Project Proposal: Implementation of a Multi-Tiered Defense-in-Depth Security Framework

1. Executive Summary: The Real-World Scenario

In the modern corporate landscape, a single firewall is no longer sufficient to protect sensitive assets. This project addresses the critical real-world problem of **"Perimeter Vulnerability."** By simulating a high-security enterprise environment, this project demonstrates how to protect a **Windows Server 2012 R2** (hosting private databases or applications) using a **Back-to-Back Firewall** architecture. This ensures that even if one security layer is compromised, the core data remains protected by secondary and tertiary defense barriers.

2. Network Architecture & Security Zones

To mirror an actual enterprise network, the topology is segmented into three distinct functional zones:

- **The Untrusted WAN (Red Zone):** Represents the public internet, containing the **NATNode-ISP** and the **Cisco c3725 Edge Router (R1)**.
- **The Demilitarized Zone (DMZ - Yellow Zone):** A neutral buffer zone hosting the **WEB-SERVER-DMZ**. This allows external users to access the company website without ever touching the internal network.
- **The Trusted Internal LAN (Green Zone):** The high-security "Vault" containing the **Windows Server**, **CORE-SW**, and departmental users (**IT-MAN** and **SALES-DEP**).

3. The Engine: High-Performance Virtualization

A key technical highlight of this submission is the utilization of the **GNS3 VM (Oracle VirtualBox)** as the server for all high-performance nodes.

- **Stability for Large Topologies:** While running **ten active nodes** simultaneously, the **GNS3 VM** provides dedicated CPU and RAM resources to the **FortiGate firewalls** and **Windows Server**, preventing the lag typically found in local simulations.
- **Logical Isolation:** By hosting the "heavy" nodes on the VM, the network remains stable and the "Servers Summary" remains **Green**, ensuring that security policies are processed with real-world timing and accuracy.

4. Technical Security Features

- **Dual Inspection:** Traffic must pass through the **Edge Firewall (FortiGate-2)** and the **Internal Firewall (FortiGate-1)**.
- **VLAN Segmentation:** The **ACCESS-SW** and **CORE-SW** use **802.1Q Trunking** to separate departments (Sales vs. IT), preventing "Lateral Movement" by unauthorized internal users.
- **Zero-Trust DMZ:** The internal firewall treats the DMZ as a potential threat zone, blocking any traffic from the **WEB-SERVER-DMZ** to the **Windows Server**.

5. Testing & Validation Plan

To prove the design works in a real-world scenario, the following tests are performed:

- **IT-MAN to Server:** Success (Proves internal productivity).
- **DMZ to Server: Blocked** (Proves the internal firewall is protecting the core asset).
- **Internal to Internet:** Success (Proves the full path through R1 and NAT is functional).

6. Troubleshooting Framework

In a corporate environment, downtime is costly. This project includes a validation protocol:

1. **Check VM Status:** Ensure the **GNS3 VM** is green and providing sufficient CPU.
2. **Verify Routing:** Use show ip route on **R1** to check the ISP path.
3. **Policy Audit:** Use FortiGate logs to ensure that firewall rules are not accidentally blocking legitimate business traffic.