

CP-CCTE CHECK POINT CERTIFIED TROUBLESHOOTING EXPERT R82



DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
2 Days	Expert	Infinity Specialisation	ILT/MLT	IGS

INTRODUCTION

The Check Point Certified Troubleshooting Expert (CCTE) provides advanced troubleshooting skills to investigate and resolve more complex issues that may occur while managing your Check Point security environment. Following an initial introduction, the curriculum moves through deep-dive modules focusing on the Security Management Server, Logs and Events, and Security Gateways. Participants will then master advanced troubleshooting for the Firewall Kernel, Access Control, NAT, Identity Awareness, and Site-to-Site VPN to ensure peak performance and stability across the entire security stack.

AUDIENCE PROFILE

This course is designed for security experts and Check Point resellers who desire to obtain the necessary knowledge required to perform more advanced troubleshooting skills while managing their security environments.

PREREQUISITES

Working knowledge of UNIX and/or Windows operating systems, Working knowledge of Networking, TCP/IP Networking, Bash Scripting in Unix-like OS, Text Editors in Unix-like OS, CCSE training/certification, Advanced knowledge of Check Point Security Products.

Check Point Courses

- Recommended Preparation:
 - Check Point Security Expert (CCSE)
- Suggested for Enhanced Learning:
 - Check Point Deployment Administrator (CPDA)
 - Check Point Security Administrator (CCSA)

COURSE OBJECTIVES

Provide advanced troubleshooting skills to investigate and resolve more complex issues that may occur while managing your Check Point Security environment.

- Identify and use Linux-based and Check Point commands and tools for system monitoring, file editing, and file viewing.
- Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Management Server and API Server issues.
- Investigate and troubleshoot traffic or security-related issues using logs and events monitoring tools.
- Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Security Gateway issues.
- Demonstrate an understanding of advanced troubleshooting tools and techniques for kernel debugging.
- Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Access Control issues.
- Investigate and troubleshoot NAT (Network Address Translation) issues.
- Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Identity Awareness issues.
- Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Site-to-Site VPN Troubleshooting issues.

MODULES

Topics

Module 1: Introduction to Advanced Troubleshooting
Lab Tasks:

- Simplify the Security Policies
- Examine the System Resources on the Security Gateways

- Examine the System Resources on the Security Management Servers
- Review CPView System Statistics
- Change the Refresh Rate of CPView
- Examine Historical CPView Data

Module 2: Advanced Security Management Server Troubleshooting
Lab Tasks:

- Troubleshoot SmartConsole Issues
- Determine the Management Condition
- Restore the Environment

Module 3: Advanced Troubleshooting with Logs and Events

Lab Tasks:

- Troubleshoot the Log Connection
- Troubleshoot SmartLog
- Restore the Environment

Module 4: Advanced Security Gateway Troubleshooting

Lab Tasks:

- Troubleshoot SIC Communication
- Troubleshoot Security Gateway Processes
- Restore the Environment

Module 5: Advanced Firewall Kernel Debugging

Lab Tasks:

- Determine the Traffic Flow
- Evaluate Traffic Issues with Basic Kernel Debugs

- Troubleshoot Traffic Issues with Advanced Kernel Debugs
- Restore the Environment

Module 6: Advanced Access Control Troubleshooting

Lab Tasks:

- Increase the Log Detail
- Repeat the Test
- Debug the Unified Policy Module
- Restore the Environment

Module 7: Advanced NAT Troubleshooting

Lab Tasks:

- Analyze Hide NAT Traffic Using Packet Captures
- Troubleshoot Static NAT Configuration with SmartConsole
- Examine Static NAT Traffic Using Packet Captures

Module 8: Advanced Identity Awareness Troubleshooting

Lab Tasks:

- Verify the Initial Problem
- Examine the Security Gateway for Configuration Issues
- Reconfigure Identity Awareness
- Test the New Rules
- Complete the Changes

Module 9: Advanced Site-to-Site VPN Troubleshooting

Lab Tasks:

- Troubleshoot IKE Issues
- Examine Configuration Issues
- Restore the Environment

ASSOCIATED CERTIFICATIONS & EXAM

This course prepares delegates to write the Check Point Certified Troubleshooting Expert #156.588 exam. A valid or expired CCSE certification is required to take the CCTE exam.