Distributed Firewall for Linux

MSC IN COMPUTER SCIENCE

THARANGA ABEYSEELA

UNIVERSITY OF MORATUWA
SRI LANKA

October, 2007

Distributed Firewall for Linux

Tharanga Abeyseela

This dissertation was submitted to the

Department of Computer Science and Engineering

Of the

University of Moratuwa

In partial fulfillment of the requirements of the

Degree of MSc in Computer Science

Department of Computer Science and Engineering
University of Moratuwa
Sri Lanka

October, 2007

To my loving parents

Who have dedicated their entire life for my education...

DECLARATION

I declare that the work included in the dissertation in part or whole has not been submitted for any other academic qualification at any institution.

Tharanga Abeyseela

(Candidate)

Mr Shantha Fernando

(Supervisor)

Abstract

The number of attacks on connected hosts has increased over the last several years [1], making the security of networks an increasingly important problem. Attacks have become more automated and can cause greater amount of damage. This increase in attacks coincides with an increased use of the Internet and with increases in the complexity of protocols, applications, and the internet itself. Critical infrastructures increasingly rely on the internet for operations. Individual users rely on the security of the internet, email, the web, and web-based applications to a greater extent than ever. Thus, a wide range of technologies and tools are needed to counter act the growing threat. At a basic level, cryptographic algorithms for confidentiality and authentication assume greater importance in network security .One of the most common ways that networks are hardened against attack is to tightly control what kind of network traffic can enter and exit the network using a firewall.

Due to developments in distributed systems and network technologies, computer systems are operated in different geographical locations with different security policies and procedures. So managing and monitoring the firewalls in distributed environments have increased the system engineers and network administrator's daily workload.

Proposed distributed firewall can operate in a centralized location (using client-server architecture) and securely propagates firewall rules to remote nodes. Wireless Short Messaging Service (SMS) has integrated as a distributed node monitoring tool in this research. And also the simple user friendly firewall rule generation engine has changed the conventional IPTABLE rule implementation. Those features not only reduce the workload of engineers but also prevent the system failures and enhanced the security measures in the distributed environment.

This work discusses the design and implementation of the distributed firewall concept, its implementation and preventing single point of failure in the architecture.

Acknowledgement

This work would not have been possible without the guidance, support and help of many individuals and parties. My heartfelt gratitude and thanks to all of you.

This effort would be both inconceivable and unlikely without the ever present leadership and mentoring of my supervisor Mr. Shantha Fernando. Thank you dear sir for all you did and always being there for me. I could not have wish for a better guide, both intellectually, as a mentor, as well as a person.

My eternal gratitude and respect to my dearest parents and brother, without whose unconditional love, encouragement and vision, this would be never possible. I also take this opportunity to thank my “Loku amma” Mrs. Kamala Gunawardena for her support during the research work.

Dr Sanath Jayasena, Msc Coordinator needs to be especially acknowledged for his support both at an administrative level as a mentor. I would also like to thank the rest of the CSE staff for their support and guidance.

My sincere thank go out to the management of Roomsnet International, especially the CEO Mr. Eric Wikramanayake, and Mr. Nadeep de silva for their understanding, flexibility and tolerance.

My heartfelt thank you to all my colleagues specially Jeewantha, Amila, Samitha, Charith, Sumedha, & Hirantha for all the understanding, support, knowledge sharing and trust. But most of all thank you guys, for your friendship and simply being there for me when ever I needed you.

Last but not least, I would like to thank my beloved wife Randika for her love, support and encouragement during my research work. Thank you Randi for all you did for me, and also needs to be especially acknowledged her family for their love and support.

October 27, 2007

Table of Contents

List of Figures

List of Tables