**Lab 16: Azure Network Security with VNets**

**Introduction:**

In Azure, Virtual Networks (VNets) provide a way to securely isolate and control traffic between Azure resources. When it comes to Azure Machine Learning (AML), VNets are essential to restrict access to your workspace, improve security, and control network communication. This lab will guide you through creating and configuring a VNet to secure your Azure Machine Learning workspace.

**Objectives:**

* Create a Virtual Network in Azure.
* Set up address spaces and subnets.
* Integrate the Virtual Network with Azure Machine Learning workspace.

**Steps:**

**Part 1: Creating a Virtual Network (VNet)**

**Step 1:** Access the Virtual Networks Service

* **Explanation**: Virtual Networks are configured within the "Virtual Networks" service in Azure.
* **How to Do It**: In the Azure portal, search for "Virtual Networks" in the search bar and click on the result to open the service.

**Step 2:** Create a New Virtual Network

* **Explanation**: A VNet provides a secure and isolated network for your Azure resources.
* **How to Do It**:
  + Click on the "Create" button to start the creation process.
  + In the "Basics" tab, select the Subscription and Resource group to use.
  + Provide a name for the Virtual Network (e.g., "AML-VNet").
  + Choose the region where your Azure Machine Learning workspace is located.

**Step 3:** Configure IP Address Space and Subnets

* **Explanation**: Configuring the address space and subnets ensures proper network segmentation and routing.
* **How to Do It**:
  + Click "Next" to navigate to the "IP Addresses" tab.
  + Check the "Address space" to ensure it's adequate for your network needs.
  + Ensure there's at least one subnet available for your resources. If needed, click "Add subnet" to create one, and provide a name and subnet address range (e.g., 10.0.0.0/24).

**Step 4:** Review and Create the VNet

* **Explanation**: Finalize the VNet setup by reviewing the configurations.
* **How to Do It**:
  + Click "Review + create" to review the VNet configurations.
  + Click "Create" to complete the process.
  + Wait for the VNet to be deployed before proceeding.

**Part 2: Integrating the VNet with Azure Machine Learning Workspace**

**Step 1:** Access the Azure Machine Learning Workspace

* **Explanation**: The workspace needs to be connected to the VNet to restrict access and control traffic.
* **How to Do It**: In the Azure portal, search for "Machine Learning" and select the Machine Learning workspace.

**Step 2:** Configure Network Settings for the Workspace

* **Explanation**: Network settings allow you to secure the workspace by restricting access to the VNet.
* **How to Do It**:
  + In the workspace menu, select "Networking."
  + Click "Private endpoint" to create a private endpoint for the workspace, which will secure the traffic.

**Step 3:** Connect the Workspace to the VNet

* **Explanation**: Integrating the workspace with the VNet ensures only authorized traffic can reach the workspace.
* **How to Do It**:
  + In the private endpoint setup, select the VNet you created earlier.
  + Choose the subnet within the VNet where the workspace should be connected.
  + Click "Create" to set up the private endpoint.

**Step 4:** Verify the Integration

* **Explanation**: Ensuring that the workspace is correctly linked to the VNet guarantees the desired security.
* **How to Do It**: In the Azure portal, navigate to the VNet and check the connected devices and resources to confirm that the workspace is listed.

**Summary:**

In this lab, you created a Virtual Network in Azure, configured its address space and subnets, and integrated it with the Azure Machine Learning workspace. This integration allows you to better control and secure network traffic, ensuring that only authorized users and applications can access your machine learning environment.