EDUSUM
#1 Online Certification Guide

CHECK POINT 156-315.80

Check Point CCSE R80 Certification Questions & Answers

Exam Summary – Syllabus –Questions

156-315.80
[Check Point Certified Security Expert (CCSE) R80](#)
100 Questions Exam – 70% Cut Score – Duration of 90 minutes

Table of Contents:

Know Your 156-315.80 Certification Well:

The 156-315.80 is best suitable for candidates who want to gain knowledge in the Check Point Security. Before you start your 156-315.80 preparation you may struggle to get all the crucial CCSE R80 materials like 156-315.80 syllabus, sample questions, study guide.

But don't worry the 156-315.80 PDF is here to help you prepare in a stress free manner.

The PDF is a combination of all your queries like-
- What is in the 156-315.80 syllabus?
- How many questions are there in the 156-315.80 exam?
- Which Practice test would help me to pass the 156-315.80 exam at the first attempt?

Passing the 156-315.80 exam makes you Check Point Certified Security Expert (CCSE) R80. Having the CCSE R80 certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Check Point 156-315.80 CCSE R80 Certification Details:

Exam Name	Check Point Certified Security Expert (CCSE) R80
Exam Code	156-315.80
Exam Price	$250 (USD)
Duration	90 mins
Number of Questions	100
Passing Score	70%
Books / Training	**CCSE Training**
Schedule Exam	**Pearson VUE**
Sample Questions	**Check Point CCSE Sample Questions**
Practice Exam	**Check Point 156-315.80 Certification Practice Exam**

156-315.80 Syllabus:

Topic	Details
Upgrading	Objectives: 1. Perform a backup of a Security Gateway and Management Server using your 2. Understanding of the differences between backups, snapshots, and upgrade-exports. 3. Upgrade and troubleshoot a Management Server using a database migration. 4. Upgrade and troubleshoot a clustered Security Gateway deployment.
Backup and Restore Security Gateways and Management Servers	- Snapshot management - Upgrade Tools - Backup Schedule Recommendations - Upgrade Tools - Performing Upgrades - Support Contract
Upgrading Standalone Full High Availability	
Lab 1: Upgrading to Check Point R77	- Install Security Management Server - Migrating Management server Data - Importing the Check Point Database - Launch SmartDashboard - Upgrading the Security Gateway
Advanced Firewall	Objectives: 1. Using knowledge of Security Gateway infrastructure, including chain modules, packet flow and kernel tables to describe how to perform debugs on firewall processes.
Check Point Firewall Infrastructure	- GUI Clients - Management
Security Gateway	- User and Kernel Mode Processes - CPC Core Process - FWM - FWD - CPWD - Inbound and Outbound Packet Flow - Inbound FW CTL Chain Modules - Outbound Chain Modules

Topic	Details
Kernel Tables	- Columns in a Chain - Stateful Inspection - Connections Table - Connections Table Format
Check Point Firewall Key Features	- Packet Inspection Flow - Policy Installation Flow - Policy Installation Process - Policy Installation Process Flow
Network Address Translation	- How NAT Works - Hide NAT Process - Security Servers - How a Security Server Works - Basic Firewall Administration - Common Commands
FW Monitor	- What is FW Monitor - C2S Connections and S2C Packets fw monitor
Lab 2: Core CLI Elements of Firewall Administration	- Policy Management and Status - Verification from the CLI - Using cpinfo - Run cpinfo on the Security Management Server - Analyzing cpinfo in InfoView - Using fw ctl pstat - Using tcpdump
Clustering and Acceleration	Objectives: 1. Build, test and troubleshoot a ClusterXL Load Sharing deployment on an enterprise network. 2. Build, test and troubleshoot a ClusterXL High Availability deployment on an enterprise network. 3. Build, test and troubleshoot a management HA deployment on an enterprise network. 4. Configure, maintain and troubleshoot SecureXL and CoreXL acceleration solutions on the corporate network traffic to ensure noted performance enhancement on the firewall. 5. Build, test and troubleshoot a VRRP deployment on an enterprise network.
VRRP	- VRRP vs ClusterXL - Monitored Circuit VRRP - Troubleshooting VRRP
Clustering and Acceleration	- Clustering Terms

Topic	Details
	- ClusterXL - Cluster Synchronization - Synchronized-Cluster Restrictions - Securing the Sync Interface - To Synchronize or Not to Synchronize
ClusterXL: Load Sharing	- Multicast Load Sharing - Unicast Load Sharing - How Packets Travel Through a Unicast - LS Cluster - Sticky Connections
Maintenance Tasks and Tools	- Perform a Manual Failover of the FW Cluster - Advanced Cluster Configuration
Management HA	- The Management High Availability Environment - Active vs. Standby - What Data is Backed Up? - Synchronization Modes - Synchronization Status
SecureXL: Security Acceleration	- What SecureXL Does - Packet Acceleration - Session Rate Acceleration - Masking the Source Port - Application Layer Protocol - An Example with HTTP HTTP 1.1 - Factors that Preclude Acceleration - Factors that Preclude Templating (Session Acceleration) - Packet Flow - VPN Capabilities
CoreXL: Multicore Acceleration	- Supported Platforms and Features - Default Configuration - Processing Core Allocation - Allocating Processing Cores - Adding Processing Cores to the Hardware - Allocating an Additional Core to the SND - Allocating a Core for Heavy Logging - Packet Flows with SecureXL Enabled
Lab 3 Migrating to a Clustering Solution	- Installing and Configuring the Secondary Security Gateway Re-configuring the Primary Gateway - Configuring Management Server Routing - Configuring the Cluster Object - Testing High Availability

Topic	Details
	- Installing the Secondary Management Server - Configuring Management High Availability
Advanced User Management	Objectives: 1. Using an external user database such as LDAP, configure User Directory to incorporate user information for authentication services on the network. 2. Manage internal and external user access to resources for Remote Access or across a VPN. 3. Troubleshoot user access issues found when implementing Identity Awareness.
User Management	- Active Directory OU Structure - Using LDAP Servers with Check Point - LDAP User Management with User Directory - Defining an Account Unit - Configuring Active Directory Schemas - Multiple User Directory (LDAP) Servers - Authentication Process Flow - Limitations of Authentication Flow - User Directory (LDAP) Profiles
Troubleshooting User Authentication and User Directory (LDAP)	- Common Configuration Pitfalls - Some LDAP Tools - Troubleshooting User Authentication
Identity Awareness	- Enabling AD Query - AD Query Setup - Identifying users behind an HTTP Proxy - Verifying there's a logged on AD user at the source IP - Checking the source computer OS - Using SmartView Tracker
Lab 4: Configuring SmartDashboard to Interface with Active Directory	- Creating the Active Directory Object in SmartDashboard - Verify SmartDashboard Communication with the AD Server
Advanced IPsec VPN and Remote Access	Objectives: 1. Using your knowledge of fundamental VPN tunnel concepts, troubleshoot a site-to-site or certificate-based VPN on a corporate gateway using IKEView, VPN log files and commandline debug tools.

Topic	Details
	2. Optimize VPN performance and availability by using Link Selection and Multiple Entry Point solutions. 3. Manage and test corporate VPN tunnels to allow for greater monitoring and scalability with multiple tunnels defined in a community including other VPN providers.
Advanced VPN Concepts and Practices	- IPsec - Internet Key Exchange (IKE) - IKE Key Exchange Process – Phase 1/ Phase 2 Stages
Remote Access VPNs	- Connection Initiation - Link Selection
Multiple Entry Point VPNs	- How Does MEP Work - Explicit MEP - Implicit MEP
Tunnel Management	- Permanent Tunnels - Tunnel Testing - VPN Tunnel Sharing - Tunnel-Management Configuration - Permanent-Tunnel Configuration - Tracking Options - Advanced Permanent-Tunnel configuration - VPN Tunnel Sharing Configuration
Troubleshooting	- VPN Encryption Issues
VPN Debug	- vpn debug Command - vpn debug on | off - vpn debug ikeon |ikeoff - vpn Log Files - vpn debug trunc - VPN Environment Variables - vpn Command - vpn tu - Comparing SAs
Lab 5: Configure Site-to-Site VPNs with Third Party Certificates	- Configuring Access to the Active Directory Server - Creating the Certificate - Importing the Certificate Chain and Generating Encryption Keys - Installing the Certificate - Establishing Environment Specific Configuration - Testing the VPN Using 3rd Party Certificates

Topic	Details
Lab 6: Remote Access with Endpoint Security VPN	- Defining LDAP Users and Groups - Configuring LDAP User Access - Defining Encryption Rules - Defining Remote Access Rules - Configuring the Client Side
Auditing and Reporting	Objectives: 1. Create Events or use existing event definitions to generate reports on specific network traffic using SmartReporter and SmartEvent in <u>order</u> to provide industry compliance information to management. 2. Using your knowledge of SmartEvent architecture and module communication, troubleshoot report generation given command-line tools and debug-file information.
Auditing and Reporting Process	- Auditing and Reporting Standards
SmartEvent	- SmartEvent Intro
SmartEvent Architecture	- Component Communication Process - Event Policy User Interface
SmartReporter	- Report Types
Lab 7: SmartEvent and SmartReporter	- Configure the Network Object in SmartDashboard - Configuring Security Gateways to work with SmartEvent - Monitoring Events with SmartEvent - Generate Reports Based on Activities

Check Point 156-315.80 Sample Questions:

Question: 1

In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?

a) SND is a feature to accelerate multiple SSL VPN connections
b) SND is an alternative to IPSec Main Mode, using only 3 packets
c) SND is used to distribute packets among Firewall instances
d) SND is a feature of fw monitor to capture accelerated packets

Answer: c

Question: 2

What is true of the API server on R80.10?
- a) By default the API-server is activated and does not have hardware requirements
- b) By default the API-server is not active and should be activated from the WebUI
- c) By default the API server is active on management and stand-alone servers with 16GB of RAM (or more)
- d) By default, the API server is active on management servers with 4 GB of RAM (or more) and on stand-alone servers with 8 GB of RAM (more)

Answer: d

Question: 3

After successfully exporting a policy package, how would you import that package into another SMS database in R80.10?

- a) import_package.py
- b) upgrade_import
- c) migrate
- d) cp_merge

Answer: b

Question: 4

When using Monitored circuit VRRP, what is a priority delta?

- a) When an interface fails the priority changes to the priority delta
- b) When an interface fails the delta claims the priority
- c) When an interface fails the priority delta is subtracted from the priority
- d) When an interface fails the priority delta decides if the other interfaces takes over

Answer: c

Question: 5

Which GUI client is supported in R80?
- a) SmartProvisioning
- b) SmartView Tracker
- c) SmartView Monitor
- d) SmartLog

Answer: c

Question: 6

What is the most recommended way to install patches and hotfixes?

a) CPUSE Check Point Update Service Engine
b) rpm –Uv
c) Software Update Service
d) UnixInstallScript

Answer: a

Question: 7

Within a Mobile Access mobile profile, where do you configure jail-broken devices?

a) Session Settings
b) Authentication Settings
c) Allowed Devices
d) Access Settings

Answer: d

Question: 8

Which is not a blade option when configuring SmartEvent?

a) Correlation Unit
b) SmartEvent Unit
c) SmartEvent Server
d) Log Server

Answer: b

Question: 9

Which web services protocol is used to communicate to the Check Point R80 Identity Awareness Web API?

a) SOAP
b) REST
c) XLANG
d) XML-RPC

Answer: b

Question: 10

What command lists all interfaces using Multi-Queue?

a) cpmq get
b) show interface all
c) cpmq set
d) show multiqueue all

Answer: a

Study Guide to Crack Check Point CCSE R80 156-315.80 Exam:

- Getting details of the 156-315.80 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 156-315.80 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Check Point provided training for 156-315.80 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 156-315.80 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 156-315.80 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for 156-315.80 Certification

Make EduSum.com your best friend during your Check Point Security Expert exam preparation. We provide authentic practice tests for the 156-315.80 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual 156-315.80 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the 156-315.80 exam.

Start Online practice of 156-315.80 Exam by visiting URL
https://www.edusum.com/check-point/156-31580-security-expert