ISSN 0125-9008 (Print); ISSN 2301-8593 (Online)
DOI: https://doi.org/10.14203/j.baca.v41i2.531
SK Dirjen Risbang -Kemristekdikti No 21/E/KPT/2018 (Peringkat 2 SINTA)

IMPLEMENTASI *VIRTUAL PRIVATE NETWORK* (VPN) DI PERPUSTAKAAN UNIVERSITAS ISLAM MALANG

Lia Umaroh[1*], Machsun Rifauddin[2]
[1,2]Institut Agama Islam Negeri Tulungagung

[*]Korespondensi: liauma18@gmail.com

Diajukan: 25-05-2019; **Direview:** 02-07-2019; **Diterima:** 17-10-2020; **Direvisi:** 12-11-2020

ABSTRACT
This study aims to explain to use a VPN in the UNISMA Library. The research method used is descriptive-qualitative and data was obtained through interviews with five informants, observation, and documentation. Data analysis techniques by collecting data, data reduction, data presentation and drawing conclusions. While the validity of the data was obtained through triangulation. The results showed that the use of VPN in the UNISMA Library to speed up internet connection and data privacy. UNISMA library uses a proxy server router operating system for VPN networks. To be able to make Mikrotik a VPN server, configuration is required which includes IP pool configuration, IP router configuration, PPP configuration, DHCP server configuration, NAT by pass firewall configuration and IP security configuration. The library selection of VPN products considers the aspects of strong authentication, encryption that is strong enough, meets standards, integration with other field network services.

ABSTRAK
Penelitian ini bertujuan untuk menjelaskan penggunaan VPN di Perpustakaan UNISMA. Metode penelitian menggunakan kualitatif-deskriptif dan data diperoleh melalui wawancara dengan 5 informan, observasi, dan dokumentasi. Teknik analisis data dengan pengumpulan data, reduksi data, penyajian data dan penarikan kesimpulan. Sedangkan keabsahan data diperoleh melalui triangulasi. Hasil penelitian menunjukkan penggunaan VPN di Perpustakaan UNISMA untuk mempercepat koneksi internet dan privasi data. Perpustakaan UNISMA menggunakan server mikrotik router operating system untuk jaringan VPN. Untuk dapat menjadikan mikrotik sebagai server VPN, diperlukan konfigurasi yang meliputi konfigurasi *IP pool*, konfigurasi *IP router*, konfigurasi PPP, konfigurasi *DHCP server*, konfigurasi *firewall NAT by pass* dan konfigurasi *IP security*. Pemilihan produk VPN tersebut, perpustakaan mempertimbangkan aspek otentikasi yang kuat, enkripsi yang cukup kuat, memenuhi standar, integrasi dengan servis network bidang lain.

Keywords: Academic library; Information technology; Internet; System network; VPN; Islamic university

1. PENDAHULUAN

Perkembangan dunia internet yang semakin pesat menjadikan munculnya standar baru, yang memiliki beragam konten pada sebuah *web*. Hal tersebut mempengaruhi pada sebuah organisasi, lembaga bisnis maupun lembaga penyalur informasi seperti perpustakaan. Salah satu manfaat teknologi informasi adalah sebagai sarana proses transfer data maupun informasi. Salah satu media transfer data adalah jaringan internet (Satwika, 2019). Semua proses yang terjadi saat ini sudah menggunakan sistem teknologi informasi yang menggunakan sistem *database*. Perkembangan informasi saat ini membuat perpustakaan mampu melakukan pengolahan informasi dengan semakin cepat dan tepat menggunakan internet. Internet merupakan interkoneksi jaringan komputer skala besar yang dihubungkan menggunakan protokol khusus (Maharani & Latifah, 2017).WAN (*Wide Area Network*) dan LAN (*Local Area Network*) sudah mampu menghubungkan semua jaringan komputer yang ada di lokal ataupn di pusat, dengan menggunakan sebuah *backup* data yang dikenal dengan *Disaster Recovery Center* dan masih ada istilah lainnya lagi. Namun, dibalik kecanggihan pemanfaatan teknologi dan internet harus didukung dengan canggihnya infrastruktur komunikasi yang dimiliki suatu perpustakaan salah satunya adalah *Virtual Private Network* (VPN).

VPN merupakan suatu bentuk private internet melalui public network (internet), dengan menekankan pada keamanan data dan akses global (Musril, 2019). VPN telah dipuji sebagai salah

satu solusi yang mengatasi semua masalah untuk meningkatnya biaya koneksi WAN dan LAN, disisi lain juga telah dikuatirkan akan menjadi titik lemah dalam sekuriti di perimeter atau perbatasan network (Brenton & Hunt, 2005). Koneksi virtual yang aman ini juga dibuat antara dua mesin, mesin dan jaringan, atau dua jaringan (Mairs, 2002). Dalam pengaplikasian VPN untuk mendapatkan koneksi yang bersifat *private*, data harus di-enskripsi dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses deskripsi (Wendy & Ramadhana, 2005). Ada banyak *platform* perangkat lunak yang dapat digunakan untuk mengimplementasikan VPN berbasis *software* solusi, seperti *Windows, Linux, Solaris, Mac,* dan *BSD* (Rahman, 2017). *Private network* dianggap lebih efisien karena kecepatan transfer data yang lebih besar dari pada kecepatan transfer data pada jaringan internet, selain itu keamanan dianggap lebih bagus karena hanya bergerak dalam lingkup terbatas saja (Masero et al., 2014).

Perpustakaan perguruan tinggi merupakan salah satu lembaga penyalur dan penyedia informasi di kalangan sivitas akademika. Untuk menyalurkan berbagai informasi yang ada dan menjalin komunikasi agar terhubung antara satu dengan yang lainnya perpustakaan menggunakan sebuah sistem dari jaringan komputer yang berbeda-beda. Mengingat pentingnya data di perpustakaan, diperlukan teknologi informasi dan VPN. Selain sebagai teknologi untuk memperlancar arus transfer data dan informasi, VPN juga penting untuk mengamankan keberadaan data tersebut agar tidak disalahgunakan.

Perpustakaan UNISMA merupakan salah satu perpustakaan perguruan tinggi yang sudah berbasiskan teknologi informasi dan telah memanfaatkan VPN. Perpustakaan sebagai lembaga pengelola informasi tentunya harus mampu mengamankan lalu lintas dari sebuah data yang terdapat pada jaringan komputer, karena data tersebut bersifat rahasia yang hanya bisa diakses oleh orang-orang tertentu. Perpustakaan UNISMA memilih menggunakan VPN sebab akses informasi dapat berlangsung secara cepat, efektif dan lebih aman. Sedangkan jaringannya dapat diterapkan pada LAN (*Local Area Network*) dan WAN (*Wide Area Network*).

VPN memungkinkan pengguna mampu terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan lokal. Pemasangan VPN di Perpustakaan UNISMA menggunakan server mikrotik *router operating system.* Dengan mikrotik tersebut, Perpustakaan UNISMA dapat melakukan perbandingan antara layanan VPN dengan layanan tanpa VPN. Keduanya dapat diimplementasikan dengan menggunakan protokol *IP Security*, data yang berjalan di dalam sebuah *tunnel* tidak dapat dimonitor karena data tersebut telah mengalami kompresi dan enskripsi (wawancara ES, 18 mei 2019). Pemanfaatan sistem VPN di Perpustakaan UNISMA ini menarik untuk diteliti dan dikaji karena sejauh ini belum ditemukan penelitian, khususnya yang terkait dengan pemanfaatan VPN di perpustakaan perguruan tinggi.

2. TINJAUAN PUSTAKA

2.1 Jaringan Komputer

Jaringan komputer adalah hubungan dua tali simpul (umumnya berupa komputer) atau lebih yang bertujuan untuk melakukan pertukaran data, dan dalam praktiknya jaringan komputer memungkinkan untuk melakukan berbagi perangkat lunak, perangkat keras, dan berbagi kekuatan pemrosesan (Kadir, 2014). Jaringan komputer mengintegrasikan sistem yang terdiri dari berbagai komputer beserta sumber dayanya yang didesain agar dapat menggunakan sumber daya yang ada, sehingga dapat mengakses informasi yang diperlukan (Afrianto & Setiawan, 2015).

Jaringan komputer merupakan sekelompok komputer otonom yang dihubungkan antara satu dengan lainnya dengan menggunakan protokol komunikasi melalui media transmisi data atau media komunikasi, sehingga saling dapat berbagi data informasi, progam-progam, penggunaan bersama perangkat keras seperti printer, hardisk dan sebagainya. Adapun manfaat dari jaringan komputer bagi sebuah organisasi, termasuk perpustakaan, yaitu: berbagi pakai peralatan dan sumber daya;

integrasi data; komunikasi; *distributed processing*; keteraturan aliran informasi; keamanan data; dan koneksitas berbagai jenis merk komputer (Oetomo, 2003; Sutedjo, 2003).

Jaringan komputer bisa juga berupa sekumpulan komputer dalam satu lokasi tertentu dan dihubungkan menggunakan media tertentu, seperti kabel jaringan atau teknologi *wireless*. Bahkan hingga jaringan besar, seperti internet, yang menggunakan satelit. Jaringan komputer yang dibentuk akan bisa digunakan untuk memindahkan suatu data, suara bahkan video antar komputer. Sebuah jaringan komputer akan disusun atas beberapa bagian, yang pertama adalah komputer itu sendiri dan yang lainnya adalah media koneksi, seperti kabel tembaga, *UTP, coaxial* atau *fiber optic*) dan peranti lainnya seperti *hub*, *switch* dan *router* (Winarno & Zaki, 2002).

2.2 Internet

Internet merupakan sekumpulan data jaringan dari sebuah komputer yang ada di seluruh dunia. Internet merupakan kepanjangan dari *interconnections networking* secara istilah ialah sistem global dari sebuah jaringan komputer yang sifatnya mendunia yang saling terhubung antara satu dengan lainnya yang menggunakan standar TCP/IP guna melakukan sebuah komunikasi maupun pertukaran data secara mendunia. Internet merupakan suatu interkoneksi sebuah jaringan komputer yang dapat memberikan layanan informasi secara lengkap, dan sudah terbukti bahwa internet dilihat sebagai media maya yang dapat menjadi rekan bisnis, politik sampai hiburan. Internet merupakan sebuah jaringan satelit komunikasi yang fungsinya sangat beragam dan menjadi pendukung internet di seluruh dunia. Dengan adanya internet dan *www* memungkinkan terciptanya perpustakaan digital. Internet yang juga dikenal dengan nama *informations superhighway*, merupakan singkatan dari *inter-networking*, yang terdiri dari sekumpulan jaringan komputer milik pemerintah, perusahaan, institusi, ataupun penyedia jasa jaringan ISP yang saling terhubung dimana masing masing jaringan komputer yang terhubung dikelola secara independen (Pendit, 2007).

2.3 Virtual Private Network

VPN merupakan sebuah jaringan publik yang menjamin ketersediaan jalur komunikasi untuk suatu perusahaan tetapi tidak dalam bentuk jalur khusus, jaringan ini memiliki karakteristik: (a) perusahaan pemakai jasa dan membayar biaya langganan plus biaya penggunaan berdasarkan waktu; (b) meski tidak memakai jalur khusus, ketersediaan koneksi dijamin; (c) kecepatan transfer lebih tinggi daripada jaringan publik; (d) keamanan tinggi karena ada fasilitas enskripsi (Kadir, 2014). VPN merupakan sebuah sistem yang dipuji sebagai solusi yang mampu mengatasi semua masalah untuk meningkatnya biaya koneksi WAN dan disisi lain juga telah dikuatirkan bahwa akan menjadi titik lemah pada sebuah sekuriti di perimeter atau perbatasan network (Brenton & Hunt, 2005).

Adapun dasar-dasar pada VPN yakni sebuah *channel* komunikasi yang sudah terotentikasi dan terenskripsi melalui sebuah *network public* seperti internet (Brenton & Hunt, 2005). VPN merupakan teknologi jaringan komputer yang memanfaatkan media komunikasi publik (*open connection* atau *virtual circuits*), seperti internet, untuk menghubungkan beberapa jaringan lokal (Satwika, 2019). *User* yang terhubung ke dalam jaringan VPN perlu akun dan sandi untuk *login* (Musril, 2019). Melalui pemanfaatan VPN mampu menghubungkan koneksi antar dua jaringan atau lebih ke dalam suatu jaringan dengan menggunakan infrastruktur telekomunikasi umum dan menggunakan metode enskripsi tertentu sebagai media pengamanannya. VPN juga dapat diartikan sebagai suatu bentuk *private* internet yang digunakan melalui internet, dengan menekankan pada keamanan data dan akses global.

Selain melakukan pengamanan jaringan pada komputer, sebuah pengendalian akan tetap dipasang kemudian perlu adanya sebuah pemeriksaan untuk mengecek ulang fungsi pengendalian. Pemeriksaan ini disebut dengan audit sistem informasi. Menurut Weber (1999) audit sistem informasi adalah suatu proses mengumpulkan dan mengevaluasi bukti untuk menentukan apakah

suatu sistem komputer telah menjaga aktiva-aktiva, menjaga intregritas data, membuat sasaran organisasi dicapai secara efektif dan menggunakan sumber daya yang efisien. Tujuan dari audit sistem informasi yaitu untuk meningkatkan: keamanan dari aktiva-aktiva, intregritas data, efektivitas sistem; dan efisiensi sistem (Jogiyanto, 2005). Menurutnya, ada beberapa prosedur dalam pengauditan sistem informasi, yaitu:

a) prosedur untuk mendapatkan pemahaman dari pengendalian-pengendalian yang ada;
b) pengujian terhadap pengendalian-pengendalian;
c) pengujian pengendalian terhadap nilai transaksi secara terperinci;
d) pengujian terhadap nilai saldo di rekening secara terperinci;
e) prosedur kaji analitik.

Menurut Farly, et al. (2017), teknologi VPN menggunakan 2 fungsi yaitu:

1) *Confidentialy*, teknologi VPN memiliki sistem kerja untuk mengenskripsi data yang melaluinya. Dengan menerapkan sistem enskripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data atau *client* dengan mudah. VPN memiliki teknologi yang dapat menjaga keutuhan data yang dikirim oleh *client* agar sampai ke tujuan tanpa cacat, hilang, rusak, ataupun dimanipulasi oleh orang lain.
2) *Origin authentications*, teknologi VPN memiliki kemampuan untuk melakukan otentifikasi terhadap sumber-sumber pengiriman data yang akan diterimanya.

3. METODE

Penelitian ini menggunakan pendekatan kualitatif – deskriptif, yaitu mendeskripsikan dan menjawab berbagai persoalan suatu fenomena atau peristiwa yang terjadi saat ini, baik tentang fenomena dalam variabel tunggal maupun korelasi dan atau perbandingan berbagai variabel (Arifin, 2011). Peneliti mencatat segala gejala (fenomena) yang dilihat dan didengar serta dibaca (via wawancara/lainnya, catatan lapangan, foto, video *tape*, dokumen pribadi atau memo, dokumen resmi/lainnya, dan lain-lain), dan peneliti harus membanding-bandingkan, mengkombinasikan, mengabstraksikan, dan menarik kesimpulan (Bungin, 2008). Objek kajian penelitian ini adalah implementasi VPN yang dilakukan oleh Perpustakaan UNISMA Malang. Pengumpulan data menggunakan metode wawancara, observasi dan tinjauan literatur.

Wawancara dilakukan kepada responden yang mampu memberikan penjelasan secara seksama terhadap permasalahan penelitian, yaitu lima orang pustakawan di Perpustakaan UNISMA dengan inisial IR, IJ, KL, MM, JK. Pemilihan informan dalam penelitian ini dilakukan dengan teknik *purposive sampling*. Sampel yang diseleksi atas dasar kriteria tertentu yang dibuat peneliti berdasarkan tujuan riset. Kriteria informan dalam penelitian ini adalah pustakawan atau staf perpustakaan yang bertugas mengelola IT perpustakaan dan pustakawan atau staf perpustakaan yang mengetahui pemanfaatn VPN di perpustakaan UNISMA. Teknik analisis data dilakukan dengan menggunakan teori *Miles & Hubberman* yaitu pengumpulan data, reduksi data, penyajian data dan terakhir adalah penarikan kesimpulan (Sugiyono, 2017). Keabsahan data penelitian diperoleh melalui *triangulasi* yang dilakukan dengan cara membandingkan antara data hasil observasi, wawancara, dan dokumen hingga mendapatkan satu kesimpulan yang sama dan tidak ada data tambahan lain di luar konteks penelitian.

4. HASIL DAN PEMBAHASAN

4.1 Alasan VPN di Perpustakaan UNISMA

VPN merupakan sebuah *channel* komunikasi yang mampu terotentifikasi dan terenskripsi melalui suatu bentuk *network* yang bersifat mendunia atau biasa disebut dengan internet. *Network*

yang bersifat umum atau mendunia dianggap memiliki keamanan yang kurang terjamin. Dari hal tersebut kemudian muncul sebuah enskripsi dan otentikasi yang digunakan untuk melindungi sebuah data saat berlangsungnya proses pengiriman maupun pertukaran data, sebuah VPN bersifat *service independent,* atau tidak memiliki ketergantungan pada suatu jenis *service* yang menggunakannya. Pada pertukaran dua *host* (*WEB, FTP, SMPT,* dsb.) akan dikirimkan melalui kanal yang sudah terenskripsi (Brenton & Hunt, 2005), seperti adanya dua *network* yang berbeda dihubungkan ke internet, kemudian kedua *network* ini melakukan pertukaran data, keduanya ingin proses tersebut berlangsung secara aman karena terdapat sebagian data yang bersifat pribadi. Koneksi dari VPN haruslah dipersiapkan masing masing dari lokasi perpustakaan tersebut.

VPN di perpustakaan UNISMA juga digunakan untuk melindungi privasi data. Koneksi VPN dalam bentuk *virtual* (maya) dan bersifat *private* (rahasia), sehingga hanya *user* tertentu saja yang bisa mengaksesnya (Musril, 2019). Dengan VPN ini teknologi komunikasi yang memungkinkan pengguna untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal yang ada. Kekurangan penggunaan jaringan internet di Perpustakaan UNISMA dikarenakan koneksi internet yang belum dapat diprediksi. Perpustakaan hanya 'menumpang' koneksi pada jaringan pihak lain sehingga tidak mempunyai kontrol langsung terhadap jaringan tersebut. Pustakawan perlu melakukan perhatian yang lebih untuk mengantisipasi terjadinya hal hal yang tidak diinginkan seperti penyadapan, *hacking*, dan tindakan *cyber crime* pada jaringan VPN (Wawancara IH, 16 Mei 2019).

Dengan memanfaatkan VPN juga semakin mempermudah, seolah olah membuat jaringan di dalam jaringan yang biasa disebut dengan *tunnel*. *Tunnel* merupakan sebuah cara membuat jalur privat dengan menggunakan infrastruktur pihak ketiga. VPN ini menggunakan salah satu dari tiga teknologi *tunneling* yang ada seperti, PPTP, L2TP dan standar terbaru, *Internet Protocol Security.* Dalam pemakaiannya, VPN juga membutuhkan sebuah perencanaan yang matang, sebagaimana dikatakan Brenton & Hunt (2005) sebagai berikut.

a) Menyiapkan sebuah alat yang mempunyai kemampuan VPN (VPN- *capable device*) di perimeter *network* tersebut. Alat ini bisa berupa sebuah *router*, sebuah *firewall*, atau sebuah alat yang khusus (*dedicated*) untuk aktivitas VPN.
b) Mengetahui alamat *subnet* ip yang digunakan oleh lokasi lain.
c) Menyetujui sebuah metode otentikasi dan mempertukarkan *certivicate digital* jika diperlukan.
d) Menyetujui sebuah metode enskripsi dan mempertukarkan *key* enskripsi sesuai kebutuhan.

Penerapan dasar alat pada masing-masing ujung dari *tunnel* VPN adalah *router* yang digunakan untuk membuat koneksi ke internet. Jika alat alat tersebut merupakan *router* cisco yang cukup baru, maka alat tersebut akan mendukung ip *security*, yang selalu menyediakan otentikasi *Diffie-Hellman* dan *enskripsi 3DES* (*triple data encryption standar*) 128 bit. Kemudian anda harus mengkonfigurasi *router* pada *network* A agar semua lalu lintas *network* ke arah luar yang menuju ke *subnet* 192.168.2.0 akan dienskripsi menggunakan 3DES. Konfigurasi ini disebut domain enskripsi di *remote*.

Setelah dikonfigurasi VPN, sebuah *network analyzer* yang ditempatkan antara kedua *router* akan menampilkan sebuah paket dengan menggunakan alamat IP *sources* dan destinasi yang digunakan oleh interface-interface pada kedua *router* tersebut. Anda tidak akan dapat melihat alamat IP dari *host* destinasi. Proses tersebut merupakan sebuah proses *tunneling*, dengan *tunneling* ini dapat membantu untuk memastikan agar seorang penyerang yang berhasil melakukan penyusupan ke *network* tidak akan bisa menebak lalu lintas yang mana, dari semua lalu lintas yang melewati VPN, yang layak untuk di-*crake*, karena semua paket yang lewat VPN akan menggunakan alamat-alamat IP dan kedua *router* di kedua ujung VPN tersebut. Kegiatan di atas

juga dapat memiliki keuntungan dimana VPN yang terpakai tidak tergantung pada jenis *platform* dan *service*.

4.2 Penggunaan VPN di Perpustakaan UNISMA

Perpustakaan UNISMA, VPN menggunakan server mikrotik *router operating system*. Mikrotik merupakan sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router network yang handal. Mikrotik adalah penamaan dari sebuah produsen *router*, yang telah berhasil membuat *router* yang handal, terdapat dua jenis mikrotik yaitu: perangkat keras (*Mikrotik Router Board*) dan perangkat lunak (*Mikrotik Router OS*) dengan beberapa sistem operasi berbasis LINUX yang dapat diinstal pada komputer rumahan (Supendar, 2016). Fitur VPN dibuat untuk *IP network* dan jaringan *wireless*, cocok digunakan ISP dan *provider hotspot*. Untuk dapat menjadikan mikrotik sebagai server VPN, diperlukan konfigurasi yang meliputi konfigurasi IP *pool*, konfigurasi *IP router*, konfigurasi PPP, konfigurasi DHCP *server*, konfigurasi *firewall NAT by pass* dan konfigurasi *IP security* (wawancara AL, 16 Mei 2019). Dalam penggunaanya, tentunya terdapat sebuah pengujian keamanan VPN dengan melakukan serangan (*attack*) pada *server* komputer menggunakan metode DOS. Serangan ini sebenarnya bertujuan untuk menghentikan maupun mematikan *service* pada komputer target. Sebenarnya dari efek serangan tersebut akan cukup mengganggu koneksi antara *client* dan *server*. Dimana dari proses tersebut akan terhenti setelah jumlah paket ping yang dikirimkan sudah terpenuhi yakni 10000 paket maka koneksi IP akan kembali (Supendar, 2016).

VPN selain digunakan sebagai akses keamanan, juga dapat digunakan sebagai pengganti *pool* modem. Dimana *pool* modem merupakan sumber masalah bagi administrasi *network*. Meskipun solusi yang stabil tersedia, biasanya solusi itu terlalu mahal bahkan melebihi anggaran dari sebuah organisasi kecil maupun organisasi besar. Adapun beberapa masalah yang biasa dihadapi oleh administrator antara lain: modem yang menjawab secara otomatis; pengkabelan bermutu rendah; kelompok modem yang dikonfigurasi dengan keliru; dan karyawan karyawan *remote* menggunakan computer-komputer personal yang mungkin tidak dikonfigurasi dengan baik atau sudah terlanjur diserang oleh virus atau kode yang merusak (Brenton & Hunt, 2005).

VPN menjadi salah satu solusi untuk *user remote* bisa secara dramatis mengurangi biaya dukungan secara teknis. Selain itu, VPN juga mendukung cara kerja saat mereka tidak ada di kantor secara fisik. Anda tidak perlu susah payah memintai sambungan telepon lagi ataupun meminta nomor sambungan khusus (semisal nomor 800). Setiap melakukan *upgrade hardware* maupun *upgrade* sambungan data yang dikeluarkan kebijakan baru maka secara otomatis sambungan telepon sudah ada aplikasi yang mendukung teknologi baru seperti ISDN (*integrated servicenya digital network*). Semua akses yang datang akan dikelola melalui koneksi internet, sebuah koneksi yang sudah dimainkan oleh perusahaan maupun perpustakaan sehingga mudah melakukan akses di internet. Hal terpenting adalah petugas harus sering melakukan pengecekan secara teliti terhadap akses ke *network*.

Selain itu, VPN juga dapat meringankan biaya, baik biaya infrastruktur maupun biaya dukungan *end user*. *Problem heldesk* untuk *remote* akses yang paling sering yakni membantu *end user* untuk mengkonfigurasi *setting network* dan melakukan koneksi ke *network*. Ketika menghubungkan ke *network* kantor, *user* terlebih dahulu harus melakukan *dial up* ke sebuah ISP, kemudian biasanya ISP akan menyediakan dukungan *help desk* tersebut. *Help desk* dari suatu organisasi hanya perlu terlibat jika *user* bisa mengakses sumber daya di internet, tetapi mengalami masalah untuk mengakses sumber daya dari dalam.

Di perpustakaan UNISMA aksesnya menggunakan jaringan WAN dan LAN (wawancara WS, 16 Mei 2019). Maka dari itu VPN dapat menggantikan *link* WAN yang sedang di-*dedicated*. VPN dapat menjadi pilihan yang cukup tepat untuk mengatasi keterbatasan LAN (Satwika, 2019). Dalam

menggunakan VPN untuk menghubungkan dua buah *network* yang terpisah secara geografis melalui internet, akan sangat menguntungkan jika kedua lokasi terpisah dengan jarak yang cukup jauh. Namun dalam penggunaan jarak dekat juga dapat menguntungkan meskipun dalam lokasi yang juga berbeda. Sebuah *network* internal akan dilindungi oleh sebuah *firewall*. Sebuah segmen DMZ ditempati oleh *server web* dan *mail relay* anda. Sebagai tambahannya, petugas harus memiliki sebuah kartu *network* ekstrak di *firewall* untuk mengelola *security* ke jumlah sambungan T1 yang *dedicated.* Rangkaian T1 yang menghubungkan ke *partner* maupun *user* melalui jaringan internet dan akan melindungi informasi yang sensitif. Informasi yang sensitif ini bisa juga dikirim melalui FTP maupun *email*.

4.3 Pemilihan Produk VPN

Sebelum memutuskan untuk menggunakan VPN, ada beberapa hal yang perlu dipertimbangkan oleh perpustakaan, diantaranya sebagai berikut.

1) Otentikasi yang kuat
   Tanpa adanya otentikasi yang kuat, anda tidak akan mempunyai cara untuk menentukan apakah sistem di ujung lain dari *tunnel* VPN benar-benar kuat seperti yang sudah diakui. Standar yang lebih baru untuk otentikasi yang menggantikan *diffie* Helman yang sudah tua dan *vulnerable*, yaitu IKE, memungkinkan sebuah *secret key* yang di-*share* untuk dimunculkan sebagai pertukaran data *public key*. Pertukaran ini menghilangkan kebutuhan untuk mempertukarkan informasi *secret key* melalui beberapa cara alternatif.

2) Enkripsi yang cukup kuat
   Dalam hal ini hendaknya memperhatikan dan menentukan level proteksi apa yang diperlukan sebelum memilih sebuah metode enkripsi. Sedangkan standar enskripsi terendah yakni 3DES. Tetapi masih banyak produk VPN menggunakan standar 56 bit, kemampuan ini sebenarnya sudah meningkat ke titik yang mana memecahkan enskripsi tidak sulit lagi. Enskripsi *secret key*, seperti 3DES yang populer kecepatan nya di VPN. Selain itu juga banyak produk VPN menggunakan *alogaritma public/private* untuk mempertukarkan *secret key* pada awalnya, tetapi kemudian menggunakan enskripsi *secret key* untuk komunikasi berikutnya.

3) Memenuhi standar
   Hal yang sama berlaku pada saat memilih sebuah metode untuk enskripsi VPN anda. Tetaplah menggunakan *alogaritma* yang telah teruji oleh waktu dan tidak memiliki *vulnerability* yang penting.

4) Integrasi dengan *service network* bidang lain
   Solusi VPN yang lebih baru bisa berintegrasi dengan *service* lain, termasuk *firewall*, direktori *user* dan *soft* pemantau. VPN 1 dari cek poin sepenuhnya terintegrasi ke seluruh aplikasi manajemen cek poin yang memungkinkan hanya integrasi *security* komplit. Tetapi juga *address translation* dan alokasi *bandwidth*. Kemampuan untuk mengelola otentikasi dari koneksi VPN secara terpusat yang mampu mengontrol sejumlah *bandwidth* yang diijinkan untuk setiap koneksi merupakan sebuah *feature* yang *powerful*.

Sebelum mengakses dan menggunakan VPN, perpustakaan hendaknya melakukan simulasi dan evaluasi terlebih dahulu, agar penggunaannya dapat secara maksimal. Sebagaimana yang dikatakan Supendar (2016), kegiatan evaluasi tersebut bertujuan untuk: (1) mengurangi resiko kegagalan saat proses perancangan dan implementasi sistem jaringan VPN dengan *pptp* maupun open VPN; dan (2) menjamin bahwa kegagalan atau kesalahan yang terjadi pada waktu proses perancangan,

pembangunan dan implementasi tidak mengganggu dan mempengaruhi lingkungan sistem yang sebenarnya

5. KESIMPULAN

Penggunaan VPN di Perpustakaan UNISMA selain untuk mempermudah dan mempercepat koneksi internet juga digunakan untuk melindungi privasi data. Kelemahan penggunaan VPN terdapat pada koneksi internet yang belum bisa diprediksi karena melanggan internet dari pihak ketiga sehingga perpustakaan tidak mempunyai kontrol langsung terhadap jaringan tersebut. Implementasi VPN di perpustakaan UNISMA menggunakan server mikrotik *router operating system*. Mikrotik tersebut digunakan untuk menjadikan komputer menjadi *router network* yang memiliki berbagai fitur untuk *IP network* dan jaringan *wireless*, serta digunakan untuk *ISP* dan *provider hotspot*. Untuk dapat menjadikan mikrotik sebagai server VPN, memerlukan konfigurasi yang meliputi konfigurasi *IP pool*, konfigurasi *IP router*, konfigurasi *PPP*, konfigurasi *DHCP server*, konfigurasi *firewall NAT by pass* dan konfigurasi *IP security*. Pemilihan Produk VPN di Perpustakaan UNISMA mempertimbangkan berbagai aspek seperti, otentikasi yang kuat, enkripsi yang cukup kuat, memenuhi standar, integrasi dengan servis network bidang lain.

DAFTAR PUSTAKA

Afrianto, I. & Setiawan, E.B. 2015. Kajian Virtual Private Network (VPN) sebagai Sistem Pengamanan Data Pada Jaringan Komputer (Studi Kasus Jaringan Komputer Unikom). *Majalah Ilmiah UNIKOM, 12*(1), 43–52. https://doi.org/10.34010/miu.v12i1.34

Arifin, Z. 2011. *Penelitian Pendidikan*. Bandung: Remaja Rosdakarya.

Brenton, C. & Hunt, C. 2005. *Network Security*. Jakarta: Elex Media Komputindo.

Bungin, B. 2008. *Analisa Data Penelitian Kualitatif*. Jakarta: Prenadamedia Group.

Farly, K. A., Najoan, X. B. N., & Lumenta, A.S.M. 2017. Perancangan dan Implementasi VPN Server dengan Menggunakan Protokol SSTP *(Secure Socket Tunneling Protocol)*: Studi Kasus Kampus Universitas Sam Ratulangi. *Jurnal Teknik Informatika, 11*(1). https://doi.org/10.35793/jti.11.1.2017.16745

Jogiyanto. 2005. *Sistem Teknologi Informasi*. Yogyakarta: Andi Offset.

Kadir, A. 2014. *Pengenalan Sistem Informasi Revisi*. Yogyakarta: Andi Offset.

Maharani, M. & Latifah, F. 2017. Penerapan Teknologi Virtual Private Network. *Journal on Networking and Security, 7*(2), 5–9.

Mairs, J. 2002. *VPNs: A Beginner's Guide*. Kanada: McGraw-Hill.

Masero, A.P., Triyono, J., & Andayati, D. 2014. Perancangan Pengelolaan Jaringan IT Institut Sains & Teknologi AKPRIND Menggunakan Teknologi VPN (Virtual Private Network). *Jurnal JARKOM, 2*(1), 21–30.

Musril, H.A. 2019. Desain Virtual Private Network (VPN) Berbasis Open Shortest Path First (OSPF). *InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan), 3*(2), 83–88. https://doi.org/10.30743/infotekjar.v3i2.1055

Oetomo, B.S.D. 2003. *Konsep dan Perancangan Jaringan Computer: Bangunan Satu Lantai, Gedung Bertingkat dan Kawasan*. Yogyakarta: Andi Offset.

Pendit, P.L. 2007. *Perpustakaan Digital: Prepektif Perguruan Tinggi Indonesia*. Jakarta: Sagung Seto.

Rahman, T. 2017. Implementasi Virtual Private Network Over GRE TUNNEL. *Indonesian Journal on Networking and Security*, *6*(3), 40–49.

Satwika, I.K.S. 2019. Analisis Quality of Service Jaringan Virtual Private Network (VPN) di STMIK Stikom Indonesia. *Jurnal Ilmiah Informatika*, *7*(01). https://doi.org/10.33884/jif.v7i01.1016

Sugiyono. 2017. *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta.

Supendar, H. 2016. Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik. *Bina Insani ICT Journal*, *3*(1).

Wendy, A. & Ramadhana, A. 2005. *Membangun VPN Linux secara Cepat*. Yogyakarta: Andi Offset.

Winarno, E. & Zaki, A. 2002. *Easy Networking*. Jakarta: Kompas Gramedia.