

CP-CCSA

CHECK POINT CERTIFIED SECURITY ADMINISTRATOR (CCSA) R81.20



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 R81 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

Working knowledge of Unix-like and Windows operating systems and TCP/IP Networking.

COURSE OBJECTIVES

After completing this course, delegates will be able to:

- Identify basic interfaces used to manage the Check Point environment.
- Describe the primary components of a Check Point Three-Tier Architecture and explain how they work together in the Check Point environment.
- Explain how communication is secured and how traffic is routed in the Check Point environment.
- Describe the basic functions of the Gaia operating system.
- Identify the basic workflow to install Security Management Server and Security Gateway for a single-domain solution.
- Create SmartConsole objects that correspond to the organization's topology for use in policies and rules.
- Identify the tools available to manage Check Point licenses and contracts, including their purpose and use.
- Identify features and capabilities that enhance the configuration and management of the Security Policy.
- Explain how policy layers affect traffic inspection.
- Articulate how Network Address Translation affects traffic.
- Describe how to configure manual and automatic Network Address Translation (NAT).
- Demonstrate an understanding of Application Control & URL Filtering and Autonomous Threat Prevention capabilities and how to configure these solutions to meet an organization's security requirements.
- Articulate how pre-shared keys and certificates can be configured to authenticate with third party and externally managed VPN Gateways.

- Describe how to analyze and interpret VPN tunnel traffic.
- Configure logging parameters.
- Use predefined and custom queries to filter log results.
- Identify how to monitor the health of supported Check Point hardware using the Gaia Portal and the command line.
- Describe the different methods for backing up Check Point system information and discuss best practices and recommendations for each method.
- Identify supported upgrade methods and procedures for Security Gateways.

MODULES

Topics

- Security Architecture
- Security Management
- SmartConsole
- Deployment
- Object Management
- Licenses and Contracts
- Policy Rule and Rulebase
- Policy Packages
- Policy Layers
- Traffic Inspection
- Network Address Translation
- Application Control
- URL Filtering
- Logging
- Snapshots
- Backup and Restore
- Gaia

- Permissions
- Policy Installation

Exercises

- Deploying SmartConsole
- Installing a Security Management Server
- Installing a Security Gateway
- Configuring Objects in SmartConsole
- Establishing Secure Internal Communication
- Managing Administrator Access
- Managing Licenses
- Creating a Security Policy
- Configuring Order Layers

- Configuring a Shared Inline Layer
- Configuring NAT
- Integrating Security with a Unified Policy
- Elevating Security with Autonomous Threat Prevention
- Configuring a Locally Managed Site-to-Site VPN
- Elevating Traffic View
- Monitoring System States
- Maintaining the Security Environment

ASSOCIATED CERTIFICATIONS & EXAM

This course will prepare delegates to take the Check Point Certified Admin (CCSA) exam #156-215.81.20, 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.