Security Test of Indonesian E-Health Community Cloud Model Test Bed on PRAGMA Cloud

Arie Surachman[1], Sri Chusri Haryanti[2], Ummi Azizah Rachmawati[3], Sri P. U. Atmoko[4],Rosini[5]
Faculty of Information Technology, Universitas YARSI, Indonesia
abiegailz@outlook.com[1]; sri.chusri@yarsi.ac.id[2]; ummi.azizah@yarsi.ac.id[3]; puji.atmoko@yarsi.ac.id[4]; rosini@yarsi.ac.id[5]

Introduction & Aim

Application of cloud computing in health sector nowadays keeps growing. Cloud computing has been implemented by some countries to revolutionize health sector. Indonesia is planning to use a cloud for e-Health. Indonesian e-Health cloud deployment model had been proposed. However, the eHealth Community Cloud model still needs a further complement. In this research, we perform a test bed of Indonesian e-Health community cloud model on PRAGMA Cloud. We set a virtual firewall and intrusion detection system for the cloud, furthermore exercise some security test against DDoS attacks.

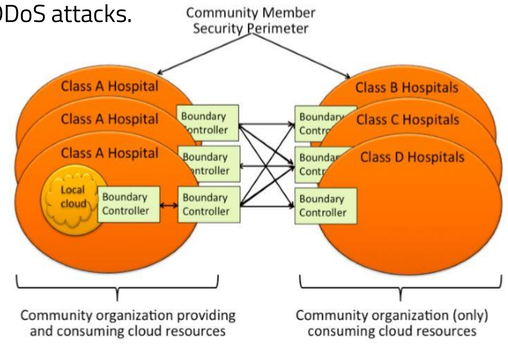

Figure 1 Indonesian e-Health Community Cloud Model

Topology

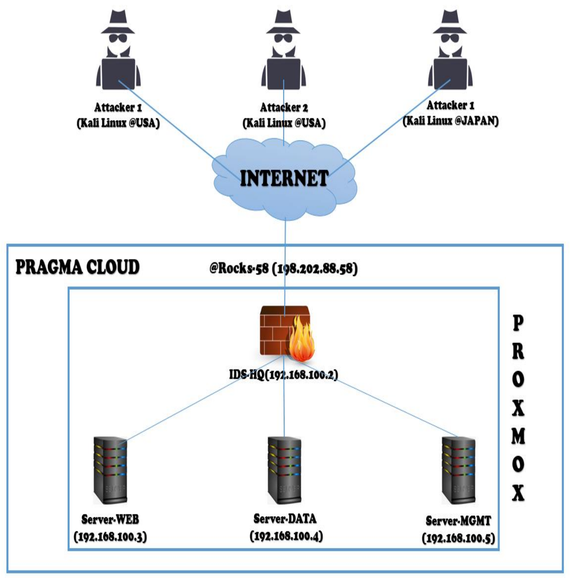

Figure 2 Topology

Method

We apply iptables & netfilter on the virtual firewall and Snort for IDS in securing the cloud model. We carried out some testing of distributed denial of service (DDoS) attacks. The Indonesian e-Health community cloud model is implemented on PRAGMA Cloud in Indiana University site, and the attackers are on San Diego Supercomputer Center (SDSC), the United States and Nara Institute of Science and Technology (NAIST), Japan.

Hardware & Software Specification

Table 1 Hardware and Software Specification

Unit	CPU	RAM	HDD	OS
Rocks-58 ProxmoxVE (198.202.88.58)	1 x Intel(R) Xeon(R) CPU E5520 @ 2.27 Ghz (1 Socket)	1Gb Ram 2133 Mhz	60 Gb	Debian 8 Jessie Integrated With Proxmox VE 4.4
IDS-HQ (192.168.100.2)	1 x Intel(R) Xeon(R) CPU E5520 @ 2.27 Ghz (1 Socket)	512 Mb Ram 2133 Mhz	20 Gb	Ubuntu Server 14.04 Trusty Tahr
Server-WEB (192.168.100.3)	1 x Intel(R) Xeon(R) CPU E5520 @ 2.27 Ghz (1 Socket)	512 Mb Ram 2133 Mhz	8 Gb	Ubuntu Server 14.04 Trusty Tahr
Server-DATA (192.168.100.4)	1 x Intel(R) Xeon(R) CPU E5520 @ 2.27 Ghz (1 Socket)	512 Mb Ram 2133 Mhz	8 Gb	Ubuntu Server 14.04 Trusty Tahr
Server-MGMT (192.168.100.5)	1 x Intel(R) Xeon(R) CPU E5520 @ 2.27 Ghz (1 Socket)	512 Mb Ram 2133 Mhz	8 Gb	Ubuntu Server 14.04 Trusty Tahr

There are four virtual servers inside Proxmox server: IDS-HQ as a firewall, Server-WEB, Server-Data and Server-MGMT

Experiments

In our experiments, the attackers exploit Slowloris.pl script to penetrate the web server.
We performed two test scenarios. In the first scenario, the cloud work without any security scheme. DDoS attacks launch and the average time that the cloud survives in the attacks is recorded. In the second scenario, DDoS attacks performed to the cloud that implements iptables, netfilter, and Snort to verify the ability to retain DDoS.

Results

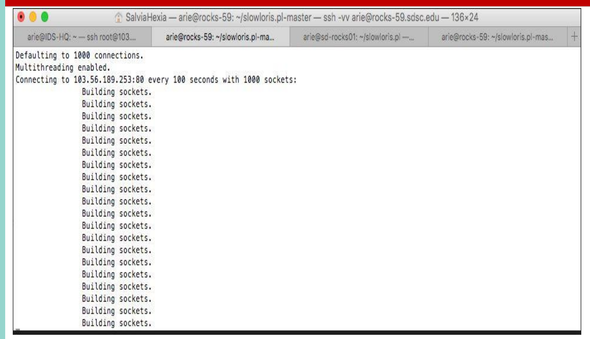

Figure 3 Penetration test to the Cloud. Attacker send 1000 packets into server.

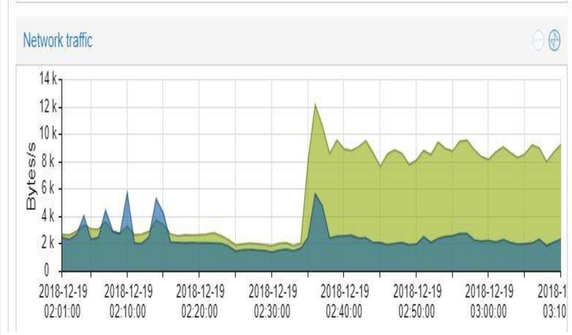

Figure 4 Increasing of network traffics from attacker into IDS-HQ, making the server is busy and inaccessible.

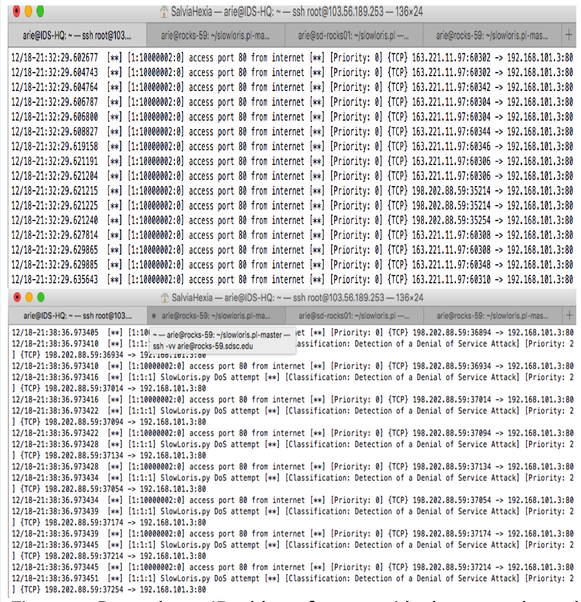

Figure 5 Snort shows IP address from outside the networks and gives alerts that there are DDoS potentials.

Discussion

From the experiment, if three attackers together perform DDoS attack to the cloud server without any security scheme in 300 seconds, the average time of the server before being inaccessible is 197.5 seconds with the standard deviation is 49.38 seconds. The experiment result yields that the cloud which implements iptables, netfilter, & Snort, manage to block the attacker IP address and survive from DDoS attacks.

Future Work

In the future, a security system that has more rules for Snort originating from outside and inside the network will be formulated. Other methods for IDS also will be exercised to improve the security of the cloud.

References

Deshmukh, R. V. and Devadkar. K. K. (2015). Understanding DDoS Attack & Its Effect in Cloud Environment. Procedia Computer Science, 49, pp.202-210.

Haryanti, S. C., Pradipta, A., Atmoko, S. P. U., Rachmawati, U. A., Suhartanto, H. (2017). Indonesian E-Health Community Cloud. Poster, SEAIP 4-8 Desember 2017, Taiwan.

Modi, C., dkk. (2013). A survey of instrusion detection techniques in Cloud. Journal of Network and Computer Applications, 42-57(36).

Munir. (2016). Statistik Pendidikan Pengantar Analisis Data untuk Penulisan Skripsi & Tesis, Jember.

Simon, M.C. Cheng. (2014). Proxmox High Availability. Packt Publishing Ltd. Pp. 41 – ISBN 978-1-78398-089-5.

Somani, G., Gaur, M.S., Sanghi, D., Conti, M. And Buyya, R. (2017). DDoS attacks in cloud computing : Issues, taxonomy, and future directions. Computer Communications, 107, pp.30-48.

Acknowledgements

Funded through a grant from the Indonesian Ministry of Research, Technology and Higher Education, No. SP DIPA-042.06.1.40156/2018-contract No. 014/INT/UM/WRII/UY/V/2018.
We would also like to show our gratitude to PRAGMA community for permission utilizing PRAGMA Cloud.