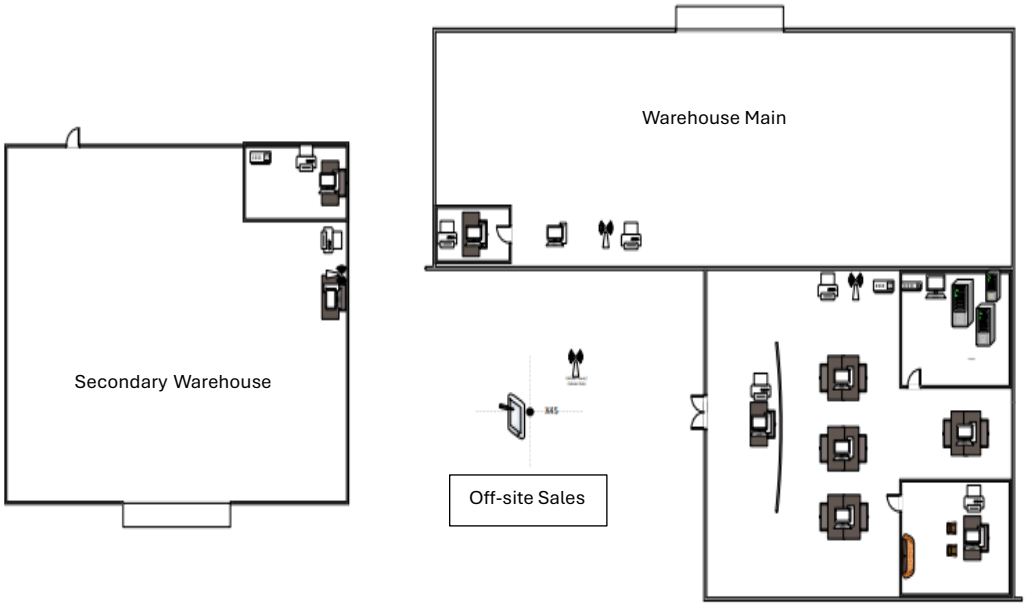
# MedConnect Supply Co.

NETWORK REDESIGN AND SECURITY ENHANCEMENT

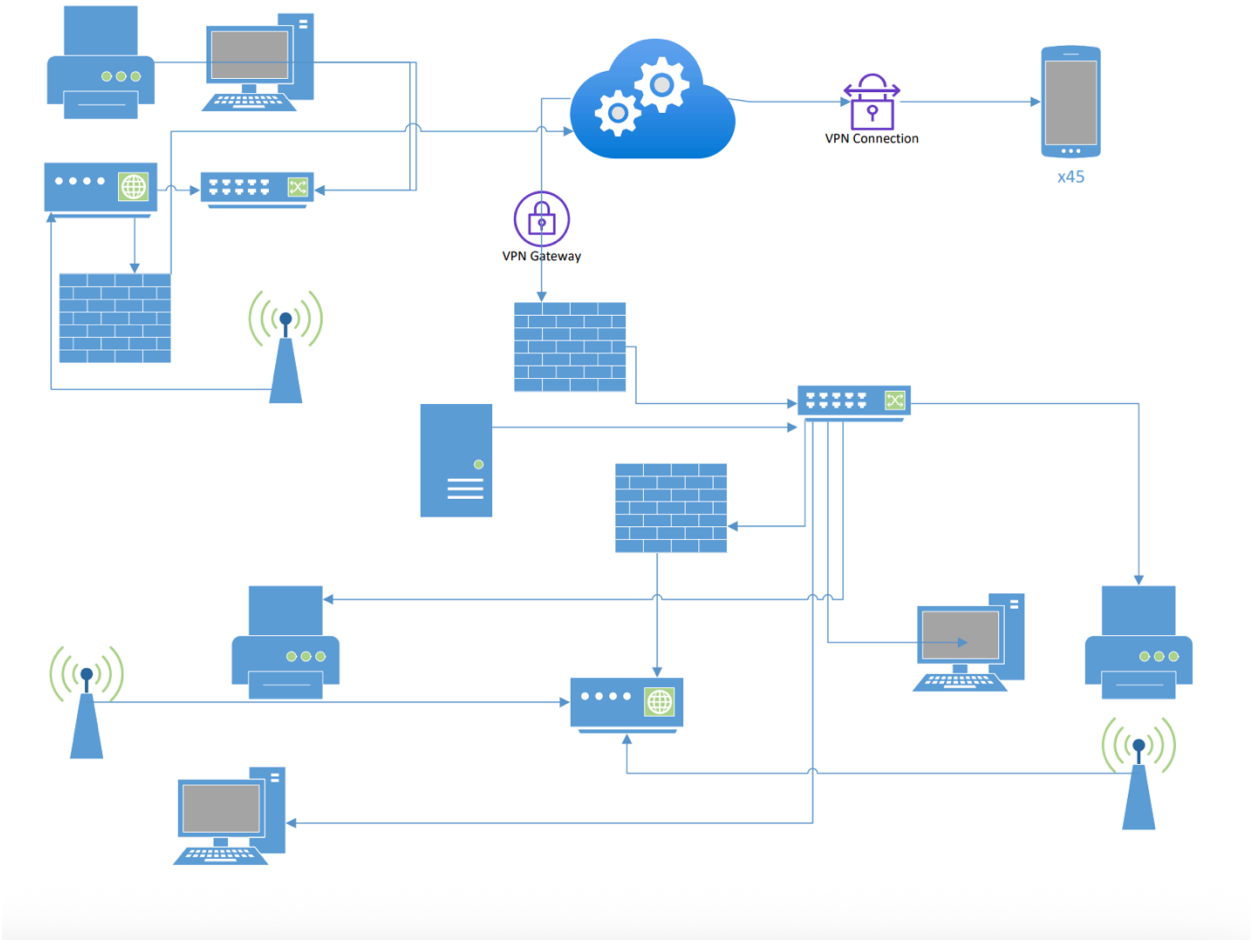
Ashley de Jesus

Table of Contents

# Physical Network Design



# Logical Network Design



# Traffic Flow Analysis

1. **Internal LAN Traffic**

   All workstation-to-server traffic remains entirely within the local LAN at each site. This includes accounting, HR, files sharing, printer traffic, warehouse inventory devices, and internal application usage.

2. **Traffic between the Two Sites**

   Sales Reps will use a VPN that securely travels between their devices, the office and the secondary warehouse to access order systems, inventory data, and internal applications. Only authenticated VPN users can send traffic between locations.

3. **Cloud Traffic**

   All servers send scheduled backups and log data to the cloud backup platform, and all users accessing Microsoft 365 or internal SaaS apps generate outbound encrypted cloud traffic. This includes replication of server configurations and storage of NPI, DEA, and order data in backups.

4. **High Priority Traffic**

   Business-critical traffic, which includes inventory data and lookups, accounting system access, warehouse handheld devices/updates, sales order submissions from iPads, and VPN traffic from remote employees. This traffic must be prioritized for low latency and reliability.

5. **Low Priority Traffic**

   Guest Wi-Fi browsing, software updates, and nightly backups are low-priority and can be rate-limited or scheduled during off-hours, so they do not impact business-critical operations.

# Vendor Comparison Tables

**Server Comparison**

| | Dell PowerEdge R350 | HPE ProLiant ML350 Gen10 | Lenovo ThinkSystem SR550 |
|---|---|---|---|
| CPU | Intel Xeon Silver | Intel Xeon Silver | Intel Xeon Silver |
| RAM | 32-64GB | 32-128GB | 32-128GB |
| Storage | RAID-Capable (SSD/HDD) | RAID-Capable (SSD/HDD) | RAID-Capable (SSD/HDD) |
| Management | iDRAC | iLO | XClarity |
| Support | Dell ProSupport | HPE Foundation Care | Lenovo Premier Support |
| Estimated Cost | $2300-3000 | $2800-4000 | $2400-3200 |

Chosen: Dell PowerEdge R350

Reason: best price for the performance ratio, strong support, and ideal for small-mid business hybrid environment

**Cloud Hosing Comparison**

| | Microsoft Azure B-Series VM | AWS EC2 (t3/x2 series) | Google Cloud E2 VM |
|---|---|---|---|
| vCPU | 4-8 | 2-4 | 4 |
| RAM | 16-32GB | 8-16GB | 16GB |
| Storage | SSD Managed Disks | EBS SSD | SSD Persistent Disk |
| SLA | 99.9% | 99.99% | 99.95% |
| Integration | Native with AD & Office 365 | Broad integrations | API-driven |
| Estimated Cost | $90-250 | $75-220 | $80-200 |

Chosen: Microsoft Azure

Reason: Seamless integration with Windows Server/Active Directory, simple backup integration, and easy VPN and central login system for MedConnect

**Sales Representatives Tablet Comparison**

| | iPad Air (Cellular) | Samsung Galaxy Tab S9 FE (5G) | Microsoft Surface Go 3 LTE |
|---|---|---|---|
| Cellular | 5G/LTE | 5G/LTE | LTE |
| OS | iPadOS | Android | Windows 11 |
| Battery Life | ~10 hours | ~12 hours | ~8-10 hours |

| | | | |
|---|---|---|---|
| MDM Support | Excellent (Apple Business Manager + MDM) | Excellent (Intune, MobileIron) | Excellent (Intune) |
| Durability | High | High | Moderate |
| Estimated Cost | $500-750 | $450-650 | $600-850 |

Chosen: iPad Air (Cellular)

Reason: Most secure, easiest to manage with MDM, best battery life + product performance, highly reliable and good price point

# Project Cost: MedConnect Network Redesign

| | PROJECT TASKS | HOUR UNIT | LABOR COST ($) | MATERIAL COST ($) | TRAVEL COST ($) | OTHER COST ($) | TOTAL PER TASK |
|---|---|---|---|---|---|---|---|
| PROJECT DESIGN | Define Project Scope and Deliverables | 10.0 | $750.00 | $0.00 | $0.00 | $0.00 | $750.00 |
| | Identify Stake Holders and Roles | 5.0 | $375.00 | $0.00 | $0.00 | $0.00 | $375.00 |
| | Develop Budget Timeline/Risk Assessment | 25.0 | $1,875.00 | $0.00 | $0.00 | $0.00 | $1,875.00 |
| | Network Evaluation | 35.0 | $2,625.00 | $0.00 | $0.00 | $0.00 | $2,625.00 |
| | Security Risk Identification | 10.0 | $750.00 | $0.00 | $0.00 | $0.00 | $750.00 |
| | **Subtotal** | **85.0** | **$6,375.00** | **$0.00** | **$0.00** | **$0.00** | **$6,375.00** |
| PROJECT DEVELOPMENT | Procure: Network Equip, Server, & PC's** | 0.0 | $0.00 | $22,000.00 | $0.00 | $0.00 | $22,000.00 |
| | Cellular Data Plan 5g/LTE or similar | 0.0 | $0.00 | $10,800.00 | $0.00 | $0.00 | $10,800.00 |
| | Procure Tablets (iPad) | 0.0 | $0.00 | $42,705.00 | $0.00 | $0.00 | $42,705.00 |
| | Misc for Tablets (cover, screen protector etc) | 0.0 | $0.00 | $3,600.00 | $0.00 | $0.00 | $3,600.00 |
| | Procure Software: MS 365, Apps for tablets etc*** | 0.0 | $0.00 | $8,000.00 | $0.00 | $0.00 | $8,000.00 |
| | MDM Software | 0.0 | $0.00 | $3,000.00 | $0.00 | $0.00 | $3,000.00 |
| | Security Software tools**** | 0.0 | $0.00 | $47,650.00 | $0.00 | $0.00 | $47,650.00 |
| | Install/Configure Servers, Network Equip & PC's | 110.0 | $8,250.00 | $0.00 | $5,000.00 | $0.00 | $13,250.00 |
| | Upgrade OS/software | 20.0 | $1,500.00 | $0.00 | $0.00 | $0.00 | $1,500.00 |
| | **Subtotal** | **130.0** | **$9,750.00** | **$137,755.00** | **$5,000.00** | **$0.00** | **$152,505.00** |
| PROJECT DELIVERY | Testing: System, Pen, Backup/Recovery | 50.0 | $3,750.00 | $0.00 | $5,000.00 | $0.00 | $8,750.00 |
| | User Acceptance Testing | 10.0 | $750.00 | $0.00 | $5,000.00 | $0.00 | $5,750.00 |
| | Staff Training | 20.0 | $1,500.00 | $0.00 | $10,000.00 | $0.00 | $11,500.00 |
| | Printing training materials | 4.0 | $100.00 | $300.00 | $0.00 | $0.00 | $400.00 |
| | IT documentation, user guides, transition | 30.0 | $2,250.00 | $2,000.00 | $0.00 | $0.00 | $4,250.00 |
| | Rollout and Data Migration | 40.0 | $3,000.00 | $0.00 | $0.00 | $0.00 | $3,000.00 |
| | Decomission old devices | 10.0 | $750.00 | $0.00 | $0.00 | $0.00 | $750.00 |
| | **Subtotal** | **164.0** | **$12,100.00** | **$2,300.00** | **$20,000.00** | **$0.00** | **$34,400.00** |
| PROJECT | Project oversight/communication | 30.0 | $2,250.00 | $0.00 | $0.00 | $0.00 | $2,250.00 |
| | Status Reporting & Meetings | 20.0 | $1,500.00 | $0.00 | $0.00 | $0.00 | $1,500.00 |
| | Final Project Review and Closure | 20.0 | $1,500.00 | $0.00 | $5,000.00 | $0.00 | $6,500.00 |
| | **Subtotal** | **70.0** | **$5,250.00** | **$0.00** | **$5,000.00** | **$0.00** | **$10,320.00** |
| OTHER COST | Misc Travel | 0.0 | $3,000.00 | $0.00 | $0.00 | $0.00 | $3,000.00 |
| | Shipping costs | 0.0 | $0.00 | $500.00 | $0.00 | $0.00 | $500.00 |
| | **Subtotal** | **0.0** | **$3,000.00** | **$0.00** | **$0.00** | **$0.00** | **$3,000.00** |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Subtotals** | **449.0** | **$36,475.00** | **$140,055.00** | **$30,000.00** | **$0.00** | **$206,600.00** |
| Risk (Contingency) 10% | 0.0 | $20,660.00 | $0.00 | $0.00 | $0.00 | **$20,660.00** |
| **Total (Scheduled)** | **449.0** | **$57,135.00** | **$140,055.00** | **$30,000.00** | **$0.00** | **$227,260.00** |

** Firewalls, coreswitches, access layer switches, wireless access points, server hardware (redundancy) UPS systm, cabeling and patch panels, PC's for office employees, backup NAS/SAN, VPN gateways, Server room security software

*** Server Licensing, Firewall/IPS subscription, Endpoint Security, MDM licensing, Cloud Services, VPN Licensing

****Security suite, SIEM or log monitoring, advanced firewall subscription

# Physical Security Plan

- **Server Room Access Control:** Server room at the main location will remain locked at all times. Access is restricted to authorized IT personnel only. Entry logging (via keycard or sign-in log) will be enforced.
- Secondary Warehouse Network Cabinet: Network switches and firewall for the secondary warehouse will be enclosed in a locked, wall-mounted cabinet with limited access.
- **Monitoring and Surveillance:** Door access points monitored by CCTV. Any access after-hours will alert IT/security.
    - Camera coverage at entrances, throughout the warehouse, and in front of the server room.
    - Access logging will be tracked for anyone who enters the server room.
- **Cooling:** There will be a wall mounted AC device in the server room to maintain safe operating temperature and humidity. Alerts will be sent to IT if thresholds are exceeded.
- **Power Protection:** UPS and surge protectors will be used to protect servers, firewalls, and switches.
- **Cable Management:** Organized patch panel with clearly labeled cables and color coded to prevent unauthorized changes.
- **Visitor Access:** Non-staff personnel must be accompanied when entering server room.

# Logical Security Plan

- **Active Directory Authentication**: All staff accounts will be managed through Active Directory with unique credentials and role-based permissions.
- **Password Policy:** Passwords must have a minimum of 12 characters mixed with upper/lower case, numbers and symbols. Users will be prompted to change passwords every 90 days.
- **Multi-Factor Authentication (MFA):** Required for VPN, cloud access, and any system storing NPI/DEA or regulated medical data.
- **Firewall & Router Security:** A Fortinet Firewall deployed at both locations with intrusion prevention (IPS), web filtering, geo-blocking, and encrypted site-to site VPN. Default admin passwords changed and firmware kept up to date.
- **VLAN Segmentation:** Separate VLANs for office, warehouse, guest Wi-Fi, and server/data zone to reduce lateral movement.
- **Endpoint Protection:** All devices (computers/tablets) protected by updating antivirus/EDR and automatic OS patching.
- **Data Encryption:** Sensitive data encrypted in transit (using a VPN between sites, and HTTPS for applications). Sensitive Server Data will be encrypted in volumes.
- **Backups:** Servers will back up nightly, to Azure cloud storage. Backup restore tests will be conducted monthly.
- **Access Control:** Data access will be restricted by departments, using an ACL. DEA and NPI-related data will be restricted to authorized users only.
- **Incident Response:** In the event of a breach, IT will isolate affected systems, disable accounts, rotate credentials and restore verified backups.

# Security Policy Recommendation

- **Acceptable Use:** Company computers, network and internet are to be used for business purposes only. Personal use should be up to the discretion of the IT/Admin team, but it is recommended to limit or eliminate the use of personal devices on the network for security reasons. If needed they could use the guest Wi-Fi network for safety.
- **Passwords:** Employees must use strong passwords, that will be changed every 90 days. Passwords should have a minimum of 12 characters including symbols, numbers, and upper/lower case letters. MFA will also be required for VPN and cloud systems.
- **Email & Internet:** Employees must not open suspicious emails or click unknown links. Personal email should not be used for company business. Email phishing training recommended quarterly for employees.
- **Data Handling:** DEA and NPI numbers, order history and regulated drug purchase data must only be stored on secure servers, or other approved cloud storage.
- **Software Installation:** Only IT staff may install update or remove software on company devices. Unauthorized installations are prohibited.
- **Remote Access:** Employees working remotely must connect through the company's VPN to access company resources.
- **Mobile Device Policy:** Company-issued tablets will use mobile device management (MDM) to enforce encryption, lock/wipe features and app control.
- **Backups:** Employees should save all work to the designated server locations to ensure it's backed up automatically.
- **Incident Reporting:** Any suspected security issues (viruses, phishing, etc) must be reported immediately to IT staff, or an administrator.
- **Physical Security:** Employees must log out of devices when leaving the workstation. Sever closet access is restricted to IT and Admin staff only.

# Access Control/ Role-Based Access Control

Purpose: Ensure users only have access to the systems, applications and data necessary for their job role, reducing security risks and protecting sensitive information.

**Role Definitions within MedConnect:**

- CEO/Management
- Accounting
- HR
- IT Administrators
- Warehouse Managers
- Warehouse Staff
- Sales Representatives
- Reception/Office Administrator

**Access Assignment granted strictly on job functions:**

- **CEO/Management**
    - Read only access to departmental reports, business dashboards, and general company data. Limited write access to management folders.
- **Accounting**
    - Access to financial software, shared accounting folders, and internal data bases relevant to invoices, billing and vendor data.
- **HR**
    - Access to HR records, employee files, payroll documents, and HR specific applications. No access to accounting or IT systems.
- **IT Administrators**
    - Full administrative access to servers, network devices, VLANs backups and all security systems.
- **Warehouse Managers**
    - Access to warehouse inventory systems, handheld device management, and warehouse reporting tools.

- **Warehouse Staff**
    - Access to only the handheld devices, inventory scanning apps, and limited workstation functions
- **Sales Representatives**
    - Access to CRM/order-entry system, cloud-enables sales apps on iPads and limited access via VPN for data submission.
- **Reception/Office Administrator**
    - Access to general administrative folders, email and internal communications.

All access will be controlled through Active Directory security groups. Least privilege will be applied to all users by default. Permissions will be reviewed quarterly and updated upon employee onboarding/offboarding. Sensitive folders will be protected with NTFS permissions and role-based restrictions.

# Backup and Recovery Strategy

**RPO/RTO/Retention**

Purpose: Ensure MedConnect's critical business data, including NPI numbers, DEA numbers, order records, accounting files and configuration data, can be restored in the event of a failure, disaster or cyberattack.

**Backup Methods**

- Daily incremental backups to cloud storage for all server data
- Weekly full backups stored in secure cloud archive.
- Local backups (NAS/SAN) used for short-term rapid restoration
- Backups are encrypted in transit and at rest.

**Recovery Point Objective**

The business can tolerate the loss of up to one day of data (24 hours), due to daily incremental backups and real-time sync for vital systems.

**Recovery Time Object**

Core services (file server, order system, authentication, VPN) must be restored within a single business day to avoid operational disruption, total time expected: 4-6 hours.

**Data Retention Policy**

- Daily backups retained for 30 days
- Weekly backups retained for 6 months
- Monthly backups retained for 1 year
- Compliance-related data (NPI, DEA order documentation) stored for 7 years or longer as required by regulatory bodies in each state.

**Testing**

Backup restoration is tested monthly, this will include: partial file restoration, full system restoration (which will be tested quarterly), full system restoration test (quarterly), and verification of cloud backup integrity.

# Incident Response Plan

**Purpose:** Provide clear steps for detecting, containing and resolving security incidents such as malware, unauthorized access, or system breaches.

**Phase 1: identification**

- Monitor alerts from firewall, endpoint security, and SIEM/logging tools
- Employees report suspicious emails, unusual device behavior, or unauthorized data access attempts

**Phase 2: Containment**

- Immediately isolate affected workstation or tablet from network
- Disable compromised user accounts in AD
- Block malicious IPs or ports in the firewall
- If necessary, route critical traffic through backup VLAN or alternate systems

**Phase 3: Eradication**

- Remove malware or unauthorized software
- Apply missing patches, or look for security updates
- Reset passwords for affected users and review access logs

**Phase 4: Recovery**

- Restore data from backups
- Reconnect devices only after they have passed security checks
- Monitor the system for reoccurrences over the next 48-72 hours

**Phase 5: Documentation and Lessons Learned**

- Record incident in IT logs
- Root cause analysis (phishing, outdated software, misconfiguration, etc.)
- Security procedures updated as needed
- Staff retrained if the issued proved to be human error

# Implementation and Schedule

**Step 1: Equipment Delivery & Inventory**

- Receive serves, switches, firewalls, access points, UPS systems, racks and iPads.
- Verify inventory and test hardware for functionality.

**Step 2: Server Room Setup**

- Install rack, UPS, cooling unit and patch panels.
- Secure and label all cabling.

**Step 3: Server Installation & Configuration**

- Install Windows Server 2022, Active Directory, file services, and backup agents.
- Configure RAID, domain settings, user groups, and server hardening.

**Step 4: Networking Installation**

- Install Fortinet firewalls at both sites.
- Install core and access switches
- Create VLANs for Office, Warehouse, Sales, Server/Data, and Guest
- Configure site-to-site VPN between locations

**Step 5: Wireless Network Setup**

- Install all access points and configure WPA3-secured SSIDs.
- Create separate SSIDs for Staff, Warehouse Devices, and Guest.

**Step 6: Cloud Backup & Azure Integration**

- Configure Azure storage for nightly backups.
- Perform initial backup and verify restore capability.

**Step 7: Tablet Deployment**

- Enroll all iPads in MDM.
- Configure VPN client, email, order entry application, and security profile.

**Step 8: Testing**

- Verify VPN connectivity, VLAN routing, server access, shared folders, wireless coverage, and backup restores.

**Step 9: Security Configuration**

- Implement password policies, MFA, and least-privilege access.
- Configure firewall rules and log monitoring.

**Step 10: Training**

- Train staff on accessing shared drives, using VPN, and recognizing security threats
- Train sales reps on tablet usage and order-entry workflow.

**Step 11: Go Live & Post-Deployment Support**

- Monitor system behavior and fix any issues during the first 1-2 weeks.

# Servers & Server Room Plan

**Server Roles:** File/Print Server, Domain Controller, Application Server, Cloud Backup Connector.

**Hardware**: Rackmount server (64GB RAM, RAID storage), Fortinet firewall, core switch, UPS.

**Location:** Secured, climate-controlled room with CCTV coverage and restricted access.

**Cooling:** Dedicated wall-mounted AC and remote temperature monitoring.

**Power:** UPS with surge protection and automated shutdown.

**Cable Management:** Fully labeled patch panels, color coded cabling.

**Monitoring:** Server and Firewall logs reviewed weekly; temperature and uptime monitored continuously.