PEMANFAATAN MIKROTIK ROUTERBOARD SEBAGAI KEAMANAN JARINGAN DARI *UDP FLOOD* DENGAN MENGGUNAKAN *FIREWALL* DI DINAS PENDIDIKAN BENGKALIS

Baytar Jagad Georaga Putra[1], Tengku Musri,M.Kom[2], Lipantri Mashur Gultom, M.Kom[3]
Program Studi Teknik Informatika, Politeknik Negeri Bengkalis, Riau, Indonesia
baytar.jagad@gmail.com[1], musri@polbeng.ac.id[2], Lipantri@polbeng.ac.id[3]

Abstract

The use of Mikrotik routerboard as network security from UDP flood using firewall filtering is expected to help in network security, especially in the Bengkalis education office, considering that attacks on security systems can occur anywhere which will certainly be very detrimental and the type of attack that often occurs is DOS Services). The DOS (Denial Of Service) attack is an attack that is being talked about in today's research world. And in general, research on this attack is focused on 2 things, namely the detection or prevention of DOS attacks that can occur in any type of network, so research is needed to find how to detect these attacks. In this advanced, DOS Attacks have developed into distributed attacks which are commonly called DDOS (Distributed Denial Of Services). And of the types of DDOS attacks that exist, a UDP-Flooding attack is a type of attack that can cause a significant effect on a router. UDP (User Datagram Protocol) Flooding is a type of attack that takes advantage of the UDP protocol by reducing the connection (connectionless) to attack the target. Flooding attacks can be overcome in various ways, especially on proxy router devices, one of which is by filtering on firewalls.
Keywords : firewall, keamanan jaringan, mikrotik,udp flood

1. PENDAHULUAN

Perkembangan teknologi dan komunikasi sangat pesat pada saat ini, Seiring dengan berkembangnya kemajuan teknologi khususnya di bidang informasi, maka peranan computer dan internet sangatlah penting bagi setiap orang dan juga untuk instansi pemerintahan dan pendidikan. Selain memiliki banyak keuntungan, internet juga memiliki kekurangan. Salah satu kekurangan dari internet yaitu pada sisi keamanan jaringan. Serangan terhadap sistem keamanan bisa terjadi di manapun yang pastinya akan sangat merugikan dan Jenis serangan yang kerap terjadi adalah DOS (*Denial of Services*). Serangan DOS (Denial Of Service) merupakan sebuah serangan yang sedang ramai dibicarakan di dunia penelitian saat ini, Di zaman yang maju ini, Serangan DOS sudah berkembang menjadi serangan yang terdistribusi yang biasa disebut DDOS (Distributed Denial Of Services). Dari jenis-jenis serangan DDOS yang ada, serangan *UDP-Flooding* adalah jenis serangan yang dapat menyebabkan efek yang signifikan pada sebuah router. UDP (*User Datagram Protocol*) *Flooding* adalah jenis serangan yang memanfaatkan protokol UDP dengan mengurangi sambungan (*connectionless*) untuk menyerang target seperti instansi dinas pendidikan. Hal ini mendorong peneliti untuk mempermudah dalam mengatasi serangan *Udp Flood* dengan memanfaatkan routerboad mikrotik.

Berdasarkan latar belakang di atas, pada penelitian ini diusulkan sebuah sistem keamanan dengan menggunakan routerboard dan memanfaatkan fitur *firewall* pada jaringan dinas pendidikan Bengkalis.

Tujuan dari pembuatan tugas akhir ini adalah membuat keamanan jaringan menggunakan routerboard mikrotik dengan mengoptimalkan fitur – fitur *firewall* pada mikrotik dan membuat keamanan jaringan dari serangan *UDP Flood* dengan filter firewall

Adapun manfaat dari pembuatan keamanan jaringan dengan menggunakan mikrotik routerboad dan memanfaatkan fitur *firewall* adalah Membantu dalam mengamankan jaringan di dinas pendidikan Bengkalis Menambah keamanan jaringan dengan optimalisasi routerboard MikroTik dan Meningkatkan perlindungan pada jaringan internet di dinas pendidikan Bengkalis serta untuk Mengetahui kerentanan keamanan informasi akibat serangan DoS dan DDoS pada router dinas pendidikan Bengkalis

2. TINJAUAN PUSTAKA

a. Aprilianto, Fadila, & Muslim, (2019) dengan judul ”Sistem Pencegahan UDP DNS Flood Dengan Filter Firewall Pada Router Mikrotik” menjelaskan bahwa *firewall* yang dikonfigurasi dalam sistem mikrotik memeriksa data yang diterima dan melacak koneksi tersebut diijinkan atau ditolak. Penggunaan *Firewall* digunakan untuk menyaring user yang terkoneksi dan melakukan penghalangan akses dari user yang diblokir.

b. Abriansya Putra,Tamsir Ariyadi, (2019) dengan judul “Implementasi Pencegahan Terhadap Serangan Flooding Attack TCP dan UDP di Kantor PDAM Tirta Musi Palembang” menjelaskan bahwa *Flooding* adalah sejenis serangan *Denial of Service* (DOS), dimana *flooding* melakukan serangan terhadap sebuah komputer atau *server* di dalam jaringan lokal maupun internet dengan cara menghabiskan sumber *(resource)* yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehinnga secara tidak langsung mecegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

c. I Gusti Komang Oka Mardiyana (2015), MikroTik Router adalah salah satu sistem operasi yang dapat digunakan sebagai router jaringan yang handal, mencakup berbagai fitur lengkap untuk jaringan dan wireless. Selain itu MikroTik dapat juga berfungsi sebagai *firewall*. Melalui penelitian ini dengan judul “Keamanan Jaringan Dengan *Firewall* Filter Berbasis Mikrotik Pada Laboratorium Komputer STIKOM Bali” akan dibahas bagaimana merancang jaringan komputer dengan menerapkan konsep *firewall* berbasis Miktorik dengan tujuan dapat mengurangi resiko ancaman yang akan mengganggu aktifitas yang yang sedang berlangsung, disesuaikan dengan kondisi tempat penelitian yaitu pada Laboratorium Komputer STIKOM Bali.

d. Imam Solikin (2017), Mikrotik dikenal sebagai router dimana dapat berupa sistem operasi atau perangkat (*routerboard*) yang memiliki fitur-fitur yang sangat lengkap dalam memanajemen sistem keamanan jaringan.Dengan penerapan mikrotik pada jaringan SMK Negeri 1 Indralaya Utara diharapkan dapat memiliki sistem keamanan jaringan yang tidak rentan terhadap berbagai bentuk gangguan atau serangan baik dalam jaringan *local* maupun dari jaringan internet.Kutipan yang berasal dari internet dituliskan dengan menyebutkan nama dan tahun. Jika tidak ada namanya, ditulis alamat websitenya.

e. Feby Ardianto (2016), *Mikrotik* merupakan sistem operasi *router*, yang di-*rilease* dengan nama *mikrotik router Os* yang mampu diinstall pada komputer biasa, tidak seperti sistem operasi *router* lainya yang hanya bisa *diinstall* pada *hardware* tertentu. Mudah dikonfigurasi dan tentunya harganya yang murah. Serta berfungsikan untuk membagi-bagi koneksi internet ke beberapa computer pengguna *user.*

3. METODE PENELITIAN

3.1 Bahan dan Alat Penelitian

Tujuan dari pembuatan pemanfaatan mikrotik routerboard sebagai keamanan jaringan dari *udp flood* menggunakan *filter firewall* di dinas pendidikan Bengkalis adalah untuk mengoptimalkan keamanan jaringan pada dari serangan *udp flood* yang bisa menggangu kinerja jaringan pada dinas pendidikan dan demi mewujudkan semua itu membutuhkan beberapa perangkat yang bisa mendukung. Beberapa hal yang perlu diperhatikan dalam melakukan keamanan jaringan antara lain :

3.1.1. Bahan

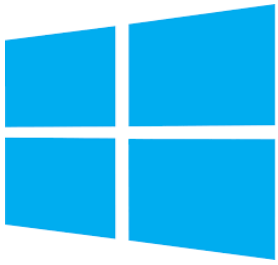
Data yang digunakan dalam melakukan pemanfaatan mikrotik routerboard sebagai keamanan jaringan dari *UDP flood* menggunakan *filter firewall* di dinas pendidikan Bengkalis yaitu berupa data-data mengenai dinas pendidikan seperti data keuangan dan data kepegawaian yang ada pada server dinas pendidikan Bengkalis.

3.1.2. Peralatan *Software*

1. Winbox

Gambar 1. Logo Winbox

2. Microsoft Windows 10



Gambar 2. Logo Windows 10

3. Aplikasi Loic

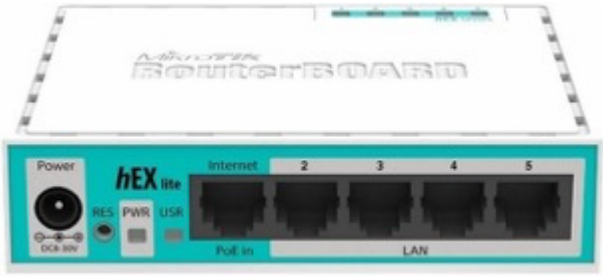
Gambar 3. Tampilan Aplikasi Loic

3.1.3. Peralatan *Hardware*

1. Laptop

Gambar 4. Laptop

2. Routerboard Mikrotik



Gambar 5. Mikrotik Routerboard

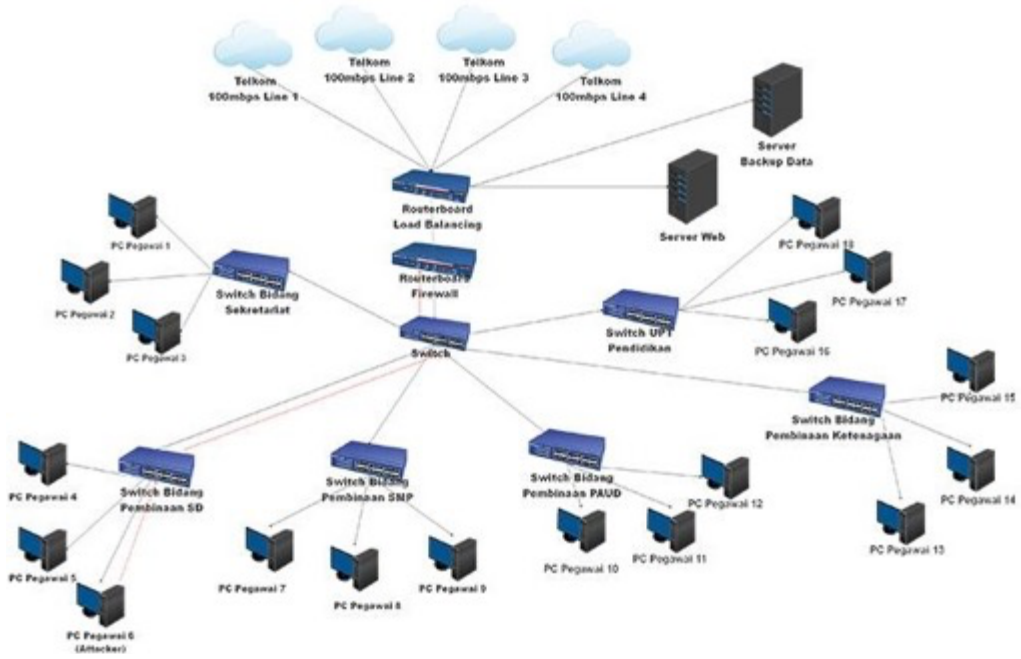
3. Kabel UTP

Gambar 6. Kabel UTP

3.2. Perancangan Sistem

3.2.1 Perancangan sistem yang berjalan

Adapun Topologi yang akan dibuat dalam perancangan dan digunakan untuk kelancaran dalam penyelesaian laporan tugas akhir sebagai berikut:

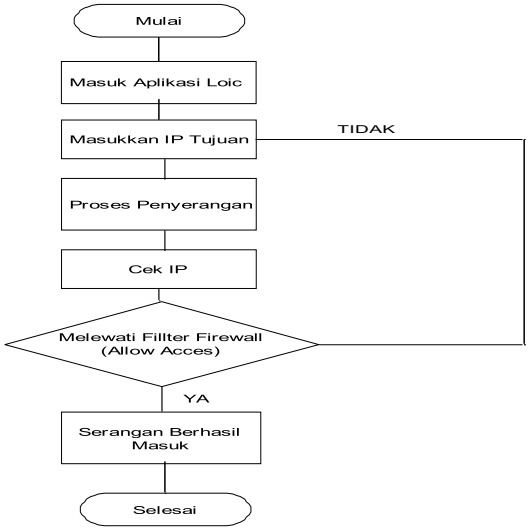


Gambar 8. Topologi

Pada konsep penyerangan *UDP flood* akan dilakukan oleh PC6 menggunakan aplikasi *UDP flooder* untuk melakukan serangan *UDP flood* yang di mana akan membanjirkan router dengan udp yang menyebabkan gangguan pada router yang bisa berdampak pada kinerja jaringan di dinas pendidikan Bengkalis. Fungsi router firewall di sini adalah untuk mengatasi serangan *UDP flood* Dengan menggunakan filter rules yang telah dibuat, setelah membuat filter rules packet yang melalui port DNS selain IP Address yang telah di *allow* jika mencoba untuk melakukan request atau *flood* DNS ke IP Public pada router mikrotik, maka packet tersebut akan langsung di drop oleh pengaturan rules tersebut.

3.2.3 Skema Penyerangan

Pada skema penyerangan penulis menjelaskan skema dalam melakukan penyerangan, yang dimana disini menjelaskan bagaimana penyerang atau *attacker* melakukan serangan kepada router dengan menggunakan aplikasi Loic. Dan dalam perancangan penulis akan menampilkan skema penyerangan dalam bentuk flowchart. Adapun flowchart yang digunakan sebagai skema penyerangan adalah sebagai berikut:



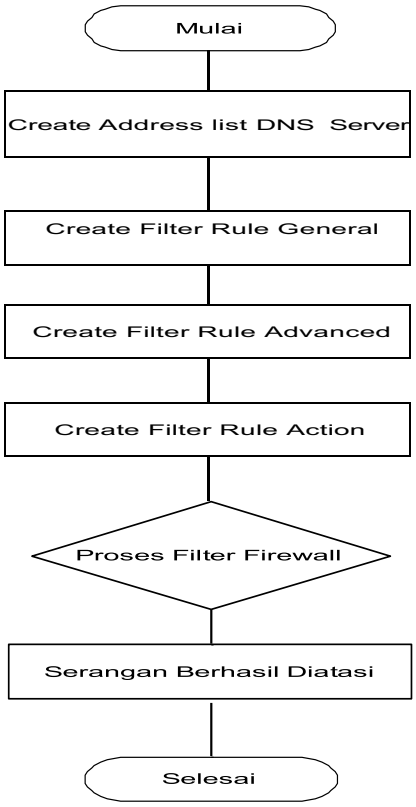
Gambar 9. Flowchart

cara yang dilakukan *attacker* untuk melakukan serangan *udp flood* tersebut meliputi beberapa tahap yang dimana *attacker* tersebut menggunakan aplikasi Loic untuk melakukan serangan *udp flood* terhadap router dinas pendidikan Bengkalis dan setelah mendapatkan IP dari router dinas pendidikan Bengkalis *attacker* tersebut tinggal memasukkan IP dari router ke dalam aplikasi dan melakukan *flooding* dan apabila serangan atau *flooding* menembus *filter firewall* maka *attacker* berhasil dalam melakukan serangan *udp flood* dan jika serangan tidak berhasil maka sang *attacker* harus memulai dari memasukkan IP lagi.

3.2.2 Skema Penangganan

Pada skema penannganan penulis akan menjelaskan bagaimana dalam melakukan penangganan dari serangan *udp flood,* pada tahap ini penulis menggunakan flowchart sebagai skema adapun flowchart sebagai berikut:

Flowchart



Gambar 10, Flowchart Penangganan *Udp Flood*

Pada flowchart ini dapat dijelaskan proses penangganan serangan *UDP flood* di dinas pendidikan Bengkalis dalam bentuk flowchart, dan pada flowchart ini dapat dijelaskan tentang proses penangganan yang akan di lakukan pada tool *firewall* yang meliputi setting pada address list DNS server yang diizinkan dan setellah tinggal melakukan create filter rule general> filter rule advanced> filter rule action.jika semua setting sudah dilakukan tahap yang harus dilakukan selanjutnya adalah proses uji coba serangan pada router *firewall,* dan untuk mengetahui serangan berhasil diatasi kita bisa melihat pada firewall > connection untuk melihat apakah ada serangan *UDP flood* yang masuk atau kita bisa melihat traffic pada interface ether2-Lan jika Tx Packet pada traffic turun maka serangan *UDP flood* sudah berhasil di filter oleh *firewall.*

4. HASIL PENELITIAN DAN PEMBAHASAN

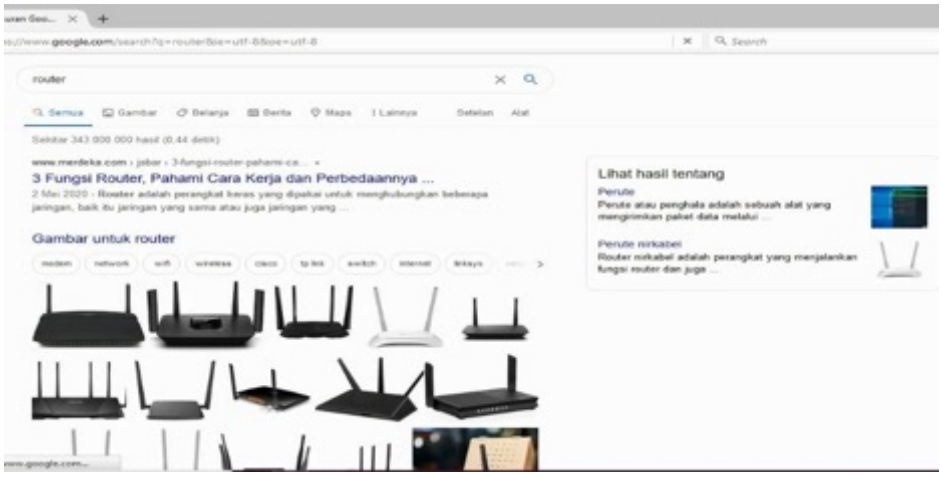
a. Konfigurasi pada router

Hal pertama yang dilakukan penulis pada tahap mengamankan jaringan dari serangan *udp flood* adalah mengumpulkan dan memasang seluruh *hardware* yang di perlukan dan memulai proses pengamanan jaringan dari serangan *udp flood.* Langkah yang harus dilakukan yaitu dengan melakukan konfigurasi pada router dengan menggunakan aplikasi winbox supaya bisa terkoneksi ke internet serta tidak lupa menerapkan rancangan flowchart dan activiti diagram yang sudah di rancang sebelumnya

Pada proses ini menampilkan hasil ketika sudah berhasil melakukan konfigurasi pada router yang dimana ketika sudah berhasil kita sebagai pengguna bisa mendapatkan akses internet

Gambar 11. Tampilan Ketika Sudah Berhasil konfigurasi router

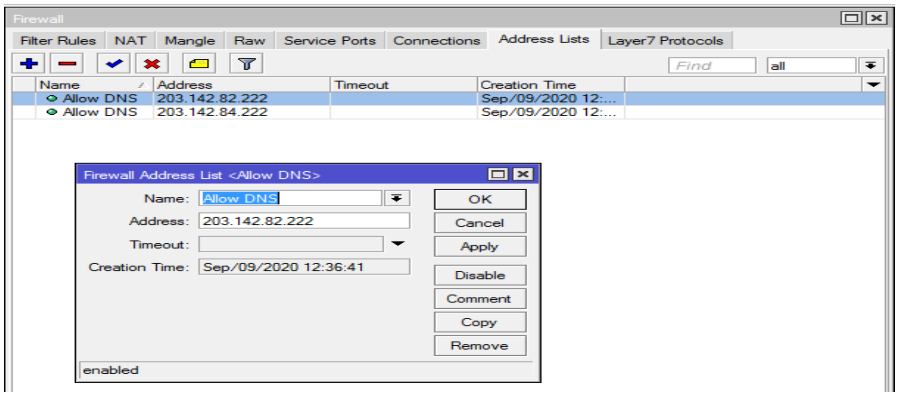
Hasilnya



Gambar 12. Tampilan Pada Mozila Firefox

a. Create address list DNS server

Pada tahap kali ini penulis menerapkan skema penangganan dari serangan *udp flood* dengan melakukan setting pada router dan melakukan proses create address list DNS server berfungsi untuk memberikan akses IP address yang dizinkan

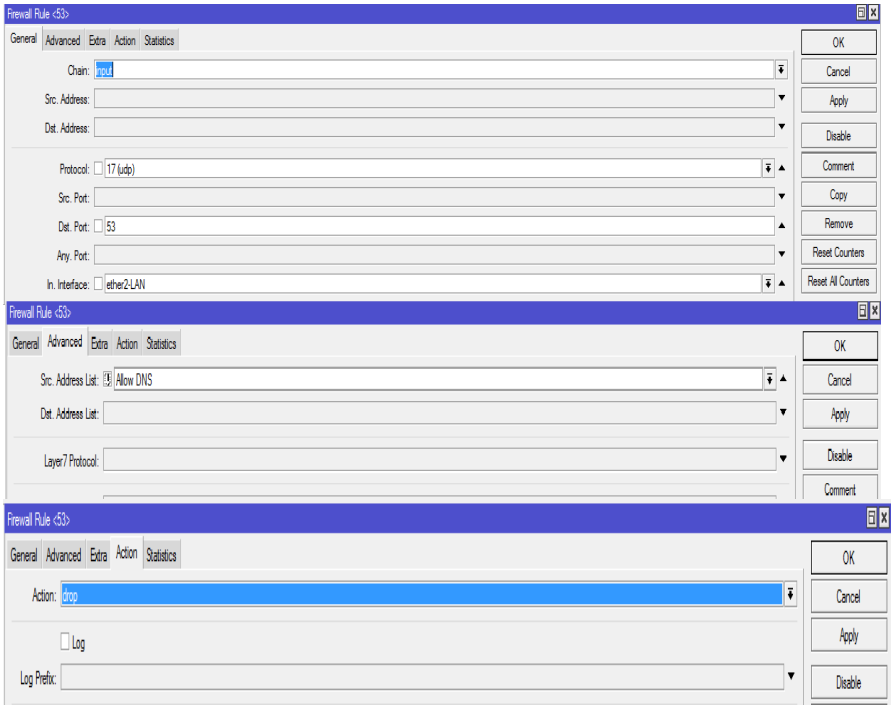


Gambar 13. Tampilan Create address list DNS server

Pada tahap ini penulis melakukan proses create address list DNS server yang nantinya akan berfungsi untuk memberi hak akses kepada client yang diizinkan. Kemudian masukkan alamat IP address DNS server yang diizinkan dalam penggunaan nantinya

b. Create Filter Rules firewall

Pada proses ini penulis menerapkan skema penanagganan dengan melakukan create filter rule pada menu firewall mikrotik routerboard menggunakan winbox yang nantinya akan berfungsi sebagai pemblock packet DNS yang bukan berasal dari DNS yang sudah di allow.



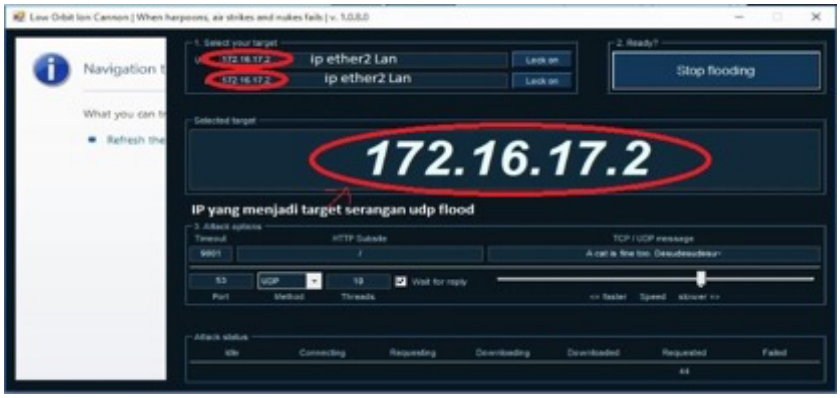
Gambar 14. Tampilan Create filter rule firewall

c. Pengujian penyerangan

Untuk mengetahui tingkat keberhasilan dari pemanfaatan mikrotik routerboard sebagai keamanan jaringan dari *udp flood* dengan menggunakan *firewall* di dinas pendidikan Bengkalis, pada proses pengujian ini peneliti akan melakukan sebuah uji coba serangan menggunakan aplikasi Loic untuk melakukan serangan kepada router yang sudah di setting *firewall* yang dimana jika

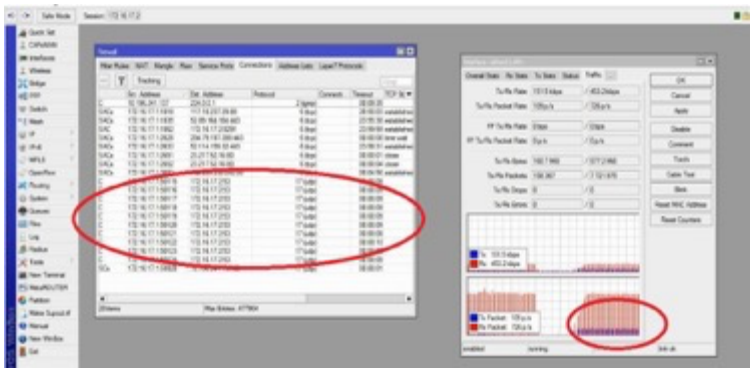
serangan nya tembus maka pengujian nya gagal dan jika berhasil maka serangan sebelum akan terhenti dan traffic pada Tx Packet juga akan menurun yang menandakan serangan berhasil diatasi. Adapaun proses sebelum dan sesudah penggunaan filter firewall bisa dilihat sebagai berikut:

Tampilan proses penyerangan pada aplikasi Loic:



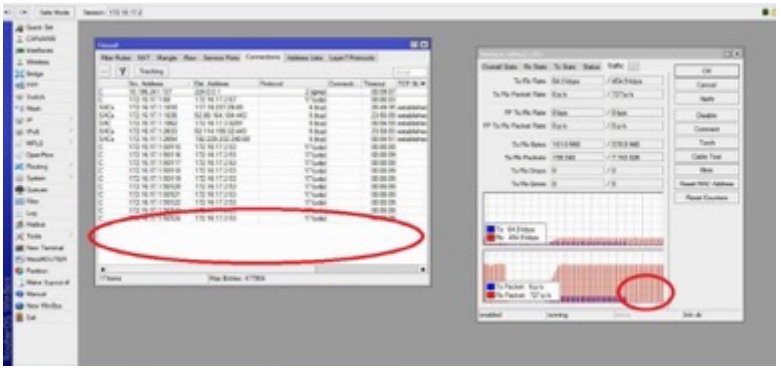
Gambar 15. Tampilan Proses Penyerangan pada aplikasi Loic

Tampilan sebelum filter *firewall*



Gambar 16. Tampilan Sebelum Di filter firewall

Tampilan sesudah filter *firewall*



Gambar 17. Tampilan Sesudah Di filter firewall

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan dari penelitian ini bahwa routerboard ini bisa mengamankan jaringan dari serangan *udp flood* menggunakan *firewall* dengan baik. Dan pemanfaatan routerboard ini juga sudah mencapai tujuan yaitu Menambah keamanan jaringan dengan optimalisasi routerboard MikroTik, membantu dalam mengamankan jaringan di dinas pendidikan Bengkalis dan meningkatkan perlindungan pada jaringan internet dinas pendidikan Bengkalis.

5.2 Saran

Adapun saran dari penulis mengenai pemanfaatan mikrotik routerboard sebagai keamanan jaringan dari *udp flood* dengan menngunakan *firewall* di dinas pendidikan Bengkalis adalah sebagai berikut :

1. Dari penelitian ini hanya bisa digunakan untuk dinas pendidikan saja. Kedepan nya diharapkan dapat dikembangkan supaya bisa digunakan di dinas lain.
2. Dari penelitian ini Bengkalis routerboard ini hanya bisa mengatasi serangan dari *udp flood* kedepannya diharapkan bisa mengatasi dari serangan yang berbeda.
3. Dari penelitian ini hanya melakukan pengujian dengan satu aplikasi penyerangan diharapkan kedepan nya bisa melakukan pengujian dengan aplikasi DDoS yang lain.

6. DAFTAR PUSTAKA

Doni Aprilianto, Triyana Fadila, dan Much Aziz Muslim (2017),Sistem Pencegahan UDP DNS Flood dengan Filter Firewall pada Router Mikrotik,. *Jurnal Techno.COM, Vol. 16, No. 2, Mei 2017*

Sugiyono (2016) "Sistem Keamanan Jaringan Komputer Menggunakan Metode Watchguard Firebox Pada PT Guna Karya Indonesia". *Jurnal CKI On SPOT, Vol. 9, No. 1, JUNI 2016* Amarudin dan Faruk Ulum, (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. *Jurnal TEKNOINFO, Vol. 12, No. 2, 2018, 72-75, ISSN 2615-224X.*

Fajar Akbar, Susafa'ati dan Musriatun Napiah. (2019) Metode *Point to Point Tunneling Protocol* Untuk Keamanan Jaringan Studi Kasus Kantor Walikota Administrasi Jakarta Barat. *Jurnal Infortech.*

Dini Nur Apriliani, Mega Ayu Sasmita dan Aisyah Trisna Windari, (2017). Pencegahan Flooding Pada Jaringan Komputer Mnggunakan Metode Blokir IP dan Port, Snort dan Wireshark. *JOEICT (Jurnal Of Education and Information Communication Technologi) Volume 1, Nomor 1, Bulan 2017: 6 – 16*

Realize dan Uni Hananti, (2017). Pengaruh Penggunaan *IPTable Firewall* dan ACID Terhadap Keamanan Jaringan. *Jurnal EdikInformatika*

Efrahim Sinyo Rio Ola Balen Langobelen, Catur Iswahyudi dan Rr. Yuliana Rachmawati, (2019). Ananlisis dan Optimalisasi dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus di Taman Pintar Yogyakarta. *Jurnal JARKOM Vol. 7 No. 2 Desember 2019*

Alva S. M. Tumigolung, Arie S. M. Lumenta dan Arthur M. Rumagit, (2015).Perancangan Sistem Pencegahan *Flooding* Data Pada Jaringan Komputer. *E-Journal Teknik Elektro dan Komputer (2015), ISSN : 2301-8402*

Irwan Tanu Kusnadi, (2018) Pengamanan Jaringan Komputer Dengan VPN, *Firewall*, IDS dan IPS. *Jurnal Informatika ISSN : 2301-7953*

Achmad Hambali dan Siti Nurniati, (2018) Implementasi Instrusion Detection System (IDS) Pada Keamanan PC Server Terhadap Serangan Flooding Data. *Jurnal Sainstech Vol. 28 No. 1, Januari 2018.*