# Check Point Certified Security Administrator (CCSA R80)

## Checkpoint 156-215.80

## Version Demo

**Total Demo Questions: 13**

**Total Premium Questions: 536**

**Buy Premium PDF**

https://dumpsboss.com

support@dumpsboss.com

## QUESTION NO: 1

While enabling the Identity Awareness blade the Identity Awareness wizard does not automatically detect the windows domain. Why does it not detect the windows domain?

**A.** Security Gateways is not part of the Domain

**B.** SmartConsole machine is not part of the domain

**C.** Security Management Server is not part of the domain

**D.** Identity Awareness is not enabled on Global properties

## ANSWER: B

**Explanation:**

To enable Identity Awareness:

1. Log in to SmartDashboard.

2. From the Network Objects tree, expand the Check Point branch.

3. Double-click the Security Gateway on which to enable Identity Awareness.

4. In the Software Blades section, select Identity Awareness on the Network Security tab.

The Identity Awareness Configuration wizard opens.

5. Select one or more options. These options set the methods for acquiring identities of managed and unmanaged assets.

- AD Query - Lets the Security Gateway seamlessly identify Active Directory users and computers.
- Browser-Based Authentication - Sends users to a Web page to acquire identities from unidentified users. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.
- Terminal Servers - Identify users in a Terminal Server environment (originating from one IP address). See Choosing Identity Sources.

Note - When you enable Browser-Based Authentication on a Security Gateway that is on an IP Series appliance, make sure to set the Voyager management application port to a port other than 443 or 80.

6. Click Next.

The Integration With Active Directory window opens.

When SmartDashboard is part of the domain, SmartDashboard suggests this domain automatically. If you select this domain, the system creates an LDAP Account Unit with all of the domain controllers in the organization's Active Directory.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62050.htm

## QUESTION NO: 2

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.

## ANSWER: A

**Explanation:**

Gateways above R71 use AES128 for SIC. If one of the gateways is R71 or below, the gateways use 3DES.

Reference:
http://dl3.checkpoint.com/paid/74/74d596decb6071a4ee642fbdaae7238f/CP_R80_SecurityManagement_AdminGuide.pdf?HashKey=1479584563_6f823c8ea1514609148aa4fec5425db2&xtn=.pdf

## QUESTION NO: 3

Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

**A.** Go to clash-Run cpstop | Run cpstart

**B.** Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway

**C.** Administrator does not need to perform any task. Check Point will make use of the newly installed CPU and Cores

**D.** Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy

## ANSWER: B

## QUESTION NO: 4

Which of the following describes how Threat Extraction functions?

**A.** Detect threats and provides a detailed report of discovered threats

**B.** Proactively detects threats

**C.** Delivers file with original content

**D.** Delivers PDF versions of original files with active content removed

**ANSWER: B**

## QUESTION NO: 5

Which of the following is NOT a tracking option? (Choose three.)

**A.** Partial log

**B.** Log

**C.** Network log

**D.** Full log

**ANSWER: A C D**

**Explanation:**

Reference:
https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_LoggingAndMonitoring_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/

CP_R80.10_LoggingAndMonitoring_AdminGuide/131914

## QUESTION NO: 6

Which of the following ClusterXL modes uses a non-unicast MAC address for the cluster IP address.

**A.** High Availability

**B.** Load Sharing Multicast

**C.** Load Sharing Pivot

**D.** Master/Backup

**ANSWER: B**

**Explanation:**

ClusterXL uses the Multicast mechanism to associate the virtual cluster IP addresses with all cluster members. By binding these IP addresses to a Multicast MAC address, it ensures that all packets sent to the cluster, acting as a gateway, will reach all members in the cluster.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7292.htm

## QUESTION NO: 7

What does it mean if Deyra sees the gateway status:

| Status | Name | IP | Versi... | Active Bla... |
|---|---|---|---|---|
| | A-GW | 10.1.1.1 | R80 | |
| | SMS | 10.1.1.101 | R80 | |

**A.** SmartCenter Server cannot reach this Security Gateway

**B.** There is a blade reporting a problem

**C.** VPN software blade is reporting a malfunction

**D.** Security Gateway's MGNT NIC card is disconnected.

## ANSWER: B

**Explanation:**


Reference: https://sc1.checkpoint.com/sc/SolutionsStatics/NEW_SK_NOID1493612962436/active1704302237.fw.png

## QUESTION NO: 8

Choose what BEST describes the Policy Layer Traffic Inspection.

**A.** If a packet does not match any of the inline layers, the matching continues to the next Layer.

**B.** If a packet matches an inline layer, it will continue matching the next layer.

**C.** If a packet does not match any of the inline layers, the packet will be matched against the Implicit Clean-up Rule.

**D.** If a packet does not match a Network Policy Layer, the matching continues to its inline layer.

## ANSWER: B

**Explanation:**

Reference: https://community.checkpoint.com/thread/1092

## QUESTION NO: 9

Your manager requires you to setup a VPN to a new business partner site. The administrator from the partner site gives you his VPN settings and you notice that he setup AES 128 for IKE phase 1 and AES 256 for IKE phase 2. Why is this a problematic setup?

**A.** The two algorithms do not have the same key length and so don't work together. You will get the error … No proposal chosen…

**B.** All is fine as the longest key length has been chosen for encrypting the data and a shorter key length for higher performance for setting up the tunnel.

**C.** Only 128 bit keys are used for phase 1 keys which are protecting phase 2, so the longer key length in phase 2 only costs performance and does not add security due to a shorter key in phase 1.

**D.** All is fine and can be used as is.

**ANSWER: C**

## QUESTION NO: 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

**ANSWER: B C**

**Explanation:**

SmartDashboard organizes the automatic NAT rules in this order:

1. Static NAT rules for Firewall, or node (computer or server) objects

2. Hide NAT rules for Firewall, or node objects

3. Static NAT rules for network or address range objects

4. Hide NAT rules for network or address range objects

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmin/6724.htm

## QUESTION NO: 11

Which of the following is NOT a VPN routing option available in a star community?

**A.** To satellites through center only

**B.** To center, or through the center to other satellites, to Internet and other VPN targets

**C.** To center and to other satellites through center

**D.** To center only

**ANSWER: A D**

**Explanation:**

SmartConsole

For simple hubs and spokes (or if there is only one Hub), the easiest way is to configure a VPN star community in R80 SmartConsole:

1. On the Star Community window, in the:

a. Center Gateways section, select the Security Gateway that functions as the "Hub".

b. Satellite Gateways section, select Security Gateways as the "spokes", or satellites.

2. On the VPN Routing page, Enable VPN routing for satellites section, select one of these options:

a. To center and to other Satellites through center - This allows connectivity between the Security Gateways, for example if the spoke Security Gateways are DAIP Security Gateways, and the Hub is a Security Gateway with a static IP address.

b. To center, or through the center to other satellites, to internet and other VPN targets - This allows connectivity between the Security Gateways as well as the ability to inspect all communication passing through the Hub to the Internet.

3. Create an appropriate Access Control Policy rule.

4. NAT the satellite Security Gateways on the Hub if the Hub is used to route connections from Satellites to the Internet.

The two Dynamic Objects (DAIP Security Gateways) can securely route communication through the Security Gateway with the static IP address.

Reference: https://sc1.checkpoint.com/documents/R80/CP_R80BC_VPN/html_frameset.htm

**QUESTION NO: 12**

Which of these statements describes the Check Point ThreatCloud?

**A.** Blocks or limits usage of web applications

**B.** Prevents or controls access to web sites based on category

**C.** Prevents Cloud vulnerability exploits

**D.** A worldwide collaborative security network

**ANSWER: D**

**Explanation:**

Reference: https://www.checkpoint.com/support-services/threatcloud-managed-security-service/

**QUESTION NO: 13**

A Cleanup rule:

**A.** logs connections that would otherwise be dropped without logging by default.

**B.** drops packets without logging connections that would otherwise be dropped and logged by default.

**C.** logs connections that would otherwise be accepted without logging by default.

**D.** drops packets without logging connections that would otherwise be accepted and logged by default.

**ANSWER: A**