Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss her

Postboks 6562 ETTERSTAD, 0606 Oslo, Norge

Email: kurs.ecs.no@arrow.com
Phone: +47 22 02 81 00

Check Point Certified Security Expert (CCSE) & Troubleshooting Expert (CCTE) Bundle R82 (includes 180 days lab access)

CODE:	LENGTH:	PRICE:
CKT_CCSECCTE_R82	40 Hours (5 days)	kr35,000.00

Description

This bundle course covers the following two Check Point training courses:

- Check Point Certified Security Expert (CCSE) R82 (3 days)
- Check Point Certified Troubleshooting Expert (CCTE) R82 (2 days)

The CCSE R82 part of the course equips students with the advanced skills to deploy, manage, and monitor Quantum Security environments, including high-availability management, advanced policy control, site-to-site VPNs, security monitoring, gateway upgrades, hotfix deployment, system import, and ElasticXL cluster deployment.
The CCTE R82 part of the course provides experienced Check Point Security Experts advanced troubleshooting skills through deep dives into Security Management, Logs and Events, and Security Gateways, covering firewall kernel, access control, NAT, Identity Awareness, and site-to-site VPNs to ensure optimal performance and stability.

Objectives

CCSE R82

- Deploy Management High Availability.
- Provide advanced policy management.
- Configure Site-to-Site VPN.
- Provide advanced security monitoring.
- Upgrade a Security Gateway.
- Use Central Deployment tool to install hotfixes.
- Perform an import of a Primary Security Management Server.
- Deploy ElasticXL Cluster.

CCTE R82

- Introductory overview
- In-depth exploration of the Security Management Server, Logs and Events, and Security Gateways.
- Advanced troubleshooting of the Firewall Kernel, Access Control, NAT, Identity Awareness, and Site-to-Site VPN to ensure optimal performance and stability across the entire security stack.

Audience

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

Prerequisites

Base Knowledge

- Unix-like and/or Windows OS
- Internet Fundamentals
- Networking Fundamentals
- Networking Security
- System Administration
- TCP/IP Networking
- Text Editors in Unix-like OS
- Bash Scripting in Unix-like OS
- Minimum of 6-months of practical experience with the management of a Quantum Security Environment.

Check Point Courses

- Check Point Certified Security Administrator (required)
- Check Point Deployment Administrator (suggested)

Programme

Programme
CCSE R82

Module 1: Management High Availability

- Explain the purpose of Management High Availability.
- Identify the essential elements of Management High Availability.

Lab Tasks

- Deploy and configure Management High Availability
- Ensure the failover process functions as expected

Module 2: Advanced Policy Management

- Identify ways to enhance the Security Policy with more object types.
- Create dynamic objects to make policy updatable from the Gateway.
- Manually define NAT rules.
- Configure Security Management behind NAT.

Lab Tasks

- Use Updatable Objects
  - Configure Network Address Translation for server and network objects
  - Configure Management behind NAT for Branch Office connections

Module 3: Site-to-Site VPN

- Discuss site-to-site VPN basics, deployment, and communities.
- Describe how to analyze and interpret VPN tunnel traffic.
  - Articulate how pre-shared keys and certificates can be configured to authenticate with third-party and externally managed VPN Gateways.
  - Explain Link Selection and ISP Redundancy options.
  - Explain tunnel management features.

Lab Task

- Configure Site-to-Site VPN with internally managed Security Gateways

Module 4: Advanced Security Monitoring

- Describe the SmartEvent and Compliance Blade solutions, including their purpose and use.

Lab Tasks

- Configure a SmartEvent Server to monitor relevant patterns and events
- Demonstrate how to configure Events and Alerts in SmartEvent
- Demonstrate how to run specific SmartEvent reports
- Activate the Compliance Blade
- Demonstrate Security Best Practice settings and alerts

- Demonstrate Regulatory Requirements Compliance Scores

Module 5: Upgrades

- Identify supported upgrade options.

Lab Task

- Upgrade a Security Gateway
- Use Central Deployment tool to install Hotfixes

Module 6: Advanced Upgrades and Migrations

- Export/import a Management Database.
- Upgrade a Security Management Server by freshly deploying the new release or using a new appliance.

Lab Task

- Prepare to perform an Advanced Upgrade with Database
- Migration on the Primary Security Management Server in a distributed environment
- Perform an import of a Primary Security Management Server in a distributed Check Point environment

Module 7: ElasticXL Cluster

- Describe the ElasticXL Cluster solution, including its purpose and use.

Lab Tasks

- Deploy an ElasticXL Security Gateway Cluster

CCTE R82

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

Follow on training:
Attend two Infinity Specialization courses and pass their exams to automatically become a Check Point Certified Security Master (CCSM).
Attend four Infinity Specialization courses and pass their exams to automatically become a Check Point Certified Security Master Elite (CCSM Elite).

- Check Point Certified Endpoint Specialist (CCES)

- Threat Prevention Specialist (CTPS)
- Check Point Certified Troubleshooting Administrator (CCTA)
- Check Point Certified Automation Specialist (CCAS)
- Check Point Certified Cloud Specialist (CCCS)
- Check Point Certified Maestro Expert (CCME)

Test and Certification

Prepare for exams #156-315.82 (CCSE R82) and #156-588 (CCTE R82) at www.VUE.com/checkpoint.
Full information on Check Point's Certification Program can be viewed at
https://www.checkpoint.com/downloads/training/check-point-certification-faq.pdf

Further Information

Please note that Check Point only offer e-kit courseware for training courses.
Each delegate will be provided with an official set of e-kit courseware.
Arrow ECS are a Check Point Platinum Elite Authorised Training Company (ATC) Partner and participate in the Infinity Global Services Credits (IGS) and Partner Coop Training Program.

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
15 Feb 2027	Virtual Classroom (GMT / UTC)	GMT	English	Instructor Led Online		kr35,000.00
10 May 2027	Virtual Classroom (CET / UTC +1)	CEDT	English	Instructor Led Online		kr35,000.00

Tilleggsinformasjon

Denne treningen er også tilgjengelig som trening på stedet. Kontakt oss for å finne ut mer.