

SKRIPSI

**ANALISIS KEAMANAN JARINGAN *VIRTUAL PRIVATE NETWORK (VPN)*
DENGAN METODE *SOURCE SOCKET TUNELLING PROTOCOL(SSTP)*
STUDI KASUS: **BMKG JAMBI****

***VIRTUAL PRIVATE NETWORK (VPN) ANALYSIS WITH SOURCE SOCKET
TUNELLING PROTOCOL (SSTP) METHOD CASE STUDY: BMKG JAMBI***



Disusun oleh :
Riza Ovit Dianasari
18101173

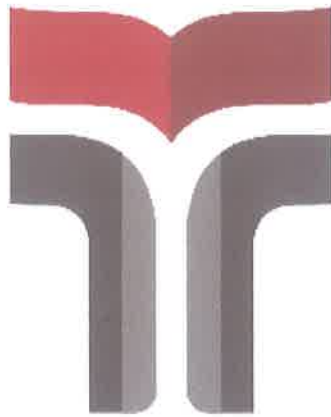
**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO INSTITUT
TEKNOLOGI TELKOM PURWOKERTO**

2022

SKRIPSI

**ANALISIS KEAMANAN JARINGAN *VIRTUAL PRIVATE NETWORK (VPN)*
DENGAN METODE *SOURCE SOCKET TUNELLING PROTOCOL(SSTP)*
STUDI KASUS: **BMKG JAMBI****

***VIRTUAL PRIVATE NETWORK (VPN) ANALYSIS WITH SOURCE SOCKET
TUNELLING PROTOCOL (SSTP) METHOD CASE STUDY: BMKG JAMBI***



Disusun oleh :

Riza Ovit Dianasari

18101173

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO INSTITUT
TEKNOLOGI TELKOM PURWOKERTO**

2022

**ANALISIS KEAMANAN JARINGAN *VIRTUAL PRIVATE NETWORK (VPN)*
DENGAN METODE *SOURCE SOCKET TUNELLING PROTOCOL (SSTP)*
STUDI KASUS: BMKG JAMBI**

***VIRTUAL PRIVATE NETWORK (VPN) ANALYSIS WITH SOURCE SOCKET
TUNELLING PROTOCOL (SSTP) METHOD CASE STUDY: BMKG JAMBI***

**Skripsi ini digunakan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Teknik (S.T.)
Di Institut Teknologi Telkom Purwokerto
2022**

Disusun oleh :
Riza Ovit Dianasari
18101173

DOSEN PEMBIMBING
Jafaruddin Gusti Amri Ginting, S.T., M.T
Irmayatul Hikmah, S.Si., M.Si.

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO INSTITUT
TEKNOLOGI TELKOM PURWOKERTO
2022**

HALAMAN PENGESAHAN
ANALISIS KEAMANAN JARINGAN *VIRTUAL PRIVATE NETWORK* (VPN)
DENGAN METODE *SOURCE SOCKET TUNELLING PROTOCOL* (SSTP)
STUDI KASUS: BMKG JAMBI

VIRTUAL PRIVATE NETWORK (VPN) ANALYSIS WITH SOURCE SOCKET
TUNELLING PROTOCOL (SSTP) METHOD CASE STUDY: BMKG JAMBI





Disusun oleh :

Riza Ovit Dianasari

18101173

Telah dipertanggungjawabkan di hadapan Tim Penguji pada tanggal 28 Juni 2022

Susunan Tim Penguji:

Pembimbing Utama	: <u>Jafaruddin Gusti Amri Ginting, S.T., M.T.</u> 
	NIDN. 0620108901
Pembimbing Pendamping	: <u>Irmayatul Hikmah, S.Si., M.Si.</u> 
	NIDN. 0610069301
Penguji 1	: <u>Kukuh Nugraha S.T., M.T.</u> 
	NIDN.0606088303
Penguji 2	: <u>Reni Dyah Wahyuningrum, S.T., M.T.</u> 
	NIDN. 0606079501

Mengetahui,

Ketua Program Studi S1 Teknik Telekomunikasi

Institut Teknologi Telkom Purwokerto


Prasetyo Yulianto, S.T., M.T.

NIDN. 0620079201

HALAMAN PERNYATAAN ORISINALITAS

Saya atas nama, **RIZA OVIT DIANASARI** selaku penulis skripsi ini menyatakan dengan sungguh-sungguh bahwa skripsi dengan judul “**ANALISIS KEAMANAN JARINGAN *VIRTUAL PRIVATE NETWORK* (VPN) DENGAN METODE *SOURCE SOCKET TUNELLING PROTOCOL* (SSTP) STUDI KASUS: **BMKG JAMBI**” merupakan karya yang benar-benar saya buat sendiri dan tidak melakukan penjiplakan atau memuat pendapat dari karya orang lain kecuali yang telah disebutkan melalui pengutipan sesuai dengan etika keilmuan yang berlaku. Apabila ditemukan pelanggaran terhadap etika keilmuan yang terdapat dalam skripsi ini, saya bersedia untuk menerima sanksinya.**

Purwokerto, 24 Juni 2022



20
METERAI
TAMPEL
A055A.JX954771440
(Riza Ovit Dianasari)

PRAKATA

Puji syukur kita panjatkan kepada Tuhan Yang Maha Esa atas berkat dan rahmat-Nya sehingga penulis dapat menyelesaikan penulisan Tugas Akhir Skripsi yang berjudul “*ANALISIS KEAMANAN JARINGAN VIRTUAL PRIVATE NETWORK (VPN) DENGAN METODE SOURCE SOCKET TUNELLING PROTOCOL (SSTP) STUDI KASUS: BMKG JAMBI*” dapat diselesaikan dengan baik.

Adapun tujuan dari penulisan ini adalah untuk memenuhi salah satu syarat menempuh ujian sarjana dan mendapatkan gelar Sarjana Teknik (S.T.) pada Fakultas Teknik Telekomunikasi dan Elektro di Institut Teknik Teknologi Telkom Purwokerto.

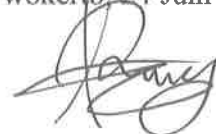
Selesainya Tugas Akhir ini tidak lepas dari bantuan, bimbingan, dan doa dari berbagai pihak. Pada kesempatan ini ingin disampaikan terima kasih kepada semua pihak yang telah membantu dalam pembuatan karya ini, oleh karena itu penulis sampaikan terima kasih banyak yang sedalam-dalamnya kepada :

1. Allah SWT yang telah memberikan kemudahan dan kelancaran kepada penulis sehingga penulis dapat menyelesaikan proposal tanpa suatu hambatan.
2. Kedua orang tua yang telah memberikan dukungan baik material, spritual, maupun motivasi-motivasi yang tiada hentinya.
3. Bapak Dr.Arifianto Fahmi,S.T.,M.T.,IPM.,selaku Rektor Institusi Teknologi Telkom Purwokerto.
4. Bapak Jafaruddin Gusti Amri Ginting, S.T., M.T. selaku dosen pembimbing I yang telah memberikan bimbingan dan arahan selama penyusunan proposal skripsi ini.
5. Ibu Irmayatul Hikmah, S.Si., M.Si. selaku dosen pembimbing II yang telah memberikan bimbingan dan arahan selama penyusunan proposal ini.
6. Ibu Shinta Romadhona, S.T., M.T. selaku wali kelas yang telah memberikan dukungan serta bimbingannya dalam penyusunan laporan.
7. Teman-teman yang sudah mendukung dan membantu.

8. Serta seluruh pihak yang telah membantu dalam proses penulisan baik secara langsung maupun tidak langsung.

Penulis menyadari bahwa dalam penyusunan proposal skripsi ini masih banyak kekurangan dan masih jauh dari kesempurnaan dalam bentuk penyajian tulisan. Maka dari itu, kritik serta saran yang membangun sangat kami harapkan demi terciptanya proposal yang lebih baik untuk kedepannya. Terlepas dari segala kekurangan yang ada, penulis berharap dengan hadirnya proposal ini dapat memberikan manfaat dan menambah ilmu pengetahuan bagi semua pihak yang pembaca.

Purwokerto, 24 Juni 2022



(Riza Ovit Dianasari)

DAFTAR ISI

HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN ORISINALITAS	iv
PRAKATA.....	vi
ABSTRAK.....	viii
<i>ABSTRACT</i>	ix
DAFTAR ISI.....	x
DAFTAR GAMBAR.....	xi
BAB I PENDAHULUAN.....	1
1.1 LATAR BELAKANG.....	1
1.2 RUMUSAN MASALAH	3
1.3 BATASAN MASALAH	4
1.4 TUJUAN PENELITIAN	4
1.5 MANFAAT PENELITIAN.....	4
1.6 SISTEMATIKA PENULISAN.....	4
BAB II DASAR TEORI	6
2.1 KAJIAN PUSTAKA	6
2.2 JARINGAN KOMPUTER.....	11
2.2.1 Macam-macam Jaringan Komputer	11
2.2.2 Kegunaan Jaringan Komputer.....	12
2.3 SERANGAN JARINGAN	13
2.4 KEAMANAN JARINGAN.....	15
2.5 <i>VIRTUAL PRIVATE NETWORK (VPN)</i>	15
2.5.2 Metode <i>Security</i> VPN	17

2.5.3	Macam-macam VPN.....	19
2.6	<i>SOURCE SOCKET TUNELLING (SSTP)</i>	20
2.6.1	<i>IP Public</i>	21
2.6.2	<i>IP Private</i>	21
2.6.3	Enkripsi Algoritma RC4	21
2.7	ROUTER.....	22
2.8	WIRESHARK	22
BAB III METODOLOGI PENELITIAN		23
3.1	OBJEK DAN SUBJEK PENELITIAN.....	23
3.2	TEKNIK PENGUMPULAN DATA.....	23
3.2.1	Studi Pustaka.....	23
3.2.2	Observasi	23
3.3	ALAT DAN BAHAN	24
3.3.1	Perangkat Keras	24
3.3.2	Perangkat Lunak	24
3.4	ALUR PENELITIAN.....	25
3.4.1	Identifikasi dan Perumusan Masalah	25
3.4.2	Mencari Solusi dan Bahan Referensi.....	26
3.4.3	Perencanaan Kebutuhan.....	26
3.4.4	PENGUJIAN SSTP PADA MIKROTIK	26
3.4.5	HASIL PENGUJIAN.....	26
3.5	TOPOLOGI JARINGAN.....	26
3.6	ALUR SIMULASI.....	28
3.6.1	Perancangan Sistem	29
3.6.2	Perancangan Topologi Jaringan.....	29

3.6.3	Konfigurasi Dasar Alamat IP	29
3.6.4	Konfigurasi VPN SSTP	33
3.6.5	Pemasangan Sertifikat.....	36
3.6.6	Melakukan <i>Attacking</i> DoS	40
3.6.7	Melakukan <i>Sniffing</i> menggunakan Wireshark.....	40
BAB IV ANALISA DAN PEMBAHASAN		41
4.1	KEAMANAN PADA MIKROTIK.....	41
4.2	KONFIGURASI DASAR	41
4.3	HASIL PENGUJIAN DOS	42
4.4	HASIL <i>SNIFFING</i> MENGGUNAKAN WIRESHARK	43
BAB V KESIMPULAN DAN SARAN		46
5.1	KESIMPULAN.....	46
5.2	SARAN.....	47
DAFTAR PUSTAKA.....		48

DAFTAR GAMBAR

Gambar 2.1 Serangan <i>Main In The Middle Attack</i>	13
Gambar 2.2 VPN <i>Remote Access</i>	16
Gambar 2.3 VPN <i>Site-to-Site</i>	17
Gambar 2.4 Struktur paket SSTP.....	20
Gambar 2.5 Mekanisme Koneksi SSTP.....	20
Gambar 3.1 Alur Penelitian.....	25
Gambar 3.2 Desain Topologi.....	27
Gambar 3.3 Alur Simulasi.....	28
Gambar 3.4 Diagram Blok Penerapan Jaringan SSTP.....	29
Gambar 3.5 DHCP <i>Client</i> pada Kantor A.....	30
Gambar 3.6 IP <i>Routes</i> pada Kantor A.....	31
Gambar 3.7 <i>Firewall NAT Masquarade</i>	32
Gambar 3.8 <i>Firewall NAT</i> pada <i>Tool General</i>	33
Gambar 3.9 Desain VPN SSTP.....	33
Gambar 3.10 SSTP pada Server.....	34
Gambar 3.11 <i>Secrets</i> pada Server.....	35
Gambar 3.12 <i>Active Connections</i> pada SSTP Tanpa Sertifikat.....	36
Gambar 3.13 <i>Certificate</i> untuk <i>Client</i>	37
Gambar 3.14 <i>Certificate</i> untuk myCA.....	37
Gambar 3.15 <i>Certificate</i> untuk Server.....	38
Gambar 3.16 VPN SSTP Saling Terhubung.....	39
Gambar 3.17 <i>Active Connections</i> VPN SSTP.....	40
Gambar 4.1 Hasil <i>Capture Sniffing</i> VPN SSTP.....	43
Gambar 4.2 Hasil <i>Capture Layer 2</i> dan <i>Layer 3</i>	44
Gambar 4.3 Hasil <i>Capture Layer 4</i>	44
Gambar 4.1 Hasil <i>Capture Sniffing</i> VPN SSTP.....	43