Check Point Certified Security Administrator (CCSA)

Course Overview

☑ Check Point Certified Security Administrator (CCSA) R81.20 is a three-day training aimed at technical personnel and covers the installation, setup and management of Check Point Software solutions. The goal of the course is to understand the basic concepts and acquire the skills necessary for the configuration of Check Point Firewall and Check Point Management.

Prerequisites

☑ Basic knowledge of TCP/IP
Knowledge of the basics of Windows and UNIX, network services and the use of the Internet

CHECK POINT
PLATINUM
ATC PARTNER
2024
CONTRIBUTION

INGRAM MICRO® | Trening Center Slovenija

DAY 03

Analysis and interpretation of VPN traffic;

Defining Users and User Groups;

Access management of all Users;

The basics of ClusterXL technology and the benefits of using it;

Periodic Administration;

DAY 01

Understanding the concept of Firewall and understanding the mechanisms used to control traffic flow;

Describing the most important elements of the Check Point Unified Security Management Architecture;

Getting to know SmartConsole features, functions and tools;

Understanding the application of Check Point solutions;

Describing the basic functions of Gaia;

Describing the basic elements of Security Policy;

Understanding Unified Security Policy traffic inspection;

DAY 02

The role of the Administrator in the creation of Management Policies;

Backup techniques;

Concepts of Layer Policy;

Recognition and understanding of Check Point security solutions and products, and how they work to protect the network;

Licensing of Check Point solutions;

Using tools designed to monitor data, find threats and improve performance;

Using tools designed for quick response and efficient changes to Firewall, tunnels, remote; Users, traffic flow and other activities;

Understanding Site-to-Site and Remote Access VPNs;

LAB OUTLINE:

Working with Gaia;

Modification of Existing Security Policies;

Configuration of Dynamic and Static NAT;

Admin Access Control;

Installation and Remote Firewall Management;

Backup;

Defining an Access Control Policy;

Defining the Security Policy;

Licensing;

Working with Check Point Logs;

Site-to-Site VPN configuration;

Providing Access to Users;

Working with ClusterXL;

Network Compliance Verification;

Working with CP View;