

SIMULASI UJI KEAMANAN JARINGAN WINDOWS 7 BLOKIR AKSES SITUS DENGAN METODE LAYER 7 PROTOCOL BERBASIS MIKROTIK DALAM VIRTUALBOX

Fauzan Jagi Daniswara^{1*}, Apriade Voutama²

^{1,2} Sistem Informasi, Fakultas Ilmu Komputer, Universita Singaperbangsa Karawang
Jl. HS. Ronggowaluyo, Telukjambe Timur, Karawang

Keywords:

Keamanan Jaringan,
MikroTik, Layer 7 Protocol,
Blokir Akses, VirtualBox

Correspondent Email:

fauzanjagi23@gmail.com

Abstrak: Keamanan jaringan merupakan elemen vital dalam pengelolaan sistem informasi, terlebih lagi pada sistem operasi lama seperti Windows 7 yang memiliki banyak kerentanan. Mikrotik sebagai perangkat manajemen jaringan menyediakan fitur firewall dan Layer 7 Protocol yang dapat dimanfaatkan untuk memblokir akses ke situs tertentu secara cerdas berbasis pola konten. Penelitian ini bertujuan untuk mensimulasikan pengujian keamanan jaringan dengan pendekatan pemblokiran akses menggunakan Layer 7 Protocol dalam lingkungan virtual menggunakan Oracle VM VirtualBox. Metode yang digunakan mencakup instalasi dan konfigurasi sistem virtual, penerapan Mikrotik sebagai pengendali lalu lintas jaringan, serta penyusunan aturan firewall berbasis Layer 7. Hasil pengujian menunjukkan bahwa konfigurasi firewall dengan Layer 7 Protocol mampu secara efektif membatasi akses ke situs-situs yang telah ditentukan dan mencatat aktivitas pemblokiran secara real-time melalui log keamanan Mikrotik. Penelitian ini memberikan kontribusi penting bagi pengembangan sistem keamanan jaringan berbasis virtual sebelum diterapkan pada jaringan produksi..

Abstract: Network security is a vital element in managing information systems, especially on legacy operating systems such as Windows 7 which have many vulnerabilities. Mikrotik as a network management device provides firewall and Layer 7 Protocol features that can be used to intelligently block access to certain sites based on content patterns. This study aims to simulate network security testing with an access blocking approach using Layer 7 Protocol in a virtual environment using Oracle VM VirtualBox. The methods used include the installation and configuration of virtual systems, the implementation of Mikrotik as a network traffic controller, and the preparation of Layer 7-based firewall rules. The test results show that the firewall configuration with Layer 7 Protocol is able to effectively limit access to predetermined sites and record blocking activities in real-time through the Mikrotik security log. This study provides an important contribution to the development of virtual-based network security systems before being applied to production networks.

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini berlangsung sangat pesat, khususnya dalam

bidang komputer dan internet, yang memberikan kemudahan dalam menghubungkan berbagai belahan dunia melalui jaringan yang tidak

mengenal batas wilayah. [1]. simulasi ini bertujuan untuk mengevaluasi efektivitas pemblokiran akses dengan metode Layer 7 Protocol dalam upaya meningkatkan kinerja filter rule di router Mikrotik. Router Mikrotik dapat memanfaatkan fitur Layer 7 Protocol untuk memblokir akses ke situs-situs tertentu berdasarkan pola data yang dikenali, sehingga meningkatkan keamanan jaringan.[2]. Website saat ini menjadi salah satu sarana utama dalam menyampaikan informasi dan menyediakan layanan digital, baik untuk keperluan individu maupun instansi. Namun demikian, keberadaan website juga memiliki risiko terhadap berbagai serangan siber yang dapat merusak data, mengganggu sistem, serta menimbulkan kerugian bagi penggunanya. Oleh sebab itu, penting dilakukan pengujian keamanan secara rutin pada website untuk mengidentifikasi kerentanan sistem, guna mencegah potensi kerugian yang disebabkan oleh celah keamanan yang tidak terdeteksi.[3]. Jaringan komputer adalah sebuah sistem telekomunikasi yang menghubungkan sejumlah komputer agar dapat saling berinteraksi dan berbagi data. Sistem ini bertujuan untuk memungkinkan setiap perangkat yang tergabung di dalamnya dapat meminta maupun menyediakan layanan. Dalam jaringan tersebut, perangkat yang menerima layanan disebut sebagai client, sedangkan perangkat yang memberikan layanan dikenal dengan sebutan server. [4]. Salah satu upaya pencegahan terhadap akses situs-situs bermuatan negatif, khususnya yang mengandung konten pornografi, dapat dilakukan dengan cara memblokir situs-situs tersebut secara permanen. Pemblokiran ini dapat diterapkan menggunakan perangkat Mikrotik.[5]. penggunaan VirtualBox dalam simulasi ini memungkinkan pengujian berbagai skenario keamanan tanpa mengganggu operasional jaringan yang sebenarnya. Fleksibilitas ini mempermudah pengembangan serta pengujian solusi keamanan yang dapat diterapkan dalam lingkungan manapun [6].

Dalam konteks pengujian keamanan jaringan Windows 7, metode pemblokiran akses berbasis Mikrotik terbukti menjadi strategi yang dapat

diandalkan untuk melindungi sistem dari potensi ancaman eksternal. Dengan demikian, organisasi atau perusahaan dapat memastikan bahwa data mereka tetap aman dan terjaga. [7][7]

Selain itu, VirtualBox sebagai platform simulasi menghadirkan keunggulan dalam aspek pengujian dan pengembangan jaringan tanpa memerlukan perangkat keras fisik yang mahal. Dengan cara ini, berbagai skenario keamanan jaringan dapat diuji dengan biaya yang lebih rendah serta risiko minimal. [8] penggunaan Mikrotik sebagai perangkat pengatur jaringan dengan dukungan Security teknik firewall berbasis Layer 7 protocol terbukti memberikan perlindungan pada jaringan lokal. Penelitian ini juga dapat mengurangi celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab, sehingga dapat mencegah serangan berbahaya dari dalam jaringan.[9]

Secara keseluruhan, simulasi pengujian keamanan jaringan dengan memblokir akses, berbasis Mikrotik dalam VirtualBox memberikan gambaran yang jelas mengenai langkah-langkah untuk mengamankan komunikasi jaringan dalam sistem yang terdistribusi. Upaya ini menjadi bagian penting dalam memastikan keamanan serta integritas data dalam suatu organisasi atau perusahaan. [10]

2. TINJAUAN PUSTAKA

sebagai perangkat jaringan yang andal, menawarkan berbagai fitur seperti firewall, kontrol akses yang dapat digunakan untuk memfilter lalu lintas jaringan dan membatasi akses berdasarkan alamat IP atau layanan tertentu. Implementasi kontrol akses jaringan MikroTik telah terbukti meningkatkan keamanan jaringan dengan melakukan otentikasi terhadap perangkat yang terhubung. [11]

2.1 VirtualBox

penggunaan VirtualBox dalam simulasi ini memungkinkan pengujian berbagai skenario keamanan tanpa mengganggu operasional jaringan yang sebenarnya. Fleksibilitas ini mempermudah pengembangan serta pengujian solusi keamanan yang dapat diterapkan dalam lingkungan produksi. [6]

2.2 Mikrotik

Mikrotik digunakan untuk mengimplementasikan metode firewall filtering yang efektif untuk meningkatkan keamanan jaringan di lingkungan kecil atau rumah. Dengan memanfaatkan Layer 7 protocol, firewall dapat menyaring trafik berdasarkan jenis aplikasi, dan teknik ini sangat berguna dalam mencegah ancaman dari aplikasi yang tidak sah. Pendekatan ini memberikan hasil yang lebih baik dalam mengurangi potensi serangan dari luar.[12]

2.3 Layer 7 Protocol

Layer 7 Protocol sebagai salah satu metode efektif untuk membatasi akses situs yang tidak diinginkan dalam jaringan, pada perangkat Mikrotik. Protokol ini memungkinkan administrator jaringan untuk mengatur lalu lintas data berdasarkan pola konten dalam paket data yang melewati jaringan, sehingga dapat memblokir akses ke media sosial atau situs hiburan saat jam pembelajaran berlangsung [13]

2.4 Blokir Akses

Blokiran akses berbasis Mikrotik dalam simulasi ini menghasilkan lingkungan jaringan yang lebih aman serta lebih terlindungi dari ancaman eksternal. Pendekatan ini menjadi langkah penting dalam memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sumber daya jaringan. [14]

2.5 Keamanan Jaringan

teknologi jaringan komputer yang pesat telah mendorong peningkatan kebutuhan akan akses informasi dalam berbagai bentuk. Internet sebagai sumber informasi utama memungkinkan berbagai aktivitas digital seperti penelusuran web (browsing), percakapan daring (chatting), hingga penulisan blog (blogging) menjadi semakin umum di kalangan pengguna di seluruh dunia. Simulasi ini memberikan wawasan mengenai bagaimana penerapan dan pengujian solusi keamanan jaringan dapat dilakukan secara efektif dalam lingkungan virtual.[15]

3. METODE PENELITIAN

Penelitian ini menggunakan metode **eksperimen** dengan pendekatan simulasi untuk menguji efektivitas konfigurasi keamanan jaringan menggunakan Mikrotik dalam VirtualBox. Eksperimen dilakukan dengan mensimulasikan lingkungan jaringan, menerapkan konfigurasi blokir akses dan IP Service, serta melakukan pengujian untuk mengevaluasi dampaknya terhadap keamanan jaringan Windows 7.

3.1 Alat dan Bahan

Adapun alat dan bahan yang digunakan dalam penelitian ini meliputi:



Gambar 1 perangkat lunak yang di perlukan

Dari gambar di atas ada beberapa perangkat lunak yang di perlukan, serta memiliki fungsi masing masing dalam pembuatan Blokir akses & IP Service

3.1.1 Oracle VM Virtualbox

Oracle VM VirtualBox adalah perangkat lunak virtualisasi yang memungkinkan pengguna menjalankan beberapa sistem operasi dalam satu komputer secara bersamaan. Dalam penelitian ini, VirtualBox digunakan sebagai lingkungan simulasi untuk menguji keamanan jaringan Windows 7 dengan metode pemblokiran akses dan pengaturan layanan IP berbasis MikroTik.

3.1.2 Windows 7 (Guest OS)

Windows 7 berfungsi sebagai **Guest OS** (sistem operasi tamu) dalam simulasi ini, di mana sistem operasi tersebut dijalankan di dalam Oracle VM VirtualBox. Tujuan utama penggunaan Windows 7 dalam penelitian ini adalah untuk menguji efektivitas metode pemblokiran akses pada situs judi online berbasis MikroTik dalam lingkungan jaringan virtual.

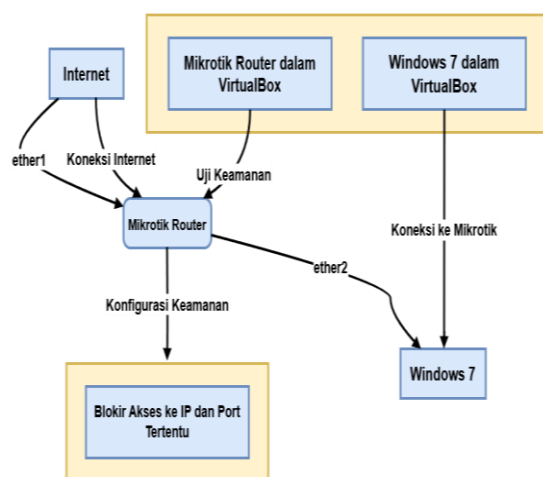
3.1.3 Mikrotik RouterOS (CHR)

RouterOS Cloud Hosted Router (CHR) digunakan sebagai **router virtual** dalam penelitian ini untuk mengontrol dan mengamankan lalu lintas jaringan yang melibatkan Windows 7 sebagai klien. Dengan menggunakan CHR dalam Oracle VM VirtualBox, penelitian ini dapat menguji efektivitas metode **layer 7 protocol** guna meningkatkan keamanan jaringan.

3.1.4 Winbox

WinBox adalah perangkat lunak berbasis GUI (Graphical User Interface) yang digunakan untuk mengelola dan mengkonfigurasi **MikroTik RouterOS**. Dalam penelitian ini, WinBox digunakan sebagai alat utama untuk menerapkan metode **layer 7 protocol** pada MikroTik RouterOS CHR yang berjalan di dalam VirtualBox.

3.2 Tahap Alur Proses Pembuatan



Gambar 2 Diagram topologi alur proses pembuatan

3.2.1 Diagram topologi alur proses pembuatan

Gambar Diagram di atas menggambarkan skenario simulasi pengujian keamanan jaringan dengan menggunakan Mikrotik dan sistem operasi Windows 7 dalam lingkungan VirtualBox. Tujuan utama dari simulasi ini adalah mengonfigurasi serta menguji firewall dan pengaturan IP Service sebagai langkah mitigasi terhadap potensi ancaman keamanan.

Diagram ini menggambarkan topologi jaringan virtual yang digunakan dalam simulasi pengujian keamanan menggunakan Mikrotik di VirtualBox. Dalam simulasi ini, jaringan terdiri dari beberapa elemen utama, yaitu koneksi internet,

router Mikrotik, serta perangkat Windows 7 yang bertindak sebagai klien dalam lingkungan pengujian.

Koneksi jaringan diawali dari sumber internet yang dihubungkan ke router Mikrotik melalui antarmuka ether1 yang berfungsi sebagai jalur WAN (Wide Area Network). Router Mikrotik kemudian meneruskan koneksi ke perangkat Windows 7 melalui ether2, yang berfungsi sebagai jalur komunikasi dalam jaringan lokal (LAN). Dengan konfigurasi ini, Windows 7 dapat berinteraksi dengan Mikrotik dan menjalankan pengujian keamanan jaringan.

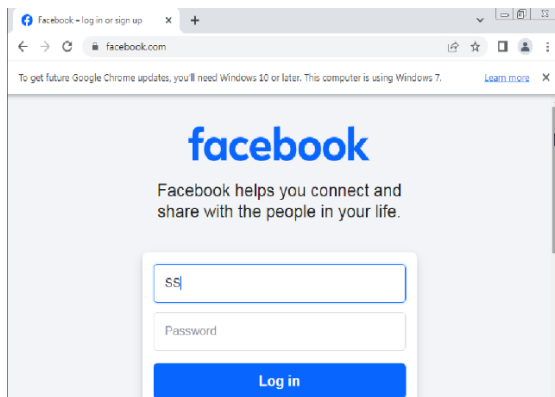
Keamanan dalam simulasi ini diterapkan melalui mekanisme firewall berbasis Layer 7 Protocol. Firewall ini berfungsi untuk menyaring dan memblokir lalu lintas data berdasarkan pola tertentu dalam komunikasi jaringan. Layer 7 Protocol memungkinkan Mikrotik untuk mendeteksi dan membatasi akses ke layanan atau aplikasi tertentu yang berpotensi membahayakan jaringan, seperti pembatasan akses terhadap aplikasi tertentu atau pemblokiran situs web yang tidak diizinkan.

Seluruh skenario ini dijalankan dalam lingkungan VirtualBox dengan dua mesin virtual utama, yaitu Mikrotik Router dan Windows 7. Router Mikrotik bertindak sebagai pengelola lalu lintas jaringan serta pengatur kebijakan keamanan, sementara Windows 7 digunakan sebagai perangkat klien untuk menguji efektivitas aturan yang telah diterapkan. Dengan adanya simulasi ini, dapat dilakukan evaluasi terhadap konfigurasi firewall dan keamanan jaringan dalam kondisi yang lebih terkontrol sebelum diterapkan pada sistem nyata.

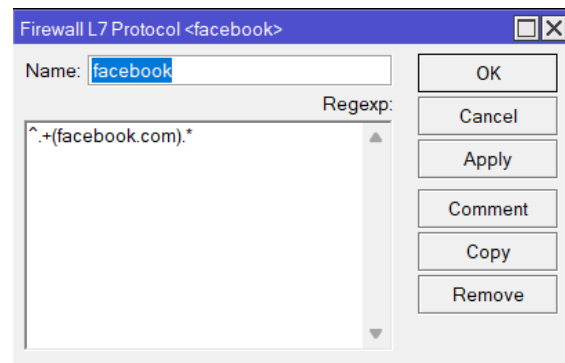
4. HASIL DAN PEMBAHASAN

Pada Bab ini membahas penjelasan hasil dari penelitian dan langkah langkah penerapan layer 7 protocol yang telah dilakukan, dari simulasi uji keamanan jaringan windows 7 pada situs dengan metode layer 7 protocol, menggunakan mikrotik, sebagai berikut.

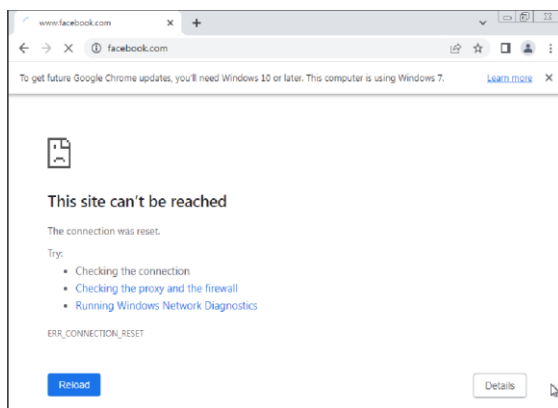
4.1 hasil penerapan blokir akses



Gambar 6 Konfigurasi List Filter layer 7 Protocol



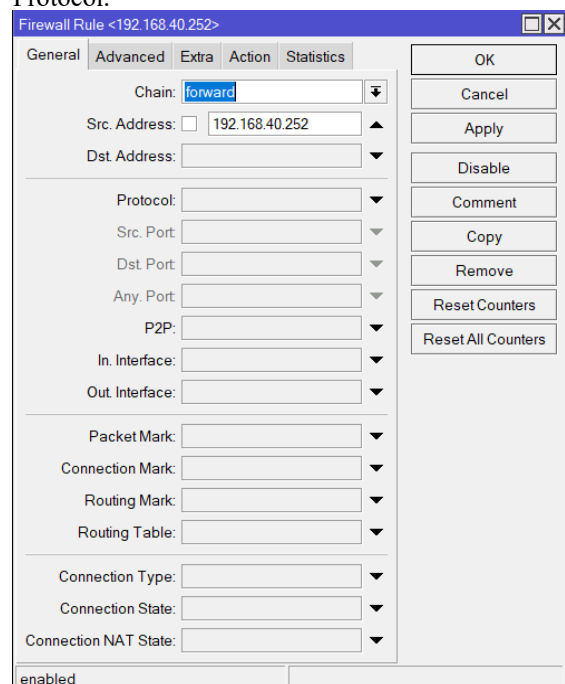
Pada gambar 5, menunjukan Konfigurasi dari layer 7 Protocol pada Firewall, untuk memblokir situs facebook menggunakan Regexp lalu memasukan script yang ingin di blokir aksesnya (^.*(facebook.com).*), jika list filter sudah di buat selanjutnya membuat Fairwall rule bertujuan untuk mamakai Script yang sudah di buat pada layer 7 Protocol.



Gambar 5 sesudah di blokir akses

Pada gambar 3 dan 4 menunjukan hasil situs Facebook pada Windows 7 yang belum di blokir akses dan sesudah di blokir akses menggunakan layer 7 protokol, di mana jika ingin memblokir situs pada Windows 7 ini, harus konfigurasi Firewall terlebih dahulu pada bagian layer 7 Protocol, untuk membuat filter list situs yang ingin di blokir, bisa kita lihat pada gambar ke 5.

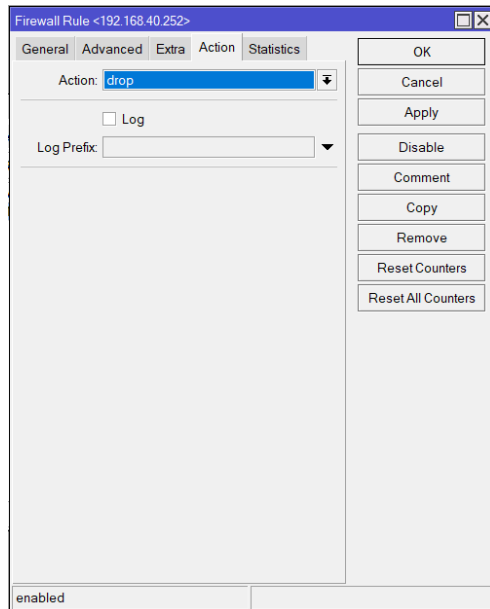
4.2 Implementasi blokir akses



Gambar 4 Konfigurasi Firewall Rule General

Pada gambar ke 6, melakukan tahap memfilter blokir

akses yang telah di buat sebelumnya pada gambar ke 5, pada bagian General, cahain di ubah menjadi Forward bertujuan untuk mengelola trafik dalam satu Interface, lalu pada bagian Src. Address masukan ip client atau ip dari windows 7 yang sudah



di buat.

pada gambar ke 7, di bagian Advanced ubah layer 7 protocolnya di isi dengan nama facebook, untuk menganalisis data serta mengidentifikasi dan memfilter lalu lintas.

Gambar 8 Konfigurasi Firewall Rule

No	Jaringan	Blokir	Sesudah Blokir
1	Akses ke situs tertentu	Dapat diakses	Diblokir menggunakan Layer 7 Protocol
2	Log pemantauan keamanan	Tidak ada aktivitas pemblokiran	Menampilkan aktivitas pemblokiran

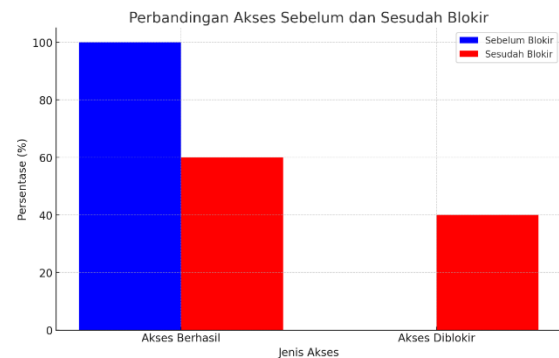
Pada gambar ke 8 ini, memperlihatkan konfigurasi pada bagian Action yang di ubah menjadi drop, bertujuan untuk memblokir koneksi ke situs, agar tidak bisa membuka facebook pada Windows 7

4.3 Analisis Hasil Pengujian

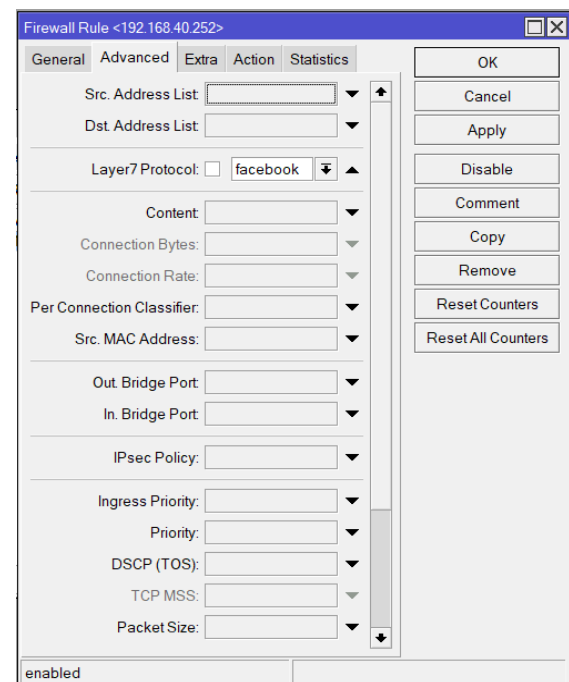
Pengujian dilakukan dengan membandingkan kondisi jaringan sebelum dan sesudah implementasi aturan keamanan menggunakan metode Layer 7 Protocol pada Mikrotik. Berikut adalah hasil yang diperoleh:

Berdasarkan hasil pengujian, metode blokir akses situs dengan Layer 7 Protocol pada Mikrotik berhasil diterapkan dengan baik. Berikut adalah beberapa analisis terkait efektivitas metode tersebut:

- Keberhasilan Pemblokiran: Aturan firewall yang diterapkan terbukti mampu membatasi akses ke situs tertentu sesuai dengan kebijakan yang telah ditentukan.



- Efektivitas Layer 7 Protocol: Penggunaan Layer 7 Protocol memungkinkan pemblokiran berbasis konten situs, sehingga lebih spesifik dibandingkan pemblokiran berdasarkan IP.



Gambar 7 Konfigurasi Firewall Rule

- Log Keamanan Mikrotik: Menunjukkan adanya upaya akses yang gagal, yang menandakan bahwa sistem telah berfungsi dengan baik dalam mencegah akses tidak sah.

Gambar 9 grafik perbandingan jumlah akses

Grafik yang dibuat menggambarkan perbandingan jumlah akses situs sebelum dan sesudah implementasi aturan keamanan menggunakan Layer 7 Protocol pada MikroTik.

- Sebelum Implementasi
 - Semua situs dapat diakses tanpa batasan, sehingga 100% akses berhasil.
 - Tidak ada pembatasan terhadap jenis situs atau layanan jaringan tertentu.
- Sesudah Implementasi
 - Beberapa situs yang telah ditentukan dalam aturan Layer 7 Protocol mengalami blokir sebesar 40%.
 - Pengguna hanya dapat mengakses 60% dari total akses sebelumnya, yaitu situs yang tidak termasuk dalam daftar blokir.

Hasil ini menunjukkan bahwa metode Layer 7 Protocol pada MikroTik efektif dalam membatasi akses ke situs tertentu sesuai dengan kebijakan keamanan yang telah ditetapkan. Selain itu, log keamanan MikroTik mencatat aktivitas percobaan akses ke situs yang telah diblokir, yang menegaskan keberhasilan implementasi aturan ini.

5 KESIMPULAN

Berdasarkan hasil simulasi dan analisis yang telah dilakukan, dapat disimpulkan bahwa metode pemblokiran akses berbasis Layer 7 Protocol pada MikroTik terbukti efektif dalam meningkatkan keamanan jaringan Windows 7 dalam lingkungan virtual. Aturan firewall yang diterapkan berhasil membatasi akses ke situs yang tidak diizinkan dan memberikan visibilitas terhadap aktivitas pemblokiran melalui fitur log MikroTik. Virtualisasi menggunakan Oracle VM VirtualBox juga terbukti menjadi solusi efisien dan aman dalam menguji berbagai skenario keamanan jaringan tanpa mengganggu jaringan fisik. Penelitian ini membuktikan bahwa integrasi antara MikroTik dan Layer 7 Protocol merupakan pendekatan yang relevan dan adaptif terhadap tantangan keamanan siber modern, khususnya dalam konteks jaringan lokal. Untuk penelitian selanjutnya, disarankan untuk mengintegrasikan fitur keamanan tambahan seperti Intrusion Detection System (IDS) atau Intrusion Prevention System (IPS) guna memperkuat lapisan pertahanan jaringan secara menyeluruh.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada dosen dan rekan-rekan mahasiswa atas masukan dan saran berharga yang diberikan selama proses pengembangan sistem ini. Dukungan tersebut sangat berkontribusi dalam menyempurnakan serta meningkatkan kualitas karya tulis ini.

DAFTAR PUSTAKA

- [1] D. Setiyanto and A. Voutama, "Pembangunan Infrastruktur Fiber To the Home Oleh Pt Ikhlas Cipta Teknologi Di Kawasan Desa Jatiranggon," *J. Ilm. Matrik*, vol. 25, no. 2, pp. 131–142, 2023, doi: 10.33557/jurnalmatrik.v25i2.2382.
- [2] C. N. Syahputri, C. Anggraini, H. F. Anugerah, I. Zufria, and M. I. Nahwi, "Penerapan Kinerja Filter Rule dengan Metode Raw dan Layer 7 Protocol di Router Mikrotik," *J. Kridatama Sains Dan Teknol.*, vol. 5, no. 02, pp. 433–447, 2023, doi: 10.53863/kst.v5i02.969.
- [3] A. R. Septa Firdaus and A. Voutama, "Memanfaatkan Kerentanan Broken Access Control pada Website Orami untuk Membatalkan Pesanan dan Meniru Identitas Pengguna," *TeIKa*, vol. 13, no. 02, pp. 113–120, 2023, doi: 10.36342/teika.v13i02.3113.
- [4] C. Kamila Wilujeng and A. Voutama, "Implementasi Firewall Filter Rules Sebagai Filtering Content Pada Jaringan Komputer Menggunakan Mikrotik," *JATI (Jurnal Mhs. Tek. Inform.)*, vol. 8, no. 3, pp. 2680–2685, 2024, doi: 10.36040/jati.v8i3.9530.
- [5] H. Gunawan, "Ancaman Keamanan Jaringan Pada Server Untuk Membatasi Website Tertentu Menggunakan Mikrotik," *Inova-Tif*, vol. 2, no. 1, p. 22, 2020, doi: 10.32832/inova-tif.v1i2.2749.
- [6] N. A. Santoso, Z. Maulidin, and R. D. Kurniawan, "Analisis Jaringan Komputer Menggunakan Teknologi Virtualisasi," vol. 11, no. September, pp. 52–60, 2022.
- [7] M. Y. Bagus, W. Di, and E. R. A. Industri, "PORT KNOCKING PADA MIKROTIK UNTUK MENINGKATKAN KEAMANAN," vol. 8, pp. 2115–2122, 2025.
- [8] A. Zainy *et al.*, "INSTALASI MIKROTIK PADA VIRTUALBOX DAN PENGKONEKSIAN ANTARA MIKROTIK DI VIRTUALBOX DENGAN WINBOX DI SMK S TERUNA PADANG SIDEMPUAN of Knowing How to Install Mikrotik on VirtualBox and Connecting Mikrotik to Winbox at SMKS Teruna Padangsidempuan," *J. Adam J. Pengabd. Masy.*, vol. 2, no. 1, pp. 106–118, 2023, [Online]. Available: <https://jurnal.spada.ipts.ac.id/index.php/adam>
- [9] F. Yohaness, "Analisa Dan Perancangan Keamanan Jaringan Lokal Menggunakan Security Onion Dan Mikrotik," *J. Inf. Syst. Technol.*, vol. 01, no. 02, pp. 37–61, 2020, [Online]. Available: <https://journal.uib.ac.id/index.php/joint/article/view/4309>
- [10] F. A. Syaifuddin, D. A. Maulana, and M. F.

- Amrulloh, "Analisis Keamanan Jaringan Menggunakan Firewall untuk Mencegah Serangan Brute Force dan Fraud," vol. 4, no. 2, pp. 895–902, 2024.
- [11] P. Oktaviani, P. Rekayasa, S. Komputer, F. Ilmu, K. Universitas, and D. Bengkulu, "IMPLEMENTASI NETWORK ACCESS CONTROL PADA JARINGAN LOCAL AREA," vol. 4, no. 1, pp. 60–72, 2024.
- [12] R. Sulaiman, A. Mardeka Raya, L. Laurentinus, and P. Padli, "Pemanfaatan Mikrotik RB942-2ND Menggunakan Metode Firewall Filtering Untuk Keamanan Jaringan Dengan Model Forensikk," *J. Teknol.*, vol. 17, no. 1, pp. 65–71, 2024, doi: 10.34151/jurtek.v17i1.4725.
- [13] A. Shomad, Y. Akbar, and D. I. Mulyana, "Implementasi Pembatasan Akses Sosial Media Menggunakan Layer 7 Protocol Pada Perangkat Mikrotik DI SMK IDN," *INFORMATICS Educ. Prof. J. Informatics*, vol. 7, no. 1, p. 27, 2022, doi: 10.51211/itbi.v7i1.1998.
- [14] K. Aziz *et al.*, "IMPLEMENTASI KEAMANAN JARINGAN DENGAN METODE FIREWALL FILTERING MENGGUNAKAN MIKROTIK DI SMKN 3 PAYAKUMBUH," vol. 8, no. 3, pp. 3343–3352, 2024.
- [15] E. Eben, M. Mukramin, and H. Abduh, "Pengembangan Manajemen Keamanan Jaringan Nirkabel (Wifi) Menggunakan Routerboard Mikrotik Dan Firewall Pada Smk Kristen Palopo," *J. Inform. dan Tek. Elektro Terap.*, vol. 12, no. 3, 2024, doi: 10.23960/jitet.v12i3.4716.