VOL. 17. NO. 1 AGUSTUS 2022
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri

INTI NUSA MANDIRI
DOI: https://doi.org/10.33480/inti.v17i1.3401

OPTIMALISASI KEAMANAN *WIDE AREA NETWORK* MENGGUNAKAN *RAW FIREWALL* MIKROTIK PADA PT. PERMATA GRAHA NUSANTARA

Mohammad Nadhir[1]; Ummu Radiyah[2*]; Muhammad Qomarudin[3]

Informatika[1,2,3]
Universitas Nusa Mandiri[1,2,3]
https://nusamandiri.ac.id[1,2,3]
dhirmohammad@gmail.com[1], ummu.urd@nusamandiri.ac.id[2],
muhammad.mqn@nusamandiri.ac.id[3]

Abstract— *The focus of this research is on optimizing network security by implementing the firewall method with raw firewall techniques on Mikrotik network devices. Firewalls limit who has the right to access the internet in the network, and who must be allowed and not allowed to pass through, this is commonly called filtering. Firewall on the network, can monitor the activity of a network. Raw Firewall is a network security technique that does not require large resources in its use. In this study, two test scenarios were carried out: (i) the first test was to perform a ping attack before the implementation of the raw firewall technique, namely using filter rules, and (ii) the second test carried out a ping attack again after the implementation of the raw firewall. The results obtained from the study show that the use of cpu resources with filter rules techniques is an average of 41% and cpu resources after the implementation of raw firewall is an average of 2% during an attack. The implementation of a raw firewall against ping attacks has succeeded in reducing the load on the cpu, so that in this condition the performance of the device is not disturbed.*

Keywords*: Mikrotik. Raw Firewall, Network Security*

Abstrak—Fokus penelitian ini adalah optimalisasi keamanan jaringan dengan implementasi metode firewall dengan teknik raw firewall pada perangkat jaringan mikrotik. Firewall membatasi siapa saja yang berhak mengakses suatu internet dalam jaringan, dan siapa saja yang harus diizinkan dan tidak diizinkan untuk lewat, hal ini biasa disebut dengan filtering. Firewall pada jaringan, dapat memantau aktifitas suatu jaringan. Raw Firewall adalah teknik keamanan jaringan yang dalam penggunaannya tidak membutuhkan resource yang besar. Pada penelitian ini dilakukan dua skenario pengujian: (i) pengujian pertama dengan melakukan serangan ping attack sebelum implementasi teknik raw firewall, yaitu menggunakan filter rules, dan (ii) pengujian kedua melakukan serangan ping attack kembali setelah implementasi firewall raw. Hasil yang diperoleh dari penelitian memperlihatkan bahwa penggunaan resource cpu dengan teknik filter rules rata-rata sebesar 41% dan resource cpu setelah implementasi raw firewall rata-rata sebesar 2% saat terjadi serangan. Implementasi raw firewall terhadap ping attack berhasil menurunkan beban pada cpu, sehingga pada kondisi ini kinerja perangkat tidak terganggu.

Kata kunci: *Mikrotik, Raw Firewall, Keamanan Jaringan*

PENDAHULUAN

Keamanan jaringan merupakan salah satu hal terpenting dalam implementasi jaringan komputer. Tidak sedikit jaringan komputer yang mengalami masalah yang disebabkan oleh kelalaian pengelola jaringan dalam membangun sebuah jaringan komputer dikarenakan kelalaian tersebut sehingga dapat membuka peluang bagi para peretas (*hacker*) untuk meretas dan merusak jaringan yang dibangun tersebut dan untuk meminimalisir terjadinya penyalahgunaan jaringan oleh para *hacker*, maka perlu adanya peningkatan keamanan jaringan (Amarudin, 2018).

Router merupakan salah satu perangkat jaringan yang memungkinkan perangkat lain untuk terhubung ke dalam jaringan intranet maupun internet. Selain itu router juga dapat menyimpan

VOL. 17. NO. 1 AGUSTUS 2022
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri

identitas lalu lintas packet data yang melewatinya, beserta dengan perpindahannya(Ridho et al., 2017). Router sering difungsikan sebagai gateway bagi jaringan internal agar dapat terhubung ke jaringan lain atau internet. Oleh karena itu, jika terjadi kendala pada router maka secara langsung akan berdampak besar terhadap performa jaringan (Pambudi & Muslim, 2017).

Adapun *Router Mikrotik* merupakan *router* yang mencangkup *Operating System* (OS) berbasis *Mikrotik* dengan berbagai fitur handal di dalamnya, salah satunya adalah fitur *Firewall* untuk menghadapi ancaman serangan siber (Muzakir & Ulfa, 2019). Pada firewall router mikrotik, terdapat beberapa fitur yang dapat digunakan untuk mengamankan jaringan, diantaranya adalah Firewall Filter Rules dan Firewall Raw. Firewall filter rules dapat dimanfaatkan untuk memblokir aktifitas jaringan yang berpotensi membahayakan, seperti memblokir website tertentu, memblokir penggunaan aplikasi seperti Torrent, VPN, port scanning, hingga recursive DNS (Langobelen et al., 2019).

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap *hardware*, *software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan atau kegiatan suatu segmen pada jaringan lokal dengan jaringan luar yang bukan merupakan ruang lingkupnya (Anugrah & Rahmanto, 2018). PT. Permata Graha Nusantara ("PERMATA") merupakan anak perusahaan dari PT. Perusahaan Gas Negara Tbk ("PGN") yang bergerak dalam bidang *Facility Management, Asset Management, Entrepreneurial Real Estate* serta *Design and Build*. Dalam aktivitasnya Permata memiliki pengelolaan dokumen perusahaan seperti mengakses data pada *server*, mengirim dan menerima data antar ruangan satu dengan ruangan lain dan gedung satu dengan gedung lainnya hingga pertukaran data yang dilakukan dalam gedung yang berbeda lokasi.

Dalam proses pengelolaan dokumen maupun akses jaringan pada PT. Permata Graha Nusantara sudah dilakukan secara semestinya dan keamanan jaringan yang ada masih terbilang standar. Di era Revolusi Industri 4.0 yang dapat dikatakan canggih, peretasan data dapat dilakukan oleh banyak kalangan dengan berbagai cara dan sudah selayaknya keamanan jaringan harus lebih diperhatikan untuk melindungi sistem dari ancaman serangan yang semakin canggih dan beragam, terlebih lagi ketika jaringan sudah terhubung ke internet maka ancaman terhadap keamanan jaringan akan semakin meningkat, misalnya DDoS (*Distributed Denial of Service*) *attack* dan sebagainya, juga serangan *hacker*, virus, trojan yang semuanya merupakan ancaman yang tidak bisa diabaikan (Anugrah & Rahmanto, 2018).

Berdasarkan laporan terkait serangan Denial of Service (DoS) yang dirilis oleh Securelist dari Kaspersky pada Quarter 1 tahun 2021, rata-rata serangan DoS per hari mencapai 1500 serangan, dengan *traffic* tertinggi 800 GB per detik terjadi di sektor swasta, dan Amerika Serikat menjadi sumber serangan DoS terbesar (41,98%) dibanding dengan negara-negara lainnya (A. Gutnikov, O. Kupreev, 2021).

DoS menjadi salah satu jenis serangan siber teratas dan cukup banyak digunakan oleh *attacker* dengan tujuan untuk melumpuhkan targetnya. Serangan DoS menggunakan volume dan intensitas tertentu yang menyebabkan target menjadi kehabisan *resource* bahkan *down* ketika menangani permintaan layanan dari pengguna, sehingga membuat pengguna layanan yang sah kesulitan atau bahkan tidak dapat mengakses layanan (Fadlil et al., 2017). Seiring dengan perkembangannya, DoS memiliki beberapa jenis tipe serangan, diantaranya SYN-Flooding, SMURF Attack, TCP-Flooding, UDP-Flooding, ICMP-Flooding, DNS-Flooding (Aprilianto et al., 2017).

Berdasarkan permasalahan yang ada di PT. Permata Graha Nusantara bahwa sistem keamanan jaringan yang digunakan adalah metode *firewall filter rules* yang mana metode tersebut masih standar. *Firewall* didefinisikan sebagai sebuah komponen atau kumpulan komponen yang membatasi akses antara sebuah jaringan yang diproteksi dan internet, atau antara kumpulan-kumpulan jaringan lainnya. *Firewall* merupakan solusi untuk 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. Dengan suatu konfigurasi yang tepat pada *firewall* maka kemungkinan untuk mengamankan suatu data atau komputer pada jaringan menjadi jauh lebih aman (Adhi Purwaningrum, 2018). Metode tersebut secara penggunaannya membutuhkan daya yang cukup besar dalam pengoperasian CPU (*Central Processing Unit*).

Pada, bulan Februari tahun 2022 pernah terjadi beberapa kali serangan *ddos attack* terhadap *server* kantor sehingga berimbas pada kinerja perangkat yang melambat dan mengakibatkan *server* lumpuh serta menggangu aktivitas perkantoran. Serangan DoS (*Denial of Service*) yang mengimplementasi protokol TCP/IP dengan mengirimkan paket-paket *SYN request* ke dalam *port-port* pada router sasaran dengan maksud menyerap seluruh sumber daya yang ada pada server sehingga server menjadi terlalu sibuk dan tidak dapat mengontrol lalu lintas jaringan dengan baik. Bahkan dapat berakibat macetnya sistem

(*hang*) (Fakhmi, Muhammad; Gultom, 2021). Dengan adanya kekurangan tersebut maka PT. Permata Graha Nusantara memerlukan optimalisasi keamanan jaringan dengan menerapkan metode *Raw Firewall* berbasis Mikrotik, kemudian dengan penerapan metode *raw firewall* menghasilkan beberapa keuntungan diantaranya menghemat penggunaan sumber daya, hal ini dikarenakan *raw firewall* memungkinkan melakukan *connection tracking*, sebelum memilih antara melewatkan atau memblokir *packet* (Haris, 2022).

Pada penelitian sebelumnya, menunjukkan DoS dapat dideteksi dengan bantuan beberapa *tools*. Pada penelitian yang dilakukan oleh (Ridho et al., 2017), serangan DoS berhasil dideteksi dengan menggunakan *Intrusion Detection System (IDS)* berbasis Snort. Sedangkan pada penelitian yang dilakukan (Mardiyanto et al., 2016), (Dwiyatno et al., 2019), dengan menggunakan *tools* honeypot berbasis Honeyd, serangan DoS dapat dideteksi secara *real time* dengan memberikan peringatan berupa *log* yang berisikan informasi serangan yang sedang terjadi, serta dapat mensimulasikan atau menduplikasi target, sehingga dapat mengecoh *attacker*, dengan membuat seolah-olah target yang diserang adalah target yang asli.

Pada penelitian lainnya terkait serangan DoS terhadap router mikrotik, serangan DoS bertipe TCP *flooding* dengan perubahan data *size* diujikan terhadap router mikrotik. Hasil yang diperoleh adalah router mikrotik mengalami peningkatan konsumsi *resource*, yaitu di sisi daya listrik dan beban CPU, namun pada penelitian ini tidak memberikan solusi terkait perlindungan dari serangan DoS (Adrian & Isnianto, 2016).

BAHAN DAN METODE

Teknik pengumpulan data yang digunakan oleh penulis dalam melakukan pengumpulan data untuk membuat penelitian ini adalah:

a. Observasi

Pada tahap observasi dilakukan untuk mengetahui aktivitas yang ada di PT. Permata Graha Nusantara dengan mempelajari, mengamati kegiatan yang berlangsung di PT. Permata Graha Nusantara.

b. Wawancara

Melakukan wawancara dengan salah satu Staf IT yang bertanggung jawab pada jaringan komputer yang ada di PT. Permata Graha Nusantara untuk mendapatkan data maupun informasi mengenai kebutuhan jaringan.

c. Studi Pustaka

Melakukan pencarian terhadap teori-teori yang ada untuk menunjang penelitian berdasarkan pemaparan referensi jurnal maupun sumber lain.

Dalam melakukan penelitian tentang optimalisasi keamanan router mikrotik terhadap serangan *ping attack* dengan menggunakan metode *raw firewall*, kemudian melakukan pengumpulan data tentang pengamanan jaringan, setelah itu melakukan evaluasi data yang telah didapatkan. Dalam perancangan sistem ini penulis membuat mekanisme *filtering* dan titik-titik yang akan ditempati *firewall* dan instalasi perangkat keras dan perangkat lunak dari sistem yang akan dirancang.

Salah satu data pendukung yang dapat dijadikan sumber tersendiri adalah kajian terdahulu yang berhubungan dengan permasalahan yang sedang dibahas dalam penelitian ini. Penelitian terdahulu dikumpulkan oleh penulis untuk membuat perbandingan antara penelitian terdahulu dengan penelitian yang dilakukan oleh penulis untuk melengkapi dan menjadi landasan dalam melakukan penelitian ini. Oleh karena itu, penulis mengambil referensi dari beberapa jurnal penelitian terdahulu. Berikut hasil perbandingan penelitian tersebut.

Penelitian terdahulu yang dilakukan oleh (Aprilianto et al., 2017) yang berjudul Sistem Pencegahan *UDP DNS Flood* dengan *Filter Firewall* pada *Router Mikrotik* menjelaskan bahwa *firewall* yang dikonfigurasi dalam sistem keamanan *Router MikroTik* melakukan pemeriksaan data yang diterima dan melacak koneksi tersebut diizinkan atau ditolak. Penggunaan *firewall* digunakan untuk menyaring *user* yang terkoneksi dan melakukan penghalangan akses dari *user* yang diblokir.

Penelitian terdahulu yang dilakukan oleh (Putra et al., 2020) dengan judul Pemanfaatan *Mikrotik Routerboard* sebagai Keamanan Jaringan dari *UDP Flood* dengan Menggunakan *Firewall* di Dinas Pendidikan Kabupaten Bengkalis menjelaskan bahwa *mikrotik routerboard* sebagai keamanan jaringan dari *UDP Flood* dengan menggunakan *firewall* bekerja dengan baik. Dengan menggunakan *routerboard mikrotik* sebagai media pengamanan jaringan sangat membantu meningkatkan perlindungan pada lalu lintas jaringan internet di dinas pendidikan Bengkalis.

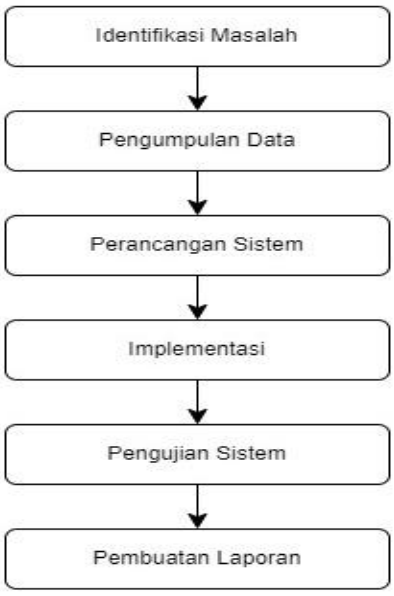
Penelitian terdahulu yang dilakukan oleh (Mardiyana, 2015), *MikroTik Router* adalah salah satu sistem operasi yang dapat digunakan sebagai *router* jaringan yang handal, mencakup berbagai fitur lengkap untuk jaringan dan *wireless*. Selain itu *MikroTik* dapat juga berfungsi sebagai *firewall*. Melalui penelitian ini dengan judul Keamanan Jaringan dengan *Firewall Filter* Berbasis *Mikrotik* Pada Laboratorium Komputer STIKOM Bali akan dibahas bagaimana merancang jaringan komputer dengan menerapkan konsep firewall berbasis Mikrotik dengan tujuan dapat mengurangi resiko ancaman yang akan mengganggu aktifitas yang yang sedang berlangsung, disesuaikan dengan

VOL. 17. NO. 1 AGUSTUS 2022
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri

kondisi tempat penelitian yaitu pada Laboratorium Komputer STIKOM Bali.

Seperti halnya pengamanan dengan *firewall filter rules*, pengamanan dengan *raw firewall* juga menggunakan dua metode yang sama, namun dengan beberapa penyesuaian konfigurasi. Berbeda dengan *firewall filter rules,* pada *raw firewall* di bagian parameter *chain*, tersedia fitur *prerouting*. Penulis menggunakan fitur tersebut, yang memungkinkan *action* dilakukan sebelum *connection tracking* yaitu pada saat proses terjadinya serangan, sebelum masuk ke dalam sistem jaringan, aliran paket tersebut sudah diputus (*drop*) sehingga dapat menghemat *resource* dan tidak membebani kinerja perangkat.

Model pengembangan sistem yang digunakan oleh penulis dalam pembuatan penelitian ini terbagi dalam beberapa tahap terlihat pada Gambar 1, yaitu:



Sumber: (Nadhir, 2022)

Gambar 1. Alur Penelitian

a. Analisa Kebutuhan

Melakukan analisa terkait permasalahan yang terjadi pada jaringan komputer yang akan dirancang dan apa saja yang diperlukan untuk merancang jaringan tersebut. Dalam hal ini penulis membutuhkan sebuah router mikrotik untuk dapat melakukan konfigurasi keamanan jaringan menggunakan metode *raw firewall*.

b. Desain

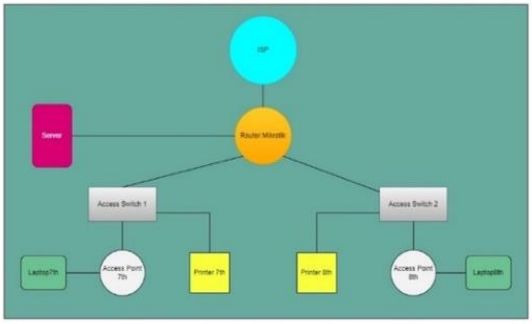
Melakukan perancangan dengan menggunakan *software* GNS3 untuk kebutuhan topologinya.

c. *Testing*

Melakukan uji coba serangan terhadap metode keamanan sebelum dan sesudah implementasi *raw firewall*.

d. Implementasi

Setelah tahapan uji coba berhasil dan sistem sudah berfungsi dengan baik, penulis baru bisa melakukan implementasi pada perusahaan.



Sumber: (Nadhir, 2022)

Gambar 2. Topologi Jaringan

HASIL DAN PEMBAHASAN

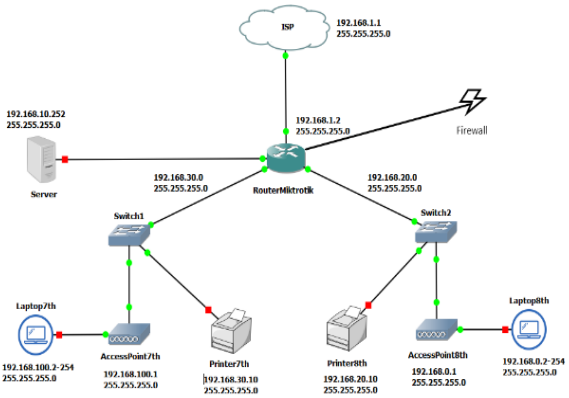
Rancangan Jaringan Usulan

A. Topologi Jaringan

Pada topologi jaringan, penulis tidak melakukan perubahan pada topologi sebelumnya, dimana yang menjadi dasar dari usulan ini adalah mengoptimalkan sistem keamanan jaringan menggunakan metode *raw firewall* berbasis mikrotik dan topologi yang digunakan masih menggunakan topologi *star* seperti yang terlihat pada Gambar 2.

B. Skema Jaringan

Berdasarkan hasil analisa permasalahan yang dihadapi, maka mengubah teknik dari *Filter Rules* ke *Raw Firewall* adalah untuk mengoptimalisasi jaringan yang sudah ada dan sebagai usulan dari pemecahan masalah. Rancangan skema jaringan secara garis besar masih sama dengan sebelumnya dikarenakan tidak mengubah apapun dan hanya menambahkan konfigurasi *firewall* pada *router* mikrotik untuk pengaturan metode keamanan jaringannya. Skema jaringan yang diusulkan ditunjukkan pada Gambar 3.



Sumber: (Nadhir, 2022)

Gambar 3. Skema Jaringan Usulan

VOL. 17. NO. 1 AGUSTUS 2022
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri
INTI NUSA MANDIRI
DOI: https://doi.org/10.33480/inti.v17i1.3401

C. Keamanan Jaringan

Pada jaringan PT. Permata Graha Nusantara sudah menggunakan metode dan teknik yang cukup baik untuk mengamankan jaringan komputer agar terhindar dari perlakuan oknum yang tidak bertanggung jawab yang berniat untuk merusak jaringan komputer tersebut. Sistem keamanan yang diterapkan adalah *firewall filter rules* dan telah terintegrasi dengan *firewall* dari mikrotik itu sendiri dan teknik yang digunakan oleh sebuah *firewall* adalah sebagai berikut:

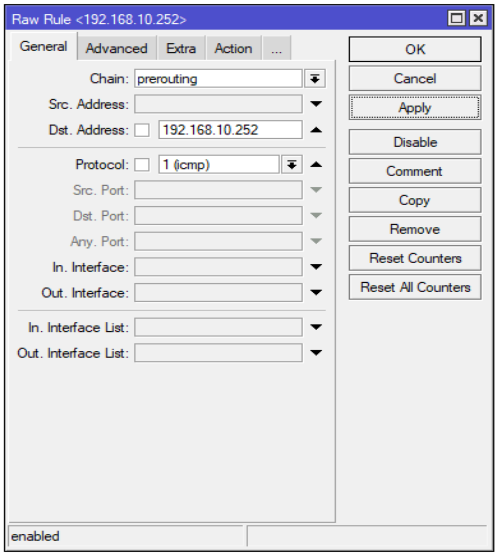
a. *Service Control* (kendali terhadap layanan), berdasarkan tipe-tipe layanan yang digunakan di Internet dan boleh diakses baik untuk ke dalam ataupun keluar *firewall*. Biasanya *firewall* akan mengecek nomor IP Address dan juga nomor port yang di gunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi *software* untuk proxy yang akan menerima dan menerjemahkan setiap permintaan suatu layanan sebelum mengizinkannya. Bahkan bisa jadi *software* pada server itu sendiri, seperti layanan untuk web ataupun untuk *mail*.
b. *Direction Control* (kendali terhadap arah), berdasarkan arah dari berbagai permintaan (*request*) terhadap layanan yang akan dikenali dan diizinkan melewati *firewall*.
c. *User control* (kendali terhadap pengguna), berdasarkan pengguna (*user*) untuk dapat menjalankan suatu layanan, artinya ada *user* yang dapat dan ada yang tidak dapat menjalankan suatu layanan, hal ini dikarenakan *user* tersebut tidak diizinkan untuk melewati *firewall*. Biasanya digunakan untuk membatasi *user* dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.
d. *Behavior Control* (kendali terhadap perlakuan), berdasarkan seberapa banyak layanan itu telah digunakan. Misal, *firewall* dapat menyaring email untuk menanggulangi dan mencegah *spam*.

D. Manajemen Jaringan

Pada tahapan manajemen atau pengaturan jaringan, salah satu yang menjadi perhatian khusus adalah kebijakan (*Policy*) yang perlu diterapkan untuk membuat dan mengatur, agar sistem yang telah dibangun berjalan dengan baik dapat berlangsung lama dan unsur kehandalan terjaga. Optimalisasi keamanan jaringan yang diterapkan pada jaringan yang dibangun dan diimplementasikan ini bertujuan untuk memanfaatkan fitur yang ada. Dilain sisi dengan perubahan teknik ini diharapkan dapat mengurangi permasalahan-permasalahan yang terdapat pada jaringan sebelumnya.

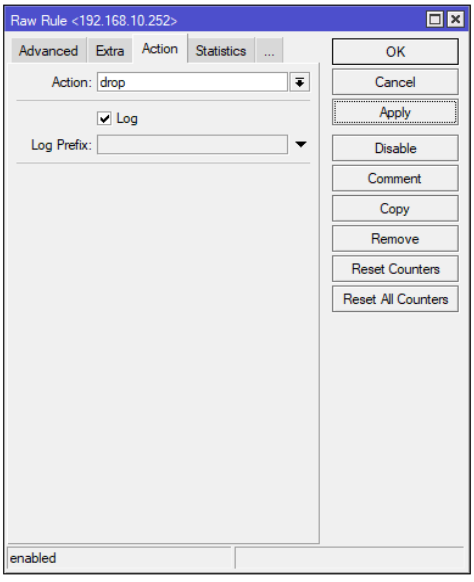
E. Rancangan Aplikasi

Pada tahap ini penulis melakukan dengan cara mengimplementasikan terlebih dahulu konfigurasi *Raw Firewall* menggunakan *Router* Mikrotik yang sudah dibuat menggunakan aplikasi WinBox. Konfigurasi yang diterapkan untuk membuat metode *raw firewall* diantaranya sebagai berikut:
Sebelum melakukan konfigurasi *Raw Firewall*, dipastikan sudah melakukan konfigurasi dasar berupa *setting IP Address*, *DNS*, *DHCP*, *Firewall NAT* telah dilakukan. Selanjutnya dapat dilakukan konfigurasi *Raw Firewall* untuk pengamanan *DDoS Attack*, dengan pengaturan seperti pada Gambar 4 dan Gambar 5.



Sumber: (Nadhir, 2022)

Gambar 4. Konfigurasi Raw Firewall pada tab General

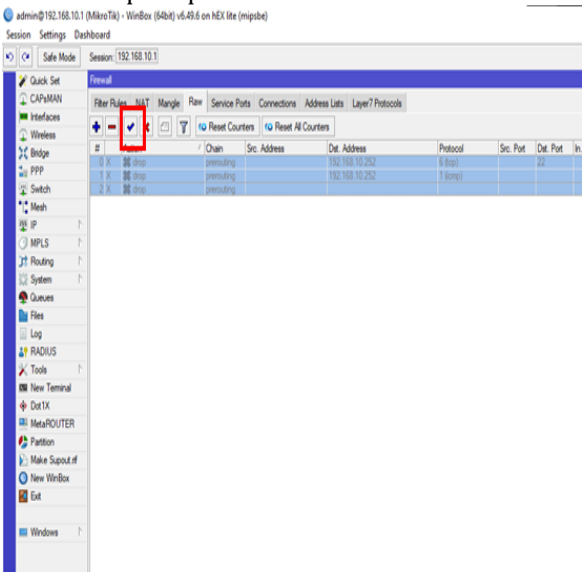


Sumber: (Nadhir, 2022)

Gambar 5. Konfigurasi *Raw Firewall* pada tab *Action*

VOL. 17. NO. 1 AGUSTUS 2022
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri

Pengaturan yang sama dilakukan pada protokol yang lainnya. Setelah beberapa parameter telah diinput, maka tinggal melakukan aktivasi Raw Firewall seperti pada Gambar 6.



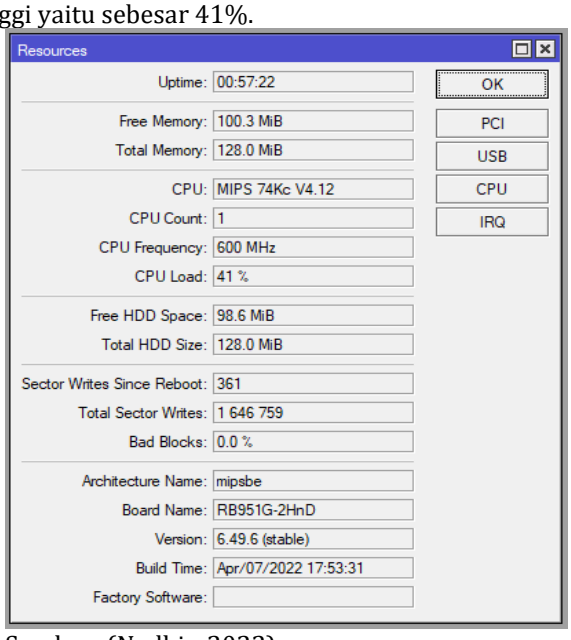
Sumber: (Nadhir, 2022)

Gambar 6. Aktivasi Raw Firewall

F. Pengujian Jaringan

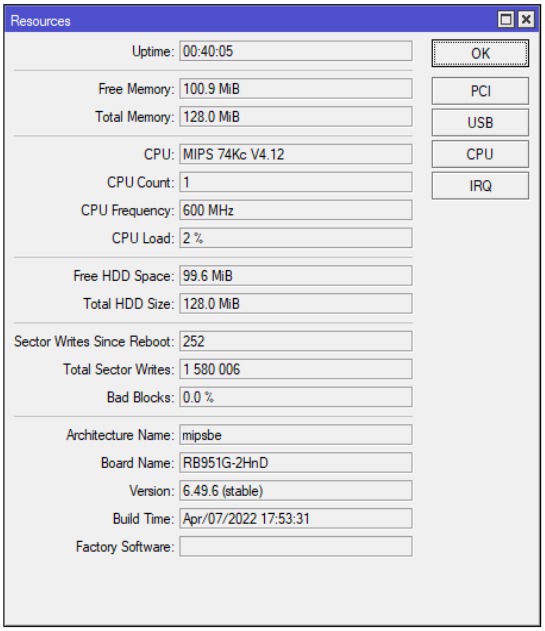
1) Pengujian Jaringan Awal

Pada pengujian jaringan awal, dilakukan pengetesan serangan *Ping Attack* terhadap jaringan yang menggunakan teknik *filter rules*, terlihat pada Gambar 7 bahwa *traffic* yang masuk ke *router* cukup padat sehingga penggunaan CPU menjadi lebih tinggi yaitu sebesar 41%.



Sumber: (Nadhir, 2022)

Gambar 7. Hasil Pengujian Awal

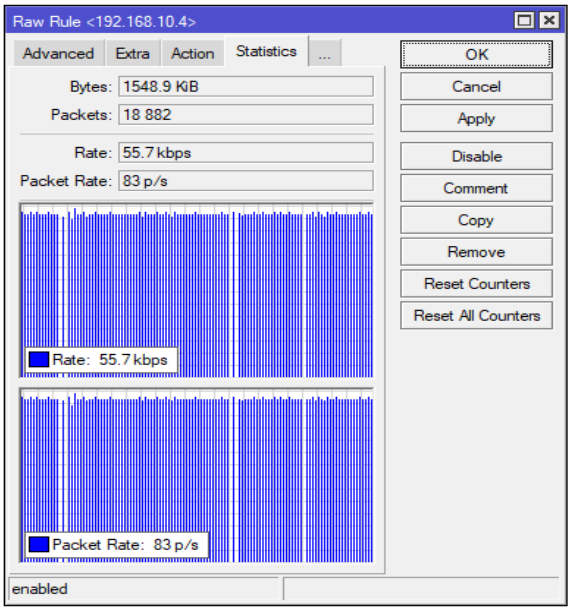


Sumber: (Nadhir, 2022)

Gambar 8. Hasil Pengujian Awal

2) Pengujian Jaringan Akhir

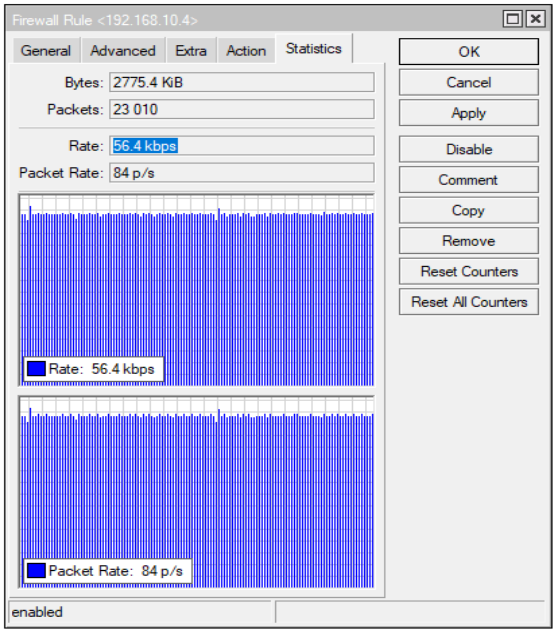
Pada pengujian jaringan akhir, dilakukan pengetesan serangan *Ping Attack* terhadap jaringan yang menggunakan metode *firewall* dengan teknik *Raw Firewall*, dari Gambar 9 terlihat bahwa *traffic* tidak terlalu padat dan penggunaan CPU lebih minim hanya sebesar 2% dibandingkan teknik *filter rules*.



Sumber: (Nadhir, 2022)

Gambar 9. Hasil Pengujian Akhir

INTI NUSA MANDIRI
DOI: https://doi.org/10.33480/inti.v17i1.3401



Sumber: (Nadhir, 2022)

Gambar 10. Hasil Pengujian Akhir

KESIMPULAN

Berdasarkan keseluruhan hasil pengujian dan analisis pada penelitian akhir ini terdapat kesimpulan bahwa dengan menerapkan teknik *raw firewall* dapat meminimalisir penggunaan pada CPU yang hanya sebesar 2% (Gambar 9). Hal ini disebabkan teknik *raw firewall* dapat memutus serangan atau aliran paket (*drop*) sebelum masuk ke dalam jaringan, sehingga tidak ada pengaruh besar terhadap *traffic* dan performa pada perangkat tetap stabil. Dengan penggunaan CPU yang minim dan kinerja perangkat yang stabil, dapat memperpanjang usia perangkat.

Metode *Raw Firewall* yang diterapkan pada sistem jaringan PT Permata Graha Nusantara ini sudah cukup baik, namun masih memerlukan pengembangan keamanan untuk menangani keamanan jaringan. Dengan perkembangan teknologi yang semakin canggih, memungkinkan serangan dapat terjadi dari mana saja dan kapan saja. Untuk itu kewaspadaan terhadap ancaman serangan perlu ditingkatkan dengan cara memberikan fitur notifikasi melalui pesan instan (telegram) secara *real time* ketika jaringan mendapat serangan. Dengan adanya notifikasi tersebut diharapkan mempermudah teknisi atau petugas dalam melakukan pengawasan dan pemantauan kondisi jaringan kantor.

REFERENSI

A. Gutnikov, O. Kupreev, dan E. B. (2021). *DDoS attacks in Q1 2021*. Securelist, 2021. https://securelist.com/ddos-attacks-in-q1-2021/102166/

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.

Adrian, R., & Isnianto, N. (2016). *Pada Performa Router*. *October*, 1257–1259.

Amarudin. (2018). *DESAIN KEAMANAN JARINGAN PADA MIKROTIK ROUTER OS*. *12*(2), 72–75.

Anugrah, I., & Rahmanto, R. H. (2018). Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone. *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*, *5*(2), 91–106. https://doi.org/10.33558/piksel.v5i2.271

Aprilianto, D., Fadila, T., & Muslim, M. A. (2017). Sistem Pencegahan UDP DNS Flood Dengan Filter Firewall Pada Router Mikrotik. *Techno.Com*, *16*(2), 114–119. https://doi.org/10.33633/tc.v16i2.1291

Dwiyatno, S., Sari, A. P., Irawan, A., & Safig, S. (2019). Pendeteksi Serangan Ddos (Distributed Denial Of Service) Menggunakan Honeypot Di Pt. Torini Jaya Abadi. *Jurnal Sistem Informasi Dan Informatika (Simika)*, *2*(2), 64–80. https://doi.org/10.47080/simika.v2i2.606

Fadlil, A., Riadi, I., & Aji, S. (2017). Review of detection DDOS attack detection using naive bayes classifier for network forensics. *Bulletin of Electrical Engineering and Informatics*, *6*(2), 140–148. https://doi.org/10.11591/eei.v6i2.605

Fakhmi, Muhammad; Gultom, L. M. (2021). Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw (Studi kasus : Sekolah Menengah Kejuruan Negeri 3 Bengkalis). *Seminar Nasional Industri Dan Teknologi (SNIT), Politeknik Negeri Bengkalis*, *30*, 260.

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

Langobelen, E. S. R. O. B., Rachmawati, Y., & Iswahyudi, C. (2019). Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus

VOL. 17. NO. 1 AGUSTUS 2022
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri

Di Taman Pintar Yogyakarta. *Jurnal JARKOM*, *7*(2), 95–102.

Mardiyana, I. G. K. O. (2015). Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik Pada Laboratorium Komputer STIKOM Bali. *Stmik Stikom*, *86*, 804–807.

Mardiyanto, B., Indriyani, T., & Suartana, I. M. (2016). Analisis dan Implementasi Honeypot dalam Mendeteksi Serangan Distributed Denial-Of-Services (DDOS) pada Jaringan Wireless. *Integer Journal*, *1*(2), 32–42.

Muzakir, A., & Ulfa, M. (2019). Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan JARINGAN. *Simetris: Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*, *10*, 15–20. https://doi.org/10.24176/simet.v10i1.2646

Pambudi, R., & Muslim, M. A. (2017). Implementasi Policy Base Routing dan Failover Menggunakan Router Mikrotik untuk Membagi Jalur Akses Internet di FMIPA Unnes. *Jurnal Teknologi Dan Sistem Komputer*, *5*(2), 57. https://doi.org/10.14710/jtsiskom.5.2.2017.57-61

Putra, B. J. G., Musri, T., & Gultom, L. M. (2020). Pemanfaatan Mikrotik Routerboard Sebagai Keamanan Jaringan Dari UDP Flood Dengan Menggunakan Firewall Di Dinas Pendidikan Bengkalis. *Seminar Nasional Industri Dan Teknologi (SNIT), Politeknik Negeri Bengkalis*, 260–269.

Ridho, F., Yudhana, A., & Riadi, I. (2017). Implementasi Log dalam Forensik Router Terhadap Serangan Distributed Denial of Service(DDoS). *Jurnal TIMES*, *VI*(2), 15–21.

