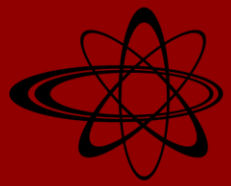


SNRG
Security and Networks Research Group

FIREWALL RULE SET OPTIMIZATION

Author Name: Mungole Mukupa

Supervisor : Mr Barry Irwin

Security and Networks Research Group

Department of Computer Science

Rhodes University

RHODES UNIVERSITY
Where leaders learn

Presentation Overview

- Introduction
- Background
- Objectives
- Method /Tools
- Deliverables
- Close up

Background

“ *People often think that having a firewall between your internal network and the “Big Bad Internet” will solve all your security problems. It may help, but a poorly setup Firewall System is more of a security risk than not having one at all”.*

FreeBSD.org Security

Firewall: Originally meant a heavy brick wall built between buildings or rooms to prevent fire spreading either way.

Firewall in computing is hardware/software or combination in a network, allowing or denying entry/exit of data based on the set rules.

Objectives

Review current Firewall systems in

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

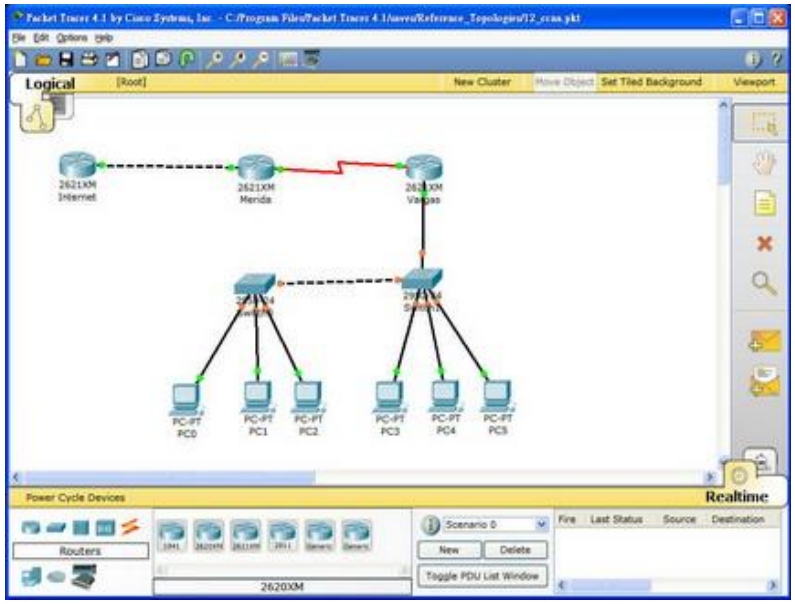
- Analyse current rule set basing schemes

- Come up with a tool for optimising firewall rules

- Build on the existing Firewall rule creating practices to achieve better rule sets

Method & Tools

- Network simulation
- Protocol specific packets
- FreeBSD operating system (Release 8/9)
- Linux Operating System (Kernel V.2.6.33)
- Developing environment in C++/Java



Deliverables

•A tool for dynamic rule set analysis and aiding in the optimization

•A defined criteria for coming up with Firewall rules that are case specific

•A Firewall rule set optimised for Faster processing performance, security, Quality of Service —Throughput Sensitive

•A testing environment for Packet Filtering using the optimised rules

•Analytical report on the comparison of IPFW, PF and IPtables

Any