**Question 2: What is the primary function of a Network Security Group (NSG) in Azure, and how does it contribute to the security of Virtual Machines (VMs)? Explain with suitable example?**

**Answer:**

The primary function of the NSG is too act as a virtual firewall that control the inbound and outbound network traffic to Azure resources such as virtual machine, subnets and network interfaces. NSG does all this work by defining security rules that either allow or deny traffic based on several criteria such as source and destination IP addresses, port numbers and protocols.

Some key features of NSG are:

1. Traffic filtering
2. Security Control
3. Inbound and Outbound rules
4. Layered security
5. Default security

Network security groups significantly enhance the security of virtual machines by controlling the traffic flow.

**Traffic Filtering:**

NSGs filter both inbound and outbound traffic to and from Azure resources. NSGs allow administrators to define rules that specify which types of incoming traffic are permitted or denied. For example, you can allow HTTP (port 80) and HTTPS (port 443) traffic while blocking all other ports. This ensures that only legitimate and expected traffic reaches your VM, reducing the risk of attacks such as brute force attempts or unauthorized access.

**Security Control:**

NSGs provide fine-grained control over network traffic. Rules can be created based on specific criteria such as:

* Source and Destination IP Addresses
* Source and Destination Ports
* Protocol Type

**Default Security Rules:**

By default, NSGs deny all inbound traffic and allow all outbound traffic. Administrators can modify these default settings to tighten security further.

**Example:**

Consider you have a web application hosted on an Azure VM, and this web application needs to communicate with a database server hosted on another VM. You want to ensure that:

* The web application VM only accepts HTTP (port 80) and HTTPS (port 443) traffic from the internet.
* The web application VM can only communicate with the database server VM on the SQL port (port 1433).
* The database server VM does not accept any inbound traffic except from the web application VM.

Here are the steps for the implementation of NSG:

**Step 1: Create the Network Security Groups (NSGs):**

Web Server NSG: Let's call this ‘WebAppNSG’.

Database Server NSG: Let's call this ‘DbServerNSG’.

**Step 2: Define Inbound and Outbound Rules for Each NSG**

**WebAppNSG**

**Inbound Rules:**

Rule 1: Allow HTTP traffic from the internet

Priority: 100

Source: Any

Source Port Range: \*

Destination: Any

Destination Port Range: 80

Protocol: TCP

Action: Allow

Rule 2: Allow HTTPS traffic from the internet.

Priority: 200

Source: Any

Source Port Range: \*

Destination: Any

Destination Port Range: 443

Protocol: TCP

Action: Allow

Rule 3: Allow SQL traffic from the web server to the database server.

Priority: 300

Source: <WebAppPrivateIP>

Source Port Range: \*

Destination: <DbServerPrivateIP>

Destination Port Range: 1433

Protocol: TCP

Action: Allow

Rule 4: Deny all other inbound traffic.

Priority: 400

Source: Any

Source Port Range: \*

Destination: Any

Destination Port Range: \*

Protocol: Any

Action: Deny

**Outbound Rules:**

Rule 1: Allow outbound traffic to the database server on port 1433.

Priority: 100

Source: Any

Source Port Range: \*

Destination: <DbServerPrivateIP>

Destination Port Range: 1433

Protocol: TCP

Action: Allow

Rule 2: Deny all other outbound traffic.

Priority: 200

Source: Any

Source Port Range: \*

Destination: Any

Destination Port Range: \*

Protocol: Any

Action: Deny

**DbServerNSG**

**Inbound Rules:**

Rule 1: Allow SQL traffic from the web server.

Priority: 100

Source: <WebAppPrivateIP>

Source Port Range: \*

Destination: <DbServerPrivateIP>

Destination Port Range: 1433

Protocol: TCP

Action: Allow

Rule 2: Deny all other inbound traffic.

Priority: 200

Source: Any

Source Port Range: \*

Destination: Any

Destination Port Range: \*

Protocol: Any

Action: Deny

**Outbound Rules:**

Rule 1: Deny all outbound traffic.

Priority: 100

Source: Any

Source Port Range: \*

Destination: Any

Destination Port Range: \*

Protocol: Any

Action: Deny

**Step 3: Associate the NSGs with the VMs**

WebAppNSG: Associate this NSG with the network interface (NIC) of the web server VM.

DbServerNSG: Associate this NSG with the network interface (NIC) of the database server VM.

**Contribution of these NSG to Security**

* The web server VM (WebAppNSG) only allows HTTP and HTTPS traffic from the internet, reducing the attack surface.
* The database server VM (DbServerNSG) only allows SQL traffic from the web server VM, preventing unauthorized access from other sources.
* The web server VM can only send traffic to the database server on port 1433, preventing it from communicating with unauthorized external services.
* The database server VM is restricted from initiating outbound traffic, reducing the risk of data exfiltration if the VM is compromised.
* By using separate NSGs for the web server and database server, you can isolate traffic flows and enforce different security policies for different parts of your application.