JURNAL RESISTOR | ISSN 2598-7542 | E-ISSN 2598-9650
Vol. 6 No 3 – Desember 2023 | https://s.id/jurnalresistor
DOI: https://doi.org/10.31598
Publishing: Prahasta Publisher

Implementasi *Port Knocking*, *Port Blocking* Pada Keamanan Jaringan Komputer Berbasis Mikrotik

Intan Putri Ayu Agita[1], Sopian Soim[2]

[1,2] Politeknik Negeri Sriwijaya, Palembang, Indonesia

intanputriayuagita@gmail.com[1], sopian_soim@polsri.ac.id[2]
Kontak WA: +6282377993067[1], +6281373140678[2]

Received : November, 2023r	Accepted : December, 2023	Published : December, 2023

Abstract

The development of the Internet in modern times like now is very sophisticated, but the more sophisticated the times, there will also be many to watch out for because of the many attacks that can be carried out by hackers, especially in the network security section. Network security is very important to pay more attention to. For this reason, security that is difficult to penetrate must be prepared to secure and minimize the risk of threats to the network. Therefore, in this study the author conducted an experiment entitled "Implementation of Port Knocking, Port Blocking on Mikrotik-Based Computer Network Security". The variables used are based on proxy with the aim of increasing the security of computer user access by preventing data and information theft, and keeping data safe. The final results of the study show that users have to authenticate on certain ports, which makes the server more secure. In addition, some ports are also closed to prevent access attacks from unauthorized parties. By combining port knocking and port blocking, attacks from unauthorized parties become more difficult.

Keywords: *Port Knocking, Port Blocking, Network Security*

Abstrak

Perkembangan Internet pada zaman modern seperti sekarang sangatlah canggih, akan tetapi semakin canggih perkembangan zaman maka akan banyak pula yang harus diwaspadai karena banyaknya serangan yang bisa dilakukan oleh para hacker terutama di bagian keamanan jaringan. Keamanan jaringan sangat penting untuk lebih diperhatikan. Untuk itu harus dipersiapkan keamanan yang sulit ditembus untuk mengamankan dan meminimalisir resiko ancaman pada jaringa. Oleh karena itu dalam penelitian ini penulis melakukan eksperimen dengan judul "Implementasi Port Knocking, Port Blocking Pada Keamanan Jaringan Komputer Berbasis Mikrotik". Variable yang digunakan ialah berbasis mikrotik dengen tujuan untuk meningkatkan keamanan akses pengguna komputer dengan mencegah pencurian data dan informasi, serta menjaga data tetap aman. Hasil akhir penelitian menunjukkan bahwa pengguna harus melakukan autentikasi pada port tertentu, yang membuat server menjadi lebih aman. Selain itu, beberapa port juga ditutup untuk mencegah serangan akses dari pihak yang tidak sah. Dengan menggabungkan metode port knocking dan penutupan port (port blocking), serangan dari pihak yang tidak berwenang menjadi lebih sulit.

Kata Kunci: *Port Knocking, Port Blocking, Keamanan Jaringan*

1. PENDAHULUAN

Saat ini, pentingnya jaringan komputer semakin meningkat, baik dalam konteks pendidikan maupun dunia kerja. Salah satu aspek krusial dalam mengelola jaringan tersebut adalah menjaga keamanannya [1]. Keamanan jaringan sangat penting untuk lebih diperhatikan, terlebih saat komputer terhubung dengan internet maka serangan pun akan semakin terus meningkat. Untuk itu harus dipersiapkan keamanan yang sulit ditembus untuk mengamankan dan meminimalisir ancaman pada jaringan [2].

Keamanan komputer merupakan bidang teknologi yang mencakup perlindungan informasi pada sistem komputer. Tujuan utamanya adalah melindungi informasi dari potensi pencurian, kerusakan, atau menjaga ketersediaan, sesuai dengan prinsip-prinsip yang tercantum dalam kebijakan keamanan [3]. Keamanan jaringan adalah konsep yang mencakup berbagai teknologi, perangkat, dan prosedur yang dirancang untuk mengidentifikasi dan mencegah akses yang tidak sah ke jaringan. Secara sederhana, sistem keamanan jaringan bertujuan untuk mencegah orang yang tidak berhak masuk ke jaringan. Keamanan jaringan bertujuan untuk mengurangi risiko ancaman seperti pencurian data dan kerusakan fisik pada perangkat *computer* [4].

Keamanan jaringan dapat diterapkan dengan beberapa metode. Adapun penelitian [5] berjudul "Implementasi Keamanan Jaringan Menggunakan Port Knocking" menunjukkan bahwa program port knocking memiliki kemampuan untuk menentukan akses mana yang dapat diakses oleh klien dan mana yang tidak. Ketika klien tidak memiliki akses, berbagi file atau berkomunikasi dengan server menjadi tidak mungkin. Metode port knocking digunakan untuk mengatur parameter sehingga perangkat komputer tidak memiliki port komunikasi yang terbuka secara bebas, namun masih dapat dijangkau dari luar untuk mencegah serangan saat port terbuka.

MikroTik Router merupakan sistem operasi yang efektif sebagai router jaringan, menyediakan beragam fitur lengkap untuk jaringan dan teknologi nirkabel. Selain berperan sebagai firewall untuk komputer lain, MikroTik memungkinkan pemberian prioritas akses internet dan data lokal kepada komputer lainnya. Fokus MikroTik adalah mengatur bandwidth dan melakukan manajemen jaringan komputer [6].

Pada penelitian ini dikembangkan dua metode yaitu port knocking dan port blocking. Kedua metode yang di simulasikan ini merupakan metode yang digunakan dalam mencegah sekaligus mengamankan akses dari attacker yang akan melakukan pembobolan keamanan jaringan.

Port knocking adalah suatu teknik yang digunakan untuk meningkatkan keamanan komputer dengan meminta pengguna atau perangkat yang ingin mengakses layanan untuk melakukan serangkaian tindakan terkendali, mirip seperti memberikan ketukan atau "ketukan pintu" pada urutan port tertentu sebelum layanan tersebut dapat diakses. Dengan kata lain, akses ke layanan komputer tidak dapat diperoleh secara langsung tanpa melakukan proses "ketukan" yang telah ditentukan terlebih dahulu, yang mungkin arus diotorisasi oleh seorang administrator [7].

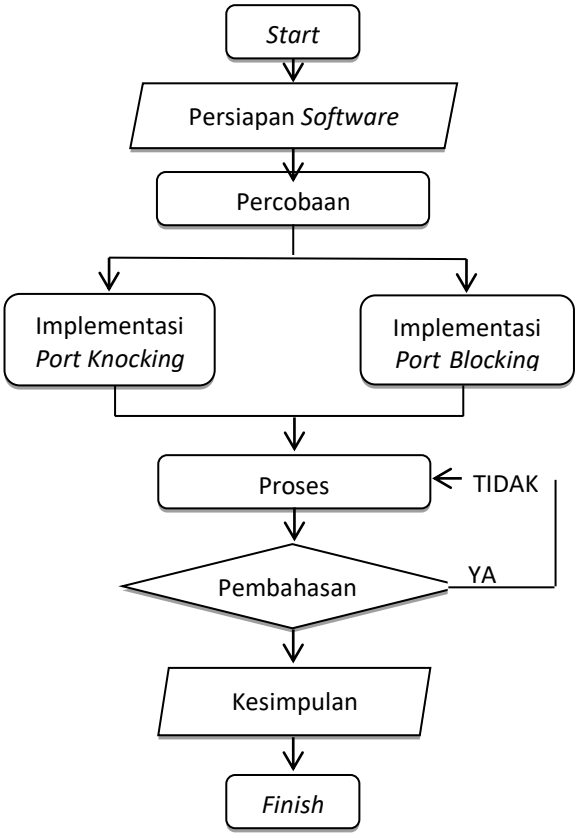
Strategi pengelolaan akses pengguna atau komputer dalam jaringan dapat melibatkan penggunaan port blocking. Port blocking memungkinkan pengendalian hak akses terhadap berbagai port di dalam Local Area Network (LAN). Secara khusus, konfigurasi port dapat berbeda dari metode standar keamanan port atau keamanan port statis. Selain itu, pendekatan keamanan port seperti pembelajaran dinamis dan keamanan port lengket juga dapat diimplementasikan. Hal ini memiliki manfaat penting dalam mencegah akses yang tidak diinginkan dari satu pihak ke pihak lain, sehingga dapat mengurangi risiko pencurian data baik oleh pihak yang tidak dikenal maupun oleh pihak yang dikenal [8].

Dalam penelitian ini dibutuhkan juga software yaitu, *Graphical Network Simulator* 3 (GNS3) adalah sebuah alat simulasi yang mampu mengemulasikan jaringan yang rumit. GNS3 memungkinkan pengguna untuk menciptakan simulasi dari desain jaringan sebelum menerapkannya dalam situasi nyata di lapangan, tanpa memerlukan perangkat jaringan fisik seperti router dan switch [9].

MikroTik RouterOS adalah sistem operasi router serbaguna yang dapat digunakan pada komputer standar, tidak terbatas pada perangkat keras khusus seperti sistem operasi router lainnya. Sistem ini menyajikan berbagai fitur, termasuk Firewall dan NAT, fungsi routing, dukungan Hotspot, Point-to-Point Tunneling Protocol (PPTP), server DNS dan DHCP, manajemen bandwidth, konfigurasi keamanan, serta berbagai fitur lainnya. Dikenal karena kemudahan konfigurasinya dan harganya yang terjangkau, MikroTik RouterOS pada dasarnya berperan dalam mendistribusikan koneksi internet ke beberapa komputer pengguna [10].

2. METODE PENELITIAN

Pada penelitian ini dilakukan simulasi keamanan jaringan mengenai port knocking dan port blocking sebagai cara untuk meningkatkan keamanan jaringan dari peyusup (*attacker*) yang mencoba melakukan pembobolan. Adapun langkah-langkah yang dilakukan yaitu :



Gambar 1 Diagram Alir Penelitian
[Sumber: Gambar Pribadi]

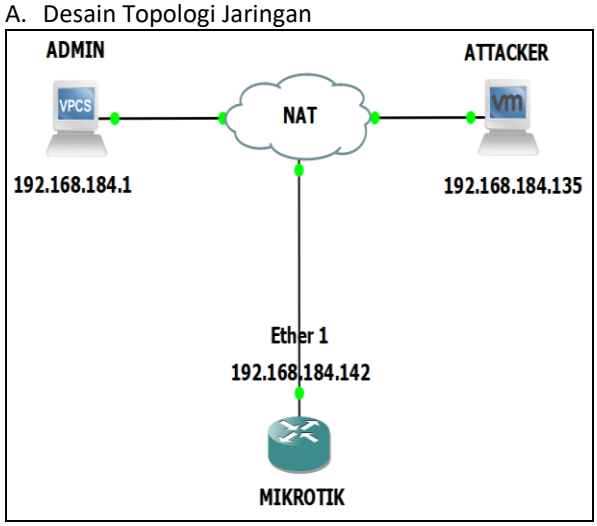
Gambar 2 di atas merupakan diagram alir penelitian. Yang pertama ialah memulai persiapan seperti menyiapkan software yang dibutuhkan yaitu GNS3, VMware Workstation Pro dan winbox64. Selanjutnya lakukan percobaan Implementasi port knocking dan port blocking, pada tahap ini dilakukan percobaan mulai dari membuat topologi jaringan kemudian lakukan setting pada mikrotik. Selanjutnya masuk ke proses pembahasan sehingga didapat lah data hasil pengujian dan dari data tersebut sehingga dapat disimpulkan.

3. HASIL DAN PEMBAHASAN

3.1 Hasil

Melalui analisis penelitian, tujuan utamanya adalah mencari solusi untuk memecahkan masalah dan mengembangkan desain rancangan keamanan jaringan. Eksperimen ini melibatkan tiga langkah: perancangan keamanan jaringan, konfigurasi MikroTik menggunakan metode port knocking dan port blocking, serta pelaksanaan pengujian awal dan pengujian akhir.

A. Desain Topologi Jaringan



Gambar 2 Topologi Jaringan
[Sumber: Gambar Pribadi]

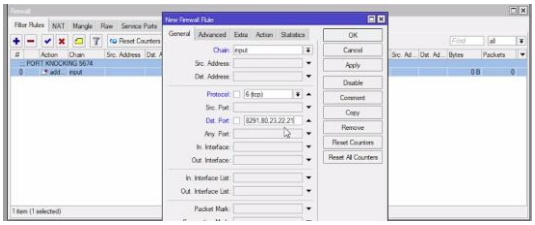
Topologi jaringan diatas terdiri dari empat perangkat yang terhubung yaitu, admin dengan alamat IP (192.168.184.1), Ether 1 dengan alamat IP (192.168.184.142), attacker dengan alamat IP (192.168.184.135) dan NAT.

Admin merupakan perangkat yang bertindak sebagai administrator atau pengelola jaringan. Ether 1 adalah perangkat jaringan yang berfungsi sebagai gateway atau router yang

menghubungkan jaringan lokal dengan jaringan luar, mungkin internet. Attacker adalah perangkat yang mungkin menjadi sumber masalah atau ancaman keamanan, seperti intrusi atau serangan terhadap jaringan. Sedangkan NAT (Network Address Translation), digunakan untuk mengizinkan komunikasi antara jaringan lokal yang berbeda yang menggunakan alamat IP yang tidak saling terhubung secara langsung.

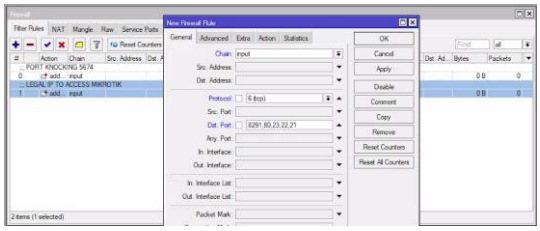
Dalam perancangan ini, penulis menciptakan dan menerapkan lapisan keamanan tambahan menggunakan metode port knocking dan port blocking. Sistem keamanan ini ditujukan untuk melindungi dari serangan eksploitasi dengan melakukan pemindaian port dan membatasi akses pengguna. Dengan cara ini, hanya pengguna yang telah melakukan proses open port knocking terlebih dahulu yang dapat mengakses secara penuh, memungkinkan pembukaan dan penutupan akses port.

B. Setting Mikrotik dengan Metode Port Knocking dan Port Blocking



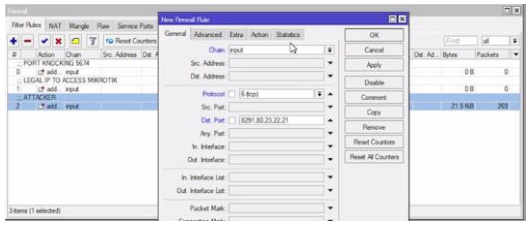
Gambar 3 Setting Firewall Port Knocking
[Sumber: Gambar Pribadi]

Konfigurasi port knocking melibatkan langkah-langkah berikut: buka menu IP, pilih Firewall, tambahkan aturan baru dengan mengklik tanda tambah (+). Pada bagian status umum, ubah Chain menjadi input. Selanjutnya, masukkan alamat IP pada Dst. Address, seperti 8291.80.23.22.21, pilih Protocol (tcp), dan akhiri dengan mengklik apply, ok.



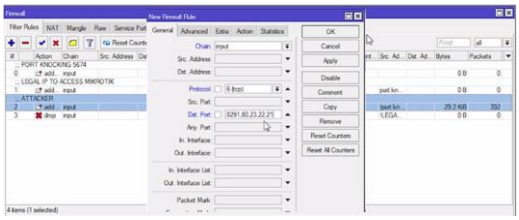
Gambar 4 Setting Firewall Port IP Legal
[Sumber: Gambar Pribadi]

Mengatur Firewall untuk Port IP Legal melibatkan langkah-langkah berikut: kembali ke menu Add(+) dan pada bagian status umum, ubah Chain menjadi input. Selanjutnya, masukkan alamat IP pada Dst. Address, seperti 8291.80.23.22.21, pilih Protocol (tcp), dan akhiri dengan mengklik apply, ok.



Gambar 5 Setting Firewall Port IP Attacker
[Sumber: Gambar Pribadi]

Mengatur konfigurasi port IP untuk para penyerang melibatkan langkah-langkah berikut: kembali ke menu Add(+) dan pada bagian status umum, ubah Chain menjadi input. Selanjutnya, masukkan alamat IP pada Dst. Address, seperti 8291.80.23.22.21, pilih Protocol (tcp), dan akhiri dengan mengklik apply, ok.

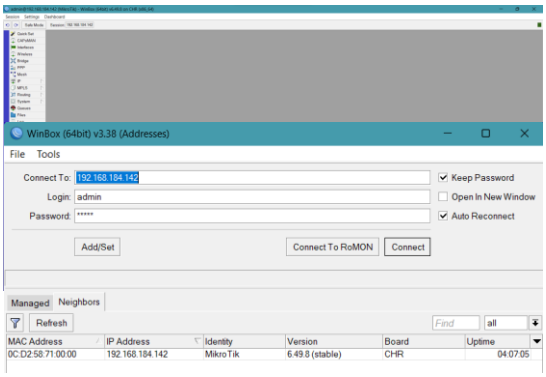


Gambar 6 Setting Firewall IP Drop
[Sumber: Gambar Pribadi]

Konfigurasi port IP untuk pengaturan drop melibatkan langkah-langkah berikut: kembali ke menu Add(+) dan pada bagian status umum, ubah Chain menjadi input. Selanjutnya, masukkan alamat IP pada Dst. Address, seperti 8291.80.23.22.21, pilih Protocol (tcp), dan akhiri dengan mengklik apply, ok.

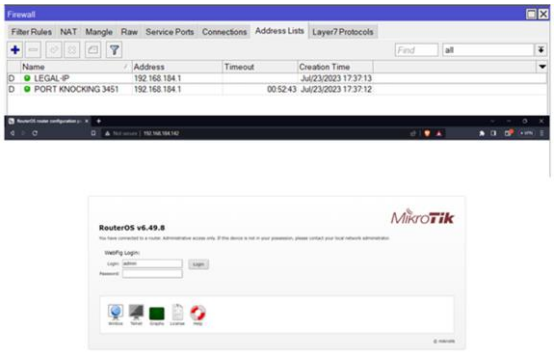
3.2 Pembahasan

Pengujian akhir menghasilkan penerapan desain keamanan jaringan baru, di mana keamanan tersebut ditingkatkan melalui penggunaan metode port knocking dan port blocking. Berikut adalah hasil dari pengujian akhir:



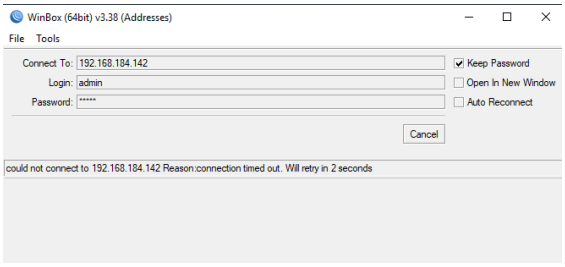
Gambar 7 Winbox Status Berhasil
[Sumber: Gambar Pribadi]

Pengujian secara remote pada router dilakukan melalui Winbox dengan menargetkan alamat IP 192.168.184.142 untuk terhubung ke router. Dalam Gambar 8, terlihat bahwa akses ke router berhasil terhubung karena telah melalui proses knocking port.



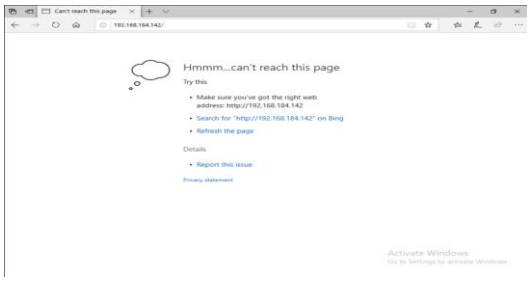
Gambar 8 Status Berhasil
[Sumber: Gambar Pribadi]

Pengujian dilakukan secara remote pada router melalui webfig dengan mengincar alamat IP target 192.168.184.142. Seperti terlihat pada gambar 9, muncul formulir login yang memungkinkan pengguna memasukkan baik username maupun password.



Gambar 9 Winbox Status Gagal
[Sumber: Gambar Pribadi]

Pengujian remote langsung pada router menggunakan Winbox menunjukkan adanya kesalahan atau ketidakmampuan untuk terhubung ke router. Gambar 10 mengindikasikan bahwa akses ke router ditolak karena belum melakukan proses knocking port.



Gambar 10 Status Gagal
[Sumber: Gambar Pribadi]

Remote router dilakukan secara langsung (tanpa proses knocking port) melalui webfig dengan menargetkan alamat IP 192.168.184.142 pada router. Gambar 11 menunjukkan bahwa formulir login yang seharusnya muncul untuk login dengan memasukkan username atau password tidak terlihat.

4. KESIMPULAN

Meningkatkan keamanan sistem jaringan dengan mengamankan port layanan yang terbuka melalui tindakan penguncian port, sehingga hanya pengguna yang sah yang dapat mengaksesnya. Teknik port knocking dan port blocking merupakan metode yang efektif untuk melindungi sistem jaringan dari akses ilegal.

Menggunakan teknik port knocking, akses ke port tertentu hanya diberikan kepada mereka yang tahu urutan koneksi yang benar. Ini berarti pengguna harus "mengetuk" atau mengirim permintaan koneksi ke port dalam urutan yang ditentukan sebelum akses ke port yang dituju diberikan.

Sementara itu, port blocking melibatkan menonaktifkan akses ke port tertentu melalui firewall atau perangkat jaringan, sehingga port tersebut tidak dapat digunakan oleh pihak eksternal. Dengan cara ini, risiko serangan pada port yang tidak digunakan dapat diminimalkan.

Kombinasi kedua teknik ini dapat digunakan untuk meningkatkan keamanan sistem jaringan Dengan mengurangi risiko

serangan dan akses ilegal ke layanan yang berjalan di dalamnya. Penting untuk merancang dan mengelola implementasi metode ini sesuai dengan kebutuhan khusus sistem jaringan Anda.

DAFTAR PUSTAKA

[1] R. O. Nitra and M. Ryansyah, "Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen," *J. Sist. dan Teknol. Inf.*, vol. 7, no. 1, p. 52, 2019, doi: 10.26418/justin.v7i1.29979.

[2] A. Amarudin, "Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking," *J. Teknoinfo*, vol. 12, no. 2, p. 72, 2018, doi: 10.33365/jti.v12i2.121.

[3] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 413, 2020, doi: 10.30865/mib.v4i2.2037.

[4] T. Brades and Irwansyah, "Pemanfataan Metode Port Knocking Dan Blocking," *Semin. Has. Penelit. Vokasi*, vol. 3, no. No.2, pp. 1–9, 2022.

[5] N. A. Santoso, K. B. Affandi, and R. D. Kurniawan, "Implementasi Keamanan Jaringan Menggunakan Port Knocking," *J. Janitra Inform. dan Sist. Inf.*, vol. 2, no. 2, pp. 90–95, 2022, doi: 10.25008/janitra.v2i2.156.

[6] I. Riadi, "Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik, Optimalisasi," *Jusi*, vol. 1, no. 1, pp. 71–80, 2011.

[7] R. Albar and R. O. Putra, "Sniffing Dan Implementasi Keamanan Jaringan Network Security Analysis Using the Method Sniffing and Implementation of Network Security on Microtik Router Os V6 . 48 . 3 Using Port Knocking Method," *J. Informatics Comput. Sci.*, vol. 8, no. 1, pp. 1–11, 2022.

[8] R. Ernawati, I. Ruslianto, and S. Bahri, "Implementasi Metode Port Knocking Pada Sistem Keamanan Server Ubuntu Virtual Berbasis Web Monitoring," *Coding J. Komput. dan Apl.*, vol. 10, no. 01, pp. 158–169, 2022, [Online]. Available: https://jurnal.untan.ac.id/index.php/jcskommipa/article/view/54226

[9] D. N. Aeni, A. F. Ikhsan, and H. Susilawati, "Jurnal FUSE – Teknik Elektro Analisis Trafik Jaringan Wifi dan Simulasi GNS3 Wifi Network Traffic Analysis and GNS3 Simulastion," vol. 1, no. 2, pp. 92–100, 2021.

[10] F. Ardianto, "Penggunaan mikrotik router sebagai jaringan server," *Pengguna. Router Mikrotik*, no. 1, pp. 26–31, 2020.