Mini Project 17: Cloud Security Part 2

Mini-Project Overview

Time Estimate: 1 hour

The purpose of this assignment is to build upon the work you did in **Mini-Project 17: Cloud Security Part 1.** As you may recall, you wrote a paper outlining the implementation of an access control solution for an insurance company that has decided to move claims information to either Azure or AWS.

You may find it helpful to refer back to part 1 for the overview of the importance of scoping a move to the cloud, and why businesses need to assess security in the context of this environment and evaluate Cloud Service Providers (CSPs) accordingly.

Project Submission Steps

Review the scenario in **Mini-Project 17: Cloud Security Part 1**, as well as the paper you wrote on how the company should implement a strong access controls solution.

Assignment

Paper (2–4 Pages)

The company was pleased with your plan for implementing an access control solution to limit access to only authorized agents of the company. In fact, they were so impressed that they now want you to come up with a plan for securely transmitting data created by cloud-based instances of the application back inside the corporate firewall. Specifically, they want to know how they can leverage VPN technologies to accomplish this.

To this end, write a 2–4 page paper on what you think the company should do. Be sure to stick with the same cloud provider you chose in **Cloud Security Part 1.** In other words, if your paper was based on Azure, then stay with that choice for this paper, and vice versa. Your paper should include critical items such as authentication methods and encryption protocol support, as well as any potential drawbacks. For example, authentication methods could be via Active Directory, or it could use certificates. Secure protocols could include PPTP, L2TP/IPSec, and SSL.