



Network Security Essentials

Course description

Learn how to design, implement, and manage secure network architectures on Google Cloud using native security services. Explore network security best practices, threat detection mechanisms, secure connectivity solutions, and AI-powered security operations to protect cloud workloads and enterprise environments from evolving cyber threats.

Participants will learn how to design secure architectures with Cloud NGFW and Cloud Armor, implement secure private connectivity, proactively detect threats using Cloud IDS and VPC Flow Logs, and secure hybrid cloud environments. The course also explores how Generative AI can enhance threat analysis, security operations, and network security automation. Through demonstrations, discussions, and real-world scenarios, learners gain practical skills for building resilient and secure cloud networks.

- Course level: Intermediate
- Duration: 1 day

Activities

This course includes instructor-led training, real-world security demonstrations, interactive discussions, threat analysis exercises, security architecture reviews, ai-powered security use cases, scenario-based learning, and best practice discussions to reinforce learning.

Course objectives

In this course, you will learn to:

- Understand the shared responsibility model for cloud security.
- Design secure network architectures on Google Cloud.
- Implement network protection using Cloud NGFW and Cloud Armor.
- Configure secure private connectivity services.
- Detect and analyze network threats proactively.
- Monitor network traffic using VPC Flow Logs and Flow Analyzer.
- Implement secure hybrid connectivity solutions.
- Utilize AI-assisted threat intelligence workflows.
- Apply security best practices for modern cloud environments.

Intended audience

This course is intended for:

- Cloud Network Engineers
- Cloud Security Engineers
- Network Security Administrators
- Security Architects
- Infrastructure Engineers
- Cloud Architects
- IT Security Professionals
- Professionals responsible for network security on Google Cloud

Prerequisites

We recommend that attendees of this course have:

- Familiarity with foundational networking concepts.
- Understanding of Google Cloud fundamentals.
- Experience with the Google Cloud Console.
- Basic knowledge of Google Cloud CLI is beneficial.

Products covered

- Cloud NGFW
- Cloud Armor
- Cloud IDS
- Cloud NAT
- Private Service Connect
- VPC Service Controls
- VPC Flow Logs
- Flow Analyzer
- Security Command Center
- Gemini

Course outline

Module 01 - Network Security Design and Architecture

- Shared Responsibility and Due Diligence
- Secure Architectures with Cloud NGFW

Module 02 - Elevating Network Security with Managed Services

- Cloud Armor Configurations
- Secure Private Connectivity
- Proactive Intrusion Detection

Module 03 - Proactive Threat Detection and Response

- Network Monitoring and Threat Analysis
- Implementing Secure Hybrid Connectivity

Module 04 - AI for Modern Network Security

- The Role of Generative AI in Network Security
- AI-Powered Workflows and Best Practices

Module 05 - Network Security Essentials Quiz and Reflection

- Review of Core Concepts

Certification details

Participants receive a course completion certificate upon successfully attending the training program.

FAQs

Who should attend this course?

This course is designed for cloud network engineers, cloud security engineers, and professionals responsible for securing Google Cloud network environments.

Is prior security experience required?

Learners should have foundational networking knowledge and familiarity with Google Cloud concepts.

What security services are covered?

The course covers Cloud NGFW, Cloud Armor, Cloud IDS, Cloud NAT, Private Service Connect, VPC Service Controls, VPC Flow Logs, Flow Analyzer, Security Command Center, and Gemini.

Is this a hands-on course?

The course includes demonstrations, discussions, and practical real-world network security scenarios.

Does the course cover hybrid cloud security?

Yes. Participants learn how to securely connect on-premises environments with Google Cloud using secure hybrid connectivity approaches.

How is AI used in network security?

The course explores AI-assisted threat intelligence, incident investigation, security automation, and best practices for AI-driven security operations.

How long is the course?

The course is delivered in a 3-hour instructor-led format.

What business benefits can organizations expect?

Organizations can strengthen network security, improve threat visibility, enhance compliance, secure hybrid environments, and accelerate security operations using Google Cloud's native security services and AI-powered capabilities.