Techno.COM, Vol. 17, No. 4, November 2018 : 384-394

Penerapan Metode *Filtering Video Streaming* dan *Malware* Pada Jaringan *Local Area Network*

Implementation of Filtering Video Streaming Method and Malware On Local Area Network

Dwi Nurmasari Pratiwi[1], Denar Regata Akbi[2]
[1,2]Teknik Informatika, Universitas Muhammadiyah Malang, Jl. Raya Tlogomas No. 246, Malang, 65144, Indonesia
e-mail: [1]nurmasari.np@gmail.com, [2]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 rekomendasii ITU-T.

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

Abstract

A computer networking is a network connection of computer that will provide access to service applications. Video Streaming is a service that can consume huge bandwidth so that it can cause other access services cannot get enough bandwidth. In addition, LAN network highly vulnerable to be penetrated by malware that makes the network is frequently down and unstable. Therefore, it is necessary for network security and filtering services. By utilizing the router mikrotik with filtering port firewall can minimize the spread of malware and reduce bandwidth usage. This study was conducted by means of literature study, design, implementation, and test analysis. The result of performance testing prior to the implementation of port filtering on the LAN network showed the bandwidth value of 98.04 Mbits, Jitter 0.046 ms, and Packet loss 0.3 ms. While the testing value of QoS after implementation of filtering port showed the result of bandwidth 364 Mbits, Jitter 0,022, and packet loss 0,047. The performance is more stable and showed a good performance on the implementation of filtering streaming video port. The test results have increased and decreased the performance values that are still in standard ITU-T recommendations.

Keywords— *Mikrotik OS, Computer Networking, 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].

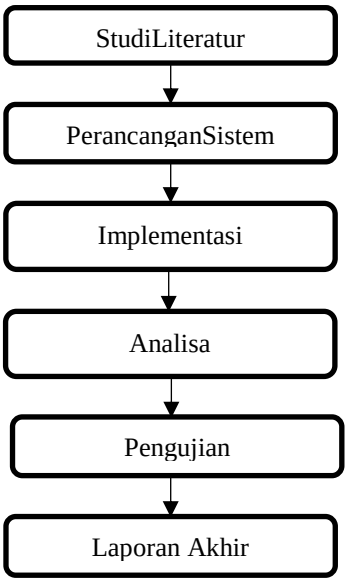
Namun, terdapat informasi kini menjadi trending adalah *video streaming*. *Video streaming* adalah sebuah layanan visual video yang dapat diputar tanpa harus men*download* terlebih dahulu[5]. Akan tetapi video streaming sangat boros *bandwidth*. Sehingga membuat jaringan sering *down* dan kurang stabil. 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 Dedi Irawan dengan judul "Keamanan Jaringan Komputer Dengan Metode Blocking Port Pada Laboratorium Komputer Program Diploma-II Sistem Informasi Universitas Muhammadiyah Metro", membangun keamaan jaringan computer menggunakan metode blocking port. Blocking port diimplemenasikan system operasi Router OS Mikrotik dan menggunakan fitur firewall untuk mendrop port komunikasi yang rentang sekali oleh virus[6]. Kemudian penelitian Imam Riadi dengan judul "Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik", implementasi menggunakan mikrotik dengan fitur firewall untuk efektifitas dari router pengujian menggunakan metode stress test[9]. Kemudian pada penelitian Sumardi, Ramadhian Agus Triyono dengan judul "Rancang Bangun Sistem Keamanan Jaringan Dengan Metode Blocking Port Pada Sekolah Mengengah Kejuruan Karya Nugraha Boyolali", Merancang bangun jaringan menggunakan metode Blocking pot yang memiliki tujuan agar jaringan stabil dan lebih kuat. Pada implementasi ini menghasilkan efektivitas jaringan lebih stabil dengan menggunakan metode blockin port[3].

Pada penelitian ini akan dilakukan implementasi dengan menerapakan filtering port 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:

- *Filtering* menggunakan *firewall winbox*
- Implementasi mikrotik dan ubuntu server pada *virtual box*
- Konfigurasi IP
- *Filtering youtube* saat
- *Filtering malware*
- *Monitoring* jaringan
- 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:

- Analisa menggunakan paramter *bandwidth, jitter*, dan *packet loss*.

- Analisa dilakukan saat implementasi *filtering port* dan sebelum *filtering port*.

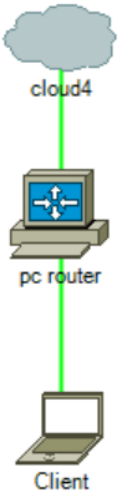
2.4. Skenario Pengujian

Skenario pengujian gambar 1 dilakukan 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*. Instalisasi Ubuntu server kemudian setting dengan menggunakan ip 192.168.2.1. Lalu proses berlanjut dengan melakukan instalisasi mikrotik dengan ip 10.0.2.15. Pengujian dilakukan dengan menganalisa Bandwidth, jitter, dan packet loss.



Gambar 2. Rancangan Jaringan

3.1. Blocking Port Malware

Kinerja dari bloking port malware yaitu dengan cara menutup jalan port yang rentan oleh masuknya virus kedalam jaringan. Setting blocking port menggunakan mikrotik dengan memanfaatkan fitur firewall. fitur ini berfungsi untuk filtering koneksi pada jaringan. Jika firewall sudah tersetting secara otomatis seluruh port yang sudah diblock/filter tidak dapat di kunjungi oleh client. Port yang tidak terfilter oleh mikrotik, saat client request ke server layanan akan dibalas oleh server sesuai dengan permintaan dari client. Blocking port ini sangatlah efisien digunakan, karena dapat meminimalisir virus dari port yang tidak terpercaya masuk dalam sebuah jaringan.

Berikut ini adalah script yang dimasukkan ke terminal untuk melakukan blocking port:

```
[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
```

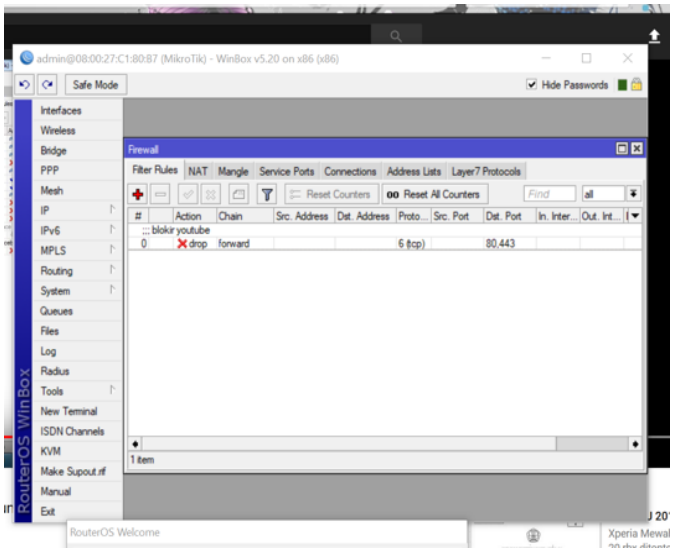
```
action=drop comment="Trinoo" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp
dst-port=31335
action=drop comment="Trinoo" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=virus protocol=udp
dst-port=31846
action=drop comment="Trinoo" disabled=no
[admin@MikroTik] /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

Proses blocking port ini dengan menutup situs youtube. Saat situs ini diblock/difilter dengan menggunakan fitur firewall, client melakukan request terhadap situs ini tidak akan bisa dilayani. Blocking port pada youtube membuat jaringan stabil karena hemat bandwidth. Berikut ini adalah proses block port pada 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.

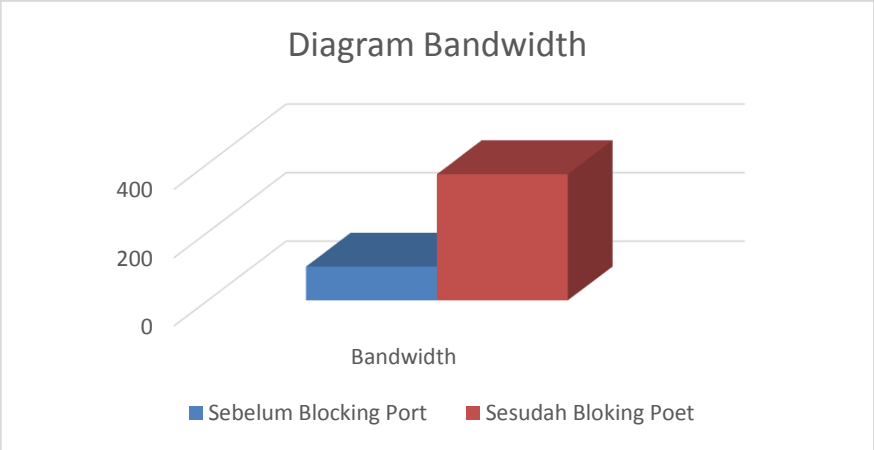
Tabel 1. Hasil Pengujian

	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.

a. Pengukuran performansi pada *Bandwidth*

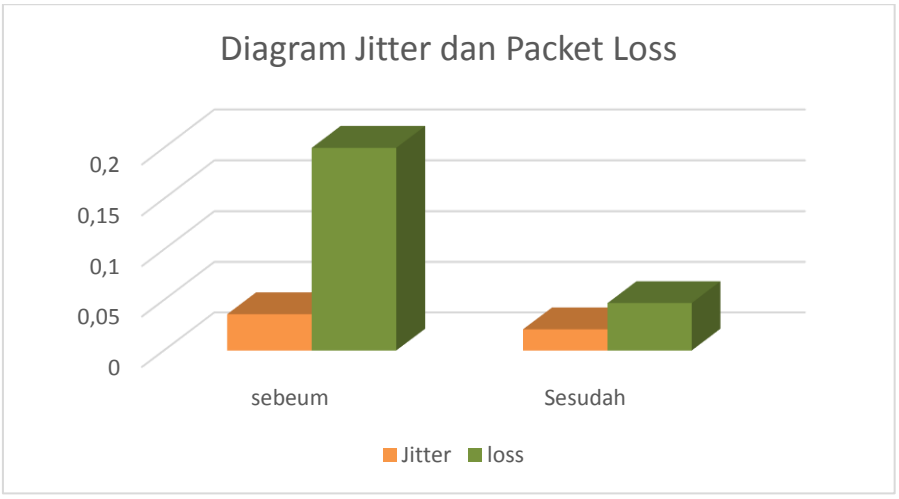
Diagram bandwidth hasil pengujian mengalami perbedaan yang sangat jauh . Kenaikan *bandwidth* terjadi saat *filtering port video streaming* dan *malware* diimplementasikan. Video streaming terlihat sangat mempengaruhi penggunaan *bandwidth*. Pengurangan penggunaan *bandwidth* berkurang karena adanya *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

b. 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 6. Diagram Jitter dan Packet loss

4. KESIMPULAN

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.

5. SARAN

Adapun saran sebagai pengembangan *filtering* jarigan LAN adalah sebagai berikut:

1. Menggunakan berbagai topologi, seperti topologi *star, ring, tree*, dan lain-lain.
2. Menambah skenario pengujian.
3. Menambah parameter pengujian dalam bidang jaringan, contoh *Round Trip Time* (RTT), QoS, monitoring jaringan, dan lain-lain.

DAFTAR PUSTAKA

[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] F. P. P. Agus Teddyana, "Pemanfaatan Remote Access Untuk Memonitoring Komputer Di Laboratorium Jaringan Komputer Politeknik Negeri Bengkalis," *Telekomun. dan Inform. (SELISIK 2016)*, no. 2503–2844, 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] I. Riadi, "Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik Pendahuluan Landasan Teori," *JUSI, Univ. Ahmad Dahlan Yogyakarta*, 2011.