Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå os her

.

Email: training.ecs.dk@arrow.com
Phone: +45 7025 4500

Check Point Certified Troubleshooting Expert (CCTE) R82 (includes 180 days' lab access)

CODE:	LENGTH:	PRICE:
CKT_CCTE_R82	16 Hours (2 dage)	kr 16,000.00

Description

Designed for experienced Check Point Security Experts, this course provides the advanced technical knowledge required to troubleshoot complex security environments. 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

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

Prerequisites

Base Knowledge

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

Check Point Courses
Recommended Preparation:
Check Point Security Expert (CCSE)
Suggested for Enhanced Learning:

- Check Point Deployment Administrator (CPDA)
- Check Point Security Administrator (CCSA)

Programme

Module 1: Introduction to Advanced Troubleshooting
•
Identify and use Linux-based and Check Point commands and tools for system monitoring, file editing, and file viewing.
•
Identify risks associated when using Linux-based and Check Point commands and tools for 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
•
Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Security Management Server and API Server issues.
Lab Tasks
•
Set the Stage
•
Troubleshoot SmartConsole Issues
•
Determine the Management Condition
•
Restore the Environment
Module 3: Advanced Troubleshooting with Logs and Events
•
Investigate and troubleshoot traffic or security-related issues using logs and events monitoring tools.
Lab Tasks
•
Set the Stage
•
Troubleshoot the Log Connection
•
Troubleshoot SmartLog
•
Restore the Environment
Module 4: Advanced Security Gateway Troubleshooting
•
Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Security Gateway issues.
Lab Tasks
•
Set the Stage
•
Troubleshoot SIC Communication
•
Troubleshoot Security Gateway Processes
•
Restore the Environment
Module 5: Advanced Firewall Kernel Debugging
•
Demonstrate an understanding of advanced troubleshooting tools and techniques for kernel debugging.
Lab Tasks
•
Set the Stage
•
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
•
Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Access Control issues.
Lab Tasks
•
Set the Stage
•

Increase the Log Detail
•
Repeat the Test
•
Debug the Unified Policy Module
•
Restore the Environment
Module 7: Advanced NAT Troubleshooting
•
Investigate and troubleshoot NAT (Network Address Translation) issues.
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
•
Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Identity Awareness issues.
Lab Tasks
•
Set the Stage
•
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
•
Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Site-to-Site VPN Troubleshooting issues.
Lab Tasks
•
Set the Stage
•
Troubleshoot IKE Issues
•
Examine Configuration Issues
•
Restore the Environment

Follow on courses

Test and Certification

Accreditation
Exam: 156-588
vue.com/checkpoint
Note: A valid or expired CCSE certification is required to take the CCTE exam.

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
18 Feb 2027	Virtual Classroom (CET / UTC +1)	CET	English	Instructor Led Online		kr 16,000.00
13 May 2027	Virtual Classroom (CET / UTC +1)	CEDT	English	Instructor Led Online		kr 16,000.00

Yderligere Information

Denne træning er også tilgængelig som træning på stedet. Kontakt os for at finde ud af mere.