UNIVERSITAS BUDI LUHUR
Kampus Pusat : Jl. Raya Ciledug - Petukangan Utara - Jakarta Selatan 12260
Telp : 021-5853753 (hunting), Fax : 021-5853489, http://www.budiluhur.ac.id
FAKULTAS TEKNOLOGI INFORMASI
FAKULTAS EKONOMI DAN BISNIS
FAKULTAS ILMU SOSIAL DAN STUDI GLOBAL
FAKULTAS TEKNIK
FAKULTAS KOMUNIKASI DAN DESAIN KREATIF

BERITA ACARA SIDANG PENDADARAN TUGAS AKHIR

S/UBL/FTI/1122/VII/26

Pada hari ini, Kamis 16 Juli 2026 telah dilaksanakan Ujian Sidang Pendadaran Tugas Akhir sebagai berikut:

Judul: IMPLEMENTASI PEMANTAUAN KEAMANAN PASCA-OTORISASI BERBASIS IDENTITAS MENGGUNAKAN METODE RULE-BASED EVENT-CONDITION-ACTION PADA JARINGAN OVERLAY WIREGUARD DI PT EBDESK TEKNOLOGI

Nama	:	Febby Syahrul Fahrurodzi
NIM	:	2211510660
Dosen Pembimbing	:	Joko Christian Chandra, S.Kom., M.Kom.

Berdasarkan penilaian pada Presentasi + Demo, Penulisan, Penguasaan Materi, Penguasaan Program maka Mahasiswa tersebut di atas dinyatakan:

LULUS

dengan nilai angka : **86** huruf : **A**

Mahasiswa tersebut di atas wajib menyerahkan hasil perbaikan tulisan Tugas Akhir dalam bentuk terjilid sesuai dengan Panduan Perbaikan Tugas Akhir, selambat-lambatnya Kamis 30 Juli 2026.

Panitia Penguji:

1	Ketua	Painem, S.Kom., M.Kom.
2	Anggota	Dr. Mohammad Syafrullah, M.Kom, M.Sc.
3	Moderator	Joko Christian Chandra, S.Kom., M.Kom.

Keterangan:
Nilai Huruf: A:85-100 A-:80-84,99 B+:75-79,99 B:70-74,99 B-:65-69,99 C:60-64,99 D:40-59,99 E-:0-39,99

UNIVERSITAS BUDI LUHUR
FAKULTAS TEKNOLOGI INFORMASI

Kartu Bimbingan Tugas Akhir

NIM: 2211510660
Nama: Febby Syahrul Fahrurodzi
Pembimbing: Joko Christian Chandra, S.Kom., M.Kom.

No.	Tanggal	Materi
1	16-04-2026	diskusi terkait tema pengembangan sistem monitoring dan self healing network menggunakan rule based pada jaringan komputer korp
2	21-04-2026	pergantian tema menjadi implementasi mekanisme OCA untuk keamanan jaringan
3	07-05-2026	Draft bab 1 dan bab 2, arahan perbaikan penulisan rumusan masalah dan komponen yang kurang pada bab 2
4	19-05-2026	Perbaikan bab 1 dan 2. Draft bab 3
5	08-06-2026	Demo sistem awal di lab, perbaikan penulisan bab 3
6	11-06-2026	Draft bab 4, perbaikan penulisan bab 3
7	25-06-2026	perbaikan penulisan bab 4, demo perbaikan
8	02-07-2026	bab 5

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama	: Febby Syahrul Fahrurodzi
Nomor Induk Mahasiswa	: 2211510660
Program Studi	: Teknik Informatika
Bidang Peminatan	: Cyber Security
Jenjang Studi	: Strata 1
Judul	: IMPLEMENTASI PEMANTAUAN KEAMANAN PASCA-OTORISASI BERBASIS IDENTITAS MENGGUNAKAN METODE RULE-BASED EVENT-CONDITION-ACTION PADA JARINGAN OVERLAY WIREGUARD DI PT EBDESK TEKNOLOGI

Laporan Tugas Akhir ini telah disetujui, disahkan dan direkam secara elektronik sehingga tidak memerlukan tanda tangan tim penguji.

Jakarta, Kamis 16 Juli 2026

Tim Penguji:

Ketua	: Painem, S.Kom., M.Kom.
Anggota	: Dr. Mohammad Syafrullah, M.Kom, M.Sc.
Pembimbing	: Joko Christian Chandra, S.Kom., M.Kom.
Ketua Program Studi	: Dr. Indra, S.Kom., M.T.I.

IMPLEMENTASI PEMANTAUAN KEAMANAN PASCA-OTORISASI BERBASIS IDENTITAS MENGGUNAKAN METODE RULE-BASED EVENT-CONDITION-ACTION PADA JARINGAN OVERLAY WIREGUARD DI PT EBDESK TEKNOLOGI

TUGAS AKHIR

Oleh:

FEBBY SYAHRUL FAHRURODZI

NIM: 2211510660

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS BUDI LUHUR

JAKARTA

2026

ABSTRAK

IMPLEMENTASI PEMANTAUAN KEAMANAN PASCA-OTORISASI BERBASIS IDENTITAS MENGGUNAKAN METODE RULE-BASED EVENT-CONDITION-ACTION PADA JARINGAN OVERLAY WIREGUARD DI PT EBDESK TEKNOLOGI

Oleh: Febby Syahrul Fahrurodzi (2211510660)

PT eBdesk Teknologi memanfaatkan jaringan overlay WireGuard melalui NetBird untuk mengamankan komunikasi antar-perangkat di lingkungan kerjanya. Namun, kendali akses pada jaringan tersebut hanya berlaku pada tahap awal saat perangkat diberi izin masuk, sedangkan aktivitas pengguna setelah izin diberikan tidak lagi terpantau karena seluruh lalu lintas berjalan dalam keadaan terenkripsi. Kondisi ini menimbulkan celah keamanan, di mana penyalahgunaan hak akses, percobaan pembobolan kata sandi, maupun pemindaian jaringan internal sulit dideteksi, terlebih pemantauan yang hanya berbasis alamat IP tidak mampu mengenali siapa pelaku sebenarnya di balik suatu aktivitas. Penelitian ini bertujuan membangun sistem pemantauan keamanan pasca-otorisasi berbasis identitas. Metode yang diusulkan terdiri atas dua bagian, yaitu metode pengembangan sistem menggunakan model Prototyping dan metode deteksi menggunakan algoritme rule-based Event-Condition-Action (ECA) yang bekerja tanpa machine learning sehingga setiap keputusan dapat ditelusuri. Lalu lintas pada jaringan overlay ditangkap dan diperkaya dengan identitas serta peran setiap pengguna, kemudian diperiksa terhadap sekumpulan aturan deteksi yang meliputi pelanggaran hak akses berbasis identitas sebagai kontribusi utama, percobaan brute force, dan port scan dengan ambang yang bersumber dari jurnal ilmiah. Setiap pelanggaran perilaku ditindaklanjuti secara otomatis melalui pencabutan izin akses pengguna, sementara seluruh peristiwa dan peringatan direkam menggunakan Elasticsearch dan disajikan pada sebuah dasbor pemantauan berbasis web. Penelitian ini menghasilkan sistem yang mampu membedakan aktivitas yang sah dan yang menyimpang berdasarkan identitas penggunanya serta menanganinya secara otomatis dan *real-time*. Pengujian dilakukan menggunakan metode pengujian fungsional pada dua kampanye terkontrol, yang menjalankan 79 percobaan berupa 33 percobaan serangan dan 46 percobaan akses sah sebagai pembanding. Hasilnya, seluruh 33 percobaan serangan (9 percobaan brute force, 8 percobaan port scan, dan 16 percobaan pelanggaran hak akses) berhasil dideteksi dengan tepat, sementara 46 percobaan akses sah tidak menghasilkan satu pun peringatan keliru. Lalu lintas yang identik menghasilkan keputusan berbeda sesuai peran penggunanya, dan pencabutan otorisasi berlangsung otomatis dengan rata-rata waktu deteksi 0,613 detik dan waktu respons 0,749 detik sehingga rentang paparan rata-rata hanya 1,361 detik. Hasil ini menunjukkan pendekatan berbasis identitas efektif menutup celah pemantauan pasca-otorisasi.

Kata kunci: Pemantauan pasca-otorisasi, Event-Condition-Action, WireGuard, NetBird, keamanan berbasis identitas

DAFTAR ISI

DAFTAR PUSTAKA

Afzal, R., & Murugesan, R. K. (2022). Rule-Based Anomaly Detection Model with *Stateful* Correlation Enhancing Mobile Network Security. Intelligent Automation & Soft Computing.

Alhamri, R. Z., Eliyen, K., & Heriadi, A. (2022). Pemanfaatan API Client Berbasis Python untuk Konfigurasi IPS pada Router MikroTik. *Jurnal Teknik Ilmu dan Aplikasi (JTIA)*, 3(2), 162–172. https://doi.org/10.33795/jtia.v3i1.110

Alsharabi, N., Bhardwaj, A., Alshammari, T. S., Alotaibi, S., Alshammari, D., & Jadi, A. (2025). Threat Hunting the Shadows: Detecting Adversary Lateral Movement with Elasticsearch. *IEEE Access*, 13.

Apache Kafka. (n.d.). *Apache Kafka Documentation: Use Cases*. Diakses 21 Juni 2026, dari https://kafka.apache.org/

Attar Bashi, Z. S. M., & Senan, S. (2025). A Comprehensive Review of Zero Trust Network Architecture (ZTNA) and Deployment Frameworks. *International Journal on Perceptive and Cognitive Computing (IJPCC)*, 11(1).

Bjarnason, E., Lang, F., & Mjöberg, A. (2023). An empirically based model of software prototyping: a mapping study and a multi-case study. *Empirical Software Engineering*, 28(5), 115.

Breve, B., Cimino, G., & Deufemia, V. (2022). Towards Explainable Security for ECA Rules. *CEUR Workshop Proceedings (EMPATHY 2022)*.

Christanto, F. W., Cholillah, P., & Hirzan, A. M. (2025). Optimizing Mikrotik-Based Network Security using Address List, Firewall Filter Rules, and Raw Firewall. *Revista de Informática Teórica e Aplicada (RITA)*, 32(3).

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2). National Institute of Standards and Technology.

Desolda, G., Greco, F., Zancanaro, M., & Costabile, M. F. (2021). Extending Task Automation Systems with Event-State-Condition-Action Capabilities. *CEUR Workshop Proceedings*.

Djuitcheu, H., Sergeev, A., Alam, K., Santhosh, D., Autenrieth, A., & Seitz, J. (2025). Lightweight Security for Private Networks: Real-World Evaluation of WireGuard. Dalam 2025 IEEE 103rd Vehicular Technology Conference (VTC2026-Spring). Nice, Prancis: IEEE.

Elastic. (n.d.). *Elasticsearch: Get Started*. Diakses 21 Juni 2026, dari https://www.elastic.co/docs/get-started

George, A. S. (2025). The Critical Role of Micro-segmentation in Modern Cybersecurity Architectures: A Comprehensive Review. *Partners Universal Multidisciplinary Research Journal (PUMRJ)*, 2(2).

Henge, S. K., Upadhyay, A., Saini, A. K., Mishra, N., Sharma, D., & Sharma, G. (2023). Analysis and detection of insider attacks using behaviour rule based architecture in enterprise multitenancy. *Journal of Discrete Mathematical Sciences & Cryptography*, 26(3), 707–718.

Henriques, J., Caldeira, F., Cruz, T., & Simões, P. (2022). An automated closed-loop framework to enforce security policies from anomaly detection. *Computers & Security*, 123, 102949.

Hussein, S. G., & Rehman, S. M. F. U. (2025). Protocol Efficiency and Resource Utilization in VPN Technologies: A Comparative Analysis of OpenVPN and WireGuard. *Journal of Techniques*, 7(4), 37–42.

Kjorveziroski, V., Bernad, C., Gilly, K., & Filiposka, S. (2024). Full-mesh VPN performance evaluation for a secure edge-cloud continuum. *Software: Practice and Experience*, 54(8).

Kusnanto, Y., Nugroho, M. A., & Kartadie, R. (2024). Implementasi Zero Trust Architecture untuk Meningkatkan Keamanan Jaringan: Pendekatan Berbasis Simulasi. *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, 9(4), 2357–2364.

Lafourcade, P., Mahmoud, D., Ruhault, S., & Lonjon, B. (2024). A Unified Symbolic Analysis of WireGuard. *Network and Distributed System Security Symposium (NDSS)*.

Mushtaq, M. M. (2025). A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains. *Sensors*, 25(19), 6118.

NetBird. (n.d.). *NetBird Documentation*. Diakses 24 Juni 2026, dari https://docs.netbird.io/

Pratama, F. I., Subroto, E. M. N., Haira, R. M., & Yaqin, M. A. (2023). Pengujian Black Box pada Aplikasi E-Commerce OpenCart dengan Metode Equivalence Partitioning dan Boundary Value Analysis. *Jurnal Ilmiah Informatika (JIMI)*, 8(1), 54-64.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology.

Simbolon, A. B., Kiswanto, D., Siregar, D., & Lumban Gaol, A. S. (2025). Rancang Bangun Sistem Analisis Log Jaringan Berbasis Web untuk Deteksi Real-Time Ancaman Canggih dan Gerakan Lateral. *JITET (Jurnal Informatika dan Teknik Elektro Terapan)*, 14(1).

Smiliotopoulos, C., Kambourakis, G., & Kolias, C. (2024). Detecting lateral movement: A systematic survey. *Heliyon*, 10(4), e26317.

Sui, Z., Shu, H., Kang, F., Huang, Y., & Huo, G. (2023). A Comprehensive Review of Tunnel Detection on Multilayer Protocols: From Traditional to Machine Learning Approaches. *Applied Sciences*, 13.

Teuwen, K. T. W., Mulders, T., Zambon, E., & Allodi, L. (2025). Ruling the Unruly: Designing Effective, Low-Noise Network Intrusion Detection Rules for Security Operations Centers. *Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIA CCS)*.

Truong, H. T. T., Le, H. D., Nguyen, H.-T., & Luong, N. T. (2024). Routing Protocol against Flooding Attack Using Median Value and Fixed Threshold. *Journal of Communications*, 19(6), 298–307.

Wang, Z., Liu, D., Sun, Y., Pang, X., Sun, P., Lin, F., Lui, J. C. S., & Ren, K. (2022). A Survey on IoT-enabled Home Automation Systems: Attacks and Defenses. *IEEE Communications Surveys & Tutorials*.