9-1-2011

Optimization of delays experienced by packets due to ACLs within a domain

John N. Davies
Glyndwr University, j.n.davies@glyndwr.ac.uk

Paul Comerford
Glyndwr University, p.comerford@glyndwr.ac.uk

Vic Grout
Glyndwr University, v.grout@glyndwr.ac.uk

Recommended Citation
Davies, J.N, Comerford, P. and Grout, V. (2011) Optimization of delays experienced by packets due to ACLs within a domain" [Paper presented to The 4th International Conference on Internet Technologies and Applications, Glyndwr University held at Glyndŵr University, 6-9th September, 2011]. Published in the Conference Proceedings pp. 277-284.

Optimization of delays experienced by packets due to ACLs within a domain

Abstract

The infrastructure of large networks is broken down into areas that have a common security policy called a domain. Security within a domain is commonly implemented at all nodes however this has a negative effect on performance since it introduces a delay associated with packet filtering. Recommended techniques for network design imply that every packet should be checked at the first possible ingress points of the network. When access control lists (ACL's) are used within a router for this purpose then there can be a significant overhead associated with this process. The purpose of this paper is to consider the effect of delays when using router operating systems offering different levels of functionality. It considers factors which contribute to the delay particularly due to ACL. Using theoretical principles modified by practical calculation a model is created for packet delay for all nodes across a given path in a domain.

Keywords

Routing, Domain, Performance, Delay through Routers, Access Control List, Firewalls, Inter-Firewall Optimisation, IP packet filtering

Disciplines

Computer and Systems Architecture | Digital Communications and Networking | Hardware Systems | Systems and Communications

Comments

Copyright © 2011 Glyndŵr University and the authors, all rights reserved. This paper was first presented at **The 4th International Conference on Internet Technologies and Applications, Glyndwr University** September 6-9, 2011, Wrexham, UK and published in the conference proceedings by Glyndŵr University.

OPTIMIZATION OF DELAYS EXPERIENCED BY PACKETS DUE TO ACLS WITHIN A DOMAIN

John N. Davies, Paul Comerford and Vic Grout

Centre for Applied Internet Research (CAIR), Glyndŵr University, Wrexham, UK
j.n.davies | p.comerford | v.grout @glyndwr.ac.uk

ABSTRACT

The infrastructure of large networks is broken down into areas that have a common security policy called a domain. Security within a domain is commonly implemented at all nodes however this has a negative effect on performance since it introduces a delay associated with packet filtering. Recommended techniques for network design imply that every packet should be checked at the first possible ingress points of the network. When access control lists (ACL's) are used within a router for this purpose then there can be a significant overhead associated with this process. The purpose of this paper is to consider the effect of delays when using router operating systems offering different levels of functionality. It considers factors which contribute to the delay particularly due to ACL. Using theoretical principles modified by practical calculation a model is created for packet delay for all nodes across a given path in a domain.

KEYWORDS

Routing, Domain, Performance, Delay through Routers, Access Control List, Firewalls, Inter-Firewall Optimisation, IP packet filtering.

1. INTRODUCTION

Modern computer networks are expected to provide reliable high performance end to end connectivity at any point in the world. They must also provide the ability to filter packets so that access to services is limited to trusted traffic defined in the security policy for the network. This must be achieved with a minimal delay without compromising the security policy. It can be a challenge for a network engineers to meet these two conflicting requirements.

Most networks contain one or multiple connections into external networks e.g. Internet which is considered a great security risk. To mitigate this, trusted networks are created which perform stringent security checks on packets which cross the network boundary in both directions. Such networks operate under a common security policy managed by a single authority and are known as domains. If network traffic is filtered at all ingress and egress points in the network then it should only contain traffic which is defined as trusted under the security policy figure 1.

Infrastructure security within a domain is normally implemented in either firewalls or routers containing Access Control Lists (ACL's). ACL's has a common implementation across all platforms [1]. Significant delays for every packet result from the introduction of such techniques due to the filtering requirement [2]. Attempts have been made to use various techniques to optimise the delay through routers caused by ACL's [6].

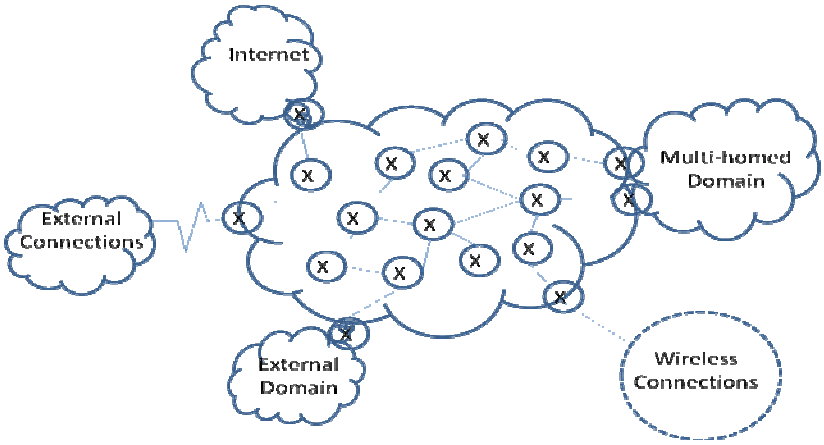

Figure 1. Typical Domain configuration

The issue of latency caused by packet filtering rules has been studied for around 10 years [3] and the existence of rule conflicts causing redundancy within an ACL was identified.

2. RELATED WORK

Rule reordering has been considered to decrease latency associated with packet classification. Studies highlighted through experimental evidence that ordered ACL's could reduce packet processing time [4]. The study did not however, consider the conflicts that may exist between different rules in an ACL. A subsequent paper does consider rule reordering, however only a simplistic treatment is given by organising similar rules into classes, individual rule reordering and conflicts are not considered [5].

Anomalies in firewall databases using algorithmic techniques have bee identified [6] and subsequent work presented a method to introduce early rejection rules for the most commonly matched traffic providing dynamic updates as traffic flows change [7].

Several schemes have been proposed for storing filtering rules in alternative data structures which facilitate faster lookup times than linear lists. This is achieved by representing the rules as a decision tree [8] [9]. Hash tables are also considered for packet classification using a single memory lookup however such schemes exhibit worst-case exponential space complexity which limits their use in devices with limited memory capacity [10].

Hardware solutions to the latency problem have been developed using Ternary Content Addressable memory (TCAM's). These evaluate all rules in the packet filter in parallel and return the rule with the lowest cost in a single memory lookup [11]. Due to their low density they are only able to handle a small number of rules [12]. TCAM's are typically only found in expensive high-end core routers [13].

There has been comparatively little research undertaken into optimisation of packet filters in a single domain. Algorithms have been proposed for identifying anomalies and implementing these in the form of a software tool which allows a network administrator to provide anomaly free policy editing and creation [14] [15] [16] [17] [18] [19] [20].

Anomalies present in multiple packet filters traversed by a packet within a domain have been studied and several types of anomaly identified as being similar to those found for single sets of filtering rules [14]. The use of binary decision diagrams (BDD's) to search for anomalies in distributed firewalls using static analysis techniques resulted in a firewall analysis tool being produced utilizing these techniques[16].

The significance of the definition of a security policy as the basis for an implementation was shown in [17]. Applications have been created to automate the conversion of security policy into a set of rules for use in routers e.g. Guarddog [18] but other than manufacturer's recommendations [19] little work has been carried out on optimization within a domain.

This paper investigates the significance of the delays encountered through the use of various ACL techniques. Factors which contribute to the delay incurred by packet passing through a router are identified and subsequently, a number of experiments were conducted to quantify these. Delays were investigated from a theoretical perspective which formed the basis of an equation which can be used to calculate the delay for a packet passing through a router running a particular OS. The equation was updated to reflect the packet delay experienced in a path across a domain. Recommendations were made to give guidance during the network design phase.

3. PACKET DELAYS WITHIN A DOMAIN

When considering the packet delay through a domain there are a number of factors that need to be considered. These factors include the route selected by the routing protocol, the bandwidth of the links along the selected route and the internal delays within the equipment. Routing Protocols optimize the route selection using a shortest path algorithm based on cost functions for each path. The delays experienced within equipment e.g. routers and switches are often ignored since the link bandwidth has generally been considered as the dominant factor. However as technology has improved the link speeds have increased and so the equipment delays have become more significant.

Analysing the delay within a domain will therefore depend on the route selected, which can be expressed as, the summation of delays through the components in the route. The link delays are easily calculated since they are proportional to the bandwidth. However the equipment delays are more difficult to quantify.

3.1. Delay measurement

From a theoretical point of view it is possible to identify the causes of delays within a router since it is basically a specialised computer system. Due to the real-time operation of the router OS they can be difficult to quantify. A practical approach was used to help identify the variation in delay caused by the nature of the processing used in routers.

A simple laboratory network was set up with the use of a dual ported Linux machine running Wireshark as a method of measuring delays across a router. An initial experiment was conducted to identify the accuracy of the measuring system by passing packets into a 100 Mbps hub and measuring the delay experienced on two of the outputs. Clearly this delay should be 0 but results from the experiment show that the average delay was 9 μsecs. This would be the error bar for a 100 Mbps network.

3.2. Delay caused by packet routing

Packets which enter a router via its network interface card are filtered by their destination network address using its routing table. The header is modified prior to the packet being sent to the port specified in the selected routing table entry. The delay of this process is dependent on the hardware components

3.2.1. Software and Hardware considerations

Performance of router hardware is highly variable since it is dependent on its underlying technology, including its processing power and memory capacity. Additionally, high throughput hardware can be purchased which exhibits performance improvements due to its specification. Networks typically comprise of equipment of varying ages which results in performance

variations. In this work, to enable other factors to be compared, consistent hardware has been used.

Router operating systems (OS) are optimised for routing of packets. Routers are also required to perform many other tasks which will be dependent on its feature set. A comparison of OS size and number of supported/running processes was undertaken using an OS with basic functionality and another with advanced services (Table 1).

	OS Size	**Number of Processes**	**Active Processes > 2**
Basic Functionality	12MBytes	73	32
Advanced Functionality	29MBytes	184	51

Table 1 – OS comparisons

If a core part of the OS is enhanced with additional functionality e.g. HTTP or DHCP Servers it can have an adverse effect on the size of the OS and its performance.

3.2.2. Measurement of Delays

Identical tests were undertaken using the ICMP ping command to quantify the delay across a router using an OS with basic and advanced functionality. Figure 2 clearly shows the difference in delays attributed to the OS version.

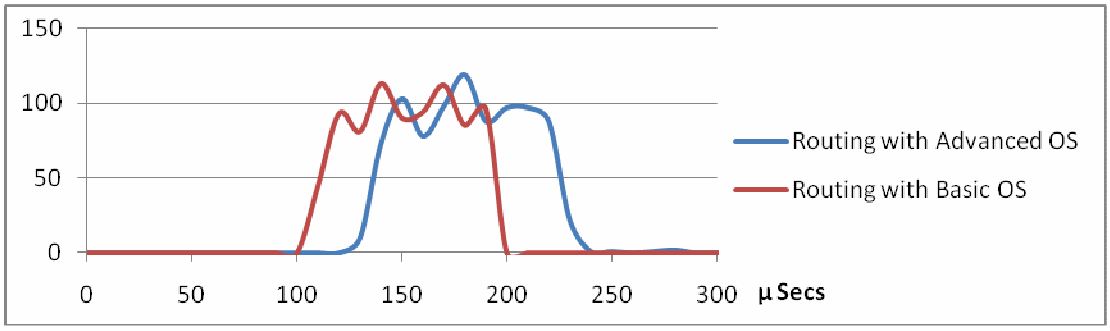

Figure 2. Delay through router

3.3. Delay as a result of implementing security

Security is typically implemented on a router using ACL's. Each rule is evaluated in turn until a matching rule is found. Standard ACL's only filter on the source IP address of a packet whereas extended ACL's provide the capability to filter on additional fields such as destination address, protocol and port numbers [20]. Figure 3 shows the delays associated with configuring ACLs.

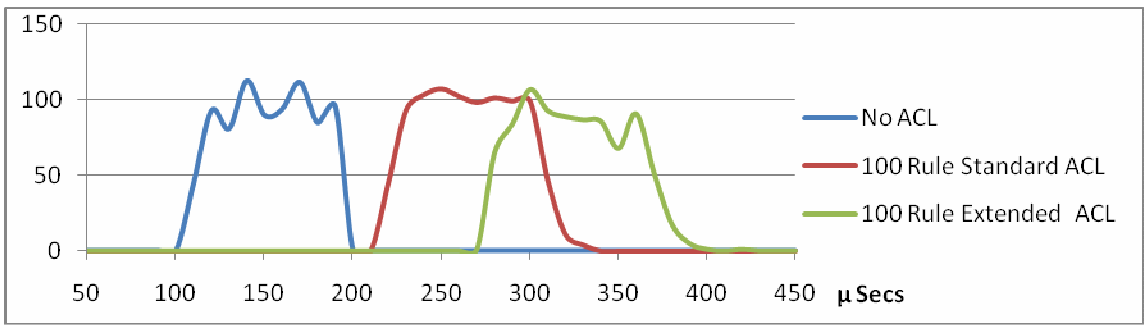

Figure 3. Delay through router with ACL running Basic OS

3.3.1. Effect of Number of Rules in ACL Basic OS

Measurements were made of the delay for packets matched against an increasing number of rules for both standard and extended ACL's. Figure 4 shows that for a Basic OS increasing the number of rules in the list have a significant effect on the delay.

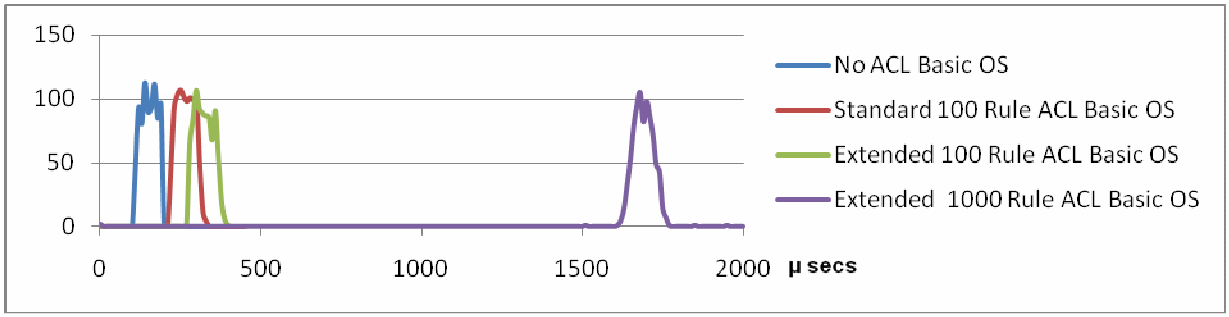

Figure 4. Delay through router with Basic OS

3.3.1. Effect of Number of Rules in ACL Advanced OS

Repeating the experiment using the same rules did not incur any additional delay using an OS with additional functionality (Figure 5).

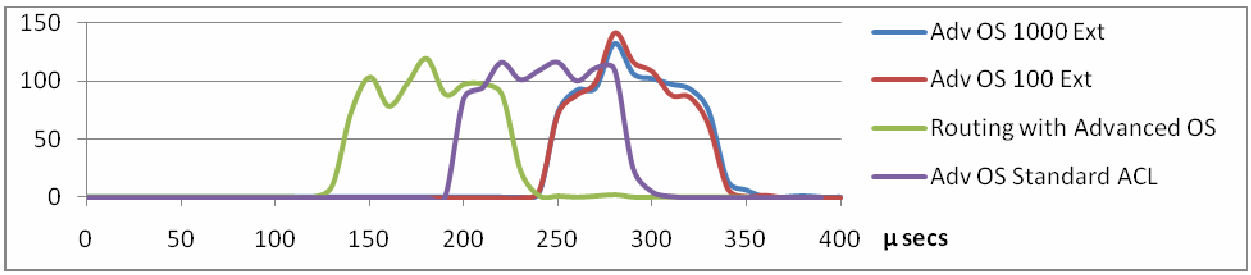

Figure 5. Delay through router with Advanced OS

4. Analysis of Delays within a Router

After considering the theoretical aspects of delays through routers then having carried out these measurements, modifications can be made to obtain a more realistic model. Additional by quantifying the parameters then a more simplified model can be created.

4.1. Theoretical approach to delays through a router

As discussed in the 3rd section a router is a specialized computer and therefore a basic equation can be defined by including parameters for the hardware (D_h), the operating system (D_{os}), the application configuration (D_a) and Services (D_s). Earlier work has shown that when configuring ACLs delays are introduced to the type of ACL (D_{ta}) used and the number of rules in an ACL D_{nr}. The model can be described as shown in the equation below.

$$\text{Router Delay } (D_r) = D_h + D_{os} + D_a + D_s + D_{ta} + D_{nr} + D_p$$

4.2. Quantifying parameters

The experiments provide results which were distributed over a large range of values. An average value of the range was calculated in order to provide a single value associated with each test. The results show that some parameters in the equation have a greater significance than others. The average delay for each parameter is shown in table 2.

IOS version	No ACL	Standard	Ext 100	Ext 1000
Basic	150	271	320	1685
Advanced	172	239	300	309

Table 2 – Average delays for all tests (times in µs)

4.3. Qualifying parameters

The results shown in table 2 indicate that there are significant differences in packet processing time depending on the OS version used.

4.3.1. Routing delays using Basic OS & Advanced OS

By using a router with a basic OS rather than an advanced OS it can be seen that standard routing is faster by around 15%. This is even without configuring any extra services on the advanced OS which it is expected would further increase the latency. When ACLs are configured then for a basic OS the average delay is increased by around 80% for a standard ACL and 110% for an extended ACL. However, by replacing the basic OS with an advanced OS and configuring a standard ACL saving of around 12% can be made and for an extended ACL 6%.

4.3.2. Effect of Number of Rules in ACL using Basic OS & Advanced OS

When using a router with a basic OS adding more rules to an ACL has a significant effect on the delays which can be of the order of 1400% for 1000 rules. The advantage of the advanced IOS functionality is that the number of rules using an ACL does not have an effect on the delay. This can be seen in figure 6.

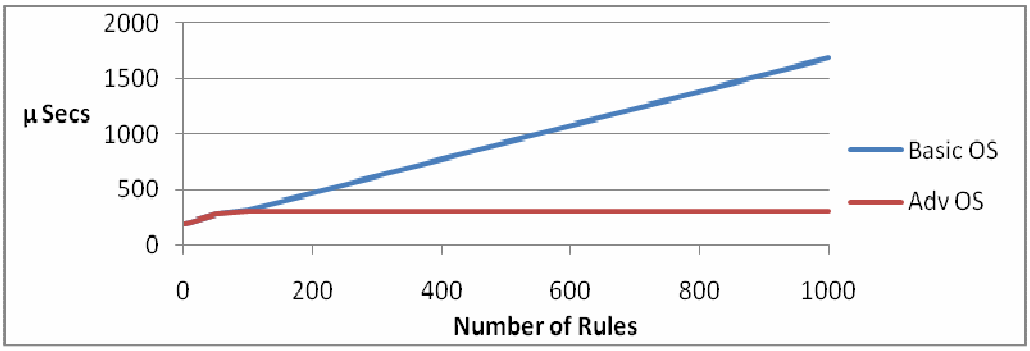

Figure 6. Delay v number of rules

5. DELAYS WITHIN A DOMAIN

Within a domain either static routes are configured or a routing protocol is used to select a route. Theoretically, the cumulative delay (D_d) for a given path can be calculated by the summation of the delays in the equation in 3.1 for each router (n) in the route.

$$\text{Domain } (D_d) = \sum_{i=1}^{n} D_{h[i]} + \sum_{i=1}^{n} D_{os[i]} + \sum_{i=1}^{n} D_{a[i]} + \sum_{i=1}^{n} D_{s[i]} + \sum_{i=1}^{n} D_{nr[i]} + \sum_{i=1}^{n} D_{p[i]}$$

6. CONCLUSIONS

By investigating the theoretical aspects of delays through routers and carrying out a series of measurements it has been possible to improve the mathematical model of delays encountered by a packet as it transverses a domain. It has also been possible to quantify the delays to understand

which components are more significant. This leads to a series of rules that can be used at best practice when designing large networks.

There are significant difference in the delays experienced using different versions of the Operating system in the router. More advanced OS add delays to the basic routing process but if other functionality is required then advanced OS have to be used.

Optimal performance can be gained by not having ACLs enabled in a router. Clearly it is not possible to remove the ACLs from all routers within a domain but there are gains to be made by reducing the number of routers that have ACLs enabled. By using an Advanced OS the number of rules in an ACL is insignificant. Since a domain has a common security policy then it should be possible to optimize the placement of ACL rules to ensure that the minimum number of routers in a domain use an ACL.

Having completed optimization on the number of routers requiring an ACL then using basic OS for router without ACL and using advanced OS for the routers that do require ACL will show an overall improvement of performance.

7. FUTURE WORK

These results have been produced for a fixed hardware configuration which was a very basic low end router and so further investigations can be carried out to understand the effect of more advanced hardware.

The effect of using additional functionality / services to the network within a router e.g. DHCP, HTTP were not studied. It would be expected that these could have considerable effects.

Optimization of the number of routers needing an ACL has not been addressed in this paper clearly there is further work to be done in this area to investigate automating the process.

REFERENCES

[1] Davies, J.N., Grout, V. & Picking, R. (2010) “Improving the Performance of IP Filtering using a Hybrid Approach to ACLs”, *8th International Network Conference INC 2010.*

[2] Grout, V., McGinn, J., Davies, J.N., Picking, R. & Cunningham, S. (2006) “Rule Dependencies in Access Control Lists”, *(IADIS) International Conference WWW/Internet 2006*

[3] Hari, B., Suri, S. & Parulkar, G. (2000) “Detecting and Resolving Packet Filter Conflicts”, *Proceedings of the 19th Joint Conference of the IEEE Computer and Communications Societies (INFOCOM00)*, pp1203-1212.

[4] Bukhatwa, F. & Patel, A. (2003) “Effects of Ordered Lists in Firewalls”, *IADIS International Conference*, 2003.

[5] Bukhatwa, F. (2004) “High Cost Elimination For Best Class Permutation in Access Lists”, *IADIS International Conference*, 2004.

[6] Al-Shaer, E.S. & Hamed, Hazem H. (2004) “Modelling and Management of Firewall Policies”, *Transactions on Network and Service Management.*, 2004

[7] El-Atawy, A., Hamed, H. & Al-Shaer, E. (2006) “Adaptive Statistical Optimization Techniques for Firewall Packet Filtering” *Infocom 2006,*

[8] Gupta, P. & McKeown, N. (2000) “Classifying packets with hierarchical intelligent cuttings”, *Micro, IEEE* , vol.20, no.1, pp.34-41, Jan/Feb 2000

[9] Singh, S. & Baboescu, F. (2003) Varghese, G. Wang, J. (2003) "Packet classification using multidimensional cutting", SIGCOMM '03, ACM, New York, NY, USA, pp. 213-224.

[10] Varghese, G. (2005) “Network Algorithmics”, Elsevier .

[11] Meiners, C.R., Liu, A.X. & Torng, E. (2007) "TCAM Razor: A Systematic Approach Towards Minimizing Packet Classifiers in TCAMs", *ICNP 2007. IEEE International Conference , pp.266-275, 16-19*

[12] Meiners et al (2010) “Hardware-based Classification for High-Speed Internet Routers” *Springer, 2010*

[13] Liu, A.X., Meiners, C.R. & Yun Zhou (2008) "All-Match Based Complete Redundancy Removal for Packet Classifiers in TCAMs," *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE pp.111-115, 13-18 April 2008*

[14] Al-Shaer, E.S. & Hamed, H.H. (2004) "Discovery of policy anomalies in distributed firewalls", *INFOCOM 2004. 23rd Annual Joint Conference of the IEEE Computer and Communications Societies , vol.4, no., pp. 2605- 2616 vol.4, 7-11 March 2004*

[15] Al-Shaer, E., Hamed, H., Boutaba, R. & Hasan, M. (2005) "Conflict classification and analysis of distributed firewall policies," *Selected Areas in Communications, IEEE Journal on , vol.23, no.10, pp. 2069- 2084, Oct. 2005*

[16] Yuan, L., Chen, H., Mai, J., Chuah, C.N., Su, Z & Mohapatra, P. (2006) "FIREMAN: a toolkit for firewall modelling and analysis," *Security and Privacy, 2006 IEEE Symposium on , vol., no., pp.15 pp.-213, 21-24 May 2006*

[17] Grout, V. & McGinn, J. (2005) “Optimisation of Policy-Based Internet Routing using Access Control Lists”, *9th IFIP/IEEE Symposium on Integrated Network Management (IM 2005), Nice, France, 15th-19th May 2005.*

[18] Guardog http://www.simonzone.com/software/guarddog/Accessed January 30 2011

[19] Cisco Systems, User Guide for ACL Manager 1.5, Optimizing ACLs http://www.cisco.com /en/US/products/sw/cscowork/ps402/products_user_guide_chapter09186a008017addf.html Accessed 4 February 2011, 2003

[20] Sedayao, J. (2001) Cisco IOS Access Lists. O’Reilly, pp. 22,31