Check Point Security Administration R77

Introduction

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

Check Point Security Administration R77 – This course provides an understanding of basic concepts and skills necessary to configure Check Point Security Gateway and Management Software. During this course, you will configure a Security Policy, and learn about managing and monitoring a secure network. In addition, you will configure user authentication, identity awareness and implement site-to-site virtual private networks.

Duration

3 Days

Prerequisites

Persons attending this course should have general knowledge of TCP/IP, and working knowledge of Windows, Linux/Unix, network technology and the internet. Knowing basics of VPN will help in VPN configuration.

Who Should Attend?

System administrators, security managers, and network engineers who manage Check Point Software Blades, and individuals seeking the CCSA 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

- **Check Point Technology Overview**
  - Describe Check Point's unified approach to network management, and the key elements of this architecture.
  - Design a distributed environment using the network detailed in the course topology.
  - Install the Security Gateway in a distributed environment using the network detailed in the course topology.

- **Deployment Platforms**
  - Given network specifications, 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 web interface.

- **Introduction to the Security Policy**
  - Given the network topology, 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.
  - Evaluate existing policies and optimize the rules based on current corporate requirements.

contd.

- Maintain the Security Management Server with scheduled backups and policy versions to ensure seamless upgrades and minimal downtime.

- **Monitoring Traffic and Connections**
    - Use queries in SmartView Tracker to monitor common network traffic and troubleshoot network and security issues
    - 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 based on corporate requirements.

- **Network Address Translation (NAT)**
    - Understand differences between Hide NAT and Static NAT, Automatic and Manual configuration
    - Configure Hide NAT for local network
    - Configure NAT rules on Web and Gateway servers.

- **Using SmartUpdate**
    - Monitor remote Gateways using SmartUpdate to evaluate the need for upgrades, new installations, and license modifications.
    - Upgrade and attach product licenses using SmartUpdate.

- **User Management and Authentication**
    - Centrally manage users to ensure only authenticated users securely access the corporate network either locally or remotely.
    - Manage users to access to the corporate LAN by using external databases.
    - Configure User Directory to integrate with Active Directory Server

- **Identity Awareness**
    - 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

- **Introduction to Check Point VPNs**
    - 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, subnet-based and gateway-based tunnels.

Lab Exercises Include

- Distributed Installations
- Branch Office Security Gateway Installations
- CLI Tools
- Building a Security Policy
- Configure the DMZ
- Monitor with SmartView Tracker
- Configure NAT
- Configure User Directory
- Configure Identity Awareness
- Site-to-Site VPN between corporate and branch office