EDUSUM

156-115.77

CCSM R77

A Success Guide to Prepare-
Check Point Security Master

edusum.com

Table of Contents

Introduction to 156-115.77 Exam on Check Point Security Master

Use this quick start guide to collect all the information about Check Point CCSM (156-115.77) Certification exam. This study guide provides a list of objectives and resources that will help you prepare for items on the 156-115.77 Security Master exam. The Sample Questions will help you identify the type and difficulty level of the questions and the Practice Exams will make you familiar with the format and environment of an exam. You should refer this guide carefully before attempting your actual Check Point CCSM R77 certification exam.

The Check Point CCSM certification is mainly targeted to those candidates who want to build their career in Security domain. The Check Point Certified Security Master (CCSM) R77.30 exam verifies that the candidate possesses the fundamental knowledge and proven skills in the area of Check Point CCSM R77.

Check Point 156-115.77 Certification Details:

Exam Name	Check Point Certified Security Master (CCSM) R77.30
Exam Code	156-115.77
Exam Price	$350 (USD)
Duration	90 min
Number of Questions	90
Passing Score	70%
Books / Training	CCSM Training
Schedule Exam	156-115.77
Sample Questions	Check Point CCSM Sample Questions
Practice Exam	**Check Point 156-115.77 Certification Practice Exam**

_____

Check Point 156-115.77 Exam Syllabus:

Topic	Details
Troubleshoot security problems	- Given a specific internal or client problem, replicate the issues in a test environment. - Given a specific internal or client problem, troubleshoot and correct the issue.

Chain Modules	- Use command fw ctl chain to study chain module behavior. Observe how policy changes impact the chain.
	- Use the command fw debug fwm on and review the file fwm.elg to find such issues as SIC, mis-configured rules, GUI client connectivity problems, and improperly entered information.
	- Given a specific internal or client need, analyze and apply the appropriate hot fix and evaluate its effectiveness.
	- Use Check Point Debugging Tools
	
	  1. Reading and identifying fwmonitor outputs
	  2. Generating and interpreting kernel debugs

NAT	- Use commands fw ctl debug and fw monitor to troubleshoot the NAT stages of Automatic Hide NAT and Automatic Static NAT. - Configure Manual NAT to define specific rules in unique NAT environments.
ClusterXL	- Using commands fw ctl debug and fw ctl kdebug troubleshoot ClusterXL connections from information displayed in debug file. - Use commands fw tab –t connections and fw tab –t connections –x to review and clear connections table. - Modify file table.def to allow traffic through a specific cluster member.
VPN Troubleshooting	- Use command vpn debug to locate source of encryption failures. - Use command fw monitor to verify VPN connectivity and identify potentially mis-configured VPN's.
SecureXL Acceleration debugging	- Use commands fw accel and kernel debug to view acceleration tables and verify accelerated connections.
Hardware Optimization	- Identify the correct Check Point Hardware/Appliances for a given scenario - Performance tuning and evaluation of complex networks and technologies - Scope proper sizing of hardware based on customer requirements - Use command ethtool to tune NIC performance. - Edit arp cache table to increase size to improve

_____

Topic	Details
	performance. - Use command fw ctl pstat to improve load capacity. - Use the fwaccel stat and fwaccel stats outputs to tune the firewall rule base.
Software Tuning	- Deploy NAT templates to reduce load on Rule Base application. - Configure cluster synchronization planning to improve network performance. - Identify performance limiting configurations - Correct and tune different scenarios - Identify the causes of performance limiting factors (internal and external factors)
Enable CoreXL	- Configure CoreXL for specific cpu task assignment.
IPS	- Configure IPS to reduce false positives. - Use command fw ctl zdebug to improve logging efficiency. - Use IPS Bypass to improve performance.
IPV6	- Deploy IPV6 in a local environment
Advanced VPN	- Identify differences between route-based VPNs and domain-based VPNs. - Configure VTI for route-based VPN gateways. - Configure OSPF for Dynamic VPN routing in a Community. - Identify the Wire Mode function by testing a VPN failover. - Configure Directional VPN Rule Match for Route-Based VPN.
Dynamic Routing	- Diagnose and solve specific routing issues in a network environment. - Multicast Design and troubleshooting PIM Sparse mode and Dense mode based on GateD and IPSRD - Design/troubleshoot OSPF/BGP in GateD and IPSO IPSRD environments - Static routing and network topologies

156-115.77 Sample Questions:

01. How would one enable 'INSPECT debugging' if one suspects IPS false positives?
a) Run command fw ctl set int enable_inspect_debug 1 from the command line.
b) Toggle the checkbox in Global Properties > Firewalls > Inspection section.
c) WebUI
d) Set the following parameter to true using GuiDBedit:
enable_inspect_debug_compilation.

02. Which file holds global Kernel values to survive reboot in a Check Point R77 gateway?
a) $FWDIR/conf/fwkern.conf
b) $FWDIR/boot/modules/fwkern.conf
c) $FWDIR/boot/confwkern.conf
d) $FWDIR/boot/fwkern.conf

03. Since R76 GAiA, what is the method for configuring proxy ARP entries for manual NAT rules?
a) WebUI or add proxy ARP ... commands via CLISH
b) SmartView Tracker
c) local.arp file
d) SmartDashboard

04. Jane wants to create a VPN using OSPF. Which VPN configuration would you recommend she use?
a) Site-to-site VPN
b) Domain-based VPN
c) Route-based VPN
d) Remote-access VPN

05. Why would you choose to combine dynamic routing protocols and VPNs?
a) All options listed.
b) In the case of one tunnel failure, other tunnels may be used to route the traffic.
c) Dynamic-routing information can propagate over the VPN, utilizing the VPN as just another point-to-point link in the network.
d) The VPN device can be automatically updated with network changes on any VPN peer Gateway without the need to update the VPN Domain's configuration.

06. What is the command to check how many connections the firewall has detected for the SecureXL device?
a) fw tab –t connections –s
b) fw tab -t cphwd_db –s
c) fw tab –t connection –s | grep template
d) fwaccel conns

07. In IPS what does a high confidence rating mean?
a) This is a rating for how confident Check Point is with catching this attack
b) This is a rating for how likely this attack is to penetrate most systems
c) There is a high likelihood of false positives
d) There is a low likelihood of false positives

08. When optimizing a customer firewall Rule Base, what is the BEST way to start the analysis?
a) With the command fwaccel stat followed by the command fwaccel stats.
b) At the top of the Rule Base.
c) Using the hit count column.
d) Using the Compliance Software Blade.

_____

09. To check what is currently set in the Firewall kernel debug input the command:
a) fw ctl multistate
b) fw ctl debug –x
c) fw ctl pstat
d) fw ctl debug

10. Your cluster member is showing a state of "Ready". Which of the following is NOT a reason one would expect for this behaviour?
a) One cluster member is configured for 32 bit and the other is configured for 64 bit
b) CoreXL is configured differently on the two machines
c) The firewall that is showing "Ready" has been upgraded but the other firewall has not yet been upgraded
d) Firewall policy has not yet been installed to the firewall

Answers to 156-115.77 Exam Questions:

Question: 01 Answer: d	Question: 02 Answer: b	Question: 03 Answer: a	Question: 04 Answer: c	Question: 05 Answer: a
Question: 06 Answer: b	Question: 07 Answer: d	Question: 08 Answer: a	Question: 09 Answer: d	Question: 10 Answer: d

Note: If you find any typo or data entry error in these sample questions, we request you to update us by commenting on this page or write an email on feedback@edusum.com

_____