Check Point
Multi-Domain Security Management
with Virtual System Extension (MDSM/VSX)

Introduction

Check Point MDSM/VSX - This course prepares the participants to appear for the **CCMSE** certification exam

This course covers everything you need to design, install, configure and manage MDSM with VSX

Duration

5 Days

Prerequisites

Should have good networking knowledge and linux command line.
Must be CCSE on R7x or have equivalent knowledge and working experience

Who Should Attend?

Systems administrators, security engineers, and network engineers who want to virtualize components of their security management, and individuals seeking the Check Point Certified Managed Security Expert (CCMSE) certification

Course Objectives

• Identify the features and functions of MDSM with VSX
• Describe the MDSM with VSX architecture
• Choose the correct MDSM implementation to cover your company's domains
• Classify the various pieces of the MDSM architecture
• Use the correct tools to troubleshoot and solve any issues
• Install MDSM
• Configure the MDSM environment
• Create an MDS Manager
• Install and configure the Smart Domain Manager
• Implement any necessary Management plug-ins
• Configure and implement a Multi-Domain Log Server for the MDSM environment
• Configure and implement a domain Log Server for a given domain
• Configure and implement a Global Policy
• Configure and implement VPNs globally and per domain
• Create a secondary MDS Manager and enable MDS High Availability
• Create and configure secondary DMS
• Configure DMS High Availability based on a domain's requirements
• Identify the VSX components
• Describe the relationship between the VSX components
• Describe the function of VSX Context Identification

Check Point
Multi-Domain Security Management
with Virtual System Extension (MDSM/VSX)

Course Objectives (contd.)

• Describe the Traffic Inspection Process
• Describe the purpose of the Virtual System within the VSX environment
• List various common deployment scenarios
• Demonstrate how to transition physical firewalls to a VSX environment
• Demonstrate hot to deploy virtual infrastructure with VLAN tagging
• Describe the difference between standard Physical Security Gateway Clusters and VSX Gateway Clusters
• Identify the different synchronization modes
• Describe common troubleshooting practices

Lab Exercises Include

• Deploying Multi-Domain Security Management
• Converting a Security Management Server to a Domain Management Server
• Importing an Existing SMS Configuration into a 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 Virtual System Load Sharing