

IMPLEMENTASI MONITORING DAN BLOKIR GAME ONLINE DI LABORATORIUM FASILKOM UNSIKA BERBASIS MANGLE DAN TELEGRAM

Aditya Rizky Darmawan^{1*}, Agung Susilo Yuda Irawan², Arip Solehudin³, Purwantoro⁴, Garno⁵

^{1,2,3,4,5}Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Singaperbangsa Karawang; Jl. HS. Ronggo Waluyo, Puseurjaya, Telukjambe Timur, Karawang, Jawa Barat 41311; (0267) 641177

Keywords:

Pemblokiran Game Online, Mangle, Bot Telegram API, Packet Filtering, Pemantauan Aktivitas Jaringan.

Correspondent Email:

2210631170109@student, unsika.ac.id

Abstrak. Penyalahgunaan internet untuk aktivitas game online di Laboratorium Fasilkom UNSIKA mengganggu kelancaran kegiatan akademik. Penelitian ini bertujuan merancang sistem pemantauan dan pemblokiran akses game online berbasis Mangle dan Telegram dengan metodologi Network Development Life Cycle (NDLC). Pemblokiran dieksekusi melalui Packet Filtering berbasis kombinasi Mangle untuk game online berbasis aplikasi dan Address List untuk game online berbasis web. Sistem secara dinamis mengisolasi IP pelanggar di Address List khusus dan mengirimkan notifikasi real-time ke Telegram administrator memanfaatkan Scripting dan Scheduler. Hasil evaluasi menunjukkan tingkat keberhasilan pemblokiran mencapai 100%. Dari segi efisiensi perangkat keras, arsitektur sistem terbukti sangat ringan, di mana tambahan beban kerja CPU router secara konsisten berada pada zona "Sangat Aman Berlebih" menurut standar CPU Utilization Factor, bahkan ketika menangani insiden pelanggaran secara massal. Selain itu, kecepatan waktu respons sistem dalam mengirimkan notifikasi peringatan ke Telegram menunjukkan hasil dibawah 10 detik dengan indeks "Memuaskan" berdasarkan standar ITU-T G.1010..



Copyright © 2026 The Author(s), Published by Jurnal Informatika dan Teknik Elektro Terapan. This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

Abstract. Internet misuse for online gaming activities in the FASILKOM UNSIKA Laboratory disrupts the smoothness of academic activities. This research aims to design an online game access monitoring and blocking system based on Mangle and Telegram using the Network Development Life Cycle (NDLC) methodology. Blocking is executed through Packet Filtering, combining Mangle for application-based online games and Address List for web-based online games. The system dynamically isolates the violator's IP in a specific Address List and sends real-time notifications to the administrator's Telegram utilizing Scripting and Scheduler. Evaluation results indicate that the blocking success rate reaches 100%. In terms of hardware efficiency, the system architecture proved to be highly lightweight, where the additional router CPU workload consistently remains in the "Highly Safe" zone according to the CPU Utilization Factor standard, even when handling mass violation incidents. Furthermore, the system's response time in sending warning notifications to Telegram shows results of under 10 seconds, achieving a "Satisfactory" index based on the ITU-T G.1010 standard.

1. PENDAHULUAN

Perkembangan teknologi informasi menjadikan infrastruktur jaringan komputer sebagai tulang punggung utama dalam mendukung operasional institusi pendidikan, termasuk di Laboratorium Fakultas Ilmu Komputer (Fasilkom) Universitas Singaperbangsa Karawang (UNSIKA) [1][2]. Penggunaan *router* MikroTik sebagai pusat kendali jaringan di lingkungan akademik telah terbukti efektif dalam menjaga stabilitas koneksi bagi pengguna [3]. Meskipun fasilitas jaringan disediakan khusus untuk menunjang kegiatan akademik seperti praktikum dan *e-learning*, kebebasan akses internet tersebut kerap disalahgunakan oleh mahasiswa untuk bermain *game online* di tengah jam perkuliahan [4][5]. Aktivitas ini tidak hanya memonopoli *bandwidth* yang mengakibatkan penurunan kualitas jaringan bagi mahasiswa lain, tetapi juga menciptakan iklim belajar yang tidak disiplin [6][7]. Oleh karena itu, diperlukan sebuah sistem keamanan jaringan yang mampu melakukan pengawasan secara proaktif dan mengeksekusi pemblokiran secara otomatis.

Berbagai penelitian sebelumnya telah berupaya mengatasi penyalahgunaan akses jaringan menggunakan pendekatan pemfilteran paket. Penelitian yang dilakukan oleh Aziz dkk. [8] dan Sianhar & Marhalim [9] mengimplementasikan metode *Firewall Filtering* dengan *Layer 7 Protocol* untuk memblokir situs dan *game online* di lingkungan sekolah. Pendekatan serupa juga diterapkan oleh Al Kautsar & Sastra [10] pada jaringan RT/RW Net. Namun, penggunaan *Layer 7 Protocol* yang melakukan inspeksi paket secara mendalam (*Deep Packet Inspection*) terbukti memberikan beban komputasi yang tinggi pada CPU *router*, di mana penelitian Ma'mun & Muflih [11] mencatatkan rata-rata peningkatan beban CPU hingga 26% saat mengeksekusi *Layer 7 Protocol*. Di sisi lain, Suhardono dkk. [12] menerapkan metode *Packet Filtering* berbasis *IP/Port* dengan integrasi *Bot Telegram API* sebagai media notifikasi pelanggaran. Walaupun berhasil melakukan pemblokiran, rata-rata waktu respons notifikasinya terbilang sangat lambat, yakni mencapai 26,9 detik.

Berdasarkan *gap analysis* dari literatur terdahulu, kebaruan pada penelitian ini difokuskan pada optimalisasi efisiensi beban kerja perangkat keras *router* dan percepatan

respons pelaporan insiden secara *real-time*. Penelitian ini mengusulkan arsitektur *Packet Filtering* yang mengkombinasikan fitur *Mangle* untuk mengenali *port* dan protokol spesifik *game* berbasis aplikasi, serta *Address List* dinamis untuk menerjemahkan domain *game* berbasis *web* secara otomatis. Pendekatan ini diusulkan untuk menghindari tingginya beban CPU akibat penggunaan *Layer 7 Protocol*. Alamat IP pelanggar kemudian diisolasi, dan sistem akan memicu fitur *Scripting* dan *Scheduler* pada MikroTik untuk mengirimkan peringatan otomatis melalui *Bot Telegram API*.

Tujuan utama dari penelitian ini adalah merancang, mengimplementasikan, serta mengevaluasi sistem pemantauan dan pemblokiran akses *game online* di Laboratorium Fasilkom UNSIKA. Evaluasi sistem dititikberatkan pada tiga metrik utama, yakni tingkat efektivitas pemblokiran, efisiensi beban kerja CPU pada *router* pengelola, serta kecepatan waktu respons pengiriman notifikasi ke Telegram, guna mewujudkan lingkungan akademik yang tertib dan kondusif.

2. TINJAUAN PUSTAKA

2.1 Jaringan Komputer

Jaringan komputer merupakan sistem yang dimana meliputi dua atau lebih komputer yang terhubung satu sama lain baik menggunakan kabel (*wired*) maupun nirkabel (*Wireless*) untuk saling melakukan pertukaran data, informasi serta sumber daya. Dengan adanya jaringan komputer, berbagai perangkat dapat saling berkomunikasi serta berinteraksi sehingga dapat saling berbagi sumber daya seperti printer, scanner, hingga koneksi internet [13].

2.2 Game Online

Game online merupakan sebuah permainan yang dapat dimainkan ketika terhubung dengan jaringan, baik melalui jaringan lokal maupun internet yang biasanya dimainkan secara bersamaan dengan pemain lain yang jumlahnya tidak terbatas yang mempunyai sifat rekreasi atau hiburan [14].

2.3 Packet Filtering

Packet Filtering merupakan metode keamanan dalam sistem jaringan komputer yang beroperasi dengan cara menyeleksi, mengelola, serta mengontrol lalu lintas paket data yang keluar dan masuk. Proses penyaringan ini dilakukan melalui inspeksi terhadap atribut pada *header* paket data, seperti

alamat IP asal dan tujuan, nomor *port*, hingga jenis protokol yang digunakan. Dengan mengevaluasi kriteria-kriteria tersebut terhadap parameter aturan yang telah ditetapkan, sistem dapat secara tegas menentukan paket data mana yang diizinkan untuk melewati *router* (*accept*) dan paket mana yang harus diblokir (*drop*), sehingga jaringan terlindungi dari akses yang tidak memiliki otorisasi [15].

2.4 Mangle

Mangle merupakan salah satu fitur yang terintegrasi di dalam sistem *Firewall* MikroTik. Fungsi utama dari fitur ini adalah untuk memberikan identifikasi atau penandaan khusus, baik berupa penanda koneksi (*connection mark*) maupun penanda paket (*packet mark*), terhadap aliran data yang melewati, masuk, maupun keluar dari antarmuka *router*. Tanda baca yang disematkan oleh *Mangle* pada sebuah paket data tidak beroperasi secara independen, melainkan akan diestafetkan dan digunakan sebagai acuan parameter oleh fitur-fitur lanjutan MikroTik lainnya, seperti dalam proses pembatasan kecepatan, perutean dinamis, hingga pengeksekusian aturan pemblokiran lalu lintas [16].

2.5 Address List

Address List merupakan salah satu fitur manajemen pada perangkat MikroTik RouterOS yang dirancang secara khusus untuk menyederhanakan kompleksitas konfigurasi keamanan jaringan. Fitur ini berfungsi untuk menghimpun, mengelompokkan, serta merepresentasikan sejumlah alamat IP, rentang jaringan (*subnet*), maupun sekumpulan nama domain ke dalam satu identitas parameter nama yang tunggal. Melalui metode pengelompokan ini, administrator jaringan tidak perlu lagi membuat aturan kebijakan secara berulang-ulang untuk setiap entitas alamat IP yang berbeda, melainkan cukup memanggil nama parameter dari kelompok tersebut [17].

2.6 Scripting & Scheduler Mikrotik

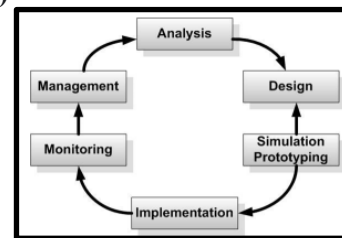
Scripting pada lingkungan MikroTik RouterOS merupakan sebuah fasilitas pemrograman internal yang disediakan untuk mengotomatisasi berbagai instruksi, tugas, dan konfigurasi manajemen jaringan. Sebuah *script* pada dasarnya bersifat pasif dan membutuhkan pemicu agar dapat dieksekusi. Untuk memfasilitasi hal tersebut, MikroTik menyediakan fitur *Scheduler* yang bertindak

sebagai subsistem penjadwalan dan manajemen waktu. *Scheduler* berfungsi sebagai pemicu utama (*trigger*) yang mengotomatisasi eksekusi *script* yang telah dibuat sebelumnya. Administrator jaringan dapat mengonfigurasi *Scheduler* agar sebuah *script* berjalan pada spesifikasi waktu dan tanggal tertentu, beroperasi secara berulang terus-menerus berdasarkan interval waktu, maupun dieksekusi secara otomatis sesaat setelah sistem operasi *router* dimuat ulang atau *startup* [18].

2.7 Bot Telegram API

Bot Telegram API (*Application Programming Interface*) merupakan sebuah antarmuka komunikasi berbasis HTTP yang dirancang secara khusus untuk memfasilitasi pengembang (*developer*) dalam membangun dan mengintegrasikan program bot ke dalam ekosistem Telegram. Bot itu sendiri bertindak layaknya akun pengguna virtual pihak ketiga yang beroperasi secara otomatis di latar belakang tanpa memerlukan campur tangan manusia. Melalui antarmuka API ini, perangkat atau aplikasi eksternal dapat melakukan berbagai interaksi dua arah secara otomatis, seperti menerima perintah, mengolah data, hingga mengirimkan pesan balasan secara dinamis ke dalam ruang obrolan [19].

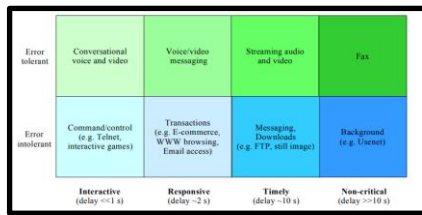
2.8 Network Development Life Cycle (NDLC)



Gambar 2.1 Tahapan NDLC

Network Development Life Cycle (NDLC) merupakan metode yang digunakan untuk merancang serta mengoptimalkan infrastruktur jaringan yang disertai pemantauan untuk memahami bagaimana kinerja dalam suatu jaringan tersebut yang memiliki 6 tahapan, yakni Analisis, Desain, Simulasi, Implementasi, Pemantauan, dan Manajemen [20].

2.9 Standar ITU-T G.1010



Gambar 2.2 Model User-Centric QoS Categories ITU-T

Standar ITU-T G.1010 adalah panduan resmi dari *International Telecommunication Union* (ITU) untuk mengevaluasi *Quality of Service* (QoS) multimedia berdasarkan ekspektasi dan persepsi pengguna akhir (*end-user*). Pengukuran kelayakan performa pada standar ini didasarkan pada dua parameter utama, yakni toleransi terhadap kehilangan informasi (*information loss*) dan waktu tunda (*delay*) [21].

2.10 CPU Utilization Factor

CPU Utilization Factor merupakan indikator yang mengukur persentase waktu prosesor saat aktif menjalankan instruksi, di luar dari waktu diamnya (*idle*). Tingkat utilisasi yang terlalu tinggi memiliki risiko masalah yang besar, karena setiap adanya penambahan, perubahan, atau koreksi sistem akan berpotensi langsung memicu kondisi *overload*. Sebaliknya, tingkat utilisasi yang terlalu rendah juga mengindikasikan ketidakefisienan anggaran (*cost-effective*). Hal ini menandakan bahwa sistem dirancang secara berlebihan (*overengineered*) dan spesifikasinya seharusnya bisa diturunkan menggunakan perangkat keras yang lebih terjangkau [22]. *CPU Utilization Factor* dibagi menjadi beberapa *zones* berdasarkan utilisasi dalam satuan persen yang tertera pada **Tabel 2.1**.

Tabel 2.1. CPU Utilization Zones

Utilization (%)	Zones
<26	Sangat aman berlebih
26-50	Sangat aman
51-68	Aman
69	Batas teoritis
70-82	Dipertanyakan
83-99	Berbahaya

100	Kritis
>100	Kelebihan beban

3. METODE PENELITIAN

Penelitian ini dilaksanakan di Laboratorium Fakultas Ilmu Komputer (Fasilkom) Universitas Singaperbangsa Karawang (UNSIKA). Metodologi yang diadaptasi sebagai fondasi pengembangan sistem adalah *Network Development Life Cycle* (NDLC). Pemilihan NDLC didasarkan pada kecocokannya dengan proses optimalisasi infrastruktur jaringan fisik yang sudah beroperasi dan fokus yang kuat pada pengujian teknis serta pemantauan jaringan. Tahapan NDLC dalam penelitian ini mencakup enam langkah berurutan.

3.1 Analisis

Tahap pengumpulan data yang dilakukan melalui metode kualitatif, yakni wawancara dengan pengelola laboratorium untuk mengidentifikasi masalah, observasi langsung terhadap kondisi fisik dan arsitektur *router*, serta kajian dokumentasi topologi jaringan untuk merumuskan spesifikasi sistem.

3.2 Desain

Penerjemahan kebutuhan sistem ke dalam rancangan teknis yang meliputi perancangan pemodelan topologi menggunakan *Cisco Packet Tracer*, penyusunan *flowchart* alur pemblokiran, perancangan kebijakan *Firewall Mangle* dan *Address List*, serta pembuatan *pseudocode* untuk logika *Scripting Telegram*.

3.3 Simulasi

Pengujian awal fungsionalitas desain yang dilakukan pada lingkungan berskala kecil yang terisolasi (*staging environment*) guna memvalidasi kemampuan deteksi *Firewall* dan *Script* pelaporan sebelum diterapkan secara massal.

3.4 Implementasi

Tahap eksekusi dengan menerapkan rancangan konfigurasi *Mangle*, *Address List*, *Filter Rule*, *Scripting*, dan *Scheduler* secara langsung ke dalam sistem operasi perangkat *router* MikroTik utama di lokasi penelitian.

3.5 Pemantauan

Tahap pengujian kinerja sistem yang menggunakan kerangka desain eksperimen.

Pemilihan perangkat yang diuji menggunakan metode *Purposive Sampling* agar sampel dapat merepresentasikan setiap segmen ruangan laboratorium secara proporsional. Khusus untuk skenario pengujian ketahanan beban kerja CPU, penentuan jumlah sampel mengadopsi Prinsip Pareto untuk menyimulasikan beban komputasi secara serentak. Evaluasi difokuskan pada efektivitas pemblokiran, tingkat utilitas CPU, dan kecepatan waktu respons notifikasi.

3.6 Manajemen

Tahap akhir guna menjamin keberlanjutan sistem melalui penyusunan pedoman dokumentasi teknis pemeliharaan jaringan dan proses serah terima tata kelola *Bot Telegram* kepada pihak pengelola laboratorium.

4. HASIL DAN PEMBAHASAN

Bagian ini menguraikan hasil implementasi sistem pemantauan dan pemblokiran akses *game online* di Laboratorium Fasilkom UNSIKA, dilanjutkan dengan evaluasi dan pembahasan komprehensif terhadap performa sistem berdasarkan tiga metrik utama: efektivitas pemblokiran, beban kerja CPU *router*, dan waktu respons notifikasi Telegram

4.1 Analisis

Tahap awal ini berfokus pada pengumpulan data dan identifikasi masalah pada infrastruktur jaringan yang sedang beroperasi, yang dijabarkan ke dalam empat proses pengamatan

4.1.1 Wawancara

Berdasarkan wawancara dengan pengelola laboratorium (Asisten Laboratorium), ditemukan tingginya insiden mahasiswa yang bermain *game online* saat perkuliahan berlangsung. Upaya mitigasi sebelumnya, yakni penerapan pembatasan hak *administrator* untuk instalasi aplikasi, dinilai tidak efektif karena tidak dapat mencegah *web game* berbasis *browser* dan justru menghambat proses praktikum mahasiswa. Selain itu, pengelola kesulitan melakukan pengawasan visual secara konstan saat kelas sedang berjalan.

4.1.2 Observasi

Pengamatan langsung terhadap arsitektur fisik laboratorium menunjukkan bahwa infrastruktur didukung oleh *router* utama MikroTik RouterBoard hEX (RB750Gr3) berspesifikasi CPU MIPS 1004Kc (4 core) 880 MHz dan memori 256 MiB.



Gambar 4.1 Pemetaan Perangkat Keras Laboratorium Komputer

Distribusi jaringan dikelola menggunakan beberapa *switch* yang terhubung ke total 124 unit komputer klien, yang tersebar di empat ruangan utama, yakni Lab Lanjut 1, Lab Lanjut 2, Lab Dasar 1, dan Lab Dasar 2 seperti yang dirincikan pada **Tabel 4.1**.

Tabel 4.1 Distribusi Perangkat Switch dan Komputer Laboratorium

Lokasi	Perangkat Switch	Jumlah Komputer
Lab Lanjut 1	1 unit TP-Link TL-SG1048 (48-Port)	31
Lab Lanjut 2	1 unit TP-Link TL-SG1048 (48-Port)	31
Lab Dasar 1	1 unit D-Link DGS-1024C (24-Port) dan 1 unit TP-Link TL-SG1024D (24-Port)	31
Lab Dasar 2	1 unit TP-Link TL-SG1024D (24-Port) dan 1 unit Cisco SG95-24 (24-Port)	31
Titik Outdoor	1 unit TP-Link 8-Port Gigabit Desktop Switch	-
Total Komputer		124

4.1.3 Kajian Dokumentasi

Analisis terhadap alur distribusi internet menunjukkan bahwa laboratorium menerapkan topologi *Tree* dengan arsitektur mendatar (*flat network*) tanpa adanya segmentasi jaringan (*Virtual Local Area Network / VLAN*). Distribusi pengalaman jaringan dikonfigurasi menggunakan skema IP statis pada segmen 172.18.3.0/25 dengan rincian pada **Tabel 4.2**.

Tabel 4.2 Skema IP Address Jaringan Laboratorium

Struktur Address	IP Address
Network Address	172.18.3.0
Subnet Mask	255.255.255.128
Broadcast Address	172.18.3.127
Default Gateway	172.18.3.1
IP Komputer Laboratorium	172.18.3.2 - 172.18.3.126

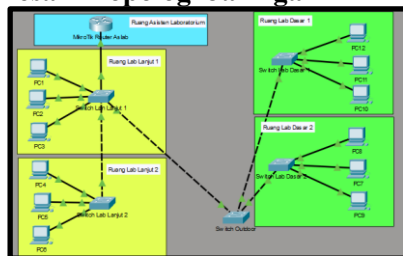
4.1.4 Analisis Data Jaringan

Hasil dari ketiga pengamatan di atas diklasifikasikan untuk merumuskan spesifikasi sistem. Sistem difokuskan pada optimalisasi perangkat MikroTik RB750Gr3 untuk mengeksekusi pemblokiran *game online* berbasis *port* aplikasi dan domain *web game* menggunakan *Firewall Mangle* dan *Address List*. Untuk menjawab kendala pengawasan visual, dirumuskan kebutuhan sistem pelaporan insiden jarak jauh menggunakan otomasi *Scripting*, *Scheduler*, dan integrasi *Bot Telegram API*.

4.2 Desain

Pada tahap ini, hasil analisis diterjemahkan ke dalam bentuk rancangan teknis yang mencakup arsitektur jaringan dan logika sistem pemblokiran. Proses perancangan dibagi menjadi beberapa aspek utama.

4.2.1 Desain Topologi Jaringan

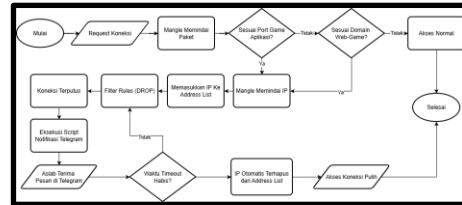


**Gambar 4.2 Topologi Laboratorium Fasilkom
UNSIKA**

Perancangan topologi fisik seperti **Gambar 4.2** disimulasikan menggunakan perangkat lunak *Cisco Packet Tracer*. Jaringan didesain menggunakan topologi *Tree* pada arsitektur mendatar (*flat network*), di mana pusat kendali berada pada *router* MikroTik di ruang Asisten

Laboratorium yang mendistribusikan koneksi ke 124 unit komputer di empat ruangan berbeda.

4.2.2 Desain Alur Sistem



Gambar 4.3 Flowchart Alur Sistem Pemblokiran

Logika sistem pemblokiran dirancang agar berjalan secara berkesinambungan tanpa intervensi manual. Alur kerja sistem divisualisasikan dalam bentuk *flowchart* seperti pada **Gambar 4.3** yang memuat empat fase utama: fase inisiasi dan pemindaian paket data oleh *Mangle*, fase isolasi IP pelanggar dan pemutusan koneksi (*Drop*), fase pelaporan insiden via Telegram, serta fase pemulihan koneksi mandiri (*Auto-Recovery*) setelah batas waktu (*timeout*) hukuman berakhir.

4.2.3 Desain Kebijakan Jaringan

Untuk menghindari pemblokiran lalu lintas akademik secara keliru (*false-positive*), sistem mendeteksi *game online* menggunakan dua parameter berbeda.

- a. **Game Berbasis Aplikasi:** Menggunakan fitur *Firewall Mangle* untuk memindai paket data protokol TCP/UDP yang mengarah ke *Destination Port* spesifik dari *server game* seperti yang dirincikan pada **Tabel 4.3**.

Tabel 4.3 Daftar Protokol dan Destination Port Game Yang Akan Dipindai

Nama Platform Game	Protokol	Destination Port
Roblox	UDP	49152 - 65535
Steam	TCP	27015-27050
	UDP	3478, 4379-4380, 27000-27250
Epic Games	TCP	3478-3479, 5060, 5062, 5222, 6250, 12000-65000
	UDP	3478-3479, 5060, 5062, 5222, 6250,

		12000-65000
--	--	-------------

b. **Game Berbasis Web:** Memanfaatkan fitur *Address List* dinamis yang secara otomatis menerjemahkan nama domain *web game* seperti dirincikan pada Tabel 4.4 menjadi sekumpulan alamat IP *server target*.

Tabel 4.4 Daftar Domain Web Game Yang Akan Dipindai

Nama Website Game	Domain
Friv	friv.com
	www.friv.com
Poki Games	poki.com
	poki.co.id
Crazy Games	crazygames.com
	crazygames.co.id

Paket data yang terdeteksi cocok dengan parameter di atas akan memicu *router* untuk menangkap alamat IP komputer pengguna dan mengisolasinya ke dalam *Address List* khusus bernama "Mahasiswa-Ngegame" selama durasi *timeout* yang ditetapkan.

4.2.4 Desain Logika Scripting

```

1 BEGIN
2 SET botToken = "TOKEN DARI TELEGRAM"
3 SET chatId = "ID GRUP TELEGRAM"
4 SET listName = "Mahasiswa-Ngegame"
5
6 FOR EACH item IN Firewall Address List WHERE list equals listName DO
7   SET ipClient = GET IP Address dari item
8   SET ipComment = GET Comment dari item
9
10  IF ipComment NOT EQUAL TO "dilaporkan" THEN
11
12    SET ipStr = CONVERT ipClient ke Tipe Data String
13    SET noPCStr = EXTRACT karakter setelah titik ketiga dari ipStr
14    SET noPCNum = CONVERT noPCStr ke Tipe Data Angka
15
16    SET ruangan = "Unknown"
17    IF noPCNum >= 1 AND noPCNum <= 31 THEN
18      SET ruangan = "Lab Lantai 1"
19    ELSE IF noPCNum >= 32 AND noPCNum <= 62 THEN
20      SET ruangan = "Lab Lantai 2"
21    ELSE IF noPCNum >= 63 AND noPCNum <= 93 THEN
22      SET ruangan = "Lab Dasar 2"
23    ELSE IF noPCNum >= 94 AND noPCNum <= 124 THEN
24      SET ruangan = "Lab Dasar 1"
25    END IF
26
27    SET time = GET Waktu Sistem Router
28    SET date = GET Tanggal Sistem Router

```

```

29 SET pesanText = "?? INSIDEN GAME ONLINE TERDETEKSI ??\n" +
30   "-----\n" +
31   "Waktu Kejadian : " + date + " " + time + "\n" +
32   "Lokasi Ruangan : " + ruangan + "\n" +
33   "Identitas Host : PC- " + noPCStr + "\n" +
34   "Alamat IP : " + ipClient + "\n" +
35   "-----\n" +
36   "Keterangan: Akses internet pada unit tersebut" +
37   "telah diisolasi dan diblokir otomatis selama" +
38   "?3 menit."
39
40 SET url = "https://api.telegram.org/bot" + botToken + "/sendMessage"
41 SET body = "chat_id=" + chatId + "&text=" + pesanText
42
43 EXECUTE HTTP POST request KE url DENGAN DATA body
44
45 UPDATE Comment pada item MENJADI "dilaporkan"
46
47 PRINT LOG INFO "Notifikasi Telegram terkirim untuk PC: " + noPCStr
48
49 END IF
50 END FOR
51 END

```

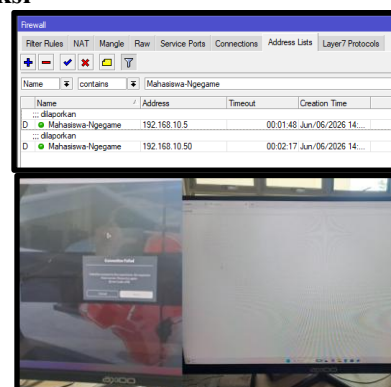
Gambar 4.4 Pseudocode Script

Setelah IP pelanggar terisolasi, sistem memerlukan instruksi otomatis untuk proses pelaporan. Desain *Scripting* dirancang seperti pada **Gambar 4.4** memanfaatkan metode perulangan (*looping*) dan kondisi (*if-else*) untuk menyortir *Address List* isolasi. *Script* akan mengekstrak alamat IP pelanggar, memotong oktet keempat IP tersebut untuk dikonversi menjadi identitas fisik (Nomor PC dan Lokasi Ruangan), dan merangkainya menjadi teks pesan. Pesan tersebut kemudian dikirimkan melalui HTTP/HTTPS *Request* ke *server Bot Telegram API*.

4.3 Simulasi

Tahap simulasi bertujuan untuk menguji validitas dan fungsionalitas logika pemblokiran serta pelaporan otomatis di dalam lingkungan yang terkendali (*staging environment*) berskala kecil sebelum diterapkan secara penuh pada jaringan utama laboratorium. Lingkungan simulasi dibangun secara independen menggunakan *router* MikroTik RB951Ui-2nD dan dua unit komputer klien sebagai perangkat penguji. Pengujian pada tahap ini dibagi ke dalam tiga skenario utama.

4.3.1 Simulasi Pemindaian dan Isolasi Koneksi



Gambar 4.5 Hasil Simulasi Pemindaian dan Isolasi Koneksi

Skenario ini menguji kemampuan *Firewall Mangle* dalam membaca dua parameter berbeda

secara simultan. Komputer penguji pertama disimulasikan mengakses *game* aplikasi, sementara komputer penguji kedua mengakses *web game*. Hasil simulasi menunjukkan bahwa *Mangle* secara akurat menangkap kedua aktivitas tersebut dan memasukkan alamat IP komputer ke dalam daftar isolasi dinamis. *Filter Rule* kemudian mengeksekusi pemutusan akses internet dengan rincian pada **Tabel 4.5**.

Tabel 4.5 Waktu Koneksi Terputus Pada Simulasi Sistem

Komputer	Akses Game	Waktu Koneksi Terputus	Rata-Rata Waktu Koneksi Terputus
Peng uji 1	Roblox	7.30 Detik	10,53 Detik
	Steam	14.42 Detik	
	Epic Games	9.87 Detik	
Peng uji 2	Friv	4.81 Detik	4.91 Detik
	Crazy Games	4.61 Detik	
	Poki Games	5.33 Detik	

4.3.2 Simulasi Eksekusi Pelaporan Otomatis



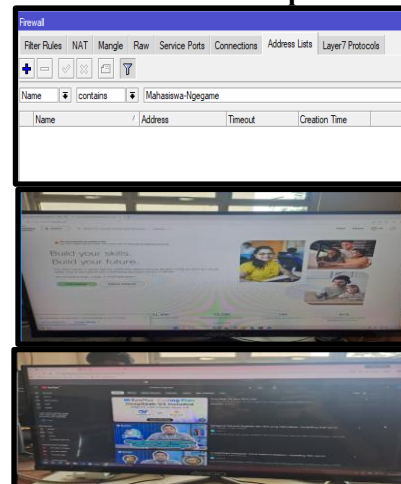
Gambar 4.6 Hasil Simulasi Eksekusi Pelaporan Otomatis

Skenario kedua difokuskan pada pengujian ketepatan waktu *Scheduler* dalam memicu *Script API Telegram*. Hasilnya, sistem berhasil mengekstrak data IP dari *Address List* dan meneruskannya menjadi notifikasi peringatan ke aplikasi Telegram administrator. Waktu respons pengiriman pesan tercatat seperti pada **Tabel 4.6**.

Tabel 4.6 Waktu Respon Telegram Pada Simulasi Sistem

Komputer	Akses Game	Waktu Respon Telegram	Rata-Rata Waktu Respon
Peng uji 1	Roblox	2.61 Detik	4.62 Detik
	Steam	7.54 Detik	
	Epic Games	3.73 Detik	
Peng uji 2	Friv	9.83 Detik	6.94 Detik
	Crazy Games	3.02 Detik	
	Poki Games	7.99 Detik	

4.3.3 Simulasi Eksekusi Pelaporan Otomatis



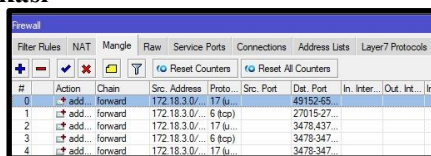
Gambar 4.7 Hasil Simulasi Pemulihan Koneksi Mandiri

Skenario terakhir bertujuan untuk memvalidasi fungsi parameter batas waktu (*timeout*) yang dikonfigurasi selama 3 menit pada *Address List*. Hasil simulasi membuktikan bahwa sistem berjalan sesuai rancangan; tepat setelah durasi 3 menit berakhir, alamat IP komputer penguji terhapus secara otomatis dari daftar blokir, sehingga akses internet pulih secara mandiri tanpa memerlukan intervensi manual dari administrator.

4.4 Implementasi

Tahap implementasi merupakan eksekusi penerapan rancangan konfigurasi secara langsung ke dalam sistem operasi *router* utama yang beroperasi di Laboratorium Fasikom UNSIKA. Proses implementasi ini diklasifikasikan ke dalam tiga mekanisme utama.

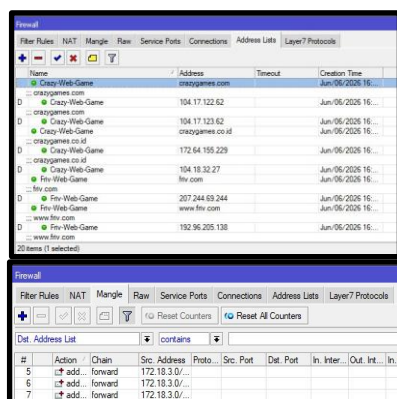
4.4.1 Konfigurasi Deteksi Game Berbasis Aplikasi



Gambar 4.8 Konfigurasi Mangle Untuk Game Berbasis Aplikasi

Langkah pertama difokuskan pada penanganan lalu lintas *game* berbasis aplikasi. Konfigurasi diterapkan melalui menu *Firewall Mangle* untuk memindai paket data dari klien yang menuju ke *Destination Port* dan Protokol (TCP/UDP) spesifik *server game*. Apabila terdeteksi, Mangle mengeksekusi parameter *Action: add src to address list* untuk memasukkan alamat IP klien tersebut ke dalam daftar isolasi dinamis bernama "Mahasiswa-Ngegame" yang dilengkapi batas waktu (*timeout*) selama 3 menit.

4.4.2 Konfigurasi Deteksi Game Berbasis Web



Gambar 4.9 Konfigurasi Mangle Untuk Game Berbasis Web

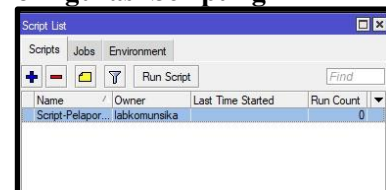
Berbeda dengan *game* aplikasi, deteksi *web game* tidak menggunakan *port* agar tidak mengganggu jalur HTTP/HTTPS utama.

Langkah ini diawali dengan memasukkan nama domain situs *game* (seperti *crazygames.com* atau *poki.com*) ke dalam *Address List* agar *router* secara otomatis mencatat IP *server web game* tersebut. Selanjutnya, *Firewall Mangle* dikonfigurasi untuk memindai lalu lintas klien yang menuju ke *Destination Address List* domain tersebut, untuk kemudian mengisolasi IP klien pelanggar ke dalam *Address List* "Mahasiswa-Ngegame" dengan durasi *timeout* 3 menit.

4.4.3 Konfigurasi Pemutusan Koneksi

IP yang terisolasi di dalam *Address List* tidak akan terputus koneksi internetnya tanpa eksekusi penindakan. Oleh karena itu, diimplementasikan *Packet Filtering* melalui menu *Firewall Filter Rule*. Aturan ini menargetkan *Source Address List* "Mahasiswa-Ngegame" dengan menerapkan *Action: Drop*. Pendekatan ini membuang paket data pelanggar secara diam-diam (*silent drop*) untuk memutus akses internet secara instan tanpa memberikan beban ekstra pada CPU *router*.

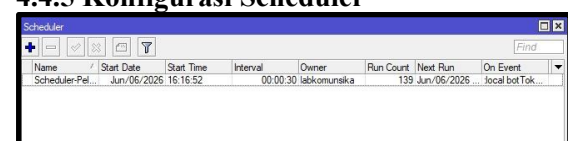
4.4.4 Konfigurasi Scripting



Gambar 4.10 Konfigurasi Scripting

Untuk mengotomatisasi pengawasan, baris kode *Script* ditanamkan ke dalam sistem RouterOS guna mengekstrak data dari *Address List* karantina. *Script* ini di program untuk membaca alamat IP pelanggar, mengkonversinya menjadi identitas fisik seperti lokasi ruangan dan nomor PC, lalu menyusunnya menjadi format teks. Pesan tersebut kemudian dikirimkan menggunakan HTTP *POST Request* ke URL *API Bot Telegram*. *Script* juga memberikan label komentar "dilaporkan" pada IP terkait untuk mencegah *spamming* pesan yang dapat memicu *Rate Limiting Telegram*.

4.4.5 Konfigurasi Scheduler



Gambar 4.11 Konfigurasi Scheduler

Agar sistem pelaporan beroperasi secara proaktif tanpa intervensi manual, fitur *Scheduler* diaktifkan sebagai pemicu. Jadwal dikonfigurasi pada mode *startup* agar langsung aktif saat *router* menyala, dengan parameter interval pengulangan diatur setiap 10 detik. Hal ini bertujuan agar pengiriman notifikasi insiden ke aplikasi Telegram administrator tetap relevan dengan klasifikasi waktu *real-time*.

4.5 Pemantauan

Tahap ini merupakan fase evaluasi komprehensif terhadap fungsionalitas dan kinerja sistem yang telah diterapkan pada *router* utama Laboratorium Fasilkom UNSIKA. Evaluasi difokuskan pada tiga metrik.

4.5.1 Efektivitas Pemblokiran

Pengujian efektivitas dilakukan menggunakan metode *Purposive Sampling*, dengan memilih satu sampel komputer dari masing-masing ruangan laboratorium (Lab Lanjut 1, Lab Lanjut 2, Lab Dasar 1, dan Lab Dasar 2) untuk merepresentasikan keseluruhan jaringan.

Tabel 4.7 Hasil Evaluasi Efektivitas Pemblokiran

Nama Komputer	IP Address	Lokasi	Game Skenario Evaluasi	Status
PC3	172.18.3.3	Lab Lanjut 1	<i>Poki Games</i>	Berhasil
			<i>Crazy Games</i>	Berhasil
			<i>Friv</i>	Berhasil
			<i>Steam</i>	Berhasil
			<i>Epic Games</i>	Berhasil
			<i>Roblox</i>	Berhasil
PC36	172.18.3.36	Lab Lanjut 2	<i>Poki Games</i>	Berhasil
			<i>Crazy Games</i>	Berhasil
			<i>Friv</i>	Berhasil

			<i>Steam</i>	Berhasil
			<i>Epic Games</i>	Berhasil
			<i>Roblox</i>	Berhasil
PC66	172.18.3.66	Lab Dasar 2	<i>Poki Games</i>	Berhasil
			<i>Crazy Games</i>	Berhasil
			<i>Friv</i>	Berhasil
			<i>Steam</i>	Berhasil
			<i>Epic Games</i>	Berhasil Koneksi
			<i>Roblox</i>	Berhasil
PC120	172.18.3.120	Lab Dasar 1	<i>Poki Games</i>	Berhasil
			<i>Crazy Games</i>	Berhasil
			<i>Friv</i>	Berhasil
			<i>Steam</i>	Berhasil
			<i>Epic Games</i>	Berhasil
			<i>Roblox</i>	Berhasil

Hasil evaluasi pada **Tabel 4.7** menunjukkan tingkat keberhasilan pemblokiran mencapai 100%. Seluruh komputer sampel secara konsisten gagal mengakses *game online* target, baik yang berbasis aplikasi maupun *web*. Koneksi internet pada perangkat pelanggar terputus secara otomatis seketika. Hal ini membuktikan bahwa metode *Packet Filtering* yang dikombinasikan dengan deteksi *Mangle*

dan *Address List* dinamis beroperasi dengan sangat presisi dalam menutup celah penyalahgunaan akses tanpa mengganggu aktivitas akademik lainnya.

4.5.2 Beban Kerja CPU

Evaluasi beban komputasi bertujuan mengukur tingkat efisiensi penggunaan CPU pada *router* MikroTik RB750Gr3. Pengukuran dilakukan dengan menyelisihkan nilai rata-rata acuan dasar (*baseline*) jaringan dengan tingkat utilisasi CPU saat sistem pemblokiran aktif. Untuk menguji ketahanan maksimal, skenario deteksi jamak dilakukan dengan mengadopsi Prinsip Pareto, yaitu menyimulasikan 20% dari total unit komputer laboratorium (25 dari 124 PC) melakukan pelanggaran secara bersamaan.

Tabel 4.8 Rekapitulasi Hasil Pemantauan Beban Kerja CPU

Skenario	Kondisi Trafik	Rata-Rata	Baseline	Beban Murni Sistem
Tunggal	Sepi	3,57 %	0,4%	3,17%
	Padat	83,42 %	82,61%	0,81%
Jamak	Sepi	5,74 %	0,4%	5,34%
	Padat	91,78 %	82,61%	9,17%

Berdasarkan pengujian, pada **Tabel 4.8** memperlihatkan bahwa tambahan beban kerja murni CPU *router* hanya berkisar antara 0,81% hingga 3,17% pada skenario deteksi tunggal, dan maksimal mencapai 9,17% pada skenario deteksi jamak saat kondisi trafik jaringan padat. Berdasarkan standar *CPU Utilization Factor*, angka ini secara konsisten berada pada zona "Sangat Aman Berlebih" (<26%). Temuan ini membuktikan bahwa arsitektur sistem berjalan dengan sangat ringan dan secara signifikan berhasil mengatasi risiko kelebihan beban komputasi yang sering menjadi kelemahan utama pada penerapan metode inspeksi paket mendalam seperti *Layer 7 Protocol*.

4.5.3 Kecepatan Waktu Respon Notifikasi Telegram

Kecepatan pelaporan dievaluasi dengan menghitung rata-rata waktu tempuh sejak IP komputer pelanggar ditangkap oleh *Address List* hingga pesan peringatan diterima oleh ponsel administrator melalui aplikasi Telegram.

Tabel 4.14 Hasil Pengukuran Kecepatan Respon

Nama Komputer	Percobaan	Kecepatan Respon	Rata-Rata Kecepatan Respon
PC3	1	5,16 detik	7,79 detik
	2	10,31 detik	
	3	7,90 detik	
	4	6,33 detik	
	5	9,99 detik	
	6	7,08 detik	
PC36	1	6,61 detik	7,52 detik
	2	2,55 detik	
	3	9,58 detik	
	4	5,06 detik	
	5	10,49 detik	
	6	10,87 detik	
PC66	1	6,67 detik	6,66 detik
	2	8,26 detik	
	3	9,64 detik	
	4	1,45 detik	

	5	5,48 detik	
	6	8,50 detik	
PC120	1	3,95 detik	3,30 detik
	2	1,84 detik	
	3	1,77 detik	
	4	2,24 detik	
	5	8,76 detik	
	6	1,29 detik	

Hasil pengukuran mencatatkan rata-rata waktu jeda pengiriman berada pada rentang 3,30 detik hingga 7,79 detik. Berdasarkan model *User-Centric QoS Categories* dari standar internasional ITU-T G.1010, waktu tempuh di bawah batas ambang 10 detik mengklasifikasikan sistem peringatan dini ini sebagai layanan yang "Memuaskan" dan *acceptable*. Keberhasilan interval waktu *Scheduler* yang dipadukan dengan parameter filter "dilaporkan" pada *script* juga terbukti andal dalam menjaga stabilitas pengiriman pesan tanpa memicu pemblokiran *Rate Limiting* dari *server* Telegram.

4.6 Manajemen

Tahap akhir dari metodologi NDLC ini bertujuan untuk memastikan keberlanjutan dan tingkat keandalan sistem dalam jangka panjang setelah masa penelitian berakhir. Pelaksanaan tahap ini direalisasikan melalui dua langkah tata kelola utama.

4.6.1 Perumusan Kebijakan Pemeliharaan

Penyusunan dokumentasi teknis berupa pedoman operasional mengenai prosedur untuk mengelola, menambahkan, dan memperbarui aturan pemblokiran (*port* aplikasi dan domain *web game*). Dokumentasi ini berfungsi sebagai pedoman mitigasi agar sistem penangkal dapat terus diperbarui menyesuaikan dengan

kemunculan infrastruktur *game online* baru di masa mendatang tanpa harus merombak struktur *script* pelaporan.

4.6.2 Serah Terima Tata Kelola

Penyerahan dokumen panduan teknis operasional beserta hak akses penuh pengelolaan grup pemantauan dan *Bot Telegram API* kepada Asisten Laboratorium Fasilkom UNSIKA selaku pemangku kebijakan. Langkah ini memastikan bahwa teknologi pengawasan digital yang dikembangkan dapat dioperasikan secara mandiri untuk menegakkan tata tertib fasilitas laboratorium secara berkelanjutan.

5. KESIMPULAN

Berdasarkan hasil analisis, implementasi, dan pengujian sistem pemantauan dan pemblokiran *game online* di Laboratorium Fasilkom UNSIKA, dapat ditarik beberapa kesimpulan utama sebagai berikut:

- Arsitektur sistem berhasil diterapkan secara presisi dengan memadukan metode *Packet Filtering*, identifikasi *Mangle (Port/Protokol)*, penerjemahan domain pada *Address List* dinamis, serta pelaporan otomatis melalui integrasi *Script* dan *Scheduler* ke *Bot Telegram API*. Kelebihan utama dari rancangan ini adalah operasionalnya yang sangat ringan (*lightweight*) karena terhindar dari inspeksi paket mendalam (*Deep Packet Inspection*).
- Evaluasi performa mencatatkan tingkat efektivitas pemblokiran sebesar 100% tanpa adanya *false-positive* pada lalu lintas akademik. Tambahan beban kerja CPU *router* tercatat sangat rendah, yakni maksimal 9,17% pada simulasi beban serentak tertinggi (zona "Sangat Aman Berlebih"). Kecepatan waktu respons pengiriman notifikasi Telegram mencatatkan rata-rata 3,30 hingga 7,79 detik, yang mengklasifikasikan sistem peringatan dini ini sebagai layanan dengan indeks "Memuaskan" (*Timely*).

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Universitas Singaperbangsa Karawang (UNSIKA), khususnya Fakultas Ilmu Komputer (Fasilkom), atas fasilitas dan dukungan yang diberikan, serta kepada rekan-rekan Asisten Laboratorium

Fasilkom UNSIKA yang telah memberikan akses dan kolaborasi teknis yang sangat membantu penyelesaian penelitian ini.

DAFTAR PUSTAKA

- [1] N. N. Monigir, *Implementasi Manajemen TIK Dalam Pendidikan*. EUREKA MEDIA AKSARA, 2025.
- [2] Leonardo, O. R. Husin, N. Roy, and D. Pratama, "Infrastruktur TI sebagai Pendukung Utama dalam Transformasi Proses Belajar di Sekolah," *Jurnal REIN (Rekayasa Informatika)*, vol. 2, no. 2, pp. 53–58, 2024.
- [3] H. Hendrawan *et al.*, "Load Balancing Dengan Metode PCC Pada Sekolah Menengah Kejuruan Negeri 1 Palopo," *JITET (Jurnal Informatika dan Teknik Elektro Terapan)*, vol. 13, no. 2, 2025.
- [4] K. Prasanti and I. H. Wiranata, "Dampak Negatif Penyalahgunaan Teknologi Terhadap Proses Pendidikan," in *Prosiding Konseling Kearifan Nusantara*, vol. 4, pp. 335–345, 2025.
- [5] E. Simanjuntak, N. A. F. Nawangsari, and R. Ardi, "Academic Cyberslacking: Why Do Students Engage in Non-Academic Internet Access During Lectures?," *Psychology Research and Behavior Management*, vol. 15, pp. 3257–3273, 2022.
- [6] Y. S. Wahyuni, "Pemblokiran Game Online Menggunakan Firewall Filter Pada Mikrotik Untuk Menciptakan Lingkungan Kerja Yang Efisien," *Eastasouth Journal of Positive Community Services*, vol. 3, no. 2, 2025.
- [7] C. A. Putri, A. I. Razita, N. M. T. Sari, and Z. Kurniawan, "Pengaruh Intensitas Bermain Game Online Terhadap Prokrastinasi Akademik Pada Mahasiswa Teknik Informatika Universitas Muhammadiyah Ponorogo," *Mars: Jurnal Teknik Mesin, Industri, Elektro Dan Ilmu Komputer*, vol. 2, no. 4, pp. 202–215, 2024.
- [8] K. Aziz, S. Zakir, W. Aprison, and L. Efriyanti, "Implementasi Keamanan Jaringan Dengan Metode Firewall Filtering Menggunakan MikroTik di SMKN 3 Payakumbuh," *JATI: Jurnal Mahasiswa Teknik Informatika*, vol. 8, no. 3, pp. 3343–3352, 2024.
- [9] Y. Sianhar and Marhalim, "Penerapan Firewall Berbasis MikroTik Dalam Optimalisasi Jaringan DI Sekolah Menengah Kejuruan," *Jurnal Informatika Teknologi dan Sains (JINTEKS)*, vol. 7, no. 2, pp. 868–877, 2025.
- [10] H. A. Al Kautsar and R. Sastra, "Implementasi Firewall MikroTik dalam Pembatasan Akses Situs Terlarang di RT/RW Net," *Computer Science (CO-SCIENCE)*, vol. 5, no. 2, pp. 123–132, 2025.
- [11] A. S. Ma'mum and G. Z. Muflih, "Implementasi Web Filtering Firewall untuk Keamanan pada Jaringan Internet di Pondok Pesantren Al Hidayah Kebumen," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 8, no. 1, pp. 46–59, 2025.
- [12] D. Suhardono, E. Wahyudi, and B. Arifwidodo, "Teknik Keamanan Akses Internet Untuk Parenting Menggunakan Metode Packet Filtering Pada MikroTik," *Techno.COM*, vol. 22, no. 4, pp. 926–936, 2023.
- [13] H. Aspriyono and A. Susanto, *Jaringan Komputer dan Perkembangannya*. ANDI, 2024.
- [14] Y. F. Rompas, J. D. Zakarias, and E. J. R. Kawung, "Pengaruh Game Online Terhadap Interaksi Sosial Di Kalangan Mahasiswa Fakultas Ilmu Sosial Dan Politik Universitas Sam Ratulangi," *Jurnal Ilmiah Society*, vol. 3, no. 1, pp. 1–11, 2023.
- [15] A. R. Barra, A. R. Sujatmika, and I. Umami, "Sistem Keamanan Jaringan Komputer Bridge Firewall Menggunakan Router Board MikroTik RB750," *Jurnal Teknologi Dan Sistem Informasi Bisnis-JTEKSIS*, vol. 4, no. 1, pp. 427–431, 2022.
- [16] A. T. C. Sianturi and P. Simanjuntak, "Implementasi Quality of Service Menggunakan Metode Queue Tree dan Mangle pada MikroTik Router OS di PT Batam Bintang Telekomunikasi," *Jurnal Comasie*, vol. 10, no. 2, pp. 41–50, 2024.
- [17] M. S. Adji, I. Kresna A., and Paradise, "Analisis QoS Filtering Website dan Pembatasan Bandwidth Menggunakan Metode Address List (Studi Kasus: WI-FI Belajar Asrama Menoreh)," *LEDGER: Journal Informatic and Information Technology*, vol. 1, no. 3, pp. 129–138, 2022.
- [18] MikroTik, "RouterOS Documentation," 2019. [Online]. Available: <https://help.mikrotik.com/docs/spaces/ROS/pages/328059/RouterOS>
- [19] Telegram, "Telegram," 2013. [Online]. Available: <https://telegram.org/>
- [20] M. Rahman, R. B. Handwika, and A. I. Zahro, "Penerapan Model Network Development Life Cycle (NDLC) Pada Infrastruktur Jaringan Internet Kantor Desa Kemiri," *Jurnal Publikasi Teknik Informatika (JUPTI)*, vol. 2, no. 3, pp. 37–47, 2023.
- [21] ITU-T, *Quality of service and performance: End-user multimedia QoS categories*. International Telecommunication Union, 2001.
- [22] P. A. Laplante and S. J. Ovaska, *Real-Time Systems Design and Analysis*, 4th ed. IEEE Press, 2012.