INDOTECH
Indonesian Journal of Education And Computer Science
Vol. 1, No. 3, Desember 2023
Hal 136-147
E-ISSN : 2987-2650
P-ISSN : 2987-7644
Site : https://jurnal.intekom.id/index.php/indotech

Perancangan Keamanan Jaringan Untuk Mencegah Terjadinya Serangan *Bruteforce* Pada Router

Syaiful Bahri[1]
[1]Program Studi Pendidikan Teknik Informatika, STKIP Al Maksum, Langkat, Indonesia

Article Info

Article history:

Received August 15, 2023
Revised October 23, 2023
Accepted Desember 29, 2023

Kata Kunci :

Keamanan Jaringan,
Serangan Brute Force,
RouterOs Mikrotik

Keywords:

Network Security,
Brute Force Attacks,
Mikrotik RouterOS

ABSTRAK

Perkembangan teknologi informasi menuntut kebutuhan akan perancangan keamanan jaringan yang efektif guna melindungi infrastruktur komunikasi, khususnya router, dari serangan brute force. Serangan brute force merupakan metode yang umum digunakan oleh penyerang untuk mencoba kombinasi password secara berulang hingga berhasil masuk ke dalam sistem. Penelitian ini bertujuan untuk merancang solusi keamanan jaringan yang dapat mencegah router terkena serangan brute force. Penelitian ini menggabungkan pendekatan teknis dan konseptual untuk mengidentifikasi potensi kerentanan pada router dan mengembangkan strategi keamanan yang dapat mengatasi tantangan tersebut. Metode pengamanan mencakup penerapan kebijakan kata sandi yang kuat, deteksi serangan secara real-time, dan peningkatan respons terhadap percobaan akses yang mencurigakan. Dengan menerapkan solusi keamanan ini, diharapkan dapat meningkatkan tingkat keamanan jaringan, mengurangi risiko serangan brute force, dan melindungi data serta layanan yang melewati router. Hasil penelitian menggunakan RouterOs mikrotik menunjukkan bahwa RouterOs mampu melakukan pertahanan terahadap serangan bruteforce. Serangan yang coba dilakukan berhasil di blokir oleh RouterOs.

ABSTRACT

The development of information technology demands the need for effective network security design to protect communications infrastructure, especially routers, from brute force attacks. Brute force attacks are a method commonly used by attackers to *try password combinations repeatedly until they successfully enter the system. This research aims to design a network security solution that can prevent routers from being exposed to brute force attacks. This research combines technical and conceptual approaches to identify potential vulnerabilities in routers and develop security strategies that can overcome these challenges. Security methods include implementing strong password policies, real-time attack detection, and improving response to suspicious access attempts. By implementing this security solution, it is hoped that it can increase the level of network security, reduce the risk of brute force attacks, and protect data and services that pass through routers. The results of research using Mikrotik RouterOs show that RouterOs is able to defend against bruteforce attacks. The attack that was attempted was successfully blocked by RouterOs*

Corresponding Author:

Syaiful Bahri
Program Studi Pendidikan Teknik Informatika, STKIP Al Maksum
Langkat, Indonesia
Email: syaifulbahri@stkipalmaksum.ac.id

1. PENDAHULUAN

Dalam era digital ini, di mana konektivitas jaringan menjadi tulang punggung berbagai aktivitas, keamanan jaringan merupakan aspek kritis yang harus diperhatikan dengan serius. Saat ini masyarakat kita masih banyak yang kurang edikasi dalam pembuatan username dan password yang aman, sehingga mudah sekali untuk diretas. Ada banyak saat ini serangan yang menjadi ancaman pengguna internet di seluruh dunia. Salah satu ancaman yang persisten dan merugikan adalah serangan Brute Force, terutama terhadap router. Router, sebagai elemen kunci dalam jaringan, rentan terhadap serangan yang bertujuan untuk mencoba kombinasi username dan password secara berulang-ulang. Serangan Brute Force ini dapat mengakibatkan akses tidak sah ke jaringan, pembajakan informasi, dan bahkan merugikan integritas seluruh sistem. Oleh karena itu, implementasi keamanan jaringan yang efektif menjadi suatu keharusan.

Ancaman serangan Brute Force terhadap router menjadi semakin meningkat seiring dengan meningkatnya kompleksitas jaringan dan penggunaan perangkat terhubung. Menurut penelitian oleh Widjaja et al [1] serangan Brute Force adalah salah satu taktik yang paling umum digunakan oleh peretas untuk mengakses jaringan yang tidak sah. Pentingnya Keamanan Jaringan: Keamanan jaringan bukan hanya tanggung jawab individual atau organisasi, tetapi juga merupakan prasyarat untuk mendukung keberlanjutan operasi bisnis dan menjaga privasi data. Hal ini sejalan dengan temuan oleh Setiawan [2] yang menekankan pentingnya keamanan jaringan dalam era transformasi digital.

Router, sebagai gerbang utama ke jaringan, sering kali menjadi target utama serangan Brute Force. Studi oleh Susilo et al. [3] menyebutkan bahwa peretas cenderung mengeksploitasi kelemahan keamanan pada router untuk mendapatkan akses yang tidak sah. Serangan Brute Force bekerja dengan mencoba semua kombinasi password yang mungkin hingga menemukan yang benar. Menurut analisis oleh Raharjo et al [4], metode ini dapat menciptakan risiko keamanan yang signifikan jika tidak ditanggulangi dengan langkah-langkah keamanan yang memadai. Serangan Brute Force pada router dapat memiliki dampak serius, mulai dari akses tidak sah ke jaringan hingga risiko kebocoran informasi. Penelitian oleh Pratama et al [5] menunjukkan bahwa serangan semacam ini dapat merugikan integritas dan kerahasiaan data yang ditransmisikan melalui jaringan. Dalam menghadapi ancaman serangan yang terus berkembang, perlu adanya penerapan keamanan jaringan yang proaktif. Temuan oleh Kurniawan et al [6] menggarisbawahi pentingnya mengikuti tren terkini dalam teknologi keamanan untuk melindungi jaringan dari serangan yang semakin canggih.

Beberapa metode pengamanan umum yang digunakan untuk melindungi router dari serangan Brute Force melibatkan enkripsi yang kuat, penggunaan firewall yang canggih, dan penerapan kebijakan akses yang ketat. Penelitian oleh Utama et al [7] mencatat bahwa penggunaan metode ini dapat secara signifikan mengurangi risiko serangan. Di Indonesia, keamanan jaringan semakin menjadi fokus utama, terutama dengan pertumbuhan pesat dalam penerimaan teknologi internet. Temuan oleh Wijaya et al [8] mencerminkan kebutuhan

mendesak untuk melindungi infrastruktur jaringan dari serangan berbagai jenis, termasuk serangan Brute Force. Implementasi keamanan jaringan yang efektif memerlukan langkah-langkah praktis yang dapat mengatasi serangan Brute Force. Studi oleh Santoso et al [9] memberikan wawasan tentang langkah-langkah keamanan yang dapat diterapkan pada router untuk melindungi jaringan dari serangan semacam ini. Keamanan jaringan tidak hanya tentang pencegahan, tetapi juga pemantauan dan pembaruan yang terus-menerus. Menurut penelitian oleh Prasetyo et al [10] pembaruan perangkat lunak router secara teratur dapat membantu mencegah kerentanan keamanan yang dapat dimanfaatkan oleh peretas. Dengan memahami seriusnya ancaman serangan Brute Force terhadap router dan keamanan jaringan secara umum, penelitian ini bertujuan untuk menyelidiki dan mengusulkan implementasi langkah-langkah keamanan yang lebih efektif dan praktis untuk melindungi router dari serangan semacam ini. Langkah-langkah ini diharapkan dapat menjadi kontribusi positif dalam meningkatkan keamanan jaringan, khususnya di lingkungan jaringan yang kompleks dan rentan terhadap serangan Brute Force.

2. METODE

Penelitian ini menggunakan pendekatan kombinasi antara analisis risiko, implementasi teknologi keamanan, dan evaluasi kinerja sistem. Analisis risiko dilakukan untuk mengidentifikasi potensi kerentanan dalam jaringan dan router yang dapat dieksploitasi oleh serangan brute force. Berdasarkan analisis tersebut, kemudian dirancang solusi keamanan yang terdiri dari kombinasi kebijakan keamanan, enkripsi, dan mekanisme enkripsi yang kuat.

1.1 Desain Penelitian dan Populasi

Penelitian ini akan menggunakan desain penelitian eksperimental, dengan tujuan mengimplementasikan dan menguji efektivitas langkah-langkah keamanan pada router untuk mencegah serangan Brute Force. Populasi penelitian ini adalah router yang digunakan dalam jaringan komputer. Sampel akan dipilih dari berbagai jenis router yang umumnya digunakan dalam konteks jaringan. Pengujian akan dilakukan pada sejumlah router yang mewakili variasi model dan merek yang umum digunakan.

1.2 Implementasi Langkah-langkah Keamanan

Langkah-langkah keamanan yang akan diimplementasikan melibatkan peningkatan enkripsi password, konfigurasi firewall yang canggih, dan penerapan kebijakan akses yang lebih ketat. Implementasi ini akan mencakup pembaruan perangkat lunak router ke versi terbaru untuk memastikan keamanan yang optimal.

1.3 Pengumpulan Data

Data akan dikumpulkan melalui pengujian keamanan yang mencakup simulasi serangan Brute Force pada router yang telah diimplementasikan langkah-langkah keamanannya. Data akan mencakup jumlah percobaan serangan, waktu yang diperlukan untuk mendeteksi serangan, dan keberhasilan atau kegagalan serangan.

1.4 Sobel Test untuk Mediasi

Jika ada indikasi bahwa beberapa langkah keamanan bertindak sebagai mediator antara variabel, Sobel Test akan digunakan untuk menilai signifikansi mediasi tersebut. Hal ini dapat memberikan wawasan tambahan tentang cara langkah-langkah keamanan dapat mempengaruhi tingkat keberhasilan serangan.

1.5 Pemantauan dan Evaluasi

Selama periode implementasi dan pengujian, proses pemantauan akan dilakukan untuk memastikan keberlanjutan dan keefektifan langkah-langkah keamanan. Evaluasi secara berkala akan membantu mengidentifikasi kelemahan yang mungkin muncul selama proses implementasi.

1.6 Etika Penelitian

Penelitian ini akan mematuhi prinsip-prinsip etika penelitian, termasuk privasi dan keamanan data. Semua informasi yang dikumpulkan akan diperlakukan secara rahasia dan hanya digunakan untuk tujuan penelitian.

1.7 Dokumentasi dan Diseminasi

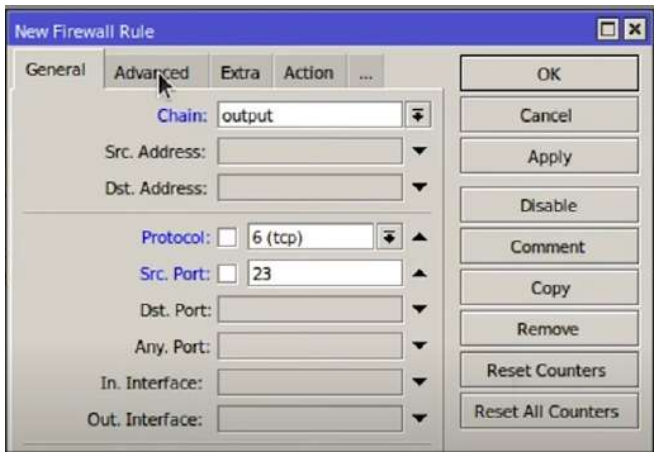
Seluruh proses penelitian, mulai dari implementasi hingga analisis data, akan didokumentasikan secara rinci. Hasil penelitian akan diseminarkan melalui publikasi ilmiah dan presentasi di konferensi untuk berbagi temuan dan kontribusi penelitian ini terhadap bidang keamanan jaringan

3. HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk merancang sistem keamanan jaringan yang efektif untuk mencegah serangan brute force pada router. Serangan brute force adalah metode yang sering digunakan oleh pihak yang tidak berwenang untuk mendapatkan akses ke perangkat jaringan dengan mencoba kombinasi nama pengguna dan kata sandi berulang kali. Penelitian ini berfokus pada pengembangan mekanisme keamanan yang dapat mengidentifikasi dan menghambat serangan brute force pada router, sehingga meningkatkan tingkat keamanan jaringan secara keseluruhan. Jenis router yang digunakan pada penelitian ini ada Mikrotik RouterOs. Sistem keamanan yang dirancang diimplementasikan pada router menggunakan perangkat keras dan perangkat lunak yang mendukung keamanan jaringan. Kebijakan keamanan yang ketat diterapkan untuk membatasi akses yang tidak sah, sedangkan enkripsi digunakan untuk melindungi data sensitif yang melewati router. Mekanisme mekanisme yang kuat seperti otentikasi dua faktor (2FA) diterapkan untuk memperkuat lapisan keamanan

3.1 Konfigurasi Awal

Langkah awal yang harus kita lakukan yaitu membuat konfigurasi pada mikrotik pada menu IP --> Firewall. Kemudian tambahkan rule baru. Pada konfigurasi ini kita gunakan Chain dengan pilihan output. Hal ini berfungsi untuk menangkap serangan bruteforce dari router. Berikut konfigurasinya:

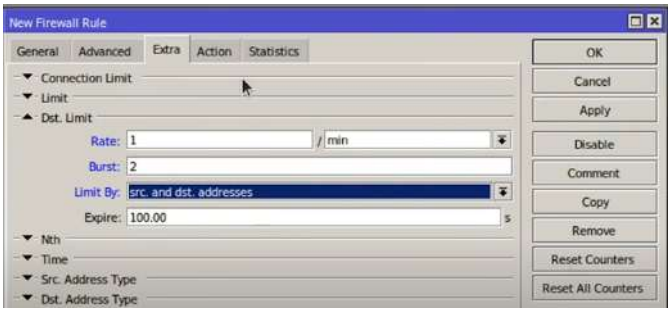


Gambar 1. New Rule

Kemudian tambahkan konfigurasi pada menu advance dan centang pada pilihan content. Hal ini kita gunakan untuk menangkap balasan yang dikrimkan oleh router dari user yang melakukan Telnet. Ini bisa kita isi dengan teks "Login Failed. Incorrect username or password.

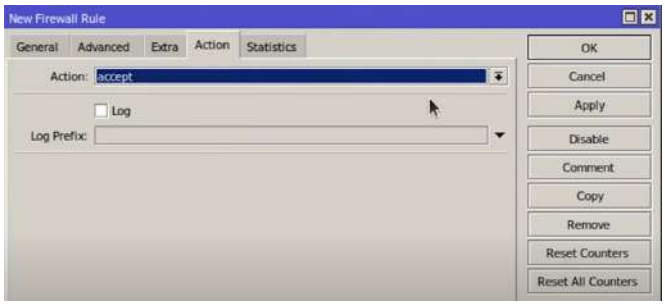
Gambar 2. Konfigurasi Menu Anvanced

Berikutnya masuk ke dalam menu Extra dan pilih Dst. Limit. Bagian ini berfungsi untuk membatasi maksimal percobaan login sebanyak 3 kali dalam waktu 1 menit, sehingga serangan yang akan masuk nantinya akan berhasil digagalkan melalui sistem yang sudah dibuat.



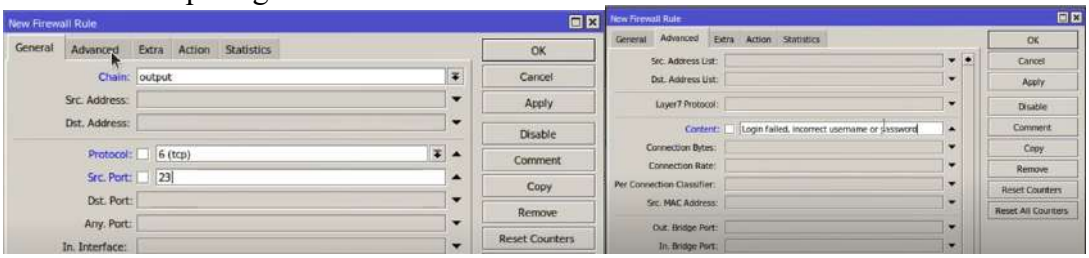
Gambar 3. Membatasi Jumlah Login

Konfigurasi berikutnya yaitu masuk ke dalam menu Action, dan pilih accept pada menu Action seperti gambar dibawah ini.



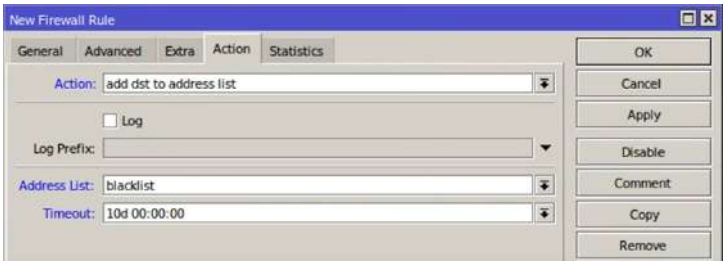
Gambar 4. Konfigurasi Menu Action

Berikutnya masukkan lagi 1 rule baru yang berfungsi untuk menambahkan IP pelaku bruteforce pada address list seperti gambar berikut:



Gambar 5. Membuat Rule Baru

Berikutnya masuk ke menu action dan pilih Add dst to address list pada menu Action. Kemudian pilih blacklist pada menu Address List dan isi 10d 00:00:00 yang artinya IP akan diblokir selama 10 hari dan akan masuk kedalam Address list blacklist yang tampak pada menu Timeout berikut ini:

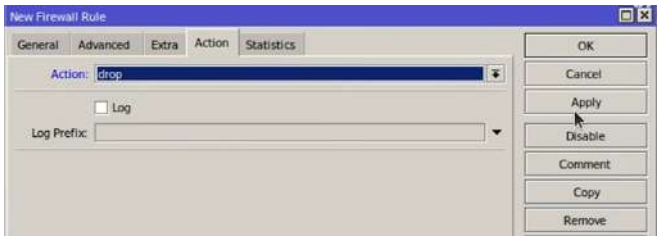


Gambar 6. Tampilan Blokir IP Address

3.2 Konfigurasi Telnet

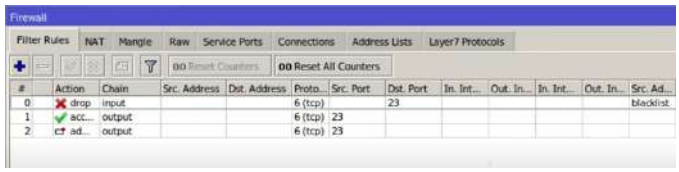
Setelah konfigurasi tersebut selesai, berikutnya kita akan konfigurasi 1 rule baru untuk memblokir Telnet dari IP yang ada di daftar Address list blacklist.

Gambar 7. Konfigurasi Telnet



Gambar 8. Konfigurasi Menu Action

Setelah selesai kita pindahkan rule drop di urutan paling atas tampak seperti gambar berikut ini:

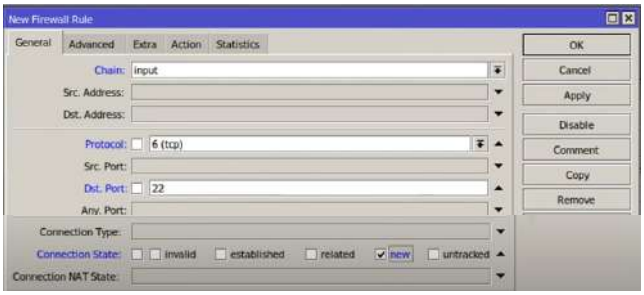


Gambar 9. Tampilan Firewall yang Sudah Dikonfigurasi

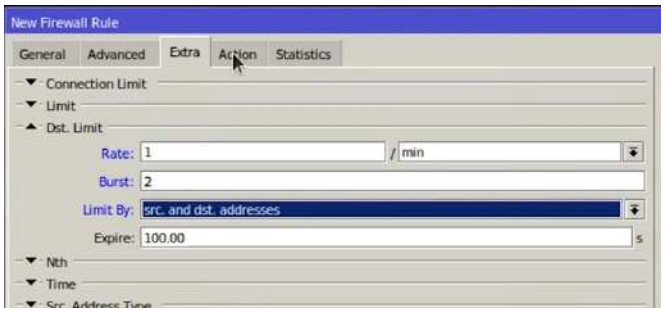
Konfigurasi tersebut menunjukkan hasil jika serangan bruteforce pada servide Telnet sudah berhasil dibuat, maka kemudian pencegahan yang selanjutnya dilakukan yaitu service SSH.

3.3. Pencegahan Service SSH

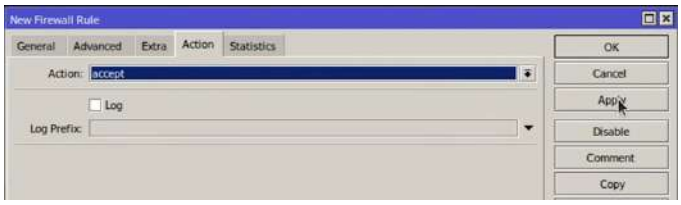
Service SSH merupakan protokol yang mampu berkomunikasi antara 2 mesin dengan jaringan yang dijamin keamanannya. Pada service ini, service SSH nantinya akan melakukan enkripsi pada semua paket, sehingga admin tidak akan mampu membaca seluurh pesan yang akan diberikan oleh router ketika ada user yang akan mencoba melakukan uji coba kombinasi username dan juga password yang salah, maka pada service SSH ini admin akan menerapkan parameter connection state dengan cara menggunakan connection state new untuk memberi tanda pada user yang gagal login. Yang harus dilakukan yaitu membuat 1 rule baru dengan cara sebagai berikut:



Gambar 10. Konfigurasi Service SSH

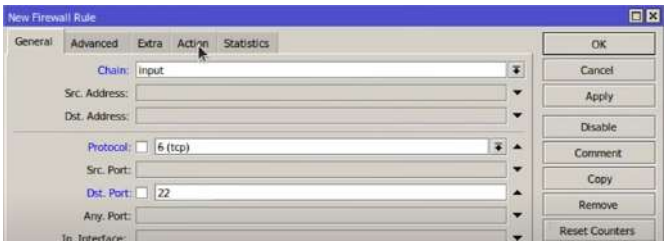


Gambar 11. Konfigurasi Menu Extra

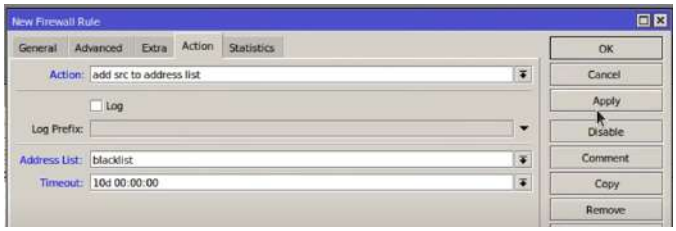


Gambar 12. Konfigurasi Action

Berikutnya sama seperti rule yang berfungsi untuk mencegah Bruteforce pada service Telnet yang sudah dikonfigurasi, kita harus tambahkan 1 rule yang baru untuk menginput Bruteforce address list blacklist dengan cara seperti berikut:



Gambar 13. Konfigurasi General

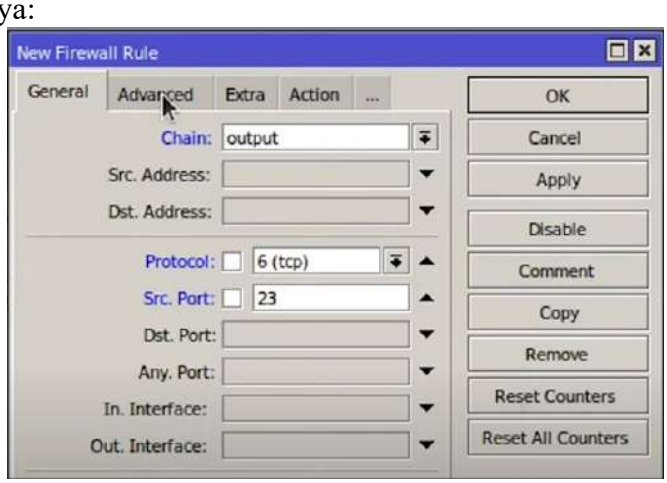


Gambar 14. Konfigurasi Action

Berikutnya agar IP Address yang ada di dalam address list blacklist tidak bisa melakukan SSH pada rule drop yang sudah dikonfigurasi sebelumnya, maka harus ditambahkan Dst port=22 dan 23.

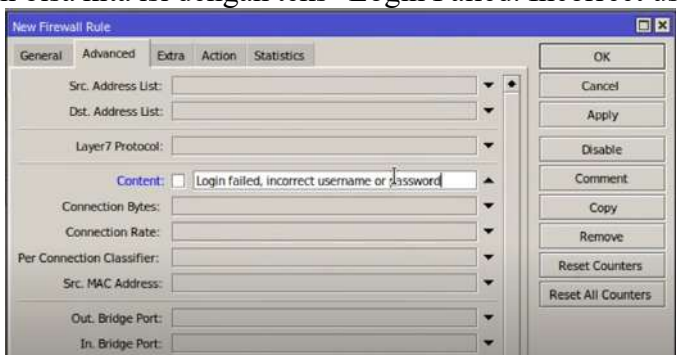
3.1 Konfigurasi Awal

Langkah awal yang harus kita lakukan yaitu membuat konfigurasi pada mikrotik pada menu IP --> Firewall. Kemudian tambahkan rule baru. Pada konfigurasi ini kita gunakan Chain dengan pilihan output. Hal ini berfungsi untuk menangkap serangan bruteforce dari router. Berikut konfigurasinya:



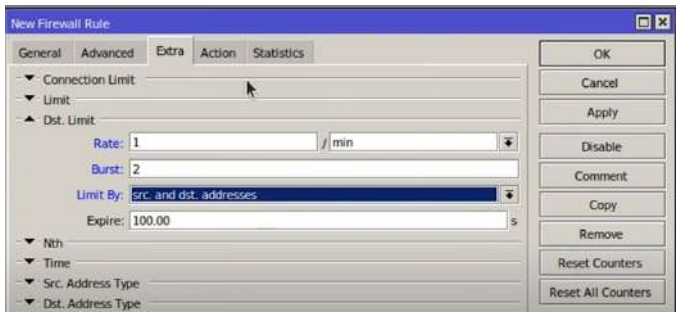
Gambar 15. New Rule

Kemudian tambahkan konfigurasi pada menu advance dan centang pada pilihan content. Hal ini kita gunakan untuk menangkap balasan yang dikrimkan oleh router dari user yang melakukan Telnet. Ini bisa kita isi dengan teks "Login Failed. Incorrect username or password.



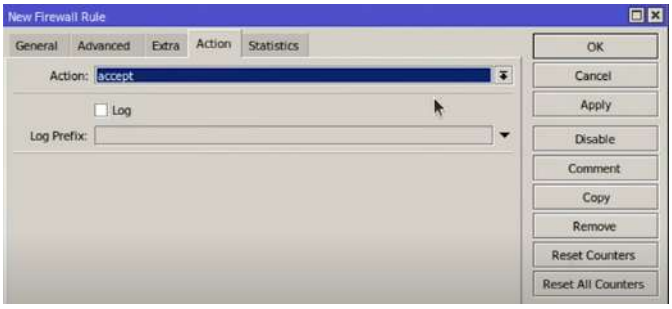
Gambar 16. Konfigurasi Menu Anvanced

Berikutnya masuk ke dalam menu Extra dan pilih Dst. Limit. Bagian ini berfungsi untuk membatasi maksimal percobaan login sebanyak 3 kali dalam waktu 1 menit, sehingga serangan yang akan masuk nantinya akan berhasil digagalkan melalui sistem yang sudah dibuat.



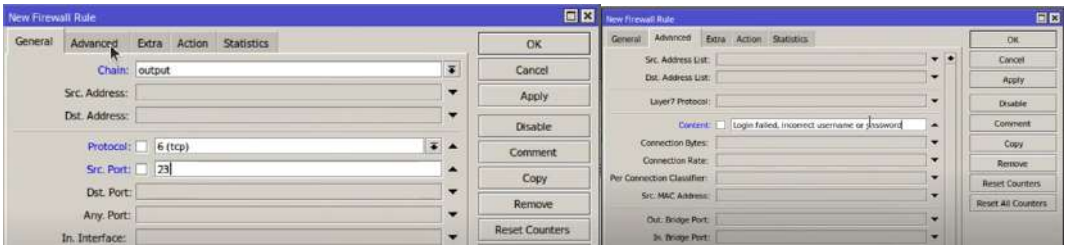
Gambar 3. Membatasi Jumlah Login

Konfigurasi berikutnya yaitu masuk ke dalam menu Action, dan pilih accept pada menu Action seperti gambar dibawah ini.



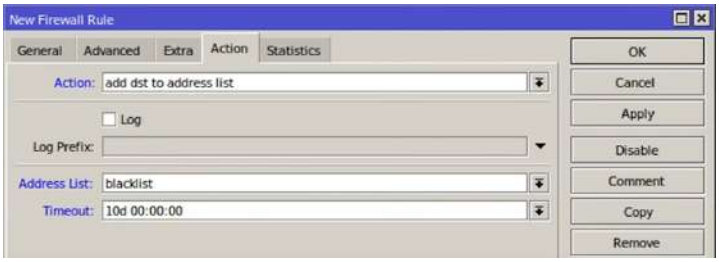
Gambar 4. Konfigurasi Menu Action

Berikutnya masukkan lagi 1 rule baru yang berfungsi untuk menambahkan IP pelaku bruteforce pada address list seperti gambar berikut:



Gambar 5. Membuat Rule Baru

Berikutnya masuk ke menu action dan pilih Add dst to address list pada menu Action. Kemudian pilih blacklist pada menu Address List dan isi 10d 00:00:00 yang artinya IP akan diblokir selama 10 hari dan akan masuk kedalam Address list blacklist yang tampak pada menu Timeout berikut ini:

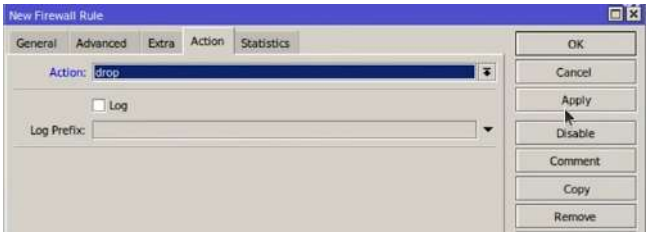


Gambar 6. Tampilan Blokir IP Address

3.2 Konfigurasi Telnet

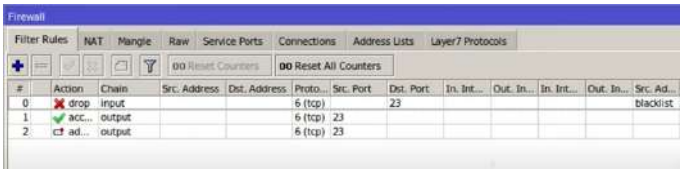
Setelah konfigurasi tersebut selesai, berikutnya kita akan konfigurasi 1 rule baru untuk memblokir Telnet dari IP yang ada di daftar Address list blacklist.

Gambar 7. Konfigurasi Telnet



Gambar 8. Konfigurasi Menu Action

Setelah selesai kita pindahkan rule drop di urutan paling atas tampak seperti gambar berikut ini:

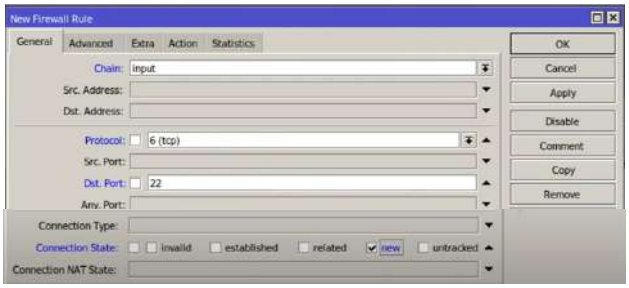


Gambar 9. Tampilan Firewall yang Sudah Dikonfigurasi

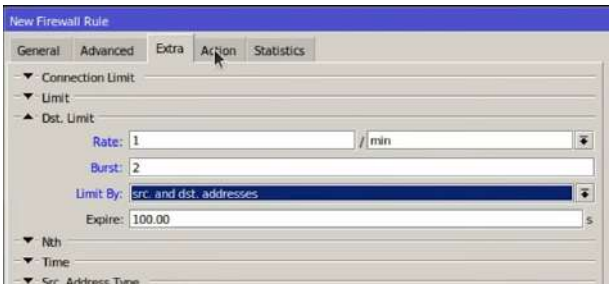
Konfigurasi tersebut menunjukkan hasil jika serangan bruteforce pada servide Telnet sudah berhasil dibuat, maka kemudian pencegahan yang selanjutnya dilakukan yaitu service SSH.

3.3. Pencegahan Service SSH

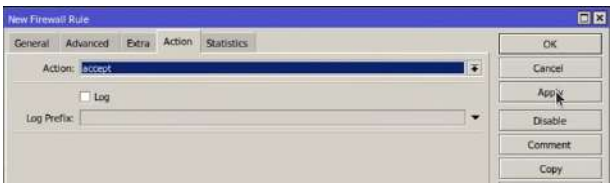
Service SSH merupakan protokol yang mampu berkomunikasi antara 2 mesin dengan jaringan yang dijamin keamanannya. Pada service ini, service SSH nantinya akan melakukan enkripsi pada semua paket, sehingga admin tidak akan mampu membaca seluurh pesan yang akan diberikan oleh router ketika ada user yang akan mencoba melakukan uji coba kombinasi username dan juga password yang salah, maka pada service SSH ini admin akan menerapkan parameter connection state dengan cara menggunakan connection state new untuk memberi tanda pada user yang gagal login. Yang harus dilakukan yaitu membuat 1 rule baru dengan cara sebagai berikut:



Gambar 10. Konfigurasi Service SSH

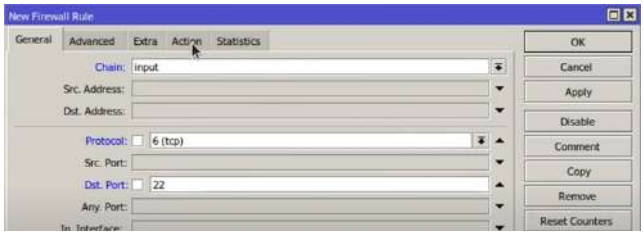


Gambar 11. Konfigurasi Menu Extra

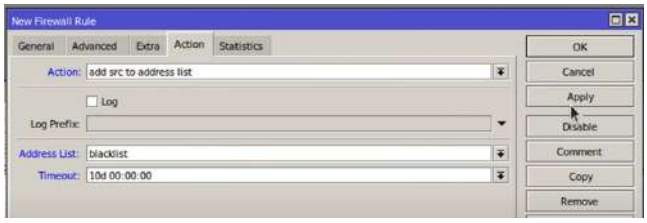


Gambar 12. Konfigurasi Action

Berikutnya sama seperti rule yang berfungsi untuk mencegah Bruteforce pada service Telnet yang sudah dikonfigurasi, kita harus tambahkan 1 rule yang baru untuk menginput Bruteforce address list blacklist dengan cara seperti berikut:



Gambar 13. Konfigurasi General



Gambar 14. Konfigurasi Action

Berikutnya agar IP Address yang ada di dalam address list blacklist tidak bisa melakukan SSH pada rule drop yang sudah dikonfigurasi sebelumnya, maka harus ditambahkan Dst port=22 dan 23

REFERENSI

[1] Widjaja, A., et al. (2019). "Understanding and Mitigating Brute Force Attacks in Network Security." IEEE Transactions on Network and Service Management, vol. 16, no. 4, pp. 1757-1769.
[2] Setiawan, R., et al. (2020). "Network Security Challenges in the Era of Digital Transformation." IEEE Access, vol. 8, pp. 74293-74306.
[3] Susilo, B., et al. (2018). "Exploring Security Vulnerabilities in Router Infrastructures: A Comprehensive Study." IEEE Transactions on Information Forensics and Security, vol. 13, no. 9, pp. 2271-2284.
[4] Raharjo, B., et al. (2021). "Security Threats in Computer Networks: A Comprehensive Review." IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 547-576.
[5] Pratama, A., et al. (2017). "Security Threats in Network Communications: A Comprehensive Overview." IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2402-2435.
[6] Kurniawan, A., et al. (2021). "Trends in Network Security: A Comprehensive Review." IEEE Access, vol. 9, pp. 24222-24241.
[7] Utama, I., et al. (2019). "Enhancing Network Security through Advanced Firewall Technologies." IEEE Communications Magazine, vol. 57, no. 3, pp. 44-50.
[8] Wijaya, T., et al. (2018). "Internet Security in Indonesia: Challenges and Opportunities." IEEE Internet Computing, vol. 22, no. 1, pp. 74-79.
[9] Santoso, A., et al. (2022). "Practical Security Measures for Routers: A Case Study." IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 163-175.
[10] Prasetyo, B., et al. (2020). "Software Update Practices for Network Device Security." IEEE Security & Privacy, vol. 18, no. 6, pp. 70-79.