e-ISSN 2962-0651
JURNAL KOMPUTER

Implementasi Sistem Keamanan Jaringan Wifi Di Desa Bukit Peninjauan II

Taufik Hidayat [1*)]; Khairil [2)]; Deri Lianda [3)]
[11,2,3)] Universitas Dehasen Bengkulu , Indonesia
Email: [1)] taufikhenita83@gmail.com

Abstrak

Jaringan WiFi publik memiliki tingkat kerentanan yang cukup tinggi terhadap penyalahgunaan akses internet, terutama untuk mengakses Website yang mengandung unsur perjudian online, pornografi, dan pinjaman online ilegal. Permasalahan tersebut juga ditemukan pada jaringan WiFi publik Desa Bukit Peninjauan II yang belum memiliki sistem Filtering Website yang efektif. Penelitian ini bertujuan untuk mengimplementasikan sistem keamanan jaringan menggunakan Firewall MikroTik yang dikombinasikan dengan DNS Static berbasis Regular Expression (Regex), TLS Host Filtering, serta pemblokiran DNS over HTTPS (DoH) dan QUIC. Metode penelitian yang digunakan adalah Network Development Life Cycle (NDLC) yang meliputi tahap analisis, perancangan, implementasi, pengujian, dan evaluasi sistem. Implementasi dilakukan pada jaringan WiFi publik Desa Bukit Peninjauan II dengan menerapkan aturan Firewall untuk memFilter akses Website berdasarkan pola domain tertentu. Hasil pengujian menunjukkan bahwa Firewall Filter, DNS Static Regex, TLS Host Filtering, pemblokiran DoH, dan pemblokiran QUIC dapat bekerja sesuai fungsi yang dirancang. Sistem berhasil membatasi akses terhadap Website yang mengandung unsur perjudian online, pornografi, dan pinjaman online ilegal tanpa mengganggu akses ke Website yang diperbolehkan. Selain itu, pemblokiran DoH dan QUIC mampu mencegah upaya Bypass terhadap mekanisme Filtering yang diterapkan. Berdasarkan hasil penelitian, sistem keamanan jaringan yang dibangun mampu meningkatkan pengendalian akses internet dan menciptakan lingkungan WiFi publik yang lebih aman, terkontrol, dan sesuai dengan kebutuhan masyarakat Desa Bukit Peninjauan II.

Kata kunci: *Firewall MikroTik; DNS Static Regex; TLS Host Filtering.*

The Implementation Of Wi-Fi Network Security System In Bukit Peninjauan II Village

Abstract

Public Wi-Fi networks are highly vulnerable to the misuse of Internet access, particularly for accessing websites containing online gambling, pornographic content, and illegal online lending services. Similar issues were identified in the public Wi-Fi network of Bukit Peninjauan II Village, which lacked an effective website filtering mechanism. This study aims to implement a network security system using MikroTik firewall integrated with DNS Static based on Regular Expressions (Regex), TLS Host Filtering, and the blocking of DNS over HTTPS (DoH) and QUIC protocols. This study used the Network Development Life Cycle (NDLC) methodology, which consists of the analysis, design, implementation, testing, and evaluation phases. The proposed system was implemented on the public Wi-Fi network of Bukit Peninjauan II Village by configuring firewall rules to filter website access based on predefined domain patterns. The results demonstrate that the implemented Firewall Filter, DNS Static Regex, TLS Host Filtering, DNS over HTTPS (DoH) blocking, and QUIC blocking functioned as intended. The system successfully restricted access to websites related to online gambling, pornographic content, and illegal online lending services without affecting access to authorized websites. Furthermore, blocking DoH and QUIC effectively prevented users from bypassing the implemented filtering mechanism. In conclusion, the proposed network security system effectively enhances Internet access control and provides a safer, more secure, and better-managed public Wi-Fi environment for the community of Bukit Peninjauan II Village.

Keywords: *MikroTik Firewall, DNS Static Regex, TLS Host Filtering.*

PENDAHULUAN

Pada saat ini perkembangan teknologi informasi berkembang dengan sangat pesat (Hari et al., 2023). Pemanfaatan jaringan internet tidak hanya terbatas pada sektor pendidikan dan pemerintahan, tetapi juga telah merambah ke lingkungan sosial dan publik, seperti fasilitas WiFi umum. Keberadaan teknologi jaringan tersebut mampu meningkatkan kinerja, efisiensi, serta kualitas layanan informasi bagi masyarakat. Perkembangan teknologi informasi dan komunikasi juga memberikan dampak signifikan terhadap aktivitas sosial dan ekonomi masyarakat, terutama dalam mendukung akses informasi secara cepat dan luas (Hari et al., 2023).

Objek penelitian ini berlokasi pada jaringan WiFi publik di Desa Bukit Peninjauan 2, yang disediakan sebagai sarana pendukung akses informasi dan komunikasi bagi masyarakat desa. Fasilitas ini memiliki peran penting dalam menunjang berbagai aktivitas, seperti kegiatan pendidikan, administrasi desa, serta komunikasi sehari-hari. Karakteristik utama dari jaringan WiFi publik yang bersifat terbuka dan dapat diakses oleh berbagai kalangan masyarakat menyebabkan jaringan tersebut memiliki tingkat kerentanan keamanan yang cukup tinggi. Meski demikian, pengaruh yang ditimbulkan dapat berbeda-beda, bermanfaat jika digunakan secara bijak, namun bisa berdampak negatif apabila disalahgunakan (Hasan et al., 2025).

Kondisi tersebut menuntut adanya pengelolaan jaringan yang baik agar penggunaannya tetap aman, tertib, dan sesuai dengan tujuan penyediaannya. Permasalahan yang dihadapi saat ini adalah belum adanya sistem pengamanan jaringan yang memadai untuk membatasi akses terhadap situs web yang mengandung konten negatif, seperti perjudian online, pornografi, maupun pinjaman online ilegal. Kondisi ini menimbulkan kesenjangan antara harapan akan penggunaan internet yang sehat dan produktif dengan kenyataan di lapangan yang masih belum terkontrol secara optimal. Selain itu, jaringan publik juga rentan terhadap berbagai ancaman keamanan, seperti penyadapan data, akses ilegal, dan penyalahgunaan layanan jaringan apabila tidak dilengkapi dengan sistem pengamanan yang memadai (Hasan et al., 2025) Seiring dengan perkembangan teknologi jaringan, metode akses internet juga mengalami perubahan, khususnya dengan meningkatnya penggunaan protokol HTTPS yang mengenkripsi lalu lintas data.

Hal ini menyebabkan metode pemblokiran berbasis alamat IP dan port menjadi kurang efektif karena informasi tujuan akses tidak dapat terlihat secara Langsung. Selain itu, munculnya teknologi seperti DNS over HTTPS (DoH) dan protokol QUIC memungkinkan pengguna untuk melewati mekanisme penyaringan jaringan konvensional. Perkembangan teknologi jaringan modern tersebut menuntut sistem keamanan yang lebih adaptif agar proses Filtering tetap dapat berjalan secara efektif pada lalu lintas terenkripsi (Hari et al., 2023).

Berdasarkan penelitian sebelumnya, penerapan sistem keamanan jaringan menggunakan Firewall terbukti efektif dalam mengendalikan lalu lintas data dan membatasi akses terhadap konten tertentu. Namun, untuk menghadapi perkembangan teknologi saat ini, diperlukan pendekatan yang lebih adaptif dan canggih. Salah satu pendekatan yang dapat digunakan adalah pemanfaatan fitur DNS Static dengan metode pencocokan pola (Regex) untuk memFilter domain secara lebih fleksibel, serta penggunaan TLS Host untuk mengidentifikasi domain pada koneksi HTTPS.

Pendekatan ini dinilai mampu meningkatkan efektivitas sistem Filtering pada jaringan modern yang didominasi oleh penggunaan protokol terenkripsi. Selain itu, diperlukan juga pengendalian terhadap penggunaan protokol DoH dan QUIC yang berpotensi digunakan untuk menghindari sistem Filtering. Dengan mengombinasikan beberapa teknik tersebut, diharapkan sistem keamanan jaringan menjadi lebih efektif dalam membatasi akses terhadap konten yang tidak diinginkan. Pengendalian lalu lintas jaringan melalui Firewall juga dapat membantu administrator jaringan dalam memonitor serta mengatur aktivitas pengguna agar tetap sesuai dengan kebijakan penggunaan jaringan yang telah ditetapkan.

LANDASAN TEORI

Teori Jaringan Komputer

Jaringan komputer merupakan sekumpulan perangkat yang saling terhubung untuk melakukan pertukaran data dan berbagi sumber daya melalui media komunikasi tertentu. Jaringan komputer memungkinkan pengguna untuk mengakses informasi secara cepat, efisien, dan terintegrasi. Dalam implementasinya, jaringan komputer dibedakan menjadi beberapa jenis berdasarkan cakupan wilayah, seperti LAN, MAN, dan *WAN*. Perkembangan jaringan komputer saat ini juga dipengaruhi oleh kemajuan teknologi internet yang memungkinkan komunikasi data dilakukan secara *real-time* dan berbasis *Cloud Computing*. Pada lingkungan publik, jaringan komputer umumnya menggunakan teknologi *WiFi* untuk mendukung mobilitas pengguna dalam mengakses layanan internet (Hari et al., 2023).

eISSN 2962-0651
JURNAL KOMPUTER

Teori Keamanan Jaringan

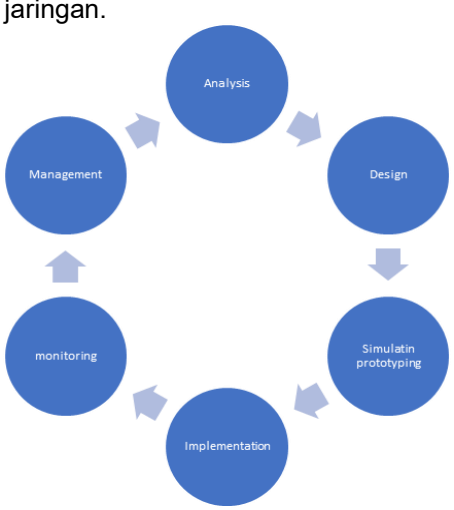
Keamanan jaringan merupakan proses perlindungan sistem jaringan komputer terhadap ancaman, akses ilegal, maupun penyalahgunaan layanan jaringan. Keamanan jaringan bertujuan menjaga kerahasiaan, integritas, dan ketersediaan data agar sistem dapat berjalan dengan aman dan stabil. Pada jaringan *WiFi* publik, tingkat ancaman keamanan cenderung lebih tinggi karena jaringan dapat diakses oleh banyak pengguna secara terbuka. Oleh karena itu, diperlukan sistem keamanan yang mampu mengontrol lalu lintas data dan membatasi aktivitas yang berpotensi membahayakan jaringan (Hasan et al., 2025).

Teori *Firewall*

Firewall merupakan sistem keamanan jaringan yang digunakan untuk mengontrol lalu lintas data berdasarkan aturan tertentu. *Firewall* bekerja dengan cara mem*Filter* paket data yang masuk dan keluar dari jaringan berdasarkan alamat IP, port, protokol, maupun domain tertentu. Implementasi *Firewall* sangat penting dalam menjaga stabilitas dan keamanan jaringan, terutama pada jaringan publik yang rentan terhadap penyalahgunaan akses internet (Prasetyo et al., 2024)

METODE PENELITIAN

Penulis menggunakan metode *Network Development Life Cycle (NDLC)* (Taufan et al., 2022). *NDLC* merupakan model pengembangan jaringan yang digunakan untuk merancang, membangun, mengimplementasikan, dan mengevaluasi sistem jaringan komputer secara bertahap. Model ini dinilai sesuai karena mampu menggambarkan proses pengembangan jaringan mulai dari tahap analisis hingga tahap pengelolaan dan pengujian jaringan.



Gambar 1. Metode Network Development Life Cycle (NDLC)

HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan implementasi sistem keamanan jaringan WiFi publik di Desa Bukit Peninjauan II dengan menggunakan perangkat MikroTik. Sistem keamanan yang diterapkan memanfaatkan beberapa fitur utama, yaitu Firewall Filter, DNS Static berbasis Regular Expression (Regex), TLS Host Filtering, pemblokiran DNS over HTTPS (DoH), pemblokiran DNS over TLS (DoT), serta pemblokiran protokol QUIC. Implementasi ini bertujuan untuk membatasi akses pengguna terhadap website yang mengandung konten negatif, seperti perjudian online, pornografi, dan pinjaman online ilegal, tanpa mengganggu akses terhadap website umum dan edukatif.

Hasil implementasi menunjukkan bahwa seluruh fitur keamanan berhasil diterapkan dan berjalan secara terintegrasi pada jaringan WiFi publik. MikroTik berfungsi sebagai gateway utama yang mengatur lalu lintas jaringan, menyediakan layanan IP Address, DNS Server, DHCP Server, serta menjalankan aturan keamanan. Sistem juga mampu melakukan filtering berdasarkan nama domain, mengenali koneksi HTTPS melalui TLS Host, serta mencegah upaya bypass melalui DoH, DoT, dan QUIC.

Tabel 1. Hasil Implementasi Fitur Keamanan

No.	Fitur Keamanan	Hasil Implementasi
1	Firewall Filter	Berhasil diterapkan

2	DNS Static Regex	Berhasil diterapkan
3	TLS Host Filtering	Berhasil diterapkan
4	Pemblokiran DNS over HTTPS (DoH)	Berhasil diterapkan
5	Pemblokiran QUIC	Berhasil diterapkan

Konfigurasi jaringan dilakukan dengan membagi interface menjadi WAN dan LAN. Interface WAN digunakan sebagai jalur koneksi ke internet melalui ISP, sedangkan interface LAN digunakan sebagai jaringan lokal pengguna WiFi. Pembagian ini membuat lalu lintas data lebih terstruktur dan memudahkan penerapan kebijakan keamanan.

Tabel 2. Interface Jaringan

Interface	Peran	Fungsi Utama
ether1	WAN	Terhubung ke ISP atau sumber internet
ether2	LAN (Bridge)	Jaringan lokal pengguna
ether3	LAN (Bridge)	Jaringan lokal pengguna
ether4	LAN (Bridge)	Jaringan lokal pengguna
ether5	LAN (Bridge)	Jaringan lokal pengguna

Pengaturan IP Address juga berhasil diterapkan. Interface WAN memperoleh IP dari jaringan ISP, sedangkan interface LAN menggunakan alamat 192.168.10.1/24 sebagai gateway jaringan lokal. DHCP Server dikonfigurasi untuk membagikan alamat IP secara otomatis kepada perangkat pengguna dengan rentang 192.168.10.2 sampai 192.168.10.254.

Tabel 3. Konfigurasi Utama Jaringan

Komponen	Konfigurasi	Fungsi
WAN	192.168.1.3/24	Jalur koneksi ke ISP
LAN / Bridge-LAN	192.168.10.1/24	Gateway jaringan lokal
DHCP Pool	192.168.10.2–192.168.10.254	Rentang IP otomatis untuk pengguna
Primary DNS	1.1.1.3	DNS utama
Secondary DNS	1.0.0.3	DNS cadangan

Pada bagian filtering website, DNS Static berbasis Regex digunakan untuk mengenali domain berdasarkan pola kata tertentu. Metode ini lebih efisien dibandingkan pemblokiran manual karena satu pola Regex dapat memblokir banyak variasi domain sekaligus. Website yang mengandung kata kunci tertentu akan diarahkan ke alamat 127.0.0.1 sehingga tidak dapat diakses pengguna.

Tabel 4. Konfigurasi DNS Static Berbasis Regex

No.	Kategori	Regular Expression (Regex)
1	Judi Online	`.*(judol
2	Pornografi	`.*(porn
3	Pinjaman Online Ilegal	`.*(pinjol

TLS Host Filtering diterapkan sebagai lapisan tambahan untuk memblokir website berbasis HTTPS. Metode ini memanfaatkan informasi nama domain pada proses TLS Handshake sehingga MikroTik tetap dapat mengenali domain tujuan meskipun koneksi menggunakan HTTPS.

Tabel 5. Pola TLS Host yang Diblokir

No.	TLS Host
1	judi
2	slot
3	casino
4	togel
5	gacor
6	maxwin
7	pinjol
8	pinjaman

e-ISSN 2962-0651
JURNAL KOMPUTER

Hasil pengujian fungsional menggunakan metode Black Box Testing menunjukkan bahwa seluruh fitur keamanan bekerja sesuai dengan rancangan. Website kategori perjudian online, pornografi, dan pinjaman online ilegal berhasil diblokir. Sebaliknya, website umum seperti Google dan website edukasi seperti Wikipedia tetap dapat diakses secara normal. Hal ini membuktikan bahwa sistem mampu melakukan pembatasan akses tanpa mengganggu penggunaan internet yang diperbolehkan.

Tabel 6. Hasil Pengujian Fungsional Sistem

No.	Skenario Pengujian	Output yang Diharapkan	Hasil Pengujian	Status
1	Akses situs perjudian	Akses diblokir	Website tidak dapat diakses	Berhasil
2	Akses situs pornografi	Akses diblokir	Website tidak dapat diakses	Berhasil
3	Akses situs pinjaman online ilegal	Akses diblokir	Website tidak dapat diakses	Berhasil
4	Akses situs umum	Akses diizinkan	Website dapat diakses	Berhasil
5	Akses situs edukasi	Akses diizinkan	Website dapat diakses	Berhasil
6	Penggunaan DNS over HTTPS (DoH)	DoH diblokir	Koneksi DoH gagal	Berhasil
7	Penggunaan protokol QUIC	QUIC diblokir	Trafik QUIC tidak dapat digunakan	Berhasil

Pengujian pemblokiran website menunjukkan bahwa seluruh kategori website negatif berhasil dibatasi oleh sistem keamanan jaringan. Pemblokiran dilakukan melalui kombinasi Firewall Filter, DNS Static Regex, dan TLS Host Filtering yang bekerja secara terintegrasi.

Tabel 7. Hasil Pengujian Pemblokiran Website

No.	Kategori Website	Hasil yang Diharapkan	Hasil Pengujian	Status
1	Judi Online	Website tidak dapat diakses	Website tidak dapat diakses	Berhasil
2	Pornografi	Website tidak dapat diakses	Website tidak dapat diakses	Berhasil
3	Pinjaman Online Ilegal	Website tidak dapat diakses	Website tidak dapat diakses	Berhasil

Pengujian DoH menunjukkan bahwa pengguna tidak dapat menggunakan layanan DNS over HTTPS untuk melewati sistem filtering. Setelah rule Firewall diterapkan, seluruh permintaan DNS tetap diproses melalui DNS Server MikroTik sehingga DNS Static Regex dapat bekerja secara optimal.

Tabel 8. Hasil Pengujian DNS over HTTPS (DoH)

No.	Skenario Pengujian	Hasil yang Diharapkan	Hasil Pengujian	Status
1	Mengaktifkan Secure DNS pada browser	DoH tidak dapat digunakan	DoH berhasil diblokir	Berhasil
2	Mengakses website diblokir menggunakan Secure DNS	Website tetap tidak dapat diakses	Website tidak dapat diakses	Berhasil

Pengujian QUIC juga menunjukkan hasil yang sesuai dengan tujuan penelitian. Pemblokiran QUIC melalui UDP port 443 berhasil dilakukan sehingga koneksi HTTPS kembali menggunakan protokol TCP. Kondisi ini mendukung efektivitas TLS Host Filtering dalam mengenali dan memblokir domain tujuan.

Tabel 9. Hasil Pengujian QUIC

No.	Skenario Pengujian	Hasil yang Diharapkan	Hasil Pengujian	Status
1	Mengakses website menggunakan protokol QUIC	QUIC tidak dapat digunakan	QUIC berhasil diblokir	Berhasil
2	Mengakses website diblokir setelah pemblokiran QUIC	Website tetap tidak dapat diakses	Website tidak dapat diakses	Berhasil

Selain pengujian pemblokiran, penelitian juga melakukan pengujian kinerja jaringan melalui ping, speedtest, dan penggunaan CPU router MikroTik. Hasilnya menunjukkan bahwa implementasi sistem keamanan tidak memberikan penurunan performa yang signifikan. Koneksi internet tetap berjalan stabil, website yang diperbolehkan tetap dapat diakses, dan router masih mampu menjalankan seluruh rule keamanan dengan baik.

Secara keseluruhan, hasil penelitian membuktikan bahwa sistem keamanan jaringan WiFi publik berbasis MikroTik berhasil diterapkan secara efektif di Desa Bukit Peninjauan II. Kombinasi Firewall Filter, DNS Static Regex, TLS Host Filtering, pemblokiran DoH, DoT, dan QUIC mampu membatasi akses terhadap website berkonten negatif tanpa mengganggu akses internet yang diperbolehkan. Dengan demikian, sistem ini dapat menjadi solusi praktis untuk meningkatkan keamanan dan pengendalian akses pada jaringan WiFi publik desa.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil implementasi, pengujian, dan evaluasi yang telah dilakukan pada jaringan *WiFi* publik Desa Bukit Peninjauan II, dapat disimpulkan bahwa :

1. Sistem keamanan jaringan menggunakan *Firewall* MikroTik, *DNS Static* berbasis *Regular Expression* (*Regex*), TLS Host Filtering, serta pemblokiran *DNS* over HTTPS (DoH) dan *QUIC* berhasil diimplementasikan dan berfungsi sesuai dengan tujuan penelitian.
2. Sistem yang dibangun mampu membatasi akses terhadap *Website* yang mengandung unsur perjudian online, pornografi, dan pinjaman online ilegal melalui mekanisme *Filtering* domain berbasis *Regex* dan TLS Host Filtering. Hasil pengujian menunjukkan bahwa *Firewall* Filter, *DNS Static Regex*, TLS Host Filtering, pemblokiran DoH, dan pemblokiran *QUIC* dapat bekerja sesuai fungsi yang dirancang sehingga proses *Filtering* dapat berjalan secara efektif pada lalu lintas *HTTP* maupun *HTTPS*.
3. Penerapan pemblokiran DoH dan *QUIC* terbukti mampu mencegah pengguna melakukan Bypass terhadap mekanisme *Filtering* yang diterapkan. Selain itu, implementasi sistem keamanan tidak memberikan dampak yang signifikan terhadap akses *Website* yang diperbolehkan sehingga kualitas layanan internet pada jaringan *WiFi* publik tetap dapat dipertahankan dengan baik. Secara keseluruhan, penelitian ini berhasil mencapai seluruh tujuan yang telah ditetapkan, yaitu mengimplementasikan sistem keamanan jaringan berbasis MikroTik yang mampu meningkatkan pengendalian akses internet pada jaringan *WiFi* publik.
4. Hasil penelitian ini memberikan kontribusi praktis berupa solusi keamanan jaringan yang dapat diterapkan pada lingkungan *WiFi* publik untuk menciptakan penggunaan internet yang lebih aman, terkontrol, dan sesuai dengan kebutuhan masyarakat.

Saran

1. Pengembangan pola Regex dan database domain.
   Sistem Filtering dapat ditingkatkan dengan menambahkan serta memperbarui pola Regular Expression (Regex) dan daftar domain yang diblokir secara berkala. Hal ini diperlukan karena domain yang mengandung konten perjudian online, pornografi, dan pinjaman online ilegal terus berkembang dan mengalami perubahan dari waktu ke waktu.

2. Penerapan metode Filtering yang lebih cerdas
   Penelitian SeLanjutnya dapat mengembangkan sistem Filtering dengan memanfaatkan teknologi machine learning atau artificial intelligence untuk mendeteksi Website berdasarkan konten, kategori, atau perilaku akses pengguna sehingga tingkat akurasi pemblokiran dapat ditingkatkan.
3. Penggunaan perangkat dengan spesifikasi yang lebih tinggi
   Untuk jaringan dengan jumlah pengguna yang lebih banyak, disarankan menggunakan perangkat MikroTik dengan kapasitas prosesor dan memori yang lebih besar agar kinerja sistem tetap optimal saat memproses aturan Firewall dan lalu lintas jaringan yang tinggi.
4. Pengembangan fitur monitoring dan pelaporan
   Sistem dapat dikembangkan dengan menambahkan fitur monitoring dan pelaporan secara otomatis, seperti pencatatan aktivitas akses Website yang diblokir, statistik penggunaan internet, serta notifikasi kepada administrator jaringan untuk memudahkan proses pengawasan dan evaluasi jaringan.
5. Penambahan mekanisme keamanan jaringan lainnya
   Penelitian berikutnya dapat mengintegrasikan sistem keamanan tambahan seperti Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Web Proxy Filtering, atau Content Filtering berbasis kategori untuk meningkatkan tingkat keamanan jaringan secara menyeluruh.
6. Perluasan objek penelitian
   Penelitian ini hanya diterapkan pada jaringan WiFi publik Desa Bukit Peninjauan II. Oleh karena itu, penelitian SeLanjutnya dapat dilakukan pada lingkungan yang lebih luas, seperti sekolah, perguruan tinggi, kantor pemerintahan, atau jaringan publik lainnya untuk mengetahui efektivitas sistem pada kondisi jaringan yang berbeda.
7. Penyesuaian terhadap perkembangan teknologi internet
   Mengingat teknologi keamanan dan komunikasi internet terus berkembang, administrator jaringan perlu melakukan pembaruan konfigurasi secara berkala agar sistem tetap mampu mengantisipasi metode Bypass terbaru serta mendukung implementasi keamanan jaringan yang lebih efektif.

DAFTAR PUSTAKA

Abeka, K. J., Ry˘sav´ya, O., & Burgetov´aa, I. (n.d.). Measurement and characterization of DNS over HTTPS traffic. 1–27.

Agus, M., Riduan, O., & Alamsyah, H. (2025). Analisa Dan Implementasi Kemanan Jaringan Berbasis Firewall RAW Terhadap Serangan DDoS Pada Router Mikrotik. 21(1), 317–328.

Arsalan, M. L., & Sukmana, H. T. (2023). Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing Menggunakan Firewall Rule (Studi Kasus : Pt . Akurat . Co) Wi-Fi Network Security Against Packet Sniffing Attacks Using Firewall Rule (Case Study : Pt . Accurate . Co). 6(2), 30–38.

Budijanto, H. A., Aidjili, M., Studi, P., Informasi, S., Studi, P., Informasi, S., Studi, P., & Informatika, T. (2022). RISTEK : Jurnal Riset , Inovasi dan Teknologi Kabupaten Batang. 6(2), 35–39.

Hari, N. H., Fauzan Prasetyo Eka Putra, U. H., & Siti Ririn Sutarsih, R. (2023). Transformasi Jaringan Telekomunikasi dengan Teknologi 5G : 5(2), 146–150. HTTPS://doi.org/10.37034/jidt.v5i1.357

Hasan, T. M., Albar, R., Ria, D., Tb, Y., & Wibawa, M. B. (2025). JARINGAN PUBLIK DENGAN TEKNIK SNIFFING SECURITY RISK ANALYSIS OF WI-FI . ID MANAGE SERVICE (WMS) ON PUBLIC NETWORKS USING SNIFFING TECHNIQUE. 11(2), 66–74.

J. Iyengar, E., & M. Thomson, E. (2021). QUIC: A UDP-Based Multiplexed and Secure Transport. 1–143. HTTPS://www.rfc-editor.org/rfc/rfc9000.html

Prasetyo, F., Putra, E., Hamzah, A., Agel, W., & Kusuma, R. O. F. (2024). Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking. 5(4), 82–87. HTTPS://doi.org/10.60083/jsisfotek.v5i4.329

Saputra, D., Panjaitan, H., & Nainggolan, E. R. (2023). Computer Science (CO-SCIENCE) Manajemen Keamanan Internet Menggunakan Metode Firewall Filtering Untuk Penyaringan Konten Pada Router Mikrotik RB1100. 3(2), 42–49.

Sulaiman, R., & Raya, A. M. (n.d.). Pemanfaatan Mikrotik Rb941-2nd menggunakan metode Firewall Filtering untuk keamanan jaringan dengan model forensik pada kantor desa. 18(2024), 364–371.

Taufan, M., Zaen, A., Ramadhan, W., Raya, J., Maras, O., Alang, B., Hulu, M., Ntb, K. S., Informasi, T., Teknik, F., Mataram, U. M., Kh, J., Dahlan, A., & Ntb, M. (2022). Penerapan Network Development Life Cycle (NDLC) Dalam Pengembangan Jaringan Komputer Pada Badan Pengelolaan Keuangan dan Aset Daerah (BPKAD) Provinsi NTB. XIV(1).