Exam Questions 156-215.81

Check Point Certified Security Administrator R81

https://www.2passeasy.com/dumps/156-215.81/

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
An administrator wishes to enable Identity Awareness on the Check Point firewalls. However they allow users to use company issued or personal laptops. Since the administrator cannot manage the personal laptops, which of the following methods would BEST suit this company?

A. AD Query
B. Browser-Based Authentication
C. Identity Agents
D. Terminal Servers Agent

Answer: B

NEW QUESTION 3
What is the purpose of the Stealth Rule?

A. To prevent users from directly connecting to a Security Gateway.
B. To reduce the number of rules in the database.
C. To reduce the amount of logs for performance issues.
D. To hide the gateway from the Internet.

Answer: A

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
What does it mean if Deyra sees the gateway status:

Status	Name	IP	Versi...	Active Bla...
❌	A-GW	10.1.1.1	R80	
✅	SMS	10.1.1.101	R80	

Choose the BEST answer.

A. SmartCenter Server cannot reach this Security Gateway
B. There is a blade reporting a problem
C. VPN software blade is reporting a malfunction
D. Security Gateway's MGNT NIC card is disconnected.

Answer: B

Explanation:

NEW QUESTION 6
In a Distributed deployment, the Security Gateway and the Security Management software are installed on what platforms?

A. Different computers or appliances.
B. The same computer or appliance.
C. Both on virtual machines or both on appliances but not mixed.
D. In Azure and AWS cloud environments.

Answer: A

Explanation:
"The Security Management ServerClosed (1) and the Security GatewayClosed (3) are installed on different computers, with a network connection (2)."
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/T

NEW QUESTION 7
Which of the following is NOT a component of Check Point Capsule?

A. Capsule Docs
B. Capsule Cloud
C. Capsule Enterprise
D. Capsule Workspace

Answer: C

NEW QUESTION 8
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 9
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 10
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 10
Fill in the bank: In Office mode, a Security Gateway assigns a remote client to an IP address once _____ .

A. the user connects and authenticates
B. office mode is initiated
C. the user requests a connection
D. the user connects

Answer: A

Explanation:
Office Mode enables a Security Gateway to assign a remote client an IP address. The assignment takes place once the user connects and authenticates. The assignment lease is renewed as long as the user is connected.

NEW QUESTION 13
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 16
What is the purpose of the CPCA process?

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

Answer: D

NEW QUESTION 21
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 22
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 23
From the Gaia web interface, which of the following operations CANNOT be performed on a Security Management Server?

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

Answer: B

NEW QUESTION 27
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 29
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 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 34
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 35
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 39
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 41
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 43
Identify the ports to which the Client Authentication daemon listens on by default?

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

Answer: A

NEW QUESTION 44
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 49
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 54
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 56
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 57
Which command shows the installed licenses?

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

Answer: A

NEW QUESTION 59
Both major kinds of NAT support Hide and Static NAT. However, one offers more flexibility. Which statement is true?

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

Answer: A

Explanation:
"An Auto-NAT rule only uses the source address and port when matching and translating. Manual NAT can match and translate source and destination addresses and ports." https://networkdirection.net/articles/firewalls/firepowermanagementcentre/fmcnatpolicies/

NEW QUESTION 61
Can multiple administrators connect to a Security Management Server at the same time?

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

Answer: C

NEW QUESTION 62
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 67
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 68
Check Point licenses come in two forms. What are those forms?

A. Central and Local.
B. Access Control and Threat Prevention.
C. On-premise and Public Cloud.
D. Security Gateway and Security Management.

Answer: A

NEW QUESTION 71
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 75
In order to see real-time and historical graph views of Security Gateway statistics in SmartView Monitor, what feature needs to be enabled on the Security Gateway?

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

Answer: C

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

NEW QUESTION 76
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 81
What is the default tracking option of a rule?

A. Tracking
B. Log
C. None
D. Alert

Answer: B

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

---

NEW QUESTION 84
Stateful Inspection compiles and registers connections where?

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

Answer: C

NEW QUESTION 89
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 91
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 94
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 96
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 98
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 99
Which Check Point software blade provides Application Security and identity control?

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

Answer: D

Explanation:
Check Point Application Control provides the industry's strongest application security and identity control to organizations of all sizes.

NEW QUESTION 103
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 106
What SmartEvent component creates events?

A. Consolidation Policy
B. Correlation Unit
C. SmartEvent Policy
D. SmartEvent GUI

Answer: B

NEW QUESTION 110
Which SmartConsole tab shows logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

A. Gateway and Servers
B. Logs and Monitor
C. Manage Seeting
D. Security Policies

Answer: B

NEW QUESTION 113
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 115
How many layers make up the TCP/IP model?

A. 2
B. 7
C. 6
D. 4

Answer: D

NEW QUESTION 120
If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss.
Providing the Active Security Management Server is responsible, which of these steps should NOT be performed:

A. Rename the hostname of the Standby member to match exactly the hostname of the Active member.
B. Change the Standby Security Management Server to Active.
C. Change the Active Security Management Server to Standby.
D. Manually synchronize the Active and Standby Security Management Servers.

Answer: A

NEW QUESTION 125
The "Hit count" feature allows tracking the number of connections that each rule matches. Will the Hit count feature work independently from logging and Track the hits even if the Track option is set to "None"?

A. No, it will not work independentl
B. Hit Count will be shown only for rules with Track options set as Log or alert
C. Yes, it will work independently as long as "analyze all rules" tick box is enabled on the Security Gateway
D. No, it will not work independently because hit count requires all rules to be logged
E. Yes, it will work independently because when you enable Hit Count, the SMS collects the data from supported Security Gateways

Answer: D

NEW QUESTION 128
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 132
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 135
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 138
Fill in the blank: Each cluster, at a minimum, should have at least _____ interfaces.

A. Five
B. Two
C. Three
D. Four

Answer: C

NEW QUESTION 143
R80.10 management server can manage gateways with which versions installed?

A. Versions R77 and higher
B. Versions R76 and higher
C. Versions R75.20 and higher
D. Version R75 and higher

Answer: B

NEW QUESTION 146
What needs to be configured if the NAT property 'Translate destination on client side' is not enabled in Global properties?

A. A host route to route to the destination IP
B. Use the file local.arp to add the ARP entries for NAT to work
C. Nothing, the Gateway takes care of all details necessary
D. Enabling 'Allow bi-directional NAT' for NAT to work correctly

Answer: C

NEW QUESTION 147
What is the BEST command to view configuration details of all interfaces in Gaia CLISH?

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

Answer: D

NEW QUESTION 150
Application Control/URL filtering database library is known as:

A. Application database
B. AppWiki
C. Application-Forensic Database
D. Application Library

Answer: B

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

NEW QUESTION 153
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 158
When dealing with rule base layers, what two layer types can be utilized?

A. Ordered Layers and Inline Layers
B. Inbound Layers and Outbound Layers
C. R81.10 does not support Layers
D. Structured Layers and Overlap Layers

Answer: A

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

NEW QUESTION 159
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 161
To ensure that VMAC mode is enabled, which CLI command you should run on all cluster members? Choose the best answer.

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

Answer: B

NEW QUESTION 165
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 167
What kind of NAT enables Source Port Address Translation by default?

A. Automatic Static NAT
B. Manual Hide NAT
C. Automatic Hide NAT
D. Manual Static NAT

Answer: C

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

NEW QUESTION 169
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 174
Which tool is used to enable ClusterXL?

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

Answer: B

NEW QUESTION 176
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 178
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 182
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 184
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 185
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 187
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 188
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 189
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 193
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 196
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 198
DLP and Geo Policy are examples of what type of Policy?

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

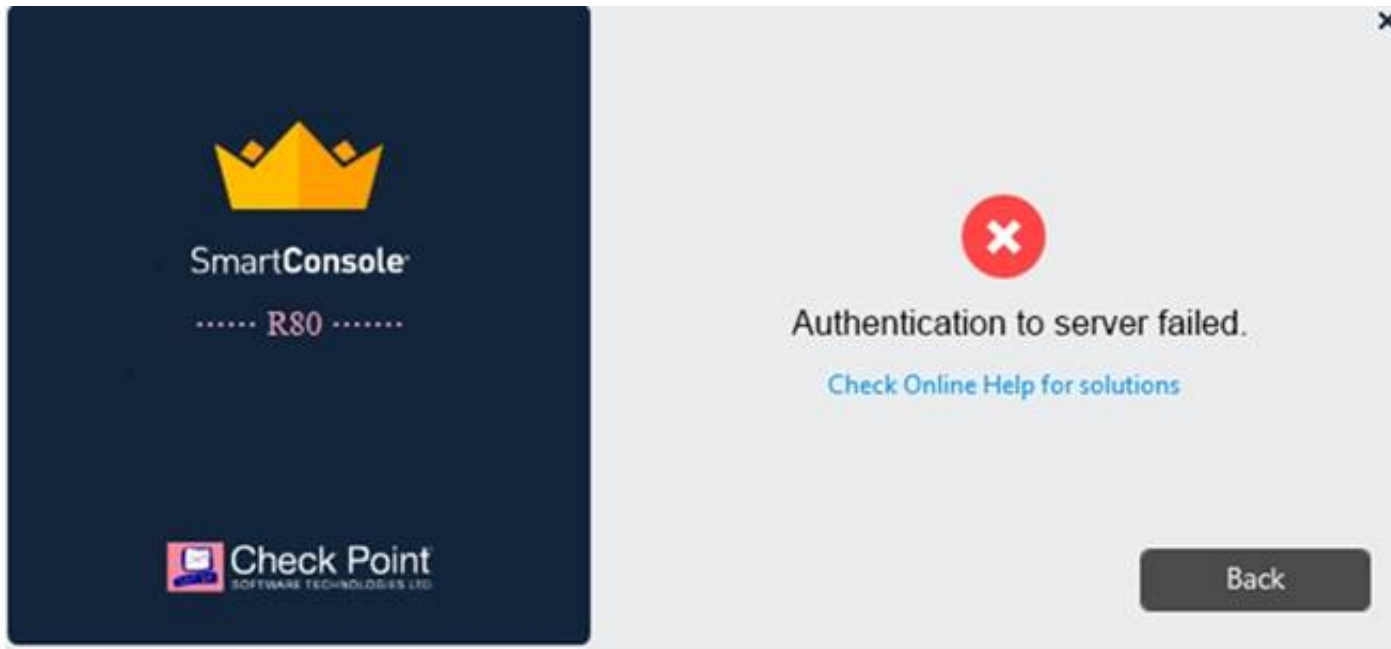**Answer:** B

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

NEW QUESTION 203
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 206
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 210
Which statement is TRUE of anti-spoofing?

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

Answer: C

NEW QUESTION 215
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 219
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 222
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 225
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 229
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 231
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 236
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 238
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 241
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 243
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 244
When should you generate new licenses?

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

Answer: C

NEW QUESTION 246
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 250
Which default Gaia user has full read/write access?

A. admin
B. superuser
C. monitor
D. altuser

Answer: A

Explanation:
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.

NEW QUESTION 253
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 257
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 262
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 266
Fill in the blank: SmartConsole, SmartEvent GUI client, and _____ allow viewing of billions of consolidated logs and shows them as prioritized security events.

A. SmartView Web Application
B. SmartTracker
C. SmartMonitor
D. SmartReporter

Answer: A

Explanation:
"The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartConsole, SmartView Web Application, and the SmartEvent GUI client consolidate billions of logs and show them as prioritized security events so you can immediately respond to security incidents"
https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=docume

NEW QUESTION 269
What is the main objective when using Application Control?

A. To filter out specific content.
B. To assist the firewall blade with handling traffic.
C. To see what users are doing.
D. Ensure security and privacy of information.

Answer: A

Explanation:
https://www.checkpoint.com/cyber-hub/network-security/what-is-application-control/

NEW QUESTION 272
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 274
When logging in for the first time to a Security management Server through SmartConsole, a fingerprint is saved to the:

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

Answer: D

NEW QUESTION 279
Security Gateway software blades must be attached to what?

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

Answer: B

Explanation:
Security Management and Security Gateway Software Blades must be attached to a Software Container to be licensed.
https://downloads.checkpoint.com/dc/download.htm?ID=11608

NEW QUESTION 284
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 286
Which of the following methods can be used to update the trusted log server regarding the policy and configuration changes performed on the Security Management Server?

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

Answer: D

NEW QUESTION 288
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 292
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 296
What protocol is specifically used for clustered environments?

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

Answer: D

NEW QUESTION 299
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 301
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 303
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
What are the three deployment considerations for a secure network?

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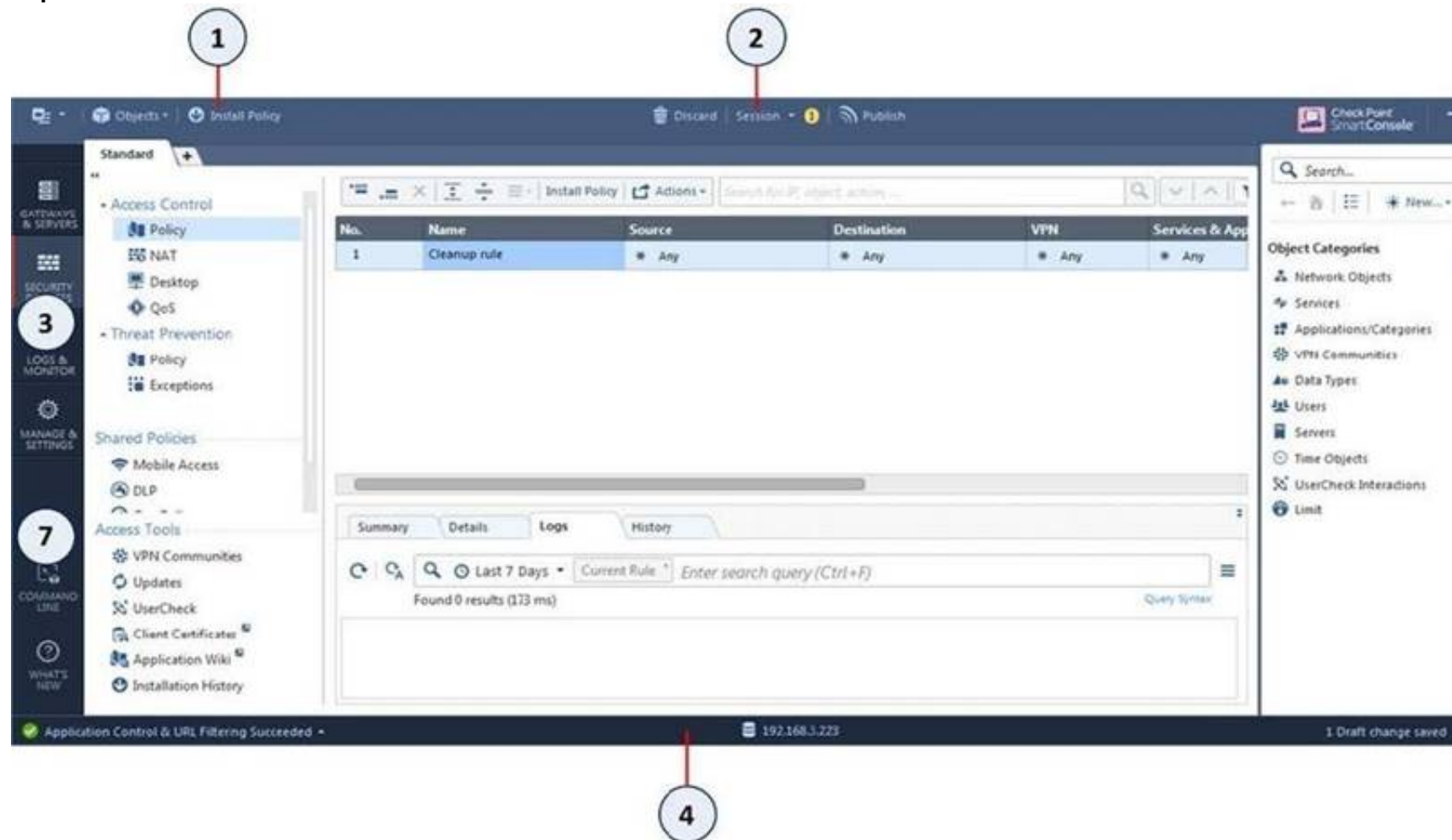D. Standalone, Distributed, and Bridge Mode

Answer: A

NEW QUESTION 307
Which of the following is NOT a valid application navigation tab in the R80 SmartConsole?

A. Manage and Command Line
B. Logs and Monitor
C. Security Policies
D. Gateway and Servers

Answer: A

Explanation:

Item	Description	Item	Description
1	Global Toolbar	5	Objects Bar (F11)
2	Session Management Toolbar	6	Validations pane
3	Navigation Toolbar	7	Command line interface button
4	System Information Area		

NEW QUESTION 308
Which SmartConsole tab is used to monitor network and security performance?

A. Manage & Settings
B. Security Policies
C. Gateway & Servers
D. Logs & Monitor

Answer: D

NEW QUESTION 310
What is the main difference between Threat Extraction and Threat Emulation?

A. Threat Emulation never delivers a file and takes more than 3 minutes to complete
B. Threat Extraction always delivers a file and takes less than a second to complete
C. Threat Emulation never delivers a file that takes less than a second to complete
D. Threat Extraction never delivers a file and takes more than 3 minutes to complete

Answer: B

NEW QUESTION 313
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 315
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 317
Which statement describes what Identity Sharing is in Identity Awareness?

A. Management servers can acquire and share identities with Security Gateways
B. Users can share identities with other users
C. Security Gateways can acquire and share identities with other Security Gateways
D. Administrators can share identifies with other administrators

Answer: C

Explanation:
 Identity Sharing
Best Practice - In environments that use many Security Gateways and AD Query, we recommend that you set only one Security Gateway to acquire identities from a given Active Directory domain controller for each physical site. If more than one Security Gateway gets identities from the same AD server, the AD server can become overloaded with WMI queries.
Set these options on the Identity Awareness > Identity Sharing page of the Security Gateway object:

NEW QUESTION 320
Which of the following is NOT an option to calculate the traffic direction?

A. Incoming
B. Internal
C. External
D. Outgoing

Answer: D

NEW QUESTION 325
The purpose of the Communication Initialization process is to establish a trust between the Security Management Server and the Check Point gateways. Which statement best describes this Secure Internal
Communication (SIC)?

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

Answer: A

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

NEW QUESTION 329
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 334
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 339
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 342
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 346
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 347
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 352
You want to store the GAiA configuration in a file for later reference. What command should you use?

A. write mem <filename>
B. show config -f <filename>
C. save config -o <filename>
D. save configuration <filename>

Answer: D

NEW QUESTION 355
Fill in the blank: With the User Directory Software Blade, you can create user definitions on a(n) _____ Server.

A. SecurID
B. LDAP
C. NT domain
D. SMTP

Answer: B

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

NEW QUESTION 357
Name the authentication method that requires token authenticator.

A. SecureID
B. Radius
C. DynamicID
D. TACACS

Answer: A

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

NEW QUESTION 358
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-215.81 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-215.81 Product From:

https://www.2passeasy.com/dumps/156-215.81/

Money Back Guarantee

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