**Azure Networking Interview Q&A**

**What is the difference between NSG and ASG ?**

ASGs are applied to VMs and are used in conjunction with NSGs. By associating an ASG tag with a network security rule, you can define rules that apply to a group of VMs sharing the same tag. ASGs simplify the management of security rules in a multi-tier application by grouping VMs that belong to the same application tier. This makes it easier to apply and manage security policies for a specific application.

**How can you block the access to a your vm from a subnet ?**

By default traffic is allowed between subnets with in the VNet in Azure. This is because of a default NSG rule “AllowVnetInBound”.

The priority of this rule is 65000, so we need to create a Deny rule with less than 65000 priority number.

**Are Azure NSGs stateful or stateless ?**

They are stateful in nature. That means if you allow a port for inbound traffic traffic to receive the request. You don’t have to open the port in outbound rules to send response back.

Example: If you host a host an application on port 80 in azure vm and allow inbound traffic for customers to access it. You don’t need to open port 80 in outbound traffic to send response back to the customer.

**What is the difference between Azure Firewall and NSG ?**

Firewall: Designed for controlling both outbound and inbound traffic to and from resources within a Virtual Network (VNet).

NSG: Typically associated with subnets or individual network interfaces to control traffic within a VNet and between VNets.

**What are the advantages of resource groups in azure ?**

* Logical Organization
* Lifecycle Management
* Resource Group Tagging
* Role-Based Access Control (RBAC)
* Cost Management
* Resource Group Templates (Azure Resource Manager Templates)
* Resource Locks

**What is the difference between Azure User Data and Custom Data ?**

User data is a new version of custom data and it offers added benefits. User data persists and lives in the cloud, accessible and updatable anytime. Custom data vanishes after first boot, accessible only during VM creation.

**What is the difference between Azure App Gateway and Azure LB ?**

**Azure Application Gateway:**

Operates at Layer 7 (Application layer) of the OSI model. Provides advanced application-level routing, SSL termination, and web application firewall (WAF) capabilities. Suited for distributing traffic based on application awareness.

**Azure Load Balancer:**

Operates at Layer 4 (Transport layer) of the OSI model. Distributes network traffic based on IP address and port. Suitable for generic TCP/UDP load balancing without application-specific features.

**Assume your company is using all the ideal Azure Networking setup and your application is deployed in the web subnet , Explain the traffic flow to your app ?**

**User Access:**

* External users access the application over the internet.
* DNS resolves the application's domain name to the associated public IP address.

**Internet Traffic to Azure:**

-Incoming internet traffic reaches Azure through Azure Front Door, Azure Application Gateway, or Azure Load Balancer, depending on the specific requirements of the application.

* These services provide load balancing, SSL termination, and other application-level features.

**Traffic Routing Within Azure:**

* Traffic is directed to the public IP address associated with the Azure Application Gateway or Load Balancer.
* The gateway or load balancer routes traffic to the backend pool of the web servers in the web subnet.

**Network Security Group (NSG) Enforcement:**

* Network Security Groups associated with the web subnet control inbound and outbound traffic.
* NSG rules ensure that only required traffic is allowed, providing security at the network layer.
* Azure Virtual Network (VNet) Components:
* The web subnet is part of an Azure Virtual Network, which acts as an isolated network environment.
* Subnets within the VNet communicate with each other through the VNet's internal routing.

**Application Servers:**

* Web servers within the web subnet process incoming requests

**Describe the purpose of Azure Bastion and when it is used for secure remote access to virtual machines.**

* Secure Remote Access:
* Elimination of Public Internet Exposure:
* Reduced Attack Surface:
* Azure Bastion Integration:
* Simplified Connectivity:
* Azure Portal-Based Access:
* Role-Based Access Control (RBAC):
* Multi-Factor Authentication (MFA):
* Audit and Monitoring: