



Training: Check Point
Check Point Cybersecurity Boot Camp (CCSB)



TRAINING GOALS:

The Check Point Cybersecurity Boot Camp (CCSB) is a volume comprised of the Check Point Certified Security Administrator (CCSA) course and a modified Check Point Certified Security Expert (CCSE) course.

Learn basic and advanced concepts and develop skills necessary to administer IT security fundamental and intermediate tasks.

COURSE OBJECTIVES – SECURITY ADMINISTRATOR PART

- Describe the primary components of a Check Point Three-Tier Architecture and explain how they work together in the Check Point environment.
- Identify the basic workflow to install Security Management Server and Security Gateway for a single-domain solution.
- Create SmartConsole objects that correspond to the organization's topology for use in policies and rules.
- Identify the tools available to manage Check Point licenses and contracts, including their purpose and use.
- Identify features and capabilities that enhance the configuration and management of the Security Policy.
- Demonstrate an understanding of Application Control & URL Filtering and Autonomous Threat Prevention capabilities and how to configure these solutions to meet an organization's security requirements.
- Describe how to analyze and interpret VPN tunnel traffic.
- Identify how to monitor the health of supported Check Point hardware using the Gaia Portal and the command line.
- Describe the different methods for backing up Check Point system information and discuss best practices and recommendations for each method.

COURSE OBJECTIVES – SECURITY EXPERT PART

- Identify the types of technologies that Check Point supports for automation.
- Explain the purpose of the Check Management High Availability (HA) deployment.
- Explain the basic concepts of Clustering and ClusterXL, including protocols, synchronization, and connection stickiness.
- Explain the purpose of dynamic objects, updatable objects, and network feeds.





- Describe the Identity Awareness components and configurations.
- Describe different Check Point Threat Prevention solutions.
- Articulate how the Intrusion Prevention System is configured.
- 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.
- Define performance tuning solutions and basic configuration workflow.
- Identify supported upgrade methods and procedures for Security Gateways.

WHO SHOULD ATTEND?

Technical professionals and experts who support, administer, or perform advanced deployment configurations of Check Point products.

CONSPECT:

- Security Management
- SmartConsole
- Deployment
- Object Management
- Licenses and Contracts
- Policy Rules and Rulebase
- Policy Packages
- Policy Layers
- Traffic Inspection
- Network Address Translation
- Application Control
- URL Filtering
- Logging
- Snapshots
- Backup and Restore
- Gaia
- Permissions
- Policy Installation
- 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
- Lab Exercises
 - Deploy SmartConsole
 - Install a Security Management Server
 - Install a Security Gateway
 - Configure Objects in SmartConsole
 - Establish Secure Internal Communication
 - Manage Administrator Access
 - Manage Licenses
 - Create a Security Policy
 - Configure Order Layers
 - Configure a Shared Inline Layer
 - Configure NAT
 - Integrate Security with a Unified Policy
 - Elevate Security with Autonomous Threat Prevention
 - Configure a Locally Managed Site-to-Site VPN
 - Elevate Traffic View
 - Monitor System States
 - Maintain the Security Environment
 - Navigate the Environment and Use 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
- Tune Security Gateway Performance

REQUIREMENTS:

One-year experience on Check Point products. Working knowledge of Windows, UNIX, networking technology, the Internet and TCP/IP is recommended.

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Check Point Software Technologies Ltd. (course completion).

This course additionally helps prepare for CCSA [#156-215.81](#) and CCSE [#156-315.81](#) exams available at Pearson VUE test centers.

TRAINER:

Authorized Check Point Software Technologies Ltd. Trainer

