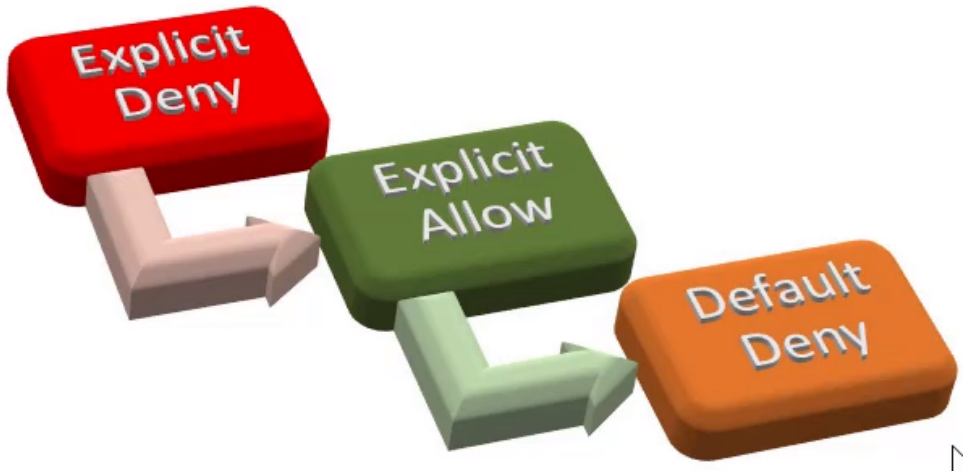
Policy Evaluation Logic

When you have Conflicting Permissions, final solution is done via Policy Evaluation Logic

- All requests are DENIED by default - “Default Deny”
- If there is an **explicit Deny,** then the **final decision is DENY**
- When there is no explicit Deny specified in the policy, it checks whether there is any explicit “Allow”
- If there is Allow then the final decision is Allow.
- However, there is no Deny or Allow specified then the final decision is “Deny”

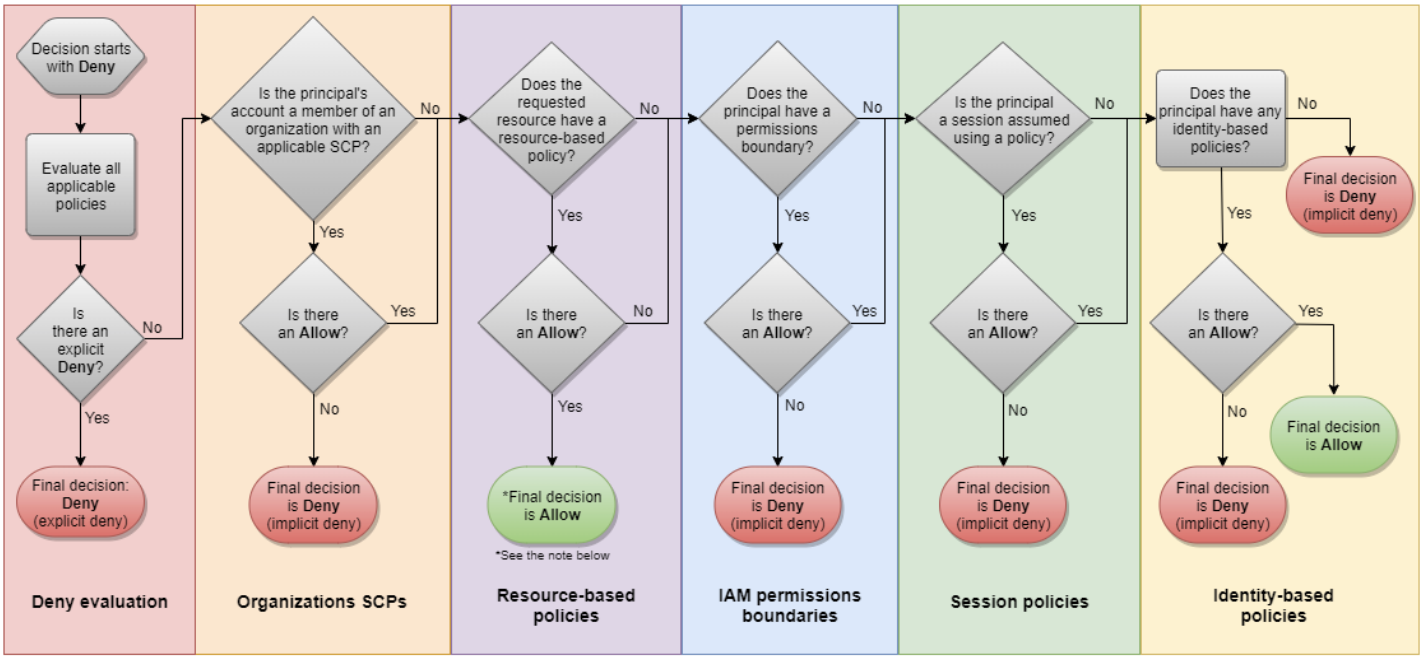


Source for the image: https://www.whizlabs.com

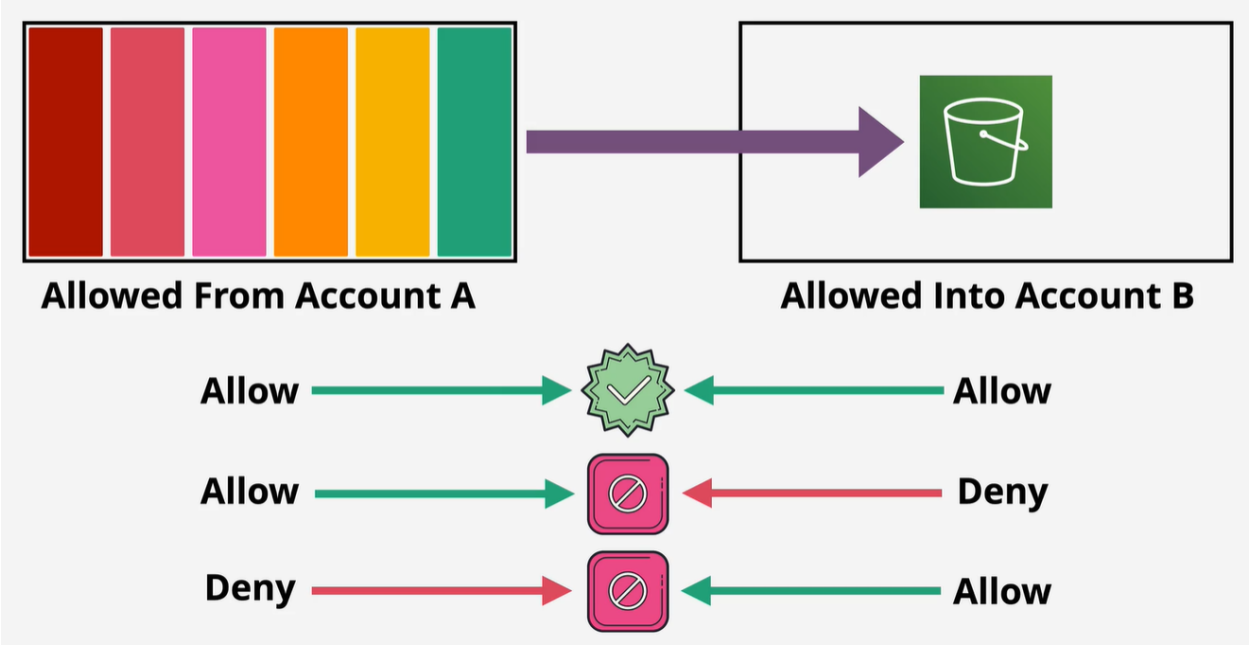
1. First look for any Explicit Deny
2. Then look for any Explicit Allow
3. If none of them applied then Default Deny

IAM Password Policy allows to create strong password for IAM account

Policy Evaluation Logic - SAME ACCOUNT



Policy Evaluation Logic - DIFFERENT ACCOUNT



Source: https://learn.cantrill.io/p/aws-certified-solutions-architect-professional

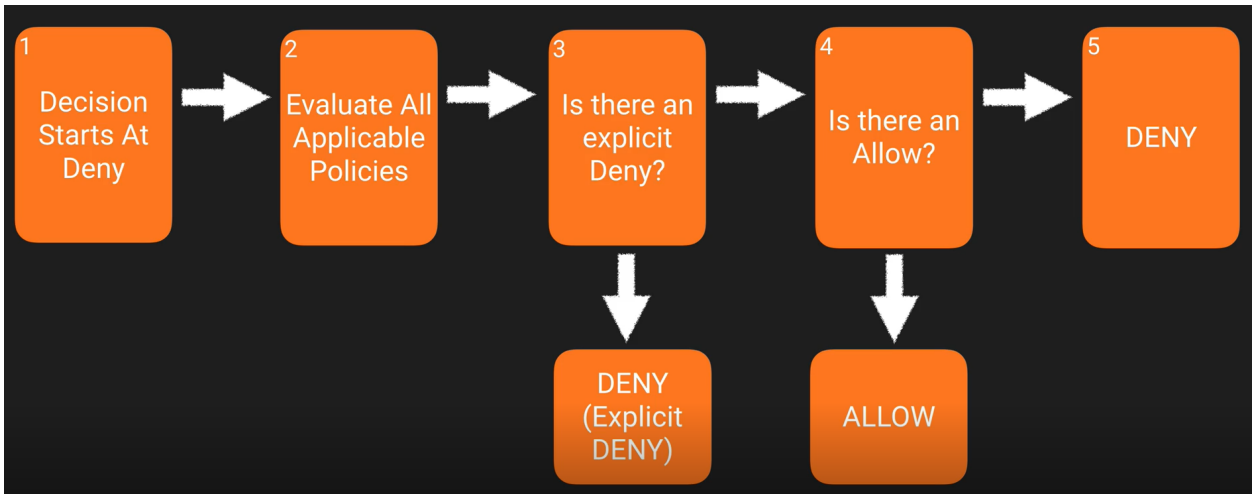
This is from CloudGuru

What happens if an IAM Policy, ACL, Bucket Policy contradicts

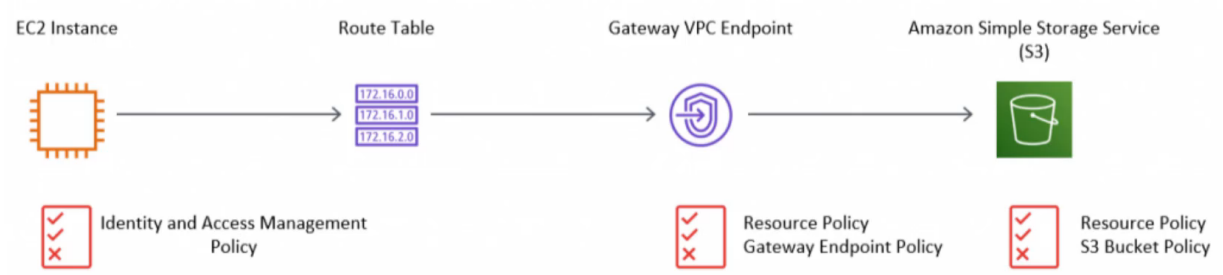
With least-privilege - Default Deny

Explicit Deny always trumps an Allow

IF no methods specifies an Allow, the the request will be denied by default



When there is a Gateway Endpoint Policy Consider this….



Read this:
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html