Google Cloud Network Configuration Analysis Report

Introduction

This report provides a comprehensive analysis of your Google Cloud network configuration, focusing on Virtual Private Clouds (VPCs), firewall rules, subnets, and VPN connectivity. It aims to identify potential areas for improvement by comparing your current setup against Google Cloud's best practices.

The report is structured as follows:

- **Network Configuration:** Details of your existing VPCs, firewall rules, subnets, and VPN connections.
- **Best Practices:** A summary of Google Cloud's recommended best practices for VPC and VPN configuration.
- **Analysis:** Evaluation of your current configuration in light of the best practices.

Network Configuration

This section presents the details of your current network configuration.

VPCs

```
---

Network name: vpc-roma-internal-hub Auto create subnetworks: False Network creation timestamp: 2024-09-12T09:33:50.505-07:00 Network description: Network Enable ULA Internal IPv6: False Network Firewall Policy: Network Gateway: Network Ipv4 Range: Network id: 3529097084580833537 Network Internal IPv6 range: Network kind: compute#network Network MTU: 0 Network Firewall Policy enforcer: AFTER_CLASSIC_FIREWALL Network Peerings: [] Network Routing config: routing_mode: "GLOBAL"

**********

Network name: vpc-roma-hub Auto create subnetworks: False Network creation timestamp: 2024-08-15T13:38:23.969-07:00 Network description: Network Enable ULA Internal IPv6: False Network Firewall Policy: Network Gateway: Network Ipv4 Range: Network id: 8688276164912077264 Network Internal IPv6 range: Network kind: compute#network Network MTU: 0 Network Firewall Policy enforcer: AFTER_CLASSIC_FIREWALL Network Peerings: [] Network Routing config: routing_mode: "GLOBAL"

**********

Network name: vpc-castilla-host Auto create subnetworks: False Network creation timestamp: 2024-08-15T13:38:24.034-07:00 Network description: Network Enable ULA Internal IPv6: False Network Firewall Policy: Network Gateway: Network Ipv4 Range: Network id: 8520995310516033967 Network Internal IPv6 range: Network kind: compute#network Network MTU: 0 Network Firewall Policy enforcer: AFTER_CLASSIC_FIREWALL Network Peerings: [] Network Routing config: routing_mode: "GLOBAL"

**********

Network name: vpc-parkway-host Auto create subnetworks: False Network creation timestamp: 2024-08-15T13:38:23.949-07:00 Network description: Network Enable ULA Internal IPv6: False Network Firewall Policy: Network Gateway: Network Ipv4 Range: Network id: 5204173912435579344 Network Internal IPv6 range: Network kind: compute#network Network MTU: 0 Network Firewall Policy enforcer: AFTER_CLASSIC_FIREWALL Network Peerings: [name: "servicenetworking-googleapis-com" import_subnet_routes_with_public_ip: false exchange_subnet_routes: true auto_create_routes: true export_custom_routes: false state_details: "[2024-08-19T14:55:02.265-07:00]: Connected." export_subnet_routes_with_public_ip: false state: "ACTIVE" import_custom_routes: false network: "https://www.googleapis.com/compute/v1/projects/qce2bb90f98bcbc47p-tp/global/networks/servicenetworking" stack_type: "IPV4_ONLY" ] Network Routing config: routing_mode: "GLOBAL"

**********

Network name: vpc-roma-host Auto create subnetworks: False Network creation timestamp: 2024-08-15T13:38:24.161-07:00 Network description: Network Enable ULA Internal IPv6: False Network Firewall Policy: Network Gateway: Network Ipv4 Range: Network id: 8038129295821101487 Network Internal IPv6 range: Network kind: compute#network Network MTU: 0 Network Firewall Policy enforcer: AFTER_CLASSIC_FIREWALL Network Peerings: [] Network Routing config: routing_mode: "GLOBAL"

**********

Network name: vpc-salitre-host Auto create subnetworks: False Network creation timestamp: 2024-08-15T13:38:23.926-07:00 Network description: Network Enable ULA Internal IPv6: False Network Firewall Policy: Network Gateway: Network Ipv4 Range: Network id: 6344913773099473360 Network Internal IPv6 range: Network kind: compute#network Network MTU: 0 Network Firewall Policy enforcer: AFTER_CLASSIC_FIREWALL Network Peerings: [] Network Routing config: routing_mode: "GLOBAL"
```

Network name: lb-network-crs-reg Auto create subnetworks: False Network creation timestamp: 2024-10-01T10:30:48.557-07:00 Network description: Network Enable ULA Internal IPv6: False Network Firewall Policy: Network Gateway: Network Ipv4 Range: Network id: 8193351776134598439 Network Internal IPv6 range: Network kind: compute#network Network MTU: 0 Network Firewall Policy enforcer: AFTER_CLASSIC_FIREWALL Network Peerings: [] Network Routing config: routing_mode: "REGIONAL"

```

### Firewall Rules

```

Firewall rule id: 3217293522729056423 Firewall rule name: deny-all Firewall rule description: Firewall rule priority: 999 Firewall rule source ranges: ['0.0.0.0/0'] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/roma-hub-project/global/networks/vpc-roma-hub Firewall rule target tags: [] Firewall rule target service accounts: [] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

Firewall rule id: 8205348981296712063 Firewall rule name: deny-all2 Firewall rule description: Firewall rule priority: 65535 Firewall rule source ranges: ['0.0.0.0/0'] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/roma-hub-project/global/networks/vpc-roma-hub Firewall rule target tags: [] Firewall rule target service accounts: [] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

Firewall rule id: 7185493328820816158 Firewall rule name: gsquare-fw Firewall rule description: Firewall rule priority: 1000 Firewall rule source ranges: [] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/roma-hub-project/global/networks/vpc-roma-hub Firewall rule target tags: ['gsqaure-noprod'] Firewall rule target service accounts: [] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

Firewall rule id: 715227665512627571 Firewall rule name: allow-all Firewall rule description: Firewall rule priority: 1000 Firewall rule source ranges: ['0.0.0.0/0'] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/castilla-host-project1/global/networks/vpc-castilla-host Firewall rule target tags: [] Firewall rule target service accounts: [] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

Firewall rule id: 8065382121770083712 Firewall rule name: castilla-back-dr-43224-firewall-rule Firewall rule description: Firewall rule priority: 1000 Firewall rule source ranges: ['0.0.0.0/0'] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/castilla-host-project1/global/networks/vpc-castilla-host Firewall rule target tags: [] Firewall rule target service accounts: ['castilla-back-dr-43224@castilla-lived.iam.gserviceaccount.com'] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

Firewall rule id: 1626850528675668945 Firewall rule name: gke-us-central1-castilla-small--9f7441e3-gke-abafa77e-all Firewall rule description: Firewall rule priority: 1000 Firewall rule source ranges: ['100.65.0.0/17'] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/castilla-host-project1/global/networks/vpc-castilla-host Firewall rule target tags: ['gke-us-central1-castilla-small--9f7441e3-gke-abafa77e-node'] Firewall rule target service accounts: [] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

Firewall rule id: 1436606086170715089 Firewall rule name: gke-us-central1-castilla-small--9f7441e3-gke-abafa77e-exkubelet Firewall rule description: Firewall rule priority: 1000 Firewall rule source ranges: ['0.0.0.0/0'] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/castilla-host-project1/global/networks/vpc-castilla-host Firewall rule target tags: ['gke-us-central1-castilla-small--9f7441e3-gke-abafa77e-node'] Firewall rule target service accounts: [] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

Firewall rule id: 2334231844190331857 Firewall rule name: gke-us-central1-castilla-small--9f7441e3-gke-abafa77e-inkubelet Firewall rule description: Firewall rule priority: 999 Firewall rule source ranges: ['100.65.0.0/17'] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/castilla-host-project1/global/networks/vpc-castilla-host Firewall rule target tags: ['gke-us-central1-castilla-small--9f7441e3-gke-abafa77e-node'] Firewall rule target service accounts: [] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

Firewall rule id: 4877858948878607313 Firewall rule name: gke-us-central1-castilla-small--9f7441e3-gke-abafa77e-vms Firewall rule

description: Firewall rule priority: 1000 Firewall rule source ranges: ['10.0.43.0/24'] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/castilla-host-project1/global/networks/vpc-castilla-host Firewall rule target tags: ['gke-us-central1-castilla-small--9f7441e3-gke-abafa77e-node'] Firewall rule target service accounts: [] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

Firewall rule id: 7841565698002994616 Firewall rule name: allow-icmp Firewall rule description: Firewall rule priority: 1000 Firewall rule source ranges: ['0.0.0.0/0'] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/parway-host-project1/global/networks/vpc-parkway-host Firewall rule target tags: [] Firewall rule target service accounts: [] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

Firewall rule id: 6668319965771087571 Firewall rule name: allow-icmp Firewall rule description: Firewall rule priority: 999 Firewall rule source ranges: ['0.0.0.0/0'] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/roma-host-project1/global/networks/vpc-roma-host Firewall rule target tags: [] Firewall rule target service accounts: [] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

Firewall rule id: 7482904111670507657 Firewall rule name: deny-all Firewall rule description: Firewall rule priority: 1000 Firewall rule source ranges: ['0.0.0.0/0'] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/roma-host-project1/global/networks/vpc-roma-host Firewall rule target tags: [] Firewall rule target service accounts: [] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

Firewall rule id: 3951965502824146267 Firewall rule name: allow-all Firewall rule description: Firewall rule priority: 1000 Firewall rule source ranges: ['0.0.0.0/0'] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/salitre-host-project1/global/networks/vpc-salitre-host Firewall rule target tags: [] Firewall rule target service accounts: [] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

Firewall rule id: 3702433387597893425 Firewall rule name: fw-ilb-to-fw Firewall rule description: Firewall rule priority: 1000 Firewall rule source ranges: ['0.0.0.0/0'] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/salitre-living/global/networks/lb-network-crs-reg Firewall rule target tags: [] Firewall rule target service accounts: [] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

Firewall rule id: 3533709407010524977 Firewall rule name: gl7-ilb-fw-allow-hc Firewall rule description: Firewall rule priority: 1000 Firewall rule source ranges: ['35.235.240.0/20', '130.211.0.0/22', '35.191.0.0/16'] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/salitre-living/global/networks/lb-network-crs-reg Firewall rule target tags: [] Firewall rule target service accounts: [] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

Firewall rule id: 6962869419929341745 Firewall rule name: gl7-ilb-fw-allow-ilb-to-backends Firewall rule description: Firewall rule priority: 1000 Firewall rule source ranges: ['10.130.0.0/23', '10.129.0.0/23'] Firewall rule source service accounts: [] Firewall rule network: https://www.googleapis.com/compute/v1/projects/salitre-living/global/networks/lb-network-crs-reg Firewall rule target tags: ['http-server'] Firewall rule target service accounts: [] Firewall rule kindcompute#firewall Firewall rule disabled: False

---

```

## Subnets

```

Subnet ip_ciddr range10.0.103.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/roma-hub-internal-project/global/networks/vpc-roma-internal-hub Subnet internal ipv6 prefix Subnet external ipv6 prefix

---

Subnet ip_ciddr range10.0.102.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/roma-hub-internal-project/global/networks/vpc-roma-internal-hub Subnet internal ipv6 prefix Subnet external ipv6 prefix

---

Subnet ip_ciddr range10.0.101.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/roma-hub-internal-project/global/networks/vpc-roma-internal-hub Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.100.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/roma-hub-internal-project/global/networks/vpc-roma-internal-hub Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.3.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/roma-hub-project/global/networks/vpc-roma-hub Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.2.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/roma-hub-project/global/networks/vpc-roma-hub Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.1.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/roma-hub-project/global/networks/vpc-roma-hub Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.0.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/roma-hub-project/global/networks/vpc-roma-hub Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range172.16.20.16/28 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/castilla-host-project1/global/networks/vpc-castilla-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.43.0/24 Subnet purposePRIVATE Subnet secondary ip range[ip_cidr_range: "100.64.0.0/17" range_name: "secondary-range-composer-pods-11" , ip_cidr_range: "100.64.128.0/20" range_name: "secondary-range-composer-services-1" , ip_cidr_range: "100.65.128.0/20" range_name: "secondary-range-composer-services-2" , ip_cidr_range: "100.65.0.0/17" range_name: "secondary-range-composer-pods-2"] Subnet networkhttps://www.googleapis.com/compute/v1/projects/castilla-host-project1/global/networks/vpc-castilla-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.42.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/castilla-host-project1/global/networks/vpc-castilla-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.41.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/castilla-host-project1/global/networks/vpc-castilla-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.40.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/castilla-host-project1/global/networks/vpc-castilla-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.83.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/parway-host-project1/global/networks/vpc-parkway-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.82.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/parway-host-project1/global/networks/vpc-parkway-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.81.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/parway-host-project1/global/networks/vpc-parkway-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.80.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/parway-host-project1/global/networks/vpc-parkway-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.23.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/roma-host-project1/global/networks/vpc-roma-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.22.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/roma-host-project1/global/networks/vpc-roma-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.21.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/roma-host-project1/global/networks/vpc-roma-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.20.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/roma-host-project1/global/networks/vpc-roma-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.63.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/salitre-host-project1/global/networks/vpc-salitre-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.62.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/salitre-host-project1/global/networks/vpc-salitre-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.61.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/salitre-host-project1/global/networks/vpc-salitre-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.0.60.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/salitre-host-project1/global/networks/vpc-salitre-host Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.1.2.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/salitre-living/global/networks/lb-network-crs-reg Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.129.0.0/23 Subnet purposeGLOBAL_MANAGED_PROXY Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/salitre-living/global/networks/lb-network-crs-reg Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.1.3.0/24 Subnet purposePRIVATE Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/salitre-living/global/networks/lb-network-crs-reg Subnet internal ipv6 prefix Subnet external ipv6 prefix

Subnet ip_ciddr range10.130.0.0/23 Subnet purposeGLOBAL_MANAGED_PROXY Subnet secondary ip range[] Subnet networkhttps://www.googleapis.com/compute/v1/projects/salitre-living/global/networks/lb-network-crs-reg Subnet internal ipv6 prefix Subnet external ipv6 prefix

```

## VPN Connectivity

```

Tunnel nameha-vpn-spoke-hub-southamerica-west1-cl-noprod-ha-tunnel1 Tunnel IKE Version: 2 Tunnel Peer ip: 34.153.33.202 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-host-project1/regions/southamerica-west1/vpnGateways/ha-vpn-hub-spoke-southamerica-west1-cl-noprod-2 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-southamerica-west1-cl-noprod-ha-tunnel2 Tunnel IKE Version: 2 Tunnel Peer ip: 34.104.51.131 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-host-project1/regions/southamerica-west1/vpnGateways/ha-vpn-hub-spoke-southamerica-west1-cl-noprod-2 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-southamerica-west1-cl-prod-ha-tunnel1 Tunnel IKE Version: 2 Tunnel Peer ip: 34.153.33.185 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-host-project1/regions/southamerica-west1/vpnGateways/ha-vpn-hub-spoke-southamerica-west1-cl-prod-2 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-southamerica-west1-cl-prod-ha-tunnel2 Tunnel IKE Version: 2 Tunnel Peer ip: 34.153.225.222 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-host-project1/regions/southamerica-west1/vpnGateways/ha-vpn-hub-spoke-southamerica-west1-cl-prod-2 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-us-central1-dev-ha-tunnel1 Tunnel IKE Version: 2 Tunnel Peer ip: 34.157.96.232 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/parway-host-project1/regions/us-central1/vpnGateways/ha-vpn-hub-spoke-us-central1-dev-2 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-us-central1-dev-ha-tunnel2 Tunnel IKE Version: 2 Tunnel Peer ip: 35.220.90.152 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/parway-host-project1/regions/us-central1/vpnGateways/ha-vpn-hub-spoke-us-central1-dev-2 Tunnel Kind: compute#vpnTunnel

---

Tunnel namevpn-to-oracle-tunnel1 Tunnel IKE Version: 2 Tunnel Peer ip: 141.148.64.14 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-us-east4-cl-noprod-ha-tunnel1 Tunnel IKE Version: 2 Tunnel Peer ip: 34.157.23.81 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-host-project1/regions/us-east4/vpnGateways/ha-vpn-hub-spoke-us-east4-cl-noprod-2 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-us-east4-cl-noprod-ha-tunnel2 Tunnel IKE Version: 2 Tunnel Peer ip: 34.157.154.122 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-host-project1/regions/us-east4/vpnGateways/ha-vpn-hub-spoke-us-east4-cl-noprod-2 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-us-east4-cl-prod-ha-tunnel1 Tunnel IKE Version: 2 Tunnel Peer ip: 34.157.17.58 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-host-project1/regions/us-east4/vpnGateways/ha-vpn-hub-spoke-us-east4-cl-prod-2 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-us-east4-cl-prod-ha-tunnel2 Tunnel IKE Version: 2 Tunnel Peer ip: 34.157.147.86 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-host-project1/regions/us-east4/vpnGateways/ha-vpn-hub-spoke-us-east4-cl-prod-2 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-us-central1-dev-ha-tunnel3 Tunnel IKE Version: 2 Tunnel Peer ip: 35.242.101.135 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-hub-

project/regions/us-central1/vpnGateways/ha-vpn-hub-spoke-us-central1-dev-1 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-us-central1-dev-ha-tunnel4 Tunnel IKE Version: 2 Tunnel Peer ip: 34.157.213.64 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-hub-project/regions/us-central1/vpnGateways/ha-vpn-hub-spoke-us-central1-dev-1 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-southamerica-west1-cl-noprod-ha-tunnel3 Tunnel IKE Version: 2 Tunnel Peer ip: 34.153.33.173 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-hub-project/regions/southamerica-west1/vpnGateways/ha-vpn-hub-spoke-southamerica-west1-cl-noprod-1 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-southamerica-west1-cl-noprod-ha-tunnel4 Tunnel IKE Version: 2 Tunnel Peer ip: 34.104.50.75 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-hub-project/regions/southamerica-west1/vpnGateways/ha-vpn-hub-spoke-southamerica-west1-cl-noprod-1 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-southamerica-west1-cl-prod-ha-tunnel3 Tunnel IKE Version: 2 Tunnel Peer ip: 34.153.33.220 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-hub-project/regions/southamerica-west1/vpnGateways/ha-vpn-hub-spoke-southamerica-west1-cl-prod-1 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-southamerica-west1-cl-prod-ha-tunnel4 Tunnel IKE Version: 2 Tunnel Peer ip: 34.104.50.176 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-hub-project/regions/southamerica-west1/vpnGateways/ha-vpn-hub-spoke-southamerica-west1-cl-prod-1 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-us-east4-cl-noprod-ha-tunnel3 Tunnel IKE Version: 2 Tunnel Peer ip: 34.157.30.163 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-hub-project/regions/us-east4/vpnGateways/ha-vpn-hub-spoke-us-east4-cl-noprod-1 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-us-east4-cl-noprod-ha-tunnel4 Tunnel IKE Version: 2 Tunnel Peer ip: 34.157.153.18 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-hub-project/regions/us-east4/vpnGateways/ha-vpn-hub-spoke-us-east4-cl-noprod-1 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-us-east4-cl-prod-ha-tunnel3 Tunnel IKE Version: 2 Tunnel Peer ip: 35.242.60.217 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-hub-project/regions/us-east4/vpnGateways/ha-vpn-hub-spoke-us-east4-cl-prod-1 Tunnel Kind: compute#vpnTunnel

---

Tunnel nameha-vpn-spoke-hub-us-east4-cl-prod-ha-tunnel4 Tunnel IKE Version: 2 Tunnel Peer ip: 34.104.124.107 Tunnel status: ESTABLISHED Tunnel Shared secret: *** Tunnel Peer GCP Gateway: https://www.googleapis.com/compute/v1/projects/roma-hub-project/regions/us-east4/vpnGateways/ha-vpn-hub-spoke-us-east4-cl-prod-1 Tunnel Kind: compute#vpnTunnel

---

```

# Best Practices

This section outlines Google Cloud's best practices for VPC and VPN configuration.

## VPC Best Practices

The document provides best practices and reference architectures for designing Virtual Private Clouds (VPCs) on Google Cloud, aimed at cloud network architects and system architects familiar with Google Cloud networking concepts. Key recommendations include:

1. **General Principles**:
2. Identify decision makers, timelines, and pre-work.
3. Consider VPC network design early in the organizational setup.

4. Keep the design simple and use clear naming conventions.
```

5. **Addresses and Subnets**:
6. Use custom mode subnets for better integration with existing IP management schemes.
7. Group applications into fewer subnets with larger address ranges.
8. **Single VPC Network and Shared VPC**:
9. Start with a single VPC network for resources with common requirements.
10. Use Shared VPC for multiple working groups and grant network user roles at the subnet level.
11. **Multiple VPC Networks**:
12. Create a single VPC network per project to map quotas.
13. Isolate sensitive data in its own VPC network.
14. **Connecting Multiple VPC Networks**:
15. Choose connection methods based on cost, performance, and security needs.
16. Use VPC Network Peering, Cloud VPN, or Cloud Interconnect as appropriate.
17. **Hybrid Design**:
18. Use dynamic routing and a connectivity VPC network for scaling hub-and-spoke architectures.
19. **Network Security**:
20. Identify clear security objectives and limit external access.
21. Use Google Cloud native firewall rules and isolate VMs using service accounts.
22. **Network Services**:
23. Use Cloud NAT for fixed external IP addresses and Private DNS zones for name resolution.
24. **API Access**:
25. Use the default internet gateway for Google APIs and deploy instances on the same subnet.
26. **Logging, Monitoring, and Visibility**:
    - Tailor logging for specific use cases and use VPC Flow Logs sampling to reduce volume.

The document also includes reference architectures illustrating these best practices, such as single project VPC networks, Shared VPC configurations, and stateful L7 firewalls between VPC networks. It emphasizes the importance of planning, simplicity, and security in VPC design.

VPN Best Practices

The best practices for configuring Cloud VPN on Google Cloud include:

1. **Project Separation**: Use separate Google Cloud projects for networking resources to simplify the configuration of Identity and Access Management (IAM) roles and permissions.
2. **Routing and Failover**:
3. Opt for dynamic routing using the Border Gateway Protocol (BGP) and High Availability (HA) VPN for better availability.
4. Choose the appropriate tunnel configuration: use active/passive for two HA VPN tunnels and active/active for more than two.
5. **Reliability**:
6. Configure your peer VPN gateway to use only one cipher for each cipher role to ensure stable cipher selection and prevent performance issues.
7. For HA VPN tunnel pairs, ensure both tunnels use the same cipher and IKE Phase 2 lifetime values.
8. **Security**:
9. Set up secure firewall rules for traffic over Cloud VPN.
10. Use strong pre-shared keys for VPN tunnels.
11. Restrict IP addresses for peer VPN gateways to prevent unauthorized tunnels.

12. Configure the strongest cipher supported by both your peer VPN gateway and Cloud VPN.

13. **Advanced Configurations and Troubleshooting**: For high-availability, high-throughput, or multiple subnet scenarios, refer to advanced configurations. Troubleshooting resources are available for common issues.

These practices aim to enhance the security, reliability, and efficiency of Cloud VPN deployments.

Analysis

This section analyzes your current network configuration based on the best practices outlined above.

VPC Analysis

1. **Issue/Observation**: Multiple VPC networks with no peerings or clear connectivity strategy.
2. **Recommendation**: Evaluate the need for VPC Network Peering or other connectivity solutions like Cloud VPN or Cloud Interconnect between these VPCs if they need to communicate. Consider consolidating VPCs where possible to simplify the network architecture.

3. **Rationale**: Best practices suggest using a single VPC network for resources with common requirements and using VPC Network Peering or other methods to connect multiple VPC networks based on cost, performance, and security needs. This can reduce complexity and improve manageability.

4. **Issue/Observation**: Firewall rules are inconsistent and potentially conflicting, such as multiple "deny-all" and "allow-all" rules.

5. **Recommendation**: Review and refine firewall rules to ensure they are specific and non-conflicting. Implement a least privilege model by allowing only necessary traffic and using service accounts and target tags to apply rules more granularly.

6. **Rationale**: Best practices emphasize clear security objectives and limiting external access. Using Google Cloud native firewall rules effectively can enhance security by ensuring only necessary traffic is allowed.

7. **Issue/Observation**: Subnets are small and numerous, which can complicate IP management and lead to fragmentation.

8. **Recommendation**: Consider consolidating subnets into fewer, larger subnets where possible, especially for applications that can be grouped together. Use custom mode subnets to better integrate with existing IP management schemes.

9. **Rationale**: Grouping applications into fewer subnets with larger address ranges aligns with best practices for simplifying network design and improving IP address management.

10. **Issue/Observation**: Lack of IPv6 configuration across the VPCs.

11. **Recommendation**: Evaluate the need for IPv6 support and enable ULA Internal IPv6 if required for future-proofing and compliance with modern networking standards.

12. **Rationale**: While not explicitly mentioned in the best practices, enabling IPv6 can be beneficial for future scalability and compatibility with global internet standards.

13. **Issue/Observation**: The use of "GLOBAL" routing mode across all VPCs without clear justification.

14. **Recommendation**: Assess whether "GLOBAL" routing mode is necessary for all VPCs. If not, consider switching to "REGIONAL" routing mode where appropriate to reduce latency and improve performance.

15. **Rationale**: Best practices suggest choosing routing modes based on specific needs. "REGIONAL" routing can be more efficient for workloads that do not require global reach.

16. **Issue/Observation**: Lack of detailed network descriptions and documentation.

17. **Recommendation**: Add detailed descriptions to each network and document the purpose and configuration of each VPC and subnet. This will aid in management and future audits.
18. **Rationale**: Keeping the design simple and using clear naming conventions and documentation aligns with best practices for maintaining a manageable and understandable network architecture.

VPN Analysis:

Review the VPN configuration to ensure strong encryption and authentication are used. If critical, consider implementing redundant VPN tunnels for high availability.

Based on your current VPN configuration and the best practices for Cloud VPN on Google Cloud, here are some specific action items and recommendations to improve your setup:

1. **Project Separation**:

2. Ensure that your VPN configurations are organized within separate Google Cloud projects for production, non-production, and development environments. This will help in managing IAM roles and permissions more effectively.

3. **Routing and Failover**:

4. Verify that you are using dynamic routing with BGP for all HA VPN tunnels. This is crucial for better availability and failover capabilities.

5. For tunnels configured in pairs (e.g., `ha-vpn-spoke-hub-southamerica-west1-cl-noprod-ha-tunnel1` and `ha-vpn-spoke-hub-southamerica-west1-cl-noprod-ha-tunnel2`), ensure they are set up in an active/passive configuration. For configurations with more than two tunnels, consider active/active setups to maximize throughput and redundancy.

6. **Reliability**:

7. Check that each pair of HA VPN tunnels (e.g., `ha-vpn-spoke-hub-southamerica-west1-cl-prod-ha-tunnel1` and `ha-vpn-spoke-hub-southamerica-west1-cl-prod-ha-tunnel2`) uses the same cipher and IKE Phase 2 lifetime values. This ensures consistent performance and reliability.

8. Ensure that your peer VPN gateways are configured to use only one cipher for each cipher role to avoid performance issues.

9. **Security**:

10. Review and update your firewall rules to ensure they are secure and only allow necessary traffic over the VPN tunnels.
11. Confirm that strong pre-shared keys are used for all VPN tunnels. Regularly update these keys to maintain security.
12. Restrict the IP addresses allowed for peer VPN gateways to prevent unauthorized access. This can be done by specifying allowed IP ranges in your firewall rules.

13. Ensure that the strongest cipher supported by both your peer VPN gateway and Cloud VPN is configured. This enhances the security of your VPN connections.

14. **Advanced Configurations and Troubleshooting**:

15. For high-availability and high-throughput scenarios, consider reviewing advanced configuration options available in GCP documentation to optimize your setup.

16. Regularly monitor your VPN tunnels for any issues and utilize GCP's troubleshooting resources to address common problems.

17. **Documentation and Monitoring**:

18. Document your VPN configurations, including tunnel names, peer IPs, and any specific settings. This will aid in troubleshooting and future audits.
19. Implement monitoring and alerting for your VPN tunnels to quickly detect and respond to any connectivity issues.

By implementing these specific action items, you can enhance the security, reliability, and efficiency of your Cloud VPN deployments on Google Cloud.