Tree Rule Firewall

A Thesis Submitted for the Degree of

Doctor of Philosophy

By

Thawatchai Chomsiri

in

Faculty of Engineering and Information Technology

UNIVERSITY OF TECHNOLOGY, SYDNEY

17th November 2016

CERTIFICATE

Date: 17th November 2016

Author: Thawatchai Chomsiri

Title: Tree Rule Firewall

Degree: Ph.D.

I certify that this thesis has not already been submitted for any degree and is not being submitted as part of candidature for any other degree.

I also certify that the thesis has been written by me and that any help that I have received in preparing this thesis, and all sources used, have been acknowledged in this thesis.

Signature of Author

Acknowledgements

I am greatly indebted to my supervisor, Professor Xiangjian (Sean) He, for his scholarly guidance, inexhaustible patience, constant encouragement, and invaluable suggestions. He is a nice, generous, helpful and hospitable person. I feel happy and comfortable with him during my PhD study. Many thanks are also expressed to my co-supervisors, Dr. Priyadarsi Nanda, for his valued suggestions and constantly technical supports. I appreciatively acknowledge the useful suggestion from Dr. Zhiyuan (Thomas) Tan. His suggestions help me to improve many paper publications of my research. I also gratefully acknowledge useful discussions with my team mainly consisting of Dr. Mian Ahmad Jan, Dr. Mohammed Ambusaidi and Dr. Aruna Jamdagni. I appreciate the supports, which I received from the Faculty of Engineering and Information Technology, and its staff. I appreciate the financial assistance, International Research Scholarship (IRS), which I have received from Graduate Research School - University of Technology Sydney. Lastly, I would like to thank my father (Mr. Weera Chomsiri), my mother (Ms. Darawadee Chomsiri) and members of my family for everything.

Table of Contents

List of Tables

List of Figures

Abbreviation

Abbreviations	Descriptions
2D-Box	Two Dimensions Box
ACL	Access Control List
Cent OS	Community ENTerprise Operating System
ConnTrack	Connection Tracking
CPU	Central Processing Unit
DEC	Digital Equipment Corporation
Dest IP	Destination IP Address
Dest Port	Destination Port
DIP	Destination IP Address
DMZ	Demilitarized Zone
DPT	Destination Port
DstIP	Destination IP Address
DstPT	Destination Port
ESXi	Elastic Sky X – integrated (ESXi is the primary component in the VMware Infrastructure software suite)
FDD	Firewall Decision Diagram
GHz	Gigahertz
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol

Abbreviations	Descriptions
Hyper-V	is formerly known as Windows Server Virtualization
IOS	Cisco's Internetworking Operating System
IP	Internet Protocol
IPSEC	Internet Protocol Security
LAN	Local Area Network
Max	Maximum
Mbps	Megabits per second
Min	Minimum
NICs	Network Interface Cards
OS	Operating System
PVFS	Procfs Virtual File System
RAM	Random-Access Memory
SIP	Source IP Address
SrcIP	Source IP Address
SrcPT	Source Port
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VM	Virtual Machine

Abstract

Firewall is a network component for deciding packets whether they will be accepted or denied. The packet decision results are dependent on rule policy pre-defined by firewall administrators. In traditional firewalls, the rule policy will be arranged in a list of rule line called 'listed rule'. The listed rule can cause three significant problems consisting of speed, security, and user friendly problems. The speed problems can occur because many packets will be matched with the rule positioned in bottom positions. Firewall may waste time to verify packets with many rules positioned above the matched rule. Moreover, the traditional firewalls also face to rule conflicts, e.g., shadowed rules. Many rules written to prevent attacking packets may be shadowed by some rules above them and cannot block any packet so that dangerous packets originated from outside can reach internal networks. Additionally, the traditional firewalls are involved with the lack of user-friendly features because administrators must have enough experience in order to create enough efficiency rules.

This research proposes a novel firewall by using a tree structure of rules to solve the above problems. In the proposed approach, firewall administrators are able to design rules in the tree format, and then a core processor of firewall will process packets according to this format. The tree structure can be seen in both users' view and firewall's view. Packets will be verified with the tree shape of rule called 'tree rule'. To decide packet, searching for a data in the tree rule can be done quickly in comparison to searching data in the listed rule of traditional firewalls. This is because searching data in the Tree is faster than sequential searching data in Arrays. Moreover, rule conflicts can be eradicated, since each packet will be verified with the corresponding 'rule path' in the tree rule. This can avoid rule conflicts and shadowed rules. Thus, security problems

caused by shadowed rules cannot be found in the tree rule firewall. Moreover, administrators can create rules easier with the GUI (Graphical User Interface) rule editor. They can design tree rule by creating nodes and links. There are ranges of IP addresses or ports inside each node. The GUI can sort the data inside nodes automatically and maintain consistency of the rule. Thus, the tree rule can be designed easily.

Therefore, the Tree-Rule firewall can provide faster functional speed, be more secure, and be easier to use compared to traditional Listed-Rule firewalls.

Papers from the Thesis

1. **T. Chomsiri**, X. He, P. Nanda, "Limitation of listed-rule firewall and the design of tree-rule firewall", in: Proceedings of the 5th International Conference on Internet and Distributed Computing Systems, China, 2012, pp. 275–287.

2. X. He, **T. Chomsiri**, P. Nanda, Z. Tan, "Improving cloud network security using the Tree-Rule firewall", **Future Generation Computer Systems**, Elsevier, 30 (2014) 116-126. [ERA **Tier-A** Journal, **IF=2.430**, SCImago Journal Rank: **Q1**]

3. **T. Chomsiri**, X. He, P. Nanda, Z. Tan, "A Stateful Mechanism for the Tree-Rule Firewall", IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom2014), 2014, pp. 122-129. [ERA **Tier-A** conference]

4. **T. Chomsiri**, X. He, P. Nanda, Z. Tan, "Hybrid Tree-rule Firewall for High Speed Data Transmission", **IEEE Transactions on Cloud Computing**, 2016, no. 1, pp. 1, PrePrints, doi:10.1109/TCC.2016.2554548. [SCImago Journal Rank: **Q1**]

5. **T. Chomsiri**, X. He, P. Nanda, Z. Tan, "An Improvement of Tree-Rule Firewall for a Large Network: Supporting Large Rule Size and Low Delay", IEEE 15th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom2016), 2016, pp. 178-184. [ERA **Tier-A** conference]