

A STUDY OF ENTERPRISE SOFTWARE SUPPORT ON nDPI

By

Gregorius Aldo Radityatama

11302005



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



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

SWISS GERMAN UNIVERSITY

Ir. Heru Purnomo Ipung, M.Eng.

Thesis Co-Advisor

Date

Dr. Ir. Gembong Baskoro, M.Sc.

Dean

Date

Gregorius Aldo Radityatama

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



SWISS GERMAN UNIVERSITY

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

Statement by the Author	2
Abstract	3
Dedication	5
Acknowledgement	6
Contents	9
List of Figures	10
List of Tables	12
1 Introduction	13
1.1 Background	13
1.2 Research Problems	14
1.3 Research Objectives	15
1.4 Significance of Study	15
1.5 Research Questions	15
1.6 Hypothesis	15
1.7 Research Scope	16
1.8 Limitations	16
1.9 Thesis Structure	16
2 Literature Review	18
2.1 History of Firewall	18
2.2 Next Generation Firewall	19
2.3 Deep Packet Inspection	20
2.3.1 Use Cases of Deep Packet Inspection	20
2.3.2 Components of Deep Packet Inspection	21
2.3.3 nDPI: Open-Source High-Speed Deep Packet Inspection	21

2.3.4	Libprotoident	22
2.3.5	nDPI and libprotoident	24
2.4	Various Methods to Identify Application Protocols	25
2.5	Challenges in Application Identification and Deep Packet Inspection	25
2.6	Enterprise Applications	26
2.6.1	Salesforce.com	28
2.6.2	Zendesk	28
2.6.3	Yammer	28
2.6.4	Adobe Creative Cloud	29
2.6.5	Microsoft Sharepoint	29
2.7	Related Works	29
3	Methodology	33
3.1	Research Methodology	33
3.2	Research Framework	33
3.3	Extraction	36
3.4	Evaluation	36
3.5	Validation	37
4	Experimental Results	38
4.1	System Overview	38
4.2	Preparation	39
4.3	Pre-Data Collection	40
4.4	Data Collection	41
4.5	Pre-Extraction	42
4.6	Rule Extraction	43
4.7	Rule Implementation and Pre-Measurements	45
4.8	Evaluation	46
4.8.1	Precision	46
4.8.2	Performance	47
4.9	Analysis	51
4.10	Limitations	52

5 Conclusion	53
5.1 Recommendation	54
5.2 Future Works	54
6 Glossary	55
Bibliography	56
A Protocol Rule List	60
B Data Collection Automation Steps	63
B.1 Salesforce	63
B.2 Zendesk	63
B.3 Adobe Creative Cloud	64
B.4 Yammer	64
B.5 Sharepoint	65
C Extraction Results - Found IP Addresses	66
D Extraction Results - Found Domain Names	71
E Curriculum Vitae	76

SWISS GERMAN UNIVERSITY