Implementasi Keamanan Jaringan Lan Menggunakan Mikrotik Dengan Metode Firewall Filtering

Bayu Santosa[1], Ali Akbar Rismayadi[2]
[1,2]Program Studi Teknik Informatika, Universitas Adhirajasa Reswara Sanjaya, Bandung
e-mail: [1]bayusantosa17@gmail.com, [2]ali@ars.ac.id

Abstrak

Dengan terus berkembangnya teknologi di bidang jaringan *internet* dan akses informasi yang tidak terbatas miliki keuntungan yang sangat banyak bagi setiap orang. Namun bila dilihat dalam penggunaannya secara nyata, jaringan *internet* memiliki banyak sekali kerugian yang ditimbulkan apabila kontrol terhadap penggunaannya tidak dibatasi dengan baik. Karena bisa disalahgunakan dengan mengakses situs-situs pornografi, kekerasan dan media sosial di *internet*. Jaringan *internet* yang tidak dibatasi di instansi dan individu, hal ini dapat menyebabkan jaringan menjadi lambat akibat akses terhadap situs tertentu yang berlebihan. Hal ini juga dapat mempengaruhi emosional. Untuk meminimalisir kerugian tersebut maka keamanan jaringan untuk membatasi akses *internet* tersebut dirasa perlu untuk dilakukan agar jaringan *internet* dapat dipergunakan sesuai dengan fungsinya bagi instansi dan individu. Hal tersebut dapat diwujudkan dengan melakukan pemblokiran akses dengan metode *firewall filtering* menggunakan *mikrotik* dengan fitur *Intrusion Prevition System* (IPS). Administrator system dapat mengetahui serangan yang terjadi pada router Mikrotik melalui notifikasi pesan yg didalamnya memuat informasi jenis serangan dan waktu terjadinya yang di kirim dengan *sistem* pesan *Telegram*.

Kata Kunci: Keamanan Jaringan, Internet, IPS, Mikrotik, firewall filtering

Abstract

With the continued development of technology in the field ofnetworks internet and unlimited access to information, there are many advantages for everyone. However, when viewed in real use, thenetwork internet has a lot of disadvantages that arise if the control over its use is not properly restricted. Because it can be misused by accessing pornographic sites, violence and social media on the internet.network Internet that is not restricted to agencies and individuals, this can cause the network to be slow due to excessive access to certain sites. It can also affect emotions. To minimize these losses, network security to limitaccess internet is deemed necessary so that thenetwork internet can be used according to its function for agencies and individuals. This can be achieved by blocking access withmethod firewall filtering using the Mikrotik router feature Prevition Intrusion System (IPS). System administrators can find out attacks that occur on Mikrotik routers through message notifications which contain information on the type of attack and the time of occurrence which are sent with the Telegram message system.

Keywords: *Network Security, Internet, IPS, Mikrotik, firewall filtering*

Corresponding Author:
Ali Akbar Rismayadi,
Email: ali@ars.ac.id

1. PENDAHULUAN

Pertumbuhan teknologi jaringan komputer saat ini mengalami kemajuanya yang semakin pesat, perkembangan tersebut bisa berdampak pada sistem keamanan yang ada didalamnya. Sehingga bagi para pengguna aplikasi yang terhubung dalam jaringan komputer harus lebih waspada dalam penggunaanya [1]. Perkembangan teknologi jaringan komputer, selain berdampak positif juga dapat menimbulkan sisi negative, beberapanya adalah merupakan serangan terhadap sistem jaringan komputer yang saling terhubung ke jaringan luas atau bisa disebut dengan jaringan internet[2].

Jaringan LAN yang saling terhubung saat ini merupakan layanan yang dibutuhkan oleh setiap institusi atau individu, komputer yang saling terhubung memiliki keunggulan lebih dibandingkan komputer independen, komputer yang saling terhubung memungkinkan data untuk dibagikan dengan perangkat keras atau perangkat lunak sehingga kinerjanya lebih efisien. [3].

Informasi berupa aliran data dari satu komputer ke komputer lain atau dari satu komputer ke komputer lain. Hal ini memungkinkan setiap komputer dan perangkat yang terhubung untuk bertukar layanan informasi dan data atau berbagi penyimpanan dan sumber daya, seperti jaringan internet bisa juga pertukaran hard drive atau aplikasi menurut phrimatha dalam [4].

Local Area Network (LAN) merupakan internal jaringan yang bersifat pribadi dan memiliki cakupan area yang terbatas, jarak antar perangkat router biasanya sekitar 200m, bisa berupa gedung atau area yang berdekatan [5].

Tentunya dalam pembangunan jaringan LAN perlu menerapkan hardware dan software mikrotik yang bisa menghubungkan dan mengamankan lalu lintas data trafik yang sedang berjalan dalam jaringan tersebut, agar perangkat bisa di monitoring dan diawasi aktivitasnya jika terjadi aktivitas yang tidak diijinkan akan otomatis tidak di berikan akses diperangkatnya[6]

Router Mikrotik merupakan device yang mendukung sistem keamanan jaringan yang didalamnya mendukung metode keamanan *firewall* dengan baik serta dengan biaya yang terjangkau, dalam pengoprasianya bisa berjalan dengan efiesien sehingga dapat disesuaikan dengan keperluan instasi atau individu itu sendiri mikrotik juga dapat digunakan untuk pemblokiran konten yang berbau negatif agar menghentikan pengguna mengakses konten tertentu[7].

Firewall dapat diartikan sebagai suatu komponen yang dapat membatasi akses antar jaringan yang dilindungi, *firewall* dapat menjadi solusi untuk mengatasi keamanan dalam suatu jaringan yang dapat dipenuhi dengan berbagai ancaman baik di dalam maupun di luar jaringan. Dengan konfigurasi yang benar, ini memungkinkan untuk melindungi lalu lintas. Lalu lintas atau lalu lintas bisa lebih baik dan lebih aman[8].

Ada banyak pendekatan untuk jaringan komputer yang telah berkembang dari pendekatan lain,bisa menjadi kemajuan dalam teknologi berbasis keamanan jaringan. Salah satu teori yang dapat dikembangkan kembali adalah dengan menggunakan *iptables* di Linux. Beberapa penelitian telah dilakukan pada keamanan jaringan., yaitu oleh Mizan Syarif Hawari dan Ibnu Febry Kurniawan (2016) yang berjudul Penerapan IP Tables *Firewall* Pada *Linux* Dengan Menggunakan Fedora [9].

Komputer yang saling terhubung merupakan sekumpulan komputer-komputer independen yang saling terhubung ke komputer lain melalui media penghubung atau sarana yang menggunakan protokol komunikasi untuk bertukar data dan informasi, program dan perangkat keras seperti printer, hard drive, dll.[10]

Tujuan utama dari keamanan jaringan komputer adalah untuk menyediakan jalur yang aman antara perangkat yang bertukar informasi dan memastikan perlindungan data. Insiden keamanan jaringan komputer adalah prilaku dimana jaringan komputer berpartisipasi dan mempengaruhi keamanan[11].

Menurut Primatha dalam Ariyadi Dan alfyuddin, *Firewall* bisa disebut dengan "pos pemeriksaan" yang mengevaluasi lalu lintas data masuk dan keluar antara jaringan internal /

pribadi kita dan dunia luar, memungkinkan lalu lintas data tertentu dan memblokir yang lain. Lalu lintas yang diblokir umumnya berupa lalu lintas ilegal yang bersifat merusak/tidak diinginkan. Tindakan penyusup, peretas, peretas, dan virus dicegah oleh *firewall* [12].

Adapun metode yang lain yang pernah dapat dikembangkan kembali adalah metode Port Blocking pada frewall mikrotik, yang telah di lakukan oleh Muhamad Ryansyah dan Muhamad Sony Maulana (2018) yang berjudul Malwer Security Menggunakan *Filtering Firewall* Dengan Metode Port Blocking Pada, Mikrotik Rb 1100 AHx2 [13].

Dari masalah yang sudah di uraikan metode *firewall filtering* dengan sistem *Intrusion Prevention System* (IPS) dirasa dan dianggap berkinerja tinggi karena memeriksa banyak faktor (port, alamat IP, dll.). Dan dapat diterapkan pada router atau switch jaringan biasa tanpa perangkat tambahan dan lebih efisien untuk digunakan.

2. METODE PENELITIAN

Metode merupakan alat yang digunakan dalam praktik implementasi keamanan jaringan yang mencakup langkah - langkah yang dijalankan peneliti untuk melakukan survei, menggambarkan suatu permasalahan, merumuskan masalah yang diidentifikasi, dan kemudian menganalisis masalah untuk menentukan sifat masalah. survei untuk memahami dan memahami masalah. Pertama menentukan ruang lingkup masalah, kemudian melakukan penelitian dan studi literatur merupakan suatu langkah - langkah kajian teoritis terhadap masalah yang dihadapi. Pencarian narasumber bibliografi di buku dan majalah Langkah selanjutnya adalah melakukan observasi lapangan untuk memahami kondisi di mana masalah secara langsung mempengaruhi hasil. [14].

2.1. Studi Literatur

Mempelajari berbagai studi literatur tentang macam konsep yang berkaitan dengan praktek implementasi, termasuk didalamya mempelajari konsep firewall filtering yang berkaitan dengan pembuatan skripsi, untuk mempelajari konsep firewall filtering, dengan mencari sumber teori yang ada yaitu dengan membaca journal dan melihat video tutorial tentang firewall filtering yang bersumber diinternet.

2.2. Intrusion Prevition System (IPS)

Intrusion Prevention System (IPS) merupkan suatu teknik keamanan jaringan komputer yang banyak digunakan menggabungkan teknik IPS dan metode *Intrusion Detection System* (IDS) kemajuan ini dapat digunakan secara sempurna untuk suatu pencegahan serangan yang menembus jaringan internal dengan memeriksa dan merekam lalu lintas paket data dan mengidentifikasi paket data dengan sensor ketika terdeteksi adanya serangan, IPS akan menolak akses (block) dan mencatat (log) semua paket data yang teridentifikasi. IPS dapat bertindak sebagai firewall, yang dikombinasikan dengan IDS, yang dapat mengenali paket data secara detail, dapat mengizinkan dan memblokir, IPS menggunakan tanda tangan untuk mengenali aktivitas lalu lintas data dalam jaringan dan perangkat akhir, yang melaluinya paket masuk dan keluar diverifikasi. (inbound-outbound) dapat dicegah, karena secepat mungkin, sebelum mereka putus dan juga mendapatkan akses ke jaringan lokal[15].

2.3. Bahan dan Alat Mikrotik

Dalam pengimplementasi ini penulis memakai perangakat mikrotik, Untuk spesifikasi alat yang digunakan penulis sebagai berikut:

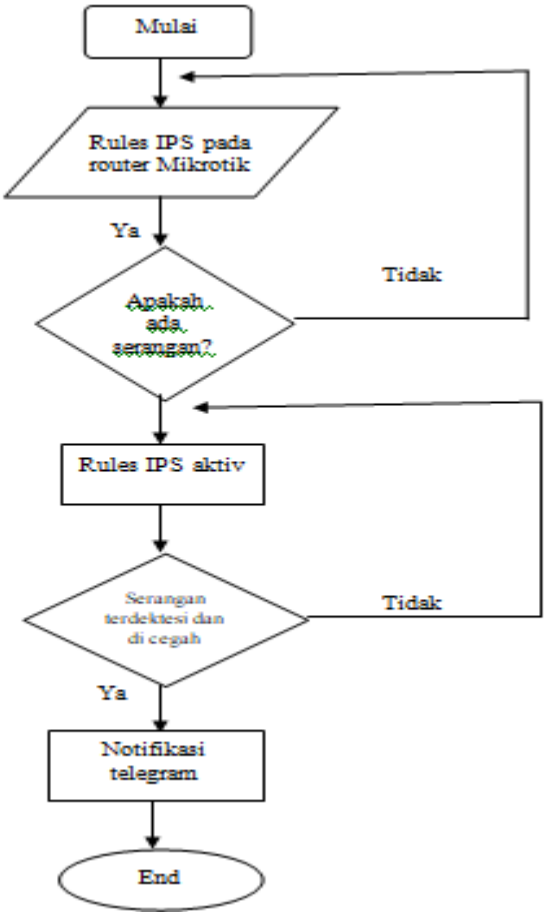
Tabel 1
Spesifikasi Mikrotik

Mikrotik Routerboard RB 750Gr3	
Product Code	RB 750 Gr3
Architecture	MMIPS
Cpu	MT7621A Core 4thr 880Mhz
Current Monitor	No
Main Storage	16MB
Ram	256MB
SFP Ports	0
LAN Ports	5
Gigabit	Yes
Switch Chip	1
MiniPCI	0
Integrated Wireless	No
MiniPCIe	0
Sim Card Slot	No
USB	Yes
Power On USB	Yes
Memory Cards	Yes
Memory Card Tipe	MicroSD
Power Jack	8-30V
802.3af Support	No
POE Input	8-30V
POE Output	No

(sumber:https://mikrotik.com/product/RB750Gr3)

2.4. Desain Flowchart Firewall Filtering

Saat membuat flowchart, jenis yang akan dibuat adalah flowchart sistem jaringan LAN dengan suatu metode *firewall filtering* dengan sistem IPS. Berikut ini adalah flowchart *firewall* dengan menggunakan IPS di Mikrotik..



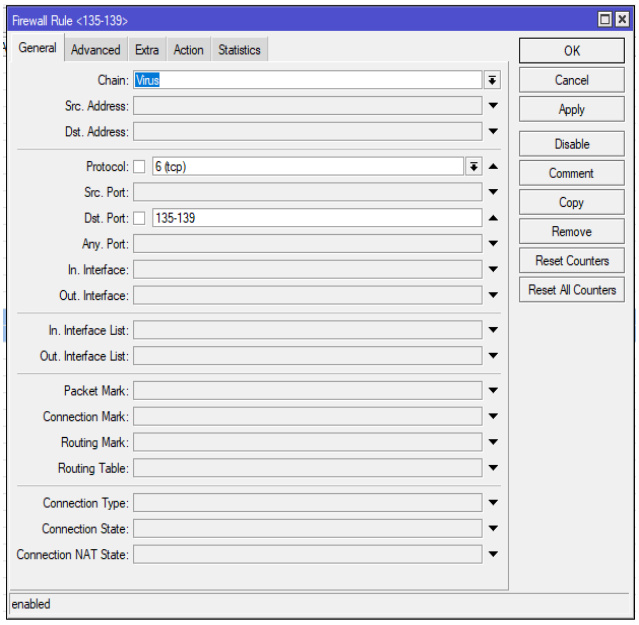
Gambar 1. Desain flowchart metode firewall filtering dengan sistem IPS

2.5. Implementasi Dan Penarikan Kesimpulan

Implementasi dan penarikan kesimpulan apakah *firewall filtering* dengan *Intrusion Prevetion System* (IPS) dapat melindungi dan mengatur akses dari eksternal jaringan LAN yang boleh diakses dan tidak boleh diakses.

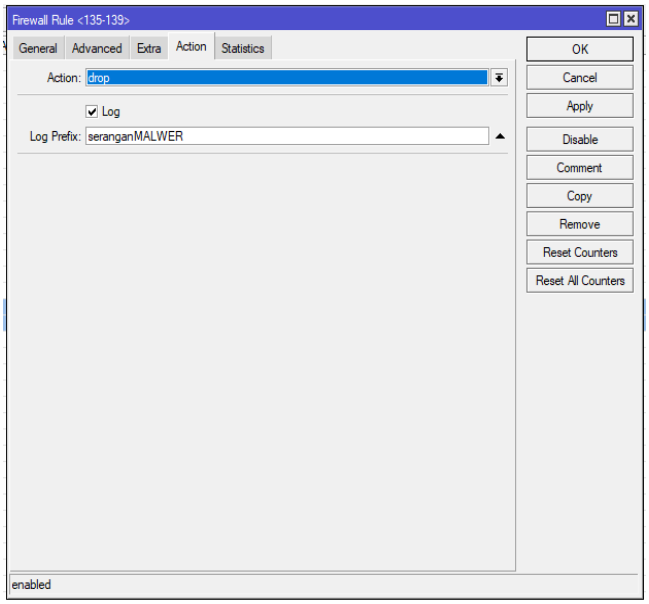
2.6. Setup Notifikasi IPS ke Telegram

Konfigurasi *Intrusion Prevention System* (IPS) dilakukan pada menu *firewall* yang ada dalam winbox. untuk mensettingnya IPS dilakukan pada filter rules. Untuk menentukan rules pada jenis serangan, maka ditentukan melalui situs dan port-port sesuai dengan setiap jenis akses ataupun serangan. Pada penelitian ini digunakan 3 jenis ketentuan akses dan serangan, yaitu situs yang dilarang diakses, serangan DDOS, dan Port yang dijadikan sarang virus Malwer.



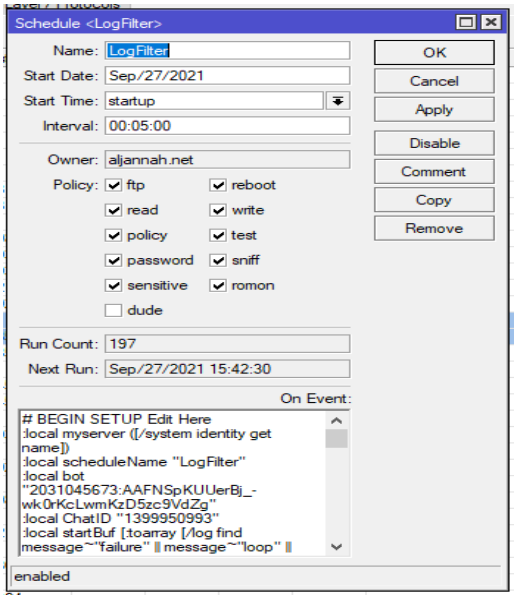
Gambar 2. Port serangan Malwer

Dalam konfigurasi IPS ini, selain menentukan port sesuai dengan jenis serangan, mengatur juga action atau tindakan yang akan dilakukan jika terdapat serangan yang masuk. IPS akan bertidak sebagai pencegah serangan, maka action dalam firewall diatur menjadi drop yang artinya serangan akan diblokir.



Gambar 3. Action Serangan

Menghubungkan Mikrotik dengan telegram bertujuan untuk memberikan notif serangan yang akan terjadi pada Mikrotik sebagai sumber internet. Untuk menghubungkannya maka perlu log prefix sesuai dengan jenis serangan. Log Prefix ini kemudian akan dieksekusi pada script yang menghubungkan Mikrotik ke telegram. Rule ini dilakukan pada schedule yang terdapat pada menu system.



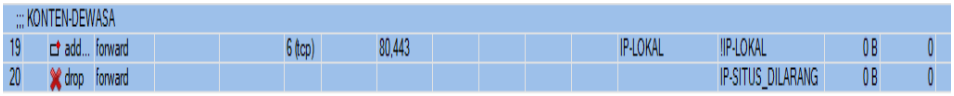
Gambar 4. koneksi Mikrotik ke Telegram

3. HASIL DAN PEMBAHASAN

3.1 Pengujian Situs

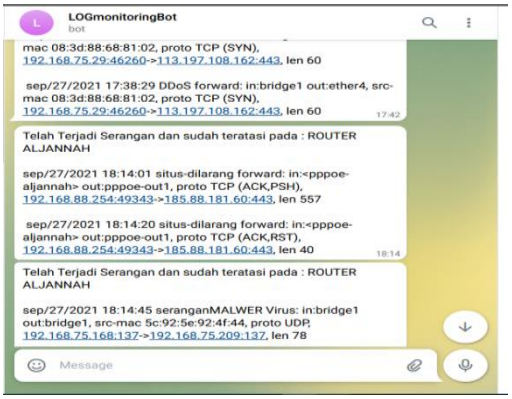
keamanan firewall filtering menggunakan rule firewall filter dengan diterapkanya motede keamanan Intrusion Prevition System (IPS) karena penulis akan menciptakan keamanan jaringan LAN dengan tindakan yang langsung diekseskusi oleh firewall dan memberikan notifikasi kepada administrator jaringan, maka dibutuhkan hardware Mikrotik dan aplikasi Winbox serta Telegram.

Sehingga pengujian diatas dapat mengamankan koneksi lalu lintas trafik data dan dapat menciptakan kenyamanan dan keamanan pengguna jaringan LAN.



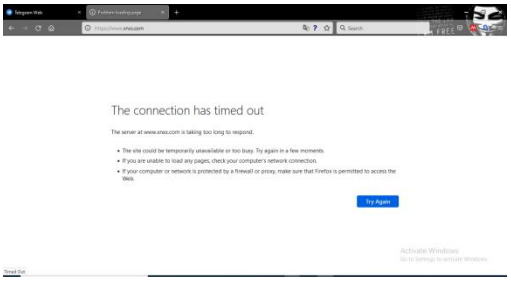
Gambar 5. Konfigurasi firewall

Pada konfigurasi ini situs yang tidak dijinkan akan terblokir secara langsung dan administrator langsung mendpatkan notifikasi terdapat client jaringan yang ingin mengakses situs dilarang dan terblokir terlihat pada gambar 6.



Gambar 6. Notifikasi Monitoring

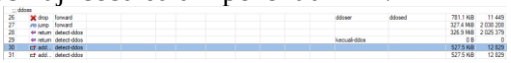
Dan berikut adalah hasil output yang diterima oleh client jaringan LAN yang ingin mengakses situs yang dilarang oleh administrator jaringan bisa dilihat pada gambar 7.



Gambar 7. Hasil output IPS

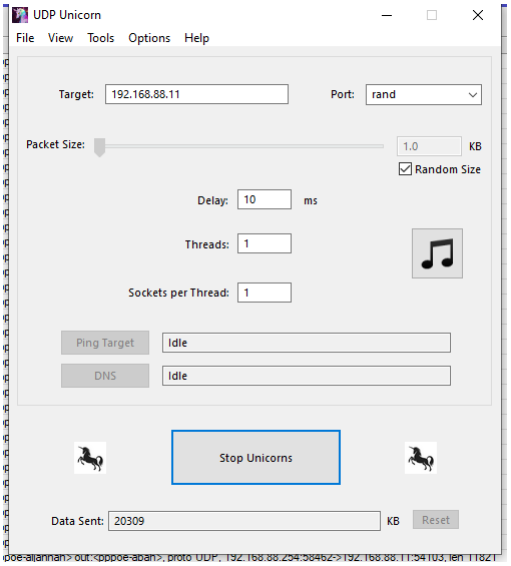
3.2. Pengujian DDOS

Pada DDos dilakukan pengujian menggunakan aplikasi unicorn melalui paket-paket jaringan tertentu, dengan paket sederhana atau dengan jumlah yang sangat besar yang bermaksud mengacaukan keadaan jaringan, pada umumnya serangan ini bertujuan menghabiskan bandwith dan membuat crash sistem sehingga tidak bisa memberikan layanan. Gambar dibawah adalah hasil uji coba dalam penelitian ini :



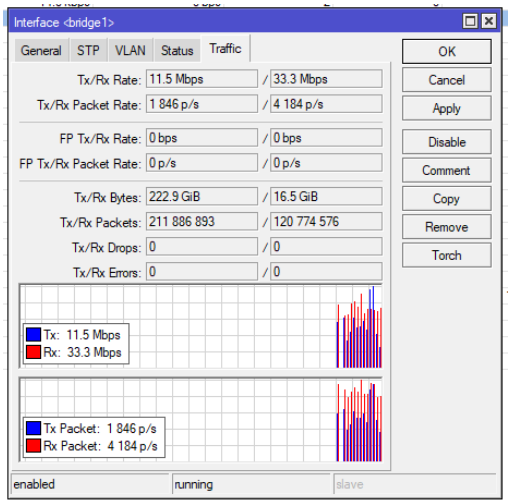
Gambar 8. penerapan IPS DDoS

Pada konfigurasi ini diujicoba dengan melakukan serangan DDoS ke router Mikrotik dengan menggunakan aplikasi penyerang unicorn dengan tujuan menghabiskan bandwith yang tersedia di dalam jaringan LAN dan mengacaukan lalu lintas paket data ujicoba penyerangan bisa dilihat pada gambar 9.



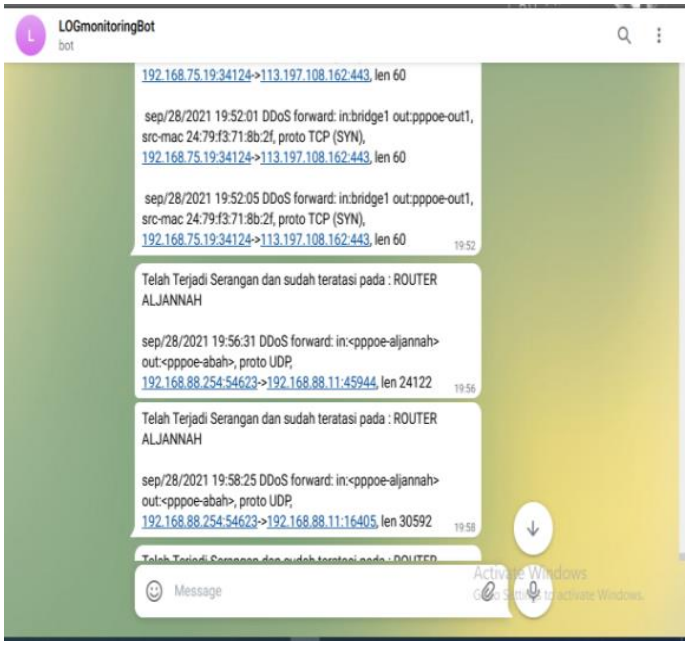
Gambar 9. unicorn DDoS

Efek yang terjadi pada router Mikrotik terlihat pada grafik interface terjadi penikatan trafik yang sangat signifikan dilihat pada gambar 10.



Gambar 10. Tampilan Serangan DDoS

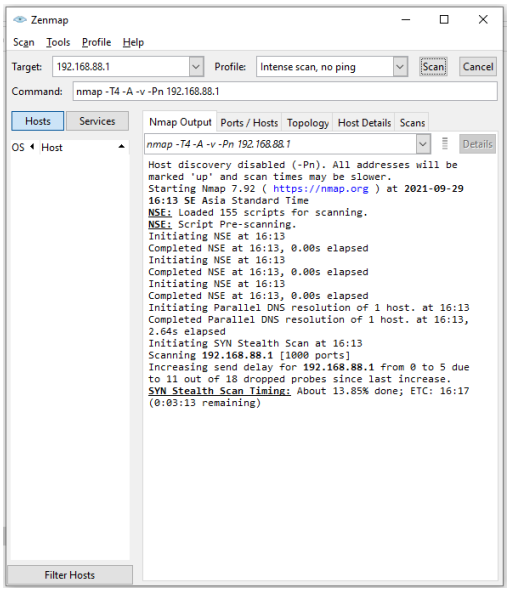
Disaat bersamaan, ketika DDoS menyerang melakukan kegiatan mengirimkan paket yang sangat banyak router mikrotik langsung memberikan laporan kepada administrator jaringan dan mencegah serangan yang terjadi secara cepat, dan laporan akan terlihat bahwa IP 192.168.88.254 telah melakukan serangan ke IP 192.168.88.11 dilihat pada gambar 11.



Gambar 11. Notifikasi telegram

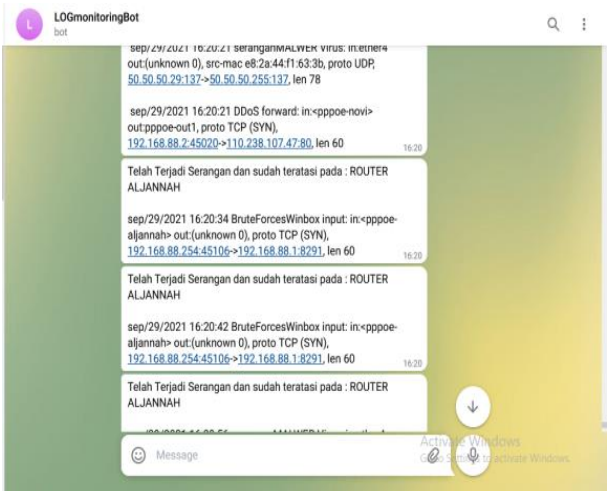
3.3. Pengujian Brute Force Port Scaning

Pengujian Brute Force port berbahaya dilakukan dengan aplikasi Znmap penyerangan dilakukan dengat port target 8291 yang digunakan pada aplikasi winbox diperuntukan sebagai sismtem akses mikrotik, pengujian dilakukan dengan memasukan password secara random berulang kali hingga mendapatkan password yang benar. Penyerangan yang akan dieksekusi pada gambar 12.



Gambar 12. Brute Force Znmap

Jika upaya penyerangan sudah dilakukan, maka secara otomatis akan muncul notifikasi melalui telegram kepada administrator jaringan. Dengan adanya notifikasi melalui telegram berarti serangan tersebut berhasil dicegah pada gambar 13.



Gambar 14. Notifikasi Brute Force Telegram

4. KESIMPULAN

4.1. Kesimpulan

Berdasarkan skripsi dengan judul Implementasi Keamanan Jaringan LAN Menggunakan Mikrotik Dengan Metode.Firewall Filtering dapat diambil kesimpulan bahwa:

1. Dengan menggunakan metode firewall filtering dapat menghilangkan akses terhadap situs-situs dewasa yang tersebar dijaringan LAN yang terhubung dengan jaringan yang lebih luas serta administrator di berikan notifikasi melalui telegram dengan sistem IPS.
2. Keamanan jaringan ini menggunakan firewall yang diatur rule acces list dengan mengizinkan atau memblok jaringan berdasarkan alamat IP address sumbernya
3. Jaringan LAN yang menggunakan mikrotik lebih aman dan lebih stabil dan lebih cepat dalam lalu lintas datanya

4. Mikrotik dapat dijadikan lapis kedua untuk menutup akses terhadap serangan virus seperti spyware dan malwer
5. Administrator dapat mengetahui IP address sumber yang harus dibuka maupun di block aksesnya.

4.2. Saran

Pengujian mikrotik firewall filtering diharapkan dapat digunakan untuk mengamakan lalu lintas trafik data agar menjauhkan pengguna dari hal hal yang negative dari jaringan eksternal maupun internal.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Bapak Ali Rismayadi, S.Kom., M.Kom selaku pembimbing dan Bapak Yudi Ramdhani, ST, M.Kom selaku guru penguji I dan Bapak Ricky Firmansyah, ST, M.Kom selaku guru penguji II. orientasi dan masukan. Penulis juga mengucapkan terima kasih kepada SDN 234 SALUYU yang telah mendukung penelitian ini.

DAFTAR PUSTAKA

[1] Amarudin, "Mikrotik Router Os Menggunakan Metode Port," 2018.

[2] S. N. Khasanah, "KEAMANAN JARINGAN DENGAN PACKET FILTERING FIREWALL (STUDI KASUS: PT. SUKSES BERKAT MANDIRI JAKARTA)," *J. KHATULISTIWA Inform. VOL. IV, NO. 2*, vol. 147, no. 2, pp. 11–40, 2016.

[3] A. A. ASTARI, "IMPLEMEN TASI KEAMANAN JARINGAN DENGAN METODE FIREWALL FILTERING MENGGUNAKAN MIKROTIK," *Simki-Techsain Vol. 02 No. 01 Tahun 2018 ISSN 2599-3011*, vol. 02, no. 01, 2018.

[4] A. A. Rismayadi, S. Topiq, and R. Nurtantho, "Membangun Mail Server Berbasis Linux Menggukan Postfix Admin," *J. Responsif*, vol. 2, no. 1, pp. 92–98, 2020.

[5] D. ReataAkbi and D. NurmsariPratiwi, "Pratiwi, Penerapan Metode Filtering Video Streaming Dan Malware Pada Jaringan Local Area Network 230," *J. Sist. Vol. 7, nomor 3 2018*, vol. 7, no. September, pp. 230–237, 2018.

[6] E. S. R. O. B. Langobelen, Y. Rachmawati, and C. Iswahyudi, "Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus Di Taman Pintar Yogyakarta," *J. JARKOM*, vol. 7, no. 1, pp. 65–75, 2020.

[7] Alfred and J. C. Chandra, "Pemanfaatan Firewall pada Jaringan Komputer SMK Fadilah," *J. I D E A L I S*, vol. 1, no. 5, pp. 422–428, 2018, [Online]. Available: http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/article/download/1037/263.

[8] F. A. Purwaningrum, A. Purwanto, and E. A. Darmadi, "Optimalisasi jaringan menggunakan firewall," *J. IKRA-ITH Inform. Vol 2 No 3*, vol. 2, no. 3, pp. 17–23, 2018.

[9] M. Hawari Syarif and I. Kurniawan Febry, "PENERAPAN IPTABLES FIREWALL PADA LINUX DENGAN MENGGUNAKAN FEDORA Mizan Syarif Hawari Ibnu Febry Kurniawan Abstrak," *J. Manaj. Inform. Vol. 6 Nomor 1 Tahun 2016 198-207 PENERAPAN*, vol. 6, pp. 198–207, 2016.

[10] E. Noor and J. C. Chandra, "IMPLEMENTASI FIREWALL PADA SMP YADIKA 5 JAKARTA," *J u r n a l I D E A L I S V o l . 3 N o . 1 , J a n u a r i 2 0 2 0* |, vol. 3, pp. 449–456, 2020.

[11] F. H ramadhani and A. Yahya Muzakir, *ANALISIS DAN IMPLEMENTASI FIREWALL DENGAN METODE PORT ADDRESS TRANSLATION PADA MIKROTIK OS*. 2018.

[12] T. Ariyadi and moh rizki Alfyuddin, "OPTIMASI BANDWIDTH DAN KEAMANAN JARINGAN DI," *Semin. Has. Penelit. Vokasi Univ. Bina Darma ISSN*, pp. 85–93, 2019.

[13] M. Ryansyah and M. S. Maulana, "Malware Security Menggunakan Filtering Firewall d engan Metode Port Blocking p ada Mikrotik RB 1100AHx 2," vol. 6, no. 3, pp. 6–10,

2018.
[14] M. Ali and F. Latifah, "IMPLEMENASI BLOCK ACCESS PENGGUNA LAYANAN INTERNET DENGAN METODE FILTER RULE dan LAYER 7 PROTOCOL," *J. Inf. Syst. Applied, Manag. Account. Res.*, vol. 5, no. 2, p. 340, 2021, doi: 10.52362/jisamar.v5i2.422.
[15] Y. Arta, A. Syukur, and R. Kharisma, "Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik," *It J. Res. Dev.*, vol. 3, no. 1, pp. 104–114, 2018, doi: 10.25299/itjrd.2018.vol3(1).1346.