Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Taufik Rahman
Assignment title:	Check - No Respository 14
Submission title:	Jurnal SINUS Taufik Rifqi.doc
File name:	Jurnal_SINUS_Taufik_Rifqi.doc
File size:	817.5K
Page count:	12
Word count:	3,326
Character count:	22,590
Submission date:	21-Aug-2024 03:05AM (UTC-0400)
Submission ID:	2435420327

Jurnal Ilmiah Sinus (JIS) Vol : xxx, No. xx, Bulan Tahun
ISSN (Print) : 1693-1173 , ISSN (Online): 2548-4028

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

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

ABSTRACT

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

I. PENDAHULUAN

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

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

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

Jurnal Ilmiah SINUS (JIS).....1

Jurnal SINUS Taufik Rifqi.doc

by Taufik Rahman

Submission date: 21-Aug-2024 03:05AM (UTC-0400)
Submission ID: 2435420327
File name: Jurnal_SINUS_Taufik_Rifqi.doc (817.5K)
Word count: 3326
Character count: 22590

Jurnal Ilmiah Sinus (JIS) Vol : xxx, No. xx, Bulan Tahun
ISSN (Print) : 1693-1173 , ISSN (Online): 2548-4028

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

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

ABSTRACT

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

I. PENDAHULUAN

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

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

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

mencegah akses yang tidak sah dan mengatur akses yang diizinkan, memungkinkan pengguna untuk merespons dengan cepat terhadap ancaman keamanan yang muncul.

II. TINJAUAN PUSTAKA

Menurut artikel yang ditulis oleh (Jamalul'ain & Nurdiawan, 2022) dengan judul "Optimalisasi Keamanan Jaringan Komputer Menggunakan Metode Knocking Port Berbasis Mikrotik, Tujuan penelitian ini adalah untuk mendeteksi serangan ataupun gangguan dari attacker serta menginvestigasi aktivitas yang dilakukan oleh attacker. Mikrotik Router ini digunakan untuk memblokir alamat IP maupun MAC address yang tidak dikenal, sehingga memantau keamanan jaringan wireless yang lebih efisien. Dalam penelitian ini, metode yang digunakan adalah menerapkan dan mengoptimalkan keamanan jaringan WLAN dengan menggunakan firewall filtering mac address yang tersedia."

Menurut artikel yang ditulis oleh (Rozan et al., 2024)yang berjudul "Implementasi Web Proxy Pada Mikrotik Untuk Mengoptimalkan Keamanan Jaringan Wirelless LAN Di Lingkungan Sekolah MAN 1 Gresik, Tujuan penelitian ini adalah untuk mengimplementasikan web proxy pada Mikrotik untuk mencegah akses ke situs-situs yang tidak diinginkan, serta meningkatkan keamanan jaringan dengan menggunakan fitur firewall dan web proxy."

Menurut artikel yang ditulis oleh (Muzakir & Ulfa, 2019) yang berjudul "Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan Jaringan, Tujuan penelitian ini adalah melihat secara komprehensif kemampuan *packet filtering* yang terdapat di *mikrotik routerboard* dalam mengatasi masalah keamanan jaringan komputer. *Filtering rule* mampu melakukan blok *url* yang ada pada *protocol HTTP* maupun *HTTPS* yang mana membuktikan bahwa kinerja dari *filtering rule* cukup baik, penelitian ini kinerja *packet filtering* menggunakan *tool network packet anayzer* Wireshark dengan cara melakukan capture paket yang lewat didalam jaringan dan menampilkan semua informasi secara detil."

Menurut artikel yang ditulis oleh (Diansyah et al., 2019)yang berjudul "Pemanfaatan Layer 7 Pada Mikrotik Untuk Manajemen Bandwidth dan Blocking Situs, penelitian ini bertujuan Untuk menghindari monopoli bandwidth, dan memastikan bahwa setiap klien memiliki jatah bandwidth mereka sendiri. Meskipun ada perbedaan, jika Situs web yang dibuka termasuk situs web asusila, maka harus dibuat filter agar tidak dapat membuka situs tersebut. Namun, berdasarkan pengalaman dalam pembocoran situs, ada beberapa situs yang sekarang lebih mudah bocor, seperti menggunakan pemfilteran DNS Nawala dan web proxy mikrotik."

Menurut artikel yang ditulis oleh (Sulistyo & Sartomo, 2022)yang berjudul "Model Keamanan Jaringan Menggunakan Firewall Port Blocking, penelitian ini bertujuan mengembangkan keamanan jaringan komputer dengan berbagai metode, termasuk metode standar, keamanan port statis, keamanan port dinamis, dan keamanan port sticky. Keamanan port statis adalah keamanan jaringan yang bekerja secara otomatis dengan alamat MAC yang terdaftar pada setiap komputer, dan alamat MAC ini tidak dapat ditukar untuk setiap perangkat jaringan."

Menurut artikel yang ditulis oleh (Syaripudin & Nugraha, 2023) yang berjudul "Analisa Dan Implementasi Blocking Website Dengan Metode 7 Layer Pada Perangkat Mikrotik Di Garage Freshmart", penelitian ini bertujuan meminimalisir permasalahan yang ada kemungkian terjadi dengan perangkat Mikrotik dapat memanfaatkan pemblokiran situs dengan metode *layer 7* pada sistem jaringan Garage Freshmart.

Menurut artikel yang ditulis oleh (Fritz Gamaliel & P. Yudi Dwi Arliyanto, 2022) yang berjudul "Perancangan Manajemen Jaringan Komputer Berbasis MikroTik dengan

Top Down Network Design" penelitian ini bertujuan mengatur *bandwidth*, mengatur *firewall*, mengatur notifikasi masalah jaringan, mengatur *wifi seamless,* mengatur *loop protect,* mengatur *failover link internet,* mengatur monitoring jaringan, maupun mengatur *tunneling*.

Menurut artikel yang ditulis oleh (Sutarti et al., 2023) yang berjudul " Analisis Web Phishing Menggunakan Metode Network Forensic Dan Block Access Situs Dengan Router Mikrotik" penelitian dengan investigasi forensik digital, yang terdiri dari tahap pengkoleksian, pemeriksaan, analisis dan pelaporan.

III. METODE PENELITIAN

Pada penelitian ini, metode penelitian terdiri dari beberapa langkah berikut:

1. Studi Literatur: Meneliti teori dan praktik mengenai firewall, khususnya Mikrotik, serta prinsip dasar blocking akses dan keamanan jaringan.
2. Analisis Kebutuhan: Mengidentifikasi kebutuhan spesifik dari Kantor Desa Cibalandong terkait keamanan jaringan melalui wawancara dan observasi.
3. Desain Sistem: Merancang konfigurasi firewall Mikrotik untuk blocking akses sesuai dengan kebutuhan yang telah diidentifikasi.
4. Implementasi: Menginstal dan mengonfigurasi sistem firewall Mikrotik di Kantor Desa Cibalandong sesuai dengan desain yang dibuat.
5. Pengujian dan Evaluasi: Melakukan serangkaian uji coba untuk menilai efektivitas konfigurasi firewall dalam blocking akses dan dampaknya terhadap keamanan jaringan.
6. Analisis Data: Menganalisis hasil pengujian untuk menilai pencapaian tujuan penelitian dan efektivitas sistem firewall yang diterapkan.

Untuk menggunakan aplikasi Winbox dalam simulasi sistem jaringan komputer, ada beberapa tahapan dan persyaratan yang harus dipenuhi.

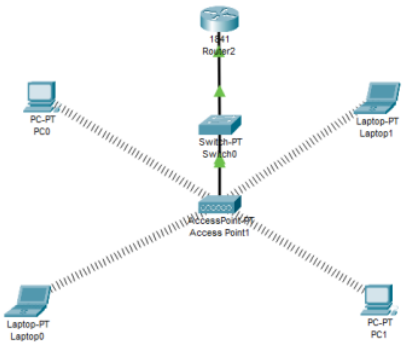
Hardware dan Software

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

Topologi Jaringan

Untuk kantor desa Cibalandong Subang, topologi jaringan yang digunakan adalah topologi star, yang memungkinkan koneksi langsung antara dua perangkat, seperti menara pemancar internet dan kantor desa. Topologi ini lebih stabil dan terjamin daripada topologi lain, seperti topologi bus atau ring, yang rentan terhadap gangguan dan kegagalan pada satu perangkat.

Dan mudah diperluas dengan menambahkan perangkat baru ke router pusat tanpa mengganggu operasi jaringan yang ada, dan hampir mendekati komponen yang ada di kantor desa cibalandong subang.



Gambar 1. Topologi Star yang digunakan di Desa Cibalandong

IV. HASIL DAN PEMBAHASAN

Hasil dari penelitian ini menunjukkan bahwa implementasi firewall Mikrotik berhasil meningkatkan keamanan jaringan di Kantor Desa Cibalandong. Beberapa temuan kunci meliputi:.

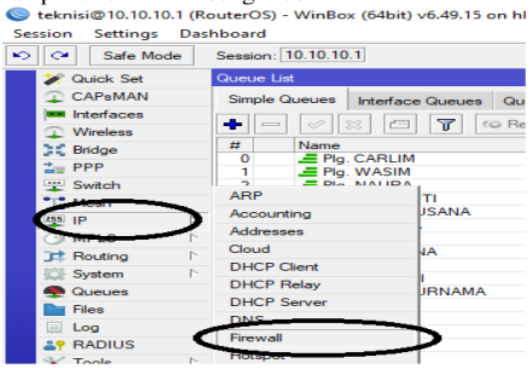
Efektivitas Blocking Akses

Konfigurasi firewall Mikrotik berhasil memblokir akses yang tidak sah sesuai dengan aturan yang diterapkan, mencegah akses dari sumber yang tidak dikenal dan mengurangi potensi risiko keamanan. Dalam kasus ini memblokir situs-situs yang dianggap mengganggu kinerja jaringan karena banyaknya pengguna yang mengaksesnya. Situs yang diblokir adalah situs berita seperti detik.com

Adapun cara penulis memblokir web dan konten-konten tersebut adalah sebagai berikut:

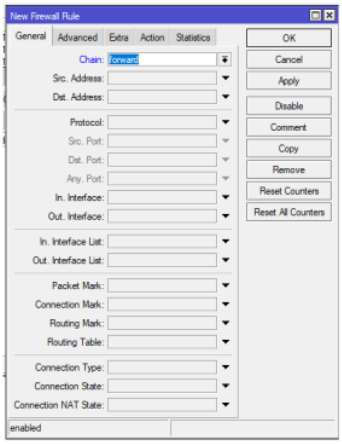
Akses ke filter web dan konten firewall.

Konfigurasi IP Firewall dapat ditemukan sebagai berikut:



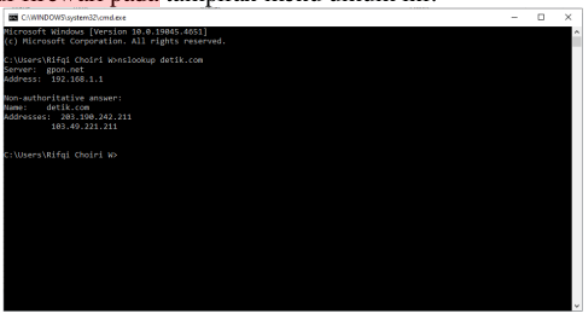
Gambar 2. Tampilan Konfigurasi Filtering

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



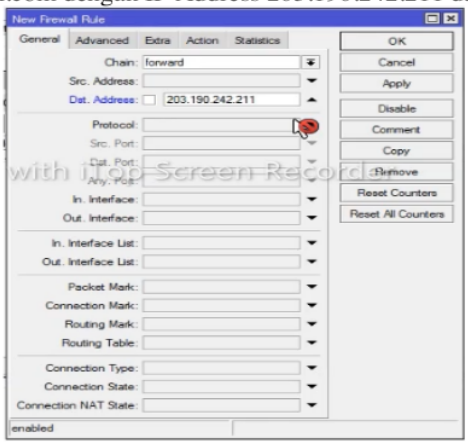
Gambar 3. Tampilan Konfigurasi Firewall Rule

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



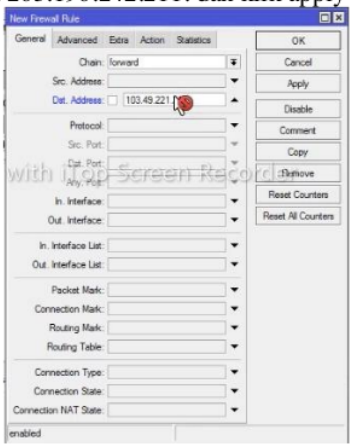
Gambar 4. Tampilan cmd nslookup

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



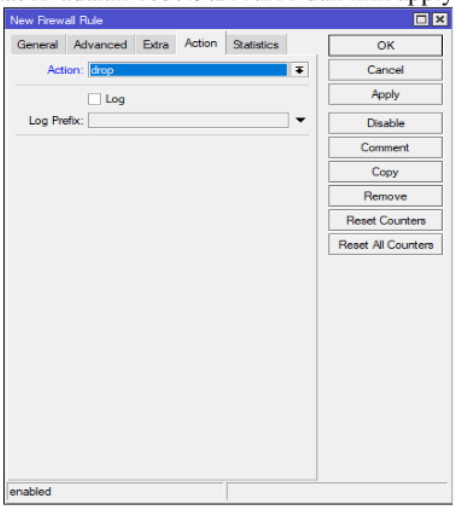
Gambar 5. Tampilan Destination Address

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



Gambar 6. Tampilan Destination Address

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



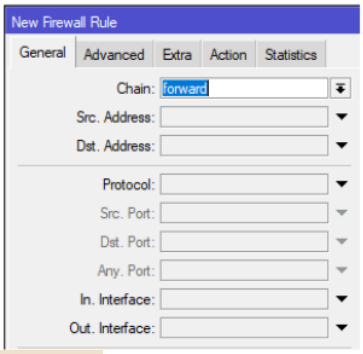
Gambar 7. Tampilan Menu Action

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

Gambar 8. List IP yang sudah di blokir

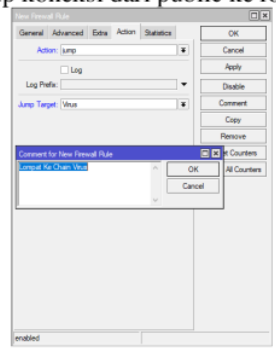
Pada antarmuka aplikasi WinBox menunjukkan bahwa ada sebuah aturan firewall yang diatur untuk menghentikan akses ke alamat IP tertentu, misalnya 203.190.242.211 dan 103.49.211.211. Aturan ini memiliki tindakan "drop", yang berarti bahwa paket data yang menuju ke alamat IP tersebut tidak akan dikirim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

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



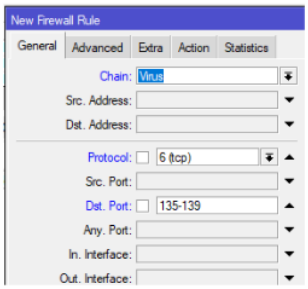
Gambar 9. Tampilan Firewall Rule

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



Gambar 10. Konfigurasi Jump

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



Gambar 11. Rule Custom-Chain Virus

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

=>add chain=virus protocol=udp dst-port=135-139 action=drop

Digunakan untuk mengelola layanan jarak jauh seperti server DHCP, server DNS, dan WINS

=>add chain=virus protocol=tcp dst-port=445 action=drop

Digunakan untuk layanan windows share.

=>add chain=virus protocol=tcp dst-port=593 action=drop

Digunakan untuk Microsoft Exchange server dan layanan model objek komponen.

=>add chain=virus protocol=tcp dst-port=1024-1030 action=drop

Digunakan untuk memungkinkan komponen perangkat lunak berkomunikasi satu sama lain melalui komputer jaringan.

=>add chain=virus protocol=tcp dst-port=1080 action=drop

Digunakan untuk menghubungkan server proxy ke klien dan server melalui pertukaran paket jaringan.

=>add chain=virus protocol=tcp dst-port=1214 action=drop

Digunakan sebagai aplikasi berbagi file peer-to-peer menggunakan protokol FastTrack.

=>add chain=virus protocol=tcp dst-port=1433-1434 action=drop

Digunakan untuk sistem manajemen database Microsoft SQL Server.

=>add chain=virus protocol=tcp dst-port=2535 action=drop

Digunakan untuk berkomunikasi, memberikan host kemampuan untuk meminta alamat multicast dari server.

=>add chain=virus protocol=tcp dst-port=2745 action=drop

Digunakan dalam sistem telekomunikasi voice over IP (VoIP) untuk pensinyalan dan panggilan.

=>add chain=virus protocol=tcp dst-port=3127-3128 action=drop

Digunakan sebagai proxy web untuk menyimpan dokumen web secara sementara.

=>add chain=virus protocol=udp dst-port=4444 action=drop

Digunakan untuk melayani permintaan dan melaporkan acara dan kesalahan.

=>add chain=virus protocol=tcp dst-port=4444 action=drop

Digunakan untuk konten server seperti Oracle.

=>add chain=virus protocol=tcp dst-port=5554 action=drop

Digunakan sebagai port nirkabel standar Fastboot.

=>add chain=virus protocol=udp dst-port=445 action=drop

Digunakan untuk file sharing

=>add chain=virus protocol=tcp dst-port=9898 action=drop

Digunakan untuk mengawasi dan mengingatkan perubahan file di berbagai sistem

=>add chain=virus protocol=tcp dst-port=10000 action=drop

Digunakan sebagai penerima dan mentransmisikan lalu lintas telepon suara yang termasuk Google Voice.

=>add chain=virus protocol=tcp dst-port=12345 action=drop

digunakan untuk mengontrol sistem komputer dari jauh.

=>add chain=virus protocol=tcp dst-port=10080 action=drop

Digunakan untuk game.

=>add chain=virus protocol=tcp dst-port=27374 action=drop

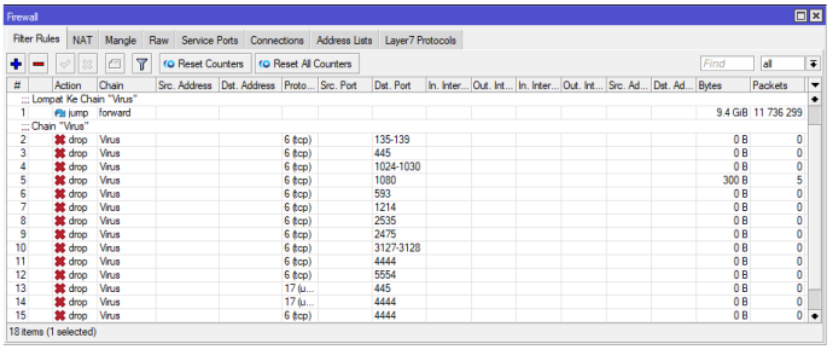
Digunakan untuk virus Trojan

Port-port ini jarang digunakan untuk komunikasi dan rentan terhadap penyebaran virus dan malware.

Kinerja Jaringan: Meskipun melakukan blocking akses, sistem firewall tidak mengakibatkan penurunan kinerja jaringan yang signifikan. Koneksi tetap stabil dan efisien.

Pengelolaan Akses: Konfigurasi firewall memungkinkan pengaturan akses yang lebih baik untuk pengguna yang sah, sesuai dengan kebijakan yang ditetapkan.

Pembahasan mencakup analisis bagaimana konfigurasi firewall Mikrotik berfungsi dalam prakteknya, tantangan yang dihadapi selama implementasi, dan perbandingan dengan solusi keamanan lain yang mungkin digunakan di lingkungan serupa.



Gambar 12. List Firewall Filter

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

Setelah mengevaluasi sistem jaringan yang ada di Kantor desa cibalandong subang, penulis menambahkan router mikrotik untuk menjembatani jaringan internet atau jaringan luar dengan jaringan lokal di Kantor desa cibalandong subang. Selain itu, penulis menggunakan mikrotik sebagai router dan juga menggunakannya sebagai filter terhadap situs-situs yang dianggap mengganggu kinerja jaringan.

Pengujian Jaringan Awal

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

Gambar 13. Tampilan Web Sebelum Diblokir

Pengujian Aturan Blocking Akses

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

Gambar 14. Tampilan Web Sesudah Diblokir

V. KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Bagian ini memuat kesimpulan dan saran. Kesimpulan dan saran dapat dibuat dalam sub bagian yang terpisah. Kesimpulan menjawab tujuan bukan mengulang teori berarti menyatakan hasil penelitian secara ringkas, tetapi bukan ringkasan pembahasan.

Berdasarkan hasil penelitian dan analisis yang telah dilakukan, dapat disimpulkan bahwa:

1. MikroTik sebagai perangkat router yang digunakan di Kantor Desa Cibalandong Subang telah terbukti efektif dalam mengoptimalkan blocking akses firewall. Dengan konfigurasi yang tepat, MikroTik dapat memblokir situs-situs yang mengganggu kinerja jaringan serta mencegah penyebaran virus melalui pengaturan port dan protokol tertentu.
2. Faktor-Faktor yang Perlu Dipertimbangkan: Dalam mengoptimalkan blocking akses firewall, beberapa faktor penting yang perlu diperhatikan adalah:
   a. Topologi jaringan yang digunakan, yang dalam kasus ini adalah topologi star yang memudahkan pengembangan tanpa mengganggu operasi jaringan lainnya.
   b. Pemilihan perangkat keras dan perangkat lunak yang sesuai, seperti penggunaan MikroTik dan Avira antivirus untuk memastikan keamanan jaringan yang optimal.
   c. Keberlanjutan dan kemudahan manajemen jaringan yang didukung oleh perangkat yang telah digunakan di Kantor Desa Cibalandong Subang.
3. Efektivitas Blocking Akses Firewall: Implementasi blocking akses firewall menggunakan MikroTik di Kantor Desa Cibalandong Subang telah berhasil meningkatkan keamanan jaringan. Hal ini terbukti dengan berkurangnya akses terhadap

situs-situs yang tidak diinginkan dan pencegahan penyebaran virus melalui port dan protokol yang rentan.

5.2 SARAN

Saran merupakan penelitian lanjutan yang dirasa masih diperlukan untuk menyempurnakan hasil penelitian.

Beberapa Saran yang dapat disampaikan adalah sebagai berikut:

a) Peningkatan Kesadaran Keamanan: Latih staf di Kantor Desa Cibalandong mengenai praktik keamanan siber dan penggunaan firewall. Edukasi tentang cara mengenali ancaman dan mengelola akses dengan benar dapat meningkatkan efektivitas sistem keamanan.
b) Pemantauan dan Pemeliharaan Rutin: Implementasikan sistem pemantauan jaringan untuk mendeteksi dan merespons potensi ancaman secara real-time. Lakukan pemeliharaan rutin dan pembaruan konfigurasi firewall untuk menanggapi perubahan kebutuhan dan ancaman baru.
c) Penilaian Berkala: Lakukan penilaian berkala terhadap konfigurasi firewall dan kebijakan keamanan. Evaluasi ini harus melibatkan simulasi serangan dan uji coba skenario untuk memastikan bahwa firewall tetap efektif dalam melindungi jaringan.
d) Dokumentasi dan Prosedur: Buat dokumentasi yang jelas mengenai konfigurasi firewall, kebijakan akses, dan prosedur respons insiden. Dokumentasi ini akan memudahkan pemeliharaan, audit, dan pelatihan staf.
e) Integrasi dengan Sistem Keamanan Lain: Pertimbangkan integrasi firewall dengan solusi keamanan tambahan seperti sistem deteksi intrusi (IDS) atau sistem pencegahan intrusi (IPS) untuk perlindungan yang lebih menyeluruh.

Saran untuk Penelitian Lanjutan

a. Evaluasi Skala Lebih Besar: Lakukan penelitian untuk mengevaluasi penerapan firewall Mikrotik di lingkungan yang lebih luas atau di berbagai jenis organisasi untuk membandingkan hasil dan efektivitasnya dalam konteks yang berbeda.
b. Analisis Dampak Jangka Panjang: Teliti dampak jangka panjang dari penerapan firewall terhadap performa jaringan dan keamanan, termasuk efek dari pembaruan konfigurasi dan perubahan kebijakan.
c. Studi Keterhubungan Teknologi: Investigasi bagaimana firewall Mikrotik berinteraksi dengan teknologi jaringan lainnya seperti perangkat keras dan perangkat lunak keamanan tambahan. Ini dapat memberikan wawasan tentang cara mengoptimalkan sistem keamanan secara keseluruhan.
d. Perbandingan Solusi Keamanan: Lakukan perbandingan mendalam antara firewall Mikrotik dan solusi keamanan jaringan lainnya, seperti firewall dari vendor lain, untuk mengevaluasi kelebihan dan kekurangan masing-masing dalam konteks yang serupa.
e. Pengembangan Metodologi Baru: Kembangkan metodologi baru untuk konfigurasi dan pengujian firewall yang dapat meningkatkan akurasi dan efisiensi evaluasi keamanan. Ini dapat mencakup teknik-teknik baru dalam analisis risiko dan pengujian penetrasi.
f. Penelitian tentang Ancaman Baru: Fokuskan penelitian pada ancaman baru dan emerging threats yang mungkin mempengaruhi efektivitas firewall. Meneliti bagaimana firewall Mikrotik dapat dikembangkan untuk mengatasi ancaman ini akan meningkatkan kemampuan pertahanan.

Mengikuti saran ini dapat membantu meningkatkan efektivitas sistem keamanan yang ada dan memberikan kontribusi signifikan pada pengetahuan di bidang keamanan jaringan.

DAFTAR PUSTAKA

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

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

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

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

Muzakir, A., & Ulfa, M. (2019). Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan Jaringan. *Simetris: Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*, *10*(1), 15–20. https://doi.org/10.24176/simet.v10i1.2646

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

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

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

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

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

Jurnal SINUS Taufik Rifqi.doc

ORIGINALITY REPORT

22%	22%	13%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Sebelas Maret Student Paper	6%
2	mikrotik.co.id Internet Source	2%
3	ojs.cbn.ac.id Internet Source	1%
4	comserva.publikasiindonesia.id Internet Source	1%
5	repository.universitasbumigora.ac.id Internet Source	1%
6	keguruan.umm.ac.id Internet Source	1%
7	ojs.cahayamandalika.com Internet Source	1%
8	ejournal.bsi.ac.id Internet Source	1%
9	journal.pubmedia.id Internet Source	1%

10	lppm.politeknikmeta.ac.id Internet Source	1 %
11	e-jurnal.lppmunsera.org Internet Source	<1 %
12	p3m.sinus.ac.id Internet Source	<1 %
13	ejournal.poltekharber.ac.id Internet Source	<1 %
14	archive.umsida.ac.id Internet Source	<1 %
15	journal.fkpt.org Internet Source	<1 %
16	repository.nusamandiri.ac.id Internet Source	<1 %
17	Submitted to LL DIKTI IX Turnitin Consortium Part II Student Paper	<1 %
18	Submitted to Tamalpais Union High School District Student Paper	<1 %
19	forum.shiftdelete.net Internet Source	<1 %
20	www.elfak.ni.ac.rs Internet Source	<1 %

21	media.neliti.com Internet Source	<1 %
22	download.garuda.kemdikbud.go.id Internet Source	<1 %
23	ejournal.uin-malang.ac.id Internet Source	<1 %
24	idm.or.id Internet Source	<1 %
25	it.proxsisgroup.com Internet Source	<1 %
26	journal.admi.or.id Internet Source	<1 %
27	www.harianumum.com Internet Source	<1 %
28	www.kompasiana.com Internet Source	<1 %
29	www.teknologipintar.org Internet Source	<1 %
30	Muhammad Sholeh Bathin, Desi Ramayanti. "SOBATHUNI : Aplikasi Rumah Sewa Berbasis Web", Jurnal Edukasi dan Penelitian Informatika (JEPIN), 2019 Publication	<1 %
31	dspace.ewha.ac.kr Internet Source	<1 %

32	ejournal.uika-bogor.ac.id Internet Source	<1 %
33	www.flickr.com Internet Source	<1 %
34	www.slideshare.net Internet Source	<1 %
35	Andi Usri Usman, Syaechurodji Syaechurodji. "REKAYASA PERANGKAT LUNAK SISTEM INFORMASI GEOGRAFIS (SIG) TATA LETAK PENYEDIA SARANA PENANGGULANGAN KEBAKARAN", Jurnal Sistem Informasi dan Informatika (Simika), 2019 Publication	<1 %
36	Submitted to Universitas International Batam Student Paper	<1 %
37	journal.iaincurup.ac.id Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	Off		

Jurnal SINUS Taufik Rifqi.doc