Comprehensive Implementation Guide: PRJ-GCP-NET-090 Hybrid Connectivity with Cloud Interconnect

1. Project Overview

This project, **PRJ-GCP-NET-090**, is designed to establish a **secure and high-performance hybrid cloud network** between an on-premises data center and Google Cloud Platform (GCP) using **Cloud Interconnect**. The primary objective is to create a robust, low-latency, and private connection that extends the corporate network into the cloud. Beyond simple connectivity, the architecture is fortified with multiple layers of GCP-native security controls, including **VPC Service Controls**, **Cloud Armor**, and **Cloud IDS**, to ensure a compliant and impenetrable data perimeter. This design addresses the critical need for secure, high-throughput data transfer and application access in modern hybrid environments.

The core components and goals of this project are summarized below:

Component	Description
Project ID	PRJ-GCP-NET-090
Title	Hybrid Connectivity with Cloud Interconnect
Cloud Provider	Google Cloud Platform (GCP)
Key Services	Cloud Interconnect, VPC Service Controls, Cloud Armor, Cloud IDS, Cloud Router, VPC Flow Logs
Goal	Secure, compliant, and high-throughput hybrid network connectivity.

The implementation focuses on leveraging GCP's global network infrastructure to provide a dedicated, private connection that bypasses the public internet, ensuring

predictable performance and enhanced security for mission-critical workloads.

2. Business Context

In today's digital landscape, organizations face increasing pressure to migrate workloads to the cloud while maintaining stringent security and compliance standards. The lack of visibility, network segmentation, and exposure to public internet threats often results in significant operational risk and potential financial loss. This project directly addresses these challenges by implementing a secure, well-architected network foundation.

The Problem

GCP networks are often vulnerable to misconfigurations that expose resources to unauthorized access or data breaches. Organizations frequently lack comprehensive visibility into network traffic, making auditing and troubleshooting difficult. Furthermore, reliance on manual firewall management can lead to security gaps and inconsistent policy enforcement across the hybrid environment.

The Solution

The solution is a secure GCP network architecture that integrates advanced security services like **Cloud Armor** for edge protection, **Cloud IDS** for internal threat detection, and **VPC Service Controls** to establish a strong data perimeter. This design implements robust network segmentation, provides comprehensive DDoS protection, and ensures complete traffic monitoring, moving away from reactive security to a proactive, defense-in-depth posture.

Quantified Business Value and ROI

The implementation of this secure hybrid connectivity solution delivers significant, quantifiable business value, translating directly into a strong Return on Investment (ROI) and efficiency gains:

Value Proposition	GCP Service	Description	Business Impact (ROI/Efficiency)
DDoS Protection	Cloud Armor	Blocks volumetric and application-layer attacks at Google's edge.	**Cost Savings:** Reduces potential downtime costs from DDoS attacks (estimated at $5,000–40,000 per hour for enterprises). **Risk Mitigation:** Protects brand reputation and ensures service continuity.
Network Visibility	VPC Flow Logs	Provide complete traffic analysis for auditing, troubleshooting, and security monitoring.	**Efficiency Gain:** Reduces mean time to resolution (MTTR) for network issues by up to 40%. **Compliance:** Provides necessary audit trails for regulatory requirements.
Data Perimeter	VPC Service Controls	Prevent data exfiltration from sensitive services (e.g., Cloud Storage, BigQuery).	**Risk Mitigation:** Prevents costly data breaches (average cost of a breach is $4.45 million). **Compliance:** Essential for handling PII and sensitive regulated data.
Centralized Management	Network Intelligence Center	Provides unified visibility and monitoring for the entire network topology and configuration.	**Efficiency Gain:** Streamlines network operations and reduces manual configuration errors, saving up to 15% in operational overhead.
High-Throughput Connectivity	Cloud Interconnect	Dedicated, private connection with guaranteed bandwidth.	**Efficiency Gain:** Accelerates data migration and synchronization between on-premises and GCP, improving application performance and reducing latency for hybrid applications.

Risk Mitigation

By implementing this architecture, the organization actively mitigates several critical risks:

- **DDoS attacks:** Cloud Armor provides a first line of defense against network and application-layer denial-of-service attacks.
- **Unauthorized network access:** Granular firewall rules and VPC segmentation restrict access to only necessary resources.
- **Data exfiltration:** VPC Service Controls create a security boundary, preventing data from leaving the defined perimeter.
- **Lateral movement of threats:** Network segmentation and Cloud IDS monitoring limit the spread of malware or unauthorized access within the VPC.

3. GRC Mapping (Governance, Risk, and Compliance)

This architecture is specifically designed to align with major global compliance frameworks, providing a foundation for a strong Governance, Risk, and Compliance (GRC) posture. The implementation of specific GCP services directly addresses common security control requirements.

Compliance Frameworks Alignment

The following table details how the implemented controls map to industry-standard security frameworks:

Framework	Requirement	Implemented Control	Description
NIST CSF	PR.AC-5 (Network segregation), PR.PT-4 (Network protection)	VPC Service Controls, Hierarchical Firewall Policies	Achieved through the creation of a secure data perimeter and consistent, organization-wide network segmentation.
ISO 27001	A.13.1 (Network security management)	Network Intelligence Center, Cloud Router	Supported by centralized management, monitoring, and defined network security policies for the hybrid connection.
CIS Controls	Control 12 (Network Infrastructure), Control 13 (Network Monitoring)	Cloud Interconnect, Cloud Router, VPC Flow Logs	Implemented via a dedicated, managed connection and comprehensive logging for all network traffic.
Zero Trust Architecture	NIST SP 800-207	VPC Service Controls, Granular Firewall Rules	Enforced by establishing a perimeter around sensitive services and applying least-privilege access rules at the network layer.

Security Controls Implemented

The defense-in-depth strategy relies on the following key security controls:

- **VPC Service Controls:** Establishes a security perimeter around sensitive GCP services to mitigate the risk of data exfiltration.
- **Cloud Armor:** Provides Web Application Firewall (WAF) and DDoS protection for internet-facing services.
- **Cloud IDS:** Offers network-level intrusion detection and threat monitoring for traffic within the VPC.
- **Hierarchical firewall policies:** Ensures consistent and centralized network segmentation policies across the organization or folders.

- **Private Google Access:** Allows instances in the VPC to securely access Google APIs and services using internal IP addresses, bypassing the public internet.

Regulatory Alignment

The project's architecture supports compliance with several key regulatory mandates:

Regulation	Requirement	Alignment
PCI DSS	Requirement 1 (Firewall), Requirement 2 (Network segmentation)	Hierarchical Firewalls and VPC segmentation provide the necessary network controls to protect the Cardholder Data Environment (CDE).
HIPAA	§ 164.312(e) (Transmission security)	Cloud Interconnect provides a private, secure, and encrypted connection for Protected Health Information (PHI) transmission.
GDPR	Article 32 (Network security)	The data perimeter enforced by VPC Service Controls and robust network security controls protect personal data from unauthorized processing.
SOC 2	CC6.6 (Network security)	The comprehensive security controls, monitoring, and logging capabilities support the Trust Services Criteria for Security.

4. Prerequisites

Successful deployment of this hybrid connectivity solution requires specific accounts, tools, and configurations to be in place both in GCP and on-premises.

1. **GCP Project:** A dedicated GCP project (e.g., `PRJ-GCP-NET-090`) must be created with billing enabled.
2. **GCP CLI:** The `gcloud` command-line tool must be installed, configured, and authenticated with the correct user credentials.
3. **Required APIs:** The following GCP APIs must be enabled in the target project:
    - Compute Engine API (`compute.googleapis.com`)
    - Cloud Interconnect API (`cloudinterconnect.googleapis.com`)

    - Cloud IDS API (`cloudids.googleapis.com`)
    - Cloud Armor API (`containersecurity.googleapis.com`)
    - Network Management API (`networkmanagement.googleapis.com`)
4. **On-Premises Setup:**
    - A physical router capable of Border Gateway Protocol (BGP) for dynamic route exchange.
    - A colocation facility or a partner connection point for the physical Cloud Interconnect connection.
5. **Permissions:** The deploying user or service account must have IAM roles with permissions to create and manage:
    - VPC networks and subnets
    - Cloud Routers and Cloud Interconnect connections
    - VPC Service Controls perimeters (requires Access Context Manager Admin roles)
    - Cloud Armor and Cloud IDS policies and endpoints.

5. Architecture Overview

The architecture is a classic hub-and-spoke model where the GCP VPC acts as the hub, securely connected to the on-premises data center.

The central element is the **VPC Network (`vpc-net-hybrid`)**, which hosts all cloud resources and is configured with custom subnets for segmentation (e.g., `subnet-general` and `subnet-sensitive`).

The **Cloud Interconnect** provides the dedicated, private link to the on-premises network, managed by a **Cloud Router** that uses BGP to dynamically exchange routes, ensuring seamless traffic flow.

Security is layered:

- **Cloud Armor** sits at the edge, protecting internet-facing services (e.g., those behind a Load Balancer) from DDoS and WAF threats.
- **VPC Service Controls** establish a secure perimeter around sensitive services (like Cloud Storage and BigQuery), preventing unauthorized access and data

exfiltration, even from compromised identities.

- **Cloud IDS** is deployed within the VPC to inspect internal and hybrid traffic for known threats and intrusions, providing deep packet inspection capabilities.
- **Hierarchical Firewall Policies** (or standard VPC firewall rules) enforce network segmentation and control traffic flow between subnets and the on-premises network.

This layered approach ensures that security is enforced at the network edge, the service layer, and within the network traffic itself.

6. Step-by-Step Implementation

This section provides the detailed, step-by-step instructions using the `gcloud` command-line tool for deploying the core components of the secure hybrid network.

6.1: Configure Project and Enable APIs

First, set the project context and ensure all necessary APIs are enabled.

```
# Set the project ID
export PROJECT_ID="PRJ-GCP-NET-090"
gcloud config set project $PROJECT_ID

# Enable required APIs: Compute, Interconnect, IDS, Cloud Armor, and Network Management
gcloud services enable compute.googleapis.com \
    cloudinterconnect.googleapis.com \
    cloudids.googleapis.com \
    containersecurity.googleapis.com \
    networkmanagement.googleapis.com
```

6.2: Create VPC Network and Subnets

A custom VPC network is created with global routing, followed by the creation of two segmented subnets for different security requirements.

```
# Create the VPC network with custom subnet mode and global BGP routing
gcloud compute networks create vpc-net-hybrid \
    --subnet-mode=custom \
    --bgp-routing-mode=global

# Create Subnet A (General Resources) in us-central1
gcloud compute networks subnets create subnet-general \
    --network=vpc-net-hybrid \
    --region=us-central1 \
    --range=10.10.0.0/24 \
    --enable-private-ip-google-access

# Create Subnet B (Sensitive Data) in us-central1
gcloud compute networks subnets create subnet-sensitive \
    --network=vpc-net-hybrid \
    --region=us-central1 \
    --range=10.10.1.0/24 \
    --enable-private-ip-google-access
```

6.3: Provision Cloud Interconnect and Cloud Router

This step involves creating the Cloud Router, which manages the BGP session with the on-premises router, and the VLAN attachment that connects to the physical Cloud Interconnect circuit.

```
# Create a Cloud Router in the VPC network
# The ASN 64512 is a private ASN commonly used for this purpose.
gcloud compute routers create router-hybrid \
    --network=vpc-net-hybrid \
    --region=us-central1 \
    --asn=64512

# Create a VLAN attachment (Placeholder - requires a provisioned
Interconnect connection)
# NOTE: The actual command requires the name of your provisioned
Interconnect connection.
# The candidate-subnets range is the link-local IP range for the BGP
session.
# gcloud compute interconnects attachments create vlan-attach-onprem \
#     --router=router-hybrid \
#     --region=us-central1 \
#     --interconnect=your-interconnect-name \
#     --candidate-subnets=169.254.1.0/29 \
#     --vlan-tag=1000
```

Important: In a production environment, the physical Cloud Interconnect circuit must be ordered and provisioned before this step. The commands above assume a Dedicated Interconnect. For Partner Interconnect, the process involves a service provider.

6.4: Implement VPC Service Controls Perimeter

Establish a service perimeter to protect sensitive GCP services from unauthorized access and data exfiltration. This requires an existing Access Policy.

```
# Create a service perimeter (replace with your organization ID and Access
Policy ID)
# This perimeter restricts access to Cloud Storage and BigQuery.
gcloud access-context-manager perimeters create perimeter-hybrid-security \
    --title="Hybrid Security Perimeter" \
    --resources="projects/$PROJECT_ID" \
    --restricted-services="storage.googleapis.com, bigquery.googleapis.com"
\
    --perimeter-type=regular
```

6.5: Deploy Cloud Armor Policy (DDoS and WAF)

Create a Cloud Armor security policy to protect internet-facing applications from common web exploits and DDoS attacks. This policy is typically attached to a global external HTTP(S) Load Balancer.

```
# Create a Cloud Armor security policy
gcloud compute security-policies create policy-cloud-armor \
    --description="DDoS and WAF protection for hybrid services"

# Add a rule to block common SQL injection attacks (WAF rule)
gcloud compute security-policies rules create 1000 \
    --security-policy=policy-cloud-armor \
    --expression="request.path.matches('/admin') &&
evaluatePreconfiguredExpr('sqli-canary')" \
    --action=deny-403 \
    --description="Block SQLi attempts" \
    --priority=1000

# Add a rule to allow traffic from the on-premises network (assuming
192.168.1.0/24 is advertised)
gcloud compute security-policies rules create 10 \
    --security-policy=policy-cloud-armor \
    --src-ip-ranges="192.168.1.0/24" \
    --action=allow \
    --description="Allow On-Premises Traffic" \
    --priority=10
```

6.6: Deploy Cloud IDS Endpoint

Deploy a Cloud IDS endpoint to monitor network traffic for threats and intrusions.

```
# Create a dedicated subnet for the Cloud IDS endpoint
# This subnet must use the purpose=INTERNAL_HTTPS_LOAD_BALANCER flag.
gcloud compute networks subnets create subnet-ids \
    --network=vpc-net-hybrid \
    --region=us-central1 \
    --range=10.10.2.0/29 \
    --purpose=INTERNAL_HTTPS_LOAD_BALANCER

# Create the Cloud IDS endpoint
gcloud ids endpoints create ids-endpoint-hybrid \
    --network=vpc-net-hybrid \
    --zone=us-central1-a \
    --severity=INFORMATIONAL \
    --async
```

6.7: Configure Firewall Policies

While Hierarchical Firewall Policies are recommended for organization-wide consistency, the following standard VPC firewall rules are used for project-level demonstration to enforce basic network segmentation and egress control.

```
# Allow all internal VPC traffic (for communication between subnets)
gcloud compute firewall-rules create allow-internal-hybrid \
    --network=vpc-net-hybrid \
    --action=ALLOW \
    --direction=INGRESS \
    --rules=all \
    --source-ranges=10.10.0.0/16 \
    --priority=1000 \
    --description="Allow all internal VPC traffic"

# Deny all egress to the internet by default (Zero Trust principle)
# This forces resources to use Private Google Access or a controlled NAT
gateway.
gcloud compute firewall-rules create deny-all-egress-to-internet \
    --network=vpc-net-hybrid \
    --action=DENY \
    --direction=EGRESS \
    --rules=all \
    --destination-ranges=0.0.0.0/0 \
    --priority=65534 \
    --description="Deny all egress to the internet by default"
```

6.8: Infrastructure as Code (IaC) with Terraform

For production environments, it is highly recommended to manage this infrastructure using **Terraform**. This ensures version control, repeatability, and state management. The following snippets illustrate the Terraform configuration for the core components.

```
 # VPC Network and Subnets
resource "google_compute_network" "vpc_net_hybrid" {
  name                    = "vpc-net-hybrid"
  auto_create_subnetworks = false
  routing_mode            = "GLOBAL"
}

resource "google_compute_subnetwork" "subnet_general" {
  name          = "subnet-general"
  ip_cidr_range = "10.10.0.0/24"
  region        = "us-central1"
  network       = google_compute_network.vpc_net_hybrid.self_link
  private_ip_google_access = true
}

# VPC Service Controls Perimeter
resource "google_access_context_manager_service_perimeter"
"perimeter_hybrid_security" {
  # Note: The parent and name fields require an existing Access Policy ID
  parent = "accessPolicies/YOUR_ACCESS_POLICY_ID"
  name   =
"accessPolicies/YOUR_ACCESS_POLICY_ID/servicePerimeters/perimeter_hybrid_security
  title  = "Hybrid Security Perimeter"
  status {
    restricted_services = [
      "storage.googleapis.com",
      "bigquery.googleapis.com",
    ]
    resources = [
      "projects/${var.project_id}",
    ]
  }
}

# Cloud Armor Policy
resource "google_compute_security_policy" "policy_cloud_armor" {
  name        = "policy-cloud-armor"
  description = "DDoS and WAF protection for hybrid services"
}

# Cloud IDS Endpoint
resource "google_ids_endpoint" "ids_endpoint_hybrid" {
  name    = "ids-endpoint-hybrid"
  project = var.project_id
  location = "us-central1"
  network = google_compute_network.vpc_net_hybrid.self_link
```

```
  severity = "INFORMATIONAL"
}
```

7. Validation & Testing

After deployment, a rigorous validation process is essential to confirm that both connectivity and the security controls are functioning as intended.

7.1. Connectivity Test

Verify the BGP session status and end-to-end network reachability to the on-premises network.

```
# Check BGP session status on the Cloud Router (should show 'UP')
gcloud compute routers get-status router-hybrid --region=us-central1

# Test connectivity from a VM in subnet-general to an on-premises IP
# Replace 'vm-instance-name' and '192.168.1.1' with actual values.
# gcloud compute ssh vm-instance-name --command "ping -c 3 192.168.1.1"
```

Successful BGP status and a successful ping confirm that the Cloud Interconnect and Cloud Router are correctly configured and routing traffic.

7.2. Security Control Validation

Validate the effectiveness of the deployed security services by attempting to violate the established policies.

Security Control	Validation Test	Expected Result
VPC Service Controls	Attempt to copy data from a protected Cloud Storage bucket to an external, unprotected location (e.g., a bucket in a different project outside the perimeter).	The operation must fail with a `PERMISSION_DENIED` error, confirming the data perimeter is active.
Cloud Armor	Send a request containing a known SQL injection payload (e.g., `' OR 1=1 --`) to a service protected by the `policy-cloud-armor`.	The request must be blocked by the WAF rule, returning a `403 Forbidden` response.
Cloud IDS	Generate suspicious network traffic (e.g., a port scan or known malware signature traffic) from a test VM within the VPC.	Alerts must be generated and visible in the Cloud IDS logs, confirming the intrusion detection system is actively monitoring traffic.
Egress Firewall	Attempt to ping an external IP address (e.g., 8.8.8.8) from a VM in the VPC.	The connection must time out or be explicitly denied due to the `deny-all-egress-to-internet` firewall rule.

8. Troubleshooting

Common issues encountered during the deployment and operation of a secure hybrid network, along with their resolutions.

Issue	Potential Cause	Resolution
No BGP Session	Incorrect ASN or IP configuration on the on-premises router or Cloud Router.	Verify the BGP peer IP and ASN are correctly configured on both sides. Use `gcloud compute routers get-status router-hybrid` to check the Cloud Router state and ensure the VLAN attachment is provisioned.
Traffic Blocked	Overly restrictive firewall or Cloud Armor policy.	Check **VPC Flow Logs** and **Cloud Armor logs** to identify the blocking rule. Adjust the priority or source/destination ranges of the firewall rules or security policy rules.
Data Exfiltration	VPC Service Controls perimeter is misconfigured or a sensitive service is not included.	Verify that all sensitive services are listed in the `restricted-services` of the perimeter. Check the **Access Context Manager logs** for violations and ensure all necessary projects are included in the perimeter's resources.
Cloud IDS Not Alerting	Incorrect traffic mirroring configuration or severity level set too high.	Ensure the traffic mirroring policy is correctly configured to send traffic to the IDS endpoint. Check the endpoint's severity level and adjust it to `INFORMATIONAL` or lower during initial testing.

9. Cost Optimization

Optimizing costs is crucial for maintaining the long-term financial viability of the hybrid cloud architecture.

1. **Cloud Interconnect Selection:** Carefully choose between **Partner Interconnect** and **Dedicated Interconnect** based on required bandwidth and availability. Dedicated Interconnect offers better cost efficiency at high volumes (10 Gbps or 100 Gbps ports), while Partner Interconnect is suitable for lower bandwidth needs or faster provisioning.
2. **Cloud IDS Logging:** Set the severity level for the Cloud IDS endpoint to **INFORMATIONAL** or higher to reduce the volume of logs and processing costs, focusing only on critical and high-severity threats.
3. **VPC Flow Logs Filtering:** Implement log filtering to only capture metadata or specific traffic flows (e.g., rejected connections) instead of all traffic. This

significantly reduces storage and analysis costs in Cloud Logging and any downstream SIEM.

4. **Resource Sizing:** Continuously monitor and right-size all Compute Engine and Cloud SQL instances to match actual workload requirements, leveraging committed use discounts (CUDs) for stable workloads.
5. **Network Tiers:** Utilize the **Standard Network Tier** for non-critical, lower-performance traffic to save on egress costs, reserving the **Premium Network Tier** for high-performance, latency-sensitive applications.

10. Security Best Practices

Beyond the initial deployment, continuous adherence to security best practices is necessary to maintain a hardened and compliant environment.

1. **Principle of Least Privilege (PoLP):** Enforce PoLP across all layers. Use IAM roles with the minimum necessary permissions for all service accounts and users. Avoid using primitive roles (Owner, Editor, Viewer) in production.
2. **Security Policy Management:** Regularly review and update Cloud Armor and firewall policies. Use the **Network Intelligence Center** for continuous monitoring of network configuration and to detect unintended changes or security policy drift.
3. **Data Encryption:** Ensure all data at rest (e.g., Cloud Storage, Cloud SQL) is encrypted with **Customer-Managed Encryption Keys (CMEK)**, providing greater control over the encryption lifecycle.
4. **Patch Management:** Implement automated patching and vulnerability scanning for all Compute Engine instances in the VPC to minimize the attack surface.
5. **Logging and Monitoring:**
    - Enable **VPC Flow Logs** for all subnets and export them to a centralized Security Information and Event Management (SIEM) system for real-time analysis and long-term retention.
    - Configure **Cloud Audit Logs** to track administrative activities and data access, ensuring a complete audit trail for compliance.
6. **Network Segmentation:** Maintain strict network segmentation between different environments (e.g., Production, Staging, Development) and between

different security zones (e.g., General vs. Sensitive subnets) using firewall rules.

11. Cleanup

To completely remove all resources created by this deployment and avoid incurring further costs, execute the following cleanup commands in reverse order of creation.

```
# Set the project ID
export PROJECT_ID="PRJ-GCP-NET-090"
gcloud config set project $PROJECT_ID

# 1. Delete Cloud IDS Endpoint
gcloud ids endpoints delete ids-endpoint-hybrid --zone=us-central1-a

# 2. Delete Cloud Armor Policy
gcloud compute security-policies delete policy-cloud-armor

# 3. Delete VPC Service Controls Perimeter (replace with your access policy
ID)
# gcloud access-context-manager perimeters delete perimeter-hybrid-security
--policy=YOUR_ACCESS_POLICY_ID

# 4. Delete VLAN Attachment (if created)
# gcloud compute interconnects attachments delete vlan-attach-onprem --
region=us-central1

# 5. Delete Cloud Router
gcloud compute routers delete router-hybrid --region=us-central1

# 6. Delete Firewall Rules
gcloud compute firewall-rules delete allow-internal-hybrid deny-all-egress-
to-internet

# 7. Delete Subnets (must be deleted before the network)
gcloud compute networks subnets delete subnet-general subnet-sensitive
subnet-ids --region=us-central1

# 8. Delete VPC Network
gcloud compute networks delete vpc-net-hybrid
```

This guide provides a comprehensive framework for deploying a secure, compliant, and high-performance hybrid network on Google Cloud Platform. The integration of

Cloud Interconnect with native security services like VPC Service Controls, Cloud Armor, and Cloud IDS ensures a production-ready solution for modern enterprise needs.