Rhodes University
Department of Computer Science
Security and Network Research Group
SNRG
Project Proposal
Computer Science Honours Project
Project Title: Firewall Rule Set Optimization

Mungole Mukupa
g10m6851

Supervisor: Mr Barry Irwin

March 7, 2010

1 Abstract

Packet filtering is a critical role in any computer networking environment [1]. Optimisation of packet filtering rule sets is important in ensuring that packet filtering brings about the increase in throughput and traffic management.The continuous growth of networks, the desire to collaborate on business transaction and the moving of most business functions to computerised Information Systems has brought challenges in the aspects of trust, confidentiality, integrity and safety of data and the systems that host it [6]. The general semantics for optimising firewall rule sets mostly consider packet filtering based on packet characteristics. [2] In this project, we seek to explore other packet and traffic characteristics for optimising firewall rule sets to achieve the desired performance increase but keep the system secure. The optimization approaches and techniques will then be used to design a tool that will aid network administrators in rule set optimisation.

2 Statement of Work

Firewalls inspect packets against a rule set sequentailly until a match is found. This project seeks to investigate if firewall rule set optimization offers a gain

in filtering performance. Also to design and implement a tool for helping administrators in optimising firewall rule sets. This is aimed at inproving firewall performance and simply rule set manipulation with regard to optimization. This is in response to the ever increasing network speeds and transmission technologies.

3 Background

A Firewall is a combination of hardware and software working to filter and manage packets in a computer network environment [7]. Packet filtering is based on rule sets configured in the firewall. These rules are based on security policies of an organisation's IT infrastructure framework. The basic work of a firewall is to control traffic between networked zones of different trust levels [4]. An internal network would be qualified as a trusted zone but it receives packets over different media from other networks through third parties like ISPs, and these are not trusted sources [5]. Firewall technologies came into play late in 1980s through pioneering works of companies like CISCO Systems Inc. They have since grown from being primary devices for filtering traffic to complex hybrid implementations including features like Quality of Service (QOS), Intrusion Prevention Systems (IPS), Bandwidth Management, traffic shaping among others [3]. This is because the need to share data has brought many challenges with a large number of threats originating from outside a network posing danges to the networks and the data they host.

4 Project Goals/ Deliverables

Many aspects of firewall rule set bulding will be explored to come up with additional features to include in optimizing the firewall rule set and designing of the optimizer tool; OptAid. The project therefore is looking to:

- To investigate ways of reducing the rule matching time to improve packet matching time by optimizing the rule set using various approaches that will be found.
- Design and implement a tool that will help in rule set optimizing.
- Present the findings in a document that can be used for further research.

5 Literature Review

Material on firewalls, security policies, rule sets design and implementation, packet filtering algorithms and other firewall security publications will be read and reviewed to build on the already existing work in this research area :

- Books on Firewalls, Network Designs and their Implementation

- Performance based materials on packet networks and packet filtering
- Programming techniques as used in Java and C/C++
- Research publications on Information Security Conferences and projects as they relate to packet discrimination.

6 Methodology

The research will take a detailed look at the current firewall systems available, review their design, performance and the rules manipulation to pick one for test purposes. The targets for this are:

- IPFW (FreeBSD)
- PF (FreeBSD)
- IPTables (Linux

This will also include looking at real world information security breaches at firewall level. Environment specific considerations will take centre stage once a firewall platform is chosen. A test environment will be set up to conduct performance testing. The test results will then be used to as a basis for developing the tool mentioned earlier.

7 Requirements

To achieve this, we will require various tools and materials for analysis, design, testing and information extraction. The ones listed below are not exhaustive of the ones to be used as the list will be revised according to project demands.

- FreeBSD operating system.
- Linux operating system.
- Firewall Builder.
- C/C++ or Java environment.
- Reading material on TCP/IP Networks and Information Security.
- Books on firewalls, information security, technical reports, security conference publications.
- Online publications on new approaches for Firewall Building.
- Dedicated Computer set, provided lab PC.
- other tools as the project demands.

8 Schedule

The project is timelined as shown in the table below:

TASK	MILESTONE	PERIOD
Requirements gathering	Project Proposal	First Term
Literature review	Understand Firewall Semantics	First Term
Set up environment	FreeBSD and Linux OS working	First Term
Documentation	Documentation	First Term
Rule set design		Second Term
Continue materail review		Second Term
Work on design	Conceptual design	Second Term
Documentation	Document	Second Term
Start designing		Third Term
Revise rule set		Third Term
Tool development	Tool Prototype	Third Term
Tool Testing		Third Term
Documentation	Documentation	Third Term
Submit Short Paper	Short Paper	Fourth Term
Implement Tool changes		Fourth Term
Tool Testing		Fourth Term
Perfect Tool Design	Working Tool	Fourth Term
Hand in deliverables	Completion	Fourth Term
Project closure		Fourth Term

References

[1] Alok Tongaonkar, N. I., and Sekar, R. Inferring higher level policies from firewall rules.

[2] Andreasson, O. Iptables tutorial 1.2.2. Available on : http://iptables-tutorial.frozentux.net/iptables-tutorial.html Accessed 13 Feb 2010.

[3] D., R. *Cisco Router Firewall Security.* Pearson Professional Education, 2004.

[4] FreeBSD, F. *FreeBSD Handbook 2010.* FreeBSD Document Project, 2010.

[5] Harrison, P. Iptables. Available on: http://www.linuxhomenetworking.com; Accessed 17 Feb 2010.

[6] K, O., and D., T. *Linux Network Administrators Guide.* ORielly, 2000.

[7] Shimonski R.J, Shinder D.L, D. S. T. *Best Damn Firewall Book Period*. Syngress, 2003.