

**IMPLEMENTASI VPN L2TP/IPSEC DAN ANALISIS KEAMANAN
KOMUNIKASI DATA PADA ROUTER CISCO SERI 1900**

TUGAS AKHIR



JIZREL EBZAN SAPUTRA LEDOH

1202001022

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN ILMU KOMPUTER
UNIVERSITAS BAKRIE
JAKARTA
2026**

**IMPLEMENTASI VPN L2TP/IPSEC DAN ANALISIS KEAMANAN
KOMUNIKASI DATA PADA ROUTER CISCO SERI 1900**

TUGAS AKHIR

Diajukan sebagai syarat untuk memperoleh gelar Sarjana Komputer



JIZREL EBZAN SAPUTRA LEDOH

1202001022

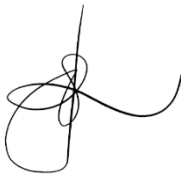
**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN ILMU KOMPUTER
UNIVERSITAS BAKRIE
JAKARTA
2026**

HALAMAN PERNYATAAN ORISINALITAS

Tugas Akhir ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Jizrel Ebzan Saputra Ledoh

NIM : 1202001022

Tanda Tangan : 

Tanggal : 08 September 2026

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama : Jizrel Ebzan Saputra Ledoh
NIM : 1202001022
Program Studi : Informatika
Fakultas : Fakultas Teknik dan Ilmu Komputer
Judul Skripsi : Implementasi VPN L2TP/IPsec Dan Analisis Keamanan Komunikasi Data Pada Router Cisco Seri 1900

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer (S.Kom) pada Program Studi Teknik Informatika Fakultas Teknik dan Ilmu Komputer, Universitas Bakrie.

DEWAN PENGUJI

Pembimbing I : Ir. Iwan Adichandra, SMIEE, MIET, MBCS

()

Pembahas I : Prof. Dr. Hoga Saragih, M.T., Ph.D., IPU., IPM

()

Pembahas II : Ir. Albert Arapenta Sembiring, S.T., M.Kom

()

Ditetapkan di Jakarta

Tanggal 13 September 2026

UNGKAPAN TERIMA KASIH

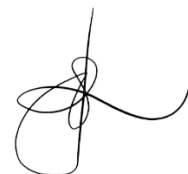
Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya penulis dapat menyelesaikan skripsi yang berjudul **“IMPLEMENTASI VPN L2TP/IPSEC DAN ANALISIS KEAMANAN KOMUNIKASI DATA PADA ROUTER CISCO SERI 1900”**. Skripsi ini disusun untuk memenuhi salah satu syarat memperoleh gelar Sarjana pada Program Studi Informatika. Penulis menyadari bahwa tanpa bantuan, bimbingan, dan dukungan dari berbagai pihak, penyusunan skripsi ini tidak akan berjalan dengan lancar.

Pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih kepada:

- 1) Tuhan Yang Maha Esa.
- 2) Ibu Prof. Sofia W. Alisjahbana, M.Sc., Ph.D., IPU., ASEAN Eng. Selaku Rektor Universitas Bakrie.
- 3) Bapak Dr. Mohammad Ihsan, ST., MT., M.Sc. Selaku Dekan Fakultas Teknik dan Ilmu Komputer Universitas Bakrie.
- 4) Bapak Ir. Iwan Adhicandra, S.T., M.Sc., Ph.D., SMIEEE. Selaku Ketua Program Studi Teknik Informatika dan Dosen Pembimbing Skripsi.
- 5) Bapak Prof. Dr. Hoga Saragih, S.T., M.T, Ph.D., IPU., IPM. Selaku Dosen Pembimbing Akademik.
- 6) Seluruh Dosen Program Studi S1 Teknik Informatika Universitas Bakrie.
- 7) Kedua Orang Tua dan Keluarga penulis.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan demi perbaikan di masa mendatang. Akhir kata, semoga skripsi ini dapat memberikan manfaat bagi penulis, pembaca, dan pihak lain yang berkepentingan.

Jakarta, 08 September 2026



Jizrel Ebzan Saputra Ledoh

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI

Sebagai civitas akademik Universitas Bakrie, saya yang bertanda tangan dibawah ini:

Nama : Jizrel Ebzan Saputra Ledoh
Program Studi : Informatika
Fakultas : Teknik dan Ilmu Komputer
Jenis Tugas Akhir : Skripsi

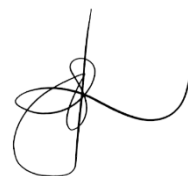
Demi mengembangkan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bakrie Hak Bebas Royalti Noneksklusif (Nonexclusive Royalti-Free Right) atas karya ilmiah saya yang berjudul:

IMPLEMENTASI VPN L2TP/IPSEC DAN ANALISIS KEAMANAN KOMUNIKASI DATA PADA ROUTER CISCO SERI 1900

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Bakrie berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta untuk kepentingan akademis.

Demikian pernyataan ini saya buat dengan sebenar-benarnya.

Jakarta, 08 September 2026



Jizrel Ebzan Saputra Ledoh

IMPLEMENTASI VPN L2TP/IPSEC DAN ANALISIS KEAMANAN KOMUNIKASI DATA PADA ROUTER CISCO SERI 1900

Jizrel Ebzan Saputra Ledoh

ABSTRAK

Virtual Private Network (VPN) merupakan teknologi yang digunakan untuk meningkatkan keamanan komunikasi data pada jaringan publik dengan memanfaatkan mekanisme tunneling dan enkripsi. Salah satu protokol yang umum digunakan adalah Layer 2 Tunneling Protocol (L2TP) yang dikombinasikan dengan Internet Protocol Security (IPsec) sehingga mampu menyediakan autentikasi, integritas data, serta kerahasiaan informasi selama proses transmisi berlangsung.

Penelitian ini bertujuan untuk mengimplementasikan serta menganalisis keamanan jaringan menggunakan Virtual Private Network (VPN) dengan protokol L2TP/Ipssec pada Router Cisco seri 1900. Implementasi dilakukan dengan membangun koneksi VPN antara client dan server melalui jaringan publik sehingga komunikasi data dapat berlangsung secara aman.

Metode penelitian yang digunakan adalah metode eksperimen dengan melakukan konfigurasi VPN pada perangkat router Cisco serta melakukan pengujian konektivitas jaringan. Analisis dilakukan melalui pengujian konektivitas menggunakan ping test, pengukuran throughput menggunakan iPerf, serta analisis paket data menggunakan Wireshark, serta evaluasi proses tunneling dan enkripsi pada komunikasi jaringan.

Hasil penelitian menunjukkan bahwa implementasi VPN L2TP/IPsec mampu meningkatkan keamanan komunikasi data serta menjaga kerahasiaan informasi yang ditransmisikan melalui jaringan publik.

Kata Kunci: Virtual Private Network, L2TP/IPsec, Router Cisco 1900, Keamanan Jaringan.

IMPLEMENTATION OF VPN L2TP/IPSEC AND DATA COMMUNICATION SECURITY ANALYSIS ON CISCO 1900 SERIES ROUTER

Jizrel Ebzan Saputra Ledoh

ABSTRACT

Virtual Private Network (VPN) is a technology used to enhance the security of data communication over public networks by utilizing tunneling and encryption mechanisms. One of the commonly used VPN protocols is Layer 2 Tunneling Protocol (L2TP) combined with Internet Protocol Security (IPsec), which provides authentication, data integrity, and confidentiality during the data transmission process.

This research aims to implement and analyze network security using Virtual Private Network (VPN) with the L2TP/IPsec protocol on Cisco 1900 series routers. The implementation is carried out by establishing a VPN connection between the client and the server through a public network so that data communication can occur securely.

The research method used is an experimental method by configuring the VPN on Cisco routers and performing network connectivity testing. The analysis was carried out through connectivity testing using ping tests, throughput measurement using iPerf, packet analysis using Wireshark, and evaluation of tunneling and encryption processes in network communication.

The results show that the implementation of L2TP/IPsec VPN can improve the security of data communication and maintain the confidentiality of information transmitted over public networks.

Keywords: Virtual Private Network, L2TP/IPsec, Cisco 1900 Router, Network Security.

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERNYATAAN ORISINALITAS	iii
HALAMAN PENGESAHAN.....	iv
UNGKAPAN TERIMA KASIH	v
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI	vi
ABSTRAK	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xii
DAFTAR TABEL	xiv
DAFTAR LAMPIRAN A	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	2
1.5 Manfaat Penelitian	3
BAB II LANDASAN TEORI	4
2.1 Penelitian Terkait	4
2.2 Dasar Teori	5
2.2.1 Jaringan Komputer	5
2.2.2 Topologi Jaringan.....	7
2.2.3 Perangkat Jaringan.....	7
2.2.4 TCP/IP	10
2.2.5 IP Address	11
2.2.6 Routing	12
2.2.7 Virtual Private Network (VPN).....	12
2.2.8 Layer 2 Tunneling Protocol (L2TP)	14
2.2.9 IP Security (IPsec).....	14
2.2.10 Router Cisco	15
2.2.11 Internet Key Exchange (IKE)	16

2.2.12	Encapsulating Security Payload dan Authentication Header.....	17
2.2.13	Ancaman Keamanan VPN	17
2.2.14	Wireshark.....	18
2.2.15	iPerf.....	18
2.2.16	PuTTY	19
2.2.17	Network Address Translation (NAT)	20
2.2.18	Authentication, Authorization, and Accounting (AAA).....	21
BAB III METODOLOGI PENELITIAN		22
3.1	Metode Penelitian	22
3.2	Alat dan Bahan Penelitian.....	22
3.2.1	Alat Penelitian	22
3.2.2	Tahapan Penelitian	23
3.3	Perancangan Sistem	24
3.3.1	Perancangan Jaringan	24
3.3.2	Desain Konfigurasi Router	25
3.4	Skenario Simulasi	26
3.5	Prosedur Penelitian	27
3.5.1	Skema Rancangan Program Penelitian.....	27
3.5.2	Skema Rancangan Alur Pengujian Koneksi Jaringan	28
3.5.3	Matriks Pengujian.....	29
3.6	Parameter Pengujian	30
3.7	Tools Pengujian	31
3.8	Jadwal dan Rencana Penelitian.....	32
BAB IV HASIL DAN PEMBAHASAN		34
4.1	Implementasi Sistem.....	34
4.2	Konfigurasi Router Cisco 1900	34
4.2.1	Konfigurasi Interface dan Routing	34
4.2.2	Konfigurasi AAA dan User VPN	35
4.2.3	Konfigurasi L2TP	35
4.2.4	Konfigurasi Virtual Template dan VPN Pool.....	36
4.2.5	Konfigurasi IPsec	37
4.2.6	Konfigurasi NAT	38
4.3	Konfigurasi Server.....	38

4.4	Konfigurasi VPN Client.....	39
4.4.1	Verifikasi Pembentukan Tunnel VPN	40
4.5	Pengujian Konektivitas Sebelum Menggunakan VPN	42
4.5.1	Ping.....	42
4.5.2	Wireshark.....	43
4.6	Pengujian Setelah Menggunakan VPN.....	44
4.6.1	Ping.....	45
4.6.2	Wireshark.....	46
4.6.3	iPerf3	47
4.6.4	Pengujian Transfer Data Besar	49
4.7	Analisis Perbandingan	49
BAB V PENUTUP.....		53
DAFTAR PUSTAKA.....		56
LAMPIRAN A DOKUMENTASI PENELITIAN		60
LAMPIRAN B DATA HASIL PEGUJIAN KONEKTIVITAS		63

DAFTAR GAMBAR

Gambar 2.1 Server	8
Gambar 2.2 Workstation.....	8
Gambar 2.3 Kabel UTP	8
Gambar 2.4 Switch	9
Gambar 2.5 Router.....	10
Gambar 2.6 Modem.....	10
Gambar 2.7 Gambaran VPN.....	13
Gambar 2.8 Protokol L2TP.....	14
Gambar 2.9 Protokol IPsec	15
Gambar 2.10 Cisco Router	16
Gambar 2.11 PuTTY Console	20
Gambar 3.1 Topologi Fisik Jaringan	25
Gambar 3.2 Topologi Logis Jaringan	25
Gambar 3.3 Diagram Alur Metodologi Penelitian	28
Gambar 3.4 Diagram Alur Pengujian Konektivitas.....	29
Gambar 3.5 Gantt Chart Jadwal Pelaksanaan Penelitian.....	33
Gambar 4.1 Konfigurasi Interface WAN dan LAN.....	35
Gambar 4.2 Konfigurasi AAA dan Akun VPN	35
Gambar 4.3 Konfigurasi Layanan L2TP	36
Gambar 4.4 Konfigurasi VPN Pool dan Virtual Template VPN.....	36
Gambar 4.5 Konfigurasi Ipsec	37
Gambar 4.6 Konfigurasi Network Address Translation (NAT)	38
Gambar 4.7 Konfigurasi IP Address Server	39
Gambar 4.8 Konfigurasi VPN Client Connection	40
Gambar 4.9 Status Security Association	41
Gambar 4.10 VPN Status Connected.....	41
Gambar 4.11 Ping Client ke WAN Sebelum VPN	42
Gambar 4.12 Ping Client ke LAN Gateway Sebelum VPN	42
Gambar 4.13 Capture Wireshark Ping Client ke WAN Sebelum VPN.....	43
Gambar 4.14 Capture Wireshark Ping Client ke Gateway LAN Sebelum VPN.....	44
Gambar 4.15 Ping Client ke Gateway LAN Setelah VPN	45
Gambar 4.16 Ping Client ke Server Setelah VPN	45

Gambar 4.17 Capture Wireshark Pembentukan Tunnel L2TP/IPsec	46
Gambar 4.18 Capture Wireshark Komunikasi Client dan Server Setelah VPN.....	46
Gambar 4.19 Pegujian Throughput Sebelum VPN.....	47
Gambar 4.20 Pengujian Throughput 1 Client ke Server Setelah VPN.....	47
Gambar 4.21 Pengujian Throughput 2 Client ke Server Setelah VPN.....	47
Gambar 4.22 Pengujian Throughput 3 Client ke Server Setelah VPN.....	47
Gambar 4.23 Pengujian Throughput 1 Server ke Client Setelah VPN.....	48
Gambar 4.24 Pengujian Throughput 2 Server ke Client Setelah VPN.....	48
Gambar 4.25 Pengujian Throughput 3 Server ke Client Setelah VPN.....	48
Gambar 4.26 Pegujian Transfer Data 1 GB	49

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait.....	4
Tabel 2.2 IP Address.....	11
Tabel 2.3 Perbandingan VPN	14
Tabel 3.1 Tabel Spesifikasi Perangkat Keras	22
Tabel 3.2 Konfigurasi IP Address	26
Tabel 3.3 Konfigurasi Router	26
Tabel 3.4 Matrix Pengujian	30
Tabel 3.5 Jadwal Pelaksanaan Penelitian	32
Tabel 4.1 Hasil Pengujian Ping Sebelum VPN	43
Tabel 4.2 Hasil Pengujian Ping Setelah VPN.....	45
Tabel 4.3 Hasil Pengujian Throughput iPerf3 Setelah VPN	48
Tabel 4.4 Pengujian Transfer Data 1 GB.....	49
Tabel 4.5 Perbandingan Konektivitas.....	50
Tabel 4.6 Perbandingan Delay.....	50
Tabel 4.7 Perbandingan Packet Loss	50
Tabel 4.8 Perbandingan Throughput	51
Tabel 4.9 Keamanan Komunikasi Data	52

DAFTAR LAMPIRAN A

Lampiran A.1 Perangkat Penelitian	60
Lampiran A.2 Cisco Router dan HP Switch	61
Lampiran A.3 Proses Pengujian	61
Lampiran A.4 Client Information	62
Lampiran A.5 Server Information	62

DAFTAR LAMPIRAN B

Lampiran B. 1 Hasil Ping dari Client ke LAN Gateway Sebelum VPN	63
Lampiran B. 2 Hasil Ping dari Client ke WAN Router Sebelum VPN	64
Lampiran B. 3 Hasil Ping dari Client ke LAN Gateway Setelah VPN	65
Lampiran B. 4 Hasil Ping dari Client ke Server Setelah VPN	66
Lampiran B. 5 Hasil Pengujian Throughput 3x dari Client ke Server Setelah VPN.....	69
Lampiran B. 6 Hasil Pengujian Throughput 3x dari Server ke Client Setelah VPN.....	72
Lampiran B. 7 Hasil Uji Load Data 1 GB dari Server Setelah VPN.....	78