Excellent — this is a complex scenario involving **hybrid data connectivity**, **network security**, **authentication/authorization**, and **data governance** for Power BI. Below is a **comprehensive, end-to-end task list** that you can use as a **project implementation plan** or **architecture checklist** for securely connecting **on-premises data** with **Azure-based data sources** through **Power BI** using **ExpressRoute private peering** and **both On-prem and VNet Data Gateways**.

**🔹 Project Goal**

Enable secure and performant **Power BI report development and access** across **on-prem and Azure** data sources, ensuring **private data transfer**, **governed access**, and **end-to-end encryption/authentication**.

**✅ Phase 1 – Planning & Prerequisites**

**1. Define Architecture and Connectivity Scope**

* Identify all **on-prem data sources** (e.g., SQL Server, Oracle, SAP, Teradata, File shares).
* Identify all **Azure data sources** (e.g., Azure SQL, Synapse, Databricks, ADLS Gen2, Cosmos DB).
* Determine **which Power BI workloads** will access which data sources (DirectQuery, Import, or Composite model).
* Confirm **ExpressRoute private peering** is established between on-prem network and Azure Virtual Network (VNet).

**2. Network and Security Assessment**

* Validate that **Power BI Service** connects to Azure VNets using **VNet Data Gateway** or **Private Endpoints**.
* Validate **firewall and NSG rules** allow gateway-to-source communication.
* Plan **DNS resolution** for hybrid name resolution (on-prem + Azure private endpoints).
* Confirm **TLS/SSL certificates** are configured for encrypted connections.

**3. Authentication and Authorization Planning**

* Choose the **identity provider** (Azure AD as primary).
* Configure **Hybrid Identity** via **Azure AD Connect** (synchronize AD users and groups).
* Define **RBAC roles** for Power BI workspace access (Admin, Member, Contributor, Viewer).
* Plan **service principals** or **Managed Identity** for automated dataset refreshes or API-based access.

**✅ Phase 2 – On-premises Data Gateway Setup**

**4. Install and Configure On-prem Data Gateway**

* Deploy **Standard Mode** Gateway on a secured on-prem server (not personal mode).
* Configure **gateway cluster** for high availability and load balancing.
* Register gateway with **Power BI Service** using the **admin account**.
* Validate outbound connectivity via **ExpressRoute** (ensure no public internet dependency).

**5. Connect On-prem Data Sources**

* Configure data sources in Power BI Gateway:
  + SQL Server (Windows Authentication / Azure AD)
  + Teradata / Oracle / SAP (use ODBC drivers)
* Assign **users/groups** for access control in gateway data sources.
* Verify **DirectQuery and Scheduled Refresh** operations work via ExpressRoute.

**✅ Phase 3 – VNet Data Gateway & Azure Integration**

**6. Deploy Azure VNet Data Gateway**

* Create the **VNet Data Gateway** resource in Azure.
* Associate it with the target **Azure Virtual Network** where Azure data sources reside.
* Ensure **Private Endpoints** for Azure SQL, Synapse, Databricks, and ADLS are configured.
* Integrate gateway with **Power BI Service (Managed VNet)**.

**7. Configure Azure Data Sources**

* Add Azure SQL / Synapse / Databricks / ADLS sources in Power BI Service.
* Ensure connections are **private (not over public endpoints)**.
* Configure **Azure Private DNS Zones** to resolve internal FQDNs.
* Test end-to-end query execution over ExpressRoute.

**✅ Phase 4 – Data Modeling and Security**

**8. Combine Data from On-prem and Azure**

* Use **Power BI Desktop** with both gateways configured:
  + On-prem via **On-prem Data Gateway**
  + Azure via **VNet Data Gateway**
* Create **Composite Models** or **Dataflows** that unify hybrid data sources.
* Validate **data lineage** via **Power BI Lineage View** or **Microsoft Purview**.

**9. Apply Data Security**

* Implement **Row-Level Security (RLS)** and **Object-Level Security (OLS)**.
* Enforce **sensitivity labels** and **data loss prevention (DLP)** policies via **Microsoft Purview**.
* Encrypt data at rest (on data source) and in transit (via TLS).
* Enable **Microsoft Defender for Cloud Apps** for Power BI data exfiltration control.

**✅ Phase 5 – Authentication & Access Control**

**10. Configure Authentication**

* Use **Single Sign-On (SSO)** via Azure AD for Power BI → Gateway → Data Source.
* For on-prem SQL Server, configure **Kerberos Constrained Delegation (KCD)**.
* For Azure SQL and Synapse, use **Managed Identity** or **Service Principal** for connections.

**11. Configure Authorization**

* Map **Power BI roles** to **Azure AD security groups**.
* Restrict workspace sharing to organizational accounts only.
* Use **Conditional Access Policies** (MFA, device compliance) for Power BI Service access.

**✅ Phase 6 – Report Publishing and Access**

**12. Report Deployment**

* Publish reports to **Power BI Service** workspace.
* Validate dataset refresh via gateways.
* Configure **scheduled refresh** frequency and retry policies.
* Test **DirectQuery latency** and performance over ExpressRoute.

**13. Report Access from On-prem Users**

* Verify users can access Power BI Service through corporate SSO.
* Confirm **all traffic routes via ExpressRoute** (private peering).
* Validate no data flows through public endpoints.

**✅ Phase 7 – Monitoring, Governance, and Operations**

**14. Monitoring & Auditing**

* Enable **Gateway performance logs** and integrate with **Azure Monitor / Log Analytics**.
* Monitor **dataset refresh failures** in Power BI Admin portal.
* Enable **Power BI Audit Logs** in Microsoft 365 compliance center.
* Track **ExpressRoute metrics** (latency, throughput, errors).

**15. Governance & Lifecycle**

* Integrate with **Microsoft Purview** for data cataloging and lineage.
* Apply **Power BI Tenant Settings** (governed export, publish, and sharing rules).
* Define **incident response plan** for data leakage or access violations.
* Periodically **review gateway configurations and access roles**.

**✅ Phase 8 – Optimization and Documentation**

**16. Performance Tuning**

* Optimize **DirectQuery models** (limit cardinality, aggregations).
* Leverage **Power BI Premium capacity** for caching large models.
* Use **Query Folding** and **Incremental Refresh** for hybrid datasets.

**17. Documentation and Handover**

* Create a **runbook** for gateway management.
* Document **network diagrams, connectivity flow, and security controls**.
* Provide **end-user and admin training** on secure Power BI usage.

**🔐 Key Security Controls Summary**

| **Area** | **Control** | **Implementation** |
| --- | --- | --- |
| Network | Private connectivity | ExpressRoute + Private Endpoints |
| Gateway | Segregated gateway clusters | On-prem & VNet Gateways |
| Identity | Centralized SSO | Azure AD + KCD |
| Data Security | Encryption + RLS/OLS | Data source + Power BI model |
| Governance | Auditing & Purview | Compliance Center + Purview |
| Access | Conditional Access | MFA, Device Trust |