Course name:	**Check Point™ Multi-Domain Security Management with Virtual System Extension R77**
Course form:	Lectures/consultations and intensive lab training
Course description:	This course is intended to provide attendants with understanding of key concepts and skills necessary to effectively configure and deploy MDSM with VSX. This course provides hands-on training for installing components of Multi-Domain Security Management with Virtual System Extension on Windows & Gaia. Attendants will configure Security Policies for multiple remote firewalls using Smart Domain Manager, and learn about managing multiple firewall-secured environments using Multi-Domain Server. Attendants will also learn how to perform advanced configuration tasks such as establishing redundant Multi-Domain Servers for High Availability management functions and migrating existing servers into Multi-Domain Security Management database.
Length:	5 days
Prerequisites:	Persons attending this course should have general knowledge of TCP/IP, and working knowledge of Windows, UNIX, network technology, internet, Security Administration CCSA, Security Engineering CCSE, CheckPoint Gaia.
Examination:	This course helps prepare for ***MDSM with VSX exam #156-820.77*.** 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 take this cours.
Course content:	**Multi-Domain Security Management with Virtual System Extension** • Identify features and functions of Multi-Domain Security Management with VSX • Describe Multi-Domain Security Management with VSX architecture **Multi-Domain Security Deployment** • Given needs of your company and your Domains, choose correct Multi-Domain Security Management implementation to cover these requirements. • Classify various pieces of Multi-Domain Security Management architecture and recognize their interactions together. • Use correct tools to troubleshoot and solve any issues that may arise in architecture, file system or processes. **Multi-Domain Security Management Installation and Configuration** • Install Multi-Domain Security Management. • Configure Multi-Domain Security Management environment. • Create Multi-Domain Server Manager. • Install and configure Smart Domain Manager. • Implement any necessary Management Plug-ins for specific environments • Troubleshoot and solve any issues that may arise during installation and configuration. **Multi-Domain Security Management Logging Features** • Configure and implement Multi-Domain Log Server for Multi- Domain Security Management environment. • Configure and implement Domain Log Server for given Domain. **Multi-Domain Security Management Advanced Features** • Configure and implement Global Policy. • Configure and implement VPNs Globally and per Domain. • Create secondary Multi-Domain Server Manager and enable Multi-Domain Server High Availability.

	• Create and configure secondary Domain Management Server, where applicable for Domains. • Where necessary, configure Domain Management Server High Availability based on Domain's requirements. • Create secondary MDS Manager and enable MDS High Arability • Create and configure secondary DMS, where applicable for Domains • Where necessary, configure DMS High Availability based on Domain's requirements. **Virtual System Extension Deployment** • Identify VSX components. • Describe relationships between VSX components. • Describe function of VSX Context Identification. • Describe Traffic Inspection Process. • Describe purpose of Virtual System within VSX environment. • Discuss various VSX deployment scenarios. **Virtual System Extension Gateway Installation and Configuration** • Demonstrate how to transition physical firewalls to VSX • environment • Demonstrate how to deploy virtual infrastructure with VLAN tagging. **Virtual System Extension Advanced Features** • Describe difference between standard Physical Security Gateway Clusters and VSX Gateway Clusters. • Identify different synchronization modes. • Describe common troubleshooting practices **Virtual System Extension Gateway Installation and Configuration** • Demonstrate how to transition physical firewalls to VSX • environment • Demonstrate how to deploy virtual infrastructure with VLAN tagging. **Virtual System Extension Advanced Features** • Describe difference between standard Physical Security Gateway Clusters and VSX Gateway Clusters. • Identify different synchronization modes. • Describe common troubleshooting practices **Lab Exercise Include** • Deploying Multi-Domain Security Management • Converting Security Management Server to Domain Management Server • Importing Existing SMS Configuration into New DMS • Assigning Administrator Privileges • Configuring a Multi-Domain Log Server • Deploying a Global Policy • Implementing MDS High Availability • Licensing Multi-Domain Management • Transitioning Physical Security Gateways into a Virtual Environment • Deploying Virtual Systems and Virtual Network Devices • Implementing VSX Gateway Virtual System Load Sharing.
Course date:	According to customer request
Course place:	Košice, Check Point ATC training center, Intas s.r.o., Stromova 10