Azure Fundamental Assignment 5

(Durgesh Kumar Shukla)

1. What is the Azure firewall? How to use the Azure firewall?
2. Differentiate authentication and authorization?
3. What is Azure Active Directory?
4. What are multifactor authentication and conditional access available in Azure?
5. What is resource lock? Describe why resource lock should be used?
6. What is Azure policy? Write it Usage.
7. What is the Azure government? What is Azure China 21Vianet?

Question 1. What is the Azure firewall? How to use the Azure firewall?
Answer:
Azure Firewall
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.
1.Azure Firewall Standard - Azure Firewall Standard provides L3-L7 filtering and threat intelligence feeds directly from Microsoft Cyber Security. Threat intelligence-based filtering can alert and deny traffic from/to known malicious IP addresses and domains which are updated in real time to protect against new and emerging attacks.
2. Azure Firewall Premium-Azure Firewall Premium provides advanced capabilities include signature-based IDPS to allow rapid detection of attacks by looking for specific patterns. These patterns can include byte sequences in network traffic, or known malicious instruction sequences used by malware

Using Azure Firewall
Use Azure Firewall Manager to centrally manage Azure Firewalls across multiple subscriptions. Firewall Manager leverages firewall policy to apply a common set of network/application rules and configuration to the firewalls in your tenant.
Firewall Manager supports firewalls in both VNet and Virtual WANs (Secure Virtual Hub) environments. Secure Virtual Hubs use the Virtual WAN route automation solution to simplify routing traffic to the firewall with a few clicks.

Deploy the firewall

- Deploy the firewall into the VNet.
- On the Azure portal menu or from the Home page, select Create a resource.
- Type firewall in the search box and press Enter.
- Select Firewall and then select Create.
- On the Create a Firewall page, use the following table to configure the firewall:
  Setting Value

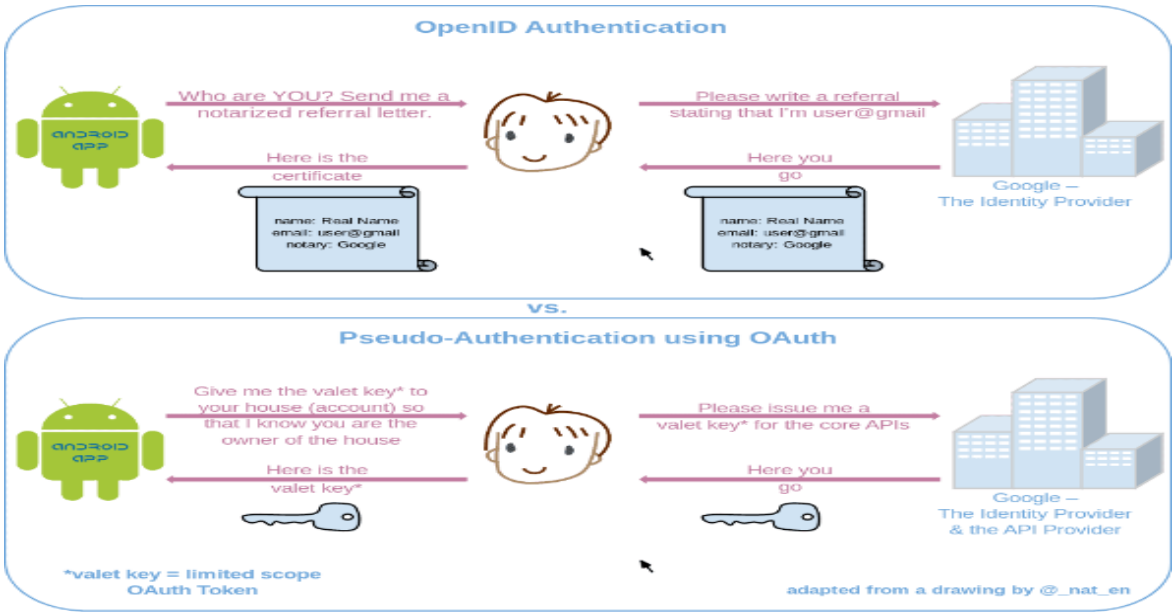
Subscription - <your subscription>
Resource group - Test-FW-RG
Name - Test-FW01
Region- Select the same location that you used previously
Firewall management- Use Firewall rules (classic) to manage this firewall
Choose a virtual network- Use existing: Test-FW-VN

Public IP address- Add new	
Name- fw-pip	

- Accept the other default values, then select Review + create.
- Review the summary, and then select Create to create the firewall.
- This will take a few minutes to deploy.
- After deployment completes, go to the Test-FW-RG resource group, and select the Test-FW01 firewall.
- Note the firewall private and public IP addresses. You'll use these addresses later.

Question 2. Differentiate authentication and authorization?
Answer:
Authentication
Authentication is the process of proving that you are who you say you are. It's sometimes shortened to AuthN. The Microsoft identity platform uses the **OpenID Connect** protocol for handling authentication.
Authorization
Authorization is the act of granting an authenticated party permission to do something. It specifies what data you're allowed to access and what you can do with that data. Authorization is sometimes shortened to AuthZ. The Microsoft identity platform uses the **OAuth** 2.0 protocol for handling authorization.

Difference b/w Authentication and Authorization
OAuth is used for Authorization and **OpenID connect** used for Authentication. OpenID Connect is built on top of OAuth 2.0. So terminology and flow are similar between the two, you can both authenticate the user using OpenID Connect and get Authorization to access a protected resource that the user owns using OAu th 2.0 in one request.

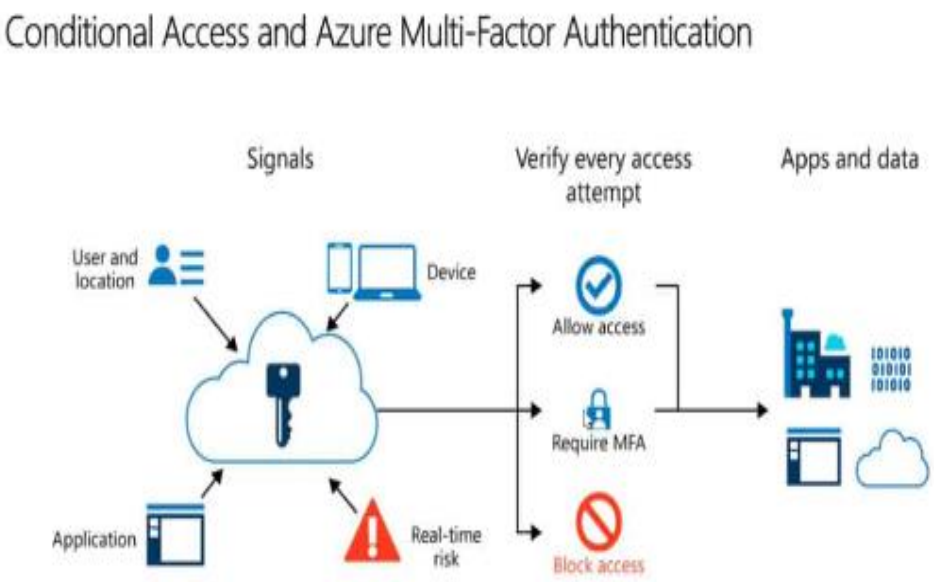


Question 3.What is Azure Active Directory?
Answer:
Azure Active Directory
Azure Active Directory (Azure AD) is a cloud-based identity and access management service. This service helps your employees access external resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications. 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.

Question 4. What are multifactor authentication and conditional access available in Azure?
Answer:
Multi Factor Authentication
Azure Multi-Factor Authentication supplies added security to your identities by acquiring two or more elements complete the authentication, that elements fall in three categories:

Something you know: Which might be a password or answer to a security question.
Something you possess: This might be a mobile app that receives a notification or a token-generating device.
Something you are: Which typically is a biometric property, such as a fingerprint or a face scan used on many mobile devices.

Conditional Access
Conditional access is an Azure tool that brings signals together to make decisions and enforce organizational policies. this is the workflow and conditional access and architecture of Azure Multi-Factor Authentication.



Question 5.What is resource lock? Describe why resource lock should be used?
Answer:
Azure Resource Lock
(* Azure operations can be divided into two categories - control plane and data plane. Locks only apply to control plane operations.)
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.
You can set the lock level to **CanNotDelete** or **ReadOnly**. In the portal, the locks are called Delete and Read-only respectively.
CanNotDelete- means authorized users can still read and modify a resource, but they can't delete the resource.
ReadOnly- means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Why use Resource Lock
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.

Question 6. What is Azure policy? Write it Usage.
Answer:
Azure Policy
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 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 a 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.
Azure Policy Usage
Common use cases for Azure Policy include implementing governance for:

- **Resource consistency**
- **Regulatory compliance**
- **Security**
- **Cost & Management**

Question 7. What is the Azure government? What is Azure China 21Vianet?
Answer:

Azure Government

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.

Azure China 21Vianet

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..

*End of the page.