

IMPLEMENTASI *FIREWALL FILTER RULES* UNTUK KEAMANAN JARINGAN DAN METODE *QUEUE TREE* UNTUK MANAJEMEN *BANDWIDTH* PADA MIKROTIK

Silvia Wulandari Situngkir^{1*}, Sanri Yuliana Siallagan², Asri Angel Tumanggor³, Dedy Kiswanto⁴

Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia¹

Email*: silviastgkr@gmail.com

Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia²

Email: sanrisiallagan2017@gmail.com

Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia³

Email: asriangel161@gmail.com

Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia⁴

Email: dedykiswanto@unimed.ac.id

ABSTRAK

Saat ini hampir seluruh sektor kehidupan seperti perkantoran, instansi pemerintah, institusi pendidikan, serta layanan publik bergantung pada jaringan internet sebagai sarana pendukung kerja dan media pertukaran informasi. Pemanfaatan internet yang optimal dapat meningkatkan produktivitas. Namun, tingginya penggunaan internet perlu diimbangi dengan manajemen *bandwidth* yang efektif. Pengelolaan *bandwidth* yang tidak terstruktur dapat menyebabkan penurunan kecepatan akses internet. Selain itu, aspek keamanan jaringan juga menjadi hal yang krusial dalam implementasi jaringan komputer. Kelalaian dalam aspek ini dapat membuka celah terhadap serangan atau peretasan jaringan. Oleh karena itu, dibutuhkan sistem *firewall* yang andal untuk mendukung kualitas jaringan yang baik. Salah satu solusi untuk mengatasi permasalahan tersebut adalah dengan penerapan *firewall* serta metode *queue tree* menggunakan perangkat MikroTik. Pendekatan ini mampu meningkatkan performa jaringan dan memperbaiki kualitas layanan internet. Dengan pengelompokan dan pembatasan lalu lintas data yang tepat, pemakaian jaringan menjadi lebih terkendali, mengurangi risiko kelebihan beban *bandwidth*, dan menciptakan lingkungan jaringan yang lebih aman serta merata. Implementasi dilakukan menggunakan router MikroTik RB941-2nD dan perangkat lunak Winbox, dengan konfigurasi yang mencakup pengaturan router, *filter rules*, serta *queue tree*. Hasil dari implementasi menunjukkan bahwa manajemen *bandwidth* serta penyaringan akses ke situs berisi konten dewasa dan perjudian *online* dapat berjalan secara efektif

Kata kunci: *Bandwidth*, *Firewall*, *Filter Rules*, MikroTik, *Queue Tree*

ABSTRACT

Currently, almost all sectors of life such as offices, government agencies, educational institutions, and public services depend on the internet network as a means of supporting work and information exchange media. Optimal internet utilization can increase productivity. However, high internet usage needs to be balanced with effective bandwidth management. Unstructured bandwidth management can cause a decrease in internet access speed. In addition, network security aspects are also crucial in the implementation of computer networks. Negligence in this aspect can open a gap to network attacks or

hacking. Therefore, a reliable firewall system is needed to support good network quality. One solution to overcome these problems is to implement a firewall and queue tree method using MikroTik devices. This approach can increase network performance and improve internet service quality. With proper grouping and restriction of data traffic, network usage becomes more controllable, reduces the risk of bandwidth overload, and creates a more secure and equitable network environment. The implementation was carried out using a MikroTik RB941-2nD router and Winbox software, with configurations that included router settings, filter rules, and queue trees. The results of the implementation show that bandwidth management and filtering access to sites containing adult content and online gambling can run effectively.

Keywords: Bandwidth, Firewall, Filter Rules, Mikrotik, Queue Tree

1. PENDAHULUAN

Saat ini semua bidang dalam kehidupan seperti seperti kantor, instansi pemerintahan, sekolah, universitas, layanan publik, dan lainnya menggunakan jaringan internet sebagai penunjang pekerjaan dan media pertukaran informasi. Produktivitas dalam pekerjaan dapat ditingkatkan dengan menggunakan internet. Keberadaan jaringan internet mempermudah manusia dalam mencari dan menerima informasi dengan cepat. Koneksi antar komputer ini bisa dilakukan melalui media kabel maupun secara nirkabel (tanpa kabel). Data yang dikirimkan dalam jaringan ini bisa berupa teks, suara, gambar, hingga video[1]. *Switch* atau *router* memakai algoritma atau protokol agar data sampai ke titik akhir atau secara umum dikenal sebagai IP menjadi tujuan transmisi. Setiap pihak dari jaringan yang menggunakan sumber daya adalah *client* dan yang memberikan berbagai jenis layanan disebut sebagai *server* [2]. Namun, kecepatan akses informasi tersebut bisa berbeda-beda, tergantung pada kapasitas *bandwidth* yang disediakan oleh masing-masing penyedia layanan, yang kadang bisa lambat maupun cepat [3]. Dengan tingginya tingkat pemakaian internet harus diimbangi dengan kapasitas manajemen *bandwidth* yang baik. Manajemen *bandwidth* merupakan metode pengendalian arus lalu lintas paket data pada sebuah jaringan komputer sehingga meminimalisir adanya keterlambatan pengiriman atau penerimaan paket data. *Bandwidth* sendiri merupakan perhitungan konsumsi transfer data telekomunikasi yang dihitung dalam bentuk satuan bit per detik (bps) yang terjadi antara *server* - *client* dalam waktu tertentu pada jaringan [4]. Manajemen *bandwidth* yang tidak teratur sangat berpengaruh terhadap kecepatan pada akses internet. Salah satu kendala yang dapat terjadi disaat kapasitas *bandwidth* yang tidak sesuai adalah *Request Time Out*, hal ini terjadi jika kapasitas *bandwidth* telah habis digunakan. Penggunaan *bandwidth* yang tidak merata juga menyebabkan *delay* atau waktu yang dibutuhkan sebuah paket dari pengirim sampai ke tujuan menjadi besar [5]. Oleh karena itu, dibutuhkan sistem manajemen jaringan yang mampu mengatur lalu lintas data serta memberikan keamanan bagi seluruh pengguna jaringan.

Ketika mengimplentasikan jaringan pada komputer, keamanan jaringan juga perlu diperhatikan. Kelalaian terhadap jaringan dapat memungkinkan peretasan dan jaringan yang dibangun. Jaringan yang baik memerlukan tingkat *firewall* yang baik pula. *Firewall* sendiri merupakan perangkat yang berperan dalam melindungi jaringan dari serangan yang berasal dari luar [6]. *Firewall* merupakan sistem yang digunakan untuk memonitoring terhadap seluruh data yang keluar atau masuk dalam jaringan. *Firewall* berperan untuk mengizinkan lalu lintas jaringan yang aman dan tidak aman. *Firewall* biasanya di implementasikan pada sebuah *gateway* atau pintu gerbang pada jaringan komputer, sehingga jaringan lokal yang berada di bawah *firewall* bisa terbebas dari

serangan yang merugikan [7]. Perangkat ini berfungsi sebagai penjaga keamanan *gateway* jaringan, memeriksa paket yang masuk dan keluar dan memperlakukannya sesuai dengan berbagai aturan penyaringan dengan kemampuan untuk memblokir, mengizinkan, atau menjatuhkan lalu lintas. Banyaknya akses internet di ruang publik seperti kantor, sekolah, dan kampus menjadikan implementasi dari *firewall filter rules* sebagai *filtering* cukup efisien untuk melakukan penyaringan terhadap *website* yang tidak sesuai untuk diakses [8].

Dalam melakukan *routing* dibutuhkan *router*. *Router* berfungsi untuk menganalisis setiap pake paket data yang melewatinya dalam suatu jaringan dan kemudian data tersebut diarahkan melalui suatu rute sehingga paket data tersebut akan sampai ke tujuan [9]. MikroTik merupakan suatu sistem operasi yang digunakan untuk menjadikan komputer MikroTik merupakan *router* jaringan yang cocok digunakan oleh ISP, *provider hotspot* dan warnet. MikroTik menawarkan fasilitas seperti manajemen *bandwidth*, *firewall*, *hotspot for plug-and-play access*, *remote winbox GUI admin*, dan *routing* yang cocok untuk jaringan *wireless* [10]. MikroTik merupakan salah satu perangkat *router* yang banyak digunakan saat ini, MikroTik menawarkan berbagai fitur untuk manajemen jaringan termasuk dalam implemetasi *firewall* dan manajemen *queue*. Fitur *firewall filter rules* pada MikroTik dapat membantu untuk mengatur dan memfilter lalu lintas data yang masuk maupun keluar jaringan, sehingga hanya trafik yang diizinkan saja yang dapat melewati sistem. *Filter rules* memiliki tiga blok *chain* seperti *input*, *process* dan *output* sehingga dapat melakukan kebijakan untuk trafik yang masuk ke sebuah jaringan untuk diterima atau tidak [11]. Salah satu protokol yang terdapat pada *filter rules* adalah protokol layer 7. Layanan atau protokol yang terdapat pada Layer 7 meliputi HTTP, FTP, SMTP, dan sebagainya [12]. Sementara itu, *Queue Tree* adalah fitur yang disediakan MikroTik yang mengharuskan penggunaanya untuk mengatur *mangle* sebelum melakukan pelimitan pada target yang berupa IP Address, port, bahkan Protocol [13]. Fitur *Queue Tree* digunakan untuk manajemen *bandwidth* secara lebih fleksibel, dengan cara membagi dan mengalokasikan kecepatan internet kepada masing-masing pengguna atau kelompok pengguna berdasarkan kebutuhan dan prioritas tertentu. Penelitian terdahulu yang dilakukan oleh firmansyah dengan implementasi manajemen *bandwidth* dengan metode *queue tree* yang dilakukan pada Cipta Banuata Anugrah Jakarta dengan MikroTik sebagai *bridge* untuk meneliti pengaruh pemakaian *bandwidth* yang diterima *client* sebelum dan sesudah menggunakan MikroTik dengan memberikan kecepatan *download* sebesar 0.97 Mbps dan Upload sebesar 2.25 Mbps, berbeda dengan administrator diberikan kecepatan *download* sebesar 1 Mbps dan Upload sebesar 2.25 Mbps sesuai dengan kebutuhan.

Implementasi *firewall* dan metode *queue tree* pada MikroTik dapat menjadi solusi efektif dalam mengoptimalkan kinerja jaringan dan meningkatkan kualitas layanan internet. Dengan adanya pembatasan dan pengelompokan trafik yang baik, maka penggunaan jaringan dapat terkontrol dengan lebih efisien, mengurangi kemungkinan terjadinya *overload* pada *bandwidth*, serta menciptakan lingkungan jaringan yang lebih aman dan adil. Melalui penelitian ini, penulis ingin mengevaluasi efektivitas dari implemetasi *firewall* dan *queue tree* dalam mengelola akses pengguna jaringan internet menggunakan MikroTik. Penelitian ini juga bertujuan untuk memberikan gambaran teknis tentang bagaimana konfigurasi dan implementasi kedua fitur tersebut dapat diterapkan secara praktis dalam skala jaringan lokal.

2. METODE

Dalam melakukan implementasi *firewall* dan manajemen *bandwidth* dengan metode *queue tree* digunakan metode pengembangan *waterfall*. Metode pengembangan *waterfall* adalah metode pengembangan sistem dimana antar satu fase ke fase yang lain dilakukan secara berurutan, sebuah langkah akan diselesaikan terlebih dahulu dimulai dari tahapan yang pertama sebelum melanjutkan ke tahapan yang berikutnya [14]. Tahapan - tahapan tersebut meliputi proses analisis, desain, implemetasi, pengujian dan pemeliharaan.



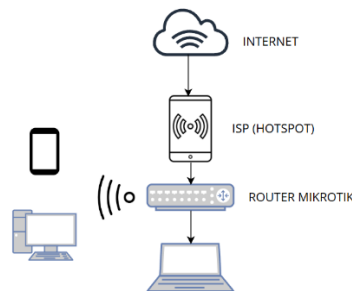
Gambar 1. Tahapan penelitian

Analisis

Pada tahap analisis, penelitian dimulai dengan mengumpulkan informasi terkait pengimplmentasian *firewall filter rules* dan manajemen *bandwidth* dengan *queue tree* pada MikroTik. Proses analisis dilakukan dengan mengidentifikasi permasalahan yang sering terjadi pada jaringan lokal dan cara memecahkan masalah tersebut melalui studi literatur dan observasi melalui penelitian terdahulu. Melalui observasi yang dilakukan, metode *firewall* dengan *filter rules* dan manajemen *bandwidth* dengan *queue tree* pada MikroTik dapat menjadi solusi yang relevan.

Desain

Sebelum proses implemetasi, perancangan desain dan topologi jaringan disesuaikan dengan kebutuhan pada jaringan.



Gambar 2. Topologi jaringan

Topologi diatas adalah gambaran dari penelitian yang dilakukan untuk mengatur sistem *filtering* dan manajemen *bandwidth* pada jaringan komputer. MikroTik sebagai *server* yang terhubung ke *hotspot* kemudian jaringan internet akan dikirimkan ke *client* yaitu laptop atau komputer melalui *wireless*. Sebelum internet sampai ke *device* lainnya, *router* akan dikonfigurasi oleh administrator dan akan diimplemetasikan *filtering* dan manajemen *bandwidth* menggunakan *winbox* sebagai *tool* dalam pengelolaannya.

Implementasi

Selanjutnya perancangan yang telah dibuat akan diimplementasikan akan bisa terwujud. Implementasi *firewall* dan manajemen dilakukan menggunakan *router* MikroTik RB941-2nD dan melakukan konfigurasi pada *Winbox*. Implementasi meliputi konfigurasi *router* MikroTik, konfigurasi *filter rules* dan *queue tree*.

Pengujian

Tahap ini bertujuan melakukan proses uji coba dari MikroTik yang sudah di konfigurasi dengan *firewall filter rules* dan manajemen *bandwidth* dengan *queue tree*. Sistem filterisasi dilakukan dengan melakukan pencarian pada situs terkait konten dewasa dan judi *online*. Proses *filtering* yang baik adalah situs dengan konten yang sudah di filter tersebut terblokir dan tidak dapat dibuka.

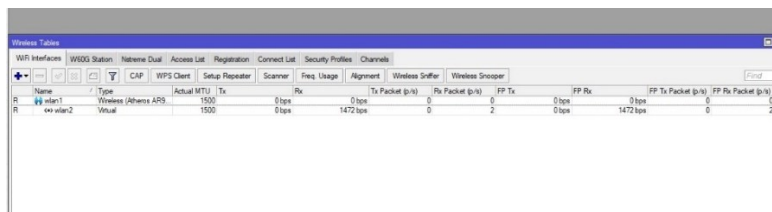
Pemeliharaan

Tahap terakhir pada metode pengembangan *waterfall* dalam penelitian ini adalah pemeliharaan. Proses pemeliharaan dilakukan secara berkelanjutan setelah sistem berhasil agar proses filterisasi dan manajemen *bandwidth* tetap berjalan dengan baik dengan semestinya. Proses pemeliharaan disesuaikan dengan kebutuhan administrator dan kebutuhan pengguna.

3. HASIL DAN PEMBAHASAN

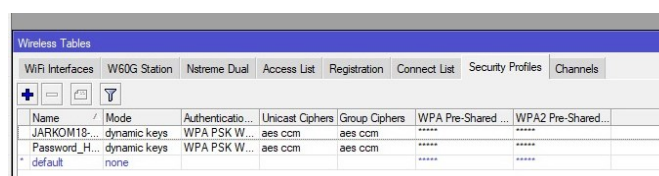
Konfigurasi Router dan IP Address

Implementasi *firewall* dan manajemen *bandwidth* dimulai dengan melakukan konfigurasi pada *router* untuk mendapatkan jaringan internet ISP dengan melakukan konfigurasi pada menu *Wireless* pada *Winbox* untuk WLAN1. Setelah melakukan konfigurasi pada WLAN1, selanjutnya dilakukan konfigurasi pada WLAN2 untuk virtual AP (*Access Point*).



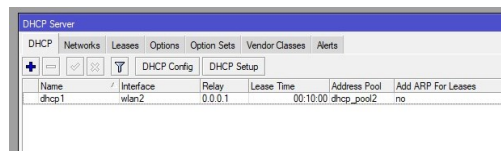
Gambar 3. Membuat *interface* untuk WLAN1 dan WLAN2

Langkah kedua dengan melakukan pengaturan *security profiles* pada MikroTik untuk menambahkan *password* jika ada yang akan *connect* pada jaringan.



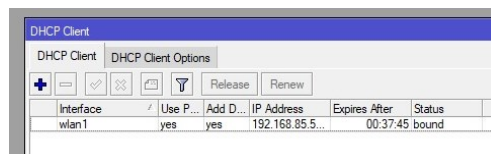
Gambar 4. Mengatur *security profiles*

Kemudian membuat setting *DHCP Server* untuk memberikan alamat IP sesuai dengan kabel LAN yang terhubung pada *router*. Pada *DHCP Server* ini terhubung dengan *port* WLAN2, maka pengaturan dilakukan melalui *port* tersebut. Dapat dilihat pada Gambar 5.



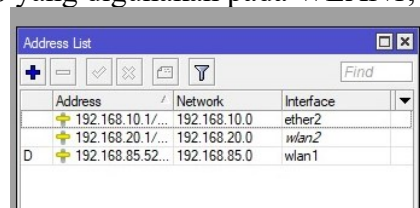
Gambar 5. Mengatur DHCP server

Setelah melakukan *setting* pada DHCP server, selanjutnya lakukan pengaturan DHCP client untuk memperoleh alamat IP secara otomatis dari sumber jaringan internet. Status DHCP client dipastikan sudah menjadi *bound* yang berarti sudah terhubung.



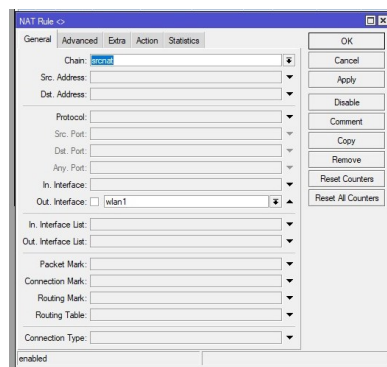
Gambar 6. Mengatur DHCP client

Berikut merupakan *address* yang digunakan pada WLAN1, WLAN2 dan *ether* 2.



Gambar 7. Mengatur IP Address

Kemudian melakukan *setting* NAT pada *winbox* untuk menerjemahkan IP lokal (*private*) ke IP publik, sehingga perangkat di jaringan lokal bisa mengakses internet melalui satu IP publik dari ISP.



Gambar 8. Mengatur NAT Rule

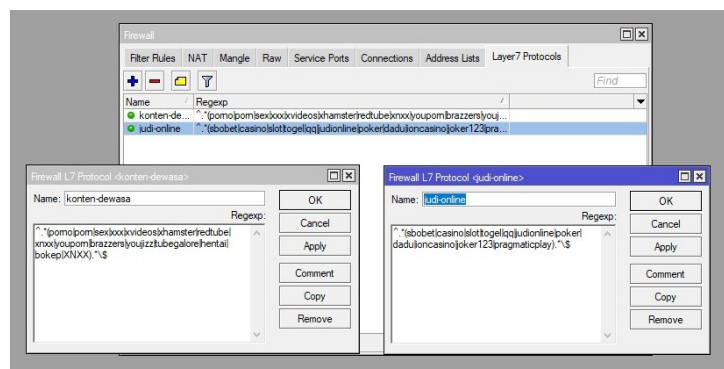
Implementasi **Firewall** dengan **Filter Rules**

Peneliti melakukan pelimitan pencarian situs konten dewasa dan judi *online*. Implementasi *firewall* pada MikroTik pada menu *Firewall* pada *Winbox* dengan *filter rules*. Blokir situs dilakukan dengan via Layer7 dan blokir DNS eksternal.

#	Action	Chain	Src. Address	Dst. Address	Proto	Src. Port	Dst. Port	In. Inter.	Out. Inter.	In. Int.	Out. Int.	Src. Ad.	Dst. Ad.	Bytes	Packets
0	drop	forward			6 (tcp)		80,443							734.9 KB	13,411
1	drop	forward			6 (tcp)									59.0 KB	116
2	drop	forward			6 (tcp)									3459.0 KB	4,563
3	drop	forward		1192.168.8...	17 (u...)		53							0 B	0
4	drop	forward		1192.168.8...	6 (tcp)		53							0 B	0

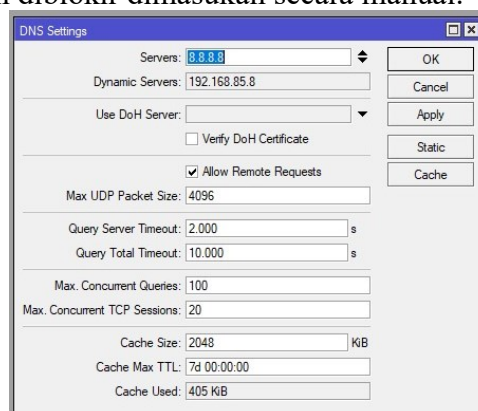
Gambar 9. Mengatur *Firewall Filter Rules*

Firewall dengan *filter rules* via Layer7 diawali dengan menambahkan *rule* konten-dewasa dimana MikroTik akan mencari *string* dalam *request* HTTP, apakah mengandung salah satu kata kata yang akan diblokir pada situs konten dewasa. Kemudian situs dengan kata kunci tersebut tidak akan dapat diakses oleh pengguna jaringan. Kemudian dibuat *rule* lainnya dengan nama *judi-online*, MikroTik akan mencari *string* dalam *request* HTTP, apakah mengandung salah satu kata kata yang akan diblokir pada situs judi *online*. Situs dengan kata kunci tersebut tidak akan dapat diakses oleh pengguna jaringan.



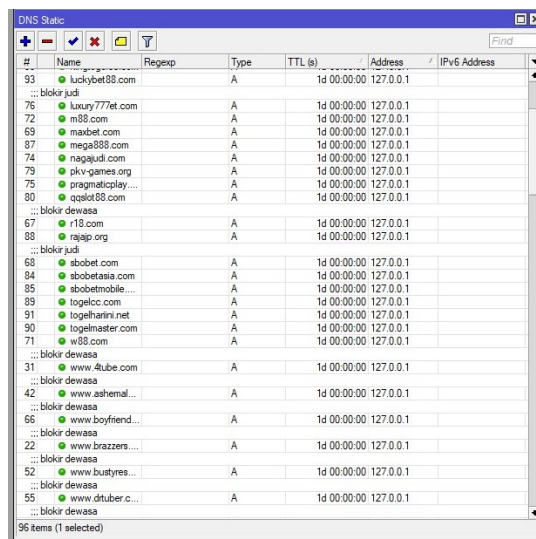
Gambar 10. Mengatur *Layer7 Protocol*

Selain dengan via Layer7, diimplemetasikan juga blokir situs dengan blokir DNS *static* yang akan dikombinasikan dengan Layer7. Pemblokiran konten melalui DNS, dimana URL dari situs yang akan diblokir dimasukan secara manual.



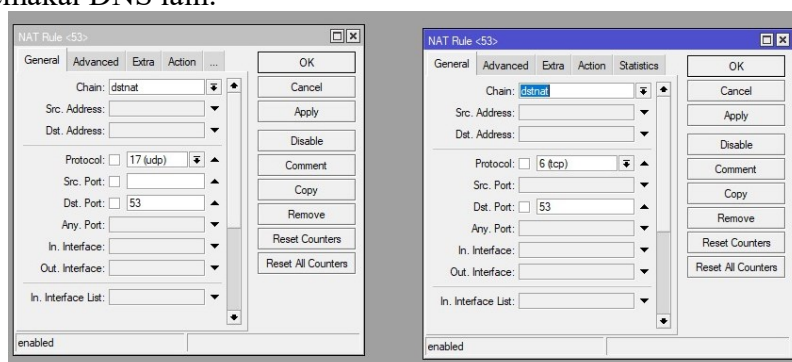
Gambar 11. Mengatur *DNS Static*

Kemudian tambahkan DNS *static* konten dewasa dan judi *online* yang akan diblokir.



Gambar 12. Tambahkan situs-situs yang akan di blokir.

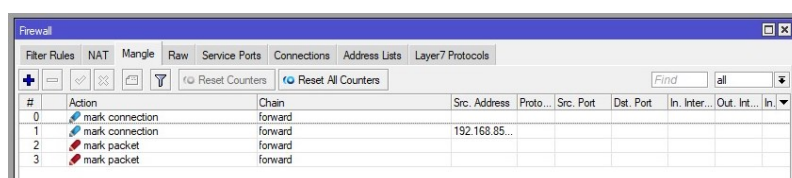
Selanjutnya melakukan *setting* UTP dan UDP pada *NAT Rule* untuk *DNS redirect*. Tujuannya agar semua permintaan DNS dari klien diarahkan ke MikroTik meskipun *user* mencoba memakai DNS lain.



Gambar 13. Mengatur NAT untuk DNS Redirect

Implementasi Manajemen *Bandwidth* dengan *Queue Tree*

Sebelum membuat *Queue Tree*, trafik harus ditandai terlebih dahulu menggunakan fitur *Mangle* di tab *Firewall*. Ini dilakukan untuk mengidentifikasi jenis trafik (misalnya berdasarkan IP atau *port*).



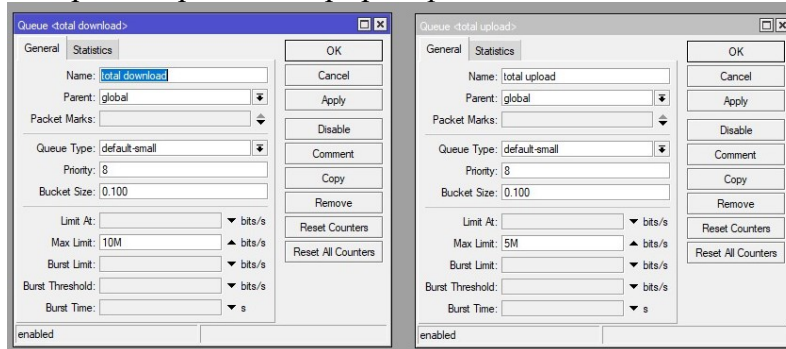
Gambar 14. Tandai Trafik dengan *Mangle*

Setelah trafik ditandai, implementasi *Queue Tree* dilakukan untuk membatasi dan mengatur *bandwidth*.

Name	Parent	Packet Marks	Limit At (bits/s)	Max Limit	Avg. R.	Queued Bytes	Bytes	Packets
total download	global			10M	0 bps	0 B	0 B	0
user download	total download	paket download		7M	0 bps	0 B	0 B	0
total upload	global			5M	0 bps	0 B	16.7 KB	24
user upload	total upload	paket upload		1M	0 bps	0 B	16.7 KB	24

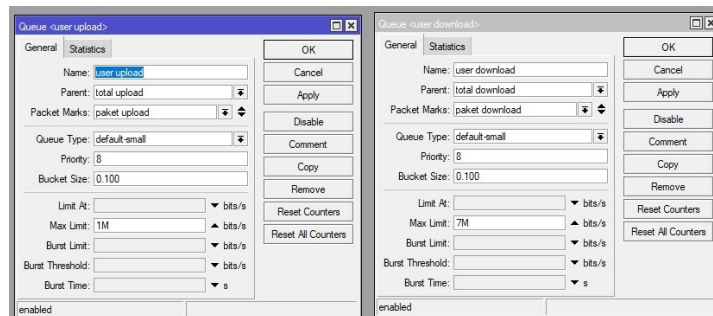
Gambar 15. Mengatur *Queue Tree*

Kemudian dilanjutkan dengan pembatasan *bandwidth* dengan trafik *download* dibatasi maksimum 10 Mbps dan upload 5 Mbps pada *parent total bandwidth*.



Gambar 16. Mengatur *Parent Queue*

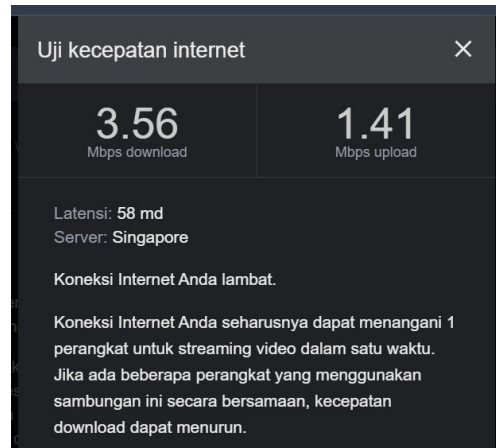
Total *bandwidth upload* dan *download* diatur di level global kemudian dibagi per *user* berdasarkan *packet mark* dengan maksimal *download* sebesar 7 Mbps dan *upload* sebesar 1 Mbps.



Gambar 16. Mengatur *Packet Mark*

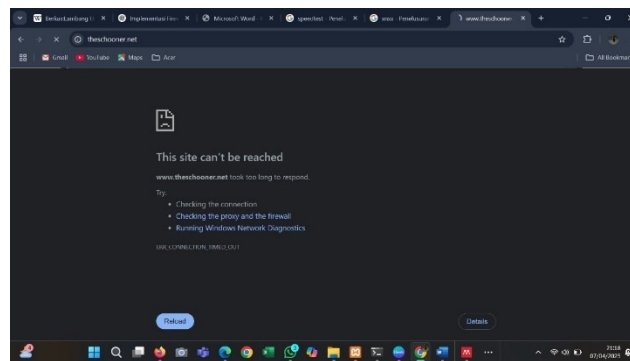
Pengujian

Pengujian diawali dengan menguji kecepatan internet jika memanajemen *bandwidth* melalui *website Speedtest* dengan Mbps *download* sebesar 3,56 Mbps dan Mbps *upload* sebesar 1.41 Mbps. Melalui pengujian, kecepatan internet masih terbilang cukup lambat tetapi dapat menangani 1 perangkat untuk *streaming* dalam satu waktu. Jika perangkat lainnya menggunakan jaringan yang sama di waktu yang bersamaan, kecepatan internet akan menurun.

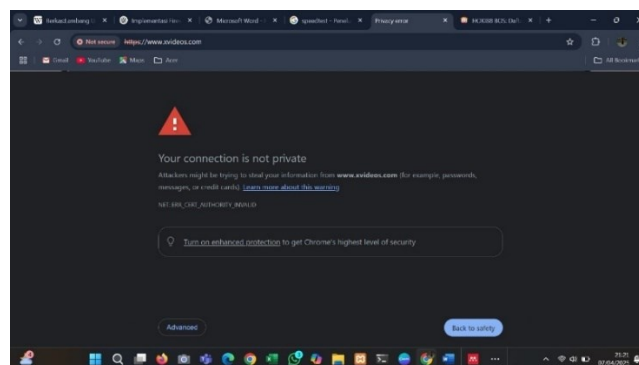


Gambar 17. Hasil Uji *Speedtest download* dan *upload*

Kemudian dilakukan pengujian *firewall* dimana situs judi *online* dan konten dewasa telah diblokir. Melalui pengujian didapatkan bahwa kedua situs tidak dapat dikunjungi.



Gambar 18. Pengujian Blokir Situs Konten Dewasa



Gambar 19. Pengujian Blokir Situs Judi *Online*

4. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan, implementasi *firewall* dengan *filter rules* dan metode *queue tree* menggunakan perangkat MikroTik RB941-2nD terbukti mampu meningkatkan efisiensi penggunaan jaringan, yang ditunjukkan dari hasil pengujian kecepatan internet sebesar 3,56 Mbps untuk *download* dan 1,41 Mbps untuk *upload*. Hal ini cukup untuk mendukung aktivitas *streaming* satu perangkat secara stabil. Selain itu, konfigurasi manajemen *bandwidth* melalui *queue tree* mampu menjaga

kestabilan akses internet dengan membagi kecepatan secara merata berdasarkan kebutuhan pengguna, sehingga mengurangi beban berlebih pada jaringan.

Dari aspek keamanan, implementasi *firewall* berhasil memberikan perlindungan dari konten yang tidak diinginkan seperti situs dewasa dan perjudian *online*, yang dibuktikan melalui pengujian dimana situs-situs tersebut tidak dapat diakses setelah diterapkan penyaringan menggunakan protokol Layer7 dan *static* DNS. Dengan konfigurasi yang tepat menggunakan *Winbox*, sistem yang diimplementasikan dapat menciptakan lingkungan jaringan yang lebih aman, tertata, dan adil bagi seluruh pengguna.

5. DAFTAR PUSTAKA

- [1] Q. Paen, P. Lede, And R. Abineno. Pengembangan Topologi Jaringan Di Sdi Umamapu. *Journal Islamic Global Network For Information Technology And Entrepreneurship*, 2(1), 30–48. <https://doi.org/10.59841/Ignite.V2i1.898>
- [2] Tangkowitz, . A. E., Palilingan, V. R., & Liando, O. E. S. (2021). Analisis dan Perancangan Jaringan Komputer di Sekolah Menengah Pertama. *EduTik : Jurnal Pendidikan Teknologi Informasi Dan Komunikasi*, 1(1), 69-82. <https://doi.org/10.53682/edutik.v1i1.1044>
- [3] A. Human Sukma, M. Ilyasyah Drilanang, S. Auzi, and D. Kiswanto. Implementasi OPENVPN Server menggunakan Red Hat Enterprise LINUX pada Amazon Web Service. *JATI : Jurnal Mahasiswa Teknik Informatika*. 2024.
- [4] J. Roberts Tamu Umbu et al. Implementasi Manajemen Bandwidth dan Filtering Firewall. *JATI : Jurnal Mahasiswa Teknik Informatika*. 2024.
- [5] W. W. Dale, F. Hariadi, R. Mikaela, and I. Malo. The Effect Of Queue Tree On Packet Loss In Bandwitch Management Online Based School Exam: Pengaruh Queue Tree pada paket loss dalam management Bandwitch Ujian Sekolah Berbasis Online. *JOINCS (Journal of Informatics, Network, and Computer Science)*. 2021.
- [6] N. M. Rahmat, P. Gulo, D. Suherdi, and S. F. Rezky. Pemanfaatan Firewall Pada Jaringan Menggunakan Mikrotik RB951Ui-2HnD. *Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD*, vol. 4, no. 2, pp. 173–179, 2021, [Online]. Available: www.facebook.com
- [7] H. P. Fitriani, F. Dani, I. Fadilah, R. D. Fauzan, and M. R. Ardhyansyah. Implementasi Mikrotik Firewall sebagai Solusi Filtering Situs Judi Online dalam Jaringan. *JATI : Jurnal Mahasiswa Teknik Informatika*. 2025.
- [8] C. Kamila Wilujeng, A. Voutama Sistem Informasi, U. Singaperbangsa Karawang Jl HSRonggo Waluyo, T. Timur, and J. Barat. Implementasi Firewall Filter Rules sebagai Filtering Congtent pada Jaringan Komputer menggunakan Mikrotik. 2024.
- [9] S. Amuda, M. Mulya, and F. Kurniadi. Analisis dan Perancangan Simulasi Perbandingan Kinerja Jaringan Komputer Menggunakan Metode Protokol Routing Statis, Open Shortest Path First (OSPF) dan Border Gateway Protocol (BGP) (Studi Kasus Tanri Abeng University). *Jurnal Sistem Komputer dan Kecerdasan Buatan*. vol. 4, pp. 53–63, 2021.
- [10] P. Putra and K. Jaya. Implementasi Bandwidth Management Menggunakan Mikrotik Router OS Studi Kasus di PT Rejeki Maha Bumi Lestari. *RESI: Jurnal Riset Sistem Informasi*, Jul. 2022.
- [11] R. Aulianita, man Musyaffa, and R. Martiwi, “Penggunaan Metode IDS Dalam Implementasi Firewall Pada Jaringan untuk Deteksi Serangan Distributed Denial

- Of Service (DDoS),” Dec. 2021.
- [12] A. Syafiq, A. D. Putra, and F. Asharudin. Penerapan Manajemen Bandwidth dan Filtering Website menggunakan Layer 7 pada Mikrotik di Tajir.net. *JuTIK : Jurnal Teknologi Informasi dan Komputer*. 2023.
- [13] I. A. Rahman, M. T. Kurniawan, and R. R. Saedudin. Analisis Perbandingan Manajemen Bandwidth Quality of Service Dengan Menggunakan Metode Simple Queue Dan Queue Tree Pada Telkom University Landmark Tower. *Jurnal Sains Komputer dan Informatika*. 2023.
- [14] B. Fachri and R. Wahyu Surbakti. Perancangan Sistem dan Desain Undangan Digital menggunakan Metode Waterfall Berbasis Website. *Journal Of Science And Social Research*. 2021. [Online]. Available: <http://jurnal.goretanpena.com/index.php/JSSR>