156-215.80$^{Q\&As}$

Check Point Certified Security Administrator

Pass CheckPoint 156-215.80 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/156-215-80.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

Which of the following is NOT a role of the SmartCenter:

A. Status monitoring

B. Policy configuration

C. Certificate authority

D. Address translation

Correct Answer: C

Reference: www.checkfirewalls.com/datasheets/smartcenter_datasheet.pdf

QUESTION 2

Which of the following is NOT a SecureXL traffic flow?

A. Medium Path

B. Accelerated Path

C. Fast Path

D. Slow Path

Correct Answer: C

SecureXL is an acceleration solution that maximizes performance of the Firewall and does not compromise security. When SecureXL is enabled on a Security Gateway, some CPU intensive operations are processed by virtualized software instead of the Firewall kernel. The Firewall can inspect and process connections more efficiently and accelerate throughput and connection rates. These are the SecureXL traffic flows:

Slow path - Packets and connections that are inspected by the Firewall and are not processed by SecureXL.
Accelerated path - Packets and connections that are offloaded to SecureXL and are not processed by the Firewall.
Medium path - Packets that require deeper inspection cannot use the accelerated path. It is not necessary for the Firewall to inspect these packets, they can be offloaded and do not use the slow path. For example, packets that are inspected by IPS cannot use the accelerated path and can be offloaded to the IPS PSL (Passive Streaming Library). SecureXL processes these packets more quickly than packets on the slow path.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92711.htm

QUESTION 3

In the Check Point Security Management Architecture, which component(s) can store logs?

A. SmartConsole

B. Security Management Server and Security Gateway

C. Security Management Server

D. SmartConsole and Security Management Server

Correct Answer: B

QUESTION 4

What is also referred to as Dynamic NAT?

A. Automatic NAT

B. Static NAT

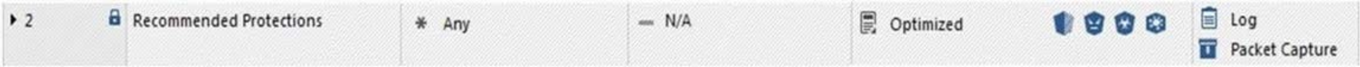
C. Manual NAT

D. Hide NAT

Correct Answer: D

QUESTION 5

View the rule below. What does the lock-symbol in the left column mean? Select the BEST answer.



▸ 2	🔒	Recommended Protections	✱ Any	— N/A	Optimized	Log Packet Capture

A. The current administrator has read-only permissions to Threat Prevention Policy.

B. Another user has locked the rule for editing.

C. Configuration lock is present. Click the lock symbol to gain read-write access.

D. The current administrator is logged in as read-only because someone else is editing the policy.

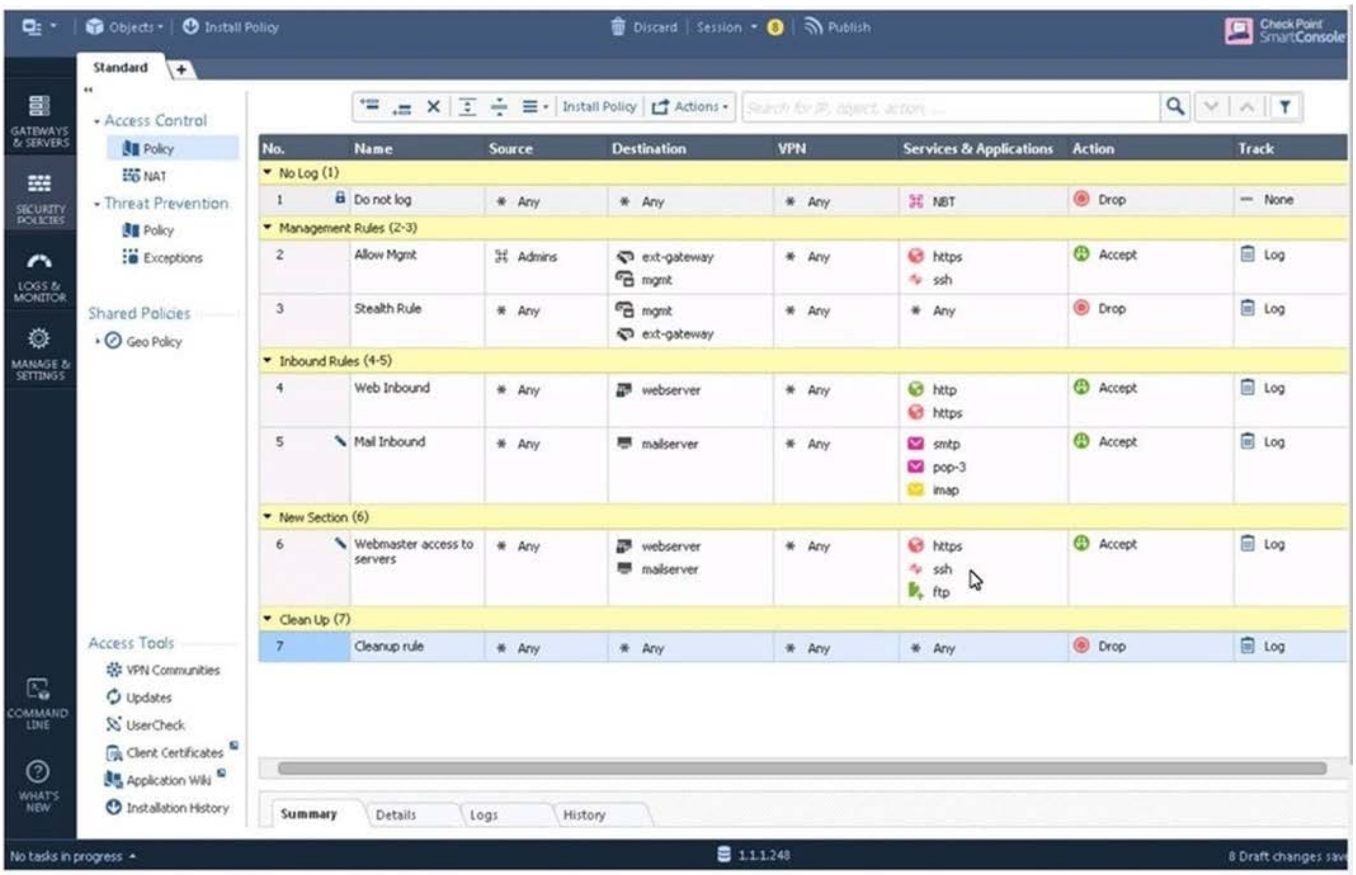
Correct Answer: B

Administrator Collaboration More than one administrator can connect to the Security Management Server at the same time. Every administrator has their own username, and works in a session that is independent of the other administrators. When an administrator logs in to the Security Management Server through SmartConsole, a new editing session starts. The changes that the administrator makes during the session are only available to that administrator. Other administrators see a lock icon on object and rules that are being edited.

To make changes available to all administrators, and to unlock the objects and rules that are being edited, the administrator must publish the session. Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/124265

QUESTION 6

Examine the following Rule Base.



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
No Log (1)							
1	Do not log	Any	Any	Any	NBT	Drop	None
Management Rules (2-3)							
2	Allow Mgmt	Admins	ext-gateway mgmt	Any	https ssh	Accept	Log
3	Stealth Rule	Any	mgmt ext-gateway	Any	Any	Drop	Log
Inbound Rules (4-5)							
4	Web Inbound	Any	webserver	Any	http https	Accept	Log
5	Mail Inbound	Any	mailserver	Any	smtp pop-3 imap	Accept	Log
New Section (6)							
6	Webmaster access to servers	Any	webserver mailserver	Any	https ssh ftp	Accept	Log
Clean Up (7)							
7	Cleanup rule	Any	Any	Any	Any	Drop	Log

No tasks in progress

1.1.1.248

8 Draft changes sav

What can we infer about the recent changes made to the Rule Base?

A. Rule 7 was created by the \\'admin\\' administrator in the current session

B. 8 changes have been made by administrators since the last policy installation

C. Te rules 1, 5 and 6 cannot be edited by the \\'admin\\' administrator

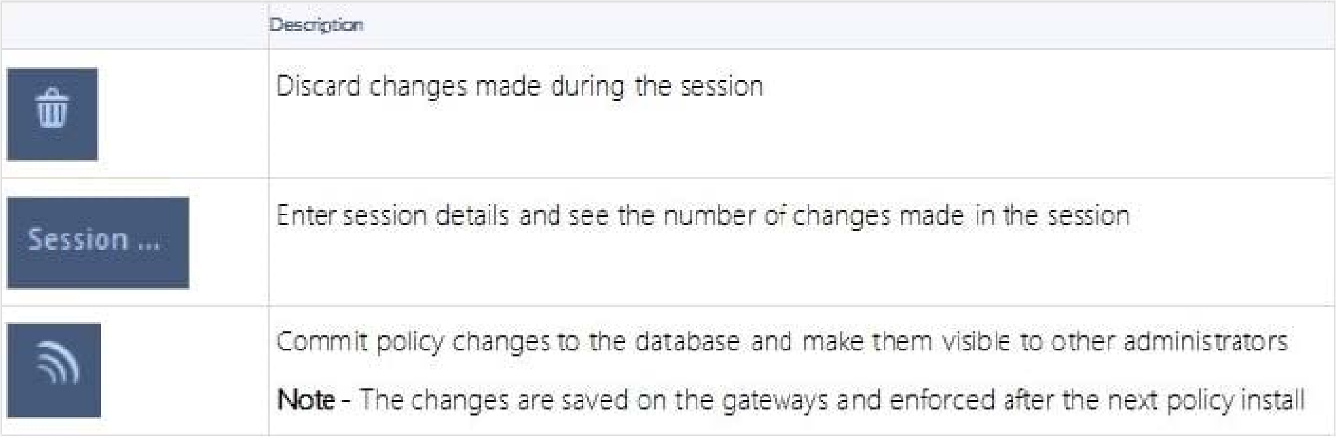
D. Rule 1 and object webserver are locked by another administrator

Correct Answer: D

Explantation:

On top of the print screen there is a number "8" which consists for the number of changes made and not saved.

Session Management Toolbar (top of SmartConsole)



	Description
🗑	Discard changes made during the session
Session ...	Enter session details and see the number of changes made in the session
)))	Commit policy changes to the database and make them visible to other administrators **Note** - The changes are saved on the gateways and enforced after the next policy install

Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/117948

QUESTION 7

Which of the following is NOT a type of Endpoint Identity Agent?

A. Terminal

B. Light

C. Full

D. Custom

Correct Answer: A

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk107415

QUESTION 8

Which of these attributes would be critical for a site-to-site VPN?

A. Scalability to accommodate user groups

B. Centralized management

C. Strong authentication

D. Strong data encryption

Correct Answer: D

QUESTION 9

In R80, Unified Policy is a combination of

A. Access control policy, QoS Policy, Desktop Security Policy and endpoint policy.

B. Access control policy, QoS Policy, Desktop Security Policy and Threat Prevention Policy.

C. Firewall policy, address Translation and application and URL filtering, QoS Policy, Desktop Security Policy and Threat Prevention Policy.

D. Access control policy, QoS Policy, Desktop Security Policy and VPN policy.

Correct Answer: D

D is the best answer given the choices.

Unified Policy

In R80 the Access Control policy unifies the policies of these pre-R80 Software Blades:

1.

Firewall and VPN

2.

Application Control and URL Filtering

3.

Identity Awareness

4.

Data Awareness

5.

Mobile Access

6.

Security Zones Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197andanchor=o129934

QUESTION 10

The WebUI offers three methods for downloading Hotfixes via CPUSE. One of them is Automatic method. How many times per day will CPUSE agent check for hotfixes and automatically download them?

A. Six times per day

B. Seven times per day

C. Every two hours

D. Every three hours

Correct Answer: D

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/
html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/112109

QUESTION 11

You work as a security administrator for a large company. CSO of your company has attended a security conference where he has learnt how hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. He wants to make sure that his company has the right protections in place. Check Point has been selected for the security vendor. Which Check Point products protects BEST against malware and zero-day attacks while ensuring quick delivery of safe content to your users?

A. IPS and Application Control

B. IPS, anti-virus and anti-bot

C. IPS, anti-virus and e-mail security

D. SandBlast

Correct Answer: D

SandBlast Zero-Day Protection Hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. Zero-day exploit protection from Check Point provides a deeper level of inspection so you can prevent more malware and zero-day attacks, while ensuring quick delivery of safe content to your users. Reference: https://www.checkpoint.com/products-solutions/zero-day-protection/

QUESTION 12

You want to establish a VPN, using certificates. Your VPN will exchange certificates with an external partner. Which of the following activities sh you do first?

A. Create a new logical-server object to represent your partner\\'s CA

B. Exchange exported CA keys and use them to create a new server object to represent your partner\\'s Certificate Authority (CA)

C. Manually import your partner\\'s Certificate Revocation List.

D. Manually import your partner\\'s Access Control List.

Correct Answer: B

QUESTION 13

You have enabled "Full Log" as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

A. Logging has disk space issues. Change logging storage options on the logging server or Security Management Server properties and install database.

B. Data Awareness is not enabled.

C. Identity Awareness is not enabled.

D. Logs are arriving from Pre-R80 gateways.

Correct Answer: A

The most likely reason for the logs data to stop is the low disk space on the logging device, which can be the Management Server or the Gateway Server.

QUESTION 14

Phase 1 of the two-phase negotiation process conducted by IKE operates in ______ mode.

A. Main

B. Authentication

C. Quick

D. High Alert

Correct Answer: A

Phase I modes

Between Security Gateways, there are two modes for IKE phase I. These modes only apply to IKEv1:

1.

Main Mode

2.

Aggressive Mode

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_VPN_AdminGuide/13847.htm

---

QUESTION 15

Which options are given on features, when editing a Role on Gaia Platform?

A. Read/Write, Read Only

B. Read/Write, Read only, None

C. Read/Write, None

D. Read Only, None

Correct Answer: B

Roles

Role-based administration (RBA) lets you create administrative roles for users. With RBA, an administrator

can allow Gaia users to access specified features by including those features in a role and assigning that

role to users. Each role can include a combination of administrative (read/write) access to some features,

monitoring (read-only) access to other features, and no access to other features.

You can also specify which access mechanisms (WebUI or the CLI) are available to the user.

Note - When users log in to the WebUI, they see only those features that they have read-only or read/write access to. If they have read-only access to a feature, they can see the settings pages, but cannot change the settings.

Gaia includes these predefined roles:

1.

adminRole - Gives the user read/write access to all features.

2.

monitorRole- Gives the user read-only access to all features. You cannot delete or change the predefined roles.

Note - Do not define a new user for external users. An external user is one that is defined on an authentication server (such as RADIUS or TACACS) and not on the local Gaia system.

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/
html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/75930

Latest 156-215.80 Dumps 156-215.80 PDF Dumps 156-215.80 VCE Dumps