

Jurusan Teknik Informatika
Program Peminatan Jaringan Komputer
Skripsi Sarjana Komputer
Semester [Genap] tahun 2005/2006

**ANALISIS DAN PERANCANGAN WIDE AREA NETWORK
BERBASIS VIRTUAL PRIVATE NETWORK PADA
PT. HOTEL INDONESIA NATOUR**

Fachrina (0600667510)

Hendry Sulivian (0600673652)

Kelas / Kelompok : 08 PAT / 04

Abstrak

Tujuan penelitian ini adalah untuk merancang suatu jaringan yang menjamin keamanan pertukaran data antara kantor pusat dan cabang. Metode yang dipilih dan dilakukan adalah menganalisis kebutuhan dan sistem berjalan (bandwidth, koneksi jaringan pusat dan cabang), konfigurasi VPN, serta buku-buku kepustakaan yang membahas tentang teknologi informasi khususnya yang berhubungan dengan jaringan komputer. Pengujian juga akan kami lakukan untuk membandingkan hasil dari sistem yang diusulkan dengan sistem berjalan. VPN (*Virtual Private Network*) menggunakan teknologi IP Tunnel dengan protocol IP Sec merupakan salah satu jenis teknologi jaringan komputer yang dirancang dan diusulkan, dengan berbagai informasi yang telah didapatkan maka dapat dijelaskan mengenai rancangan hardware maupun software yang digunakan, konfigurasi VPN linux debian, keuntungan serta kelebihanannya. Dengan VPN berbasis sistem operasi Linux Debian yang free source memberikan fasilitas administrator jaringan dan keamanan (enkripsi) transaksi data pada perusahaan yang sangat tinggi.

Kata Kunci

Analisis, Jaringan, Virtual Private Network, Debian

PRAKATA

Dengan mengucapkan puji syukur kehadirat Allah SWT atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penulisan skripsi ini dengan berusaha semaksimal mungkin sesuai dengan kemampuan yang dimiliki.

Adapun tujuan dari pembuatan penulisan skripsi ini adalah sebagai salah satu syarat untuk mencapai kelulusan jenjang Strata-1 pada program pendidikan di Universitas Bina Nusantara.

Selama mengerjakan penulisan ilmiah ini penulis banyak mendapat bantuan berbagai pihak, dan dalam kesempatan ini penulis mengucapkan banyak-banyak terima kasih kepada :

1. Prof Dr. Drs. Gerardus Polla, M.App.Sc selaku Rektor Universitas Bina Nusantara.
2. Bapak Rusdianto Roestam Ir., M.Sc, Ph. selaku Dosen Pembimbing, yang telah menyediakan waktu serta banyak membantu, membimbing, mengarahkan, dan memberikan saran-saran kepada penulis.
3. Ibu, Bapak tercinta yang telah memberikan kasih sayang dan dukungan moril, materil serta doa-doanya selama ini.
4. Agus Poerwono yang selalu setia memberikan semangat, bantuan, dan kesabarannya selama ini.
5. Agung, Ipoel, Lian, Ajie, Desta, semua teman-teman serta rekan-rekan yang tidak bisa disebutkan satu persatu yang telah memberikan bantuan dan dukungan dalam penyelesaian penulisan skripsi ini.

Semoga Allah SWT melimpahkan segala rahmat dan karunia-Nya atas kebaikan Bapak/Ibu dan Saudara-saudara sekalian.

Dengan menyadari keterbatasan pengalaman kemampuan yang dimiliki penulis, sudah tentu terdapat kekurangan serta kemungkinan jauh dari sempurna, untuk itu tidak menutup diri dan mengharapkan adanya saran serta kritik dari berbagai pihak yang sifatnya membangun dan menyempurnakan penulisan skripsi ini.

Akhir kata semoga penulisan skripsi ini dapat memberikan manfaat bagi semua pihak yang bersangkutan, khususnya bagi penulis dan umumnya bagi para pembaca

Jakarta, Juni 2006

Penulis

DAFTAR ISI

| | |
|--|-------|
| Halaman Judul Luar | i |
| Halaman Judul Dalam | ii |
| Halaman Persetujuan <i>Softcover</i> | iii |
| Halaman Pernyataan Dewan Penguji | iv |
| Abstrak | vi |
| Prakata | vii |
| Daftar Isi | ix |
| Daftar Tabel | xv |
| Daftar Gambar | xvi |
| Daftar Lampiran | xviii |
| | |
| BAB 1 PENDAHULUAN | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Ruang Lingkup | 3 |
| 1.3 Tujuan dan Manfaat | 3 |
| 1.4 Metodologi | 4 |
| 1.5 Sistematika Penulisan | 7 |
| | |
| BAB 2 LANDASAN TEORI | 8 |
| 2.1 Jaringan Komunikasi | 8 |
| 2.1.1 Model TCP/IP Layer | 8 |
| 2.1.1.1 Application Layer | 9 |

| | | |
|---------|---|----|
| 2.1.1.2 | Transport Layer | 10 |
| 2.1.1.3 | Internet Layer | 11 |
| 2.1.1.4 | Network Access Layer | 12 |
| 2.1.2 | Model OSI Layer | 13 |
| 2.1.2.1 | Physical Layer | 14 |
| 2.1.2.2 | Data Link Layer | 14 |
| 2.1.2.3 | Network Layer | 14 |
| 2.1.2.4 | Transport Layer | 15 |
| 2.1.2.5 | Session Layer | 15 |
| 2.1.2.6 | Presentation Layer | 15 |
| 2.1.2.7 | Application Layer | 15 |
| 2.2 | Klasifikasi Jaringan | 16 |
| 2.2.1 | <i>Local Area Network</i> (LAN) | 16 |
| 2.2.1.1 | Topologi Jaringan | 17 |
| 2.2.2 | <i>Metropoliltan Area Network</i> (MAN) | 19 |
| 2.2.3 | <i>Wide Area Network</i> (WAN) | 20 |
| 2.2.3.1 | Teknologi WAN | 20 |
| 2.2.3.2 | Topologi WAN | 21 |
| 2.2.3.3 | Protokol WAN | 21 |
| 2.3 | <i>IP address</i> | 22 |
| 2.3.1 | Kelas-kelas dalam <i>IP address</i> | 23 |
| 2.3.2 | Private dan Public <i>IP address</i> | 24 |
| 2.4 | <i>Virtual Private Network</i> (VPN) | 25 |
| 2.4.1 | Tipe-tipe VPN | 26 |

| | | |
|---------|--|----|
| 2.4.1.1 | <i>Site-to-site</i> VPN | 26 |
| 2.4.1.2 | <i>Extranet</i> VPN | 28 |
| 2.4.1.3 | <i>Remote Access</i> VPN | 29 |
| 2.4.2 | Topologi VPN | 30 |
| 2.4.2.1 | Topologi <i>Hub</i> dan <i>Spoke</i> | 30 |
| 2.4.2.2 | Topologi <i>Partial</i> atau <i>Full Mesh</i> | 31 |
| 2.4.2.3 | Topologi <i>Hybrid</i> | 32 |
| 2.4.3 | Arsitektur untuk VPN | 33 |
| 2.4.3.1 | Arsitektur Frame Relay atau ATM Virtual Circuit | 34 |
| 2.4.3.2 | Arsitektur IP Tunneling | 36 |
| 2.4.3.3 | Arsitektur MPLS | 37 |
| 2.5 | <i>Tunneling</i> | 41 |
| 2.5.1 | Fungsi-fungsi <i>Tunneling</i> | 42 |
| 2.5.2 | Protokol <i>Tunneling</i> Layer 2 | 43 |
| 2.5.2.1 | <i>Point-to-Point Protocol</i> (PPP) | 43 |
| 2.5.2.2 | <i>Point-to-Point Tunneling Protocol</i> (PPTP) | 44 |
| 2.5.2.3 | <i>Layer 2 Forwarding</i> (L2F) | 46 |
| 2.5.2.4 | <i>Layer 2 Tunneling Protocol</i> (L2TP) | 47 |
| 2.6 | <i>Internet Protocol Security</i> (IPSec) | 49 |
| 2.6.1 | <i>Authentication</i> | 50 |
| 2.6.1.1 | <i>User Authentication</i> | 50 |
| 2.6.1.2 | <i>Data Authentication</i> | 51 |
| 2.6.1.3 | <i>Authentication Header</i> (AH) | 51 |

| | | |
|--------------|---|-----------|
| 2.6.2 | <i>Encryption</i> | 52 |
| 2.6.2.1 | <i>Symetrical Key Encryption</i> | 53 |
| 2.6.2.2 | <i>Asymetrical Key Encryption</i> | 54 |
| 2.6.2.3 | <i>Encapsulation Security Payload (ESP)</i> | 55 |
| 2.6.3 | <i>Key Management</i> | 56 |
| 2.6.4 | Mode pada IPsec | 58 |
| 2.6.4.1 | <i>IPsec Transport Mode</i> | 58 |
| 2.6.4.2 | <i>IPsec Tunnel Mode</i> | 59 |
| 2.7 | <i>Secure Socket Layer (SSL)</i> | 60 |
| BAB 3 | ANALISIS SISTEM BERJALAN | 61 |
| 3.1 | Profil Perusahaan PT. Hotel Indonesia Natour | 61 |
| 3.1.1 | Sejarah Perusahaan PT. Hotel Indonesia Natour | 61 |
| 3.1.1.1 | PT. Hotel Indonesia Internasional | 61 |
| 3.1.1.2 | PT. Natour | 62 |
| 3.1.1.3 | PT. Hotel Indonesia Natour | 64 |
| 3.1.2 | Visi dan Misi | 64 |
| 3.1.3 | Layanan dan Produk PT. Hotel Indonesia Natour | 65 |
| 3.1.4 | Kekuatan Sumber Daya Manusia | 67 |
| 3.1.5 | Sasaran Perusahaan | 67 |
| 3.1.6 | <i>Tim Management</i> | 68 |
| 3.2 | Struktur Organisasi | 69 |
| 3.2.1 | Pembagian Tugas dan Tanggung Jawab | 71 |
| 3.3 | Sistem yang Sedang Berjalan | 79 |

| | | |
|---------|--|-----|
| 3.3.1 | Sistem Jaringan yang Sedang Berjalan | 80 |
| 3.3.1.1 | <i>Distribution Area</i> | 81 |
| 3.3.1.2 | <i>Server Farm</i> | 83 |
| 3.3.1.3 | Jaringan Akses Internet | 84 |
| 3.3.2 | Overview dari Proses Bisnis pada PT. HIN..... | 85 |
| 3.3.3 | Bisnis Perhotelan pada PT. Hotel Indonesia Natour..... | 87 |
| 3.3.4 | Analisis Penggunaan <i>Bandwidth</i> | 89 |
| 3.3.4.1 | Penggunaan <i>Bandwidth</i> pada Kantor Pusat | 89 |
| 3.3.4.2 | Penggunaan <i>Bandwidth</i> pada Kantor Cabang | 90 |
| 3.3.5 | Permasalahan yang Dihadapi | 91 |
| 3.3.6 | Usulan Pemecahan Masalah | 92 |
| 3.3.7 | Analisa Kelayakan Teknologi yang Diterapkan | 93 |
| 3.3.7.1 | Teknologi VPN..... | 93 |
| 3.3.7.2 | Dukungan Infrastruktur | 94 |
| 3.3.8 | Analisa Ancaman Keamanan pada Transaksi Internet | 95 |
| 3.3.9 | Analisa Pemilihan Topologi VPN | 97 |
| 3.3.10 | Analisa Pemilihan Tipe VPN | 98 |
| 3.3.11 | Analisa Pemilihan Kebutuhan Teknologi | 101 |
| | | |
| BAB 4 | USULAN SOLUSI RANCANGAN DAN IMPLEMENTASI | 103 |
| 4.1 | Usulan Rancangan Koneksi Kantor Cabang | 103 |
| 4.2 | Pemilihan Hardware dan Software yang Digunakan | 105 |
| 4.3 | Usulan Perubahan pada Jaringan Intranet | 106 |
| 4.4 | Usulan Solusi Perancangan VPN | 107 |

| | | |
|---------|--|-----|
| 4.5 | Pengimplementasian VPN Server | 110 |
| 4.5.1 | Instalasi Paket FreeSWAN dan Dependencynya | 111 |
| 4.5.2 | Patch dan Kompilasi Kernel | 114 |
| 4.5.3 | Instalasi pada Network | 119 |
| 4.5.4 | Konfigurasi VPN Server | 119 |
| 4.5.4.1 | Konfigurasi OpenSSL | 120 |
| 4.5.4.2 | Konfigurasi CA | 120 |
| 4.5.4.3 | Konfigurasi Sertifikat FreeSWAN | 122 |
| 4.5.5 | Konfigurasi VPN Client | 128 |
| 4.6 | Evaluasi VPN | 129 |
| 4.6.1 | Testing VPN | 130 |
| 4.6.2 | Kelebihan dan Kelemahan VPN | 133 |
| 4.6.2.1 | Kelebihan VPN | 133 |
| 4.6.2.2 | Kelemahan VPN | 135 |
| BAB 5 | KESIMPULAN DAN SARAN | 137 |
| 5.1 | Kesimpulan | 137 |
| 5.2 | Saran | 137 |
| | DAFTAR PUSTAKA | 138 |
| | RIWAYAT HIDUP | 139 |
| | LAMPIRAN-LAMPIRAN | 141 |
| | FOTOCOPY SURAT SURVEI | |

DAFTAR TABEL

| | | |
|-----------|---|-----|
| Tabel 2.1 | Kelas-kelas <i>IP address</i> | 23 |
| Tabel 2.2 | Kelompok <i>private IP address</i> | 24 |
| Tabel 2.3 | Klasifikasi Layanan VPN | 33 |
| Tabel 2.4 | Perbandingan antara PPTP, L2F dan L2PT | 49 |
| Tabel 3.1 | Perbandingan Internet, Frame Relay, Leased Line | 95 |
| Tabel 4.1 | Rancangan Koneksi gateway Kantor Pusat | 108 |
| Tabel 4.2 | Koneksi kantor cabang INNA Simpang Surabaya | 109 |

DAFTAR GAMBAR

| | | |
|-------------|--|----|
| Gambar 2.1 | TPC/IP Layer | 9 |
| Gambar 2.2 | OSI Layer | 13 |
| Gambar 2.3 | Topologi jaringan | 17 |
| Gambar 2.4 | LAN, MAN, WAN | 19 |
| Gambar 2.5 | <i>Virtual Private Networking</i> (VPN) | 26 |
| Gambar 2.6 | <i>Site-to-Site</i> VPN | 27 |
| Gambar 2.7 | <i>Extranet</i> VPN | 28 |
| Gambar 2.8 | <i>Remote Access</i> VPN | 29 |
| Gambar 2.9 | Topologi <i>hub</i> dan <i>spoke</i> | 31 |
| Gambar 2.10 | Topologi <i>partial mesh</i> | 32 |
| Gambar 2.11 | Topologi <i>hybrid</i> | 33 |
| Gambar 2.12 | Arsitektur PVC pada jaringan <i>Frame Relay</i> | 34 |
| Gambar 2.13 | Skenario VPN dengan menggunakan <i>tunnel</i> IPsec antara <i>router-router</i> | 36 |
| Gambar 2.14 | Sistem Kerja MPLS | 39 |
| Gambar 2.15 | <i>Tunneling</i> | 42 |
| Gambar 2.16 | Format pada PPP frame | 44 |
| Gambar 2.17 | Proses PPTP <i>Tunneling</i> | 45 |
| Gambar 2.18 | Format paket L2F | 47 |
| Gambar 2.19 | Proses enkapsulasi data pada L2TP | 48 |
| Gambar 2.20 | Paket yang diproteksi AH | 51 |

| | | |
|-------------|---|----|
| Gambar 2.21 | Paket IP yang diproteksi dengan AH dalam <i>transport mode</i> | 52 |
| Gambar 2.22 | Paket IP yang diproteksi dengan AH dalam <i>tunnel mode</i> | 52 |
| Gambar 2.23 | Symmetrical Key Encryption | 54 |
| Gambar 2.24 | Asymmetrical Key Encryption | 55 |
| Gambar 2.25 | Paket IP setelah ditambahkan ESP <i>header</i> | 55 |
| Gambar 2.26 | Paket IP yang diproteksi dengan ESP | 55 |
| Gambar 2.27 | Paket IP yang diproteksi dengan ESP dalam <i>transport mode</i> | 56 |
| Gambar 2.28 | Paket IP yang diproteksi dengan ESP dalam <i>tunnel mode</i> | 56 |
| Gambar 2.29 | Paket IP dalam <i>IPSec Transport Mode</i> | 59 |
| Gambar 2.30 | Paket IP dalam <i>IPSec Tunnel Mode</i> | 59 |
| Gambar 3.1 | Profil Manajemen PT. Hotel Indonesia Natour | 68 |
| Gambar 3.2 | Struktur organisasi PT. Hotel Indonesia Natour | 69 |
| Gambar 3.3 | Struktur organisasi Direktorat Utama | 73 |
| Gambar 3.4 | Struktur organisasi <i>Coorporate Affair</i> | 74 |
| Gambar 3.5 | Struktur organisasi bagian <i>Internal Auditor</i> | 75 |
| Gambar 3.6 | Struktur organisasi bagian dari <i>Coorporate Safety & Security</i> | 75 |
| Gambar 3.7 | Struktur organisasi <i>Finance Department</i> | 76 |
| Gambar 3.8 | Struktur organisasi <i>Operation Department</i> | 77 |
| Gambar 3.9 | Struktur organisasi <i>Marketing Department</i> | 78 |
| Gambar 3.10 | Struktur organisasi <i>Human Resource Department</i> | 79 |
| Gambar 3.11 | Jaringan pada PT. Hotel Indonesia Natour | 81 |
| Gambar 3.12 | Koneksi antar PC tiap lantai | 82 |
| Gambar 3.13 | Jaringan koneksi akses internet | 84 |
| Gambar 3.14 | Proses bisnis front office | 86 |

| | | |
|-------------|--|-----|
| Gambar 3.15 | Proses back office | 86 |
| Gambar 3.16 | Jaringan Internet PT. Hotel Indonesia Natour | 88 |
| Gambar 3.17 | Penggunaan <i>bandwidth</i> per hari pada Kantor Pusat PT. HIN... | 90 |
| Gambar 3.18 | Penggunaan <i>bandwidth</i> per hari pada Kantor Cabang Surabaya | 90 |
| Gambar 3.19 | Penggunaan <i>bandwidth</i> per hari pada Kantor Cabang Bali | 91 |
| Gambar 3.20 | Garis besar jaringan komunikasi antar pusat – cabang | 100 |
| Gambar 4.1 | Rancangan topologi <i>hub and spoke</i> pada PT. HIN | 104 |
| Gambar 4.2 | Perubahan router menjadi VPN Server | 107 |
| Gambar 4.3 | Koneksi kantor pusat – kantor cabang | 109 |
| Gambar 4.4 | Konfigurasi panjang bit enkripsi RSA key | 113 |
| Gambar 4.5 | Kernel Patching pada FreeSwan | 117 |
| Gambar 4.6 | Menu dari konfigurasi kernel | 118 |
| Gambar 4.7 | IPSec Option pada konfigurasi kernel linux | 118 |
| Gambar 4.8 | Konfigurasi <code>default_bit</code> pada <code>opnssl.cnf</code> | 120 |
| Gambar 4.9 | Konfigurasi <code>default_days</code> pada <code>opnssl.cnf</code> | 120 |
| Gambar 4.10 | Konfigurasi <code>CA.sh</code> | 121 |
| Gambar 4.11 | Konfigurasi CA | 122 |
| Gambar 4.12 | Konfigurasi sertifikat FreeSWAN | 123 |
| Gambar 4.13 | Pembuatan key signature dari sertifikat request | 124 |
| Gambar 4.14 | file <code>ipsec.secrets</code> VPN server kantor pusat | 126 |
| Gambar 4.15 | file <code>ipsec.secrets</code> VPN server kantor cabang | 128 |
| Gambar 4.16 | Routing table VPN server surabaya | 130 |
| Gambar 4.17 | Sniff paket data tanpa VPN | 131 |
| Gambar 4.18 | <i>Sniff</i> paket data dengan VPN | 132 |

DAFTAR LAMPIRAN

| | |
|--|-----|
| Lampiran A | 141 |
| A1. Konfigurasi <i>OpenSSL</i> pada VPN server | 141 |
| A2. Konfigurasi CA (<i>Certificate Authority</i>) pada VPN server | 143 |
| A3. Konfigurasi IPsec pada VPN server kantor pusat | 145 |
| A4. Konfigurasi IPsec pada VPN server kantor cabang simpang | 145 |
| Lampiran B | 147 |
| B1. Sertifikat autentikasi VPN server kantor pusat (vpn.hin.net.pem) | 147 |
| B2. Private key dari VPN server kantor pusat (vpn.hin.net.key) | 148 |