### **1. Design Review vs. Connectivity (Firewall) Review**

#### **Design Review:**

* Higher-level assessment.
* Triggered when a system/user wants to use a data platform (e.g., Snowflake, SingleStore).
* Focuses on **use case**, **data classification**, **access pattern**, and **integration security**.
* Mostly a **self-attestation** process (trust-based).
* Ensures the design adheres to defined standards before provisioning connectivity.

#### **Connectivity/Firewall Review:**

* Triggered **after design approval** when specific users/systems request access.
* Actual enforcement point, where access is either granted or blocked.
* Requires **validation of technical details** like source/destination, ports, environments, data classification.

### **2. Key Validation Points During Firewall Review**

1. **Secure Ports**:  
   * Only allow **secure ports** (e.g., Port 443).
   * Block non-secure ports (e.g., Port 80) unless justified.
2. **Cross-Environment Check**:  
   * **No cross-environment access** (e.g., non-prod → prod).
   * Validate source (deployment/system) and destination (workspace).
3. **Data Classification Check**:  
   * No **cross-classification access** violations.
   * For example:  
     + **DP-30 to DP-10 (write)** is **not allowed**.
     + **DP-10 reading from DP-30** may be okay.
   * Data classification should be mapped (via Middlebury engineering's inventory).
4. **User Group Validation**:  
   * Validate that users belong to the group/team for whom the workspace was designed (e.g., data engineering).
   * Question if there's a mismatch (e.g., random teams requesting access).
5. **Number of Users**:  
   * Large user base (>25 or >50 users) should raise concern.
   * Only a **handful of developers** should have access unless business justification (e.g., Tableau reports for business users).

### **3. Automation & Documentation**

* Plan to **standardize and document** the questions/checks.
* Create a **template/checklist** for:  
  + **Design Review Questionnaire**
  + **Connectivity/Firewall Approval Checklist**
* This template will include the above points.
* Aim to eventually **automate approvals** where these conditions are clearly met, reducing manual interventions.

### **4. Immediate Next Steps**

* Prepare a document that includes:  
  + Checklist for **Design Review** (self-attested).
  + Checklist for **Firewall Review** (technical validation).
* Share with team, including US-based members for urgent firewall approvals.
* Use this as a standard reference for reviewing connectivity requests.