Secure Enterprise Network Design

Alexander Irvin C. Barrios

June 2025

E-Mail: [ece.aibarrios@gmail.com](mailto:ece.aibarrios@gmail.com) | LinkedIn: [aicbarrios](https://www.linkedin.com/in/aicbarrios/) | GitHub: [aibarrios](https://github.com/aibarrios)

# Table of Contents

[Auto-generate TOC in Word after headings are applied]

# 1. Executive Summary

This self-initiated project simulates a secure, enterprise-grade network environment using Cisco and Fortinet devices. It replicates a multi-site enterprise structure comprising a headquarters (HQ), two branch offices (BO1 and BO2), and a remote access site. Emphasising redundancy, scalability, and security, it integrates AAA, NGFW, IPsec VPN, DMZ services, and dynamic routing with high availability.

# 2. Objectives

- Design and simulate a secure, scalable, and redundant enterprise network

- Implement AAA (RADIUS), VLANs, IPsec ADVPN, HSRP, NGFW, and zone-based firewall policies

- Demonstrate interoperability of Cisco and FortiGate equipment with dynamic routing protocols (OSPF, BGP)

- Develop comprehensive network documentation, topology maps, and configurations

# 3. Network Design Overview

## 3.1 Physical Topology

Illustrates device layout and interconnections. [Insert diagram image here]

## 3.2 Logical Topology

Describes VLAN, IP addressing, inter-VLAN routing, and IPsec VPN architecture. [Insert logical topology image]

# 4. Device Roles and Responsibilities

Include a table detailing each device’s purpose, IP address, and functions.

# 5. Routing and Redundancy

This section details the implementation of OSPF (with authentication), BGP (internal/external), and static routing (floating and stub). It also describes HSRP for gateway redundancy and ADVPN routing through FortiGate.

# 6. Security Design

Covers Cisco ACLs, port security, DHCP snooping, DAI, and FortiGate firewall/DoS policies.

# 7. VPN and Remote Access

Describes FortiGate IPsec ADVPN and remote access configuration, with authentication and tunnel management.

# 8. High Availability and DMZ

Describes Active-Active HA setup and virtual server implementation for simulated DMZ access.

# 9. Testing and Verification

Includes CLI output samples, verification commands, and validation screenshots or results.

# 10. Lessons Learned

Summarises technical and troubleshooting insights gained from the simulation.

# 11. Appendix

Include sample configurations, addressing schema, VLAN maps, and NAT policy examples.