



**PENGUNAAN MIKROTIK LAYER 7 PROTOCOL DAN METODE
STATEFUL PACKET INSPECTION (SPI), INTRUSION DETECTION
SYSTEM (IDS) DALAM FIREWALL UNTUK MEMAKSIMALKAN
KEAMANAN JARINGAN DI SMKS ISLAM ASSA'ADATUL ABADIYAH**

LAPORAN TUGAS AKHIR

**JIDAN SYOFI ARDANA
41521010190**

**UNIVERSITAS
MERCU BUANA**

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2025**



**PENGUNAAN MIKROTIK LAYER 7 PROTOCOL DAN METODE
STATEFUL PACKET INSPECTION (SPI), INTRUSION DETECTION
SYSTEM (IDS) DALAM FIREWALL UNTUK MEMAKSIMALKAN
KEAMANAN JARINGAN DI SMKS ISLAM ASSA'ADATUL ABADIYAH**

LAPORAN TUGAS AKHIR

**JIDAN SYOFI ARDANA
41521010190**

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana

MERCU BUANA

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2025**

HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama : Jidan Syofi Ardana
NIM : 41521010190
Program Studi : Teknik Informatika
Judul Laporan Skripsi : Penggunaan Mikrotik Layer 7 Protocol Dan Metode Stateful Packet Inspection (SPI), Intrusion Detection System (IDS) Dalam Firewall Untuk Memaksimalkan Keamanan Jaringan Di SMKS Islam Assa'adatul Abadiyah

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, 31 Juli 2025



Jidan Syofi Ardana

HALAMAN PENGESAHAN

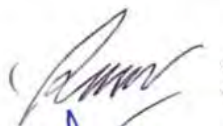
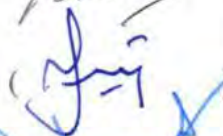
Laporan Skripsi ini diajukan oleh:

Nama : JIDAN SYOFI ARDANA
NIM : 41521010190
Program Studi : Teknik Informatika
Judul Laporan Skripsi : PENGGUNAAN MIKROTIK LAYER 7
PROTOCOL DAN METODE STATEFUL
PACKET INSPECTION (SPI), INTRUSION
DETECTION SYSTEM (IDS) DALAM
FIREWALL UNTUK MEMAKSIMALKAN
KEAMANAN JARINGAN DI SMKS ISLAM
ASSA'ADATUL ABADIYAH

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 : Raka Yusuf, S.T., M.TI.
NIDN : 0315087101
Ketua Penguji : Dr. Afiyati, S.Si., M.T.
NIDN : 0316106908
Penguji 1 : Rushendra, S.Kom., M.T.
NIDN : 0408067402
Penguji 2 : Muhammad Rifqi, S.Kom., M.Kom.
NIDN : 0301067101

()
()
()
()

Jakarta, 31 Juli 2025

Mengetahui,

Dekan

Ketua Program Studi



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



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

KATA PENGANTAR

Puji syukur kehadiran Tuhan yang Maha Esa, atas segala rahmat dan ridha-Nya sehingga penulis dapat menyelesaikan tugas akhir yang merupakan salah satu persyaratan kelulusan Program Studi Strata Satu (S1) pada jurusan Teknik Informatika, Universitas Mercu Buana.

Penulis menyadari bahwa tugas akhir ini masih jauh dari sempurna, karena kesempurnaan sejatinya hanya milik Tuhan yang Maha Esa. Oleh karena itu, saran dan masukan yang membangun senantiasa penulis terima dengan senang hati. Serta berkat dukungan, motivasi, bantuan, bimbingan, dan doa dari banyak pihak, penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Andi Adriansyah, M.Eng. selaku Rektor Universitas Mercu Buana.
2. Bapak Dr. Bambang Jokonowo, S.Si., MTI selaku Dekan Fakultas Ilmu Komputer.
3. Bapak Dr. Hadi Santoso, S.Kom., M.Kom. selaku Ketua Program Studi Teknik Informatika Universitas Mercubuna.
4. Bapak Raka Yusuf, ST, MTI. selaku dosen pembimbing tugas akhir yang telah memberikan pengarahan, motivasi, menyediakan waktu, tenaga, dan pikiran sehingga selama pembuatan tugas akhir ini terjadwal dengan baik.
5. Kedua Orang Tua saya yang selalu mensupport dan mendukung saya selama menjalani masa studi sebagai mahasiswa Universitas Mercubuna..
6. Semua teman kuliah yang selalu berbagi informasi dan memberikan dukungan dalam bentuk yang berbeda-beda.

Akhir kata, penulis berharap semoga Tuhan yang Maha Esa membalas kebaikan dan selalu mencurahkan rahmat, hidayah, serta panjang umur kepada kita semua, aamiin. Terima Kasih.

Jakarta, 31 Juli 2025



JIDAN SYOFI ARDANA

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

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

Nama : Jidan Syofi Ardana
NIM : 41521010190
Program Studi : Teknik Informatika
Judul Laporan Skripsi : Penggunaan Mikrotik Layer 7 Protocol Dan Metode Stateful Packet Inspection (SPI), Intrusion Detection System (IDS) Dalam Firewall Untuk Memaksimalkan Keamanan Jaringan Di SMKS Islam Assa'adatul Abadiyah

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.

UNIVERSITAS
MERCU BUANA

Jakarta, 31 Juli 2025
Yang menyatakan,



Jidan Syofi Ardana

ABSTRAK

Nama : JIDAN SYOFI ARDANA
NIM : 41521010190
Program Studi : Teknik Informatika
Judul Laporan Skripsi : PENGGUNAAN MIKROTIK LAYER 7
PROTOCOL DAN METODE STATEFUL
PACKET INSPECTION (SPI), INTRUSION
DETECTION SYSTEM (IDS) DALAM
FIREWALL UNTUK MEMAKSIMALKAN
KEAMANAN JARINGAN DI SMKS ISLAM
ASSA'ADATUL ABADIYAH
Dosen Pembimbing : Raka Yusuf, ST, MTI

Pesatnya perkembangan teknologi informasi telah meningkatkan risiko serangan siber, terutama di lingkungan pendidikan seperti SMKS Islam Assa'adatul Abadiyah. Ancaman seperti ddos, brute force, malware, hingga unauthorized access dapat mengganggu keamanan jaringan sekolah yang mendukung aktivitas pembelajaran dan administrasi. Penelitian ini bertujuan untuk menganalisis tingkat serangan siber yang terjadi serta mengembangkan solusi keamanan jaringan dengan memanfaatkan perangkat Mikrotik.

Metode yang digunakan dalam penelitian ini melibatkan penerapan fitur Layer 7 Protocol, Stateful Packet Inspection (SPI), dan Intrusion Detection System (IDS) pada firewall Mikrotik. Layer 7 Protocol digunakan untuk memfilter lalu lintas data berdasarkan pola aplikasi, SPI untuk memantau dan menyaring data berdasarkan koneksi yang aktif, sedangkan IDS berfungsi mendeteksi aktivitas mencurigakan atau anomali dalam jaringan.

Hasil penelitian menunjukkan bahwa solusi yang diimplementasikan mampu meningkatkan keamanan jaringan secara signifikan dengan menekan jumlah serangan yang berhasil masuk ke sistem. Penerapan teknologi ini tidak hanya melindungi data dan infrastruktur jaringan sekolah tetapi juga memastikan kelancaran proses pembelajaran berbasis teknologi.

Penelitian ini menyimpulkan bahwa kombinasi fitur Layer 7 Protocol, SPI, dan IDS pada perangkat Mikrotik merupakan pendekatan yang efektif dan efisien untuk memaksimalkan keamanan jaringan, terutama di lingkungan pendidikan. Implementasi sistem ini dapat dijadikan acuan untuk pengembangan lebih lanjut dalam menciptakan jaringan yang lebih aman di institusi pendidikan lainnya.

Kata kunci: Keamanan Jaringan, Mikrotik, Layer 7 Protocol, Stateful Packet Inspection (SPI), Intrusion Detection System (IDS), Firewall.

ABSTRACT

Nama : JIDAN SYOFI ARDANA
NIM : 41521010190
Program Studi : Teknik Informatika
Judul Laporan Skripsi : PENGGUNAAN MIKROTIK LAYER 7
PROTOCOL DAN METODE STATEFUL
PACKET INSPECTION (SPI), INTRUSION
DETECTION SYSTEM (IDS) DALAM
FIREWALL UNTUK MEMAKSIMALKAN
KEAMANAN JARINGAN DI SMKS ISLAM
ASSA'ADATUL ABADIYAH
Dosen Pembimbing : Raka Yusuf, ST, MTI

The rapid development of information technology has increased the risk of cyberattacks, particularly in educational environments like SMKS Islam Assa'adatul Abadiyah. Threats such as ddos, brute force, malware, and unauthorized access pose significant risks to the school's network security, which supports both learning and administrative activities. This study aims to analyze the frequency of cyberattacks and develop a network security solution using Mikrotik devices.

The research employs the implementation of Layer 7 Protocol, Stateful Packet Inspection (SPI), and Intrusion Detection System (IDS) on the Mikrotik firewall. The Layer 7 Protocol filters network traffic based on application patterns, SPI monitors and filters data based on active connections, and IDS detects suspicious activities or anomalies within the network.

The results indicate that the implemented solution significantly enhances network security by reducing the number of successful intrusions. This approach not only protects the school's data and network infrastructure but also ensures the smooth operation of technology-based learning activities.

This study concludes that the combination of Layer 7 Protocol, SPI, and IDS features on Mikrotik devices is an effective and efficient approach to optimizing network security, particularly in educational environments. This system implementation can serve as a reference for further development in creating more secure networks for other educational institutions.

Kata kunci: Network Security, Mikrotik, Layer 7 Protocol, Stateful Packet Inspection (SPI), Intrusion Detection System (IDS), Firewall.

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 GAMBAR.....	xi
DAFTAR LAMPIRAN	xii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	2
1.3 Tujuan Penelitian	2
1.4 Manfaat Penelitian	3
1.5 Batasan Masalah	4
BAB II TINJAUAN PUSTAKA	5
2.1 Penelitian Terdahulu	5
2.2 Teori Pendukung.....	8
2.2.1 Snort	8
2.2.2 Winbox	9
2.2.3 Mikrotik RouterOS	9
BAB III METODE PENELITIAN	10
3.1 Jenis Penelitian.....	10
3.2 Tahapan Penelitian.....	10
3.2.1 Pendekatan Penelitian	10
3.2.2 Desain Penelitian	10
3.2.3 Subjek Penelitian	15
3.2.4 Instrumen Penelitian	16
3.2.5 Teknik Pengumpulan Data	17
3.2.6 Analisis Data	17
3.2.6.2 Analisis Data Kuantitatif.....	17

3.2.6.4	Visualisasi Data	18
3.2.6.5	Interpretasi Data	19
3.2.6.6	Penyusunan Kesimpulan	19
3.2.7	Prosedur Penelitian	19
3.2.8	Evaluasi Hasil Penelitian	20
3.2.8.1	Perbandingan Data Pre-Test dan Post-Test	20
3.2.8.2	Evaluasi Efektivitas Fitur Firewall	21
3.2.8.3	Evaluasi Persepsi Pengguna	21
3.2.8.4	Pengujian Keandalan Jaringan	22
3.2.8.5	Pencapaian Tujuan Penelitian	22
3.2.8.6	Penyimpulan dan Rekomendasi	22
3.2.9	Alur Penelitian	23
BAB IV PEMBAHASAN		25
4.1	Dataset.....	25
4.1.1	Konfigurasi Dasar Mikrotik.....	25
4.1.2	Konfigurasi Dasar IDS Snort	31
4.1.3	Tools.....	33
4.2.4	Element Terhadap Dataset	33
4.3	Implementasi.....	37
4.3.1	Implementasi Dan Validasi Intrusion Detection System	37
4.3.2	Implementasi Dan Validasi Server MikroTik	41
4.3.3	Implementasi Dan Validasi Firewall Terhadap Serangan	43
4.4	Simulasi Penyerangan	48
4.4.1	Sebelum Dilakukan Pengujian	48
4.4.2	Setelah dilakukan Pengujian	53
4.4.3	Perbandingan Setelah dan Sebelum Pengujian	63
4.5	Analisis dan Pembahasan	69
BAB V KESIMPULAN DAN SARAN		76
5.1	Kesimpulan	76
5.2	Saran	77
DAFTAR PUSTAKA		79
LAMPIRAN		81

DAFTAR GAMBAR

Gambar 1. 1 Grafik Serangan Cyber.....	1
Gambar 2. 1 Mikrotik RouterBoard 2011iL-RM.....	9
Gambar 4. 1 Konfigurasi DHCP Client	25
Gambar 4. 2 Konfigurasi IP Address.....	26
Gambar 4. 3 Konfigurasi DNS Server	27
Gambar 4. 4 Konfigurasi DHCP Server	28
Gambar 4. 5 Konfigurasi NAT Firewall	29
Gambar 4. 6 IP Address Laptop.....	31
Gambar 4. 7 File Directory	32
Gambar 4. 8 Snort Ddos SYN Flood Detected Log.....	38
Gambar 4. 9 Snort SSH Brute Force Detected Log	39
Gambar 4. 10 Snort Unauthorized Access Detected Log	40
Gambar 4. 11 Snort Malware (EICAR) Detected Log.....	40
Gambar 4. 12 Sebelum Serangan	41
Gambar 4. 13 Saat atau Setelah Serangan.....	42
Gambar 4. 14 Statistik Trafik Real-time Pada Interface Jaringan	43
Gambar 4. 15 Aturan Firewall.....	45
Gambar 4. 16 Daftar Alamat IP Attacker	46
Gambar 4. 17 Layer 7 Protocol.....	47
Gambar 4. 18 Stateful Packet Inspection	48
Gambar 4. 19 Ringkasan Waktu Pemrosesan Paket dan Statistik I/O.....	49
Gambar 4. 20 Statistik dan Deteksi Ancaman.....	50
Gambar 4. 21 Statistik TCP	50
Gambar 4. 22 Rincian Lalu Lintas Berdasarkan Protokol.....	51
Gambar 4. 23 Aturan Firewall Drop, Accept, Protocol dan Dst. Port, Src. Address List, Bytes, dan Packets	53
Gambar 4. 24 Serangan Ddos.....	54
Gambar 4. 25 Serangan Brute Force	55
Gambar 4. 26 Serangan Unauthorized Access.....	56
Gambar 4. 27 Serangan Malware.....	57
Gambar 4. 28 Ringkasan Waktu Pemrosesan Paket dan Statistik I/O.....	57
Gambar 4. 29 Statistik dan dalam Deteksi Jaringan	58
Gambar 4. 30 Statistik Memori dalam Pemrosesan TCP	59
Gambar 4. 31 Waktu Pemrosesan dan Statistik Paket Total.....	59
Gambar 4. 32 Bytes dan Packet Saat Atau Setelah Pengujian.....	60
Gambar 4. 33 IP Penyerang Pada Address List Firewall.....	60
Gambar 4. 34 Kinerja CPU Saat atau Setelah Pengujian	61
Gambar 4. 35 Traffic Saat Atau Setelah Pengujian	62
Gambar 4. 36 Pengujian malware Saat atau Setelah Pengujian	63
Gambar 4. 37 Diagram Grafik Sebelum dan Sesudah Penyerangan	68

DAFTAR LAMPIRAN

Lampiran 1 Kartu Asistensi	81
Lampiran 2 Curriculum Vitae	82
Lampiran 3 Surat Pernyataan HAKI	83
Lampiran 4 Sertifikat BNSP	85
Lampiran 5 Surat Ijin Riset Perusahaan	86
Lampiran 6 Form Revisi Dosen Penguji	87
Lampiran 7 Hasil Cek Turnitin	89
Lampiran 8 Konfigurasi Snort	90
Lampiran 9 Konfigurasi Local Rules	112
Lampiran 10 Halaman Persetujuan	113

