Implementation of Virtual Firewall Mechanism for Security of Indonesian E-Health Cloud Model

Sarah Syahwenni Utari
Sri Chusri Haryanti
Ummi Azizah Rachmawati

PRAGMA 34
May 11, 2018.
Akihabara, Tokyo

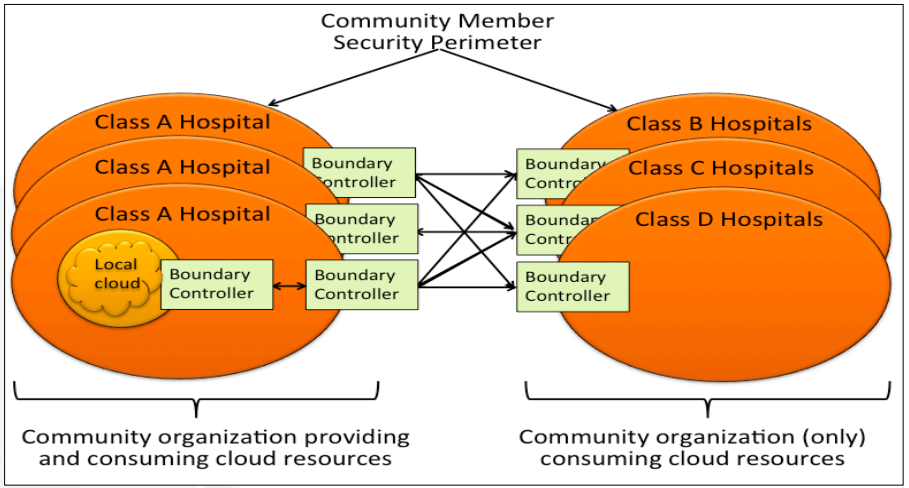
Our Works

1. Implementation of virtual firewall mechanism for Indo nesian e-health cloud model from DDoS attacks.
2. Proxmox VE is used in the virtualization environment .
3. Modification of ConfigServer & Firewall (CSF) and DDoS blocking script is used to block IPs from Attackers.
4. Two scenarios of experiment

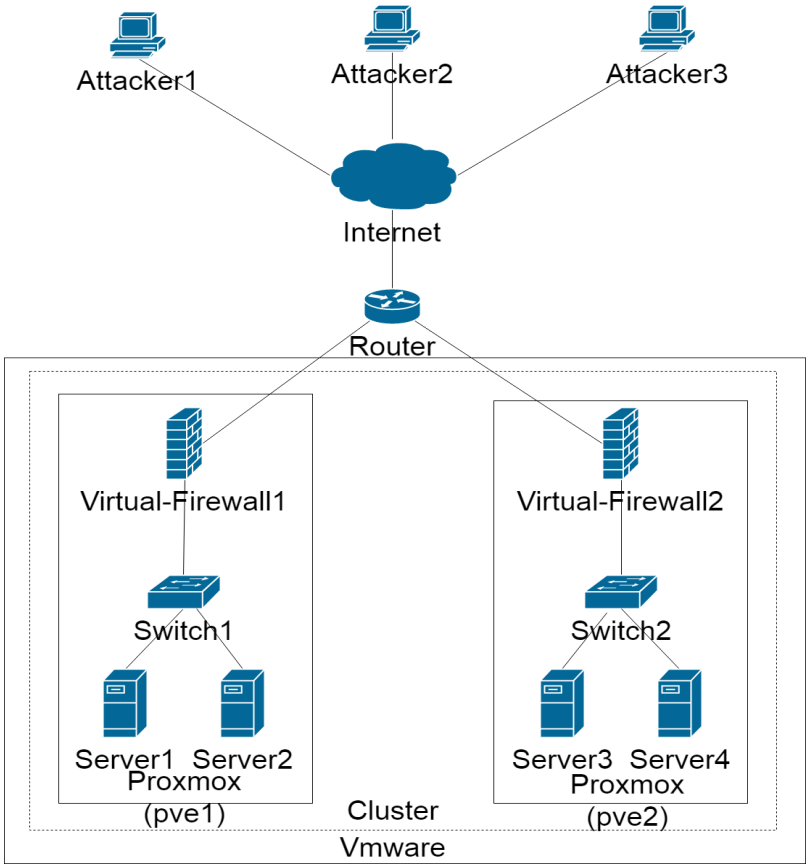
Topology

Tolopogy

Indonesian E-Health Community Cloud Model



The topology used is an adaptation of the Indonesian E-Health Cloud Deployment Model (Haryanti, S.C et al, 2017).



Software and Hardware

Software and Hardware

Node

- OS : Proxmox VE 4.4
- Memory : 5.9 GB
- Processors : 4
- Hard Disk (IDE) : 100 GB
- Network Adapter1 : Custom (VMnet2)
- Network Adapter2 :
- Custom (VMnet2)
- Network Adapter3 :
- Bridged

Virtual Router

- OS : Ubuntu Server 14.04
- Memory : 512.00 MB
- Processors : 1
- Hard Disk : 8 GB (local-lvm)
- Network Adapter1 : Bridge (vmbr1)
- Network Adapter2 : Bridge (vmbr2)

Virtual Server

- OS : Ubuntu Server 14.04
- Memory: 512.00 MB
- Hard Disk : 8 GB (local-lvm)
- Network Adapter1 : Bridge (vmbr2)

Attacker

- OS : Kali Linux
- Memory : 1 GB
- Hard Disk (IDE) : 20 GB
- Network Adapter1 :
- Custom (VMnet2)

Pseudocode

Pseudocode

If (Client require Server)
Client IP address is filtered by CSF
At CSF

Step 1: Identification of incoming client

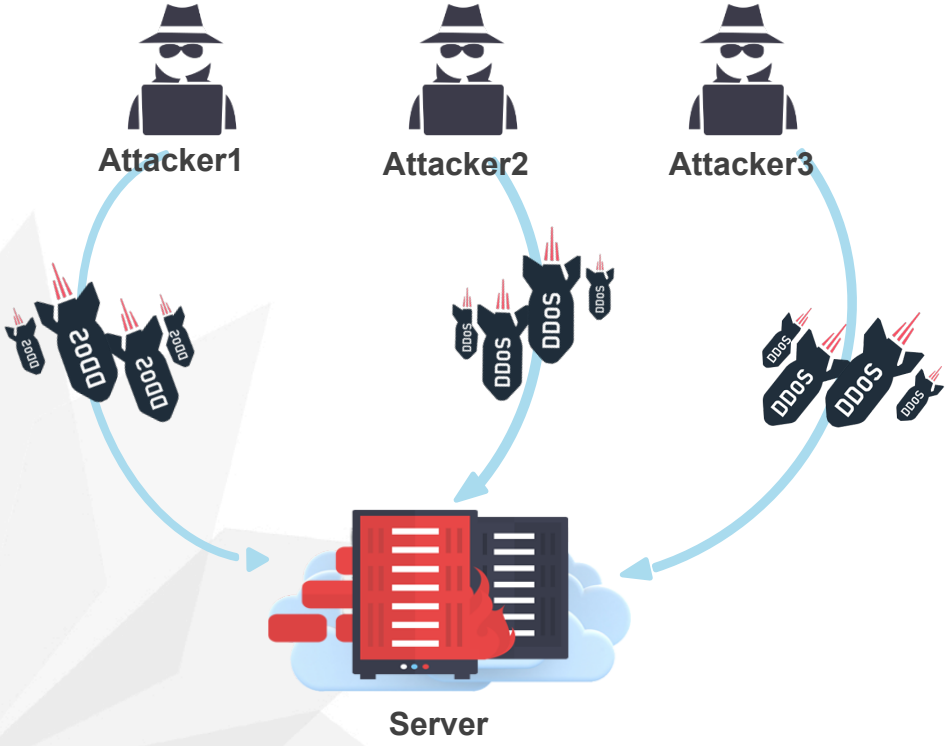
*If (Client IP address is not found in **/etc/csf/csf.allow** (Client IP))*
*ADD Client IP to **/etc/csf/csf.allow** (Client IP)*
*Else If (**/etc/csf/csf.allow** (same Client IP) > N [within session BAN_PERIOD])*
*MOVE Client IP to **/var/log/ddos.log***
*BLACKLISTED use **ddos-blocking.sh** filtered at **ddos-blocking.conf***
Alert DDoS Attack
Else
*Client IP address is found in **/etc/csf/csf.deny** (Client IP))*
can't access to Server.

Step 2 : Monitoring the request rate

If (for any Client IP (REQUEST < = MAX_PACKET))
*Forward Client IP to **csfposh.sh** to PROTECTED SERVER*
Else
*MOVE Client IP to **/var/log/ddos-blocking.log***
*BLACKLISTED use **ddos-blocking.sh** filtered at **ddos-blocking.conf***
Alert DDoS Attack.

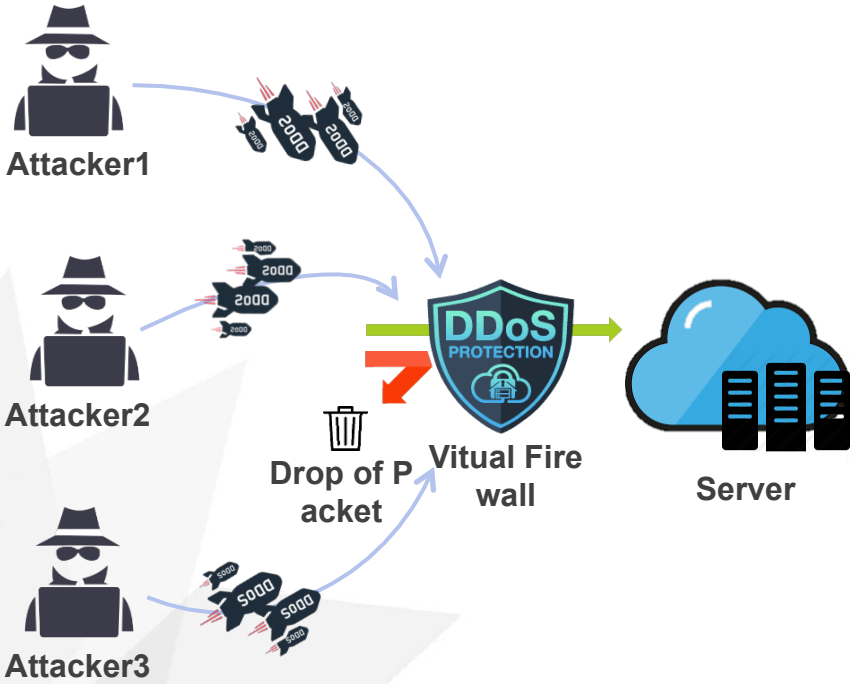
Experiment

The First Scenario

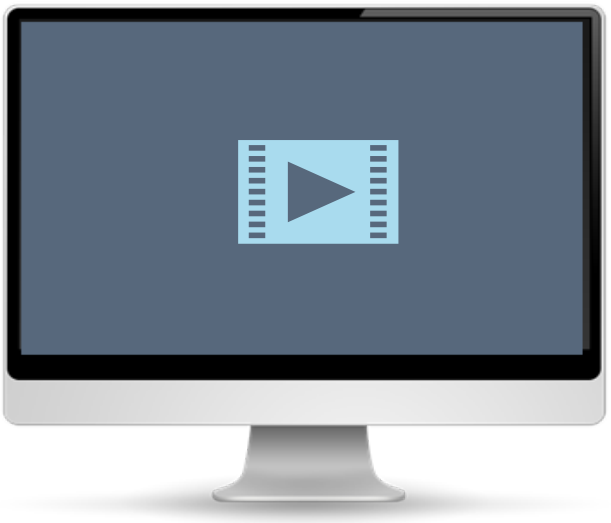


- Attacker1, Attacker2, and Attacker3 perform the DDoS attack with slowloris.pl script until the server is inaccessible
- Time per attack is 300 seconds

The Second Scenario



- On virtual router, we added vir tual firewall (SCF) and script o f DDoS-blocking script
- Attacker1, Attacker2, and Atta cker3 perform the DDoS attac kes with slowloris.pl script



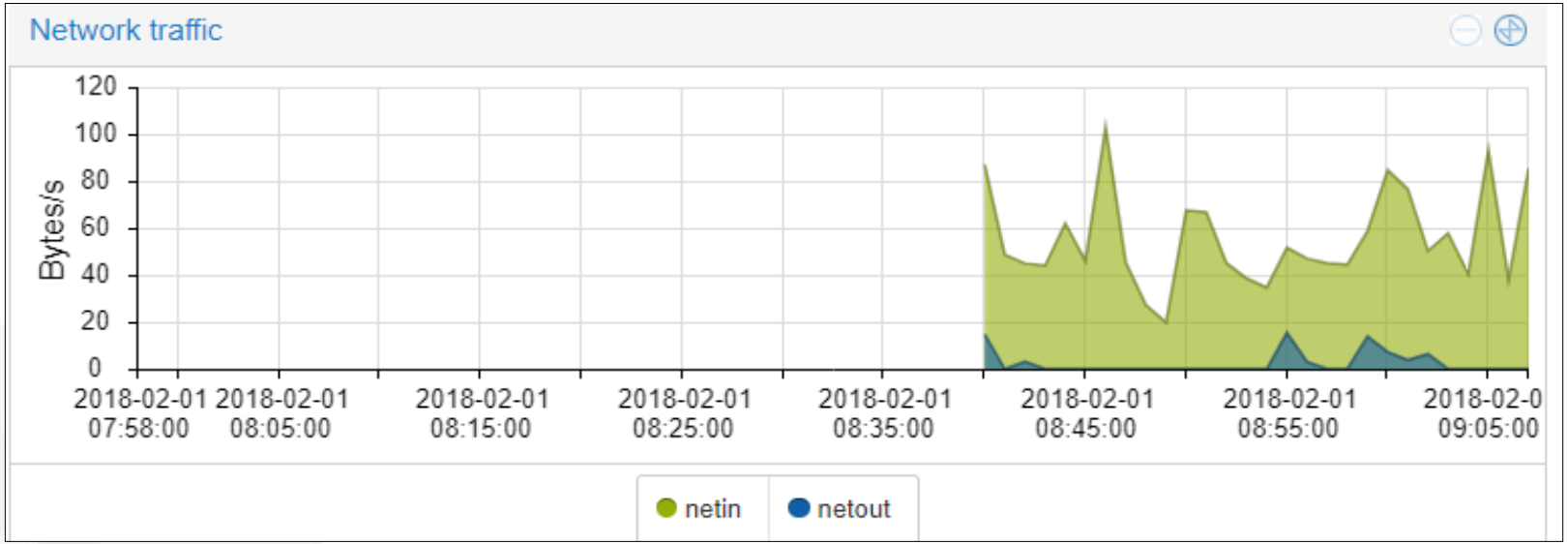
First Scenario

Second Scenario

Results

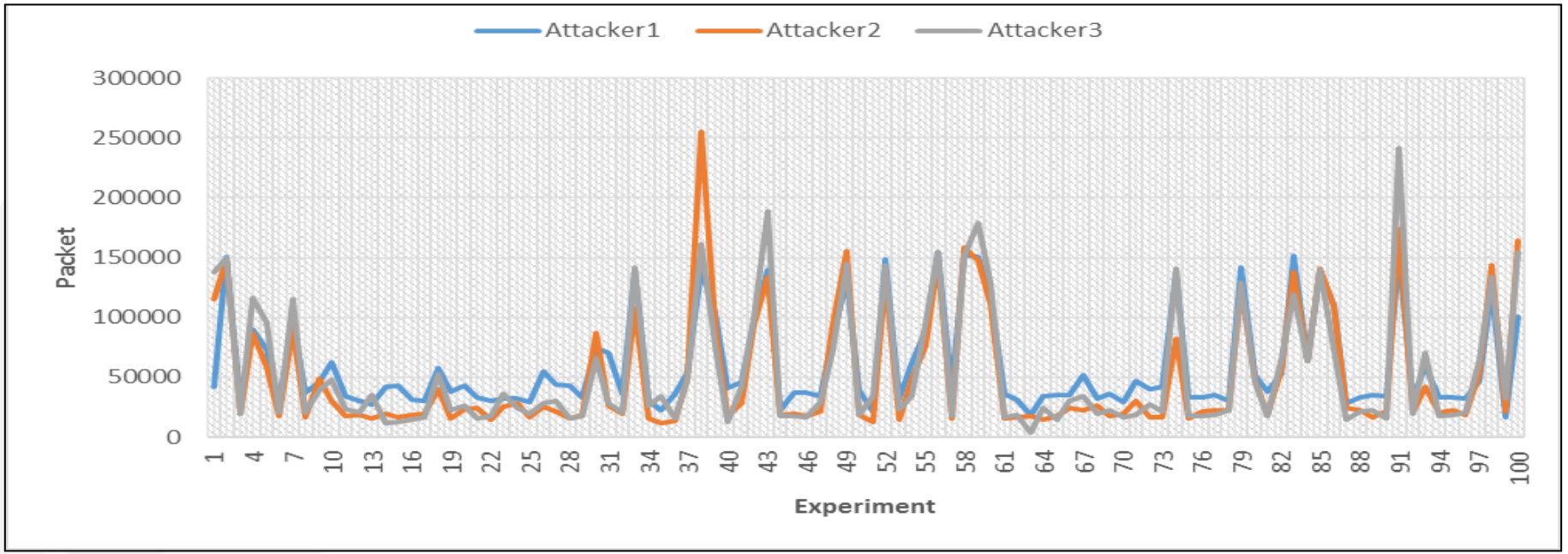
Result of The First Scenario

Traffic Network of First Scenario



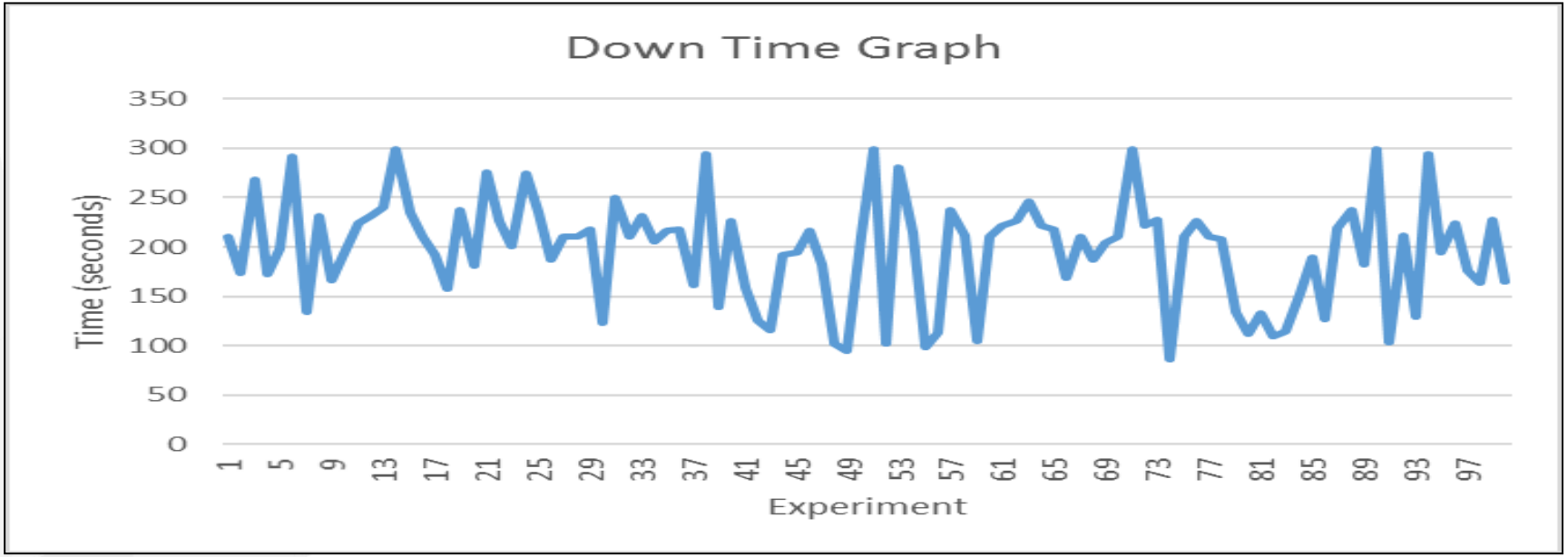
Result of The First Scenario

Graph of Attack on First Scenario



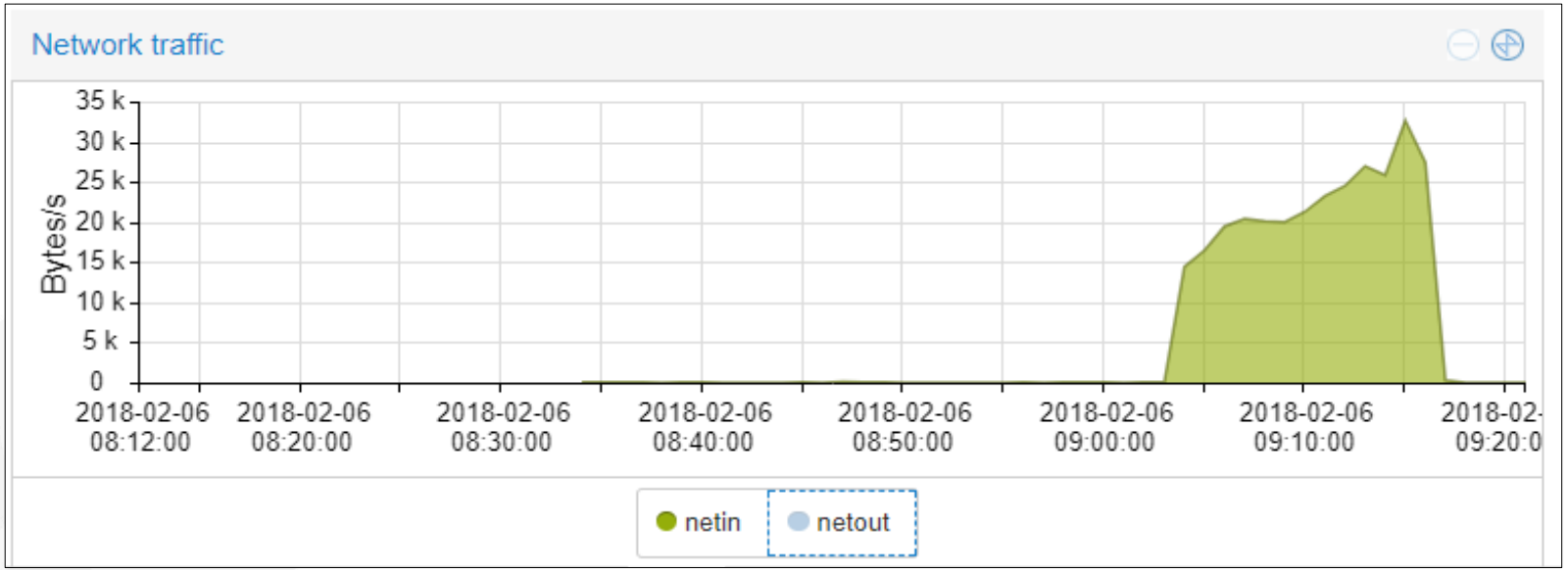
Result of The First Scenario

Downtime Graph on First Scenario



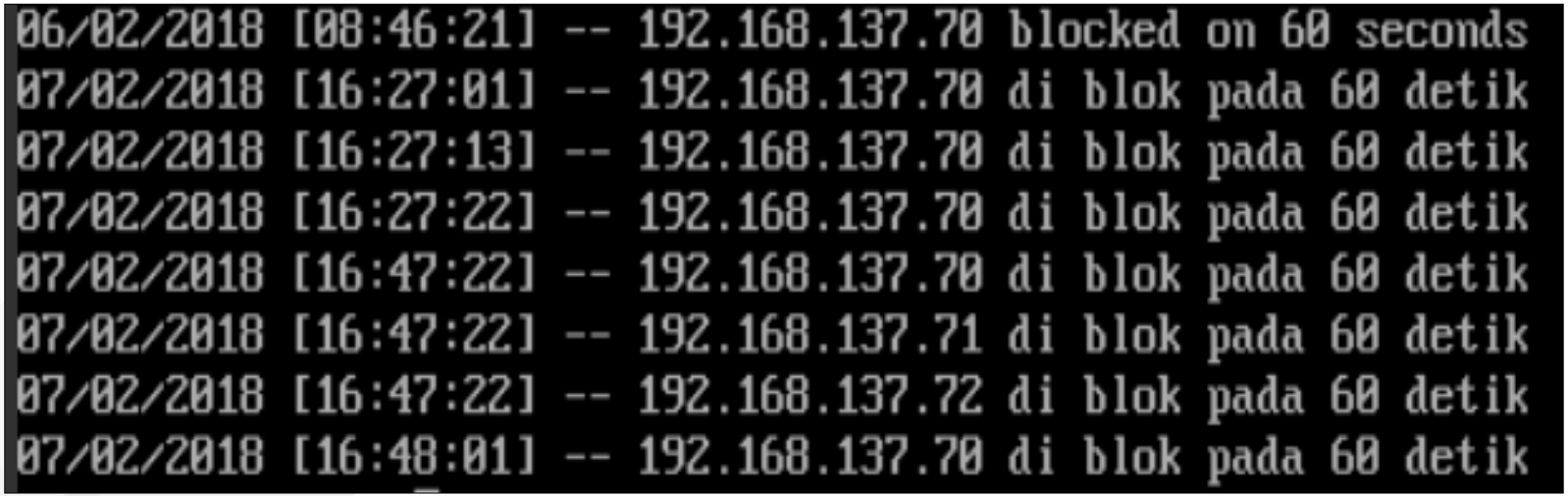
Result of The Second Scenario

Traffic Network of Second Scenario



Result of The Second Scenario

Blocklist IP Addresses



Conclusion

Conclusion

Virtual firewall by modifiying CSF on Ubuntu Server 14.04 for Indonesian e-health cloud model is working successfully

The result obtained from the 1st scenario is that the average downtime is 197.26 seconds with the standard deviation is 52.99 seconds before a server was down because of DDoS attackes.

The result of the 2ns scenario show that virtual firewall managed to block the attacker IP address and the server could withstand from DDoS attacks

Future Work

- **a security system can be designed to filter the DDoS attackes originating from within the network.**
- **The e-Health cloud security model would be tested in a testbed.**

References

[1] 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.

[2] Singh, B., Mahajan, R., Panda, S.N. and Samra, G.S., **2016**. *Detecting DDOS Attacks in Cloud-A Novel Approach*. International Journal of Computer Science and Information Security, 14(5), p.292.

[3] Al Nuaimi, N., AlShamsi, A., Mohamed, N., & Al-Jaroodi, J. (**2015**, March). *e-Health cloud implementation issues and efforts. In Industrial Engineering and Operations Management* (IEOM), 2015 International Conference on (pp. 1-10). IEEE.

[4] Ahmed, E.S.A. and Elatif, R.E., **2015**. *Network denial of service threat security on cloud computing a survey*. International Journal of Scientific Research in Science, Engineering and Tecnology, 1(5), pp. 341-50.

[5] Islam, T., Manivannan, D., & Zeadally, S. **2016**. *A classification and characterization of security threats in cloud computing*. Int. J. Next-Gener. Comput, 7(1).

[6] Mishra, A., dkk. **2013**. *Cloud Computing Security*. *International Journal on Recent and Innovation Trends in Computing and Communication, 36-39*(1).

[7] 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.

Thank you