Number: 156-215.81
Passing Score: 800
Time Limit: 120
File Version: 14.0

Exam Code: 156-215.81
Exam Name: Check Point Certified Security Administrator R81

Exam A

QUESTION 1
Which of the following methods can be used to update the trusted log server regarding the policy and configuration changes performed on the Security Management Server?

A. Save Policy
B. Install Database
C. Save session
D. Install Policy

Correct Answer: A
Section:
Explanation:
The method to update the trusted log server regarding the policy and configuration changes performed on the Security Management Server is Save Policy.Saving a policy updates the trusted log server with the latest policy and configuration changes3.
Reference:Check Point R81 Logging and Monitoring Administration Guide

QUESTION 2
From the Gaia web interface, which of the following operations CANNOT be performed on a Security Management Server?

A. Verify a Security Policy
B. Open a terminal shell
C. Add a static route
D. View Security Management GUI Clients

Correct Answer: A
Section:
Explanation:
From the Gaia web interface, the operation that CANNOT be performed on a Security Management Server is Verify a Security Policy.This operation can only be done from SmartConsole4.
Reference:Check Point R81 SmartConsole Online Help

QUESTION 3
Which of the following are types of VPN communities?

A. Pentagon, star, and combination
B. Star, octagon, and combination
C. Combined and star
D. Meshed, star, and combination

Correct Answer: D
Section:
Explanation:
The types of VPN communities are Meshed, Star, and Combination. A Meshed community is a group of Security Gateways that have VPN connections between every pair of members. A Star community has one Security Gateway as the center and other Security Gateways or hosts as satellites. A Combination community is a group of Meshed and Star communities.
Reference: [Check Point R81 Site-to-Site VPN Administration Guide]

QUESTION 4
Which deployment adds a Security Gateway to an existing environment without changing IP routing?

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

Correct Answer: B
Section:
Explanation:
The answer is B because bridge mode deployment adds a Security Gateway to an existing environment without changing IP routing. Bridge mode is a transparent mode that does not require assigning IP addresses to the Security Gateway interfaces. Distributed deployment is a deployment where the Security Management Server and the Security Gateway are installed on separate machines. Remote deployment is a deployment where the Security Gateway is installed on a remote site and connects to the Security Management Server over a VPN tunnel. Standalone deployment is a deployment where the Security Management Server and the Security Gateway are installed on the same machine.
Reference: [Check Point R81 Bridge Mode], [Check Point R81 Deployment Scenarios]

QUESTION 5
To increase security, the administrator has modified the Core protection 'Host Port Scan' from 'Medium' to 'High' Predefined Sensitivity. Which Policy should the administrator install after Publishing the changes?

A. The Access Control and Threat Prevention Policies.
B. The Access Control Policy.
C. The Access Control & HTTPS Inspection Policy.
D. The Threat Prevention Policy.

Correct Answer: D
Section:
Explanation:
To increase security, the administrator has modified the Core protection 'Host Port Scan' from 'Medium' to 'High' Predefined Sensitivity.The administrator should install theThreat Prevention Policyafter Publishing the changes3.The Threat Prevention Policy defines how the Security Gateway inspects and protects against threats such as port scans, bot attacks, and zero-day exploits4.
Reference:Check Point R81 Firewall Administration Guide,Check Point R81 Threat Prevention Administration Guide

QUESTION 6
When changes are made to a Rule base, it is important to _____ to enforce changes.

A. Publish database
B. Activate policy
C. Install policy
D. Save changes

Correct Answer: A
Section:
Explanation:
When changes are made to a Rule base, it is important toPublish databaseto enforce changes5. Publishing database saves the changes to the database and makes them available to other administrators. Installing policy applies the changes to the Security Gateways.
Reference:Check Point R81 Security Management Administration Guide, [Check Point R81 SmartConsole R81 Resolved Issues], [Check Point R81 Firewall Administration Guide]

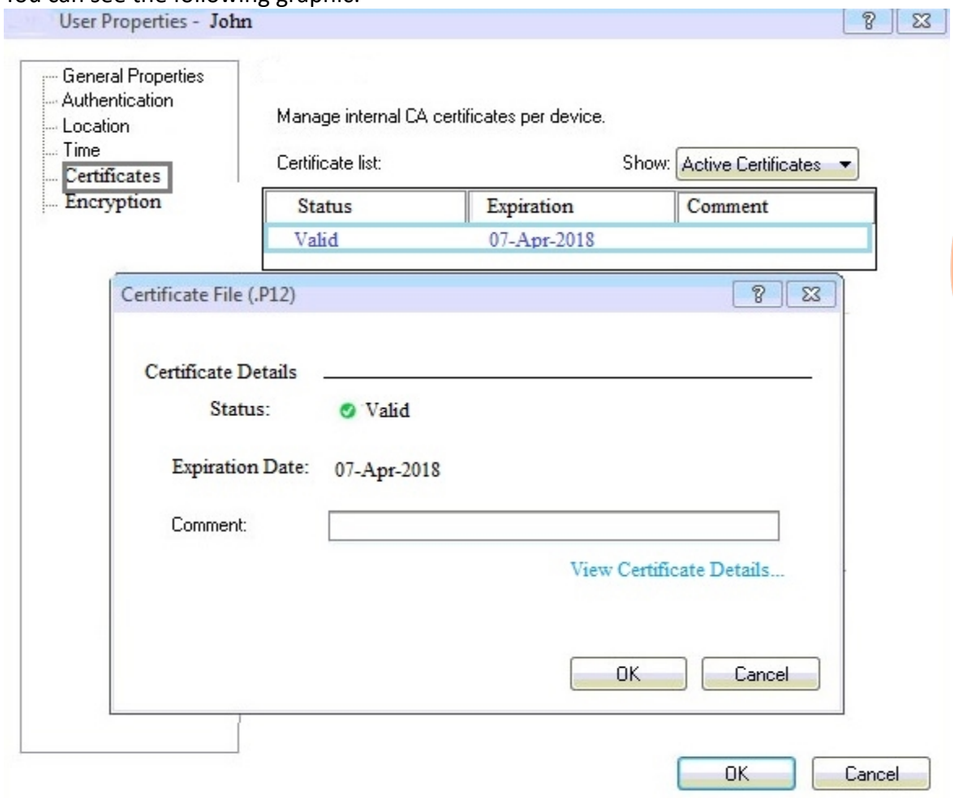
QUESTION 7

Fill in the blank: An identity server uses a _____ for user authentication.

A. Shared secret
B. Certificate
C. One-time password
D. Token

Correct Answer: A
Section:
Explanation:
The answer is A because an identity server uses a shared secret for user authentication. A shared secret is a passphrase that is known by both the identity server and the user. The identity server sends a challenge to the user, who encrypts it with the shared secret and sends it back.The identity server then verifies the response and authenticates the user12Reference:Check Point R81 Identity Awareness Administration Guide,Check Point R81 Identity Server

QUESTION 8
You can see the following graphic:



What is presented on it?

A. Properties of personal. p12 certificate file issued for user John.
B. Shared secret properties of John's password.
C. VPN certificate properties of the John's gateway.
D. Expired. p12 certificate properties for user John.

Correct Answer: A

Section:
Explanation:
The answer is A because the graphic shows the properties of a personal .p12 certificate file issued for user John. A .p12 file is a file format that contains a user's private key and public key certificate. The graphic shows that the certificate file is valid and has an expiration date of 07-Apr-2018. The graphic also shows that the certificate file is issued by an internal CA, which is a Check Point component that manages certificates for users and gateways.
Reference: Check Point R81 Certificate Management, Check Point R81 Internal CA

QUESTION 9
When configuring LDAP User Directory integration, Changes applied to a User Directory template are:

A. Reflected immediately for all users who are using template.
B. Not reflected for any users unless the local user template is changed.
C. Reflected for all users who are using that template and if the local user template is changed as well.
D. Not reflected for any users who are using that template.

Correct Answer: A
Section:
Explanation:
The answer is A because changes applied to a User Directory template are reflected immediately for all users who are using that template. A User Directory template defines the settings for connecting to an LDAP server, such as the server name, port, base DN, user filter, and group filter.When a User Directory template is modified, all users who are using that template will inherit the changes without requiring any additional actions3Reference:Check Point R81 Identity Awareness Administration Guide, [Check Point R81 User Directory Templates]

QUESTION 10
Choose what BEST describes the reason why querying logs now is very fast.

A. New Smart-1 appliances double the physical memory install
B. Indexing Engine indexes logs for faster search results
C. SmartConsole now queries results directly from the Security Gateway
D. The amount of logs been store is less than the usual in older versions

Correct Answer: B
Section:
Explanation:
The answer is B because querying logs now is very fast because the Indexing Engine indexes logs for faster search results. The Indexing Engine is a component of the Smart-1 appliance that creates indexes for log fields and values, such as source, destination, action, and time. The indexes enable quick and efficient searches of large amounts of log data.
Reference: [Check Point R81 Logging and Monitoring Administration Guide], [Check Point R81 Indexing Engine]

QUESTION 11
Check Point ClusterXL Active/Active deployment is used when:

A. Only when there is Multicast solution set up
B. There is Load Sharing solution set up
C. Only when there is Unicast solution set up
D. There is High Availability solution set up

Correct Answer: B
Section:
Explanation:
Check Point ClusterXL Active/Active deployment is used when there is Load Sharing solution set up.Load Sharing enables multiple Security Gateways to share traffic and provide high availability12.

Reference:Check Point R81,Check Point R81 ClusterXL Administration Guide

QUESTION 12
What are the advantages of a ''shared policy'' in R80?

A. Allows the administrator to share a policy between all the users identified by the Security Gateway
B. Allows the administrator to share a policy between all the administrators managing the Security Management Server
C. Allows the administrator to share a policy so that it is available to use in another Policy Package
D. Allows the administrator to install a policy on one Security Gateway and it gets installed on another managed Security Gateway

Correct Answer: C
Section:
Explanation:
A shared policy is a set of rules that can be used in multiple policy packages. It allows the administrator to create a common security policy for different gateways or domains, and avoid duplication and inconsistency. The other options are not advantages of a shared policy.
Reference: [Shared Policies Overview], [Shared Policies Best Practices]

QUESTION 13
What are the three types of UserCheck messages?

A. inform, ask, and block
B. block, action, and warn
C. action, inform, and ask
D. ask, block, and notify

Correct Answer: A
Section:
Explanation:
The three types of UserCheck messages are inform, ask, and block. Inform messages notify users about security events and do not require any user action. Ask messages prompt users to choose whether to allow or block an action.Block messages prevent users from performing an action and display a reason1.
Reference:Check Point R81 Logging and Monitoring Administration Guide

QUESTION 14
What two ordered layers make up the Access Control Policy Layer?

A. URL Filtering and Network
B. Network and Threat Prevention
C. Application Control and URL Filtering
D. Network and Application Control

Correct Answer: B
Section:
Explanation:
The two ordered layers that make up the Access Control Policy Layer are Network and Threat Prevention. Network layer contains rules that define how traffic is inspected and handled by the Security Gateway.Threat Prevention layer contains rules that define how traffic is inspected by the Threat Prevention Software Blades2.
Reference:Check Point R81 Security Management Administration Guide

QUESTION 15

Which statement is TRUE of anti-spoofing?

A. Anti-spoofing is not needed when IPS software blade is enabled
B. It is more secure to create anti-spoofing groups manually
C. It is BEST Practice to have anti-spoofing groups in sync with the routing table
D. With dynamic routing enabled, anti-spoofing groups are updated automatically whenever there is a routing change

Correct Answer: C
Section:
Explanation:
The statement that is TRUE of anti-spoofing is that it is BEST Practice to have anti-spoofing groups in sync with the routing table. Anti-spoofing prevents attackers from sending packets with a false source IP address. Anti-spoofing groups define which IP addresses are expected on each interface of the Security Gateway.If the routing table changes, the anti-spoofing groups should be updated accordingly34.
Reference:Check Point R81 ClusterXL Administration Guide,Network Defined by Routes: Anti-Spoofing

QUESTION 16
After the initial installation on Check Point appliance, you notice that the Management interface and default gateway are incorrect. Which commands could you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1.

A. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24set static-route default nexthop gateway address 192.168.80.1 onsave config
B. add interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 onsave config
C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 onsave config
D. add interface Mgmt ipv4-address 192.168.80.200 mask-length 24add static-route default nexthop gateway address 192.168.80.1 onsave config

Correct Answer: A
Section:
Explanation:
The commands you could use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1 after the initial installation on Check Point appliance are:
set interface Mgmt ipv4-address 192.168.80.200 mask-length 24. This command sets the IPv4 address and subnet mask of the Management interface.
set static-route default nexthop gateway address 192.168.80.1 on. This command sets the default gateway for IPv4 routing.
save config. This command saves the configuration changes.

QUESTION 17
What Check Point tool is used to automatically update Check Point products for the Gaia OS?

A. Check Point INSPECT Engine
B. Check Point Upgrade Service Engine
C. Check Point Update Engine
D. Check Point Upgrade Installation Service

Correct Answer: B
Section:
Explanation:
The Check Point Upgrade Service Engine (CPUSE) is a tool that automates the process of upgrading and installing Check Point products on Gaia OS1.It can also be used to update the Gaia OS itself2. The other options are not valid tools for this purpose.
Reference:Check Point Upgrade Service Engine (CPUSE) - Gaia Deployment Agent,Check Point R81 Gaia Installation and Upgrade Guide

QUESTION 18
You are the Check Point administrator for Alpha Corp with an R80 Check Point estate. You have received a call by one of the management users stating that they are unable to browse the Internet with their new tablet

connected to the company Wireless. The Wireless system goes through the Check Point Gateway. How do you review the logs to see what the problem may be?

A. Open SmartLog and connect remotely to the IP of the wireless controller
B. Open SmartView Tracker and filter the logs for the IP address of the tablet
C. Open SmartView Tracker and check all the IP logs for the tablet
D. Open SmartLog and query for the IP address of the Manager's tablet

Correct Answer: D
Section:
Explanation:
SmartLog is a unified log viewer that provides fast and easy access to logs from all Check Point components3.It allows the administrator to query for any log field, such as the IP address of the tablet, and filter the results by time, severity, blade, action, and more4. SmartView Tracker is a legacy tool that displays network activity logs from Security Gateways and other Check Point devices. It does not support remote connection to the wireless controller or querying for specific IP addresses.
Reference:SmartLog,SmartLog Queries, [SmartView Tracker]

QUESTION 19
When should you generate new licenses?

A. Before installing contract files.
B. After an RMA procedure when the MAC address or serial number of the appliance changes.
C. When the existing license expires, license is upgraded or the IP-address where the license is tied changes.
D. Only when the license is upgraded.

Correct Answer: C
Section:
Explanation:
You should generate new licenses when the existing license expires, license is upgraded or the IP-address where the license is tied changes13.These scenarios require a new license to be generated and activated on the Security Gateway or Management Server13. Therefore, the correct answer is C.When the existing license expires, license is upgraded or the IP-address where the license is tied changes

QUESTION 20
Fill in the blank: When a policy package is installed, _____ are also distributed to the target installation Security Gateways.

A. User and objects databases
B. Network databases
C. SmartConsole databases
D. User databases

Correct Answer: A
Section:
Explanation:
When a policy package is installed, user and objects databases are also distributed to the target installation Security Gateways14.The user and objects databases contain information about network objects, users, groups, services, VPN domains, and more14. Therefore, the correct answer is A.User and objects databases.

QUESTION 21
Which of the following is NOT a method used by Identity Awareness for acquiring identity?

A. Remote Access

B. Cloud IdP (Identity Provider)
C. Active Directory Query
D. RADIUS

Correct Answer: B
Section:
Explanation:
Identity Awareness uses several methods for acquiring identity, such as Active Directory Query, Identity Agent, Browser-Based Authentication, Terminal Servers, Captive Portal, and RADIUS12.Cloud IdP (Identity Provider) is not a method used by Identity Awareness12. Therefore, the correct answer is B.Cloud IdP (Identity Provider).

QUESTION 22
Which Check Point software blade provides Application Security and identity control?

A. Identity Awareness
B. Data Loss Prevention
C. URL Filtering
D. Application Control

Correct Answer: D
Section:
Explanation:
The Check Point software blade that provides Application Security and identity control is Application Control3.Application Control enables network administrators to identify, allow, block, or limit usage of thousands of applications and millions of websites3. Therefore, the correct answer is D.Application Control

QUESTION 23
How are the backups stored in Check Point appliances?

A. Saved as*.tar under /var/log/CPbackup/backups
B. Saved as*tgz under /var/CPbackup
C. Saved as*tar under /var/CPbackup
D. Saved as*tgz under /var/log/CPbackup/backups

Correct Answer: B
Section:
Explanation:
The backups are stored in Check Point appliances as *.tgz files under /var/CPbackup. This is the default location for backup files created by the backup command. Therefore, the correct answer is B. Saved as *.tgz under /var/CPbackup

QUESTION 24
You are going to perform a major upgrade. Which back up solution should you use to ensure your database can be restored on that device?

A. backup
B. logswitch
C. Database Revision
D. snapshot

Correct Answer: D

Section:
Explanation:
The back up solution that should be used to ensure your database can be restored on that device is snapshot . A snapshot creates a binary image of the entire root (lv_current) disk partition. This includes Check Point products, configuration, and operating system. A snapshot can be used to restore a Security Gateway or Security Management Server to its previous state at any time . Therefore, the correct answer is D. snapshot.

QUESTION 25
Fill in the blank: The position of an implied rule is manipulated in the _____ window.

A. NAT
B. Firewall
C. Global Properties
D. Object Explorer

Correct Answer: C
Section:
Explanation:
The position of an implied rule is manipulated in the Global Properties window. Implied rules are predefined rules that are not displayed in the rule base. They allow or block traffic for essential services such as communication with Check Point servers, logging, and VPN traffic.The position of an implied rule can be changed in the Global Properties > Firewall > Implied Rules section56.
Reference:How to view Implied Rules in R80.x / R81.x SmartConsole,Implied Rules

QUESTION 26
How can the changes made by an administrator before publishing the session be seen by a superuser administrator?

A. By impersonating the administrator with the 'Login as...' option
B. They cannot be seen
C. From the SmartView Tracker audit log
D. From Manage and Settings > Sessions, right click on the session and click 'View Changes...'

Correct Answer: D
Section:
Explanation:
The changes made by an administrator before publishing the session can be seen by a superuser administrator from Manage and Settings > Sessions, right click on the session and click 'View Changes...'.This option allows the superuser to review the changes made by another administrator in a pending session1.
Reference:Check Point R81 Security Management Administration Guide

QUESTION 27
Which Check Point software blade monitors Check Point devices and provides a picture of network and security performance?

A. Application Control
B. Threat Emulation
C. Logging and Status
D. Monitoring

Correct Answer: D
Section:
Explanation:
The Check Point software blade that monitors Check Point devices and provides a picture of network and security performance is Monitoring. The Monitoring Software Blade presents a complete picture of network and security performance, enabling fast responses to changes in traffic patterns or security events.It centrally monitors Check Point devices and alerts security administrators to changes to gateways, endpoints, tunnels, remote

users and security activities234.
Reference:Monitoring Software Blade,Check Point Integrated Security Architecture,Support, Support Requests, Training, Documentation, and Knowledge base for Check Point products and services

QUESTION 28
Your internal networks 10.1.1.0/24, 10.2.2.0/24 and 192.168.0.0/16 are behind the Internet Security Gateway. Considering that Layer 2 and Layer 3 setup is correct, what are the steps you will need to do in SmartConsole in order to get the connection working?

A. 1. Define an accept rule in Security Policy.2. Define Security Gateway to hide all internal networks behind the gateway's external IP.3. Publish and install the policy.
B. 1. Define an accept rule in Security Policy.2. Define automatic NAT for each network to NAT the networks behind a public IP.3. Publish the policy.
C. 1. Define an accept rule in Security Policy.2. Define automatic NAT for each network to NAT the networks behind a public IP.3. Publish and install the policy.
D. 1. Define an accept rule in Security Policy.2. Define Security Gateway to hide all internal networks behind the gateway's external IP.3. Publish the policy.

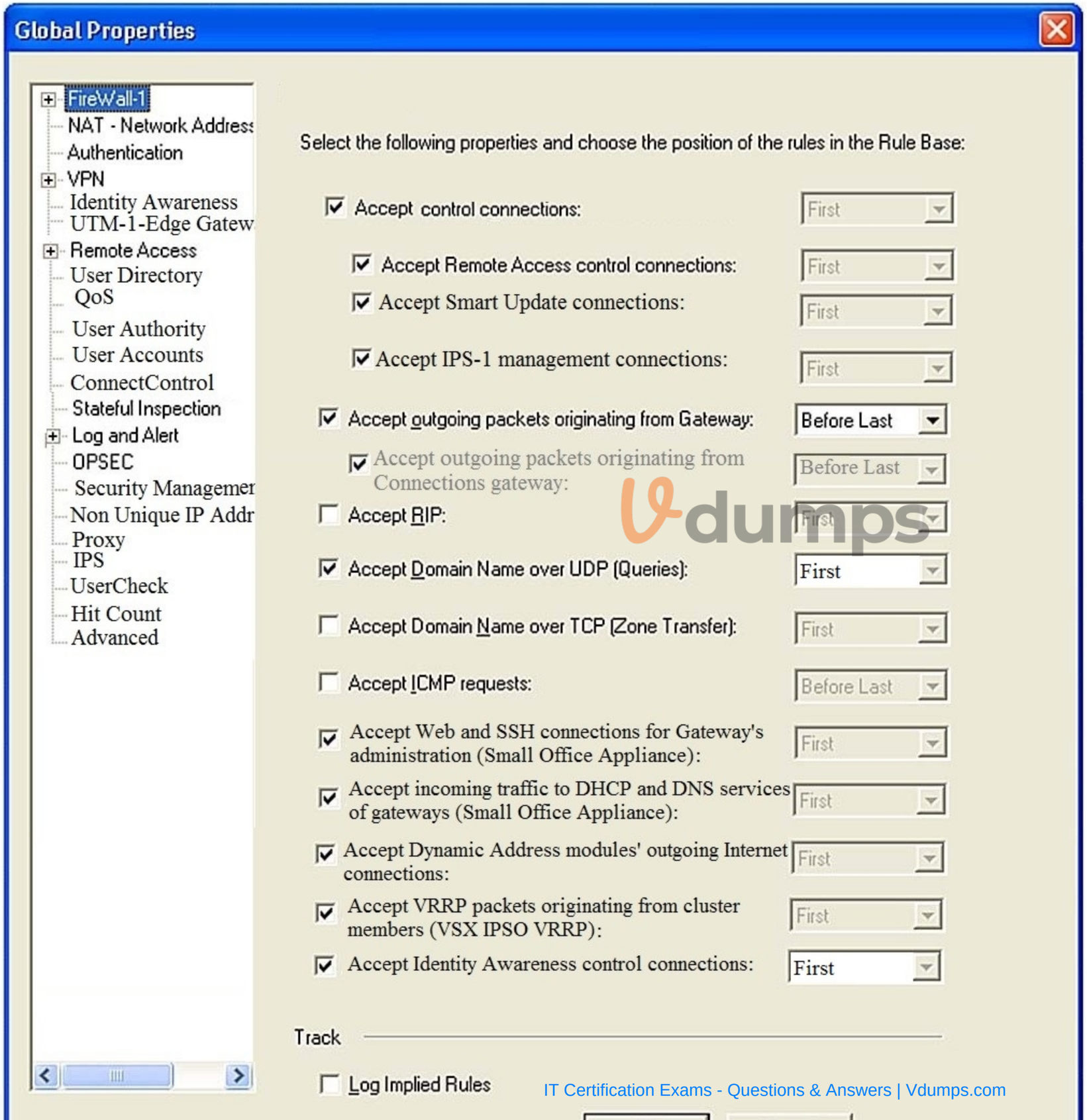
Correct Answer: C
Section:
Explanation:
The steps you will need to do in SmartConsole in order to get the connection working behind the Internet Security Gateway are:
Define an accept rule in Security Policy. This rule allows the traffic from your internal networks to pass through the Security Gateway.
Define automatic NAT for each network to NAT the networks behind a public IP. This option translates the private IP addresses of your internal networks to a public IP address assigned by your ISP router. This way, your internal networks can communicate with the Internet using a valid IP address.
Publish and install the policy. This step applies the changes you made to the Security Gateway and activates the security and NAT rules.

QUESTION 29
True or False: The destination server for Security Gateway logs depends on a Security Management Server configuration.

A. False, log servers are configured on the Log Server General Properties
B. True, all Security Gateways will only forward logs with a SmartCenter Server configuration
C. True, all Security Gateways forward logs automatically to the Security Management Server
D. False, log servers are enabled on the Security Gateway General Properties

Correct Answer: B
Section:
Explanation:
The destination server for Security Gateway logs depends on a Security Management Server configuration. This is true because the Security Management Server defines the log servers that receive logs from the Security Gateways.The log servers can be either the Security Management Server itself or a dedicated Log Server12.
Reference:Check Point R81 Logging and Monitoring Administration Guide,Check Point R81 Quantum Security Gateway Guide

QUESTION 30
Consider the Global Properties following settings:



The selected option ''Accept Domain Name over UDP (Queries)'' means:

A. UDP Queries will be accepted by the traffic allowed only through interfaces with external anti-spoofing topology and this will be done before first explicit rule written by Administrator in a Security Policy.
B. All UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.
C. No UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.
D. All UDP Queries will be accepted by the traffic allowed by first explicit rule written by Administrator in a Security Policy.

Correct Answer: A
Section:
Explanation:
The selected option ''Accept Domain Name over UDP (Queries)'' means that UDP Queries will be accepted by the traffic allowed only through interfaces with external anti-spoofing topology and this will be done before first explicit rule written by Administrator in a Security Policy. This option enables the Security Gateway to accept DNS queries from external hosts and forward them to internal DNS servers. The queries are accepted by an implied rule that is applied before the explicit rules in the Security Policy. The implied rule only allows queries from interfaces that have external anti-spoofing groups defined .
Reference: Check Point R81 Quantum Security Gateway Guide, Implied Rules

QUESTION 31
How is communication between different Check Point components secured in R80? As with all questions, select the best answer.

A. By using IPSEC
B. By using SIC
C. By using ICA
D. By using 3DES

Correct Answer: B
Section:
Explanation:
The communication between different Check Point components is secured in R80 by using SIC. SIC stands for Secure Internal Communication and it is a mechanism that ensures the authenticity and confidentiality of communication between Check Point components, such as Security Gateways, Security Management Servers, Log Servers, etc.SIC uses certificates issued by the Internal CA (ICA) and encryption algorithms such as AES-25634.
Reference:Check Point R81 Quantum Security Gateway Guide,Check Point R81 Quantum Security Management Administration Guide

QUESTION 32
Identify the ports to which the Client Authentication daemon listens on by default?

A. 259, 900
B. 256, 257
C. 8080, 529
D. 80, 256

Correct Answer: A
Section:
Explanation:
The ports to which the Client Authentication daemon listens on by default are 259 and 900. Client Authentication is a method that allows users to authenticate with the Security Gateway before they are allowed access to protected resources. The Client Authentication daemon (fwauthd) runs on the Security Gateway and listens for authentication requests on TCP ports 259 and 900 .
Reference: [Check Point R81 Remote Access VPN Administration Guide], [Check Point R81 Quantum Security Gateway Guide]

QUESTION 33
Which two Identity Awareness commands are used to support identity sharing?

A. Policy Decision Point (PDP) and Policy Enforcement Point (PEP)
B. Policy Enforcement Point (PEP) and Policy Manipulation Point (PMP)
C. Policy Manipulation Point (PMP) and Policy Activation Point (PAP)
D. Policy Activation Point (PAP) and Policy Decision Point (PDP)

Correct Answer: A
Section:
Explanation:
The answer is A because Identity Awareness commands are used to support identity sharing between Security Gateways. Policy Decision Point (PDP) is the Security Gateway that collects identities from various sources and shares them with other gateways.Policy Enforcement Point (PEP) is the Security Gateway that enforces the policy based on the identities received from the PDP12Reference:Check Point R81 Identity Awareness Administration Guide,Check Point R81 Security Management Administration Guide

QUESTION 34
True or False: In R80, more than one administrator can login to the Security Management Server with write permission at the same time.

A. False, this feature has to be enabled in the Global Properties.
B. True, every administrator works in a session that is independent of the other administrators.
C. True, every administrator works on a different database that is independent of the other administrators.
D. False, only one administrator can login with write permission.

Correct Answer: B
Section:
Explanation:
The answer is B because in R80 and above, more than one administrator can login to the Security Management Server with write permission at the same time. Every administrator works in a session that is independent of the other administrators.This is called concurrent administration and it allows multiple administrators to work on the same policy package simultaneously34Reference:Check Point R80.10 Concurrent Administration,Check Point R80.40 Security Management Administration Guide

QUESTION 35
Which one of the following is TRUE?

A. Ordered policy is a sub-policy within another policy
B. One policy can be either inline or ordered, but not both
C. Inline layer can be defined as a rule action
D. Pre-R80 Gateways do not support ordered layers

Correct Answer: C
Section:
Explanation:
The answer is C because inline layer can be defined as a rule action in a policy layer. Inline layer is a sub-policy that contains additional rules that are applied only if the parent rule matches. Ordered layer is a policy layer that contains rules that are applied in order, from top to bottom. One policy can be either inline or ordered, but not both.Pre-R80 Gateways do support ordered layers, but not inline layers5Reference:Check Point R81 Policy Layers and Sub-Policies, [Check Point R81 Security Gateway Administration Guide]

QUESTION 36
To view statistics on detected threats, which Threat Tool would an administrator use?

A. Protections
B. IPS Protections

C. Profiles
D. ThreatWiki

Correct Answer: D
Section:
Explanation:
ThreatWiki is a web-based tool that provides statistics on detected threats, such as attack types, sources, destinations, and severity. It also allows the administrator to search for specific threats and view their details and mitigation methods. The other options are not tools for viewing statistics on detected threats.
Reference: [ThreatWiki], [ThreatWiki - Threat Emulation]

QUESTION 37
What is the purpose of a Clean-up Rule?

A. Clean-up Rules do not server any purpose.
B. Provide a metric for determining unnecessary rules.
C. To drop any traffic that is not explicitly allowed.
D. Used to better optimize a policy.

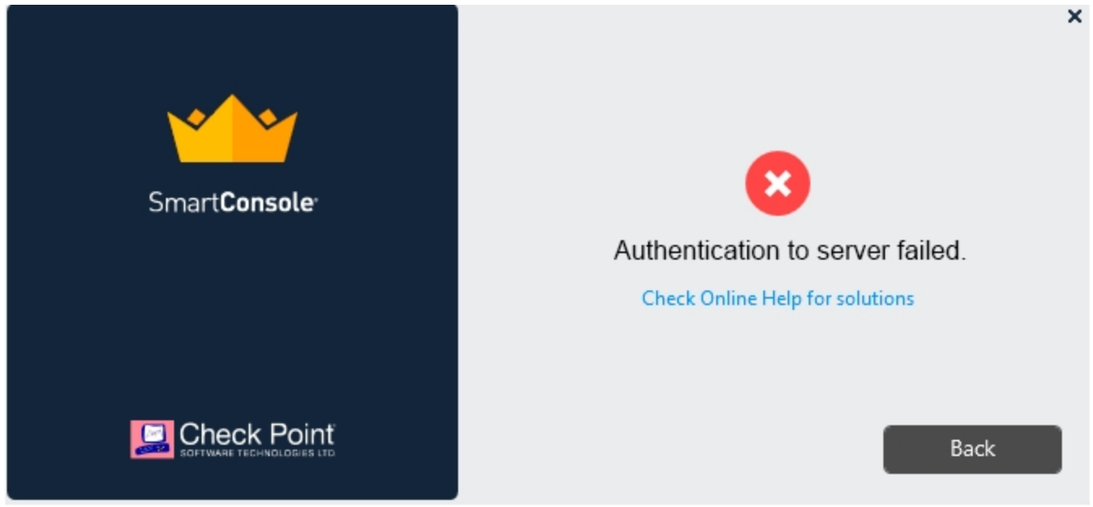
Correct Answer: C
Section:
Explanation:
A clean-up rule is a rule that is placed at the end of the security policy to drop any traffic that is not explicitly allowed by the previous rules.It is a best practice to have a clean-up rule to prevent unauthorized access and log the dropped packets for analysis12. The other options are not the purpose of a clean-up rule.
Reference:Clean-up Rule,Check Point CCSA - R81: Practice Test & Explanation

QUESTION 38
What are the two types of NAT supported by the Security Gateway?

A. Destination and Hide
B. Hide and Static
C. Static and Source
D. Source and Destination

Correct Answer: B
Section:
Explanation:
The two types of NAT supported by the Security Gateway are hide NAT and static NAT. Hide NAT translates many source IP addresses into one IP address, usually the external interface of the gateway.Static NAT translates one source IP address into another IP address, usually a public IP address34. The other options are not valid types of NAT.
Reference:Network Address Translation (NAT),Check Point CCSA - R81: Practice Test & Explanation

QUESTION 39
Vanessa is attempting to log into the Gaia Web Portal. She is able to login successfully. Then she tries the same username and password for SmartConsole but gets the message in the screenshot image below. She has checked that the IP address of the Server is correct and the username and password she used to login into Gaia is also correct.



What is the most likely reason?

A. Check Point R80 SmartConsole authentication is more secure than in previous versions and Vanessa requires a special authentication key for R80 SmartConsole. Check that the correct key details are used.
B. Check Point Management software authentication details are not automatically the same as the Operating System authentication details. Check that she is using the correct details.
C. SmartConsole Authentication is not allowed for Vanessa until a Super administrator has logged in first and cleared any other administrator sessions.
D. Authentication failed because Vanessa's username is not allowed in the new Threat Prevention console update checks even though these checks passed with Gaia.

Correct Answer: B
Section:
Explanation:
The most likely reason for Vanessa's authentication failure is that she is using the wrong details for SmartConsole. Check Point Management software authentication details are not automatically the same as the Operating System authentication details.She needs to use the credentials that were defined during the initial configuration of the Security Management Server, or the ones that were assigned to her by the administrator12. The other options are not valid reasons for this error.
Reference:SmartConsole Login,Check Point CCSA - R81: Practice Test & Explanation

QUESTION 40
What is the most complete definition of the difference between the Install Policy button on the SmartConsole's tab, and the Install Policy within a specific policy?

A. The Global one also saves and published the session before installation.
B. The Global one can install multiple selected policies at the same time.
C. The local one does not install the Anti-Malware policy along with the Network policy.
D. The second one pre-select the installation for only the current policy and for the applicable gateways.

Correct Answer: D
Section:
Explanation:
The difference between the Install Policy button on the SmartConsole's tab and the Install Policy within a specific policy is that the former installs all the policies that are selected in the Install Policy window, while the latter pre-selects the installation for only the current policy and for the applicable gateways5. The other options are not accurate differences.
Reference:Installing Policies, [Check Point CCSA - R81: Practice Test & Explanation]

QUESTION 41
What is the purpose of the CPCA process?

A. Monitoring the status of processes
B. Sending and receiving logs
C. Communication between GUI clients and the SmartCenter server
D. Generating and modifying certificates

Correct Answer: D
Section:
Explanation:
The purpose of the CPCA process is generating and modifying certificates. CPCA stands for Check Point Certificate Authority and it is a process that runs on the Security Management Server or Log Server. It is responsible for creating and managing certificates for internal communication between Check Point components, such as SIC .
Reference: [Check Point R81 Quantum Security Management Administration Guide], [Check Point R81 Quantum Security Gateway Guide]

QUESTION 42
The Network Operations Center administrator needs access to Check Point Security devices mostly for troubleshooting purposes. You do not want to give her access to the expert mode, but she still should be able to run tcpdump. How can you achieve this requirement?

A. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Create new user with any UID and assign role to the user.
B. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Create new user with UID 0 and assign role to the user.
C. Create a new access role.Add expert-mode access to the role.Create new user with UID 0 and assign role to the user.
D. Create a new access role.Add expert-mode access to the role.Create new user with any UID and assign role to the user.

Correct Answer: A
Section:
Explanation:
To achieve the requirement of giving the Network Operations Center administrator access to Check Point Security devices mostly for troubleshooting purposes, but not to the expert mode, and still allowing her to run tcpdump, you need to:
Add tcpdump to CLISH using add command. This command adds a new command to the Command Line Interface Shell (CLISH) that allows running tcpdump without entering the expert mode .
Create a new access role. This option defines a set of permissions and commands that can be assigned to a user or a group of users.
Add tcpdump to the role. This option grants the permission to run tcpdump to the role.
Create new user with any UID and assign role to the user. This option creates a new user account with any User ID (UID) and assigns the role that has tcpdump permission to the user.

QUESTION 43
When logging in for the first time to a Security management Server through SmartConsole, a fingerprint is saved to the:

A. Security Management Server's /home/.fgpt file and is available for future SmartConsole authentications.
B. Windows registry is available for future Security Management Server authentications.
C. There is no memory used for saving a fingerprint anyway.
D. SmartConsole cache is available for future Security Management Server authentications.

Correct Answer: D
Section:
Explanation:
When logging in for the first time to a Security Management Server through SmartConsole, a fingerprint is saved to the SmartConsole cache and is available for future Security Management Server authentications. The fingerprint is a unique identifier of the Security Management Server that is used to verify its identity and prevent man-in-the-middle attacks. The SmartConsole cache is a local folder on the client machine that stores temporary files and settings.

QUESTION 44

Fill in the blank: By default, the SIC certificates issued by R80 Management Server are based on the _____ algorithm.

A. SHA-256
B. SHA-200
C. MD5
D. SHA-128

Correct Answer: A
Section:
Explanation:
By default, the SIC certificates issued by R80 Management Server are based on the SHA-256 algorithm1. SHA-256 is a secure hash algorithm that produces a 256-bit digest. SHA-200, MD5, and SHA-128 are not valid algorithms for SIC certificates.
Reference:SHA-1 and SHA-256 certificates in Check Point Internal CA (ICA)

QUESTION 45
Which message indicates IKE Phase 2 has completed successfully?

A. Quick Mode Complete
B. Aggressive Mode Complete
C. Main Mode Complete
D. IKE Mode Complete

Correct Answer: A
Section:
Explanation:
Quick Mode Complete is the message that indicates IKE Phase 2 has completed successfully2. IKE Phase 2 is also known as Quick Mode or Child SA in IKEv1 and IKEv2 respectively. Aggressive Mode and Main Mode are part of IKE Phase 1, which establishes the IKE SA. IKE Mode is not a valid term for IKE negotiation.
Reference:How to Analyze IKE Phase 2 VPN Status Messages,IKEv2 Phase 1 (IKE SA) and Phase 2 (Child SA) Message Exchanges,Understand IPsec IKEv1 Protocol

QUESTION 46
Administrator Dave logs into R80 Management Server to review and makes some rule changes. He notices that there is a padlock sign next to the DNS rule in the Rule Base.

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	Log	* 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	Log	* Policy Targets
7	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	* Policy Targets

What is the possible explanation for this?

A. DNS Rule is using one of the new feature of R80 where an administrator can mark a rule with the padlock icon to let other administrators know it is important.
B. Another administrator is logged into the Management and currently editing the DNS Rule.

C. DNS Rule is a placeholder rule for a rule that existed in the past but was deleted.
D. This is normal behavior in R80 when there are duplicate rules in the Rule Base.

Correct Answer: B
Section:
Explanation:
The padlock sign next to the DNS rule in the Rule Base indicates that another administrator is logged into the Management and currently editing the DNS Rule1. This is a feature of R80 that allows multiple administrators to work on the same policy simultaneously.The padlock sign prevents other administrators from modifying the same rule until the editing administrator publishes or discards the changes2. The other options are not valid explanations for the padlock sign.
Reference:156-215.80 : Check Point Certified Security Administrator (CCSA R80) : Part 19,Multi-User Policy Editing

QUESTION 47
Fill in the blank: When tunnel test packets no longer invoke a response, SmartView Monitor displays _____ for the given VPN tunnel.

A. Down
B. No Response
C. Inactive
D. Failed

Correct Answer: A
Section:
Explanation:
When tunnel test packets no longer invoke a response, SmartView Monitor displaysDownfor the given VPN tunnel1. This means that the VPN tunnel is not operational and there is no IKE or IPsec traffic passing through it. No Response, Inactive, and Failed are not valid statuses for VPN tunnels in SmartView Monitor.
Reference:Smart View Monitor displays status for all S2S VPN tunnels - Phase1 UP

QUESTION 48
You have successfully backed up your Check Point configurations without the OS information. What command would you use to restore this backup?

A. restore_backup
B. import backup
C. cp_merge
D. migrate import

Correct Answer: A
Section:
Explanation:
The command to restore a backup of Check Point configurations without the OS information isrestore_backup4. This command restores the Gaia OS configuration and the firewall database from a compressed file. The other commands are not valid for this purpose.import backupis not a valid command.cp_mergeis a command to merge policies or objects from different databases.migrate importis a command to import a previously exported database usingmigrate export.
Reference:System Backup and Restore feature in Gaia, [cp_merge], [migrate import]

QUESTION 49
What is the best sync method in the ClusterXL deployment?

A. Use 1 cluster + 1st sync
B. Use 1 dedicated sync interface
C. Use 3 clusters + 1st sync + 2nd sync + 3rd sync

D. Use 2 clusters + 1st sync + 2nd sync

Correct Answer: B
Section:
Explanation:
The best sync method in the ClusterXL deployment is to use one dedicated sync interface56. This method provides optimal performance and reliability for synchronization traffic.Using multiple sync interfaces is not recommended as it increases CPU load and does not provide 100% sync redundancy5. Using multiple clusters is not a sync method, but a cluster topology.
Reference:Sync Redundancy in ClusterXL,Best Practice for HA sync interface

QUESTION 50
Can multiple administrators connect to a Security Management Server at the same time?

A. No, only one can be connected
B. Yes, all administrators can modify a network object at the same time
C. Yes, every administrator has their own username, and works in a session that is independent of other administrators
D. Yes, but only one has the right to write

Correct Answer: C
Section:
Explanation:
Multiple administrators can connect to a Security Management Server at the same time, and each administrator has their own username and works in a session that is independent of other administrators1. This allows concurrent administration and prevents conflicts between different administrators. The other options are incorrect. Only one administrator can be connected is false. All administrators can modify a network object at the same time is false, as only one administrator can lock and edit an object at a time. Only one has the right to write is false, as all administrators have write permissions unless they are restricted by roles or permissions.
Reference:Security Management Server - Check Point Software

QUESTION 51
What Identity Agent allows packet tagging and computer authentication?

A. Endpoint Security Client
B. Full Agent
C. Light Agent
D. System Agent

Correct Answer: B
Section:
Explanation:
The Full Identity Agent allows packet tagging and computer authentication2. Packet tagging is a feature that enables the Security Gateway to identify the source user and machine of each packet, regardless of NAT or routing. Computer authentication is a feature that enables the Security Gateway to authenticate machines that are not associated with any user, such as servers or unattended workstations. The other options are incorrect. Endpoint Security Client is not an Identity Agent, but a software that provides endpoint security features such as firewall, antivirus, VPN, etc. Light Agent is an Identity Agent that does not require installation and runs on a web browser, but it does not support packet tagging or computer authentication. System Agent is not an Identity Agent, but a software that provides system information and health monitoring for endpoints.
Reference:Check Point Identity Agent for Microsoft Windows 10

QUESTION 52
In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. Which of the following options can you add to each Log, Detailed Log and Extended Log?

A. Accounting
B. Suppression
C. Accounting/Suppression

D. Accounting/Extended

Correct Answer: C
Section:
Explanation:
In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log.You can add Accounting and/or Suppression to each of these options1. Accounting enables you to track the amount of data that is sent or received by a specific rule. Suppression enables you to reduce the number of logs that are generated by a specific rule. Therefore, the correct answer is C. Accounting/Suppression.
Reference:Logging and Monitoring Administration Guide R80 - Check Point Software

QUESTION 53
You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don't have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

A. fw ctl multik dynamic_dispatching on
B. fw ctl multik dynamic_dispatching set_mode 9
C. fw ctl multik set_mode 9
D. fw ctl miltik pq enable

Correct Answer: C
Section:
Explanation:
To optimize drops, you can use Priority Queues and fully enable Dynamic Dispatcher on the Security Gateway23. Priority Queues are a mechanism that prioritizes part of the traffic when the Security Gateway is stressed and needs to drop packets. Dynamic Dispatcher is a feature that dynamically assigns new connections to a CoreXL FW instance based on the utilization of CPU cores.To enable both features, you need to run the commandfw ctl multik set_mode 9on the Security Gateway4. Therefore, the correct answer is C.fw ctl multik set_mode 9.
Reference:CoreXL Dynamic Dispatcher - Check Point Software,Firewall Priority Queues in R80.x / R81.x - Check Point Software,Separate Config for Dynamic Dispatcher and Priority Queues

QUESTION 54
Which two of these Check Point Protocols are used by ?

A. ELA and CPD
B. FWD and LEA
C. FWD and CPLOG
D. ELA and CPLOG

Correct Answer: B
Section:
Explanation:
The two Check Point Protocols that are used by are FWD and LEA567. FWD is the Firewall Daemon that handles communication between different Check Point components, such as Security Management Server, Security Gateway, SmartConsole, etc. LEA is the Log Export API that allows external applications to retrieve logs from the Security Gateway or Security Management Server. Therefore, the correct answer is B. FWD and LEA.
Reference:Border Gateway Protocol - Check Point Software,Check Point IPS Datasheet,List of valid protocols for services? - Check Point CheckMates

QUESTION 55
To ensure that VMAC mode is enabled, which CLI command you should run on all cluster members? Choose the best answer.

A. fw ctl set int fwha vmac global param enabled
B. fw ctl get int fwha vmac global param enabled; result of command should return value 1
C. cphaprob --a if
D. fw ctl get int fwha_vmac_global_param_enabled; result of command should return value 1

Correct Answer: B
Section:
Explanation:
To ensure that VMAC mode is enabled, you should run the commandfw ctl get int fwha_vmac_global_param_enabledon all cluster members and check that the result of the command returns the value 11. This command shows the current value of the global kernel parameterfwha_vmac_global_param_enabled, which controls whether VMAC mode is enabled or disabled.VMAC mode is a feature that associates a Virtual MAC address with each Virtual IP address of the cluster, which reduces the need for Gratuitous ARP packets and improves failover performance1. The other options are incorrect. Option A is not a valid command.Option C is a command to show the status of cluster interfaces, not VMAC mode2.Option D is a command to show the value of a different global kernel parameter,fwha_vmac_global_param_enabled, which controls whether VMAC mode is enabled for all interfaces or only for non-VLAN interfaces1.
Reference:How to enable ClusterXL Virtual MAC (VMAC) mode,cphaprob

QUESTION 56
What is the SOLR database for?

A. Used for full text search and enables powerful matching capabilities
B. Writes data to the database and full text search
C. Serves GUI responsible to transfer request to the DLE server
D. Enables powerful matching capabilities and writes data to the database

Correct Answer: A
Section:
Explanation:
The SOLR database is used for full text search and enables powerful matching capabilities3. SOLR is an open source enterprise search platform that provides fast and scalable indexing and searching of data. It supports advanced features such as faceting, highlighting, spell checking, synonyms, etc.The SOLR database is used by Check Point products such as SmartLog and SmartEvent to store and query logs and events3. The other options are incorrect. Option B is false, as SOLR does not write data to the database, but only reads data from it. Option C is false, as SOLR does not serve GUI, but only provides a RESTful API for queries. Option D is false, as SOLR does not enable powerful matching capabilities and write data to the database, but only enables powerful matching capabilities.
Reference:SOLR - Check Point Software, [Apache Solr]

QUESTION 57
Which of the following commands is used to monitor cluster members?

A. cphaprob state
B. cphaprob status
C. cphaprob
D. cluster state

Correct Answer: A
Section:
Explanation:
The command that is used to monitor cluster members iscphaprob state. This command shows the state of each cluster member (Active, Standby, Down, etc.) and the reason for the state (OK, HA Failure, CCP Failure, etc.). It also shows the state synchronization status (Synchronized or Not Synchronized) and the uptime of each cluster member. The other options are incorrect. Option B is a command to show the status of cluster services, not cluster members. Option C is not a valid command by itself, as it requires an argument such asstate,status,list, etc. Option D is not a valid command at all.
Reference: [cphaprob]

QUESTION 58
Fill in the blank: Service blades must be attached to a _____.

A. Security Gateway
B. Management container

C. Management server
D. Security Gateway container

Correct Answer: A
Section:
Explanation:
Service blades must be attached to a Security Gateway. A Security Gateway is a device that enforces security policies on traffic that passes through it. A service blade is a software module that provides a specific security function, such as firewall, VPN, IPS, etc. A Security Gateway can have one or more service blades attached to it, depending on the license and hardware capabilities. The other options are incorrect. A management container is a virtualized environment that hosts a Security Management Server or a Log Server. A management server is a device that manages security policies and distributes them to Security Gateways. A Security Gateway container is not a valid term in Check Point terminology.
Reference: [Check Point R81 Security Management Administration Guide], [Check Point R81 CloudGuard Administration Guide]

QUESTION 59
Fill in the blank: An LDAP server holds one or more _____.

A. Server Units
B. Administrator Units
C. Account Units
D. Account Servers

Correct Answer: C
Section:
Explanation:
An LDAP server holds one or more Account Units. An Account Unit is a logical representation of an LDAP server in the Check Point database. It defines the connection parameters, authentication methods, and user and group information that are retrieved from the LDAP server. An Account Unit allows the Security Gateway to use the LDAP server for user authentication and identity awareness. The other options are incorrect. A Server Unit is a logical representation of a Check Point server in the Check Point database. An Administrator Unit is a logical representation of an administrator or an administrator group in the Check Point database. An Account Server is not a valid term in Check Point terminology.
Reference: [Check Point R81 Identity Awareness Administration Guide], [Check Point R81 Security Management Administration Guide], [Check Point R81 SmartConsole R81 Resolved Issues]

QUESTION 60
Fill in the blank: In Security Gateways R75 and above, SIC uses _____ for encryption.

A. AES-128
B. AES-256
C. DES
D. 3DES

Correct Answer: A
Section:
Explanation:
In Security Gateways R75 and above, SIC uses AES-128 for encryption. SIC stands for Secure Internal Communication, which is a mechanism that establishes trust between Check Point components, such as Security Gateways, Security Management Servers, Log Servers, etc. SIC uses certificates to authenticate and encrypt the communication between the components. AES-128 is an encryption algorithm that uses a 128-bit key to encrypt and decrypt data. The other options are incorrect. AES-256 is an encryption algorithm that uses a 256-bit key, but it is not used by SIC. DES and 3DES are older encryption algorithms that use 56-bit and 168-bit keys respectively, but they are not used by SIC either.
Reference: [Secure Internal Communication (SIC) between Check Point components], AES - Wikipedia, DES - Wikipedia, Triple DES - Wikipedia

QUESTION 61
What protocol is specifically used for clustered environments?

A. Clustered Protocol
B. Synchronized Cluster Protocol
C. Control Cluster Protocol
D. Cluster Control Protocol

Correct Answer: D
Section:
Explanation:
The protocol that is specifically used for clustered environments is Cluster Control Protocol (CCP). CCP is a proprietary Check Point protocol that is used for communication between cluster members and for cluster administration. CCP enables cluster members to exchange state information, synchronize connections, monitor interfaces, and perform failover operations. The other options are incorrect. Clustered Protocol, Synchronized Cluster Protocol, and Control Cluster Protocol are not valid terms in Check Point terminology.
Reference: [Cluster Control Protocol (CCP) - Check Point Software]

QUESTION 62
Which of the following is NOT a tracking option? (Select three)

A. Partial log
B. Log
C. Network log
D. Full log

Correct Answer: A, C, D
Section:
Explanation:
The options that are not tracking options are Partial log, Network log, and Full log. Tracking options are settings that determine how the Security Gateway handles traffic that matches a rule in the security policy. The valid tracking options are Log, Detailed Log, Extended Log, Alert, Mail, SNMP trap, User Defined Alert, and None. The other options are incorrect. Log is a tracking option that records basic information about the traffic, such as source, destination, service, action, etc. Detailed Log is a tracking option that records additional information about the traffic, such as NAT details, data amount, etc. Extended Log is a tracking option that records even more information about the traffic, such as matched IPS protections, application details, etc.
Reference: [Logging and Monitoring Administration Guide R80 - Check Point Software]

QUESTION 63
Which command shows the installed licenses?

A. cplic print
B. print cplic
C. fwlic print
D. show licenses

Correct Answer: A
Section:
Explanation:
The command that shows the installed licenses iscplic print. This command displays the license information on a Check Point server or Security Gateway. It shows the license type, expiration date, attached blades, etc. The other options are incorrect.print cplicis not a valid command.fwlic printis not a valid command.show licensesis not a valid command.
Reference: [How to check license status on SecurePlatform / Gaia from CLI]

QUESTION 64
Of all the Check Point components in your network, which one changes most often and should be backed up most frequently?

A. SmartManager
B. SmartConsole
C. Security Gateway
D. Security Management Server

Correct Answer: D
Section:
Explanation:
The Security Management Server is the component that changes most often and should be backed up most frequently, because it stores all the security policies and configurations for the Check Point components in your network. The other components are either clients or gateways that do not change as frequently.

QUESTION 65
Which option would allow you to make a backup copy of the OS and Check Point configuration, without stopping Check Point processes?

A. All options stop Check Point processes
B. backup
C. migrate export
D. snapshot

Correct Answer: D
Section:
Explanation:
The snapshot option would allow you to make a backup copy of the OS and Check Point configuration, without stopping Check Point processes. A snapshot is a full system backup, including network interfaces, routing tables, and Check Point products and configuration. The other options require stopping Check Point processes or do not backup the OS.

QUESTION 66
What is the Transport layer of the TCP/IP model responsible for?

A. It transports packets as datagrams along different routes to reach their destination.
B. It manages the flow of data between two hosts to ensure that the packets are correctly assembled and delivered to the target application.
C. It defines the protocols that are used to exchange data between networks and how host programs interact with the Application layer.
D. It deals with all aspects of the physical components of network connectivity and connects with different network types.

Correct Answer: B
Section:
Explanation:
The Transport layer of the TCP/IP model is responsible for managing the flow of data between two hosts to ensure that the packets are correctly assembled and delivered to the target application. It also provides error detection and correction, flow control, and multiplexing. The Transport layer uses protocols such as TCP and UDP.

QUESTION 67
Which of the following is the most secure means of authentication?

A. Password
B. Certificate
C. Token
D. Pre-shared secret

Correct Answer: B
Section:
Explanation:
Certificate is the most secure means of authentication among the given options2. A certificate is a digital document that contains information about the identity of a user or a device, and is signed by a trusted authority. A certificate can be used to prove the identity of a user or a device without revealing any sensitive information, such as passwords or tokens. Password, token, and pre-shared secret are less secure means of authentication because they can be easily compromised, stolen, or guessed by attackers.
Reference:Secure User Authentication Methods - freeCodeCamp.org,What is the Most Secure Authentication Method for Your Organization ...

QUESTION 68
What is the BEST command to view configuration details of all interfaces in Gaia CLISH?

A. ifconfig -a
B. show interfaces
C. show interfaces detail
D. show configuration interface

Correct Answer: D
Section:
Explanation:
The BEST command to view configuration details of all interfaces in Gaia CLISH isshow configuration interface3. This command displays the interface name, IP address, netmask, state, MTU, and other parameters for each interface. ifconfig -a, show interfaces, and show interfaces detail are not valid commands in Gaia CLISH.
Reference:How to configure static routes in CLISH on Gaia OS and IPSO OS,GAIA CLISH Commands - Fir3net,Gaia Administration Guide R80 - Check Point Software,Gaia Clish commands including User Defined (Extended) commands

QUESTION 69
Fill in the blank: Authentication rules are defined for _____.

A. User groups
B. Users using UserCheck
C. Individual users
D. All users in the database

Correct Answer: A
Section:
Explanation:
Authentication rules are defined foruser groupsrather than individual users1. To define authentication rules, you must first define users and groups.You can define users with the Check Point user database, or with an external server, such as LDAP1.UserCheck is a feature that enables user interaction with security events2. Individual users and all users in the database are not valid options for defining authentication rules.
Reference:How to Configure Client Authentication,UserCheck

QUESTION 70
Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

A. ThreatWiki
B. Whitelist Files
C. AppWiki
D. IPS Protections

Correct Answer: A

Section:
Explanation:
ThreatWiki is a tool that provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed3. ThreatWiki is a web-based service that collects information about files from various sources, such as Check Point customers, partners, and researchers.Administrators can use ThreatWiki to view file reputation, upload files for analysis, and download indicators of compromise3. Whitelist Files, AppWiki, and IPS Protections are not tools that provide a list of trusted files.
Reference:Threat Prevention R80.40 Administration Guide

QUESTION 71
Which of the following is an authentication method used for Identity Awareness?

A. SSL
B. Captive Portal
C. PKI
D. RSA

Correct Answer: B
Section:
Explanation:
Captive Portal is an authentication method used for Identity Awareness4. Captive Portal is a web-based authentication method that redirects users to a browser-based login page when they try to access the network. Users must provide their credentials to access the network resources.Captive Portal can be used for guest users or users who are not identified by other methods4. SSL, PKI, and RSA are not authentication methods used for Identity Awareness, but rather encryption or certificate technologies.
Reference:Identity Awareness Reference Architecture and Best Practices

QUESTION 72
The SIC Status ''Unknown'' means

A. There is connection between the gateway and Security Management Server but it is not trusted.
B. The secure communication is established.
C. There is no connection between the gateway and Security Management Server.
D. The Security Management Server can contact the gateway, but cannot establish SIC.

Correct Answer: C
Section:
Explanation:
The SIC Status ''Unknown'' means that there is no connection between the gateway and Security Management Server.This can happen if the gateway is down, unreachable, or has not been initialized yet12.
Reference:Check Point R81 Security Management Administration Guide,Free Check Point CCSA Sample Questions and Study Guide

QUESTION 73
What is a reason for manual creation of a NAT rule?

A. In R80 all Network Address Translation is done automatically and there is no need for manually defined NAT-rules.
B. Network Address Translation of RFC1918-compliant networks is needed to access the Internet.
C. Network Address Translation is desired for some services, but not for others.
D. The public IP-address is different from the gateway's external IP

Correct Answer: D
Section:
Explanation:

A reason for manual creation of a NAT rule is when the public IP-address is different from the gateway's external IP.This can happen when the gateway is behind another NAT device or firewall3.
Reference:Check Point R81 Security Gateway Administration Guide,Check Point CCSA - R81: Practice Test & Explanation

QUESTION 74
Which of the following commands is used to verify license installation?

A. Cplic verify license
B. Cplic print
C. Cplic show
D. Cplic license

Correct Answer: B
Section:
Explanation:
The command cplic print is used to verify license installation. It displays the installed licenses and their expiration dates .
Reference: [Check Point R81 Command Line Interface Reference Guide],Check Point :: Pearson VUE

QUESTION 75
To enforce the Security Policy correctly, a Security Gateway requires:

A. a routing table
B. awareness of the network topology
C. a Demilitarized Zone
D. a Security Policy install

Correct Answer: B
Section:
Explanation:
To enforce the Security Policy correctly, a Security Gateway requires awareness of the network topology. This means that the gateway knows which networks and interfaces are internal and external, and how to route packets between them .
Reference: [Check Point R81 Security Gateway Technical Administration Guide],Check Point CCSA - R81: Practice Test & Explanation

QUESTION 76
Which configuration element determines which traffic should be encrypted into a VPN tunnel vs. sent in the clear?

A. The firewall topologies
B. NAT Rules
C. The Rule Base
D. The VPN Domains

Correct Answer: D
Section:
Explanation:
The VPN Domains configuration element determines which traffic should be encrypted into a VPN tunnel vs. sent in the clear.The VPN Domain is the set of hosts and networks that are allowed to communicate securely with the gateway12. The firewall topologies, NAT rules, and the rule base do not directly affect the VPN encryption decision.
Reference:Check Point R81 Security Gateway Technical Administration Guide,CCSA/CCSE Exam Tips & Content - R80.X vs. R81.X - Check Point CheckMates

QUESTION 77

You have discovered suspicious activity in your network. What is the BEST immediate action to take?

A. Create a policy rule to block the traffic.
B. Create a suspicious action rule to block that traffic.
C. Wait until traffic has been identified before making any changes.
D. Contact ISP to block the traffic.

Correct Answer: B
Section:
Explanation:
The BEST immediate action to take when you have discovered suspicious activity in your network is to create a suspicious action rule to block that traffic.A suspicious action rule is a special type of rule that is triggered when a predefined condition is met, such as a malicious file download, a ransomware attack, or a data exfiltration attempt13. A suspicious action rule can block the traffic, quarantine the source, or send an alert to the administrator. Creating a policy rule to block the traffic may not be effective if the traffic does not match the rule criteria or if the policy installation is delayed. Waiting until traffic has been identified before making any changes may allow the threat to spread or cause more damage. Contacting ISP to block the traffic may not be feasible or timely, and may also affect legitimate traffic.
Reference:Check Point R81 Security Gateway Technical Administration Guide,Check Point CCSA - R81: Practice Test & Explanation | Udemy

QUESTION 78
Tom has connected to the Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward. What will happen to the changes already made?

A. Tom will have to reboot his SmartConsole computer, clear the cache, and restore changes.
B. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.
C. Tom's changes will be lost since he lost connectivity and he will have to start again.
D. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.

Correct Answer: D
Section:
Explanation:
Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.This is because SmartConsole uses a session mechanism that allows users to work offline and save their changes locally until they are ready to publish them to the Management13. If Tom loses connectivity, he can resume his session when he reconnects and continue working on his Rule Base changes. He does not need to reboot his SmartConsole computer, clear the cache, or restore changes. His changes will not be lost since he lost connectivity.
Reference:Check Point R81 Security Management Administration Guide,Check Point CCSA - R81: Practice Test & Explanation | Udemy

QUESTION 79
Which GUI tool can be used to view and apply Check Point licenses?

A. cpconfig
B. Management Command Line
C. SmartConsole
D. SmartUpdate

Correct Answer: D
Section:
Explanation:
The GUI tool that can be used to view and apply Check Point licenses is SmartUpdate.SmartUpdate is a centralized tool that allows you to manage licenses, software packages, and hotfixes for multiple gateways and clusters12. cpconfig, Management Command Line, and SmartConsole are not tools for license management.
Reference:Check Point R81 SmartUpdate Administration Guide,Check Point CCSA - R81: Practice Test & Explanation | Udemy

QUESTION 80
How would you determine the software version from the CLI?

A. fw ver
B. fw stat
C. fw monitor
D. cpinfo

Correct Answer: A
Section:
Explanation:
The command that can be used to determine the software version from the CLI is fw ver.This command displays the version of the firewall module and the build number3. fw stat, fw monitor, and cpinfo are not commands for software version identification.
Reference:Check Point R81 Command Line Interface Reference Guide, [156-315.81 Checkpoint Exam Info and Free Practice Test - ExamTopics]

QUESTION 81
In R80 Management, apart from using SmartConsole, objects or rules can also be modified using:

A. 3rd Party integration of CLI and API for Gateways prior to R80.
B. A complete CLI and API interface using SSH and custom CPCode integration.
C. 3rd Party integration of CLI and API for Management prior to R80.
D. A complete CLI and API interface for Management with 3rd Party integration.

Correct Answer: B
Section:
Explanation:
In R80 Management, apart from using SmartConsole, objects or rules can also be modified using a complete CLI and API interface using SSH and custom CPCode integration. This allows you to automate tasks, integrate with third-party tools, and create custom scripts . 3rd Party integration of CLI and API for Gateways or Management prior to R80 is not relevant for R80 Management. A complete CLI and API interface for Management with 3rd Party integration is not a specific option.
Reference: [Check Point R81 Security Management Administration Guide], [Check Point Learning and Training Frequently Asked Questions (FAQs)]

QUESTION 82
When connected to the Check Point R80 Management Server using the SmartConsole the first administrator to connect has a lock on:

A. Only the objects being modified in the Management Database and other administrators can connect to make changes using a special session as long as they all connect from the same LAN network.
B. The entire Management Database and other administrators can connect to make changes only if the first administrator switches to Read-only.
C. The entire Management Database and all sessions and other administrators can connect only as Read-only.
D. Only the objects being modified in his session of the Management Database and other administrators can connect to make changes using different sessions.

Correct Answer: D
Section:
Explanation:
The answer is D because in R80 and above, the first administrator to connect to the Management Server using SmartConsole gets a lock on only the objects being modified in his session of the Management Database. Other administrators can connect to make changes using different sessions, but they cannot modify the same objects as the first administrator until he publishes his changes.This is called concurrent administration and it allows multiple administrators to work on the same policy package simultaneously12Reference:Check Point R80.10 Concurrent Administration,Check Point R80.40 Security Management Administration Guide

QUESTION 83
Which is NOT an encryption algorithm that can be used in an IPSEC Security Association (Phase 2)?

A. AES-GCM-256
B. AES-CBC-256
C. AES-GCM-128

Correct Answer: B
Section:
Explanation:
The answer is B because AES-CBC-256 is not a supported encryption algorithm for IPsec Security Associations (Phase 2) in R81.The supported encryption algorithms are AES-GCM-128, AES-GCM-256, AES-CBC-128, 3DES, and NULL3Reference:Check Point R81 VPN Administration Guide

QUESTION 84
Fill in the blank: To create policy for traffic to or from a particular location, use the _____.

A. DLP shared policy
B. Geo policy shared policy
C. Mobile Access software blade
D. HTTPS inspection

Correct Answer: B
Section:
Explanation:
The answer is B because Geo policy shared policy is used to create policy for traffic to or from a particular location based on the source or destination country. DLP shared policy is used to prevent data loss by inspecting files and data for sensitive information. Mobile Access software blade is used to provide secure remote access to corporate resources from various devices.HTTPS inspection is used to inspect encrypted web traffic for threats and compliance4
Reference:Check Point R81 Geo Policy Administration Guide, [Check Point R81 Data Loss Prevention Administration Guide], [Check Point R81 Mobile Access Administration Guide], [Check Point R81 HTTPS Inspection Administration Guide]

QUESTION 85
After trust has been established between the Check Point components, what is TRUE about name and IP-address changes?

A. Security Gateway IP-address cannot be changed without re-establishing the trust
B. The Security Gateway name cannot be changed in command line without re-establishing trust
C. The Security Management Server name cannot be changed in SmartConsole without re-establishing trust
D. The Security Management Server IP-address cannot be changed without re-establishing the trust

Correct Answer: A
Section:
Explanation:
The answer is A because changing the Security Gateway IP-address requires re-establishing the trust with the Security Management Server by initializing the Secure Internal Communication (SIC). Changing the Security Gateway name in command line or changing the Security Management Server name or IP-address in SmartConsole does not require re-establishing the trust, but it may require updating the topology and pushing the policy.
Reference: [Check Point R81 Security Management Administration Guide], [Check Point R81 Security Gateway Administration Guide]

QUESTION 86
Which of the following is used to initially create trust between a Gateway and Security Management Server?

A. Internal Certificate Authority
B. Token

C. One-time Password
D. Certificate

Correct Answer: C
Section:
Explanation:
A one-time password is used to initially create trust between a Gateway and Security Management Server. The administrator generates a one-time password from SmartConsole and enters it on the gateway command line interface using the cpconfig command. This establishes a Secure Internal Communication (SIC) between the gateway and the server . The other options are not used for this purpose.
Reference: [Configuring Secure Internal Communication (SIC)], [Check Point CCSA - R81: Practice Test & Explanation]

QUESTION 87
John is the administrator of a R80 Security Management server managing r R77.30 Check Point Security Gateway. John is currently updating the network objects and amending the rules using SmartConsole. To make John's changes available to other administrators, and to save the database before installing a policy, what must John do?

A. Logout of the session
B. File > Save
C. Install database
D. Publish the session

Correct Answer: D
Section:
Explanation:
To make John's changes available to other administrators, and to save the database before installing a policy, John must publish the session.Publishing the session saves the changes to the database and makes them visible to other administrators1. The other options do not achieve this goal.
Reference:Publishing a Session

QUESTION 88
Fill in the blanks: There are _____ types of software containers _____.

A. Three; security management, Security Gateway, and endpoint security
B. Three; Security gateway, endpoint security, and gateway management
C. Two; security management and endpoint security
D. Two; endpoint security and Security Gateway

Correct Answer: A
Section:
Explanation:
There are three types of software containers: security management, Security Gateway, and endpoint security. A software container is a set of software blades that provide specific functionality. A security management container manages the security policy and configuration for one or more Security Gateways. A Security Gateway container enforces the security policy on the network traffic.An endpoint security container protects the data and network access of an endpoint device2. The other options are not valid types of software containers.
Reference:Software Containers

QUESTION 89
When an Admin logs into SmartConsole and sees a lock icon on a gateway object and cannot edit that object, what does that indicate?

A. The gateway is not powered on.
B. Incorrect routing to reach the gateway.
C. The Admin would need to login to Read-Only mode

D. Another Admin has made an edit to that object and has yet to publish the change.

Correct Answer: D
Section:
Explanation:
When an Admin logs into SmartConsole and sees a lock icon on a gateway object and cannot edit that object, it indicates that another Admin has made an edit to that object and has yet to publish the change. SmartConsole supports concurrent administration, which means that multiple Admins can work on the same security policy at the same time. However, when one Admin edits an object, such as a gateway, a rule, or a network, that object is locked for other Admins until the change is published or discarded. The lock icon shows which objects are being edited by other Admins and prevents conflicts or overwrites. The gateway being powered off, incorrect routing to reach the gateway, or logging in to Read-Only mode do not cause the lock icon to appear.
Reference: [Concurrent Administration], [SmartConsole Overview]

QUESTION 90
In order to modify Security Policies, the administrator can use which of the following tools? (Choose the best answer.)

A. SmartConsole and WebUI on the Security Management Server.
B. SmartConsole or mgmt_cli (API) on any computer where SmartConsole is installed.
C. Command line of the Security Management Server or mgmt_cli.exe on any Windows computer.
D. mgmt_cli (API) or WebUI on Security Gateway and SmartConsole on the Security Management Server.

Correct Answer: B
Section:
Explanation:
In order to modify Security Policies, the administrator can use SmartConsole or mgmt_cli (API) on any computer where SmartConsole is installed. SmartConsole is a graphical tool that allows the administrator to create, edit, and manage security policies using a web browser. mgmt_cli (API) is a command-line tool that allows the administrator to perform the same tasks using commands and scripts. Both tools can connect to the Security Management Server remotely from any computer that has SmartConsole installed.
Reference: [SmartConsole Overview], [mgmt_cli (API)]

QUESTION 91
A SAM rule Is implemented to provide what function or benefit?

A. Allow security audits.
B. Handle traffic as defined in the policy.
C. Monitor sequence activity.
D. Block suspicious activity.

Correct Answer: D
Section:
Explanation:
A SAM (Suspicious Activity Monitoring) rule is implemented to provide the function or benefit of blocking suspicious activity. A SAM rule is a rule that defines an action to be taken by the firewall when it detects a suspicious activity, such as an attack, a scan, or a policy violation. The action can be blocking, dropping, rejecting, or logging the traffic that triggered the suspicious activity. A SAM rule can be created manually or automatically by other security features, such as IPS, Anti-Bot, or SmartEvent.
Reference: [SAM Rules], [Suspicious Activity Rules]

QUESTION 92
Is it possible to have more than one administrator connected to a Security Management Server at once?

A. Yes, but only if all connected administrators connect with read-only permissions.
B. Yes, but objects edited by one administrator will be locked for editing by others until the session is published.

C. No, only one administrator at a time can connect to a Security Management Server
D. Yes, but only one of those administrators will have write-permissions. All others will have read-only permission.

Correct Answer: B
Section:
Explanation:
It is possible to have more than one administrator connected to a Security Management Server at once, but objects edited by one administrator will be locked for editing by others until the session is published. This feature is called concurrent administration and it allows multiple administrators to work on the same security policy at the same time. However, when one administrator edits an object, such as a gateway, a rule, or a network, that object is locked for other administrators until the change is published or discarded. The lock icon shows which objects are being edited by other administrators and prevents conflicts or overwrites.
Reference: [Concurrent Administration], [SmartConsole Overview]

QUESTION 93
In order to see real-time and historical graph views of Security Gateway statistics in SmartView Monitor, what feature needs to be enabled on the Security Gateway?

A. Logging & Monitoring
B. None - the data is available by default
C. Monitoring Blade
D. SNMP

Correct Answer: C
Section:
Explanation:
In order to see real-time and historical graph views of Security Gateway statistics in SmartView Monitor, the Monitoring Blade feature needs to be enabled on the Security Gateway. The Monitoring Blade is a software blade that collects and displays network and security performance data from the Security Gateway, such as traffic, throughput, connections, CPU usage, memory usage, etc. The Monitoring Blade can be enabled or disabled on each Security Gateway from the SmartConsole.
Reference: [Monitoring Blade], [SmartView Monitor]

QUESTION 94
What is the default shell for the command line interface?

A. Clish
B. Admin
C. Normal
D. Expert

Correct Answer: A
Section:
Explanation:
Clish is the default shell for the command line interface. It is a user-friendly shell that provides a menu-based and a command-line mode.Admin, Normal, and Expert are not valid shell names1.

QUESTION 95
When configuring Anti-Spoofing, which tracking options can an Administrator select?

A. Log, Alert, None
B. Log, Allow Packets, Email
C. Drop Packet, Alert, None
D. Log, Send SNMP Trap, Email

Correct Answer: A
Section:
Explanation:
Log, Alert, and None are the tracking options that an Administrator can select when configuring Anti-Spoofing. Log means that the packet will be logged in SmartView Tracker. Alert means that the packet will trigger an alert in SmartView Monitor.None means that no action will be taken2. The other options are not valid tracking options.

QUESTION 96
Which of the following log queries would show only dropped packets with source address of 192.168.1.1 and destination address of 172.26.1.1?

A. src:192.168.1.1 OR dst:172.26.1.1 AND action:Drop
B. src:192.168.1.1 AND dst:172.26.1.1 AND action:Drop
C. 192.168.1.1 AND 172.26.1.1 AND drop
D. 192.168.1.1 OR 172.26.1.1 AND action:Drop

Correct Answer: B
Section:
Explanation:
src:192.168.1.1 AND dst:172.26.1.1 AND action:Drop is the correct log query to show only dropped packets with source address of 192.168.1.1 and destination address of 172.26.1.1. The AND operator means that all conditions must be true for the query to match.The OR operator means that any condition can be true for the query to match3. The other queries will either show packets that are not dropped or packets that have different source or destination addresses.

QUESTION 97
Core Protections are installed as part of what Policy?

A. Access Control Policy.
B. Desktop Firewall Policy
C. Mobile Access Policy.
D. Threat Prevention Policy.

Correct Answer: D
Section:
Explanation:
Core Protections are installed as part of the Threat Prevention Policy.Core Protections are a set of IPS protections that are essential for securing your network against malicious traffic4. The other policies do not include Core Protections.

QUESTION 98
In HTTPS Inspection policy, what actions are available in the 'Actions' column of a rule?

A. 'Inspect', 'Bypass'
B. 'Inspect', 'Bypass', 'Categorize'
C. 'Inspect', 'Bypass', 'Block'
D. 'Detect', 'Bypass'

Correct Answer: A
Section:
Explanation:
The actions available in the ''Actions'' column of a rule in HTTPS Inspection policy are ''Inspect'' and ''Bypass''. ''Inspect'' means that the HTTPS traffic will be decrypted and inspected according to the Access Control policy.''Bypass'' means that the HTTPS traffic will not be decrypted and will be allowed without inspection1. The other options are not valid actions for HTTPS Inspection policy.

QUESTION 99
Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using _____.

A. Captive Portal and Transparent Kerberos Authentication
B. UserCheck
C. User Directory
D. Captive Portal

Correct Answer: A
Section:
Explanation:
Browser-based Authentication sends users to a web page to acquire identities using Captive Portal and Transparent Kerberos Authentication. Captive Portal is a web page that prompts users to enter their credentials.Transparent Kerberos Authentication is a method that automatically authenticates users who have a valid Kerberos ticket from the Active Directory domain controller2. UserCheck is a feature that allows users to interact with the security policy, not a method of authentication. User Directory is a component that integrates with external user databases, not a web page for authentication. Captive Portal alone is not enough to fill in the blank, as it is only one of the methods used by Browser-based Authentication.

QUESTION 100
With URL Filtering, what portion of the traffic is sent to the Check Point Online Web Service for analysis?

A. The complete communication is sent for inspection.
B. The IP address of the source machine.
C. The end user credentials.
D. The host portion of the URL.

Correct Answer: D
Section:
Explanation:
With URL Filtering, only the host portion of the URL is sent to the Check Point Online Web Service for analysis. The host portion is the part of the URL that identifies the web server, such as www.example.com.The Check Point Online Web Service uses this information to categorize the URL and return the appropriate action to the Security Gateway3. The other options are not sent to the Check Point Online Web Service for analysis, as they may contain sensitive or irrelevant data.

QUESTION 101
Choose what BEST describes the reason why querying logs now are very fast.

A. The amount of logs being stored is less than previous versions.
B. New Smart-1 appliances double the physical memory install.
C. Indexing Engine indexes logs for faster search results.
D. SmartConsole now queries results directly from the Security Gateway.

Correct Answer: C
Section:
Explanation:
The reason why querying logs now are very fast is that Indexing Engine indexes logs for faster search results.Indexing Engine is a component of R81 Management that creates and maintains an index of log data, which enables quick and efficient log searches4. The other options are not related to the speed of log querying. The amount of logs being stored may vary depending on the log retention settings. New Smart-1 appliances may have improved hardware specifications, but they do not affect the log querying process directly. SmartConsole queries results from the Security Management Server, not from the Security Gateway.

QUESTION 102
Rugged appliances are small appliances with ruggedized hardware and like Quantum Spark appliance they use which operating system?

A. Centos Linux
B. Gaia embedded
C. Gaia
D. Red Hat Enterprise Linux version 5

Correct Answer: B
Section:
Explanation:
Rugged appliances are small appliances with ruggedized hardware and like Quantum Spark appliance they use Gaia embedded as the operating system.Gaia embedded is a lightweight version of Gaia that is designed for small and medium businesses1. Centos Linux, Gaia, and Red Hat Enterprise Linux version 5 are not the operating systems used by Rugged appliances.

QUESTION 103
Which application is used for the central management and deployment of licenses and packages?

A. SmartProvisioning
B. SmartLicense
C. SmartUpdate
D. Deployment Agent

Correct Answer: C
Section:
Explanation:
SmartUpdate is the application that is used for the central management and deployment of licenses and packages.SmartUpdate allows administrators to manage licenses, software updates, and hotfixes for multiple Security Gateways and cluster members from one central location2. SmartProvisioning is an application that enables centralized management of network devices. SmartLicense is a feature that simplifies license management by using a cloud-based portal.Deployment Agent is a component that enables automatic deployment of software packages3.

QUESTION 104
Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?

A. Firewall
B. Application Control
C. Anti-spam and Email Security
D. Anti-Virus

Correct Answer: D
Section:
Explanation:
Anti-Virus is the Check Point software blade that prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud. Anti-Virus scans files and email attachments for viruses, worms, trojans, and other types of malware. It also uses ThreatCloud, a collaborative network that delivers real-time dynamic security intelligence, to detect unknown malware based on their behavior. Firewall is a software blade that enforces security policy by inspecting and controlling network traffic. Application Control is a software blade that enables administrators to control access to web applications. Anti-spam and Email Security is a software blade that protects email infrastructure from spam, phishing, and malware attacks.

QUESTION 105
Why is a Central License the preferred and recommended method of licensing?

A. Central Licensing is actually not supported with Gaia.

B. Central Licensing is the only option when deploying Gaia
C. Central Licensing ties to the IP address of a gateway and can be changed to any gateway if needed.
D. Central Licensing ties to the IP address of the management server and is not dependent on the IP of any gateway in the event it changes.

Correct Answer: D
Section:
Explanation:
Central License is the preferred and recommended method of licensing because it ties to the IP address of the management server and is not dependent on the IP of any gateway in the event it changes. Central License allows administrators to manage licenses for all Security Gateways from one central location. If the IP address of a gateway changes, the license remains valid as long as it is connected to the same management server. Central Licensing is supported with Gaia and is not the only option when deploying Gaia. Central Licensing does not tie to the IP address of a gateway and can not be changed to any gateway if needed.

QUESTION 106
What default layers are included when creating a new policy layer?

A. Application Control, URL Filtering and Threat Prevention
B. Access Control, Threat Prevention and HTTPS Inspection
C. Firewall, Application Control and IPSec VPN
D. Firewall, Application Control and IPS

Correct Answer: B
Section:
Explanation:
The default layers that are included when creating a new policy layer are Access Control, Threat Prevention, and HTTPS Inspection. Access Control is the layer that defines the basic firewall rules. Threat Prevention is the layer that enables the protection against various types of attacks, such as IPS, Anti-Virus, Anti-Bot, etc.HTTPS Inspection is the layer that allows the inspection of encrypted traffic1. The other options are not the default layers that are included when creating a new policy layer.

QUESTION 107
After a new Log Server is added to the environment and the SIC trust has been established with the SMS what will the gateways do?

A. The gateways can only send logs to an SMS and cannot send logs to a Log Server. Log Servers are proprietary log archive servers.
B. Gateways will send new firewall logs to the new Log Server as soon as the SIC trust is set up between the SMS and the new Log Server.
C. The firewalls will detect the new Log Server after the next policy install and redirect the new logs to the new Log Server.
D. Logs are not automatically forwarded to a new Log Server. SmartConsole must be used to manually configure each gateway to send its logs to the server.

Correct Answer: D
Section:
Explanation:
Logs are not automatically forwarded to a new Log Server. SmartConsole must be used to manually configure each gateway to send its logs to the server.After adding a new Log Server and establishing the SIC trust with the SMS, the administrator must use SmartConsole to assign the Log Server to each gateway in the Logs and Masters section of the gateway properties2. The other options are not correct, as gateways can send logs to both SMS and Log Server, Log Servers are not proprietary log archive servers, and gateways will not detect the new Log Server after the next policy install.

QUESTION 108
Name the utility that is used to block activities that appear to be suspicious.

A. Penalty Box
B. Drop Rule in the rulebase
C. Suspicious Activity Monitoring (SAM)

D. Stealth rule

Correct Answer: C
Section:
Explanation:
Suspicious Activity Monitoring (SAM) is the utility that is used to block activities that appear to be suspicious.SAM allows administrators to block connections from specific IP addresses or network objects for a specified period of time3. Penalty Box is a feature of SAM that automatically blocks connections from sources that generate too many log entries. Drop Rule in the rulebase is a firewall action that discards packets that match certain criteria. Stealth rule is a firewall rule that prevents direct access to the Security Gateway from external sources.

QUESTION 109
When URL Filtering is set, what identifying data gets sent to the Check Point Online Web Service?

A. The URL and server certificate are sent to the Check Point Online Web Service
B. The full URL, including page data, is sent to the Check Point Online Web Service
C. The host part of the URL is sent to the Check Point Online Web Service
D. The URL and IP address are sent to the Check Point Online Web Service

Correct Answer: C
Section:
Explanation:
When URL Filtering is set, only the host part of the URL is sent to the Check Point Online Web Service for analysis. The host part is the part of the URL that identifies the web server, such as www.example.com. The Check Point Online Web Service uses this information to categorize the URL and return the appropriate action to the Security Gateway. The other options are not sent to the Check Point Online Web Service for analysis, as they may contain sensitive or irrelevant data.

QUESTION 110
Name the pre-defined Roles included in Gaia OS.

A. AdminRole, and MonitorRole
B. ReadWriteRole, and ReadyOnly Role
C. AdminRole, cloningAdminRole, and Monitor Role
D. AdminRole

Correct Answer: A
Section:
Explanation:
The pre-defined Roles included in Gaia OS are AdminRole and MonitorRole. AdminRole is the role that has full access to all Gaia features and commands.MonitorRole is the role that has read-only access to Gaia features and commands1. The other options are not valid pre-defined Roles in Gaia OS.

QUESTION 111
Gaia has two default user accounts that cannot be deleted. What are those user accounts?

A. Admin and Default
B. Expert and Clish
C. Control and Monitor
D. Admin and Monitor

Correct Answer: D
Section:

Explanation:
Gaia has two default user accounts that cannot be deleted. They are Admin and Monitor. Admin is the user account that has full administrative privileges and can access both WebUI and CLI.Monitor is the user account that has read-only privileges and can access only WebUI2. The other options are not default user accounts in Gaia.

QUESTION 112
Which single Security Blade can be turned on to block both malicious files from being downloaded as well as block websites known to host malware?

A. Anti-Bot
B. None - both Anti-Virus and Anti-Bot are required for this
C. Anti-Virus
D. None - both URL Filtering and Anti-Virus are required for this.

Correct Answer: C
Section:
Explanation:
Anti-Virus is the single Security Blade that can be turned on to block both malicious files from being downloaded as well as block websites known to host malware. Anti-Virus scans files and email attachments for viruses, worms, trojans, and other types of malware.It also uses ThreatCloud, a collaborative network that delivers real-time dynamic security intelligence, to detect unknown malware based on their behavior3. Anti-Bot is a Security Blade that detects and blocks botnet communications, but it does not scan files or block websites. URL Filtering is a Security Blade that enables administrators to control access to web applications, but it does not scan files or detect malware.

QUESTION 113
Log query results can be exported to what file format?

A. Word Document (docx)
B. Comma Separated Value (csv)
C. Portable Document Format (pdf)
D. Text (txt)

Correct Answer: B
Section:
Explanation:
Log query results can be exported to Comma Separated Value (csv) file format. CSV is a file format that stores tabular data in plain text. It is compatible with various applications, such as Excel, Google Sheets, etc. The other options are not valid file formats for exporting log query results.

QUESTION 114
There are four policy types available for each policy package. What are those policy types?

A. Access Control, Threat Prevention, Mobile Access and HTTPS Inspection
B. Access Control, Custom Threat Prevention, Autonomous Threat Prevention and HTTPS Inspection
C. There are only three policy types: Access Control, Threat Prevention and NAT.
D. Access Control, Threat Prevention, NAT and HTTPS Inspection

Correct Answer: D
Section:
Explanation:
The four policy types available for each policy package are Access Control, Threat Prevention, NAT, and HTTPS Inspection. Access Control is the policy type that defines the basic firewall rules. Threat Prevention is the policy type that enables the protection against various types of attacks, such as IPS, Anti-Virus, Anti-Bot, etc. NAT is the policy type that defines the network address translation rules.HTTPS Inspection is the policy type that allows the inspection of encrypted traffic1. The other options are not valid policy types for each policy package.

QUESTION 115
Which tool allows for the automatic updating of the Gaia OS and Check Point products installed on the Gaia OS?

A. CPASE - Check Point Automatic Service Engine
B. CPAUE - Check Point Automatic Update Engine
C. CPDAS - Check Point Deployment Agent Service
D. CPUSE - Check Point Upgrade Service Engine

Correct Answer: D
Section:
Explanation:
CPUSE - Check Point Upgrade Service Engine is the tool that allows for the automatic updating of the Gaia OS and Check Point products installed on the Gaia OS.CPUSE is a web-based tool that simplifies the installation of software updates, hotfixes, and upgrade packages on Gaia OS2. The other options are not valid tools for updating Gaia OS and Check Point products.

QUESTION 116
The purpose of the Communication Initialization process is to establish a trust between the Security Management Server and the Check Point gateways. Which statement best describes this Secure Internal Communication (SIC)?

A. After successful initialization, the gateway can communicate with any Check Point node that possesses a SIC certificate signed by the same ICA.
B. Secure Internal Communications authenticates the security gateway to the SMS before http communications are allowed.
C. A SIC certificate is automatically generated on the gateway because the gateway hosts a subordinate CA to the SMS ICA.
D. New firewalls can easily establish the trust by using the expert password defined on the SMS and the SMS IP address.

Correct Answer: A
Section:
Explanation:
The statement that best describes Secure Internal Communication (SIC) is: After successful initialization, the gateway can communicate with any Check Point node that possesses a SIC certificate signed by the same ICA.SIC is a mechanism that ensures secure communication between Check Point components by using certificates that are issued by an Internal Certificate Authority (ICA)3. The other statements are not accurate descriptions of SIC.

QUESTION 117
What are the types of Software Containers?

A. Smart Console, Security Management, and Security Gateway
B. Security Management, Security Gateway, and Endpoint Security
C. Security Management, Log & Monitoring, and Security Policy
D. Security Management, Standalone, and Security Gateway

Correct Answer: B
Section:
Explanation:
The types of Software Containers are Security Management, Security Gateway, and Endpoint Security. Software Containers are virtual environments that run on top of Gaia OS and allow multiple instances of Check Point products to coexist on the same physical machine. The other options are not valid types of Software Containers.

QUESTION 118
Stateful Inspection compiles and registers connections where?

A. Connection Cache

B. State Cache
C. State Table
D. Network Table

Correct Answer: C
Section:
Explanation:
Stateful Inspection compiles and registers connections in the State Table. The State Table is a database that stores information about active connections and sessions on the Security Gateway. The other options are not valid names for the database that stores connection information.

QUESTION 119
Security Zones do no work with what type of defined rule?

A. Application Control rule
B. Manual NAT rule
C. IPS bypass rule
D. Firewall rule

Correct Answer: B
Section:
Explanation:
Security Zones are a feature of Application Control and Identity Awareness that allow you to define groups of network objects based on their level of trust.Security Zones do not work with Manual NAT rules, because Manual NAT rules are applied before the Application Control and Identity Awareness policy is enforced1.
Reference:Check Point R81 Security Management Administration Guide

QUESTION 120
Most Check Point deployments use Gaia but which product deployment utilizes special Check Point code (with unification in R81.10)?

A. Enterprise Network Security Appliances
B. Rugged Appliances
C. Scalable Platforms
D. Small Business and Branch Office Appliances

Correct Answer: C
Section:
Explanation:
Most Check Point deployments use Gaia, which is a unified operating system for all Check Point appliances, open servers, and virtualized gateways. However, some product deployments utilize special Check Point code, such as Scalable Platforms (formerly known as Maestro), which are high-performance security gateways that can scale up to 1.5 Tbps of firewall throughput.Scalable Platforms use a special version of Gaia OS called Gaia Embedded, which is planned to be unified with Gaia OS in R81.102.
Reference:Check Point R81 Release Notes

QUESTION 121
The Online Activation method is available for Check Point manufactured appliances. How does the administrator use the Online Activation method?

A. The SmartLicensing GUI tool must be launched from the SmartConsole for the Online Activation tool to start automatically.
B. No action is required if the firewall has internet access and a DNS server to resolve domain names.
C. Using the Gaia First Time Configuration Wizard, the appliance connects to the Check Point User Center and downloads all necessary licenses and contracts.

D. The cpinfo command must be run on the firewall with the switch -online-license-activation.

Correct Answer: C
Section:
Explanation:
The Online Activation method is available for Check Point manufactured appliances. The administrator uses the Online Activation method by using the Gaia First Time Configuration Wizard, the appliance connects to the Check Point User Center and downloads all necessary licenses and contracts. This method requires internet access and a valid User Center account.
Reference: [Check Point Licensing and Contract Operations User Guide], [Check Point R81 Gaia Installation and Upgrade Guide]

QUESTION 122
Both major kinds of NAT support Hide and Static NAT. However, one offers more flexibility. Which statement is true?

A. Manual NAT can offer more flexibility than Automatic NAT.
B. Dynamic Network Address Translation (NAT) Overloading can offer more flexibility than Port Address Translation.
C. Dynamic NAT with Port Address Translation can offer more flexibility than Network Address Translation (NAT) Overloading.
D. Automatic NAT can offer more flexibility than Manual NAT.

Correct Answer: A
Section:
Explanation:
Manual NAT can offer more flexibility than Automatic NAT because it allows the administrator to define the NAT rules in any order and position1.Automatic NAT creates the NAT rules automatically and places them at the top or bottom of the NAT Rule Base2.
Reference:Check Point R81 Firewall Administration Guide,Check Point R81 Security Management Administration Guide

QUESTION 123
What are the software components used by Autonomous Threat Prevention Profiles in R8I.20 and higher?

A. Sandbox, ThreatCloud, Zero Phishing, Sanitization, C&C Protection, JPS, File and URL Reputation
B. IPS, Threat Emulation and Threat Extraction
C. Sandbox, ThreatCloud, Sanitization, C&C Protection, IPS
D. IPS, Anti-Bot, Anti-Virus, SandBlast and Macro Extraction

Correct Answer: D
Section:
Explanation:
This answer is correct because these are the software components that are used by the pre-defined Autonomous Threat Prevention Profiles in R81.20 and higher1.These profiles provide zero-maintenance protection from zero-day threats and continuously and autonomously ensure that your protection is up-to-date with the latest cyber threats and prevention technologies2.
The other answers are not correct because they either include software components that are not part of the Autonomous Threat Prevention Profiles, such as Sandbox, ThreatCloud, Zero Phishing, Sanitization, C&C Protection, JPS, File and URL Reputation, or they omit some of the software components that are part of the Autonomous Threat Prevention Profiles, such as Anti-Bot, Anti-Virus, and Macro Extraction.
Autonomous Threat Prevention Management - Check Point Software
Check Point Quantum R81.20 (Titan) Release
Threat Prevention R81.20 Best Practices - Check Point Software
Check Point R81