**Chapter 3: DEFENSE IN DEPTH**

**Topic – 1: Azure Cloud Security Tools**

**Sentinel**

* Used for **security information** & **event monitoring** (**SIEM**).
* Security team shares **common dashboard** & acts accordingly.

**Defender For Cloud**

* Comes under category of ***cloud security posture management (CSPM)*** tool.
* Identifies **cloud vulnerabilities**.
* Can be implemented **anywhere** in the system.

**Application Insights**

* Comes under category of ***application performance management (APM)*** tool.
* Can monitor **live web apps** & its performance.
* Mainly used for performance **bottleneck detection**.

**Resource Manager**

* Used for creating & managing **assets**.
* Can automate deployments using **templates**, **reducing configuration errors**.

**Azure Monitor**

* Another **data monitoring tool**.
* Provides **thread notifications** & **data visualization** tools.

**Web Application Firewall (WAF)**

* Part of ***Azure application gateway (AAG)***.
* Protects web services against **session hijacking** & **SQL injections**.

**Topic – 2: Identity & Access Management (IAM)**

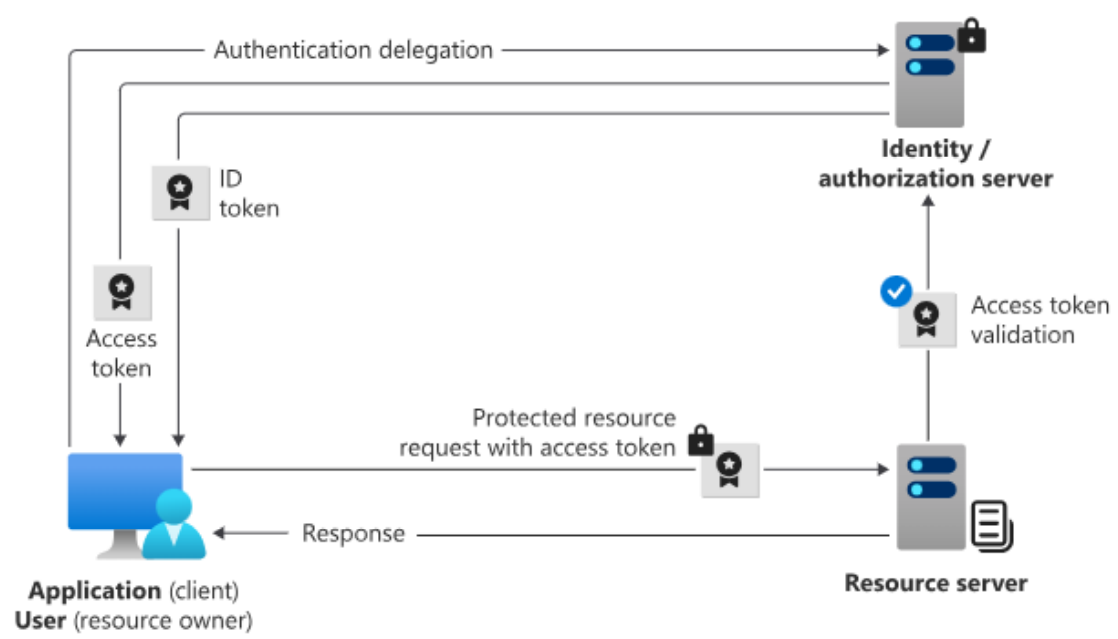
**Introduction**

* Makes sure that **authorized people**, **machines** & **software** get access to resources.

**Core Functionalities**

* **Identity management:** Stores data of authorized components using **identity providers** (**IdP**) & tracks them too.
* **Identity federation:** Allows user within **certain** organization to access resources.
* **Provisioning & deprovisioning of users:** Creating & managing user details including what level of access they have.
* **Authentication of users:** Uses either **multi-factor authentication** (**MFA**) or **single sign-on** (**SSO**) for authenticating.
* **Authorization of users:** Makes sure that users get access to resources they are entitled to.
* **Access control:** **Superset** of above two definitions.
* **Reports & monitoring:** Generates **reports** on safety qualities when any security related action is taken or changes is made.

**Working Of IAM**



**Topic – 3: Azure Active Directory (AAD)**

**Introduction**

* **Windows AD** is previous version of **Azure AD** which is **not** used anymore.
* **AAD** has **many layers** which makes it **slower**.
* **REST:** Representational State Transfer
* **LDAP:** Lightweight Directory Access Protocol
* **GPO:** Group Policy

**Azure AD v/s Windows AD**

|  |  |
| --- | --- |
| **Azure Active Directory** | **Windows Active Directory** |
| **Uses RESTful APIs.** | **Uses LDAP.** |
| **Cloud-based protocols.** | **Kerberos and NTLM.** |
| **Flat structure of users.** | **Tree structure of users.** |
| **Admins alone take control.** | **Admins & data owners take control.** |
| **Mobile device management.** | **No mobile device management.** |
| **Uses domain servers.** | **Uses GPOs servers.** |