CHECK POINT
TROUBLESHOOTING ADMINISTRATOR (CCTA)

PENTESEC
EDUCATION SERVICES

Check Point®
SOFTWARE TECHNOLOGIES LTD.

R:80

COURSE PREPARES FOR EXAM: #156-580

WHO SHOULD ATTEND?

This course is designed for security administrators and Check Point resellers who need to manage and monitor issues that may occur within their Security Management environment.

COURSE GOAL

Provide an understanding of the concepts and skills necessary to troubleshoot issues which may occur when managing the Check Point Security Management architecture and Security Gateways.

COURSE PREREQUISITES

- Working knowledge of UNIX and/or Windows operating systems
- Working knowledge of Networking TCP/IP
- CCSA training/ certification
- Advanced knowledge of Check Point Security products

Check Point
PARTNER
ELITE

CHECK POINT
STARS
PARTNER
AUTHORIZED
TRAINING CENTER

Course Topics

- An Introduction to Troubleshooting
- SmartConsole and Policy Management Troubleshooting
- Monitoring Logging Activity
- Troubleshooting Issues with NAT
- Understanding the Unified Access Control Policy
- Basic VPN Troubleshooting
- Monitoring ClusterXL Connections
- Understanding Identity Awareness

Course Objectives

- 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, andhow debug commands are structured.
- Recognise how to use various Linux commands fortroubleshooting system issues.
- Recognise communication issues that may occur betweenSmartConsole and the SMS and how to resolve them.
- Understand how to troubleshoot SmartConsole login andauthentication issues.
- Understand how to prevent and resolve licensing andcontract issues.
- Understand how to troubleshoot issues that may occurduring policy installation.
- Understand communication issues that may occur whencollecting logs and how to resolve them.
- Recall various tools to use when analysing issues with logs.
- Understand how to restore interrupted communicationsduring 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 andhow the access control applications work together.
- Understand how to troubleshoot issues that may occur withApplication Control and URL Filtering.
- Understand how the HTTPS Inspection process works andhow to resolve issues that may occur during the process.
- Understand how to troubleshoot Content Awareness issues.
- Recognise how to troubleshoot VPN-related issues.
- Understand how to monitor cluster status and work withcritical devices.
- Recognise how to troubleshoot State Synchronisation.
- Understand how to troubleshoot communication issuesbetween Identity Sources and Security Gateways.
- Understand how to troubleshoot and debug issues withinternal Identity Awareness processes.

Lab Exercises

- Monitoring Security Gateway Traffic
- Troubleshooting Issues with SmartConsole
- Troubleshooting Log Connectivity Issues
- Investigating Log Connectivity Issues
- Investigating NAT Issues
- Troubleshooting General Traffic Issues
- Evaluating HTTP and HTTPS Traffic Issues
- Troubleshooting Site-to-Site VPN Issues
- Troubleshooting Clustering Issues
- Troubleshooting Identity Awareness
- Configuring and Testing Identity Collector