Check Point Certified Security Expert
R81.20 (CCSE)

Course 9792 – 24 Hours

Overview

This course's goal is to learn advanced concepts and develop skills necessary to design, deploy, and upgrade Check Point Security environments

Who Should Attend?

Technical professionals who architect, upgrade, maintain, and support Check Point products.

Prerequisites

- Basic CCSA, Unix, and Windows training or certification
- Knowledge and experience in managing certificates, managing systems, and knowledge networks

Objectives

- Identification of basic interfaces used to manage a checkpoint environment
- Identifying the types of technologies in which Check Point supports automation
- Explain the purpose of deploying high availability (HA) management.
- Identify the workflow followed for deploying a primary server and a secondary solution
- Explain the basic concepts of Clustering and Cluster XL, including protocols, synchronization, connection stickiness
- Identify how to exclude services from synchronization or delay Explain the policy installation flow
- Explain the purpose of dynamic objects, updateable objects, and grid feeds
- Understanding how to manage user access for internal and external users
- Getting to know the components and configurations of identity awareness

- Description of various solutions to prevent checkpoint threats
- Articulating how an intrusion prevention system is defined
- Obtaining knowledge about Check Point's IoT Protect
- Explain the purpose of domain-based VPNs
- Description of situations where externally managed certificate verification is used
- Description of how remote access can provide client security
- Discuss the Mobile Access Software Blade
- Explain how to determine if the configuration conforms to best practices
- Defining performance tuning solutions and basic configuration workflow
- Identify supported upgrade and migration methods and procedures for security management servers and dedicated smart event and log servers
- Identify supported upgrade methods and procedures for security gateways

Topics

- 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 use the management API
- Deployment of a secondary security management server
- Setting up a dedicated log server
- SmartEvent layout
- Setting up a high-availability security gateway cluster
- Working with Cluster XL

- Defining dynamic and updatable objects
- Checking the status of the accelerated monitoring and installing the policy
- Increased security with HTTPS inspection
- Deployment of identity awareness
- Customize threat prevention
- Setting up a site-to-site VPN with a shared device
- Remote access VPN deployment
- Setting up a VPN for mobile access
- Monitoring policy compliance
- Report smart event statistics
- Security gateway performance tuning