Azure Management Tools, Securing Network Connectivity in Azure

Azure Portal - A web-based management interface that allows users to create, configure, monitor, and manage Azure resources through a graphical user interface.

Azure PowerShell - A set of cmdlets (command-line tools) that enable automation and scripting for managing Azure resources directly from the PowerShell environment.

Accessing Cloud Shell - A browser-based command-line interface available in the Azure Portal that provides access to Azure PowerShell or Azure CLI without needing local installation.

Azure Advisor - A personalized cloud consultant that provides best practice recommendations to optimize performance, security, reliability, and cost of your Azure resources.

Securing Network Connectivity in Azure

Network Security Groups (NSG) - Used to filter network traffic to and from Azure resources within a virtual network. NSGs contain security rules that allow or deny inbound and outbound traffic based on IP address, port, and protocol.

Application Security Groups (ASG) - Logical groupings of virtual machines that simplify management of network security rules by allowing you to apply rules based on application workload instead of individual IP addresses.

User Defined Routes (UDR) - Custom routing tables that let you control traffic flow within a virtual network by overriding Azure's default system routes.

Azure Firewall - A managed, cloud-based network security service that uses stateful inspection and threat intelligence to filter inbound, outbound, and internal (east-west) traffic.

- Network address translation (NAT) rules - Rules that translate private IP addresses to public IPs (and vice versa), enabling controlled inbound and outbound connectivity.
- Network Rules - Filter traffic based on protocols, ports, and source/destination IP addresses for non-web traffic such as SSH, RDP, and database connections.
- Application rules - Filter outbound HTTP/S traffic based on fully qualified domain names (FQDNs) to control and restrict web access.

Azure DDoS Protection - A service that protects Azure applications from large-scale, network-layer distributed denial-of-service (DDoS) attacks by absorbing and mitigating malicious traffic before it reaches your resources.

- Basic - Enabled by default at no cost and provides always-on traffic monitoring and automatic mitigation for common network-level DDoS attacks on all Azure public IPs.
- Standard - An advanced, paid offering that provides enhanced mitigation capabilities, adaptive tuning, attack analytics, cost protection, and SLA-backed protection for mission-critical applications.

Security Tools and Features of Azure

Azure Security Center - A unified infrastructure security management system that provides advanced threat protection across hybrid cloud workloads. It continuously assesses resource configurations, provides security recommendations, and detects threats using built-in analytics and threat intelligence.

- Free tier - Provides continuous security assessment, security recommendations, and basic posture management at no cost. It focuses on identifying misconfigurations and improving overall security hygiene.
- Standard tier - A paid upgrade that includes all Free tier features plus advanced threat protection, just-in-time VM access, adaptive application controls, and enhanced detection capabilities across Azure, hybrid, and on-prem environments.

Security Center Coverage - Refers to the breadth of security capabilities the service offers, including posture management, policy enforcement, threat detection, and workload protection across your Azure and hybrid environment.

- Policy and Compliance - Defines and applies security policies across your Azure environment to ensure resources meet organizational or regulatory requirements. Security Center continuously evaluates resources against these policies and reports compliance status.
- Resource Security Hygiene - Continuous monitoring of resource configurations to identify vulnerabilities, misconfigurations, insecure settings, and high-risk areas. It provides actionable recommendations to improve overall security posture.
- Threat protection - Advanced, real-time detection of attacks using Microsoft threat intelligence, machine learning, and behavioral analytics. It alerts on suspicious activities and provides recommendations for remediation.

Azure Key Vault - A cloud service that securely stores and manages cryptographic keys, secrets, certificates, and sensitive information for applications and users. It provides centralized key management, access control, and monitoring capabilities.

Azure Information Protection (AIP) - A cloud-based solution that helps organizations classify, label, and protect documents and emails by applying encryption and access policies based on content sensitivity, ensuring secure collaboration and compliance.

Azure Advanced Threat Protection (ATP) - A cloud-based security solution that detects, investigates, and responds to advanced threats, compromised identities, and malicious insider actions by analyzing user and entity behavior, integrating with Active Directory and other identity services to provide actionable threat intelligence.

Azure Governance Methodologies

Azure Policy - A service that allows you to define, assign, and enforce policies to ensure resources comply with organizational or regulatory standards.

GPOs (Group Policy Objects) - Used to manage and configure operating system, application, and user settings in Active Directory environments, including Azure Active Directory-joined devices.

Role-Based Access Control (RBAC) - Provides fine-grained access management for Azure resources by assigning users or groups to roles with specific permissions.

Locks - Mechanisms to prevent accidental deletion or modification of critical Azure resources, ensuring stability and compliance.

Azure Advisor Security Assistance - Security-related recommendations provided by Azure Advisor to optimize configurations, improve security, and reduce risks across resources.

Azure Blueprints - A service that enables deployment of repeatable environments with predefined resources, policies, and role assignments to ensure compliance and governance standards.