Jurnal Ilmiah Sinus (JIS) Vol : 23, No. 1, Januari 2025
ISSN (Print) : 1693-1173 , ISSN (Online): 2548-4028

Pengembangan Firewall Mikrotik dalam Blocking Akses untuk Meningkatkan Keamanan Jaringan Kantor Desa Cibalandong Subang

Taufik Rahman[1*)], Rifqi Choiri Wardoyo[2)]
[1,2)] Teknologi Informasi, Universitas Bina Sarana Informatika
[1)] taufik@bsi.ac.id , [2)] kikichoiri123@gmail.com

ABSTRACT

Network security is a crucial aspect in protecting data and communications from external threats, especially in a village office environment that manages important information. This study aims to develop and implement a Mikrotik firewall to improve network security at the Cibalandong Village Office, Subang, with a focus on optimizing access blocking. The research methodology includes a literature study on the basic principles of firewalls and Mikrotik, analysis of specific needs of the Cibalandong Village Office, design and implementation of firewall configurations, and evaluation of system performance. The Mikrotik firewall configuration is designed to block unauthorized access while ensuring stable and efficient network connectivity. The test results show that the Mikrotik firewall successfully blocks unwanted access according to the rules applied, without reducing network performance. In addition, functional testing such as NAT, VPN, and QoS ensure that these features function as expected, and the system shows good recovery capabilities in the face of potential disruptions. Thus, the Mikrotik firewall proves to be an effective solution to improve network security at the Cibalandong Village Office. This study emphasizes the importance of implementing a proper network security system and shows that the Mikrotik firewall can be relied on to meet the needs of protection and access management in the context of a village office network. These findings support the use of Mikrotik firewall as an optimal tool to ensure network security and performance in similar environments.

***Keywords**: Firewall, Mikrotik, Blocking, Security, Network*

I. PENDAHULUAN

Dalam era digital saat ini, keamanan jaringan menjadi aspek penting dalam melindungi data dan komunikasi dari ancaman siber. Sebagai lembaga yang mengelola berbagai informasi penting, Kantor Desa Cibalandong Subang memerlukan sistem keamanan jaringan yang efektif. Firewall adalah komponen vital dalam melindungi jaringan dari akses yang tidak sah dan ancaman dari luar. Penggunaan Mikrotik sebagai solusi firewall menawarkan fleksibilitas dan kontrol yang tinggi dalam memblokir akses. Penelitian ini bertujuan untuk mengembangkan dan mengoptimalkan konfigurasi firewall Mikrotik guna meningkatkan keamanan jaringan di Kantor Desa Cibalandong, dengan fokus pada penerapan aturan blocking akses.

Kemajuan teknologi saat ini telah menjadikan internet sebagai elemen krusial dalam kehidupan masyarakat Indonesia, berfungsi sebagai sumber utama untuk memperoleh informasi, termasuk ilmu pengetahuan, hiburan, dan pendidikan(Yel et al., 2023). Seiring dengan pesatnya perkembangan teknologi informasi, penggunaan jaringan komputer semakin meningkat(Jamalul'ain & Nurdiawan, 2022). Jaringan computer untuk berbagai keperluan, baik bisnis maupun pribadi, seperti perbankan online dan media sosial. Namun, dengan meningkatnya jumlah jaringan komputer, ancaman keamanan juga semakin tinggi. Oleh karena itu, untuk memastikan kerahasiaan, integritas, dan aksesibilitas data, keamanan jaringan menjadi sangat vital(I. P. Saputra, 2022).

Sistem jaringan terdahulu di Kantor Desa Cibalandong Subang menggunakan perangkat keamanan yang sederhana, seperti router standar tanpa fitur keamanan canggih, sehingga rentan terhadap serangan siber. Metode perlindungan yang ada hanya berupa pengaturan dasar dengan pembatasan akses yang minim, tanpa kemampuan memonitor dan menganalisis lalu lintas jaringan secara real-time. Akibatnya, risiko kebocoran data dan

gangguan layanan meningkat, sementara pemblokiran akses ke situs-situs berbahaya sulit dilakukan secara efektif. Kinerja jaringan pun terpengaruh oleh lalu lintas yang tidak terkelola, menyebabkan lambatnya kecepatan akses internet dan peningkatan latency. Dengan adanya kebutuhan akan sistem keamanan yang lebih kuat, pengembangan firewall MikroTik menjadi solusi penting untuk meningkatkan keamanan jaringan, memblokir akses tidak diinginkan, serta mengelola bandwidth secara lebih efisien.

Firewall merupakan perangkat penting untuk memperkuat keamanan jaringan komputer dengan cara mencegah akses dari pihak yang tidak diinginkan dan mengontrol siapa saja yang dapat memasuki jaringan. Untuk memaksimalkan fungsi firewall pada Mikrotik RouterOS, dibutuhkan sistem firewall yang lebih kompleks. Sistem ini tidak hanya dapat memantau dan melaporkan akses jaringan secara real-time, tetapi juga mencegah akses yang tidak sah dan mengatur akses yang diizinkan, memungkinkan pengguna untuk merespons dengan cepat terhadap ancaman keamanan yang muncul.

II. TINJAUAN PUSTAKA

Mendeteksi serangan ataupun gangguan dari attacker serta menginvestigasi aktivitas yang dilakukan oleh attacker. Mikrotik Router ini digunakan untuk memblokir alamat IP maupun MAC address yang tidak dikenal, sehingga memantau keamanan jaringan wireless yang lebih efisien. Dalam penelitian ini, metode yang digunakan adalah menerapkan dan mengoptimalkan keamanan jaringan WLAN dengan menggunakan firewall filtering mac address yang tersedia(Jamalul'ain & Nurdiawan, 2022).

Mengimplementasikan web proxy pada Mikrotik untuk mencegah akses ke situs-situs yang tidak diinginkan, serta meningkatkan keamanan jaringan dengan menggunakan fitur firewall dan web proxy(Rozan et al., 2024).

Melihat secara komprehensif kemampuan *packet filtering* yang terdapat di *mikrotik routerboard* dalam mengatasi masalah keamanan jaringan komputer. *Filtering rule* mampu melakukan blok *url* yang ada pada *protocol HTTP* maupun *HTTPS* yang mana membuktikan bahwa kinerja dari *filtering rule* cukup baik, penelitian ini kinerja *packet filtering* menggunakan *tool network packet anayzer* Wireshark dengan cara melakukan capture paket yang lewat didalam jaringan dan menampilkan semua informasi secara detil (Muzakir & Ulfa, 2019).

Untuk menghindari monopoli bandwidth, dan memastikan bahwa setiap klien memiliki jatah bandwidth mereka sendiri. Meskipun ada perbedaan, jika Situs web yang dibuka termasuk situs web asusila, maka harus dibuat filter agar tidak dapat membuka situs tersebut. Namun, berdasarkan pengalaman dalam pembocoran situs, ada beberapa situs yang sekarang lebih mudah bocor, seperti menggunakan pemfilteran DNS Nawala dan web proxy mikrotik(Diansyah et al., 2019).

Mengembangkan keamanan jaringan komputer dengan berbagai metode, termasuk metode standar, keamanan port statis, keamanan port dinamis, dan keamanan port sticky. Keamanan port statis adalah keamanan jaringan yang bekerja secara otomatis dengan alamat MAC yang terdaftar pada setiap komputer, dan alamat MAC ini tidak dapat ditukar untuk setiap perangkat jaringan(Sulistyo & Sartomo, 2022).

Meminimalisir permasalahan yang ada kemungkian terjadi dengan perangkat Mikrotik dapat memanfaatkan pemblokiran situs dengan metode *layer 7* pada sistem jaringan Garage Freshmart(Syaripudin & Nugraha, 2023).

Mengatur *bandwidth*, mengatur *firewall*, mengatur notifikasi masalah jaringan, mengatur *wifi seamless*, mengatur *loop protect*, mengatur *failover link internet*, mengatur monitoring jaringan, maupun mengatur *tunneling*(Fritz Gamaliel & P. Yudi Dwi Arliyanto, 2022). Penelitian dengan investigasi forensik digital, yang terdiri dari tahap pengkoleksian, pemeriksaan, analisis dan pelaporan(Sutarti et al., 2023).

 DOI : https://doi.org/ 10.30646/sinus. v23i1.853

III. METODE PENELITIAN

Metode penelitian dalam pengembangan firewall MikroTik untuk meningkatkan keamanan jaringan Kantor Desa Cibalandong Subang terdiri dari beberapa langkah terstruktur untuk memperoleh hasil yang optimal. Berikut adalah langkah-langkah secara rinci:

1. Studi Literatur dan Analisis Kebutuhan

Langkah awal adalah melakukan studi literatur terkait firewall MikroTik dan protokol keamanan jaringan. Penelitian ini mencakup referensi dari jurnal, buku, dan sumber online yang membahas tentang fitur-fitur keamanan MikroTik, metode blocking akses, serta implementasi firewall pada jaringan skala kecil hingga menengah. Selanjutnya, analisis kebutuhan keamanan jaringan di Kantor Desa Cibalandong Subang, meliputi kerentanan dalam sistem jaringan, serta kebutuhan spesifik oleh firewall MikroTik.

2. Perancangan Sistem Firewall MikroTik

Berdasarkan hasil analisis kebutuhan, dilakukan perancangan sistem firewall MikroTik. Tahap ini melibatkan pemetaan arsitektur jaringan eksisting dan integrasi firewall dalam jaringan tersebut. Perancangan meliputi konfigurasi fitur-fitur firewall seperti Address List untuk memfilter alamat IP yang diizinkan atau diblokir, Layer 7 Protocol untuk mengelola dan memblokir akses ke situs web tertentu, serta konfigurasi NAT (Network Address Translation) dan Mangle untuk memprioritaskan dan mengelola lalu lintas jaringan.

3. Implementasi dan Pengujian Firewall

Setelah perancangan selesai, dilakukan implementasi firewall MikroTik pada jaringan Kantor Desa Cibalandong. Langkah implementasi instalasi perangkat, konfigurasi firewall sesuai dengan hasil perancangan, serta pengaturan fitur blocking akses dan manajemen bandwidth. Pengujian dilakukan untuk mengevaluasi efektivitas firewall dalam memblokir akses ke situs yang tidak diinginkan dan memantau lalu lintas jaringan.

4. Evaluasi Kinerja

Pada tahap ini, kinerja firewall MikroTik yang telah diimplementasikan dievaluasi berdasarkan beberapa indikator, seperti kecepatan akses internet, latency, dan keberhasilan dalam memblokir akses berbahaya. Data evaluasi diperoleh dengan memonitor lalu lintas jaringan selama periode tertentu, serta melakukan wawancara dengan staf IT kantor desa untuk mendapatkan masukan terkait peningkatan atau kendala yang dihadapi.

5. Analisis dan Pelaporan Hasil

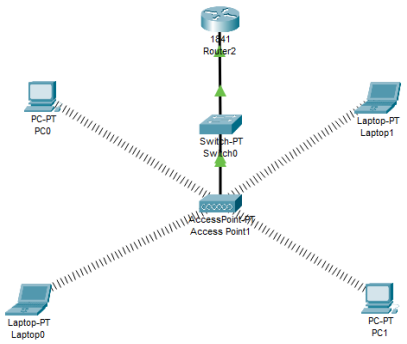
Setelah evaluasi, data yang diperoleh dianalisis untuk mengetahui dampak implementasi firewall terhadap keamanan dan kinerja jaringan. Analisis ini meliputi perbandingan antara kondisi jaringan sebelum dan setelah firewall diterapkan, serta identifikasi peningkatan atau penurunan yang terjadi.

Hardware dan Software

Untuk simulasi jaringan komputer, Anda memerlukan processor RADEON R5, 5 COMPUTE CORES 2C+3G 3.10 GHz, memori RAM 8 GB, hardisk 1 TB, monitor, keyboard, dan mouse, serta perangkat lunak yang dibutuhkan. Sistem operasi 64-bit Windows 10 dan aplikasi Winbox x64 digunakan pada jaringan komputernya.

Topologi Jaringan

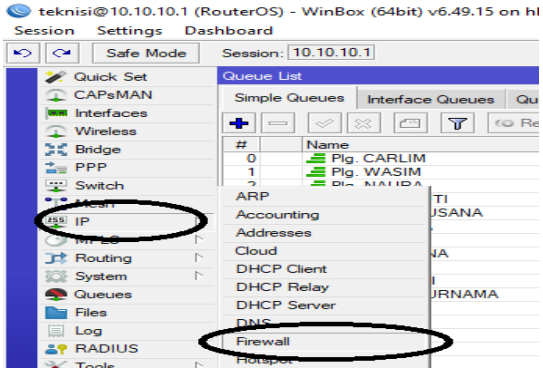
Untuk kantor desa Cibalandong Subang, topologi jaringan yang digunakan adalah topologi star, yang memungkinkan koneksi langsung antara dua perangkat, seperti menara pemancar internet dan kantor desa.



Gambar 1. Topologi Star yang digunakan di Desa Cibalandong

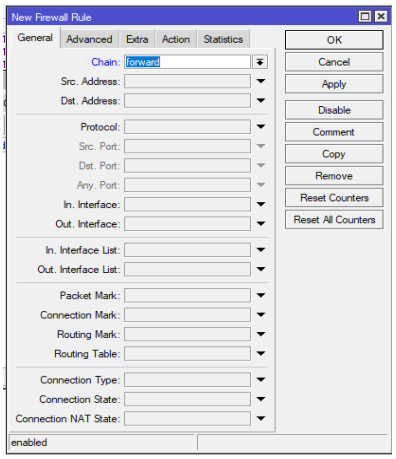
IV. HASIL DAN PEMBAHASAN

Hasil dan pembahasan implementasi firewall Mikrotik pada jaringan di Kantor Desa Cibalandong. Konfigurasi firewall Mikrotik memblokir akses yang tidak sah sesuai dengan aturan yang diterapkan, mencegah akses dari sumber yang tidak dikenal dan mengurangi potensi risiko keamanan. Dalam kasus ini memblokir situs-situs yang dianggap mengganggu kinerja jaringan karena banyaknya pengguna yang mengaksesnya. Situs yang diblokir adalah misal seperti detik.com Akses ke filter web dan konten firewall. Konfigurasi IP Firewall sebagai berikut:



Gambar 2. Tampilan Konfigurasi Filtering

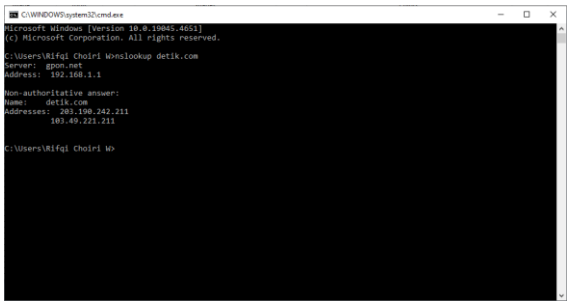
Untuk firewall filtering web, menggunakan menu winbox IP Firewall, yang ditunjukkan pada gambar 2. Salah satu fungsi firewall adalah untuk mengatur dan memantau paket data yang mengalir melalui jaringan komputer.



Gambar 3. Tampilan Konfigurasi Firewall Rule

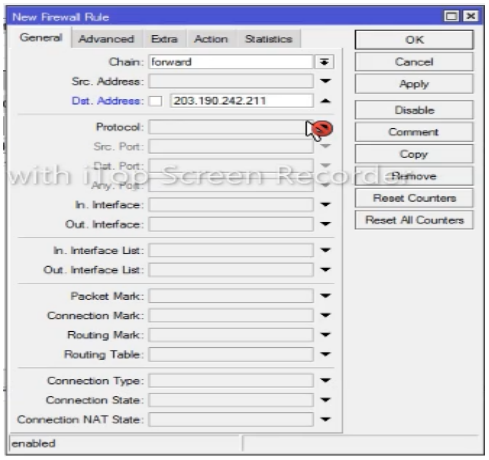
 DOI : https://doi.org/ 10.30646/sinus. v23i1.853

Gambar 3 menunjukkan tampilan awal proses filtering yang akan diblok. Tampilan firewall rule menampilkan menu umum, maju, tambahan, tindakan, dan statistik. Ada rantai khusus yang dapat digunakan untuk mengidentifikasi jenis lalu lintas yang akan diatur fitur firewall pada tampilan menu umum ini.



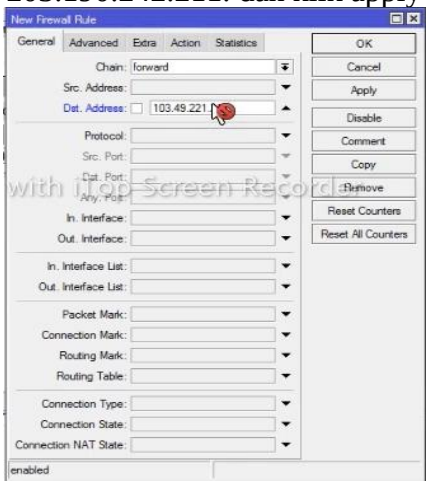
Gambar 4. Tampilan cmd nslookup

Pada gambar 4, Dengan menggunakan perintah nslookup pada CMD terdeteksi IP Address domain situs yang akan diblokir. Dalam kasus ini, mencoba memblokir detik.com dengan IP Address 203.190.242.211 dan 103.49.211.211



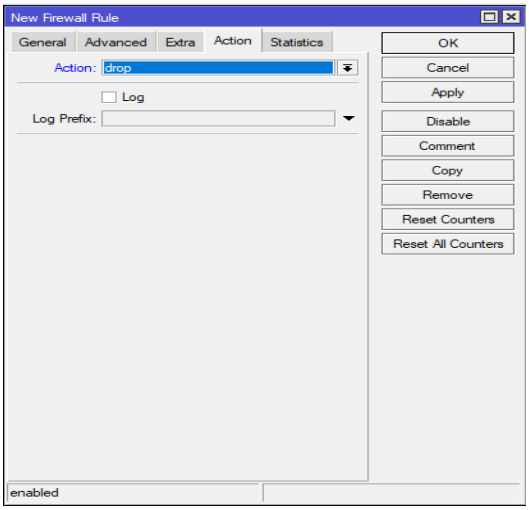
Gambar 5. Tampilan Destination Address

Selanjutnya, buka menu IP, pilih Firewall, lalu tab Filter Rules, klik Add (+), Chain: Forward, dan Alamat IP adalah 203.190.242.211. dan klik apply lalu klik ok.



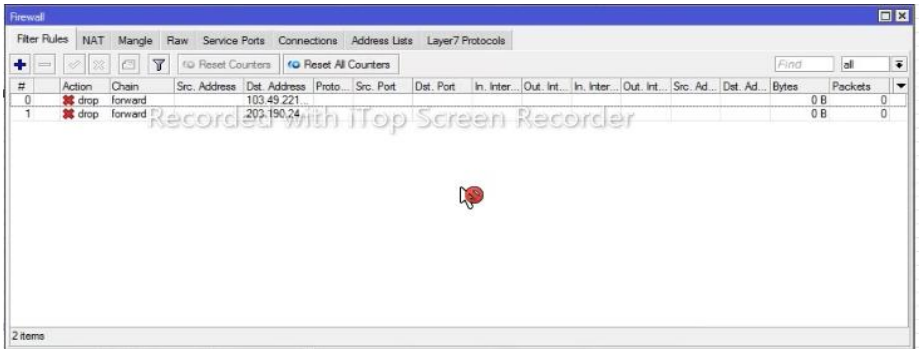
Gambar 6. Tampilan Destination Address

Selanjutnya, buka kembali menu IP, pilih Firewall, lalu tab Filter Rules, klik Add (+), Chain: Forward, dan Alamat IP adalah 103.49.211.211 dan klik apply dan klik ok.



Gambar 7. Tampilan Menu Action

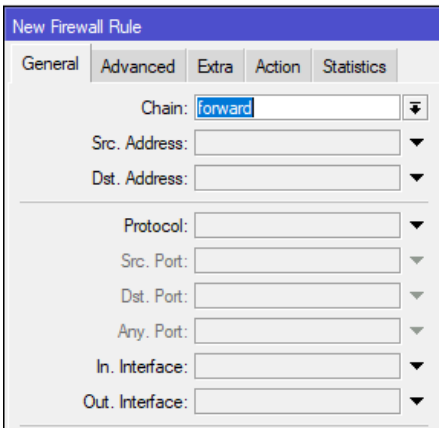
Kolom tindakan dengan berbagai opsi ditunjukkan pada gambar 7. Penulis hanya akan membahas salah satu menu, "drop", yang dapat digunakan untuk membuang paket yang akan masuk atau keluar ke router. Dengan menggunakan protokol ICMP, data yang dibuang dari router akan dibuang secara diam-diam tanpa mengirimkan pesan.



Gambar 8. List IP yang sudah di blokir

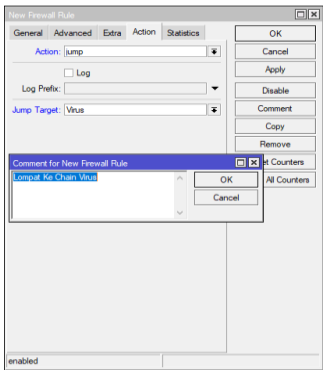
Pada antarmuka aplikasi WinBox menunjukkan bahwa ada sebuah aturan firewall yang diatur untuk menghentikan akses ke alamat IP tertentu, misalnya 203.190.242.211 dan 103.49.211.211. Aturan ini memiliki tindakan "drop", yang berarti bahwa paket data yang menuju ke alamat IP tersebut tidak akan dikirim atau dibuang.

Dengan firewall filter rule, dapat mengatur pemblokiran port-port yang sering dilewati virus. Mengkonfigurasi metode custom chain, Jump, yang berfungsi untuk melompat ke jalur yang telah ditetapkan pada paramater jump-target, untuk memblokir port-port yang sering dilewati virus. Ini dirancang untuk membuat rule-rule firewall lebih sederhana, dan juga untuk membuat administrasi jaringan Kantor Desa Cibalandong Subang lebih mudah jika ada banyak rule-rule. Proses konfigurasi custom chain adalah sebagai berikut.



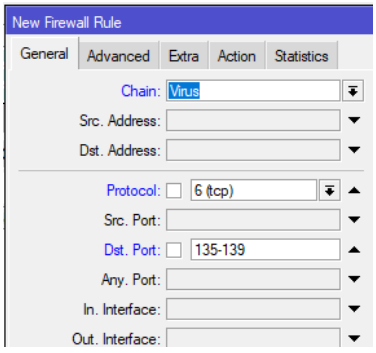
Gambar 9. Tampilan Firewall Rule

Pada Gambar 9 menunjukkan penggunaan forward untuk proses paket data yang melalui router. Proses ini mencakup koneksi dari public ke lokal atau sebaliknya.



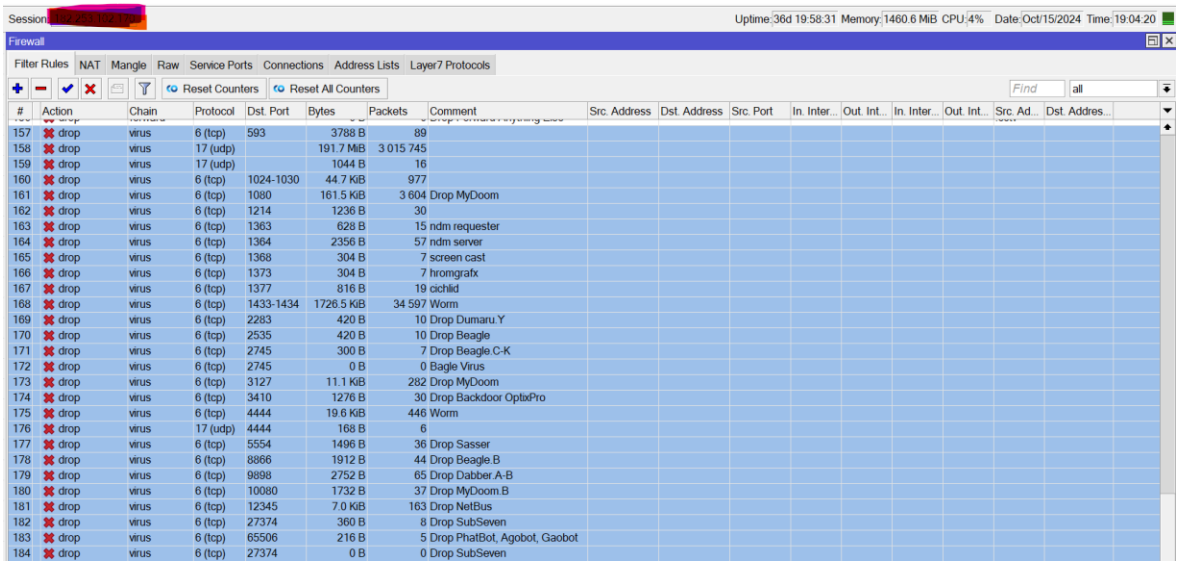
Gambar 10. Konfigurasi Jump

Pada gambar 10 action-jump diatur agar data yang melewati forward di lompatkan, sedangkan jump target virus adalah target dari forward. Beberapa parameter ditambahkan untuk membuat rantai aturan virus lebih spesifik.



Gambar 11. Rule Custom-Chain Virus

Beberapa komputer dapat berkomunikasi atau bertukar data melalui Protokol Pengendalian Transmisi (TCP) dan Protokol Datagram Pengguna (UDP). Menambahkan script berikut untuk rule protokol dan port yang sering digunakan virus:



#	Action	Chain	Protocol	Dst. Port	Bytes	Packets	Comment	Src. Address	Dst. Address	Src. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Addres...
157	drop	virus	6 (tcp)	593	3788 B	89										
158	drop	virus	17 (udp)		191.7 MiB	3 015 745										
159	drop	virus	17 (udp)		1044 B	16										
160	drop	virus	6 (tcp)	1024-1030	44.7 KiB	977										
161	drop	virus	6 (tcp)	1080	161.5 KiB	3 604	Drop MyDoom									
162	drop	virus	6 (tcp)	1214	1236 B	30										
163	drop	virus	6 (tcp)	1363	628 B	15	ndm requester									
164	drop	virus	6 (tcp)	1364	2356 B	57	ndm server									
165	drop	virus	6 (tcp)	1368	304 B	7	screen cast									
166	drop	virus	6 (tcp)	1373	304 B	7	hromgrafx									
167	drop	virus	6 (tcp)	1377	816 B	19	cichlid									
168	drop	virus	6 (tcp)	1433-1434	1726.5 KiB	34 597	Worm									
169	drop	virus	6 (tcp)	2283	420 B	10	Drop Dumaru.Y									
170	drop	virus	6 (tcp)	2535	420 B	10	Drop Beagle									
171	drop	virus	6 (tcp)	2745	300 B	7	Drop Beagle.C-K									
172	drop	virus	6 (tcp)	2745	0 B	0	Bagle Virus									
173	drop	virus	6 (tcp)	3127	11.1 KiB	282	Drop MyDoom									
174	drop	virus	6 (tcp)	3410	1276 B	30	Drop Backdoor OptixPro									
175	drop	virus	6 (tcp)	4444	19.6 KiB	446	Worm									
176	drop	virus	17 (udp)	4444	168 B	6										
177	drop	virus	6 (tcp)	5554	1496 B	36	Drop Sasser									
178	drop	virus	6 (tcp)	8866	1912 B	44	Drop Beagle.B									
179	drop	virus	6 (tcp)	9898	2752 B	65	Drop Dabber.A-B									
180	drop	virus	6 (tcp)	10080	1732 B	37	Drop MyDoom.B									
181	drop	virus	6 (tcp)	12345	7.0 KiB	163	Drop NetBus									
182	drop	virus	6 (tcp)	27374	360 B	8	Drop SubSeven									
183	drop	virus	6 (tcp)	65506	216 B	5	Drop PhatBot, Agobot, Gaobot									
184	drop	virus	6 (tcp)	27374	0 B	0	Drop SubSeven									

Gambar 12. Firewall Filter Rules

Port-port ini jarang digunakan untuk komunikasi dan rentan terhadap penyebaran virus dan malware. Kinerja Jaringan: Meskipun melakukan blocking akses, sistem firewall tidak mengakibatkan penurunan kinerja jaringan yang signifikan. Koneksi tetap stabil dan efisien. Pengelolaan Akses: Konfigurasi firewall memungkinkan pengaturan akses yang lebih baik untuk pengguna yang sah, sesuai dengan kebijakan yang ditetapkan.

Letak jump rule berada di urutan pertama, sedangkan rantai virus berada di urutan paling bawah. Ketika paket data melewati router, mereka akan diperiksa oleh aturan filter firewall. Saat proses pemeriksaan mencapai urutan 2, maka mereka akan melompat ke rantai virus di urutan 5. Paket data akan dibuang jika mengandung virus dengan protokol dan port yang ditetapkan pada rantai virus. Jika tidak mengandung virus, pemeriksaan akan dikembalikan ke atas dan dilanjutkan di rule berikutnya.

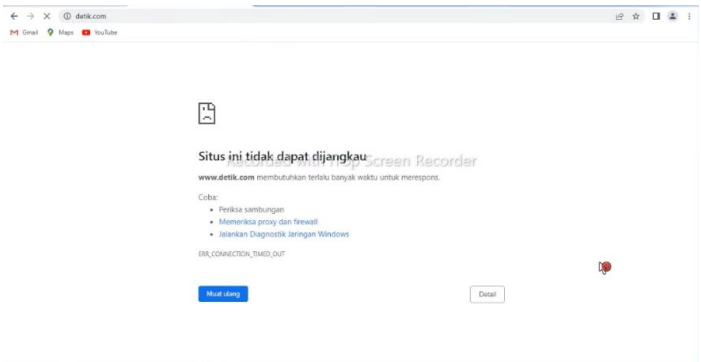
Pengujian Jaringan Awal

Sebelum pemfilteran situs dilakukan, pengujian jaringan awal dapat dilakukan. Sebagai contoh, penulis mengakses situs berita detik.com melalui komputer klien.

Gambar 13. Tampilan Web Sebelum Diblokir

Pengujian Aturan Blocking Akses

Setelah pemblokiran situs-situs tertentu yang dikonfigurasi dalam mikrotik dengan menggunakan program winbox, pengujian jaringan akhir dilakukan.



Gambar 14. Tampilan Web Sesudah Diblokir

Hasil pengujian sistem firewall MikroTik di Kantor Desa Cibalandong Subang menunjukkan bahwa firewall efektif dalam memblokir akses yang berbahaya seperti port, protokolyang sering digunakan lalu lintas oleh virus, dan mencegah serangan eksternal. Fitur Address List dan Layer 7 Protocol berhasil memfilter lalu lintas berbahaya, dan meningkatkan stabilitas jaringan. Pengujian keamanan menunjukkan firewall mampu mendeteksi dan mencegah serangan seperti port scanning dan brute force. Meskipun ada tantangan dalam konfigurasi awal yang kompleks, firewall MikroTik terbukti meningkatkan keamanan dan kinerja jaringan secara signifikan, sesuai dengan tujuan penelitian.

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian dan analisis yang telah dilakukan, dapat disimpulkan bahwa MikroTik sebagai perangkat router yang digunakan di Kantor Desa Cibalandong Subang terbukti efektif dalam mengoptimalkan blocking akses firewall. Dengan konfigurasi yang tepat, MikroTik berhasil memblokir situs-situs yang mengganggu kinerja jaringan serta mencegah penyebaran virus melalui pengaturan port dan protokol tertentu. Beberapa faktor penting yang perlu dipertimbangkan dalam pengoptimalan ini meliputi topologi jaringan star yang memudahkan pengembangan tanpa mengganggu operasi, pemilihan perangkat keras dan perangkat lunak yang sesuai seperti MikroTik dan Avira antivirus, serta keberlanjutan dan kemudahan manajemen jaringan. Implementasi blocking akses firewall tersebut telah berhasil meningkatkan keamanan jaringan, terbukti dengan berkurangnya akses ke situs-situs yang tidak diinginkan serta pencegahan penyebaran virus melalui port dan protokol yang rentan.

5.2 Saran

Saran untuk penelitian lanjutan yang diperlukan mencakup beberapa aspek penting untuk menyempurnakan hasil penelitian. Pertama, perlu ditingkatkan kesadaran keamanan dengan melatih staf di Kantor Desa Cibalandong tentang praktik keamanan siber dan penggunaan firewall secara tepat, serta implementasi pemantauan dan pemeliharaan jaringan secara rutin untuk mendeteksi dan merespons ancaman real-time. Selain itu, penilaian berkala terhadap konfigurasi firewall dan kebijakan keamanan perlu dilakukan melalui simulasi serangan dan uji coba skenario. Dokumentasi yang jelas mengenai konfigurasi firewall, kebijakan akses, dan prosedur respons insiden juga diperlukan untuk mempermudah pemeliharaan dan audit. Integrasi firewall dengan sistem keamanan lain, seperti IDS atau IPS, juga dapat meningkatkan perlindungan menyeluruh. Untuk penelitian lanjutan, disarankan melakukan evaluasi firewall Mikrotik di skala lebih besar dan berbagai organisasi untuk membandingkan hasil, serta melakukan analisis dampak jangka panjang terhadap performa dan keamanan jaringan. Studi keterhubungan teknologi dan

perbandingan solusi keamanan juga diperlukan untuk mengoptimalkan sistem secara keseluruhan. Selain itu, penelitian tentang pengembangan metodologi baru dan ancaman baru dapat memberikan wawasan tambahan untuk meningkatkan efektivitas pertahanan firewall Mikrotik di masa depan. Mengikuti saran ini akan membantu memperkuat keamanan jaringan dan memperluas pengetahuan di bidang keamanan jaringan.

DAFTAR PUSTAKA

Diansyah, T. M., Faisal, I., Lubis, A. J., & Chailoto, C. (2019). Pemanfaatan Layer 7 Pada Mikrotik Untuk Manajemen Bandwidth dan Blocking Situs. *Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)*, 610–614. https://seminar-id.com/semnas-sainteks2019.html

Fritz Gamaliel, & P. Yudi Dwi Arliyanto. (2022). Perancangan Manajemen Jaringan Komputer Berbasis Mikrotik Dengan Menggunakan Top Down Network Design. *Jurnal Informatika Dan Rekayasa Elektronik*, *5*(2), 230–243. https://doi.org/10.36595/jire.v5i2.693

I. P. Saputra, E. U. and A. H. M. (2022). Comparison of Anomaly Based and Signature Based Methods in Detection of Scanning Vulnerability. *2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 221–225. https://doi.org/10.23919/EECSI56542.2022.9946485

Jamalul'ain, A., & Nurdiawan, O. (2022). OPTIMALISASI KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN METODE KNOCKING PORT BERBASIS MIKROTIK (Studi Kasus: CV. Mitra Indexindo Pratama). *Jurnal Mahasiswa Teknik Informatika)*, *6*(2), 560–570.

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*(1), 15–20. https://doi.org/10.24176/simet.v10i1.2646

Rozan, M. A., Tahir, M., Qirani, A. P., Rizqiullah, N., Veranda, M., Puji, R., & Ghaffar, A. (2024). Implementasi Web Proxy Pada Mikrotik Untuk Mengoptimalkan Keamanan Jaringan Wireless Lan Di Lingkungan Sekolah Man 1 Gresik. *Jurnal Pendidikan Teknologi Informasi (JUKANTI)*, *7*(1), 180–188. https://doi.org/10.37792/jukanti.v7i1.1280

Sulistyo, W., & Sartomo, S. (2022). Model Keamanan Jaringan Menggunakan Firewall Port Blocking. *Krea-TIF: Jurnal Teknik Informatika*, *10*(1), 10–18. https://doi.org/10.32832/kreatif.v10i1.6678

Sutarti, Siswanto, & Bachtiar, A. (2023). Analisis Web Phishing Menggunakan Metode Network Forensic Dan Block Access Situs Dengan Router Mikrotik. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *10*(1), 71–83. https://doi.org/10.30656/prosisko.v10i1.7048

Syaripudin, A., & Nugraha, A. (2023). Analisa Dan Implementasi Blocking Website Dengan Metode 7 Layer Pada Perangkat Mikrotik Di Garage Freshmart: Analisa Dan Implementasi Blocking Website Dengan Metode 7 Layer Pada Perangkat Mikrotik Di …. *Jurnal Informatika MULTI*, *1*(4), 447–455. https://jurnal.publikasitecno.id/index.php/multi/article/view/91%0Ahttps://jurnal.publikasitecno.id/index.php/multi/article/download/91/59

Yel, M. B., Mulyana, D. I., F, J. R., Nurfaishal, M. D., & B, M. H. T. (2023). Optimalisasi Keamanan Firewall Pada Infrastruktur Jaringan Smk Idn Bogor. *Jurnal Cahaya Mandalika*, *4*(1), 594–610. https://www.ojs.cahayamandalika.com/index.php/JCM/article/view/1393