Fortinet SD-WAN
Design Guide

Enterprise Network Architecture and Implementation

BlackHawk Data

blackhawk11.com

EXECUTIVE SUMMARY

Software-Defined Wide Area Network (SD-WAN) technology has revolutionized how organizations connect their distributed locations. This design guide provides comprehensive guidance for implementing Fortinet Secure SD-WAN, combining advanced networking capabilities with industry-leading security.

Fortinet's integrated approach delivers a single-vendor solution that simplifies operations, reduces costs, and ensures consistent security policy enforcement across all locations. This guide covers architectural patterns, deployment models, and best practices validated through enterprise deployments.

SD-WAN OVERVIEW

Technology Benefits

SD-WAN addresses key challenges faced by traditional WAN architectures:

- Reduced bandwidth costs through intelligent traffic steering across multiple links
- Improved application performance with dynamic path selection based on real-time conditions
- Simplified branch operations with zero-touch deployment and centralized management
- Enhanced visibility into application performance and network health
- Rapid service provisioning without truck rolls or on-site configuration

Fortinet Secure SD-WAN

Fortinet Secure SD-WAN differentiates itself through native security integration:

Feature	Description	Benefit
NGFW Integration	FortiGate security platform built into SD-WAN	Single device for networking and security
Application Awareness	7-layer application identification	Granular traffic control and prioritization
AI-Powered Analytics	FortiAI for anomaly detection	Proactive threat and performance management
Zero Trust Access	ZTNA integration with SD-WAN	Secure access for remote users and IoT

Table 1: Fortinet Secure SD-WAN Key Features

DESIGN PRINCIPLES

Underlay Network Design

The underlay network provides the physical connectivity foundation. Best practices include:

1. Diverse connectivity: Combine MPLS, broadband, LTE/5G for redundancy
2. Provider diversity: Use different ISPs to minimize single points of failure
3. Adequate bandwidth: Size links for peak traffic plus 30% growth headroom

4. SLA alignment: Match link types to application requirements

Overlay Architecture

The SD-WAN overlay creates a virtual network abstracted from the physical infrastructure. Key considerations:

- Use ADVPN (Auto-Discovery VPN) for dynamic tunnel establishment
- Implement proper BGP design for scalable route distribution
- Configure SD-WAN zones to segment traffic by security requirements
- Enable WAN optimization for latency-sensitive applications

DEPLOYMENT MODELS

Hub-and-Spoke

The hub-and-spoke model centralizes traffic through designated hub locations. This design is ideal for:

- Organizations with centralized security inspection requirements
- Deployments where most traffic flows to/from data centers
- Simplified routing and policy management

Full Mesh

Full mesh connectivity allows direct site-to-site communication without traversing a hub. Benefits include:

- Optimized latency for site-to-site traffic
- Reduced bandwidth requirements at hub locations
- Improved resilience with multiple paths between any two sites

Partial Mesh

Partial mesh provides a balanced approach, connecting high-traffic sites directly while routing other traffic through hubs. This model offers:

- Cost-effective middle ground between hub-and-spoke and full mesh
- Flexibility to optimize for specific traffic patterns
- Scalable growth as the organization expands

SECURITY INTEGRATION

Fortinet's security fabric integrates seamlessly with SD-WAN deployments:

Security Function	Implementation	Best Practice
Firewall	FortiGate NGFW at each location	Enable all security profiles for internet-bound traffic

IPS	Inline inspection on all links	Use recommended IPS profile with appropriate filters
Web Filtering	Category-based URL filtering	Block high-risk categories, monitor others
Antivirus	Real-time file scanning	Enable on all protocols including encrypted traffic
Sandboxing	FortiSandbox integration	Submit unknown files for behavioral analysis

Table 2: Security Integration Matrix

BEST PRACTICES

Based on enterprise deployments, BlackHawk Data recommends the following best practices:

5. Start with a pilot deployment: Validate design assumptions in a controlled environment
6. Define clear SLAs: Establish performance baselines and acceptable thresholds
7. Implement change management: Document procedures for policy updates and configuration changes
8. Monitor continuously: Use FortiManager and FortiAnalyzer for centralized visibility
9. Plan for growth: Design for 3-5 year capacity requirements
10. Train operations staff: Ensure teams understand SD-WAN concepts and troubleshooting

CONCLUSION

Fortinet Secure SD-WAN provides a robust foundation for modern enterprise networking. By following the design principles and best practices outlined in this guide, organizations can achieve improved application performance, reduced costs, and enhanced security posture.

For assistance with SD-WAN design, deployment, or optimization, contact BlackHawk Data network architects at blackhawk11.com.