JRAPIK
VOL. 1 NO. 2 TAHUN 2021
Publishing
Jurnal Ranah Publik Indonesia Kontemporer
https://rapik.pubmedia.id/index.php/rapik

Implementasi Keamanan Jaringan dengan *Packet* Filtering Berbasis Mikrotik Untuk Internet Positif Di SMKN 1 Praya

Sumardi Jayanto[1*)], Ahmad Tantoni[2], Hasyim Asyari[3]

[1,2,3]*Program Studi Teknik Informatika, STMIK Lombok*
[1]*sumardiljk1987@gmail.com*, [2]*ahmad.tantoni@students.amikom.ac.id*, [3]*hasyimasyari25@gmail.com*

ARTICLE INFO

Article history:
Received 03/11/2021
Received in revised form 30/11/2021
Accepted 01/12/2021

Abstract

SMKN 1 Praya is one of the schools in NTB with national standards. This school has a very broad environment. In addition, this school also has a fairly good internet network. This can be seen by the breadth of the internet network that almost covers the entire school environment. At SMKN 1 Praya the main problem is the use of internet network data by students to be used to play games and social media during study hours so we need a system that is capable of being a protection so that users cannot use the internet to play games and social media during study hours. . Based on this, the study aims to examine the implementation of network security with mikrotic-based packet filtering at SMKN 1 Praya. In general, this study shows the success of blocking several online game applications such as mobile legend, free fire, TOT and social media such as facebook.

Keywords: *Internet Networking, Online Game, Social Media, PPDIOO, Packet Filtering.*

Abstrak

SMKN 1 Praya adalah salah satu sekolah di NTB yang berstandar nasional. Sekolah ini memiliki lingkungan yang sangat luas. Di samping itu pula sekolah ini memiliki jaringan *internet* yang cukup baik. Ini bisa dilihat dengan luasnya jaringan *internet* yang hampir menjangkau seluruh lingkungan sekolah. Di SMKN 1 Praya yang menjadi masalah utamanya adalah pemakaian data jaringan internet oleh siswa digunakan untuk bermain *games* dan media sosial pada saat jam belajar sehingga dibutuhkan sebuah sistem yang mampu menjadi proteksi agar *user* tidak dapat menggunakan internet untuk bermain *games* dan sosial media pada saat jam belajar. Berdasarkan hal tersebut maka penelitian ini bertujuan untuk menguji implementasi kemanan jaringan dengan packet filtering berbasis mikrotik pada SMKN 1 Praya. Secara umum penelitian ini menunjukkan keberhasilan pemblokiran terhadap beberapa aplikasi *games online* seperti *mobile legend*, *free fire*, *TOT* dan sosial media seperti *facebook*.

Kata kunci: *Jaringan Internet, Game Online, Media Sosial, PPDIOO, Packet Filtering.*

*)Penulis Korespondensi
E-mail : sumardiljk1987@gmail.com

PENDAHULUAN

Seiring perkembangan dunia komunikasi saat ini, khususnya penggunaan *internet, internet* saat ini menjadi kebutuhan setiap orang. Salah satunya adalah *internet* dalam dunia pendidikan. Dengan adanya jaringan *internet*, maka guru dan siswa sangat terbantu dalam pencarian materi ataupun referensi-referensi yang sangat luas. Tidak hanya *browsing* untuk mencari informasi ataupun literasi yang dilakukan oleh guru maupun juga siswa, akan tetapi juga dipergunakannya untuk media sosial dan *games online* sehingga menjadikan penggunaan internet ini memiliki dampak negatif terhadap proses pembelajaran. Hal tersebut sangat mengganggu aktivitas belajar siswa di mana siswa lebih banyak menghabiskan waktu dalam penggunaan internet dengan memanfaatkan jaringan sekolah untuk bermain *games online* dan sosial media. Hanya sedikit di antara mereka yang menggunakannya untuk *browsing* untuk mencari materi pelajaran.

Gambaran tersebut diperoleh setelah penulis melakukan prasurvey pada siswa tentang pemanfaatan jaringan *internet* di sekolah. Hasilnya dari 100 orang responden terdapat 30 orang menggunakan jaringan *internet* untuk media sosial 15 orang menggunakan jaringan *internet* untuk keperluan bermain *games online,* sementara 35 orang menggunakannya untuk bermain *games* dan media sosial dan sisanya menjawab mencari tugas sekolah dan menonton *youtube*.

Dari hasil prasurvey maka dapat diperoleh informasi bahwa penggunaan jaringan *internet* di SMKN 1 Praya lebih banyak digunakan untuk media sosial dan *games online* oleh siswa pada saat jam pembelajaran. Oleh karena itu perlu dilakukan pembatasan akses *internet* (terhadap *games* dan sosial media) pada saat jam-jam belajar. Akses *internet* akan diaktifkan secara normal ketika siswa telah selesai melaksanakan proses pembelajaran (pulang sekolah). Hal ini untuk mengurangi ancaman jaringan dari luar akibat penggunaan sosial media dan *games online*.

Berdasarkan informasi di atas, bahwa siswa di SMKN 1 Praya memanfaatkan jaringan internet di sekolah untuk kepentingan yang tidak terkait dengan kebutuhan belajar pada jam pemelajaran, maka penulis melakukan penelitian eksperimental mengenai implementasi keamanan jaringan dengan *Packet Filtering* Berbasis *Mikrotik*. Dengan demikian keberadaan *internet* di lingkungan sekolah dapat diarahkan kepada manfaat *internet* yang positif.

TINJAUAN PUSTAKA

1. Keamanan Jaringan

Sebuah penelitian menyimpulkan bahwa keamanan jaringan merupakan salah satu hal terpenting dalam implementasi jaringan komputer. Sebagian besar jaringan komputer yang mengalami permasalahan yang disebabkan oleh kelalaian pengelola jaringan dalam membangun sebuah jaringan komputer. Hal dapat membuka peluang bagi para *hacker* untuk meretas dan merusak jaringan yang dibangun tersebut. Untuk meminimalisir terjadinya penyalahgunaan jaringan oleh para hecker, maka perlu adanya peningkatan keamanan jaringan yang akan dibangun. Dalam penelitian ini telah dilakukan penelitian untuk mengembangkan keamanan jaringan komputer dengan cara penggunakan metode Port Knocking (Amarudin & Ulum, 2018).

Muzakir dan Ulfa melakukan penelitian yang membahas proses kerja dari sebuah sistem keamanan jaringan. *Firewall* berfungsi sebagai tempat untuk

pemisahan satu lapisan yang menerapkan strategi penyaringan paket *firewall*. Strategi ini melakukan penyaringan bundel informasi tergantung pada batas-batas yang telah ditentukan. Bagaimana strategi ini berfungsi pada tingkat *IP* dari kumpulan informasi dan menentukan pilihan aktivitas yang kemudian pada saat itu, dapat diterima atau ditolak (Muzakir & Ulfa, 2019).

Penelitian tentang *Vulnerability* Keamanan Jaringan *Internet* Menggunakan *Nessus* memberikan kesimpulan jaringan internet pada dasarnya tidak ada yang aman terlebih yang bersifat publik. Untuk mengurangi hal tersebut dapat menggunakan berbagai macam antara lain, metode *authentikasi*, metode *enkripsi-dekripsi*, dan penggunaan *Firewall* (Juardi, 2017).

2. Dampak Negatif Penggunaan Internet

Sisi sosial media memiliki dampak positif dan negatif terhadap perubahan sosial anak (Fitri, 2017). Sisi negatifnya adalah banyak anak-anak yang menjadi anti sosial dimana mereka terlena oleh keasyikan berbincang dalam sosial media dibandingkan bertatap muka langsung dalam dunia nyata. Begitu juga yang terjebak menjadi pemalas dan boros demi melanjutkan keasyikan mereka dalam berbincang di sosial media.

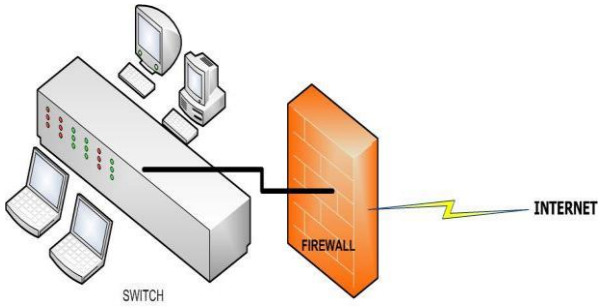
Dalam dunia remaja, internet digunakan lebih banyak untuk tujuan kesenangan Penelitian yang dilakukan terhadap siswa sekolah menengah pertama di Surakarta menunjukkan bahwa sebagian besar siswa menggunakan internet sebagai salah satu aktivitas kesenangan (Saputri, Arifah & Wulaningrum, 2014). Sementara jika penggunaan internet pada remaja tidak diikuti dengan konseling dan sistem filter pada internet sendiri, maka remaja bisa terjebak dalam dampak negatif terhadap perkembangan moral mereka (Ardi, Viola & Sukmawati, 2018). Dengan demikian kecenderungan yang dapat mengantarkan remaja di sekolah pada dampak negative perkembangan moral mereka, dapat diminimalisir dengan sistem filter terhadap internet yang mereka gunakan.

3. Sistem dan Aplikasi untuk Keamanan Jaringan

a. *Firewall*

Firewall adalah sebuah sistem yang mampu melindungi perangkat ataupun *user* yang terhubung pada sebuah jaringan. Pada umumnya *firewall* dibuat untuk melindungi jaringan *Local* dari ancaman dan gangguan yang datang dari luar setelah jaringan tersebut terhubung dengan *internet* (Sofana, 2017).

Firewall memiliki dua bagian penting yang saling membantu satu sama yang lain yaitu *router* dan *application gateway. Router* menjadi *hardware* yang bertugas menjadi pelindung pada pertahanan jaringan sedangkan *application gateway* adalah perangkat lunak yang bertugas khusus untuk melihat dan menganalisa paket yang keluar dan masuk pada jaringan (Revilia & Irwansyah, 2020).



Gambar 1. Cara Kerja *Firewall*

b. *Mikrotik*

Mikrotik adalah sistem operasi dan perangkat keras yang dapat menjadikan jaringan komputer menjadi jaringan yang andal, meliputi berbagai karakteristik yang dibuat untuk jaringan IP *network* dan jaringan nirkabel dan sangat baik jika digunakan pada jaringan *Wi-Fi*. *Mikrotik* dirancang agar mudah dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sistem jaringan komputer kecil hingga kompleks (Hardana & Irvantino, 2011).

Router Mikrotik dapat berfungsi untuk menelusuri jika terjadi penyusupan pada jaringan komputer dan *firewall* bagi komputer dapat memberikan prioritas pada komputer agar dapat mengakses data *internet* maupun jaringan lokal (Fadlil, Riadi, & Aji, 2017).

Gambar 2. *Router Mikrotik*

c. *Cisco Packet Tracer*

Packet tracer adalah sebuah aplikasi yang mampu menjadi simulator jaringan sebelum pembuatan jaringan sebenarnya. Aplikasi ini dikembangkan oleh *Cisco*. Aplikasi ini mempermudah dalam pengembangan jaringan dan pembuatan topologi.

d. *GNS3* (*Graphical Network Simulator 3*)

GNS3 adalah aplikasi yang memiliki fungsi yang sama dengan *packet tracer* yaitu sebagai simulator yang dapat dikembangkan di laboratorium dan nantinya dapat mengikuti pelatihan dan testing seperti *Cisco CCNA, CCNP, CCIP* dan *CCIE* serta *Juniper JNCIA*, *JNCIS* dan *JNCIE*. Perangkat lunak ini bersifat *opensource* yang dapat digunakan pada berbagai paltform sistem operasi seperti *Windows*, *Linux*, dan *Mac OS* X.

METODE PENELITIAN

1. Pengumpulan Data

Dalam melakukan pengumpulan data pada penelitian ini ada beberapa cara yang dilakukan penulis yaitu sebagai berikut:

a. Metode Observasi

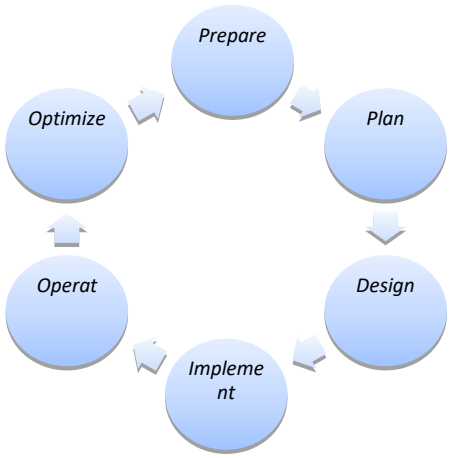
Peneliti langsung melakukan observasi ke ruang laboratorium yang terdapat pada SMKN 1 Praya untuk dapat mendapatkan informasi yang nantinya dijadikan sebagai bahan penelitian.

b. Metode Wawancara

Pada tahapan ini penulis melakukan diskusi dengan beberapa pihak terkait yaitu Kepala Bengkel Teknik Komputer dan Jaringan (TKJ) SMKN 1 Praya hasil dari diskusi tersebut dijadikan rujukan dalam melakukan penelitian.

2. Analisa Data

Dalam penelitian ini penulis melakukan analisis data dengan teknik *PPDIOO* yang terdiri dari *Prepare Plan*, *Design*, *Implement*, *Operate*, *Optimize.* Kebutuhan jaringan yang semakin luas sehingga dibutuhkan sebuah metode yang mendukung perencaan arsitektur dan desain jaringan. *PPDIOO* adalah suatu teknik perancangan jaringan yang diperkenalkan oleh *Cisco*.



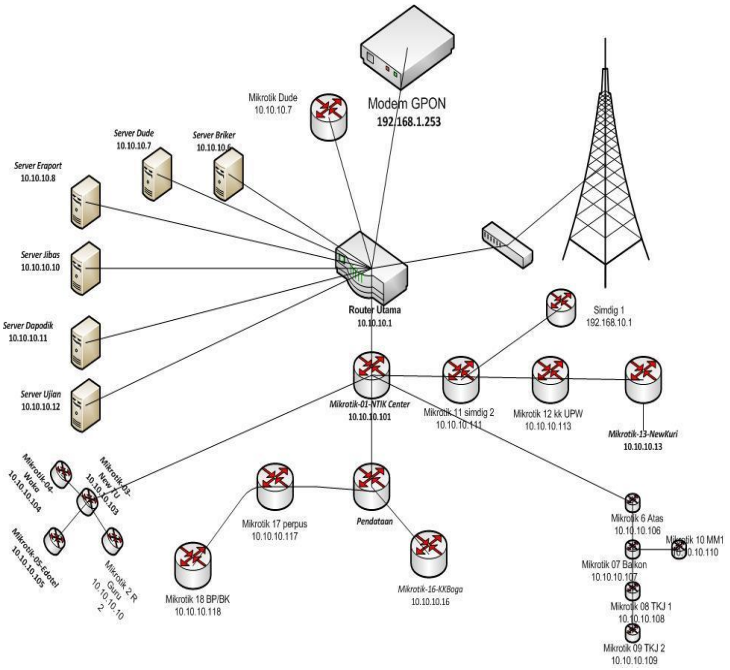
Gambar 3. Siklus Perancangan Jaringan *PPDIOO*

Metode ini merupakan sebuah siklus tentang perancangan jaringan. Perancangan ini terbagi atas beberapa tahapan yaitu: *Prepare* (Persiapan), *Plan* (Perencanaan), Design (Desain), *Implement* (Implementasi), *Operate* (Operasi), dan *Optimize* (Optimasi).

3. Tahap-Tahap Penelitian

a. Tahap *Prepare*

Pada Tahap ini penulis melakukan analisa skema jaringan atau topologi jaringan yang digunakan di SMKN 1 Praya sehingga nantinya akan menjadi sebuah rujukan membuat sebuah sistem yang mampu memblokir beberapa aplikasi yang mengganggu aktivitas pembelajaran pada jam-jam sekolah. Topologi jaringan tersebut digambarkan pada Gambar 4.



Gambar 4. Topologi Jaringan Di SMKN 1 Praya

Berdasarkan topologi jaringan diatas dimana Koneksi *internet* SMKN 1 Praya menggunakan Telkom sebagai *provider* lebih tepatnya paket *indihome* dengan *bandwidth* 100 *Mbps* dan terdapat 50 *Mbps* yang digunakan untuk *backup.* Paket *internet* tersebut kemudian menuju ke *router* pusat yang kemudian nantinya dialirkan ke seluruh jaringan. Untuk memproteksi jaringan tersebut *router* yang ada kemudian dilengkapi dengan *firewall.*

b. Tahap Rencana (*Plan*)

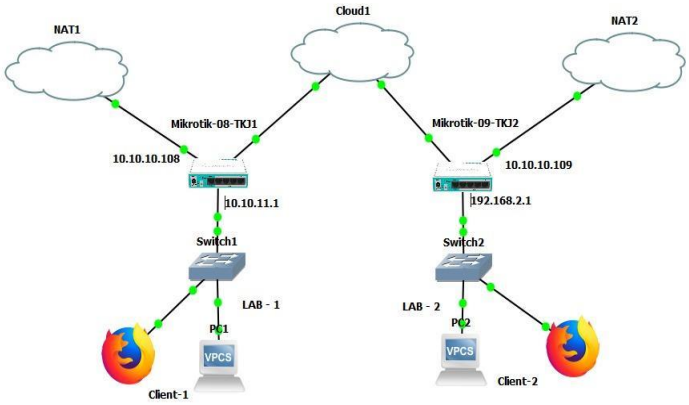
Rancangan jaringan yang akan dibuat untuk dapat mengurangi penggunaan *internet* pada saat jam belajar yaitu jam 07.30 – 14.00 seperti media sosial (*facebook*) dan *games online.* Perancangan jaringan ini akan dilakukan uji coba pada 2 buah laboratorium jaringan di SMKN 1 Praya untuk mengurangi efek kerugian jika terjadi kesalahan.

Analisis kebutuhan jaringan yang dilakukan meliputi terhadap:

1) Perangkat Keras. Untuk menjalankan sistem ini dibutuhkan perangkat keras yang mampu mendukung pengoperasian jaringan. Sistem perangkat keras tersebut harus memenuhi spesifikasi minimal dari kebutuhan *hardware* dari sistem yang akan diterapkan. Adapun alat dan bahan yang digunakan dalam merancang keamanan jaringan ini adalah sebagai berikut:
   a) 2 buah *Mikrotik RB951Ui-2^{nD}*
   b) *1* buah *Switch*
   c) 1 *dush* Kabel *UTP*
   d) 100 buah Konektor *RJ*-45
   e) Komputer, laptop, dan *Smartphone*
2) Perangkat Lunak. Untuk menerapkan sistem keamanan jaringan ini diperlukan beberapa perangkat lunak baik itu pada *server* maupun *client.* Adapun perangkat lunak tersebut antara lain :
   a) *Winbox*
   b) Web Browser (Mozilla Firefox, Google Chrome)
   c) Sistem Operasi *Windows* 7 atau *Windows* 10 (32/64) bit

c. Tahap *Design*

Pada tahapan ini penulis membuat rancangan sistem atau topologi yang telah dilengkapi *firewall* sebagaimana disajikan pada Gambar 5.



Gambar 5. Topologi Jaringan yang di usulkan

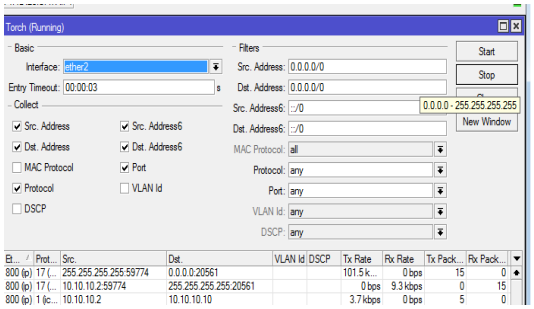
Dari Gambar 5 dapat dilihat topologi jaringan yang diusulkan. Kedua *mikrotik* mendapatkan *IP static* yang diberikan oleh *server* dengan *mikrotik* TKJ1 mendapatkan alamat *IP* 10.10.10.108 dan *mikrotik* TKJ2 dengan alamat *IP* 10.10.10.109. IP Address tersebut disesuaikan dengan yang ada pada jaringan internet SMKN 1 Praya sesuai dengan gambar 4. dari *mikrotik* diteruskan ke *switch* untuk disalurkan ke *PC client*. *IP local* yang diberikan oleh *mikrotik* TKJ 1 yaitu 10.10.11.1 yang tidak lagi diberikan secara *static* tetapi secara *DHCP*. Untuk *mikrotik* TKJ2 diberikan 192.168.2.1 sebagai *IP address local*nya. Kedua *mikrotik* di atas kemudian akan diberikan konfigurasi agar pada jam-jam tertentu beberapa aplikasi *games online* dan sosial media tidak dapat digunakan.

ANALISIS

a. Tahap implementasi (*Implentation)*

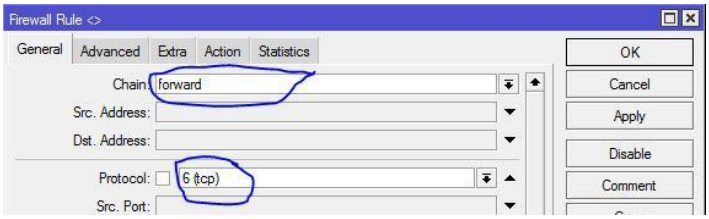
Langkah-langkah instalasi sistem keamanan jaringan :

1. Konfigurasi jaringan dasar
   Pada tahap ini penulis tidak melakukan konfigurasi jaringan karena sudah ada konfigurasi sebelumnya dan penulis mengikuti jaringan yang telah dibuat sebelumnya.
2. Konfigurasi *Packet Filtering*
   Peneliti memastikan *winbox* sudah terbuka dan jaringan *internet* berjalan dengan baik, adapun langkah-langah konfigurasinya antara lain :
   a. Peneliti melakukan pencarian *port* yang digunakan oleh *games online* dan sosial media yang akan di blokir. Hal ini dilakukan untuk mengetahui IP games atau IP sosial media yang digunakan oleh *user* yang nantinya akan menjadi bahan dalam pemblokiran.



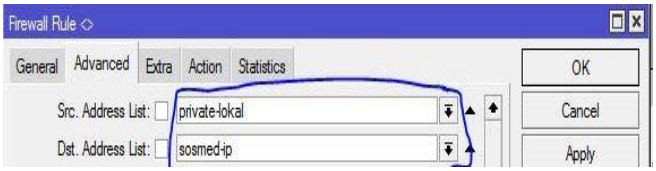
Gambar 6. pencarian *IP Games online* dan media sosial dengan fasiltas *torch*.

b. Peneliti mengatur *chain* pada *protocol TCP*.
Hal ini dimaksudkan untuk menentuakan jenis trafik yang akan dikelola pada fitur *firewall* yaitu filter *rule* dan lebih spesifik pada protocol *TCP*.



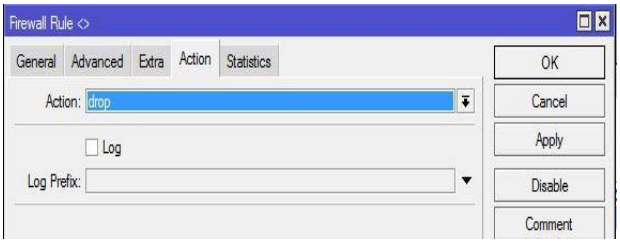
Gambar 7. Pengaturan *Filter Rule* pada *tab general*

c. Peneliti menuliskan *list address* yang akan di blokir.
Kegiatan ini bertujuan untuk mengelompokkan situs atau aplikasi yang akan di blokir.



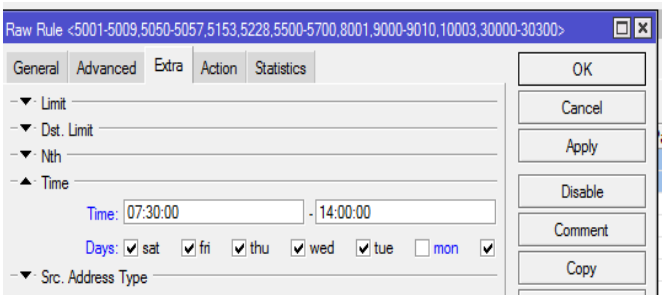
Gambar 8. Pengaturan *Filter Rule* pada *tab general*

d. Peneliti memilih *action drop*.
Hal ini dimaksudkan agar *router* membuang *packet* yang sudah di kelompokkan sebelumnya.



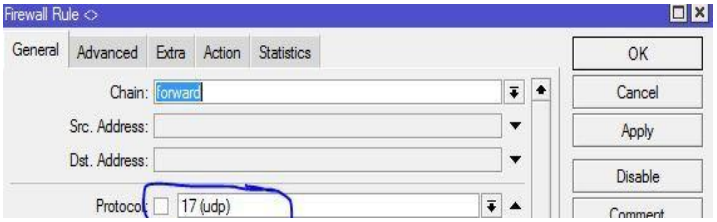
Gambar 9. Pengaturan *Filter Rule* pada *tab Action*

e. Peneliti mengatur waktu aktif pemblokiran.
Pengaturan waktu ini dibutuhkan untuk menentukan waktu yang cocok digunakan dalam mengaktifkan pemblokiran situs atau aplikasi dan kapan pemblokiran tersebut tidak aktif.



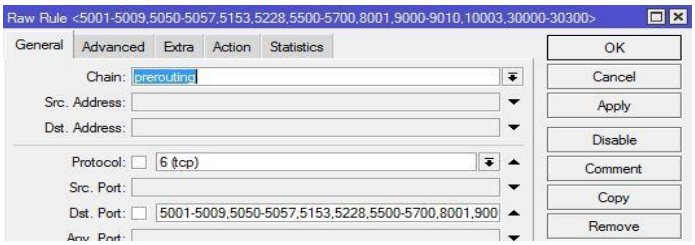
Gambar 10. Pengaturan *Filter Rule* pada *tab Extra*

f. Peneliti mengatur *chain* pada *protocol UDP.*
Pengaturan chain pada *UDP* sama fungsinya dengan *TCP* tetapi hal ini di maksudkan untuk memblokir IP yang menggunakan *protocol UDP*. Hal yang sama dilakuan pada semua *tab* pada *tools filter rule.*
.



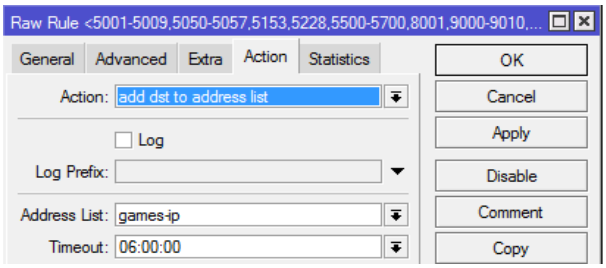
Gambar 11. Pengaturan *Filter Rule* pada *protocol UDP*

g. Pengaturan page pada *filter raw*, memasukkan *IP Address* hasil yang didapat dari tools *torch*.



Gambar 12. pengaturan *filter raw* dengan menggunakan protocol TCP

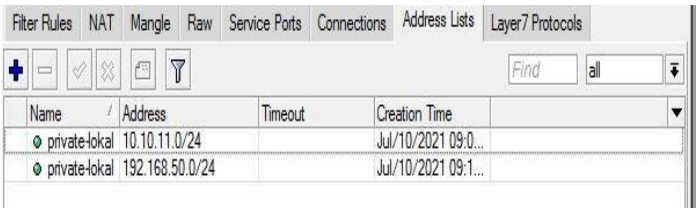
h. Peneliti mengarahkan semua *packet* data ke *list* yang dibuat.



Gambar 13. Pengaturan *tab action* pada *filter raw*

i. Langkah terakhir dari konfigurasi ini adalah dengan membuka *tab address list* kemudian isikan *network Id local* yang digunakan oleh *user* dalam melakukan koneksi *internet* seperti yang terlihat pada gambar 4.6. Hasil tangkapan *Ip* yang telah dibagi tadi baik itu *ip-games* ataupun media sosial

akan muncul secara otomatis ketika *client* telah membuka aplikasi-aplikasi tersebut.



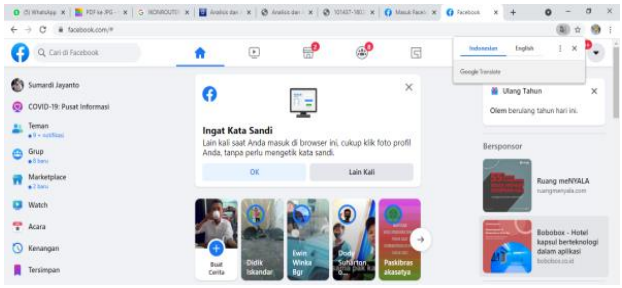
Gambar 14. Pengisian net id jaringan *local* yang dibuat

b. Tahap Beroperasi (*Operate*)

1. Sebelum dilakukan pemblokiran

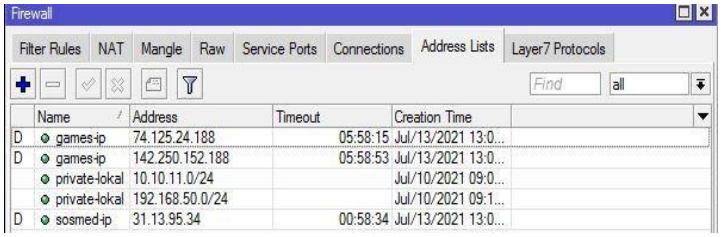
Pada tahap ini penulis melakukan pengujian sebelum membuat sebuah sistem yang mampu memblokir beberapa aplikasi yang melewati jaringan. Semua situs, atau aplikasi yang berbasis *online* akan dapat masuk tanpa adanya sebuah sistem yang mampu memfilter dengan hasil seperti gambar 15.

Gambar 15. Tampilan aplikasi *Mobile Legend* sebelum diblokir



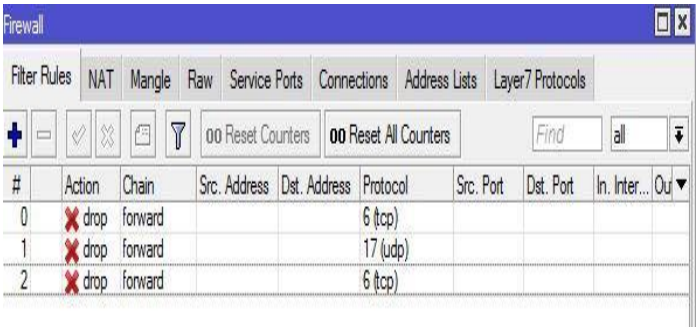
Gambar 16. Tampilan *Facebook* sebelum diblokir

2. Setelah Pemblokiran dilakukan



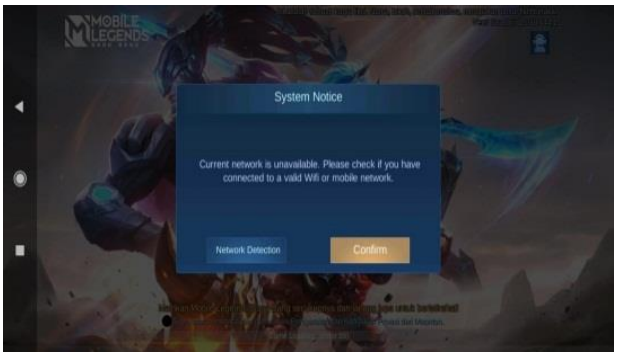
Gambar 17. Hasil *scanning Ip address* yang berhasil ditangkap oleh *tools address list.*

Dalam pelaksanaan pengujian ini ketika ada *user* yang masuk maka *IP* dari aplikasi yang telah di blok akan langsung muncul seperti pada gambar 18 dimana *IP* tersebut muncul secara otomatis.



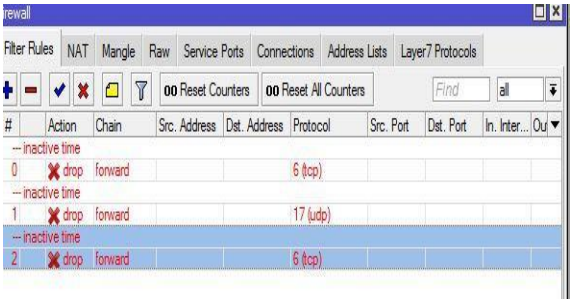
Gambar 18. *Filter Rules* sedang aktif

Pada tahap pengujian ini dilakukan pada pukul 09.00 dengan alasan pada waktu tersebut merupakan jam belajar di SMKN 1 Praya. Pada *filter rules* akan muncul sesuai dengan Gambar 18 terlihat bahwa proses blokir sedang aktif.



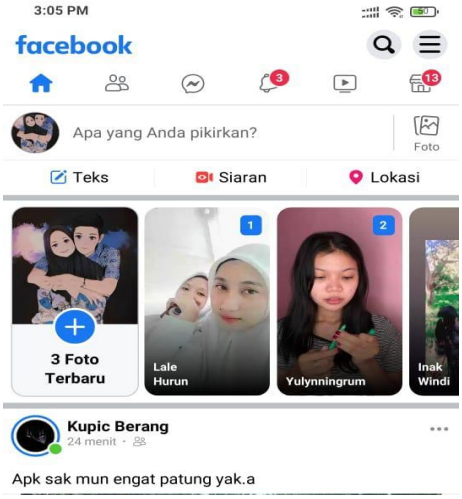
Gambar 19. Aplikasi *Mobile Legend* berhasil diblokir

Pada pengujian selanjutnya dilakukan pada saat jam belajar sekolah sudah selesai sehingga semua *packet* diteruskan dan pada tampilan *filter rules* seperti gambar 20.



Gambar 20. *filter rules* tidak aktif kembali

Langkah selanjutnya adalah kembali membuka aplikasi yang telah diblokir. Pada langkah ini *packet* dapat kembali diakses seperti Gambar 21 dan Gambar 22 berikut ini.



Gambar 21. Aplikasi *facebook* sudah dapat dibuka

Gambar 22. Aplikasi *Mobile Legend* sudah dapat dibuka

c. Tahap Optimasi (*Optimize*)

Pada tahap ini dilakukan evaluasi tentang sistem jaringan yang berjalan. Berdasarkan tahapan-tahapan yang telah dilakukan maka perlu peneliti sarankan untuk selalu mengupdate *port-port* yang digunakan oleh aplikasi. Bukan hanya itu saja sistem ini akan berjalan jika operator terus *mengupdate* nama alamat aplikasi yang terkadang berubah-ubah.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, maka dapat disimpulkan dengan telah dilakukannya pemblokiran beberapa situs dan aplikasi baik *games online* ataupun sosial media menggunakan *Packet* Filtering Berbasis Mikrotik berakibat pada tidak dapat diaksesnya *games online* dan sosial media oleh siswa yang menggunakan jaringan *internet* di sekolah pada jam-jam pelajaran.

REFERENSI

Amarudin, A., & Ulum, F. (2018). Desain Keamanan Jaringan Pada Mikrotik *Router* Os Menggunakan Metode Port Knocking. *JURNAL TEKNOINFO , 12* (2), 72-75.

Ardi, Z., Viola, K., & Sukmawati, I. (2018). An Analysis of Internet Abuses Impact on Children's Moral Development. JPPI (Jurnal Penelitian Pendidikan Indonesia), 4(1), 44–50. https://doi.org/10.29210/02018192.

Fadlil, A., Riadi, I., & Aji, S. (2017). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. *Jurnal Ilmu Teknik Elektro Komputer dan Informatika (JITEKI) , 3* (1), 1119.

Fitri, S. (2017). Dampak Positif Dan Negatif Sosial Media Terhadap Perubahan Sosial Anak. *Naturalistic : Jurnal Kajian Penelitian Pendidikan dan Pembelajaran , 1* (2), 118-123.

Hardana, & Irvantino, I. (2011). *Konfigurasi Wireless RouterBoard Mikrotik.* Yogyakarta: Andi Offset.

Juardi, D. (2017). Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus. *SYNTAX: Jurnal Informatika , 6* (1), 11-19.

Muzakir, A., & Ulfa, M. (2019). Analisis Kinerja *Packet* Filtering Berbasis Mikrotik *Router*board Pada Sistem Keamanan Jaringan. *Simetris : Jurnal Teknik Mesin, Elektro dan Ilmu Komputer , 10* (1), 15-20.

Revilia, D., & Irwansyah. (2020). Literasi Media Sosial: Kesadaran Keamanan Dan Privasi Dalam Perspektif Generasi Milenial. *Jurnal Penelitian Komunikasi dan Opini Publik* (24), 1-15.

Saputri, O. E., Arifah, S., & Wulaningrum, D.N. (2014). *Gambaran Penggunaan Internet Pada Anak Remaja Di SMP Muhammadiyah 1 Kartasura.* Skripsi thesis, Universitas Muhammadiyah Surakarta.

Sofana, I. (2017). *Jaringan Komputer Berbasis Mikrotik: Dilengkapi Latihan Dan Contoh Soal Mikrotik Training Certlfied Network Associated (MTCNA).* Bandung: Informatika.