

KAJIAN *VIRTUAL PRIVATE NETWORK* (VPN) SEBAGAI SISTEM PENGAMANAN DATA PADA JARINGAN KOMPUTER (Studi Kasus Jaringan Komputer Unikom)

IRAWAN AFRIANTO , EKO BUDI SETIAWAN
Program Studi Teknik Informatika – FTIK
Universitas Komputer Indonesia

Jaringan komputer dapat dikatakan sebagai sebuah sistem yang terdiri dari berbagai komputer beserta *resource*-nya yang didesain agar dapat menggunakan sumber daya yang ada, sehingga dapat mengakses informasi yang diperlukan. Informasi tersebut dapat diakses melalui komputer yang lain dengan konsep *computer networking*, baik itu *Local Area Network*, *Metropolitan Area Network*, *Wide Area Network* ataupun juga internet. Untuk mengamankan suatu koneksi pada jaringan dapat menggunakan jaringan yang bersifat virtual yang dikenal dengan istilah *Virtual Private Network* (VPN).

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada didalam kantor atau network itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik.

UNIKOM sebagai salah satu perguruan tinggi yang dalam melakukan kegiatan operasionalnya terdiri dari beberapa *stakeholder* yang saling terhubung dalam jaringan komputer, perlu menerapkan konsep VPN untuk mengamankan informasi yang dimiliki pada suatu jaringan, ataupun untuk memudahkan dalam mengakses jaringan lokal yang ada di UNIKOM walaupun dalam mengaksesnya menggunakan jaringan yang bersifat *public* (internet).

Hasil dari penelitian ini adalah berupa suatu rekomendasi dasar yang dapat digunakan oleh UNIKOM untuk menerapkan konsep *Virtual Private Network* (VPN) dalam pengembangan jaringan komputer yang dimiliki sehingga dalam pengaksesan informasi dapat berlangsung lebih aman dan efektif.

Kata kunci : Jaringan Komputer, *Virtual Private Network*, Internet, Unikom

PENDAHULUAN

Suatu organisasi atau institusi dalam melangsungkan kegiatannya tidak akan lepas dari pertukaran informasi antar para *stakeholder* yang satu dengan yang lain. Setiap informasi yang dihasilkan oleh salah satu *stakeholder* akan diperlukan oleh *stakeholder* lain. Untuk itu, kebutuhan informasi harus dapat diakses melalui jaringan komputer yang di desain untuk dapat mendapatkan informasi yang

diperlukan dengan cepat, mudah, aman dan akurat.

Dalam sebuah jaringan komputer, keamanan sewaktu pengiriman dan penerimaan data sangat penting untuk menjamin bahwa data yang dikirim sampai pada yang pihak yang dituju, dan tidak jatuh pada pihak yang tidak berkepentingan, terutama apabila data yang dikirimkan tersebut bersifat rahasia. Untuk itu perlu dilakukan pengamanan data pada jaringan

dengan menggunakan metode-metode tertentu. Salah satu cara untuk mengamankan data pada suatu jaringan adalah dengan mengimplementasikan *Virtual Private Network* (VPN) yang dapat membuat sebuah jaringan bersifat *private* dan aman dengan menggunakan jaringan publik atau internet.

Perguruan Tinggi sebagai salah satu institusi pendidikan yang didalamnya terdiri dari beberapa bagian yang berbeda, serta dalam masing-masing bagian juga menggunakan sistem yang berbeda, harus saling terhubung satu sama lain dengan fasilitas jaringan komputer yang dimiliki oleh suatu Perguruan Tinggi. UNIKOM merupakan salah satu perguruan tinggi yang berbasis teknologi informasi, tentunya perlu mengamankan lalu lintas data yang terdapat pada jaringan komputer yang dimiliki, karena data tersebut juga dapat bersifat rahasia yang tidak bisa diakses begitu saja oleh orang yang tidak berkepentingan.

Berdasarkan pertimbangan tersebut, maka penelitian ini diperlukan untuk mengkaji mengenai keamanan data pada jaringan komputer UNIKOM dengan menggunakan konsep *Virtual Private Network* (VPN) sehingga dalam pengaksesan informasi dapat berlangsung lebih aman dan efektif.

TINJAUAN PUSTAKA

Definisi Jaringan Komputer

Jaringan komputer dapat dikatakan sebagai sebuah sistem yang terdiri dari berbagai komputer beserta *resource*-nya yang didesain agar dapat menggunakan sumber daya yang ada, sehingga dapat mengakses informasi yang diperlukan. Tujuan dibangunnya suatu jaringan komputer adalah untuk mengirim data atau informasi dari pengirim kepada penerima secara cepat dan akurat. Jaringan komputer berdasarkan skala dan jangkauan

jaringannya dapat diklasifikasikan kedalam *Local Area Network* (LAN), *Metropolitan Area Network* (MAN), *Wide Area Network* (WAN).

Pada dasarnya setiap jaringan komputer ada yang berfungsi sebagai *client* dan juga server. Ada juga jaringan komputer yang memiliki komputer yang dikhususkan menjadi server sedangkan yang lainnya sebagai *client*. Sehingga berdasarkan fungsinya, maka jaringan komputer dapat dibagi menjadi dua jenis, yaitu *Client Server* dan *Peer to Peer*.

Internet

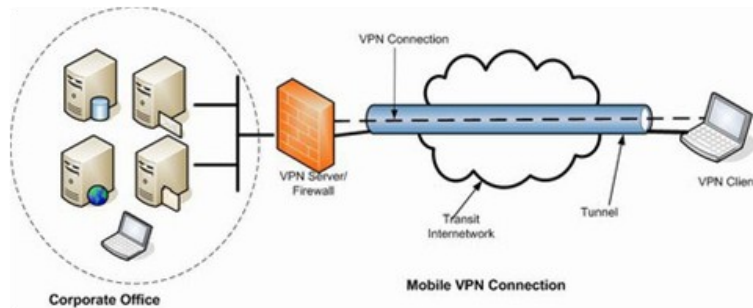
Internet merupakan jaringan komputer yang terhubung menggunakan standar sistem global *Transmission Control Protocol/Internet Protocol* (TCP/IP) sebagai protokol pertukaran paket data untuk melayani pengguna di seluruh dunia. Dengan internet, maka lalu lintas data dari seluruh belahan dunia dapat saling berbagi informasi yang diperlukan. Internet Protocol (IP) merupakan inti dari TCP/IP dan merupakan protokol terpenting dalam Internet Layer, dimana IP menyediakan pelayanan pengiriman paket pada jaringan TCP/IP yang dibangun. Teknologi internet ini menggunakan fasilitas layanan yang biasa kita sebut dengan World Wide Web (www).

Virtual Private Network (VPN)

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 cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam kantor atau LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik.

Teknologi VPN menyediakan beberapa fungsi utama untuk penggunaannya. Fungsi-fungsi utama tersebut antara lain sebagai berikut.

1. *Confidentially* (Kerahasiaan)



Gambar 1. Remote Access VPN

2. *Data Integrity* (Keutuhan data)
3. *Origin Authentication* (Autentikasi sumber)
4. *Non-repudiation*
5. Kendali akses

Teknologi Tunneling

Teknologi *tunneling* merupakan teknologi yang bertugas untuk menangani 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. Hal ini sama dengan seperti penggunaan jalur *busway* yang pada dasarnya menggunakan jalan raya, tetapi dia membuat jalur sendiri untuk dapat dilalui bus khusus.

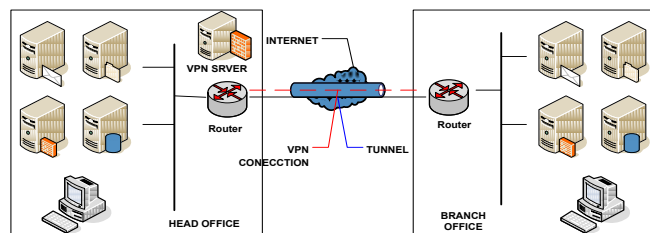
Koneksi *point-to-point* ini sesungguhnya tidak benar-benar ada, namun data yang dihantarkannya terlihat seperti benar-benar melewati koneksi pribadi yang bersifat *point-to-point*.

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. Namun, di dalam teknologi VPN, *tunnel* tidak dibiarkan begitu saja tanpa diberikan sistem keamanan tambahan. *Tunnel* dilengkapi dengan sebuah sistem enkripsi untuk menjaga data-data yang melewati *tunnel* tersebut. Proses enkripsi inilah yang menjadikan teknologi VPN menjadi mana dan bersifat pribadi.

Jenis Implementasi VPN

Pada umumnya implementasi VPN terdiri dari 2 macam. Pertama adalah *remote access* VPN, dan yang kedua adalah



Gambar 2. Site-to-Site VPN

site-to-site VPN. Remote access yang biasa juga disebut *virtual private dial-up network* (VPDN).

Konsep SSL VPN

Konsep dan Teknologi SSL (*Secure Socket Layer*) VPN dapat menjawab kebutuhan untuk mengakses sumberdaya perusahaan melalui penggunaan jaringan internet yang sudah tersedia dan bercakupan luas. Dibandingkan jaringan *leased lines* atau *frame relay*, SSL VPN menggunakan infrastruktur publik yang sudah ada di internet untuk melakukan pertukaran data antara kantor pusat sebuah perusahaan dan kantor cabangnya.

Karena dilewatkan pada jaringan internet publik, permasalahan konsep SSL VPN muncul sama seperti jaringan IP pada umumnya. Salah satu masalah jaringan internet (*IP public*) adalah tidak mempunyai dukungan yang baik terhadap keamanan. SSL VPN muncul untuk mengatasi persoalan keamanan tersebut. Dasar dari konsep SSL VPN ini adalah penggunaan infrastruktur IP untuk hubungan suatu perusahaan dengan kantor cabangnya dengan cara pengalamanan secara *private* dengan melakukan pengamanan terhadap transmisi paket data.

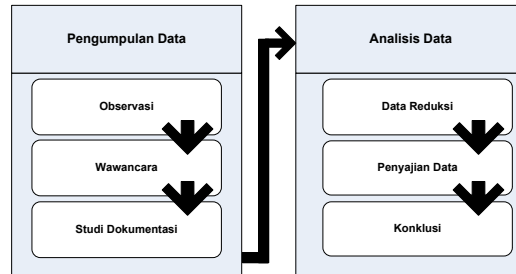
TUJUAN DAN MANFAAT PENELITIAN

Tujuan dari penelitian ini adalah untuk mengkaji dan menganalisis jaringan komputer yang ada di UNIKOM dengan menggunakan konsep *Virtual Private Network* (VPN) sehingga akan menghasilkan suatu rekomendasi keamanan dari jaringan komputer UNIKOM dengan menggunakan VPN.

Manfaat penelitian ini adalah memberikan rekomendasi bagi UNIKOM untuk mengembangkan dan meningkatkan keamanan jaringan komputer yang telah dimiliki dengan mengimplementasikan konsep *Virtual Private Network* (VPN) sehingga dalam pengaksesan informasi antar jaringan komputer dapat berlangsung lebih aman dan efektif.

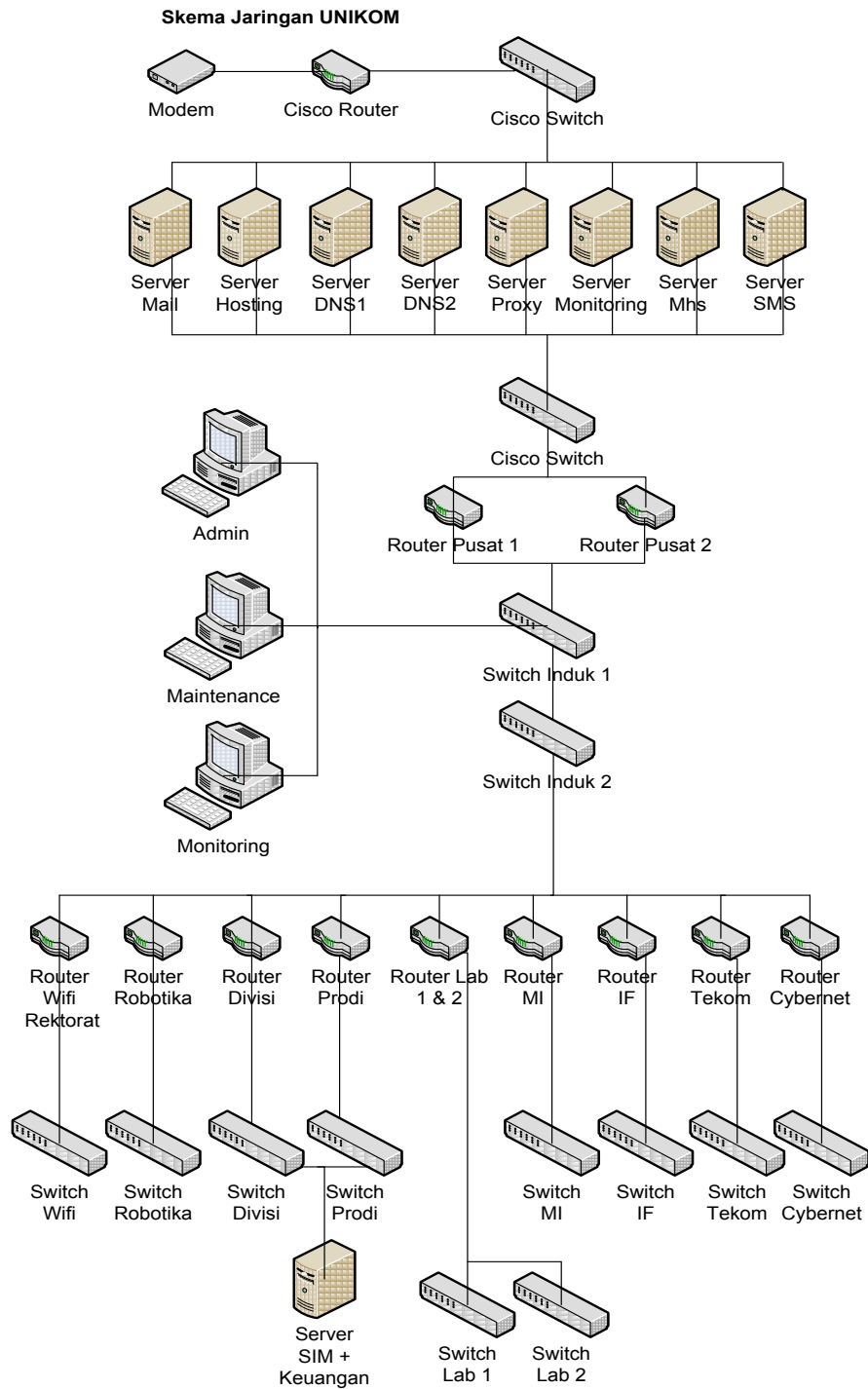
METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini terdapat pada Gambar 1.



Gambar 1. Metode Penelitian

1. Pengumpulan data
Pengumpulan data pada penelitian ini dilakukan dengan melakukan observasi yaitu peninjauan langsung ketempat yang menjadi studi kasus, melakukan wawancara dengan pihak-pihak terkait serta studi dokumenasi yang diperoleh selama kegiatan wawancara dan observasi berlangsung.
2. Analisis data
Setelah data-data dikumpulkan menggunakan teknik-teknik pengumplan data tersebut, maka berikutnya peneliti melakukan tahapan analisis data yang mencakup kegiatan data reduksi yaitu merangkum data-data yang sudah dikumpulkan, memilih hal-hal pokok dan memfokuskan pada hal-hal penting hingga meneukan pola. Tahap penyajian data digunakan untuk menyajikan data dalam bentuk uraian bersifat naratif, sementara konklusi adalah tahapan peneliti menarik kesimpulan terhadap hasil penelitian, dalam hal ini peneliti membuat rancangan dan rekomendasi infrastruktur VPN untuk Unikom.



Gambar 2. Skema Jaringan Unikom

HASIL DAN PEMBAHASAN

Kondisi Eksisting Jaringan Komputer Unikom

Skema jaringan yang dimiliki oleh UNIKOM untuk melangsungkan kegiatan dalam hal pertukaran informasi antar civitas akademika dapat dilihat pada Gambar 2.

Sistem Informasi di Unikom

Untuk mendukung seluruh kegiatan yang berlangsung di UNIKOM, telah dikembangkan berbagai sistem informasi yang memudahkan civitas akademika UNIKOM dalam beraktifitas. Sistem informasi tersebut diantaranya adalah :

1. Sistem Informasi Akademik (SIKAD)
2. PMB Online Unikom <http://pmb.unikom.ac.id>
3. Perwalian Online <http://perwalian.unikom.ac.id>
4. Nilai Online <http://nilaionline.unikom.ac.id>
5. Sistem Informasi Keuangan
6. Autodebet Online <http://autodebet.unikom.ac.id>
7. Alumni Unikom <http://alumni.unikom.ac.id>
8. Kuliah Online <http://kuliahonline.unikom.ac.id>
9. Perpustakaan online Unikom <http://elib.unikom.ac.id/>
10. Sistem Management Aset <http://aset.unikom.ac.id>
11. Jejaring Sosial <http://kampus.unikom.ac.id>
12. Blog Unikom <http://blog.unikom.ac.id>
13. Dosen dan Karyawan online
14. Beasiswa Unikom <http://beasiswa.unikom.ac.id>
15. Sistem Penjadwalan Kuliah

Rekomendasi VPN dan Aplikasi

Aplikasi yang ada di UNIKOM saat ini secara umum sudah bersifat *online*, sehingga dapat diakses dari mana saja melalui fasilitas internet. Namun

keterbukaan dan kebebasan dalam mengakses sistem informasi tersebut, akan menimbulkan ketidakamanan terhadap data yang diakses. Dilihat dari data yang diakses oleh aplikasi yang digunakan, maka dapat dianalisis bahwa beberapa aplikasi harus lebih ditingkatkan lagi dalam hal keamanannya, oleh karena itu dengan adanya VPN diharapkan transaksi aplikasi-aplikasi online Unikom dapat lebih terlindungi, karena akses yang lebih aman melalui VPN.

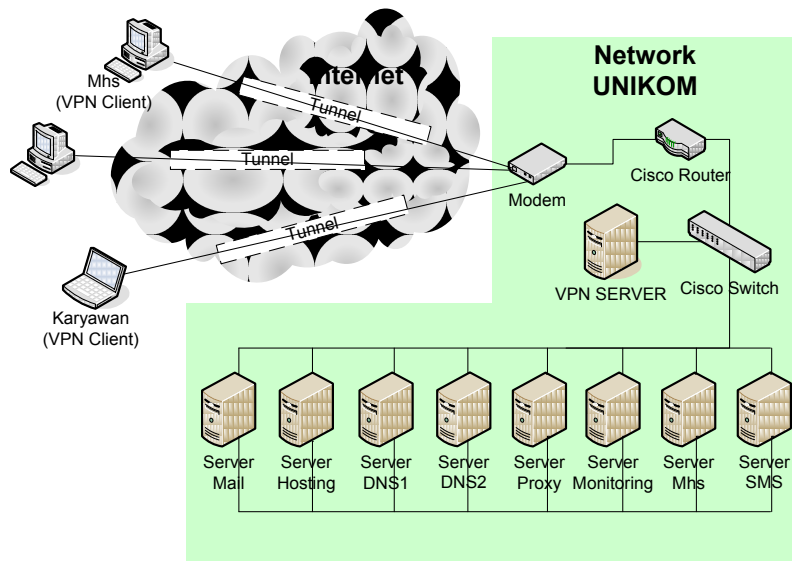
VPN secara umum bertujuan melindungi data dan informasi yang dilewatkan melalui internet melalui media tunneling yang dilengkapi dengan kriptografi atau penyandian data. Akses kedalam jaringanpun akan menjadi lebih cepat dikarenakan pengguna yang mengakses aplikasi-aplikasi dalam VPN seolah-olah berada dilingkungan LAN Unikom. VPN yang akan dikembangkan adalah VPN berjenis *Remote Access VPN* dimana akses dilakukan oleh para user yang sifatnya berpindah/tidak menetap. Keuntungan yang diperoleh dengan service VPN adalah :

1. Akses global ke jaringan Unikom melalui internet.
2. Kemudahan mengakses resources yang berada di dalam jaringan Unikom yang tidak dapat diakses dari luar Unikom secara langsung.
3. Keamanan dalam transfer data karena adanya enkripsi data.
4. Keamanan jaringan sebab hanya user yang telah melewati proses autentikasi dan otorisasi saja yang dapat menggunakan service VPN.

Sementara untuk kebutuhan perangkat yang diperlukan untuk pengembangan suatu VPN dapat dilihat pada Gambar 3.

Kebutuhan Perangkat Keras dan Perangkat Lunak VPN

Komputer VPN server pada *Remote Access Virtual Private Network* yaitu bertindak sebagai server VPN, server VPN bertugas membentuk *tunnel*, melakukan validitas *certificate*, dan sebagai gateway



Gambar 3. Arsitektur VPN Unikom

antar *vpn client*. Komputer yang bertindak sebagai *server VPN* mempunyai spesifikasi pada Tabel 1.

Tabel 1. Spesifikasi Perangkat Keras VPN

No	Komponen	Keterangan
1	Processor	Intel Core Solo 1.8 GHz
2	Memori	1.2 Gb
3	Harddisk	60 Gb
4	Operating System	Ubuntu Lucid Lynx

Sementara untuk perangkat lunak yang digunakan adalah OpenVPN hal ini dikarenakan Open VPN adalah perangkat lunak yang *free* dan handal untuk kepentingan VPN, Open VPN memiliki 2 Jenis aplikasi yang pertama adalah Open VPN Server - yaitu perangkat lunak yang dijalankan sebagai VPN server dan Open VPN Client yang digunakan pengguna VPN untuk mengakses jaringan Unikom.

Sementara untuk aplikasi online Unikom yang direkomendasikan berada dibawah layanan VPN unikom adalah

sebagai berikut :

1. Sistem Informasi Akademik (SIKAD)

Sistem Informasi Akademik (SIKAD) UNIKOM mencakup semua data dan informasi akademik yang diperlukan bagi keberlangsungan kegiatan perkuliahan di UNIKOM. Informasi tersebut sangat penting dan bersifat rahasia sehingga perlu untuk lebih dijaga dalam hal keamanan datanya. Saat ini SIKAD dapat diakses dari komputer yang sebelumnya sudah terinstall aplikasi tersebut dan belum bersifat *online*, sehingga tidak dapat diakses melalui internet dan hanya bersifat intranet. Hal tersebut mengakibatkan apabila ada beberapa stakeholder yang memerlukan akses kepada SIKAD, maka untuk mengaksesnya hanya dari komputer yang terkoneksi dengan jaringan yang ada di UNIKOM. Untuk lebih mengefektifkan dalam penggunaan SIKAD, maka direkomendasikan untuk mengonlinekan sistem informasi tersebut sehingga dapat diakses oleh para *stakeholder* melalui koneksi internet dengan keamanan yang digunakan menggunakan konsep VPN.

2. Sistem Informasi Keuangan (SIMKEU)

Informasi mengenai status keuangan dari civitas akademika diolah dan dikelola oleh Bagian Keuangan dengan menggunakan Sistem Informasi Keuangan (SIMKEU). SIMKEU bersifat private karena hanya bisa diakses oleh para *stakeholder* yang berkepentingan, tetapi dengan konsep terhubungnya semua komputer yang ada di UNIKOM dengan jaringan komputer yang dimiliki, maka informasi yang dihasilkan oleh SIMKEU rentan terhadap keamanan sehingga informasi tersebut perlu untuk diamankan dengan menggunakan konsep VPN.

3. Sistem Informasi Management Aset

Keberadaan Aset yang dimiliki oleh UNIKOM dikelola oleh bagian perlengkapan UNIKOM dengan menggunakan Sistem Informasi Management Aset. Informasi tersebut bersifat internal diakses oleh orang tertentu sehingga perlu untuk diamankan dengan menggunakan konsep VPN.

4. Sistem Informasi Dosen dan Karyawan (SIDOKAR)

Informasi mengenai personalia atau *human resource* dari Dosen dan Karyawan bersifat pribadi sehingga informasi tersebut tidak dapat diakses atau diketahui oleh pihak yang tidak berkepentingan. Untuk lebih mengamankan data pribadi dari dosen dan karyawan tersebut perlu digunakan konsep VPN.

5. Sistem Perwalian Online

Informasi mengenai rencana studi dan histori perkuliahan yang telah dilakukan oleh Mahasiswa dikelola dengan menggunakan Sistem Perwalian Online. Sangat penting sekali informasi yang ada didalamnya untuk diamankan dengan menggunakan konsep VPN karena sebelumnya Sistem Perwalian Online ini sudah bersifat online sehingga rentan dalam hal keamanan data.

KESIMPULAN DAN SARAN

Kesimpulan

1. Dengan menggunakan VPN diharapkan akses data dan informasi ke jaringan Unikom menjadi lebih aman, dikarenakan mekanisme tunneling VPN akan melakukan enkripsi data pada saat transaksi.
2. Dengan adanya VPN Jaringan Unikom akan lebih selektif dalam memberikan layanan yang dapat diakses pengguna publik maupun pengguna intern Unikom

Saran

Adapun saran-saran yang dapat disampaikan dalam penelitian ini adalah sebagai berikut :

1. Kebutuhan perangkat lunak dan perangkat keras relatif murah sehingga layanan VPN ini sebaiknya dapat implementasikan.
2. Melakukan kajian lebih mendalam mengenai service-service apa saja yang dapat di VPN kan namun tidak menghalangi akses data ke Unikom, terutama terkait dengan perangkat Webometrics Unikom.

DAFTAR PUSTAKA

- Irawan, Budhi, (2005). Jaringan Komputer, Yogyakarta : Graha Ilmu.
- Kosiur, Dave (1998). Building and Managing Virtual Private Networks, Wiley & Sons.
- Mains, John, (2001) . VPNs A Beginners Guide, McGraw Hill.
- http://www.cse.wustl.edu/~jain/cis788-99/ftp/h_7vpn.pdf, diakses 19 Agustus 2011
- <http://id.wikipedia.org/wiki/VPN>, diakses 19 Agustus 2011
- <http://thommykennedy.files.wordpress.com/2009/07/penggunaan-virtual-private-network-vpn.pdf> , diakses 20 Agustus 2011
- <http://budi.insan.co.id/courses/ec5010/projects/rusdy-report.doc>, diakses 20 Agustus 2011
- <http://indrasufian.wordpress.com/2007/09/19/pengertian-virtual-private-network-vpn/> , diakses 19 Agustus 2011
- <http://my.opera.com/kunkun87/blog/vpn-virtual-protocol-network>, diakses 20 Agustus 2011

