⇄ CSI Hybrid Infrastructure: Connectivity Options

CSI Hybrid Infrastructure: Connectivity Options

The CSI Hybrid Infrastructure is designed to bridge the gap between **Cloud Agility** and **On-Premises Security**. In today's regulatory landscape, organizations often face a "cloud dilemma": the desire for the high-availability and scalability of Azure, balanced against strict internal policies or legal requirements (such as GDPR or CJIS) that mandate data remain on physical, customer-controlled hardware.

CSI solves this by decoupling the **Application Logic** from the **Data Layer**.

- **The Cloud (Azure):** Handles user traffic, authentication, and application processing.
- **The Ground (On-Premises):** Serves as the authoritative, secure vault for your SQL data.

Core Architectural Pillars

Our hybrid framework is built on four fundamental principles:

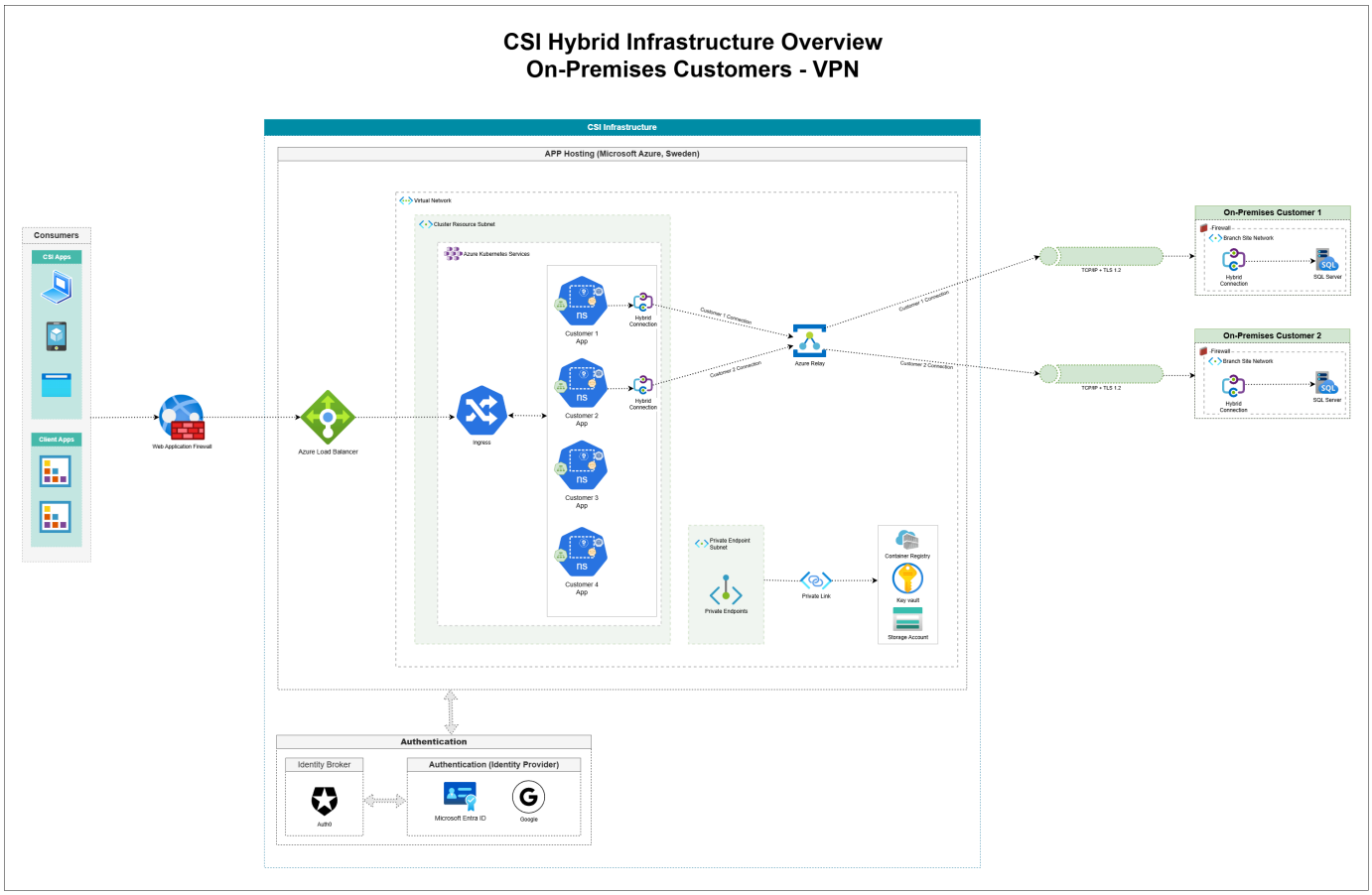
- **Data Sovereignty:** You maintain 100% ownership and physical custody of your databases. CSI only "borrows" the data for real-time processing; it is never permanently stored in the cloud.
- **Elastic Scalability:** By hosting the application in **Azure Kubernetes Service (AKS)**, the platform can automatically scale to handle thousands of concurrent users without putting stress on your local network.
- **Defense in Depth:** We implement multiple security layers, including Web Application Firewalls (WAF), Identity Federation (Auth0), and Azure Key Vault for secret management.
- **Connectivity Choice:** Recognizing that every IT environment is different, we offer three distinct paths—**Azure Relay**, **IP Whitelisting**, and **Site-to-Site VPN**—to ensure a seamless fit with your existing network policy.

1. Connectivity via Azure Relay (Hybrid Connections)

1. Introduction

CSI provides a hybrid solution where customer applications run in Microsoft Azure while data remains securely stored in the customer's on-premises SQL Server. This allows customers to maintain **data sovereignty** while leveraging CSI's scalable Azure-hosted platform.

To bridge the two, CSI uses **Azure Relay Hybrid Connections**. This ensures a secure, encrypted, outbound-only connectivity path without requiring customers to expose their internal networks or modify inbound firewall rules.



2. High-Level Architecture

- **CSI Azure Platform (AKS):**
  - Applications run in isolated pods within Azure Kubernetes Service.
  - Traffic is routed via Azure WAF, Load Balancer, and Ingress Controller.
  - Identity Management (Entra ID, Google, Auth0) remains cloud-based.
- **Customer On-Premises Environment:**
  - Customers host their SQL Server within their private network.
  - No inbound ports or public endpoints are required.
  - A lightweight **Hybrid Connection Manager (HCM)** agent is installed on a local server to bridge the connection.

3. How Azure Relay Connectivity Works

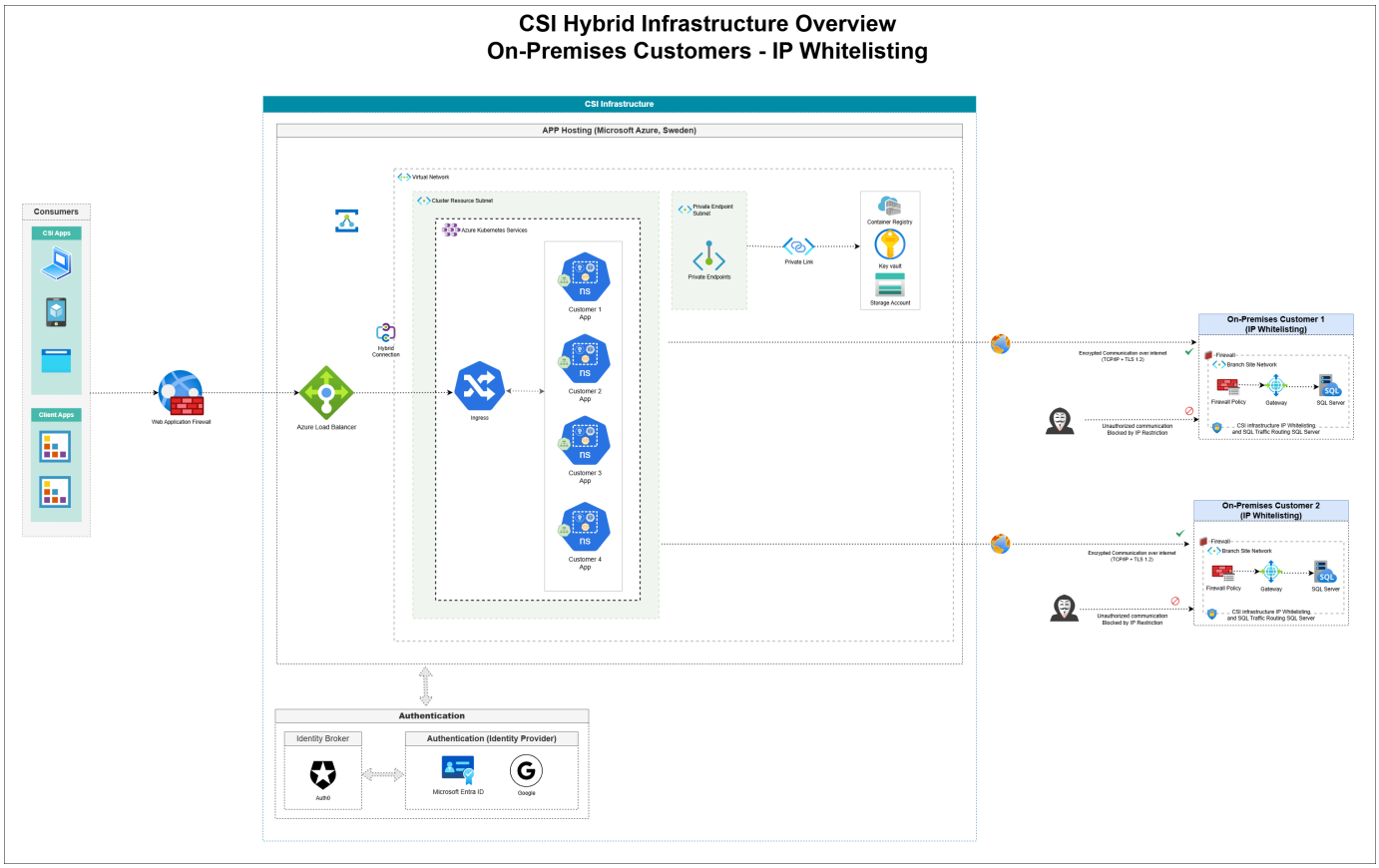
- **Outbound Secure Tunnel:** The customer's HCM initiates a secure outbound TLS 1.2 connection to Azure Relay over **Port 443**. Since this is outbound, it typically requires no special firewall exceptions.
- **Application-to-Database Communication:**
  1. **Request:** The CSI App pod sends a query to its assigned Azure Relay endpoint.
  2. **Relay:** Azure Relay forwards the request through the existing outbound HCM tunnel.
  3. **Local Handover:** The HCM passes the query to the SQL Server on the private network.
  4. **Return:** The SQL response follows the same encrypted path back to the application.
- **Security & Isolation:** Every customer has a unique Relay endpoint, ensuring isolated data streams and end-to-end encryption.

2. Connectivity via IP Whitelisting

1. Introduction

This model is designed for customers who prefer direct connectivity secured by perimeter defense. It ensures the database remains on your physical hardware to meet strict regulatory and residency requirements, while only allowing traffic from verified CSI infrastructure.

To bridge these environments, CSI utilizes a secure **IP Whitelisting** model. This ensures that only verified, encrypted traffic from CSI's dedicated Azure infrastructure can communicate with your database.



2. Architecture: A Zero Trust Approach

This model follows a **Zero Trust-inspired framework**, decoupling End-User Identity from Database Access. Even if a user's front-end credentials were compromised, the database remains inaccessible to them directly.

Layer	Security & Access Implementation
User Identity	**Federated Auth (Auth0 + Entra ID):** Users authenticate via Auth0. They never receive DB credentials; they only receive a short-lived token (JWT).
Application (AKS)	**The Secure Proxy:** The CSI App (in AKS) acts as the sole bridge. It is the only entity authorized to "speak" to your SQL Server.
Network Path	**Encrypted Public Endpoint:** Traffic travels over the internet secured by **TLS 1.2+ encryption**, making data unreadable in transit.

Layer	Security & Access Implementation
Database Perimeter	**IP Whitelisting:** Your firewall is configured to drop all traffic except for requests originating from CSI's **Static Outbound IPs**.

3. Data Access Flow (Step-by-Step)

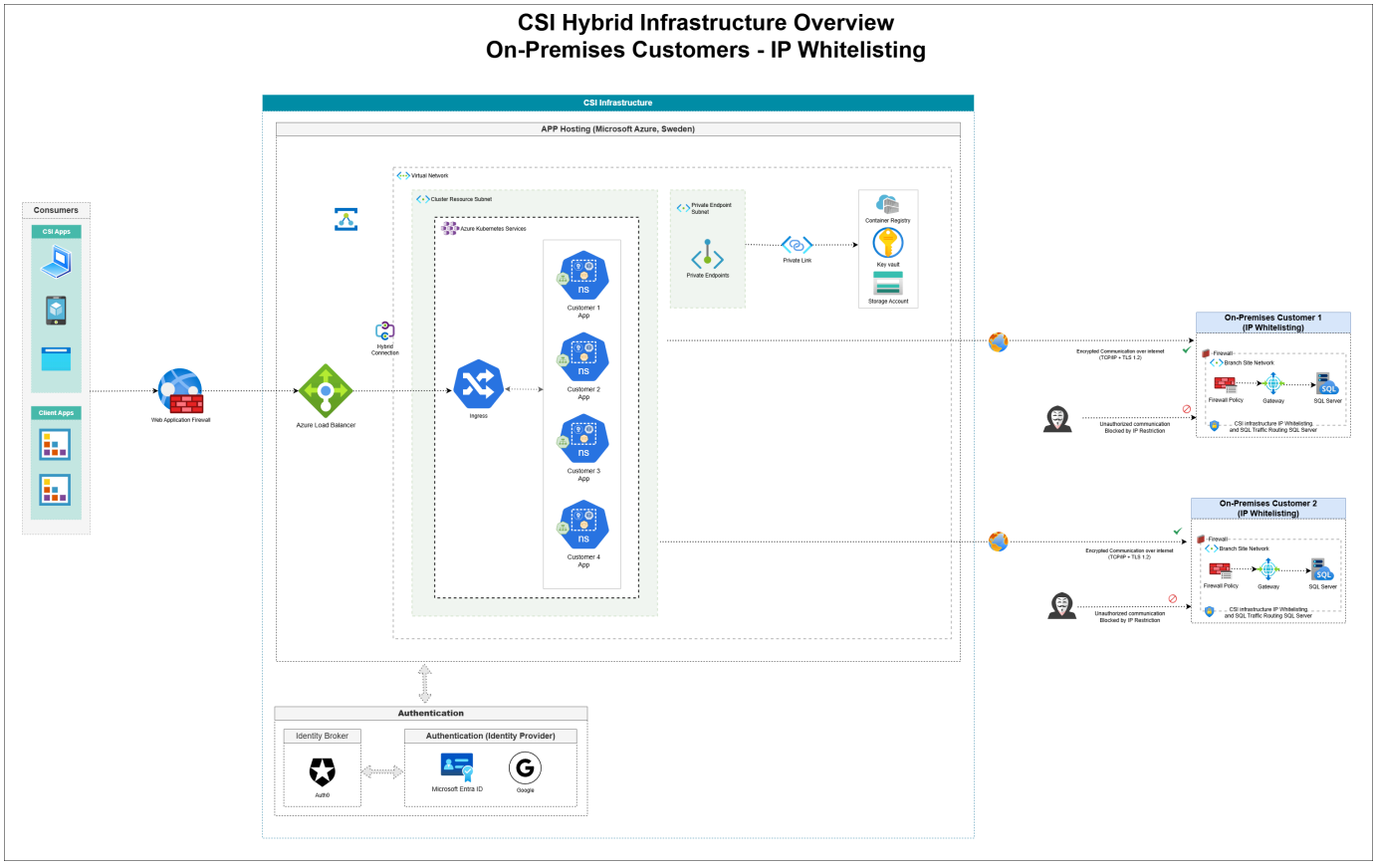
1. **Authentication:** The user logs in via Auth0/Microsoft Entra ID.
2. **Authorization:** The app sends the token to the AKS API; the API verifies user identity and permissions.
3. **Credential Retrieval:** The API retrieves SQL credentials securely from **Azure Key Vault** at runtime. Secrets are never stored in application code (**Credential Isolation**).
4. **Network Verification:** Your on-premises Firewall verifies the request is originating from a trusted, static CSI Azure IP.
5. **Secure Connection:** The API establishes an encrypted connection to the SQL Server using the retrieved credentials.

3. Connectivity via Site-to-Site VPN

1. Introduction

This architecture is designed for organizations that require a **permanent, network-level bridge** between their local data center and the cloud. It allows the Azure Virtual Network (VNet) and the on-premises network to act as a single, unified private network.

CSI uses an **Azure Site-to-Site (S2S) VPN** to establish a secure, encrypted tunnel over the public internet using industry-standard protocols.



2. High-Level Architecture

- **CSI Azure Platform (AKS):**
- Applications are hosted in AKS within a dedicated Virtual Network (VNet).
- An **Azure VPN Gateway** serves as the cloud-side endpoint.
- A **Gateway Subnet** is dedicated to managing cross-premises traffic.
- **Customer On-Premises Environment:**
- A **Customer VPN Device** (Hardware Firewall) maintains the connection.
- The **SQL Server** remains in the private local network, accessible via its internal private IP address.

3. How Site-to-Site VPN Connectivity Works

- **Secure IPsec Tunnel:** The connection uses **IPsec** and **IKE** protocols. Every data packet is encrypted before leaving one network and decrypted only upon arrival at the other.
- **Network-to-Network Communication:**

1. **Direct Routing:** The CSI application pod communicates with the SQL Server using its **local private IP address** (e.g., 10.x.x.x).
2. **Encryption:** Traffic is automatically routed to the Azure VPN Gateway for encryption.
3. **Local Delivery:** The customer's VPN device decrypts the traffic and delivers it to the SQL Server.

- **Security & Reliability:** Features industry-standard AES encryption and supports **BGP** for automatic routing synchronization.

4. Connectivity Comparison

Feature	Azure Relay (HCM)	IP Whitelisting	Site-to-Site VPN
Connection Type	Application-level	Application-to-Gateway	Network-level
Inbound Ports	**None** (Outbound only)	Required (SQL Port)	Required (VPN Ports)
Setup Complexity	Low (Agent based)	Low (Firewall rule)	High (Network config)
IP Management	IP-agnostic	Static Public IPs	Non-overlapping ranges
Maintenance	Minimal	Low	Moderate