Teknik Keamanan Akses Internet Untuk Parenting Menggunakan Metode Packet Filtering Pada Mikrotik

Internet Access Security Techniques For Parenting Using The Packet Filtering Method on Mikrotik

Dovan Suhardono[1], Eka Wahyudi[2], Bongga Arifwidodo[3*]
[1,2,3] Jurusan Teknik Telekomunikasi, Institut Teknologi Telkom Purwokerto
E-mail: [1]19101187@ittelkom-pwt.ac.id, [2]ekawahyudi@ittelkom-pwt.ac.id, [3*]bongga@ittelkom-pwt.ac.id
*Penulis Korespondensi

Abstrak

APJII melangsir data pada tahun 2021-2022 bahwa pengguna internet terus meningkat sebesar 77,02%. Kelompok usia 13 hingga 18 tahun merupakan data tertinggi pengguna akses internet. Sangat disayangkan usia tersebut pada dasarnya belum mengerti dampak dari pesatnya teknologi internet. Sehingga orang tua merupakan pengawas utama bagi anak saat menggunakan akses internet. Salah satu metode keamanan akses internet adalah metode packet filtering. Penelitian ini menggunakan metode packet filtering pada perangkat jaringan mikrotik kemudian menghasilkan notifikasi ketika terjadi pelanggaran. Informasi notifikasi akan diterima oleh administrator system melalui Telegram. Skenario penelitian ini menggunakan konfigurasi packet filtering dengan memasukkan alamat IP atau nomor port yang akan diblokir serta konfigurasi ke Telegram sebagai penerima notifikasi. Secara umum penelitian ini menunjukkan keberhasilan pemblokiran terhadap beberapa situs dan game online, serta memperoleh hasil waktu respon notifikasi dari bot Telegram yang lambat, dengan rata-rata sebesar 26,9 detik untuk media sosial dan 23,3 detik untuk game online.

Kata kunci: Mikrotik, Packet Filtering, Parenting, Telegram

Abstract

APJII released data in 2021-2022 that internet users continued to increase by 77.02%. The age group of 13 to 18 years is the highest number of internet access users. It's a shame that this age group basically doesn't understand the impact of rapid internet technology. So parents are the main supervisors for children when using internet access. One method of internet access security is the packet filtering method. This research uses the packet filtering method on Mikrotik network devices and then produces notifications when a violation occurs. Notification information will be received by the system administrator via Telegram. This research scenario uses a packet filtering configuration by entering the IP address or port number to be blocked and configuring Telegram as the notification recipient. In general, this research shows the success of blocking several sites and online games, as well as obtaining slow notification response times from Telegram bots, with an average of 26.9 seconds for social media and 23.3 seconds for online games.

Keywords: Mikrotik, Packet Filtering, Parenting, Telegram

1. PENDAHULUAN

Pengguna internet terus meningkat sebagai akibat dari koneksi internet yang lebih mudah diakses dan terjangkau, tersebarnya jaringan, serta peningkatan ketersediaan peralatan komputer hingga *smartphone*. Menurut data studi "Profil Pengguna Internet 2022" dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), Indonesia memiliki tingkat penetrasi internet sebesar 77,02% pada tahun 2021–2022. Rentang usia 13 hingga 18 tahun memiliki penetrasi internet tertinggi secara keseluruhan. Dari rentang usia tersebut, hampir semuanya (99,16%)

memiliki akses internet. Sebanyak 76,63% responden dalam kelompok usia ini mengakui peningkatan mengenai penggunaan internet mereka[1]. Yuliandre Darwis, Komisioner KPI Pusat, menyatakan bahwa orang tua memiliki peran penting mengamati bagaimana anak-anak berperilaku ketika menggunakan perangkat digital. Pasalnya, kemudahan informasi yang dapat diakses tanpa batas, hal ini sejatinya sangat baik, namun juga terdapat ancaman yang bisa saja menjadi dampak buruk pada perilaku anak. Menurut fakta yang berbeda, anak-anak usia sekolah sangat terpengaruh secara negatif oleh penggunaan internet. Jumlah kasus pengaduan anak yang melibatkan kejahatan internet dan pornografi (korban dan pelaku) mencapai 1.940 anak di bawah umur pada 2017-2019, menurut data Komisi Perlindungan Anak Indonesia (KPAI) [2]. Dari permasalahan di atas, diperlukan yang namanya *Parenting*.

Parenting dilakukan sesuai dengan perkembangan zaman, di zaman yang sudah semakin canggih ini, orang tua dituntut untuk semakin cerdas, semakin mawas, dan semakin bijak dalam melakukan edukasi terhadap anak-anak mereka yang bertujuan untuk meminimalisir dampak negatif dari kemajuan dan penggunaan teknologi yang mempengaruhi anak-anak mereka baik melalui lingkungan sekolah, pergaulan, atau lingkungan keluarga [3]. Agar anak-anak mereka dapat terpantau, perlu dilakukan adanya pembatasan akses internet sehingga orang tua dapat melakukan pengawasan terhadap hal-hal yang diakses melalui internet oleh anak-anak. Pembatasan tersebut merupakan suatu langkah yang dapat orang tua lakukan untuk mengasuh anak-anak mereka di tengah pesatnya perkembangan teknologi. Untuk melakukan pembatasan akses internet, diperlukan sebuah *router* yang memiliki fitur *firewall* untuk penyaringan paket (*Packet Filtering*).

Komunikasi paket data khususnya akses internet membutuhkan perangkat *Router* dimana fungsinya mengambil paket, menganalisisnya, dan mengirimkannya ke jaringan lain [4]. Pada tahapan selanjutnya proses komunikasi data sangat bergantung pada system distribusi yaitu *Firewall* sehingga trafik dapat dipilah dengan semestinya baik di jaringan lokal maupun [5]. Sehingga paket yang masuk dan keluar dari jaringan dapat dipantau, menghentikan paket yang mencurigakan segera tanpa menentukan apakah mereka aman atau tidak [6]. Tak lepas adanya sistem distribusi, kebutuhan teknologi keamanan jaringan akan lebih fokus terhadap lalu lintas paket yakni Paket Filtering, sehingga kontrol paket mana yang diizinkan masuk ke sistem atau jaringan dan paket mana yang dilarang [7]. Penyaringan tergantung pada sumber paket dan alamat tujuan. Namun, tidak setiap *router* memiliki karakteristik ini. Salah satu *router* yang memiliki fitur *Packet Filtering* yaitu *router* Mikrotik. *Router* Mikrotik merupakan sistem operasi yang berbasis kernel Linux ini dibuat untuk dapat mengelola jaringan komputer skala kecil, menengah, dan besar [8]. *Router* Mikrotik terdiri dari perangkat keras dan perangkat lunak dan dapat digunakan sebagai *router*, serta untuk penyaringan, *switching*, dan keperluan lainnya [9]. PC biasa dapat menjadi *router* dengan menggunakan sistem operasi dan *software* yang bernama Mikrotik. Hanya dengan board yang dilengkapi dengan OS Mikrotik, Mikrotik dapat dibedakan sebagai sistem operasi (OS) dan *board* yang tidak memerlukan komputer [10].

Berbagai penelitian telah dilakukan dengan menggunakan metode *Packet Filtering*. Pada penelitian [11] telah menganalisis kinerja dari *Packet Filtering* terhadap situs jejaring sosial dan *streaming* dengan berdasarkan pada alamat situs atau *domain*-nya. Kemudian pada penelitian [12] telah menganalisis mengenai kinerja dari Packet Filtering terhadap situs-situs yang mengandung pornografi dengan berdasarkan alamat IP. Selanjutnya pada penelitian [13] menganalisis mengenai kinerja *Packet Filtering* terhadap media sosial dan *game online* dengan berdasarkan alamat IP-nya. Pada penelitian [14] menganalisis mengenai monitoring jaringan dengan menggunakan fitur *Netwatch* pada Mikrotik dan Bot Telegram. Bot Telegram disini berfungsi mengirimkan notifikasi secara *realtime* ketika jaringan *up* and *down* kepada *administrator system*. Kemudian pada penelitian [15] menganalisis mengenai keamanan jaringan dengan menggunakan metode IPS dan Bot Telegram. Bot Telegram disini berfungsi untuk mengirimkan notifikasi secara *realtime* ketika terjadi serangan pada *server*. Notifikasi tersebut dikirimkan melalui Telegram kepada *administrator* jaringan.

Pada penelitian ini, penulis membuat sebuah sistem dengan metode filter paket port (yang dapat memblokir situs, media sosial, dan *game online*) yang mana pada penelitian sebelumnya

tidak adanya sistem notifikasi sehingga penelitian ini dengan pengembangan bot telegram. Bot Telegram disini berfungsi mengirimkan notifikasi ketika terjadi pelanggaran pengaksesan. Notifikasi tersebut akan dikirimkan kepada *administrator system*. Tujuan dari sistem tersebut adalah untuk membantu pengawasan orang tua terhadap penggunaan internet anak agar tetap terpantau.

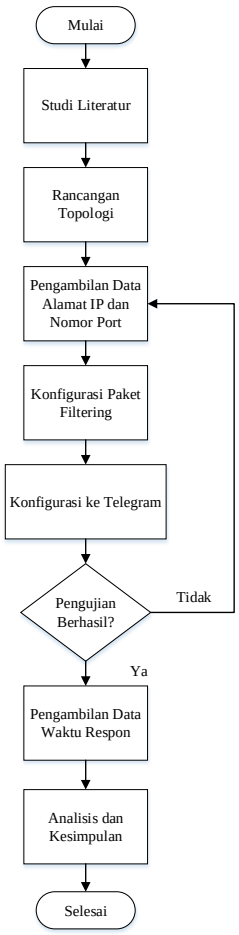
2. METODE PENELITIAN

2.1 Alur Penelitian

Penelitian ini dilakukan dengan melalui beberapa tahapan seperti pada diagram alur yang ditunjukkan pada Gambar 1. Gambar 1 menunjukan diagram alur perancangan sistem dalam penelitian ini. Langkah pertama dalam penelitian yaitu melakukan studi literatur beberapa penelitian terkait dengan pemblokiran akses internet dengan melakukan konfigurasi *packet filtering* pada *router* serta materi lain yang berhubungan dengan penelitian ini. Dengan membandingkan beberapa jurnal terkait dan melakukan perbandingan untuk menentukan judul dan juga fokus dari penelitian ini. Selain membandingkan dan menentukan fokus atau judul penelitian, tahap ini juga berfungsi untuk memahami konsep dasar dari topik tersebut.

Selanjutnya adalah menentukan rancangan topologi yang digunakan sebagai dasar dari arsitektur jaringan untuk membuat sistem yang mampu memblokir beberapa situs judi *online*, media sosial, dan *game online*. Topologi tersusun atas 1 buah *router* mikrotik yang digunakan untuk melakukan konfigurasi *packet filtering*, 3 buah laptop, dua di antaranya berperan sebagai *client* dan salah satunya menjadi *administrator system*, serta 3 buah *smartphone* sebagai *client*. Langkah selanjutnya adalah melakukan pengambilan data pertama dengan fitur *torch* yang merupakan salah satu *tools* pada mikrotik yang digunakan untuk melihat trafik jaringan secara *realtime* atau dapat dilakukan dengan menggunakan *tools nslookup* pada *command prompt* (cmd) dan akan memperoleh data yang berupa alamat IP dari situs judi *online*, media sosial, dan *game online* yang nantinya akan dikonfigurasi pada mikrotik di menu *filter rules* dengan cara memasukkan *chain* yang dipilih yaitu *chain forward* dengan protokol TCP/UDP, kemudian masukkan alamat IP dari situs judi *online*, media sosial, dan *game online* yang akan diblokir pada kolom *destination address*. Pilih *action drop* agar paket tersebut ditolak atau tidak diijinkan masuk. Selanjutnya melakukan konfigurasi pada mikrotik (winbox) agar ketika terjadi pelanggaran dalam pengaksesan internet *administrator system* akan menerima notifikasi melalui Telegram.

Setelah melakukan konfigurasi pada mikrotik, selanjutnya adalah melakukan pengujian dengan melakukan akses terhadap situs judi *online*/media sosial/*game online* apakah alamat IP yang didapatkan pada pengambilan data pertama berhasil diblokir atau tidak, jika berhasil maka langkah selanjutnya adalah melakukan pengambilan data kedua yang berupa waktu respon dari sistem notifikasi yang dilakukan sebanyak 20 kali kemudian diambil nilai rata-ratanya. Selanjutnya data-data yang sudah diperoleh dikumpulkan dalam bentuk tabel yang nantinya akan dianalisis dengan cara melihat filter rules apakah berhasil melakukan pemblokiran atau tidak dengan menggunakan alamat IP yang telah diperoleh serta menganalisis mengenai respon dari sistem notifikasi, setelah itu diambil kesimpulan ketika sudah selesai melakukan analisis.

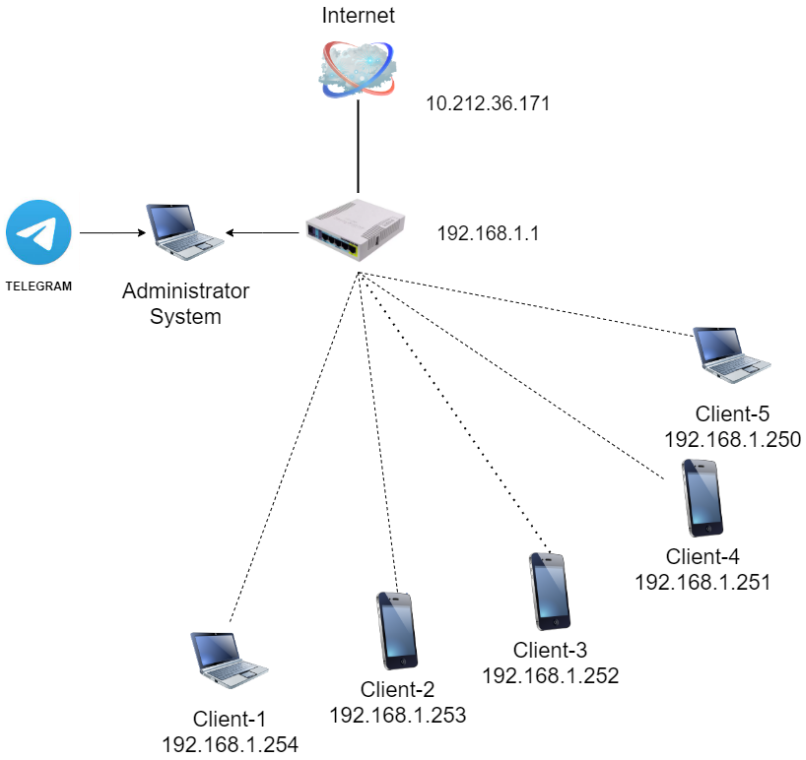


Gambar 1. Alur Penelitian

2.2 Perancangan Topologi Jaringan

Rancangan topologi yang digunakan sebagai dasar dari arsitektur jaringan untuk membuat sistem yang mampu memblokir beberapa situs judi *online*, media sosial, dan *game online* terlihat seperti pada Gambar 2 yang tersusun atas sebuah koneksi internet yang disediakan oleh *internet service provider*, 1 buah *router* mikrotik yang digunakan untuk melakukan konfigurasi *packet filtering*, 3 buah laptop, dua di antaranya berperan sebagai *client* dan salah satunya menjadi *administrator system*, serta 3 buah *smartphone* sebagai *client*. Pada topologi ini, mikrotik berperan sebagai DHCP *server* yang mengatur dan memberikan alamat IP secara otomatis kepada *client*, contohnya perangkat laptop dan *smartphone* yang disebut sebagai DHCP *client* karena perangkat-perangkat tersebut menerima alamat IP dari DHCP *server*.

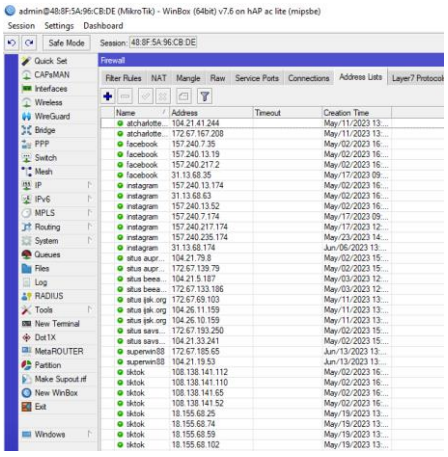
Perangkat-perangkat *client* tersebut, terhubung secara *wireless* dengan Mikrotik. *Administrator system* disini bertugas melakukan konfigurasi *packet filtering* yaitu dengan membuat beberapa *rules*, serta melakukan konfigurasi ke Telegram yang berfungsi untuk memberikan notifikasi, baik konfigurasi Telegram pada Mikrotik maupun pada laptop. Sehingga, ketika terjadi pengaksesan yang tidak sesuai dengan *rules*, maka Mikrotik akan memberikan notifikasi kepada *administrator system* melalui Telegram, yang mana notifikasi tersebut dapat diakses oleh *administrator system* melalui laptop atau *smartphone*.



Gambar 2. Topologi Jaringan

2.3 Konfigurasi Packet Filtering pada Mikrotik

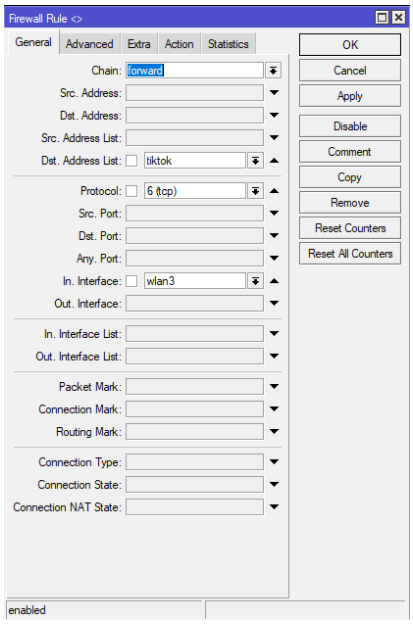
Pada penelitian ini, pemblokiran akan dilakukan dengan menggunakan *packet filtering* dengan berdasarkan alamat IP, nomor *port*, serta protokol yang digunakan, baik yang digunakan oleh situs, media sosial maupun *game online*. Namun sebelum melakukan konfigurasi *packet filtering*, pastikan sudah melakukan pengumpulan alamat IP mana saja yang akan diblokir dengan menggunakan fitur *torch*. Fitur *torch* merupakan salah satu *tools* pada mikrotik yang digunakan untuk melihat trafik jaringan secara *realtime* atau dapat dilakukan dengan menggunakan *tools nslookup* pada *command prompt* (cmd). Setelah memperoleh beberapa alamat IP, selanjutnya alamat IP tersebut kemudian akan dikumpulkan pada menu *address lists* di *software* winbox seperti yang terlihat pada Gambar 3.



Gambar 3. Address Lists

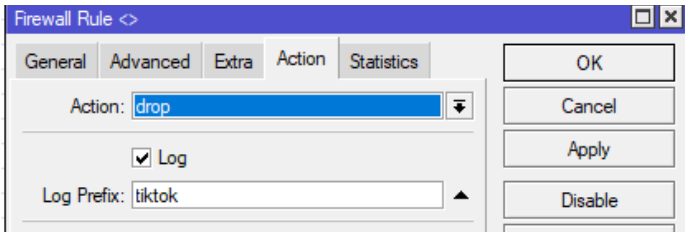
Konfigurasi *packet filtering* dilakukan dengan menggunakan alamat IP yang berhasil dikumpulkan pada menu *address lists* dan nomor *port* yang berhasil di-*capture* pada fitur *torch*,

konfigurasi dilakukan pada *software* winbox, yang pertama yaitu membuat *New Filter Rules* seperti Gambar 4, dilakukan konfigurasi dengan memasukkan *chain forward*, protokol TCP/UDP, In *Interface* mana yang akan diberi kebijakan atau aturan. Untuk situs judi dan media sosial, *rules* atau aturan yang dibuat itu berdasarkan alamat IP yang digunakan, sehingga peneliti memasukkan alamat IP dari situs judi *online* dan media sosial seperti yang terlihat pada Gambar 4 pada kol*om dst. Address*. Sedangkan untuk *game online, rules* atau aturan yang dibuat itu berdasarkan nomor *port* yang digunakan, sehingga peneliti memasukkan nomor *port* berapa saja yang digunakan oleh *game online* pada kolom *dst. Port.*



Gambar 4. *Filter Rules*

Selanjutnya yaitu membuat action seperti pada Gambar 5, konfigurasi kolom *action* dengan *action drop* agar paket tersebut ditolak atau tidak diijinkan masuk. Selanjutnya melakukan pengelompokkan alamat IP yang didapatkan sesuai dengan kategorinya yang disebut *log prefix*. Misal tiktok, nantinya pada log mikrotik dan notifikasi Telegram akan muncul informasi sedang mengakses tiktok.



Gambar 5. *Action* pada *Firewall Rules*

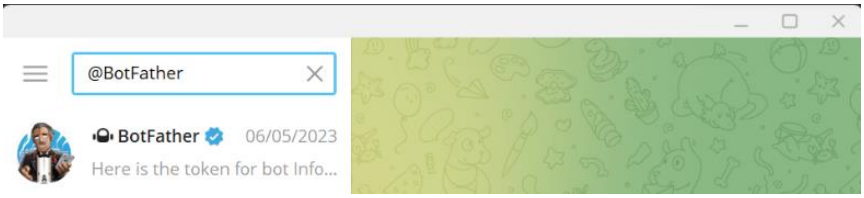
2.4 Konfigurasi ke Telegram

Setelah melakukan konfigurasi *packet filtering*, selanjutnya adalah melakukan konfigurasi ke Telegram yang dilakukan oleh *administrator system* pada laptop/PC dan Mikrotik. Konfigurasi ini digunakan untuk membuat pesan notifikasi Telegram yang kemudian akan diterima oleh *administrator system*.

2.4.1 Konfigurasi Telegram di Laptop/PC (Administrator System)

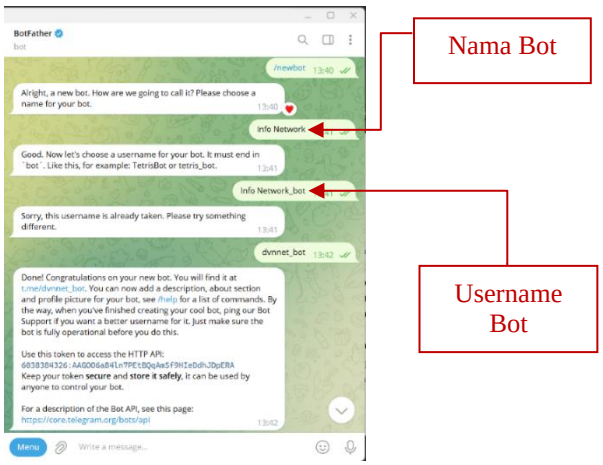
Langkah awal konfigurasi Telegram di laptop/PC yaitu dengan melakukan pembuatan bot pada aplikasi Telegram desktop. Pembuatan bot dilakukan dengan menggunakan sebuah bot yang bernama @BotFather. @BotFather merupakan akun bot

Official Telegram yang berfungsi untuk membuat bot Telegram. Pertama, pada search Telegram ketik @BotFather seperti pada Gambar 6 kemudian buka botnya dengan cara klik bot yang bercentang biru.



Gambar 6. Bot Father

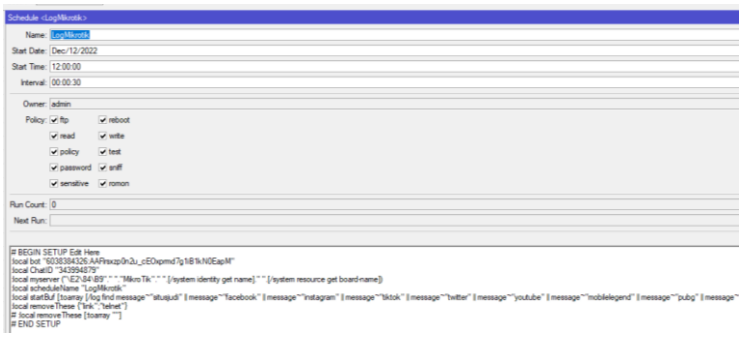
Kemudian masukkan nama bot dan *username* untuk bot baru tersebut seperti pada Gambar 7. Di sini peneliti menamai botnya dengan sebutan Info Network dengan *username* @dvnnet_bot lalu @BotFather akan mengirimkan sebuah token bot API Telegram yang digunakan untuk mendukung komunikasi dengan API Telegram.



Gambar 7. Proses Pembuatan Bot Telegram pada Laptop/PC

2.4.2 Konfigurasi Telegram di Mikrotik

Setelah melakukan konfigurasi Telegram pada laptop, selanjutnya adalah melakukan konfigurasi ke Telegram di Mikrotik yang dilakukan pada *software* winbox. Pada tahap ini, peneliti memasukkan sebuah *script* dan *log prefix* ke *system scheduler* pada Mikrotik. *Script* dan *Log prefix* tersebut digunakan untuk membuat notifikasi yang kemudian akan diterima oleh *administrator system* melalui Telegram. *System scheduler* merupakan menu pada *software* winbox yang digunakan untuk memasukkan *script*. *Script* tersebut terdapat token bot API Telegram agar dapat membaca serta mengirim *log prefix* ke Telegram. *Script* akan dimasukkan pada *on event* yang terlihat seperti pada Gambar 8.

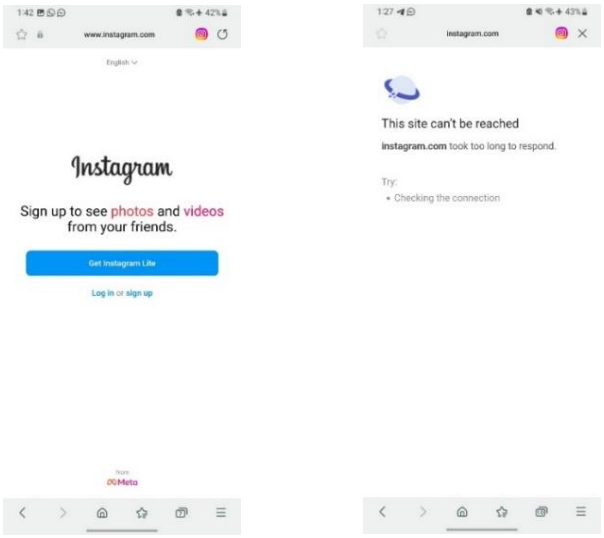


Gambar 8. *Scheduler*

3. HASIL DAN PEMBAHASAN

3.1 Hasil Pengujian Sistem

Pada penelitian ini, pemblokiran akan dilakukan dengan menggunakan *packet filtering* dengan berdasarkan alamat IP, nomor *port*, serta protokol yang digunakan, baik yang digunakan oleh situs, media sosial maupun *game online*. Pengujian sistem dilakukan dengan 2 skenario, yaitu ketika *rules packet filtering* tidak aktif dan ketika *rules packet filtering* aktif.



(a) (b)

Gambar 9. (a) Tampilan Instagram ketika *rules packet filtering* tidak aktif (b) Tampilan Instagram ketika *rules packet filtering* aktif

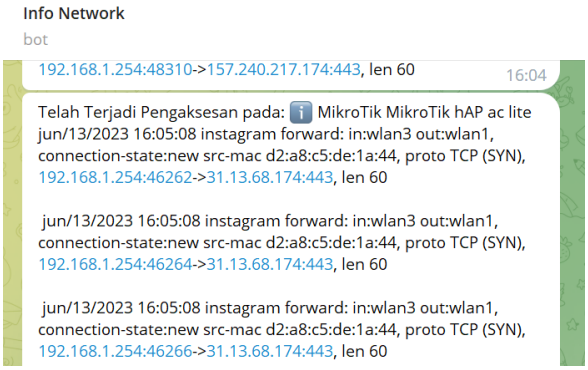
(a)

(b)

Gambar 10. (a) Tampilan Mobile Legend ketika *rules packet filtering* tidak aktif (b) Tampilan Mobile Legend ketika *rules packet filtering* aktif

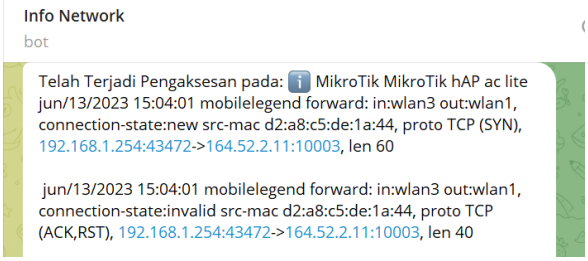
Ketika *rules packet filtering* tidak aktif, maka semua situs, media sosial, maupun *game online* dapat diakses seperti pada Gambar 9 (a) dan Gambar 10 (a). Sedangkan ketika *rules packet filtering* aktif, maka semua situs, media sosial, maupun *game online* tidak dapat diakses seperti pada Gambar 9 (b) dan Gambar 10 (b) kemudian *administrator system* akan menerima notifikasi pelanggaran.

Notifikasi pelanggaran tersebut berisi informasi pengaksesan seperti alamat IP yang mengakses, alamat IP yang diakses, dan waktu terjadi pelanggarannya. Sebagai contoh ketika mengakses media sosial yang diblokir maka akan menerima notifikasi seperti yang terlihat pada Gambar 11 yang berisi informasi bahwa pada tanggal 13 Juni 2023 pukul 16:05:08, alamat IP 192.168.1.254 mengakses sebuah alamat IP yaitu 31.13.68.174 yang mana alamat IP tersebut merupakan alamat IP yang digunakan oleh Instagram.



Gambar 11. Notifikasi Pelanggaran Pengaksesan Instagram

Sedangkan ketika mengakses *game online* yang diblokir maka akan menerima notifikasi seperti yang terlihat pada Gambar 12 yang berisi informasi bahwa pada tanggal 13 Juni 2023 pukul 15:04:01, alamat IP 192.168.1.254 mengakses sebuah nomor *port* yaitu 10003 yang mana nomor *port* tersebut merupakan nomor *port* yang digunakan oleh Mobile Legend.



Gambar 12. Notifikasi Pelanggaran Pengaksesan Mobile Legend

3.2 Hasil Waktu respon Notifikasi

Pada pengambilan data waktu respon notifikasi dilakukan untuk mengukur respon waktu dari pesan notifikasi ketika terjadi pelanggaran dalam pengaksesan. Pesan notifikasi sistem secara otomatis dikirimkan ke Telegram *administrator system*. Pada Tabel 1 berikut merupakan hasil pengujian waktu respon notifikasi dengan memanfaatkan *system scheduler* pada mikrotik dan bot API Telegram. Pengujian dilakukan pada Instagram dan Mobile Legend, masing-masing dilakukan sebanyak 20 kali.

Tabel 1. Hasil Pengujian Waktu Respon Notifikasi

Waktu Respon (Detik)		
Pengambilan Ke-	**Instagram**	**Mobile Legend**
1	76	102
2	14	54

Waktu Respon (Detik)		
Pengambilan Ke-	**Instagram**	**Mobile Legend**
3	2	38
4	38	17
5	46	3
6	7	11
7	17	15
8	11	20
9	12	12
10	57	45
11	7	11
12	20	12
13	11	13
14	76	30
15	50	15
16	50	15
17	8	11
18	17	16
19	7	15
20	12	11
Rata-Rata	26,9	23,3

Pada Tabel 1 diperoleh hasil rata-rata waktu respon notifikasi ketika terjadi pelanggaran untuk Instagram sebesar 26,9 detik bot API Telegram merespon dengan mengirimkan pesan notifikasi dan untuk Mobile Legend sebesar 23,3 detik.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil implementasi dan pengujian dari *Packet Filtering* yang berfungsi sebagai pemblokir sebuah situs maupun *game online*, dengan Telegram sebagai penerima notifikasi, dapat disimpulkan bahwa *packet filtering* bekerja sesuai dengan *rules* atau aturan yang dibuat oleh *administrator system* dan bot Telegram berhasil bekerja mengirimkan notifikasi ketika terjadi pelanggaran pengaksesan dengan waktu respon notifikasi yang lambat, dengan rata-rata sebesar 26,9 detik untuk media sosial dan 23,3 detik untuk *game online*. Saran untuk penelitian selanjutnya adalah dapat menggunakan lebih banyak situs (terutama situs judi dan pornografi) dan *game online* yang diblokir agar dapat mewujudkan intenet sehat untuk anak serta dapat melakukan pengembangan sistem notifikasi dengan menggunakan bot WhatsApp.

DAFTAR PUSTAKA

[1] "Penetrasi Internet di Kalangan Remaja Tertinggi di Indonesia." https://databoks.katadata.co.id/datapublish/2022/06/10/penetrasi-internet-di-kalangan-remaja-tertinggi-di-indonesia (accessed Dec. 24, 2022).

[2] "Peran Orang Tua dan Pola Asuh Anak Di Era Digital – DP3AP2KB PROVINSI NTB." https://dp3ap2kb.ntbprov.go.id/2022/02/15/peran-orang-tua-dan-pola-asuh-anak-di-era-digital/ (accessed Dec. 24, 2022).

[3] G. Lanang, A. Wiranata, A. Badan, A. Nasional, and P. Bali, "PENERAPAN POSITIVE PARENTING DALAM PEMBIASAAN POLA HIDUP BERSIH DAN SEHAT KEPADA ANAK USIA DINI." [Online]. Available: https://www.ejournal.ihdn.ac.id/index.php/PW/issue/archive

[4] M. Ali and F. Latifah, "IMPLEMENASI BLOCK ACCESS PENGGUNA LAYANAN INTERNET DENGAN METODE FILTER RULE dan LAYER 7 PROTOCOL," Journal of

Information System, Applied, Management, Accounting and Research, vol. 5, no. 2, p. 340, May 2021, doi: 10.52362/jisamar.v5i2.422.

[5] Gregorius Hendita Artha Kusuma, "Sistem Firewall untuk Pencegahan DDOS ATTACK di Masa Pandemi Covid-19," Journal of Informatics and Advanced Computing (JIAC), vol. 3, no. 1, 2022.

[6] W. W. Purba and R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," AITI: Jurnal Teknologi Informasi, vol. 17, no. Agustus, pp. 143–158, 2020.

[7] A. Dzulfiqri and A. Hidayat, "IMPLEMENTASI MANAJEMEN BANDWIDTH DAN FILTERING CONTENT DENGAN ROUTER MIKROTIK PADA SMP MUHAMMADIYAH 3 METRO," 2022.

[8] S. A. A. Deri Andriyana Juhana, "PERANCANGAN SISTEM KEAMANAN JARINGANMENGGUNAKAN MIKROTIK ROUTER PADA MANAGEMENT BANDWIDTHDI CV. ALGI PIN BANDUNG," TELEMATIKA, vol. 3, no. 1, 2021.

[9] L. Riyandari, T. Wahyuningsih, dan Joko Purnomo, and P. Studi Teknik Informatika STMIK Widya Utama, "RANCANG BANGUN JARINGAN INTERNET DENGAN MEMPERHATIKAN ETIKA PROFESI TI MENGGUNAKAN WEB FILTERING PADA ROUTER MIKROTIK 951G-2HND."

[10] A. M. L. Hasrul Hasrul, "PENGEMBANGAN JARINGAN WIRELESS MENGGUNAKAN MIKROTIK ROUTER OS RB750 PADA PT. AMANAH FINANCE PALU," JESIK, vol. 3, no. 1, 2017.

[11] Alfred and J. C. Chandra, "PEMANFAATAN FIREWALL PADA JARINGAN KOMPUTER SMK FADILAH," J. I D E A L I S, vol. 1, no. 5, pp. 422–428, 2018.

[12] A. Nurfauzi, E. Rikardo Nainggolan, S. N. Khasanah, A. Setiadi, S. Nusa, and M. Jakarta, Implementasi Firewall Filtering Web dan Manajemen Bandwith Menggunakan Mikrotik.

[13] S. Jayanto, A. Tantoni, H. Asyari, P. Studi, T. Informatika, and S. Lombok, "Jurnal Ranah Publik Indonesia Kontemporer Implementasi Keamanan Jaringan dengan Packet Filtering Berbasis Mikrotik Untuk Internet Positif Di SMKN 1 Praya." [Online]. Available: https://rapik.pubmedia.id/index.php/rapik

[14] Wahyat and Agus Teddyana, "Monitoring Jaringan Internet Menggunakan Notifikasi Bot API Telegram," SATIN - Sains dan Teknologi Informasi, vol. 7, no. 1, pp. 144–153, Jun. 2021, doi: 10.33372/stn.v7i1.713.

[15] R. Reza Abdullah and A. Nurhayati, "MONITORING SISTEM KEAMANAN JARINGAN BERBASIS TELEGRAM BOT PADA LOCAL AREA NETWORK," Journal of Informatics and Communications Technology, vol. 1, no. 2, pp. 45–053, 2019, [Online]. Available: www.sourcefire.com.