



CHECK POINT ADVANCED IPS (MTC-CPX-011) (2 Days)

OVERVIEW

Check Point Advanced Intrusion Prevention Systems (IPS) is a 2-day instructor-led course, you will learn advanced skills to configure and manage the Check Point IPS Software Blade. You will create, modify and monitor a client profile, monitor an attack, gather IPS statistics, customize a protection, and learn basic troubleshooting techniques.

WHO SHOULD ATTEND?

Technical persons who support, install, deploy or administer Check Point security solutions should attend this course including:

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

PREREQUISITES

Persons attending this course should have general knowledge of TCP/IP, working knowledge of Windows and/or Unix, network technology, the Internet and 6 months experience working in a Check Point security gateway environment.

COURSE OBJECTIVES

- Understand how security policies affect network processes
- Learn how data is used to fine tune processes and reduce risk
- Incorporate 5 proven IT security best practices
- Discuss IPS deployment strategies
- Discuss the layers of the IPS engine
- Describe the unique capabilities of the Check Point IPS engine
- Create and apply profiles to groups of devices that need protection against certain attacks
- Discuss how IPS Mode determines detect or prevent default protections
- Describe how the severity of an attack is determined
- Learn how to schedule automatic updates for ongoing protection
- Use Geo Protection to control traffic by country

- Learn to discover abnormal events, attacks, viruses, or worms when raw data is analyzed Discuss the major components in IPS Event Analysis Architecture
- Describe what you can do with the IPS Event Analysis Client
- Describe why having signatures available that protect against known vulnerability attacks is essential
- Describe how a good IPS solution will have zero-day threat prevention to protect against attacks which exploit unknown or undisclosed vulnerabilities
- Be able to distinguish false positives
- Describe the benefits of SecureXL and CoreXL
- Describe the function of the Passive Streaming Library (PSL)
- Be able to configure how IPS is managed during a cluster failover
- Learn how to focus on high severity and high confidence level protections
- Properly configure hosts like DNS Servers, Web Servers and Mail Servers for IPS protections

LAB EXERCISES INCLUDE

- Configure the IPS Software Blade
- Test the Security Policy and Demonstration Tool
- Test the IPS Functionality
- Change IPS Policy Enforcement
- Deploy Geo Protection in IPS
- Modify Anti-Spoofing settings
- Test IPS Geo Protection features
- Test the Default_Protection profile
- Define a new Profile
- Identify attacks with SmartEvent Viewer
- Download and install IPS protections
- Use the IPS follow-up protection review process
- Manually update the IPS Protections on the gateway to the most current available

- Download and install IPS Protections
- Follow up with IPS Protections Review
- Configure, enable and test IPS Troubleshooting mode
- Modify and test the Bypass Under Load Settings
- Configure Protection Engine settings
- Identify Top Events and Protections
- Modify Protections to defend against common attacks
- Debug the logging mechanism
- Configuring Protection Engine Settings
- Use debug to gather IPS statistics
- Use tcpdump to identify the source of an attack
- Modify protections to prevent attack source
- View Security Gateway messages

Certification Information

This course helps prepare for Check Point Advanced Intrusion Prevention Systems (IPS) **Exam # 156-748.12** available at ExamCentral (login required). Students should have at least 6 months experience with Check Point products before challenging it.



M.Tech Products Pte Ltd
(Education Services)

18 Boon Lay Way, #06-111 TradeHub 21 Singapore 609966

Tel: (65) 6516 0088 Fax: (65) 6779 6553

Email: mtc@mtechpro.com Website: <http://www.mtechpro.com>