Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com
Phone: +46 8 555 188 00

Check Point Certified Security Expert (CCSE) & Troubleshooting Expert (CCTE) Bundle

CODE:	LENGTH:	PRICE:
CKT_CPSECCTE_R81.X	40 Hours (5 days)	kr36,000.00

Description

This bundle course covers the following two Check Point training courses:
Check Point Certified Security Expert (CCSE) R81.x (3 days) And
Check Point Certified Troubleshooting Expert (CCTE) R81.x (2 days)

Objectives

Objectives CCSE:

- Provide an overview of the upgrade service and options available.
- Explain how to perform management upgrade and migration.
- Articulate the process using CPUSE features.
- Articulate the purpose and function of Management High Availability.
- Explain Primary vs Secondary, Active vs Standby and Synchronization.
- Explain disaster recovery steps in case the primary management server becomes unavailable.
- Provide overview of Central Deployment in SmartConsole.
- Articulate an understanding of Security Gateway cluster upgrade methods.
- Explain about Multi Version Cluster (MVC) upgrades.
- Discuss Gaia Commands and how they are used.
- Explain the main processes on Security Management Servers and Security Gateways.
- Describe how to work with scripts and SmartTasks to configure automatic actions.
- Explain the Management Data Plane Separation (MDPS).
- Explain kernel operations and traffic flow.
- Articulate Dynamic and Updatable Objects in Security Gateways.
- Explain the policy installation flow and files used.
- Describe the use of policy installation history.
- Explain concurrent and accelerated install policy.
- Describe an overview of APIs and ways to use and authenticate.
- Explain how to make changes in GAIA and management configuration.

- Explain how to install policy using API.
- Explain how the SecureXL acceleration technology enhances and optimizes Security Gateway performance.
- Describe how the CoreXL acceleration technology enhances and improves Security Gateway performance.
- Articulate how utilizing multiple traffic queues can make traffic handling more efficient.
- Discuss Site-to-Site VPN basics, deployment and communities.
- Describe how to analyze and interpret VPN tunnel traffic.
- Explain Link Selection and ISP Redundancy options.
- Explain tunnel management features.
- Discuss Check Point Remote Access solutions and how they differ from each other.
- Describe how client security can be provided by Remote Access.
- Explain authentication methods including machine authentication.
- Explain Multiple Entry Point (MEP).
- Discuss the Mobile Access Software Blade and how it secures communication and data exchange during remote connections.
- Describe Mobile Access deployment options.
- Discuss various features in Mobile Access like Portals, Link Translation, running Native Applications, Reverse Proxy and more.
- Explain basic concepts of Clustering and ClusterXL.
- Explain about Cluster Control Protocol (CCP) and synchronization.
- Describe advanced ClusterXL functions and modes like Load Sharing, Active-Active, VMAC mode etc.
- Discuss Cluster Correction Layer (CCL) to provide connection stickyness.
- Advanced Logs and Monitoring
- Explain how to determine if the configuration is compliant with the best practices.
- Explain how to set action items to meet the compliance.
- Discuss how SmartEvent functions to identify critical security issues.

Exercises CCSE:

- Prepare for a Security Management Server Upgrade
- Upgrade the Security Management Server
- Deploy a Secondary Security Management Server
- Configure a Distributed Log Server
- Upgrade a Security Gateway from SmartConsole
- Work with the Command Line
- Use Scripts and SmartTasks
- Configure Dynamic Objects
- Monitor Traffic

- Verify Policy Installation and Status
- Work with Gaia and Management APIs
- Work with Acceleration Features
- Configure a Locally Managed Site to Site VPN
- Configure a Site to Site VPN with an Interoperable Device
- Configure Remote Access VPN
- Configure Mobile Access VPN
- Configure a High Availability Cluster
- Work with ClusterXL
- Configure Policy Compliance
- Deploy SmartEvent

Objectives CCTE:

- Demonstrate understanding how to use advanced troubleshooting tools and techniques including: Interpreting diagnostic data with CPInfo, Collecting and reading statistical data using CPView, and Advanced troubleshooting risks.
- Describe the use of Logs and SmartEvent in troubleshooting.
- Describe the log indexing system and issues that can occur.
- Discuss methods to troubleshoot log indexing in SmartLog and SmartEvent.
- Explain the databases used in Security Management operations.
- Identify common troubleshooting database issues.
- Discuss Management Processes.
- Demonstrate understanding of advance troubleshooting tools and techniques including: How the kernel handles traffic, How to troubleshoot issues using chain modules, How to use the two main procedures for debugging the Firewall kernel, and How the two main procedures for debugging the Firewall kernel differ.
- Demonstrate understanding of user mode debugging, including collecting and interpreting process debugs.Debug user mode processes.
- Discuss advanced Identity awareness troubleshooting.
- Learn to run debugs on Identity Awareness.
- Explain Unifed Access Control flow and processes.
- Explain Access Control kernel debugs.
- Describe Access Control process debugs.
- Explain basic and advanced Site-to-Site VPN troubleshooting tools and techniques, including: Packet captures, IKE debugs, and VPN process debugs.
- Explain Client-to-Site VPN troubleshooting tools and techniques, including: Remote access troubleshooting and Mobile access troubleshooting.

Exercises CCTE:

- Collecting and Reading CPInfo
- Collecting and Reading CPView Data
- Troubleshooting SmartLog
- Troubleshooting SmartEvent
- Troubleshooting Database Issues
- Debugging Security Gateway Kernel
- Debugging User Mode Processes
- Debugging Identity Awareness
- Debugging Unified Policy Inspection
- Troubleshooting Site-to-Site VPN
- Debugging Remote Access VPN

Audience

- Technical professionals who support, install deploy or administer Check Point products.
- Security experts and Check Point resellers who desire to obtain the necessary knowledge required to perform more advanced troubleshooting skills while managing their security environments.

Follow on courses

If you already attended our CCSA + CCTA course bundle and successfully passed the respective exams:
Attend two additional Infinity Specialization courses and pass their exams to automatically become a Check Point Certified Security Master Elite (CCSM Elite).
If you are already holding a CCSA and you successfully passed the CCSE and CCTE exam:
Attend three additional Infinity Specialization courses and pass their exams to automatically become a Check Point Certified Security Master Elite (CCSM Elite).

Test and Certification

This course bundle prepares you for exams #156-315.81 (CCSE) and #156-585 (CCTA) at www.VUE.com/checkpoint Note: Exam vouchers need to be purchased separately at additional cost.

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 approximately 1 week prior to the start date of the course.

Session Dates

På begäran, kontakta oss

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.