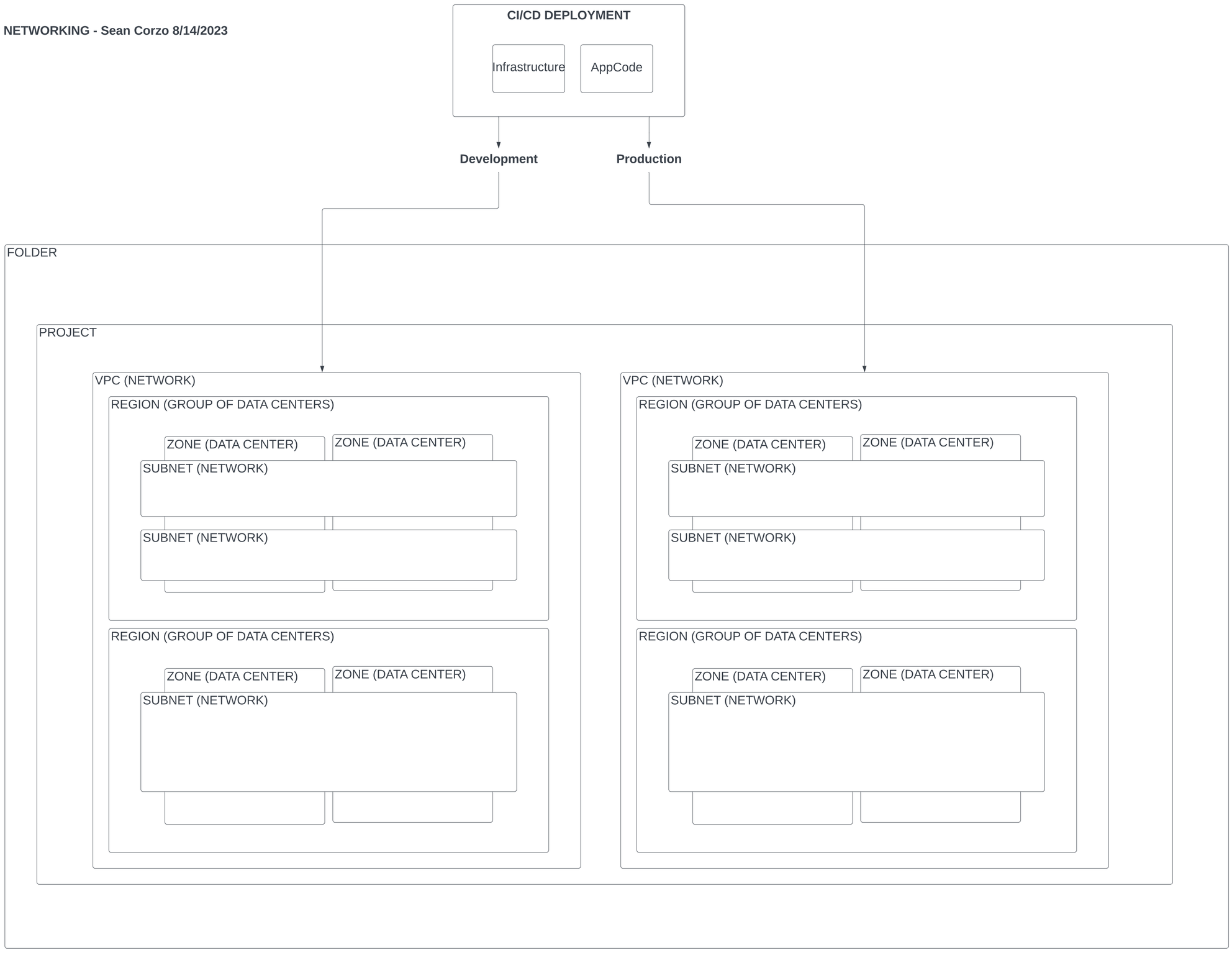
GCP CLOUD NETWORKING - Sean Corzo 8/14/2023



SUBNETS ARE ATTACHED TO VPCs AND ARE LIMITED TO SINGLE REGIONS

- Subnets are networks attached to the parent VPC Network

- Subnets: Even though subnets are attached to the VPC, they are regional resources (so cannot span multiple regions)

- You can have multiple subnets within the same region

SUBNETS CAN SEE OTHER SUBNETS

- uses ROUTING TABLE ENTRIES that exist at VPC Network Level

- a route consists of a single *destination* prefix in CIDR format and a single *next hop*.

Subnet to Subnet Routes: These are automatically created (every time you add a new subnet). There is no way to modify these routes.

REGION TO REGION MANAGED SERVICES

Most Region to Region communication between GCP managed services will require an internal load balancer.

FIREWALL

- Rules exist at VPC Network Level

VPC PEERING

For two VPCs to communicate, we need to add VPC peering

VPC Peering is not transitive meaning that if you peer network A with B and B with C, A cannot see C

Shared VPC: provides flexibility by allowing multiple projects to leverage a central VPC where connectivity can be controlled and centrally managed.

HYBRID CONNECTIVITY

ON PREM OR MULTI-CLOUD GATEWAY OPTIONS

1) use Cloud VPN (secure over public internet)
2) use Cloud Interconnect (secure over dedicated connection)

.

PRIVATE SERVICE CONNECT

By default, when you use GCP managed services (like Cloud Storage, Cloud SQL, or other services) from your applications or resources within your Virtual Private Cloud (VPC), the communication goes through the public internet.

If you need to securely access specific Google Cloud managed services or third-party services outside your VPC environment, **Private Service Connect** is the appropriate choice.

1) enable the API
2) create a VPC
3) Enable Private Google Access (Optional)
4) Activate PSC on the service itself:
   - enable it
   - set some authorization preferences (IAM)