CKP-CCAS
Automation Specialist

Overview
2-day course teaches advanced skills to configure and manage Check Point IPS. You will create and monitor a client profile, monitor an attack, customize a protection and learn basic troubleshooting techniques.

Course Design
This course is designed for Technical persons who support, install, deploy or administer Check Point Software blades should attend this course. This could include the following:

- System Administrators
- System Engineers
- Support Analysts
- Network Engineers
- Anyone seeking to extend a Check Point certification

Prerequisites
- Introduction to Check Point IPS Software Blade training
- Working knowledge of Windows and/or Unix
- Basic networking knowledge
- Experience with TCP/IP and the internet

Instructional Method
- This course is available in either classroom or self-paced online formats, and includes access to a live lab environment, as well as demonstrations and the practical application of concepts through hands-on exercises.

Learn How To
- Analyze your data to reduce your risks
- Discover abnormal events, attacks, viruses and worms
- Properly configure DNS, web and mail servers for ongoing protection

How You Will Benefit

- Identify the best IPS deployment strategy for your environment
- Discuss how security policies affect network processes
- Identify your top security events and protections
- Leverage our 5 proven IT security best practices
- Be able to distinguish false positives
- Know how to apply zero-day threat prevention

Course Topics

- Preface: Advanced IPS
  - Advanced IPS Overview
  - Check Point 3D Security
- IPS Management
  - Check Point IPS
  - Learning Objectives:
  - Check Point IPS Overview
  - IPS in SmartDashboard
  - IPS Profiles
  - Activating Protections
  - Protection Browser
  - IPS Updates
  - Network Exceptions
  - Tracking Protections Using Follow Up
  - Geo Protection
  - Bypass Under Load
  - Chapter Review
  - Lab 1: Deploying IPS
- Configuring the IPS Blade
  - Test the Security Policy and Demonstration Tool
  - Testing IPS Functionality
  - Changing IPS Policy Enforcement
  - Lab 2: Deploying Geo Protection in IPS

- Modifying Anti-Spoofing Settings
- Test IPS Geo Protection

- IPS Monitoring
  - Introducing IPS Event Analysis
  - Learning Objectives:
  - IPS Event Analysis
  - IPS Event Analysis Architecture
  - Chapter Review
  - Lab 3: Using Profiles in IPS
  - Testing the Default Protection Profile
  - Define a New Profile
  - Identifying Attacks with Smart Event
- IPS Architecture
  - Introducing IPS Architecture
  - Learning Objectives:
  - Key IPS Architecture Design Elements
  - Performance — Accelerated Integrated IPS
  - Secure — Multi-threat Detection Engine
  - Passive Streaming Library
  - Protocol Parsers
  - Context Management Infrastructure
  - Compound Signature Identification
  - INSPECTv2
  - How the Architecture Runs IPS
  - Chapter Review
  - Lab 4: Manually Updating IPS Protections (Optional)
  - Downloading and Installing IPS Protections
  - Follow Up with IPS Protection Review
  - Lab 5: IPS Troubleshooting Features
  - Configuring and Testing IPS Troubleshooting Mode
  - Configure and Test the IPS Bypass Settings
- IPS Tuning
  - Optimizing IPS

- Learning Objectives:
- Managing Performance Impact
- Tuning Protections
- Enhancing System Performance
- Configure Servers
- Engine Settings
- Chapter Review
- Lab 6: Tuning IPS Performance
- Configuring Protection Engine Settings
- Configuring Server Objects
- Identifying Top Events and Protections
- Modifying Protections to Defend Against Common Attacks
- Debugging the Logging Mechanism

- IPS Debugging
  - IPS Debugging
  - Learning Objectives:
  - IPS Debug Tools
  - SmartView Tracker Modes
  - Packet Capture
  - Kernel Debugging
  - IPS Debugging Scenarios
  - False Positives
  - Performance Issues
  - Logging Issues
  - Pattern Match Debug
  - Packet Dump Buffer
  - Debug Flags Overview
  - Chapter Review
  - Lab 7: Advanced IPS Troubleshooting
  - Using Debug to Gather IPS Statistics
  - Using tcpdump to Identify the Source of an Attack
  - Modifying Protection to Prevent Attack Source
  - Viewing Gateway Messages

- Appendix: Chapter Questions and Answers
  - IPS Management
  - IPS Monitoring
  - IPS Architecture
  - IPS Tuning
  - IPS Debugging