Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 7, July 2016, pg.210 – 224

Service Protection Constraints on ICT Security

Kadem K. Rehef

Department of Computer Science, College of Computer and Mathematical Sciences, University of Thi-Qar

Email: kademalsaadi@yahoo.com

Abstract— In the context that security is both formally and practically the definition and enforcement of rules, the concept is introduced that in addition to rules which ensure security, we need rules which ensure that users' access to the services networks are for is maintained. Examples of how service is hindered by otherwise sensible security rules are presented.

In this paper service protection rules described which can help to prevent these compromises to service and assist us to measure this impact where it occurs. These examples include demonstration in some cases of how the combined collection of rules (security and service protection) can be enforced and maintained. Finally, the issue of how to check that service protection rules are compatible with security rules is discussed. We show that service protection constraints can improve the performance of the network experienced by users while at the same time increasing network security.

Keywords: Service protection rules, Information and communications technology, Virtual Private Networks, Firewalls, Single Sign-On, Netml system, Ns-3 and Click.

I. INTRODUCTION

Network security is often conceived solely as the activity of preventing inappropriate activity within a network, or in the vicinity of a network [1]. In this paper, we consider the unintended side-effects of security, in preventing normal use, inadvertently, and how to prevent these unwanted side-effects from happening. For example, if a web site contains material for which authentication is logically required, for read access, we expect that users will be expected to authenticate only when they request access to the restricted material. A security design which required authentication for accessing unrestricted material is introducing an unnecessary and unintended restriction. Most web designers would take this into account in the design of their web site, but in the more opaque context of network security it is more difficult to minimise unnecessary restrictions. Security which is too tight is known to have a deleterious effect on security. Users who perceive security as too restrictive may feel entitled to bypass the security which is perceived to be over-restrictive to achieve their objectives. For this reason it is important to take into account the expectations of users into security design [2]. In Section II, the literature relevant to the concept of service protection constraints is reviewed, including a review of VPNs, firewalls and single-sign-on (SSO); in Section III, the concept of service protection constraints is introduced and defined precisely; in Section IV several typical problems which arise when network security is poorly designed are described; in Section V, we show how service protection constraints can be used to address these problems; in Section VI, the question of validating the combination of security rules and service protection constraints is discussed; and concluding remarks are presented in Section VII.

II. BACKGROUND AND LITERATURE REVIEW

A. Security of Networks – Security rules

It is conventional to express network security by means of rules. This is a practical approach to security, and potentially provides also a sound basis for a theory of network security. The term rule can be used informally, for example, in relation to the rules to be observed by users, and formally, for example the rules embedded in systems which are enforced by configuration of servers and routers. In this paper, we assume that security is specified by formally defined and systemically enforced rules. The task of network security designers is to choose these rules, and implement procedures which enforce them. This is not a new idea. The idea we explore in this paper is to include rules whose purpose is to protect the service experienced by users.

B. The Goal of Network Security

The aim of network security is to ensure that no data is modified except by authorised parties (integrity), to protect the confidentiality of data stored in the network, and to ensure that availability of data is not inhibited by deliberate or accidental interference by external parties [3].

C. Virtual Private Networks

In recent years, various virtual private network (VPN) technologies have been widely used to provide a secure site-to-site connectivity and remote access. Two factors which influence the widespread uptake and use of VPNs are total ownership cost savings relative to other approaches and productivity benefits for users. Total ownership cost includes the initial deployment cost plus the cost of user training, support, and facility maintenance over time. Productivity enhancements include tool effectiveness, user time savings, usability improvements, and user satisfaction [4], [5].

Secure Sockets Layer (SSL) based VPNs are an emerging technology that provides remote-access VPN capability using the SSL technology that is already built into a modern web browser. SSL VPN allows users from any Internet-enabled location to launch a web browser to establish remote-access VPN connections, thus promising productivity enhancements and improved availability, as well as further IT cost reduction for VPN client software and support [6], [7]. On the other hand, a VPN can be used to bypass network security. Well-known examples of this is their use by citizens of one country using a VPN to a different country to gain access to services supposed to be blocked in their own country. This needs to be addressed by network managers because in general it should be regarded as a loophole with potentially serious consequences that needs to be blocked.

D. Firewalls

Firewalls are an important tool for the network security, where they are used to prevent unauthorized users from accessing or interfering with a network [8]. The main mechanism used in firewalls is to check the header in each packet, discarding the packet if it matches certain patterns and accepting it when it matches others [2]. Firewalls can adopt or drop rules of this sort dynamically, according to their own higher level rules, or under the control of other servers. This increases their selectivity considerably. Firewalls can efficiently block large quantities of unwanted traffic, however the following potential weaknesses need to be considered: (a) if the rules are too complex, or the firewall is too slow, it could become a bottleneck; (b) if rules are inappropriate, some unwanted traffic might be allowed through; (c) other mistakes in the rules could block traffic which should be allowed.

E. Single Sign-On

Users often need to use many user IDs and passwords for the services they use. Single sign-on (SSO) allows users to make use of the authority from one login transaction to access a collection of services [9], [10]. SSO improves the safety and efficiency of use of the systems in which it is used, and reduces the burden on administrators [11].

F. The Netml system

The Netml system was developed at the University of Southern Queensland for teaching and research of network protocols and technology [12]. Its objective is to enable students and users from industry to create networks easily, and to understand the full complexity of a multilayer network easily by means of highly configurable visualisation tools. The main tools provided in the Netml system are analytic, and do not rely on the simulation. However, simulation is an essential technique in research and teaching. In fact, more than half of all users introduced to a system for network analysis assume that simulation is the only possible way to analyse a network. Even users who understand that there are effective mathematical models and for analysis expect the reassurance of confirming simulations to validate them. On the other hand, the development of well understood and accurate models by networking professionals – researchers or practitioners – for them to achieve well-founded confidence that they understand how networks work, and how they will behave in a variety of situations.

G. Ns-3 and Click

The Netml system is used in this paper to construct the network examples and simulate them. Simulations in Netml are carried out by generating an ns-3 C++ program and together with Click scripts for each firewall. The ns3 system [13] provides accurate and fast simulation of communication systems, with emphasis on the TCP/IP protocols. The range of technologies, protocols, and applications which may be of interest to include in simulations is very considerable, and it is therefore essential to facilitate modular extension of any simulation system. In particular, the ns3 system does not include its own native model of routers or router protocols, but instead has the capacity to model routers using the Click modular router system [14], [15], or to use other router implementations, including commercial software. Ns3 is able to include a mixture of simulation, emulation, and implementation of networking software and hardware, including interfacing with software running in virtual machines.

III. SERVICE PROTECTION CONSTRAINTS

Definition of Service Protection Constraint

A service protection constraint is statement concerning the services or performance of a network, which the network provider enforces. Some examples of service protection constraints include:

(a) Authorized users should be able to authenticate at their desktop, notebook, or other officially issued computer or device 99.999% of the time;

(b) Authorized users should be able to reset their passwords by using suitable auxiliary information or evidence within one hour;

(c) Authorized users should be able to use all of the authorized software on their officially issued or approved computers without interruptions caused by unintentional security restrictions;

(d) All staff should be able to print documents at the nearest printer (owned by their organisation) without separate authentication; To explain the intention of these service protection constraints more clearly, here are some examples which are probably not too unfamiliar, of what can happen when these constraints are not supported:

(a) A user is supplied with notebook for a specific purpose (e.g. development of multimedia) but is unable to authenticate even after trying for several hours; eventually, they return the notebook and adopt a different strategy for developing the multimedia;

(b) A user attempts to make use of an application which they are required to use in the course of their responsibilities, but a security configuration problem (e.g. Licensing, or network access) prevents the software from being usable; although the cause of this problem is understood by the user and a request to address the problem is placed immediately, the change in security configuration requires approval by a high-level manager, and is not effected for 4 weeks;

(c) A user “prints” a document, but the document does not appear at the printer; after several days the user discovers that the authentication protocol for the printer has changed and their computer must be reconfigured by IT support for printing to be enabled again.

IV. EXAMPLES OF SERVICE PROBLEMS CAUSED BY “SECURITY”

A. Restrictions on Administrator Access

Restrictions on administrator access to computers are often introduced as a security measure. Consider the following scenario:

A postgraduate student starts work on his research project on January 1. His computer is configured by the ICT staff without administrator access, because this is safer for him, and for other users. However, because of a configuration fault, this prevents the computer being used for the research until February 1. For one month, the student is unable to work effectively. To further explain: the reason the software is unusable in this particular case is because of a configuration error during installation; the configuration error was made because the ICT administrator has no expertise in the use of this particular software, and hence is unable to correctly configure it. However, because the configuration setting has been classified as restricted to administrators, the user is unable to correct the mistake. This type of service failure has many variants and is difficult to address because there is no clear culprit to blame, and perhaps correct. Probably the problem is unavoidable within a security framework where user’s are not trusted to administer their own computers. The policies of this sort are easily justified by assuming that mistakes never happen.

B. Internal Filtering and Firewalls

An example network with internal firewalls is shown in Figure 1. The legend for this figure and Figure 3 is shown in Figure 2.

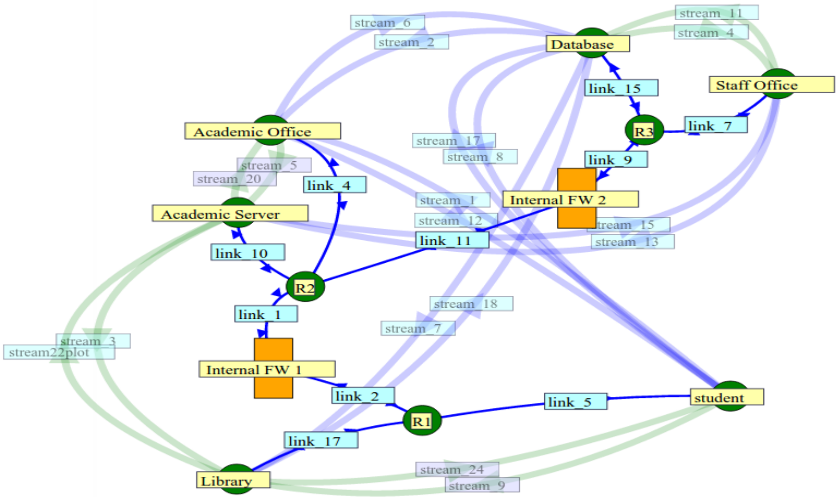

Fig. 1. Example of a filtering configuration (See Figure 2 for the legend).

Internal filtering has the potential to enhance security in environments where there are several classes of users

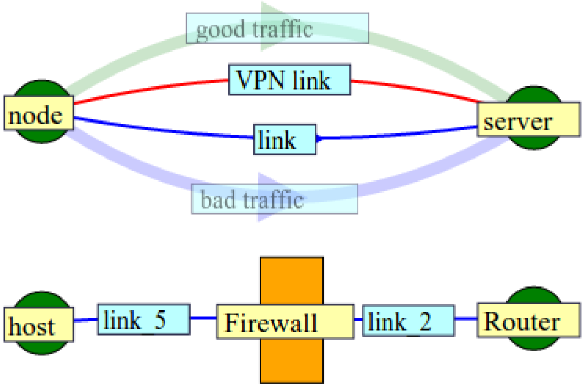

Fig. 2. Legend for Figures 1 and 3.

TABLE I. FILTERING RULES FOR INTERNAL FIREWALL 1

SRC IP	DEST IP	DEST PORT	VERDICT
10.0.14.0/24	*	*	Accept
*	10.0.14.0/24	*	Accept
10.0.12.0/24	10.0.4.0/24	*	Accept
10.0.4.0/24	10.0.12.0/24	*	Accept
*	*	*	Drop

With very different security profiles. For example, at a university, the administrative, academic and student users have quite different roles, responsibilities, and are quite reasonably perceived as introducing different risks. Filtering prevents unwanted access in a comprehensive manner which is fairly safe from unwanted interference. Traffic from different classes of user can be segregated from each other. In universities there are three main classes of users: academics, students, administrators. Other classes of users than just these three will, in general, be needed, but for simplicity in this paper we limit discussion to these three classes. Firewalls and filtering routers are configured by specifying a series of patterns to which packets are compared one-by-one. When a match is found, the matching packet many dropped or accepted. Otherwise, the next pattern is checked. The patterns used in internal FW1 in our example network are listed in Table I and the patterns used in internal FW2 are listed in Table II. The internal firewalls in a moderate to large organization like a university will usually be much more complex than these. It is not unlikely that these firewalls will contain errors which prevent access which is needed and allow access which is undesirable, by mistake. The mistakes will be logical errors in some cases, and simple blunders in others. Users affected by these firewall configuration errors will, in many cases, be unaware that their difficulties are caused by the firewalls, and the firewall administrators will therefore not receive any feedback about the firewall design from the affected users. The majority of users therefore rely on the existence of a small group of technically aware users who discover firewall configuration problems and pass on their concerns to the administrators.

TABLE II. FILTERING RULES FOR INTERNAL FIREWALL 2

SRC IP	DEST IP	DEST PORT	VERDICT
10.0.5.0/24	10.0.13.0/24	*	Accept
10.0.13.0/24	10.0.5.0/24	*	Accept
*	*	*	Drop

C. VPN Configuration

In Figure 3, the network of Figure 1 is extended to include locations outside the university from where the students and staff wish to continue using university services via the Internet. When a university student or employee wishes to access the university, we assume they make use of a VPN server, which sets up a VPN link from their computer to a location inside the university. The challenge in VPN design is to configure it so that users are able to use the services they need, in a manner which does not compromise security.

D. Printer Access

Sometimes the security rules for accessing printers prevent users who should have access from being able to print. This can be very frustrating for users because although printed documents are less important than they used to be, nevertheless they are sometimes required urgently. Since printing a document will normally take only a minute or so to complete, it comes as an unpleasant surprise to users if a security re-configuration requiring days is a prerequisite for successfully printing a document. Security configuration problems of this sort, which cause printing to fail mysteriously, are more likely to affect users with non-standard computer configurations: for example, users of Linux or Macintosh computers. For this reason, some organisations adopt the “solution” of adopting a Standard Operating Environment (SOE), which is supported by the ICT Department. Configuration problems experienced by users whose computers do not conform to the SOE can then be classified as “someone else’s problem”.

E. Single Sign-on

Single sign-on has the potential to reduce security or access to services severely if it is misconfigured:

(a) If the duration of the single sign-on authority is too long, a user’s computer might enable an attacker to gain access to valuable resources while its owner is out of their office or otherwise indisposed;

(b) If the single sign-on server itself is overloaded, or vulnerable to deliberate or accidental damage, it might become a bottleneck preventing users from accessing many resources;

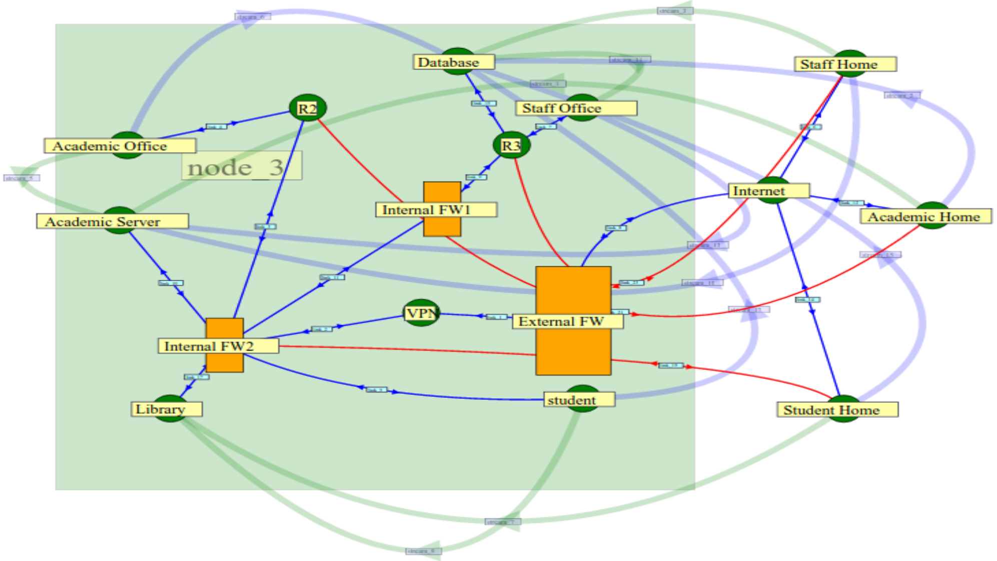

Fig. 3. Example of a filtering and VPN configuration (see Figure 2 for the legend)

(c) When a user’s authentication details (identity and password, for example), are obtained by an attacker, the range of services compromised is greatly increased by the use of single sign-on.

V. ADDRESSING PROBLEMS BY SERVICE PROTECTION CONSTRAINTS

A. Restrictions on Administrator Access

It is clearly unacceptable for a user to be prevented from using their computer for more than a month by a configuration mistake, and ICT managers probably doubt that this happens. However, in most organisations there are vulnerable users – new or junior members of staff, and users of special different software packages – and when a mistake of this sort occurs for one of these users, it will not necessarily register. To protect against such mistakes we need to adopt practices which protect such users. The following service protection rule serves this purpose: Protection of Designated Service User's should never be prevented from using their official ICT equipment for one of its designated purposes by configuration errors for more than a reasonable period (e.g. one day).

The purpose of this rule is to establish clearly that it is unacceptable for users to be denied access to their designated services for an extended period, even if this is caused by "security considerations". There are not many security practices with the potential to severely limit a user's ability to work for an extended period, but restriction of administrator access is one such practice. This can be explained as follows:

although it is conceivable to fully configure an operating system so that the user never needs administrator access, today's operating systems do not adequately support such configuration. Furthermore, all the users who are developing these operating systems do not themselves have the experience of living with such restrictions. Fortunately, there is a practical solution to this problem which is the common practice: when users report that their computer can't be used for one of its designated purposes, the user should be granted administrator access. In order to satisfy the designated service rule above, it is only necessary to require that administrator

TABLE III. SERVICE CONSTRAINT RULES (RULES FOR

TESTING)

SRC IP	DEST IP	DEST PORT	VERDICT
10.0.7.0/24	10.0.14.0/24	*	Accept
10.0.4.0/24	10.0.14.0/24	*	Accept
10.0.4.0/24	10.0.12.0/24	*	Accept
10.0.7.0/24	10.0.4.0/24	*	Drop
10.0.7.0/24	10.0.13.0/24	*	Drop
10.0.4.0/24	10.0.13.0/24	*	Drop
10.0.5.0/24	10.0.14.0/24	*	Accept
10.0.5.0/24	10.0.12.0/24	*	Drop
10.0.5.0/24	10.0.13.0/24	*	Accept
10.0.14.0/24	10.0.7.0/24	*	Accept

10.0.14.0/24	10.0.4.0/24	*	Accept
10.0.12.0/24	10.0.4.0/24	*	Accept
10.0.4.0/24	10.0.7.0/24	*	Drop
10.0.13.0/24	10.0.7.0/24	*	Drop
10.0.13.0/24	10.0.4./24	*	Drop
10.0.14.0/24	10.0.5.0/24	*	Accept
10.0.12.0/24	10.0.5.0/24	*	Drop
10.0.13.0/24	10.0.5.0/24	*	Accept

Access is granted within a reasonable period of time (at most 2 days). In order to give force to this service level constraint it should be included in the Service Level Agreement between ICT and users, and should be pointed out to new staff as part of their induction training. There also needs to be an explicit list of designated services, which would vary from user to user, while taking a standard form for most users.

B. Internal Filtering and Firewalls

The firewalls in the network depicted in Figure 1 were tested by simulation. The traffic used in these tests corresponds to the rules shown in Table III. Even though the lists of firewalls in these tables are very short, when the tests were first carried out, it was discovered that there were many errors in the firewall rules, as implemented. For example, IP addresses which were meant to be entered as 10.0.14.0 were entered instead as 10.0.0.14. Many such errors were discovered: traffic which was supposed to be blocked was not blocked, and traffic which was supposed to be allowed was blocked. After the errors were found and corrected, the simulation produced the results shown in Figure 4. All the traffic streams which were supposed to be blocked are now blocked, and the traffic streams which are meant to be allowed, are allowed. The rules in Table III are service protection constraints. The take exactly the same form as the firewall rules which are used to implement the firewall, but they express the desired outcomes, rather than the mechanism of implementation.

C. VPN Configuration

What should users be able to access via a VPN? There are many potential answers to this question, some of which could be lengthy and detailed. However, a lengthy, detailed answer would constitute an ICT maintenance problem.

TABLE IV. FILTERING RULES FOR EXTERNAL FIREWALL

SRC IP	DEST IP	DEST PORT	VERDICT
10.0.15.0/24	10.0.14.0/24	443	Accept
10.0.14.0/24	10.0.15.0/24	443	Accept
*	*	443	Drop
10.0.16.0/24	10.0.12.0/24	443	Accept
10.0.12.0/24	10.0.16.0/24	443	Accept
*	*	443	Drop
10.0.17.0/24	10.0.13.0/24	443	Accept
10.0.13.0/24	0.0.17.0/24	443	Accept
*	*	443	Drop

A better approach – we would like to suggest – is to adopt the following rule, which is an excellent example of a service protection constraint:

VPN Service Rule

Users accessing the organisation via the VPN have access to the same services as from their normal place of work. We suppose that the network in this example is the same as Figure 3 but with the addition of a VPN server and an external firewall. The rules in the internal firewalls are the same as before, and the rules in the external firewall are shown in Table IV. The VPN Service Rule can be interpreted as a logical rigorously defined rule. It has a precise meaning. But, a rule like this can be difficult to implement. So,

(i) How can this rule be implemented, in such a way that we can prove that it holds?

(ii) Is it possible that security is compromised by implementing this rule?

Implementation

The VPN Service Rule can be enforced as follows: when a user authenticates with the organisation’s VPN, a VPN link is set up between the user’s external computer and the same router to which the user normally connects when at work. The external end of this VPN link is then equipped with an IP address in the same range as their computer at work (which might be a desktop computer, or it could be the same actual computer as used from outside the organisation). Finally, the external firewall of the organisation must be configured to allow all of the VPN traffic to pass through without interference.

Validation

The fact that traffic on a VPN link tunnel's through the organisation's external firewall means that VPN links are

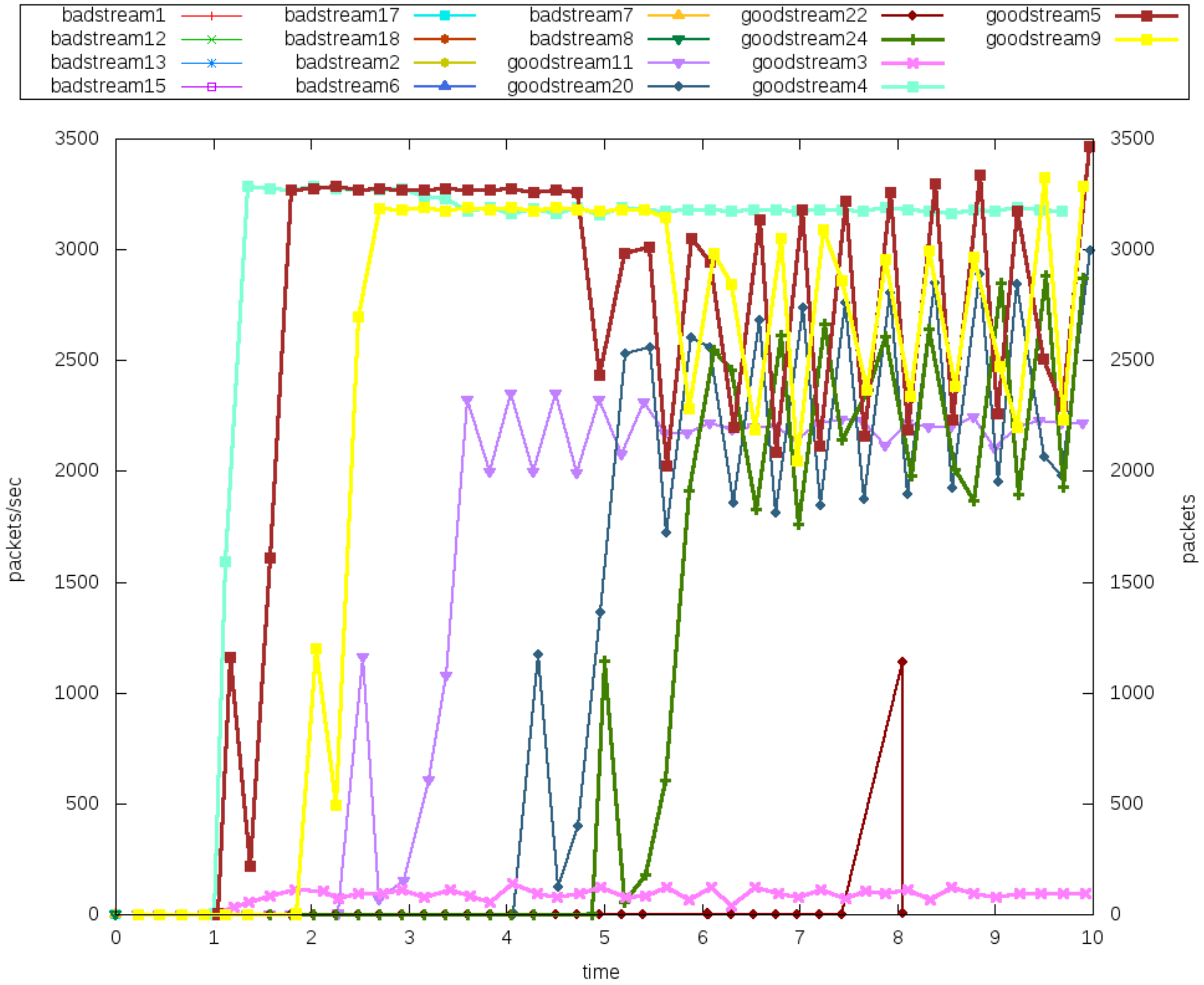

Fig. 4. Traffic throughput for network of Figure 1

A potential risk. Normally VPN links are encrypted, so it would be difficult for the firewall to check the traffic passing on the VPN link even if it was considered desirable. To minimise the risk, instead of configuring the firewall to allow all VPN traffic to pass, the firewall should block all such traffic unless associated with a source and destination which has been specifically configured. The firewall rules for such VPN links should be added to the firewall dynamically, and removed, by the VPN server. This addresses the second service protection constraint cited above. Note that in this instance the service protection constraint is specifically aiming for better security of the network, not protecting the service of the individual user of a VPN link.

D. Printer Access

The natural, and obvious, rule for printer access is: Users should (with availability 99.9%) be able to print on their nearest accessible printer, without having to undertake additional security configuration.

Implementing this rule should be within the capability of ICT technology and good practice. However, protocols for printer access have evolved along several parallel paths and it is surprisingly difficult to validate this simple and natural rule, particularly if it is required to include a full variety of operating systems.

E. Single Sign-on

Single-sign-on is a complex concept which requires careful design. It is not a principle which provides more benefits if pursued more and more comprehensively. It is likely that users will continue to keep certain domains of activity isolated from others. On the other hand, even when two domains of user activity are not linked by single-sign-on authority, they can provide auxiliary security mechanisms. The best example of this is the use of mobile phones to provide secondary authentication for banking transactions. Here are some possible service protection constraints for single-sign-on:

i) The duration of the authority associated with a certain authentication event never extends beyond the period specified in the system design;

ii) Users can configure the duration of the single-signon system up to a certain maximum value fixed by the sign-on system;

iii) Users are easily able to invalidate the authority currently in place (logout) in the single-sign-on system at any time;

iv) Users can configure the authority transfer network of the single-sign-on system, within the range of systems with which it is can be used. Because users have different practices, allowing users to customise the key features of a single-sign-on system has the potential to improve performance and security considerably.

VI. VALIDATION OF SECURITY AND SERVICE

PROTECTION RULES

In complex cases it may be difficult to be sure that an implementation of network security rules meets all the rules that we have specified. We need a procedure to check that, under a given network design, the rules hold. Furthermore, once it is allowed that security systems should satisfy service protection constraints as well as their more customary rules which restrict, we need to check the consistency of the entire collection of rules. Proving consistency of a set of rules (or aximoms) is a problem which has been tackled many times in the mathematical literature. In some cases it can be shown to be infeasible. However, there is no reason to believe that consistency of security rules and service protection constraints will be as difficult as a problem treated in this literature. Instead, it is more likely that consistency can be reduced to that of a system whose consistency is already establised by long practice (e.g that of mathematics itself). Once consistency is established we need to develop a framework which enforces the chosen rules and constraints. In the preceding sections we indicated explicitly how this can be done in two cases:

(i) The internal firewalls and filtering; and (ii) the external firewall and VPN system.

VII. CONCLUSION

The concept of service protection constraints was defined and a number of examples were explored which showed that well-known problems can potentially be managed more effectively. In some cases service protection constraints appear to be no more than test cases that can be used to improve the design and change management of ICT facilities like firewalls. However, there are other examples where the role of service protection constraints is more profound. Since service protection constraints are rules which can potentially be defined in the same language and context as security rules, they are well-suited to enhancing the design, change management, and measurement of the performance of network security. In addition, analysing the combination of security rules and service protection constraints may assist to avoid logical flaws in security design which otherwise might be regarded as unavoidable costs of good security.

REFERENCES

[1] B. Singh, “Network security and management,” in Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on, Dec 2010, pp. 1–6.

[2] C. Zacker, Networking: The Complete Reference. McGraw- Hill Professional, 2001.

[3] S. Mallard, Computer and Network Security. Steve Mallard, 2007.

[4] Z. Zhang, Y.-Q. Zhang, X. Chu, and B. Li, “An overview of virtual private network (vpn): Ip vpn and optical vpn,” Photonic Network Communications, vol. 7, no. 3, pp. 213–225, 2004.

[5] J. Tyson, “How virtual private networks work,” Retrieved on July, vol. 31, p. 2008, 2001.

[6] S. H. Sun, “The advantages and the implementation of ssl vpn,” in Software Engineering and Service Science (ICSESS), 2011 IEEE 2nd International Conference on, July 2011, pp. 548– 551.

[7] O. Flauzac, F. Nolot, C. Rabat, and L.-A. Steffenel, “Grid of security: A new approach of the network security,” in Network and System Security, 2009. NSS ’09. Third International Conference on, Oct 2009, pp. 67–72.

[8] S. McClure, J. Scambray, G. Kurtz, and Kurtz, Hacking exposed: network security secrets and solutions. McGraw-Hill, 2009.

[9] S. Bhosale, "Architecture of a single sign on (sso) for internet banking," in Wireless, Mobile and Multimedia Networks, 2008. IET International Conference on, Jan 2008, pp. 103–105.

[10] P. Tiwari and S. Joshi, "Single sign-on with one time password," in Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on, Nov 2009, pp. 1–4.

[11] Z. Liang and Y. Chen, "The design and implementation of single sign-on based on hybrid architecture," Journal of Networks, vol. 7, no. 1, pp. 165–172, 2012.

[12] R. G. Addie, Y. Peng, and M. Zukerman, "Netml: networking networks," in Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on. IEEE, 2011, pp. 1055–1060.

[13] G. Riley and T. Henderson, "The ns-3 network simulator," in Modeling and Tools for Network Simulation, K. Wehrle, M. G¨unes, and J. Gross, Eds. Springer Berlin Heidelberg, 2010, pp. 15–34. [Online]. Available: http://dx.doi.org/10. 1007/978-3-642-12331-3 2

[14] E. Kohler, "The click modular router," Ph.D. dissertation, Massachusetts Institute of Technology, 2001.

[15] L. S. P. and R. Merz, "Ns-3-click: Click modular router integration for ns-3," in Wns3, 2011.