To implement this solution efficiently, we need a **modular system architecture** that integrates **ABAC enforcement, ServiceNow approvals, and scalable country-based access controls**. Below is a detailed **system design plan**, covering components, interactions, and data flow.

**1. High-Level Architecture**

We propose a **three-layered architecture** for security and scalability:

**A. Application Layer (User & Access Management)**

* **Users (Employees, Contractors, Admins)** – Access the system via web applications, internal tools, or APIs.
* **Authentication (SSO / OAuth2 / AD Integration)** – Ensures user identity validation.
* **ServiceNow (SNOW) for Approval Requests** – Users request access via SNOW, triggering a workflow.

**B. Access Control Layer**

* **Attribute-Based Access Control (ABAC) Engine** – Enforces real-time access decisions based on user roles, countries, and approval status.
* **API Gateway / Middleware** – Intercepts access requests, validates entitlements, and forwards only authorized requests.
* **Dynamic Country Configuration Service** – Maintains the list of restricted countries and automatically enforces new rules.

**C. Data & Logging Layer**

* **Audit & Logging System** – Stores access logs for compliance reviews.
* **Approval & Policy Database** – Tracks approval statuses and policies.
* **Reports & Analytics** – Generates compliance dashboards for security teams.

**2. Component Breakdown and Interactions**

| **Component** | **Function** |
| --- | --- |
| **User Management (SSO/OAuth2)** | Authenticates users and provides role-based access. |
| **ServiceNow Workflow** | Handles access requests, approvals, and revocations. |
| **ABAC Policy Engine** | Validates real-time access based on country, user attributes, and approvals. |
| **API Gateway / Middleware** | Acts as a security checkpoint for data access. |
| **Dynamic Country List Service** | Stores restricted countries and applies rules dynamically. |
| **Audit & Logging System** | Captures access logs for security reviews. |
| **Compliance Dashboard** | Displays approval trends and security insights. |

**3. System Flow & Interactions**

**Scenario 1: User Requests Access via ServiceNow**

1. **User submits a SNOW ticket** for India/Malaysia data.
2. **Approval Workflow:** SNOW routes request → Data Owner reviews → Approves/Rejects.
3. **Approved user attributes update** (stored in DB or Active Directory).
4. **Access granted** via ABAC on next login.

**Scenario 2: User Accessing Restricted Data**

1. User requests access via **UI/API call**.
2. **API Gateway intercepts request**.
3. **ABAC Engine checks:**
   * Does the user have **global entitlement**?
   * Is the **country restricted**?
   * Does the user have **SNOW approval**?
4. **Allowed?** → Data access granted.  
   **Denied?** → Access blocked with SNOW ticket prompt.

**Scenario 3: New Country Gets Added to the Restricted List**

1. Security Team updates **Dynamic Country List Service** (via UI or API).
2. New restrictions **automatically propagate** to ABAC policies.
3. No need for **manual rule updates**.

**4. Technology Stack Recommendation**

| **Component** | **Technology Recommendation** |
| --- | --- |
| **Authentication** | OAuth2, SAML, Active Directory (AD) |
| **Approval System** | ServiceNow Workflow Automation |
| **ABAC Engine** | Open Policy Agent (OPA), XACML, AWS IAM Policies |
| **API Gateway** | Kong, Apigee, Nginx, AWS API Gateway |
| **Dynamic Country List** | PostgreSQL, DynamoDB, Redis |
| **Logging & Auditing** | ELK Stack (Elasticsearch, Logstash, Kibana), Splunk |

**5. Scalability & Performance Considerations**

✅ **Microservices-based ABAC engine** ensures modular growth.  
✅ **Cached dynamic country list** prevents frequent DB queries.  
✅ **Asynchronous logging** for minimal performance impact.  
✅ **Auto-expiry for approvals** to prevent access creep.

**Next Steps**

1. **Define API endpoints** for integration.
2. **Develop & test ABAC engine**.
3. **Automate SNOW ticket processing**.
4. **Implement compliance dashboard** for security reviews.

This design ensures a **future-proof, scalable solution** with **real-time enforcement** and **compliance transparency**.