**Research and Development Document**

**ON**

**Azure Three-Tier Architecture**

****

****

**By**

**Anirudh Sharma**

**(CT\_CSI\_CI\_66)**

**Under**

**Celebal Summer Internship**

**in**

**Cloud Infra & Security**

**Table of Contents**

**Azure Three Tier Architecture…………………………………………………………………….****3**

**Inbound and Outbound Networking…………………………………………………………….. 4**

**Azure Firewall……………………………………………………………………………………….. 5**

**Assignment………………………………………………………………………………………….. 7**

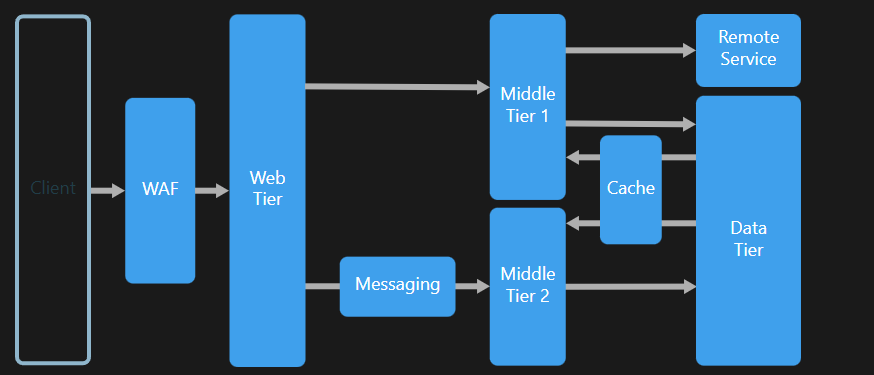
**References…………………………………………………………………………………………. 17**

**Azure Three Tier Architecture**

Three-tier architecture is a well-known software architecture pattern that separates an application into three logical layers:

1. Presentation Layer:
   * Handles client requests (HTTP/HTTPS)
   * Hosts front-end applications (e.g., HTML/CSS, React, etc.)
   * Azure Resources: Web Server VMs with Apache (Linux) or IIS (Windows)
2. Application Layer:
   * Processes business logic
   * Communicates between Web and Database Tier
   * Azure Resources: Backend App VMs (API servers, .NET, Node.js, etc.
3. Data Layer:
   * Stores application data
   * Azure Resources: SQL Server, MySQL, or NoSQL on Linux/Windows VMs

Azure N-tier architecture divides an application into logical layers and physical tiers.



Layers are a way to separate responsibilities and manage dependencies. Each layer has a specific responsibility. A higher layer can use services in a lower layer, but not the other way around.

Tiers are physically separated, running on separate machines.

A traditional three-tier application has a presentation tier, a middle tier, and a database tier. The middle tier is optional. More complex applications can have more than three tiers. The diagram above shows an application with two middle tiers, encapsulating different areas of functionality.

An N-tier application can have a closed layer architecture or an open layer architecture:

* In a closed layer architecture, a layer can only call the next layer immediately down.
* In an open layer architecture, a layer can call any of the layers below it.

## **Usage of N-Tier Architecture**

N-tier architectures are typically implemented as infrastructure-as-service (IaaS) applications, with each tier running on a separate set of VMs.

* Simple web applications.
* A good starting point when architectural requirements are not clear yet.
* Unified development of on-premises and cloud applications.

## **Benefits of N-Tier Architecture**

* Portability between cloud and on-premises, and between cloud platforms.
* Open to heterogeneous environment (Windows/Linux)

## **Challenges of N-Tier Architecture**

* Managing an IaaS application is more work than an application that uses only managed services.
* It can be difficult to manage network security in a large system.
* User and data flows typically span across multiple tiers, adding complexity to concerns like testing and observability.

**Inbound and Outbound Networking**

**Inbound networking** refers to traffic coming into your resources from the outside, while **Outbound networking** refers to traffic leaving your resources to the outside. Managing both is crucial for security and performance, ensuring resources are protected and only accessible to authorized users and applications. Azure provides various tools and features to control both inbound and outbound traffic, including Network Security Groups (NSGs), Azure Firewall, and NAT gateways.

In our previous assignments, we have learned about Inbound and Outbound Networking in Network Security Groups (NSG).

### **Examples of Inbound Traffic:**

* User browsing a website (HTTP/HTTPS to port 80/443)
* Application tier calling an API on the web tier.

### **Azure Controls:**

1. **NSG Inbound Rules**:
   * Controls who can initiate connections to a resource.
   * Rules are applied at the **subnet level** and/or **NIC level**.
2. **VM OS Firewall**:
   * Even if the NSG allows traffic, the VM’s internal firewall must also allow it.

### **Examples of Outbound Traffic:**

* Web tier connecting to backend app APIs
* VMs downloading updates or packages from the internet

### **Azure Controls:**

1. **NSG Outbound Rules**:
   * Define where the VM can send traffic.
   * By default, Azure allows outbound to the internet unless blocked.
2. **Route Tables:**
   * Can control traffic flow — e.g., force traffic through an Azure Firewall or NVA.
3. **Public IP or NAT Gateway**:
   * Required for outbound internet access (unless using a proxy or firewall).

**Azure Firewall**

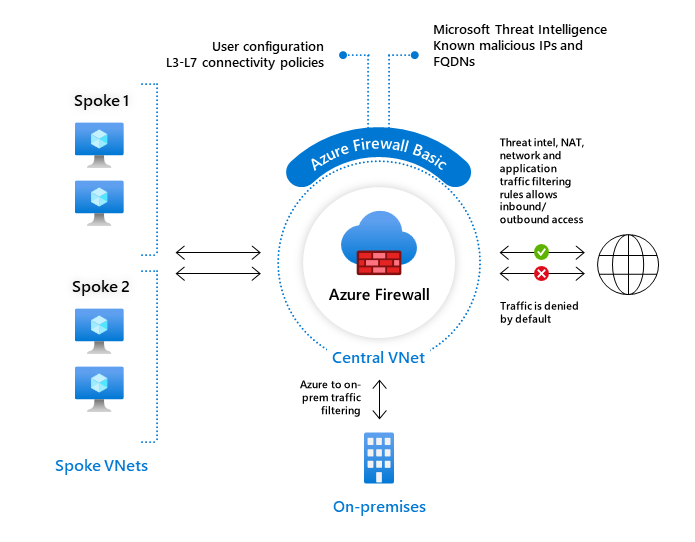
A firewall in cloud computing is a security service or virtual appliance that monitors and controls incoming and outgoing network traffic based on predetermined security rules like traditional firewalls, but designed specifically for cloud environments.

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a stateful, centralized firewall that provides built-in high availability and scalability. Azure Firewall can be used to create and enforce application and network connectivity policies across subscriptions and virtual networks.

Azure Firewall is available in three Stock Keeping Unit: Basic, Standard, and Premium.

## **Azure Firewall Basic**

Azure Firewall Basic is designed for small and medium-sized businesses (SMBs) to secure their Azure cloud environments. It provides essential protection at an affordable price.

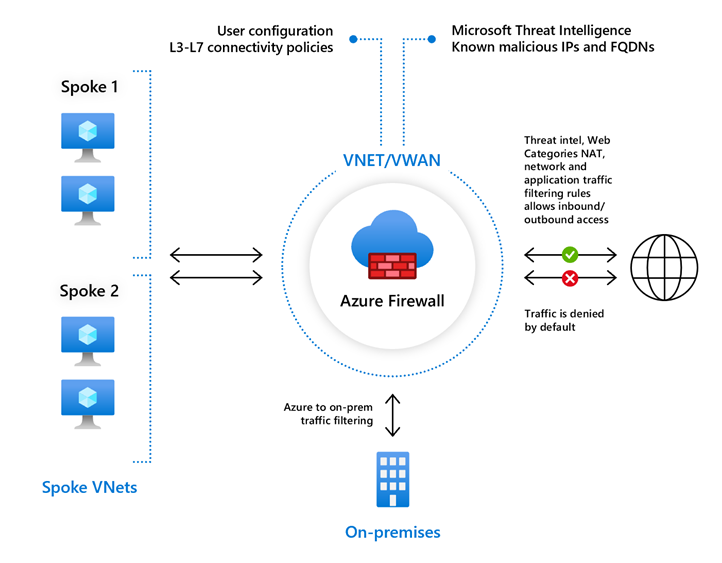


Key limitations of Azure Firewall Basic include:

* Supports Threat Intel alert mode only
* Fixed scale unit with two virtual machine backend instances
* Recommended for environments with an estimated throughput of 250 Mbps

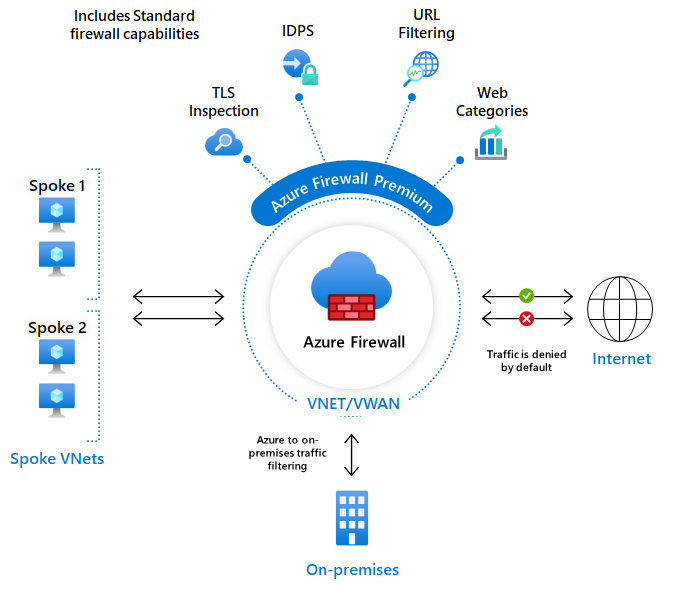
## **Azure Firewall Standard**

Azure Firewall Standard offers L3-L7 filtering and threat intelligence feeds directly from Microsoft Cyber Security. It can alert and block traffic from/to known malicious IP addresses and domains, updated in real-time to protect against new and emerging threats.



## **Azure Firewall Premium**

Azure Firewall Premium provides advanced capabilities, including signature-based IDPS for rapid attack detection by identifying specific patterns. These patterns can include byte sequences in network traffic or known malicious instruction sequences used by malware.



## **Azure Firewall Manager**

Azure Firewall Manager allows us to centrally manage Azure Firewalls across multiple subscriptions. It uses firewall policies to apply a common set of network and application rules and configurations to the firewalls in your tenant.

**Assignment**

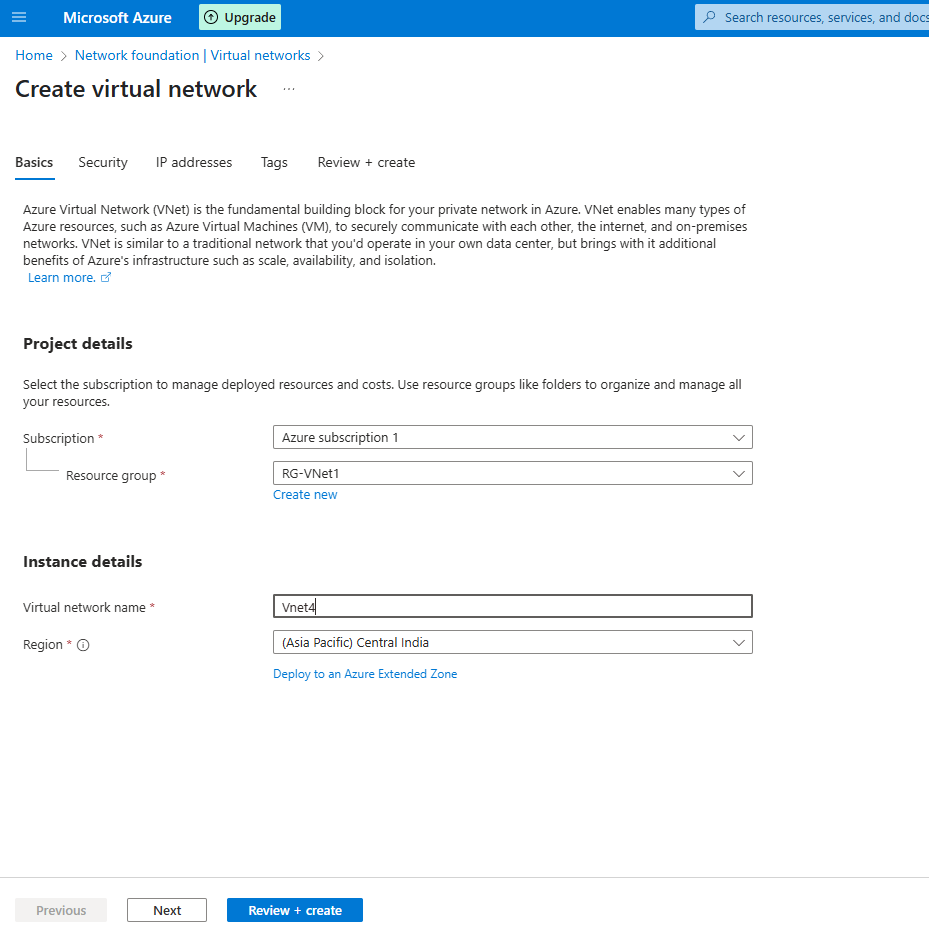
Create three subnets: 1. Web tier 2. App tier 3. DB tier DB Tier should not access any tier (Web & App tier) App tier should access the DB tier and Web tier as well, Web tier should access only App tier. Only Web tier is allowed to connect to the internet. Deploy two VM's in each tier (One VM should be Linux & another should be Windows). Configure Apache Server on Linux VM's And IIS Server on Windows.

**A computer screen shot of a diagram

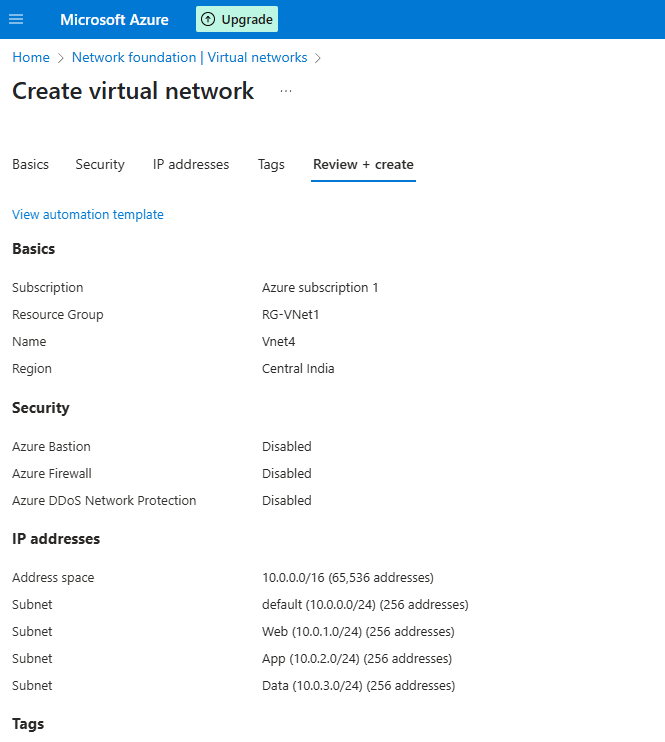
AI-generated content may be incorrect.**

**Step 1: Creating three Subnets:**

1. **Create a new Vnet (Vnet4)**

****

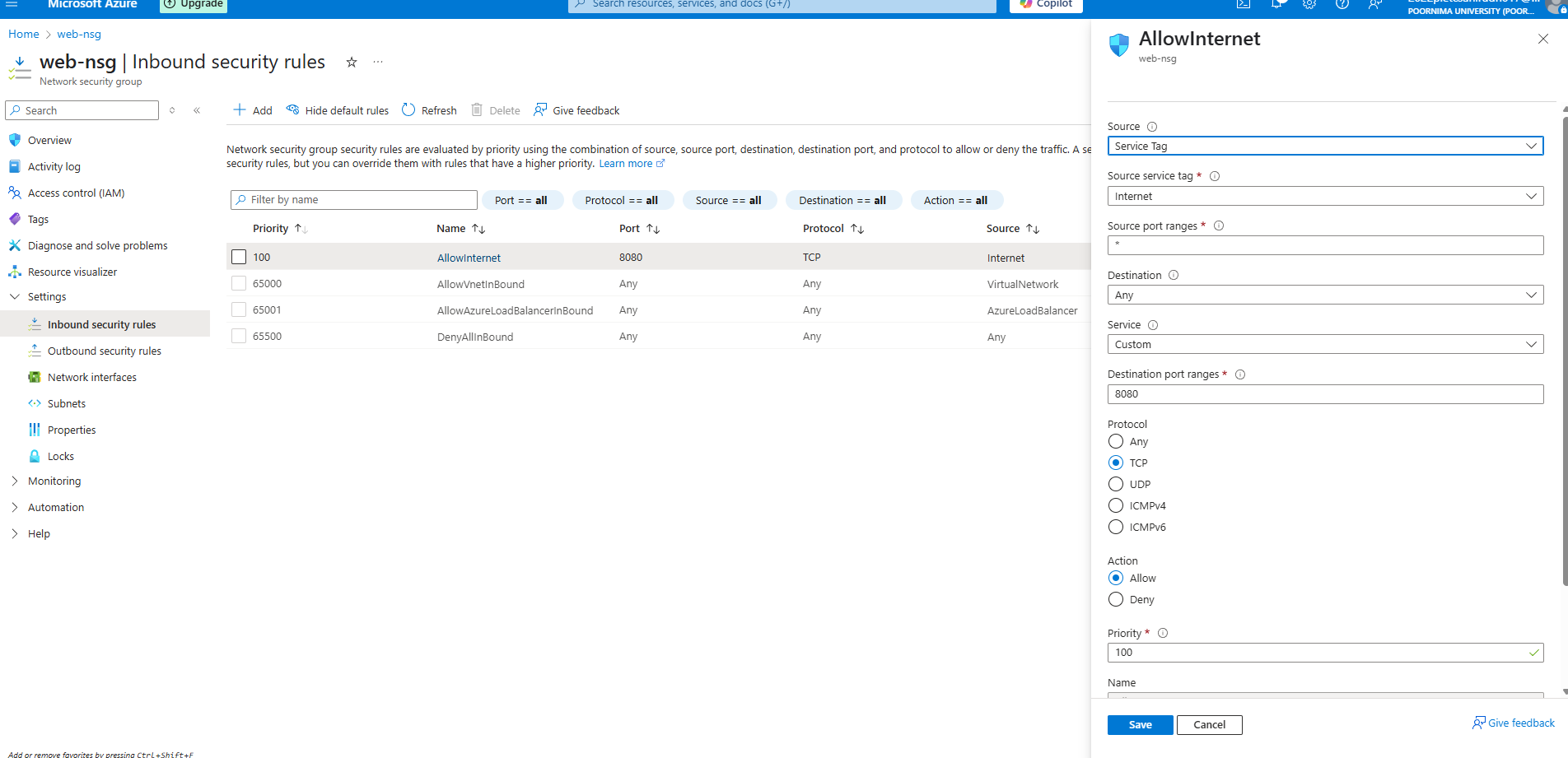
1. **Give IP in address space (10.0.0.0/16)**
2. **Provide Subnets to Web, App & Data Tier**

****

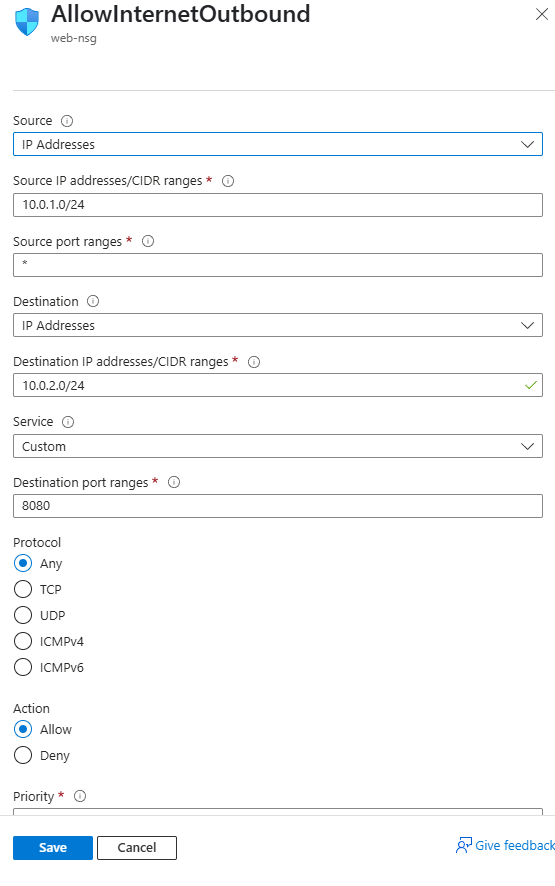
**Step 2: Creating NSG**

**Here, I am creating 3 NSGs for web, app and Data and providing rules as given in the assignment:**

**Web-nsg (Inbound)**

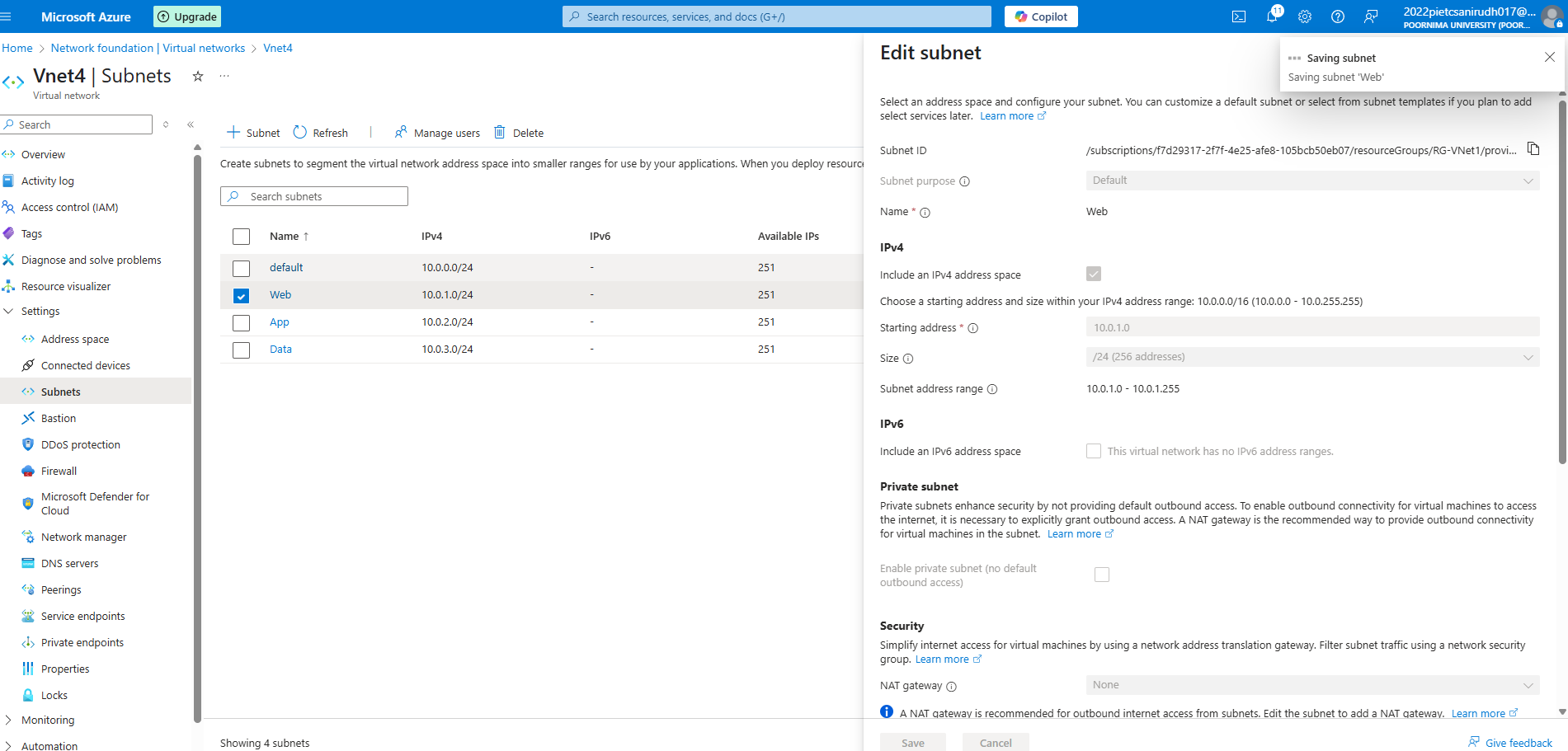
****

**Web-Nsg (Outbound):**

****

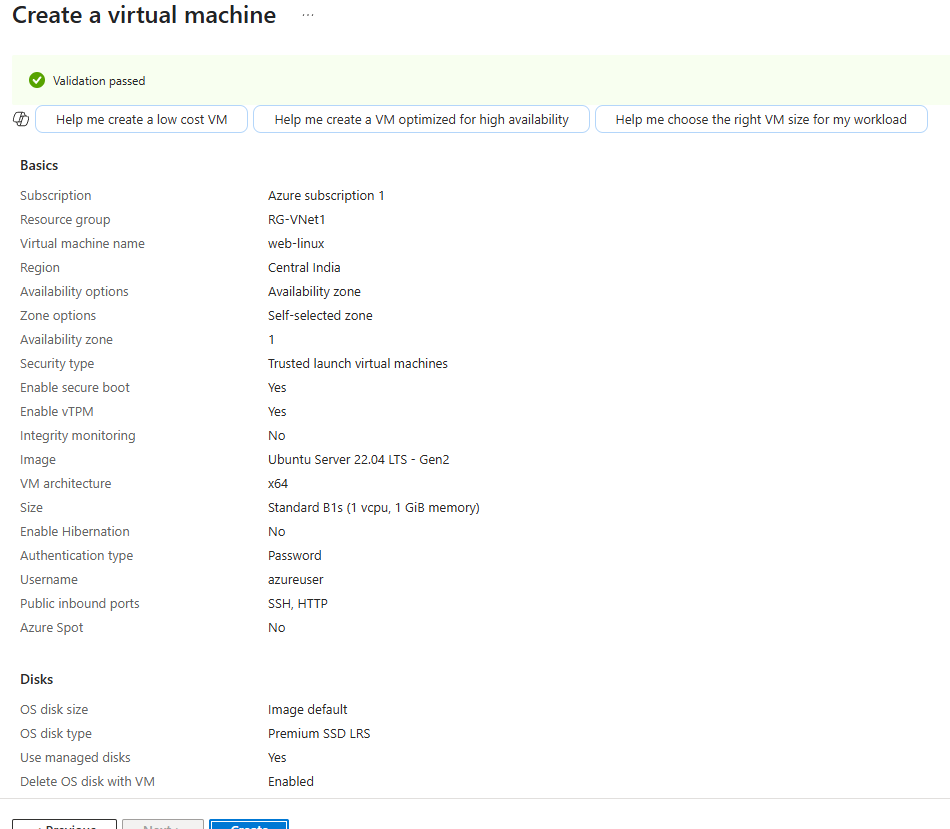
Do the same for App-nsg and Data-nsg

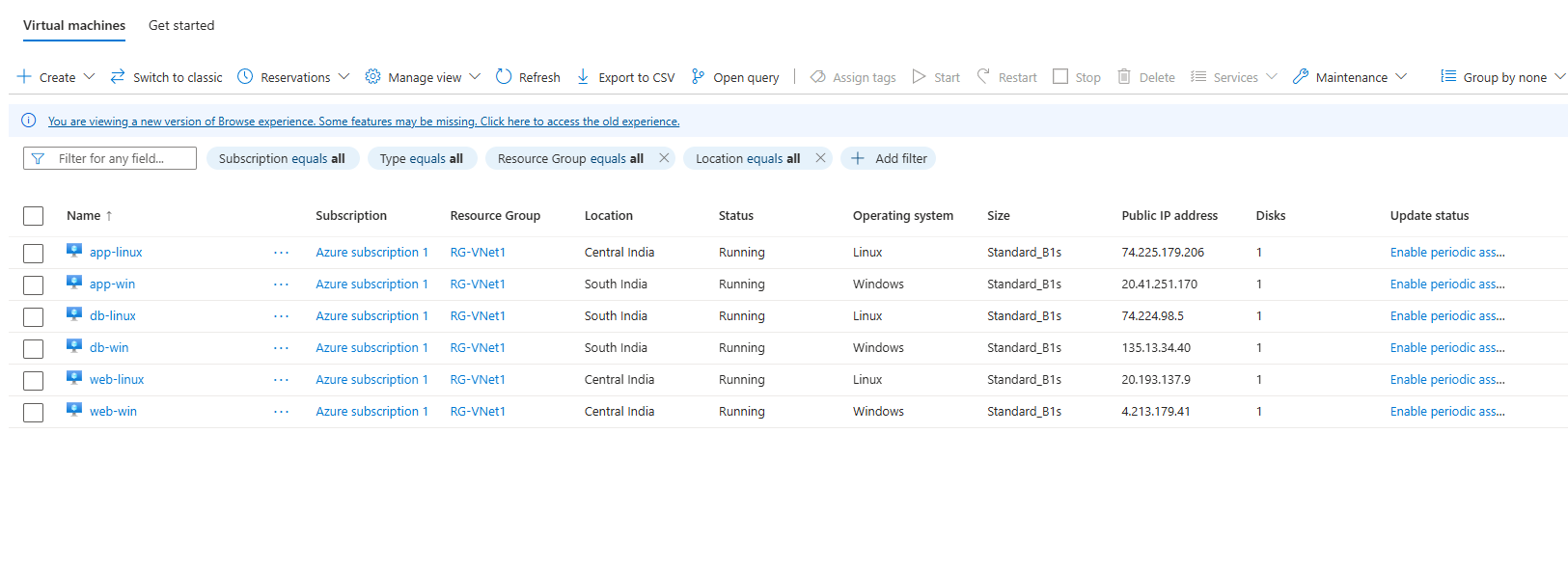
**Step 3: Associate NSG with its respective subnets**

****

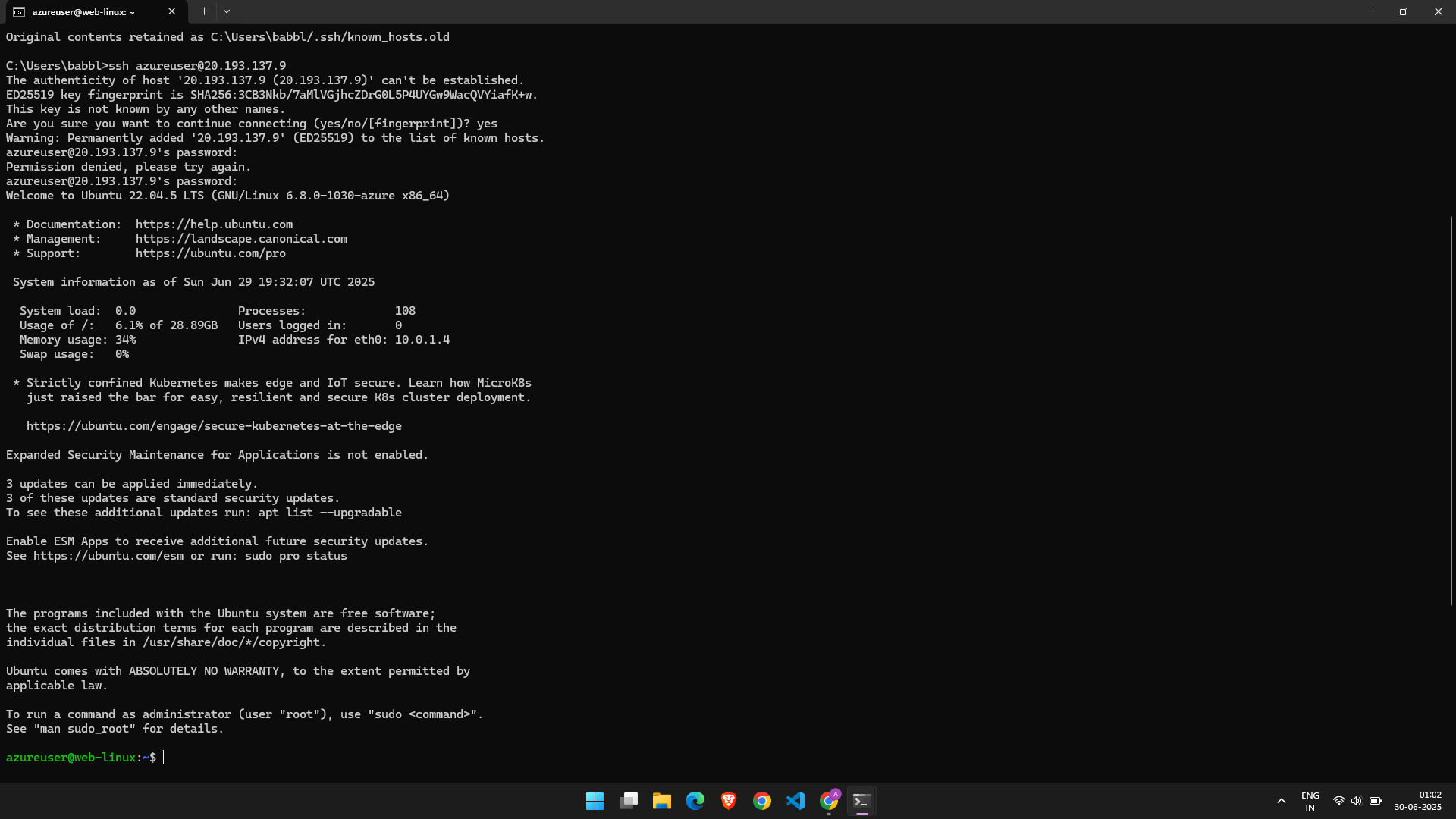
**Do the same for Data-nsg & App-nsg**

**Step 4 : Creating VM (one in windows and other in Linux)**

****

****

**Do the same for App and Data VM**



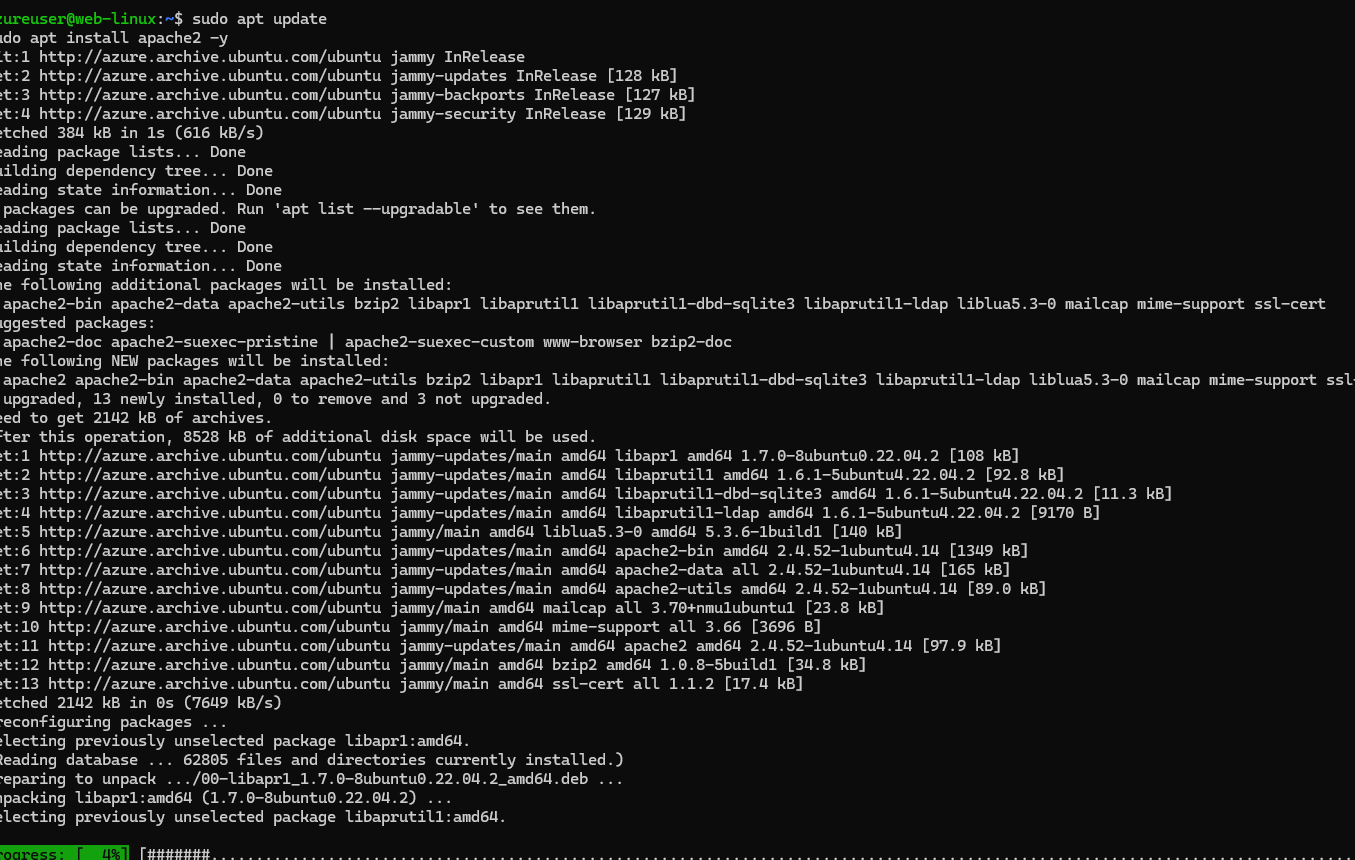
**Accessing my vm – web-linux using public IP on my local system**

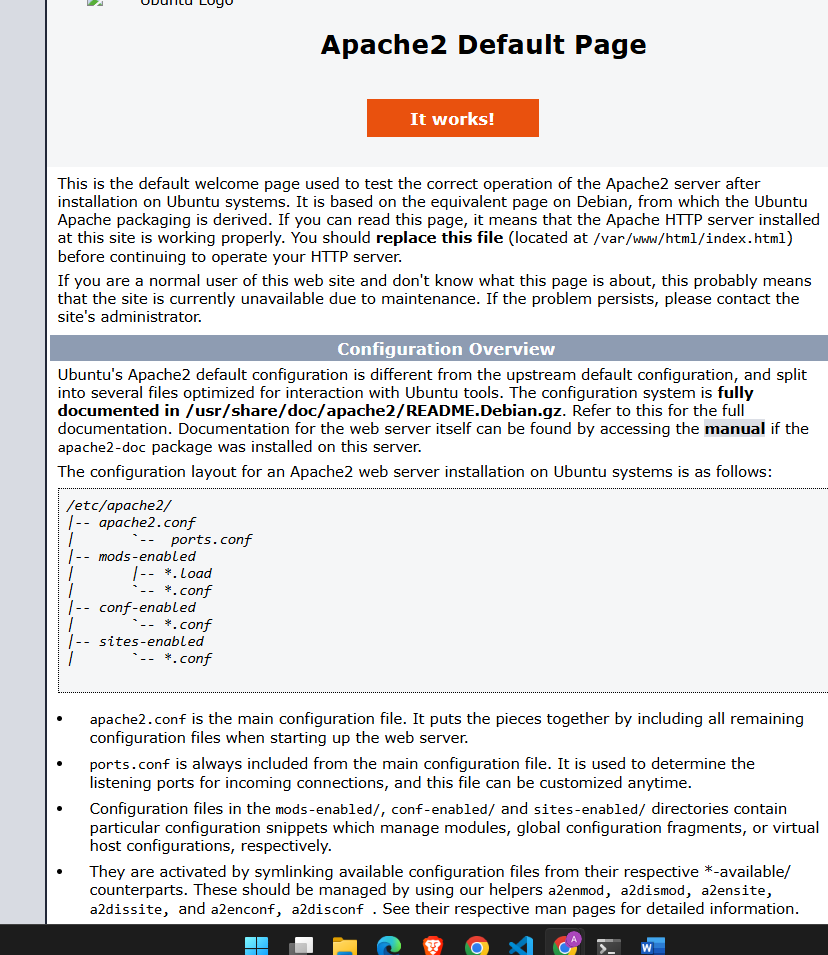
**Step 5: Configure Apache Server on Linux VM's And IIS Server on Windows.**

**Apache Server Command:**

sudo apt update

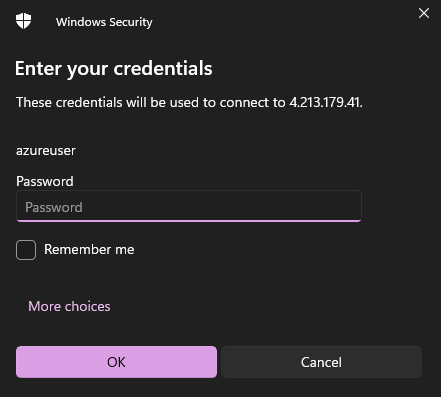
sudo apt install apache2 -y

**A computer screen shot of a computer

AI-generated content may be incorrect.**

**IIS installation command :**

Install-WindowsFeature -Name Web-Server -IncludeManagementTools

**A computer screen shot of a computer

AI-generated content may be incorrect.A screen shot of a computer

AI-generated content may be incorrect.**

**Do this in every VM of Windows and Linux Respectively.**

**Make sure that you choose correct service in Security rules for all the VMs. i.e.**

**For Linux – SSH**

**For Windows - RDP**

**References**

* **Microsoft Azure Documentation**
* **Medium**
* **Dev.to**
* **John Savill - YouTube**