CCTA
Troubleshooting Administrator

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.

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

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

Labs 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

Course Objectives

- Understand how to use Check Point resources for support
- Understand how to perform packet captures using tcmdump 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 carious 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 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