

PROGRAM STUDI TEKNIK KOMPUTER

RANCANGAN DAN IMPLEMENTASI JARINGAN VPN SIMULASI CISCO

PAKET TRACER PADA PT.PUTRA PUTRIPERKASA

TORANDO

181460049

Tugas Akhir Ini Diajukan Sebagai Syarat Untuk Mengikuti Ujian

Komprehensif Pada Fakultas Vokasi Program Studi Teknik Komputer

Universitas Bina Darma



FAKULTAS VOKASI

UNIVERSITAS BINA DARMA

PALEMBANG

2023



**RANCANGAN DAN IMPLEMENTASI JARINGAN VPN SIMULASI CISCO
PAKET TRACER PADA PT.PUTRA PUTRIPERKASA**

**TORANDO
181460049**

**Tugas Akhir Ini Diajukan Sebagai Syarat Untuk Mengikuti Ujian
Komprehensif Pada Fakultas Vokasi Program Studi Teknik Komputer**

Universitas Bina Darma

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS VOKASI

UNIVERSITAS BINA DARMA

PALEMBANG

2023

HALAMAN PENGESAHAN

RANCANGAN DAN IMPLEMENTASI JARINGAN VPN SIMULASI CISCO PAKET TRACER PADA PT.PUTRA PUTRI

PERKASA

TORANDO

181460049

Telah diterima sebagai salah satu syarat untuk memperoleh gelar
Ahli Madya pada Program Studi Teknik Komputer

Palembang, September 2023

Fakultas Vokasi

Universitas Bina Darma

Dekan,



Dr. A. Yani Ranius, S.Kom., M.M.

Pembimbing

Irwansyah, M.M., M.Kom

HALAMAN PERSETUJUAN

**Tugas akhir yang berjudul ‘RANCANGAN DAN IMPLEMENTASI
JARINGAN VPN SIMULASI CISCO PAKET TRACER PADA PT.PUTRA
PUTRIPERKASA’**

Komisi Pengaji

- 1. Irwansyah,M.M., M.Kom**
- 2. Misinem, S. Kom., M.Si.**
- 3. Rahmat Novrianda Dasmen , S.T., M.Kom.**

Mengetahui,
Program Studi Teknik Komputer
Fakultas Vokasi
Universitas Bina Darma
Ketua,



Timur Dali Purwanto, M. Kom

SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini

Nama : Torando
Nim : 181460049

Dengan ini menyatakan bahwa :

1. Dengan tugas akhir ini adalah hasil dan belum pernah diajukan untuk mendapatkan gelar akademik baik ahli madya di Universitas Bina Darma Palembang atau perguruan tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian saya sendiri dengan arahan pembimbing.
3. Di dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau di publikasikan orang lain, secara tulis dengan jelas dikutip dengan mencantumkan nama pengarang dan memasukan ke daftar rujukan.
4. Saya bersedia tugas akhir, yang saya hasilkan dicek keasliannya menggunakan plagiarism checker diunggah ke internet sehingga dapat diakses publik secara daring.
5. Surat pernyataan ini saya tulis dengan sungguh-sungguh dan apabila terbukti melakukan penyimpangan ketidak benaran dengan peraturan dan perundang-undangan yang berlaku.

Demikian surat pernyataan ini saya buat agar dapat digunakan sebagaimana mestinya

Palembang, 12 Septembaer 2023



181460049

MOTTO DAN PERSEMPAHAN

1.1 MOTTO :

“Barang siapa yang mempelajari ilmu pengetahuan yang seharusnya yang ditunjukan untuk mencari ridho Allah bahkan hanya untuk mendapat kedudukan/kekayaan dunia ini maka ia tidak akan mendapatkan baunya surga nanti pada hari kiamat (riwayat Abu Hurairah radhiyallah anhu) ”.

1.2 PERSEMPAHAN :

1. *Kedua orang tuaku tercinta, yang selalu memberikan semangat dan do`a dalam setiap langkahku.*
2. *Semua dosen Universitas Bina Darma palembang dan terutama dosenpembimbing.*
3. *Orang terdekat dikeliling peneliti, teman-teman kelas yang telah membantu dalam semua bidang mata kuliah hingga sampai menyelesaikan tugas akhir ini.*

ABSTRAK

VPN (Virtual Private Network) dalam implementasinya terbagi dua jenis yaitu VPN remote access dan site-to-site VPN. VPN Remote access adalah VPN yang digunakan untuk meremote server atau host private dengan aman melalui jaringan publik. Sedangkan VPN site-to-site digunakan untuk menghubungkan jaringan yang memiliki jarak yang cukup jauh melalui jaringan publik sehingga seakan berada pada satu jaringan local, misal antara PT. Putra Putri Perkasa, Cabang KM.14, dan Cabang Air Batu. Dalam kasus ini terjadinya komunikasi atau sharing data antara PT. Putra Putri Perkasa, Cabang KM.14, dan Cabang Air Batu melalui teknologi VPN (VirtualPrivate Network) site to site, tentunya membutuhkan sebuah scurity(keamanan) untuk menjaga kerahasiaan data-data tersebut. Protokol keamanan Internet Protocol Security (IPSec) merupakan protokol keamanan mampu memenuhi kriteria dukungan keamanan dan mememiliki tingkat keamanan yang lebih baik yang paling banyak digunakan untuk meningkatkan keamanan VPN site to site yang ada di PT. Pertamina Ubebe Adera Pengabuan.

Kata Kunci - IPSec; VPN; Sharing; Host Private.

KATA PENGANTAR

Puji dan syukur kita haturkan kehadiran Allah SWT yang telah melimpahkan hidayah dan rahmat-Nya yang memberikan banyak kesempatan. Laporan tugas akhir ini disusun untuk melengkapi salah satu syarat dalam menyelesaikan gelar bagi mahasiswa program studi Diploma III (tiga), Universitas Bina Darma. Adapun judul tugas akhir yang saya ajukan adalah “Rancangan dan Implementasi Jaringan VPN Simulasi Cisco Paket Tracer pada PT.Putra Putri Perkasa”

Terima kasih kepada berbagai pihak yang turut memiliki andil besar dan penyelesaian penelitian penelitian ini, peneliti sangat sadar sepenuhnya bahwa laporan penelitian ini tidak terlepas dari bimbingan, semangat, serta dukungan dari banyak pihak, baik bersifat moril ataupun materil, pihak-pihak tersebut antara lain:

1. Dr. Sunda Ariana, M.pd., MM. selaku rektor Bina Darma palembang.
2. Dr. A. Yani Ranius, S.kom. M.M selaku dekan Vokasi Bina Darma Palembang.
3. Timur Dali Purwanto, M.Kom. selaku ketua program studi Teknik Komputer Bina Darma Palembang.
4. Kedua Orang tua yang selalu senantiasa mendoakan dan memberikan dukungan, serta nasehat kepada peneliti sehingga menyelesaikan laporan ini.
5. Semua pihak yang tidak bisa disebutkan namanya satu persatu yang telah membantu Penelitian tugas akhir ini.

Peneliti menyadari bahwa laporan tugas akhir ini masih memiliki banyak kekurangan. Oleh sebab itu, diharapkan kritik dan saran yang membangun dan bermanfaat untuk menyempurnakan laporan ini. Semoga tugas akhir ini dapat berguna untuk memberikan manfaat bagi yang membacanya

Palembang, 26 Agustus 2023

Peneliti

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN.....	ii
HALAMAN PERSETUJUAN	iii
SURAT PERNYATAAN	iv
MOTTO DAN PERSEMBAHAN	v
ABSTRAK	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	viii
DAFTAR TABLE	xiii
DAFTAR GAMBAR.....	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	4
1.6 Metodologi Penelitian	4
1.6.1 Tempat penelitian dan Waktu Penelitian	4
1.6.2 Metode Pengumpulan Data.....	5
1.6.3 Metode Penelitian	5
1.7 Sistematika Penulisan.....	6
BAB II TINJAUAN PUSTAKA	8
2.1 Tinjauan Umum Perusahaan	8
2.1.1 Sejarah Singkat PT. Putra putri perkasa	8
2.1.2 Struktur Organisasi	8
2.1.3 Visi dan Misi PT. Putra Putri Perkasa	9

2.2	Landasan Teori.....	9
2.2.1	VPN (Virtual Private Network)	10
2.2.2	Keamanan Jaringan VPN.....	10
2.2.3	Fungsi VPN.....	11
2.2.4	Manfaat Keamanan Jaringan VPN.....	12
2.2.5	Jenis-jenis VPN.....	12
2.3	Keamanan Jaringan	14
2.4	Pengertian jaringan komputer	16
2.5	Jenis-Jenis Perangkat Jaringan Komputer.....	16
2.5.1	LAN Card.....	17
2.5.2	Hub.....	17
2.5.3	Repeater	18
2.5.4	Bridge.....	18
2.5.5	Switch	18
2.5.6	Router.....	18
2.5.7	Keamanan Jaringan Komputer.....	18
2.6	Aspek Aspek Keamanan Jaringan Komputer.....	19
2.7	Aspek Aspek Ancaman Keamanan	21
2.8	Penelitian Sebelumnya	22
	BAB III ANALISIS DAN PERANCANGAN.....	24
3.1	Analisa.....	24
3.1.1	Topologi Jaringan	24
3.1.2	Topologi Jaringan Fisik	25
3.1.3	Topologi Jaringan Logic	28
3.2	Keamanan Jaringan	29
3.3	Spesifikasi Perangkat Lunak	29

3.4	Desain Jaringan VPN	30
3.5	Topologi jaringan vpn dengan menggunakan simulasi packet tracer	32
3.6	IP Address Jaringan LAN di Kantor PT. Putra Putri Perkasa.....	33
BAB IV HASIL DAN PEMBAHASAN		34
4.1	Perancangan	34
4.2	Setting Ip Address	35
4.2.1	Konfigurasi Router PT. Putra Putri Perkasa	35
4.2.2	Konfigurasi Router Cabang KM.14	38
4.2.3	Konfigurasi Router Cabang Airbatu	42
BAB V PENUTUP.....		56
5.1	Kesimpulan	56
5.2	Saran.....	56

DAFTAR TABEL

Tabel 1 Spesifikasi Perangkat	27
Tabel 2 IP address Pada PT.Putra Putri Perkasa	28
Table 3 Routing Cisco.....	29
Tabel 4 Perangkat Lunak.....	30
Tabel 5 <i>Device / Hardware</i>	30
Tabel 6 Ip Address PT. Putra Putri Perkasa	33

DAFTAR GAMBAR

Gambar 2.1 Stuktur Organisasi	9
Gambar 3.1 Topologi jaringan	25
Gambar 3.2 topologi jaringan PT.Putra Putri Perkasa	31
Gambar 3.3 Simulasi packet tracer.....	32
Gambar 4.1 Skema Jaringan Usulan	34
Gambar 4.2 Konfigurasi Hostname.....	35
Gambar 4.3 Konfigurasi Ip Address.....	35
Gambar 4.4 Konfigurasi isakmp Policy	36
Gambar 4.5 konfiguraso Isakmp Secretkey	36
Gambar 4.6 Konfigurasi IPSEC-MAP	37
Gambar 4.7 Konfigurasi IPSEC-MAP	37
Gambar 4.8 Konfigurasi Ip Router.....	38
Gambar 4.9 Konfigurasi hostname.....	38
Gambar 4.10 Konfigurasi Ip Address.....	38
Gambar 4.11 Konfigurasi List Permit	39
Gambar 4.12 Konfigurasi Isakmp Policy	39
Gambar 4.13 Konfigurasi Isakmp Policy	40
Gambar 4.14 Konfigurasi Ipsec -Map.....	40
Gambar 4.15 Konfigurasi Ipsec-Map.....	41
Gambar 4.16 Konfigurasi Ip Router.....	41
Gambar 4.17 Konfigurasi Hostname.....	42
Gambar 4.18 Konfigurasi Ip Address.....	42

Gambar 4.19 Konfigurasi Access-List Permit	43
Gambar 4.20 Konfigurasi isakmp Policy	43
Gambar 4.21 Konfigurasi Secret Key	43
Gambar 4.22 Konfigurasi Ipsec-Map.....	44
Gambar 4.23 Konfigurasi Ipsec-Map.....	44
Gambar 4.24 Konfigurasi Ip Router.....	45
Gambar 4.25 Konfigurasi Hostname.....	45
Gambar 4.26 Konfigurasi Ip Address.....	46
Gambar 4.27 Konfigurasi Ip Router.....	46
Gambar 4.28 Ping Paket Loss	48
Gambar 4.29 Ping Paket Loss	48
Gambar 4.30 Ping Paket Loss	49
Gambar 4.31 Ping DOS Paket	49
Gambar 4.32 Pengiriman Paket.....	50
Gambar 4.33 Pengiriman Paket	50
Gambar 4.34 Hasil Pembuatan Routing	51
Gambar 4.35 Packet Loss Jaringan VPN	51
Gambar 4.36 Trace Route VPN	52
Gambar 4.37 Denial of Service Jaringan VPN.....	53
Gambar 4.38 Pengiriman Paket Jaringan VPN	54