

BAB 1

PENDAHULUAN

1.1. Latar Belakang

Cloud computing merupakan teknologi yang menggunakan jaringan internet untuk mengakses layanannya. Layanan yang disediakan seperti *Software as Service* (SaaS), *Platform as Service* (PaaS), dan *Infrastructure as Service* (IaaS). Namun ketika suatu teknologi seperti *cloud computing* yang memberikan layanannya terhubung dengan internet, keamanan merupakan salah satu yang perlu diperhatikan. Salah satu isu utama pada *cloud computing* adalah melindungi *cloud* dari serangan pada jaringan [1]. Serangan yang dapat dilakukan pada jaringan seperti *port scan*, *ping of death*, *ip spoofing*, maupun paket *sniffing*. Untuk mencegah serangan tersebut banyak dari penyedia layanan *cloud* menggunakan *firewall* untuk menangani serangan [1]. Namun menggunakan *firewall* tidak menjamin layanan *cloud computing* dapat terhindar dari serangan di jaringan. Karena dalam lingkungan *cloud computing* dimana sumber daya komputasi dan komunikasi dapat diakses bersama oleh beberapa pengguna sehingga serangan dapat berasal dari infrastruktur itu sendiri [2]. Oleh karena itu perlu adanya deteksi serangan di jaringan dari luar maupun dalam sistem *cloud*, salah satunya dengan menggunakan *Intrusion Detection System* (IDS).

IDS merupakan aplikasi yang dapat mendeteksi aktivitas yang mencurigakan dalam jaringan maupun pada sistem komputer. Dengan menggunakan IDS, lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada aktivitas mencurigakan pada jaringan. Sehingga dengan adanya IDS yang diimplementasikan pada sistem *cloud* diharapkan dapat mendeteksi serangan di jaringan.

Dari penelitian sebelumnya oleh C.Mazzariello dkk, terdapat 2 peletakan IDS yang diusulkan yaitu IDS terpisah dengan server *cloud* dan IDS pada server *cloud* [2]. Dalam Tugas Akhir ini IDS akan diimplementasikan ke dalam sistem *cloud computing* dengan 2 skenario dari penelitian sebelumnya ditambah dengan skenario IDS ditempatkan pada keduanya (pada server *cloud* dan terpisah dengan

server *cloud*). Kemudian pengaruh IDS terhadap penggunaan CPU dan memori pada server *cloud*.

1.2. Rumusan Masalah

Adapun rumusan masalah pada tugas akhir ini adalah sebagai berikut,

1. Bagaimana membangun infrastruktur sistem *cloud computing* (*private cloud*)?
2. Bagaimana mengimplementasikan IDS pada sistem *cloud computing*?
3. Bagaimana keberhasilan deteksi dengan serangan dari luar dan dalam pada sistem *cloud* yang dibangun jika,
 - a. IDS ditempatkan terpisah dengan server *cloud*?
 - b. IDS ditempatkan pada server *cloud*?
 - c. IDS ditempatkan pada keduanya (pada server *cloud* dan terpisah dengan server *cloud*)?
4. Bagaimana pengaruh IDS terhadap penggunaan CPU dan *memory* pada server *cloud* yang di bangun?

1.3. Batasan Masalah

Batasan masalah pada tugas akhir ini adalah sebagai berikut,

1. Tugas akhir ini difokuskan untuk meneliti pengaruh peletakan IDS terhadap keberhasilan deteksi serangan luar maupun dalam sistem *cloud*.
2. Framework yang digunakan untuk membangun sistem *cloud* adalah proxmox ve.
3. Jaringan yang dibangun adalah jaringan LAN berbasis IPv4.
4. IDS menggunakan snort.
5. Jenis IDS yang digunakan yaitu *Network-based Intrusion Detection System* (NIDS) dengan *knowledge-based*.
6. Sistem *cloud* yang dibangun yaitu *Infrastructure as Service* (IaaS).

1.4. Tujuan

Tujuan pada tugas akhir ini adalah sebagai berikut,

1. Mengimplementasikan pembangunan infrastruktur sistem *cloud computing* (*private cloud*) dan mengimplementasikan IDS pada sistem *cloud computing*.
2. Menganalisis keberhasilan deteksi dengan serangan dari luar dan dalam pada sistem *cloud* yang dibangun jika,
 - a. IDS ditempatkan terpisah dengan server *cloud*,
 - b. IDS ditempatkan pada server *cloud*,
 - c. IDS ditempatkan pada keduanya (pada server *cloud* dan terpisah dengan server *cloud*).
3. Mengetahui pengaruh IDS terhadap penggunaan CPU dan *memory* pada server *cloud* yang dibangun.

1.5. Metode Penelitian

Metodologi penelitian yang digunakan pada tugas akhir ini adalah sebagai berikut,

1.5.1 Metode Pembangunan Sistem

I. Studi Pustaka dan Literatur

Mengumpulkan data secara mandiri dari berbagai sumber mengenai *cloud computing*, proxmox ve, dan *intrusion detection system*, sehingga diperoleh metode penyelesaian masalah sesuai dengan tujuan riset ini.

II. Analisis kebutuhan

Mempelajari dan menganalisis kebutuhan yang diperlukan dalam melakukan sistem membutuhkan 2 buah pc untuk server *cloud*, 1 buah pc untuk server IDS, dan 2 buah *switch manageable*.

III. Perancangan sistem

Pada tahap ini akan dilakukan perancangan sistem *cloud computing* dengan menggunakan proxmox ve sebagai *infrastructure cloud*, membangun server IDS dengan menggunakan snort yang

ditempatkan terpisah dengan server *cloud* dan membangun server IDS yang ditempatkan pada server *cloud*.

IV. Implementasi

Hasil dari perancangan sistem *cloud* yang dibangun diimplementasikan dengan tiga skenario yaitu skenario pertama dengan mengimplementasikan IDS yang ditempatkan terpisah dengan server *cloud*, skenario kedua dengan mengimplementasikan IDS yang ditempatkan dalam server *cloud*, dan skenario ketiga dengan mengimplementasikan IDS yang ditempatkan terpisah dengan server *cloud* dan pada server *cloud*. Setelah itu melakukan pengujian serangan dari dalam maupun dari luar sistem *cloud*.

V. Pengujian dan analisis

Menguji sistem yang telah dibangun dengan keberhasilan deteksi serangan dari luar maupun dari dalam sistem *cloud* dengan tiga skenario peletakan IDS yang diuji. Setelah sistem dinyatakan dapat berjalan dengan baik dan dapat mendeteksi sesuai dengan rancangan maka dilakukan analisis terhadap kasus yang diteliti dalam hal ini adalah pengaruh peletakan *intrusion detection system* pada *cloud computing*.