COURSE OUTLINE

CP-CCSE
CHECK POINT CERTIFIED SECURITY EXPERT (CCSE) R82

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

INTRODUCTION

This course provides students with the advanced knowledge, skills, and hands-on experience needed to deploy, manage, and monitor existing Quantum Security Environments. Students will learn how to deploy Management High Availability, provide advanced policy management, configure Site-to-Site VPN, provide advanced security monitoring, upgrade a Security Gateway, use Central Deployment tool to install hotfixes, perform an import of a Primary Security Management Server and Deploy ElasticXL Cluster.

AUDIENCE PROFILE

This course is intended for Security Engineers, Security Analysts, Security Consultants and Security Architects.

PREREQUISITES

Before attending this course, delegates must have base knowledge of the following:

- Unix-like and/or Windows OS
- Internet Fundamentals
- Networking Fundamentals
- Networking Security
- System Administration
- TCP/IP Networking
- Text Editors in Unix-like OS
- Minimum of 6-months of practical experience with the management of a Quantum Security
- Environment.

Check Point Courses:

- Check Point Certified Security Administrator (required)
- Check Point Deployment Administrator (suggested)

COURSE OBJECTIVES

After completing this course, delegates will be able to:

- Learn to configure and manage advanced settings on Check Point Security Gateways.
- Implement clustering for high availability and load balancing.
- Master the process of upgrading Security Gateways and Management Servers.
- Troubleshoot issues related to upgrades and system performance.
- Configure, manage, and troubleshoot VPNs for both internal and external networks.
- Optimize VPN performance and ensure secure connectivity.
- Implement and maintain security acceleration technologies like SecureXL and CoreXL.
- Analyze and improve gateway performance using diagnostic tools.
- Perform backups and restores of Security Gateways and Management Servers.
- Understand disaster recovery strategies and best practices.
- Refine and optimize security policies for complex environments.
- Use advanced rulebase features to enhance security posture.
- Utilize SmartView Tracker and SmartLog for real-time monitoring and analysis.
- Generate and interpret security reports for auditing and compliance.

MODULES

Module 1: Management High Availability

- Explain the purpose of Management High Availability.
- Identify the essential elements of Management High Availability.

Lab Exercises

- Deploy and Configure Management High Availability
- Ensure the failover process functions as expected

Module 2: Advanced Policy Management

- Identify ways to enhance the Security Policy with more object types.
- Create dynamic objects to make policy updatable from the Gateway.
- Manually define NAT rules.
- Configure Security Management behind NAT.

Lab Exercises

- Use Updatable Objects
- Configure Network Address Translation for server and network objects
- Configure Management behind NAT for Branch Office connections

Module 3: Site-to-Site VPN
- Discuss site-to-site VPN basics, deployment, and communities.
- Describe how to analyze and interpret VPN tunnel traffic.
- Articulate how pre-shared keys and certificates can be configured to authenticate with third-party and externally managed VPN Gateways.
- Explain Link Selection and ISP Redundancy options.
- Explain tunnel management features.

Lab Exercise
- Configure Site-to-Site VPN with internally managed
- Security Gateways

Module 4: Advanced Security Monitoring
- Describe the SmartEvent and Compliance Blade solutions, including their purpose and use.

Lab Exercise
- Configure a SmartEvent Server to monitor relevant patterns and events
- Demonstrate how to configure Events and Alerts in SmartEvent
- Demonstrate how to run specific SmartEvent reports
- Activate Compliance Blade
- Demonstrate Security Best Practice settings and alerts
- Demonstrate Regulatory Requirements Compliance Scores

Module 5: Upgrades
- Identify supported upgrade options.

Lab Task
- Upgrade a Security Gateway
- Use Central Deployment tool to install Hotfixes

Module 6: Advanced Upgrades and Migrations
- Export/import a Management Database.
- Upgrade a Security Management Server by freshly
- deploying the new release or using a new appliance.

Lab Exercise
- Prepare to perform an Advanced Upgrade with Database
- Migration on the Primary Security Management Server in a distributed environment
- Perform an import of a Primary Security Management Server in a distributed Check Point environment

Module 7: ElasticXL Cluster
- Describe the ElasticXL Cluster solution, including its purpose and use.

Lab Exercise
- Deploy an ElasticXL Security Gateway Cluster

ASSOCIATED CERTIFICATIONS & EXAM

This course prepares delegates for the Check Point Certified Security Engineering #156-315.82 exam.