

OPTIMALISASI KEAMANAN JARINGAN BERBASIS FIREWALL DAN IDS MENGGUNAKAN PFSENSE

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika



disusun oleh
AHMAD FUADI
19.11.2974

Kepada

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2026

OPTIMALISASI KEAMANAN JARINGAN BERBASIS FIREWALL DAN IDS MENGGUNAKAN PFSENSE

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika



disusun oleh
AHMAD FUADI
19.11.2974

Kepada

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2026

HALAMAN PERSETUJUAN

SKRIPSI

**OPTIMALISASI KEAMANAN JARINGAN BERBASIS
FIREWALL DAN IDS MENGGUNAKAN PFSENSE**

yang disusun dan diajukan oleh

AHMAD FUADI

19.11.2974

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 18 Juni 2026

Dosen Pembimbing,



Andika Agus Slameto, S.Kom., M.Kom
NIK. 190302109

HALAMAN PENGESAHAN

SKRIPSI

**OPTIMALISASI KEAMANAN JARINGAN BERBASIS FIREWALL DAN
IDS MENGGUNAKAN PFSense**
yang disusun dan diajukan oleh

Nama Mahasiswa

19.11.2974

Telah dipertahankan di depan Dewan Penguji
pada tanggal 18 Juni 2026

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Theopilus Bayu Sasongko, S.Kom., M.Eng
NIK. 190302375

Subektiningsih, S.Kom., M.Kom.
NIK. 190302413

Andika Agus Slameto, S.Kom., M.Kom
NIK. 190302109

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 18 Juni 2026

DEKAN FAKULTAS ILMU KOMPUTER



Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : AHMAD FUADI

NIM : 19.11.2974

Menyatakan bahwa Skripsi dengan judul berikut:

**OPTIMALISASI KEAMANAN JARINGAN BERBASIS FIREWALL DAN
IDS MENGGUNAKAN PFSense**

Dosen Pembimbing : Andika Agus Slameto, S.Kom., M.kom

Saya yang bertanda tangan dibawah ini menyatakan bahwa, skripsi ini merupakan hasil karya saya sendiri benar-benar (ASLI) dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.

Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 18 Juni 2026

Yang Menyatakan,



ad Fuadi

Ahmad fuadi

MOTTO

*Dan aku menyerahkan urusanku kepada Allah. Sungguh,
Allah Maha Melihat akan hamba-hamba-Nya.*

Q.S Ghafir : 44

*Setiap kita pasti melewati hari-hari yang buruk,
Satu hal yang perlu kita ingat "Ini Akan Berlalu"*

Ahmad Fuaadi

Bertekun dalam Do'a, Bersabar dalam Derita.

Abd. Muis

Seorang terpelajar sudah adil sejak dalam pikiran dan perbuatan.

Pramodya Anantatoer

HALAMAN PERSEMBAHAN

Puji dan syukur kepada Allah SWT yang telah memberikan rahmat dan karunianya sehingga penelitian ini dapat terselesaikan dengan baik.

Naskah Skripsi dipersembahkan kepada :

1. Allah SWT yang telah memberikan segenap pengetahuan dan kemampuan untuk dapat menyelesaikan tugas akhir penelitian skripsi ini dan memberikan waktu yang tepat.
2. Kedua orang tua saya terkhusus ibu saya yang sudah sangat sabar menantikan akhir dari proses pembuatan tugas akhir penelitian skripsi ini, yang selalu memberikan Do'a dan dukungan yang sangat besar, yang banting tulang tak kenal lelah untuk saya agar bisa mewujudkan impiannya dan menjadi orang tua yang berhasil mendidik anaknya. Dan juga dipersembahkan untuk almarhum ayah saya yang sudah dulu mendahului kami.
3. Kedua saudara saya yang sangat saya cintai dan selalu memberikan ruang dan dukungan untuk saya.
4. Dan keluarga besar Lamado yang selalu mendukung proses saya apapun itu.
5. Keluarga besar dari ibu saya yang selalu memeberikan dukungan dan Doa.
6. Kepada seluruh kawan – kawan saya yang tidak bisa saya sebutkan satu-persatu yang sudah sangat berperan dalam kehidupan saya mengajarkan dan menemani saya tentang banyak hal.
7. Keluarga besar kelas IF-06 yang sangat luar biasa.

KATA PENGANTAR

Puji syukur kehadiran Allah SWT tuhan semesta alam yang memberikan petunjuk kepada hamba-hambanya yang ada diseluruh alam semesta hanya kepadanya tempat meminta dan hanya kepadanya tempat memohon pertolongan, serta salawat serta salam kepada baginda rosullulah Muhammad SAW, yang membawa kita lebih mengenal tuhan berdasarkan Qur'an Dan Hadistnya. Dengan segala pertolongan tuhan yang maha esa Allah SWT, sehingga penulis dapat menyelesaikan skripsi yang berjudul “Optimalisasi Keamanan Jaringan Berbasis Firewall Dan IDS Menggunakan Pfsense”. Menggunakan metode NDLC simulasi Small Office Network.

Dalam proses penyelesaian skripsi ini banyak pihak yang telah terlibat memberikan masukan, bantuan, dukungan, saran dan kritik. Yang telah penulis terima, oleh karena itu dalam kesempatan ini penulis mengucapkan terima kasih dan hormat saya kepada :

1. Kepada Prof. Dr. M. Suyanto, M.M., selaku rektor Universitas Amikom Yogyakarta
2. Kepada Andika Agus Slameto, S.Kom., M.Kom. selaku dosen Pembimbing saya atas waktu, ilmu dan masukannya pada saat pelaksanaan bimbingan dan kesabarannya dalam memberikan masukan kepada penulis dalam pengerjaan tugas akhir ini.
3. Kepada Dosen penguji Pak, Theopilus Bayu Sasongko, S.Kom., M.Eng dan ibu Subektiningsih, S.Kom., M.Kom, yang sudah menguji dan memberikan masukan.
4. Seluruh dosen Fakultas Ilmu Komputer Universitas Amikom atas segala ilmu yang diberikan selama menempuh Perkuliahan.
5. Keluarga penulis yang tidak henti memberikan semangat dan dukungan kepada penulis.

Terima kasih kepada seluruh yang terlibat kerabat, teman, saudara, dan keluarga dan semua pihak dalam membantu penulis menyelesaikan skripsi ini yang tidak dapat saya sebutkan satu-persatu. Akhir kata penulis menyadari tidak ada hal yang sempurna, penulis masih melakukan kesalahan dalam penyusunan skripsi, oleh karena itu penulis meminta maaf sedalam-dalamnya atas kesalahan yang dilakukan penulis.

Penulis berharap semoga hasil penelitian skripsi ini dapat bermanfaat untuk pengembangan selanjutnya.

Yogyakarta 18 Juni 2026

Ahmad Fuaadi

NIM : 19.11.2974

DAFTAR ISI

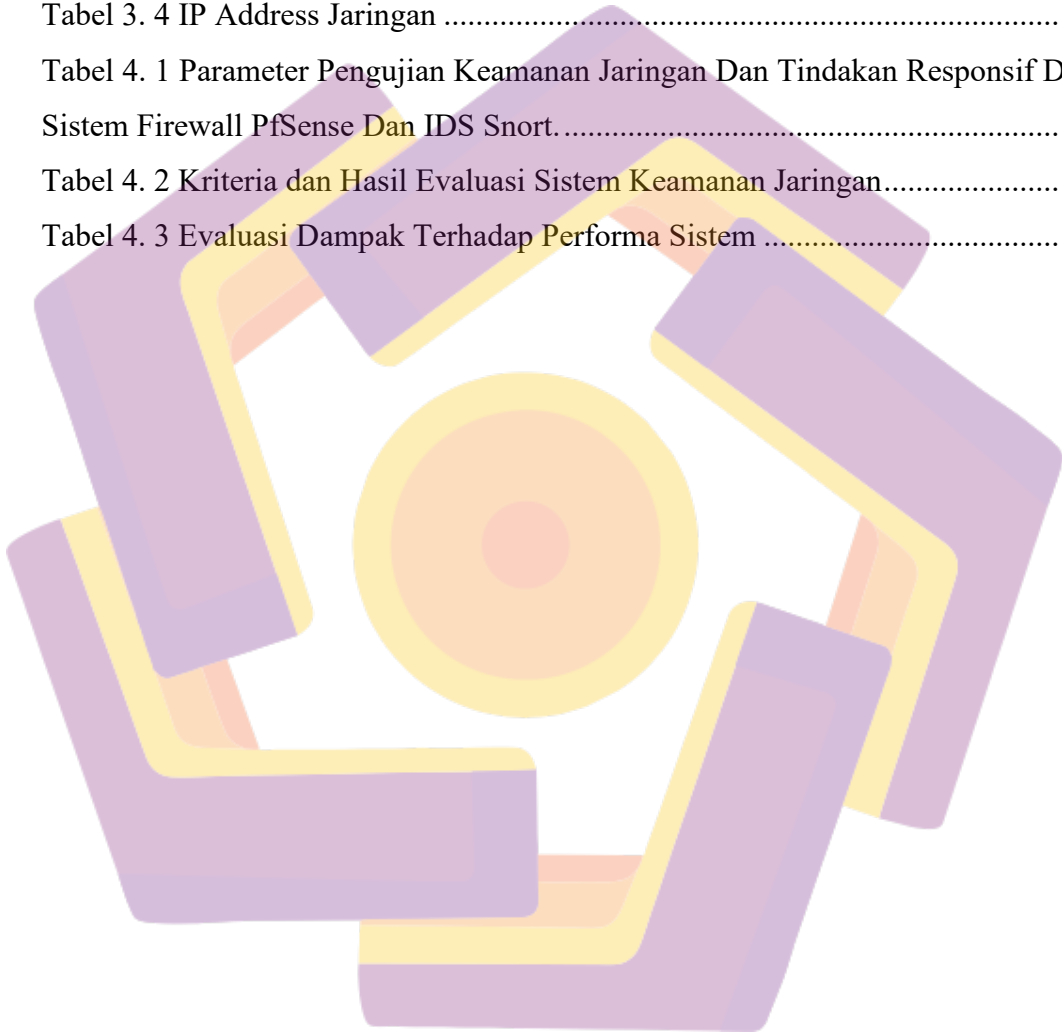
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
PERNYATAAN KEASLIAN SKRIPSI.....	iv
MOTTO	v
HALAMAN PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
INTISARI.....	xiv
ABSTRACT.....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA.....	6
2.1 Studi Literatur	6
2.2 Dasar Teori.....	10
2.2.1 PfSense.....	10
2.2.2 Firewall	11
2.2.3 IDS (Intrusion Detection Sistem).....	12

2.2.4 Snort	12
2.2.5 Linux Ubuntu	14
2.2.6 LOIC (Low Orbit Ion Cannon)	15
2.2.7 Nmap (Port Scanning).....	16
2.2.8 Hping3.....	17
2.2.9 Brute Force (Hydra)	18
2.2.10 Network Development Life Cycle (NDLC).....	19
BAB III METODE PENELITIAN.....	21
3.1 Objek Penelitian	21
3.1.1 Diagram Alur Penelitian	21
3.2 Analysis.....	23
3.2.1 Studi Literatur	24
3.2.2 Identifikasi Masalah	24
3.2.3 Analisis Kebutuhan Fungsional	24
3.2.4 Analisis Kebutuhan Non-Fungsional	24
3.2.5 Spesifikasi Perangkat Keras	25
3.3 Tahap Design (Perancangan)	27
3.3.1 Arsitektur Sistem Keamanan	27
3.3.2 Topologi jaringan dan konfigurasi IP Address.....	28
3.4 Tahap Simulation/Prototype	29
3.4.1 Simulasi Konektivitas Jaringan.....	29
3.4.2 Simulasi Segmentasi Jaringan.....	31
3.5 Tahap Implementasi	32
3.6 Tahap Monitoring.....	32
3.6.1 Monitoring Alert Snort.....	33

3.7 Manajemen.....	34
BAB IV HASIL DAN PEMBAHASAN	35
4.1 Hasil Implementasi Sistem.....	35
4.1.1 Implementasi Pada Router PfSense	35
4.1.2 Implementasi Firewall Rules.....	36
4.1.3 Implementasi IDS Snort.....	38
4.2 Dashboard PfSense.....	39
4.3 Analisis Hasil Konfigurasi Intrusion Detection System (Snort).....	40
4.4 Simulasi Pengujian Penetration Testing	41
4.4.1 Analisis Hasil Pengujian Pemindaian Jaringan (Port Scanning)	41
4.4.2 Analisis Hasil Pengujian Denial of Service (DoS/DDoS)	42
4.4.3 Hasil Pengujian Brute Force (Hydra).....	44
4.5 Pembahasan.....	46
4.5.1 Evaluasi Efektivitas Firewall PfSense Dan Isolasi Segmentasi.....	46
4.5.2 Analisis Mekanisme Deteksi Snort	48
4.5.3 Analisis Komparatif Kinerja CPU, Overhead, Throughput.....	49
4.6 Evaluasi Sistem	51
4.6.1 Kriteria Dan Indikator Keberhasilan Sistem	51
4.6.2 Evaluasi Dampak Terhadap Performa Sistem.....	52
4.6.3 Sintesis Keunggulan Sistem Berbasis pfSense-Snort	53
BAB V PENUTUP.....	54
5.1 Kesimpulan	54
5.2 Saran.....	54
DAFTAR PUSTAKA	56

DAFTAR TABEL

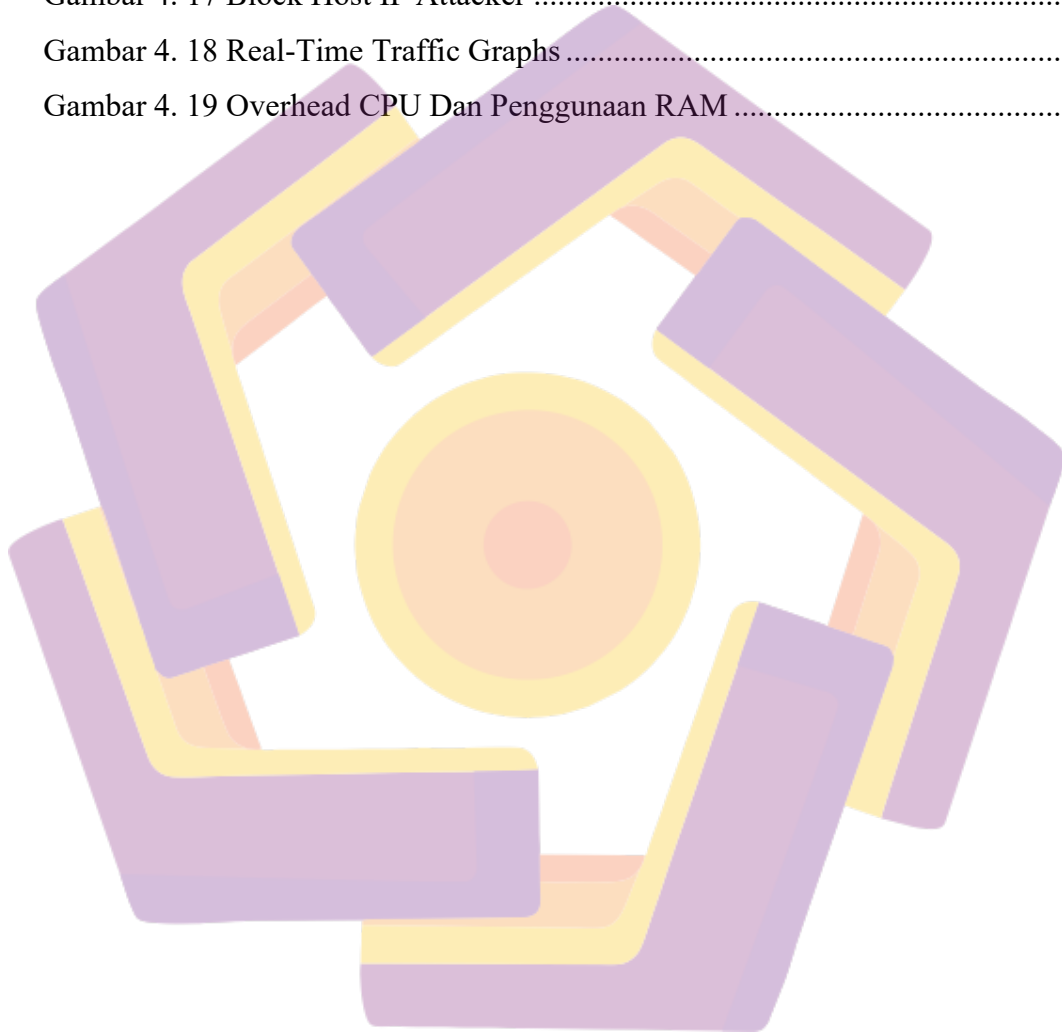
Tabel 2. 1 Keaslian Penelitian.....	9
Tabel 3. 1 Tabel Perangkat Keras (Hardware)	25
Tabel 3. 2 Spesifikasi Hardware Laptop	26
Tabel 3. 3 Spesifikasi Software.....	26
Tabel 3. 4 IP Address Jaringan	29
Tabel 4. 1 Parameter Pengujian Keamanan Jaringan Dan Tindakan Responsif Dari Sistem Firewall PfSense Dan IDS Snort.....	45
Tabel 4. 2 Kriteria dan Hasil Evaluasi Sistem Keamanan Jaringan.....	51
Tabel 4. 3 Evaluasi Dampak Terhadap Performa Sistem	52



DAFTAR GAMBAR

Gambar 2. 1 PfSense	10
Gambar 2. 2 Firewall.....	11
Gambar 2. 3 Snort	12
Gambar 2. 4 Linux / Ubuntu	14
Gambar 2. 5 LOIC Attack.....	15
Gambar 2. 6 Nmap Port Scanning.....	16
Gambar 2. 7 Hping3 Attack	17
Gambar 2. 8 Hydra Tools Brute Force.....	18
Gambar 2. 9 Network Development Life Cycle (NDLC).....	19
Gambar 3. 1 Diagram Alur Penelitian.....	21
Gambar 3. 2 Modem Router Indihome 2C6D.A, HG8145X6-10.....	25
Gambar 3. 3 Arsitektur Sistem Keamanan.....	27
Gambar 3. 4 Topologi Jaringan.....	28
Gambar 3. 5 LAN Ubuntu Ping WAN,OPT1	30
Gambar 3. 6 OPT1 Windows Ping WAN, LAN.....	30
Gambar 3. 7 Segmentasi WAN dan LAN Network.....	31
Gambar 3. 8 States Table	33
Gambar 3. 9 Alert Snort IDS.....	33
Gambar 3. 10 Dashboard PfSense.....	34
Gambar 4. 1 Implementasi Interface IP Address PfSense	35
Gambar 4. 2 Implementasi Firewall Rules WAN.....	36
Gambar 4. 3 Implementasi Firewall Rules LAN.....	37
Gambar 4. 4 Implementasi Firewall Rules OPT1	38
Gambar 4. 5 Implementasi Interface Rules IDS snort	38
Gambar 4. 6 Dashboard PfSense.....	39
Gambar 4. 7 Analisis Hasil Konfigurasi Snort	40
Gambar 4. 8 Simulasi Port Scanning	41
Gambar 4. 9 Hasil Tampilan Log Alerts Possible TCP Null Scan	42
Gambar 4. 10 Simulasi Serangan LOIC.....	43
Gambar 4. 11 Hasil Log Alerts Snort Simulasi DoS Attack.....	43

Gambar 4. 12 Simulasi Serangan Brute Force (Hydra)	44
Gambar 4. 13 Hasil Log Alerts Simulasi Brute Force (Hydra).....	44
Gambar 4. 14 Segmentasi Interface Jaringan.....	46
Gambar 4. 15 State Table.....	47
Gambar 4. 16 Firewall Rules WAN, LAN, OPT1	48
Gambar 4. 17 Block Host IP Attacker	49
Gambar 4. 18 Real-Time Traffic Graphs	50
Gambar 4. 19 Overhead CPU Dan Penggunaan RAM	51



INTISARI

Perkembangan teknologi informasi yang semakin pesat menyebabkan meningkatnya ancaman keamanan jaringan, mendorong administrator jaringan untuk meningkatkan layanan perlindungan terhadap ancaman yang berasal dari luar. Hal ini ditandai dengan banyaknya kasus pencurian data dan akses tidak sah. Oleh karena itu, penelitian ini bertujuan mengoptimalkan keamanan jaringan melalui penerapan firewall pfSense dan *Intrusion Detection Sistem* (IDS) Snort pada lingkungan simulasi small office network. Metode yang digunakan adalah *Network Development Life Cycle* (NDLC). Pada tahap implementasi, dilakukan konfigurasi pembagian segmentasi antarmuka (interface), penerapan aturan firewall (firewall rules), serta integrasi IDS Snort pada setiap segmen jaringan. Selanjutnya, dilakukan pengujian penetrasi (penetration testing) menggunakan beberapa alat simulasi serangan. Hasil pengujian menunjukkan bahwa integrasi pfSense dan Snort berhasil melakukan pemantauan dan pemblokiran otomatis ketika jaringan diserang, termasuk serangan *Port Scanning*, *Denial of Service* (DoS), dan *Brute Force*.

Kata Kunci: PfSense, Firewall, IDS, Snort, Keamanan Jaringan

ABSTRACT

The rapid advancement of information technology has led to an increase in network security threats, encouraging network administrators to improve network services and protection against external threats. Numerous cases of data theft and unauthorized access have highlighted the need for stronger security measures. Therefore, this study aims to optimize network security through the implementation of a pfSense firewall and the Snort Intrusion Detection Sistem (IDS) in a Small Office Network simulation environment. The method used is the Network Development Life Cycle (NDLC). During the implementation phase, network segmentation between interfaces was configured, firewall rules were applied, and Snort IDS was integrated into each network interface. Furthermore, security testing was conducted using several attack tools to simulate network attacks. The testing results demonstrate that the integration of the pfSense firewall and Snort successfully monitors and automatically blocks malicious activities, including Port Scanning, Denial of Service (DoS), and Brute Force attacks.

Keyword : PfSense, Firewall, Snort, IDS, Network Security