FT-CCSE-CCTE – CheckPoint Certified Security Expert and Troubleshooting Expert Fast Track (CCSE+CCTE) Bundle

CheckPoint Fast Track Bundle

–

Check Point Certified Security Expert (CCSE) R80.40 – Updated 2021

+

Check Point Certified Troubleshooting Expert (CCTE)

About this Course

- Save 20% on your CCSE + CCTE Certification with this Fast Track Bundled Offer.
- Five-day course covers everything you need to start-up, configure and manage daily operations of Check Point Security Gateway and Management Software Blades systems on the GAiA operating system.
- Learn basic concepts and develop skills necessary to administer IT security fundamental tasks.
- Security Architecture
- Admin Operations
- Deployment
- Licensing
- Gaia Portal
- Hide/Static NAT
- Firewall Basics Monitoring States
- ClusterXL Traffic Visibility
- Security Events
- Compliance Tasks
- Threat Detection Policy Layers
- Site-to-Site VPN
- Remote Access VPN User Access
- Provide advanced troubleshooting skills to investigate and resolve more complex issues that may occur while managing your Check Point Security environment.
  Advanced Troubleshooting
  Management Database and Processes
  Advanced Kernel Debugging
  User Mode Troubleshooting

Advanced Access Control
Understanding Threat Prevention
Advanced VPN Troubleshooting
Acceleration and Performance Tuning

Course Goals/Skills

- Know how to perform periodic administrator tasks
  • Describe the basic functions of the Gaia operating system
  • Recognize SmartConsole features, functions, and tools .
  • Describe the Check Point Firewall infrastructure
  • Understand how SmartConsole is used by administrators to grant permissions and user access
  • Learn how Check Point security solutions and products work and how they protect networks
  • Understand licensing and contract requirements for Check Point security products
  • Describe the essential elements of a Security Policy
  • Understand the Check Point policy layer concept
  • Understand how to enable the Application Control and URL Filtering software blades to block access to various applications
  • Describe how to configure manual and automatic NAT
  • Identify tools designed to monitor data, determine threats and recognize opportunities for performance improvements
  • Identify SmartEvent components used to store network activity logs and identify events
  • Know how Site-to-Site and Remote Access VPN deployments and communities work
  • Explain the basic concepts of ClusterXL technology and its advantages

- Understand how to use Check Point resources for support.
  Understand how to perform packet captures using tcpdump and FW Monitor command tools.
  Understand the basic process of kernel debugging, and how debug commands are structured.
  Recognize how to use various Linux commands for troubleshooting system issues.
  Recognize communication issues that may occur between SmartConsole and the SMS and how to resolve them.
  Understand how to troubleshoot SmartConsole login and authentication issues.
  Understand how to prevent and resolve licensing and contract issues.
  Understand how to troubleshoot issues that may occur during policy installation.
  Understand communication issues that may occur when collecting logs and how to resolve them.
  Recall various tools to use when analyzing issues with logs.
  Understand how to restore interrupted communications during heavy logging.
  Understand how NAT works and how to troubleshoot issues.
  Understand Client Side and Server Side NAT.
  Understand how the Access Control Policy functions and how the access control applications work together.
  Understand how to troubleshoot issues that may occur with Application Control and URL Filtering.
  Understand how the HTTPS Inspection process works and how to resolve issues that may occur during the process.
  Understand how to troubleshoot Content Awareness issues.
  Recognize how to troubleshoot VPN-related issues.
  Understand how to monitor cluster status and work with critical devices.
  Recognize how to troubleshoot State Synchronization.
  Understand how to troubleshoot communication issues between Identity Sources and Security Gateways.
  Understand how to troubleshoot and debug issues with

internal Identity Awareness processes.

Intended Audience

- Technical professionals who need to deploy and manage Endpoint Security within their security environment.

Course Format

Classic – Classroom Training

Live Virtual (Online) with Instructor

Language: English or Bulgarian

Course Materials:Digital Format. Lifetime Access. Official Learning Material from Check Point.

Lab: Individual Environment for each Delegate.

All Recordings Session (24/7)

Certificate of Course Completion

Course Duration

- 5 working days (09:00 – 17:00 / 9:00 am – 5:00 pm) UTC +2 (contact us for another Time Zone)

or

- **40 learning hours after hours (2 weeks, classes are held 4 times a week in one of the following options):**
- Sat. and Sun. 10:00 – 14:00 or 14:00 – 18:00 or 18:00 – 22:00
- Mon. and Wed. 19:00 – 23:00
- Tue. or Thu. 19:00 – 23:00

Payments

CLC

[You can enroll with your Check Point Learning Credits.]

If you are Check Point Partner you can also get free training via the [Co-op Program]. Check your eligibility and request funds [here] or For any further questions or additional

assistance, please E-Mail: Coop@checkpoint.com

We provide Invoices for Company Sponsored Trainings.

Invoices can be requested up to 7 days after the payment.

Course Schedules

[tribe_events_list category="check-point"]

[tribe_event_countdown slug="ccsa" show_seconds="yes"]

If you dont see a date, contact us.

All classes are confirmed individually after enrollment.

Course Prerequisites

- Basic knowledge of networking
- 6 months to 1 year of experience with Check Point products recommended

---

This Training will Prepare you to take the following Certification Exams (exam price included)

- Check Point Certified Security Expert (CCSE) R80.x
- Check Point Certified Troubleshooting Expert (CCTE)

- You can Certify Online or at our Test Center.

Course Objectives:

• Identify key components and configurations
• Create and confirm administrator users for the domain
• Validate existing licenses for products installed on your network
• Create and modify Check Point Rule Base objects
• Demonstrate how to share a layer between Security Policies
• Analyze network traffic and use traffic visibility tools
• Monitor Management Server States using SmartConsole
• Demonstrate how to run specific SmartEvent reports
• Configure a SmartEvent server to monitor relevant patterns
• Configure and deploy a site-to-site VPN
• Configure and test ClusterXL with a High Availability configuration
• Understand how to use CPView to gather gateway information
• Perform periodic tasks as specified in administrator job descriptions
• Test VPN connection and analyze the tunnel traffic
• Demonstrate how to create custom reports
• Demonstrate how to configure event Alerts in SmartEvent
• Utilize various traffic visibility tools to maintain Check Point logs

- Understand how to use Check Point resources for support.
  Understand how to perform packet captures using tcpdump and FW Monitor command tools.
  Understand the basic process of kernel debugging, and how debug commands are structured.
  Recognize how to use various Linux commands for

troubleshooting system issues.
Recognize communication issues that may occur between SmartConsole and the SMS and how to resolve them.
Understand how to troubleshoot SmartConsole login and authentication issues.
Understand how to prevent and resolve licensing and contract issues.
Understand how to troubleshoot issues that may occur during policy installation.
Understand communication issues that may occur when collecting logs and how to resolve them.
Recall various tools to use when analyzing issues with logs.
Understand how to restore interrupted communications during heavy logging.
Understand how NAT works and how to troubleshoot issues.
Understand Client Side and Server Side NAT.
Understand how the Access Control Policy functions and how the access control applications work together.
Understand how to troubleshoot issues that may occur with Application Control and URL Filtering.
Understand how the HTTPS Inspection process works and how to resolve issues that may occur during the process.
Understand how to troubleshoot Content Awareness issues.
Recognize how to troubleshoot VPN-related issues.
Understand how to monitor cluster status and work with critical devices.
Recognize how to troubleshoot State Synchronization.
Understand how to troubleshoot communication issues between Identity Sources and Security Gateways.
Understand how to troubleshoot and debug issues with internal Identity Awareness processes.