Document Generated: 03/03/2026

Learning Style: Virtual Classroom

Technology: Citrix

Difficulty: Intermediate

Course Duration: 5 Days

Check Point Certified Security Administrator and Expert Bundle (R81.x)

About this Course:

The CCSA part of the course (Monday to Wednesday) covers everything you need to start-up, configure and manage daily operations of Check Point Security Gateway and Management Software Blades systems on the GAiA operating

system.
The CCTA part of the course (Thursday to Friday) provides an understanding of the concepts and skills necessary to troubleshoot issues that may occur when managing the Check Point Security Management architecture and Security Gateways.

Course Objectives:

CCSA:

• Know how to perform periodic administrator tasks

• Describe the basic functions of the Gaia operating system

• Recognize SmartConsole features, functions, and tools

• Describe the Check Point Firewall infrastructure

• Understand how SmartConsole is used by administrators to grant permissions and user access

• Learn how Check Point security solutions and products work and how they protect networks

• Understand licensing and contract requirements for Check Point security products

• Describe the essential elements of a Security Policy

• Understand the Check Point policy layer concept

• Understand how to enable the Application Control and URL Filtering software blades to block access to various applications

• Describe how to configure manual and automatic NAT

• Identify tools designed to monitor data, determine threats and recognize opportunities for performance improvements

• Identify SmartEvent components used to store network activity logs and identify events

• Know how Site-to-Site and Remote Access VPN deployments and communities work

• Explain the basic concepts of ClusterXL technology and its advantages

CCTA:

• Understand how to use Check Point resources for support.

• Understand how to perform packet captures using tcmdump and FW Monitor command tools.

• Understand the basic process of kernel debugging, and how debug commands are structured.

• Recognize how to use various Linux commands for troubleshooting system issues.

• Recognize communication issues that may occur between SmartConsole and the SMS and how to resolve them.

• Understand how to troubleshoot SmartConsole login and authentication issues.

• Understand how to prevent and resolve licensing and contract issues.

• Understand how to troubleshoot issues that may occur during policy installation.

• Understand communication issues that may occur when collecting logs and how to resolve them.

• Recall various tools to use when analyzing issues with logs.

• Understand how to restore interrupted communications during heavy logging.

• Understand how NAT works and how to troubleshoot issues.

• Understand Client Side and Server Side NAT.

• Understand how the Access Control Policy functions and how the access control applications work together.

• Understand how to troubleshoot issues that may occur with Application Control and URL Filtering. • Understand how the HTTPS Inspection process works and how to resolve issues that may occur during the process.

• Understand how to troubleshoot Content Awareness issues.

• Recognize how to troubleshoot VPN-related issues.

• Understand how to monitor cluster status and work with critical devices.

• Recognize how to troubleshoot State Synchronization.

• Understand how to troubleshoot communication issues between Identity Sources and Security Gateways.

• Understand how to troubleshoot and debug issues with internal Identity Awareness processes.

Audience:

Technical professionals who support, install deploy or administer Check Point products and security administrators and Check Point resellers who need to manage and monitor issues that may occur within their Security Management environment.

Prerequisites:

Working knowledge of Windows, UNIX, networking technology, the Internet and TCP/IP.

Course Outline:

1. CCSA:

   Topics -

   • Security Architecture

   • Admin Operations

   • Deployment

   • Licensing

   • Gaia Portal

   • Hide/Static NAT

   • Firewall Basics

   • Monitoring States

   • ClusterXL

   • Traffic Visibility

   • Security Events

   • Compliance Tasks

   • Threat Detection

   • Policy Layers

   • Site-to-Site VPN

   • Remote Access VPN

• User Access

Exercises -

• Identify key components and configurations

• Create and confirm administrator users for the domain

• Validate existing licenses for products installed on your network

• Create and modify Check Point Rule Base objects

• Demonstrate how to share a layer between Security Policies

• Analyze network traffic and use traffic visibility tools

• Monitor Management Server States using SmartConsole

• Demonstrate how to run specific SmartEvent reports

• Configure a SmartEvent server to monitor relevant patterns

• Configure and deploy a site-to-site VPN

• Configure and test ClusterXL with a High Availability configuration

• Understand how to use CPView to gather gateway information

• Perform periodic tasks as specified in administrator job descriptions

• Test VPN connection and analyze the tunnel traffic

• Demonstrate how to create custom reports

• Demonstrate how to configure event Alerts in SmartEvent

• Utilize various traffic visibility tools to maintain Check Point logs

2. CCTA:

   Course Topics -

   • An Introduction to Troubleshooting

   • SmartConsole and Policy Management Troubleshooting

   • Monitoring Logging Activity

   • Troubleshooting Issues with NAT

• Understanding the Unified Access Control Policy

• Basic VPN Troubleshooting

• Monitoring ClusterXL Connections

• Understanding Identity Awareness

Lab Exercises -

• Monitoring Security Gateway Traffic

• Troubleshooting Issues with SmartConsole

• Troubleshooting Log Connectivity Issues

• Investigating Log Connectivity Issues

• Investigating NAT Issues

• Troubleshooting General Traffic Issues

• Evaluating HTTP and HTTPS Traffic Issues

• Troubleshooting Site-to-Site VPN Issues

• Troubleshooting Clustering Issues

• Troubleshooting Identity Awareness

• Configuring and Testing Identity Collector