

# Check Point Cyber Security Administrator and Engineering Bundle

---

<b>Code:</b>	CCSA+CCSE R80.20
<b>Length:</b>	5 days
<b>URL:</b>	<a href="#">View Online</a>

---

This special CCSA and CCSE bundle covering Check Point Security Administration & Engineering (R80.20) provides you with an understanding of the basic concepts and skills necessary to configure Check Point Security Gateway and Management Software Blades. CCSA-R80.20: The goal of this course is to provide an understanding of basic concepts and skills necessary to configure Check Point Security Gateway and Management Software Blades. CCSE-R80.20: The goal of this course is to provide an understanding and skills necessary to configure and optimally manage Check Point Next Generation Firewalls.

## Skills Gained

- Introduction to Check Point Technology
- Security Policy Management
- Policy Layers
- Check Point Security Solutions and Licensing
- Traffic Visibility
- Basic Concepts of VPN
- Managing User Access
- Working with ClusterXL
- Administrator Task Implementation
- System Management
- Automation and Orchestration
- Redundancy
- Acceleration
- SmartEvent
- Mobile and Remote Access
- Threat Prevention

## Who Can Benefit

This special combo or bundle course is recommended for Systems Administrators, Network Engineers, Security Managers, Support Analysts and any other IT professional working with Check Point Software Blades or seeking CCSA and CCSE certifications.

## Prerequisites

- General knowledge of TCP/IP
- Working knowledge of Windows, UNIX, networking, TCP/IP, and the Internet

# Course Details

## CCSA Course Outline

- Interpret the concept of a Firewall and understand the mechanisms used for controlling network traffic.
- Describe the key elements of Check Point's unified Security Management Architecture.
- Recognize SmartConsole features, functions and tools.
- Understand Check Point deployment options.
- Describe the basic functions of Gaia.
- Describe the essential elements of a Security Policy.
- Understand how traffic inspection takes place in a unified Security Policy.
- Summarize how administration roles and permissions assist in managing policy.
- Recall how to implement backup techniques.
- Understand the Check Point policy layer concept.
- Recognize Check Point security solutions and products and how they work to protect your network.
- Understand licensing and contract requirements for Check Point security products.
- Identify tools designed to monitor data, determine threats and recognize performance improvements.
- Identify tools designed to respond quickly and efficiently to changes in gateways, tunnels, remote users, traffic flow patterns, and other activities.
- Understand Site-to-Site and Remote Access VPN deployments and communities.
- Understand how to analyze and interpret VPN traffic.
- Recognize how to define users and user groups.
- Understand how to manage user access for internal and external users.
- Understand the basic concepts of ClusterXL technology and its advantages.
- Understand how to perform periodic administrator tasks as specified in administrator job descriptions.

## CCSA Lab Exercises

- Working with Gaia Portal
- Modifying an Existing Security Policy
- Configuring Hide and Static NAT
- Managing Administrator Access
- Installing and Managing a Remote Security Gateway
- Managing Backups
- Defining Access Control Policy Layers Defining and Sharing Security Policy Layers
- Working with Licenses and Contracts
- Working with Check Point Logs
- Maintaining Check Point Logs
- Configuring a Site-to-Site VPN
- Providing User Access
- Working with Cluster XL
- Verifying Network Compliance
- Working with CP View

## CCSE Course Outline

- Identify advanced CLI commands.
- Understand system management procedures, including how to perform system upgrades and apply patches and hotfixes.
- Describe the Check Point Firewall infrastructure.
- Describe advanced methods of gathering important gateway data using CPView and CPInfo.
- Recognize how Check Point's flexible API architecture supports automation and orchestration.
- Discuss advanced ClusterXL functions.
- Describe VRRP network redundancy advantages.
- Understand how SecureXL acceleration technology is used to enhance and improve performance.
- Understand how CoreXL acceleration technology is used to enhance and improve performance.
- Identify the SmartEvent components that store network activity logs and identify events.
- Discuss the SmartEvent process that determines which network activities may lead to security issues.
- Understand how SmartEvent can assist in detecting, remediating, and preventing security threats.
- Discuss the Mobile Access Software Blade and how it secures communication and data.
- Understand Mobile Access deployment options.
- Recognize Check Point Remote Access solutions.
- Discuss Check Point Capsule components and how they protect mobile devices and business documents.
- Discuss different Check Point Solutions for attacks such as zero-day and Advanced Persistent Threats.
- Understand how SandBlast, Threat Emulation, and Threat Extraction prevent security incidents.
- Identify how Check Point Mobile Threat Prevention can help protect data accessed on company-issued smartphones and tablets.

## CCSE Lab Exercises

- Upgrading a Security Management Server to R80.20
  - Applying Check Point Hotfixes
  - Configuring a New Security Gateway Cluster
  - Core CLI Elements of Firewall Administration
  - Configuring Manual Network Address Translation
  - Managing Objects Using the Check Point API
  - Enabling Check Point VRRP
  - Deploying a Secondary Security Management Server
  - Viewing the Chain Modules
  - Working with SecureXL
  - Working with CoreXL
  - Evaluating Threats with SmartEvent
  - Managing Mobile Access
  - Understanding IPS Protections
  - Deploying IPS Geo Protection
  - Reviewing Threat Prevention Settings and Protections
  - Deploying Threat Emulation and Threat Extraction
-

ExitCertified® Corporation and iMVP® are registered trademarks of ExitCertified ULC and ExitCertified Corporation and Tech Data Corporation, respectively  
Copyright ©2020 Tech Data Corporation and ExitCertified ULC & ExitCertified Corporation.  
All Rights Reserved.

Generated 9