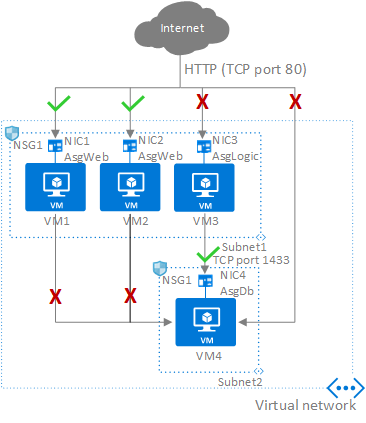
**Network Security Groups**



**Network Security Groups (NSGs)** in Azure are used to **control inbound and outbound traffic** to Azure resources by applying **security rules** based on source, destination, port, and protocol.



**Inbound** **Traffic : D**ata coming **into** an Azure resource from external sources.

**Outbound** **Traffic : D**ata going **out from** an Azure resource to other destinations.

Network Security Groups (NSGs) are based on **inbound and outbound rules** that control traffic flow to and from Azure resources by specifying source, destination, port, and protocol.

**Network Security Group (NSG) rules** are defined separately for **inbound** and **outbound traffic**, controlling what is **allowed or denied** based on direction, source, destination, port, and protocol.

**Common Ports Used in** **NSG :**

|  |  |  |
| --- | --- | --- |
| **Port** | **Protocol** | **Purpose** |
| 22 | TCP | SSH (for Linux VM remote access) |
| 3389 | TCP | RDP (for Windows VM remote access) |
| 80 | TCP | HTTP (web traffic) |
| 443 | TCP | HTTPS (secure web traffic) |
| 1433 | TCP | SQL Server default port |
| 53 | TCP/UDP | DNS (domain name resolution) |
| 25 | TCP | SMTP (email sending – usually blocked) |
| 110/995 | TCP | POP3/POP3S (email retrieval – legacy) |
| 587 | TCP | SMTP with STARTTLS (email) |