Azure Network Security Groups (NSGs)

Overview
Azure Network Security Groups (NSGs) are used to filter network traffic to and from Azure resources in an Azure virtual network. NSGs contain security rules that allow or deny inbound network traffic to, or outbound network traffic from, various Azure resources. Each rule within an NSG specifies details such as source and destination, port, and protocol.

Security Rules
NSGs can have multiple security rules, each with specific properties:

- **Name:** Unique within the NSG, up to 80 characters long, starting with a word character, ending with a word character or '_', and may include '.', '-', '_'.
- **Priority:** A value between 100 and 4096, with lower numbers having higher priority. Rules are processed in priority order.
- **Source or Destination:** Can be Any, an individual IP address, CIDR block, service tag, or application security group.
- **Protocol:** Options include TCP, UDP, ICMP, ESP, AH, or Any. ESP and AH are not available via the Azure portal but can be used via ARM templates.
- **Direction:** Specifies whether the rule applies to inbound or outbound traffic.
- **Port Range:** Can specify an individual or range of ports, enabling fewer rules. Augmented security rules can specify multiple ports or ranges in Resource Manager deployment models.
- **Action:** Either Allow or Deny.

Security rules are processed based on the five-tuple (source, source port, destination, destination port, and protocol) information. Existing connections may not be interrupted when rules are modified, as changes only affect new connections.

Default Security Rules
Azure NSGs come with default rules which can’t be removed but can be overridden by higher-priority rules:

Inbound:
- **AllowVNetInBound**: Allows traffic within the Virtual Network.
- **AllowAzureLoadBalancerInBound**: Allows traffic from Azure Load Balancer.
- **DenyAllInbound**: Denies all other inbound traffic.

Outbound:
- **AllowVnetOutBound**: Allows traffic within the Virtual Network.
- **AllowInternetOutBound**: Allows outbound traffic to the internet.
- **DenyAllOutBound**: Denies all other outbound traffic.

Augmented Security Rules
Augmented security rules simplify network security configurations by allowing multiple ports and IP addresses in a single rule. These can be combined with service tags or application security groups for easier management. There are limits to the number of addresses, ranges, and ports

specified in a rule.

Service Tags and Application Security Groups
- **Service Tags:** Represent groups of IP address prefixes for Azure services, reducing the complexity of frequent updates to security rules.
- **Application Security Groups:** Allow you to configure network security based on an application's structure, making it easier to scale security policies without manual IP address maintenance.

Azure Platform Considerations
- **Virtual IP of the Host Node:** Basic infrastructure services like DHCP, DNS, and health monitoring use specific IP addresses (168.63.129.16 and 169.254.169.254). These are not subject to NSGs unless targeted by specific service tags.
- **Licensing (Key Management Service):** Requests for Windows licensing are made outbound through port 1688.
- **Load-Balanced Pools:** Source port and address range are from the originating computer, not the load balancer.
- **Azure Service Instances:** Various Azure services require specific port access. Denying these ports may affect service functionality.
- **Sending Outbound Email:** Microsoft recommends using authenticated SMTP relay services for sending emails from Azure VMs. Outbound port 25 communication is restricted based on the subscription type.

Next Steps
- **Virtual Network Integration:** Learn about which Azure resources can be integrated with NSGs.
- **Traffic Evaluation:** Understand how network security groups evaluate traffic.
- **Tutorials and Management:** Complete tutorials on creating and managing NSGs.
- **Troubleshooting:** Diagnose and troubleshoot communication problems related to NSGs.
- **Flow Logs:** Enable NSG flow logs for analyzing network traffic to and from resources with associated NSGs.

For detailed information, refer to the specific Azure documentation on network security groups and related topics.