Network Build & Expansion

Case Study

Author: A. Brito

Date: August 2025

Note: Based on a real freelance project. Client information anonymized.

Executive Summary

Client Challenge: Business expansion into 3 local offices and 2 overseas offices exposed limitations in their existing setup (consumer-grade router, unmanaged switches, regular computers doubling as “servers”).

Objective: Redesign the network to ensure scalability, resilience, and security while supporting remote connectivity.

Outcome: Enterprise-grade Ubiquiti infrastructure, redundant ISP connections, proper server/NAS setup, VLAN segmentation, IDS/IPS, and secure VPN access — resulting in a more stable, secure, and productive IT environment.

Environment Before Project

- ISP-provided modem/router with consumer-grade switches and Wi-Fi.
- Shared drive hosted on a regular desktop computer acting as a 'server.'
- No segmentation → flat network.
- No backup or business continuity plan.
- No VPN for branch/remote offices.
- Cameras and user traffic on the same network.

Solution Design & Implementation

Core Infrastructure:

- Deployed Ubiquiti UDM Pro with dual ISP connections for automatic failover.
- Configured firewall rules for VLAN separation and least-privilege access.
- Enabled IDS/IPS and country-based geo-blocking.
- Installed 10 Unifi Access Points and 4 network switches, mounted in a network rack for organization and scalability.

Server & Storage:

- Replaced ad-hoc PC server with a Dell PowerEdge server (dual PSU, dual NICs, RAID 10).
- Added a Synology NAS with RAID 1 for shared storage.
- Configured Acronis backups: daily local → NAS, weekly cloud.

Network Segmentation (VLANs + SSIDs):

- Enterprise VLAN – Business-critical devices (servers, printers).
- Secure VLAN – Staff computers and tablets.
- Guest VLAN – Visitors with internet-only access.
- Devices VLAN – IoT + Security cameras (isolated from business traffic).
- Each VLAN mapped to a dedicated SSID (all secured with WPA2).

Remote Connectivity:

- Enabled VPN server on UDM Pro.
- Configured VPN access for branch/remote users → limited access to server, NAS, and printers only.

Identity & Access Management:

- Enforced MFA with Microsoft Authenticator for all Microsoft 365 accounts.

Before vs After

Before:

- Consumer router + unmanaged switches
- Flat network, no VLANs
- Regular PC acting as a server
- No backup strategy
- No VPN for remote users
- Cameras on same network as business apps

After:

- Enterprise Ubiquiti infrastructure with dual ISP failover
- VLANs + firewall rules for segmentation & least privilege
- Dell PowerEdge server (RAID 10) + Synology NAS (RAID 1)
- Acronis daily + weekly backups (local + cloud)
- VPN access for branch/overseas offices with limited access
- IDS/IPS enabled + country blocks
- MFA enforced across Microsoft 365

Outcomes & Benefits

- **Resilience:** Dual ISPs + RAID storage ensure uptime and business continuity.
- **Security:** IDS/IPS, VLAN isolation, MFA, and VPN hardening significantly reduce attack surface.
- **Productivity:** Staff productivity improved ~50% thanks to reliable connectivity and properly segmented resources.
- **Scalability:** Network designed to support future growth without major redesign.

Conclusion

Delivered scalable, secure infrastructure supporting business growth. Improved productivity, reduced downtime risk, and strengthened cybersecurity posture across all local and overseas offices.