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: 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 VPC networks 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, external routing, 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 VPCs, 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: 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 per cipher role to ensure stable cipher selection and prevent performance issues.
7. For HA VPN tunnel pairs, use the same cipher and IKE Phase 2 lifetime values on both tunnels.
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 connections.
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

To improve your current VPC configuration based on the best practices for Google Cloud, here are some specific action items and recommendations:

General Principles

1. **Naming Conventions**: Ensure that all VPCs, subnets, and firewall rules have clear and descriptive names. This will help in managing and identifying resources easily.

Addresses and Subnets

1. **Subnet Grouping**: Consider consolidating subnets where possible to reduce complexity. For example, if certain subnets serve similar purposes or applications, they could be grouped into larger subnets with larger address ranges.

2. **IP Management**: Since you are using custom mode VPCs, ensure that your IP ranges do not overlap and are well-documented to avoid conflicts, especially if you plan to connect these VPCs with other networks.

Single VPC Network and Shared VPC

1. **Shared VPC Usage**: If multiple projects or teams need to access shared resources, consider using Shared VPCs to centralize network management and improve security by controlling access at the subnet level.

Multiple VPC Networks

1. **Project Isolation**: You have multiple VPCs, which is good for isolating resources. Ensure that sensitive data is isolated in its own VPC network, and apply strict firewall rules to protect it.

Connecting Multiple VPC Networks

1. **VPC Peering and Connectivity**: You currently have limited VPC peering. Evaluate the need for VPC Network Peering or other connectivity options like Cloud VPN or Cloud Interconnect to facilitate communication between VPCs, especially if they need to share data or services.

Network Security

1. **Firewall Rules**:
2. Review and refine your firewall rules. For example, the `allow-all` rules are risky and should be replaced with more specific rules that only allow necessary traffic.
3. Ensure that `deny-all` rules are correctly prioritized and that there are no conflicting rules that might inadvertently allow unwanted traffic.

4. Use target tags and service accounts to apply rules to specific resources rather than broad IP ranges.

5. **Service Accounts**: Consider using service accounts to isolate VMs and apply specific firewall rules to them, enhancing security.

Network Services

1. **Cloud NAT**: If you require fixed external IP addresses for outbound traffic, consider using Cloud NAT to manage this efficiently.

API Access

1. **API Gateway**: Ensure that instances needing access to Google APIs are correctly configured to use the default internet gateway, and consider deploying them on the same subnet for efficiency.

Logging, Monitoring, and Visibility

1. **VPC Flow Logs**: Enable VPC Flow Logs for critical subnets to monitor traffic and identify potential security issues. Tailor the logging to specific use cases to avoid excessive data collection.

Additional Recommendations

1. **IPv6 Consideration**: Although you have not enabled IPv6, consider planning for future IPv6 adoption, especially if you anticipate growth or need to connect with IPv6-only networks.

2. **MTU Settings**: Review and set appropriate MTU values for your networks to optimize performance, especially if you are using Cloud Interconnect or VPNs.

By implementing these specific recommendations, you can enhance the security, efficiency, and manageability of your VPC configuration on Google Cloud.

VPN Analysis:

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

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

1. **Project Separation**:
2. Ensure that your networking resources are organized into separate Google Cloud projects, especially for production and non-production environments. This will help simplify IAM role and permission management.
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 with more than two connections (e.g., `ha-vpn-spoke-hub-us-central1-dev-ha-tunnel3` and `ha-vpn-spoke-hub-us-central1-dev-ha-tunnel4`), ensure they are configured in an active/active setup to maximize throughput and redundancy.
6. **Reliability**:
7. Check that your peer VPN gateways are configured to use only one cipher per cipher role. This helps in maintaining stable cipher selection and avoiding performance issues.
8. Ensure that HA VPN tunnel pairs (e.g., `ha-vpn-spoke-hub-southamerica-west1-cl-prod-ha-tunnel1` and `ha-vpn-spoke-hub-southamerica-west1-cl-prod-ha-tunnel2`) use the same cipher and IKE Phase 2 lifetime values on both tunnels.
9. **Security**:
10. Review and update your firewall rules to ensure they are secure and only allow necessary traffic over the VPN.
11. Regularly update and use strong pre-shared keys for all VPN tunnels. Consider using a key rotation policy.
12. Restrict the IP addresses for peer VPN gateways to only those that are necessary, minimizing the risk of unauthorized connections.
13. Configure the strongest cipher supported by both your peer VPN gateway and Cloud VPN. This may require coordination with your peer network administrators.
14. **Advanced Configurations and Troubleshooting**:
15. For high-availability and high-throughput scenarios, ensure that your configurations align with advanced setup guidelines provided by Google Cloud.
16. Regularly review logs and monitoring data to proactively identify and troubleshoot any issues. Utilize Google Cloud's monitoring and logging tools to set up alerts for any anomalies or failures in VPN connections.
17. **Documentation and Review**:
18. Document your current VPN configurations, including tunnel settings, routing policies, and security measures. This will aid in future audits and troubleshooting.
19. Schedule regular reviews of your VPN setup to ensure it continues to meet your organization's needs and adheres to best practices.

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