BAB 1

PENDAHULUAN

1.1 Latar Belakang Masalah

Pertukaran informasi atau komunikasi antar entitas dapat dilakukan dengan cepat dan mudah seiring dengan perkembangan Ilmu Pengetahuan dan Teknologi (IPTEK). Suatu perusahaan dapat menghubungkan jaringan komputer di kantor pusat dengan kantor cabangnya yang terletak saling berjauhan melalui internet, selain itu juga bisa memberikan otoritas kepada pegawainya untuk mengakses jaringan internal perusahaan melalui jaringan internet yang dikenal dengan istilah *remote access* (Frankel S. e., 2005). Salah satu aspek yang perlu menjadi perhatian adalah keamanan informasi yang menjadi aset suatu perusahaan. Ketika melakukan transmisi informasi melalui jaringan internet, terdapat potensi kerawanan seperti *eavesdropping*, *monitoring*, modifikasi atau pengubahan informasi oleh pihak yang tidak memiliki otoritas (Stallings, 2007). Solusi yang dapat digunakan untuk mengatasi kerawanan tersebut adalah dengan menggunakan *Virtual Private Network* (VPN). Suatu perusahaan lebih memilih untuk menggunakan VPN dibanding harus menggunakan *leased line* atau jalur khusus suatu *provider*. Selain lebih hemat biaya, di dalam VPN juga menyediakan fitur keamanan seperti enkripsi dan otentikasi (Lucas, et al., 2006).

Pada penelitian ini, penulis akan melakukan pembuatan prototipe VPN *gateway* yang bekerja pada *layer* 4 OSI *model* (SSL VPN). VPN berbasis perangkat keras memiliki beberapa kelebihan yaitu dapat

digunakan di berbagai sistem operasi PC *user* (*platform independent*) dan lebih stabil karena dibangun terpisah dari PC, selain itu juga memiliki fitur tambahan seperti *inbuilt firewall* dan *routing* internet (Cisco, 2001). SSL VPN dipilih karena melihat dari sudut pandang fleksibilitas atau kemudahan konfigurasi, kompatibilitas dengan *Network Address Translation* (NAT), dan tidak bermasalah dengan aturan *firewall* (Frankel, et al., 2008; OpenVPN, 2002-2015). Perangkat keras yang digunakan adalah SBC *Raspberry Pi* 3 Model B+ dengan aplikasi inti OpenVPN yang akan dimodifikasi dengan cara mengimplementasikan algoritma *stream cipher* Rabbit sebagai salah satu alternatif pilihan TLS *ciphersuites*nya. Oleh karena itu, pada penelitian ini penulis akan berusaha mengimplementasikan suatu algoritma yang tidak hanya memiliki kekuatan kriptografis yang baik namun juga memiliki performa yang secara umum lebih baik dibanding algoritma stream chiper lainnya yaitu Algoritma Rabbit (Boesgard, 2003).

Algoritma *stream cipher* Rabbit didesain sebagai algoritma yang efisien dalam implementasi pada *software*. Algoritma Rabbit didesain dan telah dipelajari secara ekstensif oleh para pakar kriptografi dari Cryptico A/S dengan memperhatikan berbagai jenis metode kriptanalisa (Rijmen, 2003). Algoritma ini juga telah distandarisasi oleh IETF melalui RFC 4503. Dari hasil pengujian serta analisa yang dilakukan, algoritma Rabbit terbukti kuat secara kriptografis dan resistan terhadap metode-metode kriptanalisa yang ada (Boesgard, 2003).

Hasil modifikasi OpenVPN pada penelitian ini selanjutnya disebut dengan OpenVPN-Rabbit atau OpenVPN-R untuk kemudian diimplementasikan pada SBC *Raspberry Pi* 3 Model B+. Konektivitas prototipe VPN *gateway* ini yang selanjutnya disebut AR6000 menggunakan dua *network interfaces*, yaitu satu *trusted network* untuk konektivitas ke PC milik *user* dan satu *untrusted network* untuk konektivitas ke VPN *relay server*. Dengan prototipe ini, *user* akan diberikan kemudahan untuk melakukan *remote access* ke dalam jaringan internalnya dan dapat melakukan *request* ke halaman *web* melalui jaringan publik secara aman.

Mengapa harus menggunakan prototipe AR6000? karena ada beberapa hal yang menjadi alasan, yaitu sesuai dengan identifikasi permasalahan sebelumnya yang diharapkan perangkat ini dapat menjadi lebih simple, flexible, manageable, dan secure.

1.2 Rumusan Permasalahan

Melihat dari latar belakang masalah yang telah diungkapkan sebelumnya, maka dirumuskan beberapa permasalahan dalam penelitian ini, yaitu:

1. Apakah Prototipe VPN Gateway berbasis SBC Raspberry Pi 3 Model B+ dengan OpenVPN-R dapat menjadi salah satu alternative yang menjamin keamanan dalam mengakses ke sumber daya atau layanan yang ada di dalam jaringan internal melalui jaringan internet (*remote access*)?
2. Apakah Algoritma Rabbit lebih baik daripada algoritma yang lain untuk OpenVPN?

3. Bagaimana mengimplementasi dan mengevaluasi OpenVPN-R pada SBC *Raspberry Pi 3 Model B+* untuk menjadi sebuah prototipe VPN *gateway*?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengevaluasi perbandingan antara VPN berbentuk prototipe dengan VPN yang sudah ada berbasis Software.
2. Melakukan perbandingan alagoritma Rabbit dengan Algoritma yang sudah ada pada OpenVPN yaitu AES-256, Camellia-256, 3DES dan SEED.
3. Mengembangkan dan mengevaluasi suatu prototipe VPN *gateway* berbasis SBC *Raspberry Pi 3 Model B+* dengan mengimplementasikan OpenVPN-R sebagai aplikasi intinya.

1.4 Manfaat Penelitian

Manfaat yang diharapkan dapat diperoleh dari penelitian ini adalah:

1. Prototipe VPN *gateway* dapat menjadi salah satu perangkat alternatif untuk mengamankan transaksi data melalui jaringan publik, baik melakukan *remote access* ke jaringan internal atau melakukan *request* ke halaman *web*.
2. Terciptanya Kemudahan dalam melakukan *remote access* yang aman dengan hanya menggunakan perangkat VPN gateway (*portable*).

3. Organisasi dan Perusahaan dapat memberikan otoritas kepada pegawainya untuk mengakses ke sumber daya atau layanan yang ada di dalam jaringan internal melalui jaringan internet (*remote access*);
4. Terciptanya suatu perangkat prototipe yang dapat menjamin keamanan transmisi informasi melalui jaringan internet.

1.5 Ruang Lingkup

Terkait dengan keterbatasan waktu dan sumber daya yang dimiliki penulis serta agar penelitian dapat dilakukan lebih mendalam dan tidak meluas, maka pembahasan hanya difokuskan pada hal-hal berikut:

1. Teknologi VPN yang digunakan yaitu SSL VPN dengan aplikasi inti OpenVPN yang dimodifikasi dengan menambahkan algoritma *stream cipher* Rabbit sebagai salah satu alternatif pilihan *Transport Layer Security* (TLS) *ciphersuites*nya.
2. Menggunakan SBC *Raspberry Pi 3 Model B+* sebagai perangkat keras utama untuk pembuatan prototipe VPN *gateway*.
3. Konektivitas dari SBC ke PC menggunakan *crossover cable* dengan alamat IP statik dan konektivitas dari SBC ke VPN *relay server* menggunakan USB *Wi-Fi dongle.*
4. Menggunakan VPN *relay server* agar penambahan *node* atau aktivasi *personal* VPN *gateway* baru lebih mudah dan fleksibel.
5. Secara *default,* konfigurasi *routing*, sertifikat kunci, dan konfigurasi NAT sudah *embedded* di dalam prototipe VPN *gateway*.

6. *Key-pair generation, certificate creation,* dan *certificate and key-pair distribution* dilakukan di awal pembuatan perangkat secara *offline*, sehingga tidak menyediakan mekanisme untuk mentransfer sertifikat kunci secara *online* ketika *user* menghendaki perubahan VPN *relay server* yang akan dituju.
7. Diagram UML yang akan digunakan untuk pemodelan rancangan sistem adalah *use case diagram*, *activity diagram,* dan *sequence diagram*.
8. Menggunakan aplikasi *Wireshark* untuk melakukan *monitoring* pada jaringan yang menggunakan prototipe VPN *gateway*.

1.6 Rencana Jadwal Penyelesaian

NO	KEGIATAN	2017																										2018											
		Mei				Juni				Juli				Agustus				September				Oktober				November				Desember				Januari				Februari				Maret			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	**Tahap 1: Pengajuan Judul dan Perancangan Proposal Penelitian Tesis**																																											
	a. Penyusunan Proposal																																											
	b. Pengajuan Proposal																																											
	c. Seminar proposal																																											
	d. Perbaikan Proposal																																											
2	**Tahap 2: Bimbingan penulisan dan penelitian Tesis**																																											
	a. Studi Literatur																																											
	b. Pengumpulan Data																																											
	c. Analisis Kebutuhan																																											
	d. Perancangan Software dan Hardware																																											
	e. Coding dan Implementasi																																											
	f. Pengujian dan Analisis																																											
	g. Seminar 80% Tesis																																											
	h. Perbaikan hHasil Seminar 80%																																											
	i. Perumusan Kesimpulan																																											
3	**Tahap 3: Pengumpulan dan Sidang Penelitian Tesis**																																											
	a. Pengumpulan Tesis																																											
	b. Sidang Tesis																																											
	c. Revisi Tesis																																											