



-The original certification question!

<https://www.it-exams.com>

Exam Number:156-215.80

Exam Name:Check Point Certified
Security Administrator (CCSA) R80

Version: Demo

Q1

Which of the following is NOT an integral part of VPN communication within a network?

- A. VPN key
- B. VPN community
- C. VPN trust entities
- D. VPN domain

Answer: A

Explanation:

VPN key (to not be confused with pre-shared key that is used for authentication).

VPN trust entities, such as a Check Point Internal Certificate Authority (ICA). The ICA is part of the Check Point suite used for creating SIC trusted connection between Security Gateways, authenticating administrators and third party servers. The ICA provides certificates for internal Security Gateways and remote access clients which negotiate the VPN link.

VPN Domain - A group of computers and networks connected to a VPN tunnel by one VPN gateway that handles encryption and protects the VPN Domain members.

VPN Community - A named collection of VPN domains, each protected by a VPN gateway.

Reference:

http://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/13868.htm

Q2

Two administrators Dave and Jon both manage R80 Management as administrators for ABC Corp. Jon logged into the R80 Management and then shortly after Dave logged in to the same server. They are both in the Security Policies view. From the screenshots below, why does Dave not have the rule no.6 in his SmartConsole view even though Jon has it in his SmartConsole view?

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Noise	* Any	* Any	* Any	NBT	Drop	- None	* Policy Targets
2	Management	Net_10.28.0.0	GW-R7730	* Any	https ssh	Accept	Log	* Policy Targets
3	Stealth	* Any	GW-R7730	* Any	* Any	Drop	Log	* Policy Targets
4	DNS	Net_10.28.0.0	* Any	* Any	* Any	Accept	- None	* Policy Targets
5	Web	Net_10.28.0.0	* Any	* Any	http https	Accept	Log	* Policy Targets
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	* Any	ftp	Accept	- None	* Policy Targets
7	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	* Policy Targets

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Noise	* Any	* Any	* Any	NBT	Drop	- None	* Policy Targets
2	Management	Net_10.28.0.0	GW-R7730	* Any	https ssh	Accept	Log	* Policy Targets
3	Stealth	* Any	GW-R7730	* Any	* Any	Drop	Log	* Policy Targets
4	DNS	Net_10.28.0.0	* Any	* Any	* Any	Accept	- None	* Policy Targets
5	Web	Net_10.28.0.0	* Any	* Any	http https	Accept	Log	* Policy Targets
6	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	* Policy Targets

- A. Jon is currently editing rule no.6 but has Published part of his changes.
- B. Dave is currently editing rule no.6 and has marked this rule for deletion.
- C. Dave is currently editing rule no.6 and has deleted it from his Rule Base.
- D. Jon is currently editing rule no.6 but has not yet Published his changes.

Answer: D

Explanation:

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/R80.10/WebAdminGuides/EN/CP_R80.10_SecurityManagement_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_SecurityManagement_AdminGuide/162331

Q3

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

Q4

Review the following screenshot and select the BEST answer.



- A. Data Center Layer is an inline layer in the Access Control Policy.
- B. By default all layers are shared with all policies.
- C. If a connection is dropped in Network Layer, it will not be matched against the rules in Data Center Layer.

D. If a connection is accepted in Network-layer, it will not be matched against the rules in Data Center Layer.

Answer: C

Q5

Which of the following is NOT a SecureXL traffic flow?

- A. Medium Path
- B. Accelerated Path
- C. High Priority Path
- D. Slow Path

Answer: C

Explanation:

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

Q6

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: BC

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

Q7

VPN gateways authenticate using _____ and _____ .

- A. Passwords; tokens
- B. Certificates; pre-shared secrets
- C. Certificates; passwords
- D. Tokens; pre-shared secrets

Answer: B

Explanation:

VPN gateways authenticate using Digital Certificates and Pre-shared secrets.

Reference:

https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/85469.htm

Q8

In R80 spoofing is defined as a method of:

- A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.

- B. Hiding your firewall from unauthorized users.
- C. Detecting people using false or wrong authentication logins
- D. Making packets appear as if they come from an authorized IP address.

Answer: D

Explanation:

IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

Reference:

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

Q9

The _____ is used to obtain identification and security information about network users.

- A. User Directory
- B. User server
- C. UserCheck
- D. User index

Answer: A

Reference:

https://www.checkpoint.com/downloads/product-related/datasheets/DS_UserDirectorySWB.pdf

Q10

Which Check Point feature enables application scanning and the detection?

- A. Application Dictionary
- B. AppWiki
- C. Application Library
- D. CPApp

Answer: B

Explanation:

AppWiki Application Classification Library

AppWiki enables application scanning and detection of more than 5,000 distinct applications and over 300,000 Web 2.0 widgets including instant messaging, social networking, video streaming, VoIP, games and more.

Reference: <https://www.checkpoint.com/products/application-control-software-blade/>

Q11

DLP and Geo Policy are examples of what type of Policy?

- A. Standard Policies
- B. Shared Policies
- C. Inspection Policies
- D. Unified Policies

Answer: B

Explanation:

The Shared policies are installed with the Access Control Policy.

Software Blade	Description
Mobile Access	Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile.
DLP	Launch Data Loss Prevention policy in a SmartConsole. Configure advanced tools to automatically identify data that must not go outside the network, to block the leak, and to educate users.
Geo Policy	Create a policy for traffic to or from specific geographical or political locations.
HTTPS Policy	The HTTPS Policy allows the Security Gateway to inspect HTTPS traffic to prevent security risks related to the SSL protocol. To launch the HTTPS Policy, click Manage & Settings > Blades > HTTPS Inspection > Configure in SmartDashboard

Reference:

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

Q12

In which deployment is the security management server and Security Gateway installed on the same appliance?

- A. Bridge Mode
- B. Remote
- C. Standalone
- D. Distributed

Answer: C

Explanation:

Installing Standalone

Standalone Deployment - The Security Management Server and the Security Gateway are installed on the same computer or appliance.

Installing Standalone

Standalone Deployment - The Security Management Server and the Security Gateway are installed on the same computer or appliance.



Item	Description
1	Standalone computer
	Security Gateway component
	Security Management Server component

Reference:

https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/89230.htm#o98246

Q13

A _____ VPN deployment is used to provide remote users with secure access to internal corporate resources by authenticating the user through an internet browser.

- A. Clientless remote access
- B. Clientless direct access
- C. Client-based remote access
- D. Direct access

Answer: A

Explanation:

Clientless - Users connect through a web browser and use HTTPS connections. Clientless solutions usually supply access to web-based corporate resources.

Reference:

https://sc1.checkpoint.com/documents/R80/CP_R80BC_Firewall/html_frameset.htm?topic=documents/R80/CP_R80BC_Firewall/92704

Q14

Which of the following statements is TRUE about R80 management plug-ins?

- A. The plug-in is a package installed on the Security Gateway.
- B. Installing a management plug-in requires a Snapshot, just like any upgrade process.

- C. A management plug-in interacts with a Security Management Server to provide new features and support for new products.
- D. Using a plug-in offers full central management only if special licensing is applied to specific features of the plug-in.

Answer: C

Q15

Gaia can be configured using the _____ or _____ .

- A. GaiaUI; command line interface
- B. WebUI; Gaia Interface
- C. Command line interface; WebUI
- D. Gaia Interface; GaiaUI

Answer: C

Explanation:

Configuring Gaia for the First Time

In This Section:

Running the First Time Configuration Wizard in WebUI

Running the First Time Configuration Wizard in CLI

After you install Gaia for the first time, use the First Time Configuration Wizard to configure the system and the Check Point products on it.

Reference:

https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/112568

Q16

Where can you trigger a failover of the cluster members?

1. Log in to Security Gateway CLI and run command clusterXL_admin down.
2. In SmartView Monitor right-click the Security Gateway member and select Cluster member stop.
3. Log into Security Gateway CLI and run command cphaprob down.

- A. 1, 2, and 3
- B. 2 and 3

C. 1 and 2

D. 1 and 3

Answer: C

Explanation:

How to Initiate Failover

Method	To Stop ClusterXL	To Start ClusterXL
<p>Run:</p> <ul style="list-style-type: none">o <code>cphaprob -d faildevice -t 0 -s ok register</code>o <code>cphaprob -d faildevice -s problem report</code> <p>and:</p> <ul style="list-style-type: none">o <code>cphaprob -d faildevice -s ok report</code>o <code>cphaprob -d faildevice unregister</code>	<p>Effect:</p> <ul style="list-style-type: none">o Disables ClusterXLo Does not disable synchronization	<p>Effect:</p> <ul style="list-style-type: none">o Enables ClusterXLo Does not initiate full synchronization
<p>Recommended method:</p> <p>Run:</p> <ul style="list-style-type: none">o <code>clusterXL_admin down</code>o <code>clusterXL_admin up</code>	<ul style="list-style-type: none">o Disables ClusterXLo Does not disable synchronization	<ul style="list-style-type: none">o Enables ClusterXLo Does not initiate full synchronization
<p>In SmartView Monitor:</p> <ol style="list-style-type: none">1. Click the Cluster object.2. Select one of the member gateway branches.3. Right click the cluster member.4. Select Down.	<ul style="list-style-type: none">o Disables ClusterXLo Disables synchronization	<ul style="list-style-type: none">o Enables ClusterXLo Does not initiate full synchronization

Reference:

https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7298.htm

Q17

Which utility allows you to configure the DHCP service on GAIA from the command line?

- A. ifconfig
- B. dhcp_cfg
- C. sysconfig
- D. cpconfig

Answer: C

Explanation:

Sysconfig Configuration Options

	Menu Item	Purpose
7	DHCP Server Configuration	Configure SecurePlatform DHCP Server.
8	DHCP Relay Configuration	Setup DHCP Relay.

Reference:

https://sc1.checkpoint.com/documents/R76/CP_R76_Splat_AdminGuide/51548.htm

NOTE: Question must be wrong because no answer is possible for GAIA system, this must be SPLAT version.

DHCP CLI configuration for GAIA reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/73181.htm#o80096

Q18

Which VPN routing option uses VPN routing for every connection a satellite gateway handles?

- A. To satellites through center only
- B. To center only
- C. To center and to other satellites through center
- D. To center, or through the center to other satellites, to internet and other VPN targets

Answer: D

Explanation:

On the VPN Routing page, enable the VPN routing for satellites section, by selecting one of these options:

To center and to other Satellites through center; this allows connectivity between Gateways; for

example, if the spoke Gateways are DAIP Gateways, and the hub is a Gateway with a static IP address To center, or through the center to other satellites, to Internet and other VPN targets; this allows connectivity between the Gateways, as well as the ability to inspect all communication passing through the hub to the Internet.

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk31021

Q19

Which product correlates logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

- A. SmartView Monitor
- B. SmartEvent
- C. SmartUpdate
- D. SmartDashboard

Answer: B

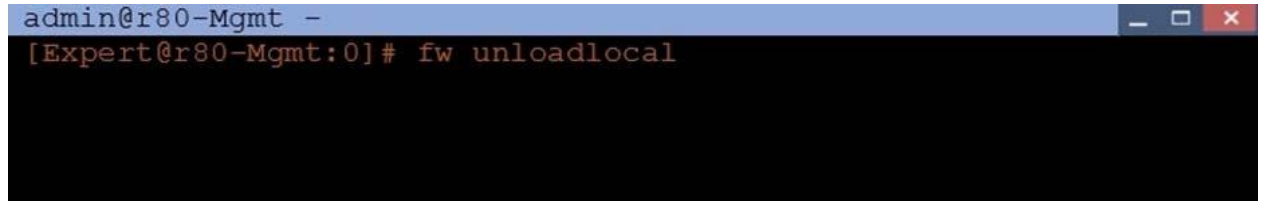
Explanation:

SmartEvent correlates logs from all Check Point enforcement points, including end-points, to identify suspicious activity from the clutter. Rapid data analysis and custom event logs immediately alert administrators to anomalous behavior such as someone attempting to use the same credential in multiple geographies simultaneously.

Reference: <https://www.checkpoint.com/products/smartevent/>

Q20

Assuming you have a Distributed Deployment, what will be the effect of running the following command on the Security Management Server?



```
admin@r80-Mgmt -  
[Expert@r80-Mgmt:0]# fw unloadlocal
```

- A. Remove the installed Security Policy.
- B. Remove the local ACL lists.
- C. No effect.
- D. Reset SIC on all gateways.

Answer: A

Explanation:

This command uninstalls actual security policy (already installed) Reference:

https://sc1.checkpoint.com/documents/R77/CP_R77_SecurityGatewayTech_WebAdmin/6751.htm

Q21

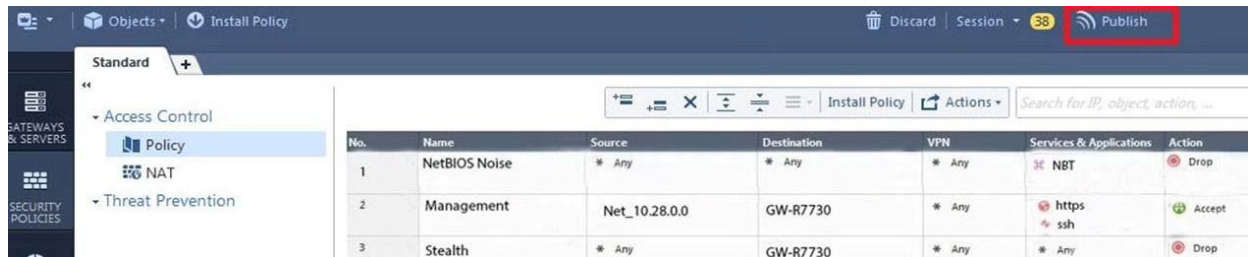
An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server. While configuring the VPN community to specify the pre-shared secret, the administrator found that the check box to enable pre-shared secret is shared and cannot be enabled. Why does it not allow him to specify the pre-shared secret?

- A. IPsec VPN blade should be enabled on both Security Gateway.
- B. Pre-shared can only be used while creating a VPN between a third party vendor and Check Point Security Gateway.
- C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS.
- D. The Security Gateways are pre-R75.40.

Answer: C

Q22

You are the senior Firewall administrator for ABC Corp., and have recently returned from a training course on Check Point's new advanced R80 management platform. You are presenting an in-house overview of the new features of Check Point R80 Management to the other administrators in ABC Corp.



How will you describe the new "Publish" button in R80 Management Console?

- A. The Publish button takes any changes an administrator has made in their management session, publishes a copy to the Check Point of R80, and then saves it to the R80 database.
- B. The Publish button takes any changes an administrator has made in their management session and publishes a copy to the Check Point Cloud of R80 and but does not save it to the R80
- C. The Publish button makes any changes an administrator has made in their management session visible to all other administrator sessions and saves it to the Database.
- D. The Publish button makes any changes an administrator has made in their management session visible to the new Unified Policy session and saves it to the Database.

Answer: C

Explanation:

To make your changes available to other administrators, and to save the database before installing a policy, you must publish the session. When you publish a session, a new database version is created.

Reference:

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

Q23

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

Q24

With the User Directory Software Blade, you can create R80 user definitions on a(an) _____ Server.

- A. NT domain
- B. SMTP
- C. LDAP
- D. SecurID

Answer: C

Reference:

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

Q25

Which of the following is NOT a component of a Distinguished Name?

- A. Organizational Unit

- B. Country
- C. Common Name
- D. User container

Answer: D

Explanation:

Distinguished Name Components

CN=common name, OU=organizational unit, O=organization, L=locality, ST=state or province, C=country name

Reference:

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

Q26

What are the three authentication methods for SIC?

- A. Passwords, Users, and standards-based SSL for the creation of secure 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

Answer: B

Explanation:

Secure Internal Communication (SIC)

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 policies 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

Q27

You have enabled "Extended 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. Content Awareness is not enabled.
- C. Identity Awareness is not enabled.
- D. Log Trimming is enabled.

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.

Q28

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

Answer: A

Explanation:

The order of NAT priorities is:

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

Q29

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

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

Q30

Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server Operating System. He can do this via WebUI or via CLI. Which command should he use in CLI?

- 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.

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.

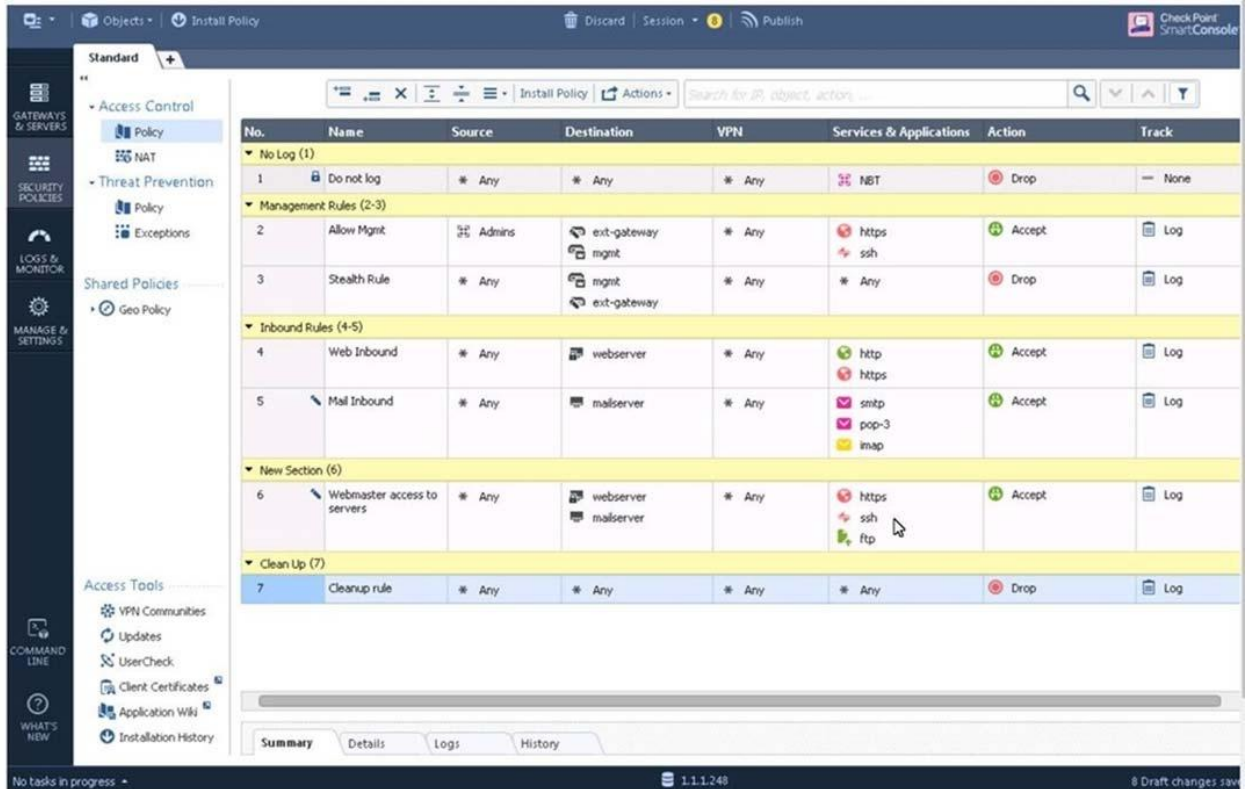
Description	Use the <code>lock database override</code> and <code>unlock database</code> commands to get exclusive read-write access to the database by taking write privileges to the database away from other administrators logged into the system.
Syntax	<ul style="list-style-type: none">o <code>lock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

Reference:

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

Q31

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

Answer: D

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)

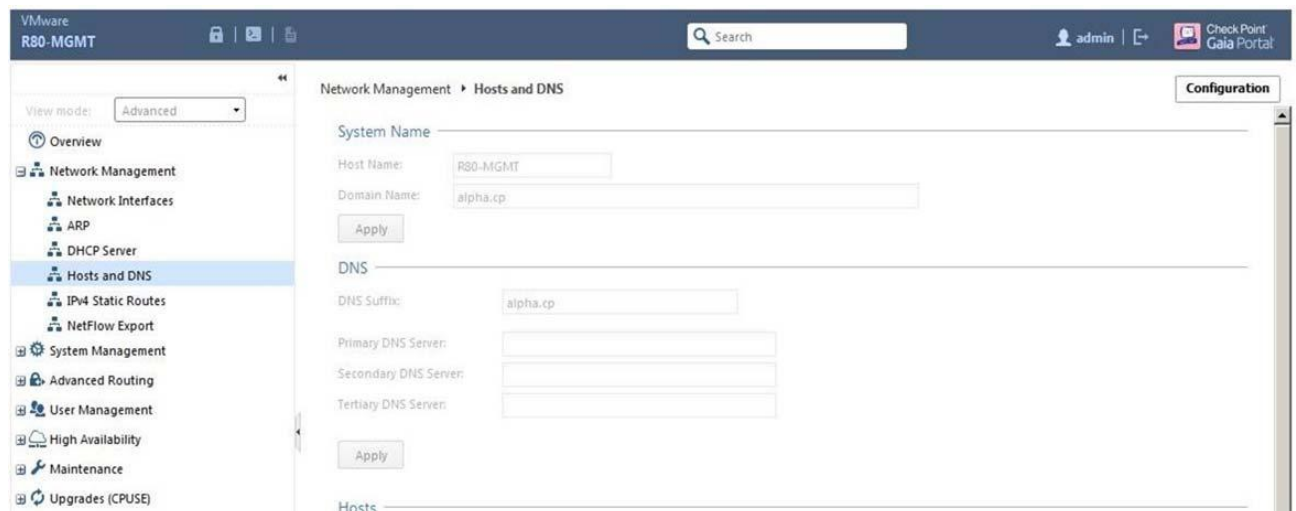
	Description
	Discard changes made during the session
	Enter session details and see the number of changes made in the session
	Commit policy changes to the database and make them visible to other administrators Note - The changes are saved on the gateways and enforced after the next policy install

Reference:

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

Q32

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.

Answer: B

Explanation:

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