Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com
Phone: +31 20 582 6109

Check Point Certified Security Administrator (CCSA) and Expert (CCSE) R81.X Boot Camp

CODE:	LENGTH:	PRICE:
CKT_CCSAEBC_R81.X	40 Hours (5 days)	€4,250.00

Description

This Fastrack combines the Check Point Certified Security Administrator (CCSA) R80.x and Check Point Certified Expert (CCSE) R80.x courses within 5 days. You save one day of the regular training time.

Objectives

CCSA Objectives:

- Know how to perform periodic administrator tasks.
- Describe the basic functions of the Gaia operating system.
- Recognize SmartConsole features, functions, and tools.
- Understand how SmartConsole is used by administrators to give user access.
- Learn how Check Point security solutions and products work and how they protect networks.
- Understand licensing and contract requirements for Check Point security products.
- Describe the essential elements of a Security Policy.
- Understand the Check Point policy layer concept.
- Understand how to enable the Application Control and URL Filtering software.
- Blades to block access to various applications.
- Describe how to configure manual and automatic NAT.
- Identify tools designed to monitor data, determine threats and recognize opportunities for performance improvements.
- Describe different Check Point Threat Prevention solutions for
- network attacks.
- Articulate how the Intrusion Prevention System is configured, maintained and tuned.
- Understand the Infinity Threat Prevention system.
- Knowledge about Check Point’s IoT Protect.

CCSE Objectives:

- 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 s and s.
- 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

Audience

Students with previous knowledge of managing cybersecurity operations or Check Point products.
This fast track also prepares for the CCSA and CCSE certification.

Prerequisites

Previous experience is recommended:

- General knowledge of TCP/IP
- Experience with Windows and/or UNIX, Network Technology and the Internet.
- Experience in managing cybersecurity operations or Check Point products.

Programme

CCSA Exercices:

- Configure the Security Management Server.
- Use the WebUI to run the First Time Wizard.
- Install the Smart Console.
- Install the Alpha Gateway using the network detailed in the course

- topology.

- Demonstrate how the Security Management Server and Gateway communicate.
- Test SIC Status.
- Create multiple administrators and apply different roles and permissions for simultaneous administration.
- Validate existing licenses for products installed on the network.
- Create and configure host, network and group objects.
- Create a simplified Security Policy.
- Demonstrate how to use Security Zones in policy.
- Demonstrate how to share a layer between Security Polices.
- Configure Network Address Translation for server and network objects.
- Enable Identity Awareness.
- Deploy user access roles for more granular control of the security Policy.
- Generate network Traffic and use traffic visibility tools to monitor the data.
- Use SmartConsole and SmartView Monitor to view status, alerts, and

- block suspicious traffic.

CCSE Exercises:

- 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

Test and Certification

CCSA - Check Point Certified Security Administrator (exam 156-215.81)
The CCSA is the first certification that shows you have the ability to install Check Point's most popular product, the FireWall-1, and use it to protect your corporate network. You will also be able to define and implement security policies, ensuring secure access to corporate information.
CCSE - Check Point Certified Security Expert (exam 156-315.81)
The CCSE is almost an industry standard for Internet security. It gives you the knowledge and experience to configure the VPN-1/FireWall-1 as an Internet security solution for the entire corporate network. Users can gain access to this network via a Virtual Private Network and exchange information - both on the road and between different branches. You will also be introduced in detail to encryption techniques as well as anti-virus measures.

Session Dates

On request. Please contact us

Additional Information

This training is also available as onsite training. Please contact us to find out more.