CP-CCSE

CHECK POINT CERTIFIED SECURITY EXPERT (CCSE) R81.10

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

INTRODUCTION

This advanced three-day Check Point Cyber Security Engineering course provides an understanding of upgrading and advanced configuration of Check Point software blades, installing and managing VPNs (on both internal and external networks), gaining the maximum security from Security Gateways, and resolving Gateway performance issues.

Learn How To:

- Backup your Security Gateway and Management Server
- Build, test and troubleshoot a clustered Security Gateway
- Upgrade and troubleshoot a Management Server
- Configure and maintain security acceleration solutions
- Manage, test and optimize corporate VPN tunnels

AUDIENCE PROFILE

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

PREREQUISITES

Before attending this course, delegates should have successfully completed the CCSA training certification course (R81 Not R77), with working knowledge of Windows and/or UNIX, networking technology, the Internet and TCP/IP.

COURSE OBJECTIVES

After completing this course, delegates will be able to:

- Provide an overview of the upgrade service and options available.
- Explain how to perform management upgrade and migration.
- Articulate the process using CPUSE features.
- Articulate the purpose and function of Management High Availability.
- Explain Primary vs Secondary, Active vs Standby and Synchronization.
- Explain disaster recovery steps in case the primary management server becomes unavailable.
- Provide overview of Central Deployment in SmartConsole.
- Articulate an understanding of Security Gateway cluster upgrade methods.
- Explain about Multi Version Cluster (MVC) upgrades.
- Discuss Gaia Commands and how they are used.
- Explain the main processes on s and s.
- Describe how to work with scripts and SmartTasks to configure automatic actions.
- Explain the Management Data Plane Separation (MDPS)
- Explain kernel operations and traffic flow
- Articulate Dynamic and Updatable Objects in Security Gateways
- Explain the policy installation flow and files used.

- Describe the use of policy installation history.
- Explain concurrent and accelerated install policy.
- Describe an overview of APIs and ways to use and authenticate.
- Explain how to make changes in GAIA and management configuration.
- Explain how to install policy using API.
- Explain how to determine if the configuration is compliant with the best practices.
- Explain how to set action items to meet the compliance.
- Discuss how SmartEvent functions to identify critical security issues.
- Explain how the SecureXL acceleration technology enhances and optimizes Security Gateway performance.
- Describe how the CoreXL acceleration technology enhances and
- improves Security Gateway performance.
- Articulate how utilizing multiple traffic queues can make traffic handling more efficient.
- Discuss Site-to-Site VPN basics, deployment and communities.
- Describe how to analyze and interpret VPN tunnel traffic.
- Explain Link Selection and ISP Redundancy options.
- Explain tunnel management features.
- Discuss Check Point Remote Access solutions and how they differ from each other.
- Describe how client security can be provided by Remote Access.
- Explain authentication methods including machine authentication.
- Explain Multiple Entry Point (MEP).
- Discuss the Mobile Access Software Blade and how it secures communication and data exchange during remote connections.
- Describe Mobile Access deployment options.
- Discuss various features in Mobile Access like Portals, Link
- Translation, running Native Applications, Reverse Proxy and more.
- Explain basic concepts of Clustering and ClusterXL.
- Explain about Cluster Control Protocol (CCP) and synchronization.
- Describe advanced ClusterXL functions and modes like Load Sharing,
- Active-Active, VMAC mode etc.
- Discuss Cluster Correction Layer (CCL) to provide connection stickyness.
- Advanced Logs and Monitoring
- Describe the components of SmartEvent and their deployment options.
- Discuss how SmartEvent can assist in reporting security threats.
- Explain how to customize event definitions and set an Event Policy.

MODULES

Topics

- Management Upgrade and Migration
- Management High Availability
- Security Gateway Upgrades
- Advanced Check Point Maintenance
- Security Gateway Operations
- Policy installation
- Gaia and Management APIs
- Acceleration
- Site-to-Site VPN
- Remote Access VPN
- Mobile Access VPN
- Clustering
- Advanced Logs and Monitoring

Exercises

- Prepare for a Security Management Server Upgrade
- Upgrade the Security Management Server
- Deploy a Secondary Security Management Server
- Configure a Distributed Log Server
- Upgrade a Security Gateway from SmartConsole
- Work with the Command Line
- Use Scripts and SmartTasks

- Configure Dynamic Objects
- Monitor Traffic
- Verify Policy Installation and Status
- Work with Gaia and Management APIs
- Work with Acceleration Features
- Configure a Locally Managed Site to Site VPN
- Configure a Site-to-Site VPN with an Interoperable Device
- Configure Remote Access VPN
- Configure Mobile Access VPN
- Configure a High Availability Cluster
- Work with ClusterXL
- Configure Policy Compliance
- Deploy SmartEvent

ASSOCIATED CERTIFICATIONS & EXAM

The Check Point Certified Security Engineering #156-315.81 exam covers the following topics:

- Check Point Technology Overview
- Deployment Platforms and Security Policies
- Monitoring Traffic and Connections
- Network Address Translations
- User Management and Authentication
- Using SmartUpdate
- Implementing Identity Awareness
- Configuring VPN tunnels
- Resolving security administration issues