BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Universitas Sangga Buana YPKP merupakan Perguruan Tinggi Swasta yang terdapat di Bandung. Universitas Sangga Buana Yayasan Pendidikan Keuangan dan Perbankan, yang disingkat USB YPKP terdiri dari tiga Fakultas, yang merupakan hasil penggabungan Fakultas Ekonomi USB YPKP dengan Fakultas Teknik USB YPKP ditambah dengan pendirian Fakultas baru, yaitu Fakultas Ilmu Komunikasi dan Administrasi (FIKA). Lingkungan Universitas Sangga Buana YPKP mempunyai kemudahan dalam mengakses internet sehingga kebutuhan seperti *browsing*, *chatting*, *download* dan juga sebagai sarana pertukaran informasi dilingkungan internalnya, oleh karena itu tidak lepas dari masalah keamanan data yang termuat di dalamnya.

Kemajuan teknologi dan ilmu pengetahuan telah mendorong manusia untuk berusaha mengatasi segala permasalahan yang timbul di sekitarnya. Pemanfaatan teknologi yang sering digunakan salah satunya adalah internet[4]. Salah satu manfaat internet telah banyak digunakan oleh kalangan umum, khususnya dunia pendidikan. Berdasarkan pengamatan inventarisasi jenis serangan pada jaringan Universitas Sangga Buana YPKP, terdapat beberapa jenis serangan dari dalam jaringan yang paling sering terjadi, diantaranya serangan *spam* DoS terhadap *server mail* yang terdapat di Universitas Sangga Buana YPKP dengan cara mengirim ratusan e-mail, *flooding* terhadap *webserver* dengan cara melakukan ping yang sangat besar yang bertujuan untuk membuat *webserver* sibuk sehingga tidak dapat menangani permintaan lagi, *spoofing* terhadap jaringan *wireless* dengan cara menggunakan IP *static* di kampus Universitas Sangga Buana YPKP, sehingga alokasi IP yang seharusnya menggunakan DHCP tidak berjalan sebagaimana mestinya, dan disamping itu pengaksesan data saat ini menjadi suatu kebutuhan yang tinggi dimana setiap *administrator*, staff IT, dan pegawai

Universitas Sangga Buana YPKP perlu untuk mengakses data berupa data keuangan, data kepegawaian, dan data kemahasiswaan dimanapun berada tanpa terbatasi waktu dan tempat. Hal tersebut menyebabkan tidak terpenuhinya aspek keamanan *confidentiality* dan *availability*.

Firewall dan VPN (*Virtual Private Network*) pada sistem operasi IPCop yaitu mekanisme pengamanan yang dapat dilakukan untuk melindungi dari serangan yang sering terjadi. *Firewall* yaitu sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas dari jaringan yang tidak aman[4]. VPN (*Virtual Private Network*) yaitu jaringan pribadi yang menggunakan medium nonpribadi misalnya internet untuk menghubungkan antar *remotesite* secara aman[1]. IPCop adalah suatu distribusi Linux yang menyediakan fitur *simple-to-manage firewall appliance* berbasis perangkat keras PC. IPCop juga dibangun dengan *ProPolice* untuk mencegah serangan pada semua aplikasi, memiliki pilihan konfigurasi *kernel* yang mengizinkan kita memilih sesuai dengan keadaan yang kita inginkan, aman dan stabil serta merupakan *Linux based firewall* yang sangat mudah dikonfigurasi.

Berdasarkan permasalahan tersebut, dapat diketahui bahwa di Universitas Sangga Buana YPKP memerlukan suatu sistem jaringan yang baik yaitu dengan membangun *firewall* dan VPN *(Virtual Private Network)* pada sistem operasi IPCop. Hal ini bertujuan untuk menangani serangan yang sering terjadi pada jaringan Universitas Sangga Buana YPKP.

1.2 Rumusan Masalah

Berdasarkan masalah yang ada pada latar belakang, maka dapat ditarik rumusan permasalahan sebagai berikut :

1. Bagaimana cara mengatasi serangan *spam* DoS, serangan *flooding,* dan serangan IP *spoofing* yang sering terjadi di Universitas Sangga Buana YPKP?
2. Bagaimana cara melindungi data agar bisa diakses diberbagai tempat dan tanpa terbatasi oleh waktu?

Identifikasi masalah yang didapat dari masalah tersebut yaitu, bagaimana cara membangun *firewall* dan VPN *(Virtual Private Network)* menggunakan sistem operasi IPCop untuk keamanan data di Universitas Sangga Buana YPKP.

1.3 Maksud dan Tujuan

Maksud dari penelitian ini adalah untuk membangun *firewall* dan VPN *(Virtual Private Network)* menggunakan sistem operasi IPCop untuk keamanan data di Universitas Sangga Buana YPKP.

Tujuan dari penelitian ini adalah :

1. Mengamankan *server mail*, *webserver*, dan jaringan *wireless* dengan menggunakan *firewall.*
2. Melindungi data dengan menggunakan *Virtual Private Network* (VPN) agar dapat diakses diberbagai tempat dan tanpa terbatasi oleh waktu.

1.4 Batasan Masalah

Berdasarkan rumusan masalah tersebut, maka penulis membatasi permasalahan dalam membangun *firewall* dan VPN *(Virtual Private Network)* menggunakan sistem operasi IPCop untuk keamanan data di Universitas Sangga Buana YPKP, meliputi:

1. Implementasi berupa konfigurasi *firewall* dan VPN *(Virtual Private Network)* menggunakan sistem operasi IPCop.
2. Serangan yang dimaksud adalah serangan yang sering terjadi pada jaringan internal Universitas Sangga Buana YPKP saja.
3. Melakukan pengujian untuk mengevaluasi fungsionalitas, performa, skalabilitas, tingkat keamanan *firewall* serta mengidentifikasi masalah seperti interoperabilitas dengan komponen lain.
4. Data yang diamankan yaitu data keuangan, data kepegawaian, dan data kemahasiswaan.
5. Pengujian menggunakan *tools* yaitu :
    a. Sistem operasi yang digunakan yaitu IPCop (Linux).
    b. Dijalankan pada lingkup virtual pada sistem operasi Windows 7.

1.5 Metode Penelitian

Dalam melakukan penelitian ini, penulis menggunakan beberapa metode dalam melakukan pengumpulan data, diantaranya :

1. Studi Pustaka

Penulis mengumpulkan dan mempelajari buku-buku atau *ebook* yang berhubungan dengan penelitian yang dilakukan. Untuk melihat referensi selengkapnya terdapat pada halaman daftar pustaka.

2. Studi Lapangan

a. Observasi

Pengamatan langsung ke lapangan (observasi) yang dilakukan oleh penulis, tempat pelaksanaannya yaitu di Universitas Sangga Buana YPKP, Jl. PHH. Mustopa No.68 Telp. 022-7275489, 7202841 Fax. 022-7201756 Kota Bandung 40124.

b. Wawancara

Dalam melakukan pengumpulan data, penulis juga melakukan wawancara secara langsung kepada pihak yang terlibat. Wawancara dilakukan kepada Bapak Renol Burjulius, S.T., M.Kom, App, CEH selaku Dosen Program Studi Teknik Informatika dan Ketua PUDI (Pusat Data Dan Informasi) di Universitas Sangga Buana YPKP.

3. Studi Literatur.

Dalam melakukan penelitian penulis juga menggunakan literatur sejenis yang digunakan baik berasal dari jurnal-jurnal maupun skripsi yang mempunyai topik yang mendekati dengan topik yang dibahas penulis.

3.1 Metode Pengembangan Sistem.

Metode pengembangan sistem ini menggunakan metode *Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) Network Lifecycle* seperti pada Gambar 1.1 yang terdiri dari beberapa tahap, yaitu:

a. *Prepare*

Dalam model pengembangan sistem PPDIOO fase pertama dimulai dari *fase prepare*. Pada *fase* ini dilakukan proses perumusan masalah, mengidentifikasi konsep dari sistem yang akan diimplementasikan, jenis

dan tipe penerapannya, serta komponen pendukung sehingga spesifikasi kebutuhan sistem dapat diperjelas.

b. *Planning*

Untuk tahap selanjutnya adalah tahap *plan*. Penulis melakukan perencanaan dalam membuat rincian spesifikasi. Dalam penelitian ini terdapat perencanaan dalam membuat infrastruktur dan komponen pendukung yang akan dikonfigurasi.

c. *Design*

Dalam tahapan *design* ini dibuat suatu topologi jaringan untuk proses keamanan. Serta konfigurasi yang dilakukan pada masing-masing perangkat.

d. *Implement*

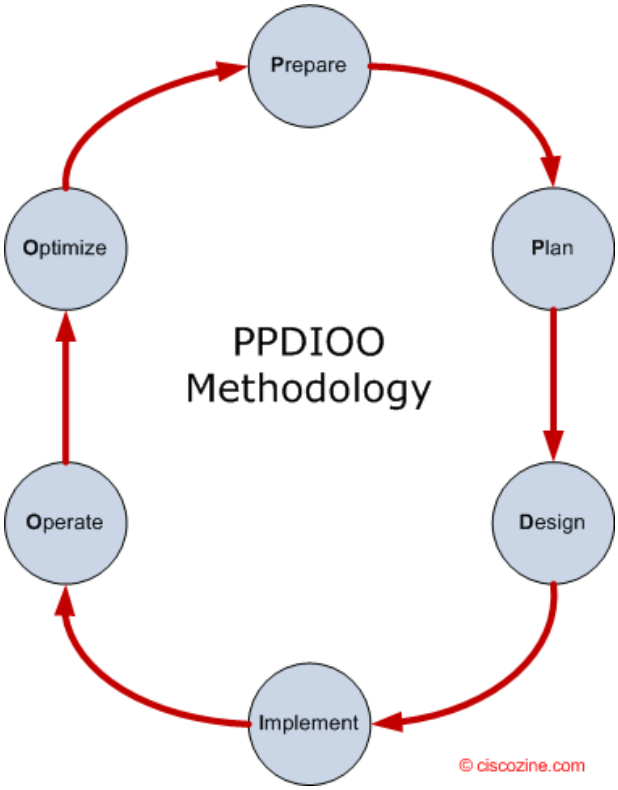
Tahap selanjutnya adalah tahap implementasi, pada tahap ini menerapakan semua yang telah direcanakan. Dalam tahap ini mencakup instalasi serta konfigurasi terhadap rancangan topologi, dan konfigurasi yang dilakukan pada masing-masing perangkat.

e. *Operate*

Dalam tahap ini diperlukan adanya pemantauan terhadap *server* agar berjalan sesuai dengan analisa awal dan pemantauan terhadap infrastruktur *hardware*. Proses pengujian termasuk dalam fase ini, dalam melakukan pengujian menggunakan parameter yang ditentukan terhadap *firewall* dan sejumlah komponen pendukung agar dipastikan sudah berjalan dengan baik dan benar dan sudah menjawab permasalahan yang telah dirumuskan.

f. *Optimize*

Tahap ini memerlukan perhatian khusus terhadap kebijakan yang perlu dibuat untuk mengatur dan membuat sistem agar dapat berjalan dengan baik. Perawatan, pemeliharaan dan pengelolaan terhadap *server* termasuk dalam *fase* ini.



Gambar 1.1 Metode *Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) Network Lifecycle*[10].

1.6 Sistematika Penulisan

Sistematika penulisan proposal penelitian ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang penelitian, identifikasi masalah, maksud dan tujuan penelitian, batasan masalah, metodologi penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas tentang profil tempat studi kasus yaitu Universitas Sangga Buana YPKP Bandung dan berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian.

BAB III ANALISIS MASALAH

Bab ini menguraikan deskipsi sistem, analisis kebutuhan dalam pembangunan sistem serta perancangan system yang dikembangkan. Dalam tugas akhir ini, analisis yang dilakukan adalah terhadap analisis yang difokuskan terhadap *Firewall* dan VPN *(Virtual Private Network).* Perancangan yang dilakukan adalah dengan mengkonfigurasi *Firewall* dan VPN *(Virtual Private Network)* menggunakan sistem operasi IPCop di Universitas Sangga Buana YPKP Bandung.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini merupakan tahap implementasi dari sistem yang telah dibuat dan pengujian terhadap sistem yang telah diimplementasikan. Implementasi Firewall dan VPN *(Virtual Private Network)* menggunakan sistem operasi IPCop, merupakan hasil konfigurasi di Universitas Sangga Buana YPKP Bandung. Kemudian dilakukan pengujian fungsionalitas, performa, skalabilitas, tingkat keamanan *Firewall* dan VPN *(Virtual Private Network)* di Universitas Sangga Buana YPKP Bandung.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran yang sudah diperoleh dari hasil penulisan tugas akhir. Berdasarkan hasil analisi, perancangan, implementasi, perancangan, implementasi, dan pengujian fungsionalitas, performa, skalabilitas, tingkat keamanan *Firewall* dan VPN *(Virtual Private Network)* di Universitas Sangga Buana YPKP Bandung, maka dapat disimpulkan beberapa hasil sesuai tujuan penelitian yang dilakukan. Serta memberikan beberapa saran agar lebih mengoptimalkan perfomansi keamanan jaringan yang digunakan oleh Universitas Sangga Buana YPKP.