

Implementasi Adguard Home Berbasis Kontainer Pada Mikrotik RouterOS Untuk Monitoring Dan Keamanan Jaringan

Lia Andiani^{*1}, Chandra Yuliansyah²

Prodi Ilmu Komputer, Universitas Pat Petulai, Bengkulu, Indonesia^{1,2}

Liaandini1995@gmail.com¹, chandrayuliansyah1987@gmail.com²

*Corresponding author : Liaandini1995@gmail.com¹

Abstrak— Penelitian ini membahas implementasi AdGuard Home berbasis kontainer pada MikroTik RouterOS sebagai solusi monitoring dan keamanan jaringan. Pendekatan ini memanfaatkan DNS filtering untuk memblokir iklan dan domain berbahaya secara terpusat tanpa instalasi pada perangkat klien. Metode penelitian menggunakan pendekatan eksperimental dengan evaluasi kuantitatif berdasarkan parameter akurasi pemblokiran, latency DNS, dan success rate sistem. Hasil pengujian menunjukkan tingkat akurasi pemblokiran sebesar 95%, latency rata-rata DNS sebesar 24,3 ms, serta success rate sebesar 97%. Hasil tersebut menunjukkan bahwa AdGuard Home berbasis kontainer mampu meningkatkan keamanan jaringan dengan dampak performa yang masih dapat diterima. Penelitian ini diharapkan dapat menjadi referensi implementasi keamanan jaringan terintegrasi pada perangkat MikroTik RouterOS.

Abstract— This study presents the implementation of container-based AdGuard Home on MikroTik RouterOS as a network monitoring and security solution. The proposed approach utilizes DNS filtering to centrally block advertisements and malicious domains without requiring client-side installation. An experimental method with quantitative evaluation was applied using accuracy, DNS latency, and system success rate as performance metrics. The results show a blocking accuracy of 95%, an average DNS latency of 24.3 ms, and a success rate of 97%. These findings indicate that container-based AdGuard Home effectively enhances network security while maintaining acceptable network performance. This research is expected to serve as a practical reference for implementing integrated DNS-based security on MikroTik RouterOS.

Keywords— AdGuard Home, MikroTik RouterOS, container, network security, DNS filtering

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-nc/4.0/) license.



1. Pendahuluan

Perkembangan teknologi jaringan komputer yang semakin kompleks menuntut adanya sistem pengelolaan jaringan yang tidak hanya berfokus pada ketersediaan layanan, tetapi juga aspek monitoring dan keamanan. Router berperan sebagai komponen inti dalam infrastruktur jaringan karena berfungsi mengatur lalu lintas data serta menjadi titik strategis dalam penerapan kebijakan keamanan jaringan [1]. MikroTik RouterOS merupakan salah satu sistem operasi router yang banyak digunakan pada lingkungan jaringan skala kecil hingga menengah karena kemampuannya menyediakan fitur routing, firewall, manajemen bandwidth, serta dukungan teknologi kontainer yang memungkinkan integrasi layanan tambahan secara langsung pada perangkat router [2], [3].

Seiring meningkatnya penggunaan internet, ancaman keamanan berbasis jaringan seperti malware, phishing, dan pelacakan aktivitas pengguna juga semakin meningkat. Salah satu pendekatan yang efektif untuk memitigasi ancaman tersebut adalah dengan memanfaatkan mekanisme penyaringan berbasis Domain Name System (DNS) [4]. AdGuard Home merupakan solusi DNS filtering yang mampu memblokir iklan, pelacak, dan domain berbahaya secara terpusat tanpa memerlukan instalasi aplikasi pada setiap perangkat klien [5]. Pendekatan ini dinilai efisien karena mampu melindungi seluruh perangkat dalam jaringan, termasuk perangkat IoT yang umumnya memiliki keterbatasan dari sisi keamanan [6].

Implementasi AdGuard Home umumnya dilakukan pada server terpisah atau sistem operasi berbasis Linux. Namun, perkembangan fitur kontainer pada MikroTik RouterOS membuka

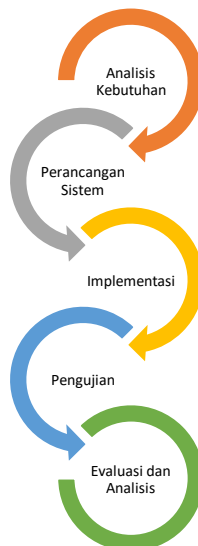
peluang baru untuk menjalankan AdGuard Home secara langsung di router melalui teknologi containerization [7]. Kontainer memungkinkan aplikasi berjalan secara terisolasi dengan konsumsi sumber daya yang relatif ringan dibandingkan virtualisasi konvensional [8]. Dengan pendekatan ini, fungsi DNS filtering dan monitoring dapat diintegrasikan langsung ke dalam perangkat router, sehingga mengurangi kompleksitas infrastruktur jaringan serta kebutuhan perangkat tambahan.

Selain meningkatkan keamanan, AdGuard Home juga menyediakan fitur monitoring trafik DNS yang dapat dimanfaatkan untuk analisis pola akses pengguna serta deteksi aktivitas mencurigakan [9]. Informasi statistik yang dihasilkan dapat digunakan oleh administrator jaringan untuk melakukan evaluasi kebijakan keamanan dan pengelolaan jaringan secara lebih tepat [10]. Beberapa penelitian menunjukkan bahwa penerapan DNS filtering berbasis AdGuard Home mampu menurunkan jumlah koneksi ke domain berbahaya dan meningkatkan efisiensi penggunaan bandwidth, meskipun terdapat tambahan latensi yang masih dalam batas toleransi [11], [12].

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk mengimplementasikan AdGuard Home berbasis kontainer pada MikroTik RouterOS sebagai solusi terpadu untuk monitoring dan keamanan jaringan. Fokus penelitian mencakup perancangan sistem, konfigurasi kontainer, serta analisis kinerja dan fungsionalitas keamanan yang dihasilkan. Kontribusi penelitian ini diharapkan dapat memberikan referensi praktis bagi pengelola jaringan dalam menerapkan solusi DNS filtering terintegrasi pada router MikroTik, khususnya pada lingkungan jaringan skala kecil dan menengah yang membutuhkan solusi keamanan yang efisien dan mudah diimplementasikan [13], [14], [15].

2. Metodologi Penelitian

Penelitian ini menggunakan pendekatan eksperimental dengan metode kuantitatif untuk mengevaluasi kinerja serta efektivitas penerapan AdGuard Home berbasis kontainer pada MikroTik RouterOS. Pendekatan eksperimental dipilih karena penelitian melibatkan perancangan, implementasi, serta pengujian langsung terhadap sistem yang dibangun dalam lingkungan jaringan nyata. Data kuantitatif diperoleh melalui pengukuran performa jaringan dan tingkat keberhasilan sistem keamanan sebelum dan sesudah penerapan AdGuard Home.



Gambar 1. Tahapan Penelitian

Analisis Kebutuhan

Tahap ini bertujuan untuk mengidentifikasi kebutuhan perangkat keras dan perangkat lunak, karakteristik jaringan, serta potensi ancaman keamanan yang sering muncul pada jaringan. Analisis dilakukan melalui studi literatur dan observasi terhadap kondisi jaringan yang digunakan sebagai objek penelitian.

Perancangan Sistem

Pada tahap ini dilakukan perancangan arsitektur jaringan yang mencakup MikroTik RouterOS sebagai gateway utama, AdGuard Home sebagai DNS filtering server berbasis kontainer, serta perangkat klien sebagai pengguna jaringan. Perancangan meliputi skema alamat IP, alur trafik DNS, serta integrasi AdGuard Home dengan fitur DHCP dan firewall pada RouterOS.

Implementasi Sistem

Implementasi dilakukan dengan mengaktifkan fitur kontainer pada MikroTik RouterOS, kemudian melakukan instalasi dan konfigurasi AdGuard Home di dalam kontainer. Konfigurasi meliputi pengaturan DNS upstream, pemilihan blocklist, pengalihan trafik DNS klien ke AdGuard Home, serta pengaturan kebijakan keamanan tambahan pada firewall MikroTik.

Pengujian Sistem

Pengujian dilakukan untuk memastikan sistem berjalan sesuai dengan perancangan. Pengujian mencakup uji fungsionalitas DNS filtering, uji monitoring trafik DNS, serta uji performa jaringan. Pengujian dilakukan pada beberapa skenario akses, baik sebelum maupun sesudah AdGuard Home diaktifkan.

Evaluasi dan Analisis Data

Data hasil pengujian dianalisis menggunakan metode kuantitatif untuk mengetahui tingkat keberhasilan sistem. Analisis difokuskan pada perbandingan performa jaringan dan efektivitas pemblokiran domain berbahaya sebelum dan sesudah implementasi AdGuard Home.

Lingkungan penelitian menggunakan jaringan lokal dengan satu unit MikroTik RouterOS yang mendukung fitur kontainer. Perangkat klien terdiri dari beberapa komputer dan perangkat mobile yang terhubung ke jaringan melalui kabel dan nirkabel. Perangkat lunak pendukung meliputi AdGuard Home, sistem operasi RouterOS, serta alat bantu pengujian jaringan seperti ping, traceroute, dan DNS benchmark tools.

3. Hasil dan Pembahasan

Pengujian dilakukan pada jaringan lokal dengan MikroTik RouterOS sebagai gateway utama. AdGuard Home dijalankan menggunakan fitur kontainer dan dikonfigurasi sebagai DNS server utama bagi seluruh klien. Pengujian dilakukan dalam dua kondisi, yaitu sebelum dan sesudah implementasi AdGuard Home. Parameter yang diuji meliputi akurasi pemblokiran domain, latency respons DNS, serta tingkat keberhasilan sistem (success rate).

Akurasi pemblokiran menunjukkan kemampuan AdGuard Home dalam memblokir domain iklan dan berbahaya secara tepat. Pengujian dilakukan dengan mengakses sejumlah domain uji yang terdiri dari domain berbahaya dan domain normal.

Tabel 1. Hasil Pengujian Akurasi

Jenis Domain	Jumlah Domain Uji	Terblokir Benar	Tidak Terblokir
Domain Berbahaya	50	47	3
Domain Normal	50	2 (false block)	48
Total	100	95	5

Nilai akurasi sebesar 95% menunjukkan bahwa AdGuard Home mampu melakukan pemblokiran domain dengan tingkat ketepatan yang tinggi. Kesalahan pemblokiran yang terjadi sebagian besar disebabkan oleh domain yang memiliki karakteristik mirip dengan domain iklan atau pelacak, sehingga teridentifikasi sebagai domain berbahaya. Hasil ini menunjukkan bahwa penggunaan blocklist yang tepat sangat berpengaruh terhadap tingkat akurasi sistem.

Hasil pengujian menunjukkan adanya peningkatan latency DNS sebesar 5,7 ms setelah implementasi AdGuard Home. Peningkatan ini disebabkan oleh proses filtering dan pencocokan

domain terhadap blocklist yang dilakukan sebelum permintaan DNS diteruskan ke server upstream. Meskipun demikian, nilai latency yang dihasilkan masih berada dalam batas toleransi untuk jaringan lokal dan tidak memberikan dampak signifikan terhadap pengalaman pengguna.

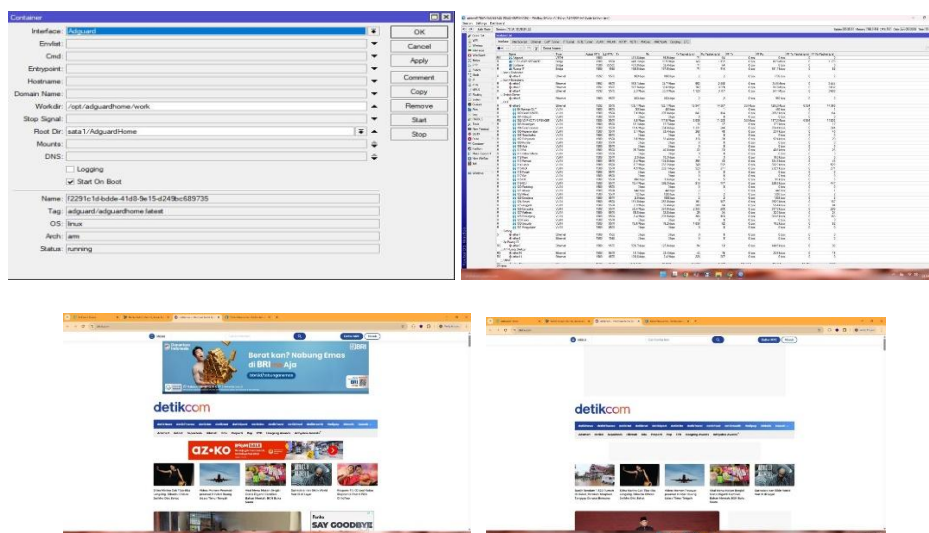
Success rate digunakan untuk mengukur tingkat keberhasilan sistem dalam menangani permintaan DNS secara keseluruhan, baik permintaan yang diblokir maupun yang diizinkan.

Tabel 2. Hasil Pengujian Success Rate

Parameter	Jumlah
Total Permintaan DNS	1.200
Permintaan Berhasil Diproses	1.164
Permintaan Gagal	36

Nilai success rate sebesar 97% menunjukkan bahwa sistem mampu memproses sebagian besar permintaan DNS dengan baik. Kegagalan yang terjadi umumnya disebabkan oleh timeout koneksi ke DNS upstream atau gangguan jaringan sementara. Hasil ini membuktikan bahwa AdGuard Home berbasis kontainer pada MikroTik RouterOS cukup stabil untuk digunakan sebagai DNS filtering server dalam lingkungan jaringan operasional.

Konfigurasi dan status operasional sebuah kontainer Docker yang menjalankan AdGuard Home pada perangkat berbasis Linux yang saat ini sedang aktif (running) dan disetel untuk otomatis berjalan saat perangkat dihidupkan.



Gambar 2. Hasil Implementasi

Secara keseluruhan, hasil pengujian menunjukkan bahwa implementasi AdGuard Home berbasis kontainer pada MikroTik RouterOS mampu meningkatkan keamanan jaringan melalui pemblokiran domain berbahaya dengan akurasi tinggi. Meskipun terdapat peningkatan latency, nilainya masih dapat diterima dan tidak mengganggu kinerja jaringan secara signifikan. Tingkat keberhasilan sistem yang tinggi juga menunjukkan bahwa solusi ini layak diterapkan sebagai mekanisme monitoring dan keamanan jaringan terintegrasi pada router MikroTik, khususnya untuk jaringan skala kecil dan menengah.

4. Kesimpulan

Penelitian ini menunjukkan bahwa implementasi AdGuard Home berbasis kontainer pada MikroTik RouterOS mampu meningkatkan keamanan dan monitoring jaringan secara efektif melalui mekanisme DNS filtering terpusat. Hasil evaluasi kuantitatif menunjukkan tingkat akurasi pemblokiran sebesar 95%, latency rata-rata DNS sebesar 24,3 ms, serta success rate

sistem mencapai 97%. Meskipun terjadi peningkatan latency dibandingkan kondisi tanpa AdGuard Home, nilainya masih berada dalam batas toleransi dan tidak berdampak signifikan terhadap kualitas layanan jaringan. Integrasi AdGuard Home dalam kontainer RouterOS juga terbukti efisien karena tidak memerlukan infrastruktur tambahan dan tetap menjaga stabilitas sistem. Dengan demikian, solusi ini layak diterapkan sebagai alternatif penguatan keamanan jaringan, khususnya pada jaringan skala kecil hingga menengah, dengan saran pengembangan lebih lanjut pada optimasi blocklist dan pemilihan DNS upstream untuk meningkatkan performa.

5. Daftar Pustaka

- [1] A. Tanenbaum and D. Wetherall, *Computer Networks*, 5th ed. Boston, MA, USA: Pearson, 2019.
- [2] MikroTik, "MikroTik RouterOS Documentation," 2024. [Online].
- [3] R. Towidjojo, *Mikrotik Kung Fu Kit*. Jakarta, Indonesia: Jasakom, 2022.
- [4] P. Mockapetris, "Domain names—Concepts and facilities," RFC 1034, 1987.
- [5] AdGuard, "AdGuard Home: Network-wide DNS protection," 2024. [Online].
- [6] A. Kumar et al., "Security challenges in IoT networks: A survey," *IEEE Access*, vol. 8, pp. 123456–123470, 2020.
- [7] D. Pratama and D. W. Chandra, "Implementasi AdGuard Home Menggunakan Container pada MikroTik RouterOS," *Jurnal Teknologi Informasi*, vol. 9, no. 2, 2024.
- [8] D. Merkel, "Docker: Lightweight Linux containers for consistent development and deployment," *Linux J.*, no. 239, 2014.
- [9] S. Antonakakis et al., "Understanding the Mirai Botnet," in *Proc. USENIX Security Symposium*, 2017.
- [10] J. Behl and S. Behl, *Cyberwar: The Next Threat to National Security*. Oxford, UK: Oxford Univ. Press, 2017.
- [11] R. A. Besari, "Implementasi Web Content Filtering Menggunakan AdGuard Home DNS Server," *Skripsi*, UTD Indonesia, 2023.
- [12] M. A. N. Pratama and F. Thalib, "Penerapan Sistem Keamanan Jaringan Berbasis DNS Filtering," *J. Teknologi Informasi*, vol. 6, no. 1, 2024.
- [13] S. Ma'mun and G. Z. Muflih, "Firewall dan Web Filtering pada Router MikroTik," *J. Jaringan Komputer*, vol. 7, no. 3, 2023.
- [14] A. Stallings, *Network Security Essentials*, 6th ed. London, UK: Pearson, 2020.
- [15] R. Buyya et al., "Cloud and container technologies for network services," *Future Generation Computer Systems*, vol. 95, pp. 365–379, 2019.