

IMPLEMENTASI FIREWALL PADA MIKROTIK UNTUK KEAMANAN JARINGAN

Bintang Cahya¹, Febrian Rizki Adi Sutiyo², Yoga El Saputra³, Muhammad Elfarizi⁴

¹Teknik Informatika/UIN SUSKA Riau, Jl.HR.Subrantas, Cahyabintang212@gmail.com

²Teknik Informatika/UIN SUSKA Riau, Jl.HR.Subrantas, Febrianrizkiadisutiyo@gmail.com

³Teknik Informatika/UIN SUSKA Riau, Jl.HR.Subrantas, Yogaelsaputra04@gmail.com

⁴Teknik Informatika/UIN SUSKA Riau, Jl.HR.Subrantas, Muhammadelfarizi777@gmail.com

ABSTRACT

Pada saat ini perkembangan teknologi informasi sangat pesat. jaringan komputer sudah menjadi bagian penting dalam kehidupan sehari-hari. Meskipun perkembangan ini membawa banyak kemudahan dan manfaat, namun juga membawa tantangan baru terutama dalam hal keamanan jaringan. Keamanan jaringan sangat penting karena informasi sensitif dan data pribadi terus melewati infrastruktur jaringan. Keamanan jaringan merupakan suatu metode yang mengharuskan organisasi untuk mengantisipasi potensi ancaman. Sistem Operasi bernama Mikrotik RouterOS adalah sebuah perangkat lunak yang bisa digunakan pada komputer agar komputer bisa menjadi sebuah router jaringan yang hebat dalam hal fitur yang dibuat untuk ip network dan jaringan nirkabel, serta sangat pas bila digunakan oleh ISP dan provider Hotspot. Firewall adalah teknologi keamanan siber yang digunakan untuk meningkatkan keamanan komputer yang terhubung ke jaringan, seperti Jaringan Area Lokal (LAN) atau Internet. Setelah mengimplementasikan firewall hasil yang diperoleh adalah website yang ditentukan, hasilnya implementasi firewall dalam memblok website berhasil diterapkan dan terbukti berhasil.

Keywords: Mikrotik, Firewall, Keamanan Jaringan,

This work is licensed under a Creative Commons Attribution 4.0 International License.



I. PENDAHULUAN

Pada saat ini perkembangan teknologi informasi sangat pesat (Hairun et al., 2023). jaringan komputer sudah menjadi bagian penting dalam kehidupan sehari-hari. Meskipun perkembangan ini membawa banyak kemudahan dan manfaat, namun juga membawa tantangan baru terutama dalam hal keamanan jaringan. Keamanan jaringan sangat penting untuk melindungi data (Yudi mulyanto et al., 2021). Keamanan jaringan sangat penting karena informasi sensitif dan data pribadi terus melewati infrastruktur jaringan. Keamanan jaringan merupakan suatu metode yang mengharuskan organisasi untuk mengantisipasi potensi ancaman (Andoro et al., 2022).

Berkembangnya teknologi yang semakin cepat membuat keamanan jaringan perlu diperhatikan. Keamanan jaringan komputer merupakan bagian yang sangat penting dalam suatu sistem (Arta et al., 2018). Pada dasarnya ada beberapa kerentanan dalam keamanan jaringan komputer(Rizal et al., 2020). Penelitian yang dilakukan oleh (Rizal et al., 2020) membahas keamanan jaringan menggunakan metode Port Blocking dan Port Knocking, kelebihan dari metode ini Kelebihan port knocking adalah dapat dikonfigurasi secara manual ke port knocking (dikonfigurasi sebagai knocking) dan server Mikrotik dapat diakses dari mana saja selama terhubung dengan jaringan .

Jika tidak selektif mengaktifkan semua port yang sedang digunakan, maka virus dan malware dapat menyebar di jaringan komputer, untuk melindungi jaringan dari penyebaran virus dan malware, dapat menutup port komunikasi yang tidak digunakan dan port komunikasi yang rentan terhadap eksloitasi virus (Irawan, 2015).

Keamanan jaringan adalah salah satu pertimbangan terpenting ketika mengimplementasikan jaringan komputer. Tanpa adanya keamanan jaringan maka jaringan komputer tidak akan bisa beroperasi (Santoso et al., 2022). Kelalaian pengelola dalam membangun jaringan komputer dapat mengakibatkan berbagai masalah. Kelalaian ini dapat memungkinkan peretas meretas dan merusak jaringan yang dibangun. Keamanan jaringan yang sedang dibangun perlu diperkuat untuk mencegah penyalahgunaan jaringan oleh hacker (Amarudin, 2018) (Putra & Ramdhani, 2021).

Untuk itu dalam penelitian ini kami menggunakan metode firewall. Adapun penelitian keamanan yang menggunakan metode firewall dilakukan (Astari, 2018) menggunakan metode filtering firewall menggunakan MikroTik. Hasilnya, link yang berbau pornografi atau media sosial berhasil diblokir, dan link yang tidak berbau pornografi atau media sosial tidak diblokir dan berhasil mengisi link yang dimaksud.

II. LITERATURE REVIEW

1.1 Mikrotik

Sistem Operasi bernama Mikrotik RouterOS adalah sebuah perangkat lunak yang bisa digunakan pada komputer agar komputer bisa menjadi sebuah router jaringan yang hebat dalam hal fitur yang dibuat untuk ip network dan jaringan nirkabel, serta sangat pas bila digunakan oleh ISP dan provider Hotspot (Muin et al., 2017). Mikrotik dapat digunakan sebagai firewall (Pamuji et al., 2020). Mikrotik adalah perangkat jaringan perangkat lunak dan perangkat keras yang dapat memfilter, mengalihkan, dan beroperasi sebagai router, di antara fungsi-fungsinya (Amarudin, 2018).

MikroTik adalah perusahaan Latvia yang mengkhususkan diri dalam pengembangan perangkat keras dan perangkat lunak untuk jaringan komputer. Produk utama MikroTik meliputi perangkat router dan sistem penyedia layanan Internet nirkabel (ISP nirkabel). Sistem operasi yang digunakan perangkat MikroTik adalah sistem operasi berbasis Linux yang disebut RouterOS. MikroTik RouterOS menawarkan berbagai fitur routing dan switching yang canggih dan populer di kalangan pengguna jaringan yang membutuhkan solusi yang andal dan terjangkau. RouterBOARD adalah rangkaian perangkat keras MikroTik yang mendukung RouterOS dan mencakup berbagai model mulai dari router kecil hingga perangkat rak untuk jaringan besar. Produk MikroTik banyak digunakan di berbagai ukuran jaringan, mulai dari rumah tinggal hingga perusahaan besar.

1.2 Metode Firewall

Firewall adalah teknologi keamanan siber yang digunakan untuk meningkatkan keamanan komputer yang terhubung ke jaringan, seperti Jaringan Area Lokal (LAN) atau Internet (Akbar & Permana, 2019). Firewall atau dalam Bahasa Indonesia diartikan sebagai Dinding Api adalah alat yang dapat mengurangi lubang keamanan dalam suatu organisasi computer. Perancangan

yang dibuat bisa memenuhi standar kerangka kerja, terutama dalam pembatasan penggunaan kuota data, serta dapat digunakan untuk menyaring informasi yang masuk melalui router (Andoro et al., 2022). Firewall telah terbukti dapat melindungi jaringan dengan menyaring data secara selektif untuk meningkatkan kinerja sistem (Putra & Ramdhani, 2021). Keamanan jaringan menggunakan firewall penting untuk melindungi sistem dan data dari ancaman dunia maya. Firewall berfungsi sebagai garis pertahanan pertama Anda, memantau dan mengendalikan lalu lintas antara jaringan internal dan eksternal. Untuk meningkatkan efisiensi firewall pada Mikrotik RouterOS, diperlukan sistem firewall yang lebih kompleks (Pratomo, 2023). Dengan menetapkan kebijakan akses yang ketat, firewall mencegah akses tidak sah dan melindungi dari serangan seperti malware, penolakan layanan (DoS), dan serangan lainnya. Selain itu, firewall juga memungkinkan deteksi dan pemantauan aktivitas mencurigakan, memberikan lapisan pertahanan tambahan terhadap potensi ancaman dunia maya. Dengan menerapkan firewall yang efektif, organisasi dapat mengurangi risiko keamanan dan menjaga kelangsungan operasional dan integritas data di lingkungan jaringan mereka.

Firewall menggunakan berbagai metode untuk melindungi jaringan Anda dari ancaman dunia maya. Metode utamanya adalah

- 1. Pemfilteran Paket**

Firewall memeriksa semua paket data yang melewati jaringan berdasarkan aturan tertentu, seperti: Alamat IP, nomor port, dan protokol. Paket yang tidak memenuhi kriteria ini mungkin diblokir.

- 2. Stateful Inspection**

Firewall tidak hanya mempertimbangkan paket individual, namun juga mengingat status koneksi. Hal ini memungkinkan firewall untuk memahami konteks lalu lintas dan memutuskan apakah akan menerima atau menolak paket berdasarkan status koneksi sebelumnya.

- 3. Pemfilteran Proxy**

Firewall bertindak sebagai perantara antara pengguna dan sumber daya eksternal. Periksa dan filter lalu lintas data untuk mengurangi kemungkinan serangan langsung pada server internal.

- 4. Deep Packet Inspection (DPI)**

Firewall memeriksa isi sebenarnya dari paket data untuk mendeteksi dan mencegah ancaman seperti malware. Hal ini memerlukan analisis rinci tentang isi paket, bukan hanya headernya.

5. Terjemahan Alamat Jaringan (NAT)

Firewall menggunakan NAT untuk menyembunyikan alamat IP internal dari luar jaringan. Hal ini meningkatkan keamanan dengan membuat alamat IP internal Anda tidak terlihat oleh pihak luar.

6. Virtual Private Network (VPN)

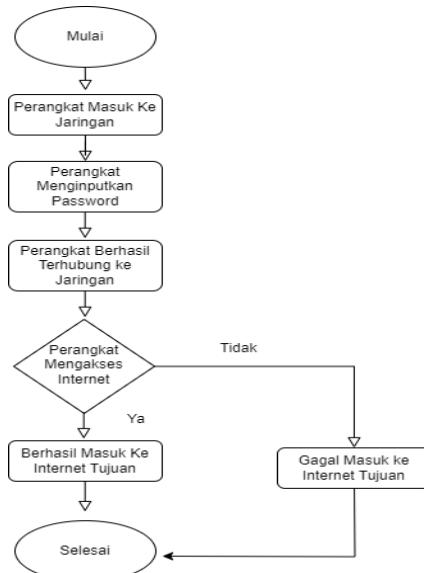
Firewall dapat mendukung implementasi VPN yang menyediakan saluran terenkripsi untuk mengamankan komunikasi antara lokasi yang terpisah secara fisik.

7. Logging dan Pemantauan

Firewall mencatat aktivitas lalu lintas sehingga administrator dapat memantau dan merespons kejadian mencurigakan dengan cepat.

III. METHODOLOGY

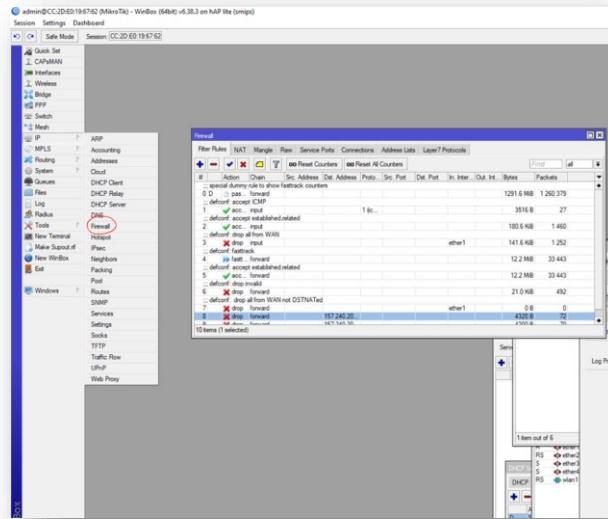
Pengumpulan informasi mencakup tinjauan literatur dan survei. Penelitian literatur digunakan untuk mengumpulkan informasi dengan mengumpulkan tulisan, artikel, esai, dan bacaan yang berkaitan dengan keamanan komputer. Penelitian saat ini terdiri dari observasi langsung. Aktivitas ini mengarsipkan poin-poin penting yang diidentifikasi dalam lingkungan dan peralatan aktual, hubungan perangkat keras satu sama lain, penggunaan media transmisi, perencanaan alamat IP, konektivitas web, dan pendekatan penggunaan web.



Gambar 1. Langkah-langkah penelitian

Berikut langkah-langkah dalam implementasi penggunaan firewall dalam memblok situs web.

1. Akses menu firewall



Gambar 2 Menu Firewall

2. Cek ip address web yang ingin kita blok menggunakan perintah nslookup pada cmd

```
C:\Users\Febrian Rizky>nslookup instagram.com
Server:  router
Address: 192.168.88.1
Non-authoritative answer:
Name:  instagram.com
Addresses:  2a03:2880:f24d:e0:face:b00c:0:4420
          157.240.208.174
```

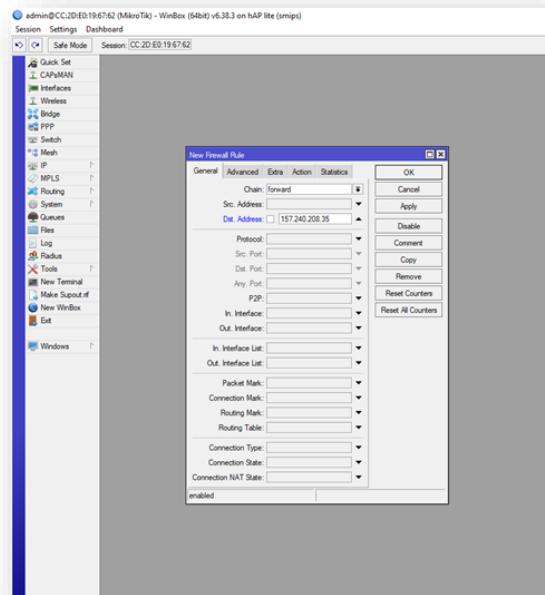
Gambar 3 Cek Ip Address Pada Cmd

3. Klik tombol tambah

#	Add	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
... special dummy rule to show fasttrack counters												
0	D	pas...	forward								1306.6 MB	1 275 402
1	✓ acc...	input			1 (c...						3516 B	27
2	✓ acc...	input									181.8 kB	1 468
3	✗ drop	input						ether1			145.3 kB	1 285
4	✗ fast...	forward									12.3 kB	33 967
5	✓ acc...	forward									12.3 kB	33 967
6	✗ drop	forward									21.0 kB	492
7	✗ drop	forward						ether1			0 B	0
8	✗ drop	forward		157.240.20...							4440 B	74
9	✗ drop	forward		157.240.20...							4300 B	74
10 items (1 selected)												

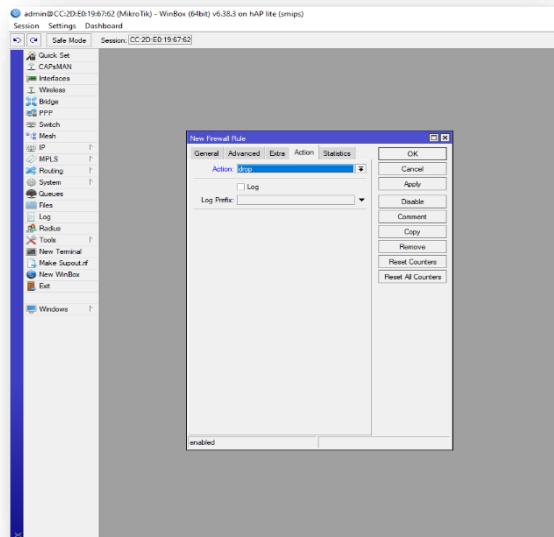
Gambar 4 Menu Tambah Firewall

- Pada new Firewall Rules menu General isi Dst. Address dengan Alamat IP Facebook.com



Gambar 5 New Firewall Rules Menu General

5. Pilih menu action, isi action dengan drop



Gambar 6 New Firewall Rules Menu Action

6. Filter rules untuk memblokir website facebook dan Instagram sudah masuk

Order	Action	Chain	Src. Address	Dst. Address	Proto.	Src. Port	Dst. Port	In. Inter.	Out. Int.	Bytes	Packets
0	drop	forward						1260.6 MB	1 220 109		
1	deforw accept ICMP	forward						3516 B	27		
2	deforw accept established,related	forward						172.1 KB	1 395		
3	deforw accept input	input						137.1 KB	1 212		
4	deforw accept wan	input						12.1 MB	32 626		
5	deforw forward	forward						12.1 MB	32 626		
6	deforw accept established,related	forward						20.7 KB	405		
7	deforw accept input	input						0 B	0		
8	drop	forward		157.240.20...				3600 B	60		

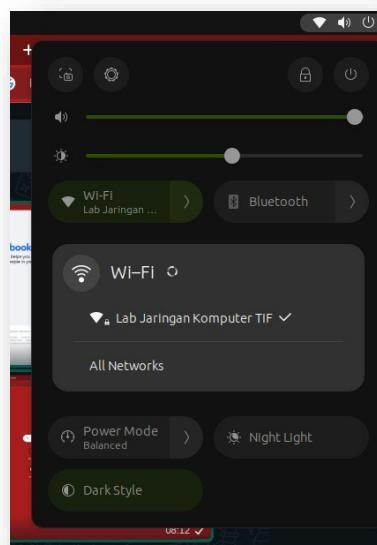
Gambar 7 Filter Rules

7. Lakukan hal sama untuk Instagram.com

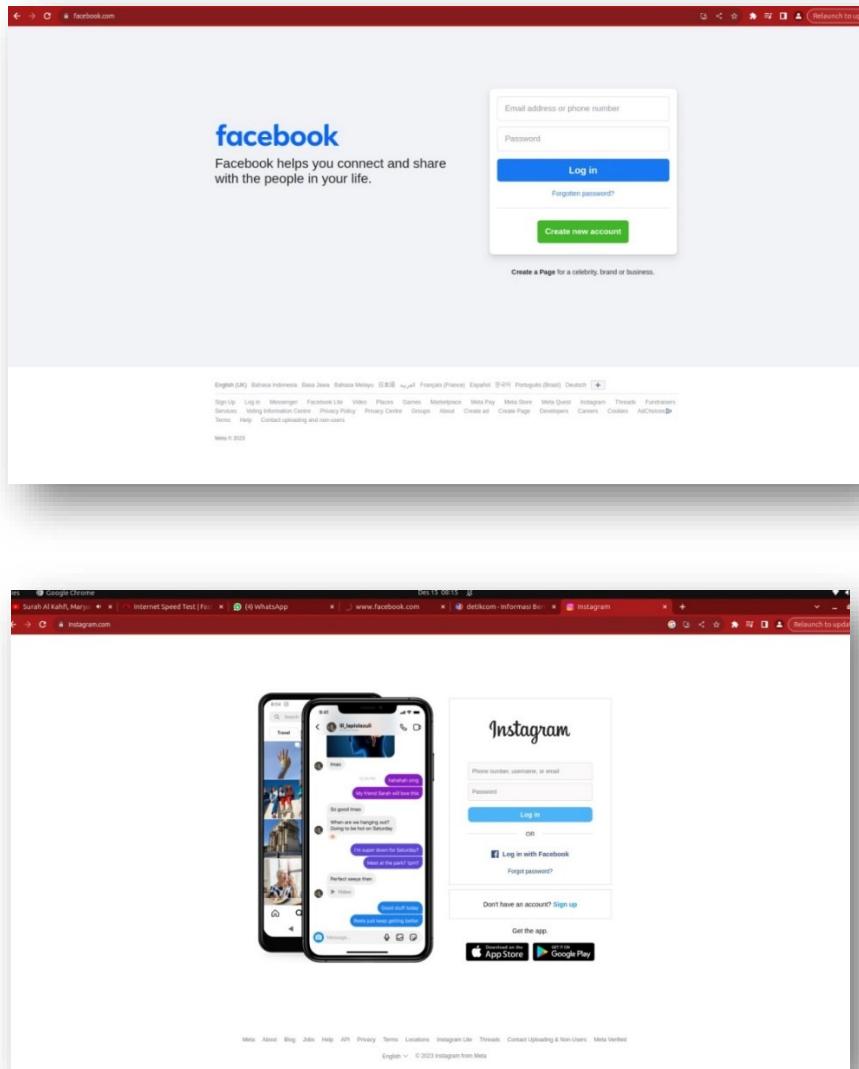
IV. RESULTS AND ANALYSIS

Implementasi firewall memiliki dampak positif pada keamanan jaringan. Dengan kemampuannya mengendalikan lalu lintas, mencegah akses tidak sah, dan mendeteksi serangan dunia maya, firewall memberikan perlindungan yang efektif. Melalui pemeriksaan paket dan metode pemantauan aktif, firewall dengan cepat mendeteksi dan merespons ancaman, memberikan lapisan pertahanan yang kuat terhadap potensi serangan seperti malware dan penolakan layanan. Setelah mengimplementasikan firewall hasil yang diperoleh adalah website yang ditentukan berhasil diblok dan tidak dapat diakses. Adapun pengujinya sebagai berikut.

1. Uji coba menggunakan computer yang terhubung dengan jaringan yang dirancang

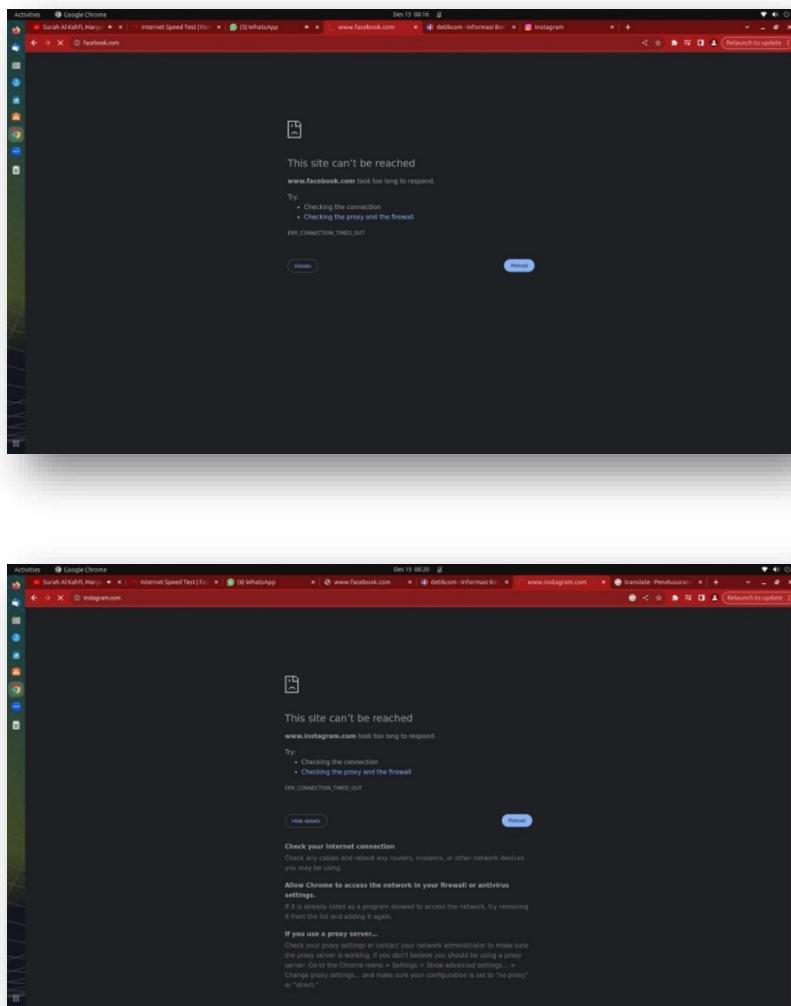


Gambar 8 Jaringan Yang Digunakan



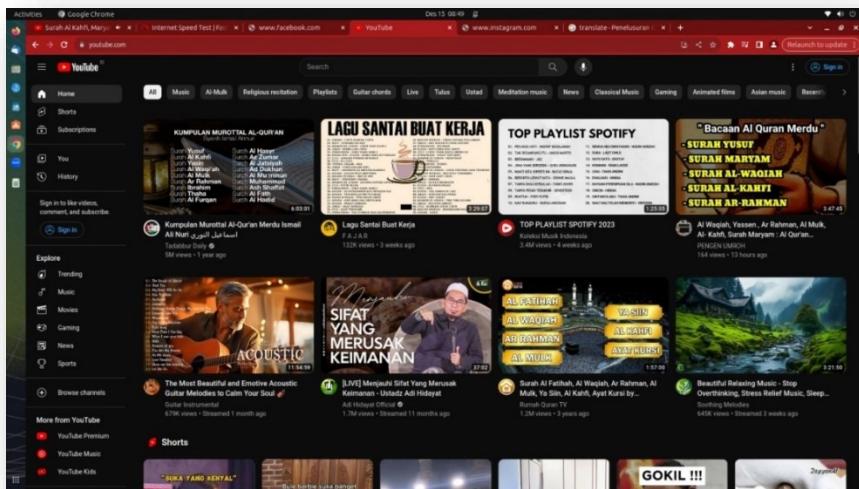
Gambar 9 Tampilan Website Sebelum Menerapkan Firewall

2. Setelah menerapkan firewall



Gambar 10 Tampilan Website Setelah Menerapkan Firewall

3. Mengakses website yang tidak di blok



Gambar 11 Tampilan Mengakses Website Yang Tidak Diblok

V. KESIMPULAN DAN SARAN

Pesatnya perkembangan teknologi informasi menjadikan jaringan komputer sebagai elemen penting dalam kehidupan sehari-hari. Keamanan jaringan merupakan aspek penting dalam melindungi data sensitif dan pribadi yang terus melintasi infrastruktur jaringan. Dalam situasi seperti ini, langkah-langkah keamanan seperti firewall adalah solusi yang efektif. Penelitian ini menekankan pentingnya keamanan jaringan komputer, dengan penekanan khusus pada keamanan menggunakan metode firewall saat menggunakan perangkat MikroTik. Pentingnya keamanan jaringan tergambar dari risiko yang dapat timbul akibat kecerobohan dalam pembangunan jaringan komputer, termasuk kemungkinan serangan hacker. Oleh karena itu, penerapan metode firewall khususnya dengan MikroTik merupakan langkah efektif untuk mengurangi risiko dan menjaga integritas data. Oleh karena itu, penelitian ini memberikan kontribusi terhadap pemahaman keamanan jaringan komputer dan memberikan dasar untuk pengembangan lebih lanjut untuk melindungi sistem dan data dari ancaman dunia maya. Hasilnya implementasi firewall dalam memblok website berhasil diterapkan dan terbukti berhasil.

DAFTAR PUSTAKA

- Akbar, S., & Permana, I. (2019). Implementasi Firewall Dengan Mikrotik Pada Smk Pgri 11 Ciledug. *IDEALIS: InDonEsiA JournaL Information ...*, 119–125. <https://jom.fti.budiluhur.ac.id/index.php/IDEALIS/article/view/2425%0Ahttps://jom.fti.budiluhur.ac.id/index.php/IDEALIS/article/download/2425/934>
- Amarudin. (2018). Analisis Dan Implementasi Keamanan Jaringan Pada Mikrotik Router Menggunakan Metode Port Knocking. *Seminar Nasional Sains Dan Teknologi 2018*, 1–7.
- Andoro, I. F. B., Agung Budijanto, H., & Aidjili, M. (2022). Analisa Keamanan Jaringan Dengan Mikrotik. *RISTEK: Jurnal Riset, Inovasi Dan Teknologi Kabupaten Batang*, 6(2), 35–39. <https://doi.org/10.55686/ristik.v6i2.111>
- Arta, Y., Syukur, A., & Kharisma, R. (2018). Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik. *It Journal Research and Development*, 3(1), 104–114. [https://doi.org/10.25299/itjrd.2018.vol3\(1\).1346](https://doi.org/10.25299/itjrd.2018.vol3(1).1346)
- Astari, A. A. (2018). Implementasi Keamanan Jaringan Dengan Metode Firewall Filtering Menggunakan Mikrotik. *Jurnal Simki-Techsain*, 02(01), 9. http://simki.unpkediri.ac.id/mahasiswa/file_artikel/2018/49b68be9ba26a905f0a3b0883b428eb4.pdf
- Hairun, A. N., Katili, M. R., Takdir, R., & Tuloli, M. S. (2023). *Penerapan firewall di router OS mikrotik pada aplikasi e-rapor*. 5(2), 108–119. <https://doi.org/10.37905/jji>.
- Irawan, D. (2015). Keamanan jaringan komputer dengan metode blocking port pada laboratorium komputer program diploma-iii sistem informasi universitas muhammadiyah metro. *Manajemen Informatika Program Diploma III UM Metro*, 02(05), 1–9.
- Muin, M. A., Sugiantoro, B., Amikom Yogyakarta, S., Sunan, U., & Yogyakarta, K. (2017). "TRANSFORMASI Jurnal Informasi & Pengembangan Iptek" (STMIK BINA PATRIA) IMPLEMENTASI FIREWALL DENGAN MENGGUNAKAN MIKROTIK ROUTEROS™ (Studi Kasus : STMIK Bina Patria). *Jurnal TRANSFORMASI*, 13(1), 58–61. www.facebook.com
- Pamuji, S. A., Iswahyudi, C., & Informatika, T. (2020). Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus Di Taman Pintar Yogyakarta. *Jurnal JARKOM*, 7(1), 65–75.
- Pratomo, A. B. (2023). Pengembangan Sistem Firewall Pada Jaringan Komputer Berbasis Mikrotik Routeros Developing a Firewall System on a Computer Network Based on Mikrotik Routeros. *Bulletin of Network Engineer and Informatics (Bufnets)*, 1(2), 51–59. <https://doi.org/10.59688/bufnets>
- Putra, S. P., & Ramdhani, Y. (2021). Memanfaatkan Fitur Firewall Rules Pada Mikrotik Untuk Keamanan Jaringan Di Hotel Lenora Bandung. *EProsiding Teknik Informatika (PROTEKTIF)*, 2(1), 122–126. <https://eprosiding.ars.ac.id/index.php/pti>

- Rizal, R., Ruuhwan, R., & Nugraha, K. A. (2020). Implementasi Keamanan Jaringan Menggunakan Metode Port Blocking dan Port Knocking Pada Mikrotik RB-941. *Jurnal ICT : Information Communication & Technology*, 19(1), 1–8. <https://doi.org/10.36054/jict-ikmi.v19i1.119>
- Santoso, N. A., Affandi, K. B., & Kurniawan, R. D. (2022). Implementasi Keamanan Jaringan Menggunakan Port Knocking. *Jurnal Janitra Informatika Dan Sistem Informasi*, 2(2), 90–95. <https://doi.org/10.25008/janitra.v2i2.156>
- Yudi mulyanto, M. Julkarnain, & Jabi Afahar, A. (2021). Implementasi Port Knocking Untuk Keamanan Jaringan Smkn 1 Sumbawa Besar. *Jurnal Informatika Teknologi Dan Sains*, 3(2), 326–335. <https://doi.org/10.51401/jinteks.v3i2.1016>