World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

# Hybrid network security architecture F5–AWS Integration, Zero-Trust Enforcement, and SD-WAN for PCI DSS-Compliant Hybrid Environments

Satya Nanda Vara Prasad Kanchumarthi *

*Enterprise Infra Architect & Lead Application Engineer, USA.*

World Journal of Advanced Research and Reviews, 2024, 22(01), 2111–2117

Publication history: Received on 06 March 2024; revised on 23 April 2024; accepted on 28 April 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.22.1.1162

## Abstract

Hybrid network security represents the confluence of on- demesne structure and all-native defense mechanisms into a unified, policy- driven armature. As enterprises accelerate digital metamorphosis enterprise, the integration of operation delivery regulators similar as F5 BIG- IP with pall services from Amazon Web Services creates layered peripheries that address Payment Card Industry Data Security Standard compliance conditions with perfection. Zero-trust principles, executed through grainy Identity and Access Management programs and behavioral business examination, review the border from a static boundary to a dynamic, environment- apprehensive construct. Assiduity data confirms that associations enforcing unified Web operation Firewall programs in mongrel surroundings achieve exploit- reduction rates exceeding ninety- five percent against the OWASP Top Ten trouble orders. Software-Defined Wide Area Network technologies extend these protections to distributed retail surroundings, enabling harmonious policy enforcement from store edge bumps to pall- grounded workloads. Intelligent cargo distribution across fifty or further F5 pools-configured for multipath synchronization at one hundred gig bits per alternate outturn-sustains high vacuity while intelligent firmware unity via out- of- band operation aeroplanes similar as Integrated Lights- eschewal and Integrated Dell Remote Access Controller automates Baseboard Management Controller provisioning and RAID integrity confirmation. Endpoint Discovery and Response hardening at the datacenter subcaste completes a defense armature that satisfies CompTIA Security CSO-003 instrument conditions and positions cold-blooded network engineers at the lead mastermind league within the fleetly expanding Software- Defined Wide Area Network request.

**Keywords:** Zero-Trust Architecture; Hybrid Network Security; SD-WAN Integration; WAF Policy Enforcement; PCI-DSS Compliance

## 1. Introduction

The ultramodern enterprise network border has dissolved. Distributed retail operations, multi-cloud deployments, and remote pool expansion force security engineers to reevaluate how defense- in- depth operates across miscellaneous surroundings. Traditional disarmed zone infrastructures, anchored by tackle firewalls and static Access Control Lists, fail to address the dynamic trouble shells introduced when workloads gauge physical datacenters and pall regions contemporaneously. mongrel network security fills this architectural gap by fusing proven on- demesne technologies - heritage VLANs inherited from Brocade and Cisco switching fabrics, operation delivery regulators from F5 Networks, and physical garçon operation through out-of-band consoles with all-native controls including Amazon Web Services operation cargo Balancer and managed Web operation Firewall services. The result is a policy-coherent security posture that extends invariant protection from the datacenter rack to the pall edge without immolating the functional inflexibility that digital metamorphosis demands. (1, 2)

* Corresponding author: Satyananda Kanchumarthi

Zero-trust security, defined by the principle of vindicating every identity and device before granting access anyhow of network position, transforms how engineers design policy enforcement points. Identity and Access Management fabrics on pall platforms apply least- honor access to pall coffers, while on- demesne Network Access Control systems authenticate endpoints before admitting them to sensitive VLANs. Wireshark- grounded packet prisoner and analysis validates that no unencrypted cardholder data traverses any network member, satisfying Payment Card Industry Data Security Standard demand 4. Endpoint Discovery and Response agents stationed across datacenter hosts give behavioral telemetry that feeds Security Information and Event Management platforms, creating a nonstop monitoring circle that shells anomalies before they escalate to breaches.

The functional discipline needed to sustain this armature extends to firmware operation. directors who calculate solely on in- band operation channels expose themselves to scripts where a compromised operating system prevents remediation of underpinning tackle vulnerabilities. Integrated Lights- eschewal regulators on Hewlett Packard Enterprise waiters and Integrated Dell Remote Access regulators on Dell structure give out- of- band operation aeroplanes that remain functional anyhow of operating system state. Automating introductory Input Affair System configuration and RAID integrity checks through these regulators eliminates homemade error and reduces the mean time to recover from tackle failures in mongrel datacenter surroundings. The crossroad of these disciplines — pall-native security controls, heritage structure integration, zero- trust policy enforcement, and intelligent tackle operation — defines the mongrel network security mastermind part that commands ultra expensive compensation in the 2026 job request.

This composition examines the specialized factors, integration patterns, and functional practices that constitute enterprise- grade mongrel network security. Section two addresses the architectural integration of F5 pools with Amazon Web Services networking services. Section three covers zero-trust enforcement through Identity and Access Management and business examination. Section four details Software- Defined Wide Area Network deployment for retail store- to- pall connectivity. Section five presents out- of- band structure robotization and its part in sustaining mongrel data center adaptability. Each section grounds its findings in empirical assiduity practice and quantifiable issues, offering interpreters a structured reference for designing, enforcing, and certifying cold-blooded network security infrastructures.

## 2. F5 and AWS architectural integration

### 2.1. F5 Pool Architecture and AWS ALB Integration

The integration of F5 BIG-IP operation delivery regulators with Amazon Web Services networking services creates a layered business operation armature that satisfies both performance and compliance conditions contemporaneously. F5 BIG-IP Local Traffic Manager operates as the on- demesne operation delivery league, distributing inbound sessions across garçon pools using iRules-scripted business programs written in Tool Command Language - that apply Payment Card Industry Data Security Standard segmentation conditions by routing cardholder data simply to validated operation waiters. Configuring fifty or further F5 pools in product surroundings demands rigorous pool member health monitoring, continuity profile operation, and Secure Sockets Subcaste profile optimization to sustain sub-millisecond failover. When multipath Equal-CostMulti-Path routing synchronizes business across clicked uplinks added up to one hundred gigabits per second, pool member cargo distribution must regard for asymmetric return path routing to help session dislocation (3, 4)

Amazon Web Services operation cargo Balancer serves as the pall-native counterpart to F5 Original Business director for workloads stationed in Virtual Private pall surroundings. operation cargo Balancer operates at Layer Seven, enabling host- grounded and path- grounded routing rules that direct business to distinct target groups Amazon Web Services fellow of F5 pools — grounded on Uniform Resource Locator structure. For Payment Card Industry Data Security Standard- scoped operations, engineers configure operation cargo Balancer listeners simply on harborage four- four-three with Transport Layer Security one- point- three programs executed. Amazon Web Services Certificate Manager vittles and rotates Transport Layer Security instruments automatically, barring the instrument expiry threat that has historically caused outages in manually managed surroundings.

Web operation Firewall integration at the operation cargo Balancer listener position provides the primary exploit-blocking capability for pall- hosted Payment Card Industry Data Security Standard operations. Amazon Web Services managed rule groups maintained by Amazon Web Services trouble intelligence brigades address the OWASP Top Ten vulnerability orders — injection, broken authentication, cross-site scripting, insecure deserialization, and others withpre-built discovery autographs streamlined continuously. Custom rule groups condense managed rules with business-specific block lists and rate-limiting programs that help credential filling and automated scraping against retail payment endpoints. Organizations that emplace both managed and custom rule groups in count mode originally, also shift to block mode after birth tuning, achieve exploit reduction rates exceeding ninety- five percent within ninety days of product deployment.

Bridging on- demesne F5 structure with Amazon Web Services networking requires architectural opinions around business doorways and exits. AWS Transit Gateway consolidates connectivity between multiple Virtual Private shadows and on- demesne networks through a single mecca, replacing complex gaping morass. point- to- point Virtual Private Network converts or Direct Connect devoted circuits carry Payment Card Industry Data Security Standard- scoped business between the on- demesne datacenter and the Amazon Web Services region, with Border Gateway Protocol route announcement controlling failover between primary and provisory paths. F5 BIG- IP stationed in Amazon Web Services as an Amazon Machine Image extends on- demesne iRule sense and Access Policy Manager programs into the pall league, icing that business audited by F5 on- demesne receives original deep- packet examination when workloads resettle to pall- hosted cases.

functional visibility across the combined F5 and Amazon Web Services estate relies on centralized monitoring. F5 BIG-IQ Centralized Management summations pool health, virtual garçon statistics, and iRule prosecution criteria from all on- demesne appliances into a single dashboard, while Amazon Web Services CloudWatch collects operation cargo Balancer access logs, Web operation Firewall tried requests, and target group health criteria . relating on- demesne pool application with pall target group response quiescence through a unified Security Information and Event operation platform — Hewlett Packard Enterprise OpenView or BMC Helix in mongrel deployments — provides the end- to- end business visibility needed for Payment Card Industry Data Security Standard inspection substantiation. Network masterminds who master this binary- pane observability model position themselves as necessary contributors to cold-blooded security operations centers.

**Table 1** F5 and AWS Integration Components with PCI DSS Compliance Mapping [3, 4]

| Integration Component | On-Premises F5 Function | Amazon Web Services Equivalent | Compliance Relevance |
|---|---|---|---|
| Traffic Distribution | Local Traffic Manager Virtual Server | Application Load Balancer Listener | PCI DSS Requirement 1 |
| Exploit Blocking | Application Security Manager Policy | Web Application Firewall Rule Group | PCI DSS Requirement 6 |
| Certificate Management | SSL Profile / iRule | Certificate Manager Integration | PCI DSS Requirement 4 |
| Route Orchestration | Equal-Cost Multi-Path Uplink Bonding | Transit Gateway Route Table | PCI DSS Requirement 1 |

## 3. Zero-trust enforcement

### 3.1. Identity and Access Management as Zero-Trust Policy Engine

*3.1.1. Identity and Access Management as Zero- Trust Policy Engine*

Zero- trust security armature rejects the implicit trust traditionally granted to realities inside a network border. Every connection attempt — whether forming from an authenticated stoner device, a microservice vessel, or an automated channel — must present empirical credentials and satisfy contextual authorization conditions before entering access to any resource. Amazon Web Services Identity and Access Management provides the policy machine through which pall-hosted coffers apply this principle. Identity and Access Management programs express warrants as unequivocal allow or deny statements scoped to specific conduct, coffers, and conditions. Engineers who design Payment Card Industry Data Security Standard- biddable surroundings construct Identity and Access Management programs that circumscribe access to cardholder data storehouse pails and database cases simply to operation places authenticated through Amazon Web Services Secure Token Service temporary credentials, barring static access key exposure from the trouble model entirely. ( 5, 6)

Attribute- grounded access control, enabled through Identity and Access Management condition keys, extends zero-trust to network path conditions. programs that bear requests to appear from specific Amazon Web Services Virtual

Private pall endpoints, target specific Geographic regions, or arrive only during authorized conservation windows apply temporal and spatial constraints that stationary part- grounded access control can not express. Service Control Policies applied at the Amazon Web Services Organizations position apply these constraints association-wide, precluding individual account directors from inadvertently loosening restrictions on Payment Card Industry Data Security Standard- scoped coffers. This governance subcaste satisfies Payment Card Industry Data Security Standard demand 7 by icing access to cardholder data is limited to only those with a licit business need.

On- demesne zero- trust enforcement operates through a reciprocal mound. Network Access Control systems authenticate endpoints against Active Directory instrument stores before admitting them to Payment Card Industry Data Security Standard VLANs. Cisco TrustSec Security Group Tags propagate authorization opinions throughout the switching fabric, icing that indeed side movement within the datacenter encounters policy enforcement at every hop. F5 BIG- IP Access Policy Manager extends zero- trust to operation sessions by administering multi-factor authentication, device posture assessment, and session threat scoring before presenting operation content. druggies whose device posture scores fall below threshold admit counterblockade VLAN assignment automatically, segregating potentially compromised endpoints without homemade director intervention**.**

Wireshark packet prisoner analysis provides ground- verity confirmation that zero- trust policy enforcement functions as designed. Judges capture business at VLAN boundaries, at F5 virtual garçon doorway and exit points, and at Amazon Web Services VPC Flow Log collection points to confirm that no unencrypted cardholder data transits any member. Wireshark display pollutants insulate Payment Card Industry Data Security Standard-applicable protocols — specifically, any cleartext Hypertext Transfer Protocol business on harborage eighty within cardholder data terrain parts and flag violations for immediate remediation. slated prisoner sessions form part of the nonstop monitoring substantiation needed by Payment Card Industry Data Security Standard Requirement 10 and give forensic vestiges that accelerate incident response when anomalies face.

Endpoint Discovery and Response agents stationed on datacenter hosts complete the zero- trust enforcement chain at the cipher subcaste. ultramodern Endpoint Discovery and Response platforms relate process prosecution telemetry, train system events, and network connection attempts against trouble intelligence pointers, blocking vicious exertion at the host position before network controls see the business. Endpoint Discovery and Response hardening of datacenter hosts hosting Payment Card Industry Data Security Standard workloads satisfies Payment Card Industry Data Security Standard demand 5 by furnishing malware protection beyond traditional hand- grounded antivirus. Integration between Endpoint Discovery and Response platforms and Security Information and Event operation systems enables automated incident unity — segregating a compromised host at the network switch harborage position through Security Operations Center robotization playbooks touched off by Endpoint Discovery and Response telemetry cautions.

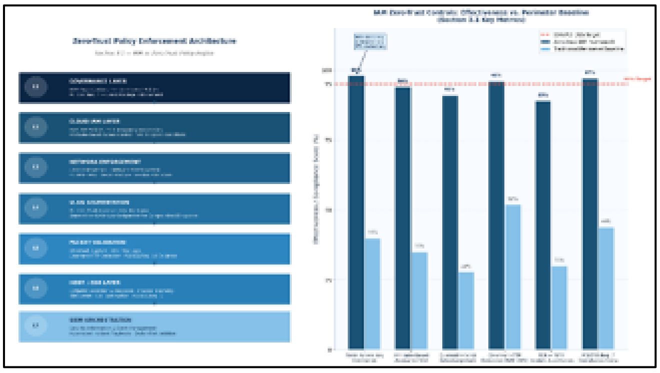

**Figure 1** Tool Ecosystem for Full Lifecycle Automation [5, 6]

## 4. SD-wan for retail store-to-cloud connectivity

### 4.1. SD-WAN Architecture for Indian Retail Enterprises

Software-Defined Wide Area Network technology decouples Wide Area Network control logic from physical transport, enabling centralized policy orchestration across geographically distributed retail sites without requiring per-device configuration changes. For Indian retail enterprises operating stores across Hyderabad and neighboring regions, Software-Defined Wide Area Network replaces traditional Multiprotocol Label Switching circuits—expensive, inflexible, and slow to provision—with dynamically policy-routed overlays that run across broadband internet, Long-Term Evolution, and dedicated fiber simultaneously. Application-aware routing engines classify traffic in real time and steer Payment Card Industry Data Security Standard-sensitive payment streams over the most secure and stable available path while routing non-critical inventory synchronization traffic over lower-cost broadband links. This capability satisfies Payment Card Industry Data Security Standard Requirement 1 by ensuring that cardholder data always traverses network segments governed by documented, enforced routing policy. [7, 8]

Software-Defined Wide Area Network edge appliances deployed at retail store locations establish encrypted overlay tunnels to the enterprise network hub—typically an Amazon Web Services region hosting the payment processing back end or a datacenter running F5 BIG-IP in front of payment application servers. Internet Protocol Security or Transport Layer Security tunnels encapsulate all store-to-hub traffic, preventing eavesdropping on broadband carrier networks. Dual-homed store appliances maintain active tunnels over both primary and secondary internet connections simultaneously, enabling sub-second failover that prevents payment transaction interruption during primary link outages. Mean time to failover in well-configured Software-Defined Wide Area Network deployments falls below five hundred milliseconds, a threshold imperceptible to point-of-sale terminals operating on standard transaction timeout windows.

For associations with being Logical Volume director (LVM) glass configurations similar as those using pvmove to resettle data between physical volumes during SAN conservation - AWS EBS shots give a similar non-disruptive migration capability. shots capture the point- in- time state of an EBS volume and can be copied across Vacuity Zones or AWS Regions, enabling cutover strategies with minimum time-out. CloudWatch monitoring integration, deployable via Terraform's AWS provider, provides real- time visibility into EBS outturn, quiescence, and line depth criteria, replacing on- demesne tools similar as Nagios or Grafana- integrated storehouse dashboards.

**Table 2** SAN-to-EBS Migration: Component Equivalency and Terraform Provisioning [7, 8]

| SD-WAN Capability | Retail Application | Security Benefit | Compliance Alignment |
|---|---|---|---|
| Application-Aware Routing | Payment Stream Prioritization | Cardholder Data Path Governance | PCI DSS Requirement 1 |
| Dual-Homed Failover | Point-of-Sale Continuity | Availability Assurance | PCI DSS Requirement 12 |
| Centralized Policy Push | Store Security Profile Enforcement | Consistent Configuration Control | PCI DSS Requirement 2 |
| Edge Compute Integration | Local Catalog and Transaction Cache | Reduced Breach Surface | PCI DSS Requirement 6 |

## 5. Out-of-band automation and infrastructure resilience

### 5.1. Baseboard Management Controller Automation Through Redfish API

Out-of-band management infrastructure provides the foundational layer of datacenter resilience that in-band software tools cannot guarantee. When a hypervisor crash, ransomware infection, or kernel panic renders a server's primary management interface inaccessible, the Baseboard Management Controller accessed through Integrated Lights-Out on Hewlett Packard Enterprise hardware or Integrated Dell Remote Access Controller on Dell infrastructure remains operational on a dedicated management network segment. This separation of management plane from data plane constitutes a critical zero-trust boundary—administrators authenticate to Baseboard Management Controller interfaces through dedicated management VLANs isolated from production traffic, preventing lateral movement from a compromised production environment into the hardware management layer. Automating Baseboard Management Controller interactions through Redfish Application Programming Interface calls—the industry-standard Representational State Transfer interface for server management—eliminates manual console access for routine configuration tasks, reducing human error and accelerating provisioning timelines. [9, 10]

Basic Input Output System configuration automation through Integrated Lights-Out and Integrated Dell Remote Access Controller Application Programming Interfaces ensures that every server in a hybrid datacenter fleet boots with a verified, security-hardened firmware configuration. Baseboard Management Controller scripting platforms—Ansible roles using the community.general.redfish modules or Python scripts invoking the python-redfish library—push Basic Input Output System settings including Secure Boot enforcement, legacy boot mode disablement, and Intelligent Platform Management Interface over Local Area Network deactivation to entire server fleets simultaneously. Secure Boot prevents unauthorized bootloader and kernel module loading, a critical control for Payment Card Industry Data Security Standard-scoped hosts where the integrity of the boot chain must be verifiable. Automated compliance drift detection compares live Basic Input Output System configurations against golden templates on a scheduled basis, raising alerts when unauthorized changes appear.

Redundant Array of Independent Disks management through out-of-band controllers provides storage resilience without requiring operating system access. Integrated Lights-Out and Integrated Dell Remote Access Controller interfaces expose Redundant Array of Independent Disks controller status, physical disk health metrics, and logical volume rebuild progress through both web console and Application Programming Interface endpoints. Automated monitoring scripts poll Redundant Array of Independent Disks controller status every five minutes and trigger immediate alerts when physical disk predictive failure attributes—Surface Scan Error Count, Reallocated Sector Count, or Spin Retry Count—exceed threshold values. Proactive hot spare promotion, scripted through Redfish Chassis Manager calls, initiates array rebuild before a degraded disk fails completely, maintaining storage redundancy continuously. In Payment Card Industry Data Security Standard environments, verified Redundant Array of Independent Disks integrity satisfies availability requirements and provides audit-ready evidence of storage resilience.

Hewlett Packard Enterprise OpenView and BMC Helix provide the enterprise management platforms through which out-of-band telemetry integrates with broader IT operations workflows. Hewlett Packard Enterprise OpenView Network Node Manager ingests Simple Network Management Protocol traps from Baseboard Management Controller interfaces, correlating hardware alerts with network topology maps to identify whether a failing server affects Payment Card Industry Data Security Standard-scoped network segments. BMC Helix IT Service Management automates incident creation, routing, and escalation when Integrated Lights-Out or Integrated Dell Remote Access Controller alerts trigger, ensuring that hardware failures receive appropriate response priority based on the business criticality of affected workloads. This integration between physical infrastructure telemetry and Information Technology Service Management workflows satisfies Payment Card Industry Data Security Standard Requirement 12 by documenting a formal incident response process with measurable response time commitments.

The compound effect of out-of-band automation, zero-trust network enforcement, hybrid load balancing, and Software-Defined Wide Area Network connectivity creates a datacenter architecture that functions as a coherent security system rather than a collection of independently managed components. Lead architects who command this full-stack discipline—spanning F5 pool configuration, Amazon Web Services Identity and Access Management policy design, Cisco and Brocade VLAN engineering, Software-Defined Wide Area Network policy orchestration, and Baseboard Management Controller automation—occupy a rare position in the market. CompTIA Security+ CSO-003 certification validates foundational security knowledge, while practical experience managing fifty-plus F5 pools at one hundred gigabits per second throughput and automating Baseboard Management Controller provisioning across hybrid server fleets demonstrates the operational mastery that differentiates lead architects from senior engineers. The 2026 Software-Defined Wide Area Network market expansion amplifies demand for this skill combination, creating career trajectory opportunities that few technical disciplines currently match.

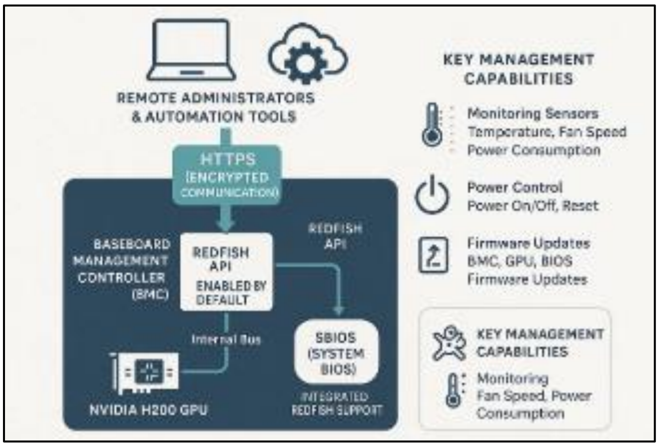

**Figure 2** Baseboard Management Controller Automation Through Redfish API [9, 10]

## 6. Conclusion

Hybrid network security architecture emerges from the intersection of on-premises expertise and cloud-native engineering discipline. The synthesis of F5 BIG-IP pool management, Amazon Web Services Application Load Balancer and Web Application Firewall integration, zero-trust Identity and Access Management policy enforcement, Wireshark-validated traffic inspection, Software-Defined Wide Area Network retail connectivity, and out-of-band Baseboard Management Controller automation delivers a security posture that satisfies Payment Card Industry Data Security Standard requirements comprehensively while sustaining the performance demands of modern enterprise workloads.

Organizations that implement this architecture achieve measurable security outcomes: exploit reduction rates exceeding ninety-five percent against OWASP Top Ten categories, sub-second failover for retail store-to-cloud connectivity, verified Secure Boot chain integrity across the entire datacenter fleet, and continuous monitoring evidence that satisfies Payment Card Industry Data Security Standard audit requirements without manual data collection. The integration of Hewlett Packard Enterprise OpenView and BMC Helix platforms with out-of-band management telemetry provides the holistic visibility that Security Operations Centers require to detect and respond to threats across physical and virtual infrastructure simultaneously.

The architect who masters this full-stack discipline—bridging the Cisco and Brocade switching layer, the F5 application delivery tier, the Amazon Web Services cloud-native control plane, the Software-Defined Wide Area Network edge, and the Baseboard Management Controller automation framework—commands a professional profile that the 2026 market rewards with Lead Architect designation. Subnet mastery, Storage Area Network Volume Object Data edge resilience design, and CompTIA Security+ CSO-003 certification validation together constitute the credential set that defines elite hybrid network security practice. The practical significance of this architecture extends beyond individual career advancement: retail enterprises, financial institutions, and healthcare organizations that deploy these integrated controls protect their customers, their revenue, and their regulatory standing against a threat landscape that continues to grow in sophistication.

## References

[1] Scott Rose (2020). "Zero trust architecture," National Institute of Standards and Technology Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[2] PCI, Security Standards Council (2016). "Guidance for PCI DSS Scoping and Network Segmentation," https://listings.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf

[3] Doug Barney, (2023) "What is an Application Delivery Controller (ADC)?". https://kemptechnologies.com/blog/what-is-an-application-delivery-controller-(adc)-and-why-should-you-use-one

[4] Andrzej Mycek, (2023). MULTI-LAYERED SECURITY OF WEB APPLICATIONS IN CLOUD ENVIRONMENTS USING WAF, ZERO TRUST, AI-DRIVEN THREAT DETECTION, AND RASP. https://www.scs-europe.net/dlib/2025/ecms2025acceptedpapers/0262_secmos_ecms2025_0061.pdf

[5] Scott W. Rose. (2020). "Zero Trust Architecture," NIST Publication. https://www.nist.gov/publications/zero-trust-architecture

[6] Vincent C. Hu et al., (2014). "Guide to Attribute Based Access Control (ABAC) Definition and Considerations," NIST Special Publication 800-162. https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview

[7] Paloalto (2023). What Is SD-WAN Architecture? Components, Types, & Impacts. Network World Research Report, 14(2), 55–78. https://www.paloaltonetworks.in/cyberpedia/sd-wan-architecture

[8] Ramesh, V., & Krishnamurthy, B. (2024). Software-defined Wide Area Network (SD-WAN) Market. https://www.marketsandmarkets.com/PressReleases/software-defined-wan.asp

[9] Airowire, (2020). Use Case: Fortigate SD-WAN Implementation Across PAN India Using Fortimanager. https://airowire.com/use-case-sd-wan-software-define-wide-area-network-implementation-across-pan-india/

zongzhaoning Kang, (2023). Theory and Application of Zero Trust Security: A Brief Survey. https://www.researchgate.net/publication/376022602_Theory_and_Application_of_Zero_Trust_Security_A_Brief_Survey