

CompTIA CloudNetX (CNX-001)

This CompTIA CloudNetX training prepares you to design and secure modern hybrid cloud networks. As you prepare for the CNX-001 exam, you'll learn how to take control of on-prem, multi-cloud, and SD-WAN environments. From architecting resilient connectivity, to implementing Zero Trust security and diagnosing complex network failures, this course puts real hybrid network design skills in your hands. You'll learn how to segment networks, monitor performance, automate provisioning, and troubleshoot issues across hybrid environments so you can start planning, deploying, and maintaining scalable cloud networking infrastructure.

[CBT Nuggets course material](#) →

WEEK 1

Analyze Requirements for Cloud Network Design

Business Requirements Analysis

Technical Requirement Identification

Workload Communication Analysis

Availability and Failure Domain Analysis

Security and Segmentation Inputs

Address Planning Inputs

Challenge

Analyze Workload Communication Patterns

Introduction

Identify Application Communication Flows

Map Workload Dependencies

Classify Traffic Types

Analyze Communication Protocols

Document Communication Requirements

Capture and Analyze Workload Traffic

Challenge

Design VPC/VNet Network Architectures

Introduction

Cloud Network Isolation Concepts

CIDR Planning for Cloud Networks

Subnet Design Strategies

Route Table Behavior

Network Security Constructs

Challenge

Design Subnetting for Cloud Environments

Introduction

Cloud Subnetting vs Traditional Segmentation

Availability Zone-Aware Subnet Design

Workload-Based Subnet Allocation

IP Address Consumption in Cloud Platforms

Subnet Integration with Cloud Services

Designing for Security and Compliance Zones

Challenge

Design IP Addressing for Hybrid Environments

Introduction

Hybrid Addressing Fundamentals

Address Space Planning and CIDR Strategy

Subnet Design Across Hybrid Environments

Challenge

Design Hybrid Cloud Connectivity

Introduction

Hybrid Cloud Connectivity Fundamentals

Connectivity Models and Transport Options

Routing Design for Hybrid Connectivity

Challenge

Design Multi-Cloud Connectivity

Introduction

Define Multi-Cloud Connectivity

Compare Connectivity Models

Design Cloud-to-Cloud Routing

Design Resilient Interconnects

Challenge

Design Transit Networking Solutions

Introduction

Define Transit Networking

Compare Transit Design Models

Design Transit Routing and Path Control

Apply Segmentation in Transit Architectures

Challenge

Design Hub-and-Spoke Cloud Topologies

Introduction

What Hub-and-Spoke Solves

Core Components of a Hub-and-Spoke Design

Traffic Flow and Routing Behavior

Security and Segmentation in the Topology

Scalability, Resilience, and Design Tradeoffs

Challenge

Design Cloud Network Segmentation

Introduction

Why Segmentation Matters in Cloud

Segmentation Models and Approaches

Routing and Segmentation Boundaries

Security Controls and Enforcement Points

Challenge

Design Highly Available Cloud Network Foundations

Introduction

Why High Availability Matters

High-Availability Design Principles

Availability Zones, Regions, and Failure Domains

Challenge

Design Highly Available Cloud Network Resilience

Introduction

Designing Highly Available Connectivity Paths

Routing and Failover Behavior

Highly Available Shared Services and Traffic Flows

Challenge

Design Cloud Load Balancing Solutions

Introduction

Why Cloud Load Balancing Matters

Core Functions of Cloud Load Balancers

Compare Layer 4 and Layer 7 Load Balancing

Regional and Global Load Balancing Approaches

Challenge

Design Resilient Load Balancing Architectures

Introduction

Design for Health, Resiliency, and Failover

Design Backend Placement and Failover Readiness

Design Public and Internal Load Balancing

Challenge

Design DNS for Cloud Networks

Introduction

Cloud DNS Fundamentals

Public and Private DNS Zones

Cloud and Hybrid DNS Resolution

Highly Available DNS Design

Challenge

Design Cloud DNS Operations and Security

Introduction

DNS Forwarding and Delegation

DNS for App Access and Discovery

DNS Security and Access Control

Troubleshooting Cloud DNS

Challenge

Design DR Networking Strategies

Introduction

DR Networking Fundamentals

Recovery Objectives and Network Requirements

Redundant Connectivity and Failover Paths

Routing and Traffic Steering for DR

Hybrid and Multi-Site DR Design

Challenge

Design Identity-Based Access Controls

Introduction

Define Identity-Based Access Control

Identify Identity Sources and Trust Signals

Design Policy Decisions Around Identity

Apply Identity to Cloud Segmentation Design
Challenge

Design Security Group and ACL Policies

Introduction
Define Security Groups and ACLs
Compare Stateful and Stateless Policies
Design Least-Privilege Policy Rules
Apply Policies to Cloud Segmentation
Challenge

Design Compliance Segmentation

Introduction
Define Compliance Segmentation
Identify Sensitive Flows
Design Trust Zones
Apply Policies to Regulated Workloads
Challenge

Plan Encrypted Connectivity

Introduction
Encrypted Connectivity Fundamentals
Identify VPN Connection Requirements
Validate VPN Security and Traffic Flow
Challenge

Implement Encrypted Connectivity

Introduction
Review the Lab Topology
Implement the Cloud VPN Connection

Configure the On-Premises VPN Peer
Challenge

Secure Hybrid Cloud VPNs

Introduction
From Working VPN to Secure VPN
Review VPN Security and Network Scope
Secure Routes and Access Policies
Validate the Secure Access Model
Challenge

Implement Remote Cloud Access

Introduction
Identify Remote Access Requirements
Compare Remote Access VPN Options
Plan Identity and Authentication Controls
Configure Client VPN Access
Challenge

Implement Cloud Firewall Architectures

Introduction
Identify Firewall Placement Requirements
Validate Firewall Insertion Requirements
Compare Firewall Placement Models
Challenge

WEEK 2

Implement the AWS Cloud Firewall

Introduction

Plan Traffic Inspection Paths

Build Our Game Plan

Verify Existing Environment

Deploy the AWS Network Firewall

Configure Cloud Routing for the Firewall

Apply and Validate Firewall Rules

Challenge

Implement Ingress and Egress Filtering

Introduction

Identify Ingress and Egress Requirements

Compare Filtering Control Points

Configure Firewall Filtering Rules

Challenge

Implement Segmentation and East-West Inspection

Introduction

Understand East-West Cloud Traffic

Plan Cloud Microsegmentation

Apply Segmentation Policy

Challenge

Implement Zero Trust Networking

Introduction

Define Zero Trust Networking

Identify Protected Cloud Resources

Map Users, Workloads, and Access Paths

Apply Least-Privilege Network Access

Challenge

Implement Network Traffic Logging

Introduction

Plan Network Logging Requirements

Enable Traffic Flow Logs

Monitor Allowed and Denied Traffic

Challenge

Monitor Cloud Network Health

Introduction

Why We Monitor Cloud Network Health

Identify Cloud Network Health Signals

Track Latency, Loss, and Throughput

Define Synthetic Monitoring

Challenge

Apply Network Troubleshooting Methodologies

Introduction

Define the Connectivity Problem

Gather and Organize Troubleshooting Evidence

Form and Test Troubleshooting Hypotheses

Apply Isolation and Correlation Techniques

Challenge

Troubleshoot Hybrid and Cloud Connectivity

Introduction

Trace the End-to-End Network Path

Check Routes and Propagation

Troubleshoot Inter-Region Connectivity

Challenge

Troubleshoot Cloud Routing and Path Symmetry

Introduction

Identify the Routing Failure

Review Cloud Route Tables

Trace the Forward Traffic Path

Verify the Return Traffic Path

Troubleshoot Asymmetric Routing

Challenge

Troubleshoot Cloud Addressing Issues

Introduction

Identify the Addressing Problem

Troubleshoot Overlapping IP Ranges

Validate NAT Gateway Behavior

Challenge

Troubleshoot Cloud Application Access

Introduction

Define the Application Access Problem

Trace the Client Access Path

Troubleshoot DNS Resolution

Validate Load Balancers

Challenge

Troubleshoot Security Misconfigurations

Introduction

Identify the Security Control Point

Review Expected Access Requirements

Troubleshoot Security Group Rules

Check Network ACL and Firewall Policy

Challenge

Optimize Cloud Network Performance

Introduction

Define Network Performance Goals

Measure Latency, Loss, and Throughput

Identify Network Bottlenecks

Challenge

Manage Cloud Network Automation and Drift

Introduction

Define the Intended Network State

Automate Network Provisioning

Manage Network Configuration Changes

Detect Cloud Network Drift

Challenge