eProceeding of TIK
E-ISSN: 2797-1724, P-ISSN: 3031-1454
Vol. 6 No. 1 2026 pp. 19-28

Implementasi Stateful Multilayer Inspection dan Proxy Eksternal untuk Mitigasi Serangan DoS pada Router MikroTik

Muhammad Farhan[1], Amri [2*], Novira Dwina[3]

[1,2,3]Jurusan Teknologi Informasi dan Komputer, Politeknik Negeri Lhokseumawe, Indonesia

*Penulis Korespondensi: amri@pnl.ac.id

This is an open access article under the CC BY-SA license.

Abstrak

Serangan DoS merupakan salah satu bentuk serangan jaringan yang membanjiri perangkat target dengan paket berlebihan sehingga mengakibatkan penurunan kinerja, gangguan layanan, bahkan kegagalan sistem. Router MikroTik dipilih karena banyak digunakan pada skala jaringan kecil hingga menengah, sementara *proxy eksternal* berbasis VPS digunakan untuk menyembunyikan identitas IP asli client. Metode penelitian yang digunakan adalah eksperimen dengan melakukan pengujian serangan DoS menggunakan variasi beban paket dari 100 hingga 10.000 paket, baik sebelum maupun sesudah penerapan metode. Efektivitas metode diukur melalui parameter CPU Load, *Free Memory*, serta kestabilan akses Winbox pada router MikroTik. Hasil penelitian menunjukkan bahwa penerapan *Stateful Multilayer Inspection* dapat menekan peningkatan CPU Load dan menjaga kestabilan *Free Memory* meskipun terjadi lonjakan serangan penggunaan *External Proxy* berhasil menggantikan IP asli client dengan IP VPS sehingga menambah lapisan keamanan jaringan.

Kata kunci: *Stateful Multilayer Inspection*, *Proxy Eksternal*, DoS, MikroTik, Keamanan Jaringan.

1. Pendahuluan

Dengan meningkatnya jumlah serangan siber, seperti *malware, phishing*, dan serangan DoS. Keamanan data dan sistem informasi menjadi sangat penting di era digital saat ini. *Firewall* dapat melindungi komputer dan jaringan pada berbagai ancaman, dari dalam maupun luar jika dapat diatur dengan benar[1]. Ada beberapa masalah yang perlu diperhatikan ketika menggunakan firewall, keterbatasan akses yang terlalu ketat pada *firewall* dapat mencegah pengguna mengakses aplikasi atau situs web yang penting untuk pekerjaan dan mengganggu produktivitas pengguna. Pengaturan yang tidak sesuai juga dapat menyebabkan celah keamanan dalam jaringan yang menyebabkan sistem rentan terhadap serangan. *Firewall* yang tidak dioptimalkan juga dapat memperlambat kinerja jaringan, karena proses penyaringan dan pemantauan lalu lintas yang intensif dapat memperlambat akses ke jaringan.

Dengan munculnya masalah ini, salah satu solusi yang dapat digunakan adalah penggunaan *Stateful Multilayer Inspection Firewall dan proxy external*. Metode ini menggabungkan keunggulan *firewall Packet Filtering*, NAT *Firewall, Circuit-Level Firewall*, dan *Proxy Firewall* dalam satu sistem. Jadi, tingkat keamanan metode ini dapat secara khusus melindungi infrastruktur komputer pada beberapa bagian jaringan, Metode ini dapat memahami setiap koneksi sehingga dapat memberikan perlindungan yang lebih baik terhadap serangan yang lebih kompleks seperti serangan DoS, DDoS *intrusi*, dan *malware*[2].

Dalam implementasinya pada mikrotik router digunakan sebagai pemantau koneksi yang di sedang berlangsung, sehingga dapat membeda antar paket yang berbahaya dan paket yang tidak berbahaya. di sisi lain, penggunaan *proxy external* semakin populer sebagai cara untuk memperkuat keamanan jaringan. *Proxy external* berfungsi sebagai perantara antara pengguna dan internet menyembunyikan alamat IP asli dan menyediakan lapisan tambahan untuk mengontrol akses dan *privasi*[3].

A. *Firewall*

Firewall adalah alat untuk menerapkan kebijakan keamanan. Namun, kebijakan keamanan dibuat dengan mempertimbangkan fasilitas yang disediakan dan konsekuensi keamanannya. Firewall juga dikenal sebagai benteng pertahanan lapisan pertama dalam jaringan komputer, membangun pembatasan antara jaringan lokal yang terkendali dengan jaringan luar seperti internet[4]. Untuk solusi mengatasi keamanan di dalam dunia internet baik itu

keamanan komputer maupun keamanan jaringan yang banyak dipenuhi dengan berbagai ancaman baik dari dalam maupun dari luar, pada penelitian ini firewall memberikan pengamanan pada jaringan untuk mengurangi serangan jaringan yang di tujukan pada server.

B. Keamanan Jaringan

Keamanan jaringan adalah sistem yang digunakan untuk mencegah ancaman dari luar, yang dapat merusak jaringan, serta ancaman yang berasal dari dalam, seperti ancaman pencurian data perusahaan. Sistem berhenti bekerja karena kata sandi diketahui oleh orang lain. Orang yang tidak berkepentingan dan segala jenis serangan serta upaya penyusupan atau pemindaian untuk memberikan perlindungan atau perlindungan pada jaringan wifi[5]. Sistem keamanan jaringan mengidentifikasi pengguna yang tidak memiliki akses ke jaringan untuk mencegah aktivitas yang tidak diinginkan. Dengan menghubungkan komputer satu sama lain melalui jaringan, baik kabel maupun nirkabel, orang lain dapat mengakses, mengubah, atau menghapus data dalam jaringan.

C. Mikrotik

MikroTik merupakan perangkat jaringan yang berasal dari Latvia dan pertama kali didirikan pada tahun 1996. Perusahaan ini mengembangkan perangkat lunak Router OS yang dapat diinstal pada komputer biasa agar berfungsi sebagai router dengan fitur-fitur canggih. Seiring perkembangannya, MikroTik juga merilis Router Board, yaitu perangkat keras khusus yang sudah terintegrasi dengan RouterOS sehingga lebih stabil dan mudah digunakan. MikroTik *Router* OS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk mengubah komputer menjadi *router* jaringan yang andal, termasuk berbagai fitur yang dibuat untuk jaringan IP dan jaringan nirkabel, cocok untuk digunakan oleh ISP dan penyedia hotspot[6]

D. Denial of Service (DoS)

Denial of Service (DoS) merupakan salah satu bentuk serangan jaringan yang bertujuan untuk membuat suatu layanan menjadi tidak dapat diakses oleh pengguna yang sah. Serangan ini biasanya dilakukan dengan cara membanjiri sistem target menggunakan lalu lintas palsu dalam jumlah besar sehingga sumber daya yang ada, seperti CPU, memori, dan bandwidth, terkuras habis. Akibatnya, perangkat yang diserang, baik server maupun router, tidak mampu merespons permintaan dari pengguna sebenarnya. Selain itu serangan DoS menyebabkan CPU *router* lumpuh, sehingga perlu penanganan tersendiri agar serangan CPU tidak membebani CPU. Dimanfaatkan *cookies* paket SYN dan *Firewall Raw* agar koneksi yang dideteksi sebagai serangan DoS berada pada kondisi *pre-routing* sehingga tidak membebani CPU[7].

E. Stateful Multilayer Inspection

Metode *Stateful Multilayer Inspection* adalah menggabungkan keunggulan dari NAT Firewall, *Packet Filtering*, *Circuit-Level* Firewall, dan *Proxy* Firewall dalam satu sistem. Jadi, tingkat keamanan metode ini secara khusus dapat melindungi infrastruktur komputer pada bagian tertentu dari jaringan[4]. Metode ini mampu melakukan analisis lebih mendalam hingga ke konteks koneksi dan lapisan aplikasi. Dengan demikian, setiap paket data tidak hanya diperiksa secara individual, tetapi juga berdasarkan status koneksi yang sedang berlangsung, seperti apakah koneksi tersebut valid, baru, atau mencurigakan.

F. External Proxy

External proxy merupakan sistem yang berfungsi untuk memproses permintaan menggunakan proxy dan bekerja sebagai perantara jaringan bagi pengguna dan server tujuan. Menggunakan proxy juga membuat aktivitas yang dilakukan menggunakan internet akan lebih aman karena informasi pengguna akan disamarkan dengan bantuan proxy tersebut. External proxy adalah suatu layanan jaringan yang berfungsi sebagai perantara antara pengguna dengan server tujuan di internet. Dengan menggunakan proxy, setiap permintaan yang dilakukan client tidak dikirimkan secara langsung ke server, melainkan dialihkan terlebih dahulu ke proxy. Selanjutnya, proxy akan meneruskan permintaan tersebut ke server tujuan dan mengembalikan respons ke client. Mekanisme ini membuat alamat IP asli pengguna tidak terlihat oleh server tujuan, karena yang terbaca hanyalah alamat IP dari proxy[5].

G. Virtual Private Server (VPS)

Virtual Private Server (VPS) adalah teknologi virtualisasi dimana anda bisa memiliki sebuah *server virtual* yang *resource Central processing unit* (CPU), *Random-access memory* (RAM), dan *Storage*nya dialokasikan secara pasti tanpa harus memiliki *server* secara fisik. Teknologi ini memungkinkan pengguna untuk memiliki akses *root* dan meng *custom server* sesuai dengan kebutuhan pengguna[6]. Dalam pemanfaatan *Virtual Private Server* (VPS) kebutuhan untuk perangkat keras (hardware) dan perangkat lunak (software) tergantung dari berapa jumlah *Virtual Private Server* (VPS) yang akan di *Host* dan juga spesifikasi dari *Virtual Private Server* (VPS) yang diinginkan.

2. Metode

2.1 Metode dan Variabel Penelitian

Pada penelitian ini menggunakan beberapa metode dalam penyusunan skripsi yaitu:

1. Studi Literatur
   Pada tahap ini dilakukan pengumpulan referensi berupa buku, jurnal, dan penelitian terdahulu yang berkaitan dengan keamanan jaringan, firewall dan *proxy*.
2. Perancangan Sistem
   Menyusun rancangan topologi jaringan, penentuan perangkat keras dan perangkat lunak yang digunakan, serta skenario serangan yang akan diuji.
3. Implementasi
   Melakukan konfigurasi firewall Stateful Multilayer Inspection pada MikroTik dan menghubungkannya dengan proxy eksternal berbasis VPS.
4. Pengujian dan kesimpulan
   Setelah implementasi selesai maka akan dilakukan pengujian pada sistem keamanan jaringan mikrotik dan hasil pengujian apakah desain sistem yang dirancang sesuai dengan tujuan yang ingin dicapai peneliti serta membuat kesimpulan untuk dapat menjadi rekomendasi pengembangan di masa depan.

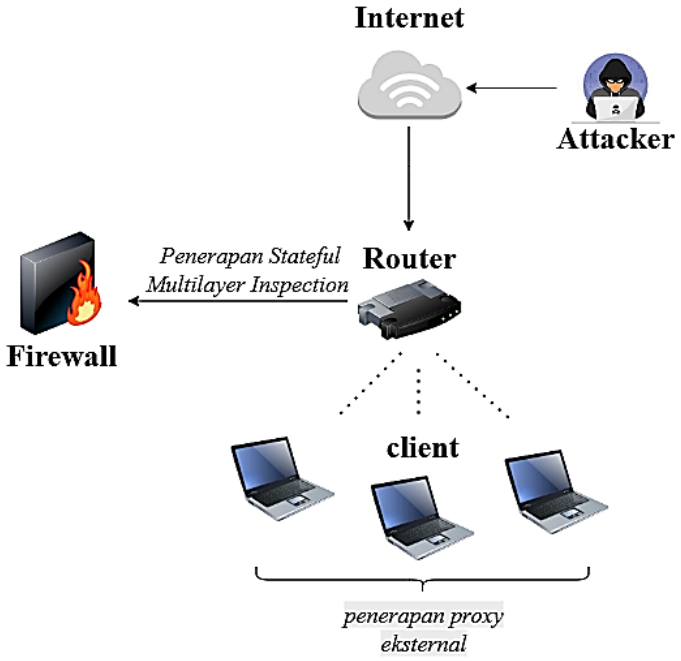
2.2 Data dan Pengumpulan Data

Data primer dan sekunder digunakan dalam penelitian ini. Data primer diperoleh melalui observasi langsung di lokasi penelitian, sedangkan data sekunder diperoleh dengan membaca dan mempelajari literatur terkait, seperti jurnal, buku, dan penelitian sebelumnya. Semua sumber referensi dipilih berdasarkan relevansinya dengan penelitian ini. Beberapa metode pengumpulan data telah disebutkan diantaranya:

1. Studi Pustaka Pengumpulan data dilakukan dengan membaca dan mempelajari literatur yang relevan dengan topik penelitian. Sumber-sumber ini dapat termasuk buku, artikel, jurnal, dan sumber lainnya.
2. Observasi Proses di mana penulis melihat langsung objek yang akan diteliti untuk mengetahui keadaan sebenarnya.

2.3 Rancangan Sistem

Dalam penelitian ini, implementasi terhadap sistem yang nantinya akan diterapkan dapat berjalan tanpa ganguan dan kendala yang signifikan, oleh karna itu. Agar penelitian ini dilaksanakan secara lebih sistematis dan jelas, dibutuhkan sebuah perancangan sistem, perancangan awal sistem yang nantinya akan diimplementasikan dalam penelitian ini dapat dilihat pada gambar 1.



Gambar 1. Rancangan Sistem

Berdasarkan Gambar 1, terdapat beberapa komponen utama yang saling terhubung sebagai berikut.

1.Layanan internet berfungsi sebagai jalur komunikasi yang menghubungkan penyerang eksternal (attacker) dengan router. Kanal ini juga menjadi jalur uji ketika host attacker mengirimkan trafik berlebih (DoS) menuju alamat yang dilindungi.

2.Router MikroTik berperan sebagai pengatur lalu lintas dan titik kontrol keamanan utama. Router MikroTik menjadi perangkat inti dalam penelitian ini. Fungsinya adalah menerapkan Stateful Multilayer Inspection Firewall untuk memantau status koneksi, melakukan filtering paket serta memblokir trafik mencurigakan. Stateful Multilayer Inspection pada filter rules untuk mendeteksi serta membatasi koneksi

berisiko ketika terjadi serangan DoS, tanpa mengganggu trafik normal. Dengan peran ganda tersebut, MikroTik memudahkan observasi langsung terhadap CPU load dan kestabilan Winbox sebelum dan sesudah penerapan metode.

3.Proxy Eksternal VPS berbasis Ubuntu Server menjalankan Squid Proxy sebagai perantara permintaan client ke internet. Tujuan utamanya ialah menyembunyikan IP publik asli jaringan lokal dan menggantinya dengan IP VPS, sehingga meningkatkan privasi dan menambah lapisan kontrol akses.

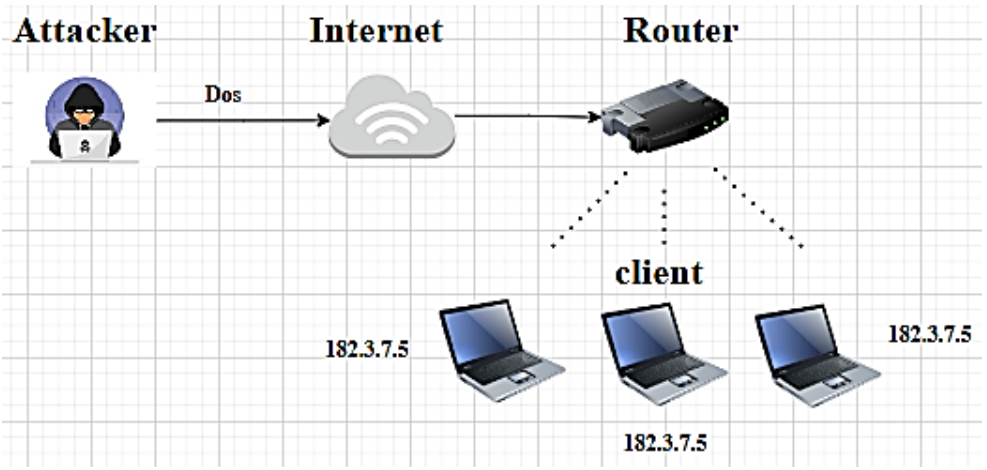
4.Attacker berperan untuk melakukan serangan DoS menggunakan tools seperti K6. Trafik serangan diarahkan ke target yang ditentukan sehingga efeknya dapat diukur baik pada sisi resource

5.Terdapat beberapa perangkat client yang terhubung ke router MikroTik. Pada sisi client ini juga diterapkan proxy eksternal yang diarahkan menuju VPS, sehingga alamat IP asli dari jaringan internal tidak terbaca oleh server tujuan.

6.Stateful Multilayer Inspection pada router untuk mendeteksi serta membatasi koneksi berisiko ketika terjadi serangan DoS, tanpa mengganggu trafik normal. Dengan peran ganda tersebut, MikroTik memudahkan observasi langsung terhadap CPU load dan kestabilan Winbox sebelum dan sesudah penerapan metode.

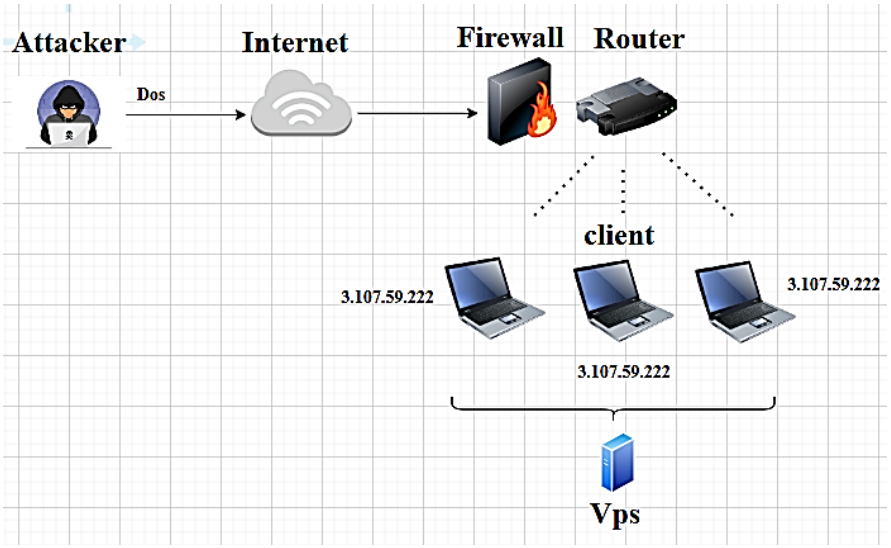
2.4 Teknik Pengujian

Dalam penelitian ini, pengujian dilakukan untuk mengetahui seberapa efektif metode Stateful Multilayer Inspection Firewall dan Proxy Eksternal dalam menangani serangan DoS (Denial of Service) yang membanjiri router MikroTik dengan lalu lintas palsu secara terus menerus. Tujuan dari pengujian ini adalah untuk mengamati bagaimana sistem bertahan saat menerima serangan langsung terhadap jaringan, baik sebelum maupun sesudah metode keamanan diterapkan. Pada tahap awal, pengujian dilakukan tanpa menggunakan metode firewall dan proxy sebagaimana ditunjukkan pada gambar 2.



Gambar 2. Alur Sebelum Penerapan Metode

Pada gambar 2 dapat dilihat pengujian dilakukan tanpa menggunakan metode Stateful Multilayer Inspection Firewall dan proxy eksternal, sehingga seluruh lalu lintas masuk akan langsung diterima oleh router tanpa penyaringan apapun. Pada kondisi ini, penyerang akan mengirimkan paket sebanyak 10.000 secara bertahap untuk melihat seberapa cepat router mengalami gangguan atau tidak mampu menangani beban lalu lintas dan pada kondisi ini ip dari client pun masih belum terganti dengan ip dari proxy. Setelah itu, metode *Stateful Multilayer Inspection Firewall* dan *Proxy Eksternal* diterapkan. *Firewall* akan menyaring paket berdasarkan status koneksi dan mendeteksi koneksi yang mencurigakan untuk diblokir, sementara *proxy eksternal* akan menyembunyikan IP asli dan akan memberikan ip dari *proxy*. Sebagaimana ditunjukkan pada gambar 3.



Gambar 3. Alur Sesudah Penerapan Metode

Pada gambar 3 ditunjukkan alur sistem jaringan setelah penerapan metode *Stateful Multilayer Inspection Firewall dan proxy eksternal*. Pada kondisi ini, serangan DoS yang dikirimkan oleh attacker melewati jaringan internet menuju router. Namun sebelum masuk ke router, paket terlebih dahulu diperiksa oleh *firewall*. *Firewall* ini melakukan inspeksi pola trafik sehingga mampu memblokir koneksi berbahaya yang dikirimkan secara berulang, sementara koneksi normal tetap diteruskan. Di sisi client, setiap permintaan akses internet tidak langsung menggunakan alamat IP publik jaringan internal, melainkan diarahkan menuju VPS yang menjalankan layanan *Squid Proxy*. Dengan mekanisme ini, alamat IP asli client digantikan oleh alamat IP VPS. Hal ini memastikan bahwa identitas jaringan internal tetap terlindungi karena yang terdeteksi oleh server tujuan maupun pihak luar adalah IP VPS, bukan IP asli *client*. Dengan adanya *Stateful Multilayer Inspection Firewall dan proxy eksternal*, router tidak hanya mampu menahan beban serangan DoS dengan menurunkan jumlah koneksi yang masuk dan menjaga stabilitas Winbox, tetapi juga meningkatkan aspek privasi jaringan dengan menyembunyikan alamat IP publik client.

3. Hasil dan Pembahasan

Penelitian ini dilakukan untuk menguji efektivitas metode *Stateful Multilayer Inspection dan External Proxy* dalam mencegah dan mengurangi dampak dari serangan *denial of service* pada *router*.

3.1. Hasil Penelitian

pengujian yang dilakukan berdasarkan dua skenario yaitu sebelum dan sesudah penerapan metode Stateful Multilayer Inspection dan External Proxy pada router dijelaskan pada berikut ini.

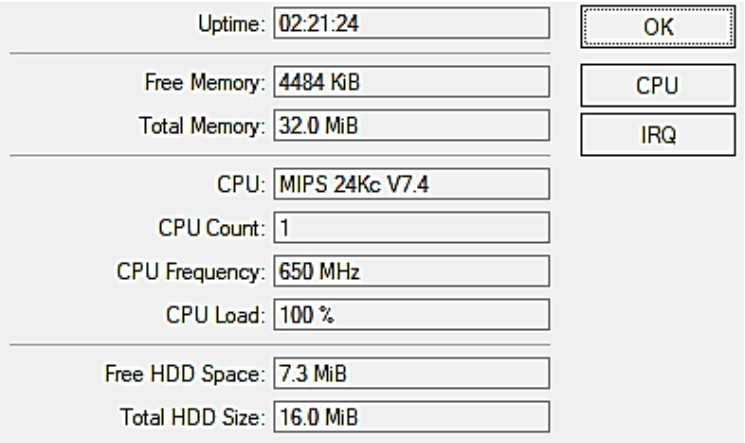
3.1.1 Pengujian Denial of Service *(Dos) ke Router*

Pada pengujian ini, serangan denial of service menggunakan tools K6 untuk membuka banyak koneksi ke router target. Adapun hasil yang didapatkan pada pengujian dengan 10.000 paket dapat dilihat pada gambar 4 berikut.

	Src. Address	Dst. Address	Proto...	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C	192.168.10.253:33164	192.168.10.1:8291	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	60 B/0 B
C	192.168.10.253:33224	192.168.10.1:8291	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	60 B/0 B
C	192.168.10.253:33226	192.168.10.1:8291	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	60 B/0 B
C	192.168.10.253:33280	192.168.10.1:8291	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	60 B/0 B
C	192.168.10.253:33322	192.168.10.1:8291	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	60 B/0 B
C	192.168.10.253:33330	192.168.10.1:8291	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	60 B/0 B
C	192.168.10.253:33356	192.168.10.1:8291	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	60 B/0 B
C	192.168.10.253:33406	192.168.10.1:8291	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	60 B/0 B
C	192.168.10.253:33440	192.168.10.1:8291	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	60 B/0 B
C	192.168.10.253:33448	192.168.10.1:8291	6 (tcp)		00:00:03	syn sent	480 bps/0 bps	300 B/0 B
C	192.168.10.253:33456	192.168.10.1:8291	6 (tcp)		00:00:04	syn sent	480 bps/0 bps	120 B/0 B
C	192.168.10.253:33462	192.168.10.1:8291	6 (tcp)		00:00:04	syn sent	0 bps/0 bps	60 B/0 B
C	192.168.10.253:33472	192.168.10.1:8291	6 (tcp)		00:00:04	syn sent	480 bps/0 bps	360 B/0 B
C	192.168.10.253:33474	192.168.10.1:8291	6 (tcp)		00:00:04	syn sent	480 bps/0 bps	300 B/0 B
C	192.168.10.253:33484	192.168.10.1:8291	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	60 B/0 B
C	192.168.10.253:33490	192.168.10.1:8291	6 (tcp)		00:00:03	syn sent	480 bps/0 bps	360 B/0 B
C	192.168.10.253:33506	192.168.10.1:8291	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	60 B/0 B
C	192.168.10.253:33508	192.168.10.1:8291	6 (tcp)		00:00:03	syn sent	480 bps/0 bps	300 B/0 B
C	192.168.10.253:33526	192.168.10.1:8291	6 (tcp)		00:00:03	syn sent	480 bps/0 bps	300 B/0 B
C	192.168.10.253:33542	192.168.10.1:8291	6 (tcp)		00:00:03	syn sent	480 bps/0 bps	360 B/0 B
C	192.168.10.253:33546	192.168.10.1:8291	6 (tcp)		00:00:04	syn sent	480 bps/0 bps	300 B/0 B

Gambar 4. Log Jaringan Masuk dengan Pengujian 10.000 Paket

Gambar 4 menampilkan log koneksi yang masuk pada router MikroTik. Kondisi ini menunjukkan bahwa serangan dengan 10.000 paket. Berdasarkan hasil pengujian diatas dengan 10.000 paket dapat dilihat pada gambar 5 berikut.



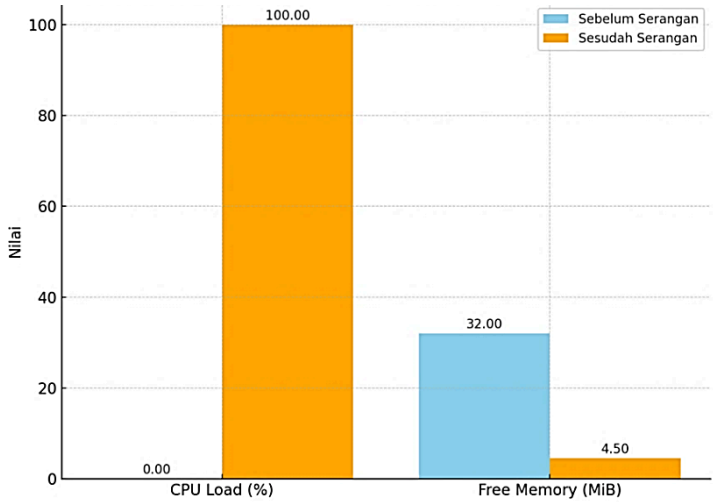
Gambar 5. Tampilan Menu *Resources pada router*

Gambar 5 memperlihatkan bahwa CPU Load mencapai 100% Lonjakan ini menandakan bahwa prosesor router sudah tidak memiliki kapasitas tambahan untuk menangani trafik lebih lanjut. Pada saat yang sama, *Free Memory* menurun hingga tersisa 4.5 MiB dari kapasitas awal 32.0 MiB. Hal ini menunjukkan bahwa hampir seluruh memori telah dialokasikan untuk menampung koneksi palsu. Rincian hasil pengujian 10.000 paket dapat dilihat pada Tabel 1 berikut.

Tabel 1. Pengujian dengan 10.000 Paket

Parameter	**Sebelum Serangan**	**Sesudah Serangan**
CPU *Load*	0%	100%
Free Memory	32.0 Mib	4.5 Mib

Tabel 1 memperlihatkan kondisi router MikroTik sebelum dan sesudah menerima serangan dengan 10.000 paket. Hasil pengujian menunjukkan bahwa CPU Load melonjak dari 0% menjadi 100%. Kondisi ini menegaskan bahwa prosesor router telah bekerja pada kapasitas penuh dan tidak mampu lagi menangani tambahan beban. Hal ini menimbulkan risiko sangat tinggi terhadap kestabilan jaringan, karena perangkat berada pada titik jenuh. Selain itu, *Free Memory* juga mengalami penurunan signifikan dari 32.0 MiB menjadi 4.5 MiB. Penurunan ini menunjukkan bahwa hampir seluruh memori telah dialokasikan untuk menampung koneksi palsu akibat serangan. Jika kondisi ini terus berlangsung, router berisiko tidak mampu lagi melayani koneksi baru dan dapat menyebabkan terhentinya layanan jaringan secara keseluruhan. Hasil pengukuran dari kedua kondisi tersebut dapat dilihat pada gambar 6 berikut.



Gambar 6. Perbandingan *Router* Sebelum dan Sesudah *Dos*

Gambar 6 memperlihatkan perbandingan kondisi router MikroTik sebelum dan sesudah dilakukan serangan DoS dengan 10.000 paket. Terlihat bahwa CPU Load melonjak drastis hingga mencapai 100%, sementara Free Memory menurun signifikan dari 32,0 MiB menjadi hanya 4,5 MiB. Kondisi ini memperlihatkan bahwa router sudah tidak lagi dalam posisi aman, melainkan berada pada titik jenuh. Walaupun router masih dapat diakses, kestabilan sistem sangat rapuh, dan setiap peningkatan jumlah serangan berpotensi besar menyebabkan router gagal beroperasi.

3.1.2 Pengujian dengan Mengunjungi Situs tanpa External Proxy

Hasil yang didapatkan pada pengujian sebelum menggunakan *external proxy* dapat dilihat pada gambar 7 berikut.

Gambar 7 IP Sebelum Menggunakan *Proxy External*

Gambar 7 menunjukkan bahwa saat melakukan pengujian sebelum metode *external proxy* diterapkan, ip publik yang terdeteksi oleh situs pengecekan ip adalah 182.3.7.5. Ini merupakan ip asli dari jaringan client yang digunakan untuk mengakses internet. Kondisi ini menunjukkan bahwa identitas asli pengguna masih terbuka dan dapat dikenali dengan mudah oleh server tujuan atau pihak ketiga. Hal ini menimbulkan potensi risiko keamanan dan privasi, karena ip address dapat dilacak dan diekspos.

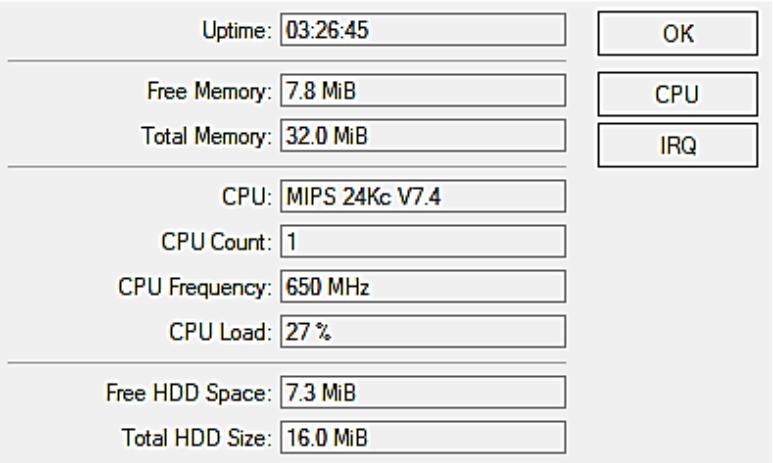
3.1.3 *Pengujian* Denial of Service *(Dos) setelah penerapan* Stateful Multilayer Inspection

Pada pengujian ini Router akan diserang menggunakan DoS namun telah diterapkan metode *Stateful Multilayer Inspection. Adapun hasil yang didapatkan pada pengujian setelah menerapkan Stateful Multilayer Inspection dengan 10.000 paket dapat dilihat pada gambar 8 berikut.*

	Src. Address	Dst. Address	Proto...	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C	192.168.1.1	224.0.0.1	2 (ig...		00:09:49		0 bps/0 bps	27.5 KiB/0 B
SAC	192.168.10.253:47342	192.168.10.1:8291	6 (tcp)		00:00:04	fin wait	0 bps/0 bps	1341 B/60 B
SAC	192.168.10.253:47344	192.168.10.1:8291	6 (tcp)		00:00:04	fin wait	0 bps/0 bps	1497 B/60 B
SAC	192.168.10.253:47346	192.168.10.1:8291	6 (tcp)		00:00:04	fin wait	0 bps/0 bps	1341 B/60 B
SAC	192.168.10.253:47348	192.168.10.1:8291	6 (tcp)		00:00:04	fin wait	0 bps/0 bps	1341 B/60 B
SAC	192.168.10.253:47382	192.168.10.1:8291	6 (tcp)		00:00:04	fin wait	0 bps/0 bps	1549 B/60 B
SAC	192.168.10.253:47396	192.168.10.1:8291	6 (tcp)		00:00:04	fin wait	0 bps/0 bps	1549 B/60 B
SAC	192.168.10.253:47404	192.168.10.1:8291	6 (tcp)		00:00:04	fin wait	0 bps/0 bps	1393 B/60 B
SAC	192.168.10.253:47408	192.168.10.1:8291	6 (tcp)		00:00:04	fin wait	0 bps/0 bps	1393 B/60 B
SAC	192.168.10.253:47420	192.168.10.1:8291	6 (tcp)		00:00:04	fin wait	0 bps/0 bps	1497 B/60 B
SAC	192.168.10.253:47422	192.168.10.1:8291	6 (tcp)		00:00:04	fin wait	0 bps/0 bps	1549 B/60 B
SACs	192.168.10.254:49715	31.13.95.60:5222	6 (tcp)		23:59:56	established	0 bps/0 bps	25.3 KiB/31.2 KiB
SACs	192.168.10.254:50402	216.239.38.120:443	17 (u...		00:02:38		0 bps/0 bps	8.6 KiB/7.7 KiB

Gambar 8 Log setelah penerapan Metode dengan Pengujian 10.000 Paket

Gambar 8 menampilkan aktivitas log koneksi pada router MikroTik ketika dilakukan serangan DoS dengan beban 10.000 paket. Terlihat bahwa IP 192.168.10.253 sebagai sumber serangan berulang kali mencoba melakukan koneksi ke port router target. Namun, berkat penerapan metode Stateful Multilayer Inspection, mayoritas permintaan dari attacker tidak berhasil mendominasi log seperti pada pengujian tanpa metode. Koneksi berbahaya tersebut dapat terfilter secara efektif, sehingga serangan tidak sepenuhnya membebani sumber daya router. Berdasarkan hasil pengujian diatas dengan 10.000 paket dapat dilihat pada gambar 9.



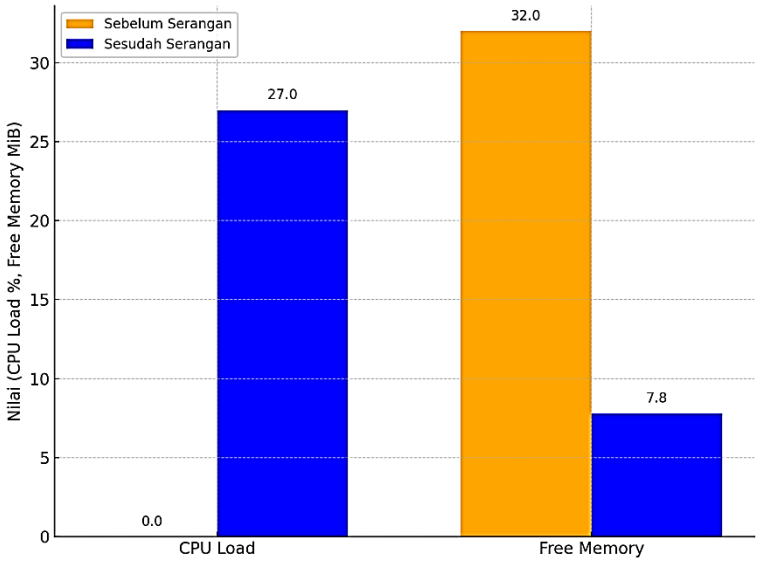
Gambar 9. Tampilan Menu *Resources pada router*

Gambar 9 memperlihatkan kondisi *resources* router saat menerima serangan 10.000 paket setelah metode diterapkan. CPU Load tercatat 27%, jauh lebih rendah jika dibandingkan kondisi tanpa metode, di mana CPU langsung mencapai 100%. Sementara itu, *Free Memory* masih stabil di angka 7.8 MiB, berbeda dengan kondisi tanpa metode yang mengalami penurunan signifikan. Rincian hasil pengujian 10.000 paket dapat dilihat pada Tabel 2 berikut.

Tabel 2 Pengujian dengan 10.000 Paket

Parameter	**Sebelum Serangan**	**Sesudah Serangan**
CPU *Load*	0%	27%
Free Memory	32.0 Mib	7.8 Mib

Tabel 4.24 menunjukkan perbandingan kondisi router sebelum dan sesudah menerima serangan DoS dengan 10.000 paket setelah metode *Stateful Multilayer Inspection* diterapkan. CPU Load hanya meningkat hingga 27%, jauh lebih terkendali dibandingkan dengan kondisi tanpa metode yang mencapai 100%. Selain itu, *Free Memory* berada di 7.8 MiB, menandakan bahwa serangan tidak menghabiskan seluruh kapasitas memori router. Hasil pengukuran dari kedua kondisi tersebut dapat dilihat pada gambar 10 berikut.

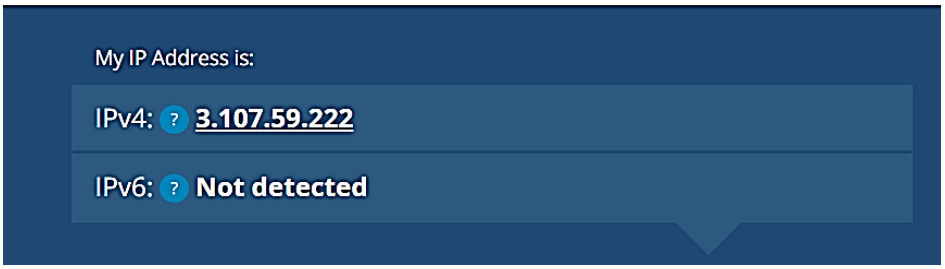


Gambar 10 Perbandingan router sebelum dan sesudah serangan 10.000 paket

Gambar 10 memperlihatkan perbandingan parameter CPU Load dan *Free Memory* sebelum dan sesudah serangan 10.000 paket setelah metode diterapkan. Terlihat bahwa CPU Load memang mengalami peningkatan, namun tetap dalam batas wajar. *Free Memory* juga relatif stabil. Hal ini membuktikan bahwa metode *Stateful Multilayer Inspection* mampu menahan dampak serangan DoS skala besar, sehingga router tetap dapat beroperasi dengan stabil.

3.1.4 Pengujian dengan Mengunjungi Situs Menggunakan External Proxy

Adapun hasil yang didapatkan pada pengujian sesudah menggunakan *external proxy* dapat dilihat pada gambar 11 berikut.



Gambar 11. IP Setelah Menggunakan *Proxy External proxy*

Gambar 11 menunjukkan bahwa setelah metode external proxy diterapkan, IP publik yang terdeteksi oleh situs pengecekan IP adalah 3.107.59.222. IP tersebut merupakan milik VPS tempat proxy diinstal, bukan lagi IP asli dari jaringan client. Kondisi ini membuktikan bahwa identitas asli pengguna telah berhasil disembunyikan, sehingga server tujuan atau pihak ketiga tidak dapat mengetahui IP sebenarnya dari client lokal.

4. Kesimpulan

Berdasarkan hasil dari pengujian yang dilakukan pada Router sebelum dan sesudah pengaplikasian *stateful multi layer* dan *external proxy* pada router maka dapat diambil kesimpulan sebagai berikut:

1. *Metode Stateful Multilayer Inspection* terbukti mampu mengurangi dampak serangan DoS terhadap router MikroTik. Hal ini terlihat dari hasil pengujian, di mana tanpa metode CPU Load dapat melonjak hingga lebih dari 70–100% dan memori cepat terkuras, sedangkan setelah metode diterapkan CPU Load jauh lebih rendah stabil di bawah 30% dan penggunaan memori lebih terkontrol.
2. *External Proxy* berbasis VPS (Squid Proxy) berhasil menyembunyikan IP publik asli client dengan menggantinya menggunakan IP VPS. Dengan demikian, selain meningkatkan privasi pengguna, metode ini juga menambah lapisan keamanan jaringan terhadap pengintaian dari pihak ketiga.

REFERENSI

[1] Adhi Purwaningrum, F., Purwanto, A., Agus Darmadi, E., Tri Mitra Karya Mandiri Blok Semper Jomin Baru,

P., & -Karawang, C. (2018). *Optimalisasi Jaringan Menggunakan Firewall*. *2*(3), 17–23.

[2] Pribadi, Z. A. (2022). *Analisis dan Implementasi Firewall dengan Metode Stateful Multilayer Inspection Pada Mikrotik Router OS*. *1*, 1–9.

[3] Royal, S. (2023). *3 1,2,3*. *3*(3). EXTERNAL PROXY MENGGUNAKAN ROUTER MIKROTIK DALAM OPTIMASI BANDWIDTH LABORATORIUM. 175–180

[4] Kamila Wilujeng, Cahya, and Apriade Voutama. 2024. "Implementasi Firewall Filter Rules Sebagai Filtering Content Pada Jaringan Komputer Menggunakan Mikrotik." JATI (Jurnal Mahasiswa Teknik Informatika) 8(3):2680–85. doi: 10.36040/jati.v8i3.9530.

[5] Arini, A., Arsalan, M. L., & Sukmana, H. T. (2024). Keamanan jaringan Wi-Fi terhadap serangan packet sniffing menggunakan firewall rule (studi kasus: PT Akurat.co). Cyber Security dan Forensik Digital, 6(2), 30–38. https://doi.org/10.14421/csecurity.2023.6.2.4075

[6] Mulyanto, Y., & Algi Fari, A. (2022). Analisis Keamanan Login Router Mikrotik Dari Serangan *Bruteforce* Menggunakan Metode Penetration Testing (Studi Kasus: SMK NEGERI 2 SUMBAWA). *Jurnal Informatika, Teknologi dan Sains*, *4*(3), 145–155. https://doi.org/10.51401/jinteks.v4i3.1897

[7] Alhamri, R. Z., & Heriadi, A. (2022). Pemanfaatan API client berbasis Python untuk konfigurasi IPS pada router Mikrotik. Jurnal Teknik Ilmu dan Aplikasi, 3(2), 195–205.

[8] Sefriansyah, S., Khairil, K., & Sapri, S. (2022). Penerapan Metode Stateful Multilayer Inspection Untuk Keamanan Jaringan Pada Smk N 1 Kota Bengkulu. *Djtechno: Jurnal Teknologi Informasi*, *3*(2), 234–243. https://doi.org/10.46576/djtechno.v3i2.2730

[9] Hakim, A. L. (2018). *Konfigurasi MikroTik untuk External Proxy*. Lukmanlab. https://www.lukmanlab.com/konfigurasi-mikrotik-untuk-external-proxy/

[10] Syani, M. (2020). Implementasi intrusion detection system (IDS) menggunakan Suricata pada Linux Debian 9 berbasis cloud virtual private *server*s (VPS). *Jurnal Teknik Komputer dan Informatika*, 1(1), 13–20.

[11] Djayali, A. D., Muzammil, M., & Samad, A. (2021). Implementasi aplikasi meeting online pada virtual private *server* di masa pandemi. *Simkom*, 6(1), 23–33. https://doi.org/10.51717/simkom.v6i1.52