A STUDY OF ENTERPRISE SOFTWARE SUPPORT ON nDPI

By

Gregorius Aldo Radityatama

11302005

Bachelor's Degree

in

Information Technology

Faculty of Engineering and Information Technology

SWISS GERMAN UNIVERSITY

The Prominence Tower

Jalan Jalur Sutera Barat No. 15, Alam Sutera

Tangerang, Banten 15143 - Indonesia

August 2017

A STUDY OF ENTERPRISE SOFTWARE SUPPORT ON nDPI

By

Gregorius Aldo Radityatama

11302005

Bachelor's Degree

in

Information Technology

Faculty of Engineering and Information Technology

SWISS GERMAN UNIVERSITY

The Prominence Tower

Jalan Jalur Sutera Barat No. 15, Alam Sutera

Tangerang, Banten 15143 - Indonesia

August 2017

Revision after the Thesis Defense on 19 July 2017

Statement by the Author

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

Gregorius Aldo Radityatama

Student Date

Approved by:

Charles Lim, MSc., ECSA, ECSP, ECIH, CEH, CEI

Thesis Advisor Date

Ir. Heru Purnomo Ipung, M.Eng.

Thesis Co-Advisor Date

Dr. Ir. Gembong Baskoro, M.Sc.

Dean Date

Abstract

A STUDY OF ENTERPRISE SOFTWARE SUPPORT ON nDPI

By

Gregorius Aldo Radityatama

Charles Lim, MSc., ECSA, ECSP, ECIH, CEH, CEI Advisor

Ir. Heru Purnomo Ipung, M.Eng. Co-Advisor

SWISS GERMAN UNIVERSITY

Next Generation Firewall (NGFW) adds new capabilities of a standard firewall with an ability to inspect packets' contents, thus increasing precision. Three main usages of NGFW are to improve the Quality of Service (QoS) of a business, as an application-based filtering firewall, and to protect the network from known malware. A complete NGFW system has three main components: Deep Packet Inspection (DPI), Intrusion Prevention System (IPS), and an extra-firewall intelligence mechanism. Out of these three components, an essential part is the Packet Inspection engine. One example of open-source DPI implementations is called nDPI. The purpose of this thesis is to design and implement protocols needed by nDPI so that it has better enterprise-grade software support. To achieve this, this thesis analyzes 5 (five) various applications and their unique identifiers in each of the packets. Then, an additional set of rules will be added to the existing one. To test and validate, there will be a measurement of precision and performance of nDPI compared to the original, and to the commercial implementation of NGFW. As the result, it is proven that nDPI can be improved with new protocols at more than 90% of accuracy, with CPU execution time increase of less than 3,5% and less than 1% of peak heap memory increase.

Keywords: Next Generation Firewall, Deep Packet Inspection, Protocol Identification, nDPI

Dedication

I dedicate this thesis to my beloved country, Indonesia. Also, I dedicate this thesis to my lecturers and colleagues that helped and supported me to the completion of this thesis.

Acknowledgement

I would like to thank my thesis advisors, Charles Lim, MSc., ECSA, ECSP, ECIH, CEH, CEI and Ir. Heru Purnomo Ipung, M.Eng. for their help and guidance so that I am able to finish this research.

I also give my thanks to friends and family for their care and support.

Contents