BAB 3
ANALISIS DAN PERANCANGAN SISTEM

3.1 Analisis Sistem

Analisa merupakan suatu tindakan untuk mengetahui lebih jauh tentang obyek yang akan diteliti. Bab ini akan menguraikan proses analisis implementasi dan perancangan firewall dan VPN (*Virtual Private Network)* menggunakan sistem operasi IPCop. Sebelum dilakukan implementasi dan perancangan sistem, terlebih dahulu dilaksanakan analisis kebutuhan pokok sistem yang akan dibangun.

Analisis sistem merupakan suatu tahapan yang bertujuan untuk mengetahui dan mengamati apa saja yang terlibat dalam suatu sistem. Analisis sistem bertujuan untuk mendapatkan pemahaman secara keseluruhan tentang sistem yang akan dibangun berdasarkan masukan dari pihak-pihak luar dan juga pengalaman analisis yang berkepentingan dengan sistem tersebut.

3.1.1 Analisis Masalah

Penelitian dalam tugas akhir ini adalah menganalisa masalah keamanan jaringan yang sering terjadi di Universitas Sangga Buana YPKP. Masih terdapat adanya beberapa masalah yang dirasakan oleh Universitas Sangga Buana YPKP diantaranya adalah *spam DoS*, *flooding*, *spoofing*, dan tidak terjaminnya pengiriman data seperti data keuangan, data kepegawaian, dan data kemahasiswaan yang aman melalui internet. Sehingga penelitian ini lebih difokuskan terhadap keamanan jaringan yang akan digunakan oleh Universitas Sangga Buana YPKP.

3.1.1.1 Permasalahan Yang Dihadapi

Ada 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.

3.1.1.2 Pemecahan Masalah Yang Diusulkan

Berdasarkan hasil pengamatan dan survei yang dilakukan, maka pemecahan masalah yang akan diusulkan yaitu pemecahan yang pertama dengan *firewall* untuk mengatasi serangan *spam* DoS terhadap *server mail,* mengatasi serangan *flooding* terhadap *webserver,* melindungi jaringan *wireless* dari serangan IP *spoofing,* dimana tujuan dari *firewall* adalah mengatur dan mengontrol lalu lintas jaringan, melakukan autentikasi terhadap akses, melindungi sumber daya dalam jaringan *private*, mencatat semua kejadian, dan melaporkan kepada *administrator.* Pemecahan yang kedua yaitu dengan VPN (*Virtual Private Network*) untuk melindungi data berupa data keuangan, data kepegawaian, dan data kemahasiswaan agar dapat diakses diberbagai tempat dan tanpa terbatasi oleh waktu membutuhkan sistem yang memiliki tingkat keamanan pengiriman data yang tinggi, dimana tujuan dari VPN (*Virtual Private Network*) adalah untuk menghubungkan antar *remotesite* secara aman dan tidak dapat disadap dengan mudah.

3.1.1.3 Analisis Jenis Serangan

Bentuk-bentuk serangan yang sering terjadi terhadap jaringan dan hal-hal yang membahayakan keamanan jaringan di Universitas Sangga Buana YPKP adalah hal-hal sebagai berikut:

1. *Spam DoS* terhadap *server mail*

Serangan *spam DoS* ini sering membanjiri *server mail* dengan paket data yang tidak diminta dengan cara belum pernah terjadi sebelumnya. Hal ini menyebabkan '*Overflow* Kapasitas' terhadap *server mail* yang dimiliki Universitas Sangga Buana YPKP.

2. *Flooding* terhadap *webserver*

Paket-paket *flooding* adalah salah satu jenis paket dalam protokol *Transmission Control Protocol* yang dapat digunakan untuk membuat koneksi antara dua *host* dan dikirimkan oleh *host* yang hendak membuat koneksi, sebagai langkah pertama pembuatan koneksi dalam proses "*TCP Three-way Handshake*". Dalam sebuah serangan *flooding*, penyerang mengirimkan paket-paket *flooding* ke dalam *port-port* yang sedang berada dalam keadaan "*Listening*" yang berada dalam *host* Universitas Sangga Buana YPKP.

3. IP *spoofing* terhadap jaringan *wireless*

IP *spoofing* juga dikenal sebagai *Source Address Spoofing*. Yaitu pemalsuan IP *attacker* sehingga sasaran menganggap alamat IP *attacker* adalah alamat IP dari *host* di dalam *network* bukan dari luar *network*.

Dari hasil analisis jenis serangan yang sering terjadi pada jaringan di Universitas Sangga Buana YPKP, maka dibutuhkan keamanan yang sangat tinggi untuk melindungi data dan jaringan di Universitas Sangga Buana YPKP.

3.1.2 Analisis Jaringan di Universitas Sangga Buana YPKP

Analisis jaringan yang akan dibahas pada sub bab ini meliputi Analisis Topologi Jaringan, Analisis Spesifikasi Perangkat Jaringan, Analisis Pengguna, Analisis Perangkat Lunak, Analisis Perangkat Keras, Spesifikasi Perangkat Keamanan, Analisis *Subnetting*, Analisis Internet *Protocol*, Analisis *Firewall*, dan Analisis VPN (*Virtual Private Network).*

3.1.2.1 Analisis Topologi Jaringan Komputer di Universitas Sangga Buana YPKP

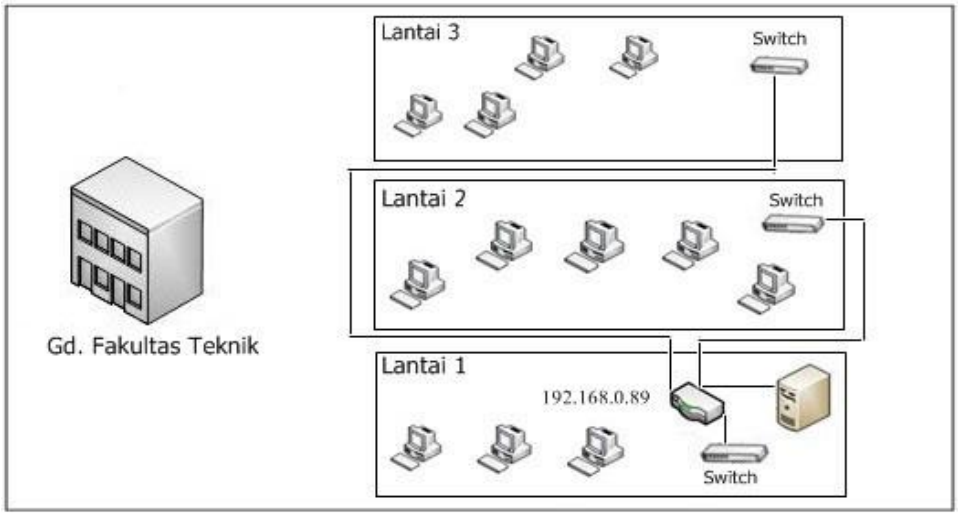
Lingkungan Universitas Sangga Buana YPKP Bandung terdiri atas 3 gedung antara lain Gedung Fakultas Teknik, Gedung Fakultas Ekonomi, dan Gedung Fakultas Ilmu Komunikasi dan Administrasi.

Gedung Fakultas Teknik merupakan gedung yang mengelola bagian-bagian secara umum, meliputi bagian Tata Usaha, *Customer Service*, bagian data dari semua gedung yang ada di lingkungan Universitas Sangga Buana YPKP, dan Bidang Program dan Kerjasama.

Gedung Fakultas Ekonomi merupakan gedung mengelola bagian-bagian dari Program Studi yang ada di Fakultas Ekonomi meliputi Program Studi Manajemen, Akuntansi, dan Keuangan dan Perbankan, pemantauan data yang dikelola oleh Fakultas Ekonomi, Bidang Program dan Kerjasama dan lain-lain.

Gedung Ilmu Komunikasi dan Administrasi gedung mengelola bagian-bagian dari Program Studi yang ada di Fakultas Ilmu Komunikasi dan Administrasi meliputi Program Studi Ilmu Komunikasi dan Ilmu Administrasi sama halnya dengan Fakultas Ekonomi, Bidang Program dan Kerjasama dan lain-lain.

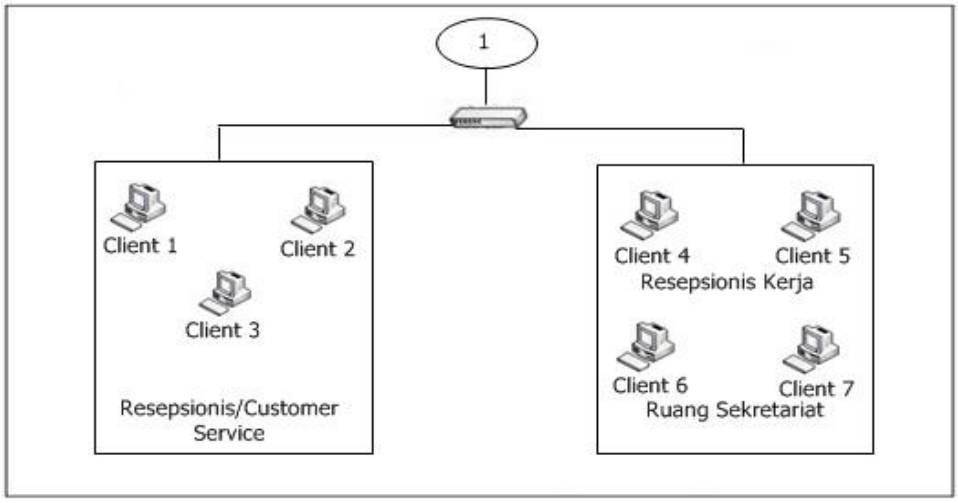
Oleh karena itu, penelitian ini lebih difokuskan kepada gedung Fakultas Teknik. Karena gedung Fakultas Teknik merupakan tempat penyedia jaringan internet utama, yang kemudian dialokasikan ke gedung-gedung lainnya agar dapat mengakses internet dan data sesuai kebutuhan dari gedung-gedung yang mengakses. Berikut topologi jaringan komputer gedung Fakultas Teknik yang akan digambarkan dan pengalokasiannya di setiap lantai.



Gambar 3.1 Topologi Umum Jaringan Komputer

di Gedung Fakultas Teknik Universitas Sangga Buana YPKP

3.1.2.2 Topologi Jaringan Komputer Lantai 1 Gedung Fakultas Teknik Universitas Sangga Buana YPKP



Gambar 3.2 Topologi Jaringan Komputer di Lantai 1 Gedung Fakultas Teknik Universitas Sangga Buana

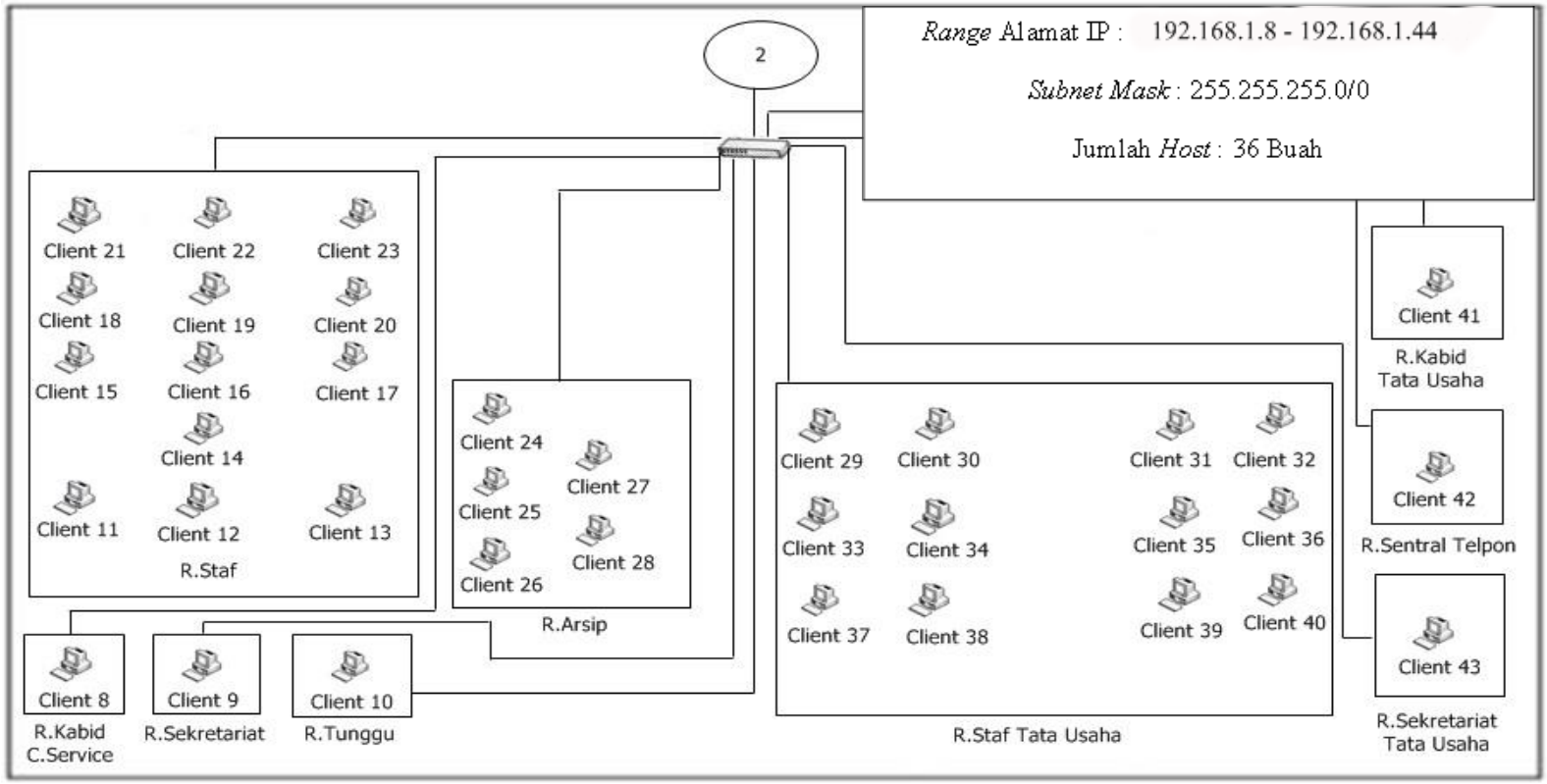
Range Alamat IP : 192.168.1.1 – 192.168.1.7

Subnet Mask : 255.255.255.0/0

Jumlah *Host* : 7 Buah

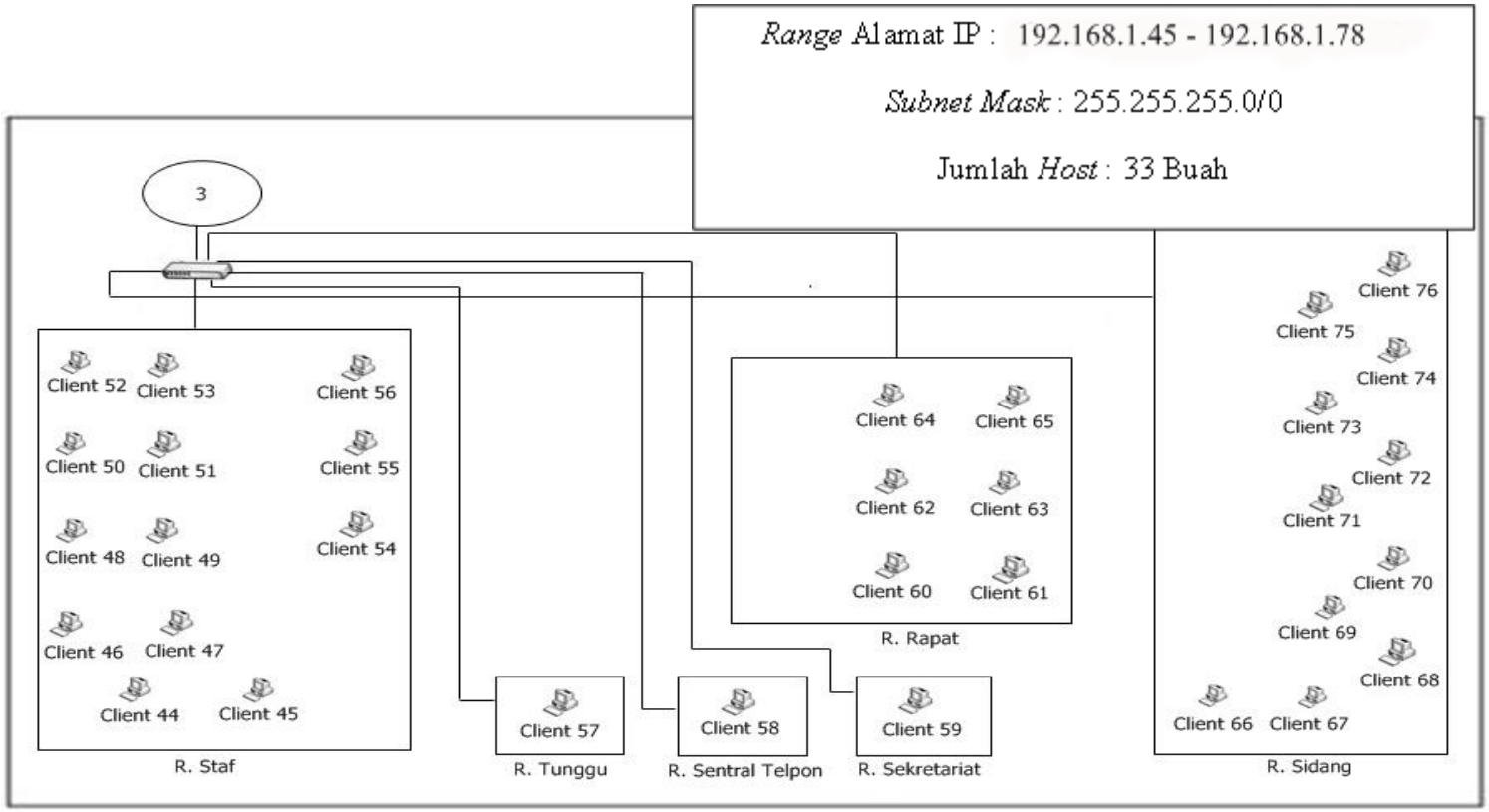
Lantai 1 di Universitas Sangga Buana YPKP Bandung digunakan sebagai lantai dasar. Tempat untuk mengakses internet atau jaringan komputer melalui *internet outlet* yang disediakan oleh Universitas Sangga Buana YPKP Bandung di lantai dasar hanya ruangan resepsionis/*customer service* sejumlah 3 *client*, ruang kerja resepsionis sejumlah 2 *client*, dan ruang sekretariat sejumlah 2 *client*. Maka total jaringan yang disediakan di lantai dasar sejumlah 7 buah.

3.1.2.3 Topologi Jaringan Komputer Lantai 2 Gedung Fakultas Teknik Universitas Sangga Buana YPKP



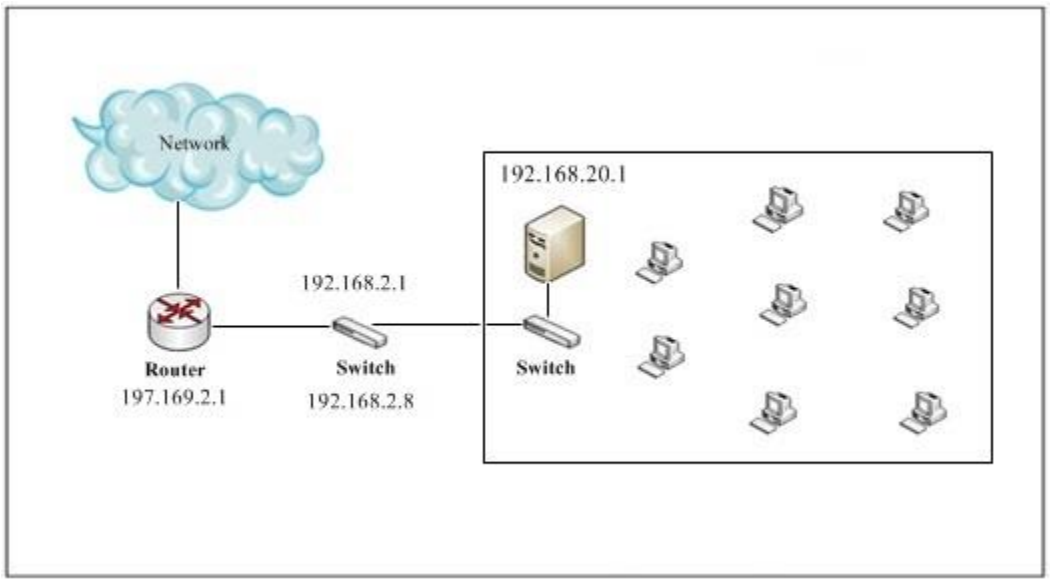
Gambar 3.3 Topologi Jaringan Komputer di Lantai 2 Gedung Fakultas Teknik Universitas Sangga Buana YPKP

3.1.2.4 Topologi Jaringan Komputer Lantai 3 Gedung Fakultas Teknik Universitas Sangga Buana YPKP



Gambar 3.4 Topologi Jaringan Komputer di Lantai 3 Gedung Fakultas Teknik Universitas Sangga Buana YPKP

3.1.2.5 Topologi Jaringan Komputer Kantor Cabang (Pembantu) Universitas Sangga Buana YPKP



Gambar 3.5 Topologi Jaringan Komputer Kantor Cabang (Pembantu) Universitas Sangga Buana YPKP

3.1.2.6 Spesifikasi Perangkat Jaringan

Berikut ini adalah perangkat jaringan yang digunakan di Universitas Sangga Buana YPKP:

Switch Cisco Catalyst

1. Jumlah port : 24 port
2. Kecepatan : 10/100 Mbps
3. Managable : Managable

Router Cisco

1. Exinda 1700 Traffic Management
2. Jumlah port : 12 port ethernet

Fasilitas :

1. Monitoring dan filtering layer 7.
2. Melakukan report dengan format html atau csv.
3. Membuat policy bandwidth.
4. Mendukung kompresi data.

3.1.2.7 Analisis Pengguna

User adalah pengakses atau pengguna komputer di Universitas Sangga Buana YPKP. Hampir semua pegawai bisa menjalankan atau mengoperasikan komputer. Dan di setiap instansi pemerintah pasti mempunyai staff IT tersendiri. Staff IT di Universitas Sangga Buana YPKP bertugas menjaga dan memelihara komputer serta mengawasi jaringan internet. Berikut karakteristik *user* yang ada di Universitas Sangga Buana YPKP seperti pada tabel 3.1.

Tabel 3.1 Karakteristik *User*

User	Knowledge
Administrator Jaringan	Kualifikasi yang harus dimiliki administrator jaringan yaitu memiliki keahlian di bidang jaringan komputer, menangani LAN, mengkonfigurasi jaringan.
Staff IT	Kualifikasi yang harus dimiliki staff IT adalah memiliki pengetahuan dasar di bidang jaringan komputer dan bisa menangani masalah jaringan.
Karyawan	Kualifikasi yang harus dimiliki karyawan yaitu memiliki kemampuan dasar di bidang komputer, dapat mengoperasikan Sistem Operasi Windows 7 dan pernah menggunakan aplikasi jaringan khususnya yang berkaitan dengan internet.

3.1.2.8 Analisis Perangkat Lunak (*Software*)

Software atau perangkat lunak merupakan perangkat yang digunakan dalam mengoperasikan komputer. Berikut merupakan sistem operasi yang digunakan pada komputer *server* dan komputer *client* pada penelitian di Universitas Sangga Buana YPKP:

Tabel 3.2 *Operating System Server* dan *Client*

Server	Client
Windows 2008 Server R2	Windows Xp, windows 7

3.1.2.9 Analisis Perangkat Keras (*Hardware*)

Universitas Sangga Buana YPKP memiliki 12 *server*, 4 *router*, 8 *switch*, dan 80 komputer *client* yang berada di seluruh gedung Universitas Sangga Buana YPKP.

Tabel 3.3 Jumlah *Hardware* di Universitas Sangga Buana YPKP

Jenis	Jumlah
Server	12 unit
Router	4 unit
Switch	8 unit
Komputer *client*	80 unit

3.1.2.10 Analisis Spesifikasi Perangkat Keamanan

Ada beberapa perangkat keras serta perangkat lunak yang digunakan untuk menjamin keamanan jaringan komputer di Universitas Sangga Buana YPKP. Perangkat tersebut adalah sebagai berikut :

1. Cisco ASA

1. Jumlah port : 8 ethernet port + 2 management port + 2 console port
2. Memori RAM : 512 MB
3. Memori Flash : 64 MB

Fasilitas :

1. Mendukung *service* Web-based Cisco Adaptive Security Device Manager (ASDM) *application*.

2. Bitdefender Antivirus

Merupakan software anti-virus yang digunakan di Bitdefender untuk melindungi seluruh komputer dari serangan virus, Trojan ataupun worm. Bitdefender Antivirus terdiri dari 2 mode, yaitu antivirus client dan antivirus server. Antivirus server bertugas untuk melakukan update secara periodic. Kemudian update antivirus tersebut akan dibagikan kepada antivirus client yang telah terinstall pada sebagian besar komputer klien.

3.1.2.11 Analisis *Subnetting* di Universitas Sangga Buana YPKP

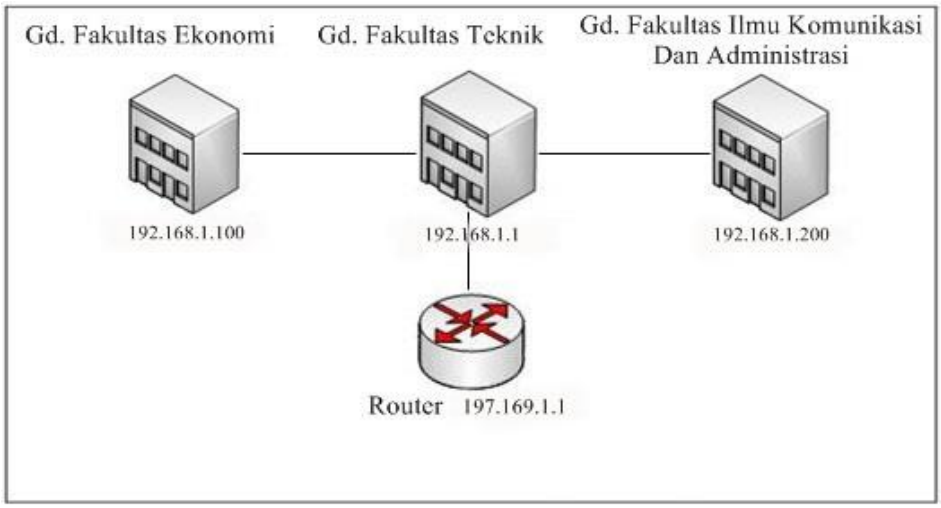
Analisis *subnetting* adalah menganalisis teknik memecah suatu jaringan besar menjadi jaringan yang lebih kecil dengan cara mengorbankan bit Host ID pada *subnet mask* untuk dijadikan *network* ID baru. Universitas Sangga Buana YPKP juga mempunyai 3 gedung, yaitu Gedung Fakultas Teknik, Gedung Fakultas Ekonomi, dan Gedung Fakultas Ilmu Komunikasi dan Administrasi. Oleh karena itu, teknik *subnetting* digunakan untuk memudahkan pembagian jaringan di Universitas Sangga Buana YPKP Bandung. *Subnet* yang digunakan dibagi menjadi 3, yaitu :

1. 192.168.1.100 : *Subnet* ini digunakan pada gedung Fakultas Ekonomi.

2. 192.168.1.1 : *Subnet* ini digunakan pada gedung Fakultas Teknik.

3. 192.168.1.200 : *Subnet* ini digunakan pada gedung Fakultas Ilmu Komunikasi dan Administrasi.

Berikut adalah *subnetting* yang digunakan di Universitas Sangga Buana YPKP Bandung.



Gambar 3.6 *Subnetting* di Universitas Sangga Buana YPKP.

Berdasarkan penggunaan *subnetting* di Universitas Sangga Buana YPKP Bandung, maka dapat diperoleh keterangan lebih lanjut tentang penentuan jumlah *host* di setiap gedung. Khusus di gedung Fakultas Teknik dapat diketahui secara jelas.

Network Address	:	192.168.1.1
Network Class	:	*class* C
Subnet Mask	:	255.255.255.0/24
Subnet ID	:	192.168.1.0
Broadcast Address	:	192.168.1.255

Jumlah Host per Network : 100

Range IP *Address* : 192.168.1.1 - 192.168.1.100

3.1.2.12 Analisis Internet *Protocol* di Universitas Sangga Buana YPKP Bandung

Penggunaan IP *Address* di Universitas Sangga Buana YPKP Bandung terbagi atas 2 jenis IP, yaitu IP *Public* dan IP Dinamis. IP yang digunakan oleh komputer *server* merupakan IP kelas A yaitu 127.237.252.1 dan IP yang digunakan oleh *client* merupakan IP kelas C sesuai dengan *subnet* yang digunakan oleh Universitas Sangga Buana YPKP Bandung yaitu 192.168.1.1 untuk semua *client* yang berada di gedung Fakultas Ekonomi dan gedung Fakultas Ilmu Komunikasi & Administrasi menggunakan 192.168.1.100 dan 192.168.1.200. Dalam perencanaannya, penggunaan IP untuk *client* nantinya merupakan hasil pemberian berdasarkan *format* dibawah ini :

[Gedung] [Lantai] [Hub/Akses Point] [Port] [Client]

Contoh penggunaan IP berdasarkan format tersebut antara lain :

FT.01.A.01.01

Keterangan :

FT = Gedung Fakultas Teknik.

01 = Lantai 1 yang berada di gedung Fakultas Teknik.

A = *Hub* yang digunakan untuk gedung Fakultas Teknik.

01 = *Port* yang digunakan di *Hub*.

01 = *Client* yang digunakan oleh setiap PC.

Berdasarkan keterangan tersebut, semua komputer *client* yang ada di Universitas Sangga Buana YPKP akan menggunakan kode tersebut di setiap *client* yang disediakan untuk mengakses jaringan internet. Hal ini akan memudahkan

administrator untuk mengetahui jika ada komputer yang tidak bisa mengakses ke jaringan komputer.

3.1.2.13 Analisis IP (*Internet Protocol*)

Dalam penelitian ini, analisis IP (*Internet Protocol*) di Universitas Sangga Buana YPKP Bandung akan dibagi menjadi beberapa bagian yaitu IP *Public*, IP Statis, dan IP Dinamis yang digunakan oleh Universitas Sangga Buana YPKP Bandung.

3.1.2.13.1 IP *Public*

Server di Universitas Sangga Buana YPKP mempunyai kegunaan masing-masing. Alamat IP yang digunakan oleh setiap *server* berbeda-beda. Berikut tabel *server* yang digunakan dan keterangannya.

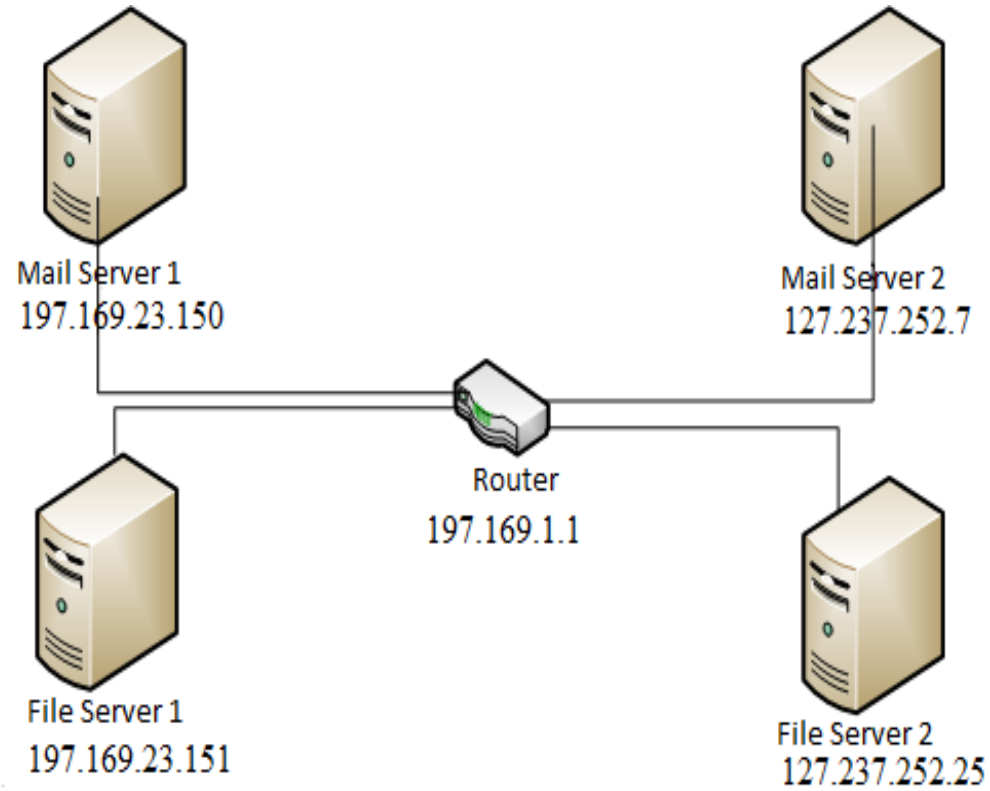
Tabel 3.4 Nama *Server* Universitas Sangga Buana YPKP Bandung dan Fungsinya.

Nama *Server*	Alamat IP	Keterangan
Gateway	127.237.252.1	Digunakan sebagai *Local Host.*
Email Server 1	127.237.252.7	Digunakan untuk menampung *email.*
DNS *Server* + Website1	127.237.252.22	Digunakan untuk penyimpanan data, *primary*.
DNS *Server* + Website 2	127.237.252.23	Digunakan untuk penyimpanan data, *secondary*.
Perpustakaan *Server*	127.237.252.9	Digunakan untuk Sistem

		Informasi Perpustakaan.
File *Server*	127.237.252.25	Digunakan untuk penyimpanan data (*Upload dan Download*).

3.1.2.13.2 IP Statis

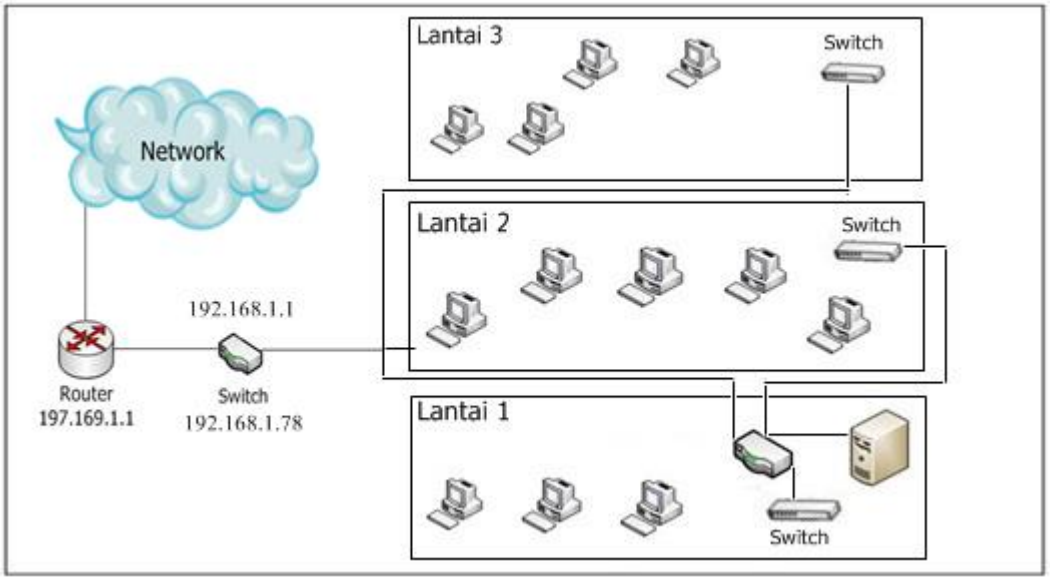
IP Statis yang digunakan oleh Universitas Sangga Buana YPKP Bandung hanya digunakan pada *router, mail server,* dan *file server.* Awalnya, *mail server* memiliki alamat IP 192.168.23.150 dan *file server* memiliki alamat IP 192.168.23.151. Kemudian disatukan oleh *router* dengan IP *Public*, sehingga alamat IP dari *mail server* menjadi 127.237.252.7 dan alamat IP *file server* menjadi 127.237.252.25.



3.1.2.13.3 IP Dinamis

Universitas Sangga Buana YPKP Bandung menggunakan DHCP *Server* untuk memberikan alamat kepada komputer *client.* Pemberian alamat IP secara dinamis, dapat membantu *administrator* di Universitas Sangga Buana YPKP Bandung dalam pemberian alamat IP. Karena *client* lain dapat menggunakan alamat IP yang tidak sedang digunakan.

IP dinamis merupakan pemberian alamat yang secara otomatis oleh *router* kepada komputer *client*. Berikut arsitektur DHCP di Gedung Fakultas Teknik Universitas Sangga Buana YPKP Bandung :



Gambar 3.7 Arsitektur DHCP Gedung Fakultas Teknik Universitas Sangga Buana YPKP

3.1.2.14 Analisis Firewall

Analisis *firewall* adalah mekanisme kontrol akses pada level jaringan, aplikasi penghambat yang dibangun untuk memisahkan jaringan privat dengan jaringan publik (internet). *Firewall* diimplementasikan pada : *software*, *hardware*, *router Access*, ataupun *server access* atau beberapa *router acess* ataupun beberapa *server access.* Menggunakan suatu (*rule*)/*Policy* berupa daftar akses (*access list*), dan metode lain untuk menjamin keamanan jaringan privat.

Pada *firewall* terjadi beberapa proses yang memungkinkannya melindungi jaringan. Ada tiga macam proses yang terjadi pada *firewall,* yaitu:

1. Modifikasi *header* paket, digunakan untuk memodifikasi kualitas layanan *bit* paket TCP sebelum mengalami proses *routing*.

2. Translasi alamat jaringan, translasi yang terjadi dapat berupa translasi satu ke satu (*one to one*), yaitu satu alamat IP privat dipetakan kesatu alamat IP publik atau translasi banyak kesatu (*many to one*) yaitu beberapa alamat IP privat dipetakan kesatu alamat publik.

3. *Filter* paket, digunakan untuk menentukan nasib paket apakah dapat diteruskan atau tidak.

3.1.2.14.1 Teknologi Firewall

Teknologi *firewall* yang digunakan dalam permasalahan yang sering terjadi, yaitu *Packet Filtering Gateway*, Prinsipnya adalah memperbolehkan (*grant*) atau membatalkan (*deny*) terhadap suatu access, *Packet Filtering Gateway* didasarkan pada:

1. Paket yang dibolehkan/tidak dibolehkan berdasarkan alamat IP sumber/tujuan
2. Paket yang dibolehkan/tidak dibolehkan berdasarkan *port* sumber/tujuan
3. Paket yang dibolehkan/tidak dibolehkan berdasarkan protokol
4. Paket yang dibolehkan/tidak dibolehkan berdasarkan *flag* pada protokol tertentu

Packet filtering gateway dapat diartikan sebagai *firewall* yang bertugas melakukan filterisasi terhadap paket-paket yang datang dari luar jaringan Universitas Sangga Buana YPKP yang dilindungi.

3.1.2.14.2 Koneksi Paket

Koneksi paket dalam proses pengirimannya dari pengirim kepada penerima harus melalui aturan *firewall*, dapat dikelompokan kepada tiga kelompok koneksi, yaitu :

1. Koneksi TCP

Sebuah koneksi TCP dikenal sebagai koneksi yang bersifat *Connection Oriented* yang berarti sebelum melakukan pengiriman data, mesin-mesin tersebut akan melalui 3 langkah cara berhubungan (3-*way handshake*).

2. Koneksi IP

Sebuah frame yang diidentifikasi menggunakan kelompok protokol Internet (IP) harus melalui aturan *firewall* yang didefinisikan menggunakan protokol IP sebelum paket tersebut mendapat jawaban koneksi dari tujuan paket tersebut. Salah satu paket yang merupakan kelompok protokol IP adalah ICMP, yang sering digunakan sebagai aplikasi pengujian koneksi (*link*) antar *host.*

3. Koneksi UDP

Berbeda dengan koneksi TCP, koneksi UDP bersifat *connectionless*. Sebuah mesin yang mengirimkan paket UDP tidak akan mendeteksi kesalahan terhadap pengiriman paket tersebut. Paket UDP tidak akan mengirimkan kembali paket-paket yang mengalami *error*. Model pengiriman paket ini akan lebih efisien pada koneksi *broadcasting* atau *multicasting.*

3.1.2.15 Analisis VPN (*Virtual Private Network*)

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Dengan adanya *site-to-site* VPN, keamanan menjadi prioritas utama selain fungsi lainnya yaitu untuk menghubungkan antara dua atau lebih tempat yang letaknya berjauhan,

seperti halnya kantor pusat dengan kantor cabang yang dimiliki oleh sebuah instansi atau perusahaan.

3.1.2.15.1 Analisis Kebutuhan Sistem *Site-To-Site* VPN

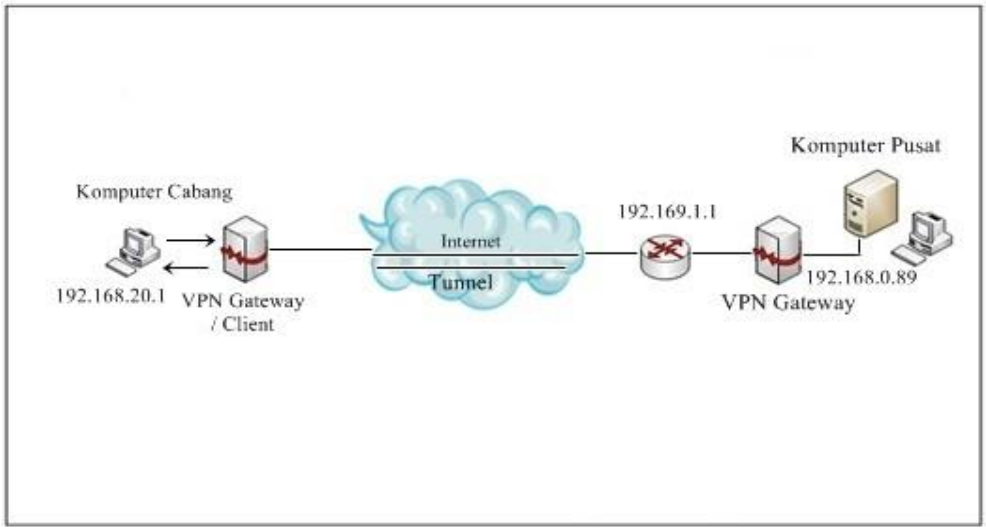
VPN merupakan perpaduan dari teknologi *tunneling* dengan teknologi enkripsi. Teknologi *tunneling* bertugas untuk manangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Sedangkan teknologi enkripsi menjamin kerahasiaan data yang berjalan di dalam *tunnel*.

3.1.2.15.2 Jenis Implementasi VPN

Dilihat dari jenis implementasi VPN yang ada, dalam penelitian ini termasuk dalam kategori *Site-to-site* VPN.

Site-to-site VPN merupakan jenis implementasi VPN yang menghubungkan antara dua tempat atau lebih yang letaknya berjauhan, seperti halnya menghubungkan kantor pusat dengan kantor cabang, baik kantor yang dimiliki perusahaan itu sendiri maupun kantor perusahaan mitra kerjanya.

VPN yang digunakan untuk menghubungkan kantor pusat dengan kantor cabang suatu perusahaan disebut *intranet site-to-site* VPN. Sedangkan bila VPN digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, supplier atau pelanggan), implementasi ini termasuk jenis ekstranet. Berikut merupakan gambar topologi jaringan *site-to-site* VPN :



Gambar 3.8 Gambaran Topologi Jaringan *site-to-site* VPN

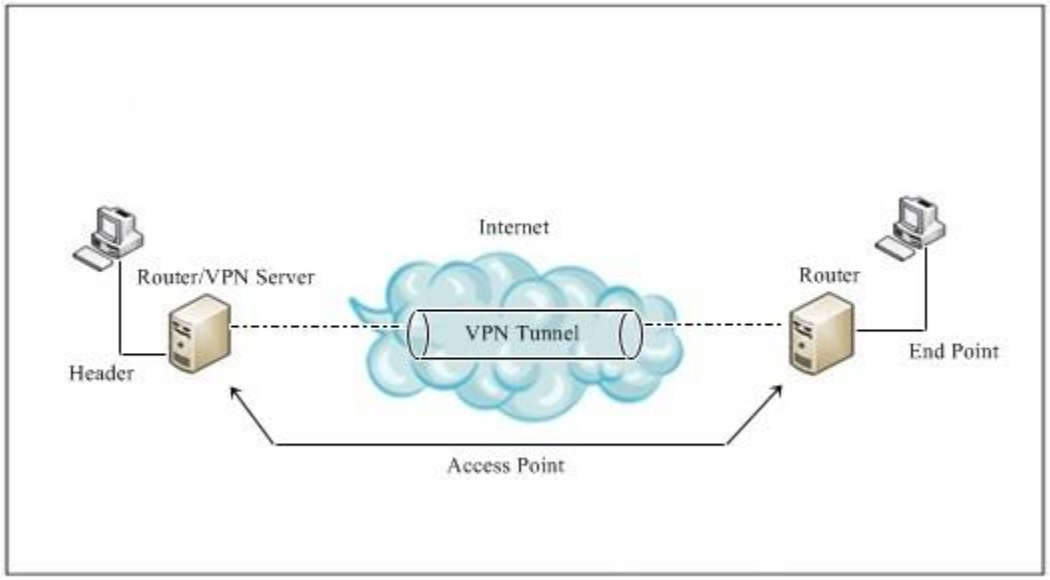
3.1.2.15.3 Protokol Yang Digunakan Dalam VPN

Untuk membangun *site-to-site* VPN, dibutuhkan protokol yang berfungsi mengatur komunikasi diantara beberapa komputer di dalam sebuah jaringan, aturan itu termasuk di dalamnya petunjuk yang berlaku bagi cara-cara atau metode mengakses sebuah jaringan, topologi fisik, tipe-tipe kabel dan kecepatan transfer data.

Protokol yang digunakan pada VPN menekankan pada authentikasi dan enkripsi. Adanya sistem authentikasi akan mengijinkan klien dan *server* untuk menempatkan identitas orang yang berbeda di dalam jaringan secara benar. Enkripsi mengijinkan data yang dikirim dan diterima tersembunyi dari publik saat melewati jaringan publik.

Dalam penelitian ini protokol yang digunakan adalah Tunnel. Tunnel dalam VPN sebenarnya hanya *logical point-to-point connection* dengan otentikasi dan enkripsi. Analoginya adalah jika sebuah organisasi/perusahaan mempunyai kantor di 2 gedung yang berbeda. Proses Enkapsulasi adalah paket lama dibungkus dalam paket baru. alamat ujung tujuan terowongan (*tunnel endpoints*) diletakkan di *destination address* paket baru, yang disebut dengan *encapsulation header*. Tujuan akhir tetap ada pada *header* paket lama yang

dibungkus (*encapsulated*). Saat sampai di *endpoint*, kapsul dibuka, dan paket lama dikirimkan ke tujuan akhirnya. Enkapsulasi dapat dilakukan pada lapisan jaringan yang berbeda. Dibawah ini merupakan gambar dari cara kerja Tunnel pada *site-to-site* VPN:



Gambar 3.9 Gambaran Cara Kerja Tunnel Pada *site-to-site* VPN

3.1.2.15.4 Perangkat VPN

Pada dasarnya, semua perangkat komputer yang dilengkapi dengan fasilitas pengalamatan IP dan diinstal dengan aplikasi pembuat *tunnel* dan algoritma enkripsi dan dekripsi, dapat dibangun komunikasi VPN di dalamnya. Komunikasi VPN dengan *tunneling* dan enkripsi ini dapat dibangun antara sebuah *router* dengan *router* yang lain, antara sebuah *router* dengan beberapa *router*, antara PC dengan server VPN *concentrator*, antara *router* atau PC dengan *firewall* berkemampuan VPN.

Teknologi yang digunakan untuk mengatasi serangan yang terjadi yaitu teknologi *tunneling* merupakan teknologi yang bertugas untuk manangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Disebut *tunnel* karena koneksi *point-to-point* tersebut sebenarnya terbentuk dengan melintasi jaringan umum, namun koneksi tersebut tidak mempedulikan paket-paket data

milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya.

Teknologi ini dapat dibuat di atas jaringan dengan pengaturan IP *Addressing* dan IP *Routing* yang sudah matang. Maksudnya, antara sumber *tunnel* dengan tujuan *tunnel* telah dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP. Apabila komunikasi antara sumber dan tujuan dari *tunnel* tidak dapat berjalan dengan baik, maka *tunnel* tersebut tidak akan terbentuk dan VPN pun tidak dapat dibangun. Apabila *tunnel* tersebut telah terbentuk, maka koneksi *point-to-point* palsu tersebut dapat langsung digunakan untuk mengirim dan menerima data.

3.2 Analisis Kebutuhan Sistem

Berdasarkan uraian permasalahan yang ada saat ini di Universitas Sangga Buana YPKP. Permasalahannya yaitu serangan *spam* DoS terhadap *server mail*, serangan *flooding* terhadap *webserver*, serangan terhadap jaringan *wireless* dari serangan IP *spoofing*. Oleh karena itu diusulkan untuk membuat solusi permasalahan dengan membangun sebuah *firewall* dan VPN (*Virtual Private Network*) menggunakan sistem operasi IPCop.

3.2.1 Analisis Kebutuhan Perangkat Lunak

1. Sistem operasi IPCop Linux yang akan digunakan sebagai *attacker*, *server* dan sebagai *firewall*.

2. Sistem operasi Windows 7 yang akan digunakan sebagai *client* untuk melakukan pengujian.

3. PuTTY untuk mengakses *service* melalui sistem operasi windows *client*.

3.2.2 Analisis Kebutuhan Perangkat Keras.

Kebutuhan perangkat keras minimum:

1. Pada sisi *server*: Komputer dengan prosessor 586 atau lebih, 512 MB RAM dan *disk space* minimal 6 GB yang menjalankan sistem operasi IPCop (Linux).

2. Pada sisi *client*: Komputer dengan prosessor 586 atau lebih, 512 MB RAM dan *disk space* minimal 4 GB.

3.3 Perancangan Sistem

Perancangan sistem adalah suatu proses yang menggambarkan bagaimana suatu sistem dibangun untuk memenuhi kebutuhan pada fase analisis. Adapun tahapan yang dilakukan dalam perancangan sistem ini membahas mengenai tujuan perancangan sistem, dan perancangan topologi jaringan yang akan digunakan di Universitas Sangga Buana YPKP.

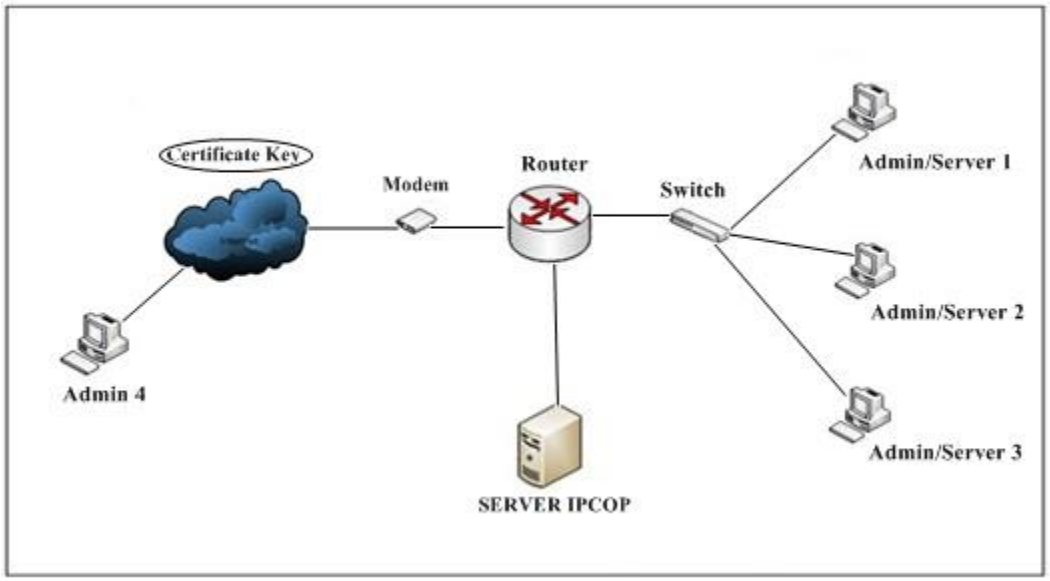
3.3.1 Tujuan Perancangan Sistem

Perancangan sistem merupakan tindak lanjut dari tahap analisa. Perancangan sistem bertujuan untuk memberikan gambaran sistem yang akan dibuat. Dengan kata lain perancangan sistem didefinisikan sebagai penggambaran atau pembuatan sketsa dari beberapa elemen yang terpisah kedalam satu kesatuan yang utuh dan memiliki fungsi. Selain itu, perancangan sistem bertujuan untuk lebih mengarahkan sistem yang terinci, yaitu pembuatan perancangan yang jelas dan lengkap yang nantinya akan digunakan untuk pembuatan simulasi. Hasil dari analisis ini, kemudian dapat digunakan oleh Universitas Sangga Buana YPKP dalam membangun *firewall* dan VPN (*Virtual Private Network*) menggunakan sistem operasi IPCop untuk keamanan data.

3.3.2 Gambaran Sistem

Gambaran sistem ini yang akan digunakan di Universitas Sangga Buana YPKP. Berdasarkan uraian permasalahan yang telah dipaparkan sebelumnya, tujuan dari gambaran sistem yang dibangun untuk membuat solusi dari

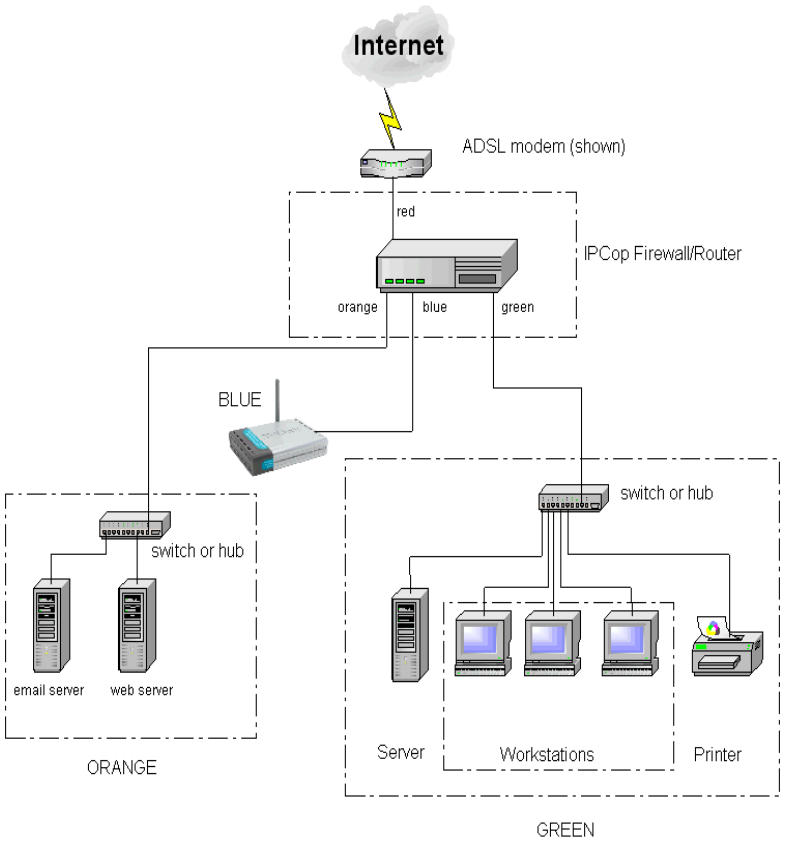
permasalahan yang sering terjadi. Berikut ini gambaran sistem yang akan dibangun dengan diilustrasikan pada gambar 3.8.



Gambar 3.10 Gambaran Sistem.

3.3.3 Perancangan Topologi Jaringan IPCop

Gambaran Topologi Jaringan IPCop di Universitas Sangga Buana YPKP Bandung. Perancangan IPCop ini merupakan gambaran secara global yang digunakan untuk Fakultas Teknik berfungsi untuk mencegah serangan dari jaringan internal dan jaringan eksternal. Berikut perancangan IPCop secara global, akan diilustrasikan pada gambar 3.9 :



Gambar 3.11 Perancangan Topologi Jaringan IPCop.

3.3.3.1 Kebutuhan NIC (Network Interface Card)

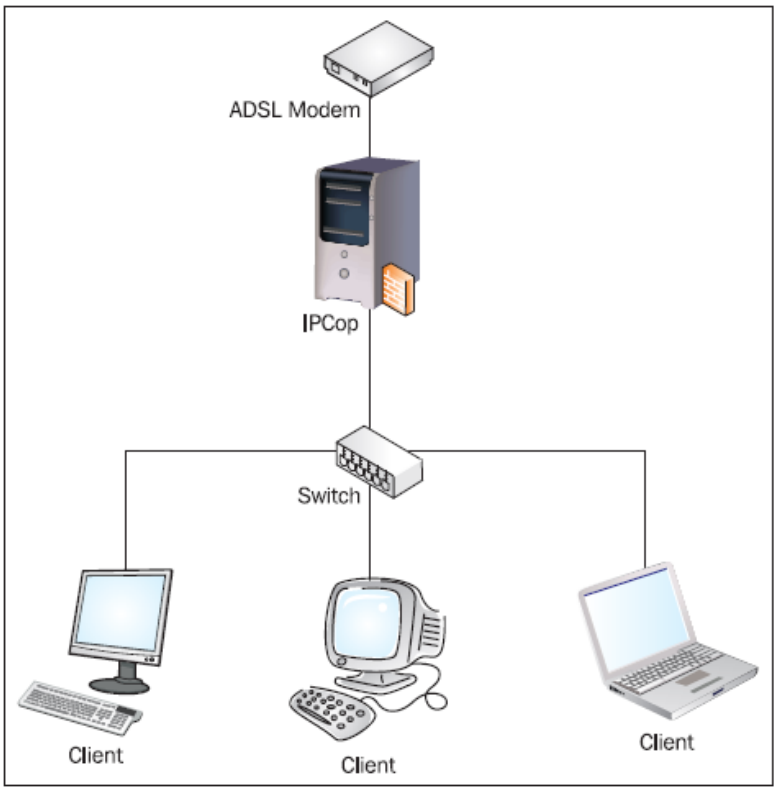
Tabel 3.5 Kebutuhan NIC (Network Interface Card).

Connection	Modem	ISDN	USB ADSL	Ethernet
RED, GREEN	1 NIC (G)	1 NIC (G)	1 NIC (G)	2 NICs (G,R)
RED, BLUE, GREEN	2 NICs (B,G)	2 NICs (B,G)	2 NICs (B,G)	3 NICs (B,G,R)
RED, ORANGE, GREEN	2 NICs (O,G)	2 NICs (O,G)	2 NICs (O,G)	3 NICs (O,G,R)
RED, ORANGE, BLUE, GREEN	3 NICs (O,B,G)	3 NICs (O,B,G)	3 NICs (O,B,G)	4 NICs (O,B,G,R)

Tipe konfigurasi dasar yang digunakan adalah RED/GREEN, dimana IPCop melindungi internal *network* (GREEN) dari internet. Jika untuk mengkonfigurasi *wireless access point*, dapat menghubungkannya ke interface BLUE dan mengkonfigurasi IPCop untuk membatasi akses di *wireless* LAN tersebut. Jika untuk mengkonfigurasi beberapa *server* yang diperbolehkan diakses via internet, dapat diletakkan di *untrusted* DMZ pada interface ORANGE.

Interface RED dapat dihubungkan dengan modem atau NIC, terdapat delapan Tipe Konfigurasi Network.

3.3.4 Perancangan Firewall

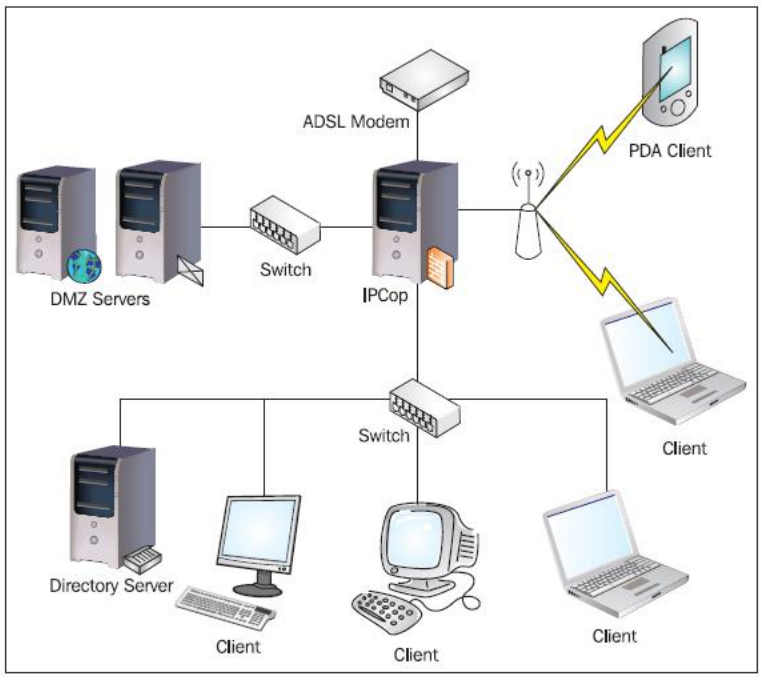


Gambar 3.12 Perancangan Firewall.

Perancangan firewall yang akan digunakan untuk keamanan jaringan di Universitas Sangga Buana YPKP.

3.3.5 Perancangan Topologi VPN

Topologi VPN ini adalah topologi yang akan digunakan untuk implementasi *Site To Site* VPN yang memungkinkan para *user* melakukan koneksi ke jaringan LAN jaringan luar dari tempat yang berbeda di mana dia berada dan dikoneksikan secara aktif sepanjang waktu (24 jam).



Gambar 3.13 Perancangan VPN.

3.3.6 Konfigurasi Sistem Operasi Komputer *Server* dan *Client*

Operating system atau sistem operasi merupakan kumpulan perintah-perintah dasar untuk menjalankan dan mengoperasikan komputer. Oleh karena itu, penentuan sistem operasi yang akan digunakan dalam penelitian ini terbagi atas sistem operasi yang berbeda antara komputer *server* dan komputer *client.*

3.3.6.1 Sistem Operasi Komputer *Server*

Dalam penelitian ini, sistem operasi yang digunakan oleh komputer *server* adalah IPCop (*Linux*).

3.3.6.2 Sistem Operasi Komputer *Client*

Sistem operasi yang digunakan oleh komputer *client* adalah *Windows 7* dan *Windows XP*.