Network Security Groups

Introduction

Network security is a critical aspect of managing cloud environments. One of the essential tools in Azure for managing network security is the Network Security Group (NSG). An NSG can filter network traffic to and from Azure resources within a virtual network. This paper explores the properties of NSG rules, default security rules, augmented security rules, service tags, application security groups, Azure platform considerations, and best practices for configuring NSGs.

Security Rules

Properties of a Security Rule

A network security group rule specifies the following properties:
- Name: A unique identifier for the rule, up to 80 characters long.
- Priority: A number between 100 and 4096 that determines the order in which rules are processed.
- Source or Destination: Can be an IP address, CIDR block, service tag, or application security group.
- Protocol: The network protocol (TCP, UDP, ICMP, ESP, AH, or Any).
- Direction: Whether the rule applies to inbound or outbound traffic.
- Port Range: Specifies the ports affected by the rule.
- Action: Determines whether traffic is allowed or denied.

Default Security Rules

Azure provides default security rules in each NSG to ensure basic network security:

Inbound Rules

1. AllowVNetInBound: Allows traffic within the virtual network.
2. AllowAzureLoadBalancerInBound: Allows traffic from the Azure load balancer.
3. DenyAllInbound: Denies all other inbound traffic.

Outbound Rules

1. AllowVNetOutBound: Allows traffic within the virtual network.
2. AllowInternetOutBound: Allows outbound traffic to the internet.
3. DenyAllOutBound: Denies all other outbound traffic.

Augmented Security Rules

Augmented security rules simplify security configurations by allowing multiple ports and IP addresses in a single rule. This feature reduces the number of rules needed and simplifies network security management.

Service Tags and Application Security Groups

Service Tags

Service tags represent a group of IP address prefixes from specific Azure services, simplifying the management of security rules.

Application Security Groups

Application security groups allow you to group VMs and define network security policies based on these groups. This approach enables scalable and manageable security configurations.

Azure Platform Considerations

Virtual IP of the Host Node

Azure uses virtual IP addresses (168.63.129.16 and 169.254.169.254) for basic infrastructure services. These IPs are generally exempt from NSG rules unless explicitly denied.

Licensing (Key Management Service)

Windows VMs require access to Key Management Service (KMS) host servers for licensing, typically over port 1688.

Virtual Machines in Load-Balanced Pools

NSG rules should account for the source port and address from the originating computer, not the load balancer.

Azure Service Instances

Ensure that NSG rules do not block necessary ports for Azure services like HDInsight, Application Service Environments, and Virtual Machine Scale Sets.

Sending Outbound Email

Azure's policy on outbound email traffic over port 25 varies based on the subscription type. It's recommended to use authenticated SMTP relay services.

Next Steps

- Familiarize with Azure resources deployable into virtual networks and associable with NSGs.
- Understand the evaluation process of network traffic with NSGs.
- Use tutorials and management guides for hands-on experience with NSGs.
- Troubleshoot communication issues using Azure diagnostic tools.
- Enable NSG flow logs for traffic analysis.