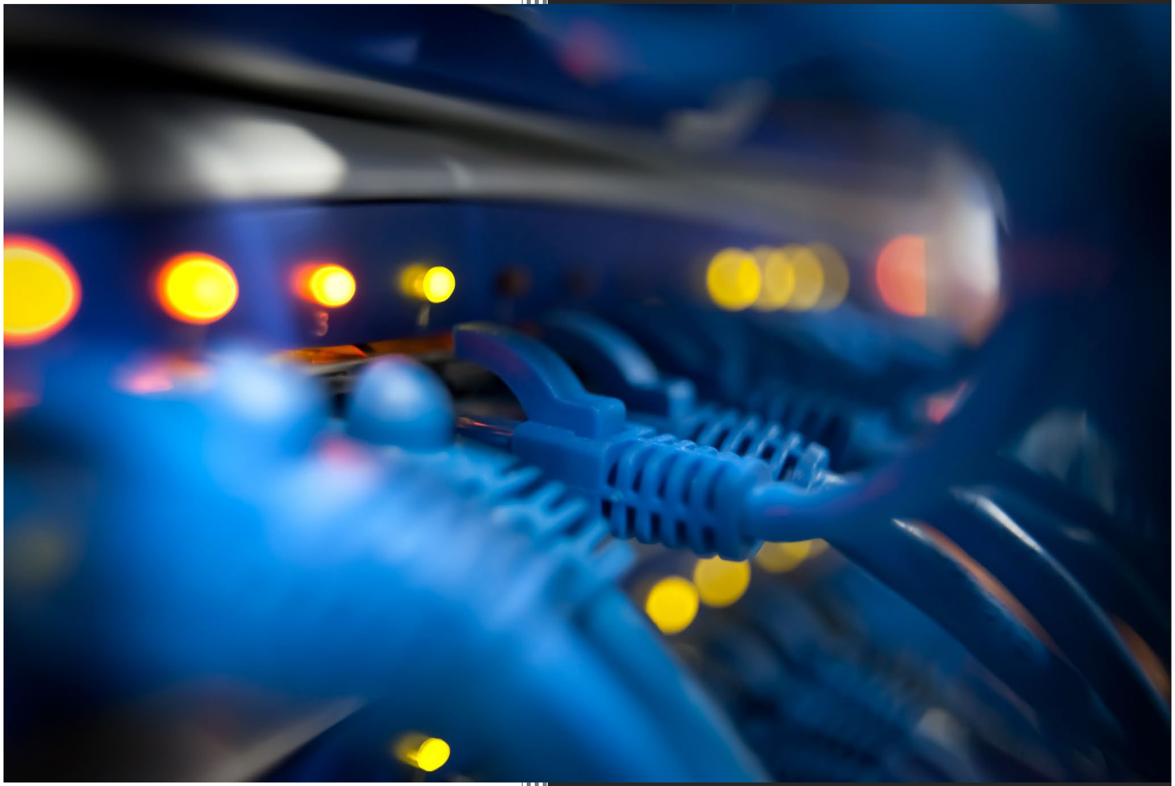
2025

Enterprise Network Architecture Proposal



Gabrielle Decker

ITD-3543 Enterprise Networking

1/1/2025

1 TABLE OF CONTENTS

2 Executive Summary: A Strategic Investment in Your Company's Future

2.1 The Business Challenge

The company stands at a pivotal moment, with a clear trajectory for growth from its current 300-500 employees. However, this ambition is constrained by an implied network infrastructure that is rapidly approaching its limits. The increasing reliance on cloud-based applications, the critical need for seamless and reliable collaboration between the two corporate offices, and the escalating sophistication of cybersecurity threats demand a fundamental re-evaluation of the company's digital backbone. Continuing with the status quo will inevitably lead to performance bottlenecks that stifle productivity, service outages that impact revenue, and security vulnerabilities that expose the company to significant financial and reputational risk. The current network is not a platform for growth; it is a barrier to it.

2.2 The Proposed Solution

This proposal outlines a comprehensive redesign of the enterprise network, transforming it from a liability into a strategic business enabler. The new architecture is built upon three foundational pillars designed to directly support the company's long-term objectives:

- **Scalability**: A modular, hierarchical network design that provides a repeatable blueprint for growth. This architecture can accommodate a growing workforce and the addition of new office locations without requiring costly and disruptive redesigns.
- **Resilience**: A highly available infrastructure featuring two internet providers per site with SD-WAN technology. If one provider fails, traffic shifts automatically in seconds. This ensures business continuity by providing intelligent, automatic failover for inter-office and internet connectivity, virtually eliminating downtime caused by provider outages.
- **Security**: A modern security framework founded on Zero Trust principles. This proactive approach means a user must prove who they are and that their device is healthy before they get access. This trust is continually re-checked, and if anything looks wrong, access is reduced or blocked to protect critical company assets.

2.3 Key Business Benefits

The implementation of this new network architecture will yield tangible and significant business advantages, including:

- **Enhanced Productivity**: By optimizing traffic for critical cloud and voice applications and providing high-speed, reliable connectivity, employees will experience a faster, more responsive network, enabling them to work more efficiently.
- **Reduced Operational Risk**: A multi-layered, Zero Trust security posture dramatically reduces the company's attack surface and contains the impact of potential breaches. Furthermore, the resilient, high-availability design minimizes the risk of costly downtime, ensuring business operations continue uninterrupted.

- **Future-Proofed Investment**: The proposed architecture is not a short-term fix. It is a strategic platform designed to seamlessly integrate with future cloud services, support a growing and increasingly remote workforce, and scale cost-effectively as the company expands.

2.4 The Investment

This strategic initiative requires a total estimated initial investment (Capital Expenditure) of $61,420. This includes all necessary hardware and professional services for design, installation, and configuration. The annual recurring costs (Operational Expenditure) for security subscriptions, software licensing, and support are estimated at $13,094. This investment is essential to build the secure, scalable, and resilient foundation required to support the company's strategic growth plan over the next three to five years.

3 Proposed Network Architecture: A Foundation for Growth and Reliability

This section details the core design philosophy, explaining the foundational models and technologies chosen to create a network that is not only powerful and reliable today but is also inherently prepared for the challenges and opportunities of tomorrow.

3.1 The Hierarchical Network Model: Built for Scalability

The proposed internal network at each office is based on the industry-standard three-tier hierarchical model, a design methodology proven to deliver scalability, performance, and simplified management. This model logically divides the network into distinct layers, each with a specific function.

- **The Access Layer**: This is the entry point to the network where end-user devices connect. Switches at this layer provide connectivity and enforce initial security policies like port security and VLAN assignment.
- **The Distribution Layer**: This layer serves as the aggregation point for all Access layer switches. At each site, two core switches will act as a single logical system for speed and resilience, forming a 10G/25G backbone. Every access layer switch will uplink to both core switches at 10 Gbps. This design uses fast-converging protocols like RSTP for Layer 2 stability and VRRP/MLAG for first-hop Layer 3 redundancy, ensuring high availability.
- **The Collapsed Core**: For a mid-sized company, a full three-tier implementation is unnecessary. This design utilizes a "collapsed core" architecture, where the functions of the Core and Distribution layers are combined into the single, resilient, high-performance distribution block at each site. This provides high-speed routing in a cost-effective package suited to the company's scale.

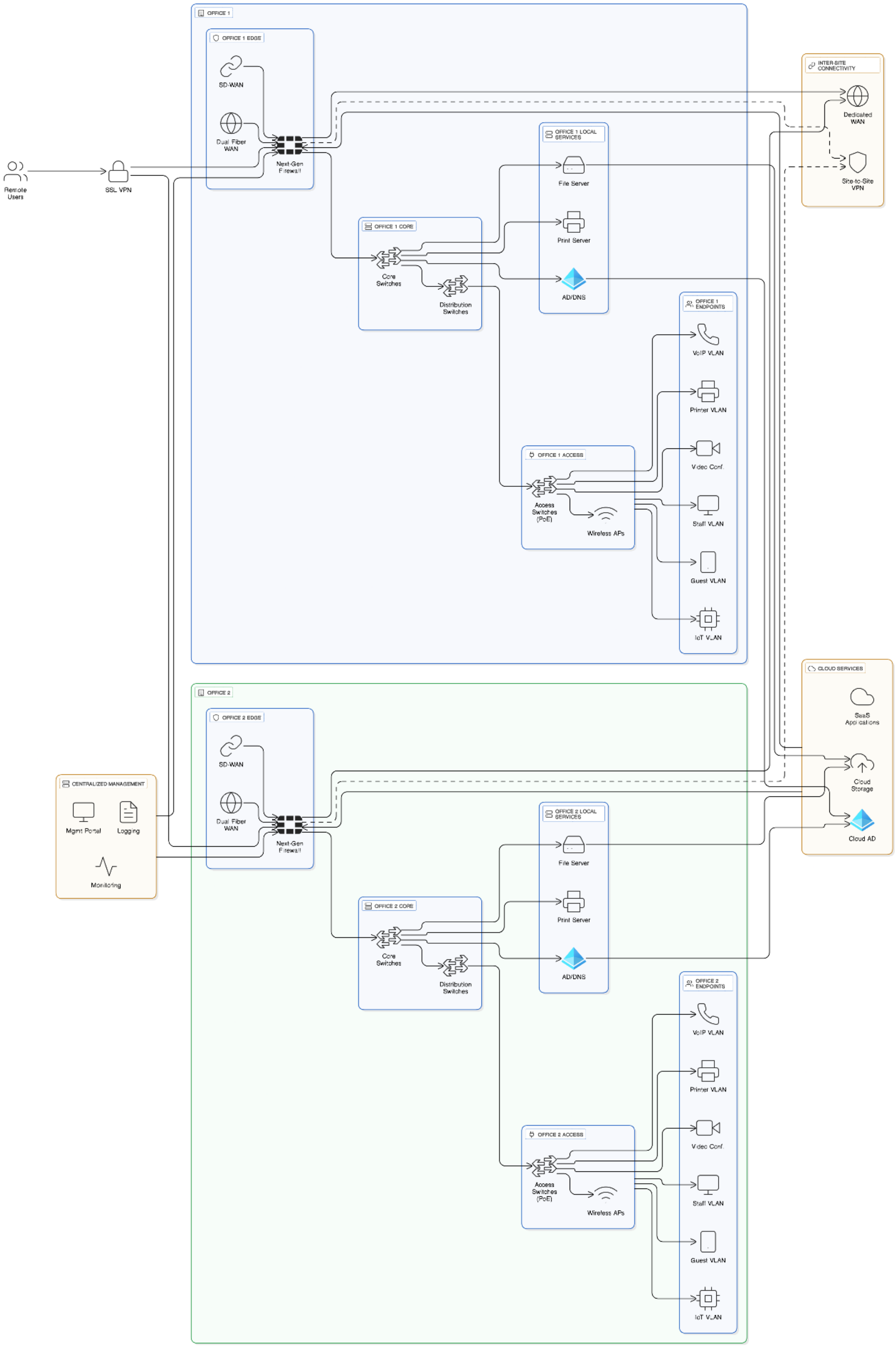


Figure 1 High-Level Network Topology. View full size here.

3.2 Inter-Office Connectivity with Software-Defined WAN (SD-WAN)

To connect the two offices and provide access to cloud services, this design leverages a modern Software-Defined WAN (SD-WAN) approach, eliminating the need for expensive and rigid private circuits like MPLS. Each office will be equipped with two independent internet connections from diverse providers and a tertiary cellular (LTE/5G) connection. During implementation, provider diversity will be fully documented (confirming separate last-mile media, physical paths, and building entry points), and any residual risks from shared conduits will be identified. An SD-WAN appliance at each site will manage all three connections, delivering superior performance and resilience.

Key Benefits of This SD-WAN Approach Include:

- **Application-Aware Routing**: The system will be configured with application-level SLAs (defining acceptable loss, latency, and jitter) for critical services like voice, video, M365, and Zoom. It will then intelligently steer traffic over the best-performing path in real-time to meet these SLAs and ensure a high-quality user experience.
- **Automatic Failover and Increased Uptime**: If a primary internet connection fails, traffic is seamlessly rerouted over the secondary or tertiary links in seconds, with no disruption to end-users, dramatically increasing business continuity.
- **Direct Cloud Access**: SD-WAN provides a secure, direct internet breakout at each office. Critical SaaS traffic (for services like Microsoft 365, Zoom, and Salesforce) will be split-tunneled locally, sending it straight to the internet. This avoids inefficiently backhauling or "hairpinning" traffic through a central site, which significantly reduces latency.
- **Centralized Management and Cost Savings**: The entire multi-site WAN is managed from a single cloud-based dashboard, simplifying administration and reducing overhead. Using affordable broadband and cellular internet connections instead of costly MPLS circuits delivers superior performance at a fraction of the cost.

4 Logical Network Design: Ensuring Security and Performance Through Segmentation

A well-structured logical design is paramount for enhancing security, optimizing performance, and simplifying administration. This is achieved through strategic IP addressing and the implementation of Virtual Local Area Networks (VLANs).

4.1 Strategic IP Addressing and VLAN Segmentation

The design strategy is to maintain a small number of business-based segments (e.g., staff, servers, voice, guests, IoT). All traffic between these segments will be blocked by default, with access granted only by specific business role and need. VLANs are the technology used to create these logical segments, isolating groups based on function regardless of physical location. The core security policy is to deny all inter-VLAN traffic by default, with firewall rules permitting only the specific ports and protocols necessary for business operations. This practice provides critical benefits:

- **Enhanced Security**: By creating virtual boundaries, security threats are contained. If a device on the guest VLAN becomes compromised, the infection is confined and prevented from moving laterally to access sensitive corporate data.
- **Improved Performance**: Dividing the network into smaller broadcast domains with VLANs reduces unnecessary "chatter," which reduces network congestion and leads to a faster user experience.
- **Simplified Administration**: Grouping devices logically allows administrators to apply specific security and traffic policies to entire groups at once, simplifying configuration and troubleshooting.

A hierarchical IP addressing plan will be implemented, with each office assigned a unique block and smaller subnets allocated to each VLAN, ensuring no overlaps and reserving space for future growth.

This table will be replicated at each office with a unique IP subnet range.

Table 1 Proposed VLAN and IP Subnet Plan

VLAN ID	VLAN Name	Purpose / User Group	IP Subnet (Office 1 Example)	Security Posture
10	Management	Network Infrastructure (Switches, APs, Firewalls)	10.10.10.0/24	Highly Restricted, IT Admin access only
20	Corporate Data	Employee Desktops, Laptops, and Trusted Devices	10.10.20.0/23	High Trust, access to internal servers and applications
30	VoIP	Voice over IP Handsets and Conferencing Systems	10.10.30.0/24	High Priority (QoS), access to voice services only
40	Printers	Networked Printers and Scanners	10.10.40.0/24	Medium Trust, limited access to/from Corporate Data VLAN
50	IoT	Smart Devices, Security Cameras, Building Controls	10.10.50.0/24	Untrusted, isolated, internet access via proxy if needed
60	Servers	On-Premise File Servers, Domain Controllers	10.10.60.0/24	Highly Restricted, access controlled by firewall rules
99	Guest Wireless	Guest and Visitor Personal Devices	10.10.99.0/24	Untrusted, internet only, fully isolated from all internal networks

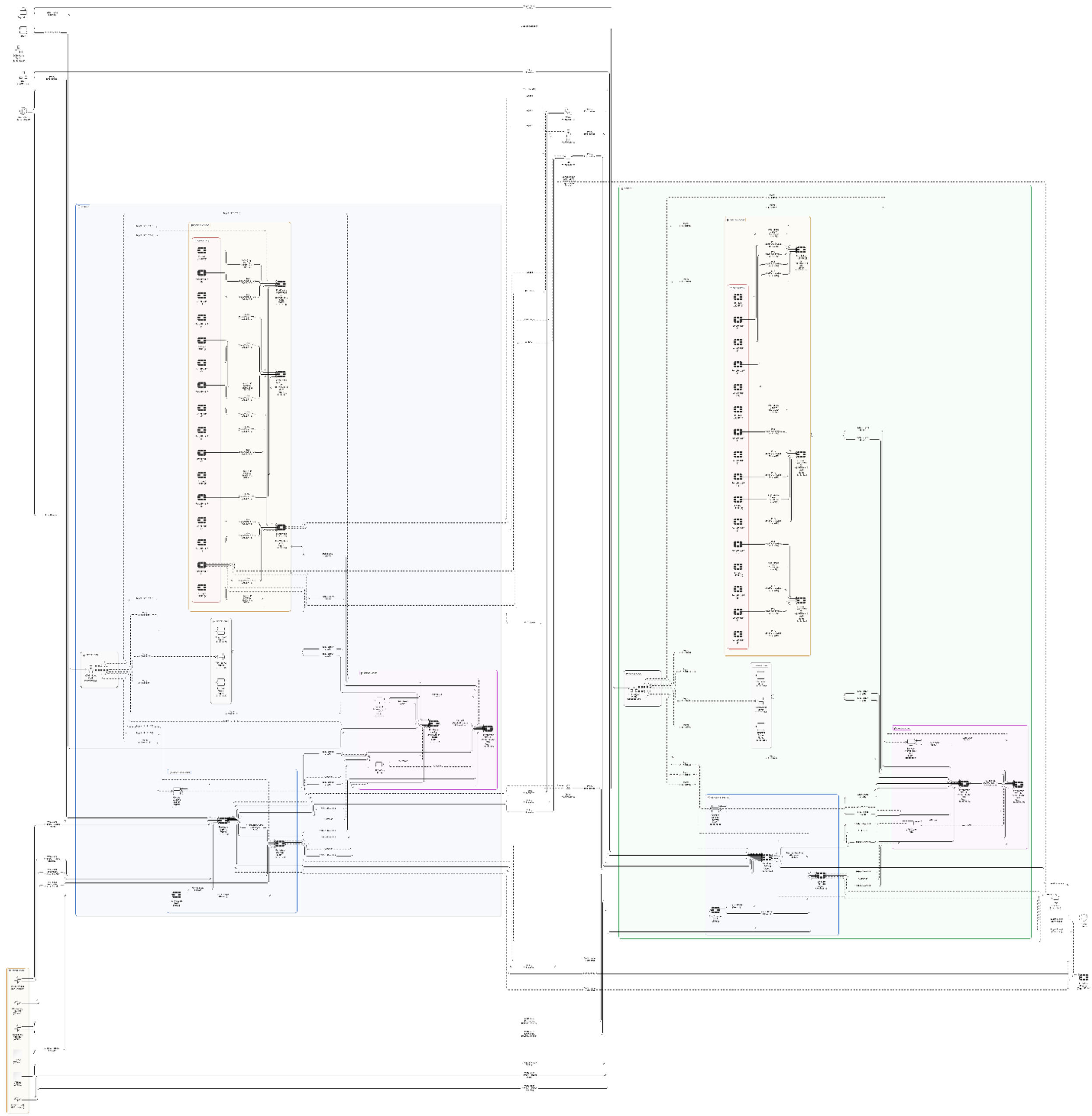


Figure 2 Physical Infrastructure Implementation of VLAN Segmentation Strategy. View full size here.

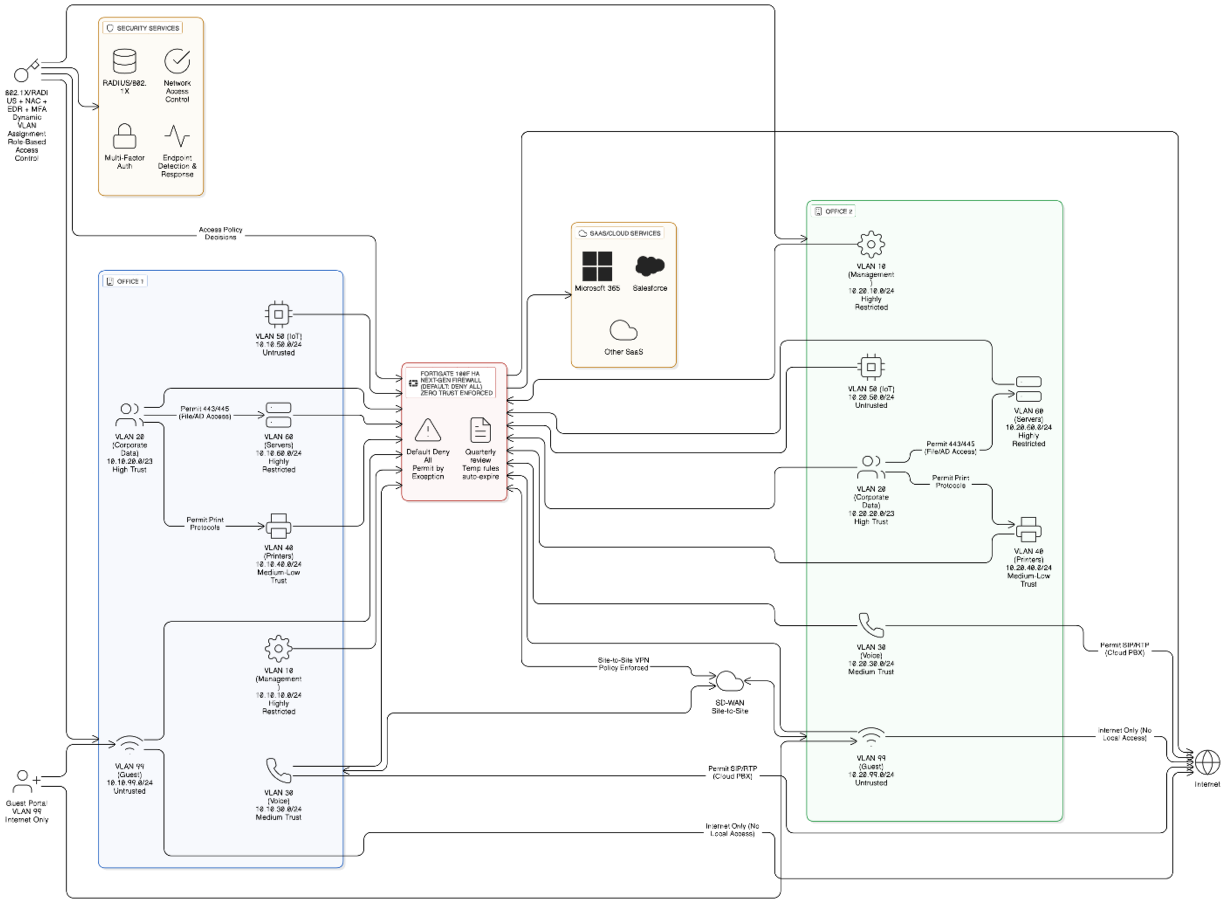
5 Advanced Security Architecture: Implementing a Zero Trust Framework

The traditional "castle-and-moat" security model is obsolete. This design is built upon a Zero Trust security framework. In simple terms, this means: a user must first prove who they are and that their device is healthy before they get access. This trust is continually re-checked, and if anything looks wrong, access is immediately reduced or blocked. This model operates on the fundamental principle that no user or device is inherently trusted, regardless of its location.

5.1 The Zero Trust Principle: "Never Trust, Always Verify"

Zero Trust is achieved by adhering to three core principles:

- **Continuous Verification**: User identities and device health are continuously validated. Every request to access a resource triggers a new verification process.
- **Least Privilege Access**: Users and systems are granted only the minimum level of access necessary to perform their function, minimizing the "blast radius" of a potential compromise. While VLANs provide foundational segmentation, the primary enforcement of least-privilege access will be based on user and device identity, using RADIUS attributes to dynamically assign policies.
- **Assume Breach**: The network is designed with robust micro-segmentation to prevent lateral movement, assuming an attacker is already inside the network.



802.1X/RADIUS + NAC + EDR + MFA Dynamic VLAN Assignment Role-Based Access Control
SECURITY SERVICES
RADIUS/802.1X
Network Access Control
Multi-Factor Auth
Endpoint Detection & Response
Access Policy Decisions
OFFICE 1
VLAN 50 (IoT) 10.10.50.0/24 Untrusted
VLAN 20 (Corporate Data) 10.10.20.0/23 High Trust
Permit 443/445 (File/AD Access)
VLAN 60 (Servers) 10.10.60.0/24 Highly Restricted
Permit Print Protocols
VLAN 40 (Printers) 10.10.40.0/24 Medium-Low Trust
VLAN 10 (Management) 10.10.10.0/24 Highly Restricted
VLAN 99 (Guest) 10.10.99.0/24 Untrusted
VLAN 30 (Voice) 10.10.30.0/24 Medium Trust
Guest Portal VLAN 99 Internet Only
FORTIGATE 100F HA NEXT-GEN FIREWALL (DEFAULT: DENY ALL) ZERO TRUST ENFORCED
Default Deny All Permit by Exception
Quarterly review Temp rules auto-expire
SAAS/CLOUD SERVICES
Microsoft 365
Salesforce
Other SaaS
OFFICE 2
VLAN 10 (Management) 10.20.10.0/24 Highly Restricted
VLAN 50 (IoT) 10.20.50.0/24 Untrusted
VLAN 60 (Servers) 10.20.60.0/24 Highly Restricted
Permit 443/445 (File/AD Access)
VLAN 20 (Corporate Data) 10.20.20.0/23 High Trust
Permit Print Protocols
VLAN 40 (Printers) 10.20.40.0/24 Medium-Low Trust
VLAN 30 (Voice) 10.20.30.0/24 Medium Trust
Permit SIP/RTP (Cloud PBX)
Site-to-Site VPN Policy Enforced
SD-WAN Site-to-Site
VLAN 99 (Guest) 10.20.99.0/24 Untrusted
Internet Only (No Local Access)
Permit SIP/RTP (Cloud PBX)
Internet Only (No Local Access)
Internet

Figure 3 Zero Trust Network Segmentation and Policy Enforcement Architecture. View full size here.

5.2 Perimeter and Internal Defense with Next-Generation Firewalls (NGFWs)

The primary enforcement point will be a high-availability (HA) cluster of Next-Generation Firewalls (NGFWs) deployed at the edge of each office to eliminate any single point of failure. These provide deep visibility and control over applications and data.

Key NGFW capabilities include:

- **Intrusion Prevention System (IPS)**: Actively scans all traffic for known cyberattacks and malware, blocking threats in real-time.
- **Application Control**: Allows for granular policies, such as permitting access to Salesforce while blocking high-risk applications like peer-to-peer file sharing.
- **Encrypted Traffic Inspection**: The NGFWs will be configured with a phased approach to TLS/SSL inspection. Initially, decryption policies will target high-risk traffic categories while bypassing sensitive and trusted applications to maintain performance. This allows for the detection of threats hidden in encrypted traffic without causing operational disruption. The selected firewall models have been sized to provide 30-40% performance headroom with these security services enabled.
- **Internal Micro-segmentation**: The firewalls will inspect all "east-west" traffic between internal VLANs. This traffic will be logged, and alerting will be configured to detect and flag unusual lateral movement that could indicate a breach. The default policy is to block all inter-segment traffic; access is only granted by specific role-based rules.

5.3 Secure Wireless and Remote Access

- **Corporate Wireless Network**: The employee Wi-Fi network will be secured using WPA3-Enterprise, with a transition mode enabled for WPA2-Enterprise to support legacy devices. Authentication will be handled via RADIUS/802.1X, requiring unique corporate credentials. Standard RF hygiene features (e.g., band-steering, client load-balancing, and setting minimum data rates) will be enabled to ensure efficient and stable performance.
- **Guest Wireless Network**: A separate guest Wi-Fi network on an isolated VLAN will provide internet access only. It will be rate-limited to preserve bandwidth for corporate use and will utilize a captive portal with short-lived credentials for access control.
- **Secure Remote Access**: The NGFW provides a built-in SSL VPN service. Access will be enforced with Multi-Factor Authentication (MFA) and will require that the connecting device meets corporate compliance policies (e.g., EDR running, OS patched). MFA will be the standard for all administrative access (firewalls, switches, cloud portals) and critical SaaS applications.

5.4 Endpoint and Server Security Integration

This network architecture is designed to integrate with a robust Endpoint Detection and Response (EDR) solution installed on all company servers and endpoints. EDR is critical for visibility into device health, which informs Zero Trust access policies. All critical alerts from the EDR platform will be integrated into the company's security monitoring workflow, whether that is a formal Security Operations Center (SOC) or an on-call notification system.

5.5 Security Policy Governance

A mature security posture requires consistent oversight. All firewall and security policies will be subject to a formal review on a quarterly basis to ensure they are still relevant and effective. To prevent the accumulation of unnecessary risk, any temporary access rules required for projects or troubleshooting will be created with an automatic expiration date.

6 Hardware Recommendations and Budgetary Analysis

6.1 Equipment Selection Philosophy

Equipment from Fortinet has been chosen for its tightly integrated security and networking products, which offer a unified management experience from a "single pane of glass". The hardware selection prioritizes models with redundant power supplies to maximize uptime. The number of access ports and wireless APs has been sized to meet current needs with a 25-30% headroom for growth, allowing for a scalable, cost-effective initial deployment.

6.2 Bill of Materials and Investment Summary

The following table details all required hardware, software, and services, separated into one-time Capital Expenditures (CapEx) and recurring annual Operational Expenditures (OpEx). All prices are budgetary estimates.

Table 2 Detailed Bill of Materials and Budget Estimate

Category	Vendor & Model	Purpose	Qty	Unit Cost (CapEx)	Total Cost (CapEx)	Annual Unit Cost (OpEx)	Total Annual (OpEx)
Security	Fortinet FortiGate 100F	Primary Firewall, SD-WAN, and VPN Appliance (HA Pair)	4	$2,100	$8,400	$1,316	$5,264
	Fortinet FortiExtender 201F	Tertiary LTE/5G Failover Appliance	2	$600	$1,200	$100	$200
Switching	Fortinet FortiSwitch 424E	Distribution/Core Layer 3 switch with 10G SFP+ (HA Pair)	4	$4,000	$16,000	$450	$1,800
	Fortinet FortiSwitch 148F-FPOE	Access Layer 48-port PoE+ switch for user devices	6	$1,950	$11,700	$235	$1,410
Wireless	Fortinet FortiAP 431F	Wi-Fi 6 Indoor Access Point for general coverage	12	$510	$6,120	$110	$1,320
	Fortinet FortiAP U431F	Wi-Fi 6E Indoor Access Point for high-density areas	4	$750	$3,000	$150	$600
Services	Professional Services	Network Design, Installation,	1	$15,000	$15,000	-	-

		Configuration, and Training					
Licensing	FortiCloud Premium	Centralized Cloud Management, Logging, and Analytics	1	-	-	$2,500	$2,500
Totals					$61,420		$13,094

Notes:

1. All prices are budgetary estimates and subject to change.
2. The OpEx for the FortiGate 100F includes the Unified Threat Protection (UTP) security bundle.
3. LTE/5G data plan costs are separate from the hardware OpEx shown above.
4. Licensing for endpoint security (EDR) and identity services (MFA) are not included in this network budget and should be accounted for separately.

6.3 Power and Management Resiliency

All specified core and edge equipment will be deployed with redundant power supplies where available. This hardware will be connected to uninterruptible power supplies (UPS) sized to provide a minimum of 30 minutes of runtime during an outage. For ultimate resilience, an out-of-band (OOB) management solution, such as a cellular console server, is recommended to ensure administrative access to the infrastructure even during a total primary network failure.

6.4 Strategic Investment Priorities

This proposal balances cost control with the need to build a resilient and secure foundation. The investment strategy is prioritized as follows:

- **Spend Now**: These are non-negotiable investments for the core architecture. This includes the dual core switches per site, high-availability firewalls, diverse ISP circuits, and comprehensive UPS, logging, and management systems.
- **Stage for Later**: These are valuable capabilities that can be implemented in a later phase as needs evolve and budgets permit. This includes full, deep-packet TLS decryption across all traffic, a dedicated Network Access Control (NAC) solution like FortiNAC, and deploying Wi-Fi 6E access points everywhere.
- **Save Now**: These are areas where costs can be managed effectively in the initial deployment. This includes purchasing fewer access switches and growing as ports are consumed, using Wi-Fi 6E only in designated high-density zones, and leveraging LTE/5G as a cost-effective tertiary link instead of a more expensive private line.

7 Scalability, Operations, and Future-Proofing

- Supporting Growth and Expansion
- **Modular Growth**: The hierarchical design is inherently modular. As the company grows, scaling the network is a simple matter of adding more access layer switches and wireless access points without disruption to the core.

- **Repeatable Design for New Locations**: The entire architecture constitutes a standardized, repeatable blueprint. Combined with the SD-WAN's zero-touch provisioning, a new site can be brought online securely in a fraction of the time required by traditional methods.
- **Proactive IP Address Planning**: The hierarchical IP addressing scheme has been designed with foresight, with large blocks of addresses reserved for future sites to prevent complex re-addressing projects.

7.1 Aligning with a Cloud-First Strategy

- **Optimized Cloud Access**: The SD-WAN provides intelligent, direct internet access at each site, ensuring low-latency, high-performance connections for SaaS and cloud-hosted applications.
- **Foundation for SASE**: The investments in SD-WAN and Zero Trust principles position the company to adopt a Secure Access Service Edge (SASE) model in the future to further enhance security for a distributed workforce.

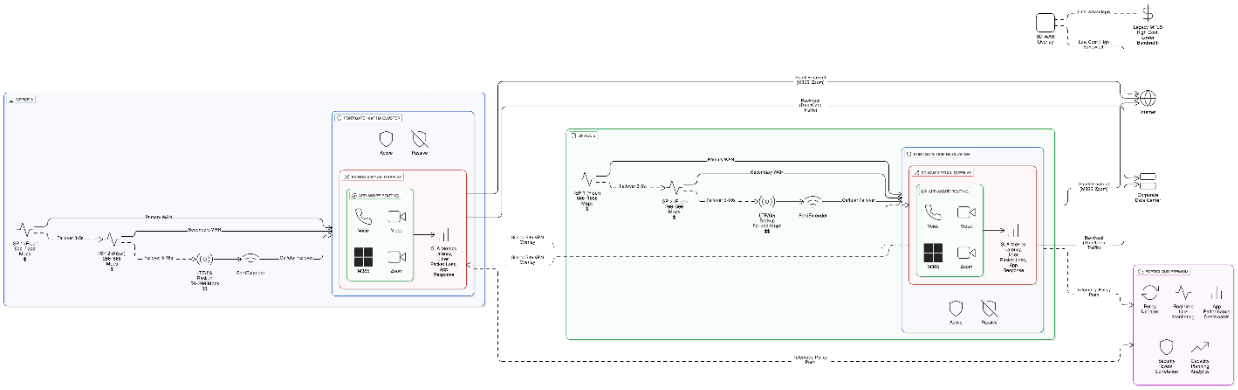

SD-WAN Overlay
Low Cost, High Bandwidth
Legacy MPLS High Cost, Lower Bandwidth
Internet
Corporate Data Center
Backhaul (Data Center Traffic)
Telemetry/Policy Push
Primary WAN
Secondary WAN
Cellular Failover
FortiExtender
LTE/5G Backup
Active
Passive
APP-AWARE ROUTING
Voice
Video
M365
Zoom
SLA Metrics: Latency, Jitter, Packet Loss, App Response
Policy Updates
Real-time Link Monitoring
App Performance Dashboards
Security Event Correlation
Capacity Planning Analytics

Figure 4 SD-WAN Traffic Engineering: Application-Specific Routing and Failover Operations. View full size here.

7.2 Operations, Management, and Disaster Recovery

- **Centralized Management**: The entire multi-site network will be managed from a single cloud dashboard. Configurations will be based on standardized templates to ensure consistency and detect configuration drift.
- **Log Management**: A tiered log retention policy will be implemented (e.g., 12 months for security events, 90 days for full traffic logs), and the licensing and storage have been sized to accommodate this.
- **Disaster Recovery**: All network device configurations will be backed up regularly to a separate, off-site location. Critical server data will be backed up to both the secondary corporate site and to immutable cloud object storage to ensure business continuity.

8 PRE-IMPLEMENTATION CHECKLIST

To ensure the final design and bill of materials are perfectly aligned with business requirements, the following sizing and validation checks will be completed prior to any hardware purchase:

☐ **Workforce Sizing**: Confirm current and projected 3to 5-year headcount for each site, including the expected percentage of users who will be primarily wireless versus wired.

☐ **PoE Budget Calculation**: Sum the maximum potential power draw for all Power-over-Ethernet devices (APs, phones, cameras) on a per-switch basis and ensure a 30% power budget headroom.

☐ **Firewall Throughput Validation**: Verify that the proposed firewall models can handle the projected throughput with all required security services enabled (IPS, App Control, SD-WAN, and the planned scope of TLS inspection).

☐ **Voice and Video Requirements**: Confirm if any specific toll-quality SLAs or contact center functionalities impose unique latency or jitter constraints on the network.

☐ **Backup and Replication Impact**: Determine if large-scale data backups will traverse the WAN. If so, establish a schedule and rate-limiting policies to ensure backups do not impact critical production traffic.

9 REFERENCES

Abrams, J. (2024, April 10). Comparing the benefits of microsegmentation vs. vlans. *Akamai Technologies*. akamai.com/blog/security/comparing-the-benefits-of-microsegmentation-versus-vlans

Asus. (2025, April 23). *[Wireless Router] What is WPA3? What are the advantages of using WPA3?* ASUS USA. asus.com/us/support/faq/1042478

Cloudflare. (2025). *Zero Trust security*. Cloudflare. cloudflare.com/learning/security/glossary/what-is-zero-trust

Fortinet. (2025a). *Next generation firewall (NGFW) - See top products*. Fortinet. fortinet.com/products/next-generation-firewall

Fortinet. (2025b). *Understanding the top benefits of SD-WAN - The comprehensive guide*. Fortinet. fortinet.com/resources/cyberglossary/benefits-of-sd-wan

Popa, L. (2024, September 24). *What is Hierarchical Network Design?* Auvik. auvik.com/franklyit/blog/hierarchical-network-design