R80.40 Check Point SOFTWARE TECHNOLOGIES LTD

CHECK POINT

CERTIFIED SECURITY ADMINISTRATOR (CCSA)

AUDIENCE

Technical professionals who support, install deploy or administer Check Point products.

GOALS

Learn basic concepts and develop skills necessary to administer IT security fundamental tasks.

PREREQUISITES

Working knowledge of Windows, UNIX, networking technology, the Internet and TCP/IP.

TOPICS

Security Architecture | Admin Operations | Deployment | Licensing | Gaia Portal | Hide/Static NAT | Firewall Basics | Monitoring States | ClusterXL | Traffic Visibility | Security Events | Compliance Tasks | Threat Detection | Policy Layers | Site-to-Site VPN | Remote Access VPN | User Access

OBJECTIVES

- Know how to perform periodic administrator tasks
- Describe the basic functions of the Gaia operating system
- Recognize SmartConsole features, functions, and tools
- Describe the Check Point Firewall infrastructure
- Understand how SmartConsole is used by administrators to grant permissions and 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
- Identify SmartEvent components used to store network activity logs and identify events
- Know how Site-to-Site and Remote Access VPN deployments and communities work
- Explain the basic concepts of ClusterXL technology and its advantages

EXERCISES

- Identify key components and configurations
- Create and confirm administrator users for the domain
- Validate existing licenses for products installed on your network
- Create and modify Check Point Rule Base objects
- Demonstrate how to share a layer between Security Policies
- Analyze network traffic and use traffic visibility tools
- Monitor Management Server States using SmartConsole
- Demonstrate how to run specific SmartEvent reports
- Configure a SmartEvent server to monitor relevant patterns
- Configure and deploy a site-to-site VPN
- Configure and test ClusterXL with a High Availability configuration
- Understand how to use CPView to gather gateway information
- Perform periodic tasks as specified in administrator job descriptions
- Test VPN connection and analyze the tunnel traffic
- Demonstrate how to create custom reports
- Demonstrate how to configure event Alerts in SmartEvent
- Utilize various traffic visibility tools to maintain Check Point logs

CERTIFICATION INFORMATION

CCSA

Prepare for exam #156-215.80 **VUE.com/checkpoint**

R80.40 Check Point SOFTWARE TECHNOLOGIES LTD

CHECK POINT CERTIFIED SECURITY EXPERT (CCSE)

AUDIENCE

Technical professionals who perform advanced deployment configurations of Check Point products.

GOALS

Validate and enhance your skills and optimally manage Check Point advanced security management systems.

PREREQUISITES

CCSA training and certification with a working knowledge of Windows and/or UNIX, networking technology, the Internet and TCP/IP.

TOPICS

Management Maintenance | Management Migration | Management | High Availability | Policy Automation | Gateway Maintenance | The Firewall Kernel | User-Mode Processes | ClusterXL | Traffic Acceleration | Core Acceleration | Interface Acceleration | Threat Prevention | Threat Emulation | Advanced Site-to-Site VPN | Remote Access VPN | Mobile Access

OBJECTIVES

- Articulate Gaia system management procedures.
- Explain how to perform database migration procedures.
- Articulate the purpose and function of Management High Availability.
- Describe how to use Check Point API tools to perform management functions.
- Articulate an understanding of Security Gateway cluster upgrade methods.
- Discuss the process of Stateful Traffic inspection.
- Articulate an understanding of the Check Point Firewall processes and debug procedures.
- Describe advanced ClusterXL functions and deployment options.
- 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.
- Describe different Check Point Threat Prevention solutions for network attacks.
- Explain how SandBlast, Threat Emulation, and Threat Extraction help to prevent security incidents.
- Recognize alternative Check Point Site-to-Site deployment options.
- Recognize Check Point Remote Access solutions and how they differ from each other.
- Describe Mobile Access deployment options.

EXERCISES

- Perform an upgrade of a Security Management server in a distributed environment.
- Use the migrate_export command to prepare to migrate a Security Management Server.
- Deploy a Secondary Management Server.
- Demonstrate how to define new network and group objects using the Check Point API.
- Perform an upgrade of Security Gateways in a clustered environment.
- Use Kernel table commands to evaluate the condition of a Security Gateway.
- Use common commands to evaluate the condition of a Security Gateway.
- Configure Virtual MAC.
- Demonstrate how SecureXL affects traffic flow.
- Describe how the CoreXL acceleration technology enhances and improves Security Gateway performance.
- Demonstrate how to monitor and adjust interface traffic queues.
- Identify specific threat protections used by Check Point Threat Prevention.
- Demonstrate how to enable Mobile Access for remote users.

CERTIFICATION INFORMATION

CCSE

Prepare for exam #156-315.80 at VUE.com/checkpoint