

CheckPoint

Exam Questions 156-215.82

Check Point Certified Security Administrator - R82



NEW QUESTION 1

What is true of the URL Filtering Software Blade?

- A. It??s part of HTTPS Inspection Policy
- B. It??s part of URL Filtering policy
- C. It??s part of the Access Control Policy
- D. It??s part of Threat Prevention Policy

Answer: C

NEW QUESTION 2

Where is it possible to view SmartConsole locked account?

- A. Administrators list under Permissions & administrators
- B. View Sessions in Gaia portal
- C. View Sessions in SmartConsole
- D. cpview in ssh

Answer: A

Explanation:

The correct verified answer is A. The uploaded answer key shows C, but that is not the correct administrative location for a locked SmartConsole administrator account. Check Point documentation for unlocking administrator accounts states that an administrator with Manage Administrators permission can go to the Manage&Settings view, right-click the locked administrator, and select Unlock Administrator. That points directly to the administrator list under Permissions&Administrators, not the View Sessions page. View Sessions in SmartConsole is for active or saved administrative sessions and session ownership, not primarily for unlocking an administrator account locked by login restrictions. Gaia Portal sessions are Gaia OS sessions, not SmartConsole account lock status. CPView is a monitoring/performance utility, not an administrator account unlock interface. This is an important correction because confusing sessions with administrator-account lockout leads to wrong operational action during a real lockout incident. Reference topics: Administrator Account Management, locked administrators, Manage&Settings, Permissions and Administrators, Unlock Administrator.

NEW QUESTION 3

What is a Security Policy?

- A. A collection of rules and settings that control network traffic and enforce the organization guidelines for data protection.
- B. This is stored on the Security Gateway and enforced by the Security Management Server.
- C. This is a written policy which has to conform with the Regulatory Compliance standards.
- D. This is stored on the Security Management Server and enforced by the log server.

Answer: A

Explanation:

The correct answer is A. In Check Point R82, a Security Policy is the rule-based configuration that controls traffic and enforces organizational security requirements, including access to resources and data protection. The official glossary describes a Security Policy as a collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection. Option B reverses the architecture: the policy is configured and managed on the Security Management Server, then installed on Security Gateways for enforcement. The Security Management Server does not enforce production traffic. Option C describes a governance document, which may influence technical policy design, but it is not what SmartConsole calls a Security Policy. Option D is also wrong because a Log Server stores and processes logs; it does not enforce policy. The Security Gateway is the enforcement component. In CCSA terms, this is foundational: administrators define rules, publish changes, and install the policy to gateways, where traffic is actually inspected and acted upon. Reference topics: Security Policy Management, Access Control Policy, Security Gateway enforcement, SmartConsole policy configuration.

NEW QUESTION 4

Select the correct description of the Identity Collector.

- A. Acquires identities using Identity Agents installed on user endpoint computer
- B. Acquires identities using Identity Agents installed on Active Directory Domain Controllers, Cisco Identity Services Engine Servers or NetIQ eDirectory Servers
- C. Acquire identities from Identity Agents installed on a Windows-based application server that hosts Terminal Servers, Citrix XenAp
- D. and Citrix XenDesktop services
- E. Acquires identities seamlessly from Microsoft Active Directory

Answer: B

NEW QUESTION 5

Which Identity Awareness Client can collect identities from not only Active Directory Domain Controllers, but also from Cisco Identity Services Engine Servers or NetIQ eDirectory Servers?

- A. Identity Agent for a User Endpoint Computer
- B. Identity Agent for a Terminal Server v2
- C. Identity Agent for a Terminal Server
- D. Identity Collector

Answer: D

NEW QUESTION 6

What is the main benefit of Identity Awareness?

- A. It allows you to configure security policy based on the source or destination network and user agent.

- B. It allows you to configure security policy based user or machine identity.
- C. It allows you to configure security policy based on password length
- D. RADIUS group membership and the source operating system.
- E. It allows you to configure security policy based on source network, destination network
- F. LDAP Group membership and source operating system.

Answer: B

NEW QUESTION 7

What are some of the common tasks that the SmartConsole is used for?

- A. Create and manage policies, Monitor logs, Maintain licenses and contracts
- B. Create and manage license
- C. Monitor policies, Maintain performance
- D. Manage all devices on the corporate network, including firewalls, security gateway, switches, routers and load balancers.
- E. Redeploy the management server and gateways during troubleshooting

Answer: A

NEW QUESTION 8

Which tool should be used to display real-time and historical graphical views of traffic and block suspicious network activity while you investigate the traffic?

- A. SmartView Tracker
- B. SmartEvent
- C. SmartView Monitor
- D. SmartView Web Application

Answer: C

Explanation:

The correct answer is C. SmartView Monitor provides real-time and historical graphical views of traffic, system counters, gateway status, and activity. It also supports operational response actions such as blocking specified suspicious traffic while the administrator investigates. Option A, SmartView Tracker, is legacy terminology and not the correct R82 answer for this monitoring function. Option B, SmartEvent, is used for event analysis, correlation, and reporting, but the specific combination of traffic monitoring and immediate blocking during investigation points to SmartView Monitor. Option D, SmartView Web Application, is used for web-based log/report views, not this real-time monitoring and blocking function. The key phrase in the question is "real-time and historical graphical views of traffic" combined with "block suspicious network activity," which maps directly to SmartView Monitor's monitoring and response capabilities. Reference topics: SmartView Monitor, traffic counters, real-time monitoring, blocking specified traffic during investigation.

NEW QUESTION 9

What is a common use case for Application Control and URL Filtering rules?

- A. Block Applications and Inform Users
- B. To create and manage security policies
- C. To install policies
- D. Monitor Applications

Answer: A

NEW QUESTION 10

What is the purpose of the Change Log in SmartConsole?

- A. To install security policies
- B. To manage user sessions
- C. To keep a record of changes made to objects
- D. To monitor network traffic

Answer: C

NEW QUESTION 10

When looking at the Ordered Access Control Layers in the SmartConsole they are organized sequentially. How does the security gateway enforce the rules?

- A. All ordered layers are analyzed in parallel
- B. If there is a matched drop rule in any layer then the traffic is allowed.
- C. After checking each layer the firewall engages the relevant blades and starts to evaluate again one at a time while working with the other access control blades.
- D. Each layer is evaluated independently.
- E. All ordered layers are analyzed in parallel
- F. If there is a matched accept rule in any layer then the traffic is allowed.

Answer: C

NEW QUESTION 15

What is a best practice for managing SmartConsole administrator accounts?

- A. Allow unlimited concurrent sessions
- B. Limit the use of Super User accounts
- C. Use simple passwords
- D. Assign roles based on maximum privilege

Answer: B

NEW QUESTION 20

What is the command line to verify the backup was created?

- A. show backup last-successful
- B. show backup list-successful
- C. show backup successful
- D. show backups

Answer: D

NEW QUESTION 25

By default, alerts about specific security events are sent by which method?

- A. pop-ups
- B. log
- C. SNMP
- D. mail

Answer: A

NEW QUESTION 29

Which of the following is a best practice for policy layers?

- A. Avoid sharing layers across policies
- B. Use only one layer per policy
- C. Disable implicit cleanup rules
- D. Share layers with other policy packages

Answer: D

Explanation:

The correct answer is D. Sharing layers with other policy packages is a best practice when the same set of controls should be reused consistently across multiple policies. Shared layers reduce duplication, support common policy modules, and make governance easier because updates to a shared layer can be maintained centrally. Option A is the opposite of the intended best practice where reuse is appropriate. Option B is too restrictive; one of the benefits of the Check Point layered policy model is the ability to separate network, application, content, or identity logic into manageable layers. Option C is wrong because implicit cleanup behavior exists as part of layer processing; administrators should add explicit cleanup rules for visibility, not try to disable the implicit mechanism. The proper design is modular but controlled: use shared layers where consistency is needed, use ordered and inline layers appropriately, and keep cleanup behavior explicit and logged where possible. Reference topics: Policy Layers, Shared Layers, Ordered Layers, Inline Layers, Access Control policy design.

NEW QUESTION 34

What is the primary purpose of SmartConsole Objects?

- A. To provide out-of-the-box threat prevention
- B. To monitor user activity
- C. To manage network traffic
- D. To simplify and enhance cybersecurity management

Answer: D

Explanation:

The correct answer is D. SmartConsole objects simplify and enhance cybersecurity management by allowing administrators to define reusable representations of assets, networks, users, services, applications, zones, and other entities. Instead of manually entering IP addresses, networks, or services repeatedly in every rule, administrators create objects and reference them throughout the policy. This improves consistency, reduces configuration errors, and makes later changes easier. Option A is wrong because out-of-the-box threat prevention is provided through Threat Prevention blades, protections, profiles, and ThreatCloud updates, not by SmartConsole objects alone. Option B is wrong because monitoring user activity is handled through logging, Identity Awareness, SmartView, and audit/security logs. Option C is too generic; the Security Gateway enforces traffic handling, while objects are management abstractions used to construct policy. The official R82 documentation states SmartConsole is used to configure required objects and policies, and the glossary defines network objects as logical representations used by administrators in Security Policies. That is why the best answer is the broad management value of objects, not enforcement or monitoring by themselves. Reference topics: Object Management, SmartConsole Objects, Managing Objects, Security Policy object reuse.

NEW QUESTION 36

Which statement is a best practice concerning a Cleanup rule?

- A. A Cleanup rule should be placed at the bottom of the rulebase.
- B. A Cleanup rule is optional and not considered Best Practice.
- C. A Cleanup rule could be used to terminate VPN tunnels on purpose.
- D. A Cleanup rule should be placed at the top of the rulebase to increase security and performance alike.

Answer: A

NEW QUESTION 41

What provides the trusted client option in SmartConsole?

- A. IP address(es) allowed to connect to the Gaia Portal

- B. IP address(es) allowed to connect to the Security Management Server using SmartConsole
- C. IP address(es) allowed to connect to the Security Management Server using ssh
- D. IP address(es) allowed to connect to the Security Gateway(s)

Answer: B

Explanation:

The correct answer is B. In Check Point administration, ??trusted clients?? or GUI Clients define which computers are allowed to connect to the Security Management Server using SmartConsole. This is an administrative access-control mechanism for management connectivity, not traffic inspection. The trusted client definition can be a specific IP address, network, address range, or unrestricted ??Any?? setting, depending on how the administrator configures GUI Clients. Option A is wrong because Gaia Portal access is controlled by Gaia OS access and user settings, not SmartConsole trusted clients. Option C is wrong because SSH access is command-line access to Gaia, not SmartConsole GUI access. Option D is wrong because SmartConsole does not normally connect directly to gateways for policy administration; it connects to the management server, which then manages gateways. This feature is important because it reduces the management attack surface by preventing unauthorized administrator workstations from even attempting SmartConsole login to the Security Management Server. Reference topics: Administrator Account Management, GUI Clients, Trusted Clients, SmartConsole management access.

NEW QUESTION 46

What is the purpose of the Explicit Default Cleanup Rule?

- A. To forward unmatched traffic
- B. To accept unmatched traffic
- C. To drop unmatched traffic
- D. To encrypt unmatched traffic

Answer: C

NEW QUESTION 47

What are the valid types of Administrator Accounts?

- A. Gaia account, Operating system account, SmartConsole account
- B. System account, Security Management Server account, SmartConsole account
- C. Gaia account, Security Management Server account, SmartConsole account
- D. Expert account, Security Management Server account, SmartConsole account

Answer: C

Explanation:

The correct answer is C. The valid administrator account types in this context are Gaia account, Security Management Server account, and SmartConsole account. A Gaia account is used for platform administration through Gaia Portal or Gaia Clish. A Security Management Server administrator account controls access to the management database and management functions. A SmartConsole administrator account is used to log in through SmartConsole and perform tasks according to assigned permission profiles. Option A is redundant and less precise because ??Operating system account?? overlaps Gaia but does not name the Security Management Server account type. Option B omits Gaia and uses vague ??System account?? wording. Option D is wrong because Expert is a shell/mode, not a standalone administrator account type. This separation matters because a person may have SmartConsole permissions without Gaia OS access, or Gaia OS access without permission to modify security policies in SmartConsole. Reference topics: Administrator Account Management, Gaia accounts, Security Management Server administrators, SmartConsole administrators.

NEW QUESTION 51

What is the correct default permission profile?

- A. Super Admin
- B. Super Profile
- C. Super Permission
- D. Super User

Answer: D

NEW QUESTION 56

One of the key component of the Three-Tier Architecture of Check Point R82 is:

- A. SmartDashboard
- B. SmartProvisioning
- C. SmartUpdate
- D. SmartConsole

Answer: D

NEW QUESTION 60

What is a best practice when creating custom objects in SmartConsole?

- A. Use inconsistent naming conventions
- B. Edit default objects directly
- C. Clone default objects and edit the clone
- D. Avoid using groups

Answer: C

NEW QUESTION 63

SmartView Web Application is accessed from a web browser with which URL?

- A. <https:// /smartconsole/>
- B. <https:// /smartlog/>
- C. <https://>
- D. <https:// /smartview/>

Answer: D

NEW QUESTION 67

What is one main purpose of URL Filtering?

- A. Automatic translation of foreign web sites into your preferred language.
- B. Specify the application which should be blocked during business hours, such as Facebook-Game, Indeed-Chat, among others.
- C. Synchronizing verdicts on URL Categories for better hit rates.
- D. Use URL Categories to block access to malicious or non-work-related websites.

Answer: D

NEW QUESTION 68

With Autonomous Threat-Prevention, you can choose a profile that best fits your needs. What are the available options?

- A. Perimeter, Cloud North-West, East-West, Lateral Movement, External Network.
- B. Perimeter, Cloud/Data Center, Internal Network, Guest Network
- C. Perimeter, Cloud/Data Center, East-West-Traffic, Guest Network
- D. Perimeter, Fully Overlapping Encryption Domain, Partially Overlapping Encryption Domain, Proper Subset.

Answer: B

NEW QUESTION 70

What is the purpose of the "Fail Mode" setting in HTTPS Inspection?

- A. To enforce strict NAT policies
- B. To define how the gateway handles inspection failures
- C. To disable inspection for internal traffic
- D. To allow only HTTP traffic

Answer: B

NEW QUESTION 71

Which of the following groups represents valid administrator types in the Quantum Security environment?

- A. Quantum global admin, Quantum local admin, Quantum cloud admin
- B. CloudGuard admin, Harmony admin, Infinity admin
- C. Firewall admin, Management admin, OS admin
- D. Gaia admin, Primary SMS admin, SmartConsole admin

Answer: D

Explanation:

The correct answer is D. In a Check Point Quantum Security environment, administrators must distinguish between different administrative scopes. A Gaia admin manages the Gaia operating system through Gaia Portal or Gaia Clish. A Security Management Server administrator manages the security-management database and administrative access. A SmartConsole administrator logs in through SmartConsole to manage objects, policies, gateways, logs, and related security configuration according to permission profile. Option A invents generic ??Quantum global/local/cloud?? labels and is not the official administrator grouping for this CCSA context. Option B mixes Check Point product pillars and portal-level terminology, but it does not describe the core R82 administrator account types in the local Quantum Security environment. Option C is too generic and not official enough; ??firewall admin?? or ??OS admin?? may describe job functions, but not the account categories tested here. The key concept is separation of platform administration from security-management administration. Reference topics: Administrator Account Management, Gaia administrators, Security Management Server administrators, SmartConsole administrator access.

NEW QUESTION 72

Select the correct predefined profile of the Autonomous Threat Prevention.

- A. Hardened
- B. Monitor
- C. Recommended
- D. Optimized

Answer: B

NEW QUESTION 75

Which Identity Awareness client is used in high-volume environments that use Microsoft Active Directory, Cisco Identity Services, NetIQ eDirectory, or Syslog?

- A. Identity Agent for a Terminal Server
- B. Identity Collector
- C. RADIUS Accounting
- D. Identity Agent for a User Endpoint Computer

Answer: B

NEW QUESTION 78

Which of these is one of the Identity Sources used by the Identity Awareness Blade?

- A. Identity Proxy API
- B. LDAP Authentication
- C. RADIUS Accounting
- D. Certificate Enrolment Service (CES)

Answer: C

NEW QUESTION 79

What is the difference between the Access Control policy and NAT policy?

- A. The Access Control policy is a collection of rules that control network acces
- B. The NAT rules can be used to make the gateway change IP addresses and port numbers in packets.
- C. The Access Control policy is an enforced on the Security Gated
- D. The NAT rules are enforced on a separate NAT Gateway.
- E. The Access Control policy is a collection of rules that control application and web site acces
- F. The NAT rules allow or deny connections on the gateway and can also change IP addresses and port numbers in packets.
- G. The Access Control policy is a collection of rules that mostly blocks network acces
- H. The NAT rules are used to allow access through the gatewa
- I. A NAT rule causes the gateway to allow access to or from the IP addresses and translates the packet according to the rule.

Answer: A

NEW QUESTION 83

Which statement best describes Trusted Clients?

- A. These are trusted administrators allowed to connect to the Security Management Server using SmartConsole
- B. These are specific devices or IP addresses allowed to connect to the Security Management Server using SmartConsole
- C. These are Security Gateways allowed to connect to the Security Management Server using SmartConsole
- D. These are trusted users allowed to connect to the Security Management Server using SmartConsole

Answer: B

NEW QUESTION 88

The Objects menu provides more management capabilities than the GATEWAYS & SERVERS New menu. It lets you add all types of custom objects. What other object management tool can the administrator use to manage objects in a separate window?

- A. The Objects Pane
- B. The Categories Explorer
- C. The Object Explorer
- D. The More object types menu

Answer: C

NEW QUESTION 92

What are the key components that make up the Check Point Three-Tier Architecture?

- A. Gaia WebUI Portal, Security Management and Security Gateway installed together on same server
- B. Security Dashboard, Management Database Server, Firewall
- C. Web Security Console, Log Server, Firewall
- D. SmartConsole, Security Management Server, Security Gateway

Answer: D

NEW QUESTION 97

What is a benefit of https inspection?

- A. Blocking sites
- B. Filtering malicious content
- C. Controlling bandwidth
- D. Monitoring applications

Answer: B

Explanation:

The correct answer is B. A direct security benefit of HTTPS Inspection is filtering malicious content inside encrypted traffic. Modern malware delivery, phishing, command-and-control activity, and file downloads often use HTTPS. If the gateway cannot inspect encrypted content, Threat Prevention, Anti-Virus, Threat Emulation, URL Filtering, and Application Control may have reduced visibility. Option A is partially related because URL Filtering can block sites, but site blocking is not the main technical benefit of HTTPS Inspection itself. Option C is wrong because bandwidth control is not the purpose of HTTPS Inspection. Option D is also only partially related: inspection can improve application visibility, but the stronger security answer is malicious-content filtering. HTTPS Inspection enables deeper inspection by decrypting traffic according to policy, applying security blades, and then re-encrypting traffic. Reference topics: HTTPS Inspection, Threat Prevention with HTTPS traffic, malicious content filtering, encrypted traffic visibility.

NEW QUESTION 98

What methods could be used with Custom Queries for querying logs?

- A. The syntax consists of Boolean operators, wildcards, fields and ranges.
- B. The syntax is referred to as PCRE which stands for Perl compatible Regular Expression.
- C. The syntax has to be converted into BASE64 format to randomize some security- relevant parameters.
- D. The syntax is the same as used in fw monitor or tcpdump.

Answer: A

NEW QUESTION 100

Which of the following best describes how Access Role objects enhance identity-based policies in SmartConsole?

- A. They store logs of user activity for auditing
- B. They replace the need for traditional firewall rules
- C. They allow grouping of users, computers, and networks into a single rule condition
- D. They authenticate users before granting access

Answer: C

NEW QUESTION 104

What are the different types of Policy Layers supported in an Access Control Policy?

- A. Ordered Layers - Inline Layers
- B. Static Policy Layers - Updateable Policy Layers
- C. Global Access Layers - Exception Layers
- D. Firewall Layers - Application Layers - Content Layers

Answer: A

NEW QUESTION 106

Select one of the Common Types of Policies.

- A. Content Awareness
- B. Application & URL Filtering
- C. Firewall
- D. Access Control

Answer: D

NEW QUESTION 109

Which menu in SmartConsole provides the most comprehensive object management capabilities?

- A. Rule menu
- B. Object Explorer
- C. Objects menu
- D. New menu

Answer: B

Explanation:

The correct answer is B. Object Explorer provides the most comprehensive object-management capability in SmartConsole. While the Objects menu can create many object types and the New menu under Gateways&Servers is useful for infrastructure objects, Object Explorer is the broader management interface for searching, filtering, viewing, editing, importing, exporting, and organizing objects. Option A is wrong because the Rule menu is tied to rulebase operations, not full object lifecycle management. Option C is useful but less comprehensive than Object Explorer because it is primarily a menu-based creation and access point. Option D is too limited; ??New?? creates objects in a specific context but does not provide the full object inventory and management window. For larger CCSA/R82 environments, Object Explorer is the correct tool when the administrator needs a central view of object categories, object relationships, and object-management actions. Reference topics: Object Management, Object Explorer, SmartConsole object lifecycle, CSV import/export.

NEW QUESTION 110

Which tool provides a graphical interface for centralized management of the Check Point Security environment?

- A. Gaia Portal
- B. Security Management Server
- C. SmartConsole
- D. SmartEvent

Answer: C

NEW QUESTION 114

In addition to the ability to add New objects, the Object Explorer lets you:

- A. Export one or more objects to the JSON file
- B. Import one or more objects from the JSON file
- C. Import/Export one or more objects from the CSV file

D. Export one or more objects to the CSV file

Answer: C

Explanation:

The correct answer is C. Object Explorer supports importing and exporting objects using CSV files. This capability is useful for bulk object administration, object inventory review, object migration preparation, and consistency checks across environments. Option A is incomplete and uses JSON rather than the tested CSV capability. Option B is also JSON-based and therefore incorrect for this question. Option D is partially correct because export to CSV is supported, but the more complete answer is import/export from CSV. In real administration, CSV import/export is valuable when many hosts, networks, or service objects must be reviewed or moved in a controlled way. It is not a substitute for understanding policy dependencies, but it is a powerful object-management feature. Reference topics: Object Explorer, CSV import/export, SmartConsole object management, bulk object administration.

NEW QUESTION 116

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

156-215.82 Practice Exam Features:

- * 156-215.82 Questions and Answers Updated Frequently
- * 156-215.82 Practice Questions Verified by Expert Senior Certified Staff
- * 156-215.82 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 156-215.82 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 156-215.82 Practice Test Here](#)