

Systematic review of automatic translation of high-level security policy into firewall rules

Ivan Kovačević*, Bruno Štengl†, Stjepan Groš‡

University of Zagreb Faculty of Electrical Engineering and Computing, Zagreb, Croatia

*ivan.kovacevic@fer.hr, †bruno.stengl@fer.hr, ‡stjepan.gros@fer.hr

Abstract—Firewalls are security devices that perform network traffic filtering. They are ubiquitous in the industry and are a common method used to enforce organizational security policy. Security policy is specified on a high level of abstraction, with statements such as “web browsing is allowed only on workstations inside the office network”, and needs to be translated into low-level firewall rules to be enforceable. There has been a lot of work regarding optimization, analysis and platform independence of firewall rules, but an area that has seen much less success is automatic translation of high-level security policies into firewall rules. In addition to improving rules’ readability, such translation would make it easier to detect errors.

This paper surveys of over twenty papers that aim to generate firewall rules according to a security policy specified on a higher level of abstraction. It also presents an overview of similar features in modern firewall systems. Most approaches define specialized domain languages that get compiled into firewall rule sets, with some of them relying on formal specification, ontology, or graphical models. The approaches’ have improved over time, but there are still many drawbacks that need to be solved before wider application.

Keywords—network security, security policy, firewall

I. INTRODUCTION

Security policy defines a system’s security requirements through standards, rules, and practices [1]. In firewall implementations, security policies are implemented using a set of firewall rules that match network packets and define actions that are performed over such packets. In traditional firewalls, rules are written in domain specific languages that use various low-level technical details, such as IP addresses, ports, and protocols, which makes them challenging to define and manage. Mayer et al. [2] compares the readability of such rules to assembly code.

Organizations would benefit from the ability to describe security policies on a higher level of abstraction, where they would be more concerned with the semantics of what they want to achieve rather than low-level technical details. For instance, a single high-level policy statement could allow all workstations access to domain controller (DC) services, such as offered by Active Directory, instead of having multiple rules that filter packets according to source subnets, server IP address and characteristic DC service ports. Such policy definitions would be more comprehensive and much easier to understand and manage, especially in large Enterprise networks. Furthermore, it would be useful to be able to enforce such policies using existing firewall systems that companies already use. Another area

that would benefit from such capabilities are approaches that generate models of IT systems for cyber security exercises, such as [3], where abstract policies need to be implemented on concrete firewall systems used during a cyber exercise.

In accordance with the aforementioned motivation, our survey aims to find approaches that generate firewall configurations based on security policies defined at a high level of abstraction. Here, *high level of abstraction* refers to the fact that definitions of such policies avoid relying on network-related technical details, including various aliases thereof (e.g. *home_network*). Instead, they use formulations closer to natural language, or an abstract visual definition through a graphical user interface (GUI). In addition, the approaches’ must provide a concrete implementation, and not be limited to a proposal or patent only describing a framework or idea. Other types of approaches, such as those focusing on firewall rule verification and error detection, are outside the scope of this paper. Last but not least, our survey focuses only on papers for which the full text is available in English.

In parallel to the aforementioned approaches, next generation firewall (NGFW) systems [4] introduce various high-level concepts that enable a more direct mapping between policies and firewall rules. This survey includes a brief overview of their features, focusing on those which mirror functionality of the surveyed approaches.

This paper is organized as follows. Section II describes the methods used to perform the survey. Next, Section III provides an overview of the surveyed papers, and shows examples of similar functionality offered by modern firewall systems. The results and their significance are discussed in Section IV. Finally, the paper presents related work in Section V and wraps up with conclusions in Section VI.

II. METHODS

This section describes the methods used to survey the literature. Several literature searches were performed using Google Scholar and Semantic Scholar, supported by the software tool Publish or Perish [5]. The following search terms were used: (i) *high-level firewall rules*, (ii) *high-level firewall policies*, (iii) *management of firewall rules*, (iv) *management of firewall policies*, and (v) *generating firewall rules from high-level policies*. From each search, 50 most relevant results were collected,

yielding 500 papers in total. After removing duplicate papers, 304 papers remained. Out of these, only 23 papers representing 17 distinct approaches remained within the scope of this survey. The remaining approaches were analyzed according to research questions listed below. Each question is designated with a label and describes potential answers where necessary:

- 1) *Level (H/M/L)*: What is the level of abstraction of security policies defined as inputs to the approach? Possible values include the following:
 - H: Policies are defined using natural language, as spoken by management and policy makers.
 - M: Policies are defined using formal specification or graphs with concepts like users, types of applications, types of roles, etc. They do not primarily focus on technical details such as IP addresses, ports, etc., and instead link such details using a knowledge base and/or separate configuration.
 - L: Defines policies with technical details that are hidden behind concepts similar to roles, instead of being stated as low-level firewall rules. An example would be defining policies related to the *public_web_server* role, and separately label several servers with the aforementioned role.
- 2) *KB (yes/no/partial/N.A.)*: Does the approach include a predefined knowledge base, or predefined rule conversion (expert) rules? If large parts of the knowledge base must be tailored specifically for the organizational IT system where they are to be deployed, it is considered as a partial KB.
- 3) *GUI (yes/no/N.A.)*: Does the approach include a GUI and/or a visualization component?
- 4) *Output rules*: Which types of low-level firewall rules can the approach generate? Examples could include iptables rules and Cisco firewall rules.
- 5) *Category*: What is the central concept used to define and process policies? Possible categories include the following:
 - *Ontology*: the approach uses ontologies to define the high-level security policy.
 - *Language*: the approach is based on features characteristic to high-level programming languages, such as operators or inheritance, or defines policies using markup languages such as XML.
 - *Formal*: the approach uses formal predicates to define the security policy, e.g. as a collection of conditions that must always be met. Such formal specification of high-level policy is used to generate low-level rules using various automated reasoning and optimization algorithms.
 - *Graph*: the approach uses graphs, such as Petri nets, to link entities and define high-level policies.
- 6) *Usability*: Do authors report a usability study? If yes, what type? Possible types include the following:
 - *Study*: Authors report a usability study with target users, in which it was confirmed that the approach makes policies easier to manage than low-level

rules and that its expressiveness is sufficient for real-world usage scenarios.

- *Claims*: Authors describe experiments in which they define policies and claim that they were successful in using the system.
- *N.A.*: Usability was not evaluated.

III. RESULTS

By applying the method outlined in Section II, we initially found 304 unique papers. We propose a rough informal categorization of those papers according to research areas as shown in Fig. 1. Papers within the scope of this survey are labeled as *Automatic translation of high-level security policies*, and their overview is provided in Section III-A. Remaining categories are briefly explained in Section III-B. There are many border cases in which papers could potentially be categorized into alternative categories, so it is possible that other researchers could obtain slightly different paper counts. Finally, Section III-C provides an overview of comparable features of some modern firewall systems commonly used in the industry.

A. Automatic translation of high-level security policies

Some properties of the surveyed approaches are outlined in Table I. Among these approaches, high-level security policies are frequently defined using a programming language inspired syntax or XML documents. Formal methods and graphical models are used to a lesser degree, with only one approach relying on an ontology. The following paragraphs provide brief examples of policy definitions for each category.

Basile et al. [21] use sentences close to natural language to describe high-level security requirements. Subjects, objects and actions that can be used in sentences are pre-configured in the approaches' knowledge base. A few examples of such requirements are shown in Listing 1. The first one bans users from visiting gambling sites, and the second one allows user Alice to access Internet between 18:30 and 20:00 hours. The security requirements are automatically translated to configurations of appropriate network devices.

Gaaserud [17] defines a syntax similar to programming languages, which supports variables and inheritance, and can be used to define rules more comprehensive than traditional low-level firewall rules. Listing 2 shows a simplified example where this syntax is used to describe the Facebook web application and define a rule that grants access to it from the internal network. In a similar manner, other applications and locations on the network can be described, which would enable specifying policy based on applications and groups of resources rather than IP addresses, ports and protocols.

Adão et al. [24] define the security policy using high-level goals that need to be enforced. These goals are specified using formal predicates that describe desirable states of packets at certain locations in the network. The formally specified goals transparently support network

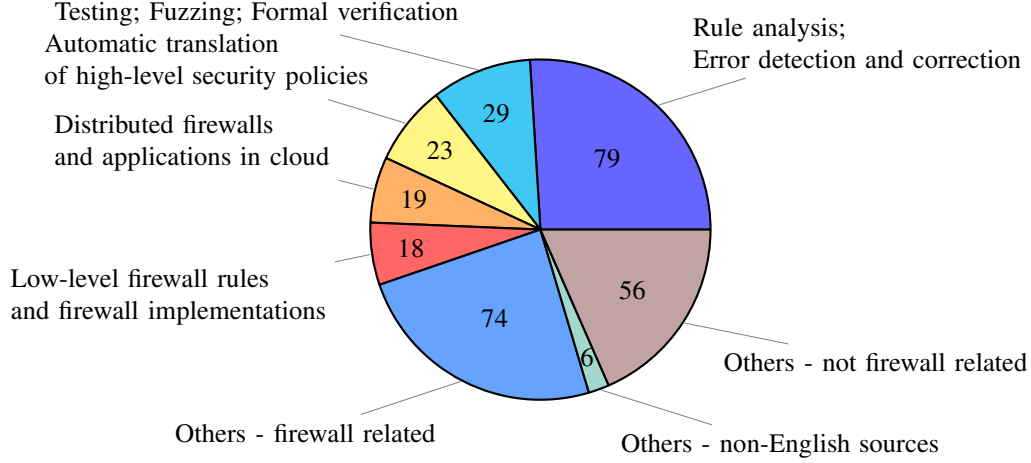


Fig. 1: Rough categorization of initial search results. Duplicate results are excluded. Individual categories of papers are explained in Section III.

TABLE I: Overview of the surveyed approaches. In cases in which approaches were published through multiple papers, the year of the most recent one is indicated. Individual columns and categories are explained in Section II.

| Approach | Year | Level | KB | GUI | Category | Usability | Output rules |
|---------------------------|------|-------|---------|-----|----------|-----------|---|
| Bartal et al. [6, 7] | 2004 | L | partial | yes | Language | Study | Lucent VPN, Check Point FireWall-1, Cisco PIX Firewall, Cisco IOS |
| Cuppens et al. [8] | 2004 | M | no | no | Formal | N.A. | iptables, tested with netfilter |
| Zhang et al. [9] | 2007 | L | no | no | Language | Study | format similar to iptables |
| Xu et al. [10] | 2007 | M | partial | yes | Graph | Study | Colored Petri net formalism |
| Bandara et al. [11, 12] | 2009 | L | no | no | Formal | Claims | N.A. |
| Hassan and Bahgat [13] | 2009 | M | partial | no | Language | N.A. | N.A. (vendor specific) |
| Basile et al. [14] | 2010 | H | yes | yes | Ontology | Claims | N.A. |
| Kropiwiec et al. [15, 16] | 2011 | L | no | no | Language | Claims | iptables |
| Gaaserud [17] | 2013 | L | no | no | Language | Study | Palo Alto PanOS |
| Al-Shaer [18, 19] | 2014 | L | partial | yes | Language | Study | format similar to iptables |
| Deng et al. [20] | 2015 | L | no | no | Language | Claims | ClickOS-based firewall implementation |
| Basile et al. [21] | 2015 | H | yes | yes | Language | N.A. | packet filtering virtual network function |
| Sapia et al. [22, 23] | 2016 | L | no | yes | Graph | Study | Packet filter |
| Adão et al. [24] | 2016 | L | no | no | Formal | Claims | Netfilter |
| Rivera et al. [25] | 2019 | M | partial | no | Language | Study | iptables |
| Brighenti et al. [26] | 2020 | M | no | no | Graph | N.A. | N.A. |
| Karafili et al. [27, 28] | 2020 | L | yes | no | Formal | Claims | N.A. |

Listing 1: Examples of high-level security requirements from Basile et al. [21].

```
"do not access gambling sites"
"allow Internet traffic
  from 18:30 to 20:00 for Alice"
```

address translation (NAT) and are used to automatically generate, optimize, and localize low-level firewall rules. Localization here refers to the task through which rules need to be placed on multiple firewalls throughout the network, with each having its own surroundings and potentially a different NAT configuration. Unfortunately, goals are stated using complex logical formulas and their notation does not seem to be very comprehensible.

Sapia et al. [22, 23] develop an educational tool, SP2Model, that can be used to model firewall rules in a graphical manner. After network resources have been defined, users are presented with a graphical interface where they can draw a graph that describes the security policy. This graph still retains low-level rule semantics, and it is questionable whether it could be applicable in larger networks.

Brighenti et al. [26] propose a specialized solution for Kubernetes [29] clusters that automatically generates firewall rules according to defined services and their communication requirements. Users can manually allow additional communication flows. We classify this as a graph approach because the service definitions effectively form a graph, with services as nodes and their communication requirements as edges.

Finally, Basile et al. [14] propose an ontology that

Listing 2: An example of a configured application and defined rule from Gaaserud [17].

```

application facebook {
    protocol tcp
    port 80, 443
    signature "www.facebook.com"
}
rule "facebook access" {
    application facebook
    from internal
    to external
    source client -network
    destination any
    action allow
}

```

describes the network resources and their connectivity. High-level policies are initially defined as statements, after which the developed tool leads its users through policy refinement and generates low-level firewall rules. Policy refinement and rule generation are performed by applying automatic reasoning over the populated ontology.

B. Categories outside the scope of this survey

This subsection briefly describes initially collected papers that are outside the scope of this survey. Most such papers belong to the category *rule analysis and error detection and correction*. The main goal of papers in this category is to analyze existing firewall policies or security policies specified on a higher level of abstraction, and make them easier to comprehend for firewall administrators and policy makers. Some of them can also highlight potential configuration errors and suggest corrections. One such approach is Bodei et al. [30], where authors convert low-level firewall rules into a high-level formal representation that can be analyzed.

Many papers are concerned with testing, fuzzing, or formal verification of existing firewall policies. Formal verification approaches, such as Kutenko and Polubelova [31], propose formal models that can be used to model firewall policies and automatically verify whether a firewall configuration satisfies its corresponding model. Testing and fuzzing approaches, such as Al-Shaer et al. [32], aim to generate test packets to check whether a given firewall configuration handles them as expected. The test packets are generated according to predefined criteria.

Several papers deal with problems regarding *distributed firewalls and applications in cloud*. One such approach is Zhang et al. [33], where authors optimize the placement of firewall rules over multiple switches in a Software Defined Network (SDN).

In a number of papers, policies are defined on a higher level of abstraction than traditional firewall rules, but still retain a one-to-one correspondence to low-level technical details. As policies in this category are on a lower level

of abstraction than papers in the scope of this survey, we label them as *low-level rules*. In some other cases, such as Lupaescu et al. [34], the policies are described on a sufficiently high level of abstraction, but are used directly on a custom firewall implementation rather than being compiled into low-level firewall rules. Such papers are labeled as *firewall implementations* and are shown grouped together with low-level rules.

There are three categories representing other research areas. Papers labeled as *Others - firewall related* present various subjects related to firewalls, those labeled as *Others - non-English sources* are written in languages other than English, and the ones labeled as *Others - not firewall related* deal with research unrelated to firewalls, such as CPU architectures.

C. Comparable features of modern firewall systems

Neupane et al. [35] recently published a focused survey of NGFWs and their capabilities. NGFWs combine extensive packet analysis with data from multiple sources, such as authentication logs, making them able to enforce policies aware of application-specific payloads and users' identities, and provide intrusion prevention capabilities [4]. An extensive analysis of NGFWs is outside the scope of this paper. Instead, this subsection focuses on two features offered by Check Point Quantum NGFW [36], namely *identity awareness* and *application control*, which mirror common functionality proposed by the surveyed approaches. It must be noted that the authors of this survey are not in any way endorsed by Check Point and that this is only one of several NGFW systems frequently used in the industry.

Identity Awareness [36] collects information about users and network resources from services such as *Active Directory*, and associates network traffic with individual user accounts and devices. This enables straightforward implementation of policies that target individual users and devices instead of IP addresses. Such policies are much easier to maintain in modern organizations where users often work with multiple devices and connect through wireless networks and virtual private networks (VPNs).

Application control [36] involves deep packet inspection and is used to identify application specific network traffic. Consequently, admins can define policies that target individual applications regardless of ports, protocols, and other low-level technical details. Applications are detected using packet signatures from Check Point's internal database. Furthermore, applications are organized into categories and have an associated risk score [37] that can be used when defining policies. For instance, a single firewall rule can filter all traffic related to applications inside the *Anonymizer* category, such as VPN providers.

IV. DISCUSSION

The main goals of defining policies on a higher level of abstraction are to make them easier to comprehend and maintain, as well as to reduce the amount of domain

knowledge required for the users who configure them. Most of the approaches relying on languages, graphical methods, and ontology certainly manage to improve policy comprehensibility. However, defining policies in approaches based on formal specifications requires extensive knowledge of formal logic and theorem proving, so these approaches effectively manage to replace the need for experienced network admins with a need for experts in formal methods, and consequently do not significantly improve comprehensibility.

Important advantages of formal specification and ontology based approaches are that the high-level policies can be automatically checked for inconsistencies out-of-the-box and that the generated low-level firewall rules are guaranteed to adhere to the specification. Other types of approaches, such as [19], can in some cases also include components that provide similar functionality, but we leave an overview of such functionality for future work.

Another goal of high-level policy definition is to support transparent firewall management in large enterprise systems with numerous network segments and firewalls, which could require a very large set of rules to maintain. In this regard, most categories of approaches seem to, *at least in theory*, support such application, with the exception of graphical approaches that are either highly specialized, like [26], or are limited by the capabilities of their GUIs, like [22, 23]. The latter is caused by the inherent problem of visualizing large Enterprise networks, where visualizations can easily end up being very complicated and cluttered. A possible way of addressing this limitation would be to extend user interfaces of such approaches with abstraction of individual subsystems in the network.

In some approaches, information about users and resources can be imported from policy management software, such as Active Directory, while others require their users to define user identities and resources manually. A great advantage of the former is that resources and users can change over time, and this eliminates the need to handle such changes manually.

Most approaches suffer from a drawback that they need extensive configuration of domain specific data, such as descriptions of applications in [17], to produce rules. As technologies evolve and resources are upgraded or replaced, knowledge bases and configurations must be continuously updated as well. As can be seen in Section III-C, modern firewall systems already allow specifying rules that are aware of applications, users, and resources. Their vendors solve the aforementioned problem by delivering such firewalls together with additional services, often including continuous maintenance of the provided products and their knowledge bases. Specifically, Check Point maintains and delivers a large collection of application signatures and offers a service through which administrators can request assistance and report erroneous detection.

Last but not least, readers may observe that just six approaches performed validation of their results with domain experts, with the rest performing only case studies

or performance evaluation. Proper validation with multiple domain experts is important as it can uncover practical problems with the approach and provide possible solutions.

V. RELATED WORK

We found only one recent survey with a similar scope. Zaliva [38] comments some properties of approaches working with high-level policies, but does so very briefly, with the paper focusing primarily on detection of rule conflicts and anomalies. At the time of writing, [38] is over a decade old and misses the majority of approaches surveyed in this paper. In addition, this survey does not publish a methodology, making the reproducibility of its results challenging.

VI. CONCLUSION

This paper provided a survey of approaches that aim to translate high-level definitions of security policies into low-level firewall rules. The surveyed approaches support definition of policies using either natural language, various domain languages, formal specification, or ontology. Each of them comes with its own advantages and disadvantages. Common drawbacks include the fact that the proposed high-level policy definition is often difficult to write and maintain, and that knowledge bases and configurations need constant maintenance. A potential solution to the latter would be to deliver such functionality through services, in a similar manner to which vendors of NGFW systems like Check Point already deliver their products.

ACKNOWLEDGMENT

This work has been supported by the European Union's European Regional Development Fund, Operational Programme Competitiveness and Cohesion 2014-2020 for Croatia, through the project Center of competencies for cyber-security of control systems (CEKOM SUS), grant KK.01.2.2.03.0019.

REFERENCES

- [1] C. L. Schuba and E. H. Spafford, "A reference model for firewall technology," in *Proceedings 13th Annual Computer Security Applications Conference*. IEEE, 1997, pp. 133–145.
- [2] A. Mayer, A. Wool, and E. Ziskind, "Fang: A firewall analysis engine," ... *on Security and Privacy. S&P 2000*, 2000. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/848455/>
- [3] I. Kovačević, S. Groš, and A. Đerek, "Automatically generating models of IT systems," *IEEE Access*, vol. 10, pp. 13 536–13 554, 2022.
- [4] J. Pescatore and G. Young, "Defining the next-generation firewall," *Gartner RAS Core Research Note*, 2009.
- [5] A. W. Harzing, "Publish or perish," <https://harzing.com/resources/publish-or-perish>, 2007, accessed: 2022-01-25.

- [6] Y. Bartal, A. Mayer *et al.*, “Firmato a novel firewall management toolkit,” *ACM Transactions on Computer ...*, 2004. [Online]. Available: <https://dl.acm.org/doi/abs/10.1145/1035582.1035583>
- [7] —, “Firmato: A novel firewall management toolkit,” *Proceedings of the 1999 ...*, 1999. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/766714/>
- [8] F. Cuppens, N. Cuppens-Boulahia *et al.*, “A formal approach to specify and deploy a network security policy,” 2004.
- [9] B. Zhang, E. Al-Shaer *et al.*, “Specifications of a high-level conflict-free firewall policy language for multi-domain networks,” *Proceedings of the 12th ...*, 2007. [Online]. Available: <https://dl.acm.org/doi/abs/10.1145/1266840.1266871>
- [10] H. Xu, M. M. Ayachit, and A. Reddyreddy, “Formal modeling and analysis of xml firewall for service-oriented systems,” 2007.
- [11] A. Bandara, A. Kakas *et al.*, “Using argumentation logic for firewall configuration management,” *2009 IFIP/IEEE ...*, 2009. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/5188808/>
- [12] —, “Using argumentation logic for firewall policy specification and analysis,” *International Workshop on ...*, 2006. [Online]. Available: https://link.springer.com/chapter/10.1007/11907466_16
- [13] A. A. Hassan and W. M. Bahgat, “A framework for translating a high level security policy into low level security mechanisms,” 2009.
- [14] C. Basile, A. Liroy *et al.*, “Ontology-based security policy translation,” 2010.
- [15] C. D. Kropiwiec, E. Jamhour *et al.*, “Multi-constraint security policies for delegated firewall administration,” 2011.
- [16] —, “Multi-constraint security policies for delegated firewall administration,” 2008.
- [17] A. K. Gaaserud, “Towards an unified policy for next-generation firewalls : Creating a high-level language for ngfw,” 2013.
- [18] E. Al-Shaer, “Automated firewall analytics: Design, configuration and optimization,” 2014.
- [19] —, “Specification and refinement of a conflict-free distributed firewall configuration language,” 2014.
- [20] J. Deng, H. Hu *et al.*, “Vanguard: An nfvsdn combination framework for provisioning and managing virtual firewalls,” ... *IEEE Conference on ...*, 2015. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/7387414/>
- [21] C. Basile, A. Liroy *et al.*, “A novel approach for integrating security policy enforcement with dynamic network virtualization,” *Proceedings of the ...*, 2015. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/7116152/>
- [22] H. Sapia, R. E. García *et al.*, “Teaching-learning firewall configuration using a visual modeling web based tool: The sp2model and its application to computer science course,” 2016.
- [23] K. M. Trevisani and R. E. García, “Spml: A visual approach for modeling firewall configurations,” 2008.
- [24] P. Adão, R. Focardi *et al.*, “Localizing firewall security policies,” 2016.
- [25] D. Rivera, F. Monje *et al.*, “Automatic translation and enforcement of cybersecurity policies using a high-level definition language,” *Entropy*, 2019. [Online]. Available: <https://www.mdpi.com/585308>
- [26] D. Brighenti, G. Marchetto *et al.*, “Introducing programmability and automation in the synthesis of virtual firewall rules,” *2020 6th IEEE ...*, 2020. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/9165434/>
- [27] E. Karafili, F. Valenza *et al.*, “Towards a framework for automatic firewalls configuration via argumentation reasoning,” 2020.
- [28] E. Karafili and F. Valenza, “Automatic firewalls’ configuration using argumentation reasoning,” ... *on Emerging Technologies for Authorization and ...*, 2020. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-64455-0_8
- [29] Kubernetes, “Kubernetes,” <https://kubernetes.io/>, 2022, accessed: 2022-02-14.
- [30] C. Bodei, P. Degano *et al.*, “Language-independent synthesis of firewall policies,” *2018 IEEE European ...*, 2018. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/8406593/>
- [31] I. Kotenko and O. Polubelova, “Verification of security policy filtering rules by model checking,” *Proceedings of the 6th IEEE ...*, 2011. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/6072862/>
- [32] E. Al-Shaer, A. El-Atawy, and T. Samak, “Automated pseudo-live testing of firewall configuration enforcement,” *IEEE Journal on Selected ...*, 2009. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/4808474/>
- [33] S. Zhang, F. Ivancic *et al.*, “An adaptable rule placement for software-defined networks,” 2014.
- [34] F.-L. Lupaescu, I. Ivanciu *et al.*, “A firewall application for performance evaluation of the pyretic controller in software-defined networks,” 2016.
- [35] K. Neupane, R. Haddad, and L. Chen, “Next generation firewall for network security: A survey,” in *SoutheastCon 2018*. IEEE, 2018, pp. 1–6.
- [36] Check Point, “Check point quantum,” <https://www.checkpoint.com/quantum/>, 2022, accessed: 2022-02-02.
- [37] CheckPoint, “Check point appwiki,” <https://appwiki.checkpoint.com/appwikisdb/public.htm>, 2022, accessed: 2022-02-02.
- [38] V. Zaliva, “Firewall policy modeling, analysis and simulation: a survey,” *SourceForge, Tech. Rep.*, 2008. [Online]. Available: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.500.389>

This figure "figure1.jpg" is available in "jpg" format from:

<http://arxiv.org/ps/2212.03645v1>