Sirvis

White Paper Summary

Fortinet SD-WAN Infrastructure Modernization

White Paper Summary

Fortinet SD-WAN Infrastructure Modernization

Overview

We have partnered to modernize its wide-area network by deploying a comprehensive **Fortinet Secure SD-WAN** solution across more than twenty clinical and administrative sites. This transformation initiative replaces legacy WAN architecture with a secure, scalable, and application-aware infrastructure built on **FortiGate Next-Generation Firewalls**, **cloud-hosted management**, and **Zero Trust–aligned endpoint controls**. The implementation was documented in **September 2025**, and represents a full-stack redesign incorporating network, security, and endpoint management modernization.

Strategic Objectives

The project was designed to deliver the following outcomes:

- **Stronger Security Posture**
  Integration of Next-Generation Firewall (NGFW) services, IPS, AV, DNS filtering, web filtering, SSL inspection, and geolocation controls.

- **Improved Application Performance**
  Intelligent SD-WAN path selection, latency/jitter/packet-loss SLAs, and application-aware routing to optimize clinical applications, VoIP/Zoom Phone, and cloud services.

- **Operational Agility & Centralized Management**
  Unified management using **FortiManager Cloud**, analytics via **FortiAnalyzer Cloud**, and endpoint control through **FortiClient EMS Cloud**.

- **Cost Optimization & Resiliency**
  Dual-WAN designs with dynamic failover reduce dependence on private circuits while improving reliability and uptime across all sites.

Solution Architecture

1. Network & Hardware Foundation

Each of 19 sites received FortiGate appliances sized to its role—models **61F, 81F, 101F, and 201F**.
Common components per site include:

- **Dual WAN circuits** (static or DHCP)
- **VLAN segmentation** for clinical, guest, voice, and internal networks
- **IPSec S2S tunnels** to the central data center (dual tunnel per site)
- **OSPF routing** for dynamic branch-to-data-center connectivity

This creates a consistent, resilient network design across all locations.

---

2. SD-WAN Design

SD-WAN Zones

All sites share two standardized zones:

- **CH_SD_WAN_INTERNET** — all Internet-bound traffic
- **CH_SD_WAN_DC** — secure internal traffic routed to the data center

SD-WAN Members & Path Selection

Members include:

- WAN1 and WAN2 Internet circuits
- S2S tunnel interfaces for DC traffic

SLAs define performance thresholds (e.g., 250ms latency, 50ms jitter, ≤5% packet loss), enabling real-time path selection.

Traffic Prioritization Rules

Typical rule sets include:

- **Zoom Phone / Voice prioritization**
- **Branch-to-Datacenter routing via SLA**

- **Guest Internet isolation**
- **Application-aware routing using SLA-based fallbacks**

This ensures latency-sensitive workloads receive the best available path.

---

3. Security Architecture

Each site deploys a consistent, layered security stack:

- **Next-Generation Firewall** policies governing internal, guest, and DC traffic
- **Geolocation Blocking** to restrict high-risk regions
- **Content & Threat Protection**
    - CH-WebFilter (web filtering)
    - CH-IPS (intrusion prevention)
    - CH-AntiVirus
    - CH-DNS Filters for internal and guest networks
    - Application control ("block-high-risk")

Security is uniformly enforced across all branches with centralized policy templates.

---

4. IPSec VPN Architecture

All sites maintain redundant IPSec tunnels to the customer Data Center.

- **IKEv2** across all peers
- Strong crypto proposals **(AES256-GCM, AES256-SHA256)**
- Encrypted pre-shared keys
- **DPD-enabled** for rapid failover
- **No NAT traversal** when not required

This creates a hardened, redundant, encrypted backbone across the entire enterprise.

---

5. Routing Architecture

Static Routing

- Default routes placed into the SD-WAN Internet zone at each site.

Dynamic Routing – OSPF

- Each site operates OSPF with:
  - Unique router IDs tied to tunnel addressing
  - Area 0.0.0.0
  - Point-to-point adjacency over IPSec tunnels
  - Route advertisements for all internal VLANs

This enables scalable, automated branch-to-core routing.

---

6. Endpoint Protection & Zero Trust (FortiClient EMS Cloud)

Customer adopted FortiClient EMS Cloud for **Zero Trust–aligned endpoint security** and unified endpoint policy enforcement.

Key EMS capabilities deployed:

On/Off-Fabric Detection

- Automatically identifies whether a device is on a trusted network
- Applies appropriate enforcement via:
  - Local FortiGate firewall (on-fabric)
  - EMS policies (off-fabric)

Remote Access VPN Profile

- Auto-provisioned IPsec VPN
- Ensures consistent, secure remote access
- Reduces configuration errors and support overhead

ZTNA Destination Profiles

- App-level identity enforcement (e.g., internal vCenter access)

- Eliminates need for full tunneling for internal resources

Web & Video Filtering

- Category/risk-based filtering for browsing and media usage
- Reduces threats & protects bandwidth for clinical applications

System Hardening Policies

- OS-level protection
- Anti-tamper settings
- Device compliance enforcement

EMS Tags

Dynamic endpoint tagging based on:

- Risk level
- Domain membership
- OS type
- User
- Compliance status

Tags automatically map endpoints to the correct security policies.

---

7. Centralized Cloud Management Stack

FortiManager Cloud

- Centralized provisioning
- Policy packages per site
- Unified SD-WAN templates

FortiAnalyzer Cloud

- Log aggregation and long-term retention
- Analytics dashboards for security, SD-WAN performance, VPN uptime
- Automated reports and compliance insights

FortiClient EMS Cloud

- Endpoint visibility
- Zero Trust enforcement
- Remote access and ZTNA orchestration

Together, these services provide a **single-pane-of-glass operations model** for customer.

Conclusion

The Fortinet SD-WAN deployment at customer represents a **holistic modernization of network, security, and endpoint management infrastructure**.

By standardizing on FortiGate NGFW appliances, implementing dual-WAN SD-WAN intelligent routing, strengthening security with advanced UTM features, and introducing Zero Trust endpoint controls through EMS Cloud, customer now operates a highly resilient, secure, scalable, and centrally managed network.

This architecture supports the organization's mission-critical clinical operations, improves performance for providers and staff, and significantly elevates cybersecurity maturity across all locations.