Abstrak—Serangan siber terhadap platform digital terus meningkat, baik dari sisi frekuensi maupun tingkat kecanggihan, yang berdampak signifikan pada website pelaporan konten digital Indonesia yang menangani data pengguna sensitif. Penelitian ini mengusulkan metode implementasi firewall dengan penerapan multi-level microsegmentation untuk meningkatkan proteksi server pada platform pelaporan konten digital, sekaligus menjawab tantangan trade-off antara keamanan dan performa dalam infrastruktur digital Indonesia. Metode yang diusulkan dievaluasi menggunakan konfigurasi jaringan komparatif, dimana satu konfigurasi menerapkan metode yang diusulkan – multi-level microsegmentation, sementara konfigurasi lainnya tidak menggunakan segmentasi apapun. Efektivitas keamanan dan performa sistem diukur melalui pengujian laboratorium terkontrol selama lima jam per skenario. Temuan menunjukkan bahwa konfigurasi microsegmented berhasil mencapai peningkatan empat kali lipat dalam mitigasi ancaman internal, dengan tingkat keberhasilan 51% dalam memblokir serangan, dibandingkan dengan tingkat keberhasilan 12% pada skenario non-segmented. Namun demikian, peningkatan keamanan ini menimbulkan overhead performa berupa kenaikan latency (52,7%), jitter (36,7%), dan packet loss (283,2%), serta penurunan throughput sebesar 9,5%. Penelitian ini memberikan kontribusi berupa pendekatan baru dalam penerapan teknik microsegmentation untuk aplikasi web pengguna terotorisasi dalam konteks Indonesia. Pendekatan ini menyediakan kerangka strategis untuk menyeimbangkan keamanan yang robust dengan aksesibilitas platform pada sistem pelaporan konten digital.