Course name:	**Check Point™ Security Administration R77 (CCSA R77)**
Course form:	Lectures/consultations and intensive lab training
Course description:	Check Point Secuirty Administration course provides an understanding of basic concepts and skills necessary to configure Check Point Security Gateway and Management Software Blades. During this course, attendants will configure Security Policy and will learn about managing and monitoring secure network. In addition, attendants will upgrade and configure Security Gateway to implement virtual private network for both internal and external, remote users.
Length:	3 days
Prerequisites:	Persons attending this course should have general knowledge of TCP/IP, and working knowledge of Windows, UNIX, network technology and the internet.
Examination:	This course helps prepare for ***Check Point Certified Security Administrator exam #156-215.77*****.** The exam contains 90 multiple-choice, scenario-based questions. A passing score is 70% or higher in 120 minutes. The exam is based on 80% course materials and 20% hands-on experience with Check Point products. Students should have at least 6 months experience with Check Point products before tackling it.
Course content:	**Introducing to Check Point Technology** • 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 sysconfig and cpconfig from the Gateway command line. **Introducing to 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. • Maintain the Security Management Server with scheduled backups and policy versions to ensure seamless upgrades and minimal downtime. **Monitoring Traffic and Connection** • Use Queries in SmartView Tracker to monitor IPS and common network traffic and troubleshoot events using packet data. • Using packet data on a given corporate network, generate reports, troubleshoot system and security issues, 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 based on corporate requirements. **Network Address Translation** • 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. • Use SmartUpdate to apply upgrade packages to single or multiple VPN-1 Gateways. • 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 access to the corporate LAN by using external databases. **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 Rules for use in an Identity Awareness rule. • Implementing 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 installation • Branch office security gateway installation • CLI tools • Building a Security Policy • Configure the DMZ • Monitor with SmartView Tracker • Configure the NAT • Configure user directory • Identity awareness • Site-to-site VPN between corporate and branch office
Course date:	According to customer request
Course place:	Košice, Check Point ATC training center, Intas s.r.o., Stromova 10