EDUSUM

#1 Online Certification Guide

156-915.77

CCSE R77

A Success Guide to Prepare-
Check Point Security Expert Update

edusum.com

Table of Contents

Introduction to 156-915.77 Exam on Check Point Security Expert Update

Use this quick start guide to collect all the information about Check Point CCSE (156-915.77) Certification exam. This study guide provides a list of objectives and resources that will help you prepare for items on the 156-915.77 Security Expert Update 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 CCSE R77 certification exam.

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

Check Point 156-915.77 Certification Details:

Exam Name	Check Point Certified Security Expert (CCSE) R77.30 Update
Exam Code	156-915.77
Exam Price	$250 (USD)
Duration	90 min
Number of Questions	90
Passing Score	70%
Books / Training	CCSE Training
Schedule Exam	156-915.77
Sample Questions	Check Point CCSE Sample Questions
Practice Exam	**Check Point 156-915.77 Certification Practice Exam**

Check Point 156-915.77 Exam 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 - Columns in a Chain - Stateful Inspection
Kernel Tables	- Connections Table - Connections Table Format

Topic	Details
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 - 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

Topic	Details
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 - 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

Topic	Details
	- 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. 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

Topic	Details
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
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 order 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

156-915.77 Sample Questions:

01. Choose the BEST sequence for configuring user managemetn in SmartDashboard, using an LDAP server.
a) Configure a workstation object for the LDAP server, configure a server object for the LDAP Account Unit, and enable LDAP in Global Properties.
b) Configure a server object for the LDAP Account Unit, and create an LDAP resource object
c) Enable LDAP in Global Properties, configure a host-node object for the LDAP server, and configure a server object for the LDAP Account Unit.
d) Configure a server object for the LDAP Account Unit, enable LDAP in Global Properties, and create an LDAP resource object.

02. During an upgrade to the management server, the contract file is transferred to a gateway when the gateway is upgraded. Where is the contract file retrieved from:
a) ISO
b) Technical Support
c) Management.
d) User Center.

03. How many Events can be shown at one time in the Event preview pane?
a) 5,000
b) 30,000
c) 15,000
d) 1,000

04. User definitions are stored in _____.
a) $FWDIR/conf/fwmuser.conf
b) $FWDIR/conf/users/NDB
c) $FWDIR/conf/fwauth.NDB
d) $FWDIR/conf/conf/fwusers.conf

05. Remote clients are using IPSec VPN to authenticate via LDAP server to connect to the organization. Which gateway process is responsible for the authentication?
a) vpnd
b) cvpnd
c) fwm
d) fwd

06. A zero downtime upgrade of a cluster:
a) Upgrades all cluster members except one at the same time
b) Is only supported in major releases (R70,to R71, R71 to R77)
c) Treats each individual cluster member as an individual gateway
d) Requires breaking the cluster and upgrading members independently.

07. For Management High Availability synchronization, what does the Advance status mean?
a) The peer SMS has not been synchronized properly.
b) The peer SMS is properly synchronized.
c) The peer SMS is more up-to-date.
d) The active SMS and its peer have different installed policies and databases.

08. If both domain-based and route-based VPN's are configured, which will take precedence?
a) Route-based
b) Must be chosen/configured manually by the Administrator in the Policy > Global Properties
c) Domain-based
d) Must be chosen/configured manually by the Administrator in the VPN community object

09. At what router prompt would you save your OSPF configuration?
a) ocalhost.localdomain(config-router-ospf)#
b) localhost.localdomain(config-if)#
c) localhost.localdomain(config)#
d) localhost.localdomain#

10. A ClusterXL configuration is limited to ___ members.
a) There is no limit.
b) 16
c) 6
d) 2

Answers to 156-915.77 Exam Questions:

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