TechPeople

https://techpeople.us/job/network-security-architect-gcp-security

Network Security Architect – GCP Security

Hiring organization
TechPeople

Employment Type
Contractor

Duration of employment
12 – 24 mos.

Industry
TELECOM

Job Location
Plano, TX (Hybrid) / C2C

Date posted
April 5, 2024

Description

- Location: Plano, TX (Hybrid)
- # of Positions: 1
- Eligibility: Open
- Client Name / Domain: TELECOM

- Bill Rate: $?? per hour
- Employment Mode: Contract / Corp-to-Corp
- Contract Duration: 12+ mos. Contract
- Experience: 10 – 15+ years
- Skills: VPC, Google Could Platform, Firewalls, Google Kubernetes, Clusters, Load Balancing, Security, IaaS, SaaS, PaaS

Client is looking for an experienced Network Security Architect to lead engineering assessments and selection of investments for a range of network technology across Google Cloud / LAN / WAN / wireless / Security and evolving capabilities and strategies for network technology deployment into the enterprise.

Responsibilities

1.1 **Designing an overall network architecture. Considerations include:**

- High availability, failover, and disaster recovery strategies
- DNS strategy (e.g., on premises, Cloud DNS)
- Security and data exfiltration requirements
- **Load balancing**
  - Applying quotas per project and per VPC
  - Hybrid connectivity (e.g., Google private access for hybrid connectivity)
- **Container networking**
  - IAM roles
  - SaaS, PaaS, and IaaS services
  - Microsegmentation for security purposes (e.g., using metadata, tags, service accounts)

1.2 Designing Virtual Private Cloud (VPC) instances. Considerations include:

- IP address management and bring your own IP (BYOIP)
  - Standalone vs. Shared VPC
  - Multiple vs. single

    - Regional vs. multi regional
    - VPC Network Peering
    - Firewalls (e.g., service account based, tag based)
- Custom routes
    - Using managed services (e.g., Cloud SQL, Memorystore)
- Third party device insertion (NGFW) into VPC using multi NIC and internal load balancer as a next hop or equal cost multi path (ECMP) routes

1.3 Designing a hybrid and multi cloud network. Considerations include:

- Dedicated Interconnect vs. Partner Interconnect
- Multi cloud connectivity
- Direct Peering
- IPsec VPN
- Failover and disaster recovery strategy
- Regional vs. global VPC routing mode
- Accessing multiple VPCs from on premises locations (e.g., Shared VPC, multi VPC peering topologies)
- Bandwidth and constraints provided by hybrid connectivity solutions
- Accessing Google Services/APIs privately from on premises locations
- IP address management across on premises locations and cloud
- DNS peering and forwarding

1.4 Designing an IP addressing plan for Google Kubernetes Engine. Considerations include:

Public and private cluster nodes
Control plane public vs. private endpoints
Subnets and alias IPs
RFC 1918, non RFC 1918, and privately used public IP (PUPI) address options

2.1 Configuring VPCs. Considerations include:

- Google Cloud VPC resources (e.g., networks, subnets, firewall rules)
- VPC Network Peering
- Creating a Shared VPC network and sharing subnets with other projects
- Configuring API access to Google services (e.g., Private Google Access, public interfaces)
- Expanding VPC subnet ranges after creation

2.2 Configuring routing. Considerations include:

- Static vs. dynamic routing
- Global vs. regional dynamic routing
- Routing policies using tags and priority
- Internal load balancer as a next hop
- Custom route import/export over VPC Network Peering

2.3 Configuring and maintaining Google Kubernetes Engine clusters. Considerations include:

- VPC native clusters using alias IPs
- Clusters with Shared VPC
- Creating Kubernetes Network Policies
- Private clusters and private control plane endpoints
- Adding authorized networks for cluster control plane endpoints

2.4 Configuring and managing firewall rules. Considerations include:

- Target network tags and service accounts
- Rule priority
- Network protocols
- Ingress and egress rules
- Firewall rule logging
- Firewall Insights
- Hierarchical firewalls

2.5 Implementing VPC Service Controls. Considerations include:

- Creating and configuring access levels and service perimeters
- VPC accessible services
- Perimeter bridges
- Audit logging
- Dry run mode

3.1 Configuring load balancing. Considerations include:

- Backend services and network endpoint groups (NEGs)
- Firewall rules to allow traffic and health checks to backend services
- Health checks for backend services and target instance groups
- Configuring backends and backend services with balancing method (e.g., RPS,
- CPU, Custom), session affinity, and capacity scaling/scaler
- TCP and SSL proxy load balancers

Qualifications

- Subject Matter Expertise in the following areas
    - Network Architecture
    - DNS Strategy – onPrem and Cloud DNS
    - Security and Data Exfiltration
    - Load Balancing
    - Container Networking – SaaS, PaaS, IaaS services

Contacts

If you are interested in applying for this role, please send your updated resume to tpjobs@techpeople.us