

ANALISIS *SECURE GATEWAY SOPHOS FIREWALL* TERINTEGRASI *NETDATA* DAN NOTIFIKASI *TELEGRAM* PADA WAROENG DIGITAL

Rangga Azizzan Hussaen

Teknik Informatika dan Komputer, Politeknik Negeri Jakarta

Depok, Jawa Barat

rangga.azizzan.hussaen.tik22@mhs.wpnj.ac.id

Abstract - The access restriction system on Waroeng Digital network infrastructure is no longer in use because it requires manual domain updates and lacks support for a device monitoring system that provides rapid disruption notifications to network administrators. This study aims to implement a secure gateway using Sophos Firewall to restrict access to online gambling sites and to apply a Netdata-based network monitoring system (NES) integrated with Telegram as a notification medium.. The methods used are web filtering on Sophos Firewall, as well as monitoring based on ICMP and SNMPv2 protocols using the Netdata NMS. Network service quality testing is carried out using the standard TIPHON QoS parameters, which include throughput, jitter, delay, and packet loss. The test results show that the Category-Based Web Filtering method achieved an accuracy of 61%, while the Custom URL Filtering method achieved an accuracy of 100% against testing of 100 online gambling domains and 100 non-gambling domains. The Netdata monitoring system successfully monitored the availability and resources of 17 wireless router devices, Mikrotik, and Sophos Firewalls, sending notifications via Telegram. QoS testing results obtained a download throughput of 5.806 Mbps, upload throughput of 5.624 Mbps, a delay of 4.8 ms, jitter of 0.532 ms, and 0% packet loss. The measured QoS parameters are still categorized as Good to Very Good, indicating that the implemented system can operate effectively without reducing network performance.

Keywords: Network Monitoring System, Netdata, Sophos Next-Gen Firewall, Telegram API.

Abstrak - Sistem pembatasan akses pada infrastruktur jaringan Waroeng Digital tidak lagi digunakan karena memerlukan pembaharuan domain secara manual, serta belum didukung sistem monitoring perangkat yang memberikan notifikasi gangguan secara cepat kepada administrator jaringan. Penelitian bertujuan untuk mengimplementasikan secure gateway menggunakan Sophos Firewall untuk membatasi akses situs perjudian daring serta menerapkan network monitoring system (NMS) berbasis Netdata yang terintegrasi Telegram sebagai media notifikasi. Metode yang digunakan adalah web filtering pada Sophos Firewall, serta sistem monitoring berbasis protokol ICMP dan SNMPv2 menggunakan NMS Netdata. Pengujian kualitas layanan jaringan dilakukan menggunakan parameter QoS standar TIPHON yang meliputi throughput, jitter, delay, dan packet loss. Hasil pengujian menunjukkan bahwa metode Category-Based Web Filtering memperoleh accuracy sebesar 61%, sedangkan metode Custom URL Filtering memperoleh accuracy sebesar 100% terhadap pengujian 100 domain gambling/judi online dan 100 domain non-gambling. Sistem monitoring Netdata berhasil memantau availability dan penggunaan sumber daya pada 17 perangkat wireless router, Mikrotik, dan Sophos Firewall, serta mengirimkan notifikasi melalui Telegram.. Hasil pengujian QoS didapatkan throughput download 5,806 Mbps, throughput upload 5,624 Mbps, delay 4,8 ms, jitter 0,532ms, dan packet loss 0%. Parameter QoS yang diukur masih dalam kategori Bagus hingga Sangat Bagus, sehingga sistem yang diimplementasikan dapat berjalan dengan baik tanpa menurunkan performa jaringan.

Kata kunci: Network Monitoring System, Netdata, Sophos Next-Gen Firewall, Telegram API.

I. PENDAHULUAN

Perkembangan penggunaan internet di Indonesia terus meningkat sehingga pengelolaan infrastruktur jaringan menjadi aspek penting untuk menjaga keamanan dan kualitas layanan, termasuk pada penyedia layanan internet berskala kecil.

Berdasarkan survei APJII tahun 2024, jumlah pengguna internet Indonesia mencapai 221,56 juta jiwa [1] sehingga kebutuhan terhadap sistem keamanan dan monitoring jaringan semakin meningkat.

Waroeng Digital merupakan penyedia layanan jaringan berskala kecil menyediakan akses internet bagi pengguna melalui infrastruktur jaringan yang terdiri atas 17 perangkat *wireless router* serta sebuah *Mikrotik* sebagai *gateway* utama. Seiring bertambahnya jumlah perangkat yang terhubung dalam infrastruktur jaringan, proses pengelolaan dan pemantauan menjadi lebih kompleks. Maka diperlukan mekanisme pemantauan yang mampu membantu administrator dalam mendeteksi dan menangani gangguan secara lebih efektif [2]. Namun, berdasarkan hasil observasi dan wawancara yang dilakukan, infrastruktur tersebut belum memiliki sistem *monitoring* jaringan secara terpusat. Administrator masih melakukan pemantauan perangkat secara manual menggunakan *IP Scan* dan *ping* pada aplikasi *Winbox* atau menunggu laporan dari pengguna sehingga proses deteksi gangguan menjadi lebih lambat.

Berdasarkan hasil observasi dan wawancara, sebelumnya pernah diterapkan mekanisme pembatasan akses situs perjudian daring dengan menambahkan *domain* secara manual ke dalam daftar pemblokiran. Metode tersebut dinilai kurang efektif karena memerlukan pembaruan *domain* secara berkala. Berdasarkan laporan KOMDIGI tahun 2025, sebanyak 1,3 juta konten judi online telah ditangani [3] sehingga mekanisme pembaruan manual semakin sulit dipertahankan. Kondisi tersebut menunjukkan perlunya mekanisme pembatasan akses yang lebih efektif dan mudah dikelola.

Penelitian sebelumnya telah mengimplementasikan *Network Monitoring System* menggunakan *LibreNMS* maupun *Zabbix* yang terintegrasi *Telegram* sebagai media notifikasi real-time [4], [5]. Sementara itu, pada penelitian lain menerapkan *firewall* untuk pembatasan akses situs maupun mitigasi ancaman siber [6], [7]. Namun penelitian-penelitian tersebut masih berfokus pada aspek monitoring maupun keamanan jaringan secara terpisah dan belum mengevaluasi efektivitas mekanisme *web filtering* menggunakan *Confusion Matrix* serta dampaknya terhadap kualitas layanan jaringan. Berbeda dengan penelitian sebelumnya, penelitian ini mengintegrasikan *Sophos Firewall*, *Netdata*, dan *Telegram* pada lingkungan UMKM, serta mengevaluasi dua metode *web filtering* (*Category-Based Web Filtering* dan *Custom URL Filtering*) menggunakan *Confusion Matrix* dan analisis *Quality of Service* (QoS).

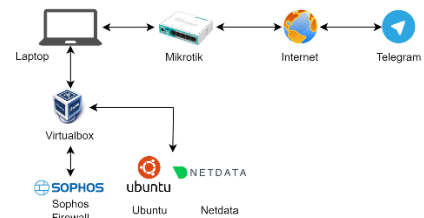
Penelitian ini menggunakan metode *Network Development Life Cycle* (NDLC), pengujian *web filtering* berbasis *Confusion Matrix*, serta evaluasi *Quality of Service* (QoS). Penelitian ini bertujuan untuk menganalisis implementasi *Secure Gateway*

Sophos Firewall yang terintegrasi dengan *Netdata* dan *Telegram* terhadap efektivitas pembatasan akses situs perjudian daring, kemampuan monitoring perangkat jaringan, serta dampaknya terhadap kualitas layanan jaringan.

II. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan jenis penelitian studi kasus pada infrastruktur jaringan Waroeng Digital [8]. Data penelitian diperoleh melalui observasi, wawancara dengan pemilik usaha, dan studi literatur. Tahapan penelitian menggunakan metode *Network Development Life Cycle* (NDLC) untuk implementasi sistem pembatasan akses menggunakan *Sophos Firewall* serta sistem *monitoring* berbasis *Netdata* yang terintegrasi dengan *Telegram*.

Pengujian *web filtering* menggunakan dua dataset, yaitu anti-gambling-domain dari *GitHub* dan *Top Access Domain* dari *DataForSEO*. Masing-masing dataset terdiri atas 100 sampel *domain*. *Domain* perjudian dipilih menggunakan simple random sampling, sedangkan *domain* non-gambling dipilih dari 100 *domain* dengan peringkat akses tertinggi pada dataset *DataForSEO* yang telah diverifikasi tidak termasuk kategori perjudian. Jumlah sampel memenuhi ketentuan minimum *Central Limit Theorem*. Topologi sistem yang digunakan dalam penelitian ditunjukkan pada Gambar 1.



Gambar 1. Topologi Rancangan Sistem

Pengujian monitoring dilakukan pada 17 *wireless router*, *Mikrotik*, dan *Sophos Firewall*. Pengujian dilakukan pada tiga kondisi operasional perangkat, yaitu *clear*, *warning*, dan *critical* berdasarkan nilai ambang batas (*threshold*) CPU dan RAM yang telah dikonfigurasi pada *Netdata* [9]. Analisis data dilakukan secara deskriptif kuantitatif. Efektivitas *web filtering* dievaluasi menggunakan *Confusion Matrix* melalui identifikasi *True Positive* (TP), *False Positive* (FP), *True Negative* (TN), dan *False Negative* (FN), kemudian dihitung nilai *accuracy* menggunakan Persamaan (1).

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \times 100\% \quad (1)$$

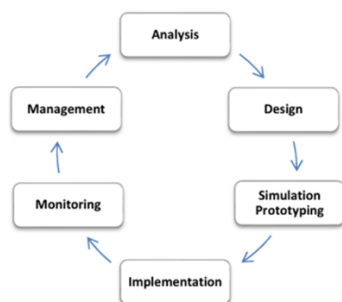
Sistem *monitoring* dievaluasi berdasarkan keberhasilan deteksi kondisi perangkat dan pengiriman notifikasi *Telegram*. Dampak implementasi sistem dianalisis menggunakan parameter *Quality of Service* (QoS) yang meliputi *throughput*, *delay*, *jitter*, dan *packet loss*.

Analisis sistem *monitoring* dilakukan berdasarkan keberhasilan deteksi *threshold* yang ditetapkan, pengiriman notifikasi *Telegram*, serta dampak implementasi terhadap performa jaringan berdasarkan parameter *Quality of Service* (QoS). Parameter yang dianalisis meliputi *throughput*, *delay*, *packet loss*, dan *jitter*. Kategori penilaian *Quality of Service* mengacu pada standar TIPHON sebagaimana ditunjukkan pada Tabel I.

Tabel I. Kategori QoS Berdasarkan Standar TIPHON

Kategori Kualitas	Indeks	Throughput	Delay	Jitter	Packet Loss
Sangat Bagus	4	> 2.1 Mbps	< 150 ms	0 ms	0-2%
Bagus	3	1200 Kbps – 2.1 Mbps	150 – 300 ms	> 0 - 75ms	3%-14%
Sedang	2	338 – 1200 Kbps	300 – 450 ms	> 75 - 125 ms	15%-24%
Buruk	1	0 – 388 Kbps	> 450 ms	> 125 - 225 ms	>25%

Pengembangan sistem menggunakan metode *Network Development Life Cycle* (NDLC) yang terdiri atas tahapan *analysis*, *design*, *simulation/prototyping*, *implementation*, *monitoring*, dan *management* [10], sebagaimana ditunjukkan pada Gambar 2. Pada penelitian ini, implementasi dibatasi hingga tahap *monitoring*.

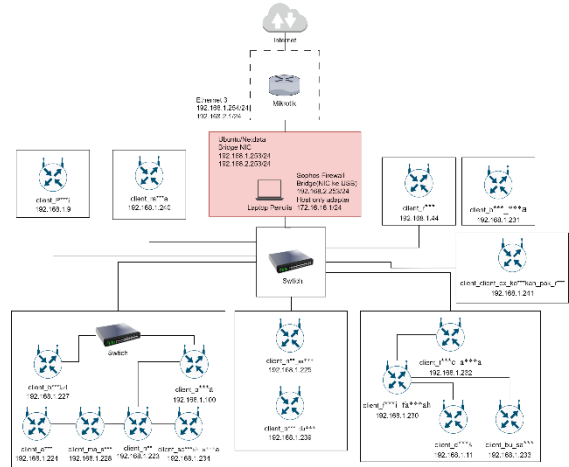


Gambar 2. *Network Development Life Cycle*

III. HASIL DAN PEMBAHASAN

A. Implementasi Sistem

Implementasi sistem yang diterapkan dalam jaringan produksi yang ada digambarkan seperti pada Gambar 3.



Gambar 3. Topologi Jaringan Implementasi

Sistem diimplementasikan pada perangkat laptop yang diposisikan di antara *Mikrotik* dan *switch* utama sehingga seluruh lalu lintas jaringan melewati *Sophos Firewall*. Posisi tersebut memungkinkan sistem menjalankan fungsi pembatasan akses (*web filtering*) sekaligus *monitoring* terhadap perangkat jaringan.

B. Pengujian Web Filtering

Tabel II. *Confusion Matrix Category-Based Web Filtering*

Kategori Aktual	Block	Allow
Gambling	22 (TP)	78 (FN)
Non Gambling	0 (FP)	100 (TN)

$$\begin{aligned}
 \text{Accuracy} &= \frac{22+100}{22+0+100+78} \times 100\% \\
 &= \frac{122}{200} \times 100\% \\
 &= 61\%
 \end{aligned}$$

Berdasarkan Tabel II diperoleh 22 true positive, 0 false positive, 78 false negative, dan 100 true negative, sehingga metode *Category-Based Web Filtering* menghasilkan nilai *accuracy* sebesar 61%. Nilai tersebut menunjukkan bahwa *Sophos Firewall* hanya mampu memblokir domain yang telah dikategorikan sebagai Gambling pada basis data URL bawaan, sedangkan domain yang belum teridentifikasi masih dapat diakses.

Tabel III. *Confusion Matrix Custom URL Filtering*

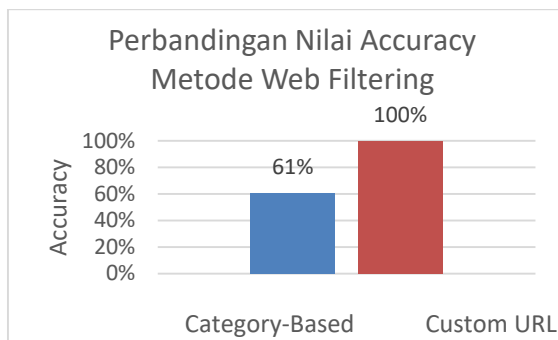
Kategori Aktual	Block	Allow
Gambling	100 (TP)	0 (FN)
Non Gambling	0 (FP)	100 (TN)

$$Accuracy = \frac{100+100}{100+0+100+0} \times 100\%$$

$$= \frac{200}{200} \times 100\%$$

$$= 100\%$$

Berbeda dengan metode sebelumnya, pada Tabel III *Custom URL Filtering* menghasilkan 100 *true positive* dan 100 *true negative* tanpa *false positive* maupun *false negative*, sehingga nilai *accuracy* mencapai 100%. Hal ini menunjukkan bahwa mekanisme pemblokiran berbasis daftar *domain* secara manual lebih efektif dalam membatasi akses terhadap seluruh domain yang menjadi sampel pengujian. Sistem *Sophos Firewall* menyediakan mekanisme *Custom Web Category* sehingga administrator dapat menambahkan *domain* yang belum dikenali ke dalam kebijakan *web filtering* [11].



Gambar 4. Perbandingan Accuracy Web Filtering

Pada Gambar 4 menunjukkan bahwa metode *Custom URL Filtering* memiliki tingkat *accuracy* yang lebih tinggi dibanding *Category-Based Web Filtering*. Perbedaan tersebut disebabkan karena metode *Category-Based Web Filtering* bergantung pada hasil kategorisasi URL pada basis data *Sophos Firewall*. Oleh karena itu, *domain* yang belum memiliki kategori atau diklasifikasikan ke kategori selain Gambling tidak akan diblokir oleh kebijakan berbasis kategori [12], sedangkan *Custom URL Filtering* menggunakan daftar *domain* yang ditentukan langsung oleh administrator.

C. Pengujian Monitoring

Tabel IV. Hasil Uji Pengujian Monitoring Wireless router

Kondisi	Threshold	Nilai Aktual	Status Aktual	Telegram
Normal	Packet loss < 100% selama 3 menit	0%	Clear	-
Critical	Packet loss =	100%	Critical	Terkirim

	100% selama > 3 menit			
Recovery	Host dapat dijangkau	0%	Clear	Terkirim

Hasil pada Table IV menunjukkan seluruh pengujian kondisi normal, *critical*, dan *recovery* pada *wireless router* berhasil dilakukan menggunakan protokol ICMP [13]. *Netdata* akan memberikan notifikasi *alert* saat perangkat dalam kondisi *down*, sedangkan notifikasi dikirimkan kepada administrator melalui Telegram Bot API [14].

Tabel V. Hasil Uji Monitoring CPU Mikrotik

Kondisi	Threshold	Nilai Aktual	Status Aktual	Telegram
Normal	<75%	25.57%	Clear	-
Warning	≥75%	76%	Warning	Terkirim
Critical	≥90%	92%	Critical	Terkirim
Recovery	<75%	74%	Clear	Terkirim

Berdasarkan hasil uji pada Tabel V sistem alerting perangkat *Mikrotik* menggunakan protokol SNMPv2 membuktikan mekanisme *recovery* berhasil [15]. *Alert Mikrotik* pada *Netdata* berhasil dikirimkan ke platform *Telegram*.

Tabel VI. Hasil Uji Monitoring RAM Mikrotik

Kondisi	Threshold	Nilai Aktual	Status Aktual	Telegram
Normal	<70%	44,41%	Clear	-
Warning	≥70%	71,03%	Warning	Terkirim
Critical	≥80%	80,60%	Critical	Terkirim
Recovery	<70%	69,70%	Clear	Terkirim

Berdasarkan hasil uji pada Tabel VI sistem alerting perangkat *Mikrotik* menggunakan protokol SNMPv2 menunjukkan seluruh penerapan *threshold alert* berhasil *men-trigger*. *Alert Mikrotik* pada *Netdata* berhasil dikirimkan ke platform *Telegram*.

Tabel VII. Hasil Uji Monitoring CPU Sophos Firewall

Kondisi	Threshold	Nilai Aktual	Status Aktual	Telegram
Normal	<75%	13,44%	Clear	-
Warning	≥75%	77,15%	Warning	Terkirim
Critical	≥90%	92,19%	Critical	Terkirim
Recovery	<75%	73,2%	Clear	Terkirim

Data pada Tabel VII sistem alerting perangkat Sophos Firewall menggunakan protokol SNMPv2 menunjukkan mekanisme alert CPU berjalan sesuai threshold. Alert Mikrotik pada Netdata berhasil dikirimkan ke platform Telegram.

Tabel VIII. Hasil Uji Monitoring RAM Sophos Firewall

Kondisi	Threshold	Nilai Aktual	Status Aktual	Telegram
Normal	<75%	54,84%	Clear	-
Warning	≥75%	75,02%	Warning	Terkirim
Critical	≥90%	90,00%	Critical	Terkirim
Recovery	<75%	62,72%	Clear	Terkirim

Data pada Tabel VIII sistem alerting perangkat *Sophos Firewall* menggunakan protokol SNMPv2 menunjukkan utilisasi RAM juga dapat dipantau secara real-time. *Alert Mikrotik* pada *Netdata* berhasil dikirimkan ke platform *Telegram*.

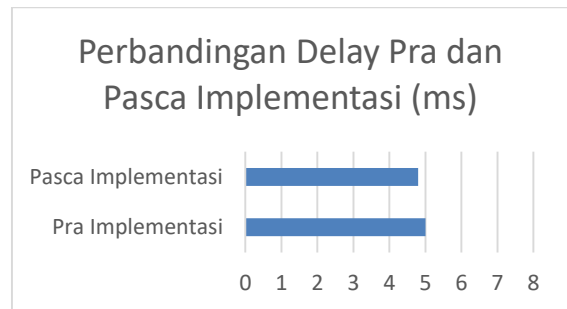
D. Analisis Kualitas Quality of Service

Tabel IX. Perbandingan Rata-Rata Pra Implementasi dan Pasca Implementasi

Parameter	Pra Implementasi	Pasca Implementasi	Selisih	Perubahan
Download	5,676 Mbps	5,806 Mbps	0,13 Mbps	2,29 %
Upload	5,654 Mbps	5,624 Mbps	-0,03 Mbps	-0,53 %
Delay	5 ms	4,8 ms	-0,2 ms	-4 %
Jitter	0,412 ms	0,532 ms	0,12 ms	29,13 %
Packet Loss	0,4%	0%	-0,4%	-100%

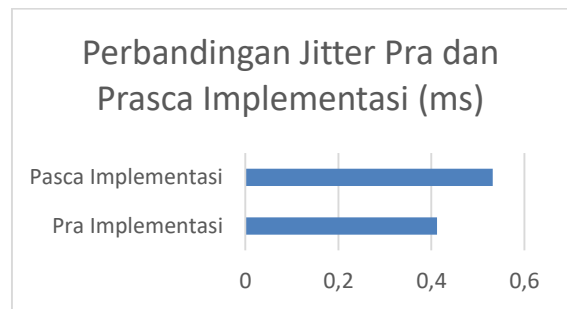
Berdasarkan Tabel IX seluruh parameter QoS setelah implementasi masih berada pada kategori Bagus hingga Sangat Bagus menurut standar TIPHON. Perubahan *throughput* relatif kecil,

sedangkan *delay*, *jitter*, dan *packet loss* tidak menunjukkan penurunan kualitas layanan yang signifikan.



Gambar 5. Perbandingan *Delay* Pra dan Pasca Implementasi

Pada Gambar 5 menunjukkan bahwa *delay* setelah implementasi menurun dari 5 ms menjadi 4,8 ms sehingga implementasi sistem tidak memberikan dampak negatif terhadap waktu tunda jaringan.



Gambar 6. Perbandingan *Jitter* Pra dan Pasca Implementasi

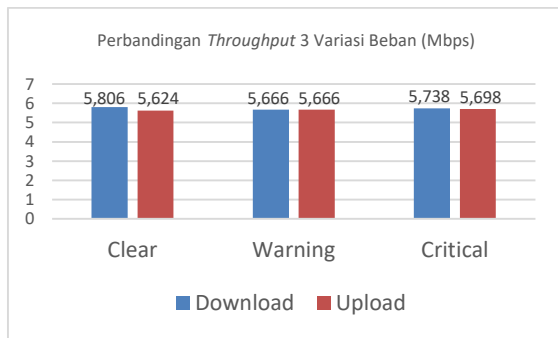
Pada Gambar 6 *jitter* meningkat dari 0,412 ms menjadi 0,532 ms, namun masih berada pada kategori Sangat Bagus menurut standar TIPHON sehingga tidak memengaruhi kualitas layanan.

Tabel X. Perbandingan Rata-Rata QoS Variasi Beban Pasca Implementasi

Status RAM dan CPU	Download	Upload	Delay	Jitter	Packet Loss
Clear	5,806 Mbps	5,624 Mbps	4,8 ms	0,532 ms	0%
Warning	5,666 Mbps	5,666 Mbps	22,6 ms	11,798 ms	0%
Critical	5,738 Mbps	5,698 Mbps	116,8 ms	15,058 ms	7,2%

Berdasarkan Tabel X peningkatan beban perangkat menyebabkan kenaikan *delay* dan *jitter* secara bertahap. Pada kondisi *critical*, *delay* meningkat menjadi 116,8 ms dan *packet loss* mencapai 7,2%, sedangkan *throughput* relatif stabil. Hal ini menunjukkan bahwa implementasi *network monitoring system Netdata* dan *Sophos Firewall*

masih mampu mempertahankan *throughput* meskipun kualitas transmisi mulai menurun ketika perangkat berada pada kondisi beban tinggi.



Gambar 7. Perbandingan Throughput Variasi Bebeban

Pada Gambar 7 grafik *throughput* menunjukkan bahwa perubahan beban CPU dan RAM tidak memberikan penurunan *throughput* yang signifikan. Perubahan *throughput* antar variasi beban relatif kecil dan masih dipengaruhi oleh fluktuasi lalu lintas jaringan selama pengujian.

IV. KESIMPULAN DAN SARAN

Implementasi sistem *secure gateway Sophos Firewall* yang terintegrasi dengan *network monitoring system (NMS) Netdata* dan notifikasi *Telegram* pada infrastruktur jaringan Waroeng Digital dinyatakan berhasil. Sistem ini terbukti dapat beroperasi secara bersamaan untuk memantau ketersediaan 17 *wireless router* melalui protokol ICMP, serta mengawasi penggunaan CPU dan RAM pada perangkat *MikroTik* dan *Sophos Firewall* menggunakan protokol *SNMPv2*.

Pada pengujian fitur *Category-Based Filtering* terhadap 100 sampel *domain* situs gambling/judi online dan 100 *domain* non-gambling, diperoleh hasil *accuracy* sebesar 61% dengan 22 *domain* gambling/judi online berhasil diblokir (*true positif*), 78 *domain* gambling/judi online masih dapat diakses (*false negative*), dan 100 *domain* non-gambling tetap dapat diakses (*true negative*). Rendahnya tingkat *accuracy* ini dikarenakan hasil *URL Category Lookup* pada *database* bawaan *Sophos Firewall* yang mengklasifikasikan beberapa *domain* diluar kategori Gambling seperti *General Business*, *Parked Domain*, atau *No records found* [14]. Hal ini menginformasikan bahwa efektivitas *web filtering* dengan metode *Category-Based Web Filtering* sangat bergantung pada tingkat akurasi dan pembaruan *database* dari penyedia sistem *Sophos Firewall*. Pada metode *Custom URL Filtering*, sistem menghasilkan *accuracy* sebesar 100%, dengan seluruh 100 *domain* gambling/judi online berhasil diblokir dan 100 *domain* non-gambling tetap dapat diakses.

Sistem *monitoring Netdata* berhasil mendeteksi perubahan kondisi seluruh perangkat uji berdasarkan nilai ambang batas (*threshold*) yang telah dikonfigurasi.. Seluruh skenario baik dalam kondisi *warning*, *critical*, maupun *recovery* berhasil ditampilkan pada dasbor *Netdata* dan memberikan notifikasi pada platform *Telegram*.

Quality of Service (QoS) dengan standar *TIPHON* membuktikan bahwa integrasi sistem ini tidak menimbulkan penurunan performa jaringan. Seluruh parameter pasca-implementasi berada pada indeks Bagus hingga Sangat Bagus, dengan rata-rata *throughput download* 5,806 Mbps, rata-rata *throughput upload* 5,624 Mbps, rata-rata *delay* 4,8 ms, *jitter* 0,532 ms, dan *packet loss* 0%. Parameter ini menunjukkan bahwa infrastruktur tambahan dapat beroperasi tanpa mengurangi kualitas layanan jaringan.

Berdasarkan pengujian QoS pada variasi kondisi beban pasca implementasi, peningkatan beban sistem dari kondisi *Clear*, *Warning*, hingga *Critical* menyebabkan nilai *delay* meningkat dari 4,8 ms menjadi 22,6 ms dan 116,8 ms, nilai *jitter* meningkat dari 0,532 ms menjadi 11,798 ms dan 15,058 ms, nilai *packet loss* meningkat dari 0% menjadi 7,2% pada kondisi *critical*. Sementara pada nilai *throughput* relatif stabil dengan *throughput download* berada pada rentang 5,666–5,806 Mbps dan *throughput upload* pada rentang 5,624–5,698 Mbps. Meskipun terjadi peningkatan pada beberapa parameter QoS seiring bertambahnya beban pada sistem, kualitas layanan jaringan masih berada pada kategori Bagus hingga Sangat Bagus berdasarkan standar *TIPHON*.

Secara keseluruhan, penelitian ini berhasil mengimplementasikan sistem jaringan yang lebih aman dan terpantau bagi Waroeng Digital. Integrasi sistem dapat meminimalkan ketergantungan pada pengecekan manual dengan mengotomatisasi pemantauan perangkat terpusat, memberikan notifikasi gangguan secara cepat, dan menyederhanakan mekanisme manajemen pembatasan akses situs gambling bagi administrator.

Penelitian selanjutnya disarankan mengembangkan mekanisme *Custom URL Filtering* yang diperbaharui secara otomatis maupun berkala. Pengembangan tersebut diharapkan dapat meningkatkan efektivitas pembatasan akses terhadap *domain* yang belum dikategorikan sebagai Gambling oleh *Sophos Firewall* serta mengurangi pembaruan daftar *domain* secara manual. Pada penerapan sistem *monitoring* dapat dikembangkan dengan parameter lain seperti penggunaan *bandwidth*, suhu perangkat dan lain sebagainya untuk mendapatkan data yang lebih bervariasi,

dengan sistem notifikasi terintegrasi dengan media lain sesuai dengan kebutuhan.

V. REFERENSI

- [1] APJII. APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang. [Online]. Available: <https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang>. [Accessed: 23-Jun-2026].
- [2] Supriadi A, Saptadi NTS, Arisandi D, Sallaby AF, Faisal M, Sumarta SC, Nurdin AM, Rachman AN, Saryani. Pengantar Jaringan Komputer. Banten: Sada Kurnia Pustaka. 2024.
- [3] KOMDIGI. Sebanyak 1,3 Juta Konten Judi Diblokir, Komdigi-BPK Perkuat Tata Kelola Ruang Digital. [Online]. Available: <https://portal.komdigi.go.id/kanal-publik/berita-kini/9300>. [Accessed: 24-Jun-2026].
- [4] Christanto FW, Faizi MA, Firdaus EA. Network and Server Performance Monitoring Using LibreNMS, Telegram, and UniFi Controller. 2024 3rd International Conference on Creative Communication and Innovative Technology (ICCIIT). Piscataway. 2024.
- [5] Pillo-Guanoluisa D, Herrera LB, Alba AJ, Báez DS, Buestán VF. Real-Time Network Infrastructure Monitoring: A Zabbix and Telegram Integration Case Study in the Energy Sector (EMELNORTE S.A.). ETCM 2025 – 9th Ecuador Technical Chapters Meeting. Quito. 2025.
- [6] Nggandung MHI, Hariadi F, Uly NB. Mikrotik-Based Firewall as a Filter Site Blocking in Pahunga. Journal of Artificial Intelligence and Engineering Applications. 2025;5(1):436-451.
- [7] Ferdian ED, Bangun AM. Implementasi Fitur Hosts and Services pada Sophos Firewall untuk Mitigasi Serangan Malware. Jurnal Teknik SILITEK. 2025;5(3):1698-1707.
- [8] Veronica A, Ernawati, Rasdiana, Abas M, Yusriani, Hadawiah, Hidayah N, Sabtohadhi J, Marlina H, Mulyani W, Zulkarnaini. Metodologi Penelitian Kuantitatif. Padang: Global Eksekutif Teknologi. 2022.
- [9] Netdata. Alert Configuration Reference. Netdata Documentation. [Online]. Available: <https://learn.netdata.cloud/docs/alerts-&-notifications/alert-configuration-reference>. [Accessed: 21-Jul-2026].
- [10] Siswanto D, Priyandoko G, Tjahjono G, Putri RS, Sabela NB, Muzakki MI. Development of Information and Communication Technology Infrastructure in School Using an Approach of the Network Development Life Cycle Method. Journal of Physics: Conference Series. 2021;1908(1).
- [11] Sophos. How to Configure Web Filtering and URL Matching in Sophos Firewall. Sophos Knowledge Base. [Online]. Available: https://support.sophos.com/support/s/article/KBA-000004901?language=en_US. [Accessed: 21-Jul-2026].
- [12] Sophos. Categories – Sophos Firewall. Sophos Documentation. [Online]. Available: <https://docs.sophos.com/nsg/sophos-firewall/21.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Web/Categories/index.html>. [Accessed: 21-Jul-2026].
- [13] Netdata, "Ping collector," Netdata Documentation, [Online]. Available: <https://learn.netdata.cloud/docs/collecting-metrics/collectors/synthetic-testing/ping>. [Accessed: 21-Jul-2026] Netdata. Ping Collector. Netdata Documentation. [Online]. Available: <https://learn.netdata.cloud/docs/collecting-metrics/collectors/synthetic-testing/ping>. [Accessed: 21-Jul-2026].
- [14] Telegram. Bot API. Telegram Documentation. [Online]. Available: <https://core.telegram.org/bots/api>. [Accessed: 21-Jul-2026].
- [15] Netdata. SNMP Devices. Netdata Documentation. [Online]. Available: <https://learn.netdata.cloud/docs/network-performance-monitoring/device-metrics/integrations/snmp-devices>. [Accessed: 21-Jul-2026].