Click here and write your Article Category

Mengamankan Perangkat Jaringan dari Serangan DDoS Menggunakan Fitur Firewall-RAW di Router MikroTik

Syaiful Bahri[1], Doni El Rezen Purba[2]
[1] *Program Studi Pendidikan Teknik Informatika, STKIP Al Maksum, Stabat, Indonesia*
[2]*Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas, Jalan Setia Budi No.479 F, Tanjung Sari Medan, Indonesia.*

ARTICLE INFORMATION

Received :February 2024
Revised: Februari 2024
Available online: April 2024

KEYWORDS

DDoS attacks, Firewall-RAW, MikroTik Router

CORRESPONDENCE

Phone: 081263823278
E-mail: syaifulbahri@stkipalmaksum.ac.id

A B S T R A C T

DDoS (Denial of Service) attacks are a serious threat in network security that can cause services to become unavailable due to unusually high traffic volumes. This research aims to secure network devices from DDoS attacks by using the Firewall-RAW feature on the MikroTik Router. In tests carried out using MikroTik RouterOS, DDoS attacks were effectively prevented by using firewall rules that were set to reject packets that exceeded a predetermined threshold. However, the test results also show that the CPU Load of the device is still affected by DDoS attacks, although to a limited extent. This emphasizes that protecting against DDoS attacks is not an easy task, but the use of firewall rules can help reduce the system load due to these attacks. The recommended next step is to ensure the router device has sufficient CPU resources to anticipate the impact of a DDoS attack that may occur in the future. However, it is important to remember that firewall rules are only an additional protective measure and do not guarantee absolute protection from DDoS attacks. Therefore, there is a need for a comprehensive security strategy and appropriate infrastructure improvements to reduce the risk of greater DDoS attacks.

PENDAHULUAN

Dalam zaman ini, konektivitas internet telah menjadi kebutuhan pokok dalam kehidupan sehari-hari, memainkan peran penting dalam berbagai aktivitas. Oleh karena itu, menjaga keamanan jaringan komputer yang terhubung ke internet menjadi suatu hal yang sangat krusial. Ancaman dari para peretas dapat berdampak serius, mulai dari pencurian data hingga merusak integritas jaringan komputer tersebut [1]. Dalam era di mana teknologi informasi dan komunikasi memegang peranan penting dalam hampir setiap aspek kehidupan, keamanan jaringan menjadi salah satu aspek yang tak terelakkan untuk dipertimbangkan dengan serius [2]. Serangan siber, khususnya Serangan Denial of Service (DDoS), telah menjadi ancaman yang semakin meresahkan bagi organisasi, perusahaan, dan bahkan individu yang mengandalkan konektivitas jaringan untuk menjalankan operasi sehari-hari mereka sehingga diperlukan sistem yang dapat mendeteksi serangan ini dengan baik [3]. Jenis serangan yang sering digunakan oleh hackeradalah (Denial of Services) DoS yang bersifat mengirimkan sejumlah paket melalui internet protocol (IP) secara terus menerus yang dapat mengganggu organisasi dari jaringan komputer dengan tujuanmelumpuhkan server [4]. Serangan DDoS mengintensifkan volume lalu lintas ke suatu situs web atau layanan jaringan, yang pada gilirannya dapat mengakibatkan penurunan kinerja, pemadaman sementara, atau bahkan kegagalan total dalam menyediakan layanan [5]. Target pertama attacker sebelum menyerang sistem yaitu mematikan terlebih dahulu kinerja router [6]. Jika mengabaikan keamanan tersebut maka tidak menutup kemungkinan orang yang tidak bertanggung jawab mengambil data-data penting atau bahkan menyerang sistem yang dapat membuat sistem menjadi down atau dikenal dengan serangan Distributed Denial of Service (DDoS) [7]. Jika terjadi kendala pada router maka secara langsung akan berdampak besar terhadap performa jaringan [8]. Adapun Router Mikrotik merupakan router yang mencangkup Operating System (OS) berbasis Mikrotik dengan berbagai fitur handal didalamnya, salah satunya adalah fitur Firewall untuk menghadapi ancaman serangan siber [9]. Dalam upaya melindungi infrastruktur jaringan dari serangan DDoS, banyak organisasi dan penyedia layanan internet mengandalkan teknologi firewall sebagai lapisan pertahanan utama mereka. Salah satu solusi yang sering digunakan dalam memitigasi serangan DDoS adalah penggunaan fitur Firewall-RAW yang tersedia dalam router jaringan, khususnya router MikroTik. Fitur ini memungkinkan administrator jaringan untuk menangkap dan mengolah paket lalu lintas jaringan sebelum melewati proses normal routing dan firewalling. Firewall raw juga dapat melakukan blokir seperti halnya dengan firewall filter rules, namun dengan konsumsi resource yang lebih hemat. Hal ini dikarenakan firewall raw memungkinkan melakukan connection tracking, sebelum memilih antara melewatkan atau memblokir packet [10].

Penelitian ini bertujuan untuk mendalami implementasi dan efektivitas fitur Firewall-RAW dalam mengamankan perangkat jaringan dari serangan DDoS pada Router MikroTik. Melalui analisis yang teliti, penelitian ini akan mengeksplorasi berbagai aspek teknis, strategis, dan praktis yang terlibat dalam penggunaan fitur ini sebagai alat pertahanan terhadap serangan DDoS yang semakin canggih dan kompleks. Penting untuk mencatat bahwa keberhasilan mitigasi serangan DDoS tidak hanya bergantung pada teknologi semata, tetapi juga pada pemahaman yang mendalam tentang karakteristik serangan tersebut, pola lalu lintas yang tidak biasa, dan tindakan pencegahan yang tepat waktu. Oleh karena itu, penelitian ini tidak hanya akan fokus pada kemampuan teknis dari fitur Firewall-RAW, tetapi juga akan mempertimbangkan aspek-aspek strategis dan praktis dalam penerapannya. Dengan melihat latar belakang ini, penting untuk menyoroti pentingnya penelitian ini dalam konteks keamanan cyber saat ini. Dengan meningkatnya frekuensi dan kompleksitas serangan DDoS, diperlukan pendekatan yang holistik dan terpadu untuk melindungi infrastruktur

jaringan dari ancaman ini. Penelitian ini diharapkan dapat memberikan wawasan baru, pemahaman yang lebih dalam, dan

rekomendasi praktis bagi para profesional keamanan jaringan, administrator sistem, dan para pengambil keputusan dalam menghadapi ancaman serangan DDoS yang semakin berkembang.

Pada tahap awal, akan dilakukan tinjauan literatur yang komprehensif untuk mengidentifikasi perkembangan terbaru dalam teknologi dan praktik mitigasi serangan DDoS. Tinjauan ini akan mencakup berbagai pendekatan yang telah diusulkan dan diimplementasikan dalam melindungi jaringan dari serangan DDoS, termasuk teknik-teknik yang terkait dengan penggunaan firewall sebagai alat pertahanan. Setelah memahami kerangka teoritis dan praktis yang mendasari mitigasi serangan DDoS, penelitian akan melanjutkan dengan fokus pada fitur Firewall-RAW yang tersedia dalam Router MikroTik. Router MikroTik dipilih sebagai subjek penelitian karena popularitasnya dan kemampuannya yang telah terbukti dalam mengelola dan melindungi jaringan yang kompleks. Selanjutnya, metodologi penelitian akan diuraikan dengan detail untuk menjelaskan pendekatan yang akan digunakan dalam menguji efektivitas fitur Firewall-RAW dalam mengatasi serangan DDoS. Metodologi ini akan mencakup langkah-langkah eksperimental, parameter yang diukur, dan analisis data yang akan dilakukan untuk mengevaluasi performa dan efektivitas fitur tersebut. Selain itu, penelitian ini juga akan mempertimbangkan tantangan dan kendala yang mungkin dihadapi dalam mengimplementasikan dan memelihara fitur Firewall-RAW. Hal ini termasuk pertimbangan terkait konfigurasi, manajemen lalu lintas, dan pemecahan masalah dalam situasi serangan nyata. Terakhir, penelitian ini akan menyimpulkan dengan merangkum temuan utama, implikasi praktis, dan saran untuk penelitian lebih lanjut dalam bidang mitigasi serangan DDoS menggunakan fitur Firewall-RAW di Router MikroTik. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi yang berharga bagi pemahaman dan praktik keamanan jaringan dalam menghadapi ancaman serangan siber yang terus berkembang.

METODE PENELITIAN

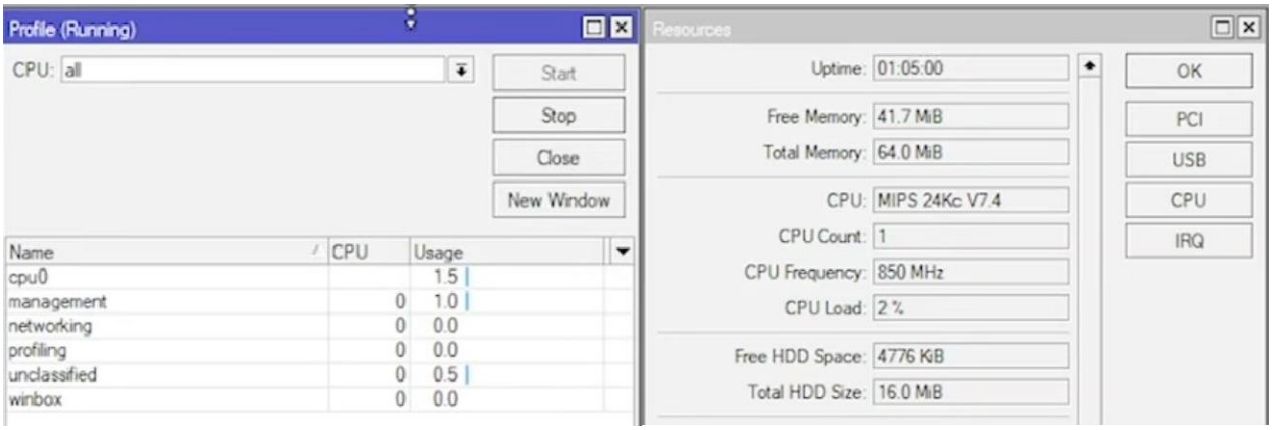
Metode penelitian yang akan digunakan dalam penelitian ini akan melibatkan serangkaian langkah yang sistematis untuk menguji efektivitas fitur Firewall-RAW dalam mengamankan perangkat jaringan dari serangan DDoS menggunakan Router MikroTik. Berikut adalah gambaran rinci tentang metodologi yang akan diterapkan. Langkah pertama dalam metodologi ini akan melibatkan tinjauan literatur yang komprehensif tentang topik keamanan jaringan, serangan DDoS, dan fitur Firewall-RAW pada Router MikroTik. Studi literatur ini akan membantu dalam memahami kerangka teoritis yang mendasari penelitian ini, serta memperoleh wawasan tentang praktik terbaik yang telah diusulkan dalam mitigasi serangan DDoS. Berdasarkan temuan dari studi literatur, berbagai skenario serangan DDoS akan dikembangkan untuk menguji efektivitas fitur Firewall-RAW. Skenario-serangan ini akan mencakup variasi dalam jenis serangan, intensitas lalu lintas, dan pola perilaku yang berbeda dari penyerang. Lingkungan uji coba akan disusun dengan menggunakan perangkat keras dan perangkat lunak yang diperlukan untuk mensimulasikan serangan DDoS dan menerapkan fitur Firewall-RAW. Ini akan melibatkan konfigurasi Router MikroTik dengan setup jaringan yang sesuai untuk memfasilitasi pengujian.

Pengujian akan dilakukan dengan mengirimkan lalu lintas sesuai dengan skenario serangan yang telah dikembangkan ke jaringan yang disiapkan. Selama pengujian, data akan dikumpulkan secara real-time untuk memantau respons sistem terhadap serangan dan penggunaan fitur Firewall-RAW. Selama pengujian, data akan dikumpulkan tentang kinerja jaringan, tingkat keberhasilan mitigasi serangan, dan dampak penggunaan fitur Firewall-RAW terhadap kinerja jaringan secara keseluruhan. Data ini akan dianalisis dengan menggunakan metode statistik dan teknik analisis yang sesuai. Hasil dari pengujian akan dievaluasi untuk mengevaluasi efektivitas fitur Firewall-RAW dalam mengatasi serangan DDoS. Ini akan melibatkan analisis terhadap parameter-parameter kinerja seperti tingkat drop paket, latensi, dan throughput jaringan, serta tingkat keberhasilan dalam mengidentifikasi dan memblokir serangan. Temuan dari pengujian akan divalidasi dan dibahas dalam konteks temuan literatur yang ada. Implikasi praktis dari temuan ini akan dipertimbangkan, termasuk saran untuk penggunaan optimal fitur Firewall-RAW dalam mengamankan perangkat jaringan dari serangan DDoS. Metode penelitian ini akan memungkinkan peneliti untuk melakukan evaluasi yang komprehensif terhadap efektivitas fitur Firewall-RAW dalam mengamankan perangkat jaringan dari serangan DDoS. Dengan pendekatan yang sistematis dan terstruktur ini, diharapkan penelitian ini dapat memberikan wawasan yang berharga bagi praktik keamanan jaringan dan pengembangan teknologi firewall yang lebih efektif di masa depan.

HASIL DAN PEMBAHASAN

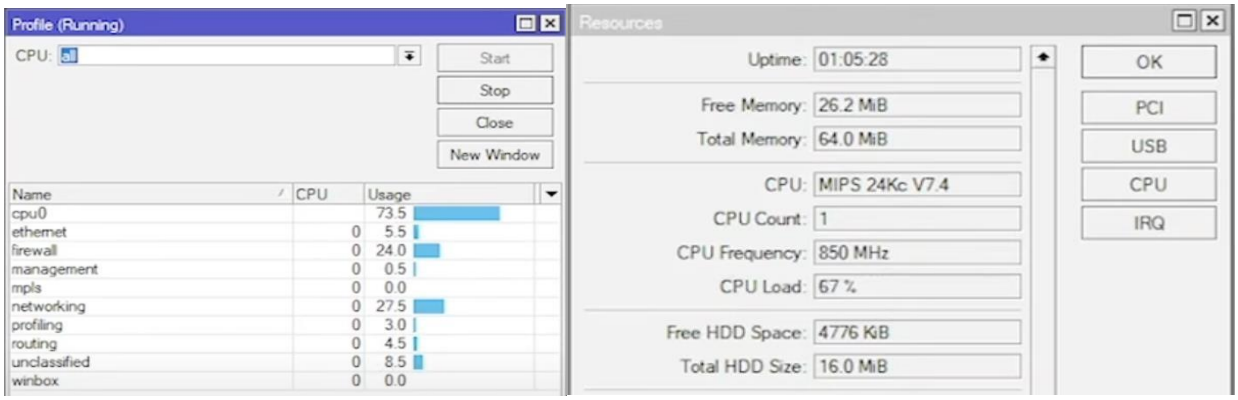
1. Identifikasi Masalah

Pada penelitian ini yang pertama dilakukan yaitu melihat kondisi terkini dari system router yang digunakan. Pada penelitian ini menggunakan MikrotikOS sebagai router yang berfungsi untuk mencegah dari serangan DDOS. Serangan ini bekerja dengan mengirim banyak paket data secara bersamaan sehingga akan membuat sistem menjadi kebanjiran paket yang masuk dan akhirnya membuat sistem atau server menjadi down, maka dari itu yang harus dilakukan yaitu mencegah paket data tersebut masuk kedalam sistem, sehingga serangan DDoS tidak berhasil membanjiri paket data ke sistem ataupun server yang diserang. Hal pertama yang akan dilihat dari pengujian ini aadalah Profile pada router. Pada bagian ini akan dilihat apakah kondisi router dalam keadaan normal atau tidak normal. Pada kondisi normal, CPU load tidak memiliki nilai yang sangat tinggi, namun apabila nilai CPU load sangat tinggi, maka bosa dipastikan router terkena serangan DDoS. Berikut tampilan router yang normal dan yang terkena serangan DDoS:



Gambar 1. Tampilan Router yang Normal

Pada tampilan tersebut dapat dilihat bahwa router dalam keadaan normal. Hal itu dibuktikan dengan nilai CPU Load tidak mengalami lonjakan yang sangat besar. Namun jika nilainya besar, maka router terkena serangan DDoS seperti gambar berikut ini:



Gambar 2. Tampilan Router yang Terkena Serangan DDOS

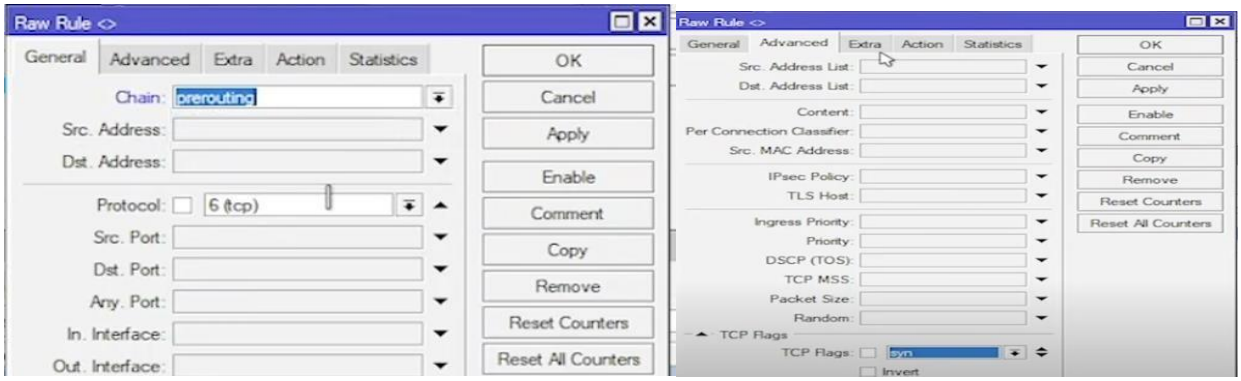
Tampak pada gambar diatas router terkena serangan DDoS ygn dibuktikan dari nilai CPU load yang meningkat drastis dalam waktu yang singkat. Router yang terkena serangan DDoS tersebut dapat diminimalisir dengan dilakukannya beberapa pengaturan yang mampu menghalangi masuknya serangan DDoS tersebut.

2. Demonstrasi

Pada langkah ini dilakukan penanganan pencegahan serangan DDoS melalui fitur IP Firewall RAW. Sebenarnya tindakan yang bisa dilakukan yaitu Firewall RAW dan Filter, namun yang akan digunakan pada penelitian ini yaitu Firewall RAW, karena apabila terdapat traffic TCP Syn Attack nantinya langsung dilakukan Drop dan tidak masuk lagi ke Connection Tracking dan jika menggunakan Firewall Filter maka nanti trafficnya masih masuk ke router dan tercatat di Connection Tracking. Namun jika menggunakan Firewall RAW, sebelum masuk ke connection tracking maka masuk ke local process nanti akan langsung di Drop oleh router. Langkah yang kita lakukan yaitu:

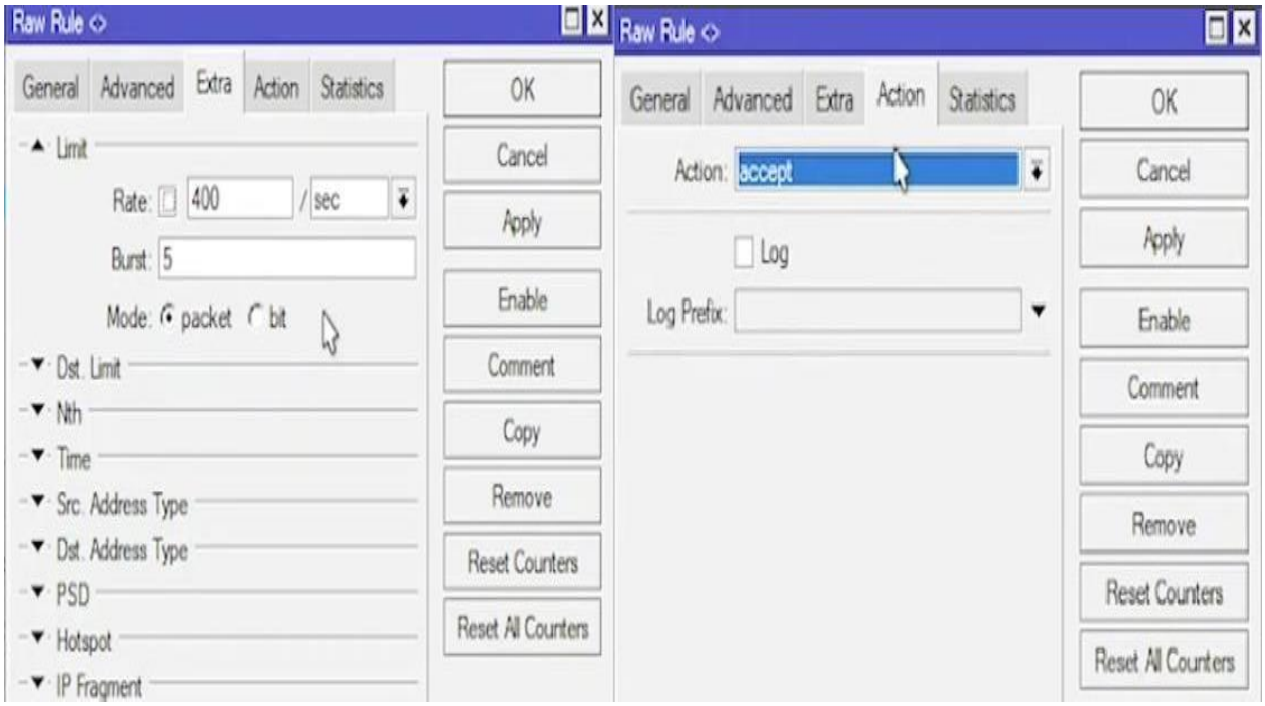
a. Masuk ke menu IP Firewall > Raw

Pada bagian ini tambahkan new rule, lalu pada bagian General terdapat pilihan Chain : prerouting dan pilihan protocol pilih 6(tcp). Kemudian masuk ke menu Advanced dan cari pilihan TCP Flags yang letaknya ada dibawah. Lalu isi TCP flags dengan syn.



Gambar 3. Konfigurasi Mencegah Serangan DDoS

Berikutnya masuk ke menu sebelahnya yaitu Extra, dan pilih Limit dengan isi Rate: 400 dan Burst 5. Pada pilihan ini berfungsu agar router nantinya akan mengizinkan TCP Syn lewat hanya sebatas 400 paket saja sesuai yang kita buat, apabila terjadi kiriman paket lebih dari 400 maka akan di drop. Hal inilah yang membentengi router dari serangan DDoS. Berikutnya yaitu pilih menu Action dan isi dengan pilihan accept. Kemudian klik apply.

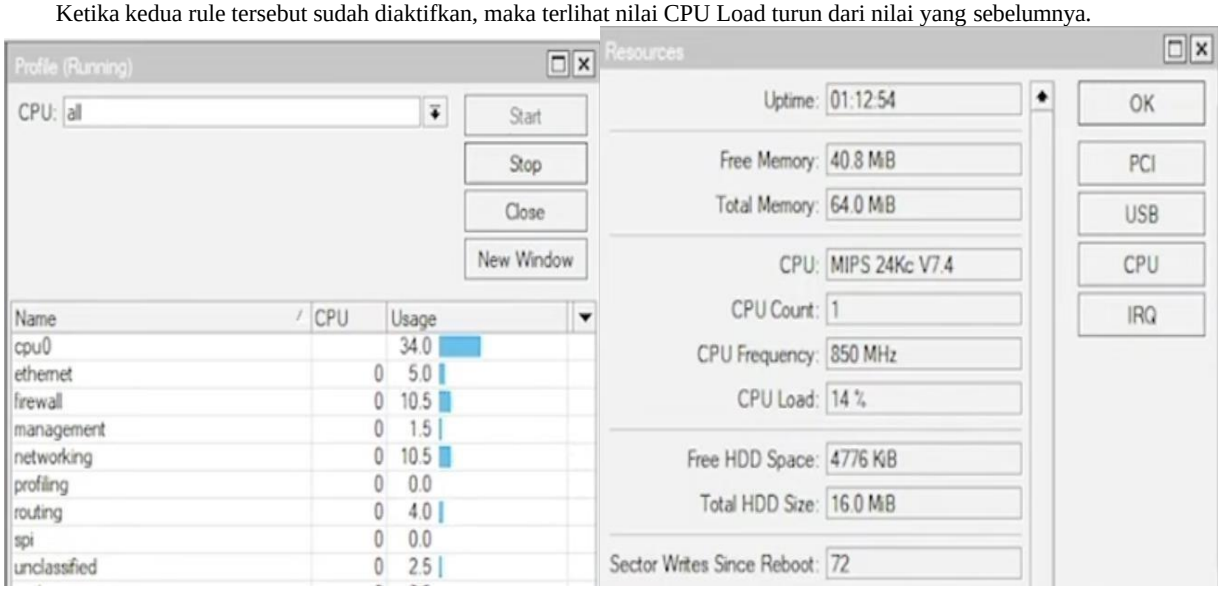


Gambar 4. Konfigurasi Mencegah Serangan DDoS (2)

Berikutnya yaitu membuat 1 rule lagi untuk paket drop. Caranya sama seperti yang sebelumnya yaitu di menu General pilih Chain : prerouting. Lalu di menu Advanced pilih TCP flags :syn. Lalu di menu Extra pilih Limit--> rate: 400. Dan yang terakhir inilah yang membedakan pengaturan keduanya. Pada rule drop ini, di menu Action pilih Drop. Hal ini berfungsi agar semua pengaturan pada rule 0 yang sudah dilakukan apabila selain dari yang sudah ditentukan pada rule 0 tersebut maka akan di drop.

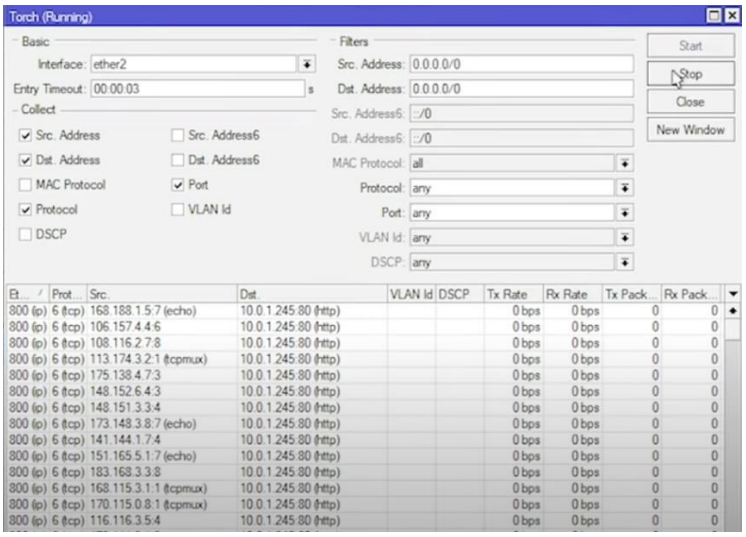
3. Pengujian Serangan DDoS

Ketika kedua rule tersebut sudah diaktifkan, maka terlihat nilai CPU Load turun dari nilai yang sebelumnya.



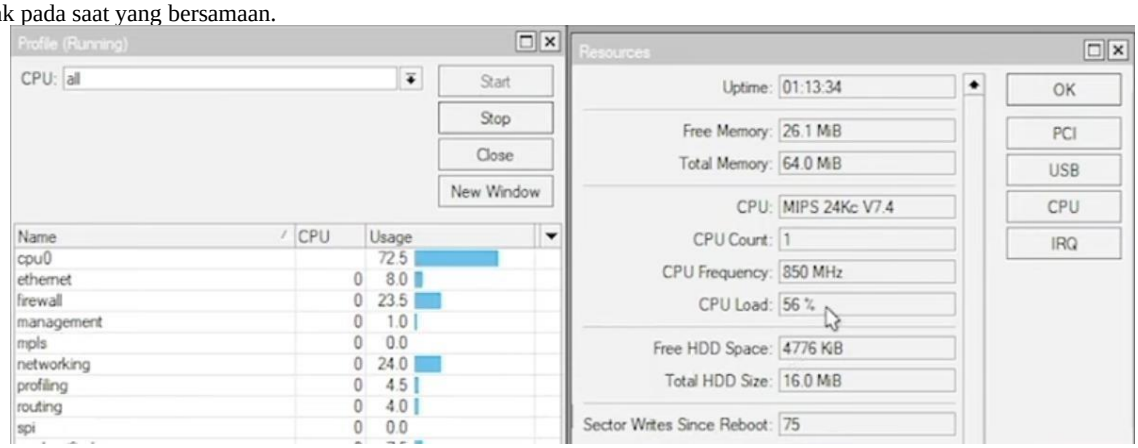
Gambar 5. CPU Load yang Kembali Normal

Apabila kita cek di tool Torch maka akan terlihat paket yang masuk masih tetap ada, namun masih bisa dikontrol oleh router sehingga serangan DDoS tidak berhasil masuk ke router.



Gambar 6. Melihat Paket Data yang Masuk Melalui Tool Torch

Dan apabila rule yang sudah dibuat tadi di disable, maka akan terlihat kembali peningkatan nilai pada CPU Load. Hal ini terjadi karena tidak ada yang membatasi jumlah paket masuk ke router, sehingga berapapun paket yang dikirimkan ke router maka router akan menerimanya dan besar kemungkinan router bisa mengalami down karena tidak sanggup menampung data yang sangat banyak pada saat yang bersamaan.



Gambar 7. Tampilan CPU Load yang Kembali Meningkat

KESIMPULAN

Serangan *DDoS* merupakan serangan yang sering terjadi agar perangkat target menjadi *down* karena tidak sanggup menerima paket data yang begitu banyak masuk pada saat yang bersamaan. Maka dari itu *router* perlu dibuatkan *rule* agar apabila ada paket data yang masuk melebihi jumlah yang sudah ditentukan maka paket tersebut akan di *drop* secara otomatis oleh *system*. Berdasarkan hasil pengujian yang dilakukan menggunakan *Mikrotik RouterOS*, serangan *DDoS* berhasil dicegah dengan baik, namun disini *CPU Load*-nya masih ada efek dari serangan walaupun tidak terlalu besar. Hal itu menunjukkan jika serangan *DDoS* tersebut memang tidak mudah untuk dicegah, namun salah satu cara yang bisa digunakan yaitu menerapkan *rule* seperti pengujian diatas. Namun *rule* pada penelitian ini hanya membantu agar perangkat tersebut tidak terlalu terbebani, bukan 100% mencegah dari serangan *DDoS*. Langkah selanjutnya yang harus kita lakukan yaitu memastikan perangkat *router* memiliki *resource CPU* yang cukup, sehingga apabila terjadi serangan maka efeknya tidak terlalu besar karena sudah diantisipasi dengan menggunakan *router* yang *resource*-nya besar.

REFERENCES

[1] A. Fadlil, I. Riadi, and S. Aji, “Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan,” Jurnal Ilmiah Teknik Elektro Komputer dan Informatika, vol. 3, no. 1, pp. 11–19, 2017

[2] Dwiyatno,S., Sari,A. P., Irawan, A., & Safig, S.(2019). Pendeteksi Serangan Ddos (Distributed Denialof Service) Menggunakan Honeypot di PT. Torini Jaya Abadi. JurnalSistem Informasi dan Informatika(SIMIKA), 2(2), 64-80. DOI: https://doi.org/10.47080/simika.v2i2.606.

[3] Winanto, C. A. (2016) “Deteksi serangan Denial of Service mengunakan Artificial Immune System,” Computer Engineering, 2(Faculty of Computer Science, Sriwijaya University), pp. 456–459.

[4] A. Fadlil and S. Aji, “DDoS Attacks Classification using Numeric Attribute-based Gaussian Naive Bayes,” IJACSA) International Journal of Advanced Computer Science and Applications, vol. 8, no. 8, 2017

[5] Liang,X.,& Znati, T. (2019). On The Performance Of Intelligent Techniques For Intensive And StealthyDDos Detection. Computer Networks, 164. DOI: https://doi.org/10.1016/j.comnet.2019.106906.
[6] Yudhana,A.,Riadi,I.,& Ridho, F. (2018). DDoS Classification Using Neural Network and Naïve Bayes Methods for Network Forensics. International Journal of Advanced Computer Science and Applications(IJACSA),9(11), 177-183.DOI: http://dx.doi.org/10.14569/IJACSA.2018.091125
[7] W. Meng, J. Lopez, S. Xu, C. Su, and R. Lu, "IEEE Access Special Section Editorial: Internet-of-Things Attacks and Defenses: Recent Advances and Challenges," IEEE Access, vol. 9, pp. 108846–108850, 2021, doi: 10.1109/ACCESS.2021.3101889
[8] R. Pambudi dan M. A. Muslim, "Implementasi Policy Base Routing dan Failover Menggunakan Router Mikrotik untuk Membagi Jalur Akses Internet di FMIPA Unnes," J.Teknol. dan Sist. Komput., vol. 5, no. 2, hal. 57, 2017, doi: 10.14710/jtsiskom.5.2.2017.57-61.
[9] A. Muzakir dan M. Ulfa, "Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan jaringan," Simetris J. Tek. Mesin, Elektro dan Ilmu Komput., vol. 10, no. 1, hal. 15–20, 2019, doi: 10.24176/simet.v10i1.2646
[10] B. Jaya, Y. Yunus, dan S. Sumijan, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS)," J. Sistim Inf. dan Teknol., vol. 2, no. 4, hal. 5–9, 2020, doi: 10.37034/jsisfotek.v2i4.81