Secure SD-WAN Network Architecture for a Multi-Site Enterprise

Overview

This project presents the design of a future-state secure network architecture for a rapidly growing multi-site enterprise. The goal was to replace a fragile, inconsistent WAN design with a scalable, fault-tolerant, and security-first SD-WAN architecture capable of supporting business expansion, cloud integration, and modern collaboration workloads.

The design prioritizes availability, performance, and security, while maintaining operational simplicity through standardization and centralized management.

Business & Security Challenges

- Inconsistent security controls across sites
- Single points of failure in WAN connectivity
- Lack of firewall protection at some locations
- Limited scalability for rapid workforce growth
- Increasing reliance on voice, video, and cloud services

Architecture Goals

- High availability through redundancy and failover
- Consistent security controls across all sites
- Scalability for rapid user and site growth
- Performance optimization for voice and video traffic
- Centralized visibility and monitoring
- Zero Trust access principles

Proposed Network Architecture

Dual-Hub SD-WAN Topology

- Primary hub: Dallas

- Secondary / disaster recovery hub: Houston
- Spoke sites: Memphis, Kansas City
- Dual business-class ISP connections at each hub
- Encrypted SD-WAN tunnels interconnecting all sites

Security Enhancements

- Next-Generation Firewalls (NGFWs) deployed at every site
- Zero Trust Network Access (ZTNA) principles
- Multi-Factor Authentication (MFA) for users and administrators
- Centralized logging and monitoring using SIEM and NetFlow
- Deep packet inspection and intrusion prevention

Network Segmentation & Access Control

- Data VLAN
- Voice VLAN
- Video VLAN
- Server VLAN
- Management VLAN
- Guest VLAN
- Inter-VLAN restrictions using ACLs and 802.1X

Performance & Reliability

- Quality of Service (QoS) policies for voice and video
- Centralized VoIP services with Session Border Controller
- Prioritized latency-sensitive traffic across SD-WAN paths
- Redundant core switches and multi-ISP connectivity
- Service replication between hubs for business continuity

Future-Proofing & Automation

- IPv6 dual-stack readiness
- Template-based site deployment
- Automated provisioning and configuration management

- Compatibility with cloud services and IoT expansion

Key Deliverables

- Secure dual-hub SD-WAN architecture design
- Enterprise-wide security standardization
- Network segmentation and access control strategy
- Redundancy and disaster recovery planning
- Future-ready addressing and automation approach

Skills Demonstrated

- Enterprise network architecture design
- SD-WAN and WAN security
- Zero Trust networking concepts
- Firewall and segmentation strategy
- Network resilience and redundancy planning
- Translating business requirements into secure infrastructure

Outcome & Impact

This design delivers a secure, scalable, and resilient enterprise network that eliminates single points of failure, enforces consistent security controls across all locations, improves performance for collaboration and cloud workloads, supports rapid organizational growth, and reduces operational and cybersecurity risk.

What I Would Improve Next

- Deploy real-time threat detection rules within the SIEM
- Integrate endpoint telemetry for stronger Zero Trust enforcement
- Conduct failover and disaster recovery simulations
- Implement automated compliance checks for network configurations