ANALISIS PERFORMA ACCESS CONTROL LIST DENGAN METODE FIREWALL POLICY BASE DAN ZERO TRUST ARCHITECTURE (ZTA)

TUGAS AKHIR

Diajukan Untuk Memenuhi
Persyaratan Guna Meraih Gelar Sarjana
Informatika Universitas Muhammadiyah Malang

Muhammad Andika Saputra

202110370311184

Sistem dan Keamanan Jaringan

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH MALANG
2025

LEMBAR PERSETUJUAN

Analisis Performa Access Control List dengan Metode Firewall Policy Base dan Zero Trust Architecture (ZTA)

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
Informatika Universitas Muhammadiyah Malang

Menyetujui,
Malang, *17 Juli 2025*

Dosen Pembimbing 1	Dosen Pembimbing 2
Ir Denar Regata Akbi S.Kom., M.Kom.	**Diah Risqiwati ST., MT.**
NIP. 10816120591PNS.	**NIP. 10814100545PNS.**

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Analisis Performa Access Control List dengan Metode Firewall Policy Base dan Zero Trust Architecture (ZTA)

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
InformatikaUniversitas Muhammadiyah Malang

Disusun Oleh :

MUHAMMAD ANDIKA SAPUTRA

202110370311184

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji pada tanggal 17 Juli 2025

Menyetujui,

Dosen Penguji 1	Dosen Penguji 2
Ir. Wildan Suharso S.Kom., M.Kom	**Bashor Fauzan Muthohirin S.Kom., M.Kom**
NIP. 10817030596PNS.	**NIP. 20230126071994PNS.**

Mengetahui,
Ketua Jurusan Informatika

M.Galih Wasis Wicaksono S.kom. M.Cs.
NIP. 10814100541PNS.

ii

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NAMA : MUHAMMAD ANDIKA SAPUTRA

NIM 202110370311184

FAK./JUR. : Informatika

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **"Analisis Performa Access Control List dengan Metode Firewall Policy Base dan Zero Trust Architecture (ZTA)"** beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko/sanksi yang berlaku.

Mengetahui,
Dosen Pembimbing

Malang, 17 Juli 2025
Yang Membuat Pernyataan

MUHAMMAD ANDIKA SAPUTRA

Ir Denar Regata Akbi S.Kom., M.Kom.

ABSTRAK

Keamanan jaringan menjadi prioritas utama dalam menjaga integritas dan ketersediaan layanan digital. Salah satu pendekatan yang umum digunakan adalah Access Control List (ACL) dengan metode Firewall Policy Base (FPB), yang memberikan kontrol akses berdasarkan aturan statis antarzona jaringan. Namun, pendekatan ini dinilai kurang adaptif terhadap ancaman siber modern. Penelitian ini membandingkan metode FPB dengan Zero Trust Architecture (ZTA), sebuah pendekatan berbasis prinsip "Never Trust, Always Verify" yang memverifikasi setiap permintaan akses berdasarkan identitas dan konteks. Simulasi dilakukan menggunakan GNS3 dengan skenario pengujian melalui Iperf3 (mengukur throughput, latency, jitter), Traceroute (mengamati hop dan RTT), serta Wireshark (menganalisis pemblokiran TCP dan UDP). hasil pengujian menunjukkan bahwa ZTA secara konsisten memblokir koneksi tidak sah dari zona external dan memberikan performa tinggi bagi perangkat internal yang tervalidasi. Sebaliknya, FPB masih memberikan akses terbuka dari luar dengan performa rendah dan kontrol terbatas. Berdasarkan hasil ini, ZTA dinilai lebih unggul dalam meningkatkan keamanan jaringan tanpa mengorbankan efisiensi performa, sedangkan FPB tetap sesuai untuk implementasi pada jaringan berskala kecil yang membutuhkan konfigurasi sederhana.

Kata kunci: Keamanan Jaringan, Access Control List (ACL), Firewall Policy Base, Zero Trust Architecture (ZTA), Performa Jaringan, kontrol akses, Segmentasi.

ABSTRAK

Network security is a top priority in maintaining the integrity and availability of digital services. One commonly used approach is the Access Control List (ACL) with the Firewall Policy-Based (FPB) method, which provides access control based on static rules between network zones. However, this approach is considered less adaptive to modern cyber threats. This study compares the FPB method with Zero Trust Architecture (ZTA), an approach based on the "Never Trust, Always Verify" principle that verifies every access request based on identity and context. Simulations were conducted using GNS3 with test scenarios through Iperf3 (measuring throughput, latency, jitter), Traceroute (observing hop counts and RTT), and Wireshark (analyzing TCP and UDP blocking). Test results show that ZTA consistently blocks unauthorized connections from the external zone and provides high performance for validated internal devices. In contrast, FPB still provides open access from the outside with low performance and limited control. Based on these results, ZTA is considered superior in improving network security without sacrificing performance efficiency, while FPB remains suitable for implementation on small-scale networks that require simple configurations.

Keywords: Network Security, Access Control List (ACL), Firewall Policy Base, Zero Trust Architecture (ZTA), Network Performance, access control, Segmentation.

LEMBAR PERSEMBAHAN

Dengan penuh rasa syukur, saya mempersembahkan tugas akhir ini kepada semua pihak yang telah memberikan dukungan, kasih sayang, dan motivasi sepanjang perjalanan akademik saya. Tanpa bantuan dan doa mereka, saya tidak akan sampai pada titik ini. Setiap langkah yang saya ambil, setiap tantangan yang dihadapi, dan setiap kesulitan yang dilalui, selalu didukung oleh orang-orang terdekat yang senantiasa memberi semangat dan kepercayaan.

Tugas akhir ini saya persembahkan kepada:

1. Kedua orang tua saya, yang telah memberikan kasih sayang, doa, dan dukungan tanpa henti sepanjang hidup saya. Mereka adalah sumber semangat dan motivasi terbesar dalam hidup saya.
2. Dosen Pembimbing I, Ir. Denar Regata Akbi, S.Kom., M.Kom., yang telah memberikan bimbingan, arahan, dan dukungan yang luar biasa dalam menyelesaikan tugas akhir ini.
3. Dosen Pembimbing II, Diah Risqiwati, S.T., M.T., yang telah membantu saya dengan memberikan masukan berharga dan arahan yang sangat bermanfaat selama proses penelitian ini.
4. Teman-teman ,saudara yang telah memberikan dukungan moral dan ide-ide cemerlang dalam mengerjakan tugas akhir ini. Terima kasih atas kebersamaan dan semangat yang telah terjalin.
5. Universitas Muhammadiyah Malang, yang telah menyediakan wadah untuk saya menimba ilmu, serta seluruh staf pengajar dan tenaga kependidikan yang turut berperan dalam perjalanan akademik saya.
6. Diri saya sendiri, sebagai bentuk perjuangan dan pencapaian yang telah diraih dalam menuntut ilmu dan menghadapi berbagai tantangan. Setiap langkah dalam perjalanan ini penuh dengan proses belajar yang tak terhitung jumlahnya, dari hal-hal kecil hingga keputusan besar yang mempengaruhi arah penelitian ini. Tidak hanya menyelesaikan tugas akademik, namun juga berusaha untuk selalu berkembang, memperbaiki diri, dan mengatasi hambatan-hambatan yang muncul selama perjalanan panjang ini. Pengalaman ini mengajarkan tentang ketekunan, keberanian untuk menghadapi kesulitan, serta pentingnya menjaga semangat meskipun terkadang kelelahan datang. Semoga pencapaian ini menjadi bekal untuk perjalanan selanjutnya, baik dalam dunia profesional maupun dalam kehidupan pribadi yang penuh dengan tantangan baru.
7. Seseorang yang selalu menemani**,** yang dengan sabar mendukung dan memberikan semangat sepanjang perjalanan ini. Kehadirannya selalu memberikan rasa tenang dan kekuatan di saat-saat sulit. Dukungan yang tulus dan pengertian yang diberikan tidak hanya sekadar menjadi motivasi,

tetapi juga menjadi sumber kebahagiaan dan ketenangan di tengah segala kesibukan dan tekanan. Keberadaan dan kepercayaannya memberi saya kekuatan untuk terus maju, menjalani setiap tantangan dengan penuh optimisme dan harapan.

Semoga tugas akhir ini dapat memberikan manfaat dan kontribusi positif dalam bidang sistem dan keamanan jaringan. Saya berharap karya ini bisa menjadi bagian dari upaya terus-menerus untuk mencapai tujuan yang lebih besar, baik untuk diri saya sendiri maupun untuk masyarakat ilmu pengetahuan.

Malang,28 Juli 2025

Muhammad Andika Saputra

KATA PENGANTAR

Tugas akhir ini disusun untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana pada Program Studi Informatika Universitas Muhammadiyah Malang. Penelitian ini berjudul **"Analisis Performa Access Control List dengan Metode Firewall Policy Base dan Zero Trust Architecture (ZTA)",** yang bertujuan untuk mengevaluasi efektivitas dan performa kedua metode pengendalian akses jaringan dalam mengatasi ancaman siber yang semakin kompleks.

Keamanan jaringan merupakan salah satu aspek yang paling krusial dalam dunia digital saat ini. Dengan meningkatnya ancaman terhadap integritas data dan privasi, perlindungan jaringan menjadi prioritas utama. Salah satu metode tradisional yang digunakan adalah Access Control List (ACL) dengan pendekatan Firewall Policy Base (FPB), yang efektif pada jaringan berskala kecil. Namun, metode ini memiliki keterbatasan, terutama dalam menghadapi ancaman internal yang dinamis. Sebagai alternatif, Zero Trust Architecture (ZTA) hadir dengan filosofi “Never Trust, Always Verify” yang menawarkan pendekatan keamanan berbasis identitas dan autentikasi berkelanjutan.

Penelitian ini berfokus pada perbandingan performa dan efektivitas kontrol akses antara kedua metode tersebut, menggunakan simulasi jaringan yang dilakukan dengan perangkat lunak GNS3, Wireshark, dan Iperf3. Diharapkan, hasil dari penelitian ini dapat memberikan rekomendasi bagi organisasi dalam memilih solusi keamanan jaringan yang tepat dan adaptif terhadap perkembangan ancaman siber yang terus berkembang. Semoga penelitian ini dapat menjadi kontribusi bagi perkembangan keamanan jaringan dalam menghadapi tantangan dunia digital.

Malang,28 Juli 2025

Muhammad Andika Saputra

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

[1] M. Wahyudi, “Analisis Performa Access Control List menggunakan Metode Firewall Policy Base Performance Analysis of the Access Control List Using the Firewall Policy-Based Method Article Info ABSTRAK,” vol. 20, no. 2, pp. 283–292, 2021, doi: 10.30812/matrik.v20i1.1068.

[2] IBM, “Cost of a Data Breach Report 2024,” 2024.

[3] Y. Kusnanto, M. A. Nugroho, and R. Kartadie, “IMPLEMENTASI ZERO TRUST ARCHITECTURE UNTUK MENINGKATKAN KEAMANAN JARINGAN: PENDEKATAN BERBASIS SIMULASI,” vol. 9, no. 4, pp. 2357–2364, 2024, doi: 10.29100/jipi.v4i1.6943.

[4] H. Haeruddin, F. Favian, and S. E. Prasetyo, “IMPLEMENTASI ZERO TRUST NETWORK UNTUK MENINGKATKAN KEAMANAN JARINGAN MENGGUNAKAN FERRUMGATE DENGAN METODE NDLC,” *Infotech: Journal of Technology Information*, vol. 10, no. 2, pp. 307–318, Nov. 2024, doi: 10.37365/jti.v10i2.324.

[5] L. Alevizos, V. Thong Ta, and M. Hashem Eiza, “Augmenting Zero Trust Architecture to Endpoints Using Blockchain: A State-of-The-Art Review,” 2021.

[6] Z. R. Mojaveri and A. Farago, “Routing Packet Traffic via Enhanced Access Control List for Network Congestion Avoidance,” Jan. 2021, [Online]. Available: http://arxiv.org/abs/2101.10558

[7] R. Chandramouli and Z. Butcher, “A zero trust architecture model for access control in cloud-native applications in multi-location environments,” Sep. 2023. doi: 10.6028/NIST.SP.800-207A.

[8] Y. Ge and Q. Zhu, “Zero Trust for Cyber Resilience,” Dec. 2023, [Online]. Available: http://arxiv.org/abs/2312.02882

[9] S. Ghasemshirazi, G. Shirvani, and M. A. Alipour, “Zero Trust: Applications, Challenges, and Opportunities,” 2023.

[10] Q. Syahputra, D. Akbi, and D. Risqiwati, “Deteksi Dan Mitigasi Serangan DDoS Pada Software Defined Network Menggunakan Algoritma Decision Tree,” *REPOSITOR*, vol. 2, no. 11, pp. 1491–1502, 2020, doi: https://doi.org/10.22219/repositor.v2i11.30964.

[11] K. Ragothaman, Y. Wang, B. Rimal, and M. Lawrence, “Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions,” Feb. 01, 2023, *MDPI*. doi: 10.3390/s23041805.

[12] “Implementasi Moodle dan Ubuntu Server Berbasis LAN untuk Evaluasi Pembelajaran Peserta Didik,” *Jurnal Ilmiah Komputasi*, vol. 22, no. 3, Oct. 2023, doi: 10.32409/jikstik.22.3.3384.

[13] M. Alicea and I. Alsmadi, “Misconfiguration in firewalls and network access controls: Literature review,” Nov. 01, 2021, *MDPI*. doi: 10.3390/fi13110283.

[14] Wahyudi and Dedih, “Proteksi Jaringan Menggunakan Access Control List pada Local Area Network,” 2023.

[15] A. A. Putra, I. Ispandi, and B. O. Lubis, “Perancangan Firewall dan Spanning Tree Protocol Sebagai Sistem Keamanan Jaringan Komputer,” *Jurnal Teknologi Informatika dan Komputer*, vol. 9, no. 1, pp. 48–60, Mar. 2023, doi: 10.37012/jtik.v9i1.1340.

[16] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, “Zero Trust Architecture (ZTA): A Comprehensive Survey,” 2022, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2022.3174679.

[17] M. L. Gambo and A. Almulhem, “Zero Trust Architecture: A Systematic Literature Review,” Feb. 2025, [Online]. Available: http://arxiv.org/abs/2503.11659

[18] S. Ahmadi, “Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities,” *Journal of Engineering Research and Reports*, vol. 26, no. 2, pp. 215–228, Feb. 2024, doi: 10.9734/jerr/2024/v26i21083.

[19] Y. Kannan, “Access Control List (ACL) Compliance Verification And Alarm Systems: Strengthening Network Security.” [Online]. Available: www.ijfmr.com

[20] S. Esabella and Y. Bella Fitriana, “Analisis Keamanan Jaringan Menggunakan Metode Security Policy Development Life Cycle (SPDLC),” *Media Online*, vol. 4, no. 1, pp. 634–641, 2023, doi: 10.30865/klik.v4i1.1157.

[21] M. Raharjo, W. Bismi, and R. Adi Purnama, “Optimizing Network Security Point to Point with ACL Filtering and TTL Methods,” 2023. [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/infortech

[22] M. KholilRomadhoni, L. S. Kenanga, D. R. Akbi, and D. Risqiwati, “Performance Evaluation of Outgoing Interface Selection Method on Fortigate SD-WAN for Network Optimization,” *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, May 2025, doi: 10.22219/kinetik.v10i2.2120.

[23] Dr. B. KalaiSelvi and Aruna. K, “Network Traffic Analysis Using Wireshark,” *International Journal of Research Publication and Reviews*, vol. 4, no. 12, pp. 1960–1965, Dec. 2023, doi: 10.55248/gengpi.4.1223.123506.

[24] E. B. Fernandez and A. Brazhuk, “A critical analysis of Zero Trust Architecture (ZTA),” 2024.

[25] M. Hirai, D. Kotani, and Y. Okabe, “Linking Contexts from Distinct Data Sources in Zero Trust Federation,” *Journal of Information Processing*, vol. 32, pp. 288–296, 2024, doi: 10.2197/ipsjjip.32.288.

[26] Dwi Rizki Mugianto and Rahmat Budiarto, “EVALUASI PENGUJIAN KEAMANAN ARSITEKTUR ZERO TRUST NETWORK PADA JARINGAN SMART HOME UNTUK MENGATASI SERANGAN DATA SNIFFING,” 20

[27] J. Zong, C. Lee, A. Lundgard, J. Jang, D. Hajas, and A. Satyanarayan, “Rich Screen Reader Experiences for Accessible Data Visualization,” May 2022, [Online]. Available: http://arxiv.org/abs/2205.04917

UNIVERSITAS
MUHAMMADIYAH
MALANG

FAKULTAS TEKNIK

INFORMATIKA

informatika.umm.ac.id | informatika@umm.ac.id

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : Muhammad Andika Saputra

NIM : 202110370311184

Judul TA : ANALISIS PERFORMA ACCESS CONTROL LIST DENGAN METODE FIREWALL POLICY BASE DAN ZERO TRUST ARCHITECTURE (ZTA)

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	8 %
2.	Bab 2 – Daftar Pustaka	25 %	7 %
3.	Bab 3 – Analisis dan Perancangan	25 %	4 %
4.	Bab 4 – Implementasi dan Pengujian	15 %	0 %
5.	Bab 5 – Kesimpulan dan Saran	5 %	3 %
6.	Makalah Tugas Akhir	20%	4 %

) Hasil cek plagiarism diisi oleh pemeriksa (staf TU)

***) Maksimal 5 kali (4 Kali sebelum ujian, 1 kali sesudah ujian)**

Mengetahui,

Pemeriksa (Staff TU)

(.....)