Check Point Certified Security Administration R77.30 (CCSA) (R77I)

Course Overview

Validate your understanding and skills necessary to configure and optimally manage Check Point Next Generation Firewalls.

Prerequisites

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

Course Objectives

- Describe Check Point's unified approach to network management, and the key elements of it
- Design a distributed environment
- Install the Security Gateway in a distributed environment
- 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 and configure network, host and gateway objects
- Verify SIC establishment between the Security Management Server and the Gateway using SmartDashboard
- 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 current corporate requirements
- Maintain the Security Management Server with scheduled backups and policy versions to ensure seamless upgrades with minimal downtime
- Use Queries in SmartView Tracker to monitor IPS and common network traffic and trouble¬shoot events using packet data
- Use packet data to generate reports, trouble¬shoot system and security isues, and ensure network functionality
- Using SmartView Monitor, configure alerts and 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 to 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
- Use Identity Awareness to provide granular level access to network resources
- 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

Detailed Course Outline

- Introduction to Check Point technology
- Deployment platforms
- Introduction to the Security Policy
- Monitoring traffic and connections
- Network Address Translation
- Using SmartUpdate
- User management and authentication
- Identity Awareness
- Introduction to Check Point VPNs

Lab exercises

- Install and configure Security Management Servers and Security Gateways
- Apply commands in the Command Line Interface
- Working with Administrators and performing backups.
- Creating objects and rules
- Saving, installing and testing a Security Policy
- Defining new policies and combining them
- Creating DMZ related objects and rules
- Working with SmartView Tracker and SmartView Monitor
- Configuring and testing Hide and Static NAT
- Configuring and testing Identify Awareness
- Defining VPN domains and testing encryption
- Working with queries in SmartLog