

Network Security Essentials

Key information

Course code	Network Security Essentials
Course version	1.0
Course title	Network Security Essentials
Description	<p>This course provides a practical guide to securing networks on Google Cloud.</p> <p>The course will cover core network security principles and their application using Google Cloud's managed services.</p> <p>Network security concepts and best practices will be explored through practical demonstrations and real-world application scenarios.</p> <p>The course uses presentations, demos, and discussions, with real-world examples, to ensure effective learning.</p>
What you'll learn	<ul style="list-style-type: none">• 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.
Duration	3 hours
Level	Intermediate
Format	Instructor-led

Content overview

Who this course is for	<ul style="list-style-type: none">• Cloud Network Engineer• Cloud Security Engineer <p>Anyone involved in designing, implementing, or managing network security on Google Cloud.</p>
Total modules	5
Total videos	0
Total Labs	0
Total classroom activities	2 discussions, 5 demos
Prerequisites	Familiarity with foundational networking and Google Cloud concepts. Experience with the Google Cloud console and CLI is also beneficial.
Products	Google Cloud NGFW, Cloud Armor, Cloud IDS, Cloud NAT, Private Service Connect, VPC Service Controls, VPC Flow Logs, Flow Analyzer, Security Command Center, Gemini
Not covered	This course does not cover advanced Security Operations (SecOps) beyond the scope of a network security professional's responsibilities.

Content breakdown

Module 1 title	Network Security Design and Architecture
Module 1 topics	<ol style="list-style-type: none">1. Shared Responsibility and Due Diligence2. Secure Architectures with Cloud NGFW
Module 1 objectives	<ul style="list-style-type: none">• Explain the shared responsibility model in depth, focusing on common customer configuration pitfalls.• Design and implement secure network architectures using Cloud NGFW and microsegmentation.
Module 1 activities	1 discussion, 1 demo

Module 2 title	Elevating Network Security with Managed Services
Module 2 topics	<ol style="list-style-type: none"> 1. Cloud Armor Configurations 2. Secure Private Connectivity 3. Proactive Intrusion Detection
Module 2 objectives	<ul style="list-style-type: none"> • 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.
Module 2 activities	1 demo
Module 3 title	Proactive Threat Detection and Response
Module 3 topics	<ol style="list-style-type: none"> 1. Network Monitoring and Threat Analysis 2. Implementing Secure Hybrid Connectivity
Module 3 objectives	<ul style="list-style-type: none"> • 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.
Module 3 activities	1 demo
Module 4 title	AI for Modern Network Security
Module 4 topics	<ol style="list-style-type: none"> 1. The Role of Generative AI in Network Security 2. AI-Powered Workflows and Best Practices
Module 4 objectives	<ul style="list-style-type: none"> • 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.
Module 4 activities	1 discussion, 2 demos
Module 5 title	Network Security Essentials: Quiz/Reflection
Module 5 topic	<ol style="list-style-type: none"> 1. Review of Core Concepts
Module 5 objective	<ul style="list-style-type: none"> • Evaluate understanding of core course concepts through scenario-based questions.
Module 5 activities	5 scenario-based multiple choice questions

