# ****Cybersecurity and Secure WAN Design Report****

### ****Project:**** BrightMart Superstores Secure Wide Area Network (WAN)

### ****Author:**** DAVID AKINLALU

### ****Date:**** October, 2025

## ****1. Executive Summary****

BrightMart Superstores operates multiple retail outlets across several cities, each maintaining separate inventory records. The absence of a centralised tracking system has resulted in inefficiencies, including product shortages in some branches and overstocking in others. Additionally, outdated network infrastructure has left sensitive business and customer data vulnerable to interception and unauthorised access.

This report details the design and deployment of a **secure Wide Area Network (WAN)** interconnecting all BrightMart branches with the central headquarters. The new infrastructure enables **real-time inventory synchronisation**, enhances **data confidentiality and integrity**, and improves **overall operational efficiency**.

## ****2. Project Objectives****

* Establish a **secure, scalable WAN** connecting all branch locations to the headquarters.
* Implement **real-time inventory synchronisation** to ensure data consistency across all stores.
* Enhance **cybersecurity posture** through network segmentation, encryption, and access control.
* Provide a **foundation for centralised monitoring**, reporting and incident response.
* Support future scalability for additional branches or digital services.

## ****3. Existing Challenges****

| **Issue** | **Description** | **Impact** |
| --- | --- | --- |
| **Decentralised inventory records** | Each branch maintains separate records. | Stock mismatches and inefficiencies. |
| **Outdated infrastructure** | Legacy routers and switches without security controls. | High risk of data breaches. |
| **Lack of encryption** | Unsecured communication between branches. | Vulnerable to interception. |
| **Manual restocking decisions** | Based on outdated data. | Lost sales and customer dissatisfaction. |

## ****4. Proposed Network Design****

The new WAN design connects all BrightMart branches through a **hub-and-spoke topology**, with the **Headquarters (HQ)** serving as the central hub.

### ****Key Design Elements****

**Core Router (HQ):** Central point of control for all branch connections.

**Branch Routers:** Establish secure VPN tunnels to HQ.

**Servers:**

Inventory Database Server – hosts real-time synchronized data.

Authentication Server – manages user credentials and access rights.

Firewall & IDS/IPS – monitor and control inbound/outbound traffic.

### ****Technologies Used****

**Cisco Routers and Switches** (configured via Packet Tracer).

**IPSec VPN** for encrypted WAN communication.

**VLAN segmentation** to separate internal departments (e.g., Sales, Inventory, Management).

**Access Control Lists (ACLs)** for traffic filtering.

**Syslog and SNMP** for monitoring network performance and security events.

(The complete topology and configuration are demonstrated in the attached file: portfolio github.pkt.)

## ****5. Security Implementation****

| **Security Control** | **Description** | **Purpose** |
| --- | --- | --- |
| **VPN Encryption (IPSec)** | Encrypts WAN traffic between HQ and branches. | Prevents data interception. |
| **Firewalls** | Configured at HQ and each branch router. | Blocks unauthorised access. |
| **Intrusion Detection/Prevention (IDS/IPS)** | Monitors network for suspicious activity. | Early detection of threats. |
| **Access Control Lists (ACLs)** | Applied to routers and switches. | Limits access to authorised systems. |
| **User Authentication (AAA)** | Centralised control using RADIUS/TACACS+. | Ensures accountability and identity management. |
| **Regular Patching & Firmware Updates** | Keeps all devices secure. | Prevents exploitation of known vulnerabilities. |

## ****6. Real-Time Inventory Synchronization****

* Implemented through **centralised database replication**.
* Each branch updates stock levels in real time via secure WAN links.
* Data is synchronised automatically at HQ, ensuring accurate stock visibility across all outlets.
* **REST APIs** or **secure database connectors** handle inter-branch communication.

## ****7. Risk Assessment****

| **Threat** | **Likelihood** | **Impact** | **Mitigation** |
| --- | --- | --- | --- |
| Data interception | Medium | High | IPSec VPN encryption |
| Unauthorised access | High | High | Strong access control & authentication |
| Malware infection | Medium | Medium | Endpoint protection & IDS |
| Hardware failure | Low | High | Redundant routers & backups |
| Insider threats | Medium | High | Least privilege policies & audit logs |

## ****9. Testing and Validation****

**Packet Tracer Simulation:** Verified VPN tunnel integrity, routing tables, and VLAN segmentation.

**Ping and Traceroute Tests:** Confirmed secure data flow between branches and HQ.

**Access Control Verification:** Tested ACL rules to ensure proper isolation.

**Failover Simulation:** Confirmed network resilience under link failure scenarios.

## ****10. Conclusion****

The implemented **secure WAN architecture** successfully addresses BrightMart’s operational and cybersecurity challenges. It establishes a foundation for centralised management, real-time inventory updates, and future scalability while ensuring the protection of sensitive data.

This project demonstrates a comprehensive application of **network engineering and cybersecurity principles**, aligning with real-world enterprise deployment standards.