

**ANALYSIS OF HYBRID DDOS DEFENSE USING ANYCAST
TO MITIGATE DDOS IMPACT**

By
Gede Barkah Widagdo
22014208

MASTER'S DEGREE
in
INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY
EduTown BSD City
Tangerang 15339
Indonesia

February 2016

**ANALYSIS OF HYBRID DDOS DEFENSE USING ANYCAST
TO MITIGATE DDOS IMPACT**

By
Gede Barkah Widagdo
22014208

MASTER'S DEGREE
in
INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY
EduTown BSD City
Tangerang 15339
Indonesia

Revision after the Thesis Defense on 1st February 2016

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 acknowledgment is made in this thesis.

Gede Barkah Widagdo

Date

Approved by:

Dr. Maulahikmah Galinium, S.Kom, M.Sc

Thesis Advisor

Date

SWISS GERMAN UNIVERSITY

Charles Lim, M.Sc

Thesis Co-Advisor

Date

Dr. Ir. Gembong Baskoro, M.Sc

DEAN

Date

Gede Barkah Widagdo

ABSTRACT

ANALYSIS OF HYBRID DDoS DEFENSE USING ANYCAST TO MITIGATE DDoS IMPACT

By

Gede Barkah Widagdo

Swiss German University
Bumi Serpong Damai

Dr. Maulahikmah Galinium, S.Kom, M.Sc., Advisor
Charles Lim, BSc., MSc., Co-Advisor

Distributed Denial of Service (DDoS) attack is a huge threat for online business. The toughest challenge defending against DDoS attacks is where the attacker has many botnets and distributed the internet so they have capability to overwhelm the selected node. (Specht and Lee, 2004) classified DDoS attack into 2 classification are bandwidth depletion and resource depletion attack. Bandwidth depletion attack such as ICMP Flood and NTP Amplification, and Resource depletion attack such as SYN Flood and Slowloris Attack, those are among the most popular type of DDoS attack in 2014 - 2015. High volume of IP datagrams, huge number of packet and huge number of connections can causing a denial of service in the victim side. With this kind of attack, defenses at the victim are useless because legitimate traffic is suppressed before it even reaches the victim. An effective solution must be "in" the network, where it can drop traffic before damage or reach the victim. Some mitigation techniques have been proposed, but no one has proposed DDoS defense to mitigate bandwidth depletion and resource depletion as a package of DDoS defense. Hybrid DDoS Defense is an attempt to fill the gap. The idea is how to drop traffic before it gets to the victim. Hybrid DDoS Defense met this criteria, Hybrid DDoS defense put firewalls in multiple locations and one location is the center of the services to be protected, a firewall is use for sanitize the traffic so web server only received legitimate request. Hybrid DDoS defense tested by bandwidth depletion and

resource depletion attack, result is traffic distributed to multiple nodes so as to weaken DDoS attacks, it lighten the firewall to sanitize the incoming traffic then send legitimate traffic to the server (the target of attack).

Hybrid DDoS defense deployment have capability to mitigate both of DDoS attacks classification are bandwidth depletion and resource depletion until 90%. In addition, we showed the comparison of DDoS defense in the victim deployment and hybrid deployment.



Keywords: Denial of Services, Anycast, Bandwidth Depletion, Resource Depletion



SWISS GERMAN UNIVERSITY

DEDICATION

I would like to dedicate this research project to my beloved country, Indonesia. I believe this thesis research can contribute to the advancement of science and technology in Indonesia, no matter how subtle.



ACKNOWLEDGMENT

I would like to express my deepest gratitude to Mr. Maulahikmah Galinium and Mr. Charles Lim, for the time, support, advice, and guidance given throughout this research project and the completion of this thesis report. It is because of their priceless contributions that this thesis report and the whole research project can arrive at this point.

I would like to thank all of my friends for their companionship and to the countless number of people who have helped me throughout this research project, either directly or indirectly.

Last, but the most important, I would like to thank my whole family especially my wife for the countless moral supports throughout my life. It is because of their guidance that I become the person as who I am today. It is because of their affections that I become as happy as I am today.



SWISS GERMAN UNIVERSITY

TABLE OF CONTENTS

STATEMENT BY THE AUTHOR	2
ABSTRACT	3
DEDICATION	6
ACKNOWLEDGMENT	7
LIST OF FIGURES	11
LIST OF TABLES	14
1 INTRODUCTION	17
1.1 Background	17
1.2 Research Problem	19
1.3 Research Objective	20
1.4 Research Question	20
1.4.1 Scope of Research	22
1.5 Significance of Study	22
1.6 Hypothesis	22
1.7 Thesis Structure	23
2 LITERATURE REVIEW	24
2.1 The Internet Environment	24
2.1.1 Security awareness of Internet user	24
2.1.2 Security policy in the Internet	24
2.1.3 Internet Layer Design Flaw	25
2.1.3.1 Network and Transport Layer Flaw	26
2.1.3.2 Application Vulnerability	28
2.2 Threat Model	28
2.3 Denial of Service Attack	28
2.4 Distributed Denial of Service Attack	29
2.4.1 Bandwidth Depletion Attack	29
2.4.1.1 Flood Attack	29
2.4.1.2 Amplification Attack	30



SWISS GERMAN UNIVERSITY

2.4.2	Resource Depletion Attack	30
2.5	BGP Anycast	31
2.6	Firewall	31
2.7	DDoS Defense Based on Location Deployment	32
2.7.1	Source Network	32
2.7.2	Intermediate Network	33
2.7.3	Victim Network	33
2.8	Related Works	34
3	METHODOLOGY	36
3.1	Network Model	36
3.2	Threat Model	37
3.3	Simulation Architecture	38
3.3.1	Network Layer Rules	39
3.3.2	Transport Layer Rules	39
3.3.3	Application Layer Anti DDoS	39
3.3.4	Web loadbalancer	39
3.3.5	Bandwidth Depletion Attack	40
3.3.5.1	ICMP Flood	40
3.3.5.2	NTP Amplification Attack	40
3.3.6	Resource Depletion Attack	40
3.3.6.1	SYN Attack	40
3.3.6.2	Slow HTTP Get Attack (Slowloris)	41
3.4	Evaluation	41
4	EXPERIMENTS AND RESULTS	42
4.1	Experimental Setup	42
4.1.1	Hardware and Software	42
4.1.2	Virtual Machine Configuration	42
4.1.3	IOS on Unix Configuration	43
4.1.4	Network Simulation Scenarios	43
4.1.5	Distributed Firewall	44
4.1.6	Cluster Web Server	44
4.1.7	Network Topology Scenarios	45
4.2	Attack Scenario and Result	46
4.2.1	DDoS Defense Deployment against Bandwidth Depletion Attack, ICMP Flood Attack	46

4.2.1.1	Victim DDoS Defense Deployment against ICMP Flood Attack	46
4.2.1.2	Hybrid DDoS Defense Deployment against ICMP Flood Attack	52
4.2.2	DDoS Defense Deployment against Bandwidth Depletion Attack, Amplification Attack	59
4.2.2.1	Victim DDoS Defense Deployment against NTP Amplification	59
4.2.2.2	Hybrid DDoS Defense Deployment against NTP Amplification	64
4.2.3	DDoS Defense Deployment against Resource Depletion Attack, SYN Flood Attack	71
4.2.3.1	Victim DDoS Defense Deployment against SYN Flood Attack	71
4.2.3.2	Hybrid DDoS Defense Deployment against SYN Flood Attack	75
4.2.4	DDoS Defense Deployment against Resource Depletion Attack, Slow HTTP GET Attack	83
4.2.4.1	Victim DDoS Defense Deployment against Slow HTTP GET Attack	83
4.2.4.2	Hybrid DDoS Defense Deployment against Slow HTTP GET Attack	87
4.3	Summary and Observation	94
5	CONCLUSION	102
5.1	Recommendations	103
5.2	Future Work	103
A	GLOSSARY	105
B	CONFIGURATION AND SCRIPT	106
	REFERENCES	111
C	CURRICULUM VITAE	115