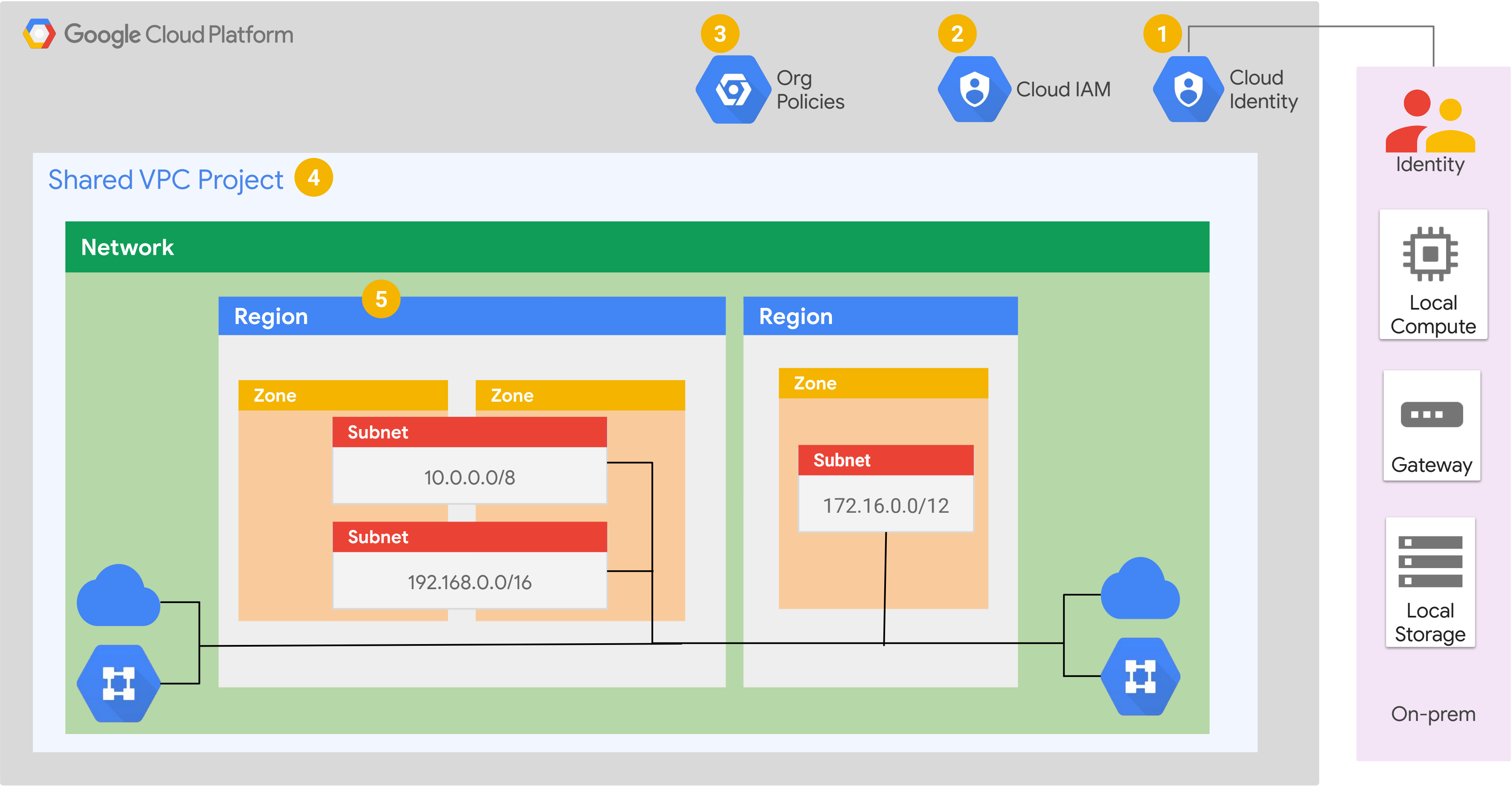
High Level Security Model

Google Cloud

Accounts, Access, and Identification

1. Use +Google Cloud Identity to establish unified Identity with on-prem
2. Create roles with least privilege access through +Cloud IAM
3. Establish +Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage +Shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets

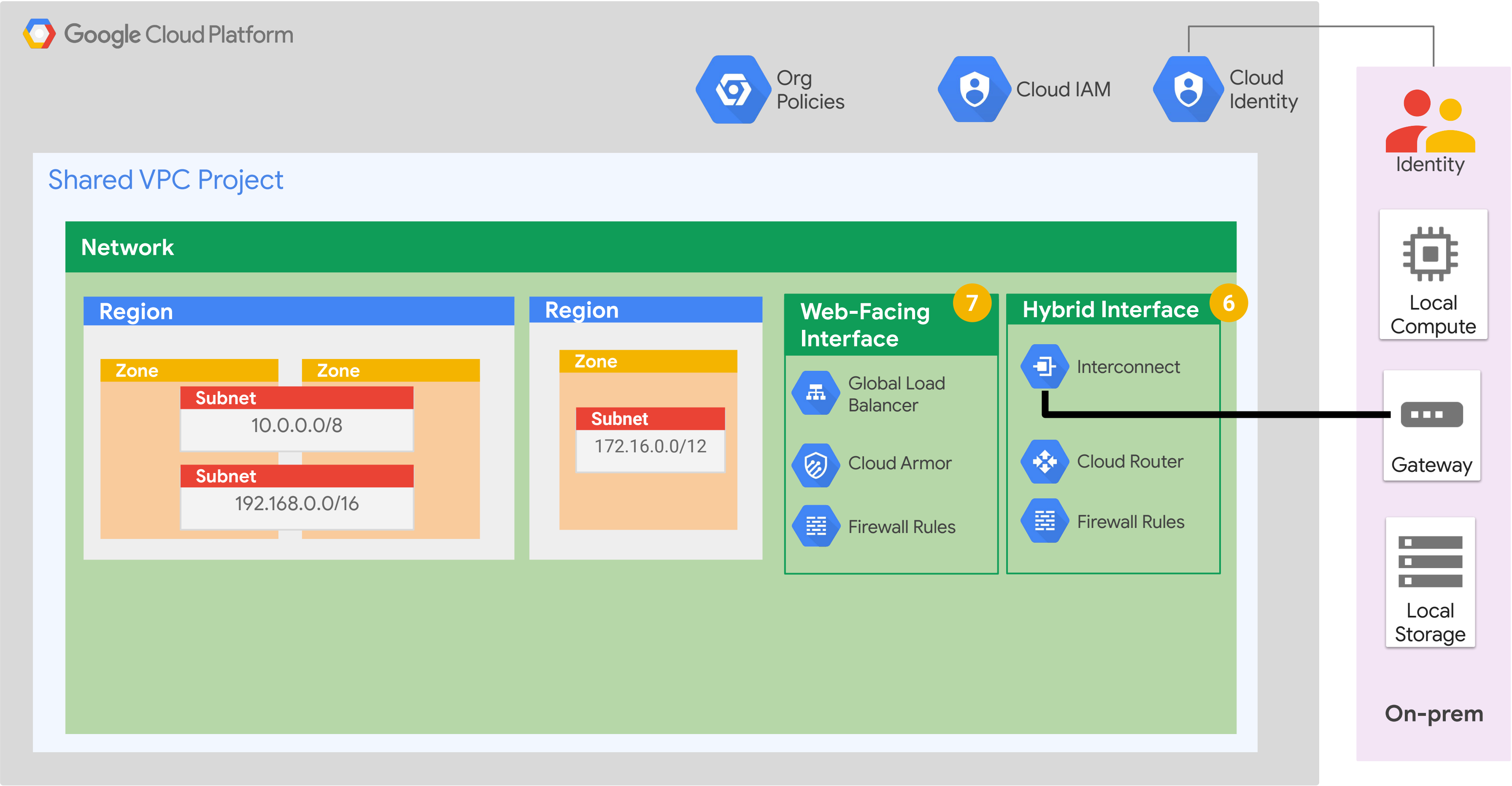
+FedRAMP Moderate Product
** FedRAMP High Product*


Google Cloud Platform
3
Org Policies
2
Cloud IAM
1
Cloud Identity
Shared VPC Project
4
Network
Region
5
Region
Zone
Zone
Zone
Subnet
10.0.0.0/8
Subnet
192.168.0.0/16
Subnet
172.16.0.0/12
Identity
Local Compute
Gateway
Local Storage
On-prem

Network Security

6. Use [+]Cloud Interconnect or [+]Cloud VPN, along with Cloud Router, to establish a hybrid connectivity to on-prem
7. Secure application infrastructure against DDoS and external threats with [+]Cloud Load Balancer, [+]Cloud Armor & [+]Firewalls

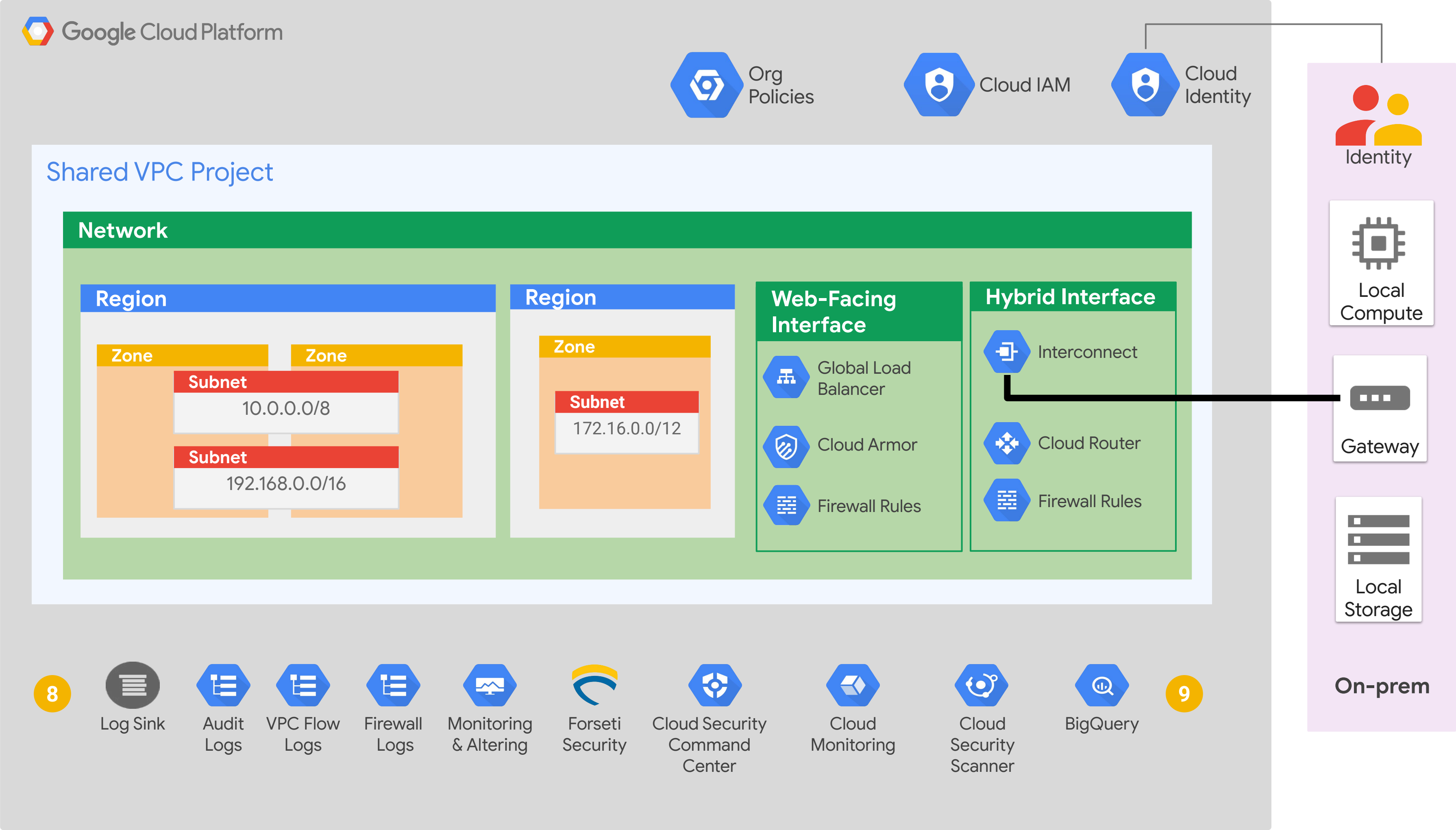
[+]FedRAMP Moderate Product
** FedRAMP High Product*


Google Cloud Platform
Org Policies
Cloud IAM
Cloud Identity
Shared VPC Project
Network
Region
Zone
Zone
Subnet
10.0.0.0/8
Subnet
192.168.0.0/16
Region
Zone
Subnet
172.16.0.0/12
Web-Facing Interface
7
Global Load Balancer
Cloud Armor
Firewall Rules
Hybrid Interface
6
Interconnect
Cloud Router
Firewall Rules
Identity
Local Compute
Gateway
Local Storage
On-prem

Logging, Monitoring and Alerting

8. Leverage +Log Sink to collect logs from +Cloud Audit Logs, +VPC Flow Logs, and +Firewall logs
9. Monitor environment with Cloud Native tools like +Cloud Operations Suite, Cloud Security Command Center, +Cloud Security Scanner, Forseti, and *BigQuery

+FedRAMP Moderate Product
** FedRAMP High Product*

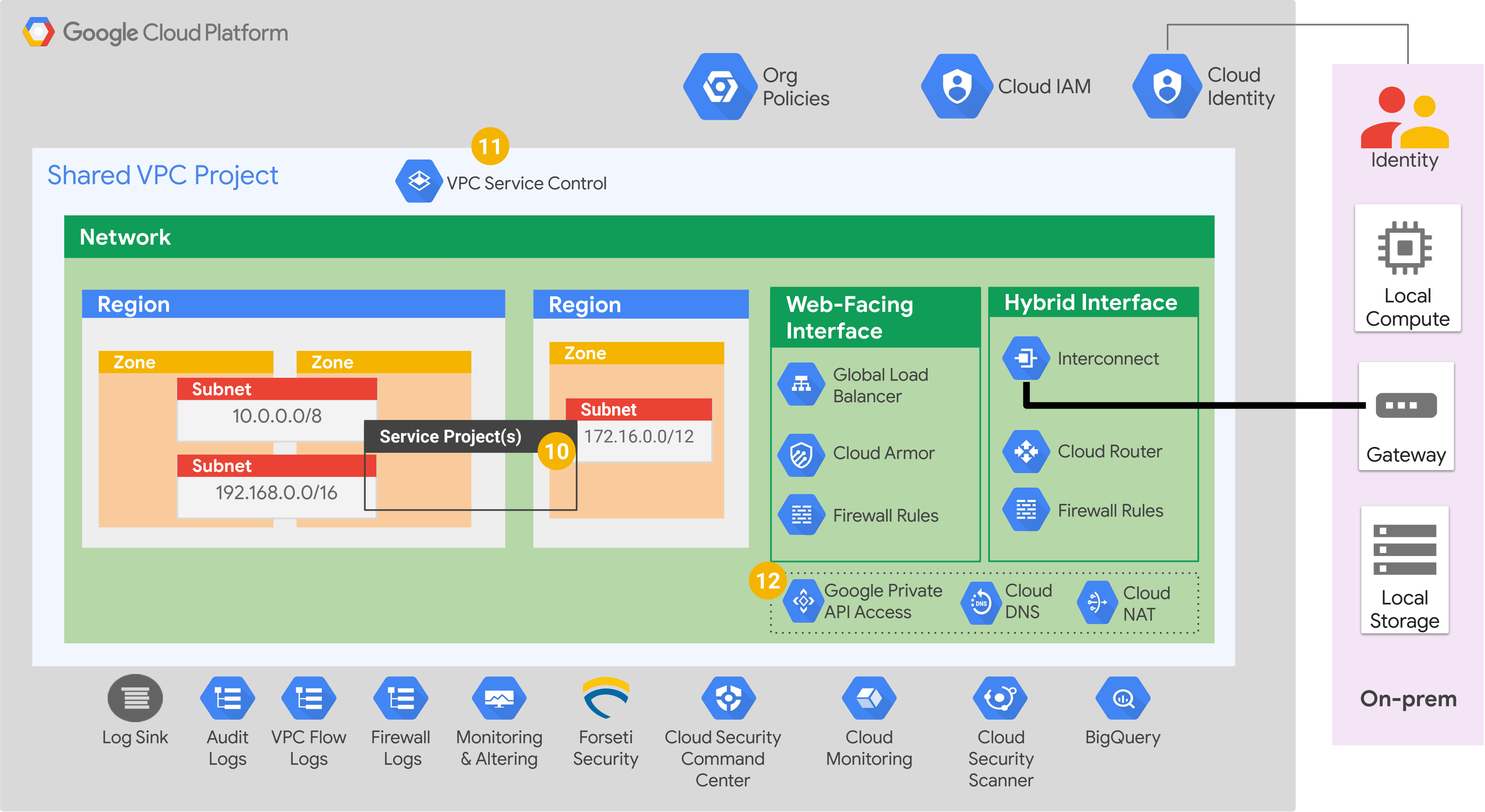

Google Cloud Platform
Org Policies
Cloud IAM
Cloud Identity
Shared VPC Project
Network
Region
Zone
Zone
Subnet
10.0.0.0/8
Subnet
192.168.0.0/16
Region
Zone
Subnet
172.16.0.0/12
Web-Facing Interface
Global Load Balancer
Cloud Armor
Firewall Rules
Hybrid Interface
Interconnect
Cloud Router
Firewall Rules
8
Log Sink
Audit Logs
VPC Flow Logs
Firewall Logs
Monitoring & Altering
Forseti Security
Cloud Security Command Center
Cloud Monitoring
Cloud Security Scanner
BigQuery
9
Identity
Local Compute
Gateway
Local Storage
On-prem

Securing Services

10. Create a Shared VPC +Service Project to host workloads
11. Create security perimeter with +VPC Service Controls
12. Access GCP services and the Internet through +GCP private access, +Cloud DNS, and Cloud NAT

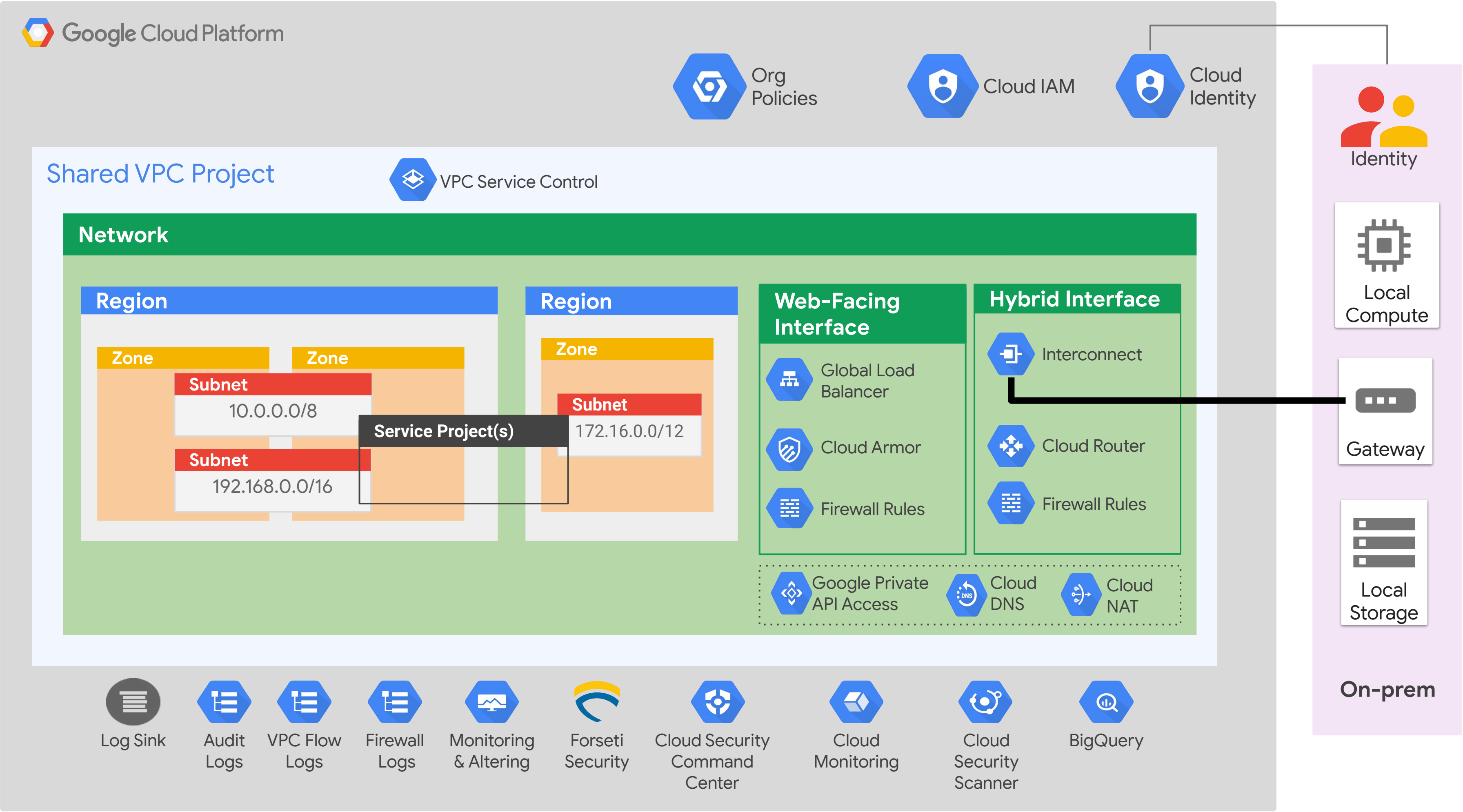
+FedRAMP Moderate Product

** FedRAMP High Product*


Google Cloud Platform
Org Policies
Cloud IAM
Cloud Identity
Shared VPC Project
11
VPC Service Control
Network
Region
Zone
Zone
Subnet
10.0.0.0/8
Subnet
192.168.0.0/16
Service Project(s)
10
Region
Zone
Subnet
172.16.0.0/12
Web-Facing Interface
Global Load Balancer
Cloud Armor
Firewall Rules
Hybrid Interface
Interconnect
Cloud Router
Firewall Rules
12
Google Private API Access
Cloud DNS
Cloud NAT
Log Sink
Audit Logs
VPC Flow Logs
Firewall Logs
Monitoring & Altering
Forseti Security
Cloud Security Command Center
Cloud Monitoring
Cloud Security Scanner
BigQuery
Identity
Local Compute
Gateway
Local Storage
On-prem

Putting it all together

Google Cloud


Google Cloud Platform
Org Policies
Cloud IAM
Cloud Identity
Shared VPC Project
VPC Service Control
Network
Region
Zone
Zone
Subnet
10.0.0.0/8
Subnet
192.168.0.0/16
Service Project(s)
Region
Zone
Subnet
172.16.0.0/12
Web-Facing Interface
Global Load Balancer
Cloud Armor
Firewall Rules
Hybrid Interface
Interconnect
Cloud Router
Firewall Rules
Google Private API Access
Cloud DNS
Cloud NAT
Log Sink
Audit Logs
VPC Flow Logs
Firewall Logs
Monitoring & Altering
Forseti Security
Cloud Security Command Center
Cloud Monitoring
Cloud Security Scanner
BigQuery
Identity
Local Compute
Gateway
Local Storage
On-prem