INTISARI

IMPLEMENTASI *NETWORK INTRUSION PREVENTION SYSTEM* MENGGUNAKAN SNORT PADA INFRASTRUKTUR JARINGAN *CLOUD* OPENSTACK

Penggunaan jaringan *cloud computing* yang semakin tren belakangan ini memacu untuk mengembangkan sistem keamanan jaringan untuk sistem tersebut. Banyak perusahaan yang masih ragu berpindah dari infrastruktur fisik ke infrastruktur *cloud* karena keamanannya dinilai lebih rentan terhadap serangan. Penggunaan *firewall* dan antivirus dinilai belum cukup untuk melindungi jaringan *cloud* yang tehubung ke internet. Pada penelitian ini penulis meneliti tentang kinerja dari sistem kemanan yang bisa digunakan pada jaringan *cloud*. Salah satu sistem keamanan yang digunakan untuk melindungi jaringan dari serangan adalah *Network Intrusion Prevention System (NIPS)*. Peneliti menggunakan *platform* openstack untuk membuat infrastruktur *cloud*. Aplikasi *Network Intrusion Prevention System (NIPS)* yang digunakan adalah snort. Snort mendeteksi dan memberitahukan terjadi sebuah gangguan atau serangan kemudian langsung memberi respon, respon berupa *block* dan mencatat *log*. Kinerja *Network Intrusion Prevention System (NIPS)* dianalisis berdasarkan bagaimana responnya terhadap serangan dan tingkat akurasi dalam mendeteksi serangan.

Kata Kunci: *Openstack, Network Intrusion Prevention System, Snort.*

ABSTRACT

IMPLEMENTATION OF NETWORK INTRUSION PREVENTION SYSTEM USING SNORT IN CLOUD NETWORK INFRASTRUCTURE OPENSTACK

The use of increasingly recent cloud computing networks is spurring to develop a network security system for the system. Many companies are still hesitant to move from physical infrastructure to cloud infrastructure because its security is considered more vulnerable to attack. The use of firewalls and antivirus is not enough to protect the cloud network connected to the internet. In this study, the authors examine the performance of the security system that can be used on the cloud network. One of the security systems used to protect the network from attack is the Network Intrusion Prevention System (NIPS). Author use the Openstack platform to create cloud infrastructure. The Network Intrusion Prevention System (NIPS) application used is snort. Snort detects and notifies an interruption or attack then responds instantly, the response is block and logs. The Network Intrusion Prevention System (NIPS) performance is analyzed based on how they respond to attacks and the accuracy of detecting attacks.

Keywords: *Openstack, Network Intrusion Prevention System, Snort.*