BAB II
KERANGKA TEORITIS

A. Penelitian Rujukan

Pada penelitian sebelumnya sudah banyak dilakukan pada kasus yang berbeda dengan metode yang sama sebagai bahan pertimbangan pada penelitian ini dan untuk mengetahui perbedaan penelitian sebelumnya dengan penelitian akan dilakukan. Berikut adalah penelitian yang telah dilakukan sebelumnya:

1. **Rancang Bangun Keamanan Data Jaringan Komputer Dengan Menggunakan Metode IPSEC VPN** (Studi Kasus: PT. Agrabudi Komunika) (Harun Sujadi, Amiq Burhanuddin, Program Studi Teknik Informatika, Fakultas Teknik Universitas Majalengka 2017)

   Pada penelitian tersebut permasalahan yang dibahas adalah perusahaan tersebut memiliki masalah dalam pengirim data ke perusahaan cabang di daerah lain. Selain itu perusahaan tersebut juga menggunakan jaringan yang terkoneksi ke internet yang memiliki kelemahan yaitu membutuhkan perhatian yang serius pada keamanan jaringan publik. Alat yang digunakan yaitu menggunakan GNS3 dan menggunakan protokol IPSec. Hasil yang di dapat adalah untuk mengamankan sebuah data yang akan dikirim, yaitu dapat menggunakan IPSec VPN. Karena dengan adanya IPSec VPN proses pengiriman data dan penerimaan data dengan nyaman tanpa adanya ganguan dari pihak ketiga karena data yang telah dikirim sudah terenkripsi dengan baik.

2. **Implementasi Keamanan Jaringan Komputer Pada Virtual Private Network (VPN) Menggungakan IPSEC** (Rudol, Program Studi Teknik Informatika STMIK Budi Darma 2017)

   Pada penelitian tersebut permasalahan yang dibahas adalah pada penerapan jaringan VPN yang menggunakan perangkat keras Mikrotik Routerboard dengan protokol IPSec, ada beberapa masalah yang biasa terjadi adalah gangguan pada traffic, serangan pada server, dan pengiriman data dari client yang tidak terdaftar. Pada implementasinya, Peneliti membuat sebuah program aplikasi yang bertujuan memblokir IP client yang tidak terdaftar. Alat yang digunakan yaitu Microsoft Visual Studio .Net 2008 dan Phptriad 2.3 (Mysql). Hasil dari penelitian ini yaitu jaringan yang menggunakan IPSec pada Virtual Private Network jauh lebih aman dengan manggunakan Transport Mode dan Tunnel mode yang ada pada IPSec itu sendiri sehingga jaringan VPN benar-

benar aman dan serangan yang di lakukan menggunakan ping of death dapat di cegah dengan melakukan pemblokiran IP client yang tidak terdaftar.

3. **Implementasi Remote Desktop Melalui VPN Berbasis IPSEC Pada Smartphone Dengan Menggunakan Vyatta OS** (Kiki Agnia Maryam Larasati, Moch. Fahru Rizal, Eddy Prasetyo Nugroho, Teknik Komputer, Universitas Telkom 2015)

   Pada penelitian tersebut permasalahan yang dibahas adalah Remote User VPN dengan Vyatta OS dan pengamanan data saat proses transmisi. Penggunaan OS Android di bahas dalam skema monitoring dan akses data. Penelitian ini bertujuan untuk menyediakan jalur komunikasi private untuk terhubung dengan LAN perusahaan guna monitoring dan mengakses data perusahaan menggunakan smartphone. Prototipe jaringan dibangun dengan aplikasi remote desktop melalui VPN (Virtual Private Network) berbasis IPSec. Hasil dari penelitian ini menyimpulkan bahwa teknologi VPN berbasis IPSec yang dibangun berhasil menyediakan layanan akses data, resource monitoring dan trafik, dan remote desktop yang aman. Protokol keamanan IPSec berfungsi dengan baik dalam mengenkripsi data yang dikirim, sehingga sniffer tidak dapat membaca trafik protokol-protokol yang berjalan antara client dan web server maupun pada saat proses remote desktop.

4. **Analisis Dan Optimalisasi Keamanan Jaringan Menggunakan Protokol IPSEC** (Syarif Hidayatulloh, Universitas BSI 2014)

   Pada penelitian tersebut permasalahan yang dibahas yaitu penelitian ini fokus dalam menganalisa dan mengeskplorasi fitur keamanan jaringan dalam Microsoft windows. Microsoft windows dapat memenuhi kebutuhan sistem dalam mengimplementasikan IPSec tanpa membutuhkan tambahan perangkat lunak lain sehingga lebih efisien dan dapat menghindari penggunaan banyak aplikasi dalam sebuat desain sistem keamanan jaringan.

   Dengan menggunakan IPSec keamanan pada jaringan komputer akan meningkat karena IPSec melakukan enkripsi terhadap data yang dikirim pada jaringan tersebut. Seandainya terjadi penyadapan data oleh pihak ketiga, maka data asli tidak dapat dilihat dengan mudah tanpa mengetahui kunci enkripsi yang digunakan. IPSec akan melindungi data secara otomatis tanpa sepengetahuan pengguna jaringan komputer sehingga pengguna dapat melakukan pengiriman data seperti biasa tanpa ada prosedur khusus yang harus dilakukan.

Implementasi IPSec dapat dilakukan dengan mudah sehingga tidak memerlukan keahlian khusus yang harus dimiliki administrator jaringan.

IPSec dapat diimplementasikan dalam berbagai kasus baik dalam model jaringan client server seperti contoh diatas ataupun model jaringan point to point dengan memanfaatkan fitur tunnel dalam IPSec.

5. **Implementasi Virtual Private Network Openstack Terkoneksi Dengan Virtual Private Network Mikrotik Untuk Komunikasi Data Lebih Aman** (Cholifah Sulistin Angraeni, Hary Nugroho, Ega Dian Pramesta, Akademi Teknik Telekomunikasi Sandhy Putra Jakarta 2017)

   Pada penelitian ini penulis menerapkan sistem VPN (Virtual Private Network) untuk mempermudah komunikasi melalui jaringan publik, dan terkoneksi dengan jaringan lokal (LAN). VPN dapat terjadi antara dua PC atau lebih dengan menggunakan jaringan yang berbeda. Sistem operasi perangkat lunak yang dapat digunakan untuk menjadikan PC sebagai router network yaitu MikroTik yang memiliki keamanan jaringan IPSec (Internet Protocol Security). VPN dapat dibentuk dengan menggunakan teknologi tunneling dan enkripsi. Penggunaan enkripsi dalam teknologi VPN, jaringan VPN tidak dapat dibaca oleh pihak-pihak yang tidak berkepentingan karena melewati proses dekripsi terlebih dahulu. Hasil yang di dapat dari penelitian ini yaitu nilai Bandwidth yang dihasilkan pada saat melakukan Upload File memiliki hasil 0,267 Mbit/sec dan untuk hasil Download File bernilai 0,162 Mbit/sec. Sedangkan untuk hasil Packet Loss pada saat melakukan Upload File memiliki hasil yang bagus yaitu 0%, dan untuk nilai yang didapat pada saat mendownload yaitu 0%. Menurut standar TIPHON dan ITU-T nilai-nilai Packet Loss yang didapat memenuhi standar kategori degredasi, nilai yang sangat bagus adalah 0%, untuk kategori bagus memiliki nilai 3%, pada katagori sedang memiliki nilai 15%, dan untuk kategori jelek memilki nilai 25%.

6. **Analisis Unjuk Kerja Virtual Private Network PPTP Dan L2TP Pada Jaringan Berbasis Mikrotik** (Yulyus Effendi Pradana, Jusak, Yosefine Triwidyastuti, Program Studi Sistem Komputer Institut Bisnis Dan Informasi STIKOM Surabaya 2016)

   Pada penelitian tersebut permasalahan yang dibahas yaitu kebutuhan akan komunikasi data saat ini sudah menjadi kebutuhan yang utama bagi instusi ataupun perusahaan yang sedang mendirikan cabang-cabangnya di berbagai lokasi. Adanya kendala apabila antara cabang yang satu dengan yang lainnya

tidak dapat berkomunikasi seperti yang mengharuskan mengakses file-file yang ada pada database server yang berada di kantor pusat yang tidak di routing pada jaringan Internet. Untuk mengimplementasikan ide tersebut maka akan dibuat video streaming yang menggunakan teknologi VPN dengan menggunakan protokol PPTP dan L2TP. Selanjutnya adalah melakukan analisis unjuk kerja protokol PPTP dan L2TP yang menggunakan parameter berdasar QoS (Quality of Service) pada jaringan VPN dengan menggunakan parameter yang meliputi seperti Latency (delay), Throughput, dan Packet loss. Dengan adanya analisis menggunakan jaringan VPN ini diharapkan para pengguna teknologi video streaming dapat untuk mengetahui sejauh mana unjuk kerja pada jaringan dengan protokol PPTP dan L2TP untuk layanan video streaming. Hasil dari penelitian ini yaitu nilai delay, throughput dan packet loss di kedua protokol VPN PPTP dan L2TP tidak terlalu memiliki perbedaan yang besar dan terlihat sama dikarenakan karena pada dasarnya protokol PPTP dan L2TP sama-sama melewati jaringan cloud internet hanya perbedaan enkapsulasi pada format header L2TP lebih banyak dibandingkan dengan format header PPTP. Dari kedua implementasi di atas dapat disimpulkan jika network administrator ingin keadaan jaringan dengan nilai QOS yang bagus dengan mengesampingkan keamanan jaringan maka tunneling dengan protokol PPTP dapat digunakan, akan tetapi jika network administrator ingin memprioritaskan keamanan jaringan maka tunneling dengan protokol L2TP merupakan pilihan yang tepat karena L2TP dapat dikombinasikan dengan enkripsi IPSec yang jauh lebih aman daripada enkripsi pada protokol PPTP yaitu MPPE (Microsoft Point To Point Encryption). L2TP dengan IPSec menyediakan keamanan berlapis yang dapat menjamin keamanan data yang dilewatkan didalamnya.

B. Landasan Teori

1. Informasi

Informasi ibarat darah yang mengalir didalam tubuh suatu organisasi sehingga informasi ini sangat penting didalam suatu organisasi. Suatu sistem yang kurang mendapatkan informasi akan menjadi luruh, kerdil, dan akhirnya mati. Informasi adalah data yang telah diklasifikasikan atau diolah atau diinterpretasi untuk digunakan dalam proses pengambilan keputusan. Nilai informasi berhubungan dengan keputusan, bila tidak ada pilihan atau keputusan, maka informasi menjadi tidak diperlukan. Tata Sutabri, S.Kom, MMSi (2016, p.26)

Sumber infnormasi adalah data. Data merupakan kenyataan yang menggambarkan suatu kejadian serta merupakan suatu kesatuan yang nyata dan merupakan suatu bentuk yang masih mentah yang belum dapat bercerita banyak sehingga perlu diolah lebih lanjut melalui suatu model untuk menghasilkan informasi. Jelaslah kiranya bahwa data merupakan sumber dan bahan informasi.

2. Jaringan Komputer

Jaringan komputer adalah sebuah kumpulan komputer, printer, dan peralatan lainnya yang saling terhubung. Informasi dan data bergerak melalui kabel-kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data. Edy Victor Haryanto (2012, p.12)

Konsep jaringan komputer lahir pada tahun 1940-an di Amerika dari sebuah proyek pengembangan komputer MODEL I di laboratorium Bell dan grup riset *Harvard University* yang dipimpin Prof. H. Aiken. Pada mulanya, proyek tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer untuk dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (*batch processing*), sehingga beberapa program bisa dijalankan dalam sebuah komputer dengan kaidah antrian.

3. Jaringan Lokal

Jaringan lokal atau Local Area Network (LAN) dapat didefinisikan sebagai network atau jaringan sejumlah sistem komputer yang lokasinya terbatas di dalam satu gedung, satu kompleks gedung atau suatu kampus dan tidak menggunakan media fasilitas komunikasi umum seperti telepon, melainkan pemilik dan pengelola media komunikasinya adalah pemilik LAN itu sendiri. Gin-gin Yugianto & Oscar Rachman (2012, p.2)

Dari definisi diatas dapat diketahui bahwa sebuah LAN dibatasi oleh lokasi secara fisik. Adapun penggunaan LAN itu sendiri mengakibatkan semua komputer yang terhubung dalam jaringan dapat bertukar data atau dengan kata lain berhubungan. Kerjasama ini semakin berkembang dari hanya pertukaran data hingga penggunaan peralatan secara bersama.

4. Internet

Internet atau Internetworking secara umum didefinisikan sebagai jaringan komputer terbesar di dunia yang menghubungkan semua jaringan komputer yang ada (Intranet, Wide Area Network, Metropolitan Area Network, Personal Area

Network, dan lain-lain) beserta dengan semua komputer, perangkat terhubung (smartphone, tablet, komputer benam, switch, router, hub, dan perangkat penghubung lainnya), serta pengguna komputer itu sendiri ke dalam satu wadah jaringan komputer dunia. I Putu Agus Eka Pratama, S.T, M.T (2015, p.37)

5. Topologi

Topologi dalam jaringan mengandung dua pengertian dilihat dari sisi pengkabelan dan dari sisi aliran data. Jika dilihat dari aliran data pada jaringan, maka topologi yang dimaksud adalah topologi ogika. Topologi logika jaringan komputer adalah gambaran bagaimana aliran data dalam suatu jaringan. Dari kenampakan fisik pengkabelan, maka topologi yang dimaksud adalah topologi fisik. Topologi fisik jaringan komputer adalah konfigurasi semua komputer baik workstation maupun server, peralatan sert kabel dalam suatu jaringan. Topologi merupakan gambaran bagaimana komputer dan peralatan jaringan tersusun dalam suatu jaringan. Wagito (2007, p.15)

Pada jaringan komputer, dikenal setidaknya enam buah topologi pada jaringan komputer. Keenam jenis topologi pada jaringan tersebut memiliki karakteristik, kelebihan, dan kekurangan masing-masing. Keenam topologi pada jaringan komputer ini meliputi topologi bus, topologi star, topologi peer to peer (P2P), topologi ring, topologi tree, dan topologi mesh.

6. IP Public

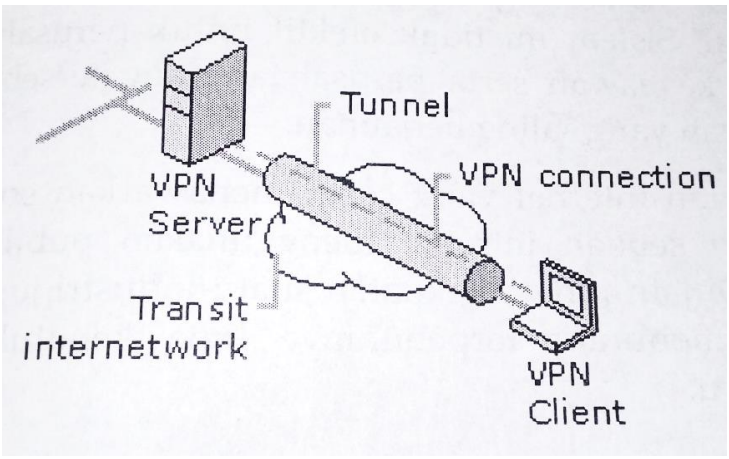
IP Address Public merupakan IP Address yang bersifat unik (pada bagian network identifier) untuk setiap komputer dan digunakan pada jaringan internet. IP Address Public ini hanya dimiliki oleh masing-masing komputer diseluruh dunia, termasuk juga perangkat-perangkat terhubung lainnya, untuk memudahkan di dalam saling mengenali satu sama lain. Umunya pengguna internet memperoleh IP Address Public secara otomatis dari provider (penyedia jasa layanan akses internet). Alamat dari IP Address Public dapat diakses dari manapun juga, asalkan terhubung ke dalam jaringan internet. I Putu Agus Eka Pratama, S.T, M.T (2015, p.390)

7. Virtual Private Network (VPN)

VPN (Virtual Private Network) merupakan suatu cara untuk membuat sebuah jaringan bersifat “private” dan aman dengan menggunakan jaringan publik misalnya internet. VPN dapat mengirim data antara dua komputer yang

melewati jaringan publik sehingga seolah-olah terhubung secara point to point. Aris Wendy & Ahmad SS Ramadhana (2005, p.1)

VPN dapat terjadi antara dua end-system atau dua PC atau bisa juga antara dua atau lebih jaringan yang berbeda. VPN dapat dibentuk dengan menggunakan teknologi tunneling dan encryption, data dienkapsulasi (dibungkus) dengan header yang berisi informasi routing untuk mendapatkan koneksi point to point sehingga data dapat melewati jaringan publik dan dapat mencapai akhir tujuan. Sedangkan untuk mendapatkan koneksi bersifat private, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi.



Gambar 2.1 Konsep VPN

Teknologi VPN menyediakan tiga fungsi utama untuk penggunanya. Ketiga fungsi utama tersebut antara lain sebagai berikut:

a. Confidentially (Kerahasiaan)

   Dengan digunakannnya jaringan publik yang rawan pencurian data, maka teknologi VPN menggunakan sistem kerja dengan cara mengenkripsi semua data yang lewat melauinya. Dengan adanya teknologi enkripsi tersebut, maka kerahasiaan data dapat lebih terjaga. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak. Dengan menerapkan sistem enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah.

b. Data Intergrity (Keutuhan Data)

   Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai

gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.

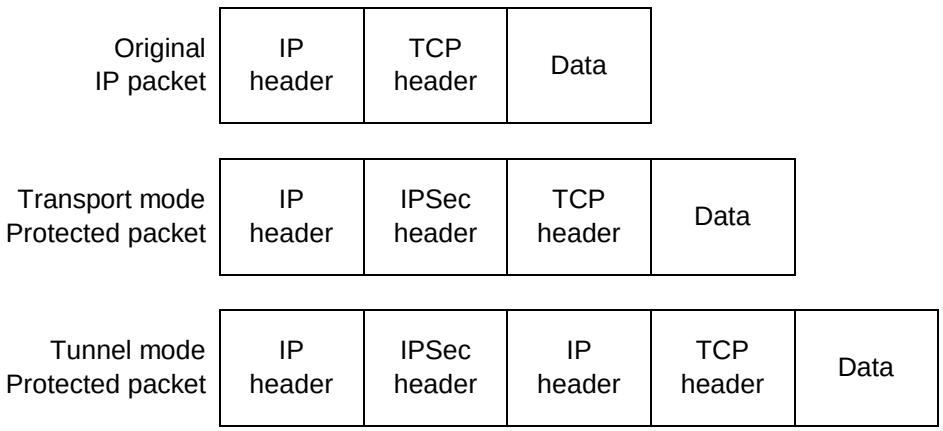
c. Origin Authentication (Autentikasi Sumber)

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain.

8. Internet Protocol Security (IPSec)

IPSec merupakan protokol standar yang digunakan untuk memberikan keamanan untuk berkomunikasi melalui jaringan IP dengan menggunakan layanan enkripsi keamanan (cryptographic security services). Aris Wendy & Ahmad SS Ramadhana (2005, p.8)

IPSec menyediakan keamanan pada level network layer, IPSec didesain sebagai cryptographic protokol yang berfungsi untuk keamanan data dan key exchange. Protokol IPSec diimplementasikan kedalam network layer, yaitu layer ketiga pada OSI layer yang mengerjakan layanan network routing, flow control, segmentation (desegmentation) dan error control functions.



Gambar 2.2 Format Datagram IPSec

IPsec mendukung dua buah sesi komunikasi keamanan, yakni sebagai berikut:

a. Protokol Authentication Header (AH)

   Menawarkan autentikasi pengguna dan perlindungan dari beberapa serangan (umumnya serangan man in the middle), dan juga menyediakan fungsi autentikasi terhadap data serta integritas terhadap data. Protokol ini mengizinkan penerima untuk merasa yakin bahwa identitas si pengirim adalah benar adanya, dan data pun tidak dimodifikasi selama transmisi. Namun, protokol AH tidak menawarkan fungsi enkripsi terhadap data yang ditransmisikannya. Informasi AH dimasukkan ke dalam header paket IP yang dikirimkan dan dapat digunakan secara sendirian atau bersamaan dengan protokol Encapsulating Security Payload.

b. Protokol Encapsulating Security Payload (ESP)

   Protokol ini melakukan enkapsulasi serta enkripsi terhadap data pengguna untuk meningkatkan kerahasiaan data. ESP juga dapat memiliki skema autentikasi dan perlindungan dari beberapa serangan dan dapat digunakan secara sendirian atau bersamaan dengan Authentication Header. Sama seperti halnya AH, informasi mengenai ESP juga dimasukkan ke dalam header paket IP yang dikirimkan.

Kelebihan IPSec dibanding protokol VPN yang lain yaitu :

a. Tersedia di semua perangkat dan sistem operasi modern.
b. IPSec sangat mudah dikonfigurasi.
c. IPSec lebih baik daripada PPTP dikarenakan metode enkripsi yang baik antara *endpoint* VPN.

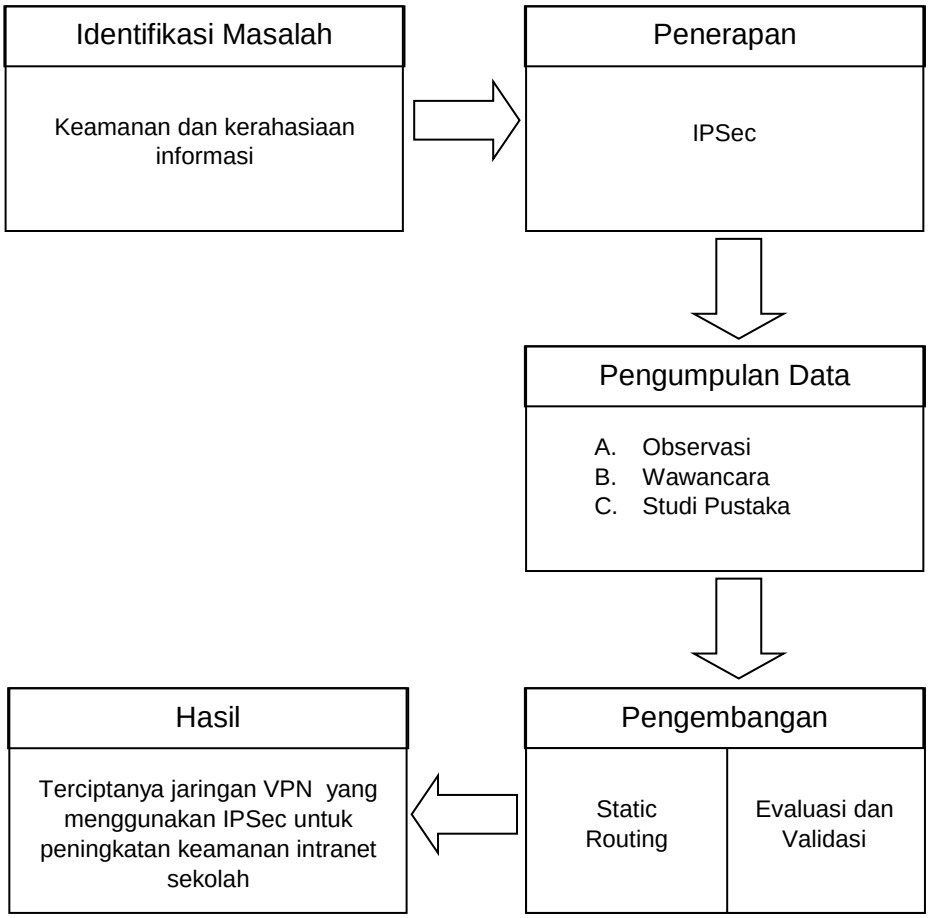
9. TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protokol) didefinisikan sebagai pasangan paket protokol didalam jaringan komputer, yang secara hirarkis dibentuk dari susunan modul-modul interaktif yang saling mendukung satu sama lain. I Putu Agus Eka Pratama, S.T, M.T (2015, p.90)

TCP/IP dibangun dengan dukungan empat buah layer perangkat lunak yang berbasiskan pada perangkat keras di jaringan komputer. Itu sebabnya didalam pemodelan layer komputer terdapat layer TCP/IP selain pemodelan layer OSI. Pemodelan layer TCP/IP lebih banyak digunakan saat ini karena simpel, mudah dipahami, serta semakin mendukung aplikasi dan fungsionalitas serta perkembangan dunia jaringan komputer saat ini.

C. Kerangka Pemikiran

Berikut adalah kerangka pemikiran untuk pemecahan masalah dalam penelitian ini yang digambarkan pada gambar 2.3.



Gambar 2.3 Kerangka Pemikiran

Penjelasan tentang kerangka pemikiran pada penelitian ini adalah:

1. Identifikasi masalah untuk menetapkan tujuan penelitian.
2. Melakukan penerapan IPSEC pada VPN untuk meningkatkan keamanan intranet sekolah.
3. Melakukan pengumpulan data untuk mengetahui kondisi yang ada dan memenuhi kebutuhan setiap user.
4. Melakukan pengembangan melalui tahap perancangan, tahap implementasi, dan tahap pengujian.
5. Melakukan evaluasi terhadap jaringan VPN yang dikembangkan.