Vol. 12 No.1 Oktober 2025 http://dx.doi.org/10.22202/ei.2025.v12i1.10339

Jurnal Edik Informatika
Penelitian Bidang Komputer Sains dan Pendidikan Informatika
Website: ejournal.upgrisba.ac.id/index.php/eDikInformatika

Implementasi Mekanisme Keamanan DNS dalam Menghadapi Serangan UDP Pada Router Mikrotik

Ahmad Fauzi[1], Andry Maulana[2]
[1]Universitas Bina Sarana Informatika
[2]Universitas Nusa Mandiri
ahmad.azy@bsi.ac.id

INFO ARTIKEL

Diterima:
24 September 2025
Direview:
26 September 2025
Disetujui:
29 Oktober 2025

Keywords:

DNS, UDP Packet loss, Mikrotik Router, Network Security, Firewall.

Abstract

The Domain Name System (DNS) is a critical service in computer networks that is often targeted by various types of attacks, one of the most common being UDP Packet loss. Such attacks can degrade network performance, increase latency, and even disrupt service availability. The objective of this research is to implement DNS security mechanisms on Mikrotik routers to mitigate UDP-based attacks and evaluate their effectiveness in maintaining service quality.The research method consists of three main stages: designing a UDP attack scenario on DNS services, configuring security mechanisms on the Mikrotik router using firewall and traffic filtering features, and testing network performance before and after the security implementation. The evaluation parameters include throughput, packet loss, latency, and service availability.The results show that the security configuration on the Mikrotik router significantly reduces the impact of UDP Packet loss attacks against DNS. After implementing the proposed security mechanisms, there was a notable decrease in packet loss, improved throughput stability, and higher DNS service availability compared to the unprotected condition.In conclusion, the implementation of security mechanisms on Mikrotik routers provides an effective, practical, and cost-efficient solution for strengthening DNS resilience against UDP attacks, especially in small to medium-scale networks.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah menjadikan internet sebagai bagian penting dalam kehidupan modern. Hampir seluruh aktivitas manusia, mulai dari komunikasi, transaksi bisnis, hingga layanan publik, bergantung pada infrastruktur jaringan yang aman dan andal. *Domain Name System* (DNS) menjadi fondasi penting dalam sistem jaringan komputer karena berfungsi menerjemahkan nama domain ke alamat IP yang dapat dikenali oleh mesin (Syawaludin, *et all* 2020). Tanpa DNS, pengguna harus mengingat deretan angka alamat IP untuk mengakses layanan internet.

Namun, peran strategis DNS tersebut menjadikannya sasaran empuk serangan siber. Salah satu jenis serangan paling umum adalah serangan berbasis *User Datagram Protocol* (UDP). Serangan ini dilakukan dengan mengirim paket UDP dalam jumlah besar ke

server DNS sehingga menyebabkan konsumsi sumber daya berlebih dan gangguan layanan. Laporan dari *Cisco Network Security* menunjukkan bahwa serangan ke layanan DNS menyumbang lebih dari 16% insiden DDoS yang terjadi di seluruh dunia pada 2023. Dampaknya bisa berupa akses internet yang melambat, tingginya latency, hingga terhentinya layanan penting secara global (Academy n.d.), Fenomena ini menandakan bahwa DNS merupakan titik lemah yang perlu mendapatkan perhatian khusus dari sisi keamanan jaringan.

Berbagai teknologi mitigasi telah ditawarkan untuk melindungi DNS (Nguyen. 2019) menegaskan bahwa serangan DDoS berbasis UDP, seperti kasus Mirai Botnet, memiliki kemampuan melumpuhkan sistem skala besar. Sementara itu (Cervone. 2020) menyoroti solusi DNSSEC sebagai lapisan keamanan tambahan, namun implementasinya membutuhkan kompetensi teknis tinggi dan infrastruktur yang memadai. Pada lingkungan pendidikan, usaha kecil, atau penyedia layanan internet skala menengah, kebutuhan akan solusi keamanan yang lebih sederhana, efisien, dan terjangkau masih menjadi tantangan utama. Router Mikrotik merupakan perangkat yang banyak digunakan karena fitur keamanan jaringan yang lengkap serta harga yang ekonomis (MikroTik, 2020). Dengan memanfaatkan *firewall, traffic filtering*, serta kemampuan membatasi lalu lintas UDP, perangkat ini berpotensi menjadi solusi efektif dalam mencegah gangguan terhadap layanan DNS.

Secara teoretis, penelitian ini berkontribusi pada penguatan literatur mengenai mekanisme mitigasi serangan DNS berbasis *firewall router.* Dari sisi praktis, penelitian ini memberikan panduan konfigurasi keamanan yang dapat dengan mudah diimplementasikan oleh administrator jaringan pada lingkungan berskala kecil hingga menengah. Penelitian ini bertujuan merancang dan menguji efektivitas konfigurasi keamanan DNS pada Router Mikrotik untuk menghadapi serangan UDP, serta mengevaluasi performa jaringan sebelum dan setelah penerapan mekanisme keamanan tersebut. Dengan pendekatan eksperimental, diharapkan hasil penelitian ini dapat membantu pengelola jaringan dalam menjaga stabilitas, keandalan, dan ketersediaan layanan DNS di tengah meningkatnya ancaman siber.

METODE

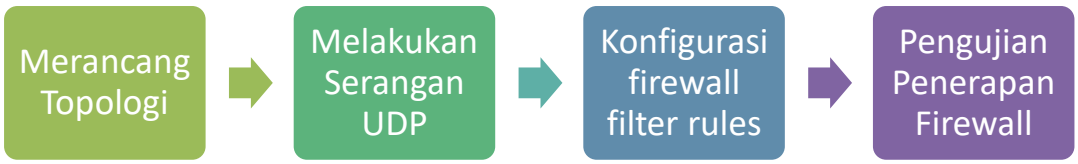
Penelitian ini menggunakan pendekatan eksperimental dengan desain pre-test dan post-test untuk membandingkan performa jaringan sebelum dan sesudah penerapan mekanisme keamanan DNS pada Router Mikrotik selama berlangsungnya serangan UDP *Packet loss.* Variabel bebas pada penelitian ini adalah penerapan mekanisme keamanan DNS yang diimplementasikan dalam dua kondisi, yaitu ketika router tidak memiliki konfigurasi keamanan serta ketika konfigurasi *firewall raw rules* telah diaktifkan. Sementara itu, variabel terikat terdiri dari parameter kinerja jaringan yang meliputi t*hroughput, packet loss, latency*, dan *availability* layanan DNS.

Hipotesis yang diuji dalam penelitian ini adalah bahwa penerapan mekanisme keamanan pada Router Mikrotik dapat menurunkan *packet loss*, meningkatkan *throughput*, menurunkan *latency*, serta meningkatkan *availability* layanan DNS selama serangan UDP *Packet loss*. Sebagai pembanding, hipotesis nol menyatakan bahwa tidak terdapat perbedaan signifikan kinerja jaringan sebelum dan sesudah konfigurasi keamanan diterapkan. Untuk mendukung pengujian hipotesis tersebut, penelitian ini menggunakan sejumlah alat dan instrumen seperti Router Mikrotik RB750 sebagai target layanan DNS sekaligus perangkat utama mitigasi, Hping3 atau Mikrotik Traffic Generator untuk melakukan simulasi serangan UDP *Packet loss*, serta PING, *Bandwidth Tes*t, Wireshark, dan Torch Mikrotik untuk melakukan pengukuran dan pemantauan parameter jaringan.

Prosedur pengujian dilakukan melalui tiga skenario, yakni kondisi jaringan normal tanpa serangan, kondisi serangan UDP *Packet loss* tanpa adanya konfigurasi keamanan, dan kondisi serangan UDP *Packet loss* ketika mekanisme keamanan telah diaktifkan. Setiap skenario dilakukan sebanyak lima kali ulangan dengan durasi serangan selama 60 detik pada setiap ulangan untuk meningkatkan reliabilitas hasil pengujian. Selain itu, urutan pengujian diacak menggunakan metode *balanced randomization* guna mengurangi bias urutan dan efek sisa dari pengujian sebelumnya.

Parameter penelitian diukur berdasarkan performa throughput dalam satuan Mbps, persentase *packet loss*, nilai *latency* dalam milidetik, serta keberhasilan DNS dalam menyelesaikan proses *resolve domain*. Seluruh data hasil pengukuran kemudian dianalisis menggunakan statistik deskriptif berupa rata-rata, standar deviasi, serta interval kepercayaan 95%. Sebelum dilakukan analisis inferensial, terlebih dahulu dilakukan uji normalitas menggunakan metode Shapiro–Wilk untuk menentukan jenis uji statistik yang digunakan. Apabila data terdistribusi normal, maka analisis perbedaan dilakukan menggunakan uji Paired t-test, sedangkan jika tidak normal digunakan uji Wilcoxon Signed-Rank Test dengan tingkat signifikansi sebesar $\alpha = 0{,}05$.

Penelitian ini dilaksanakan dalam lingkungan jaringan yang dirancang sesuai topologi penelitian, terdiri dari Router Mikrotik sebagai penyedia layanan DNS, satu perangkat client sebagai pengakses layanan DNS, serta satu perangkat *attacker* sebagai generator serangan yang terhubung melalui jaringan eksternal menuju router. Dengan prosedur dan metode pengujian tersebut, penelitian ini diharapkan mampu menghasilkan temuan yang valid, reliabel, dan dapat direplika pada lingkungan jaringan berskala kecil hingga menengah.



Gambar 1. Tahapan Penelitian

HASIL DAN PEMBAHASAN

Merancang Topologi

Berdasarkan tahapan penelitian yang sudah dibuat maka dalam perancangan topologi jaringan dibutuhkan beberapa perangkat keras yang di tentukan dalam bentuk topologi jaringan, dimana Tolopogi jaringan komputer adalah sebuah gambaran dengan menggunakan simbol-simbol *networking* guna untuk menggambarkan sebuah pola atau struktur jaringan baik sudah dibentuk atau yang akan dibentuk, sehingga pada penelitian ini menggunakan topologi sebagai berikut:

Gambar 2. Topologi Penelitian

Topologi yang ditampilkan menggambarkan jaringan sederhana dengan tiga elemen utama: Internet (luar) di bagian atas, Router Mikrotik di tengah sebagai penghubung dan pengendali lalu lintas, dan LAN (jaringan lokal) di bagian bawah yang mewakili perangkat pengguna. Dari Internet menuju Router Mikrotik terdapat ancaman yang dilabeli Public Enemy — penyerang eksternal yang mengirim lalu lintas berbahaya (mis. UDP *Packet loss*) menuju layanan di jaringan. Di sisi LAN, terdapat *Local Enemy* — penyerang yang berasal dari dalam jaringan lokal dan dapat mencoba menyerang layanan internal atau memanfaatkan jalur keluar melalui router. Panah pada gambar menunjukkan arah aliran lalu lintas: lalu lintas normal dan berbahaya mengalir dari Internet ke Router Mikrotik lalu ke LAN, sementara Router Mikrotik berfungsi sebagai titik kontrol yang dapat menerapkan kebijakan keamanan (firewall, filtering, pembatasan UDP, pemblokiran dinamis) untuk menahan atau memitigasi serangan baik dari public maupun *local enemy*. Topologi ini menekankan peran Router Mikrotik sebagai lapisan perlindungan sentral antara sumber ancaman dan aset jaringan lokal dan berdasarkan dari topologi tersebut dibutuhkan sebuah hardware sebagai berikut:

Tabel 1. Spesifikasi Hardware

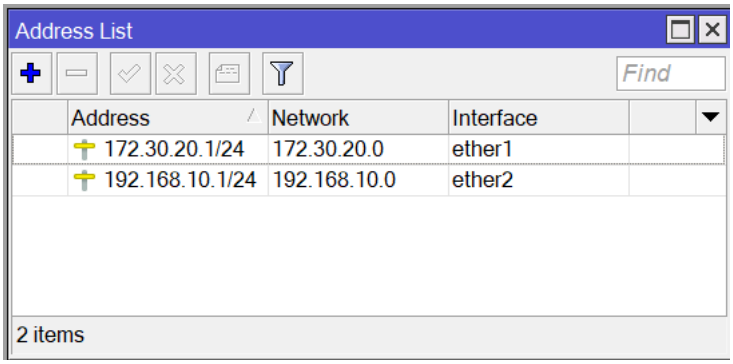
No.	HARDWARE	TIPE	SPESIFIKASI
1	Router	Mikrotik Router Board RB 750r2 (Hexlite)	Arsitektur: MIPSBE CPU : QCA9531 / QCA9533 Jumlah Inti CPU : 1 Frekuensi CPU : 850 MHz RAM : 64 MB Penyimpanan Internal : 16 MB FLASH Lisensi RouterOS : Level 4
2	Switch	TP-Link TL-SF1008D	Antarmuka (Interface) : 8 port RJ45 dengan kecepatan **10/100Mbps** Standar dan Protokol : IEEE 802.3, IEEE 802.3u, IEEE 802.3x Kapasitas Switching : 1.6 Gbps Tingkat Penerusan Paket (Packet Forwarding Rate) : 1.19 Mpps Tabel Alamat MAC (MAC Address Table) : 2K Metode Transfer : Store and Forward
3	Komputer	Asus Vivobook M1403QA	Operating System: Windows 11 Home Single Processor: AMD Ryzen 5 5600H with Radeon Graphics (12 CPUs), ~3.3GHz Memory: 8192MB RAM

Setelah ditentukan hardware dan dilakukan penerapan peracangan jaringan yang sesuai dengan topologi sehingga terdapat tabel IP address sebagai berikut:

Tabel 2. Tabel IP Address

NO	HARDWARE	INTERFACE	IP ADDRESS	SUBNETMASK
1	Router	ETH 1	172.30.20.1 (Public)	255.255.255.0
2		ETH 2	192.168.10.1 (LAN)	255.255.255.0
3	Komputer	LAN Card	192.168.10.10	255.255.255.0

Dengan IP address yang sudah ditentukan melalui dokumentasi tabel IP maka selanjutnya dalam Model penelitian yang sudah dirancang tahap selanjutnya adalah melakukan konfigurasi baik di sis Router maupun di sisi client.

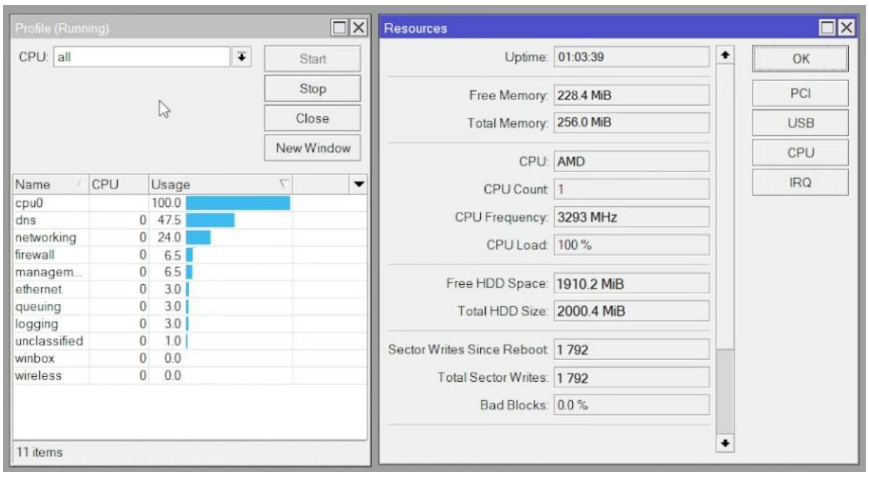


Gambar 2. IP Address

Pada penelitian ini penulis sudah melakukan konfigurasi terhadap router dengan settingan standar dimana pada router tersebut sudah tersetting IP Address, DNS dan mendapatkan akses internet begiru juga dari sisi client yang sudah mendapatkan IP dan dapat berseluncur di jaringan internet, sehingga penulis hanya berfokus pada konfigurasi kemanan serangan DNS.

Melakukan Serangan UDP

Pada settingan mikrotik belum ada pengamanan pada DNS mikrotik sehingga bila di coba dilakukan serangan akan di ketahui melalui tools Profil.



Gambar 3. Serangan tanpa kemanan DNS

Gambar tersebut menunjukkan tampilan monitoring kinerja pada Router Mikrotik

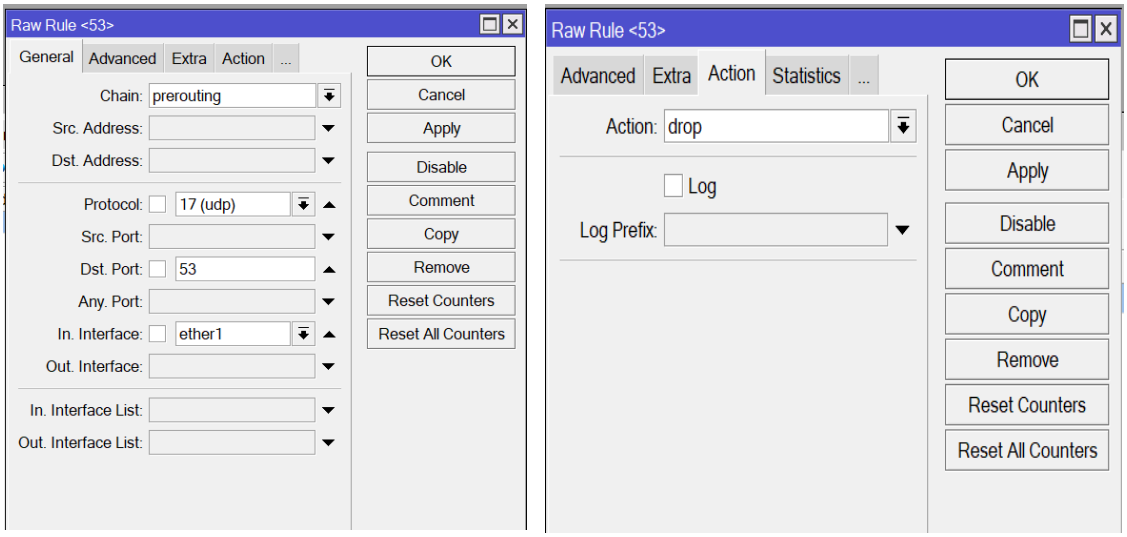
melalui menu Profile (Running) dan Resources. Pada bagian Profile terlihat bahwa penggunaan CPU mencapai 100% dengan beban terbesar berasal dari layanan DNS sebesar 47,5%, diikuti oleh aktivitas networking sebesar 24%, serta firewall dan management masing-masing 6,5%. Sementara itu, komponen lain seperti ethernet, queuing, dan logging hanya menggunakan sumber daya kecil, bahkan beberapa layanan seperti winbox dan wireless tidak menunjukkan aktivitas. Kondisi ini mengindikasikan bahwa layanan DNS sedang terbebani sangat tinggi, kemungkinan akibat banyaknya permintaan atau serangan berbasis UDP *Packet loss* yang ditujukan ke server DNS.

Pada bagian Resources ditampilkan informasi umum perangkat, di mana router sudah berjalan selama 1 jam 3 menit 39 detik dengan total memori 256 MB dan sisa memori bebas 228,4 MB. Prosesor yang digunakan adalah AMD dengan satu inti CPU berfrekuensi 3293 MHz, namun seluruh kapasitasnya digunakan penuh (CPU load 100%). Dari sisi penyimpanan, router memiliki total kapasitas 2000,4 MB dengan ruang bebas 1910,2 MB serta tidak ditemukan adanya bad block.

Secara keseluruhan, kondisi ini menggambarkan bahwa Router Mikrotik sedang mengalami beban kerja berat yang mayoritas berasal dari proses DNS. Hal tersebut dapat menjadi indikasi adanya serangan terhadap layanan DNS atau tingginya trafik yang masuk, sehingga mendukung pentingnya penerapan mekanisme keamanan pada router untuk menjaga stabilitas jaringan.

Konfigurasi Firewall Filter

Untuk melalukan perlindungan dari serangan UDP pada DNS Mikrotik maka dilakukan konfigurasi pada menu IP lalu pilih firewall dan menu RAW sehingga di dapatkan konfigurasi sebagai berikut:



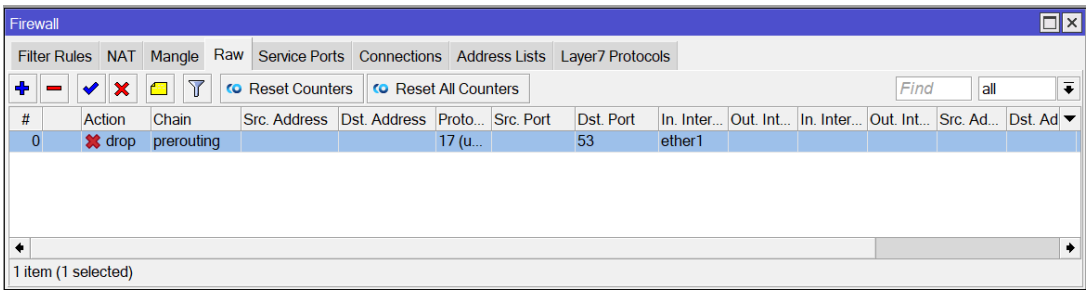
Gambar 4. Konfigurasi RAW untuk DNS

Gambar tersebut menunjukkan tampilan konfigurasi Raw Rule pada Router Mikrotik yang digunakan untuk menyaring paket data pada tahap awal sebelum diproses lebih lanjut oleh sistem. Pada konfigurasi tersebut, chain yang digunakan adalah prerouting, artinya aturan ini akan bekerja saat paket pertama kali masuk ke router sebelum diarahkan ke proses lain. Protokol yang difilter adalah UDP (protocol 17) dengan tujuan port 53, yaitu port standar layanan DNS. Dengan demikian, aturan ini berfungsi untuk memantau dan mengendalikan trafik UDP yang mengarah ke layanan DNS.

Selain itu, pada bagian In. Interface dipilih ether1, yang biasanya merupakan interface utama yang terhubung ke internet. Hal ini berarti semua paket UDP menuju port 53 yang

masuk melalui jalur internet akan difilter sesuai aturan ini. Bagian penting lain terdapat pada tab Action (tidak terlihat pada gambar), di mana administrator dapat menentukan tindakan terhadap paket, misalnya drop untuk memblokir trafik mencurigakan atau accept jika dianggap valid.

Konfigurasi ini umumnya digunakan untuk mencegah serangan seperti UDP *Packet loss* terhadap DNS, yang berpotensi membebani CPU router dan menurunkan kinerja jaringan. Dengan adanya raw rule ini, paket berbahaya dapat langsung dibuang sebelum mencapai proses lain di router, sehingga lebih efisien dalam mengurangi beban dan meningkatkan ketahanan layanan jaringan.



Gambar 5. Settingan filter firewall

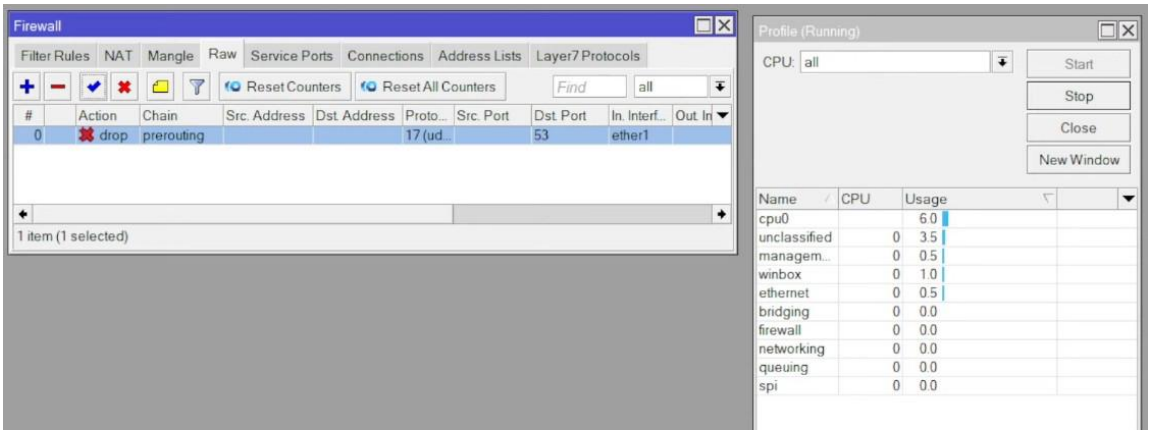
Gambar tersebut memperlihatkan konfigurasi pada menu Firewall – Raw di Router Mikrotik. Aturan yang ditampilkan menunjukkan bahwa semua paket dengan protokol UDP (protocol 17) yang menuju ke port 53 akan diproses melalui chain prerouting dan kemudian dikenai aksi drop. Aturan ini diterapkan pada interface ether1, yang umumnya merupakan interface utama yang terhubung langsung ke internet. Dengan demikian, setiap paket UDP yang mengarah ke layanan DNS melalui port 53 dari jalur internet akan langsung dibuang sebelum diproses lebih lanjut oleh router.

Konfigurasi ini dibuat untuk mengantisipasi dan meminimalisir serangan UDP *Packet loss* terhadap DNS, di mana serangan tersebut dapat membebani CPU dan mengganggu ketersediaan layanan jaringan. Dengan menempatkan aturan pada chain prerouting, paket berbahaya dapat dihentikan lebih awal sehingga tidak sampai memengaruhi proses lain dalam sistem. Secara keseluruhan, gambar ini menunjukkan salah satu implementasi mekanisme keamanan pada Router Mikrotik yang efektif untuk melindungi layanan DNS dari potensi serangan berbasis UDP.

Pengujian Penerapan Firewall

Pada tahap ini dilakukan pengujian setelah penerapan aturan firewall pada Router Mikrotik dengan tujuan untuk mengetahui efektivitas mekanisme keamanan dalam menghadapi serangan UDP yang ditujukan ke layanan DNS. Sebagaimana dijelaskan sebelumnya, serangan UDP *Packet loss* pada port 53 berpotensi membebani CPU dan menurunkan kinerja jaringan secara signifikan. Oleh karena itu, firewall dikonfigurasi dengan aturan drop pada trafik UDP port 53 yang masuk melalui interface ether1, sehingga paket berbahaya dapat dibuang lebih awal sebelum diproses lebih lanjut oleh sistem.

Pengujian ini dimaksudkan untuk membandingkan kondisi jaringan setelah penerapan firewall dengan kondisi sebelumnya saat router menerima serangan tanpa perlindungan. Fokus utama pengamatan meliputi penggunaan CPU, stabilitas layanan DNS, serta ketersediaan jaringan. Dengan cara ini dapat diperoleh gambaran nyata sejauh mana konfigurasi firewall mampu mengurangi dampak serangan, menjaga kestabilan sistem, dan meningkatkan performa router.



Gambar 6. Serangan dengan kemanan DNS

Gambar tersebut memperlihatkan hasil penerapan aturan firewall pada Router Mikrotik untuk melindungi layanan DNS dari serangan berbasis UDP. Pada sisi kiri, tampak konfigurasi firewall di tab Raw, di mana sebuah aturan telah ditetapkan dengan aksi drop terhadap semua paket dengan protokol UDP (17) yang menuju ke port 53 melalui interface ether1. Aturan ini ditempatkan pada chain prerouting, sehingga paket berbahaya dapat langsung dibuang sebelum memasuki proses lebih lanjut di router.

Di sisi kanan, terlihat tampilan Profile (Running) yang menunjukkan penggunaan CPU setelah aturan firewall dijalankan. Data memperlihatkan bahwa beban CPU kini sangat rendah, yaitu hanya 6%, dengan rincian penggunaan oleh beberapa layanan seperti unclassified 3,5%, winbox 1%, serta ethernet dan wireless masing-masing 0,5%. Tidak ada penggunaan signifikan dari layanan DNS ataupun networking seperti yang terlihat pada kondisi sebelumnya.

Hal ini menunjukkan bahwa aturan firewall berhasil mengurangi beban CPU secara drastis dengan cara memblokir trafik UDP yang masuk ke port DNS. Dengan demikian, konfigurasi tersebut terbukti efektif dalam mencegah serangan UDP *Packet loss* yang dapat membebani sistem, sekaligus menjaga stabilitas performa Router Mikrotik dan jaringan secara keseluruhan.

KESIMPULAN DAN SARAN

Berdasarkan hasil pengujian yang telah dilakukan, dapat disimpulkan bahwa penerapan aturan firewall pada Router Mikrotik terbukti efektif dalam memitigasi serangan UDP yang ditujukan ke layanan DNS. Sebelum konfigurasi diterapkan, CPU router menunjukkan beban kerja yang sangat tinggi hingga mencapai 100%, dengan penggunaan terbesar berasal dari layanan DNS. Namun setelah aturan firewall berupa *drop* paket UDP port 53 diimplementasikan pada interface ether1, penggunaan CPU menurun drastis hingga berada pada tingkat normal sekitar 6%. Hal ini menunjukkan bahwa mekanisme keamanan mampu mengurangi dampak serangan UDP *Packet loss* secara signifikan, menjaga kestabilan performa router, serta memastikan layanan DNS tetap tersedia dan dapat digunakan dengan baik oleh pengguna jaringan.

Untuk meningkatkan efektivitas pengamanan jaringan, disarankan agar konfigurasi firewall tidak hanya difokuskan pada serangan UDP terhadap DNS, tetapi juga diperluas mencakup berbagai potensi serangan lain seperti TCP SYN *Packet loss*, ICMP *Packet loss*, maupun eksploitasi port terbuka. Selain itu, administrator jaringan perlu melakukan pemantauan rutin terhadap kinerja router menggunakan fitur monitoring bawaan maupun aplikasi pihak ketiga agar deteksi dini terhadap anomali trafik dapat dilakukan dengan cepat. Penelitian selanjutnya

DAFTAR PUSTAKA

Academy, Cisco Networking. "Introduction Cyber Security." *www.netacad.com*. www.netacad.com.

Ayub, Muhammad, Andry Maulana, and Ahmad Fauzi. 2021. "Penerapan Firewall Dan Protokol IpSec/L2TP Sebagai Solusi Keamanan Akses Jaringan Publik." *Computer Science (CO-SCIENCE)* 1(2): 81–90.

Cervone, H. Frank. 2020. 7 portal: Libraries and the Academy *Computer Network Security and Cyber Ethics (Review)*.

Fauzi, Ahmad, Firmansyah Firmansyah, and Tommi Alfian Armawan Sandi. 2024. "Perancangan Keamanan Router Mikrotik Dari Serangan FTP Dan SSH Brute Force." *Jurnal Infortech* 6(1): 9–14.

Herlambang, ML. 2018. *Panduan Lengkap Menguasai Router Masa Depan Menggunakan Mikrotik Router OS*. 1st ed. Jakarta: Penerbit Andi.

Mugi Raharjo, Frengki Pernando, Ahmad Fauzi. 2019. "Perancangan Performansi Quality Of Service Dengan Metode Virtual Routing Redudancy Protocol (VRRP)." *Teknik komputer* V(1): 87–92. https://ejournal.bsi.ac.id/ejurnal/index.php/jtk/article/view/4555.

Nam H Nguyen. 2019. *Buku Panduan Keamanan Cyber Penting Di Bahasa Indonesia Essential Cyber Security Handbook In Indonesian*. Nam H Nguyen.

Prabantini, Dwi. 2022. *Panduan Lengkap Menguasai Router Masa Depan Menggunakan Mikrotik RouterOS*. Andi Yogyakarta.

Sharma, S, Sarabjit Singh, and Meenakshi Sharma. 2023. "Performance Analysis of Load Balancing Algorithms." *World Academy of Science, ...*: 269–72. http://masters.donntu.edu.ua/2010/fknt/babkin/library/article11.pdf.

Syawaludin, Haekal Alief, Ahmad Fauzi, and Susy Rosyida. 2020. "Perancangan Dan Implementasi Jaringan Tunnel Dengan Metode Pptp Pada Yayasan Pendidikan Bina Putera Indonesia." *Jurnal Edik Informatika* 7(1). http://dx.doi.org/10.22202/ei.2020.v7i1.4346.

Tambunan, Sarah Rouli. 2017. "Peran Internet Dalam Komunikasi Pemasaran." : 16–29.