Check Point Security Engineering R77

Introduction

This course prepares the participants to appear for the **CCSE** certification exam

Check Point Security Engineering is an advanced course that teaches how to effectively build, modify, deploy and troubleshoot Check Point Security systems on the Gaia OS. We will study firewall processes and take a close look at user and kernel processing and Stateful Inspection. Labs include configuring security gateways, implementing VPNs, and performing advanced troubleshooting tasks on the firewall.

Duration

3 Days

Prerequisites

Successful completion of this course depends on knowledge of multiple disciplines related to network-security activities including UNIX and Windows operating systems, Certificate management, system administration, networking (TCP/IP) knowledge, and Check Point Security Administration course/CCSA Certification.

Who Should Attend?

This course is designed for expert users and resellers who need to perform advanced deployment configurations of a security gateway. This could include System Administrators, Support Analysts, Network Engineers and anyone seeking CCSE certification

Platform and Version

This course is based on the Check Point Security Management Server R77 and Security Gateway R77 deployed on GAiA operating system

Course Objectives

- ✓ Perform a backup of a Security Gateway and Management Server using your understanding of the differences between backup, snapshot and upgrade-export
- ✓ 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 for troubleshooting firewall functions
- ✓ Build, test and troubleshoot a ClusterXL Load Sharing deployment
- ✓ Build, test and troubleshoot a ClusterXL High Availability deployment
- ✓ Build, test and troubleshoot a management HA deployment
- ✓ Configure, maintain and troubleshoot SecureXL and CoreXL acceleration solutions 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 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 tools
- ✓ 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

Check Point Security Engineering R77

K-SECURE
IT Security Services

Lab Exercises Include

- Upgrade to Check Point R77
- Core CLI elements of firewall administration
- Migrate to a clustering solution
- Configure SmartDashboard to interface with Active Directory
- Configure site-to-site VPNs with third-party certificates
- Remote Access VPN
- SmartEvent and SmartReporter