

IMPLEMENTASI WEB FILTERING FIREWALL UNTUK MENDUKUNG INTERNET SEHAT DI SMP NEGERI 4 MAULIRU

(Implementation Of Web Filtering Firewall To Support a Healthy Internet At SMP Negeri 4 Mauliru)

Andri Umbu Wuhi¹, Fajar Hariadi², Novem Berlian Uly³

^{1,2}Program Studi Teknik Informatika, Universitas Kristen Wira Wacana Sumba

³Program Studi Sistem Informasi, Universitas Kristen Wira Wacana Sumba

E-mail: ¹andriumbuwuhi13@gmail.com, ²fajar@unkriswina.ac.id, ³novemuly@unkriswina.ac.id

KEYWORDS:

Firewall, Web Filtering, Healthy Internet.

ABSTRACT

At SMP Negeri 4 Mauliru it supports healthy internet but this is only in the form of an appeal but there is no technology that has really been implemented to implement healthy internet for this reason it is necessary to implement a web filtering firewall using a proxy to prevent student teachers from accessing pornographic sites , online gambling and online games. The aim of this research is to implement a web filtering firewall on the internet network at SMP Negeri 4 Mauliru to support the creation of a healthy internet. This research adopts a web proxy approach which aims to filter inappropriate content. This method involves the use of a web proxy to block access to web content based on certain keywords in online game blocking using ports. Based on the implementation results, it was found that pornographic sites, online gambling and online games could be blocked and after blocking had an impact on increasing network quality on the internet network at SMP Negeri 4 Mauliru with a throughput presentation of 385%, reducing packet loss by 98%, increasing delay of 22.40%, reducing jitter by 81%.

KATA KUNCI:

Firewall, Web Filtering, Internet Sehat.

ABSTRAK

Di SMP Negeri 4 Mauliru itu mendukung internet sehat namun selami ini hanya di dalam bentuk himbauan tapi belum ada teknologi yang betul – betul diterapkan untuk melakukan penerapan internet sehat untuk itu perlu diterapkan web filtering firewall dengan menggunakan mikrotik untuk mencegah siswa – siswi guru mengakses situs pornografi, judi online dan game online. Tujuan penelitian ini adalah menerapkan web filtering firewall pada jaringan internet di SMP Negeri 4 Mauliru untuk mendukung terciptanya internet sehat. Penelitian ini mengadopsi pendekatan web proxy yang bertujuan untuk memfilter konten yang tidak sesuai. Metode ini melibatkan penggunaan web proxy untuk menghalangi akses ke konten web berdasarkan kata kunci tertentu dalam pemblokiran game online menggunakan port. Berdasarkan hasil penerapan didapatkan hasil bahwa dari situs pornografi, judi online dan game online itu dapat diblokir dan setelah dilakukan pemblokiran berdampak pada kenaikan kualitas jaringan pada jaringan internet di SMP Negeri 4 Mauliru dengan presentasi throughput sebesar 385%, menurunkan packet loss sebesar 98%, meningkatkan delay sebesar 22.40%, menurunkan jitter sebesar 81% .

PENDAHULUAN

Dengan evolusi teknologi yang terus berlanjut, kebutuhan akan komunikasi antar manusia semakin penting. Internet menjadi salah satu teknologi yang sangat dibutuhkan dalam kehidupan sehari-hari, memfasilitasi komunikasi, meningkatkan pengetahuan, dan mendukung berbagai pekerjaan yang terkait dengan teknologi internet. Salah satu lembaga yang memerlukan akses internet adalah sekolah, yang merupakan institusi formal untuk proses pembelajaran. Sekolah memiliki tanggung jawab untuk meningkatkan kualitas pendidikan, dan internet dapat menjadi alat yang sangat berguna dalam mendukung proses belajar-mengajar dan aktivitas pendidikan lainnya.

Web filtering firewall adalah teknologi keamanan jaringan yang mengontrol lalu lintas data masuk ke dalam jaringan dengan memutuskan mana yang diperbolehkan dan mana yang diblokir berdasarkan kriteria tertentu terkait konten web[1]. Penggunaan internet sering kali menyebabkan kecanduan pada anak-anak dan remaja, yang dapat mempengaruhi perubahan dalam pola sikap mereka dan mengakibatkan ketidakstabilan emosional, walaupun tidak selalu berujung pada perilaku kenakalan remaja yang memerlukan intervensi khusus[2]. Jika penggunaan internet oleh anak-anak tidak diawasi dengan baik oleh orang tua, hal ini dapat berdampak negatif pada kehidupan sosial, psikologis, dan bahkan akademik mereka[3]. Internet sehat membantu melindungi kesehatan mental siswa dengan menyediakan akses yang aman dan terawasi ke konten-konten yang mendukung pertumbuhan positif. Ini membantu mencegah dampak negatif seperti kecanduan, *cyberbullying*, atau akses ke konten yang tidak sesuai.

SMP Negeri 4 Mauluru adalah lembaga pendidikan yang berada di Mauluru Kec. Kampera Kab. Sumba Timur yang mau juga mendukung tercapainya internet sehat dan aman ini. Dengan jumlah siswa sebanyak 335 dengan jumlah guru 25 orang. Salah satu bentuk dukungan SMP Negeri 4 Mauluru terhadap internet sehat disekolah adalah dukungan terhadap internet sehat di SMP Negeri 4 Mauluru selama ini guru-guru hanya melakukan anjuran, ceramah dan himbauan terhadap siswa-siswi SMP Negeri 4 Mauluru dalam penggunaan internet yang sehat di sekolah bentuk dukungan ini masih kurang cukup apabila tidak didukung dengan teknologi yang betul-betul bisa membatasi akses siswa-siswi terhadap konten-konten negatif tetapi belum ada bentuk dukungan secara nyata dengan menggunakan teknologi.

Adapun tujuan dan alasan diterapkan *web filtering firewall* pada jaringan internet di SMP Negeri 4 Mauluru adalah untuk mendukung terciptanya internet sehat dan melindungi siswa – siswi SMP Negeri 4 Mauluru dari mengakses konten *online* yang tidak pantas atau berbahaya, seperti situs dewasa, kekerasan, atau perjudian. Tindakan ini bertujuan untuk menciptakan lingkungan belajar yang aman dan mendukung bagi para siswa. Siswa-siswi juga dapat meningkatkan fokus pada pembelajaran dengan menghalangi akses ke situs-situs yang tidak terkait dengan pembelajaran, *web filtering firewall* membantu meningkatkan fokus siswa pada materi pelajaran.

Penelitian ini diharapkan memberikan manfaat dengan menerapkan Implementasi *Web Filtering Firewall* Untuk Mendukung Internet Sehat Di SMP Negeri 4 Mauluru adalah diharapkan dapat memberikan manfaat berupa pembatasan akses siswa dan guru terhadap konten-konten negatif, judi *online* dan *game online* di internet. Dan di harapkan siswa-siswi tidak dapat lagi mengakses situs-situs yang telah di blokir, Siswa-siswi diharapkan juga dapat lebih fokus pada pembelajaran karena tidak dapat mengakses situs-situs yang bersifat negatif.

Anak-anak bisa mengakses konten pornografi melalui internet, media sosial, iklan, permainan, film, atau klip video. Ketika mereka melihat konten pornografi, baik secara sengaja maupun tidak sengaja, hal ini bisa membangkitkan rasa ingin tahu yang mendorong mereka untuk mencari lebih banyak konten serupa.[4].

Perjudian adalah aktivitas di mana para pemain bertaruh dengan memilih salah satu dari beberapa opsi yang tersedia, di mana hanya satu opsi yang benar dan akan menang. Pemain yang kalah dalam taruhan akan memberikan taruhannya kepada pemenang[5].

Game online adalah permainan yang dimainkan melalui koneksi internet atau terhubung ke dalam jaringan internet[6]. Umumnya, jenis-jenis jaringan yang digunakan termasuk jaringan internet, modem, dan koneksi kabel

METODE PENELITIAN

Metode berikut diadopsi sebagai tahap penelitian dalam penelitian ini.



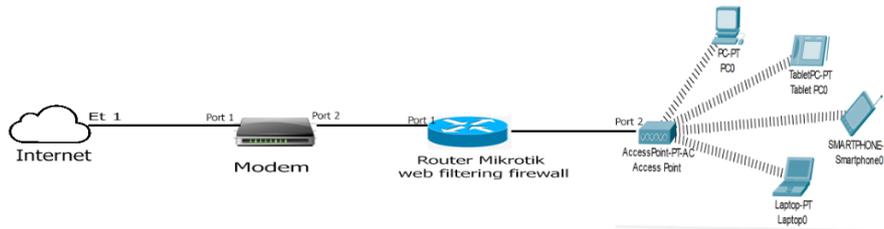
Gambar 1. Alur Perancangan Web *Filtering Firewall*

Tahapan – tahapan yang dilakukan sebagai berikut : Langkah pertama Analisis : Peneliti melakukan wawancara dan observasi di SMP Negeri 4 Mauliru pada tanggal 16 April 2024 yang berfokus pada penggunaan jaringan internet di SMP Negeri 4 Mauliru dengan ISP Bakti Kominfo dan didapatkan bahwa belum ada penerapan *filtering* pada *mikrotikRB760iGS* di SMP Negeri 4 Mauliru sehingga penggunaan jaringan internet di SMP Negeri 4 Mauliru masih bebas setelah itu peneliti melakukan pengujian awal terhadap situs pornografi, judi *online* dan *game online* menggunakan jaringan internet di SMP Negeri 4 Mauliru sebelum penerapan web *filtering firewall* pada *mikrotik* di SMP Negeri 4 Mauliru didapatkan masih bisa diakses menggunakan jaringan internet di sekolah. Hardware yang dibutuhkan pada penelitian ini adalah *Router Mikrotik* adalah sistem operasi dan perangkat lunak yang mengubah PC biasa atau perangkat keras *MikroTik RouterBoard* menjadi sebuah *router*. Pengembangan pertama *MikroTik* dilakukan di Latvia oleh John Truly dan Arnis Riekstins sekitar tahun 1996. *MikroTik* hadir dalam dua jenis, yaitu versi perangkat lunak yang dapat di *instal* pada komputer pribadi, dan versi perangkat keras yang sudah terintegrasi atau dikenal sebagai *RouterBoard*[7]. Langkah kedua desain : Rancangan untuk menerapkan web *filtering firewall* dengan mengonfigurasi *router mikrotik* untuk menyaring dan memblokir situs-situs yang negatif, judi *online* dan *game online* yang mengganggu mental atau konsentrasi siswa-siswi SMP Negeri 4 Mauliru dalam belajar. Langkah ketiga implementasi : untuk mengonfigurasi menggunakan *software winbox* dalam pemblokiran situs pornografi dan judi *online* menggunakan kata kunci lalu diblokir menggunakan *regular expression*. Langkah – langkah dalam pemblokiran situs pornografi dan judi *online* yaitu pertama kita masuk dalam *winbox* yang sudah terhubung dengan *router mikrotik*, pada situs pornografi ada 10 kata kunci yang digunakan dalam pemblokiran situs dan 7 kata kunci yang digunakan dalam pemblokiran situs judi *online*. Untuk melakukan pemblokiran menggunakan *regular expression* pilih menu IP lalu kita pilih DNS dan pilih *Static* maka kita akan masuk pada tampilan DNS *Static* lalu klik tanda tambah (+) maka akan muncul tampilan DNS *Static Entry* pada halaman inilah peneliti melakukan pemblokiran menggunakan *regular expression*. Pada kolom *Regexp* kita isikan kata kunci dari situs pornografi atau situs judi *online* seperti gambar. 3 dibawah lalu klik *apply* dan ok. *Winbox* adalah sebuah *utility* yang digunakan untuk melakukan *remote* ke server *mikrotik* kita dalam mode GUI[8]. Langkah keempat Pengujian : Pengujian dilakukan dengan 2 cara yaitu dengan membandingkan antara pengujian awal setiap situs yang masih bisa diakses tersebut, apakah setelah penerapan web *filtering firewall* masih bisa diakses atau tidak dan didapatkan bahwa situs judi pornografi, judi *online* dan *game online* tidak bisa lagi diakses setelah penerapan web *filtering firewall* dengan menggunakan jaringan internet di SMP Negeri 4 Mauliru. Selain itu juga akan dilakukan pengukuran QOS ulang berupa *trouputh*, *delay*, *jitter*, dan *packet loss* dengan menggunakan *software wireshark* untuk membandingkan kualitas jaringan sebelum penerapan *firewall* dan sesudah penerapan *firewall* di SMP Negeri 4 Mauliru. *Wireshark* adalah sebuah perangkat lunak analisis protokol jaringan yang komprehensif. Program ini mampu merekam semua paket data yang melewati jaringan, serta menyaring dan menampilkan informasi tersebut dengan tingkat detail yang tinggi[9] Hasil akhir : Pada bagian analisis hasil

akhir akan dilakukan perbandingan antara pengujian awal dan pengujian akses internet situs negatif, judi *online* dan *game online* setelah penerapan *web filtering firewall* di SMP Negeri 4 Mauluru.

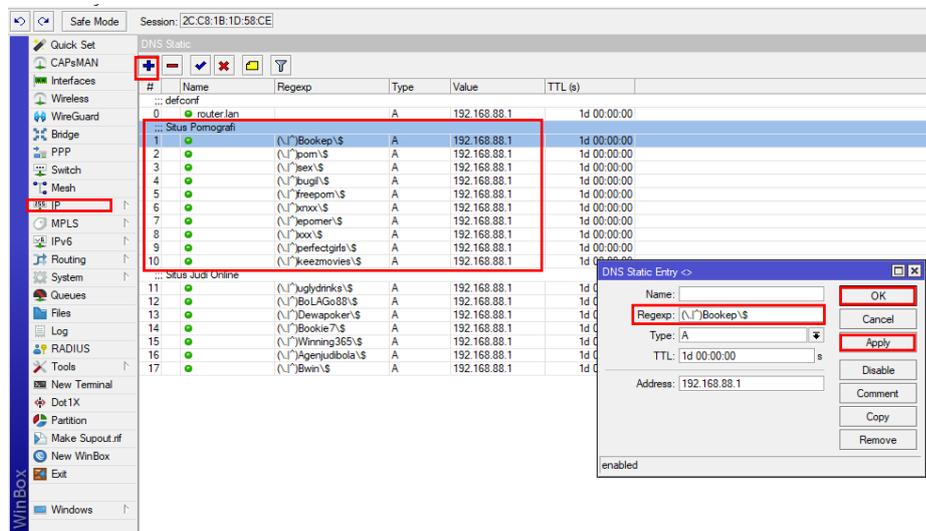
HASIL DAN PEMBAHASAN

Dalam penelitian ini penulis telah mempersiapkan desain topologi jaringan untuk implementasi *web filtering firewall* yang berisi ISP Bakti Kominfo, Modem, Mikrotik Router, dan *access point* yang terhubung dengan internet. Desain jaringan lokal pada penelitian ini seperti pada Gambar 2



Gambar 2. Topologi Jaringan Setelah Penerapan Web Filtering Firewall

a. Proses pemblokiran situs – situs Pornografi



Gambar 3. Tampilan Pemblokiran Situs Pornografi

Dalam pemblokiran situs pornografi menggunakan kata kunci lalu diblokir menggunakan *regular expression*. Langkah – langkah dalam pemblokiran situs pornografi yaitu pertama kita masuk dalam *winbox* yang sudah terhubung dengan *router mikrotik*, setelah itu pilih menu IP lalu kita pilih DNS dan pilih *Static* maka kita akan masuk pada tampilan di atas pada situs pornografi ada 10 kata kunci yang digunakan dalam pemblokiran situs pornografi. Untuk melakukan pemblokiran menggunakan *regular expression* kita klik tanda tambah (+) maka akan muncul tampilan *DNS Static Entry* pada halaman inilah peneliti melakukan pemblokiran menggunakan *regular expression*. Pada kolom *Regexp* kita isikan kata kunci dari situs pornografi seperti gambar di atas lalu klik *apply* lalu *ok*. Daftar *regexp* yang dipakai dapat diperhatikan pada tabel berikut:

Tabel 1. Daftar *regexp* Situs Pornografi

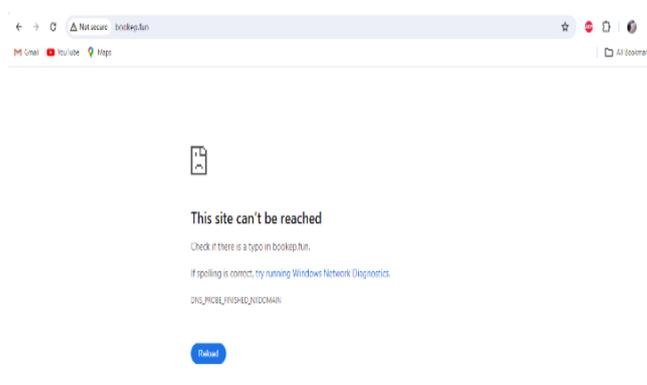
Nama Situs	Filter Regexp
	(\)Bookep\S (\)porn\.com\S (\)sex\.com\S (\)bugil\S

Situs Pornografi	(\./^)^freeporn\.\$ // (\./^)^xnxx\.\$ // (\./^)^eporner\.\$ // (\./^)^xxx\.\$ // (\./^)^perfectgirls\.\$ // (\./^)^keezmovies\.\$
------------------	--

Setelah dilakukan pemblokiran maka situs *Bookep* akan terblokir secara otomatis jika ada yang mengaksesnya dengan menggunakan jaringan internet di SMP Negeri 4 Mauluru. Pengujian pada situs yang telah diblokir menggunakan *regular expression* diuji dengan menggunakan browser.



a)

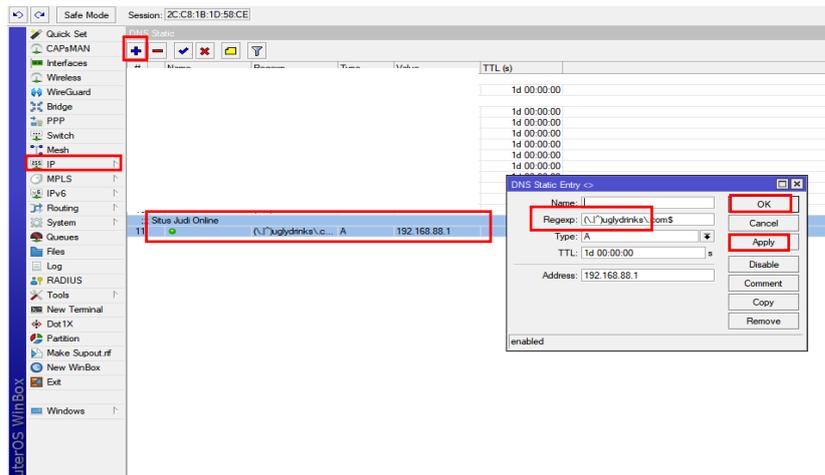


b)

Gambar 4. a) Tampilan Situs Sebelum di Blokir, b) Tampilan Situs Setelah di Blokir

Akses ke domain *bookep.fun* akan diblokir sehingga halaman web tidak akan ditampilkan atau tidak dapat diakses seperti pada Gambar 4. b).

b. Proses pemblokiran situs – situs Judi online



Gambar 5. Tampilan Pemblokiran Situs Judi Online

Pada pemblokiran situs judi *online* sama hal cara pemblokiran situs pornografi menggunakan kata kunci lalu diblokir menggunakan *regular expression*. Langkah – langkah dalam pemblokiran situs judi *online* yaitu pertama kita masuk dalam *winbox* yang sudah terhubung dengan *router mikrotik*, setelah itu pilih menu IP lalu kita pilih DNS dan pilih *Static* maka kita akan masuk pada tampilan di atas pada situs judi *online* ada 7 kata kunci yang digunakan dalam pemblokiran situs judi *online*. Untuk melakukan pemblokiran menggunakan *regular expression* kita klik tanda tambah (+) maka akan muncul tampilan *DNS Static Entry*

pada halaman inilah peneliti melakukan pemblokiran menggunakan *regular expression*. Pada kolom *Regex* kita isikan kata kunci dari situs judi *online* seperti gambar di atas lalu klik *apply* lalu ok.

Daftar *regex* yang dipakai dapat diperhatikan pada tabel berikut:

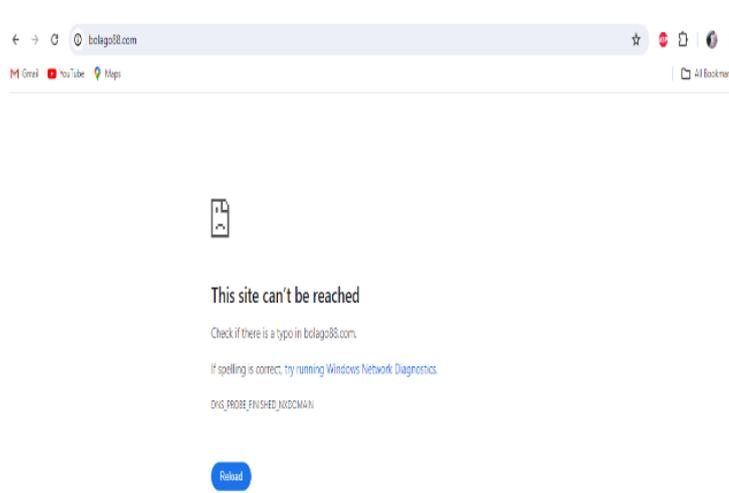
Tabel 2. Daftar *Regex* Judi Online

Nama Situs	Filter <i>Regex</i>
Situs Judi Online	(\./^) <i>uglydrinks</i> \\$ // (\./^) <i>BoLAGo88</i> \\$ // (\./^) <i>Dewapoker</i> \\$ // (\./^) <i>Bookie7</i> \\$ // (\./^) <i>Winning365</i> \\$ // (\./^) <i>Agenjudibola</i> \\$ // (\./^) <i>Bwin</i> \\$

Setelah dilakukan pemblokiran maka situs *uglydrinks* akan terblokir secara otomatis jika ada yang mengaksesnya dengan menggunakan jaringan internet di SMP Negeri 4 Mauluru. Pengujian pada situs yang telah diblokir menggunakan *regular expression* diuji dengan menggunakan browser.



a)

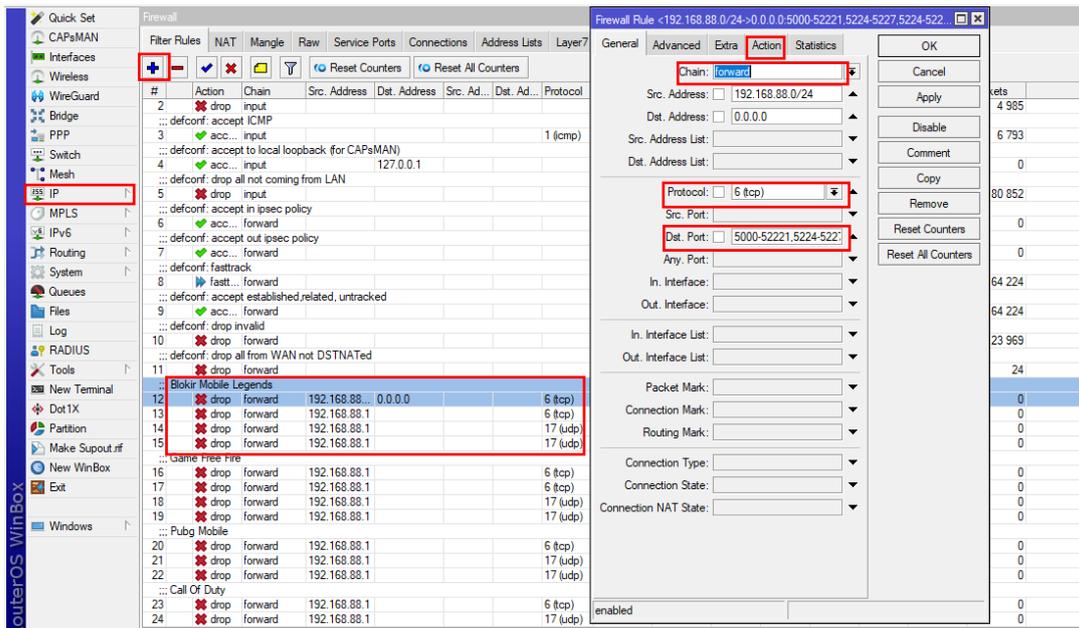


b)

Gambar 6. a) Tampilan Situs Sebelum di Blokir, b) Tampilan Situs Setelah di Blokir

Akses ke domain *uglydrinks* akan diblokir sehingga halaman web tidak akan ditampilkan atau tidak dapat diakses seperti pada Gambar 6. b).

c. Proses Pemblokiran *Game Oline*



Gambar 7. Proses Pemblokiran *Game Mobile legends*

Dalam pemblokiran *game online* dengan cara menggunakan *port tcp* dan *port udp* dari *game*. Langkah – langkah dalam pemblokiran *game online* yaitu pertama kita masuk dalam *winbox* yang sudah terhubung dengan *router mikrotik*, setelah itu pilih menu *IP* lalu kita pilih *firewall* maka kita akan masuk pada tampilan di atas. Untuk melakukan pemblokiran menggunakan *port – port* dari *game online* kita klik tanda tambah (+) maka akan muncul tampilan *firewall rule* pada halaman inilah peneliti melakukan pemblokiran menggunakan *port game online*. Pada kolom *chain* kita pilih *forward* lalu di bagian *protocol* kita pilih *tcp* dan di bagian *Dst. Port* kita masukkan *port game online* yang termasuk dalam *port tcp* seperti pada gambar di atas.



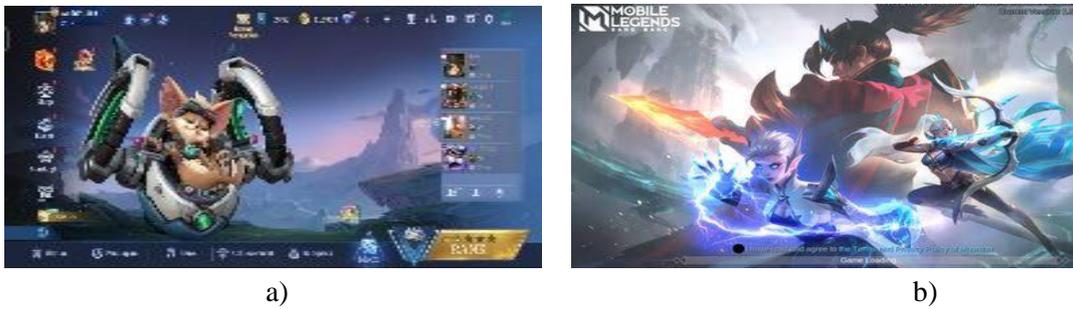
Gambar 8. Pada Tab *Action* Pilih *Drop*

Setelah melakukan setingan pada gambar 7 kita masuk di tab *action*, pada tab *action* ini kita pilih *drop* lalu *apply* dan klik *ok*. Daftar *port udp* dan *tcp* yang digunakan dapat dilihat pada tabel berikut:

Tabel 3. Daftar *Port Game Online*

Nama Game	Port Yang Digunakan
<i>Mobile Legends</i>	TCP : 5000-52221, 5224-5227, 5224- 5227, 5229-5241, 5243-5287, 5289-5352,5354-5509,5517,5520-5529 TCP : 5551-5569, 56015700, 8443, 9000-9010, 9443, 10003, 30000-30900 UDP : 2702, 3702, 4001-4009, 5000-5221, 5224-5241, 5243-5287, 5289-5352, 5354-5509 UDP : 5507, 5517-5529, 5551-5569, 5601-5700, 8001, 8130
<i>Free Fire</i>	TCP : 6006, 6008, 6674, 7000-7999, 8001-8012, 9006, 9137, 10000-10015, 11000-11019 TCP : 12006, 12008, 13006, 15006, 20561, 39003, 39006, 39698, 39779, 39800 UDP : 6006, 6008, 6674, 7000-7999, 8008, 8001-8012, 8130, 8443, 9008, 9120 UDP : 10000-10015, 10100, 11000-11019, 12008, 13008.
<i>PUBG Mobile</i>	TCP : 7889,10012,13004,14000,17000,17500,18081,20000-20002,2037 UDP : 8011, 9030, 10491, 10612, 12235, 13004, 13748, 14073, 17000, 17500, 20000-20002 UDP : 7086-7995, 10039, 10096, 11096, 11455, 12070-12460, 13894, 13972, 41182-41192.
<i>Call of Duty (COD Mobile)</i>	TCP : 3013, 10000-10019, 18082, 50000, 65010, 65050. UDP : 7085-7995, 8700, 9030, 10010-10019, 17000-20100.

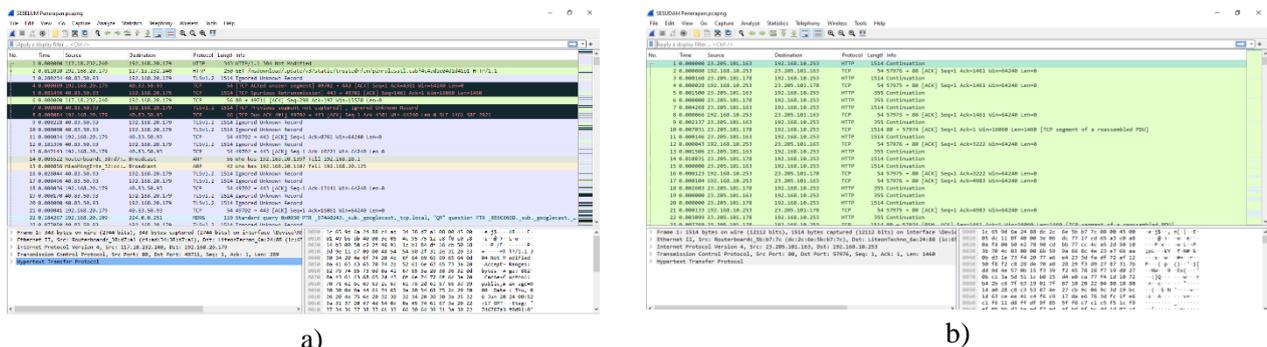
Pengujian pada *game online* yang telah diblokir dilakukan dengan cara mengakses *game mobile legends* tersebut.



Gambar 9. a) Tampilan *Game* Sebelum di Blokir, b) Tampilan *Game* Setelah di Blokir

Saat mengakses *game mobile legends* akan menghasilkan tampilan seperti pada Gambar 9. b) karena aksesnya diblokir sehingga *game mobile legends* akan *loading* dan tidak bisa masuk di dalam *game* tersebut.

Quality of Service (QoS) adalah suatu metode untuk mengukur dan mengelola performa serta kualitas dalam sebuah jaringan[10]. Berbagai layanan memiliki kebutuhan yang berbeda dalam hal performansi seperti throughput, packet loss, delay, dan jitter. Selain dilakukan pengujian terhadap keberhasilan akses dan pemblokiran dilakukan juga pengujian QOS sebelum dan sesudah implementasi web *filtering firewall*.



Gambar 10. a) Hasil *capture* sebelum penerapan *filtering*, b) hasil *capture* setelah penerapan *filtering*.

Dari hasil *capture* tersebut dilakukan perhitungan *throughput*, *packet loss*, *delay* dan *jitter* sebelum penerapan *web filtering firewall* dan setelah penerapan *web filtering firewall*.

a. *Throughput*

$$\begin{aligned} \text{Throughput} &= \frac{\text{Jumlah byte}}{\text{time span}} \\ \text{Throughput} &= \frac{26996993 \text{ byte}}{526.957 \text{ second}} \\ \text{Throughput} &= 51231.87091 \text{ Bps} \\ \text{Throughput} &= 51231.87091 \times 8 \text{ bps} \\ \text{Throughput} &= 409.85 \text{ kbps} \end{aligned}$$

$$\begin{aligned} \text{Throughput} &= \frac{\text{Jumlah byte}}{\text{time span}} \\ \text{Throughput} &= \frac{141923106 \text{ byte}}{571.167 \text{ second}} \\ \text{Throughput} &= 248479.1768 \text{ Bps} \\ \text{Throughput} &= 248479.1768 \times 8 \text{ bps} \\ \text{Throughput} &= 1987.83 \text{ kbps} \end{aligned}$$

b. *Packet Loss*

$$\begin{aligned} \text{Packet Loss} &= \frac{\text{Paket Hilang}}{\text{paket dikirim}} \\ \text{Packet Loss} &= \frac{2791}{46679} \\ \text{Packet Loss} &= 0.059791341 \\ \text{Packet Loss} &= 0.059791341 \times 100 \\ \text{Packet Loss} &= 5.98\% \end{aligned}$$

$$\begin{aligned} \text{Packet Loss} &= \frac{\text{Paket Hilang}}{\text{paket dikirim}} \\ \text{Packet Loss} &= \frac{176}{193119} \\ \text{Packet Loss} &= 0.000911355 \\ \text{Packet Loss} &= 0.059791341 \times 100 \\ \text{Packet Loss} &= 0.09\% \end{aligned}$$

c. *Delay*

$$\begin{aligned} \text{Delay} &= \frac{\text{Total Delay}}{\text{paket diterima}} \\ \text{Delay} &= \frac{526.956877}{46679} \\ \text{Delay} &= 0.01128895 \text{ s} \\ \text{Delay} &= 0.01128895 \text{ s} \times 1000 \\ \text{Delay} &= 11.29 \text{ ms} \end{aligned}$$

$$\begin{aligned} \text{Delay} &= \frac{\text{Total Delay}}{\text{paket diterima}} \\ \text{Delay} &= \frac{48859076.62}{193119} \\ \text{Delay} &= 252.9998427 \text{ s} \\ \text{Delay} &= 252.9998427 \text{ s} \times 1000 \\ \text{Delay} &= 25.30 \text{ ms} \end{aligned}$$

d. *Jitter*

$$\begin{aligned} \text{Jitter} &= \frac{\text{Total Variasi Delay}}{\text{paket diterima} - 1} \\ \text{Jitter} &= \frac{761.268265}{46678} \\ \text{Jitter} &= 0.016308931 \text{ s} \\ \text{Jitter} &= 0.016308931 \text{ s} \times 1000 \\ \text{Jitter} &= 16.31 \text{ ms} \end{aligned}$$

$$\begin{aligned} \text{Jitter} &= \frac{\text{Total Variasi Delay}}{\text{paket diterima} - 1} \\ \text{Jitter} &= \frac{571.166757}{193118} \\ \text{Jitter} &= 0.002957605 \text{ s} \\ \text{Jitter} &= 0.002957605 \text{ s} \times 1000 \\ \text{Jitter} &= 2.96 \text{ ms} \end{aligned}$$

KESIMPULAN DAN SARAN

Dengan adanya *web filtering firewall* ditunjukkan dengan hasil pengujian beberapa situs pornografi, judi *online* dan *game online* sudah berhasil dilakukan pemblokiran sedangkan dengan adanya *web filtering firewall* ternyata berhasil meningkatkan *throughput* sebesar 385% di mana *throughput* awal 409.85 kbps sedangkan *throughput* setelah dilakukan *web filtering firewall* menjadi 1987.83 kbps. Dari sisi *packet loss* terjadi penurunan di mana sebelum implementasi didapatkan *packet loss* sebesar 5.98 % sedangkan setelah implementasi hanya sebesar 0.07 % sehingga kualitas jaringan dianggap lebih bagus. Dari sisi *delay* terjadi

penurunan di mana sebelum implementasi didapatkan *delay* sebesar 11.29 ms sedangkan setelah implementasi hanya sebesar 25.30 ms sehingga kualitas jaringan dianggap lebih bagus. Dari sisi *jitter* terjadi penurunan di mana sebelum implementasi di dapatkan *jitter* sebesar 16.31 ms sedangkan setelah implementasi hanya sebesar 4.41 ms sehingga kualitas jaringan dianggap lebih bagus. Dari seluruh parameter tersebut dapat disimpulkan bahwa dengan adanya web *filtering firewall* selain bisa menciptakan internet sehat di SMP Negeri 4 Mauluru dapat juga menghasilkan peningkatan kualitas jaringan.

Saran yang diberikan adalah untuk memastikan bahwa implementasi teknologi *firewall* tidak hanya sekedar tentang memblokir akses yang tidak diinginkan, tetapi juga tentang membentuk kesadaran akan pentingnya penggunaan internet yang bertanggung jawab. Dengan adanya upaya ini, sekolah dapat berperan sebagai garda terdepan dalam melindungi siswa dari konten yang tidak sesuai dan potensial merugikan. Melalui penerapan kebijakan dan teknologi yang tepat, seperti web *filtering firewall*, sekolah dapat membantu membentuk perilaku yang positif dalam penggunaan internet, mempromosikan pendidikan yang aman, produktif, dan etis di dunia digital saat ini.

DAFTAR PUSTAKA

- [1] D. Wicaksono, "Firewall Sistem Keamanan Jaringan Menggunakan Firewall dengan Metode Port Blocking dan Firewall Filtering," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 2, pp. 1380–1392, 2022, doi: 10.35957/jatisi.v9i2.2103.
- [2] W. Yuwono, S. Ng, D. Yosuky, and D. Ng, "Program Internet Sehat Dan Aman Melalui Implementasi Bahan Ajar Digital," *Pros. Natl. Conf. Community Serv. Proj.*, vol. 4, pp. 217–224, 2022.
- [3] Z. Azhar, N. Mulyani, J. Hutahaeen, A. Z. Hasibuan, and H. Sitorus, "Sosialisasi Penggunaan Komputer Dan Internet Sehat Bagi Siswa Siswi Sekolah Menengah Kejuruan," *JMM (Jurnal Masy. Mandiri)*, vol. 7, no. 3, p. 2194, 2023, doi: 10.31764/jmm.v7i3.14251.
- [4] F. Lase and N. Halawa, "Menjaga Dan Mendidik Anak Di Era Digital Terhadap Bahaya Pornografi," *Zadama J. Pengabd. Masy.*, vol. 1, no. 1, pp. 57–68, 2022, doi: 10.56248/zadama.v1i1.21.
- [5] R. September, R. September, and A. September, "Perkembangan Judi Online dan Dampaknya Terhadap Masyarakat : Tinjauan Multidisipliner," *Triwikama J. Ilmu Sos.*, vol. 01, no. 05, pp. 1–7, 2023, [Online]. Available: <https://ejournal.warunayama.org/index.php/triwikrama/article/view/248/239>
- [6] N. Kurnada and R. Iskandar, "Analisis Tingkat Kecanduan Bermain Game Online terhadap Siswa Sekolah Dasar," *J. Basicedu*, vol. 5, no. 6, pp. 5660–5670, 2021, doi: 10.31004/basicedu.v5i6.1738.
- [7] U. M. Deni Ahmad, I. Sehat, D. A. N. Aman, T. Informatika, and S. Dci, "Jurnal teknik informatika," vol. 8, no. 2, 2020.
- [8] Didi Susianto, "Implementasi Queue Tree Untuk Manajemen Bandwidth Menggunakan Router Board Mikrotik," *J. Cendikia Vol 12No. 1Cendikia 2016 ISSN 0216-9436 Bandar Lampung, April 2016*, vol. 12, no. 1, pp. 1–8, 2019.
- [9] Reivaldi Kesuma, "Desain Dan Implementasi Pada Wifi Pustikom Free Access Di Pusat Teknologi Informasi Dan Komunikasi Universitas Negeri Jakarta Menggunakan Mikrotik Dan Wireshark Untuk Analisis Terhadap Serangan Packet Sniffing Dan Netcut," *PINTER J. Pendidik. Tek. Inform. dan Komput.*, vol. 4, no. 2, pp. 37–40, 2020, doi: 10.21009/pinter.4.2.7.
- [10] R. Hanifia, "Penerapan Quality of Service (QoS) Differentiated Service Pada Jaringan Multi-Protocol Label Switching (MPLS)," *J. Manaj. Inform.*, vol. 9, no. 2, pp. 1–7, 2019.