CheckPoint

Exam Questions 156-215.81

Check Point Certified Security Administrator R81

NEW QUESTION 1
Name the file that is an electronically signed file used by Check Point to translate the features in the license into a code?

A. Both License (.lic) and Contract (.xml) files
B. cp.macro
C. Contract file (.xml)
D. license File (.lie)

Answer: B

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

NEW QUESTION 2
Which of the following is NOT an authentication scheme used for accounts created through SmartConsole?

A. RADIUS
B. Check Point password
C. Security questions
D. SecurID

Answer: C

NEW 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

Answer: D

NEW QUESTION 4
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

Answer: C

NEW QUESTION 5
Fill in the blanks: Gaia can be configured using _____ the _____.

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

Answer: A

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/C

NEW QUESTION 6
The default shell of the Gaia CLI is cli.sh. How do you change from the cli.sh shell to the advanced shell to run Linux commands?

A. Execute the command 'enable' in the cli.sh shell
B. Execute the 'conf t' command in the cli.sh shell
C. Execute the command 'expert' in the cli.sh shell
D. Execute the 'exit' command in the cli.sh shell

Answer: C

NEW QUESTION 7
Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

A. Go to clash-Run cpstop | Run cpstart
B. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway
C. Administrator does not need to perform any tas
D. Check Point will make use of the newly installed CPU and Cores

E. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy

Answer: B

NEW QUESTION 8
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.Createnew 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.

Answer: A

NEW QUESTION 9
Which statement is NOT TRUE about Delta synchronization?

A. Using UDP Multicast or Broadcast on port 8161
B. Using UDP Multicast or Broadcast on port 8116
C. Quicker than Full sync
D. Transfers changes in the Kernel tables between cluster members

Answer: A

NEW QUESTION 10

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

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.

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.

Answer: B

NEW QUESTION 10
Fill in the blank: The _____ feature allows administrators to share a policy with other policy packages.

A. Concurrent policy packages
B. Concurrent policies
C. Global Policies
D. Shared policies

Answer: D

Explanation:
"The Shared Policies section in the Security Policies shows the policies that are not in a Policy package. They are shared between all Policy packages."
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 12
URL Filtering employs a technology, which educates users on web usage policy in real time. What is the name of that technology?

A. WebCheck
B. UserCheck
C. Harmony Endpoint
D. URL categorization

Answer: B

Explanation:

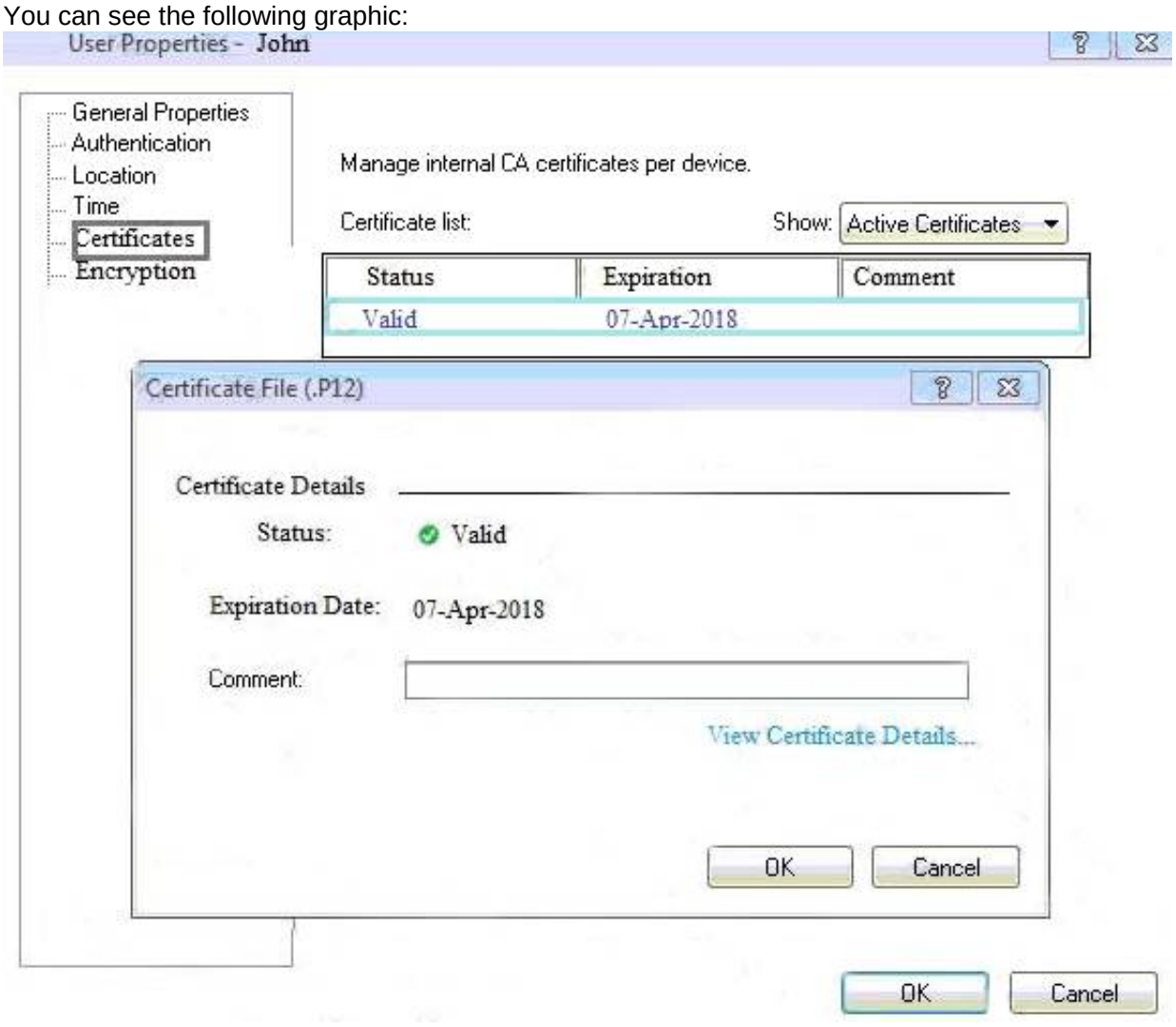
UserCheck alerts users while attemping to browse a suspicious/blocked or otherwise policy-limited website through a message in their web browsers shown before the actual page loads.

NEW QUESTION 14
When enabling tracking on a rule, what is the default option?

A. Accounting Log
B. Extended Log
C. Log
D. Detailed Log

Answer: C

NEW QUESTION 16
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.

Answer: A

NEW QUESTION 17
You are the Check Point administrator for Alpha Corp. You received a call that one of the users is unable to browse the Internet on their new tablet which is connected to the company wireless, which goes through a Check Point Gateway. How would you review the logs to see what is blocking this traffic?

A. Open SmartLog and connect remotely to the wireless controller
B. Open SmartEvent to see why they are being blocked
C. Open SmartDashboard and review the logs tab
D. From SmartConsole, go to the Log & Monitor and filter for the IP address of the tablet.

Answer: D

NEW QUESTION 18
Fill in the blank: When LDAP is integrated with Check Point Security Management, it is then referred to as _____.

A. User Center
B. User Administration
C. User Directory
D. UserCheck

Answer: C

Explanation:
User Directory lets you configure:
High Availability, to duplicate user data across multiple servers for backup. See Account Units and High Availability.

Multiple Account Units, for distributed databases.
Define LDAP Account Units, for encrypted User Directory connections. See Modifying the LDAP Server. Profiles, to support multiple LDAP vendors. See User Directory Profiles. https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 23
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.

Answer: D

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu

NEW QUESTION 25
Which path below is available only when CoreXL is enabled?

A. Slow path
B. Firewall path
C. Medium path
D. Accelerated path

Answer: C

NEW QUESTION 27
What is the purpose of the Clean-up Rule?

A. To log all traffic that is not explicitly allowed or denied in the Rule Base
B. To clean up policies found inconsistent with the compliance blade reports
C. To remove all rules that could have a conflict with other rules in the database
D. To eliminate duplicate log entries in the Security Gateway

Answer: A

Explanation:
These are basic access control rules we recommend for all Rule Bases:
There is also an implied rule that drops all traffic, but you can use the Cleanup rule to log the traffic.

NEW QUESTION 29
Fill in the blank: In Security Gateways R75 and above, SIC uses _____ for encryption.

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

Answer: A

NEW QUESTION 30
Fill in the blanks: Default port numbers for an LDAP server is _____ for standard connections and _____ SSL connections.

A. 675, 389
B. 389, 636
C. 636, 290
D. 290, 675

Answer: B

Explanation:
A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP and UDP port 389, or on port 636 for LDAPS. Global Catalog is available by default on ports 3268, and 3269 for LDAPS.

NEW QUESTION 32
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

Answer: D

NEW QUESTION 33
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

Answer: D

NEW QUESTION 37
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.

Answer: A

Explanation:
Core protections - These protections are included in the product and are assigned per gateway. They are part of the Access Control policy. ThreatCloud protections - Updated from the Check Point cloud, (see Updating IPS Protections). These protections are part of the Threat Prevention policy.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/To

NEW QUESTION 39
Using ClusterXL, what statement is true about the Sticky Decision Function?

A. Can only be changed for Load Sharing implementations
B. All connections are processed and synchronized by the pivot
C. Is configured using cpconfig
D. Is only relevant when using SecureXL

Answer: A

NEW QUESTION 42
Which Threat Prevention Software Blade provides protection from malicious software that can infect your network computers? (Choose the best answer.)

A. IPS
B. Anti-Virus
C. Anti-Malware
D. Content Awareness

Answer: B

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/To "Check Point Antivirus Software Blade prevents and stops
threats such as malware, viruses, and Trojans from entering and infecting a network"
Also here -https://www.checkpoint.com/downloads/products/antivirus-datasheet.pdf

NEW QUESTION 44
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

Answer: B

NEW QUESTION 47
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.

Answer: C

Explanation:
Prevent Access to Malicious Websites
The Antivirus Software Blade scans outbound URL requests and ensures users do not visit websites that are known to distribute malware.
Stop Incoming Malicious Files
Check Point Antivirus Software Blade prevents and stops threats such as malware, viruses, and Trojans from entering and infecting a network.
https://www.checkpoint.com/downloads/products/antivirus-datasheet.pdf

NEW QUESTION 48
Which of the following is NOT a tracking option? (Select three)

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

Answer: ACD

NEW QUESTION 49
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

Answer: C

Explanation:
Ref: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 52
Fill in the blank: _____ is the Gaia command that turns the server off.

A. sysdown
B. exit
C. halt
D. shut-down

Answer: C

NEW QUESTION 55
Fill in the blank: Service blades must be attached to a _____.

A. Security Gateway
B. Management container
C. Management server
D. Security Gateway container

Answer: A

NEW QUESTION 57
Session unique identifiers are passed to the web api using which http header option?

A. X-chkp-sid
B. Accept-Charset
C. Proxy-Authorization
D. Application

Answer: C

NEW QUESTION 60
What licensing feature is used to verify licenses and activate new licenses added to the License and Contracts repository?

A. Verification tool
B. Verification licensing
C. Automatic licensing
D. Automatic licensing and Verification tool

Answer: D

NEW QUESTION 64
What is the main difference between Static NAT and Hide NAT?

A. Static NAT only allows incoming connections to protect your network.
B. Static NAT allow incoming and outgoing connection
C. Hide NAT only allows outgoing connections.
D. Static NAT only allows outgoing connection
E. Hide NAT allows incoming and outgoing connections.
F. Hide NAT only allows incoming connections to protect your network.

Answer: B

Explanation:

Hide NAT only translates the source address to hide it behind a gateway.

NEW QUESTION 65
Fill in the blanks: The _____ collects logs and sends them to the _____.

A. Log server; Security Gateway
B. Log server; security management server
C. Security management server; Security Gateway
D. Security Gateways; log server

Answer: D

Explanation:
Gateways send their logs to the log server.

NEW QUESTION 67
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.

Answer: B

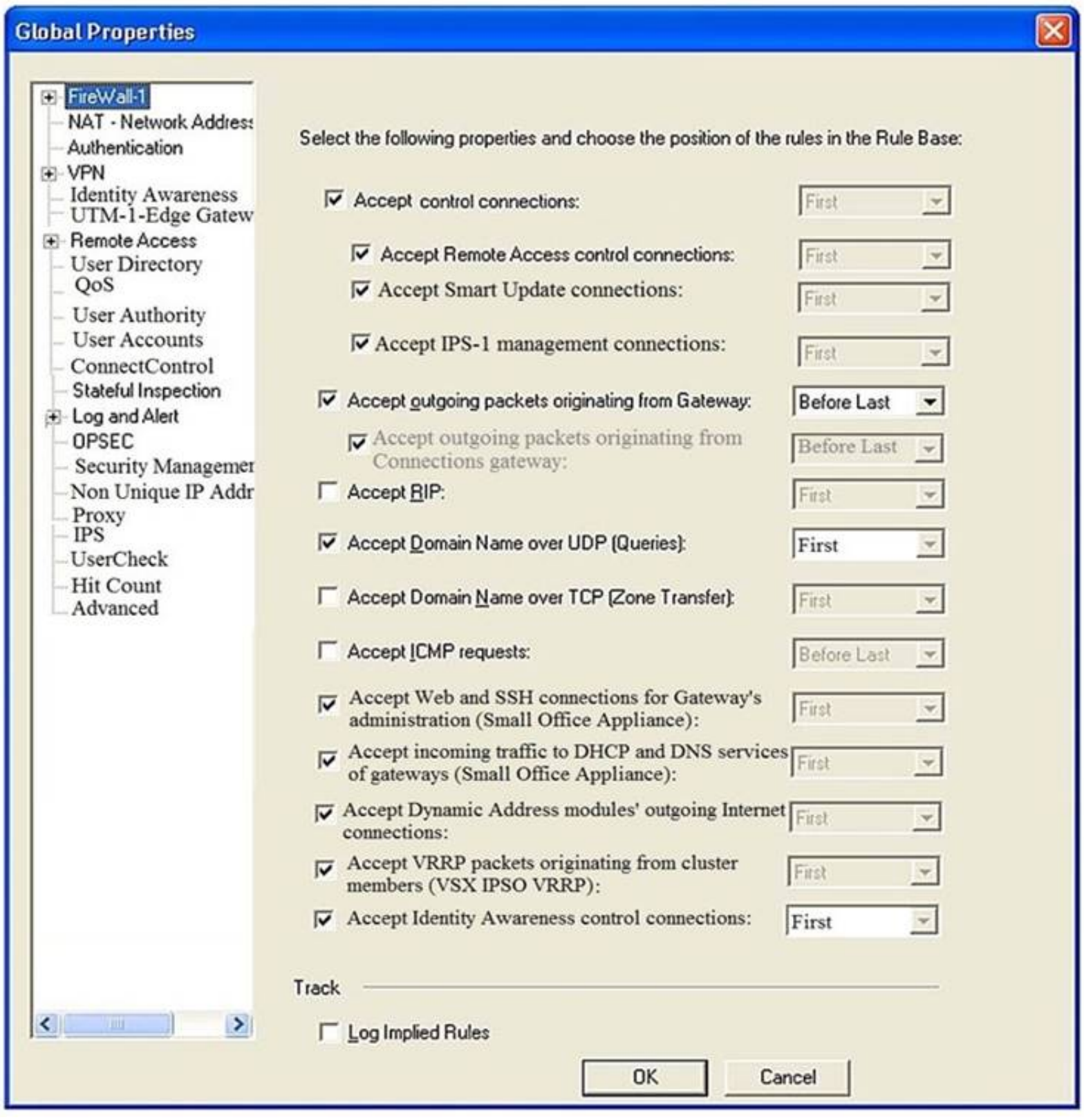
NEW QUESTION 71
The Gateway Status view in SmartConsole shows the overall status of Security Gateways and Software Blades. What does the Status Attention mean?

A. Cannot reach the Security Gateway.
B. The gateway and all its Software Blades are working properly.
C. At least one Software Blade has a minor issue, but the gateway works.
D. Cannot make SIC between the Security Management Server and the Security Gateway

Answer: C

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu

NEW QUESTION 72
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.

Answer: A

NEW QUESTION 74
Fill in the blank: Back up and restores can be accomplished through _____.

A. SmartConsole, WebUI, or CLI
B. WebUI, CLI, or SmartUpdate
C. CLI, SmartUpdate, or SmartBackup
D. SmartUpdate, SmartBackup, or SmartConsole

Answer: A

Explanation:
Backup and RestoreThese options let you: To back up a configuration:
The Backup window opens.

NEW QUESTION 79
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

Answer: D

NEW QUESTION 83
What is the BEST method to deploy Identity Awareness for roaming users?

A. Use Office Mode
B. Use identity agents
C. Share user identities between gateways
D. Use captive portal

Answer: B

Explanation:
Using Endpoint Identity Agents give you:

NEW QUESTION 87
Which deployment adds a Security Gateway to an existing environment without changing IP routing?

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

Answer: B

NEW QUESTION 88
Which information is included in the “Extended Log” tracking option, but is not included in the “Log” tracking option?

A. file attributes
B. application information
C. destination port
D. data type information

Answer: B

NEW QUESTION 92
Please choose correct command syntax to add an “emailserver1” host with IP address 10.50.23.90 using GAiA management CLI?

A. host name myHost12 ip-address 10.50.23.90
B. mgmt add host name ip-address 10.50.23.90
C. add host name emailserver1 ip-address 10.50.23.90
D. mgmt add host name emailserver1 ip-address 10.50.23.90

Answer: D

NEW QUESTION 96
SmartEvent does NOT use which of the following procedures to identity events:

A. Matching a log against each event definition
B. Create an event candidate
C. Matching a log against local exclusions
D. Matching a log against global exclusions

Answer: C

NEW QUESTION 101
Which is a suitable command to check whether Drop Templates are activated or not?

A. fw ctl get int activate_drop_templates
B. fwaccel stat
C. fwaccel stats
D. fw ctl templates –d

Answer: B

NEW QUESTION 106
Which backup utility captures the most information and tends to create the largest archives?

A. backup
B. snapshot
C. Database Revision
D. migrate export

Answer: B

NEW QUESTION 107
Which SmartConsole application shows correlated logs and aggregated data to provide an overview of potential threats and attack patterns?

A. SmartEvent
B. SmartView Tracker
C. SmartLog
D. SmartView Monitor

Answer: A

Explanation:
https://www.checkpoint.com/downloads/products/smartevent-datasheet.pdf

NEW QUESTION 111
What type of NAT is a one-to-one relationship where each host is translated to a unique address?

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

Answer: B

NEW QUESTION 112
View the rule below. What does the pen-symbol in the left column mean?

3	HR can access to social network applications	HR	Internet
4	All employees can access YouTube for work purposes	Corporate LANs Branch Office LAN Data Center LAN	Internet

A. Those rules have been published in the current session.
B. Rules have been edited by the logged in administrator, but the policy has not been published yet.
C. Another user has currently locked the rules for editing.
D. The configuration lock is presen
E. Click the pen symbol in order to gain the lock.

Answer: B

NEW QUESTION 115
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.

Answer: B

NEW QUESTION 120
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.

Answer: C

NEW QUESTION 121
What is the purpose of Captive Portal?

A. It manages user permission in SmartConsole
B. It provides remote access to SmartConsole
C. It authenticates users, allowing them access to the Internet and corporate resources
D. It authenticates users, allowing them access to the Gaia OS

Answer: C

Explanation:
Captive Portal is a simple method that authenticates users with a web interface. When users try to access a protected web resource, they enter authentication information in a form that shows in their web browser.
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_IdentityAwareness_AdminG

NEW QUESTION 126
You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

A. fwd
B. fwm
C. cpd
D. cpwd

Answer: B

NEW QUESTION 129
In which scenario is it a valid option to transfer a license from one hardware device to another?

A. From a 4400 Appliance to a 2200 Appliance
B. From a 4400 Appliance to an HP Open Server
C. From an IBM Open Server to an HP Open Server
D. From an IBM Open Server to a 2200 Appliance

Answer: A

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

NEW QUESTION 130
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

Answer: D

NEW QUESTION 135
In _____ NAT, the _____ is translated.

A. Hide; source
B. Static; source
C. Simple; source
D. Hide; destination

Answer: A

NEW QUESTION 138
Choose what BEST describes users on Gaia Platform.

A. There are two default users and neither can be deleted.
B. There are two default users and one cannot be deleted.
C. There is one default user that can be deleted.
D. There is one default user that cannot be deleted.

Answer: A

Explanation:
These users are created by default and cannot be deleted: admin
Has full read/write capabilities for all Gaia features, from the Gaia Portal and the Gaia Clish. This user has a User ID of 0, and therefore has all of the privileges of a root user.
monitor
Has read-only capabilities for all features in the Gaia Portal and the Gaia Clish, and can change its own password.
You must give a password for this user before the account can be used.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/U

NEW QUESTION 141
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

Answer: B

NEW QUESTION 144
Using R80 Smart Console, what does a "pencil icon" in a rule mean?

A. I have changed this rule
B. Someone else has changed this rule
C. This rule is managed by check point's SOC
D. This rule can't be changed as it's an implied rule

Answer: A

NEW QUESTION 147
Which Threat Prevention Profile is not included by default in R80 Management?

A. Basic – Provides reliable protection on a range of non-HTTP protocols for servers, with minimal impact on network performance
B. Optimized – Provides excellent protection for common network products and protocols against recent or popular attacks
C. Strict – Provides a wide coverage for all products and protocols, with impact on network performance
D. Recommended – Provides all protection for all common network products and servers, with impact on network performance

Answer: D

NEW QUESTION 149
Which part of SmartConsole allows administrators to add, edit delete, and clone objects?

A. Object Browser
B. Object Editor
C. Object Navigator
D. Object Explorer

Answer: D

NEW QUESTION 153
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

Answer: A

Explanation:
A policy package is a collection of different types of policies. After installation, the Security Gateway enforces all the policies in the package. A policy package can have one or more of these policy types:
The installation process:
If there are verification errors, the policy is not installed. If there are verification warnings (for example, if anti-spoofing is not enabled for a Security Gateway with multiple interfaces), the policy package is installed with a warning.

NEW QUESTION 157
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

Answer: D

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/T

NEW QUESTION 161
Which of the following is considered to be the more secure and preferred VPN authentication method?

A. Password
B. Certificate
C. MD5
D. Pre-shared secret

Answer: B

Explanation:
References:

NEW QUESTION 163
A stateful inspection firewall works by registering connection data and compiling this information. Where is the information stored?

A. In the system SMEM memory pool.
B. In State tables.
C. In the Sessions table.
D. In a CSV file on the firewall hard drive located in $FWDIR/conf/.

Answer: B

Explanation:
The information stored in the state tables provides cumulative data that can be used to evaluate future connections.....
https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/what-is-a-stateful-firewall/

NEW QUESTION 165
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

Answer: A

NEW QUESTION 168
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…'

Answer: D

Explanation:
From the Smartconsole, you can possibly view the changes via Manage & setting, Sessions

NEW QUESTION 171
What are the Threat Prevention software components available on the Check Point Security Gateway?

A. IPS, Threat Emulation and Threat Extraction
B. IPS, Anti-Bot, Anti-Virus, SandBlast and Macro Extraction
C. IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction
D. IDS, Forensics, Anti-Virus, Sandboxing

Answer: C

NEW QUESTION 174
Which of the following is used to extract state related information from packets and store that information in state tables?

A. STATE Engine
B. TRACK Engine
C. RECORD Engine
D. INSPECT Engine

Answer: D

Explanation:
Stateful Inspection, the packet is intercepted at the network layer, but then the INSPECT Engine takes over.
It extracts state-related information required for the security decision from all application layers and maintains this information in dynamic state tables for evaluating subsequent connection attempts.

NEW QUESTION 175
Which one of the following is a way that the objects can be manipulated using the new API integration in R80 Management?

A. Microsoft Publisher
B. JSON
C. Microsoft Word
D. RC4 Encryption

Answer: B

NEW QUESTION 180
In SmartConsole, on which tab are Permissions and Administrators defined?

A. Manage and Settings
B. Logs and Monitor
C. Security Policies
D. Gateways and Servers

Answer: A

NEW QUESTION 184
Which of the following describes how Threat Extraction functions?

A. Detect threats and provides a detailed report of discovered threats
B. Proactively detects threats
C. Delivers file with original content
D. Delivers PDF versions of original files with active content removed

Answer: B

NEW QUESTION 189
Which of the following commands is used to monitor cluster members?

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

Answer: A

NEW QUESTION 190
Which of the following is used to enforce changes made to a Rule Base?

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

Answer: A

NEW QUESTION 193
When configuring LDAP with User Directory integration, changes applied to a User Directory template are:

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

Answer: D

Explanation:
You can change the User Directory templates. Users associated with this template get the changes immediately. If you change user definitions manually in SmartConsole, the changes are immediate on the server.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 197
Where can administrator edit a list of trusted SmartConsole clients?

A. cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server.
B. In cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server, in SmartConsole: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients.
C. WebUI client logged to Security Management Server, SmartDashboard: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients, via cpconfig on a Security Gateway.
D. Only using SmartConsole: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients.

Answer: B

NEW QUESTION 200
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.

Answer: B

NEW QUESTION 202

Which tool is used to enable ClusterXL?

A. SmartUpdate
B. cpconfig
C. SmartConsole
D. sysconfig

Answer: B

NEW QUESTION 207
When should you generate new licenses?

A. Before installing contract files.
B. After a device upgrade.
C. When the existing license expires, license is upgraded or the IP-address associated with the license changes.
D. Only when the license is upgraded.

Answer: C

NEW QUESTION 209
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

Answer: B

NEW QUESTION 214
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

Answer: A

NEW QUESTION 216
When comparing Stateful Inspection and Packet Filtering, what is a benefit that Stateful Inspection offers over Packer Filtering?

A. Stateful Inspection offers unlimited connections because of virtual memory usage.
B. Stateful Inspection offers no benefits over Packet Filtering.
C. Stateful Inspection does not use memory to record the protocol used by the connection.
D. Only one rule is required for each connection.

Answer: D

NEW QUESTION 218
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

Answer: C

Explanation:
To establish the initial trust, a gateway and a Security Management Server use a one-time password. After the initial trust is established, further communication is based on security certificates.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 219
When an encrypted packet is decrypted, where does this happen?

A. Security policy
B. Inbound chain
C. Outbound chain
D. Decryption is not supported

Answer: A

NEW QUESTION 222
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 Serve
B. Log Servers are proprietary log archive servers.
C. 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.
D. The firewalls will detect the new Log Server after the next policy install and redirect the new logs to the new Log Server.
E. Logs are not automatically forwarded to a new Log Serve
F. SmartConsole must be used to manually configure each gateway to send its logs to the server.

Answer: D

Explanation:
https://sc1.checkpoint.com/documents/SMB_R80.20/AdminGuides/Locally_Managed/EN/Content/Topics/Conf
https://sc1.checkpoint.com/documents/SMB_R80.20/AdminGuides/Locally_Managed/EN/Content/Topics/Conf

NEW QUESTION 225
To quickly review when Threat Prevention signatures were last updated, which Threat Tool would an administrator use?

A. Protections
B. IPS Protections
C. Profiles
D. ThreatWiki

Answer: B

NEW QUESTION 226
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.

Answer: B

Explanation:
More than one administrator can connect to the Security Management Server at the same time. Every administrator has their own username, and works in a session that is independent of the other administrators.

NEW QUESTION 231
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.

Answer: D

NEW QUESTION 232
In the Check Point Security Management Architecture, which component(s) can store logs?

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

Answer: B

NEW QUESTION 235
Which type of attack can a firewall NOT prevent?

A. Network Bandwidth Saturation
B. Buffer Overflow
C. SYN Flood
D. SQL Injection

Answer: A

NEW QUESTION 238
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

Answer: B

NEW QUESTION 241
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

Answer: C

NEW QUESTION 242
The competition between stateful inspection and proxies was based on performance, protocol support, and security. Considering stateful Inspections and Proxies, which statement is correct?

A. Stateful Inspection is limited to Layer 3 visibility, with no Layer 4 to Layer 7 visibility capabilities.
B. When it comes to performance, proxies were significantly faster than stateful inspection firewalls.
C. Proxies offer far more security because of being able to give visibility of the payload (the data).
D. When it comes to performance, stateful inspection was significantly faster than proxies.

Answer: C

NEW QUESTION 244
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

Answer: C

NEW QUESTION 245
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

Answer: B

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T

NEW QUESTION 250
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

Answer: A

NEW QUESTION 251
A security zone is a group of one or more network interfaces from different centrally managed gateways. What is considered part of the zone?

A. The zone is based on the network topology and determined according to where the interface leads to.
B. Security Zones are not supported by Check Point firewalls.
C. The firewall rule can be configured to include one or more subnets in a zone.
D. The local directly connected subnet defined by the subnet IP and subnet mask.

Answer: A

Explanation:
The Interface window opens. The Topology area of the General pane shows the Security Zone to which the interface is already bound. By default, the Security Zone is calculated according to where the interface Leads To.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 253

Which of the following is NOT supported by Bridge Mode on the Check Point Security Gateway?

A. Data Loss Prevention
B. Antivirus
C. Application Control
D. NAT

Answer: D

Explanation:
NAT rules (specifically, Firewall kernel in logs shows the traffic as accepted, but Security Gateway does not actually forward it). For more information, see sk106146. https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/T

NEW QUESTION 258
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

Answer: A

NEW QUESTION 259
Which GUI tool can be used to view and apply Check Point licenses?

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

Answer: D

Explanation:
SmartUpdate GUI is the recommended way of managing licenses.

NEW QUESTION 260
Which of the following licenses are considered temporary?

A. Plug-and-play (Trial) and Evaluation
B. Perpetual and Trial
C. Evaluation and Subscription
D. Subscription and Perpetual

Answer: A

NEW QUESTION 262
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

Answer: A

NEW QUESTION 266
What object type would you use to grant network access to an LDAP user group?

A. Access Role
B. User Group
C. SmartDirectory Group
D. Group Template

Answer: B

NEW QUESTION 270
Which of the following Windows Security Events will NOT map a username to an IP address in Identity Awareness?

A. Kerberos Ticket Renewed
B. Kerberos Ticket Requested
C. Account Logon
D. Kerberos Ticket Timed Out

Answer: D

NEW QUESTION 271
Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?

A. Export R80 configuration, clean install R80.10 and import the configuration
B. CPUSE online upgrade
C. CPUSE offline upgrade
D. SmartUpdate upgrade

Answer: C

NEW QUESTION 272
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

Answer: B

NEW QUESTION 277
What key is used to save the current CPView page in a filename format cpview_"cpview process ID". cap"number of captures"?

A. S
B. W
C. C
D. Space bar

Answer: C

NEW QUESTION 281
Which of the following is NOT a role of the SmartCenter:

A. Status monitoring
B. Policy configuration
C. Certificate authority
D. Address translation

Answer: C

NEW QUESTION 284
An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server (SMS). While configuring the VPN community to specify the pre-shared secret, the administrator did not find a box to input the pre-shared secret. Why does it not allow him to specify the pre-shared secret?

A. The Gateway is an SMB device
B. The checkbox "Use only Shared Secret for all external members" is not checked
C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS
D. Pre-shared secret is already configured in Global Properties

Answer: C

NEW QUESTION 286
True or False: In a Distributed Environment, a Central License can be installed via CLI on a Security Gateway

A. True, CLI is the prefer method for Licensing
B. False, Central License are handled via Security Management Server
C. False, Central License are installed via Gaia on Security Gateways
D. True, Central License can be installed with CPLIC command on a Security Gateway

Answer: D

NEW QUESTION 289
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

Answer: A

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T

NEW QUESTION 291
Which Identity Source(s) should be selected in Identity Awareness for when there is a requirement for a higher level of security for sensitive servers?

A. AD Query
B. Terminal Servers Endpoint Identity Agent
C. Endpoint Identity Agent and Browser-Based Authentication
D. RADIUS and Account Logon

Answer: C

Explanation:
Endpoint Identity Agents and Browser-Based Authentication - When a high level of security is necessary.
Captive Portal is used for distributing the Endpoint Identity Agent. IP Spoofing protection can be set to prevent packets from being IP spoofed.

NEW QUESTION 293
When defining group-based access in an LDAP environment with Identity Awareness, what is the BEST object type to represent an LDAP group in a Security Policy?

A. Access Role
B. User Group
C. SmartDirectory Group
D. Group Template

Answer: A

NEW QUESTION 298
Fill in the blank: In order to install a license, it must first be added to the _____.

A. User Center
B. Package repository
C. Download Center Web site
D. License and Contract repository

Answer: B

NEW QUESTION 299
What is the most recommended installation method for Check Point appliances?

A. SmartUpdate installation
B. DVD media created with Check Point ISOMorphic
C. USB media created with Check Point ISOMorphic
D. Cloud based installation

Answer: C

NEW QUESTION 303
Which tool is used to enable cluster membership on a Gateway?

A. SmartUpdate
B. cpconfig
C. SmartConsole
D. sysconfig

Answer: B

Explanation:
References:

NEW QUESTION 306
Fill in the blank: Once a certificate is revoked from the Security GateWay by the Security Management Server, the certificate information is _____.

A. Sent to the Internal Certificate Authority.
B. Sent to the Security Administrator.
C. Stored on the Security Management Server.
D. Stored on the Certificate Revocation List.

Answer: D

NEW QUESTION 311
How many users can have read/write access in Gaia Operating System at one time?

A. One
B. Three
C. Two
D. Infinite

Answer: A

Explanation:
if another user has r/w access, you need to use "lock database override" or "unlock database" to claim r/w access. Ref:
https://sc1.checkpoint.com/documents/R80.20_GA/WebAdminGuides/EN/CP_R80.20_Gaia_AdminGuide/html

NEW QUESTION 312
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

Answer: A

NEW QUESTION 313
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

Answer: D

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/To

NEW QUESTION 315
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

Answer: B

Explanation:
https://community.checkpoint.com/t5/Management/Workaround-for-manual-NAT-when-security-zones-are-use

NEW QUESTION 319
Access roles allow the firewall administrator to configure network access according to:

A. remote access clients.
B. a combination of computer or computer groups and networks.
C. users and user groups.
D. All of the above.

Answer: D

Explanation:
To create an access role:
The Access Role window opens.
Your selection is shown in the Networks node in the Role Preview pane.
A window opens. You can search for Active Directory entries or select them from the list. You can search for AD entries or select them from the list.
The access role is added to the Users and Administrators tree.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 323
Fill in the blank: An Endpoint identity agent uses a _____ for user authentication.

A. Shared secret
B. Token
C. Username/password or Kerberos Ticket
D. Certificate

Answer: C

Explanation:
Two ways of auth: Username/Password in Captive Portal or Transparent Kerberos Auth through Kerberos Ticket.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T

NEW QUESTION 324
Which type of Check Point license is tied to the IP address of a specific Security Gateway and cannot be transferred to a gateway that has a different IP address?

A. Formal
B. Central
C. Corporate
D. Local

Answer: D

Explanation:
Local licensing is associated with the IP address of the Security Gateway, to which the license will be applied.
Each time the IP address of the Security Gateway changes, a new license must be generated and installed.
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW QUESTION 327
What are the three main components of Check Point security management architecture?

A. SmartConsole, Security Management, and Security Gateway
B. Smart Console, Standalone, and Security Management
C. SmartConsole, Security policy, and Logs & Monitoring
D. GUI-Client, Security Management, and Security Gateway

Answer: A

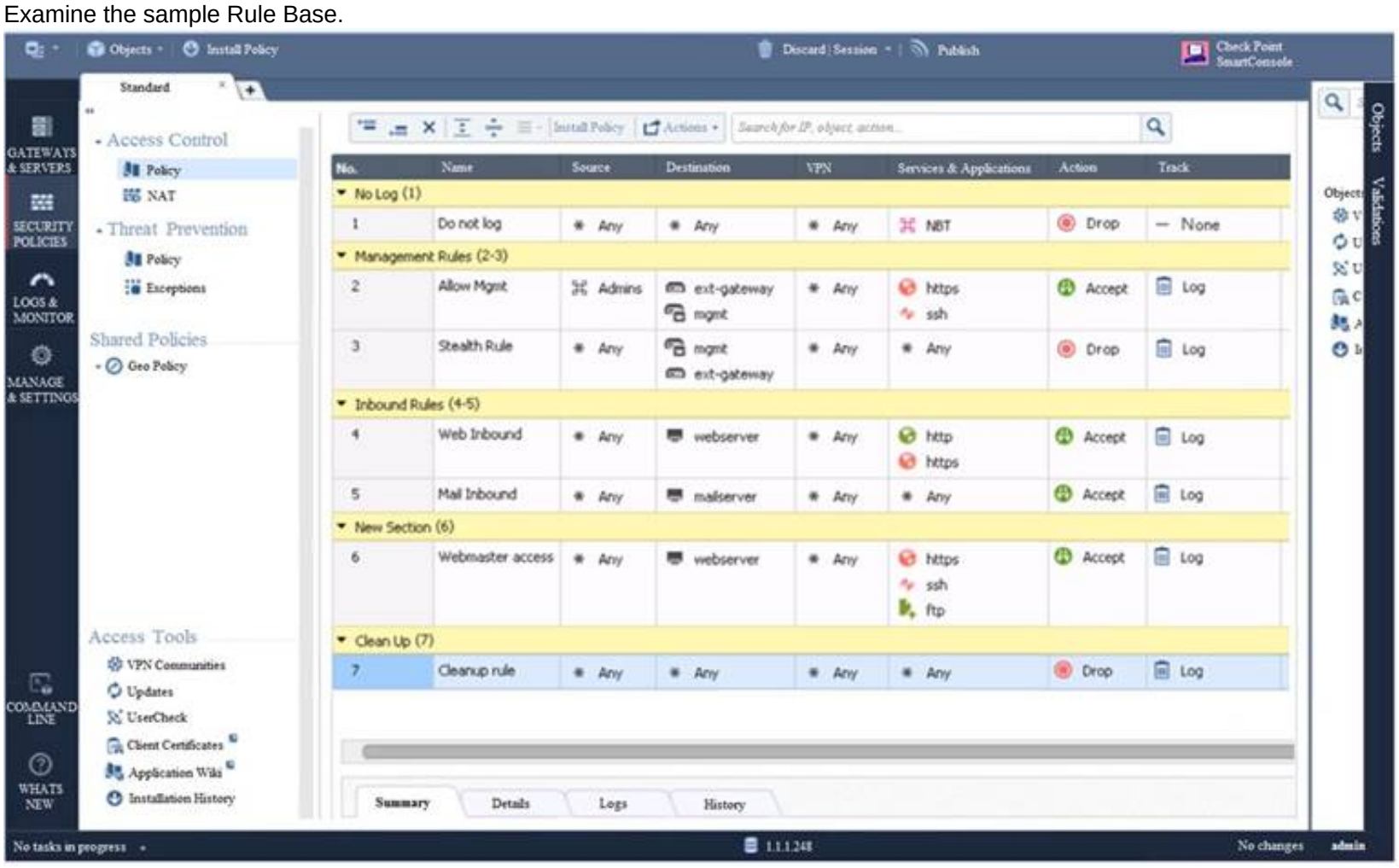
NEW QUESTION 331
Which is a main component of the Check Point security management architecture?

A. Identity Collector
B. Endpoint VPN client
C. SmartConsole
D. Proxy Server

Answer: C

Explanation:
https://community.checkpoint.com/t5/Check-Point-for-Beginners-2-0/Part-1-The-Architecture/ba-p/88043 Security Gateway (SG) is usually deployed on the perimeter to control and secure traffic with Firewall and
Threat Prevention capabilities.
Security Management Server (SMS) defines and controls security policies on the Gateways. It can also be used to as a log server with built-in system of log indexing (SmartLog) and event correlation (SmartEvent – a SIEM-like solution for Check Point products). Usually, SMS is the main element of central management with multiple Security Gateways in operation. Nevertheless, you need an SMS even if your security system has a single gateway only.
SmartConsole is a GUI administration tool to connect to SMS. Through this tool, a security administrator is able to prepare and apply security policies to the Security Gateways.

NEW QUESTION 332
Examine the sample Rule Base.



What will be the result of a verification of the policy from SmartConsole?

A. No errors or Warnings
B. Verification Erro
C. Empty Source-List in Rule 5 (Mail Inbound)
D. Verification Erro
E. Rule 4 (Web Inbound) hides Rule 6 (Webmaster access)

F. Verification Erro
G. Rule 7 (Clean-Up Rule) hides Implicit Clean-up Rule

Answer: C

NEW QUESTION 333
In SmartEvent, a correlation unit (CU) is used to do what?

A. Collect security gateway logs, Index the logs and then compress the logs.
B. Receive firewall and other software blade logs in a region and forward them to the primary log server.
C. Analyze log entries and identify events.
D. Send SAM block rules to the firewalls during a DOS attack.

Answer: C

Explanation:
https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_LoggingAndMonitoring_Ad

NEW QUESTION 338
You have created a rule at the top of your Rule Base to permit Guest Wireless access to the Internet. However, when guest users attempt to reach the Internet, they are not seeing the splash page to accept your Terms of Service, and cannot access the Internet. How can you fix this?

No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	0	Guest Access	GuestUsers	* Any	* Any	* Any	Accept	Log

A. Right click Accept in the rule, select “More”, and then check “Enable Identity Captive Portal”
B. On the firewall object, Legacy Authentication screen, check “Enable Identity Captive Portal”
C. In the Captive Portal screen of Global Properties, check “Enable Identity Captive Portal”
D. On the Security Management Server object, check the box “Identity Logging”

Answer: A

NEW QUESTION 342
SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

A. Smart Cloud Services
B. Load Sharing Mode Services
C. Threat Agent Solution
D. Public Cloud Services

Answer: A

NEW QUESTION 347
What is a role of Publishing?

A. The Publish operation sends the modifications made via SmartConsole in the private session and makes them public
B. The Security Management Server installs the updated policy and the entire database on Security Gateways
C. The Security Management Server installs the updated session and the entire Rule Base on Security Gateways
D. Modifies network objects, such as servers, users, services, or IPS profiles, but not the Rule Base

Answer: A

NEW QUESTION 350
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

Answer: B

Explanation:
Backup configurations are stored in: /var/CPbackup/backups/

NEW QUESTION 354
When using Monitored circuit VRRP, what is a priority delta?

A. When an interface fails the priority changes to the priority delta
B. When an interface fails the delta claims the priority
C. When an interface fails the priority delta is subtracted from the priority
D. When an interface fails the priority delta decides if the other interfaces takes over

Answer: C

NEW QUESTION 356
What is the difference between SSL VPN and IPSec VPN?

A. IPSec VPN does not require installation of a resident VPN client
B. SSL VPN requires installation of a resident VPN client
C. SSL VPN and IPSec VPN are the same
D. IPSec VPN requires installation of a resident VPN client and SSL VPN requires only an installed Browser

Answer: D

NEW QUESTION 358
What is NOT an advantage of Stateful Inspection?

A. High Performance
B. Good Security
C. No Screening above Network layer
D. Transparency

Answer: A

NEW QUESTION 361
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

Answer: B

NEW QUESTION 366
Which of the following is NOT a policy type available for each policy package?

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

Answer: A

Explanation:
References:

NEW QUESTION 367
Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?

A. Application Control
B. Threat Emulation
C. Anti-Virus
D. Advanced Networking Blade

Answer: B

NEW QUESTION 371
Which repositories are installed on the Security Management Server by SmartUpdate?

A. License and Update
B. Package Repository and Licenses
C. Update and License & Contract
D. License & Contract and Package Repository

Answer: D

Explanation:
References:

NEW QUESTION 372
The CDT utility supports which of the following?

A. Major version upgrades to R77.30
B. Only Jumbo HFA’s and hotfixes
C. Only major version upgrades to R80.10
D. All upgrades

Answer: D

NEW QUESTION 377
Phase 1 of the two-phase negotiation process conducted by IKE operates in _____ mode.

A. Main
B. Authentication
C. Quick
D. High Alert

Answer: A

Explanation:
Phase I modes
Between Security Gateways, there are two modes for IKE phase I. These modes only apply to IKEv1:

NEW QUESTION 379
Can you use the same layer in multiple policies or rulebases?

A. Yes - a layer can be shared with multiple policies and rules.
B. No - each layer must be unique.
C. No - layers cannot be shared or reused, but an identical one can be created.
D. Yes - but it must be copied and pasted with a different name.

Answer: A

Explanation:
https://community.checkpoint.com/t5/Management/Sharing-a-layer-across-different-policies/td-p/1660

NEW QUESTION 384
When installing a dedicated R80 SmartEvent server, what is the recommended size of the root partition?

A. Any size
B. Less than 20GB
C. More than 10GB and less than 20 GB
D. At least 20GB

Answer: D

NEW QUESTION 388
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

156-215.81 Practice Exam Features:

* 156-215.81 Questions and Answers Updated Frequently

* 156-215.81 Practice Questions Verified by Expert Senior Certified Staff

* 156-215.81 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 156-215.81 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year