CheckPoint

Exam Questions 156-215.81

Check Point Certified Security Administrator R81

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
What are the two types of NAT supported by the Security Gateway?

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

Answer: B

Explanation:
A Security Gateway can use these procedures to translate IP addresses in your network:

NEW QUESTION 2
Which statement is NOT TRUE about Delta synchronization?

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

Answer: A

NEW QUESTION 3
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 4
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 5
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 6
You are the Check Point administrator for Alpha Corp. You received a call that one of the users is unable to browse the Internet on their new tablet which is connected to the company wireless, which goes through a Check Point Gateway. How would you review the logs to see what is blocking this traffic?

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

Answer: D

NEW QUESTION 7
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 8
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 9
Which tool allows you to monitor the top bandwidth on smart console?

A. Logs & Monitoring
B. Smart Event
C. Gateways & Severs Tab
D. SmartView Monitor

Answer: D

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

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
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 11
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 12
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 17
Which command shows the installed licenses?

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

Answer: A

NEW QUESTION 18
Fill in the blanks: The _____ collects logs and sends them to the _____.

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

Answer: D

Explanation:
Gateways send their logs to the log server.

NEW QUESTION 23
What is the SOLR database for?

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

Answer: A

NEW QUESTION 25
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 28
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 33
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 35

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 39
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 40
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 42
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 45
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 48
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 49
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 50
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 55
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 59
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 62
What is the purpose of Captive Portal?

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

Answer: C

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

NEW QUESTION 64
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 68
In _____ NAT, the _____ is translated.

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

Answer: A

NEW QUESTION 73
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 78
Choose what BEST describes users on Gaia Platform.

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

Answer: A

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

NEW QUESTION 83
You are the Check Point administrator for Alpha Corp with an R80 Check Point estate. You have received a call by one of the management users stating that they are unable to browse the Internet with their new tablet connected to the company Wireless. The Wireless system goes through the Check Point Gateway. How do you review the logs to see what the problem may be?

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

Answer: B

NEW QUESTION 88
Which message indicates IKE Phase 2 has completed successfully?

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

Answer: A

NEW QUESTION 93
Which of the following is considered a "Subscription Blade", requiring renewal every 1-3 years?

A. IPS blade
B. IPSEC VPN Blade
C. Identity Awareness Blade
D. Firewall Blade

Answer: A

NEW QUESTION 97
Which part of SmartConsole allows administrators to add, edit delete, and clone objects?

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

Answer: D

NEW QUESTION 101
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 102
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 104
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 109
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 113
Why is a Central License the preferred and recommended method of licensing?

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

Answer: D

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

NEW QUESTION 115
Which of the following commands is used to monitor cluster members in CLI?

A. show cluster state
B. show active cluster
C. show clusters
D. show running cluster

Answer: A

NEW QUESTION 117
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 119
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 124
An administrator can use section titles to more easily navigate between large rule bases. Which of these statements is FALSE?

A. Section titles are not sent to the gateway side.
B. These sections are simple visual divisions of the Rule Base and do not hinder the order of rule enforcement.
C. A Sectional Title can be used to disable multiple rules by disabling only the sectional title.
D. Sectional Titles do not need to be created in the SmartConsole.

Answer: C

Explanation:
Section titles are only for visual categorization of rules.

NEW QUESTION 129
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 132
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 137
Which of the following is NOT a method used by Identity Awareness for acquiring identity?

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

Answer: B

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

NEW QUESTION 138
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 141
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 142
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 145
Which of the following Windows Security Events will NOT map a username to an IP address in Identity Awareness?

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

Answer: D

NEW QUESTION 148
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 153
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 157
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 162
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 166
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 168
Which firewall daemon is responsible for the FW CLI commands?

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

Answer: A

NEW QUESTION 171
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 175
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 177
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 179

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

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

Answer: C

NEW QUESTION 184
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 186
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 190
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 192
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 193
Which software blade enables Access Control policies to accept, drop, or limit web site access based on user, group, and/or machine?

A. Application Control
B. Data Awareness
C. Identity Awareness
D. Threat Emulation

Answer: A

NEW QUESTION 194
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 198

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 203
Fill in the blank: An Endpoint identity agent uses a _____ for user authentication.

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

Answer: C

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

NEW QUESTION 208
When configuring Anti-Spoofing, which tracking options can an Administrator select?

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

Answer: A

Explanation:
Configure Spoof Tracking - select the tracking action that is done when spoofed packets are detected: Log - Create a log entry (default)
Alert - Show an alert None - Do not log or alert
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 212
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 213
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 218
Which of the following is NOT a valid configuration screen of an Access Role Object?

A. Users
B. Networks
C. Time
D. Machines

Answer: C

NEW QUESTION 223
When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

A. None, Security Management Server would be installed by itself.
B. SmartConsole
C. SecureClient
D. SmartEvent

Answer: D

NEW QUESTION 228
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 232
Which repositories are installed on the Security Management Server by SmartUpdate?

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

Answer: D

Explanation:
References:

NEW QUESTION 236
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 238
Can you use the same layer in multiple policies or rulebases?

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

Answer: A

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

NEW QUESTION 239
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 244
.....

Relate Links

100% Pass Your 156-215.81 Exam with Exambible Prep Materials

https://www.exambible.com/156-215.81-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/