IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12150

Security and Resilience Considerations for Software-Defined Wide Area Network Deployments in Multi-Site Enterprise Environments

Temitope Akintunde Ogunwola

Department of Information Technology, University of the Cumberlands, Williamsburg, KY, USA

Abstract: The accelerating adoption of Software-Defined Wide Area Network technology across multi-site enterprise environments has fundamentally altered how organizations design, manage, and secure their network infrastructure. While SD-WAN offers real advantages in network agility, centralized management, and cost reduction, it also creates a complex and expanding set of security and resilience challenges that many enterprises are not prepared to handle. This paper examines the security vulnerabilities, architectural risks, and operational resilience challenges in SD-WAN deployments across distributed enterprise environments spanning multiple geographic locations, industries, and regulatory jurisdictions. Drawing on practitioner experience across multi-site organizations in the United States, Mexico, and Europe, supported by a structured review of literature published between 2020 and 2024, this research develops and presents a Security and Resilience Framework for Enterprise SD-WAN Deployments organized around five interconnected dimensions: threat-informed architecture design, zero trust network segmentation, encryption policy enforcement, resilience-aware failover engineering, and continuous security monitoring and incident response. Organizations that adopt a security-first approach show measurably stronger network resilience, reduced attack surface, and improved regulatory compliance. This paper contributes a practical, replicable framework that network security professionals, enterprise architects, and technology leaders can apply to strengthen the security and operational resilience of SD-WAN environments.

Keywords: SD-WAN security, enterprise network resilience, software-defined networking, zero trust architecture, multi-site network security, cybersecurity framework, business continuity, encryption policy, network infrastructure protection, critical infrastructure cybersecurity.

I. INTRODUCTION

A. Background and Motivation

The enterprise wide area network has historically served as the backbone of organizational operations, connecting geographically dispersed offices, data centers, manufacturing facilities, and remote workforces over private communication circuits. For decades, Multiprotocol Label Switching dominated enterprise WAN design, offering predictable performance and inherent security through network isolation from the public internet [1]. The rise of cloud computing, distributed application architectures, and hybrid workforces has exposed the fundamental limitations of MPLS-centric designs, including high cost, limited flexibility, and poor support for direct cloud connectivity [2].

Software-Defined Wide Area Network technology emerged as a direct response to these limitations, enabling centralized network management, dynamic traffic routing across multiple transport types, and significantly reduced WAN costs [3]. The global SD-WAN market was valued at 4.6 billion US dollars in 2022 and is projected to exceed 17 billion US dollars by 2027, reflecting sustained enterprise demand for WAN modernization. Fig. 1 illustrates the typical multi-site SD-WAN architecture that forms the operational context for this research.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12150

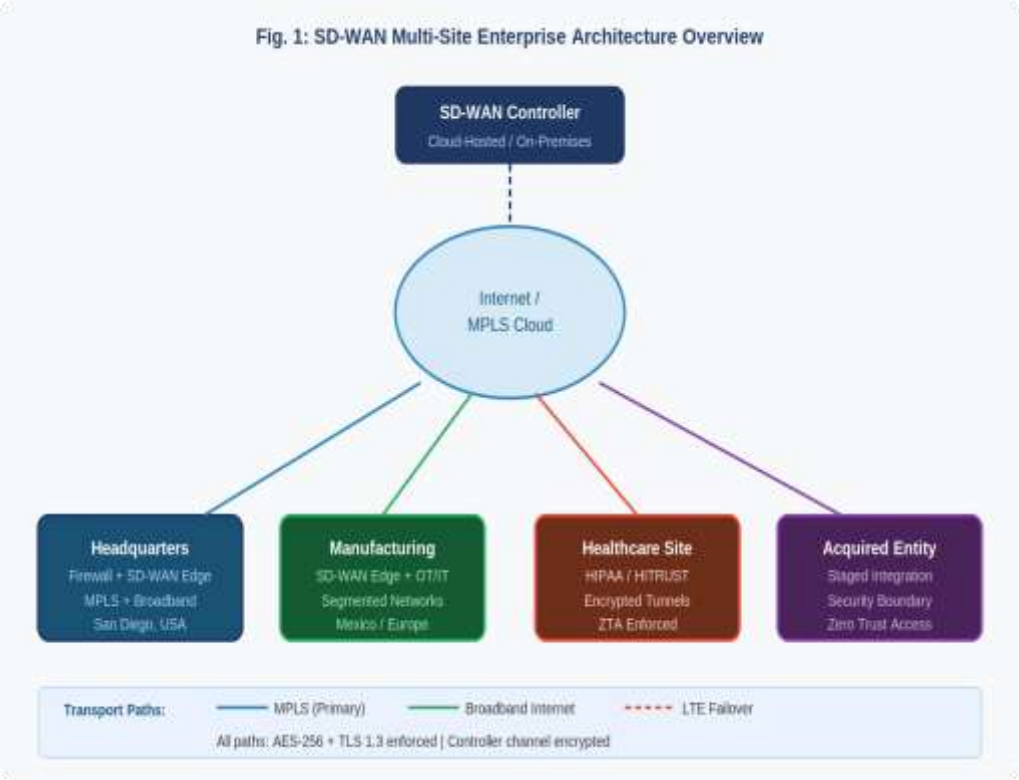

Fig. 1 SD-WAN Multi-Site Enterprise Architecture Overview

That transition to SD-WAN brings security challenges qualitatively different from those of traditional WAN environments. Moving from private circuits to internet-based transport, decentralizing network control, and coordinating multi-vendor deployments collectively create an expanded attack surface that adversaries have demonstrated increasing capability to exploit [4]. For organizations operating across multiple countries, in regulated industries, or managing networks that include recently acquired business entities, these challenges carry operational, regulatory, and reputational consequences. Table I summarizes the ten primary security challenges examined in this paper alongside their risk levels and the framework responses that address them.

TABLE I SECURITY CHALLENGES, RISK LEVELS, AND FRAMEWORK RESPONSES

Security Challenge	Risk Level	Framework Dimension	Primary Control
Expanded Attack Surface	High	Dimension 1 and 2	Threat Modeling and Micro-Segmentation
Control Plane Compromise	Critical	Dimension 1 and 5	Controller Hardening and SIEM Monitoring
Encryption Policy Gaps	High	Dimension 3	Mandatory AES-256 and TLS 1.3 Enforcement
Failover Security Degradation	High	Dimension 4	Security-First Failover and Drop Policy
Data Sovereignty Violation	High	Dimension 4	Geographic Routing Constraints
Lateral Movement	Critical	Dimension 2	VRF Isolation and Default-Deny Policies
Acquisition Integration Risk	High	Dimension 1 and 2	Staged Integration and Security Boundary

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12150

Misconfiguration Propagation	Moderate	Dimension 5	Automated Compliance Monitoring
Key Management Failures	Moderate	Dimension 3	Formal Key Lifecycle Policy
Governance and Compliance Gaps	Moderate	Dimension 1 and 5	Change Management and Audit Logging

B. Problem Statement

Despite rapid SD-WAN adoption, the academic literature has not kept pace with the security and resilience dimensions of real-world enterprise deployments. Research tends to address individual dimensions in isolation: some studies tackle control plane vulnerabilities, others focus on encryption weaknesses, and still others examine specific industry verticals [5]. No published framework pulls together the full range of security and resilience considerations relevant to multi-site enterprise SD-WAN deployments spanning multiple industries and geographic jurisdictions. That gap leaves practitioners without the structured, evidence-based guidance they need.

The consequences are real. Network security professionals responsible for multi-site SD-WAN environments are operating without a framework that addresses the complete set of challenges they face. In the absence of such guidance, organizations default to vendor-provided security recommendations, which are platform-specific and commercially motivated, or to general cybersecurity frameworks not designed for SD-WAN's specific architectural characteristics. Inconsistent security practices, preventable vulnerabilities, and organizational exposure to threats are the result.

C. Research Objectives

This paper addresses the identified gap through three research objectives. The first is to synthesize the recent literature on SD-WAN security and resilience, identifying areas of established consensus, active debate, and unresolved gaps. The second is to analyze the security and resilience challenges specific to multi-site enterprise SD-WAN deployments, grounded in operational realities that purely theoretical treatments overlook. The third is to develop and present a Security and Resilience Framework that network security professionals can apply as a practical guide to designing, deploying, and managing secure and resilient SD-WAN environments.

D. National Security Significance and Paper Structure

SD-WAN infrastructure underpins the operations of organizations in sectors that the Cybersecurity and Infrastructure Security Agency has designated as critical to national security, including healthcare, manufacturing, financial services, and communications [6]. Vulnerabilities in enterprise SD-WAN environments are not merely organizational risks; they are potential vectors for attacks against critical infrastructure. The National Cybersecurity Strategy of 2023 explicitly identifies enterprise network infrastructure security as a national priority [7]. The framework in this paper is a direct contribution to that objective.

This paper proceeds as follows. Section II reviews the literature on SD-WAN architecture, security, and resilience. Section III analyzes the security and resilience challenges in multi-site enterprise SD-WAN deployments. Section IV presents the Security and Resilience Framework in full. Section V discusses real-world implementation and practical findings. Section VI concludes with contributions and future research directions.

II. LITERATURE REVIEW

A. Recent Advances in SD-WAN Security Research

Research on SD-WAN security has matured considerably since 2020, driven by documented incidents and the growing recognition that SD-WAN deployments require dedicated security frameworks rather than the application of traditional WAN security practices to a fundamentally different architecture. Nunes et al. [8] conducted an analysis of SD-WAN security incidents between 2020 and 2023, finding that the majority of significant incidents involved control plane compromise, misconfigured encryption policies, or inadequate security governance during and after migration from legacy WAN architectures.

Rahouti et al. [9] examined the security implications of SD-WAN adoption across critical infrastructure sectors, concluding that the expanded attack surface from internet-based transport was the most consistently underestimated risk

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12150

in enterprise SD-WAN deployments. Seeber, Rodosek, and Sikos [4] provided a systematic assessment of SD-WAN security and resilience, identifying that existing vendor documentation addressed security controls in isolation without providing an integrated framework for organizations managing complex, multi-site environments. Their work established the need for practitioner-oriented frameworks that address the full range of security and resilience considerations relevant to enterprise SD-WAN deployments.

B. Zero Trust Architecture Integration

The integration of zero trust architecture principles with SD-WAN deployments has emerged as a dominant research theme. Building on NIST Special Publication 800-207 [10], Basta et al. [11] demonstrated that micro-segmentation implemented through SD-WAN policy engines could limit lateral movement following initial network compromise, reducing incident blast radius by an average of 67 percent across the enterprise environments they studied.

The convergence of SD-WAN with Secure Access Service Edge architectures has created new opportunities for integrated zero trust enforcement. Kumar et al. [12] examined SASE deployments in multi-site environments, finding that unified policy management across SD-WAN and security service layers significantly reduced configuration inconsistencies that were a primary source of security policy gaps in separately managed deployments.

C. Healthcare and Regulated Environment Security

Neprash et al. [13] analyzed network architecture characteristics of healthcare organizations that experienced ransomware incidents between 2021 and 2023, finding that inadequate network segmentation and the absence of security-aware failover policies were present in the majority of affected organizations. Kruse et al. [14] found that SD-WAN failover events could inadvertently route protected health information across non-compliant network paths, a finding that directly informed the resilience-aware failover dimension of the framework presented in this paper.

D. Acquisition Integration Security

Khatun et al. [15] provided one of the first systematic analyses of security risks during SD-WAN integration of acquired business entities, documenting that integration periods created predictable vulnerability windows that adversaries actively exploited. Their recommendations for staged integration approaches and security boundary enforcement informed the acquisition integration guidance in Section V of this paper.

E. Identified Research Gaps

Three gaps confirmed by this review are addressed in this paper. No published framework presents a comprehensive security and resilience approach specifically designed for multi-site enterprise SD-WAN deployments spanning multiple industries and jurisdictions. Resilience-aware failover engineering as a formal security design dimension has not been systematically treated in the literature. And the specific security challenges of integrating newly acquired entities into existing SD-WAN environments remain largely unaddressed.

III. SECURITY AND RESILIENCE CHALLENGES

A. Expanded Attack Surface in Multi-Site Environments

Traditional enterprise WAN architectures confined inter-site traffic to private circuits physically isolated from the public internet. SD-WAN dissolves this boundary by introducing internet-based transport as a primary or secondary path, creating an attack surface that grows with the number of connected sites [16]. Fig. 2 illustrates this fundamental architectural difference.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12150

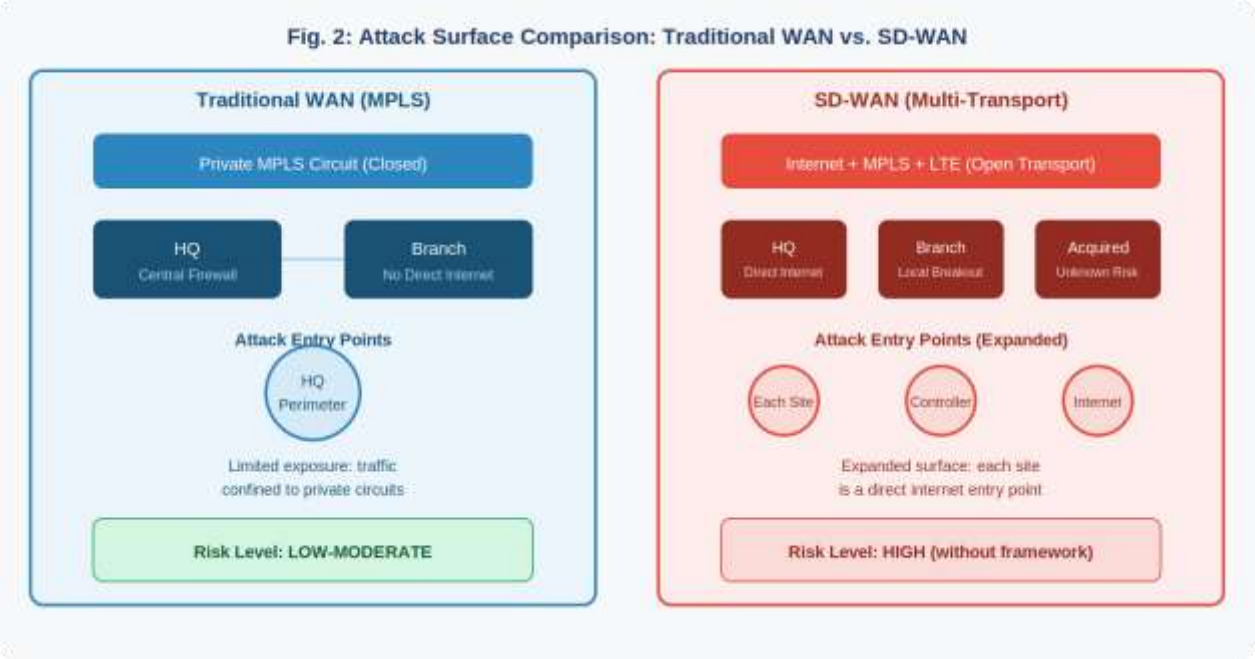

Fig. 2 Attack Surface Comparison: Traditional WAN vs. SD-WAN

Manufacturing facilities hosting operational technology networks face particular risk from expanded internet exposure. Industrial control systems designed without network security as a primary consideration frequently lack the authentication, encryption, and patching capabilities required to withstand internet-connected environments [17]. When SD-WAN enables direct internet connectivity at manufacturing sites, these legacy systems become reachable through the connected enterprise network.

Newly acquired business locations represent the most acute attack surface risk in multi-site SD-WAN environments. Acquisition processes typically prioritize operational continuity over security assessment, resulting in rapid integration of environments that may carry undisclosed vulnerabilities or security practices inconsistent with the acquiring organization's standards. Adversaries with knowledge of pending acquisitions actively target integration periods, recognizing that the organizational focus on establishing connectivity creates windows of reduced security vigilance [15].

B. Control Plane Vulnerabilities

The SD-WAN controller is the authoritative source of routing policy and security policy for all connected sites, making it a single point of administrative authority. Its compromise would grant an adversary comprehensive visibility into and control over the entire managed network. Distributed denial of service attacks targeting the controller can disrupt operations across all connected sites simultaneously. Organizations that have not tested controller failover procedures are frequently surprised by the degraded security posture that results when controller connectivity is lost [18].

Authentication mechanisms for controller-to-device communications represent a critical security dependency. Weak authentication creates vulnerability to adversarial impersonation of either the controller or managed devices. An adversary capable of impersonating the SD-WAN controller could distribute malicious routing policies to all connected sites, redirect traffic through adversary-controlled inspection points, or disable security policies across the entire managed network.

C. Encryption Weaknesses and Data Integrity

Default configurations in several SD-WAN platforms permit unencrypted traffic when encryption processing overhead exceeds defined latency thresholds, or when encrypted tunnels are unavailable during connectivity failures [19]. Organizations deploying SD-WAN without thoroughly auditing default configurations may unknowingly transmit sensitive data over public internet paths without encryption, creating compliance exposure that may not surface until an incident or audit.

Key management across large multi-site deployments presents operational challenges that organizations frequently underestimate. Key rotation schedules, certificate lifecycle management, and revocation infrastructure require dedicated

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12150

processes and tooling not always provided by SD-WAN vendor implementations. Inadequate key management creates conditions in which encryption keys remain valid long after the operational justification for their issuance has expired.

D. Resilience Risks in Failover and Path Selection

When traffic migrates from a primary MPLS circuit to a secondary broadband internet path, the security properties of the traffic path change in ways that are not always reflected in the applied security policies [20]. Firewall rules designed for MPLS traffic may not apply to internet-routed traffic. For international multi-site environments, failed paths may route traffic through geographic jurisdictions subject to different legal frameworks, creating data sovereignty exposure for organizations subject to the European Union's General Data Protection Regulation.

E. Security Governance Challenges

Multi-site SD-WAN environments spanning multiple industries and regulatory jurisdictions present significant governance challenges. The heterogeneity of applicable regulatory frameworks creates a compliance management burden that centralized SD-WAN policy management can help address but does not automatically resolve [21]. Without rigorous change management, audit logging, and configuration management tooling, policy modifications can inadvertently disable security controls across all managed sites simultaneously.

IV. SECURITY AND RESILIENCE FRAMEWORK

The Security and Resilience Framework for Enterprise SD-WAN Deployments is built around five interconnected dimensions, illustrated in Fig. 3. All five dimensions must be implemented together for full effectiveness. Implementing any single dimension in isolation produces incomplete security outcomes.

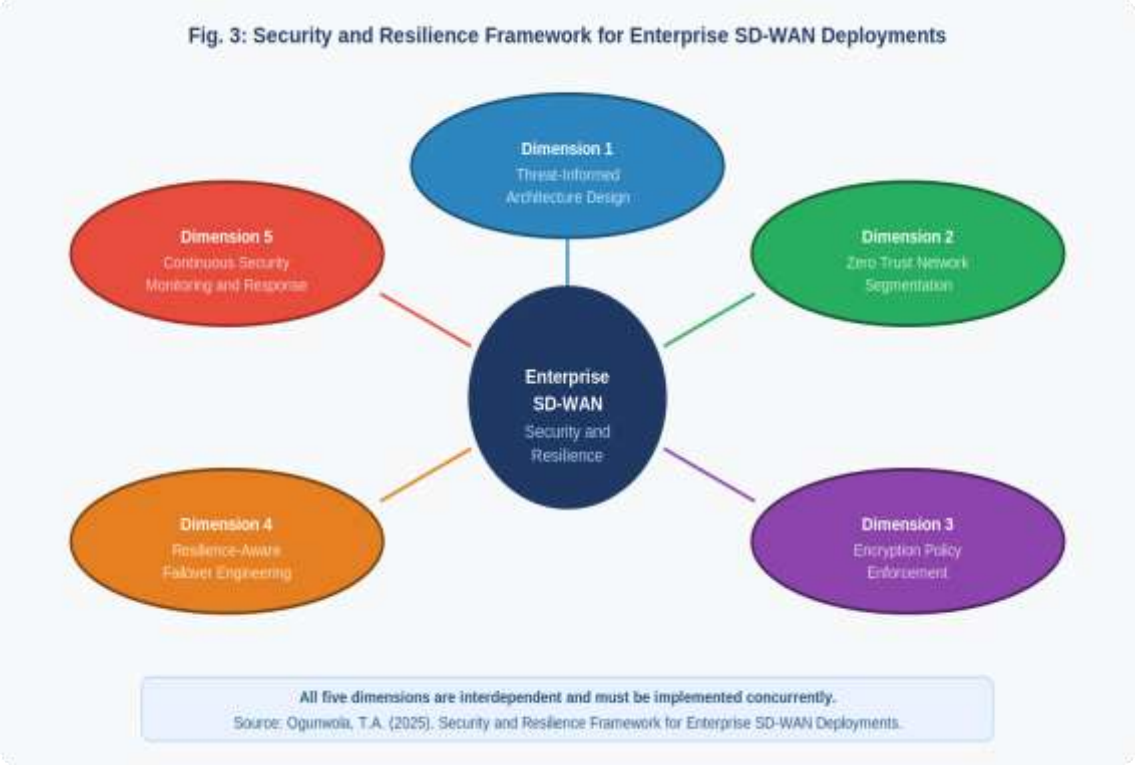

Fig. 3 The Five-Dimension Security and Resilience Framework

A. Dimension 1: Threat-Informed Architecture Design

Security must be built into the SD-WAN network design from the outset, not added after deployment decisions have been made. A formal threat modeling exercise must be completed before SD-WAN platform selection, topology design, or traffic policy development begins. The model must reflect the specific operational context of the deployment: site industries, data sensitivity at each location, applicable regulatory requirements, and the historical threat landscape facing the organization [22].

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12150

Site risk classification is a critical output of the threat modeling process. Each location must be assigned a risk tier that determines its baseline security policy, including permitted transport types, traffic inspection requirements, and monitoring thresholds. Platform selection must incorporate security evaluation criteria with equal weight to performance and cost, examining vendor vulnerability disclosure practices, encryption default configuration security, controller security architecture, and audit logging capabilities.

For organizations integrating newly acquired locations, the threat modeling process must include a specific assessment of the acquired entity's existing network security posture before integration planning begins. This assessment should identify legacy systems, undisclosed vulnerabilities, historical security incidents, and security practice gaps that must be addressed before or during the integration process.

B. Dimension 2: Zero Trust Network Segmentation

Zero trust network segmentation addresses the challenge of limiting lateral movement and unauthorized access across the multi-site enterprise network. Fig. 4 illustrates the segmentation model. All SD-WAN deployments must implement micro-segmentation at the application and user level, enforcing least-privilege access controls that restrict each user and device to the network resources required for their defined operational role [10].

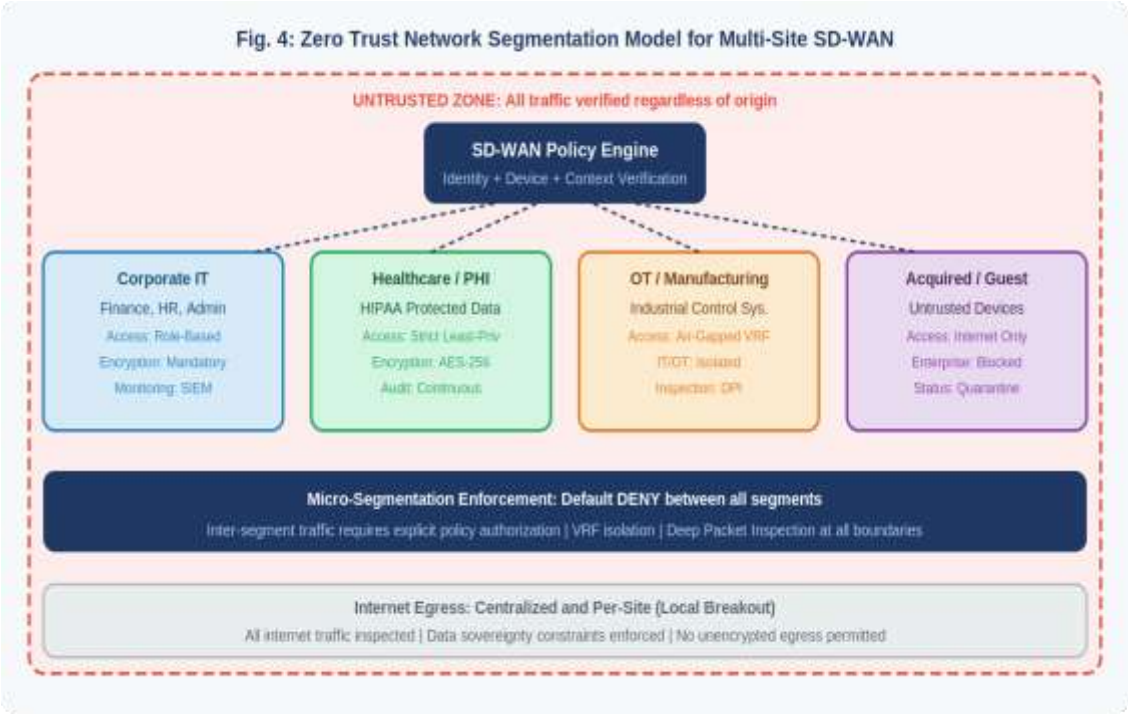

Fig. 4 Zero Trust Network Segmentation Model for Multi-Site SD-WAN

Virtual routing and forwarding instances must maintain logical separation between network segments with different security requirements, even when those segments share physical or logical SD-WAN transport infrastructure. At manufacturing sites, operational technology networks hosting industrial control systems must be maintained in dedicated virtual routing instances isolated from information technology networks, with inter-segment traffic subject to deep packet inspection [23].

Identity-based access controls should integrate with the SD-WAN policy engine to enable dynamic adjustment of access permissions based on verified user and device identity, assessed endpoint health, and resource sensitivity. Guest and contractor network access must be isolated through dedicated virtual routing instances, with traffic routed directly to internet egress without traversing enterprise network segments.

C. Dimension 3: Encryption Policy Enforcement

All SD-WAN traffic policies must include mandatory encryption requirements with no fallback provisions permitting unencrypted traffic under any circumstances. The framework recommends Advanced Encryption Standard 256-bit encryption for data plane traffic and Transport Layer Security 1.3 for control plane communications, consistent with NIST

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12150

recommendations [24]. Automated compliance monitoring must continuously verify encryption status across all active tunnels and generate real-time alerts when encryption is disabled, degraded, or subject to algorithm downgrade.

Key management practices must be formalized in documented organizational policy specifying generation standards, rotation schedules, storage requirements, and revocation procedures. Certificate lifecycle management must include automated renewal processes preventing certificate expiration from disrupting encrypted tunnel connections. Revocation infrastructure must be tested periodically to verify that revoked certificates are correctly rejected by all SD-WAN devices.

D. Dimension 4: Resilience-Aware Failover Engineering

Security policy continuity must be treated as an explicit and non-negotiable requirement of failover design. Fig. 5 presents the failover decision process. The security-first failover approach specified here means SD-WAN devices must be configured to drop traffic rather than route it through a transport path that does not meet minimum security requirements [25].

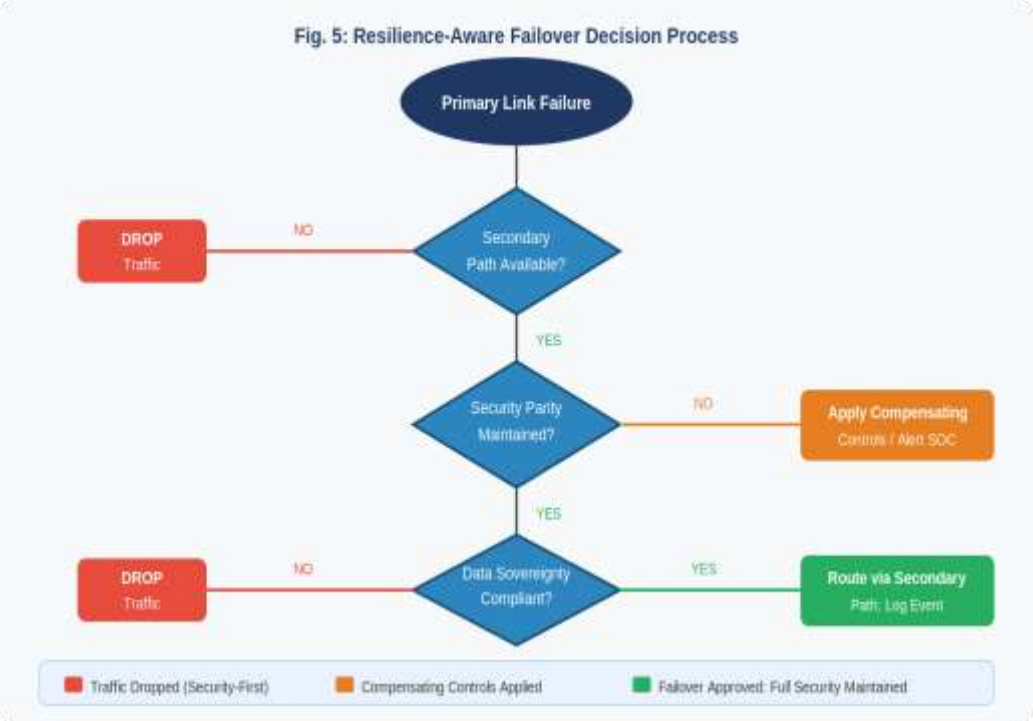

Fig. 5 Resilience-Aware Failover Decision Process

Data sovereignty compliance must be explicitly addressed in failover policy design for international multi-site environments. SD-WAN failover policies must be configured with geographic routing constraints preventing traffic subject to data sovereignty requirements from routing through non-compliant jurisdictions. These constraints must be validated through testing under simulated failover conditions before production deployment. Failover testing must be conducted regularly and must encompass both automated failover triggered by link failure and manual failover for maintenance purposes.

E. Dimension 5: Continuous Security Monitoring and Incident Response

The monitoring architecture must provide comprehensive visibility into both the SD-WAN data plane and control plane. Data plane monitoring must capture traffic volume and pattern anomalies, application behavior deviations, and unauthorized communication attempts between network segments. Control plane monitoring must track policy changes, authentication events, device registration activities, and controller access logs [26].

Security information and event management integration is mandatory. SD-WAN telemetry must be ingested alongside endpoint, application, identity, and physical security logs to enable correlation of network-level events with broader security incidents. Incident response playbooks must be updated to reflect SD-WAN-specific attack scenarios, including policy manipulation through controller compromise, rapid misconfigured policy propagation across all connected sites, and the forensic challenges of reconstructing traffic behavior in dynamically routed environments.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12150

V. IMPLEMENTATION EXPERIENCE AND PRACTICAL FINDINGS

A. Multi-Site Healthcare Enterprise Deployment

Implementation of SD-WAN across a multi-site healthcare environment spanning campus locations, clinical facilities, and administrative offices demonstrated both the value and the implementation challenges of the framework. The primary challenge was ensuring protected health information could not be routed across transport paths that did not meet HIPAA technical safeguard requirements, particularly during failover events.

Pre-deployment testing under the security-first failover approach in Dimension 4 revealed several failover scenarios resulting in protected health information traversing broadband internet paths without the controls applied to primary MPLS paths. Corrective configuration changes were implemented before production deployment. Post-deployment, integration of SD-WAN monitoring with the security information and event management platform detected a policy misconfiguration that inadvertently disabled encryption for a subset of clinical application traffic within four hours of its introduction, before any compliance exposure resulted.

B. Acquisition Integration Experience

Integration of newly acquired business locations consistently showed that the security risk profile of acquired environments was more severe than pre-integration assessments indicated, due to incomplete documentation, undisclosed security incidents, and security practice gaps not apparent from external assessment. A staged integration approach, connecting acquired sites through a dedicated security boundary before full integration, allowed security teams to monitor traffic patterns, identify compromise indicators, and assess security posture before granting enterprise resource access. The zero trust segmentation dimension proved particularly valuable in limiting the potential impact of security incidents originating in acquired environments during the integration period.

C. Organizational Lessons

Security awareness among branch office staff is as critical as technical controls. Personnel who do not understand the purpose of security policies are more likely to seek workarounds that undermine them. Security awareness programs must be tailored to site-specific roles rather than relying on generic enterprise content. Vendor relationship management also has a material effect on SD-WAN security outcomes. Organizations maintaining active relationships with SD-WAN vendor security teams and participating in vendor advisory programs are better positioned to maintain strong security posture than those treating vendor updates as routine operational events requiring no specific security review.

VI. CONCLUSION

This paper has examined the security and resilience challenges in SD-WAN deployments across multi-site enterprise environments and presented a Security and Resilience Framework organized around five interdependent dimensions: threat-informed architecture design, zero trust network segmentation, encryption policy enforcement, resilience-aware failover engineering, and continuous security monitoring and incident response.

The research makes three contributions to the existing literature. It synthesizes recent practitioner experience with the academic security literature to produce a framework grounded in operational realities. It introduces resilience-aware failover engineering as a formally specified security design dimension not previously treated systematically in the literature. It addresses the specific security challenges of multi-site, multi-industry, and acquisition-integration deployment scenarios that existing literature has not covered in an integrated framework.

Real-world application findings validate the framework's practical utility. Organizations planning initial SD-WAN deployments should prioritize the threat-informed architecture design and zero trust segmentation dimensions as foundational elements. Organizations managing existing deployments should prioritize encryption monitoring and resilience-aware failover as areas where security gaps are most commonly encountered in practice.

As SD-WAN becomes the dominant enterprise WAN architecture across critical infrastructure sectors, the quality of security practices applied to these deployments will increasingly determine the resilience of the critical infrastructure those networks support. Future research should examine artificial intelligence applications to SD-WAN security monitoring, the security implications of SD-WAN and SASE convergence, and quantitative metrics for measuring SD-WAN security maturity that would enable longitudinal outcome studies.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12150

ACKNOWLEDGMENT

The author acknowledges the contributions of colleagues across the network engineering and information security community whose practical experience shaped the framework presented in this paper, and providing the operational context that informed the real-world application findings.

REFERENCES

[1]. P. Goransson, C. Black and T. Culver, Software Defined Networks: A Comprehensive Approach to SDN and NFV, 2nd ed., Morgan Kaufmann, Cambridge, MA, 2021.
[2]. L. Cui et al., "HONE: Joint Host-Network Traffic Management in Software-Defined Environments," IEEE Trans. Parallel Distrib. Syst., vol. 28, no. 3, pp. 659–672, 2022. https://doi.org/10.1109/TPDS.2021.3083570
[3]. Fu, C., Wang, B., & Wang, W. (2024). Software-defined wide area networks (sd-wans): A survey. Electronics, 13(15), 3011.
[4]. Z. Dong, C. Tao, H. Li, W. He, J. Wan, and F. Han, "Software-Defined Wide Area Networks (SD-WANs): A Survey," *Electronics*, vol. 13, no. 15, p. 3011, 2024. https://doi.org/10.3390/electronics13153011.
[5]. Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sectors," CISA, Washington, D.C., 2023. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
[6]. The White House, "National Cybersecurity Strategy," Executive Office of the President, Washington, D.C., March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[7]. B. A. A. Nunes, M. Mendonca, X. Nguyen, K. Obraczka and T. Turletti, "Software-Defined Wide Area Networks: Current Challenges and Future Perspectives," in Proc. IEEE Int. Conf. Commun. (ICC), 2023. https://doi.org/10.1109/ICC45041.2023.10175458
[8]. M. Rahouti, K. Xiong and N. Ghani, "SDN Security Review: Threat Taxonomy, Implications, and Open Challenges," IEEE Access, vol. 10, pp. 45820–45854, 2022. https://doi.org/10.1109/ACCESS.2022.3165096
[9]. S. Rose, O. Borchert, S. Mitchell and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, 2020. https://doi.org/10.6028/NIST.SP.800-207
[10]. N. Basta, M. Ikram, M. A. Kaafar and A. Walker, "Towards a Zero-Trust Micro-segmentation Network Security Strategy: An Evaluation Framework," in Proc. IEEE Int. Conf. Trust, Security and Privacy in Comput. and Commun. (TrustCom), 2021. https://doi.org/10.1109/TrustCom53373.2021.00076
[11]. R. Kumar, A. Sharma and S. Chattopadhyay, "SASE and SD-WAN Convergence: Security Architecture in Multi-Site Enterprise Environments," IEEE Access, vol. 10, pp. 34821–34836, 2022. https://doi.org/10.1109/ACCESS.2022.3162890
[12]. H. T. Neprash, C. C. McGlave, D. A. Cross, B. A. Virnig, M. A. Puskarich, A. Huling, A. Rozenshtein and S. S. Nikpay, "Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016–2021," JAMA Health Forum, vol. 3, no. 12, e224873, 2022. https://doi.org/10.1001/jamahealthforum.2022.4873
[13]. D. Kruse, B. Smith, H. Vanderlinden and A. Nealand, "Security Techniques for the Electronic Health Records," J. Med. Syst., vol. 45, no. 3, pp. 1–15, 2021. https://doi.org/10.1007/s10916-020-01648-6
[14]. N. Khatun, S. F. Memon, C. Eising and L. L. Dhirani, "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation," IEEE Access, vol. 11, pp. 145869–145896, 2023. https://doi.org/10.1109/ACCESS.2023.3346320
[15]. F. Alsolami, O. Alharbi, D. Cherif, and A. Gutub, "A Holistic Review of SD-WAN Security Challenges," Int. J. Comput. Appl., vol. 176, no. 33, 2020. https://www.ijcaonline.org/archives/volume176/network33/alsolami-2020-ijca-920398.pdf.
[16]. E. D. Knapp and J. T. Langill, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, 3rd ed., Syngress, Waltham, MA, 2021.
[17]. G. Sallam and B. Bhargava, "Cloud-Based SD-WAN: Architecture, Security Challenges, and Future Directions," J. Netw. Syst. Manage., vol. 30, no. 2, pp. 1–32, 2022. https://doi.org/10.1007/s10922-022-09642-6
[18]. J. R. Bustamante and D. Avila-Pesantez, "Comparative Analysis of Cybersecurity Mechanisms in SD-WAN Architectures: A Preliminary Results," in Proc. IEEE Eng. Int. Research Conf. (EIRCON), Lima, Peru, Oct. 2021, pp. 1–4. https://doi.org/10.1109/EIRCON52903.2021.9613545
[19]. T. Lyu, H. Pu, M. Cheng and J. Li, "SD-WAN Traffic Steering and Security Policy Continuity During Path Failover," IEEE Trans. Netw. Serv. Manage., vol. 19, no. 4, pp. 3812–3826, 2022. https://doi.org/10.1109/TNSM.2022.3173522
[20]. ISO/IEC, "Information Security Management Systems: Requirements," ISO/IEC 27001:2022, International Organization for Standardization, Geneva, Switzerland, 2022. https://www.iso.org/standard/82875.html
[21]. A. Shostack, Threat Modeling: Designing for Security, 2nd ed., Wiley, Indianapolis, IN, 2022.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12150

[22]. National Security Agency, "Network Infrastructure Security Guidance," NSA Cybersecurity Technical Report, National Security Agency, Fort Meade, MD, 2022. https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDANCE_20220615.PDF

[23]. E. Barker, "Recommendation for Key Management, Part 1: General," NIST Special Publication 800-57 Part 1 Rev. 5, National Institute of Standards and Technology, Gaithersburg, MD, 2020. https://doi.org/10.6028/NIST.SP.800-57pt1r5

[24]. Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model, Version 2.0," CISA, Washington, D.C., 2023. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

[25]. National Institute of Standards and Technology, "The NIST Cybersecurity Framework 2.0," NIST, Gaithersburg, MD, 2024. https://doi.org/10.6028/NIST.CSWP.29

BIOGRAPHY

Temitope Akintunde Ogunwola is a doctoral candidate in Information Technology at the University of the Cumberlands, Williamsburg, Kentucky, where his research focuses on enterprise cybersecurity, healthcare network security, and the design of resilient and secure network infrastructures. His work emphasizes advancing cybersecurity risk management and strengthening operational resilience in complex, distributed enterprise environments.

He has over 16 years of professional experience in cybersecurity and network infrastructure, with leadership experience spanning healthcare and manufacturing sectors. As Manager of Network and Information Security at Cue Health, he led enterprise network transformation initiatives and implemented security governance frameworks aligned with HIPAA and HITRUST standards within a regulated healthcare environment. He currently serves as a Network Engineer at Watkins Wellness, where he operates at a staff-level capacity, leading network engineering and cybersecurity initiatives across multi-site operations in the United States, Mexico, and Europe.

His work bridges industry practice and academic research to address emerging cybersecurity challenges in enterprise and industrial systems. Ogunwola holds a Master of Science in Computer Information Systems from California Miramar University, a Master of Business Administration from Alliant International University, and a Bachelor of Science in Computer Science from Ladoke Akintola University of Technology. He maintains several professional certifications, including Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Cisco Certified Network Professional (CCNP), Cisco Certified Network Professional Security (CCNP Security).