MIND (Multimedia Artificial Intelligent Networking Database) Journal

MIND Journal | ISSN (p): 2528-0015 | ISSN (e): 2528-0902 | Vol. 11 | No. 1 | Halaman 102 - 114
DOI : https://doi.org/10.26760/mindjournal.v11i1.102-114 Juni 2026

Evaluasi Kinerja dan Keamanan Jaringan Menggunakan IDS *Snort* pada Disdukcapil Tasikmalaya

HEGIRA MUSYAFA KARTIWAN*, FATCKU ROCHMAN, HELMY DZULFIKAR

Program Studi Sistem Informasi, Universitas Siliwangi, Tasikmalaya, Indonesia

Email: 247007111028@student.unsil.ac.id

Received 23 April 2026 **|** *Revised* 2 Juni 2026 **|** *Accepted* 15 Juni 2026

ABSTRAK

Penelitian ini mengevaluasi kinerja dan keamanan jaringan di Disdukcapil Kabupaten Tasikmalaya yang rentan karena belum memiliki sistem keamanan memadai. Menggunakan metode Network Development Life Cycle (NDLC) dan simulasi Graphical Network Simulator-3 (GNS3), diimplementasikan Intrusion Detection System (IDS) berbasis Snort yang diintegrasikan dengan iptables sebagai IPS. Hasil menunjukkan serangan SYN Flood menurunkan throughput hingga 99,99% dan meningkatkan latency 95 kali lipat. Snort berhasil mendeteksi seluruh serangan dengan detection rate 100%, sementara mekanisme IPS auto-block memulihkan performa jaringan mendekati kondisi normal. Penelitian ini merekomendasikan solusi keamanan open-source yang efektif dan ekonomis bagi instansi pemerintah.

***Kata kunci**: Snort, keamanan jaringan, quality of service, NDLC, GNS3, IPS*

ABSTRACT

This study evaluates the network performance and security of Disdukcapil Tasikmalaya Regency, which is vulnerable due to the lack of security systems. Using the Network Development Life Cycle (NDLC) method and Graphical Network Simulator-3 (GNS3) simulation, a Snort-based Intrusion Detection System (IDS) integrated with iptables as an IPS was implemented. Results show that SYN Flood attacks reduce throughput by 99.99% and increase latency 95-fold. Snort successfully detected all attacks with a 100% detection rate, while the IPS auto-block mechanism restored network performance close to normal. This research recommends an effective and economical open-source security solution for government agencies.

***Keywords**: Snort, network security, quality of service, NDLC, GNS3, IPS*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa transformasi digital di berbagai sektor, termasuk pemerintahan. Dinas Kependudukan dan Pencatatan Sipil (Disdukcapil) sebagai salah satu Satuan Kerja Perangkat Daerah (SKPD) memiliki peran vital dalam pengelolaan data kependudukan yang bersifat sensitif dan strategis. Keberhasilan pelayanan publik di Disdukcapil sangat bergantung pada ketersediaan infrastruktur jaringan komputer yang andal, stabil, dan aman. Jaringan komputer menjadi tulang punggung dalam mendukung berbagai aktivitas operasional, mulai dari proses administrasi kependudukan, layanan pencatatan sipil, hingga integrasi data dengan sistem kependudukan nasional . Tanpa didukung oleh jaringan yang memadai, efektivitas dan efisiensi pelayanan publik dapat terganggu, yang berpotensi menimbulkan dampak negatif terhadap kepercayaan masyarakat **(Santoso & Dianing Asri, 2024)**.

Ancaman terhadap keamanan jaringan komputer semakin kompleks seiring meningkatnya ketergantungan pada sistem digital. Serangan siber seperti *port scanning*, *brute force login*, dan *Denial of Service* (DoS) menjadi ancaman serius yang dapat mengganggu ketersediaan layanan dan membahayakan integritas data **(Intan Sabila dkk., 2025)**. Apabila tidak terdeteksi sejak dini, aktivitas ini dapat menjadi pintu masuk bagi serangan yang lebih merusak. *Intrusion Detection System* (IDS) menjadi komponen penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data pada jaringan skala kecil-menengah, termasuk pada instansi pemerintah seperti Disdukcapil yang mengelola data kependudukan yang sangat sensitif **(Nasution & Haris Munandar, 2025)**.

Hasil observasi dan wawancara lapangan di Disdukcapil Kabupaten Tasikmalaya menunjukkan bahwa infrastruktur jaringan yang ada tidak dilengkapi dengan *firewall*, sistem pemantauan lalu lintas jaringan, antivirus server, maupun dokumentasi topologi jaringan yang memadai **(Anam & Fachri, 2025)**. Kondisi ini menciptakan celah keamanan yang berpotensi dieksploitasi oleh pihak tidak bertanggung jawab untuk melakukan intrusi yang membahayakan data kependudukan sensitif.

Salah satu solusi yang banyak diadopsi untuk meningkatkan keamanan jaringan adalah penggunaan IDS berbasis *open-source*. *Snort* merupakan sistem deteksi intrusi yang diterima luas dalam industri untuk memantau lalu lintas jaringan secara *real-time* dengan kemampuan mendeteksi berbagai jenis serangan berdasarkan pola tertentu **(Intan Sabila dkk., 2025)**. Keunggulan *Snort* terletak pada fleksibilitasnya dalam dikonfigurasi sesuai kebutuhan serta kemampuannya untuk diintegrasikan dengan *firewall* seperti *iptables* guna memberikan respons otomatis terhadap ancaman **(Nasution & Haris Munandar, 2025)**.

Penelitian terdahulu yang relevan telah menunjukkan efektivitas *Snort* dalam berbagai konteks keamanan jaringan. Perancangan jaringan internet di SMK Strada Jakarta menggunakan metode *Network Development Life Cycle* (NDLC) dengan simulasi GNS3 dan *MikroTik Router* OS berhasil meningkatkan stabilitas jaringan melalui manajemen *bandwidth* dan segmentasi VLAN **(Santoso & Dianing Asri, 2024)**. Implementasi kombinasi *Snort* dan *iptables* pada infrastruktur jaringan skala kecil-menengah mampu mencapai *True Positive Rate* (TPR) sebesar 93,3% dan *False Positive Rate* (FPR) hanya 2% dalam mendeteksi serangan *port scanning*, *brute force*, dan ICMP flood, dengan waktu deteksi rata-rata 0,8 detik untuk *port scanning* **(Nasution & Haris Munandar, 2025).**

Evaluasi kerentanan keamanan jaringan nirkabel menggunakan metode *penetration testing* dengan *Aircrack-ng* dan teknik *dictionary attack* berhasil membobol jaringan WPA2-PSK dengan sandi sederhana dalam waktu kurang dari satu menit, sehingga direkomendasikan penggunaan sandi yang kompleks serta migrasi ke protokol WPA3 **(Anam & Fachri, 2025)**.

Pengujian kerentanan *router MikroTik* terhadap serangan *brute force* menggunakan alat Hydra, Medusa, dan Ncrack menemukan bahwa *port* SSH, Telnet, FTP, dan HTTP rentan terhadap serangan tersebut, kemudian metode filtering addresslist dengan tiga level blokir bertingkat efektif memblokir IP penyerang secara otomatis **(Raharjo dkk., 2024)**.

Evaluasi efektivitas IDS mencakup beberapa dimensi penting: tingkat deteksi serangan, keakuratan deteksi (termasuk *false positive* rate), kecepatan respons, dan dampak terhadap kinerja jaringan secara keseluruhan. Aspek terakhir ini krusial namun sering diabaikan penerapan IDS tanpa mempertimbangkan *overhead* performa dapat menciptakan bottleneck baru pada jaringan. Standar TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) menyediakan kerangka evaluasi QoS yang terstruktur melalui parameter *throughput*, *packet loss*, delay, dan *jitter* , sehingga cocok digunakan sebagai acuan dalam mengukur *trade-off* antara keamanan dan performa setelah penerapan IDS/IPS. Eskalasi dan variasi serangan siber modern telah mendorong inovasi berkelanjutan pada arsitektur IDS, bergeser dari metode konvensional menuju pendekatan yang lebih cerdas. Pengembangan model IDS berbasis *Double Layer Gated Recurrent Unit* (GRU) dengan pendekatan feature fusion berhasil mencapai akurasi 98,60% pada pengujian dengan dataset standar IDS, lebih tinggi dibandingkan GRU tunggal dan metode *machine learning* konvensional. Demikian pula pengembangan IDS berbasis *machine learning* menggunakan algoritma J48, Naïve Bayes, dan AdaBoostM1 pada dataset UNSW-NB15 dan CICIDS2017 menghasilkan akurasi tertinggi oleh algoritma J48 sebesar 99,839% setelah seleksi fitur **(Maulani & Umam, 2023; Ardiansyah & Pamuji, 2025; Wijaya, 2025; Suryadi & Marzuki, 2023).**

Implementasi *Snort* untuk mendeteksi serangan *port scanning* Nmap pada simulasi jaringan virtual berbasis *VirtualBox* membuktikan bahwa *Snort* mampu mendeteksi secara *real-time* berbagai teknik pemindaian seperti SYN *Scan*, Ping *Scan*, UDP *Scan*, dan *Aggressive Scan* dengan menghasilkan peringatan (*alert*) berdasarkan *rule* yang telah dikonfigurasi **(Intan Sabila dkk., 2025)**. GNS3 (*Graphical Network Simulator* 3) juga terbukti efektif digunakan untuk simulasi jaringan kompleks seperti implementasi *Virtual Extensible* LAN (VXLAN) untuk interkoneksi lokasi yang berbeda secara geografis, yang berhasil menciptakan konektivitas *layer* 2 di atas jaringan *layer* 3 dalam satu segmen IP yang sama **(Do Abdullah dkk., 2024)**.

Dari perspektif *trade-off* keamanan dan performa, penelitian **(Iqbal Maqdum Razzanda & Muhammad Koprawi, 2024)** membuktikan bahwa implementasi *Snort* sebagai IDS dikombinasikan dengan *iptables* sebagai IPS mampu mendeteksi serangan TCP *Port Scanning* dan *ICMP Flood*ing secara akurat sekaligus memblokir serangan secara *real-time*, dengan tingkat keberhasilan penuh pada kedua jenis serangan. Integrasi Deep Packet Inspection (DPI) dengan IDS juga terbukti meningkatkan True Positive Rate deteksi DDoS dari 87,4% menjadi 95,2% sekaligus menurunkan False Positive Rate dari 12,6% menjadi 4,8%, dengan kompensasi berupa peningkatan *latency* rata-rata 2,6 ms sebuah *trade-off* yang secara umum dapat diterima **(Syujak dkk., 2024)**. Selain itu, evaluasi QoS jaringan menggunakan standar TIPHON menunjukkan bahwa parameter delay di bawah 150 ms, *packet loss* 0–2%, dan *jitter* di bawah 75 ms dikategorikan sebagai "Sangat Bagus" dan "Bagus", sehingga standar ini menjadi acuan yang tepat untuk mengevaluasi dampak penerapan IDS terhadap kualitas layanan jaringan **(Andrean Ardiansyah & Fandi Yulian Pamuji, 2025)**. Evaluasi efektivitas IDS sendiri mencakup empat dimensi utama: tingkat deteksi, keakuratan (*false positive*/negative rate), kecepatan respons, dan dampak terhadap kinerja jaringan **(Isma Elan Maulani & Aldo Faisal Umam, 2023)** dimensi keempat inilah yang menjadi fokus pembeda penelitian ini.

Berdasarkan tinjauan literatur terdahulu, teridentifikasi tiga kesenjangan penelitian (*research gap*) utama. Pertama, masih terbatasnya kajian komprehensif yang mengevaluasi dampak multi-skenario serangan terhadap parameter *Quality of Service* (QoS) sekaligus mengkomparasikan efektivitas IDS dan IPS, khususnya pada infrastruktur jaringan instansi pemerintah tingkat kabupaten. Kedua, mayoritas studi terdahulu cenderung bersifat deskriptif dalam memaparkan degradasi performa jaringan, tanpa menguraikan mekanisme teknis yang mendasarinya, sehingga analisis kausalitas antara serangan dan penurunan kinerja masih belum mendalam. Ketiga, aspek *trade-off* antara *overhead* keamanan dan keterbatasan hardware pada instansi pemerintah daerah jarang dibahas secara eksplisit, padahal instansi seperti Disdukcapil umumnya beroperasi dengan infrastruktur komputasi terbatas menjadikan efisiensi implementasi IDS sebagai pertimbangan praktis yang tidak dapat diabaikan.

Penelitian ini hadir untuk mengisi celah tersebut melalui evaluasi kinerja jaringan berbasis standar TIPHON pada empat skenario terstruktur (*baseline*, serangan tanpa IDS, dengan IDS, dengan IPS *auto-block*) di konteks jaringan Disdukcapil Kabupaten Tasikmalaya. Analisis mencakup penjelasan teknis mekanisme degradasi performa pada setiap jenis serangan serta kuantifikasi *trade-off* antara keamanan dan performa jaringan. Penelitian ini bertujuan: (1) mengevaluasi dampak serangan *port scanning*, *brute force* SSH, *SYN Flood*, dan *ICMP Flood* terhadap parameter QoS jaringan; (2) mengimplementasikan IDS berbasis *Snort* dan IPS dengan integrasi *iptables*; (3) menganalisis *trade-off* antara *overhead* keamanan dan performa jaringan dalam konteks keterbatasan hardware instansi pemerintah daerah; serta (4) menyusun rekomendasi implementasi IDS dan IPS yang efisien, ekonomis, dan berdaya guna tinggi, guna menjembatani kebutuhan keamanan siber dengan keterbatasan infrastruktur perangkat keras pada instansi pemerintah daerah.

2. METODE PENELITIAN

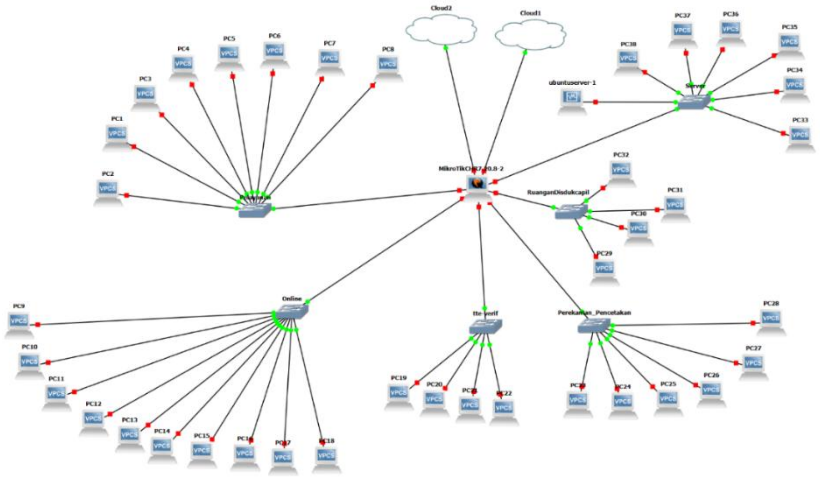
Penelitian ini menggunakan metode *Network Development Life Cycle* (NDLC) sebagai kerangka kerja yang terdiri dari empat tahapan terstruktur dan berkesinambungan, disesuaikan dengan ruang lingkup evaluasi jaringan berbasis simulasi.

2.1. *Analysis*

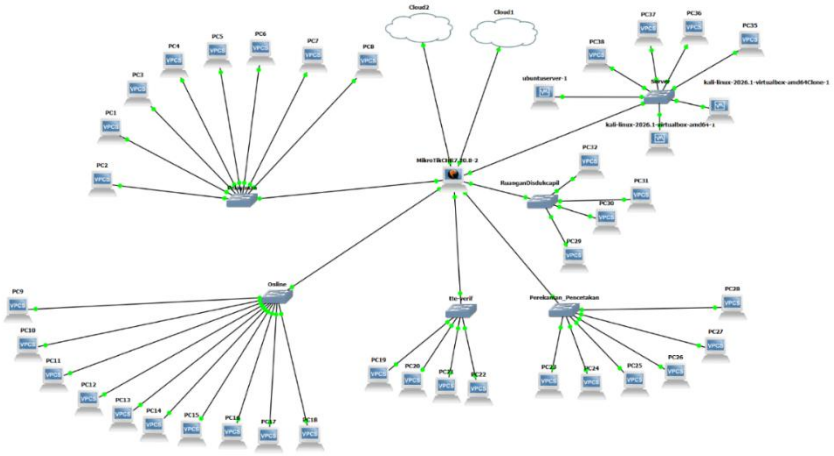
Tahap analisis bertujuan untuk memahami kondisi jaringan komputer yang sedang berjalan (*existing network*) di Disdukcapil Kabupaten Tasikmalaya. Pengumpulan data dilakukan melalui observasi langsung terhadap infrastruktur jaringan dan wawancara dengan staf teknis. Data mencakup topologi jaringan, perangkat keras, pengalamatan IP, serta kebijakan keamanan yang diterapkan. Hasil observasi mengungkapkan bahwa jaringan terdiri dari sekitar 32 komputer di kantor utama, koneksi *bandwidth* tinggi, satu aplikasi utama (SIAK), VPN ke pemerintah pusat, dan tidak memiliki *firewall*, *antivirus server*, maupun dokumentasi topologi.

2.2. *Design*

Pada tahap ini dirancang dua desain topologi jaringan: (1) Desain topologi eksisting yang merepresentasikan kondisi jaringan Disdukcapil saat ini berdasarkan data analisis, digunakan sebagai *baseline* evaluasi; (2) Desain topologi baru (rekomendasi) yang mengintegrasikan IDS berbasis *Snort* sebagai komponen keamanan jaringan tambahan. Kedua topologi dibuat menggunakan aplikasi GNS3.



Gambar 1. Topologi Jaringan Eksisting



Gambar 2. Topologi Jaringan Rekomendasi

2.3. *Simulation Prototyping*

Simulasi dilakukan menggunakan GNS3 dengan VM Ubuntu sebagai platform operasional Snort 2.9.20. Versi ini dipilih atas dasar kestabilan operasional yang telah teruji serta ketersediaan dokumentasi dan referensi implementasi yang jauh lebih luas dibandingkan Snort 3 yang relatif baru. Selain itu, Snort 2.9.20 memiliki kompatibilitas yang lebih unggul dengan mekanisme integrasi iptables melalui skrip Bash yang merupakan komponen inti dari sistem *auto-block* pada penelitian ini. Pengujian pada kedua topologi disimulasikan menggunakan empat skenario serangan: (1) *port scanning* menggunakan Nmap; (2) brute force SSH menggunakan Hydra; serta (3) SYN *flood* dan (4) ICMP *flood* menggunakan hping3. Pendekatan simulasi ini dipilih dengan pertimbangan etis, guna menghindari risiko terganggunya layanan publik dan menjaga keamanan data kependudukan yang sensitif apabila pengujian dilakukan langsung pada jaringan aktif.

2.4. *Monitoring & Evaluation*

Evaluasi kinerja jaringan diukur berdasarkan parameter *throughput*, *latency*, *packet loss*, dan *bandwidth utilization* menggunakan *Wireshark* dan *iPerf3*. Evaluasi keamanan dilakukan dengan menganalisis kemampuan *Snort* dalam mendeteksi dan menghasilkan *alert* terhadap

serangan. Hasil dari kedua topologi dibandingkan untuk mengukur efektivitas desain jaringan baru.

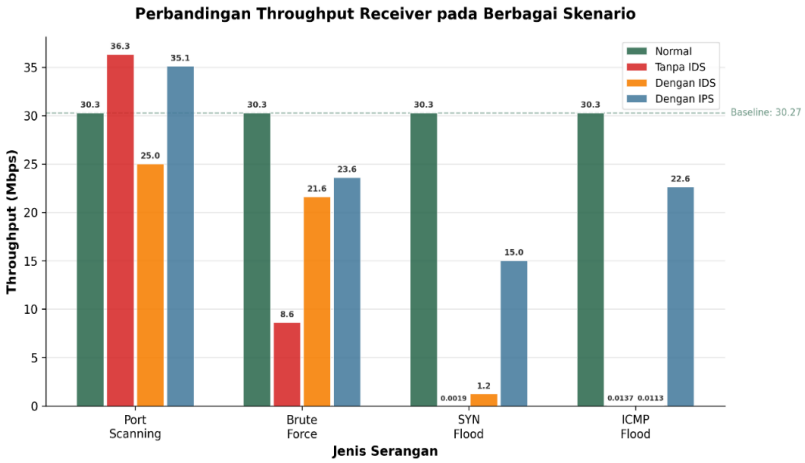
3. HASIL DAN PEMBAHASAN

3.1 Konfigurasi Jaringan Simulasi

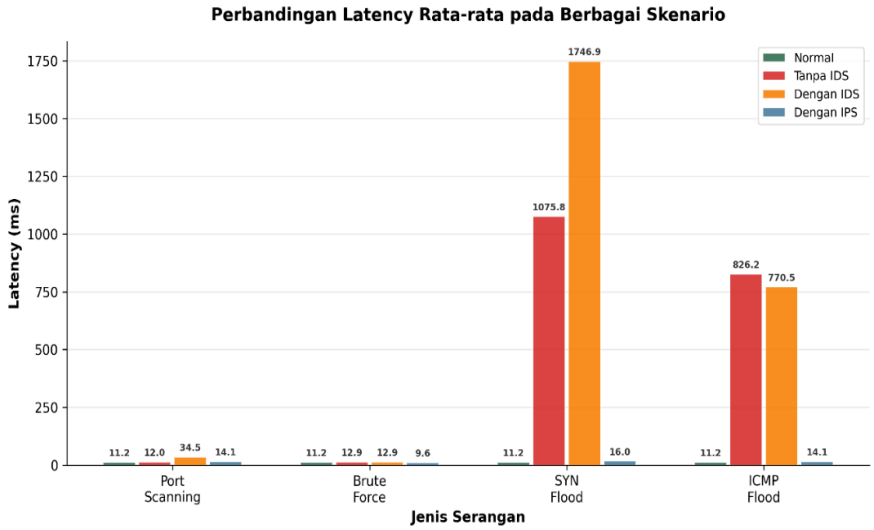
Infrastruktur jaringan disimulasikan melalui GNS3 menggunakan MikroTik CHR 7.20.8 sebagai *router* utama. Arsitektur jaringan dirancang menggunakan *star topology* yang dibagi ke dalam enam segmen VLAN untuk merepresentasikan pembagian area kerja operasional di Disdukcapil. Pendekatan segmentasi VLAN ini selaras dengan studi Umah dkk. (2025) yang menunjukkan bahwa penerapan VLAN dapat meningkatkan *throughput* hingga 60% dan menurunkan *packet loss* hingga 80% pada jaringan LAN: Pelayanan (Loket), Online, TTE-Verif, RuanganDisdukcapil, Perekaman_Pencetakan, dan Server. *Router* dikonfigurasi dengan tujuh *interface Ethernet* (ether1 sebagai *gateway* WAN, ether2–ether7 sebagai *gateway* masing-masing VLAN dengan subnet /24). Keamanan jaringan diimplementasikan melalui Ubuntu Server (10.10.10.95) yang menjalankan *Snort* 2.9.20 sebagai IDS/IPS. Untuk memastikan performa deteksi yang optimal, *Virtual Machine* (VM) tersebut dialokasikan memori sebesar 3.457 MB dan 2 vCPU pada lingkungan *VirtualBox* menggunakan akselerasi KVM *Paravirtualization*. Seluruh ekosistem simulasi ini beroperasi di atas *host machine* berspesifikasi prosesor Intel Core i7-8650U dan RAM 32 GB, sedangkan, Kali Linux berperan sebagai mesin penyerang. *Snort* dikonfigurasi dengan aturan lokal (*local.rules*) untuk mendeteksi empat jenis ancaman: *ICMP Flood*, SYN *Scan*, SSH *Brute Force*, dan Nmap Xmas *Scan*.

3.2 Kinerja Jaringan Kondisi Normal (*Baseline*)

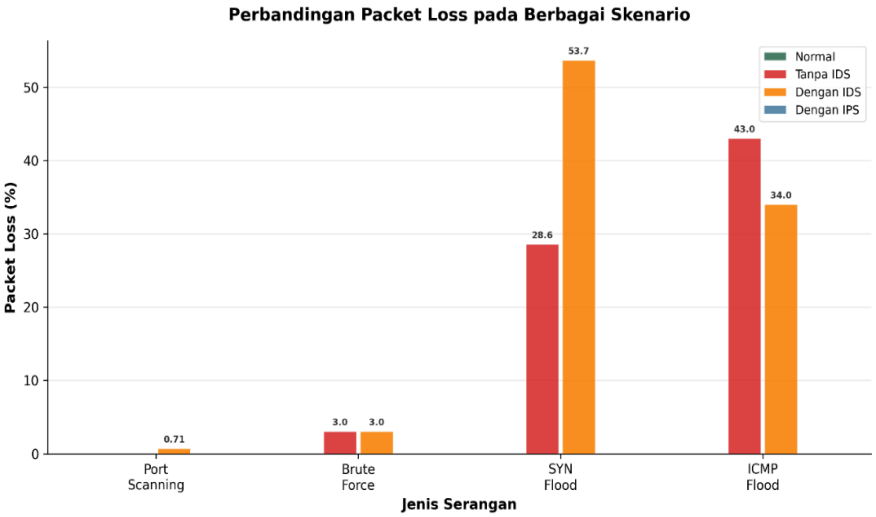
Pengujian *baseline* dilakukan menggunakan iPerf3 (*throughput* TCP/UDP) dan ping (*latency/packet loss*) selama 30 detik per sesi, diulang tiga kali. Hasil rata-rata: *throughput* TCP receiver 30,27 Mbits/sec, *throughput* UDP *receiver* 9,90 Mbits/sec, *latency* rata-rata 11,247 ms, dan *packet loss* 0%. Nilai *latency* ini termasuk kategori "Sangat Bagus" berdasarkan standar TIPHON yang menetapkan delay di bawah 150 ms pada indeks 4 ("Sangat Bagus"), *packet loss* 0–2% pada indeks 4, dan *jitter* di bawah 75 ms pada indeks 3 ("Bagus") (Ardiansyah & Pamuji, 2025). Nilai QoS *baseline* ini merupakan acuan penting untuk mengkuantifikasi degradasi performa pada skenario serangan dan pemulihan pada skenario IPS. Variasi retransmission TCP (rata-rata 154,3 paket) disebabkan oleh persaingan sumber daya CPU pada lingkungan virtualisasi GNS3, hal ini merupakan artefak simulasi yang umum terjadi dan bukan indikasi degradasi jaringan sesungguhnya. Secara keseluruhan, kondisi *baseline* menunjukkan performa QoS yang memadai sebagai acuan komparatif antar skenario.



Gambar 3. Perbandingan *Throughput Receiver* pada Empat Skenario Pengujian



Gambar 4. Perbandingan *Latency* Rata-Rata pada Empat Skenario Pengujian



Gambar 5. Perbandingan *Packet Loss* pada Empat Skenario Pengujian

3.3 Dampak Serangan Tanpa IDS

Skenario ini merepresentasikan kondisi eksisting jaringan Disdukcapil. Tiga jenis serangan diujikan: (1) *Port Scanning* (*Nmap Aggressive Scan*): tidak menyebabkan degradasi signifikan, *throughput* justru sedikit meningkat menjadi 36,3 Mbits/sec karena lalu lintas Nmap turut tercatat iPerf3, namun *retransmission* naik dari 154,3 menjadi 267; (2) *Brute Force SSH* (*Hydra*): *throughput* turun drastis dari 30,27 menjadi 8,61 Mbits/sec (penurunan 71,56%) dan *packet loss* naik menjadi 3,03%, akibat server kewalahan memproses permintaan autentikasi berulang yang membutuhkan komputasi kriptografi intensif per percobaan login; (3) *SYN Flood* (*hping3*): dampak paling destruktif, *throughput* turun hampir nol (1,91 Kbits/sec), *latency* melonjak 95 kali lipat menjadi 1.075,824 ms, dan *packet loss* mencapai 28,57%. Secara teknis, *SYN Flood* menyebabkan *exhaustion* pada *TCP half-open connection queue* di sisi server: setiap paket *SYN* yang masuk mengalokasikan *resource* untuk menunggu ACK yang tidak pernah datang, sehingga *connection table* jenuh dan server tidak mampu melayani koneksi *TCP* yang *legitimate*. Mekanisme inilah yang menjelaskan mengapa *throughput* efektif

iPerf3 mendekati nol meskipun paket serangan sendiri berukuran kecil; (4) *ICMP Flood* (*hping3*): *throughput* turun 99,95% menjadi 13,7 Kbits/sec, *latency* 826,158 ms, dan *packet loss* 43%. Secara teknis, *ICMP Flood* membanjiri *buffer* antrian *NIC* (*Network Interface Card*) dan *CPU interrupt handler—prosesor* habis melayani interrupt dari banjir paket *ICMP* sehingga tidak tersisa kapasitas untuk memproses paket *TCP/UDP* yang sah. Kondisi ini sangat berbahaya bagi operasional layanan kependudukan Disdukcapil karena aplikasi SIAK yang berbasis jaringan akan mengalami timeout dan kegagalan transaksi data kependudukan.

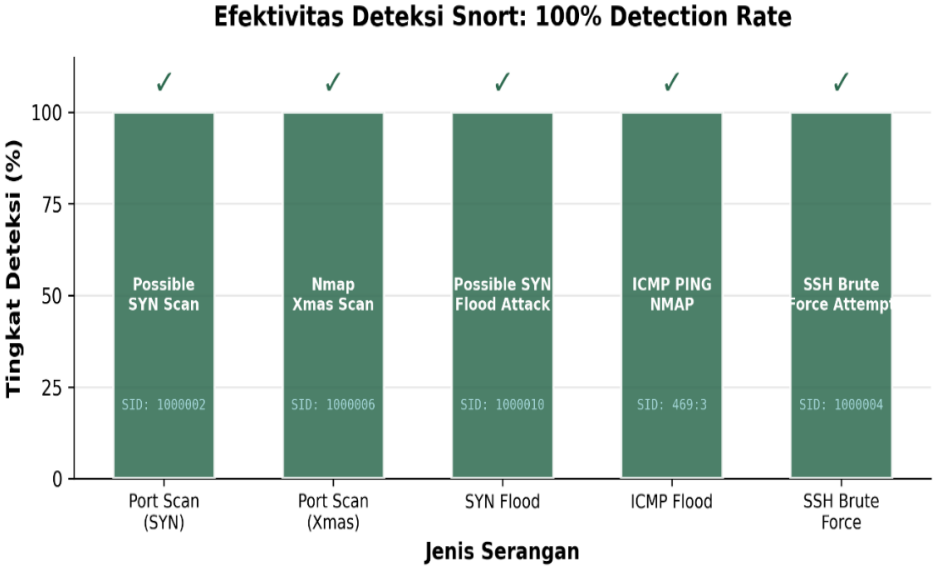
3.4 Efektivitas *Snort* sebagai IDS

Snort dalam mode NIDS berhasil mendeteksi seluruh jenis serangan secara *real-time*. Untuk *port scanning*, dihasilkan *alert*: Possible SYN Scan (sid:1000002), Nmap Xmas Scan (sid:1000006), dan SCAN nmap XMAS (sid:1228:7). Untuk *brute force* SSH, *alert* "SSH Brute Force Attempt" (sid:1000004) berhasil dihasilkan. Untuk SYN Flood, *alert* "Possible SYN Flood Attack" (sid:1000010) muncul berulang. Sementara itu, untuk *ICMP Flood*, *alert* "ICMP PING NMAP" (sid:469:3) dihasilkan secara masif. Keberadaan IDS menyebabkan sedikit *overhead* pada *throughput* saat *port scanning* (turun ke 25,0 Mbits/sec), namun fenomena menarik terjadi pada skenario *brute force*: *throughput* justru meningkat dari 8,61 Mbits/sec (tanpa IDS) menjadi 21,6 Mbits/sec (dengan IDS aktif). Hal ini dapat dijelaskan secara teknis, di mana proses inspeksi paket oleh Snort memperkenalkan *packet inspection latency* pada IDS. Fausto dkk. (2022) membuktikan secara eksperimental bahwa implementasi IDS dalam arsitektur jaringan memicu *delay* per paket yang bervariasi berdasarkan pola *flow* yang dikenali sistem; *flow* yang sudah dikenal memiliki *latency* inspeksi yang lebih rendah dibandingkan *flow* baru.

Dalam konteks serangan *brute force* SSH, setiap percobaan *login* yang berulang membentuk pola *flow* yang konsisten dan dikenali oleh Snort, sehingga *overhead* inspeksi menjadi lebih terprediksi dan terstruktur. *Micro-delay* yang diperkenalkan pada setiap paket SSH *brute force* secara kumulatif mengurangi laju percobaan autentikasi per satuan waktu, sehingga memberikan lebih banyak *window time* bagi *CPU server* untuk memproses trafik iPerf3 yang sah (*legitimate*). Mekanisme inilah yang menjelaskan peningkatan *throughput* yang teramati. Temuan ini sejalan dengan observasi Maulani & Umam (2023) yang menyatakan bahwa IDS yang aktif dapat secara tidak langsung memoderasi beban serangan pada sistem target. Secara keseluruhan, *trade-off* antara *overhead* IDS dan peningkatan keamanan jauh lebih menguntungkan dibanding risiko serangan tanpa deteksi, terutama mengingat sensitivitas data kependudukan yang dikelola Disdukcapil. Hasil ini juga didukung oleh penelitian terdahulu yang menunjukkan efektivitas Snort dalam mendeteksi berbagai jenis serangan secara presisi melalui investigasi forensik jaringan **(Khaliq & Sari, 2022; Pradita & Pramono, 2024).**

Untuk melengkapi evaluasi efektivitas IDS, dilakukan pengukuran *false positive rate* (FPR) melalui pengujian pada kondisi *traffic* normal tanpa serangan. Hasil menunjukkan bahwa Snort tidak menghasilkan satu pun *alert* selama periode *traffic* sah (*legitimate*) berlangsung (jumlah *alert* = 0), sehingga FPR tercatat 0%. Hal ini mengindikasikan bahwa *rule* yang dikonfigurasi cukup presisi dan tidak menghasilkan gangguan pada operasional normal jaringan. Pada skenario *ICMP Flood*, Snort menghasilkan 593.938 *alert* dengan seluruhnya terklasifikasi sebagai *ICMP-related*, mengonfirmasi *true positive rate* (TPR) 100% tanpa *false negative* yang terdeteksi. Hasil ini melampaui *benchmark* yang dilaporkan oleh **Nasution & Munandar (2025)** yang mencatat TPR 93,3% dan FPR 2% pada infrastruktur serupa, menunjukkan bahwa konfigurasi *rule* lokal yang disesuaikan berkontribusi signifikan terhadap presisi deteksi.

Hasil FPR 0% kemungkinan dipengaruhi oleh kondisi simulasi yang terkontrol, di mana traffic legitimate bersifat homogen dan tidak mencakup variasi pola komunikasi yang kompleks seperti pada jaringan produksi sesungguhnya.



Gambar 6. Efektivitas Deteksi *Snort* Terhadap Seluruh Jenis Serangan

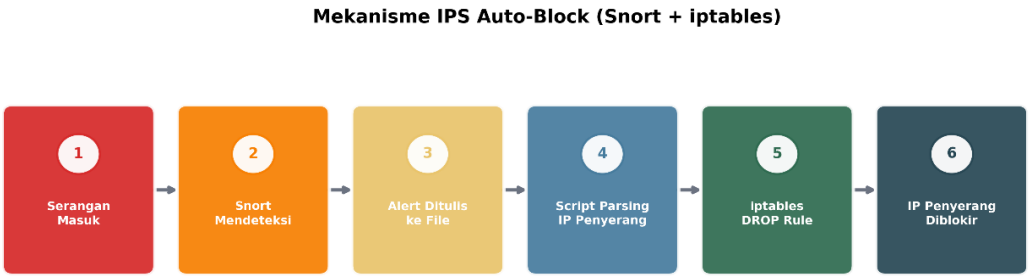
3.5 Efektivitas IPS *Auto-Block* (*Snort* dan *iptables*)

Skrip *auto-block* mengintegrasikan Snort dengan *iptables* melalui mekanisme tiga tahap: (1) Snort memantau dan menghasilkan *alert* berbasis *rule* ke *file log*; (2) skrip Bash membaca *log* secara *real-time* menggunakan *tail -F* dan mengekstrak IP sumber penyerang; (3) *iptables* menambahkan aturan DROP untuk memblokir seluruh trafik dari IP tersebut. Pendekatan ini konsisten dengan arsitektur IPS yang diterapkan oleh Razzanda & Koprawi (2024), di mana *iptables* berfungsi sebagai *enforcement layer* setelah deteksi oleh NIDS. Hasil pemblokiran menunjukkan pemulihan kinerja yang dramatis pada seluruh jenis serangan. Setelah IP penyerang diblokir pada skenario *SYN Flood*, *throughput* pulih dari 1,91 Kbits/sec menjadi 15,0 Mbits/sec dan *latency* turun dari 1.075,824 ms menjadi 15,966 ms. Pemulihan yang tidak mencapai 100% kondisi *baseline* (30,27 Mbits/sec) disebabkan oleh *inherent latency* pada *pipeline* deteksi-respons yang bersifat sekuensial.

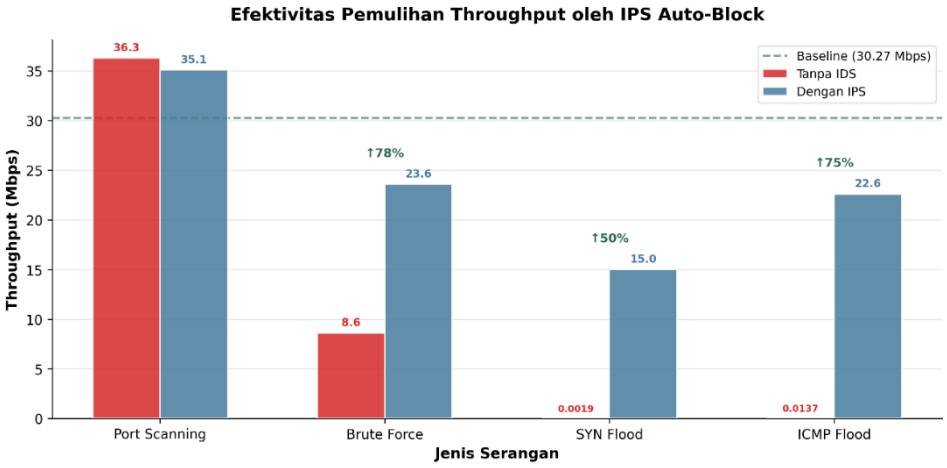
Mekanisme *auto-block* berbasis skrip Bash menghadapi risiko *race condition* antara dua proses yang berjalan asinkron: Snort menulis *alert* ke *file log* secara berkelanjutan, sementara skrip Bash membaca *log* tersebut melalui *polling* berkala menggunakan *tail -F*. Terdapat jeda waktu yang tidak dapat dieliminasi sepenuhnya antara momen Snort mendeteksi *threshold* serangan, momen *alert* dituliskan ke *file log*, dan momen *iptables* mengeksekusi aturan DROP terhadap IP penyerang. Selama jeda ini yang dapat berkisar dari beberapa milidetik hingga beberapa detik tergantung beban sistem, paket serangan masih dapat masuk dan membebani jaringan, sehingga kondisi jaringan tidak sempurna pulih ke *baseline*.

Kondisi ini diperparah pada skenario *flood* intensitas tinggi seperti *SYN Flood* dan *ICMP Flood*, di mana volume paket yang masuk selama jeda *pipeline* justru cukup untuk mempertahankan degradasi parsial meskipun pemblokiran akhirnya berhasil dieksekusi. Pada implementasi produksi, risiko *race condition* ini dapat diminimalkan melalui penggunaan Snort dalam mode *inline* yang mengintegrasikan deteksi dan *blocking* secara langsung pada jalur paket melalui *netfilter*, atau melalui format *log unified2* yang lebih efisien dibanding format *alert text* dalam hal kecepatan penulisan dan pembacaan *log*. Pada skenario *ICMP Flood*, *throughput* pulih ke

22,6 Mbits/sec dan *latency* turun 98,3% menjadi 14,061 ms dengan *packet loss* kembali 0%. Tabel berikut merangkum perbandingan *throughput receiver* pada keempat skenario.



Gambar 7. Diagram Alur Mekanisme IPS *Auto-Block*



Gambar 8. Efektivitas Pemulihan *Throughput* oleh Mekanisme IPS *Auto-Block*

Tabel 1. Perbandingan *Throughput* Receiver pada Empat Skenario Pengujian

Jenis Serangan	Normal	Tanpa IDS	Dengan IDS	Dengan IPS
Port Scanning	30,27 Mbps	36,3 Mbps	25,0 Mbps	35,1 Mbps
Brute Force SSH	30,27 Mbps	8,61 Mbps	21,6 Mbps	23,6 Mbps
SYN Flood	30,27 Mbps	1,91 Kbps	1,23 Mbps	15,0 Mbps
ICMP Flood	30,27 Mbps	13,7 Kbps	11,3 Kbps	22,6 Mbps

Temuan ini konsisten dengan hasil penelitian Nasution dkk. (2025) yang menunjukkan bahwa kombinasi *Snort* dan *iptables* mencapai *True Positive Rate* (TPR) 93,3% dengan *False Positive Rate* (FPR) 2% pada infrastruktur jaringan skala kecil-menengah. Perbandingan dengan penelitian Syujak dkk. (2024) yang mengintegrasikan DPI dengan IDS menunjukkan bahwa pendekatan berbasis *signature* (*Snort*) memiliki *overhead latency* lebih rendah (<5 ms vs 5,8 ms untuk DPI), namun memiliki kelemahan dalam mendeteksi serangan *zero-day* yang belum memiliki *signature*, sebuah *trade-off* yang perlu dipertimbangkan dalam pemilihan arsitektur keamanan. Dari dimensi evaluasi IDS yang dikemukakan Maulani & Umam (2023), penelitian ini telah memenuhi keempat aspek: tingkat deteksi (100% untuk semua jenis serangan), keakuratan (tidak ada *false negative* terdeteksi), kecepatan respons (deteksi *real-time* dengan *Snort*), dan dampak kinerja jaringan (*overhead* terukur dan terkuantifikasi). Rekomendasi implementasi bagi Disdukcapil mencakup: (1) penerapan *Snort* sebagai IDS pada segmen

server untuk deteksi *real-time*; (2) integrasi *iptables* melalui skrip *auto-block* untuk respons otomatis; (3) konfigurasi aturan lokal yang disesuaikan dengan pola ancaman relevan; (4) monitoring berkala *rule set* untuk mengantisipasi ancaman baru; dan (5) evaluasi berkala parameter QoS menggunakan standar TIPHON untuk memastikan *overhead* IDS tetap dalam batas yang dapat diterima.

Hasil pengujian menunjukkan bahwa meskipun terdapat sedikit *overhead* pada *throughput* saat IDS aktif, performa jaringan secara keseluruhan tetap stabil. Hal ini membuktikan bahwa efisiensi implementasi IDS berbasis Snort sangat relevan bagi instansi pemerintah daerah yang seringkali beroperasi dengan infrastruktur komputasi terbatas, namun tetap membutuhkan perlindungan siber yang andal. Terlepas dari hasil tersebut, penelitian ini memiliki beberapa keterbatasan yang perlu diakui. Pertama, seluruh pengujian dilakukan dalam lingkungan simulasi GNS3, sehingga hasil yang diperoleh belum tentu merepresentasikan kondisi jaringan produksi secara penuh, mengingat adanya perbedaan karakteristik lalu lintas dan beban kerja pada jaringan nyata. Kedua, pengujian serangan dilakukan dari satu titik penyerang tunggal (Kali Linux), sedangkan skenario ancaman nyata dapat melibatkan serangan terdistribusi dari banyak sumber secara simultan. Ketiga, Snort yang digunakan adalah versi 2.9.20 yang sudah tidak mendapatkan pembaruan aktif, sehingga kemampuan deteksi terhadap ancaman *zero-day* dan pola serangan terbaru dapat terbatas dibandingkan Snort 3 atau solusi IDS berbasis *machine learning*.

4. KESIMPULAN

Penelitian ini berhasil mengevaluasi kinerja dan keamanan jaringan komputer di Disdukcapil Kabupaten Tasikmalaya melalui simulasi GNS3 dalam empat skenario terstruktur. Berdasarkan pengujian tersebut, diperoleh beberapa simpulan: (1) Kondisi jaringan eksisting sangat rentan karena tidak memiliki *firewall*, IDS, maupun dokumentasi topologi; serangan *SYN Flood* mampu melumpuhkan jaringan dengan *throughput* turun 99,99% dan *latency* melonjak 95 kali lipat, sementara *ICMP Flood* menyebabkan *packet loss* 43%, kondisi yang secara teknis disebabkan oleh *exhaustion* TCP *half-open queue* dan *CPU interrupt overload*; (2) Snort terbukti efektif mendeteksi seluruh jenis serangan yang diujikan secara *real-time*, memenuhi keempat dimensi evaluasi IDS: tingkat deteksi, keakuratan, kecepatan respons, dan dampak performa; (3) Terdapat *trade-off* yang terukur antara keamanan dan performa: IDS menyebabkan *overhead throughput* hingga 17,5% saat *port scanning*, namun secara paradoksal meningkatkan *throughput* 151% saat *brute force* akibat efek moderasi beban serangan; (4) Integrasi Snort dengan *iptables* melalui skrip *auto-block* berhasil memulihkan *throughput* dari 1,91 Kbits/sec menjadi 15,0 Mbits/sec pada skenario *SYN Flood*, dan *packet loss* kembali ke 0% pada semua skenario pasca-blokir; (5) Penerapan IDS/IPS berbasis Snort merupakan solusi efektif dan ekonomis untuk instansi pemerintah dengan sumber daya terbatas, dengan performa yang sebanding dengan implementasi serupa pada infrastruktur skala kecil-menengah. Saran untuk penelitian selanjutnya mencakup: perluasan cakupan simulasi ke kantor kecamatan; pengembangan IDS berbasis *machine learning* (seperti pendekatan *Random Forest* dengan akurasi 99,94% untuk deteksi DDoS) untuk meningkatkan kemampuan mendeteksi serangan *zero-day*; penggunaan format *output* Snort *unified2* atau JSON untuk meningkatkan keandalan *auto-block*; serta evaluasi QoS berkala menggunakan standar TIPHON sebagai *monitoring* keberhasilan implementasi jangka panjang.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Dinas Kependudukan dan Pencatatan Sipil (Disdukcapil) Kabupaten Tasikmalaya atas izin dan kemudahan akses selama pelaksanaan observasi dan wawancara penelitian ini, serta kepada Dosen Pengampu mata kuliah Desain dan Manajemen Jaringan Komputer, Helmy Dzulfikar, S.T., M.Kom., atas bimbingan dan arahannya dalam penyusunan penelitian ini.

DAFTAR RUJUKAN

Anam, F., & Fachri, F. (2025). Evaluasi Kerentanan Keamanan Jaringan Nirkabel Menggunakan Metode Penetration Testing Dengan Aircrack-Ng. *Rabit; Jurnal Teknologi Dan Sistem Infoormasi Univrab*, *10*(1), 1–8.

Andrean Ardiansyah, & Fandi Yulian Pamuji. (2025). *Quality Of Service Jaringan Internet*. *9*(5), 8530–8537.

Do Abdullah, S., Lutfi, S., Fuad, A., Wahyudin Nur, A., & Ibrahim, A. (2024). Analisis Dan Desain VXLAN Untuk Interkoneksi Lokasi Yang Berbeda Di Universitas Khairun. *Jambura Journal Of Electrical And Electronics Engineering*, *6*, 212–217.

Fausto, A., Gaggero, G., Patrone, F., & Marchese, M. (2022). Reduction Of The Delays Within An Intrusion Detection System (IDS) Based On Software Defined Networking (SDN). *Ieee Access*, *10*, 109850–109862. Https://Doi.Org/10.1109/Access.2022.3214974

Intan Sabila, M., Tahir, M., Dwi Mardania, S., & Ilham Arifin, R. (2025). Implementasi Snort Sebagai Ids Dalam Mendeteksi Serangan Port Scanning Nmap Pada Simulasi Jaringan Virtual. *Jati (Jurnal Mahasiswa Teknik Informatika)*, *9*(4), 6944–6948. Https://Doi.Org/10.36040/Jati.V9i4.14340

Iqbal Maqdum Razzanda, & Muhammad Koprawi. (2024). Implementasi IDS Dan IPS Terhadap Serangan Tcp Port Scanning Dan Icmp Flooding. *Indonesian Journal Of Computer Science*, *13*(1), 3056–3068.

Isma Elan Maulani, & Aldo Faisal Umam. (2023). *Evaluasi Efektivitas Sistem Deteksi Intrusi Dalam Menjamin Keamanan Jaringan*. *3*(8), 662–667.

Khaliq, A., & Sari, S. N. (2022). Jaringan Untuk Identifikasi Serangan Jaringan Menggunakan Sistem Deteksi Intrusi (IDS). *Jurnal Nasional Teknologi Komputer*, *2*(3), 150–158.

Nasution, M., & Haris Munandar, M. (2025). Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Dan IDS Pada Infrastruktur Jaringan Skala Kecil-Menengah. *Jurnal Media Informatika [Jumin]*, *6*(6), 2732–2740. Http://Ejournal.Sisfokomtek.Org/Index.Php/Jumin

Nasution, M., Haris Munandar, M., & Korespondensi, E. P. (2025). *Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Dan IDS Pada Infrastruktur Jaringan Skala Kecil-Menengah*. Http://Ejournal.Sisfokomtek.Org/Index.Php/Jumin

Pradita, G., & Pramono, A. (2024). Implementasi Monitoring Keamanan Jaringan Pada Server Ubuntu Menggunakan Snort Intrusion Detection Prevention System (IDPS) Dan Telegram Bot Sebagai Media Notifikasi Di Pt Ss Utama. *Jati (Jurnal Mahasiswa Teknik Informatika)*, *8*(4), 5827–5834. Https://Doi.Org/10.36040/Jati.V8i4.10069

Raharjo, M., Firmansyah, Watmah, S., Alfian Armawan Sandi, T., & Lasmana Putra, J. (2024). Penetration Testing Pada Sistem Keamanan Jaringan Dengan Metode Filtering Addresslist Dan Ipservice. *Insantek – Jurnal Inovasi Dan Sains Teknik Elektro*, *5*(2), 71–75. Https://Doi.Org/10.31294/Insantek.V5i2.5947

Santoso, A., & Dianing Asri, S. (2024). Perancangan Jaringan Internet Dengan Simulasi Menggunakan GNS3 (Studi Kasus: Smk Strada Jakarta). *Jati (Jurnal Mahasiswa Teknik Informatika)*, *8*(4), 8040–8048. Https://Doi.Org/10.36040/Jati.V8i4.10625

Suryadi, A., & Marzuki, M. I. (2023). Pengembangan Intrusion Detection System (IDS) Berbasis Machine Learning. *Incomtech: Jurnal Telekomunikasi Dan Komputer*, *13*(3), 189–195. Http://Publikasi.Mercubuana.Ac.Id/Index.Php/Incomtech

Syujak, A. R., Diantoro, K., Yuni T, V., Soderi, A., & Sucipto, P. A. (2024). Integrasi Deep Packet Inspection Dengan Intrusion Detection System (IDS) Untuk Identifikasi Serangan Ddos Dalam Jaringan Skala Besar. *Jurnal Minfo Polgan*, *13*(2), 1971–1975. Https://Doi.Org/10.33395/Jmp.V13i2.14324

Umah, N. T., Yudanto, F. A., & Rilvani, E. (2025). Evaluasi Segmentasi VLAN Dalam Optimalisasi Kinerja Dan Keamanan Pada Jaringan Lan Di Universitas Pelita Bangsa. *Jurnal Ilmiah Ilkominfo - Ilmu Komputer & Informatika*, *8*(1), 38–47. Https://Doi.Org/10.47324/Ilkominfo.V8i1.313

Wijaya, M. R. (2025). Inovasi Model Intrusion Detection System (IDS) Menggunakan Double Layer Gated Recurrent Unit (GRU) Dengan Fitur Berbasis Fusion. *Jurnal Ilmiah Edutic : Pendidikan Dan Informatika*, *12*(1), 10–21. Https://Doi.Org/10.21107/Edutic.V12i1.28822