Google Cloud Network Security Fundamentals Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

This foundational training course provides a comprehensive deep dive into Google Cloud's robust network security offerings, essential for protecting modern cloud-native architectures. As organizations rapidly migrate critical workloads, securing the Virtual Private Cloud (VPC) network becomes paramount. Google Cloud Network Security Fundamentals Training Course addresses this need by focusing on core concepts, best practices, and the practical implementation of key Google Cloud Platform (GCP) services like VPC Firewall Rules, Cloud Load Balancing, VPC Service Controls, and Cloud IDS. Trainees will gain the skills necessary to build a Zero Trust network architecture, manage perimeter defense, and ensure data exfiltration prevention, aligning with industry-leading security frameworks.

This program is specifically designed to empower IT and security professionals to assume their roles as the first line of defense in the cloud. We emphasize hands-on proficiency through real-world lab exercises and case studies, ensuring participants can immediately apply their learning to secure their enterprise's cloud deployment. By mastering Identity and Access Management (IAM) as it pertains to networking, implementing robust network segmentation, and leveraging advanced threat detection tools, graduates will be ready to tackle the challenges of modern cloud security engineering and contribute significantly to their organization's overall cybersecurity posture.

Programme Curriculum

Google Cloud Network Security Fundamentals Training Course

Introduction

This foundational training course provides a comprehensive deep dive into Google Cloud's robust network security offerings, essential for protecting modern cloud-native architectures. As organizations rapidly migrate critical workloads, securing the Virtual Private Cloud (VPC) network becomes paramount. Google Cloud

Network Security Fundamentals Training Course addresses this need by focusing on core concepts, best practices, and the practical implementation of key Google Cloud Platform (GCP) services like VPC Firewall Rules, Cloud Load Balancing, VPC Service Controls, and Cloud IDS. Trainees will gain the skills necessary to build a Zero Trust network architecture, manage perimeter defense, and ensure data exfiltration prevention, aligning with industry-leading security frameworks.

This program is specifically designed to empower IT and security professionals to assume their roles as the first line of defense in the cloud. We emphasize hands-on proficiency through real-world lab exercises and case studies, ensuring participants can immediately apply their learning to secure their enterprise's cloud deployment. By mastering Identity and Access Management (IAM) as it pertains to networking, implementing robust network segmentation, and leveraging advanced threat detection tools, graduates will be ready to tackle the challenges of modern cloud security engineering and contribute significantly to their organization's overall cybersecurity posture.

Course Duration

5 days

Course Objectives with Strong Trending Keywords

1. Define and articulate the division of security responsibilities between Google Cloud and the customer.
2. Implement least privilege access control using IAM roles and service accounts for secure network resource management.
3. Design and configure Virtual Private Cloud (VPC) networks, subnets, and routes for effective network segmentation.
4. Master the configuration and best practices for VPC Firewall Rules to enforce strict perimeter defense
5. Securely extend the corporate network to GCP using Cloud VPN and Cloud Interconnect with proper encryption and routing.
6. Apply SSL Policies and integrate Google Cloud Armor with Load Balancers for DDoS mitigation and application-layer security.
7. Utilize VPC Service Controls to establish a secure security perimeter around sensitive data and services.
8. Deploy and configure Cloud IDS for real-time threat detection and visibility into malicious network activity.
9. Implement VPC Flow Logs and integrate with Cloud Logging/Monitoring for continuous network security monitoring and auditing.
10. Explain how GCP network security features support a modern Zero Trust security architecture.
11. Configure Private Google Access and Serverless VPC Access to ensure internal-only communication with Google APIs and serverless environments.
12. Understand and implement security features of Cloud DNS to prevent DNS-based attacks and ensure secure name resolution.
13. Identify common network misconfigurations and implement remediation strategies using Google Cloud tools.

Target Audience

1. Cloud Security Engineers / Analysts
2. Network Engineers moving to the cloud (GCP)
3. Security Architects designing GCP deployments
4. DevOps Engineers or SREs responsible for secure cloud operations
5. Security Consultants specializing in Google Cloud Platform

6. IT Professionals preparing for the Google Cloud Professional Security Engineer Certification
7. System Administrators managing cloud infrastructure
8. Compliance Officers needing to understand cloud network controls

Course Modules

Module 1: Foundations and the Shared Responsibility Model

- Google Cloud's approach to enterprise security and global infrastructure.
- Understanding the Shared Security Responsibility Model
- The Resource Hierarchy as a security boundary.
- Integrating Cloud Identity with your existing identity provider
- Case Study: Analyzing a public-facing web app deployment where a misconfigured firewall rule led to a customer data breach, emphasizing the customer's responsibility.

Module 2: Identity and Access Management (IAM) for Networks

- Users, Groups, Service Accounts, Roles
- Implementing the Principle of Least Privilege for network-related actions.
- Securing Service Accounts and using Workload Identity Federation to manage access.
- Applying Organization Policies to enforce network-wide restrictions
- Case Study: A development team needed restricted network access for CI/CD pipelines; demonstrating how to use a custom IAM role and service account key rotation.

Module 3: Virtual Private Cloud (VPC) and Segmentation

- Designing single and shared VPC architectures for large enterprises.
- Configuring subnets and understanding IP addressing best practices.
- Implementing Route Tables and applying security zoning via Network Segmentation.
- Securing traffic between VPCs using VPC Peering and its security implications.
- Case Study: Designing a multi-tier application environment using three separate, highly-segmented subnets in one VPC, secured by custom routes and firewall rules.

Module 4: Perimeter Defense with Cloud Firewall Rules

- Deep dive into VPC Firewall Rules.
- Implementing stateful firewall rules and creating a default "Deny All" security posture.
- Using Hierarchical Firewall Policies to enforce security across the Organization.
- Best practices for firewall tags and service accounts as targets/sources.
- Case Study: A company's internal application was accidentally exposed to the internet; using Hierarchical Firewall Policies to centrally enforce a strict Egress deny policy to prevent data leakage.

Module 5: Advanced Network Security Services

- Protecting applications from DDoS attacks with Google Cloud Armor
- Deploying and configuring Cloud Intrusion Detection System for deep packet inspection.
- Leveraging Secure Web Proxy for secure outbound web access with granular policy control.
- Utilizing Private Service Connect to securely consume managed services.
- Case Study: A high-traffic e-commerce website was subjected to a Layer 7 attack; implementing Cloud Armor's WAF to mitigate the threat without impacting legitimate traffic.

Module 6: Data Perimeter Control with VPC Service Controls

- Defining a Service Perimeter and understanding the concept of a "security boundary."
- Restricting data access to authorized networks/clients for supported services
- Preventing Data Exfiltration by blocking data movement outside the perimeter.
- Using Access Levels to grant context-aware, conditional access to the perimeter.
- Case Study: A financial institution needed to prevent unauthorized employees from copying sensitive data from BigQuery to a personal cloud storage bucket; deploying a VPC SC perimeter to enforce this boundary.

Module 7: Network Monitoring, Logging, and Auditing

- Enabling and analyzing VPC Flow Logs for network traffic visibility and forensics.
- Setting up custom metrics and alerts in Cloud Monitoring based on flow log data
- Using Cloud Audit Logs to track administrative and data access API calls.
- Implementing Packet Mirroring for in-depth network traffic inspection by a security appliance.
- Case Study: Investigating a suspected internal data breach by analyzing VPC Flow Logs and Cloud Audit Logs to trace the source, destination, and timing of unauthorized access attempts.

Module 8: Secure Hybrid and Perimeterless Access

- Securing Cloud VPN and Cloud Interconnect for reliable, encrypted connections.
- Implementing Identity-Aware Proxy for secure, perimeter-less access to applications
- Configuring Private Google Access for VMs without external IPs to access Google APIs.
- Reviewing security implications and best practices for Cloud DNS and DNS filtering.
- Case Study: Implementing IAP to grant external contractors secure, auditable, and context-aware access to an internal VM-hosted application without using a traditional VPN.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com