**Azure fundamental assignment 5**

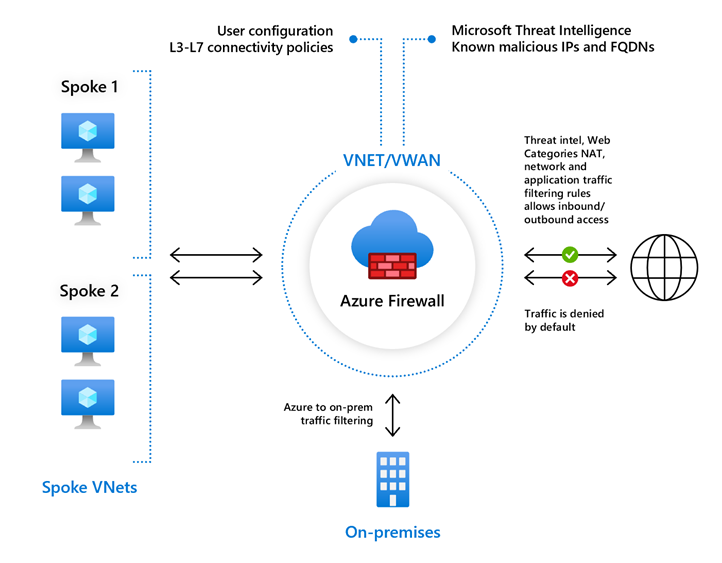
1. What is the Azure firewall? How to use the Azure firewall?

Azure Firewall is a cloud-native, intelligent network firewall security service that provides the best threat protection for cloud workloads running on Azure. It is a complete stateful firewall as a service with built-in high availability and unlimited cloud scalability. It provides both east-west and north-south traffic inspections.

The Azure Firewall is available in two SKUs, Standard and Premium.

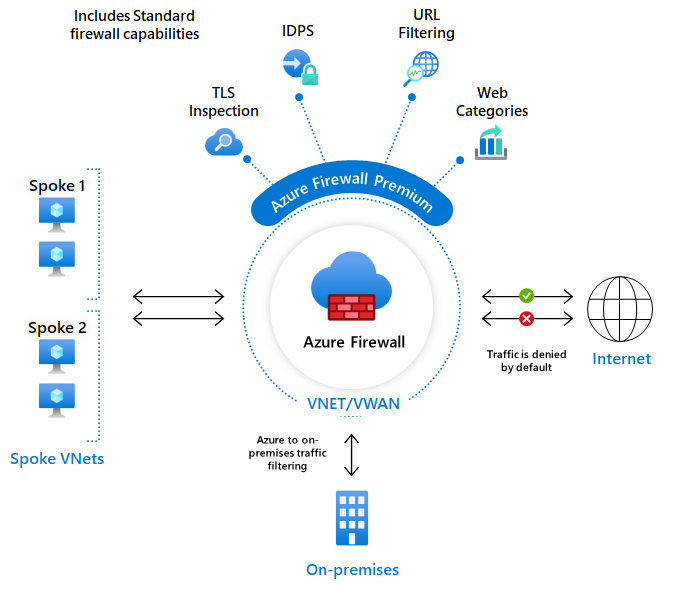
**Azure Firewall Standard**

Azure Firewall Standard provides L3L7 filtering and threat intelligence feeds directly from Microsoft Cyber ​​Security. Threat intelligence-based filtering is updated in real time to alert and deny traffic to and from known malicious IP addresses and domains and to protect against emerging attacks.



**Azure Firewall Premium**

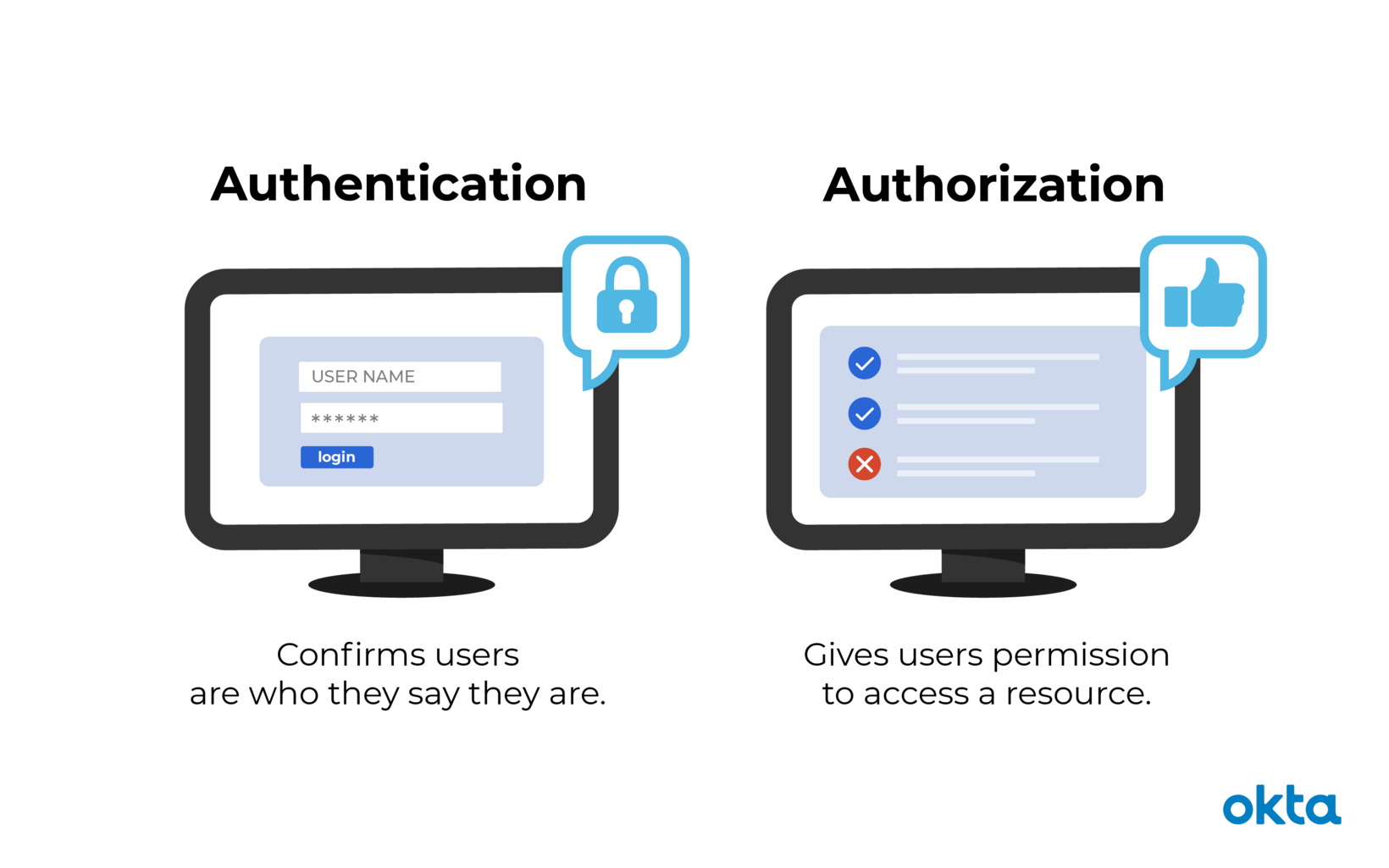
Azure Firewall Premium provides advanced features, including signature-based IDPS, to help you detect attacks quickly by looking for specific patterns. These patterns can include byte sequences of network traffic and known malicious instruction sequences used by malware. Over 50 categories have over 58,000 signatures and are updated in real-time to protect against emerging exploits. Exploit categories include malware, phishing, coin mining, and Trojan horse attacks.

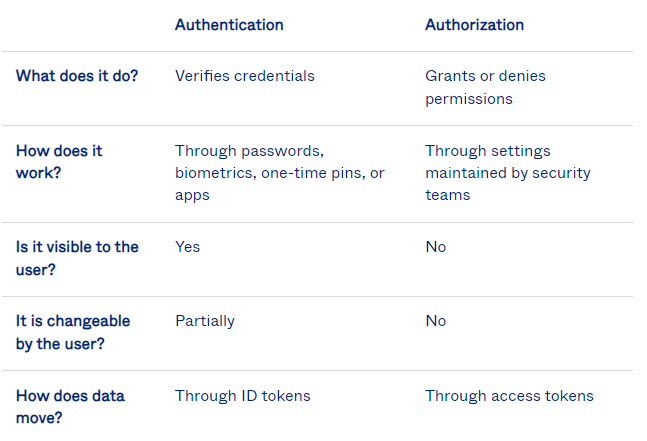


how to use firewalls:

* Set up a test network environment
* Deploy a firewall
* Create a default route
* Configure an application rule to allow access to [www.google.com](http://www.google.com)
* Configure a network rule to allow access to external DNS servers
* Configure a NAT rule to allow a remote desktop to the test server
* Test the firewall

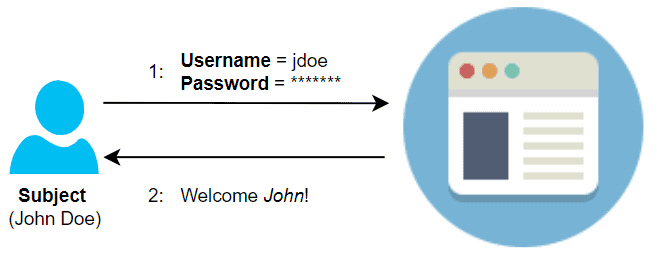
1. Differentiate authentication and authorization?





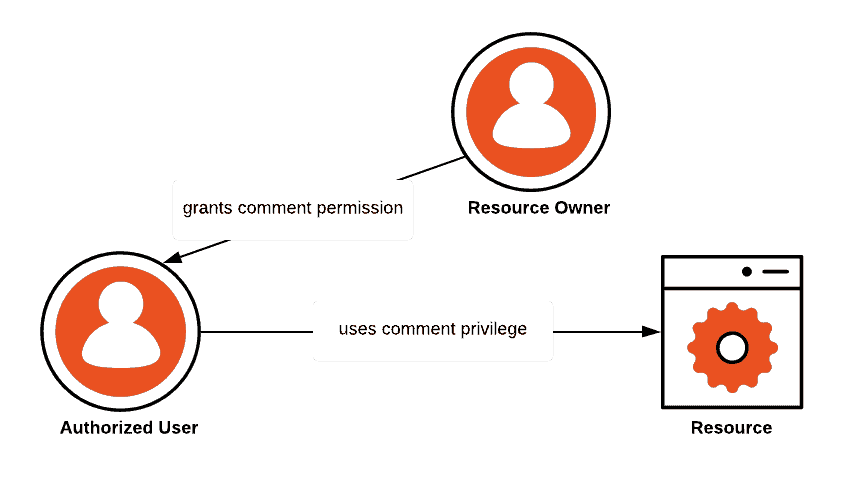
**Authentication** is the process of proving who you are and who you say you are? Microsoft identity platform implements the OpenID Connect protocol for handling authentication, authentication, and authorization

Azure App Service provides built-in authentication support, so you can sign in users and access data by writing minimal or no code in your web app



**Authorization** is the act of granting an authenticated party permission to do something. Microsoft identity platform implements the OAuth 2.0 protocol for handling authorization.

Azure App Service provides built-in authorization support, so you can sign in users and access data by writing minimal or no code in your web app, RESTful API, and mobile back end, and also Azure Functions.



1. What is Azure Active Directory?

Azure Active Directory is Microsoft`s multitenant, cloudbased 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.

AD stands for Active Directory.  In order to understand what Active Directory is, you’ll need to understand the basics of a Domain Controller.

A Domain Controller is a server on the network that centrally manages access for users, PCs and servers on the network. It does this using AD.

Active Directory is a database that organises your company’s users and computers. It provides authentication and authorization to applications, file services, printers, and other resources on the network. It uses protocols such as Kerberos and NTLM for authentication and LDAP to query and modify items in the Active Directory databases.

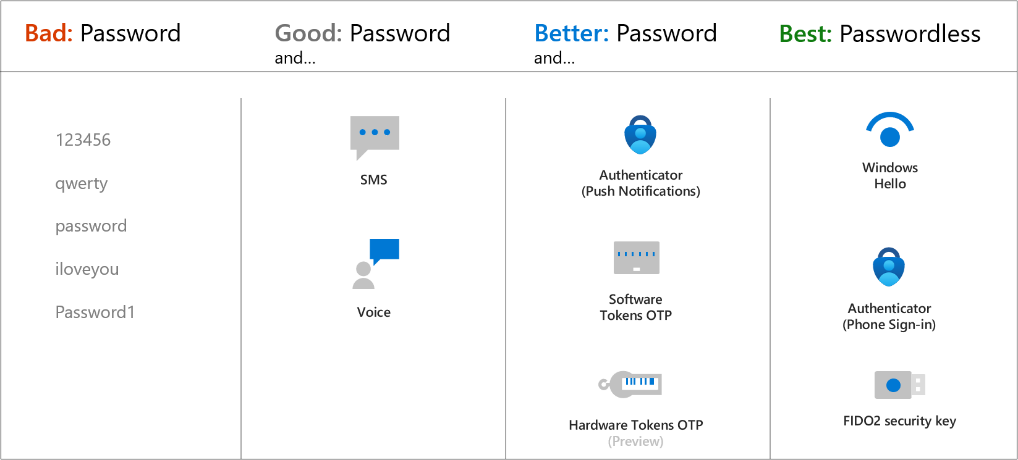
### Key Functions of AD

Active Directory Domain Services (to give it is the full and proper name)  run on the Domain Controller and have the following key functions:

* Secure Object store, including Users, Computers and Groups
* Object organization – Organisational Units (OU), Domains and Forests
* Common Authentication and Authorization provider
* LDAP, NTLM, Kerberos (secure authentication between domain-joined devices)
* Group Policy – for fine-grained control and management of PCs and Servers on the domain

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

Azure Active Directory (Azure AD) Multi-Factor Authentication helps safeguard access to data and applications, providing another layer of security by using a second form of authentication. Organizations can enable multifactor authentication (MFA) with Conditional Access to make the solution fit their specific needs.



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.

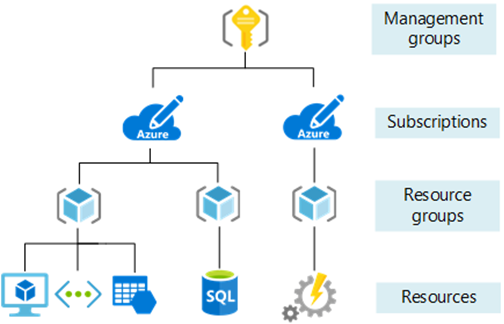
If you only use a password to authenticate a user, it leaves an insecure vector for attack. If the password is weak or has been exposed elsewhere, an attacker could be using it to gain access. When you require a second form of authentication, security is increased because this additional factor isn't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

Azure 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.

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

Resource Locking within Azure provides a method to lock subscriptions, resource groups or individual resources to protect them from accidental deletion and changes; even for administrators (depending on their RBAC role).



Resource Locks come in 2 levels; CanNotDelete (**displayed as ‘Delete’ in the portal**) or ReadOnly (**displayed as ‘Read-only’ in the portal**).

Now you may think that once deployed putting ReadOnly locks on everything is probably the best thing to go and do. And in some select scenarios I may even agree with you, however this is not best practice; so only do this if you absolutely have too!

Resource Locks can be applied at the following Azure governance scoping levels:

* Subscription
* Resource Group
* Resource

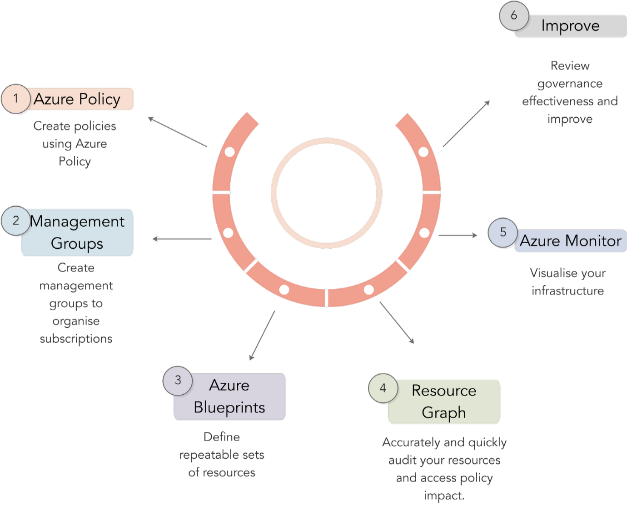
In my opinion, applying locks at the Subscription level is way to high in the governance hierarchy structure and makes using Azure clunky; as everything you deploy within that subscription will inherit the lock from the subscription level.

Taking it to the other end of the governance hierarchy at placing locks at the Resource level can again be very tedious and difficult to manage and keep on top of. However in some cases it can actually be very useful.

1. What is Azure policy? Write it Usage.

The Azure Policy is a free Azure service that permits you to make policies, and assign them to resources, and receive alerts or take action in cases of non-compliance with these policies.

The Azure Policy permits you to make sure that all resources are configured with required services, and it will tell you when systems are out of compliance. So if you want all of your resources to be configured with Azure Backups, for example, it will either alert you when a VM does not have Azure Backups configured or can automatically configure Azure Backups on that VM.



The Azure Policy is used by 100% of Azure’s top 300 enterprise users and is a critical part of any mature Azure deployment. As a part of a broad Azure governance apply, Azure Policy ensures that individuals on the far side of your central IT team (i.e. developers and LOB teams) will still have access to cloud resources, and might launch resources on demand, while not sacrificing security and compliance. The basic building blocks of Azure Policy are:

The Azure Policy is a service in Azure that permits you to produce polices that enforce and management the properties of a resource. The Azure Policy evaluates state by examining properties on resources that area unit portrayed in Resource Manager and properties of some Resource suppliers. The Azure Policy does not restrict actions. The benefits are as follows:-

* It provides a mechanism of auditing nuanced configurations of Azure resources.
* It blocks resource configurations that are non-compliant.
* It supports the flexibility to “Deploy If Not Exists” (DINE Policy Affect).
* It gives developers the liberty to use their tool of alternative.

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 rely on Microsoft Azure Government to provide best-in-class security and compliance. Azure Government provides a dedicated cloud that enables government agencies and their partners to move mission-critical workloads to the cloud. The Azure Government service may process data in accordance with various US government regulations and requirements.

To provide the highest level of security and compliance, Azure Government uses only physically separated data centres and networks in the United States. Compared to Azure Global, Azure Government adds to customers through a contractual obligation to store customer data in the United States and limit potential access to systems that process customer data to validated Americans. Provides a protective layer for.

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..