**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. It provides both east-west and north-south traffic inspection.

Managed network security service to control traffic in and out of a Azure Virtual Network

Stateful: Once traffic in is allowed, traffic out is automatically allowed

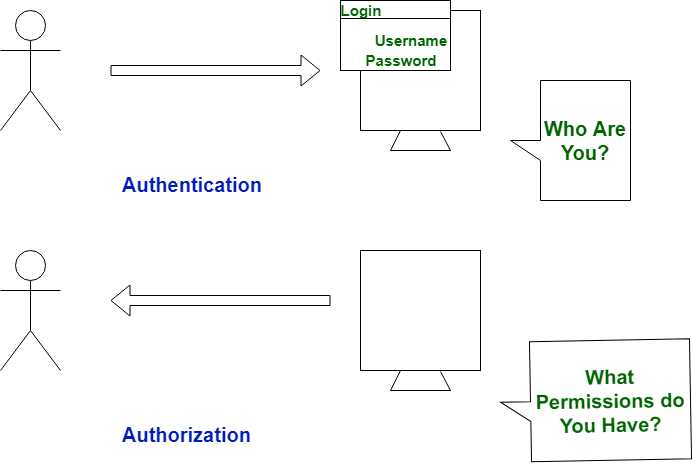
Centralized Configuration: With one Azure firewall, you can control traffic to multiple virtual networks (having hundreds of resources) across multiple subscriptions

Example : If your enterprise has 10 virtual networks (across multiple subscriptions) with 100 VMs, you can control traffic with one Azure Firewall

Integrates with Azure Monitor: Provides logging and analytics (

REMEMBER) Web application firewall (WAF) Restrict traffic into web applications OWASP etc Supported by Azure Application Gateway, Azure Content Delivery Network.

1. **Differentiate authentication and authorization?**



|  | **Authentication** | **Authorization** |
| --- | --- | --- |
| 1. | In authentication process, the identity of users are checked for providing the access to the system. | While in authorization process, person’s or user’s authorities are checked for accessing the resources. |
| 2. | In authentication process, users or persons are verified. | While in this process, users or persons are validated. |
| 3. | It is done before the authorization process. | While this process is done after the authentication process. |
| 4. | It needs usually user’s login details. | While it needs user’s privilege or security levels. |
| 5. | Authentication determines whether the person is user or not. | While it determines **What permission do user have?** |

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.

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 cellphone or a fingerprint scan.

If you only use a password to authenticate a user, it leaves an insecure vector for attack. If the password is weak or has been exposed elsewhere, an attacker could be using it to gain access. When you require a second form of authentication, security is increased because this additional factor isn't something that's easy for an attacker to obtain or duplicate.

**Azure portal** > **Azure Active Directory** > **Security** > **Conditional Access** > **Create new policy from template**.

Azure Active Directory (AD) Conditional Access **provides added security by allowing access to your applications across cloud and on-premises only from trusted and compliant devices**. It is a policy-based approach. You can configure a Conditional Access policy with the required conditions to apply the access controls.

[Security defaults](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults) are great for some but many organizations need more flexibility than they offer. Many organizations need to exclude specific accounts like their emergency access or break-glass administration accounts from Conditional Access policies. The policies referenced in this article can be customized based on organizational needs. Organizations can [use report-only mode for Conditional Access to determine the results of new policy decisions.](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-only)

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

Resource locks are basically just locks that we can associate to different scopes within our Azure cloud infrastructure allowing us to override permissions at that resource scope and down. When we talk about the scope of the resource lock, we can lock subscriptions, we can lock resource groups and individual resources, and the lock restrictions that we have based off of the type of lock we select will apply to all users and roles that have access to that resource. Also, it’s worth noting that locks are inherited by child resources. So, if we apply a lock on a subscription it is inherited by all the resource groups that have been created under that subscription along with the resources that will be created under the resource groups.

## Types of Azure Locks

There are two types of resource locks in Azure.

### ReadOnly locks

This type of lock allows the authorized users that have permissions to the resource to be able to view (read) the resource, but they can't delete or update the resource. So, there can be no modifications or deletions. Because it gives read-only permissions, even if the user has permissions to do other things such as modifying and deleting the resource, they would not be able to do so

### CanNotDelete locks

This type of lock allows the authorized users to read and modify the resource, but they can't delete the resource because it overrides those delete permissions that the authorized users may have been granted based off of a specific role.

## Example - Using Azure Delete Lock

In this example, we would like to point out the fact that applying resource locks are management level operations. In this example, we will create a storage account and apply a cannot delete lock on it. What happens in this case is that we will not be able to delete the storage account itself but we would be allowed to delete any data that resides within the storage account.

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.

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?**

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, with operations controlled by screened US citizens.

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..