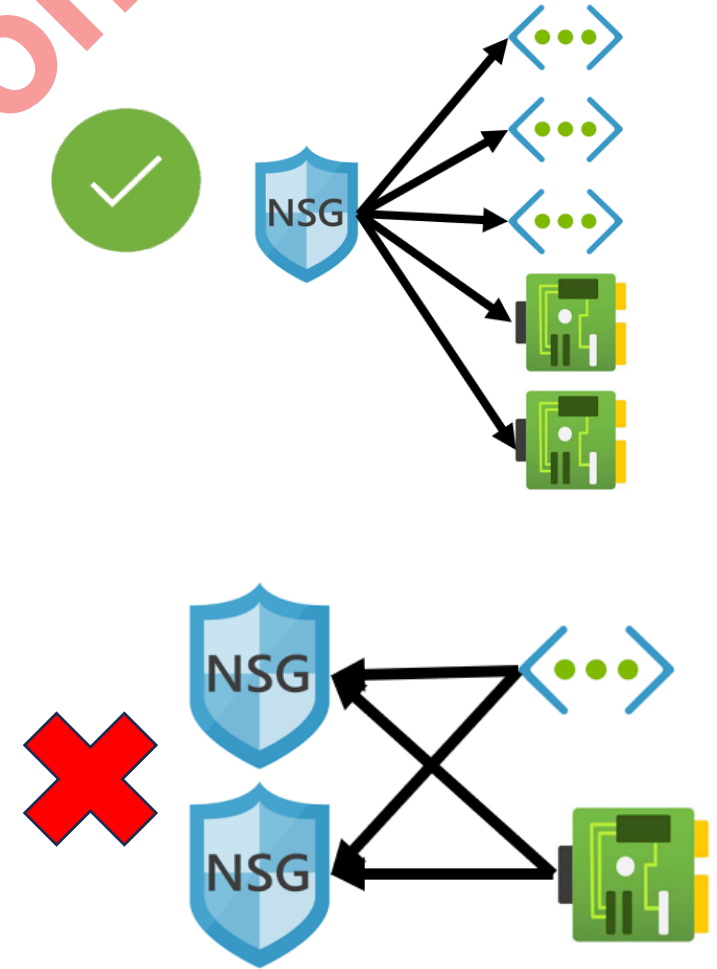


Azure Network Security Groups & Keys Point About it

Azure Network Security Groups

- ✓ Fundamental component of network security in Microsoft Azure to **control inbound and outbound traffic** to and from Azure resources
- ✓ Operate based on **security rules** that define the allowed or denied
- ✓ Can be applied to NIC or Subnet
- ✓ Standard Azure subscription - **up to 5,000 NSGs**. Each NSG - maximum of 1,000 rules
- ✓ One Subnet or NIC can have only One NSG attached but One NSG can be attached to multiple NIC or Subnets ✓



Azure Network Security Groups & Keys Point About it

Azure Network Security Groups

- ✓ If required, you can also **nest NSGs** for a particular resource
- ✓ Each NSG – some **default rules** that allow outbound traffic and deny inbound traffic
- ✓ New NSG rule creation need some **inputs** like source, destination etc.
- ✓ Rules have associated priority; **Lower numbers indicate higher priority.**
- ✓ Can be configured to **log network traffic** using Azure Network Watcher
- ✓ NSGs can be **integrated with Azure Firewall** for additional layer of security
- ✓ For access control, NSGs use Azure's **RBAC** ✓

