

JTKSI (Jurnal Teknologi Komputer dan Sistem Informasi)

JTKSI, Volume 7, Nomor 3, September 2024

E ISSN: 2620-3030; P ISSN: 2620-3022, pp.163-169

Accredited SINTA Nomor 72/E/KPT/2024

<https://jurnal.ftikomibn.ac.id/index.php/jtksi/index>

Received: 24 Juli 2024 Revised: 11 Agustus 2024; Accepted: 24 Agustus 2024

Implementasi Sistem *Port Knocking* Dalam Meningkatkan Keamanan Mikrotik Di PIT PT CDE COAL Bengkulu Utara

Suwandi Ramadhan¹, Dedy Abdullah², Yulia Darmi³, Khairullah⁴

^{1,2,3,4}Program Studi Teknik Informatika, Universitas Muhammadiyah Bengkulu

^{1,2,3,4}Kampus I, Jl. Bali, Kampung Bali, Teluk Segara, Kota Bengkulu, 38119

E-mail : suwandi.ramadhan00@gmail.com¹, dedy_Abdullah@umb.ac.id², yuliadarmi10juli@gmail.com³, khairullah@umb.ac.id⁴

Abstrak

Dalam era teknologi modern, perkembangan komputer dan jaringan telah menghadirkan berbagai tantangan baru, khususnya dalam hal keamanan. Internet of Things (IoT) dan teknologi jaringan generasi terbaru seperti 5G telah mengubah cara kita berinteraksi dengan perangkat dan jaringan, membawa risiko keamanan yang signifikan. Oleh karena itu, PT Cakrawala Dinamika Energi (PT CDE) menghadapi masalah serupa di lokasi penambangannya. Keamanan jaringan di area tersebut masih rentan terhadap serangan pihak tidak bertanggung jawab. Penelitian ini bertujuan untuk memperkuat keamanan jaringan di PT CDE dengan menggunakan sistem port knocking pada mikrotik. Metode port knocking menambah lapisan keamanan dengan hanya mengizinkan akses setelah serangkaian 'ketukan' pada port tertentu dilakukan secara benar. Implementasi dilakukan dengan menambahkan aturan-aturan firewall khusus pada mikrotik untuk mengatur login port dan address list. Keberhasilan sistem diuji melalui beberapa percobaan login, baik oleh admin yang sah maupun oleh penyusup yang tidak melakukan urutan port dengan benar. Hasil penelitian menunjukkan bahwa penerapan sistem port knocking berhasil meningkatkan keamanan mikrotik di PIT PT CDE. Semua percobaan login oleh penyusup, menggunakan berbagai IP perangkat yang berbeda, berhasil diblokir. Sebaliknya, login oleh admin yang sah berhasil dilakukan setelah mengikuti urutan port knock yang benar. Dengan hasil ini, diharapkan keamanan jaringan di area penambangan dapat lebih terjamin, sekaligus memberikan dasar bagi pengembangan lebih lanjut dalam manajemen keamanan jaringan.

Kata Kunci: Mikrotik, Port Knocking, Firewall, Keamanan

Abstract

In the modern technological era, the development of computers and networks has presented various new challenges, particularly in terms of security. The Internet of Things (IoT) and next-generation network technologies such as 5G have transformed the way we interact with devices and networks, bringing significant security risks. Therefore, PT Cakrawala Dinamika Energi (PT CDE) faces similar issues at its mining site. Network security in this area remains vulnerable to attacks by unauthorized parties. This research aims to enhance network security at PT CDE by using a port knocking system on MikroTik. The port knocking method adds a layer of security by only allowing access after a correct sequence of 'knocks' on specific ports has been performed. Implementation was carried out by adding special firewall rules on MikroTik to manage login ports and address lists. The system's success was tested through several login attempts by both authorized admins and intruders who did not follow the correct port sequence. The research results show that the implementation of the port knocking system successfully increased the security of MikroTik at the PT CDE mining site. All login attempts by intruders, using various different device IPs, were blocked. Conversely, authorized admin logins were successful after following the correct port knocking sequence. With these results, it is hoped that network security in the mining area can be further assured, providing a foundation for further development in network security management.

Keywords : Mikrotik, Port Knocking, Firewall, Security

I. PENDAHULUAN

Perkembangan teknologi komputer telah mengalami transformasi yang signifikan seiring berjalannya waktu. Awalnya, komputer hadir sebagai

alat pengolahan data yang terpusat dan bersifat monolitik. Namun, sejak ditemukannya mikroprosesor pada tahun 1970-an, komputasi menjadi lebih terjangkau dan dapat diakses oleh masyarakat umum.

Sejalan dengan itu, perkembangan jaringan komputer mengemuka sebagai langkah lanjutan, mengubah lanskap teknologi dengan memungkinkan komunikasi dan pertukaran informasi antar komputer. Awalnya dikenal sebagai ARPANET pada tahun 1969. Jaringan komputer terus berkembang menjadi internet yang luas dan kompleks yang kita kenal saat ini. Kini, dengan munculnya Internet of Things (IoT) dan teknologi jaringan generasi berikutnya seperti 5G, komputer tidak hanya berfungsi sebagai alat pengolahan data lokal tetapi juga sebagai entitas yang terhubung secara global, menciptakan era baru dalam interkoneksi dan aksesibilitas informasi.

Keamanan sistem jaringan dipengaruhi oleh perkembangan ini. Oleh karena itu, pengguna yang terhubung ke jaringan internet harus berhati-hati terhadap peretasan atau penyusupan yang disebabkan oleh pihak yang tidak bertanggung jawab. Sudah ada banyak contoh kasus situs-situs maupun sistem sistem yang diretas oleh pihak-pihak tidak bertanggung jawab ini seperti situs KPAI pada tahun 2019 (Dhani Irawan, 2019). Malware, trojan, virus, dan pemindaian port adalah beberapa contoh resiko keamanan jaringan yang sering ditemukan. Menggunakan jaringan yang terbuka portnya ini mampu meningkatkan resiko keamanan baik itu keamanan jaringan dan keamanan komputer itu sendiri karena peretas bisa saja masuk ke komputer user melalui jaringan yang terbuka tersebut.

PT Cakrawala Dinamika Energi merupakan perusahaan yang bergerak di bidang pertambangan batubara penanaman modal asing (PMA) yang berlokasi di Kabupaten Bengkulu Utara, Provinsi Bengkulu, Indonesia. PT CDE sudah bergerak di bidang pertambangan sejak tahun 2018 (IT Team CDE Group, 2022). Di PT CDE ini terdapat area penambangan batubara yang dinamakan PIT dimana setiap PIT terdapat "Pondok Checker" yang berfungsi untuk para checker lapangan mendata ritase setiap mobil OHT dan DT yang mengangkut baik itu Batubara (BB) ataupun Over Burden (OB). Di pondok checker menggunakan internet dengan jaringan satelit yang disalurkan ke mikrotik kemudian dilanjutkan ke access point dan laptop-laptop checker dan device user di area "pondok checker".

Permasalahan yang ada di PIT PT CDE Coal ini yaitu masih kurangnya keamanan jaringan yang ada untuk mikrotik yang mengatur bandwidth yang dikhawatirkan adanya peretasan dari pihak yang tidak bertanggung jawab baik itu untuk mengubah konfigurasi jaringan maupun mengambil data-data penting yang ada di laptop-laptop user di area PIT PT CDE Coal ini.

II. LANDASAN TEORI

A. Implementasi

Implementasi merujuk pada tahap eksekusi atau penerapan suatu rencana, program, atau sistem ke dalam konteks praktis atau operasional. Dalam konteks umum, implementasi dapat dikatakan sebagai serangkaian langkah-langkah untuk mengubah konsep atau desain menjadi kenyataan yang dapat digunakan. Ini mencakup konfigurasi perangkat, pelaksanaan kebijakan, atau penerapan solusi teknologi dalam lingkungan nyata.

Secara etimologis pengertian implementasi menurut Kamus Webster berasal dari Bahasa Inggris yaitu *to implement*. Dalam kamus tersebut, *to implement* (mengimplementasikan) berarti *to provide the means for carrying out* (menyediakan dampak/akibat terhadap sesuatu). Sementara itu dalam Kamus Besar Bahasa Indonesia, *implementasi* adalah pelaksanaan atau penerapan. Pengertian lain dari implementasi yaitu penyediaan sarana untuk melakukan sesuatu yang menimbulkan dampak atau akibat terhadap suatu hal. Pengertian dari implementasi juga bisa berbeda tergantung dari disiplin ilmunya. (Siti Nur Aeni, 2022)

B. Sistem

Sistem dalam konteks yang luas merujuk pada kumpulan elemen atau komponen yang saling terhubung dan berintegrasi untuk mencapai suatu tujuan atau fungsi tertentu. Sistem dapat terdiri dari unsur-unsur fisik atau abstrak seperti perangkat keras, perangkat lunak, proses, manusia atau informasi. Pentingnya sistem terletak pada integritasnya yang harmonis dimana setiap bagian memiliki peran dan kontribusi masing-masing dalam menjacapi kinerja keseluruhan. Sistem dapat ditemukan di berbagai bidang seperti teknologi informasi, lingkungan, bisnis.

Sistem juga dapat disimpulkan sebagai gabungan dari elemen, komponen atau variable yang saling berhubungan satu dengan yang lainnya untuk mencapai suatu tujuan tertentu (Maydianto & Muhammad Rasid Ridho, 2021).

C. Port Knocking

Port Knocking merupakan sebuah metode untuk membangun komunikasi dari mana saja dengan perangkat komputer yang tidak membuka *port* komunikasi apapun secara bebas (Windu Farhan Fatoni et al., 2022). Dengan kata lain, perangkat komputer tidak memiliki *port* komunikasi yang terbuka bebas untuk diakses tetapi perangkat *router* masih tetap dapat diakses tetapi dengan menggunakan pola ketukan yang sudah dikonfigurasi dan hanya orang yang ditentukan saja yang mengetahui pola ketukan port tersebut.

Sebelum *port* dapat diakses *user* harus mengirimkan serangkaian permintaan koneksi ke sejumlah *port* tertentu dengan urutan yang benar. Port knocking dapat meningkatkan keamanan karena mengurangi jejak serangan potensial karena port yang terbuka tidak terlihat secara langsung melalui pemindaian port biasa. Metode ini memberikan lapisan keamanan tambahan dengan mengharuskan *user* untuk "mengetuk" atau memicu pola tertentu sebelum mendapatkan akses ke layanan yang diinginkan.

D. Mikrotik RouterBoard

Mikrotik *RouterBoard* adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router network handal yang mencakup berbagai fitur yang dibuat untuk IP *Network* dan jaringan *wireless* digunakan oleh ISP, *provider*, *hotspot*, dan warnet. Mikrotik di desain untuk mudah digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga ke skala yang *kompleks*. Fungsi lainnya yaitu digunakan untuk mengontrol akses jaringan internet setiap

pengguna dengan menggunakan *bandwidth* manajemen (Martselane Adias Sabara & Ari Prayoga, 2020).

III. METODE PENELITIAN

Perancangan Program

Penelitian ini akan dilakukan dari bulan Maret-April 2024 di PIT PT Cakrawala Dinamika Energi yang berada di Desa Air Sebayur, Kecamatan Pinang Raya, Kabupaten Bengkulu Utara, Provinsi Bengkulu. Alat dan Bahan

Bahan yang digunakan dalam penelitian ini adalah konfigurasi *rules firewall port knocking* yang digunakan untuk pengimplementasian sistem ke dalam mikrotik.

Alat yang digunakan dalam penelitian dikelompokkan menjadi 2 macam yaitu alat yang sudah ada di PIT dan alat tambahan yang digunakan untuk pengimplementasian konfigurasi antara lain :

Alat yang Sudah Ada :

- a. Antena Ubiquiti



Gambar 1 Antena Ubiquiti

- b. Modem Ubiquiti



Gambar 2 Modem Ubiquiti

- c. Mikrotik RB 450 GX4



Gambar 3 Mikrotik RB 450 GX4

- d. Access Point Asus



Gambar 4 Access Point Asus

- 1. Alat Tambahan

- a. Laptop



Gambar 5 Laptop

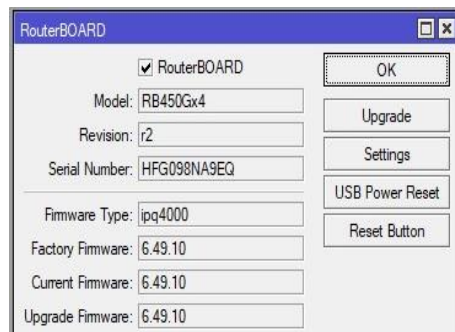
Perancangan

Pada tahap perancangan ini peneliti merancang konfigurasi mikrotik dengan mengatur *rules-rules firewall* yang akan diimplementasikan yaitu mengatur login *port* dan *address list* yang nantinya akan menjadi tempat penampungan IP yang login dan IP perangkat yang ada di mikrotik

IV. HASIL DAN PEMBAHASAN

Implementasi

Implementasi dari sistem *port knocking* ini diterapkan pada mikrotik di PIT PT Cakrawala Dinamika Energi dengan mengatur *rules firewall* pada mikrotik dengan seri mikrotik RB 450 GX4 yang merupakan mikrotik yang digunakan di PIT PT CDE untuk mengatur lalu lintas jaringan di PIT.



Gambar 6 RouterBOARD

- 1. Mengatur *port*

Di tahap pertama peneliti mengatur *port* yang akan dibuka untuk login ke dalam mikrotik sehingga *port* yang aktif hanya *port* yang di *enable* saja untuk memperkecil celah keamanan yang ada di mikrotik.

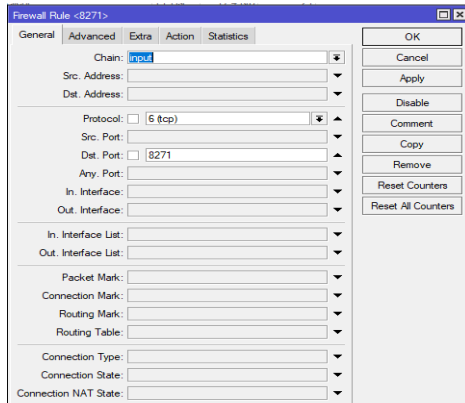
Name	Port	Available From	Certificate
X api	8728		
X api-ssl	8729		none
X ftp	21		
X ssh	22		
X telnet	23		
winbox	8291		
www	80		
X www-ssl	443		none

Gambar 7 IP Service List

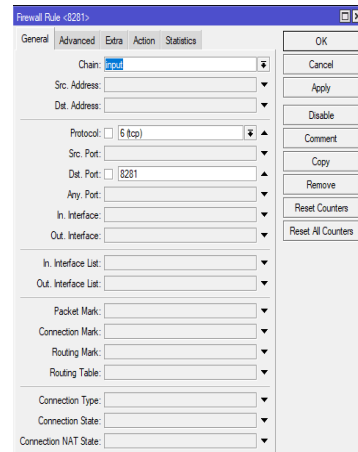
Port yang kita buka di sini yaitu *port winbox* dengan nomor 8291 dan *port www* dengan nomor 80.

2. Mengatur rules firewall

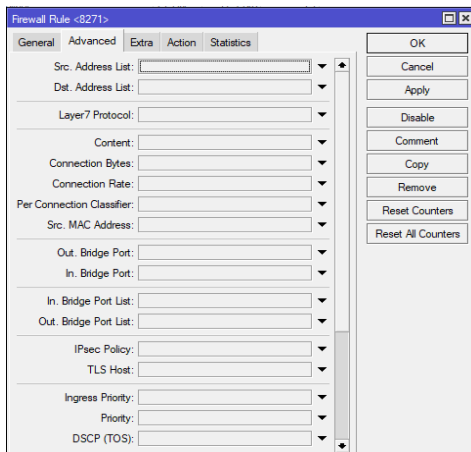
a. Knock-8271



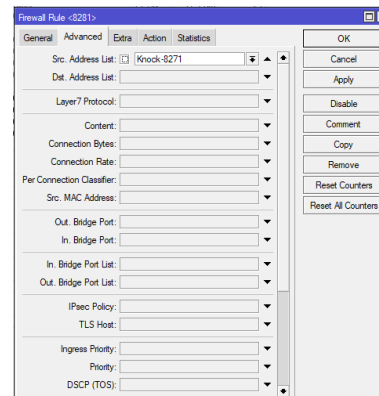
Gambar 8 Knock-8271 – General



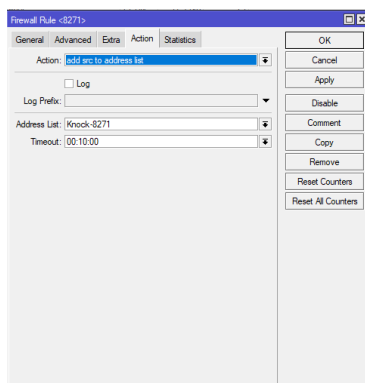
Gambar 11 Safe-IP – General



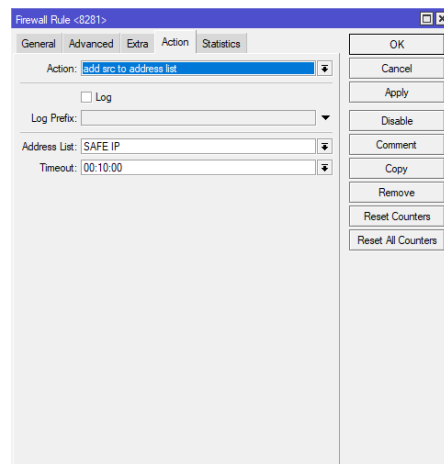
Gambar 9 Knock-8271 – Advanced



Gambar 12 Safe IP – Advanced



Gambar 10 Knock-8271 – Action



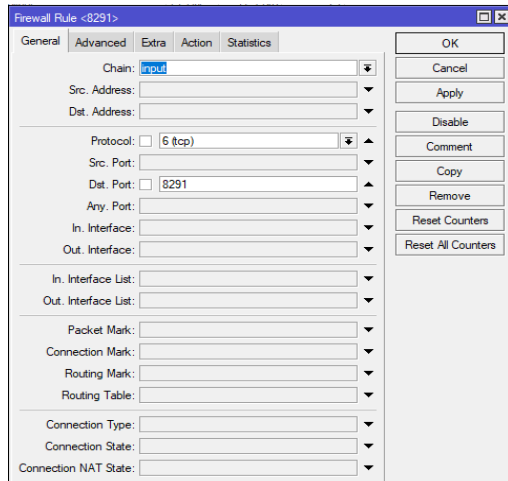
Gambar 13 Safe IP – Action

Di sini peneliti menambahkan *Firewall* untuk apabila user login ke mikrotik menggunakan *port* 8271 maka user tersebut akan IP *user* tersebut akan ditambahkan ke dalam *address list* “knock-8271” dengan rentan waktu login 00:10:00 (10 menit).

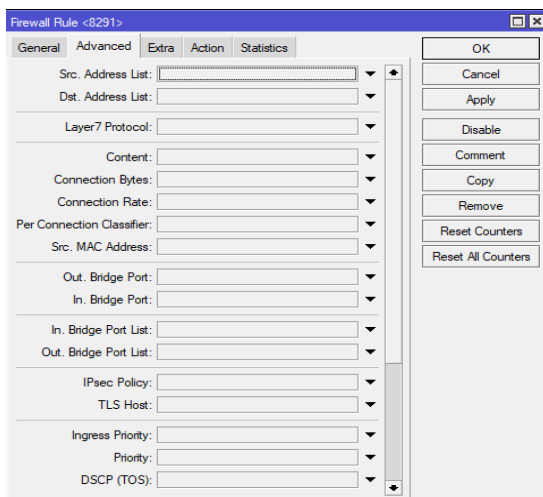
b. Safe-IP

Peneliti mengatur apabila ada *user* yang login ke mikrotik ke *port* 8281 dan berasal dari Knock-8271 maka IP *user* akan ditambahkan ke *address list* “Safe-IP” dengan interval login 00:10:00 (10 menit).

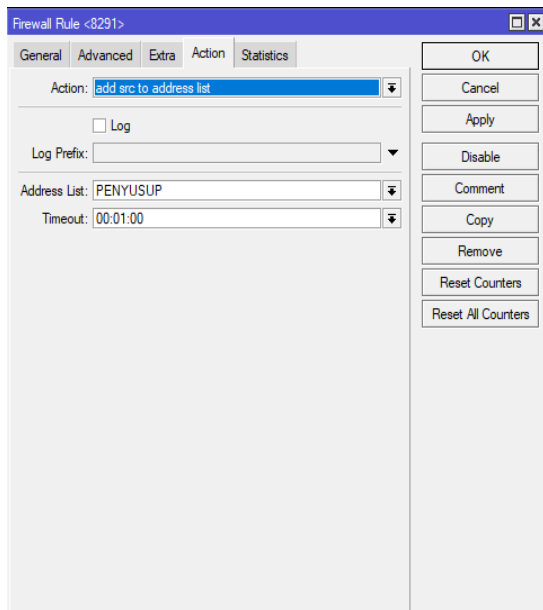
c. Penyusup



Gambar 14 Penyusup – General



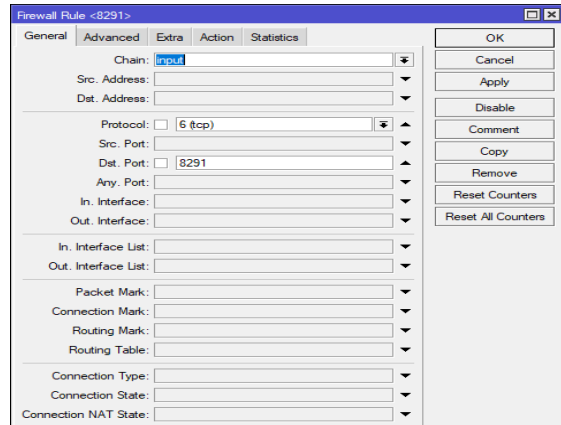
Gambar 15 Penyusup – Advanced



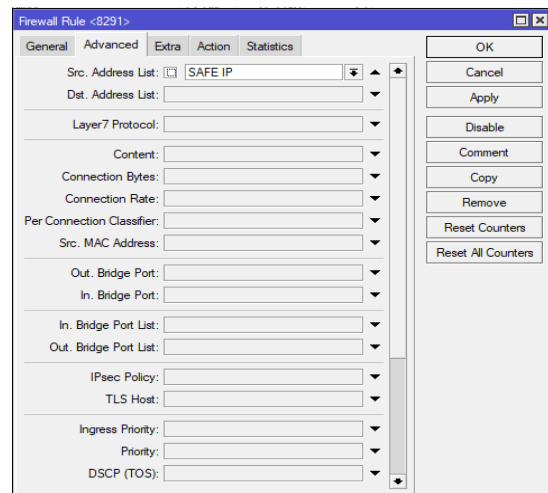
Gambar 16 Penyusup – Action

Konfigurasi ini jika *user* masuk ke dalam mikrotik langsung ke *port* 8291 tanpa masuk dulu ke *port* 8271 dan *port* 8281 maka IP *user* itu akan ditambahkan ke *address list* "Penyusup" dengan rentan waktu 00:10:00 (10 menit).

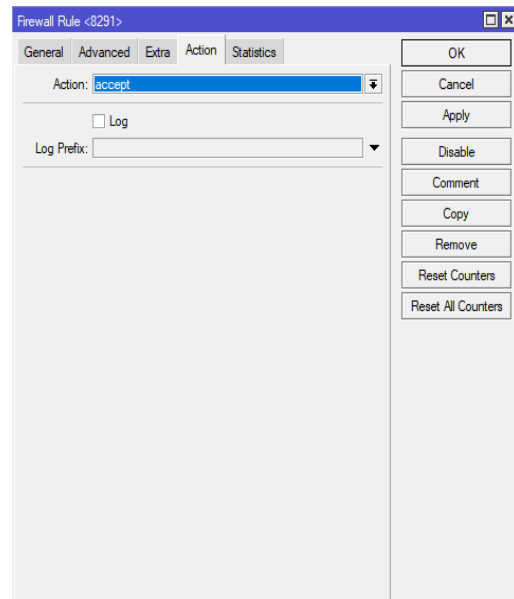
d. Acc Login



Gambar 17 Acc Login – General



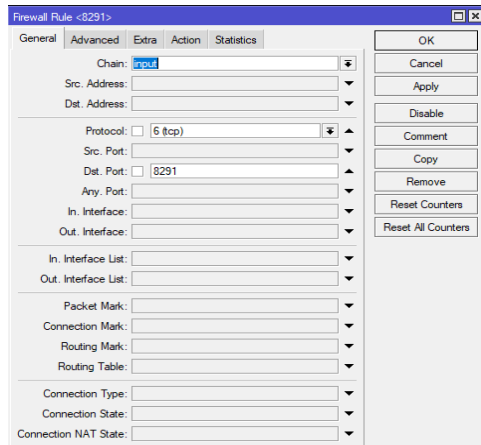
Gambar 18 Acc Login – Advanced



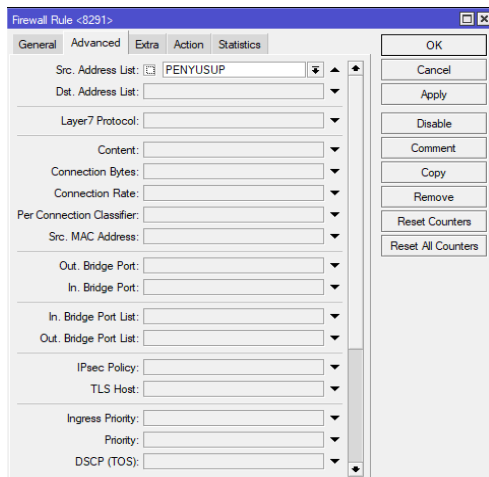
Gambar 19 Acc Login – Action

Di sini peneliti mengatur apabila ada *user* yang login ke mikrotik menuju *port* 8291 dan IP *user* tersebut berasal dari *address list* "Safe IP" maka *action* yang akan dilakukan adalah *accept* dan memperbolehkan *user* tersebut masuk ke dalam mikrotik dan mengkonfigurasi mikrotik.

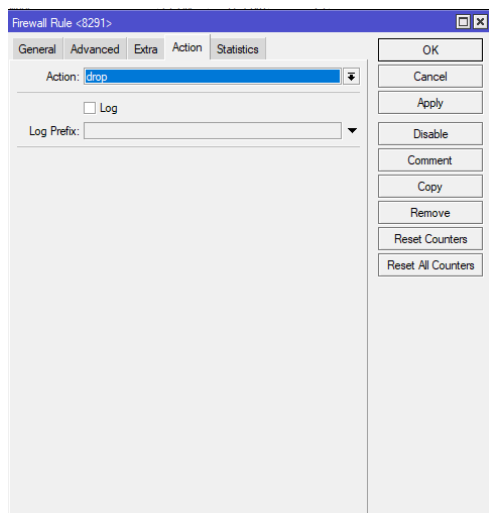
e. Drop Penyusup



Gambar 20 Drop Penyusup – General



Gambar 21 Drop Penyusup – Adcanned



Gambar 22 Drop Penyusup – Action

Konfigurasi ini mengatur apabila IP *user* masuk ke dalam *port* 8291 dan IP *user* tersebut sudah masuk ke dalam "Penyusup" maka *action* yang akan dilakukan yaitu *drop*.

V. KESIMPULAN

Setelah melihat hasil percobaan pada tabel uji coba di atas maka dapat disimpulkan bahwa implementasi sistem *port knocking* mampu meningkatkan keamanan

pada jaringan mikrotik terbukti dengan 10 kali percobaan login menggunakan IP perangkat yang berbeda dan dengan urutan *port knock* yang salah sehingga IP perangkat tersebut semuanya di *block* oleh mikrotik dan tidak diizinkan untuk login ke dalam mikrotik. Dari hasil penelitian ini juga peneliti berharap nantinya akan ada perbaikan-perbaikan baik dari sisi konfigurasi *firewall* yang lebih baik lagi dan lebih mudah dipahami nanti kedepannya.

DAFTAR PUSTAKA

- [1] Dhani Irawan. (2019, September). *Situs KPAI Diretas! Hacker Lempar Pesan soal KPK Dipadamkan*. Detik.Com.
- [2] Eksan Nuryakin Habillah, A. (2022). Terbit online pada laman web jurnal: <https://ejournalunsam.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,> 04(01), 1–7.
- [3] IT Team CDE Group. (2022). *PT Cakrawala Dinamika Energi*. Cde-Coal.Com.
- [4] Martselane Adias Sabara, & Ari Prayoga. (2020). Konfigurasi Manajemen Bandwidth Menggunakan Router Mikrotik RB2011UiAS-RM Untuk Mengontrol Penggunaan Internet Di Pt Rekan Usaha Mikro Anda Tegal. *Jurnal POLEKTRO*, 09(2), 1–4.
- [5] Maydianto, & Muhammad Rasid Ridho. (2021). Rancang Bangun Sistem Informasi Point Of Sale Dengan Framework Codeigniter Pada CV Powershop. *Jurnal Comasie*, 04(02), 2–10.
- [6] Mendrofa, Y., & Fauzi, R. (2023). Implementasi keamanan jaringan menggunakan port knocking. *Jurnal comasie*.
- [7] Oktaviansyah, P. D., Korespondensi, P., Paradika, :, & Oktaviansyah, D. (2022). <https://jurnal.netplg.com/jnca> Penerapan Sistem Pengamanan Port pada Mikrotik Menggunakan Metode Port Knocking Penerapan Sistem Pengamanan Port pada Mikrotik Menggunakan Metode Port Knocking. *NetPLG Journal of Network and Computer Applications*, 1(2).
- [8] 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>
- [9] 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>
- [10] Siti Nur Aeni. (2022, March 30). *Memahami pengertian implementasi, tujuan, faktor, dan contohnya*. Katadata.Co.Id.

- [11] Windu Farhan Fatoni, Arif Hidayat, & Mustika. (2022). Implementasi Sistem Keamanan Jaringan Komputer Dengan Metode Port Knocking Pada LKP Surya Komputer. *Jurnal Mahasiswa Ilmu Komputer (JMik)*, 03(01), 2–13