Volume 6 No. 2 (July - December 2026), pp. 358-375 | ISSN 2962-2360 (online) | ISSN 2962-3669 (print)
Arcitech: Journal of Computer Science and Artificial Intelligence
https://journal.iaincurup.ac.id/index.php/arcitech/article/view/17833 | DOI : https://dx.doi.org/10.29240/arcitech.v6i2.17833

Evaluasi Layering Firewall RAW-Filter untuk Mitigasi Trafik Berindikasi DDoS pada MikroTik RouterOS v6

Arif Rahmadi Wibowo[1], Desi Ramayanti[2]
[1,2]Program Studi Teknik Informatika, Universitas Dian Nusantara, Jakarta, Indonesia
Email : 411221163@mahasiswa.undira.ac.id, desi.ramayanti@undira.ac.id

Article Information

Article history

Received 25 July 2026
Revised 20 August 2026
Accepted 14 September 2026
Available 22 October 2026

Keywords

Network Security
DDoS Mitigation
MikroTik RouterOS
RAW Firewall
Stateful Filtering

Corresponding Author:

Desi Ramayanti,
Universitas Dian Nusantara,
Email :
desi.ramayanti@undira.ac.id

Abstract

This study evaluates a layered MikroTik RouterOS v6 firewall configuration that combines the RAW and Filter tables to mitigate traffic patterns indicative of Distributed Denial of Service (DDoS) activity on a production edge router. Five sequential scenarios (S0-S4) were observed: normal baseline, unprotected high-load traffic, Filter only, RAW only, and RAW-Filter. Performance was described using CPU utilization, TCP SYN, UDP, and ICMP packet counters, and average latency. Relative to the unprotected scenario (S1), RAW-Filter (S4) reduced peak CPU utilization from 55% to 25% (54%), total SYN packets from 2,952 to 2,068 (30%), and total UDP packets from 484,054 to 55,746 (88%); total ICMP packets increased from 915 to 1,032 (12%), while average latency remained 24 ms. RAW only (S3), however, produced the lowest observed CPU load (7% average; 11% peak), indicating a trade-off between early dropping and the additional stateful policy enforcement provided by the layered configuration. Because the scenarios were executed sequentially on one production network and the manuscript does not report repeated randomized trials or inferential statistics, the findings should be interpreted as descriptive operational evidence rather than proof of statistically significant causal superiority. The study provides practical evidence for baseline-driven firewall tuning while identifying the need for controlled replication, dynamic thresholds, and broader service-availability metrics.

Keywords : Network Security; DDoS Mitigation; MikroTik RouterOS; RAW Firewall; Stateful Filtering

Abstrak

Penelitian ini mengevaluasi konfigurasi firewall berlapis pada MikroTik RouterOS v6 yang mengombinasikan tabel RAW dan Filter untuk memitigasi pola trafik yang berindikasi Distributed Denial of Service (DDoS) pada edge router di lingkungan produksi. Lima skenario berurutan (S0-S4) diamati, yaitu baseline normal, trafik beban tinggi tanpa proteksi, Filter saja, RAW saja, dan RAW-Filter. Kinerja dideskripsikan menggunakan utilisasi CPU, counter paket TCP SYN, UDP, dan ICMP, serta latensi rata-rata. Dibandingkan skenario tanpa proteksi (S1), RAW-Filter (S4) menurunkan CPU peak dari 55% menjadi 25% (54%), total paket SYN dari 2.952 menjadi 2.068 (30%), dan total paket UDP dari 484.054 menjadi 55.746 (88%); total paket ICMP meningkat dari 915 menjadi 1.032 (12%), sedangkan latensi rata-rata tetap 24 ms. RAW saja (S3) justru menghasilkan beban CPU terendah yang teramati (rata-rata 7%; peak 11%), sehingga hasil menunjukkan adanya trade-off antara early drop dan penegakan kebijakan stateful tambahan pada konfigurasi berlapis. Karena skenario dijalankan secara berurutan pada satu jaringan produksi dan manuskrip tidak melaporkan pengulangan teracak maupun statistik inferensial, temuan harus ditafsirkan sebagai bukti operasional deskriptif, bukan sebagai bukti superioritas kausal yang signifikan secara statistik. Studi ini memberi bukti praktis untuk tuning firewall berbasis baseline sekaligus menegaskan kebutuhan replikasi terkontrol, ambang dinamis, dan metrik ketersediaan layanan yang lebih luas.

Kata Kunci : Keamanan Jaringan; Mitigasi DDoS; MikroTik RouterOS; Firewall RAW; Stateful Filtering

Copyright@2026 Arif Rahmadi Wibowo, Desi Ramayanti
This is an open access article *under the CC-BY-NC-SA license.*

1. Pendahuluan

Distributed Denial of Service (DDoS) tetap menjadi ancaman terhadap ketersediaan layanan karena serangan dapat membanjiri sumber daya komputasi, state koneksi, dan kapasitas jaringan. Literatur mutakhir menunjukkan bahwa pertahanan DDoS berkembang dari filtering berbasis aturan menuju mekanisme yang lebih adaptif pada programmable networks, tetapi filtering di titik tepi tetap penting untuk membuang trafik yang tidak diinginkan sedini mungkin dan mengurangi biaya pemrosesan lanjutan (Li dkk., 2023; Wabi dkk., 2024; Dai dkk., 2024). Pada RouterOS, tabel RAW diproses pada tahap prerouting sebelum connection tracking, sedangkan tabel Filter mendukung kebijakan stateful setelah connection tracking; urutan ini secara arsitektural memungkinkan early drop di RAW diikuti penegakan kebijakan yang lebih kontekstual di Filter (MikroTik Documentation, 2025; MikroTik Documentation, 2026).

Pada jaringan perusahaan manufaktur peralatan saji berbahan keramik yang menjadi studi kasus, catatan operasional menunjukkan beberapa kejadian jalur outgoing down pada jam sibuk. Ketika insiden terjadi, CPU router dilaporkan meningkat dari sekitar 10% menjadi 50%, sedangkan trafik receive (Rx) mencapai 70-80 Mbps dan melampaui kapasitas paket bandwidth 60 Mbps. Kondisi tersebut menunjukkan adanya lonjakan trafik yang perlu dimitigasi, tetapi karakter serangan, sumber trafik, offered load, dan mekanisme pembangkitan trafik belum didokumentasikan secara memadai untuk menyatakan seluruh lonjakan tersebut sebagai DDoS terkontrol. Oleh sebab itu, penelitian ini menggunakan istilah trafik berindikasi DDoS dan menilai perubahan metrik operasional antar-konfigurasi.

Penelitian terdahulu pada MikroTik memperlihatkan bahwa RAW dapat mengurangi beban pemrosesan ketika trafik berlebih dibuang sebelum connection tracking, sedangkan Filter tetap diperlukan untuk kontrol state dan kebijakan akses (Haris dkk., 2022; Christanto dkk., 2025; Riduan dkk., 2025; Sitorus dkk., 2025; 'Ibad dkk., 2026). Pada konteks yang lebih luas, pendekatan mitigasi modern juga menekankan pemisahan antara deteksi/penandaan trafik dan aksi mitigasi agar respons dapat dilakukan dekat dengan jalur data serta disesuaikan dengan kondisi jaringan (Hnamte dkk., 2024; Ma dkk., 2024; Coscia dkk., 2024). Posisi penelitian ini bukan mengusulkan algoritma DDoS baru, melainkan mengevaluasi secara operasional kontribusi RAW, Filter, dan kombinasi keduanya pada satu edge router produksi dengan baseline yang sama.

Tujuan penelitian adalah: (1) mengimplementasikan layering RAW-Filter berbasis ambang statis pada MikroTik RouterOS v6; (2) membandingkan CPU load, trafik TCP SYN/UDP/ICMP, dan latensi pada skenario baseline, tanpa proteksi, Filter saja, RAW saja, serta RAW-Filter; dan (3) menyusun implikasi konfigurasi serta prosedur pemantauan dan rollback untuk lingkungan operasional. Kontribusi utama

penelitian bersifat empiris-praktis, yaitu memberikan bukti kasus produksi mengenai trade-off antara early drop pada RAW dan stateful enforcement pada Filter. Klaim mengenai packet loss, frekuensi outage, atau service availability hanya dapat dibuat apabila metrik tersebut benar-benar diukur.

Berdasarkan tujuan tersebut, pertanyaan penelitian dirumuskan sebagai berikut. RQ1: bagaimana layering RAW-Filter dapat diterapkan pada RouterOS v6 berdasarkan baseline trafik? RQ2: bagaimana perbedaan CPU load, counter SYN/UDP/ICMP, dan latensi antar-skenario S0-S4? RQ3: apakah kombinasi RAW-Filter memberikan trade-off operasional yang lebih seimbang dibanding RAW saja atau Filter saja? Evaluasi dibatasi pada satu router MikroTik RB1100AHx4, satu lingkungan perusahaan, RouterOS v6, dan metrik yang tersedia dalam manuskrip.

2. Kajian Terdahulu

Literatur DDoS mutakhir menunjukkan bahwa efektivitas mitigasi tidak hanya bergantung pada kemampuan mendeteksi trafik anomali, tetapi juga pada lokasi dan biaya aksi mitigasi. Survei Li dkk. (2023) menempatkan programmable networks, resource scheduling, dan koordinasi lintas domain sebagai arah penting pertahanan DDoS, sementara Zhao dkk. (2024) menekankan keragaman keluarga serangan yang perlu dibedakan ketika mengevaluasi mekanisme pertahanan. Pada SDN, Wabi dkk. (2024) mengelompokkan teknik deteksi ke pendekatan statistik, machine learning, neural network, dan teknik lain; Fouladi dkk. (2022), Hnamte dkk. (2024), serta Najar dan Naik (2024) memperlihatkan integrasi deteksi dengan aksi mitigasi pada lingkungan terprogram. Studi-studi tersebut menegaskan kebutuhan evaluasi yang jelas terhadap overhead, false positive, dan keberlanjutan layanan, bukan hanya kemampuan memblokir paket.

Pada level router dan firewall, temuan yang lebih dekat dengan konteks penelitian menunjukkan manfaat early filtering. Haris dkk. (2022) melaporkan bahwa konfigurasi RAW pada MikroTik dapat menurunkan beban CPU dan menormalkan respons ping pada pengujian DoS. Lutfi dkk. (2022) membahas kebijakan penempatan filter terhadap DDoS pada router MikroTik, sedangkan Rokhman dkk. (2023) menerapkan kombinasi Filter dan RAW pada lingkungan jaringan institusi. Christanto dkk. (2025) membandingkan address-list, Filter rules, dan RAW serta menemukan RAW lebih efektif untuk skenario DDoS ber-volume tinggi. Riduan dkk. (2025), Sitorus dkk. (2025), dan 'Ibad dkk. (2026) juga mengevaluasi firewall MikroTik pada SYN/UDP/ICMP flood atau skenario DDoS. Secara arsitektural, dokumentasi RouterOS menegaskan bahwa RAW dapat menjatuhkan paket sebelum connection tracking, sedangkan Filter digunakan untuk inspeksi dan kebijakan stateful (MikroTik Documentation, 2025; MikroTik Documentation, 2026).

Gap yang ditargetkan penelitian ini harus ditempatkan secara lebih sempit: masih terbatas bukti lapangan yang membandingkan RAW saja, Filter saja, dan layering RAW-Filter pada router produksi yang sama dengan baseline operasional dan prosedur rollback yang terdokumentasi. Kebaruan penelitian karena itu bersifat evaluatif dan deployment-oriented, bukan kebaruan algoritmik. Dibanding pendekatan terprogram dan adaptif yang menggunakan moving-target defense, reinforcement learning, automatic rule generation, atau traffic control dinamis (Ribeiro dkk., 2023; Yungaicela dkk., 2023; Coscia dkk., 2024; Ma dkk., 2024; Vladov dkk., 2026; Biševac dkk., 2026), penggunaan ambang statis pada penelitian ini juga menjadi batas penting yang perlu dievaluasi secara eksplisit.

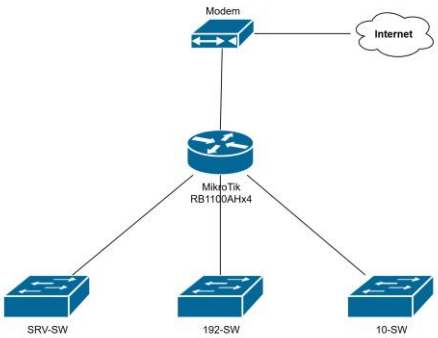
3. Metodologi Penelitian

Penelitian menggunakan desain kuasi-eksperimental lapangan dengan perbandingan lima kondisi konfigurasi pada satu edge router produksi. Istilah kuasi-eksperimental digunakan karena skenario dijalankan pada trafik nyata secara berurutan dan manuskrip tidak melaporkan randomisasi, replikasi independen, maupun kontrol penuh terhadap offered load. Variabel keluaran yang tersedia adalah CPU load, counter paket TCP SYN, UDP, dan ICMP, serta latensi rata-rata. Analisis utama bersifat deskriptif antar-skenario; tanpa pengulangan dan ukuran dispersi yang memadai, istilah "signifikan" tidak digunakan dalam makna statistik.

PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) digunakan sebagai kerangka rekayasa untuk merencanakan deployment jaringan, bukan sebagai pengganti desain eksperimen. Tahapannya membantu mendokumentasikan baseline, desain aturan, implementasi bertahap, pemantauan, dan rollback (Al Muzaki dkk., 2025). Validitas perbandingan tetap ditentukan oleh konsistensi beban uji, durasi, urutan skenario, teknik sampling, serta pengendalian faktor pengganggu.

3.1. *Prepare*

Pada tahap Prepare, vektor pemantauan ditetapkan pada TCP SYN, UDP, dan ICMP, dengan target latensi yang sama. Out-interface pada Router RB1100AHx4 dikelompokkan ke Interface List "WAN", kemudian tiga aturan mangle digunakan sebagai counter tanpa mengubah keputusan firewall. Baseline dikumpulkan pada kondisi non-sibuk dan sibuk untuk CPU average/peak, SYN/UDP/ICMP, dan latensi. Manuskrip menyebut total durasi 600 detik, sementara bagian hasil menjelaskan pencatatan per menit yang kemudian dikonversi menjadi packet per second (pps); interval sampling final harus dikonfirmasi agar prosedur dapat direplikasi. Nilai peak jam sibuk digunakan sebagai dasar awal penentuan ambang RAW.



Gambar 1. Topologi ringkas jaringan perusahaan

Tabel 1. *Baseline* Berdasar *Mangle Counter*

Baseline	**CPU (%)**		**SYN (pps)**		**UDP (pps)**		**ICMP (pps)**		**Latensi**
	Avg	***Peak***	***Avg***	***Peak***	***Avg***	***Peak***	***Avg***	***Peak***	***Avg***
Non-Sibuk	26	29	7	7	17	17	2	3	21
Sibuk	31	40	8	9	112	272	2	2	29

3.2. *Plan*

Rencana pengujian terdiri atas S0 (baseline normal), S1 (trafik beban tinggi/berindikasi serangan tanpa proteksi), S2 (Filter), S3 (RAW), dan S4 (RAW-Filter). Durasi setiap skenario dinyatakan sama. Perbandingan utama menggunakan CPU average/peak, SYN/UDP/ICMP average/peak atau total sesuai tabel, serta latensi rata-rata. Agar perbandingan kausal dapat dinilai, protokol harus menjelaskan sumber/generator trafik, jumlah host penyerang, jenis flood, target, rate atau offered load, durasi efektif, urutan skenario, waktu pelaksanaan, dan apakah trafik sah dipertahankan setara pada setiap skenario.

Tabel 2. Desain Skenario Uji

Skenario	**Deskripsi**	***RAW***	***Filter***	**Target**
S0	*Baseline* (normal)	*OFF*	*OFF*	Profil normal
S1	Serangan, tanpa proteksi	*OFF*	*OFF*	CPU & paket berpotensi tinggi
S2	*Filter* saja	*OFF*	*ON*	Efek *stateful*, beban *conntrack* masih terasa
S3	*RAW* saja	*ON*	*OFF*	*Early drop*, CPU *load* turun
S4	*RAW–Filter*	*ON*	*ON*	Target terbaik

3.3. *Design*

Pada tahap Design, RAW ditempatkan pada prerouting sebagai penyaring awal sebelum connection tracking, sedangkan Filter menerapkan kebijakan stateful setelah connection tracking. Ambang awal dihitung dari peak baseline dengan margin 1,2. Pendekatan tersebut konsisten dengan arsitektur RouterOS yang memproses RAW

prerouting sebelum connection tracking (MikroTik Documentation, 2025) dan dengan prinsip mitigasi dekat data plane untuk mengurangi overhead pemrosesan (Li dkk., 2023; Dai dkk., 2024). Namun, nilai desimal sumber pada Tabel 3 (8,6; 271,9; 2,2) tidak tampak pada Tabel 1 yang hanya menampilkan nilai pembulatan, sehingga asal nilai mentah dan aturan pembulatannya harus dijelaskan.

Tabel 3. Penentuan Ambang *RAW* Awal

Metrik	Nilai *Peak*	*Margin*	Ambang Awal
SYN	8,6 (bulat: 9)	1,2	10,8 (bulat: 11)
UDP	271,9 (bulat: 272)	1,2	326,4 (bulat: 326)
ICMP	2,2 (bulat: 2)	1,2	2,4 (bulat: 2)

3.4. *Implement*

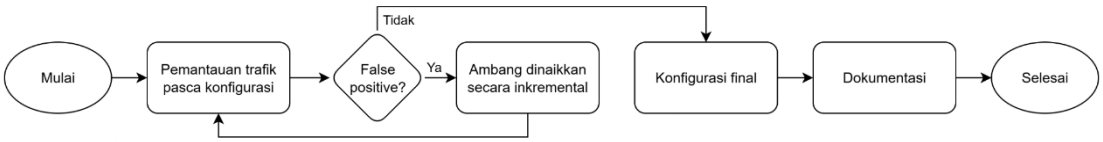
Implementasi dilakukan pada perangkat produksi dalam time window yang disepakati. RAW mula-mula dijalankan dalam mode observasi untuk menandai sumber yang melampaui ambang sebelum aksi drop diaktifkan. Setelah evaluasi operasional, aturan drop pada RAW dan penegakan Filter diaktifkan bertahap. Konfigurasi diekspor dan tangkapan layar disimpan untuk audit serta rollback. Prosedur ini mengurangi risiko perubahan langsung pada jaringan produksi, tetapi kriteria "tidak ada false positive" perlu didefinisikan secara terukur.

3.5. *Operate*

Skenario S0-S4 dijalankan secara berurutan pada trafik nyata dengan durasi yang dilaporkan seragam. Metrik yang dicatat adalah CPU, SYN/UDP/ICMP dari counter, dan latensi ke target yang sama. Karena kondisi jaringan produksi dapat berubah antar-waktu, hasil antar-skenario diperlakukan sebagai perbandingan deskriptif. Replikasi beberapa kali per skenario, randomisasi/counterbalancing urutan, atau penggunaan traffic generator dengan offered load yang terkontrol diperlukan untuk memperkuat inferensi kausal.

3.6. *Optimize*

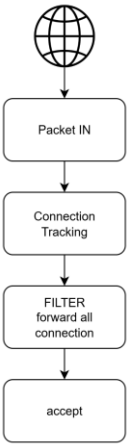
Tahap Optimize membandingkan S1 dengan konfigurasi terlindungi dan menyesuaikan ambang RAW secara inkremental sekitar 10-15% ketika ditemukan anomali. Setelah konfigurasi dianggap stabil, parameter dan SOP aktivasi, pemantauan, serta rollback didokumentasikan. Untuk mencegah bias evaluasi, manuskrip perlu menjelaskan apakah tuning dilakukan pada data yang berbeda dari data yang digunakan untuk melaporkan hasil akhir S4; pemisahan fase tuning dan evaluasi akan meningkatkan kredibilitas pengujian.



Gambar 2. Alur Pemantauan Jaringan

4. Hasil dan Pembahasan

Infrastruktur pengujian menggunakan edge router MikroTik RB1100AHx4 dengan RouterOS v6 yang terhubung ke uplink ISP melalui interface-list WAN. Pada kondisi awal, kebijakan firewall belum menerapkan early rate-aware filtering sebelum connection tracking. Pengukuran baseline pada Tabel 1 membedakan jam non-sibuk dan jam sibuk. Nilai baseline tersebut digunakan untuk menyusun ambang awal RAW, sedangkan Gambar 3 menggambarkan alur paket pada konfigurasi awal.



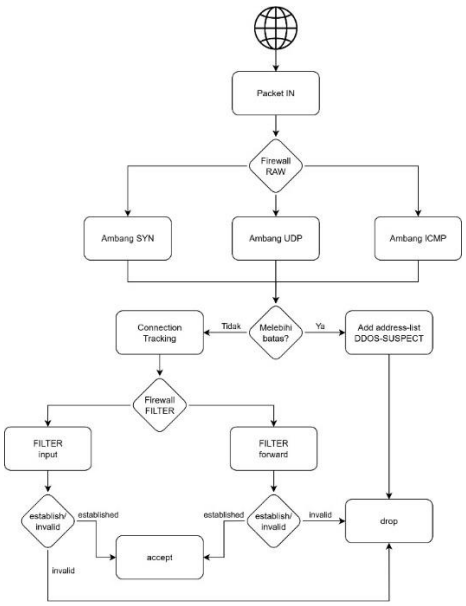
Gambar 3. Diagram alur paket MikroTik pada konfigurasi awal

Observasi awal menunjukkan bahwa lonjakan paket berasosiasi dengan peningkatan trafik bandwidth, penggunaan CPU, dan antrean pemrosesan. Tanpa mekanisme early filtering pada pre-connection tracking, trafik berlebih tetap memasuki connection tracking dan Filter sehingga biaya pemrosesan dapat meningkat. Pemblokiran sumber yang dilakukan secara manual juga memperlambat respons operasional. Pernyataan ini menjelaskan motivasi deployment, tetapi tidak dengan sendirinya membuktikan bahwa setiap lonjakan merupakan DDoS; karakteristik serangan harus dikaitkan dengan protokol uji yang terdokumentasi.

Solusi yang diuji menempatkan RAW sebagai gerbang berbasis ambang pada prerouting dan Filter sebagai penegak kebijakan stateful. RAW menandai atau menjatuhkan trafik yang melampaui ambang sebelum connection tracking, sedangkan

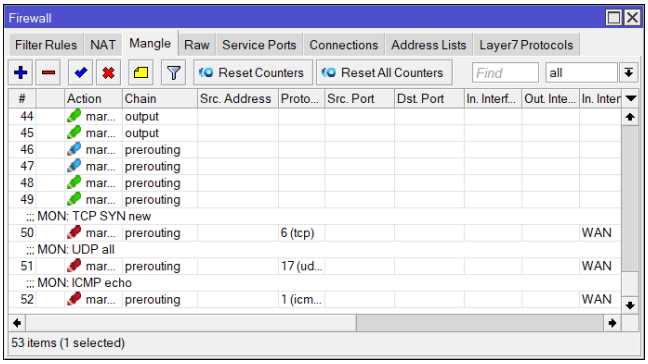
Filter menerima established/related, menolak invalid, dan membuang sumber yang telah ditandai. Sasaran desain adalah mengurangi overhead pemrosesan tanpa menaikkan latensi secara material, bukan mengasumsikan sejak awal bahwa konfigurasi gabungan pasti merupakan konfigurasi terbaik.

Alur paket usulan pada Gambar 4 memproses trafik melalui RAW terlebih dahulu dan membandingkannya dengan ambang per vektor (SYN, UDP, ICMP). Paket yang tidak melewati kriteria drop diteruskan ke connection tracking, sedangkan sumber yang melampaui ambang dapat dimasukkan ke address-list dan dibuang lebih awal. Setelah connection tracking, Filter menerapkan kebijakan stateful pada jalur input dan forward.



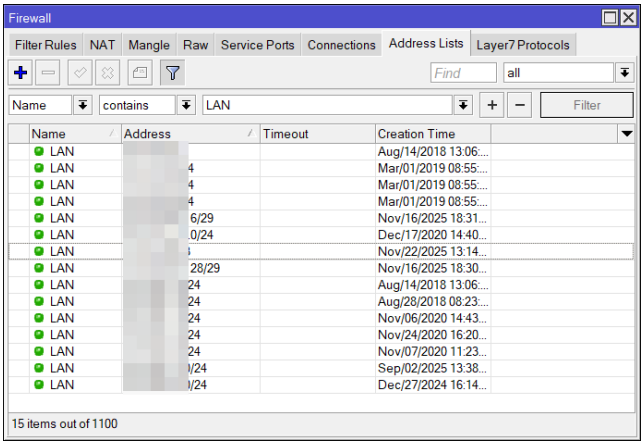
Gambar 4. Diagram alur paket MikroTik usulan

Mangle counter pada Gambar 5 digunakan untuk memantau SYN, UDP, dan ICMP sebagai dasar baseline. Manuskrip menyebut pencatatan per menit pada bagian hasil, sedangkan bagian metode juga menyebut interval satu detik; satu definisi interval sampling harus dipilih dan diterapkan konsisten pada seluruh tabel dan perhitungan pps.

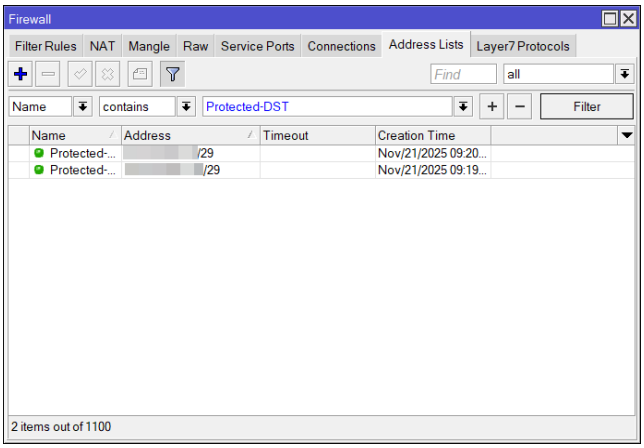


Gambar 5. Konfigurasi Firewall pada tabel Mangle

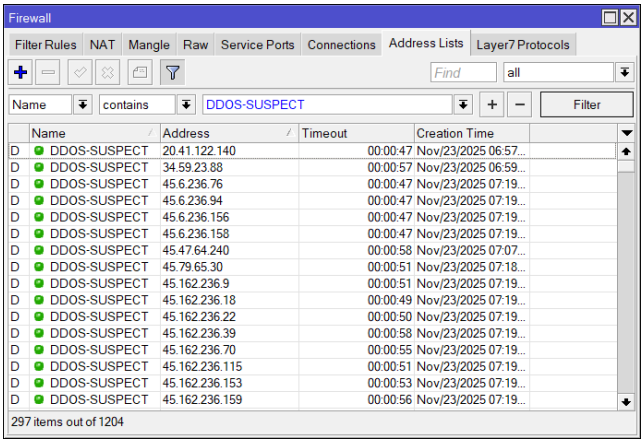
Gambar 6, 7, dan 8 menunjukkan address-list untuk jaringan lokal, alamat publik yang dilindungi, dan sumber yang ditandai sebagai DDOS-SUSPECT. Pemisahan daftar ini membantu membatasi cakupan proteksi agar trafik LAN yang sah tidak otomatis terkena aturan drop.



Gambar 6. Address-list untuk IP lokal (LAN)



Gambar 7. Address-list untuk IP publik



Gambar 8. Address-list untuk IP yang terindikasi serangan DDoS

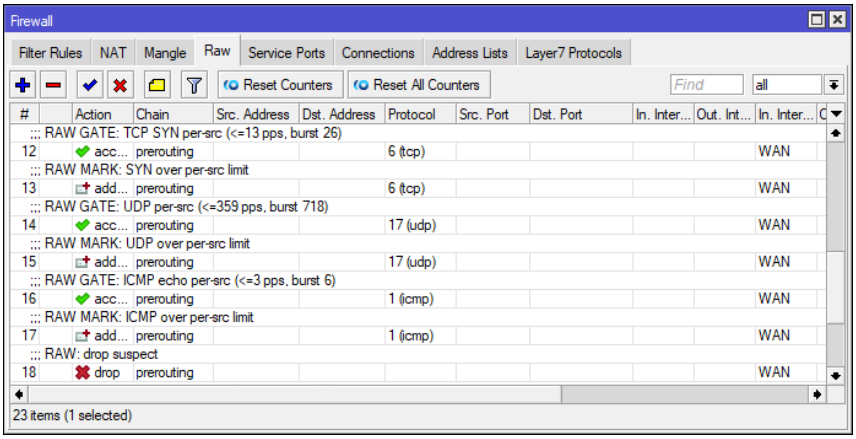
Setelah address-list disiapkan, konfigurasi RAW diterapkan sebagaimana Gambar 9. Ambang awal berasal dari baseline jam sibuk dan kemudian disesuaikan secara inkremental. Persamaan (1) dan (2) menunjukkan penambahan 10% dan 15% terhadap nilai x_n, tetapi simbol x_n, kondisi pemilihan persamaan, serta alasan penggunaan dua tingkat penyesuaian tersebut perlu didefinisikan agar proses penetapan ambang dapat direproduksi secara tepat.

$$Ambang = x_n + (x_n \times 0{,}1) \quad (1)$$

$$Ambang = x_n + (x_n \times 0{,}15) \quad (2)$$

Tabel 4. Ambang Statis yang Disesuaikan

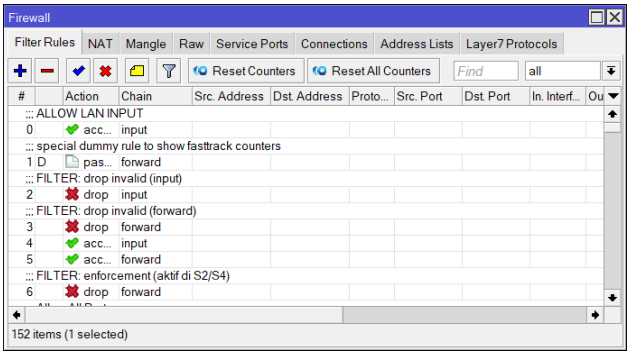
Ambang	SYN	UDP	ICMP
Awal	11	326	2
Disesuaikan	12,1	358,6	2,2



Gambar 9. Konfigurasi Firewall pada tabel RAW

Aturan Filter pada Gambar 10 menerapkan mekanisme stateful: koneksi established/related diterima, koneksi invalid ditolak, dan trafik dari address-list DDOS-

SUSPECT dibuang sebagai lapisan penyaringan tambahan. Konfigurasi lengkap dalam bentuk export teks yang telah disanitasi akan lebih reproduktif daripada tangkapan layar saja.



Gambar 10. Konfigurasi Firewall pada Filter Rules

Evaluasi dilakukan pada lima skenario S0-S4 dengan durasi yang dilaporkan sama. CPU load, SYN/UDP/ICMP, dan latensi dicatat pada target yang sama; jumlah hit RAW/Filter disebut dicatat sebagai bukti operasional, tetapi nilai hit tersebut belum disajikan dalam tabel hasil. Interval sampling juga perlu diselaraskan dengan penjelasan metode agar konversi ke pps dapat diaudit.

Tabel 5 merangkum CPU average/peak, SYN/UDP/ICMP average/peak dalam pps, dan latensi rata-rata. Tabel ini digunakan untuk membandingkan pola beban antar-skenario. Tabel 6 terpisah menyajikan total paket atau nilai ringkas S1 dan S4 untuk menghitung perubahan relatif; kedua jenis agregasi tidak boleh dipertukarkan dalam narasi.

Tabel 5. Ringkasan Kinerja Per Skenario

Skenario	CPU (%)		SYN (pps)		UDP (pps)		ICMP (pps)		Latensi
	Avg	*Peak*	*Avg*	*Peak*	*Avg*	*Peak*	*Avg*	*Peak*	*Avg*
S0	31	40	8	9	112	272	2	2	29
S1	48	55	5	6	896	903	2	2	24
S2	31	36	6	7	299	384	2	2	32
S3	7	11	4	5	137	188	2	2	29
S4	13	25	4	4	103	137	2	2	24

Tabel 5 menunjukkan bahwa S1 memiliki CPU tertinggi (48% average; 55% peak) dan UDP tertinggi (896 pps average; 903 pps peak). S2 menurunkan CPU peak menjadi 36%, tetapi UDP tetap 299 pps average. S3 menghasilkan CPU terendah (7% average; 11% peak) dengan UDP 137 pps average, sedangkan S4 menghasilkan CPU 13% average dan 25% peak dengan UDP terendah di antara skenario terlindungi, yaitu 103 pps average dan 137 pps peak. Dengan demikian, data tidak mendukung pernyataan bahwa S4 unggul pada setiap metrik: S3 lebih baik untuk CPU, sedangkan S4

memberikan kombinasi filtering berlapis dengan UDP lebih rendah dan latensi 24 ms. Pemilihan konfigurasi "terbaik" harus didasarkan pada kriteria multi-metrik yang dinyatakan eksplisit.

Tabel 6 membandingkan S1 dan S4 secara relatif. Persentase perubahan dihitung sebagai ((S1 - S4) / S1) x 100% untuk metrik yang lebih kecil dianggap lebih baik. Dengan rumus ini, CPU peak turun 54%, total SYN turun 30%, total UDP turun 88%, total ICMP justru meningkat 12%, dan latensi rata-rata tidak berubah (24 ms). Karena tidak tersedia distribusi pengulangan atau confidence interval, persentase ini merupakan perubahan deskriptif, bukan hasil uji signifikansi statistik.

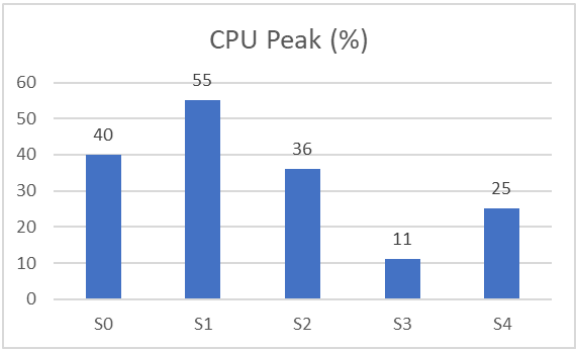
$$Perbaikan = \frac{(S1-S4)}{S1} \times 100\% \qquad (3)$$

Tabel 6. Perbandingan relatif metrik S1 dan S4

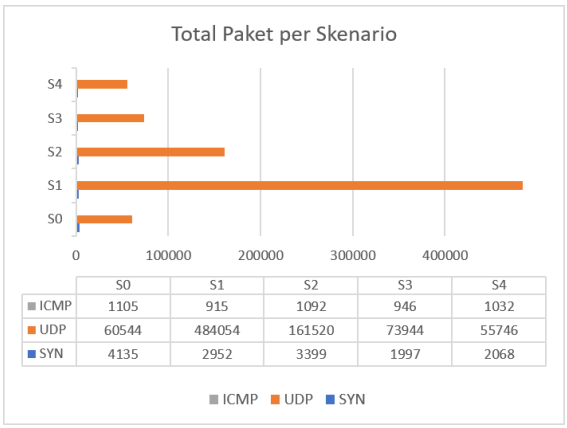
Metrik	S1	S4	Perbaikan
CPU peak (%)	55	25	54%
SYN (total paket)	2952	2068	30%
UDP (total paket)	484054	55746	88%
ICMP (total paket)	915	1032	-12%
Latensi rata-rata (ms)	24	24	0%

Berbeda dari SYN dan UDP, total ICMP pada S4 meningkat dari 915 menjadi 1.032 paket (sekitar 12%). Peningkatan absolutnya adalah 117 paket. Berdasarkan data yang tersedia, dampak kausal peningkatan ICMP terhadap CPU atau latensi tidak dapat dinilai secara inferensial karena penelitian tidak melaporkan replikasi, ukuran dispersi, atau analisis hubungan antar-metrik. Oleh karena itu, peningkatan ICMP dicatat sebagai anomali yang memerlukan penjelasan lebih lanjut, bukan dinyatakan "tidak signifikan".

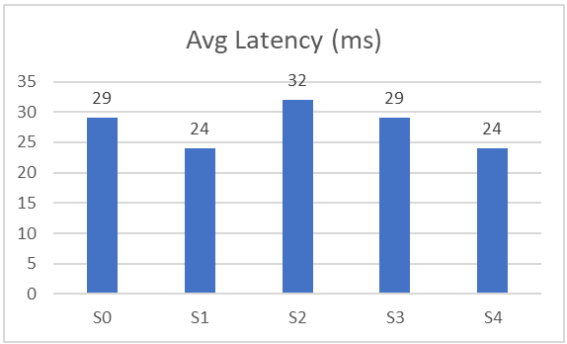
Gambar 11 memperlihatkan perbandingan CPU peak, Gambar 12 membandingkan total paket SYN/UDP/ICMP, dan Gambar 13 menunjukkan latensi rata-rata. Ketiganya mendukung pembacaan deskriptif pada Tabel 5 dan Tabel 6, tetapi tidak menggantikan kebutuhan terhadap pengulangan eksperimen dan analisis variasi apabila manuscript ingin membuat klaim inferensial.



Gambar 11. Perbandingan CPU *Peak* Per Skenario (S0-S4)



Gambar 12. Total Paket SYN, UDP, dan ICMP Per Skenario (S0-S4)



Gambar 13. Rata-rata Latensi Per Skenario (S0-S4)

Pada tingkat operasional, RAW dan Filter memiliki fungsi yang saling melengkapi tetapi tidak identik. RAW mengurangi sebagian beban sebelum connection tracking, sedangkan Filter mempertahankan kontrol stateful terhadap koneksi established/related, invalid, dan sumber yang telah ditandai. Data S0-S4 menunjukkan bahwa manfaat tersebut harus dibaca sebagai trade-off: S3 paling ringan terhadap CPU, sementara S4 menerapkan kontrol berlapis dengan UDP lebih rendah dan latensi yang tidak meningkat dibanding S1. Proteksi dibatasi pada alamat tujuan layanan yang ditentukan agar trafik LAN yang sah tidak otomatis terkena aturan drop; efektivitas strategi ini terhadap false positive tetap memerlukan metrik eksplisit.

4.1. Pembahasan dan Ancaman Validitas

Secara mekanistik, penurunan CPU pada konfigurasi yang menggunakan RAW konsisten dengan urutan pemrosesan RouterOS: RAW prerouting dievaluasi sebelum connection tracking sehingga paket yang tidak diperlukan dapat dihentikan lebih awal (MikroTik Documentation, 2025; MikroTik Documentation, 2026). Prinsip yang sama terlihat pada penelitian DDoS modern yang mendorong mitigasi sedekat mungkin

dengan data plane untuk mengurangi overhead dan mempercepat respons (Dai dkk., 2024; Ma dkk., 2024). Namun, hasil S3 dan S4 menunjukkan bahwa penambahan Filter stateful memiliki biaya pemrosesan: S3 mencatat CPU peak 11%, sedangkan S4 25%. Karena itu, manfaat layering harus dinilai sebagai trade-off antara resource efficiency dan policy enforcement, bukan sekadar berdasarkan satu metrik.

Posisi hasil terhadap state of the art juga perlu proporsional. Pendekatan adaptif seperti reinforcement learning, dynamic thresholding, dan automatic rule generation telah dikembangkan untuk merespons perubahan trafik secara dinamis (Yungaicela dkk., 2023; Coscia dkk., 2024; Biševac dkk., 2026). Penelitian ini tidak bersaing pada kebaruan algoritmik tersebut; kontribusinya adalah bukti deployment berbasis fitur native MikroTik yang lebih sederhana dan mudah dioperasionalkan. Keunggulan praktis ini penting untuk lingkungan yang membutuhkan solusi ringan, tetapi generalisasi ke router, versi RouterOS, pola trafik, dan kapasitas uplink lain tetap perlu diuji.

Ancaman validitas utama berasal dari desain lapangan berurutan pada satu jaringan produksi. Manuskrip belum mendokumentasikan attack generator, offered load yang setara, jumlah sumber, random seed atau pengulangan, randomisasi urutan skenario, confidence interval, serta kontrol terhadap perubahan trafik sah. Selain itu, service availability tidak diukur secara langsung melalui uptime, request success rate, outage duration, throughput, packet loss, jitter, memory, atau ukuran connection-tracking table. Akibatnya, hasil yang tersedia cukup untuk menunjukkan pola operasional yang menjanjikan, tetapi belum cukup untuk menyimpulkan superioritas kausal atau generalisasi luas.

5. Kesimpulan

Berdasarkan lima skenario yang diamati pada satu router produksi, penggunaan RAW berasosiasi dengan penurunan beban CPU dan trafik UDP dibanding kondisi tanpa proteksi. Konfigurasi RAW saja (S3) menghasilkan CPU terendah, sedangkan RAW-Filter (S4) memberikan kombinasi early drop dan stateful filtering dengan CPU peak 25%, total SYN 30% lebih rendah, total UDP 88% lebih rendah, dan latensi rata-rata sama-sama 24 ms dibanding S1. Hasil tersebut menunjukkan trade-off antar-metrik; karena itu, S4 lebih tepat diposisikan sebagai konfigurasi berlapis yang operasional daripada dinyatakan sebagai konfigurasi yang secara universal paling baik.

Keterbatasan penelitian meliputi satu perangkat MikroTik RB1100AHx4, RouterOS v6, satu lingkungan perusahaan, ambang statis, dan metrik yang terbatas pada CPU, SYN/UDP/ICMP, serta latensi. Skenario dijalankan secara berurutan pada trafik nyata, sementara detail attack generator, offered load, pengulangan, randomisasi, dan statistik inferensial belum tersedia. Karena itu, efek yang dilaporkan bersifat deskriptif dan generalisasi ke lingkungan lain perlu dilakukan secara hati-hati. Klaim tentang

service availability, packet loss, atau penurunan frekuensi outage tidak dibuat karena metrik tersebut belum dilaporkan secara langsung.

Penelitian selanjutnya perlu menggunakan traffic generator yang terkontrol, pengulangan independen, randomisasi atau counterbalancing urutan skenario, serta ukuran dispersi dan confidence interval. Evaluasi juga perlu menambahkan throughput, packet loss, jitter, memory, connection-tracking occupancy, false-positive rate, legitimate-flow success rate, dan durasi outage. Dynamic thresholding atau mekanisme adaptif dapat dibandingkan dengan ambang statis, tetapi konfigurasi yang lebih kompleks tetap harus dinilai dari overhead, explainability operasional, dan kemudahan rollback pada perangkat tepi.

6. Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada pihak perusahaan yang telah memberikan izin, dukungan, serta fasilitas yang diperlukan sehingga penelitian ini dapat dilaksanakan dengan baik. Ucapan terima kasih juga disampaikan kepada dosen pembimbing selaku penulis korespondensi yang telah memberikan bimbingan, arahan, masukan, serta dukungan selama proses penyusunan dan penyelesaian penelitian ini. Seluruh bantuan dan kerja sama yang diberikan sangat berarti dalam mendukung keberhasilan penelitian ini.

7. Pernyataan Penulis

7.1. Kontribusi Penulis

Konseptualisasi, A.R.W. dan D.R.; metodologi, A.R.W. dan D.R.; investigasi, A.R.W.; kurasi data, A.R.W.; analisis formal, A.R.W. dan D.R.; visualisasi, A.R.W.; penulisan—draf awal, A.R.W.; penulisan—tinjauan dan penyuntingan, D.R.; supervisi, D.R.; administrasi proyek, A.R.W. Seluruh penulis telah membaca dan menyetujui versi akhir manuskrip.

7.2. Pendanaan

Penelitian ini tidak menerima pendanaan eksternal.

7.3. Konflik Kepentingan

Para penulis menyatakan tidak terdapat konflik kepentingan.

7.4. Penggunaan Kecerdasan Artifisial

Kecerdasan artifisial generatif atau teknologi berbantuan AI tidak digunakan untuk menghasilkan data ilmiah, hasil eksperimen, atau kesimpulan ilmiah yang dilaporkan dalam penelitian ini. Para penulis tetap bertanggung jawab penuh atas keakuratan, orisinalitas, integritas, dan seluruh isi artikel. Apabila alat berbantuan AI

digunakan secara terbatas untuk dukungan bahasa atau teknis selama penyusunan manuskrip, seluruh keluarannya telah ditinjau dan diverifikasi oleh penulis.

7.5. Persetujuan Etik

Penelitian ini tidak melibatkan partisipan manusia maupun hewan yang memerlukan persetujuan etik. Penelitian dilaksanakan pada infrastruktur jaringan dan metrik trafik operasional di lingkungan produksi dengan izin dari organisasi terkait.

7.6. Ketersediaan Data

Data yang mendukung temuan penelitian ini tersedia dari penulis korespondensi berdasarkan permintaan yang wajar. Log operasional terperinci, informasi alamat IP, dan konfigurasi jaringan lengkap dapat dibatasi atau disanitasi karena pertimbangan kerahasiaan organisasi dan keamanan siber. Data kinerja agregat yang digunakan dalam analisis telah disajikan dalam artikel.

Bibliografi

Al Muzaki, D. F., Efendi, T. F., & Muqorobin. (2025). Penerapan jaringan hotspot berbasis Mikrotik menggunakan metode PPDIO (Prepare, Plan, Design, Implement, Operate, Optimize). Bulletin of Computer Science Research, 5(4), 490-502. https://doi.org/10.47065/bulletincsr.v5i4.592

Biševac, S., Bojović, Ž., Bojović, P. D., & Doknić, I. (2026). Closed-loop CPU-aware traffic control for SDN-enabled 5G/6G networks in Open vSwitch dataplanes. Smart Cities, 9(6), 91. https://doi.org/10.3390/smartcities9060091

Christanto, F. W., Cholillah, P., & Hirzan, A. M. (2025). Optimizing Mikrotik-based network security using address list, firewall filter rules, and raw firewall. Revista de Informática Teórica e Aplicada, 32(3), 66-76. https://doi.org/10.22456/2175-2745.142954

Coscia, A., Dentamaro, V., Galantucci, S., Maci, A., & Pirlo, G. (2024). Automatic decision tree-based NIDPS ruleset generation for DoS/DDoS attacks. Journal of Information Security and Applications, 82, 103736. https://doi.org/10.1016/j.jisa.2024.103736

Dai, Y., Huang, T., & Wang, S. (2024). DAmpADF: A framework for DNS amplification attack defense based on Bloom filters and NAmpKeeper. Computers & Security, 139, 103718. https://doi.org/10.1016/j.cose.2024.103718

Fouladi, R. F., Ermiş, O., & Anarim, E. (2022). A DDoS attack detection and countermeasure scheme based on DWT and auto-encoder neural network for SDN. Computer Networks, 214, 109140. https://doi.org/10.1016/j.comnet.2022.109140

Haris, A. I., Riyanto, B., Surachman, F., & Ramadhan, A. A. (2022). Analisis pengamanan jaringan menggunakan router Mikrotik dari serangan DoS dan

pengaruhnya terhadap performansi. Komputika: Jurnal Sistem Komputer, 11(1), 67-76. https://doi.org/10.34010/komputika.v11i1.5227

Hnamte, V., Najar, A. A., Nhung-Nguyen, H., Hussain, J., & Naik, S. M. (2024). DDoS attack detection and mitigation using deep neural network in SDN environment. Computers & Security, 138, 103661. https://doi.org/10.1016/j.cose.2023.103661

'Ibad, M. I., Mahmud, W., & Wilujeng, G. (2026). Analysis of MikroTik firewall effectiveness in mitigating DDoS attacks using the Network Development Life Cycle (NDLC) approach. SISTEMASI, 15(5), 1731. https://doi.org/10.32520/stmsi.v15i5.6347

Li, Q., Huang, H., Li, R., Lv, J., Yuan, Z., Ma, L., Han, Y., & Jiang, Y. (2023). A comprehensive survey on DDoS defense systems: New trends and challenges. Computer Networks, 233, 109895. https://doi.org/10.1016/j.comnet.2023.109895

Lutfi, S., Khairan, A., Muin, Y., & Salmin, M. (2022). Optimal filter assignment policy against distributed denial of service attack on router Mikrotik. MATEC Web of Conferences, 372, 04008. https://doi.org/10.1051/matecconf/202237204008

Ma, J., Su, W., Li, Y., & Peng, Y. (2024). Synchronizing DDoS detection and mitigation based graph learning with programmable data plane, SDN. Future Generation Computer Systems, 154, 206-218. https://doi.org/10.1016/j.future.2023.12.033

MikroTik Documentation. (2025). Packet Flow in RouterOS. Last updated October 31, 2025. https://help.mikrotik.com/docs/spaces/ROS/pages/328227/Packet+Flow+in+RouterOS

MikroTik Documentation. (2026). Filter: RAW Filtering. https://help.mikrotik.com/docs/spaces/ROS/pages/48660574/Filter

Najar, A. A., & Naik, S. M. (2024). Cyber-Secure SDN: A CNN-based approach for efficient detection and mitigation of DDoS attacks. Computers & Security, 139, 103716. https://doi.org/10.1016/j.cose.2024.103716

Ribeiro, M. A., Fonseca, M. S. P., & de Santi, J. (2023). Detecting and mitigating DDoS attacks with moving target defense approach based on automated flow classification in SDN networks. Computers & Security, 134, 103462. https://doi.org/10.1016/j.cose.2023.103462

Riduan, M. A. O., Riska, & Alamsyah, H. (2025). Analisa dan implementasi keamanan jaringan berbasis Firewall RAW terhadap serangan DDoS pada router Mikrotik. Jurnal Media Infotama, 21(1), 317-328. https://doi.org/10.37676/jmi.v21i1.7835

Rokhman, M. N., Rizaldy, E. F., Abdullah, N., & Puspitasari, N. F. (2023). Implementasi firewall filter rule dan RAW sebagai metode pengamanan jaringan pada Perpustakaan XYZ. Jurnal Elektrosista, 11(1), 58-75. https://doi.org/10.63824/jtep.v11i1.142

Sitorus, M. A., Nasution, D., & Iqbal, M. (2025). Analisis efektivitas RAW Firewall Mikrotik dalam mitigasi serangan DDoS pada infrastruktur jaringan. Journal of

Science and Social Research, 8(2), 3354-3358. https://doi.org/10.54314/jssr.v8i2.3930

Vladov, S., Ścisło, Ł., Sachenko, A., Krupiński, J., Vysotska, V., Korniienko, M., Uhrovetskyi, O., Krykun, V., Levchenko, K., & Sachenko, A. (2026). Neural network method for detecting UDP flood attacks in critical infrastructure microgrid protection systems with law enforcement agencies' rapid response. Energies, 19(1), 209. https://doi.org/10.3390/en19010209

Wabi, A. A., Idris, I., Olaniyi, O. M., & Ojeniyi, J. A. (2024). DDoS attack detection in SDN: Method of attacks, detection techniques, challenges and research gaps. Computers & Security, 139, 103652. https://doi.org/10.1016/j.cose.2023.103652

Yungaicela, N. M., Vargas-Rosales, C., & Pérez-Díaz, J. A. (2023). SDN/NFV-based framework for autonomous defense against slow-rate DDoS attacks by using reinforcement learning. Future Generation Computer Systems, 149, 637-649. https://doi.org/10.1016/j.future.2023.08.007

Zhao, Z., Li, Z., Zhou, Z., Yu, J., Song, Z., Xie, X., Zhang, F., & Zhang, R. (2024). DDoS family: A novel perspective for massive types of DDoS attacks. Computers & Security, 138, 103663. https://doi.org/10.1016/j.cose.2023.103663