

# CHECK POINT

# SECURITY MASTER

## WHO SHOULD ATTEND

This course is for customers and partners who want to learn the advanced skills to troubleshoot and configure Check Point Security Gateway and Management Software Blades:

- System Administrators
- Security Engineers
- Network Engineers
- CCSEs seeking higher certification

## PREREQUISITES

- CCSE
- General knowledge of TCP/IP
- Working knowledge of Windows and UNIX
- Working knowledge of network technology
- Working knowledge of the Internet

## TABLE OF CONTENTS

Chapter 1: Introduction to Security Master

Chapter 2: Chain Modules

Chapter 3: NAT

Chapter 4: ClusterXL

Chapter 5: VPN Troubleshooting

Chapter 6: SecureXL Acceleration Debugging

Chapter 7: Hardware Optimization

Chapter 8: Software Tuning

Chapter 9: Enable CoreXL

Chapter 10: IPS

Chapter 11: IPv6

Chapter 12: Advanced VPN

## CERTIFICATION INFORMATION

# CCSM

Prepares for exam #156-115.77 at  
[VUE.com/checkpoint](http://VUE.com/checkpoint)

80 multiple-choice questions with a passing score of 70% in 90 minutes. Valid CCSE required.

## COURSE OBJECTIVES AND TOPICS INCLUDE:

- Firewall-1 administration and infrastructure review
- How policy changes impact chain module behavior
- Identify management issues and problems with commands
- Use commands to troubleshoot NAT stages
- Configure Manual NAT to define specific rules
- Use commands to review and clear connections table
- Modify files to allow traffic through a specific cluster member
- Locate the source of encryption failures using commands
- Use commands to verify VPN connectivity
- Identify any potentially mis-configured VPNs
- Tune NIC performance
- Increase size and improve hardware performance
- Improve load capacity
- Tune the firewall rule base
- Reduce load on Rule Base application
- Improve network performance
- Improve logging efficiency
- Use IPS Bypass to manage performance
- Deploy IPv6 in a local environment
- Identify differences between VPNs
- Configure VPN Tunnel Interface (VTI)
- Configure Open Shortest Path First (OSPF)
- Identify the wire mode function by testing a VPN failover

## LAB EXERCISES INCLUDE:

- Evaluate Chain Modules
- Modify Security Policies
- Examine how rules and objects affect optimization
- Troubleshoot Secure Internal Communication issues
- Identify a mis-configured rule
- Identify the source of GUI client connectivity problems
- Improve load capacity through optimization
- Optimize network performance
- Configure Manual NAT
- Troubleshoot ClusterXL and SecureXL
- Configure IPS to reduce false positives
- Identify the speed of the system's CPU
- Identify connections in the ClusterXL debug file
- Troubleshoot a mis-configured VPN
- Identify VPN configuration problems
- Identify acceleration status of current connections
- Identify the source of an encryption failure