NETWORKING

1. Azure Network Security Group (NSG):

An NSG is a fundamental component of Azure's network security strategy. It acts as a virtual firewall that filters network traffic to and from Azure resources within an VNet. Think of it as a set of Access Control List (ACL) rules that define which network packets are allowed or denied.

- Purpose: To control inbound (incoming) and outbound (outgoing) network traffic to maintain a secure and isolated environment for your Azure resources, particularly Virtual Machines (VMs).
    - Inbound Traffic: Rules on the subnet's NSG are processed first. If traffic is allowed by the subnet NSG, then rules on the NIC's NSG are processed. For traffic to reach the VM, it must be allowed by both NSGs.
    - Outbound Traffic: Rules on the NIC's NSG are processed first. If traffic is allowed by the NIC NSG, then rules on the subnet's NSG are processed. For traffic to leave the VM, it must be allowed by both NSGs.
    - Best Practice: While you can associate NSGs at both levels, for simplicity and to avoid complex troubleshooting, it's often recommended to apply NSGs predominantly at the subnet level unless you have a specific need for per-VM rules.

How Network Security Groups (NSGs) Work:

A NSG inspects incoming (inbound) and outgoing (outbound) network traffic at the Layer 3 (IP address) and Layer 4 (Port and Protocol) of the OSI model. Its primary job is to enforce security rules to determine which traffic flows are allowed and which are blocked.

- Direction: Whether it applies to Inbound or Outbound traffic.
- Priority: A number (100-4096) that dictates the order of evaluation.
- Source/Destination: The origin or target of the traffic.
- Port Range: The communication port(s) involved (e.g., 80, 443, 3389).
- Protocol: The network protocol (e.g., TCP, UDP, ICMP, Any).
- Action: Whether to Allow or Deny the traffic.
- Traffic Flow and Rule Evaluation:
    a. When a network packet arrives at or attempts to leave an Azure resource, it encounters any associated NSG(s).
    b. The NSG evaluates the packet against its security rules.
    c. As soon as a rule's criteria (Direction, Source, Source Port, Destination, Destination Port, Protocol) match the packet's information, the Action (Allow or Deny) specified in that rule is immediately applied.
    d. No further rules are processed for that specific packet once a match is found. This makes rule priority critical.
- Stateful Filtering: NSGs are stateful firewalls. This means that if you establish an outbound connection (e.g., a VM connects to a website on the internet), the NSG automatically allows the return inbound traffic for that established connection without needing a separate inbound rule.
- Association Points: NSGs can be associated at two levels:
    - Subnet Level: All resources within that subnet inherit the NSG's rules.
    - NIC Level: Rules apply only to that specific VM's network interface.
    - Combined Evaluation: If an NSG is on both the subnet and the NIC:
        - Inbound: Subnet NSG rules are evaluated first, then NIC NSG rules.
        - Outbound: NIC NSG rules are evaluated first, then Subnet NSG rules.

2. Azure Application Security Groups (ASG):

Application Security Groups (ASGs) allow you to configure network security as a natural extension of an application's structure. Instead of specifying explicit IP addresses in NSG rules, you can group VMs by application workload (e.g., "WebServers," "DatabaseServers") and then define NSG rules using these ASGs.

- Simplifies Rule Management: ASGs drastically reduce the number of NSG rules needed, especially in large and dynamic environments where VM IP addresses might change.
- Enhanced Granularity: You can apply security policies at a finer grain, focusing on application tiers rather than just subnets or individual IPs.
- Scalability: When new VMs are added to an application tier, you simply add them to the corresponding ASG, and the NSG rules automatically apply. No need to update NSG rules manually.
- Relationship with NSG: ASGs are used within NSG rules as sources or destinations. An ASG itself does not filter traffic; it provides a logical grouping that NSGs use.

How Application Security Groups (ASG) Work:

Application Security Groups do not filter traffic themselves. Instead, they act as logical groupings of Virtual Machines (VMs) or more specifically, their Network Interfaces (NICs). Their primary purpose is to simplify and streamline the creation and management of Network Security Group (NSG) rules.

- Logical Grouping: Instead of defining NSG rules by individual IP addresses, ASGs allow you to group VMs based on their application workload, role, or function. For example, you can create ASGs like WebServers, AppServers, or DatabaseServers.

- Referenced by NSG Rules: ASGs become Source or Destination objects within NSG security rules. When you define an NSG rule, you can specify an ASG instead of an IP address range.
- Dynamic IP Resolution: The Azure platform automatically handles the underlying IP addresses for the VMs within an ASG. When a VM is added to or removed from an ASG, or its IP address changes, the NSG rules referencing that ASG are dynamically updated in the background without requiring any manual modification to the NSG rules themselves. This is a key benefit for scalability and reducing management overhead.
- Application-Centric Security: ASGs enable an application-centric approach to network security. Instead of thinking about "allow IP A to talk to IP B," you can think in terms of "allow WebServers to talk to AppServers on port 8080." This makes security policies much more intuitive and aligned with your application's architecture.
- Micro-segmentation: ASGs facilitate micro-segmentation within your virtual networks. You can run multiple application tiers within the same subnet, yet still apply distinct NSG rules that govern traffic between those application tiers, leveraging ASGs as sources and destinations.
- The interaction between NSGs and ASGs is crucial:
- NSGs enforce the traffic rules.
- ASGs define the "objects" (groups of VMs) that those rules apply to.
- By combining NSGs with ASGs, you can achieve more scalable, flexible, and easily manageable network security policies, especially in complex or dynamic environments with many VMs and application tiers.

Allowing Specific IPs to Access VMs and Denying General Internet Access Using NSG:

Allowing only authorized systems (identified by their IP addresses) to connect to your VMs while simultaneously preventing those VMs from initiating connections to the broader public internet.

The core principle involves leveraging NSG security rules and their priority order to create specific "allow" exceptions within a general "deny" policy.

1. How Inbound Access is Controlled (Allow Specific IPs, Deny Internet)

By default, every NSG includes a high-priority rule that allows all traffic from within the Virtual Network (AllowVnetInBound, priority 65000) and a very low-priority rule that denies all other inbound traffic (DenyAllInbound, priority 65500). This DenyAllInbound rule is crucial as it acts as the default internet denial.

To allow specific external IPs to access a VM, the working involves:

Creating "Allow" Rules for Authorized IPs:

- **Mechanism:** You create new Inbound security rules within the NSG. These rules specify the Source as the trusted specific IP address(es) or CIDR block(s). You then define the Destination as Any (or the specific private IP of the VM), the required Destination Port Ranges (e.g., 3389 for RDP, 80,443 for web traffic), and the relevant Protocol (e.g., TCP).
- **Priority:** Crucially, these "Allow" rules are assigned a lower priority number (e.g., 100, 110, 120) than the default DenyAllInbound rule (65500). This ensures they are evaluated and matched before the general denial rule.

- Working: When traffic arrives at the VM:
    a. The NSG first checks your custom "Allow" rules (e.g., priority 100, 110).
    b. If the traffic's source IP, destination port, and protocol match one of your "Allow" rules, the traffic is immediately permitted, and no further rules are evaluated.
    c. If the traffic does not match any of your specific "Allow" rules (e.g., it's from an unauthorized internet IP, or on a blocked port), it will eventually fall through to the default DenyAllInbound rule, which will block it.
- Default Denial of Internet: The built-in DenyAllInbound rule (priority 65500, Source Any, Destination Any, Protocol Any, Action Deny) effectively denies all inbound traffic that is not explicitly allowed by a higher-priority custom rule. This means any traffic originating from the general internet that isn't from your specified allowed IPs will be blocked by default without needing an additional "Deny Internet" rule.

2. How Outbound Access is Controlled (Deny Internet):

By default, an NSG includes an AllowInternetOutBound rule (priority 65001) that permits all outbound traffic to the public internet, and a DenyAllOutbound rule (priority 65500) that denies everything else. To prevent VMs from accessing the internet while still allowing other necessary outbound connections (e.g., to other VMs within the VNet or to specific Azure services), the working involves:

Overriding the Default "Allow" with a Specific "Deny":

- Mechanism: You create a new Outbound security rule with the Destination set to the Internet Service Tag, Destination Port Ranges as * (or specific ports if you want to deny only certain internet traffic types), Protocol as Any, and Action as Deny.

- Priority: This "Deny Internet" rule must be assigned a lower priority number (e.g., 400) than the default AllowInternetOutBound rule (65001). This ensures your explicit denial takes precedence.
- When a VM attempts to initiate an outbound connection the NSG evaluates its outbound rules.
- If the traffic is destined for the public internet, it will match your custom "Deny Internet" rule. The traffic is then blocked, and no further rules are evaluated.
- If the traffic is not destined for the public internet (e.g., it's to another VM in the VNet), those specific "Allow" rules will be processed and can permit traffic before the general "Deny Internet" rule is hit. This allows for selective outbound access.

Types of Public IP Allocation Methods :

Azure offers two primary allocation methods for Public IP addresses:

Dynamic Public IP:

- Working: The IP address is not assigned to the resource at the time of creation. Azure assigns an IP address from a pool of available IPs when the resource is started or associated with the public IP.
- Behavior: This IP address can change over time. If the associated resource (like a VM) is stopped (deallocated) and then started again, it might receive a different public IP address. The IP address is released back into the pool when the resource is stopped or deleted.
- Use Cases: Suitable for development/test environments, non-critical VMs, or scenarios where the public IP address is not required to be constant.
- Cost: Generally more cost-effective as the IP is only held when the resource is running.

CONCLUSION

- Network Security Groups (NSGs): Function as stateful firewalls, controlling VM traffic (inbound/outbound) via priority-based rules.
- Application Security Groups (ASGs): Simplify NSG management by allowing logical grouping of VMs based on application roles, facilitating scalable and intuitive security policies.
- Public IP Addresses:
  - Types: Dynamic and Static allocation methods.
  - SKUs: Basic and Standard SKUs.
- Service Tags: Provided as an abstraction for Azure service IP ranges, simplifying NSG rule creation and maintenance by automatically updating IP lists.
- Networking Component Management:
  - Covered the creation of Public IP addresses and Network Interfaces (NICs).
  - Explained the processes of associating and de-associating Public IPs with VM Network Interfaces.

Submitted by:
Sambit Kumar Panda

References:

https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview
https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups
https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses
https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/associate-public-ip-address-vm?tabs=azure-portal
https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview
https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/virtual-network-network-interface-addresses?tabs=nic-address-portal