Digital Transformation Technology (Digitech) | e-ISSN: 2807-9000
Volume 4, **Number** 2, September 2024
https://doi.org/10.47709/digitech.v4i2.5003

Analisis Keamanan Jaringan Menggunakan Firewall untuk Mencegah Serangan Brute Force dan Fraud

Farellian Aldam Syaifuddin[1*], Dany Achmad Maulana[2], Muhammad Faishol Amrulloh[3]
[1,2,3]Program Studi Informaika, Universitas Yudharta Pasuruan
[1]farellian26@gmail.com, [2]danyachmad75@gmail.com, [3]faishol@yudharta.ac.id

open access
Histori Artikel:
Diajukan: 25 November 2024
Disetujui: 1 Desember 2024
Dipublikasi: 14 Desember 2024
Kata Kunci:
Analisis, Fraud, Firewall, Brute Force, Keamanan Jaringan
Digital Transformation Technology (Digitech) *is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).*

Abstrak
Keamanan jaringan merupakan aspek penting dalam menjaga integritas dan kerahasiaan data di lingkungan rumah sakit, termasuk Rumah Sakit Umum Daerah Bangil (RSUD Bangil). Salah satu ancaman yang sering dihadapi adalah serangan brute force dan fraud yang dapat membahayakan sistem informasi rumah sakit. Penelitian ini bertujuan untuk menganalisis penerapan firewall sebagai langkah mitigasi terhadap ancaman-ancaman tersebut. Firewall digunakan untuk memantau dan mengendalikan lalu lintas data yang masuk dan keluar jaringan, serta mendeteksi dan mencegah percakapan yang mencurigakan yang dapat digunakan dalam serangan brute force dan fraud. Penelitian ini menggunakan metode analisis dengan pendekatan studi kasus pada RSUD Bangil, melibatkan observasi terhadap konfigurasi firewall dan evaluasi terhadap efektivitas pengaturan yang ada. Hasil penelitian menunjukkan bahwa penggunaan firewall yang tepat dapat secara signifikan mengurangi risiko serangan brute force dan fraud, meskipun tetap diperlukan pembaruan dan penguatan sistem secara berkala untuk menghadapi ancaman yang terus berkembang. Penelitian ini memberikan rekomendasi bagi RSUD Bangil dalam meningkatkan sistem keamanannya dengan penerapan firewall yang lebih terstruktur dan pemantauan lebih intensif terhadap aktivitas jaringan.

PENDAHULUAN

Di era modern, jaringan komputer semakin penting untuk pendidikan dan pekerjaan. Salah satu hal penting dalam mengelola jaringan komputer adalah keamanan jaringan, karena banyaknya akses ke jaringan akan meningkatkan peluang kejahatan (Nitra & Ryansyah, 2019). Semakin banyak server publik yang terhubung ke jaringan internet, maka keamanan data dan arus lalu lintas jaringan ini harus diperhatikan karena dapat menyebabkan kerentanan terhadap pelanggaran jaringan internet seperti pencurian data, pemalsuan data, dan pengubahan data (Halaman web), pembocoran data, penyalahgunaan data individu, dan kejahatan lain-lain (Mulyanto et al., 2024).

Rumah Sakit Umum Daerah (RSUD) Bangil Kabupaten Pasuruan adalah rumah sakit yang berdiri dan diresmikan pada tahun 1981. Rumah sakit ini menjadi tipe D pada tahun 1985 dan kemudian menjadi tipe C pada tahun 1993 berdasarkan SK Menkes No. 20/Menkes/SK/II/1993. RSUD Bangil berfokus pada pelayanan sosial kepada masyarakat yang tidak mampu dan berfungsi sebagai pusat tujuan untuk Puskesmas dan unit unit kesehatan di wilayah Kabupaten Pasuruan. RSUD Bangil bertujuan untuk memberikan layanan kesehatan yang baik, merata, dan terjangkau bagi masyarakat. Layanan ini akan didukung oleh tenaga kerja profesional dengan unit kerja yang mandiri.

Masalah utama yang dihadapi adalah kurangnya sistem keamanan yang memadai pada jaringan yang ada, terutama untuk melindungi router Mikrotik dari serangan Brute Force dan Fraud. Tanpa perlindungan yang cukup, router Mikrotik rentan terhadap eksploitasi yang dapat mengungkapkan username dan password login pengguna, memungkinkan orang yang tidak bertanggung jawab untuk mengakses jaringan. Hal ini dapat menyebabkan data penting hilang dan penyalahgunaan sumber daya jaringan. Akibatnya, penguatan sistem keamanan jaringan menjadi sangat penting. (Sembiring et al., 2011) Dalam analisis ini, Firewall digunakan untuk mendeteksi dan mencegah serangan Brute Force. Penipuan online, atau yang sering disebut sebagai Cyber Fraud, merupakan salah satu bahaya besar yang telah muncul di era teknologi modern. Karena kemajuan teknologi informasi dan koneksi internet yang semakin luas, penipu telah menggunakan berbagai teknik yang sangat canggih untuk mengecoh dan merampok individu dari berbagai lapisan masyarakat. Fenomena ini telah melibatkan berbagai taktik, seperti serangan phishing yang telah berhasil membuat orang memberikan data pribadi mereka, hingga penipuan investasi online yang telah menyebabkan kerugian finansial besar. Tujuan dari ini adalah untuk memperkuat pertahanan jaringan terhadap ancaman yang dapat merusak integritas dan kerahasiaan data, serta memastikan bahwa operasi jaringan tetap aman dan tidak terpengaruh oleh serangan (Rizki & Zaky, 2019).

Penelitian yang dilakukan oleh (Sulistyo, n.d.) menjelaskan bahwa bahwa pentingnya mengatur firewall

pada router Mikrotik untuk mencegah serangan brute force dan fraud. Router Mikrotik yang tidak memiliki perlindungan cukup rentan terhadap eksploitasi; individu yang tidak bertanggung jawab dapat mengakses jaringan dengan mengungkapkan username dan password pengguna. Penelitian serupa pernah dilakukan oleh (Dzardi, n.d.) yang dimana penipu telah menggunakan berbagai metode yang sangat canggih untuk mengecoh dan merampok orang dari berbagai lapisan masyarakat berkat kemajuan teknologi informasi dan penyebaran internet. Fenomena ini telah melibatkan berbagai strategi, seperti serangan phishing yang berhasil membuat orang memberikan data pribadi mereka, dan penipuan investasi online yang telah menyebabkan kerugian finansial besar. Dan juga pada penelitian yang dilakukan oleh (Eka Putra et al., 2024) menjelaskan bahwa mikrotik telah menjadi pilihan umum dalam industri teknologi informasi. Karena telah ditunjukkan sebagai jaringan router komputer yang dapat diandalkan, Selain memiliki banyak fitur dan alat yang luar biasa, mikrotik sangat cocok untuk perangkat jaringan, baik kabel maupun nirkabel. Mikrotik adalah router yang sangat disukai di dunia teknologi informasi karena sifatnya yang open source. Router sangat penting karena memiliki kemampuan untuk mengatur koneksi antara berbagai komputer. Tidak membutuhkan banyak hardware dan pengoperasiannya mudah.

Tujuan dari penelitian ini adalah untuk menemukan dan menganalisis potensi ancaman keamanan jaringan serta pengembangan solusi untuk melindungi sistem jaringan dari serangan brute force dan fraud. Dan juga penggunaan firewall merupakan salah satu protokol kemanan jaringan komputer, dengan mempertimbangkan latar belakang dan masalah di atas, penelitian ini bertujuan untuk menganalisis sistem keamanan jaringan melalui penggunaan metode firewall dari mikrotik untuk mencegah adanya serangan brute force dan fraud terhadap router mikrotik yang digunakan. Metode ini memungkinkan firewall untuk mem-blacklist address penyerang sehingga tidak bisa melakukan penyerangan brute force dan fraud.

STUDI LITERATUR

1. Analisis

Analisis adalah proses atau metode untuk memecah, mengidentifikasi, dan memeriksa komponen-komponen atau elemen-elemen dari suatu objek, masalah, atau fenomena dengan tujuan untuk memahami struktur, hubungan, pola, atau prinsip yang mendasarinya. Tujuan dari analisis ini adalah untuk mendapatkan lebih banyak informasi dan mendapatkan pemahaman yang lebih baik tentang apa yang sedang dianalisis (Nurhasanah et al., 2021).

2. Jaringan

Jaringan komputer adalah sekumpulan komputer dan perangkat keras lainnya yang terhubung satu sama lain untuk berkomunikasi dan berbagi sumber daya, seperti data, aplikasi, atau perangkat lainnya, seperti printer dan hard drive. Jaringan ini memungkinkan perangkat untuk bertukar informasi melalui berbagai media, seperti gelombang radio, kabel, atau sinyal optik. Jaringan komputer dapat dibangun untuk berbagai tujuan, seperti untuk membuat lebih mudah bagi orang untuk berkomunikasi satu sama lain atau untuk mempercepat komunikasi antar individu. Adanya jaringan komputer memungkinkan kita melakukan berbagai tugas, seperti mengirim email, berbagi file, mengakses situs web, dan menjalankan aplikasi berbasis jaringan dengan lebih cepat dan efisien (Novira, 2022).

3. Firewall

Sistem keamanan jaringan yang dikenal sebagai firewall berfungsi untuk mengawasi dan mengontrol lalu lintas data yang masuk dan keluar dari suatu jaringan komputer. Firewall berfungsi sebagai "pagar" antara jaringan internal (seperti jaringan pribadi atau perusahaan) dan jaringan eksternal (seperti internet) untuk melindungi jaringan dari ancaman luar (seperti peretas, virus, dan malware) serta memastikan bahwa komunikasi yang terjadi hanya berasal dari sumber yang sah dan dapat dipercaya (Andono & Darmawan, 2019).

4. Brute Force

Brute force adalah teknik pemecahan masalah atau pencarian solusi yang mengandalkan pemeriksaan menyeluruh terhadap semua kemungkinan atau kombinasi yang ada. Brute force sering digunakan dalam komputer untuk memecahkan enkripsi atau menyelesaikan masalah algoritma dengan mencoba semua kombinasi kata sandi, kunci, atau solusi yang mungkin hingga menemukan yang tepat. Brute force cenderung sangat memakan waktu dan sumber daya, terutama pada masalah yang kompleks dengan banyak kemungkinan, meskipun metode ini dapat menjamin keberhasilan karena seluruh kemungkinan diuji. Metode ini sering dianggap tidak efisien jika dibandingkan dengan metode yang lebih canggih, seperti penggunaan algoritma heuristik atau terstruktur yang dapat mempercepat proses pencarian (Mudzakkar et al., 2023).

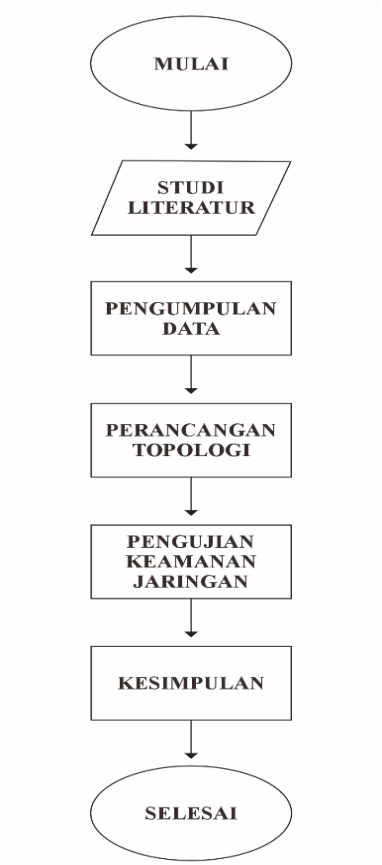
5. Fraud

Dalam konteks jaringan, fraud adalah tindakan atau manipulasi yang dilakukan oleh pihak yang tidak bertanggung jawab dengan tujuan untuk mendapatkan akses tidak sah ke sistem atau data, mengeksploitasi kerentanannya, atau merugikan pihak lain. Serangan fraud jaringan biasanya menggunakan metode seperti phishing, spoofing, atau penipuan identitas. Dalam skenario ini, pelaku berpura-pura menjadi orang lain, seperti pengguna atau administrator, untuk mengelabui sistem atau orang untuk memberikan informasi sensitif seperti kredensial login, data pribadi, atau informasi kartu kredit. Karena penyerang dapat memanfaatkan akses yang

diperoleh untuk melakukan aktivitas ilegal atau merusak infrastruktur jaringan, serangan jenis ini dapat menyebabkan kerugian finansial, reputasi, dan keamanan data yang signifikan (Rizki & Zaky, 2019).

METODE

Untuk membantu peneliti menyelesaikan penelitian dengan lebih terorganisir, metode penelitian menunjukkan langkah-langkah yang harus diikuti. Prosedur ini digambarkan pada gambar 1 di bawah ini.



Gambar 1. Flowchart Tahapan Penelitian

Studi Literatur

Dalam studi literatur, peneliti mengkaji berbagai sumber, termasuk buku, jurnal, dan artikel ilmiah, kemudian menggabungkan hasil penelitian tersebut untuk membangun pemahaman yang lebih baik tentang subjek tersebut yang dapat mendukung penelitian ini (Barra et al., 2022).

Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah metode observasi, yang berarti subjek diamati secara langsung. Metode pengumpulan data ini merupakan peningkatan metode pengumpulan data untuk mendukung penelitian yang dilakukan (Aditya, 2023).

Perancangan Topologi

Pada langkah ini, para peneliti memeriksa berbagai jenis topologi, seperti topologi bintang, cincin, mesh, atau pohon, untuk mengevaluasi manfaat dan kekurangan masing-masing. Perhitungan kapasitas jaringan, pemilihan perangkat keras yang dibutuhkan, dan perencanaan jalur koneksi adalah semua bagian dari perancangan ini (Barovih et al., 2022).

Pengujian Keamanan Jaringan

Pada langkah ini, perangkat yang diperlukan untuk pengujian jaringan disiapkan; kemudian, firewall dikonfigurasi untuk serangan brute force dan fraud; kemudian, perangkat mikrotik dikonfigurasi untuk jaringan, dan firewall digunakan untuk mengawasi aktifitas brute force dan fraud yang berjalan (Dasmen et al., 2022).

HASIL

Hasil ini menunjukkan bahwa penerapan firewall dalam sistem keamanan jaringan dapat melindungi secara efektif terhadap serangan brute force dan fraud sambil mempertahankan kinerja sistem yang optimal.

1. Implementasi Topologi Jairngan

Topologi jaringan seperti Firewall SOPHOS, Cloud Core Router Mikrotik (CCR1036-8G-2S+), Fiber Optic NETVILE, Server lokal, Cloud Router Switch Mikrotik (CRS354-48G-4S+2Q+), Access Point, dan banyak lagi telah diimplementasikan dengan sukses. Selain itu, jalur internet yang dikonfigurasi dari ISP ke firewall dan didistribusikan ke pengguna melalui cloud core mikrotik dan switch router cloud berjalan dengan baik.

2. Kinerja Hardware

Penggunaan Mikrotik CCR1036-8G-2S+Core dengan spesifikasi:

- CPU 1.2 GHz
- 8 port Gigabit ethernet + 2 SFP+ (10G)
- 1 port serial dan 1 port USB
- LCD Touch-screen berwarna
- RAM 4GB (dapat diupgrade hingga 16GB)

Beban router hanya mencapai 4% setelah implementasi sistem keamanan.

3. Keamanan Jaringan

Serangan SSH ke Port 22 berhasil diidentifikasi dan dihentikan. Alamat IP penyerang telah ditemukan oleh sistem dan dimasukkan ke dalam blacklist. Selain itu, firewall berhasil melakukan drop terhadap alamat IP yang masuk ke dalam list address. Dengan menerapkan enkripsi pada Port 22, pihak ketiga tidak dapat membaca data sensitif seperti username dan password. Protokol yang digunakan untuk memblokir trafik brute force SSH berhasil digunakan firewall untuk memblokir 3398,8 KiB paket dan 58 ribu paket dengan kecepatan hampir 458 bps dan tingkat paket 0-500 per detik. Data ini membantu administrator jaringan memantau beban dan menemukan aktivitas mencurigakan.

Pada Fraud Raw Rule telah menunjukkan proses memblokir sejumlah besar data - 838.6 MiB dan 17 juta paket. Dengan kecepatan hampir 370 kbps dan 888 paket per detik, trafik yang diblokir saat ini cukup tinggi. Administrator jaringan dapat menggunakan data ini untuk memantau beban aturan dan mengidentifikasi serangan potensial seperti konfigurasi drop frud TCP, DDoS, port scanning, dan aktivitas tidak biasa lainnya. Address list biasanya digunakan oleh aturan firewall untuk memblokir trafik dari alamat tersebut, meningkatkan keamanan alamat, atau untuk mengidentifikasi alamat IP atau subnet yang berbahaya atau berpotensi sebagai ancaman.

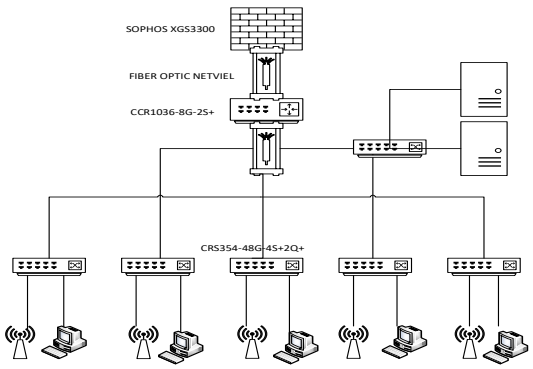
4. Mitigasi Ancaman

Sistem keamanan berhasil mencegah serangan brute force dengan memblokir upaya login berulang. Pencegahan fraud berhasil dilakukan melalui implementasi firewall. Keamanan data sensitif terjaga melalui enkripsi dan pembatasan akses.

PEMBAHASAN

A. Rancangan Topologi Jaringan

Untuk topologi jaringan yang digunakan atau dikembangan dalam penelitian ini terdiri dari Firewall SOPHOS, Cloud Core Router Mikrotik (CCR1036-8G-2S+), Fiber Optic NETVILE, Server lokal, Cloud Router Switch Mikroik (CRS354-48G-4S+2Q+), Access Point, dan beberapa Pengguna. Internet dari ISP menuju ke firewall yang terhubung ke cloud core mikrotik kemudian dibagi ke beberapa cloud router switch dan diteruskan ke pengguna. Contoh topologi yang dibangun dapat dilihat pada Gambar 2.

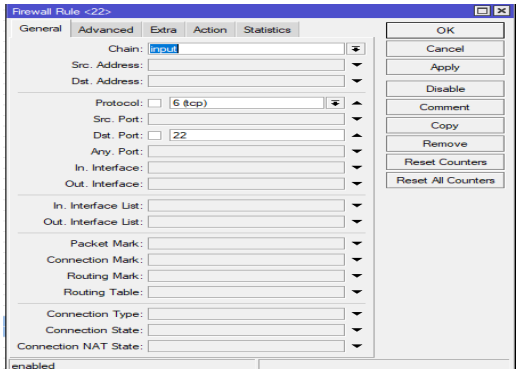


Gambar 2. Topologi Jaringan

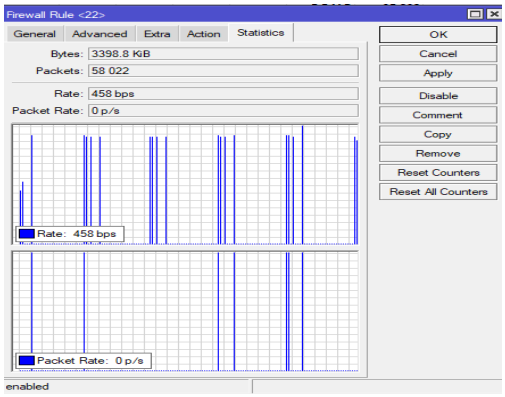
B. Pengujian Keamanan Jaringan

CCR1036-8G-2S+Core CPU 1.2 GHz Mikrotik memiliki 8 port Gigabit Ethernet, 2 port SFP+ (10G), 1 port serial, dan 1 USB. Ini juga memiliki layar touchscreen berwarna. Perangkat ini ideal untuk penggunaan besar, seperti di rumah sakit umum, karena memiliki 4GB RAM 64bit yang dapat ditingkatkan hingga 16GB. Port 22 yang terenkripsi digunakan dalam pengujian ini untuk komunikasi aman, tetapi sering menjadi sasaran serangan brute force atau dictionary. Dengan menggunakan protokol SSH di port 22, login dan pengelolaan server yang aman dijamin melalui koneksi terenkripsi.

Pertama, kami melakukan serangan brute force SSH melalui firewall. Kami melakukannya dengan menggunakan Winbox dan menggunakan username dan password admin yang telah diatur. Selanjutnya, rule ditambahkan ke firewall dengan perintah add chain=input untuk mengontrol trafik yang sah; kemudian, tambahkan protocol=tcp6, port=22, dan tambahkan aksi=drop. Gambar 3 menunjukkan hal ini.



Gambar 3. Konfigurasi SSH Brute Force



Gambar 4. Statistic Firewall Brute Force

Protokol yang digunakan untuk memblokir trafik brute force SSH berhasil digunakan, seperti yang ditunjukkan pada Gambar 4.

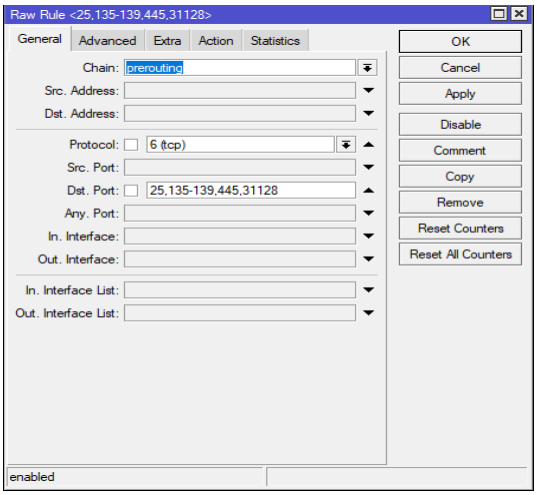


Gambar 5. Address List

Pencegahan berhasil diterapkan dapat dilihat pada Gambar 5.

C. Pengujian Kedua Fraud

Pada mikrotik ini biasanya mengacu pada teknik atau upaya untuk mendeteksi, mencegah, atau memitigasi penyalahgunaan jaringan seperti pencurian bandwidth, penggunaan ilegal, atau pelanggaran aturan jaringan. MikroTik memiliki fitur yang dapat mencegah dan menangani penipuan, seperti: pencegahan pencurian bandwitch, Blokir pengguna Tidak sah, Deteksi Trafik Abnormal, Blokir situs dan konten berbahaya dan lain sebagainya.

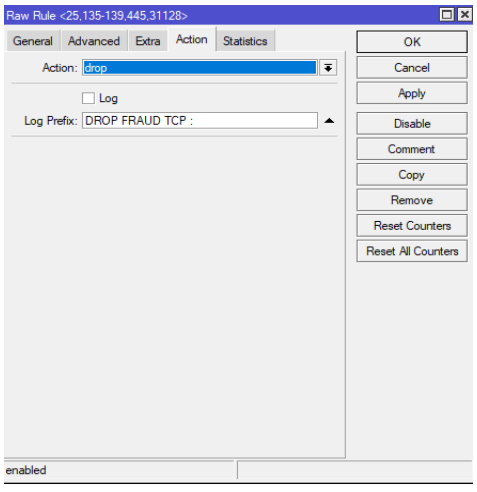


Gambar 6. Raw Rule

Pada Gambar 6. menunjukan langkah konfigurasi Fraud. Konfigurasi ini merupakan bagian dari prosedur keamanan yang bertujuan untuk mendeteksi dan memblokir paket mencurigakan atau berbahaya yang masuk ke jaringan melalui port yang telah diketahui sering menjadi sasaran serangan. Untuk meningkatkan efisiensi dibandingkan dengan table firewall lainnya, aturan ini diterapkan pada Table Raw.

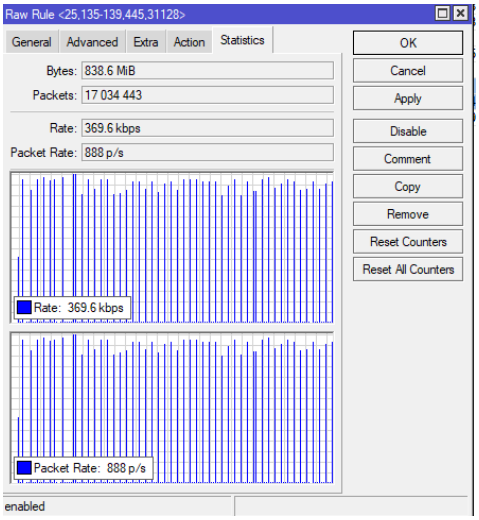
Chain: prerouting Sebelum keputusan rute diproses, aturan ini diterapkan pada trafik. Artinya, paket dari luar jaringan akan diperiksa sebelum diarahkan. Metode: 6 (TCP)Aturan ini hanya akan memproses paket protokol TCP. Jumlah Pelabuhan: 25,135-139,445,31128 Filter ini hanya berlaku untuk paket yang dikirim ke port tertentu.

Daftar port yang disebutkan di bawah ini: 25 adalah port SMTP yang digunakan untuk pengiriman email, port135–139 adalah protokol NetBIOS, yang sering digunakan untuk berkomunikasi di jaringan Windows, port 445 adalah protokol SMB, yang digunakan untuk berbagi file dan printer, dan 31128 adalah port khusus yang mungkin terkait dengan aplikasi tertentu.



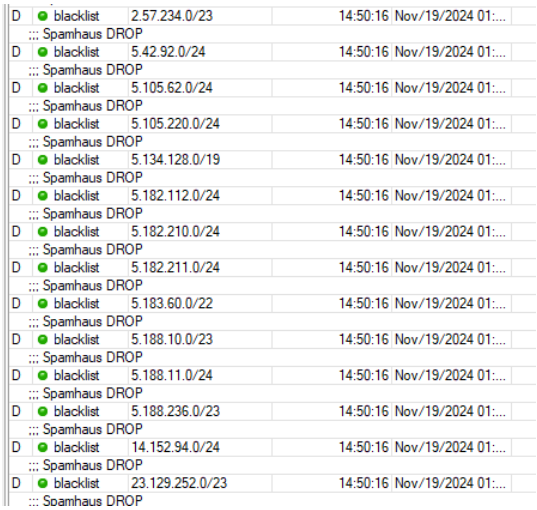
Gambar 7. Action Fraud

Pada Gambar 7. bertujuan untuk menghilangkan trafik TCP yang menuju port tertentu yang dianggap sensitif atau berbahaya, sehingga tidak dapat masuk ke jaringan atau diproses oleh router. Label DROP FRAUD TCP akan memudahkan identifikasi dalam analisis log karena administrator dapat melihat aktivitas yang terkait dengan aturan ini melalui log MikroTik jika log diaktifkan.



Gambar 8. Statistic Traffic

Gambar 8. di atas merupakan gambar statistik ini menunjukkan seberapa efektif aturan memblokir trafik Drop fraud TCP.



Gambar 9. Address List

Pada Gambar 9. Address List di Firewall MikroTik digunakan untuk menyimpan daftar alamat IP atau subnet tertentu yang dapat digunakan oleh aturan firewall untuk berbagai tujuan, seperti pemblokiran, pembatasan akses, atau pengelolaan trafik.

KESIMPULAN

Berdasarkan analisis dan diskusi yang telah dilakukan dalam penelitian ini tentang penggunaan firewall untuk melindungi jaringan RSUD Bangil dari serangan brute force dan penipuan, beberapa kesimpulan adalah penggunaan firewall pada jaringan RSUD Bangil menunjukkan peningkatan keamanan sistem, seperti yang ditunjukkan oleh: Kemampuan sistem untuk mendeteksi dan memblokir serangan secara otomatis, beban kinerja

router tetap stabil pada level 4% setelah penginstalan, dan kemampuan sistem untuk menemukan dan memasukkan alamat IP yang mencurigakan ke dalam blacklist. Sistem keamanan yang diterapkan berhasil mencegah dua jenis serangan utama: Serangan brute force melalui pembatasan akses dan pemblokiran otomatis. Dan upaya fraud melalui implementasi firewall dan enkripsi data sensitif. 1)Penggunaan kombinasi perangkat keras dan konfigurasi yang tepat, meliputi: Firewall SOPHOS, Cloud Core Router Mikrotik (CCR1036-8G-2S+) dan Cloud Router Switch Mikrotik (CRS354-48G-4S+2Q+) Memberikan solusi keamanan yang komprehensif tanpa mengorbankan performa jaringan. Sistem pemantauan dan pengelolaan keamanan yang diterapkan memungkinkan pemantauan aktivitas jaringan secara real-time, respons cepat terhadap ancaman keamanan, dan pengelolaan akses yang lebih terorganisir. Meskipun sistem telah dipasang, diperlukan pembaruan konfigurasi keamanan secara teratur, pengawasan terus-menerus terhadap serangan baru, dan pelatihan staf IT untuk mengelola sistem keamanan. Penelitian ini menunjukkan bahwa, sambil mempertahankan efisiensi operasional sistem, penerapan firewall yang tepat dapat meningkatkan keamanan jaringan rumah sakit, khususnya dalam menghadapi ancaman brute force dan fraud.

REFERENSI

Aditya, V. T. (2023). Manajemen Ancaman Dan Keamanan Jaringan Melalui Penggunaan Firewall Dengan Mikrotik Pada Pt Dinamika Mediakom Tugas Akhir.

Andono, S., & Darmawan, M. (2019). Teknologi Layanan Jaringan. https://www.google.co.id/books/edition/Teknologi_Layanan_Jaringan_SMK_MAK_Kelas/_vwWEAAAQBAJ?hl=en&gbpv=1&dq=pengertian+firewall+pada+jaringan+komputer&pg=PA124&printsec=frontcover

Barovih, G., Hidayat, M. K., & Ajismanto, F. (2022). Pemanfaatan Firewall Rule Base dan SSL dalam Penerapan Sistem Keamanan Jaringan.

Barra, A. R., Sujatmika, A. R., & Umami, I. (2022). Sistem Keamanan Jaringan Komputer Bridge Firewall Menggunakan Router Board Mikrotik Rb750. 4(1).

Dasmen, R. N., M. Hendra Firmansyah, M. Khadafi, & Tri Yolanda. (2022). Penerapan Keamanan Jaringan Menggunakan Metode Firewall Security Port: Network Security Implementation Using Firewall Security Port Method. Decode: Jurnal Pendidikan Teknologi Informasi, 2(1), 1–7. https://doi.org/10.51454/decode.v2i1.29

Dzardi, Y. (n.d.). Analisis Cyber Fraud Pada Platform Jual Beli Game Online: Studi Kasus Pada Platform Steam.

Eka Putra, F. P., Amir Hamzah, Agel, W., & Firmansyah Kusuma, R. O. (2024). Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking. Jurnal Sistim Informasi dan Teknologi, 82–87. https://doi.org/10.60083/jsisfotek.v5i4.329

Mudzakkar, M., Siaulhak, S., & Jumarniati, J. (2023). Analisis Deteksi Dan Pencegahan Eksploitasi Jaringan Brute Force Exploit Menggunakan Firewall Pada Kantor Bappeda Kota Palopo. Sibatik Journal: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, dan Pendidikan, 2(4), 1097–1106. https://doi.org/10.54443/sibatik.v2i4.718

Mulyanto, Y., Susanto, E. S., Akbar, M. I., & Idifitriani, F. (2024). Analisis Keamanan Jaringan Komputer Menggunakan Metode Intrusion Detection System (IDS) dan Firewall. Digital Transformation Technology, 3(2), 864–870. https://doi.org/10.47709/digitech.v3i2.3402

Nitra, R. O., & Ryansyah, M. (2019). Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen. Jurnal Sistem dan Teknologi Informasi (JUSTIN), 7(1), 52. https://doi.org/10.26418/justin.v7i1.29979

Novira, C. (2022). Jaringan Komputer. 1.

Nurhasanah, A., Pribadi, R. A., & Nur, M. D. (2021). Analisis Kurikulum 2013. 07.

Rizki, F. M., & Zaky, M. (2019). Analisis Kriminologis Korban Cyber Fraud Pada Transaksi Game Online Melalui Steam. 1.

Sembiring, I., Widiasari, I., & Prasetyo, S. D. (2011). Analisa dan Implementasi Sistem Keamanan Jaringan Komputer dengan Iptables sebagai Firewall Menggunakan Metode Port Knocking. Jurnal Informatika, 5(2). https://doi.org/10.21460/inf.2009.52.74

Sulistyo, W. (n.d.). Model Keamanan Jaringan Menggunakan Firewall Port Blocking.