CheckPoint

Exam Questions 156-215.81

Check Point Certified Security Administrator R81

NEW QUESTION 1
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

Answer: B

NEW QUESTION 2
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 3
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 4
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.

Answer: B

NEW QUESTION 5
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

Answer: C

NEW QUESTION 6
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

Answer: B

NEW QUESTION 7
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 8
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 9
Which of the following is an authentication method used for Identity Awareness?

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

Answer: B

NEW QUESTION 10
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 10
Which of the following is NOT a tracking log option in R80.x?

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

Answer: C

NEW QUESTION 11
To provide updated malicious data signatures to all Threat Prevention blades, the Threat Prevention gateway does what with the data?

A. Cache the data to speed up its own function.
B. Share the data to the ThreatCloud for use by other Threat Prevention blades.
C. Log the traffic for Administrator viewing.
D. Delete the data to ensure an analysis of the data is done each time.

Answer: B

Explanation:
Data from malicious attacks are shared between the Threat Prevention Software Blades and help to keep your network safe. For example, the signatures from

threats that Threat Emulation identifies are added to the ThreatCloud for use by the other Threat Prevention blades. src https://infosec.co.il/wp-content/uploads/2020/06/12-GAiA-R80.40-Threat-Prevention.pdf page 28.

NEW QUESTION 16
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 17
When a SAM rule is required on Security Gateway to quickly block suspicious connections which are not restricted by the Security Policy, what actions does the administrator need to take?

A. SmartView Monitor should be opened and then the SAM rule/s can be applied immediatel
B. Installing policy is not required.
C. The policy type SAM must be added to the Policy Package and a new SAM rule must be applied.Simply Publishing the changes applies the SAM rule on the firewall.
D. The administrator must work on the firewall CLI (for example with SSH and PuTTY) and the command 'sam block' must be used with the right parameters.
E. The administrator should open the LOGS & MONITOR view and find the relevant lo
F. Right clicking on the log entry will show the Create New SAM rule option.

Answer: A

Explanation:
A Security GatewayClosed with SAM enabled has Firewall rules to block suspicious connections that are not restricted by the security policyClosed. These rules are applied immediately (policy installation is not required).
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu

NEW QUESTION 18
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 23
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 25
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 29

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 33
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 37
In Unified SmartConsole Gateways and Servers tab you can perform the following functions EXCEPT _____.

A. Upgrade the software version
B. Open WebUI
C. Open SSH
D. Open service request with Check Point Technical Support

Answer: C

NEW QUESTION 41
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 43
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 48
Which command shows the installed licenses?

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

Answer: A

NEW QUESTION 49
How do logs change when the "Accounting" tracking option is enabled on a traffic rule?

A. Involved traffic logs will be forwarded to a log server.
B. Provides log details view email to the Administrator.
C. Involved traffic logs are updated every 10 minutes to show how much data has passed on the connection.
D. Provides additional information to the connected user.

Answer: C

Explanation:
Accounting - Select this to update the log at 10 minutes intervals, to show how much data has passed in the connection: Upload bytes, Download bytes, and browse time. https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu

NEW QUESTION 51
Which two Identity Awareness daemons are used to support identity sharing?

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

Answer: D

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

NEW QUESTION 52
The _____ software blade package uses CPU-level and OS-level sandboxing in order to detect and block malware.

A. Next Generation Threat Prevention
B. Next Generation Threat Emulation
C. Next Generation Threat Extraction
D. Next Generation Firewall

Answer: B

NEW QUESTION 55
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

Answer: B

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

NEW QUESTION 58
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 59
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 62
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 64
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 69
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.

Answer: D

NEW QUESTION 70
What data MUST be supplied to the SmartConsole System Restore window to restore a backup?

A. Server, Username, Password, Path, Version
B. Username, Password, Path, Version
C. Server, Protocol, Username, Password, Destination Path
D. Server, Protocol, Username, Password, Path

Answer: D

Explanation:
References:

NEW QUESTION 71
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 76
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

Answer: C

NEW QUESTION 79
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 82
Where is the “Hit Count” feature enabled or disabled in SmartConsole?

A. On the Policy Package
B. On each Security Gateway
C. On the Policy layer
D. In Global Properties for the Security Management Server

Answer: B

Explanation:
References:

NEW QUESTION 83
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 86
What Identity Agent allows packet tagging and computer authentication?

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

Answer: B

Explanation:
Identity Agent Description Full
Default Identity AgentClosed that includes packet tagging and computer authentication. It applies to all users on the computer on which it is installed.
Administrator permissions are required to use the Full Identity Agent type. For the Full Identity Agent, you can enforce IP spoofing protection. In addition, you can leverage computer authentication if you specify computers in Access Roles.
Light
Default Identity Agent that does not include packet tagging and computer authentication. You can install this Identity Agent individually for each user on the target computer. Light Identity Agent type does not require Administrator permissions.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T

NEW QUESTION 91
Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older?

A. The rule base can be built of layers, each containing a set of the security rule
B. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
C. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
D. Time object to a rule to make the rule active only during specified times.
E. Sub Policies are sets of rules that can be created and attached to specific rule
F. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule.

Answer: D

NEW QUESTION 94
What is true about the IPS-Blade?

A. in R80, IPS is managed by the Threat Prevention Policy
B. in R80, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
C. in R80, IPS Exceptions cannot be attached to "all rules"
D. in R80, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same

Answer: A

NEW QUESTION 98
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.

Answer: A

Explanation:
The users and user groups are arranged on the Account Unit in the tree structure of the LDAP server. User management in User Directory is external, not local. You can change the User Directory templates. Users associated with this template get the changes immediately. You can change user definitions manually in

SmartDashboard, and the changes are immediate on the server.

NEW QUESTION 102
Which type of Check Point license ties the package license to the IP address of the Security Management Server?

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

Answer: A

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

NEW QUESTION 107
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 110
Which option will match a connection regardless of its association with a VPN community?

A. All Site-to-Site VPN Communities
B. Accept all encrypted traffic
C. All Connections (Clear or Encrypted)
D. Specific VPN Communities

Answer: B

NEW QUESTION 111
In _____ NAT, the _____ is translated.

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

Answer: A

NEW QUESTION 115
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.

Answer: D

Explanation:
https://supportcenter.checkpoint.com/supportcenter/portal?action=portlets.SearchResultMainAction&eventSubm

NEW QUESTION 116
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 119
What is the purpose of a Stealth Rule?

A. A rule used to hide a server's IP address from the outside world.
B. A rule that allows administrators to access SmartDashboard from any device.
C. To drop any traffic destined for the firewall that is not otherwise explicitly allowed.
D. A rule at the end of your policy to drop any traffic that is not explicitly allowed.

Answer: C

NEW QUESTION 121
How would you determine the software version from the CLI?

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

Answer: A

NEW QUESTION 125
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 130
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 135
What are the three components for Check Point Capsule?

A. Capsule Docs, Capsule Cloud, Capsule Connect
B. Capsule Workspace, Capsule Cloud, Capsule Connect
C. Capsule Workspace, Capsule Docs, Capsule Connect
D. Capsule Workspace, Capsule Docs, Capsule Cloud

Answer: D

NEW QUESTION 138
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 143
Which tool is used to enable ClusterXL?

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

Answer: B

NEW QUESTION 145

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.

Answer: C

Explanation:
"Online activation: this method of activation is available for Check Point manufactured appliances. These appliances should be configured to have internet connectivity during the completion of the First Time Configuration Wizard for software version R77 and below. Customers using R80 and higher will be able to use this feature during or after the completion of the First Time Configuration Wizard."
https://supportcenter.checkpoint.com/supportcenter/portal?eventsubmit_dogoviewsolutiondetails=&solutionid=s

NEW QUESTION 146
What is the RFC number that act as a best practice guide for NAT?

A. RFC 1939
B. RFC 1950
C. RFC 1918
D. RFC 793

Answer: C

Explanation:
https://datatracker.ietf.org/doc/html/rfc1918

NEW QUESTION 150
When a Security Gateways sends its logs to an IP address other than its own, which deployment option is installed?

A. Distributed
B. Standalone
C. Bridge

Answer: A

NEW QUESTION 154
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 159
Which of the following is NOT a valid deployment option for R80?

A. All-in-one (stand-alone)
B. Log server
C. SmartEvent
D. Multi-domain management server

Answer: D

NEW QUESTION 161
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

Answer: A

Explanation:
Inform User Inform
Shows when the action for the ruleClosed is inform. It informs users what the company policy is for that site. Blocked Message
Block
Shows when a request is blocked. Ask User
Ask
Shows when the action for the rule is ask. It informs users what the company policy is for that site and they must click OK to continue to the site.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_DataLossPrevention_AdminGuide/

NEW QUESTION 162
To view the policy installation history for each gateway, which tool would an administrator use?

A. Revisions
B. Gateway installations
C. Installation history
D. Gateway history

Answer: C

NEW QUESTION 167
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

Answer: A

Explanation:
There are three types of Software Containers: Security Management, Security Gateway, and Endpoint Security.

NEW QUESTION 171
Which Threat Prevention profile uses sanitization technology?

A. Cloud/data Center
B. perimeter
C. Sandbox
D. Guest Network

Answer: B

Explanation:
Strict Security for Perimeter Profile & Perimeter Profile use sanitization as a technology in Threat prevention profile

NEW QUESTION 172
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 177
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 181
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 183
In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?

A. SND is a feature to accelerate multiple SSL VPN connections
B. SND is an alternative to IPSec Main Mode, using only 3 packets
C. SND is used to distribute packets among Firewall instances
D. SND is a feature of fw monitor to capture accelerated packets

Answer: C

NEW QUESTION 185
What Check Point technologies deny or permit network traffic?

A. Application Control, DLP
B. Packet Filtering, Stateful Inspection, Application Layer Firewall.
C. ACL, SandBlast, MPT
D. IPS, Mobile Threat Protection

Answer: B

NEW QUESTION 188
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

Answer: D

NEW QUESTION 193
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

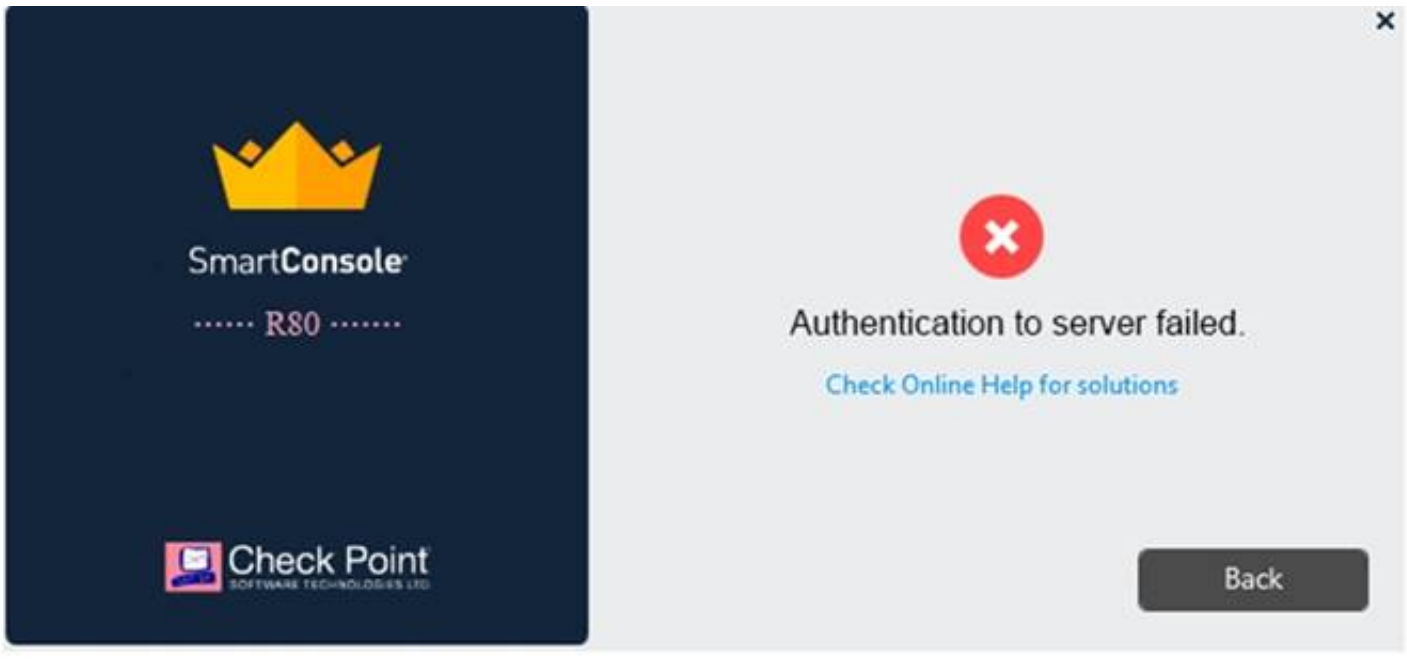
NEW QUESTION 196
DLP and Geo Policy are examples of what type of Policy?

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

Answer: B

Explanation:
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_NextGenSecurityGateway_G

NEW QUESTION 200
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 SmartConsol
B. Check that the correct key details are used.
C. Check Point Management software authentication details are not automatically the same as the Operating System authentication detail
D. Check that she is using the correct details.
E. SmartConsole Authentication is not allowed for Vanessa until a Super administrator has logged in first and cleared any other administrator sessions.
F. Authentication failed because Vanessa's username is not allowed in the new Threat Prevention console update checks even though these checks passed with Gaia.

Answer: B

NEW QUESTION 204
A Check Point Software license consists of two components, the Software Blade and the Software Container. There are _____ types of Software Containers: _____ .

A. Two; Security Management and Endpoint Security
B. Two; Endpoint Security and Security Gateway
C. Three; Security Management, Security Gateway, and Endpoint Security
D. Three; Security Gateway, Endpoint Security, and Gateway Management

Answer: C

Explanation:
There are three types of Software Containers: Security Management, Security Gateway, and Endpoint Security. Ref: https://downloads.checkpoint.com/dc/download.htm?ID=11608

NEW QUESTION 208
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 213
Identity Awareness allows easy configuration for network access and auditing based on what three items?

A. Client machine IP address.
B. Network location, the identity of a user and the identity of a machine.
C. Log server IP address.
D. Gateway proxy IP address.

Answer: B

NEW QUESTION 218
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 222
When a Security Gateway sends its logs to an IP address other than its own, which deployment option is installed?

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

Answer: A

NEW QUESTION 227
Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

A. UDP port 265
B. TCP port 265
C. UDP port 256

D. TCP port 256

Answer: B

NEW QUESTION 230
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

Answer: A

NEW QUESTION 231
Which method below is NOT one of the ways to communicate using the Management API's?

A. Typing API commands using the "mgmt_cli" command
B. Typing API commands from a dialog box inside the SmartConsole GUI application
C. Typing API commands using Gaia's secure shell (clash)19+
D. Sending API commands over an http connection using web-services

Answer: D

NEW QUESTION 233
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

Answer: B

Explanation:
The network topology represents the internal network (both the LAN and the DMZ) protected by the gateway. The gateway must be aware of the layout of the network topology to:

NEW QUESTION 238
What are the three deployment options available for a security gateway?

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

Answer: A

Explanation:
https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/86429.htm

NEW QUESTION 242
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 245
What command from the CLI would be used to view current licensing?

A. license view
B. fw ctl tab -t license -s
C. show license -s
D. cplic print

Answer: D

NEW QUESTION 249
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 252
Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster.

A. Symmetric routing
B. Failovers
C. Asymmetric routing
D. Anti-Spoofing

Answer: B

NEW QUESTION 253
Which firewall daemon is responsible for the FW CLI commands?

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

Answer: A

NEW QUESTION 255
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 256
Fill in the blank: It is Best Practice to have a _____ rule at the end of each policy layer.

A. Explicit Drop
B. Implied Drop
C. Explicit CleanUp
D. Implicit Drop

Answer: C

NEW QUESTION 260
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 265
In which deployment is the security management server and Security Gateway installed on the same appliance?

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

Answer: A

Explanation:
https://www.youtube.com/watch?v=BFNnBKQz5HA

NEW QUESTION 269
In order for changes made to policy to be enforced by a Security Gateway, what action must an administrator perform?

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

Answer: C

NEW QUESTION 273
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 277
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.

Answer: C

Explanation:
SIC Status
After the gateway receives the certificate issued by the ICA, the SIC status shows if the Security Management Server can communicate securely with this gateway:

NEW QUESTION 279
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 281
Which of the following is NOT an identity source used for Identity Awareness?

A. Remote Access
B. UserCheck
C. AD Query
D. RADIUS

Answer: B

NEW QUESTION 286
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 291
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

Answer: B

NEW QUESTION 295
Which of the following is NOT an advantage to using multiple LDAP servers?

A. You achieve a faster access time by placing LDAP servers containing the database at remote sites
B. You achieve compartmentalization by allowing a large number of users to be distributed across several servers
C. Information on a user is hidden, yet distributed across several servers.
D. You gain High Availability by replicating the same information on several servers

Answer: C

NEW QUESTION 299
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 304
Fill in the blanks: A _____ license requires an administrator to designate a gateway for attachment whereas a _____ license is automatically attached to a Security Gateway.

A. Formal; corporate
B. Local; formal
C. Local; central
D. Central; local

Answer: D

NEW QUESTION 308
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 311
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)

Answer: B

NEW QUESTION 313
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

Answer: B

Explanation:
Shared Policies
The Shared Policies section in the Security Policies shows the policies that are not in a Policy package. T are shared between all Policy packages.

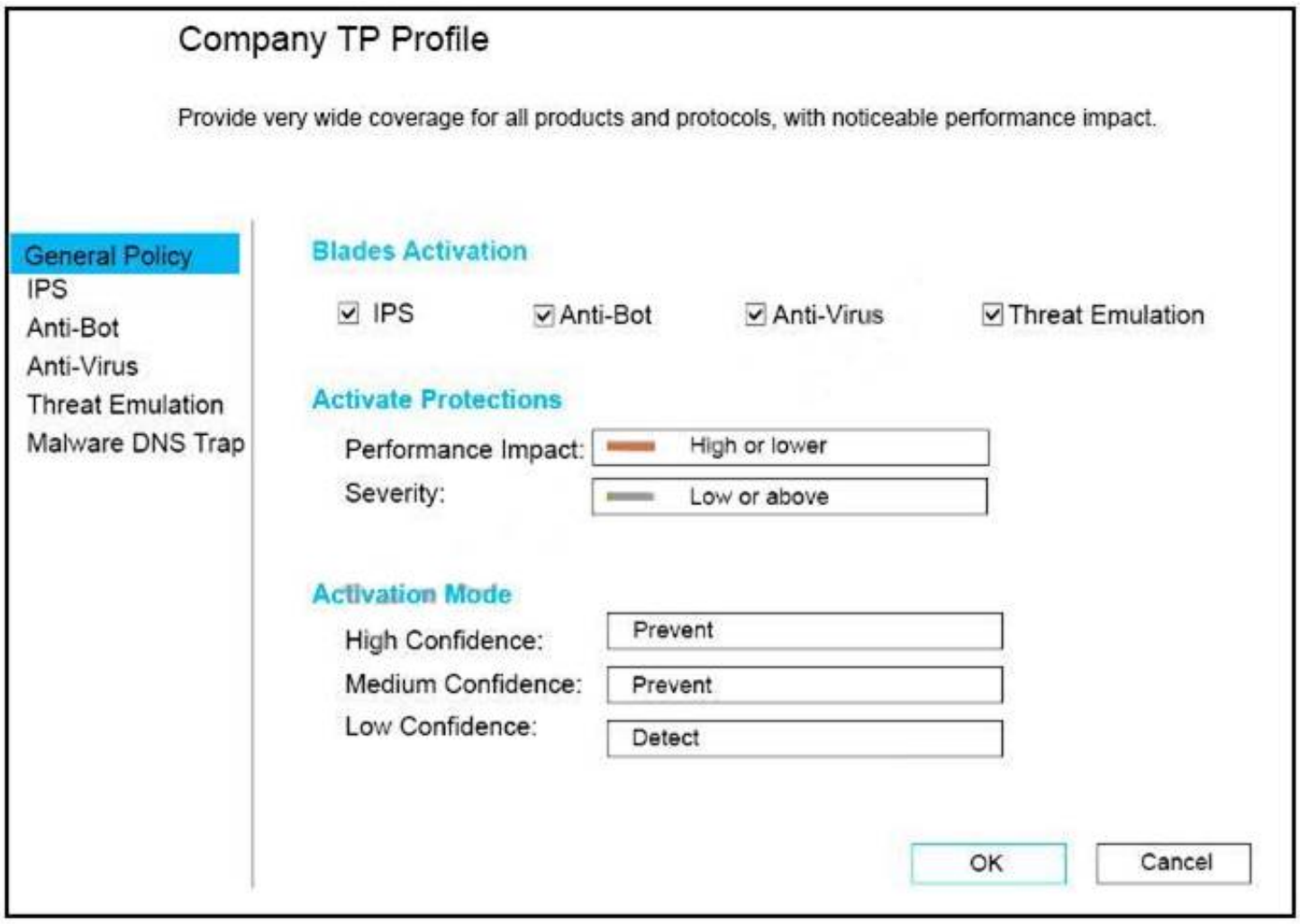
Shared policies are installed with the Access Control Policy. Software Blade
Description Mobile Access
Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile.
DLP
Launch Data Loss Prevention policy in a SmartConsole. Configure advanced tools to automatically identify data that must not go outside the network, to block the leak, and to educate users.
Geo Policy
Create a policy for traffic to or from specific geographical or political locations.

NEW QUESTION 314
Identity Awareness allows the Security Administrator to configure network access based on which of the following?

A. Name of the application, identity of the user, and identity of the machine
B. Identity of the machine, username, and certificate
C. Network location, identity of a user, and identity of a machine
D. Browser-Based Authentication, identity of a user, and network location

Answer: C

NEW QUESTION 317
CPU-level of your Security gateway is peaking to 100% causing problems with traffic. You suspect that the problem might be the Threat Prevention settings.
The following Threat Prevention Profile has been created.



How could you tune the profile in order to lower the CPU load still maintaining security at good level? Select the BEST answer.

A. Set High Confidence to Low and Low Confidence to Inactive.
B. Set the Performance Impact to Medium or lower.
C. The problem is not with the Threat Prevention Profil
D. Consider adding more memory to the appliance.
E. Set the Performance Impact to Very Low Confidence to Prevent.

Answer: B

NEW QUESTION 322
What is the default shell of Gaia CLI?

A. clish
B. Monitor
C. Read-only
D. Bash

Answer: A

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

NEW QUESTION 326
Fill in the blank: Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or _____.

A. On all satellite gateway to satellite gateway tunnels

B. On specific tunnels for specific gateways
C. On specific tunnels in the community
D. On specific satellite gateway to central gateway tunnels

Answer: C

Explanation:
Each VPN tunnel in the community may be set to be a Permanent Tunnel. Since Permanent Tunnels are constantly monitored, if the VPN tunnel is down, then a log, alert, or user defined action, can be issued. A VPN tunnel is monitored by periodically sending "tunnel test" packets. As long as responses to the packets are received the VPN tunnel is considered "up." If no response is received within a given time period, the VPN tunnel is considered "down." Permanent Tunnels can only be established between Check Point Security Gateways. The configuration of Permanent Tunnels takes place on the community level and:

NEW QUESTION 329
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 333
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 338
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 339
True or False: More than one administrator can log into the Security Management Server with SmartConsole with write permission at the same time.

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

Answer: C

Explanation:
Multiple R/W admins can log into SmartConsole and edit rules but they can't edit a rule that is being worked on by another admin.

NEW QUESTION 342
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 346
You have enabled "Extended Log" as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

A. Identity Awareness is not enabled.
B. Log Trimming is enabled.
C. Logging has disk space issues
D. Content Awareness is not enabled.

Answer: D

NEW QUESTION 347

.....

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