UNIVERSITY OF BERGEN

Firewalls: Enforcement of Security Policy in networks

by

Harald Nordås

Supervisor: Prof. Øyvind Ytrehus

Thesis for the degree Master of Science in Informatics

November 2014

in the

Faculty of Mathematics and Natural Sciences

Department of Informatics

Selmer Centre

Abstract

Firewalls are set up to protect computer networks. Originally, networks were just coupled together, in order to achieve connection. With the ability to reach networks all over the world, one started to denote this the Internet. When the Internet evolved, the focus of design was on connectivity, efficiency and reliability, but not on security. Gradually, the need to control the traffic gave rise to enhanced security features of the routers connecting the networks. In the 1990s this was no longer sufficient, because people were able to circumvent this simple barrier. Dedicated devices then developed into more advanced mechanisms. The concept of a digital firewall was born.

Today a plethora of threats to a network challenge the firewall and organisations who are managing the firewall system. This thesis will go into the many tasks involved in managing a firewall system. We will look at challenges but also suggest solutions to some of the issues.

Acknowledgements

The author would first like to thank prof. Øyvind Ytrehus for his critical, but very helpful remarks and suggestions.

Numerous other people have contributed and given me support, and among them I would like to mention PhD student Stian Fauskanger and Lecturer Odd Rydland.

This thesis is dedicated to my family, who have been most understanding during the process of writing.

Contents

Abstract i

Acknowledgements ii

List of Figures v

List of Tables vi

1 Introduction 1
- 1.1 What are firewall systems ? . . . 2
- 1.2 Structure of the thesis . . . 3

2 An overview of a firewall system 4
- 2.1 Overview of a typical firewall system . . . 4
- 2.2 Features . . . 4
- 2.3 Setup of a new firewall system . . . 5
  - 2.3.1 Security gateways . . . 5
  - 2.3.2 Management . . . 6
    - 2.3.2.1 Problems in management . . . 8
  - 2.3.3 Additional components . . . 8
  - 2.3.4 Cloud security . . . 9
- 2.4 Outsourcing. . . . 9

3 A survey of some firewall research papers 10
- 3.1 The Structural Firewall Query Language and Firewall Decision Diagrams 10
- 3.2 Automatic Correction of Firewall Policy Faults . . . 12
- 3.3 Towards a New Design of Firewall . . . 12

4 Modelling firewalls as part of a CAS 14
- 4.1 What is a CAS ? . . . 14
- 4.2 How does malware spread on the Internet ? . . . 14
- 4.3 How to limit the effect of malware. . . . 16
- 4.4 Pitfalls in management operations . . . 17

5 Comparing different vendors 18
- 5.1 Vendors. . . . 18
- 5.2 3 largest systems of NGFW . . . 19
- 5.3 Strengths and weaknesses. . . . 20
  - 5.3.1 Check Point . . . 20

5.3.2 Palo Alto Networks 20
5.3.3 Fortinet 21

6 Questionnaire **24**
6.1 Purpose of survey 24
6.2 Common problems in management 24
6.3 What we found could be improved 25

7 Suggestions for better management of firewall systems **26**
7.1 Utilise inbuilt tools 26
7.1.1 Remove unused rules 26
7.1.2 Remove duplicate objects and unused objects 27
7.2 Routines 27
7.3 External tools 27
7.4 Managed Security 28
7.5 DNS 28
7.5.1 OpenDNS and Umbrella 28
7.5.2 Infoblox 29

8 Conclusion and summary **31**
8.1 Summary 31
8.2 Conclusions 31
8.3 Extensions of thesis work 32

A Copy of questionnaire **33**

B Summary of answers to questionnaire **38**

Bibliography **46**

List of Figures

2.1 Enterprise network by courtesy of Check Point 5

2.2 Classification of applications irrespective of port. 6

2.3 Menu of protection options (Check Point). 6

2.4 Event management menu (Check Point). 7

3.2 Average verifying time versus number of rules 13

4.1 Development of functions over time. 15

4.2 Instantaneous fractions of isolated nodes (red line) and infected nodes (green line) in a diverse network. 16

5.1 Gartner : Magic Quadrant for Enterprise Network Firewalls 19

5.4 Vendor claimed vs. NSS rated throughput in Mbps 23

7.1 Policy overview of rules (Check Point) 27

7.2 Hybrid C&C topology 29

7.3 Infoblox setup. 30

List of Tables

3.1 Conflicting policy 11

5.2 Comparison of three vendors of NGFW. 21

5.3 Comparison of gateway specifications from three vendors of NGFW 22

Chapter 1

Introduction

Firewalls originally separated the parts of a building most likely to have a fire. This would typically be the kitchen, described by Lightoler [1]. By preventing or slowing down the spread of fire, both lives and property were saved.

In the modern setting, we would like to protect computer networks.

Internet stems from ARPANET, a research network developed in a project sponsored by the US military. Due to the concerns of the sponsor, several important servers located in different parts in the country needed to be connected, to avoid single point of failure. This was such a big success, so the universities copied the idea. The design objective was to connect different networks. The military assumed a closed network, so at first security was not important. When more networks and computers were interconnected, people started using the big network in all sorts of ways. One aspect was trying to break into systems. The motivations for breaking in could be to show technical skills, to manipulate information, or to gain economical benefits to mention a few. Steve Jobs even described this in his biography [2][p.47], were he and a friend sold an illegal device they baptised : "the blue box". With this device it was possible to get access to the telephone system and call for free.

Some sort of better protection of the systems connected to the Internet was obviously required. On one side was the need for openness, i.e. to be able to connect to any computer that one is entitled to access. On the other side was the need for secured access.

1.1 What are firewall systems ?

A network router is designed to send and receive Internet Protocol (IP) traffic. We can add an Access Control List to open or stop specific IP-addresses or IP-subnets. Then we call this routers with packet filters. This is the simplest form of firewalls, because they can accept or deny traffic in and out of a network. A router operates on the 3 first layers of the OSI stack : physical, link and network.

A more specialised device for just looking at one type of service, is called an application layer firewall or proxy. This device looks thoroughly at one type of application or traffic, e.g. webtraffic at tcp port 80. Now we move up in the OSI stack to layer 4 - 7. Here we have the ability to check the webtraffic for computer viruses and stop traffic trying to access websites that are blacklisted. This is definitely more advanced than a router, but the disadvantage is that we would need a proxy for every application or service the computers are using. In other words this does not scale well.

A modern firewall has the ability to keep track of packets and to know what state the sessions are in. The term stateful inspection denotes this feature. This is necessary to stop sophisticated attacks. An example is an attacker sending packets from the outside to a server, but not replying to the server's responses. The server could run out of bufferspace waiting for communication that will never take place. A firewall can terminate this more quickly and stop the attacker.

A firewall can perform both the function of a router and an application layer gateway. In addition it has the capacity to handle all sorts of traffic and in theory stop all kinds of attacks.

This thesis looks at firewall systems protecting large networks. The vendors of firewall systems classify this as their high end models or enterprise systems.

Smaller networks for approximately 50 people or less can use the vendors' low end systems. A server running Microsoft Windows or Linux has the option to set up an inbuilt firewall, but host based firewalls are not part of the thesis.

We assume some knowledge of computer networks, but (hopefully) explain components and terminology as they appear.

1.2 Structure of the thesis

First we put firewalls in the context of network systems, how they fit in and how to classify them. Then we need to look closer into a typical configuration, to get a better understanding of how components function together.

With several vendors to choose from, a comparison gives an overview.
Feedback from managers of enterprise systems gives confirmation and correction to some hypothesis of firewall systems.

At the end we give some advice on how to better handle a firewall system and suggest how to cope with future threats. The last part is summing up what we found and point out future questions to investigate.

Chapter 2

An overview of a firewall system

The term NGFW (Next Generation Firewall) arose in 2012 due to new functionality; mainly the ability to recognise applications, i.e. level 7 in the OSI model. Combined with integration of users/groups (like Microsoft Active Directory), it created a more powerful control of traffic.

2.1 Overview of a typical firewall system

A minimum configuration for enterprises can typically look like Figure 2.1. A NGFW consists of (3) a management station, (2) a security gateway, (4) a central machine for logging. (1) is internet and (5) is server and pc-network.

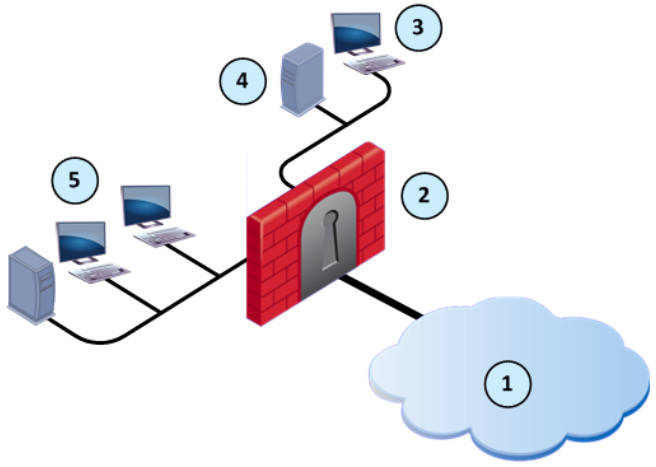


FIGURE 2.1: Enterprise network by courtesy of Check Point

2.2 Features

Traffic inspection is performed by the security gateway. The gateways are set up in a cluster to avoid single point of failure and they do the actual ”work”. The security policy of the company is controlled from the management station, and out of the security policy rules are created and managed. The rules are checked and pushed to the security gateways in a process often termed as ”burning” the rule set. Consolidation of logs and report generation are typically done on the central logging machine. To efficiently retrieve forensic evidence or advanced search results, a good logging system is essential. In a large enterprise the amount of data demands a dedicated server for logs.

2.3 Setup of a new firewall system

This section explains how a minimum configuration might look like. A few rules in the rule-base are more or less standard, because they are common to most organisations. An example is the last rule, called the cleanup rule. Here everything is dropped and often logged. The bigger the organisation is, the longer and more complicated the rule-base will be to accommodate their different needs.

2.3.1 Security gateways

A security review must be based on the security policy of the organisation. This will produce a list of security objectives to adhere to.
Requirements for auditing follows the security policy and the scope can be small or large. For instance, if a security incident needs to be used as evidence in the court of law, correlated date and time is crucial.
One might also certify for ”Information Security Management” or more popularly ”IT Governance” : ISO 27001 [3], where all of these themes are important.

An acceptable trade-off between security and performance for filtering has to be decided. Both logging and inspection of traffic are resource demanding (CPU, memory and disk). Applications need to be detected, otherwise Palo Alto has illustrated in Figure 2.2 that the situation becomes unmanageable. Previously one opened tcp port 80, and the application could tunnel all sorts of traffic inside this port. With application control and classification, one can ”look” inside the session and accept or deny part of the connection.

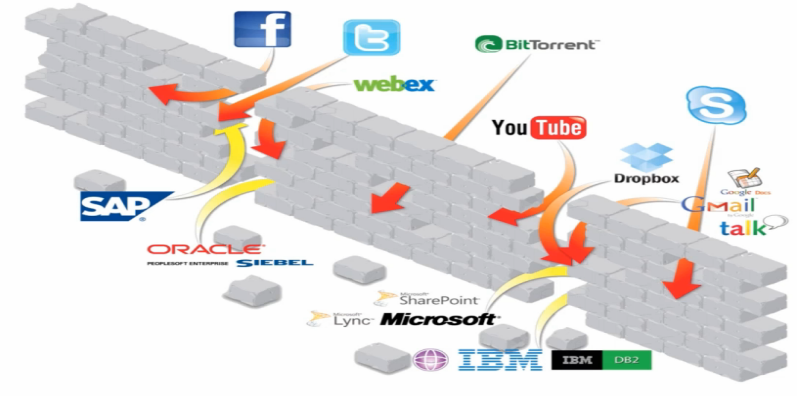


FIGURE 2.2: Classification of applications irrespective of port.

A NGFW is GUI-based, but a Command Line Interface (CLI) for specific features and options can sometimes be necessary.

The gateways perform the actual filtering and packet inspection, and there are 9 different protections or functions (as in Figure 2.3) to configure. Each of these have their own

FIGURE 2.3: Menu of protection options (Check Point).

rule set.

2.3.2 Management

A separate management station is recommended, both for performance and for separation of services.
An enterprise system also would have a machine for analysing and correlating logs into events. From the management station or a dedicated application one can search logs, create reports, and handle anomalies based on findings. An example of an event management menu is in Figure 2.4.

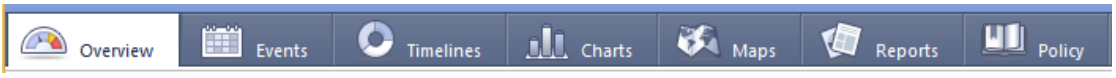


FIGURE 2.4: Event management menu (Check Point).

Categories of business or organisation can have regulations both international (PCI DSS) and national ("Finanstilsynsloven" for Norway). An example taken from PCI DSS version 1.2 requirement 1: *"Install and maintain a firewall configuration to protect cardholder data."* Check Point has an option to buy a compliance-check for the rule

set. This option automatically inserts missing rules so the organisation is correctly configured.

Secure intercommunication for gateways, management and other modules is based on internal certificates. The management station is acting as the Certificate Authority. The firewall system will setup internal (or implied) rules in the rule set for this purpose and place it as the top entries. Implied rules have to be first due to the necessity to communicate internally between the modules in the firewall system. The management and gateway cluster must verify communication, before an update of firewall rules can take place. Likewise the gateway cluster must verify the central log server, before logs are transferred.

2.3.2.1 Problems in management

The increasing number of functions and protections to configure, makes it challenging to choose the correct option. The functions can best be described as layers.

When the rule base becomes larger than 100 rules, it can be difficult to insert a new rule in the right place. How do we know if a rule further down is more restrictive or more permissive ? The firewall software performs checks for this, but can fail to assist if one use many objects or groups in a field. The advantage with putting several objects in a group, is that it becomes more readable and can give a better overview. The disadvantage is that the number of objects can get very high, for instance more than 50. In addition, if groups are used in many rules or in many fields in the rule, it becomes hard to know if the logic is correct. This is due to the number of combination of fields (like 5 in each rule) and rules.

On top of that, we have seen that there can be up to 9 different functions (Figure 2.3) to configure, each with some form of a rule set. Then we have to decide the right amount of logging in the firewall system.

In a big company there might be even different vendors of firewalls, and enforcing a new policy across the whole network often is complicated and takes time to complete.

2.3.3 Additional components

DDOS stands for Distributed Denial of Service and statistics show that attack trends are on the rise [4]. Typically a choice of DDOS-defense is becoming more and more necessary. In a big enterprise one would set up separate appliances for DDOS. An appliance is a specialised, high performance hardware device with limited configuration

ability. The Internet traffic is terminated in the DDOS appliance and is forwarding filtered traffic to the gateways.

IPS (Intrusion Prevention System) are taking care of the most advanced threats. IPS is a protection that can be installed on the gateway. IPS can be extremely resource demanding when performing deep packet inspection, and therefore is has the option to be separated to offload the gateways. An IPS appliance can be connected next to the gateways in parallel.

2.3.4 Cloud security

Various services are moving to the cloud. A cloud is an extremely big and professional datacenter. There can be several such datacenters on each continent. Amazone, Microsoft and other cloud providers are offering virtual computers, backup and storage to a low price. There are also several virtual products to handle the security in these systems. Gartner [5] has estimated that only 5% of the companies using cloud services are including a virtual firewall. There seems to be a scepticism on how to trust a virtual appliance above the hypervisor layer. The hypervisor is placed right on top of the the physical layer, and is a software module simulating the functions of the physical layer. The various operating systems installed on a virtual machine, thinks that they are interacting with the physical layer but instead it is actually the hypervisor. A firewall gateway is inserted on the lowest (physical) layer in the OSI stack. In a virtual environment the hypervisor exists between the firewall and the physical layer. This means the firewall gateway has given away some control and must trust others. A security survey published by Budapest University of Technology and Economics [6] clearly indicates the need for improved tools and countermeasures in virtualized environments. They found several attack vectors to use on the guest machine, the host machine and on the hypervisor layer.

2.4 Outsourcing.

Given the laboursome task of supporting a complete NGFW, some may opt to outsource this chore. A general security company in Norway (Infratek) has chosen this model, by using a security firm (Cumulus IT) responsible for computer and communication security. One might also choose the ISP as responsible for setting up the firewall. This has been suggested by [7].

In the case of cloud computing, one could let the Cloud Service Provider (CSP) take care of the firewall system. Last year this idea was discussed at the IEEE 8th International Conference on Industrial and Information Systems by [8].

Chapter 3

A survey of some firewall research papers

All firewalls have a rule set, defining traffic going into and out of the different networks. A more detailed example (Table 3.1) is described later.

The rule set is the key element to control traffic. We have seen that a firewall system consists of many layers of protection. Efficiency considerations demand the packets to be stopped or passed on with the first match in the rule set.

3.1 The Structural Firewall Query Language and Firewall Decision Diagrams

In 2009 Liu and Gouda published a paper [9] focusing on query processing time for the firewall rule set. First they describe the firewall query by introducing a SQL-like query language : Structural Firewall Query Language (SFQL). They also propose a new query processing algorithm called FDD (Firewall Decision Diagram). Experiments conducted showed the efficiency by using less than 10 milliseconds to process a query over a firewall that has up to 10 000 rules. Here a tree-structure is also used to represent the firewall-rules, and so the processing of queries is quicker than a linear search. A firewall is denoted ”consistent” if no two rules in the firewall conflict and ”inconsistent” otherwise.

Note that a firewall with conflicting rules is logically inconsistent, but semantically consistent because of the first-match. Semantical consistency could also be called operational consistency, because first-match simply means that a packet is accepted or dropped by the first rule that gives a match. It is easier and more efficient to process

queries on a consistent firewall type. Liu and Gouda convert any firewall, consistent or inconsistent to an FDD. The query is done on the FDD, which is always compact and consistent.

In [10], Alex X. Liu extends FDD further. Actually Liu suggests a new design of firewalls. Structured firewall design is aiming to achieve : 1) Correct rule ordering. 2) Thorough consideration of traffic. 3) Keeping the number of rules small. Some other improvements are redundancy rules removal and firewall query processing. Liu claimed in his article that the aims were reachable.

In 2012 Alex X. Liu [11] published an article on firewall policy and the impact of change. With hundreds or thousands of rules, it is no easy task to implement new rules or to modify existing ones. As a consequence, most firewalls on the Internet have policy errors [12] and [13, p.58–65].
Rules can be deleted, inserted, modified, and swapped. A tool takes the current policy and the proposed changes and outputs the impact of the change. Traffic that will be accepted and/or dropped can be verified as intended before the actual change is made, hereby reducing errors and greatly assisting in management. If we look at Table 3.1, we can see an example of change of source IP in the first field in the first line that would result in wrong policy. Now the first rule will accept source IP from the last rule, and this is wrong since the rules have different decisions in the last coloumn.

Src IP	Dest IP	Src Port	Dest Port	Protocol	Decision
10.3.5.∗	172.18. ∗ .∗	∗	∗	*IP*	*Accept*
...	...	...	...	...	...
10.3.5.100	172.18. ∗ .∗	∗	∗	*IP*	*Deny*

TABLE 3.1: Conflicting policy

For an unordered rule set, we define a variable d for packet-fields to be at most 5. This is like the first 5 coloumns in Table 3.1. The number of rules denoted variable N and varies from 1 (ordered rule set) up to N, which is for the worst case of an unordered rule set. Time and space analysis gives a worst case $O(N^d)$, but in practice performs far better. O() means order and is reducing a (complicated) formulae to the component that is growing fastest when the numbers in the variable approaches infinity. The algorithm was tested on both artificial and real-life firewalls, and gave similar results.

3.2 Automatic Correction of Firewall Policy Faults

Chen, Liu, Hwang and Xie [14] formed a group to look into automation of the correction of policy faults. Policy fault is defined as misconfiguration. A faulty firewall policy can evaluate some packets to unexpected decisions. They denote such packets misclassified packets. They proposed an approach to automatically correct all or parts of misclassified packets of a faulty firewall policy. Then they tested this on real-life firewalls and found it to be effective on 3 types of faults :

(1) *Wrong extra rules*. The administrator adds a new rule, but forgets to delete old rules that filter a similar set of packets.

(2) *Wrong decisions*. This type of fault indicate that the decisions of some rules are wrong.

(3) *Wrong order*. This type of fault indicate that the order of rules is wrong.

Clearly it is very useful to correct human introduced misconfigurations in a large rule set.

3.3 Towards a New Design of Firewall

In 2013, Khummanee and Khumseela published a paper [15] focusing on the firewall rule set. The rule structure can be viewed as two parts : <***predicate***> → <***decision***>.
The first part consists of IP-adr, port-number and protocol, and the last part is simply "*Accept*" or "*Deny*" as the rightmost coloumn in Table 3.1. This sounds simple enough, but rules are often in conflict, unnecessarily complex, difficult to understand, improperly aligned, and incorrect due to administrator's ignorance. The authors of [15] propose two improvements : (1) Single Domain Decision (SDD) firewall - a new firewall rule management policy that ensures no matching rules can have both "*Accept*" and "*Deny*" decision. They prove that they can eliminate Ehab S. Al- Shaer [16]'s four anomalies (Shadowing, Correlation, Generalization and Redundancy). To compensate for the extra cost of generating more rules, they solve this by : (2) Binary Tree Firewall (BTF) - a data structure and an algorithm to fast check the firewall rules. To get the rules logically correct, they need to split some rules and as a result the number of rules are increased. How much the number of rules increase is not stated on average or otherwise.

A generic firewall typically has an average verifying time of $O(N^2)$. SDD and BTF improves this to O(log N) in their experiments see Figure 3.2. They measured execution

times for general firewall rules and SDD separatly. The numbers were produced by simulation software written in Java language and run on a PC with Microsoft Windows 7.

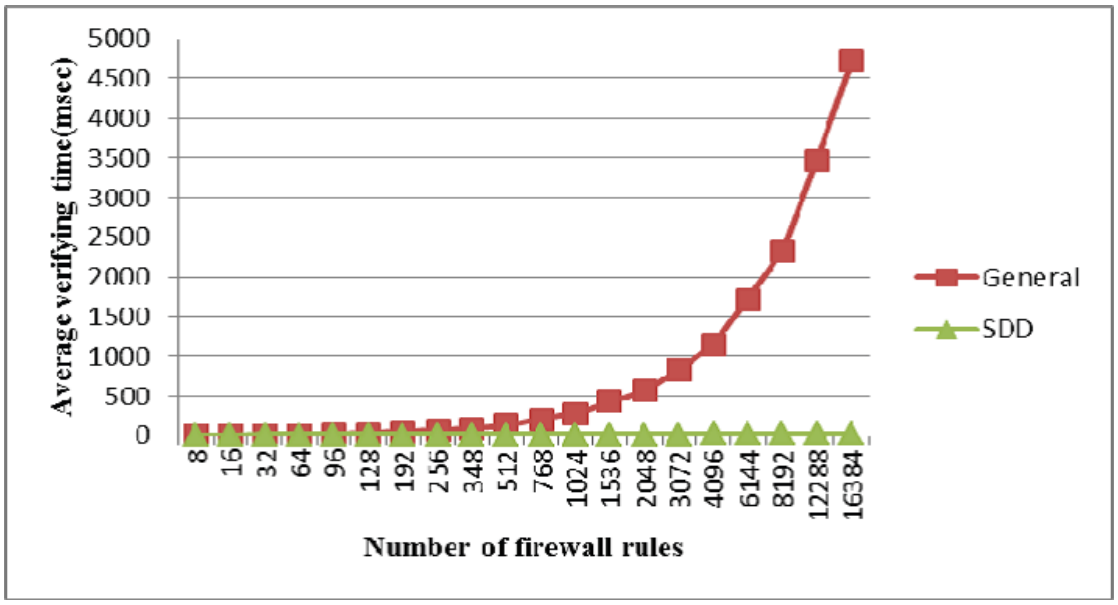


FIGURE 3.2: Average verifying time versus number of rules

Commentary : The improvements look impressive, but it is not noticeable if the number of rules is less than 1000. Only big organisations with a complicated and long rule set will gain on average verifying time.

An improvement of verifying time from speed $O(N^2)$ to O(log N) is a simplification. Most of the times we have a constant involved, and the order O comes into play when the number (N or rules) goes to infinity.

We also have to keep in mind that the results are from simulation, and not from a real world firewall system.

Chapter 4

Modelling firewalls as part of a CAS

4.1 What is a CAS ?

A CAS is a Complex Adaptive System. The brain, power grids, ecosystems and the internet can all be represented as large complex networks. A complex system has many interactions between its different parts causing emergent properties. Emergence denotes global behavior caused by interacting local behavior generated by a large number of elements. The complexity can be reduced by removing interactions. Dynamical processes are described by Barrat [17].

If we look at the development of the number of protections and functions a firewall can offer, we see in Figure 4.1 that it can be a challenge to manage all of this.

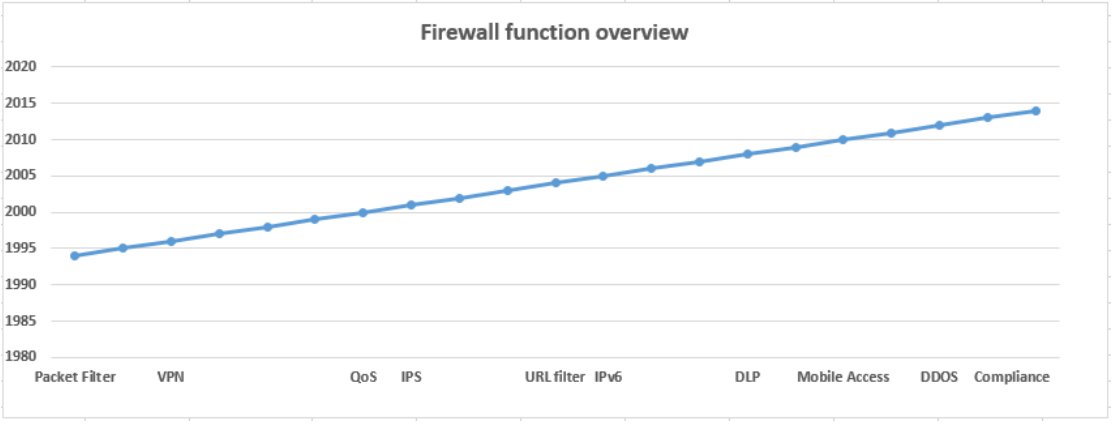


FIGURE 4.1: Development of functions over time.

Protection is when a firewall can defend against a threat, for instance stopping access to hacking-sites by the URL filter. A Next Generation Firewall (NGFW) is not a CAS, but a complicated system. It is possible to foresee the consequences of disabling logging or the VPN-feature. The NGFW operates in a CAS environment with people, Internet and so on.

4.2 How does malware spread on the Internet ?

Human infectious diseases and epidemiology may serve as analogies to malware spreading. Malware is an abbreviation for malicious software and is a common name for evil software. To illustrate a very simplistic example, we can set up a small differential equation. Let $I(t)$ be the number of infections at time t and $dI(t)/dt$ be the epidemic rate. A homogeneous model implies exponential growth from initial condition $I(0) = I_0$ and β is the rate of contact to other hosts :

$I(t) = I_0^{\beta t}$

In practice the computers in many networks are connected in scale-free networks like a business network or the Internet. Scale-free network is were the vertices (like computers) have a small number of edges but a few (like the firewalls) have a large number of edges. Edges in this topology can be seen as connections. A malware is mostly targeted to the same type (i.e. homogeneous) of computers (e.g. Microsoft Windows XP, Apple OS X) or software (e.g. Java version 6, Adobe Reader 9). The spreading will be faster on a scale-free network compared to a random network [18, p.258]. We can set up a differential equation that fits more accurately. Pasor-Satorras and Vespignani [19] suggest a more sophisticated equation, but the simple equation is illustrating the principle.

The ultimate goal of the mathematics behind this theory is to bring insights into how defenses can be built to limit the spreading of malware. Thomas M. Chen and Nasir Jamil [20] demonstrate a modified community of households (COH) model, that dampen a worm outbreak by limiting bandwidth.

To simulate the spread of computer virus, one can use the software : ”Netlogo” as a visual and dynamic demonstration.

4.3 How to limit the effect of malware.

Immunisation of hubs on a network is described as quite effective by Anderson [21], R. Pastor-Satorras and A. Vespignani [22] and Barrat [17]. A hub is a vertice in a graph

or network that has many edges or connections. By concentrating on the hubs, Hole [23] confirmed this to be the best option for immunisation in simulation to halt malware from spreading. Domain Name Search (DNS) servers and routers with Border Gateway Protocol (BGP) represent hubs on the Internet. Without these technologies there will be very limited connection. Firewalls also represent hubs in the internet context, because they have many connections in and out of networks. With the brand of firewall with the largest marketshare, one has a type of monoculture or homogeneous network.

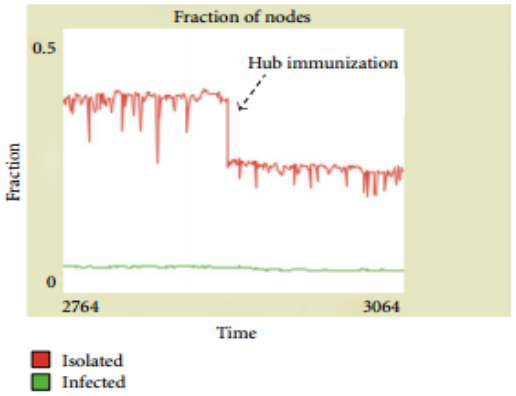


FIGURE 4.2: Instantaneous fractions of isolated nodes (red line) and infected nodes (green line) in a diverse network.

In Figure 4.2 we see a model of a network with infections, taken from [23]. If the largest hub is immunised, meaning made permanently resistant to virus attacks, then the instantaneous fraction of isolated nodes drops significantly.

Firewalls are hard to infect, but a fresh vulnerability was nevertheless discovered. A Unix Bash vulnerability (covered under CVE-2014-7169 named Shellshock) was publicly disclosed on 24th of September 2014, and had the possibility to infect firewalls built on Linux/Unix-code. The Unix Bash shell process certain requests, and vulnerable versions of Bash can execute arbitrary commands. A malware can exploit unpatched Bash shells and gain unauthorized access to the system. To test if a system was vulnerable, one could type this command :

env x='() :;; echo vulnerable' bash -c "echo this is a test"

If the word **vulnerable** was displayed, your system was definitely affected. By 25th September 2014, Andy Greenberg [24] reported that botnets or robot networks based on compromised computers were being used by attackers. Two of the biggest firewall vendors (Check Point and Palo Alto) had to inform their customers and deliver a patch quickly.

By controlling traffic flow, a firewall's ability to stop malware spread is one form of immunisation. A method is to blacklist callhome URLs of Trojans. A Trojan is a

malware program and often part of a botnet. That means a PC can be infected by a Trojan, but the Trojan will be stopped when trying to communicate back to command-and-control (C&C) server. The firewall manager will get a report on all PC's being infected by such Trojans, and from this one can take action.

4.4 Pitfalls in management operations

To immunise the firewalls sounds simple enough. The vendors highly recommend to always install the latest software version of their product. The advantage is that then we will have the most updated features and fixed software-bugs. The disadvantage is that there will inevitably be introduced new errors in the software. A simple metric like Source Line of Code (SLOC) and history confirms this. SLOC and number of defects are strongly correlated [25]. A rate of one bug per 1000 lines of code is a conservative estimate. Ten to fifteen percent of security patches introduce new vulnerabilities, according to [25].

Every new version of firewall software has a list of errors fixed. The following documentation [26] from : "Check Point R77.20 Resolved Issues" is quite common.

Bugs in the firewall software have caused serious disruptions. A national example from Norway 12th of June 2014 when most people had problems using their credit- and debet-cards. This was due to a software-update of a Check Point cluster at Evry AS [27].

Chapter 5

Comparing different vendors

Greg Young, Adam Hils and Jeremy D'Hoinne have written the newest Gartner report [5] from 15th of April 2014 and it gives a good overview of the situation in the firewall market. Gartner aims to help companies considering to buy or switch firewall system. The report studies purpose-built appliances for enterprise corporate networks. Appliances must be able to support single or multiple firewall deployments and corresponding capable management and reporting consoles. The report takes into account the marked share, but also other factors like the ability to launch products according to customer needs and the company's vision. Gartner has classified the different vendors in 4 quadrants in Figure 5.1, and defined the upper right quadrant to be the most favorable.

5.1 Vendors.

There are several vendors of firewalls, offering products from small systems to large systems. Free products like : IPtabels, IPCop, M0n0wall for Linux and Windows Firewall, ZoneAlarm for Microsoft Windows are aimed at mostly protecting a host.
We focus on commercial systems that offer the most complete feature-set for networks. Vendors here are : Check Point Software Technologies, Palo Alto Networks, Fortinet, Juniper Networks, Cisco and a handful more. We concentrate on the two names in the leading quadrant and Fortinet from the challenging quadrant taken from [5] see Figure 5.1

FIGURE 5.1: Gartner : Magic Quadrant for Enterprise Network Firewalls

5.2 3 largest systems of NGFW

Check Point, Palo Alto and Fortinet are dominant players in the field. Technical capabilities of appliances will vary from year to year, so the following comparison is valid for 2014.

5.3 Strengths and weaknesses.

5.3.1 Check Point

Check Point has good and helpful statistics about unused rules and objects. They have the most comprehensive list of products and scale well. The software can be installed on a general (prelisted) hw-platform, on appliances, and on virtualized environments. The offer for managed security is new in the market, as none of their competitors are selling a similar service.

They have some open APIs (Application Programmer Interface), and can therefore integrate with third party tools like Splunk. Splunk is a software program capable of merging log-data from different systems and offers detailed search-options. In fact, 350 partners can integrate products with Check Point. An updated database of applications gives better control of traffic. The Check Point management console is ranked highest by customers with a large number of firewalls. A service provider can manage different customers from the same console. Check Point serves almost every Fortune 500 company and has a huge user base [28].

Check Point has subdivided some of the protections and functions (called blades) and management options (full Eventview and Reports). This is often bundled in a confusing way and priced separately. High price causes some customers to consider replacement, according to Gartner. Other competitors have included what Check Point sells separately as blades.

5.3.2 Palo Alto Networks

Palo Alto has a novel approach to firewalls. They focus on applications and divide the network in zones. With full integration to the user database (like Microsoft Active Directory), this gives a comprehensive control of traffic.

From the user perspective this is quite intuitive and straightforward. Reports are included for no extra license. By grouping applications by category, an automatic database update provides dynamic filtering for new applications. One can fine-tune traffic inside for instance Facebook, by allowing read for all but write updates only for the Marketing department.

Appliances run on specialised hardware that process packets in parallel. Palo Alto was the first vendor with application control, and this is one of the reasons for them being the second biggest in the market. Their IPS is also ranked high by customers. The management console is the second most popular and their pricing structure is simple.

Palo Alto has a small third party product support ecosystem. They lack an entry-level platform for small branches of a distributed enterprise. The clients would like to see better log handling and management console for big enterprises, according to Gartner.

5.3.3 Fortinet

Fortinet offers appliances with purpose built ASICs (Application-specific integrated circuit). Advanced Threat Protection can be added and gives a sandbox-environment to

detect unknown threats. This threat information can be shared with FortiGuard labs to benefit all customers. Fortinet was founded in year 2000, and has a good marketshare in the small and midsize business (SMB)-sector with Unified Threat Management (UTM). UTM are appliances with the most common protections integrated. This product cover the basic need for most smaller businesses. Now Fortinet is aiming for the bigger enterprise market. Fortinet claims they have a large research and development team and uses it to go quickly to market with new features. Fortinet offers a low price and high port density in their appliances, compared to Check Point and Palo Alto.

Fortinet's weak point is searching in logs if you have gigabytes of data. With no separate tool for searching, a slow and inflexible user experience appears. The management console is not suited for environments with many different firewalls and configurations. The enterprise sector demands other and more advanced features and management compared to the SMB-sector. Comparisons summarized in Table 5.2, market share of security appliance from [29]. Cisco has the biggest marked share (18.4%), but many small vendors togehter sum up almost 50 %.

Criteria	*CheckPoint*	*PaloAlto*	*Fortinet*
Appliance	*X*	*X*	*X*
VM alternative to Amazone EC2 fw	*X*	*X*	*X*
Management console	*excellent*	*good*	*average*
Advanced search in logs	*X*	*X*	
Application database	*X*	*X*	
Performance	*high*	*high*	*high*
Market share (%)	12.9	7.1	7.3
Cost	*high*	*high*	*low*

TABLE 5.2: Comparison of three vendors of NGFW.

Performance of gateway models from midrange to high end in Table 5.3 :

Capacity	*CheckPoint*	*PaloAlto*	*Fortinet*
Firewall throughput	50 - 400 Gbps	20 - 120 Gbps	40 - 560 Gbps
Maximum sessions	10 - 210 Millions	4 - 24 Millions	10 - 280 Millions

TABLE 5.3: Comparison of gateway specifications from three vendors of NGFW

Firewall throughput is theoretical and tested using stateless protocols and big packets. If web-browsing were to be used, this would consist of smaller packets and the maximum throughput value would drop. Maximum sessions or connections are the average rate per second. This is also in the most favourable situations. You would not achieve so

many sessions, if for instance each session was passing 10 Gigabit per second of data traffic. The two measures are in conflict.

In Table 5.3 it looks like Palo Alto have much lower performance, but they measure always with all protections on. Palo Alto process packets in parallel, and therefore their performance drops in small steps when one turns on protections. After a protection is turned on, the performance remains stable. Palo Alto claims that their competitors include and process protections in serial, and so their competitors performance decreases linearly for every protection turned on. The Table 5.3 should have been with the same number of protections turned on, in order to be able to compare performance.

The numbers from Palo Alto are also in favourable situations, but seems more realistic due to the appliances' parallel construction.

NSS Labs [30] made an independent performance rating in 2013 Figure 5.4 of different firewall appliances. Here they for instance found that Fortinet performed less than 50% of what Fortinet publish as throughput.

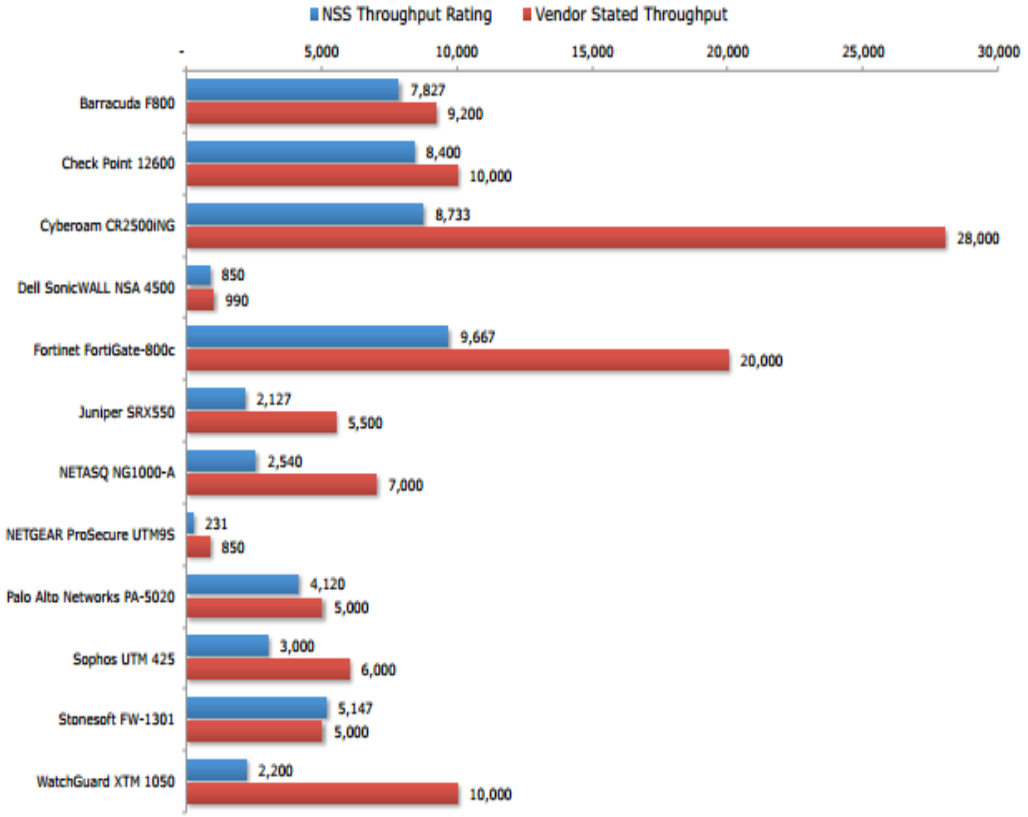


FIGURE 5.4: Vendor claimed vs. NSS rated throughput in Mbps

Chapter 6

Questionnaire

A questionnaire was sent out to some bigger institutions in Norway. The response was as expected (21 out of about 200). In general, the response to a questionnaire will vary greatly. In this case, most common reasons for not filling in the questionnaire were that they are not using firewalls (like universities/colleges in Norway), they could not answer (company policy) and some did not have time.

We will be careful with drawing firm conclusions, but instead suggest trends. I have also had meetings with Atea, which provides firewall sale and support to customers in Scandinavia. Atea claimed that more and more SMB drop internal management of the firewall. Instead SMB buy support from a professional partner.

6.1 Purpose of survey

We wanted to find out how management is performed, problems with today's solution and see if some areas could be improved. Was there a big difference between small and big companies ? Was the number of years of experience by the persons operating the firewall system, influencing the average network downtime caused by the firewall ? What was the distribution of brands of firewalls ? Was there a correlation between a large number of rules and frequent downtime ?

6.2 Common problems in management

Most people (17) could get statistics on rules not in use, but under half (8) actually did delete rules not used.

6 institutions reported that changes in firewall never had caused downtime for their users. For the others a shorter or longer break once or twice a year was common.

Only one company considered using OpenDNS, described in Ch. 7. 2 companies (one SMB and one big) are evaluating the option for outsourcing, but most big companies do not consider outsourcing. Two of the big companies used 3rd party software as extra aid in management. Big companies also had the biggest number of rules and users, as expected. The distribution of brands of firewalls ended up with Check Point (13), Cisco (3) and the rest had other brands. Unfortunately none reported using Palo Alto or Fortinet.

It seems that average downtime was rare (less than once a year) when the firewall administrators had more than 10 years of experience . 6 out of 21 had not caused unplanned downtime when managing the firewall. This is impressive, but such a central component is very sensitive to failure. That is why the gateways are set up in cluster, so one gateway can be taken out while not disturbing the data communication for users. Many incidents can cause the cluster to stop : power outage, memory leakage, infrastructure fail in the network, software bugs, errors in the rule set of the firewall to name a few.
We could not find a correlation between a large number of rules and frequent downtime.

6.3 What we found could be improved

Many people (14) wanted a check of their rule-set, but only 2 used a 3rd party software as aid. The software from AlgoSec, FireMon and Tufin could be too expensive, or organisations do not have time to invest in it. 18 out of 21 had 100 or more rules, so a 3rd part software could probably be an option well worth to contemplate. A computer is generally better than a human at checking and sorting large amount of data like a large firewall rule set.

Less than a third (6) are regularly auditing their firewall. The benefits of hiring a company for audit could be several. One would get an evaluation of the current setup. A check to see if regulatory compliance requirements are followed. Identification of possible shortfalls and deficits. A consideration of alternative solutions and immediate and long term recommendations. The downside is of course the time and cost of hiring external auditors.

Chapter 7

Suggestions for better management of firewall systems

In this thesis, we have stated some issues with firewall systems. In this chapter we suggest some solutions.

7.1 Utilise inbuilt tools

The vendors have created some tools that they claim will greatly improve manageability. We take a brief look at some of the options.

7.1.1 Remove unused rules

To improve readability and efficiency, as few rules as possible is a clear goal.
Check Point's Management Console (from software version R77.0) displays expired rules, rules not active (that is disabled), and unused rules (that is, with zero hits) as seen in Figure 7.1. All of these categories can be deleted, improving both efficiency and readability. About half of the respondents in the questionnaire do not delete unused rules. If the rule set is growing more than 100 rules, then one has to start considering deleting unused rules.

When a report-module is included, it will often come with a report for analysis of the rule set. Even if no changes are recommended, it can give helpful statistics about the situation and aid in improving the rule set.

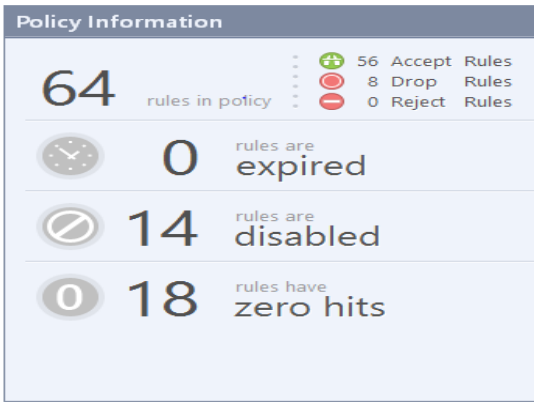


FIGURE 7.1: Policy overview of rules (Check Point)

7.1.2 Remove duplicate objects and unused objects

Again, to ease the management, we define as few objects as possible. An object is typically a host (IP-address), a net (several consecutive IP-addresses), users, TCP- or UDP-port number or a group of any of these. When a rule is deleted, one has to remember to delete the objects involved if they are not used elsewhere. 4 people in the questionnaire do not know how many objects they have defined in one group or one field.

7.2 Routines

To be able to handle a firewall system efficiently, good routines are essential.
The software needs to be regularly upgraded and patched. Unless one performs this, one will miss bug fixes, stability and improvements. Memory leaks in the firewall software can easily halt the gateway from handling traffic. The Shellshock (Ch. 3.3) is another example of a patch that would require a quick install due to security. Half of the representatives in the questionnaire are not routinely looking through rules and objects in their firewall system.

A regular audit of the firewall system, will be a good reminder of regular check and walk-through. With 6 out of 21 respondents telling they do have audits, here is a potential for improvements.

7.3 External tools

In Chapter 3 we introduced some research done on firewall systems. None of this is available as products or included by the firewall vendors.

There are commercial software tools on the market that can assist in evaluating a current configuration of a NGFW.

AlgoSec, FireMon and Tufin are examples of independent 3rd party tools for checking and simplifying the rule set. These tools have a broader function and a common name is : firewall policy management (FPM). Big companies use FPM, because their solutions are comparatively larger than SMB companies. From the questionnaire only the big organisations (2) used FPM.

7.4 Managed Security

Security-aware businesses, like banks for instance, are hiring in 3rd party companies specialising in security. We also note that Check Point is offering managed security that is checking IPS, logs and so on 24/7 for known and new threats. The service is called : "ThreatCloud Managed Security Service". Check Point together with partners are continuously harvesting logs from several nodes around the world. By examining and correlating this huge amount of information, they are able to extract patterns not easily picked up by one person or one single company. The service "Threatcloud" can be purchased separately, but is without the log-analysis and management.

Experts focusing on a narrow field and spending time to verify possible threats, are doing a much better job compared to an individual person/team in a average company. Both time and people with in-depth knowledge are mostly what organisations are missing. Only 2 companies in the questionnaire are currently considering outsourcing of the firewall services.

7.5 DNS

DNS is an acronym for Domain Name System, and is the way computers resolve URLs into IP-addresses. With the right name but the incorrect IP, your traffic will be redirected to the wrong server. DNS is vulnerable to incorrect entries, but can also be used as a filter. That is, only legitimate traffic would pass in and out of a company's network because access to hacking URLs would be denied.

7.5.1 OpenDNS and Umbrella

One might ask how OpenDNS can actually benefit in managing threats ?
OpenDNS is a company offering secure DNS as an external service. As stated : to be

able to navigate easily on the Internet, everybody uses DNS. This goes both ways : to be able to get out of your own network and for others to reach services on your network. If all computers in your organisation are forced to use dns-servers from OpenDNS, no pc will get to blacklisted URLs, according to OpenDNS.

Likewise, known hacker-sites / spam-sites will be denied access from Internet to our DMZ. DMZ is an acronym for DeMilitarized Zone, and describe a separate part of the network behind a firewall and reachable from the Internet. Umbrella is a commercial company that is offering this functionality. They keep track of huge amounts of data and are analysing IP-addresses (URLs) continuously. ”Good” and ”Bad” sites on Internet can change, so it is impossible for one person or small team to always be updated on this. With the right tools and specialised knowledge this is nevertheless now possible.

Umbrella Security Labs have published a case study [31] where they could monitor a botnet by using recursive and passive DNS from their own openDNS database. Their point is that one need to examine the DNS-traffic in order to stop the bots from communicating. Since 2011 the bots have refined their communication setup, so it is no longer just a central command-and-control (C&C) server controlling the botnet. This is explained in Figure 7.2 from Umbrella :

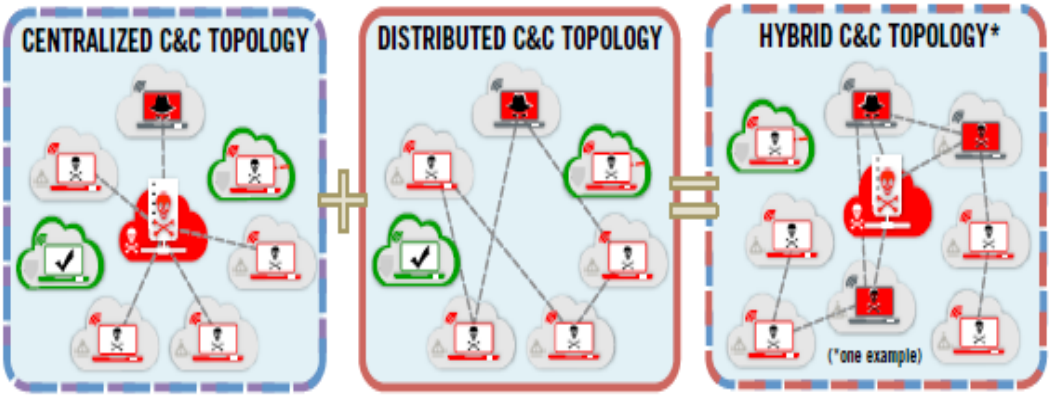


FIGURE 7.2: Hybrid C&C topology

The firewall vendors will have to adjust their defense to tackle this new bot topology.

7.5.2 Infoblox

The vendor Infoblox originally started with appliance-solutions for internal DNS and DHCP-services in large organizations. Now they have expanded their products to include a secure DNS : ”The Infoblox Secure DNS Solution”. Infoblox is performing the same

functions as OpenDNS, and is a competitor on the market. They also offer a complete package and a recommendation on how to set up the DNS-service as in Figure 7.3.

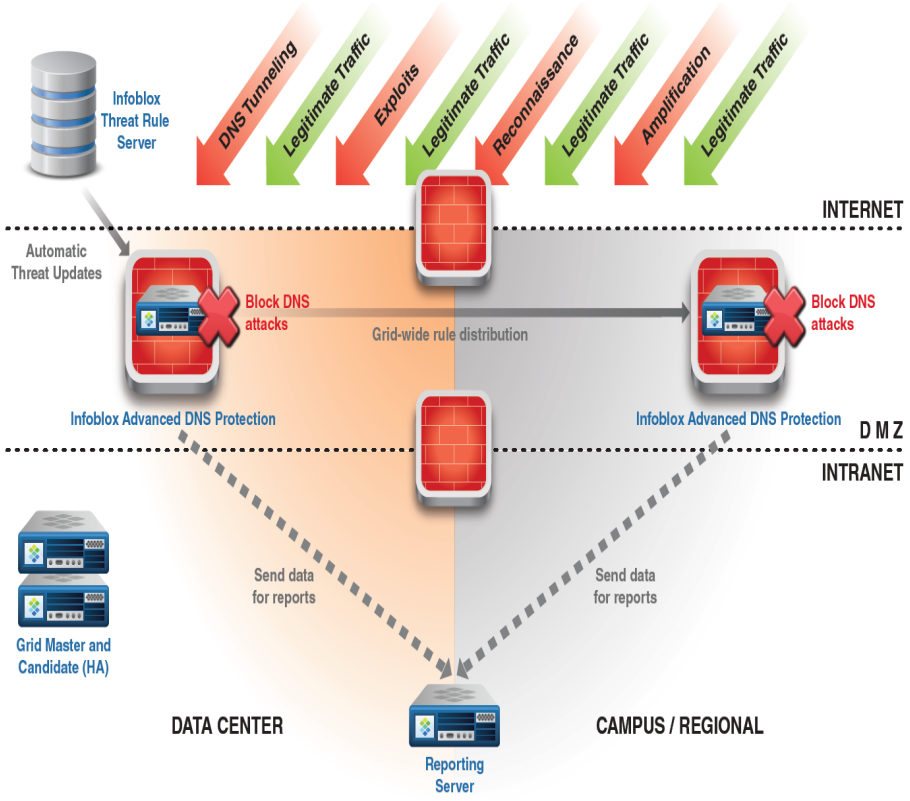


FIGURE 7.3: Infoblox setup.

According to Arbor Networks ninth annual "Worldwide Infrastructure Security Report", just over one-third of respondents have experienced customer-impacting DDoS attacks on their DNS infrastructure during November 2012 - October 2013. An increase from one-quarter last year.

The disadvantage with both Umbrella and Infoblox is that they are reactive services, like antivirus. We are able to blacklist the address only when a threat from an IP-address or URL is discovered. One company answered that they considered to use OpenDNS and 15 companies answered that they would not consider this service.

There could also be privacy issues with OpenDNS. OpenDNS is able to harvest and store all the DNS and/or URL requests from a company. Potentially this can reveal secrets a competing company are willing to buy.

Chapter 8

Conclusion and summary

8.1 Summary

We have learned that it is no trivial task to manage a firewall system. For an inexperienced person, there is a lot to take in and one has to continuously be updated on new threats and defense mechanisms. Next Generation Firewall gives you great control of the traffic-flow, but also adds extra time to manage this. SMB companies are often not willing to spend the time and money on internal people for firewall management. Outsourcing is then a viable option.

8.2 Conclusions

From the questionnaire, it seems to be no immediate need for 3rd party tools, even when the number of rules could be up to 1000. Most organisations would like to correct their rule set for logical errors, so this is a contradiction. 3rd party tools could be very helpful, if one is to correct a big rule set.

Most organisations also seem confident with their firewall system, maybe because they have little downtime and almost everybody had more than 5 years experience with firewall management.

The majority of respondents would not consider the use of OpenDNS, and that means their firewall is performing ok. It could also mean that the solution from OpenDNS has to prove its value and information about the product needs better marketing.

8.3 Extensions of thesis work

Research is helical [32, p.6–7] like a spiral. More than often new follow-up questions and studies arise. This is also the case here.

A broader interview-base or worldwide questionnaire would give firmer evidence of findings. We could also correlate the answers to find differences between small and large organisations.

With added questions about improvements, more suggestions about solutions in firewall management could be expected to appear.

What is the upper limit of firewall rules one can have implemented, before it gets unmanageable ? What is the highest number of objects in a field or recommended combination of objects and fields ? Is the only solution to purchase products from Tufin, AlgoSec or FireMon ?

OpenDNS and the service from Umbrella/Infoblox are not tested, so it would be very interesting to verify if they can give improved protection. One setup could be to have two identical firewall systems, one with Umbrella/Infoblox and one without. Then test computers behind the firewalls and see if the number of malware detected is the same.

Appendix A

Copy of questionnaire

This was the questionnaire sent out to 200 companies.

Firewall

A short questionnaire about firewalls and issues in management.

*Må fylles ut

How many users are there in your organisation ? *
Helping in getting an overview.

- ◯ Less than 100
- ◯ 100 - 999
- ◯ 1000 - 5000
- ◯ More than 5000

How many firewall clusters are there deployed ? *

- ◯ 1
- ◯ 2
- ◯ 3 or more

How many persons are managing the firewall solution ? *

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4 or more

How many rules are configured in the rulebase ? *
Standard policy rules, (not IPS etc), but include rules disabled.

- ◯ Less than 50
- ◯ 50 - 99
- ◯ 100 - 499
- ◯ 500 - 999
- ◯ More than 999

How many groups of rules are configured ?
Groups are used to simplify the overview of the rulebase.

- ◯ Not in use
- ◯ 2 - 9
- ◯ 10 - 29
- ◯ 30 - 49
- ◯ 50 - 99
- ◯ More than 99

What is the largest number of objects defined in one group ? *
Objects meaning hosts, networks.

- ◯ Less than 8
- ◯ 8 - 15
- ◯ 16 - 39
- ◯ 40 - 99
- ◯ More than 99
- ◯ Don't know

What is the largest number of objects defined in one field ? *
Field meaning : source, destination, service etc. Count objects in groups (if groups used).

- ◯ Less than 8
- ◯ 8 - 12
- ◯ 13 -19
- ◯ 20 - 49
- ◯ 50 - 99
- ◯ More than 99

Can you get statistics on rules not in use ? *

- ◯ Yes
- ◯ No

Do you delete rules not in use or disabled ? *

- ◯ Yes
- ◯ No

If No, why are rules not deleted ?
Both rules that are not used (eg last 2 months) and disabled rules.

- ◯ Have not enough time
- ◯ Too complicated, uncertain of consequences later
- ◯ The rule might be used again in the future
- ◯ Delete only unused rules after 6 - 12 months
- ◯ A combination of 2 or more options
- ◯ Other reasons not mentioned

Is there a need to correct logical errors in the rulesbase ? *
If software existed that could find and correct errors in a large rulesbase, eg more than 100 rules ?

- ◯ Yes
- ◯ No

Do you currently use 3rd party software to analyse and optimise the rulesbase ? *
Examples : AlgoSec, FireMon and Tufin

- ◯ Yes
- ◯ No

Do you routinely look through rules and objects in the firewall ? *
This includes all protections like IPS and so on.

- ◯ Yes
- ◯ No

Have changes/maintenace work resulted in down-time for users ? *
Downtime that was not planned.

- ◯ Yes
- ◯ No

If Yes, how often does this happen on average ?
Downtime more than 5 minutes.

- ◯ Less than once a year
- ◯ Once a year

- ◯ Once every 6 months
- ◯ More than once every month

Is there performed an audit of the firewall solution ? *
Audit by 3rd party or other department at some interval

- ◯ Yes
- ◯ No

Do you consider the use of OpenDNS/Umbrella as a mean to offload the firewall ?

- ◯ We use this already
- ◯ Yes
- ◯ Never heard of
- ◯ No

Do you consider outsourcing of the firewall solution ? *

- ◯ Yes
- ◯ No

If Yes, what factors do you include ?

- ☐ Management is increasingly demanding
- ☐ Costly to have experienced people inhouse
- ☐ Management of firewall not part of core business
- ☐ Availability 24/7
- ☐ Other

How many years have you worked with firewalls ?

- ◯ Less than a year
- ◯ 1 - 4 years
- ◯ 5 - 10 years
- ◯ More than 10 years

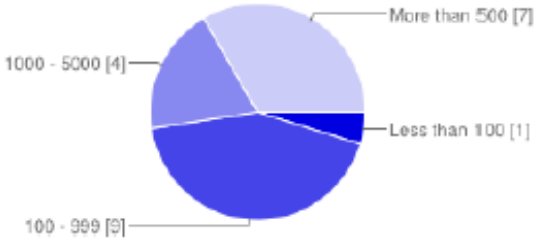
What vendor do you have ? *
If more than 1, choose the most important.

- ◯ Palo Alto
- ◯ Fortinet
- ◯ Check Point
- ◯ Cisco
- ◯ Other

Appendix B

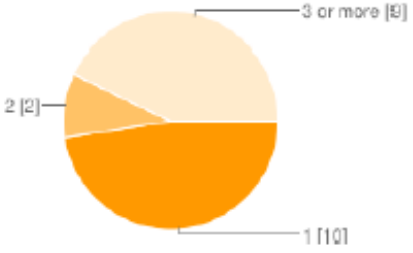
Summary of answers to questionnaire

How many users are there in your organisation ?



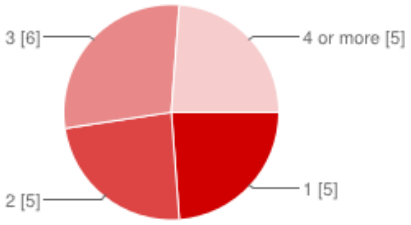
Less than 100	**1**	5 %
100 - 999	**9**	43 %
1000 - 5000	**4**	19 %
More than 5000	**7**	33 %

How many firewall clusters are there deployed ?



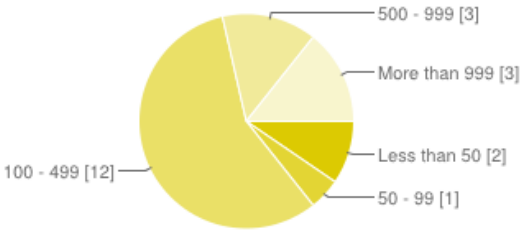
1	**10**	48 %
2	**2**	10 %
3 or more	**9**	43 %

How many persons are managing the firewall solution ?



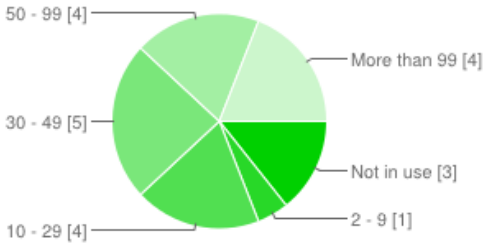
1	**5**	24 %
2	**5**	24 %
3	**6**	29 %
4 or more	**5**	24 %

How many rules are configured in the rulebase ?



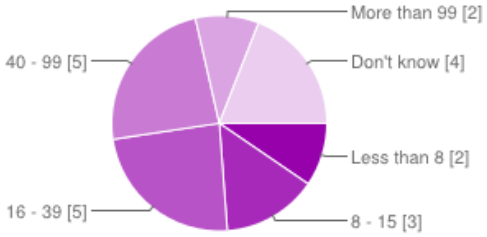
Less than 50	**2**	10 %
50 - 99	**1**	5 %
100 - 499	**12**	57 %
500 - 999	**3**	14 %
More than 999	**3**	14 %

How many groups of rules are configured ?



Not in use	**3**	14 %
2 - 9	**1**	5 %
10 - 29	**4**	19 %
30 - 49	**5**	24 %
50 - 99	**4**	19 %
More than 99	**4**	19 %

What is the largest number of objects defined in one group ?

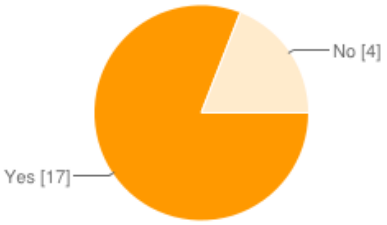


Less than 8	**2**	10 %
8 - 15	**3**	14 %
16 - 39	**5**	24 %
40 - 99	**5**	24 %
More than 99	**2**	10 %
Don't know	**4**	19 %

What is the largest number of objects defined in one field ?

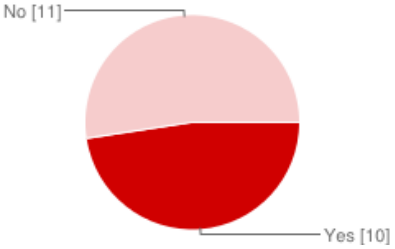
Less than 8	**1**	5 %
8 - 12	**1**	5 %
13 -19	**4**	19 %
20 - 49	**6**	29 %
50 - 99	**4**	19 %
More than 99	**1**	5 %
Don't know	**4**	19 %

Can you get statistics on rules not in use ?



Yes	**17**	81 %
No	**4**	19 %

Do you delete rules not in use or disabled ?

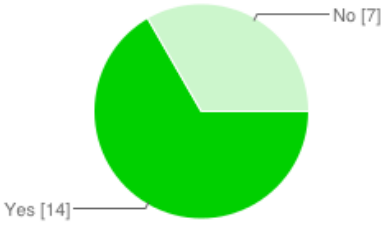


Yes	**10**	48 %
No	**11**	52 %

If No, why are rules not deleted ?

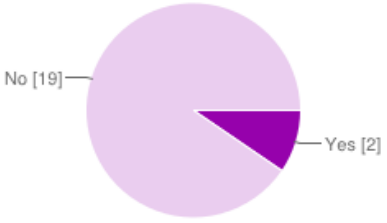
Have not enough time	**0**	0 %
Too complicated, uncertain of consequences later	**2**	10 %
The rule might be used again in the future	**2**	10 %
Delete only unused rules after 6 - 12 months	**4**	19 %
A combination of 2 or more options	**2**	10 %
Other reasons not mentioned	**3**	14 %

Is there a need to correct logical errors in the rulesbase ?



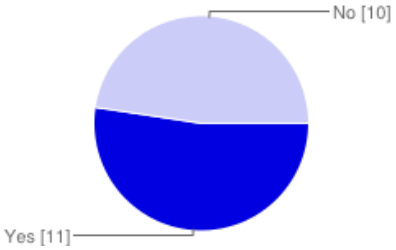
Yes	**14**	67 %
No	**7**	33 %

Do you currently use 3rd party software to analyse and optimise the rulesbase ?



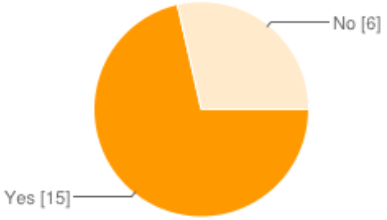
Yes	**2**	10 %
No	**19**	90 %

Do you routinely look through rules and objects in the firewall ?



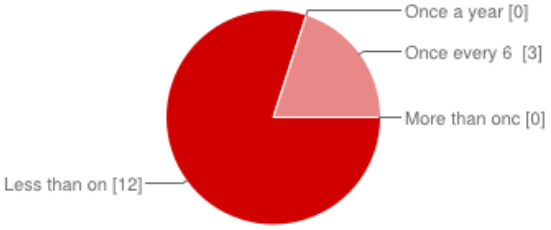
Yes	**11**	52 %
No	**10**	48 %

Have changes/maintenace work resulted in down-time for users ?



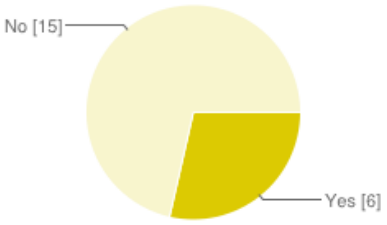
Yes	**15**	71 %
No	**6**	29 %

If Yes, how often does this happen on average ?



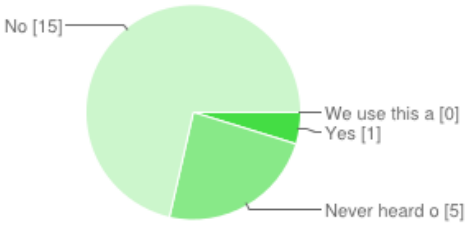
Less than once a year	**12**	57 %
Once a year	**0**	0 %
Once every 6 months	**3**	14 %
More than once every month	**0**	0 %

Is there performed an audit of the firewall solution ?



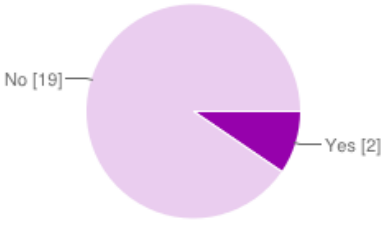
Yes	**6**	29 %
No	**15**	71 %

Do you consider the use of OpenDNS/Umbrella as a mean to offload the firewall ?



We use this already	**0**	0 %
Yes	**1**	5 %
Never heard of	**5**	24 %
No	**15**	71 %

Do you consider outsourcing of the firewall solution ?

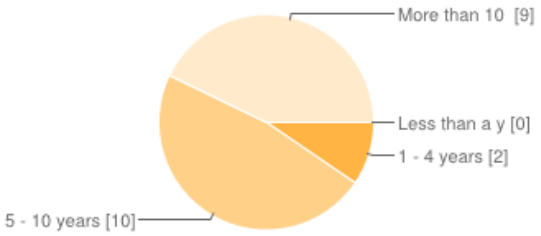


Yes	**2**	10 %
No	**19**	90 %

If Yes, what factors do you include ?

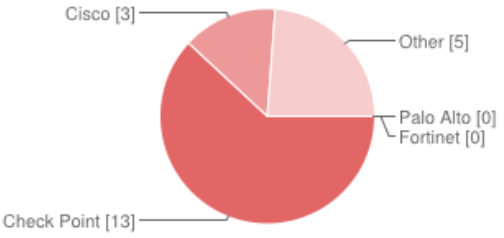
Management is increasingly demanding	**2**	10 %
Costly to have experienced people inhouse	**0**	0 %
Management of firewall not part of core business	**1**	5 %
Availability 24/7	**0**	0 %
Other	**0**	0 %

How many years have you worked with firewalls ?



Less than a year	**0**	0 %
1 - 4 years	**2**	10 %
5 - 10 years	**10**	48 %
More than 10 years	**9**	43 %

What vendor do you have ?



Palo Alto	**0**	0 %
Fortinet	**0**	0 %
Check Point	**13**	62 %
Cisco	**3**	14 %
Other	**5**	24 %

Bibliography

[1] Thomas Lightoler. *The gentlemans and farmer's architect.* R. Sayer, London, UK, 1764.

[2] Walter Isaacson. *Steve Jobs.* Cappelen Damm, 2011. ISBN 978-82-02-36987-3.

[3] 2013. URL `http://www.iso.org/iso/home/standards/management-standards/iso27001.html`.

[4] 2014. URL `http://www.stateoftheinternet.com/security-cybersecurity-attack-trends-and-statistics.html`.

[5] 15 April 2014. URL `https://www.gartner.com/doc/2709919/magic-quadrant-enterprise-network-firewalls`.

[6] Gabor Pek, Levente Buttyan, and Boldizsar Bencsath. A Survey of Security Issues in Hardware Virtualization. *ACM Computing Surveys (CSUR)*, 45, June 2013.

[7] A.R. Khakpour and A.X. Liu. First step toward cloud-based firewalling. In *Reliable Distributed Systems (SRDS), 2012 IEEE 31st Symposium on*, pages 41–50, Oct 2012.

[8] G. Liyanage and S. Fernando. Firewall model for cloud computing. In *Industrial and Information Systems (ICIIS), 2013 8th IEEE International Conference on*, pages 86–91, Dec 2013.

[9] Alex X. Liu and Mohamed G. Gouda. Firewall Policy Queries. *IEEE Transactions on Parallel and Distributed Systems*, 20, 2009.

[10] Alex X. Liu. *Firewall Design and Analysis*, volume 4. World Scientific, 2011.

[11] Alex X. Liu. Firewall Policy Change-impact Analysis. *ACM Transactions on Internet Technology*, 11, March 2012.

[12] Wool. A quantitative study of firewall configuration error. *IEEE Computing*, 37: 62–67, 2004.

[13] Wool. Trends in firewall configuration errors : Measuring the holes in swiss cheese. *IEEE Computing*, 14:58–65, 2010.

[14] Chen, Liu, Hwang, and Xie. First Step Towards Automatic Correction of Firewall Policy Faults. *ACM Transactions on Autonomous and Adaptive Systems*, 7, July 2012.

[15] S. Khummanee, A. Khumseela, and S. Puangpronpitag. Towards a new design of firewall: Anomaly elimination and fast verifying of firewall rules. In *Computer Science and Software Engineering (JCSSE), 2013 10th International Joint Conference on*, pages 93–98, May 2013.

[16] E.S. Al-Shaer and H.H. Hamed. Modeling and management of firewall policies. *Network and Service Management, IEEE Transactions on*, 1(1):2–10, April 2004. ISSN 1932-4537.

[17] Marc Barrat, Alain Barthelemy and Alessandro Vespignani. *Dynamical Processes on Complex Networks*. Cambridge University Press, 2008.

[18] Duncan J. Watts. The "New" Science of Networks. *Annual Review of Sociology*, 30, 2004.

[19] Romualdo Pastor-Satorras and Alessandro Vespignani. Epidemic dynamics and epidemic states in complex networks. *Physical Review E*, 63, 2001.

[20] Yang Xiao. *Handbook of Security and Networks*. Cambridge University Press, 2008.

[21] R. M. Anderson and R. M. May. *Infectious Diseases of Humans: Dynamics and Control*. Oxford University Press, 1992.

[22] Romualdo Pastor-Satorras and Alessandro Vespignani. Immunisation of Complex Networks. *Physical Review E*, Februar 2008. URL `arxiv.org/pdf/cond-mat/0107066v2.pdf`.

[23] Kjell Jørgen Hole. Towards a Practical Technique to Halt Multiple Virus Outbreaks on Computer Networks. *Journal of Computer Networks and Communications*, 2012.

[24] 2014. URL `http://www.wired.com/2014/09/hackers-already-using-shellshock-bug-create-botnets-ddos-attacks/`.

[25] C. Perril. The danger of complexity: More code, more bugs. *TechRepublic*, Februar 2010. URL `http://www.techrepublic.com/blog/security/the-danger-of-complexity-more-code-more-bugs`.

[26] 2014. URL `http://supportcontent.checkpoint.com/documentation_download?ID=31853`.

[27] 12 June 2014. URL http://e24.no/digital/dnbs-nettbanker-er-nede-igjen/23228741.

[28] 2014. URL https://www.checkpoint.com/about-us/company-information/corporate-fact-sheet/facts-a-glance/.

[29] 2014. URL http://www.idc.com/getdoc.jsp?containerId=prUS25126214.

[30] 2013. URL http://www.fortinet.pl/wp-content/uploads/2013/06/2013-FW-CAR-Performance.pdf.

[31] D. Mahjoub. Monitoring a fast flux botnet using recursive and passive dns: A case study. In *eCrime Researchers Summit (eCRS), 2013*, pages 1–9, Sept 2013.

[32] Paul D. Leedy and Ellis Ormrod. *Practical Research. Planning and Design*. Pearson, 10th edition, 2012.