

# **PERBANDINGAN KINERJA DARI PROTOKOL VPN SSTP, OPENVPN DAN IPSEC BERBASIS MIKROTIK**

## **TUGAS AKHIR**

Disusun sebagai salah satu syarat untuk kelulusan  
Program Strata 1, Program Studi Teknik Informatika,  
Universitas Pasundan Bandung

oleh:

**Muhammad Fuad Fauda**  
**11.304.0132**



**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS PASUNDAN  
BANDUNG  
JUNI 2016**

**LEMBAR PENGESAHAN  
LAPORAN TUGAS AKHIR**

Telah diujikan dan dipertahankan dalam Sidang Sarjana Program Studi Teknik Informatika Universitas Pasundan Bandung, pada hari dan tanggal sidang sesuai berita acara sidang, tugas akhir dari :

Nama : Muhammad Fuad Fauda  
Nrp : 11.304.0132

Dengan judul :

**“PERBANDINGAN KINERJA DARI PROTOKOL VPN SSTP, OPENVPN DAN  
IPSEC BERBASIS MIKROTIK”**

Bandung, 22 Juni 2016

Menyetujui,

Pembimbing Utama,

Pembimbing Pendamping,

(Doddy Ferdiansyah, S.T, M.T)

(Ferry Mulyanto, ST, M.Kom.)

## LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa :

1. Tugas akhir ini adalah benar-benar asli dan belum pernah diajukan untuk mendapatkan gelar akademik, baik di Universitas Pasundan Bandung maupun di Perguruan Tinggi lainnya
2. Tugas akhir ini merupakan gagasan, rumusan dan penelitian saya sendiri, tanpa bantuan pihak lain kecuali arahan dari tim Dosen Pembimbing
3. Dalam tugas akhir ini tidak terdapat karya atau pendapat orang lain, kecuali bagian-bagian tertentu dalam penulisan laporan Tugas Akhir yang saya kutip dari hasil karya orang lain telah dituliskan dalam sumbernya secara jelas sesuai dengan norma, kaidah, dan etika penulisan karya ilmiah, serta disebutkan dalam Daftar Pustaka pada tugas akhir ini
4. Kakas, perangkat lunak, dan alat bantu kerja lainnya yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab saya, bukan tanggung jawab Universitas Pasundan Bandung

Apabila di kemudian hari ditemukan seluruh atau sebagian laporan tugas akhir ini bukan hasil karya saya sendiri atau adanya plagiasi dalam bagian-bagian tertentu, saya bersedia menerima sanksi akademik, termasuk pencabutan gelar akademik yang saya sandang sesuai dengan norma yang berlaku di Universitas Pasundan, serta perundang-undangan lainnya

Bandung, 22 Juni 2016

Yang membuat pernyataan,

Materai  
6000,-

( **Muhammad Fuad Fauda** )

NRP. 11.304.0132



## ABSTRAK

Informasi merupakan salah satu faktor pendukung keberhasilan bisnis dari suatu organisasi atau perusahaan. Namun, ada beberapa jenis informasi yang bersifat rahasia dan hanya boleh diakses oleh orang-orang yang berhak atas informasi tersebut. Sehingga kerahasiaan dari informasi tersebut dapat dijaga. Oleh karena itu, dibutuhkan sebuah teknologi yang dapat memungkinkan para karyawan dapat mengakses informasi yang bersifat rahasia dan hanya bisa diakses pada jaringan *Intranet* perusahaan. Selain dapat diakses melalui jaringan publik, kecepatan tranfer akan informasi tersebut harus diperhatikan. VPN merupakan salah satu solusi untuk mengatasi permasalahan tersebut.

Tugas akhir ini akan membandingkan kinerja dari protokol SSTP, OpenVPN dan IPSec . Dimulai dari studi pustaka, analisis lalu melakukan pengujian kinerja dari jaringan VPN dengan menggunakan metode autentikasi *digital certificate* dan parameter yaitu *throughput*. Sehingga kita dapat mengetahui perbandingan kinerja dari protokol VPN SSTP, OpenVPN dan IPSec.

Hasil yang akan didapatkan dari Tugas Akhir ini adalah sebuah perbandingan kinerja dari protokol VPN SSTP, OpenVPN dan IPSec berdasarkan *throughput*. Sehingga dapat diketahui protokol mana yang memiliki kinerja paling baik berdasarkan *throughput* dan dapat digunakan untuk kebutuhan impelentasi dari VPN.

**Kata Kunci** : VPN, SSTP, OpenVPN, IPSec , *Throughput*.

## ABSTRACT

Information is one of the factors supporting the business success of an organization or company. However, there are some types of information that is confidential and can only be accessed by authorized people. So that the confidentiality of such information can be kept. Therefore, we need a technology that can enable employees to access secret information and only be accessed on the corporate Intranet . Besides accessible via a public network, the speed of information transfer must be considered. VPN is a solution to solve these problems.

This final assignment would compare the performance of the protocol SSTP, OpenVPN and IPSec. Starting from the literature, analysis and testing the performance of the network VPN using digital certificate authentication method and parameters throughput. So that we can compare the performance of the VPN protocols SSTP, OpenVPN and IPSec.

The results of this final assignment is a comparison of the performance VPN protocols SSTP, OpenVPN and IPSec based on throughput. So that can know the protocol which has the best performance based on throughput and can be used for the needs of VPN implementation.

**Keywords:** VPN, SSTP, OpenVPN, IPSec, Throughput.

## KATA PENGANTAR

Bismillahirrahmanirrahim

Puji syukur kami panjatkan kehadirat Allah SWT karena atas izin dan kehendak-Nya penulis dapat menyelesaikan Laporan Tugas Akhir yang berjudul **“Perbandingan Kinerja dari Protokol VPN SSTP, OPENVPN dan IPSEC Berbasis Mikrotik”**. Tugas Akhir ini disusun dan diajukan demi memenuhi salah satu syarat untuk melakukan penyusunan Tugas Akhir di jurusan Teknik Informatika Universitas Pasundan Bandung. Didalam penyusunan Tugas Akhir ini, penulis dibantu oleh banyak pihak, oleh karena ini penulis mengucapkan banyak terima kasih yang sebesar-besarnya kepada :

1. Allah SWT yang telah memberikan nikmat sehat serta kelancaran bagi penulis sehingga pada akhirnya dapat menyelesaikan laporan tugas akhir ini.
2. Kedua orang tua, Ibu dan Bapak yang selalu memberikan dukungan baik secara moril maupun materil.
3. Kedua pembimbing, Bapak Doddy Ferdiansyah, S.T, M.T dan Bapak Ferry Mulyanto, S.T, M.Kom.
4. Seluruh Dosen – dosen Teknik informatika di UNIVERSITAS PASUNDAN BANDUNG, yang selama ini telah memberikan bekal ilmu.
5. Kepada rekan-rekan jurusan Teknik Informatika angkatan 2011 yang tidak bisa semua penulis sebutkan.

Penulis sadari bahwasanya dalam pembuatan Tugas Akhir ini masih jauh dari kesempurnaan, maka dari itu kritik serta saran untuk memperbaiki keberhasilan penulis di masa yang akan datang.

Akhir kata, semoga penulisan laporan ini dapat bermanfaat bagi penulis dan bagi perkembangan ilmu Teknologi dimasa yang akan datang.

Bandung , Juni 2016

Penulis

## DAFTAR ISI

|                                                                          |      |
|--------------------------------------------------------------------------|------|
| ABSTRAK .....                                                            | i    |
| ABSTRACT .....                                                           | ii   |
| KATA PENGANTAR .....                                                     | iii  |
| DAFTAR ISI .....                                                         | iv   |
| DAFTAR TABEL .....                                                       | vii  |
| DAFTAR GAMBAR .....                                                      | viii |
| DAFTAR SIMBOL .....                                                      | xii  |
| DAFTAR ISTILAH .....                                                     | xiii |
| BAB 1 PENDAHULUAN .....                                                  | 1-1  |
| 1.1 Latar Belakang .....                                                 | 1-1  |
| 1.2 Identifikas Masalah .....                                            | 1-2  |
| 1.3 Tujuan Tugas Akhir.....                                              | 1-2  |
| 1.4 Lingkup Tugas Akhir .....                                            | 1-2  |
| 1.5 Metodologi Tugas Akhir.....                                          | 1-2  |
| 1.6 Sistematika Penulisan Tugas Akhir .....                              | 1-4  |
| BAB 2 LANDASAN TEORI.....                                                | 2-1  |
| 2.1 VPN ( <i>Virtual private network</i> ) .....                         | 2-1  |
| 2.2 Jenis-Jenis VPN.....                                                 | 2-2  |
| 2.2.1 <i>Remote access</i> VPN.....                                      | 2-2  |
| 2.2.2 <i>Intranet</i> VPN .....                                          | 2-3  |
| 2.2.3 <i>Extranet</i> VPN.....                                           | 2-4  |
| 2.3 Enkripsi Data.....                                                   | 2-5  |
| 2.3.1 <i>Symmetric Cryptosystems</i> .....                               | 2-6  |
| 2.3.2 <i>Asymmetric Cryptosystems</i> .....                              | 2-7  |
| 2.4 Infrastruktur Kunci Publik ( <i>Public Key Infrastructure</i> )..... | 2-9  |
| 2.4.1 Fungsi PKI.....                                                    | 2-9  |
| 2.4.2 Komponen PKI.....                                                  | 2-10 |
| 2.5 Teknologi <i>Tunneling</i> .....                                     | 2-11 |
| 2.5.1 Kelebihan <i>Tunneling</i> .....                                   | 2-12 |
| 2.6 IP <i>Security</i> .....                                             | 2-12 |
| 2.6.1 Protokol Keamanan ( <i>Security Protocols</i> ) .....              | 2-13 |
| 2.6.2 <i>Key Manangement</i> .....                                       | 2-16 |
| 2.7 SSTP .....                                                           | 2-17 |
| 2.7.1 Proses Koneksi VPN berbasis SSTP .....                             | 2-17 |
| 2.8 OpenVpn.....                                                         | 2-17 |
| 2.8.1 Keuntungan OpenVPN .....                                           | 2-18 |

|                                                  |                                                             |      |
|--------------------------------------------------|-------------------------------------------------------------|------|
| 2.9                                              | Protokol.....                                               | 2-18 |
| 2.10                                             | Parameter <i>Quality Of Service (QoS)</i> .....             | 2-19 |
| 2.10.1                                           | <i>Throughput</i> .....                                     | 2-19 |
| 2.10.2                                           | <i>Packet Loss</i> .....                                    | 2-19 |
| 2.10.3                                           | <i>Delay</i> .....                                          | 2-20 |
| 2.10.4                                           | <i>Jitter</i> .....                                         | 2-21 |
| 2.11                                             | Kinerja VPN.....                                            | 2-21 |
| <b>BAB 3 ANALISIS DAN PERANCANGAN</b> .....      |                                                             | 3-1  |
| 3.1                                              | Kerangka Tugas Akhir.....                                   | 3-1  |
| 3.2                                              | Skema Analisis.....                                         | 3-3  |
| 3.3                                              | Analisis Fitur VPN Berbasis Mikrotik.....                   | 3-4  |
| 3.3.1                                            | PPTP.....                                                   | 3-4  |
| 3.3.2                                            | SSTP.....                                                   | 3-5  |
| 3.3.3                                            | L2TP.....                                                   | 3-6  |
| 3.3.4                                            | IPSEC.....                                                  | 3-7  |
| 3.3.5                                            | OpenVPN.....                                                | 3-9  |
| 3.4                                              | Analisis Lingkungan Implementasi Jaringan VPN.....          | 3-11 |
| 3.5                                              | Analisis Throughput.....                                    | 3-11 |
| 3.6                                              | Analisis Kebutuhan Perangkat Lunak dan Perangkat Keras..... | 3-11 |
| 3.6.1                                            | Perangkat Lunak.....                                        | 3-11 |
| 3.6.2                                            | Perangkat Keras.....                                        | 3-11 |
| 3.7                                              | Menetapkan Media Transmisi.....                             | 3-12 |
| 3.8                                              | Parameter Pengujian Kinerja.....                            | 3-12 |
| 3.9                                              | Skenario Pengujian Kinerja.....                             | 3-12 |
| 3.10                                             | Topologi Jaringan.....                                      | 3-13 |
| 3.10.1                                           | Topologi Logik.....                                         | 3-13 |
| 3.10.2                                           | Topologi Fisik.....                                         | 3-13 |
| 3.11                                             | Hasil Analisis.....                                         | 3-14 |
| <b>BAB 4 IMPLEMENTASI DAN PERBANDINGAN</b> ..... |                                                             | 4-1  |
| 4.1                                              | Implementasi VPN.....                                       | 4-1  |
| 4.1.1                                            | Penggunaan Perangkat Keras.....                             | 4-1  |
| 4.1.2                                            | Konfigurasi <i>Digital Certificate</i> .....                | 4-1  |
| 4.1.3                                            | Konfigurasi <i>IP Address</i> .....                         | 4-5  |
| 4.1.4                                            | Konfigurasi <i>IP Pool</i> .....                            | 4-6  |
| 4.1.5                                            | Konfigurasi DNS.....                                        | 4-6  |
| 4.1.6                                            | Konfigurasi <i>Routing</i> .....                            | 4-7  |
| 4.1.7                                            | Konfigurasi <i>VPN Server</i> .....                         | 4-8  |

|                     |                                                              |      |
|---------------------|--------------------------------------------------------------|------|
| 4.1.8               | Konfigurasi VPN <i>Client</i> .....                          | 4-12 |
| 4.1.9               | Percobaan Koneksi VPN.....                                   | 4-20 |
| 4.2                 | Pengujian Kinerja VPN.....                                   | 4-22 |
| 4.2.1               | Pengujian Kinerja Protokol SSTP.....                         | 4-22 |
| 4.2.2               | Pengujian Kinerja Protokol OpenVPN.....                      | 4-28 |
| 4.2.3               | Pengujian Kinerja Protokol IPsec.....                        | 4-34 |
| 4.3                 | Perbandingan Kinerja VPN.....                                | 4-40 |
| 4.4                 | Hasil Kesimpulan Pengujian dan Perbandingan Kinerja VPN..... | 4-42 |
| BAB 5 PENUTUP.....  |                                                              | 5-1  |
| 5.1                 | Kesimpulan.....                                              | 5-1  |
| 5.2                 | Saran.....                                                   | 5-1  |
| DAFTAR PUSTAKA..... |                                                              | xiv  |

## DAFTAR TABEL

|                                                                                                         |      |
|---------------------------------------------------------------------------------------------------------|------|
| Tabel 2.1 Degredasi <i>Packet Loss</i> [FAD13] .....                                                    | 2-20 |
| Tabel 2.2 Jenis <i>Delay</i> [FAD13] .....                                                              | 2-20 |
| Tabel 2.3 <i>One Way delay</i> [FAD13].....                                                             | 2-20 |
| Tabel 2.4 Degredasi <i>Jitter</i> [FAD13].....                                                          | 2-21 |
| Tabel 3.1 Langkah-langkah Analisis .....                                                                | 3-4  |
| Tabel 3.2 Fitur Protokol VPN berbasis mikrotik .....                                                    | 3-10 |
| Tabel 3.3. Perangkat Lunak yang digunakan.....                                                          | 3-11 |
| Tabel 3.4 Spesifikasi <i>Server</i> VPN.....                                                            | 3-11 |
| Tabel 3.5 Spesifikasi <i>Client</i> VPN.....                                                            | 3-12 |
| Tabel 4.1 Spesifikasi <i>Router</i> Mikrotik RB751U-2HnD [MIK05] .....                                  | 4-1  |
| Tabel 4.2 Spesifikasi Laptop [LEN13] .....                                                              | 4-1  |
| Tabel 4.3 Hasil Pengujian Menggunakan Protokol SSTP pada Pagi Hari.....                                 | 4-24 |
| Tabel 4.4 Hasil Pengujian Menggunakan Protokol SSTP pada Siang Hari .....                               | 4-26 |
| Tabel 4.5 Hasil Pengujian Menggunakan Protokol SSTP pada Sore Hari.....                                 | 4-28 |
| Tabel 4.6 Hasil Pengujian Menggunakan Protokol OpenVPN pada Pagi Hari.....                              | 4-30 |
| Tabel 4.7 Hasil Pengujian Menggunakan Protokol OpenVPN pada Siang Hari.....                             | 4-32 |
| Tabel 4.8 Hasil Pengujian Menggunakan Protokol OpenVPN pada Sore Hari .....                             | 4-34 |
| Tabel 4.9 Hasil Pengujian Menggunakan Protokol VPN IPSec pada Pagi Hari .....                           | 4-36 |
| Tabel 4.10 Hasil Pengujian Menggunakan Protokol VPN IPSec pada Siang Hari .....                         | 4-38 |
| Tabel 4.11 Hasil Pengujian Menggunakan Protokol VPN IPSec pada Sore Hari.....                           | 4-40 |
| Tabel 4.12 Pengujian protokol VPN IPSec pada saat di encapsulasi dan <i>nat</i> tidak diaktifkan .....  | 4-43 |
| Tabel 4.13 Pengujian protokol VPN IPSec pada saat di dencapsulasi dan <i>nat</i> tidak diaktifkan ..... | 4-43 |
| Tabel 4.14 Pengujian protokol VPN IPSec di encapsulasi dan <i>nat</i> diaktifkan.....                   | 4-44 |
| Tabel 4.15 Pengujian protokol VPN IPSec di decapsulasi dan <i>nat</i> diaktifkan.....                   | 4-44 |

## DAFTAR GAMBAR






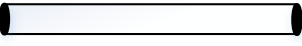
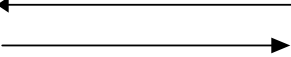


|                                                                                                              |      |
|--------------------------------------------------------------------------------------------------------------|------|
| Gambar 1.1 Metodologi Tugas Akhir.....                                                                       | 1-3  |
| Gambar 2.1 <i>Virtual Private Network</i> .....                                                              | 2-2  |
| Gambar 2.2 Topologi <i>Remote access</i> VPN (Meeta Gupta, 2003).....                                        | 2-3  |
| Gambar 2.3 Topologi <i>Intranet</i> VPN(Meeta Gupta, 2003).....                                              | 2-4  |
| Gambar 2.4 Topologi <i>Extranet</i> VPN(Meeta Gupta, 2003).....                                              | 2-5  |
| Gambar 2.5 Model Enkripsi Tradisional(Meeta Gupta, 2003).....                                                | 2-6  |
| Gambar 2.6 <i>Symmetric Cryptosystem</i> (Meeta Gupta, 2003).....                                            | 2-6  |
| Gambar 2.7 Pertukaran Data Algoritma Diffie-Hellman(Meeta Gupta, 2003).....                                  | 2-8  |
| Gambar 2.8 Pertukaran Data Algoritma RSA(Meeta Gupta, 2003).....                                             | 2-9  |
| Gambar 2.9 <i>Tunneling Process</i> (Meeta Gupta, 2003).....                                                 | 2-12 |
| Gambar 2.10 Posisi IPSEC dalam model OSI.....                                                                | 2-12 |
| Gambar 2.11 IPSEC <i>Transport mode</i> (Metaa Gupta, 2003).....                                             | 2-14 |
| Gambar 2.12 IPSEC <i>Tunnel mode</i> (Metaa Gupta, 2003).....                                                | 2-14 |
| Gambar 2.13 Paket <i>ip</i> setelah <i>header</i> ESP dan <i>Trailer</i> ditambahkan(Metaa Gupta, 2003)..... | 2-15 |
| Gambar 2.14 Format ESP <i>Header</i> (Metaa Gupta, 2003). ....                                               | 2-15 |
| Gambar 2.15 Paket <i>ip</i> setelah <i>header</i> (Metaa Gupta, 2003).....                                   | 2-16 |
| Gambar 2.16 Format IPSEC <i>Authentication Header</i> (AH).....                                              | 2-16 |
| Gambar 2.17 Jenis-jenis <i>delay [FAD13]</i> .....                                                           | 2-20 |
| Gambar 3.1 Kerangka TA bagian 1.....                                                                         | 3-1  |
| Gambar 3.2 Kerangka TA bagian 2.....                                                                         | 3-2  |
| Gambar 3.3 Skema Analisis.....                                                                               | 3-3  |
| Gambar 3.4 PPTP <i>Server</i> .....                                                                          | 3-5  |
| Gambar 3.5 SSTP <i>Server</i> .....                                                                          | 3-6  |
| Gambar 3.6 L2TP <i>Server</i> .....                                                                          | 3-7  |
| Gambar 3.7 <i>Proposal</i> IPSEC.....                                                                        | 3-8  |
| Gambar 3.8 IPSEC <i>Peer</i> .....                                                                           | 3-9  |
| Gambar 3.9 OVPN <i>Server</i> .....                                                                          | 3-10 |
| Gambar 3.10 Topologi Logik <i>Remote access</i> VPN.....                                                     | 3-13 |
| Gambar 3.11 Topologi Logik <i>Intranet</i> VPN.....                                                          | 3-13 |
| Gambar 3.12 Topologi Fisik <i>Remote Access</i> VPN.....                                                     | 3-14 |
| Gambar 3.13 Topologi Fisik <i>Intranet</i> VPN.....                                                          | 3-14 |
| Gambar 4.1 <i>Ca Certificate Key</i> .....                                                                   | 4-2  |
| Gambar 4.2 <i>Ca Certificate</i> .....                                                                       | 4-2  |
| Gambar 4.3 <i>Server Certificate Key</i> .....                                                               | 4-2  |
| Gambar 4.4 <i>Server Csr</i> .....                                                                           | 4-3  |
| Gambar 4.5 <i>Server Certificate</i> .....                                                                   | 4-3  |

|                                                                                         |      |
|-----------------------------------------------------------------------------------------|------|
| Gambar 4.6 <i>Client Certificate Key</i> .....                                          | 4-3  |
| Gambar 4.7 <i>Client Csr</i> .....                                                      | 4-4  |
| Gambar 4.8 <i>Client Certificate</i> .....                                              | 4-4  |
| Gambar 4.9 <i>Import digital certificate</i> pada Mikrotik.....                         | 4-5  |
| Gambar 4.10 Mengubah Nama <i>Interface</i> Mikrotik.....                                | 4-5  |
| Gambar 4.11 Pemasangan <i>ip address</i> pada Internet dan <i>interface Local</i> ..... | 4-6  |
| Gambar 4.12 Konfigurasi <i>ip pool</i> .....                                            | 4-6  |
| Gambar 4.13 Konfigurasi DNS .....                                                       | 4-7  |
| Gambar 4.14 <i>Route List</i> .....                                                     | 4-7  |
| Gambar 4.15 <i>Routing</i> Untuk Koneksi ke Internet.....                               | 4-8  |
| Gambar 4.16 <i>Routing</i> ke lokal.....                                                | 4-8  |
| Gambar 4.17 Konfigurasi <i>Profile PPP</i> .....                                        | 4-9  |
| Gambar 4.18 Pembuatan <i>User</i> .....                                                 | 4-9  |
| Gambar 4.19 Konfigurasi <i>SSTP Server</i> .....                                        | 4-10 |
| Gambar 4.20 Konfigurasi <i>OVPN Server</i> .....                                        | 4-10 |
| Gambar 4.21 <i>IPSec Mode Config</i> .....                                              | 4-11 |
| Gambar 4.22 <i>IPSec Peer</i> .....                                                     | 4-11 |
| Gambar 4.23 <i>IPSec Proposal</i> .....                                                 | 4-12 |
| Gambar 4.24 <i>Certificate not Trusted</i> .....                                        | 4-13 |
| Gambar 4.25 <i>Microsoft Management Console</i> .....                                   | 4-13 |
| Gambar 4.26 <i>Import Certificate Microsoft Management Console</i> .....                | 4-14 |
| Gambar 4.27 <i>Certificate Trusted</i> .....                                            | 4-14 |
| Gambar 4.28 <i>Set Up a Connection or Network</i> .....                                 | 4-15 |
| Gambar 4.29 <i>Connect to the Internet</i> .....                                        | 4-15 |
| Gambar 4.30 <i>Connect to a Workplace</i> .....                                         | 4-15 |
| Gambar 4.31 <i>Connect VPN SSTP</i> .....                                               | 4-16 |
| Gambar 4.32 <i>SSTP Properties</i> .....                                                | 4-16 |
| Gambar 4.33 buat <i>file OpenVPN Client</i> .....                                       | 4-17 |
| Gambar 4.34 <i>Shrew Client</i> .....                                                   | 4-17 |
| Gambar 4.35 Tab <i>General Shrew Client</i> .....                                       | 4-18 |
| Gambar 4.36 Tab <i>Authentication Shrew Client</i> .....                                | 4-18 |
| Gambar 4.37 Tab <i>Phase 1 Shrew Client</i> .....                                       | 4-19 |
| Gambar 4.38 Tab <i>Phase 2 Shrew Client</i> .....                                       | 4-19 |
| Gambar 4.39 Tab <i>Policy Shrew Client</i> .....                                        | 4-20 |
| Gambar 4.40 Percobaan Koneksi Menggunakan Protokol VPN SSTP .....                       | 4-21 |
| Gambar 4.41 Percobaan Koneksi Menggunakan Protokol VPN OpenVPN.....                     | 4-21 |
| Gambar 4.42 Percobaan Koneksi Menggunakan Protokol VPN IPSec .....                      | 4-22 |

|                                                                                                     |      |
|-----------------------------------------------------------------------------------------------------|------|
| Gambar 4.43 Hasil Pengujian <i>Intranet</i> VPN SSTP pada kategori <i>file small</i> .....          | 4-23 |
| Gambar 4.44 Hasil Pengujian <i>Intranet</i> VPN SSTP pada kategori <i>file medium</i> .....         | 4-23 |
| Gambar 4.45 Hasil Pengujian <i>Intranet</i> VPN SSTP pada kategori <i>file large</i> .....          | 4-23 |
| Gambar 4.46 Hasil Pengujian <i>Remote Access</i> VPN SSTP pada kategori <i>file small</i> .....     | 4-23 |
| Gambar 4.47 Hasil Pengujian <i>Remote Access</i> VPN SSTP pada kategori <i>file medium</i> .....    | 4-24 |
| Gambar 4.48 Hasil Pengujian <i>Remote Access</i> VPN SSTP pada kategori <i>file large</i> .....     | 4-24 |
| Gambar 4.49 Hasil Pengujian <i>Intranet</i> VPN SSTP pada kategori <i>file small</i> .....          | 4-25 |
| Gambar 4.50 Hasil Pengujian <i>Intranet</i> VPN SSTP pada kategori <i>file medium</i> .....         | 4-25 |
| Gambar 4.51 Hasil Pengujian <i>Intranet</i> VPN SSTP pada kategori <i>file large</i> .....          | 4-25 |
| Gambar 4.52 Hasil Pengujian <i>Remote Access</i> VPN SSTP pada kategori <i>file small</i> .....     | 4-25 |
| Gambar 4.53 Hasil Pengujian <i>Remote Access</i> VPN SSTP pada kategori <i>file medium</i> .....    | 4-26 |
| Gambar 4.54 Hasil Pengujian <i>Remote Access</i> VPN SSTP pada kategori <i>file large</i> .....     | 4-26 |
| Gambar 4.55 Hasil Pengujian <i>Intranet</i> VPN SSTP pada kategori <i>file small</i> .....          | 4-27 |
| Gambar 4.56 Hasil Pengujian <i>Intranet</i> VPN SSTP pada kategori <i>file medium</i> .....         | 4-27 |
| Gambar 4.57 Hasil Pengujian <i>Intranet</i> VPN SSTP pada kategori <i>file large</i> .....          | 4-27 |
| Gambar 4.58 Hasil Pengujian <i>Remote Access</i> VPN SSTP pada kategori <i>file small</i> .....     | 4-27 |
| Gambar 4.59 Hasil Pengujian <i>Remote Access</i> VPN SSTP pada kategori <i>file medium</i> .....    | 4-28 |
| Gambar 4.60 Hasil Pengujian <i>Remote Access</i> VPN SSTP pada kategori <i>file large</i> .....     | 4-28 |
| Gambar 4.61 Hasil Pengujian <i>Intranet</i> VPN OpenVPN pada kategori <i>file small</i> .....       | 4-29 |
| Gambar 4.62 Hasil Pengujian <i>Intranet</i> VPN OpenVPN pada kategori <i>file medium</i> .....      | 4-29 |
| Gambar 4.63 Hasil Pengujian <i>Intranet</i> VPN OpenVPN pada kategori <i>file large</i> .....       | 4-29 |
| Gambar 4.64 Hasil Pengujian <i>Remote Access</i> VPN OpenVPN pada kategori <i>file small</i> .....  | 4-29 |
| Gambar 4.65 Hasil Pengujian <i>Remote Access</i> VPN OpenVPN pada kategori <i>file medium</i> ..... | 4-30 |
| Gambar 4.66 Hasil Pengujian <i>Remote Access</i> VPN OpenVPN pada kategori <i>file large</i> .....  | 4-30 |
| Gambar 4.67 Hasil Pengujian <i>Intranet</i> VPN OpenVPN pada kategori <i>file small</i> .....       | 4-31 |
| Gambar 4.68 Hasil Pengujian <i>Intranet</i> VPN OpenVPN pada kategori <i>file medium</i> .....      | 4-31 |
| Gambar 4.69 Hasil Pengujian <i>Intranet</i> VPN OpenVPN pada kategori <i>file large</i> .....       | 4-31 |
| Gambar 4.70 Hasil Pengujian <i>Remote Access</i> VPN OpenVPN pada kategori <i>file small</i> .....  | 4-31 |
| Gambar 4.71 Hasil Pengujian <i>Remote Access</i> VPN OpenVPN pada kategori <i>file medium</i> ..... | 4-32 |
| Gambar 4.72 Hasil Pengujian <i>Remote Access</i> VPN OpenVPN pada kategori <i>file large</i> .....  | 4-32 |
| Gambar 4.73 Hasil Pengujian <i>Intranet</i> VPN OpenVPN pada kategori <i>file small</i> .....       | 4-33 |
| Gambar 4.74 Hasil Pengujian <i>Intranet</i> VPN OpenVPN pada kategori <i>file medium</i> .....      | 4-33 |
| Gambar 4.75 Hasil Pengujian <i>Intranet</i> VPN OpenVPN pada kategori <i>file large</i> .....       | 4-33 |
| Gambar 4.76 Hasil Pengujian <i>Remote Access</i> VPN OpenVPN pada kategori <i>file small</i> .....  | 4-33 |
| Gambar 4.77 Hasil Pengujian <i>Remote Access</i> VPN OpenVPN pada kategori <i>file medium</i> ..... | 4-34 |
| Gambar 4.78 Hasil Pengujian <i>Remote Access</i> VPN OpenVPN pada kategori <i>file large</i> .....  | 4-34 |
| Gambar 4.79 Hasil Pengujian <i>Intranet</i> VPN IPSec pada kategori <i>file small</i> .....         | 4-35 |

|                                                                                                      |      |
|------------------------------------------------------------------------------------------------------|------|
| Gambar 4.80 Hasil Pengujian <i>Intranet</i> VPN IPsec pada kategori <i>file medium</i> .....         | 4-35 |
| Gambar 4.81 Hasil Pengujian <i>Intranet</i> VPN IPsec pada kategori <i>file large</i> .....          | 4-35 |
| Gambar 4.82 Hasil Pengujian <i>Remote Access</i> VPN IPsec pada kategori <i>file small</i> .....     | 4-35 |
| Gambar 4.83 Hasil Pengujian <i>Remote Access</i> VPN IPsec pada kategori <i>file medium</i> .....    | 4-36 |
| Gambar 4.84 Hasil Pengujian <i>Remote Access</i> VPN IPsec pada kategori <i>file large</i> .....     | 4-36 |
| Gambar 4.85 Hasil Pengujian <i>Intranet</i> VPN IPsec pada kategori <i>file small</i> .....          | 4-37 |
| Gambar 4.86 Hasil Pengujian <i>Intranet</i> VPN IPsec pada kategori <i>file medium</i> .....         | 4-37 |
| Gambar 4.87 Hasil Pengujian <i>Intranet</i> VPN IPsec pada kategori <i>file large</i> .....          | 4-37 |
| Gambar 4.88 Hasil Pengujian <i>Remote Access</i> VPN IPsec pada kategori <i>file small</i> .....     | 4-37 |
| Gambar 4.89 Hasil Pengujian <i>Remote Access</i> VPN IPsec pada kategori <i>file medium</i> .....    | 4-38 |
| Gambar 4.90 Hasil Pengujian <i>Remote Access</i> VPN IPsec pada kategori <i>file large</i> .....     | 4-38 |
| Gambar 4.91 Hasil Pengujian <i>Intranet</i> VPN IPsec pada kategori <i>file small</i> .....          | 4-39 |
| Gambar 4.92 Hasil Pengujian <i>Intranet</i> VPN IPsec pada kategori <i>file medium</i> .....         | 4-39 |
| Gambar 4.93 Hasil Pengujian <i>Intranet</i> VPN IPsec pada kategori <i>file large</i> .....          | 4-39 |
| Gambar 4.94 Hasil Pengujian <i>Remote Access</i> VPN IPsec pada kategori <i>file small</i> .....     | 4-40 |
| Gambar 4.95 Hasil Pengujian <i>Remote Access</i> VPN IPsec pada kategori <i>file medium</i> .....    | 4-40 |
| Gambar 4.96 Hasil Pengujian <i>Remote Access</i> VPN IPsec pada kategori <i>file large</i> .....     | 4-40 |
| Gambar 4.97 Grafik Perbandingan Kinerja Protokol VPN pada Pagi Hari .....                            | 4-41 |
| Gambar 4.98 Grafik Perbandingan Kinerja Protokol VPN pada Siang Hari .....                           | 4-41 |
| Gambar 4.99 Grafik Perbandingan Kinerja Protokol VPN pada Sore Hari .....                            | 4-41 |
| Gambar 4.100 <i>Error</i> IPsec .....                                                                | 4-42 |
| Gambar 4.101 Protokol VPN IPsec menggunakan <i>firewall nat action accept</i> tidak diaktifkan ..... | 4-43 |
| Gambar 4.102 Protokol VPN IPsec menggunakan <i>firewall nat action accept</i> di aktifkan. ....      | 4-44 |
| Gambar 4.103 Protokol VPN OpenVPN pada saat <i>firewall nat action accept</i> diaktifkan .....       | 4-45 |
| Gambar 4.104 Protokol VPN SSTP pada saat <i>firewall nat action accept</i> diaktifkan .....          | 4-45 |

## DAFTAR SIMBOL

| Simbol                                                                              | Nama Simbol                 | Keterangan                                                         |
|-------------------------------------------------------------------------------------|-----------------------------|--------------------------------------------------------------------|
|    | Perangkat <i>Smartphone</i> | Mengambarkan perangkat <i>smartphone</i> sebagai <i>VPN client</i> |
|    | <i>BTS / Tower</i>          | Mengambarkan sebuah pemancar sinyal                                |
|    | <i>Switch</i>               | Mengambarkan sebuah perangkat jaringan yaitu <i>switch</i>         |
|    | <i>Server</i>               | Mengambarkan sebuah perangkat jaringan yaitu <i>server</i>         |
|    | Awan                        | Mengambarkan sebuah jaringan Internet                              |
|    | Pipa                        | Mengambarkan sebuah <i>vpn tunneling</i>                           |
|    | Arah Panah                  | Mengambarkan alur komunikasi                                       |
|  | Petir                       | Mengambarkan sebuah media transmisi gelombang radio                |
|  | Garis lurus                 | Mengambarkan sebuah media transmisi kabel                          |

## DAFTAR ISTILAH

| No  | Istilah                    | Keterangan                                                                                                                                        |
|-----|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | <i>Routing</i>             | Pengalamatan secara langsung menuju alamat tujuan tanpa melalui host lain.                                                                        |
| 2.  | <i>Online</i>              | Keadaan komputer yang terkoneksi.                                                                                                                 |
| 3.  | <i>Digital certificate</i> | Digunakan untuk mengidentifikasi secara unik suatu entitas selama transmisi.                                                                      |
| 4.  | <i>Client</i>              | Komputer dalam jaringan yang menggunakan sumber daya yang disediakan oleh server atau pemakai layanan.                                            |
| 5.  | <i>Server</i>              | Suatu sistem komputer yang menyediakan jenis layanan tertentu untuk client dalam suatu jaringan komputer.                                         |
| 6.  | <i>Ip</i>                  | Deretan angka biner antara 32 bit sampai 128 bit yang dipakai sebagai alamat identifikasi untuk tiap komputer host dalam jaringan Internet.       |
| 7.  | <i>Transport</i>           | Komponen utama untuk mencapai misi tersebut.                                                                                                      |
| 8.  | <i>Link</i>                | Referensi yang akan dituju.                                                                                                                       |
| 9.  | <i>Software</i>            | Perangkat lunak.                                                                                                                                  |
| 10. | <i>Hardware</i>            | perangkat keras.                                                                                                                                  |
| 11. | <i>Spoofing</i>            | Teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi.                                                     |
| 12. | <i>Network</i>             | Jaringan dari system komunikasi data.                                                                                                             |
| 13. | <i>Resource</i>            | Sumber daya yang diperlukan.                                                                                                                      |
| 14. | <i>Remote</i>              | Fasilitas yang disediakan untuk dapat berbagi file dan bisa menjalankan komputer satu dari komputer lain dengan syarat terhubung dengan jaringan. |
| 15. | <i>Mobile</i>              | benda yang berteknologi tinggi dan dapat bergerak tanpa menggunakan kabel.                                                                        |
| 16. | <i>Dial-up</i>             | Teknologi informasi untuk akses Internet dengan menggunakan jaringan telepon tetap atau telepon bergerak.                                         |
| 17. | <i>Import</i>              | Pemindahan file.                                                                                                                                  |
| 18. | <i>Connect</i>             | Menghubungkan ke jaringan internet atau lokal.                                                                                                    |
| 19. | <i>Public</i>              | Secara umum atau diketahui oleh semua orang.                                                                                                      |
| 20. | <i>Private</i>             | Secara lokal atau diketahui oleh orang itu sendiri.                                                                                               |
| 21. | <i>Properties</i>          | Suatu tampilan yang terdapat menu-menu pada suatu aplikasi.                                                                                       |
| 22. | <i>General</i>             | Suatu tampilan yang terdapat format pada suatu aplikasi.                                                                                          |