

Network Security Essentials

This course provides a practical guide to securing networks on Google Cloud. The course will cover core network security principles and their application using Google Cloud's managed services. Network security concepts and best practices will be explored through practical demonstrations and real-world application scenarios. The course uses presentations, demos, and discussions, with real-world examples, to ensure effective learning.

**DURATION**

2-3 hours

**LEVEL**

200 - Intermediate

**FORMAT**

Instructor-led

**SCALABLE**

1-50, scaled to 1000

What you'll learn

- Describe the shared responsibility model and its practical implications for security on Google Cloud.
- Design and implement secure network architectures with native services like Cloud NGFW and Cloud Armor.
- Proactively detect and mitigate network threats using VPC Flow Logs and Cloud IDS.
- Secure hybrid connectivity with advanced services like VPC Service Controls.
- Leverage generative AI to enhance security operations and automation.

Overview	5 modules
Who this course is for	• Cloud Network Engineer, Cloud Security Engineer, and anyone involved in designing, implementing, or managing network security on Google Cloud.
Products	• Cloud NAT • Cloud Next Generation Firewall • Google Cloud Armor Enterprise • Cloud Intrusion Detection System • Advanced Networking • Access Context Manager • AI Perimeter Policy • Security Command Center Enterprise • Gemini Enterprise • Google Cloud NGFW • Cloud Armor • Cloud IDS • Private Service Connect • VPC Service Controls • VPC Flow Logs • Flow Analyzer • Security Command Center • Gemini
Prerequisites	• Familiarity with foundational networking and Google Cloud concepts. • Experience with the Google Cloud console and CLI is also beneficial.
Not covered	• This course does not cover advanced Security Operations (SecOps) beyond the scope of a network security professional's responsibilities.

Module 01 Network Security Design and Architecture

Topics	• Shared Responsibility and Due Diligence • Secure Architectures with Cloud NGFW
Objectives	• Explain the shared responsibility model in depth, focusing on common customer configuration pitfalls. • Design and implement secure network architectures using Cloud NGFW and microsegmentation.
Activities	• 1 discussion • 1 demo

Module 02 Elevating Network Security with Managed Services

Topics	• Cloud Armor Configurations • Secure Private Connectivity • Proactive Intrusion Detection
Objectives	• Apply advanced Cloud Armor features to protect against sophisticated web attacks and bot traffic. • Configure Cloud NAT and Private Service Connect to meet strict security and compliance requirements. • Implement Cloud IDS to proactively detect and analyze malicious network activity and compliance.
Activities	• 1 demo

Module 03 Proactive Threat Detection and Response

Topics	• Network Monitoring and Threat Analysis • Implementing Secure Hybrid Connectivity
Objectives	• Analyze network traffic patterns for potential threats using advanced queries of VPC Flow Logs and the Flow Analyzer. • Implement secure hybrid connectivity between on-premises and Google Cloud environments for large-scale deployments.
Activities	• 1 demo

**Module
04****AI for Modern Network Security**

Topics	• The Role of Generative AI in Network Security • AI-Powered workflows and best practices
Objectives	• Leverage AI-assisted threat intelligence to accelerate the investigation and remediation of network security events. • Discuss the ethical considerations and best practices for using AI in network security, and demonstrate its use in practical, network-specific scenarios.
Activities	• 1 discussion • 2 demos

**Module
05****Network Security Essentials: Quiz/Reflection**

Topics	• Review of Core Concepts
Objectives	• Evaluate understanding of core course concepts through scenario-based questions.
Activities	• 5 scenario-based multiple choice questions