IMPLEMENTASI *VIRTUAL PRIVATE NETWORK* SEBAGAI MEDIA KOMUNIKASI DATA TERENKRIPSI DI PANGKALAN DATA PERGURUAN TINGGI UNIVERSITAS INDONESIA TIMUR MAKASSAR

Oleh :

Ucok

DosenTeknik Informatika,Fakultas Ilmu Komputer UIT
E-mail: ucok_sinaga@gmail.com

ABSTRAK

Sebuah pangkalan data perguruan tinggi dapat berhubungan antar jaringan lokal (*private*) yang ada di lokasi berbeda dengan menggunakan *leased line*. Namun biaya yang dibutuhkan untuk membangun infrastuktur jaringan yang luas menggunakan *leased line* sangat besar. Oleh karena itu VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan publik yang sudah ada (internet). Kantor pdpt melakukan *transfer* data antar operator ataupun sebaliknya dengan menggunakan *email*. *Email* yang digunakan memiliki keterbatasan *size* dan sangat rentan terhadap pihak-pihak yang tidak berwenang serta tidak terjamin keabsahan data/ informasi yang dikirim. Untuk itu dibutuhkan sebuah jaringan *private* yang dapat menghubungkan jaringan local pdpt dengan jaringan luar pdpt dengan menggunakan media jaringan publik yang sudah ada (*internet*), dan dapat menjaga keabsahan serta dapat menentukan pihak-pihak yang berhak menerima data/ informasi yang dikirim.

Kata Kunci: VPN, PPTP, Komunikasi Data.

A. PENDAHULUAN

Virtual Private Network yang artinya membuat jaringan *private* secara *virtual* di atas jaringan *public* (umum) seperti internet. Saat ini jaringan komputer sangatlah penting dalam menunjang komunikasi khususnya di sekolah. Banyak keuntungan yang dapat diperoleh dari penggunaan jaringan komputer, misalnya komunikasi antar klien menjadi lebih mudah dan cepat, remote server melalui jaringan komputer atau juga untuk aplikasi client-server di dalam sekolah. Banyak sekali manfaat dari hal di atas, tetapi ada satu hal yang tidak boleh di lupakan yaitu Keamanan. Keamanan jaringan komputer sangat penting untuk efisiensi dan efektifitas kinerja dari suatu jaringan komputer.

Sebuah pangkalan data perguruan tinggi dapat berhubungan antar jaringan lokal (*private*) yang ada di lokasi berbeda dengan menggunakan *leased line*. Namun biaya yang dibutuhkan untuk membangun infrastuktur jaringan yang luas menggunakan *leased line* sangat besar. Di sisi lain pangkalan data ingin mengoptimalkan biaya dalam membangun jaringan mereka. Oleh karena itu VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan publik yang sudah ada (internet).

Kantor pdpt melakukan *transfer* data antar operator ataupun sebaliknya dengan menggunakan *email*. *Email* yang digunakan memiliki keterbatasan *size* dan sangat rentan terhadap pihak-pihak yang tidak berwenang serta tidak terjamin keabsahan data/ informasi yang dikirim. Untuk itu dibutuhkan sebuah jaringan *private* yang dapat menghubungkan jaringan local pdpt dengan jaringan luar pdpt

dengan menggunakan media jaringan publik yang sudah ada (*internet*), dan dapat menjaga keabsahan serta dapat menentukan pihak-pihak yang berhak menerima data/ informasi yang dikirim.

Berdasarkan dari uraian diatas maka penulis tertarik untuk mengambil judul : Implementasi Virtual Private Network Sebagai Media Komuikasi Data Terenkripsi Di Pangkalan Data Perguruan Tinggi Universitas Indonesia Timur Makassar.

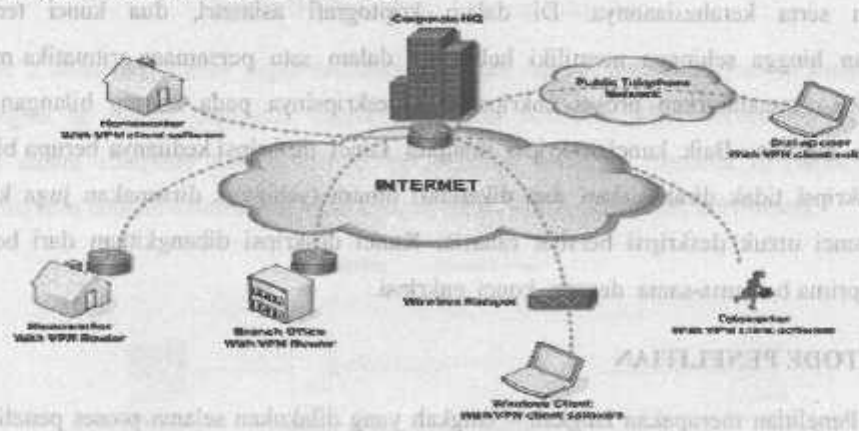
B. TINJAUAN PUSTAKA

Jaringan Komputer

Penggabungan komputer dan komunikasi telah memiliki pengaruh besar di sistem komputer yang terorganisir. Konsep "Pusat komputer" sebagai sebuah ruangan dengan komputer besar yang membawa pengguna mereka bekerja untuk pengolahan data sekarang telah benar-benar usang (meskipun pusat data memegang ribuan Internet server menjadi umum). Model lama satu komputer melayani semua kebutuhan komputasi organisasi telah digantikan oleh di mana sejumlah besar komputer yang terpisah tetapi saling berhubungan melakukan pekerjaan. Sistem ini disebut jaringan komputer (Muhammad iswan).

VPN

White paper, Analisis dan Peracancangan VPN menggunakan VPN PPTP mengatakan secara spesifik "*Teknologi VPN merupakan teknologi yang sangat cepat pertumbuhannya dan menyediakan transmisi data yang aman melalui infrasruktur jaringan publik. Meskipun VPN tidak sangat kebal terhadap serangan keamanan, VPN menyediakan enkripsi end to end yang sangat efektif. VPN juga efektif digunakan saat klien melintas atau rooming pada tipe jaringan wireless yang berlainan karena eroperasi pada level koneksi jaringan yang berlainan. VPN secara khusus mempunyaitiga skenario yang berbeda yaitu untuk remote user, koneklivitas LAN to LAN, dan untuk penggunaan Extranet. VPN menggunakan teknik kriptografi untuk melindungi informasi IP saat melintas dari satu jaringan ke jaringan yang lain atau dari lokasi satu ke lokasi yang lain. Data akan dibungkus dengan teknik 'tunnel', yang akan mengenkripsi dan mengisolasi data sehingga dapat menggunakan jaringan lalu lintas public dengan lebih aman*" (bina nusantara).



Gambar 1. Arsitektur VPN

Keamanan *VPN*

Seperti yang telah dijelaskan bahwa VPN menggunakan intranet sebagai media perantaranya, maka keamanan pada jaringan VPN sangatlah diperlukan agar data yang dikirim dan diterima dapat terjamin keamanannya. Beberapa ide keamanan yang dapat diterapkan pada teknologi VPN adalah enkripsi, autentikasi, autorisasi, dan firewall (bina nusantara).

Tunelling

Teknologi *tunneling* merupakan teknologi yang bertugas untuk menangani dan meneydiakan 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 memperdulikan paket-paket data milik orang lain yang sama-sama melintasi umum tersebut,tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya.Teknologi ini dapat dibuat diatas jaringan dengan pengaturan *IP Addressing* dan *IP Routing* yang sudah baik atau telah terhubung sehingga antara sumber *tunnel* dengan tujuan *tunnel* dapat saling berkomunikasi antara sumber *tunnel* dengan tujuan *tunnel* dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP.

Apabila komunikasi antara sumber dan tujuan dari *tunnel* tidak dapat berjalan dengan baikmmaka *tunnel* tersebut tidak akan terbentuk dan VPN pun tidak dapat dibangun. Setelah *tunnel* tersebut terbentuk maka koneksi *point-to-point* tersebut dapat langsung digunakan untuk mengirim dan menerima data.Dalam penerapannya di VPN, *tunnel* dilengkapi dengean sebuah sistem enkripsi untuk menjaga data-data yang terlewati *tunnel* tersebut. Proses enkripsi inilah yang menjadikan teknologi VPN menjadi aman dan bersiifat pribadi (bina nusantara).

RSA

Algoritma RSA merupakan penerapan dari kriptografi asimetri, yakni jenis kriptografi yang menggunakan dua kunci yang berbeda: kunci publik (*public key*) dan kunci pribadi (*private key*). Dengan demikian, maka terdapat satu kunci, yakni kunci publik, yang dapat dikirimkan melalui saluran yang bebas, tanpa adanya suatu keamanan tertentu. Hal ini bertolak belakang dengan kriptografi simetri yang hanya menggunakan satu jenis kunci dan kunci tersebut harus terjaga keamanan serta kerahasiaannya. Di dalam kriptografi asimetri, dua kunci tersebut diatur sedemikian hingga sehingga memiliki hubungan dalam satu persamaan aritmatika modulo.

RSA mendasarkan proses enkripsi dan deskripsinya pada konsep bilangan prima dan aritmatika modulo. Baik kunci enkripsi maupun kunci deskripsi keduanya berupa bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diketahui umum (sehingga dinamakan juga kunci publik), namun kunci untuk deskripsi bersifat rahasia. Kunci deskripsi dibangkitkan dari beberapa buah bilangan prima bersama-sama dengan kunci enkripsi.

C. METODE PENELITIAN

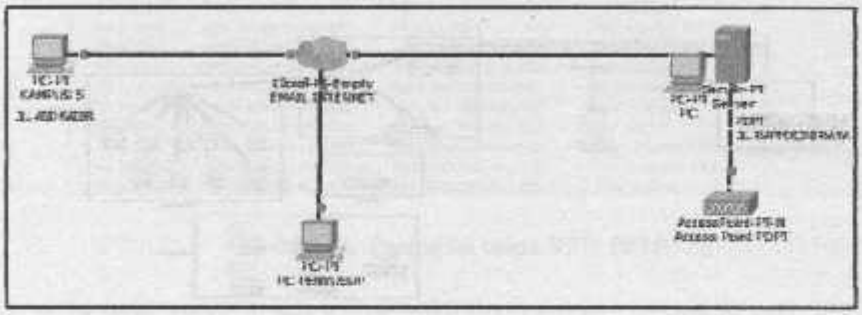
Tahapan Penelitian merupakan langkah – langkah yang dilakukan selama proses penelitian sehingga penelitian ini diharapkan dapat lebih terarah. Dalam penelitian ini terdapat Tiga tahapan yang dilakukan, antara lain observasi, wawancara, studi literatur. Penelitian ini menggunakan metode *System Development Life Cycle (SDLC)* yang diterdir dari tahap perencanaan, tahap analisa, tahap

perancangan, tahap implemetai, tahap uji coba dan tahap penggunaan. Konsep perancangan sistem menggunakan model *prototype*.

D. HASIL DAN PEMBAHASAN

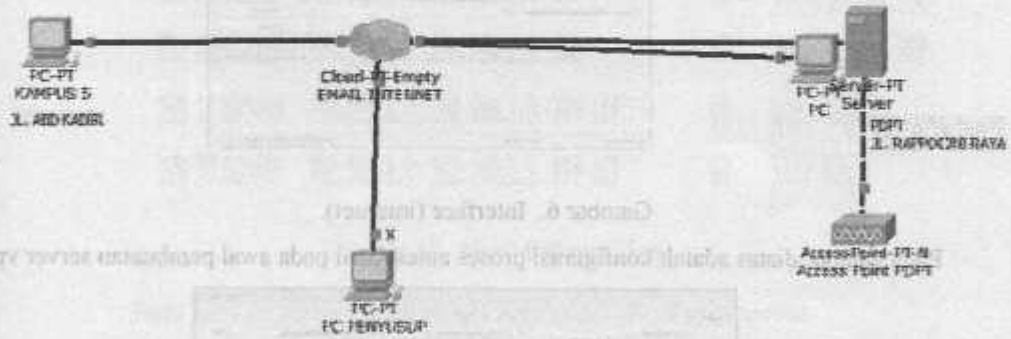
Analisa dan Perancangan.

Dari hasil analisis kondisi awal maka rancangan sistem digambarkan seperti gambar berikut :



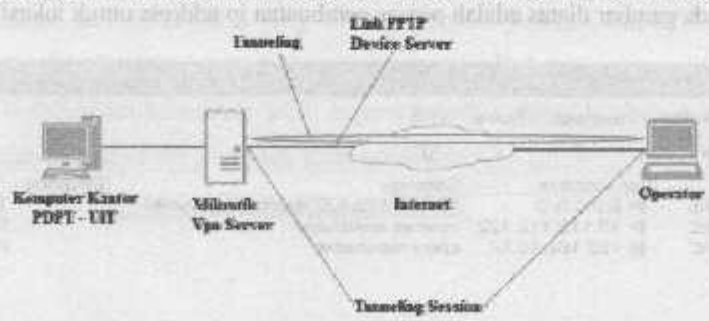
Gambar 2. Arsitektur Jaringan lama

Pada gambar diatas komputer Operator mengirim data melalui email melalui internet kemudiankomputer kantor mengunduh data tersebut melaui email. Akan tetapi topologi ini masih rentan terhadap pihak-pihak yang tidak berwenang menerima data tersebut.



Gambar 3. Rancangan Jaringan diusulkan

Pada gambar 2 komputer kantor dapat terhubung dengan laptop guru walaupun ip *public* pegawai berbeda dengan ip *public* computer kantor. Disinilah mikrotik VPN server berperan sebagai penghubung antara computer kantor dan laptop pegawai walaupun berbeda ip *public* dan dapat berkomunikasi data dengan aman tanpa takut dengan pihak-pihak yang tidak berwenang.

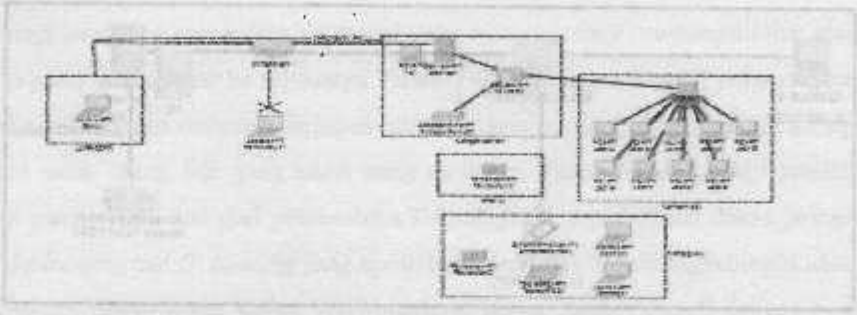


Gambar 4. Rancangan Komunikasi Data

Pada gambar diatas komunikasi data antara computer guru dengan computer kantor menggunakan metode *tunneling* (terowongan) yang membuat terowongan virtual diatas jaringan publik. Metode *tunneling* ini menggunakan protocol *Point to Point Protocol* (PPTP).

Implementasi.

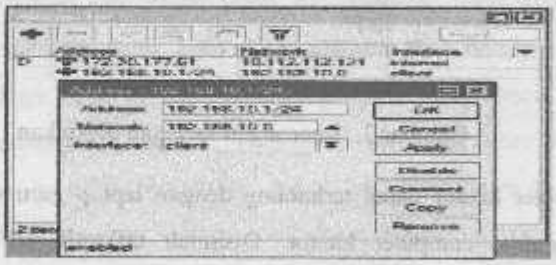
Dari hasil penilitian yang telah dilakukan oleh penulis dapat di paparkan gambaran topologi jaringan sebagai berikut:



Gambar 5. Topologi Jaringan

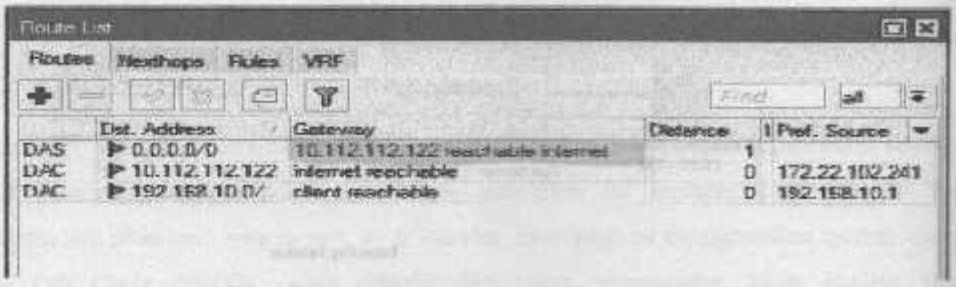
Gambar 6. Interface (internet).

Pada gambar diatas adalah konfigurasi proses autentikasi pada awal pembuatan server vpn.



Gambar 7. *Addres List*

pada gambar diatas adalah proses pembuatan ip address untuk lokasi alamat ip user vpn .

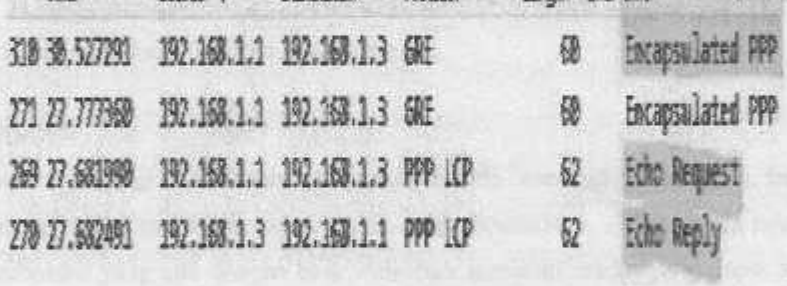


Gambar 8. Route list.

Pada gambar diatas adalah konfigurasi ip route atau dinamic gateway pada mikrotik

Gambar 9. Pengujian tanpa VPN PPTP

Pada gambar diatas dapat dilihat pada saat mengirim data dari client ke server, data tersebut langsung diterima oleh server tanpa melalui proses enkripsi.



Time	Source	Destination	Protocol	Length	Info
270 27.777960	192.168.1.1	192.168.1.3	GRE	60	Encapsulated PPP
269 27.681980	192.168.1.1	192.168.1.3	PPP LCP	62	Echo Request
270 27.682491	192.168.1.3	192.168.1.1	PPP LCP	62	Echo Reply

Gambar 10. Hasil Enkripsi data

Pada gambar diatas adalah proses autentikasi client pada server

E. KESIMPULAN

Dari Hasil pembahasan yang telah diuraikan pada bab sebelumnya, maka dapat diambil kesimpulan sebagai berikut:

1. Hasil menunjukkan bahwa system pengiriman data yang tidak menggunakan VPN lebih rentan. Hal ini dapat dilihat dari paket-paket yang ditangkap, pada jaringan tanpa VPN datanya tidak terenkripsi, jadi mudah diambil maupun dimanfaatkan oleh pihak lain.
2. Jaringan VPN memberikan keamanan lebih terjamin karena menggunakan system authentikasi pada username dan password yang berbeda pada setiap user

DAFTAR PUSTAKA

Muhammad iswan, *implementasi VPN remote access dengan linux openswan*, Halaman 9, *http://repository.unjkt.ac.id/dspace/bitstream/123456789/3723/1/L.MUHAMMAD%20ISWAN-FST.pdf*, 24 Februari 2016.

Hesti rahayu, *analilis dan perancangan vpn menggunakan vpn pptp yang disimulasikan dengan vmware pada client isp jadtayu network*, halaman 4, *http://repository.amikom.ac.id/index.php/detail/4241/ANALISIS%20DAN%20PERANCANGAN%20VPN%20MENGGUNAKAN%20VPN%20PPTP%20YANG%20DISIMULASIKAN%20DENGAN%20VMWARE%20PADA%20CLIENT%20ISP%20JADTAYU%20NETWORKS*, 24 Februari 2016.

Bina nusantara, *implementasi topologi jaringan vpn menggunakan openvpn*, halaman 6,7,13,14,15,16,17,18,19,20,21,23,24,26,30,31, *http://library.binus.ac.id/eColls/eThesisdoc/Bab2/2013-1-01083-IF%20Bab2001.pdf* , 25 Februari 2016.

Yulius Caesar, *PENERAPAN VIRTUAL PRIVATE NETWORKMENGGUNAKAN MIKROTIK ROUTER PADA RS IMMANUEL BANDUNG* , halaman 7, *https://www.academia.edu/13969543/PENERAPAN_VIRTUAL_PRIVATE_NETWORK_MENGGUNAKAN_MIKROTIK_ROUTER_PADA_RS_IMMANUEL_BANDUNG_SKRIPSI*, 27 Februari 2016.

Utami, Jurnal komunikasi data, Halaman 1, https://www.academia.edu/10253546/KOMUNIKASI_DATA, 26 Februari 2016.

Efrianto, *email*, halaman 1, *http://blog.unsri.ac.id/download/29298.pdf*, 27 Februari 2016.

Dadan Rosnawan, APLIKASI ALGORITMA RSA UNTUK KEAMANAN DATA PADA SISTEM INFORMASI BERBASIS WEB, Halaman 23,36 , http://lib.unnes.ac.id/7975/1/8562.pdf , 10 juni 2016