2-day instructor-led course teaches how to fight today’s evolving security threats with Check Point’s Next Generation Threat Prevention and Secure Web Gateway solutions. Learn how to activate Application Control, URL Filtering, Identity Awareness, IPS, Anti-Bot, and Anti-Virus protections through guided discussion and hands-on practice.

WHO SHOULD ATTEND?
Technical persons who support, install, deploy or administer Check Point Security solutions should attend this course. This includes:
- System Administrators and Engineers
- Support Analysts
- Network Engineers
- Channel Partners

PREREQUISITES
Persons attending this course should have 6 months experience working with Check Point security gateways; CCSA certification or equivalent knowledge, and general knowledge of TCP/IP, Windows and/or Unix, network technology and the Internet.

COURSE OBJECTIVES
- Identify the Application Control Software Blade as part of a total security management solution.
- Identify and address Web 2.0 application access issues including malware threats, bandwidth impact issues and productivity loss
- Identify important aspects of Application Awareness blade management including how to detect and control application usage and educate users
- Monitor all Facebook and Facebook Application traffic in your organization
- Block YouTube and other streaming media applications
- Update your local Application Database with the most recently added data and applications
- View all current activity occurring in the Application Control Rule Base
- Identify the IPS Software Blade as part of a total security management solution
- Identify and address strategies for implementing the Check Point Intrusion Prevention software blade including sandbox mode, status at a glance and unified management
- Identify important aspects of IPS software blade management including testing and deployment and activation of protections
- Enable Identity Awareness on a gateway together with Application Control to create policy rules
- Discuss the Threat landscape
- Discuss how SensorNET collects and analyzes attack information
- Understand the anatomy of a Bot
- Discuss how Bots are used in an attack
- Learn how Bots infect your computer
- Explain how the Antivirus Software Blade stops incoming malicious files
- Describe Check Point’s data mining process
- Know how to leverage the ThreatWiki
- Discuss the challenges and benefits of log management
- Describe how SmartLog transforms data into security intelligence

LAB EXERCISES INCLUDE
- Investigating Threats in Threat Wiki
- Applying IPS Protections
- Reviewing Anti-Bot & Anti-Virus Protections
- Configuring User Directory
- Protecting your Network from Threats on the Web
- Using SmartEvent to Develop a Corporate Web and Application Profile
- Working with Captive Portal
Training Agenda

DAY 1
09:00-10:30  Check Point 101
10:30-12:00  Practical Exercises
12:00-1:00   Lunch
1:00-01:30   HTTPS Inspection
01:30-03:00  Secure Web Gateway
03:00-04:30  Practical Exercises
04:30-05:00  Summary / Q&A

DAY 2
09:00-11:00  Threat Prevention
11:00-12:00  Practical Exercises
12:00-01:00  Lunch
01:00-03:00  Practical Exercises continued
03:00-03:30  Logging & Management
03:30-04:00  Upgrading to R77
04:00-04:30  600 Appliances
04:30-05:00  Summary / Q&A