**Azure fundamental assignment 5**

1. What is the Azure firewall? How to use the Azure firewall?

Azure Firewall is a cloud-native and intelligent network firewall security service that provides the best of breed threat protection for your cloud workloads running in Azure. It's a fully stateful, firewall as a service with built-in high availability and unrestricted cloud scalability.

1. Differentiate authentication and authorization?

|  |  |
| --- | --- |
| **uthentication** | **Authorization** |
| Authentication verifies who the user is. | Authorization determines what resources a user can access. |
| Authentication works through passwords, one-time pins, biometric information, and other information provided or entered by the user. | Authorization works through settings that are implemented and maintained by the organization. |
| Authentication is the first step of a good identity and access management process. | Authorization always takes place after authentication. |
| Authentication is visible to and partially changeable by the user. | Authorization isn’t visible to or changeable by the user. |
| Example: By verifying their identity, employees can gain access to an HR application that includes their personal pay information, vacation time, and 401K data. | Example: Once their level of access is authorized, employees and HR managers can access different levels of data based on the permissions set by the organization. |

1. What is Azure Active Directory?

Azure Active Directory (Azure AD) is a cloud-based identity and access management service. This service helps your employees access external resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications. Azure AD also helps them access internal resources. These are resources like apps on your corporate network and intranet, along with any cloud apps developed by your own organization. For more information about creating a tenant for your organization, see Quickstart: Create a new tenant in Azure Active Directory.

1. What are multifactor authentication and conditional access available in Azure?

Multi-factor authentication (MFA) creates an extra step to verify user identity who wants to gain access to your server or database. MFA provides greater security with that layered authentication approach. When hosting MFA on-premises, you can lock down the server or cloud applications that are tied in with Microsoft ADFS (Active Directory Federation Services) in the environment that you have deployed.

Conditional Access brings signals together, to make decisions, and enforce organizational policies. Azure AD Conditional Access is at the heart of the new identity-driven control plane.

MFA Management Console

Go to your Groups and select MFA authentication

You should see a list of your users with an indication if they have already enabled MFA

Enable MFA for your administrators or selected users

By enabling MFA, your users or admins will be prompted to set up their second form of authentication device when they log into the Office.com portal

Configuring Conditional Access

Enable MFA based on IF statements, such as work locations or device

Conditional access allows you to better define and identify those who have a higher sign-in risk

1. What is resource lock? Describe why resource lock should be used?

As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.

Azure Resource Locking helps prevent inadvertent resource deletion and modification.

Azure Role Based Access Control (RBAC) allows us to restrict access to resources and resource actions. RBAC should be used as a first line of defense against unwanted resource access. That said, RBAC alone may not be sufficient in all environments. Take for instance the situation where it is desired for a user or other access identity to have full access to all resources (super user). While these identities may have sufficient access to delete and modify resources, we may want to provide an additional layer of defense to prevent inadvertent access

1. What is Azure policy? Write it Usage.

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management. Policy definitions for these common use cases are already available in your Azure environment as built-ins to help you get started.

1. What is the Azure government? What is Azure China 21Vianet?

US government agencies or their partners interested in cloud services that meet government security and compliance requirements, can be confident that Microsoft Azure Government provides world-class security and compliance. Azure Government delivers a dedicated cloud enabling government agencies and their partners to transform mission-critical workloads to the cloud. Azure Government services can accommodate data that is subject to various US government regulations and requirements.

Microsoft Azure operated by 21Vianet (Azure China) is a physically separated instance of cloud services located in China. It's independently operated and transacted by Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet"), a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd..