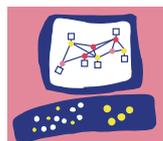




Check Point Certified Security Administrator (CCSA)

Exam 156-215.80 Check Point Security Administrator R80.1 (CCSA)

Multiple Choice Questions



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.





(156-215.80) Check Point Certified Security Administrator (CCSA) R80

Question 1

What are the three authentication methods for SIC?

- A. Passwords, Users, and standards-based SSL for the creation of security channels
- B. Certificates, standards-based SSL for the creation of secure channels, and 3DES or AES128 for encryption
- C. Packet Filtering, certificates, and 3DES or AES128 for encryption
- D. Certificates, Passwords, and Tokens

Correct Answer: B

Explanation:

Secure Internal Communication (SIC) lets Check Point platforms and products authenticate with each other. The SIC procedure creates a trusted status between gateways, management servers and other Check Point components. SIC is required to install polices on gateways and to send logs between gateways and management servers. These security measures make sure of the safety of SIC: Certificates for authentication Standards-based SSL for the creation of the secure channel 3DES for encryption

Reference:

https://sc1.checkpoint.com/documents/R76/CP_R76_SecMan_WebAdmin/html_frameset.htm?topic=documents/R76/CP_R76_SecMan_WebAdmin/71950

Question 2

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

Explanation:

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 3

What is the order of NAT priorities?

- A. Static NAT, IP pool NAT, hide NAT
- B. IP pool NAT, static NAT, hide NAT
- C. Static NAT, automatic NAT, hide NAT
- D. Static NAT, hide NAT, IP pool NAT

Correct Answer: A

Explanation:

The order of NAT priorities are:

1. Static NAT
2. IP Pool NAT
3. Hide NAT

Since Static NAT has all of the advantages of IP Pool NAT and more, it has a higher priority than the other NAT methods.

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmin/6724.htm#o6919

Question 4

Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

- A. UserCheck
- B. Active Directory Query
- C. Account Unit Query
- D. User Directory Query

Correct Answer: B

Explanation:

AD Query extracts user and computer identity information from the Active Directory Security Event Logs. The system generates a Security Event log entry when a user or computer accesses a network resource. For example, this occurs when a user logs in, unlocks a screen, or accesses a network drive.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62402.htm

Question 5

Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server. He can do this via WebUI or a via CLI. Which command should be use in CLI? Choose the correct answer.

- A. Remove database lock
- B. The database feature has one command lock database override.
- C. override database lock
- D. The database feature has two commands: lock database override and unlock database. Both will work.

Correct Answer: D

Explanation:

Use the database feature to obtain the configuration lock. The database feature has two commands:

- `lock database [override]`
- `unlock database`

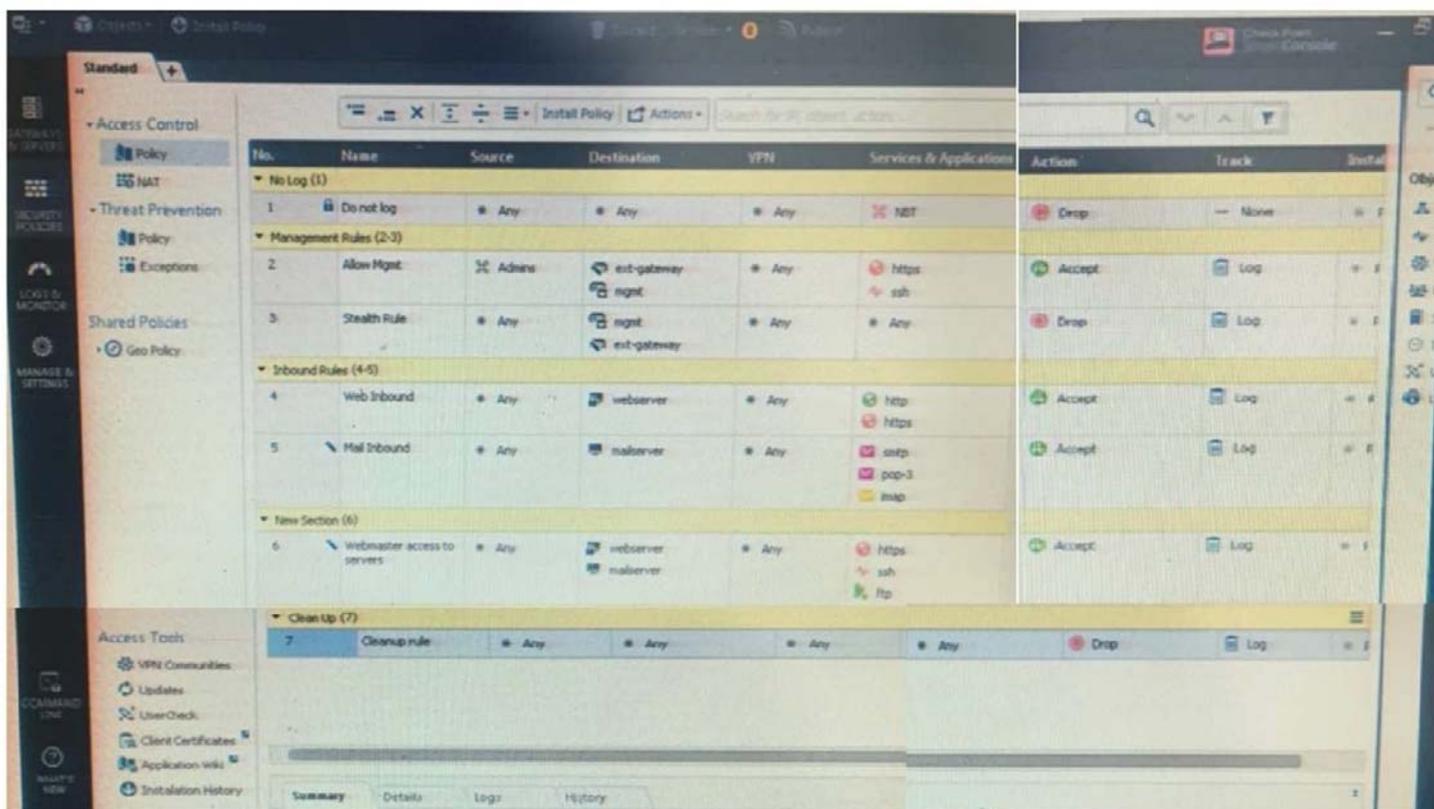
The commands do the same thing: obtain the configuration lock from another administrator.

Description	Use the <code>lock database override</code> and <code>unlock database</code> commands to get exclusive read-write access to the database by taking write privileges to the database away from other administrators logged into the system.
Syntax	<ul style="list-style-type: none"> o <code>lock database override</code> o <code>unlock database</code>

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/75697.htm#o73091

Question 6

Examine the following Rule Base.



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. The 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: B

Explanation:

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)

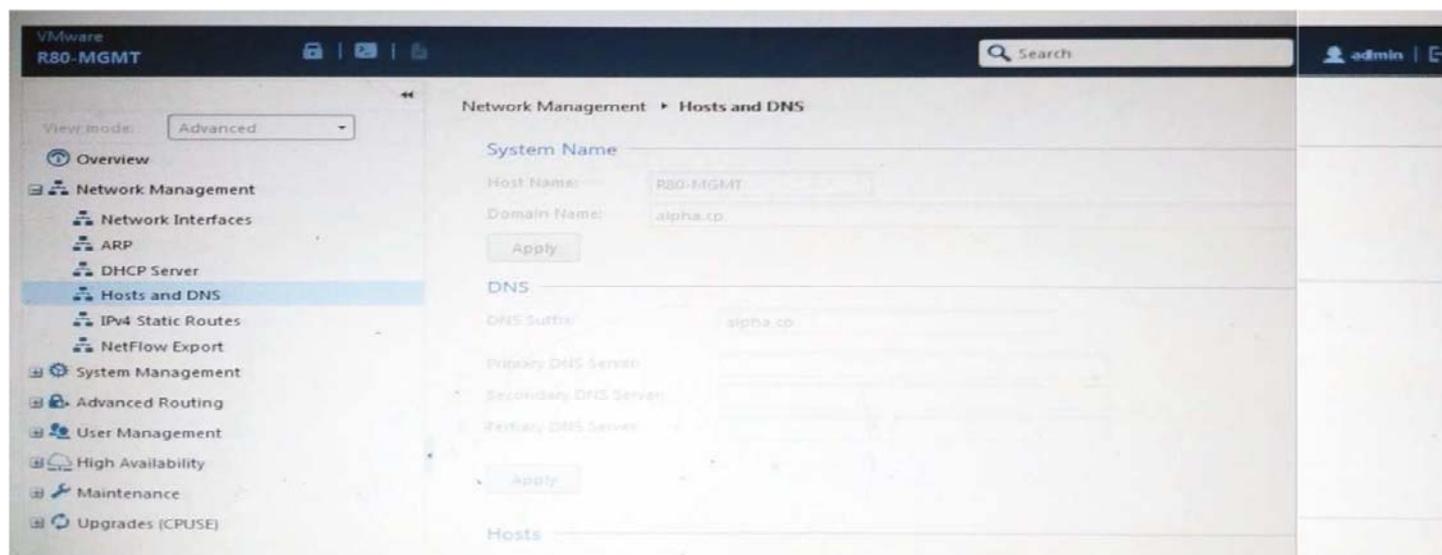
	Description
	Discard changes made during the session
	Enter session details and see the number of changes made in the session
	Commit policy changes to the database and make them visible to other administrators Note - The changes are saved on the gateways and enforced after the next policy install

Reference:

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

Question 7

ALPHA Corp has a new administrator who logs into the Gaia Portal to make some changes. He realizes that even though he has logged in as an administrator, he is unable to make any changes because all configuration options are greyed out as shown in the screenshot image below. What is the likely cause for this?



- A. The Gaia `/bin/confd` is locked by another administrator from a SmartConsole session.
- B. The database is locked by another administrator SSH session.
- C. The Network address of his computer is in the blocked hosts.
- D. The IP address of his computer is not in the allowed hosts.

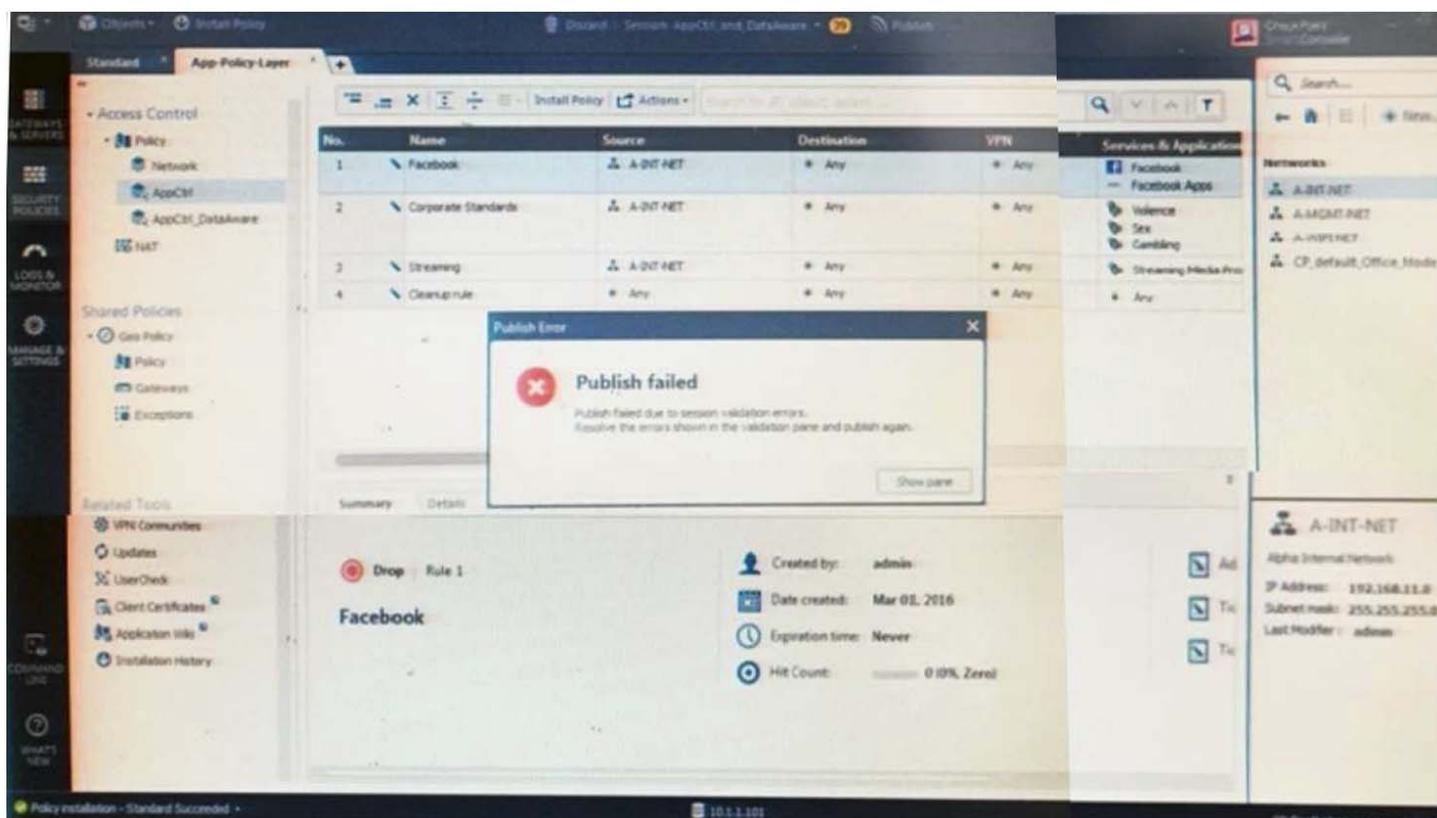
Correct Answer: B

Explanation:

There is a lock on top left side of the screen. B is the logical answer.

Question 8

Administrator Kofi has just made some changes on his Management Server and then clicks on the Publish button in SmartConsole but then gets the error message shown in the screenshot below. Where can the administrator check for more information on these errors?



- A. The Log and Monitor section in SmartConsole
- B. The Validations section in SmartConsole
- C. The Objects section in SmartConsole
- D. The Policies section in SmartConsole

Correct Answer: B

Explanation:

Validation Errors

The validations pane in SmartConsole shows configuration error messages. Examples of errors are object names that are not unique, and the use of objects that are not valid in the Rule Base.

To publish, you must fix the errors.

Reference:

https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197

Question 9

You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?

- A. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules.
- B. Create a separate Security Policy package for each remote Security Gateway.
- C. Create network object that restrict all applicable rules to only certain networks.
- D. Run separate SmartConsole instances to login and configure each Security Gateway directly.

Correct Answer: B

Question 10

Harriet wants to protect sensitive information from intentional loss when users browse to a specific URL: <https://personal.mymail.com>, which blade will she enable to achieve her goal?

- A. DLP
- B. SSL Inspection
- C. Application Control
- D. URL Filtering

Correct Answer: A

Explanation:

Check Point revolutionizes DLP by combining technology and processes to move businesses from passive detection to active Data Loss Prevention. Innovative MultiSpect™ data classification combines user, content and process information to make accurate decisions, while UserCheck™ technology empowers users to remediate incidents in real time. Check Point's self-educating network-based DLP solution frees IT/security personnel from incident handling and educates users on proper data handling policies—protecting sensitive corporate information from both intentional and unintentional loss.

Reference:

<https://www.checkpoint.com/downloads/product-related/datasheets/DLP-software-blade-datasheet.pdf>

Question 11

To optimize Rule Base efficiency the most hit rules should be where?

- A. Removed from the Rule Base.
- B. Towards the middle of the Rule Base.
- C. Towards the top of the Rule Base.
- D. Towards the bottom of the Rule Base.

Correct Answer: C

Explanation:

Explanation: It is logical that if lesser rules are checked for the matched rule to be found the lesser CPU cycles the device is using. Checkpoint match a session from the first rule on top till the last on the bottom.

Question 12

Which of the following is NOT a license activation method?

- A. SmartConsole Wizard
- B. Online Activation
- C. License Activation Wizard
- D. Offline Activation

Correct Answer: A

Question 13

Which policy type has its own Exceptions section?

- A. Thread Prevention
- B. Access Control
- C. Threat Emulation
- D. Desktop Security

Correct Answer: A

Explanation:

The **Exceptions Groups** pane lets you define exception groups. When necessary, you can create exception groups to use in the Rule Base. An exception group contains one or more defined exceptions. This option facilitates ease-of-use so you do not have to manually define exceptions in multiple rules for commonly required exceptions. You can choose to which rules you want to add exception groups. This means they can be added to some rules and not to others, depending on necessity.

Reference:

https://sc1.checkpoint.com/documents/R77/CP_R77_ThreatPrevention_WebAdmin/82209.htm#o97030