# Secure Network Design

This playbook outlines the steps for designing network architectures with a focus on security. It includes recommendations for using segregation, defining network zones, and employing secure communication protocols to enhance protection.

### Step 1: Assessment

Conduct a thorough assessment of your current network, including identifying all devices, understanding traffic flow, recognizing sensitive data, and cataloging existing security measures.

### Step 2: Requirements

Determine security requirements based on company policy, legal regulations, and risk analysis. Define what needs to be protected and to what degree.

### Step 3: Network Segregation

Design network segregation strategies to reduce access between network segments. Utilize firewalls and Virtual Local Area Networks (VLANs) to control traffic and create barriers.

### Step 4: Define Zones

Define network zones based on function, data sensitivity, and security requirements. Common zones include Public, External, Internal, DMZ (Demilitarized Zone), and Secure Zones.

### Step 5: Secure Protocols

Select and implement secure communication protocols. Prioritize encrypted protocols like HTTPS, SSH, and TLS, and phase out insecure protocols like HTTP and FTP.

### Step 6: Access Management

Establish strict access controls and authentication mechanisms to ensure that only authorized users and devices can connect to network segments or zones.

### Step 7: Monitoring

Implement a network monitoring solution to detect suspicious activity, unauthorized access, or potential breaches. Regularly audit and adjust security settings.

### Step 8: Testing & Validation

Regularly test your network security through penetration testing, vulnerability scanning, and mock exercises. Validate that the security measures are effective and adjust as needed.

### Step 9: Documentation

Document your network architecture, security policies, procedures, and any changes made. Documentation aids in maintenance and future security assessments.

### Step 10: Training

Provide training to staff on network security best practices, incident response, and the specific security features of your network. Continual education helps maintain a secure network environment.

## General Notes

### Review Cycles

Network designs should be reviewed regularly to ensure they remain secure against emerging threats and incorporate the latest security technologies and strategies.

### Compliance

Ensure your network design complies with relevant industry standards and regulatory requirements, such as ISO/IEC 27001, HIPAA, or GDPR.