

Check Point Secure Web Gateway

Learn to block access to malware infested websites and dangerous Apps

2-day hands-on course teaches how Check Point's Secure Web Gateway enables safe use of the Web and Apps with real-time multi-layered protection that blocks access to malicious malware, phishing and dangerous applications by constantly updating URLs and antivirus signatures from our global network of security intelligence sensors.

WHO SHOULD ATTEND?

This course is designed for customers and partners who want to add a secure web gateway solution to their security strategy. This could include the following:

- System Administrators
- Support Analysts
- Network Engineers

PREREQUISITES

Successful completion of this course depends on knowledge of multiple disciplines related to network-security activities including UNIX and Windows operating systems, Certificate management, system administration, security administration and networking (TCP/IP).

COURSE TOPICS

- How to leverage the ThreatCloud for global security intelligence
- How to identify and block malware
- How to block dangerous websites
- How to apply granular control of applications
- Why IPS is essential to a secure web
- How to get 360 degree visibility of your security profile and events
- The value of a Unified Security Policy

COURSE OBJECTIVES INCLUDE

- Explain the best practices for IT Security
- Describe how ThreatCloud fights cybercrime
- Apply Antivirus
- Explain how URL Filtering categorizes websites
- Discuss how Application Control enables granular control of Web applications and social networking widgets
- Apply proactive intrusion prevention
- Detect infected hosts, identify bot outbreaks, block bot communication
- Describe how Identity Awareness provides granular visibility of users, groups and machines

- Describe how SmartEvent enables you to view users' online behavior and applications
- Explain how Captive Portal authenticates users
- Describe the different between Terminal Server Identity Agent and Endpoint Identity Agent
- Deploy Application Control & URL Filtering
- Configure the Application Control & URL Filtering Policy
- Test Basic Application Control & URL Filtering Functionality
- Deploy SmartEvent Monitor Application Control and URL Filtering Activity
- Configure Application Control & URL Filtering Tracking Mechanisms
- Generate Traffic that Triggers Application Control & URL Filtering
- Customize SmartEvent to Present Application Control & URL Filtering Events
- Investigate Application Control & URL Filtering Events
- Identify Application Control & URL Filtering Activity

LAB EXERCISES INCLUDE

- Configuring User Directory Integration
- Protecting your network from threats on the web
- Developing a corporate web and application profile
- Defining User Exceptions and Advanced Policy Configurations
- Handling HTTPS Inspection
- Blocking high bandwidth applications and URLs
- Working with Captive Portal

CERTIFICATION INFORMATION

This exam prepares for Secure Web Gateway exam #156-726.77 available at VUE test centers www.vue.com/checkpoint.