a respondent [14]. In Paper II, an SLR [19] has been utilized. An SLR is used to identify, evaluate and interpret all relevant research in a particular area. It is performed in accordance with a predefined strategy that comprises 1) Development of a protocol that includes all the elements of the review, including research questions the review is intended to answer, search terms, inclusion criteria, etc.; 2) Primary and secondary selection procedures; 3) Meta analysis (if needed) and 4) Data synthesis. In Paper III, we conduct a user study with students in order to test whether cognitive aspects affect the user–system interaction. For this purpose, a subjective mental effort questionnaire [36] is applied and the obtained data are analyzed by the paired sample t-test. Another method utilized in the verification stage is the Spearman rank correlation test.

5 Contributions

To address the research questions outlined in Section 3, this thesis makes the following contributions:

1. Understanding of the firewall management challenges

   In Paper I, we conduct a series of semi-structured interviews with IT professionals. We gain insight into the firewall management process from system administrators’ perspective, including what difficulties they face, how they interact within groups and what means or procedures are used to simplify this process. The results of the interviews also help us to identify that the lack of firewall usability is one of the challenges. This contributes to answering Research Question 1.

2. Identifying state of the art in firewall usability and producing the taxonomy of existing approaches

   In Paper II, we present an SLR with a focus on the usability of firewall configuration. We retrieve and screen 1,202 papers, of which 14 are selected and summarized. This SLR gives us the understanding of what has already been done and helps us to pinpoint the open challenges that exist in the field. Another contributions is a taxonomy of existing
approaches that address usability aspects of firewalls. This contributes to answering Research Question 2.

3. Understanding of the impact of cognitive aspects in the examination of firewall rule sets

In Paper III, we propose a hypothesis that the cognitive effort needed to understand a rule is not affected by its immediately preceding rule. We test that with a user study and the results reject the hypothesis. Furthermore, we present a function that indicates the relation between the cognitive effort reduction and the similarity between examined rules. The necessity of taking cognitive aspects into account is tested in the validation study. This contributes to answering both Research Questions 1 and 2.

4. The proposal of means to measure the usability of firewall rule sets

It is necessary to have metrics in order to be able to compare different firewall solutions with respect to their usability. In Paper III, we introduce and mathematically formalize a set of four firewall usability metrics. We validate the quality of the proposed metrics by conducting a user study with system administrators. This user study shows a very strong positive correlation between how our metrics and system administrators characterize the usability. This contributes to answering Research Question 2.

6 Summary of Appended Papers

Paper I – Challenges in Managing Firewalls

In this paper, we address the question: what are the main difficulties system administrators deal with when working with firewalls? Semi-structured interviews were used as the method of inquiry in this study. We draw some conclusions from the interviews’ results such as (i) it is not always beneficial to have more people responsible for security measures and (ii) firewall misconfigurations are a common problem. The paper shows that there are existing usability issues related to the management of firewalls.

Paper II – Systematic Literature Review on Usability of Firewall Configuration

In this paper, we present an SLR with a focus on the usability of firewall configuration. Usability problems, as pointed out in the literature, entail poorly configured firewalls. During the selection procedures, 1,202 papers are retrieved and screened, 35 papers are chosen for further investigation, of which 14 papers are selected and summarized. As main contributions, we propose a taxonomy of existing solutions as well as a synthesis and in-depth discussion about the state of the art in firewall usability.
Paper III – Measuring the Usability of Firewall Rule Sets

In this paper, we introduce a set of metrics that can measure the usability of firewall rule sets in terms of how easy it is for IT professionals to understand and manage them. These metrics are derived from semi-structured interviews with system administrators, in which we elicit the usability challenges related to the management of firewall rule sets, and findings from related work. We also identify a cognitive aspect that influences the examination of firewall rule sets and how it can be quantified. We validate the metrics by conducting another user study with system administrators. We show that there is a very strong correlation between the results of a ranking exercise performed by the system administrators and an implementation of our metrics.

7 Concluding Remarks and Outlook

Even though each of the appended papers has its own research goals, their findings significantly contribute to the achievement of the main goal of this thesis, i.e. to help system administrators better manage firewalls. By means of semi-structured interviews with system administrators, we found out what difficulties they face and concluded that there are usability problems related to the management of firewalls. The conducted SLR gave us an overview of the research area and helped us to identify existing gaps and sparsely studied sub-fields. An important aspect overlooked by the related work is the absence of metrics for measuring the usability of firewall rule sets. As a result, we proposed a set of metrics and validated their quality with a user study that showed a very strong positive correlation between how our metrics and system administrators characterize the usability of rule sets.

In the near future, we aim to continue working with the metrics, proposed in Paper III. In particular, the weights of the metrics were assigned an equal value, however, they might contribute differently to the total usability and this requires further investigation. In the middle term, we want to suggest alternative ways of presenting information in firewall rule sets. For this purpose, we plan to run user studies that will help us to assess different visualization techniques.

References


Usable Firewall Rule Sets

Network security is an important aspect that must be taken into account. Firewalls are systems that are used to make sure that authorized network traffic is allowed and unauthorized traffic is prohibited. However, setting up a firewall correctly is a challenging task. Their configuration files might be hard to understand even for system administrators.

The overall aim of this thesis is to identify firewall usability gaps and to mitigate them. To achieve the first part of the objective, we conduct a series of interviews with system administrators. In the interviews, system administrators are asked about the problems they face when dealing with firewalls. After having ascertained that the usability problems exist, we conduct a systematic literature review to get an understanding on the state of the art of the field. This review classifies available solutions and identifies open challenges. To achieve the second part of the objective, a set of usability metrics is proposed and mathematically formalized. A strong correlation between our metrics and how system administrators describe usability is identified.