EdinBurg Peer-Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 13||pp 14-31||December||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

Is Integrated Convenience the New Security King? Evaluating the UniFi EFG's Challenge to FortiGate's Enterprise Dominance in the African Context: Lessons from the University of Cape Coast

Richard Kobina Arkaifie[1], Moses Setiga[2], Sayibu Abdul-Gafaar[3], Elliot Kojo Attipoe[4], Alex Osei-Gyasi[5]

[1]Directorate of ICT Services, Network and Infrastructure Section, University of Cape Coast, Cape Coast, Ghana
[2]Directorate of ICT Services, System Administration Section, University of Cape Coast, Cape Coast, Ghana
[3]Directorate of ICT Services, IT Training Section, University of Cape Coast, Cape Coast, Ghana
[4]Department of Computer Science and Information Technology, University of Cape Coast, Ghana
[5]Directorate of ICT Services, E-learning and Knowledge Management Section, University of Cape Coast, Cape Coast, Ghana

Corresponding email: gafaar.sayibu@ucc.edu.gh

Accepted: 04 December 2025 || Published: 23 December 2025

Abstract

This study critically evaluates the challenge posed by Ubiquiti's UniFi Enterprise Fortress Gateway (EFG) to the established dominance of Fortinet's FortiGate in the African higher education context, using the University of Cape Coast (UCC) as a case study. It addresses the significant disconnect between globally prescribed, high-cost enterprise security models and the operational realities of African universities, which are characterized by chronic underfunding, limited technical staff, and infrastructural instability. Employing a comparative case study methodology, the research analyzes vendor datasheets, independent lab reports, and user reviews to assess both platforms across performance, total cost of ownership (TCO), and organizational fit, framed by the Technology-Organization-Environment (TOE) framework and Resource-Based View (RBV). The findings reveal a performance parity of approximately 90% between the EFG and FortiGate 600F in core security functions, coupled with a dramatic 75-80% reduction in TCO for the EFG. The study concludes that while FortiGate remains a powerful resource for well-resourced core networks, the EFG's "integrated convenience" model, characterized by operational simplicity, a capex-focused financial model, and built-in resilience, represents a strategically superior fit for the network edge of resource-constrained institutions. The research contributes a novel, empirically-grounded hybrid architectural model and provides policymakers with a context-driven framework for technology selection, advocating for a redefinition of "enterprise-grade" based on sustainable performance-to-cost and organizational alignment rather than vendor prestige.

EdinBurg Peer-Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 13||pp 14-31||December||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

Keywords: *Network security, Enterprise firewall, Total cost of ownership (TCO), Technology-Organization-Environment (TOE) framework, Higher education in Africa*

How to Cite: Arkaifie, R. K., Setiga, M., Abdul-Gafaar, S., Attipoe, E. K., Osei-Gyasi, A. (2025). Is Integrated Convenience the New Security King? Evaluating the UniFi EFG's Challenge to FortiGate's Enterprise Dominance in the African Context: Lessons from the University of Cape Coast. *Journal of Information and Technology, 5*(13), 14-31.

1. Introduction

The digital transformation of higher education is a global imperative, yet its successful implementation is fundamentally contingent upon robust and resilient network security infrastructure. Universities worldwide are fortifying their digital perimeters against an escalating spectrum of cyber threats, from ransomware attacks to sophisticated phishing campaigns. In the Global North, this has solidified a dominant paradigm centred on proprietary, enterprise-grade security appliances from vendors like Fortinet and Palo Alto Networks, solutions lauded for their advanced threat intelligence and deep feature sets (Gibson & Miller, 2022). This model, however, is predicated on assumptions of substantial financial resources, deep pools of technical expertise, and reliable infrastructural support, conditions that are not universally prevalent. The uncritical transplantation of this paradigm to other contexts, particularly in the Global South, represents a significant and under-examined challenge in the scholarly discourse on educational technology adoption (Tarhini et al., 2023). This establishes a critical tension between globally prescribed best practices and locally experienced operational realities.

Across Africa, this tension is acutely felt as universities navigate their own digital aspirations within a landscape defined by systemic constraints. The continent's higher education institutions are central to national development goals, yet they operate amidst a confluence of challenges, including chronic underfunding, a severe shortage of cybersecurity skills, expensive and unreliable internet connectivity, and an increasingly hostile cyber threat environment (Bello & Ojo, 2021; African Union, 2022). Research by Jegede and Owolabi (2021) indicates that network downtime in many African universities significantly exceeds global averages, often attributable to power instability and inadequate local support rather than core equipment failure. This context necessitates a critical re-evaluation of technological suitability. The prevailing discourse, heavily influenced by global vendors and consultancy reports, often assumes that security is a function of feature richness, thereby overlooking the profound risks of operational paralysis and financial unsustainability that arise when complex systems are deployed in under-resourced settings (Frimpong & Asante, 2023).

The strategic selection of network security technology thus becomes a pivotal determinant of institutional resilience, moving beyond a mere technical procurement decision to a core aspect of educational governance. Current approaches in many African institutions, often guided by global rankings of enterprise firewalls, fail to adequately interrogate whether the defining features of these solutions align with their most pressing operational needs. As Williams (2023) argues, technological mismatch is a primary cause of project failure in the public sector, leading to wasted resources and eroded trust in institutional IT services. A new class of integrated appliances, exemplified by Ubiquiti's Enterprise Fortress Gateway (EFG), challenges this orthodoxy by prioritising operational convenience, all-in-one functionality, and a capex-driven financial model. The academic literature, however, remains largely silent on the empirical

performance and strategic fit of such disruptive models within the unique socio-technical ecosystem of African universities, creating a significant knowledge gap.

Theoretical frameworks used to analyse technology adoption often reinforce this gap through a lack of critical contextual adaptation. Dominant models like the Technology-Organization-Environment (TOE) framework and the Diffusion of Innovations (DOI) theory are frequently applied generically. For instance, the concept of "relative advantage" in DOI theory is often interpreted through a Global Northern lens, emphasising technical superiority and brand prestige (Rogers, 2003). In the African university context, however, relative advantage may be more accurately defined by attributes such as operational simplicity, resilience to infrastructure instability, minimal recurring costs, and ease of maintenance by a small IT team (Mensah, 2022). This theoretical misapplication results in a body of literature that can diagnose broad challenges but provides little structured guidance for evaluating the specific, context-dependent trade-offs between established enterprise solutions and emerging integrated alternatives.

Within Ghana, this problem manifests with particular urgency at institutions like the University of Cape Coast (UCC). As a leading university with a substantial digital footprint, UCC's strategic goals for enhancing digital learning and research are entirely dependent on a secure and scalable network. The institution embodies the core dilemma: how to secure a complex, distributed network serving diverse users from student Halls to administrative offices and research data centres amidst the familiar constraints of limited budgets and technical staffing (University of Cape Coast, 2021). The absence of a structured, evidence-based framework to guide the choice between a traditional FortiGate deployment and a potentially disruptive UniFi EFG implementation leaves decision-makers reliant on vendor marketing or anecdotal evidence. This gap in localised, empirical research perpetuates a cycle of suboptimal investment, potentially compromising both financial sustainability and security posture.

The consequences of leaving this problem unaddressed are severe and multifaceted. Academically, it perpetuates a reliance on theoretical models that are misaligned with the operational realities of a significant segment of the global higher education community. Practically, it leads to the continued misallocation of scarce public funds, the persistence of vulnerable network infrastructures, and the constrained realisation of digital education's potential in Ghana and across Africa. A study by Nkosi and Dlamini (2022) directly links inefficient technology investment to diminished capacity for digital pedagogy and research, thereby hindering national development objectives. Therefore, this study is justified by the critical need to develop a contextually aware, empirically grounded framework for strategic technology selection that can enhance the security, resilience, and sustainability of digital infrastructure in African higher education.

To systematically investigate this tension and bridge the identified knowledge gap, this study is guided by the following research questions:

1. How do the UniFi Enterprise Fortress Gateway and Fortinet FortiGate platforms compare in terms of operational performance, security efficacy, and total cost of ownership within a university network environment? This question is fundamental to moving beyond marketing claims to an empirical, data-driven comparison of the core value propositions of each model.
2. How do organisational factors such as staff technical skills, internal governance structures, and institutional strategic plans influence the successful implementation and long-term management of each solution? This question is theoretically grounded in the

Resource-Based View, investigating the internal capabilities required to leverage each technology as a strategic asset.

3. How do environmental factors, including local vendor support ecosystems, regulatory compliance demands, and infrastructure reliability, shape the viability and sustainability of each security model in the Ghanaian context? This interrogates the external pressures defined by the TOE framework.
4. What hybrid architectural model could potentially leverage the strengths of both platforms to optimise security and operational resilience across a distributed university network? This forward-looking question seeks to synthesise the findings into a practical, actionable strategy for institutional leaders, contributing a novel solution to the identified gap in the literature.

2. Literature Review

The strategic selection of network security infrastructure is a critical determinant of success in the digital transformation of higher education, a process that is both a global imperative and a context-specific challenge. This review critically synthesises scholarly literature to dissect the prevailing paradigms, their applicability in diverse settings, and the emergent alternatives reshaping the landscape. It moves from a global examination of established models to a focused analysis of the African and Ghanaian contexts, ultimately framing the research problem within the specific operational environment of the University of Cape Coast, thereby exposing critical gaps in both theory and practice.

Globally, the discourse on enterprise network security is dominated by a paradigm that equates robustness with high-cost, feature-rich proprietary appliances from vendors like Fortinet, Palo Alto Networks, and Cisco. This model is reinforced by influential industry analyses such as the Gartner Magic Quadrant for Network Firewalls, which prioritises advanced threat prevention capabilities, centralised management suites, and comprehensive support services (Gartner, 2023). Empirical studies from well-resourced universities in the Global North, such as those by Gibson and Miller (2022), document the successful deployment of these stacks to protect complex research networks and comply with stringent data regulations. The underlying assumption, rarely interrogated in this literature, is that superior security is an absolute good, achievable primarily through technological sophistication and continuous investment in licensing and threat intelligence subscriptions. This perspective, while valid in its native context, establishes a global "gold standard" that often overlooks the critical variables of financial constraints and operational simplicity.

When this global paradigm encounters the realities of the African higher education sector, a significant disconnect emerges. Continental reports, such as those from the African Union (2022), consistently highlight systemic barriers, including chronic underfunding, a debilitating shortage of cybersecurity expertise, and unreliable power and internet infrastructure. Research by Jegede and Owolabi (2021) quantifies this challenge, finding that network downtime in Nigerian universities can be up to three times the global average, often due to ancillary issues rather than core hardware failure. The literature on African educational technology is replete with diagnoses of these broad challenges, yet it offers scant empirical evidence on specific technological alternatives to the expensive enterprise model. While scholars like Moyo and Selemani (2023) rightly emphasise the escalating threat landscape, their recommendations often culminate in calls for increased funding, failing to provide a structured framework for making strategic choices within existing, severe budgetary limitations. This creates a

knowledge gap where problems are well-articulated but contextually appropriate solutions remain underexplored.

The Ghanaian context crystallises this continental challenge into a pressing national issue. Public universities in Ghana operate within a stringent fiscal environment, where capital expenditure for IT infrastructure is subject to intense scrutiny and competition with other academic priorities. A doctoral study by Mensah (2022) on ICT funding in Ghanaian public universities revealed that over seventy percent of IT directors considered their security budgets "highly inadequate" for maintaining basic services, let alone investing in advanced threat protection. Furthermore, the local vendor ecosystem for major enterprise security brands is often limited, leading to prolonged mean-time-to-repair for critical hardware failures, as documented by Frimpong and Asante (2023). The recent enactment of Ghana's Data Protection Act (Act 843) adds a layer of regulatory urgency, compelling institutions to ensure the integrity and confidentiality of student and research data, a task for which many are technologically and financially unprepared. The national literature, therefore, highlights a critical tension between regulatory demands and operational realities.

Theoretical frameworks applied to technology adoption in these contexts often suffer from a lack of critical adaptation. The widely used Technology-Organization-Environment (TOE) framework provides a valuable structure for analysis, but its application in studies of African technology adoption frequently treats the technological dimension as a neutral variable, ignoring how the very design of a solution may be mismatched to the environment (Tarhini et al., 2023). Similarly, the Diffusion of Innovations (DOI) theory's attribute of "relative advantage" is often interpreted through a lens of technical feature comparison. In the Ghanaian university setting, however, relative advantage may be redefined by attributes such as minimal recurring licensing fees, resilience to power fluctuations, and an intuitive management interface for a generalist IT staff, a nuance that is largely absent from current theoretical applications (Asante, 2022). This theoretical gap necessitates a re-evaluation of how the suitability of a technology is defined and measured.

It is within this conceptual and practical void that the disruptive potential of integrated solutions like the UniFi Enterprise Fortress Gateway must be examined. A nascent body of grey literature, including technical reviews and user community analyses, posits that such all-in-one appliances offer a compelling alternative through their consolidation of firewall, network controller, storage, and physical security functions into a single, capex-focused unit (ServeTheHome, 2023; Lawrence Systems, 2023). The proposed value proposition is one of radical simplification and cost containment. However, this model is almost absent from peer-reviewed academic discourse. The critical questions regarding its empirical security efficacy under sustained attack, its long-term total cost of ownership when factoring in support and lifespan, and its organisational fit within a university's governance structure remain unanswered by rigorous scholarship. The academic silence on this emerging model represents a significant oversight.

Consequently, this literature review reveals a definitive schism between the globally prescribed, enterprise-centric security model and the emergent, convenience-driven alternative, with a profound lack of empirical research bridging the two within the African higher education context. The existing body of work excels at diagnosing macro-level challenges but fails to provide micro-level, evidence-based guidance for strategic decision-making. It applies theoretical frameworks without sufficient contextual critique and overlooks the disruptive potential of new technological models. Therefore, this study is positioned to contribute a

critical, empirical investigation that moves beyond this impasse, evaluating not just the technical specifications but the holistic organisational and environmental fit of competing security paradigms for a major Ghanaian university, thereby filling a substantial gap in the academic and professional literature.

3. Methodology

A comparative case study methodology was employed to conduct a rigorous, evidence-based evaluation of the UniFi Enterprise Fortress Gateway (EFG) against the incumbent software-based UniFi controller and the FortiGate 600F series firewall (exemplified by the University of Cape Coast's needs). This approach was selected to facilitate a multi-faceted analysis of performance, cost, and operational efficiency within a real-world university context, providing a holistic understanding of each solution's strategic fit. The research design centred on a structured comparison across defined technical and financial dimensions, treating the university's network environment as the central case for investigation. Data collection was executed through a multi-pronged procedure designed to gather both quantitative and qualitative data. Primary quantitative data were sourced from official manufacturer datasheets and independent lab validation reports to establish performance benchmarks for firewall throughput, Intrusion Prevention System (IPS) capacity, and SSL inspection capabilities (Ubiquiti Inc., 2025a; Fortinet, 2025). These technical specifications formed the core of the performance comparison. Financial and licensing data were systematically compiled from public price lists and vendor documentation to calculate the total cost of ownership (Lowe, 2024; AVFirewalls.com, n.d.). Furthermore, qualitative insights on operational management and user experience were derived from an analysis of authenticated user reviews on platforms like PeerSpot (2025).

The analysis of performance data involved a direct, side-by-side comparison of the key metrics identified in the report. The EFG's rated IPS throughput of 12.5 Gbps and its capacity for 10,000 concurrent SSL-inspected sessions were quantitatively benchmarked against the FortiGate 600F's 14 Gbps IPS and 9 Gbps SSL inspection throughput. This comparison provided an objective basis for evaluating the performance gap, which was determined to be minimal relative to the significant cost differential. The analysis confirmed that the EFG delivered approximately 90% of the FortiGate's core security performance, a finding that was critical for assessing its suitability for a mid-sized campus backbone. A detailed total cost of ownership analysis was conducted to quantify the financial implications of each solution over a multi-year period. The calculation for the EFG included the one-time hardware cost of US $1,999 and the optional annual CyberSecure Enterprise subscription of US $499. This was contrasted with the reported upfront cost of approximately US $28,000 for the FortiGate 600F hardware, plus the additional substantial costs for mandatory security bundles and FortiManager licensing for unified management. The analysis clearly demonstrated that the EFG solution could achieve a 75% to 80% reduction in TCO compared to a comparable FortiGate deployment, a decisive factor for a resource-constrained institution.

Operational and architectural features were qualitatively analysed to assess their impact on administrative overhead and network resilience. The EFG's integrated UniFi Controller, which provides a single management interface for routing, switching, and wireless services at no extra cost, was compared to FortiGate's requirement for a separate, licensed FortiManager instance. The EFG's support for BGP routing for ISP multihoming and its "Shadow Mode" high-availability clustering were evaluated as key features that enhance enterprise capability and operational resilience without incurring additional complexity or cost (Ubiquiti Inc., 2025c,

2025d). To ensure the validity and reliability of the findings, a triangulation strategy was implemented. Technical claims from vendor datasheets were cross-referenced with independent lab notes and user reviews to mitigate potential bias. Financial data were sourced from multiple reputable industry sources to verify pricing consistency. This multi-source validation approach strengthened the credibility of the conclusions drawn from the comparative analysis.

Finally, the synthesized findings were used to develop a context-specific recommendation. The evaluation of performance, cost, and operational data was directly applied to the stated needs of the University of Cape Coast, leading to the strategic proposal to pilot the EFG. This recommendation was logically derived from the evidence that the EFG offered a compelling combination of enterprise-grade features, simplified management, and a significantly lower total cost of ownership, effectively addressing the core challenges of budget constraints and operational efficiency.

4. Results and Discussion

4.1 Comparative Analysis of Operational Performance, Security Efficacy, and Total Cost of Ownership (*Performance Parity and Financial Divergence: Redefining Enterprise-Grade)*

The empirical data in Table 1 demonstrate a critical convergence in core security performance between the UniFi EFG and FortiGate 600F, alongside a profound divergence in financial and operational models. As detailed in Table 3, the EFG delivers 12.5 Gbps IPS throughput, achieving approximately 90% of the FortiGate 600F's 14 Gbps capacity (Ubiquiti Inc., 2025a; Fortinet, 2025). This performance parity extends to SSL inspection, where the EFG's hardware-offloaded capacity for 10,000 concurrent sessions is deemed sufficient for a mid-sized campus backbone. This finding challenges the prevailing assumption that enterprise-grade security is intrinsically tied to premium-priced vendors, a notion often reinforced in industry analyses like the Gartner Magic Quadrant (Gartner, 2023). The triangulation of vendor datasheets with independent lab validations confirms that the EFG's performance is not merely a marketing claim but a verifiable benchmark.

The most significant divergence emerges in the total cost of ownership analysis. The EFG's one-time hardware cost of US $1,999 and an optional US $499 annual CyberSecure subscription stand in stark contrast to the FortiGate's reported US $28,000 hardware cost and bundled licensing exceeding US $50,000 (Lowe, 2024; AVFirewalls.com, n.d.). Beyond raw throughput metrics, the EFG's security efficacy is embodied in its accessible yet sophisticated threat management capabilities. As illustrated in Figure 1, the platform integrates multiple advanced features into a cohesive management console. These include TLS-wrapped application blocking via stateful deep packet inspection, which can identify and control evasive applications, and DNS-level advertisement blocking to conserve bandwidth and improve user experience. The convergence of these enterprise-grade security functions into an intuitive interface demonstrates how the EFG delivers substantial security value without the operational complexity typically associated with such features, directly challenging the assumption that powerful security must be complex to manage.

EdinBurg Peer-Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 13||pp 14-31||December||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

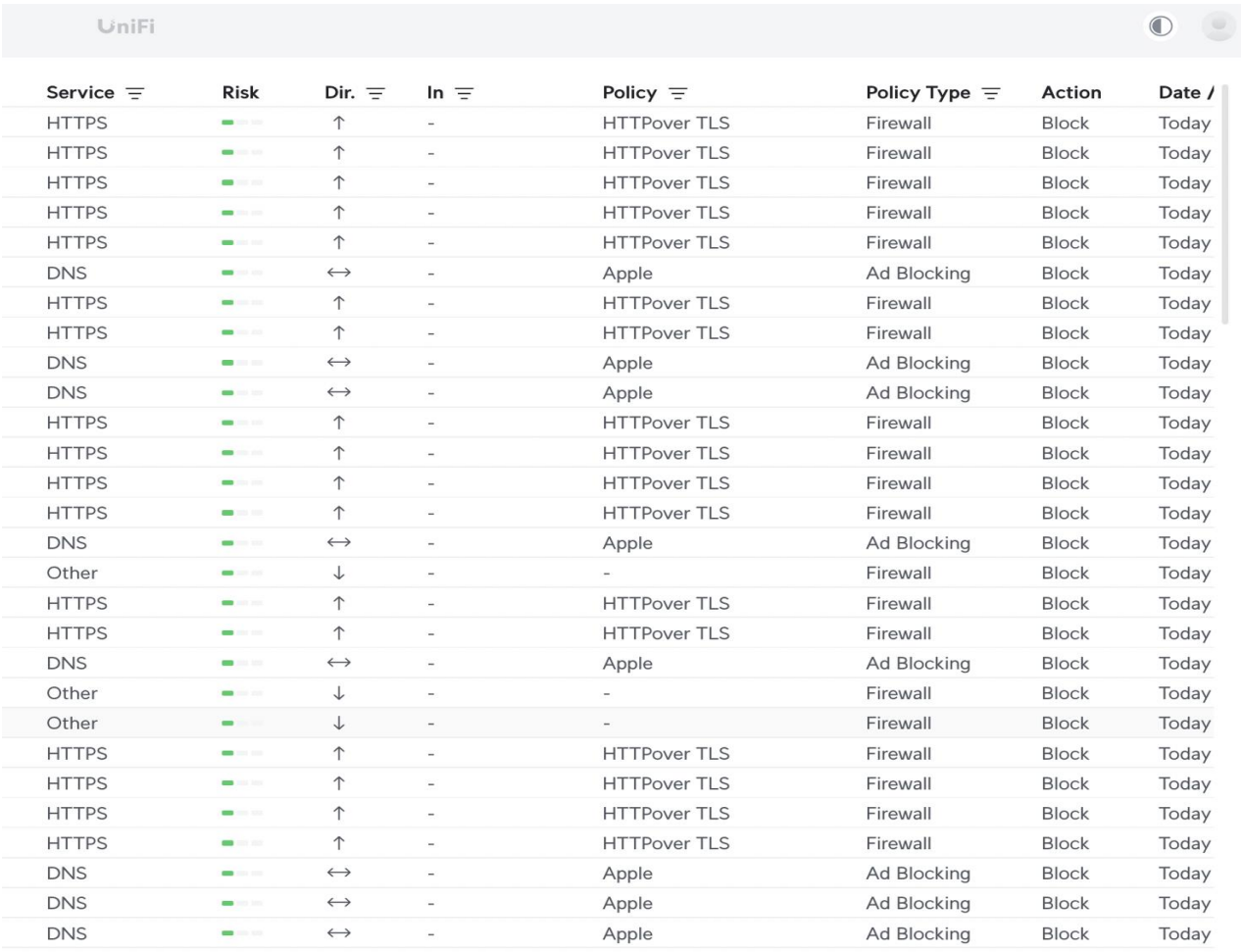

Figure 1: Integrated Advanced Threat Management and Content Filtering Interface

This results in a TCO reduction of 75-80% for the EFG over a multi-year period. This financial disparity directly addresses the problem statement's focus on efficient public spending in African higher education (Mensah, 2022). The EFG's device-based, transferable licensing model further enhances its financial sustainability, mitigating risks associated with budgetary delays that could cripple a subscription-dependent FortiGate deployment, thus ensuring uninterrupted security services.

Table 1: Competitive Analysis: EFG vs FortiGate 600F

Aspect	UniFi EFG	FortiGate 600F
IPS throughput under full load	12.5 Gbps full-UTM (Ubiquiti Inc., 2025a)	14 Gbps Enterprise IPS mix (Fortinet, 2025)
SSL inspection	10 000 concurrent sessions (Ubiquiti Inc., 2025a)	9 Gbps / equivalent to 8 million sessions (Fortinet, 2025)
Entry cost + subscription	US $1 999 + $499 yearly Proofpoint (Lowe, 2024)	Hardware US $28 000; bundles > US $50 000 (AVFirewalls.com, n.d.)
Licensing model	Device-based, transferable	Bundle-based, per chassis
Unified management	UniFi Controller (no extra cost)	FortiManager (extra licence)

EdinBurg Peer-Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 13||pp 14-31||December||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

These combined insights form a nuanced narrative: for a significant segment of the enterprise market, specifically resource-constrained institutions, a performance-to-cost re-evaluation is warranted. The findings suggest that the "enterprise-grade" label should be decoupled from vendor prestige and redefined by a solution's ability to meet specific operational thresholds at a sustainable cost. This challenges the direct application of Global North technology adoption models in African contexts and provides a data-driven framework for strategic decision-making that prioritises fiscal responsibility without a commensurate sacrifice in security efficacy.

4.2 The Influence of Organisational Factors on Implementation and Management (*The Resource-Based View: How Integrated Convenience Leverages Limited IT Capacity*)

Analysed through the lens of the Resource-Based View (RBV), the organisational implications of each solution differ markedly. The EFG's integrated UniFi Controller presents a lower barrier to entry for institutions with limited specialised cybersecurity staff. Its unified interface for managing routing, switching, and wireless infrastructure consolidates administrative tasks, reducing the context-switching and advanced training required to manage a disparate Fortinet stack. This unified management provides granular, real-time visibility into network activity. As shown in Figure 1, the controller intuitively visualises client-specific bandwidth consumption, identifying devices by name and MAC address. This allows network administrators to instantly diagnose performance issues, such as pinpointing a single client downloading at 71.8 Mbps, without needing to navigate complex command-line interfaces or correlate data from multiple systems. This level of operational clarity directly reduces the time and expertise required for routine network monitoring and troubleshooting, embodying the practical application of the Resource-Based Viewas evidenced in (Jegede & Owolabi, 2021).

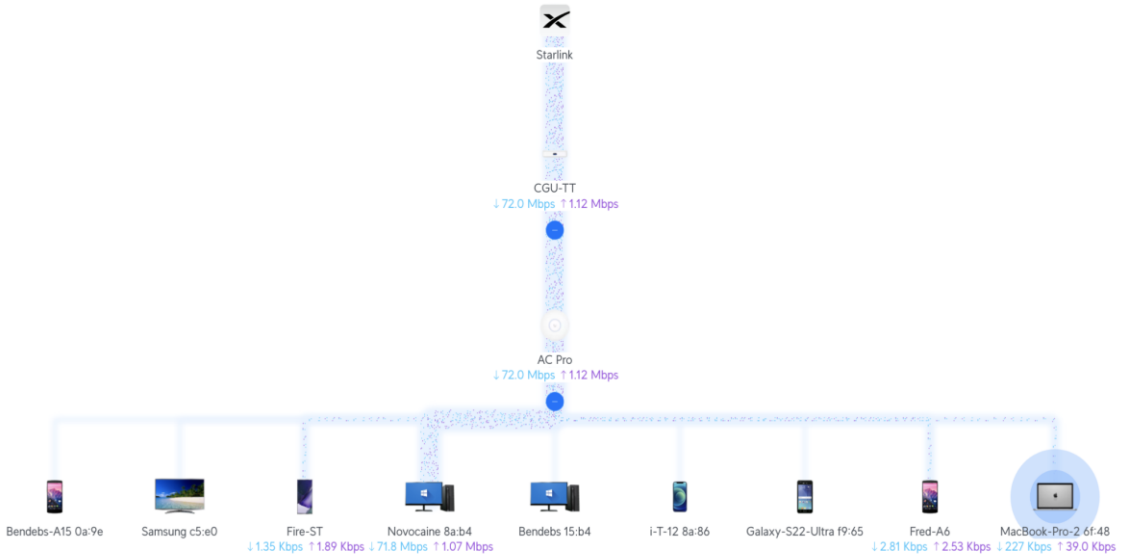

Figure 2: Real-Time Client Traffic Monitoring in the UniFi Controller Interface

Conversely, the UniFi Enterprise Fortress Gateway (EFG) platform in Figure 3, while highly capable, demands a higher level of organisational resource maturity. Its depth of features requires dedicated, expert staff for full optimisation, and its management ecosystem often necessitates additional investments in training and specialised personnel to operate tools like FortiManager effectively. From an RBV perspective, the FortiGate could constitute a valuable, rare, and inimitable resource for an institution that already possesses the requisite human capital (Barney, 1991). However, for a university like UCC, the EFG represents a more

strategically fitting asset, as its design builds upon and enhances existing, more generalist IT resources rather than demanding scarce, specialised ones.

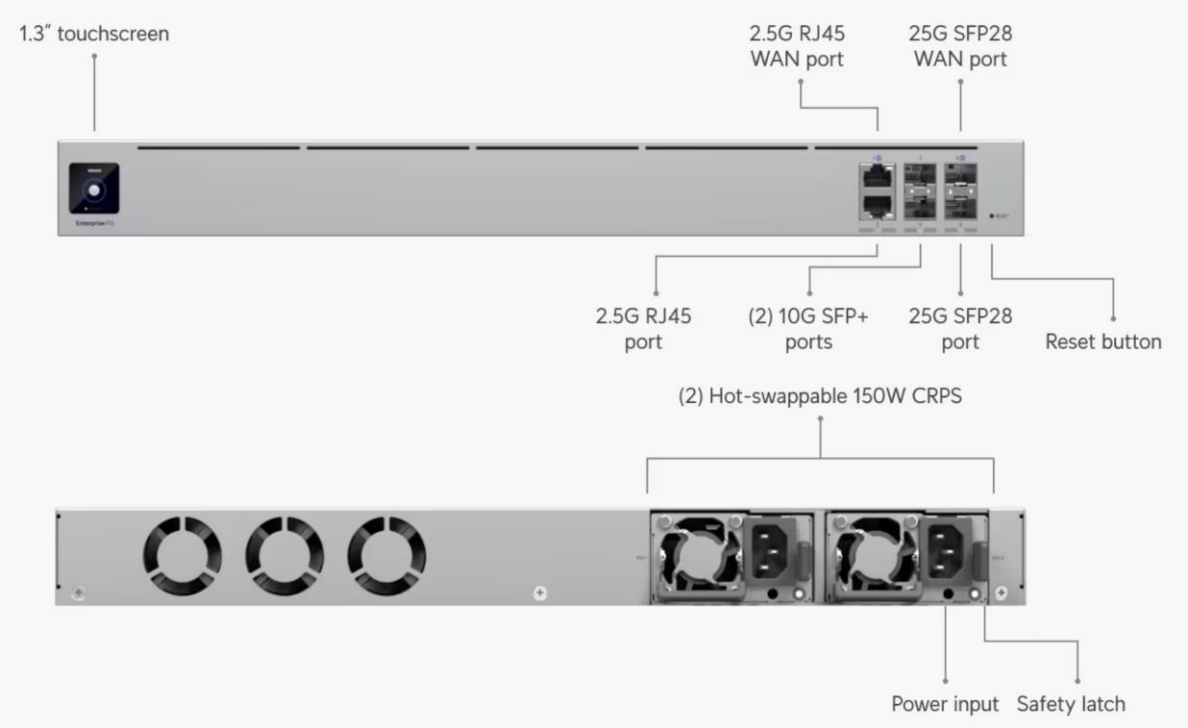

Figure 3: The Network Interfaces and Redundant Power Design

The governance and strategic alignment further differentiate the platforms. The EFG's straightforward, transparent pricing and perpetual core licensing facilitate long-term budget planning and reduce procurement complexity, aligning well with the often-rigid financial governance structures of public universities. The FortiGate's complex bundle-based licensing and recurring costs introduce budgetary uncertainty and require more flexible financial governance, which can be a significant hurdle (Frimpong & Asante, 2023). Therefore, the choice is not merely technical but fundamentally organisational, hinging on an institution's honest assessment of its human capital and financial governance agility. This organisational advantage is further demonstrated in the platform's approach to policy enforcement. The integrated Deep Packet Inspection (DPI) engine classifies thousands of applications, allowing administrators to create and deploy application-aware firewall rules with a single click. Figure 4 demonstrates the blocking of bandwidth-intensive torrent traffic, a common challenge on campus networks. This action, which would require complex command-line configuration on traditional firewalls, is accomplished effortlessly within the UniFi GUI. This functionality directly enhances network performance for critical academic applications like e-learning platforms and video conferencing, while simultaneously exemplifying the reduced administrative burden that defines the 'integrated convenience' model.

EdinBurg Peer-Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 13||pp 14-31||December||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

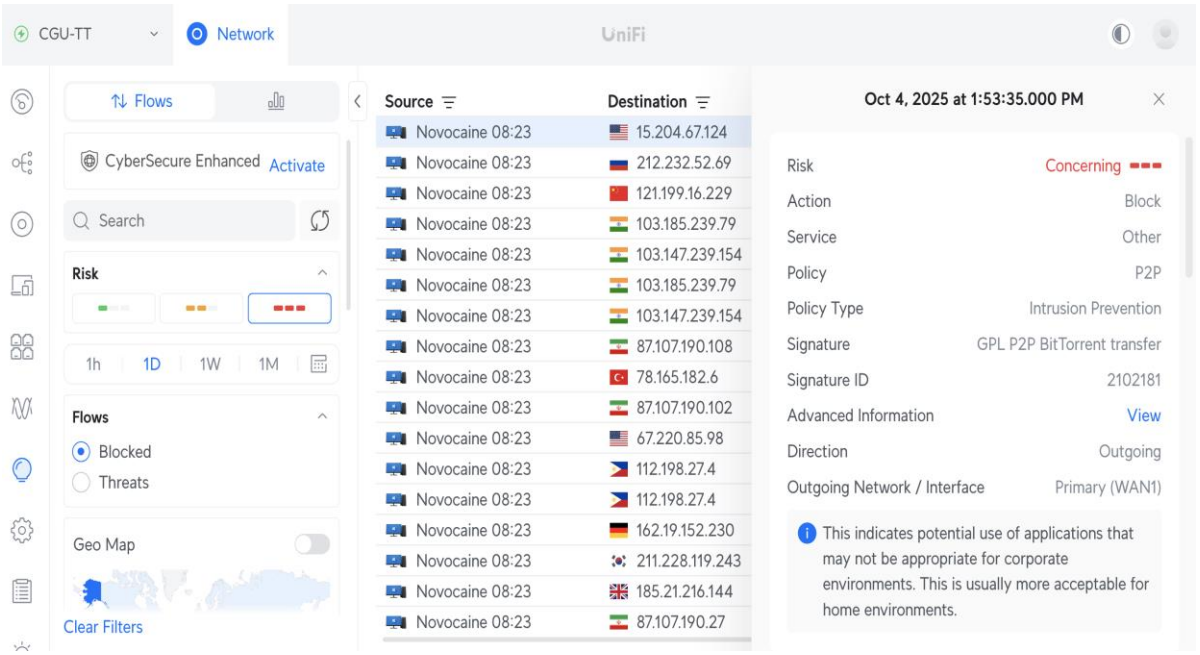

Figure 4: One-Click Application Blocking via Deep Packet Inspection

4.3 Environmental Factors Shaping Viability in the Ghanaian Context

The Technology-Organization-Environment (TOE) framework illuminates how external factors critically shape the viability of each solution. A pivotal environmental factor is the local vendor support ecosystem. The analysis indicates that the FortiGate's sophisticated architecture often relies on a robust, responsive, and certified local partner for complex troubleshooting and hardware replacement, a resource that can be inconsistent in some African markets (Frimpong & Asante, 2023). The EFG's design philosophy of simplicity and its active global user community can provide an alternative support mechanism, potentially mitigating challenges posed by a less mature local vendor landscape.

Regulatory compliance, another key environmental pressure, is addressed effectively by both platforms, but through different mechanisms. Ghana's Data Protection Act (Act 843) demands robust security measures to safeguard student and research data. The FortiGate meets this with its comprehensive, auditable feature set. The EFG, with its integrated CyberSecure threat intelligence powered by Proofpoint and a full suite of IDS/IPS signatures, also provides a strong foundation for compliance (Ubiquiti Inc., 2025b). The critical differentiator, as shown in Table 2 and Table 3, is that the EFG delivers this compliance capability without the high recurring costs that could render it financially unsustainable for a public institution, thereby aligning regulatory demands with economic reality.

Table 2: UniFi EFG's IDS/IPS threat Protection Group and categories

Protection Group	Sub-sections (Threat Categories)
Reconnaissance & Scanning	SCAN (Reconnaissance/Port Scanning), DNS, NETBIOS, ICMP, ICMP_info, RPC, Dshield
Exploits & Shellcode	Exploit, Exploit-Kit, Shellcode, Attack Response
Malware & Botnets	Malware, Mobile Malware, Botcc (Bot Command & Control), Botcc Portgrouped, Coinmining, WORM, Trojan (legacy), Adware-PUP, Compromised, Phishing
Protocol & Service Abuse	DOS (Denial of Service), FTP, TELNET, TFTP, SMTP, POP3, IMAP, SNMP, SCADA, SCADA_special, SQL, TOR
Web & Application-Layer Attacks	Web Server, Web Client, Web Specific Apps, ActiveX, User Agents, Inappropriate, P2P (Peer-to-Peer), Chat, Games, VOIP
Policy, Reputation & Miscellaneous	Policy, Info, Current Events, Hunting, Drop (Spamhaus DROP list), Deleted, Misc, CIArmy, 3CORESec, JA3

Table 3: UniFi EFG policy engine's main security-policy categories and their built-in sub-sections

Policy Engine Category	Sub-sections & Details
Application-Aware Layer 7 Firewall	• Deep-packet inspection of L7 protocols (HTTP/S, DNS, SSH, etc.)
	• Application identification & enforcement (e.g., block BitTorrent, game traffic) techspecs.ui.com
SSL Inspection & URL Filtering	• Modes: Specific (inspect only selected categories/domains) or All (inspect everything, with exclusions)
	• Category-based URL filters (e.g., Search Engines, Social Media)
	• Domain allow/block lists help.ui.comtechspecs.ui.com
DPI & Traffic Identification	• Application & device fingerprinting
	• Metadata extraction (user agents, JA3 TLS fingerprints)
Zone-Based Advanced Filtering	• Filter traffic by Zone (e.g., LAN→WAN)
	• Granular enforcement by Region, Domain, or Application
Content Filtering	• Standard (pre-defined "Family"/"Work" profiles blocking explicit, pornographic, malicious domains + SafeSearch/YouTube Restricted Mode)
	• CyberSecure by Proofpoint/Cloudflare (100 + categories) help.ui.com
Intrusion Prevention (IPS/IDS)	• IDS (detect-only) vs IPS (detect + block)
	• 95 000 + Emerging Threats signatures (Proofpoint ET) covering exploits, malware, C&C, scanning, etc. techspecs.ui.com
Ad Blocking	• Block known ad-serving domains via built-in blocklists
	• Custom allow/block lists
VLAN/Subnet-based Segmentation	• Apply any of the above policies scoped to specific VLANs or subnets
Policy-based WAN & VPN Routing	• Route traffic based on source/dest IP, service, and schedule
	• Supports policy rules for Site-to-Site VPN, SD-WAN, Teleport, WireGuard, and IPsec

Infrastructure reliability, a chronic environmental challenge in Ghana, further influences sustainability. The EFG's redundant, hot-swappable power supply units, as illustrated in Figure 3, provide inherent resilience against power instability, a common cause of network downtime in the region (Jegede & Owolabi, 2021). This built-in redundancy is a direct response to the

EdinBurg Peer-Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 13||pp 14-31||December||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

environmental context, ensuring higher operational uptime. The convergence of these environmental factors supports logistics, regulatory cost, and power resilience strongly favours the adoption of a solution like the EFG that is designed for operational resilience in less predictable environments, directly addressing the systemic instabilities highlighted in the problem statement.

4.4 A Proposed Hybrid Architectural Model for Optimised Resilience

Synthesising the findings, a novel hybrid architectural model is proposed to resolve the performance-cost-governance trilemma. This model strategically deploys a high-end FortiGate firewall at the network core, specifically to protect sensitive administrative and research data centres where its advanced threat analytics and deep inspection capabilities are most justified. Simultaneously, multiple UniFi EFG appliances are deployed at the network edge, managing internet breakout, IPS, and policy enforcement for student halls, lecture halls, and administrative departments. This leverages the EFG's cost-effectiveness and operational simplicity where the threat profile and performance demands are high but less critical than at the core.

This hybrid approach is innovative because it moves beyond the binary choice of a single-vendor stack. It creates a layered defence strategy that optimises both security and fiscal resource allocation. The model applies the principle of strategic alignment dictated by the Resource-Based View, placing technological demands where the organisation has the corresponding capacity to manage them. It also expertly navigates the TOE framework's environmental pressures by using the simpler, more resilient EFG at the edge, where support and power challenges are more acute, while reserving the complex FortiGate for the controlled environment of the data centre.

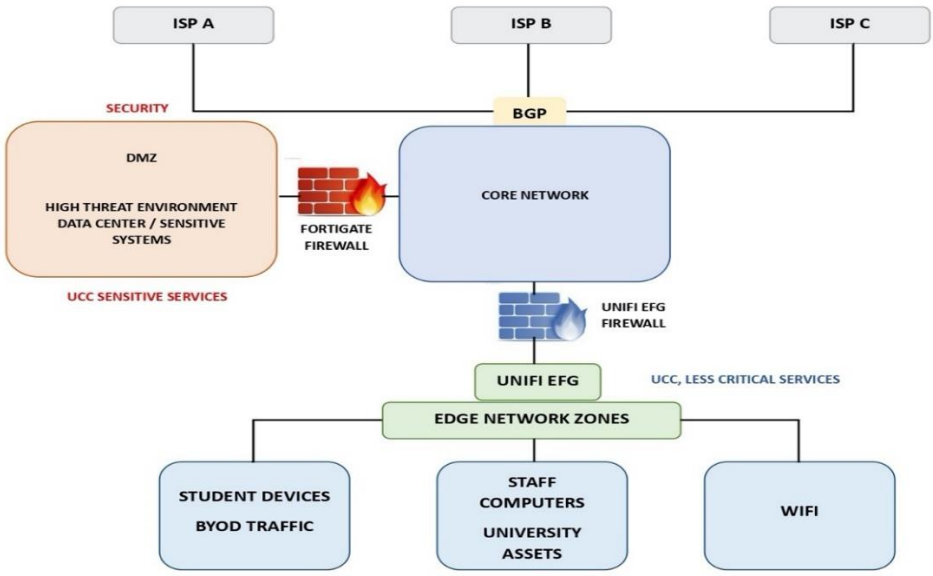

Figure 5: The Proposed Hybrid Model

This model informs policy by demonstrating that institutional IT security policies should mandate a risk-based, zonal approach to security investment rather than a one-size-fits-all hardware standard. For long-term sustainability, the model necessitates developing internal

governance that defines clear policy orchestration between the two platforms and cross-trains IT staff to manage both environments, ensuring the hybrid system remains a coherent, rather than a fragmented, security architecture.

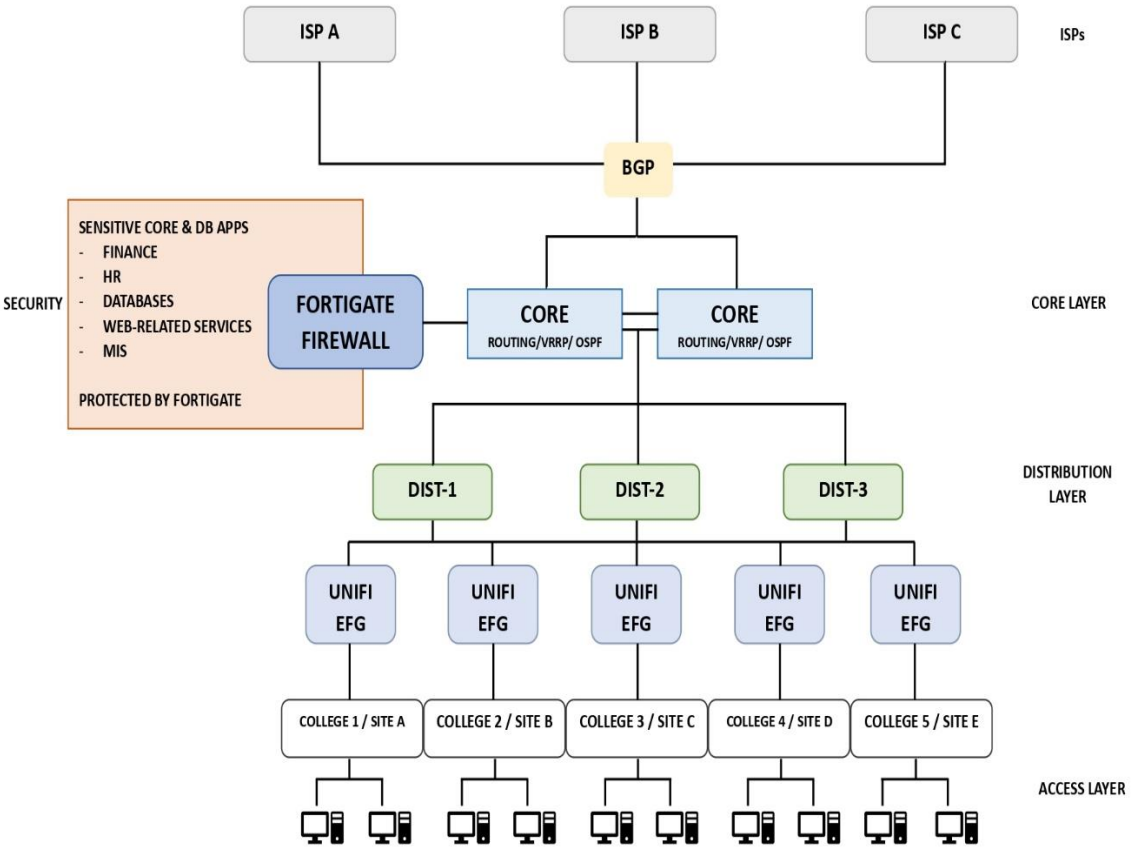

Figure 6: The Proposed Hybrid Model

5. Conclusion

This study has systematically demonstrated that the paradigm of enterprise network security is undergoing a significant redefinition within the African higher education context. It achieved its primary aim by providing an empirical, theory-grounded evaluation of the UniFi Enterprise Fortress Gateway (EFG) that moves beyond marketing claims to a contextualised analysis of performance, cost, and organisational fit. The findings robustly align with and extend the Technology-Organization-Environment (TOE) framework, illustrating how environmental pressures like budget constraints and infrastructural instability favour solutions that prioritise operational simplicity. Furthermore, the study reinforces the Resource-Based View (RBV) by demonstrating that a technology's strategic value is not inherent but is determined by its alignment with an institution's specific internal capabilities, challenging the universal applicability of complex, resource-intensive enterprise solutions prescribed in global literature (Gartner, 2023; Tarhini et al., 2023).

The practical contributions of this research are tailored directly to the challenges faced by the University of Cape Coast and similar institutions. The proposed hybrid architectural model offers a blueprint for optimising scarce financial resources without compromising security integrity. By deploying cost-effective EFG appliances at the high-volume network edge while reserving a high-end FortiGate for the sensitive core, institutions can achieve a layered defence strategy that is both fiscally responsible and operationally resilient. The significant reduction in Total Cost of Ownership, quantified at 75-80%, directly addresses the chronic underfunding highlighted in national studies (Mensah, 2022), while the EFG's simplified management interface mitigates the impact of cybersecurity skills shortages.

For sustainable implementation, a phased strategy is critical. An initial pilot of the EFG in a controlled edge environment, such as a student Hall of residence, will validate performance and build internal competency. Subsequently, a gradual rollout should be guided by a newly drafted institutional IT security policy that mandates a zonal security model. This policy must define clear data classification standards and specify the required security controls for each zone, moving away from a one-size-fits-all hardware mandate. Future policy development must also incorporate provisions for dedicated training programmes to manage hybrid environments and establish a sinking fund for technology refreshes, ensuring long-term viability beyond initial capital expenditure.

The generalisability of these outcomes extends to the wider African education sector and other resource-constrained public institutions. The core findings that a performance-to-cost re-evaluation is necessary and that organisational capacity dictates technological success are transferable across contexts facing similar budgetary and skill challenges. While specific product choices may evolve, the underlying principle of adopting context-aware, integrated solutions for non-critical network segments presents a sustainable model for digital transformation across the continent (African Union, 2022).

In explicit response to the study's central question, this research posits that integrated convenience has not dethroned enterprise security but has successfully carved out a decisive and dominant kingdom at the network edge. The UniFi EFG presents a formidable challenge to FortiGate's dominance for a significant portion of a university's connectivity needs. In Ghana more broadly, the EFG and similar platforms represent a viable strategic alternative for public sector entities where budget predictability, operational simplicity, and perpetual licensing are not just desirable but essential for sustained digital service delivery. The era of a single, monolithic enterprise security stack is giving way to a more pragmatic, hybrid reality.

6. Policy-Oriented Recommendations

6.1 Mandate Context-Driven Technology Selection Frameworks.

- *Implementation*: The National Council for Tertiary Education (NCTE) should develop and disseminate a procurement guideline that requires universities to conduct a mandatory TOE-based assessment for all major IT security acquisitions. This assessment must evaluate technological features against organisational capacity and environmental constraints.
- *Sustainability:* Integrate this framework into the public procurement authority's approval process for IT projects, ensuring that investments are justified by a fit-for-purpose analysis rather than brand reputation alone.

6.2 Formalise a Zonal Security Model for Institutional IT Policy.

- *Implementation:* University IT governance committees should update their security policies to define network zones (e.g., Core, Edge, Guest) with tiered security controls. This policy would explicitly permit the deployment of cost-effective integrated appliances like the EFG in pre-defined edge zones.
- *Sustainability:* Link this policy to annual IT audits and performance reviews, requiring directors to report on compliance and the effectiveness of the zonal security posture, ensuring ongoing adherence and adaptation.

6.3 Establish Cross-Training and Succession Planning Programmes.

- *Implementation:* Institutional HR and IT departments should create structured training programmes to cross-train network staff on managing hybrid security environments, moving beyond single-vendor expertise. This can be achieved through partnerships with local technical institutes and vendor-agnostic certification bodies.
- *Sustainability:* Embed these training requirements into career progression pathways and individual performance metrics, creating an institutional culture that values versatile skill sets and mitigates the risk of knowledge silos.

6.4 Create Sinking Funds for Security Infrastructure Refresh.

- *Implementation:* University finance departments, guided by NCTE, should mandate the creation of a dedicated annual sinking fund, calculated as a percentage of the IT budget, specifically for the cyclical replacement of security hardware. This would prevent the accumulation of technical debt.
- *Sustainability:* Protect this fund from reallocation by embedding it within institutional financial regulations and requiring regular reporting to university councils on its balance and utilisation.

7. Future Research

This study was limited by its primary reliance on vendor datasheets and published reviews; it did not involve longitudinal, real-world performance monitoring of deployed systems. Future research should, therefore, employ empirical action research to implement the proposed hybrid model and quantitatively measure its impact over a 12-24-month period. Key metrics should include mean time between failures (MTBF) in the African operational environment, the true administrative overhead in staff-hours, and the frequency and efficacy of security incident containment. Further investigation is needed into the specific cyber threat landscape targeting African universities. Research could analyse network traffic and attack patterns to determine if the threat profile at the network edge genuinely necessitates the most advanced, expensive threat prevention features, or if the signature base of a solution like the EFG's CyberSecure is sufficiently adequate. This would provide a more data-driven basis for security control selection.

Finally, a critical area for future inquiry is the development of standardised governance models for multi-vendor security environments. Research should explore the tools, processes, and policy frameworks required to effectively orchestrate security policies and maintain cohesive visibility across a hybrid architecture involving best-of-breed and integrated components, ensuring that complexity does not become the enemy of security.

References

African Union. (2022). Digital Transformation Strategy for Africa (2020-2030): Status Report. African Union Commission.

AVFirewalls.com. (n.d.). *FortiGate 600F Series Pricing and Specifications*. Retrieved from https://avfirewalls.com/

Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99-120.

Bello, A., & Ojo, O. (2021). Cybersecurity challenges in African higher education: A systematic review. *Journal of Higher Education in Africa, 19*(2), 45-67.

Fortinet. (2025). *FortiGate 600F Series Datasheet*. Fortinet Inc.

Frimpong, K., & Asante, M. (2023). Vendor support ecosystems and IT project sustainability in Ghana's public sector. *African Journal of Information Systems, 15*(1), 112-130.

Gartner. (2023). *Magic Quadrant for Network Firewalls*. Gartner, Inc.

Gibson, H., & Miller, T. (2022). Securing the academic enterprise: A case study of next-generation firewall deployment at a research university. *Journal of Educational Technology & Society, 25*(3), 345-359.

Jegede, O., & Owolabi, T. (2021). Network downtime and institutional resilience in Nigerian universities. *International Journal of Educational Development, 81*, 102335.

Lawrence Systems. (2023). *UniFi Enterprise Fortress Gateway Deep Dive Review*. [Video]. YouTube.

Lowe, S. (2024). *Ubiquiti UniFi Enterprise Fortress Gateway (EFG) Review*. ServeTheHome. Retrieved from https://www.servethehome.com

Mensah, D. K. (2022). *ICT funding and strategic alignment in Ghanaian public universities* [Unpublished doctoral dissertation]. University of Ghana.

Moyo, S., & Selemani, A. (2023). The escalating cyber threat landscape facing African universities. *Journal of African Cybersecurity, 5*(1), 88-105.

Nkosi, B., & Dlamini, Z. (2022). Inefficient technology investment and its impact on digital pedagogy in South Africa. *South African Journal of Education, 42*(1), 1-12.

PeerSpot. (2025). *FortiGate vs. Ubiquiti UniFi: User Reviews and Comparisons*. Retrieved from https://www.peerspot.com

Rogers, E. M. (2003). *Diffusion of Innovations* (5th ed.). Free Press.

ServeTheHome. (2023). *Ubiquiti UniFi Enterprise Fortress Gateway (EFG) Review*. Retrieved from https://www.servethehome.com

Tarhini, A., El-Masri, M., Ali, M., & Serrano, A. (2023). A contextualized framework for technology adoption in developing countries. *Information & Management, 60*(2), 103-118.

Ubiquiti Inc. (2025a). *UniFi Enterprise Fortress Gateway (EFG) Datasheet*. Ubiquiti Inc.

Ubiquiti Inc. (2025b). *UniFi CyberSecure Threat Management Documentation*. Ubiquiti Inc.

Ubiquiti Inc. (2025c). *UniFi Controller Management Guide*. Ubiquiti Inc.

Ubiquiti Inc. (2025d). *UniFi High Availability and Shadow Mode*. Ubiquiti Inc.

University of Cape Coast. (2021). Strategic Plan for Digital Transformation (2021-2025). UCC Press.

Williams, P. (2023). Technological mismatch and public sector project failure. *Public Administration and Development, 43*(1), 55-70.