

**IMPLEMENTASI VPN DENGAN METODE PPTP(POINT TO POINT
TUNNELING PROTOCOL) DI KANTOR KECAMATAN SRANDAKAN
BANTUL
SKRIPSI**

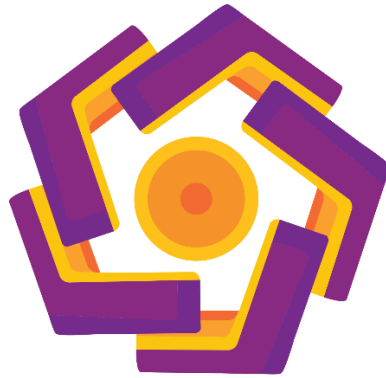


**disusun oleh
Fahreza Adi Saputra
17.11.1022**

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021**

**IMPLEMENTASI VPN DENGAN METODE PPTP(PPOINT TO POINT
TUNNELING PROTOCOL) DI KANTOR KECAMATAN SRANDAKAN
BANTUL**

SKRIPSI



disusun oleh

Fahreza Adi Saputra

17.11.1022

PROGRAM SARJANA

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2021

PERSETUJUAN

SKRIPSI

**IMPLEMENTASI VPN DENGAN METODE PPTP(PPOINT TO POINT
TUNNELING PROTOCOL) DI KANTOR KECAMATAN SRANDAKAN
BANTUL**

yang dipersiapkan dan disusun oleh

Fahreza Adi Saputra
17.11.1022

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 11 Agustus 2021

Dosen Pembimbing,

Ria Andriani, M.Kom

NIK. 190302458

PENGESAHAN
SKRIPSI
IMPLEMENTASI VPN DENGAN METODE PPTP(POINT TO POINT
TUNNELING PROTOCOL) DI KANTOR KECAMATAN

SRANDAKAN BANTUL

yang dipersiapkan dan disusun oleh

Fahreza Adi Saputra

17.11.1022

telah dipertahankan di depan Dewan Penguji

pada tanggal 16 September 2021

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Wahyu Sukestvastama Putra, S.T., M.Eng

NIK. 190302328

Melwin Syafrizal, S.Kom., M.Eng

NIK. 190302327

Ria Andriani, M.Kom

NIK. 190302458

Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar Sarjana Komputer

Tanggal 26 September 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, S.Kom., M.Kom.

NIK. 190302096

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, 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.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggung jawab saya pribadi.

Yogyakarta, 30 September 2021



Fahreza Adi Saputra

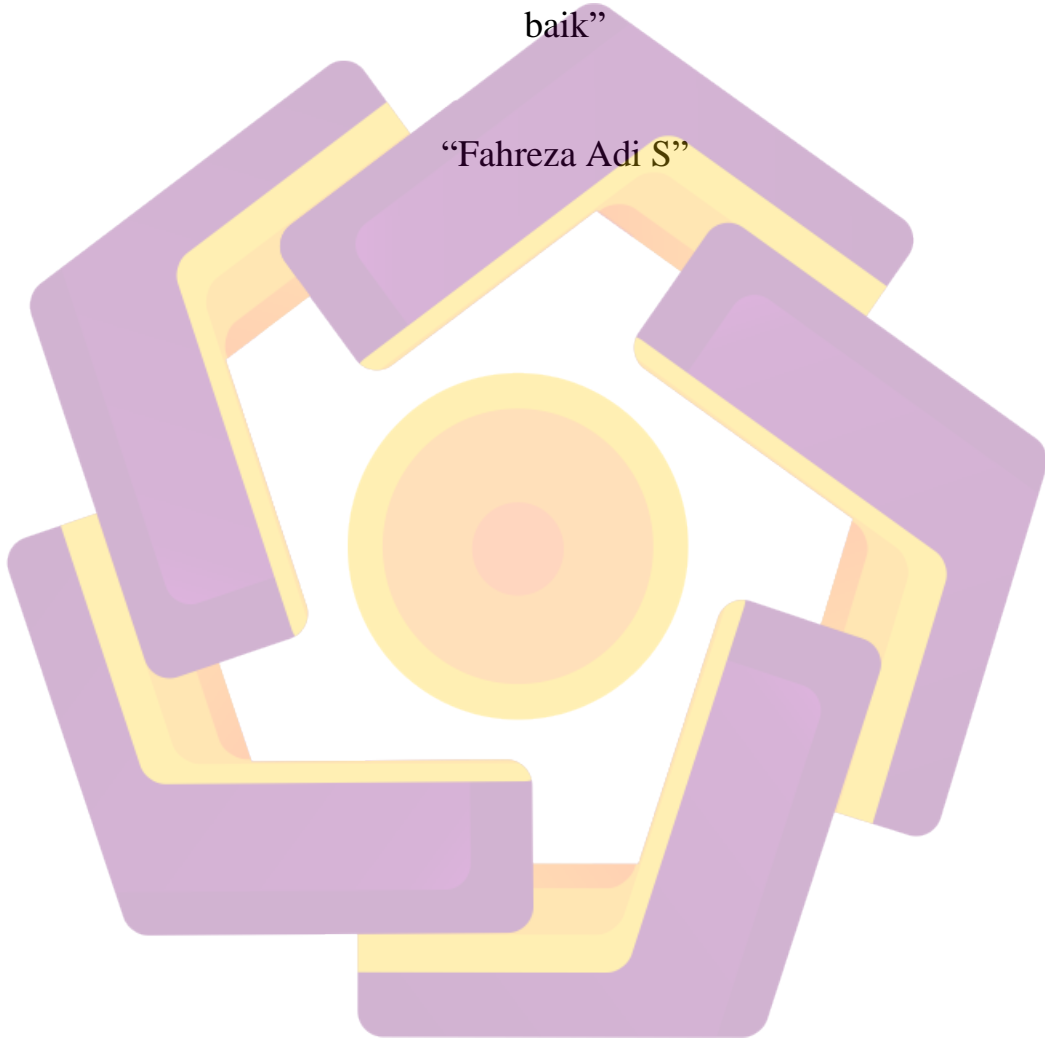
NIM. 17.11.1022

MOTTO

“Slowly But Surely”

“Tetap tenang walaupun banyak masalah yang datang silih berganti tetapi tetap semangat walaupun hanya sedikit perubahan yang lebih baik”

“Fahreza Adi S”



PERSEMBAHAN

Puji syukur kita panjatkan kehadirat Allah SWT atas berkah dan karunia-Nya skripsi ini dapat terselesaikan dengan baik dan lancar. Dengan ini saya persembahkan skripsi ini untuk semua pihak yang terlibat langsung maupun tidak langsung, yaitu kepada :

1. Kepada orang tua dan teman-teman saya yang terus memberikan semangat serta doa hingga saya dapat menyelesaikan tugas akhir/skripsi.
2. Dosen pembimbing ibu Ria Andriani, M.Kom yang terhormat senantiasa membimbing saya dari awal hingga akhir skripsi ini terselesaikan.
3. Dosen-dosen Universitas Amikom Yogyakarta yang telah memberikan ilmu serta bimbingan kepada saya selama perkuliahan.
4. Pihak Kantor Kecamatan Srandakan yang telah mengizinkan saya untuk melakukan penelitian ini sehingga berjalan dengan lancar.
5. Teman-teman Universitas Amikom Yogyakarta yang khususnya kelas 17-IF-02 yang telah menemani saya dan memberikan semangat serta membantu dalam pengerjaan skripsi ini.
6. Teman-teman Tuyak Bangkit, Wahyu, Firza, Ilham, Ana, Lutfi, Ica, Aul, Nia, Vita, dan Khususnya untuk Renaldi yang selalu memberikan petuah dan wejangan sehingga saya bisa menyelesaikan skripsi ini.
7. Teman-teman squad Mobile Legend Irsyad, Farhan, Bunga, Renaldi, Lupek, Firza, dan Bangkit yang selalu solid dalam bermain.
8. *Last but not least, I wanna thank me, for believing in me, for doing all this hard work, for having no days off, for never quitting, for just being me at all times.*

KATA PENGHANTAR

Puji syukur penulis ucapkan kepada Allah SWT, yang mana telah memberikan kesehatan dan karunia-Nya kepada penulis serta kekuatan untuk menyelesaikan skripsi yang berjudul “ **IMPLEMENTASI VPN DENGAN METODE PPTP(POINT TO POINT TUNNELING PROTOCOL) DI KANTOR KECAMATAN SRANDAKAN BANTUL**”. Tidak lupa penulis mengucapkan shalawat dan salam kepada junjungan Nabi Besar Muhammad SAW. Penyelesaian tulisan ini terlepas bantuan dari berbagai pihak yang terkait secara langsung maupun tidak langsung, terutama dan teristimewa dipersembahkan kepada kedua orang tua tercinta yang senantiasa memberikan rasa sayang, didikan, serta doa yang selalu di panjatkan pada Allah kepada penulis.

Skripsi ini dapat terselesaikan dengan bantuan berbagai pihak, maka dari itu penulis menyatakan rasa hormat dan terimakasih kepada:

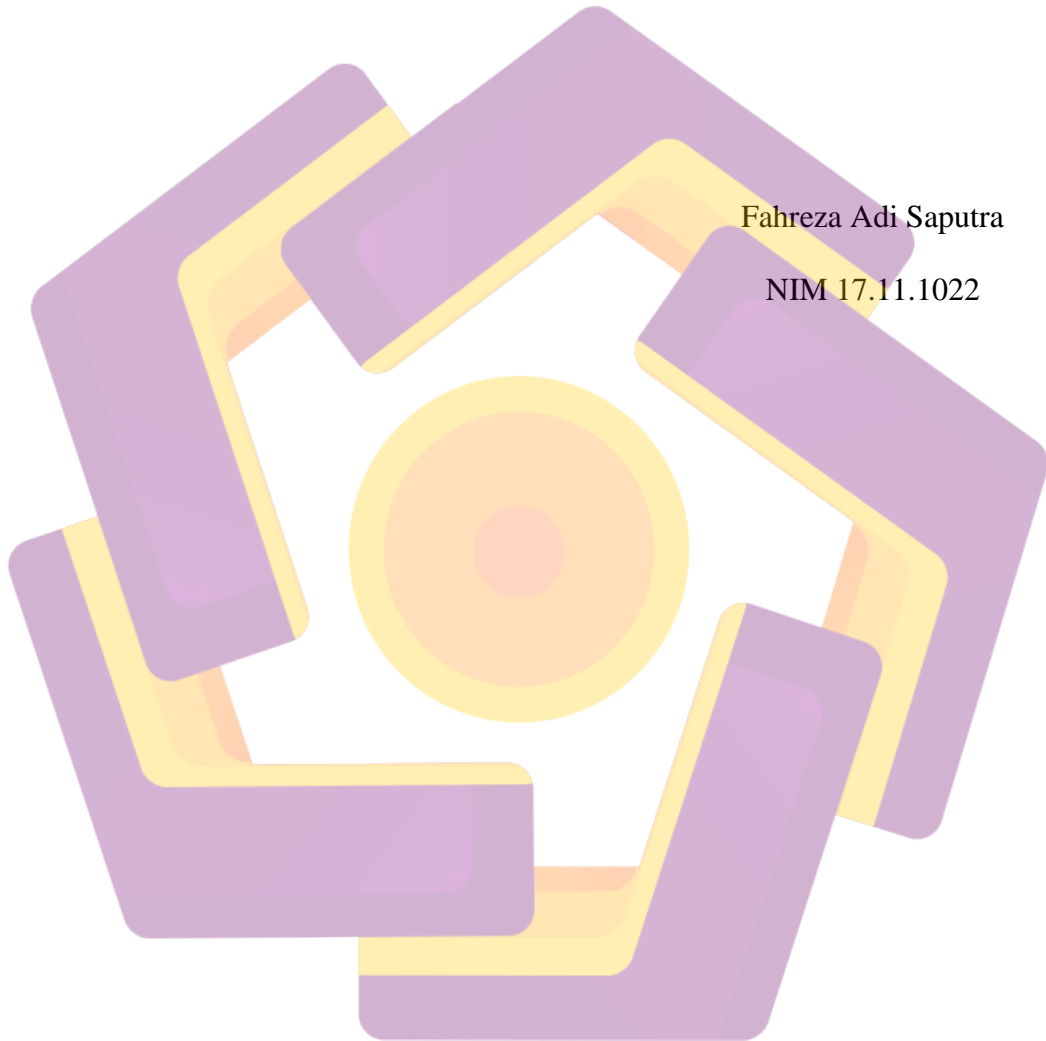
1. Prof. Dr. M. Suyanto, MM. selaku Rektor Universitas AMIKOM Yogyakarta.
2. Bapak Hanif Al Fatta, S.Kom., M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
3. Ibu Windha Mega Pradnya D, M.Kom selaku ketua Program Studi Informatika Universitas AMIKOM Yogyakarta.
4. Ria Andriani, M.Kom selaku pembimbing yang senantiasa memberikan masukan serta nasihat dalam penulisan skripsi ini.
5. Bapak Wahyu Sukestyastama Putra, S.T., M.Eng dan Bapak Melwin Syafrizal, S.Kom., M.Eng selaku dosen penguji, terima kasih atas saran dan kritiknya sehingga penelitian ini menjadi lebih baik lagi.

Penulis menyadari masih ada kekurangan dan kelemahan dalam pembuatan skripsi ini. Maka penulis mengharapkan adanya kritik dan saran dari segala pihak agar menambah kesempurnaan dalam skripsi ini.

Yogyakarta, 26 September 2021

Fahreza Adi Saputra

NIM 17.11.1022



DAFTAR ISI

PERSETUJUAN	iii
PENGESAHAN	iv
MOTTO	vi
PERSEMBAHAN	vii
KATA PENGHANTAR	viii
DAFTAR ISI	x
DAFTAR GAMBAR	xiv
DAFTAR TABEL	xviii
INTISARI	xix
ABSTRACT	xx
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Maksud dan Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	4
1.6 Metode Penelitian.....	4
1.6.1 Analisa Penelitian.....	4
1.6.2 Metode Pengumpulan Data.....	5

1.7	Sistematika Penulisan.....	6
BAB II LANDASAN TEORI.....		8
2.1	Kajian Pustaka.....	8
2.2	Landasan Teori.....	13
2.2.1	Jaringan Komputer.....	13
2.2.2	Internet.....	13
2.2.3	Pengertian Mikrotik RouterOS.....	13
2.2.4	Virtual Private Network.....	15
2.2.5	Fungsi VPN.....	16
2.2.6	Jenis VPN.....	17
2.2.7	Point-to-Point Tunneling Protocol (PPTP).....	18
2.2.8	Tunneling.....	19
2.2.9	Enkripsi.....	19
2.2.11	Ping.....	20
2.2.12	CMD.....	20
2.2.13	Winbox.....	20
2.2.14	Wireshark.....	21
2.2.15	FreeNAS.....	21
2.2.16	Sniffing.....	21
BAB III ANALISA DAN PERANCANGAN.....		23

3.1	Deskripsi Perusahaan	23
3.2	Identifikasi Masalah	23
3.3	Alur Penelitian.....	24
3.3.1	Metode Pengumpulan Data.....	25
3.3.2	Pengumpulan Data	26
3.5	Alat dan Bahan	26
3.5.1	Perangkat Keras	27
3.5.2	Perangkat Lunak.....	30
3.6	Perancangan Jaringan	31
3.6.1	Denah Jaringan.....	31
3.6.2	Perancangan Jaringan Sebelum Menggunakan VPN.....	31
3.6.3	Perancangan Jaringan Setelah Menggunakan VPN.....	32
3.7	Skenario Pengujian.....	35
3.8	Monitoring.....	35
3.9	Management	35
BAB IV IMPLEMENTASI DAN PEMBAHASAN.....		37
4.1	Implementasi	37
4.1.1	Konfigurasi Mikrotik Dasar	37
4.1.2	Konfigurasi VPN Server	43
4.1.3	Instalasi Storage Server.....	48

4.2	Pengujian	55
4.2.1	Pengujian Koneksi VPN Client dan Akses File Server	55
4.2.2	Pengujian Keamanan Sebelum dan Setelah VPN	62
4.3	Hasil Pengujian Dan Pembahasan	75
4.3.1	Hasil Pengujian Konektifitas Pada VPN Server dan File Server....	75
4.3.2	Hasil Perbandingan Keamanan Sebelum dan Setelah Menggunakan VPN	76
4.4	Monitoring	78
4.5	Management	79
BAB V KESIMPULAN DAN SARAN		81
5.1	Kesimpulan.....	81
5.2	Saran.....	82
Daftar Pustaka.....		lxxxiii
LAMPIRAN.....		lxxxv

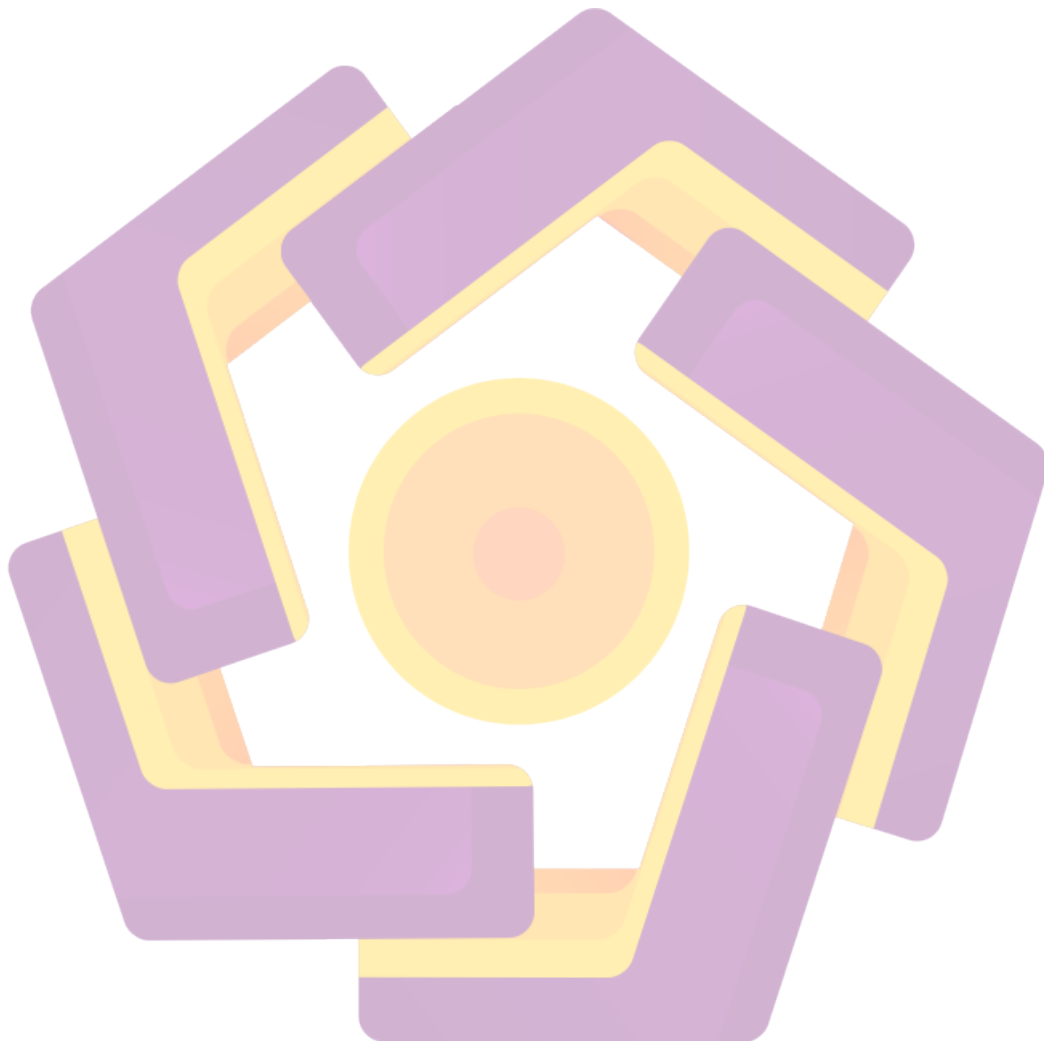
DAFTAR GAMBAR

Gambar 2. 1 RouterBoard RB941-2nd-TC (sumber: mikrotik.co.id)	14
Gambar 2. 2 Contoh Jaringan VPN source : (mikrotik.co.id)	16
Gambar 3. 1 Struktur Kecamatan Srandakan	23
Gambar 3. 2 Alur Penelitian	25
Gambar 3. 3 Topologi Jaringan Kantor Kecamatan Srandakan	31
Gambar 3. 4 Topologi Sebelum Perancangan	32
Gambar 4. 1 Konfigurasi IP Address Pada Address List	37
Gambar 4. 2 Konfigurasi NAT	38
Gambar 4. 3 Menu Action Dalam Konfigurasi NAT	38
Gambar 4. 4 Konfigurasi destination NAT	39
Gambar 4. 5 Menu Action pada destination NAT	40
Gambar 4. 6 Konfigurasi DHCP Client	40
Gambar 4. 7 Tampilan Address list setelah konfigurasi DHCP client	41
Gambar 4. 8 Uji koneksi pada menu terminal dengan melakukan ping pada DNS Google	41
Gambar 4. 9 Konfigurasi DHCP server untuk Interface Bridge	42
Gambar 4. 10 Konfigurasi Routing Static	43
Gambar 4. 11 Konfigurasi PPTP Server	44
Gambar 4. 12 Membuat IP Pool VPN Server	45
Gambar 4. 13 Menambahkan IP Address Pada Pool	45
Gambar 4. 14 Membuat PPP Profile	46
Gambar 4. 15 Service PPTP	46

Gambar 4. 16 Membuat User VPN	47
Gambar 4. 17 Tampilan Web GUI FreeNAS	48
Gambar 4. 18 Membuat Akun Group	49
Gambar 4. 19 Tampilan Group Setelah Dibuat	50
Gambar 4. 20 Membuat User pada FreeNAS	50
Gambar 4. 21 Tampilan User setelah jadi	51
Gambar 4. 22 Menambahkan Dataset pada Menu Pool	52
Gambar 4. 23 Tampilan Setelah Dataset Selesai Dibuat	53
Gambar 4. 24 Menambahkan Sharing SMB	53
Gambar 4. 25 Tampilan Sharing SMB Setelah Dibuat	54
Gambar 4. 26 Mengaktifkan Service SMB Pada FreeNAS	54
Gambar 4. 27 Menambahkan VPN connection pada Windows	55
Gambar 4. 28 Form Login VPN pada Windows	56
Gambar 4. 29 Client Terkoneksi ke VPN Server	56
Gambar 4. 30 Tampilan IP Address VPN Client	57
Gambar 4. 31 Ping dari Client ke Server VPN	57
Gambar 4. 32 Ping dari Server VPN ke Client	58
Gambar 4. 33 Mengkoneksikan File Server	58
Gambar 4. 34 Form Login Credential Windows	59
Gambar 4. 35 Tampilan File Sharing setelah login	59
Gambar 4. 36 Pengujian Hak Akses sesuai foldernya	60
Gambar 4. 37 Pengujian Hak Akses ketika tidak sesuai foldernya	60
Gambar 4. 38 Ping dari Client ke File Server	61

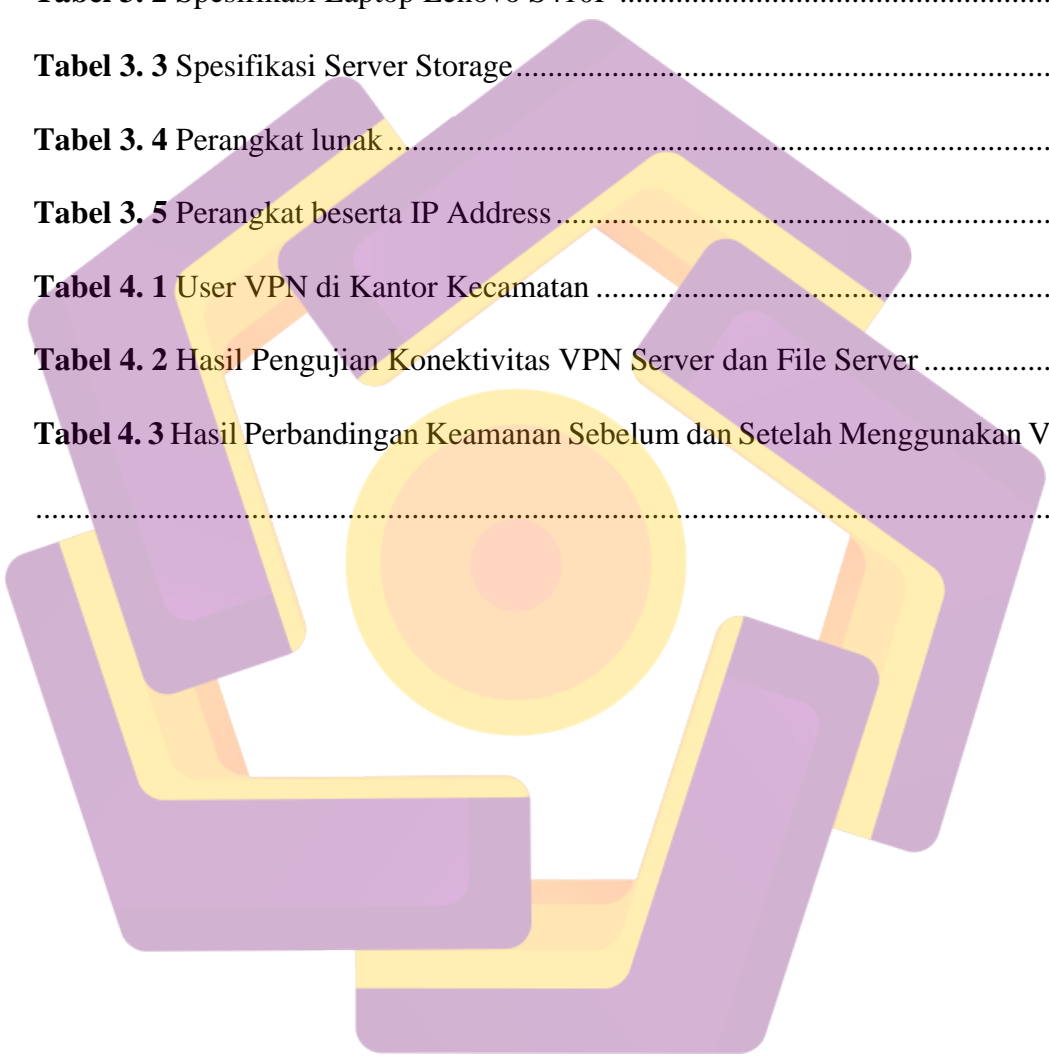
Gambar 4. 39 Ping dari File Server ke Client.....	61
Gambar 4. 40 Flowchart Pengujian Keamanan Jaringan Login Website.....	62
Gambar 4. 41 User Mengakses Login Website	63
Gambar 4. 42 Scan Traffik saat User Melakukan Login Website.....	63
Gambar 4. 43 Memfilter target dan protokol yang ditangkap	64
Gambar 4. 44 Hasil paket yang tertangkap saat user login	65
Gambar 4. 45 Sniffing Data Melalui Koneksi VPN.....	66
Gambar 4. 46 Memfilter protokol yang ditangkap melewati VPN	66
Gambar 4. 47 Flowchart Pengujian Admin Jaringan Login ke WebFig Mikrotik	67
Gambar 4. 48 Admin Jaringan Saat Login Mikrotik WebFig	68
Gambar 4. 49 Scan Traffik saat Admin Jaringan Melakukan Login Mikrotik WebFig.....	68
Gambar 4. 50 Hasil paket yang tertangkap saat admin Jaringan login Mikrotik	69
Gambar 4. 51 Memfilter protokol yang ditangkap Melewati VPN.....	69
Gambar 4. 52 Memfilter protokol yang ditangkap Saat Login Mikrotik Melewati VPN.....	70
Gambar 4. 53 Flowchart Pengujian User Mengirimkan File ke File Server	71
Gambar 4. 54 File Uji Coba Dikirim ke File Server	71
Gambar 4. 55 Scan Traffik saat User Mengirimkan File Ke Server	72
Gambar 4. 56 Memfilter protokol yang ditangkap.....	73
Gambar 4. 57 Hasil Sniffing saat User mengirim File Ke Server	73
Gambar 4. 58 Scan Traffik Saat User Mengirimkan File Melalui Koneksi VPN	74

Gambar 4. 59 Memfilter protokol yang ditangkap Melalui Koneksi VPN	75
Gambar 4. 60 Monitoring Kondisi Jaringan Kantor Srandakan.....	78
Gambar 4. 61 Backup Konfigurasi Mikrotik.....	79
Gambar 4. 62 Log System Pada Mikrotik	80



DAFTAR TABEL

Tabel 2. 1 Perbandingan Penelitian	11
Tabel 3. 1 Spesifikasi Mikrotik RB 941-2nD-TC	27
Tabel 3. 2 Spesifikasi Laptop Lenovo S410P	28
Tabel 3. 3 Spesifikasi Server Storage	29
Tabel 3. 4 Perangkat lunak	30
Tabel 3. 5 Perangkat beserta IP Address	33
Tabel 4. 1 User VPN di Kantor Kecamatan	47
Tabel 4. 2 Hasil Pengujian Konektivitas VPN Server dan File Server	75
Tabel 4. 3 Hasil Perbandingan Keamanan Sebelum dan Setelah Menggunakan VPN	76



INTISARI

Kantor Kecamatan Srandakan Bantul merupakan salah satu Instansi Pemerintah Daerah Bantul yang mencakup berbagai bidang, seperti bidang pemerintahan, ekonomi, pembangunan, kesejahteraan rakyat, pembinaan kehidupan masyarakat serta urusan pelayanan umum. Namun kegiatan bekerja di instansi terganggu karena adanya pandemi COVID-19 yang menyebabkan pemerintah memberlakukan kebijakan Pembatasan Sosial Berskala Besar (PSBB) untuk menekan penyebaran virus ini sehingga mengakibatkan pekerja instansi harus bekerja dari rumah atau biasa disebut *Work From Home* (WFH). Oleh karena itu dibutuhkan suatu sarana yang dapat mendukung kegiatan tersebut. Salah satunya adalah dengan membuat rancangan teknologi VPN.

Sedangkan pada penelitian ini akan dibangun sebuah jaringan VPN menggunakan *router* Mikrotik dengan metode PPTP (*Point to Point Tunneling Protocol*) sehingga dapat mempermudah karyawan dalam berkomunikasi tanpa memikirkan lokasi, Selain itu *user* masih bisa melakukan *remote access* jaringan lokal meskipun berada di luar jaringan kantor. Tidak hanya itu keamanan juga lebih terjamin.

Berdasarkan hasil pengujian terhadap keamanan jaringan di Kantor Kecamatan Srandakan Bantul sebelum menggunakan VPN Server membuktikan bahwa penyadapan penyerang masih bisa memperoleh data berupa informasi login website, login mikrotik, maupun melihat isi data Ketika melakukan pertukaran data. Sedangkan Ketika user mengkoneksikan VPN Server penyadap tidak dapat melihat isi data di dalamnya, kemudian dengan adanya penerapan VPN dengan metode PPTP karyawan yang sedang bekerja dari rumah atau work form home dapat saling berkomunikasi, dengan itu pekerjaan dan pertukaraan informasi akan menjadi semakin fleksibel dan semakin cepat.

Kata Kunci : *Virtual Private Network, Point to Point Tunneling Protocol, Mikrotik*

ABSTRACT

The Srandakan Bantul District Office is one of the Bantul Regional Government Agencies that covers various fields, such as the fields of government, economy, development, people's welfare, community life development and public service affairs. However, work activities in agencies were disrupted due to the COVID-19 pandemic which caused the government to impose a Large-Scale Social Restriction (PSBB) policy to suppress the spread of this virus, resulting in agency workers having to work from home or commonly called Work From Home (WFH). Therefore we need a facility that can support these activities. One of them is by designing VPN technology.

While in this study, a VPN network will be built using a Mikrotik router with the PPTP (Point to Point Tunnelling Protocol) method so that it can make it easier for employees to communicate without thinking about location. In addition, users can still remotely access the local network even though they are outside the office network. Not only that, security is also more guaranteed.

Based on the test results on network security at the Srandakan Bantul District Office before using the VPN Server, it proved that the wiretapping attackers could still obtain data in the form of website login information, proxy logins, or view data contents when exchanging data. Meanwhile, when the user connects to the VPN Server, the eavesdropper cannot see the contents of the data in it, then with the application of a VPN with the PPTP method, employees who are working from home or work form home can communicate with each other, with that work and information exchange will become more flexible and faster.

Keyword : Virtual Private Network , Point to Point Tunneling Protocol, Mikrotik