Digital Transformation Technology (Digitech) | e-ISSN: 2807-9000
Volume 3, **Number** 2, September 2023
https://doi.org/10.47709/digitech.v3i2.3379

Analisis Keamanan Jaringan Dari Serangan Malware Menggunakan Firewall Filtering Dengan Port Blocking

Fauzan Prasetyo Eka Putra[1*], Achmad Zulfikri[2], Moh Abroril Huda[3], Hasbullah[4], Mahendra[5], Miftahus Surur[6]
[1,2,3,4,5,6]Universitas Madura, Indonesia.
[1]prasetyo@unira.ac.id, [2]achamadzulfikri20@gmail.com, [3]moh.abrorilhuda@gmail.com, [4]hasbullahsd009@gmail.com, [5]maa.hendra04@gmail.com, [6]miftahuss43@gmail.com.

Histori Artikel:
Diajukan: 29 Desember 2023
Disetujui: 30 Desember 2023
Dipublikasi: 31 Desember 2023

Kata Kunci:
Keamanan Jaringan; malware; filtering firewall; port blocking.

Abstrak
Keamanan jaringan komputer sangat penting untuk melawan ancaman siber yang semakin berkembang pesat, terutama serangan malware yang canggih. Penelitian ini berfokus pada filter firewall dan port blocking untuk melindungi jaringan komputer dari serangan malware. Meningkatnya intensitas serangan malware telah menyebabkan latar belakang penelitian ini, yang merusak baik organisasi maupun individu, menyebabkan kebocoran data, gangguan operasional, dan kerugian finansial yang besar. Dalam penelitian ini, strategi filtering firewall dan port blocking digunakan untuk memeriksa efektivitas perlindungan jaringan komputer. Sebagai pertahanan utama, filter firewall melacak dan mengatur lalu lintas data yang masuk dan keluar jaringan. Blokir port meningkatkan keamanan dengan membatasi akses ke port-port tertentu yang dapat dieksploitasi oleh malware. Hasil penelitian diharapkan akan memberikan wawasan yang lebih mendalam tentang keamanan jaringan komputer untuk melawan ancaman malware yang terus berkembang. Penelitian ini diharapkan dapat memperkaya literatur tentang keamanan jaringan dengan memberikan panduan praktis bagi administrator jaringan dan pengambil keputusan di tingkat organisasi untuk meningkatkan strategi keamanan mereka. Penelitian ini diharapkan dapat membangun dasar untuk kebijakan keamanan jaringan yang lebih baik di era digital yang penuh tantangan ini.

PENDAHULUAN

Dengan terus meningkatnya perkembangan teknologi, khususnya pada jaringan komputer, maka diperlukan suatu solusi yang dapat memberikan perlindungan maksimal terhadap jaringan komputer(Haidar Hari et al., n.d.). Jaringan komputer sekarang banyak digunakan dalam lingkungan profesional dan pendidikan dan dianggap penting.(Kumar & Kumar, 2014). Salah satu faktor yang sangat penting dalam jaringan komputer adalah keamanan jaringan(Santoso et al., 2022). Port yang terbuka sering menjadi target berbagai serangan, yang kemudian memungkinkan pengguna yang tidak sah atau mereka yang tidak memiliki hak akses untuk mengambil kendali dengan mudah atas port yang telah diakses. kontrol atas port yang diakses mudah dilakukan oleh mereka yang tidak memiliki otorisasi atau tidak memiliki kepentingan(Gunawan et al., 2022). Virus, malware, trojan, dan pemindaian port adalah beberapa ancaman keamanan yang paling sering terjadi. Pemindaian port adalah teknik untuk menemukan port komputer yang tersedia di jaringan(Santoso et al., 2022). Seperti yang telah disebutkan, sistem jaringan komputer kini sedang mengalami kendala. Oleh karena itu, keamanan jaringan sangat penting untuk melindungi jaringan dari malware dan virus(Ocanitra & Ryansyah, 2019).

Dengan perlindungan terhadap ancaman eksternal yang dapat membahayakan jaringan dan mencuri data perusahaan, keamanan jaringan adalah teknik yang digunakan untuk mencegah pencurian data perusahaan. dengan menawarkan perlindungan terhadap ancaman eksternal yang mungkin membahayakan jaringan dan mencegah pencurian data dari perusahaan dengan memberikan keamanan atau perlindungan. Virus, trojan, malware adalah salah satu bahaya keamanan yang umum ditemukan. Penyerang dapat menargetkan port yang terbuka dengan mudah. Serangan pada port terbuka dapat dicegah dengan menggunakan teknik port blocking pada router mikrotik(Keamanan Jaringan Bpkad Provinsi Sumsel et al., n.d.-a).

Masalah dengan keamanan jaringan sering kali muncul dari port yang terbuka dan terautentikasi. Sehingga, Jaringan diakses ilegal oleh pengguna yang tidak sah. maka dari itu diperlukan suatu teknik filtering firewall dengan port blocking(Suchendra et al., 2017). Sistem keamanan yang dikhususkan untuk jaringan disebut port blocking(n.d.-b, pp. 99–107). Dengan firewall, pemblokiran port adalah ketika semua port yang tersedia diblokir, tetapi pengguna tetap dapat mengaksesnya karena mereka tahu cara melarang port terbuka, sehingga mereka tetap dapat menggunakannya. Secara umum, pemblokiran port di tempat kerja berarti memfilter semua port yang

tersedia dan hanya mengizinkan pengguna saat ini untuk mengakses port yang telah mereka pilih, termasuk membuat indikator kemajuan tambahan(Eksan Nuryakin Habillah, n.d.).

Firewall adalah alat keamanan jaringan yang mengawasi lalu lintas (traffic) yang masuk dan keluar dari jaringan dan menentukan apakah paket data boleh diterima atau diblokir menggunakan aturan khusus. dengan firewall filtering, konten atau packet yang illegal, tidak pantas atau tidak sah, aksesnya akan di blok dan disaring dengan cara menyaring packet tersebut(Jurnal & Jakaria, 2020). Dengan membuat aturan yang baik, firewall akan lebih mudah memfilter trafik dan bandwidth jaringan. Mengatasi masalah penyebaran malware dalam jaringan yang menyebabkan jaringan lambat. Salah satu dampak malware pada jaringan adalah kelebihan bandwidth yang dapat dengan cepat menguras atau membuat data masuk dan keluar menjadi lebih lambat dari biasanya. (Rizal et al., 2020).

Penyebaran malware menjadi lebih cepat dan sederhana sehubungan dengan teknologi komputer dan spesialisasi komputer. Langkah pertama dalam infeksi malware komputer adalah dengan menginfeksi satu file di komputer. Selanjutnya, malware tersebut menyebar ke seluruh file di komputer, tidak hanya file yang terinfeksi malware tersebut. Jika sejumlah besar malware menyusup ke jaringan melalui jaringan internal atau eksternal yang terhubung ke Internet, dan file di dalam jaringan tersebut disusupi karena komputer di jaringan tersebut terus terhubung, setiap komputer pasti akan bertukar file dengan cara yang sama. Seringnya memanfaatkan jaringan komputer dapat menimbulkan gangguan pada jaringan komputer(*91-237-1-PB*, n.d.). Malware terdiri dari semua program komputer jahat, perangkat lunak jahat, seperti virus, trojans, spyware, dan worm(Al-Saadoon et al., 2011). Virus komputer menempel pada file komputer, biasanya executable, dan trojan melakukan social engineering pada file berbahaya, membuatnya terlihat seperti file yang tidak berbahaya. Spyware adalah perangkat lunak yang termasuk kode untuk mendapatkan akses ke data pengguna. jika PC terinfeksi malware, itu akan berjalan lebih lambat, bahkan jika PC memiliki processor dan RAM yang bagus. Namun, jika mamware menginfeksi pc, pc tersebut akan lambat dan jaringannya tidak akan stabil(Rizky et al., 2016).

Sejumlah penelitian terdahulu yang menjelaskan tentang penggunaan filtering firewall dan port blocking dalam mengurangi risiko serangan malware pada jaringan komputer. Namun, penelitian ini umumnya kurang mendalami aspek penggunaan port blocking sebagai strategi selektif dalam menanggapi ancaman yang berkembang pesat(Ilham et al., 2022; Nur Khasanah STMIK Nusa Mandiri Jakarta, 2016; Robbahul Barra et al., 2022). Oleh karena itu, penelitian ini bertujuan mengisi celah literatur dengan mendalam tentang implementasi filtering firewall dengan penekanan pada port blocking, dengan tujuan untuk lebih memahami dan meningkatkan keamanan jaringan dari serangan malware yang semakin kompleks(Sulistyo, 2022).

Penelitian ini relevan dan penting untuk analisis keamanan jaringan komputer terhadap serangan virus maupun malware(Prasetyo et al., n.d.). Berdasarkan latar belakang dan permasalahan diatas, maka dilakukan penelitian untuk menganalisis sistem keamanan jaringan dengan menggunakan teknik firewall dan port blocking. Dengan mengoptimalkan kinerja firewall, port terbuka yang rentan terhadap malware dan virus dapat ditutup.

STUDI LITERATUR

Sejumlah kajian penelitian sebelumnya yang membahas tentang keamanan jaringan komputer terhadap serangan malware menggunakan filtering firewall dengan port blocking.
Berikut ini kajian-kajian penelitian terdahulu:

1. (Ryansyah et al., 2018) dalam penelitian ini, tujuan dilakukannya adalah menangani masalah lambatnya jaringan yang disebabkan oleh penyebaran malware di jaringan kampus. Salah satu efek adanya malware dalam jaringan kampus adalah overload trafik bandwidth. Dengan membuat rule-rule firewall yang baik, akan lebih mudah untuk mengfilter lalu lintas trafik jaringan dan bandwidth, sehingga dapat menciptakan suatu keamanan jaringan. peneliti menggunakan mikrotik router board RB 1100 AHx2 dimana hasilnya dengan mikrotik tersebut dapat menyaring aktifitas malware.
2. (Wicaksono & Widiasari, 2022)metode port blocking dan firewall filtering yang digunakan dalam sistem keamanan jaringan, dibahas dalam penelitian ini. Dalam penelitian ini, router Mikrotik dan aplikasi Winbox digunakan secara terpisah untuk membuat rule firewall. Rule firewall ini membatasi port komunikasi dan membatasi akses internet melalui web proxy dengan menghalangi situs web http dan https dari jaringan. Hasil penelitian ini diuji dengan melihat sisa port komunikasi yang terbuka menggunakan aplikasi Nmap Zenmap dan dengan menggunakan browser untuk mengakses web situs yang dialihkan dan diblokir. Jaringan internet akan lebih aman dan lebih rentan terhadap serangan dari luar dengan memaksimalkan dan mengoptimalkan kinerja firewall.
3. (Gunawan et al., 2022) penelitian ini dilakukan karena melihat latar belakang masalah di suatu sekolah, dimana jaringan di sekolah tersebut sering mengalami serangan malware, sehingga peneliti melakukan suatu keamanan dengan filtering firewall dan port blocking di mikrotik dengan membatasi penggunaan suatu jaringan komputer, menutup dan memblok akses malware ke jaringan, hasilnya jaringan akan lebih stabil, cepat dan juga aman.

METODE

Metode penelitian memaparkan suatu langkah-langkah dalam pelaksanaan penelitian, untuk memudahkan peneliti dalam menyelesaikan penelitian secara runtut dan terstruktur. langkah-langkah penelitian dapat dilihat pada gambar 1 dibawah.

Gambar 1. Flowchart penelitian

Studi Literatur

Studi literatur dilakukan dengan melakukan penelusuran tentang topik penelitian yang akan dilakukan. Jurnal ilmiah, buku, maupun internet yang berkaitan dengan topik penelitian sebelumnya yang dapat digunakan untuk mendukung penelitian ini(Ernawati et al., n.d.).

Pengumpulan Data Kebutuhan

Pengumpulan data ini merupukan cara untuk mengumpulkan data-data yang mendukung pada penelitian yang dilakukan, pada penelitian ini pengumpulan data dilakukan adalah dengan cara observasi, yaitu objek akan diamati secara langsung, misalnya pada penelitian ini pengamatan dilakukan dengan mengamati penyaringan dan pengeblokan port pada suatu aktivitas malware pada mikrotik(Irawan et al., 2018).

Perangcangan Sistem Topologi

Pada tahap ini, akan dilakukan suatu perancangan topologi jaringan agar dapat menjadi solusi terhadap permasalahan, juga akan melakukan analisis kebutuhan lainnya, misalnya perangkat yang akan digunakan untuk melakukan pemblokiran port dengan firewall, dengan menggunakan perangkat yaitu, Mikrotik(Gunawan et al., 2022).

Pengujian Jaringan

Dalam tahap ini, yang dilakukan adalah mempersiapkan perangkat yang diperlukan untuk pengujian jaringan, termasuk konfigurasi firewall dan port blocking, kemudian melakukan konfigurasi jaringan pada perangkat mikrotik, melakukan pengamanan dengan port blocking pada aktifitas malware yang berjalan(Ernawati et al., n.d.).

HASIL DAN PEMBAHASAN

A. Gambaran Analisis

Dalam Analisis Keamanan Jaringan menggunakan Firewall Port Blocking, tugas jaringan yang perlu diselesaikan antara lain menganalisis topologi jaringan (koneksi jaringan yang menghubungkan dua komputer atau lebih berdasarkan elemen-elemen yang membentuk jaringan). Kedua, implementasi topologi jaringan mengacu pada desain atau konsep pelaksanaan penelitian yang dilakukan. Ketiga, sidik jari jaringan adalah metode dalam sidik jari jaringan yang dimaksudkan untuk mendeteksi alamat Mac yang tidak diketahui dan memulai mode yang tidak diketahui, tidak menentu, dan terlindungi. Keamanan jaringan ini menggunakan tiga metode: keamanan port standar, keamanan port statis, dan keamanan port lengket. Switch yang digunakan dalam pengujians dikelompokkan berdasarkan port pada jaringan area lokal (LAN). Memanfaatkan port yang selalu terbuka bersamaan dengan port pada jaringan berfungsi untuk mengubah topologi LAN menjadi topologi star.

Kelemahan lain dari Sticky Port Security adalah Pelanggaran Keamanan Sticky Port. Mekanisme kompromi ini memberikan pilihan mode. Jadi, ketika port dibuka dan ditutup secara otomatis, paket tidak dibuka melainkan ditutup, dan tidak ada informasi yang diberikan untuk membuka dan menutupnya. Paket terhenti dan tidak ada koneksi yang dapat dilakukan. Mempertahankan alamat IP yang ditetapkan secara statis memerlukan waktu dan mungkin berdampak negatif pada administrator. Petunjuk cara mengubah alamat IP dapat dilakukan menggunakan antarmuka baris perintah (CLI). Proses perubahan alamat IP otomatis menggunakan Dynamic Host Configuration Protocol (DHCP) membantu administrator meminimalkan waktu yang diperlukan untuk mengubah alamat IP. Topologi jaringan yang sesuai diperlukan untuk paket ini. Topologi yang paling umum adalah bus, token, ring, dan star, dan bisnis sering menggunakan topologi ini. Topologi extended star merupakan topologi yang digunakan dalam penelitian ini. Tata cara perancangan jaringan komputer LAN sesuai kebutuhan masing-masing komputer client dapat dilihat pada setiap link jaringan yang akhirnya selesai dibuat. Menyebarkan penetapan alamat IP statistik mempunyai dampak negatif pada kehidupan kerja administrator. Jika etapan IP dilakukan secara perseorangan maka akan memakan waktu yang sangat lama. Salah satu cara sederhana untuk mengatasi masalah ini dan mempersingkat waktu pemecahan masalah adalah dengan mengatur DHCP untuk secara otomatis mengatur alamat IP router Anda. Administrator jaringan sering kali mengaktifkan DHCP saat mengatur alamat IP atau mendapatkannya secara otomatis(Ryansyah et al., 2018).

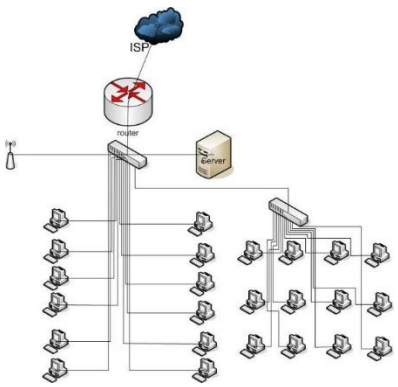
Terdapat beberapa informasi tentang port malware, seperti pada tabel 1 berikut:

Tabel 1. Data port malware

No.	Port	Nama
1	udp/31337	Back Orifice
2	tcp/12345	NetBus
3	tcp/12361	Whack-a-mole
4	tcp/21544	Girlfriend
5	tcp/5000,5001	Socket de Troie
6	tcp/3129,40421	Masters Paradise
7	tcp/6500	Devil
8	2140/udp	Deep Throat
9	23456	Evil FTP
10	6969	GateCrasher
11	456	Hacker Paradise
12	2801	Phineas P
13	4950/tcp	ICQ Trojan
14	7000	Remote Grab
15	530001	Shutdown Windows Jarak jauh

B. Rancangan Topologi Jaringan

Topologi jaringan yang dikembangkan pada penelitian ini terdiri dari router, board Mikrotik, ISP (Internet Service Provider), dan beberapa pengguna, antara lain server lokal, WLAN (Wireless Local Area Networks), dan LAN (Local Area Networks). Internet terhubung langsung ke router dan kemudian dibagi menjadi beberapa segmen jaringan yang dihubungkan melalui port berdasarkan lokasi kamar dan lemari. Selain switch jaringan, terdapat beberapa titik akses point di setiap lokasi dengan alamat IP berbeda tergantung wilayah(Ryansyah et al., 2018). Banyak topologi jaringan yang dibangun seperti terlihat pada gambar 2.

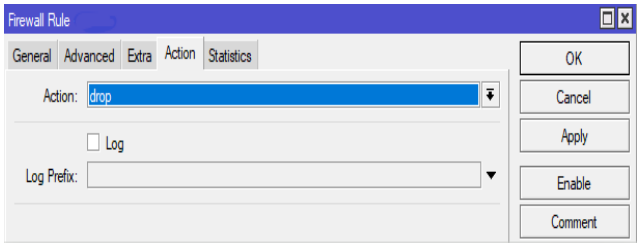


Gambar 2. Topologi Jaringan

C. Analisis Pengujian Jaringan

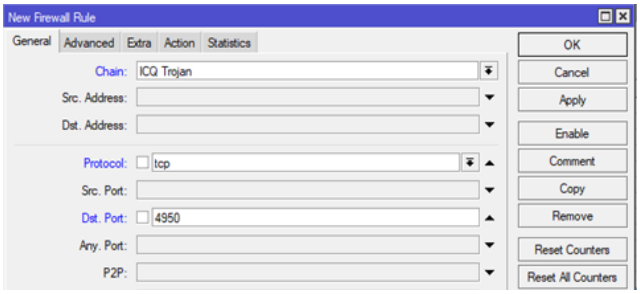
Penelitian ini menggunakan router Mikrotik tipe RB1100AHx2 yang memiliki spesifikasi CPU dual-core sehingga mampu menjangkau hingga seratus paket per hari dan mengurangi hardware coding. Berisi tiga port Ethernet gigabit, dua switch kelompok 5-port, dan kemampuan bypass Ethernet. Satu slot kartu microSD dan dua gigabyte RAM SODIMM dihilangkan. Memanfaatkan spesifikasi yang tepat dapat membantu pertumbuhan jaringan(Ryansyah et al., 2018).Login mikrotik

Untuk menambahkan rule ke pengaturan firelwall, harus mengakses router board sebagai admin utama. Setelah itu, dapat menambahkan rule, seperti pada gambar 3



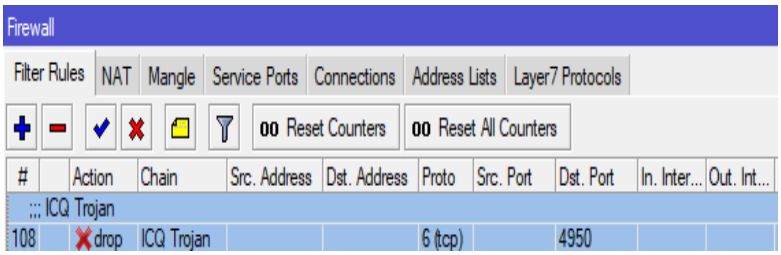
Gambar 3. Firewall Rule blok ICQ Trojan

1. Pengaturan firewall block ICQ trojan



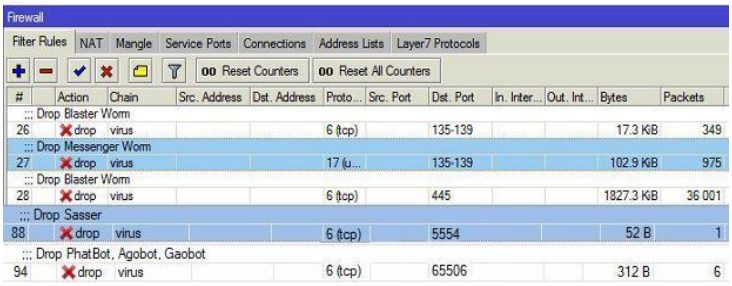
Gambar 4. Firewall Rule Mikrotik

Pada gambar diatas, merupakan cara untuk membuat peraturan firewall dengan nama virus, protokol, dan port. dapat juga menggunakan perintah / ip firewall filter add chain= ICQ Trojan protocol tcp dst-port 4950 action = drop comment = ICQ Trojan(Ryansyah et al., 2018), sehingga meanghasilkan seperti gambar dibawah.



Gambar 5. Hasil pengaturan Firewall untuk blok ICQ Trojan

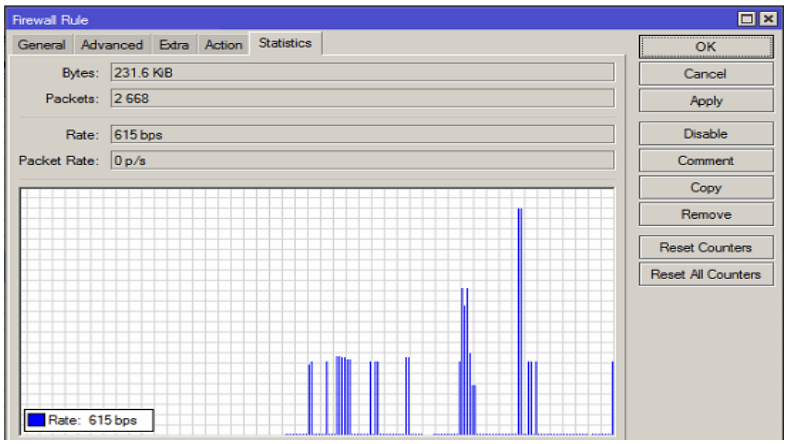
Metode ini tersedia untuk router Mikrotik. Namun, seiring dengan bertambahnya jumlah malware dan port, semakin banyak fitur terkait malware tentang port dan jenis malware lainnya yang dapat dipelajari dan ditemukan di banyak sumber. Analisis menunjukkan bahwa malware telah memasuki jaringan ketika byte, paket, dan data statistik sedang dipertukarkan. Berdasarkan informasi di atas, dapat dikatakan bahwa malware ada pada setiap pengguna atau perangkat komputer yang digunakan. Anda dapat mencegah perangkat pengguna lain agar tidak masuk ke dalam jaringan. terinfeksi oleh malware dengan memblokir akses ke perangkat jahat sebelum menggunakan jaringan router Anda(Ryansyah et al., 2018), seperti yang ditunjukkan pada gambar 6.



Gambar 6. Hasil Pengaturan Firewall di Mikrotik

2. Pengaturan firewall untuk block virus
   Jaringan komputer dapat diserang oleh virus, sehingga diperlukan suatu pemblokiran terhadap virus tersebut. sebelum dilakukan pemblokiran, sebaiknya melakukan pencarian port port mana saja yang berpotensi diserang oleh virus(Gunawan et al., 2022).
   Untuk melakukan pemblokiran virus maka dapat dilakukan dengan cara membuka tools yang ada di mikrotik yaitu terminal kemudian ketik ip firewall / add chain = virus protocol = tcp dst-port = 135-139 action = drop comment = "Blaster Worm".
   penggunaan tool harus menyesuaikan dengan jenis virus dan port yang diserang.

Setelah memasukkan jenis virus dan port yang dapat diserang serta memblokirnya, langkah selanjutnya adalah memeriksa statistik malware yang berjalan di jaringan. Hal ini dapat dilihat pada tab Statistics pada menu firewall Mikrotik.



Gambar 8. Firewall Rule Mikrotik

Hasil analisa dan kajian penelitian ini sangat membantu karena tidak hanya bandwidth yang memperlambat akses jaringan, namun ada faktor lain yang dapat menyebabkan peningkatan trafik jaringan. Dalam penelitian ini, metode seperti itu dapat digunakan untuk meminimalkan kondisi lalu lintas jaringan di perusahaan besar.

KESIMPULAN DAN SARAN

Dengan memblokir malware dan virus dalam port komputer dan membatasi penggunaan jaringan komputer menggunakan mikrotik dapat menghilangkan kekhawatiran dan kecemasan bagi setiap pengguna yang terhubung ke jaringan. Kemudian Jaringan akan lebih stabil, cepat, dan aman. Keuntungannya juga administrator memiliki kemampuan untuk menentukan port mana yang harus dibuka dan yang harus ditutup, dan mereka juga dapat bertindak sebagai lapis kedua untuk mencegah akses malware ke jaringan.

REFERENSI

Al-Saadoon, G. M. W., Professor, A., & Al-Bayatti, H. M. Y. (2011). A Comparison of Trojan Virus Behavior in Linux and Windows Operating Systems. In *World of Computer Science and Information Technology Journal (WCSIT)* (Vol. 1, Issue 3).

Eksan Nuryakin Habillah, A. (n.d.). *Terbit online pada laman web jurnal:*

https://ejurnalunsam.id/index.php/jicom/ Implementasi Keamanan Jaringan Metode Port Knocking dan Port Blocking Berbasis Mikrotik PT Securindo Packatama Indonesia. https://ejurnalunsam.id/index.php/jicom/

Ernawati, R., Ruslianto, I., Bahri, S., Rekayasa, J., Komputer, S., Mipa, F., Tanjungpura, U., Prof, J., Hadari, H., & Pontianak, N. (n.d.). *Coding: Jurnal Komputer dan Aplikasi Implementasi Metode Port Knocking Pada Sistem Keamanan Server Ubuntu Virtual Berbasis Web Monitoring*.

Gunawan, I., Okta Kirana, I., & Artikel, G. (2022). Optimasi Sistem Keamanan Jaringan Komputer Terhadap Serangan Malware Menggunakan Filtering Firewall dengan Metode Port Blocking Optimization of Computer Network Security System Against Malware Attacks Using Firewall Filtering with Port Blocking Method Article Info ABSTRAK. *JOMLAI: Journal of Machine Learning and Artificial Intelligence*, *1*(2), 2828–9099. https://doi.org/10.55123/jomlai.v1i2.816

Haidar Hari, N., Prasetyo Eka Putra, F., Hasanah, U., & Ririn Sutarsih, S. (n.d.). *Transformasi Jaringan Telekomunikasi dengan Teknologi 5G: Tantangan, Potensi, dan Implikasi*. https://doi.org/10.37034/jidt.v5i1.357

Ilham, M., Gunawan, I., & Siregar, Z. A. (2022). Keamanan Jaringan Wlan Dengan Metode Firewall Filtering Menggunakan Mikrotik Pada Smp Negeri 1 Dolok Merawan. *Juisik*, *2*(3). http://journal.sinov.id/index.php/juisik/indexHalamanUTAMAJurnal:https://journal.sinov.id/index.php

Irawan, G. T., Djaohar, M., & M. Ficky Duskarnaen. (2018). Perancangan Dan Implementasi Sistem Keamanan Jaringan Menggunakan Firewall dan Web Proxy Berbasis Mikrotik di SMA Negeri 1 Kota Sukabumi. *PINTER : Jurnal Pendidikan Teknik Informatika Dan Komputer*, *2*(1), 27–32. https://doi.org/10.21009/pinter.2.1.4

Jurnal, H., & Jakaria, D. A. (2020). *Jurnal Teknik Informatika Implementasi Firewall Dan Web Filtering Pada Mikrotik Routeros Untuk Mendukung Internet Sehat Dan Aman (Insan)*. *8*(2).

Keamanan Jaringan Bpkad Provinsi Sumsel, U., Brades, T., Komputer, T., Vokasi, F., & Bina Darma, U. (n.d.-a). *Seminar Hasil Penelitian Vokasi (Semhavok) Pemanfataan Metode Port Knocking Dan Blocking*.

Keamanan Jaringan Bpkad Provinsi Sumsel, U., Brades, T., Komputer, T., Vokasi, F., & Bina Darma, U. (n.d.-b). *Seminar Hasil Penelitian Vokasi (Semhavok) Pemanfataan Metode Port Knocking Dan Blocking*.

Kumar, G., & Kumar, K. (2014). Network security – An updated perspective. *Systems Science and Control Engineering*, *2*(1), 325–334. https://doi.org/10.1080/21642583.2014.895969

Nur Khasanah STMIK Nusa Mandiri Jakarta, S. (2016). *Keamanan Jaringan Dengan Packet Filtering Firewall (Studi Kasus: Pt. Sukses Berkat Mandiri Jakarta): Vol. Iv* (Issue Desember).

Ocanitra, R., & Ryansyah, M. (2019). *Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen*. *7*(1), 7–12.

Prasetyo, F., Putra, E., Arman, D., Putra, M., Firdaus, A., & Hamzah, A. (n.d.). Analisis Kecepatan Dan Kinerja Jaringan 5G (Generasi ke 5) Pada Wilayah Perkotaan. *Informatics for Educators And Professionals: Journal of Informatics*, *8*(1), 47–51.

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

Rizky, D., #1, S., Widiyasono, N., & Mubarok, H. (2016). Investigasi Serangan Malware Njrat Pada PC. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *2*(2).

Robbahul Barra, A., Sujatmika, R., & Umami, I. (2022). Sistem Keamanan Jaringan Komputer Bridge Firewall Menggunakan Router Board Mikrotik RB750. *Jurnal Teknologi Dan Sistem Informasi Bisnis-JTEKSIS*, *4*(1), 427. https://doi.org/10.47233/jteksis.v4i2.561

Ryansyah, M., Sony Maulana, M., Mandiri Jakarta Jl Damai No, N., Jati Barat, W., & Selatan, J. (2018). *Malware Security Menggunakan Filtering Firewall Dengan Metode Port Blocking Pada Mikrotik RB 1100AHx2*. *6*(3).

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

Suchendra, D. R., Fitra Rahman, A., Juli, S., & Ismail, I. (2017). Penerapan Sistem Pengamanan Port Pada Layanan Jaringan Menggunakan Port Knocking. In *Jurnal LPKIA* (Vol. 10, Issue 2).

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

Wicaksono, D., & Widiasari, I. R. (2022). *Sistem Keamanan Jaringan Menggunakan Firewall Dengan Metode Port Blocking Dan Firewall Filtering*. *9*(2), 1380–1392. http://jurnal.mdp.ac.id