ANALISIS SERANGAN *FLOODING* DATA PADA *ROUTER* MIKROTIK

Ade Hendri Hendrawan, S.Kom., M.Kom.[1)]
[1)] Universitas Ibn Khaldun Bogor
hendri@ft.uika-bogor.ac.id

Abstrak- Media I*nternet* Sudah Bagian Dari Kehidupan Dalam Keperluan Komunikasi Dimana Dalam Penggunaan Dari Kemajuan Teknologi, Semakin Banyak Nya Penguna bisa berdampak timbul permasalahan diantaranya gangguan berupa paket yang mengarah ke Server jaringan komputer dan dapat terjadi kapan saja. Seorang dalam bertugas sebagai administrator. Perlu menganalisa langsung apakah setiap konten yang masuk tersebut adalah data yang diharapkan ataupun data yang tidak diinginkan. Kalau paket tersebut merupakan data yang tidak diinginkan, komputer bisa mengamil alih tindakan dengan melakulan blok IP asal paket. Pemodelan suatu sistem yang digunakan untuk mengatasi flooding data pada suatu jaringan. Sistem dibuat dengan jalan membuat suatu firewall yang aktif yang bisa mendifinisikan setiap data yang masuk kedalam server, apakah data yang datang itu merupakan sebuah data flood atau data yang diperlukan oleh user.

Kata kunci: LAN, WLAN, Mikrotik, *Flooding.*

1 PENDAHULUAN

Media *internet* sudah menjadi bagian kehidupan manusia untuk keperluan komunikasi dengan skala besar dalam kemajuan teknologi. Layanan *internet* untuk perusahaan, instansi pemerintahan, perkantoran, universitas dll, lebih dominan menggunakan jaringan komputer berbasis *Local Area Network* dan *Wireless Local Area Network* untuk penunjang komunikasi antar komputer. Topologi yang sering diterapkan pada LAN dan WLAN adalah topologi *start* dengan satu titik terpusat *device*, lebih seringnya menggunakan *device router*. Mikrotik *router* OS di lab riset Teknik Informatika UIKA digunakan sebagai *router* dari LAN dan WLAN. Ukuran kinerja *router* sangat diperlukan untuk memadai kapasitas pengguna dengan pengiriman data yang begitu banyak, dan apabila terlalu banyak permintaan data dari *user*, akan terjadi *Flood* data atau kebanjiran data baik melalui transmisi *Internet Protocol* (IP) *address* atau *mac address*. *Flooding/Denial Of Service* (DOS) adalah pengiriman data skala besar yang sengaja dilakukan untuk mengurangi kinerja *router* dalam media transmisi data. *Flooding* lebih sering digunakan pada *layer data link*, dikirim dari *layer* fisik menuju *data link* dan pencatatan *mac address* pada kompresi data dilakukan secara terus menerus tanpa masuk ke *layer* berikutnya. Dengan adanya *flooding* sangat merugikan *bandwidth* dan *user* lain, maka dilakukan analisa terhapad *flooding* agar mengetahui ciri-ciri dari *flooding* data jika terjadi pada *router* mikrotik.

2 METODE

Dalam penyusunan skripsi ini akan melalui 4 tahapan kegiatan, yaitu perancangan sistem, konfigurasi jaringan, pengujian dan analisa hasil pengujian. Tahapan-tahapan dalam metode penelitian dapat di gambarkan seperti ditunjukkan pada gambar di bawah ini.

Gambar 3.1 Metode Penelitian

2.3.1 Perancangan Sistem

Pada tahap ini akan dilakukan perancangan perangkat sistem dengan memanfaatkan alat dan bahan yang telah tersedia sebelumnya.

2.3.2 Konfigurasi Jaringan

Pada tahap ini akan dibahas berbagai konfigurasi jaringan untuk membuat simulasi Jaringan lokal komputer berbasi mikrotik dengan

beberapa client di lab riset teknik informatika Universitas Ibn Khaldun Bogor.

2.3.3 Penyerangan

Untuk memonitor *Flooding* data pada jalur lalu lintas *Router* Mikrotik di gunakan simulasi penyerangan dengan Backtrack, untuk mengetahui dan memonitor jaringan mengunakan *tools* wireshark.

2.3.4 Analisa Penyerangan

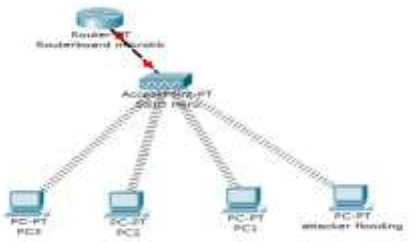
Pada tahap ini penulis akan menganalisa hasil penyerangan dengan memonitoring jalur lalu lintas pada *Router* Mikrotik dengan menggunakan *tools* wireshark. Setelah mendapatkan hasil dari monitoring makan hasilnya akan di imflementasikan dalam bentuk grafik dan ficture agar lebih mudah dipahami.

3 HASIL DAN BAHASAN SISTEM PAKAR JARINGAN KOMPUTER

3.1 Infrastruktur Perancangan Sistem

Bagian ini akan di bahas mengenai perancangan *wireless* berbasis *vitual access point* yang meliputi perancangan topologi, implementasi dan konfigurasi yang di bangun di lab riset teknik informatika Universitas Ibn Khaldun Bogor.

1. Topologi Jaingan
   Topologi yang digunakan dalam penelitian *wireless* berbasis *vitual access point* di mikrotik pada laboratorium riset teknik informatika universitas ibn khaldun Bogor di tunjukkan pada Gambar 3.1



Gambar 3.1 Topologi jaringan

2. Alokasi alamat IP
   Setelah dilakukan konfigurasi jaringan seperti Gambar 3.1, maka setiap *device* diberikan alamat IP, pada konfigurasi ini digunakan alamat IP :

Tabel 3.1 Alokasi IP

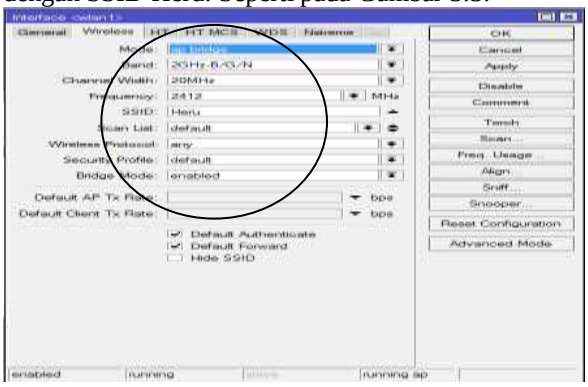
SSID/PC	IP
SSID Hendri	192.168.80.1/24
PC 1	192.168.80.5/24
PC 2	912.168.80.218/24
Attacker PC	192.168.80.219/24

3.2 Konfigurasi Jaringan

Bagian ini akan dibahas mengenai konfigurasi jaringan di awali dengan tahapan dengan mengaktifkan WLAN *master* yang secara default tersedia pada RB 751u-2hnd seperti Gambar 3.2

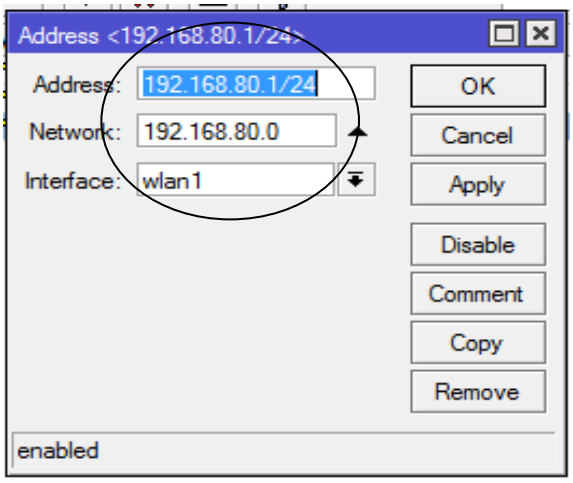
Gambar 3.2 Mengaktifkan WLAN Master

Setelah mengaktifkan WLAN *master*, tahapan selanjutnya mengganti mode *wireless* menjadi AP-Bridge dan mengganti SSID yang secara default diberi nama *Mikrotik*, diganti dengan SSID Heru. Seperti pada Gambar 3.3.



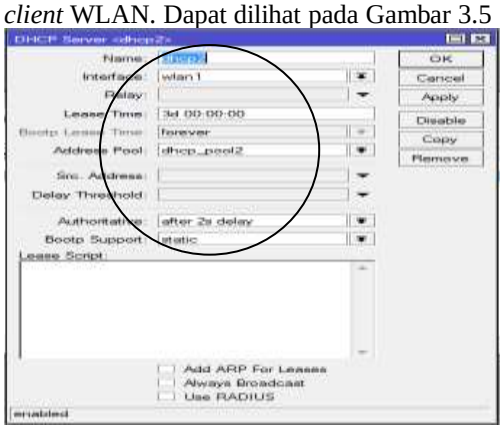
Gambar 3.3 Mengganti nama SSID Default Menjadi SSID Heru

Tahapan selanjutnya mengkonfigurasi IP pada WLANdengan SSID Heru, seperti Gambar 3.4



Gambar 3.4 Konfigurasi IP address pada WLAN master

Setelah mengkonfigurasi IP address pada WLAN, mengkonfigurasi DHCP Server yang bertujuan memberikan IP secara automatis pada *client* WLAN. Dapat dilihat pada Gambar 3.5



Gambar 3.5 Konfigurasi DHCP Server pada WLAN

3.6 Penyerangan

Pada tahapan ini dilakukan penyerangan flooding/DDOS dari klien hotspot WLAN SSID Heru. OS yang digunakan ketika penyerangan DDOS attack adalah Bactrack 5r berbasis linux. Tahapan DDOS attack adalah login hotspot WLAN agar dapat mengetahui Mac address router mikrotik, seperti pada Gambar 3.6 dibawah ini.

Gambar 3.6 *Login Hostpot*

Setelah *login hotspot* dan mendapatkan IP *address* 192.168.80.219, tahapan selanjutnya adalah membuka terminal backtrack dan men-*scan* identitas router dengan *tools* nmap, seperti pada Gambar 3.7 dibawah ini.

Gambar 3.7 *scan router* dengan *nmap*

Dari proses *scan* tersebut didapatkan *mac address router* yaitu D4:CA:6D:6B:8E:3F. Maka tahapan selanjutnya yaitu dengan menuliskan perintah macof –h. seperti pada Gambar 3.8 dibawah ini.

Gambar 3.8 *Tool Flooding*

Dengan keterangan macof tersebut dapat penjelasan yang harus dilakukan untuk DDOS *attack*, dengan memulai DDOS *attack mac address router* seperti pada Gambar 3.9 dan Gambar 3.10 dibawah ini.

Gambar 3.9 Keterangan *macof Flooding*

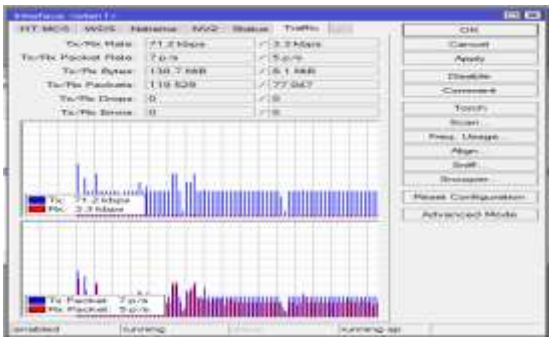
Gambar 3.10 DDOS attack

3.4 Analisis Serangan

Pada tahapan ini, dilakukan analisa dari tahapan sebelumnya, yaitu penyerangan *DDoS attack*. Analisa ditinjau dari trafik jaringan pada *router* sebelum dilakukan serangan, sesudah melakukan penyerangan dan melakukan penyerangan dan dicegah pada *router* mikrotik menggunakan *tools firewall*.

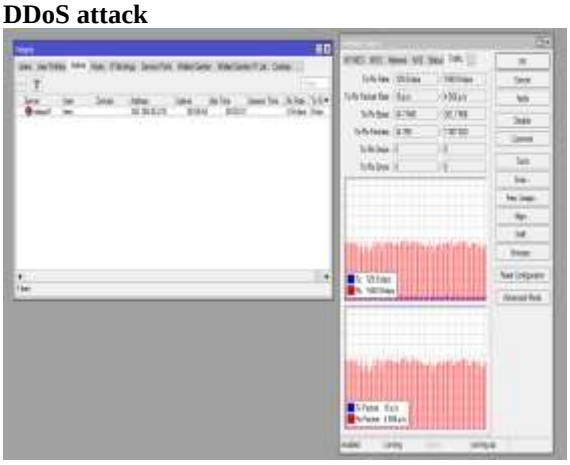
3.4.1 Trafik jaringan sebelum dilakukan serangan DDoS attack

Analisa sebelum dilakukan serangan ditinjau dari trafik jaringan pada *interface* WLAN di *router* mikrotik. Trafik pada interface WLAN dapat dilihat pada Gambar 3.11 yang di lihat pada *Grafical User Interface* (GUI) winbox di bawah ini.



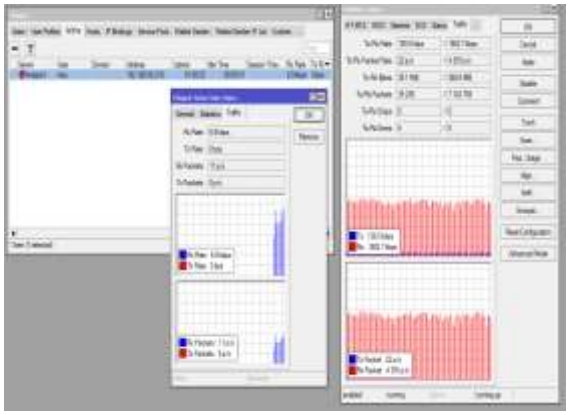
Gambar 3.11 Trafik dalam keadaan normal

3.4.2 Trafik jaringan saat dilakukan serangan DDoS attack



Gambar 3.12 *Traffic* jaringan WLAN dan *Traffic* jaringan *user Hostpot*

Pada Gambar 3.11 di atas terlihat *user hotspot* hanya 1 yang aktif dan *user hotspotattacker* OS bracktrack secara otomatis hilang pada *list user hotspot*, terdapat perbedaan *traffic* jaringan antara klien *hotpot* yang aktif dan *traffic* WLAN. Penggunaan WLAN hanya dipakai oleh 1 klien *hotspot* yang aktif dengan Rx (*receive rate*) 4,5 kbps dan Tx (*transfer rate*) 0 kbps , sedangkan *traffic*jaringan pada WLAN lebih besar Rx dan Tx. Secara lebih detail dapat dilihat pada Gambar 3.12 dibawah ini.



Gambar 3.13 *Traffic* jaringan WLAN dan *user*

pada gambar sebelah kiri *traffic* jaringan *user hotspot* terlihat lebih kecil dan sebelah kanan *traffic* jaringan WLAN lebih besar.

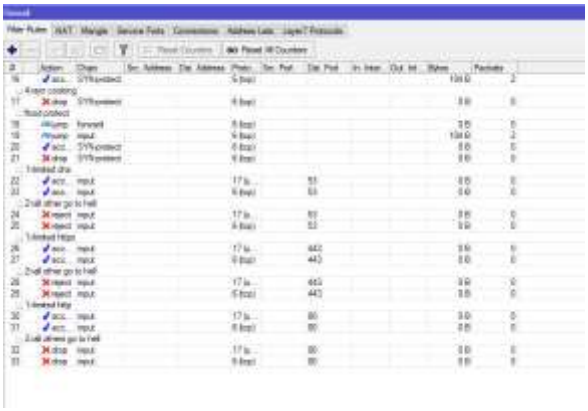
3.4.3 Trafik GUI winbox sesudah melakukan pencegahan pada DDoS *attack*

Pencegahan DDoS attack dilakukan menggunakan *tools firewall* pada mikrotik, dengan konfigurasi melalui terminal seperti pada Gambar 3.13 dan hasil dari konfigurasi tersebut dapat dilihat pada Gambar 3.14 di bawah ini.

```
ip firewall filter
add action=add-src-to-address-list address-list=blocked-addr \
    address-list-timeout=1d chain=input comment=\
    "1>limit incoming connection(Script Anti Flooding)" connection-limit=100,32 \
    disabled=no protocol=tcp
add action=tarpit chain=input comment="2>action tarpit" connection-limit=3,32 \
    disabled=no protocol=tcp src-address-list=blocked-addr
add action=jump chain=forward comment="3>SYN Flood protect" connection-state=\
    new disabled=yes jump-target=SYN-Protect protocol=tcp tcp-flags=syn
add action=accept chain=SYN-Protect connection-state=new disabled=no limit=\
    400,5 protocol=tcp tcp-flags=syn
add action=drop chain=SYN-Protect comment="4>syn cookies" connection-state=new \
    disabled=no protocol=tcp tcp-flags=syn
add action=jump chain=forward comment="Flood protect" connection-state=new \
    disabled=no jump-target=SYN-Protect protocol=tcp tcp-flags=syn
add action=jump chain=input connection-state=new disabled=no jump-target=\
    SYN-Protect protocol=tcp tcp-flags=syn
add action=accept chain=SYN-Protect connection-state=new disabled=no limit=\
    400,5 protocol=tcp tcp-flags=syn
add action=drop chain=SYN-Protect connection-state=new disabled=no protocol=tcp \
    tcp-flags=syn
add action=accept chain=input comment="1>limited dns" disabled=no dst-port=53 \
    limit=2400/1m,5 protocol=udp
add action=accept chain=input disabled=no dst-port=53 limit=2400/1m,5 protocol=\
    tcp
add action=reject chain=input comment="2>all others go to hell" disabled=no \
    dst-port=53 protocol=udp reject-with=icmp-protocol-unreachable
add action=reject chain=input disabled=no dst-port=53 protocol=tcp reject-with=\
    icmp-protocol-unreachable
add action=accept chain=input comment="1>limited https" disabled=no dst-port=\
    443 limit=2400/1m,5 protocol=udp
add action=accept chain=input disabled=no dst-port=443 limit=2400/1m,5 \
    protocol=tcp
add action=reject chain=input comment="2>all others go to hell" disabled=no \
    dst-port=443 protocol=udp reject-with=icmp-network-unreachable
add action=reject chain=input disabled=no dst-port=443 protocol=tcp \
    reject-with=icmp-network-unreachable
add action=accept chain=input comment="1>limited http" disabled=no dst-port=80 \
    limit=2400/1m,5 protocol=udp
add action=accept chain=input disabled=no dst-port=80 limit=2400/1m,5 protocol=\
    tcp
add action=drop chain=input comment="2>all others go to hell" disabled=no \
    dst-port=80 protocol=udp
add action=drop chain=input disabled=no dst-port=80 protocol=tcp
```

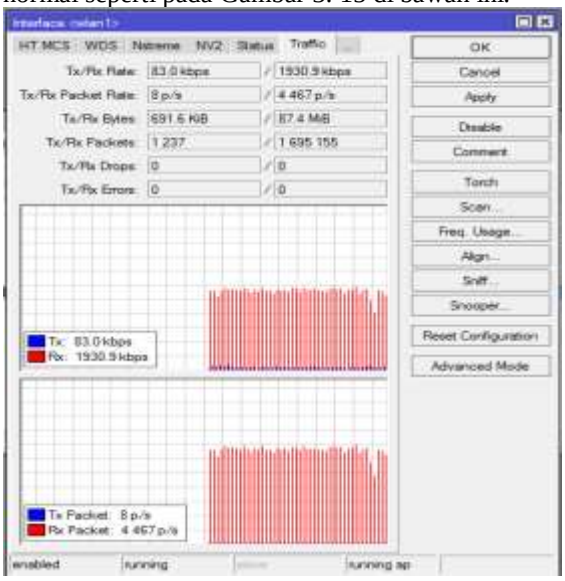
Gambar 3.14 konfigurasi pencegahan DDos attack

Dari hasi konfigurasi pencegahan DDoS *attack* menggunakan *firewall*, maka hasil konfigurasi dapat dilihat pada GUI winbox.



Gambar 3.15 GUI *winbox firewall*

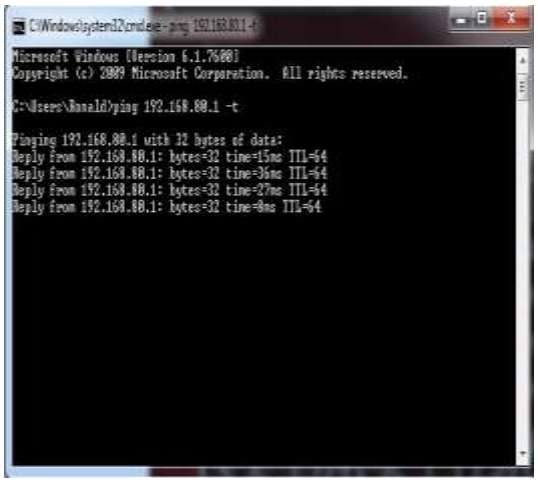
Setelah dilakukan pencegahan DDos Atack sangat terpengaruh terhadap trafik dan bandwicth pada interface WLAN dengan akses flooding masih berjalan, hasilnya bandwicth kembali normal seperti pada Gambar 3. 15 di bawah ini.



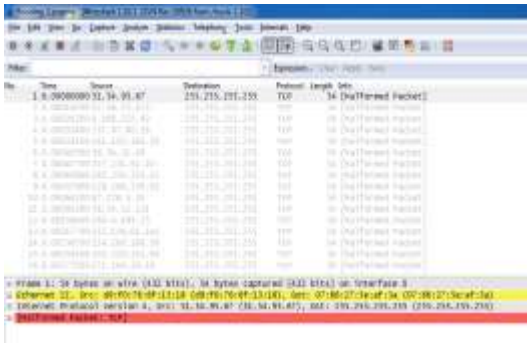
Gambar 3.16 *Traffic* ketika penutupan *firewall*

3.4.3 Analisis menggunakan Wireshark

Pada analisis menggunakan wireshark, analisa dilakukan oleh klien *hotspot* yang lain, dengan cara melakukan ping menuju IP router dan melakukan *capture* jaringan menggunakan wireshark. Seperti pada Gambar 3.17 dan 4.18 dibawah ini.



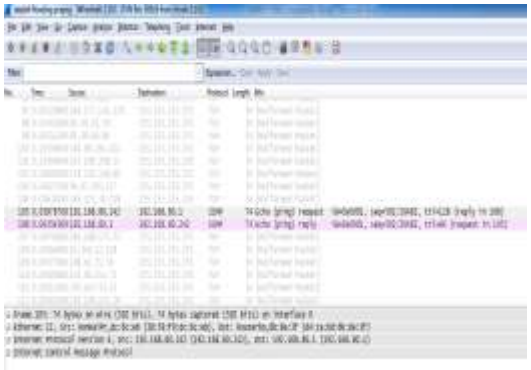
Gambar 3.17 *ping to router*



Gambar 3.18 *Capture wireshark*

Setelah melakukan ping dari klien ke *router* dan di *capture* melalui aplikasi wireshark terdapat banyak packet disetiap frame yang *MALFORMED PACKET* atau paket yang rusak.

Analisa dengan ping tersebut dilakukan selama 5 menit pada 5x pengujian, dan packet yang terkirim dan diterima terdapat pada frame ±100,800 dan 1400. Seperti pada Gambar 3.15 dibawah ini.



Gambar 3.19 *Frame packet wireshark*

Pengujian selama 5x tersebut didapatkan QoS, hasil QoS tersebut adalah *delay* dan *throughput* yang di tabelkan dan dibuat grafik dibawah ini.

Dari Gambar 3.11 di atas trafki jaringan pada *interface* WLAN dikatakan normal, berdasarkan nilai QoS dengan parameter *delay* dan *throughut* yang tidak melebihi nilai *delay* dan *throughput* yang direkomendasikan ITU-T. table *delay* dan *throughput* yang menyatakan nilai trafik normal dapat dilihat pada table 4.2 untuk nilai *delay* dan table 4.3 untuk nilai *throughput* dibawah ini.

Tabel 3.2 Delay trafik normal

Lama Penguji an	Pdt	Pdk	Delay (s)	Dela y (ms)
5 menit pertama	2,001042	1,999975	0,001067	1,067
5 menit kedua	2,001057	1,999966	0,001091	1,091
5 menit ketiga	2,002141	1,999943	0,002198	2,198
5 menit keempat	2,000729	1,99964	0,001089	1,089
5 menit kelima	3,000862	2,99994	0,000922	0,922

Pengujian *packet delay* dilakukan dengan menggunakan wireshark, untuk menguji menggunakan rumus dibawah ini:

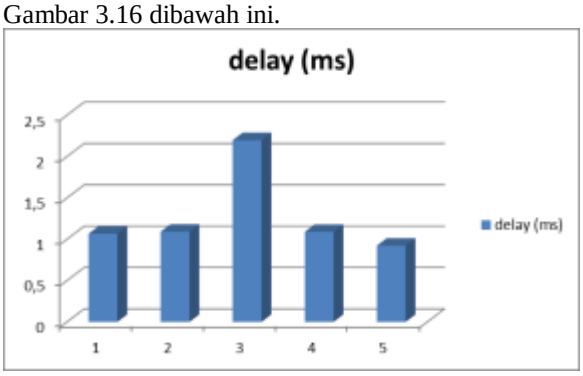
Pengukuran *packet delay* pada 5 menit

Packet delay = (waktu *packet* yang diterima-waktu *packet* dikirimkan)

= 2,001042 – 1,999975 = 0,001067 s

= 1,067 ms

Hasil perhitungan delay trafik normal yang ditabelkan, dapat dilihat secara grafik pada Gambar 3.16 dibawah ini.



Gambar 3.20 grafik delay trafik normal

Parameter QoS selanjutnya yaitu nilai dari throughput yang ditabelkan pada table 4.3 dibawah ini.

Tabel 3.3 *troughput trafik normal*

lama pengujian	rata-rata paket (s)	paket (s)	throughput
5 menit pertama	69,02	2,985	23,12227806
5 menit kedua	66,008	2,121	31,12116926
5 menit ketiga	59,041	2,1	28,1147619
5 menit keempat	58,999	2,22	26,57612613
5 menit kelima	60,098	2,13	28,21502347

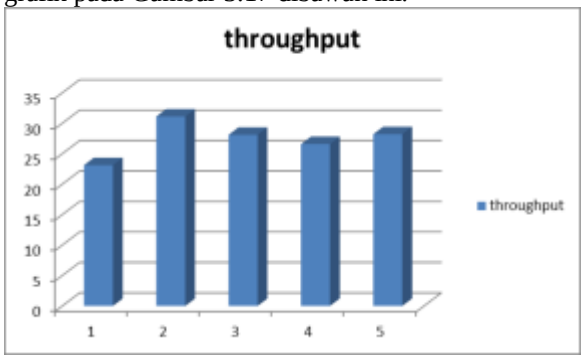
Pada pengujian *packet throughput* dilakukan menggunakan wireshark, untuk menguji dilakukan dengan rumus dibawah ini:
Pengukuran *throughput* pada 5 menit pertama

Througput = *Packet* data yang diterima / Lama pengamatan

= 69,02/2,985

= 23,12227806 bps

Hasil perhitungan *throughput* trafik normal yang ditabelkan, dapat dilihat secara grafik pada Gambar 3.17 dibawah ini.



Gambar 3.21 *trougput trafik normal*

Tabel 3.4 Delay

Lama Pengujian	Replay	Request	Delay (s)	Delay (ms)
5x menit pertama	0.043543	0.039787	0.003756	3.756
5x menit kedua	0.834991	0.826406	0.008504	8.504
5x menit ketiga	0.292908	0.277958	0.01495	14.95
5x menit keempat	0.732056	0.706995	0.025061	25.061
5x menit kelima	0.418389	0.385855	0.032534	32.534

Pengujian *packet delay* dilakukan dengan menggunakan wireshark, untuk menguji menggunakan rumus dibawah ini:
Pengukuran *packet delay* pada 5 menit

Packet delay = (waktu *packet* yang diterima-waktu *packet* dikirimkan)

= 0.043543– 0,039787 = 0.003756 s

= 3.756 ms

Gambar 3.22 Grafik *Delay*

Tabel 3.5 *Trougtput*

Lama Pengujian	average pkt/s	pkt/s	Throughput
5 menit pertama	2142.567	67.186	31.8900813
5 menit kedua	2105.274	70.084	30.0392957
5 menit ketiga	2157.739	44.208	48.8087903
5 menit keempat	1949.543	32.721	59.5807891
5 menit kelima	1875.509	81.298	23.0695589

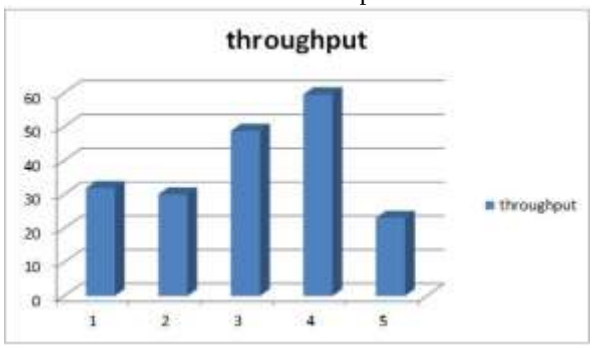
Pada pengujian *packet throughput* dilakukan menggunakan wireshark, untuk menguji dilakukan dengan rumus dibawah ini:

Pengukuran *throughput* pada 5 menit pertama

Througput = *Packet* data yang diterima / Lama pengamatan

=

2142.567/67.186 = 31.8900813 bps



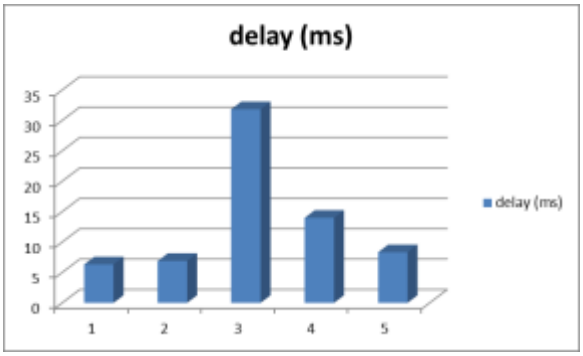
Gambar 3.23 Grafik *Throughput*

Untuk perbandingan dengan akses *flood* ketika sesudah dicegah menggunakan *firewall* maka didapatkan hasil QoS pada table 4.4 untuk *delay* dan 4.5 untuk *throughput.*

Tabel 3.6 *Delay* sesudah di tutup *firewall*

Lama penguji a	Pdt	Pdk	delay (s)	delay (ms)
5 menit pertam a	3.48421 2	3.47787 8	0.0063 3	6.334
5 menit kedua	0.2385	0.23160 8	0.0068 9	6.892
5 menit ketiga	0.47285 2	0.44101 7	0.0318 4	31.83 5
5 menit keempa t	0.20019	0.18620 5	0.0139 9	13.98 5
5 menit kelima	0.46169 4	0.45336 2	0.0083 3	8.332

Dari hasil tabel di atas, terjadi penurunan yang signifikan pada *delay* dan dapat dilihat pada gambar grafik 4.18 di bawah ini.

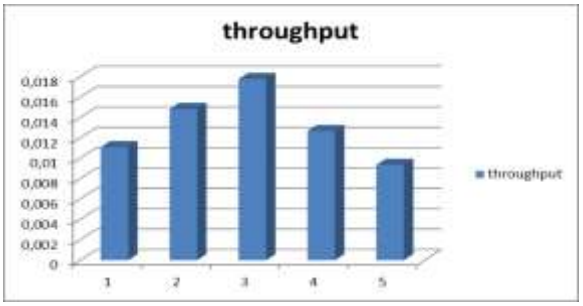


Gambar 3.24 Grafik *Delay* ketika tertutup *firewall*

Parameter QoS selanjutnya yaitu dengan *throughput* ketika *firewall* sudah ditutup untuk DDoS *attack.* Table dan grafik dapat dilihat pada table 4.5 dan gambar grafik pada Gambar 3.19 dibawah ini.

Tabel 3.7 *Troughput* sesudah di tutup firewall

Lama pengujian	avg paket(s)	paket (s)	throughput
5 menit pertama	24.652	2219.25	0.0111083
5 menit kedua	33.519	2256.54	0.0148542
5 menit ketiga	40.318	2265.68	0.0177951
5 menit keempat	28.095	2215.89	0.0126789
5 menit kelima	21.218	2264.67	0.0093691



Gambar 3.25 Throughput

4 KESIMPULAN

Berdasarkan hasil dan bahasan tersebut, maka dapat ditarik simpulan sebagai berikut:

1. Trafik jaringan WlAN pada mikrotik secara tiba-tiba meningkat, sedangkan pada moritoring winbox trafik jaringan user lebih kecil dari trafik jaringan WLAN.

2. Pada saat di*capture* dan melakukan *ping*, pembanjiran paket data yang menyebabkan *malformed packet*/paket rusak.
3. Ketika *firewall* pada mikrotik ditutup untuk mencegah DDoS *attack*, hasil QoS menjadi normal kembali

5 DAFTAR PUSTAKA

[1] JHONSEN, Jhon Edison, *Membangun Wireless LAN*, Elex Media Komputindo,Gramedia, Jakarta, 2005.

[2] PURBO,O,W., *CHIP Spesial,Internet Wireless dan HotSpot*, Elex Media Komputindo, Gramedia,Jakarta, 2006.

[3] HANDRIYANTO, Dwi Febrian, *Kajian Penggunaan* Mikrotik *Router OS Sebagai Router pada Jaringan Komputer*, Jurnal, Fakultas Teknik Informatika, Universitas Sriwijaya.

[4] Herlambang, *Panduan Lengkap Menguasai Router Masa Depan Menggunakan* Mikrotik *Router Os*, ANDI Publisher, Yogyakarta , 2008.

[5] I, Hardana dan Irvantino, *Konfigurasi Wireless Router board* Mikrotik, Andi, Yogyakarta, 2011.

[6] MULYANA, E, S, *Pengenalan protocol jaringan Wireless Komputer*, ANDI, Yogyakarta , 2008.

[7] YOANESS, *Mengenal Teknologi Quality Of Services (Qos) di internet*, Bandung,2010.

[8] Tanenbaum, Andrew S . 1996 . Jaringan Komputer Edisi Bahasa Indonesia Jilid 1.Prehallindo : Jakarta.

[9] *Attacking Side With* Backtrack *(ASWB)*, http://republicofnote.blogspot.com/2013/01/free-download-ebook-tutorial-hacking-with-backtrack.html. (06 Agustus 2014)

[10] S'to, 2004. Seni *Hacking* I. (Jasakom, Jogja Karta).