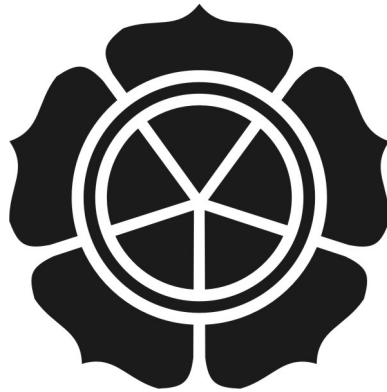


**PENERAPAN OPENSWAN UNTUK KEAMANAN TRANSMISI DATA
DI PT.TIME EXCELINDO**

SKRIPSI

Untuk memenuhi sebagian persyaratan
Mencapai derajat Sarjana S1
Pada jurusan Teknik Informatika



disusun oleh

Febtian Anas Raharjo

07.11.1561

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2011**

PERSETUJUAN

SKRIPSI

**Penerapan Openswan Untuk Keamanan Transmisi Data Di
PT. Time Excelindo**


yang dipersiapkan dan disusun oleh

Febtian Anas Raharjo

07.11.1561

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 03 November 2010

Dosen Pembimbing,



Melwin Syafrizal, S.Kom, M.Eng
NIK. 190302105

PENGESAHAN

SKRIPSI

**Penerapan Openswan Untuk Keamanan Transmisi Data Di PT. Time
Excelindo**

yang dipersiapkan dan disusun oleh

Febtian Anas Raharjo

07.11.1561

telah dipertahankan di depan Dewan Penguji
pada tanggal 22 Februari 2011

Susunan Dewan Penguji

Nama Penguji

**Sudarmawan, M.T.
NIK. 190302035**

**Erik Hadi Saputra, S.Kom, M.Eng.
NIK. 190302107**

**Emha Taufik Luthfi, ST, M.Kom
NIK. 190302125**

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 22 Februari 2011



KETUA STMIK AMIKOM YOGYAKARTA

**Prof. Dr. M. Suyanto, M.M.
NIK. 190302001**

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri, dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

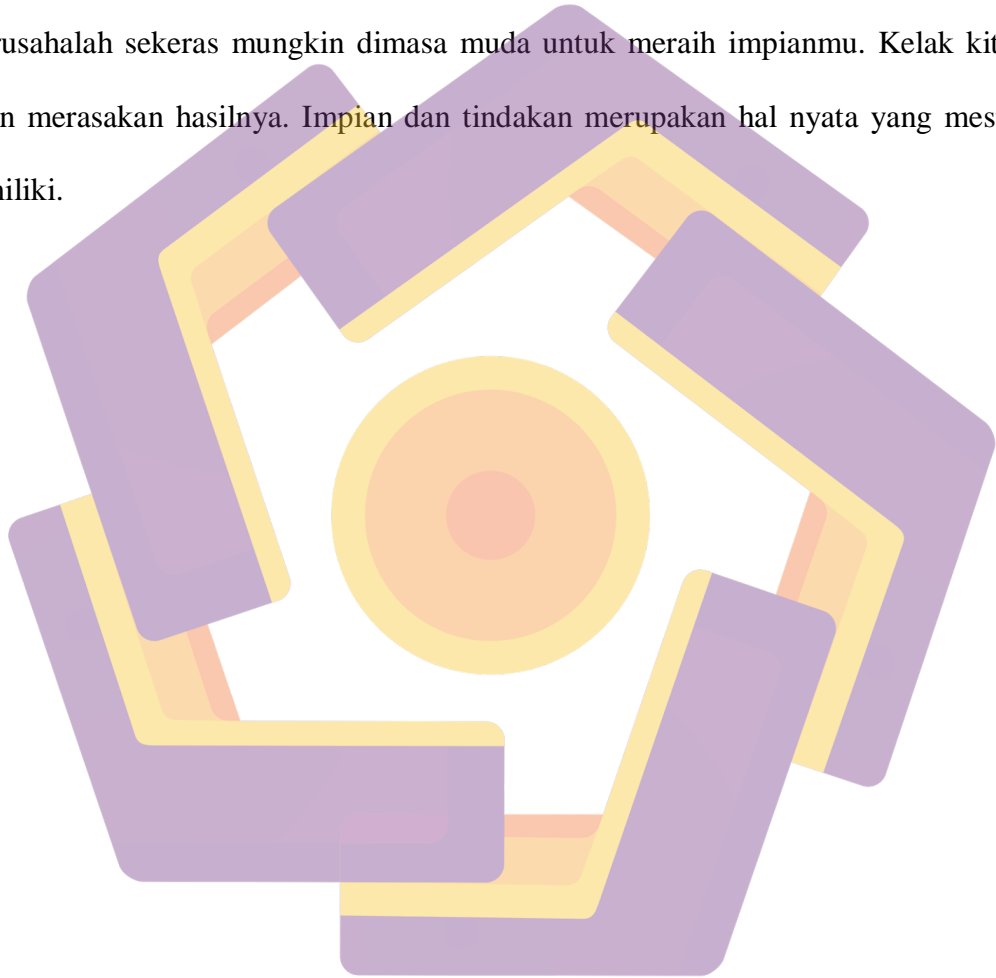
Yogyakarta, 25 Februari 2011

Febtian Anas Raharjo
NIM. 07.11.1561

MOTTO

“Waktu merupakan kesempatan, jangan sia-siakan waktu yang kita miliki”

Jika kita yakin akan impian kita, janganlah kita sia-siakan waktu yang kita miliki. Berusahalah sekeras mungkin dimasa muda untuk meraih impianmu. Kelak kita akan merasakan hasilnya. Impian dan tindakan merupakan hal nyata yang mesti dimiliki.



HALAMAN PERSEMBAHAN

Kudedikasikan Skripsi ini buat :

- ✚ Allah SWT yang senantiasa memberikan rahmad dan hidayahnya kepada penulis dengan kelancaran yang selama ini diberikan sehingga dapat menyelesaikan Skripsi ini.
- ✚ Nabi Muhammad SAW, yang senantiasa memberikan safa'atnya dan memberikan teladan yang baik kepada seluruh umatnya.
- ✚ Bapak dan ibu yang tersayang yang selalu berdoa tanpa henti untuk harapan akan keberhasilan anak-anaknya.
- ✚ Kakakku Supraja Harjawinata dan adikku Isti Arum Sari.
- ✚ Gia Riefti Cressenda, inspirasi karir masa depanku.
- ✚ Teman-teman momohum (Dian Mitra Widiyansah, Tejo dan Dody)

KATA PENGANTAR

Assalamu'alaikum Wr. Wb

Dengan memanjatkan puji syukur kehadiran Allah SWT. Yang telah melimpahkan rahmat dan hidayahnya serta keberhasilan yang selalu diberikannya, sehingga akhirnya dapat menyelesaikan skripsi ini dengan baik. Teriring dengan Sholawat dan salam yang tetap tercurahkan kepada Nabi Muhammad SAW, yang membawa petunjuk dan suri tauladan untuk kebaikan umatnya di dunia dan akhirat. Amin.

Tugas akhir berupa skripsi ini disusun sebagai salah satu syarat untuk mendapatkan gelar Sarjana (S1) pada jurusan Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer, AMIKOM Yogyakarta. Adapun judul Skripsi ini adalah : Penerapan Openswan Untuk Keamanan Transmisi Data DI PT. Time Excelindo.

Dalam menyelesaikan Skripsi ini, penulis banyak mendapatkan bantuan serta bimbingan dari berbagai pihak, baik secara langsung maupun tidak langsung. Oleh karena itu dalam kesempatan ini dengan segala kerendahan hati dan rasa hormat, penulis menyampaikan rasa terimakasih kepada :

1. Bapak Melwin Syafrizal, Mkom, selaku pembimbing dan Instruktur saya di STMIK AMIKOM Yogyakarta.
2. Bapak Sudarmawan, selaku Ketua Jurusan Teknik Informatika.
3. Rekan-rekan saya di PT. Time Excelindo. Prasetyo, Andi, Tafaul.
4. Karyawan PT. Time Excelindo yang telah memberikan kesempatan dan bantuannya, terimakasih atas kerjasamanya.

5. Teman-teman hebatku. Tejo, Dody, Dian.
6. Orang-orang yang sukses sebagai inspirasiku.
7. Serta semua pihak yang tidak dapat disebut satu persatu.
8. Teman-temanku, masa depan masih panjang, ayo tetap berjuang.

Penulis menyadari bahwa dalam penelitian Skripsi ini masih terdapat kekurangan dalam berbagai hal. Oleh karena itu, penulis mengharapkan bimbingan, saran dan kritik yang dapat membangun guna menyempurnakan Skripsi ini sehingga Skripsi ini telah tersusun ini dapat memberikan manfaat.

Wassalamu'alaikum, Wr. Wb.

Yogyakarta, 24 Februari 2011

Penulis

Febtian Anas Raharjo
NIM. 07.11.1561

DAFTAR ISI

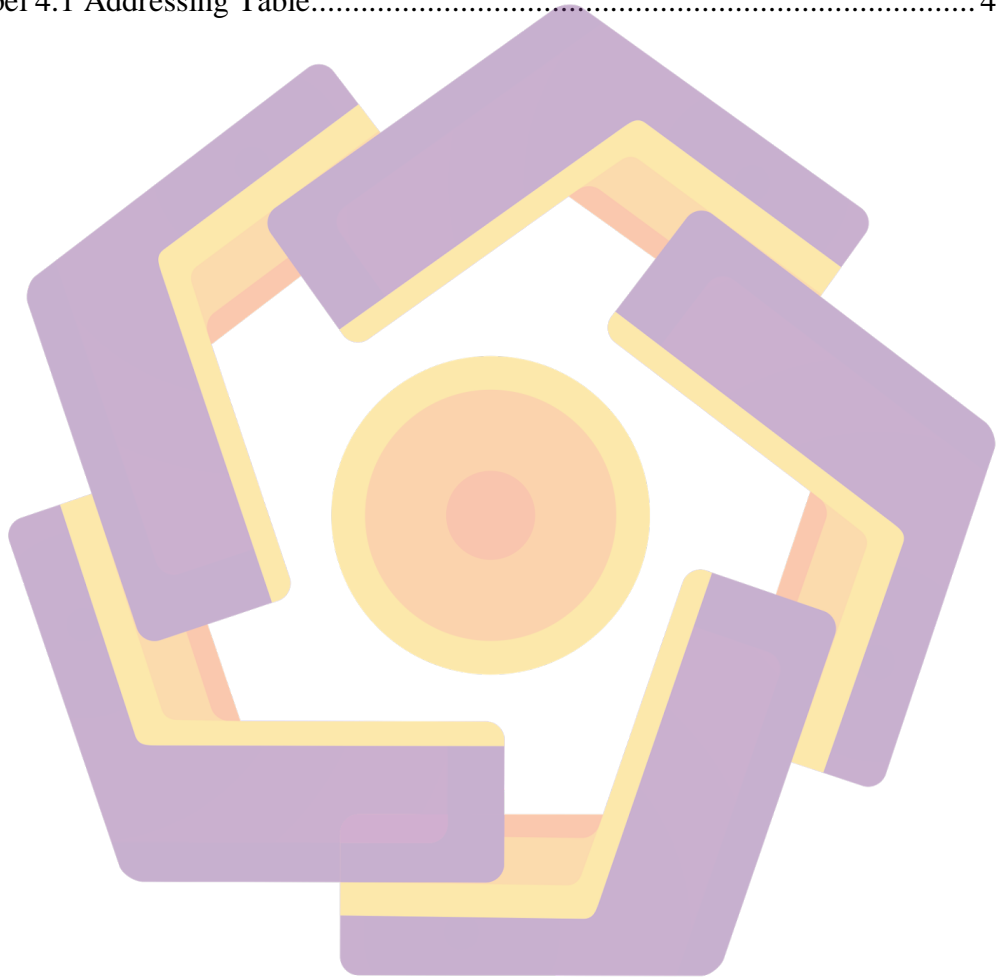
Judul.....	i
Lembar Persetujuan	ii
Lembar Pengesahan	iii
PERNYATAAN	iv
MOTTO.....	v
HALAMAN PERSEMBAHAN.....	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR GAMBAR.....	xiii
ABSTRACT	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Metode Pengumpulan Data.....	4
1.7 Sistematika Penulisan Laporan	5
BAB II LANDASAN TEORI	7
2.1 Tinjauan Pustaka	7
2.1.1 Kelebihan Sistem.....	7
2.1.2 Kekurangan Sistem.....	8
2.2 Virtual Private Network (VPN)	9
2.2.1 Implementasi Remote Access VPN	10
2.2.2 Implementasi Site-to-Site VPN.....	10
2.3 Openswan.....	11
2.3.1 Protokol Authentication Header (AH).....	12
2.3.2 Protokol Encapsulating Security Payload (ESP)	13
2.3.3 Domain of Interpretation (DOI)	14
2.3.4 Key Management	14

2.3.5	Security Association (SA)	15
2.3.5.1	Transport Mode.....	15
2.3.5.2	Tunnel Mode	15
2.4	Teknologi Enkripsi	16
2.4.1	Algoritma Asimetris	17
2.4.2	Algoritma Simetris	18
2.4.3	Cara Kerja Enkripsi di IPSec	19
2.5	Fitur – Fitur IPSec	20
2.6	Transmisi Data	22
2.6.1	Gelombang Radio	22
2.6.2	Prinsip-Prinsip Antena.....	23
2.6.2.1	Line of Sight	23
2.6.2.2	Fresnel Zone.....	23
2.6.2.3	Hambatan	24
2.6.2.4	Penguatan antena.....	24
2.6.2.5	Intentional radiator	24
2.6.2.6	Equivalent Isotropically Radiated Power (EIRP)	24
2.6.3	Perangkat Infrastruktur WLAN.....	25
2.6.3.1	Root Mode	25
2.6.3.2	Bridge Mode	26
2.6.3.3	Repeater Mode	26
BAB III ANALISIS DAN PERANCANGAN SISTEM		28
3.1	Gambaran Umum	28
3.2.1	Profil Perusahaan.....	29
3.2	Analisis Sistem.....	30
3.2.1	Analisis Keamanan Jaringan.....	31
3.2.1.1	Checking IP Range	31
3.2.1.2	Scanning Port	32
3.2.1.3	DoS.....	34
3.2.1.4	Man in the middle attack	35
3.2.1.4.1	<i>Root Compromise</i>	35

3.2.1.4.2	File Modification.....	36
3.2.1.5	Solusi	38
3.2.2	Analisis Kebutuhan Sistem.....	39
3.2.2.1	Kebutuhan Perangkat Keras.....	39
3.2.2.2	Kebutuhan Perangkat Lunak.....	40
3.2.3	Analisis Kelayakan Sistem	40
3.2.3.1	Kelayakan Teknologi.....	40
3.2.3.2	Kelayakan Hukum.....	41
3.2.3.3	Kelayakan Operasional.....	41
3.3	Perancangan Sistem jaringan VPN	41
BAB IV IMPLEMENTASI DAN PEMBAHASAN.....		44
4.1	Implementasi VPN	44
4.2	Remote dan Instalasi.....	44
4.3	Konfigurasi VPN.....	47
4.4	Pembahasan.....	53
4.5	Keamanan Data	54
4.5.1	Setelah Menggunakan VPN.....	54
BAB V PENUTUP		56
5.1	Kesimpulan	56
5.2	Saran.....	56
DAFTAR PUSTAKA		58

DAFTAR TABEL

Tabel 3.1 Kategori Layanan VPN	39
Tabel 3.2 Spesifikasi Hardware.....	40
Tabel 4.1 Addressing Table.....	44



DAFTAR GAMBAR

Gambar 2.0 Skema jaringan VPN	9
Gambar 2.1 IPsec Framework	11
Gambar 2.2 Arsitektur IPsec.....	12
Gambar 2.3 Paket IP Sebelum memasukkan AH.....	12
Gambar 2.4 Authentication Header.....	13
Gambar 2.5 Encapsulation Security Payload	13
Gambar 2.6 Transport dan tunnel mode protokol IPsec	16
Gambar 2.7 Asimetris	18
Gambar 2.8 Skema enkripsi	19
Gambar 2.9 Line of Sight dan Fresnel Zone	23
Gambar 2.10 Root mode	26
Gambar 2.11 Bridge mode	26
Gambar 2.12 Repeater mode.....	27
Gambar 3.1 Jaringan PT. Time Excelindo	29
Gambar 3.2 Range IP Public	32
Gambar 3.3 Host yang aktif	33
Gambar 3.4 Port Aktif.....	33
Gambar 3.5 Flood packet	34
Gambar 3.6 Koneksi Down.....	34
Gambar 3.7 Capturing akses device	35
Gambar 3.8 Radio	36
Gambar 3.11 Kinerja VPN dan Man in The Middle Attack	38
Gambar 3.12 Skema jaringan VPN.....	42
Gambar 3.13 Tunnel VPN Site-to-Site	43
Gambar 4.2 Remote VPN.....	45
Gambar 4.3 Remote Menggunakan Putty	45
Gambar 4.4 Openswan Running.....	46
Gambar 4.5 Openswan Restart.....	46
Gambar 4.6 Openswan Stop.....	47
Gambar 4.8 Forwarding	47
Gambar 4.7 PSK.....	48
Gambar 4.9 Tunnel	53
Gambar 4.13 Request Time Out.....	55

INTISARI

Keamanan data pada komunikasi melalui jaringan komputer sekarang telah menjadi sebuah persoalan penting karena jaringan internet merupakan lokasi yang sangat rentan terhadap kemungkinan hacking dan data-sniffing. Salah satu cara untuk membangun keamanan komunikasi data dalam jaringan internet adalah dengan menggunakan jaringan Virtual Private Network (VPN). Dengan VPN, paket yang akan dikirim terlebih dahulu dienkripsi sehingga data tidak akan dapat dengan mudah diketahui walaupun data telah disadap.

Penggunaan Openswan merupakan sistem keamanan yang membuat jalur pribadi atau virtual yang melewati jalur yang tidak dapat dipercaya, inilah yang disebut virtual dimana jalur virtual yang terbuat ini tidak nyata dan penggunaan protokol IPsec. Dan kunci untuk membuka enkripsi hanya diketahui oleh VPN Server dan Client yang terhubung. Enkripsi dan dekripsi menyebabkan data tidak dapat dimodifikasi dan dibaca sehingga integritas data terjamin.

PT. Time Excelindo merupakan perusahaan yang bergerak di bidang internet service provider yang memberikan solusi teknologi yang efisien dan efektif kepada para konsumen, penggunaan Openswan merupakan pilihan aplikasi VPN dari sekian banyak sistem keamanan jaringan komputer agar konsumen tetap merasa aman ketika melakukan pertukaran data di internet.

Kata kunci : VPN, Openswan, Keamanan data, Integritas Data.

ABSTRACT

Data security on the communication through computer networks have now become an important issue because the Internet is a location that is very vulnerable to the possibility of hacking and data-sniffing. One way to build data communications security in the Internet network is to use Virtual Private Network (VPN). With VPN, the packet will be sent in advance will be encrypted so that data can't easily be found even though the data has been bugged.

The use Openswan is a security system that makes private line or virtual paths passing through that can not be trusted, this is called virtual in which virtual lane that made it's not real and use the IPsec protocol. And the key to unlock the encryption known only to the VPN Server and Client is connected. Encryption and decryption cause data can not be modified and read so that data integrity is guaranteed.

PT. Time Excelindo is a company engaged in the field of internet service providers that provide technology solutions that efficiently and effectively to consumers, the use Openswan VPN application is the choice of many computer network security system for consumers to feel safe when exchanging data on the internet.

Keywords: *VPN, Openswan, Data Security, Data Integrity.*