IMPLEMENTASI VPN BERBASIS IPSEC
DENGAN LINUX FREES/WAN

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Mencapai Gelar Sarjana Teknik Jurusan Elektro
Universitas Muhammadiyah Surakarta

Disusun Oleh :

IQBAL AMRULLAH

D 400 020 103

FAKULTAS TEKNIK JURUSAN TEKNIK ELEKTRO

UNIVERSITAS MUHAMMADIYAH SURAKARTA

2008

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dari cara pandang jaringan, salah satu masalah jaringan internet (IP *public*) adalah tidak mempunyai dukungan yang baik terhadap keamanan. Internet dahulu didesain oleh perguruan - perguruan tinggi sebagai sebuah jaringan terbuka dimana pengguna dapat mengakses, berbagi, dan menambah informasi semudah mungkin. Sebuah cara harus ditemukan untuk mengamankan sebuah jaringan publik tanpa melanggar sifat-sifat yang telah ada. Sesungguhnya sebuah jawaban ideal harus menyediakan tidak saja tingkat keamanan tinggi tetapi juga keamanan yang sedemikian rupa sehingga pengguna dapat dengan mudah mengakses, mengubah, dan berbagi lebih banyak informasi, tidak lupa, dibawah kondisi - kondisi yang secara hati - hati dikendalikan dan dipelihara.

VPN muncul untuk mengatasi persoalan tersebut. Secara umum, vpn (*virtual private network*) adalah sebuah proses dimana jaringan umum (*public network / internet*) diamankan untuk mengfungsikannya sebagaimana jaringan privat (*private network*). Sebuah vpn tidak didefinisikan oleh rangkaian khusus atau rute, tetapi didefinisikan oleh mekanisme keamanan dan prosedur - prosedur yang hanya mengizinkan pengguna - pengguna yang ditunjuk akses ke vpn dan informasi yang mengalir melaluinya.

Untuk menjawab permasalahan diatas, maka penulis dalam tugas akhir ini akan mengimplementasikan vpn berbasis *ipsec* (*IP security*) yang bekerja pada *network*

layer model referensi OSI (*Open System Interconnection*) dengan menggunakan sistem operasi Debian GNU / Linux 3.0 dan perangkat lunak untuk manajemen kunci memakai FreeS/WAN.

1.2 Perumusan Masalah

Dari latar belakang masalah yang telah diuraikan diatas, maka dapat dirumuskan beberapa masalah :

1. Bagaimana membangun jaringan intranet atau privat yang mempunyai dukungan tidak saja tingkat keamanan tinggi tetapi juga keamanan yang sedemikian rupa sehingga pengguna dapat dengan mudah mengakses, mengubah, dan berbagi lebih banyak informasi, tidak lupa, dibawah kondisi - kondisi yang secara hati - hati dikendalikan dan dipelihara.
2. Bagaimana mengimplementasikan vpn (*virtual private network*) berbasis *ipsec* (*IP security*) pada jaringan intranet yang mendukung tingkat keamanan yang tinggi.

1.3 Batasan Masalah

Perancangan sistem ini terdapat batasan-batasan masalah yang meliputi :

1. Sistem dibangun menggunakan sistem operasi Debian GNU/Linux 3.0 dengan kernel linux 2.4.18.
2. *Software* yang digunakan untuk implementasi *ipsec* pada Debian GNU/Linux 3.0 yaitu FreeS/WAN (*Free Secure Wide Area Network*).
3. VPN (*Virtual Private Network*) dibangun pada *layer* 3 (*network layer*).
4. VPN (*Virtual Private Network*) diimplementasikan dengan menggunakan *IP version 4* (*ipv4*).

5. Menggunakan algoritma MD5 utuk authentikasi.
6. Menggunakan algoritma 3DES untuk enkripsi.
7. Metode *authentikasi* IKE (*Internet Key E*xchange) menggunakan algoritma enkripsi RSA (PKCS).
8. Tidak membahas kriptografi secara detail.
9. Simulasi VPN (*Virtual Private Network*) dilakukan secara lokal / *offline*.
10. Analisa jaringan vpn menggunakan dua *tool monitoring* jaringan, yaitu *ping* dan *tcpdump*..

1.4 Tujuan Penelitian

Tugas Akhir ini bertujuan untuk mengimplementasikan vpn (*virtual private network*) berbasis *ipsec* (*IP security*) dengan Linux FreeS/WAN.

1.5 Manfaat Penelitian

Manfaat yang bisa diambil dari Tugas Akhir ini antara lain :

1. Sebagai sarana pembelajaran bagi penulis dan pembaca tentang keamanan jaringan komputer dan pembangunan sistem.
2. Memberikan sebuah solusi dalam pertukaran data atau informasi yang terjamin keamanannya.

1.6 Tinjauan Pustaka

Dalam penyusunan tugas akhir ini, penulis mengambil referensi dari sebuah buku yang dibuat oleh Aris Wendy Sunyoto dan Achmad Ramadhana dengan judul Membangun VPN Linux Secara Cepat, diterbitkan oleh Andi Publisher Yogyakarta tahun 2005. Buku ini berisi mengenai desain dan instalasi vpn berbasis linux. VPN

yang dibahas dalam buku ini adalah FreeS/WAN yang dikembangkan dari *ipsec* yang menggunakan authentikasi dan enkripsi.

Pembahasan dalam buku membangun VPN Linux secara cepat berkisar pada koneksitas sistem operasi Linux dengan Linux. Suatu sistem akan bernilai tinggi apabila dapat diterapkan diseluruh *platform* sistem operasi, tak terkecuali *ipsec*. Maka dari itu dalam penyusunan tugas akhir ini, penulis menambahkan konfigurasi agar *ipsec* bisa berinteraksi dengan sistem operasi Windows, dalam hal ini penulis menggunakan Windows XP. Dengan memakai *script* dari Marcus Muller, interaksi *ipsec* pada FreeS/WAN dengan Windows XP bisa dijalankan.

1.7 Sistematika Penulisan

Tugas Akhir ini nantinya disusun dengan sistematika penulisan sebagai berikut :

BAB I : PENDAHULUAN

Merupakan bab pendahuluan yang menguraikan latar belakang masalah, rumusan masalah, pembatasan masalah, tujuan, dan sistematika penulisan.

BAB II : LANDASAN TEORI

Membahas Tinjauan Penelitian Terdahulu, Model Referensi OSI, Kriptografi, IPSec, Implementasi IPSec, Cara Kerja IPSec.

BAB III : PERANCANGAN SISTEM

Membahas langkah dari proses perancangan implementasi vpn berbasis IPSec dengan Linux FreeS/WAN beserta implementasi perancangan sistem.

BAB IV : PENGUJIAN DAN ANALISA

Menunjukkan hasil pengujian dari perancangan implementasi vpn berbasis *ipsec* dengan Linux FreeS/WAN disertai dengan analisa sehingga didapatkan bukti kuat dari hipotesis yang dilakukan.

BAB V : PENUTUP

Menguraikan kesimpulan Tugas Akhir dan saran - saran sebagai bahan pertimbangan untuk pengembangan penelitian selanjutnya.

DAFTAR PUSTAKA

LAMPIRAN