Enhancing Security Infrastructure for Family Smiles Dentistry

Prepared by: Oyindamola Olayiwola

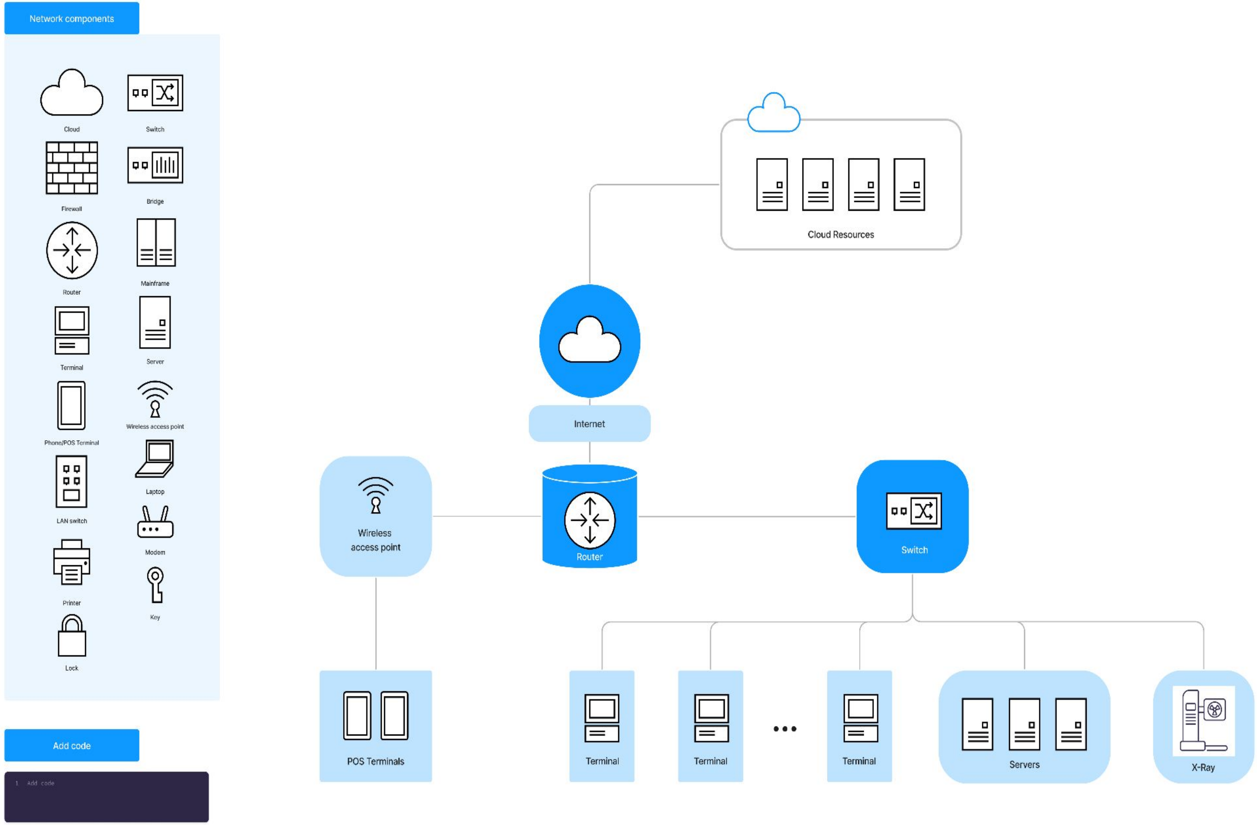
Current Network Architecture

Our network infrastructure comprises enterprise-grade routers, switches, firewalls, and Wi-Fi access points, with internal devices operating on the 192.168.0.0/24 range and specific external IPs for our SoHo, Midtown, and Park Slope offices. While functional, our current setup faces several limitations

Servers require regular updates to maintain security and performance, and our workstations lack advanced security measures, posing potential risks. POS terminals need enhanced security protocols to safeguard transactions, and our Wi-Fi encryption methods could be updated to more secure standards. Additionally, some network devices are outdated, potentially compromising overall security.

While the current network functions adequately, these limitations and vulnerabilities highlight areas for improvement. By updating servers, enhancing workstation security, implementing robust POS security measures, upgrading Wi-Fi encryption, and replacing outdated equipment, we can significantly enhance our overall security posture.

Current Network Architecture

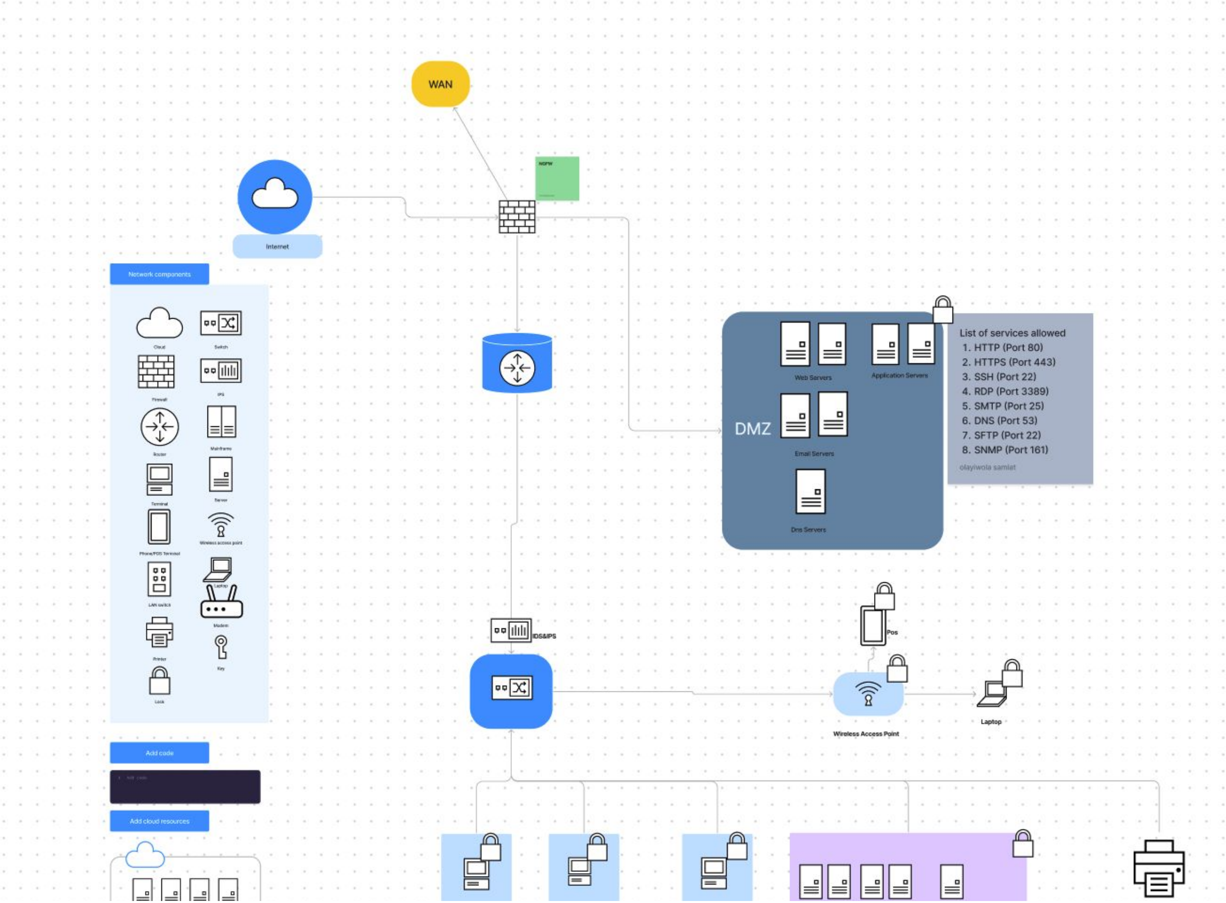


Threat Landscape

Here's a list of the threats identified in the dental practice network infrastructure:

- Data Breaches
- Ransomware Attacks
- Phishing Attacks
- Malware Infections
- Denial-of-Service (DoS) Attacks
- Weak Patch Management/ Manual Patch Management
- Shared EHR Login
- Insider Threats
- Physical Security Issues
- Social Engineering
- Full Account Privilege
- Lack of Disaster recovery plan

Proposed Network Architecture



List of services allowed

1. HTTP (Port 80)
2. HTTPS (Port 443)
3. SSH (Port 22)
4. RDP (Port 3389)
5. SMTP (Port 25)
6. DNS (Port 53)
7. SFTP (Port 22)
8. SNMP (Port 161)

olayiwola samiat

Infrastructure Component

Next-Generation Firewall

Multi-factor Authentication Solution

Endpoint Detection and response Solution

Automated Patch Management System

Identity and Access Management System

Backup and Disaster Solution

Network Access Control

IDPS

Security Awareness Training Program

Security Information and Event Management System

Roles & Responsibilities

Chief Information Security Officer (CISO)

- Formulate and execute the organization's comprehensive information security strategy.
- Supervise the security measures of the entire IT infrastructure to ensure robustness and resilience.
- Guarantee adherence to relevant regulations and standards such as HIPAA, ensuring legal and regulatory compliance.
- Develop, update, and enforce security policies and procedures across the organization.
- Align security measures with business goals by coordinating with various departments within the organization.
- Lead efforts in responding to security incidents, manage incident response teams, and oversee remediation actions.

IT Security Manager

- Manage the day-to-day operations of the security infrastructure.
- Supervise the implementation and maintenance of security tools (e.g., NGFW, SIEM, EDR, IAM).
- Conduct regular security assessments and audits.
- Develop and oversee the execution of patch management processes.
- Ensure all security policies and procedures are followed.
- Report security metrics and incidents to the CISO.

Network Security Engineer

- Design, implement, and manage network security solutions (e.g., NGFW, NAC, IDPS).
- Monitor network traffic for suspicious activity.
- Conduct vulnerability assessments and penetration testing.
- Implement and manage VPNs and secure remote access solutions.
- Respond to network security incidents and take corrective actions.

Security Analyst

- Monitor security events using the SIEM system.
- Analyze and investigate security incidents.
- Conduct threat intelligence and stay updated on emerging threats.
- Develop and update incident response playbooks.
- Participate in forensic analysis during security incidents.
- Generate security reports for management.

Systems Administrator

- Manage server and endpoint security configurations.
- Implement and oversee automated patch management systems.
- Ensure secure configurations of operating systems and applications.
- Manage backups and disaster recovery solutions.
- Conduct regular system audits and vulnerability scans.

Compliance Officer

- Ensure adherence to healthcare regulations (e.g., HIPAA).
- Develop and maintain compliance documentation.
- Conduct regular compliance audits and risk assessments.
- Train staff on compliance requirements and best practices.
- Coordinate with the IT Security Manager and CISO to address compliance issues.

Documentation Framework for Enhanced IT Infrastructure

- Infrastructure Overview Document
- Network Configuration Documentation
- Security Policies and Procedures
- Patch Management Plan
- Backup and Disaster Recovery Plan
- User Access Management Documentation
- System Configuration Documentation
- Incident Response Documentation
- Compliance Documentation
- Training Materials
- Vendor and Third-Party Management Documentation
- Monitoring and Logging Documentation
- Maintenance and Support Documentation

Cost Analysis for Enhanced Security Infrastructure

Security Item	Cost	Justification
(NGFW)	$5,000 - $10,000 (one-time purchase)	Advanced threat protection, application awareness, and content filtering capabilities mitigate network breaches and data exfiltration.
Security Information and Event Management (SIEM) System	$15,000 - $30,000 (annual subscription)	Real-time monitoring, threat detection, and incident response capabilities ensure prompt detection and mitigation of security threats.
Multi-Factor Authentication (MFA) Solution	$2,000 - $5,000 (one-time purchase)	Additional layer of security reduces the risk of unauthorized access due to stolen or compromised credentials.
Endpoint Detection and Response (EDR) Solution	$3,000 - $7,000 (annual subscription)	Timely and consistent application of security updates reduces the window of vulnerability to known exploits and vulnerabilities.
Network Access Control (NAC) System	$7,000 - $12,000 (one-time purchase)	Security policies for devices connecting to the network reduce the risk of

Security Item	Cost	Justification
Automated Patch Management System	$3,000 - $7,000 (annual subscription)	Timely and consistent application of security updates reduces the window of vulnerability to known exploits and vulnerabilities.
Identity and Access Management (IAM) System	$8,000 - $15,000 (one-time purchase)	Centralized user access management and role-based access control policies enhance access controls and compliance
Enhanced Backup and Disaster Recovery Solution	$20,000 - $40,000 (annual subscription)	Data resilience and quick recovery minimize downtime and protect against data breaches.
Intrusion Detection and Prevention System (IDPS)	$12,000 - $25,000 (one-time purchase)	Monitoring network traffic for suspicious activity enhances threat detection capabilities.

Conclusion

Key Takeaways:

- Investment in enhanced security infrastructure is crucial for protecting patient data and minimizing cyber threats.
- Each component and role plays a vital role in strengthening the security posture.
- The proposed enhancements and documentation will ensure compliance and improve overall security.

Next Steps:

- Develop and implement the proposed security strategy.
- Phase-wise implementation of new infrastructure components.
- Continuous monitoring and improvement of security measures.

Question?