### **Project Deliverable #6: Midterm Presentation and VPN Access Control Configuration**

#### 

#### **1. Purpose of the Deliverable**

To successfully present the midterm project overview, covering the VPN project's scope, objectives, and business impact while implementing and validating VPN access control policies designed for secure remote work. This deliverable aims to demonstrate project milestones, solutions for encountered challenges, and the security measures essential for business use.

#### **2. Components of the Deliverable**

* **Midterm Presentation Preparation**:
  + **Objective**: To deliver a structured project update, focusing on the business scope (98%) with minimal technical content (2%) as guided by the project advisor.
  + **Key Content**:
    - **Project Scope and Objectives**: Present the VPN’s role in enhancing secure remote communication, targeting a comprehensive solution for site-to-site and client-based VPN access.
    - **Team Contributions**: Acknowledgment of each team member's specialized roles, including network engineering, documentation, security, design, compliance, and R&D, contributing to the VPN’s development.
    - **Research Integration**: Incorporate findings on advanced security protocols, including IPsec, SSL/TLS, and MPLS, with detailed insights into their contribution to VPN security.
    - **Challenges & Resolutions**: Highlight the recent challenges faced with routing issues and protocol compatibility, detailing the collaborative problem-solving process led by Karan and Ishan Patel.
    - **Business Impact**: Emphasize the significance of VPN access control policies for supporting secure remote working, ensuring data integrity and network security in business settings.
* **VPN Access Control Configuration**:
  + **Overview**: Configuration of VPN access control policies in Cisco Packet Tracer, enabling user role-based access control to prevent unauthorized access, vital for secure remote connectivity.
  + **Security Protocol Integration**: Advanced research led by Ishan Patel, Charmi Balar, and Karan on IPsec, SSL/TLS, and MPLS protocols has been incorporated to strengthen VPN security.
  + **Testing and Validation**: The team, led by Karan and Ishan Patel, tested the configuration and functionality of access control policies. Testing included routing configurations to ensure VPN security features aligned with remote work requirements, passing all initial tests.
  + **Remote Work & Access Control Research**: Continued research on Remote Working and VPN Access Control Policies informed policy configurations, especially focusing on secure remote work.
* **Additional Activities in Week 8**:
  + **Lecture & Quiz on Stress Management**: Completed on October 21, 2024, with the participation of all team members, contributing 1 hour each to develop skills in managing project-related stress effectively.
  + **Team Meetings**: Held two team meetings during the week to finalize presentation content, align tasks, and review project activities for the midterm update.

#### **3. Next Steps**

* **Midterm Review Adjustments**: Adjust access control policies and configurations based on feedback received during the midterm presentation.
* **Protocol Testing**: Continue integrating and testing advanced security protocols to ensure VPN robustness and maintain compliance with secure remote working standards.
* **Documentation**: Update the documentation with details on completed configurations, testing results, and research findings to maintain a comprehensive project log.