



**Implementasi Keamanan Jaringan dan Pembatasan *Bandwidth* di PT
Mahoni Edukasi Digital untuk Meningkatkan Efisiensi dan Kinerja
Jaringan**

LAPORAN SKRIPSI

Alvin Raykhan

41519120081

UNIVERSITAS
MERCU BUANA

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2024**



**Implementasi Keamanan Jaringan dan Pembatasan *Bandwidth* di PT Mahoni
Edukasi Digital untuk Meningkatkan Efisiensi dan Kinerja Jaringan**

LAPORAN SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana

UNIVERSITAS
MERCU BUANA

Oleh:

ALVIN RAYKHAN

41519120081

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

2024

HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda tangan dibawah ini:

Nama : ALVIN RAYKHAN
NIM : 41519120081
Program Studi : Teknik Informatika
Judul Laporan Skripsi : Implementasi Keamanan Jaringan dan Pembatasan
Bandwidth di PT Mahoni Edukasi Digital untuk
Meningkatkan Efisiensi dan Kinerja Jaringan

Menyatakan bahwa Laporan skripsi ini adalah hasil karya saya sendiri dan bukan plagiat, serta semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Apabila ternyata ditemukan di dalam Laporan skripsi saya terdapat unsur plagiat, maka saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.

Jakarta, 17 Januari 2025



ALVIN RAYKHAN

HALAMAN PENGESAHAN

Laporan Skripsi ini diajukan oleh:

Nama : ALVIN RAYKHAN
NIM : 41519120081
Program Studi : Teknik Informatika
Judul Laporan Skripsi : Implementasi Keamanan Jaringan dan Pembatasan *Bandwidth* di PT Mahoni Edukasi Digital untuk Meningkatkan Efisiensi dan Kinerja Jaringan

Telah berhasil dipertahankan pada sidang di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Strata 1 pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Mercu Buana.

Disahkan oleh:

Pembimbing : Dhanny Permatasari Putri, S. Kom., M.T.

NIDN : 0328087903

Ketua Penguji : Dr. Hadi Santoso, S. Kom., M.Kom.

NIDN : 0225067701

Penguji 1 : Dr. Bagus Priambodo, S.T., M.TI.

NIDN : 0313057905

Penguji 2 : Dr. Ir. Eliyani.

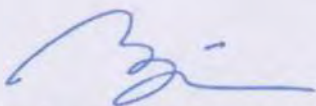
NIDN : 0321026901

MERCU BUANA

Jakarta, 03 Februari 2025

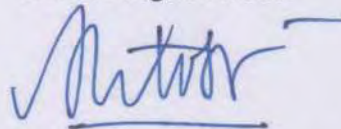
Mengetahui,

Dekan



Dr. Bambang Jokonowo, S.Si., MTI
NIDN : 0320037002

Ketua Program Studi



Dr. Hadi Santoso, S.Kom., M.Kom
NIDN : 0225067701

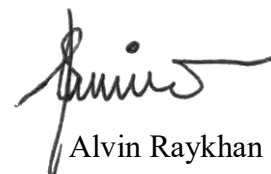
KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan Laporan Skripsi ini. Penulisan Laporan Skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Komputer pada Fakultas Ilmu Komputer Universitas Mercu Buana. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan Laporan Skripsi ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Prof. Dr. Ir. Andi Adriansyah, M.Eng selaku Rektor Universitas Mercu Buana
2. Dr. Bambang Jokonowo, S.Si., M.T.I selaku Dekan Fakultas Ilmu Komputer
3. Hadi Santoso, Dr, S.Kom, M.Kom selaku Ketua Program Studi Teknik Informatika
4. Dhanny Permatasari Putri, S.Kom, MT selaku Dosen Pembimbing serta Dosen Pembimbing Akademik yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan skripsi ini
5. Orang Tua dan Keluarga Besar yang selalu menyemangati saya dalam perjalanan kehidupan.
6. Annisa Amalia yang selalu menemani dan menyemangati dengan kopi item.
7. Rekan-rekan kerja yang selaku menyemangati dan mengarahkan dalam Kuliah.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga Laporan Skripsi ini membawa manfaat bagi pengembangan ilmu.

Jakarta, 03 Februari 2025



Alvin Raykhan

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Mercu Buana, saya yang bertanda tangan dibawah ini :

Nama : ALVIN RAYKHAN
NIM : 41519120081
Program Studi : Teknik Informatika
Judul Laporan Skripsi : Implementasi Keamanan Jaringan dan Pembatasan
Bandwidth di PT Mahoni Edukasi Digital untuk
Meningkatkan Efisiensi dan Kinerja Jaringan

Demi pengembangan ilmu pengetahuan, dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak bebas Royalti Non-Eksklusif (Non-Exclusive Royalty-free Right)** atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Laporan Magang/Skripsi/Tesis/Disertasi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 17 Januari 2025



ALVIN RAYKHAN

ABSTRAK

Nama : Alvin Raykhan
NIM : 41519120012
Program Studi : Teknik Informatika
Judul Laporan Skripsi : Implementasi Keamanan Jaringan dan Pembatasan *Bandwidth* di PT Mahoni Edukasi Digital untuk Meningkatkan Efisiensi dan Kinerja Jaringan
Pembimbing : Dhanny Permatasari Putri, S.Kom, MT

Penelitian ini membahas tentang implementasi manajemen *bandwidth* dan keamanan jaringan. Ketersediaan akses internet pada perusahaan diharapkan dapat menjadi salah satu sarana yang efektif untuk meningkatkan efisiensi dan kinerja perusahaan. PT. Mahoni Edukasi Digital merupakan perusahaan yang berfokus pada pendidikan digital. Penelitian ini mengambil studi kasus yang telah diimplementasikan di PT. Mahoni Edukasi Digital dengan alokasi *bandwidth* sebesar 25Mbps. Melalui penerapan metode *Hierarchical Token Bucket* dan *Port Knocking* pada router Mikrotik diharapkan implementasi dapat lebih terorganisasi dan terstruktur. Proses penelitian meliputi pengumpulan data, analisis, pemilihan perangkat keras, perancangan topologi jaringan, dan analisis jaringan dengan metode QoS (*Quality of Service*). Hasil penelitian menunjukkan bahwa kualitas jaringan berdasarkan uji coba yang dilakukan telah memenuhi standar TIPHON. Selain itu, untuk mengamankan *website* dan *database* perusahaan dari para hacker maka dibuatlah suatu sistem untuk melindungi komunikasi antara *client* dengan *server* yang disebut dengan *Port Knocking*. Pada penelitian ini, untuk melindungi komunikasi antara *client* dengan *server* dan *database webserver*, terdapat *shadow port* yang berguna untuk memindahkan *database* pada *webserver* sehingga hacker tidak dapat mengetahui lokasi *database* dari *webserver*. Cara ini dapat mengurangi kelemahan pada *webserver* yang menjadi incaran hacker.

Kata Kunci : QoS, Hierarchical Token Bucket, Bandwidth, Port Knocking

ABSTRACT

This study discusses the implementation of bandwidth management and network security. The availability of internet access in companies is expected to be one of the effective means to improve the efficiency and performance of the company. PT. Mahoni Edukasi Digital is a company that focuses on digital education. This study takes a case study that has been implemented at PT. Mahoni Edukasi Digital with a bandwidth allocation of 25Mbps. Through the application of the Hierarchical Token Bucket and Port Knocking methods on Mikrotik routers, it is expected that the implementation can be more organized and structured. The research process includes data collection, analysis, hardware selection, network topology design, and network analysis with the QoS (Quality of Service) method. The results of the study indicate that the network quality based on the trials conducted has met the TIPHON standard. In addition, to secure the company's website and database from hackers, a system was created to protect communication between the client and the server called Port Knocking. In this study, to protect communication between the client and the server and the webserver database, there is a shadow port that is useful for moving the database to the webserver so that hackers cannot find out the location of the database from the webserver. This method can reduce weaknesses in the webserver that are targeted by hackers.

Keywords: QoS, Hierarchical Token Bucket, Bandwidth, Port Knocking

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERNYATAAN KARYA SENDIRI.....	ii
HALAMAN PENGESAHAN.....	iii
KATA PENGANTAR	iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS	v
ABSTRAK.....	vi
ABSTRACT.....	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN.....	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	7
1.3 Batasan Masalah.....	8
1.4 Tujuan Dan Manfaat	8
1.4.1 Tujuan.....	8
1.4.2 Manfaat.....	9
1.5 Sistemika Penulisan	9
BAB II TINJAUAN PUSTAKA.....	11
2.1 Landasan Teori.....	11
2.1.1 Internet.....	11
2.1.2 Bandwidth.....	11

2.1.3	Router Mikrotik	12
2.1.4	Port Knocking	12
2.1.5	Winbox	12
2.1.6	Management Bandwidth.....	12
2.1.7	HTB.....	12
2.2	Penelitian Terkait.....	13
2.3	CRITICAL REVIEW	18
2.3.1	Summary.....	20
2.3.2	Synthesize.....	21
2.3.3	Comparison.....	21
2.3.4	Claim atau Kontribusi penelitian	22
BAB III	METODOLOGI.....	25
3.1	Lokasi Penelitian	25
3.2	Sarana Pendukung	25
3.3	Jenis Penelitian	26
3.4	Teknik Pengumpulan Data.....	26
3.5	Diagram Alir Penelitian	29
BAB IV	PEMBAHASAN DAN HASIL	31
4.1	Perancangan Arsitektur Jaringan.....	31
4.1.1	Perangkat Kebutuhan Sistem Hardware dan Software	32
4.2	konfigurasi Jaringan Mikrotik	35
4.2.1	Konfigurasi Router Mikrotik.....	35
4.2.2	Konfigurasi HTB	37
4.2.3	Konfigurasi Port Knocking	40
4.3	Pengujian Jaringan.....	44
4.3.1	Pengujian di hari pertama.....	56
4.3.2	Pengujian di hari kedua.....	62

4.3.3 Pengujian di hari ketiga.....	68
4.4 Hasil Perbandingan Pengujian.....	74
4.4.1 Pagi Hari.....	74
4.4.2 Siang Hari.....	75
4.4.3 Sore Hari	76
BAB IV KESIMPULAN DAN SARAN	80
5.1 Kesimpulan	80
5.2 Saran	81
DAFTAR PUSTAKA	82
LAMPIRAN.....	84



DAFTAR TABEL

Table 1 Penetrasi Internet Indonesia	2
Table 2 Hasil wawancara dengan bagian Departement Technical Support	4
Table 3 Hasil wawancara dengan bagian Kepala Departement Sales.....	5
Table 4 Hasil wawancara dengan bagian Departement Accounting dan Finance	6
Table 5 Penelitian Terkait.....	16
Table 6 Perbandingan Metode Penelitian Saya	23
Table 7 Perangkat Keras	25
Table 8 Perangkat Lunak	25
Table 9 Hasil Pengujian Hari Pertama di Pagi Hari Pada Perangkat Dept.IT dan Finance.....	58
Table 10 Hasil Pengujian Hari Pertama di Siang Hari Pada Perangkat Dept.IT dan Finance.....	60
Table 11 Hasil Pengujian Hari Pertama di Sore Hari Pada Perangkat Dept.IT dan Finance.....	62
Table 12 Hasil Pengujian Hari Kedua di Pagi Hari Pada Perangkat Dept.IT dan Finance.....	64
Table 13 Hasil Pengujian Hari Kedua di Siang Hari Pada Perangkat Dept.IT dan Finance.....	66
Table 14 Hasil Pengujian Hari Kedua di Sore Hari Pada Perangkat Dept.IT dan Finance.....	68
Table 15 Hasil Pengujian Hari Ketiga di Pagi Hari Pada Perangkat Dept.IT dan Finance.....	70
Table 16 Hasil Pengujian Hari Ketiga di Siang Hari Pada Perangkat Dept.IT dan Finance.....	72
Table 17 Hasil Pengujian Hari Ketiga di Sore Hari Pada Perangkat Dept.IT dan Finance.....	74

DAFTAR GAMBAR

Gambar 1 Lokasi Penggunaan KIPIN Classroom.....	3
Gambar 2 Proses Critical review.....	18
Gambar 3 Pengolahan Data Menggunakan Harzing's Publish or Perish.....	19
Gambar 4 Pengolahan Data Menggunakan VOSViewer	20
Gambar 5 Data Gangguan.....	26
Gambar 6 Metode Network Development Life Cycle (NDLC)	27
Gambar 7 Aplikasi Wireshark.....	28
Gambar 8 Pengujian Sistem.....	29
Gambar 9 Diagram Alir Penelitian.....	30
Gambar 10 Hasil software Acrylic Wifi Heatmap	31
Gambar 11 Usulan Topologi.....	32
Gambar 12 Router RB951Ui-2 nD.....	33
Gambar 13 Access Point.....	34
Gambar 14 Winbox	34
Gambar 15 Wireshark.....	35
Gambar 16 Konfigurasi IP	35
Gambar 17 Login Winbox dengan VPN	36
Gambar 18 Tampilan menu interfaces	36
Gambar 19 Tampilan Address List	37
Gambar 20 Hasil Konfigurasi DHCP	37
Gambar 21 Konfigurasi Mangle - General	38
Gambar 22 Mangle – Action.....	38
Gambar 23 Konfigurasi dengan terminal	38
Gambar 24 Queue Parent.....	39
Gambar 25 Queue Child	39
Gambar 26 Hasil konfigurasi Queue.....	40
Gambar 27 Konfigurasi Blok Port 22 dan 443 dengan Terminal	40
Gambar 28 Konfigurasi Blok Port 22 dan 443 dengan Terminal	41
Gambar 29 Konfigurasi untuk urutan knocking	41
Gambar 30 Konfigurasi untuk urutan knocking dengan Terminal	42
Gambar 31 Tampilan Hasil Konfigurasi Urutan Knocking.....	42

Gambar 32 Membuka Akses Port setelah Port Knocking	43
Gambar 33 Konfigurasi Terminal untuk Aturan Akses Port Knocking	43
Gambar 34 Konfigurasi Penutupan Akses yang Tidak Terotorisasi	44
Gambar 35 Pengujian upload dan download bandwidth IP 10.10.1.0/24	45
Gambar 36 Pengujian upload dan download bandwidth IP 10.10.5.0/24	45
Gambar 37 Pengujian dengan Torch lewat Terminal.....	46
Gambar 38 Hasil Port Blocking IP Public	47
Gambar 39 Perintah Port Knocking Untuk Membuka Port 99 Dari Client	47
Gambar 40 Monitoring Dari Port Knocking daemon di Webserver Untuk Membuka Port 99.....	47
Gambar 41 Login Phpmyadmin Saat Setelah Ketukan Dari Client	50
Gambar 42 Perintah Untuk Menutup Kembali Port 99 Yang Terbuka	50
Gambar 43 Proses Dari Ketukan Untuk Menutup Port 99	50
Gambar 44 Topologi Dimana Peretas Melakukan Aksinya Saat Sistem Keamanan Jaringan yang Dibangun hanya Menggunakan Firewall	51
Gambar 45 Hasil Serangan dengan Websploit Sebelum Memakai Metode Port	51
Gambar 46 Hasil Serangan Peretas yang Meretas Login Page Name dari Server sehingga Peretas dapat masuk ke Phpmyadmin.....	53
Gambar 47 Topologi Sistem Keamanan Jaringan Menggunakan Metode Port Knocking.....	53
Gambar 48 Hasil Proses Serangan yang Dilakukan Peretas Setelah Webserver Menggunakan Metode Port Knocking.....	53
Gambar 49 Hasil Saat Metode Port Knocking Diterapkan di port 80, dimana Phpmyadmin tidak Ditemukan Walau di Scan	54
Gambar 50 Hasil Saat Metode Port Knocking Dapat Melindungi Database Phpmyadmin	54
Gambar 51 Penggunaan Wireshark.....	56
Gambar 52 Hasil Pengujian Hari Pertama di Pagi Hari Pada Perangkat Dept.IT.....	56
Gambar 53 Hasil Pengujian Hari Pertama di Pagi Hari Pada Perangkat Dept.Finance	57
Gambar 54 Hasil Pengujian Hari Pertama di Siang Hari Pada Perangkat Dept.IT.....	58
Gambar 55 Hasil Pengujian Hari Pertama di Siang Hari Pada Perangkat Dept.Finance	59
Gambar 56 Hasil Pengujian Hari Pertama di Sore Hari Pada Perangkat Dept.IT	60

Gambar 57 Hasil Pengujian Hari Pertama di Sore Hari Pada Perangkat Dept.Finance	61
Gambar 58 Hasil Pengujian Hari Kedua di Pagi Hari Pada Perangkat Dept.IT	62
Gambar 59 Hasil Pengujian Hari Kedua di Pagi Hari Pada Perangkat Dept.Finance	63
Gambar 60 Hasil Pengujian Hari Kedua di Siang Hari Pada Perangkat Dept.IT	64
Gambar 61 Hasil Pengujian Hari Kedua di Siang Hari Pada Perangkat Dept.Finance	65
Gambar 62 Hasil Pengujian Hari Kedua di Sore Hari Pada Perangkat Dept.IT	66
Gambar 63 Hasil Pengujian Hari Kedua di Sore Hari Pada Perangkat Dept.Finance	67
Gambar 64 Hasil Pengujian Hari Ketiga di Pagi Hari Pada Perangkat Dept.IT	68
Gambar 65 Hasil Pengujian Hari Ketiga di Pagi Hari Pada Perangkat Dept.Finance	69
Gambar 66 Hasil Pengujian Hari Ketiga di Siang Hari Pada Perangkat Dept.IT	70
Gambar 67 Hasil Pengujian Hari Ketiga di Siang Hari Pada Perangkat Dept.Finance	71
Gambar 68 Hasil Pengujian Hari Ketiga di Sore Hari Pada Perangkat Dept.IT	72
Gambar 69 Hasil Pengujian Hari Ketiga di Sore Hari Pada Perangkat Dept.Finance	73
Gambar 70 Standar Delay Menurut TIPHON	77
Gambar 71 Standar Jitter Menurut TIPHON	78
Gambar 72 Standar Throughput Menurut TIPHON	78
Gambar 73 Standar Packet Loss Menurut TIPHON	78

DAFTAR LAMPIRAN

Lampiran 1 Kartu Asitensi.....	84
Lampiran 2 Halaman Pernyataan Luaran Tugas Akhir.....	86
Lampiran 3 Hasil Cek Turnitin	87
Lampiran 4 Curriculum Vitae	88
Lampiran 5 Surat Pernyataan HAKI	90
Lampiran 6 Surat Pengalihan Hak Cipta	91
Lampiran 7 Sertifikat BNSP	92
Lampiran 8 Surat Ijin Riset Perusahaan	93
Lampiran 9 Formulir Revisi Dosen Penguji	94

