Check Point Security Administration and Security Engineering Bundle (R77.30 GAiA)

Code:	CCSA+CCSE R77.30
Length:	5 days
URL:	View Online

This special CCSA and CCSE bundle covering Check Point Security Administration & Engineering (R77.30 GAiA) provides you with an understanding of the basic concepts and skills necessary to configure Check Point Security Gateway and Management Software Blades. During this course, you will configure a Security Policy and learn about managing and monitoring a secure network, upgrading and configuring a Security Gateway, and implementing a virtual private network. This part prepares you for CCSA certification. The advanced part of the course provides you training on how to build, modify, deploy and troubleshoot Check Point Security Systems on the GAiA operating system. Hands-on lab exercises teach how to debug firewall processes, optimize VPN performance and upgrade Management Servers. This advanced part prepares you for CCSE certification.

Skills Gained

In this combo bundle program students will cover following administration and Engineering skills

- Introduction to Check Point technology
- Deployment platforms
- Introduction to the security policy
- Monitoring traffic and connections
- Using SmartUpdate
- User management and authentication
- Identity awareness
- Introduction to Check Point VPNs
- Check Point firewall technology
- Troubleshooting Check Point firewall technology
- Advanced upgrading concepts and practices
- Clustering firewall, management concepts, and practices
- Software acceleration features
- Advanced VPN concepts and implementations
- Reporting tools, deployment options, and features

Who Can Benefit

This special combo or bundle course is recommended for Systems Administrators, Network Engineers, Security Managers, Support Analysts and any other IT professional working with Check Point Software Blades or seeking CCSA and CCSE certifications.

Prerequisites

Prior to taking this course, it is recommended that learners possess the following:

- General knowledge of TCP/IP
- Working knowledge of Windows, UNIX, network technology, and the Internet

Course Details

Course Outline

- Check Point's unified approach to network management and key components
- Design a distributed environment and Install the Security Gateway in it
- Perform a backup and restore the current gateway installation from the command line
- Identify critical files needed to purge or backup, import and export users and groups, and add or delete administrators from the command line
- Deploy gateways using the Gaia web interface
- Create & configure network, host, and gateway objects
- Using SmartDashboard verify SIC establishment between the Security Management Server and the gateway
- Create a basic Rule Base in SmartDashboard that includes permissions for administrative users, external services, and LAN outbound use
- Configure NAT rules on Web and Gateway servers
- Evaluate existing policies and optimize the rules based on corporate requirements
- Maintain the Security Management Server with scheduled backups and policy versions to ensure seamless pgrades with minimal downtime
- Use Queries in SmartView Tracker to monitor IPS and common network traffic and troubleshoot events using packet data
- Use packet data to generate reports, troubleshoot system and security issues, and ensure network functionality
- Using SmartView Monitor, configure alerts & traffic counters, view a gateway's status, monitor suspicious activity rules, analyze tunnel activity and monitor remote user access
- Monitor remote gateways using SmartUpdate to evaluate the need for upgrades, new installations, and license modifications
- Use SmartUpdate go apply upgrade packages to single or multiple VPN-1 gateways
- Upgrade and attach product licenses using SmartUpdate
- Centrally manage users to ensure only authenticated users securely access the corporate network either locally or remotely
- Manage users to access the corporate LAN by using external databases
- Provide granular-level access to network resources using Identity Awareness
- Acquire user information used by the security gateway to control access
- Define access roles for use in an Identity Awareness rule
- Implement Identity Awareness in the Firewall Rule Base
- Configure a pre-shared secret site-to-site VPN with partner sites
- Configure permanent tunnels for remote access to corporate resources
- Configure VPN tunnel sharing, given the difference between host-based, subunit-based, and gateway- based tunnels
- Perform a backup of a security gateway and Management Server using your understanding of the differences between

backups, snapshots and update-exports

- Upgrade and troubleshoot a Management Server using a database migration
- Upgrade and troubleshoot a clustered Security Gateway deployment
- Use knowledge of Security Gateway infrastructures, chain modules, packet flow, and kernel tables to perform debugs on firewall processes
- Build, test, and troubleshoot a ClusterXL Load Sharing deployment on an enterprise network
- Build, test, and troubleshoot a ClusterXL High Availability deployment on an enterprise network
- Build, test, and troubleshoot a management HA deployment on an enterprise network
- Configure, maintain, and troubleshoot SecureXL and CoreXL acceleration solutions on the corporate network traffic to ensure noted performance enhancement
- Using an external user database such as LDAP, configure User Directory to incorporate user information for authentication services on the network
- Manage internal and external user access to resources for remote access or across a VPN
- Troubleshoot user-access issues found when implementing Identity Awareness
- Troubleshoot a site-to-site or certificate-based VPN on a corporate gateway using IKE View, VPN log files, and command-line debug tools
- Optimize VPN performance and availability by using Link Selection and Multiple Entry Point solutions
- Manage and test corporate VPN tunnels to allow for greater monitoring and scalability with multiple tunnels defined in a community including other VPN providers
- Create events or use existing event definitions to generate reports on specific network traffic using SmartReporter and SmartEvent to provide industry compliance information to management
- Troubleshoot report generation given command-line tools and debug-file information

---