Check Point
SOFTWARE TECHNOLOGIES LTD

CHECK POINT SECURITY MASTER
STUDY GUIDE - R80

WELCOME TO THE FUTURE OF CYBER SECURITY

CHECK POINT CERTIFIED

SECURITY MASTER

CCSM

International Headquarters:	5 Ha'Solelim Street Tel Aviv 67897, Israel Tel: +972-3-753 4555
U.S. Headquarters:	959 Skyway Road, Suite 300 San Carlos, CA 94070 Tel: 650-628-2000 Fax: 650-654-4233
Technical Support, Education & Professional Services:	6330 Commerce Drive, Suite 120 Irving, TX 75063 Tel: 972-444-6612 Fax: 972-506-7913 E-mail any comments or questions about our courseware to courseware@us.checkpoint.com. For questions or comments about other Check Point documentation, e-mail CP_TechPub_Feedback@checkpoint.com.
Document #:	CPTS-DOC-CCSM-SG-R80

Preface

The Check Point Certified Security Master Course

The *Check Point Security Master* course is designed for security experts who need to perform advanced deployment configurations of a Security Gateway and are working towards their Check Point Certified Cyber Security Master (CCSM) certification.

A course at a location & time convenient to you can be found by visiting this link: https://store.checkpoint.com/training-certification/#/courses/Check-Point-Certified-Master-(CCSM)-R80.10

The following *Check Point Security Master Study Guide – R80* supplements knowledge you have gained from the Security Master course, and is not a sole means of study.

Check Point Certified Cyber Security Master

- Our top technical certification proves the ability to perform advanced troubleshooting
- CCSMs get Expert level access to SecureKnowledge
- The CCSM is entitled to fast path access to Tier 3 Support
- Our CCSMs belong to a small group of elite security professionals in the world

Exam Details:

The Check Point Certified Security Master – R80 exam (exam # 156-115.80) is delivered by Pearson Vue: http://www.pearsonvue.com/checkpoint/

- Exam has 100 questions
- Exam to be completed in 90 minutes in all English speaking countries. Non-English speaking countries receive an accommodation of 15 additional minutes
- Passing score 70%

The prerequisites for this exam are:

- R80 Check Point Certified Cyber Security Expert certification (CCSE) or,
- R77 Check Point Certified Cyber Security Master certification (CCSM)

CCSM Objectives

Chapter 1 - Advanced Database Management

- Obtain a deeper knowledge of the Security Management Architecture.
- Understand how the Security Management Server uses key processes and debugs.
- Review how objects are represented in the database.
- Understand how GuiDBedit operates.

Do you know…?

What is Solr?

Which ports are used for SIC?

Which database does R80.x use for storing all objects?

What is the syntax of a command for debugging issues with the internal Certificate Authority?

Which process is responsible for the Management HA synchronization?

Which command can be used to see the list of processes monitored by the Watch Dog process?

Chapter 2 – Kernel Mode and User Mode Troubleshooting

- Understand how to use **fw monitor** to capture packets.
- Understand how to use the **fw debug** process and debug infrastructures for User mode debugging.
- Discuss how to enable and use core dumps when a User mode process crashes.

Do you know…?

When running a debug with fw monitor, which parameter will create a more verbose output?

What is the proper command for allowing the system to create core files?

Which command will clean the buffer and change all kernel debug properties to the default?

What are benefits of the 'fw ctl zdebug' command?

Which directory are the usermode core files located in?

What are some special considerations that should be taken into consideration while running fw monitor on production firewall?

Chapter 3 - SmartConsole and Policy Management

- Understand how to troubleshoot and debug SmartConsole issues.
- Understand how to troubleshoot and debug issues that may occur during policy installation.

Do you know…?

Which process is first called when the policy installation command is initiated from the SmartConsole?

Explain what the SCConfigManager.exe tool is used for and how to use it?

What information is contained in a crash report from a SmartConsole application crash?

Chapter 4 – Advanced Network Address Translation

- Understand how to troubleshoot and debug NAT issues using Gaia commands.
- Understand Client Side and Server Side NAT.
- Describe how to configure port mapping services.

Do you know…?

Which kernel debug flag should you use to troubleshoot NAT connections?

What is the difference between Client-Side and Server-Side NAT?

What table would you review to investigate a port exhaustion error when using Hide NAT?

Chapter 5 - VPN Troubleshooting

- Recognize how to debug VPN-related issues.

Do you know…?

Which Check Point utility should be used use to assist in analyzing the output of vpn and ike debug?

What is the benefit of running “vpn debug trunc” over “vpn debug on”?

Which command would you use in the process of deleting the IPSec Key to a specific given peer?

Chapter 6 - Troubleshooting Access Control Policies

- Understand the infrastructure processes and components used for policy installation and processing packets in Access Control policies.
- Understand how to troubleshoot and debug issues that may occur with Application Control and URL Filtering.
- Understand how to debug HTTPS Inspection related issues.
- Understand how to troubleshoot and debug Content Awareness issues.

Do you know…?

Which Daemon should be debugged for HTTPS Inspection related issues?

Which daemon would you debug if you have issues with acquiring identities via identity sharing and sharing identities with other gateways?

What does CMI stand for in relation to the Access Control Policy?

Packet processing infrastructure consists of which components?

Chapter 7 - Troubleshooting Threat Prevention Policies

- Understand how to troubleshoot and debug issues that may occur with Threat Prevention Policies.
- Understand how to troubleshoot Anti-Bot and Antivirus issues.
- Discuss how to use IPS Bypass to manage performance issues.
- Understand how to configure IPS to reduce false positives.

Do you know…?

Which process is enabled when the Policy Conversion process has the debug turned on using the INTERNAL_POLICY_LOADING=1 command?

Which daemon is the main CLI process and daemon for Threat Extraction?

How many layers are incorporated in IPS detection and what are they called?

Which daemon is responsible for anti-spam?

Which Threat Prevention daemon is the core Threat Emulation engine and responsible for emulation files and communications with Threat Cloud?

What are some measures you can take to prevent IPS false positives?

Chapter 8 – Optimization and Tuning

- Understand how the server hardware and operating system affects the performance of the Security Gateway.
- Understand how to evaluate hardware configurations for optimal performance.
- Discover additional tools to assist in monitoring CPU utilization.

Do you know…?

What is the command to check the number of CoreXL firewall instances?

What is the default and maximum number of entries in the ARP Cache Table in a Check Point appliance?

How long (in hours) does the CPSizeMe script run by default?

Chapter 9 – Advanced Clustering

- Understand how to monitor cluster status and work with critical devices.
- Recognize how to troubleshoot state synchronization.

Do you know…?

Which command would you use in order to test a ClusterXL failover?

What ClusterXL mechanism is used to verify that the interfaces of other cluster members are UP and communicates the status of cluster members?

What ClusterXL mechanism is used to verify that the interfaces of other cluster members are UP and communicates the status of cluster members?

What does changing the cphaconf set_ccp parameter do?

What command can the administrator run to view the status of the registered critical devices?

What does changing the cphaconf set_ccp parameter do?

Chapter 10 - Acceleration Debugging

- Recognize how to use **fwaccel** and **sim** to enable and disable accelerated traffic.
- Understand how to use **fwaccel dbg** and **sim dbg** commands.
- Understand how to configure CoreXL to enhance Security Gateway performance.

Do you know…?

What mechanism can be used to confirm that important traffic such as control connections are not dropped when a Security Gateway is under high load?

What table does the command "fwaccel conns" pull information from?

Which command would show the synchronization statistics between cluster members?

What is the command to view the SecureXL connection table?

Which command would you use to check CoreXL instances for IPv6 traffic?

What does SIM handle?

Chapter 11 – Deploying IPv6

- Understand how to deploy IPv6 in a local environment

Do you know…?

How would an administrator view the routing table on the Security Gateway of production network where IPv6 is being used?

What is the command to monitor IPv6 traffic in Expert mode?

Which Check Point feature is not supported when running IPv6?

Conclusion

You knew all that?

Already have your CCSE R80 or a CCSM R77?

Does your Pearson VUE profile email address match your User Center profile email address?

Then you are ready. Go to Pearson VUE and request exam:

Check Point Certified Security Master – R80 (156-115.80)

Good testing!