

CP-CCSE

CHECK POINT CERTIFIED SECURITY EXPERT (CCSE) R81.20



DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
3 Days	Expert	Check Point Security	ILT/MILT	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 architect, upgrade, maintain, and support Check Point products.

PREREQUISITES

CCSA Training or Certification, fundamental Unix and Windows knowledge, certificate management experience, system administration and networking knowledge.

COURSE OBJECTIVES

After completing this course, delegates will be able to:

- Provide an overview of the upgrade service and options available.
- Identify basic interfaces used to manage the Check Point environment.
- Identify the types of technologies that Check Point supports for automation.
- Explain the purpose of the Check Management High Availability (HA) deployment.
- Identify the workflow followed to deploy a Primary and solution Secondary servers.
- Explain the basic concepts of Clustering and ClusterXL, including protocols, synchronization, connection stickyness.
- Identify how to exclude services from synchronizing or delaying synchronization.
- Explain the policy installation flow.
- Explain the purpose of dynamic objects, updatable objects, and network feeds.
- Understand how to manage user access for internal and external users.
- Describe the Identity Awareness components and configurations.
- Describe different Check Point Threat Prevention solutions.
- Articulate how the Intrusion Prevention System is configured.
- Obtain knowledge about Check Point's IoT Protect.
- Explain the purpose of Domain-based VPNs.
- Describe situations where externally managed certificate authentication is used.

- Describe how client security can be provided by Remote Access.
- Discuss the Mobile Access Software Blade.
- Explain how to determine if the configuration is compliant with the best practices.
- Define performance tuning solutions and basic configuration workflow.
- Identify supported upgrade and migration methods and procedures for Security Management Servers and dedicated Log and SmartEvent Servers.
- Identify supported upgrade methods and procedures for Security Gateways.

MODULES

Topics

- Security Architecture
- Advanced Deployments
- Management High Availability
- Advanced Gateway Deployment
- Advanced Policy Configuration
- Advanced User Access Management
- Custom Threat Protection
- Advanced Site-to-Site VPN
- Remote Access VPN
- Mobile Access VPN
- Advanced Security Monitoring
- Performance Tuning
- Advanced Security Maintenance

Exercises

- Navigate the Environment and Using the Management API
- Deploy Secondary Security Management Server
- Configure a Dedicated Log Server
- Deploy SmartEvent
- Configure a High Availability Security Gateway Cluster
- Work with ClusterXL
- Configure Dynamic and Updateable Objects
- Verify Accelerated Policy Installation and Monitoring Status
- Elevate Security with HTTPS Inspection
- Deploy Identity Awareness

- Customize Threat Prevention
- Configure a Site-to-Site VPN with an Interoperable Device
- Deploy Remote Access VPN
- Configure Mobile Access VPN
- Monitor Policy Compliance
- Report SmartEvent Statistics
- Tuning Security Gateway Performance

ASSOCIATED CERTIFICATIONS & EXAM

The Check Point Certified Security Engineering #156-315.81.20 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