EDUSUM

#1 Online Certification Guide

156-215.80

CCSA R80

A Success Guide to Prepare-
Check Point Security Administrator

edusum.com

Table of Contents

Introduction to 156-215.80 Exam on Check Point Security Administrator

Use this quick start guide to collect all the information about Check Point CCSA (156-215.80) Certification exam. This study guide provides a list of objectives and resources that will help you prepare for items on the 156-215.80 Security Administrator 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 CCSA R80 certification exam.

The Check Point CCSA certification is mainly targeted to those candidates who want to build their career in Security domain. The Check Point Certified Security Administrator (CCSA) R80 exam verifies that the candidate possesses the fundamental knowledge and proven skills in the area of Check Point CCSA R80.

Check Point 156-215.80 Certification Details:

Exam Name	Check Point Certified Security Administrator (CCSA) R80
Exam Code	156-215.80
Exam Price	$250 (USD)
Duration	90 minutes
Number of Questions	90
Passing Score	70%
Books / Training	CCSM Training
Schedule Exam	156-215.80
Sample Questions	Check Point CCSA Sample Questions
Practice Exam	**Check Point 156-215.80 Certification Practice Exam**

Check Point 156-215.80 Exam Syllabus:

Topic	Details
Introduction to Check Point Architecture	1. Performance-based 1. Identify the basic functions of the Web UI. 2. Create and confirm admin users for the network. 3. Configure network messages. 4. Confirm existing network configuration settings. 5. Install and tour the GUI. 2. Knowledge-based 1. Describe the key elements of Check Point's unified, 3-tiered architecture. 2. Interpret the concept of a firewall and understand the mechanisms used for controlling network traffic. 3. Recognize SmartConsole features, functions and tools. 4. Understand Check Point deployment options.
Security Policy Management	1. Performance-based 1. Create multiple administrators and apply different roles/permissions for concurrent administration. 2. Create and configure network, host and gateway objects. 3. Evaluate and manipulate rules in a unified Access Control security policy. 4. Apply policy layers and analyze how they affect traffic inspection. 5. Prepare and schedule backups for the gateway. 2. Knowledge-based 1. Describe the essential elements of a unified security policy. 2. Understand how traffic inspection takes place in a unified security policy. 3. Summarize how administration roles and permissions assist in managing policy. 4. Recall how to implement Check Point backup techniques.

Topic	Details
Check Point Security Solutions	1. Performance-based 1. Evaluate and manage different Check Point security solutions deployed for network access control. 2. Evaluate and manage Check Point security solutions for threat protection. 3. Examine how the Compliance blade monitors your Check Point security infrastructure. 4. Validate existing licenses for products installed on your network. 2. Knowledge-based 1. Recognize Check Point security solutions & products and the way they protect your network. 2. Understand licensing and contract requirements for Check Point security solutions.
Traffic Visibility	1. Performance-based 1. Generate network traffic and use traffic visibility tools to monitor the data. 2. Compare and contrast various tools available for viewing traffic 2. Knowledge-based 1. Identify tools designed to monitor data, determine threats and recognize opportunities for performance improvements. 2. Identify tools designed to respond quickly and efficiently to changes in gateways, tunnels, remote users and traffic flow patterns or security activities.
Basic Concepts of VPN	1. Performance-based 1. Configure and deploy a site-to-site VPN. 2. Test the VPN connection and analyze the tunnel traffic. 2. Knowledge-based 1. Understand VPN deployments and Check Point Communities. 2. Understand how to analyze and interpret VPN tunnel traffic.

Topic	Details
Managing User’s Access	1. Performance-based 1. Create and define user access for a guest wireless user. 2. Test Identity Awareness connection. 2. Knowledge-based 1. Recognize how to define users and user groups for your environment. 2. Understand how to manage user access for internal users and guests.
Working with Cluster XL	1. Performance-based 1. Install and configure ClusterXL with a High Availability configuration. 2. Knowledge-based 1. Describe the basic concept of ClusterXL technology and its advantages.
Administrator Task Implementation	1. Performance-based 1. Review rule-base performance for policy control. 2. Knowledge-based 1. Understand how to perform periodic administrator tasks as specified in Administrator job descriptions.
SmartEvent Reports	1. Performance-based 1. Generate reports that effectively summarize network activity. 2. Knowledge-based 1. Recognize how to effectively create, customize and generate network activity reports.

156-215.80 Sample Questions:

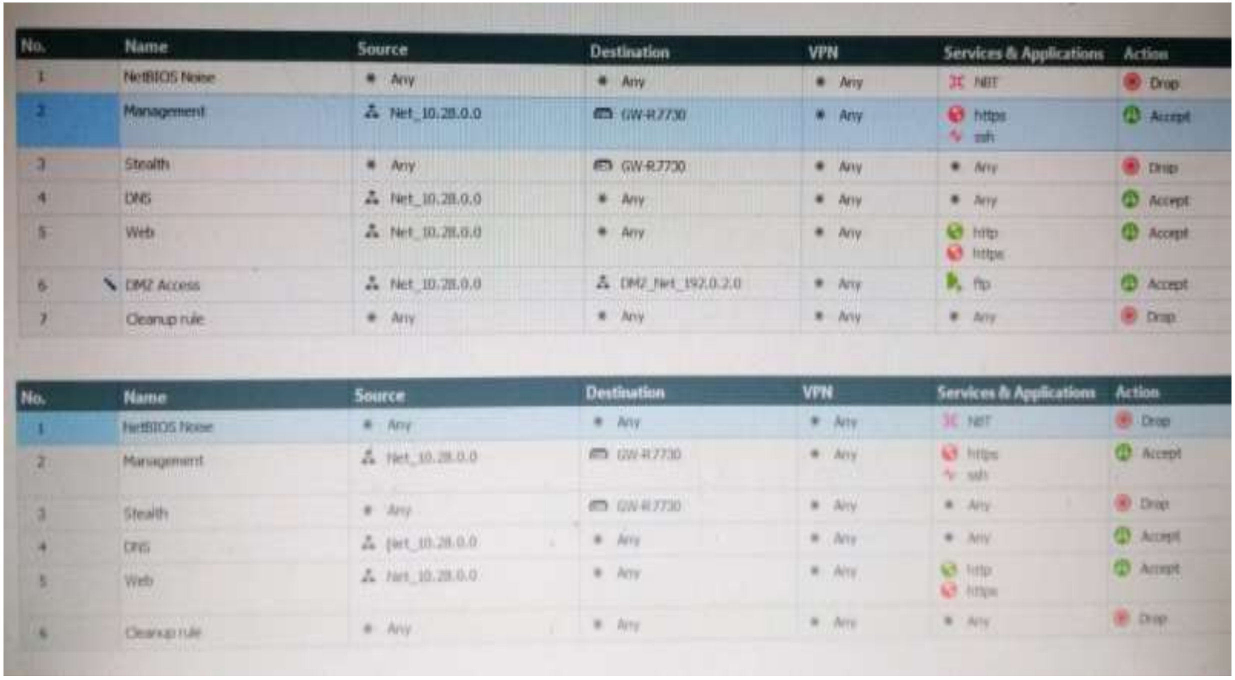
01. Which of the following is NOT an integral part of VPN communication within a network?
a) VPN key
b) VPN community
c) VPN trust enttes
d) VPN domain

02. Fill in the blanks: VPN gateways authenticate using ___________ and ___________.
a) Passwords; tokens
b) Certificates; pre-shared secrets
c) Certificates; passwords
d) Tokens; pre-shared secrets

03. Vanessa is firewall administrator in her company; her company is using Check Point firewalls on central and remote locations, which are managed centrally by R80 Security Management Server. One central location has an installed R77.30 Gateway on Open server. Remote location is using Check Point UTM-1 570 series appliance with R71. Which encryption is used in Secure Internal Communication (SIC) between central management and firewall on each location?
a) On central firewall AES128 encryption is used for SIC, on Remote firewall 3DES encryption is used for SIC.
b) On both firewalls, the same encryption is used for SIC. This is AES-GCM-256.
c) The Firewall Administrator can choose which encryption suite will be used by SIC.
d) On central firewall AES256 encryption is used for SIC, on Remote firewall AES128 encryption is used for SIC.

04. Which Check Point feature enables application scanning and the detection?
a) Application Dictionary
b) Application Library
c) AppWiki
d) CPApp

05. Two administrators Dave and Jon both manage R80 Management as administrators for Alpha Corp. Jon logged into the R80 Management and then shortly after Dave logged in to the same server. They are both in the Security Policies view. From the screenshots below, why does Dave not have the rule no.6 in his SmartConsole view even though Jon has it his in his SmartConsole view?



No.	Name	Source	Destination	VPN	Services & Applications	Action
1	NetBIOS Noise	Any	Any	Any	NBT	Drop
2	Management	Net_10.28.0.0	GW-R7730	Any	https ssh	Accept
3	Stealth	Any	GW-R7730	Any	Any	Drop
4	DNS	Net_10.28.0.0	Any	Any	Any	Accept
5	Web	Net_10.28.0.0	Any	Any	http https	Accept
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	Any	ftp	Accept
7	Cleanup rule	Any	Any	Any	Any	Drop

No.	Name	Source	Destination	VPN	Services & Applications	Action
1	NetBIOS Noise	Any	Any	Any	NBT	Drop
2	Management	Net_10.28.0.0	GW-R7730	Any	https ssh	Accept
3	Stealth	Any	GW-R7730	Any	Any	Drop
4	DNS	Net_10.28.0.0	Any	Any	Any	Accept
5	Web	Net_10.28.0.0	Any	Any	http https	Accept
6	Cleanup rule	Any	Any	Any	Any	Drop

a) Jon is currently editing rule no.6 but has Published part of his changes.
b) Dave is currently editing rule no.6 and has marked this rule for deletion.
c) Dave is currently editing rule no.6 and has deleted it from his Rule Base.
d) Jon is currently editing rule no.6 but has not yet Published his changes.

06. DLP and Geo Policy are examples of what type of Policy?
a) Standard Policies
b) Shared Policies
c) Inspection Policies
d) Unified Policies

07. Which of the following is NOT a SecureXL traffic flow?
a) Medium Path
b) Accelerated Path
c) Fast Path
d) Slow Path

08. Fill in the blank: The ___________ is used to obtain identification and security information about network users.
a) User Directory
b) User server
c) User Check
d) User index

09. In R80 spoofing is defined as a method of:
a) Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
b) Hiding your firewall from unauthorized users.
c) Detecting people using false or wrong authentication logins
d) Making packets appear as if they come from an authorized IP address.

10. Which of the following Automatically Generated Rules NAT rules have the lowest implementation priority?
a) Machine Hide NAT
b) Address Range Hide NAT
c) Network Hide NAT
d) Machine Static NAT

Answers to 156-215.80 Exam Questions:

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

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