**Azure fundamental assignment 5**

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

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics.

Some prerequisites before using Azure firewall are –

* Have an active Azure subscription
* Set up the network
* Create a resource group
* Create a Virtual Network (VNet), Subnets
* Create a VM
* Create Firewall

To deploy the firewall into the VNet follow below steps:

1. On the Azure portal menu or from the Home page, select Create a resource.
2. Type firewall in the search box and press Enter.
3. Select Firewall and then select Create.
4. On the Create a Firewall page, fill the details to configure the firewall
5. Accept the other default values, then select Review + create.
6. *Differentiate authentication and authorization?*

Authentication is the process of verifying who someone is, whereas authorization is the process of verifying what specific applications, files, and data a user has access to.

|  |  |
| --- | --- |
| **Authentication** | **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 99K 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 is Microsoft’s multi-tenant, cloud-based directory, and identity management service. For an organization, Azure AD helps employees sign up to multiple services and access them anywhere over the cloud with a single set of login credentials.

Active Directory (AD) is an OS directory service that facilitates working with interconnected, complex, and different network resources in a unified manner.

Azure Active Directory (Azure AD) 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.

Azure AD is intended for IT admins, App developers, Microsoft 365, Office 365, Azure, or Dynamics CRM Online subscribers.

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

**Multi-factor authentication** is a process in which users are prompted during the sign-in process for an additional form of identification, such as a code on their mobile phone or a fingerprint scan. Azure AD Multi-Factor Authentication works by requiring two or more of the following authentication methods:

* Something you know, typically a password.
* Something you have, such as a trusted device that's not easily duplicated, like a phone or hardware key.
* Something you are - biometrics like a fingerprint or face scan.

Azure AD Multi-Factor Authentication can also further secure password reset. When users register themselves for Azure AD Multi-Factor Authentication, they can also register for self-service password reset in one step. Administrators can choose forms of secondary authentication and configure challenges for MFA based on configuration decisions.

When users sign into an application or service and receive an MFA prompt, they can choose from one of their registered forms of additional verification. The following additional forms of verification can be used with Azure AD Multi-Factor Authentication:

* Microsoft Authenticator app
* Windows Hello for Business
* FIDO2 security key
* OATH hardware token (preview)
* OATH software token
* SMS
* Voice call

The modern security perimeter now extends beyond an organization's network to include user and device identity. Organizations can use identity-driven signals as part of their access control decisions.

**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.

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. Example: A payroll manager wants to access the payroll application and is required to do multi-factor authentication to access it.

Administrators are faced with two primary goals:

* Empower users to be productive wherever and whenever
* Protect the organization's assets

Use Conditional Access policies to apply the right access controls when needed to keep your organization secure.

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

**Resource Locks** provide a way for administrators to lock down Azure resources to prevent deletion or changing of a resource. These locks sit outside of the Role Based Access Controls (RBAC) hierarchy and when applied will place the restriction on the resource for all users. These are very useful when you have an important resource in your subscription which users should not be able to delete or change and can help prevent accidental and malicious changes or deletion.

There are two types of resource locks that can be applied:

1. CanNotDelete – This prevents anyone from deleting a resource whilst the lock is in place, however they may make changes to it.
2. ReadOnly – As the name suggests, it makes the resource read only, so no changes can be made, and it cannot be deleted.

Resource locks can be applied to subscriptions, resource groups or individual resources as required. When you lock Subscription, all resources in that subscription (including ones added later) inherit the same lock. Once applied, these locks impact all users regardless of their roles, if it becomes necessary to delete or change a resource with a lock in place then the lock will need to be removed before this can occur.

By using Resource Locks, we can put in place an extra line of defence against accidental or malicious changing and/or deletion of your most important resources. It’s not perfect, as your administrators can still remove these locks, but doing so requires a conscious effort, as the only purpose for removing a lock is to circumvent it. As these locks sit outside of RBAC you can apply them and be sure that they are impacting all your users, regardless of what roles or custom permissions you may have granted the

1. *What is Azure policy? Write it Usage.*

**Azure Policy** is a service in Azure which allows you create polices which enforce and control the properties of a resource. When these policies are used, they enforce different rules and effects over your resources, so those resources stay compliant with your IT governance standards. 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.

All Azure Policy data and objects are encrypted at rest.

To summarize, Azure policy is basically 3 components: policy definition, assignment, and parameters.

* Policy definition is the conditions which you want controlled. There are built in definitions such as controlling what type of resources can be deployed to enforcing the use of tags on all resources.
* Policy assignment is the scope of what the policy definition can take effect around. Scope of assignment can be assigned to an individual, resource, resource group or management group. Policy assignments are inherited by all child resources.
* Policy parameters are used by reducing the number of policy definitions you must create. Parameters would be used to define which type of VM SKUs to deploy or defining a specific location.

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

Azure Government is the mission-critical cloud, delivering breakthrough innovation to US government customers and their partners. Only US federal, state, local and tribal governments and their partners have access to this dedicated instance, operated by screened US citizens. Azure Government offers the broadest level of certifications of any cloud provider to simplify even the most critical government compliance 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.