Rancang Bangun Jaringan VPN Berbasis IPSEC Menggunakan Mikrotik Routerboard Pada PT. Zahir Internasional

Fitri Sjafrina, Pipit Dewi Arnesia dan Arif Aqim
STMIK Jakarta STI&K
Jl. BRI No.17, Radio Dalam Kebayoran Baru Jakarta Selatan 12140
{fitris596, pdarnesia}@gmail.com

ABSTRAK

Virtual Private Network (VPN) adalah sebuah jaringan private dan aman dengan menggunakan jaringan publik seperti internet. Salah satu teknik pengamanan teknologi VPN adalah Internet Protocol Security (IPSec). IPSec merupakan sekumpulan standar protokol yang menyediakan keamanan dan kerahasiaan dalam pertukaran data di layer network. Rancang bangun VPN dengan teknologi IPSec dapat diterapkan pada Mikrotik Routerboard, VPN berteknologi IPSec memberikan kemudahan dalam komunikasi dan informasi keamanan data pada jaringan kantor pusat dan cabang. Jenis implementasi jaringan VPN menggunakan site-to-site di sistem operasi berbasis Windows. Uji koneksi Jaringan VPN dapat menggunakan perintah Packet Internet Gropher (Ping) dan sharing folder antara kantor pusat dan cabang. Metode rancang bangun VPN dengan Sistem Network Development Life Cycle (NDLC). VPN dirancang dari tahapan simulation prototype, demo VPN dan IPSec di Mikrotik Routerboard, uji coba koneksi dan manajemen VPN. Seluruh proses rancang bangun sistem yang telah dilakukan, kantor pusat dan cabang dapat terhubung langsung dalam jaringan lokal. Sistem Operasi Windows dapat memenuhi implementasi jaringan VPN berbasis IPSec. Data yang ditransmisikan melalui VPN akan mengalami kompresi, sehingga transmisi data dapat lebih cepat dan aman. Melalui IPSec keamanan jaringan komputer lebih terjamin karena menggunakan sistem autentifikasi. Jaringan VPN akan lebih baik lagi jika VPN server menggunakan Mikrotik RouterOS versi terbaru, penambahan bandwith pada komputer cabang dan monitoring atas akses data keluar masuk pada kantor pusat.

Kata Kunci: *VPN, IPSec, Jaringan, Routerboard, Mikrotik*

PENDAHULUAN

PT Zahir Internasional adalah perusahaan pembuat dan pengembang peranti lunak akuntansi dengan nama Zahir Accounting sejak tahun 1996 yang diasaskan oleh putra bangsa Indonesia. Zahir Accounting diberdayakan oleh tim terbaik dan inovator cerdas meliputi *programmer* andal yang membuat produk hebat, tim implementasi yang berpengalaman membangun sistem di berbagai bisnis, dan staf dukungan pelanggan yang memberi pelayanan terbaik.

PT Zahir Internasional juga turut berperan serta dalam bidang pendidikan dengan giat menyediakan *software* Zahir Accounting ke sekolah menengah (SMA/MA/SMK) dan perguruan tinggi sebagai bentuk tanggung jawab sosial perusahaan (*Corporate Social Responsibility*/CSR). Sampai dengan saat ini Zahir Accounting telah digunakan di lebih dari 30 perguruan tinggi ternama di Indonesia.

Zahir telah memperoleh beberapa anugerah di tingkat nasional sebagai bukti nyata kesungguhan mengembangkan mutu produk dan layanan purnajualnya, di antaranya: Penghargaan APICTA Indonesia oleh Menkominfo tahun 2002-2004, Penghargaan Presiden RI tahun 2003, Penghargaan Enterprise 50 tahun 2006, Juara Pertama Teknopreneur Award tahun 2008, dan Best Choice Award tahun 2013. Selain itu, PT Zahir Internasional juga telah memperoleh sertifikat ISO 9001:2008 pada tahun 2010.

Zahir merupakan *software* manajemen bisnis dan keuangan berbahasa Indonesia dan Inggris, fleksibel, berfasilitas lengkap, dan berdaya guna tinggi yang dirancang agar tepat dengan kebutuhan perusahaan kecil, menengah, dan besar di Indonesia bahkan manca negara.

Saat ini teknologi jaringan komputer di perusahaan tersebut, masih menggunakan jaringan LAN dalam pelaksanaan kegiatan operasional kerja setiap hari dan Mikrotik Routerboard untuk mengatur penggunaan *bandwith* internet.

Akan tetapi, seiring dengan penggunaan data komunikasi dan informasi yang sangat tinggi, menimbulkan beberapa masalah dalam keamanan jaringan komputer tersebut. Untuk mengatasi masalah keamanan dalam berbagi komunikasi dan informasi, maka diperlukan teknologi *Virtual Private Network (VPN)*. VPN merupakan suatu jaringan LAN yang terhubung dengan internet. Salah satu teknik pengamanan teknologi VPN adalah dengan *Internet Protocol Security (IPSec)*. IPSec dibangun berdasarkan teknologi *Internet Protocol (IP)* yang bekerja pada lapisan jaringan dan menyediakan layanan kriptografi untuk keamanan dalam transmisi data. IPSec juga mendukung layanan autentifikasi, integritasi, kontrol akses, dan kerahasiaan dengan cara *tunnel* pada jaringan dan memproteksi serangan dengan menyembunyikan alamat IP. Rancang bangun jaringan VPN dengan teknologi IPSec dapat diterapkan pada Mikrotik Routerboard. Mikrotik Routerboard adalah sebuah sistem operasi *router* yang dapat menjalankan dan mengatur aktifitas jaringan secara menyeluruh, mulai dari manajemen *bandwith*, *routing*, *firewall* dan lain sebagainya.

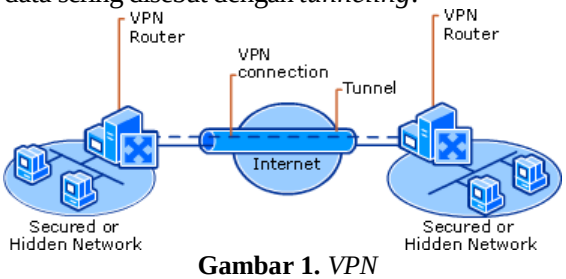
Virtual Private Network(VPN)

Virtual Private Network (VPN) merupakan sebuah jaringan *private* yang menghubungkan satu *node* jaringan ke *node* jaringan lainnya dengan menggunakan jaringan internet. Data yang dilewatkan akan di *encapsulation* (dibungkus) dan dienkripsi supaya data tersebut terjamin kerahasiaannya.

Virtual Private Network (VPN) adalah fasilitas yang memungkinkan koneksi jarak jauh (*remote access*) menggunakan jaringan publik untuk akses *Local Area Network* (LAN) pada suatu perusahaan.

VPN 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*. Data dienkapsulasi dengan *header* yang berisi informasi *routing* untuk mendapatkan koneksi *point-to-point* sehingga dapat melewati jaringan publik dan dapat mencapai tujuan akhir.

Untuk mendapatkan koneksi bersifat privasi, data yang dikirim harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses deskripsi. Proses enkapsulasi data sering disebut dengan *tunneling*.



Gambar 1. *VPN*

IP Security(IPSec)

IP *Security* (IPSec) adalah sekumpulan standar dan protokol yang bertujuan untuk menyediakan keamanan dan kerahasiaan dalam pertukaran data di *layer network*.

IPSec didefinisikan oleh sebuah badan internasional bernama IETF (*Internet Engineering Task Force*), yang terdiri dari pada ilmuwan, praktisi, operator, dan vendor jaringan yang mempunyai misi untuk memajukan internet melalui penelitian dan pengembangan yang dilakukannya.

Dua teknik utama yang digunakan pada IPSec adalah Otentikasi dan Enkripsi. Otentikasi bertujuan untuk mengecek keaslian dari sumber atau pengirim paket data. Apakah benar sebuah paket dikirimkan dari sumber atau alamat IP seperti yang tertera di *header* paket atau jangan-jangan paket dikirim dari sumber yang dipalsukan *spoofing*).

Teknik yang digunakan pada otentikasi juga berkhasiat untuk mengecek integritas dari paket data. Integritas data berarti paket yang diterima harus sama dengan paket yang dikirim, jangan sampai berbeda. Jika berbeda, maka ada kemungkinan paket tersebut telah diubah oleh seseorang atau sesuatu di tengah perjalanan sehingga paket tersebut tidak layak lagi untuk diterima.

Teknik kedua pada IPSec adalah enkripsi, tujuannya untuk menjaga kerahasiaan (*confidentiality*) dari paket data yang dikirim.

Kerahasiaan disini artinya paket tersebut hanya boleh dibaca oleh penerima yang dituju. Cara menjaga kerahasiaan data adalah

dengan melakukan enkripsi pada paket tersebut sebelum dikirimkan.

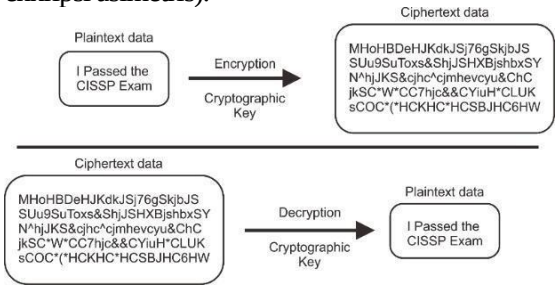
Jika paket yang sudah dienkripsi jatuhke tangan seseorang yang tidak berhak untuk menerima paket tersebut, maka paket tersebut tidak akan berguna bagi orang tersebut karena paket terenkripsi tidak akan bias dibaca tanpa *key* enkripsi yang tepat. Paket terenkripsi hanya bisa dibuka dan dibaca oleh orang yang mempunyai *key* enkripsi untuk membukanya.

Enkripsi bekerja dengan cara mengubah data berbentuk teks biasa (*clear text atau plain text*) menjadi kode-kode acak yang tidak bisa dibaca, yang disebut "*cipher text*".

Proses perubahan ini menggunakan algoritma enkripsi dan kunci enkripsi (*encryption key*). Kunci enkripsi disebut juga kunci kriptografi (*cryptographic key*).

Terlihat pada gambar 2 bahwa teks yang berbunyi "*I Passed…*" setelah mengalami proses enkripsi akan menjadi rangkaian teks yang tidak bisa dibaca dan dimengerti, bahkan oleh seorang super jenius sekalipun.

Di sisi penerima, proses sebaliknya dilakukan yaitu proses dekripsi (*decryption*) dimana *cipher text* yang tidak bisa dibaca diubah menjadi teks biasa kembali, dengan menggunakan algoritma dekripsi dan sebuah *key* kriptografi/enkripsi, dimana *key* untuk dekripsi tersebut bias sama dengan *key* yang digunakan untuk enkripsi (disebut enkripsi simetris) atau berbeda dengan *key* yang digunakan untuk enkripsi (disebut metode enkripsi asimetris).



Gambar 2. *Enkripsi dan Dekripsi*

Mikrotik

Mikrotik adalah nama perusahaan pemegang lisensi mikrotik yang berlokasi di Riga, ibukota Latvia, sebuah negara pecahan Uni Soviet yang bersebelahan dengan Rusia. Mikrotik merupakan produsen *software* dan *hardware router* mikrotik. Dengan mikrotik maka teknologi internet menjadi lebih cepat, handal dan terjangkau untuk kalangan pengguna yang lebih luas.

Mikrotik RouterOS adalah sebuah s*oftware* yang berfungsi mengubah PC (komputer) menjadi sebuah *router*. Mikrotik RouterOS layaknya IOS *cisco* yang di*install* di dalam *Router Cisco*, hanya saja IOS *cisco* tidak bisa di*install* di dalam komputer kecuali menggunakan emulator seperti GNS3 dan dinamis. Pada dasarnya RouterOS merupakan sistem operasi Mikrotik *RouterBoard* yang berbasis kernel Linux v2.6.

Selain *install* di dalam PC, Mikrotik RouterOS juga bisa di*install* pada sebuah *hardware* khusus yang bernama *RouterBoard*. Ketika kita membeli sebuah Mikrotik *RouterBoard* biasanya sudah ter*install* RouterOS di dalamnya.

METODE PENELITIAN

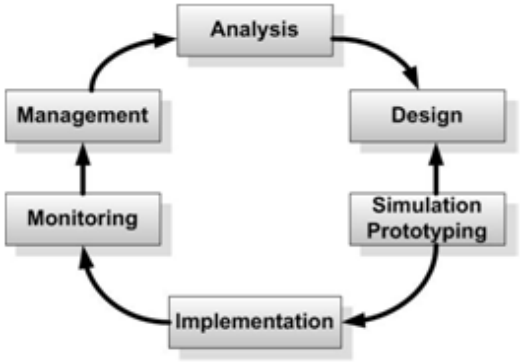
Penelitian ini menggunakan dua (2) metode, yaitu (a). Pengumpulan data dan (b). Pengembangan Sistem.

a. Metode Pengumpulan Data

Penelitian kualitatif berakar pada latar alamiah sebagai keutuhan, dan mengadakan analisis data secara induktif yang mengarahkan sasaran penelitiannya pada usaha menemukan teori dari dasar yang bersifat deskriptif. Proses dalam penelitian kualitatif lebih dipentingkan daripada hasil, dan hasil penelitiannya disepakati oleh kedua belah pihak yaitu peneliti dan subjek penelitian.

b. Metode Pengembangan Sistem

Metode yang digunakan dalam melakukan rancang bangun dan pengembangan sistem yaitu menggunakan *Network Development Life Cycle*(NDLC). Metode ini memiliki enam tahapan, yaitu tahap *analysis, design, simulation prototyping, implementation, monitoring,* dan *management*, seperti pada gambar 3.



Gambar 3. *Network Development Life Cycle*

HASIL &PEMBAHASAN

Analisa

Model pengembangan sistem NDLC dimulai pada fase analisis dimana pada tahap ini membahas proses analisis pembangunan VPN sistem dan perancangan VPN sistem. Sebelum dilakukan pengembangan dan perancangan sistem, terlebih dahulu dilaksanakan analisis kebutuhan-kebutuhan pokok Jaringan VPN yang akan dibangun.

- Sistem Yang Sedang Berjalan

Sistem yang sedang berjalan saat ini, data antar kantor pusat dan cabang tidak dapat di*share* secara langsung. Jika akan mengirim dan *sharing* data menggunakan elektronik mail (*e-mail*).

- Kebutuhan Perangkat Sistem

Mencakup kebutuhan dari perangkat lunak, perangkat keras, dan kebutuhan konektifitas dari jaringanVPN yang akan dibangun.VPN yang digunakan untuk menghubungkan kantor cabang dengan kantor pusat, menggunakan *router* hanya di kantor pusat. Rancang bangun ini termasuk jenis *Remote Access* VPN. Berikut kebutuhan yang dimaksud.

1. Perangkat Keras

Spesifikasi perangkat keras yang digunakan sebagai *router* VPN (Mikrotik Routerboard tipe RB750) memiliki spesifikasi seperti pada Tabel 1.

Tabel 1. *Spesifikasi Perangkat Keras*

No.	Produk	Seri
1	*Product Code*	RB750
2	*Architecture*	MIPS-BE
3	CPU	AR7241 400MHz
4	*Current Monitor*	No
5	*Main Storage*/NAND	64Mb
6	RAM	32Mb
7	SFP *Ports*	0
8	LAN *Ports*	5
9	Gigabit	No
10	*Switch Chip*	1
11	MiniPCI	0
12	SIM *Card Slots*	No
13	USB	No
14	*Memory Cards*	No
15	*Power Jack*	10-28V
16	802.3af *Support*	No
17	POE *Input*	10-28V
18	POE *Output*	No
19	*Serial Port*	No
20	*Voltage Monitor*	No
21	*Temperature Sensor*	No
22	*Dimentions*	113x89x28mm
23	*Operating System*	RouterOS
24	RouterOS *License*	Level 5

2. Perangkat Lunak

Spesifikasi perangkat lunak yang digunakan sebagai *server* VPN adalah Mikrotik RouterOS level5;

a. Spesifikasi perangkat lunak yang digunakan pada komputer pengguna (*client*) adalah *Windows 7 Home Basic*;
b. *Winbox Loader* v2.2.16 sebagai aplikasi mode GUI untuk me*remote* dan mengkonfigurasi Mikrotik RouterOS;
c. *Ms. Visio* 2010 untuk desain topologi sistem VPN;
d. *Oracle VM Virtual Box* v5.1.2 sebagai mesin *virtual* untuk komputer. Piranti lunak ini dapat meng*install* sistem operasi tanpa harus mengganggu sistem operasi yang sudah ada.

3. Kebutuhan Konektifitas

Kebutuhan konektifitas yang digunakan adalah kebutuhan *bandwith*

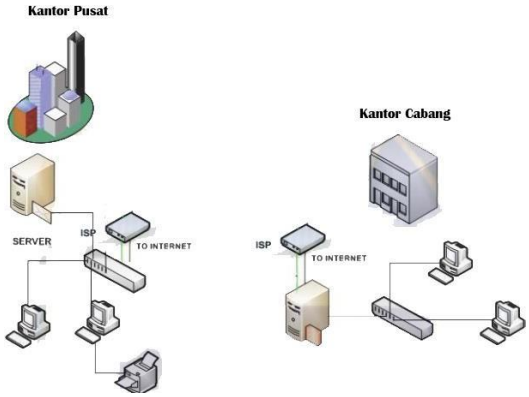
internet dengan *high speed* internet *residential package* dari *Internet Service Provider* dengan kecepatan *up to* 100 Mbps.

Rancang Bangun

Rancang bangun terdiri dari topologi fisik dan topologi logis pada jaringan VPN, sebagai berikut :

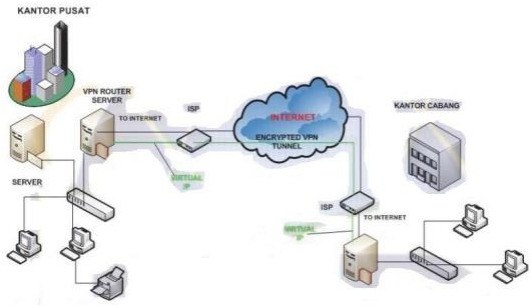
1. Topologi Fisik

Topologi jaringan yang bersifat fisik, koneksi pengkabelan antar *interface* pada masing- masing perangkat keras dapat saling terhubung. Pada gambar 4, topologi yang menghubungkan kantor pusat dan kantor cabang menggunakan topologi *star*. Topologi *star* memiliki ciri utama yaitu; adanya konsentrator yang berubah *hub/switch* maupun *router*.



Gambar 4. *Topologi Jaringan Lama*

Dalam penelitian ini *switch*, terlihat pada Gambar 5 digunakan sebagai konsentrator yang berfungsi menghubungkan beberapa *client* dalam jaringan.



Gambar 5. *Topologi Jaringan Baru*

2. Topologi Logis

Topologi logis ini merupakan rancang bangun terhadap pengalamatan IP pada masing-masing perangkat PC, *router*, dan *switch* saling terkoneksi.

Koneksi VPN antara kantor pusat dengan kantor cabang melalui jaringan internet. *Virtual* IP pada kantor pusat adalah 192.168.1.1 dengan *subnet mask* 255.255.255.0. *Virtual* IP pada kantor cabang adalah 192.168.0.1 dengan *subnet mask* 255.255.2555.0.

Kantor pusat terhubung dengan internet melalui ISP dengan alamat IP 122.144.4.190 dengan *subnet mask* 255.255.255.0. *Local Area Network* pada kantor pusat memiliki *network* ID192.18.1.1/24.

Kantor cabang terhubung dengan internet melalui ISP dengan alamat IP 202.158.78.182 dengan *subnet mask* 255.255.255.0. *Local Area Network* pada kantor cabang memiliki *network* ID 192.168.0.1/24.

Simulasi Prototipe

Merupakan pembuatan simulasi dengan aplikasi simulator. Tahap simulasi prototipe menggunakan *virtual* Mikrotik R*outerboard* dalam *software virtual box*, 2 buah laptop dan 2 buah modem USB. Simulasi Jaringan VPN ini bertujuan untuk mensimulasikan koneksi jaringan sebelum diimplementasikan secara nyata pada perangkat keras yang sebenarnya.

Implementasi

Merupakan proses dimana hasil dari tahap-tahap sebelumnya diimplementasikan. Proses implementasi yang akan dilakukan adalah instalasi dan konfigurasi dengan menggunakan *routerboard*, maka mikrotik sudah terinstalasi di dalam *routerboard*.

1. Konfigurasi Mikrotik

IP Address, DHCP Client, DNS Server, Masquarade Firewall, Hotspot dan Security Firewall.

2. Konfigurasi VPN

a. TambahkanIP Add di AddressList
b. Set IPPool.
c. SetDHCP, DHCP Network.
d. Set L2TP Server, PPP Profile .
e. Set PPP Secret.
f. Set IPSec Peer, IPSec Proposal.

3. Konfigurasi Client

a. Klik *Start >> Control Panel >> Network and Internet >> Network and Sharing Center >> Set up a new connection or network.*

b. Pilih *Connect to a workplace*, klik *next*.
c. Klik *Use my Internet connection (VPN)* kemudian isi internet address tujuannya, klik *next* untuk mengisi *user name* dan *password* dan tunggu hingga muncul "*The connection already to use"*.
d. VPN *client* sudah siap digunakan dari *taskbar connection*.

Monitoring

Merupakan kegiatan memonitor aktifitas pengoperasian dan pengamatan uji coba koneksi jaringan dengan langkah selanjutnya adalah koneksi akses *remote* VPN yang sudah dibangun untuk menggunakan sambungan sederhana maka langkah-langkahnya sebagai berikut:

a. *Double* klik Zahir pada *taskbar connection* hingga muncul *Dialog Connect* VPN; seperti terlihat pada gambar 6.

Gambar 6. *Dialog Network Connection*

b. Masukkan *user name* dan *password* yang sudah terdaftar di VPN *server* kemudian klik *Connect*;
c. Setelah proses *Authentication* sukses, maka VPN sudah terkoneksi dengan jaringan.

Manajemen

Aktifitas manajemen meliputi aktifitas perawatan dan pemeliharaan dari keseluruhan sistem yang sudah dibangun. Pada tahap manajemen terdapat dua proses yaitu, manajemen *user* dan *backup* konfigurasi sistem.

1. Manajemen *User*

Grup user pada mikrotik diperlukan untuk memberikan izin hak akses *user* terhadap sistem.

2. Backup Konfigurasi

Backup konfigurasi dilakukan karena untuk mengantisipasi kegagalan sistem pada waktu mendatang. Ketika sistem terdapat *erro r*maka dapat me*load* kembali file *backup* tersebut sehingga *router* mikrotik tidak perlu untuk dikonfigurasi ulang.

PENUTUP

Kantor pusat dan cabang dapat terhubung ke jaringan VPN dengan konektifitas *bandwith* internet yang *high speed* internet *residential package* dari *Internet Service Provider memiliki* kecepatan *up to* 100 Mbps. VPN berbasis IPSec dapat diimplementasikan pada Mikrotik Routerboard dengan konfigurasi Mikrotik IP *Address*, DHCP *Client*, DNS *Server*, *Masquarade Firewall*, *Hotspot* dan *Security Firewall*, dimana hasil dari tahapan sebelumnya melalui proses implementasi yang dilakukan adalah instalasi dan konfigurasi menggunakan *routerboard* dengan mikrotik yang sudah diinstalasi di dalam *routerboard*. Selanjutnya memonitor aktifitas pengoperasian dan pengamatan uji coba koneksi jaringan dengan cara koneksi akses *remote* VPN yang sudah dibangun menggunakan sambungan sederhana yang terdaftar di VPN *server*, kemudian klik *Connect*; setelah proses *Authentication* sukses, maka VPN sudah terkoneksi dengan jaringan.

Agar konektifitas berlanjut, maka perlu manajemen untuk mengatur aktifitas perawatan dan pemeliharaan dari keseluruhan sistem yang sudah dibangun terdapat dua proses yaitu, manajemen *user* dan *backup* konfigurasi sistem guna mengantisipasi kegagalan sistem pada waktu mendatang. Jika sistem terdapat *error* maka dapat me*load* kembali file *backup, router* mikrotik tidak perlu dikonfigurasi ulang, Hal tersebut memberi kemudahan bagi setiap *client* menggunakan jaringan VPN berbasis sistem operasi Windows tanpa membutuhkan perangkat lunak lain, data yang ditransmisikan melalui jaringan

VPN berteknologi IPSec memberikan keamanan lebih terjamin karena menggunakan autentifikasi pada *username* dan *password* yang berbeda pada setiap *user*.

DAFTAR PUSTAKA

[1] Prasetya, Aditya. (2011).Rancang bangundan Penerapan Teknologi VPN(Virtual Private Network) Untuk Komunikasi Data (Studi Kasus: Gardanet Corporation). Skripsi. Sarjana Universitas Islam Negeri*SyarifHidayatullah*.

[2] Micro, Andi. (2012). Dasar-dasar Jaringan Komputer. Retrieved from http://www.andimicro.com/2011/02/ebook-dasar-dasar-jaringan-komputer.html/.

[3] Sofana, Iwan. (2012). Cisco CCNP & Jaringan Komputer. *Bandung: Informatika*.

[4] Utomo, PS. (2010). Analisis Kinerja VPN Berbasis Mikrotik Pada Proses Kompresi-Dekompresi dan Enkripsi-DeskripsiDibandingkan VPN Berbasis OpenSource. *Skripsi. Sarjana UniversitasIslam NegeriSyarif Hidayatullah*.

[5] Hidayatulloh, Syarif. (2014). Analisis dan Optimalisasi KeamananJaringanMenggunakan Protokol IPSec, (*Online*).

[6] Sumbang, Nada. (2011). Tutorial Mikrotik E-book+Video. Retrieved fromhttp://www.nadasumbang.com/category/mikrotik/.

[7] Moleong, Lexy J. (2012. Metodologi Penelitian Kualitatif. *Bandung:Rosda*