PENERAPAN METODE FILTERING VIDEO STREAMING DAN MALWARE PADA JARINGAN LOCAL AREA NETWORK

[1]Dwi Nurmasari Pratiwi, [2]Denar Regata Akbi
[1,2]Teknik Informatika, Universitas Muhammadiyah Malang
Jl. Raya Tlogomas No. 246, Malang
Email: nurmasari.np@gmail.com, dnarregata@umm.ac.id

ABSTRAK

Jaringan komputer adalah jaringan penghubung komputer yang akan memberikan akses pada aplikasi layanan. Video Streaming merupakan layanan yang dapat mengkonsumsi bandwidth besar sehingga menyebabkan layanan akses lainnya tidak mendapatkan bandwidth yang cukup. Selain itu jaringan LAN sangat rentan sekali akan dimasuki oleh malware yang membuat jaringan sering down dan tidak stabil.Oleh karena itu, diperlukan adanya pengamanan jaringan dan filtering layanan. Dengan memanfaatkan router mikrotik dengan filtering port firewall dapat meminimalisir terjadinya penyebaran malware dan mengurangi penggunaan bandwidth. Metode Penelitiann yang dilakukan dengan studi literatur, perancangan, impelentasi, analisa pengujian. Hasil pengujian performansi sebelum implementasi filtering port pada jaringan LAN menunujukkan nilai bandwidth 98,04 Mbits, Jitter 0,046 ms, dan Packet loss 0,3 ms. Sedangkan pengujian nilai QoS setelah penerapan filtering port menunjukkan hasil bandwidth 364 Mbits, Jitter 0,022, dan packet loss 0,047. Performansi lebih stabil dan menunjukkan kinerja yang baik pada implementasi filteirng port video streaming. Hasil pengujian kenaikan dan penurunan nilai performansi masih dalam standart rekomendasi ITU-T.

Kata kunci: Mikrotik OS, Jaringan Komputer, iperf, QoS, LAN.

1 PENDAHULUAN

Di era globalisasi ini teknologi informasi perkembangannya semakin hari semakin pesat, tidak hanya di Indonesia saja bahkan seluruh dunia. Kini seluruh kegiatan dapat dilakukan menggunakan internet. Didalam internet terdapat informasi yang sederhana hingga kompleks, serta informasi yang bersifat *independent* maupun kelompok. Selain informasi berupa data internet juga memberikan layanan gambar, video, dan suara[1]. *Local Area Network* (LAN) adalah jaringan yang mempunyai sifat internal seperti hanya milik pribadi dan area jangkauan terbatas. Jarak antar *node* biasanya sekitar 200 m[2]. misalnya saja, antar gedung maupun kantor yang jaringan fisiknya berdekatan dan saling terhubung dengan yang lainnya. Untuk menghubungkan jaringan *Local Area Network* (LAN) memerlukan mikrotik. Mikrotik adalah sistem operasi yang berfungsi sebagai router pada jaringan. Karena kehandalanya mikrotik mempunyai banyak fitur lengkap dan jaringan *wireless*. Mikrotik juga memiliki kegunaan sebagai *firewall* untuk komputer lain[3]. Selain itu mikrotik dapat memberikan prioritas pada komputer lain supaya dapat mengakses data internet atau lokal. Tujuan mikrotik yaitu untuk melakukan manajemen jaringan dan pengaturan *bandwidth*[4].

Namun, terdapat informasi kini menjadi trending adalah *video streaming*. *Video streaming* adalah sebuah layanan visual video yang dapat diputar tanpa harus men*download* terlebih dahulu[5]. Akan tetapi video streaming sangat boros *bandwidth*. Sehingga membuat jaringan sering *down* dan kurang stabil. Jaringan LAN juga memiliki kelemahan terhadap keamanan jaringan. *Malware* seperti virus, *trojan*, dan *worm* mudah sekali masuk dalam jaringan tersebut. Apabila *walmare* ini masuk dalam jaringan maka akan terjadi kerusakan data dan jaringan tidak stabil[6]. *Filtering port* adalah sebuah *filtering* untuk jaringan tertentu yang dapat meminimalisir terjadinya proses penggunaan *bandwidth* dan manajemen pada jaringan lokal[7]. *Filtering port* ini memanfaatkan fungsi mikrotik dengan fitur *firewall*. *Firewall* adalah fitur pendukung "pos pemeriksaan" untuk mengevaluasi keluar dan masuknya *traffic* di lokal ataupun *private network*. *Firewall* mengizinkan traffik tertentu dan melakukan *filtering* pada jaringan[8]. *Filtering port* dilakukan pada *video streaming* dan malware.

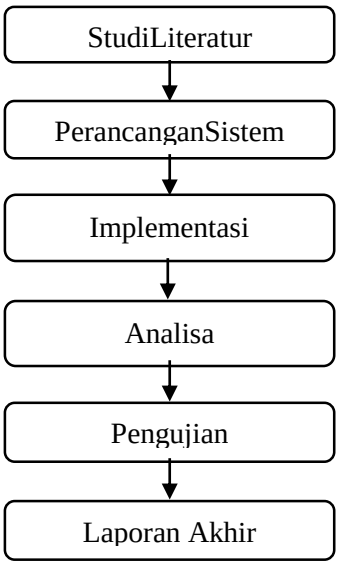
Pada penelitian sebelumnya *blocking port* melalui firewall dilakukan dengan cara membangun jaringan secara *real*. Perangan tersebut menggunakan komputer, lancard, hub, dan mikrotik[9]. Pemblokiran berhasil dilakukan dengan baik. Hasil dari percobaan sistem jaringan menjadi stabil.

Kemudian pada penelitian sebelumnya menggunakan metode *stress test*. Menggunakan ubuntu 9.04 sebagai client. Penelitian ini membuktikan bahwa firewall dapat memenuhi kebutuhan sistem *filtering*.

Berdasarkan penjabaran latar belakang diatas, akan dilakukan implementasi dengan menerapakan filtering port *video streaming* pada jaringan *Local Area Network* (LAN). *Filtering port* diimplementasikan pada *video streaming* dan *malware*, sehingga pengguna tidak perlu khawatir jaringan akan *down* dan kurang stabil. *Filtering port* bertujuan untuk meningkatkan performansi dari sebuah jaringan.

2 METODE PENELITIAN

Metode penelitian yang digunakan adalah sebagai berikut:



Gambar 1. Alur Penelitian

2.1 Tahapan Studi Literatur

Tahap studi literaturgambar 1 merupakan tahap mengumpulkan berbagai macam informasi sehubungan dengan proses yang akan dikembangkan, seperti buku-buku, artikel ilmiah, dan jurnal ilmiah yang menjelaskan permasalahan yang diambil.

2.2 Tahapan Perancangan Sistem

Perancangan dan implementasi gambar 1 pada penelitian ini menggunakan windows 10, ubuntu server, winbox, mikrotik router OS dan tools iperf. Berikut ini rancangan sistem:

1. Filtering menggunakan firewall winbox
2. Implementasi mikrotik dan ubuntu server pada virtual box
3. Konfigurasi IP
4. Filtering youtube saat
5. Filtering malware
6. Monitoring jaringan
7. Tahap studi literatur

2.3 Tahapan Analisa

Tahap analisa gambar 1 adalah tahap apabila proses implementasi dan pengujian sudah dilakukan. Analisis dilakukan menggunakan parameter bandwidth. Ada beberapa analisis yang dilakukan:

1. Analisa menggunakan paramter *bandwidth*, *jitter*, dan *packet loss*.
2. Analisa dilakukan saat implementasi *filtering port* dan sebelum *filtering port*.

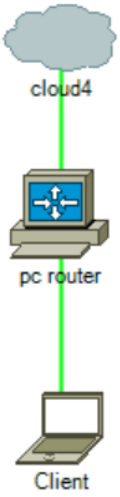
2.4 Skenario Pengujian

Skenario pengujian gambar 1dilakukan setelah perancangandan implementasi dilakukan. Pengujian dilakukan pada jaringan LAN terhadap parameter *bandwidth*, *jitter*, dan *packet loss* saat sebelum dan sesudah menerapkan *filtering*. Pengujian dilakukan dengan kondisi sebagai berikut.

Saat *client* ingin mengakses youtube, *request* dari *client* melewati router yang berfungsi sebagai penghubung jaringan dan routing, kemudian diteruskan ke server, setelah data didistribusikan dan diproses oleh server data akan dikirim kembali ketujan sesuai dengan permintaan client. Saat terdapat port yang mencurigakan ingin diakses oleh *client* secara otomatis router akan merespon mengirim data ke server untuk menyaring port tersebut. Parameter yang dibutuhkan dalam pengujian yaitu parameter *bandwidth*, *jitter*, dan *packet loss*.

3 HASIL DAN PEMBAHASAN

Dari gambar 2 dibuatlah sebuah jaringan lokal yang tersambung pada pc *routing* dengan akses *video streaming* berupa *youtube*. Menggunakan topologi *Bus*. Kemudian akan dilakukan *filtering port* pada *youtube* dan *malware*. Pengujian dilakukan dengan menganalisa Bandwidth, jitter, dan packet loss.



Gambar 2. Rancangan Jaringan

3.1 Blocking Port Malware

```
[admin@MikroTik] > /ip firewall filter
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=135-13
9 action=drop comment="Blaster Worm"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp dst-port=135-13
9 action=drop comment="Messenger Worm"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=445 ac
tion=drop comment="Blaster Worm"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp dst-port=445 ac
tion=drop comment="Blaster Worm"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=593 ac
tion=drop comment="______"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=1024-1
030 action=drop comment="______"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=1080 a
ction=drop comment="Drop MyDoom"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=1214 a
ction=drop comment="______"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=1363 a
ctio=drop comment="ndm requester"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=1364 a
ctio=drop comment="ndm server"
```

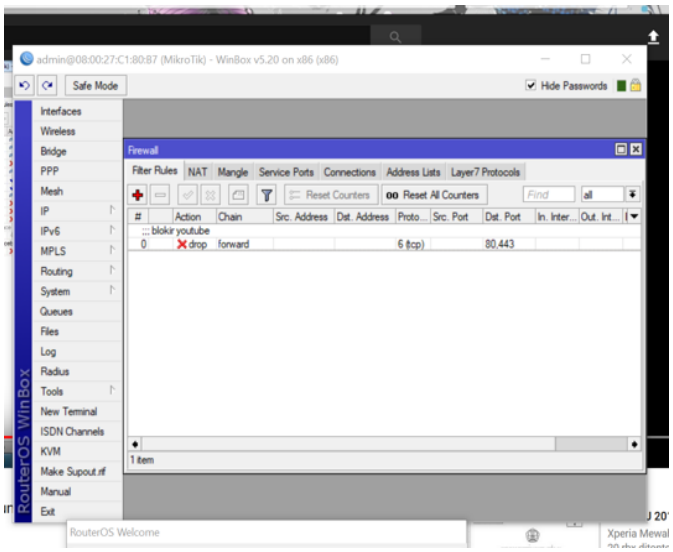
```
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=1368 a
ctio=drop comment="screen cast"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=1373 a
ctio=drop comment="hromgrafx"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=1377 a
ctio=drop comment="cichlid"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=2745 a
ctio=drop comment="Bagle Virus"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=2283 a
ctio=drop comment="Dumaru.Y"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=2535 a
ctio=drop comment="Beagle"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=2745 a
ctio=drop comment="Beagle.C-K"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=3127-3
128 actio=drop comment="MyDoom"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=3410 a
ctio=drop comment="Backdoor OptixPro"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=4444 a
ctio=drop comment="Worm"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp dst-port=4444 a
ctio=drop comment="Worm"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=5554 a
ctio=drop comment="Drop Sasser"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=8866 a
ctio=drop comment="Drop Beagle.B"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=9898 a
ctio=drop comment="Drop Dabber.A-B"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=10000
actio=drop comment="Drop Dumaru.Y"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=10080
actio=drop comment="Drop MyDoom.B"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=12345
actio=drop comment="Drop NetBus"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=17300
actio=drop comment="Drop Kuang2"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=27374
actio=drop comment="Drop SubSeven"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=tcp dst-port=65506
actio=drop comment="Drop PhatBot,Agobot,Gaobot"
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp dst-port=12667
action=drop comment="Trinoo" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp dst-port=27665
action=drop comment="Trinoo" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp dst-port=31335
action=drop comment="Trinoo" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp dst-port=27444
action=drop comment="Trinoo" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp dst-port=34555
action=drop comment="Trinoo" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp dst-port=35555
action=drop comment="Trinoo" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp dst-port=27444
action=drop comment="Trinoo" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp dst-port=27665
```

```
action=drop comment="Trinoo" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp dst-port=31335
action=drop comment="Trinoo" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp dst-port=31846
action=drop comment="Trinoo" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp dst-port=34555
action=drop comment="Trinoo" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp dst-port=35555
action=drop comment="Trinoo" disabled=no
[admin@MikroTik] /ip firewall filter> add action=drop chain=forward comment=";;Blo
ck W32.Kido - Conficker" disabled=no protocol=udp src-port=135-139,445
[admin@MikroTik] /ip firewall filter> add action=drop chain=forward comment="" dis
abled=no dst-port=135-139,445 protocol=udp
[admin@MikroTik] /ip firewall filter> add action=drop chain=forward comment="" dis
abled=no src-port=135-139,445,539
failure: ports can be specified if proto is tcp or udp
[admin@MikroTik] /ip firewall filter> add action=drop chain=forward comment="" dis
abled=no protocol=tcp src-port=135-139,445,539
[admin@MikroTik] /ip firewall filter> add action=drop chain=forward comment="" dis
abled=no dst-port=135-139,445,593 protocol=tcp
[admin@MikroTik] /ip firewall filter> add action=accept chain=input comment="Allow
 limited pings" disabled=no limit=50/5s,2 protocol=icmp
[admin@MikroTik] /ip firewall filter> add action=accept chain=input comment="" dis
abled=no limit=50/5s,2 protocol=icmp
[admin@MikroTik] /ip firewall filter> add action=drop chain=input comment="drop FT
P Brute Forcers" disabled=no dst-port=21 protocol=tcp src-address-list=FTP_BlackLi
st
[admin@MikroTik] /ip firewall filter> add action=drop chain=input comment="" disab
led=no dst-port=21 protocol=tcp src-address-list=FTP_BlackList
[admin@MikroTik] /ip firewall filter> add action=accept chain=output comment="" co
ntent="530 Login incorrect" disabled=no dst-limit=1/1m,9,dst-address/1m protocol=t
cp
[admin@MikroTik] /ip firewall filter> add action=add-dst-to-address-list address-l
ist=FTP_BlackList address-list-timeout=1d chain=output comment="" content="530 Log
in incorrect" disabled=no protocol=tcp
[admin@MikroTik] /ip firewall filter> add action=drop chain=input comment="drop SS
H&TELNET Brute Forcers" disabled=no dst-port=22-23 protocol=tcp src-address-list=I
P_BlackList
[admin@MikroTik] /ip firewall filter> add action=add-src-to-address-list address-l
ist=IP_BlackList address-list-timeout=1d chain=input comment="" connection-state=n
ew disabled=no dst-port=22-23 protocol=tcp src-address-list=SSH_BlackList_3
[admin@MikroTik] /ip firewall filter> add action=add-src-to-address-list address-l
ist=SSH_BlackList_3 address-list-timeout=1m chain=input comment="" connection-stat
e=new disabled=no dst-port=22-23 protocol=tcp src-address-list=SSH_BlackList_2
[admin@MikroTik] /ip firewall filter> add action=add-src-to-address-list address-l
ist=SSH_BlackList_2 address-list-timeout=1m chain=input comment="" connection-stat
e=new disabled=no dst-port=22-23 protocol=tcp src-address-list=SSH_BlackList_1
[admin@MikroTik] /ip firewall filter> add action=add-src-to-address-list address-l
ist=SSH_BlackList_1 address-list-timeout=1m chain=input comment="" connection-stat
e=new disabled=no dst-port=22-23 protocol=tcp
[admin@MikroTik] /ip firewall filter> add action=drop chain=input comment="drop po
rt scanners" disabled=no src-address-list=port_scanners
[admin@MikroTik] /ip firewall filter> add action=add-src-to-address-list address-l
ist=port_scanners address-list-timeout=2w chain=input comment="" disabled=no proto
col=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg
```

```
[admin@MikroTik] /ip firewall filter> add action=add-src-to-address-list address-l
ist=port_scanners address-list-timeout=2w chain=input comment="" disabled=no proto
col=tcp tcp-flags=fin,syn
[admin@MikroTik] /ip firewall filter> add action=add-src-to-address-list address-l
ist=port_scanners address-list-timeout=2w chain=input  comment="" disabled=no prot
ocol=tcp tcp-flags=syn,rst
[admin@MikroTik] /ip firewall filter> add action=add-src-to-address-list address-l
ist=port_scanners address-list-timeout=2w chain=input comment="" disabled=no proto
col=tcp tcp-flags=fin,psh,urg,!rst,!ack
[admin@MikroTik] /ip firewall filter> add action=add-src-to-address-list address-l
ist=port_scanners address-list-timeout=2w chain=input comment="" disabled=no proto
col=tcp tcp-flags=fin,syn,rst,psh,ack,urg
[admin@MikroTik] /ip firewall filter> add action=add-src-to-address-list address-l
ist=port_scanners address-list-timeout=2w chain=input comment="" disabled=no proto
col=tcp tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg
[admin@MikroTik] /ip firewall filter>
```

Gambar 3. Blocking Port Malware

3.2 Blocking Port Youtube



Gambar 4. Blocking Port Youtube

Hasil penelitan dan mengujian performansi jaringan LAN menggunakan perintah tools iperf. iperf berfungsi untuk mengukur parameter bandwidth, jitter, dan packet loss pada port TCP. Perintah pengujian iperf3. Exe –c 192.168.2.1 –u –b –M.

Tabel 1. Hasil Pengujian

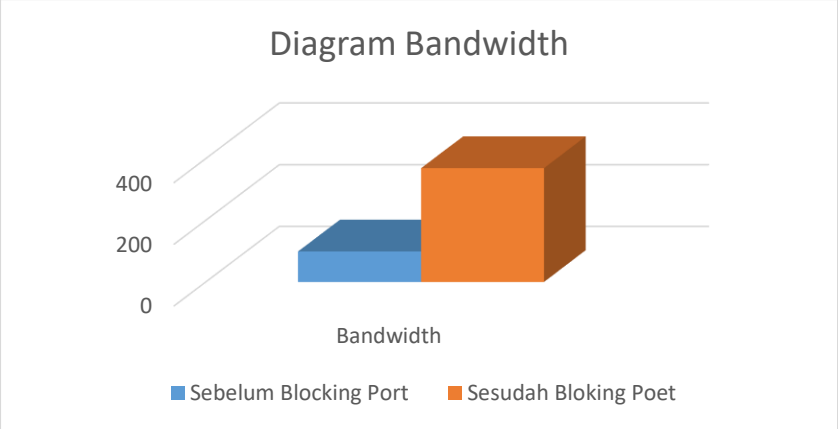
	Sebelum filtering port	Sesudah filtering port
Bandwidth	99,04 Mbits	369 Mbits
Jitter	0,036	0,021
Lost	0,2	0,075

Pengujian dilakukan sesuai dengan perancangan yang telah ditentukan. Hasil pengujian pada Tabel 1 terjadi perbedaan pada bandwidth, jitter, dan packet loss. Performansi sesudah penerapan filtering port lebih bagus dibandingkan dengan sebelum dilakukan filtering port.

1. Pengukuran performansi pada *Bandwidth*
   Diagram bandwidth hasil pengujian mengalami perbedaan yang sangat jauh . Kenaikan *bandwidth* terjadi saat *filtering port video streaming* dan *malware* diimplementasikan. Video streaming terlihat sangat mempengaruhi penggunaan *bandwidth*. Pengurangan penggunaan *bandwidth* berkurang

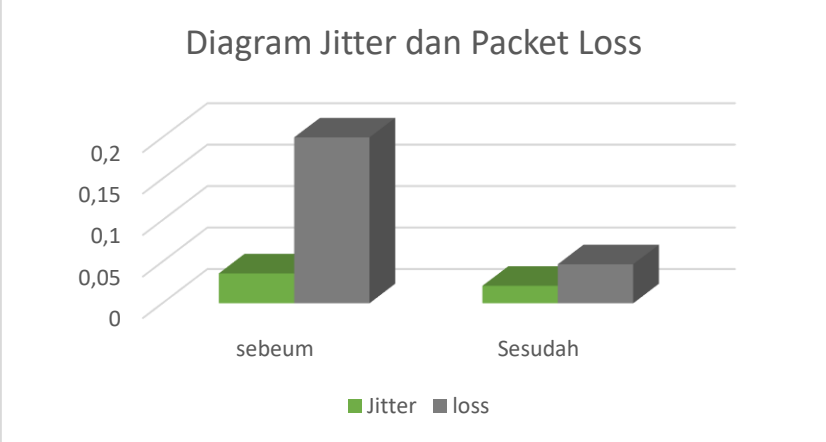
E-ISSN:2540-9719
ISSN:2302-8149

karena adanya *filtering port*. Nilai bandwidth sebelum filtering port 99,04 Mbits, sedangkan sesudah penerapan *filtering port* adalah 369 Mbits. Lebih jelasnya bisa dilihat pada gambar 5.



Gambar 5. Diagram Bandwidth

2. Pengukuran performansi *Jitter* dan *Packet Loss*
   Nilai jitter dan packet loss juga cendurung mengalami kenaikan. Kenaikan terjadi saat sesudah implementasi *filtering port* pada *video streaming* dan *malware*. Namun sebelum maupun sesudah filtering port mash dalam standart rekomendasi ITU-T yaitu kurang dari 50ms, rata-rata nilai jitter dan packet loss masoh dibawah 1 *ms*. Lebih jelasnya bisa dilihat pada gambar 6.



Gambar 5. Diagram Jitter dan Packet loss

4 PENUTUP

Berdasarkan seluruh tahapan penelitina yang telah dilakukan pada *filtering port* jaringan LAN dapat simpulkan bahwa implementasi sesuai dengan rancangan pada jaringan berjalan dengan baik. *Filtering port video streaming* dan *malware* memberi pengaruh terhadap performansi jaringan. Sebelum dilakukan filtering port nilai bandwidth sangat rendah sekali begitu juga dengan nilai packet loss dan jitter. Namun kenaikan dan penurunan nilai bandwidth, packet loss, dan jitter masih dalam standart rekomendasi ITU-T.

REFERENSI

[1] Yuisar, L. Yulianti, and Y. S. H, "Analisa pemanfaatan proxy server sebagai media filtering dan caching pada jaringan komputer," J. Media Infotama, vol. 11, no. 1, pp. 81–90, 2015.

[2] A. Tedyyana and F. P. Putra, "PEMANFAATAN REMOTE ACCESS UNTUK MEMONITORING KOMPUTER DI LABORATORIUM JARINGAN KOMPUTER POLITEKNIK NEGERI BENGKALIS," Semin. Nas. Telekomun. dan Inform., pp. 141–146, 2016.

[3] R. A. T. Sumardi, "Rancang Bangun Sistem Keamanan Jaringan Dengan Metode Blocking Port Pada Sekolah Menengah Kejuruan Karya Nugraha Boyolali," Indones. J. Netw. Secur., vol. 2, no. Jaringan, pp. 16–21, 2013.

[4] P. Sapriyadi, Surya and W. Fajar, "MANAJEMEN BANDWIDTH DENGAN ROUTER OS MIKROTIK MENGGUNAKAN METODE PER CONNECTION QUEUE," SENATIK, pp. 0–3, 2017.

[5] A. Sangsari, Isnawaty, and L. F. Aksara, "Analisis QoS (Quality of Service) Pada Layanan Video Streaming yang Menggunakan Protokol RTMP (Real Time Messaging Protocol)," semanTIK, vol. 2, no. 2, pp. 177–188, 2016.

[6] D. Irawan, "Keamanan jaringan komputer dengan metode blocking port pada laboratorium komputer program diploma-iii sistem informasi universitas muhammadiyah metro," Manaj. Inform. Progr. Diploma III UM Metro, vol. 02, no. 05, pp. 1–9, 2015.

[7] R. Hikmaturokhman, A., Purwanto, A., & Munadi, "Analisis Perancangan Dan Implementasi Firewall Dan Traffic Filtering Menggunakan Cisco Router," Semin. Nas. Inform., vol. 1, no. 3, pp. 1–8, 2015.

[8] F. Fitriastuti and D. P. Utomo, "IMPLEMENTASI BANDWDITH MANAGEMENT DAN FIREWALL SYSTEM MENGGUNAKAN MIKROTIK OS 2 . 9 . 27," J. Tek., vol. 4, no. 1, pp. 1–9, 2014.

[9] Fitri, M. Yamin2, and L. B. Aksara, "Perbandingan metode differentiated service dengan metode integrated service untuk analisa quality of service (QOS video streaming) pada jaringan Multi Protocol Label Switching (MPLS)," semanTIK, vol. 3, no. 1, pp. 135–142, 2017.

[10] Myo Thant, Kyaw Myat Thu, Kyaw Zaw Ye, Si Thu Thant Sin, "Development Of Firewall Optimazion Model Using by Packet Filter", 978-1-5090-0888-9 IEEE, pp. 273-278, 2016

[11] Haider Mohammed Turki Al-Hilfi, Bassam Abdulmunem Salih, Ion Marghescu, "Design of Secure WLAN by Using "Packet Filtering Firewall"", 970-1-5090-4442-9 IEEE, pp. 1857-1962, 2017.

[12] Praveen N, Dr. K Kumar, "Software-defined netwroking: Reconfigurable Network system in LAN Topology", 978-1-4673-9206-8 IEEE, 2016.

[13] Stefan cel Mare, "Local Management for QoS parameters", ISSN: 2247-5443 IEEE., 2016.

[14] Ananda Kumar K S, Balakrishna R, "Comparative Analysis of Delay and Throuhput using IEEE 802.11 and Receiver Centric-MAC Protocol in Wireless Sensor Networks", 978-1-5090-5682 IEEE, pp. 1-5, 2017.

[15] Dadiek Pranindito, Levana Rizki Daenira, Eko Fajar Cahyadi, "Perancangan NGN Berbasis Open IMS Core Pada Jaringan MPLS VPN", ISBN: 9-789-7936-499-93, 2017.

[16] Naning Dwiyanti, Martianda E, Citra D. Murdaningtyas, "Performance of QoS Paramters for UHF TV Broadcast on Batu TV", 978-1-5386-0712-1 IEEE., pp. 245-250, 2017.

[17] Saurabh Sharma, Dr. Rashi Agarwal, "Optimizing QoS Parameters Using Computational Intelligence in MANETS", ISBN: 978-1-5090-6471-71 IEEE., pp. 708-715, 2017.