

CP-CCTA



CHECK POINT CERTIFIED TROUBLESHOOTING ADMINISTRATOR

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
2 Days	Specialist	Infinity Specialisation	ILT/VILT	IGS

INTRODUCTION

This course provides students with the fundamental skills to effectively troubleshoot Quantum Security Management Servers and Security Gateways that run on the Gaia operating system. After an introduction to troubleshooting, the fundamentals of traffic monitoring and packetcaptures are covered followed by packet capture analysis using both CII and Wireshark. The focus then shifts to processes, SmartConsole, log collection, Identity Awareness, and Application Control and URL Filtering troubleshooting.

AUDIENCE PROFILE

- Security Administrators
- Security Engineers
- Security Analysts
- Security Consultants
- Security Architects

PREREQUISITES

- Unix-like and/or Windows OS
- Internet Fundamentals
- Networking Fundamentals
- Networking Security
- System Administration
- TCP/IP Networking
- Text Editors in Unix-like OS

COURSE OBJECTIVES

After completing this course, delegates will be able to:

- Apply a symptom-based method with the OSI model to isolate issues.
- Capture traffic with fw monitor, tcpdump, and CLI tools, including on Software Blades.
- Analyze captures with CLI tools to verify policy, NAT, and routing behavior.
- Analyze packet captures in Wireshark using marks, statistics, and expert information.
- Monitor logs and troubleshoot log collection using structured scenarios.
- Troubleshoot Check Point user-space and kernel-space processes, including the User Space Firewall.
- Resolve SmartConsole issues using guided troubleshooting workflows.
- Troubleshoot Identity Awareness using updated ports and pdp/pep commands.
- Troubleshoot Application Control and URL Filtering with improved workflows

COURSE CONTENT

Module 1: Introduction to Troubleshooting

- Identify the principles of troubleshooting methodology.
- Understand how to use the OSI (Open Systems Interconnection) model for cause isolation.
- Identify resources available to troubleshoot Check Point Security Gateways and Security Management Servers that
- run on the Gaia operating system.

Lab Tasks

- Analyze Resources and Performance
- Analyze System Information with CPStat
- Analyze Statistical Data with CPView
- Collect CPInfo Output on the Security Management Server
- Collect CPInfo Output on the Security Gateway
- Analyze the CPInfo Output

Module 2: Traffic Monitoring Fundamentals

- Describe the functions of packet captures.
- Describe how logs and monitoring are used when troubleshooting.
- Investigate and troubleshoot potential traffic flow issues.
- Monitor network activity and performance.

Lab Tasks

- Analyze Logs
- Trace Rules and Craft Policy
- Test Policy and NAT Rules
- Examine Routing and State Logging

Module 3: Packet Capture Fundamentals

- Understand the impact of packet captures and packet capture limitations.
- Understand the use and limitations of four tools that can be used when capturing packets.
- Investigate and troubleshoot potential traffic flow issues using packet captures.
- Monitor network activity and performance using packet captures.

Lab Tasks

- Capture Traffic with the FW Monitor Expression Filter
- Capture Traffic with the FW Monitor Simple Filter
- Capture Traffic with the tcpdump Utility

- Capture Traffic with Check Point PCAP

Module 4: Packet Capture Analysis Using CLI

- Identify command line output formats for tcpdump, cppcap, fw monitor -e, and fw monitor -F.
- Identify cppcap flags and their impact on output verbosity.
- Understand how CPMonitor can be used during packet capture analysis.
- Analyze packet captures in CLI.

Lab Tasks

- Create Issues
- Troubleshoot Fundamental Traffic Issues
- Troubleshoot Policy Configuration Issues
- Troubleshoot Routing Issues
- Troubleshoot NAT Issues
- Restore the environment

Module 5: Packet Capture Analysis Using Wireshark

- Understand Wireshark coloring rules and the modifications you can make.
- Identify file saving methodology for captures being analyzed in Wireshark.
- Analyze packet captures in Wireshark.

Lab Tasks

- Configure Wireshark for use with Check Point
- Save Packet Captures
- Analyze FW Monitor Packet Captures in Wireshark
- Analyze Interface Packet Captures in Wireshark

Module 6: Check Point Processes Troubleshooting

- Demonstrate an understanding of user space, kernel space, and Check Point User Space Firewall processes.
- Investigate and troubleshoot process issues.

Lab Tasks

- Verify Process States
- Analyze Process Connectivity

Module 7: SmartConsole Troubleshooting

- Investigate and troubleshoot issues with Check Point SmartConsole.

Lab Tasks

- Activate the Bad Actor
- Troubleshoot SmartConsole Login Issues
- Restore the Environment

Module 8: Log Collection Troubleshooting

- Troubleshoot log collection issues and interrupted communications.

Lab Tasks

- Activate the Bad Actor
- Troubleshoot Gateway Log Connectivity
- Troubleshoot the Security Management Server Log Collection
- Restore the Environment

Module 9: Identity Awareness Troubleshooting

- Identify and use the appropriate troubleshooting commands/tools to resolve advanced Identity Awareness issues.

Lab Tasks

- Activate the Bad Actor
- Troubleshoot Identity Awareness
- Restore the Environment

Module 10: Application Control and URL Filtering Troubleshooting

- Investigate and troubleshoot Application Control and URL Filtering issues.

Lab Tasks

- Activate the Bad Actor
- Troubleshoot URL Filtering
- Restore the Environment

ASSOCIATED CERTIFICATIONS & EXAM

This course prepares delegates to write the Check Point Certified Troubleshooting Administrator #156-583 exam.

Note: A valid expired CCSA/CCSE certification is required to take the CCTA exam.