CP-CCSA

CHECK POINT CERTIFIED SECURITY ADMINISTRATOR (CCSA) R81.10

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
3 Days	Administrator	Check Point Security	ILT/VILT	CLCs

INTRODUCTION

This three-day course 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.

Learn How To:

‒ Install R80 management and a security gateway in a distributed environment

‒ Configure objects, rules, and settings to define a security policy

‒ Work with multiple concurrent administrators and define permission profiles

‒ Configure a Virtual Private Network and work with Check Point clustering

‒ Perform periodic administrator tasks as specified in administrator job descriptions

AUDIENCE PROFILE

Technical professionals who support, install deploy or administer Check Point products.

PREREQUISITES

Before attending this course, delegates should have Working knowledge of Windows, UNIX, networking technology, the Internet and TCP/IP.

COURSE OBJECTIVES

After completing this course, delegates will be able to:

‒ 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

‒ Describe different Check Point Threat Prevention solutions for network attacks.

‒ Articulate how the Intrusion Prevention System is configured, maintained, and tuned.

– Understand the Infinity Threat Prevention system.

– Knowledge about Check Point's IoT Protect.

MODULES

Topics
– Security Architecture
– Application control
– Deployment
– Licensing
– Gaia Portal
– Hide/Static NAT
– URL Filtering
– Monitoring States
– IoT
– Traffic Visibility
– Security Events
– Threat Extraction
– Threat Emulation
– Policy Layers
– Browser SmartConsole
– Infinity Threat Prevention
– User Access

Exercises
– Identify key components and Configure the Security Management Server.
– Use the WebUI to run the First Time Wizard.
– Install the Smart Console.

– Install the Alpha Gateway using the network detailed in the course topology.
– Demonstrate how the Security Management Server and Gateway
– communicate.
– Test SIC Status.
– Create multiple administrators and apply different roles and
– permissions for simultaneous administration.
– Validate existing licenses for products installed on the network.
– Create and configure host, network, and group objects.
– Create a simplified Security Policy.
– Demonstrate how to use Security Zones in policy.
– Demonstrate how to share a layer between Security Polices.

– Configure Network Address Translation for server and network objects.
– Enable Identity Awareness.
– Deploy user access roles for more granular control of the security Policy.
– Generate network Traffic and use traffic visibility tools to monitor the data.
– Use SmartConsole and SmartView Monitor to view status, alerts, and block suspicious traffic.

ASSOCIATED CERTIFICATIONS & EXAM

This course will prepare delegates to take the Check Point Certified Admin (CCSA) exam #156-215.81, which will validate proficiency across:

– Check Point Technology

– Security Policy Management

– Monitoring Traffic and Connections

– Network Address Translations

– Basic Concepts of VPN

– Managing User Access

– Working with ClusterXL

– Administrator Task Implementation

You will have ninety minutes to answer up to 90 questions.