Penerapan Protokol SSL dan IPSec pada *Integrated* VPN's *Technology* (IVPNT)

Claudia Dwi Amanda, Fitria Sekarwulan, Danang Jaya
Deputi Bidang Perkajian Persandian, Lembaga Sandi Negara
amanda_hectic@yahoo.com, querydanangjaya@yahoo.com

ABSTRAK

Penggunaan teknologi Virtual Private Network (VPN) sebagai solusi pengamanan saat ini masih tambal sulam. Berbagai solusi produk VPN, secara hardware dan software, telah banyak beredar pasar, namun manajemen VPN menyulitkan para pengguna (end-user). Untuk itu diperlukan sebuah aplikasi yang dapat menggunakan protokol VPN dengan kemudahan manajemen aplikasi VPN yang dapat mengurangi kompleksitas penggunaan VPN (SSL dan IPSec) dan mengintegrasikan fitur keamanan dan teknologi komunikasi VPN. Integrated Virtual Private Network Technology (IVPNT) merupakan rancang bangun solusi VPN layanan VPN yang menggunakan protokol SSL dan IPSec yang menyediakan keamanan end-to-end, termasuk dengan fungsi manajemen VPN berbasis Command Line Interface (CLI). Hasil dari pengujian yang dilakukan jaringan IVPNT menggunakan protokol SSL dan IPSec, telah terbukti terlindungi dengan cara pesan yang ditransmisikan terlihat acak sehingga pesan tersebut tidak dapat dipahami oleh pihak yang tidak berwenang.

***Kata Kunci** : Virtual Private Network (1), Secure Socket Layer (2), IPSecurity (3)*

1. PENDAHULUAN

Setiap entitas pengguna informasi elektronik, akan membutuhkan suatu sistem yang dapat menyediakan layanan konektivitas antar individu dan/atau antar instansi maupun sistem koneksi dengan mitra kerja. Sehubungan dengan kebutuhan tersebut, maka suatu instansi perlu mempertimbangkan untuk membangun suatu sistem jaringan komunikasi yang memiliki jangkauan luas, namun akses terbatas hanya untuk *stakeholder* yang berwenang. Dengan kata lain, instansi memerlukan suatu sistem jaringan komunikasi yang bersifat khusus untuk memenuhi kebutuhan transaksi informasi elektronik.

Implementasi jaringan yang bersifat khusus dapat dilakukan secara fisik menggunakan *leased line* maupun secara logikal, yaitu *Virtual Private Network* (VPN) yang memanfaatkan infrastruktur jaringan telekomunikasi publik. Pada dasarnya, VPN merupakan suatu proses pembentukan kanal telekomunikasi yang bersifat privat dan relatif aman pada suatu infrastruktur jaringan publik, misalnya internet. VPN membangun suatu *secure tunnel* virtual dengan memanfaatkan media jaringan publik yang telah tersedia, sehingga jika dilihat dari sudut pandang ekonomis, maka biaya penggunaan VPN lebih murah dibandingkan penggunaan jaringan *leased line* yang membutuhkan biaya pembangunan infrastruktur jaringan, perijinan, pemeliharaan, dan sebagainya. VPN menggunakan protokol *Secure Socket Layer* (SSL) yang bekerja pada *transport layer* dan *Internet Protocol Security* (IPSec) yang bekerja pada *network layer* [2]. Kebutuhan kedua protokol tersebut tergantung pada aplikasi yang akan beroperasi menggunakan VPN.

Alshamsi dan Saito [1] membandingkan antara protokol SSL dan IPSec secara teknis dalam hal algoritma yang digunakan, ukuran yang dihasilkan, mode koneksi, operasi kriptografi, dan hal-hal lainnya dengan kesimpulan bahwa penggunaan SSL atau IPSec bergantung pada kebutuhan keamanan yang diperlukan. Beberapa tahun selanjutnya, Degabriele dan Paterson [2] menjelaskan tentang serangan baru yang efisien dan realistis, serangan tersebut dilakukan pada IPSec khususnya di *encryption-only* ESP. Sehingga SSL dapat dikatakan lebih aman dibandingkan IPSec dalam hal ketahanan

terhadap serangan. Adanya perbedaan layer pada kedua protokol tersebut, mengakibatkan SSL VPN dan IPSec VPN pada umumnya tidak diimplementasikan secara bersamaan dalam satu alat atau aplikasi. Oleh karena itu, Penulis memberikan alternatif layanan dengan menggabungkan kedua protokol VPN agar *user* dapat memilih protokol yang sesuai dengan kebutuhan dengan nama "*Integrated* VPN's *Technology* (IVPNT)".

Perancangan VPN *user interface* yang mampu mengakomodasi pemilihan kedua protokol tersebut, biasanya memiliki kesulitan dalam proses konfigurasi VPN. Salah satu teknik untuk menyelesaikan masalah tersebut adalah melakukan manajemen *user interface* menggunakan *Command Line Interface* (CLI) yang *user friendly,* sehingga proses pembangunan VPN tidak menjadi rumit. Konfigurasi VPN berkorelasi dengan pengaturan sistem pada sistem operasi, sehingga manajemen *user interface* tersebut harus dapat berkomunikasi dengan sistem pada sistem operasi.

Penulis akan memanfaatkan distro linux sebagai sistem operasi untuk mengoperasikan aplikasi layanan VPN dengan protokol SSL dan IPSec. Aplikasi layanan VPN tersebut akan diinstalasi ke dalam distro tersebut dengan media *Single Board Computer* (SBC). Berdasarkan hal-hal tersebut, aplikasi layanan VPN yang terinstalasi dalam SBC diharapkan dapat menjadi alternatif untuk melakukan komunikasi ke jaringan privat melalui jaringan publik secara efektif dan efisien.

Paper ini terdiri atas beberapa bagian, antara lain penjelasan tentang teori-teori terkait IVPNT pada bagian 2, metode yang digunakan untuk membuat IVPNT pada bagian 3, hasil implementasi ditunjukkan pada bagian 4, dan yang terakhir adalah kesimpulan pada bagian 5.

2. LANDASAN TEORI

VPN adalah sebuah metode yang menggunakan *tunneling* untuk membangun sebuah jaringan privat pada jaringan publik, sedemikian sehingga keamanan pada jaringan privat tersebut ekuivalen dengan keamanan yang disediakan oleh *leased line* [6]. Salah satu elemen penting dari VPN adalah enkripsi yang berfungsi untuk melindungi data sensitif (rahasia) ketika melewati internet. Oleh karena itu dibutuhkan *virtual private tunnel*, yang dapat mengenkripsi paket data atau *frame*, kemudian melakukan enkapsulasi antara kedua *host* atau jaringan [4].

SSL adalah sebuah protokol yang memberikan enkripsi pada *traffic* berbasis jaringan. SSL adalah sebuah protokol jaringan yang mempunyai tanggung jawab untuk mengamankan, mengenkripsi saluran komunikasi antara sebuah server dan sebuah *client* [7]. IPSec adalah sebuah metode untuk melindungi datagram IP. Perlindungan terebut dalam bentuk *data origin authentication*, *connectionless data integrity authentication*, dan *data content confidentiality* [3].

Pada umumnya VPN menggunakan protokol *Secure Socket Layer* (SSL) yang bekerja pada *transport layer* dan *Internet Protocol Security* (IPSec) yang bekerja pada *network layer* [4]. Kebutuhan kedua protokol tersebut tergantung pada aplikasi yang akan beroperasi menggunakan VPN. Adanya perbedaan layer pada kedua protokol tersebut, mengakibatkan SSL VPN dan IPSec VPN pada umumnya tidak diimplementasikan secara bersamaan dalam satu alat atau aplikasi. Perbandingan antara SSL dan IPSec dapat dilihat pada Tabel 1 [5].

Tabel 1. Perbandingan SSL dan IPSec

	Access Control	Encryp-tion	Authen-tication	Integrity Checking	Address Conceal-ment	Session Monitoring
SSL	y	y (paket)	y (paket)	y (paket)	y	n
IPSec	y	y (data)	y	y	n	y

Berdasarkan Tabel 1, terdapat beberapa kelebihan dan kekurangan dari masing-masing protokol, sehingga dipandang perlu untuk merancang suatu sistem VPN yang dapat

mengakomodasi dua protokol tersebut sebagai alternatif untuk penyelenggaraan VPN sesuai dengan kebutuhan tingkat pengamanan jaringan. Kondisi tersebut dibutuhkan agar *user* dapat menggunakan protokol secara tepat dalam melakukan operasi aplikasi yang diinginkan.

Dari tabel di atas, dapat dilihat bahwa SSL melakukan layanan terhadap paket, sedangkan IPSec melakukan layanan terhadap data, sesuai dengan layer tempat kedua protokol tersebut diimplemetasikan. Hal ini menyebabkan SSL digunakan oleh *user* yang membutuhkan akses *high-level*, sedangkan IPSec digunakan oleh *user* yang membutuhkan akses *low-level*. Dari segi biaya yang dikeluarkan, SSL lebih dapat menghemat biaya dibandingkan dengan IPSec [7].

Kombinasi dari beberapa layanan pada tabel dilakukan dengan tujuan untuk menjamin tingkat keamanan tertentu. Akses kontrol disediakan oleh kedua protokol sehingga dapat membatasi pihak yang ingin melakukan akses terhadap suatu sumber daya. Enkripsi, otentikasi, pemeriksaan integritas disediakan oleh kedua protokol untuk melayani informasi (berupa paket atau data) sesuai dengan level jaringan yang ada sehingga informasi dapat dirahasiakan, pihak yang terkait dapat diotentikasi, dan mencegah adanya perubahan terhadap informasi yang ditransmisikan [6].

Layanan *address concealment* bertujuan untuk melindungi dari serangan *denial-of-service* [5], layanan tersebut disediakan oleh SSL sehingga IPSec rawan oleh serangan tersebut. Sedangkan pada *session monitoring* yang bertujuan untuk mengontrol sesi komunikasi yang berlangsung, layanan tersebut disediakan oleh IPSec sehingga dapat melakukan *troubleshoot* saat VPN berlangsung dan melakukan *monitoring interface end-user*.

3. METODE

Dalam pembuatan paper ini, penulis menggunakan model proses pengembangan perangkat lunak Model Sekuensial Linear. Pada pengembangan aplikasi IVPNT, penulis menggunakan metodologi pengembangan perangkat lunak terstruktur. Penulis melakukan studi literatur terkait dengan rancang bangun IVPNT, menganalisis permasalahan dan kebutuhan dari IVPNT, mendesain sistem, melakukan implementasi, kemudian pengujian terhadap sistem IVPNT.

Penulis menggunakan satu buah laptop, tiga buah PC, dan satu buah SBC yang telah terinstalasi aplikasi IVPNT. Sedangkan *software-software* yang digunakan oleh Penulis untuk membuat komponen inti maupun pendukung dalam aplikasi IVPNT antara lain paket SSL, paket IPSec, VirtualBox, Clonezillla, dan Wireshark.

Langkah awal dalam membuat IVPNT adalah melakukan *remastering* Linux Ubuntu terlebih dahulu agar menghasilkan distro untuk IVPNT. Adapun proses pembuatan distro IVPNT secara umum terdiri dari dua tahapan utama, yaitu persiapan spesifikasi kebutuhan sistem dan tahap proses. Tahap proses merupakan inti utama pembuatan distro untuk IVPNT dengan menjelaskan urutan langkah-langkah yang dilakukan. Adapun hal yang dilakukan pertama kali adalah melakukan instalasi *tools* yang diperlukan seperti *squashfs-tools*, *Mkisoft*, dan *VirtualBox*. Kemudian meletakkan file-file untuk IVPNT ke dalam direktori kerja tersendiri untuk memudahkan proses kustomisasi.

Setelah distro selesai dibuat, tentukan direktori-direktori untuk konfigurasi. Dalam IVPNT terdapat tiga buah direktori yaitu *etc*, *scripts*, dan *template*. Direktori *etc* berisi file-file untuk konfigurasi program CLI, direktori *scripts* berisi file-file *bash shell script* untuk CLI, dan direktori *template* berisi *template* konfigurasi file. Proses implementasi IVPNT terdiri dari tiga tahap, yaitu :

a. Tahap Awal

Pada tahap persiapan, admin telah mempersiapkan konfigurasi yang ingin digunakan. Admin juga memastikan bahwa sistem IVPNT dapat berjalan dengan baik. Hal ini bertujuan agar memudahkan pengguna dalam pemilihan protokol yang ingin digunakan. Menu IVPNT terdiri dari *configuration, network, connection, log,*

shell prompt. Gambar 1 adalah tampilan menu dari IVPNT :

Gambar 1. Tampilan Menu IVPNT.

b. Tahap Pemrosesan Data

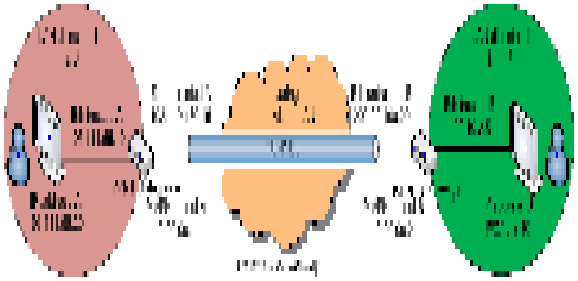
Pada tahap pemrosesan data, admin telah dapat menggunakan aplikasi IVPNT. Pada halaman CLI akan ditampilkan halaman meu. Pada tampilan CLI, admin dapat menetapkan protokol maupun parameter-parameter dengan mengetikkan kode sesuai perintah yang ingin dilakukan. Untuk menggunakan menu *shell prompt*, admin memasukkan *password* ke dalam *field* yang telah disediakan. Jika terverifikasi, maka admin dapat menggunakan aplikasi IVPNT.

c. Tahap Akhir

Pada tahap akhir, admin telah dapat memilih dan menggunakan protokol yang telah disediakan oleh aplikasi IVPNT. Admin juga dapat menggunakan aplikasi yang memanfaatkan protokol yang telah ditetapkan oleh aplikasi tersebut.

Pada implementasinya, IVPNT digunakan untuk mengamankan jaringan privat dengan memanfaatkan jaringan LAN-to-LAN. Dengan menggunakan jaringan LAN-to-LAN, antara komputer admin (SBC) dengan komputer klien dapat dihubungkan menggunakan kabel. Sebelum klien terhubung dengan admin untuk melakukan komunikasi secara aman, klien mempunyai IP *address* yang sebenarnya (IP *real*). Setelah klien berhasil terhubung, maka komunikasi secara aman dapat dilakukan. Hal ini ditandai dengan klien berhubungan melalui IP *gateway*.

Dari penjelasan tersebut, dapat dilihat bahwa SBC digunakan pada sisi admin untuk menyediakan layanan pemilihan untuk protokol VPN, dimana di dalam SBC tersebut telah terinstalasi aplikasi IVPNT. Aplikasi IVPNT berbasis CLI, sehingga pada sisi admin dimudahkan dengan cukup mengakses aplikasi tersebut menggunakan *command line* admin. Komponen minimal yang harus dipenuhi agar sistem dapat berjalan sesuai dengan keinginan ialah ketersediaan sumber daya listrik yang dapat digunakan untuk menjalankan komputer/laptop dan alat dan/atau infrastruktur komunikasi yang digunakan untuk menghubungkan sistem IVPNT. Gambar 2 merupakan ilustrasi dari skenario implementasi IVPNT :



Gambar 2. Skenario IVPNT

Pegawai dari kota A dengan IP *address* 193.111.55.20 dengan eth *trusted* A 193.111.55.10, dapat terhubung secara privat dengan Pegawai dari kota B dengan IP *address* 192.10.2.10 dengan eth *trusted* B 192.10.2.5 melalui IP VPN *tunnel* yang dibangun ,yaitu 10.99.99.1 untuk IVPNT *gateway* A dan 10.99.99.2 untuk IVPNT *gateway* B. Hasil yang diinginkan adalah pegawai dari kota A dapat terhubung dengan pegawai kota B melalui *tunnel* yang telah dibangun, komunikasi yang terjadi adalah *gateway-to-gateway.*

4. IMPLEMENTASI DAN ANALISIS

Pada tahap ini meliputi pengujian performa dan pengujian keamanan. Pengujian performa dilakukan untuk menguji waktu rata-rata proses inisialisasi yang terjadi saat terbentuknya koneksi antara dua pihak yang akan berkomunikasi dan waktu rata-rata transmisi data. Transmisi data dilakukan dengan cara mengirimkan paket data *ping* ke alamat IP privat tujuan. Ukuran data sebesar 65507 *bytes* yaitu ukuran maksimal untuk paket *ping*. Percobaan dilakukan sebanyak 30 kali. Setiap percobaan

dilakukan pengambilan durasi waktu proses. Hal tersebut merujuk pada ukuran sampel yang layak dalam penelitian antara 30 sampai dengan 500. Waktu rata-rata proses inisialisasi yang dibutuhkan adalah 1.357278s. Pengujian durasi waktu proses transmisi data dilakukan untuk beberapa ukuran paket data dalam 30 *sequence*. Dengan ukuran data dari 10 kb – 60 kb, waktu rata-rata yang dibutuhkan adalah 29.218680 s.

Pengujian keamanan trafik data dilakukan untuk membuktikan apakah lalu-lintas paket data yang melalui jaringan privat terlindungi/dapat dipahami atau tidak dapat dipahami, bila *tunnel* VPN telah terbentuk. Pengujian keamanan trafik data menggunakan *Wireshark* sebagai *tool* aplikasi untuk melakukan *sniffer* paket data pada jaringan.

Pengujian tersebut dilakukan dengan cara melakukan *capture* (penangkapan) terhadap paket data yang melalui jaringan privat. Salah satu contoh sesi yang di-*capture* yaitu pada saat pengiriman data. Jika jaringan publik menggunakan layanan IVPNT, maka terbentuk saluran privat sehingga data yang melaluinya akan terlindungi. Dengan kata lain, bahwa jika pihak yang tidak berwenang melakukan *sniffer* pada jaringan IVPNT, maka data paket yang ditransmisikan tidak dapat dipahami.

Berdasarkan desain *security requirement*, pada perancangan sistem IVPNT ini, keamanan yang dibangun masih terbatas pada :

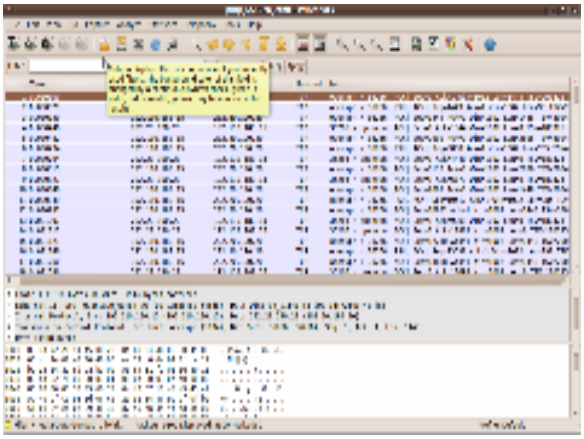
a. Transmisi Data

Menggunakan protokol SSL dan IPSec, sehingga diperlukan paket OpenVPN dan OpenSWAN yang diinstalasi ke dalam sistem IVPNT.

b. Keamanan Data

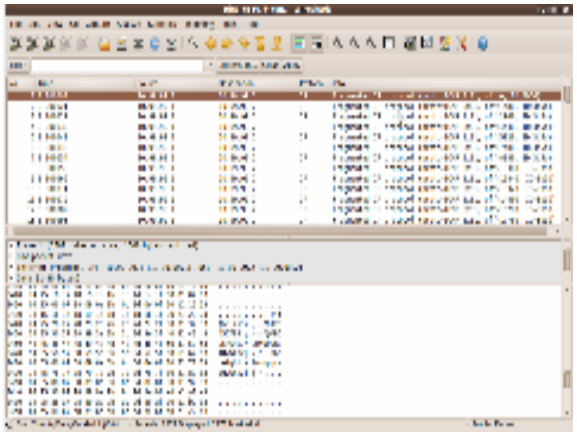
Menggunakan algoritma enkripsi, otentikasi, dan pertukaran kunci sesuai dengan yang disediakan oleh paket OpenVPN dan OpenSWAN.

Sampel hasil uji keamanan trafik data dengan melakukan *sniffing* jaringan publik menggunakan *Wireshark* pada jalur eth *untrusted* dapat dilihat pada Gambar 3 dan 4, sedangkan sampel hasil uji keamanan trafik data dengan melakukan *sniffing* jaringan IVPNT menggunakan tools yang sama dapat dilihat pada Gambar 5. Gambar di bawah ini adalah hasil pengujian keamanan trafik data pada jaringan eth *untrusted* :



Gambar 3. Hasil Uji Keamanan pada Jaringan eth *Untrusted* (Tampilan Awal)

Gambar 4. Hasil Uji Keamanan pada Jaringan eth *Untrusted* (Isi Data)



Gambar 5. Hasil Uji Keamanan pada Jaringan *Tunnel*

Berdasarkan hasil pengujian keamanan trafik data pada kedua jaringan yang berbeda (eth *untrusted* dan *tunnel*), dapat dianalisa bahwa paket data yang melalui jaringan publik eth *untrusted* terlindungi. Pada Gambar 3 dapat dilihat bahwa informasi tentang pengiriman data tidak dapat dilihat, yang dilihat hanyalah data tersebut diamankan oleh VPN. Pada Gambar 4, data juga terlihat acak sehingga informasi yang ditransmisikan tidak dipahami oleh siapapun. Gambar 5 memperlihatkan saat paket data melalui jaringan *tunnel,* informasi tentang pengiriman data dapat dilihat dan isi data juga terbaca, hal ini disebabkan VPN melindungi pesan dengan membuat *tunnel*.

5. KESIMPULAN

Berdasarkan hasil penelitian, maka dapat disimpulkan hal-hal sebagai berikut :

1. Aplikasi IVPNT menggunakan protokol SSL dan IPSec untuk menghubungkan dua *gateway* melalui jaringan publik dapat beroperasi sesuai dengan desain;
2. Berdasarkan hasil pengujian performa, didapatkan rata-rata lamanya waktu untuk proses inisialisasi sebesar 1.357278 s;
3. Hasil pengujian keamanan trafik data pada jaringan IVPNT menggunakan protokol SSL dan IPSec, telah terbukti terlindungi.

Referensi

[1] Alshamsi, AbdelNasir & Takamichi Saito, (2005), "A Technical Comparison of IPSec and SSL," *Proc. of the 19th International Conference on Advanced Information Networking and Applications*, vol. 2.

[2] Degabriele, Jean Paul & Kenneth G. Paterson, (2007), "Attacking the IPSec Standards in Encryption-only Configurations, " *Proc. of the 2007 IEEE Symposium on Security and Privacy*.

[3] Doraswamy, Naganand, Dan Harkins. 2003. *IPSec : The New Security for and Integrating Virtual Private Networks*. PACKT Publishing.

[4] Hosner, Charlie. 2004. *OpenVPN and the SSL VPN Revolution*. Sans Institute.

[5] Murhammer, Martin W. et al. 1998. *TCP/IP Tutorial and Technical Overview*. USA : IBM.

[6] Stallings, William. 2005. *Cryptography and Network security Principles and Practices 4 th edition.* USA : Prentice Hall.

[7] Steinberg, Joseph & Timothy Speed. 2005. *SSL VPN : Understanding,evaluating, and planning secure, web-based remote access.* Birmingham : Packt Publishing Ltd.