Managing identities is a very imp task to do in any organization so IAM is responsible for this. IAM is all about creating an account of the user in Authorized source and use that identity to provision to end points (i.e. Laptops, databases)

In case of Web Access Management, WAM uses that identities and grants access to web resources. In WAM, we need to write correct set of policies such that an user have only access to allowed web pages. Whenever accessing any web page, it will go and check attributes from LDAP.

**LDAP:**

* LDAP stands for Lightweight Directory Access Protocol.
* As the name suggests the operations are much faster as compared to Relational databases.
* It is a client server based standard protocol which is used to connect with directory.

Three major principles of WAM are as follows:

1. Authentication: Proving that you are the one who you are proving to be. Ex: For logging into any application, we need to enter the credentials which includes username and passwords.
2. Authorization: It includes giving access to right set of identities based on Least privileged access. Least Privileged access means that a user have minimum access to any target application to perform basic functions.
3. Auditing: It includes a review phase to check what someone is doing on web access.

**SSO:**

SSO stands for Single Sign On. It allows users to log into multiple applications using same set of credentials. SAML stands for Security Assertion Markup Language. It is a standard which uses SSO. As the user’s identity is stored in directory so it would make more sense to fetch those identities from the active directory and log users into different applications.

But the question may arise that using same set of credentials may be lead to security breach.

**How to enhance security in SSO?**

User id and password is not sufficient these days so adding extra layer of security is very important.

* First layer of authentication is something that we know such as user id and password. It is not a safer option.
* Second layer of authentication is something we have. Ex. Tokens, Authenticator, smart card, badges
* Third layer of authentication is something we are. Ex. Biometric, Retinal Scan, Voice Print

**Load Balancer:**

Before knowing about load balancer, it is very important to know about what is server? Server is a machine running some program and we can utilize that program. So Load Balancer is distributing the load on different servers

Proxy is an act that someone else does on our behalf.

Load balance can act as a

1. Forward Proxy: forward proxy is the intermediate through which client request is sent and then it fetches the data from the server and returns to the client. It has some firewalls. Through which it checks for request and returns the response accordingly. It protects the client

Server

Client

1. Reverse Proxy: It rather protects the server side. So, whenever any request is made by the internet or server side it goes through the reverse proxy. Reverse proxy server is a superset of Load Balancer which means every reverse proxy server can be a load balancer but every load balancer can’t be reverse proxy server.

Internal requests within the network can be handled by internal servers whereas external network requests can be handled by external servers. So, these external servers are known as DMZ (demilitarized zone)