**Network Security Group (NSG) in Azure**

A **Network Security Group (NSG)** is an Azure resource used to control inbound and outbound network traffic to and from Azure resources. It acts as a virtual firewall, allowing or denying network traffic based on security rules.

**Key Features of NSG**

* **Traffic Filtering**: Allows or denies traffic based on source/destination IP, port, and protocol.
* **Inbound & Outbound Rules**: Defines rules to manage incoming and outgoing traffic.
* **Security Rule Prioritization**: Lower rule numbers take precedence over higher ones.
* **Association with Subnets & Network Interfaces**: Can be applied at different levels:
  + **Subnet Level**: Affects all VMs in the subnet.
  + **Network Interface Level**: Affects only the specific VM's network interface.

**Default Security Rules in NSG**

| **Priority** | **Name** | **Source** | **Destination** | **Port** | **Protocol** | **Action** |
| --- | --- | --- | --- | --- | --- | --- |
| 65000 | AllowVnetInbound | VirtualNetwork | VirtualNetwork | Any | Any | Allow |
| 65001 | AllowAzureLoadBalancer | AzureLoadBalancer | Any | Any | Any | Allow |
| 65500 | DenyAllInbound | Any | Any | Any | Any | Deny |
| 65000 | AllowVnetOutbound | VirtualNetwork | VirtualNetwork | Any | Any | Allow |
| 65500 | DenyAllOutbound | Any | Any | Any | Any | Deny |

**Best Practices for Using NSG**

* Apply NSGs at both the subnet and NIC levels for layered security.
* Use security groups with well-defined rules to restrict traffic.
* Log NSG flow logs in Azure Monitor for auditing and troubleshooting.
* Avoid overly permissive rules (e.g., allowing all traffic on all ports).
* Regularly review and update rules to align with security policies.