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

Correct Answer: A

Explanation/Reference:
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.

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

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 & Apps
1	NetBIOS Noise	* Any	* Any	* Any	NBT
2	Management	Net_10.28.0.0	GW-R7730	* Any	https ssh
3	Stealth	* Any	GW-R7730	* Any	* Any
4	DNS	Net_10.28.0.0	* Any	* Any	* Any
5	Web	Net_10.28.0.0	* Any	* Any	http https
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	* Any	ftp
7	Cleanup rule	* Any	* Any	* Any	* Any

No.	Name	Source	Destination	VPN	Services & Apps
1	NetBIOS Noise	* Any	* Any	* Any	NBT
2	Management	Net_10.28.0.0	GW-R7730	* Any	https ssh
3	Stealth	* Any	GW-R7730	* Any	* Any
4	DNS	Net_10.28.0.0	* Any	* Any	* Any
5	Web	Net_10.28.0.0	* Any	* Any	http https
6	Cleanup rule	* Any	* Any	* Any	* Any

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.

Correct Answer: D

Explanation/Reference:
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.

http://dl3.checkpoint.com/paid/74/74d596decb6071a4ee642fbdaae7238f/CP_R80_SecurityManagement_AdminGuide.pdf?

QUESTION 3
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.

Correct Answer: A

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

http://dl3.checkpoint.com/paid/74/74d596decb6071a4ee642fbdaae7238f/CP_R80_SecurityManagement_AdminGuide.pdf?

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.

Correct Answer: C

Explanation/Reference:

QUESTION 5
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

Explanation/Reference:
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.

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

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

Correct Answer: BC

Explanation/Reference:
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

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

QUESTION 7
Fill in the blanks: VPN gateways authenticate using_____and_____.

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

Correct Answer: B

Explanation/Reference:
VPN gateways authenticate using Digital Certificates and Pre-shared secrets.

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

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.

Correct Answer: D

Explanation/Reference:
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.

http://dl3.checkpoint.com/paid/74/74d596decb6071a4ee642fbdaae7238f/CP_R80_SecurityManagement_AdminGuide.pdf?

QUESTION 9
Fill in the blank: The_____is used to obtain identification and security information about network users.

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

Correct Answer: A

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

QUESTION 10
Which Check Point feature enables application scanning and the detection?

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

Correct Answer: B

Explanation/Reference:
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.

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

QUESTION 11
DLP and Geo Policy are examples of what type of Policy?

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

Correct Answer: B

Explanation/Reference:
The Shared policies are installed with the Access Control Policy.