E-ISSN : 2988-1986
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 9 No 1 Tahun 2025

STUDI EVALUASI CLOUDFLARE WARP TERHADAP PERFORMA KECEPATAN DAN KEAMANAN DATA SEBAGAI ALTERNATIF VPN

(EVALUATION STUDY OF CLOUDFLARE WARP ON NETWORK SPEED PERFORMANCE AND DATA SECURITY AS VPN ALTERNATIVE)

Iman Setiawan[1], Delfian Ruly Havatilla[2], Ahmad Syukron[3], Abid Husein[4].
[1,2,3,4]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa,
Jl. Inspeksi Kalimalang No.9, Cibatu, Cikarang Sel., Kabupaten Bekasi, Jawa Barat.
[1]imansetiawan1998@mhs.pelitabangsa.ac.id, [2]delfiansteel@mhs.pelitabangsa.ac.id,
[3]ahmad.s01@mhs.pelitabangsa.ac.id, [4]abid30@mhs.pelitabangsa.ac.id .

Abstrak

Cloudflare WARP merupakan layanan VPN ringan berbasis protokol WireGuard yang dirancang untuk meningkatkan keamanan dan privasi tanpa mengorbankan performa koneksi internet. Penelitian ini merupakan pengujian awal secara sederhana yang bertujuan untuk mengevaluasi efektivitas Cloudflare WARP dalam menjaga kecepatan dan keamanan koneksi, terutama saat digunakan pada jaringan publik. Pengujian dilakukan dengan membandingkan dua kondisi—tanpa dan dengan penggunaan WARP—melalui serangkaian parameter dasar seperti bandwidth, latency, jitter, packet loss, serta aspek keamanan jaringan. Hasil pengujian menunjukkan bahwa penggunaan WARP tidak memberikan dampak signifikan terhadap performa kecepatan jaringan, dengan bandwidth tetap stabil di kisaran 51–55 Mbps, latency hanya mengalami kenaikan ringan dari 15–17 ms menjadi 17–24 ms, dan packet loss tetap rendah. Dari sisi keamanan, WARP terbukti mampu menyembunyikan IP asli pengguna, mencegah DNS dan IP leak, mengenkripsi lalu lintas data, serta memfilter seluruh port akses. Berdasarkan hasil tersebut, Cloudflare WARP dinilai layak sebagai solusi VPN ringan yang memberikan proteksi identitas digital tanpa mengurangi kenyamanan pengguna, khususnya saat terhubung ke jaringan Wi-Fi publik.

Keyword: Cloudflare WARP, VPN, Keamanan Jaringan, Performa Internet, WireGuard.

Abstract

Cloudflare Cloudflare WARP is a lightweight VPN service based on the WireGuard protocol, designed to enhance user privacy and security without compromising internet performance. This study presents a simple preliminary evaluation aimed at assessing the effectiveness of Cloudflare WARP in maintaining connection speed and security, especially when used on public networks. The testing compares two conditions—with and without WARP—using basic network parameters such as bandwidth, latency, jitter, packet loss, and several security aspects. The results indicate that WARP does not significantly degrade network performance, with bandwidth remaining stable at 51–55 Mbps, latency increasing slightly from 15–17 ms to 17–24 ms, and packet loss staying low. From a security perspective, WARP successfully hides the user's real IP address, prevents DNS and IP leaks,

Article History
Received: Juni 2025
Reviewed: July 2025
Published: July 2025

Plagiarism Checker No 235
Prefix DOI :
10.8734/Kohesi.v1i2.365
Copyright : Author
Publish by : Kohesi

encrypts traffic, and filters all open ports. These findings suggest that Cloudflare WARP is a viable lightweight VPN solution that provides identity protection without sacrificing user experience, particularly on public Wi-Fi networks.
***Keywords**: Cloudflare WARP, VPN, Network Security, Internet Performance, WireGuard*

PENDAHULUAN

Dalam era digital saat ini, kebutuhan akan koneksi internet yang aman dan cepat menjadi sangat penting, terutama ketika aktivitas daring melibatkan pertukaran data sensitif atau dilakukan melalui jaringan publik seperti *Wi-Fi* di tempat umum. Baik individu maupun organisasi kini sangat bergantung pada internet untuk menunjang berbagai aktivitas, mulai dari pekerjaan jarak jauh, penyimpanan data berbasis cloud, hingga transaksi finansial. Oleh karena itu, jaminan terhadap privasi, integritas data, serta kecepatan dan kestabilan koneksi menjadi hal yang esensial.

Salah satu solusi yang umum digunakan untuk meningkatkan keamanan saat mengakses internet adalah layanan *Virtual Private Network (VPN)*. *VPN* bekerja dengan cara mengenkripsi lalu lintas data dan menyembunyikan alamat IP asli pengguna, sehingga mampu mencegah berbagai ancaman seperti penyadapan (*sniffing*), pencurian data, dan serangan *Man-in-the-Middle* (Ali dkk., 2025). Namun, meskipun efektif dari sisi keamanan, VPN tradisional memiliki sejumlah kelemahan, seperti meningkatnya *latency*, penurunan kecepatan transfer data (*throughput*), serta ketidakstabilan *IP*, terutama saat koneksi diarahkan melalui *server* yang jauh secara geografis atau menggunakan protokol yang berat.

Sebagai alternatif dari *VPN* konvensional, *Cloudflare WARP* hadir sebagai solusi VPN ringan dan modern yang berbasis protokol WireGuard. Layanan ini dirancang bukan untuk menyamarkan lokasi sepenuhnya, melainkan untuk mengenkripsi lalu lintas data dan mengoptimalkan jalur koneksi secara efisien. Dengan pendekatan ini, pengguna tetap dapat menikmati koneksi yang cepat dan aman tanpa perlu konfigurasi teknis yang kompleks. Keunggulan lain dari *WARP* adalah ketersediaannya secara gratis, serta komitmen *Cloudflare* dalam menjaga keamanan data pengguna melalui kebijakan tanpa pencatatan *IP* permanen, tanpa pelacakan aktivitas, dan penggunaan enkripsi DNS untuk mencegah kebocoran data.

Beberapa penelitian telah membuktikan bahwa protokol *WireGuard*, yang menjadi fondasi *Cloudflare WARP*, memiliki efisiensi yang jauh lebih baik dibandingkan protokol *VPN* lain seperti *IPsec*. Penelitian yang dilakukan Hermawan dan Saputra (2025) mereka menemukan bahwa penggunaan *WireGuard* mampu mengurangi latency hingga 97,66% dan meningkatkan throughput lebih dari 600% dalam implementasi jaringan *hybrid cloud*. Berdasarkan latar belakang tersebut, penelitian ini dilakukan untuk mengevaluasi performa dan keamanan *Cloudflare WARP* sebagai alternatif *VPN*. Pengujian dilakukan dengan membandingkan dua kondisi koneksi internet tanpa dan dengan Cloudflare WARP dengan mengukur parameter teknis seperti bandwidth, *latency, jitter, packet loss*, serta keamanan data melalui pengujian *DNS leak, IP leak,* enkripsi lalu lintas, dan *port filtering*.

LANDASAN TEORI

Virtual Private Network (VPN) adalah teknologi yang memungkinkan pengguna untuk membuat koneksi pribadi yang aman melalui jaringan publik. *VPN* bekerja dengan mengenkripsi lalu lintas data dan menyembunyikan alamat IP pengguna, sehingga melindungi identitas serta menjaga privasi saat berselancar di internet (Cloudflare Inc., 2024). Dalam praktiknya, *VPN* banyak digunakan ketika mengakses jaringan terbuka seperti *Wi-Fi* publik untuk mencegah penyadapan atau pelacakan aktivitas pengguna. Namun demikian, *VPN* konvensional sering kali menimbulkan penurunan performa koneksi, seperti kecepatan internet yang melambat, peningkatan latency, serta rute data yang tidak optimal.

Cloudflare WARP merupakan solusi alternatif *VPN* yang dikembangkan oleh *Cloudflare* dan ditawarkan secara gratis kepada publik. Layanan ini dirancang untuk memberikan perlindungan privasi tanpa mengorbankan kecepatan koneksi. Berbasis protokol *WireGuard*, *WARP* mengenkripsi lalu lintas data pengguna dan mengarahkannya melalui jaringan global *Cloudflare*, sehingga tidak hanya aman, tetapi juga cepat dan efisien (Cloudflare Inc., 2024). *Cloudflare* menunjukkan komitmen kuat dalam menjaga keamanan dan privasi pengguna dengan tidak mencatat alamat IP secara permanen, tidak menjual data ke pihak ketiga, serta tidak menggunakan data untuk tujuan iklan atau pelacakan. Permintaan DNS yang dikirim melalui *WARP* juga diamankan dengan *DNS over HTTPS (DoH)* atau *DNS over TLS (DoT),* yang mencegah kebocoran informasi melalui resolver. Selain itu, *Cloudflare* secara rutin menjalani audit independen untuk memastikan transparansi sistem dan memperkuat kepercayaan pengguna terhadap layanannya.. Salah satu keunggulan *WARP* dibanding *VPN* lainnya adalah kemampuannya menjaga IP tetap tersembunyi serta mencegah *DNS leak* dan *IP leak* tanpa perlu konfigurasi rumit (DNS Leak Test, 2024; IPLeak.net, 2024).

Dalam pengujian performa jaringan, beberapa parameter penting yang digunakan meliputi *bandwidth, latency, jitter, dan packet loss*. Bandwidth mengukur kapasitas transfer data, sementara latency mengukur kecepatan respon koneksi. Jitter mencerminkan kestabilan delay antar paket, dan packet loss menunjukkan efisiensi transmisi data (iperf.fr, 2024). Selain performa, aspek keamanan diuji dengan tools seperti *Wireshark* untuk memastikan lalu lintas terenkripsi, dan *Nmap* untuk mendeteksi celah seperti port terbuka (Wireshark Foundation, 2024). Melalui kombinasi perlindungan identitas, kemudahan penggunaan, dan tersedianya layanan secara gratis, *Cloudflare WARP* menjadi pilihan yang relevan untuk pengguna yang ingin mendapatkan keamanan jaringan tanpa biaya tambahan dan tanpa kehilangan performa koneksi.

METODOLOGI

Penelitian ini menggunakan pendekatan eksperimen kuantitatif dengan metode komparatif, yaitu membandingkan dua kondisi koneksi internet tanpa menggunakan *Cloudflare WARP* dan dengan menggunakan *Cloudflare WARP* untuk mengukur perbedaan performa dan tingkat keamanan data. Pengujian dilakukan dalam lingkungan nyata menggunakan perangkat client dan server yang terkoneksi secara langsung melalui jaringan publik. Hasil dari kedua kondisi kemudian dianalisis berdasarkan parameter-parameter teknis yang telah ditentukan.

Pengujian ini bertujuan untuk mendapatkan gambaran menyeluruh tentang efektivitas *Cloudflare WARP* dalam menjaga performa koneksi sekaligus meningkatkan keamanan data pengguna. Untuk memastikan validitas dan konsistensi hasil, setiap pengujian dilakukan sebanyak tiga kali, kemudian hasil dari masing-masing parameter dirata-ratakan. Pendekatan ini digunakan agar data yang diperoleh lebih stabil, mengurangi pengaruh dari fluktuasi jaringan, dan memberikan gambaran kinerja yang lebih representatif.

Penelitian dilaksanakan di lingkungan nyata (*real-world environment*), menggunakan sebuah laptop pribadi sebagai perangkat client dengan spesifikasi prosesor *Intel Core* i3-1215U dan *RAM* sebesar 12 GB. Perangkat ini terhubung ke jaringan internet melalui koneksi *Wi-Fi* dari perpustakaan kampus Universitas Pelita Bangsa. Sementara itu, sebagai *server* uji digunakan layanan *VPS (Virtual Private Server)* gratis dari *Oracle Free Tier* dengan spesifikasi 2 vCPU dan 1 GB RAM. Server ini berfungsi sebagai titik akhir pengujian koneksi untuk mengukur performa dan aspek keamanan data. Pengujian dilakukan dalam dua kondis yaitu dengan menggunakan *Cloudflare WARP* dan tanpa menggunakan *Cloudflare WARP*, untuk mengetahui pengaruh langsung dari layanan tersebut terhadap parameter jaringan. Berikut adalah parameter yang diuji beserta alat dan penjelasan masing-masing pengujian:

Tabel Parameter Pengujian

Aspek	Parameter	Alat Uji	Penjelasan
Kecepatan Data	*Bandwidth / Throughput*	iperf3 (TCP mode)	Mengukur besar data yang dikirimkan per detik dari client ke server
	Latency / Ping	*Ping (Windows command)*	Mengukur waktu respon komunikasi ke server dalam milidetik
	Jitter	*iperf3* (UDP mode)	Mengukur fluktuasi waktu antar pengiriman paket data
	Packet Loss	*ping dan iperf3 -u*	Menghitung jumlah paket data yang hilang selama transmisi
	Page Load Speed	*Stopwatch / log manual*	Mengukur waktu muat halaman situs secara manual
Keamanan Data	*DNS Leak*	*dnsleaktest.com*	Mengidentifikasi apakah DNS mengungkapkan alamat server ISP asli
	IP Leak	*ipleak.net*	Mengecek apakah IP asli pengguna masih terlihat saat menggunakan WARP
	Enkripsi Lalu Lintas	*Wireshark*	Menganalisis apakah data dalam jaringan telah dienkripsi
	Port Filtering	*nmap*	Melakukan pemindaian port untuk mendeteksi celah terbuka
	IP Persistence	Pencatatan log IP publik	Mencatat kestabilan alamat IP selama periode waktu tertentu

HASIL DAN PEMBAHASAN

Hasil

Pengujian kecepatan dilakukan untuk mengetahui dampak penggunaan *Cloudflare WARP* terhadap performa koneksi. Parameter yang diuji meliputi *bandwidth, latency, jitter, packet loss,* dan waktu muat halaman. Masing-masing pengujian dilakukan sebanyak tiga kali untuk dua kondisi (dengan dan tanpa *WARP*), kemudian dirata-ratakan guna memperoleh hasil yang stabil dan representatif. Hasil lengkap ditampilkan pada tabel berikut

Tabel Hasil Pengujian Aspek Kecepatan Data

Parameter	Tanpa Cloudflare WARP	Dengan Cloudflare WARP	Keterangan
Bandwidth (Avg.)	51.3 Mbps	51.3 Mbps	Stabil, tidak ada penurunan performa
Latency (Ping)	Rata-rata 15–17 ms	Rata-rata 17–24 ms	Naik sedikit, tetapi masih responsif
Jitter	0.081 – 0.544 ms	0.08 – 0.692 ms	Sama-sama stabil, sedikit fluktuatif dengan WARP
Packet Loss	0%	1%	Masih dalam batas wajar
Page Load Speed	50–66 ms	68–72 ms	Selisih kecil, hampir tidak terasa

Pengujian aspek keamanan bertujuan mengevaluasi efektivitas *Cloudflare WARP* dalam melindungi identitas dan data pengguna. Parameter yang diuji mencakup *DNS leak*, *IP leak*, enkripsi lalu lintas, *port filtering*, dan kestabilan IP (*IP persistence*). Pengujian dilakukan langsung pada dua kondisi jaringan untuk melihat perbedaan tingkat keamanan. Hasil pengujian disajikan pada tabel berikut:

Tabel Hasil Pengujian Aspek Keamanan Data

Parameter	Tanpa Cloudflare WARP	Dengan Cloudflare WARP	Keterangan
DNS Leak	DNS Cloudflare, lokasi 3Jakarta	DNS Cloudflare, lokasi Singapura	Tidak ada kebocoran, tetapi server DNS berubah
IP Leak	IP asli terlihat	IP disamarkan oleh Cloudflare	Identitas pengguna berhasil disembunyikan
Enkripsi Lalu Lintas	Aman	Aman	Kedua koneksi telah terenkripsi
Port Filtering	Semua port filtered (IPv4 dan IPv6)	Semua port filtered (IPv4 dan IPv6)	Tidak ada port terbuka, aman
IP Persistence	IP tetap sama selama 1 jam penuh	IP tetap sama (IPv6) selama 1 jam penuh	Stabil untuk pemakaian jangka panjang

Pembahasan

Hasil pengujian menunjukkan bahwa penggunaan *Cloudflare WARP* tidak memberikan penurunan performa kecepatan jaringan yang signifikan. *Bandwidth* tetap stabil pada kisaran 51–55 Mbps, baik saat menggunakan maupun tanpa menggunakan *WARP*. Peningkatan *latency* dan *jitter* saat *WARP* diaktifkan memang terjadi, namun masih berada dalam batas wajar, yakni dari 15–17 ms menjadi 17–24 ms untuk *latency*, dan dari 0.08–0.54 ms menjadi 0.08–0.69 ms untuk *jitter*. *Packet loss* juga tergolong rendah, hanya mencapai 1% saat menggunakan *WARP*, sedangkan koneksi biasa tidak mengalami kehilangan paket. Sementara itu, selisih waktu muat halaman antara kedua kondisi sangat kecil dan tidak berdampak pada pengalaman pengguna secara nyata.

Dari sisi keamanan, *Cloudflare WARP* memberikan perlindungan yang jauh lebih baik dibandingkan koneksi biasa. Berdasarkan hasil uji *DNS leak* dan *IP leak*, *Cloudflare WARP* mampu menyembunyikan alamat IP asli pengguna dan mengganti DNS ke *server Cloudflare* di luar lokasi pengguna, sehingga meningkatkan privasi. Enkripsi lalu lintas juga terdeteksi aktif saat menggunakan *WARP*, memastikan bahwa data tidak dapat dengan mudah disadap atau diakses oleh pihak ketiga. Selain itu, hasil pemindaian *port* menggunakan *Nmap* menunjukkan bahwa seluruh port dalam kondisi terfilter, yang menandakan bahwa sistem tidak memiliki celah terbuka yang rentan terhadap serangan dari luar.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil pengujian dan analisis yang telah dilakukan, dapat disimpulkan bahwa *Cloudflare WARP* merupakan layanan *VPN* yang efektif dan efisien untuk meningkatkan keamanan koneksi internet tanpa memberikan dampak negatif yang signifikan terhadap performa kecepatan jaringan. Pengujian menunjukkan bahwa *bandwidth* tetap stabil, *latency* dan *jitter* hanya mengalami peningkatan kecil, dan waktu muat halaman masih dalam batas normal. Hal ini membuktikan bahwa *WARP* dapat digunakan tanpa mengorbankan kenyamanan pengguna sehari-hari, bahkan pada jaringan publik seperti *Wi-Fi* kampus atau tempat umum lainnya.

Dari sisi keamanan, *Cloudflare WARP* memberikan perlindungan yang unggul dengan menyembunyikan *IP* asli pengguna, mencegah *DNS* dan *IP leak*, serta mengenkripsi seluruh lalu lintas data. Selain itu, *port* jaringan terdeteksi dalam kondisi terfilter dan *IP* publik tetap konsisten selama koneksi aktif. Keunggulan ini diperkuat oleh komitmen *Cloudflare* terhadap privasi pengguna, yang ditunjukkan melalui kebijakan untuk tidak menyimpan *IP* secara permanen, tidak menjual data pengguna, serta tidak memanfaatkan lalu lintas *WARP* untuk kepentingan iklan atau pelacakan. Penggunaan teknologi seperti *DNS over HTTPS (DoH)* atau *DNS over TLS (DoT)*, serta audit keamanan independen yang rutin dilakukan, menunjukkan keseriusan *Cloudflare* dalam menjaga kepercayaan dan keamanan penggunanya. Dengan demikian, *Cloudflare WARP* sangat layak dipertimbangkan sebagai solusi pengamanan koneksi internet yang ringan, aman, dan tetap cepat.

Saran

Berdasarkan hasil yang diperoleh, disarankan agar pengguna yang sering terhubung ke jaringan publik seperti *Wi-Fi* kampus, kafe, atau tempat umum mempertimbangkan penggunaan *Cloudflare WARP* sebagai solusi keamanan tambahan yang ringan dan efisien. Untuk pemanfaatan yang lebih optimal, pengguna dapat mengaktifkan fitur *WARP+* bila membutuhkan jalur koneksi yang lebih cepat. Penelitian selanjutnya dapat memperluas cakupan pengujian, misalnya dengan melibatkan berbagai jenis perangkat (*desktop* dan *mobile*), jaringan di lokasi geografis yang berbeda, atau membandingkan performa *WARP* dengan layanan *VPN* lainnya guna memperoleh perspektif yang lebih menyeluruh terhadap efektivitas solusi *VPN* modern dalam berbagai skenario penggunaan.

DAFTAR PUSTAKA

Ali, T. S., Santoso, I., Quiko, A. S., & Santoso, G. (2025). Pengaruh Virtual Private Network (VPN) terhadap keamanan dan performa akses jaringan. JAREKOM: Jurnal Jaringan dan Rekayasa Komputer, 1(1), 22–33. https://doi.org/10.9020/jarekom.v1i1.903

Aptrio, Z., Khairil, K., & Supardi, R. (2025). Penerapan proxy server pada jaringan internet di Kantor Camat Selebar. Jurnal Media Infotama, 21(1), 152–157. https://doi.org/10.37676/jmi.v21i1.7540

Budi, R. S., & Sembiring, I. (2025). Implementasi keamanan jaringan komputer dengan iptables sebagai firewall menggunakan port knocking metode dinamis. JIPI: Jurnal Ilmiah Penelitian dan Pembelajaran Informatika, 10(1), 720–738. https://doi.org/10.29100/jipi.v10i1.5750

Cloudflare Inc. (2024). What is Cloudflare WARP? https://www.cloudflare.com/warp/

DNS Leak Test. (2024). Test your VPN for DNS leaks. https://www.dnsleaktest.com

Fitrian, H. P., Destiara, N. A., Destianti, N. E., & Khowat, G. M. (2025). Analisis penerapan teknologi Virtual Private Network (VPN) sebagai solusi keamanan data di jaringan publik. JATI: Jurnal Manajemen Informatika, 9(1). https://doi.org/10.36040/jati.v9i1.12712

Hermawan, R., & Saputra, Y. M. (2025). Analisis perbandingan penggunaan metode tunneling Cloud Virtual Private Network dan WireGuard Virtual Private Network pada implementasi infrastruktur hybrid cloud. Journal of Internet and Software Engineering, 6(1), 1–12. https://doi.org/10.22146/jise.v6i1.14450

IPLeak.net. (2024). Test your VPN for IP leaks. https://ipleak.net

iperf.fr. (2024). iPerf - The ultimate speed test tool for TCP, UDP and SCTP. https://iperf.fr

Murya, R. A., Arfian, M. H., Anwar, N., & Sutanto, I. (2025). Implementasi VPN antar cabang menggunakan teknologi SDWAN Fortigate dengan metode load balance. IKRAITH-INFORMATIKA, 9(1).

Nmap.org. (2024). Nmap Security Scanner. https://nmap.org

Pratikno, R. S., Trinata, C., & Hertantyo, G. B. (2025). Kajian literatur analisis keamanan jaringan. Pendas: Jurnal Ilmiah Pendidikan Dasar, 20(2), 250–260.

Putra, F. P. E., Setiawan, Y., Arifin, S., & Hidayatullah, W. (2025). Peran VPN dalam menjaga privasi pengguna jaringan publik. Jurnal Informatika dan Teknologi Komputer, 5(1). https://doi.org/10.55606/jitek.v5i1.5834

Ramadhani, A., Palasara, N., & Gani, A. (2025). Filtering firewall dan manajemen bandwidth untuk keamanan jaringan pada Kelurahan Buaran Indah. REMIK: Riset dan E-Jurnal Manajemen Informatika Komputer, 9(1), 346–355. https://doi.org/10.33395/remik.v9i1.14482

Wireshark Foundation. (2024). Wireshark: The world's foremost network protocol analyzer. https://www.wireshark.org

Alamin, U., & Mu'min, M. A. (2025). Analisis keamanan jaringan pada sistem kendali jarak jauh untuk infrastruktur kritis. JPST: Jurnal Penelitian Sains dan Teknologi, 1(1). https://doi.org/10.63866/jpst.v1i1.39