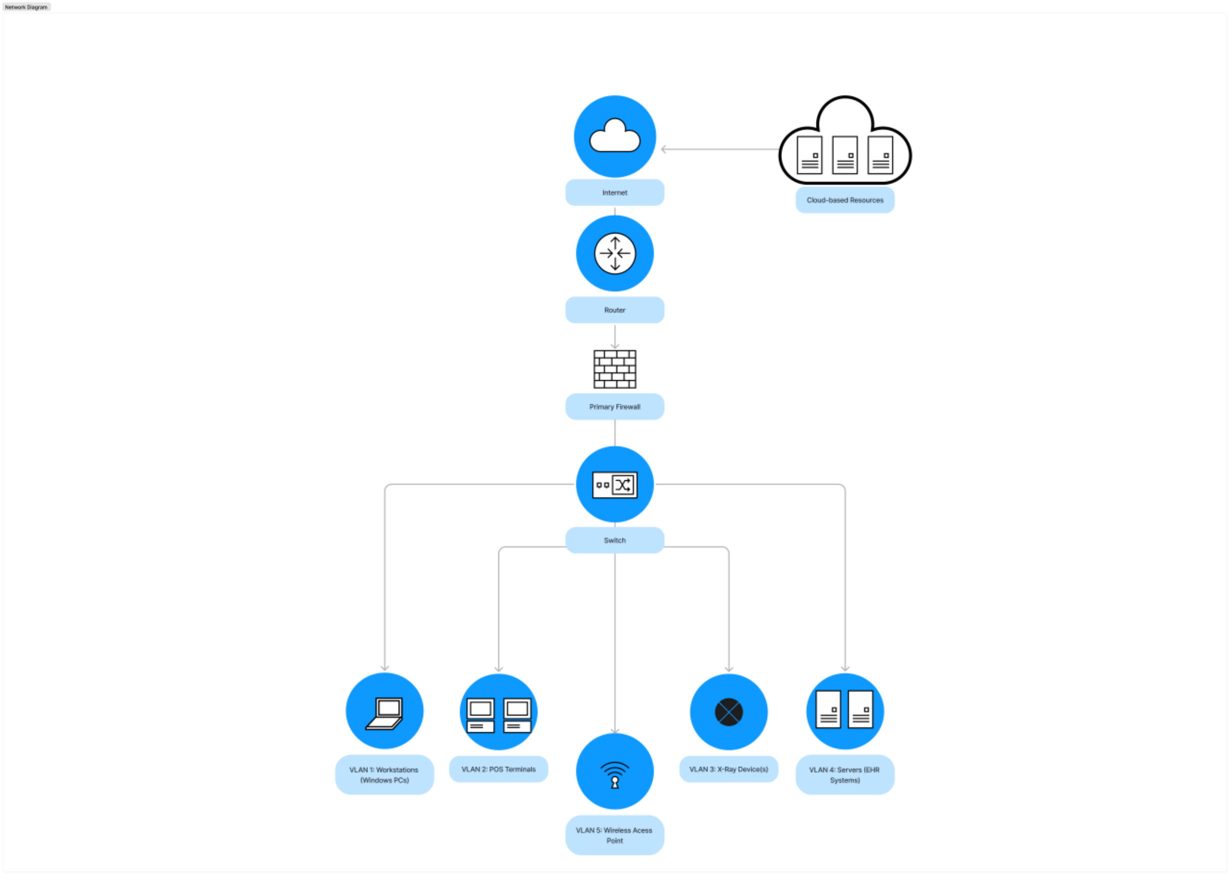
2. Future-state Network Architecture Diagram



2.1 <u>Diagram Explanation:</u>

- **Router**: Connects the internal network to the internet.
- **Firewall**: Positioned after the router to inspect and filter incoming and outgoing traffic.
- **Switch**: Central device connecting different VLANs.

VLANs:

- **VLAN 1**: Front Desk Workstations (Windows PCs)
- **VLAN 2**: POS Terminals
- **VLAN 3**: Digital X-ray Devices
- **VLAN 4**: Servers (EHR System)
- **VLAN 5**: Wireless Access Points

Network Segmentation and Security:

Network Segmentation:

  - Different categories of devices are placed in separate VLANs to limit broadcast domains and reduce potential attack vectors.
  - Firewalls are used to control and monitor traffic between VLANs.

- **Ingress/Egress Protection**:
  - The firewall ensures that only authorized traffic enters or leaves the network.
  - Firewall rules and Access Control Lists (ACLs) provide an additional layer of security.
- **Data Protection**:
  - Sensitive data is encrypted both at rest and in transit.
  - Implementing role-based access controls (RBAC) and multi-factor authentication (MFA) enhances data security.
- **Business-Critical Equipment Protection**:
  - Dedicated firewalls and continuous monitoring protect critical systems like the EHR.
  - Regular security audits help maintain the integrity and security of the network.

This upgraded network architecture improves security by isolating different device categories, minimizing the risk of lateral movement by attackers, and ensuring sensitive data and critical systems have additional layers of protection.

2.2 <u>Original Network Architecture (Flat Network) Comparison:</u>

In the original flat network design, all devices are connected to the same external-facing router via a network switch or wireless access points. This includes:

- Network Router
- Network Switch
- Front desk workstations
- Digital X-ray sensors and imaging devices
- Point-of-sale (POS) terminals for handling payments
- Wireless access points
- Servers for Patient health records storage system

Security Risks in a Flat Network Design

1. **Lack of Segmentation:**
   - All devices share the same network, meaning a compromised device can potentially affect all other devices.
   - There is no isolation between different categories of devices, increasing the risk of lateral movement by attackers.
2. **Single Point of Failure:**

  - The network relies heavily on a single router and switch, making it vulnerable if these devices are compromised.

3. **Inadequate Traffic Control:**
   - Traffic is not inspected between devices on the same network, making it easier for malicious traffic to spread.
4. **Limited Access Control:**
   - Without segmentation, implementing granular access control policies is challenging.

Future-State Network Architecture

Network Segmentation:

- Devices are segregated into different VLANs based on their roles and security requirements:
  - **VLAN 1:** Front Desk Workstations
  - **VLAN 2:** POS Terminals
  - **VLAN 3:** Digital X-ray Devices
  - **VLAN 4:** Servers (EHR System)
  - **VLAN 5:** Wireless Access Points

Improved Security Measures:

Network Segmentation:
- Each VLAN isolates devices based on their function, reducing the risk of lateral movement in case of a breach.
- Segmentation helps contain attacks and limits the spread of malware.

Dedicated Firewalls:
- Firewalls are strategically placed between VLANs and at the network perimeter.
- They inspect and control traffic between different segments, preventing unauthorized access.

Enhanced Traffic Control:
- ACLs and firewall rules control the flow of traffic, ensuring only legitimate and necessary communications occur between VLANs.
- Continuous monitoring and intrusion detection systems can be implemented to detect and respond to suspicious activities.

Access Controls and Authentication:
- Role-Based Access Controls (RBAC) ensure users have the minimum necessary access to perform their tasks.
- Multi-Factor Authentication (MFA) adds an extra layer of security for accessing critical systems and sensitive data.

Data Protection:

- Sensitive data is encrypted both at rest and in transit.
- Regular security audits and vulnerability scans help maintain the security posture.

2.3 Why the Future-State Network Architecture is Safer:

Isolation of Devices:

- Segmentation isolates devices into secure zones, making it harder for an attacker to move laterally across the network.

Controlled Access:

- Firewalls and ACLs provide robust control over who can access what, reducing the attack surface.

Enhanced Monitoring:

- Improved visibility and monitoring across segmented networks help quickly detect and respond to anomalies.

Minimized Impact of Breaches:

- In case of a compromise, segmentation limits the potential impact and prevents attackers from gaining access to the entire network.

Scalability and Manageability:

- Segmented networks are easier to manage and scale, with policies applied to specific segments without affecting the whole network.