Check Point Security Administrator

Master the skills to deploy and manage Check Point Software Blade Architecture

Check Point Security Administrator is a foundation course for Check Point's Security Management and Gateway Systems. This 4-day course provides hands-on training to attain the skills necessary to configure R71 Check Point Software Blades including Firewall, IPSEC VPN, IPS, Network Policy Management, Logging & Status, and Monitoring, URL Filtering, Antivirus/Anti-malware, Anti-spam & Email Security. During this course, students will configure a Security Policy, secure communications across the Internet and defend against network threats.

WHO SHOULD ATTEND?

Technical persons who support, install, deploy or administer Check Point Software Blades should attend this course. This could include the following:
- System Administrators
- System Engineers
- Security Managers
- Network Engineers
- Anyone seeking CCSA certification

PREREQUISITES

Persons attending this course should have a working knowledge of networking concepts, Windows Server and/or UNIX, and experience with TCP/IP and the Internet.

COURSE TOPICS
- Check Point Technology Overview
- Check Point Software Blades
- Deployment Platforms
- Introduction to Security Policy
- Monitor Traffic and Connections
- Use SmartUpdate
- Upgrade to R71
- User Management and Authentication
- Encryption and VPNs
- Introduction to VPNs
- Messaging and Content Security
- Check Point IPS

COURSE OBJECTIVES INCLUDE
- Design a distributed environment
- Install the Security Gateway version R71 in a distributed environment
- Deploy Gateways from the Gateway command line
- Perform a backup and restore the current Gateway installation
- Use the Command Line to support troubleshooting common problems on the Security Gateway
- Create a basic Rule Base in SmartDashboard
- Configure NAT rules on Web and Gateway servers
- Use queries in SmartView Tracker to monitor IPS traffic and troubleshoot events using packet data
- Upgrade and attach product licenses using SmartUpdate
- Perform a preinstallation compatibility assessment for upgrading to R71
- Manage users to access to the corporate LAN
- Establish VPN connections to partner sites with advanced IKE
- Configure permanent tunnels for remote access to corporate resources
- Configure Web-filtering and antivirus policies to filter traffic
- Create and install IPS policies

LAB EXERCISES INCLUDE
- Install and configure a Security Management Server
- Configure a Security Gateway
- Launch SmartDashboard
- Configure a Branch Gateway
- Create Rules for Corporate Gateway
- Create a DMZ Object
- Observe NAT using fw monitor
- Launch SmartView Tracker
- Download HFA Package
- Create a VPN Community
- Test VPN Connection
- Save a Certificate for Export
- Modify Rule Base
- Install and Verify Security Gateway Configuration
- Test Encryption with Certificates
- Create a Remote Access Group
- Configure Office Mode IP Pool
- Test Remote Connection
- Analyze Attacks
- Configure IPS to Block Attacks

CERTIFICATION INFORMATION

This course helps prepare for CCSA R71 exam # 156-215.71 available at VUE test centers. It contains 90 multiple-choice, scenario-based questions. A passing score is 70% or higher in 120 minutes. The exam is based on 80% course materials and 20% hands-on experience with Check Point products. Students should have at least 6 months experience before challenging it.

www.companyname.com
Company Name | 12345 Street name, City name, State 12345
email: name@companyname.com | Phone: (000)000-000