Flowspec, a new method for security incident mitigation

Bachelor thesis

Author(s): Paul Bongers

Version: 1.1

Date: July 11th 2012

SURFnet bv | Radboudkwartier 273 | PO Box 19035, NL-3501 DA Utrecht

T +31 302 305 305 | F +31 302 305 329 | admin@surfnet.nl | www.surfnet.nl

Education: Fontys Hogescholen
HBO-ICT ICT Management & Security
Rachelsmolen 1
5612 MA Eindhoven

Company: SURFnet bv
Radboudkwartier 273
PO Box 19035
3501 DA Utrecht

Author: Paul Bongers
Student number: 2108360

Company supervisor: Xander Jansen
First assessor: Jacqueline van den Broek
Second assessor: Stefan Roijers
External expert: Dhr. G. van Loon

Foreword

This document is written as thesis to graduate for my Bachelors degree HBO-ICT at Fontys University of Applied Sciences in Eindhoven. In this document I have described the activities I have performed at SURFnet BV where I did my final internship. I wrote this thesis in English because SURFnet has many international relationships and the activities I have performed might be interesting for other parties as well because they address a problem many companies are facing in today's world.

During the execution of this project I have received support from several people. I would like to thank those people for their support. I want to thank Jacqueline van de Broek for her help with my final preparations to be allowed to start this internship and Stefan Roijers for his support and clarifications during this internship. I want to thank Xander Jansen for his support and views during this internship. He was the one person who convinced me to start using the technology even though the research was still not completely finished. I would also like to thank Wim Biemolt, Niels den Otter and Jeffrey Everling for their help in realizing this project. I want to thank my parents and friends for their support, even on the moments I had almost given up on the project. Lastly I want to thank all my coworkers at SURFnet for the great time I had.

Thank you all guys. Without your support, help and clarifying views I would not have been able to finish this project.

Contents

Summary

This final internship has been carried out at SURFnet bv. SURFnet is a non-profit task-organization that strives to innovate the internet by collaborating with its clients and suppliers. The assignment has been put out by the SURFcert team. This is a team that helps clients stop attacks performed by hackers.

In the current situation this team has a few options to choose from, each of which has its own limitations. The assignment that has been put out was to find out if a particular technology can be used to stop hacking attacks in addition to the current options.

Research has been done to find out what the conditions were for starting to use the technology and to see if the technology complies with these conditions. Also part of the research was to find out if the equipment that SURFnet uses is suitable for using the technology. The results of this research have overall been positive and even though not all conditions were satisfied, a positive advice has been given to start using that technology. The reason that this advise was given, even though not all conditions were satisfied, is that changes to the technology have already been proposed that tackle these shortcomings and that the current version of the technology provides significant advantage over the other options.

Glossary

ACL – Access Control List

Arbor Peakflow SP CP – Arbor Peakflow SP Collector Platform

CERT – Computer Emergency Response Team

CSIRT – Computer Security Incident Response Team

Gbps – Gigabit per second

ISP – Internet Service Provider

MWS – Middleware Services (SURFnet department)

NOC – Network Operating Center

PID – Project Initiation Document (PRINCE2 Project management method)

RFC – Request for Comments

TMS – Threat Management System

TSP – ‘Tien Stappen Plan’

1 Preface

What if you would have to sift through hundreds of spam mails to find that one email you were expecting? What if you would no longer be able to do all your banking and shopping online? This might be the case if organizations like SURFnet would not be able to block malicious network traffic.

This final internship has been carried out at SURFnet bv. SURFnet is a non-profit task organization that strives to innovate the internet by collaborating with its clients and suppliers. The assignment that led to this internship has been put out by the SURFcert team. This is a team that helps institutions connected to SURFnet's network to mitigate network based attacks on their systems.

Currently the SURFcert team has a few options to choose from when they want to mitigate an attack. Each of these options has its limitations. RFC 5575 – Dissemination of flow specification rules is a proposed standard that provides the possibility to distribute traffic flow specifications. It is expected to provide additional possibilities for SURFcert to mitigate network based attacks. Therefore an assignment has been put out to research if flowspec can be used in addition to the current options the SURFcert team has.

In order to investigate this, more information was needed. First the requirements for the technology to be used would have to be defined. The technology would have to comply with those requirements. Either the systems currently used by SURFnet would then have to support it or new systems would have to be purchased. If all this is found to be positive, the technology could be used.

In chapter 2 more information is given on the company, the department and the SURFcert team, chapter 3 explains the details of the assignment and chapter 4 explains the project approach. Chapters 5, 6 and 7 describe the three phases that have gone through based on the chosen method. Chapter 8 contains the conclusion and recommendations.

2 Organization

SURFnet is a non-profit task organization that provides networking and communications services for higher education and research facilities. SURFnet enables these facilities to collaborate easily and effectively by the use of ICT. By working with these institutions to create innovative ICT solutions, SURFnet is able to transcend the individual interests of the institutions.

SURFnet also challenges parties to create new and better products, services and business models and encourages them to use open standards. For its suppliers SURFnet functions as a testing environment where they can test new applications within a large user group.

2.1 History

In the early 1980s the Informatics Promotion Plan was drawn up in response to the request of the Dutch government to innovate with the use of ICT. In March 1987 the SURF foundation was founded by the Dutch research universities, the universities of applied science (represented by their organization HBO-raad) and the major research institutions after they had documented their innovation activities in the SURF Strategic Plan. SURF's initial activities concerned researching the possibilities and impossibilities of a research network. As a result, SURFnet1 was launched in 1988 and a working company, SURFnet bv, was started to operate and manage this network. Since then several successive generations of the network have followed. The current generation, SURFnet6, has been operational since 2006 and SURFnet7 is currently being developed within GigaPort.

2.2 Organization structure

Within SURFnet there are several departments, each of which has its own area of expertise and responsibilities. An overview of these departments is given in figure 1. The young talents 'department' is special, as it isn't actually a department. The young talents program is a two year program that provides talented and ambitious graduates with an opportunity to gain working experience in several departments, perform complex assignments or projects and participate in a training or guidance program.

Besides these departments there are also teams and virtual teams. Teams are set up for a year according to the innovations that are planned in the year plan. A team is build from employees of all departments that are concerned with that team. Virtual teams are groups of people, not necessarily all employees of SURFnet, that develop and innovate new and existing services. They are also responsible for providing support for these services.

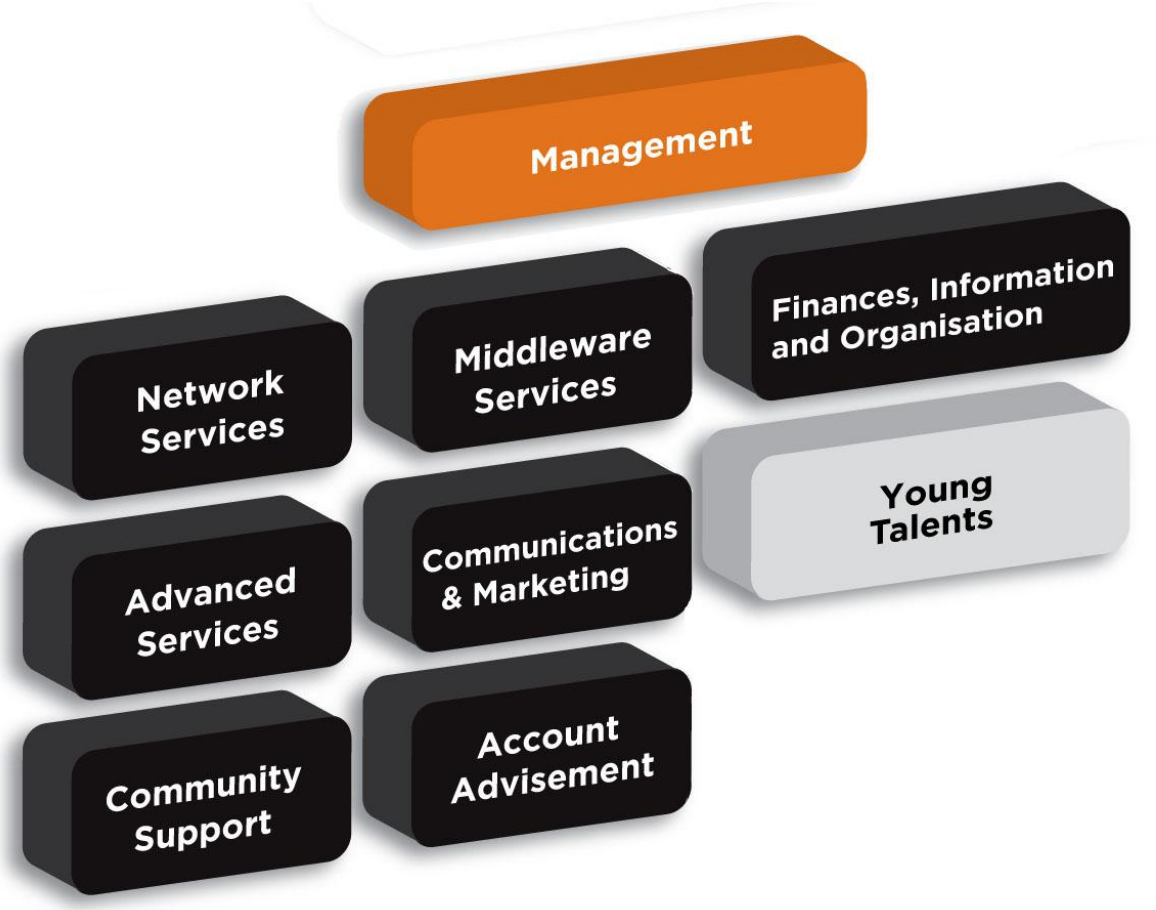


Figure 1

2.3 The project

This project has been carried out on behalf of the SURFcert team. This is a virtual team of 10 kernel members, including a chairman. Five of these kernel members are employees of SURFnet. The other five members are employees of connected institutions. The SURFcert team provides connected institutions with 24/7 support for incident response.

Since SURFcert is a virtual team, it has no office. The responsibility of the team lays with the department Middleware services (MWS). Therefore a workplace has been made available in the department's office. Besides the responsibility of SURFcert, MWS is responsible for several other security and middleware related services, for example SURFfederation, eduroam and DNSSEC.

3 Assignment

3.1 Initial situation

In recent years network based attacks have increased in number and in sophistication. Targets of these attacks differ from great multinational corporations to the website of your local convenience store. SURFnet and its customers are also targeted more and more often. Besides being targeted, it also happens that computer systems within the network of SURFnet participate in an attack. In these cases the SURFcert team has to act. In the first case, the CSIRT[1] of the targeted institution will try and mitigate the problem. In the last case, SURFcert will most likely request the CSIRT of the institution from which the attack is originating to solve the problem.

Whenever one of SURFnet's customers is unable to mitigate a problem they will ask for help of SURFcert. SURFcert will normally act in one of three ways:

- A null-route can be created which causes all traffic matching specific criteria to be dropped.
- Access Control Lists (ACL's) can be applied which enables more fine grained filtering of traffic with a variety of actions (i.e. rate limiting, blocking specific ports, etcetera).
- Traffic to a specific IP address can be redirected to a Threat Management System (TMS) before it is delivered to its final destination. The TMS filters the malicious packets, so only 'clean' packets reach their destination.

In certain cases SURFcert will contact the Internet Service Provider (ISP) of the attacker and ask them to resolve the situation.

3.2 Problem statement

All of the above possibilities have limitations. For the first two SURFcert depends on the Network operating center (NOC)[2] to implement the required rules on the routers. The NOC will then apply the requested actions within two hours. When mitigation is urgent, this might be too long. Also, when a rule doesn't have the desired effect, a new request has to be placed to change the rule, which may take another two hours to be processed. The third option can only be applied for a limited number of IP addresses and only has a 2 Gbps connection[3] (two times 1 Gbps). Also, the third option doesn't support IPv6.

Because of these limitations and the prospect that the number and rate of network based attacks will only increase further, SURFcert is looking for ways to be able to respond more quickly and more effectively whenever an attack occurs.

---

[1] CSIRT stands for Computer Security Incident Response Team. Alternatively the term CERT (Computer Emergency Response Team) is used.

[2] The NOC is an external party that is responsible for the operational network management, such as incident management, configuration management and change management, as well as supporting research activities related to SURFnet's network.

[3] Gbps stands for Gigabit per second

About two years ago, SURFnet had an intern do research to see if RFC[4] 5575 – Dissemination of Flow Specification Rules, commonly known as flowspec, could be used for this. Back then they found that it wasn't yet ready to be used for the intended purpose.

3.3 Project objectives

Recently SURFnet wanted to look into in again, because it was expected that this technology had evolved and is now ready to be used the way they intend to. In order to answer that question a project has been set up. The project has the following objectives:

- Identify the requirements
- Find out if flowspec meets these requirements
- Find out if SURFnet's equipment supports flowspec
- Advise on how to follow up

It is also requested that a proof-of-concept implementation will be realized if it turns out that the technology can be used.

3.4 Research questions

In order to achieve the above objectives the following research question has been formulated:

What is the best way to use flowspec, or a similar technique, in SURFnet's network to mitigate network based attacks?

In addition, the following sub questions have been formulated to help answer this research question.

- What requirements does the technique have to meet?
- Does the technique comply with those requirements?
- In which part of the network (inside or outside of SURFnet's network) can the technique be used and how can this be controlled?
- What are the hardware and software requirements for the technique?
- Does SURFnet's equipment comply with those requirements?
- What parties are currently involved with the mitigation of network based attacks? How are they involved?
- What is the current mitigation procedure?
- What are the implications of implementing the technique for the related procedures?

[4] An RFC is a Request for Comments, a memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems.

4 Project approach

4.1 Method

This project has been executed based on the ‘Tien stappen plan’ (TSP). TSP is a method for performing a final internship following ten steps. It is described in the book ‘Competent afstuderen en stagelopen’ (ISBN 978 90 01 77563 6) by Piet Kempen and Jimme Keizer. The ten steps of TSP are divided over three phases. The phases are orientation, research & solution and implementation.

In the first phase 5 steps are taken in order to define the assignment, to get an idea of the situation of the company and the branch and to agree on the assignment and methods. This allows for getting a better view of the assignment, the context of the assignment and the feasibility of the project.

In the next phase 3 steps are taken starting with preparing the research. After the necessary preparations are made the actual research is done. In the third step, instead of making an implementation plan as the method describes, recommendations were documented on how to follow up after this project is finished. This is because the nature of the assignment was to find out if flowspec is ready to be used and advise on the next steps as to start using it in a production environment instead of actually implementing it.

The third phase consists of two steps. The first of the two is implementing the solution that was found in the second phase. Since this project was not meant to result in an implementation in the production environment, a proof-of-concept was created. The last step is finalization and graduating.

4.2 Planning

To be able to monitor the progress and feasibility of the project, a master plan has been made (see figure 2). This plan was not meant as a very strict plan, but as a way to monitor the progress and be able to track delays.

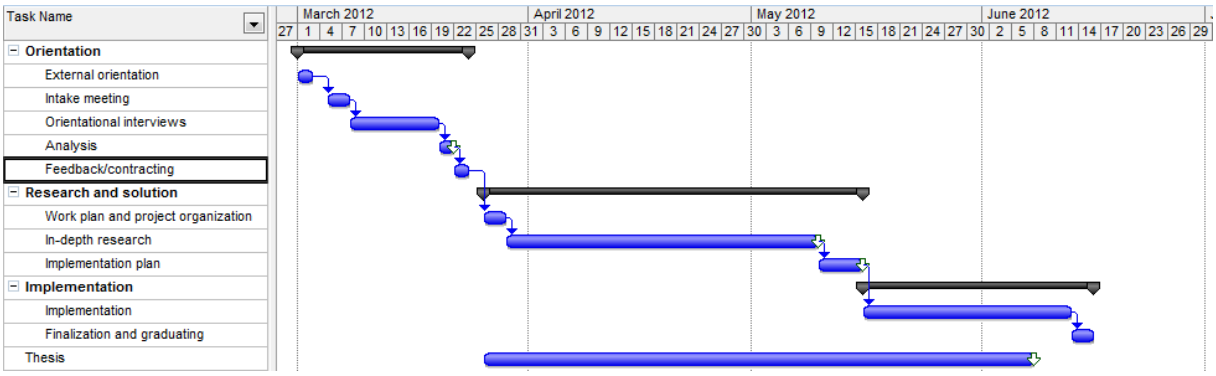


Figure 2: Original master plan

Initially this master plan was made following the recommendations in the literature (15% of the available time for orientation, 50% for research & solution and 35% for implementation). As the project proceeded a few changes have been made to this plan.

For the research & solution phase a more detailed plan was made for all anticipated activities (see figure 3). Again, this was no strict plan, but a means to monitor the progress. This plan however had to

fit within the master plan. If changing it resulted in more of less time needed in respect to the last change, the master plan also had to be changed.

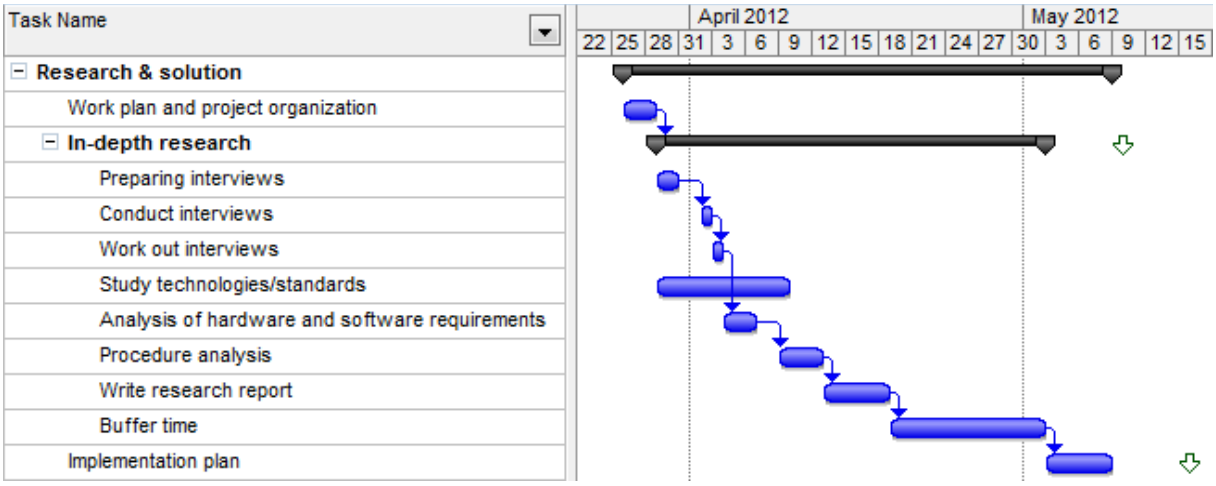


Figure 3: Original detail plan of phase 2

5 Orientation

During this phase of the project the first five steps of TSP were completed. The first three of them were meant to get enough information to get a clear view of the company, the department and the assignment. This information was used to write a project initiation document (PID)[5] which was done in step four. This PID was the basis for agreeing on the final assignment in the fifth step.

5.1 External orientation

In order to get an idea of the majority of the problem news archives were searched for items about information security. The items that turned up can be divided in two categories: Articles about hacking and cracking[6] and articles about new developments in information security. The generosity of the articles were about hacking and cracking, more specifically, businesses having been or being attacked. This confirmed initial expectations based on personal knowledge about the possibilities of ICT systems and the idea that news articles on the topic are published more and more often. It also suggested that network based attacks are a growing problem for about any computer system that is somehow connected to the internet.

5.2 Intake meeting

An intake meeting, as described in 'Competent afstuderen en stagelopen', has not taken place. The intake meeting described has the following objectives:

- To get to know the client better.
- To get more information about the client's view on the assignment.
- To get permission to work according to TSP.
- To agree on orientational interviews and feedback on the results.

These objectives have still been achieved, even though a meeting as described never took place. On the first day of the internship a tour was given through the building. A brief introduction was given to coworkers during this tour. Because several coworkers were on leave, not all of them were met.

During weekly meetings with the company supervisor ideas were exchanged on the course of the project for as long as the PID was not finished. Topics included the supervisors' views, TSP and general progress of the internship. Also during the process of writing the PID, inquiries were made to gain information that could not be found on the public or internal websites.

5.3 Orientational interviews

Only one person has been interviewed for an orientational interview, namely Niels den Otter. This was because he was the one person who would know the most of the last time research was done on the subject. As it turned out, the results of the last research were lost, if anything had been documented at all. The only thing that was still known was that bugs were found during the implementation and

[5] The project initiation document is part of the project management method PRINCE2. However, PRINCE2 is not used intentionally during the rest of the project.

[6] The difference between hacking and cracking is that hacking, by definition, is not done with ill intent while cracking is generally done for personal benefit of to damage the victim. The media however don't often make this difference.

therefore the use of flowspec was misadvised. For this project documentation of the routers would be made available as well as documentation of the Arbor Peakflow SP Collector Platform (CP) that should provide an interface to define flowspec and be capable of publishing these flowspecs.

During the interview it was also asked what was expected of the new technology, as to get a general idea of the expectations before finally committing to the project. This would later help preparing the interviews that were conducted in the next phase.

5.4 Analysis

During this step, all the information gathered was used to reflect on the assignment. This was done by writing a Project Initiation Document. In this document the final assignment was defined, as well as the main research question and the sub questions. Also the boundaries of the project have been defined, the ways of communicating different sorts of information and the frequency of communication.

By documenting all this, a clear view of the project is created and measurable goals were defined, making assessment of the project possible.

5.5 Feedback/contracting

In the third full week of the project, the PID has been topic of a meeting with the company supervisor and the second assessor, who also is the graduate teacher. During this meeting feedback has been given by both on the contents of the PID. Using this feedback, a few changes were made to the PID. The PID was then agreed on by the company supervisor and has from that point on served as a contract with SURFnet describing the activities that were to be part of the internship.

6 Research

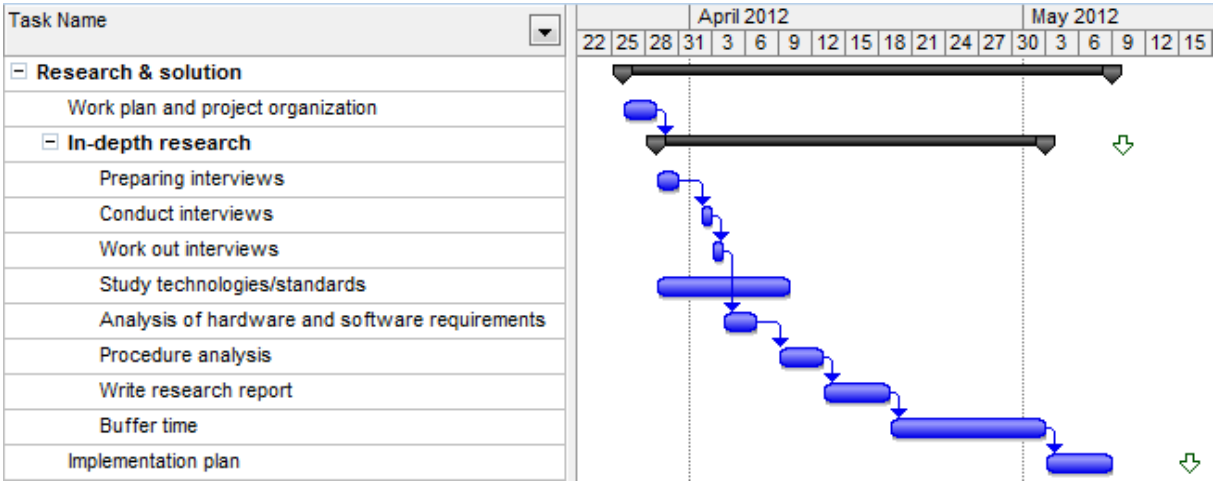
During this phase the next three steps of TSP were executed. The first step of this phase (step six in TSP) was meant to prepare the in-depth research in the seventh step. After the in-depth research, an implementation plan would be written for implementing the found solution.

6.1 Work plan and project organization

During the previous phase the final assignment was defined as well as the research question and sub questions. For each of the sub questions considerations were made on the method to use for acquiring the information needed to answer the question.

Because much information that was needed was already known within SURFnet, or at least was expected to be known, it was decided to interview people who are directly involved with the solution to be found. Additionally literature study would have to be done to gain insight in the technology and get information on how well the technology is supported by different hardware and software.

As already mentioned in paragraph 4.2 a more detailed planning was made for this phase. In this planning all anticipated activities have been described along with an estimated duration. Also some buffer time was planned to be able to respond to small changes in the planning.



6.2 In-depth research

Because it would be hard and too time-consuming to interview all ten members of the SURFcert team a decision was made who of the kernel members would be interviewed. This decision was made together with the company supervisor. It was important to interview people employed at SURFnet as well as people employed at a connected institution. Of the five people employed at SURFnet it was preferred to interview someone of the department Network Services as well as someone of Middleware Services. Thus the following people were asked for an interview:

- Luuk Oostenbrink of the department Network Services
- Wim Biemolt of the department Middleware Services and chairman of SURFcert
- Peter Peters of University of Twente
- JP Velders of University of Amsterdam
- Jaap van Ginkel of University of Amsterdam

Four of these people have ultimately been interviewed, because the day Peter, JP and Jaap where at SURFnet for lecturing at a TRANSIT course, Jaap was busy for that course and was also on duty for the SURFcert kernel.

The interview has been divided into two parts. The first part was meant to provide insight in the current situation, the procedures and the parties involved with the mitigation of incidents. The second part was meant to define the further part of the research. This included the requirements for a new solution, possible interesting alternatives and foreseen changes in the mitigation procedure.

With the first interview with Luuk, Xander Jansen, the company supervisor and SURFcert kernel member, was also present. Therefore his ideas have been documented as well. After the interviews were conducted, the results have been combined and worked out in a single document. This document has then been reviewed by Xander and Wim.

Parallel to preparing, conducting and evaluating the interviews, time was spent reading the RFC of flowspec. This proved quiet hard. Eventually the RFC was read completely. It provided insight on the possibilities of flowspec, the manner of publishing and installing rules and the manner of logging recommended. As it turned out, to be able to use flowspec the network hardware would have to run software that supports flowspec.

Together with Xander it was decided to start testing flowspec at this point. One reason for this decision was that reality might prove different then theory suggested. Another reason was that it would be more motivating to also ‘play’ with the hardware already instead of having to do all the theory first. Although the testing of flowspec and later the realization of the proof-of-concept was done parallel to the last part of the research, it is documented in a separate chapter for readability.

Even though the testing of flowspec had already started, research still needed to be done because no one knew how well it was supported or what versions were supported. It was however known within SURFnet that there was some level of support for flowspec. To find out how well it is supported, the manuals of the hardware and corresponding software were looked at. Also the release notes of the routers’ software were reviewed.

All the results that were found, along with the methods used to get them were documented in a report. This report ‘Next generation incident mitigation’ has been added to this thesis. At first the report was written in Dutch. When it was decided that this thesis would be written in English, the report had to be translated. This also took quite some time. After translating the report was finished in English since it hadn't been completed yet.

6.3 Recommendations on project follow-up

After the research was completed, recommendations were made on how to follow up on this project. These recommendations were presented during a session were the SURFcert team along with the department Middleware Services and a select few of the department Network Services had been invited. Also the graduate teacher has been present at this presentation.

Even though not all requirements have been met, still a positive advice has been given to start using flowspec because it eliminates a few shortcomings of the current possibilities and the future prospect is that the current shortcomings of flowspec will be addressed in the near future. It is also advised to pull some strings with suppliers to quicken the adoption of the drafts that have already been written to address these shortcomings.

The recommendations that were presented during this session have also been documented in the research report ‘Next generation incident mitigation’ attached to this thesis.

7 Implementation

The last phase is the implementation phase. It consists of two steps: Implementing the solution and Finalization the project and graduating. Since no implementation of the solution was required in the live environment of even in a testing environment, but instead a proof-of-concept implementation was asked, the realization of this proof-of-concept will be documented here.

7.1 Realization proof-of-concept

Parallel to the previous phase testing of the technology had already started. To be able to do this, a small test setup was created. Together with Jeffrey Everling, a student working a part time job at SURFnet, the necessary configuration was done to set up all preliminaries to use flowspec. After that the configuration of flowspec continued. Except for a minor error in the documentation, this configuration was straightforward.

Once flowspec was configured, a few tests were done. The nature of these tests was to find out if the setup worked, rules were installed correctly and if measured results matched the rules defined. At first it seemed that results did not match expectations. Therefore other tests were done using a different utility that would provide more accurate results. With this utility results were found that more or less matched the expectations.

This same setup was later used as proof-of-concept to demonstrate how it worked.

7.2 Finalization and graduating

To make sure that no brain-drain would occur once this project is at an end, documentation was written explaining the steps needed to configure flowspec in another environment. Also all documents that were written as a part of this project have been made available as reference. As one of the last parts of the project this thesis is written.

8 Conclusion and recommendations

It was found that not all requirements were met by the current version of flowspec. However, some drafts were found proposing small changes and additions to the current version tackling these shortcomings. The adoption of the drafts might be quickened if SURFnet pulls some strings with its suppliers to fast track these drafts. Therefore it has been recommended for SURFnet to do so.

Also was found that the hardware and software currently used by SURFnet supports flowspec. This has led to a positive advice to start implementing flowspec. Since the proof of concept involved an older version of Arbor Peakflow SP CP and a newer version of Junos OS running on the routers as well as that only one router was used it has been recommended that the setup is tested in SURFnet's test network before using it in a production environment. The full research report has been attached to this thesis.

Evaluation

During this internship I discovered that it is hard for me to focus on strictly theoretical stuff. I was often distracted during the desktop research. When Xander suggested that I started testing, this became much easier because I could change between theoretical and practical activities.

I also discovered that it is hard for me to focus on deadlines that are too far in the future. This resulted in much work on my thesis near the end of my internship. In the future I will plan progress of such documents in deadlines for specific chapters. I hope this will result in better planning and spreading of the activities that have I have to perform.

Writing the research report and this thesis proved to be quite hard. At the beginning of June I decided together with Xander and Stefan that it might be better for me to graduate in August instead of in June. This provided me with more time to work on the documents and therefore more ease of mind.

As of yet, I have found no definitive reason why the writing of these documents has been so hard for me. Possible reasons could be that I strive to be perfect and ask too much of myself, that I have had too much on my mind at a single time or that I think too long before writing stuff down. Of course other reasons may exist as well and there does not have to be a single reason for it.

Altogether it has been a great experience and I have learned a lot about computer networks, new technologies and also about myself.

Bibliography

Websites

SURF corporate website, http://www.surf.nl/

SURFnet corporate website, http://www.surfnet.nl/

SURFnet intranet, https://intern.surfnet.nl/

Wikipedia, http://en.wikipedia.org/wiki/Request_for_Comments

Appendices

Appendix A - Next generation incident mitigation