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

Charles Lim, M.Sc
Thesis Co-Advisor Date

Dr. Ir. Gembong Baskoro, M.Sc
DEAN Date

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 of Denial of Service (DDoS) attack is a huge threat for online business. The thoughtest 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

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.

TABLE OF CONTENTS