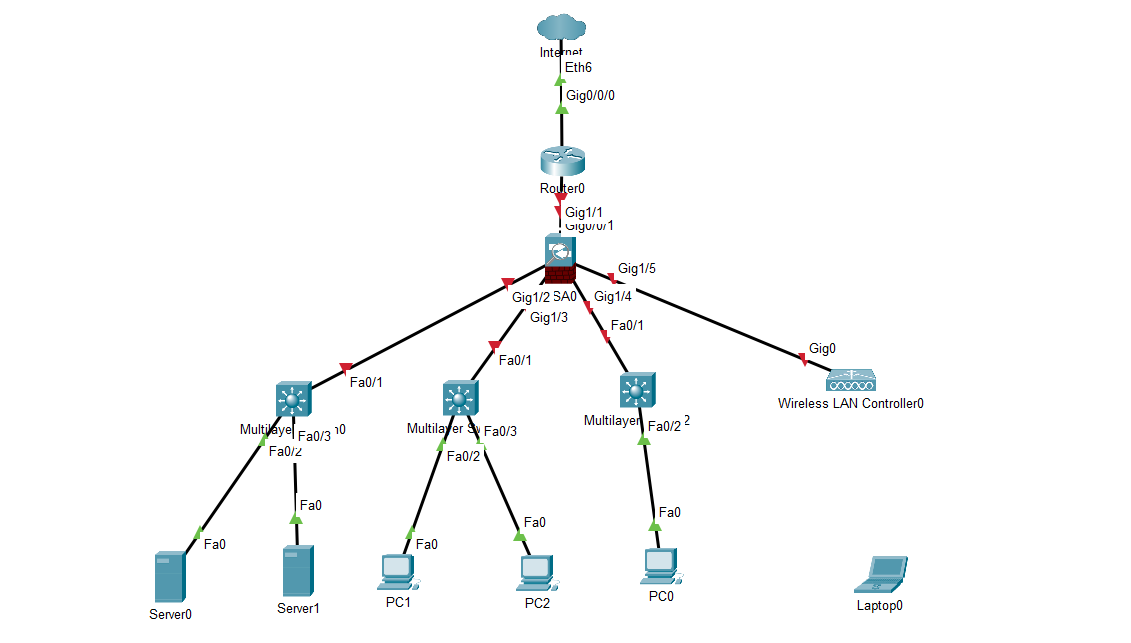
**Week 6:  Capstone Network Security Project**

**Objective:**  Simulate a secure network environment with monitoring and defense.

**Task#01: Design a secure network topology with VLANs, firewall, VPN, and IDS placement.**

**Solution:**



This diagram illustrates a **secure network setup for an organization**, built using Cisco Packet Tracer components. Its main goal is to protect internal systems and data by carefully controlling who can access what, both from the internet and within the network.

The core of the design is a **Main Router**, which acts as the central **firewall** and **VPN concentrator**. It connects the entire internal network to the **Internet (Cloud)** and enforces strict rules on all incoming and outgoing traffic. Remote users can securely connect through the VPN to access internal resources.

The internal network is divided into several isolated sections using **VLANs (Virtual Local Area Networks)**, implemented on **Multi-Layer Switches**:

* **DMZ VLAN:** For public-facing servers (like websites or email servers) that need to be accessible from the internet, but are kept separate from the main internal network.
* **Internal LAN VLAN:** For employee computers and internal servers, where most daily work happens.
* **Management VLAN:** A highly restricted network specifically for IT administrators to securely manage network devices.
* **Guest Wi-Fi VLAN:** Provides internet access for visitors, completely isolated from all company resources.

While Packet Tracer doesn't have dedicated security appliances, the design conceptually includes **IDS/IPS (Intrusion Detection/Prevention Systems)** on critical servers and at key network points to monitor for suspicious activity.

In essence, this topology creates a **layered defense**, ensuring that even if one part of the security is bypassed, other layers are in place to detect or prevent further intrusion, thereby enhancing the overall security posture of the network.