SMARTICS Journal, Vol.12 No.02, 2026. P144-154
ISSN online: 2476-9754, ISSN print: 2623-0429
DOI : https://doi.org/10.21067/smartics.v12i2.14779

Anomali Deteksi Log Trafic Sistem Keamanan Jaringan menggunakan *Intrusion Detection System* berbasis Snort pada Web Server

Wahyu Eko Febrianto[a], Ahmad Zulham Fahamsyah Havy[b], Muhammad Faishol Amrulloh[c]
[a,b,c]Universitas Yudharta, Pasuruan, Indonesia
[*]correspondence email : zulham92@yudharta.ac.id

Abstract—The growth of network and web service usage has increased the need for security systems capable of detecting and mitigating abnormal network activity. One threat that can disrupt service availability is the Distributed Denial of Service (DDoS) attack—specifically UDP Flood attacks—which can cause bandwidth saturation. This study aims to analyze abnormal traffic patterns on a web server and implement a Snort-based Intrusion Detection System (IDS) alongside a mitigation mechanism using the RAW Firewall on a MikroTik Cloud Core Router (CCR). A quantitative approach was employed, utilizing traffic and network log analysis to identify attack characteristics, including protocols, source and destination addresses, service ports, packet sizes, and packet transmission patterns. Analysis revealed relatively small UDP packets being repeatedly sent from multiple source IP addresses to port 53 (DNS) at high frequency, indicating UDP Flood/DDoS activity. Prior to mitigation, inbound traffic averaged 207.94 Mbps with a peak of 306.20 Mbps , whereas the available bandwidth capacity was only 100 Mbps . This situation caused bandwidth saturation and negatively impacted web server service quality. Mitigation was achieved by applying a RAW Firewall rule on the MikroTik CCR to drop UDP packets destined for port 53 during the *prerouting* stage. Following mitigation, inbound traffic dropped to an average of 43.21 Mbps with a peak of 60.72 Mbps . Consequently, peak traffic decreased by approximately 80.17% , returning to a level below the 100 Mbps bandwidth capacity. The results demonstrate that combining Snort IDS for detection and the MikroTik RAW Firewall for mitigation effectively reduces the impact of UDP Flood/DDoS attacks while enhancing the stability and availability of web server services.

Index Terms—Intrusion Detection System; Snort; DDoS; Web Server.

Abstrak—* Perkembangan penggunaan jaringan dan layanan web meningkatkan kebutuhan terhadap sistem keamanan yang mampu mendeteksi serta memitigasi aktivitas jaringan yang bersifat abnormal. Salah satu ancaman yang dapat mengganggu ketersediaan layanan adalah Distributed Denial of Service (DDoS), khususnya serangan berbasis UDP Flood yang dapat menyebabkan saturasi bandwidth. Penelitian ini bertujuan untuk menganalisis pola trafik abnormal pada web server serta mengimplementasikan Intrusion Detection System (IDS) berbasis Snort dan mekanisme mitigasi menggunakan Firewall RAW pada MikroTik Cloud Core Router (CCR). Penelitian menggunakan pendekatan kuantitatif dengan analisis trafik dan log jaringan untuk mengidentifikasi karakteristik serangan, meliputi protokol, alamat sumber dan tujuan, port layanan, ukuran paket, serta pola pengiriman paket. Hasil analisis menunjukkan adanya trafik UDP berukuran relatif kecil yang dikirim secara berulang dari beberapa alamat IP sumber menuju port 53 (DNS) dengan frekuensi tinggi, sehingga terindikasi sebagai aktivitas UDP Flood/DDoS. Sebelum mitigasi, trafik inbound mencapai rata-rata 207,94 Mbps dengan trafik maksimum 306,20 Mbps , sementara kapasitas bandwidth yang tersedia hanya 100 Mbps . Kondisi tersebut menyebabkan bandwidth mengalami saturasi dan berdampak terhadap kualitas layanan web server. Mitigasi dilakukan dengan menerapkan rule Firewall RAW pada MikroTik CCR untuk membuang paket UDP menuju port 53 pada tahap *prerouting*. Setelah penerapan mitigasi, trafik inbound turun menjadi rata-rata 43,21 Mbps dengan trafik maksimum 60,72 Mbps . Dengan demikian, trafik maksimum mengalami penurunan sekitar 80,17% dan kembali berada di bawah kapasitas bandwidth 100 Mbps. Hasil penelitian menunjukkan bahwa kombinasi Snort IDS sebagai mekanisme deteksi dan Firewall RAW MikroTik sebagai mekanisme mitigasi mampu mengurangi dampak serangan UDP Flood/DDoS serta meningkatkan stabilitas dan ketersediaan layanan web server.

Kata kunci — Intrusion Detection System,; Snort; DDoS, Web Server.

I. PENDAHULUAN

Perkembangan teknologi informasi di era digital telah mendorong peningkatan penggunaan server dan jaringan komputer dalam berbagai sektor, seperti bisnis, pemerintahan, dan Pendidikan[1].Namun, peningkatan tersebut juga diiringi dengan meningkatnya ancaman keamanan siber yang semakin kompleks dan beragam. Serangan seperti *brute force*, *Denial of Service* (DoS), dan port scanning menjadi ancaman nyata yang dapat mengganggu ketersediaan layanan serta membahayakan integritas dan kerahasiaan data [2]. Keamanan jaringan merupakan aspek krusial dalam menjaga stabilitas dan keandalan sistem informasi. Pendekatan keamanan tradisional seperti penggunaan *firewall* dinilai belum cukup untuk menghadapi serangan siber *modern*, karena hanya berfungsi sebagai penyaring lalu lintas berdasarkan aturan tertentu tanpa mampu mendeteksi pola serangan secara mendalam [3].Oleh karena itu, diperlukan mekanisme tambahan yang mampu melakukan deteksi aktivitas mencurigakan secara lebih proaktif. *Intrusion Detection System* (IDS) hadir sebagai solusi yang mampu memantau lalu lintas jaringan secara real-time dan mengidentifikasi adanya aktivitas abnormal atau potensi serangan [4]. IDS bekerja dengan menganalisis pola lalu lintas jaringan menggunakan metode *signature-based* maupun *anomaly-based detection* [5]. Salah satu *tools* IDS yang banyak digunakan adalah *Snort*, yang dikenal sebagai solusi *open-source* dengan kemampuan deteksi yang cukup baik dan fleksibel untuk berbagai kebutuhan jaringan [6].

Meskipun IDS memiliki keunggulan dalam mendeteksi serangan, implementasinya masih menghadapi beberapa kendala, seperti tingginya tingkat false positive dan false negative, serta kebutuhan konfigurasi yang tepat agar dapat bekerja secara optimal. Selain itu, tidak semua organisasi mampu mengimplementasikan IDS secara efektif karena keterbatasan sumber daya manusia dan infrastruktur.
Penelitian sebelumnya menunjukkan bahwa kombinasi IDS seperti Snort dengan mekanisme *firewall* seperti *iptables* mampu meningkatkan efektivitas dalam mendeteksi dan mencegah serangan jaringan [7]. Sistem ini tidak hanya mampu mendeteksi aktivitas mencurigakan, tetapi juga secara otomatis melakukan tindakan pencegahan terhadap serangan yang teridentifikasi. Namun, implementasi dan evaluasi performa IDS pada lingkungan *web server* masih perlu dikaji lebih lanjut, khususnya dalam mengukur tingkat akurasi deteksi terhadap berbagai jenis serangan [8].

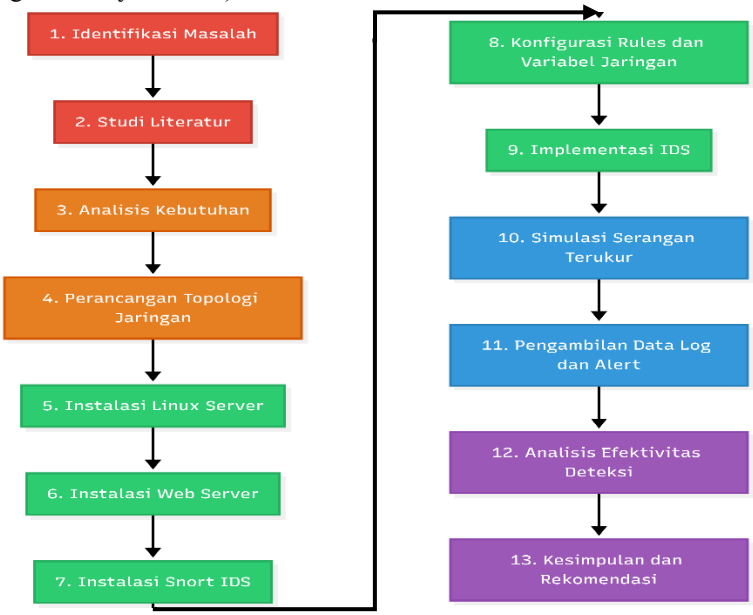
Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk melakukan analisis dan implementasi sistem keamanan jaringan berbasis *Intrusion Detection System* (IDS) menggunakan *Snort* yang dikombinasikan dengan *iptables* pada *web server* [9]. Penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan efektivitas sistem keamanan jaringan, khususnya dalam mendeteksi dan mencegah serangan siber secara lebih optimal, serta menjadi referensi bagi pengembangan sistem keamanan berbasis open-source di masa mendatang.

Keamanan jaringan merupakan sekumpulan kebijakan, prosedur, dan teknologi yang diterapkan untuk mencegah, mendeteksi, dan memitigasi akses yang tidak sah, penyalahgunaan, maupun modifikasi yang merusak pada sistem jaringan komputer [10]. Secara teoretis, implementasi keamanan informasi wajib mengacu pada model *Confidentiality, Integrity, and Availability* (CIA Triad) yang dijelaskan sebagai berikut [11]. *Web server* merupakan salah satu target utama serangan siber karena posisinya yang terekspos langsung ke jaringan publik (internet). Berdasarkan klasifikasi dari *Open Web Application Security Project* (OWASP), berikut adalah bentuk ancaman dan serangan yang paling sering terjadi pada *web server* [12], [13]. Setiap platform *web server* memiliki karakteristik arsitektur dan potensi kerentanan yang berbeda. Tiga platform *web server* terbesar yang mendominasi pasar global saat ini adalah Apache HTTP Server, Nginx, dan Internet Information Services (IIS) [14]. Statistik dari laporan keamanan tahunan menunjukkan bahwa lebih dari 70% serangan siber di tingkat aplikasi menargetkan kerentanan miskonfigurasi dan ketidakpatuhan terhadap *patching* rutin [15]. Hal ini menegaskan perlunya sistem pemantauan aktif yang mampu mendeteksi anomali lalu lintas sebelum mencapai lapisan aplikasi web terdalam. *Intrusion Detection System* (IDS) didefinisikan sebagai perangkat lunak atau perangkat keras yang berfungsi memantau lalu lintas jaringan atau aktivitas sistem komputer untuk mendeteksi tanda-tanda aktivitas mencurigakan, pelanggaran kebijakan keamanan, maupun upaya akses ilegal [16].

Perkembangan IDS dimulai dari laporan perintis James P. Anderson pada tahun 1980 yang memperkenalkan konsep audit log komputer untuk mendeteksi ancaman internal dan eksternal. Selanjutnya, Dorothy E. Denning pada tahun 1987 memformulasikan model deteksi intrusi berbasis profil anomali statistikal, yang meletakkan dasar bagi pengembangan arsitektur IDS modern seperti yang dikenal saat ini [17]. Implementasi IDS menawarkan kelebihan signifikan berupa visibilitas tinggi terhadap lalu lintas jaringan, kemampuan forensik digital melalui pencatatan log historis yang mendalam, serta pemenuhan standar regulasi keamanan [18]. Namun, IDS memiliki keterbatasan inheren, antara lain ketidakmampuannya menganalisis lalu lintas data yang terenkripsi secara mendalam tanpa adanya proses *decryption proxy*, beban komputasi yang tinggi pada lalu lintas jaringan berkecepatan tinggi, serta risiko tingginya alarm palsu yang dapat membebani administrator jaringan (*alert fatigue*) [19].

II. METODE

Penelitian ini menggunakan pendekatan kuantitatif dengan jenis penelitian eksperimen laboratorium (*laboratory experiment*). Pendekatan kuantitatif dipilih karena penelitian ini berfokus pada pengumpulan, pengukuran, dan analisis data numerik yang bersifat objektif, seperti waktu deteksi (*detection time*), jumlah paket data (*packet count*), nilai *throughput*, tingkat akurasi deteksi (*detection rate*), serta persentase *false positive* dan *false negative* [10]. Sebagai penelitian eksperimen, metode ini melibatkan manipulasi variabel bebas untuk melihat dampaknya terhadap variabel terikat dalam suatu lingkungan yang terkendali. Dalam konteks ini, manipulasi dilakukan dengan menerapkan konfigurasi *Intrusion Detection System* (IDS) berbasis Snort dengan variasi aturan (*rules*) tertentu, lalu memberikan paparan berupa simulasi serangan siber yang terstruktur pada lingkungan *web server*. eksperimental, seperti studi kasus pasif atau survei, tidak mampu menyediakan data performa sistem secara dinamis saat berada di bawah tekanan serangan (*under attack*). Menurut Creswell [11], metode eksperimen sangat tepat digunakan ketika peneliti ingin menguji hubungan sebab-akibat antara perlakuan yang diberikan (konfigurasi Snort) dengan luaran yang dihasilkan (stabilitas *web server* dan akurasi deteksi). Keterkaitan antara metode eksperimen dengan implementasi IDS Snort terletak pada tahapan pengujian hipotesis dan validasi sistem. Implementasi Snort bertindak sebagai instrumen pertahanan yang kinerjanya akan diuji. Melalui rancangan eksperimen, sistem Snort akan dihadapkan pada skenario serangan nyata yang dikondisikan, seperti *SQL Injection*, *Cross-Site Scripting* (XSS), *Brute Force*, *Port Scanning*, dan *Denial of Service* (DoS). Aktivitas penelitian ini dilaksanakan secara sistematis berdasarkan siklus pengembangan dan pengujian sistem keamanan jaringan. Rangkaian prosedur penelitian digambarkan melalui diagram alir (*flowchart*) berikut:



Gambar 1. Tahapan Penelitian

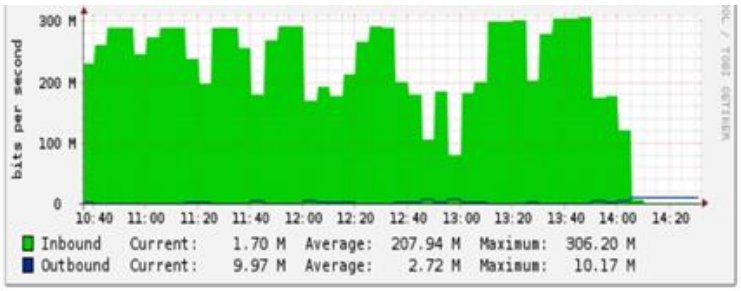
III. HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan data monitoring penggunaan bandwidth pada jaringan Metro Ethernet Telkom yang digunakan oleh instansi pemerintah daerah. Monitoring dilakukan menggunakan aplikasi TelkomCare MRTG Graph yang menampilkan kondisi trafik jaringan secara real-time maupun historis. Parameter utama yang diamati meliputi trafik Inbound dan Outbound dalam satuan bit per detik (bps).

Monitoring bertujuan untuk mengetahui pola penggunaan bandwidth, tingkat utilisasi jaringan, serta mendeteksi adanya lonjakan trafik yang berpotensi memengaruhi kualitas layanan jaringan. Data hasil monitoring divisualisasikan dalam bentuk grafik sehingga memudahkan administrator jaringan dalam melakukan evaluasi terhadap performa koneksi Metro Ethernet.

A. Hasil Monitoring Trafik Jaringan Internet Dedicated Instansi XYZ

Monitoring Trafik Harian



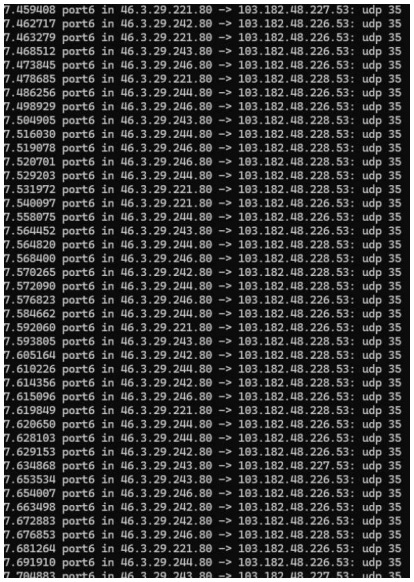
Gambar 2. Adanya Serangan Ddos Dari Network Pelanggan

Berdasarkan hasil monitoring trafik jaringan menggunakan perangkat monitoring jaringan, terlihat adanya peningkatan trafik yang sangat signifikan pada sisi inbound menuju jaringan pelanggan. Grafik menunjukkan bahwa trafik masuk (inbound) secara konsisten berada pada kisaran 180–306 Mbps, dengan nilai rata-rata sebesar 207,94 Mbps dan puncak trafik mencapai 306,20 Mbps. Sementara itu, trafik keluar (outbound) relatif rendah dengan rata-rata hanya 2,72 Mbps dan nilai maksimum 10,17 Mbps.

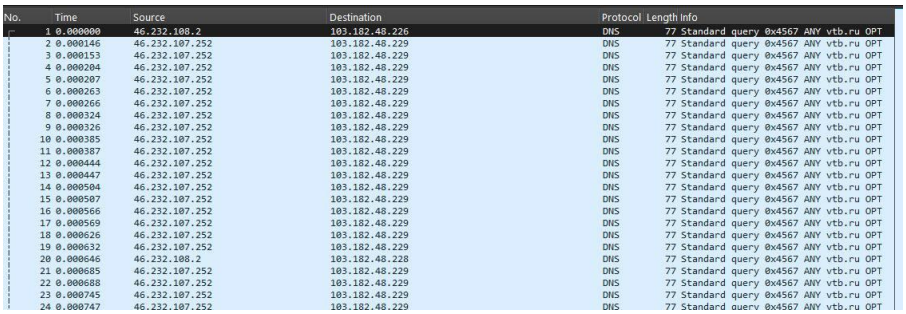
Kondisi tersebut mengindikasikan adanya pola trafik yang tidak normal karena bandwidth layanan yang dimiliki pelanggan hanya sebesar 100 Mbps. Dengan demikian, trafik inbound yang mencapai lebih dari 300 Mbps berarti mencapai sekitar 306% dari kapasitas bandwidth yang tersedia. Besarnya trafik yang melebihi kapasitas link menyebabkan bandwidth pelanggan mengalami saturasi (congestion), sehingga layanan jaringan menjadi tidak optimal bahkan berpotensi mengalami gangguan atau tidak dapat diakses.

Ketidakseimbangan yang sangat mencolok antara trafik inbound dan outbound merupakan salah satu karakteristik umum dari serangan jaringan, khususnya Distributed Denial of Service (DDoS) atau flooding attack. Pada kondisi normal, trafik inbound dan outbound cenderung memiliki pola yang lebih proporsional sesuai aktivitas pengguna. Namun, pada grafik terlihat bahwa peningkatan trafik hanya terjadi pada arah inbound tanpa diikuti peningkatan trafik outbound yang signifikan. Hal ini menunjukkan bahwa sebagian besar paket yang diterima bukan berasal dari aktivitas komunikasi yang sah, melainkan merupakan paket-paket yang dikirim secara masif untuk memenuhi kapasitas bandwidth target.

Apabila dibandingkan dengan kapasitas bandwidth pelanggan sebesar 100 Mbps, maka trafik rata-rata sebesar 207,94 Mbps telah melebihi kapasitas sebesar 107,94 Mbps, sedangkan trafik maksimum sebesar 306,20 Mbps melebihi kapasitas sebesar 206,20 Mbps. Kondisi tersebut menyebabkan perangkat jaringan harus memproses paket dalam jumlah yang jauh lebih besar daripada kemampuan link yang tersedia. Akibatnya, terjadi peningkatan packet loss, latency, serta penurunan kualitas layanan (Quality of Service/QoS) yang dirasakan oleh pengguna.



Gambar 3. Gambar Pola Serangan Di Web Server



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	46.232.108.2	103.182.48.226	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
2	0.000146	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
3	0.000153	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
4	0.000204	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
5	0.000207	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
6	0.000263	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
7	0.000266	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
8	0.000324	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
9	0.000326	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
10	0.000385	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
11	0.000387	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
12	0.000444	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
13	0.000447	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
14	0.000504	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
15	0.000507	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
16	0.000566	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
17	0.000569	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
18	0.000626	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
19	0.000632	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
20	0.000646	46.232.108.2	103.182.48.228	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
21	0.000685	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
22	0.000688	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
23	0.000745	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT
24	0.000747	46.232.107.252	103.182.48.229	DNS	77	Standard query 0x4567 ANY vtb.ru OPT

Gambar 3. Gambar Pola Serangan Di Router Firewall Pelanggan

Berdasarkan hasil monitoring trafik jaringan pada web server, diperoleh log paket yang menunjukkan adanya lalu lintas jaringan dengan karakteristik yang tidak normal. Gambar menunjukkan sejumlah besar paket UDP yang masuk melalui interface port6 menuju alamat IP web server 103.182.48.226, 103.182.48.227, dan 103.182.48.228 pada port 53 (DNS). Paket-paket tersebut berasal dari beberapa alamat IP sumber, seperti 46.3.29.221, 46.3.29.242, 46.3.29.243, 46.3.29.244, dan 46.3.29.246, yang dikirim secara berulang dalam interval waktu yang sangat singkat.

Karakteristik utama yang terlihat dari log tersebut adalah tingginya frekuensi pengiriman paket UDP dengan ukuran paket relatif kecil, yaitu sekitar 35 byte, namun dilakukan secara terus-menerus. Meskipun ukuran setiap paket kecil, akumulasi jumlah paket yang sangat besar mampu menghasilkan trafik yang tinggi sehingga membebani bandwidth dan sumber daya server.

Pola komunikasi yang ditampilkan memperlihatkan bahwa beberapa alamat IP sumber secara bergantian mengirimkan paket ke beberapa alamat IP tujuan pada port yang sama, yaitu UDP port 53. Aktivitas tersebut menunjukkan adanya pola UDP Flood Attack, yaitu serangan yang bertujuan memenuhi kapasitas jaringan dan sumber daya server dengan mengirimkan paket UDP dalam jumlah besar tanpa memperhatikan apakah layanan yang dituju benar-benar memerlukan komunikasi tersebut.

Selain itu, penggunaan port 53 mengindikasikan bahwa penyerang berusaha mengeksploitasi layanan Domain Name System (DNS). Dalam praktiknya, pola seperti ini sering dijumpai pada serangan DNS Flood maupun DNS Amplification, di mana lalu lintas DNS dimanfaatkan untuk menghasilkan volume trafik yang jauh lebih besar daripada permintaan normal. Walaupun dari log yang ditampilkan belum dapat dipastikan apakah merupakan DNS Amplification atau UDP Flood murni, pola paket yang terus-menerus menuju port DNS menunjukkan adanya aktivitas yang bersifat mencurigakan dan berpotensi sebagai serangan Denial of Service (DoS/DDoS).

Dari sisi distribusi sumber serangan, terlihat bahwa trafik berasal dari beberapa alamat IP yang berbeda namun memiliki pola pengiriman yang identik. Hal ini mengindikasikan bahwa serangan tidak dilakukan oleh satu host saja, melainkan berasal dari beberapa sumber secara bersamaan. Karakteristik tersebut merupakan salah satu indikasi Distributed Denial of Service (DDoS), di mana sejumlah perangkat atau host mengirimkan paket secara simultan untuk meningkatkan volume trafik menuju target.

Apabila dikaitkan dengan hasil monitoring bandwidth sebelumnya, di mana trafik inbound mencapai lebih dari 300 Mbps pada bandwidth pelanggan yang hanya 100 Mbps, maka log paket ini memperkuat dugaan bahwa lonjakan trafik tersebut disebabkan oleh serangan UDP Flood terhadap layanan DNS pada web server. Serangan tersebut mengakibatkan kapasitas bandwidth menjadi penuh (bandwidth saturation), sehingga permintaan dari pengguna yang sah sulit diproses dan kualitas layanan web server mengalami penurunan.

Implementasi Intrusion Detection System (IDS) berbasis Snort pada penelitian ini berperan dalam mendeteksi pola serangan tersebut melalui pencocokan signature terhadap paket UDP yang memiliki karakteristik mencurigakan. Dengan adanya IDS, administrator jaringan dapat memperoleh notifikasi secara real-time mengenai aktivitas abnormal sehingga tindakan mitigasi, seperti pemblokiran alamat IP sumber, penerapan rate limiting, atau aktivasi mekanisme anti-DDoS pada firewall, dapat dilakukan sebelum serangan menyebabkan gangguan layanan yang lebih luas. Hasil Analisis Pola Serangan Berdasarkan log yang diamati, karakteristik serangan dapat dirangkum sebagai berikut.

Tabel I . Hasil Analisis

Parameter	: Hasil Analisis
Jenis Protokol	: UDP
Target layanan	: DNS (Port 53)
Target IP	: 103.182.48.226, 103.182.48.227, 103.182.48.228
IP sumber	: Beberapa IP (46.3.29.221, 46.3.29.242, 46.3.29.243, 46.3.29.244, 46.3.29.246)
Ukuran paket	: ±35 byte

Pola serangan Pengiriman paket secara berulang dengan interval sangat singkat

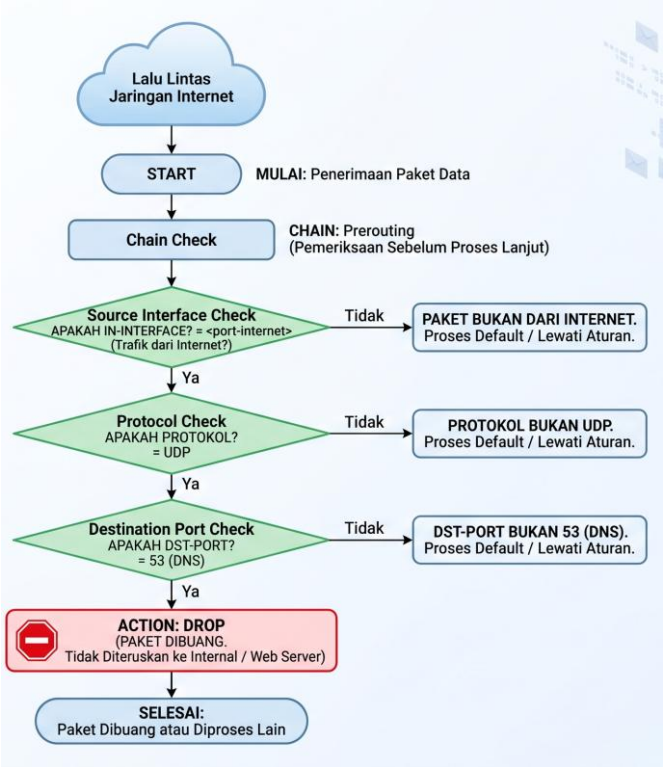
Indikasi serangan UDP Flood / DNS Flood (berpotensi DDoS)

Dampak Peningkatan trafik inbound, saturasi bandwidth, penurunan performa web server.

3.2 Mitigasi dan Solusi Serangan DDoS

Berdasarkan hasil analisis trafik jaringan, diketahui bahwa web server mengalami serangan Distributed Denial of Service (DDoS) dengan karakteristik UDP Flood yang menargetkan layanan DNS (UDP port 53). Serangan tersebut mengakibatkan trafik inbound meningkat hingga melebihi kapasitas bandwidth pelanggan sebesar 100 Mbps, sehingga menyebabkan terjadinya bandwidth saturation, peningkatan latency, packet loss, dan penurunan kinerja layanan web server.

Sebagai langkah mitigasi, dilakukan konfigurasi firewall pada Mikrotik Cloud Core Router (CCR) menggunakan fitur Firewall RAW. Pemilihan firewall RAW didasarkan pada kemampuannya untuk memproses paket pada tahap prerouting, yaitu sebelum paket memasuki proses connection tracking. Dengan mekanisme tersebut, paket yang teridentifikasi sebagai bagian dari serangan dapat dibuang (drop) lebih awal sehingga mengurangi beban CPU router dan meningkatkan efisiensi proses penyaringan trafik.



Gambar 4. Flowchart Penyaringan Serangan DNS

Konfigurasi firewall yang diterapkan adalah sebagai berikut:

```
/ip firewall raw
add chain =prerouting \
   protocol =udp \
   dst-port =53 \
   in-interface =<port-internet> \
   action =drop \
   comment="Drop UDP Flood ke DNS"
```

Konfigurasi tersebut memiliki fungsi sebagai berikut:

- chain=prerouting menunjukkan bahwa proses pemeriksaan dilakukan sebelum paket diproses lebih lanjut oleh router.
- protocol=udp membatasi aturan hanya pada paket dengan protokol UDP.
- dst-port=53 memfokuskan penyaringan pada paket yang ditujukan ke layanan DNS yang menjadi target serangan.
- in-interface=<port-internet> memastikan hanya trafik yang berasal dari jaringan internet yang diperiksa.

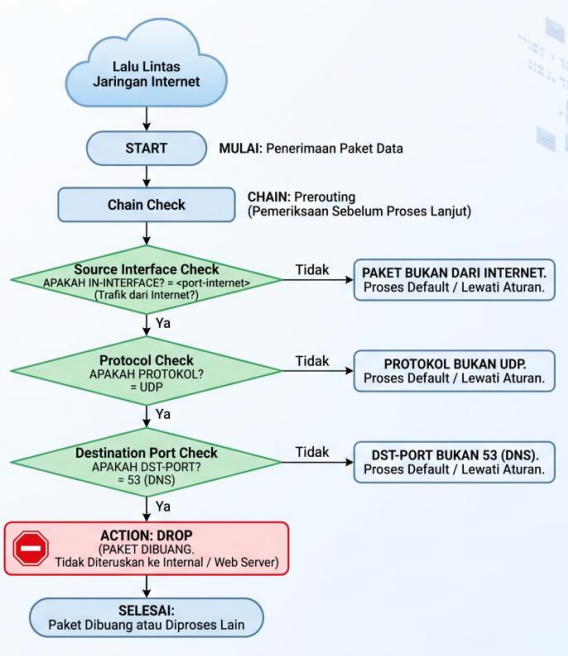
action=drop memerintahkan router untuk langsung membuang paket yang memenuhi kriteria tanpa meneruskannya ke jaringan internal maupun web server.

Penerapan rule tersebut bertujuan menghentikan aliran paket UDP yang menuju port DNS sebelum mencapai web server. Dengan demikian, trafik hasil serangan tidak lagi menghabiskan kapasitas bandwidth maupun sumber daya server. Selain itu, karena paket dibuang pada tahap RAW, router tidak perlu melakukan proses connection tracking terhadap paket-paket tersebut, sehingga penggunaan CPU dan memori router tetap terjaga meskipun terjadi serangan dengan volume trafik yang tinggi.

Setelah rule firewall diimplementasikan, trafik abnormal menuju port 53 dapat ditekan secara signifikan sehingga penggunaan bandwidth kembali mendekati kondisi normal. Akibatnya, layanan web server dapat kembali diakses oleh pengguna yang sah tanpa mengalami gangguan yang disebabkan oleh serangan UDP Flood.

Meskipun demikian, penerapan rule drop terhadap seluruh paket UDP pada port 53 perlu disesuaikan dengan arsitektur jaringan yang digunakan. Apabila server memang menyediakan layanan DNS publik, maka rule tersebut berpotensi memblokir permintaan DNS yang sah. Oleh karena itu, konfigurasi ini lebih tepat diterapkan pada kondisi di mana web server tidak menjalankan layanan DNS publik, atau digunakan sebagai mitigasi darurat (emergency mitigation) saat serangan berlangsung. Untuk implementasi jangka panjang, mitigasi dapat dikombinasikan dengan mekanisme Intrusion Detection System (IDS) berbasis Snort, firewall filtering yang lebih spesifik, rate limiting, address list, atau layanan anti-DDoS dari penyedia upstream agar keamanan jaringan tetap terjaga tanpa mengganggu layanan yang sah.

Berdasarkan hasil implementasi tersebut, penggunaan Firewall RAW pada Mikrotik CCR terbukti efektif sebagai mekanisme mitigasi awal terhadap serangan UDP Flood/DDoS karena mampu menghentikan paket berbahaya sejak tahap prerouting, mengurangi beban perangkat jaringan, dan menjaga ketersediaan layanan web server selama serangan berlangsung.



Gambar 4. Flowchart Penyaringan Serangan DNS

Setelah dilakukan implementasi mitigasi menggunakan Firewall RAW pada Mikrotik Cloud Core Router (CCR) dengan melakukan pemblokiran paket UDP menuju port 53, dilakukan kembali proses monitoring untuk mengevaluasi efektivitas mekanisme mitigasi terhadap serangan DDoS.

Berdasarkan hasil monitoring yang ditunjukkan pada Gambar 4.4, terlihat bahwa kondisi trafik jaringan telah mengalami perubahan yang signifikan dibandingkan sebelum mitigasi diterapkan. Trafik inbound berada pada nilai rata-rata 43,21 Mbps, dengan trafik maksimum mencapai 60,72 Mbps, sedangkan trafik outbound memiliki rata-rata 5,04 Mbps dengan nilai maksimum 34,05 Mbps.

Nilai trafik inbound tersebut masih berada di bawah kapasitas bandwidth pelanggan sebesar 100 Mbps, sehingga tidak lagi menyebabkan kondisi overload seperti yang terjadi sebelum mitigasi. Sebelumnya, trafik inbound tercatat mencapai lebih dari 306 Mbps, atau sekitar tiga kali lipat dari kapasitas bandwidth yang tersedia. Setelah penerapan firewall, puncak trafik berhasil ditekan menjadi 60,72 Mbps, yang berarti terjadi penurunan trafik puncak sekitar 80% dibandingkan kondisi sebelum mitigasi. Penurunan tersebut menunjukkan bahwa sebagian besar paket hasil serangan berhasil difilter sebelum memasuki jaringan pelanggan.

Selain penurunan volume trafik, grafik juga memperlihatkan pola lalu lintas jaringan yang lebih stabil. Fluktuasi trafik inbound masih terjadi sebagai konsekuensi aktivitas pengguna dan layanan jaringan yang normal, namun tidak ditemukan lagi lonjakan ekstrem yang menyebabkan saturasi bandwidth. Trafik

outbound juga menunjukkan pola yang lebih wajar, di mana peningkatan sesaat merupakan respons terhadap aktivitas komunikasi yang sah dari server kepada pengguna.

Keberhasilan mitigasi ini dipengaruhi oleh penerapan rule firewall pada fitur RAW Mikrotik CCR, yaitu:

```
/ip firewall raw
add chain=prerouting protocol=udp dst-port=53 \
in-interface=<port-internet> action=drop
```

Rule tersebut bekerja dengan membuang seluruh paket UDP yang ditujukan ke port 53 sejak tahap prerouting, sehingga paket hasil serangan tidak diproses lebih lanjut oleh mekanisme connection tracking maupun diteruskan ke web server. Pendekatan ini mampu mengurangi beban pemrosesan pada router sekaligus mencegah konsumsi bandwidth oleh trafik yang tidak sah.

Dari hasil monitoring dapat disimpulkan bahwa implementasi mitigasi memberikan dampak positif terhadap performa jaringan. Bandwidth pelanggan yang sebelumnya mengalami saturasi kini dapat dimanfaatkan secara optimal oleh trafik yang sah. Ketersediaan layanan web server juga meningkat karena sumber daya jaringan tidak lagi dipenuhi oleh paket-paket hasil serangan DDoS.

Tabel II. Perbandingan Kondisi Sebelum dan Sesudah Mitigasi

Parameter	Sebelum Mitigasi	Sesudah Mitigasi
Kapasitas Bandwidth	100 Mbps	100 Mbps
Trafik Inbound Rata-rata	207,94 Mbps	43,21 Mbps
Trafik Inbound Maksimum	306,20 Mbps	60,72 Mbps
Kondisi Bandwidth	Overload (melebihi kapasitas)	Normal (di bawah kapasitas)
Dampak terhadap Web Server	Gangguan layanan, latency tinggi, packet loss	Layanan stabil dan dapat diakses normal
Status Mitigasi	Belum diterapkan	Firewall RAW Mikrotik CCR aktif

Berdasarkan perbandingan tersebut, implementasi rule Firewall RAW pada Mikrotik CCR terbukti efektif dalam mengurangi dampak serangan UDP Flood/DDoS. Trafik yang sebelumnya melebihi kapasitas bandwidth berhasil ditekan hingga berada pada kisaran 43–61 Mbps, atau sekitar 43–61% dari kapasitas link 100 Mbps. Dengan demikian, bandwidth kembali berada dalam kondisi aman, kualitas layanan jaringan meningkat, dan web server mampu melayani permintaan pengguna secara normal tanpa mengalami gangguan akibat serangan DDoS. Hasil ini menunjukkan bahwa mekanisme filtering pada tahap prerouting merupakan solusi yang efisien untuk meminimalkan dampak serangan berbasis UDP terhadap infrastruktur jaringan pelanggan.

B. Hasil Penelitian

Berdasarkan hasil penelitian mengenai Analisis dan Implementasi Sistem Keamanan Jaringan Menggunakan *Intrusion Detection System* (IDS) Berbasis Snort pada Web Server, dapat disimpulkan beberapa hal sebagai berikut.

1. Serangan *Distributed Denial of Service* (DDoS) berhasil diidentifikasi melalui analisis trafik jaringan dan log paket menggunakan Intrusion Detection System (IDS) berbasis Snort. Hasil monitoring menunjukkan adanya pola trafik yang tidak normal berupa peningkatan trafik inbound secara signifikan dengan karakteristik paket UDP Flood yang menargetkan port 53 (DNS). Log serangan memperlihatkan banyak alamat IP sumber yang secara bersamaan mengirimkan paket UDP berukuran kecil dengan frekuensi tinggi menuju web server, sehingga mengindikasikan terjadinya serangan DDoS.
2. Serangan DDoS menyebabkan terjadinya saturasi bandwidth pada jaringan pelanggan. Sebelum dilakukan mitigasi, trafik inbound mencapai rata-rata 207,94 Mbps dengan puncak trafik sebesar 306,20 Mbps, sedangkan kapasitas bandwidth pelanggan hanya 100 Mbps. Kondisi tersebut menyebabkan bandwidth mengalami overload, meningkatkan latency, packet loss, serta menurunkan kualitas layanan web server sehingga akses dari pengguna menjadi terganggu.
3. Implementasi mitigasi menggunakan Firewall RAW pada Mikrotik *Cloud Core Router* (CCR) terbukti efektif dalam menekan dampak serangan DDoS. Dengan menerapkan rule firewall yang

memblokir paket UDP menuju port 53 pada tahap prerouting, paket-paket yang teridentifikasi sebagai bagian dari serangan dapat dibuang sebelum diproses lebih lanjut oleh router. Pendekatan ini mampu mengurangi beban pemrosesan perangkat jaringan sekaligus mencegah trafik serangan menghabiskan kapasitas bandwidth.

4. Hasil monitoring setelah implementasi mitigasi menunjukkan peningkatan performa jaringan yang signifikan. Trafik inbound turun menjadi rata-rata 43,21 Mbps dengan trafik maksimum 60,72 Mbps, sehingga seluruh trafik berada di bawah kapasitas bandwidth 100 Mbps. Kondisi tersebut menunjukkan bahwa jaringan kembali beroperasi secara normal, layanan web server menjadi lebih stabil, dan gangguan akibat serangan DDoS dapat diminimalkan.
5. Integrasi IDS berbasis Snort dengan mekanisme filtering pada firewall Mikrotik memberikan pendekatan keamanan jaringan yang efektif. IDS berfungsi mendeteksi aktivitas serangan secara real-time melalui analisis signature, sedangkan firewall bertindak sebagai mekanisme mitigasi dengan memblokir trafik berbahaya. Kombinasi kedua mekanisme tersebut mampu meningkatkan aspek *Confidentiality, Integrity, dan Availability* (CIA) pada layanan web server, khususnya dalam menjaga ketersediaan (*availability*) layanan terhadap ancaman serangan DDoS.

Berdasarkan hasil penelitian yang telah dilakukan, beberapa saran yang dapat diberikan untuk pengembangan penelitian maupun implementasi di lingkungan operasional adalah sebagai berikut.

1. Implementasi IDS sebaiknya dikombinasikan dengan *Intrusion Prevention System* (IPS) sehingga proses deteksi tidak hanya menghasilkan notifikasi, tetapi juga mampu melakukan tindakan pencegahan secara otomatis terhadap trafik yang terindikasi sebagai serangan.
2. Konfigurasi firewall perlu dikembangkan menjadi lebih adaptif dengan menerapkan mekanisme seperti rate limiting, connection limiting, address list dinamis, atau blacklist otomatis berdasarkan hasil deteksi IDS. Pendekatan tersebut memungkinkan mitigasi dilakukan secara lebih selektif tanpa mengganggu trafik pengguna yang sah.
3. Penelitian selanjutnya dapat mengembangkan integrasi otomatis antara Snort dan Mikrotik melalui mekanisme scripting atau API sehingga setiap alert yang dihasilkan IDS dapat langsung memicu penambahan rule firewall secara real-time. Integrasi ini akan mempercepat proses respons terhadap serangan dan mengurangi ketergantungan pada intervensi administrator jaringan.
4. Pengujian pada penelitian berikutnya disarankan menggunakan berbagai jenis serangan jaringan, seperti TCP SYN Flood, ICMP Flood, HTTP Flood, Slowloris, brute force, maupun eksploitasi aplikasi web. Dengan demikian, kemampuan IDS dan mekanisme mitigasi dapat dievaluasi secara lebih komprehensif terhadap berbagai bentuk ancaman keamanan jaringan.
5. Penelitian selanjutnya juga dapat membandingkan performa beberapa solusi IDS maupun *Next Generation Firewall* (NGFW), seperti Suricata, Zeek, atau sistem keamanan berbasis machine learning, untuk memperoleh solusi yang memiliki tingkat akurasi deteksi, kecepatan respons, dan efisiensi sumber daya yang lebih baik.
6. Monitoring jaringan secara berkelanjutan perlu diterapkan sebagai bagian dari kebijakan keamanan jaringan organisasi. Pemantauan trafik secara periodik, pembaruan signature IDS, evaluasi konfigurasi firewall, serta penerapan manajemen log yang terpusat akan meningkatkan kemampuan organisasi dalam mendeteksi, menganalisis, dan merespons ancaman siber secara lebih cepat dan efektif.

IV. KESIMPULAN

Hasil penelitian ini menunjukkan bahwa penerapan *Intrusion Detection System* (IDS) berbasis Snort yang dipadukan dengan Firewall RAW pada *Mikrotik Cloud Core Router* (CCR) merupakan solusi yang efektif dalam mendeteksi sekaligus memitigasi serangan *Distributed Denial of Service* (DDoS) pada web server. Implementasi tersebut tidak hanya mampu menekan volume trafik berbahaya hingga berada di bawah kapasitas bandwidth yang tersedia, tetapi juga meningkatkan ketersediaan layanan dan stabilitas jaringan. Dengan demikian, pendekatan yang diusulkan dapat menjadi salah satu referensi dalam

pengelolaan keamanan jaringan pada instansi pemerintah, institusi pendidikan, maupun organisasi yang mengandalkan layanan web sebagai infrastruktur utama.

V. DAFTAR PUSTAKA

[1] Nasution, M., & Munandar, M. H. (2025). Implementasi Sistem Keamanan Jaringan Menggunakan Firewall dan IDS pada Infrastruktur Jaringan Skala Kecil-Menengah JURNAL MEDIA INFORMATIKA [JUMIN]. 6(6), 2732–2741.

[2] Anggraini, N. D., Amrulloh, M. F., & Havy, A. Z. F. (2025). Analisis Pengembangan Intrusion Detection System (IDS) Menggunakan Random Forest Untuk Meningkatkan Keamanan Jaringan. *Al-Faqih Ilmu Sosial Dan Teknik*, *1*. https://journal.salahuddinal-ayyubi.com/index.php/AFJISH/article/view/534

[3] Ardiansyah, F., Zuhra, N. N., Zahra, L., Alfarisyi, R., Nisa, H., & Astiyanto, R. A. (2026). Implementasi Keamanan Jaringan Menggunakan Firewall dan Intrusion Detection System (IDS) pada Infrastruktur Jaringan Skala Kecil – Menengah. 2(1), 124–126.

[4] S, D. S., Kautsar, A., & Setyawan, A. (2025). SisInfo Intrusion Detection System Menggunakan Snort dan Telegram Sebagai Media Notifikasi SisInfo. 7(1), 40–49.

[5] Davies, T., Eiza, M. H., Shone, N., & Lyon, R. (2025). A Collaborative Intrusion Detection System Using Snort IDS Nodes.

[6] Ishaq, K., & Javed, H. A. (2023). Implementing Snort Intrusion Prevention System (IPS) for Network Forensic Analysis.

[7] Bagus, I. N., Wirianda, A., Huwae, R. B., & Jatmika, A. H. (2025). Pengujian Efektivitas Intrusion Detection Systems (IDS) Snort , Suricata , dan Zeek terhadap Serangan SYN Flood Testing the Effectiveness of Intrusion Detection Systems (IDS) Snort , Suricata , and Zeek against SYN Flood Attacks. 7(2), 95–108. https://doi.org/10.30812/bite.v7i2.5226

[8] Ilham, K. F., Alwi, E. I., & Fattah, F. (2023). Penerapan dan Analisis Network Security Snort Menggunakan Intrusion Detection System pada Serangan UDP Flood. 8(1), 94–100.

[9] M, G., F, Alfonsi, M, P., & A, G. (2023). A high throughput Intrusion Detection System (IDS) to enhance the security of data transmission among research centers. *IOP Publishing for Sissa Medialab*.

[10] Agustino, Leo, (2020, Dasar-dasar kebijakan publik Edisi Revisi Ke-2. Bandung:CV. Alfabeta.

[11] Ambarwati Adrian, dan Herdiyeni, 2020, A alisis Pengaruh Data Scaling Terhadap Performa Algoritme Machine Learning untuk Identifikasi Tanaman. Jurnal RESTI, 4(1) p. 117-122

[12] Andre Pardamean Lumban Gaol (2025), Penerapan Sistem Keamanan Jaringan menggunakan Intrusion Prevention System dengan Machine Learning, Sistemasi: Jurnal Sistem Informasi Volume 14, Nomor 6, 2025: 2615-2629 ISSN:2302-8149 e-ISSN:2540-9719

[13] Ayu Pelita Br (2025), Analisis Keamanan Jaringan Menggunakan *Intrusion Detection System* Pada STMIK Pelita Nusantara. Jurnal Data Science Penusa, vol 2, number 2

[14] G. W. Sasmito. 2017. Penerapan Metode Waterfall Pada Desain Sistem Informasi Geografis Industri Kabupaten Tegal, Vol. 2, No. 1

[15] Kuni Inayah (2024), Analisis Kinerja *Intrusion Detection System* Berbasis *Algoritma Random Forest* Menggunakan DataSet *Unbalanced Honeynet BSSN*. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)
Vol. 4, No. 11, Agustus 2024, hlm. 867-876 p-ISSN: 2355-7699

[16] Lumban Gaol, Andre Pardamean**.** (2025). *Penerapan Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System Dengan Machine Learning*. Eprints Politeknik Negeri Bengkalis

[17] Purwanto dan Sulistyastuti (2019, *Implementasi* Kebijakan. Publik: Konsep dan Aplikasinya di Indonesia. Yogyakarta: Gava Media

[18] Wibawa, Samudra, dkk. 2019. Evaluasi Kebijakan Publik. Jakarta: Rajawali Press

[19] Wu, 2009, *Hybrid Intrusion Detection System Using Machine Learning Techniques*.