Question: 1

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

Question: 2

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 his 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.

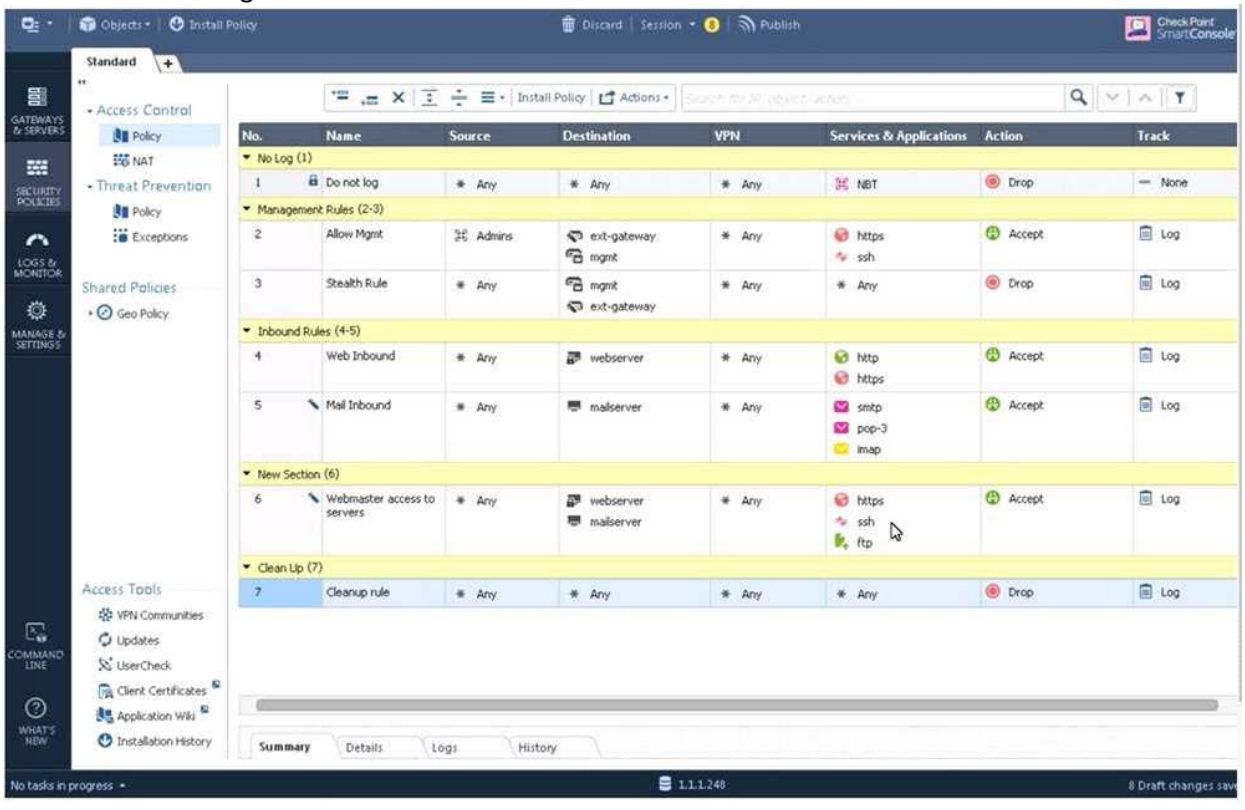
Answer: D

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.

Question: 3

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

Question: 4

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

Question: 5

Which of the following is NOT a SecureXL traffic flow?

A. Medium Path
B. Accelerated Path
C. Fast 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.

Question: 6

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:

Question: 7

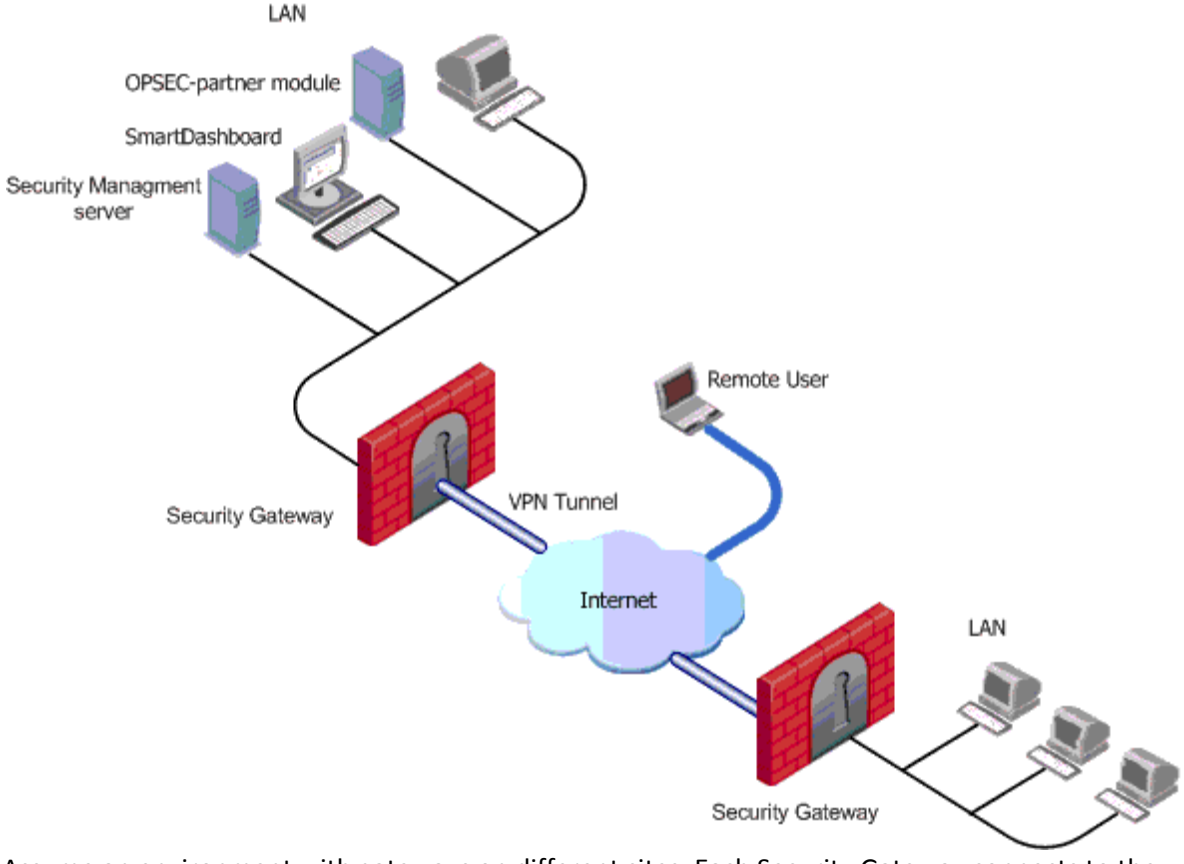
What are the three essential components of the Check Point Security Management Architecture?

A. SmartConsole, Security Management Server, Security Gateway

B. SmartConsole, SmartUpdate, Security Gateway
C. Security Management Server, Security Gateway, Command Line Interface
D. WebUI, SmartConsole, Security Gateway

Answer: A

Explanation:
Deployments
Basic deployments:



Assume an environment with gateways on different sites. Each Security Gateway connects to the Internet on one side, and to a LAN on the other.
You can create a Virtual Private Network (VPN) between the two Security Gateways, to secure all communication between them.
The Security Management server is installed in the LAN, and is protected by a Security Gateway. The Security Management server manages the Security Gateways and lets remote users connect securely to the corporate network. SmartDashboard can be installed on the Security Management server or another computer.
There can be other OPSEC-partner modules (for example, an Anti-Virus Server) to complete the network security with the Security Management server and its Security Gateways.

Question: 8

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.

Question: 9

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

Question: 10

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.