**Inbound and Outbound Rules in Azure**

Inbound and outbound rules control network traffic to and from resources in Azure, primarily using **Network Security Groups (NSGs)** and firewall rules. These rules help define what type of traffic is allowed or denied.

**1. Inbound Rules**

➡ Controls traffic coming **into** an Azure resource (e.g., Virtual Machine (VM), load balancer, etc.).

* Determines what traffic is **allowed or denied** from external or internal sources.
* Used to **secure resources** by limiting access only to necessary ports and IP addresses.

**Example of Inbound Rule:**

* **Allow SSH (Port 22)** from a specific IP to a VM.
* **Allow HTTP (Port 80)** to a web server from the internet.
* **Deny all other inbound traffic** for security.

🔹 **Example Rule in NSG:**

| **Priority** | **Source** | **Source Port** | **Destination** | **Destination Port** | **Protocol** | **Action** |
| --- | --- | --- | --- | --- | --- | --- |
| 100 | Any | Any | VM | 22 (SSH) | TCP | Allow |
| 200 | Any | Any | VM | Any | Any | Deny |

**2. Outbound Rules**

➡ Controls traffic going **out** from an Azure resource to other networks or the internet.

* Determines what traffic a resource can **send** to external destinations.
* Helps to **prevent unauthorized access** or **limit internet exposure**.

**Example of Outbound Rule:**

* **Allow traffic to the internet** from an application server.
* **Block database server** from accessing the internet.
* **Allow only specific external APIs** for outbound traffic.

🔹 **Example Rule in NSG:**

| **Priority** | **Source** | **Source Port** | **Destination** | **Destination Port** | **Protocol** | **Action** |
| --- | --- | --- | --- | --- | --- | --- |
| 100 | VM | Any | Internet | 443 (HTTPS) | TCP | Allow |
| 200 | VM | Any | Any | Any | Any | Deny |

**Key Differences:**

| **Feature** | **Inbound Rule** | **Outbound Rule** |
| --- | --- | --- |
| **Controls** | Traffic **coming into** a resource | Traffic **going out** from a resource |
| **Example Usage** | Allow SSH (Port 22) access | Allow HTTPS (Port 443) for outbound connections |
| **Security Concern** | Protects resources from unauthorized access | Prevents data exfiltration and unnecessary external access |

Would you like help setting up specific NSG rules for your Azure environment? 🚀