**Home Network Segmentation & Security Implementation Project**

**Project Manager & Network Engineer:** Joseph Hardy  
**Date Completed:** March 12, 2025  
**Document Type:** Implementation Report & Technical Project Documentation

**Executive Summary**

This report details the step-by-step planning, implementation, and testing of a segmented home network using Ubiquiti UniFi equipment. The primary objective was to design a secure, scalable, and manageable network that simulates enterprise-grade principles in a residential setting. Core areas of focus included VLAN segmentation, firewall rule implementation, wireless SSID isolation, and device adoption.

**Project Objectives**

* Redesign home network with security-first principles
* Deploy VLAN segmentation to separate network functions (e.g., IoT, Guests, Secure)
* Configure firewall rules to control inter-VLAN traffic
* Establish multi-SSID wireless access mapped to VLANs
* Test and verify all segmentation, isolation, and access control measures
* Create reusable documentation to demonstrate cybersecurity, network design, and project management skills

**Scope**

**In-Scope:**

* ISP Modem Bridge Setup
* UniFi Dream Machine Pro configuration
* Switch and AP deployment
* VLANs, firewall rules, DHCP
* Wi-Fi SSID segmentation
* Testing and validation

**Out of Scope:**

* Physical cabling upgrades
* External threat mitigation tools (beyond IDS/IPS)
* Multi-WAN failover setup

**A white sheet with black text

AI-generated content may be incorrect.**

A close-up of a computer

AI-generated content may be incorrect.

**Implementation Phases**

**Phase 1: Planning & Design**

* Mapped existing network topology
* Identified required VLANs: Management, Secure, IoT, Guest, Camera
* Defined IP address schema and DHCP pools
* Established firewall rule framework
* Created logical network diagrams

**Phase 2: Physical Deployment**

* Placed and powered all network equipment
* Set PoE switch ports for VLAN tagging
* Connected Flex Mini to main switch for downstream segmentation

**Phase 3: System Configuration**

* Logged into UDM Pro, performed firmware updates
* Switched UniFi GUI to dark mode for visibility
* Adopted and updated UniFi devices
* Created VLANs with subnet mapping:
  + VLAN 1: Management (192.168.10.0/24)
  + VLAN 20: Secure (192.168.20.0/24)
  + VLAN 30: IoT (192.168.30.0/24)
  + VLAN 40: Camera (192.168.40.0/24)
  + VLAN 50: Guest (192.168.50.0/24)
* Created DHCP scopes per VLAN

**Phase 4: Security Configuration**

* Enabled IDS/IPS system-wide
* Applied country IP block list (2 high-risk regions)
* Configured honeypot in Management VLAN
* Restricted admin interface to Management + Secure VLANs only

**Phase 5: Wireless SSID Setup**

* Created 4 SSIDs:
  + "SecureNet" - VLAN 20
  + "IoT-Net" - VLAN 30
  + "CameraNet" - VLAN 40
  + "GuestAccess" - VLAN 50 (portal + isolation)
* Broadcast settings:
  + Secure & Guest: 2.4/5GHz
  + IoT & Camera: 2.4GHz only
* Enabled client isolation for Guest VLAN

**Phase 6: Firewall Rule Implementation**

* Allow Management VLAN outbound to all VLANs
* Allow Secure VLAN to access all networks
* Block IoT ↔ Secure/Management communication
* Allow Guest → IoT casting only
* Block all guest traffic to Secure/Management VLANs
* Add parental control rules for specific devices (time/content)

**Phase 7: Testing & Validation**

* Verified VLAN assignment per port
* Conducted ping tests between VLANs
* Validated DHCP on each VLAN
* Confirmed SSID → VLAN routing
* Performed casting tests from Guest → IoT
* Confirmed firewall rules block unauthorized lateral movement

**Outcome & Deliverables**

* Fully segmented and secure home network
* Documented configurations for repeatability
* Functional wireless environment with isolated VLAN traffic
* Practical showcase of cybersecurity and network engineering capabilities

**Contact**

**Joseph Hardy**  
Cybersecurity Graduate | Aspiring IT Security Professional  
GitHub: [JoHaa-D](https://github.com/JoHaa-D)  
Email: joseph.hardy603@gmail.com