Penerapan Firewall Untuk Keamanan Jaringan Pada SMKN 3 Kota Bengkulu

[1]Pangeran Al Amin, [2]Khairil, [3]Abdussalam Al Akbar

[1] Mahasiswa, Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu
Jalan Lintas Curup Muara Aman, RT.4/RW.1, Kelurahan Tes, Kecamatan Lebong Selatan
; e-mail: pangeran.alamin01@gmail.com
[2,] Dosen Tetap, Program Studi Sistem InformasiFakultas Ilmu Komputer, Universitas Dehasen Bengkulu
Jl. Meranti Raya No. 32 Kota Bengkulu 38228 Telp. (0736) 22027, 26957 Fax. (0736) 341139;
e-mail: , khairil@unived.ac.id)
[3] Dosen Tetap, Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu
Jl. Meranti Raya No. 32 Kota Bengkulu 38228 Telp. (0736) 22027, 26957 Fax. (0736) 341139;
e-mail: akbarabenk@unived.ac.id)

(Received: Nopember 2025, Revised: Februari 2026, Accepied: April 2026)

Abstract*-The use of computer networks at SMK Negeri 3 Kota Bengkulu increases the need for security against threats such as illegal access and DoS/DDoS attacks. This study implements a Mikrotik firewall using Filter Rules, Raw Rules, Mangle Rules, and DDoS limits using the Security Life Cycle (SLC) method.Test results show that Filter Rules are effective in blocking illegal access, Raw Rules are efficient in handling volumetric attacks because they work before connection tracking, and Mangle Rules are useful for traffic management. The application of DDoS limits has been proven to reduce the number of excessive connections so that the network remains stable.This study proves that the Mikrotik firewall can enhance school network security and can serve as a reference for implementing more comprehensive security policies.*
Keywords: Firewall, Mikrotik, Filter Rule, Raw Rule, Mangle Rule, DDoS

Intisari-*Pemanfaatan jaringan komputer di SMK Negeri 3 Kota Bengkulu meningkatkan kebutuhan akan keamanan dari ancaman seperti akses ilegal dan serangan DoS/DDoS. Penelitian ini menerapkan firewall Mikrotik menggunakan Filter Rule, Raw Rule, Mangle Rule, serta batas limit DDoS dengan metode Security Life Cycle (SLC). Hasil pengujian menunjukkan Filter Rule efektif memblokir akses ilegal, Raw Rule efisien menangani serangan volumetrik karena bekerja sebelum connection tracking, dan Mangle Rule bermanfaat untuk manajemen trafik. Penerapan limit DDoS terbukti mampu menekan jumlah koneksi berlebih sehingga jaringan tetap stabil. Penelitian ini membuktikan firewall Mikrotik dapat meningkatkan keamanan jaringan sekolah dan dapat dijadikan acuan penerapan kebijakan keamanan yang lebih komprehensif.*
Kata kunci: Firewall, Mikrotik, Filter Rule, Raw Rule, Mangle Rule, DDoS

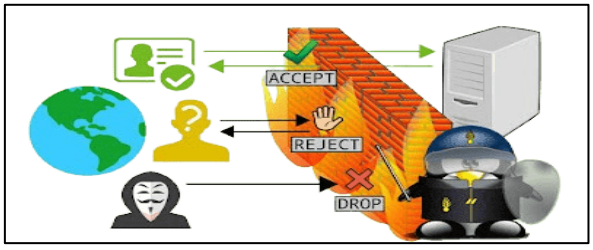
I . PENDAHULUAN

Masalah keamanan jaringan merupakan salah satu tantangan utama yang harus dihadapi oleh sekolah, terutama dalam hal melindungi data, mencegah akses yang tidak diizinkan, dan menjaga performa jaringan agar tetap optimal. Salah satu metode yang sering digunakan untuk melindungi jaringan dari ancaman eksternal maupun internal adalah dengan menerapkan sistem *firewall*. *Firewall* berfungsi sebagai penghalang atau penyaring antara jaringan internal sekolah dengan jaringan luar, serta dapat mengendalikan lalu lintas data berdasarkan kebijakan keamanan tertentu. Mikrotik adalah salah satu solusi *firewall* yang banyak digunakan, karena menawarkan fleksibilitas tinggi dengan harga yang relatif terjangkau. Mikrotik menyediakan fitur-fitur *firewall* yang dapat diatur sedemikian rupa untuk memenuhi kebutuhan keamanan spesifik, seperti pemblokiran akses dari IP tertentu, pembatasan akses situs tertentu, serta monitoring lalu lintas jaringan. Oleh karena itu, penerapan *firewall* berbasis Mikrotik di SMK Negeri 3 Kota Bengkulu diharapkan mampu memberikan solusi yang efektif dalam menjaga keamanan jaringan sekolah.

II. TINJAUAN PUSTAKA

Firewall

Menurut Mudzakkar (2023:3), *firewall* adalah teknik yang sangat berguna penting dalam mengamankan jaringan. *Firewall* merupakan model mekanisme sistem yang diterapkan pada perangkat keras, perangkat lunak, atau pada sistem itu sendiri dengan tujuan melindungi segmen pada jaringan pribadi dari jaringan luar yang tidak terpecaya. Tujuannya adalah untuk menyaring, membatasi, atau bahkan menolak semua koneksi dan aktivitas yang dilakukan pada segmen tersebut. Segmen pada jaringan pribadi dapat berupa *workstation, server, router,* atau jaringan LAN.
(Sumber: https://miqbal.staff.telkomuniversity.ac.id)



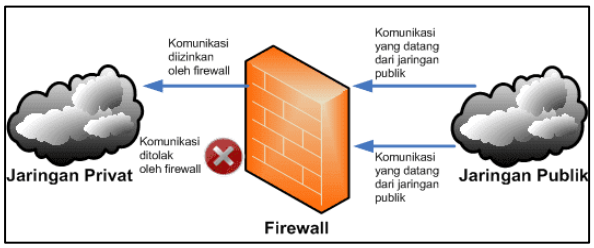
Gambar 1. *Firewall*

Cara Kerja *Firewall*

Menurut Shidqi Mardhatillah (2023:10), *firewall* mempunyai beberapa kebijakan untuk melindungi

P-ISSN 1858-2680
E-ISSN 2723-4673

data dari pihak asing, akan tetapi tidak semua dapat dilindungi baik data atau informasi data dari internal dari dalam jaringan. *Firewall* mendorong sistem keamanan jaringan supaya bisa memisahkan jaringan kita dari jaringan yang tidak kita kenal. Terdapat dua *firewall* untuk bisa menolak akses. (Sumber: https://aptika.kominfo.go.id)

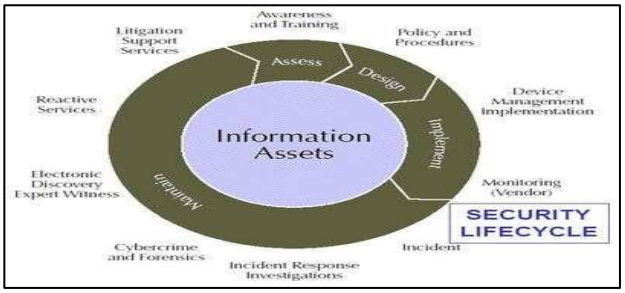


Gambar 2. Cara Kerja Firewall

III. METODOLOGI PENELITIAN

Metode Penelitian

Dengan metode yang digunakan oleh penulis adalah Metode SLC (Security Life Cycle), bisa dilihat pada gambar 5. di bawah ini :



Gambar 3. Security Life Cycle (SLC)

A. *Assess* (Penilaian)

1. Mengidentifikasi potensi ancaman keamanan jaringan, seperti port scanning, website terindikasi virus seperti *malware*, dan akses tidak sah.
2. Mengevaluasi kelemahan sistem jaringan yang ada, seperti kurangnya pemfilteran lalu lintas data.
3. Mengidentifikasi kebutuhan jaringan sekolah, seperti:

1) Pemblokiran akses ke situs yang tidak sesuai kebijakan sekolah.
2) Mengamankan aset-aset yang perlu diamankan seperti server database, server aplikasi, dan file server juga menjadi prioritas perlindungan untuk memastikan akses hanya diberikan kepada pihak yang berwenang.

IV. HASIL DAN PEMBAHASAN

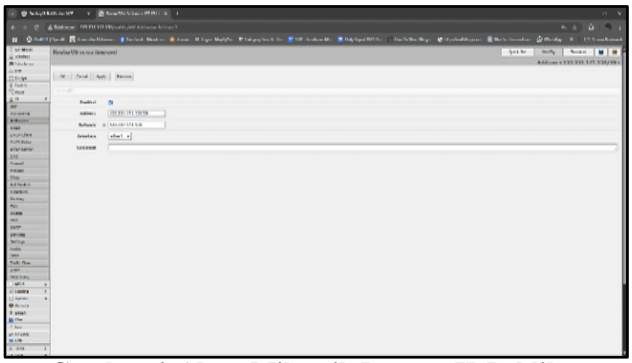
A.Hasil

Hasil implementasi menunjukkan bahwa firewall Mikrotik mampu menyaring lalu lintas jaringan sesuai dengan kebijakan keamanan yang telah ditetapkan. Melalui Filter Rules, sistem dapat memblokir akses ke situs-situs yang tidak sesuai dengan kebijakan sekolah, menutup port yang tidak digunakan, dan menghentikan koneksi mencurigakan secara otomatis. Sementara itu, Mangle digunakan untuk menandai (marking) lalu lintas data tertentu, yang kemudian dapat digunakan untuk keperluan pengelompokan, pembatasan bandwidth, atau pengaturan lanjutan lainnya. Fungsi Raw dimanfaatkan untuk menghentikan trafik yang terindikasi serangan bahkan sebelum mencapai proses koneksi (connection tracking), sehingga lebih efisien dalam menangani serangan seperti SYN Flooding. Selain itu, Address List digunakan sebagai daftar dinamis untuk menyimpan IP address dari sumber-sumber yang dicurigai melakukan serangan, seperti port scanning atau DoS attack, yang kemudian akan diblokir secara otomatis oleh rule selanjutnya.

Akses Mikrotik Dengan IP Publik

Adapun perintah konfigurasi IP publik sebagai berikut:

/ip address add address=123.231.171.130/29 interface=ether1 /ip route add gateway=123.231.171.129



Gambar 4. Akses Mikrotik Dengan IP Publik

Penjelasan:

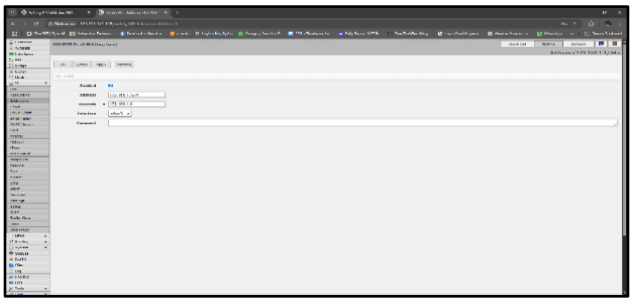
a) Perintah pertama menambahkan alamat IP publik ke interface ether1, yang berfungsi sebagai interface WAN.
b) Perintah kedua menambahkan default gateway yang mengarah ke IP gateway dari ISP, sehingga router dapat meneruskan paket ke internet.

Konfigurasi IP Lokal pada Interface LAN

Selanjutnya, konfigurasi dilakukan pada interface lokal (LAN) yaitu ether2, yang akan menghubungkan jaringan internal atau client ke router. IP lokal yang digunakan adalah 192.168.1.1/24.

Perintah konfigurasi sebagai berikut:

/ip address add address=192.168.1.1/24 interface=ether9



Gambar 7. Konfigurasi IP Lokal pada Interface LAN

P-ISSN 1858-2680
E-ISSN 2723-4673

Penjelasan:

a) Perintah tersebut menetapkan IP lokal 192.168.1.1 pada interface ether2.
b) Subnet /24 menunjukkan bahwa jaringan lokal memiliki rentang IP dari 192.168.1.1 hingga 192.168.1.254.

/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade

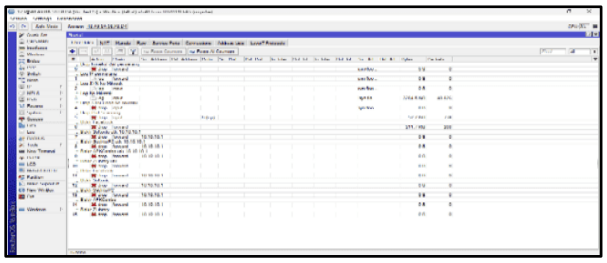
Gambar 8. Konfigurasi NAT (Network Address Translation) Masquerade

Penjelasan:

a) chain=srcnat menunjukkan bahwa rule ini berlaku untuk lalu lintas yang keluar (source NAT).
b) out-interface=ether1 berarti hanya koneksi yang keluar melalui interface WAN yang akan dikenai NAT.
c) action=masquerade adalah tindakan untuk menyamarkan IP lokal menjadi IP publik.

1) Daftar situs yang termasuk dalam blacklist kebijakan sekolah:

a.) https://www.softonic-id.com
b.) https://getintopc.com
c.) https://apkcombo.com
d.) https://www.zlibrary.to



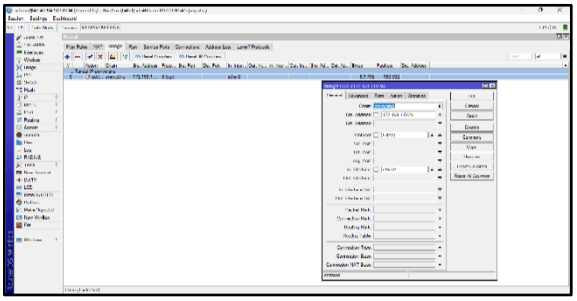
Gambar 9. Pemblokiran Akses Situs Tidak Diinginkan

Pencegahan Serangan DoS

1. Tandai IP Penyerang (Manggle Rule)

1) Tab General

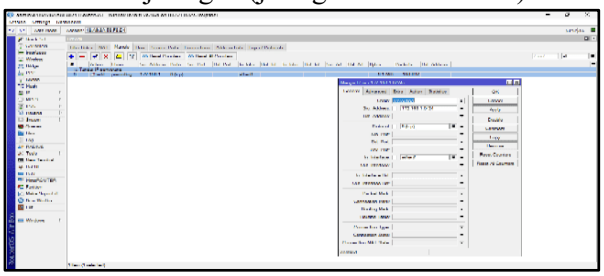
a.) Chain: prerouting



Gambar 10. Tandai IP Penyerang (Manggle Rule) Chain: Prerouting

b.) Src. Address: 172.168.1.0/24

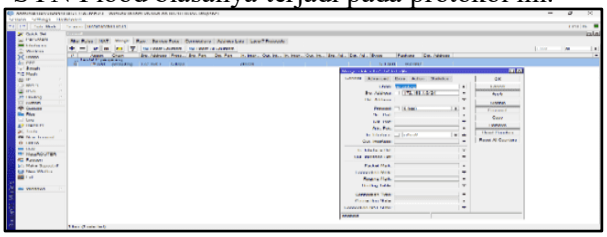
Rule ini hanya akan memproses IP sumber dari subnet jaringan lokal tertentu, yaitu rentang IP 172.168.1.0 hingga 172.168.1.255. Umumnya digunakan jika hanya ingin mendeteksi serangan dari dalam jaringan (jaringan lokal tertentu).



Gambar 11. Tandai IP Penyerang (Manggle Rule) Src. Address: 172.168.1.0/24

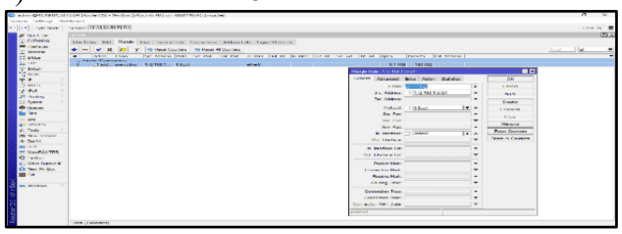
c.) Protocol: tcp

Fokus hanya pada trafik TCP, karena serangan SYN Flood biasanya terjadi pada protokol ini.



Gambar 12 Tandai IP Penyerang (Manggle Rule) Protocol: tcp

d.) In. Interface: ether8

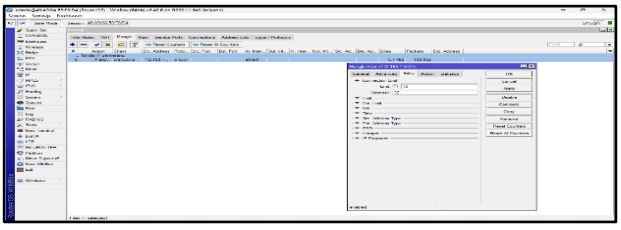


Gambar 13. Tandai IP Penyerang (Manggle Rule) In. Interface: ether8

2) Tab Extra

Connection Limit:

Limit: 10, Jika satu IP membuat lebih dari 10 koneksi aktif ke router, maka IP tersebut akan dianggap mencurigakan. Netmask: 32, memastikan pengecekan berlaku untuk tiap alamat IP individu.



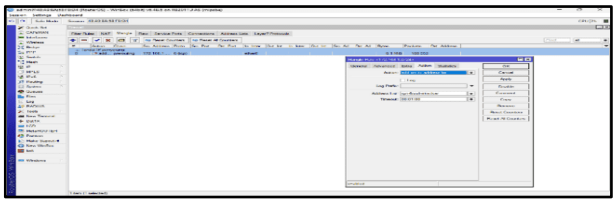
Gambar 14. Tandai IP Penyerang (Manggle Rule) Connection Limit

3) Tab Action

a.) Action: add src to address list

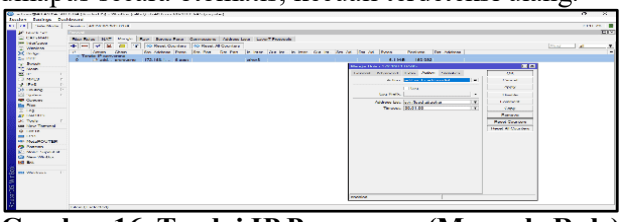
P-ISSN 1858-2680
E-ISSN 2723-4673

Jika sebuah IP memenuhi kriteria di atas (lebih dari 10 koneksi aktif), maka IP tersebut akan ditambahkan secara otomatis ke address list.



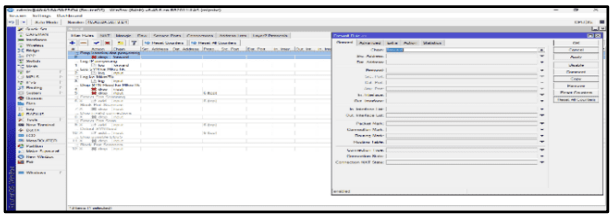
Gambar 15 Tandai IP Penyerang (Manggle Rule) Action: add src to address list

b.) Address List: syn-flood-attacker
IP akan masuk ke dalam daftar syn-flood-attacker, yang nantinya digunakan oleh rule firewall lain untuk memblokir atau memantau lebih lanjut
c.) Timeout: 00:01:00
IP penyerang akan tetap berada dalam address list selama 1 menit sejak terdeteksi. Setelah itu akan dihapus secara otomatis, kecuali terdeteksi ulang.



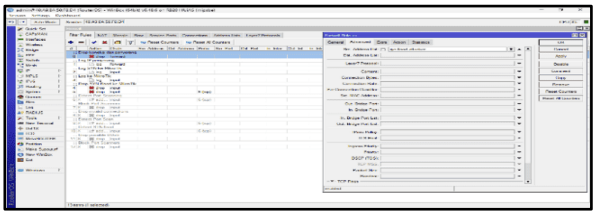
Gambar 16. Tandai IP Penyerang (Manggle Rule) Address List: syn-flood-attacker

Tujuan dan Fungsi:
a.) Chain: forward
Menandakan aturan ini berlaku untuk trafik yang melewati router (bukan yang masuk/keluar dari router langsung).



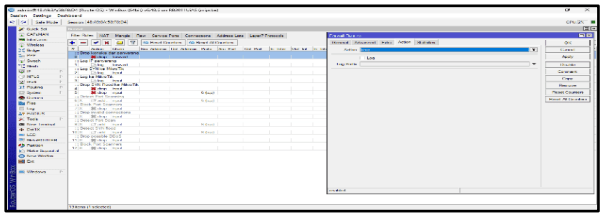
Gambar 17. Drop Koneksi Penyerang (Filter Rules) Chain: forward

Tab Advanced
b.) Src. Address List: synflood-attacker
Ini adalah daftar alamat IP sumber yang dianggap melakukan serangan SYN Flood dan sebelumnya sudah dimasukkan ke dalam address list tersebut oleh aturan deteksi SYN Flood.



Gambar 18. Drop Koneksi Penyerang (Filter Rules) Src. Address List: synflood-attacker

Tab Action
c.) Action: drop
Artinya semua koneksi dari IP yang ada dalam daftar synflood-attacker akan diblokir tanpa pemberitahuan (dibuang begitu saja).



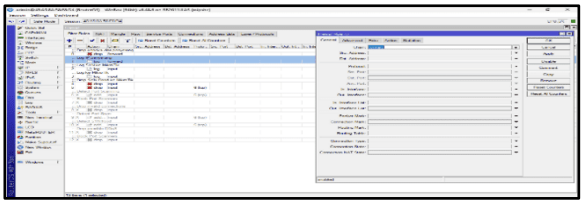
Gambar 19. Drop Koneksi Penyerang (Filter Rules) Action: drop

Fungsi Utama:
Mencegah koneksi berbahaya dari penyerang (misalnya SYN Flood) agar tidak mengganggu trafik internal atau memanfaatkan router untuk menyebarkan serangan.

2. Log IP Penyerang

Rule ini digunakan untuk mencatat (log) alamat IP penyerang yang terdeteksi berdasarkan kriteria tertentu, sehingga administrator jaringan bisa memantau dan menganalisis aktivitas yang mencurigakan.

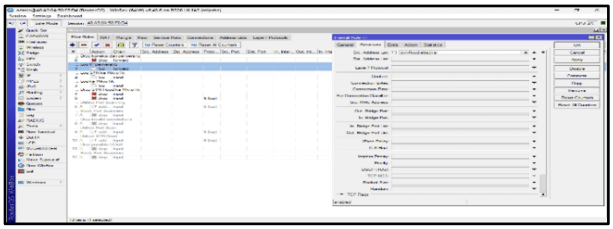
1) Tab General
a.) Chain: forward
Artinya rule ini bekerja pada lalu lintas yang diteruskan (bukan ke/dari router itu sendiri, tapi melewati router).



Gambar 20 Log IP Penyerang Chain: forward

b.) Src. Address / Dst. Address: Kosong
Tidak dibatasi alamat IP sumber/tujuan secara spesifik pada bagian ini.
c.) Protocol, Ports, Interfaces: Tidak ditentukan
Filter lebih spesifik dilakukan di tab lain (seperti Advanced).

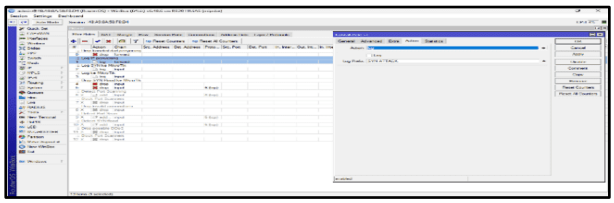
2) Tab Advanced
a.) Src. Address List: synflood-attacker
Hanya IP yang masuk dalam daftar ini yang akan dicatat. Artinya IP ini sudah ditandai sebelumnya sebagai pelaku SYN Flood Attack melalui rule lain.



Gambar 21. Log IP Penyerang Src. Address List: synflood-attacker

P-ISSN 1858-2680
E-ISSN 2723-4673

3) Tab Action
Action: log
a.) Log Prefix: SYN ATTACK:
Menambahkan prefiks ini ke setiap entri log yang dihasilkan agar mudah dikenali dalam log MikroTik (misalnya, saat mengecek di menu Log).

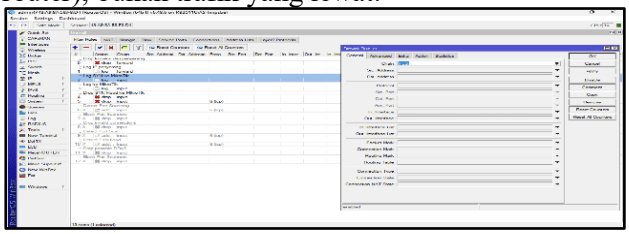


Gambar 22. Log IP Penyerang Log Prefix: SYN ATTACK

Fungsi Utama:
a.) Melacak sumber serangan.
b.) Melihat frekuensi dan pola.
c.) Menyimpan bukti aktivitas berbahaya.

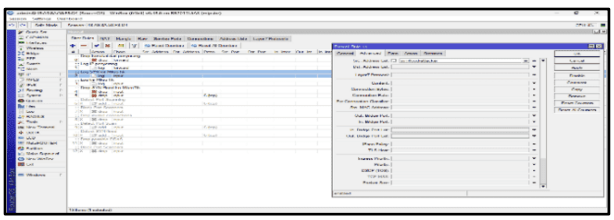
3. Log SYN Ke Mikrotik

Rule ini digunakan untuk mencatat aktivitas serangan SYN Flood yang diarahkan langsung ke router MikroTik
1) Tab General
a.) Chain: input
Artinya rule ini berlaku untuk lalu lintas yang ditujukan ke router itu sendiri (misalnya ke IP publik router), bukan trafik yang lewat.



Gambar 23. Log SYN Ke Mikrotik Chain: input

b.) Src. Address / Dst. Address / Protocol / Port: Kosong
Tidak dibatasi secara spesifik di tab ini. Rule ini akan menangkap semua koneksi yang memenuhi syarat di tab Advanced.
2) Tab Advanced
a.) Src. Address List: syn-flood-attacker
Rule ini hanya berlaku untuk IP yang sudah terdaftar dalam address list "syn-flood-attacker", yang artinya IP tersebut telah dikenali sebelumnya sebagai pelaku SYN flood attack.
b.) Field lain dibiarkan kosong, yang berarti tidak ada filter tambahan.



Gambar 24. Log SYN Ke Mikrotik Src. Address List: syn-flood-attacker

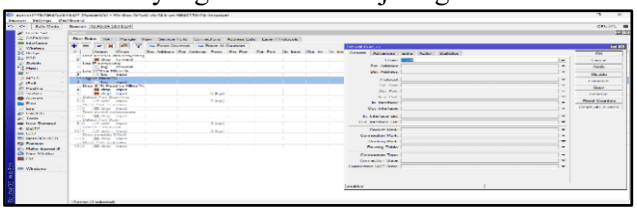
3) Tab Action
Action: log
Rule ini tidak memblokir atau menjatuhkan paket, hanya mencatat (logging) informasi dari paket yang sesuai.
Log Prefix: SYN ATTACK INPUT
Prefiks ini akan muncul di menu log MikroTik, membantu membedakan entri log dari jenis serangan lain.

Fungsi Rule Ini

Digunakan untuk monitoring dan forensik, agar administrator dapat:
a.) Mengetahui apakah router sedang diserang SYN Flood secara langsung.
b.) Melihat IP penyerang yang diarahkan ke router.
c.) Menelusuri waktu dan frekuensi serangan.

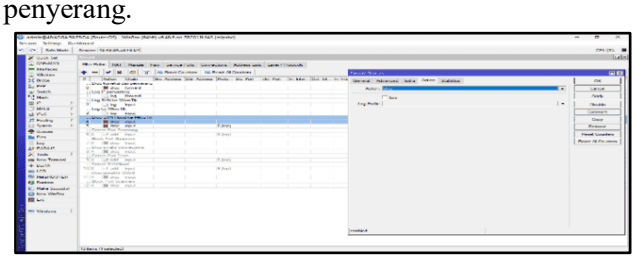
1. Drop SYN Flood Ke Mikrotik

Rule ini bertujuan untuk memblokir (drop) trafik SYN yang dianggap sebagai serangan dan diarahkan langsung ke router MikroTik, berdasarkan daftar alamat penyerang yang telah diidentifikasi sebelumnya.
1) Tab General
Chain: input
Rule ini berlaku untuk trafik yang ditujukan langsung ke MikroTik itu sendiri, misalnya ke IP publik router, bukan trafik yang diteruskan ke jaringan internal.



Gambar 25. Drop SYN Flood Ke Mikrotik Chain: input

2) Tab Advanced
Src. Address List: syn-flood-attacker
Hanya akan memproses trafik yang berasal dari alamat IP yang terdaftar dalam address list bernama "syn-flood-attacker". IP di daftar ini biasanya dimasukkan oleh rule deteksi SYN Flood.
3) Tab Action
Action: drop
Trafik yang cocok dengan kriteria di atas akan langsung dibuang tanpa diproses lebih lanjut dan tidak ada log yang dicatat (kecuali ada rule log sebelumnya). Ini berguna untuk mengurangi beban CPU dan mencegah eksploitasi lebih lanjut oleh penyerang.

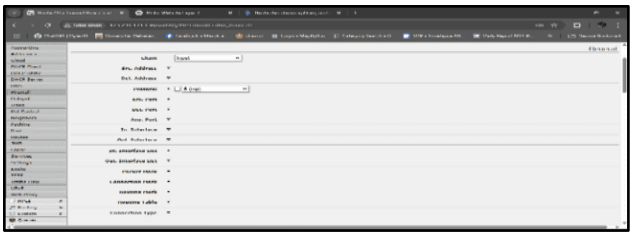


Gambar 26. Drop SYN Flood Ke Mikrotik Action: drop

P-ISSN 1858-2680
E-ISSN 2723-4673

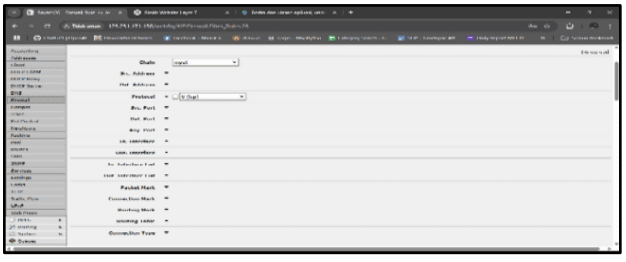
Kegunaan Rule Ini:
Mencegah kerusakan atau overload akibat serangan SYN Flood yang menyerang langsung MikroTik. Meningkatkan keamanan router, terutama jika router diekspos ke internet.
Efektif jika digunakan bersama dengan rule log dan deteksi, misalnya:
a.) Rule yang mendeteksi pola SYN Flood → memasukkan IP ke address list.
b.) Rule log untuk mencatat serangan.
c.) Rule ini untuk memutus trafik dari penyerang.

2. Drop Port Scanning
Rule ini dibuat untuk memblokir upaya port scanning terhadap MikroTik. Port scanning sering digunakan oleh penyerang untuk mencari port terbuka sebelum melakukan eksploitasi lebih lanjut.
1) Tab General
Chain: input
a.) Artinya rule ini memproses trafik yang ditujukan langsung ke router MikroTik, bukan trafik yang diteruskan ke jaringan lokal.



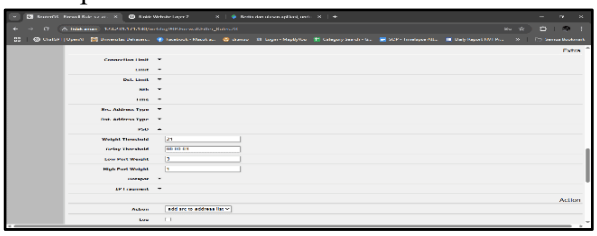
Gambar 27. Drop Port Scanning

b.) Protocol: tcp
Rule ini hanya berlaku untuk trafik dengan protokol TCP, karena sebagian besar port scanning menggunakan TCP SYN atau koneksi TCP lainnya untuk mendeteksi layanan aktif.



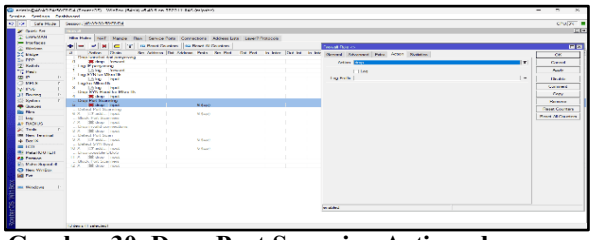
Gambar 28. Drop Port Scanning Protocol: tcp

2) Tab Extra
a.) Weight Threshold: 21
Jumlah "berat" koneksi dari satu IP yang dianggap sebagai port scanning. Jika jumlah total weight dari koneksi melebihi nilai ini, maka dianggap mencurigakan.
b.) Delay Threshold: 00:00:03
Jika beberapa koneksi dari satu IP terjadi dalam waktu 3 detik, maka sistem akan menghitung dan membandingkan weight-nya. Ini mendeteksi scanning cepat.
c.) Low Port Weight: 3
Koneksi ke port rendah (misalnya: 0–1023) akan diberi nilai weight 3. Karena port ini sering digunakan untuk service penting (HTTP, SSH, FTP), maka diberi bobot lebih tinggi.
d.) High Port Weight: 1
Koneksi ke port tinggi (di atas 1023) diberi bobot lebih rendah (1). Biasanya karena ini port dinamis atau ephemeral.



Gambar 29. Drop Port Scanning Tab Extra

3) Tab Action
a.) Action: drop
Semua koneksi yang memenuhi kriteria rule ini akan langsung dibuang tanpa diproses lebih lanjut.
b.) Tidak akan dicatat di log (kecuali ada rule log terpisah sebelumnya).



Gambar 30. Drop Port Scanning Action: drop

4) Fungsi dan Tujuan
a.) Melindungi MikroTik dari pemindaian port (port scan) yang bisa menjadi langkah awal dari serangan.
b.) Mengurangi kemungkinan eksploitasi layanan terbuka di MikroTik.
c.) Meningkatkan keamanan jaringan, terutama jika MikroTik memiliki IP publik atau terbuka ke internet.
5) Catatan Penting
Rule ini biasanya bekerja bersama rule pendeteksi scanning, seperti:
a.) Rule sebelumnya yang mendeteksi pola port scan berdasarkan TCP flags atau connection rate dan menambahkan IP ke address list penyerang.
b.) Rule ini akan menindaklanjuti dengan langsung memblokir trafik TCP dari penyerang.

Pemantauan dan Logging
Sistem mencatat log koneksi yang mencurigakan dengan prefix seperti "SYN ATTACK:" sehingga memudahkan proses monitoring oleh administrator.

1. Log Ke Mikrotik
Rule ini berfungsi untuk mencatat aktivitas dari IP yang telah dicurigai melakukan serangan SYN Flood, yaitu IP yang telah dimasukkan sebelumnya ke dalam address list syn-flood-attacker. Logging ini sangat penting sebagai bagian dari proses monitoring dan dokumentasi keamanan jaringan, serta membantu

P-ISSN 1858-2680
E-ISSN 2723-4673

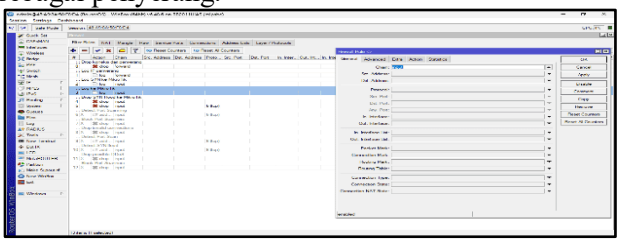
dalam analisis forensik terhadap serangan yang masuk.

a.) Tab General

Chain: input:

Rule ini berlaku untuk trafik yang ditujukan langsung ke router MikroTik itu sendiri.

Dengan chain input, rule akan mencatat semua koneksi masuk ke router dari IP yang telah ditandai sebagai penyerang.

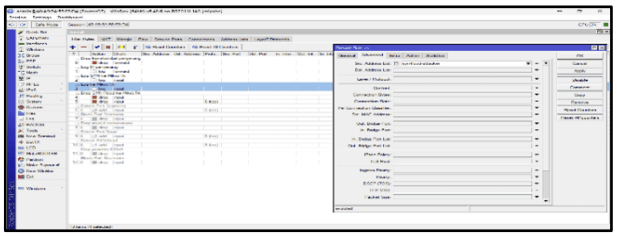


Gambar 31. Log Ke Mikrotik

b.) Tab Advanced

Src. Address List: syn-flood-attacker:

Rule hanya akan dipicu apabila sumber IP termasuk dalam daftar syn-flood-attacker, yaitu daftar IP yang sebelumnya telah dideteksi melakukan koneksi mencurigakan (misalnya lebih dari 10 koneksi aktif secara bersamaan).



Gambar 31. Log Ke Mikrotik Src. Address List: syn-flood-attacker

c.) Tab Action

Action: log:

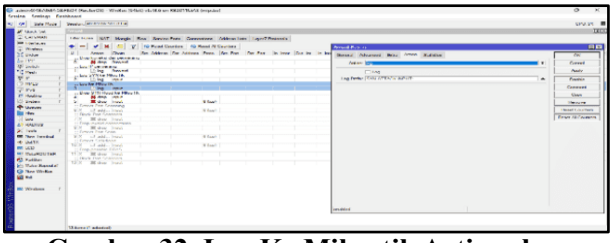
Paket dari IP dalam address list syn-flood-attacker tidak akan diblokir langsung oleh rule ini, tetapi akan dicatat ke dalam log MikroTik, untuk keperluan pengawasan dan pencatatan.

Log Prefix: SYN ATTACK INPUT:

Log akan ditandai dengan prefix ini agar mudah dikenali dan difilter di sistem log.

Contoh tampilan log:

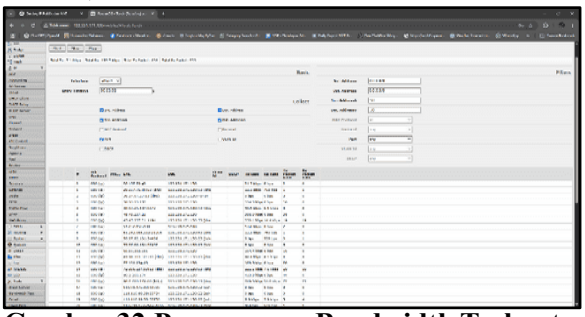
SYN ATTACK INPUT: input: in:ether8 src-address=172.168.1.22



Gambar 32. Log Ke Mikrotik Action: log

Tujan dan Fungsi

Memberikan informasi real-time kepada administrator jaringan bahwa ada trafik masuk dari IP yang telah ditandai sebagai penyerang. Menciptakan jejak log yang bisa dianalisis, baik melalui log internal MikroTik maupun dikirim ke syslog server eksternal. Rule ini tidak memblokir, melainkan hanya mendokumentasikan — sangat berguna sebelum dilakukan tindakan lebih lanjut (misalnya drop otomatis).



Gambar 32 Penggunaan Bandwidth Terkontrol

Pengujian Sistem

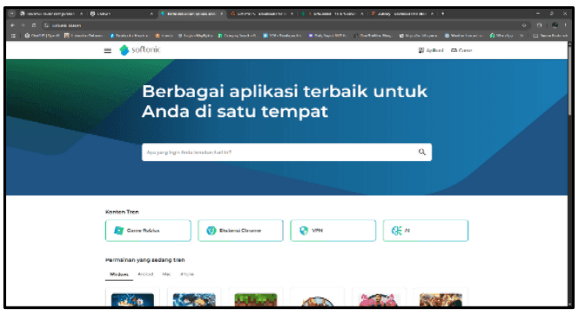
Beberapa skenario pengujian seperti:

A. Akses situs terlarang

1) https://www.softonic-id.com

Softonic-id.com merupakan salah satu situs yang menyediakan berbagai perangkat lunak yang dapat diunduh secara gratis. Meskipun sekilas tampak sebagai penyedia layanan unduhan yang sah, situs ini sering kali menjadi sumber distribusi installer pihak ketiga yang telah dimodifikasi. Installer tersebut berpotensi menyisipkan adware, spyware, atau bahkan malware yang dapat membahayakan perangkat pengguna. Selain itu, tampilan situs yang dipenuhi iklan pop-up dan tautan menyesatkan dapat mengarahkan pengguna ke situs phishing yang berbahaya.

2) https://getintopc.com



Gambar 33. Akses Situs softonic-id.com

Getintopc.com adalah situs yang dikenal luas sebagai tempat untuk mengunduh perangkat lunak populer, termasuk versi berbayar secara gratis. Situs ini umumnya menyediakan file instalasi yang telah disertai crack atau keygen, yang pada dasarnya merupakan bentuk pembajakan perangkat lunak. Penggunaan perangkat lunak bajakan selain melanggar hak cipta juga berisiko tinggi terhadap keamanan sistem. File unduhan dari situs ini berpotensi mengandung malware berbahaya seperti trojan, backdoor, atau keylogger yang dapat mencuri informasi pengguna secara diam-diam. Mengingat

P-ISSN 1858-2680
E-ISSN 2723-4673

risikonya, situs ini sebaiknya dihindari dalam penggunaan perangkat lunak secara etis dan aman.

Gambar 34. Akses Situs getintopc.com

3) https://apkcombo.com

Apkcombo.com adalah situs yang menyediakan file APK dari berbagai aplikasi Android yang dapat diunduh secara langsung tanpa melalui Google Play Store. Meskipun memberikan kemudahan bagi pengguna untuk mendapatkan aplikasi versi lama atau aplikasi yang tidak tersedia di wilayah tertentu, situs ini menyimpan risiko keamanan yang cukup serius. File APK yang tersedia tidak selalu dapat dijamin keasliannya, dan sangat mungkin telah dimodifikasi oleh pihak ketiga. Aplikasi yang telah dimodifikasi (modded) ini berpotensi membawa spyware, adware, atau bahkan malware yang dapat mencuri data pribadi pengguna.

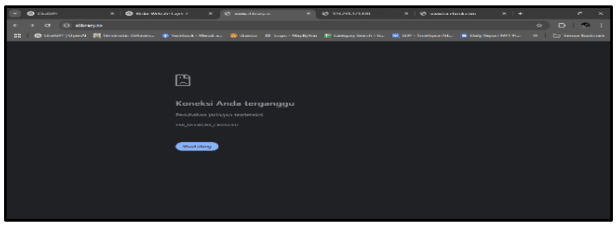
Gambar 35. Akses Situs apkcombo.com

4) https://www.zlibrary.to

Zlibrary.to adalah situs yang menyediakan akses gratis ke jutaan buku digital dalam berbagai format seperti PDF dan EPUB. Meskipun keberadaannya menjadi alternatif populer bagi pelajar dan akademisi, situs ini beroperasi dengan melanggar hukum hak cipta karena mendistribusikan buku-buku berbayar tanpa izin dari penerbit atau penulis. Selain itu, karena sering diblokir oleh otoritas di berbagai negara, situs ini kerap muncul dalam bentuk mirror atau kloning yang tidak resmi. Beberapa versi mirror ini bahkan diketahui menyisipkan malware atau menerapkan teknik phishing untuk mencuri data pengguna.

Gambar 16. Akses Situs zlibrary.to

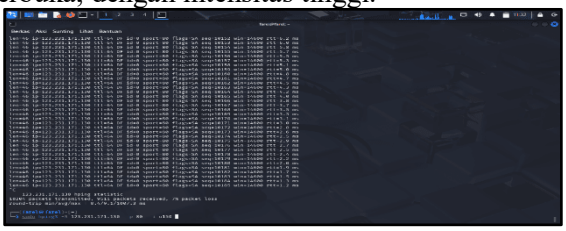
Ketika aturan firewall diaktifkan situs yang termasuk dalam daftar blacklist sudah tidak dapat diakses atau sudah diblokir melalui aturan firewall.



Gambar 37. Akses Situs Terlarang Ketika Firewall Diaktifkan

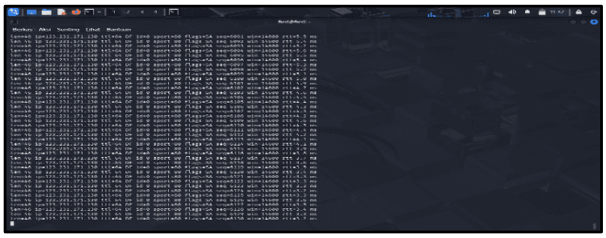
B. Serangan DoS menggunakan Hping3

Pengujian ini dilakukan untuk mengetahui sejauh mana kemampuan firewall Mikrotik dalam menangani serangan Denial of Service (DoS) berbasis protokol TCP, khususnya jenis serangan SYN Flood. Untuk melakukan simulasi serangan, digunakan aplikasi Hping3, yaitu sebuah tool jaringan berbasis CLI (Command Line Interface) yang umum digunakan untuk melakukan audit keamanan dan simulasi serangan jaringan. Dalam pengujian ini, Hping3 dikonfigurasi untuk mengirimkan paket TCP SYN secara terus-menerus ke IP publik dari router Mikrotik, melalui port terbuka, dengan intensitas tinggi.



Gambar 38. Serangan DoS menggunakan Hping3

Firewall Mikrotik yang telah dikonfigurasi sebelumnya menggunakan kombinasi fitur Filter Rules, Mangle, Raw, dan Address List. Secara khusus, rule untuk mendeteksi serangan SYN Flood dirancang untuk menangkap koneksi SYN yang tidak wajar, menandai IP sumber serangan, mencatat log dengan prefix “SYN ATTACK INPUT:”, dan secara otomatis memblokir IP tersebut melalui address list syn-flood-attacker.

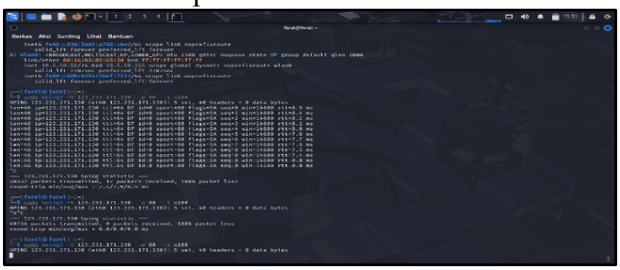


Gambar 39. Serangan DoS menggunakan Hping3 Ketika Tools Berjalan

Hasil pengujian menunjukkan bahwa firewall Mikrotik berhasil mendeteksi lalu lintas abnormal yang dihasilkan oleh Hping3. IP sumber serangan langsung masuk ke dalam daftar address list dan

P-ISSN 1858-2680
E-ISSN 2723-4673

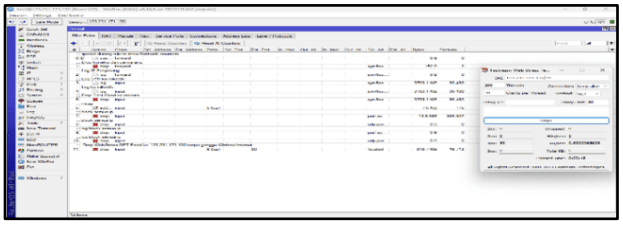
koneksinya diblokir secara real-time oleh rule dengan aksi drop. Hal ini terlihat dari tidak adanya respons atau peningkatan trafik signifikan pada interface target, serta munculnya log serangan di sistem Mikrotik. Router tetap stabil dan tidak mengalami overload selama proses simulasi dilakukan.



Gambar 40. Serangan DoS menggunakan Hping3 Ketika Firewall Diaktifkan

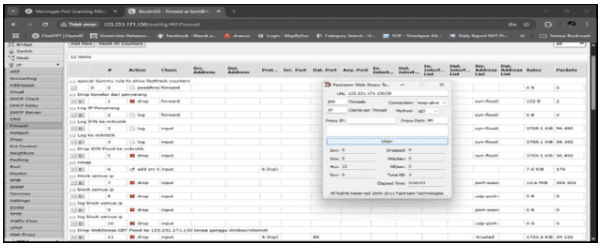
C. Uji WebStress Tester

Pada pengujian ini, serangan diarahkan ke jaringan internal yang dilindungi oleh firewall Mikrotik, melalui antarmuka ether5. Firewall telah dikonfigurasi dengan berbagai aturan pengamanan, seperti penggunaan Filter Rules dan Raw Rules untuk memblokir koneksi abnormal, serta penambahan IP penyerang ke dalam Address List secara otomatis. Sistem juga dilengkapi dengan fitur logging untuk mencatat aktivitas serangan dengan prefix tertentu.



Gambar 41. Uji WebStress Tester

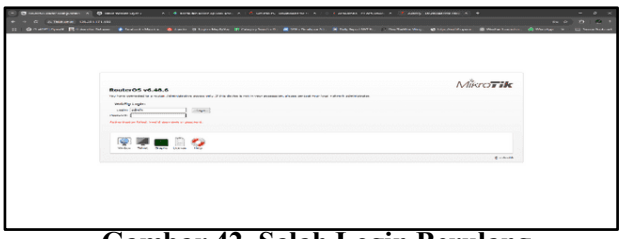
Berdasarkan hasil yang ditampilkan pada aplikasi Fasstream Web Stress Tester, terlihat bahwa tidak ada data yang berhasil dikirim ke target (0 KB/s), dan seluruh koneksi yang dibuat oleh aplikasi ditolak oleh sistem. Selain itu, tidak tampak peningkatan trafik pada interface target (ether5), baik pada kolom Rx (receive) maupun Tx (transmit), yang mengindikasikan bahwa serangan tidak berhasil menembus sistem pertahanan jaringan.



Gambar 41. Uji WebStress Tester Ketika Firewall Diaktifkan

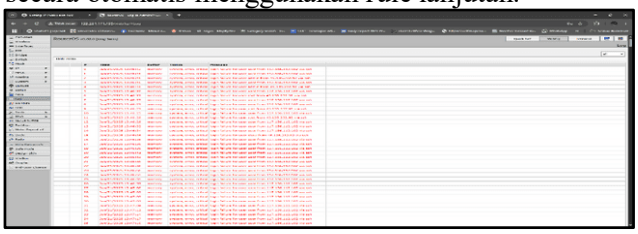
D. Salah login berulang

Pengujian ini bertujuan untuk mengamati respons sistem firewall terhadap aktivitas login yang mencurigakan, seperti percobaan masuk secara terus-menerus dengan kata sandi yang salah. Dalam simulasi ini, dilakukan login berulang ke antarmuka Mikrotik menggunakan kredensial yang tidak valid



Gambar 42. Salah Login Berulang

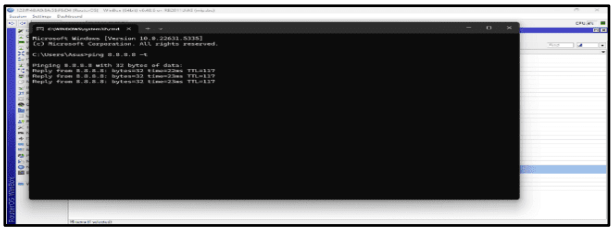
Firewall yang telah dikonfigurasi menggunakan fitur Filter Rules dan Logging mencatat aktivitas login gagal tersebut. Setiap percobaan login yang tidak berhasil dicatat dalam sistem log, sehingga administrator dapat memantau adanya upaya brute force atau akses tidak sah. Jika percobaan dilakukan secara terus-menerus dalam waktu singkat, IP pelaku dapat dimasukkan ke dalam address list dan diblokir secara otomatis menggunakan rule lanjutan.



Gambar 43 Pencatatan Salah Login Berulang

Berdasarkan hasil pengujian, sistem firewall berhasil mencatat aktivitas login yang mencurigakan dan memberikan log yang informatif. Hal ini menunjukkan bahwa firewall mampu mendeteksi potensi ancaman keamanan dari dalam jaringan, dan pengujian dinilai berhasil.

E. Pengujian koneksi melalui ping dan kecepatan transfer



Gambar 44. Pengujian koneksi melalui

Hasil pengujian menunjukkan bahwa koneksi antar perangkat tetap berjalan normal dengan waktu ping yang rendah dan tanpa kehilangan paket. Proses transfer file antar komputer dalam jaringan lokal (LAN) juga berlangsung dengan lancar dan kecepatan stabil. Tidak ditemukan indikasi hambatan akibat konfigurasi firewall, yang berarti pengaturan keamanan tidak mengganggu kinerja jaringan secara umum. Dengan demikian, dapat disimpulkan bahwa pengujian koneksi melalui ping dan kecepatan transfer berhasil, dan firewall yang diterapkan tidak

P-ISSN 1858-2680
E-ISSN 2723-4673

menurunkan kualitas layanan jaringan yang digunakan dalam aktivitas pembelajaran.

B.Pembahasan

Penerapan firewall *Mikrotik* di SMK Negeri 3 Kota Bengkulu secara signifikan meningkatkan keamanan jaringan. Berdasarkan metode Security Life Cycle (SLC), tahapan mulai dari Assess, Design, Implement, hingga Maintain dijalankan secara sistematis.

A. Assess: Mengidentifikasi ancaman seperti malware, situs tidak pantas, dan *DoS*. Pada tahap Assess, dilakukan identifikasi terhadap potensi ancaman yang dapat mengganggu sistem jaringan, seperti malware, situs yang tidak sesuai dengan kebijakan sekolah, serta serangan *Denial of Service (DoS)*. Identifikasi ini menjadi landasan penting dalam merancang sistem pertahanan jaringan yang relevan dengan kondisi nyata di lapangan. Tahap selanjutnya, yaitu Design, difokuskan pada perancangan aturan-aturan keamanan (firewall rules) yang mencakup pemblokiran IP mencurigakan, filtering konten berbasis domain dan kata kunci, serta pengelompokan akses pengguna berdasarkan peran (seperti guru, siswa, dan staf administrasi). Selain itu, pada tahap ini juga dirancang strategi pengaturan *bandwidth* agar lebih efisien dan sesuai prioritas.

B. Design: Membuat rules untuk pemblokiran IP, filtering content, dan segregasi akses.

C. Implement: Mengkonfigurasi router *Mikrotik*, menetapkan aturan firewall dan pengelompokan akses berdasarkan user. Pada tahap Implement, perancangan tersebut diwujudkan melalui konfigurasi teknis pada perangkat *Mikrotik*. Berbagai fitur firewall digunakan secara terpadu untuk membangun sistem pertahanan berlapis. Fitur *Filter Rules* digunakan untuk menyaring dan memblokir lalu lintas yang tidak sah berdasarkan IP, port, dan protokol. Fitur *Mangle* digunakan untuk menandai koneksi abnormal yang dapat mengindikasikan serangan, seperti koneksi TCP dengan frekuensi tinggi dalam waktu singkat. Fitur *Raw* dimanfaatkan untuk menghentikan paket berbahaya sejak awal sebelum melalui proses connection tracking, sehingga mempercepat respons sistem terhadap ancaman. Selain itu, fitur *Address List* digunakan untuk menyimpan IP address yang teridentifikasi sebagai sumber serangan agar dapat diblokir secara otomatis. Seluruh aktivitas mencurigakan dicatat menggunakan fitur logging, dengan prefix khusus seperti "SYN ATTACK INPUT", guna memudahkan proses pemantauan oleh administrator jaringan.

D. Maintain: Melakukan pemantauan, pembaruan rules, dan backup konfigurasi secara rutin. Tahap terakhir dalam siklus, yaitu Maintain, dilakukan untuk menjaga agar sistem keamanan tetap berjalan optimal. Pemeliharaan dilakukan melalui pemantauan trafik secara rutin, pembaruan aturan firewall jika muncul pola serangan baru, pencadangan konfigurasi secara berkala, dan evaluasi performa sistem secara menyeluruh. Tahap ini penting untuk memastikan sistem keamanan tidak hanya mampu menanggulangi ancaman saat ini, tetapi juga adaptif terhadap ancaman yang mungkin muncul di masa depan.Berdasarkan implementasi firewall berbasis *Mikrotik* di SMK Negeri 3 Kota Bengkulu, didapatkan bahwa setiap rule memiliki peran yang berbeda. *Filter Rule* banyak digunakan untuk pemblokiran akses dan serangan langsung, *Raw Rule* lebih difokuskan pada efisiensi dalam penanganan serangan berintensitas tinggi, sedangkan *Mangle Rule* membantu dalam pengaturan dan klasifikasi lalu lintas jaringan. Selain itu, pengujian dengan *Web Stress Tester* dan *Hping3* menunjukkan bahwa firewall dapat merespons berbagai serangan dengan cukup baik. Serangan berbasis *SYN Flood* berhasil diblokir, percobaan akses ke situs terlarang juga terhambat, dan koneksi jaringan tetap stabil berkat pengaturan *bandwidth* serta penggunaan batas limit untuk *DDoS*. Dengan demikian, pembahasan ini memperkuat bahwa kombinasi *Filter*, *Raw*, dan *Mangle Rule* yang dikonfigurasi secara tepat mampu meningkatkan keamanan dan stabilitas jaringan sekolah.Fitur firewall seperti *Filter Rules*, *Raw*, dan *Mangle* sangat efektif dalam mencegah serangan, terutama terhadap *SYN Flooding* dan *port scanning*. *Logging* dan pengaturan *bandwidth* yang baik juga mendukung stabilitas sistem.

Dari hasil pengujian, dapat disimpulkan bahwa penerapan firewall ini:

a.) Mampu memblokir akses ilegal secara otomatis.
b.) Efektif menangani beban jaringan saat diuji dengan simulasi serangan.
c.) Meningkatkan efisiensi pemakaian jaringan untuk aktivitas pembelajaran.

C. Hasil Pengujian

Berdasarkan hasil pengujian yang telah dilakukan, diperoleh temuan sebagai berikut:

1. Filter Rule

Penggunaan *Filter Rule* pada firewall *Mikrotik* terbukti mampu memblokir serangan *SYN Flood* dan berbagai bentuk akses ilegal yang terdeteksi melalui daftar alamat (*Address List*). Selain itu, *Filter Rule* juga efektif dalam mencegah akses ke situs-situs yang dianggap tidak sesuai dengan kebijakan sekolah atau berpotensi membahayakan pengguna jaringan. Meskipun demikian,

P-ISSN 1858-2680
E-ISSN 2723-4673

kelemahan utama dari *Filter Rule* adalah membutuhkan lebih banyak sumber daya (resource) sistem karena bekerja setelah proses *connection tracking*. Hal ini berarti setiap paket harus melalui tahap pencatatan koneksi sebelum dapat difilter, sehingga dalam kondisi serangan berintensitas tinggi kinerja router dapat menurun.

2. Raw Rule
   Penggunaan *Raw Rule* lebih ringan dibandingkan dengan *Filter Rule* karena aturan ini bekerja sebelum *connection tracking*. Dengan demikian, paket yang mencurigakan atau berbahaya dapat langsung dibuang sebelum masuk ke dalam proses pencatatan koneksi. Dari hasil pengujian, *Raw Rule* terbukti efektif dalam menangani serangan *DDoS* dengan jumlah paket yang sangat tinggi (packet rate). Hal ini membuat *Raw Rule* sangat cocok digunakan sebagai lapisan pertama dalam mitigasi serangan volumetrik. Dengan sifatnya yang efisien, *Raw Rule* dapat mengurangi beban sistem sekaligus meningkatkan stabilitas jaringan ketika menghadapi serangan berskala besar.
3. Mangle Rule
   Penggunaan *Mangle Rule* dalam penelitian ini berfokus pada fungsi penandaan (marking) terhadap paket, koneksi, maupun rute (routing). Hasil pengujian menunjukkan bahwa *Mangle Rule* lebih tepat digunakan untuk keperluan manajemen *bandwidth* dan pengelompokan trafik jaringan, bukan sebagai pemblokir serangan secara langsung. Dengan adanya penandaan ini, administrator jaringan dapat lebih mudah dalam mengatur prioritas trafik sehingga koneksi jaringan menjadi lebih stabil dan penggunaan *bandwidth* lebih efisien. Dengan kata lain, *Mangle Rule* merupakan pendukung penting dalam optimalisasi performa jaringan, meskipun bukan alat utama untuk menghentikan serangan.
4. Penggunaan Limit pada Serangan DDoS
   Penerapan batasan dengan parameter *limit* maupun *connection-limit* pada firewall *Mikrotik* terbukti mampu membatasi jumlah koneksi yang diizinkan dari satu sumber IP. Dari hasil uji coba, konfigurasi ini menunjukkan adanya penurunan signifikan terhadap jumlah paket berlebih yang masuk ke jaringan selama simulasi serangan *DDoS*. Pada pengujian menggunakan *Hping3* di *Kali Linux*, serangan dibatasi maksimal 500 paket per detik, sedangkan dengan *Web Stress Tester* dibatasi 200 koneksi simultan. Jika serangan melebihi batas tersebut, server berisiko mengalami *down*. Dengan adanya pembatasan ini, kestabilan jaringan tetap terjaga dan layanan tetap tersedia meskipun terjadi percobaan serangan *DDoS*, sehingga teknik pembatasan ini sangat penting dalam mempertahankan ketersediaan (*availability*) layanan jaringan pada kondisi serangan.

V. PENUTUP

A.Kesimpulan

Dengan adanya log, administrator dapat melakukan deteksi dini dan analisis forensik terhadap potensi serangan, sehingga tindakan pencegahan dapat dilakukan lebih cepat dan tepat sasaran. Implementasi pemblokiran terhadap situs-situs yang tidak sesuai dengan kebijakan sekolah, seperti situs berisi *malware*, konten negatif, atau potensi eksploitasi, turut menciptakan lingkungan digital yang aman dan mendukung proses pembelajaran. Fitur firewall dalam menyaring akses ke situs-situs terlarang ini memperkuat penerapan kebijakan internet sehat di lingkungan pendidikan.Dari hasil pengujian juga diperoleh gambaran bahwa setiap rule memiliki fungsi yang berbeda. *Filter Rule* efektif dalam memblokir akses ilegal dan serangan sederhana, *Raw Rule* lebih efisien untuk menangani serangan dengan intensitas tinggi seperti *DDoS* karena bekerja sebelum *connection tracking*, sedangkan *Mangle Rule* berfungsi untuk menandai paket, koneksi, maupun rute sehingga mendukung pengaturan *bandwidth* dan klasifikasi trafik jaringan. Secara keseluruhan, kombinasi penggunaan *drop rule, log rule, blacklist,* serta penerapan *Filter Rule, Raw Rule,* dan *Mangle Rule* memberikan perlindungan berlapis, adaptif, dan efisien tanpa mengganggu performa jaringan. Dengan demikian, firewall *MikroTik* dapat dijadikan solusi efektif dan terjangkau dalam menjaga keamanan jaringan, khususnya di lingkungan sekolah atau institusi pendidikan.

B.Saran

Dengan melakukan pembaruan secara berkala, sistem keamanan jaringan dapat tetap relevan dan efektif dalam menghadapi ancaman baru.Selain itu, perlu dipertimbangkan untuk menambahkan sistem monitoring terpusat, seperti syslog server atau integrasi dengan perangkat lunak manajemen jaringan, guna meningkatkan kemampuan dalam mendeteksi dan merespons insiden secara real-time. Monitoring yang komprehensif akan membantu administrator dalam mengidentifikasi pola serangan dan mengambil keputusan secara lebih cepat dan tepat.Penulis juga menyarankan agar pihak sekolah memberikan pelatihan teknis secara berkala kepada staf TI atau administrator jaringan, khususnya terkait konfigurasi firewall, deteksi serangan, serta prosedur mitigasi. Dengan peningkatan kapasitas sumber daya manusia, maka pengelolaan keamanan jaringan dapat berjalan lebih optimal dan responsif terhadap ancaman.Terakhir, penerapan sistem keamanan jaringan sebaiknya tidak hanya bersifat teknis, melainkan juga diiringi dengan upaya edukatif kepada para pengguna jaringan, khususnya siswa dan

P-ISSN 1858-2680
E-ISSN 2723-4673

guru. Edukasi mengenai penggunaan internet yang aman dan bertanggung jawab akan memperkuat perlindungan jaringan dari sisi perilaku pengguna serta menciptakan budaya digital yang sehat di lingkungan sekolah.

DAFTAR PUSTAKA

[1] Akbar, M., Agung, T. A., Marcellino, I. I., & Fauzi, A. (2021). Analisis Keamanan Jaringan Komputer Pada Sekolah Menengah Atas Negeri 04 Bandung. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *4*(4), 258-264.

[2] Arunawati, A. P. (2020). "Webstress Tool: Pengertian – Contoh dan Fungsinya. Astuti, I. K. (2020). Jaringan komputer, pp. 3-4.

[3] Dinda, S. R. O., & Sunardi, H. (2023). Perancangan Dan Implementasi Pembagian Bandwidth Menggunakan Mikrotik Di PT. Satria Jaya Prima (2023). Journal of Intelligent Networks and IoT Global, 1(1), 39-45.

[4] Haniyah, W., Hidayat, M. C., Putra, Z. F. I., Pertama, V. A., & Setiawan, A. (2024). A Simulasi Serangan Denial of Service (DoS) menggunakan Hping3 melalui Kali Linux. *Journal of Internet and Software Engineering*, *1*(2), 8-8.

[5] Haris, A. I., Riyanto, B., Surachman, F., & Ramadhan, A. A. (2022). Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi. *Komputika: Jurnal Sistem Komputer*, *11*(1), 67-76.

[6] Hidayat, S., Silvanie, A., ASISTYASARI, A., & Nuryaman, Y. (2023). OPTIMALISASI MANAJEMEN TRAFIK DAN KEAMANAN DATA PADA JARINGAN INTRANET IBI-K 1957 DENGAN METODE USER BEHAVIOUR ANALYSIS. JTIK (Jurnal Teknik Informatika Kaputama), 7(2), 315-316.

[7] Ilhamdi, Y., & Kunang, Y. N. (2021, November). Analisis Malware Pada Sistem Operasi Windows Menggunakan Teknik Forensik. In *Bina Darma Conference on Computer Science* (Vol. 3, pp. 256-264).

[8] Inggi, R., & Alam, H. P. (2023). Analisis Forensik Web Browser Pada Perangkat Android. *Simtek: jurnal sistem informasi dan teknik komputer*, *8*(1), 215-220.

[9] Kurniawan, D. (2020). Membasmi Virus Komputer dan Android. Elex Media Komputindo.

[10] Kusuma, G. H. A. (2021). Perancangan Skema Sistem Keamanan Jaringan Web Server menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19. *Journal of Informatics and Advanced Computing (JIAC)*, *2*(2), 1-4.

[11] Mudzakkar, M., Siaulhak, S., & Jumarniati, J. (2023). Analisis Deteksi Dan Pencegahan Eksploitasi Jaringan Brute Force Exploit Menggunakan Firewall Pada Kantor Bappeda Kota Palopo. SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan, 2(4), 1098-1099.

[12] Nursapdahi, N., Fitrani, A. S., Rosid, M. A., & Aji, S. (2022, August). Studi Analisa Serangan Sql Injection. In *Prosiding SEMNAS INOTEK (Seminar Nasional Inovasi Teknologi)* (Vol. 6, No. 1, pp. 185-190).

[13] Pratomo, A. B. (2023). Pengembangan Sistem Firewall Pada Jaringan Komputer Berbasis Mikrotik Routeros. *Bulletin of Network Engineer and Informatics*, *1*(2), 51-59.

[14] Purba, W. W., & Efendi, R. (2020). Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. *AITI*, *17*(2), 144-145.

[15] Purwanti, P. (2024). Visualisasi Data Cyber Security Attack Dengan Fitur Prediksi Serangan Dan Mitigasi Risiko: Perspektif Generative Gemini AI. *Jurnal Minfo Polgan*, *13*(2), 2340-2350.

[16] Ridho, M. A., & Arman, M. (2020). Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *9*(3), 373-379.

[17] Rosaly, R. (2019). Pengertian Flowchart Beserta Fungsi dan Simbol-simbol Flowchart yang Paling Umum Digunakan.

[18] Santoso, J. D. (2019). Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System. INFOS Journal-Information System Journal, 1(3), 44-50.

[19] Sari, R. D. I. P., Rahmah, A., Zuhroh, F., Hidayat, T. R. P., & Rakhmawati, N. A. (2023). Analisis Bibliometrik Mengenai Serangan Phishing Pada Media Sosial Menggunakan VosViewer. *Jurnal Ilmiah Informatika Komputer*, *28*(3), 230-240.

[20] Sedayu, A., & Harafani, H. (2022). Implementasi Managemen Bandwidth Mengunakan Metode Simple Queue Pada PT BPR Depo Mitra Mandiri: Mikrotik, Managemen Bandwith, Simple Queue. Jurnal Informatika Software dan Network (JISN), 3(1), 1-4

[21] Syafrizal, M. (2020). *Pengantar jaringan komputer*. Penerbit Andi.

[22] Wilujeng, C. K., & Voutama, A. (2024). IMPLEMENTASI FIREWALL FILTER RULES SEBAGAI FILTERING CONTENT PADA JARINGAN KOMPUTER MENGGUNAKAN MIKROTIK. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(3), 2680-2685.

[23] Zulkarnain, Z. (2020). Analisis keamanan ftp server menggunakan serangan man-in-the-middle attack. *Telcomatics*, *5*(1).

P-ISSN 1858-2680
E-ISSN 2723-4673