## Lab 7-01: Understanding IAM and Basic Network Security in the Cloud

### Service Introduction

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS services and resources for your users. Basic network security in the cloud involves setting up Virtual Private Clouds (VPCs), subnets, security groups, and network Access Control Lists (ACLs) to ensure secure communication and access control.

### Problem

Your organization is moving its infrastructure to AWS and needs to ensure that only authorized personnel can access specific resources. Additionally, you need to set up a secure network architecture to protect your applications and data from unauthorized access and potential threats.

### Solution

Use AWS IAM to create and manage users, groups, and roles and apply policies that define permissions for accessing AWS resources. Set up a secure VPC with appropriate subnets, security groups, and network ACLs to control inbound and outbound traffic. This will ensure that access to resources is strictly controlled and your network infrastructure is secure, meeting compliance and security requirements.

#### Task 1: Create a New User in IAM

|  |
| --- |
| 1. Navigate to IAM.      1. In the left navigation menu, click **Users.** 2. In the upper right corner, click **Create user.**      1. For User name, enter ips-user.      1. Select Provide user access to the AWS Management Console. 2. For Console password, select Autogenerated password. 3. Click **Next.**      1. For Permissions options, select Attach policies directly.      1. In the Permission policies menu that appears, click on the checkbox next to AdministratorAccess.      1. Click **Next.**      1. Click **Create user.**      1. Click **Return** **to users list.**      1. On the pop-up menu that appears, click **Continue.**      1. You should now see ips-user. |

#### Task 2: Create Firewall Rules to Allow Certain Traffic within the Network

|  |
| --- |
| 1. In the AWS Management console, navigate to **VPC** through search bar**.**      1. In the upper left corner, under Filter VPC, click on the dropdown menu and select the default VPC that appears. 2. In the left navigation menu, under Security, click **Security groups.** 3. In the upper right corner, click **Create security group.**      1. For the Security group name, enter ips-sg. 2. For Description, enter sg for our services.      1. Under Inbound rules, click Add rule and select the following:  * For Type, select HTTP. * Next to Source, select the 0.0.0.0/0 CIDR block. * Under Inbound rules, click Add rule again. * For Type, select HTTPS. * Next to Source, select the 0.0.0.0/0 CIDR block. * Under Inbound rules, click Add rule one last time. * For Type, select All ICMP - IPv4. * Next to Source, select the 0.0.0.0/0 CIDR block.      1. Scroll down, and click **Create** **security group.** |