Methotika : Jurnal Ilmiah Teknik Informatika
e-ISSN : 2776 – 5792
Vol. 2, No.2 Oktober 2022, pp. 92-97
http://ojs.fikom-methodist.net/index.php/methotika

Analisis Dan Implementasi Penggunaan Firewall Raw Untuk Pengamanan dan Peningkatan Performansi Jaringan

Nehemia Cristiano Marbun[1], Naikson Fandier Saragih[2], Mufria Jonatan Purba[3]
[1,3]Fakultas Ilmu Komputer, Universitas Methodist Indonesia

Info Artikel

Histori Artikel:

Received, Sep 9, 2019
Revised, May 20, 2020
Accepted, Jun 11, 2020

Keywords:

Firewall Raw,
chain prerouting,
SYN FLood,
UDP Flood,
ICMP Flood,
TCP/IP

ABSTRAK

PT. RackH Lintas Asia perusahaan ISP yang terus mengupayakan lingkungan yang aman untuk jaringan komputernya. Kenyataannya masih ada gangguan keamanan router yang terhubung ke server. Firewall biasa masih berpeluang mengalami gangguan keamanan. Gangguan keamanan pada akhirnya juga akan berpengaruh pada performansi jaringan yang menurun. Implementasi dimulai dengan konfigurasi firewall raw pada chain prerouting dan output. Konfigurasi protocol pada tcp, udp, dan icmp, dan bagian action disetting drop. Selanjutnya ujicoba menggunakan data jenis serangan yang bersumber dari hasil wawancara dengan system engineer ditambah data sekunder yang bersumber dari studi literatur. Total seluruhnya uji coba sebanyak 14 serangan dalam satu minggu. Serangan menggunakan tools cmd dan hping3 untuk ping flood, LOIC dan hping3 untuk syn flood, LOIC dan hping3 untuk UDP Flood. Tools Torch dan Resource digunakan untuk melihat performansi berupa penggunaanmemory dan CPU pada saat diserang dan sebelum diserang. Wireshark digunakan untuk analisis packet data pada layer TCP/IP. Uji coba serangan berhasil dimana packet dibuang (drop) pada chain prerouting, demikian juga pada chain output. Hanya packet serangan UDP yang tidak terdeteksi pada chain output. Hasil Analisis berupa tahapan proses packet melalui tanpa penggunaan firewall raw dan menggunakan firewall raw. Demikian juga analisis untuk performansi. Analisis packet data pada layer TCP/IP sebelum dan sesudah diserang. Dengan menggunakan Firewall didapat peningkatan performance dari penggunaan CPU sebesar..% dan memory sebesar…%

Penulis Koresponden:

Naikson Fandier Saragih,
Fakultas Ilmu Komputer,
Universitas Methodist Indonesia, Medan,
Jl. Hang Tuah No.8, Medan - Sumatera Utara.
Email: naikson@naikson.com

1. PENDAHULUAN

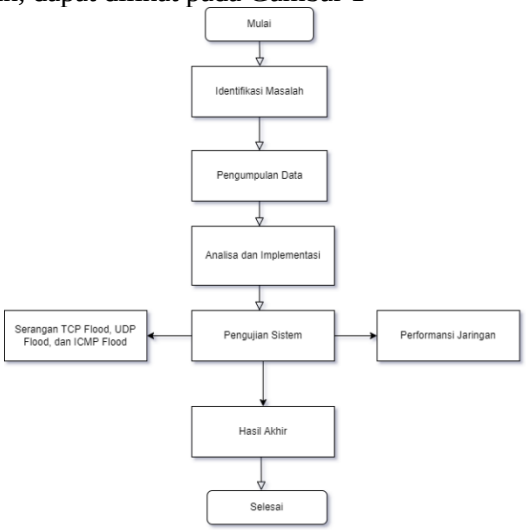
Keamanan jaringan internet merupakan unsur yang fundamental pada sebuah jaringan Internet untuk menjaga dan menjamin kerahasiaan data dan lainnya. Router merupakan salah satu perangkat yang sangat penting dalam sebuah jaringan komputer yang terhubung ke internet. Untuk jaringan Intranet akses router dimungkinkan dan tentunya pengamanannya menjadi sangat penting. Mikrotik Routerboard merupakan salah satu jenis router yang memiliki berbagai fitur yang lengkap dalam mendukung keamanan jaringan seperti *firewall*. *Firewall* akan memfilter data yang diterima dan melacak koneksi yang dibuat untuk menentukan data apakah koneksi tersebut diizinkan atau ditolak. *Firewall raw* merupakan fitur baru pada mikrotik yang memungkinkan untuk melewatkan atau mendrop suatu koneksi sebelum masuk ke proses *connection-tracking*, oleh karena itu maka penggunaan *firewall raw* bisa mengurangi beban *Central Processing Unit* (CPU) secara signifikan.

PT RackH Lintas Asia (RackH) hadir sebagai perusahaan IT terbaik yang fokus pada layanan Aplikasi, *Website Hosting* dan *Internet Service Provider* (ISP) yang sudah berpengalaman dan berkomitmen memberikan pelayanan terbaik kepada semua pelanggan.

Router adalah alat yang digunakan untuk mengirim paket data melalui suatu jaringan. Pada PT. RackH Lintas Asia router yang digunakan ialah Mikrotik RouterBoard. Serangan yang terjadi pada RouterBoard akan mengakibatkan router menjadi down sehingga keamanan jaringan menjadi terganggu. Pengamanan RouterBoard terhadap serangan merupakan hal yang sangat penting. Serangan jenis DDoS seperti SYN Flood, UDP Flood, dan ICMP Flood merupakan serangan yang sering menyerang router. Firewall raw digunakan untuk meningkatkan pengamanan router mikrotik sehingga serangan atau packet yang dicurigai akan di drop sehingga tidak akan mengganggu lalu lintas jaringan router

2. METODE PENELITIAN

Tahapan metode penelitian, dapat dilihat pada Gambar 1



Gambar 1. Tahapan Penelitian

1. Identifikasi masalah
   Identifikasi masalah meliputi keamanan mikrotik dan serangan pada router.
2. Pengumpulan data
   Metode pengumpulan data menggunakan wawancara dan studi literatur
3. Analisis dan Implementasi Sistem
   a. Analisis dilakukan untuk mengetahui proses *filtering firewall* (*Filter rules*, NAT, *Mangle*, dan *Raw*). *Torch* dan *Wireshark* akan digunakan untuk melihat packet data yang masuk pada setiap serangan yang berkaitan dengan *Firewall Filtering* khususnya *Firewall Raw*.
   b. Perancangan dilakukan untuk melakukan konfigurasi *Firewall Raw* dan melakukan perancangan terhadap serangan dan pengamanan yang akan dilakukan.
   c. Implementasi sistem akan dilakukan berdasarkan hasil analisa data dan perancangan yang sudah dilakukan sebelumnya. Tahap implementasi ini akan dilakukan terhadap *firewall raw* pada *router* mikrotik.
4. Pengujian Sistem
   Pengujian ini dilakukan terhadap proses hasil dari konfigurasi *firewall raw* dengan menguji serangan berdasarkan skenario serangan.
5. Dokumentasi
   Membuat dokumentasi sistem dari tahap awal sampai tahap akhir dari pengujian sistem, dan membuat dalam bentuk format penelitian.

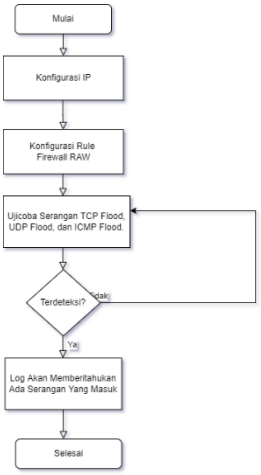
Skema serangan yang digunakan dalam pengujian ini adalah menggunakan kerangka kerja Hping3 pada sistem operasi Kali Linux. Seperti yang dijelaskan pada tabel di bawah ini. Serangan yang akan diujikan adalah jenis *DDoS* yaitu *TCP Flooding*, *UDP Flooding*, dan *ICMP Flooding*. Serangan akan dilakukan menggunakan *Software* dan *Tools* sesuai dengan serangan yang akan di uji coba. Dalam proses

ini *Aplikasi* dan *tools* akan meluncurkan serangan Syn *Flood*, UDP *Flood*, dan *Ping of Death* langsung ke jaringan target *Router* yang diserang. Dengan memasukkan IP target dan *port* yang akan diserang. Jika serangan berhasil menembus sistem keamanan pada router maka serangan berhasil dilakukan. Jika tidak kemudian ulangi proses yang sama dengan memasukkan alamat ip dan *port* target yang akan diserang, dapat dilihat pada Tabel 1.

Tabel 1. Tabel Serangan

Jenis Serangan	Aplikasi dan Tools	IP Tujuan	Port	Keterangan
SYN *Attack*	LOIC dan Hping3	10.100.10.1	80	Serangan SYN Attack berhasil masuk dan mengakibatkan CPU Load pada router mencapai 100%
UDP *Attack*	LOIC dan Hping3	10.100.10.1	80	Serangan UDP Attack berhasil masuk dan membuat CPU Load menjadi 99%
Ping of Death	CMD dan Hping3	10.100.10.1	80	Serangan Ping of Death Attack berhasil masuk dan membuat CPU Load menjadi 75%

Skenario penanganan terhadap serangan yang dilakukan yaitu dengan menggunakan *Firewall Raw* sebagai sistem keamanan yang diterapkan dalam melakukan pencegahan terjadinya serangan *Syn Flood*, *UDP Flood*, dan *ICMP Flood*. *Firewall Raw* akan memeriksa data yang diterima dan melacak koneksi tersebut diizinkan atau ditolak. Data yang ditolak adalah data yang dikirimkan *port* yang telah diblokir aksesnya oleh *Firewall Raw*. *Firewall raw* akan memblokir alamat IP. Data yang diizinkan masuk kedalam jaringan yaitu data yang dikirimkan oleh *port* yang tidak diblokir oleh *Firewall Raw*, dapat dilihat pada Gambar 2.



Gambar 2. Skenario Penanganan

3. HASIL DAN PEMBAHASAN

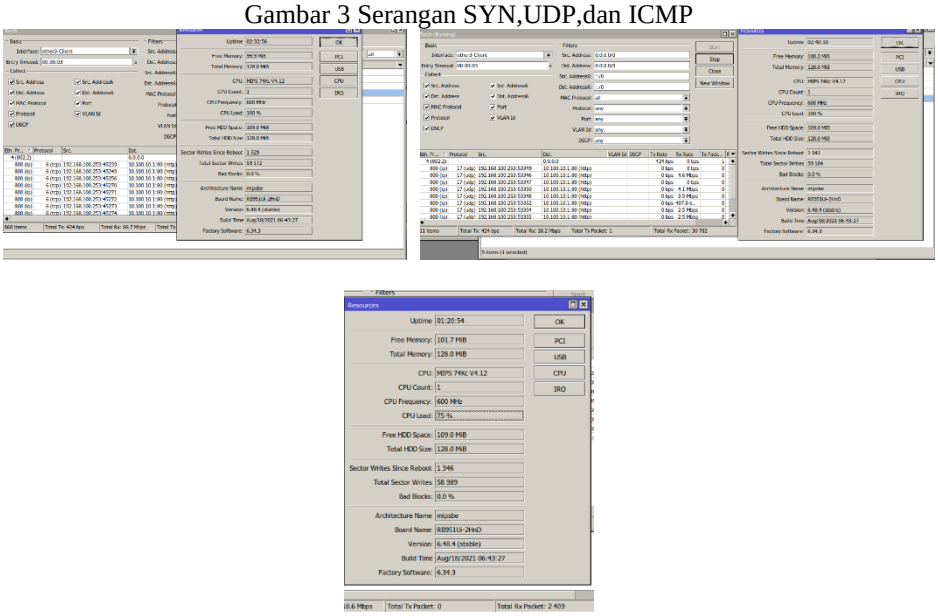
Skema Konfigurasi Firewall Raw, Chain prerouting,Protocol TCP, dapat dilihat pada Tabel 2.

Tabel 2. Skema

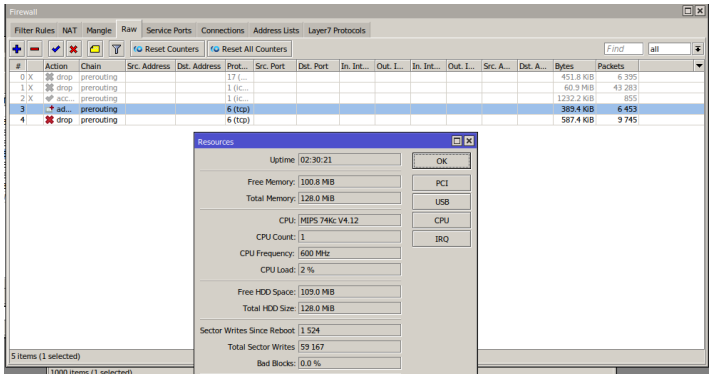
Serangan	Chain	Protocol	Action
SYN Attack	Prerouting	TCP	Drop
UDP Attack	Prerouting	UDP	Drop
Ping of Death	Prerouting	ICMP	Drop

Untuk memulai serangan, pada IP target isi dengan IP router yang sudah dikonfigurasi diatas sebelumnya. Method penyerangan ialah *TCP* dan *UDP* karena akan menguji serangan *SYN Attack* dan *UDP Attack*. Dan *Script CMD* untuk melakukan serangan ICMP *Flood*/atur untuk kecepatan packet yang akan diserang. Kemudian tekan IMMA CHARGIN MAH LAZER untuk memulai serangan, dapat dilihat pada Gambar 3, Gambar 4, Gambar 5, Gambar 6, Gambar 7.

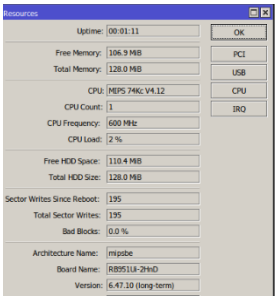
Gambar 3 Serangan SYN,UDP,dan ICMP



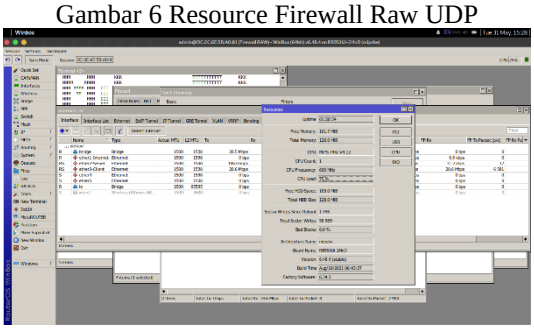
Gambar 4. Resource Ketika Diserang SYN Attack, UDP Attack,dan Ping of Death



Gambar 5. Resouce Firewall Raw SYN



Gambar 6 Resource Firewall Raw UDP



Gambar 7 Resource Firewall Raw ICMP

Berdasarkan hasil pengujian yang sudah dilakukan dengan menguji serangan SYN Attack, UDP Attack, dan Ping of Death, maka hasil penelitian tersebut akan disajikan menggunakan tabel sesuai dengan proses yang sudah dilakukan, dapat dilihat pada Tabel 3, Tabel 4, Tabel 5.

Tabel 3. Hasil Analisa Serangan SYN

No	Analisa	Keterangan
1.	Serangan SYN *Attack* pada router menggunakan *Softwar*e LOIC dan *tools* hping3.	Serangan berhasil masuk melalui IP target.
2.	*Protocol* Serangan yang berhasil masuk	TCP
3.	Kondisi sebelum diserang SYN *Attack*	CPU *Load* 2%, m*emory* 106.9 MiB
4.	*IP Address* penyerang *IP Address* target	192.168.100.253 10.100.10.1
5.	Kondisi setelah diserang SYN *Attack*	CPU *Load* 100%, m*emory* 99 MiB
6.	*Packet* yang di *drop* oleh *chain prerouting*	*Bytes* : 389.4 KiB *Packet* : 6453
7.	*Packet* yang di *drop* oleh *chain output*	*Bytes* : 13.4 MiB *Packet* : 352.572
8.	Keamanan Router Mikrotik	*Firewall Raw*
9.	*Log Activity*	Terdapat serangan SYN yang masuk dan di *drop* oleh *Firewall Raw*
10.	Kondisi CPU setelah menggunakan *Firewall Raw*	CPU *Load* 1%, m*emory* 100.8 MiB

Tabel 4. Hasil Analisa Serangan UDP

No	Analisa	Keterangan
1.	Serangan UDP *Attack* pada router menggunakan *Software* LOIC dan *tools* hping3.	Serangan berhasil masuk melalui IP target.
2.	Protocol Serangan yang berhasil masuk	UDP
3.	Kondisi sebelum diserang UDP *Attack*	CPU *Load* 5%, *memory* 104.3 MiB
4.	*IP Address* penyerang *IP Address* target	192.168.100.253 10.100.10.1
5.	Kondisi setelah diserang UDP *Attack*	CPU *Load* 100%, *memory* 100.2 MiB
6.	*Packet* yang di *drop* oleh *chain prerouting*	*Bytes* :190.7 kib *Packet* : 2369
6.	Keamanan Router Mikrotik	*Firewall Raw*
7.	*Log Activity*	Terdapat serangan UDP yang masuk dan didrop oleh *Firewall Raw*
8.	Kondisi CPU setelah menggunakan *Firewall Raw*	CPU *Load* 2%, *memory* 106.9 MiB

Tabel Analisa Ping of Death

No	Analisa	Keterangan
1.	Serangan ICMP *Flood* pada router menggunakan *Tools CMD* dan hping3.	Serangan berhasil masuk melalui IP target.
2.	*Protocol* Serangan yang berhasil masuk	ICMP
3.	Kondisi sebelum diserang ICMP *Flood*	CPU *Load* 3%, *memory* 101.7 MiB
4.	*IP Address* penyerang *IP Address* target	192.168.100.253 10.100.10.1
5.	Kondisi setelah diserang UDP *Flood*	CPU *Load* 75%, *memory* 105.2 MiB
6.	*Packet* yang di *drop* oleh *chain prerouting*	*Bytes* : 69.0 MiB *Packet* : 43 269
7.	*Packet* yang di *drop* oleh *chain output*	*Bytes* : 26.7 MiB *Packet* : 997 738
8.	Keamanan Router Mikrotik	*Firewall Raw*
9.	*Log Activity*	Terdapat serangan ICMP yang masuk dan didrop oleh *Firewall Raw*
10.	Kondisi CPU setelah menggunakan *Firewall Raw*	CPU *Load* 2%, *memory* 101.4 MiB

4. KESIMPULAN

Hasil analisis dan implementasi serta pengujian pada sistem yang sedang berjalan, penulis dapat memberikan kesimpulan sebagai berikut:

1. Tanpa adanya *Firewall* Raw, serangan DDoS seperti *TCP Flood*, *UDP Flood*, dan *ICMP Flood* dapat menembus router sehingga membuat router down dan membuat *CPU Load* pada router meningkat sampai 100%.
2. Saat *Firewall Raw* sudah diimplementasikan pada router, Serangan DDoS seperti *TCP Flood*, *UDP Flood*, dan *ICMP Flood* tidak dapat menembus router yang membuat *CPU Load* menjadi meningkat sampai 100% dan membuat router menjadi down.

REFERENSI

[1] Haris, Arief Indriarto, Budhi Riyanto, Farry Surachman, and Ardito Adi Ramadhan. "Analisis Pengamanan Jaringan Menggunakan Router Mikrotik Dari Serangan DoS Dan Pengaruhnya Terhadap Performansi." *Komputika : Jurnal Sistem Komputer* 11, no. 1 (2022): 67–76. https://doi.org/10.34010/komputika.v11i1.5227.

[2] Haeruddin, Haeruddin. "Analisa Dan Implementasi Sistem Keamanan Router Mikrotik Dari Serangan Winbox Exploitation, Brute-Force, DoS." Jurnal Media Informatika Budidarma 5, no. 3 (2021): 848. https://doi.org/10.30865/mib.v5i3.2979.

[3] Muhammad Abdul Muin, Bambang Sugiantoro. "IMPLEMENTASI FIREWALL DENGAN MENGGUNAKAN MIKROTIK ROUTEROSTM (Studi Kasus : STMIK Bina Patria)." Jurnal Transformasi 13, no. 1 (2017): 58–61.

[4] Jaya, Budi, Y Yuhandri, and S Sumijan. "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS)." Jurnal Sistim Informasi Dan Teknologi 2 (2020): 115–23. https://doi.org/10.37034/jsisfotek.v2i4.32.

[5] Riyadi, Valens. "Router Optimation with Firewall/Raw." Www.Mum.Mikrotik.Com, 2017. http://mikrotik.co.id/artikel_lihat.php?id=150.

[6] Kurniati, Rezki, Jaroji. "Seminar Nasional Industri Dan Teknologi (SNIT), Politeknik Negeri Bengkalis." Perancangan Aplikasi Antrian Pasien Di Rumah Sakit Menggunakan Metode Fast, no. Lcm (2019): 270–76.

[7] Irfan, Zumardi. Implementasi Keamanan Jaringan Berbasis Firewall Raw Terhadap Brute Force Login Cyber Attack, 2020.

[8] Triyana, Norma, and Adrian Eka. "Analisis Dns Amplification Attack." Jurnal of Education and Information Communication Technology 1, no. 1 (2017): 17–22.