**Week Dates:** September 16 - September 20, 2024

**Team Progress:** During Week 3, our team made notable progress in the project, although some challenges surfaced. We began by assigning roles through the Project Team Sign-off Organization Form, ensuring that each member had clear responsibilities. We also collaborated to create a team name and logo, overcoming creative hurdles with effective brainstorming.

The AIP Team Mandate Form set clear goals and procedures, guiding us forward. Leadership played a crucial role as we presented our company to the class, merging everyone's ideas into a cohesive and compelling presentation.

On September 20, we welcomed a new team member, which further enhanced our capacity for collaboration and allowed us to divide tasks more efficiently.

**Research Activities:** This week, the team focused heavily on researching various aspects of VPN technologies, specifically targeting Site-to-Site VPN and Client VPN configurations. Key areas explored included:

* **VPN Protocols:**We explored secure protocols like IPsec and OpenVPN, evaluating encryption methods such as AES-256 and comparing authentication techniques, including pre-shared keys and certificates.
* **Routing Configurations:**We studied static route setups to ensure proper traffic flow between the Canadian and Indian offices. Additionally, we reviewed best practices for implementing Access Control Lists (ACLs) to restrict access based on user roles.
* **Client VPN Setup:**Research on setting up remote access VPNs for employees focused on user authentication and IP address allocation.

**Discussions on Topologies:**

* **Network Topologies for Site-to-Site VPN:**The team explored various topologies, including hub-and-spoke and mesh configurations, aiming to find the most effective structure for communication between the two offices.
* **Client VPN Integration:**We also discussed how Client VPNs could be integrated for remote users, ensuring secure access to both offices' resources while maintaining security standards.

**Roadblocks Encountered:**

* **Complex Configurations:**Some team members found it difficult to grasp the complexities of VPN gateway and protocol configurations.
* **Packet Tracer Limitations:**We encountered limitations in Packet Tracer, which restricted our ability to simulate more advanced VPN setups effectively.

**Solutions Implemented:**

* **Enhanced Training:**Peer-led training sessions helped simplify complex topics, ensuring better understanding across the team. We also used online resources and tutorials to improve our practical skills in Packet Tracer.
* **Alternative Simulation Tools:**We discussed switching to GNS3 for more robust VPN simulation features, planning a gradual transition if Packet Tracer proves insufficient for our needs.

**Next Steps:**

* Finalize the Site-to-Site VPN configuration in Packet Tracer based on our research and the SOP that will be provided by the project advisor.
* Begin setting up the Client VPN, focusing on user authentication and access controls.
* Prepare a preliminary report on the security measures for both VPN connections.